



FortiManager - Release Notes

Version 6.0.3

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



September 17, 2019

FortiManager 6.0.3 Release Notes

02-603-519402-20190917

TABLE OF CONTENTS

| | |
|--|-----------|
| FortiManager 6.0.3 Release | 5 |
| Supported models | 5 |
| What's new in FortiManager 6.0.3 | 6 |
| System Settings | 6 |
| Special Notices | 7 |
| Managing FortiGate with VDOMs that use Global Profiles | 7 |
| IOC Support on FortiManager | 7 |
| FortiManager 6.0.2 support for FortiOS 6.0.3 | 8 |
| Reconfigure SD-WAN after Upgrade | 8 |
| FortiGate VM 16/32/UL license support | 8 |
| Hyper-V FortiManager-VM running on an AMD CPU | 8 |
| VM License (VM-10K-UG) Support | 8 |
| Recreate Guest List for Guest user group | 9 |
| FortiOS 5.4.0 Support | 9 |
| SSLv3 on FortiManager-VM64-AWS | 9 |
| Upgrade Information | 10 |
| Downgrading to previous firmware versions | 10 |
| Firmware image checksums | 10 |
| FortiManager VM firmware | 10 |
| SNMP MIB files | 12 |
| Product Integration and Support | 13 |
| FortiManager 6.0.3 support | 13 |
| Feature support | 16 |
| Language support | 16 |
| Supported models | 17 |
| FortiGate models | 18 |
| FortiCarrier models | 20 |
| FortiDDoS models | 21 |
| FortiAnalyzer models | 21 |
| FortiMail models | 22 |
| FortiSandbox models | 23 |
| FortiSwitch ATCA models | 23 |
| FortiSwitch models | 23 |
| FortiWeb models | 24 |
| FortiCache models | 25 |
| FortiProxy models | 25 |
| FortiAuthenticator models | 25 |
| Compatibility with FortiOS Versions | 26 |
| FortiOS 5.6.4 compatibility issues | 26 |
| FortiOS 5.6.3 compatibility issues | 26 |
| FortiOS 5.6.0 and 5.6.1 compatibility issues | 27 |
| FortiOS 5.4.10 compatibility issues | 27 |

| | |
|---|-----------|
| FortiOS 5.4.9 compatibility issues | 27 |
| FortiOS 5.2.10 compatibility issues | 28 |
| FortiOS 5.2.7 compatibility issues | 28 |
| FortiOS 5.2.6 compatibility issues | 28 |
| FortiOS 5.2.1 compatibility issues | 28 |
| FortiOS 5.2.0 compatibility issues | 29 |
| Resolved Issues | 30 |
| Known Issues | 33 |
| Appendix A - FortiGuard Distribution Servers (FDS) | 34 |
| FortiGuard Center update support | 34 |
| Change Log | 36 |

FortiManager 6.0.3 Release

This document provides information about FortiManager version 6.0.3 build 255.



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 on page 5](#)
- [What's new in FortiManager 6.0.3 on page 6](#)

Supported models

FortiManager version 6.0.3 supports the following models:

| | |
|------------------------|---|
| FortiManager | FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, and FMG-MFGD. |
| FortiManager VM | FMG-VM64, 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 in FortiManager 6.0.3

The following is a list of new features and enhancements in 6.0.3. For details, see the *FortiManager Administrator Guide*:



Not all features/enhancements listed below are supported on all models

System Settings

Admin Profile - Device Lock and Permission improvement

Change to Admin Profile to allow granular permissions to be assigned per Device and Policy Package with ADOM unlocked, allowing administrators to execute scripts on the Devices & Policy Packages.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.3.

Managing FortiGate with VDOMs that use Global Profiles

FortiManager managing FortiGates with VDOMs enabled and running FortiOS 6.0.0 or later is unable to import global ADOM objects 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 tlsv1
end
```

Upgrade Information

You can upgrade FortiManager 5.6.0 or later directly to 6.0.3. If you are upgrading from versions earlier than 5.6.x, you should upgrade to the latest patch version of FortiManager 5.6, then 6.0.0.



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

This section contains the following topics:

- [Downgrading to previous firmware versions on page 10](#)
- [Firmware image checksums on page 10](#)
- [FortiManager VM firmware on page 10](#)
- [SNMP MIB files on page 12](#)

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.

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 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 6.0.3 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 6.0.3 support on page 13](#)
- [Feature support on page 16](#)
- [Language support on page 16](#)
- [Supported models on page 17](#)

FortiManager 6.0.3 support

The following table lists 6.0.3 product integration and support information:

| | |
|--------------------------------|--|
| Web Browsers | <ul style="list-style-type: none">• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.• Mozilla Firefox version 61• Google Chrome version 68 Other web browsers may function correctly, but are not supported by Fortinet. |
| FortiOS/FortiOS Carrier | <ul style="list-style-type: none">• 6.0.0 to 6.0.3• 5.6.5 to 5.6.6• 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 FortiOS 5.6.4 compatibility issues on page 26.• 5.6.2 to 5.6.3 FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.2 to 5.6.3, with some minor interoperability issues. For information, see FortiOS 5.6.3 compatibility issues on page 26.• 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 FortiOS 5.6.0 and 5.6.1 compatibility issues on page 27.• 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 FortiOS 5.4.10 compatibility issues on page 27.• 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 [FortiOS 5.4.9 compatibility issues on page 27](#).

- 5.4.1 to 5.4.8
- 5.2.8 to 5.2.13

FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see [FortiOS 5.2.10 compatibility issues on page 28](#).

- 5.2.7

FortiManager 5.2.6 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see [FortiOS 5.2.7 compatibility issues on page 28](#).

- 5.2.6

FortiManager 5.2.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see [FortiOS 5.2.6 compatibility issues on page 28](#).

- 5.2.2 to 5.2.5
- 5.2.1

FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see [FortiOS 5.2.1 compatibility issues on page 28](#).

- 5.2.0

FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues. For information, see [FortiOS 5.2.0 compatibility issues on page 29](#).

FortiAnalyzer

- 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

- 5.0 to 5.3
- 4.0 to 4.3

FortiCache

- 4.2.7
- 4.2.6
- 4.1.2
- 4.0.0 to 4.0.4

FortiClient

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

FortiMail

- 5.4.5
- 5.3.12
- 5.2.10

| | |
|-------------------------|--|
| | <ul style="list-style-type: none"> • 5.1.7 • 5.0.10 |
| FortiSandbox | <ul style="list-style-type: none"> • 2.5.0 to 2.5.2 • 2.4.0 and 2.4.1 • 2.3.2 and 2.3.3 • 2.2.2 • 2.1.3 • 1.4.0 and later • 1.3.0 • 1.2.0 and later |
| FortiSwitch ATCA | <ul style="list-style-type: none"> • 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later |
| FortiWeb | <ul style="list-style-type: none"> • 6.0.1 • 5.9.1 • 5.8.6 • 5.8.3 • 5.8.1 • 5.8.0 • 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 | <ul style="list-style-type: none"> • 4.5.0 • 4.4.1 • 4.2.3 • 4.1.11 <p>Limited support. For more information, see Feature support on page 16.</p> |
| Virtualization | <ul style="list-style-type: none"> • 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 |



To confirm that a device model or firmware version is supported by 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.

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 | ✓ | ✓ |

| Language | GUI | Reports |
|------------|-----|---------|
| 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 6.0.3.



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 18](#)
- [FortiCarrier models on page 20](#)
- [FortiDDoS models on page 21](#)
- [FortiAnalyzer models on page 21](#)
- [FortiMail models on page 22](#)
- [FortiSandbox models on page 23](#)
- [FortiSwitch ATCA models on page 23](#)
- [FortiSwitch models on page 23](#)
- [FortiWeb models on page 24](#)
- [FortiCache models on page 25](#)
- [FortiProxy models on page 25](#)
- [FortiAuthenticator models on page 25](#)

FortiGate models

| Model | Firmware Version |
|---|------------------|
| <p>FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG50E, 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, FG200D, 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</p> <p>FortiGate 5000 Series: FG-5001D, FG-5001E, FG-5001E1</p> <p>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</p> <p>FortiGate Hardware Low Encryption: FG-100D-LENC, FG-600C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>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</p> <p>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</p> <p>FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D</p> | 6.0 |
| <p>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,</p> <p>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>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</p> <p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> | 5.6 |

| Model | Firmware Version |
|--|------------------|
| 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 | |
| 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 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 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 | 5.4 |

| Model | Firmware Version |
|--|------------------|
| 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, FG-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 | 5.6 |

| Model | Firmware Version |
|---|------------------|
| 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 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 | |
| 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-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 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 | 4.2, 4.1, 4.0 |

FortiAnalyzer models

| Model | Firmware Version |
|--|------------------|
| 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. | 5.6 |
| 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). | |

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

FortiMail models

| Model | Firmware Version |
|---|------------------|
| FortiMail: FE-60D, FE-200D, FE-200E, FE-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 FortiMail Low Encryption: FE-3000C-LENC FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN | 5.3.12 |
| 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-XENSERVR | 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 |
| 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-XENSERVR, 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-XENSERVR, FWB-HYPERV | 5.4.1 |

| Model | Firmware Version |
|---|------------------|
| 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-XENSERVR, 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-XENSERVR | 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 6.0.3. Compatibility issues have been identified for the following FortiOS releases:

| | |
|-------------|---|
| FortiOS 5.6 | FortiOS 5.6.4 compatibility issues on page 26 |
| | FortiOS 5.6.3 compatibility issues on page 26 |
| | FortiOS 5.6.0 and 5.6.1 compatibility issues on page 27 |
| FortiOS 5.4 | FortiOS 5.4.10 compatibility issues on page 27 |
| | FortiOS 5.4.9 compatibility issues on page 27 |
| FortiOS 5.2 | FortiOS 5.2.10 compatibility issues on page 28 |
| | FortiOS 5.2.7 compatibility issues on page 28 |
| | FortiOS 5.2.6 compatibility issues on page 28 |
| | FortiOS 5.2.1 compatibility issues on page 28 |
| | FortiOS 5.2.0 compatibility issues on page 29 |

FortiOS 5.6.4 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 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: <ul style="list-style-type: none">• <code>rsso-endpoint-block-attribute</code>, <code>rsso-endpoint-block-attribute</code>, or <code>sso-attribute</code> for RADIUS users.• <code>sdn</code> and its <code>filter</code> attributes for firewall address objects.• <code>azure</code> SDN connector type.• <code>ca-cert</code> attribute for LDAP users. |

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. |

FortiOS 5.6.0 and 5.6.1 compatibility issues

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

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

FortiOS 5.4.10 compatibility issues

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

| Bug ID | Description |
|--------|--|
| 508337 | FortiManager cannot edit the following configurations for replacement message: <ul style="list-style-type: none"><code>system replacemsg mail "email-decompress-limit"</code><code>system replacemsg mail "smtp-decompress-limit"</code><code>system replacemsg nntp "email-decompress-limit"</code> |

FortiOS 5.4.9 compatibility issues

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

| Bug ID | Description |
|--------|--|
| 486592 | FortiManager may report verification failure on the following attributes for RADIUS users: <code>rsso-endpoint-attribute</code> <code>rsso-endpoint-block-attribute</code> <code>sso-attribute</code> |

FortiOS 5.2.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 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. |

FortiOS 5.2.7 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 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. |

FortiOS 5.2.6 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 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. |

FortiOS 5.2.1 compatibility issues

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

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

FortiOS 5.2.0 compatibility issues

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

The following issues have been fixed in 6.0.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

| Bug ID | Description |
|--------|--|
| 304522 | Wildcard admin is unable to approve a workflow session. |
| 413390 | FGFM connection flapping when FortiGate is moved to another ADOM. |
| 423921 | Cannot get CSF group name. |
| 434984 | Unable to create/edit/delete ADOMs when system setting is read only. |
| 439512 | FortiManager attempts to delete user groups that are used only under system admin, if not defined in the management VDOM. |
| 450434 | The "wtp-mode" option is unset after change of AP config from AP Manager. |
| 451684 | List all conflicting Global assigned objects in Import Wizard and report. |
| 453417 | Import of PKCS #12 local certificate failed. |
| 474629 | When Security Profile Groups are created on FortiManager, all Security Profile Groups are pushed to all FortiGate units on next policy push. |
| 480400 | Device Manager > System Information does not display correct FortiGate system time. |
| 481901 | Add a CLI command to reset hitcount for all ADOMs and dbcach. |
| 485859 | Should remove Botnet from Application Control for 5.6/6.0 ADOMs. |
| 491926 | Rename ADOM interface during Import Policy may fail to add policy. |
| 492893 | Installing custom IPS and <i>AppCtl</i> signatures with the same Attack ID will fail installation or not function correctly on FortiGate. |
| 494108 | When adding an interface to a zone, the <i>Block intra-zone traffic</i> option is unset. |
| 494253 | Some service objects are not visible in GUI of specific ADOMs when backend has invalid service config. |
| 499053 | Wrong interface-pair view for Proxy Policy. |
| 499066 | Can't verify PKI admin client certificate, if the CA chain has more than 2 certificates. |
| 499341 | A new LDAP admin user with GUI access is using an admin profile of a previously created LDAP admin user. |
| 499568 | Missing Guest Management support in FortiManager Policy & Objects tab. |
| 500480 | After editing an address that is used in an address group, the status did not change for 'Policy Package Status'. |
| 501096 | Policy package status of all devices going in Modified state when policy package is imported for |

| Bug ID | Description |
|--------|--|
| | new devices. |
| 501467 | Application fgdsrv crashes several times per day - parseFragment: url index out of range. |
| 501485 | ADOM upgrade from 5.4 to 5.6 tries to change 'Web Filter Local Category' ID from 179 to 192. |
| 501195 | Upgrading FGT-60D by FortiManager sometimes fails due to the firmware image transfer stopping. |
| 503072 | Application crond crashes are caused by hitcount updates. |
| 504394 | AP Manager - WiFi profile FAP221E does not display RADIO 2 option. |
| 504422 | Install verification fails after FortiGate HA failover due to vdom-link macaddr mismatch. |
| 504541 | Page is not loading properly for AP profiles under AP Manager in 5.2 ADOM. |
| 504636 | Some address objects are not visible in GUI of specific ADOMs when backend has invalid address config. |
| 504999 | Install SD-WAN static route to FortiGate failed. |
| 505004 | Columns overlap in policy list page. |
| 505276 | VPN Monitor stuck loading for 5.2/5.4 ADOMs. |
| 507075 | Upgrade of ADOM 'root' from 5.6 to 6.0 hangs and crashes <i>svc cdb reader</i> . |
| 507092 | FortiManager cannot show 1 ADOM interface page when interface dynamic mapping is missing device information. |
| 507300 | FortiManager should not download the FortiGate delta package from FortiGuard. |
| 507394 | FortiManager displays the "Error:response with errors" error when creating a new script that is over the tablesize limit. |
| 507628 | After successful installation, device config status may show as out of sync or modified or conflict |
| 507919 | Need to import firewall internet-service-custom, although it is not directly used by firewall policy. |
| 508810 | Administrative Distance is missing for Static Route with Destination type Named Address. |
| 509173 | Policy package installation for root ADOM fails after upgrading from 5.4.5 to 5.6.4. |
| 509185 | FortiManager installs default certificate instead of dynamically mapped certificate that is used in dynamically mapped virtual server. |
| 509769 | 5.4 ADOM cannot assign profile to FAP221. |
| 509854 | If firewall address groups are recursively defined (for example, its member contains itself), this causes the security console to crash. |
| 510641 | Edit policy and click OK. The table scrolls back to top. |
| 510910 | When a new object is created from an IPv4 policy, the previous content of the related field is cleared. |
| 510929 | GUI Import wizard should display "Renamed Objects" before importing objects. |

| Bug ID | Description |
|--------|---|
| 510936 | Adding a new device to address object dynamic mapping sets the interface to 'any' for previous associated devices. |
| 511170 | FortiAnalyzer/Fortimanager cannot sync with some NTP servers. |
| 511753 | SNMP event power-supply-failure is missing for some devices. |
| 512350 | <code>system.ha.hbdev</code> will not always save. This is applicable to CLI only. |
| 513243 | On the device level interface config page, the allow access config cannot disable HTTP. |
| 513255 | GUI slowness is caused by viewing, editing, or cloning IPsec phase1/phase2 in Device Manager. |
| 514300 | The log <i>FortiAnalyzer filter</i> setting cannot be retrieved or configured on FortiManager. |
| 516789 | Fabric Connector for VMWare NSX not importing any object and displays error message 'Internal Error' for NSX version 6.3.3. |
| 516889 | FortiManager will use FortiGuard update for FortiGate certificate bundle support. |
| 517204 | Add/Retrieve fails with "data not exist" if "external-resource" category is used in "ftgd-dns filters" in DNS filter. |
| 517235 | Device Manager System DHCP Server Lease Time changes not editable via GUI. |
| 517243 | Refreshing "Policy & Objects" pane clears the "Last Modified" tab on the policies. |
| 517533 | Cannot specify more than one DNS server in AP Manager SSID profile. |
| 518668 | Inconsistent user-database options when configuring a local Authentication Scheme. |
| 519188 | RADIUS VSA attributes can be used to gain read-write access to all ADOMs. |
| 519206 | Web Server Error 500 when trying to filter device Session List. |

Known Issues

The following issues have been identified in 6.0.3. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

| Bug ID | Description |
|--------|--|
| 478257 | VPN Manager should filter out invalid interfaces for the default VPN interface. |
| 501202 | AP Manager Wifi profiles missing LAN ports configuration settings on FortiManager GUI. |
| 507629 | Clicking the Cancel button in the Install wizard causes task errors. |
| 510625 | FortiOS-VM traffic drop when Invalid Response received from FortiManager during license check. |
| 510663 | Despite the FDS proxy settings, FortiManager is attempting to connect directly to the productapi.fortinet.com. |
| 517232 | Invalid Source/Destination "Negate Cell" option for certain policy types and missing "Negate Cell" for IPv4 policy source address. |
| 518680 | IP Pool not imported due to error create mapping fail related to "arp-intf" which is a members of a zone setting in ippool. |
| 519108 | Scheduled Remote CLI Scripts are stuck at 1%. |
| 520899 | When editing the Address Group Dynamic mapping configuration entry for the second time, the GUI will show an empty member list. Close the address group configuration page and re-edit the mapping entry as a first time edit. |
| 522310 | B255: Unable to edit Global ADOM DB to change global version from GUI. |
| 523156 | GUI failed to create or edit SSL VPN portal profile in 5.2, 5.4, and 5.6 ADOMs. |

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 | Version | Antivirus | WebFilter | Vulnerability Scan | Software |
|------------------------|---|-----------|-----------|--------------------|----------|
| FortiClient (Windows) | • 6.0.0 and later | ✓ | ✓ | ✓ | ✓ |
| FortiClient (Windows) | • 5.6.0 and later • 5.4.0 and later | ✓ | | ✓ | |
| FortiClient (Mac OS X) | • 6.0.0 and later • 5.6.0 and later • 5.4.0 and later | ✓ | | ✓ | |
| FortiMail | • 5.4.5 • 5.4.2 • 4.3.7 • 4.2.9 • 5.1.6 | ✓ | | | |
| FortiSandbox | • 2.5.0, 2.5.1 • 2.4.0, 2.4.1 • 2.3.2 • 2.2.1 • 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0, 1.2.3 | ✓ | | | |
| FortiWeb | • 5.9.0 | ✓ | | | |

| Platform | Version | Antivirus | WebFilter | Vulnerability Scan | Software |
|----------|---|-----------|-----------|--------------------|----------|
| | <ul style="list-style-type: none">• 5.8.6• 5.6.0• 5.5.4• 5.4.1• 5.3.8• 5.2.4• 5.1.4• 5.0.6 | | | | |



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

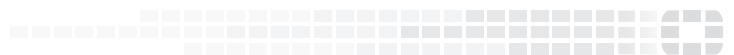
```
config fmupdate support-pre-fgt-43
set status enable
end
```

Change Log

| Date | Change Description |
|------------|--|
| 2018-11-02 | Initial release of 6.0.3. |
| 2018-11-07 | Added FMG-VM64-GCP to <i>Supported Models</i> . |
| 2018-11-09 | Resolved issues added (423921, 512350). Special notice added for Resolved Issue 499568 in the Special Notices section. Known Issue added (523156). |
| 2018-11-13 | Added a Known Issue (520899). |
| 2018-11-21 | Updated to fix issue with checkmark symbol in tables. |
| 2018-12-17 | Added Known Issue 510625. |
| 2019-01-11 | Updated <i>Special Notices</i> and <i>Product Integration</i> . |
| 2019-01-29 | Added 501195 to <i>Resolved Issues</i> . |
| 2019-09-17 | Added a special notice. |



FORTINET®



Copyright© 2019 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.