FortiManager - Release Notes

Version 6.4.6

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 6, 2022
FortiManager 6.4.6 Release Notes
02-646-721291-20220106

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-06-01	Initial release.
2021-06-04	Updated FortiOS/FortiOS Carrier on page 16.
2021-06-08	Updated Special Notices on page 9.
2021-06-10	Updated Known Issues on page 43.
2021-06-15	Updated Resolved Issues on page 32.
2021-06-17	Updated Resolved Issues on page 32 and Known Issues on page 43.
2021-06-18	Updated Resolved Issues on page 32 and Known Issues on page 43.
2021-06-21	Updated Resolved Issues on page 32 and FortiGate special branch models on page 23.
2021-06-23	Updated Known Issues on page 43.
2021-06-24	Added support for FortiOS 6.0.12 to FortiOS/FortiOS Carrier on page 16. Moved FortiGate models from FortiGate special branch models on page 23 to FortiGate models on page 21. Updated FortiCarrier models on page 24.
2021-06-25	Updated Known Issues on page 43. Added 673383 to Resolved Issues on page 32 and added an entry to Special Notices on page 9.
2021-06-28	Added note about ports to Management extension applications on page 8.
2021-06-29	Added 725717 to Known Issues on page 43.
2021-06-30	Added 728117 to Known Issues on page 43.
2021-07-08	Added support for FortiSandbox 3.2 and 4.0 to FortiSandbox on page 17 and FortiSandbox models on page 28.
2021-07-20	Updated Resolved Issues on page 32.
2021-07-22	Updated FortiMail on page 17. Updated FortiClient on page 17.
2021-08-30	Updated FortiAuthenticator models on page 26.
2021-09-07	Added FortiTester models on page 29.
2021-09-27	Removed FortiSandbox 4.0.
2021-10-05	Removed 623159 from Resolved Issues on page 32.
2021-11-26	Added 695782 to Resolved Issues on page 32.

Date	Change Description
2022-01-05	Added FMG-3700G to Supported models on page 7.
2022-01-06	Updated FortiMail models on page 27.

FortiManager 6.4.6 Release

This document provides information about FortiManager version 6.4.6 build 2363.

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

FortiManager version 6.4.6 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300E, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, 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).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 12.

See also Appendix B - Default and maximum number of ADOMs supported on page 48.

You can use the FortiManager VM subscription license with new FMG-VM installations.

For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.6.

FortiManager uses port TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the FortiManager 6.4 Ports and Protocols Guide.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, 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).

Minimum system requirements

Some management extension applications supported by FortiManager 6.4.6 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
SD-WAN Orchestrator	At least 12GB of memory is recommended to support SD-WAN Orchestrator MEA.
Wireless Manager (WLM)	A minimum of 4 CPU cores and 8 GB RAM is typically required. Depending on the number of running applications, the allocated resources should be increased.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.6.

ADOM version enforcement

Starting in FortiManager 6.4.6, ADOM versions are enforced. ADOM version N and N+1 are allowed, and the enforcement affects policy package installation.

For example, if you have ADOM version 6.0, and it contains a FortiGate running FortiOS 6.4, you cannot install a version 6.0 policy package to the FortiGate. The policy package installation fails with the following error message: `Device preparation failed: version mismatched,adom:6.0; dev:6.4.`

Management Extension Applications (MEA) and upgrade

Upgrading FortiManager when Management Extension Applications (MEA) are enabled may reset your *System Settings* to the default settings.

To prevent your *System Settings* from being lost, please disable all Management Extension Applications (MEA) prior to upgrading FortiManager.

Policy Hit Count on unused policy

FortiManager 6.4.3 and later no longer displays policy hit count information on the *Policy & Objects* > *Policy Packages* pane. However, you can view hit count information by using the *Unused Policies* feature and clearing the *Unused Only* checkbox. For more information, see the FortiManager 6.4 New Features Guide.

Wireless Manager (FortiWLM) not accessible

If Wireless Manager was enabled in FortiManager 6.4.0, you can no longer access it in the FortiManager GUI when you upgrade FortiManager to 6.4.2. When you try to access FortiWLM, you are redirected to the FortiManager dashboard.

SD-WAN Orchestrator not accessible

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI after upgrading to FortiManager 6.4.2.

To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

Support for FortiOS 6.4 SD-WAN Zones

In 6.4 ADOMs, SD-WAN member interfaces are grouped into SD-WAN zones. These zones can be imported as normalized interfaces and used in firewall policies.

Customers upgrading FortiGates from FortiOS 6.2 to 6.4 who cannot upgrade the ADOM are advised to temporarily disable SD-WAN central management until they can upgrade the ADOM to 6.4. This is to prevent FortiManager from attempting to delete the newly created SD-WAN zones on the FortiGate.

FortiGuard Rating Services with FortiGate 6.4.1 or Later

FortiManager 6.4.1 or later is the supported version to provide FortiGuard rating services to FortiGate 6.4.1 or later.

Citrix XenServer default limits and upgrade

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

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

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.

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 t1sv1
end
```

Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.6.

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

This section contains the following topics:

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.

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 Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 6.4.6 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 6.4.6 support

This section identifies FortiManager 6.4.6 product integration and support information:

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 6.4.6 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 88
- Google Chrome version 91

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

FortiOS/FortiOS Carrier

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

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

FortiADC

This section lists FortiManager 6.4.6 product integration and support for FortiADC:

- 6.0.1
- 5.4.4

FortiAnalyzer

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

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

FortiAuthenticator

This section lists FortiManager 6.4.6 product integration and support for FortiAuthenticator:

- 6.0. to 6.2
- 5.0 to 5.5
- 4.3 and later

FortiCache

This section lists FortiManager 6.4.6 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 6.4.6 product integration and support for FortiClient:

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

FortiDDoS

This section lists FortiManager 6.4.6 product integration and support for FortiDDoS:

- 5.4.1
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 19.

FortiMail

This section lists FortiManager 6.4.6 product integration and support for FortiMail:

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

FortiSandbox

This section lists FortiManager 6.4.6 product integration and support for FortiSandbox:

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

FortiSOAR

This section lists FortiManager 6.4.6 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

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

- 5.2.3
- 5.0.0 and later

FortiTester

This section lists FortiManager 6.4.6 product integration and support for FortiTester:

- 3.9
- 3.8
- 3.7

FortiWeb

This section lists FortiManager 6.4.6 product integration and support for FortiWeb:

- 6.3.10
- 6.2.4
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

Virtualization

This section lists FortiManager 6.4.6 product integration and support for virtualization:

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

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
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 6.4.6.

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

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, 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-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:**FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, 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, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D,FortiGate-2200E, FortiGate-2201E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:** FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600C-DC, FortiGate-3600E-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-80CM, FortiWiFi-81CM, FortiWiFi-60F, FortiWiFi-61F **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, 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, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F **FortiGate DC:** FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

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-200F, FortiGate-201F	6.4
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-200F, FortiGate-201F, FortiGate-400E-Bypass, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F	6.2

Model	Firmware Version
FortiGate DC: FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ,	
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E **FortiGate DC:** FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:** FortiWiFi-41F, FortiWiFi-41F-3G4G,	6.0

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC **FortiCarrier 7000 Series:** FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC **FortiCarrier 7000 Series:** FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F	6.2

Model	Firmware Version
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	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiCarrier 6000 Series:** FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC **FortiCarrier 7000 Series:** FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand,FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

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. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiAuthenticator models

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

Model	Firmware Version
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3

FortiCache models

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E	5.4

Model	Firmware Version
FortiMail Low Encryption: FE-3000C-LENC	
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

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

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	3.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2
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

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FSR-VM	6.4
FortiSOAR VM: FSR-VM	6.0

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

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.9
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.8
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.7

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, ortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3

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-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
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-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6

Model	Firmware Version
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-XENSERVER, 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-XENSERVER, 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-XENSERVER	5.2.4

Resolved Issues

The following issues have been fixed in 6.4.6. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
590098	When adding a new WTP profile, FortiManager tries to set a default `handoff-sta-thresh` and unset radio bands, which do not match the defaults for many of the E-series APs.
591994	AP region settings may be unset in Central Management mode.
635643	5G channels may be mismatch between FortiManager and FortiGate for *radio-1* and *radio-2* with FAP-231E.
648812	DHCP server is incorrectly created for *Bridge SSID*.
674636	SSID may be empty in *AP Manager* > *WiFi Profiles* > *SSID* column.
692911	FortiManager may not be able to display correct information for wireless radio in wireless profile for FortiWiFi-80F-2R.
706233	FortiManager may not detect changes in *AP Manager* > *SSID* > *Pre-shared Key Password* and display the message *No record found*.
712669	FortiManager may set `darrp` as enable on radio in monitor mode resulting in installation failure.

Device Manager

Bug ID	Description
485037	*Monitor* > *Map View* may fail if proxy is enabled.
521976	Users may not be able to enable *CSV format* within system template.
544982	*Policy Package Status* may become out-of-sync for all devices when adding one device to *Install On*.
560444	FortiManager may not set `pmf` to *enable* causing install to always fails with WPA3-SAE, WPA3-Enterprise, or WPA3-SAE-Transition within 6.4 ADOM.
594211	FortiManager should be able to create new VLAN interface on fabric interface and install to FortiGate.

Bug ID	Description
603820	FortiManager fails to import policy when *reputation-minimum* and *reputation-direction* are set.
610585	*Device Manager* cannot save *DHCP for Unknown MAC address* with action sets to *block*.
624325	Creating or editing transparent VDOM to disable may stuck at 20%.
636357	Retrieve may fail on FortiGate cluster with *Failed to reload configuration. invalid value* error.
649260	*Device Manager* may return an error when deleting *VPN phase1*.
654611	Under *Advanced* mode and within a VDOM, clicking *Device Manager* on the top menu returns the no permission error.
658832	FortiManager is unable to retrieve *priority-members* if outgoing interface is using the Manual strategy in SD-WAN rule.
659387	FortiManager should be able to provision *CLI-template*, *SD-WAN-template*, and *Policy Package* together to the model device.
664120	When FortiGate HA secondary unit is down, action is displayed as *promote* in *Device Manager*.
665955	FortiManager is not reflecting proper `admintimeout` value in CLI only object.
667738	667738
670535	Install fails when creating a new DHCP reservation due to missing MAC address.
672344	If managed FortiAnalyzer is in HA, setting Send Logs to *Managed FortiAnalyzer* in the system template may cause install error.
676002	FortiManager is not allowing to re-install policy when user selects all devices with VDOMs from Device Manager.
678495	FortiManager VPN L2TP may prompt *invalid ip range*.
680516	*Host Name* is truncated when name has more than 31 characters.
681627	FortiManager is accepting DNS source IP even though it is not part of the available interfaces.
683411	FortiManager may not display a FortiGate under the *Device Manager* > *Managed Devices*.
684372	When using VDOMs, *Policy Package* status remains in modified status after using *Push to device*.
684462	FortiManager truncates the device configuration when downloading from View configuration option.
684961	Registration with NSX-T may fail with error: *Register service failed*.
688541	FortiManager should not unset `dynamic-vlan` of wireless-controller VAP and gateway of router settings after import.
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.

Bug ID	Description
690566	Changed to the *Disclaimer Page* may not be saved with error.
692200	FortiManager may return conflict after a `zero-touch-provisioning` cluster deployment.
692669	Browser may display a message, *A webpage is slowing down your browser*, while checking revision difference.
693622	There may be inconsistent behavior between FortiGate and FortiManager when changing port speeds for FortiGate-3600E or FortiGate-3601E.
696136	Auto-link may fail caused by input device in SD-WAN.
696496	When Workspace is enabled, auto-link may fail.
696576	Explicit FTP proxy available certificates are not consistent with the ones available in the FortiGate.
696848	Users may not be able to retrieve configuration or import policy from managed devices with `dvmcore` constantly crashing.
697098	Retrieving HA configuration may fail when adding FortiGate.
697535	*Device Manager* should not allow user to add ssl.root to a zone.
697746	FortiManager needs to support adding FortiAnalyzer with serial number that has prefix, *FAVMXX*, to FortiManager.
697924	When there are many devices, all managed FortiGates may show connection down state.
698625	FortiManager may not be able to view, add, or edit software switch members.
698709	When importing policies, firewall policies may not be loaded.
699031	FortiManager may display duplicated devices when *Display Device/Group* tree view is enabled in Workflow mode.
699182	FortiManager may fail to add FortiGate-101F as model device.
699450	SDWAN monitor is showing historical *Traffic* for interface which is down in defined Time period.
701446	SD-WAN monitor take several minutes to display map if device tunnel is flapping.
702555	FortiManager may lose device *admin user* and geo-location information during on board process with model device.
702590	The system template may stop being displayed on the *Devices & Groups* page.
704197	FortiManager may fail to create a FortiSwitch in a 6.0 ADOM.
704789	SD-WAN monitor is missing *Health Check Status* information and probes.
705547	Route monitor may shows incorrect interface information.
706194	When editing a model device and assignigning a Policy Package, clicking the *OK* button may not take effect.

Bug ID	Description
708937	FortiManager may randomly updating the geographical coordinates of a FortiGate device.
709302	SD-WAN monitor search function on the table view does not actually search but highlight.
710616	FortiManager may not be able to set *HTTPS* or *SHH Port* to a value higher than 63335 under *Provisioning Templates*.
711034	There may be issues to display meta data fields when creating or editing a device group.
713267	Searching for FortiGate name when editing a device group should display FortiGate device name with all the VDOMs.

Bug ID	Description
554251	A user may not be able to see the fabric topology of devices in the user's assigned ADOM.

FortiSwitch Manager

Bug ID	Description
667703	After added FortiSwitch, running a script to provision may fail.
676739	FortiManager may not be possible to delete VLAN interfaces created by FortiSwitch Manager.
690995	FortiSwitch Manager should not install the *auto-detected* setting to FortiGate.
700023	Install may fail with `switch-controller managed-switch:poe-pre-standard-detection` after upgrade.
700136	In FortiSwitch Manager, the *Map to Normalized interface* menu always displays *none* when editing a VLAN.
706953	Maximum one *device entry* can be found in device information column under FortiSwitch port.
707909	Template may be removed and Fortilink interface and comments fields may be empty.
708901	The assigned FortiSwitch template name that has more than sixteen characters may fail ADOM integrity check.
713492	In the per-device mapping of the VLANs in FortiSwitch Manager, the "Specify" for the gateway is not saved in the database.
713553	FortiSwitch Template flow counter interval value variance between 6.0 and 6.2 ADOMs.

Global ADOM

Bug ID	Description
662216	*Where Used* in Global ADOM may not show object usage in ADOM.
689965	Replacement message type *UTM* is not being pushed from global ADOM to local ADOM.
695782	Connection to FortiGate may fail with multiple `fgfmsd` crashes.

Others

Bug ID	Description
600490	SD-WAN controller cannot load page when changing HTTPS to non default 443.
667442	FortiManager may not be able to connect to FortiGate CLI via SSH widget or execute TCL scripts.
669191	The `fdssvd` daemon may randomly crash.
673383	Should not allow installation of v6.0 policy package to v6.4 device.
681625	The `svc cdb` reader process may crash during upgrade of ADOM.
681707	The `diagnose cdb upgrade check +all` command may unset *defmap-intf*.
682404	The `rtmmond` process memory usage may constantly increasing.
683841	FortiManager databases may randomly lose integrity.
686460	ADOM integrity check may run slowly and it takes several minutes to response for each ADOM.
687155	FortiManager should improve the error message for running CLI Template.
688188	HA re-transmission may not work and crash.
690969	The `dmworker` process may consume high memory and CPU resources with failures due to busy handler.
691568	FortiManager GUI may randomly become non responsive.
695549	`_created timestamp` is missing in REST API return data for policy.
697132	In some occasions, FortiManager is not accessible until device is rebooted every couple of days.
697361	FortiExtender status may not be correctly displayed.
704545	When there are a lot of workflow sessions and users try to disable the workflow mode via GUI, FortiManager may stop responding.
706516	*Securityconsole* may crash when there are quotes around group name.
715601	Under some conditions, disk usage may reach 100% after a few days.

Policy and Objects

Bug ID	Description
487186	FortiManager may install a different local category ID to FortiGate causing conflict with custom URL rating list.
587634	FortiManager may not be able to create new wildcard FQDN type address to FortiGate 6.2.
593072	After a non-Super User deletes a device, *super_user* admin cannot edit zone or interface with the deleted device's dynamic mappings.
617894	FortiManager is missing IPV6 *none* values after modifying policy.
630431	Some application and filter overrides are not displayed on GUI.
654172	There may be *webfilter local category ID* mismatch between FortiManager and FortiGate causing incorrect action when using *Custom URL* List.
659543	FortiManager is not allowing reorder between *Policy Blocks*.
672035	There may be an error when importing AWS credential from FortiGate to FortiManager.
673554	FortiManager should not allow policy to set destination address with a *Virtual Server* when inspection-mode is set as *flow*.
675501	Policy check may show negative values.
675509	FortiManager may randomly set IPv4 IP Pool object to overload.
683167	*Policy Package* single entry change may impact all *Policy Package Installation Targets* status.
684081	*Policy Check* and *Find Unused Policies* may not work for FortiGate in Policy-Based mode.
684728	FortiManager and FortiGate should have equivalent filter list entries.
686902	FortiManager may not be able to configure `ipv4-split-exclude` attribute via CLI Object.
686962	FortiManager is not allowed to rename application control profile.
687460	The same filter may behave differently between source address and destination address.
687784	FortiManager may not be able to add rule with ISDB object when a rule is created with add above or below option.
688589	Setting the *Local Webfilter Category Action* to *Allow* should not disable the action when installed on FortiGate.
690269	Newly imported *Cisco ACI* connector object does not appear for selection until browser is refreshed.
690509	FortiManager may fail to install *ACI-Direct* connector to FortiGate due to `server-list` command.
692114	*Where Used* returns no record found when IPS Custom Signature is being used.
693763	Saving address object may return error: *firewall/address/organization : The data is invalid for selected url*.

Bug ID	Description
694605	FortiManager may not be able to push the entire Azure SDN Connector configuration.
696072	FortiManager GUI should allow users to configure HTTPS health check monitor including fields such as *http-match* and *http-get* in the monitor.
700743	Viewing *Policy & Objects* may be slower after upgrade.
701290	FortiManager should not allow users to create a wildcard FQDN address object with non-wildcard FQDN.
702138	NGFW security policy *Application* category *Unknown applications* is missing on FortiManager while it is present on FortiGate.
702621	When adding a remote usergroup with LDAP service unreachable, the *Manually specify* option is only available after a timeout.
703639	Installing a policy package for a device using CLI template may stall.
704637	Firewall policy and VIPs may get deleted on policy package installation.
705025	*Find Unused Policies* may report incorrect session data for security policy.
706126	The *Find Unused Policies* option may be missing in dual pane mode.
707953	IPS sensor may incorrectly set action to *pass* instead *block* when quarantine is set.
708877	FortiManager 6.0 ADOM should not allow users to set ISDB objects that are not supported on FortiOS 6.0.
709435	FortiManager may not be able to import existing Azure SDN Connector from FortiGate.
711121	Enabling *FortiGuard Outbreak Prevention* database does not match FortiGate's behavior.
712150	Search in *Address* may not work after upgrading to FortiManager to 6.4.5.
712900	When new folders are created and the default policy package is deleted, then the new policy package cannot be created.
713216	When policy package is large, there is slowness loading policy package, installing policy package, or viewing sessions revision diff in workflow mode.
719104	FortiManager may not be able to select *Internet Service* group members when creating *Internet Service* group.

Revision History

Bug ID	Description
638060	Installing an existing revision or renaming a revision should be allowed in backup ADOM.
657344	Installing from 6.0 ADOM may try to *unset inspection-mode* and *unset ssl-ssh-profile* on FortiGate 6.2.

Bug ID	Description
664284	FortiManager may not be able to configure SSH certificate.
667148	When a policy install is performed, *Install preview* shows a lot of firewall policies with *metafield* changes without any actual change been done.
673101	When *set cfg-save manual* is configured, FortiManager may try to delete objects that do not exist in the FortiGate configuration.
675867	The `ssl-anomaly-log` 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.
683728	Installation fail due to VIP mapped IP range error when installing v6.2 policy package to v6.4 device.
685509	FortiManager may unset `authmethod-remote` causing install failure.
686036	FortiManager may remove allow access configurations for secondary IP when a policy package is installed.
687769	FortiManager may not be able to set `auto-asic-offload` to disable.
688474	FortiManager may fail to retrieve FortiGate configuration when adding device due to invalid data source with `wtp-profile`.
689270	The following attributes under *configs vpn ssl setting* may have invalid range: *login-attempt-limit*, *login-block-time*, *http-request-header-timeout*, *http-request-body-timeout* and *router bgp keep-alive-timer*.
691240	FortiManager should not unset the value *forward-error-correction* with certain FortiGate platforms.
691835	FortiManager should be able to move one VLAN to a different zone without deleting many rules or zones.
693225	FortiManager may install *unset inspection-mode* to Footage 6.2 device in 6.0 ADOM.
693231	FortiManager tries to purge webfilter `ftgd-local-rating` when directly referenced in *URL Category* of a policy.
694380	Installation may fail when `set whitelist enable` in `ssl-ssh-profile` is pushed to FortiGate 6.2 from a in 6.0 ADOM.
697642	Connecting unauthorized FortiSwitch to a managed FortiGate may cause issues on FortiManager when `auto-update` is disabled.
698350	Install may fail with error: *[VPN manager] failed to update vpn node with device info*.
700495	FortiManager 6.2 ADOM may be sending set *synproxy* to FortiGate-1801F.
701870	Process may stall at 85% when pushing multiple policy packages from Global ADOM.

Bug ID	Description
709456	FortiManager may be missing configuration revisions after performed HA failover.
714173	Policy package installation from 6.2 ADOM changes `cert-validation-timeout` default value to `block`.
715313	FortiManager may not enable the option *FortiGuard Category Based Filter* after FortiManager is synchronized with FortiGate.

Script

Bug ID	Description
668947	Changes using CLI Script may not be applied to devices in the container or folder.
671998	TCL scripts may not work when `ssh-kex-sha1` and `ssh-mac-weak` are not enabled on FortiGate.
683208	Importing CLI script should be highlighted by default.
702576	Objects may not present on the corresponding device configuration after running a script to rename objects.
715305	When changing system setting `opmode` from `nat` to `transparent` via a script, FortiManager may return failure to commit to database stating that there is no interface.
715623	Running a script on device database may not update *Save* status.

Services

Bug ID	Description
680857	FortiExtender, FortiAP, or FortiSwitch upgrades can fail due to custom image being deleted during or after a failed upgrade.
691738	FortiManager may not be able to connect to FDS server via IPv6 proxy.
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 *06002000NIDS02504* extend IPS database to default download list.
701341	FortiGuard Firmware Images may not show up-to-date FortiOS versions.
704584	FAP firmware may not be listed and cannot be imported.
714596	For web filter query, FortiManager should support category 9 mapping data.
714787	FortiManager should have a `diagnose` command to force web filtering database merge.

System Settings

Bug ID	Description
517964	FortiManager may create incorrect certificate and it cannot be deleted.
598194	FortiManager two-factor authentication admin login is missing the option for *FTK Mobile* push notification authentication.
625683	Changes made by ADOM upgrade may not update *Last Modified* date/time and user admin.
635181	FortiManager is unable to delete mail server with error message *used* displayed.
637377	If *Manage Device Configurations* is *none* in admin profile, user may not be able to see the interface in the policy.
652417	FortiManager HA may go out of synchronization periodically based on the logs.
667284	FortiManager should have better log message when aborting device upgrade.
677528	Address object search may not display the address group which contains the searched object within the group.
684907	Changing of *FortiGuard Server Location* in *License Information Dashboard* may not take any effect.
686569	Creating and deleting the static route may remove specific connected route.
687223	Users may not be able to upgrade ADOM because of `profile-protocol-options`.
688517	Upgrading ADOM may fail due to FortiExtender Object.
689917	If a policy is configured with a Proxy Options profile with *HTTP Policy Redirect* enabled, the ADOM upgrade should enable the related option `set http-policy-redirect enable` to preserve the HTTP redirect feature.
690921	ADOM upgrade from 6.0 to 6.2 should not add custom *ssl-ssh-profile* to policies which were not configured for SSL inspection.
695058	Radius response packets should not timeout with less of the *remoteauthtimeout* setting.
695360	ADOM upgrade may be slow and it may take several minutes to start.
697082	Schedule SCP backup may fail due to incorrect default port number.
699185	If Management Extension Applications (MEA) are enabled, all system settings may be lost after upgraded FortiManager.
699253	Admin profile should not need system level access to view list of time zones in *Device Manager*.
700142	FortiManager should allow user to configure more than eight hosts per SNMP community.
704504	*License Information* may keep loading for admin user with FortiGuard and System Settings with read-write permissions.
705185	ADOM upgrade may cause per device mapping of VLANs in FortiSwitch Manager change to 0.

Bug ID	Description
705762	Session can be approved twice by different users of the same approval group.
708939	Dashboard is showing incorrect GB per day and device quota information when FortiManager is enabled.
711446	Copy may fail due to invalid protocol options when both FortiGate and ADOM are upgraded to v6.2.
713233	FortiManager may fail to upgrade firmware resulting in cdbupgrade task error on console and process crashes.
714210	LDAP admin group search should be done with the service or administrator bind account.
714635	FortiManager backup file size may increasing gradually when IPS package get updated.

VPN Manager

Bug ID	Description
681110	VPN manager may not push any configuration on ADOM 6.0 for dial up VPN on FortiGate.
695879	Edit community may not be able to set VPN zone to off via GUI.
697308	VPN Manager is setting `dst-name` to all when using `dst-name` object group address in protected subnet.
701772	AP may not show up in AP manager after running CLI templates.
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	CVE references
672953	FortiManager 6.4.6 is no longer vulnerable to the following CVE-Reference: • CVE-2021-24022
716350	FortiManager 6.4.6 is no longer vulnerable to the following CVE-Reference: • CVE-2021-32589

Known Issues

The following issues have been identified in 6.4.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
633171	There may be *DFS Channel* mismatch between FortiManager and FortiGate for FAP-223E.
673020	Creating SSID interface with central AP Manager automatically generates normalized interface name that has no default mapping configuration.
701487	FortiManager may not be able to assign AP profile after upgraded firmware.

Device Manager

Bug ID	Description
545239	After adding FortiAnalyzer fabric ADOM to FortiManager,Device Manager's *Log Status*, *Log Rate*, or *Device Storage* column cannot get data from FortiAnalyzer.
563690	Device Manager fails to add FortiAnalyzer which contains a FortiGate HA device with error: *Serial number does not match database*.
596711	FortiManager CLI Configuration shows incorrect default wildcard value for *router access-list*.
610568	FortiManager may not follow the order in CLI Script template.
615044	Configuration status may appear modified after adding FortiGate to FortiManager.
636638	Fabric view may stall at loading.
640907	FortiManager is unable to configure FortiSwitch port mirroring.
660491	Device Manager system interface should not allow duplicated secondary IP address.
670577	When creating an API admin from CLI Configuration, the *Trusted Host* section is missing.
673548	FortiManager may not be able to make changes to the FortiGate interface settings when the interface type is *Software Switch*.
674904	FortiManager may not be able to import a policy with interface binding contradiction on *srcintf* error.

Bug ID	Description
690493	License check setting may not be saved.
701348	Once VRPP instance is created, user should be able to edit or delete it.
702906	*DHCP Relay Service* may not be deleted when it is configured on VLAN interface.
709214	System template should allow source interface to be selected when specify is activated as `interface-select-method`.
710570	*Any* statement is not accepted by FortiManager in the *perfix-list* configuration.
714710	Secondary interface configuration may not appear in Device Manager.
725717	The `mcast-session-counting` command causes the install to fail after upgracing 6.4.6
728117	Install fails after upgrading FortiManager to 6.4.6 due to `set pri-type-max 1000000`. **Workaround**: Perform a *Retrieve* and then re-attempt the *Install*.

Global ADOM

Bug ID	Description
667197	User should not be able to delete global object when ADOM is not locked.
680798	FortiManager may return error, *Could not read zone validation results*, when assigning global ADOM changes with *Automatically Install Policies to ADOM Devices*.
693510	*Display Options* for *Object Config* will reset to default after some time.

Others

Bug ID	Description
657997	Assigning device to system template may not work via JSON when FortiManager is in Workspace mode.
727458	FortiManager 6.4.6 does not allow access to all VDOMs if Workspace mode is disabled while a lock is still active.

Policy & Objects

Bug ID	Description
584288	FortiManager may not be able to load configuration of virtual server on policy page.
636537	*CLI Only Objects* > *user* > *peergrp* is not able to delete *peergrp*.
642708	*View Mode* may unexpectedly changed from *Interface Pair View* to *By Sequence mode*.
652753	When an obsolete internet service is selected, FortiManager may show entries 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 lot of time to update web filter URL filter list.
663109	FortiManager should not allow users to select a profile group in a flow-based policy that uses a proxy-based feature.
666258	User should not be able to create a firewall policy with an Internet service with *Destination direction in Source* by using drag and drop.
679282	Editing a global object in an ADOM is not possible generating error, *undefined is not iterable*.
682356	FortiManager may not be able to map normalized interface.
686911	Workflow session may not be able to compare with error: *Can not compare because of invalid Revision Diff data*.
688586	Exporting Policy Package to *CSV* shows *certificate-inspection* in the *ssl-ssh-profile* column even when the profile is not in use.
689589	Internet Services may not match between FortiManager and FortiGate.
711964	Wildcard certificate should be able to be used for *Deep Inspection*.
716114	FortiManager should push changed in `ssl-ssh-profile` with *Untrusted SSL Certificates* setting reverted from *Block* to *Allow*.
719774	IP reputation for the policies are not working without source or destination.

Revision History

Bug ID	Description
635957	Install fails for subnet overlap IP between two interfaces.
618305	FortiManager changes configuration system csf settings.
606737	User may not be able to install policy package due to change with external interface with VIP settings.

Services

Bug ID	Description
567664	HA secondary device does not update FortiMeter license.

System Settings

Bug ID	Description
579964	FMGVM64-Cloud needs to provide GUI support for ADOM upgrade in system information dashboard.
687968	FortiManager should not change to `ipv6-autoconf` to `disable` when management access is changed to the `ipv6-autoconf enable` state.
690926	FortiManager is removing *SD-WAN* field description upon ADOM upgrading from 6.2 to 6.4.
709873	Global task assignment *Time Used* may not be accurate.

VPN Manager

Bug ID	Description
699759	When installing a policy package, per-device mapped object used in SSL VPN cannot be installed.
712633	VPN Manager pushes default `dpd-retrycount` and `dpd-retryinterval`, but it cannot display them.

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
```

Appendix B - Default and maximum number of ADOMs supported

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

Hardware models

The following table identifies the default number of ADOMs supported for FortiManager hardware models G series and later. It also identifies the hardware models that support the ADOM subscription license and the maximum number of ADOMs supported.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
3000G Series	500	✓	1200

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the FortiManager Data Sheet.

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.