

Release Notes

FortiManager 7.2.4



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



February 11th, 2025

FortiManager 7.2.4 Release Notes

02-724-953352-20250211

TABLE OF CONTENTS

Change Log	6
FortiManager 7.2.4 Release	8
Supported models	8
Special branch supported models	8
FortiManager VM subscription license	9
Management extension applications	9
Supported models for MEA	9
Minimum system requirements	9
Special Notices	11
Apache-mode changed from prefork to event	11
FortiGuard web filtering category v10 update	11
Install On column for policies	12
FortiManager 7.2.3 and later firmware on FortiGuard	12
Option to enable permission check when copying policies	12
Management Extensions visibility in the GUI	12
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	13
SD-WAN Orchestrator removed in 7.2	13
Changes to FortiManager meta fields	13
Setup wizard requires FortiCare registration	13
Access lists as ADOM-level objects	14
View Mode is disabled in policies when policy blocks are used	14
Reconfiguring Virtual Wire Pairs (VWP)	14
Scheduling firmware upgrades for managed devices	14
Modifying the interface status with the CLI	14
SD-WAN with upgrade to 7.0	15
Citrix XenServer default limits and upgrade	15
Multi-step firmware upgrades	15
Hyper-V FortiManager-VM running on an AMD CPU	16
SSLv3 on FortiManager-VM64-AWS	16
Upgrade Information	17
Downgrading to previous firmware versions	17
Firmware image checksums	17
FortiManager VM firmware	18
SNMP MIB files	19
FortiManager instances on Azure Stack	19
Product Integration and Support	20
Supported software	20
Web browsers	21
FortiOS and FortiOS Carrier	21
FortiADC	21
FortiAnalyzer	21

FortiAnalyzer-BigData	22
FortiAuthenticator	22
FortiCache	22
FortiClient	22
FortiDDoS	22
FortiDeceptor	23
FortiFirewall and FortiFirewallCarrier	23
FortiMail	23
FortiProxy	23
FortiSandbox	24
FortiSOAR	24
FortiSwitch ATCA	24
FortiTester	24
FortiWeb	24
Virtualization	24
Feature support	25
Language support	26
Supported models	26
FortiGate models	27
FortiGate special branch models	30
FortiCarrier models	31
FortiCarrier special branch models	32
FortiADC models	34
FortiAnalyzer models	34
FortiAnalyzer-BigData models	35
FortiAuthenticator models	35
FortiCache models	35
FortiDDoS models	35
FortiDeceptor models	36
FortiFirewall models	36
FortiFirewallCarrier models	37
FortiMail models	38
FortiProxy models	38
FortiSandbox models	39
FortiSOAR models	39
FortiSwitch ATCA models	39
FortiTester models	39
FortiWeb models	40
Compatibility with FortiOS Versions	41
FortiManager 7.2.4 and FortiOS 7.0.14 compatibility issues	41
Resolved Issues	43
AP Manager	43
Device Manager	43
FortiSwitch Manager	44
Global ADOM	44
Others	45
Policy and Objects	45

Revision History	47
Script	47
System Settings	47
VPN Manager	47
Common Vulnerabilities and Exposures	48
Known Issues	49
AP Manager	49
Device Manager	49
FortiSwitch Manager	51
Others	51
Policy & Objects	53
Revision History	55
Script	55
Services	55
System Settings	56
VPN Manager	56
Appendix A - FortiGuard Distribution Servers (FDS)	58
FortiGuard Center update support	58
Appendix B - Default and maximum number of ADOMs supported	59
Hardware models	59
Virtual Machines	59

Change Log

Date	Change Description
2023-09-28	Initial release.
2023-09-29	Updated Resolved Issues on page 43 and Known Issues on page 49 .
2023-10-03	Updated Resolved Issues on page 43 .
2023-10-12	Updated Resolved Issues on page 43 and Known Issues on page 49 .
2023-10-17	Updated Resolved Issues on page 43
2023-10-19	Updated Management extension applications on page 9 .
2023-11-09	Updated Known Issues on page 49 .
2023-11-10	Updated Resolved Issues on page 43 and Known Issues on page 49 .
2023-11-15	Updated Known Issues on page 49 .
2023-11-16	Updated FortiOS and FortiOS Carrier on page 21 .
2023-11-28	Added FortiManager instances on Azure Stack on page 19 .
2023-12-06	Updated Known Issues on page 49 and Resolved Issues on page 43
2023-12-18	Updated Known Issues on page 49 .
2024-01-05	Updated Special Notices on page 11 .
2024-01-11	Updated Supported models on page 8 .
2024-01-15	Updated Supported models on page 8 .
2024-01-26	Updated FortiProxy on page 23 .
2024-01-29	Updated Special Notices on page 11 .
2024-02-08	Updated FortiOS and FortiOS Carrier on page 21 . Updated Compatibility with FortiOS Versions on page 41 . Updated Resolved Issues on page 43 .
2024-02-09	Updated Compatibility with FortiOS Versions on page 41 . Added FortiManager 7.2.4 and FortiOS 7.0.14 compatibility issues on page 41 .
2024-02-21	Updated Upgrade Information on page 17 . Updated Special Notices on page 11 .
2024-02-27	Updated Known Issues on page 49 .
2024-02-29	Updated Special Notices on page 11 .
2024-03-11	Updated Special Notices on page 11 : Access lists as ADOM-level objects.
2024-03-12	Updated Resolved Issues on page 43 .

Date	Change Description
2024-03-13	Updated FortiMail models on page 38 .
2024-03-26	Updated Resolved Issues on page 43 .
2024-04-02	Updated Known Issues on page 49 .
2024-04-08	Updated Special Notices on page 11 .
2024-05-06	Updated Known Issues on page 49 .
2024-05-23	Updated Supported models on page 8 .
2024-06-19	Added support for FMG-1000G in Supported models on page 8 .
2024-07-11	Updated Management extension applications on page 9 .
2024-08-19	Updated Known Issues on page 49 .
2024-12-03	Updated Special Notices on page 11 .
2024-12-10	Updated Supported models on page 8 with information about access to FortiManager container versions.
2025-02-11	Updated Resolved Issues on page 43 and Known Issues on page 49 .

FortiManager 7.2.4 Release

This document provides information about FortiManager version 7.2.4 build 1460.



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 8](#)
- [FortiManager VM subscription license on page 9](#)
- [Management extension applications on page 9](#)

Supported models

FortiManager version 7.2.4 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_ALI, 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).

Special branch supported models

The following models are released on a special branch of FortiManager 7.2.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1460.

FMG-410G	is released on build 6042.
FMG-1000G	is released on build 6043.
FMG-3100G	is released on build 6044.



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 18](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 59](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.2.4.



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

As of FortiManager 7.2.3, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one MEA is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

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_ALI, 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
- 16 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
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 7.2.4.

Apache-mode changed from prefork to event

Before version 7.2.3, the default "apache-mode" utilized the "prefork" mode. However, starting from version 7.2.4, the default configuration switches to the "event" mode.

This change is aimed at supporting the HTTP/2.0 protocol. With HTTP/2.0, there is no limit on the maximum concurrency of HTTP requests, potentially leading to slower GUI performance if the client's environment imposes restrictions, whether network or implementation-related. HTTP/2 may face issues such as head-of-line blocking and resource prioritization, leading to slower performance compared to HTTP/1. Additionally, server push and intermediaries struggling with encrypted headers can further complicate matters. Implementing HTTP/2 requires more computational resources, which may affect response times. These complexities highlight scenarios where HTTP/1 might outperform HTTP/2.

If customers experience GUI slowness, they have the option to revert to the "prefork" mode using the following commands:

```
config system global
(global)# set apache-mode prefork
(global)# end
```

FortiGuard web filtering category v10 update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency web sites. In order to use the new categories, customers must upgrade their Fortinet products to one of the versions below.

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS.

<https://support.fortinet.com/Information/Bulletin.aspx>

Install On column for policies

Prior to version 7.2.3, the 'Install-on' column for policies in the policy block had no effect. However, starting from version 7.2.3, the 'Install-on' column is operational and significantly impacts the behavior and installation process of policies. It's important to note that using 'Install-on' on policies in the policy block is not recommended. If required, this setting can only be configured through a script or JSON APIs.

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](#).

Option to enable permission check when copying policies

As of 7.2.3, a new command is added in the CLI:

```
config system global
  set no-copy-permission-check {enable | disable}
end
```

By default, this is set to `disable`. When set to `enable`, a check is performed when copying policies to prevent changing global device objects if the user does not have permission.

Management Extensions visibility in the GUI

As of FortiManager 7.2.3, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one management extension application (MEA) is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

FortiManager creates faulty dynamic mapping for VPN manager interface during PP import

If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for *VPN Manager*.

It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database:

```
diagnose cdb check policy-packages <adom>
```

After executing this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

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](#).

Setup wizard requires FortiCare registration

Starting in FortiManager 7.2.1, the FortiManager Setup wizard requires you to complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM. Previously the step was optional.

For FortiManager units operating in a closed environment, contact customer service to receive an entitlement file, and then load the entitlement file to FortiManager by using the CLI.

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
```

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, including recommended upgrade paths. See [FortiManager 7.2.4 Upgrade Guide](#).



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 7.2.4 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 17](#)
- [Firmware image checksums on page 17](#)
- [FortiManager VM firmware on page 18](#)
- [SNMP MIB files on page 19](#)
- [FortiManager instances on Azure Stack on page 19](#)

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.

FortiManager instances on Azure Stack

After upgrading FortiManager on Azure Stack from version 7.2.3 to 7.2.4, the instance will become unreachable. To re-establish connectivity, dissociate the Public IP of the instance and then re-associate it via the Azure Stack client portal.

Product Integration and Support

This section lists FortiManager 7.2.4 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 20](#)
- [Feature support on page 25](#)
- [Language support on page 26](#)
- [Supported models on page 26](#)

Supported software

FortiManager 7.2.4 supports the following software:

- [Web browsers on page 21](#)
- [FortiOS and FortiOS Carrier on page 21](#)
- [FortiADC on page 21](#)
- [FortiAnalyzer on page 21](#)
- [FortiAnalyzer-BigData on page 22](#)
- [FortiAuthenticator on page 22](#)
- [FortiCache on page 22](#)
- [FortiClient on page 22](#)
- [FortiDDoS on page 22](#)
- [FortiDeceptor on page 23](#)
- [FortiFirewall and FortiFirewallCarrier on page 23](#)
- [FortiMail on page 23](#)
- [FortiProxy on page 23](#)
- [FortiSandbox on page 24](#)
- [FortiSOAR on page 24](#)
- [FortiSwitch ATCA on page 24](#)
- [FortiTester on page 24](#)
- [FortiWeb on page 24](#)
- [Virtualization on page 24](#)



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 7.2.4 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 96
- Google Chrome version 114

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 7.2.4 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 7.2.4 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0 to 7.2.7
 - 7.0.0 to 7.0.14
 - 6.4.0 to 6.4.16
-



Some FortiOS versions are supported with compatibility issues. For more details, see [Compatibility with FortiOS Versions on page 41](#).

FortiADC

FortiManager 7.2.4 supports the following versions of FortiADC:

- 7.2.0 and later
- 7.1.0 and later
- 7.0.0 and later

FortiAnalyzer

FortiManager 7.2.4 supports the following versions of FortiAnalyzer:

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

FortiAnalyzer-BigData

FortiManager 7.2.4 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAuthenticator

FortiManager 7.2.4 supports the following versions of FortiAuthenticator:

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

FortiCache

FortiManager 7.2.4 supports the following versions of FortiCache:

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

FortiClient

FortiManager 7.2.4 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 7.2.4 supports the following versions of FortiDDoS:

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

Limited support. For more information, see [Feature support on page 25](#).

FortiDeceptor

FortiManager 7.2.4 supports the following versions of FortiDeceptor:

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

FortiFirewall and FortiFirewallCarrier

FortiManager 7.2.4 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 7.2.4 supports the following versions of FortiMail:

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

FortiProxy

FortiManager 7.2.4 supports configuration management for the following versions of FortiProxy:

- 7.2.2 to 7.2.3
- 7.0.7 to 7.0.10



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 25](#).

FortiManager 7.2.4 supports logs from the following versions of FortiProxy:

- 7.2.0 to 7.2.8
- 7.0.0 to 7.0.14
- 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 7.2.4 supports the following versions of FortiSandbox:

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

FortiSOAR

FortiManager 7.2.4 supports the following versions of FortiSOAR:

- 7.3.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiSwitch ATCA

FortiManager 7.2.4 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.2.4 supports the following versions of FortiTester:

- 7.1.0 and later
- 7.0.0 and later
- 4.2.0 and later

FortiWeb

FortiManager 7.2.4 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.2.4 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 6.5 and later

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			✓	✓	✓
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 7.2.4.



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 27](#)
- [FortiGate special branch models on page 30](#)
- [FortiCarrier models on page 31](#)
- [FortiCarrier special branch models on page 32](#)
- [FortiADC models on page 34](#)
- [FortiAnalyzer models on page 34](#)
- [FortiAnalyzer-BigData models on page 35](#)
- [FortiAuthenticator models on page 35](#)

- [FortiCache models on page 35](#)
- [FortiDDoS models on page 35](#)
- [FortiDeceptor models on page 36](#)
- [FortiFirewall models on page 36](#)
- [FortiFirewallCarrier models on page 37](#)
- [FortiMail models on page 38](#)
- [FortiProxy models on page 38](#)
- [FortiSandbox models on page 39](#)
- [FortiSOAR models on page 39](#)
- [FortiSwitch ATCA models on page 39](#)
- [FortiTester models on page 39](#)
- [FortiWeb models on page 40](#)

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 30](#).

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-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, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F	7.2
FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1	
FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	
FortiGate 7000 Series: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	

Model	Firmware Version
FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiWiFi: FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-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-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-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, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-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-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiWiFi: FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE	7.0

Model	Firmware Version
FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-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-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, 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-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, 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-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-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-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiGate Hardware Low Encryption: FortiGate-100D-LENC FortiWiFi: FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G	6.4

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.2.4 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 27](#).

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.12	6689
FortiGate-90G, FortiGate-91G	7.0.12	6708
FortiGate-120G, FortiGate-121G	7.0.12	5334
FortiGate-900G, FortiGate-901G	7.0.12	6728
FortiGate-1000F, FortiGate-1001F	7.0.12	6660
FortiGate-3200F, FortiGate-3201F	7.0.12	6661
FortiGate-3700F, FortiGate-3701F	7.0.12	6661
FortiGate-4800F, FortiGate-4801F	7.0.12	6661
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.12	0163
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.12	0163
FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.12	0163
FortiGateRugged-70F	7.0.12	6668
FortiGateRugged-70F-3G4G	7.0.12	6669
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL	7.0.12	6690

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F, FortiGate-401F	6.4.13	5455

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-600F, FortiGate-601F	6.4.13	5455
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	6.4.13	1926
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	6.4.13	1926
FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	6.4.13	1926
FortiWiFi-80F-2R-3G4G-DSL	6.4.7	5003

FortiCarrier models

The following FortiCarrier models are released with FortiCarrier firmware.

For information about supported FortiCarrier models on special branch releases of FortiCarrier firmware, see [FortiCarrier special branch models on page 32](#).

Model	Firmware Version
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.2

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 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-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	7.0
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-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-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.2.4 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see [FortiCarrier models on page 31](#).

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.12	6661
FortiCarrier-3700F, FortiCarrier-3701F	7.0.12	6661
FortiCarrier-4800F, FortiCarrier-4801F	7.0.12	6661
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.12	0163
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.12	0163
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.12	0163

FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	6.4.13	1926
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	6.4.13	1926
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	6.4.13	1926

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, 7.1, 7.2

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, 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-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.2
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-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, 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

FortiAnalyzer-BigData models

Model	Firmware Version
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F FortiAnalyzer-BigData VM: FortiAnalyzer-BigData-VM64	7.2
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F FortiAnalyzer-BigData VM: FortiAnalyzer-BigData-VM64	7.0

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, FAC-3000F FortiAuthenticator VM: FAC-VM	6.4
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

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-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F FortiDDoS VM: FortiDDoS-VM	6.4
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F FortiDDoS VM: FortiDDoS-VM	6.3
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F FortiDDoS VM: FortiDDoS-VM	6.2

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-100G, FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	5.0
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.3
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.2

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.2.4 supports these models on the identified FortiFirewall firmware version and build number.

FortiFirewall 7.2

Model	Firmware Version
FortiFirewall: FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2

FortiFirewall 7.0

Model	Firmware Version	Firmware Build (for special branch)
FortiFirewall: FortiFirewall-3001F	7.0.10	4955
FortiFirewall: FortiFirewall-3501F	7.0.10	4940
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	7.0	
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.0	

FortiFirewall 6.4

Model	Firmware Version	Firmware Build (for special branch)
FortiFirewall: FortiFirewall-1801F, FortiFirewall-2600F FortiFirewall DC: FortiFirewall-1801F-DC, FortiFirewall-2600F-DC	6.4.12	5423
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	6.4	
FortiFirewall: FortiFirewall-4200F, FortiFirewall-4400F	6.4	1999
FortiFirewall: FortiFirewall-4401F FortiFirewall DC: FortiFirewall-4401F-DC	6.4.12	5423
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.2.4 supports these models on the identified FortiFirewallCarrier firmware version and build number.

FortiFirewallCarrier 7.2

Model	Firmware Version
FortiFirewallCarrier: FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.2

FortiFirewallCarrier 7.0

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0.10	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0.10	4940
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4.9	5318

FortiFirewallCarrier 6.4

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4.9	5318

FortiFirewallCarrier 6.2

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-2000F, FE-3000F	7.2
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	6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E, FortiProxy VM: FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G FortiProxy VM: FortiProxy-AliCloud, 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	1.0, 1.1, 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	4.2
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	3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	7.0, 7.2, 7.3

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-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F	7.1

Model	Firmware Version
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-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	
FortiTester: FortiTester-60F, 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-IBM-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-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2

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 FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0, 7.2

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.2.4.

FortiManager 7.2.4 and FortiOS 7.0.14 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.4 and FortiOS 7.0.14. FortiOS 7.0.14 includes syntax changes not supported by FortiManager 7.2.4.



When specific platforms are indicated, the syntax change applies to both the FortiGate and FortiCarrier platform for the model.

For example, (4 platforms: 3980E,3960E) indicates FortiGate-3980E, FortiCarrier-3980E, FortiGate-3960E, FortiCarrier-3960E.

The following objects were removed:

- (attr) system console baudrate
- (attr) system global admin-ble-button (2 platforms: 400F,401F)
- (attr) system global admin-reset-button (2 platforms: 400F,401F)

The following default value changed:

- system interface mediatype (by platforms)

Additional option changes:

```
antivirus profile analytics-max-upload
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options cifs oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options cifs uncompressed-oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options ftp oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options ftp uncompressed-oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options http oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options http uncompressed-oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options imap oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options imap uncompressed-oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options mapi oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options mapi uncompressed-oversize-limit
  int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options nntp oversize-limit
```

```
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options nntp uncompressed-oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options pop3 oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options pop3 uncompressed-oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options smtp oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options smtp uncompressed-oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options ssh oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
firewall profile-protocol-options ssh uncompressed-oversize-limit
int-range (tag|lmt): 1,798 -> 1,797 (1 platforms: 301E)
system interface mediatype
option-list (tag|opt): ["qsfp28-cr4", "qsfp28-lr4", "qsfp28-sr4"] -> None (5
platforms: 3960E, 3980E)
option-list (tag|opt): None -> ["cr", "cr4", "gmii", "lr", "lr4", "none", "sgmii",
"sr", "sr4"] (4 platforms: 3960E,3980E)
option-list (tag|opt): None -> ["serdes-copper-sfp", "serdes-sfp", "sgmii-sfp"] (1
platforms: 3980E)
```

Resolved Issues

The following issues have been fixed in 7.2.4. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
865486	The FortiManager's <i>AP Manager</i> permits the use of invalid channels with a 40MHz channel width.
892773	Assigning AP Profile returns invalid value.

Device Manager

Bug ID	Description
768289	There is a discrepancy in the usage of quotation marks (") when configuring DHCP relay from FortiManager or retrieving it from FortiGate.
831624	<i>SD-WAN Monitor</i> under the <i>Monitors</i> displays time frame as "invalid date - invalid date".
895001	The "gui-ztna" configuration is displayed as enabled on the FortiManager even though this setting is disabled on the FortiGate.
896127	When attempting to create a VLAN type with a name longer than 15 characters, FortiManager displays an error message.
896367	The geographic coordination config of FortiGates on <i>Device Manager</i> is being reset to 0, 0 after a certain period of time.
899350	Promote button is missing for FortiGate 80F Clusters.
899541	An error message, "upgrade image failed", is shown, even though the upgrade has been completed successfully.
902908	Managed FortiAnalyzer is not listed under <i>System Template</i> .
905367	An error message, "upgrade image failed", is shown even though the upgrade has been completed successfully.
905869	Invalid default value for VRF ID is observed when creating static route.
910391	When FortiManager operates in a non-default workspace mode, it may attempt to purge the

Bug ID	Description
	configuration of the FortiGate devices due to database corruption.
911535	Adding a Model device with MetaVariables changes the status of other devices which using the MetaVariables to Modified/unknown.
915361	FortiWifi devices are displayed in FortiManager under the Vulnerable devices as FortiAP.
917810	FortiManager displays an event log with the "update temp cachedb failed" error message when changing the FortiGate management VDOM to mgmt-vdom.
917969	FortiManager is unable to search static routes via its interface name.
919613	When using a space character in "psksecret", the FortiManager is unable to install the "psksecret" and displays an error message.
921094	In 6.2 or 6.4 ADOMs, problems might occur when attempting to add or modify static routes.
922543	FortiManager attempts to unset authentication mode in ospf settings.
925546	Assigned Devices on Provisioning Template\CLI Temp shows incorrect VDOM.
925684	Only a maximum of 10 devices can be previewed before installation using 'install preview'.
925854	FortiManager fails to load the security fabric data for FortiGates (Versions 7.0.5+ & 7.2.5).
931736	Adding a new cli template script into existing cli template group changes the order of cli templates to alphabetical order.
936544	When importing CLI Templates, GUI displays a blank page.

FortiSwitch Manager

Bug ID	Description
881766	Event logs or task manager do not show which user authorized a Fortiswitch.
947651	<i>Per Device</i> under the <i>FortiSwitch Manager</i> cannot edit FortiSwitch name and GUI returns error "invalid value".

Global ADOM

Bug ID	Description
894714	FortiManager does not allow creating/modifying or removing the per-device mapping in global objects in assigned ADOM.
925188	The per-device mapping for any assigned global objects cannot be modified.

Others

Bug ID	Description
880465	TCP ports 8902 & 8903 are opened and in listening mode after the upgrade.
885665	Unable to specify type of objects in FortiProxy ADOM.
894947	FortiManager fails to trigger the event handler for its local events after enabling the FortiAnalyzer feature.
895982	Admin with a super user profile is not able to create the Firmware Template when FortiManager is working in the Workflow mode.
900512	FortiManager ADOM Upgrade fails with the error message, "Peer type cannot be peer when authentication method is pre-share key".
910175	When provisioning the FortiExtender via CLI template, FortiManager displays the "mismatch interface" error message.
914027	FortiManager does not display/use the latest ISDB version for all of its ADOMs.
916463	The approval emails are not being sent to the "Email Notification" admins when a new session is created and submitted for approval.
918129	FortiManager does not support the AWS Security Token Service in AWS SDN connector.
919981	Installation fails to Azure FortiGate standalone as FortiManager attempts to set the peervd to "root".
921273	Unable to upgrade ADOMs due to the XSS vulnerability characters check on wireless-controller.
925778	FortiGates are displayed offline and Inactive on FortiWLM MEA.
928163	Unable to export packages under <i>FortiGuard</i> .
930425	When downloading the install preview, the file name doesn't include the timestamp.

Policy and Objects

Bug ID	Description
696367	Hit count, first used, and last used may not get updated on FortiManager.
780058	FortiManager's GUI does not support the "src-vendor-mac" objects in Firewall policy.
830640	"Send files to FortiSandbox for inspection" option is being enabled when creating an antivirus profile.
863819	Unable to delete unused objects.
869863	NSX connector; unable to deselect the group with no users.

Bug ID	Description
873358	Installation fails as FortiManager tries to set "cgn-client-startip" and "cgn-client-endip" settings when ippool object has been modified.
880418	The default values of the Application Control Profile entries cannot be changed.
883064	Any admin make changes to "Object Selection Pane", either set it to <i>Dock to Right</i> , <i>Dock to Bottom</i> , or <i>Classic Dual Pane</i> , it will affect all other admin's GUI preferences.
889586	Azure Service Tags not displayed correctly in FortiManager.
894597	Default value for "unsupported-ssl-version" in ssl-ssh-profile gets modified during the installation.
896461	FortiManager disables ip6-send-adv after opening and closing interface configuration.
898883	Exported firewall policies do not contain firewall address values IP, netmask and other details.
899135	Installation fails as FortiManager tries to unset the "arp-profile" during the installation.
902298	FortiManager does not generate error messages when invalid or obsolete application IDs are used in the policy. Instead, it allows installation and sets the category to "pass" or "monitor".
912114	FortiManager is unable to import OpenStack SDN connector and the following error message is displayed: "send_sdn_connector_openstack_cmd: Failed to get openstack token".
914945	Unable to modify or clone the "SSL/SSH inspection profile" in the <i>Policy & Object</i> on the ADOM 7.0 version.
914981	In <i>Policy & Object</i> , local policy is not displayed if view mode " <i>Interface pair view</i> " is selected.
916459	The option " <i>Allow Websites When a Rating Error Occurs</i> " is not being saved correctly in the default web filter.
919415	Unable to " <i>Edit</i> " and " <i>Delete</i> " Installation Target after enabling classic dual pane mode.
919681	The incoming and outgoing interfaces are not loading after creating a custom policy package in a 7.2 FortiGate ADOM.
920740	Unable to create a per device mapping for a virtual server
922648	FortiManager unable to push WiFi SSID to FortiGates.
924680	Policy packages containing geo-based ISDB objects may not be successfully installed to the FortiGates.
925058	"Web URL Filter" entries are not visible in the <i>Web Filter Profile</i> .
925076	FortiManager tries to install different preconnection-id under <i>VPN SSL WEB Portal > Profile > Bookmark-Group > GUI-Bookmark > Book</i> .
939979	After editing authentication-rule/portal mapping, FortiManager installs unexpected changes to these rules.

Revision History

Bug ID	Description
904710	Restoring a revision of a policy removes the information of all the SD-WAN rules.

Script

Bug ID	Description
913360	Device script is trying to add additional configuration; therefore, installation gets failed.
923966	When FortiManager is operating in Workspace mode, there are no options to save changes after executing a CLI script.
931196	Scheduled Scripts created by the LDAP users cannot be run and FortiManager displays "Data is not ready" error message.

System Settings

Bug ID	Description
842732	FortiManager does not display the Secondary HA member's status correctly.
888374	Admin user's ADOM setting can not be synced to secondary when adom-access is set to specify.
890956	SAML SSO Authentication only works with the default local certs.
861997	Unable to delete a particular non-default empty ADOM.
930200	Unable to change the time and timezone from the GUI.

VPN Manager

Bug ID	Description
847479	Despite being configured for 'SHA-256,' FortiManager is installing 'SHA-1' certificates on FortiGates.
863424	The "Latest Patch Level" should be available with action "Check-up-to-date" under the SSL VPN Portal.
923221	Provision Template - IPsec Tunnel: cannot Activate IPsec_Fortinet_Recommended; GUI

Bug ID	Description
	returns error.
931564	In <i>VPN Manager</i> , ipsec vpn map, topology view, and traffic view do not display map normally.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
539972	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-44256
900221	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-36554
921579	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-42788
922503	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-41838
928114	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-42787
934151	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-42791
941847	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-44249
946239	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2024-40585
947396	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-44253
949519	FortiManager 7.2.4 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"> CVE-2023-41842

Known Issues

The following issues have been identified in 7.2.4. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
884233	FortiManager displays the AP critical security vulnerability info even after FortiAPs are being upgraded.
906061	It takes a significant amount of time to assign a profile to each FortiAPs.
982548	FortiGate configuration install may fail with a reason, "Need to unset channel list in radio-1 first."
987111	Unable to save the SSID configuration changes under the <i>AP Manager</i> .
1002043	<i>AP Manager</i> view does not show SSIDs and Radio Channels.

Device Manager

Bug ID	Description
723720	'strong-crypto' feature change under the CLI configuration cannot be installed to Fortigate.
751612	After upgrading to 7.2.4 version, Read/Write Access level profile for SD-WAN and provisioning template is not properly set.
811104	Import policy package fails after installing web-proxy through CLI configurations.
880934	FortiManager reverts Syslog mode settings on local FortiGates (when FortiGates are in FIPS mode).
894948	FortiManager fails to push the FortiAnalyzer override settings to the FortiGate.
902577	The status of the FortiLink split-interface radio button under FortiManager's <i>Device Manager</i> does not match the configuration in FortiGates.
920394	Installation failed due to the incorrect install order during ZTP.
923808	Even with the "set dhcp-relay-request-all-server enable" option enabled, FortiManager does not keep the DHCP server & relay configurations on the same interface.
935586	When managed devices go down/appear offline, not all fgfm tunnels are automatically

Bug ID	Description
	recovered by FortiManager.
936168	Unable to assign Device Group to the Firmware Template.
939804	<p>Creating/Modifying the IPSEC Phase1 Interface Mode might trigger the following error message: "The string contains XSS vulnerability characters." This ONLY occurs when <code>dev-id = ''</code>.</p> <p>Workaround: Manually removing the value ' ' from dev-id.</p>
939921	The firmware upgrade in ADOM mode backup is not allowed.
949546	When zones have identical names except for case, only 1 of the zones may be visible in <i>Device Manager</i> .
950391	FortiManager attempts to unset the "peervd" parameter under the system "cluster-sync", resulting in installation failure.
952404	FortiManager cannot install the Static Route config under the Provisioning Template due to a static route template error after upgrading to FortiManager 7.2.4/7.4.1.
956567	Not able to edit/delete Logging Devices Group.
956920	Monitor Health Check graphs return incomplete or no value.
960315	Unable to create/edit "ssh-public-key1" with "sh-ed25519" for admin users from FortiManager's <i>Device Manager</i> ; it displays an "invalid value" error message.
960315	Unable to create/edit "ssh-public-key1" with "sh-ed25519" for admin users from FortiManager's <i>Device Manager</i> ; it displays an "invalid value" error message.
961447	<p>After upgrading FortiManager (VMs & FortiManager Cloud) to versions 7.2.4 or 7.4.1, devices may not be able to be retrieved or refreshed.</p> <p>Workarounds:</p> <p>A) Reduce the license use (delete one device).</p> <p>B) Request/purchase a license upgrade.</p> <p>C) On the already managed FortiGates that need to be retrieved, run:</p> <pre>diag fdsm cfg-upload <comment></pre> <p>D) When adding a new FortiGate to the last license seat, it will initially fail on the retrieve step, but the device is added to DVM. Within about 120 seconds, an auto-retrieve is triggered and the first revision of the new device is created normally.</p>
966118	FortiManager tries to purge all entries under table "system global split-port-mode" for its <i>System</i> template.
967611	<i>Device Manager</i> interface link status is blank for various Interface type (Tunnel, Aggregate, VDOM Link, Software Switch).
969542	Sometimes IPsec Tunnel Template displays "Response with errors" message when editing the template.
969698	FortiManager allows the creation of an empty service value for Internet Service routes.
973064	Installation to FortiGate with NP7 Acceleration feature enabled might fail when FortiManager

Bug ID	Description
	attempted to modify the QoS settings. Changing the "default-qos-type" to values other than its default may result in a FortiGate reboot (FOS Behavior).
975310	Unable to unset interface IP for a VLAN interface in <i>Device Manager</i> .
981031	<i>Device Inventory</i> widget shows wrong date for "last seen".
984868	<i>Device Manager</i> page turns blank after right-clicking on a device.
986466	When modifying the BGP template with a new route map rule, a failure error message may be displayed.
988964	FortiManager tries to push switch-controller command to devices that do not have this command.
1000686	HA autolink failure occurs when LAN interfaces do not exist.
1006838	"Admin User" settings get modified if username is more than 37 characters.
1009883	Unable to set the Radius-Server addresses as FQDN. Workaround: Run the script directly on the FortiGate and then retrieve config back to the FortiManager.

FortiSwitch Manager

Bug ID	Description
940419	When adding FortiSwitch on FortiManager, the error message, "Import error - invalid port number" is displayed.
967213	While attempting to deploy a FortiSwitch template to a model device, FortiManager generates the following error message: "VLAN interface does not match FortiLink."

Others

Bug ID	Description
583349	FortiManager does not provide support for image upgrades on "ONDEMAND" devices.
703585	FortiManager may return 'Connection aborted' error with JSON API request.
777831	When FortiAnalyzer is added as a managed device to FortiManager, " <i>Incident & Events</i> " tile will be displayed instead of " <i>FortiSoC</i> ".
796858	Subject Key Identifier extension is missing on FortiManager ADOM CA certificate.
862651	Even after enabling all MEAs, the warning to enable the application is displayed.

Bug ID	Description
875584	<p>FortiManager cannot upgrade ADOMs to 7.2 due to the following error: "copy system replacemsg spam.smtp-spam-emailblock".</p> <p>Workaround: Delete replacement message "smtp-spam-emailblock" from System templates.</p>
922957	The "fmgd" process may crash while loading the ADOM when multiple Policy Packages are locked.
924201	Jinja templates do not identify new variables automatically when a new variable is added.
930305	Firmware template upgrade preview shows incorrect versions for the upgrade.
935430	When FortiAnalyzer is managed by FortiManager and FortiManager's local logs are being sent to FortiAnalyzer, installing PP to FortiGates may display the following message: "Confirm Deletion FortiManager is going to sync the following device deletion to FortiAnalyzer,...".
941203	FortiManager does not support the use of Certificate Templates to create certificates with a "range=global" setting for FortiGates operating in multi-vdom mode.
949994	When the FortiAnalyzer feature is activated on the FortiManager, attempting to download FortiGate logs/log files from the FortiManager results in an error message.
954564	FortiManager attempts to change FortiExtender serial number and returns an installation error.
956335	Unable to upgrade root ADOM from v6.4 to v7.0 with "med-location-service" object error
961155	<p>Event Logs cannot be downloaded via GUI.</p> <p>Workaround: To export the local event logs, you may use the following command:</p> <pre>diagnose system export umlog ftp locallog <(s)ftp server> <username> <password> <directory(/folder)> <filename(elogs-fmg.tgz)></pre>
961249	Significant CPU utilization has been detected in the miglogd process upon enabling the locallog FortiAnalyzer feature.
963490	Installation fails as FortiManager attempts to "set role primary" feature for the "lan-extension backhaul" under the "extender-controller".
963744	FortiManager's HA status becomes unsynchronized when the "private-data-encryption" feature is enabled.
971122	FortiManager does not support all authentication types that are supported by FortiOS, leading to a certificate error in the FortiClient EMS connector.
976448	Unable to login FortiManager Cloud.
982564	When upgrading the root ADOM, the process might fail with the following error message: "...The string contains XSS vulnerability characters...".
991052	FortiManager AWS is not able to form GeoRedundant Cluster as VRRP HA fails to sync.

Policy & Objects

Bug ID	Description
630648	A FortiManager instance running on Microsoft Azure is unable to import the SDN connector for a dynamic firewall address and is displaying an error message stating "wrong input parameter."
751443	<p>FortiManager displays policy installation copy failures error when ipsec template gets unassigned.</p> <p>Workaround: Ensure a fresh FMG's backup is created prior to any changes. Instead of unassigning IPSec template, modify IPSec template and replace the reference to IPSec tunnel interface with another interface.</p>
843716	FortiManager tries to unset url-map for TCP forwarding ZTNA virtual server
845022	SDN Connector failed to import objects from VMware VSphere.
854359	An installation error occurs when FortiManager attempts to install wildcard FQDN addresses 'mzstatic-apple' and 'cdn-apple' within the 'custom-deep-inspection' SSL-SSH profile.
855073	<p>The "where used" feature (under the Source & Destination objects) incorrectly displays "No Record Found" even when these objects are in use.</p> <p>Workaround: Run the following command:</p> <pre>diagnose cdb upgrade force-retry add-missing-ref</pre>
875103	Local categories gets purged if used in Profile Mode Security Profiles.
888798	Changing deep inspection ssl-ssh-profile to "inspect all ports" may cause installation error.
899226	Unable to create Central SNAT explicit port translations on FortiManager.
900229	In policy-based policy packaged, application IDs are displayed instead of their names.
904751	WebRating overrides can't be deployed or deleted via FortiManager.
905377	Threat Feeds with name starting with 'g-' are not installed to FortiGates without VDOM enabled.
907925	IPS profile/Signature tab is not visible for admins with non-default admin profile.
908353	When ISDB name changed, FortiManager is not automatically updating the new ISDB object name.
908445	FortiManager does not display correct edit page for virtual server VIP when edit object in policy table.
917225	FortiManager is unable to install policy packages to multiple devices due to "securityconsole" crashes.
920983	The policy blocks using a group object do not get updated when the objects within the group are modified.

Bug ID	Description
938019	Policy Package Status not changed on modification of nested group used in policy block.
942659	Syncing EMS tags from FortiManager fails when the EMS Connector is configured in multi-site mode.
945632	Modifying the Policy Installation Target does not trigger a status change in the Policy Package when adding an "install on" to a single policy.
945853	FortiManager doesn't sync previously deleted EMS tags.
949515	Security Policy Installation Verification fails because the <code>internet-service-negate</code> feature gets enabled every time after modifying the policy.
955010	Comments on policies may be cleared when a blank area within the text field is clicked.
957225	ADOM admin users not able to view the managed FortiGate in the policy push wizard.
958206	Policy package import fails due to a certificate error in the SSL VPN web realm configuration for the virtual host server.
958923	Installing policy packages that utilize an SSL/SSH Inspection profile may fail with the error message: "Server certificate replace mode cannot support category exempt."
959116 959877	The timestamps displayed for 'First/Last Used' under the Hit Count for Firewall Policies within the <i>Policy & Objects</i> section are invalid.
959890	Per-device mapping search for VDOMs is not possible for users.
960660	The Clone Reverse feature is not functioning when the firewall policy includes an internet service address object.
960778	Installation failed because FortiManager attempts to remove a static entry, "QuarantinedDevices."
963008	Impossible to merge duplicate objects.
963536	The policy package feature "Export to Excel" is not functioning.
965719	FortiManager is unable to enable the log setting for implicit deny rule under the policy package.
970056	The policy installation fails when FortiManager attempts to apply changes related to the "management address" on the interface of the FortiGates.
972392	Users do not receive a proper warning when creating a firewall address with the IP address "0.0.0.0/0."
978814	When attempting to use the "Export to Excel" feature under the Firewall Policy with extensive rules, GUI may slow down and become unresponsive for some time.
979554	EMS connectors are randomly getting disabled on FortiManager, despite no changes being made to EMS settings on either FortiManager or FortiGate.
982638	Invalid IPS signature breaks the GUI when users are trying to edit the IPS profile in the FortiManager.

Bug ID	Description
984935	The "view mode" and "Routing Object" options are not displayed on the GUI.
986262	EMS Cloud tags are not updated on FortiManager.
989423	FortiManager SD-WAN interfaces are not available as Normalized interfaces.
997752	Install preview randomly hangs and doesn't return any data on next screen.
1003309	When an address object is cloned it is not automatically included in the original address group.
1008413	FortiManager Fails to Load IPS Signatures in the Profile.
1012400	The policy package installation is hanging due to a crash in the 'securityconsole' application.

Revision History

Bug ID	Description
513317	FortiManager may fail to install policy after FortiGate failover on Azure.
801614	FortiManager might display an error message, "Failed to create a new revision." for some FortiGates when retrieving their configurations.
894523	Object revision timestamp is taken from previous revision.

Script

Bug ID	Description
937528	Unable to send DHCP options "set value" using CLI template and using Script .
1020938	After the image upgrade, users may encounter a "Temporarily Unavailable" page message. This problem specifically occurs when special characters, like "\$ (. .) ", are used within a TCL script in an ADOM. The Meta variable parsing function incorrectly identifies these characters as meta variable delimiters.

Services

Bug ID	Description
863094	The query status is not functioning correctly, and the "top 10 unrated sites" section actually displays ratings.

Bug ID	Description
938365	FortiManager's GUI does not display an option under FortiGuard Settings to support the 7.2 version for FortiClient and FortiMail.
980334	"Download to Excel" option on Licensing Status under the FortiGuard does not work.
985074	Changing the FortiGuard Server Location under the license info widget results in a blank page popup.

System Settings

Bug ID	Description
853429	Creating FortiManager's configuration backup via scp cannot be done.
881309	In SSO configuration, whether the settings for "ext-auth-accprofile-override" and "ext-auth-adom-override" are enabled or disabled, the users are granted an adom/accprofile override if the IdP sends valid ADOMs and "profilename" attributes.
930449	Testing the syslog server displays the message, "Failed to send a test log to syslog server".
936694	After removing a device, FortiManager generates repeated 'sync dvmdb to faz' tasks for all logged-in administrative users.
941082	A password prompt is consistently requested with each new login attempt when applying password policies to a local account linked to FortiToken Cloud Mobile for multi-factor authentication (MFA).
966148	RADIUS remote users are unable to successfully install changes to FortiGates.

VPN Manager

Bug ID	Description
678319	Once "os-check" option is enabled, "os-check-list" table is not loaded.
784385	<p>If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for <i>VPN Manager</i>.</p> <p>Workaround: It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to the workaround. Perform the following command to check & repair the FortiManager's configuration database:</p> <pre>diagnose cdb check policy-packages <adom></pre> <p>After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.</p>

Bug ID	Description
897574	Address Objects with Meta Variables do not function correctly when creating Static routes using the <i>VPN Manager</i> .
906097	<i>VPN Manager</i> IPsec community Phase 2 encryption setting can't be changed to AES256GCM from the GUI.
942222	The configuration settings for the "peergroup" are not being retained properly.

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 licenses are fully stackable.
 - For FortiManager-VM perpetual licenses, only the number of managed devices is stackable.
-



www.fortinet.com

Copyright© 2025 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.