



# FortiManager - Release Notes

Version 6.2.2

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



September 1, 2020

FortiManager 6.2.2 Release Notes

02-622-585539-20200901

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>FortiManager 6.2.2 Release</b>	<b>6</b>
Supported models	6
What's new	6
<b>Special Notices</b>	<b>7</b>
Multi-step firmware upgrades	7
Multicast policies with zones or zone members	7
Policy Re-installation with Multiple VDOMs	7
Wildcard Address Support in Policy	7
Import Authentication Rules and Schemes	7
Support of the NGFW mode in 6.2.1	8
Managing FortiGate with VDOMs that use Global, Shared Profiles	8
Managing FortiAnalyzer Devices	8
IOC Support on FortiManager	8
Hyper-V FortiManager-VM running on an AMD CPU	9
SSLv3 on FortiManager-VM64-AWS	9
<b>Upgrade Information</b>	<b>10</b>
Downgrading to previous firmware versions	10
Firmware image checksums	10
FortiManager VM firmware	10
SNMP MIB files	12
<b>Product Integration and Support</b>	<b>13</b>
FortiManager 6.2.2 support	13
Web browsers	13
FortiOS/FortiOS Carrier	14
FortiAnalyzer	15
FortiAuthenticator	15
FortiCache	15
FortiClient	15
FortiMail	16
FortiSandbox	16
FortiSwitch ATCA	16
FortiWeb	16
FortiDDoS	16
Virtualization	17
Feature support	17
Language support	18
Supported models	18
FortiGate models	19
FortiGate special branch models	21
FortiCarrier models	22
FortiDDoS models	23
FortiAnalyzer models	24

---

FortiMail models .....	24
FortiSandbox models .....	25
FortiSwitch ATCA models .....	26
FortiSwitch models .....	26
FortiWeb models .....	26
FortiCache models .....	28
FortiProxy models .....	28
FortiAuthenticator models .....	28
<b>Compatibility with FortiOS Versions .....</b>	<b>29</b>
FortiManager 6.2.2 and FortiOS 6.0.8 compatibility issues .....	29
FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues .....	29
FortiManager 6.2.2 and FortiOS 5.6.12 compatibility issues .....	30
FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues .....	30
FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues .....	30
FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues .....	30
FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues .....	31
FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues .....	31
FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues .....	31
FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues .....	32
<b>Resolved Issues .....</b>	<b>33</b>
Common Vulnerabilities and Exposures .....	37
<b>Known Issues .....</b>	<b>38</b>
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>40</b>
FortiGuard Center update support .....	40

# Change Log

Date	Change Description
2019-10-09	Initial release of 6.2.2.
2019-10-09	Added 544012 to Resolved Issues.
2019-10-10	Updated <a href="#">FortiGuard Distribution Servers (FDS) on page 40</a> .
2019-10-11	Added 588869 to Known Issues and Special Notices.
2019-10-16	Added 589101, 589240, and 589269 to Known Issues.
2019-10-20	Added Nutanix to <a href="#">Virtualization on page 17</a> .
2019-10-22	Added 509665 to Known Issues.
2019-10-23	Removed Nutanix.
2019-10-28	Removed info about a common vulnerability and exposure that was fixed in 6.2.1.
2019-10-29	Added <a href="#">FortiGate special branch models on page 21</a> .
2019-11-05	Updated <a href="#">FortiGate special branch models on page 21</a> .
2019-11-19	Updated <a href="#">Special Notices on page 7</a> .
2019-11-22	Updated <a href="#">Product Integration and Support on page 13</a> .
2019-12-02	Updated <a href="#">FortiOS/FortiOS Carrier on page 14</a> .
2019-12-12	Updated to add support for FortiOS 5.6.12 and 6.0.8. Also added <a href="#">FortiManager 6.2.2 and FortiOS 6.0.8 compatibility issues on page 29</a> and <a href="#">FortiManager 6.2.2 and FortiOS 5.6.12 compatibility issues on page 30</a>
2020-01-28	Updated <a href="#">Special Notices on page 7</a> and <a href="#">Known Issues on page 38</a> .
2020-02-18	Added 569307 to <a href="#">Resolved Issues on page 33</a> .
2020-03-02	Added bug 592646 to <a href="#">Known Issues on page 38</a> .
2020-07-31	Changed mantis ID from 572283 to 572284 to correct typo in <a href="#">Resolved Issues on page 33</a> .
2020-09-01	Updated <a href="#">Special Notices on page 7</a> and added 468776 to <a href="#">Known Issues on page 38</a> .

# FortiManager 6.2.2 Release

This document provides information about FortiManager version 6.2.2 build 1183.



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

---

This section includes the following topics:

- [Supported models on page 6](#)
- [What's new on page 6](#)

## Supported models

FortiManager version 6.2.2 supports the following models:

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

## What's new

For information about what's new in FortiManager 6.2.2, see the [FortiManager New Features Guide](#).



Not all features/enhancements are supported on all models.

---

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.2.2.

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our [support site](#). To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

## Multicast policies with zones or zone members

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

## Policy Re-installation with Multiple VDOMs

As outlined in bug id 588869, using *Re-Install Policy* against multiple VDOMs could cause significant configuration loss. Use *Install Wizard* to avoid this problem. As always, use *Install Preview* to confirm changes prior to Install.

## Wildcard Address Support in Policy

With FortiOS 6.2.2 defines all wildcard address objects as regular address objects with type set as FQDN, FortiManager 6.2.2 can only select FQDN type address in policy and install to FortiOS 6.2.2 devices.

## Import Authentication Rules and Schemes

If `kerberos-keytab user` is referenced in `config authentication scheme > set kerberos-keytab`, FortiManager purges the authentication scheme and authentication rule after upgrading to FortiManager 6.2.1 and later. After upgrading, import the authentication rule and authentication scheme from FortiOS to the FortiManager ADOM before modifying and installing any configurations to FortiOS.

## Support of the NGFW mode in 6.2.1

Within a version 6.2 ADOM, policy package with NGFW mode set as policy based only supports FortiOS 6.2.1.

## Managing FortiGate with VDOMs that use Global, Shared Profiles

FortiManager managing FortiGates with global, shared g-xx profiles in VDOMs and running FortiOS 6.0.0 or later is unable to import global, shared g-xx profiles from FortiGate devices.

Before adding the FortiGate units to FortiManager, perform the following steps to unset the global ADOM objects. After the default configurations are unset, you can successfully add the FortiGate units to FortiManager.

1. On the Fortigate for each VDOM, unset the following global ADOM objects by using the CLI:

```
config wireless-controller utm-profile
  edit "wifi-default"
    set comment "Default configuration for offloading WiFi traffic."
  next
  edit "g-wifi-default"
    set comment "Default configuration for offloading WiFi traffic."
    set ips-sensor "g-wifi-default"
    set application-list "g-wifi-default"
    set antivirus-profile "g-wifi-default"
    set webfilter-profile "g-wifi-default"
    set firewall-profile-protocol-options "g-wifi-default"
    set firewall-ssl-ssh-profile "g-wifi-default"
  next
end

FGVMULCV30310000 (utm-profile) # ed g-wifi-default
FGVMULCV30310000 (g-wifi-default) # sh
config wireless-controller utm-profile
  edit "g-wifi-default"
    set comment "Default configuration for offloading WiFi traffic."
  next
end
```

2. After the global ADOM objects are unset, you can add the FortiGate unit to FortiManager.

## Managing FortiAnalyzer Devices

FortiManager 6.2 can only manage and process logs for FortiAnalyzer 6.2 devices.

## IOC Support on FortiManager

Please note that FortiManager does not support IOC related features even when FortiAnalyzer mode is enabled.



## 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.

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol tlsv1
end
```

# Upgrade Information

You can upgrade FortiManager 6.0.3 or later directly to 6.2.2.



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

---

This section contains the following topics:

- [Downgrading to previous firmware versions on page 10](#)
- [Firmware image checksums on page 10](#)
- [FortiManager VM firmware on page 10](#)
- [SNMP MIB files on page 12](#)

## Downgrading to previous firmware versions

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

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

## Firmware image checksums

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

## FortiManager VM firmware

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

## Aliyun

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

## Amazon Web Services

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

## Citrix XenServer and Open Source XenServer

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

## Linux KVM

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

## Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

## Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

### VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtualappliances.html>. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

# Product Integration and Support

This section lists FortiManager 6.2.2 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.2.2 support on page 13](#)
- [Feature support on page 17](#)
- [Language support on page 18](#)
- [Supported models on page 18](#)

## FortiManager 6.2.2 support

This section identifies FortiManager 6.2.2 product integration and support information:

- [Web browsers on page 13](#)
- [FortiOS/FortiOS Carrier on page 14](#)
- [FortiAnalyzer on page 15](#)
- [FortiAuthenticator on page 15](#)
- [FortiCache on page 15](#)
- [FortiClient on page 15](#)
- [FortiMail on page 16](#)
- [FortiSandbox on page 16](#)
- [FortiSwitch ATCA on page 16](#)
- [FortiWeb on page 16](#)
- [FortiDDoS on page 16](#)
- [Virtualization on page 17](#)



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

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



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

---

## Web browsers

This section lists FortiManager 6.2.2 product integration and support for web browsers:

- Microsoft Edge 40
- Mozilla Firefox version 69
- Google Chrome version 77

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

## FortiOS/FortiOS Carrier

This section lists FortiManager 6.2.2 product integration and support for FortiOS/FortiOS Carrier:

FortiOS or FortiOS Carrier		Compatibility Issues
6.2	6.2.0 and later	
6.0	6.0.4 to 6.0.8	FortiManager 6.2.2 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.8, with some minor interoperability issues. For information, see <a href="#">FortiManager 6.2.2 and FortiOS 6.0.8 compatibility issues on page 29</a> .
	6.0.0 to 6.0.3	FortiManager 6.0.2 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.3, with some minor interoperability issues. For information, see <a href="#">FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 29</a> .
5.6	5.6.7 to 5.6.12	FortiManager 6.2.2 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.12, with some minor interoperability issues. For information, see <a href="#">FortiManager 6.2.2 and FortiOS 5.6.12 compatibility issues on page 30</a> .
	5.6.5 to 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 <a href="#">FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 30</a> .
	5.6.4	FortiManager 5.6.3 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see <a href="#">FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 30</a> .
	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 <a href="#">FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 30</a> .
	5.6.0 to 5.6.1	FortiManager 5.6.0 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see <a href="#">FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 31</a> .
5.4	5.4.11 to 5.4.12	
	5.4.10	FortiManager 5.4.5 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.10, with some minor interoperability issues. For information, see <a href="#">FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 31</a> .
	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 <a href="#">FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 31</a> .

FortiOS or FortiOS Carrier	Compatibility Issues
5.4.1 to 5.4.8	FortiManager 6.2.2 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.8, with some minor interoperability issues. For information, see <a href="#">FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 32</a> .

## FortiAnalyzer

This section lists FortiManager 6.2.2 product integration and support for FortiAnalyzer:

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

## FortiAuthenticator

This section lists FortiManager 6.2.2 product integration and support for FortiAuthenticator:

- 6.0.0 and later
- 5.0 to 5.5
- 4.3 and later

## FortiCache

This section lists FortiManager 6.2.2 product integration and support for FortiCache:

- 4.2.9
- 4.2.7
- 4.2.6
- 4.1.6
- 4.1.2
- 4.0.4

## FortiClient

This section lists FortiManager 6.2.2 product integration and support for FortiClient:

- 6.2.1
- 6.0.8
- 6.0.0
- 5.6.6
- 5.6.3
- 5.6.0
- 5.4.0 and later

## FortiMail

This section lists FortiManager 6.2.2 product integration and support for FortiMail:

- 6.0.5
- 5.4.9
- 5.4.5
- 5.3.12

## FortiSandbox

This section lists FortiManager 6.2.2 product integration and support for FortiSandbox:

- 3.1.0
- 3.0.5
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

## FortiSwitch ATCA

This section lists FortiManager 6.2.2 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

## FortiWeb

This section lists FortiManager 6.2.2 product integration and support for FortiWeb:

- 6.1.1
- 6.0.5
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

## FortiDDoS

This section lists FortiManager 6.2.2 product integration and support for FortiDDoS:

- 5.1.0
- 5.0.0



- 4.7.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see [Feature support on page 17](#).

## Virtualization

This section lists FortiManager 6.2.2 product integration and support for virtualization:

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

## Feature support

The following table lists FortiManager feature support for managed platforms.

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

## Language support

The following table lists FortiManager language support information.

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

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

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

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.2.2.



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.

This section contains the following topics:

- [FortiGate models on page 19](#)
- [FortiGate special branch models on page 21](#)
- [FortiCarrier models on page 22](#)
- [FortiDDoS models on page 23](#)
- [FortiAnalyzer models on page 24](#)
- [FortiMail models on page 24](#)
- [FortiSandbox models on page 25](#)
- [FortiSwitch ATCA models on page 26](#)

- [FortiWeb models on page 26](#)
- [FortiCache models on page 28](#)
- [FortiProxy models on page 28](#)
- [FortiAuthenticator models on page 28](#)

## FortiGate models

Model	Firmware Version
<p><b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3600C-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC</p> <p><b>FortiWiFi:</b> FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM</p> <p><b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager</p> <p><b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D</p> <p><b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p>	6.2
<p><b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, 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-DSLJ, FG-60E-POE, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101F, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E</p>	6.0

Model	Firmware Version
<b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate DC:</b> FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC <b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FW-60E-DSL, FW-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-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, FG-5001E, FG-5001E1 <b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC, FG-7060E-8-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-50E, FG-51E, FG-60D, 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-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FGT-300D, FG-400D, FG-500D, 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 <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D <b>(Update only) FortiGate 7000 series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC, FG-7060E-8-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-50E, FWF-51E, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM <b>FortiGate Rugged:</b> FGR-60D, FGR-90D	5.4

## FortiGate special branch models

Model	Firmware Version
<b>FortiGate:</b> FortiGate-60F, FortiGate-61F, FortiGate-1100E, FortiGate-1101E <b>FortiGate Rugged:</b> FortiGateRugged-90D	6.2
<b>FortiGate:</b> Add FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC <b>FortiGate DC:</b> FortiGate-3400E-DC, FortiGate-3401E-DC <b>FortiGate VM:</b> FortiGate-VM64-RAXONDEMAND	6.0
<b>FortiGate:</b> Add FortiGate-60E-DSL, FortiGate-60E-DSLJ <b>FortiGate 5000 Series:</b> FortiGate-5001E1 <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F	5.6

Model	Firmware Version
<b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC <b>FortiWiFi:</b> FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ	
<b>FortiGate:</b> FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-500E, FortiGate-501E, FortiGate-2000E, FortiGate-2500E, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1 <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F <b>FortiGate 7000 Series:</b> FortiGate-7030EFG-7030E-Q, FortiGate-7000E, FortiGate-7030E-S, FortiGate-7040E-1, FortiGate-7040E-2, FortiGate-7040E-3, FortiGate-7040E-4, FortiGate-7040E-5, FortiGate-7040E-6, FortiGate-7040E-8, FortiGate-7040E-8-DC, FortiGate-7060E-1, FortiGate-7060E-2, FortiGate-7060E-3, FortiGate-7060E-4, FortiGate-7060E-5, FortiGate-7060E-6, FortiGate-7060E-8 <b>FortiWiFi:</b> FortiWiFi-50E-2R, FortiWiFi-60E, FortiWiFi-61E, FortiWiFi-92D, FortiWiFi-60E-DSL <b>FortiGate VM:</b> FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-OPC <b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D	5.4

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E <b>FortiGate 6000 series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

Model	Firmware Version
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E <b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-3810D-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FG-3600E, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E <b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-3810D-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
<b>FortiDDoS:</b> FI-1500E, FI-2000E	5.0
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.	6.2
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, 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-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	6.0
<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-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	5.2
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	
<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	5.0
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0



Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4
<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
<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
<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
<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

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.1
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-AWS, FSA-VM	3.0
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	2.5.2
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.1 2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.0 2.1.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.3 1.4.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-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

## FortiSwitch models

Model	Firmware Version
<b>FortiSwitch:</b> FortiSwitch-108D-POE, FortiSwitch-108D-VM, FortiSwitch-108E, FortiSwitch-108E-POE, FortiSwitch-108E-FPOE, FortiSwitchRugged-112D-POE, FortiSwitch-124D, FortiSwitch-124D-POE, FortiSwitchRugged-124D, FortiSwitch-124E, FortiSwitch-124E-POE, FortiSwitch-124E-FPOE, FortiSwitch-224D-POE, FortiSwitch-224D-FPOE, FortiSwitch-224E, FortiSwitch-224E-POE, FortiSwitch-224E-FPOE, FortiSwitch-248D, FortiSwitch-248D-POE, FortiSwitch-248D-FPOE, FortiSwitch-248E-POE, FortiSwitch-248E-FPOE, FortiSwitch-424D, FortiSwitch-424D-POE, FortiSwitch-424D-FPOE, FortiSwitch-448D, FortiSwitch-448D-POE, FortiSwitch-448D-FPOE, FortiSwitch-524D, FortiSwitch-524D-FPOE, FortiSwitch-548D, FortiSwitch-548D-FPOE, FortiSwitch-1024D, FortiSwitch-1048D, FortiSwitch-1048E, FortiSwitch-3032D, FortiSwitch-3632D	N/A  There is no fixed supported firmware versions. If FortiGate supports it, FortiManager will support it.

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVR	6.0.1
<b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-600D	5.9.1

Model	Firmware Version
<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	
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E	4.0, 4.1, 4.2
<b>FortiCache VM:</b> FCH-VM64, FCH-KVM	

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E	1.0/1.1
<b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E	4.3, 5.0-5.5, 6.0
<b>FortiAuthenticator VM:</b> FAC-VM	
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E	4.0-4.2
<b>FortiAuthenticator VM:</b> FAC-VM	

# Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.2.2. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.0	<a href="#">FortiManager 6.2.2 and FortiOS 6.0.8 compatibility issues on page 29</a>
	<a href="#">FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues on page 29</a>
FortiOS 5.6	<a href="#">FortiManager 6.2.2 and FortiOS 5.6.12 compatibility issues on page 30</a>
	<a href="#">FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues on page 30</a>
	<a href="#">FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues on page 30</a>
	<a href="#">FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues on page 30</a>
	<a href="#">FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues on page 31</a>
FortiOS 5.4	<a href="#">FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues on page 31</a>
	<a href="#">FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues on page 31</a>
	<a href="#">FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues on page 32</a>

## FortiManager 6.2.2 and FortiOS 6.0.8 compatibility issues

The following syntax introduced in FortiOS 6.0.8 is not directly supported by FortiManager 6.2.2.

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

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

## FortiManager 6.0.2 and FortiOS 6.0.3 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager 6.0.2 and FortiOS 6.0.3.

Bug ID	Description
516113	Install verification may fail on policy status field. For details, see the following Special Notice: <a href="#">Special Notices on page 7</a> .
516242	Install verification may fail on the wtp profile's <code>handoff-sta-thresh</code> parameter.

## FortiManager 6.2.2 and FortiOS 5.6.12 compatibility issues

The following syntax introduced in FortiOS 5.6.12 is not directly supported by FortiManager 6.2.2.

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

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

## FortiManager 5.6.5 and FortiOS 5.6.6 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager 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.

## FortiManager 5.6.3 and FortiOS 5.6.4 compatibility issues

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

Bug ID	Description
486921	FortiManager may not be able to support the syntax for the following objects: <ul style="list-style-type: none"> <li><code>rsso-endpoint-block-attribute</code>, <code>rsso-endpoint-block-attribute</code>, or <code>sso-attribute</code> for RADIUS users.</li> <li><code>sdn</code> and its <code>filter</code> attributes for firewall address objects.</li> <li><code>azure</code> SDN connector type.</li> <li><code>ca-cert</code> attribute for LDAP users.</li> </ul>

## FortiManager 5.6.1 and FortiOS 5.6.3 compatibility issues

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

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

## FortiManager 5.6.0 and FortiOS 5.6.0 and 5.6.1 compatibility issues

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

Bug ID	Description
451036	FortiManager may return verification error on <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.

## FortiManager 5.4.5 and FortiOS 5.4.10 compatibility issues

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

Bug ID	Description
508337	FortiManager cannot edit the following configurations for replacement message: <ul style="list-style-type: none"> <li><code>system replacemsg mail "email-decompress-limit"</code></li> <li><code>system replacemsg mail "smtp-decompress-limit"</code></li> <li><code>system replacemsg nntp "email-decompress-limit"</code></li> </ul>

## FortiManager 5.6.3 and FortiOS 5.4.9 compatibility issues

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

Bug ID	Description
486592	FortiManager may report verification failure on the following attributes for RADIUS users: <ul style="list-style-type: none"> <li><code>rsso-endpoint-attribute</code></li> <li><code>rsso-endpoint-block-attribute</code></li> <li><code>sso-attribute</code></li> </ul>

## FortiManager 5.4.4 and FortiOS 5.4.8 compatibility issues

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

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



# Resolved Issues

The following issues have been fixed in 6.2.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
412143	Renaming user in policy objects does not update SSLVPN portal mapped user.
494367	Users cannot search address in policy where the address is a part of a nested group.
500037	FortiToken provision may not work.
502967	FortiManager attempts to push the incorrect VWP name to certain VDOMs when a FortiGate has multiple VDOMs with VWPs configured and the VWP uses the same dynamic interface.
521904	Policy and Object's folders do not reflect policy package status.
522284	Access Point templates still have 5GHz channels that are not valid.
529051	Map to Policy Interface & Scan outgoing connection to Botnet Sites disappears in v6.0.3 when running FortiManager in workflow mode.
529770	Policy package integrity check provides no clarification on intended database changes.
530717	Under Policy & Objects > Policy Package > right click > add address in policy, the page is stuck on loading with Microsoft Edge.
531585	A Proxy policy's source address field should display all address objects in the search list despite the interface binding defined for the addresses.
536078	Device Manager's System->Virtual Domain cannot display more than 50 VDOMs.
537312	Event logs should not have the userfrom field when an internal process triggers the log.
537338	Policy & Objects created time and last modified timestamp reset after ADOM upgrade.
539137	User may not be able to access FortiManager using IPv6 address even if user sets IPv6 allow access on HTTPS and HTTP.
539196	FortiManager should not show FortiGuard subscription status Expired if a trial license is expired.
539928	Objects used in SD-WAN rules show as not in use in address list.
540034	There may be repetitive fmgd crashes in FortiManager crash log.
544012	Missing DHCP mode in per-device mapping for FortiSwitch VLAN interface.
544597	VLAN interface is not available for EMAC VLAN on Device Manager > System > Interfaces.
546334	Dynamic interface is not visible in policies until web page refreshes.
547007	FortiManager may incorrectly show that a script finishes running.
547052	FortiManager GUI should not allow creating Security Profiles without any SSL/SSH Inspection Profile defined.

Bug ID	Description
548027	After FortiGate upgrades, verification may fail on "set nat enabled" if "set central-nat enable" is configured.
548034	System Settings' LDAP may not work with nested directory groups.
549932	FortiManager cannot use FQDN as Proxy address.
551566	Device Detection and its related settings are not available in SSID Central Management.
552222	When running "cdb check policy-packages", FortiManager prompts central fap object not found errors.
552403	FortiManager does not reflect SD-WAN Template rule has negated source or destination.
553860	Hub-to-Hub IPsec Phase1 interface install use remote-gw as interface IP even though public IP is defined under the Advance section.
553912	FortiManager should hide the Quick Mode Selector setting if mode-cfg enabled.
554325	When creating an administrator with remote user group within Device Manager, it may prompt the error: "The remote-group "tacgroup" is not in admin user's vdom."
554901	EU country ID is available in FortiManager but is not part of latest geographical database.
555175	User may mistakenly configures FortiManager to run script against a group of targets when targeting a single device.
556985	FortiManager prompts unclear message when device configuration file is no found.
557471	FortiManager should prompt the list of firmware images for FortiGate 6000 and 7000 series.
559009	FortiManager should allow users to select SD-WAN interface on IPv6 policy.
561008	Second IP in central management removed by master FortiManager on re-connection.
561946	Upgrading FortiManager may fail due to incorrect limit for user adgrp.
563918	FortiManager should prompt more clear error when ADOM upgrade fails.
564182	FortiManager should always responds with "invalid VDOM name" when accessing FortiManager with incorrect hyperlinks.
564202	Policy package cannot export to excel when there is more than 20,000 policies.
564625	Re-importing a policy package may result in changing policy package status to "modified".
564937	FortiManager allows users not to set device type when creating a user device resulting in install failure.
565636	FortiManager may prompt verification error on Global ADOM's gall address.
565772	User may not be able to add a black hole route.
566138	FortiManager may not correctly install Application Control configurations.
566310	FortiManager is unable to push or change GeoIP override country code to FortiGate.
566390	Policy installation may fail due to FortiGuard certifications.

Bug ID	Description
567514	Multiple policies may be deleted by accident if they are selected on the background from the previous filtered result.
567770	Install custom internet service to FortiGate fails when None is selected for Master Service ID.
568626	FortiManager can only modify the order of DNS forwarder only if the IP addresses are in quotes ("" ) and when the IP addresses are not separated by comma.
568988	FortiManager is unable to create access list entries with IPv4 format based subnet mask or wild card entries.
569188	After upgrade, installation may fail on VPN configurations.
569468	Firmware version value may be incorrect in device list after upgrade.
569551	FortiManager should be able to save quotas within web filter profile.
569945	When editing a policy, Select All objects may not work when there is no object selected on a field.
569952	FortiSwitch Templates are incorrectly set mac-addr values to all zeros for all interfaces.
570109	FortiManager cannot configure fail-detect-option in interface's advanced options.
570936	AP Manager is pushing incorrect syntax for FAPU24JEV wtp-profile causing installation failure.
571164	VPN Manager has problem adding secondary WAN interface from a hub in star community.
571203	Changing interface order in SD-WAN SLA rule does not result in configuration push.
571722	AP Manager should hide WIDE profiles if they cannot be used in certain modes.
572191	Users are unable to remove ADOM when ADOM is set as a FortiAnalyzer ADOM.
572284	Policy hit counts may always show zero for FortiGate 7000 series.
572544	When creating a Managed AP, FortiManager should properly save the "Name" and "AP Profile" fields, and it should not accept FAP's serial number with lower cases.
572756	The upgrade schedule status should correctly display for all the selected devices.
573221	FortiManager should be able to use default Replacement Message Group in policy package.
573250	Find Duplicate Objects may show inaccurate results.
573710	FortiManager should not use unused user group after changing the portal type from "Authentication" to "Disclaimer Only".
574148	Upgrading ADOM from v6.0 to v6.2 may fail due to "replacement message-Web Proxy authorization fail".
574548	Upgrading ADOM from v5.6 to v6.0 may fail due to VDOM conflict in wtp.
574826	FortiManager port negotiation switches to 100 half-duplex mode after a reboot.
574847	Global objects in local ADOM should not be editable.
574988	CLI only Object cannot create router BGP AS-path list and community list, and prompts the error "entry does not exist".

Bug ID	Description
575343	Users are unable to disable the tunnel interface with IP 0.0.0.0 within Device Manager.
575349	ADOM address objects override Global objects with the same name if promoted as part of the Address Group.
575736	The dhcp-lease-time setting from AP Manager installs under “wireless-controller vap” instead of “system dhcp server”.
575823	FortiManager should not allow user to delete extra proposals when SUITE-B PRF is enabled.
576267	SSL/SSH inspection profile change does not change all related policy package status to modified.
576308	Policy package exported as CSV contains hit count data only for IPv4 but not for IPv6.
576320	Policy status of all devices used in VPN Manager is changing to 'modified' after deleted some unrelated devices.
576565	Creating VXLAN may gradually take more time.
576841	FortiSwitch VLAN template should support IPv6 and dynamic mapping of IPv6 address.
576867	FortiAnalyzer wipes out NTPv3 authentication related settings after reboot.
576999	FortiManager prompts “runtime error -999” when changing setting in IPS profile on Global ADOM.
577158	Installation may fail when SSID dynamic interface is renamed.
577183	Scripts should be able to modify fsp vlan.
577463	Script scheduling should not be affected by the order of configuration.
577939	VPN Manager may install different PSKs to gateways.
577964	FortiManager should install imported CA certificates to managed FortiGate device.
578045	FortiManager is unable to configure OSPF routes with md5 keys via CLI script.
578622	Installation may fail when creating FortiLink interface.
579075	LDAP admin user may not be able to access FortiManager when there are many LDAP groups.
579286	The default value for weight or volume-ratio should not be zero on interfaces.
579646	Global Header/Footer policy cannot use Threat Feeds.
579844	When user login with remote Radius authentication with assigned VDOM and access profile, FortiManager may not show the installation target devices.
580486	Adding ADOM fails with errorCode 102 : 'Fail to lock adom Global workspace' when workspace-mode is set to normal.
580676	FortiManager may not delete and change a policy and it affects another policy package.
580951	LDAP admin user with specific Policy Package Access set should correctly see policy package status and not "Never Installed".
582685	Web Filter Profiles with URL filter lists may take a long time to load.

Bug ID	Description
583010	Policy Block Name sets as a pre-fix to the individual Policy name for multiple times.
583467	FortiManager cannot edit the MTU parameter on an interface in Device Manager.
583741	Temporary device revision files may not be deleted.

## Common Vulnerabilities and Exposures

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

Bug ID	Description
542636	FortiManager 6.2.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2019-6695</li></ul>
569307	FortiManager 6.2.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2019-17654</li></ul>

# Known Issues

The following issues have been identified in 6.2.2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
468776	Unable to retrieve device due to <i>data not exist</i> (g-xxxx firewall object).
592646	SD-WAN monitor is blank when the monitor interface data does not match the configuration data.
603414	FortiManager shows an incorrect firmware upgrade path for the FortGate. See <a href="#">Special Notices on page 7</a> .
509665	Global v5.2 assigned to ADOM v5.4 and <code>webfilter ftgd-local-rating</code> might set to wrong category.
574731	Some hardware specific SNMP traps are missing from the device SNMP settings and the system provisioning templates.
574841	Central Management FortiSwitch Template GUI cannot assign VLANs with Microsoft Edge.
576098	The event log should may show the correct username.
576601	In the FortiGate's GUI, the VPN Phase2 selectors can be managed separately, which is completely missing in FMG -> VPN Manager -> Monitor.
576645	VPN Manager's <code>dpd-retryinterval</code> range is too small.
577199	Import policy package does not add interfaces in dynamic mapping for zone if the zone mapping is already empty.
577201	FortiManager should grey out the 'Next' button when zone validation occurs while "Re-install Policy".
577884	Deleting an unused object may change the policy package status.
578004	The policy interface colors are different in Device Manager and Policy & Objects.
578501	FortiManager does not show Global Icon for global Objects assigned to ADOMs.
578929	The warning message "input must be a number" should be displayed if an unexpected value is entered into "Heart Beat Interval" for HA.
579563	Workflow Session List menu seems to always match the first wildcard TACACS admin.
579573	FortiManager tries to delete <code>replacemsg-group</code> that is auto-created by adding tunnel SSID.
580484	Signature "Apache.Optionsbleed.Scanner" cannot be selected as IPS Signature anymore but only "Rate based Signature".
580533	Saving configuration with an incorrect IP or net mask format does not trigger an error.
580932	LVM information may show disk unused.
581140	The <code>FmDeviceEntPolicyPackageState</code> SNMP always returns (-1), which indicates never installed,

Bug ID	Description
	regardless of the actual policy package status.
581481	Handling of custom Application Control signatures may not be consistent between FortiManager and FortiGate.
581495	Interface Validation may display the interface mapping prompt multiple times for the same unmapped interface.
581812	Sorting Extenders by device Name does not work.
581825	In workflow mode, changes to the SSL VPN portals do not trigger policy package status to "Modified".
581940	SD-WAN monitor may show a visual gap when monitoring traffics.
582882	FortiManager may install duplicated members during device install.
584046	License information for FortiAnalyzer shown in Device Manager is not correct.
584118	FortiManager may not correctly keep router access-list rule default value causing subsequent installation to fail.
584392	Admin user with read-only profile should not be allowed to "Revoke Release" in DHCP query and "Bring Tunnel Down/Up" in Query IPsec.
585021	Adding or modifying rate based signature within IPS profile, FortiManager resets all rate-based signatures to default setting.
585480	SD-WAN Monitor shows No Data for Performance SLA Statistics.
586026	FortiManager should display zone icon based on existing and non-existing dynamic mappings.
586275	Policy package difference does not show user or admin details.
586450	FortiManager should check if a script is applicable to global and report an error if the script cannot be ran.
586557	Workflow session removes user group for FortiSwitch Security Policy.
586571	VPN Manager may set add-route to disable when creating a managed gateway in dial-up topology as spoke and the option to select "Add Route" is set "off".
586636	FortiManager Event Log may show policy package installed on different units.
588869	Re-install policy on FortiGate with multiple VDOMs wipes config when different VDOM in different package.
589101	When an external gateway is defined within VPN Manager, the change cannot be installed to FortiGate with the error: <i>no hub configured for vpn XXX</i> .
589240	VPN Manager GUI cannot select a VDOM when adding a managed gateway. <b>Workaround:</b> Use a CLI script to configure a managed gateway with the desired VDOM.
589269	When upgrading FortiGate, FortiManager may upgrade the device to version 6.0.3 prior to upgrading to version 6.2.2. <b>Workaround:</b> Please select the <i>Skip All Intermediate Steps in Upgrade Path if Possible</i> option when upgrading FortiGate.

## Appendix A - FortiGuard Distribution Servers (FDS)

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

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

### FortiGuard Center update support

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

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



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

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





**FORTINET®**



Copyright© 2020 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.