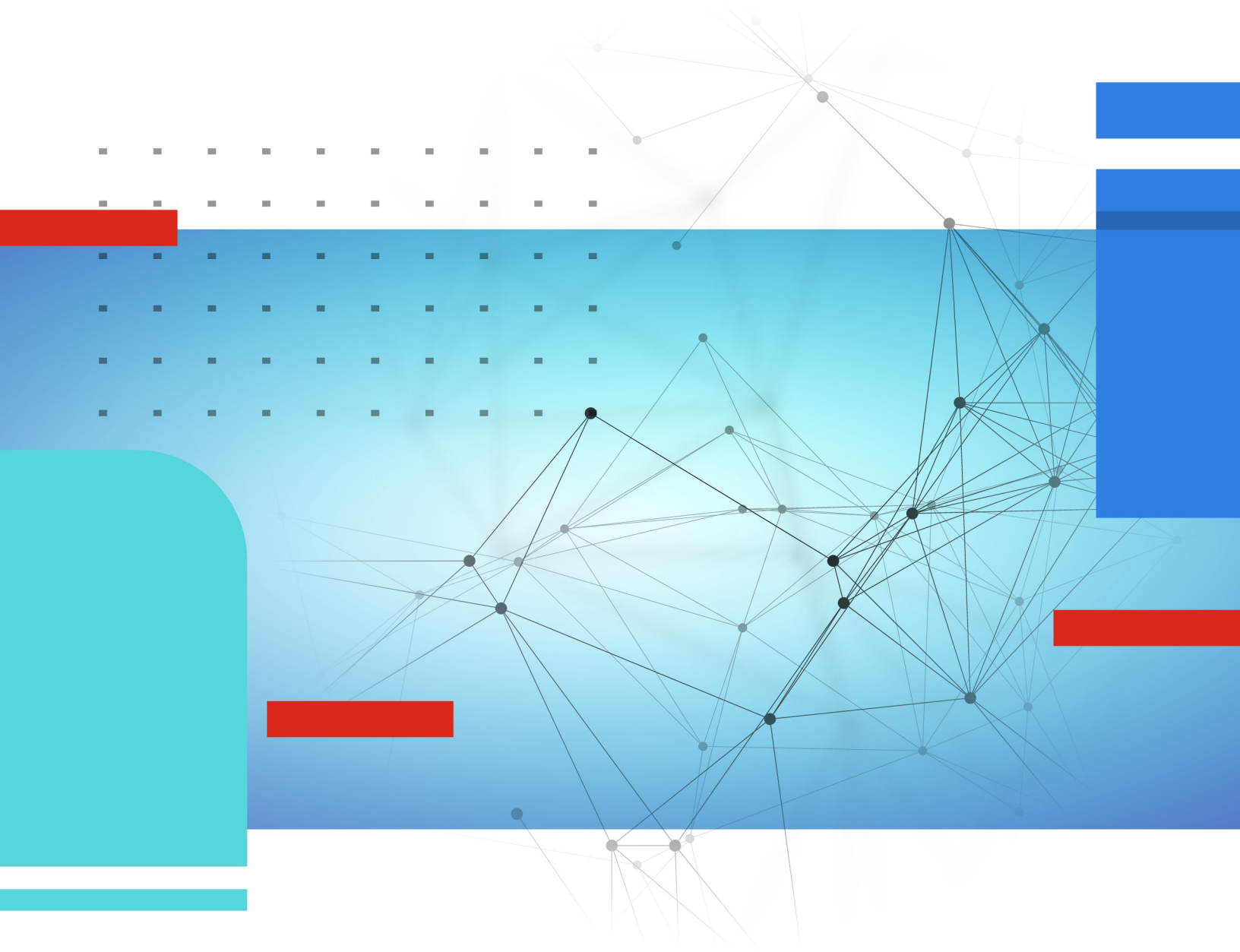
Release Notes

FortiManager 7.6.1



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com



October 24th, 2024
FortiManager 7.6.1 Release Notes
02-761-1088124-20241024

TABLE OF CONTENTS

Change Log **6**
FortiManager 7.6.1 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**
Log insertion interruption when upgrading from 7.40/7.4.1 to 7.6.0/7.6.1 10
Shell access has been removed 10
Enable fcp-cfg-service for Backup Mode ADOMs 10
FortiSOAR MEA license must be activated or uploaded 11
System Templates include new fields 11
Custom certificate name verification for FortiGate connection 11
Additional configuration required for SSO users 12
When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade 12
FortiGuard web filtering category v10 update 12
FortiManager 7.2.3 and later firmware on FortiGuard 13
Configuration backup requires a password 13
FortiManager-400E support 13
Serial console has changed for FortiManager deployments on Xen 14
OpenXen in PV mode is not supported in FortiManager 7.4.1 14
Option to enable permission check when copying policies 14
Install On column for policies 15
Changes to FortiManager meta fields 15
View Mode is disabled in policies when policy blocks are used 15
Reconfiguring Virtual Wire Pairs (VWP) 15
Citrix XenServer default limits and upgrade 15
Multi-step firmware upgrades 16
Hyper-V FortiManager-VM running on an AMD CPU 16
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 22

FortiAnalyzer-BigData 22
FortiAuthenticator 22
FortiCache 22
FortiCASB 22
FortiClient 22
FortiDDoS 23
FortiDeceptor 23
FortiFirewall and FortiFirewallCarrier 23
FortiMail 23
FortiPAM 23
FortiProxy 23
FortiSandbox 24
FortiSASE 24
FortiSOAR 24
FortiSwitch ATCA 24
FortiTester 25
FortiToken 25
FortiWeb 25
Virtualization 25
Feature support 26
Language support 27
Supported models 27
FortiGate models 28
FortiGate special branch models 31
FortiCarrier models 32
FortiCarrier special branch models 34
FortiADC models 35
FortiAnalyzer models 35
FortiAnalyzer-BigData models 36
FortiAuthenticator models 36
FortiCache models 36
FortiDDoS models 37
FortiDeceptor models 37
FortiFirewall models 37
FortiFirewallCarrier models 38
FortiMail models 39
FortiPAM models 39
FortiProxy models 40
FortiSandbox models 40
FortiSOAR models 40
FortiSwitch ATCA models 40
FortiTester models 41
FortiWeb models 41
FortiExtender MODEM firmware compatibility 42
Compatibility with FortiOS Versions 43
FortiManager 7.6.1 and FortiOS 7.2.9 compatibility issues 43
FortiManager 7.6.1 and FortiOS 7.2.10 compatibility issues 44

Resolved Issues **46**
Common Vulnerabilities and Exposures 46
Known issues **47**
New known issues 47
Existing known issues 47
AP Manager 47
Device Manager 48
FortiSwitch Manager 49
Others 49
Policy & Objects 50
Script 51
System Settings 52
Appendix A - FortiGuard Distribution Servers (FDS) **53**
FortiGuard Center update support 53
Appendix B - Default and maximum number of ADOMs supported **54**
Hardware models 54
Virtual Machines 54

Change Log

Date	Change Description
2024-10-24	Initial release of 7.6.1.

FortiManager 7.6.1 Release

This document provides information about FortiManager version 7.6.1 build 3344.



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 7.6.1 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400G, FMG-410G, FMG-1000F, FMG-1000G, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3100G, 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_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_IBM, 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 54.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.6.1.

FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the 7.6 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-3100G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_IBM, 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 7.6.1.

Log insertion interruption when upgrading from 7.40/7.4.1 to 7.6.0/7.6.1

Log insertion might be interrupted if FortiManager is upgraded directly from version 7.4.0/7.4.1 to 7.6.0. This issue only occurs if FortiAnalyzer Features are enabled on the FortiManager.

To avoid this issue, upgrade to a later FortiManager 7.4 version (for example, 7.4.2 or 7.4.3) before upgrading to 7.6.0/7.6.1. As a general best practice, Fortinet recommends upgrading to the latest patch version available before upgrading to the next major version.

Shell access has been removed

As of FortiManager 7.6.0, shell access has been removed.

The following CLI variables have been removed, which were previously used to enable shell access:

```
config system admin setting
   set shell-access {enable | disable}
   set shell-password <passwd>
```

The following CLI command has been removed, which was previously used to access shell when enabled:

```
execute shell
```

Enable fcp-cfg-service for Backup Mode ADOMs

When performing a configuration backup from the CLI of FortiGates managed by FortiManager in Backup Mode ADOMs, you must enable the "`fcp-cfg-service`" using the following command on the FortiManager:

```
config system global
   set fcp-cfg-service enable
end
```

FortiSOAR MEA license must be activated or uploaded

In previous versions, the trial license was automatically activated when the FortiSOAR MEA was enabled. Beginning in FortiManager 7.6.0, which includes the FortiSOAR MEA 7.6.0, you must activate the trial license or upload a license to use the FortiSOAR MEA.

After enabling the FortiSOAR MEA, go to *Management Extensions* > *FortiSOAR* to activate or upload the license. For more information, see the Management Extensions documentation in the FortiManager Document Library.

System Templates include new fields

Beginning in FortiManager 7.4.3, the *Hostname*, *Timezone*, *gui-device-latitude*, and *gui-device-longitude* fields have been added to System Templates.

System Templates created before upgrading to 7.4.3 must be reconfigured to specify these fields following the upgrade. If these fields are not specified in a System Template, the default settings will be applied the next time an install is performed which may result in preferred settings being overwritten on the managed device.

Custom certificate name verification for FortiGate connection

FortiManager 7.4.3 introduces a new verification of the CN or SAN of a custom certificate uploaded by the FortiGate admin. This custom certificate is used when a FortiGate device connects to a FortiManager unit. The FortiGate and FortiManager administrators may configure the use of a custom certificate with the following CLI commands:

FortiGate-related CLI:

```
config system central-management
   local-cert Certificate to be used by FGFM protocol.
   ca-cert CA certificate to be used by FGFM protocol.
```

FortiManager-related CLI:

```
config system global
   fgfm-ca-cert set the extra fgfm CA certificates.
   fgfm-cert-exclusive set if the local or CA certificates should be used exclusively.
   fgfm-local-cert set the fgfm local certificate.
```

Upon upgrading to FortiManager 7.4.3, FortiManager will request that the FortiGate certificate must contain the FortiGate serial number either in the CN or SAN. The tunnel connection may fail if a matching serial number is not found. If the tunnel connection fails, the administrator may need to re-generate the custom certificates to include serial number.

Alternatively, FortiManager 7.4.3 provides a new CLI command to disable this verification. Fortinet recommends to keep the verification enabled.

```
config system global
   fgfm-peercert-withoutsn set if the subject CN or SAN of peer's SSL certificate sent in
        FGFM should include the serial number of the device.
```

When the CLI setting `fgfm-peercert-withoutsn` is disabled (default), the FortiGate device's certificate must include the FortiGate serial number in the subject CN or SAN. When the CLI setting `fgfm-peercert-withoutsn` is enabled, the FortiManager unit does not perform the verification serial number in subject CN or SAN.

Additional configuration required for SSO users

Beginning in 7.4.3, additional configuration is needed for FortiManager Users declared as wildcard SSO users.

When configuring Administrators as wildcard SSO users, the `ext-auth-accprofile-override` and/or `ext-auth-adom-override` features, under *Advanced Options*, should be enabled if the intent is to obtain the ADOMs list and/or permission profile from the SAML IdP.

When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade

When FortiManager is upgraded to 7.4.2/7.6.0 or later, it creates a new CA <ADOM Name>_CA3 certificate as part of a fix for resolved issue 796858. See Resolved Issues in the FortiManager 7.4.2 Release Notes. These certificates are installed to the FortiGate devices on the next policy push. As a result, the next time any IPSEC VPNs which use FortiManager certificates rekey, they will fail authentication and be unable to re-establish.

The old CA <ADOM Name>_CA2 cannot be deleted, as existing certificates rely on it for validation. Similarly, the new CA <ADOM Name>_CA3 cannot be deleted as it is required for the fix. Therefore, customers affected by this change must follow the below workaround after upgrading FortiManager to v7.4.2/7.6.0 or later.

A maintenance period is advised to avoid IPSEC VPN service disruption.

Workaround:

Re-issue *all* certificates again to *all* devices, and then delete the old CA <ADOM Name>_CA2 from all devices. Next, regenerate the VPN certificates.

To remove CA2 from FortiManager, *Policy & Objects* > *Advanced* > *CA Certificates* must be enabled in feature visibility.

FortiGuard web filtering category v10 update

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

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

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

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

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.

Configuration backup requires a password

As of FortiManager 7.4.2, configuration backup files are automatically encrypted and require you to set a password. The password is required for scheduled backups as well.

In previous versions, the encryption and password were optional.

For more information, see the FortiManager Administration Guide.

FortiManager-400E support

FortiManager 7.4.2 and later does not support the FortiManager-400E device.

FortiManager 7.4.2 introduces an upgrade of the OpenSSL library to address known vulnerabilities in the library. As a result, the SSL connection that is setup between the FortiManager-400E device and the Google Map server hosted by Fortinet uses a SHA2 (2048) public key length. The certificate stored on the BIOS that is used during the setup of the SSL connection contains a SHA1 public key length, which causes the connection setup to fail. Running the following command shows the key length.

```
FMG400E # conf sys certificate local
   (local)# ed Fortinet_Local
      (Fortinet_Local)# get
      name : Fortinet_Local
      password : *
      comment : Default local certificate
      private-key :
      certificate :
```

```
        Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN
             = FL3K5E3M15000074, emailAddress = support@fortinet.com
        Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
             Authority, CN = support, emailAddress = support@fortinet.com
        Valid from: 2015-03-06 16:22:10 GMT
        Valid to: 2038-01-19 03:14:07 GMT
        Fingerprint: FC:D0:0C:8D:DC:57:B6:16:58:DF:90:22:77:6F:2C:1B
        Public key: rsaEncryption (1024 bits)
        Signature: sha1WithRSAEncryption
        Root CA: No
        Version: 3
        Serial Num:
        1e:07:7a
        Extension 1: X509v3 Basic Constraints:
        CA:FALSE
        ...
(Fortinet_Local)#
```

Serial console has changed for FortiManager deployments on Xen

As of FortiManager 7.4.1, the serial console for Xen deployments has changed from hvc0 (Xen specific) to ttyS0 (standard).

OpenXen in PV mode is not supported in FortiManager 7.4.1

As of FortiManager 7.4.1, kernel and rootfs are encrypted. OpenXen in PV mode tries to unzip the kernel and rootfs, but it will fail. Therefore, OpenXen in PV mode cannot be used when deploying or upgrading to FortiManager 7.4.1. Only HVM (hardware virtual machine) mode is supported for OpenXen in FortiManager 7.4.1.

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.

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.

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.

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*.

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.

Upgrade Information



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

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



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 7.4 supports ADOM versions 7.0, 7.2, and 7.4, but FortiManager 7.6 supports ADOM versions 7.2, 7.4, and 7.6. Before you upgrade FortiManager 7.4 to 7.6, ensure that all ADOM 7.0 versions have been upgraded to ADOM version 7.2 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 7.6.1 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- Supported software on page 20
- Feature support on page 26
- Language support on page 27
- Supported models on page 27
- FortiExtender MODEM firmware compatibility on page 42

Supported software

FortiManager 7.6.1 supports the following software:

- Web browsers on page 21
- FortiOS and FortiOS Carrier on page 21
- FortiADC on page 21
- FortiAnalyzer on page 22
- FortiAnalyzer-BigData on page 22
- FortiAuthenticator on page 22
- FortiCache on page 22
- FortiCASB on page 22
- FortiClient on page 22
- FortiDDoS on page 23
- FortiDeceptor on page 23
- FortiFirewall and FortiFirewallCarrier on page 23
- FortiMail on page 23
- FortiPAM on page 23
- FortiProxy on page 23
- FortiSandbox on page 24
- FortiSASE on page 24
- FortiSOAR on page 24
- FortiSwitch ATCA on page 24
- FortiTester on page 25
- FortiToken on page 25
- FortiWeb on page 25
- Virtualization on page 25



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 7.6.1 supports the following web browsers:

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

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

FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.6.1 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the Fortinet Document Library.

See FortiManager compatibility with FortiOS.

FortiManager 7.6.1 supports the following versions of FortiOS and FortiOS Carrier:

- 7.6.0
- 7.4.0 to 7.4.4
- 7.2.0 to 7.2.10



Some FortiOS versions are supported with compatibility issues. For more details, see Compatibility with FortiOS Versions on page 43.

FortiADC

FortiManager 7.6.1 supports the following versions of FortiADC:

- 7.4.0 and later
- 7.2.0 and later
- 7.1.0 and later

FortiAnalyzer

FortiManager 7.6.1 supports the following versions of FortiAnalyzer:

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

FortiAnalyzer-BigData

FortiManager 7.6.1 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAuthenticator

FortiManager 7.6.1 supports the following versions of FortiAuthenticator:

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

FortiCache

FortiManager 7.6.1 supports the following versions of FortiCache:

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

FortiCASB

FortiManager 7.6.1 supports the following versions of FortiCASB:

- 23.2.0 and later

FortiClient

FortiManager 7.6.1 supports the following versions of FortiClient:

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

FortiDDoS

FortiManager 7.6.1 supports the following versions of FortiDDoS:

- 7.0.0 and later
- 6.6.0 and later
- 6.5.0 and later
- 6.4.0 and later

Limited support. For more information, see Feature support on page 26.

FortiDeceptor

FortiManager 7.6.1 supports the following versions of FortiDeceptor:

- 5.3.0 and later
- 5.2.0 and later
- 5.1.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.6.1 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 7.6.1 supports the following versions of FortiMail:

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

FortiPAM

FortiManager 7.6.1 supports the following versions of FortiPAM:

- 1.1.0 and later
- 1.0.0 and later

FortiProxy

FortiManager 7.6.1 supports configuration management for the following versions of FortiProxy:

- 7.4.0 to 7.4.3
- 7.2.2, 7.2.3, 7.2.7, and 7.2.9
- 7.0.7 to 7.0.16



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

FortiManager 7.6.1 supports logs from the following versions of FortiProxy:

- 7.4.0 to 7.4.4
- 7.2.0 to 7.2.11
- 7.0.0 to 7.0.18
- 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 7.6.1 supports the following versions of FortiSandbox:

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

FortiSASE

FortiManager 7.6.1 supports the following versions of FortiSASE:

- 23.2

FortiSOAR

FortiManager 7.6.1 supports the following versions of FortiSOAR:

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

FortiSwitch ATCA

FortiManager 7.6.1 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.6.1 supports the following versions of FortiTester:

- 7.3.0 and later
- 7.2.0 and later
- 7.1.0 and later

FortiToken

FortiManager 7.6.1 supports the following versions of FortiToken:

- 3.0.0 and later

FortiWeb

FortiManager 7.6.1 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.6.1 supports the following virtualization software:

Public Cloud

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Alibaba Cloud
- Google Cloud Platform
- IBM Cloud
- Microsoft Azure
- Oracle Cloud Infrastructure

Private Cloud

- Citrix XenServer 7.2
- OpenSource XenServer 4.2.5
- Microsoft Hyper-V Server 2016, 2019, and 2022
- Nutanix

  - AHV 20220304 and later
  - AOS 6.5 and later
  - NCC 4.6 and later
  - LCM 3.0 and later
- RedHat 9.1
  - Other versions and Linux KVM distributions are also supported
- 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 7.6.1.

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

This section contains the following topics:

- FortiGate models on page 28
- FortiGate special branch models on page 31
- FortiCarrier models on page 32
- FortiCarrier special branch models on page 34
- FortiADC models on page 35
- FortiAnalyzer models on page 35
- FortiAnalyzer-BigData models on page 36
- FortiAuthenticator models on page 36

- FortiCache models on page 36
- FortiDDoS models on page 37
- FortiDeceptor models on page 37
- FortiFirewall models on page 37
- FortiFirewallCarrier models on page 38
- FortiMail models on page 39
- FortiPAM models on page 39
- FortiProxy models on page 40
- FortiSandbox models on page 40
- FortiSOAR models on page 40
- FortiSwitch ATCA models on page 40
- FortiTester models on page 41
- FortiWeb models on page 41

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see FortiGate special branch models on page 31.

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60F, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-100F, FortiGate-101F, 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-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC **FortiGate 7000 Series**: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.6

Model	Firmware Version
FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-ACDC, FortiGate-3000F-DC, FortiGate-3001F-ACDC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC **FortiWiFi:** FWF-40F, FWF-40F-3G4G, FWF-60F, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R-3G4G-DSL, 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-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, FGR-70F, FGR-70F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100F, 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-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC **FortiGate 7000 Series**: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.4

Model	Firmware Version
FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, 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-80F-2R-3G4G-DSL, FWF-81F-2R-3G4G-DSL, 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, FGR-70F, FGR-70F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC **FortiGate 7000 Series**: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.2

Model	Firmware Version
FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, 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, FortiGate-4800F-DC, FortiGate-4801F-DC **FortiWiFi:** FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.6.1 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 28.

FortiOS 7.0

FortiGate Model	FortiOS Version
FortiGate-80F-DSL	7.0.15
FortiGate-90G, FortiGate-91G	7.0.15
FortiGate-120G, FortiGate-121G	7.0.15
FortiGate-900G, FortiGate-901G	7.0.15
FortiGate-1000F, FortiGate-1001F	7.0.15
FortiGate-3200F	7.0.15
FortiGate-3201F	7.0.15
FortiGate-3700F, FortiGate-3701F	7.0.15
FortiGate-4800F, FortiGate-4800F-DC, FortiGate-4801F, FortiGate-4801F-DC	7.0.15
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.15

FortiGate Model	FortiOS Version
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.15
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.15
FortiGateRugged-70F, FortiGateRugged-70F-3G4G	7.0.15
FortiWiFi-50G-5G	7.0.12
FortiWiFi-80F-2R-3G4G-DSL	7.0.15
FortiWiFi-81F-2R-3G4G-DSL	7.0.15

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 34.

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6001F, 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-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3000F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4800F-DC, FortiCarrier-4801F-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.6

Model	Firmware Version
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6001F, 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-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **FortiCarrier-DC**: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-IBM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.4
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6001F, 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-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.2

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.6.1 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see FortiCarrier models on page 32.

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version
FortiCarrier-3200F	7.0.15
FortiCarrier-3201F	7.0.15
FortiCarrier-3700F, FortiCarrier-3701F	7.0.15
FortiCarrier-4800F, FortiCarrier-4800F-DC, FortiCarrier-4801F, FortiCarrier-4801F-DC	7.0.15
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.15
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.15
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.15

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	7.1, 7.2, 7.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, 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	7.4
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, 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
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, 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	6.6
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	7.0
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F **FortiDDoS VM**: FortiDDoS-VM	6.6
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 **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	5.0, 5.1, 5.2, 5.3
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.6.1 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version
FortiFirewall: FortiFirewall-1801F, FortiFirewall-2600F, FortiFirewall-3001F, FortiFirewall-3501F, FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F **FortiFirewall DC**: FortiFirewall-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.6
FortiFirewall: FortiFirewall-1801F, FortiFirewall-2600F, FortiFirewall-3001F, FortiFirewall-3501F, FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F	7.4

Model	Firmware Version
FortiFirewall DC: FortiFirewall-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	
FortiFirewall: FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F **FortiFirewall DC**: FortiFirewall-4200F-DC, FortiFirewall-4401F-DC **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.0

FortiFirewall special branch models

Model	Firmware Version	Firmware Build (for special branch)
FortiFirewall: FortiFirewall-3001F	7.0.10	4955
FortiFirewall: FortiFirewall-3501F	7.0.10	4955

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.6.1 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version
FortiFirewallCarrier: FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F **FortiFirewallCarrier DC**: FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.6
FortiFirewallCarrier: FortiFirewallCarrier-1801F, FortiFirewallCarrier-2600F, FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F **FortiFirewallCarrier DC**: FortiFirewallCarrier-1801F-DC, FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.4
FortiFirewallCarrier: FortiFirewallCarrier-2600F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4801F	7.2

Model	Firmware Version
FortiFirewallCarrier DC: FortiFirewallCarrier-4200F-DC **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	
FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.0

FortiFirewall special branch models

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-1801F, FortiFirewallCarrier-4401F	7.2.6	4609
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0.10	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0.10	4940

FortiMail models

Model	Firmware Version
FortiMail: FE-200F, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FortiMail Cloud	7.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FortiMail Cloud	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

FortiPAM models

Model	Firmware Version
FortiPAM: FortiPAM-1000G, FortiPAM-3000G **FortiPAM VM:** FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1

FortiProxy models

Model	Firmware Version
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, 7.2, 7.4
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-500G, FSA-1000D, FSA-1000F, FSA-1500G, 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, 4.4
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-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-BYOL, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.3
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-BYOL, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.2
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

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-100F, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-400F, FortiWeb-600D, FortiWeb-600E, FortiWeb-600F, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, 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	7.4

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, 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	7.2
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	7.0

FortiExtender MODEM firmware compatibility

See the FortiOS Release Notes for a list of MODEM firmware filename and version for each FortiExtender model and where in the world the MODEMs are compatible.

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.6.1.

FortiManager 7.6.1 and FortiOS 7.2.9 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.6.1 and FortiOS 7.2.9.



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

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

The following objects were added:

- `(attr) firewall shaping-profile npu-offloading`
- `(attr) switch-controller managed-switch radius-nas-ip (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller managed-switch radius-nas-ip-override (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller security-policy 802-1X authserver-timeout-tagged (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller security-policy 802-1X authserver-timeout-tagged-vlanid (133 platforms: excludes 5001E1,5001E)`
- `(attr) system csf legacy-authentication`
- `(attr) system federated-upgrade source`
- `(attr) system npu background-sse-scan scan-stale (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu background-sse-scan scan-vt (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu background-sse-scan stats-qual-access (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu background-sse-scan stats-qual-duration (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu background-sse-scan udp-qual-access (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu background-sse-scan udp-qual-duration (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)`
- `(attr) system npu default-tcp-refresh-dir (24 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)`
- `(attr) system npu default-udp-refresh-dir (24 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)`
- `(attr) system npu nss-threads-option (21 platforms: 3500F,4401F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)`
- `(attr) user radius switch-controller-nas-ip-dynamic (133 platforms: excludes 5001E1,5001E)`

The following objects were removed:

- `(attr) system ha logical-sn (113 platforms: excludes 60F,70F-3G4G,81F-2R,40F-3G4G,601E,60F-3G4G,70F,80F,81F-2R-POE,80F-BYPASS,40F,80F-2R,81F-2R-3G4G-POE,81F-POE,61F,81F,71F,80F-POE)`

The following default values changed:

- `report setting fortiview (disable -> enable)`
- `report setting pdf-report (disable -> enable)`
- `system global ssh-kex-algo (diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 -> diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521)`
- `system npu sse-ha-scan gap (6000 -> 200)`

Additional option changes:

```
system global ssh-kex-algo
   ++ 3 opts: diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-
      group18-sha512
web-proxy explicit pref-dns-result
   ++ 2 opts: ipv4-strict ipv6-strict
```

Other changes:

```
system csf group-password
   tag: mu -> None
system global faz-disk-buffer-size
   tag: lmt -> None
   tag: lsz -> None
```

FortiManager 7.6.1 and FortiOS 7.2.10 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.6.1 and FortiOS 7.2.10.



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

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

The following objects were added:

- `(attr) firewall shaping-profile npu-offloading`
- `(attr) switch-controller managed-switch radius-nas-ip (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller managed-switch radius-nas-ip-override (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller security-policy 802-1X authserver-timeout-tagged (133 platforms: excludes 5001E1,5001E)`
- `(attr) switch-controller security-policy 802-1X authserver-timeout-tagged-vlanid (133 platforms: excludes 5001E1,5001E)`
- `(attr) system csf legacy-authentication`

- (attr) system federated-upgrade source
- (attr) system npu background-sse-scan scan-stale (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu background-sse-scan scan-vt (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu background-sse-scan stats-qual-access (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu background-sse-scan stats-qual-duration (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu background-sse-scan udp-qual-access (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu background-sse-scan udp-qual-duration (21 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,3001F)
- (attr) system npu default-tcp-refresh-dir (24 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)
- (attr) system npu default-udp-refresh-dir (24 platforms: 3500F,1801F,4401F,1800F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)
- (attr) system npu nss-threads-option (21 platforms: 3500F,4401F,3000F,4201F,3501F,4200F,4400F,2600F,3001F)
- (attr) user radius switch-controller-nas-ip-dynamic (133 platforms: excludes 5001E1,5001E)

The following objects were removed:

- (attr) system ha logical-sn (113 platforms: excludes 60F,70F-3G4G,81F-2R,40F-3G4G,601E,60F-3G4G,70F,80F,81F-2R-POE,80F-BYPASS,40F,80F-2R,81F-2R-3G4G-POE,81F-POE,61F,81F,71F,80F-POE)

The following default values changed:

- report setting fortiview (disable -> enable)
- report setting pdf-report (disable -> enable)
- system global ssh-kex-algo (diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 -> diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521)
- system npu sse-ha-scan gap (6000 -> 200)

Additional option changes:

```
system global ssh-kex-algo
  ++ 3 opts: diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-
       group18-sha512
web-proxy explicit pref-dns-result
  ++ 2 opts: ipv4-strict ipv6-strict
```

Other changes:

```
system csf group-password
  tag: mu -> None
system global faz-disk-buffer-size
  tag: lmt -> None
  tag: lsz -> None
```

Resolved Issues

The following issues have been fixed in 7.6.1. To inquire about a particular bug, please contact Customer Service & Support.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1086790	FortiManager 7.6.1 is no longer vulnerable to the following CVE Reference: • CVE-2024-47575

Known issues

Known issues are organized into the following categories:

- New known issues on page 47
- Existing known issues on page 47

To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

New known issues

No new issues have been identified in version 7.6.1.

Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.6.1.

AP Manager

Bug ID	Description
955558	FortiManager unsets the Protected Management Frame (PMF) setting when the SSID security mode is configured to OWE-enabled in the *AP Manager*.
1040365	FortiManager is generating false vulnerability reports for certain FortiAPs: • U431F • U231F
1050466	The 802.11ax-5g AP profile is missing for all FortiAPs that support WiFi 6. This issue has been observed in FortiManager 7.6.0 and ADOM 7.6.
1060238	FortiManager is attempting to unset the FortiAP's name.
1076200	Policy install fails due to FortiManager installs unexpected changes related to "<wifi_intf> address". **Workaround**: Create a CLI template with all subnet addresses and assign to device.

Device Manager

Bug ID	Description
796842	Failed to reload the configuration due to the "datasrc invalid" error message.
952422	IPsec templates created by SDWAN Overlay does not create tunnels for all the underlay interfaces.
963025	When using the static route template, the "SD-WAN Zone" does not appear under the Interface column.
1003899	FortiManager generates a VPN certificate that is not accepted by the FIPS-enabled FortiGate devices.
1020257	Packet Capture feature for managed FortiGates does not work; it starts but immediately stops.
1034355	When assigning a provisioning template with Admin Settings configuration, FortiManager changes the hostname of the device.
1050126	Setting up a FortiGate-HA with ZTP fails because the FortiLink is not deleted during the "HA config pushed to FGT" process.
1053194	If the "`system interface speed`" attribute is changed from the FortiManager, it may potentially cause an installation failure. Modifying the "`system interface speed`" is not currently supported on the FortiManager and must be done on the FortiGate side.
1063835	FortiManager ZTP installation to FortiGate versions 7.2.8 and lower may fail due to differing default "`ssh-kex-algo`" settings between FortiManager and FortiGate.
1070943	Unable to upgrade the devices using the Device Group Upgrade Firmware feature. **Workaround**: Upgrade devices individually by using the "Device Firmware Upgrade" feature or Create New Firmware Template for single devices or device groups and use the "Assign to Devices/Groups feature.
1074717	An error might be observed when the SD-WAN template health check name contains a space, displaying the following message: "Bad health check name...".
1075281	Unable to add FortiAnalyzer to FortiManager, when "`fgfm-peercert-withoutsn`" is enabled. **Workaround**: Set the "`fgfm-peercert-withoutsn`" to disable and then add FortiAnalyzer to FortiManager.
1075747	SD-WAN Monitor does not display the members under the SD-WAN Rules (Map View or Table View).

FortiSwitch Manager

Bug ID	Description
1040428	FortiSwitch diagnostics tools do not display thecable test diagnose results, device information on Ports, and update Registration status.
1053220	Unable to delete FortiSwitches when central management is enabled for FortiSwitch. **Workaround**: Remove the FortiSwitch on FortiGate and retrieve on the FortiManager.
1060242	Unable to change the FortiSwitch name from the *FortiSwitch Manager*.

Others

Bug ID	Description
998198	When upgrading ADOM, the upgrade process fails with the following error: "invalid value - can not find import template 'XYZ'". **Workaround**: Locate the scripts, delete them, upgrade the ADOM and then import the scripts.
1015890	Unable to upgrade ADOM from v6.4 to v7.0 due to "switch-controller traffic-policy" error.

1019261	Unable to upgrade ADOM from 7.0 to 7.2, due to the error "Do not support urlfilter-table for global scope webfilter profile".
	Workaround:
	Run the following script against the ADOM DB:
	`config webfilter profile`
	`edit "g-default"`
	`config web`
	`unset urlfilter-table`
	`end`
	`next`
	`end`

1019784	ADOM Upgrade from 7.0 to 7.2 fails with the "Fail(errno=0):invalid value" error message.
1049457	When FortiAnalyzer is added as a managed device, users may encounter an issue in the FortiManager GUI when expanding the log details.

1053830	MEAs cannot be enabled from FortiManager's GUI.
	Workaround:
	Use the following CLI command to enable them (in this example, `universalconnector`):
	`config system docker`
	`set status enable`
	`set universalconnector enable`
	`end`

Bug ID	Description
1055417	Unable to upgrade the firmware version of the FortiGates in HA cluster by using the firmware template when HA is in-sync status. The failure to upgrade FortiGate HA cluster firmware is caused by a crash in "dmserver" daemon.
1058585	When enabling Fabric Management, the "csfd" process might not start immediately. **Workaround**: Reboot the Supervisor or Member FortiManagers to initiate the "csfd" process.
1060337	The log insertion might be interrupted if FortiManager is upgraded directly from version (7.4.0/7.4.1) to 7.6.0/7.6.1. This will only occur if FortiAnalyzer Features are enabled on FortiManager. **Workaround**: To avoid this issue, upgrade the FortiManager to 7.4.2/7.4.3 first and then to 7.6.0/7.6.1. For more details see Special Notices on page 10.
1062128	After upgrading to the latest available build, the FortiManager GUI displays the warning message: "A new firmware version is available".
1066132	When enabling the FortiAnalyzer features on FortiManager, a server error message might appear under "*FortiView* > *System* > *Resource Usage*".

Policy & Objects

Bug ID	Description
843716	FortiManager tries to unset url-map for TCP forwarding ZTNA virtual server.
963536	The policy package feature "Export to Excel" is not functioning.
971610	FortiManager does not able to import the Central SNAT, DNAT, DOS, local-in, and traffic shaping policies.
991720	FortiManager still has an option to enable the "match-vip" through the policy package for "allow" policies. However, this is not supported anymore on the FortiGates. **Workaround**: Disable the option under advance option in Firewall Rule.
1004056	The installation may encounter an error related to Syntax support for the "ssh-enc-algo" command. **Workaround**: Please try manually retrieving the configurations.
1005161	The policy package status changes for all devices even when an address object is opened and saved without any modifications. This issue is particularly observed in objects utilizing the per-device mapping feature.
1013948	After upgrading to FortiManager versions 7.2.5 or 7.4.3, the installation preview may hang. However, the installation process itself can be completed successfully.

Bug ID	Description
1014035	Video filter profile config is not getting pushed completely from FortiManager to FortiGate.
1025012	Configuring the SSL/SSH inspection profile may result in the following error: "The server certificate replacement mode cannot support category exemptions." **Workaroud**: 1. Modify the SSL/SSH inspection profiles. 2. Toggle from *Protecting SSL Server* to *Multiple Clients Connecting to multiple Servers*. 3. Remove the categories from the *Exempt from SSL inspection* list. 4. Toggle back to *Protecting SSL Server* and click *OK*. 5. Install.
1029787	The Firewall Policy pane in the FortiManager GUI may occasionally display both "Standard Security Profiles" (SSL no-inspection and protocol default profiles) and "Security Profile Groups" simultaneously.
1029921	Under the "Web Application Firewall" security profiles, users are unable to disable the signatures through the GUI.
1039766	The Firewall Policy Lookup feature does not display the list of source interfaces for FortiGates.
1040160	When installing policy to a FortiGate that uses FortiSandbox inline scanning on an AV profile, FortiManager unsets the configuration on install.
1066617	Unable to create the IP address object type wildcard, the following error message is displayed: "Invalid IP netmask". **Workaround**: Create CLI script and run it on ADOM DB or use Metadata variables.
1068736	Best Quality SDWAN rules installation may fail with the following error message: "Commit failed: Bad health check name".
1070800	FortiManager is attempting to install the "cli-cmd-audit" command on a FortiGate (FortiGate-101E and FortiGate-2000E) running version 7.2.8, which does not support this command, leading to an installation error.
1079678	FortiManager does not provide any warning when there is a "deny all" policy in the middle of a Policy Package. This can be still seen on the "task monitor".

Script

Bug ID	Description
931088	Unable to delete VDOMs using the FortiManager script. Interfaces remain in the device database, causing the installation to fail.

System Settings

Bug ID	Description
1005098	Verification of the LDAP Server through the LDAP Browser may display an "Operation Error" message. **Workaround**: If an "Operation Error" occurs during LDAP Server Browser verification, re-enter the password and attempt the verification process again.
1027547	In certain cases (currently under investigation), the License Status on FortiManager may be incorrectly displayed as "Expired" despite the license being active in the account. **Workaround**: Restart the FortiManager when feasible.
1040377	Despite unchecking the backup strategy option and receiving the "Setup Complete" message, the "Setup Wizard" continues to display during future logins on the Secondary members.
1047252	Incorrect warning message displayed in FortiManager GUI during upgrade from Feature build to Mature build.
1060943	FGFM Tunnel does not automatically come back online after disabling the "Offline Mode". **Workaround**: Reboot the FortiManager after disabling the offline mode.

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 443 to communicate with the proxy server in *tunnel* mode by default. Alternatively, you can configure web proxy to use *proxy* mode using port 80. For more information, see the FortiManager Administration Guide.

FortiGuard Center update support

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

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

Appendix B - Default and maximum number of ADOMs supported

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

Hardware models

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

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

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

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

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

Virtual Machines

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

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



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



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.