FortiManager - Release Notes

Version 6.0.7

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

December 14, 2020
FortiManager 6.0.7 Release Notes
02-607-592664-20201214

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-11-13	Initial release of 6.0.7.
2019-11-19	Updated Special Notices on page 7.
2019-11-22	Updated Product Integration and Support on page 13.
2019-11-27	Updated Resolved Issues on page 32.
2019-12-12	Updated to add support for FortiOS 5.6.12 and 6.0.8. Also added FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues on page 28 and FortiManager 6.0.7 and FortiOS 5.6.12 compatibility issues on page 28.
2020-01-22	Updated Resolved Issues on page 32.
2020-11-02	Updated Known Issues on page 41.
2020-12-14	Updated Resolved Issues on page 32.

FortiManager 6.0.7 Release

This document provides information about FortiManager version 6.0.7 build 0405.

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

This section includes the following topics:

Supported models

FortiManager version 6.0.7 supports the following models:

FortiManager	FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-300F, FMG-400E, FMG-1000D, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3900E, FMG-3700F, FMG-4000D, FMG-4000E, and FMG-MFGD.
FortiManager VM	FMG-VM64, FMG-VM64-ALI, FMG-VM64-AWS, FMG-VM64-AWS-OnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.7.

Multicast policies with zones or zone members

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

Managing FortiGate with VDOMs that use Global 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 t1sv1
end
```

Upgrade Information

You can upgrade FortiManager 5.6.0 or later directly to 6.0.7.

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

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 6.0.7 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 6.0.7 support

This section identifies FortiManager 6.0.7 product integration and support information:

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

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

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

Web browsers

This section lists FortiManager 6.0.7 product integration and support for web browsers:

- Microsoft Edge 40
  Due to limitation on Edge, the browser may not completely render a page with a large set of policies or objects.
- Mozilla Firefox version 70
- Google Chrome version 78

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

FortiOS/FortiOS Carrier

This section lists FortiManager 6.0.7 product integration and support for FortiOS/FortiOS Carrier:

FortiOS or FortiOS Carrier		Compatibility Issues
6.0	6.0.0 to 6.0.8	FortiManager 6.0.7 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.8, with some minor interoperability issues. For information, see FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues on page 28.
5.6	5.6.5 to 5.6.12	FortiManager 6.0.7 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.12, with some minor interoperability issues. For information, see FortiManager 6.0.7 and FortiOS 5.6.12 compatibility issues on page 28.
	5.6.4	FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 29.
	5.6.2 to 5.6.3	FortiManager 5.6.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.3, with some minor interoperability issues. For information, see FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 29.
	5.6.0 to 5.6.1	FortiManager 5.6.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 29.
5.4	5.4.11 to 5.4.12	
	5.4.10	FortiManager 5.4.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10, with some minor interoperability issues. For information, see FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 29.
	5.4.9	FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9, with some minor interoperability issues. For information, see FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 30.
	5.4.1 to 5.4.8	
5.2	5.2.9 to 5.2.15	
	5.2.8 to 5.2.10	FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see FortiManager 5.4.1 and FortiOS 5.2.10 compatibility issues on page 30.

FortiOS or FortiOS Carrier	Compatibility Issues
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 FortiManager 5.2.6 and FortiOS 5.2.7 compatibility issues on page 30.
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 FortiManager 5.2.4 and FortiOS 5.2.6 compatibility issues on page 31.
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 FortiManager 5.2.1 and FortiOS 5.2.1 compatibility issues on page 31.
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 FortiManager 5.2.1 and FortiOS 5.2.0 compatibility issues on page 31.

FortiAnalyzer

This section lists FortiManager 6.0.7 product integration and support for FortiAnalyzer:

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

FortiAuthenticator

This section lists FortiManager 6.0.7 product integration and support for FortiAuthenticator:

- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiManager 6.0.7 product integration and support for FortiCache:

- 4.2.9
- 4.2.6
- 4.1.6
- 4.0.0 to 4.0.4

FortiClient

This section lists FortiManager 6.0.7 product integration and support for FortiClient:

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

FortiMail

This section lists FortiManager 6.0.7 product integration and support for FortiMail:

- 6.0.7
- 5.4.10
- 5.3.13

FortiSandbox

This section lists FortiManager 6.0.7 product integration and support for FortiSandbox:

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

FortiSwitch ATCA

This section lists FortiManager 6.0.7 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiWeb

This section lists FortiManager 6.0.7 product integration and support for FortiWeb:

- 6.0.5
- 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

FortiDDoS

This section lists FortiManager 6.0.7 product integration and support for FortiDDoS:

- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 17.

Virtualization

This section lists FortiManager 6.0.7 product integration and support for virtualization:

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

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.0.7.

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

This section contains the following topics:

FortiGate models

Model	Firmware Version
FortiGate: FGT-30E-3G4G-GBL, FGT-60F, FGT-61F, FGT-3400E, FGT-3401E, FGT-3600E, FGT-3601E, FGT-400E, FGT-401E, FGT-600E, FGT-601E, FGT-60E-DSL, FGT-60E-DSLJ, FWF-60E-DSL, FWF-60E-DSLJ, FGT-VM64-RAXONDEMAND, FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101F, FG-101E, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3300E, FG-3301E, FG-3815D, FG-3960E, FG-3980E, FG-6000F **FortiGate 5000 Series:** FG-5001D, FG-5001E, FG-5001E1 **FortiGate 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **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:** FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Hardware Low Encryption:** FG-100D-LENC, FG-600C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP,VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

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

Model	Firmware Version
FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **Note:** All license-based LENC is supported based on the FortiGate support list. **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

FortiCarrier models

Model	Firmware Version
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E	6.0

Model	Firmware Version
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	
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E **FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E **FortiCarrier-DC:** FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FCR-3810D-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E **FortiCarrier 6000 Series:** FG-6300F, FG-6301F, FG-6500F, FG-6501F **FortiCarrier 7000 Series:** FG-7030E, FG-7040E, FG-7060E **FortiCarrier-DC:** FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FCR-3810D-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, , FGT-3810A, FGT-3810D, FGT-3950B, FGT-3951B, FGT-5100B, FGT-5100C, FGT-5001D, FGT-5101C, FS-5203B, FT-5902D **FortiCarrier-DC:** FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3810A-DC, FGT-3810D-DC, FGT-3950B-DC, FGT-3951B-DC **FortiCarrier-VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-Xen	5.2

FortiDDoS models

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

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F, FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FE-VM64	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4.5

Model	Firmware Version
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-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1

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

FortiCache models

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

FortiProxy models

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

FortiAuthenticator models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.0.7. Compatibility issues have been identified for the following FortiOS releases:

FortiManager 6.0.7 and FortiOS 6.0.8 compatibility issues

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

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

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

FortiManager 6.0.7 and FortiOS 5.6.12 compatibility issues

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

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

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

FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues

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

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

FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues

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

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

FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues

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

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

FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues

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

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

FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues

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

Bug ID	Description

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

FortiManager 5.4.1 and FortiOS 5.2.10 compatibility issues

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

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

FortiManager 5.2.6 and FortiOS 5.2.7 compatibility issues

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

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

FortiManager 5.2.4 and FortiOS 5.2.6 compatibility issues

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

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

FortiManager 5.2.1 and FortiOS 5.2.1 compatibility issues

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

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

FortiManager 5.2.1 and FortiOS 5.2.0 compatibility issues

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

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

Resolved Issues

The following issues have been fixed in 6.0.7. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
547361	AP Profile in *AP Manager* offers redundant options for specific AP models, which can lead to failed installation.
548329	WiFi profiles *SSID DHCP Server* toolbar is hidden if *System Settings* is set to *None* in an *Admin Profile*.
564936	*AP Manager* does not allow *Security Exempt List* when *Portal Type* does not contain *Authentication*.
570936	*AP Manager* is pushing incorrect syntax for FAPU24JEV `wtp-profile`, causing installation failure.
570937	*AP Manager* should allow individual configure LAN ports.
571722	*AP Manager* should hide *WIDE* profiles if they cannot be used in certain modes.
572544	When creating a managed AP, FortiManager should properly save the *Name* and *AP Profile* fields, and it should not accept FAP's serial number with lowercase letters.

Device Manager

Bug ID	Description
483821	Two default values are incorrect in FMG database ("wad-worker-count" and "socket-size").
508020	Web & IPS conflict information is not visible while importing policy package.
514299	If the address objects have the same configuration, FortiManager should not add dynamic mapping for the same identical objects during the import.
528965	FortiManager needs to support four modes for SD-WAN service's output interface: Auto, Manual, Priority, and SLA Assign.
536078	Device Manager may not be able to display more than 50 VDOMs.

Bug ID	Description
539928	Objects used in SD-WAN rules show as not in use in address list.
542961	FortiManager is unable to change FGT's administrator password from *CLI Configurations*.
544597	VLAN interface is not available for EMAC VLAN on *Device Manager* > *System* > *Interfaces*.
544880	FortiManager should not allow adding loopback interface to a zone.
547528	FortiManager may be slow to view large device revisions on Firefox.
549638	MAC address *Access Control List* entries under *DHCP server* get duplicated when editing an entry.
549674	Users should be able to create a new SD-WAN template even if *System Settings* is set to *None* in the *Admin Profile*.
550237	Read-only admin should not be allowed to add detected devices.
550239	System SNMP user is missing the value `aes256cisco` for the field `priv-proto`.
550513	Users should be able to change *IPSec Phase1* within *IPSec Phase2* settings.
551077	FortiManager may not be able to import policies from FortiGate SLBC.
551701	FortiManager is unable to set *OSPF Interface Network Type* as *P2MP*.
553491	Enabling or disabling multiple interfaces should be allowed in *Device Manager*.
554154	FortiManager should be able to select multiple FortiExtender units for upgrade from the *Extender* tab.
555394	Policy route's columns for *Source* and *Destination* show port information instead of subnet addresses.
555635	Certificate is not visible on GUI after restoring the configuration, which was exported from FortiManager.
564182	FortiManager should always respond with *invalid VDOM name* when accessing FortiManager with incorrect hyperlinks.
564625	Re-importing a policy package may result in changing policy package status to *modified*.
568626	FortiManager can only modify the order of DNS forwarder only if the IP addresses are in quotes ("") and when the IP addresses are not separated by a comma.
569468	Firmware version value is incorrect in device list after upgrade.
569900	FortiManager may hang when adding devices from root ADOM within the unregistered device list.
570109	FortiManager cannot configure `fail-detect-option` in interface's advanced options.
571581	FortiManager may not show zone changes in policy package diff.
574988	CLI only object cannot create router BGP `AS-path` list and `community` list, and prompts the error "*entry does not exist*".
575823	FortiManager should not allow user to delete extra proposals when `SUITE-BPRF` is enabled.

Bug ID	Description
576320	Policy status of all devices used in *VPN Manager* is changing to *modified* after deleting some unrelated devices.
576565	Creating VXLAN may gradually take more time.
577937	Editing *Restrict Access* in VLAN interface settings removes interface from zone.
579648	FortiManager `fgfmsd` crashes when a FortiGate with 6.2.1 firmware sends registration request to FMG
581812	Sorting Extenders by *Device Name* does not work.
583467	FortiManager cannot edit the MTU parameter on an interface in *Device Manager*.
586550	*Device Manager* does not detect newly joined Telemetry group on FortiGate.

FortiClient Manager

Bug ID	Description
548572	FortiManager shows unclear message in FortiClient Profile with *Response with errors* instead of *Device groups cannot be empty*.

FortiSwitch Manager

Bug ID	Description
586557	User group for FortiSwitch Security Policy should not be removed once Workflow session is created and submitted.

Global ADOM

Bug ID	Description
509665	Global v5.2 assigned to ADOM v5.4 and `webfilterftgd-local-rating` might set to wrong category.
551072	Assignment of `object-tag` from 5.6 Global ADOM to 6.0 ADOM should not fail.
580600	FortiManager may not respond when assigning Global Objects.
587511	`gSSO_Guest_User` should work the same as predefined `SSO_Guest_User`.

Others

Bug ID	Description
529770	Policy package integrity check provides no clarification on intended database changes.
538915	Firmware version is not displayed on *NOC - SOC* page.
540034	There may be repetitive `fmgd` crashes in FortiManager's crashlog.
541880	The `dmserver` daemon may crash when installing to multiple devices and CPU usage reaches 100%.
551937	FortiManager should only allow the browser to save and paste credentials at the logon prompt only.
552222	When running `cdbcheckpolicy-packages`, FortiManager prompts `central fap object not found` errors.
561008	Second IP in central management removed by master FortiManager on re-connection.
561279	The `newcli` process may crash when running the `diagnose cdb upgrade check +all` command.
561946	Upgrading FortiManager may fail due to incorrect limit for user `adgrp`.
574826	FortiManager port negotiation switches to 100 half-duplex mode after a reboot.
576558	Delete invalid orphan entries" errors found by `diag cdb upgrade check +all` are not fixed.
580832	FortiManager may show disk unused under LVM.
586241	When locking an ADOM and deleting it with workflow enabled, the workflow stays with status changes to `(null)`.
586991	`Logver` field is missing when FortiAnalyzer is enabled, affecting report related features.
589805	Installing policy package via JSON API with missing interface in zone definition deletes zone and corresponding firewall policies on FortiGate.

Policy and Objects

Bug ID	Description
571235	Enabling policy hit count locks ADOM and provokes GUI slowness.
494367	Users cannot search address in policy where the address is a part of a nested group.
521904	Policy and Object's folders do not reflect policy package status.
528881	Users are not able to remove all FSSO objects from selected list that has a large number of entries.
530717	Under *Policy & Objects* > *Policy Package* > *right click* > *add address in policy*, the page is stuck on loading with Microsoft Edge.

Bug ID	Description
531585	A proxy policy's source address field should display all address objects in the search list despite the interface binding defined for the addresses.
534220	Users cannot add entries for per-device mapping with existing VIP group when a VIP binds to a port that is part of SD-WAN.
540045	Search is not persistent after creating or cloning a new object.
544404	A remote user approves a session, session list shows zero session.
545484	ADOM unable to create per-device mappings for local certificate.
546334	Dynamic interface is not visible in policies until web page refreshes.
547052	FortiManager GUI should not allow creating security profiles without any SSL/SSH inspection profile defined.
547055	FortiManager GUI should prevent CA certificate to be changed on built-in SSL/SSH inspection profiles.
549504	Wildcard remote admin cannot run schedule install.
553704	FortiManager may be stuck at loading when using the *Find Duplicate Objects* function.
554092	FortiManager is unable to use interface member of a zone as *Source Interface* filter for VIP object.
554901	EU country ID is available in FortiManager, but the ID is not part of the latest geographical database.
558408	When user installs a policy package to more than 20 devices, some of the task for this installation may hang and `dmserver` crashes.
559009	FortiManager should allow users to select SD-WAN interface on IPv6 policy.
559104	Incorrect ADOM name may be displayed in *Where Used*.
559112	FortiManager may not be able to edit a proxy policy that was inserted above or below.
559751	Duplicated `##seq` appears in policy packages, and they cannot be fixed with `diagnose` command.
560694	If *hitcount* is updated while ADOM is locked, policies matched by traffic are highlighted as modified.
562160	FortiManager should be able to create dynamic mapping for `object-tagging` category.
563169	When user changes *webfilter* settings, *username* in last modified column should always be updated.
563629	Clicking on "+" function should allow users to add Wildcard FQDN objects.
564203	Policy package cannot export to Microsoft Excel when policy is more than 20,000 policies.
564405	FortiManager may not be able to modify `Tag-Format` field under `Anti-spam` profile.
566599	IPS Rate Based Signatures may be applied in the wrong order.
567514	Multiple policies may be deleted by accident, if they are selected on the background from the

Bug ID	Description
	previous filtered result.
569551	FortiManager should be able to save quotas within webfilter profile.
576267	SSL/SSH inspection profile change does not change all related policy package statuses to *modified*.
579844	When user logs in with remote Radius authentication with assigned VDOM and access profile, FortiManager may not show the installation target devices.
580676	FortiManager may not delete and change a policy, and it affects another policy packages.
581481	FortiManager should allow adding a custom Application Control signature with the same attack ID as an existing one.
582685	Web Filter Profiles with URL filter lists may take a long time to load.
588548	Under workspace, addresses may be removed from a firewall policy when merging duplicated addresses.
588869	Re-installing policy package on FortiGate with multiple VDOMs may wipe out configuration on a VDOM that belongs to a different policy package.
590179	Drop-down cannot populate OCI Certificate for OCI Fabric Connector.
581495	Interface Validation should prompt only once per unmapped interface.

Revision History

Bug ID	Description
524611	FortiManager tries to set `profile-type` group even if there is no `profile-group` specified causing installation to fail.
539994	Installing to FortiGate fails when `wildcard-fqdn` address is used in SSL profile.
548027	After FortiGate upgrades, verification may fail on `set nat enabled` if `set central-nat enable` is configured.
549001	Installation may fail after changed inspection mode from *Proxy* to *Flow*.
555796	Installing policy on 6K series FortiGate may remove the interface setting `set forward-error-correction rs-fec`.
556985	FortiManager prompts unclear message when device configuration file is not found.
560689	Auto-Update revision is missing `set stp-bpdu-guard enabled`.
565436	After FortiManager processed many auto-update requests, FortiManager may not be able to create a new revision.
565636	FortiManager may prompt verification error on Global ADOM's gall address.
565970	One specific unused `adgrp` is getting pushed to FortiGate that does not use by FSSO anywhere.

Bug ID	Description
566138	FortiManager may not correctly install Application Control configurations.
566390	Policy installation may fail due to FortiGuard certifications.
567770	Install custom internet service to FortiGate fails when *None* is selected for *Master Service ID*.
577964	FortiManager should install imported CA certificates to managed FortiGate device.
586992	FortiManager does not install broadcast-forward enabled on *Virtual Switch* to managed FortiGate.
589858	The BGP `scan-time` value of `0` can be set on FortiGate, but FortiManager resets it to default by `unset scan-time` on the next policy push.

Script

Bug ID	Description
519495	Running a script always returns the error, *the script is not eligible*, even though the actual error may be different.
530838	When viewing script results, there are several new lines in unexpected places.
550502	Installing DDoS policies via a CLI script may fail.
555175	User may mistakenly configures FortiManager to run script against a group of targets when targeting a single device.
559844	FortiManager may not be able to set `client-idle-timeout` to `0` in device database.
564937	FortiManager allows users not to set device type when creating a user device resulting in install failure.
565053	FortiManager cannot unset *Security Exempt List*.
577463	Script scheduling should not be affected by the order of configuration.
586817	Script may not be getting applied completely on policy package.
587015	When user tries to set signature with non escaped quotes from script, the signature becomes separate strings, and the installed string may not be what it is expected.

Services

Bug ID	Description
539196	FortiManager should not show FortiGuard subscription status *Expired*, if a trial license is expired.
543404	FortiManager should display log on *FortiGuard Distribution Server Download Log*.

Bug ID	Description
551096	FortiMeter Program License is expired and it is displayed as *FREZ* even though FortiGate Traffic is still passing.
557355	FortiManager may not connect to FortiGuard when `fds-ssl-protocol` is set to either `tlsv1.1` or `tlsv1.2`.
562021	FortiManager should support HTTPS proxy.

System Settings

Bug ID	Description
498133	0150: Syslog is not sent using IPv6.
529051	Map to Policy Interface & Scan out going connection to Botnet Sites disappears in v6.0.3 when running FortiManager in workflow mode.
537312	Event logs should not have the user from field when an internal process riggers the log.
537338	FortiManager should not reset objects' *Created Time* and *Last Modified* timestamps after upgrading ADOMs.
539137	User may not be able to access to FortiManager using IPv6 address, even if user sets *IPv6 allow access on HTTPS and HTTP*.
548034	System Settings' LDAP may not work with nested directory groups.
562239	Dynamic mappings may be deleted after ADOM upgrade.
563918	FortiManager should prompt more clear error when ADOM upgrade fails.
564400	ADOM upgrade may show the error *firewall ssl-ssh-profile ssl-exempt wildcard-fqdn. detail: table limit*.
576098	Event log may not show the correct username when changing a non policy related object.
579075	LDAP admin user may not be able to access FortiManager when there are many LDAP groups.
580486	Adding ADOM fails with errorCode 102: 'Fail to lock adom Global workspace' when workspace-mode is set to normal.
584749	System Settings may not show the ADOM-VDOM association.
587242	[b349] HA Cluster fails after upgrading to 6.0.6 with peer IP using IPv6.
588884	Event log for merging duplicated objects is missing object name.

VPN Manager

Bug ID	Description
546790	Table row's height too short to display the monitors for multiple phase 2 entries.
553860	Hub-to-Hub IPsec Phase1 interface install uses `remote-gw` as interface IP even though public IP is defined under the *Advance* section.
554857	Policy package does not go out-of-sync after *VPN Manager* is enabled.
556340	*VPN manager > create a new VPN communities* displays *IKE Version* default value as *2* instead of *1*.
563961	Selection menus for *authusrgrp* and *ipv4-split-include* are not working in the gateway configuration for Dial-Up.
571164	*VPN Manager* has problem adding secondary WAN interface from a hub in star community.
574727	*VPN Manager* may not display SSL-VPN settings for some devices.
576308	Policy package exported as CSV contains hit count data only for IPv4, but not for IPv6.
577939	*VPN Manager* may install different PSKs to gateways.

Common Vulnerabilities and Exposures

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

Bug ID	Description
542636	FortiManager is no longer vulnerable to the following CVE-Reference: • CVE-2019-6695
565905	FortiManager is no longer vulnerable to the following CVE Reference: • CVE-2019-1147
565947	FortiManager is no longer vulnerable to the following CVE Reference: • CVE-2019-11478
565967	FortiManager is no longer vulnerable to the following CVE Reference: • CVE-2019-11479

Known Issues

The following issues have been identified in 6.0.7. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
547768	FortiManager should allow easier management of the compliance exempt lists.
580533	0349: Saving configuration with incorrect IP/mask format does not display an error for inner configurations.
586809	FortiManager incorrectly counts VDOM license for FortiGate 7000 series.
594709	Device Manager may not be able to generate Policy Package Diff result.

Others

Bug ID	Description
552085	FortiManager live migration fails with Microsoft Hyper-V, and it is not accessible via GUI and SSH.
565515	User may not be able to create a new SNMP host under *System Templates*. Workaround: Please add a new SNMP host for System Templates under *CLI Configurations* within *Device Manager*.
574731	0349/1121: Some hardware specific SNMP traps are missing from the device SNMP settings and the system provisioning templates.
581140	The SNMP, `FmDeviceEntPolicyPackageState`, always returns (`-1`), which indicates never installed, regardless of the actual policy package status.

Policy and Objects

Bug ID	Description
491813	FortiManager should group IPS Sensor entries with same filters as one rule.
505887	Internet Service should separate into source and destination.
545759	*From* or *To* column filter displays unmapped interfaces in the drop-down list.
548573	FortiManager changes UUIDs of existing objects after policy install.
569576	1121: Web rating override category change is not reflected in GUI.
577199	Importing policy package does not add interfaces in dynamic mappings for zone, if the zone mapping is empty.
577660	Despite table limits on firewall `central-nat` of `300k-max` and 30K-per VDOMs, FortiManager still shows *10k limit reached* error.
577884	Deleting an unused object should not change policy package status.
578004	The policy interface colors are different between *Device Manager* and *Policy & Objects*.
580484	Signature, *Apache.Optionsbleed.Scanner*, cannot be selected as IPS Signature, but only as *Rate based Signature*.
581825	In workflow mode, changes to the SSL VPN portals do not trigger *Modified* status on the policy package.
585021	Adding or modifying rate-based signatures on IPS profile resets all rate-based signatures to default settings.
585681	Advanced search may not work for application control filter overrides.
589771	Policy package installation fails when a firewall policy contains a VIP group mapped to a zone interface.

Revision History

Bug ID	Description
543507	Install fails for newly defined transparent VDOM's management IP.
578231	FortiManager tries to push `casi-profile` on a deny policy.
584118	Router `access-list` rule's default value is mismatched, causing installation failure.
586275	Policy package diff does not show user or admin details.
591818	Install fails with *No response from remote* when making `addrgrp` changes.
592062	Custom Internet service created on FortiManager systematically fails to be installed on target FortiGate.

Script

Bug ID	Description
578679	Running a script on a device may fail when script filter has been set for "some version" or "some platform".

Services

Bug ID	Description
520875	FortiManager should keep the same FortiGate On-Demand contract as FortiGuard.

System Settings

Bug ID	Description
571181	An admin user with read-write system permissions and restricted to one ADOM can change their permission to *All ADOMs*.
588852	Idle time is constantly reset for inactive users.
592332	FortiManager ADOM incorrectly handles object names as not case sensitive.

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
```