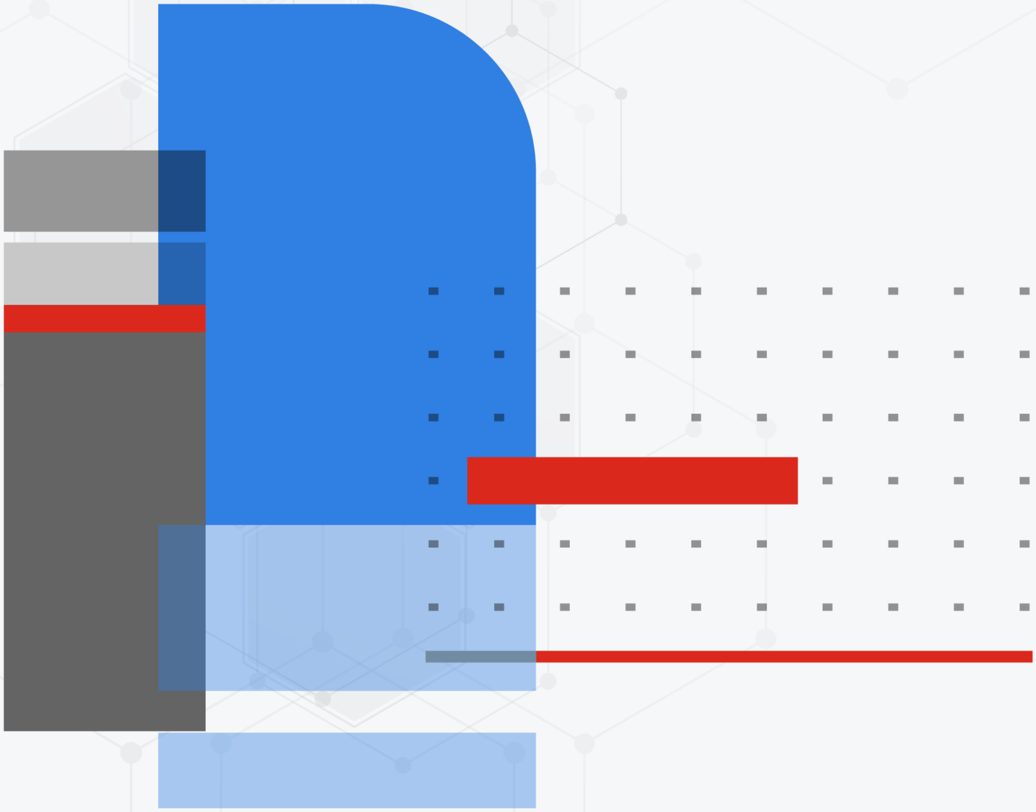
Release Notes

FortiManager 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 18, 2024
FortiManager 7.4.0 Release Notes
02-740-896575-20240118

TABLE OF CONTENTS

Change Log ... **6**

FortiManager 7.4.0 Release ... **7**

Supported models ... 7

FortiManager VM subscription license ... 7

Management extension applications ... 7

Supported models for MEA ... 8

Minimum system requirements ... 8

Special Notices ... **10**

FortiManager 7.2.3 and later firmware on FortiGuard ... 10

FortiManager 7.4.0 GUI issues in Google Chrome and Microsoft Edge ... 10

Option to enable permission check when copying policies ... 10

Management Extensions visibility in the GUI ... 11

ADOM upgrade for FortiManager 7.4 ... 11

Install On column for policies ... 11

SD-WAN Orchestrator removed in 7.2 ... 11

Changes to FortiManager meta fields ... 11

Setup wizard requires FortiCare registration ... 12

Access lists as ADOM-level objects ... 12

View Mode is disabled in policies when policy blocks are used ... 12

Reconfiguring Virtual Wire Pairs (VWP) ... 12

Fortinet verified publisher docker image ... 12

Scheduling firmware upgrades for managed devices ... 14

Modifying the interface status with the CLI ... 14

SD-WAN with upgrade to 7.0 ... 14

Citrix XenServer default limits and upgrade ... 15

Multi-step firmware upgrades ... 15

Hyper-V FortiManager-VM running on an AMD CPU ... 15

SSLv3 on FortiManager-VM64-AWS ... 15

Upgrade Information ... **17**

Downgrading to previous firmware versions ... 17

Firmware image checksums ... 17

FortiManager VM firmware ... 18

SNMP MIB files ... 19

Product Integration and Support ... **20**

Supported software ... 20

Web browsers ... 21

FortiOS and FortiOS Carrier ... 21

FortiADC ... 21

FortiAnalyzer ... 21

FortiAnalyzer-BigData ... 22

FortiAuthenticator ... 22

FortiCache ... 22

FortiClient 22
FortiDDoS 22
FortiDeceptor 23
FortiFirewall and FortiFirewallCarrier 23
FortiMail 23
FortiProxy 23
FortiSandbox 24
FortiSOAR 24
FortiSwitch ATCA 24
FortiTester 24
FortiWeb 24
Virtualization 24
Feature support 25
Language support 26
Supported models 26
FortiGate models 27
FortiGate special branch models 30
FortiCarrier models 30
FortiCarrier special branch models 32
FortiADC models 33
FortiAnalyzer models 33
FortiAnalyzer-BigData models 33
FortiAuthenticator models 34
FortiCache models 34
FortiDDoS models 34
FortiDeceptor models 34
FortiFirewall models 35
FortiFirewallCarrier models 36
FortiMail models 36
FortiProxy models 36
FortiSandbox models 37
FortiSOAR models 37
FortiSwitch ATCA models 37
FortiTester models 37
FortiWeb models 38
Compatibility with FortiOS Versions 39
FortiManager 7.4.0 and FortiOS 7.0.12 compatibility issues 39
FortiManager 7.4.0 and FortiOS 7.2.5 compatibility issues 40
Resolved Issues 44
AP Manager 44
Device Manager 44
FortiSwitch Manager 45
Others 46
Policy and Objects 46
Revision History 48
Script 49
System Settings 49

VPN Manager 49
Common Vulnerabilities and Exposures 49
Known Issues 51
AP Manager 51
Device Manager 51
FortiSwitch Manager 52
Global ADOM 53
Others 53
Policy & Objects 54
Script 55
System Settings 55
VPN Manager 55
Appendix A - FortiGuard Distribution Servers (FDS) 56
FortiGuard Center update support 56
Appendix B - Default and maximum number of ADOMs supported 57
Hardware models 57
Virtual Machines 57

Change Log

Date	Change Description
2023-05-15	Initial release.
2023-05-18	Updated Known Issues on page 51.
2023-05-23	Updated FortiGate models on page 27.
2023-05-31	Updated: • Web browsers on page 21 • Known Issues on page 51 • Special Notices on page 10
2023-06-05	Updated: • Web browsers on page 21 • Known Issues on page 51 • Special Notices on page 10
2023-06-13	Updated Known Issues on page 51.
2023-06-14	Added: • FortiManager 7.4.0 and FortiOS 7.0.12 compatibility issues on page 39 • FortiManager 7.4.0 and FortiOS 7.2.5 compatibility issues on page 40
2023-06-21	Updated Resolved Issues on page 44 and Known Issues on page 51.
2023-06-26	Updated Known Issues on page 51.
2023-07-04	Updated Known Issues on page 51 and Resolved Issues on page 44.
2023-07-10	Updated FortiProxy on page 23.
2023-07-12	Updated Known Issues on page 51.
2023-07-26	Updated Special Notices on page 10.
2023-08-21	Updated Known Issues on page 51.
2023-09-20	Updated FortiGate special branch models on page 30.
2023-10-12	Updated Resolved Issues on page 44 and Known Issues on page 51.
2023-10-19	Updated Management extension applications on page 7.
2023-11-15	Updated Known Issues on page 51.
2023-12-18	Updated Known Issues on page 51.
2024-01-05	Added the *FortiManager 7.2.3 and later firmware on FortiGuard* Special Notice.
2024-01-18	Updated Special Notices on page 10.

FortiManager 7.4.0 Release

This document provides information about FortiManager version 7.4.0 build 2223.

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

This section includes the following topics:

- Supported models on page 7
- FortiManager VM subscription license on page 7
- Management extension applications on page 7

Supported models

FortiManager version 7.4.0 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_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 18.

See also Appendix B - Default and maximum number of ADOMs supported on page 57.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.4.0.

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

As of FortiManager 7.4.0, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one MEA is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the FortiManager Documents Library.

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
- 16 GB RAM
- 500 GB disk space

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

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

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

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

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage
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 7.4.0.

FortiManager 7.2.3 and later firmware on FortiGuard

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

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

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

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

FortiManager 7.4.0 GUI issues in Google Chrome and Microsoft Edge

The FortiManager 7.4.0 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 21.

Option to enable permission check when copying policies

As of 7.4.0, a new command is added in the CLI:

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

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

Management Extensions visibility in the GUI

As of FortiManager 7.4.0, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one management extension application (MEA) is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the FortiManager Documents Library.

ADOM upgrade for FortiManager 7.4

Currently, there is no ADOM upgrade option for ADOM version 7.2 to move to version 7.4. In order to manage FortiGates running 7.4, please add the devices to a 7.4 ADOM.

Install On column for policies

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

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 lists as ADOM-level object configurations from FortiGate. Previously, 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, 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 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.

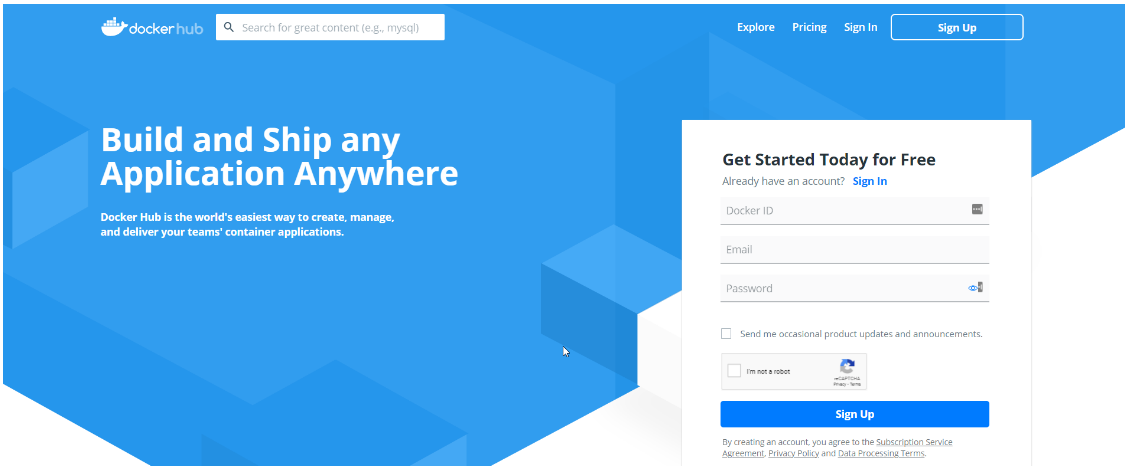
Before installing the VWP, you must first remove the old VWP from the device's database, otherwise a policy and object validation error may occur during installation. You can remove the VWP from the device database by going to *Device Manager* > *Device & Groups*, selecting the managed device, and removing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



Build and Ship any Application Anywhere

Docker Hub is the world's easiest way to create, manage, and deliver your teams' container applications.

Get Started Today for Free

Already have an account? Sign In

Docker ID

Email

Password

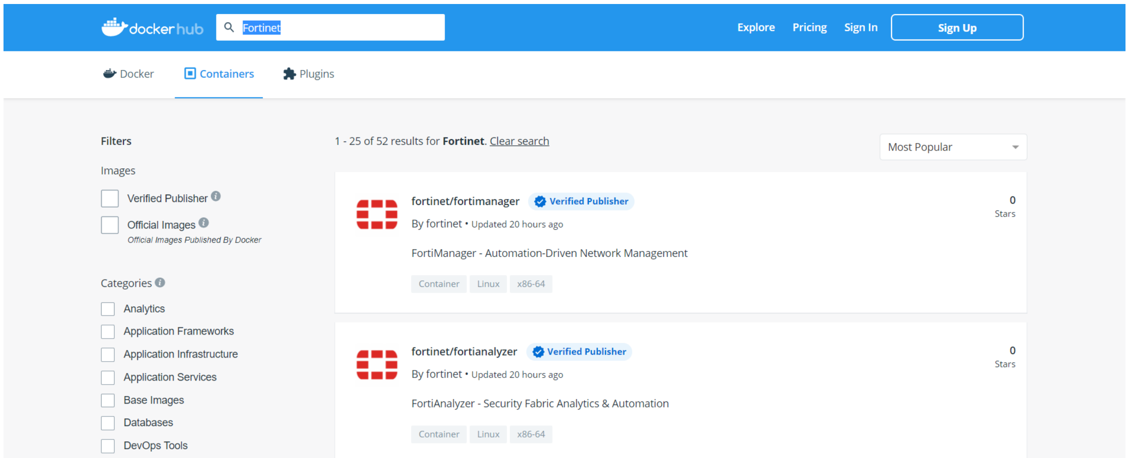
□ Send me occasional product updates and announcements.

□ I'm not a robot

Sign Up

By creating an account, you agree to the Subscription Service Agreement, Privacy Policy and Data Processing Terms.

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.



Filters

Images

□ Verified Publisher

□ Official Images
Official Images Published By Docker

Categories

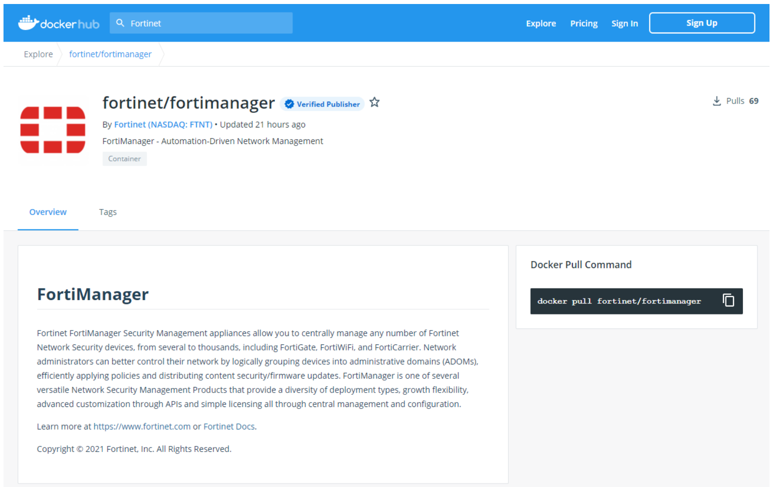
□ Analytics
□ Application Frameworks
□ Application Infrastructure
□ Application Services
□ Base Images
□ Databases
□ DevOps Tools

1 - 25 of 52 results for **Fortinet**. Clear search

fortinet/fortimanager Verified Publisher
By fortinet • Updated 20 hours ago
FortiManager - Automation-Driven Network Management
Container Linux x86-64
0 Stars

fortinet/fortianalyzer Verified Publisher
By fortinet • Updated 20 hours ago
FortiAnalyzer - Security Fabric Analytics & Automation
Container Linux x86-64
0 Stars

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.



fortinet/fortimanager Verified Publisher ☆

By Fortinet (NASDAQ: FTNT) • Updated 21 hours ago

FortiManager - Automation-Driven Network Management

Container

Pulls 69

FortiManager

Fortinet FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, FortiWiFi, and FortiCarrier. Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), efficiently applying policies and distributing content security/firmware updates. FortiManager is one of several versatile Network Security Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing all through central management and configuration.

Learn more at https://www.fortinet.com or Fortinet Docs.

Copyright © 2021 Fortinet, Inc. All Rights Reserved.

Docker Pull Command

```
docker pull fortinet/fortimanager
```

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 the *FortiManager Upgrade Guide* in the Fortinet Document Library.

You can upgrade FortiManager 7.2.0 or later directly to 7.4.0.

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

For example, FortiManager 7.2 supports ADOM versions 6.4, 7.0, and 7.2, but FortiManager 7.4 supports ADOM versions 7.0, 7.2, and 7.4. Before you upgrade FortiManager 7.2 to 7.4, ensure that all ADOM 6.4 versions have been upgraded to ADOM version 7.0 or later. See the *FortiManager Upgrade Guide* in the Fortinet Document Library.

This section contains the following topics:

- Downgrading to previous firmware versions on page 17
- Firmware image checksums on page 17
- FortiManager VM firmware on page 18
- SNMP MIB files on page 19

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

The section contains the following topics:

- Supported software on page 20
- Feature support on page 25
- Language support on page 26
- Supported models on page 26

Supported software

FortiManager 7.4.0 supports the following software:

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

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

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

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

Web browsers

FortiManager 7.4.0 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 7.4.0 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the Fortinet Document Library.

See FortiManager compatibility with FortiOS.

FortiManager 7.4.0 supports the following versions of FortiOS and FortiOS Carrier:

- 7.4.0
- 7.2.0 to 7.2.5
- 7.0.0 to 7.0.12

FortiADC

FortiManager 7.4.0 supports the following versions of FortiADC:

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

FortiAnalyzer

FortiManager 7.4.0 supports the following versions of FortiAnalyzer:

- 7.4.0
- 7.2.0 and later
- 7.0.0 and later

FortiAnalyzer-BigData

FortiManager 7.4.0 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAuthenticator

FortiManager 7.4.0 supports the following versions of FortiAuthenticator:

- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later

FortiCache

FortiManager 7.4.0 supports the following versions of FortiCache:

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

FortiClient

FortiManager 7.4.0 supports the following versions of FortiClient:

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

FortiDDoS

FortiManager 7.4.0 supports the following versions of FortiDDoS:

- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later

Limited support. For more information, see Feature support on page 25.

FortiDeceptor

FortiManager 7.4.0 supports the following versions of FortiDeceptor:

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

FortiFirewall and FortiFirewallCarrier

FortiManager 7.4.0 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiMail

FortiManager 7.4.0 supports the following versions of FortiMail:

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

FortiProxy

FortiManager 7.4.0 supports configuration management for the following versions of FortiProxy:

- 7.2.3
- 7.2.2
- 7.0.7

Configuration management support is identified as *Management Features* in these release notes. See Feature support on page 25.

FortiManager 7.4.0 supports logs from the following versions of FortiProxy:

- 7.2.0 to 7.2.5
- 7.0.0 to 7.0.11
- 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 7.4.0 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 7.4.0 supports the following versions of FortiSOAR:

- 7.4.0 and later
- 7.3.0 and later
- 7.2.0 and later

FortiSwitch ATCA

FortiManager 7.4.0 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.4.0 supports the following versions of FortiTester:

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

FortiWeb

FortiManager 7.4.0 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.4.0 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2

- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 6.5 and later

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

Language support

The following table lists FortiManager language support information.

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.4.0.

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

This section contains the following topics:

- FortiGate models on page 27
- FortiGate special branch models on page 30
- FortiCarrier models on page 30
- FortiCarrier special branch models on page 32
- FortiADC models on page 33
- FortiAnalyzer models on page 33
- FortiAnalyzer-BigData models on page 33
- FortiAuthenticator models on page 34

- FortiCache models on page 34
- FortiDDoS models on page 34
- FortiDeceptor models on page 34
- FortiFirewall models on page 35
- FortiFirewallCarrier models on page 36
- FortiMail models on page 36
- FortiProxy models on page 36
- FortiSandbox models on page 37
- FortiSOAR models on page 37
- FortiSwitch ATCA models on page 37
- FortiTester models on page 37
- FortiWeb models on page 38

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see FortiGate special branch models on page 30.

⚠ The following FortiGate models are not supported in 7.4 by FortiManager 7.4.0 due to FortiOS syntax issues:

- FortiGate-91E
- FortiGateRugged-70F/70F-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-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.4

Model	Firmware Version
FortiGate 7000 Series: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC **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-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-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-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500E, FortiGate-501E, 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 **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	7.2

Model	Firmware Version
FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-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-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	7.0

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.4.0 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see FortiGate models on page 27.

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.11	4974
FortiGate-900G, FortiGate-901G	7.0.10	6566
FortiGate-1000F, FortiGate-1001F	7.0.10	6503
FortiGate-3200F, FortiGate-3201F	7.0.10	6506
FortiGate-3700F, FortiGate-3701F	7.0.10	6506
FortiGate-4800F, FortiGate-4801F	7.0.10	6506
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.10	0111
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.10	0116
FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.10	0111
FortiGateRugged-70F, FortiGateRugged-70F-3G4G	7.0.11	6565

FortiCarrier models

The following FortiCarrier models are released with FortiCarrier firmware.

For information about supported FortiCarrier models on special branch releases of FortiCarrier firmware, see FortiCarrier special branch models on page 32.

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC **FortiCarrier 7000 Series**: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **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-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-IBM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F **FortiCarrier 5000 Series**: 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-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.2
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 5000 Series**: FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1	7.0

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.4.0 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see FortiCarrier models on page 30.

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.10	6506
FortiCarrier-3700F, FortiCarrier-3701F	7.0.10	6506
FortiCarrier-4800F, FortiCarrier-4801F	7.0.10	6506
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.10	0111
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.10	0116
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.10	0111

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	7.0, 7.1, 7.2

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E **FortiAnalyzer VM**: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.2, 7.4
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-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0

FortiAnalyzer-BigData models

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

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200E, FAC-300F, FAC-400E, FAC-800F, FAC-2000E, FAC-3000E, FAC-3000F **FortiAuthenticator VM:** FAC-VM	6.5
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E, FAC-3000F **FortiAuthenticator VM:** FAC-VM	6.4
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.3

FortiCache models

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F **FortiDDoS VM**: FortiDDoS-VM	6.5
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F **FortiDDoS VM**: FortiDDoS-VM	6.4
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F **FortiDDoS VM**: FortiDDoS-VM	6.3

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-100G, FDC-1000F, FDC-1000G	5.0

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

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.4.0 supports these models on the identified FortiFirewall firmware version and build number.

FortiFirewall 7.4

Model	Firmware Version
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC	7.4
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.4

FortiFirewall 7.2

Model	Firmware Version
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2

FortiFirewall 7.0

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

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.4.0 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0.10	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0.10	4940
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	1999
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4.12	5423

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000F, FE-3000F	7.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FortiMail Cloud	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FML-VM, FortiMail Cloud	6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E, **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FortiProxy-KVM, FortiProxy-VM64	1.0, 1.1, 1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FSA-VM	3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	7.2, 7.3, 7.4

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-4000E	7.2

Model	Firmware Version
FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.1
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0

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, 7.2

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.4.0.

FortiManager 7.4.0 and FortiOS 7.0.12 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.4.0 and FortiOS 7.0.12. FortiOS 7.0.12 includes syntax changes not supported by FortiManager 7.4.0.

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

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

The following options were changed:

```
system global http-request-limit
  int-range (tag|lmt): 134217728,378297344 -> 134217728,384212992 (1 platforms: 60F-
       3G4G)
  int-range (tag|lmt): 134217728,861320192 -> 134217728,830530560 (1 platforms: 80F)
  int-range (tag|lmt): 134217728,395325440 -> 134217728,383242240 (1 platforms: 60E-DSL)
  int-range (tag|lmt): 134217728,1796664320 -> 134217728,1783577600 (1 platforms: 300E)
  int-range (tag|lmt): 134217728,1644344320 -> 134217728,1631371264 (1 platforms: 800D)
  int-range (tag|lmt): 134217728,1750113280 -> 134217728,1737104384 (1 platforms: 400E-
       BYPASS)
  int-range (tag|lmt): 134217728,861179904 -> 134217728,830612480 (1 platforms: 80F-
       BYPASS)
  int-range (tag|lmt): 134217728,428093440 -> 134217728,443324416 (1 platforms: 90E)
  int-range (tag|lmt): 134217728,859765760 -> 134217728,811363328 (1 platforms: 81F-2R)
  int-range (tag|lmt): 134217728,405515264 -> 134217728,410984448 (1 platforms: 60F)
  int-range (tag|lmt): 134217728,788836352 -> 134217728,779671552 (1 platforms: 101F)
  int-range (tag|lmt): 134217728,394435584 -> 134217728,386069504 (1 platforms: 81E)
  int-range (tag|lmt): 134217728,687936512 -> 134217728,679543808 (1 platforms: 140E-
       POE)
  int-range (tag|lmt): 134217728,689605632 -> 134217728,681216000 (1 platforms: 100EF)
  int-range (tag|lmt): 134217728,394478592 -> 134217728,386050048 (1 platforms: 81E-POE)
  int-range (tag|lmt): 134217728,1828137984 -> 134217728,1819059200 (1 platforms: 100F)
  int-range (tag|lmt): 134217728,1654361088 -> 134217728,1643625472 (1 platforms: 200F)
  int-range (tag|lmt): 134217728,390627328 -> 134217728,382415872 (1 platforms: 60E)
  int-range (tag|lmt): 134217728,861128704 -> 134217728,830902272 (1 platforms: 80F-POE)
system link-monitor probe-timeout
  int-range (tag|lmt): 20,200 -> 20,5000
```

FortiManager 7.4.0 and FortiOS 7.2.5 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.4.0 and FortiOS 7.2.5. FortiOS 7.2.5 includes syntax changes not supported by FortiManager 7.4.0.

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

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

The following type changed:

- `vpn certificate ocsp-server source-ip` type changed from `<ip4class>` to `<string>`

The following objects were added:

- `(attr) firewall policy ip-version-type`
- `(attr) firewall policy ips-voip-filter`
- `(attr) firewall policy policy-behaviour-type`
- `(attr) firewall profile-group ips-voip-filter`
- `(attr) firewall proxy-policy ips-voip-filter`
- `(attr) firewall security-policy ips-voip-filter`
- `(attr) system admin gui-dashboard widget source`
- `(attr) system csf file-mgmt`
- `(attr) system csf file-quota`
- `(attr) system csf file-quota-warning`
- `(attr) system federated-upgrade ha-reboot-controller`
- `(attr) system npu dedicated-management-affinity (1 platforms: 200F)`
- `(attr) system npu dedicated-management-cpu (1 platforms: 200F)`
- `(attr) system sso-admin gui-dashboard widget source`
- `(attr) system sso-forticloud-admin gui-dashboard widget source`
- `(attr) system sso-fortigate-cloud-admin gui-dashboard widget source`
- `(node) system virtual-wire-pair outer-vlan-id (12 platforms: 4201F,4200F,1800F,4401F,3500F,3501F,1801F)`
- `(attr) user domain-controller change-detection`
- `(attr) user domain-controller change-detection-period`
- `(attr) videofilter profile default-action`
- `(attr) videofilter profile log`
- `(attr) voip profile sip call-id-regex`
- `(attr) voip profile sip content-type-regex`
- `(attr) vpn certificate setting source-ip`
- `(attr) vpn ipsec phase1-interface auto-discovery-crossover`
- `(attr) vpn ipsec phase1-interface dev-id`
- `(attr) vpn ipsec phase1-interface dev-id-notification`
- `(attr) vpn ssl settings server-hostname`
- `(attr) wireless-controller wtp ble-major-id`
- `(attr) wireless-controller wtp ble-minor-id`

- `(attr) wireless-controller wtp-group ble-major-id`
- `(attr) wireless-controller wtp-profile radio-1 optional-antenna`
- `(attr) wireless-controller wtp-profile radio-2 optional-antenna`
- `(attr) wireless-controller wtp-profile radio-3 optional-antenna`
- `(attr) wireless-controller wtp-profile radio-4 optional-antenna`

The following objects were removed:

- `(attr) firewall proxy-policy voip-profile`
- `(attr) videofilter youtube-channel-filter default-action`
- `(attr) videofilter youtube-channel-filter override-category`
- `(attr) vpn certificate setting ssl-ocsp-source-ip`

The following default values changed:

- `system lte-modem auto-connect` default value changed from `disable` to `enable`
- `system lte-modem gps-service` default value changed from `disable` to `enable`
- `system npu hash-config` default value is changed depending on the platform
- `system replacemsg admin format` default value changed to `none`
- `system replacemsg admin header` default value changed to `none`
- `system replacemsg alertmail format` default value changed to `none`
- `system replacemsg alertmail header` default value changed to `none`
- `system replacemsg auth format` default value changed to `none`
- `system replacemsg auth header` default value changed to `none`
- `system replacemsg automation format` default value changed to `none`
- `system replacemsg automation header` default value changed to `none`
- `system replacemsg custom-message format` default value changed to `none`
- `system replacemsg custom-message header` default value changed to `none`
- `system replacemsg fortiguard-wf format` default value changed to `none`
- `system replacemsg fortiguard-wf header` default value changed to `none`
- `system replacemsg ftp format` default value changed to `none`
- `system replacemsg ftp header` default value changed to `none`
- `system replacemsg http format` default value changed to `none`
- `system replacemsg http header` default value changed to `none`
- `system replacemsg icap format` default value changed to `none`
- `system replacemsg icap header` default value changed to `none`
- `system replacemsg mail format` default value changed to `none`
- `system replacemsg mail header` default value changed to `none`
- `system replacemsg nac-quar format` default value changed to `none`
- `system replacemsg nac-quar header` default value changed to `none`
- `system replacemsg spam format` default value changed to `none`
- `system replacemsg spam header` default value changed to `none`
- `system replacemsg sslvpn format` default value changed to `none`
- `system replacemsg sslvpn header` default value changed to `none`
- `system replacemsg traffic-quota format` default value changed to `none`
- `system replacemsg traffic-quota header` default value changed to `none`

- `system replacemsg utm format` default value changed to `none`
- `system replacemsg utm header` default value changed to `none`
- `system replacemsg webproxy format` default value changed to `none`
- `system replacemsg webproxy header` default value changed to `none`
- `videofilter profile fortiguard-category filters log` default value changed from `disable` to `enable`
- `videofilter youtube-channel-filter log` default value changed from `disable` to `enable`
- `voip profile feature-set` default value changed from `proxy` to `voipd`
- `vpn certificate ocsp-server source-ip` default value changed from `0.0.0.0` to null

Additional option changes:

```
application list entries parameters
   tag: None -> tz
endpoint-control fctems ca-cn-info
   tag: None -> xs
firewall address
   tab-size (tag|tz): 65000,65000,0 -> 100000,100000,0 (6 platforms:
         2500E,1500DT,1800F,1801F,2000E,1500D)
   tab-size (tag|tz): 40000,40000,0 -> 50000,50000,0 (2 platforms: 1101E,1000D)
firewall ippool port-per-user
   int-range (tag|lmt): 32,60416 -> 32,60417
log npu-server server-group
   tab-size (tag|tz): 512,256,0 -> 16,0,0 (12 platforms:
         4201F,4200F,1800F,4401F,3500F,3501F,1801F)
log npu-server server-info
   tab-size (tag|tz): 512,256,0 -> 16,0,0 (12 platforms:
         4201F,4200F,1800F,4401F,3500F,3501F,1801F)
system global http-request-limit
   int-range (tag|lmt): 134217728,2147483647 -> 134217728,1073741824 (33 platforms:
         3000D,5001E,1000D,4201F,600E,1101E,4401F,1500D,3200D,3601E,3100D,1800F,3401E,3501
         F,1801F,1500DT,2000E,4200F,3400E,2500E,3500F)
   int-range (tag|lmt): 134217728,853097472 -> 134217728,1073741824 (1 platforms: 80F-2R)
   int-range (tag|lmt): 134217728,853334016 -> 134217728,1073741824 (1 platforms: 80F-
         POE)
   int-range (tag|lmt): 134217728,853332992 -> 134217728,1073741824 (1 platforms: 80F)
   int-range (tag|lmt): 134217728,1773837312 -> 134217728,1073741824 (1 platforms: 400E)
   int-range (tag|lmt): 134217728,851954688 -> 134217728,1073741824 (1 platforms: 81F-2R)
   int-range (tag|lmt): 134217728,386418688 -> 134217728,1073741824 (1 platforms: 60F)
   int-range (tag|lmt): 134217728,387472384 -> 134217728,1073741824 (1 platforms: 40F)
   int-range (tag|lmt): 134217728,852159488 -> 134217728,1073741824 (1 platforms: 81F)
   int-range (tag|lmt): 134217728,1634093056 -> 134217728,1073741824 (1 platforms: 800D)
   int-range (tag|lmt): 134217728,398662656 -> 134217728,1073741824 (1 platforms: 40F-
         3G4G)
   int-range (tag|lmt): 134217728,1772238848 -> 134217728,1073741824 (1 platforms: 401E)
   int-range (tag|lmt): 134217728,1786169344 -> 134217728,1073741824 (1 platforms: 300E)
   int-range (tag|lmt): 134217728,939444224 -> 134217728,1073741824 (1 platforms: 201E)
   int-range (tag|lmt): 134217728,1644056576 -> 134217728,1073741824 (1 platforms: 200F)
   int-range (tag|lmt): 134217728,680290304 -> 134217728,1073741824 (1 platforms: 101E)
   int-range (tag|lmt): 134217728,369893376 -> 134217728,1073741824 (1 platforms: 60F-
         3G4G)
   int-range (tag|lmt): 134217728,372878336 -> 134217728,1073741824 (1 platforms: 60F)
system interface mediatype
   tag: None -> nd (28 platforms:
         401E,300E,1000D,4201F,600E,1101E,4401F,1500D,3601E,1800F,3401E,3501F,1801F,2000E,
         1500DT,400E,4200F,3400E,2500E,3500F)
```

```
system interface speed
  option-list (tag|opt): None -> ["40000auto"] (2 platforms: 5001E)
  option-list (tag|opt): None -> ["2500auto", "400Gauto", "400Gfull", "5000auto"] (19
       platforms: 4201F,4200F,3601E,3400E,1800F,3401E,1101E,4401F,3501F,3500F,1801F)
system link-monitor interval
  int-range (tag|lmt): 500,3600000 -> 20,3600000
system link-monitor probe-timeout
  int-range (tag|lmt): 500,5000 -> 20,5000
system lte-modem network-type
  option-list (tag|opt): ["cdma-hrpd"] -> None (2 platforms: 60F-3G4G,40F-3G4G)
system npu sw-np-bandwidth
  option-list (tag|opt): None -> ["7G", "8G", "9G"] (12 platforms:
       3200D,3000D,3100D,1101E,5001E,800D,1500DT,1500D)
system sdwan health-check interval
  int-range (tag|lmt): 500,3600000 -> 20,3600000
system sdwan health-check probe-timeout
  int-range (tag|lmt): 500,3600000 -> 20,3600000
system speed-test-server name
  tag: None -> xs
voip profile feature-set
  option-list (tag|opt): ["flow", "proxy"] -> None
  option-list (tag|opt): None -> ["ips", "voipd"]
vpn certificate ocsp-server source-ip
  tag: None -> sz
```

Resolved Issues

The following issues have been fixed in 7.4.0. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
781561	User may not be able to access *AP Manager* with custom `read only` admin profile.
881548	Unable to install successfully when creating a SSID using its default value.
889811	Under WIFI and switch controller for Managed FortiAPs, there is not any LLDP info found.
910182	*AP Manager* doesn't load if admin profile permission is Read-Only.

Device Manager

Bug ID	Description
801886	FortiManager does not assign the correct VDOM name when configuring a new inter-vdom link interface.
803425	Installation failed due to the some of the "`os-check-list`" items which are not supported by the FortiGates anymore.
817346	Editing interface with normalized interface mapping displays some unnecessary messages for mapping change.
831874	FortiManager's GUI is keep refreshing when clicking on the devices under the *Managed Devices*.
836933	Changes on the External-Resource settings from ADOMs for specific VDOMs/FortiGates alter the External-Resource settings for other ADOMs and VDOMs.
876040	Status of Certificates is displayed as "pending" under the System's Certificates.
879833	Adding a model device with variable to FortiManager displays an error message "a[i].replace is not a function".
881308	The default value of the "router.static.vrf" leads to installation failure when attempting to install blackhole routes to FortiGates.

Bug ID	Description
885454	After upgrading FortiManager, certificates for FGT-1100E's are missing from the *Device Manager*.
886917 888930	FortiManager's ipsec templates remove the sdwan member and bgp neighbor attached to an ipsec interface. This causes the sdwan member to be removed even when it's used.
887903	System template interface table gets purged when trying to create VLAN type with name length greater than 15.
888658	Editing DHCP Settings of a FortiGate interface displays the following error message: "You have no permission to access this device/vdom".
891216	Unable to edit/save interface with DHCP relay enabled.
891341	Installation fails due to the Copy failure error; system template created with some empty string values which are assigned to devices.
891967	When management VDOM is non-root and has been assigned to a different ADOM, FortiManager displays the error, "Can not access device global setting if management VDOM is not in current ADOM".
893592	Exporting the Device List to CSV and Excel file doesn't include the FortiAPs and FortiSwitches info.
896127	When attempting to create a VLAN type with a name longer than 15 characters, FortiManager displays an error message.
896998	Unable to get access to the Certificates via Device Manager > DEVICE_NAME > VDOM_NAME > System.
897863	After de-selecting the '`allow-dns`' feature under the application control list, the changes cannot be saved.
898814	FortiManager keeps changing the `cert-id-validation`'s value to its default value during the installation.
899541	An error message "upgrade image failed" is shown, even though the upgrade has been completed successfully.
899903	FortiManager GUI does not list all NTP interfaces.

FortiSwitch Manager

Bug ID	Description
872802	FortiManager automatically sets "`default`" as `dnsfilter-profile` under `dns-server` for fortilink interface.
890205	Selecting multiple ports to "*Edit*" is not possible as it is greyed out.

Others

Bug ID	Description
788006	FortiManager consumes license count for the Admin Type VDOMs.
802922	The application "`newcli`" process crashes when the "`diagnose cdb upgrade check +all`" command runs.
814425	Sorting FortiExtenders by Network, RSSI, RSRP, RSRQ, and SINR does not work properly.
829046	After the upgrade, some of the metadata variables are missing.
832351	FortiManager does not allow users to enter to the root ADOM; it displays the "ADOM license was expired..." message.
851586	FortiManager displays "invalid scope" errors when running the "`diagnose cdb check policy-packages`" command.
869955	BGP Template route map option does not support Meta Variables.
871608	Unable to retrieve routing information from FortiGate via FortiManager when there is a large routing table.
873110	FortiManager displays "expired" instead of "not licensed" for non-purchased FortiGuard services.
875006	When clicking on the warning message, which indicates critical security vulnerabilities, a list of all types of security vulnerabilities is displayed.
883548	FortiManager/FortiAnalyzer is forcing its users to upgrade the Firmware version upon login.
891869	FortiManager wrongly recommends lower version for upgrade the FortiGates.
895081	Some FortiGates were unable to be upgraded from FortiManager due to firmware ID discrepancies between FortiManager and FortiGuard.
899570	Unable to add the "FortiGateRugged-60F" FGT to the FortiManager.
899750	ADOM upgrade makes the Policy Packages status modified.
906533	Group options, when creating/editing the workflow approval group, displays wrong info.

Policy and Objects

Bug ID	Description
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
739489	It's not possible to enable NAT with Outgoing Interface Address by directly right-clicking on the NAT section of a firewall policy.

Bug ID	Description
774058	Rule list order may not be saved under *File Filter Profile*.
803460	*User Definitions* entries under the *User & Authentication* cannot be removed from FortiManager.
814468	FortiManager purges `gcp-project-list` and unsets several values from GCP sdn-connector.
821114	EMS ZTNA Tags in FortiManager and FortiGate are using different naming convention; therefore, installing the policies with those tags to FortiGates do not work.
827416	FortiManager does not display any copy failure errors when utilized objects do not have any default values or per-device mapping.
862014 880359	FortiManager is purging 'replacement message group custom' configuration after install verification fails.
866724	Copy Failed error has been observed with the error message "Virtual server limit reached!"; this limit is 50 for FGT AWS ONDEMAND.
866826	Failed to modify Virtual Server addresses in Firewall Polices with Deny Action.
867809	During installation, FortiManager unsets status for the proxy policies.
870800	Even though each interface is mapped to be used in specific vdoms, the already mapped interface still can be selected for other VDOMs.
873006	Firewall Address entries cannot be modified and GUI displays an error message, "Object already exists."
875547	Policy & Package cannot be imported if the type of firewall address in FortiGates are "`interface-subnet`" and subnet's value is different from its value on FortiManager.
877477	Domain Name Threat Feeds are not available in *DNS Filter > Remote Categories*.
880431	Unable to define Exempt IP in IPS Sensor.
880575	When using the "reinstall policy" option to install to devices with different policy packages, the corresponding event log shows the same policy package pushed to all devices.
881634	When multiple VDOMs are selected for installation using the Re-install Policy feature, FortiManager only applies "`re-install policy`" for one VDOM from each devices.
881857	Multiple security console Application crashes have been observed during the Policy Package installation when static router template and router static entry in device db are used.
882477	Error Message "Object already exists" is displayed when editing per device mapping for Address Group.
882996	Unable to install to FortiGates when using null values for "`local-gw6`" and "`remote-gw6`".
883527	Install Preview does not display any info during the installation when using device groups in PP Installation Targets.
884275	Not able to move policy blocks properly.

Bug ID	Description
885827	FortiManager does not save and keep the selected "collapse all" mode for the policy package.
885992	Duplicate section names are created for policy package when ViewMode interface pair View is selected.
886370	FortiManager doesn't sort by interface per view results correctly; the results are not displayed in alphabetical order.
886906	When scrolling the policy page down/up the policy page appeared to be blank.
887278	Installation failed due to the limit on max entery for "`endpoint-control fctems`".
888483	The "automation email" under the "Replacement Message Group" is blank.
889068	Unable to push policies when VDOMs are in different ADOMs.
889563	FortiManager, for ADOM version 6.4, does not support Creating, Importing, and Inserting Above or Below actions for a deny policy with a "Log Violation Traffic" disabled.
891832	The install preview for policy package being used by multiple FortiGates is taking some time to load.
891996	"Find and Replace" feature does not displaythe entries correctly and it does not allow any changes.
895979	FortiManager attempts setting the Zone as the interface for firewall policy during the installation.
899339	FortiManager does not seek for confirmation when deleting an object from firewall policy.
912635	FortiManager attempts to purge the DLP objects that were downloaded from FortiGuard by the FortiGates.
912670	FortiManager attempts to install "`set global-label`" which creates some error message logs but does not cause any installation failure.
912732	The installation fails when the IPS signature contains CVE references.

Revision History

Bug ID	Description
513317	FortiManager may fail to install policy after FortiGate failover on Azure.
672609	After import, FortiManager may prompt password error on administrator during install.
801614	FortiManager might display an error message, "Failed to create a new revision." for some FortiGates when retrieving their configurations.

Script

Bug ID	Description
876917	"Capture Diff to a Script" does not work properly. It does not display the changes.

System Settings

Bug ID	Description
853429	Creating FortiManager's configuration backup via scp cannot be done.
873078	FortiManagers HA cannot be configured as the initial sync never completes.
884168	FortiManager suggests wrong versions to upgrade FortiGates in order to resolve the PSIRT Vulnerability.
884396	The firmware upgrade notification on the FortiManager and FortiAnalyzer keeps appearing continuously after each login.
884848	FortiManager HA is not syncing after upgrade as the synchronization between the cluster units never completes.
894366	Any changes related to "lan" interface on FGT-40F, where the role is defined as "LAN", FortiManager tries installing firewall address "lan address" with type interface-subnet linked to interface "lan". The Install Verification fails for "lan address" as "entry not found in database".

VPN Manager

Bug ID	Description
798995	It's not possible to delete an SSL VPN portal profile from FortiManager GUI if the profile has been already installed.
857051	Installing a policy package with IPSec VPN to FortiGates fail with the following error: "TCL error (The remote gateway is a duplicate of another IPsec gateway entry)".
888272	Single entry of SSLVPN settings cannot be selected under *VPN Manager*.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
841029	FortiManager 7.4.0 is no longer vulnerable to the following CVE Reference: • CVE-2023-25607
850883	FortiManager 7.4.0 is no longer vulnerable to the following CVE Reference: • CVE-2023-36638
889979	FortiManager 7.4.0 is no longer vulnerable to the following CVE Reference: • CVE-2023-41679

Known Issues

The following issues have been identified in 7.4.0. To inquire about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
861941	FortiManager attempts to install "`arrp-profile`" even if "`darrp`" is disabled.
865486	The FortiManager's *AP Manager* permits the use of invalid channels with a 40MHz channel width.
884233	FortiManager displays the AP critical security vulnerability info even after FortiAPs are being upgraded.
892773	Assigning AP Profile returns invalid value.
906930	FortiManager displays an error for Subnets overlap for a Bridge SSID.

Device Manager

Bug ID	Description
768289	There is a discrepancy in the usage of quotation marks ("") when configuring DHCP relay from FortiManager or retrieving it from FortiGate.
831624	*SD-WAN Monitor* under the Monitors displays time frame as "`invalid date - invalid date`".
895001	The "gui-ztna" configuration is displayed as enabled on the FortiManager even though this setting is disabled on the FortiGate.
896367	The geographic coordination config of FortiGates on *Device Manager* is being reset to `0,0` after a certain period of time.
899350	Promote button is missing for FortiGate 80F Clusters.
902908	Managed FortiAnalyzer is not listed under System Template.
905869	Invalid default value for VRF ID is observed when creating static route.
906558	Importing a Revision fails and displays a runtime error.
909867	FortiManager attempts to configure unsupported syntax for "`sdwan health-check`".

Bug ID	Description
910391	When FortiManageroperates in a non-default workspace mode, it may attempt to purge the configuration of the FortiGate devices due to database corruption.
911535	Adding a Model device with MetaVariables changes the status of other devices which using the MetaVariables to Modified/unknown.
912833	When adding FortiGates with Open Authentication (OAuth) Method, Fortinet Security Fabric dialog box does not display the FortiManager's related info.
915361	FortiWiFi devices are displayed in FortiManager under the Vulnerable devices as FortiAP.
917969	FortiManager is unable to search static routes via its interface name.
918292	The SDWAN services cannot be modified, and attempting to make changes results in an "Invalid Value" error message.
921094	In 6.2 or 6.4 ADOMs, problems might occur when attempting to add or modify static routes. **Workarounds**: Please create a fresh backup of your FMG and FGT, then try either of the following: • Configure static routes directly on the FortiGate and retrieve routes from FortiGates to FortiManager. The configuration will not be lost during the next installation. • Run Scripts (static routes config) as target: Remote FortiGate Directly (via CLI) to FGT and auto-retrieve by a script manager or a manual retrieve if auto-update is disabled.
925546	Assigned Devices on Provisioning Template/CLI Template shows incorrect VDOM.
925684	Only a maximum of 10 devices can be previewed before installation using "install preview".
925854	FortiManager fails to load the Security fabric data for FortiGates (Versions 7.0.5+ & 7.2.5).
931736	Adding a new cli template script into existing cli template group changes order of cli templates to alphabetical order.
939804	Creating/Modifying the IPSEC Phase1 Interface Mode might trigger the following error message: "The string contains XSS vulnerability characters."

FortiSwitch Manager

Bug ID	Description
881766	Event logs or task manager do not show which user authorized a FortiSwitch.
922068	*FortiSwitch Manager* does not display any ports for managed switches.

Global ADOM

Bug ID	Description
894714	FortiManager does not allow creating/modification or removing the per-device mapping in global objects in assigned ADOM.
906058	Firewall address cannot be deleted from Global ADOM; it displays an error message indicating that the object is being used in ADOM root.
925188	The per-device mapping for any assigned global objects cannot be modified.

Others

Bug ID	Description
880465	TCP ports 8902 & 8903 are opened and in listening mode after the upgrade.
885665	Unable to specify type of objects in FortiProxy ADOM.
894947	FortiManager fails to trigger the event handler for its local events after enabling the FortiAnalyzer features.
895982	Admin with a super user profile is not able to create the Firmware Template when FortiManager is working in the Workflow mode.
897157	Unexpected changes in existing static routes, created by static route template after upgrade to 7.0.7, 7.2.2, 7.4.0.
910175	When provisioning the FortiExtender via CLI template, FortiManager displays the "mismatch interface" error message.
914027	FortiManager does not display/use the latest ISDB version for all of its ADOMs.
916463	The approval emails are not being sent to the "Email Notification" admins when a new session is created and submitted for approval.
917834	Report Definitions cannot be viewed or modified from FortiManager when FortiAnalyzer is being managed by FortiManager.
918129	FortiManager does not support the AWS Security Token Service in AWS SDN connector.
919088	GUI may not work properly in Google Chrome and Microsoft Edge version 114.
919981	Installation fails to Azure FortiGate standalone as FortiManager attempts to set the peervd to "root".
921273	Unable to upgrade ADOMs due to the XSS vulnerability characters check on wireless-controller.
925778	FortiGate's are displayed offline and inactive on FortiWLM MEA.
930305	Firmware template upgrade preview shows incorrect versions for the upgrade.

Policy & Objects

Bug ID	Description
777017	FortiManager purges the "`arrp-profile`" when installing the v6.2 policy packages to v6.4 FortiGates.
845022	SDN Connector failed to import objects from VMware VSphere.
863819	Unable to delete unused objects.
869863	NSX connector, unable to unselect the group with no users.
873358	Installation fails as FortiManager tries to set "`cgn-client-startip`" and "`cgn-client-endip`" settings when ippool object has been modified.
880418	The default values of the Application Control Profile entries cannot be changed.
883064	If any admin makes changes to "Object Selection Pane", either setting it to "Dock to Right", "Dock to Bottom", or "Classic Dual Pane", it will affects all other Admin's GUI preferences.
889586	Azure Service Tags not displayed correctly in FortiManager.
894597	Default value for `unsupported-ssl-version` in `ssl-ssh-profile` gets modified during the installation.
896461	FortiManager disables `ip6-send-adv` after opening and closing interface configuration.
896491	Installation fails with unclear error message: "vdom copy failed".
898883	Exported firewall policies do not contain firewall address values IP, netmask, and other details.
902298	FortiManager does not generate error messages when invalid or obsolete application IDs are used in the policy. Instead, it allows installation and sets the category to "pass" or "monitor".
911146	Under the *Policy & Objects*, GUI does not display the Address Object list.
912114	FortiManager is unable to import OpenStack SDN connector and the following error message is displayed: "send_sdn_connector_openstack_cmd: Failed to get openstack token".
914945	Unable to modify or clone the "SSL/SSH inspection profile" in the Policy & Object on the ADOM 7.0 version.
914981	In *Policy & Objects*, local policy is not displayed if view mode "Interface pair view" is selected.
916459	The option "Allow Websites When a Rating Error Occurs" is not being saved correctly in the default web filter.
919415	Unable to "*Edit*" and "*Delete*" Installation Target after enable classic dual pane mode.
919681	The incoming and outgoing interfaces are not loading after creating a custom policy package in a 7.2 FortiGate ADOM.
920740	Unable to create a per device mapping for a virtual server.
920983	The policy blocks using a group object do not get updated when the objects within the group are modified.

Bug ID	Description
922648	FortiManager unable to push WiFi SSID to FortiGates.
925058	"Web URL Filter" entries are not visible in the Web Filter Profile.
925076	FortiManager tries to install different preconnection-id under VPN SSL WEB Portal > Profile > Bookmark-Group > Gui-Bookmark > Book.

Script

Bug ID	Description
913360	Device script is trying to add additional configuration therefore installation gets failed.
931196	Scheduled Scripts created by the ldap users cannot be run and FortiManager displays "Data is not ready" error message.

System Settings

Bug ID	Description
733279	After changing the http or https port, FortiManager displays an "Unknown Error." error message.
861997	Unable to delete a particular non-default empty ADOM.
890956	SAML SSO Authentication only works with the default local certs.

VPN Manager

Bug ID	Description
847479	Despite being configured for 'SHA-256,' FortiManager is installing 'SHA-1' certificates on FortiGates.
863424	The "Latest Patch Level" should be available with action "Check-up-to-date" under the SSL VPN Portal.
931564	In *VPN Manager*, ipsec vpn map, topology view, and traffic view does not display map normally.

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.

FORTINET®

www.fortinet.com