FortiManager - Release Notes

Version 6.4.0

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

May 7, 2021
FortiManager 6.4.0 Release Notes
02-640-613202-20210507

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-04-09	Initial release.
2020-04-13	Updated Special Notices on page 8.
2020-04-29	Updated Special Notices on page 8.
2020-04-30	Removed FMG-VM64-KVM-CLOUD from Supported models on page 6.
2020-05-01	Added *Citrix XenServer limits and upgrade* to Special Notices on page 8.
2020-05-15	Added 476783 and 511903 to Resolved Issues on page 28.
2020-06-05	Updated FortiGate special branch models on page 20.
2020-06-15	Removed FortiGate models from FortiCarrier models list.
2020-06-16	Updated Supported models on page 6.
2020-06-26	Updated Resolved Issues on page 28.
2020-09-16	Updated FortiOS/FortiOS Carrier on page 14.
2020-09-17	Updated Resolved Issues on page 28.
2021-02-18	Updated Supported models on page 6.
2021-02-22	Updated Virtualization on page 16.
2021-03-04	Added Management extension applications on page 6.
2021-05-07	Updated Downgrading to previous firmware versions on page 10

FortiManager 6.4.0 Release

This document provides information about FortiManager version 6.4.0 build 2002.

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 6.4.0 supports the following models:

FortiManager	FMG-200F, FMG-300E, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3700F, 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).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.0.

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-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 6.4.0 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
SD-WAN Orchestrator	SD-WAN Orchestrator MEA requires 8 GB of RAM.
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 6.4.0.

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.

ADOM Upgrade for FortiManager 6.4

Currently, there is no ADOM upgrade option for ADOM version 6.2 to move to version 6.4. It also means that ADOMs with version 6.2 cannot properly support FortiGates running 6.4. In order to manage FortiGates running 6.4, add them to a 6.4 ADOM.

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 6.4.0.

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. In addition the local password is erased.

A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

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

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

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

Aliyun

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Linux KVM

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

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.

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

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 6.4.0 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 6.4.0 support

This section identifies FortiManager 6.4.0 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 6.4.0 product integration and support for web browsers:

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

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

FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.0 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0
- 6.2.0 to 6.2.3
- 6.0.0 to 6.0.9

FortiAnalyzer

This section lists FortiManager 6.4.0 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 6.4.0 product integration and support for FortiAuthenticator:

- 6.0.0 and later
- 5.0 to 5.5
- 4.3 and later

FortiCache

This section lists FortiManager 6.4.0 product integration and support for FortiCache:

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

FortiClient

This section lists FortiManager 6.4.0 product integration and support for FortiClient:

- 6.2.9
- 6.2.6
- 5.6.6
- 5.4.0 and later

FortiMail

This section lists FortiManager 6.4.0 product integration and support for FortiMail:

- 6.0.9
- 5.4.11
- 5.3.13

FortiSandbox

This section lists FortiManager 6.4.0 product integration and support for FortiSandbox:

- 3.1.2
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiManager 6.4.0 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.4.0 product integration and support for FortiWeb:

- 6.3.2
- 6.2.3
- 6.1.2
- 6.1.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

FortiDDoS

This section lists FortiManager 6.4.0 product integration and support for FortiDDoS:

- 5.3.0
- 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 16.

Virtualization

This section lists FortiManager 6.4.0 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 and 6.7

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.4.0.

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-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-61E, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, 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-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-800D-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E **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 **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-80C-DC, FortiGate-600C-DC, RortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3600C-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC **FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, 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 DC:** FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list.	6.0

Model	Firmware Version
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 **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	

FortiGate special branch models

Model	Firmware Version
FortiGate: FortiGate-100F, FortiGate-101F, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E	6.4
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F,FortiGate-1100E, FortiGate-1101E **FortiGate 6000 Series:** FortiGate-6000F **FortiGate 7000 Series:** FortiGate-7000E **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61F	6.2
FortiGate: FortiGate-30E-3G4G-GBL,FortiGate-40F, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1101E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC **FortiGate DC:** FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:** FortiWiFi-60F, FortiWiFi-61F	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-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-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiCarrier-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

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

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
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	5.0

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

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.4.1

Model	Firmware Version
FortiSandbox VM: FSA-VM	2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ATCA models

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

FortiSwitch models

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

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, 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
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

Model	Firmware Version
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
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

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

FortiProxy models

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

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
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.0-4.2

Resolved Issues

The following issues have been fixed in 6.4.0. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
588096	FortiManager removes the Multiple Pre-shared Key entry after it is edited.
604642	Changing SSID Groups makes changes on all member SSIDs.
521404	Refresh or close button does not work in the AP Health Monitor widget.
553985	FortiManager incorrectly sets "security-external-web" when external authentication is selected.
561911	FortiManager may take over two minutes to display map in AP Manager.
568631	Per-Device Mapping for FortiAP SSID in Bridge mode should not have IP and it is missing VLAN field.
570937	AP Manager should allow individual configure LAN Ports.
578123	Multiple dhcp-relay-ip cannot be defined.
585157	FortiManager is missing 802.11ax/ac related settings on FAPU431F and FAPU433F.
593366	AP Manager may not be able to search for a SSID.
595674	When attempting to place an AP on a map, there is a considerable border around map image where it is not possible to place an AP to the far right or complete bottom of the floor.
597818	ADOM upgrade may delete Floor Map in AP Manager.
600899	FortiManager is unable to delete WiFi profile with forward slash in the name.
603511	AP Manager may try to unset authentication for SSID when device is configured under per-device mapping.

Device Manager

Bug ID	Description
619377	FortiManager cannot retrieve FortiGate-800D containing more than 2048 Firewall custom services.
576850	There may be possible VDOM Name inconsistencies between FortiManager and FortiGate.
594905	FortiManager may take longer to load a system interface.
610015	Scroll bar in the install preview pop-up is not working properly.
544222	In device configuration's log setting, both local traffic log and event logging have *Enable All* buttons that may not work.
544337	FortiManager is missing Firmware information when creating or editing a device group.
555635	Certificate is not visible on GUI after restoring the configuration, which was exported from FortiManager.
563373	FortiManager should support FortiGate-VM FNDN.
593505	Provisioning Template sets incorrect syslog severity level under log settings.
601223	Device database configuration may mismatch with FortiGate even if auto-update happens.
602706	SD-wan Template may keep loading.
616619	Using script or CLI only page, user can create interface-policy without setting srcaddr, dstaddr, or service even though they are required fields.
411914	System Template's "Enable FortiGuard Security Updates" option should check if "antispam-force-off" and "webfilter-force-off" are disabled.
459895	FortiManager may not configure an IPS profile on an One-Arm sniffer interface.
523463	Firmware version not displayed in backup ADOM.
540502	Installation may fail due to interface's address mode changes to PPPoE.
541911	When workspace is enabled, FortiManager cannot run CLI template after it is assigned to a device.
544562	The "Force this Admin to Change Password Next Time He/She Logs on" option on administrator is not installed to FortiGate.
568626	FortiManager can only modify the order of DNS forwarder only if the IP addresses are in quotes ("") and when the IP addresses are not separated by comma.
572337	Config Status may display Modified instead of Conflict status following a failed policy package install.
573293	After upgrade, FortiManager may not be able to import policy package in Workflow mode.
580485	After defined per-device mapping a to model device, all policy packages status are changed to Modified.

Bug ID	Description
580533	Build 0349: Saving configuration with incorrect IP/mask format does not display an error for inner configurations.
581812	Sorting Extenders by Device Name does not work.
584463	CLI Template's comment field cannot be saved.
586550	Device Manager does not detect newly joined Telemetry group on FortiGate.
587513	FortiManager should not unset the IPv6 configuration on FortiGate when registering with the "Add Model Device" method.
587610	FortiManager is unable to show policy package diff of Security Policy.
587693	Users should able to delete interfaces from aggregate interface.
589814	User should be able to make interface changes using CLI Configuration.
589826	Device Manager cannot create EMAC VLAN interfaces over VLAN interface created in root VDOM.
590064	*Device view* > *VDOM* GUI should show which VDOM is the management VDOM.
590321	Sorting filtered static routes list does not work.
590385	FortiManager should not have limit of 1024 for VPN local certificate.
590602	Zero in seconds is lost in Web Filter Override expire time.
591517	FortiManager should not change VDOM configuration scope with CLI Template.
591894	User should be able to specify PAC or HTTPS port on GUI after upgrade.
591981	After modified "set max-revs" value, the change is not immediately reflected on GUI.
592279	AP Manager does not accept certain wtp-profile settings when switching country.
592646	When creating a SD-WAN and disabling its status, it causes neither monitor map view nor table view can be displayed.
593244	User may not be able to change the option, "Send logs to FortiAnalyzer/Manager" under Provisioning Template.
593480	When there is no interface assigned to SD-WAN, neither map view nor table view can be shown.
594211	FortiManager should be able to create new VLAN interface on fabric interface and install to FortiGate.
594348	FortiManager should show buttons to create, edit, and delete TACACS+ on the CLI Configuration page.
594709	Device Manager may not be able to generate Policy Package Diff result.
594853	FortiManager may create duplicate VDOMs when retrieve configuration for multiple devices.
595683	When using workflow mode, changing anything on a policy ID does not modify status of Policy Package.

Bug ID	Description
595803	When configuring PPPoE from CLI Configuration, installation fails with unexpected deletion of system-interface.
595941	Importing policy package may unexpectedly convert regular address objects to dynamic address objects.
597284	When creating a new switch through a script, all configuration is visible in Device Manager but no port configuration is installed.
598230	Removing Per-device mapping causes all referenced Policy Packages status to become modified.
598650	SD-WAN monitor table view may not show data for FortiGate 5.6 device.
598912	Device Manager may not be able to display newly created VDOMs.
599141	After upgrade, Policy Route menu no longer displays Source Addresses or Destination Addresses.
599768	FortiManager may not be able to display the second shelf manager.
599769	FortiManager may not be able to "Enable Security Fabric" on some FortiGate platforms.
602275	FortiManager may not be able to remove VDOM or device when FortiAnalyzer feature is enabled.
603215	Fabric is not enabled in allow access after enabling FortiLink on an interface.
603405	FortiManager cannot set radio-2 band to "802.11ax" under CLI Configuration.
603522	Fabric should be shown as an option for administrative access.
603542	Password field should not be deleted when making changes to PPPoE interface.
603606	FortiManager should accept volume ratio value of 0 within SD-WAN configuration.
603820	FortiManager fails to import policy when reputation-minimum and reputation-direction are set.
604269	FortiManager should permit Virtual Wire Pair to use Aggregate interface.
604808	Verification may fail on system interface tc-mode or phy-mode when installing to FortiGate-60E-DSLJ.
605178	FortiManager should be able to set "None" interface under on Policy Route.
605946	Import may fail where there are objects with truncated names.
606628	FortiManager may fail to retrieve configuration with SAML SP IDP certificate.
607672	Import may fail with error "user group match is not a member".
608642	Importing policy should not make dynamic mapping for policy object when there is only change on hidden attributes.
609757	Adding a new device on SD-WAN Template may cause Config status to change to Modified on all devices.

FortiClient Manager

Bug ID	Description
548572	FortiManager shows unclear message in FortiClient Profile with "Response with errors" instead of "Device groups cannot be empty".

FortiSwitch Manager

Bug ID	Description
503722	FortiSwitch Manager and AP Manager reports switches and APs connected to FortiGates as online when the devices are no longer powered on.
573043	Saving FSW VLANs configuration may trigger error and lead to data loss in Per Device Mapping.
587526	VLANs in FortiSwitch templates must support per-device secondary IP.
597715	Under FortiSwitch Manager Per device mode, FortiManager may prompt error *[object Object]* when trying to create a VLAN with in use VLAN ID.
601242	Installation may fail due to qtn.fortilink configuration cannot be deleted.
601712	Under Workflow mode, FortiManager may lose FortiSwitch templates and VLAN configuration.

Global ADOM

Bug ID	Description
578089	Address objects cannot be deleted from the FortiManager's Global ADOM if they are not being used anywhere.
582171	FortiManager may not be able to assign all objects from 5.6 global ADOM to a 6.0 ADOM.
587511	*gSSO_Guest_User* should work the same as predefined *SSO_Guest_User*.

Others

Bug ID	Description
609040	Device manager may be empty after upgrade.

Bug ID	Description
364541	The command, diagnose dvm support list, should include all supported platforms.
581140	The SNMP, FmDeviceEntPolicyPackageState, always returns (-1), which indicates never installed, regardless of the actual policy package status.
591206	The SNMP trap, fmDeviceTable, should show VDOM information as well.
611548	The dbcache.db file size may keep increasing.
550140	The system-support-fgt configuration is lost if there is a version lower than 5.4 selected prior to upgrade.
551937	FortiManager should only allow the browser to save and paste credentials at the logon prompt only.
552085	FortiManager live migration fails with Microsoft Hyper-V and it is not accessible via GUI and SSH.
565515	User may not be able to create a new SNMP host under System Templates. Workaround: Please add a new SNMP host for System Templates under CLI Configurations within Device Manager.
571235	Enabling policy hit count may lock ADOM and provoke GUI slowness.
574731	Builds 0349 and 1121: Some hardware specific SNMP traps are missing from the device SNMP settings and the system provisioning templates.
579648	FortiManager may generate "fgfmsd" crashes when FortiGate sends registration request to FortiManager.
584053	FortiManager may show fmgd crashes after switched among pages.
586991	"Logver" field is missing when FortiAnalyzer is enabled affecting report related features.
589805	Installing policy package via JSON API with missing interface in zone definition deletes zone and corresponding firewall policies on FortiGate.
590037	FortiManager CPU usage may spike when going to interface and VPN Phase1 or Phase2 page.
590649	On FortiClient or FortiDDoS ADOM, the SOC page may refresh constantly.
593245	FortiManager may show incorrect warning when changing admin profile via CLI.
593421	Running ADOM integrity check may cause cdb reader to crash.
593819	FortiManager may generate several fmgd crash logs.
595589	When running a script on a device with large configuration, dmworker may crash with high CPU spike.
595741	After ADOM upgrade, FortiManager may report an error on reaching the max limit of firewall-service-custom.
601978	Diagnostic command may fail to repair database when device is in standalone mode but there are entries in HA member table.
602216	FortiManager is unable to add SNMP hosts when set alias is configured on a port.

Policy and Objects

Bug ID	Description
622040	Security Policy is missing Implicit Deny policy.
615823	VPN tunnel is not unset when changing the action of the firewall policy from IPSEC to Accept.
598938	FortiManager should allow setting wildcard-fqdn type firewall address as destination on proxy policy.
602176	Creating a proxy policy with a profile group adds additional security profile.
604577	When logged in as a Restricted Admin or regular User, it is not possible to reference "Web content filter" in a web profile.
612672	The policy block hit count stays at zero even if the counter increments properly on the FortiGate side.
488897	SSL VPN policy can be created with a FSSO user group assigned to the policy.
491813	FortiManager should group IPS Sensor entries with same filters as one rule.
505887	Internet Service should separate into source and destination
528881	Users are not able to remove all FSSO objects from selected list that has a large number of entries.
544404	When a remote user approves a session, session list shows zero sessions.
545605	Searching on Created Time or Last Modified does not work on policy table.
548573	FortiManager changes UUIDs of existing objects after policy install.
563629	Clicking on "+" function should allow users to add Wildcard FQDN objects.
566446	With a 5.6 ADOM and install to 6.0 FortiGate needs to keep the configured multicast policies and zone on FortiGate.
569576	Build 1121: Web rating override category change is not reflected in GUI.
571473	FortiManager should have "Configure Default Value" option for IP Pool.
573250	Find Duplicate Objects may show inaccurate results due to obj-id.
574560	Installation from FortiManager may fail with the error, "No response from remote" FortiGate.
578004	The policy interface colors are different between Device Manager and Policy & Objects.
580484	Signature, "Apache.Optionsbleed.Scanner", cannot be selected as IPS Signature but only as "Rate based Signature".
581495	Interface Validation should prompt only once per unmapped interface.
581607	FortiManager 6.2.2 may not be able to install class-id to a FortiOS 6.2.1 device.
581825	In workflow mode, changes to the SSL VPN portals do not trigger "Modified" status on the policy package.

Bug ID	Description
585021	Adding or modifying rate based signature on IPS profile resets all rate based signature to default settings.
587624	Application Control profile page is blank for User with read-write permissions on Policy & Objects.
588548	Under workspace, addresses may be removed from a firewall policy when merging duplicated addresses.
588684	Central SNAT option in missing under Policy Package menu when mode is NGFW policy-based.
589645	GUI disables FSSO status after its removed one of the FSSO user groups with a policy.
589771	Policy Package installation fails when a Firewall Policy contains a VIP Group mapped to a zone interface.
589775	Entry without content should not be created when creating an Application Control Profile.
589795	User should be allowed to create a new tag in firewall policy or select an existing tag.
589808	After edited policy in policy package, the screen view should remain on the edited policy.
590322	When an Internet Service Database object is used in the destination field on proxy rule, the field is displayed as an empty field.
590896	FortiManager has no source interface column in the general view of Proxy Policy.
593853	Certificate generation fails if the CA certificate does not match ADOM name.
594549	Editing Per-Device mapping for zone containing slash in the name generates "Method failure" error message.
594811	Using copy and paste on multiple proxy policies may insert rules in reverse order.
594866	Internet Services may not match between FortiManager and FortiGate.
594957	SSL/SSH Inspection profile should not allow "Untrusted SSL Certificates" to be set to Block.
595646	After selecting a proxy policy and using the "Insert Above/Below" button, the new policy should be created with the same proxy type of the selected policy.
597668	FortiManager should be able to install the scheduled policy package even though it is scheduled by wildcard user.
597879	Policy package installation fails with commit check error on system interface dhcp-relay-type.
598493	FortiManager should get all datacenter information from exsi vm info.
598656	When long-vdom-name is enabled on FortiGate, installing from FortiManager may show nothing to install.
601073	When renaming address object, the error "invalid value" is prompted when it should be "object already exists".
601081	FortiManager is missing the feature to change IPS Signatures status.

Bug ID	Description
602600	FortiManager may show any duplicate sections in the policy page.
602871	FortiManager may show zero on First use, Last used, and Byte count on policy.
604159	Cloning an existing policy package adds the "clone_of_" to the name even the feature is disabled.
605947	FortiManager is unable to configure hold down-interval for Virtual Server.
606721	FortiManager should not allow users to create firewall address with a name which is in conflict with the name of existing wildcard-fqdn addresses.
607370	When workspace is enabled, auto-install fails with error "no write permission".
607958	FortiManager should be able to modify Per-device mapping for global VIP in local ADOM.
608105	When making changes to Virtual server or Health check for load balance, should be detected and installed to FortiGate properly.
608236	FortiManager is unable to install ssl-ssh-profile policy updates when disabling protocols on a policy.

Revision History

Bug ID	Description
612781	FortiManager should try to remove any referenced policies prior to creating a zone interface.
492088	FortiManager attempts to change Chassis ID on FortiGate 7000 series when installing configuration.
543507	Install fails for newly defined transparent VDOM's management IP.
555796	Installing policy on 6K series FortiGate may remove the interface setting "set forward-error-correction rs-fec".
560888	FortiManager may unexpectedly reset some parameters for IPS sensor entry.
605899	FortiManager should not mandate the use of the access key, secret key, and region fields for SDN Connector.
609110	Config revision created by Script_manager causes error when restored onto the FortiGate directly.
610687	FortiManager should not unset forward-error-correct during install.
613057	During install verification, FortiManager is changing the IP of uni-cast heartbeat interfaces after FortiGate cluster failover.
513317	FortiManager may fail to install a policy after FortiGate failover on Azure.
539829	FortiManager should be able to delete FortiGate default admin user from FortiManager.

Bug ID	Description
539994	Installing to FortiGate fails when wildcard-fqdn address is used in SSL profile.
560638	When checking the Revision Diff between two revisions for multiple times, the result may not be consistent.
560689	Auto-Update revision is missing "set stp-bpdu-guard enabled".
578231	FortiManager tries to push "casi-profile" on a Deny Policy.
582882	Switch interface should not have duplicate members during device install.
583833	Auto Link Install skips installation for VLAN interface.
584118	Router access-list rule's default value is mismatched causing installation failure.
586979	FortiManager may complain about duplicate tags and fail to install policy package.
586992	FortiManager does not install broadcast-forward enabled on "Virtual Switch" to managed FortiGate.
587005	FortiManager should support the radius-server-vdom setting and be able to install it.
589858	The BGP "scan-time" value of 0 can be set on FortiGate, but FortiManager resets it to default by "unset scan-time" on the next policy push.
590325	Installing EMAC-VLAN may fail on verifying device-identification setting.
592062	Custom Internet Service created on FortiManager systematically fails to be installed on the target FortiGate.
592315	Installation of Policy Package against a device group may generate copy fail error for one FortiGate device.
594147	FortiManager does not perform interface binding contradiction check when a firewall policy is using an address group and the user changes an address group member.
597353	Policy install may remove auth-redirect-addr when disclaimer is set.
598173	When changing the "User Group Source" from Local to Collector Agent, FortiManager should automatically unset the undesired commands.
599413	Policy Package Diff is showing differences for passwords when there is no actual difference.
600085	Some special characters may cause revision history not saved with a full tmp folder.
600833	When trying to create a local certificate, and assign and install it for remote administration, the install operation fails due to incorrect order of configurations.
601668	FortiManager may install overlapping VIP objects to FortiGate.
602272	Installing UUIDs from local-in policies for FortiGate-60F may cause installation failure.
605187	FortiManager may fail add members into a zone.
607216	When master-device is set on custom device, type should not be available on FortiManager.

Script

Bug ID	Description
593217	FortiManager is unable to delete Virtual-Switch members via script if the remaining members of interfaces is less than two.
535066	Task Monitor for script task shows browser 500 error if the return button is selected.
587015	When user tries to set signature with non escaped quotes from script, the signature becomes separate strings, and the installed string may not be what is expected.
590889	Using the search bar to assign devices under provisioning templates clears the previous selected device list.
594238	FortiManager should be able to create overlapping secondary IPs via a script if interfaces are assigned to different VDOMs.
594238	FortiManager should be able to create overlapping secondary IPs via a script if interfaces are assigned to different VDOMs.

Services

Bug ID	Description
563624	FortiManager dbcontract updated with the entitlement file shows different contracts compared to FortiManager dbcontract updated from FDS.
535066	Task Monitor for script task shows browser 500 error if the return button is selected.
587015	When user tries to set signature with non escaped quotes from script, the signature becomes separate strings, and the installed string may not be what it is expected.
590889	Using the search bar to assign devices under provisioning templates clears the previous selected device list.
594238	FortiManager should be able to create overlapping secondary IPs via a script if interfaces are assigned to different VDOMs.

System Settings

Bug ID	Description
611825	FortiManager fails to edit the device interface when FortiSwitch is set to RO within admin profile.
592156	Upgrade task for managed devices in Task Monitor always shows Pending status with 0.

Bug ID	Description
599812	Stager or pusher admin has no permission to view VDOM interface mapping.
202924	FortiManager should be able to restore a large backup file via web interface.
535607	Upgrading ADOM may take a long time due to hit count statistics.
570266	When saving the values of the administrative access, the values do not save when unchecking HTTPS first before any other value.
571181	An admin user with read-write system permissions and restricted to one ADOM can change their permission to All ADOMs.
576098	Event log may not show the correct username when changing a non policy related object.
581450	ADOM upgrade may hang when DNS or URL filter name is null.
584392	Admin user with read-only profile should not be allowed to "Revoke Release" in DHCP query and "Bring Tunnel Down/Up" in Query IPsec.
584749	System Settings may not show the ADOM-VDOM association.
587242	Build 349: HA Cluster fails after upgrading to 6.0.6 with peer IP using IPv6.
587295	Admin users with prof_admin_regional profile should be allowed to see all application signatures.
588852	Idle time is constantly reset for inactive users.
588884	Event log for merging duplicated objects is missing object name.
594556	Admin user may not able to authorize FortiGate.
595660	FortiManager should generate event logs for imported images.
596562	Administrators allowed to access to only specific ADOMs cannot see "Managed Devices" in those ADOMs.
596580	Upgrade ADOM may fail on FSSO/SSO.
597765	ADOM upgrade may stuck with "svc cdb reader" crashes.
599847	FortiManager may not be able to move VDOMs with long names among different ADOMs.
604069	IPv6 communication fails after setting interface status between down and up.
606545	There may be HA synchronization issues when policy hit count is disabled.
608378	FortiManager is unable to upgrade ADOM due to name conflicts in wildcard FQDN address.
611637	Policies are not visible when workflow session is created in an ADOM that is upgraded.

VPN Manager

Bug ID	Description
616352	FortiManager may show empty value for phase1 and phase2 proposals.
554080	VPN monitor may not list all mesh tunnels if the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service.
562729	VPN Manager SSL VPN monitor's Active Connections column may be blank.
574727	VPN Manager may not display SSL-VPN settings for some devices.
586613	FortiManager may randomly install incorrect Phase1 proposal settings.
587760	Address group dynamic mapping is ignored when it is used as a protected subnet with VPN Manager.
589101	VPN Manager prompts the copy error "no hub configured for vpn" if the hub is external gateway with no device assigned.
589669	FortiManager shows installation error when there are two Hubs in VPN community where Hub-to-Hub Interface is set to 'None'.
590765	The tunnel-search and net-device attributes are not being installed if device role is set as spoke.
599242	For Dialup tunnels, auto-negotiate should only be applied to spokes.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
476783	FortiManager 6.4.0 is no longer vulnerable to the following CVE-Reference: • CVE-2020-9289
511903	FortiManager 6.4.0 is no longer vulnerable to the following CVE-Reference: • CVE-2004-0230
597311	FortiManager 6.4.0 is no longer vulnerable to the following CVE-Reference: • CVE-2004-1653
606144	FortiManager 6.4.0 is no longer vulnerable to the following CVE-Reference: • CVE-2019-9193
603256	FortiManager 6.4.0 is no longer vulnerable to the following CVE-Reference: • CVE-2020-12811

Known Issues

The following issues have been identified in 6.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
610116	FortiManager cannot choose platform mode between Dual 5G and Single 5G for FAP-U431F or FAP-U433F.
620460	FortiManager needs to update Frequent Handoff and AP Handoff as global settings instead of per radio.
620522	Import fails on FAP-U431F or FAP-U433F, which has DFS channels configured for Japan or Taiwan region.
624238	Changing AP mode to dedicated monitor may cause install to fail.
555159	AP Manager still shows the SSID after deleting it from Device Manager,
620117	AP Manager needs to support of FortiAP-U431F and FortiAP-U433F.
623903	AP Manager cannot upgrade FortiAP's firmware image.
607107	FortiManager prompts installation errors when certain channels are selected for Radio 2 in 5 GHZ band of FAP-421E.

Device Manager

Buzz ID	Description
619025	FortiManager's SD-WAN shows internal DNS on SLA as PING.
544982	Policy Package Status may get out-of-sync for all devices when adding one device to Install On.
615092	FortiManager should allow using FQDN for FortiAnalyzer logging.
616264	IPv6 extra-address may not convert properly.
619106	When importing a policy, the conflict page may truncate outputs.
589453	Application group of type category should not be used for SD-WAN rules.

Buzz ID	Description
593364	FortiManager does not install md5 key for OSPF interface configured from Device Manager.
594474	FortiManager ADOM in backup mode is not backing up device configuration changes from super_admin remote radius accounts.
595058	When the user sets *Scheduled Updates* configuration to *1 hour* in FortiGuard on Device Manager, FortiManager installation preview is configured as *set time 1:60*.
599819	Changing static route from subnet to named address does not push the change to FortiGate.
601692	FortiManager is unable to overwrite IPv6 default route.
525051	Automation stitch cannot add FortiGates to automation.
552492	VAP is always loading under CLI configuration.
558176	Interface-subnet type addresses interface are re-set to zone after they are imported leading to copy fail during install.
547768	FortiManager should allow easier management of the compliance exempt lists.
586809	FortiManager incorrectly counts VDOM licenses for FortiGate 7000 series.
598916	When creating user groups via CLI Only Objects, comma separated values are treated as a string instead of a list.

Global ADOM

Bug ID	Description
623916	Installing global firewall policy with internet service name may fail for FortiGate 6.4.
624186	Install may fail when un-assigning and reassigning global policy package.
624265	FortiManager may fail to edit global policy to change source or destination address from IPv4 to IPv6.

Others

Bug ID	Description
622411	Valid zone and interface mappings are deleted after running the `diag cdb check policy-packages` command.

Policy & Objects

Buzz ID	Description
621400	FortiManager incorrectly sets service to *None* when service is set as *Specify* causing the install to fail.
622292	When a IPv6 SNAT policy is created on FortiGate and then imported to FortiManager, the policy summary table cannot show the source or destination address.
612317	FortiManager shows incorrect country code for Cyprus under *User* definition.
614710	Result of search in device interface should display zone that the interface is a member of.
617031	Right-clicking on *IPv4/Proxy Policy* or *Installation Targets* should not reload the page if the related information is already displayed.
618321	FortiManager is unable to create RSSO Group if Agent is configured with custom name.
618499	Right-clicking to edit the zone incorrectly prompts dynamic interface window.
523350	FortiManager does not show the default certificate under SSL/SSH Inspection within policy.
578501	FortiManager should show global icon for global objects assigned to ADOMs.
586026	FortiManager should display zone icon based on existing and non existing dynamic mappings.
599780	If there is one or more devices that has policy validation error, FortiManager does not add devices that are "ready to install".
545759	From or To column filter displays unmapped interfaces in the drop-down list.
547052	FortiManager GUI should not allow creating Security Profiles without any SSL/SSH Inspection Profile defined.
577201	Next button should be inactive until zone validation is fixed in the case of 'Re-Install Policy'.

Revision History

Bug ID	Description
594933	Re-installing Policy Package cannot skip to install policy package, which fails validation.
597650	FortiManager cannot install allowed DNS and URL threat feed configuration.
473517	FortiManager should have a proper progress bar for device install preview.

Script

Bug ID	Description
623841	When device filter is set, FortiManager may return loading fail when running a script.

Services

Bug ID	Description
437935	FAD-VM license may not be validated on FortiManager.
541192	FortiManager should keep firmware image files when the files are for different FortiExtender devices.

System Settings

Bug ID	Description
611215	SNMP Hosts in SNMP Community are not displayed in the GUI if ADOM is unlocked.
556334	Standard ADOM users should be able to assign system templates to FortiGate devices.
586626	Users should be able to identify who locked their assigned ADOM.

VPN Manager

Bug ID	Description
621187	When a route is added in the Portal of SSL VPN, the policy package is shown as modified but install preview shows "No command to install".
621209	VPN monitor should show the corresponding VPN community tunnels only under each community.
596953	When the user goes to *VPN manager* > *Monitor*, and selects a specific community from the tree menu to show only that community's tunnels, the monitor page displays a white screen.

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
```

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.