FortiManager - Release Notes

Version 6.4.2

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

May 7, 2021
FortiManager 6.4.2 Release Notes
02-642-651939-20210507

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-06	Initial release.
2020-08-07	Updated Resolved Issues on page 28.
2020-08-10	Updated FortiGate special branch models on page 20 and Known Issues on page 34.
2020-08-13	Updated Special Notices on page 8.
2020-08-17	Updated FortiClient on page 14.
2020-09-16	Updated FortiOS/FortiOS Carrier on page 14.
2020-10-15	Updated Virtualization on page 16.
2021-01-04	Updated Supported models on page 6.
2021-02-18	Updated Supported models on page 6.
2021-02-23	Updated Virtualization on page 16.
2021-03-04	Added Management extension applications on page 7
2021-04-12	Added FortiManager VM subscription license on page 6.
2021-05-07	Updated Downgrading to previous firmware versions on page 10.

FortiManager 6.4.2 Release

This document provides information about FortiManager version 6.4.2 build 2122.

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 6.4.2 supports the following models:

FortiManager	FMG-200F, FMG-200G, 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).

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 10.

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

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

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.2.

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 6.4.2 have minimum system requirements. See the following table:

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

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.2.

Wireless Manager (FortiWLM) not accessible

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

SD-WAN Orchestrator not accessible

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

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

```
diagnose docker upgrade sdwancontroller
```

Support for FortiOS 6.4 SD-WAN Zones

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

FortiGuard Rating Services with FortiGate 6.4.1 or Later

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

Citrix XenServer default limits and upgrade

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

To increase the size of the ramdisk setting:

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

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

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

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

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

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
end
```

Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.2.

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 6.4.2 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 6.4.2 support

This section identifies FortiManager 6.4.2 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 6.4.2 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 79
- Google Chrome version 84

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

FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.2 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.2
- 6.2.0 to 6.2.5
- 6.0.0 to 6.0.10

FortiAnalyzer

This section lists FortiManager 6.4.2 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 6.4.2 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 6.4.2 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 6.4.2 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.7

- 5.6.6
- 5.4.0 and later

FortiMail

This section lists FortiManager 6.4.2 product integration and support for FortiMail:

- 6.0.10
- 5.4.11
- 5.3.13

FortiSandbox

This section lists FortiManager 6.4.2 product integration and support for FortiSandbox:

- 3.1.3
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiManager 6.4.2 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.4.2 product integration and support for FortiWeb:

- 6.3.5
- 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 6.4.2 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 6.4.2 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, 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	✓	✓	✓	✓
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 6.4.2.

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

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-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 **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F,	6.4

Model	Firmware Version
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	
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 **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate DC:** FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D, FortiWiFi-60F, FortiWiFi-61F, **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

FortiGate special branch models

Model	Firmware Version
FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G	6.4
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-1800F, FortiGate-1801F **FortiGate 6000 Series:** FortiGate-6000F **FortiGate 7000 Series:** FortiGate-7000E **FortiGate Rugged:** FortiGateRugged-90D **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWifi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E	6.0

Model	Firmware Version
FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC **FortiGate DC:** FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:** FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-41F, FortiWiFi-41F-3G4G,	

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

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

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 **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ATCA models

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

FortiSwitch models

Model	Firmware Version
FortiSwitch: FortiSwitch-108D-POE, FortiSwitch-108D-VM, FortiSwitch-108E, FortiSwitch-108E-POE, FortiSwitch-108E-FPOE, FortiSwitchRugged-112D-POE, FortiSwitch-124D, FortiSwitch-124D-POE, FortiSwitchRugged-124D, FortiSwitch-124E, FortiSwitch-124E-POE, FortiSwitch-124E-FPOE, FortiSwitch-224D-POE, FortiSwitch-224D-FPOE, FortiSwitch-224E, FortiSwitch-224E-POE, FortiSwitch-224E-FPOE, FortiSwitch-248D, FortiSwitch-248D-POE, FortiSwitch-248D-FPOE, FortiSwitch-248E-POE, FortiSwitch-248E-FPOE, FortiSwitch-424D, FortiSwitch-424D-POE , FortiSwitch-424D-FPOE, FortiSwitch-448D, FortiSwitch-448D-POE, FortiSwitch-448D-FPOE, FortiSwitch-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	5.8.6

Model	Firmware Version
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	
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
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 6.4.2. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
599666	Empty LLDP status information is shown under AP Manager.
619796	When "JSON API Access" is set properly, admin user cannot authorize or deauthorize FAP, FSW, or FEX.
556036	FortiManager cannot configure AP profile *short-guard-interval*.

Device Manager

Bug ID	Description
581940	SD-WAN Monitor may show gaps on the SD-WAN monitoring graph.
593364	FortiManager does not install md5 key for OSPF interface configured from Device Manager.
599852	When password policy is set as enforced, FortiManager should not accept password if it does not meet the policy.
603291	Group membership may be incorrect after adding a VDOM.
603820	FortiManager fails to import policy when reputation-minimum and reputation-direction are set.
612355	Policy Package status remains in modified status after using "Push to device" on an updated object.
619106	When importing a policy, the conflict page may truncate outputs.
626598	Custom Device Meta Fields cannot be modified.
633767	Japanese typo in NTP Service of DHCP Server setting.
637630	FortiManager is not showing interface status in device manager interface page.
637672	Importing AP Profile in AP Manager may cause Config Status changes to "Modified".
642348	Policy package diff from Device Manager may not work.

Bug ID	Description
642817	Importing an interface may report *datasrc invalid* error if trying to map an interface to an ADOM with a different name.
643172	FortiManager does not support `dnsproxy-worker-count` higher than two.
644223	FortiManager is unable to add FortiAnalyzer and triggers an error: *Object does not exist*.
647664	The loopback interface should not be allowed to be added into the zone interface in *Device Manager*.
648842	CLI only object is missing the `fmg-source-ip4` setting.
649195	Editing an address group does not trigger any configuration change when installation target is set to specific device(s).
649711	FortiManager is unable to add FortiAnalyzer and fail to synchronize FortiAnalyzer with current ADOM data with error: *Fail(errno=-3):Object does not exist.*
650768	When using the model device auto-link feature, FortiManager should keep the remote FortiGate configuration during auto-link install.

FortiSwitch Manager

Bug ID	Description
585926	FortiSwitch Manager under per-device or central mode has no support for multiple FortiLink interfaces.
642959	When re-installing or installing any policy package, FortiManager tries to install *security-8021x-dynamic-vlan-id* even if there is no 8021x authentication configured on FortiManager.

Global ADOM

647736	Global ADOM policy package assignment may fail.

Others

Bug ID	Description
626338	The `exec fmpolicy` CLI command may not print out a policy package correctly.

Bug ID	Description
643784	FortiManager is crashing on security console and wizard is stopped at 50% of deployment.
647791	Cloning VDOM object may fail via CLI.

Policy and Objects

Bug ID	Description
540716	Under *Policy Package*, the *Column Settings* dropdown list does not display the *Session Count*, *Session First Used*, and *Session Last Used* options .
545605	Searching on *Created Time* or *Last Modified* does not work on policy table.
569226	Section title should always be displayed for filtered policy and section title should not be deleted after policy was deleted.
578501	FortiManager should show global icon for global objects assigned to ADOMs.
591540	Export policy package to excel returns empty packages when table is not loaded.
593417	FortiManager shows incorrect action for allowing invalid SSL certificates.
594888	FortiManager is unable to export policies to excel when *consolidated firewall mode* is enabled.
601385	Restricted mode admin cannot install Web Rating Overrides changes.
615117	Policy Package section is not sent over to FortiGate if Policy Blocks are under the section in FortiManager.
617031	Right-clicking on *IPv4/Proxy Policy* or *Installation Targets* should not reload the page if the related information is already displayed.
626060	FortiManager cannot set per-device mapping for `user-radius-accounting-server-source-ip`.
628389	When workspace is enabled, Policy Package Status may change to *Modified* but there is nothing to be installed.
630033	Editing firewall policy and adding *FSSO Groups* is not displayed correctly.
630055	Some custom application signatures have id 0 in application list.
630582	Deleted policy IDs may still appear in the GUI.
630891	Cloned policy may not get installed onto devices.
631134	Profile type should be set to group if drag and drop security profile group into policy.
632715	In DoS policy, changing quarantine from attacker to none keeps quarantine-expiry set incorrectly.
633431	Changing to *Classical Dual Pane* disables *Policy Hit Count*.
633727	FortiManager is unable to display summary of policy package diff for a VDOM with a long

Bug ID	Description
	name.
636010	FortiManager cannot push custom application signatures from different policy packages to the same FortiGate.
636133	When is `bfd` disabled, FortiManager should exclude `bfd-desired-min-tx` and `bfd-required-min-rx` from installation.
637688	FortiManager prompts the error message, "The data is invalid for selected url", when copying and pasting policy to a different policy package.
639753	After a FortiToken is activated on the FortiGate, the next policy install from FortiManager would unset "reg-id" and "os-ver" on the token.
640400	FortiManager may purge the list of resolved IPs of a dynamic address on the FortiGate.
643098	FortiManager may have slow installation of policy package due to many VIPs with the same external VIP.
643113	Changing an *Accept* policy to *Deny* in a policy that contains a *Security Profile Group* results in installation failure.
643930	Finding *Duplicate Objects* does not display duplicated addresses if wildcard is empty.
643957	When there are many firewall addresses, FortManager may be slow to show all addresses under *CLI Only Objects*.
645367	Discarded policy deletion in Policy Package may delete all policies while they are still visible in the GUI.
645661	A valid custom IPS signature may still trigger invalid IPS data error.
645960	FortiManager only sets profile feature set to proxy if the AV profile is used in proxy based policy.
647337	FortiManager may fail to retrieve FSSO user groups via FortiGate.
461746	FortiManager is unable to delete IP Pool Object when disabling Dynamic IP Pool in a policy.
630891	Cloned policy is not installed on devices (global ADOM v5.6).

Revision History

Bug ID	Description
594933	Re-installing Policy Package cannot skip to install policy Package, which fails validation.
610687	FortiManager should not unset `forward-error-correct` during install.
613901	FortiManager may not be able to show more than one log based on one revision ID.
622540	FortiManager prompts error, 'no hub configured', for a site even the site is not part of VPN Manager.

Bug ID	Description
632129	The `syslogd` setting `source-ip` is still visible after setting status to disable, which causes verification failure.
633515	FortiManager should improve the error message when FortiManager receives blank or invalid configurations from FortiGate.
634345	Install preview may not show CLI configurations correctly.
637076	Installing PPPoE interface may fail.
641145	FMG-GCP-VM may always revert MTU to 1460.
643803	Policy Package Diff may shows all objects as new changes.
645929	If FortiGate and FortiManager have the same ISDB version, objects should match and installs should not fail due to mismatched internet service objects.
646372	When the user applies changes to a policy package, then all the policy packages in this ADOM change to a "Modified" state.

Script

Bug ID	Description
634242	After applying profile-type group on a firewall policy via a script, proxy and SSL profiles should be removed from the corresponding firewall policy.

Services

Bug ID	Description
569679	Port 8888 or 8889 should not always be opened.
647680	When importing firmware image for FAP 321E, FortiManager reports the platform as a invalid model.
654214	FortiManager cannot connect to FDS server via proxy when using FortiGuard Anycast.

System Settings

Bug ID	Description
618213	When trying to upgrade FortiManager cluster from FortiManager Master GUI, FortiManager

Bug ID	Description
	Master is rebooting before finishing to send firmware to FortiManager Slave.
628006	Even though a user has 'Manage Device Configurations' R/W privileges, the user appears to have partial permissions within Device Manager.
637044	FortiManager may not be able to save changes under Workspace mode and prompt error "Workspace request failed, please try again."
643246	FortiManager may not be able to save the remote server LDAP configuration with special characters in Organizational Unit names.
644660	Installation preview may stuck and system may running out of memory.
493533	FortiManager needs to rename custom 'default' protocol option after upgrade.
641018	Upgrading Global ADOM may fail due to *Fortinet_NSX* local certificate.

Known Issues

The following issues have been identified in 6.4.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
607107	FortiManager prompts installation errors when certain channels are selected for Radio 2 in 5 GHZ band of FAP-421E.
599189	FortiManager should be able to handle upgrading more than 10 APs at once.
607170	Dynamic VLAN option is not saved in SSID in AP Manager.
633171	There may be a DFS Channel mismatch between FortiManager and FortiGate for FAP-223E.
645030	Adding FortiGate using custom admin profile may fail to list FAP in AP Manager.
645713	FortiManager is able to create SSID which cannot be deleted after.
648812	DHCP server is incorrectly created for Bridge SSID.
653329	FortiManager is sending the wrong device setting after changing the FAP name.

Device Manager

Bug ID	Description
547768	FortiManager should allow easier management of the compliance exempt lists.
552492	VAP is always loading under CLI configuration.
595058	The user sets *Scheduled Updates* configuration to *1 hour* in FortiGuard; however, in the FortiManager *Device Manager*, the installation preview is configured as "set time 1:60".
598916	When creating user groups via *CLI Only Objects*, comma separated values are treated as a string instead of a list.
610568	FortiManager may not follow the order in CLI Script template.
627749	Admin user with `device-config` set as `read in admin profile` cannot download configuration revision.
640907	FortiManager is unable to configure FortiSwitch port mirroring.

Bug ID	Description
598424	Interface cannot create more than 48 IP-MAC bindings in DHCP reservation from GUI.
602393	Device joined telemetry not showing on FortiManager under Telemetry group.
604125	FortiManager may not be able to edit VDOM link interface from VDOM level.
605688	Pac file data limited to 4000 characters under CLI Configuration.
607923	*Security Fabric Connection* option is removed from VLAN interface after changes are applied.
613029	SD-WAN Monitor is showing effect of exceeded SLA even if when it is disabled.
625541	Changing a certificate on FortiGate triggers auto-update that may incorrectly update partial configuration on multiple VDOMs.
627664	FortiManager cannot work with socket-size 0 and changes it to 1 automatically.
630316	After auto-conf IPv6 address is changed on FortiGate, the address is not updated into device database.
635316	Return button is not working when viewing HA mode.
636012	Importing a policy may report conflict for the default SSH CA certificates.
636357	Retrieve may fail on FortiGate cluster with "Failed to reload configuration. invalid value" error.
636638	Fabric view may stuck at loading.
638061	FortiGate 7000 may not be added and result with failure to update device information.
639854	No IPv6 format in router GUI for BGP.
644596	FortiManager is unable to deauthorize explicit proxy user(s).
645086	Policy Lookup shows an error even though device is in sync.
649157	Mapping interface containing "/" results error "Object does not exist" during import policy.
649566	CLI Template is not able to install same name interface using *vpn ipsec phase1-interface* and *config system ipsec-aggregate*.
649769	FortiManager cannot view full list of Extenders.
649785	*SD-WAN* > *Monitor* may hang for an ADOM with 1500 devices.
651560	SD-WAN monitor may stuck loading when the admin user belongs to device group.
651712	SD-WAN monitor keeps loading and not displaying anything in backup mode ADOM.
652052	FortiManager may fail to add another FortiManager in Fabric ADOM.
652427	FortiManager may not be able to configure any value on the access list prefix.
652481	Allow access is missing under interface on AWS FortiGate and may cause installation to fail.
653388	IPsec VPN Phase-1 tunnel interface is not added in VDOM interface list with long VDOM name.
653465	FortiManager may not be able to edit DHCP options function on GUI.

FortiSwitch Manager

Bug ID	Description
650453	FortiSwitch template and VLAN shall appear for firewall policy creation.
651788	FortiSwitch Manager not showing correct online or offline status.

Global ADOM

Bug ID	Description
632400	When installing global policy, FortiManager may delete policy routes and settings on an ADOM.

Others

Bug ID	Description
632822	The *merged_daemons* process goes to 100% usage and prevents radius authentication.
647337	FortiManager fails to retrieve FSSO user groups via FortiGate
481129	FortiManager is lacking API for policy consistency check.
647156	FortiManager cannot clone any of the `deep-inspection` ssl-ssh-profiles using JSON API.

Policy & Objects

Bug ID	Description
523350	FortiManager does not show the default certificate under SSL/SSH Inspection within a policy.
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.
586026	FortiManager should display zone icon based on existing and non existing dynamic mappings.
611980	Policy is not installed on selected devices when one device is excluded due to Zone validation failed.

Bug ID	Description
612317	FortiManager shows incorrect country code for Cyprus under User definition.
618321	FortiManager is unable to create *RSSO Group* if *Agent* is configured with custom name.
620092	*Interface Pair View* is not working for Security Policies.
623100	FortiManager is constantly changing UUID for firewall address object.
630431	Some application and filter overrides are not displayed on GUI.
631158	FortiManager is unable to import firewall objects of `fsso fortiems-cloud` user due to Server cannot be empty.
634241	VIP created using CLI script is not available to use in policy.
635966	Azure SDN connector only fetches the first page of results.
640157	Verification may fail due to wrong default setting of 'log.memory.global-setting' > 'set max-size'.
525625	When configuring web filter rating override, the configuration is pushed to all the VDOMs even when web filter is not used.
531112	Consolidated policy is missing implicit deny policy.
568482	FortiManager ADOM web filter profile configuration promoted to Global database does not rename associated FortiGuard local categories.
580880	FortiManager is unable to see dynamic mapping for Local Certificate if workflow session is created.
583151	FortiManager should not change default value of scan-mode and ssl-ssh-profile/inspection-mode when installing v6.0 policy package to v6.2.
585177	FortiManager is unable to create VIPv6 virtual server objects.
597011	Importing groups from *Aruba ClearPass* may fail.
599129	While editing policy from Policy Package, it is not possible to select SSL/SSH Inspection profile.
613171	FortiManager is unable to export 3000 Policies to Excel Spreadsheet and return error *InternalError: "too much recursion"*.
617894	FortiManager is missing IPV6 none values after modifying policy.
623833	Username cannot exceed 35 characters.
631311	Promoting object groups to global may attempt to install contained objects back to ADOM upon global policy package assignment.
645058	Existing objects may disappear while editing policy and adding new one in batch mode.
647189	FortiManager dynamic object filter generator is adding a "*s*" at the end of tag resulting in non-working object.
648767	No connection request is sent out for ClearPass connector in ADOM.

Bug ID	Description
648815	Package with address group in SSL inspection cannot be installed to FortiGate.
650339	Source or destination address may not show in policy.
652753	FortiManager may show entry IDs instead of names when an obsolete internet service is selected.
655248	*Policy Consistency Check* may return duplicate address object names.
615624	Firewall policy and proxy policy cannot select IP type *external resource* as address.
651955	Thread feed is not deleted by install even it is removed from a policy.
654562	FortiManager may fail to install profile-group and apply it on a policy.
632771	Sometimes users are not updated on FortiManager after a new session is created on ISE.

Revision History

Bug ID	Description
597650	FortiManager cannot install allowed DNS and URL threat feed configuration.
604927	FortiManager can create custom device without category which may lead to failed installation.
618305	FortiManager changes configuration system `csf` settings.
586275	Policy Package Diff does not show user or admin details.
496870	Fabric SDN Connector is installed on FortiGate even if it is not in used.
587682	Installing mobile token that does not belong to target FortiGate may fail.
606005	FortiManager may not show interface delta changes.
606737	User may not be able to install policy package due to change with external interface with VIP settings.
611169	Install may fail with error "*Associated Interface conflict detected!*"
612263	FortiManager may not install ADSL vci and VPI to FWF-60E-DSL.
623159	Zone validation in re-Install Policy is not saving the user choice and deleting all related policies.
635786	Default *hbdev* values may change after upgrade.
635957	Install fails for subnet overlap IP between two interfaces.
637103	Scrolling in install preview is not smooth and may get stuck.
647180	Install copy may fail with error message "*ftgd-wf - - The category is already set in another filter*."

Bug ID	Description
650239	Installation fails with "*wireless-controller vap mesh-backhaul*" setting despite setting being disabled on FortiManager.
652337	VPN Manager changes may result in unnecessary FortiGate configuration changes.
654496	When installing configuration to a device after Auto link, FortiManager may send incorrect system ntp commands causing install to fail.
655246	The *adom-rev-auto-delete* option may not work to automatically delete revisions.
656505	Install may fail for *youtube-channel-filter* after creating a web filter profile.

Script

Bug ID	Description
630016	FortiGate user can see scripts from all ADOMs.
632014	When editing CLI script group, the user cannot see full CLI script name.
611396	After locked on a device, FortiManager cannot show the list of devices to run a script.
613575	After script is run directly on CLI, FortiManager may fail to reload configuration.

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.
567664	HA secondary device does not update FortiMeter license.
587730	FortiGate-VM64-AZURE may not be listed in firmware image page.
591821	FortiManager may not honor the `fgd-pull-interval` and adjust download times accordingly.
603414	FortiManager may show incorrect firmware upgrade path.
616320	FortiManager may ignore FortiGuard update schedule.
652764	*FortiManager Enforce Firmware Version* may fail to upgrade FortGate to a custom build.
654129	FortiManager may not have the correct upgrade path for FortiGate KVM.

System Settings

Bug ID	Description
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.
596212	SSH filter profile is unset in firewall profile group upon ADOM upgrade.
611215	SNMP Hosts in SNMP Community are not displayed in the GUI if ADOM is unlocked.
631733	Changing *trusted IP* can be saved and installed.
479723	FortiManager may have no control to Fabric View in admin profile.
489837	Certificate request CRS does not include the SAN DNS.
598194	FortiManager two-factor authentication admin login is missing the option for FTK Mobile push notification authentication.
614127	FortiManager should show details in the fnbamd debug if login fails due to trusted hosts.
623457	FortiManager prompts error while importing CA certificate.
625683	Changes made by ADOM upgrade may not update "Last Modified" date/time and user admin.
639099	There are many "cdb event log for object changed" in event logs after upgrade.
650326	After HA failover, the new master may have incorrect policies.
652417	FortiManager HA may go out of synchronization periodically based on the logs.
654637	Changing a non super user password may not take effect after an upgrade.
655515	FortiManager may not be able to clone the Security Fabric ADOM.

VPN Manager

Bug ID	Description
596953	The *Monitor* page displays a white screen when the user goes to *VPN manager* > Monitor, and selects a specific community from the tree menu to show only that community's tunnels.
576601	FortiManager should be able to manage phase2 selectors separately.
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.
645093	VPN Manager error Peer type cannot be peer when authentication method is pre-share key.
647413	User should be able to select the OS to allow or deny an SSL-VPN tunnel connection.

Bug ID	Description
650454	Installation may fail when Dialup VPN interface is PPPoE logical interface.
653328	FortiManager is unable to edit a SSL portal in VPN Manager containing "/" special character.

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
```