



# FortiManager - Release Notes

Version 5.6.6



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET 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](mailto:techdocs@fortinet.com)



November 16, 2018

FortiManager 5.6.6 Release Notes

02-566-514064-20181116



# TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>Change Log</b>   | <b>5</b>  |
| <b>Introduction</b>                                       | <b>6</b>  |
| Supported models  | 6         |
| Minimum screen resolution                                 | 6         |
| <b>Special Notices</b>                                    | <b>7</b>  |
| 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         |
| <b>Upgrade Information</b>                                | <b>10</b> |
| Upgrading to FortiManager 5.6.6                           | 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        |
| <b>Product Integration and Support</b>                    | <b>13</b> |
| FortiManager 5.6.6 support                                | 13        |
| Feature support   | 16        |
| Language support  | 17        |
| Supported models  | 18        |
| <b>Compatibility with FortiOS Versions</b>                | <b>25</b> |
| 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        |
| <b>Resolved Issues .....</b>                                    | <b>29</b> |
| AP Manager .....  | 29        |
| Device Manager .....  | 29        |
| HA .....  | 30        |
| Policy and Objects .....  | 30        |
| Revision History .....  | 32        |
| Script .....  | 32        |
| Services .....  | 33        |
| System Settings .....   | 33        |
| VPN Manager .....   | 33        |
| Others .....  | 34        |
| Common Vulnerabilities and Exposures .....                      | 34        |
| <b>Known Issues .....</b>                                       | <b>35</b> |
| Device Manager .....  | 35        |
| Policy & Objects .....  | 35        |
| System Settings .....   | 35        |
| Others .....  | 35        |
| <b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b> | <b>37</b> |
| FortiGuard Center update support .....                          | 37        |



# Change Log

| Date       | Change Description   |
|------------|--|
| 2018-10-02 | Initial release of 5.6.6.  |
| 2018-10-04 | Added the following Mantis to <i>Resolved Issues</i> : 482721, 437064, 472011, 462721, 473644, and 474994. |
| 2018-10-09 | Added 442727 to <i>Resolved Issues</i> .   |
| 2018-10-15 | Added 498356 to <i>Resolved Issues</i> .   |
| 2018-11-01 | Added 507677 to <i>Resolved Issues</i> .   |
| 2018-11-02 | Added FMG-300F to <i>Supported Models</i> .  |
| 2018-11-08 | Added FMG-VM64-GCP to <i>Supported Models</i>  |
| 2018-11-16 | Added 423921 to <i>Known Issues</i> .  |



# Introduction

This document provides the following information for FortiManager 5.6.6 build 1750:

- [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 5.6.6 supports the following models:

|                        |  |
|------------------------|--|
| <b>FortiManager</b>    | 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.  |
| <b>FortiManager VM</b> | 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 5.6.6.

## 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 5.6.6

You can upgrade FortiManager 5.4.0 or later directly to 5.6.6. 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 5.6.6, 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 5.6.6.

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 5.6.6 support

The following table lists 5.6.6 product integration and support information:

| Web Browsers |
|--------------|
|--------------|

- |   |
|---|
| <ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11 or Edge 40<br/>Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.</li><li>• Mozilla Firefox version 62</li><li>• Google Chrome version 69</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p> |
|---|



**FortiOS/FortiOS Carrier**

- 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](#).



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



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



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

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



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

## Feature support

The following table lists FortiManager feature support for managed platforms.

| Platform             | Management Features | FortiGuard Update Services | Reports | Logging |
|----------------------|---------------------|----------------------------|---------|---------|
| <b>FortiGate</b>     | ✓                   | ✓                          | ✓       | ✓       |
| <b>FortiCarrier</b>  | ✓                   | ✓                          | ✓       | ✓       |
| <b>FortiAnalyzer</b> |                     |                            | ✓       | ✓       |
| <b>FortiCache</b>    |                     |                            | ✓       | ✓       |
| <b>FortiClient</b>   |                     | ✓                          | ✓       | ✓       |
| <b>FortiDDoS</b>     |                     |                            | ✓       | ✓       |
| <b>FortiMail</b>     |                     | ✓                          | ✓       | ✓       |



| 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 5.6.6.



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

### FortiGate models

| Model   | Firmware Version |
|---|------------------|
| <b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E,<br><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D<br><b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC<br><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC<br><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.<br><b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D<br><b>FortiGate VM:</b> 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<br><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D | 5.6              |



| Model  | Firmware Version |
|--|------------------|
| <b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E<br><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1<br><b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F<br><b>FortiGate 7000 Series:</b> FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8<br><b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC<br><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC<br><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.<br><b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D<br><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM<br><b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D | 5.4              |



| Model  | Firmware Version |
|--|------------------|
| <b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B<br><b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C<br><b>FortiGate DC:</b> FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC<br><b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC<br><b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D<br><b>FortiGate Rugged:</b> FGR-60D, FGR-100C<br><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN<br><b>FortiSwitch:</b> FS-5203B, FCT-5902D | 5.2              |

### FortiCarrier Models

| Model  | Firmware Version |
|--|------------------|
| <b>FortiCarrier:</b> 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<br><b>FortiCarrier DC:</b> 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<br><b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM | 5.4              |



| Model  | Firmware Version |
|--|------------------|
| <b>FortiCarrier:</b> 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<br><b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC<br><b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC<br><b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND | 5.2              |

### FortiDDoS models

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

### FortiAnalyzer models

| Model   | Firmware Version |
|---|------------------|
| <b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.  | 5.6              |
| <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).  |                  |
| <b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.  | 5.4              |
| <b>FortiAnalyzer VM:</b> FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.  |                  |
| <b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B<br><b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN                               | 5.2              |
| <b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B<br><b>FortiAnalyzer VM:</b> 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 |
|---|------------------|
| <b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B<br><b>FortiMail Low Encryption:</b> FE-3000C-LENC<br><b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN | 5.3.7            |
| <b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B<br><b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN   | 5.2.8            |
| <b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B<br><b>FortiMail VM:</b> FE-VM64  | 5.1.6            |
| <b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B<br><b>FortiMail VM:</b> FE-VM64   | 5.0.10           |

**FortiSandbox models**

| Model  | Firmware Version                            |
|--|---|
| <b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D<br><b>FortiSandbox VM:</b> FSA-VM | 2.4.0<br>2.3.2                              |
| <b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D<br><b>FortiSandbox VM:</b> FSA-VM                       | 2.2.0<br>2.1.0                              |
| <b>FortiSandbox:</b> FSA-1000D, FSA-3000D<br><b>FortiSandbox VM:</b> FSA-VM                                  | 2.0.0<br>1.4.2                              |
| <b>FortiSandbox:</b> FSA-1000D, FSA-3000D  | 1.4.0 and 1.4.1<br>1.3.0<br>1.2.0 and later |

**FortiSwitch ACTA models**

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



**FortiWeb models**

| Model   | Firmware Version |
|---|------------------|
| <b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D<br><b>FortiWeb VM:</b> FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN                                | 5.9.1            |
| <b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D<br><b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN | 5.8.6            |
| <b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D<br><b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN  | 5.7.2            |
| <b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D<br><b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN   | 5.6.1            |
| <b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E<br><b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE  | 5.5.6            |
| <b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E<br><b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV   | 5.4.1            |
| <b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E<br><b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV   | 5.3.9            |



| Model   | Firmware Version |
|---|------------------|
| <b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E<br><b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR | 5.2.4            |

#### FortiCache models

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

#### FortiProxy models

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

#### FortiAuthenticator models

| Model  | Firmware Version |
|--|------------------|
| <b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-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 5.6.6.

## 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:<br>system replacemsg mail "email-decompress-limit"<br>system replacemsg mail "smtp-decompress-limit"<br>system replacemsg nntp "email-decompress-limit" |

## 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:<br>rsso-endpoint-attribute<br>rsso-endpoint-block-attribute<br>sso-attribute |

## 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.<br>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 5.6.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

| Bug ID | Description  |
|--------|--|
| 450434 | The "wtp-mode" is unset after changed AP configuration from AP Manager.  |
| 496657 | AP Manager GUI's device list is missing some FortiGate devices with managed APs.                                   |
| 500022 | FortiManager should let users to select FortiAP from firmware list.  |
| 504394 | The WiFi profile for FAP221E should display RADIO 2.   |
| 509769 | When attempting to assign the default profile to FAP221E, FortiManager returns an error on unknown <i>wtp-ip</i> . |

## Device Manager

| Bug ID | Description  |
|--------|--|
| 480400 | FortiManager does not show the correct FortiGate's system time under Device Manager.                         |
| 488577 | FortiManager GUI should display more than 50 SD-WANs to allow more firewalls to be managed.                  |
| 491367 | User may not be able to import policies it take a long time to load zone mapping.                            |
| 491926 | Renaming ADOM interface during import fails to add policies.   |
| 492801 | When FIPS is enabled, the AES256 option should be available on FortiManager's VPN phase1.                    |
| 494537 | Virtual switch-interface moves to root VDOM after changing it directly on FortiGate 140D-POE.                |
| 494923 | IKE version grayed out in existing tunnels, unlike FortiOS GUI.  |
| 495785 | Import process keeps loading and becomes unresponsive where there are 7000 policies configured on FortiGate. |
| 500177 | FortiManager does not push IPsec Phase1 XAUTH user group configuration to the firewall.                      |
| 500293 | FortiManager fails to configure Alert email settings on no management VDOM when FortiGate has no disk.       |



| Bug ID | Description   |
|--------|---|
| 503926 | Import should simply add all SD-WAN status check entries to FortiManager without any error.                                 |
| 505916 | Copying firewall policy from one policy package to another causing source policy package to go in to <i>Modified</i> state. |
| 509329 | Importing policies may consume high CPU resources.  |

## HA

| Bug ID | Description  |
|--------|--|
| 462721 | [fg-7k ha] Failed to change HA device sequence.  |
| 500682 | Cluster members should be able to ping each other if there are no trusted host restrictions. |

## Policy and Objects

| Bug ID | Description   |
|--------|---|
| 293781 | If reset operation is done via FortiGate's GUI, new <i>Hit Count</i> details should be reflected in FortiManager's GUI.                                       |
| 442727 | <code>internet-service-id</code> does not match between FortiManager and FortiGate. FortiManager displays ID instead of internet service name upon retrieval. |
| 453702 | FortiManager should be able to filter policy using Hit Count, Bytes, Packets, First Used, or Last Used.   |
| 459753 | The message, <i>waiting for other session id (xxxx), username (xxxxx)</i> , should be truncated.  |
| 461772 | Wildcard FQDN should be available to be selected when editing firewall policy.  |
| 467535 | Explicit proxy policy should be configurable with Application Profile that blocks Proxy Category.   |
| 472011 | If you accidentally delete a global used object, policy assignment to local ADOM fails, but suggest using a better error message.                             |
| 473973 | Drag-and-drop should not allow coexisting of both security profiles and profile groups.   |
| 474629 | When Security Profile Groups are created on the FortiManager, they are all pushed to all FortiGates on the next policy install.                               |
| 476220 | Users are unable to edit objects from the Explicit Proxy Policy view within a 5.4 ADOM.   |
| 476227 | FortiManager should not clear any filters applied on Policy or Objects when admin locks the ADOM or changes the view.   |



| Bug ID | Description   |
|--------|---|
| 479258 | The import policy operation on one device should not cause other packages to change status.   |
| 492293 | When selecting an object on a policy with many objects, the user still needs to scroll down to find the highlighted object.   |
| 492893 | Installing custom IPS and Application Control signatures with the same Attack ID will cause install to fail.  |
| 494253 | FortiManager may not display all service objects when it encounters an error on an object.  |
| 496827 | Users are unable to delete LDAP server if user group is deleted before removing the LDAP members.   |
| 498356 | Hit counters and bytes not correct in FortiManager for some rules.  |
| 498642 | LDAP browse from ADOM objects does not work if the primary LDAP server is not reachable.  |
| 499721 | Cloning replacement message group does not keep custom HTML rather sets to default.   |
| 501313 | Policy Package Clone fails caused by invalid installation targets.  |
| 501477 | Push to device function installs all the address objects to FortiGate even when the objects are not being used.   |
| 502047 | Policy install fails when IP pool object type is changed from fixed port range to overload.   |
| 503664 | Right-pane object selector does not show profile groups.  |
| 505469 | User may not be able to install an external CA certificate.   |
| 507677 | Cannot edit IPS filters in IPS profiles.  |
| 507677 | After creating an IPS filter, it is not possible to edit it in order to add or remove certain signatures.   |
| 507919 | FortiManager must recognize that internet-service-custom object is part of master internet-service object and need to be installed or imported properly.  |
| 508324 | Policy package status should remain synchronized after cloning a policy packing and its installation targets are removed.   |
| 508456 | In workspace mode, when a referenced object is deleted, but the changes are discarded, FortiManager leaves behind the object reference in the policy, despite the address object already deleted. |
| 508584 | <i>wisp-servers</i> should be available in GUI under the advanced web filter options.   |
| 509173 | Policy Package Install may fail after upgrading from 5.4.5 to 5.6.4.  |
| 509185 | FortiManager may install default certificate instead of the dynamically mapped certificate.   |
| 509790 | When creating a new LDAP user on FortiManager, the LDAP browser ID column is showing the user <i>cn</i> instead of <i>SAMAccount</i> .  |
| 509854 | If firewall address groups are recursively defined, FortiManager may run into infinite loop. This causes the data check to fail causing the security console daemon to crash.                     |



| Bug ID | Description   |
|--------|---|
| 510936 | Adding a new device to address object should not set the interface to <i>any</i> for previous associated devices. |
| 512167 | FortiManager may not be able to configure a custom IPS signature due to change with "--protocol" on FortiGate.    |

## Revision History

| Bug ID | Description   |
|--------|---|
| 473169 | Users are unable to proceed to device install screen through install wizard if default device selection for ADOM is set to <i>unselect all</i> .  |
| 477678 | FortiManager should not unset <i>admin-scp</i> when it is set as enabled.   |
| 484608 | Installation fails when creating a dial-up VPN with peer type set to use a dial-up user group.  |
| 486536 | Policy package install fails due to <i>VIP overlap</i> error with FQDN VIP.   |
| 490500 | RADIUS source IP and VAP errors occur when installing a policy that has security profiles on FortiWiFi-60E.   |
| 499734 | Install attempt to any of the managed devices may hang due to null interface within system DHCP server entries.   |
| 504382 | After setting a ssl/ssh profile with <i>Multiple Clients Connecting to Multiple Servers</i> and setting a non-CA certificate in the <i>CA certificate</i> field, and then selecting <i>Protecting SSL Server</i> with a non-CA certificate, FortiManager returns an error during install. |
| 508080 | FortiManager pushes a lot of move commands to FortiGate when moving a policy from top to bottom.  |
| 515102 | When installing policy package, FortiManager should not apply media type parameter on VLAN interfaces.  |

## Script

| Bug ID | Description  |
|--------|--|
| 459030 | Changes made on <i>ha-mgmt-interface</i> via CLI script should be installed.   |
| 499342 | When running a CLI script on Policy Package/ADOM, a firewall address with .067 (example 10.10.10.067/32) is configured. The script runs without error. The subnet is accepted but the address is configured as .55 (10.10.10.55/32) instead. |
| 507394 | FortiManager may return an error, <i>Error:response with errors</i> , when creating a new script.  |



## Services

| Bug ID | Description  |
|--------|--|
| 478050 | When FortiManager provides services to FortiGate HA, FortiManager shows duplicate entries under FortiGuard > Package Management > Service Status after the FortiGate failover. |
| 501456 | Web filter license and service should activate or deactivate immediately after contract is received or withdrawn via update process.   |
| 508469 | FortiManager may render the values for the horizontal axis with a gray area.   |

## System Settings

| Bug ID | Description   |
|--------|---|
| 469471 | FortiManager is not able to resolve IP address for the domain name, <i>smtp.office365.com</i> .         |
| 474712 | Auto-backup process does not work and results in out-of-sync FortiGate configuration in Backup ADOM.    |
| 488836 | Wildcard TACACS+ admin should be able to access more than one ADOM.                                     |
| 499066 | FortiManager cannot verify PKI admin client certificate if the CA chain has more than two certificates. |
| 510459 | The device <i>lock</i> and <i>unlock</i> actions should generate event logs.                            |

## VPN Manager

| Bug ID  | Description  |
|---------|--|
| 437064  | Create SSL VPN is missing Authentication/Portal Mapping and default value.                           |
| 481717  | VPN Monitor may not show some tunnels connections.   |
| 504541  | FortiManager should allow users to upload AP profiles and create new AP Profiles under 5.2 ADOM.     |
| 504957  | VPN Manager Monitor took more than 10 minutes to load page with 16000 tunnels.                       |
| 4785376 | FortiManager is unable to install VPN script and install log reports duplicated VPN remote gateways. |



## Others

| Bug ID | Description  |
|--------|--|
| 482721 | The filtering of the Event Logs does not work properly with combination "NOT" logic in one column.                 |
| 492852 | After enabling workflow, there is high consumption on CPU resources caused by the <i>svc dvmdb reader</i> process. |
| 494072 | Central DNAT is incorrectly translated to Central SNAT in Japanese language on GUI.                                |
| 501485 | FortiManager should not change <i>Web Filter Local Category ID</i> during ADOM upgrade.                            |
| 501507 | Strong-crypto parameter should be visible using JSON API.  |
| 507434 | Console unable to accept username with space character.  |

## Common Vulnerabilities and Exposures

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

| Bug ID | Description   |
|--------|---|
| 464795 | FortiManager 5.6.6 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2017-17541</li></ul> |
| 473644 | FortiManager 5.6.6 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2018-1354</li></ul>  |
| 474994 | FortiManager 5.6.6 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2018-1355</li></ul>  |



# Known Issues

The following issues have been identified in 5.6.6. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Device Manager

| Bug ID | Description   |
|--------|---|
| 506163 | FortiManager GUI may not display zone members.  |
| 506697 | Logical interfaces on FortiGate are not shown under the HA port monitor page on the FortiManager. |

## Policy & Objects

| Bug ID | Description   |
|--------|---|
| 510929 | During import, there is no notification to remind users that some objects may be renamed.               |
| 511717 | Policy package install fails intermittently when installing traffic shaping configuration to FortiGate. |

## System Settings

| Bug ID | Description   |
|--------|---|
| 508680 | Setting for specified policy package with in admin user is gone after ADOM upgrade. |

## Others

| Bug ID | Description   |
|--------|---|
| 423921 | Cannot get CSF group name.<br><b>Note:</b> GUI displays the wrong Security Fabric name. |



| Bug ID | Description  |
|--------|--|
| 511580 | The category-override setting under web filter profile may be changed after upgraded FortiManager.                                 |
| 512410 | FortiManager's Master unit may no delete temporary file, showconf, causing the tmp directory to fill up and retrieves to fail.     |
| 512705 | When using XML API to get the latest revision of FortiGate device, FortiManager may show the administrator password in clear text. |



# 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"><li>• 5.0.0 and later</li><li>• 5.2.0 and later</li><li>• 5.4.0 and later</li><li>• 5.6.0 and later</li></ul>                           | ✓         |          | ✓                  |          |
| FortiClient (Windows)  | <ul style="list-style-type: none"><li>• 4.3.0 and later</li></ul>   | ✓         |          |                    |          |
| FortiClient (Windows)  | <ul style="list-style-type: none"><li>• 4.2.0 and later</li></ul>   | ✓         | ✓        |                    | ✓        |
| FortiClient (Mac OS X) | <ul style="list-style-type: none"><li>• 5.0.1 and later</li><li>• 5.2.0 and later</li><li>• 5.4.0 and later</li><li>• 5.6.0 and later</li></ul>                           | ✓         |          | ✓                  |          |
| FortiMail              | <ul style="list-style-type: none"><li>• 4.2.0 and later</li><li>• 4.3.0 and later</li><li>• 5.0.0 and later</li><li>• 5.1.0 and later</li><li>• 5.2.0 and later</li></ul> | ✓         | ✓        |                    |          |
| FortiSandbox           | <ul style="list-style-type: none"><li>• 1.2.0, 1.2.3</li><li>• 1.3.0</li><li>• 1.4.0 and later</li></ul>  | ✓         |          |                    |          |



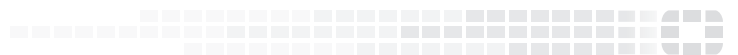
| Platform | Version   | Antivirus | AntiSpam | Vulnerability Scan | Software |
|----------|---|-----------|----------|--------------------|----------|
| FortiWeb | <ul style="list-style-type: none"><li>• 5.0.6</li><li>• 5.1.4</li><li>• 5.2.0 and later</li><li>• 5.3.0</li></ul> | ✓         |        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



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
```





Copyright© 2018 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.