



# FortiManager - Release Notes

Version 5.6.2

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



February 23, 2018

FortiManager 5.6.2 Release Notes

02-562-469176-20180223

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Supported models	6
Minimum screen resolution	6
What's new in FortiManager 5.6.2	7
Virtual Wire Policy Support	7
SDN Connector for VMware NSX and Cisco ACI	7
<b>Special Notices</b>	<b>8</b>
Virtual Wire Pair Support after Upgrade to 5.6.2 or Later	8
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	9
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	10
<b>Upgrade Information</b>	<b>11</b>
Upgrading to FortiManager 5.6.2	11
Upgrading from 5.2.x	11
Downgrading to previous firmware versions	12
FortiManager VM firmware	12
Firmware image checksums	13
SNMP MIB files	13
<b>Product Integration and Support</b>	<b>14</b>
FortiManager 5.6.2 support	14
Feature support	17
Language support	18
Supported models	18
<b>Compatibility with FortiOS Versions</b>	<b>25</b>
Compatibility issues with FortiOS 5.6.3	25
Compatibility issues with FortiOS 5.6.0 and 5.6.1	25
Compatibility issues with FortiOS 5.4.8	25
Compatibility issues with FortiOS 5.2.10	25
Compatibility issues with FortiOS 5.2.7	26
Compatibility issues with FortiOS 5.2.6	26

---

Compatibility issues with FortiOS 5.2.1 .....	26
Compatibility issues with FortiOS 5.2.0 .....	26
<b>Resolved Issues .....</b>	<b>28</b>
AP Manager .....	28
Device Manager .....	28
Policy and Objects .....	28
Services .....	29
System Settings .....	29
Others .....	30
<b>Known Issues .....</b>	<b>31</b>
Device Manager .....	31
Policy & Objects .....	31
Services .....	32
System Settings .....	32
Workspace and Workflow .....	32
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>33</b>
FortiGuard Center update support .....	33

# Change Log

Date	Change Description
2018-01-25	Initial release of 5.6.2.
2018-01-30	Added 463164 to <i>Resolved Issues &gt; Policy and Objects</i> .
2018-02-08	Added <i>Virtual Wire Pair Support after Upgrade to 5.6.2 or Later</i> section to <i>Special Notices</i> .
2018-02-19	Added information about upgrading from 5.2.x.
2018-02-23	Added 453417 to <i>Known Issues &gt; System Settings</i> .

# Introduction

This document provides the following information for FortiManager 5.6.2 build 1631:

- [Supported models](#)
- [What's new in FortiManager 5.6.2](#)
- [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 5.6.2 supports the following models:

<b>FortiManager</b>	FMG-200D, FMG-300D, FMG-300E, 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-HV (including Hyper-V 2016), FMG-VM64-KVM, 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.

## What's new in FortiManager 5.6.2

The following is a list of new features and enhancements in 5.6.2. For details, see the *FortiManager Administrator Guide*:



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

---

### Virtual Wire Policy Support

FortiManager now supports the addition of Virtual Wire Pair policies. You can create Virtual Wire Pair objects from *Object Configurations > Interface* and then use the objects in the Virtual Wire Pair policies.

### SDN Connector for VMware NSX and Cisco ACI

You can now create VMware NSX and Cisco ACI Connectors from FortiManager, use the Connectors to dynamically learn NSX or ACI objects, import the objects to its local object database and then use the objects in its central policies.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.6.2.

## 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 5.6.2

You can upgrade FortiManager 5.4.0 or later directly to 5.6.2. 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 5.6.2, 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 5.6.2.

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.

### 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 5.6.2 support

The following table lists 5.6.2 product integration and support information:

Web Browsers
<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11 or Edge 40</li></ul> <p>Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.</p> <ul style="list-style-type: none"><li>• Mozilla Firefox version 57</li><li>• Google Chrome version 63</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>

**FortiOS/FortiOS Carrier**

- 5.6.2 to 5.6.3  
FortiManager 5.6.2 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.2, 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 5.6.2 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 25](#).
- 5.4.1 to 5.4.8  
FortiManager 5.6.2 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 25](#).
- 5.2.8 to 5.2.13  
FortiManager 5.6.2 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 25](#).
- 5.2.7  
FortiManager 5.6.2 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 26](#).
- 5.2.6  
FortiManager 5.6.2 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 26](#).
- 5.2.2 to 5.2.5
- 5.2.1  
FortiManager 5.6.2 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 26](#).
- 5.2.0  
FortiManager 5.6.2 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 26](#).

**FortiAnalyzer**

- 5.6.0 to 5.6.2
- 5.4.0 to 5.4.4
- 5.2.0 to 5.2.10
- 5.0.0 to 5.0.13

**FortiCache**

- 4.2.6
- 4.1.2
- 4.0.0 to 4.0.4

<b>FortiClient</b>	<ul style="list-style-type: none"><li>• 5.6.3</li><li>• 5.6.0</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>• 5.4.2</li><li>• 5.3.7</li><li>• 5.2.9</li><li>• 5.1.6</li><li>• 5.0.10</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 2.5.1</li><li>• 2.5.0</li><li>• 2.4.1</li><li>• 2.4.0</li><li>• 2.3.2</li><li>• 2.2.1</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 ATCA</b>	<ul style="list-style-type: none"><li>• 5.2.3</li><li>• 5.0.0 and later</li><li>• 4.3.0 and later</li><li>• 4.2.0 and later</li></ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"><li>• 5.8.6</li><li>• 5.6.0</li><li>• 5.5.4</li><li>• 5.4.1</li><li>• 5.3.8</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>• 4.4.1</li><li>• 4.2.3</li><li>• 4.1.11</li></ul> <p>Limited support. For more information, see <a href="#">Feature support on page 17</a>.</p>



**Virtualization**

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 6.2
- Linux KVM Redhat 6.5
- Microsoft Azure
- Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2
- OpenSource XenServer 4.2.5
- VMware
  - ESX versions 4.0 and 4.1
  - ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5



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		✓	✓	✓
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 import language translation files for these languages via the command line interface 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, 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 5.6.2.



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, <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D <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 <b>FortiGate Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM <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, FG-3980E, FG-2000E, FG-2500E <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 7000 Series:</b> FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC <b>FortiGate Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM <b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

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

### FortiCarrier Models

Model	Firmware Version
<b>FortiCarrier:</b> 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 <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 <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 <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC <b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC <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 <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-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 <b>FortiMail Low Encryption:</b> FE-3000C-LENC <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 <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 <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 <b>FortiMail VM:</b> FE-VM64	5.0.10

**FortiSandbox models**

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

**FortiSwitch 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 <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

**FortiWeb models**

Model	Firmware Version
<b>FortiWeb:</b> FWB-2000E	5.6.0
<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	5.5.3
<b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
<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	5.4.1
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	
<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	5.3.8
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	
<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	5.2.4
<b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	

**FortiCache models**

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

**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 5.6.2.

## Compatibility issues with FortiOS 5.6.3

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

## Compatibility issues with 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 5.4.8

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 5.6.2 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 5.6.2 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 5.6.2 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 5.6.2 and FortiOS version 5.2.1.

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

## Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.6.2 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 5.6.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
462441	The prerequisite checks for <code>set login-passwd</code> may be missing.
375895	Users may not be able to select a VDOM upon creating a WiFi SSID interface.

## Device Manager

Bug ID	Description
464607	Wrong error pop-up may be displayed when users try to edit settings under <i>CLI-Only objects/system/lte-modem</i> .
460407	Users may not be able to select multiple guest groups under admin account in <i>Restrict Admin to Guest Account Provisioning Only</i> .
443074	<i>RADIUS Accounting</i> is missing when users edit loopback interface.
460403	FortiManager may not generate a VxLAN correctly.
399893	Named addresses in Router table may not be displayed in GUI.
470437	Device may be not visible in Device Manager GUI when it is set to <i>Manage Only</i> .

## Policy and Objects

Bug ID	Description
452094	The cursor location may not be at the newly inserted policy.
457220	Users may not use wildcard characters in <i>Policy Package Column Filter</i> search.
464311	<i>Apply &amp; Refresh</i> in FSSO may modify the device status other VDOMS in ADOMs.

Bug ID	Description
407664	The right click menu for local user may be missing the <i>grouping</i> function.
464028	<code>tcp-portrange</code> may be unset during installation for custom proxy services.
443785	Dynamic IP Pool selection menu may be missing in right click menu.
466600	The results of <i>Where used</i> may be incorrect after users edit some entries of the initial results.
459897	Once the users have selected a <i>Policy Package Folder</i> , the menu tools may be unavailable.
465124	Column filter drop down menu may get blocked by the lower pane.
466306	The policies may not be displayed if the policy package name contains a slash.
307891	Interface selection may not filter out not feasible interfaces.
455813	Users may get an incorrect error pop-up when they try to create an LDAP user.
465177	Installation may fail with newly created FSSO configurations.
468013	Changes to nested Address Group may not be installed to the FortiGate.
466033	Users may not be able to create SNAT in v5.4 ADOMs.
465924	In advanced ADOM mode, VDOMs in different ADOMs may block FSSO retrieval via FortiGate.
468675	The protocol-number in custom service may not be installed to FortiGates.
469480	Users may not be able to import policies when the interfaces to be imported have different types from the ones in the ADOM.
463164	When creating a new ADOM, FortiManager automatically creates default ADOM interfaces in the ADOM database.

## Services

Bug ID	Description
466346	Users may not be able to update entitlement file via CLI.
461735	FOS-VM managed by FortiManager Web Filtering license may be displayed as <i>Expired</i> .

## System Settings

Bug ID	Description
466182	An admin user with <i>all permissions read-write</i> may not be able to edit a device in Device Manager.

Bug ID	Description
466843	An admin user with <i>read-write permissions</i> to Log View/FortiView/NOC may not be able to view devices in the device list in Log View.

## Others

Bug ID	Description
464103	JSON API may return an incorrect name for a long VDOM.

Bug ID	Description
--------	-------------

# Known Issues

The following issues have been identified in 5.6.2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
465854	DHCP Server IP ranges may be removed upon device installation.
469667	The <i>Close</i> button in Install Preview may be displayed as <i>Cancel</i> .
467091	MTU settings in FortiExtender may be removed upon installation.
462852	FortiManager may not enable <code>vlanforward</code> on interfaces pertaining to a virtual wire pair.
469281	<i>Config Status</i> may become <i>Modified</i> after a restricted admin installs changes to another device.
463408	Users may not be able to set <i>Administrative distance</i> for <i>None (Blackhole)</i> devices in static route.

## Policy & Objects

Bug ID	Description
468001	Users may be unable to paste a firewall policy into a new Policy Package.
469792	FSSO per-device mappings may be removed unexpectedly.
371732	Users may not be able to create or edit virtual server in right object selection pane.
468724	Policy sections may get expanded unexpectedly.
467794	A policy may be moved to another section when users use drag and drop.
456244	After scrolling in policy list, the focus may not be go back to the newly inserted policy or the position where a policy just deleted.
470289	Users may not be able to set <i>install on to default</i> or <i>none</i> for a policy if there are no targets currently configured.

## Services

Bug ID	Description
469404	Antispam databases may take up disk space.

## System Settings

Bug ID	Description
469958	ADOM upgrade from v5.4 to v5.6 may fail because of ADOM interface default value is "".
453417	Importing a PKC12 local certificate may not work as expected.

## Workspace and Workflow

Bug ID	Description
470285	After locking an ADOM, users may need to refresh to display the policies.



# 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.