



FortiManager - Release Notes

Version 6.0.1

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



September 17, 2019

FortiManager 6.0.1 Release Notes

02-601-491728-20190917

TABLE OF CONTENTS

FortiManager 6.0.1 Release	5
Supported models	5
What's new	6
Central Change Management	6
AP Manager	6
FortiSwitch Manager	6
Fabric Connectors	6
System Settings	6
FortiManager ServiceNow Connector	6
Special Notices	7
Managing FortiGate with VDOMs that use Global Profiles	7
ADOM Upgrade for FortiManager 6.0	7
Reconfigure SD-WAN after Upgrade	8
FortiGate VM 16/32/UL license support	8
Hyper-V FortiManager-VM running on an AMD CPU	8
VM License (VM-10K-UG) Support	8
FortiOS 5.4.0 Support	8
SSLv3 on FortiManager-VM64-AWS	8
Upgrade Information	10
Downgrading to previous firmware versions	10
Firmware image checksums	10
FortiManager VM firmware	10
SNMP MIB files	12
Product Integration and Support	13
FortiManager 6.0.1 support	13
Feature support	16
Language support	16
Supported models	17
FortiGate models	18
FortiCarrier models	20
FortiDDoS models	21
FortiAnalyzer models	21
FortiMail models	22
FortiSandbox models	22
FortiSwitch ATCA models	23
FortiWeb models	23
FortiCache models	24
FortiAuthenticator models	24
Compatibility with FortiOS Versions	25
FortiOS 6.0.2 compatibility issues	25
FortiOS 5.6.4 compatibility issues	25
FortiOS 5.6.3 compatibility issues	26

FortiOS 5.6.0 and 5.6.1 compatibility issues	26
FortiOS 5.4.9 compatibility issues	26
FortiOS 5.2.10 compatibility issues	26
FortiOS 5.2.7 compatibility issues	27
FortiOS 5.2.6 compatibility issues	27
FortiOS 5.2.1 compatibility issues	27
FortiOS 5.2.0 compatibility issues	28
Resolved Issues	29
AP Manager	29
Device Manager	29
FortiClient Manager	30
Global ADOM	30
HA	30
Policy and Objects	31
Revision History	31
Script	32
Services	32
System Settings	32
VPN Manager	32
Workplace and Workflow	33
Others	33
Common Vulnerabilities and Exposures	33
Known Issues	35
Device Manager	35
Policy & Objects	35
Revision History	35
Script	36
Others	36
Appendix A - FortiGuard Distribution Servers (FDS)	37
FortiGuard Center update support	37
Change Log	39

FortiManager 6.0.1 Release

This document provides information about FortiManager version 6.0.1 build 0150.



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

This section includes the following topics:

- [Supported models on page 5](#)
- [What’s new on page 6](#)

Supported models

FortiManager version 6.0.1 supports the following models:

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

What's new

FortiManager version 6.0.1 includes the following new features and enhancements:



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

Central Change Management

The following Central Change Management features and enhancements have been added

AP Manager

Added AP Manager enhancements to support BlueTooth, QoS and Hotspot 2.

FortiSwitch Manager

Added Dynamic Mapping for VLANs.

Fabric Connectors

Fabric Connectors bug fixes and improvements.

System Settings

Added one click ADOM upgrade support from 5.6 ADOM > 6.0 ADOM.

FortiManager ServiceNow Connector

The Security Operations FortiManager Integration version 1.1.19 application is now available on ServiceNow store. This app enables users to respond to incidents quickly and contain security threats. For more information, see <https://store.servicenow.com>.

See also the *Security Operations FortiManager 6.0.1 Integration App 1.1 User Guide* on the [Document Library](#).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.0.1.

Managing FortiGate with VDOMs that use Global Profiles

FortiManager managing FortiGates with VDOMs enabled and running FortiOS 6.0.0 or later is unable to import global ADOM objects from FortiGate devices. Before adding the FortiGate units to FortiManager, perform the following steps to unset the global ADOM objects. After the default configurations are unset, you can successfully add the FortiGate units to FortiManager.

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

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

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

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

ADOM Upgrade for FortiManager 6.0

Upgrade is available for ADOM version 5.0 to migrate to version 5.2, 5.4, and 5.6. Currently, there is no ADOM upgrade option for ADOM version 5.6 to move to version 6.0.

Reconfigure SD-WAN after Upgrade

The SD-WAN module has been fully redesigned in FortiManager v6.0 to provide granular monitor and control. Upgrading SD-WAN settings from 5.6 to 6.0 is not supported. Please reconfigure SD-WAN after upgraded to v6.0.

FortiGate VM 16/32/UL license support

FortiOS 5.4.4 introduces new VM license types to support additional vCPUs. FortiManager 5.6.0 supports these new licenses with the prefixes of FGVM16, FGVM32, and FGVMUL.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

VM License (VM-10K-UG) Support

FortiManager 5.4.2 introduces a new VM license (VM-10K-UG) that supports 10,000 devices. It is recommended to upgrade to FortiManager 5.4.2 or later before applying the new license to avoid benign GUI issues.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.2 and later no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.2 or later.



The following ADOM versions are not affected: 5.0 and 5.2.

SSLv3 on FortiManager-VM64-AWS

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

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

end

Upgrade Information

You can upgrade FortiManager 5.6.0 through 5.6.4 directly to 6.0.1. Upgrade from 5.6.5 and later to 6.0.1 is not supported. You must upgrade from 5.6.4 and earlier.

If you are upgrading from versions earlier than FortiManager 5.6.4, you should upgrade to 5.6.4, then 6.0.1.



For 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.

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, <https://www.fortinet.com/products/management/fortimanager.html>. VM installation guides are available in the [Fortinet Document Library](#).

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 6.0.1 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.0.1 support on page 13](#)
- [Feature support on page 16](#)
- [Language support on page 16](#)
- [Supported models on page 17](#)

FortiManager 6.0.1 support

The following table lists 6.0.1 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.• Mozilla Firefox version 60• Google Chrome version 66 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS/FortiOS Carrier	<ul style="list-style-type: none">• 6.0.0 to 6.0.1 FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 6.0.0 and 6.0.1. For 6.0.2, see FortiOS 6.0.2 compatibility issues on page 25.• 5.6.4 FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.4, with some minor interoperability issues. For information, see FortiOS 5.6.4 compatibility issues on page 25.• 5.6.2 to 5.6.3 FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.2 to 5.6.3, with some minor interoperability issues. For information, see FortiOS 5.6.3 compatibility issues on page 26.• 5.6.0 to 5.6.1 FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.6.0 to 5.6.1, with some minor interoperability issues. For information, see FortiOS 5.6.0 and 5.6.1 compatibility issues on page 26.• 5.4.9 FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.9, with some minor interoperability issues. For information, see

[FortiOS 5.4.9 compatibility issues on page 26.](#)

- 5.4.1 to 5.4.8
- 5.2.8 to 5.2.13

FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.10, with some minor interoperability issues. For information, see [FortiOS 5.2.10 compatibility issues on page 26.](#)

- 5.2.7

FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see [FortiOS 5.2.7 compatibility issues on page 27.](#)

- 5.2.6

FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see [FortiOS 5.2.6 compatibility issues on page 27.](#)

- 5.2.2 to 5.2.5
- 5.2.1

FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see [FortiOS 5.2.1 compatibility issues on page 27.](#)

- 5.2.0

FortiManager 6.0.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues. For information, see [FortiOS 5.2.0 compatibility issues on page 28.](#)

FortiAnalyzer

- 6.0.0
- 5.6.0 to 5.6.3
- 5.4.0 to 5.4.4
- 5.2.0 to 5.2.10
- 5.0.0 to 5.0.13

FortiAuthenticator

- 5.2.2

FortiCache

- 4.2.7
- 4.2.6
- 4.1.2
- 4.0.0 to 4.0.4

FortiClient

- 5.6.6
- 5.6.3
- 5.6.0
- 5.4.0 and later
- 5.2.0 and later

FortiMail

- 5.4.5
- 5.3.12
- 5.2.10
- 5.1.7
- 5.0.10

FortiSandbox

- 2.5.0 to 2.5.2
- 2.4.0 and 2.4.1
- 2.3.2 and 2.3.3
- 2.2.2
- 2.1.3
- 2.0.3
- 1.4.0 and later
- 1.3.0
- 1.2.0 and later

FortiSwitch ATCA

- 5.2.3
- 5.0.0 and later
- 4.3.0 and later
- 4.2.0 and later

FortiWeb

- 5.9.1
- 5.8.6
- 5.8.3
- 5.8.1
- 5.8.0
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1
- 5.3.9
- 5.2.4
- 5.1.4
- 5.0.6

FortiDDoS

- 4.5.0
- 4.4.1
- 4.2.3
- 4.1.11

Limited support. For more information, see [FortiManager 6.0.1 support on page 13](#).

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



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			✓	✓
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	✓	✓

Language	GUI	Reports
Korean	✓	✓
Portuguese		✓
Spanish		✓

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

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages and import the language translation files into FortiManager by using one of the following commands:

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.0.1.



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 18](#)
- [FortiCarrier models on page 20](#)
- [FortiDDoS models on page 21](#)
- [FortiAnalyzer models on page 21](#)
- [FortiMail models on page 22](#)
- [FortiSandbox models on page 22](#)
- [FortiSwitch ATCA models on page 23](#)
- [FortiWeb models on page 23](#)
- [FortiCache models on page 24](#)
- [FortiAuthenticator models on page 24](#)

FortiGate models

Model	Firmware Version
<p>FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, 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, FG200D, 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-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E</p> <p>FortiGate 5000 Series: FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG1500D-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</p> <p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>FortiWiFi: FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D</p> <p>FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen</p> <p>FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	6.0
<p>FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-60E-DSL, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E,</p> <p>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC</p> <p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p>	5.6

Model	Firmware Version
FortiWiFi: FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1 FortiGate 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiGate 7000 Series: FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC Note: All license-based LENC is supported based on the FortiGate support list. FortiWiFi: FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM FortiGate Rugged: FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

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

FortiCarrier models

Model	Firmware Version
FortiCarrier: 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 FortiCarrier DC: FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3800D-DC, FCR-3810D-DC, FCR-3815D-DC FortiCarrier VM: FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D	5.2

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

FortiDDoS models

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

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E FortiMail Low Encryption: FE-3000C-LENC	5.4.5
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B FortiMail Low Encryption: FE-3000C-LENC FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.12
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.10
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B FortiMail VM: FE-VM64	5.1.7
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B FortiMail VM: FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0.3 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ATCA models

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

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.9.1
FortiWeb VM: FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.8.6
FortiWeb VM: FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.7.2
FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.6.1
FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	5.5.6
FortiWeb VM: FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	
FortiWeb: 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

Model	Firmware Version
FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVEN, FWB-HYPERV	
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVEN, and FWB-HYPERV	5.3.9
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVEN	5.2.4

FortiCache models

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

FortiAuthenticator models

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

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.0.1. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.0	FortiOS 6.0.2 compatibility issues on page 25
FortiOS 5.6	FortiOS 5.6.4 compatibility issues on page 25
	FortiOS 5.6.3 compatibility issues on page 26
	FortiOS 5.6.0 and 5.6.1 compatibility issues on page 26
FortiOS 5.4	FortiOS 5.4.9 compatibility issues on page 26
FortiOS 5.2	FortiOS 5.2.10 compatibility issues on page 26
	FortiOS 5.2.7 compatibility issues on page 27
	FortiOS 5.2.6 compatibility issues on page 27
	FortiOS 5.2.1 compatibility issues on page 27
	FortiOS 5.2.0 compatibility issues on page 28

FortiOS 6.0.2 compatibility issues

Bug ID	Description
504469	FortiManager fails to import policy and objects from FortiGate 6.0.2 devices. Note: FortiManager 6.0.2 release will fully support FortiGate 6.0.2 devices.

FortiOS 5.6.4 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 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">• <code>rsso-endpoint-block-attribute</code>, <code>rsso-endpoint-block-attribute</code>, or <code>sso-attribute</code> for RADIUS users.• <code>sdn</code> and its <code>filter</code> attributes for firewall address objects.• <code>azure</code> SDN connector type.• <code>ca-cert</code> attribute for LDAP users.

FortiOS 5.6.3 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 and FortiOS 5.6.3.

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

FortiOS 5.6.0 and 5.6.1 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 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.

FortiOS 5.4.9 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 and FortiOS 5.4.9.

Bug ID	Description
486592	FortiManager may report verification failure on the following attributes for RADIUS users: <code>rsso-endpoint-attribute</code> <code>rsso-endpoint-block-attribute</code> <code>sso-attribute</code>

FortiOS 5.2.10 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 and FortiOS 5.2.10.

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

FortiOS 5.2.7 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 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.

FortiOS 5.2.6 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 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.

FortiOS 5.2.1 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager version 6.0.1 and FortiOS version 5.2.1.

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

FortiOS 5.2.0 compatibility issues

The following table lists known interoperability issues that have been identified with FortiManager version 6.0.1 and FortiOS version 5.2.0.

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

Resolved Issues

The following issues have been fixed in 6.0.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
399726	Users may not be able to delete the last AP.
450434	FortiManager may unset <code>wtp-mode</code> after users change AP config from AP Manager.
455177	<i>Advanced Options</i> may not be available in the central FortiAP config page.
462857	Following changes in an AP profile, FortiManager may install unrelated local user group and radius server to VDOM root.
464811	Updated AP name may get reverted back to its default name if users do not install the change for a period of time.
481651	<code>fapc-compatibility</code> may be unset.

Device Manager

Bug ID	Description
408280	FortiManager may show FortiGate mobile token status as <i>Unknown</i> while it is <i>Pending</i> .
434101	FortiManager is missing <i>Endpoint Control</i> replacement message in device configuration and system template.
448102	There may be an error displayed when users try to modify CLI-Only objects under <i>System > HA</i> .
460403	FortiManager may not be able to automatically generate an interface of type <code>vxlان</code> .
463169	<code>set apn</code> is not available in device db under <code>system lte-modem</code> for FortiWiFi-30E-3G4G-INTL.
467773	All zones are displayed in every FortiGate.
474245	Policy Install fails due to <code>set disk-usage log</code> command inconsistency.
477009	VM Meter may not show both Master and Slave licensing information in the GUI.
479258	After adding and importing a new device, other devices may have <i>Modified</i> policy package status.
480290	Users may be able to change VDOM of aggregated/redundant interfaces.

Bug ID	Description
480541	When <code>long-vdom-name</code> is not enabled, the GUI error pop up message may be empty when users create a VDOM with name longer than 11 characters.
482018	<i>Others</i> interfaces may not show up after collapsing.
482033	FortiManager should use the same GUI style for the Column Name as <i>Source</i> & <i>Destination</i> under Policy route.
484600	FortiManager may not support enable/disable routes in Device Manager.
485722	Diffie-Hellman Groups 30, 29, 28, 27 and GCM encryption algorithms may be missing in IPsec Phase 2.
486042	FortiManager GUI may allow assigning zone bundled interfaces as SD-WAN link members.
486515	Users may be unable to change upload-option for <code>fortianalyzer2</code> .
491102	Password expiration date is set for new administrators even though the feature is disabled.

FortiClient Manager

Bug ID	Description
366095	Users may be unable to move a FortiClient profile from the GUI.

Global ADOM

Bug ID	Description
460461	The IPS package database version on Global ADOM may not be displayed in command <code>diagnose dvm adom list</code> .
470486	Automatic-Install may fail to detect changes to push to ADOMs.
482925	Internet Service destination is not displayed in IPv4 Header/Footer Policy in Global ADOM.

HA

Bug ID	Description
414616	Hostname may not be updated when users promote Slave device to be Master in FortiGate cluster.
465503	Installation to a FortiGate HA may fail after an HA failover.
480462	FortiManager Slave may fail to sync when users add a bunch of admin users on the Master.

Policy and Objects

Bug ID	Description
290293	Zone default mapping may be missing <i>Block intra-zone traffic</i> option.
442307	When users try to search for an address object, the address group that includes the address may not show up in the search result.
444671	GUI may not display <code>logtraffic-start</code> policy settings.
450922	IPS sensor with more than 8192 signature entries may be created.
459314	Users can delete used objects without options to disable it.
459655	Per-device mapping firewall address value changes may not change policy package status to <i>Modified</i> .
463920	Address groups should highlight the addresses searched.
471030	FortiManager allows users to use <i>Wildcard</i> entries under Web Rating Overrides.
472825	Web Filter profile may not be changed in Explicit Proxy Policy when profile name contains +.
475241	Users may be unable to clone global assigned FSSO objects in local ADOMs.
475496	Source, destination and services may not be ordered alphabetically in policy package.
475594	Users may be not able to create new firewall service custom objects due to the table size limit.
478915	Objects panel cannot be completely minimized.
481560	There is no validation check for FQDN addresses.
482361	After users rename a section, there may be one policy left under the old section name.
484261	Users may be unable to remove FSSO server2/3/4/5 with per-device mappings.
485687	Central NAT policy package installation may not follow the same logic that used in regular policy packages.
487123	Users may fail to add multiple Health Check in a Per-Device Mapping Virtual Server object.

Revision History

Bug ID	Description
478606	The preview of a VDOM may show commands from other VDOMs.
480723	Copying may not work when a webfilter and an URL filter share the same name.
481383	FortiManager tries to set <code>max-miss-heartbeats</code> for FortiSwitch ports.
486536	Installation may fail due to <code>vip overlap</code> error with FQDN VIP.

Bug ID	Description
487117	FortiManager may try to install <code>ssl-hpkp-age</code> and <code>ssl-hsts-age</code> despite it being disabled.
487833	Installation may fail for VIP policies with a zone as a source interface.

Script

Bug ID	Description
471661	Advanced Device Filters may be displayed when users are editing CLI script.
480982	Progress bar for installing script may not work if the admin user has <i>None</i> access to <code>import-policy-packages</code> .

Services

Bug ID	Description
452732	Changing FDS/FGD schedule update and polling frequency may not work.
483670	FortiManager may not download image from FortiGuard to upgrade the FortiGate's firmware.
485720	FOSVM licenses may be updated when FortiManager's FortiMeter license changes.

System Settings

Bug ID	Description
354283	The error message may be unclear when users try to delete a login admin session.
481018	DST change may be incorrect for Israel.
485392	Unclear error messages may be displayed after adding a FortiAnalyzer into Device Manager.

VPN Manager

Bug ID	Description
484608	Dialup VPN configuration may fail when peer type is set to <i>dialup group</i> .
487098	Random auto-generated PSK may be identical in two separate VPN Manager topologies.

Workplace and Workflow

Bug ID	Description
478444	Policy package status may not change to <i>Modified</i> in workflow mode.

Others

Bug ID	Description
471095	ADOM upgrade may fail because of webfilter URLfilter.
476643	Signature list may not be listed in extended database mode.
480551	SNMPwalk may fail with <code>Error: OID not increasing: IP-MIB::ipAdEntAddr</code> .
480577	GUI may get stuck at <i>Temporarily Unavailable</i> upon upgrading.
481763	<code>diagnose cdb upgrade check</code> may not fix all errors for <code>objcfg-intergrity</code> .
481901	There is no way for users to reset the hit count for all ADOMs and <code>dbcache</code> .
485906	The <code>admin_server_cert</code> may not work in FIPS mode.

Common Vulnerabilities and Exposures

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

Bug ID	Description
464795	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2017-17541
468740	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-1351
473644	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-1354
474994	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-1355
479513	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-1065
480025	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-7492

Bug ID	Description
482793	FortiManager6.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2018-0739

Known Issues

The following issues have been identified in 6.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
487425	Policy Package status may incorrectly change when making changes to a package has device groups as target.
494537	FortiManager incorrectly moves the virtual switch-interface to the root VDOM when directly changing the interface configurations on FortiGate.
494923	The IKE version buttons are greyed out on an existing tunnel and the version can only be changed via CLI-only options.
495013	Device should not show up as <i>Modified</i> after installation.

Policy & Objects

Bug ID	Description
493227	FortiManager should be able to specify which traffic shaper policy will be installed on a specific device.
493484	FortiManager cannot support IPS signatures with unknown options; returns an error.
494108	When adding or removing an interface from a zone, <code>block intra-zone traffic</code> should not be unset.
494367	FortiManager cannot search addresses within nested groups.
494403	Changing RSSO Agent should be possible to install without the need to make other configuration changes.

Revision History

Bug ID	Description
491448	Install policy package with a FortiManager HA may fail on slave devices.

Script

Bug ID	Description
486445	Scheduled TCL scripts may fail when using a wildcard RADIUS user.

Others

Bug ID	Description
494072	The <i>Central DNAT</i> option is incorrectly translated to <i>Central SNAT</i> when Japanese is selected as the language for the Web GUI.
494586	The <code>svc cdb reader daemon</code> consumes high CPU resources when viewing VPN Phase 2 configuration.
494953	The <i>View</i> button in the <i>Where Used</i> dialog may not display the correct entries if sections are not expanded.

Appendix A - FortiGuard Distribution Servers (FDS)

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

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

FortiGuard Center update support

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

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

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



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

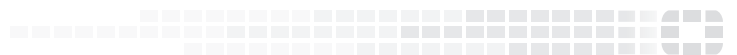
```
config fmupdate support-pre-fgt-43
  set status enable
end
```

Change Log

Date	Change Description
2018-06-07	Initial release of 6.0.1.
2018-06-26	Added 473644 and 474994 to <i>Resolved Issues</i> .
2018-06-27	Added note to <i>Product Integration > Supported Models > FortiGate Models > 6.0 > FortiGate Hardware Low Encryption</i> .
2018-07-06	Updated <i>What's New</i> to include <i>FortiManager ServiceNow Connector</i> . Added 464795 to <i>Resolved Issues > Common Vulnerabilities and Exposures</i> .
2018-07-13	Updated <i>Product Integration and Support > Language Support</i> to clarify that you can create your own language translation files for Russian, Hebrew, and Hungarian, and import the language translation files into FortiManager by using the CLI.
2018-07-27	Added FortiOS 6.0.2 to <i>Compatibility with FortiOS Versions</i> .
2018-08-30	Updated FortiMail support in <i>FortiManager 6.0.0 Support</i> .
2018-09-07	Updated <i>Product Integration and Support > FortiManager 6.0.0 Support > Virtualization</i> .
2018-11-01	Clarified supported upgrade path.
2019-09-17	Added a special notice.



FORTINET®



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.