# FortiManager - Release Notes

Version 6.2.0

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

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

**FORTINET BLOG**
https://blog.fortinet.com

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

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

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://fortiguard.com/

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

**FEEDBACK**
Email: techdoc@fortinet.com

August 19, 2020
FortiManager 6.2.0 Release Notes
02-620-523220-20200819

# TABLE OF CONTENTS

# FortiManager 6.2.0 Release

This document provides information about FortiManager version 6.2.0 build 1050.

The recommended minimum screen resolution for the FortiManager GUI is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:



## Supported models

FortiManager version 6.2.0 supports the following models:

| | |
|---|---|
| **FortiManager** | FMG-200F, FMG-300E, FMG-300F, FMG-400E, FMG-2000E, FMG-3000F, FMG-3700F, FMG-3900E, FMG-4000E, and FMG-MFGD. |
| **FortiManager VM** | FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, 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). |

## What's new

For information about what's new in FortiManager 6.2.0, see the FortiManager New Features Guide.

Not all features/enhancements are supported on all models.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.2.0.

## 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.

## ADOM Upgrade for FortiManager 6.2

Currently, there is no ADOM upgrade option for ADOM version 6.0 to move to version 6.2. It also means that ADOMs with version 6.0 cannot properly support FortiGates running 6.2. In order to manage FortiGates running 6.2, add them to a 6.2 ADOM.

## 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 6.2.0.

For details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:



## Downgrading to previous firmware versions

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

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

## Firmware image checksums

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

## FortiManager VM firmware

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

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

The section contains the following topics:



## FortiManager 6.2.0 support

This section identifies FortiManager 6.2.0 product integration and support information:



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

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

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

### Web browsers

This section lists FortiManager 6.2.0 product integration and support for web browsers:

- Microsoft Edge 40
- Mozilla Firefox version 66
- Google Chrome version 73

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

## FortiOS/FortiOS Carrier

This section lists FortiManager 6.2.0 product integration and support for FortiOS/FortiOS Carrier:

| FortiOS or FortiOS Carrier | | Compatibility Issues |
|---|---|---|
| 6.2 | 6.2.0 | |
| 6.0 | 6.0.4 | |
| | 6.0.0 to 6.0.3 | FortiManager 6.0.2 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.3, with some minor interoperability issues. For information, see FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 26. |
| 5.6 | 5.6.7 to 5.6.8 | |
| | 5.6.5 to 5.6.6 | FortiManager 5.6.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.6, with some minor interoperability issues. For information, see FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 26. |
| | 5.6.4 | FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 27. |
| | 5.6.2 to 5.6.3 | FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.3, with some minor interoperability issues. For information, see FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 27. |
| | 5.6.0 to 5.6.1 | FortiManager 5.6.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 27. |
| 5.4 | 5.4.10 | FortiManager 5.4.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10, with some minor interoperability issues. For information, see FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 28. |
| | 5.4.9 | FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9, with some minor interoperability issues. For information, see FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 28. |
| | 5.4.1 to 5.4.8 | FortiManager 6.2.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8, with some minor interoperability issues. For information, see FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 28. |

## FortiAnalyzer

This section lists FortiManager 6.2.0 product integration and support for FortiAnalyzer:

- 6.2.0
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later
- 5.2.0 and later
- 5.0.0 and later

## FortiAuthenticator

This section lists FortiManager 6.2.0 product integration and support for FortiAuthenticator:

- 5.3
- 4.3

## FortiCache

This section lists FortiManager 6.2.0 product integration and support for FortiCache:

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

## FortiClient

This section lists FortiManager 6.2.0 product integration and support for FortiClient:

- 6.0.5
- 6.0.0
- 5.6.6
- 5.6.3
- 5.6.0
- 5.4.0 and later
- 5.2.0 and later

## FortiMail

This section lists FortiManager 6.2.0 product integration and support for FortiMail:

- 6.0.4
- 5.4.9
- 5.4.5
- 5.3.12
- 5.2.10
- 5.1.7
- 5.0.10

## FortiSandbox

This section lists FortiManager 6.2.0 product integration and support for FortiSandbox:

- 3.0.4
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2
- 2.1.3
- 1.4.0 and later
- 1.3.0
- 1.2.0 and later

## FortiSwitch ATCA

This section lists FortiManager 6.2.0 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later
- 4.3.0 and later
- 4.2.0 and later

## FortiWeb

This section lists FortiManager 6.2.0 product integration and support for FortiWeb:

- 6.1.0
- 6.0.3
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1
- 5.3.9
- 5.2.4

- 5.1.4
- 5.0.6

## FortiDDoS

This section lists FortiManager 6.2.0 product integration and support for FortiDDoS:

- 5.0.0
- 4.7.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3
- 4.1.11

Limited support. For more information, see Feature support on page 15.

## Virtualization

This section lists FortiManager 6.2.0 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- 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 6.2.0.

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

This section contains the following topics:



## FortiGate models

| Model | Firmware Version |
|---|---|
| **FortiGate:** FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FortiGate-60E-POE, FortiGate-61E, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E<br>**FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1<br>**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<br>**FortiGate Hardware Low Encryption:** FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC<br>**FortiWiFi:** FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM | 6.2 |

| Model | Firmware Version |
|---|---|
| **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<br>**FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D<br>**FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen | |
| **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-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E<br>**FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1<br>**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<br>**FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC<br>**Note:** All license-based LENC is supported based on the FortiGate support list.<br>**FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D<br>**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<br>**FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D | 6.0 |
| **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<br>**FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1<br>**FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F<br>**FortiGate 7000 Series:** FG-7030E, FG-7040E, FG-7060E | 5.6 |

| Model | Firmware Version |
|---|---|
| **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<br>**FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC<br>**Note:** All license-based LENC is supported based on the FortiGate support list.<br>**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<br>**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<br>**FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D | |
| **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<br>**FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1<br>**FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F<br>**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<br>**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<br>**FortiGate Hardware Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC<br>**Note:** All license-based LENC is supported based on the FortiGate support list.<br>**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<br>**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<br>**FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D | 5.4 |

## 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<br>**FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC<br>**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<br>**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<br>**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<br>**FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F<br>**FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E<br>**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<br>**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<br>**FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F<br>**FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E<br>**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<br>**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<br>**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 | 5.2 |

| Model | Firmware Version |
|---|---|
| **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-Xen | |

## FortiDDoS models

| Model | Firmware Version |
|---|---|
| **FortiDDoS:** FI-1500E | 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.<br><br>**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.<br><br>**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.<br><br>**FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen). | 5.6 |
| **FortiAnalyzer:** FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.<br><br>**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 | 5.2 |

| Model | Firmware Version |
|---|---|
| **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN | |
| **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<br>**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 | 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<br>**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<br>**FortiMail Low Encryption:** FE-3000C-LENC<br>**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<br>**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<br>**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<br>**FortiMail VM:** FE-VM64 | 5.0 |

## FortiSandbox models

| Model | Firmware Version |
|---|---|
| **FortiSandbox:** FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D<br>**FortiSandbox VM:** FSA-KVM, FSA-VM | 2.5.2 |
| **FortiSandbox:** FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D<br>**FortiSandbox VM:** FSA-VM | 2.4.1<br>2.3.3 |

| Model | Firmware Version |
|---|---|
| **FortiSandbox:** FSA-1000D, FSA-3000D, FSA-3500D<br>**FortiSandbox VM:** FSA-VM | 2.2.0<br>2.1.3 |
| **FortiSandbox:** FSA-1000D, FSA-3000D<br>**FortiSandbox VM:** FSA-VM | 2.0.3<br>1.4.2 |
| **FortiSandbox:** FSA-1000D, FSA-3000D | 1.4.0 and 1.4.1<br>1.3.0<br>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<br>**FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C | 5.0.0 |
| **FortiSwitch-ATCA:** FS-5003A, FS-5003B | 4.3.0<br>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<br>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<br>**FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER | 6.0.1 |

| Model | Firmware Version |
|---|---|
| **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<br>**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<br>**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<br>**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<br>**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<br>**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<br>**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<br>**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<br>**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<br>**FortiCache VM:** FCH-VM64 | 4.0, 4.1, 4.2 |

## FortiProxy models

| Model | Firmware Version |
|---|---|
| **FortiProxy:** FPX-400E, FPX-2000E<br>**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<br>**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<br>**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 6.2.0. Compatibility issues have been identified for the following FortiOS releases:



## 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 6. |
| 516242 | Install verification may fail on the wtp profile's `handoff-sta-thresh` parameter. |

## 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. |

| Bug ID | Description |
|---|---|
| 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:<br>• `rsso-endpoint-block-attribute`, `rsso-endpoint-block-attribute`, or `sso-attribute` for RADIUS users.<br>• `sdn` and its `filter` attributes for firewall address objects.<br>• `azure` SDN connector type.<br>• `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:<br>• `system replacemsg mail "email-decompress-limit"`<br>• `system replacemsg mail "smtp-decompress-limit"`<br>• `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:<br>`rsso-endpoint-attribute`<br>`rsso-endpoint-block-attribute`<br>`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 6.2.0. For inquires about a particular bug, please contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 356454 | The Central SSL-VPN or SSL-VPN query unexpectedly shows users from all VDOMs that are managed in another ADOM. |
| 411314 | The `diagnose cdb check adom-integrity` command cannot recover ADOM with address name that has a leading or trailing space. |
| 417358 | Search result is lost after editing an object. |
| 434611 | Policy check should detect policies with "none" objects and report them as a specific category under Policy Consistency Check. |
| 436774 | FortiManager is missing permission settings when managing FortiAnalyzer. |
| 443240 | HA-status changes to standalone from ELBC cluster when making changes to FortiGuard server setting directly on FortiGate. |
| 474245 | The "set disk-usage log" command should not be installed for devices with log disk. |
| 478257 | VPN Manager should filter out invalid interfaces for the default VPN interface. |
| 486445 | Scheduled TCL scripts fail when executed against a single device, multiple devices, or a Device Group. |
| 489373 | Passwords should allow special characters on certificate templates in FortiManager. |
| 489817 | `exec device replace` fails when the target serial number already exists in database as an unregistered device. |
| 492088 | FortiManager attempts to change Chassis ID on FortiGate 7000 series when installing configuration. |
| 496827 | Unable to delete the LDAP server, if the user group is deleted before removing the LDAP members. |
| 497179 | The Monitor in the VPN Manager does not respect the units when sorting by incoming or outgoing data. |
| 498107 | When an address is a member of a dynamic address group, its *Where Used* results does not say which dynamic group it belongs to. |
| 500069 | DOS Policy Anomaly configuration settings are missing the Quarantine, Quarantine-Expiry, and Quarantine-Log options. |
| 500410 | FortiManager GUI should allow configuring Phase 2 Selector Local and Destination addresses with an IPv6 type with subnet, range, IP, or name. |
| 500697 | Application signature list is either empty or displayed as *undefined*. |

| Bug ID | Description |
|---|---|
| 500991 | There should be a clear error message on why the policy package install failed after reclaimed tunnel. |
| 501202 | AP Manager Wi-Fi profiles missing LAN ports configuration settings on FortiManager GUI. |
| 503722 | FortiSwitch Manager and AP Manager reports switches and APs connected to FortiGates as online when the devices are no longer powered on. |
| 503915 | Users may not be able to change device password via JSON APIs. |
| 504302 | The *IPv4 Split include* option for IPSec should be available under the Range assignment mode. |
| 504962 | When creating new vdom-link from the global interface menu, all the VDOMs should be visible in the management VDOM. |
| 506163 | Device Manager GUI no longer displays interface zone members following upgrade. |
| 506697 | Under HA's port monitor, we should be able to see all port-monitored interfaces, such as aggregated, loop-back, or VLAN interface. |
| 507044 | FortiManager always overrides the device-level configured parameters to DPD default values making impossible to tune DPD settings when using VPN Manager. |
| 507107 | FortiManager should not unset the *switch-controller-igmp-snooping* and *switch-controller-dhcp-snooping* settings. |
| 508340 | With the ADOM option *Perform Policy Check Before Every Install* enabled and no changes to install, an install will fail with the *Validation Failed* message. |
| 510665 | After an interface is created, the configuration status is not updated. |
| 511256 | Policy Package status should show as modified after making changes in web filter profile. |
| 511580 | After upgrade, install may fail on web filtering profile. |
| 511826 | FortiManager should remove the mandatory requirement of having a hub-to-hub interface when two hubs are defined in a VPN community using VPN Manager. |
| 512046 | When workspace is enabled, IPv6 session based counters are synchronized with FortiGate. |
| 513675 | Policy push should not be allowed if another user has the device locked. |
| 513763 | User should be allowed to change country code in existing or cloned AP profile settings. |
| 513799 | FortiManager should only display detected rogue APs that are online. |
| 515541 | FortiManager is not updating the password of FortiGates under managed FortiAnalyzer. |
| 516158 | FortiManager should not add domain-filter syntax during ADOM upgrade. |
| 516621 | When a new profile with password/secret field, such as TACACS, Radius, etc., is created, FortiManager populates secret values with a dummy value that is longer than the allowed maximum length. |
| 517060 | User should able to change the action for multiple signatures at once. |
| 517061 | ADOM upgrade may fail when the IPs in FortiSwitch VLAN DHCP server are configured with zero. |

| Bug ID | Description |
|---|---|
| 517232 | Invalid Source/Destination "Negate Cell" option for certain policy types and missing "Negate Cell" for IPv4 policy source address. |
| 517618 | Users should be able to use "Header" type Explicit Policy address as Source Address in Explicit Proxy policies. |
| 517768 | FortiManager should allow users to create routes with interface that is dedicated to management. |
| 517874 | FortiManager should be able to use 'US only' FortiGaurd servers with any license configuration. |
| 518148 | The System replacement messages for *Manage Images* should not be grayed out. |
| 518680 | IP Pool not imported due to an error while creating mapping failed due to "arp-intf" which is a member of a zone setting in IP pool. |
| 518708 | When viewing the devices in Device Manager, the list automatically scrolls back to the top for every heartbeat interval. |
| 518756 | When *vdom-netflow* is disabled, FortiManager should not push any collector-ip and source-ip settings to FortiGate. |
| 518949 | When exporting a Policy Package using CSV, it does not include Footer policies. |
| 518984 | Cluster members should show consistent results in dashboard and device settings. |
| 519108 | Scheduled Remote CLI Scripts are struck at 1%. |
| 519229 | When using workspace mode, modification to device group is not recognized as a change. |
| 519252 | After FortiManager was upgraded, cloning a policy package changes the package inspection mode. |
| 519297 | When FortiManager manages FortiGate v5.6 or earlier devices, FortiManager should not support fsso-type group for switch-controller security-policy. |
| 519487 | FortiGate fails to receive FortiGuard updates from FortiManager when ssl-static-key-ciphers is disabled. |
| 519495 | Running a script always returns the error, *the script is not eligible*, even though the actual error may be different. |
| 520092 | FortiManager should not update any dynamic attributes for SCEP generated objects. |
| 520548 | It should be possible to close the pop up window and see current number of successful tasks for the policy assignment of a global package. |
| 520651 | When querying a policy package, FortiManager API's response may be missing the VDOM information. |
| 520691 | FortiManager should Warn user in install wizard if there is an IP address being installed that is 0.0.0.0/0. |
| 520976 | Revision diff always shows changes with policy package settings. |
| 521117 | FortiManager should not check for empty service when internet-service is disabled, which may cause copy to fail. |

| Bug ID | Description |
|---|---|
| 521379 | FortiManager may disable the reliable option for FortiAnalyzer log settings. |
| 521649 | Policy counters may not be accurately synchronized with the FortiGate devices. |
| 521673 | FortiManager does not trigger policy package status to shown as modified when LDAP configuration is changed. |
| 521900 | SD-WAN rule protocol options 'ANY' is not saved on GUI. |
| 522025 | Under Policy & Objects, the frame column width is reset to default when user refreshes or re-enters the same object list. |
| 522206 | GTP global tunnel limit is not configurable on FortiManager. |
| 522310 | Unable to edit Global ADOM DB to change global version from GUI (which will reset Global config). As a workaround, use CLI `exec reset adom-settings global` or upgrade global version. |
| 522440 | FortiManager should support the IPS signature syntax, `--icmp.type !=`. |
| 522713 | ADOM upgrade stuck at 5%. |
| 522779 | Secured backups fail due to issue with the SSH certificate. |
| 522828 | FortiManager unsets dhcp-snooping when installing from a 5.4 ADOM. |
| 523480 | IPS Filter does not include ALL if filtered based on OS. |
| 523639 | VPN Manager Monitor page stuck loading when an external gateway is defined. |
| 523705 | In webfilter profile, FortiManager should only allow configuring quota for categories set to monitor, warning, or authenticate. |
| 523878 | FortiManager should not install the CLIs, `system csf {upstream-ip upstream-port group-name group-password}`, which are read-only attributes on FGT-6000F. |
| 524202 | Upgrading Global Database removes all ADOMs from policy package Assignment section. |
| 524607 | FortiManager should not allow illegal change with ssl-ssh-profile causing installation to fail. |
| 524752 | IPS custom signature using protocol type ICMP is valid in FortiOS syntax and therefore should be able to import into FortiManager. |
| 525926 | The Local Users column is always empty even if a token is assigned. |
| 526002 | When having multiple hosts within an SNMP community, it's not possible to edit a host and change the status of HA-direct. |
| 526287 | Policy install may be stuck at 67%. |
| 526642 | Some SMTP/splice options under firewall profile-protocol options cannot be disabled. |
| 526934 | Web UI should not enable HTTP access under Interface Settings when a user views interface settings. |
| 526938 | Searching an IP address in interface list should show the interface and the zone in which the interface is a member of. |

| Bug ID | Description |
|---|---|
| 527140 | FortiManager is unable to add multiple DHCP Relay Servers from the Device Manager System Interface Menu. |
| 527407 | Users may not be able to change the FortiGate HA management interface IP. |
| 528633 | IS-IS interfaces cannot be deleted from GUI. |
| 528916 | Users may not be able to upgrade ADOM after ADOM name has been changed. |
| 528931 | FOS-VM may be getting invalid license from FMGR-VM-Meter. |
| 528938 | FortiManager does not allow users to manually set SD-WAN member sequence ID. |
| 528977 | FortiGuard 7000 Service Status shows slave chassis with serial number instead of host name. |
| 529036 | VPN Manager should not show the options for main and aggressive mode when IKEv2 is selected. |
| 529475 | Webfilter and Application profiles are not available in the FortiClient profile GUI. |
| 529480 | Policy look-up can only list policy package installation target device but not device group member. |
| 530207 | Installing configuration after fail-over in cluster causes installation fail because of difference in management-ip. |
| 530249 | Policies that are Last Modified matched by actual traffic always shows recently modified by 'admin' even if the default admin user is not present in the FortiManager configuration. |
| 530376 | Users are unable to select Schedule Object for SSID in AP Manager. |
| 530735 | FortiManager may not be able to configure a full-mesh VPN among FortiGates with multi-VDOMs. |
| 530749 | FortiManager is unable to import policy configuration from devices with a long VDOM name. |
| 530792 | When configuring Per-Device Mappings for Real Servers, mode is missing and users cannot create multiple real servers. |
| 530837 | Users should not be allowed to delete default meta fields. |
| 531508 | When trying to add a new gateway from VPN Manager, FortiManager returns an error *peer invalid value*. |
| 531573 | FortiManager is not able to set Type of Service field for SD-WAN service. |
| 531610 | FortiManager is showing *Create New* option under script even though ADOM is not locked. |
| 531645 | FortiManager should be able to configure dynamic mappings for SD-WAN via a script. |
| 531813 | With Safari, there are two issues when user editing device group: there are two scroll bars in the *Edit Device Group* window and *Edit Device Group* window size that cannot be changed. |
| 531963 | SSL/SSH Profile should not allow the user to enable "Allow Invalid SSL Certificates" when Inspection mode is "SSL Certificate Inspection". |
| 532075 | When editing comment/description, FortiManager may display the slash character, /, as #x2F. |
| 532275 | Within the System Admin Profile, users may not be able to change access control due to JavaScript errors. |

| Bug ID | Description |
|---|---|
| 532488 | Bytes/Hit/packet count should not be a parameter to consider in the diff as these are not part of the configuration. |
| 532721 | Once a Local ID value is configured for a VPN Node within VPN Manager, it can no longer be removed. |
| 532943 | FortiGate's system time is now shown on FortiManager when timezone index is set at 79, 80, or 83. |
| 533141 | Retrieving configuration under Workspace mode does not allow further changes under AP manager. |
| 533857 | FortiManager is unable to automatically register devices via Pre-Shared Key method if a revision is imported prior to registering the devices. |
| 534559 | Editing WiFi interface which is a zone member should not enable block intra-zone traffic. |
| 534784 | FSSO Agent with option "Select FSSO groups via FortiGate" does not work if the policy has no pending changes. |
| 534784 | Adding section for traffic shaping policies causes runtime error. |
| 534927 | When there is a dynamic interface and a multicast interface that has the same name within a policy package, the install wizard was not be able to create dynamic mappings. |
| 535170 | FortiManager does not accept FQDN address configuration containing the _ character. |
| 535525 | Dynamic/Dial-up Type IPSec Tunnel Interface cannot be added as an SD-WAN member. |
| 535621 | Retrieving or importing configuration revision fails if configuration contains a large number of CRLs. |
| 535743 | Downstream FortiManager does not update signature until changing the schedule setting in the second tier FortiManager's FDN. |
| 536043 | When ADOM is locked, FortiManager may display incorrect values or configurations from some objects or policies. |
| 536805 | Install fails for DoS policy quarantine-expiry. |
| 537135 | There is no GUI validation when an invalid subnet mask is used as destination for a Static Route. |
| 537236 | LDAP query failure over slow satellite connection. |
| 537752 | FortiManager tries to add full scan options while using quick scan in default AV profile. |
| 537775 | Proxy policy should not allow empty source address. |
| 538029 | Occasionally, duplicate sequence number may appear in some policy packages. |
| 539184 | FortiManager should not install forward-error-correction on VLANs. |
| 539998 | Install fails when deny rule contains DNS filter profile. |
| 540065 | FortiManager should be able to display CA certificate under 6.0 ADOM. |
| 540095 | Scheduled TCL Script intermittently fails to run on the scheduled time after upgrade. |

| Bug ID | Description |
|---|---|
| 540936 | Remote wildcard users break user profile access to workflow sessions. |
| 542823 | Script fails to set accprofile on device database. |
| 543567 | FortiManager does not install new certificate obtained from FortiAuthenticator. |
| 545457 | AP Manager may not be able to show map. |
| 545480 | When attempting to remove a VDOM from a FortiGate by running a script, the script fails unexpectedly and the VDOM is not deleted. |
| 547740 | When FortiManger is running in workspace mode, FortiManager may unexpectedly delete firewall policy. |

# Known Issues

The following issues have been identified in 6.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 546131 | Importing SDN Connector fails within Global ADOM. |
| 546246 | Restore ADOM revision does not restore removed installation targets. |
| 546303 | Install fails when FortiManager sets VDOM mode to no-vdom. |
| 546656 | Import Azure SDN fails if subscription ID is not configured. |
| 547173 | FortiManager cannot install allow-routing for VLAN generated address. |
| 547854 | FortiManager cannot manage shaping profiles with the same name from multiple FortiGate. |
| 548131 | VAP interface page cannot show interface IP and SSID configuration. |
| 548136 | SSID configuration change cannot trigger install. |
| 548350 | After enabling Split-task VDOM, installing `vdom-property` fails for `snmp-index`. |
| 548416 | Changes on *Existing Static Route* does not show up on Installation Preview. |
| 548442 | Administrator with read-only profile can restart and upgrade FortiAP and FortiSwitch firmware. |
| 548682 | FortiManager generates invalid application override configuration for application profile. |
| 548976 | Unauthorized device alert directs to a page showing duplicate devices. |
| 549023 | FortiManager fails to set `allowaccess` on VWP interface. |
| 549043 | FortiManager cannot render the Virtual Wire Pair entry properly after edited an interface. |
| 549065 | Default AP profile shows incorrect country name. |
| 549113 | In the case that FortiGate is in NGFW policy-based mode, URL/Application control profiles should not be visible on FortiManager side. |
| 549175 | FortiManager does not install active directory group filter changes to FortiGate. |
| 549207 | Import Wizard fails to create dynamic mapping for Address, VIP, or IP Pool object or group if name has more than 63 characters. |
| 549260 | When enabling Split-task VDOM by script, installation fails as it tries to delete global certificate in the FG-Traffic VDOM. |
| 549287 | FortiManager is missing application category selection on traffic shaping policy page. |
| 549293 | FortiManager loses customization on the application and filter override page. |
| 549384 | FortiManager cannot show any query when FortiGate has CSF enabled but the CSF group is not established on FortiManager. |

| Bug ID | Description |
|---|---|
| 549449 | Creating FortiSwitch template using the Import feature does not link the template to the FortiSwitch. |
| 549483 | When editing Application and Filter Overrides action to Allow or Monitor, FortiManager always shows that action as Traffic Shaping. |
| 549504 | Wildcard remote admin cannot run schedule install. |
| 549546 | If an address group contains many addresses, user cannot hover the number icon to view the address members. |
| 549566 | Device Manager does not show a FortiGate in a CSF group when the FortiGate is connected to the root FortiGate's FG-Traffic VDOM. |
| 549587 | All the FortiSwitch ports are incorrectly displayed as POE enabled. |
| 549638 | MAC address Access control list entries under DHCP server get duplicated on editing the other entries. |
| 549693 | ADOM revision diff on a large database may take hours. |
| 549776 | Installing DLP sensor to FortiGate fails when setting `full-archive-proto`. |
| 549818 | FortiManager cannot display external resource setting on consolidated policy list. |
| 549824 | Consolidated policy page is missing external resource as data source. |
| 549827 | FortiManager failed to retrieve `aes128gcm-prfsha` encryption from FortiGate. |
| 549851 | Deleted APs are still shown in AP Manager's Floor Map. |
| 550015 | FortiManager can communicate with mail server with secure option enabled. |
| 550078 | When defining a SSID, some security modes are missing: `wpa3-sae`, `wpa3-sae-transition`, and `owe`. |
| 550105 | FortiManager may not be able to change interface mapping of a zone via Device Manager. |
| 550127 | Threat Feeds types are not displayed consistently in Policy Objects and Fabric View. |
| 550140 | The `fmupdate fds-settings` and `system-support-fgt` configurations are lost if version 5.4 is configure prior to upgrade. |
| 550141 | With 6.2 ADOM, FortiGate installation purges devices on FortiGate. |
| 550157 | Assigned AP profile is not shown while editing APs from Map View. |
| 550161 | Under per-device management, managed AP status information is missing in Map View. |
| 550237 | Administrator with read-only profile can add Detected Device in Device Manager. |
| 550239 | The `aes256cisco` entry is missing for the `priv-proto` field. |
| 550344 | FortiManager is unable to import firewall policy due to invalid FQDN error. |
| 550430 | FortiManager fails to import Azure SDN connector if resource group is configured. |
| 550441 | After upgrade, verification fails for company-identifier with a DLP sensor. |

| Bug ID | Description |
|---|---|
| 550460 | Duplicated default QoS profiles are listed when editing a FortiSwitch template. |
| 550513 | User cannot change IPsec Phase1 in existing IPsec Phase2 within Device Manager. |
| 550537 | Installing WAN Optimize proxy policy fails on FortiGate 60E or 80E. |
| 550546 | FortiManager is unable to retrieve ssl-ssh-profile for ssh-tunnel type Proxy policy. |
| 550579 | Under IPS Profile, the Rate Based Signatures table can never show any signatures. |
| 550591 | After upgrade, user cannot edit VPN table with the error: *invalid value-prop[dpd]: option (enable)*. |
| 550629 | Search in Floor Map's edit mode may not return proper results. |
| 550691 | Installation fails when changing tag type with Email Filter profile. |
| 550809 | FortiManager cannot set defined value on segment with IPv6 template address. |
| 550821 | Users may not be able to change revision history comments. |
| 550926 | AP Manager cannot delete SSID from FortiGate when the SSID is no longer in use. |
| 550949 | FortiManager cannot list FortiClient images. |
| 551091 | FortiManager is unable to bring up IPSec tunnel between FortiGates if the certificates are generated by FortiManager. |
| 551154 | Under per-device management, advanced options are kept loading when creating SD-WAN performance SLA. |
| 551180 | FortiManager may not be able to change some local categories within Web Filter profile to disable. |
| 551200 | FortiManager cannot select any internet service group on SD-WAN rules within Device Manager. |
| 551231 | Under per-device management, editing a SD-WAN rule generates duplicate entry. |
| 560332 | Some CLI widgets are not available in the root ADOM when using multiple wildcard accounts. The error *Non-root ADOM user cannot access CLI* is shown. |
| 468776 | Unable to retrieve device due to *data not exist* (g-xxxx firewall object). |

# 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
```

# Change Log

| Date | Change Description |
|---|---|
| 2019-04-11 | Initial release of 6.2.0. |
| 2019-04-15 | Added a special notice. Added support for FortiClient 6.0.5. |
| 2019-04-18 | Removed the following supported models: FMG-200D, FMG-300D, FMG-1000D, FMG-4000D. |
| 2019-04-22 | Removed 544042 from *Known Issues*. |
| 2019-04-25 | Edited a special notice. Updated the Appendix. |
| 2019-04-29 | Updated to keep only the latest versions of supported products for each minor release in *Product Integration*. |
| 2019-04-30 | Removed FortiGate models for FortiOS 5.2. |
| 2019-05-27 | Added a special notice. |
| 2019-06-10 | Added 560332 to *Known Issues*. |
| 2019-07-24 | Updated the *Product Integration* section. |
| 2019-09-17 | Added a special notice. |
| 2020-08-19 | Added 468776 to *Known Issues* and updated *Special Notices*. |