Release Notes

FortiManager 7.2.1

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

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-08-09	Initial release.
2022-08-09	Updated Known Issues on page 54.
2022-08-11	Updated Special Notices on page 11.
2022-08-23	Updated Special Notices on page 11.
2022-08-26	Updated Upgrade Information on page 19.
2022-08-29	Updated Special Notices on page 11.
2022-09-07	Added 839168 to Known Issues on page 54 and added special notice to Special Notices on page 11.
2022-09-08	Added a second workaround to Special Notices on page 11.
2022-09-30	Updated FortiOS and FortiOS Carrier on page 23.
2022-10-20	Added 841187 to Known Issues on page 54 and added FortiManager 7.2.1 and FortiOS 7.0.8 compatibility issues on page 41.
2022-10-27	Updated FortiProxy on page 25.
2022-11-02	Updated Resolved Issues on page 44.
2022-11-03	Updated FortiGate models on page 29.
2022-11-10	Updated FortiOS and FortiOS Carrier on page 23.
2022-11-16	Updated FortiSandbox on page 25.
2022-11-17	Updated Known Issues on page 54.
2022-11-21	Updated Known Issues on page 54.
2022-11-30	Updated Appendix A - FortiGuard Distribution Servers (FDS) on page 67
2022-12-19	Updated Resolved Issues on page 44.
2023-01-30	Added 844985 to Known Issues on page 54.
2023-02-15	Updated Resolved Issues on page 44.
2023-03-16	Updated Resolved Issues on page 44 and Known Issues on page 54.
2023-04-25	Updated Known Issues on page 54.
2023-06-01	Updated Special Notices on page 11 and Web browsers on page 23.
2023-06-05	Updated: • Special Notices on page 11 • Web browsers on page 23

Date	Change Description
	• Known Issues on page 54
2023-09-25	Updated FortiClient on page 24.
2024-01-05	Added the *FortiManager 7.2.3 and later firmware on FortiGuard* Special Notice.
2024-03-11	Updated Special Notices on page 11: Access lists as ADOM-level objects.

FortiManager 7.2.1 Release

This document provides information about FortiManager version 7.2.1 build 1215.

> 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 8
- Management extension applications on page 8

Supported models

FortiManager version 7.2.1 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_DOCKER, 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), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

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 20.

See also Appendix B - Default and maximum number of ADOMs supported on page 68.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.2.1.

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

Supported models for MEA

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

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_DOCKER, 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), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

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

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

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

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

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	• 8 vCPU • 32 GB RAM • 500 GB disk storage	No change
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage

Management Extension Application	Minimum system requirements	Recommended system resources for production*
Policy Analyzer	• 4 vCPU • 8 GB RAM	No change
Universal Connector	• 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage	No change
Wireless Manager (FortiWLM)	• 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 7.2.1.

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.

FortiManager 7.2.1 GUI issues in Google Chrome and Microsoft Edge

The FortiManager 7.2.1 GUI may not work properly in Google Chrome version 114 (114.0.5735.91) and Microsoft Edge version 114 (114.0.1823.37).

For information about supported web browsers, see Web browsers on page 23.

FMG-VM acquires incorrect certificate after upgrade

FortiManager virtual machines with an older perpetual license only use one certificate. After upgrading FMG-VMs with a perpetual license to FortiManager 7.2.1, a second, default certificate with a serial number (in the CLI) or common name (in the GUI) of *FAZ-VM0000000001* is automatically added to the FMG-VM, and FortiManager attempts to use the default certificate with the incorrect value for FGFM tunnels with managed FortiGates.

This issue does not affect FMG-VMs with a subscription license and FMG-VMs with a newer perpetual that uses two certificates.

You can use either of the following workarounds:

1. Use the CLI to configure the FGFM tunnel to use the certificate with the correct serial number or CN value.
2. Go to FortiCloud, download the license file again, which includes two local certificates, and apply the license to FortiManager. The new local certificates automatically overwrite the existing local certificates.

Workaround 1:

1. Go to *System Settings > Certificates > Local Certificates*, and check the *CN* (common name) field for the local certificates.
   In the following example, the incorrect *SN* value of *FAZ-VM0000000001* is displayed:

2. Configure the FGFM tunnel to use the default certificate with the correct serial number or CN value:
   In this example, the *Fortinet_Local* certificate has the correct value:

   ```
   config system global
       set fgfm-local-cert "Fortinet_Local"
   ```

3. If the FMG-VMs are in an HA cluster, configure the cluster to use the default certificate with the correct serial number or CN value:
   In this example, the *Fortinet_Local* certificate has the correct value:

   ```
   config system ha
       set local-cert Fortinet_Local
   ```

Workaround 2:

1. In FortiCloud (https://support.fortinet.com/), go to *Products > Product List*, and click the FMG-VM product.
   The product details are displayed.
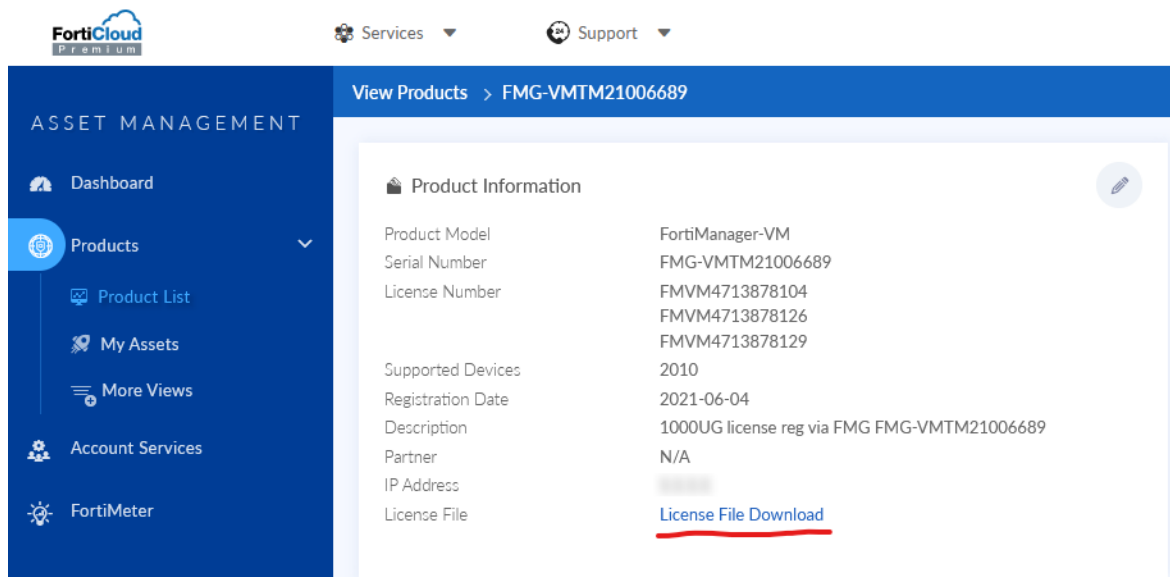
2. Click *License File Download* to download the license file with two default certificates.

3. In FortiManager, go to *System Settings > Dashboard > License Information*, and click the *Upload License* button to upload the license and the two local certificates.
The new local certificates automatically overwrite the existing local certificates.

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*.

Fortinet verified publisher docker image

FortiManager docker images are available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

1. Go to *dockerhub* at https://hub.docker.com/.
   The dockerhub home page is displayed.
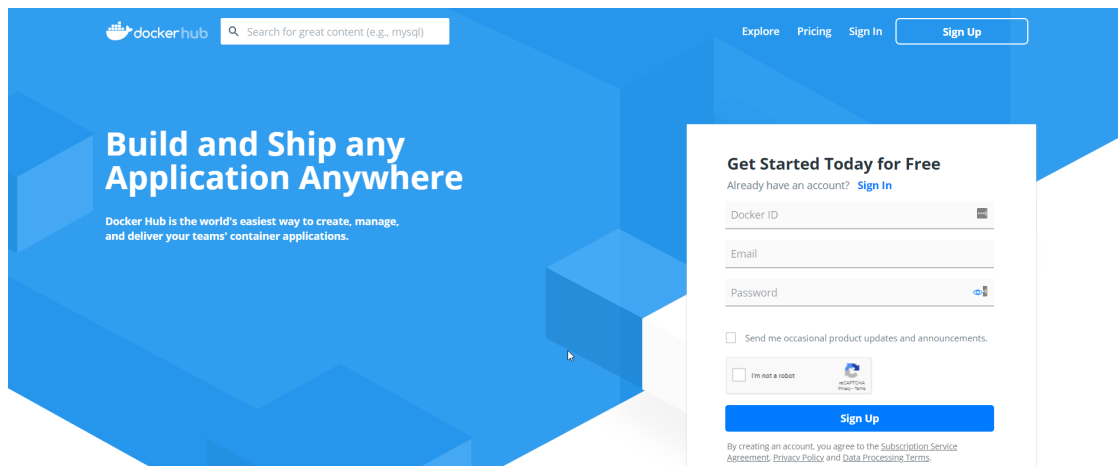
2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
   The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.
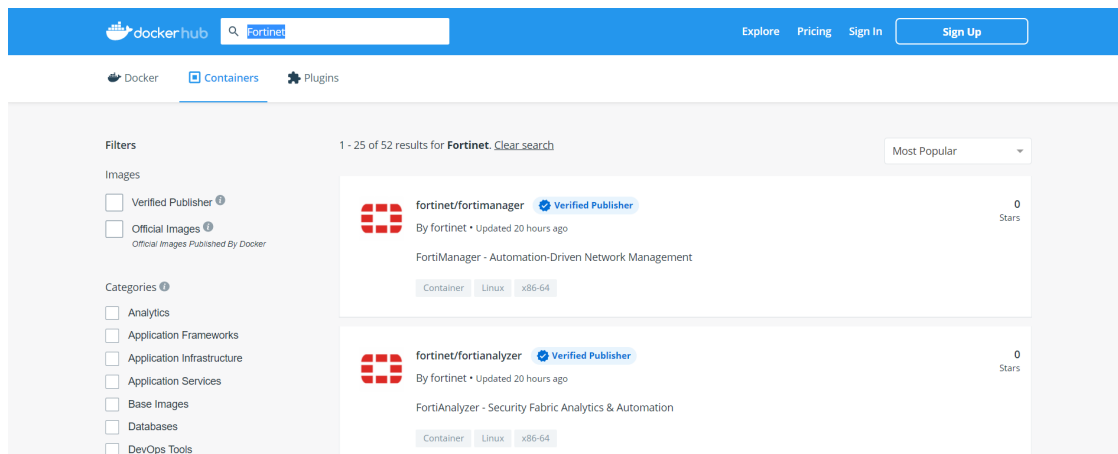
4. Click *fortinet/fortimanager*.
   The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.
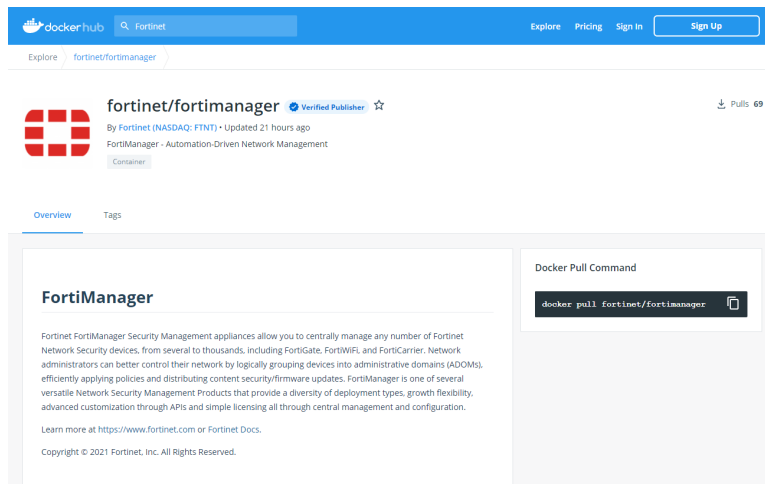
5. On the *Overview* tab, copy the docker pull command, and use it to download the image.
   The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

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 t1sv1
```

```
end
```

Upgrade Information

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

See FortiManager 7.2.1 Upgrade Guide.

You can upgrade FortiManager 7.0.1 or later directly to 7.2.1.

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 7.2.1 Upgrade Guide.

This section contains the following topics:

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

FortiManager VM firmware

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Google Cloud Platform

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

Linux KVM

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

Microsoft Azure

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

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

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

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

Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

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

VMware ESX/ESXi

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

> For more information see the FortiManager Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 7.2.1 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

Supported software

FortiManager 7.2.1 supports the following software:

> 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 7.2.1 supports the following web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 96
- Google Chrome version 113

Please note the GUI may not work properly in Google Chrome version 114 (114.0.5735.91) and Microsoft Edge version 114 (114.0.1823.37).

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 7.2.1 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 7.2.1 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0 to 7.2.3
- 7.0.0 to 7.0.9
- 6.4.0 to 6.4.10

FortiADC

FortiManager 7.2.1 supports the following versions of FortiADC:

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

FortiAnalyzer

FortiManager 7.2.1 supports the following versions of FortiAnalyzer:

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

FortiAuthenticator

FortiManager 7.2.1 supports the following versions of FortiAuthenticator:

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

FortiCache

FortiManager 7.2.1 supports the following versions of FortiCache:

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

FortiClient

FortiManager 7.2.1 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 7.2.1 supports the following versions of FortiDDoS:

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

Limited support. For more information, see .

FortiDeceptor

FortiManager 7.2.1 supports the following versions of FortiDeceptor:

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

FortiFirewall and FortiFirewallCarrier

FortiManager 7.2.1 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 7.2.1 supports the following versions of FortiMail:

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

FortiProxy

FortiManager 7.2.1 supports configuration management for the following versions of FortiProxy:

- 7.0.5

Configuration management support is identified as *Management Features* in these release notes. See Feature support on page 26.

FortiManager 7.2.1 supports logs from the following versions of FortiProxy:

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

FortiSandbox

FortiManager 7.2.1 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 7.2.1 supports the following versions of FortiSOAR:

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

FortiSwitch ATCA

FortiManager 7.2.1 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.2.1 supports the following versions of FortiTester:

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

FortiWeb

FortiManager 7.2.1 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.2.1 supports the following virtualization software:

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

Feature support

The following table lists FortiManager feature support for managed platforms.

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

Language	GUI	Reports
Korean	✓	✓
Portuguese		✓
Spanish		✓

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

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages 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 7.2.1.

> Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- FortiGate models on page 29
- FortiGate special branch models on page 31
- FortiCarrier models on page 33
- FortiCarrier special branch models on page 34
- FortiADC models on page 35
- FortiAnalyzer models on page 35
- FortiAuthenticator models on page 36
- FortiCache models on page 36
- FortiDDoS models on page 37
- FortiDeceptor models on page 37
- FortiFirewall models on page 37
- FortiFirewallCarrier models on page 37
- FortiMail models on page 38
- FortiProxy models on page 38
- FortiSandbox models on page 38
- 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 31.

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-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-400E-Bypass, FortiGate-401E, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, 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-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F	7.2

FortiGate 5000 Series: 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-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-KVM, 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

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-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-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-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,	7.0
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	
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-KVM, 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	

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-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 7.2.1 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see .

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-70F, FortiGate-71F	7.0.5	4530
FortiGate-3700F, FortiGate-3701F	7.0.6	6118
FortiGate-3000F	7.0.5	4451
FortiGate-3001F	7.0.5	4436

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F, FortiGate-401F	6.4.8	5206
FortiGate-600F	6.4.8	5306
FortiGate-601F	6.4.8	5301
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	6.4.8	1823
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiGate-7000F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	6.4.8	1823
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.4.7	5003

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.10	5168
FortiGate-200F, FortiGate-201F	6.2.8	7128
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	6.2.10	1211
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiGate-7000F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	6.2.10	1211
FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219

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 .

Model	Firmware Version
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-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, 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-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, 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	7.2

Model	Firmware Version
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-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-KVM, 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-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 7.2.1 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 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3700F FortiCarrier-3701F	7.0.6	6118
FortiCarrier-3000F	7.0.5	4451
FortiCarrier-3001F	7.0.5	4436

FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC FortiCarrier-7000F, , FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	6.4.8	1823

FortiADC models

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

FortiAnalyzer models

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

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

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.2, 6,3, 6.4

FortiCache models

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

FortiDDoS models

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

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.2
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.1
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.0

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.2.1 supports these models on the identified FortiFirewall firmware version and build number.

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

FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.2.1 supports these models on the identified FortiFirewallCarrier firmware version and build number.

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

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-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	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	6.4

FortiProxy models

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

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.2
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

Model	Firmware Version
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	6.4, 7.0, 7.2

FortiSwitch ATCA models

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

FortiTester models

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

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-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	

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-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7,0
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.3

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.2.1.

FortiManager 7.2.1 and FortiOS 7.0.8 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.1 and FortiOS 7.0.8 in mantis 841187. FortiOS 7.0.8 includes syntax changes not supported by FortiManager 7.2.1.

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

The following default values changed:

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

The following objects were added:

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

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

The following objects were removed:

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

Additional option changes:

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

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

Resolved Issues

The following issues have been fixed in 7.2.1. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
697444	SSID with MPSK may not pass verification during an install.
755815	The `local-standalone` and `local-authentication` features are inconsistent with FOS/FGT.
767774	The `power-level` and `power-value` installation failed as FortiManager attempts to change `power-level` and `power-value` under the `wireless-controller settings` at the same time.
794836	Protected Management Frames (PMF) feature always gets disabled when security mode is set to WPA2 (Enterprise or Personal).
810804	FortiManager does not support configuration for wireless-controller nac-profile.

Device Manager

Bug ID	Description
587404	FortiManager sets incorrect `captive-portal-port` value when installing version 6.0 policy package to version 6.2 devices.
676415	SAML account with remote certificate not imported to FortiManager Cloud.
704106	Certificate Enrollment fails using SCEP on Microsoft server with sub-ca certificate chains.
721242	FMG displays error *record internal is reserved* when creating a software switch named *internal*.
739746	When VDOM is enabled, FortiManager shows multiple firmware templates on Device Manager with different statuses.
743112	*Interface Bandwidth* widget on FortiManager under Device Manager does not display any data for FGTs.
746697	Cannot delete the `phase2-interface` within the IPSEC template.
753548	Error message *peer must be set* is displayed when configuring *IPSec Tunnel Templates*.

Bug ID	Description
757045	Installation failed with *invalid ip address* error when configuring multiple IP addresses for system dns-database's forwarder as the meta field.
759264	Applied system template does not apply properly on *Install Wizard* mode after modifying config on device level.
763234	Installation failed due to the syntax difference between FGT and FMG in setting `log-disk-quota` for VDOMs.
764491	Unable to configure more than one IP addresses for `vrdst` under the `interface vrrp` setting.
770600	Comma between IP address and subnet causes problems when saving *Prefix List Rule* under *BGP Templates*.
773147	Installation fails due to the unexpected system interface config changes for settings related to `pvc`.
775552	The *View device revision* under *Revision History* does not display the full and complete device configuration.
777391	Non-root Admins with access to only one ADOMs cannot properly build the HA Clusters in FortiManager.
778131	FMG did not support the per-device mapping for user SAML configurations.
784602	Max values for Link status under the Performance SLA for SDWAN template have been set wrongly.
785373	Configuration for `engine-count` in IPS global cannot be set higher than 8.
787205	Interface member field under the *System Templates* does not display any members.
787905	PM/AM feature for AV&IPS Scheduled Updates under the FortiGuard's *Device Manager* cannot be set correctly.
791117	Unable to create simultaneous static routes with named address objects.
792553	Removing VLANs from zone and adding a new VLAN to the same zone deletes that zone.
793021	Creating the interface type *software switch* throws an error when adding a *VLAN* interface as a member.
793495	Cannot select all objects filtered by the search under Device Manager.
793510	Special characters in meta fields are displayed in HTML numeric code.
793941	Unable to install VPN psk with special characters through CLI template.
795913	*Error Probe Failure* has been observed when adding FortiAnalyzer to FortiManager.
796447	FortiManager shows *CLI Provisioning* templates, even after removing association of provisioning template.
796842	Failed to reload the configuration due to the *datasrc invalid* error message.
796920	The *OPEN* mode is missing from the System Template WiFi SSID.

Bug ID	Description
799259	Duplicate CSF groups for 7.0 FGTs (7.0.2+) due to syntax returning `upstream-ip` instead of `upstream`.
800773	FortiManager doesn't show the filter configuration for syslogd correctly.
801022	Config status gets modified even though the installation preview is empty.
803683	Installation failed due to the `config wireless-controller snmp` settings.
804237	Unable to modify the firmware templates under the *Device & Groups*.
804523	After creating SD-WAN, IPsec, BGP, and CLI templates, the installation failed.
806622	Installation failed after configuring the link-monitor.
807404	Installation failed because of different values for `monitoring npu-hpe` between FortiManager and FGT-4201F.
809793	Unable to create VDOM link with vcluster.
811460	No option to set `add-route` enable/disable in P1 of IPsec template.
811487	Static Route template does not have option for SD-WAN configurations.
812335	BGP template does not have the option to enable `ebgp-enforce-multihop` feature.
812687	Unable to add FortiGate WiFi-80F-2R to FMG when Trusted Platform Module (TPM) is enabled.
813339	First install after adding a FGT to the FMG failed due to FMG's attempt to install a new SSID passphrase for the virtual access point (VAP).
814190	FMG's export or import template feature is not working properly.
816443	SNMPv3 IPv4 notification host does not exist on the FMG's GUI anymore.
820990	IPsec VPN deployment by using ZTP creates some issues on the FGT routing.
822644	Creating a *New Action* for *Interface* under *Provisioning Templates > System Templates* makes FMG's GUI unresponsive.
829404	SD-WAN Widget does not display any data for "Bandwidth Overview" and "Traffic Growth" under the *Managed Devices*' dashboard.
830105	FMG attempts to install 1.0.0.0 as the `remote-gw` IP address for all the `phase1-interfaces` when two or more IPsec `phase1-interfaces` have same `remote-gw` IP address.

FortiSwitch Manager

Bug ID	Description
772396	*Dynamic Port Policy* feature was not supported under the *FortiSwitch Manager* section of FortiManager.

Bug ID	Description
786283	IP Address Assignment Rules cannot be removed under the VLAN per device mapping.
803175	FortiSwitch template does not enable all the PoE interfaces.
817436	LLDP profile cannot be changed when *Access Mode* is set to *NAC* in FortiSwitch template.

Global ADOM

Bug ID	Description
767325	Failed to assign global ADOM v6.2 policy to local ADOM v6.4 due to policy IPv6 changed duplicate object.
768527	After upgrading the global ADOM, installation failed due to the custom ssl-ssh-profile configuration.
794206	Policy installation fails due to Global Object adding prefix `g-` in threat feed.
811660	Global Database object assignment to ADOMs fails.
815130	Global Policy Assignment in FMG displays the *TCL error - dstintf in policy cannot be empty* error.

Others

Bug ID	Description
575863	Failed to upgrade ADOMs as FortiManager forces users to upgrade unregistered devices first.
671516	FMG/FAZ cannot accept more than 100 concurrent admin sessions (using JSON APIs).
741767	FGT's firmware upgrade API is missed from the documentation.
747648	FMG does not support some of the FEX models and versions under FEX profiles.
759333	After upgrading ADOM 6.2 to 6.4, status of all policy packages changes to *Modified*.
764388	FortiManager's GUI does not support *ACI FortiSDNConnector* and *Nuage* configurations.
766485	FortiManager and FortiAnalyzer frequently generate error logs with message "service:geoip, fgd server 'gip.fortinet.net' was unreachable.".
770040	FortiManager's web interface and especially API calls are very slow if `object-revision-status` feature is enabled.
781831	FortiManager should be able to retrieve EMS tags using hostname of FortiClient EMS, if it can resolve the hostname.

Bug ID	Description
782139	FortiManager GUI does not display any of the proxy settings and webcache for FortProxy devices.
783226	*Fabric View* may keep loading.
784034	HA Configuration in Zero-touch provisioning (ZTP) does not synchronize to the secondary FortiGate.
784037	FortiManager offers low encryption cipher suite in TLS 1.2.
786281	During the installation, FortiManager displays *Policy Consistency Check* failure without any clear reason.
786786	New API deployment on FortiManager to support the NSXT API integration does not send any notification from the NSXTService Manager to FortiManager.
788006	FortiManager consumes license count for the Admin Type VDOMs.
792296	ADOM upgrade fails due to the virtual wire pair policy.
792887	Verification fail for default dnsfilter profile due to wrongly installed `set category 0`.
794256	Unable to export update manager log files for the `sftp fdssvrd`.
794304	*Interface Bandwidth* widget is displayed in ADOM 6.2 in FortiManager version 6.4.
795111	Unable to add or modify a FPX *Explicit Proxy*' policy from a FortiProxy ADOM in FortiManager.
797165	FortiManager has some unsupported commands for the FortiToken user definition.
798220	FortiExtender status is always offline.
799835	A significant and continuous increase in memory usage by "rtmmond" has been observed.
799835	A significant and continuous increase in memory usage by "rtmmond" has been observed.
804244	ADOMs created by XML API cannot be locked or unlocked.
805226	ADOM upgrade uses too much memory, and this makes the upgrade process too slow.
806109	After ADOM upgrade, `log-all` is disabled for all protocols under *Email Filter* profile.
811114	On the FortiProxy ADOM, interface for configuring the `web-proxy explicit-proxy` cannot be selected from the dropdown menu list.
813443	FortiManager does not support the FGT-GCP different IP addresses on interfaces and different source DNS IP addresses.
815875	After upgrading FortiManager, device-level status has been modified and *Install preview* shows that pdf-report and FortiView features will be enabled on the FGTs, even if these are already enabled on the FGTs.
816444	Extender manager doesn't display RSSI/RSRP/RSRQ/SINR info.
816834	FMG does not support FortiWeb and activate its license.

Bug ID	Description
817667	FMG cannot upgrade the ADOM to v7.0 due to several cdb crashes during the upgrade.
819495	FortiManager JSON API `set` and `update` work similarly for template and policy package `scope member`.
820656	FGT 7.2.1 failed to fetch the FortiGuard rating from FortiManager without raw database flags.
820862	Extenders are not displayed on FortiManager.
822263	*FortiGuard > Service Status* does not correctly display the secondary service status of the FortiGate's cluster.
823111	After upgrading to 7.0.4, FMG removes the `dev-obj` data upon rebooting.
823278	Unable to manually import Query Category FortiGuard package.
823294	SSH connection between FortiGate and FortiAnalyzer/FortiManager v7.0.4/7.2.1 or later fails due to `server_host_key_algorithms` mismatch.
825052	Not able to add the FortiProxy to the FortiProxy ADOM.
826718	Failed to delete the hanging task from task monitor.
828808	EMS Connector unable to connect to FortiClient EMS Cloud.

Policy and Objects

Bug ID	Description
620680	FMG does not support the geographic fields data for firewall internet-service objects.
705302	Remote VPN Certificate installation failed, and certificate disappeared from FortiManager; however, on the FortiGate the certificate installed successfully.
706809	Policy Check export does not have the last hit-count details anymore.
714375	No warning messages when assigning a normalized interface that is already in use.
721253	FortiManager may not import all the roles and address groups from ClearPass.
725132	When modifying IP address of Default VPN Interface of spoke in Device Manager, hub remote gateway should be modified to reflect that change.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPsec policy.
731037	There may be *File Filter* file type mismatch between FortiGate and FortiManager.
737424	Policy package import fails due to the *Device mapping::"query failed."* error.
751767	Export to Excel when filters are applied for a policy package does not work.
758680	Unable to complete the Cisco pxGrid fabric connector's configuration on FortiManager.

Bug ID	Description
760918	Unable to change the action field for the default IPS profile and their clones.
765154	Installation fails when trying to disable the *safe search* on existing DNS filter from FortiManager.
767255	FortiManager fails to install the custom signature because it is too long.
768125	Default configurations of the Potentially Liable category under the Webfilter are different from their corresponding ones on FortiGate.
773333	The configurations for two-factor-authentication and two-factor-notification should not lead to installation failure.
773403	FortiManager may now differentiate between the ISDB objects *Predefined Internet Services* and *IP Reputation Database*.
775128	Unable to create more than 20 SAML users in policy package object.
777017	FortiManager purges the `arrp-profile` when installing the v6.2 policy packages to v6.4 FGTs.
778171	After the upgrade, FortiManager is changing the *config antivirus quarantine* setting, causing the installation to fail.
789238	Installation error occurs when configuring a VIP with per-device mapping and setting an External IP Range to an IPv4 Range.
791357	Installation failed when using `custom-deep-inspection`.
792980	Installation fails when trying to install SAML user configuration.
793603	Registering a service under the connector configuration displays an error "Failed to run script.".
796505	Modifying the *Sections* under *Policy & Objects* leads to some unexpected changes or behavior.
796512	Wrong direction definition has been displayed for `Tor-Relay.Node` ISDB object.
798094	Re-assignment of tokens in FMG policy and objects, deletes and re-adds the firewall policies that are used those objects.
798955	Traffic shaping policy changes do not trigger any changes or updates on the policy packages status.
798958	Policy Consistency Check fails due to the firewall service's name.
799538	The export policy feature displays limited numbers of the group objects.
801876	Installation failed due to "Copy global shared objects" failure.
802072	"Auto-asic-offload" cannot be disabled for the first time in the policy.
802934	FortiManager'sPolicy Package Diff displays policy objects change even though there is not any changes.
805178	Installation failed due to the unnecessary setting changes of logtraffic feature in proxy policy.

Bug ID	Description
805211	Installation failed due to the wrong fsw vlan type for the default nac and nac_segment vlans.
805642	New policies created in policy package do not inherit the `global-label` section.
805649	Any modification to the *peer group* object within the *VPN Manager* pane, changes the policy status to *Modified* for all devices, even though spoke devices have different policy packages than hub devices.
805966	Verification fails due to the "resource-limits.proxy".
808900	Incorrect error message is displayed when re-installing the same policy to FortiGate immediately after the first installation.
809276	Cloning administrators doesn't copy the specified ADOMs for the cloned administrator and wrongly displays *All ADOMs*.
809888	*Replacement Message Group* under *Security profiles* gets removed by FMG during the installation.
811503	Installation failure due to the extender-controller `error 33 - duplicate`.
811715	FSSO dynamic addresses were visible on two address groups.
813237	View Mode feature does not work properly when workspace mode is enabled on FMG.
814090	*Export to Excel* does not work if the policy package has policies other than default *Implicit Deny*.
814468	FMG purges `gcp-project-list` and unsets several values from GCP `sdn-connector`.
815812	Installation failed because FortiManager tried to remove the credentials for Amazon Web Services (AWS) type of SDN Connector and enabled the `use-metadata-iam` feature.
816347	Objects field search under the *Add Object(s)* feature does not properly locate any firewall object addresses for source and destination.
818512	In WorkFlow Mode, adding a single policy removes and re-adds the entire policies.
819665	*Installation Preview* does not display the *DNS-Filter* configuration changes.
819713	FortiManager in task manager does not show the specific admin name who refreshes the hit-count.
820939	*Firewall Users* does not populate the user authenticated through explicit proxy authentication method.
821412	The Policy Block's name cannot be edited if "/" character is being used.
827602	Unable to import EMS Tags from EMS Server.
827607	The enable/disable status feature for the EMS Connector is not available on FortiManager.
828492	Policy installation fails when using `sdn-addr-type all`.

Revision History

Bug ID	Description
496870	Fabric SDN Connector is installed on FortiGate, even when not in use.
691240	FortiManager should not unset the value `forward-error-correction` with certain FortiGate platforms.

Script

Bug ID	Description
793407	Installation fails if one of the BGP network prefix entries is a `supernet`.
800149	FortiManager reorders the <ID>s in ascending order for BGP and static settings.

Services

Bug ID	Description
704584	FAP firmware may not be listed and cannot be imported.
752849	FortiManager doesn't have the proper version string of FGT's IPGeo Info.
796345	FortiManager does not recognize the entitlement file for some FGTs.
798979	FortiManager cannot download the latest IPS DB.
808121	FortiManager ignores `add_no_service` setting for the *Unauthorized Devices*.

System Settings

Bug ID	Description
687223	Users may be unable to upgrade ADOM because of `profile-protocol-options.`
753690	SNMPv3 security option configuration has discrepancy between GUI and CLI.
780245	Install Wizard shows all devices are selected, even though *Default Device Selection for Install* is set to *Deselect All*.
794461	In Workflow mode, admins are not able to approve or reject sessions by emails.
795655	FortiManager loads the *Administrator* list under *System Setting* very slowly.

Bug ID	Description
796058	Search box in the *Edit Meta Fields* page under *System Settings* does not work.
799519	If Management Extension Applications (MEA) are enabled, all system settings may be lost after upgrading FortiManager.
799619	When *Advanced ADOM Mode* is enabled, FortiManager under the *Device Inventory* displays all devices from all VDOMs.
803200	FortiManager does not synchronize with NTP server.
807788	Unable to disable the trusted hosts from the GUI.
807983	FortiManager doesn't display *NTP daemon change time* event log when it synchronizes with the NTP server at booting.
811633	Restricted Administrators using the API requests have full read-write access.
817244	Sorting function feature does not work properly based on the *Device* column in the *Meta Fields* under *System Settings*.
818969	Unable to poll SNMP with SNMP engine ID.
819383	FortiManager disk usage rises to 100% when `traffic-shaping-history` enabled.
821221	Enabling the debug by remote users with *Super_User* admin profiles disconnects them from the FMG's GUI and CLI.
827854	Installation target disappears in workflow mode if session is approved through email.

VPN Manager

Bug ID	Description
615890	IPsec VPN *authusergrp* option *Inherit from Policy* is missing when setting *xauthtype* as *auto server*.
794168	Installation becomes very slow when FortiManager acts as CA server.
796104	FortiManager deletes and re-creates VPN routes with different IDs on every install.
807063	Unable to delete any of the new *Authentication* or *Portal Mapping* entries under *SSL VPN Settings*.
810027	FortiManager spoke IP setting for VPN configuration sets properly, but the policy package does not change on the hub phase1.

Known Issues

The following issues have been identified in 7.2.1. To inquire about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
661938	FortiManager displays an error when trying to edit and save managed APs.
819137	Installation failed if Distributed Automatic Radio Resource Provisioning (DARRP) is disabled on AP Profile.
822525	FortiManager does not take the per device mapping authentication config for SSID under the Wifi Profiles.
824032	Some of the FAPs Radio configuration settings under the AP's profile are missing.
853345	The clients are connected to the Wireless Access Point; however, "clients" section under the diagnostics & tools of AP does not display any info.
861579	Unable to add the AP to the *AP Manager* due to the error "Parent object does not exists" message.

Device Manager

Bug ID	Description
723006	FortiManager does not support creating the "DHCP Reservation" under the "Network Monitors Widget".
738276	FortiManager's GUI does not display the "Routing Objects" under "Router".
745122	FortiManager unsets the ipv6 configuration during the installation to the FortiGate.
745586	Local firmware images are duplicated under the *Device Manager*.
748579	CLI configurations for SD WAN template is not working properly.
761066	FortiManager does not display the VLAN's protocols on GUI for FortiGates.
763036	Physical Interface Members are not displayed for the "Hardware Switch" type on FortiManager when FortiGates are added using *Model Device* method to the FortiManager.
773338	Unable to save the Virtual Router Redundancy Protocol (VRRP) settings for FortiGate's

Bug ID	Description
	interfaces.
786264	Unable to delete default "wireless-controller" "vap" configuration from the device DB.
788923	SD-WAN template does not change the value of "`service-sla-tie-break`" for a SDWAN Zone.
789249	FortiManager does not have Logging Options after enabling One-Arm Sniffer under Interface.
789544	Status of the "Firmware Template" has been changed to "Unknown" after upgrade.
794764	FortiGate Modem Interface is not visible under *Device Manager*.
797404	After successfully running all the Assigned Templates to FortiGates, the status is displayed as *Modified*.
800191	During the ZTP deployment, `set hostname` command does not push to FortiGate.
801415	FortiManager adds quotations to IP addresses when configuring trusted hosts for "`switch-controller snmp-community`" under the GUI's CLI Configuration.
801547	When removing an entry in the static route template, static route entries are shifted and the installation fails.
804142	Creating the "EMACVLAN" type Interface on FortiManager displays an error "VLAN ID is required".
807771	FortiManager unsets the gateway settings in SDWAN template after upgrading ADOM from v6.4 to v7.0.
810936	After Upgrade, managed FortiAnalyzer on FortiManager does not display the Traffic logs under the *Log View* for HA devices.
811067	When creating/editing a blueprint, the "Firmware Enforcement" value is different from the default "Enforce Firmware Version" value.
812213	Default factory setting on FortiGate does not match with its default factory setting on FortiManager's DB. This causes status conflict if the FortiGate is added to the FortiManager using the "*Add Model Device*" method.
815901	The router static entries created by IPSEC template are deleted and re-created after upgrade.
818905	FortiManager unsets the certificate for "`endpoint-control fctems`" setting during the installation.
820436	FortiManager displays an error, "Failed to update device management data.", when adding a model device based on ZTP approach.
820506	FortiGate BGP neighbor password field shows long, random string when BGP neighbor config is edited.
821866	For FortiGates with FGSP (FortiGate Session Life Support Protocol) configuration, "`ipsec-tunnel-sync`" feature under the cluster-sync cannot be disabled.
823092	Not able to add multiple OU (Organization Unit) fields in the Certificate Templates.
823281	Changing Time/Schedule for scripts under the *Device Manager* makes the *OK* button grayed

Bug ID	Description
	out.
824318	The *Description* column for interfaces displays wrong info (Up or Down).
826141	VLan interface cannot be created and mapped toa hardware switch interface on the FortiManager.
828122	"Device Detection" gets enabled by FortiManager during the installation.
828897	*SD-WAN Monitor* map doesn't load all devices.
829240	"*Import CLI Script*" feature is part of the "*More*" button entries under the *Device Manager*'s Scripts.
830085	FortiManager's GUI does not display the "Replacement Messages" under *System* for its *Managed Devices* after visualising it via "Feature Visibility".
830727	FortiManager-DOCKER platform does not support adding the FortiAnalyzer-DOCKER device.
831290	Failed to delete template group with "/" in their names.
831733	Unable to create any new entries for any of the sub tables of the BGP Router like Neighbors, Neighbor Groups, and etc. due to "datasrc invalid." error message.
832321	Configuration changes on the AP/Switch/Extender settings do not apply on the device db when these changes are created from the system template.
832599	When installing the "config system snmp community" settings to FortiGates, some of the entries are deleted.
832753	FortiManager does not install configurations from CLI Template group to FortiGates.
834947	"Resource-limits" proxy default value is missing under the *Device Manager*'s CLI Configurations.
835106	FortiManager cannot sync its devices with FortiAnalyzer when adding it to the *Device Manager*; it displays the error message, "Serial number already in use".
835451	Editing SD-WAN/IPSec template (with no actual changes) removes all assigned devices.
838285	The DHCP server config under the FortiGate's interfaces does not work properly; it shows the DHCP status as OFF and once fixed creates another identical entry under the DHCP Server.
838334	Unable to modify, install, or add members to Zone under the *System Template*.
839243	"Assigned to Device/Group" under the *System Templates* does not keep its config after FortiManager's upgrade.
842923	Auto-update fails to sync FortiManager's device DB when interfaces are modified directly in the root VDOM of the FortiGates.
844979	Multiple issues under log settingsfor upload-time, FortiAnalyzer Cloud store-and-upload have been observed.
845552	FortiManager's GUI freezed after clicking on the "*Upgrade Preview*" and "*Upgrade History*" under *Device Manager > Firmware Templates*.

Bug ID	Description
845656	When BGP is enabled and no IP address is defined for `set-ip-nexthop` under the `route-map` config, FortiManager tries to set the IP to 0.0.0.0, and this may break the BGP network.
847631	Failed to reload the FortiGate's configuration.
848485	"Enable FortiGuard DDNS" feature, under the DNS settings of each managed devices, cannot be unset.
849507	IPSec Template clone does not preserve phase 2 dhgrp setting.
850941	"Upgrade Now" page under the *Firmware Templates* does not show up when multiple devices are selected.
853061	Installation fails as FortiManager attempts configuring "allowas-in6" on neighbor when configuring router bgp via BGP template.
853810	Failed to edit the managed devices to modify the location.
854401	Unable to access to the FortiGates via SSH and GUI Console Widget once the FIPS mode is enabled from FortiManager.
855032	FortiManager displays the total devices/VDOMs count wrongly when split VDOM enabled on FortiGates.
855425	*System Template* and *CLI Template* config did not install to all model device FortiGates.
857039	After modifying the SSH Administrative Access for FortiGate's interface on *Device Manager*, FortiManager attempts to install the PPPOE's password again to the FortiGate.
858591	Editing the interfaces for any of the managed devices displays an error message.
859249	After upgrade, *Firmware Templates* under the *Device Manager* is blank. Even new entries cannot be created.
859638 860071	FortiManager's *SD-WAN Monitor* does not display the Health Check status correctly.
860208	FortiManager's GUI does not save the http port number when configuring the "Explicit Web Proxy" under the *Device Manager*.
861220	Leaving the SD-WAN member empty when configuring the SD-WAN using the template fails due to the syntax differences between FortGate and FortiManager.
861238	*SD-WAN Monitor*, under *Device Manager > Monitors*, displays an Unknown status (a grey question mark) icon for HA devices under the Map View.
863062	Modifying the SDWAN Overlay Template removes the corresponding BGP template network config.
863417	Proper IP configuration did not apply to FortiGates when provisioned via ZTP.
865583	"`replacemsg-override-group`" under the system's interface of managed devices is blank.
866243	The *SD-WAN Monitor* info for specific devices are not consistent with the map view SD-WAN

Bug ID	Description
	interface status (based on performance SLA).
866920	System switch-interface member (internal) cannot be used and provisioning template CLI scripts execute out of order.
870848	*SD-WAN Monitor*, under Device Manager > Monitors, does not display any FortiGate devices which are running in 6.2 version.
874811	FortiManager tries to set the "set-ip-nexthop" to "0.0.0.0" during the installation.
874831	FortiManager attempts to install unknown and undesired static route when modifying or adding some new static routes.

FortiSwitch Manager

Bug ID	Description
818842	FortiManager displays "Failed loading data" for "Security Policy", "LLDP Profile", and "QoS Policy" features when editing ports in Per-device mode FortiSwitch Management.
820167	Refreshing the FortiSwitch changes the status to "Unknown".
820182	Using *Export to Excel* feature for managed switches under the *FortiSwitch Manager* exports a corrupted file.
829700	FortiManager shows errors while installing FSW configuration.
830099	*FortiSwitch Manager* displays the "Missing Switch ID or Platform Info" error.
833262	*FortiSwitch Manager* does not display the list of firmware images for the FSW 108F-FPOE model.
847846	*FortiSwitch Manager* does not display the correct switches and switchport status info.
868949	Installation fails as *FortiSwitch Manager* creates an alias name longer than the total limit 25 characters.

Global ADOM

Bug ID	Description
789164	Unable to delete the web rating override entries from ADOM Global Database.
835172	Global ADOM Assignment fails when assigning some profile groups.
835439	Global Policy assignment is not completed successfully due to some missing objects on Global ADOM.

Bug ID	Description
838174	FortiManager does not provide a clear error message when Global IPS Header/Footer profile assignment fails.
842934	Global address group cannot be modified from FortiManager GUI.
847533	Unassigned Policy Package cannot be removed from Global ADOM.
868212	Assigning global policies to ADOMS by admins with access to specific ADOMs fails.

Others

Bug ID	Description
671471	In ADOM backup mode, when address objects are modified on FortiGates, modified objects are not imported into FortiManager.
711100	FortiManager does not handle RMA and replaced FortiGates efficiently when ZTP has been used.
739219	FortiManager's timeout parameters cannot be set by users as it is hardcoded.
742819	Promote to global feature should not be possible since GLOBAL ADOM are not accessible in FortiManager Cloud.
745958	Unable to config ipsec tunnel using the ipsec tunnel template.
746516	Preferred Version cannot be saved for *Managed Devices* under the Firmware Images of FortiGuard Pane.
750242	FortiManager's DB in HA clusters are not properly synced together.
757524	FortiManager displays many "duplicate license for [FGT devices SN Number] copy AVDB to AVEN" error messages.
777028	FortiManager does not support the FortiCarrier-7121F.
793085	Sub Type Filter on Event Log search does not show any results, even if logs are present.
795624	FortiManager does not let users to copy the contents of the "View Progress Report".
799378	FortiManager's admins are not able to run FortiManager's CLI scripts/commands from remote stations.
811018	FortiManager does not support copying of the objects from the Policy Packages and pasting them to the search field.
811798	Policy Package status gets not updated on the GUI after a successful installation.
816936	FortiManager does not support the FGT/FGC 7KE/7KF syntax.
818513	FortiManager does not support the FortiProxy v7.2.
820071	Upgrading the FOS/FGT firmware version via FortiManager did not complete successfully.

Bug ID	Description
820248	cloningsame ADOM multiple times fails with error "Unknown DVM error".
820578	"svc authd" process is consuming 100% of CPU.
820921	FortiManager displays incorrect device firmware versions for FortiSandbox and FortiMail.
821940	Static Route cannot be created under the *Device Manager* when FortiManager works in Workflow mode.
823547	In Advanced ADOM mode, it is not possible to create a new VDOM in a new ADOM via JSON API request.
824316	FortiManager displays an error when "adom-integrity" is performed.
826881	FortiManager attempts to apply some changes to voice, video, and interface configurations.
829726	Already existing CLI Templates cannot be modified after the upgrade.
830881	ADOM upgrade fails due to the ID of the sdwan applications; they are larger than the initial defined values.
831453	FortiManager shows an error message when multiple FortiGates are selected to be upgraded to the new version.
831616	FortiManager cannot install policy package when using Provisioning Templates as tasks got stuck.
833162	FortiManager does not support the FortiProxy 7.0.6.
833623	Estimated Bandwidth for Upstream & Downstream under the interfaces and Upload & Download values under the SD-WAN Monitor's table-view are displayed differently.
835313	FortiManager displays many "duplicate licence" messages for "copy AVDB to AVEN".
835748	FortiManager's GUI takes very noticeable time to load properly when navigating to Policy & Objects tab.
836489	Firmware Images under the FortiGuard for "All" or "Managed" devices display same list.
838949	Using the 'refresh' feature in the FortiExtender GUI does not refresh the stats of (RSSI, RSRP, etc.) of the associated devices.
839035	"Check License" under the FortiGuard's Licensing Status does not keep the changes.
839586	FortiManager does not save applying the configuration of "Enable AntiVirus and IPS service for FortiDeceptor" under FortiGuard settings pane.
840068	Unable to export device stored FortiGuard signatures through tftp protocol.
841187	FortiManager does not support the FGT/FOS 7.0.8 Syntax. See FortiManager 7.2.1 and FortiOS 7.0.8 compatibility issues on page 41.
845753	IPSec installation fails on Google Cloud Platform (GCP) ONDEMAND FortiGate.
850377	In Workflow Mode, when new session is created, the Policies disappear.
850467	Unprivileged Users might be able to disclose unauthorized information via API.

Bug ID	Description
855840	'allowaccess' on interfaces completely removed on GCP ONDEMAND FortiGate.
857659	FortiManager did not download the "AI Malware Engine" Package from FortiGuard Server.
865200	Users encountered unsatisfactory performance of FortiManager due to several crashes on the "Application fmgd" process.
870893	Unable to install pp to FortiGates, after FortiManager's DB got restored.
874369	Upgrading FortiManager fails due to some invalid data for managed FortiExtender's Objects.
876425	FortiManager does not display the output of "`execute dmserver showconfig`".
919088	GUI may not work properly in Google Chrome and Microsoft Edge version 114.

Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
688586	Exporting Policy Package to *CSV* format shows *certificate-inspection* in the *"ssl-ssh-profile*" column even when the profile is not in use.
724011	FortiManager needs to support multiple server certificate list in ssl/ssh profile.
841187	FOS 7.0.7 syntax support. See FortiManager 7.2.1 and FortiOS 7.0.8 compatibility issues on page 41.
844985	Per-device mapping is not supported for Virtual Server with "IP" type.
698838	"Download Conflict File" does not display all of the firewall objects conflicts when importing policy packages from FortiGate to FortiManager.
703408	FortiManager does not display the interface type Geneve for interface mapping.
704354	"Blocked Certificates" and "Server certificate SNI check" features cannot be configured on SSL/SSH profile.
707481	Deleting DNS filter profile does not delete the associated Domain filter.
711202	FortiManager does not support managing SAML user objects from *Policy and Objects*.
716892	Exporting to "Excel/CSV" does not include the value for fields "Log & Last Modified By".
731961	When FortiManager is working in the workspace mode, the installation for those FortiManagers with larger DB may take longer time to be completed.
738988	FortiManager does not detect the settings related to Web Cache Communication Protocol (WCCP) in SSLVPN Policies on the FortiGate.
741269	Unable to install configuration to FortiGates due to the error message "Resource temporarily unavailable".

Bug ID	Description
742293	FortiManager, via ADOM 6.0, is not able to install "set logtraffic all" to proxy-policy with action deny.
747340	FortiManager does not support variables for source IP field under the Advanced Options of the Fabric Connectors' Threat Feeds.
752993	VPN IPSEC installation fails as phase1 settings on FortiManager are not consistent with the ones on FortiOS.
762392	The rating lookups does not return the correct category for the URL when it ends with "/" character.
765487	Install Wizard for Policy Package with no changes displays "No record found.", which is not a clear message.
783195	FortiManager changes the "`cert-validation-timeout`" value to block when installing to the FortiGates.
810073	Fail to import the firewall policy due to the "interface mapping undefined" error message.
812886	On FortiManager, an internet-service-custom objects without protocol number or port-range can be configured on firewall proxy-policy; however, FGT/FOS does not support this.
812909	FortiManager unsets the "`bypass-watchdog`" setting on FGT400E-Bypass.
814364	FortiManager does not support the FCT EMS prefix; therefore, policies with ZTNA Tags cannot be installed properly to the FortiGates.
814970	EMS Connector is not able to import Tags when Multi-Site enabled on EMS Server.
815281	SDN Dynamic Address object filter does not display the list properly.
816108	The "`group-poll-interval`" value for FSSO fabric connector cannot configured properly.
817220	FortiManager does not support the "userPrincipalName" as the common Name Identifier for LDAP Server configuration.
819847	FortiManager displays a false warning message "Duplicate Objects With Same Values" when creating the Firewall Objects' Service entries under the Policy & Objects.
822843	FortiManager displays an error when using the access-proxy type VIP and normal VIP in firewall policies as they are both using the same external IP.
825411	Installation fails when an application group with category 32 (unknown applications) is configured on FortiManager, even though this category is accepted on the FortiGate.
825530	Explicit web proxy policy does not allow selecting any source address objects.
825873	FortiManager does not support FortiGate/FortiOS global scope (g-) objects.
826928	During the installation, FortiManager attempts to remove the physical ports which are members of the virtual-switch config.
826946	FortiManager does not show anything to install on FortiGates even though the Policy Package has been modified.
827242	For Policies under the Advanced Options, "`custom-log-field`" uses Names instead of

Bug ID	Description
	IDs.
830043	Creating the Custom ipv6 service where icmpcode is not configured causes the Policy Package to get into a conflict state.
830502	FortiManager fails to create the CSV for Policy Package.
831225	Cloning a policy with VIP referencing SDWAN member causes subsequent installs to fail.
831273	FortiManager does not allow deleting the entries for "server-info" under the log "npu-server".
831407	NSX-T connector configuration does not display "VM16" and "VMUL" types.
831484	FortiManager was not able to connect to the "NSX-T Connector" and several "Application connector" failures have been observed.
832962	If Firmware Template status is "Unknown", FortiManager allows installing the Policy & Packages repeatedly to the FortiGates.
834102	Editing Fortinet Single Sign-On Agent entry under the Endpoint/Identity removes FSSO user groups from the Firewall Policy.
834401	Upgrading ADOMs do not complete if there are some empty values for "`profile-type`" and "`utm-status`".
834447	Objects are not visible in the '*Addresses*' tab when per-device mapping feature is enabled.
834558	Installing tunnel interfaces which are created by ipsec template fails.
834806	Installation fails due to extra back slashes when installing the custom IPS signatures to the FortiGates.
836103	FortiManager pushes old internet-service-names "Facebook" instead of "Meta".
836783	FortiManager changes the "`use-metadata-iam`" value for the SDN connectors.
836933	Changes on the External-Resource settings from ADOMs for specific VDOMs/FortiGates alter the External-Resource settings for other ADOMs and VDOMs.
837555	Connector's Service Name, after FortiManager's upgrade, does not display the correct name.
838533	SASE zone cannot be removed from SDWAN Template.
841492	FortiManager unsets the system HA settings after pushing an unsuccessful installation Policy Package to FortiGates.
843765	FortiManager does not display the proxy address members under the proxy address group.
844985	Per-device mapping is not supported for Virtual Server with "IP" type.
845638	"ztna-ems-tag"s created on FortiGates are not same as ZTNA Tags created on FortiManager; hence, the installed tags from FMG to FGTs, used in firewall does not police the traffic properly.
847932	Hit count for a policy package does not always match the total count of all installation targets.
848666	"Install Device" task stuck without any progress when installing the templates and firewall policies to the FortiGates.

Bug ID	Description
849470	When creating a new firewall policy via API Request the "global-label" option is skipped.
850204	Installing an AWS connector with Metadata IAM enabled displays an error message.
851331	Cloning Firewall Addresses under the Firewall Objects does not clone the "Add To Groups" entries.
853815	New created LDAP users are displayed based on the <CN> attributes and not the <sAMAccountName> attributes or User ID parameters.
853851	FortiManager displays all the FortiTokens for the FortiToken settings under the User Definition even though some of them are already being assigned.
858183	After firmware's upgrade, virtual wire pair interfaces are missing in virtual wire pair interface policy.
859217	Rearranging the Destination NAT (DNAT) objects whose names contain special characters displays an error message "object does not exist".
862727	Policy Package installation failed due to the error "native vlan must be set" message.
862839	Cloning the Policy Packages on FortiManager creates the duplicate UUIDs.
863882	'Last Modified Time' field is empty when exporting Policy Packages to Excel.
866826	Failed to modify Virtual Server addresses in Firewall Polices with Deny Action.
870688	Editing the "Install On" changes the Policy status to "Modified" for all FortiGates existing on that rule.
873896	Unable to remove "(null)" objects under "endpoint-control".
874188	Installation fails due to FortiManager's attempts to remove the "endpoint-control fctems" entries.
875980	FortiManager unsets EMS connector Serial Number and the tenant-id during the installation.
838648	"Rename objects to import" inconsistency with "datasrc duplicate" error.

Revision History

Bug ID	Description
809191	Configuration change of HA-logs setting is not reflected into the revision history.

Script

Bug ID	Description
808398	"View script executing history" displays scripts related to other ADOMs.
817172	Running scripts to add static route has been failed due to the "duplicate of static route" error.
821778	Using scripts do not create the ssl-ssh-profile with certificate inspection mode; instead, it sets the value to deep-inspection mode.
829918	Scripts contain meta variables do not work after upgrade.
833285	Installation failed when executing multiple Jinja scripts.

Services

Bug ID	Description
779997	When upgrading the multiple FortiGates at the same time from the "*Firmware Upgrade*" feature does not let users to click "*OK*".
827982	Downstream FortiManager cannot get all the FDS/FGD packages from upstream FortiManagers in cascade mode network design.
837942	In cascade mode, FortiManager as local FortiGaurd Server does not download IPS signature for extended database.

System Settings

Bug ID	Description
753204	Admins of a specific ADOM are able to see tasks of others ADOMs.
777153	FortiManager displays an error when setting up a "Remote Authentication Server" with "No Certificate" option.
801580	Fail to use the Online Help as does not use the proxy config setting which has been set for FortiManager/FortiAnalyzer.
815728	FortiManager takes very long hours to rebuild the HA Cluster back to synchronization status.
822776	Query Distinguished Name does not display the LDAP users in FortiManager when Secure connection is enabled.
823898	FMG does not use all of the configured "ssl-cipher-suites" under its "system global" settings.
825078	New admins with ADOM only access cannot see the previously assigned header and footer

Bug ID	Description
	policies on that ADOM.
829751	Installation tasks got stuck at 0 % and failedtostart any new installation tasks.
830242	FortiManager in Advanced Mode does not show the number of allowed VDOMs correctly.
833989	Cannot set/change the service access settings on the interfaces when the language is not set to English/French.
839168	FMG-VM with perpetual license uses built-in image with serial number *FAZ-VM0000000001* to manage devices. For a workaround, see Special Notices on page 11.
841782	In Workflow mode, admins are not able to click on the "Approve this request" received from the emails as it displays "Unable to complete action" or "Invalid adom name" error messages.
841931	When FortiManager works in Workspace Mode, users are able to disable "Per-Device Mapping" without locking the ADOMs.
843520	After firmware upgrade, FortiManager/FortiAnalyzer's HA Cluster is broken and Access to the Secondary fails.
848934	SNMPv3 does not work properly on FortiManager and FortiAnalyzer.
850469	Radius group attribute filter does not work with Microsoft NFS.
851029	FortiManager's HA cluster breaks after upgrading the FortiManager.
853353	*SDWAN Monitor* Map does not show up when admin profile has been set to "None" for *System Settings*.
862592	Upgrading FortiManager did not finish and GUI displays the "Temporarily Unavailable" message.
862814	Event logs did not log FortiManager admins and their actions on managed devices.
864041	SNMPv3 stopped working after upgrading the FortiManager.
864931	Unable to login into FortiManager using TACACS and Radius credentials.

VPN Manager

Bug ID	Description
762401	FortiManager is unable to preserve the Specify custom IP ranges option for SSL VPN Address range setting.
831076	Static Route (Protected Subnet of the HUB) is not installed to Spoke during install, with HUB and Spoke Dial-up VPN setup.
866248	Configuring a new mesh VPN using VPN Manager failed due to the extra character in the encryption method for Phase2.

Appendix A - FortiGuard Distribution Servers (FDS)

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

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

FortiGuard Center update support

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

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

Appendix B - Default and maximum number of ADOMs supported

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

Hardware models

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

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

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

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

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

Virtual Machines

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

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

FortiManager VM subscription and perpetual licenses are stackable.

FÜRTINET