

Release Notes

FortiManager 7.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 10th, 2024

FortiManager 7.2.0 Release Notes

02-720-783051-20241210

TABLE OF CONTENTS

Change Log	6
FortiManager 7.2.0 Release	7
Supported models	7
FortiManager VM subscription license	7
Management extension applications	8
Supported models for MEA	8
Minimum system requirements	8
Special Notices	10
FortiManager 7.2.3 and later firmware on FortiGuard	10
SD-WAN Orchestrator removed in 7.2	10
Changes to FortiManager meta fields	10
Access lists as ADOM-level objects	11
View Mode is disabled in policies when policy blocks are used	11
Reconfiguring Virtual Wire Pairs (VWP)	11
Scheduling firmware upgrades for managed devices	11
Modifying the interface status with the CLI	11
ADOM upgrade for FortiManager 7.2	12
SD-WAN with upgrade to 7.0	12
Citrix XenServer default limits and upgrade	12
Multi-step firmware upgrades	12
Hyper-V FortiManager-VM running on an AMD CPU	13
SSLv3 on FortiManager-VM64-AWS	13
Upgrade Information	14
Downgrading to previous firmware versions	14
Firmware image checksums	14
FortiManager VM firmware	15
SNMP MIB files	16
Product Integration and Support	17
Supported software	17
Web browsers	18
FortiOS and FortiOS Carrier	18
FortiADC	18
FortiAnalyzer	18
FortiAuthenticator	18
FortiCache	19
FortiClient	19
FortiDDoS	19
FortiDeceptor	19
FortiFirewall and FortiFirewallCarrier	19
FortiMail	19
FortiProxy	20
FortiSandbox	20

FortiSOAR	20
FortiSwitch ATCA	20
FortiTester	21
FortiWeb	21
Virtualization	21
Feature support	21
Language support	22
Supported models	23
FortiGate models	23
FortiGate special branch models	26
FortiCarrier models	28
FortiADC models	29
FortiAnalyzer models	29
FortiAuthenticator models	30
FortiCache models	30
FortiDDoS models	31
FortiDeceptor models	31
FortiFirewall models	31
FortiFirewallCarrier models	31
FortiMail models	32
FortiProxy models	32
FortiSandbox models	32
FortiSOAR models	32
FortiSwitch ATCA models	33
FortiTester models	33
FortiWeb models	33
Compatibility with FortiOS Versions	35
FortiManager 7.2.0 and FortiOS 7.0.8 compatibility issues	35
Resolved Issues	38
AP Manager	38
Device Manager	38
Global ADOM	39
Others	40
Policy and Objects	40
Revision History	41
Script	42
Services	42
System Settings	42
VPN Manager	43
Known Issues	44
AP Manager	44
Device Manager	44
Others	45
Policy & Objects	45
Revision History	46
Script	46

Services	47
System Settings	47
VPN Manager	47
Appendix A - FortiGuard Distribution Servers (FDS)	48
FortiGuard Center update support	48
Appendix B - Default and maximum number of ADOMs supported	49
Hardware models	49
Virtual Machines	49

Change Log

Date	Change Description
2022-04-11	Initial release.
2022-04-19	Updated Special Notices on page 10 .
2022-05-04	Updated FortiAnalyzer models on page 29 .
2022-05-20	Updated Known Issues on page 44 and Resolved Issues on page 38 .
2022-07-07	Updated Upgrade Information on page 14 .
2022-07-19	Updated Upgrade Information on page 14 .
2022-08-23	Updated Special Notices on page 10 .
2022-08-26	Updated Upgrade Information on page 14 .
2022-08-29	Updated Special Notices on page 10 .
2022-10-20	Added 841187 to Known Issues on page 44 and added FortiManager 7.2.0 and FortiOS 7.0.8 compatibility issues on page 35 .
2022-10-28	Updated FortiProxy on page 20 .
2022-11-03	Updated FortiGate models on page 23 .
2022-11-16	Updated FortiSandbox on page 20 .
2022-11-23	Updated FortiGate special branch models on page 26 .
2022-11-30	Updated Appendix A - FortiGuard Distribution Servers (FDS) on page 48 .
2023-09-25	Updated FortiClient on page 19 .
2024-01-05	Added the <i>FortiManager 7.2.3 and later firmware on FortiGuard</i> Special Notice.
2024-03-11	Updated Special Notices on page 10 : Access lists as ADOM-level objects.
2024-12-03	Updated Special Notices on page 10 .
2024-12-10	Updated Supported models on page 7 with information about access to FortiManager container versions.

FortiManager 7.2.0 Release

This document provides information about FortiManager version 7.2.0 build 1124.



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 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 8](#)

Supported models

FortiManager version 7.2.0 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-IBM, FMG-VM64-HV (including Hyper-V 2016, 2019, and 2022), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).



For access to container versions of FortiManager, contact [Fortinet Support](#).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 15](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 49](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.2.0.



FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiManager 7.0 Ports Guide](#).

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-IBM, FMG-VM64-HV (including Hyper-V 2016, 2019, and 2022), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	<ul style="list-style-type: none"> • 8 vCPU • 32 GB RAM • 500 GB disk storage 	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAuthenticator	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
FortiPortal	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
FortiSigConverter	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
FortiSOAR	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM • 500 GB disk storage 	<ul style="list-style-type: none"> • 16 vCPU • 64 GB RAM • No change for disk storage
Policy Analyzer	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
Universal Connector	<ul style="list-style-type: none"> • 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage 	No change
Wireless Manager (FortiWLM)	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.2.0.

FortiManager 7.2.3 and later firmware on FortiGuard

Starting in FortiManager 7.2.1, a setup wizard executes to prompt the user for various configuration steps and registration with FortiCare. During the execution, the FortiManager unit attempts to communicate with FortiGuard for a list of FortiManager firmware images currently available on FortiGuard – older and newer.

In the case of FortiManager 7.2.2, a bug in the GUI prevents the wizard from completing and prevents the user from accessing the FortiManager unit. The issue has been fixed in 7.2.3 and later and a CLI command has been added to bypass the setup wizard at login time.

```
config system admin setting
    set firmware-upgrade-check disable
end
```

Fortinet has not uploaded FortiManager 7.2.3 and later firmware to FortiGuard in order to work around the GUI bug, however, the firmware is available for download from the [Fortinet Support website](#).

SD-WAN Orchestrator removed in 7.2

Starting in 7.2.0, the SD-WAN Orchestrator is no longer available in FortiManager. Instead, you can use the *SD-WAN Overlay Template* wizard to configure your SD-WAN overlay network.

For more information, see [SD-WAN Overlay Templates](#) in the FortiManager Administration Guide.

Changes to FortiManager meta fields

Beginning in 7.2.0, FortiManager supports policy object metadata variables.

When upgrading from FortiManager 7.0 to 7.2.0 and later, FortiManager will automatically create ADOM-level metadata variable policy objects for meta fields previously configured in System Settings that have per-device mapping configurations detected. Objects using the meta field, for example CLI templates, are automatically updated to use the new metadata variable policy objects.

Meta fields in *System Settings* can continue to be used as comments/tags for configurations.

For more information, see [ADOM-level meta variables for general use in scripts, templates, and model devices](#).

Access lists as ADOM-level objects

Starting in 7.2.0, FortiManager supports IPv4 and IPv6 access list firewall policies as ADOM-level object configurations from FortiGate. Previously, these access lists were controlled by the device database/FortiGate configuration.

After upgrading to 7.2.0 from an earlier release, the next time you install changes to a FortiGate device with an IPv4 or IPv6 access list firewall policy (`config firewall acl/acl6`), FortiManager will purge the device database/FortiGate configuration which may have previously contained the access list.

To address this, administrators can re-import the FortiGate policy configuration to an ADOM's policy package or re-create the IPv4/IPv6 access list firewall policy in the original package.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain policies with multiple interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

Reconfiguring Virtual Wire Pairs (VWP)

A conflict can occur between the ADOM database and device database when a Virtual Wire Pair (VWP) is installed on a managed FortiGate that already has a configured VWP in the device database. This can happen when an existing VWP has been reconfigured or replaced.

Before installing the VWP, you must first remove the old VWP from the device's database, otherwise a policy and object validation error may occur during installation. You can remove the VWP from the device database by going to *Device Manager > Device & Groups*, selecting the managed device, and removing the VWP from *System > Interface*.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from `up/down` to `enable/disable`.

For example:

```
config system interface
edit port2
```

```
set status <enable/disable>
next
end
```

ADOM upgrade for FortiManager 7.2

Currently, there is no ADOM upgrade option for ADOM version 7.0 to move to version 7.2. In order to manage FortiGates running 7.2, please add the devices to a 7.2 ADOM.

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```
2. Confirm the setting is in effect by running `xenstore-ls`.

```
limits = ""
pv-kernel-max-size = "33554432"
pv-ramdisk-max-size = "536,870,912"
boot-time = ""
```

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

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.

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



Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM.

See [FortiManager 7.2.0 Upgrade Guide](#).

You can upgrade FortiManager 7.0.1 or later to 7.2.0.



Before upgrading FortiManager, check ADOM versions. Check the ADOM versions supported by the destination firmware and the current firmware. If the current firmware uses ADOM versions not supported by the destination firmware, upgrade ADOM versions in FortiManager before upgrading FortiManager to the destination firmware version.

For example, FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0, but FortiManager 7.2 supports ADOM versions 6.4, 7.0, and 7.2. Before you upgrade FortiManager 7.0 to 7.2, ensure that all ADOM 6.2 versions have been upgraded to ADOM version 6.4 or later. See [FortiManager 7.2.0 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 14](#)
- [Firmware image checksums on page 14](#)
- [FortiManager VM firmware on page 15](#)
- [SNMP MIB files on page 16](#)

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade 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, go to *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, Amazon AWSOnDemand, 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.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

Linux KVM

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

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_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.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

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 Data Sheet](#) available on the Fortinet web site. 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 7.2.0 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:

- [Supported software on page 17](#)
- [Feature support on page 21](#)
- [Language support on page 22](#)
- [Supported models on page 23](#)

Supported software

FortiManager 7.2.0 supports the following software:

- [Web browsers on page 18](#)
- [FortiOS and FortiOS Carrier on page 18](#)
- [FortiADC on page 18](#)
- [FortiAnalyzer on page 18](#)
- [FortiAuthenticator on page 18](#)
- [FortiCache on page 19](#)
- [FortiClient on page 19](#)
- [FortiDDoS on page 19](#)
- [FortiDeceptor on page 19](#)
- [FortiFirewall and FortiFirewallCarrier on page 19](#)
- [FortiMail on page 19](#)
- [FortiProxy on page 20](#)
- [FortiSandbox on page 20](#)
- [FortiSOAR on page 20](#)
- [FortiSwitch ATCA on page 20](#)
- [FortiTester on page 21](#)
- [FortiWeb on page 21](#)
- [Virtualization on page 21](#)



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

FortiManager 7.2.0 supports the following web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 96
- Google Chrome version 97

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

FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.2.0 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiOS](#).

FortiManager 7.2.0 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0
- 7.0.0 to 7.0.9
- 6.4.0 to 6.4.10

FortiADC

FortiManager 7.2.0 supports the following versions of FortiADC:

- 7.0.0 and later
- 6.2.0 and later
- 6.1.0 and later

FortiAnalyzer

FortiManager 7.2.0 supports the following versions of FortiAnalyzer:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiAuthenticator

FortiManager 7.2.0 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

FortiCache

FortiManager 7.2.0 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

FortiClient

FortiManager 7.2.0 supports the following versions of FortiClient:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later
- 6.2.1 and later

FortiDDoS

FortiManager 7.2.0 supports the following versions of FortiDDoS:

- 6.3.0 and later
- 6.2.0 and later
- 6.1.0 and later

Limited support. For more information, see [Feature support on page 21](#).

FortiDeceptor

FortiManager 7.2.0 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later
- 3.3 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.2.0 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiMail

FortiManager 7.2.0 supports the following versions of FortiMail:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiProxy

FortiManager 7.2.0 supports configuration management for the following versions of FortiProxy:

- 7.0.2



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 21](#).

FortiManager 7.2.0 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.5
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

FortiSandbox

FortiManager 7.2.0 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later
- 3.1.0 and later

FortiSOAR

FortiManager 7.2.0 supports the following versions of FortiSOAR:

- 7.0.0 and later
- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

FortiManager 7.2.0 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiTester

FortiManager 7.2.0 supports the following versions of FortiTester:

- 7.0.0 and later
- 4.2.0 and later
- 4.1.0 and later

FortiWeb

FortiManager 7.2.0 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

Virtualization

FortiManager 7.2.0 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
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 *FortiManager 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 7.2.0.



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 23](#)
- [FortiGate special branch models on page 26](#)
- [FortiCarrier models on page 28](#)
- [FortiADC models on page 29](#)
- [FortiAnalyzer models on page 29](#)
- [FortiAuthenticator models on page 30](#)
- [FortiCache models on page 30](#)
- [FortiDDoS models on page 31](#)
- [FortiDeceptor models on page 31](#)
- [FortiFirewall models on page 31](#)
- [FortiFirewallCarrier models on page 31](#)
- [FortiMail models on page 32](#)
- [FortiProxy models on page 32](#)
- [FortiSandbox models on page 32](#)
- [FortiSOAR models on page 32](#)
- [FortiSwitch ATCA models on page 33](#)
- [FortiTester models on page 33](#)
- [FortiWeb models on page 33](#)

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see [FortiGate special branch models on page 26](#).

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500E, FortiGate-501E, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-ARM64-KVM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.2
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	7.0

Model	Firmware Version
FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-ARM64-KVM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiGate Hardware Low Encryption: FortiGate-100D-LENC FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM	6.4

Model	Firmware Version
FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.2.0 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 23](#).

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	7.0	Build 291 and special branch 4334
FortiGate-3500F FortiGate-3501F	7.0	Build 294 and special branch 4344
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	7.0	Build 291 and special branch 4334
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	7.0	Build 291 and special branch 4334
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC	7.0	Build 291 and special branch 4334

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.4.8	6165
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.4.8	6165
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.4.8	6165
FortiGate-80F-POE, FortiGate-81F-POE	6.4.7	5944
FortiWiFi-80F-2R FortiWiFi-81F-2R	6.4.7	5944

FortiGate Model	FortiOS Version	FortiOS Build
FortiWiFi-81F-2R-3G4G-POE FortiWiFi-81F-2R-POE		
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC	6.4.6	5868
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	6.4.6	1766
FortiGate-7000E, FortiGate-7000F	6.4.6	1766

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.10	5168
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

FortiCarrier models

[illegible]

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier 6K and 7K: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7000F, FortiCarrier-7121F, FortiCarrier-7121F-2 FortiCarrier 6K and 7K DC: FortiCarrier-6000F-DC, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC, FortiCarrier-7060E-8-DC, FortiCarrier-7121F-DC, FortiCarrier-7121F-2-DC FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALL, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	7.0
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	6.2
FortiADC: FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	6.0, 6.1

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FAZ-3700G.	7.2

Model	Firmware Version
FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E FortiAuthenticator VM: FAC-VM	6.2, 6.3, 6.4

FortiCache models

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-2000F	6.3
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS VM: FortiDDoS-VM	6.1, 6.2, 6.3

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.1
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.0
FortiDeceptor: FDC-1000F, FDC-3000D FortiDeceptor VM: FDC-VM	3.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.2.0 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	6.2	1262
FortiFirewall: FortiFirewall-4200F	6.2.7	5141
FortiFirewall: FortiFirewall-4400F	6.2.7	5148

FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.2.0 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E FortiMail VM: FML-VM, FortiMail Cloud	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E FortiMail VM: FML-VM, FortiMail Cloud	6.2, 6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FortiProxy-KVM, FortiProxy-VM64	1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FSA-VM	3.1, 3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	6.0, 6.4, 7.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
FortiSwitch-ATCA: FS-5003A, FS-5003B FortiController: FTCL-5103B	5.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.1

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F	6.4, 7.0

Model	Firmware Version
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E	6.3
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.2.0.

FortiManager 7.2.0 and FortiOS 7.0.8 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.0 and FortiOS 7.0.8 in mantis 841187. FortiOS 7.0.8 includes syntax changes not supported by FortiManager 7.2.0.

- `system ddns ddns-key` **changed from user to passwd_aes256**
- `system dhcp server ddns-key` **changed from user to passwd_aes256**
- `system mobile-tunnel n-mhae-key` **changed from user to passwd_aes256**

The following default values changed:

- `router bgp neighbor allowas-in` **default value changed from 0 to 3**
- `router bgp neighbor allowas-in6` **default value changed from 0 to 3**
- `router bgp neighbor-group allowas-in` **default value changed from 0 to 3**
- `router bgp neighbor-group allowas-in6` **default value changed from 0 to 3**
- `system external-resource user-agent` **default value changed from curl/7.58.0 to not specified**
- `system ftm-push server-cert` **default value changed from self-sign to Fortinet_Factory**
- `system npu default-qos-type` **default value changed from policing to shaping**
- `system npu policy-offload-level` **default value changed from full-offload to disable**

The following objects were added:

```
(attr) antivirus profile cifs fortindr
      (attr) antivirus profile fortindr-error-action
      (attr) antivirus profile fortindr-timeout-action
      (attr) antivirus profile ftp fortindr
      (attr) antivirus profile http fortindr
      (attr) antivirus profile http unknown-content-encoding
      (attr) antivirus profile imap fortindr
      (attr) antivirus profile nntp fortindr
      (attr) antivirus profile pop3 fortindr
      (attr) antivirus profile smtp fortindr
      (attr) antivirus profile ssh fortindr
      (attr) endpoint-control fctems dirty-reason
      (attr) endpoint-control fctems ems-id
      (attr) endpoint-control fctems out-of-sync-threshold
      (attr) endpoint-control fctems serial-number
      (attr) endpoint-control fctems status
      (attr) firewall access-proxy-virtual-host replacemsg-group
      (attr) firewall ippool subnet-broadcast-in-ippool
      (attr) firewall profile-protocol-options ftp explicit-ftp-tls
      (attr) firewall vip6 ndp-reply
      (attr) log threat-weight malware fortindr
      (attr) switch-controller igmp-snooping query-interval
```

```

(attr) system external-resource server-identity-check
(node) system fortindr
(attr) system global ip-fragment-mem-thresholds
(attr) system sdn-connector external-account-list external-id
(attr) system settings nat46-force-ipv4-packet-forwarding
(attr) system settings nat64-force-ipv6-packet-forwarding
(attr) vpn ipsec phase1 fgsp-sync
(attr) vpn ipsec phase1-interface fgsp-sync
(attr) wireless-controller vap sae-h2e-only
(attr) wireless-controller vap sae-pk
(attr) wireless-controller vap sae-private-key
(attr) wireless-controller vap sticky-client-threshold-6g

```

The following objects were removed:

```

(attr) antivirus profile cifs fortiai
      (attr) antivirus profile fortiai-error-action
      (attr) antivirus profile fortiai-timeout-action
      (attr) antivirus profile ftp fortiai
      (attr) antivirus profile http fortiai
      (attr) antivirus profile imap fortiai
      (attr) antivirus profile mapi fortiai
      (attr) antivirus profile nntp fortiai
      (attr) antivirus profile pop3 fortiai
      (attr) antivirus profile smtp fortiai
      (attr) antivirus profile ssh fortiai
      (attr) antivirus settings cache-clean-result
      (attr) firewall vip6 arp-reply
      (attr) log threat-weight malware fortiai
      (attr) system automation-trigger ioc-level
      (attr) system cluster-sync ike-heartbeat-interval
      (attr) system cluster-sync ike-monitor
      (attr) system cluster-sync ike-monitor-interval
      (attr) system cluster-sync ike-use-rfc6311
(node) system fortiai

```

Additional option changes:

```

extender-controller extender-profile model
  option-list (tag|opt): None -> ["FX04DI", "FX04DN"]
switch-controller managed-switch ports speed
  option-list (tag|opt): ["10000", "1000fiber", "25000cr4", "25000sr4", "40000",
"5000full"] -> None (102 platforms: excludes 5001E1,5001E)
  option-list (tag|opt): None -> ["10000full", "1000full-fiber", "25000cr", "25000sr",
"40000cr4", "40000full", "40000sr4", "50000cr", "50000sr", "5000auto"] (102 platforms:
excludes 5001E1,5001E)
wireless-controller setting country
  option-list (tag|opt): None -> ["MN"]
wireless-controller wtp radio-1 band
  option-list (tag|opt): None -> ["802.11ax-6G"]
wireless-controller wtp radio-2 band
  option-list (tag|opt): None -> ["802.11ax-6G"]
wireless-controller wtp radio-3 band
  option-list (tag|opt): None -> ["802.11ax-6G"]
wireless-controller wtp radio-4 band
  option-list (tag|opt): None -> ["802.11ax-6G"]
wireless-controller wtp-group platform-type
  option-list (tag|opt): None -> ["231FL", "231G", "233G", "431FL", "431G", "432FR",

```



```
"433FL", "433G", "U231G", "U441G"]
  wireless-controller wtp-profile ap-country
    option-list (tag|opt): None -> ["MN"]
  wireless-controller wtp-profile platform type
    option-list (tag|opt): None -> ["231FL", "231G", "233G", "431FL", "431G", "432FR",
"433FL", "433G", "U231G", "U441G"]
  wireless-controller wtp-profile radio-1 band
    option-list (tag|opt): None -> ["802.11ax-6G"]
  wireless-controller wtp-profile radio-2 band
    option-list (tag|opt): None -> ["802.11ax-6G"]
  wireless-controller wtp-profile radio-3 band
    option-list (tag|opt): None -> ["802.11ax-6G"]
  wireless-controller wtp-profile radio-4 band
    option-list (tag|opt): None -> ["802.11ax-6G"]
```

Resolved Issues

The following issues have been fixed in 7.2.0. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
770234	5GHz DFS channels on AP Profile were not supported for FAP U231F.
772213	FortiManager may try to delete default wtp 11ac-only profile on FortiWiFi-60F causing install to fail.
781561	User may not be able to access AP Manager with a custom read-only admin profile.
785471	FortiManager was deleting wireless-controller wtp and the objects referenced by wtp during the first installation after the upgrade.

Device Manager

Bug ID	Description
545239	After added FortiManager fabric ADOM to FortiManager, Device Manager's log status, Log Rate, or Device Storage column cannot get data from FortiAnalyzer.
651560	SD-WAN monitor may stuck loading when admin user belongs to device group.
677836	The Client Address Range setting should allow users to configure assign-IPs from firewall address or group.
691611	FortiManager does "auto-retrieve" causing all policy package status to go "unknown" after a new VDOM is created on FortiGate.
705212	When editing device in HA cluster, admin password change is not applied to secondary unit.
725334	Importing policy package shows ngfw-mode policy-based with the inspection-mode set to proxy.
729413	FortiManager is missing peer options with dial up user configuration with VPN IPSec Phase 1.
743102	<i>Device & Groups > VPN Phase1/Phase2</i> does not show the proposal column when using FGT-VM type "FGVMIB".
751427	Provisioning template with empty name cannot be deleted or edited.

Bug ID	Description
755519	Zero-touch provisioning with script installation may fail due to duplicated snmp-index.
759255	User may not be able to click on the check box to import configuration with 6.2 ADOM.
759708	The Provisioning Template 's status on Summary Dashboard always displays "Modified".
763797	Installation fails due to configuring forward-error-correction on FortiGate's interfaces.
763907	Certificates CN information may be invalid when FortiGate is registered by Zero-Touch-Provisioning.
764841	FortiManager is unable to use secondary IP as source IP in DNS database.
765762	FortiManager is unable to install the Switch Controller > VLAN interface configuration during the ZTP process.
770567	When a device uses IPsec Tunnel Provisioning template with enable value for aggregate member, FortiManager may create a new system interface with the same name which is not expected behavior.
773336	FortiToken provision button is greyed out in Device Manager while it is enabled on FortiGate with the same token.
776605	Editing provisioning CLI template without any modification may cause device status changed to Modified.
779260	When <i>sdwan-monitor-history</i> is enabled, replace last 5 minutes with last 10 minutes.
779836	FortiManager cannot install TCP-connect using Random port for SD-WAN.
779900	Administrative user gui-dashboard information should be deleted upon VDOM deletion.
780833	FortiManager cannot use space to set location under SNMP configuration.
783517	Input-Device <i>under CLI Configuration > System > SD-WAN > Service</i> displays loading for a long time.
791274	When optional meta fields are being used, users cannot edit the devices.
794368	Removing the objects from Device Level DB did not delete the objects' reference from ADOM Level DB.
771165	

Global ADOM

Bug ID	Description
691562	Threat feeds global objects are not installed to destination ADOM when using the assign all object option.
740942	"srcintf" selector in Traffic Shaping Header or Footer Policy may not work in Global ADOM.
752328	Global database may be locked when viewing Workflow Session Diff.

Bug ID	Description
795327	When adding an ADOM to Global Database, the message "Double global assignment exists" keeps showing up.

Others

Bug ID	Description
707911	FortiManager should be able to assign VLAN interface to FortiExtender.
715601	Under some conditions, disk usage may reach 100% after a few days.
774872	FortiManager should support more than 88 characters for password when backing up all settings.
775574	There is a Criteria Latency field which is different between FortiGate and FortiManager when creating the manual interface option for SD-WAN rules.
776342	System NPU values may be different between FortiManager and FortiGate-1801F.
776413	FortiManager's lock/commit operation is very slow when FortiManager-HA is enabled.
780548	"Push Update" does not work for pending device under the <i>FGuard > License Status</i> .
781642	FortiManager displays "failed to copy BRANCH_BGP_Recommended" error when performing the "check adom-integrity" test.
786281	During the installation, FortiManager displays Policy Consistency Check failure.
792887	Verification fail for default dnsfilter profile due to wrongly install "set category 0".

Policy and Objects

Bug ID	Description
696367	Hit count, first used, and last used may not get updated on FortiManager.
701750	The App Control set to Monitor in FortiManager causes the App to be disappeared from FortiGate.
770210	Where Used may not be reporting used objects properly.
770256	FortiManager displays error when using "push to install" for objects utilized by policy blocks.
771941	FortiManager is unable to import or create virtual server with real servers using the same IP but different "http-host".
774435	Right-click menu to add object may return an error: "cgn-resource-quote:out of range".

Bug ID	Description
776361	Policy lookup may not work if the managed devices are in Transparent mode.
777554	There may be slowness when using Find Duplicate Objects with Merge tools.
777879	Copy fail error due to external-resource used in webfilter profile.
778111	Removing the objects from Device Level DB did not delete the object's reference from ADOM Level DB.
779853	When creating a Central DNAT policy in FortiManager, more services may not be added to policy with error: can't assign to property "from" on NaN: not an object.
779947	Address group changes for per-device mapping does not apply to FortiGate when Address group is used in policy route.
781118	6.4 version ADOM policy package failed to enable policy NAT from GUI.
781258	IPv4 & IPv6's ACLs are not available when Policy Offload Level is set to "Full Offload".
782435	Moving a policy by dragging may not work properly.
783899	There may not be empty lines in "IPS Signature and Filters".
785341	Consolidated policy NAT is always disabled on the GUI.
786684	Installation fails because the virtual-wan-link did not exist.
786740	FortiManager displays Install failure due to adding "g-" prefix to the external-resource objects.
789957	Created time doesn't indicate AM or PM on the <i>Tools > Find Unused Policies</i> .
797091	"Synchronize Firewall Addresses" under the FortiClient EMS Connector does not automatically create and synchronize addresses for all EMS tags.

Revision History

Bug ID	Description
725717	After upgrade, installation may fail due to mcast-session-counting.
729148	Install fails when new transparent mode VDOM is added directly via FortiGate CLI and imported into FortiManager.
775577	AutoUpdate may purge firewall shaping-profile.

Script

Bug ID	Description
766019	Failed to run the Post-Run CLI Template due to the "datasrc invalid" error.
767577	Installing a script to device database fails if switch-interface member contains VXLAN interface.
780604	When creating a new phase1 interface, <code>dpd=on-idle</code> settings may not be saved.
787113	TCL scripts fails to run if the admin's password is longer than 36 characters.

Services

Bug ID	Description
754038	FortiGate firmware upgrade via FortiManager may break FortiGate HA cluster.

System Settings

Bug ID	Description
762663	FortiManager should have the CA Identifier as configurable for SCEP server request.
768636	Password cannot be longer than 63 characters for configuration auto backup.
768682	Setting a Cluster ID for a model HA cluster results in an invalid group ID under config system HA.
775091	Two factor authentication fails when special characters are used in CN.
777726	FortiManager may not generate event logs for meta field changes.
778405	Script Groups should be copied with their members when cloning an ADOM.
782345	FortiManager may not be able to upgrade ADOM from 6.2 to 6.4: <code>err=-2,Policy ippool (ippool6) name cannot be empty.</code>
783066	The number of FortiGate devices registered is in the upper limit of the license count may causes HA becomes asynchronized.
787588	Webfiltering HTTPS 8888 is not working after FortiManager is upgraded from 6.4.7 to 7.0.4.
790409	<code>idle_timeout</code> under admin's setting is not converted properly after performing the upgrade.

VPN Manager

Bug ID	Description
779498	VPN monitor may not display correct information when FortiManager is in advanced ADOM mode.
780154	Policy package should be pushed to VPN hubs without error, "interface IP is 0".

Known Issues

The following issues have been identified in 7.2.0. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
697444	SSID with MPSK may not pass verification during an install.
708100	AP Manager cannot show Channels when 160 MHz channel width is set.

Device Manager

Bug ID	Description
587404	FortiManager sets incorrect captive-portal-port value when installing v6.0 PolicyPackage to v6.2 devices.
660491	Device Manager system interface should not allow duplicated secondary IP address.
704106	Certificate Enrollment fails using SCEP on Microsoft server with sub-ca certificate chains.
743112	Interface Bandwidth widget on FortiManager under device manager does not display any data for FortiGates.
748578	Retrieve FortiGate configuration may fail due to FSSO connector.
756650	<i>Router > OSPF > Interface</i> is missing configuration window for md5 keys.
764369	FortiManager tries to install Security Fabric trusted list to all downstream FortiGates when a new one is added.
767185	Unable to create route map rule using 'match-interface' when using the BGP templates under the provisioning templates.
770600	Comma between IP address and subnet causes saving problem on Prefix List Rule under BGP Templates.
773147	Installation fails due to the unexpected system interface config changes for "pvc" related settings.
791117	Unable to create simultaneous static routes with named address objects.
793941	Unable to install VPN psk with special characters through CLI template.

Bug ID	Description
795913	Error Probe Failure has been observed when adding FortiAnalyzer to FortiManager.
799259	Duplicate CSF groups for 7.0 FGTs (7.0.2+) due to syntax returning upstream-ip instead of upstream.

Others

Bug ID	Description
729175	FortiManager should highlight device consisting of specific IP address under <i>Fabric View</i> .
781831	FortiManager should be able to retrieve EMS tags using hostname of FortiClient EMS Server if its able to resolve the hostname.
783226	<i>Fabric View</i> may keep loading.

Policy & Objects

Bug ID	Description
523350	FortiManager does not show the default certificate under SSL/SSH Inspection within policy.
652753	When an obsolete internet service is selected, FortiManager may show entries IDs instead of names.
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
688586	Exporting Policy Package to "CSV" shows "certificate-inspection" in the "ssl-ssh-profile" column even when the profile is not in use.
698448	'Block Malicious URLs Discovered by FortiSandbox' in Web Filter Profile cannot be saved.
705302	Remote VPN certificate installation failed and cert disappeared from FortiManager however on the FortiGate the certificate installed successfully.
713692	Web Filter Profile install may fail when using pre-defined URL filter.
719774	IP reputation for the policies are not working without source or destination.
721253	FortiManager may not import all the roles and address groups from ClearPass.
724011	FortiManager needs to support multiple server certificate list in ssl/ssh profile.
725024	"Proxy Policy" page shows empty when the "View Mode" is selected as "Interface Pair View".
725132	When modifying IP address of Default VPN Interface of spoke in Device Manager, hub remote gateway should be modified to reflect that change.

Bug ID	Description
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
731037	There may be File Filter file type mismatch between FortiGate and FortiManager.
751767	Export to excel when filters are applied for a policy package does not work.
758494	Searching members inside an address group does not work.
758680	Unable to complete the Cisco pxGrid fabric connector's configuration on FortiManager.
767255	FortiManager fails to install the custom signature because it is too long.
773249	FortiManager may not display the correct number of firewall address objects while adding the objects to DoS policy.
774058	Rule list order may not be saved under File Filter Profile.
774111	FortiManager does not support Dynamic firewall address with sub-type Switch Controller NAC Policy TAG.
775128	Unable to create more than 20 SAML users in policy package object.
777017	FortiManager purges the "arrp-profile" when installing the v6.2 policy packages to v6.4 FGTs.
779965	Users may not be able to export firewall Header and Footer policies to Excel.
792980	Installation fails when trying to install SAML user configuration.
801876	Installation failed due to "Copy global shared objects" failure.
841187	FOS 7.0.7 syntax support. See FortiManager 7.2.0 and FortiOS 7.0.8 compatibility issues on page 35 .

Revision History

Bug ID	Description
496870	Fabric SDN Connector is installed on FortiGate even if it is not in used.
691240	FortiManager should not unset the value forward-error-correction with certain FortiGate platforms.
779864	FortiManager cannot install ISDB object 'Microsoft-Intune'.

Script

Bug ID	Description
793407	Installation fails if one of the BGP network prefix entry is a supernet.

Services

Bug ID	Description
704584	FAP firmware may not be listed and cannot be imported.
798979	FortiManager cannot download the latest IPS DB.

System Settings

Bug ID	Description
752916	FortiManager should be able to set desired permissions for Extender Manager in administrator profile settings.
753690	SNMPv3 security option configuration has discrepancy between GUI and CLI.
799504	Local restricted administrator users are able to view the task monitor.
799519	If Management Extension Applications (MEA) are enabled, all system settings may be lost after upgrading the FortiManager.

VPN Manager

Bug ID	Description
615890	IPSec VPN Authusergrp option "Inherit from Policy" is missing when setting xauthtype as auto server.
699759	When install a policy package, per device mapped object used in SSL VPN cannot be installed.

Appendix A - FortiGuard Distribution Servers (FDS)

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

- 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 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:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiADC	✓	
FortiCache	✓	
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiDDoS	✓	
FortiEMS	✓	
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiSOAR	✓	
FortiTester	✓	
FortiWeb	✓	

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



FortiManager VM subscription and perpetual licenses are stackable.



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.