FortiManager - Release Notes

Version 6.0.12

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

April 8, 2024
FortiManager 6.0.12 Release Notes
02-6012-918383-20240408

TABLE OF CONTENTS

Change Log **5**
FortiManager 6.0.12 Release **6**
Supported models 6
Special Notices **7**
FortiGuard web filtering category v10 update 7
Multicast policies with zones or zone members 7
Managing FortiGate with VDOMs that use Global, Shared Profiles 7
IOC Support on FortiManager 8
FortiManager 6.0.2 support for FortiOS 6.0.3 8
Reconfigure SD-WAN after Upgrade 8
FortiGate VM 16/32/UL license support 9
Hyper-V FortiManager-VM running on an AMD CPU 9
VM License (VM-10K-UG) Support 9
Recreate Guest List for Guest user group 9
FortiOS 5.4.0 Support 9
SSLv3 on FortiManager-VM64-AWS 9
Upgrade Information **11**
Downgrading to previous firmware versions 11
Firmware image checksums 11
FortiManager VM firmware 11
SNMP MIB files 13
Product Integration and Support **14**
FortiManager 6.0.12 support 14
Web browsers 14
FortiOS/FortiOS Carrier 15
FortiAnalyzer 15
FortiAuthenticator 15
FortiCache 15
FortiClient 15
FortiMail 16
FortiSandbox 16
FortiSwitch ATCA 16
FortiWeb 16
FortiDDoS 16
Virtualization 17
Feature support 17
Language support 17
Supported models 18
FortiGate models 19
FortiCarrier models 22
FortiDDoS models 22
FortiAnalyzer models 23
FortiMail models 23

FortiSandbox models 24
FortiSwitch ATCA models 24
FortiSwitch models 25
FortiWeb models 25
FortiCache models 26
FortiProxy models 26
FortiAuthenticator models 27
Compatibility with FortiOS Versions 28
FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues 28
FortiManager 6.0.7 and FortiOS 5.6.12 compatibility issues 28
FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues 29
FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues 29
FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues 29
FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues 29
FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues 30
FortiManager 5.4.1 and FortiOS 5.2.10 compatibility issues 30
FortiManager 5.2.6 and FortiOS 5.2.7 compatibility issues 30
FortiManager 5.2.4 and FortiOS 5.2.6 compatibility issues 31
FortiManager 5.2.1 and FortiOS 5.2.1 compatibility issues 31
FortiManager 5.2.1 and FortiOS 5.2.0 compatibility issues 31
Resolved Issues 32
Known Issues 33
Appendix A - FortiGuard Distribution Servers (FDS) 34
FortiGuard Center update support 34

Change Log

Date	Change Description
2023-06-08	Initial release of 6.0.12.
2024-01-29	Updated Special Notices on page 7.
2024-04-08	Updated Special Notices on page 7.

FortiManager 6.0.12 Release

This document provides information about FortiManager version 6.0.12 build 0485.

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 on page 6

Supported models

FortiManager version 6.0.12 supports the following models:

FortiManager	FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000D, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3900E, FMG-3700F, FMG-4000D, FMG-4000E, and FMG-MFGD.
FortiManager VM	FMG-VM64, FMG-VM64-ALI, FMG-VM64-AWS, FMG-VM64-AWS-OnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016), 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 6.0.12.

FortiGuard web filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency web sites. In order to use the new categories, customers must upgrade their Fortinet products to one of the versions below.

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS.

https://support.fortinet.com/Information/Bulletin.aspx

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.

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.

IOC Support on FortiManager

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

FortiManager 6.0.2 support for FortiOS 6.0.3

FortiManager 6.0.2 treats the `status` field of firewall policies as a mandatory field, and it is set to `enable` by default. FortiOS 6.0.3 has reverted this change. As a result, FortiManager may report verification failures on installations. The verification report shows that the policy `status` field has to be installed with the `enable` setting:

```
"---> generating verification report
   (vdom root: firewall policy 1:status)
   remote original:
   to be installed: enable

<--- done generating verification report


install failed"
```

Reconfigure SD-WAN after Upgrade

The SD-WAN module has been fully redesigned in FortiManager v6.0 to provide granular monitor and control. Upgrading SD-WAN settings from 5.6 to 6.0 is not supported. Please reconfigure SD-WAN after upgraded to v6.0.

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.6.0 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

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.

VM License (VM-10K-UG) Support

FortiManager 5.4.2 introduces a new VM license (VM-10K-UG) that supports 10,000 devices. It is recommended to upgrade to FortiManager 5.4.2 or later before applying the new license to avoid benign GUI issues.

Recreate Guest List for Guest user group

After upgrading to FortiManager 6.0.3, recreate the guest list for the *Guest* user group in ADOM Policy Object before installing device settings to FortiGate devices. For more information, see Bug ID 499568 in *Resolved Issues*.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.2 and later no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2 or later.

The following ADOM versions are not affected: 5.0 and 5.2.

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 5.6.0 or later directly to 6.0.12.

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

This section contains the following topics:

- Downgrading to previous firmware versions on page 11
- Firmware image checksums on page 11
- FortiManager VM firmware on page 11
- SNMP MIB files on page 13

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

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

Firmware image checksums

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

FortiManager VM firmware

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

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.

Google GCP

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

Linux KVM

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

Microsoft Azure

The files for Microsoft Azure have AZURE in the file names, 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 file names, 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 6.0.12 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 6.0.12 support on page 14
- Feature support on page 17
- Language support on page 17
- Supported models on page 18

FortiManager 6.0.12 support

This section identifies FortiManager 6.0.12 product integration and support information:

- Web browsers on page 14
- FortiOS/FortiOS Carrier on page 15
- FortiAnalyzer on page 15
- FortiAuthenticator on page 15
- FortiCache on page 15
- FortiClient on page 15
- FortiMail on page 16
- FortiSandbox on page 16
- FortiSwitch ATCA on page 16
- FortiWeb on page 16
- FortiDDoS on page 16
- Virtualization on page 17

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 6.0.12 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
  Due to limitation on Edge, the browser may not completely render a page with a large set of policies or objects.
- Mozilla Firefox version 84
- Google Chrome version 83

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

FortiOS/FortiOS Carrier

This section lists FortiManager version 6.0.12 product integration and support for FortiOS/FortiOS Carrier:

- 6.0.0 to 6.0.17
- 5.6.0 to 5.6.14
- 5.4.0 to 5.4.13
- 5.2.0 to 5.2.15

FortiAnalyzer

This section lists FortiManager 6.0.12 product integration and support for FortiAnalyzer:

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

FortiAuthenticator

This section lists FortiManager 6.0.12 product integration and support for FortiAuthenticator:

- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiManager 6.0.12 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.0 to 4.0.4

FortiClient

This section lists FortiManager 6.0.12 product integration and support for FortiClient:

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

FortiMail

This section lists FortiManager 6.0.12 product integration and support for FortiMail:

- 6.0.10
- 5.4.11
- 5.3.13

FortiSandbox

This section lists FortiManager 6.0.12 product integration and support for FortiSandbox:

- 2.5.0 to 2.5.2
- 2.4.0 and 2.4.1
- 2.3.2 and 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiManager 6.0.12 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.0.12 product integration and support for FortiWeb:

- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

FortiDDoS

This section lists FortiManager 6.0.12 product integration and support for FortiDDoS:

- 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 17.

Virtualization

This section lists FortiManager 6.0.12 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		✓	✓	✓
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 6.0.12.

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 on page 19
- FortiCarrier models on page 22
- FortiDDoS models on page 22
- FortiAnalyzer models on page 23
- FortiMail models on page 23
- FortiSandbox models on page 24
- FortiSwitch ATCA models on page 24
- FortiSwitch models on page 25
- FortiWeb models on page 25
- FortiCache models on page 26
- FortiProxy models on page 26
- FortiAuthenticator models on page 27

FortiGate models

Model	Firmware Version
FortiGate: FGT-30E-3G4G-GBL, FGT-60F, FGT-61F, FGT-3400E, FGT-3401E, FGT-3600E, FGT-3601E, FGT-400E, FGT-401E, FGT-600E, FGT-601E, FGT-60E-DSL, FGT-60E-DSLJ, FWF-60E-DSL, FWF-60E-DSLJ, FGT-VM64-RAXONDEMAND, FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-40F, FG-40F-3G4G,FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, 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-100F, FG-101F, FG-101E, FG-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-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG3700D, FG-3800D, FG-3810D, FG-3300E, FG-3301E, FG-3815D, FG-3960E, FG-3980E, FG-6000F **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F, FG-6300F-DC, FG-6301F-DC, FG-6500F-DC, FG-6501F-DC **FortiGate 7000 Series:** FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7040E-9-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6,FG-7060E-8, FG-7060E-9, FortiGate-7060E-8-DC **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-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60F, FWF-61E, FWF-61F, 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-60E-DSL, 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-6300F, FG-6301F, FG-6500F, FG-6501F, FG-6300F-DC, FG-6301F-DC, FG-6500F-DC, FG-6501F-DC **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 **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-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-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-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-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-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F, FG-6300F-DC, FG-6301F-DC, FG-6500F-DC, FG-6501F-DC	5.4

Model	Firmware Version
FortiGate 7000 Series: FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8, 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 **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-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, 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-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

FortiCarrier models

Model	Firmware Version
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
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-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E **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
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E **FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E **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
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, , FGT-3810A, FGT-3810D, FGT-3950B, FGT-3951B, FGT-5100B, FGT-5100C, FGT-5001D, FGT-5101C, FS-5203B, FT-5902D **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3810A-DC, FGT-3810D-DC, FGT-3950B-DC, FGT-3951B-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-Xen	5.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.7, 4.6, 4.5, 4.4, 4.3, 4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F, FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FAZ-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-800F, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-800F, 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-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FE-VM64	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	5.4.5
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	5.3.12

Model	Firmware Version
FortiMail Low Encryption: FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	
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	5.2.10
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	5.1.7
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	5.0.10

FortiSandbox models

Model	Firmware Version
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-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B	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: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.9
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

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

FortiProxy models

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

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 and 5.0-5.3
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 6.0.12. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.0	FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues on page 28
FortiOS 5.6	FortiManager 6.0.7 and FortiOS 5.6.12 compatibility issues on page 28
	FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 29
	FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 29
	FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 29
FortiOS 5.4	FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 29
	FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 30
FortiOS 5.2	FortiManager 5.4.1 and FortiOS 5.2.10 compatibility issues on page 30
	FortiManager 5.2.6 and FortiOS 5.2.7 compatibility issues on page 30
	FortiManager 5.2.4 and FortiOS 5.2.6 compatibility issues on page 31
	FortiManager 5.2.1 and FortiOS 5.2.1 compatibility issues on page 31
	FortiManager 5.2.1 and FortiOS 5.2.0 compatibility issues on page 31

FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues

The following syntax introduced in FortiOS 6.0.8 is not directly supported by FortiManager 6.0.7.

```
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 6.0.7 and FortiOS 5.6.12 compatibility issues

The following syntax introduced in FortiOS 5.6.12 is not directly supported by FortiManager 6.0.7.

```
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 5.6.3 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 version 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 5.4.1 and FortiOS 5.2.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.4.1 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured.

FortiManager 5.2.6 and FortiOS 5.2.7 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.2.6 and FortiOS 5.2.7.

Bug ID	Description
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365782	Install may fail on system global optimize or system fips-cc entropy-token.

FortiManager 5.2.4 and FortiOS 5.2.6 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.2.4 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

FortiManager 5.2.1 and FortiOS 5.2.1 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 5.2.1 and FortiOS 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

FortiManager 5.2.1 and FortiOS 5.2.0 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager 5.2.1 and FortiOS 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Resolved Issues

There are no reported resolved issues in FortiManager version 6.0.12. To inquire about a particular bug, please contact Customer Service & Support.

Known Issues

There are no reported known issues in FortiManager version 6.0.12. To inquire about a particular bug, please contact Customer Service & Support.

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 (Windows)	✓		✓	
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.