FortiManager - Release Notes

Version 6.2.6

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
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 6.2.6 Release Notes
02-626-657816-20210507

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-27	Initial release of 6.2.6.
2020-08-28	Added FGT-1800F to firmware version 6.2 in FortiGate models on page 20.
2020-09-01	Updated Known Issues on page 43,FortiGate models on page 20, and FortiGate special branch models on page 23.
2020-11-09	Updated Known Issues on page 43.
2020-12-21	Updated FortiSwitch models on page 28.
2021-05-07	Updated Downgrading to previous firmware versions on page 11.

FortiManager 6.2.6 Release

This document provides information about FortiManager version 6.2.6 build 1349.

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 6.2.6 supports the following models:

FortiManager	FMG-200D, 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-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.2.6.

Multi-step firmware upgrades

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

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

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

Newly deployed, factory reset, or disk format may trigger upgrade code on subsequent reboot

For a newly deployed VM instance or appliance, a disk format or a factory reset on a FortiManager unit running version 6.2.3 may trigger the upgrade code upon rebooting the system, which in turn may update the database configuration, although no upgrades are required. This issue does not affect FortiManager units upgraded from versions prior to 6.2.3.

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

Multicast policies with zones or zone members

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

Wildcard Address Support in Policy

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

Import Authentication Rules and Schemes

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

Support of the NGFW mode in 6.2.1

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

Managing FortiGate with VDOMs that use Global, Shared Profiles

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

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

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

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

FGVMULCV30310000 (utm-profile) # ed g-wifi-default
FGVMULCV30310000 (g-wifi-default) # sh
config wireless-controller utm-profile
    edit "g-wifi-default"
        set comment "Default configuration for offloading WiFi traffic."
    next
end
```

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

Managing FortiAnalyzer Devices

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

IOC Support on FortiManager

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

Hyper-V FortiManager-VM running on an AMD CPU

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

SSLv3 on FortiManager-VM64-AWS

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

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

Upgrade Information

You can upgrade FortiManager 6.0.3 or later directly to 6.2.6.

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

This section contains the following topics:

Unintended downgrade of FortiGate units

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

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. In addition the local password is erased.

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

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

Firmware image checksums

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

FortiManager VM firmware

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

Aliyun

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Linux KVM

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

Microsoft Azure

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

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

Microsoft Hyper-V Server

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

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

Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

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

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

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 6.2.6 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

FortiManager 6.2.6 support

This section identifies FortiManager 6.2.6 product integration and support information:

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

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

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

Web browsers

This section lists FortiManager 6.2.6 product integration and support for web browsers:

- Microsoft Edge80 (80.0.361 or later)
- Mozilla Firefox version 74
- Google Chrome version 85

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

FortiOS/FortiOS Carrier

This section lists FortiManager 6.2.6 product integration and support for FortiOS/FortiOS Carrier:

FortiOS or FortiOS Carrier		Compatibility Issues
6.2	6.2.0 and later	
6.0	6.0.10	
	6.0.9	FortiManager6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.9. For information about minor interoperability issues with different versions, see FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues on page 31.
	6.0.4 to 6.0.8	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.8. For information about minor interoperability issues with different versions, see FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues on page 31.
	6.0.0 to 6.0.3	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.3. For information about minor interoperability issues with different versions, see FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 32.
5.6	5.6.7 to 5.6.12	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.8. For information about minor interoperability issues with different versions, see FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues on page 32
	5.6.5 to 5.6.6	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.6. For information about minor interoperability issues with different versions, see FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 32.
	5.6.4	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4. For information about minor interoperability issues with different versions, see FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 32.
	5.6.2 to 5.6.3	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.3. For information about minor interoperability issues with different versions, see FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 33.
	5.6.0 to 5.6.1	FortiManager6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1. For information about minor interoperability issues with different versions, see FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 33.
5.4	5.4.11 to 5.4.12	

FortiOS or FortiOS Carrier	Compatibility Issues
5.4.10	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10. For information about minor interoperability issues with different versions, see FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 33.
5.4.9	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9. For information about minor interoperability issues with different versions, see FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 34.
5.4.1 to 5.4.8	FortiManager 6.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8. For information about minor interoperability issues with different versions, see FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 34.

FortiAnalyzer

This section lists FortiManager 6.2.6 product integration and support for FortiAnalyzer:

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

FortiAuthenticator

This section lists FortiManager 6.2.6 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 6.2.6 product integration and support for FortiCache:

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

FortiClient

This section lists FortiManager 6.2.6 product integration and support for FortiClient:

- 6.2.1
- 6.0.8
- 6.0.0
- 5.6.6
- 5.6.3
- 5.6.0
- 5.4.0 and later

FortiMail

This section lists FortiManager 6.2.6 product integration and support for FortiMail:

- 6.0.5
- 5.4.9
- 5.4.5
- 5.3.12

FortiSandbox

This section lists FortiManager 6.2.6 product integration and support for FortiSandbox:

- 3.1.0
- 3.0.5
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiManager 6.2.6 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.2.6 product integration and support for FortiWeb:

- 6.1.1
- 6.0.5
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1

- 5.5.6
- 5.4.1

FortiDDoS

This section lists FortiManager 6.2.6 product integration and support for FortiDDoS:

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

Limited support. For more information, see Feature support on page 18.

Virtualization

This section lists FortiManager 6.2.6 product integration and support for virtualization:

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

Feature support

The following table lists FortiManager feature support for managed platforms.

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

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

Language support

The following table lists FortiManager language support information.

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.2.6.

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

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FG-401E-DC, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FGT-1800F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E-DC,FortiGate-3401E, FortiGate-3401E-DC, FortiGate- 3600E, FortiGate- 3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **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	6.2

Model	Firmware Version
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-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-80CM, FortiWiFi-81CM **FortiGate-VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-90D **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-401E-DC, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C,FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate DC:** FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-40F, FWF-40F-3G4G, FWF-41F, FWF-41F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FW-60E-DSL, FW-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D **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

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

Model	Firmware Version
FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-60D, FGR-90D	

FortiGate special branch models

Model	Firmware Version
FortiGate: FortiGate-60E-DSL, FortiGate-60E-DSLJ **FortiGate Rugged:** FortiGateRugged-90D	6.2
FortiGate: FortiGate-30E-3G4G-GBL, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1101E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC **FortiGate DC:** FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC **FortiGate VM:** FortiGate-VM64-RAXONDEMAND **FortiWiFi:**FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60F, FortiWiFi-61F	6.0
FortiGate: FortiGate-60E-DSL, FortiGate-60E-DSLJ **FortiGate 5000 Series:** FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F **FortiGate 7000 Series:** FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC **FortiWiFi:** FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ	5.6
FortiGate: FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-500E, FortiGate-501E, FortiGate-2000E, FortiGate-2500E, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series:** FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F	5.4

Model	Firmware Version
FortiGate 7000 Series: FortiGate-7030EFG-7030E-Q, FortiGate-7000E, FortiGate-7030E-S, FortiGate-7040E-1, FortiGate-7040E-2, FortiGate-7040E-3, FortiGate-7040E-4, FortiGate-7040E-5, FortiGate-7040E-6, FortiGate-7040E-8, FortiGate-7040E-8-DC, FortiGate-7060E-1, FortiGate-7060E-2, FortiGate-7060E-3, FortiGate-7060E-4, FortiGate-7060E-5, FortiGate-7060E-6, FortiGate-7060E-8 **FortiWiFi:** FortiWiFi-50E-2R, FortiWiFi-60E, FortiWiFi-61E, FortiWiFi-92D, FortiWiFi-60E-DSL **FortiGate VM:** FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-OPC **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D	

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E **FortiGate 6000 series:** FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiGate 7000 series:** FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC **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
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E **FortiCarrier 6000 Series:** FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC **FortiCarrier-DC:** FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FCR-3810D-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, 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: 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-448E, FortiSwitch-448E-POE, FortiSwitch-448E-FPOE, FortiSwitch-524D, FortiSwitch-524D-FPOE, FortiSwitch-548D, FortiSwitch-548D-FPOE, FortiSwitch-1024D, FortiSwitch-1048D, FortiSwitch-1048E, FortiSwitch-3032D, FortiSwitch-3632D	N/A There is no fixed supported firmware versions. If FortiGate supports it, FortiManager will support it.

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-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	5.7.2

Model	Firmware Version
FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, 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-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

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.2.6. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.0	• FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues on page 31 • FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues on page 31 • FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 32
FortiOS 5.6	• FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues on page 32 • FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 32 • FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 32 • FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 33 • FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 33
FortiOS 5.4	• FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 33 • FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 34 • FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 34

FortiManager 6.2.3 and FortiOS 6.0.9 compatibility issues

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

FortiManager 6.2.3 does not support the following FortiOS syntax:

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

FortiManager 6.2.3 and FortiOS 6.0.8 compatibility issues

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

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

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

FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues

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

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

FortiManager 6.2.3 and FortiOS 5.6.12 compatibility issues

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

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

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

FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues

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

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

FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues

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

Bug ID	Description
486921	FortiManager may not be able to support the syntax for the following objects: • `rsso-endpoint-block-attribute`, `rsso-endpoint-block-attribute`, or `sso-attribute` for RADIUS users. • `sdn` and its `filter` attributes for firewall address objects. • `azure` SDN connector type. • `ca-cert` attribute for LDAP users.

FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues

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

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

FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues

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

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

FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues

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

Bug ID	Description
508337	FortiManager cannot edit the following configurations for replacement message: • `system replacemsg mail "email-decompress-limit"` • `system replacemsg mail "smtp-decompress-limit"` • `system replacemsg nntp "email-decompress-limit"`

FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues

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

Bug ID	Description

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

FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues

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

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

Resolved Issues

The following issues have been fixed in 6.2.6. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
556036	FortiManager cannot configure AP profile *short-guard-interval*.
599666	Empty *LLDP* status information is shown under *AP Manager*.
610724	Unauthorized APs should be displayed so that users can authorize the APs.
644584	Upgrading an AP may get stuck at 5 % and no task is created for it.
645030	Adding FortiGate using custom admin profile may fail to list FAP in AP Manager.
645713	FortiManager allows the user to create SSID which cannot be deleted later.
653329	FortiManager is sending the wrong device setting after changing the FAP name.
587879	AP Manager central mode is missing AP group with VLAN ID.
607170	Dynamic VLAN option is not saved in SSID in AP Manager.
654171	There may be duplicate entries in *objcfg_wireless_controller_wtp* preventing the user to delete some custom WTP profiles.

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.
598794	IPSec Phase 1 setting shows inconsistencies between *Lock* and *Unlock*.
599852	When password policy is set as *enforced*, FortiManager should not accept the 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.
605688	`Pac-file-data`is limited to 4000 characters under CLI Configuration.

Bug ID	Description
610071	FortiManager should not allow duplicated names when creating a new interface based VPN *phase1.*
611315	SD-WAN should be allowed to configure port for HTTP health-check server.
612355	Policy Package status remains in *modified* status after using *Push to device* on an updated object.
616271	FortiManager prompts a, *response format error*, when adding per-device mapping to a new interface in a new workflow session
619106	When importing a policy, the conflict page may truncate outputs.
624596	Device Manager's *Connect to CL*I function with SSH may prompt an error message.
625831	Deleting a device from Device Manager may take a long time and FortiManager becomes very slow.
626598	Custom Device *Meta* fields cannot be modified.
631576	Device list may be empty under device group when trying to edit it.
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*.
637794	FortiManager is unable to import firewall policy if the SD-WAN member interface referenced is `dstaddr`.
638351	FortiManager is unable to set *FAZ IP* override setting as global setting.
643172	FortiManager does not support *dnsproxy-worker-coun*t higher than two.
644223	FortiManager is unable to add FortiAnalyzer and triggers an error: *Object does not exist*.
649195	Editing an address group does not trigger any configuration change when the installation target is set to specific device(s).
649711	FortiManager is unable to add FortiAnalyzer and fails to synchronize FortiAnalyzer with current ADOM data with error: *Fail(errno=-3):Object does not exist.*
650545	Import may get stuck in an infinite loop when there is a recursive reference.
558176	Interface-subnet type addresses' interface are re-set to zone after import, causing the copy to fail during install.
649566	CLI Template is not able to install an interface with the same name using *vpn ipsec phase1-interface* and *config system ipsec-aggregate*.
653388	IPsec VPN Phase-1 tunnel interface is not added to the VDOM interface list in a VDOM that has a long name.
653465	FortiManager may not be able to edit DHCP options function on the GUI.
656984	Importing system template CLI may fail.

Bug ID	Description
552492	VAP is always loading under CLI configuration.
633767	There is a typo in Japanese in NTP Service of DHCP Server setting.
651712	SD-WAN monitor keeps loading and not displaying anything in backup mode ADOM.

FortiSwitch Manager

Bug ID	Description
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*n configured on FortiManager.
651788	FortiSwitch Manager is not showing the correct online or offline status.

Global ADOM

Bug ID	Description
645702	Global policy install should not show warnings when a policy package has no installation target.
647736	Global ADOM policy package assignment may fail.

Others

Bug ID	Description
551710	*/bin/ha* may have high memory usage.
623147	FortiManager may never form a HA due to variance in certificates.
626338	The `exec fmpolicy` CLI command may not print out a policy package correctly.
635616	The ADOM integrity check may fail with SD-WAN dynamic interface members.
643784	FortiManager is crashing on security console and wizard is stopped at 50% of deployment.
647791	Cloning VDOM object may fail via the CLI.
647156	FortiManager cannot clone any of the *deep-inspection* ssl-ssh-profiles using JSON API.
657566	After upgrade, copy may fail for central SD-WAN with configuration error *error service - 2 :-2 - Please assign a member*.

Policy and Objects

Bug ID	Description
525625	When configuring web filter rating override, the configuration is pushed to all the VDOMs even a web filter is not used.
540716	Under *Policy*,there is no *Session Count*, *Session First Used*, *Session Last Used* options in the *Column Settings* drop-down list.
553462	FortiManager may prompt the error, *Zone member VLAN is used by another zone*, when installing policy package.
569226	The section title should always be displayed for filtered policy and the section title should not be deleted after policy was deleted.
578501	FortiManager should show global icon for global objects assigned to ADOMs.
581588	Central SNAT policy does not support showing IPv6 address in the table.
593417	FortiManager shows incorrect action for allowing invalid SSL certificates.
596533	Renaming policy package changes the implicit policy's *Log Violation Traffic* setting to *No Log*.
609300	FortiManager may not be able to import all *Cisco ACI Fabric Connector* address.
612445	Policy package for v5.6 cannot be installed on v6.0 devices if default deep SSL inspection is used.
613840	Process bar does not show correct status when some addresses fail to import for fabric connector.
614710	Search result in device interface should display the zone that the interface is a member of.
615117	*Policy Package* section is not sent over to FortiGate if *Policy Blocks* are under the section in FortiManager.
620890	Unlock and discard changes on policy package may create duplicate section titles.
625665	Policy package installation may fail due to certificates errors after creating a new VDOM.
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* when there is nothing to be installed.
628748	When scrolling through *URL Filter* list under *Web Filter Profile*, the list either takes time to load or it does not show all URLs.
630055	Some custom application signatures have *id 0* in the application list.
630582	Deleted policy IDs may still appear in the GUI.
630891	Cloned policy may not get installed onto devices.
631405	FortiManager should check for *mgmt* interface configuration for *dedicated to mgmt* setting before allow using the interface on a policy.
632545	Installing policy package may result in an error: *Could not read zone validation results*.

Bug ID	Description
632715	In DoS policy, changing quarantine from *attacker* to *none* keeps *quarantine-expiry* set incorrectly.
632771	Sometimes users are not updated on FortiManager after a new session is created on ISE.
633248	Web proxy profile is not being installed on FortiGate when the proxy type is *Transparent-web*.
633431	Changing to *Classical Dual Pane* disables *Policy Hit Count*.
633727	FortiManager is unable to display summary of policy package diff for VDOM with a long name.
634597	FortiManager may unset speed on ports which are configured with 10000full.
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.
636732	Copying policy causes interface binding contradiction for object member.
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.
640662	Policy page shows a blank entry for the *Users* column when device group is selected.
643098	FortiManager may have slow installation of policy package due to many VIPs have the same external VIP.
643113	Changing an *Accept* policy to *Deny* when the policy contains a Security Profile Group results in installation failure.
643930	Finding *Duplicate Object*s shows does not display duplicated addresses if wildcard is empty.
643957	When there are many firewall addresses, FortiManager 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 on the GUI.
645661	A valid custom IPS signature may still trigger invalid IPS data error.
647337	FortiManager may fail to retrieve FSSO user groups via FortiGate.
599129	While editing policy from *Policy Package*, it is not possible to select *SSL/SSH Inspection* profile.
618321	FortiManager is unable to create *RSSO Group* if *Agent* is configured with a custom name.
620092	*Interface Pair* view is not working for *Security Policies*.
634241	VIP created using CLI script is not available to use in a policy.

Bug ID	Description
644689	FortiManager may not be able to load application control profile.
583151	FortiManager should not change the default value of *scan-mode* and *ssl-ssh-profile/inspection-mode* when installing v6.0 policy package to v6.2.
600165	Firewall consolidated policy is still named as *SSL Inspection & Authentication* when it is profile based.
623833	Username cannot exceed 35 characters.
640157	Verification may fail due to wrong default setting of *log.memory.global-setting* > *set max-size*'.

Revision History

Bug ID	Description
586275	Policy Package Diff does not show user or admin details.
594933	Re-installing Policy Package cannot skip to *Install Policy Package*, which fails validation.
604680	FortiManager sets FSSO to disable even though FSSO group is in use.
610032	After upgrade, installation fails due to the *set mediatype* command of an interface.
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.
632129	*syslogd* setting *source-ip* is still visible after setting status to *disable*, which causes a verification failure.
633515	FortiManager should improve error message when FortiManager receives blank or invalid configurations from FortiGate.
643803	Policy Package Diff may shows all objects as new changes.
646372	When a customer applies changes to a policy package, then all the policy packages in this ADOM change to a *Modified* state.
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.
647180	Install copy may fail with error message *ftgd-wf - - The category is already set in another filter*.
634032	Installing a policy may fail due to log disk setting.
657344	Installing from 6.0 ADOM may try to *unset inspection-mode* and *unset ssl-ssh-profile* on FortiGate 6.2.

Script

Bug ID	Description
611396	When a device is locked, FortiManager cannot show the list of devices to run a script.
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.
592660	Running a script remotely may trigger a full configuration retrieve instead of a partial configuration retrieve.

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.
652764	FortiManager to Enforce Firmware Version may fail to upgrade FortGate to a custom build.

System Settings

Bug ID	Description
493533	FortiManager needs to rename custom *default* protocol option after upgrade.
556334	Standard ADOM users should be able to assign system templates to FortiGate devices.
557949	Changing a password should be enabled by default for all admin users.
579563	*Workflow Session List* menu seems to always match the first wildcard *TACACS* admin.
596212	SSH filter profile is unset in firewall profile group upon ADOM upgrade.
618213	When trying to upgrade FortiManager cluster from FortiManager Master GUI, FortiManager Master reboots before finishing to send firmware to FortiManager secondary device.
618607	Upgrading 5.4 ADOM does not convert *delay-tcp-npu-sessoin* to *delay-tcp-npu-session* and delete the option.
628006	Even though a user has *Manage Device Configurations* read/write 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 the error *Workspace request failed, please try again*.

Bug ID	Description
640505	Remote admin authentication with RADIUS may stop working.
641018	Upgrading Global ADOM may fail due to *Fortinet_NSX* local certificate.
644660	Installation preview may get stuck and system may run out of memory.
647575	Cloning an ADOM may fail with *error 0: invalid value*.
655515	FortiManager may not be able to clone the Security Fabric ADOM.
650326	After an HA failover, the new master may have incorrect policies.
654370	Users may not be able to access Java console with an error message: *Too many concurrent connections*.

VPN Manager

Bug ID	Description
594889	Dial-up IPSec VPN tunnel should show tunnel up on VPN manager monitor as it appears on FortiGate.
621209	VPN monitor should show the corresponding VPN community tunnels only under each community.
622046	Local ID should be visible from the GUI and should be able to modify it when using dial-up group.
650454	Installation may fail when *Dialup VPN* interface is *PPPoE logical interface*.

Known Issues

The following issues have been identified in 6.2.6. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
599189	FortiManager should be able to handle upgrading more than 10 APs at once.
633171	There may be DFS Channel mismatch between FortiManager and FortiGate for FAP-223E.

Device Manager

Bug ID	Description
547768	FortiManager should allow easier management of the compliance exempt lists.
598424	Interface cannot create more than 48 IP-MAC bindings in DHCP reservation from the GUI.
598916	When creating user groups via *CLI Only Objects*, comma separated values are treated as a string instead of a list.
601692	FortiManager is unable to overwrite IPv6 default route.
604125	FortiManager may not be able to edit the VDOM link interface from VDOM level.
607923	*Security Fabric Connection* option is removed from VLAN interface.
610568	FortiManager may not follow the order in CLI Script template.
613029	SD-WAN Monitor is showing effect of exceeded SLA even when it is disabled.
616537	FortiGate and FortiManager GUI should use similar terminology for configuring weight and volume-ratio in SD-WAN.
627664	FortiManager cannot understand *socket-size 0* and changes it to *1* automatically.
627749	Admin user with *device-config* set as *read* in admin profile cannot download configuration revision.
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.

Bug ID	Description
636638	Fabric View keeps loading indefinitely.
638061	FortiGate 7000 may not be added and fails to update device information.
645086	*Policy Lookup* shows an error even though the device is in sync.
649769	FortiManager cannot view full list of Extenders.
649785	*SD-WAN > Monitor* may hang for an ADOM with 1500 devices.
652427	FortiManager may not be able to configure the *any* value on the access list prefix.
652481	*Allow access* is missing under interface on AWS FortiGate and may cause the installation to fail.
575215	When creating an new interface for a VDOM, FortiManager may list interfaces that may belong to another AODM.
598431	Install wizard may show a blank area when scrolling down the wizard to select device(s).
618354	Importing a policy with a profile group will display *ssl-ssh profile* and *proxy options* in the GUI.
646421	FortiManager may not be able to configure the VDOM property resources setting.
649821	Installation may fail for FortiGate-600D.
657933	Importing policy should be successful even with the zone name contains the / character.
468776	FortiManager fails to retrieve device configuration and displays *data not exist* error (*g-xxxx firewall object*).

FortiSwitch Manager

Bug ID	Description
650453	FortiSwitch template and VLAN is missing when creating a new firewall policy.
637220	FortiManager may not able to upgrade FortiSwitch firmware.

Global ADOM

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

Others

Bug ID	Description
662438	FortiManager tries to purge all web rating override entries.

Policy & Objects

Bug ID	Description
531112	Consolidated policy is missing implicit deny policy.
580880	FortiManager is unable to see dynamic mapping for Local Certificate when workflow session is created.
585177	FortiManager is unable to create VIPv6 virtual server objects.
586026	FortiManager should display *Zone* icon based on existing and non existing dynamic mappings.
597011	Importing groups from *Aruba ClearPass* may fail.
598938	FortiManager should allow setting *wildcard-fqdn* type firewall address as a destination on proxy policy.
601385	A *Restricted* mode admin cannot install *Web Rating Overrides* changes.
602176	Creating a proxy policy with a profile group adds additional security profile.
612317	FortiManager shows the wrong country code for Cyprus under *User definition*.
615624	Firewall policy and proxy policy cannot select *IP type external resource* as address.
617031	Right-clicking on *IPv4/Proxy Policy* or *Installation Targets* should not reload the page if the related information is already displayed.
617894	FortiManager is missing IPV6 *none* values after modifying a policy.
618499	Right-clicking to edit zone incorrectly prompts dynamic interface window.
622040	*Security Policy* is missing *Implicit Deny* policy.
630431	Some application and filter overrides are not displayed on the GUI.
631158	FortiManager is unable to import firewall objects of *fsso fortiems-cloud* user because *Server* cannot be empty.
635966	Azure SDN connector only fetches the first page of results.
647189	FortiManager dynamic object filter generator is adding an "s" at the end of tag resulting in non working object.
648767	No connection request is sent out for *ClearPass* connector in an ADOM.

Bug ID	Description
652753	When an obsolete internet service is selected, FortiManager may show entry IDs instead of names.
654562	FortiManager may fail to install a profile-group and apply it on a policy.
608535	*NAT* option is missing from *Central NAT* policy package.
651785	*Address* section under *Policy & Objects* > *Security Profiles* > *SSL/SSH Inspection* may load indefinitely.
658528	The URL remote category, *FortiGuard Threat Feed*, is not available in the dro down menu for *Proxy Address*.

Revision History

Bug ID	Description
597650	FortiManager cannot install allowed DNS and URL threat feed configuration.
606737	User may not be able to install a policy package due to a 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.
618305	FortiManager changes configuration system csf settings.
623159	When re-installing a policy, *Zone* validation 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.
654496	Installing configuration to device after Auto link, FortiManager may send incorrect system *ntp* commands causing the install to fail.
655246	The *adom-rev-auto-delete* option may not work to automatically delete revisions.

Script

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

Bug ID	Description
630016	FortiGate user can see scripts from all ADOMs.
632014	When editing a CLI script group, the user cannot see the full CLI script name.

Services

Bug ID	Description
541192	FortiManager should keep firmware image files when the files are for different FortiExtender devices.
567664	HA secondary device does not update the FortiMeter license.
587730	FortiGate-VM64-AZURE may not be listed in firmware image page.
654129	FortiManager may not have the correct upgrade path for FortiGate KVM.
592089	Firmware upgrade of FortiGate devices via *Firmware Manager* may be slow if there are offline devices.

System Settings

Bug ID	Description
611215	*SNMP Hosts* in *SNMP Community* are not displayed in the GUI if ADOM is unlocked.
625683	Changes made by ADOM upgrade may not update *Last Modified* date/time and user admin.
631733	Changing the *trusted IP* cannot be saved and installed.
639099	There are many *cdb event log for object changed* in event logs after upgrade.
654637	Changing a non-Super_User password may not take effect after upgrade.
619750	When upgrading an ADOM from 5.4 to 5.6, FortiManager does not add *tcp-session-without-syn* in all firewall policies.

VPN Manager

Bug ID	Description
596953	The *Monitor* page displays a white screen in *VPN manager* > *Monitor*, and the user selects a specific community from the tree menu to show only that community's tunnels.

Bug ID	Description
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 a pre-share key.
658221	The dns-suffix on SSL VPN portal is not installed if web-mode is disabled.

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
```