



FortiManager - Release Notes

Version 6.2.8

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/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



December 10, 2021

FortiManager 6.2.8 Release Notes

02-628-717614-20211210

TABLE OF CONTENTS

Change Log	6
FortiManager 6.2.8 Release	7
Supported models	7
Special Notices	8
VPN Manager in a Fabric type ADOM	8
Multi-step firmware upgrades	8
Newly deployed, factory reset, or disk format may trigger upgrade code on subsequent reboot	8
Multicast policies with zones or zone members	8
Wildcard Address Support in Policy	9
Import Authentication Rules and Schemes	9
Support of the NGFW mode in 6.2.1	9
Managing FortiGate with VDOMs that use Global, Shared Profiles	9
Managing FortiAnalyzer Devices	10
IOC Support on FortiManager	10
Hyper-V FortiManager-VM running on an AMD CPU	10
SSLv3 on FortiManager-VM64-AWS	10
Upgrade Information	11
Unintended downgrade of FortiGate units	11
Downgrading to previous firmware versions	11
Firmware image checksums	11
FortiManager VM firmware	12
SNMP MIB files	13
Product Integration and Support	14
FortiManager 6.2.8 support	14
Web browsers	14
FortiOS/FortiOS Carrier	15
FortiAnalyzer	15
FortiAuthenticator	15
FortiCache	16
FortiClient	16
FortiMail	16
FortiSandbox	16
FortiSwitch ATCA	16
FortiWeb	17
FortiDDoS	17
Virtualization	17
Feature support	17
Language support	18
Supported models	19
FortiGate models	19
FortiGate special branch models	22

FortiCarrier models	23
FortiDDoS models	24
FortiAnalyzer models	25
FortiMail models	25
FortiSandbox models	26
FortiSwitch ATCA models	27
FortiSwitch models	27
FortiWeb models	27
FortiCache models	29
FortiProxy models	29
FortiAuthenticator models	29
Compatibility with FortiOS Versions	30
FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues	30
FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues	30
FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues	31
FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues	31
FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues	31
FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues	31
FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues	32
FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues	32
FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues	32
FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues	33
FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues	33
Resolved Issues	34
AP Manager	34
Device Manager	34
FortiSwitch Manager	36
Global ADOM	36
Others	36
Policy and Objects	37
Revision History	38
Script	38
Services	38
System Settings	39
VPN Manager	39
Common Vulnerabilities and Exposures	40
Known Issues	41
AP Manager	41
Device Manager	41
FortiSwitch Manager	41
Policy & Objects	42
Revision History	42
Script	43
Services	43
System Settings	43

Appendix A - FortiGuard Distribution Servers (FDS)	44
FortiGuard Center update support	44

Change Log

Date	Change Description
2021-05-13	Initial release of 6.2.8.
2021-06-04	Updated FortiOS/FortiOS Carrier on page 15.
2021-06-17	Updated Resolved Issues on page 34 and Known Issues on page 41.
2021-07-14	Updated FortiGate special branch models on page 22.
2021-07-20	Updated Resolved Issues on page 34.
2021-07-22	Updated FortiClient on page 16.
2021-08-10	Updated FortiGate models on page 19.
2021-08-20	Updated FortiOS/FortiOS Carrier on page 15 and FortiMail on page 16.
2021-08-30	Updated FortiAuthenticator models on page 29.
2021-12-10	Updated FortiGate models on page 19.

FortiManager 6.2.8 Release

This document provides information about FortiManager version 6.2.8 build 1435.



The recommended minimum screen resolution for the FortiManager 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 7](#)

Supported models

FortiManager version 6.2.8 supports the following models:

FortiManager	FMG-200D, FMG-200F, FMG-300E, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.2.8.

VPN Manager in a Fabric type ADOM

After Upgrading to FortiManager 6.2.8, the VPN Manager may fail to install to any device participating in a full mesh VPN.

Customers using VPN Manager in a fabric type ADOM should not upgrade to 6.4.4 until the issue is resolved.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

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 FortiManager 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 FortiManager units upgraded from versions prior to 6.2.3.

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

Multicast policies with zones or zone members

Starting in FortiManager 6.0.7 and 6.2.1, multicast policies in ADOMs with version 5.6 or earlier cannot reference zones or zone members. Either upgrade the ADOM to 6.0 or later, or remove references to zones or zone members.

Wildcard Address Support in Policy

With FortiOS 6.2.2 defines all wildcard address objects as regular address objects with type set as FQDN, FortiManager 6.2.2 can only select FQDN type address in policy and install to FortiOS 6.2.2 devices.

Import Authentication Rules and Schemes

If `kerberos-keytab` user is referenced in `config authentication scheme > set kerberos-keytab`, FortiManager purges the authentication scheme and authentication rule after upgrading to FortiManager 6.2.1 and later. After upgrading, import the authentication rule and authentication scheme from FortiOS to the FortiManager ADOM before modifying and installing any configurations to FortiOS.

Support of the NGFW mode in 6.2.1

Within a version 6.2 ADOM, policy package with NGFW mode set as policy based only supports FortiOS 6.2.1.

Managing FortiGate with VDOMs that use Global, Shared Profiles

FortiManager managing FortiGates with global, shared g-xx profiles in VDOMs and running FortiOS 6.0.0 or later is unable to import global, shared g-xx profiles from FortiGate devices.

Before adding the FortiGate units to FortiManager, perform the following steps to unset the global ADOM objects. After the default configurations are unset, you can successfully add the FortiGate units to FortiManager.

1. On the Fortigate for each VDOM, unset the following global ADOM objects by using the CLI:

```
config wireless-controller utm-profile
  edit "wifi-default"
    set comment "Default configuration for offloading WiFi traffic."
  next
  edit "g-wifi-default"
    set comment "Default configuration for offloading WiFi traffic."
    set ips-sensor "g-wifi-default"
    set application-list "g-wifi-default"
    set antivirus-profile "g-wifi-default"
    set webfilter-profile "g-wifi-default"
    set firewall-profile-protocol-options "g-wifi-default"
    set firewall-ssl-ssh-profile "g-wifi-default"
  next
end

FGVMULCV30310000 (utm-profile) # ed g-wifi-default
FGVMULCV30310000 (g-wifi-default) # sh
config wireless-controller utm-profile
  edit "g-wifi-default"
```

```
        set comment "Default configuration for offloading WiFi traffic."
    next
end
```

2. After the global ADOM objects are unset, you can add the FortiGate unit to FortiManager.

Managing FortiAnalyzer Devices

FortiManager 6.2 can only manage and process logs for FortiAnalyzer 6.2 devices.

IOC Support on FortiManager

Please note that FortiManager does not support IOC related features even when FortiAnalyzer mode is enabled.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-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 FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-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 FortiManager 6.0.3 or later directly to 6.2.8.



For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

- [Unintended downgrade of FortiGate units on page 11](#)
- [Downgrading to previous firmware versions on page 11](#)
- [Firmware image checksums on page 11](#)
- [FortiManager VM firmware on page 12](#)
- [SNMP MIB files on page 13](#)

Unintended downgrade of FortiGate units

An incorrect calculation of the upgrade path by FortiManager 6.2.2 using the *Device Manager > Firmware* page may inadvertently result in the FortiGate unit being downgraded to an earlier FortiOS version. Customers must upgrade their FortiManager units to 6.2.3 first and then perform the upgrade of the FortiGate units.

Downgrading to previous firmware versions

FortiManager 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. In addition the local password is erased.

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 | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```

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>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager 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 FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager 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 FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager 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 FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager 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 `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager 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, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager 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 the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtualappliances.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 FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 6.2.8 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.2.8 support on page 14](#)
- [Feature support on page 17](#)
- [Language support on page 18](#)
- [Supported models on page 19](#)

FortiManager 6.2.8 support

This section identifies FortiManager 6.2.8 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 16](#)
- [FortiClient on page 16](#)
- [FortiMail on page 16](#)
- [FortiSandbox on page 16](#)
- [FortiSwitch ATCA on page 16](#)
- [FortiWeb on page 17](#)
- [FortiDDoS on page 17](#)
- [Virtualization on page 17](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



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

Web browsers

This section lists FortiManager 6.2.8 product integration and support for web browsers:

- Microsoft Edge80 (80.0.361 or later)
- Mozilla Firefox version 88
- Google Chrome version 90

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier

This section lists FortiManager 6.2.8 product integration and support for FortiOS/FortiOS Carrier:

FortiOS or FortiOS Carrier		Compatibility Issues
6.2	6.2.0 to 6.2.9	
6.0	6.0.0 to 6.0.13	See FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues on page 30 . See FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues on page 30 . See FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 31 .
5.6	5.6.0 to 5.6.13	See FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues on page 31 . See FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 31 . See FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 31 . See FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 32 . See FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 32 .
5.4	5.4.1 to 5.4.13	See FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 32 . See FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 33 . See FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 33 .

FortiAnalyzer

This section lists FortiManager 6.2.8 product integration and support for FortiAnalyzer:

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

FortiAuthenticator

This section lists FortiManager 6.2.8 product integration and support for FortiAuthenticator:

- 6.0 to 6.3
- 5.0 to 5.5
- 4.3

FortiCache

This section lists FortiManager 6.2.8 product integration and support for FortiCache:

- 4.2.9
- 4.2.7
- 4.2.6
- 4.1.6
- 4.1.2
- 4.0.4

FortiClient

This section lists FortiManager 6.2.8 product integration and support for FortiClient:

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

FortiMail

This section lists FortiManager 6.2.8 product integration and support for FortiMail:

- 6.2.7
- 6.0.10
- 5.4.10
- 5.3.13

FortiSandbox

This section lists FortiManager 6.2.8 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 FortiManager 6.2.8 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.2.8 product integration and support for FortiWeb:

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

FortiDDoS

This section lists FortiManager 6.2.8 product integration and support for FortiDDoS:

- 5.1.0
- 5.0.0
- 4.7.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see [Feature support on page 17](#).

Virtualization

This section lists FortiManager 6.2.8 product integration and support for virtualization:

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

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

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

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.2.8.



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

This section contains the following topics:

- [FortiGate models on page 19](#)
- [FortiGate special branch models on page 22](#)
- [FortiCarrier models on page 23](#)
- [FortiDDoS models on page 24](#)
- [FortiAnalyzer models on page 25](#)
- [FortiMail models on page 25](#)
- [FortiSandbox models on page 26](#)
- [FortiSwitch ATCA models on page 27](#)
- [FortiWeb models on page 27](#)
- [FortiCache models on page 29](#)
- [FortiProxy models on page 29](#)
- [FortiAuthenticator models on page 29](#)

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FG-401E-DC, 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-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E-DC, FortiGate-3401E, FortiGate-3401E-DC, 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	6.2

Model	Firmware Version
FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, 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-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, FortiGateRugged-90D FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-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-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-401E-DC, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E FortiGate 5000 Series: FG-5001D, FG-5001E, FG-5001E1 FortiGate DC: FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC FortiGate Hardware Low Encryption: FG-100D-LENC, FG-600C-LENC Note: All license-based LENC is supported based on the FortiGate support list. FortiWiFi: FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-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-61E, FWF-90D, FWF-90D-POE, FWF-92D	6.0

Model	Firmware Version
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	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1 FortiGate 6000 Series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiGate 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC, FG-7060E-8-DC FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC Note: All license-based LENC is supported based on the FortiGate support list. FortiWiFi: FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FGT-300D, FG-400D, FG-500D, 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 FortiGate 5000 Series: FG-5001C, FG-5001D (Update only) FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC, FG-7060E-8-DC	5.4

Model	Firmware Version
FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC	
Note: All license-based LENC is supported based on the FortiGate support list.	
FortiWiFi: FWF-30D, FWF-30D-POE, FWF-30E, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE	
FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM	
FortiGate Rugged: FGR-60D, FGR-90D	

FortiGate special branch models

The following FortiGate models are released on a special branch of FortiOS. FortiManager supports these models.

Model	Firmware Version
FortiGate: FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-200F, FortiGate-201F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4400F, FortiGate-4401F FortiGate Rugged: FortiGateRugged-90D	6.2
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1101E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiGate DC: FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC FortiGate VM: FortiGate-VM64-RAXONDEMAND FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60F, FortiWiFi-61F	6.0
FortiGate: FortiGate-60E-DSL, FortiGate-60E-DSLJ FortiGate 5000 Series: FortiGate-5001E1 FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiWiFi: FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ	5.6

Model	Firmware Version
FortiGate: FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-500E, FortiGate-501E, FortiGate-2000E, FortiGate-2500E, FortiGate-3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1 FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F FortiGate 7000 Series: FortiGate-7030EFG-7030E-Q, FortiGate-7000E, FortiGate-7030E-S, FortiGate-7040E-1, FortiGate-7040E-2, FortiGate-7040E-3, FortiGate-7040E-4, FortiGate-7040E-5, FortiGate-7040E-6, FortiGate-7040E-8, FortiGate-7040E-8-DC, FortiGate-7060E-1, FortiGate-7060E-2, FortiGate-7060E-3, FortiGate-7060E-4, FortiGate-7060E-5, FortiGate-7060E-6, FortiGate-7060E-8 FortiWiFi: FortiWiFi-50E-2R, FortiWiFi-60E, FortiWiFi-61E, FortiWiFi-92D, FortiWiFi-60E-DSL FortiGate VM: FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-OPC FortiGate Rugged: FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D	5.4

FortiCarrier models

Model	Firmware Version
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-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F FortiCarrier-7000 series: FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, 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 FortiGate 6000 series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC	6.0

Model	Firmware Version
FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E FortiCarrier 6000 Series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-3810D-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FG-3600E, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E FortiCarrier 6000 Series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-3810D-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4

FortiDDoS models

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

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: 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
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: 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.	6.0
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).	
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.	5.6
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).	
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.	5.4
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.	
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
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	

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0

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

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox-VM: FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ATCA models

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

FortiSwitch models

Model	Firmware Version
FortiSwitch: FortiSwitch-108D-POE, FortiSwitch-108D-VM, FortiSwitch-108E, FortiSwitch-108E-POE, FortiSwitch-108E-FPOE, FortiSwitchRugged-112D-POE, FortiSwitch-124D, FortiSwitch-124D-POE, FortiSwitchRugged-124D, FortiSwitch-124E, FortiSwitch-124E-POE, FortiSwitch-124E-FPOE, FortiSwitch-224D-POE, FortiSwitch-224D-FPOE, FortiSwitch-224E, FortiSwitch-224E-POE, FortiSwitch-224E-FPOE, FortiSwitch-248D, FortiSwitch-248D-POE, FortiSwitch-248D-FPOE, FortiSwitch-248E-POE, FortiSwitch-248E-FPOE, FortiSwitch-424D, FortiSwitch-424D-POE, FortiSwitch-424D-FPOE, FortiSwitch-448D, FortiSwitch-448D-POE, FortiSwitch-448D-FPOE, FortiSwitch-448E, FortiSwitch-448E-POE, FortiSwitch-448E-FPOE, FortiSwitch-524D, FortiSwitch-524D-FPOE, FortiSwitch-548D, FortiSwitch-548D-FPOE, FortiSwitch-1024D, FortiSwitch-1048D, FortiSwitch-1048E, FortiSwitch-3032D, FortiSwitch-3632D	N/A There is no fixed supported firmware versions. If FortiGate supports it, FortiManager will support it.

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E 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-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVR	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-600D	5.9.1

Model	Firmware Version
FortiWeb VM: FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

FortiCache models

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

FortiProxy models

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

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	6.0 to 6.3
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-2000E, FAC-3000B, FAC-3000D, FAC-3000E	4.3
FortiAuthenticator VM: FAC-VM	

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.2.8. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.0	<ul style="list-style-type: none">• FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues on page 30• FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues on page 30• FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 31
FortiOS 5.6	<ul style="list-style-type: none">• FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues on page 31• FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 31• FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 31• FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 32• FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 32
FortiOS 5.4	<ul style="list-style-type: none">• FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 32• FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 33• FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 33

FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 6.2.3 and FortiOS 6.0.9.

FortiManager 6.2.3 does not support the following FortiOS syntax:

```
log fortianalyzer-cloud filter
log fortianalyzer-cloud override-filter
log fortianalyzer-cloud override-setting
log fortianalyzer-cloud setting
log fortiguard setting
    conn-timeout (attr)
```

FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues

The following syntax introduced in FortiOS 6.0.8 is not directly supported by FortiManager 6.2.3.

```
config system fortiguard
    set protocol {protocol}
end
```

In order to set the protocol used for FortiGuard communications by the FortiGate, either configure it on the FortiGate directly or by running a CLI script on “Remote FortiGate Directly”.

FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager 6.0.2 and FortiOS 6.0.3.

Bug ID	Description
516113	Install verification may fail on policy status field. For details, see the following Special Notice: Special Notices on page 8 .
516242	Install verification may fail on the wtp profile's <code>handoff-sta-thresh</code> parameter.

FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues

The following syntax introduced in FortiOS 5.6.12 is not directly supported by FortiManager 6.2.3.

```
config system fortiguard
    set protocol {protocol}
end
```

In order to set the protocol used for FortiGuard communications by the FortiGate, either configure it on the FortiGate directly or by running a CLI script on "Remote FortiGate Directly".

FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager 5.6.5 and FortiOS 5.6.6.

Bug ID	Description
513066	FortiManager 5.6.5 does not support the following new value in FortiOS 5.6.6: <code>system sdn-connector</code> command with the <code>azure-region</code> variable set to <code>germany usgov local</code> . If set on FortiGate, the values will be unset during the next configuration installation from FortiManager.
513069	FortiManager 5.6.5 does not support the following new value in FortiOS 5.6.6: <code>system snmp user</code> command with the <code>community events</code> variable set to <code>av-oversize-blocked</code> or <code>faz-disconnect</code> . If set on FortiGate, the values will be unset during the next configuration installation from FortiManager.

FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.6.3 and FortiOS 5.6.4.

Bug ID	Description
486921	<p>FortiManager may not be able to support the syntax for the following objects:</p> <ul style="list-style-type: none"> • <code>rsso-endpoint-block-attribute</code>, <code>rsso-endpoint-block-attribute</code>, or <code>sso-attribute</code> for RADIUS users. • <code>sdn</code> and its <code>filter</code> attributes for firewall address objects. • <code>azure</code> SDN connector type. • <code>ca-cert</code> attribute for LDAP users.

FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.6.1 and FortiOS 5.6.3.

Bug ID	Description
469993	FortiManager has a different default value for <code>switch-controller-dhcp-snooping</code> from that on FortiGate.

FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1.

Bug ID	Description
451036	FortiManager may return verification error on <code>proxy enable</code> when installing a policy package.
460639	FortiManager may return verification error on <code>wtp-profile</code> when creating a new VDOM.

FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.4.5 and FortiOS 5.4.10.

Bug ID	Description
508337	<p>FortiManager cannot edit the following configurations for replacement message:</p> <ul style="list-style-type: none"> • <code>system replacemsg mail "email-decompress-limit"</code> • <code>system replacemsg mail "smtp-decompress-limit"</code> • <code>system replacemsg nntp "email-decompress-limit"</code>

FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.6.3 and FortiOS 5.4.9.

Bug ID	Description
486592	FortiManager may report verification failure on the following attributes for RADIUS users: rsso-endpoint-attribute rsso-endpoint-block-attribute sso-attribute

FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.4.4 and FortiOS 5.4.8.

Bug ID	Description
469700	FortiManager is missing three wtp-profiles: FAP221E, FAP222E, and FAP223E.

Resolved Issues

The following issues have been fixed in 6.2.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
591994	AP region settings may be unset in central management mode.
648812	DHCP server is incorrectly created for <i>Bridge SSID</i> .
674636	SSID may be empty on <i>AP Manager > WiFi Profiles > SSID</i> column.
692911	FortiManager may not be able to display correct information for wireless radio in wireless profile for FortiWiFi-80F-2R.

Device Manager

Bug ID	Description
485037	<i>Monitor > Map View</i> may fail if proxy is enabled.
575215	When creating a new interface for a VDOM, FortiManager may list interfaces that may belong to another ADOM.
594211	FortiManager should be able to create new VLAN interface on the fabric interface and install to FortiGate.
603820	FortiManager fails to import a policy when <i>reputation-minimum</i> and <i>reputation-direction</i> are set.
610585	Device Manager cannot save <i>DHCP for Unknown MAC address</i> with action sets to <i>block</i> .
624325	Creating or editing a transparent VDOM to disable may stall at 20%.
631842	FortiGuard Scheduled Updates <i>Hours</i> field may not be saved after clicking <i>Apply</i> .
636012	Importing policy may report conflict for the default SSH CA certificates.
642362	Under <i>Workflow</i> mode, <i>config status</i> may change to <i>Modified</i> when the session has not changed.
646537	Under <i>System > Explicit Proxy</i> , the multiple selections for listen on interfaces may not be saved.

Bug ID	Description
654190	FortiManager should not modify <i>IPv4 addressing mode</i> when <i>IPv6 addressing mode</i> is changed.
654611	Under <i>Advanced</i> mode and within a VDOM, clicking <i>Device Manager</i> on the top menu returns the <i>No Permission</i> error.
656433	FortiManager device delete process may stall.
658832	FortiManager is unable to retrieve <i>priority-members</i> if the outgoing interface is using the <i>Manual strategy</i> in SD-WAN rule.
662656	When importing policies contain <i>policy block</i> or <i>global policy</i> , import wizard should give a warning that those policies will not be imported.
665344	User with full Read/Write DVM privileges should be allowed to see and modify the <i>System Provisioning Templates</i> .
666634	FortiManager may fail to import GCP SDN connector object.
667142	FortiManager is unable to edit or hover mouse over <i>OSPF route</i> after the seventh line.
667738	GUI should generate an error message when using invalid IP address or special characters in interface name.
667826	Device Manager may show <i>No entry found</i> with <code>rtmmond</code> and security console crashes.
668958	After enabling <i>DHCP rely</i> on one interface, DHCP server is disabled on another interface during install.
670535	Install fails when creating a new DHCP reservation due to missing MAC address.
670839	FortiManager should be able to configure <i>IPSec Phase2</i> selector using the same IP range.
673008	SD-WAN Rules order changes to the default when creating a rule and moving it to the top.
677241	Interface speed is set incorrectly on <i>port group</i> due to missing aggregate membership verification.
678066	Install may fail when changing FortiGate admin password from FortiManager.
678495	FortiManager VPN L2TP may prompt <i>invalid ip range</i> message.
680516	<i>Host Name</i> is truncated when name has more than 31 characters.
683411	FortiManager may not display a FortiGate under the <i>Device Manager > Managed Devices</i> .
684372	When using VDOMs, <i>Policy Package</i> status remains in modified status after using <i>Push to device</i> .
684462	FortiManager truncates the device configuration when downloading from <i>View configuration</i> option.
686144	SD-WAN monitor table view may not match the FortiGate performance SLA monitor.
688470	When importing policy, the <i>interface zone</i> , <i>intra-zone</i> , may not import to ADOM database.
688972	SD-WAN rules may lose all interface members after upgrade.

Bug ID	Description
689014	FortiManager may return an error when changing FortiGate device log configuration from FortiManager with management VDOM moved to another VDOM.
690012	Changing the value of a meta-data field for a device should trigger the change with configuration status.
690566	Changes to the <i>Disclaimer Page</i> may not be saved with error.
696848	Users may not be able to retrieve configuration or import policy from managed devices with <code>dvmcore</code> constantly crashing.
697924	When there are many devices, all managed FortiGates may show connection down state.

FortiSwitch Manager

Bug ID	Description
676739	FortiManager may not be able to delete VLAN interfaces created by FortiSwitch Manager.
708901	The assigned FortiSwitch template name that has more than sixteen characters may fail the ADOM integrity check.

Global ADOM

Bug ID	Description
632400	When installing global policy, FortiManager may delete policy routes and settings on an ADOM.
667423	Assigned header policy from the global ADOM shows up on excluded policy package.
670280	Promoting the <i>Profile Group</i> object should not promote the default <i>Protocol</i> option.

Others

Bug ID	Description
615315	FortiManager may fail to pull docker from registry server with inode exhausted.
656956	There may be crashes with <code>rtmmond</code> when FortiWLM is enabled.
667421	FortiManager may report repeated <code>miglogd</code> crashes which causes log loss.
670479	FortiManager configuration file size may be large due to a bulk of <i>resync</i> files.

Bug ID	Description
671444	FortiManager may fail to check-in configuration revision with the HA secondary unit.
681625	The <code>svc cdb</code> reader process may crash during upgrade of ADOM.
682404	The <code>rtmmond</code> process memory usage may increase constantly.
683841	FortiManager databases may randomly lose integrity.
688188	HA re-transmission may not work and crash.
691568	FortiManager GUI may randomly becomes non responsive.
695549	The <code>_created</code> timestamp is missing in REST API return data for policy.
697132	In some occasions, FortiManager is not accessible until the device is rebooted every couple of days.
706516	Security console may crash when there are quotation marks around the group name.

Policy and Objects

Bug ID	Description
523350	FortiManager does not show the default certificate under <i>SSL/SSH Inspection</i> within the policy.
587634	FortiManager may not be able to create new wildcard FQDN type address to FortiGate 6.2.
612317	FortiManager shows the incorrect country code for <i>Cyprus</i> under <i>User definition</i> .
630431	Some application and filter overrides are not displayed on GUI.
631372	Setting <code>server-cert-mode</code> to <code>replace</code> may cause install failure if <code>inspect-all</code> is <code>certificate-inspection</code> .
633727	FortiManager is unable to display summary of policy package diff for VDOM with a long name.
651991	After adding and removing Security Profile, policy Security Profile changes from <i>no-inspection</i> to empty.
660483	IPS signatures may not match between FortiGate and FortiManager.
675199	Local web category override is not installed if the web filter is part of policy block package.
677385	IPS profile may not load.
686913	Default entry "1" under the <i>Intrusion Prevention > IPS Signatures and Filters</i> may not be visible in the GUI.
687460	The same filter may behave differently between <i>source address</i> and <i>destination address</i> .
688336	Find and replace may not work for security profiles.

Revision History

Bug ID	Description
657344	Installing from 6.0 ADOM may try to <i>unset inspection-mode</i> and <i>unset ssl-ssh-profile</i> on FortiGate 6.2.
660525	Installing from FortiManager may unset <i>comment</i> , <i>organization</i> , and <i>subnet-name</i> during install.
662438	FortiManager may try to purge all web rating override entries.
667148	When a policy install is performed, <i>Install preview</i> shows lot of firewall policies with metafield changes without any actual change been done.
675867	The <code>ssl-anomaly-log</code> configuration may be incorrectly pushed by FortiManager when installing 5.6 ADOM policy to 6.0 FortiGate.
677659	FortiManager may fail to retrieve device configuration on web category with log threat-weight.
679139	When a policy package is shared between many firewalls, web rating override purge may fail in some scenarios.
686036	FortiManager may remove <i>allow access</i> configurations for secondary IP when a policy package is installed.
691240	FortiManager should not unset the value <i>forward-error-correction</i> with certain FortiGate platforms.
693225	FortiManager may install <code>unset inspection-mode</code> to FortiGate 6.2 device in 6.0 ADOM.
694380	Installation may fail when <code>set whitelist enable</code> in <code>ssl-ssh-profile</code> is pushed to FortiGate 6.2 from a in 6.0 ADOM.
709456	FortiManager may be missing configuration revisions after performed HA failover.

Script

Bug ID	Description
669198	Running a script in <i>Policy & Objects</i> does not update <i>Save</i> status.

Services

Bug ID	Description
587730	FortiGate-VM64-AZURE may not be listed in firmware image page.

Bug ID	Description
680857	FortiExtender, FortiAP, or FortiSwitch upgrades can fail due to custom image being deleted during or after a failed upgrade.
694903	Some firmware upgrade paths may have issues.
695685	FortiGate HA firmware upgrade may fail when both HA units need disk check.
699768	FortiManager should add <i>06002000NIDS02504 extend IPS database</i> to default download list.
714596	For web filter query, FortiManager should support <i>category 9</i> mapping data.
714787	FortiManager should have a <code>diagnose</code> command to force web filtering database merge.

System Settings

Bug ID	Description
631733	Changing <i>trusted IP</i> can be saved and installed.
637377	If <i>Manage Device Configurations</i> is <i>none</i> in admin profile, user may not be able to see interface in policy.
642205	While FortiAnalyzer model is disabled, FortiManager may fail to create an ADOM due to oversize with disk quota.
660226	HA may crash when upgrading.
662970	Firewall addresses may not be visible on GUI after upgrading FortiManager.
677461	FortiManager is not able to identify ADOMs that are locked by none super user administrators.
687223	Users may not be able to upgrade ADOM because of <code>profile-protocol-options</code> .
690921	ADOM upgrade from 6.0 to 6.2 should not add custom <code>ssl-ssh-profile</code> to policies which were not configured for SSL inspection.

VPN Manager

Bug ID	Description
596953	Going to <i>VPN manager > Monitor</i> , and selecting a specific community from the tree menu to show only that community's tunnels, the monitor page displays a white screen.
608221	There is no <i>XAUTH USER</i> column in VPN Manager Monitor.
620801	<i>SSLVPN > Edit SSLVPN Settings > IP Range</i> only shows configuration from ADOM database objects.
681110	VPN manager may not push any configuration on ADOM 6.0 for <i>dial up VPN</i> on FortiGate.

Bug ID	Description
685704	After upgrading FortiManager, install to any device participating in the full mesh VPN may fail with copy error <i>fetch device/vdom list failed</i> .
704614	FortiManager may not be able to push policy package due to VPN related error.

Common Vulnerabilities and Exposures

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

Bug ID	Description
716350	FortiManager 6.2.8 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2021-32589

Known Issues

The following issues have been identified in 6.2.8. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
633171	There may be <i>DFS Channel</i> mismatch between FortiManager and FortiGate for FAP-223E.

Device Manager

Bug ID	Description
596711	FortiManager CLI Configuration shows incorrect default wildcard value for router access-list.
598431	Install wizard may show a blank area when scrolling down the wizard to select device(s).
604125	FortiManager may not be able to edit VDOM link interface from VDOM level.
610568	FortiManager may not follow the order in CLI Script template.
615044	Configuration status may be shown modified after added FortiGate to FortiManager.
636357	Retrieve may fail on FortiGate cluster with "Failed to reload configuration. invalid value" error.
636638	Fabric view may stuck at loading.
670577	When creating an API admin from CLI Configuration, trusted host section is missing.
674904	FortiManager may not be able to import policy with interface binding contradiction on srcintf error.
697098	Retrieving HA configuration may fail when adding FortiGate.

FortiSwitch Manager

Bug ID	Description
637220	FortiManager may not be able to upgrade FortiSwitch firmware.

Policy & Objects

Bug ID	Description
580880	FortiManager is unable to see dynamic mapping for <i>Local Certificate</i> if workflow session is created.
584288	FortiManager may not be able to load configuration of virtual server on policy page.
585177	FortiManager is unable to create VIPv6 virtual server objects.
598938	FortiManager should allow setting <i>wildcard-fqdn</i> type firewall address as destination on proxy policy.
602176	Creating a proxy policy with a profile group adds additional security profile.
608535	NAT option is missing from <i>Central NAT</i> policy package.
615624	Firewall policy and proxy policy cannot select IP type external resource as address.
618499	Right-click to edit zone incorrectly prompts dynamic interface window.
631158	FortiManager is unable to import firewall objects of <i>fsso fortiems-cloud</i> user due to Server cannot be empty.
652753	When an obsolete internet service is selected, FortiManager may show entry IDs instead of names.
655601	FortiManager may be slow to add or remove a URL entry on web filter with a large list.
659296	FortiManager may take a long time to update web filter URL filter list.
666258	User should not be able to create a firewall policy with an Internet service with <i>Destination direction</i> in <i>Source</i> by using drag and drop.
670061	FortiManager does not report error when an unsupported FQDN address format is created.
703639	Installing policy package for a device using CLI template may get stuck.
704637	Firewall policy and VIPs may get deleted on policy package installation.
711314	VDOM-specific <i>Disclaimer Page</i> config is purged from 'default' <code>replacemsg-group</code> during Policy Package installation.

Revision History

Bug ID	Description
623159	Zone validation in re-Install Policy is not saving the user choice and deleting all related policies.
635957	Install fails for subnet overlap IP between two interfaces.

Bug ID	Description
637103	Scrolling in install preview is not smooth and may get stuck.
664284	FortiManager may not be able to configure SSH certificate.

Script

Bug ID	Description
613575	After script is run directly on CLI, FortiManager may fail to reload configuration.

Services

Bug ID	Description
567664	HA slave does not update FortiMeter license.

System Settings

Bug ID	Description
670497	After upgraded FortiManager, it may delete syslog configuration.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			



To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```



FORTINET®



Copyright© 2021 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.