

FortiManager - Release Notes

Version 5.6.8

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 COOKBOOK

<http://cookbook.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: techdocs@fortinet.com



August 06, 2019

FortiManager 5.6.8 Release Notes

02-568-535963-20190806

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
Minimum screen resolution	6
Special Notices	7
Recreate Guest List for Guest user group	7
FortiAP Manager per-device management option	7
Traffic Shaping Policies	7
WebSocket Implementation	7
Virtual Wire Pair Support after Upgrade to 5.6.2 or Later	7
FortiGate VM 16/32/UL license support	8
Hyper-V FortiManager-VM running on an AMD CPU	8
IPsec connection to FortiOS for logging	8
VM License (VM-10K-UG) Support	8
System Configuration or VM License is Lost after Upgrade	8
FortiOS 5.4.0 Support	9
Local in-policy after upgrade	9
ADOM for FortiGate 4.3 Devices	9
SSLv3 on FortiManager-VM64-AWS	9
Port 8443 reserved	9
Upgrade Information	10
Upgrading to FortiManager 5.6.8	10
Upgrading from 5.2.x	10
Downgrading to previous firmware versions	11
FortiManager VM firmware	11
Firmware image checksums	12
SNMP MIB files	12
Product Integration and Support	13
FortiManager 5.6.8 support	13
Feature support	16
Language support	17
Supported models	18
Compatibility with FortiOS Versions	25
Compatibility issues with FortiOS 5.6.6	25
Compatibility issues with FortiOS 5.6.5	25
Compatibility issues with FortiOS 5.6.3	25
Compatibility issues with FortiOS 5.6.0 and 5.6.1	26
Compatibility issues with FortiOS 5.4.10	26

Compatibility issues with FortiOS 5.4.9	26
Compatibility issues with FortiOS 5.4.8	26
Compatibility issues with FortiOS 5.2.10	27
Compatibility issues with FortiOS 5.2.7	27
Compatibility issues with FortiOS 5.2.6	27
Compatibility issues with FortiOS 5.2.1	28
Compatibility issues with FortiOS 5.2.0	28
Resolved Issues	29
Device Manager	29
Policy and Objects	29
Revision History	30
Services	30
System Settings	30
VPN Manager	31
Others	31
Common Vulnerabilities and Exposures	31
Known Issues	33
AP Manager	33
Others	33
Appendix A - FortiGuard Distribution Servers (FDS)	34
FortiGuard Center update support	34

Change Log

Date	Change Description
2019-01-31	Initial release of 5.6.8.
2019-02-05	Changed description of 526297 in <i>Resolved Issues</i> .
2019-02-06	Changed 526297 to 526287 in <i>Resolved Issues</i> to match description.
2019-02-12	Added 462710 to <i>Known Issues</i> .
2019-03-04	Added 520123 to <i>Resolved Issues</i> .
2019-03-18	Updated <i>Product Integration and Support > Supported Models > FortiGate models</i> for 5.6 and 5.4 to add FortiGate 6000 Series, FortiGate 7000 Series, FG-7060E-8-DC, FortiCarrier 6000 Series, FortiCarrier 7000 Series, and FCR-7060E-8-DC.
2019-03-21	Added support for FortiOS 5.6.8.
2019-08-06	Added support for FortiOS 5.6.9.

Introduction

This document provides the following information for FortiManager 5.6.8 build 1800:

- [Supported models](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Compatibility with FortiOS Versions](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [FortiGuard Distribution Servers \(FDS\)](#)

For more information on upgrading your device, see the FortiManager *Upgrade Guide*.

Supported models

FortiManager version 5.6.8 supports the following models:

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

Minimum screen resolution

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

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.6.8.

Recreate Guest List for Guest user group

After upgrading to FortiManager 5.6.7, recreate the guest list for the *Guest* user group in ADOM Policy Object before installing device settings to FortiGate devices.

FortiAP Manager per-device management option

FortiAP Manager now supports a new per-device AP management option. When this option is enabled, the WiFi settings are managed at each FortiGate device level. The Central WiFi settings of the ADOM are not applied to the per-device managed APs.

Traffic Shaping Policies

Starting from FortiManager 5.6.0, configuration for traffic shaping policies has been moved from individual FortiGate devices (the device database) to the ADOM database Policy Package. For FortiManager units that are upgraded from a previous release, a one-time operation of Importing all traffic shaping policies into the ADOM must be performed (a one-time manual or scripted reconfiguration can also be performed). Otherwise, the FortiManager will delete (purge) all existing traffic shaping policies on the FortiGate when installing the original policy package.

WebSocket Implementation

As of version 5.6.0, WebSocket protocol has been implemented to allow for more efficient communication between the FortiManager and the browser. WebSocket protocol uses the standard TCP 80/443 browser ports, and is transparent to the operator. If your browser is using a proxy to access the FortiManager, ensure there are no limitations or restrictions on the using WebSocket.

Virtual Wire Pair Support after Upgrade to 5.6.2 or Later

FortiManager 5.6.2 or later supports Virtual Wire Pair policies. After you upgrade FortiManager, you should import all policies and objects again from FortiGate units that use Virtual Wire Pair policies. Otherwise, a subsequent install may

delete all policies on FortiGate units that reference a Virtual Wire Pair.

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.

IPsec connection to FortiOS for logging

FortiManager 5.4.2 and later does not support an IPsec connection with FortiOS 5.0/5.2. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiManager. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

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.

System Configuration or VM License is Lost after Upgrade

When upgrading FortiManager from 5.4.0 or 5.4.1 to 5.4.x or 5.6.0, it is imperative to reboot the unit before installing the 5.4.x or 5.6.0 firmware image. Please see the *FortiManager Upgrade Guide* for details about upgrading. Otherwise, FortiManager may lose system configuration or VM license after upgrade. There are two options to recover the FortiManager unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

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.

Local in-policy after upgrade

After upgrading to FortiManager 5.4.1 or later, you must import or reconfigure local in-policy entries. Otherwise, the subsequent install of policy packages to FortiGate will purge the local in-policy entries on FortiGate.

ADOM for FortiGate 4.3 Devices

FortiManager 5.4 and later no longer supports FortiGate 4.3 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.3 to a supported version, retrieve the latest configuration from the devices, and move the devices to an ADOM database with the corresponding version.

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
```

Port 8443 reserved

Port 8443 is reserved for `https-logging` from FortiClient EMS for Chromebooks.

Upgrade Information

Upgrading to FortiManager 5.6.8

You can upgrade FortiManager 5.4.0 or later directly to 5.6.8. If you are upgrading from versions earlier than 5.4.x, you should upgrade to the latest patch version of FortiManager 5.4 first.



When upgrading from FortiManager 5.4 or 5.6.0 to 5.6.1, it is required to run the following CLI for proper rendering of GUI pages:

```
diagnose cdb upgrade force-retry resync-dbcache
```



When upgrading from FMG 5.2, an *Import Policy Package* should be performed on all FortiGates using *Local-In-Policies*. As of FMG 5.4, these are handled in Policies & Objects.



During upgrade from 5.2.4 or earlier, invalid dynamic mappings and duplicate package settings are removed from the ADOM database. Please allow sufficient time for the upgrade to complete.



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

Upgrading from 5.2.x

Starting with FortiManager 5.4.0, you can create a maximum number of Global and ADOM objects for each object category, and the maximum is enforced. The maximum numbers are high and unlikely to be met. The purpose of the maximum is to help avoid excessive database sizes, which can impact performance.

During upgrade from FortiManager 5.2.x to 5.4.x to 5.6.8, objects are preserved, even if the 5.2 ADOM contains more than the maximum number of allowed objects. If you have met the maximum number of allowed objects, you cannot add additional objects after upgrading to FortiManager 5.6.8.

Following are examples of object limits:

- Firewall service custom: 8192 objects
- Firewall service group: 2000 objects

If you have reached the maximum number of allowed objects, you can reduce the number of objects by deleting duplicate or obsolete objects from the ADOM.

You can also reach the maximum number of allowed objects if you have multiple FortiGate/VDOMs in the same ADOM. You can reduce the number of objects by moving the FortiGates/VDOMs into different ADOMs.

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}
```

FortiManager VM firmware

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer 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](#).

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*.

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

FortiManager 5.6.8 support

The following table lists 5.6.8 product integration and support information:

Web Browsers

- Microsoft Internet Explorer version 11 or Edge 40
Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.
 - Mozilla Firefox version 64
 - Google Chrome version 71
- Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier

- 5.6.9
- 5.6.8
- 5.6.7
- 5.6.6
FortiManager 5.6.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.6, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.6.6 on page 25](#).
- 5.6.4 to 5.6.5
FortiManager 5.6.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.5, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.6.5 on page 25](#).
- 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 [Compatibility issues with FortiOS 5.6.3 on page 25](#).
- 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 [Compatibility issues with FortiOS 5.6.0 and 5.6.1 on page 26](#).
- 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 [Compatibility issues with FortiOS 5.4.10 on page 26](#).
- 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 [Compatibility issues with FortiOS 5.4.9 on page 26](#).
- 5.4.1 to 5.4.8
FortiManager 5.4.4 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.4.8 on page 26](#).
- 5.2.8 to 5.2.13
FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.2.10 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 [Compatibility issues with FortiOS 5.2.7 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 [Compatibility issues with FortiOS 5.2.6 on page 27](#).
- 5.2.2 to 5.2.5
- 5.2.1
FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.2.1 on page 28](#).
- 5.2.0
FortiManager 5.2.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues. For information, see [Compatibility issues with FortiOS 5.2.0 on page 28](#).

FortiAnalyzer	<ul style="list-style-type: none">• 5.6.0 and later• 5.4.0 and later• 5.2.0 and later• 5.0.0 and later
FortiCache	<ul style="list-style-type: none">• 4.2.8• 4.1.6• 4.0.0 to 4.0.4
FortiClient	<ul style="list-style-type: none">• 5.6.0 to 5.6.6• 5.4.0 and later• 5.2.0 and later
FortiMail	<ul style="list-style-type: none">• 5.4.7• 5.3.12• 5.2.10• 5.1.7• 5.0.10 <p>Limited support. For more information, see Feature support on page 16.</p>
FortiSandbox	<ul style="list-style-type: none">• 2.5.2• 2.4.1• 2.3.3• 2.2.2• 2.1.2• 1.4.0 and later• 1.3.0• 1.2.0 and 1.2.3
FortiSwitch	<ul style="list-style-type: none">• 5.2.5
FortiWeb	<ul style="list-style-type: none">• 5.9.1• 5.8.6• 5.8.3• 5.8.1• 5.8.0• 5.7.2• 5.6.1• 5.5.6• 5.4.1• 5.3.9• 5.2.4• 5.1.4• 5.0.6

FortiDDoS	<ul style="list-style-type: none"> • 4.6.0 • 4.5.0 • 4.4.2 • 4.3.2 • 4.2.3 • 4.1.12 <p>Limited support. For more information, see Feature support on page 16.</p>
FortiAuthenticator	<ul style="list-style-type: none"> • 5.2.2
Virtualization	<ul style="list-style-type: none"> • Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 7.2 • Linux KVM Redhat 7.1 • Microsoft Azure • Microsoft Hyper-V Server 2002 and 2016 • OpenSource XenServer 4.2.5 • VMware ESXi versions 5.0, 5.5, 6.0, 6.5, and 6.7



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

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



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

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer			✓	✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓

Platform	Management Features	FortiGuard Update Services	Reports	Logging
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 and import the language translation files into FortiManager by using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information about commands, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.6.8.



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.

FortiGate models

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

Model	Firmware Version
<p>FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-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</p> <p>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate 6000 Series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>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</p> <p>FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC, FG-7060E-8-DC</p> <p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>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</p> <p>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</p> <p>FortiGate Rugged: FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D</p>	5.4

Model	Firmware Version
<p>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</p> <p>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</p> <p>FortiGate DC: FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC</p> <p>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</p> <p>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</p> <p>FortiGate Rugged: FGR-60D, FGR-100C</p> <p>FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p>FortiSwitch: FS-5203B, FCT-5902D</p>	5.2

FortiCarrier Models

Model	Firmware Version
<p>FortiCarrier 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E</p> <p>FortiCarrier DC: FCR-7060E-8-DC</p>	5.6

Model	Firmware Version
<p>FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C</p> <p>FortiCarrier 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E</p> <p>FortiCarrier DC: FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3800D-DC, FCR-3810D-DC, FCR-3815D-DC, FCR-7060E-8-DC</p> <p>FortiCarrier VM: FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM</p>	5.4
<p>FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D</p> <p>FortiCarrier DC: FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC</p> <p>FortiCarrier Low Encryption: FCR-5001A-DW-LENC</p> <p>FortiCarrier VM: FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND</p>	5.2

FortiDDoS models

Model	Firmware Version
<p>FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B</p>	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
<p>FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.</p> <p>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).</p>	5.6
<p>FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.</p> <p>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.</p>	5.4

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B FortiAnalyzer VM: FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B FortiAnalyzer VM: FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B FortiMail Low Encryption: FE-3000C-LENC FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
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	5.2.8
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	5.1.6
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-VM	2.4.0 2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0.0 1.4.2

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D 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-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

FortiCache models

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

FortiProxy models

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

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E, FAC-VM	4.0 and 4.1

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.6.8.

Compatibility issues with FortiOS 5.6.6

The following table lists interoperability issues that have been identified with FortiManager version 5.6.5 and FortiOS 5.6.6.

Bug ID	Description
513066	FortiManager 5.6.5 does not support the following new value in FortiOS 5.6.6: <code>system sdn-connector</code> command with the <code>azure-region</code> variable set to <code>germany usgov local</code> . If set on FortiGate, the values will be unset during the next configuration installation from FortiManager.
513069	FortiManager 5.6.5 does not support the following new value in FortiOS 5.6.6: <code>system snmp user</code> command with the <code>community events</code> variable set to <code>av-oversize-blocked</code> or <code>faz-disconnect</code> . If set on FortiGate, the values will be unset during the next configuration installation from FortiManager.

Compatibility issues with FortiOS 5.6.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.6.4 and FortiOS version 5.6.5.

Bug ID	Description
496117	Install fails for purging dnsfilter profile.

Compatibility issues with FortiOS 5.6.3

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 <code>switch-controller-dhcp-snooping</code> from that on FortiGate.

Compatibility issues with FortiOS 5.6.0 and 5.6.1

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.

Compatibility issues with FortiOS 5.4.10

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: <pre>system replacemsg mail "email-decompress-limit" system replacemsg mail "smtp-decompress-limit" system replacemsg nntp "email-decompress-limit"</pre>

Compatibility issues with FortiOS 5.4.9

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: <pre>rsso-endpoint-attribute rsso-endpoint-block-attribute sso-attribute</pre>

Compatibility issues with FortiOS 5.4.8

The following table lists interoperability issues that have been identified with FortiManager version 5.4.4 and FortiOS 5.4.8.

Bug ID	Description
469700	FortiManager is missing three wtp-profiles: FAP221E, FAP222E, and FAP223E.

Compatibility issues with FortiOS 5.2.10

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.

Compatibility issues with FortiOS 5.2.7

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.

Compatibility issues with FortiOS 5.2.6

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.

Compatibility issues with FortiOS 5.2.1

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> , <code>retrieve</code> may not work as expected.

Compatibility issues with FortiOS 5.2.0

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.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The <code>set dedicated-management-cpu enable</code> and <code>set user-anonymize enable</code> CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.6.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
513225	There is a performance issue when editing or cloning IPsec phase 1 or phase 2 in Device Manager.
520964	FortiManager is not able to assign FQDN address object to Static Route Named Address.
524947	FortiManager is able to edit a VPN Tunnel interface even if the IP Address is set to default value.
525927	When "Import all objects" is selected, FortiManager should import all FortiTokens.
527650	FortiManager cannot import a local certificate with a large number of alternative names for subject.
530066	After upgraded FortiManager, the 'Mapped policy interface' list under device manager does not show up.
520123	0255: After install to 500 devices, multiple devices are out of sync when auto update disabled.

Policy and Objects

Bug ID	Description
517618	Users should be able to use "Header" type Explicit Policy address as Source Address in Explicit Proxy policies.
521663	FortiManager should correctly handle adding a user into a user group with a user name that contains the '\$' character.
522721	FortiManager allows longer section titles than FortiGate's limit.
523649	FortiManager is not updating last modified time when modifying a web filter category.
525926	The "Local Users" column is always empty even token is assigned.

Bug ID	Description
525938	Token used in device's local admin configuration is displayed as not used in ADOM database.
530717	When adding an address via the right-click menu on the policy page, the page is stuck at the loading status.
530749	FortiManager is unable to import policy configuration for long VDOM name.

Revision History

Bug ID	Description
474245	Policy Install fails due to "set disk-usage log" command inconsistency in Device Manager.
520976	Revision diff always shows changes with policy package settings.
521379	FortiManager may disable the reliable option for FortiAnalyzer log settings.
522828	FortiManager should get dhcp-snooping configuration from FortiGate in Auto-update and retrieve process, and should not unset the configuration.
523712	FortiManager tries to push trailing spaces when configuring a VIP.
526287	B0255: Policy install stuck at 67%.
535170	FortiManager does not accept FQDN address configuration of "_aaa._tcp.gmail.com".

Services

Bug ID	Description
517874	FortiManager should be able to use 'US only' FortiGuard servers with any license configuration.
525646	Users cannot delete Web Filtering and Anti-Spam databases on FortiManager.
528931	FOS-VM may retrieve INVALID License from FMGR-VM-Meter causing Traffic Outage.

System Settings

Bug ID	Description
502882	The search filter does not work for Event Log when level is set at four or five.

Bug ID	Description
530498	Read-Only admin should not be allowed to enable VPN Manager.

VPN Manager

Bug ID	Description

Others

Bug ID	Description
526232	The "execute reset hitcount" command tries to reset the 5.2 ADOMs, which have no hit counts.
532075	When editing comment/description, FortiManager may display the slash character, "/", as "/".
529332	FortiManager cannot correct scope errors when "diagnose cdb check policy-packages" is ran.

Common Vulnerabilities and Exposures

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

Bug ID	Description
464795	FortiManager 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">CVE-2017-17541

Bug ID	Description
473644	FortiManager 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li data-bbox="415 296 630 323">• CVE-2018-1354
474994	FortiManager 5.6.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li data-bbox="415 386 630 413">• CVE-2018-1355

Known Issues

The following issues have been identified in 5.6.8. For inquires about a particular bug or to report a bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
462710	FortiManager cannot detect unauthorized FortiAP units that have been automatically added to managed FortiGate units. As a workaround, perform a manually retrieve operation on the managed FortiGate.

Others

Bug ID	Description
496746	FortiManager may be able to add a FortiGate when both devices are in FIPS mode.

Appendix A - FortiGuard Distribution Servers (FDS)

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

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

FortiGuard Center update support

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

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	<ul style="list-style-type: none">• 5.0.0 and later• 5.2.0 and later• 5.4.0 and later• 5.6.0 and later	✓		✓	
FortiClient (Windows)	<ul style="list-style-type: none">• 4.3.0 and later	✓			
FortiClient (Windows)	<ul style="list-style-type: none">• 4.2.0 and later	✓	✓		✓
FortiClient (Mac OS X)	<ul style="list-style-type: none">• 5.0.1 and later• 5.2.0 and later• 5.4.0 and later• 5.6.0 and later	✓		✓	
FortiMail	<ul style="list-style-type: none">• 4.2.0 and later• 4.3.0 and later• 5.0.0 and later• 5.1.0 and later• 5.2.0 and later	✓	✓		
FortiSandbox	<ul style="list-style-type: none">• 1.2.0, 1.2.3• 1.3.0• 1.4.0 and later	✓			

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiWeb	<ul style="list-style-type: none">• 5.0.6• 5.1.4• 5.2.0 and later• 5.3.0	✓			

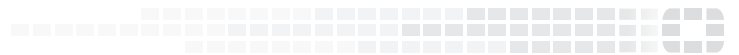


To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

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



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.