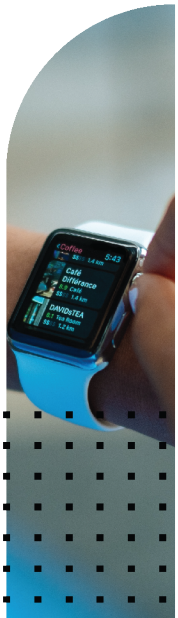
Release Notes

FortiManager 7.0.0



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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

January 5, 2024
FortiManager 7.0.0 Release Notes
02-700-690783-20240105

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-22	Initial release.
2021-04-23	Updated FortiGate models on page 21 and FortiGate special branch models on page 23.
2021-04-26	Updated Special Notices on page 9.
2021-06-18	Updated Resolved Issues on page 30 and Known Issues on page 42.
2021-06-23	Updated FortiGate special branch models on page 23.
2021-06-28	Added note about ports to Management extension applications on page 7.
2021-07-08	Added FortiSandbox 3.2 and 4.0 support to FortiSandbox on page 17 and FortiSandbox models on page 26.
2021-07-22	Updated FortiClient on page 17.
2021-07-29	Added *Scheduling firmware upgrades for managed devices* to Special Notices on page 9. Added 713714 to Known Issues on page 42.
2021-11-26	Added Microsoft Hyper-V Server 2019 to Virtualization on page 18 and added 695782 to Resolved Issues on page 30.
2024-01-05	Updated Special Notices on page 9.

FortiManager 7.0.0 Release

This document provides information about FortiManager version 7.0.0 build 0047.

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 7.0.0 supports the following models:

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

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 FortiManager7.0.0.

FortiManager uses port TCP/443 or 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 7.0 Ports 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, and FMG-3900E.
FortiManager VM	FMG-VM64, 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).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAuthenticator	• 4 vCPU • 8 GB RAM	No change
FortiPortal	• 4 vCPU • 8 GB RAM	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage
SD-WAN Orchestrator	• 4 vCPU • 8 GB RAM	• 4 vCPU • 12 GB RAM
Wireless Manager (FortiWLM)	• 4 vCPU • 8 GB RAM	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.0.

FortiManager 7.2.3 and later firmware on FortiGuard

Starting in FortiManager 7.2.1, a setup wizard executes to prompt the user for various configuration steps and registration with FortiCare. During the execution, the FortiManager unit attempts to communicate with FortiGuard for a list of FortiManager firmware images currently available on FortiGuard – older and newer.

In the case of FortiManager 7.2.2, a bug in the GUI prevents the wizard from completing and prevents the user from accessing the FortiManager unit. The issue has been fixed in 7.2.3 and later and a CLI command has been added to bypass the setup wizard at login time.

```
config system admin setting
   set firmware-upgrade-check disable
end
```

Fortinet has not uploaded FortiManager 7.2.3 and later firmware to FortiGuard in order to work around the GUI bug, however, the firmware is available for download from the Fortinet Support web site https://support.fortinet.com.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

ADOM Upgrade for FortiManager 7.0

Currently, there is no ADOM upgrade option for ADOM version 6.4 to move to version 7.0. In order to manage FortiGates running 7.0, please add the devices to a 7.0 ADOM.

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

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 6.4.0 or later directly to 7.0.0.

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. 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.

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.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

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.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

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 7.0.0 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 7.0.0 support

This section identifies FortiManager 7.0.0 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 7.0.0 product integration and support for web browsers:

- Microsoft Edge 80 (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 7.0.0 product integration and support for FortiOS/FortiOS Carrier:

- 7.0.0
- 6.4.0 to 6.4.5
- 6.2.0 to 6.2.7

FortiADC

This section lists FortiManager 7.0.0 product integration and support for FortiADC:

- 6.0.1
- 5.4.5

FortiAnalyzer

This section lists FortiManager 7.0.0 product integration and support for FortiAnalyzer:

- 7.0.0
- 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 7.0.0 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 7.0.0 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 7.0.0 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later

FortiDDoS

This section lists FortiManager 7.0.0 product integration and support for FortiDDoS:

- 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 7.0.0 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 7.0.0 product integration and support for FortiSandbox:

- 4.0.0
- 3.2.2
- 3.1.4
- 3.0.6

- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiManager 7.0.0 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

This section lists FortiManager 7.0.0 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 7.0.0 product integration and support for FortiWeb:

- 6.3.11
- 6.2.4
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.3
- 5.6.2
- 5.5.7
- 5.4.1

Virtualization

This section lists FortiManager 7.0.0 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5

- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

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		✓

Language	GUI	Reports
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 7.0.0.

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-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E **FortiGate 5000 Series**: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **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, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiWiFi**: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F **FortiGate VM**: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-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	7.0
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-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 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	6.4

Model	Firmware Version
FortiGate Hardware Low Encryption: FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	
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-81E, FortiGate-81E-POE, 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 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-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

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-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-200F **FortiWiFi**: FortiWiFi-40F, FortiWiFi-40F-3G4G	6.4
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-200F, FortiGate-201F, FortiGate-400E-Bypass, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4201F **FortiGate 6000 Series:** FortiGate-6000F **FortiGate 7000 Series:** FortiGate-7000E **FortiGate DC:** FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FotiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-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-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.0
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC	6.4

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-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

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-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzerVM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0.0
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	6.4

Model	Firmware Version
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	
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

FortiAuthenticator models

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

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	4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

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-1000F, FSA-2000E, FSA-3000E **FortiSandbox-VM:** FSA-AWS, FSA-VM	4.0

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

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

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	6.2, 6.3

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

Resolved Issues

The following issues have been fixed in 7.0.0. 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.
593168	DFS channel list in WiFi template is inconsistent between FortiManager and FortiGate.
635643	5G channels be mismatch between FortiManager and FortiGate for *radio-1* and *radio-2* with *FAP-231E*.
648812	DHCP server is created incorrectly for *Bridge SSID*.
667215	FortiManager should be able to classify Rogue FortiAPs.
669906	FortiManager may not be able to install *mpsk-key* from AP Manager.
679115	An available interface cannot be selected when authorizing FortiExtender.
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	Monitor > map view may fail if proxy is enabled.
594211	FortiManager should be able to create new VLAN interface on fabric interface and install to FortiGate.
604855	CLI Template should not prevent the `lan` interface from being deleted once all the dependencies have been removed.
609744	*Device Manager* > *System* > *Interface* may not be able to delete SSID interface.
610134	FortiManager may not be able to save the admin setting page.
610585	Device Manager cannot save DHCP for Unknown MAC address with action sets to block.
616387	Device configuration dashboard cannot update *hostname* or *VDOM*.

Bug ID	Description
624325	Creating or editing transparent VDOM to disable may stall at 20%.
627664	FortiManager cannot cooperate with *socket-size 0* and changes it to *1* automatically.
636012	Importing a policy may report conflict for the default *SSH CA* certificates.
643845	After auto link, FortiGate HA cluster members have the same *hostname*.
645086	Policy Lookup shows an error even though the device is in sync.
646421	FortiManager may not be able to configure VDOM property resources setting.
649785	*SD-WAN* > *Monitor* may hang for an ADOM with 1500 devices.
649821	Installation may fail for FortiGate-600D.
654611	Under Advanced mode and within a VDOM, clicking "Device Manager" on the top menu returns the no permission error.
655264	VDOM count is not correct when *vdom-mode split-vdom* is configured on FortiGate with *VM0xV* license.
656433	FortiManager device delete process may hang .
657988	FortiManager may lose connection and fail to install after FortiGate HA switching roll.
659387	FortiManager should be able to provision *CLI-template*, *SD-WAN-template*, and *Policy Package* together to the model device.
662243	FortiManager is unable to clone *SNMP Community* under *System Templates*.
662656	When importing polices that contain *policy block* or *global policy*,the import wizard should provide a warning that those polices will not be imported.
665344	Users with full *R/W DVM* privileges should be allowed to see and modify the *System Provisioning Templates*.
666833	GUI returns no warning when 4-byte AS or invalid community is configured on Standard community.
667826	Device Manager may show "*No entry found*" with *rtmmond* and the security console crashes.
669129	FortiManager does not create dynamic mapping for an address group causing import failure.
669155	SD-WAN monitor hangs at loading when the admin profile is set to *Read-Only* for SD-WAN.
669704	FortiManager does not allow user to configure FortiGate admin password longer than 32 characters.
670535	Install fails when creating a new DHCP reservation due to missing MAC address.
670839	FortiManager should be able to configure IPSec Phase2 selector using the same IP range.
671348	FortiManager should allow more than ten incoming source interfaces for policy routing decision.
672319	*View Config*, *View Install Log* , and *Revision Diff* in *Workspace* mode should not be greyed out when the ADOM is unlocked.

Bug ID	Description
672338	FortiManager may unset interface weight in SD-WAN when installing within 6.0 ADOM.
673008	SD-WAN Rules order changes to the default when creating a rule and moving it to the top.
673641	When creating a policy, all the *vwpare* names are shown and not only the names from the installation target.
674282	FortiManager sends *unset entry-id* if the FortiGate implements NAC access-mode at FortiSwitch *switchport* level.
674938	FortiManager should add support for *set use-shortcut-sla* option in SD-WAN rules.
676002	FortiManager is not allowing to re-install policy when user selects all devices with VDOMs from Device Manager.
677241	Interface speed is set incorrectly on the port group due to missing aggregate membership verification.
678066	Install may fail when changing FortiGate admin password from FortiManager.
680516	*Host Name* is truncated when the name has more than 31 characters.
681627	FortiManager is accepting DNS source IP even though it is not part of the available interfaces.
684372	When using VDOMs, the *Policy Package* status remains in modified status after using *Push to device*.
684462	FortiManager truncates the device configuration when downloading from *View configuration* option.
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.
689920	FortiWeb serial number may not be correctly recognized and firmware version is not available in the *Add device* wizard.
690012	Changing the value of a meta-data field for a device should trigger the change with configuration status.
690241	FortiManager may fail to auto-link with FortiGate with the error: *Failed to update device management data 'invalid value - devmgmtdatafailed|invalid value*.
690566	Changes to the *Disclaimer Page* may not be saved and displays an error.
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 due to the input device in SD-WAN.
696496	Auto-link may fail when *Workspace* is enabled.

Bug ID	Description
696848	Users may not be able to retrieve configuration or import policy from managed devices and *dvmcore* crashes frequently.
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 devices with serial numbers that have a prefix of *FAVMXX*.
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.
699182	FortiManager may fail to add FortiGate-101F as model device.
699450	The SDWAN monitor is showing historical traffic for an interface when it is *Down* in the defined time period.
701446	SD-WAN monitor may take several minutes to display a map if the device tunnel is flapping.
702555	FortiManager may lose device *admin user* and geo-location information during the onboard process for a 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.
710616	FortiManager may not be able to set a *HTTPS* or *SHH Port* to value higher than *63335* under *Provisioning Templates*.
711034	There may be to displaying *Meta Fields* data when creating or editing a *Device Group*.

Fabric View

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
650453	FortiSwitch template and VLAN shall appear for firewall policy creation.
667703	After adding a FortiSwitch, running a script to provision may fail.
678804	FortiSwitch template is not working as expected in *switchport NAC access-mode*.
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	A maximum of 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.

Global ADOM

Bug ID	Description
632400	When installing a global policy, FortiManager may delete policy routes and settings on an ADOM.
662216	Searching for *Where Used* in a Global ADOM may not show object usage in an ADOM.
667423	Assigned header policy from the global ADOM shows up on excluded policy package.
670280	Promoting the Profile Group object should not promote the default *Protocol* option.
689965	Replacement message type *UTM* is not being pushed from global ADOM to local ADOM.

Others

Bug ID	Description
649399	After upgrade, install may fail if a FortiGate was assigned to a system template.
656956	There may be crashes with *rtmmond* when FortiWLM is enabled.

Bug ID	Description
659916	FortiManager may consume high memory usage by the *svc sys* daemon.
661069	ADOM restricted access user is able to pull Device Manager information from ADOMs via JSON API.
665617	FortiManager may consume high CPU resource when locking ADOM or loading policy.
667421	FortiManager may report repeated *miglogd* crashes which causes lost logs.
667442	FortiManager may not be able to connect to FortiGate CLI via SSH widget or execute TCL scripts.
670479	FortiManager configuration file size may be large due to a bulk of resync files.
671444	FortiManager may fail to check-in configuration revision with the HA secondary unit.
673210	When checking unused policy, implicit policy information is not included.
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.
690969	The dmworker process may consume high memory and CPU resources with failures due to busy handler.
691568	FortiManager GUI may randomly becomes non responsive.
695549	The `_created` timestamp is missing in the REST API return data for *Policy*.
695782	Connection to FortiGate may fail with multiple `fgfmsd` crashes.
697132	In some circumstances, FortiManager is not accessible unless the device is rebooted every couple of days.

Policy and Objects

Bug ID	Description
494367	Users cannot search for an address in a policy where the address is a part of a nested group.
523350	FortiManager does not show the default certificate under SSL/SSH Inspection within policy.
547052	FortiManager GUI should not allow creating *Security Profiles* without any *SSL/SSH Inspection Profile* defined.
565301	Exporting policy package to Excel may not work.
587634	FortiManager may not be able to create new *wildcard FQDN* type address to FortiGate 6.2.

Bug ID	Description
601229	FortiManager is missing *device-type* option for *custom device* dynamic mapping.
608268	Users may not be able to edit firewall policy due to *session-ttl:out of range* in v5.6 or v6.0 ADOM.
612317	FortiManager shows incorrect country code for *Cyprus* under *User* definition.
615936	FortiManager is missing the SSH protocol in DLP filter.
617894	FortiManager is missing IPV6 none values after modifying policy.
630431	Some application and filter overrides are not displayed in the GUI.
633727	FortiManager is unable to display summary of policy package diff for a VDOM with a long name.
647189	FortiManager dynamic object filter generator is adding an "s" at the end of the tag preventing the object from working.
651991	After adding and removing *Security Profile*, the policy *Security Profile* changes from *no-inspection* to empty.
657026	GUI hangs during loading when applying changes made to *Anti Virus* profile.
658528	The URL remote category, *FortiGuard Threat Feed*, is not available in the dropdown menu for *Proxy Address*.
660483	IPS signatures may not match between FortiGate and FortiManager.
661590	FortiManager should fail the install with a proper error message without selecting security profile group on proxy policy.
667414	FortiManager may freeze when editing the *Comment* field in a policy package with many policies.
668649	Install may hang at 75% when no VLAN interface is configured for *fsp managed-switch*.
669389	Install may fail due to web filter profile in flow mode with setting changes available in proxy mode only.
670019	There is no *Decrypted Traffic Mirror* option in policy when only one port mapping is enabled in *Full SSL/SSH* Inspection.
670833	*Search* box for address may not always work.
671265	Global object assignment may not work.
671693	*Internet Service Group* should show an error or a warning when the direction setting is not the same.
671985	*Decrypted Traffic Mirror* setting is not being removed from policy after it is changed in the SSL Inspection method.
671988	FortiManager is not able to push dynamic objects to FortiGate after receiving the configurations from *NSXT* connector.
673305	Policy package install may hang and fail due to high memory usage.

Bug ID	Description
673311	Full *SSL/SSH Inspection* profile's *Invalid SSL Certificates* setting does not take effect when *Inspect All Ports* is selected.
673554	FortiManager should not allow a policy to set the destination address with a *Virtual Server* when inspection-mode is set as *flow*.
673554	FortiManager should not allow a policy to set the destination address with a Virtual Server when inspection-mode is set as *flow*.
674899	FortiManager may not be able to edit proxy addresses objects.
675199	Local web category override is not installed if web filter is part of policy block package.
675501	Policy check may show negative values.
675509	FortiManager may randomly set IPv4 IP Pool object to overload.
675541	Deleting an override entry should trigger modified status for policy packages with *FortiGuard Category Based Filter* enabled within web filter profile.
675587	Firewall VIP hover-over popup should not show ports when port forwarding is disabled.
677385	IPS profile may not load.
678439	FortiManager may always configure empty application parameter values.
681342	Devices are evicted from Installation target after authorizing a new device.
682370	Having changed an IPS profile on security profile, the change is not visible when editing the policy again.
686591	FortiManager may not be able to add individual *VWP* interface members to multicast policy.
688589	Setting the *Local Webfilter Category* action to *Allow* should not disable the action when installed on FortiGate.
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*.
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 and 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.
703639	Installing policy package for a device using CLI template may stall.

Revision History

Bug ID	Description
579286	Installation may fail for FortiGate 6.2 within ADOM 6.0 due to configuration changes with *virtual-wan-link* member weight and volume-ratio, and *internet-service-ctrl*.
637465	Installation fails when installing global v6.2 IPv4 policy to v6.4 FortiGate.
642075	Install may fail with delete *metadata-server* error.
657344	Installing from 6.0 ADOM may try to "*unset inspection-mode* and *unset ssl-ssh-profile* on FortiGate 6.2.
657344	Installing from 6.0 ADOM may try to *unset inspection-mode* and *unset ssl-ssh-profile* on FortiGate 6.2.
660525	Installing from FortiManager, may unset *comment*, *organization*, and *subnet-name* during install.
662438	FortiManager may try to purge all web rating override entries.
662661	Default value of *global: system npu ip-reassembly:max-timeout* NPU setting in ADOM 6.0 for FortiGate-1800F should be changed to *10000* to avoid *Conflict* status.
667148	When a policy install is performed, Install preview shows a lot of firewall policies with *metafield* changes without any actual change being performed.
673101	When *set cfg-save manual* is configured, FortiManager may try to delete objects that do not exist in the FortiGate configuration.
673327	With traffic shaper in *Mbps* or *Gbps*, FortiManager should convert it to Kbps if installation target is non 64 bits FortiGate model.
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.
686036	FortiManager may remove *Allow Access* configurations for secondary IP when a policy package is installed.
689270	The following attributes under *configs vpn ssl setting* may have an 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.
693231	FortiManager tries to purge webfilter *ftgd-local-rating* when directly referenced in URL Category of a policy.

Bug ID	Description
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 get stuck at 85% when pushing multiple policy packages from Global ADOM.
709456	FortiManager may be missing configuration revisions after performing HA failover.
688474	FortiManager may fail to retrieve FortiGate configuration when adding a device due to invalid data source with *wtp-profile*.

Script

Bug ID	Description
663820	The *LDAP* port value remains *636* on device database and FortiManager is not accepting custom port number via CLI script.
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.
702576	Objects may not be present on the corresponding device configuration after running a script to rename objects.

Services

Bug ID	Description
644021	FortiManager should be able to use custom certificate for the update related services.
644173	FortiManager should improve FortiGuard disk space quota usage logging and inquiry.
671387	FortiManager installs the latest IPS and application control signatures on managed device despite that *To Be Deployed Version* is configured.
673307	FortiManager may return *invalid license* to FortiMail and cause *AntiSpam* license to expire.
674511	FortiManager should count FMG expired device number.
677875	Scheduling firmware upgrades may cause *fds_svrd* to consume 100% CPU resource.
691738	FortiManager may not be able to connect to FDS server via IPv6 proxy.
694903	There may be issues with some firmware upgrade paths.
699768	FortiManager should add *06002000NIDS02504* extend IPS database to default download list.

Bug ID	Description
701341	FortiGuard Firmware Images may not show up-to-date FortiOS versions.
704584	FAP firmware may not be listed and cannot be imported.

System Settings

Bug ID	Description
553488	*TACACS* is unable to assign multiple ADOMs to admins.
598194	FortiManager two-factor authentication *admin login* is missing the option for *FTK Mobile* push notification authentication.
623457	FortiManager prompts error while importing CA certificate.
631733	Changing *trusted IP* can be saved and installed.
642205	While FortiAnalyzer model is disabled, FortiManager may fail to create an ADOM due to over size with disk quota.
654370	Users may not be able to access Java console with an error message: *Too many concurrent connections*.
660226	HA may crash when upgrading.
662970	Firewall addresses may not be not visible on GUI after upgrading FortiManager.
667445	FortiManager may show errors on *dynamic_mapping.local-int* during upgrade.
674661	After upgrade, FortiGate VDOM that contains FortiToken user cannot be managed anymore and policy install generates an error.
677118	Upgrading ADOM from 6.2 to 6.4 may fail due to replacement message.
677461	FortiManager is not able to identify ADOMs that are locked by non super user administrators.
684907	Changing the *FortiGuard Server Location* in the *License Information* dashboard may not take any effect.
686569	Creating and deleting the static route may remove a specific connected route.
687223	Users may not be able to upgrade an ADOM because of *profile-protocol-options*.
688517	Upgrading an ADOM may fail due to a 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.
690400	System Admin User ssh-public-key cannot choose *ed25519*.
690921	Upgrading an ADOM from 6.0 to 6.2 should not add custom *ssl-ssh-profile* to policies which were not configured for SSL inspection.

Bug ID	Description
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.
699185	If Management Extension Applications (MEA) are enabled, all system settings may be lost after upgrading FortiManager.
699253	Admin profile should not need system level access to view list of time zones in Device Manager.
704504	*License Information* may keep loading for admin user with *FortiGuard* and *System Settings* with read-write permissions.
705762	Session can be approved twice by different users of the same approval group.
614127	FortiManager should show details in the `fnbamd` debug if login fails due to trusted hosts.

VPN Manager

Bug ID	Description
596953	Go to *VPN manager* > *monitor* and select a specific community from the tree menu to show only that community's tunnels and the monitor page displays a white screen.
608221	There is no *XAUTH USER* column in *VPN Manager Monitor*.
620801	*SSLVPN* > *Edit SSLVPN Settings* > *IP Range*, only shows configuration from ADOM database objects.
647394	VPN Manager with *VPN zone* feature disabled may trigger policy copy failure.
653328	FortiManager is unable to edit a SSL portal in VPN Manager containing "/" special character.
658221	The dns-suffix on SSL VPN portal is not installed if web-mode is disabled.
681110	VPN manager may not push any configuration on ADOM 6.0 for dial up VPN on FortiGate.
697308	VPN Manager is setting *dst-name* to *All* when using `dst-name` object group address in a 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.

Known Issues

The following issues have been identified in 7.0.0. 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.
674636	SSID may be empty in *AP Manager> WiFi Profiles> SSID* column.
701487	FortiManager may not be able to assign AP profile after upgrading the firmware.
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
521976	Users may not be able to enable *CSV format* within system template.
649260	*Device Manager* may return an error when deleting VPN phase1.
664120	When FortiGate HA secondary unit is down, *action* is displayed as *promote* on *Device Manager*.
672344	If managed FortiAnalyzer is in HA, setting *Send Logs* to *Managed FortiAnalyzer* in the system template may cause an install error.
692200	FortiManager may return conflict after a zero-touch-provisioning cluster deployment.
696576	Explicit FTP proxy available certificates are not consistent with the ones available in the FortiGate.
700566	FortiManager should allow user to select different VDOMs when creating an EMAC VLAN.
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.

Bug ID	Description
708937	FortiManager may randomly update the geographical coordinates of a FortiGate device.
709214	System template should allow *source* interface to be selected when *specify* is activated as *interface-select-method*.
709302	SD-WAN monitor search function on the table view does not actually search but highlight.
710570	*Any* statement is not accepted by FortiManager in the *prefix-list* configuration.
713267	Searching for a FortiGate name when editing a device group should display the FortiGate device name with all the VDOMs.
713714	Legacy device and group schedule firmware upgrade will be ignored. FortiGates are upgraded immediately.
714710	Secondary interface configuration may not appear in *Device Manager*.

FortiSwitch Manager

Bug ID	Description
667703	After adding a FortiSwitch, running a script to provision may fail.
713492	In the per-device mapping of the VLANs in FortiSwitch Manager, the *Specify* option for the gateway is not saved in the database.
713553	FortiSwitch Template sflow counter displays an interval value variance between 6.0 and 6.2 ADOMs.

Global ADOM

Bug ID	Description
693510	*Display Options* for *Object Config* will reset to default unexpectedly.

Others

Bug ID	Description
669191	The `fdssvd daemon` may randomly crash.
704545	When there is 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.

Policy & Objects

Bug ID	Description
487186	FortiManager may install a different local category ID to FortiGate causing conflict with custom URL rating list.
636537	*CLI Only Objects* > *user* > *peergrp* is not able to delete *peergrp*.
642708	*View Mode* may unexpectedly change from *Interface Pair View* to *By Sequence* mode.
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 and AWS credential from FortiGate to FortiManager.
684728	FortiManager and FortiGate should have equivalent filter list entries.
688586	Exporting Policy Package to *CSV* shows `certificate-inspection` in the `ssl-ssh-profil`" column even when the profile is not in use.
702621	When adding a remote user group when the LDAP service is unreachable, the *Manually specify* option is only available after a timeout.
704637	Firewall policy and VIPs may get deleted on policy package installation.
705025	*Find Unused Policies* may report incorrect session data for security policy.
707953	IPS sensor may incorrectly set the 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.
711964	Wildcard certificate should be able to be used for *Deep Inspection*.
712150	*Search in Address* may not work after upgrading FortiManager to 6.4.5.
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 a backup ADOM.
685509	FortiManager may unset `authmethod-remote` causing install failure.
693225	FortiManager may install *unset inspection-mode* to FortiGate 6.2 device in 6.0 ADOM.
694380	Installation may fail when *set safelist enable* in *ssl-ssh-profile* is pushed to FortiGate 6.2 from an 6.0 ADOM.
715313	FortiManager may not enable the option *FortiGuard Category Based Filter* after FortiManager is synchronized with FortiGate.

Script

Bug ID	Description
688479	Using *TCL Script* to take device configuration backup may not work.
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
695685	FortiGate HA firmware upgrade may fail when both HA units need disk check.
701777	*Application ID* is not being configured after policy script execution.
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
625683	Changes made by ADOM upgrade may not update *Last Modified* date/time and user admin.

Bug ID	Description
637377	If *Manage Device Configurations* is *none* in admin profile, the user may not be able to see the interface in the policy.
667284	FortiManager should have better log message when aborting device upgrade.
687171	Users may not be able to assign devices to the ADOMs to which they have full access.
690926	FortiManager is removing *SD-WAN* field description upon ADOM upgrading from 6.2 to 6.4.
697082	Schedule SCP backup may fail due to incorrect default port number.
700142	FortiManager should allow users to configure more than eight hosts per SNMP community.
705185	ADOM upgrade may cause per-device mapping of VLANs in FortiSwitch Manager change to 0.
708939	Dashboard is showing incorrect *GB per day* and *device quota* information when *FortiManager* is enabled.
709873	Global task assignment time may not be accurate.
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 is updated.

VPN Manager

Bug ID	Description
695879	Editing a community may not be able to set *VPN zone* to *Off* via GUI.
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.

www.fortinet.com