



# FortiManager - Release Notes

Version 6.0.6

**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](mailto:techdoc@fortinet.com)



September 13, 2019

FortiManager 6.0.6 Release Notes

02-606-569660-20190913

# TABLE OF CONTENTS

<b>FortiManager 6.0.6 Release</b>	<b>5</b>
Supported models	5
<b>Special Notices</b>	<b>6</b>
Common Vulnerabilities and Exposures	6
Managing FortiGate with VDOMs that use Global Profiles	6
IOC Support on FortiManager	7
FortiManager 6.0.2 support for FortiOS 6.0.3	7
Reconfigure SD-WAN after Upgrade	7
FortiGate VM 16/32/UL license support	7
Hyper-V FortiManager-VM running on an AMD CPU	7
VM License (VM-10K-UG) Support	8
Recreate Guest List for Guest user group	8
FortiOS 5.4.0 Support	8
SSLv3 on FortiManager-VM64-AWS	8
<b>Upgrade Information</b>	<b>9</b>
Downgrading to previous firmware versions	9
Firmware image checksums	9
FortiManager VM firmware	9
SNMP MIB files	11
<b>Product Integration and Support</b>	<b>12</b>
FortiManager 6.0.6 support	12
Feature support	15
Language support	15
Supported models	16
FortiGate models	17
FortiCarrier models	19
FortiDDoS models	20
FortiAnalyzer models	20
FortiMail models	21
FortiSandbox models	22
FortiSwitch ATCA models	22
FortiSwitch models	22
FortiWeb models	23
FortiCache models	24
FortiProxy models	24
FortiAuthenticator models	24
<b>Compatibility with FortiOS Versions</b>	<b>25</b>
FortiOS 5.6.4 compatibility issues	25
FortiOS 5.6.3 compatibility issues	25
FortiOS 5.6.0 and 5.6.1 compatibility issues	26
FortiOS 5.4.10 compatibility issues	26
FortiOS 5.4.9 compatibility issues	26

---

FortiOS 5.2.10 compatibility issues .....	27
FortiOS 5.2.7 compatibility issues .....	27
FortiOS 5.2.6 compatibility issues .....	27
FortiOS 5.2.1 compatibility issues .....	27
FortiOS 5.2.0 compatibility issues .....	28
<b>Resolved Issues</b> .....	<b>29</b>
Common Vulnerabilities and Exposures .....	29
<b>Known Issues</b> .....	<b>30</b>
<b>Appendix A - FortiGuard Distribution Servers (FDS)</b> .....	<b>32</b>
FortiGuard Center update support .....	32
<b>Change Log</b> .....	<b>33</b>

# FortiManager 6.0.6 Release

This document provides information about FortiManager version 6.0.6 build 349.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 5](#)

## Supported models

FortiManager version 6.0.6 supports the following models:

<b>FortiManager</b>	FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000D, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3900E, FMG-4000D, FMG-4000E, and FMG-MFGD.
<b>FortiManager VM</b>	FMG-VM64, FMG-VM64-ALI, FMG-VM64-AWS, FMG-VM64-AWS-OnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.6.

## Common Vulnerabilities and Exposures

FortiManager 6.0.6 is no longer vulnerable to the issue described in the following link - <https://fortiguard.com/psirt/FG-IR-19-144>.

## 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 6.0.6.



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

---

This section contains the following topics:

- [Downgrading to previous firmware versions on page 9](#)
- [Firmware image checksums on page 9](#)
- [FortiManager VM firmware on page 9](#)
- [SNMP MIB files on page 11](#)

## Downgrading to previous firmware versions

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

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

## Firmware image checksums

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

## FortiManager VM firmware

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

## Aliyun

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

## Amazon Web Services

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

## Citrix XenServer and Open Source XenServer

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

## Google GCP

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

## Linux KVM

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

## Microsoft Azure

The files for Microsoft Azure have AZURE in the 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 6.0.6 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.0.6 support on page 12](#)
- [Feature support on page 15](#)
- [Language support on page 15](#)
- [Supported models on page 16](#)

## FortiManager 6.0.6 support

The following table lists 6.0.6 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Edge 40 Due to limitation on Edge, it may not completely render a page with a large set of policies or objects.</li><li>• Mozilla Firefox version 67</li><li>• Google Chrome version 75</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 6.0.0 to 6.0.6</li><li>• 5.6.5 to 5.6.10</li><li>• 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 <a href="#">FortiOS 5.6.4 compatibility issues on page 25</a>.</li><li>• 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 <a href="#">FortiOS 5.6.3 compatibility issues on page 25</a>.</li><li>• 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 <a href="#">FortiOS 5.6.0 and 5.6.1 compatibility issues on page 26</a>.</li><li>• 5.4.10 to 5.4.12 FortiManager 5.4.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10, with some minor interoperability issues. For information, see <a href="#">FortiOS 5.4.10 compatibility issues on page 26</a>.</li><li>• 5.4.9</li></ul>

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 26](#).

- 5.4.1 to 5.4.8
- 5.2.8 to 5.2.14

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 27](#).

- 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 27](#).

- 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 27](#).

- 5.2.1 to 5.2.5

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 27](#).

- 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 28](#).

#### **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 5.5
- 4.0 to 4.3

#### **FortiCache**

- 4.2.9
- 4.2.6
- 4.1.2
- 4.0.0 to 4.0.4

#### **FortiClient**

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

#### **FortiMail**

- 5.4.9
- 5.3.13
- 5.2.10
- 5.1.7
- 5.0.10

<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>• 2.5.0 to 2.5.2</li> <li>• 2.4.0 and 2.4.1</li> <li>• 2.3.2 and 2.3.3</li> <li>• 2.2.2</li> <li>• 2.1.3</li> <li>• 1.4.0 and later</li> <li>• 1.3.0</li> <li>• 1.2.0 and later</li> </ul>
<b>FortiSwitch ATCA</b>	<ul style="list-style-type: none"> <li>• 5.2.3</li> <li>• 5.0.0 and later</li> <li>• 4.3.0 and later</li> <li>• 4.2.0 and later</li> </ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"> <li>• 6.0.4</li> <li>• 5.9.1</li> <li>• 5.8.6</li> <li>• 5.8.3</li> <li>• 5.8.1</li> <li>• 5.8.0</li> <li>• 5.7.2</li> <li>• 5.6.1</li> <li>• 5.5.6</li> <li>• 5.4.1</li> <li>• 5.3.9</li> <li>• 5.2.4</li> <li>• 5.1.4</li> <li>• 5.0.6</li> </ul>
<b>FortiDDoS</b>	<ul style="list-style-type: none"> <li>• 4.5.0</li> <li>• 4.4.1</li> <li>• 4.2.3</li> <li>• 4.1.11</li> </ul> <p>Limited support. For more information, see <a href="#">Feature support on page 15</a>.</p>
<b>Virtualization</b>	<ul style="list-style-type: none"> <li>• Amazon Web Service AMI, Amazon EC2, Amazon EBS</li> <li>• Citrix XenServer 7.2</li> <li>• Linux KVM Redhat 7.1</li> <li>• Microsoft Azure</li> <li>• Microsoft Hyper-V Server 2012 and 2016</li> <li>• OpenSource XenServer 4.2.5</li> <li>• VMware ESXi versions 5.0, 5.5, 6.0, 6.5 and 6.7</li> </ul>



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 6.0.6.



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

This section contains the following topics:

- [FortiGate models on page 17](#)
- [FortiCarrier models on page 19](#)
- [FortiDDoS models on page 20](#)
- [FortiAnalyzer models on page 20](#)
- [FortiMail models on page 21](#)
- [FortiSandbox models on page 22](#)
- [FortiSwitch ATCA models on page 22](#)
- [FortiSwitch models on page 22](#)
- [FortiWeb models on page 23](#)
- [FortiCache models on page 24](#)
- [FortiProxy models on page 24](#)
- [FortiAuthenticator models on page 24](#)



## FortiGate models

Model	Firmware Version
<p><b>FortiGate:</b> FGT-30E-3G4G-GBL, FGT-3400E, FGT-3401E, FGT-3600E, FGT-3601E, FGT-400E, FGT-401E, FGT-600E, FGT-601E, FGT-60E-DSL, FGT-60E-DSLJ, FWF-60E-DSL, FWF-60E-DSLJ, FGT-VM64-RAXONDEMAND, FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-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><b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> 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</p> <p><b>FortiGate DC:</b> 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><b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> 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><b>FortiGate VM:</b> 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><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	6.0
<p><b>FortiGate:</b> 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><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E</p>	5.6

Model	Firmware Version
<b>FortiGate DC:</b> 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 <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> 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 <b>FortiGate VM:</b> 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 <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	
<b>FortiGate:</b> 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 <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 6000 Series:</b> FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 Series:</b> 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 <b>FortiGate DC:</b> 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 <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> 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 <b>FortiGate VM:</b> 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 <b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
<b>FortiGate:</b> 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 <b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C <b>FortiGate DC:</b> 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 <b>FortiGate Low Encryption:</b> 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 <b>FortiWiFi:</b> 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 <b>FortiGate Rugged:</b> FGR-60D, FGR-100C <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN <b>FortiSwitch:</b> FS-5203B, FCT-5902D	5.2

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC <b>FortiCarrier-VM:</b> 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
<b>FortiCarrier:</b> 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 <b>FortiCarrier 6000 Series:</b> FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E	5.6

Model	Firmware Version
<b>FortiCarrier-DC:</b> 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 <b>FortiCarrier-VM:</b> 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	
<b>FortiCarrier:</b> 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 <b>FortiCarrier 6000 Series:</b> FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E <b>FortiCarrier-DC:</b> 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 <b>FortiCarrier-VM:</b> 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
<b>FortiCarrier:</b> 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 <b>FortiCarrier-DC:</b> 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 <b>FortiCarrier-VM:</b> 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
<b>FortiDDoS:</b> 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
<b>FortiAnalyzer:</b> 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
<b>FortiAnalyzer VM:</b> 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
<b>FortiAnalyzer:</b> 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.  <b>FortiAnalyzer VM:</b> 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
<b>FortiAnalyzer:</b> 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  <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> 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  <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.0

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E  <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4.5
<b>FortiMail:</b> 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  <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.12
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B  <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.10
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B  <b>FortiMail VM:</b> FE-VM64	5.1.7
<b>FortiMail:</b> 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  <b>FortiMail VM:</b> FE-VM64	5.0.10

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	2.5.2
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.1 2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.0 2.1.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.3 1.4.2
<b>FortiSandbox:</b> 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
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

## FortiSwitch models

Model	Firmware Version
<b>FortiSwitch:</b> 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
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVR	6.0.1
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> 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
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> 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
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
<b>FortiWeb:</b> 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 <b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1

Model	Firmware Version
<b>FortiWeb:</b> 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  <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
<b>FortiWeb:</b> 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  <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E <b>FortiCache VM:</b> FCH-VM64	4.0

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E <b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	1.0

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	4.3 and 5.0-5.3
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	4.0-4.2



# Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.0.6. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 5.6	<a href="#">FortiOS 5.6.4 compatibility issues on page 25</a>
	<a href="#">FortiOS 5.6.3 compatibility issues on page 25</a>
	<a href="#">FortiOS 5.6.0 and 5.6.1 compatibility issues on page 26</a>
FortiOS 5.4	<a href="#">FortiOS 5.4.10 compatibility issues on page 26</a>
	<a href="#">FortiOS 5.4.9 compatibility issues on page 26</a>
FortiOS 5.2	<a href="#">FortiOS 5.2.10 compatibility issues on page 27</a>
	<a href="#">FortiOS 5.2.7 compatibility issues on page 27</a>
	<a href="#">FortiOS 5.2.6 compatibility issues on page 27</a>
	<a href="#">FortiOS 5.2.1 compatibility issues on page 27</a>
	<a href="#">FortiOS 5.2.0 compatibility issues on page 28</a>

## 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"><li>• <code>rsso-endpoint-block-attribute</code>, <code>rsso-endpoint-block-attribute</code>, or <code>sso-attribute</code> for RADIUS users.</li><li>• <code>sdn</code> and its <code>filter</code> attributes for firewall address objects.</li><li>• <code>azure</code> SDN connector type.</li><li>• <code>ca-cert</code> attribute for LDAP users.</li></ul>

## 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"><li><code>system replacemsg mail "email-decompress-limit"</code></li><li><code>system replacemsg mail "smtp-decompress-limit"</code></li><li><code>system replacemsg nntp "email-decompress-limit"</code></li></ul>

## 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 6.0.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
538934	When configuration file is large, installing to device may delete configuration on FortiGate.
540657	There is an ordering issue on admin users where multiple wildcard users are configured on the same server.
558445	For SD-WAN Interface Member, the Per-Device Mapping option is not available on 6.0.5 GUI.
558482	User may not be able to create LDAP users on FortiManager 6.0.5.
559521	The fgdupd daemon may keep crashing.
560332	Add 'move' option in CLI to change admin setting order.
561709	Login may not work for XML API.

## Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Vulnerability
FortiManager 6.0.6 is no longer vulnerable to the issue described in the following link - <a href="https://fortiguard.com/psirt/FG-IR-19-144">https://fortiguard.com/psirt/FG-IR-19-144</a> .

# Known Issues

The following issues have been identified in 6.0.6. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
540347	FortiManager has no option available to configure VLAN IDs under VLAN Pooling.
547361	AP Profile in AP Manager may offer redundant options for specific AP models which can lead to fail installation.
548329	WiFi Profiles SSID DHCP Server Toolbar is hidden if System Settings is set to None in an Admin Profile.
549001	Installation error after changing inspection mode from Proxy to Flow.
549113	In case FortiGate is in NGFW policy-based mode, URL or Application control profiles should not be visible on FortiManager.
549615	Users should be able to set the login-timestamp from CLI script.
549638	MAC address Access control list entries under DHCP server are duplicated when editing one of the entries.
549674	FortiManager is unable to create SD-WAN Template in Central Management Mode if System Settings is set to None in an Admin Profile.
550513	User cannot change IPSec Phase1 on an existing IPSec Phase2 interface.
551072	Assignment of object-tag from 5.6 Global ADOM to 6.0 ADOM should not fail.
551077	FortiManager may not be able to import policies from FortiGate SLBC.
551237	User without Super User Profile is unable to manage Tags from Tag Management.
551701	FortiManager is unable to Set OSPF Interface Network Type as P2MP.
552110	FortiManager cannot show where used for FortiSwitch Security Policy.
552144	Install copy fails when setting captive portal user group for FortiSwitch's VLAN.
553270	Imported SSIDs cannot be selected within AP Profile until the SSIDs have been edited.
553276	When SSID is in bridge mode, external link to captive portal and CMCC Radius Secret are missing on AP Manager's SSID page.
553704	Find Duplicate Objects may get stuck loading.
553860	FortiManager should have public IP for remote-gw under IPSec Phase1 interface.
553926	Split-tunneling information may not be retrieved completely for managed AP.
553933	User should be able to configure split-tunneling related information on AP profile and managed AP pages.

Bug ID	Description
553985	FortiManager incorrectly sets security-external-web when external authentication is selected.
553991	When redirect after captive portal is set, verification may fail on security-redirect-url due to missing http:// prefix.
554001	Configuration may modify FQDN addresses after FortiManager and FortiGate are both upgrade to version 6.0.5.
554092	FortiManager is unable to use interface member of a zone as Source Interface filter for VIP object.
554154	FortiManager is unable to select multiple FortiExtender units for upgrade of firmware from Extender tab.
554491	Device Manager generates incorrect configuration for Filter MAC Addresses on SSID that causes installation to fail.
554500	Device Manager's SSID page cannot save links to authentication portal and redirect after captive capital.
554761	FortiManager is missing to generate software switch related configurations for Quarantine Host for SSID.
554778	AP Manager may not be able to import AP Profile for FAP-421E/423E/S421E/S423E.
554882	7000 series HA members may show up as unregistered after failover.
554901	EU country ID is available on FortiManager, but the ID is not part of latest geographic database.
554946	Sub-admin clicks View on where Used may lead to disappearance of dual panel.
555159	After deleting an SSID from Device Manager, AP Manager still shows the SSID.
555257	Search box for SSID selection within AP Profile may not work well.
555730	Install may fail if zone member is used in a Multicast policy.
556192	Resetting hitcount in ADOM 5.4 fails.
556192	FortiManager may fail to run execute fips kat all and diagnose system fips kat-error commands.
556368	FortiManager may show Device objects from another ADOM.

# Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

## FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Windows)	✓		✓	
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			



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

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

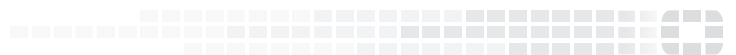


# Change Log

Date	Change Description
2019-07-18	Initial release of 6.0.6.
2019-07-24	Updated the <i>Product Integration</i> section.
2019-08-06	Added FMG-VM64-AWS-OnDemand to <i>Supported Models</i> .
2019-09-13	Updated the <i>Upgrade Information</i> section to remove an old sentence from the introduction.
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.