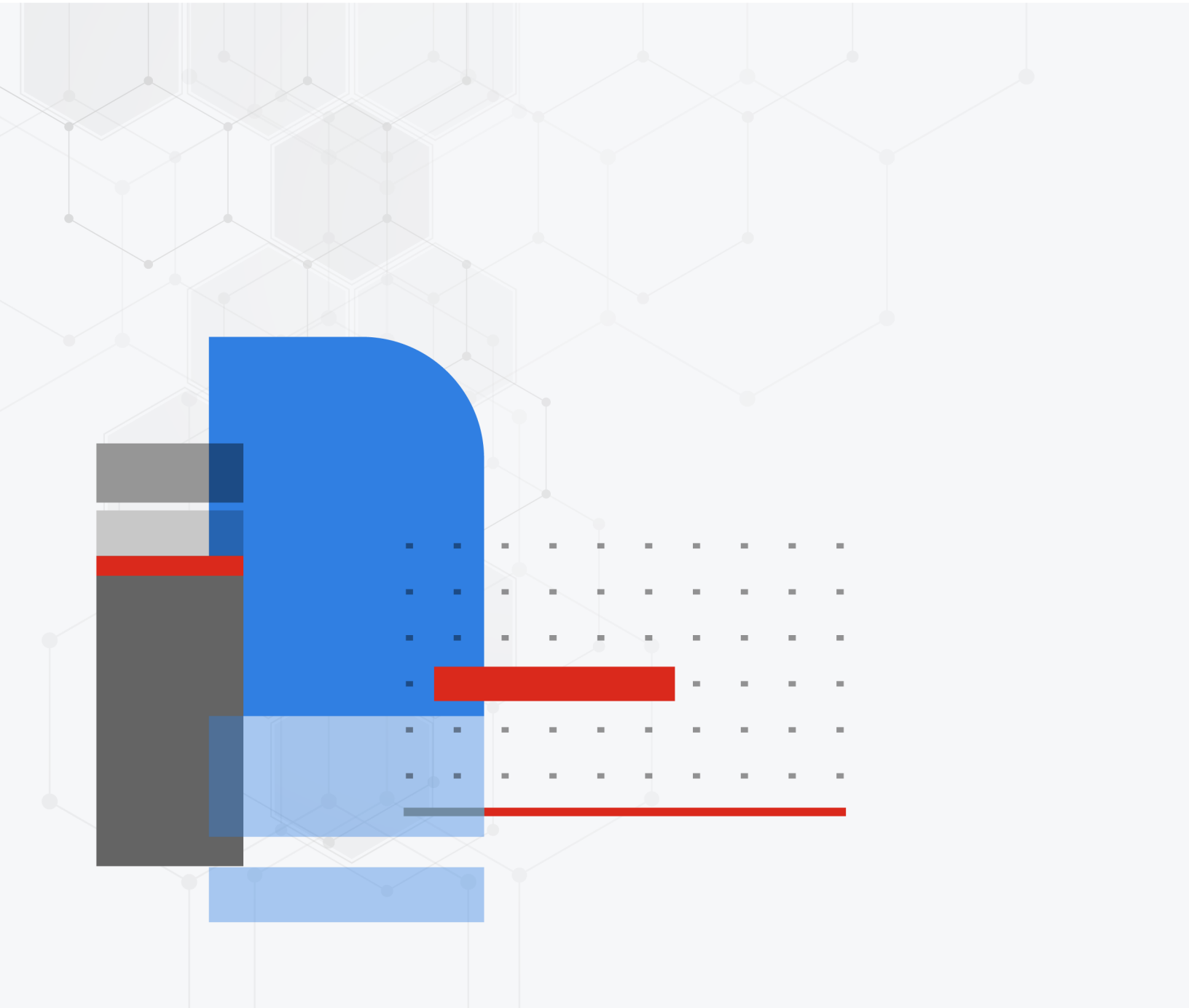




Release Notes

FortiManager 7.4.10



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



February 23, 2026

FortiManager 7.4.10 Release Notes

02-7410-1243946-20260223

TABLE OF CONTENTS

Change Log	6
FortiManager 7.4.10 Release	7
Supported models	7
Special branch supported models	7
FortiManager VM subscription license	8
Special Notices	9
Device database enters an incorrect state	9
MEAs removed in FortiManager 7.4.8	9
New Admin Profile permission	9
FortiSwitch 110G support	9
Unauthorized devices appearing in Device Manager despite having fgfm-deny-unknown enabled	10
New CLI option for managing FortiGate HA clusters	10
Adding VM devices to FortiManager	11
The system interface speed is read-only in FortiManager	11
Custom certificate name verification for FortiGate connection	11
The names of policies derived from policy blocks no longer automatically include the policy block name	12
Upgrading from 7.4.3 to 7.4.8 with FIPS mode enabled	12
Device blueprint header	13
Shell access has been removed	13
Enable fcp-cfg-service for Backup Mode ADOMs	13
System Templates include new fields	13
Additional configuration required for SSO users	14
When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade	14
Apache-mode changed from prefork to event	14
FortiGuard web filtering category v10 update	15
FortiManager 7.2.3 and later firmware on FortiGuard	15
Configuration backup requires a password	16
FortiManager-400E support	16
Serial console has changed for FortiManager deployments on Xen	17
OpenXen in PV mode is not supported in FortiManager 7.4.1	17
Default GUI theme changed	17
Option to enable permission check when copying policies	17
Install On column for policies	18
SD-WAN Orchestrator removed in 7.2	18
Changes to FortiManager meta fields	18
Setup wizard requires FortiCare registration	18
Access lists as ADOM-level objects	19
View Mode is disabled in policies when policy blocks are used	19
Reconfiguring Virtual Wire Pairs (VWP)	19

Scheduling firmware upgrades for managed devices	19
Modifying the interface status with the CLI	20
SD-WAN with upgrade to 7.0	20
Citrix XenServer default limits and upgrade	20
Multi-step firmware upgrades	21
Hyper-V FortiManager-VM running on an AMD CPU	21
SSLv3 on FortiManager-VM64-AWS	21
Upgrade Information	22
Downgrading to previous firmware versions	22
Firmware image checksums	22
FortiManager VM firmware	23
SNMP MIB files	24
Product Integration and Support	25
Supported software	25
Web browsers	26
FortiOS and FortiOS Carrier	26
FortiADC	26
FortiAnalyzer	27
FortiAnalyzer-BigData	27
FortiAP	27
FortiAuthenticator	27
FortiCache	28
FortiCASB	28
FortiClient	28
FortiDDoS	28
FortiDeceptor	28
FortiFirewall and FortiFirewallCarrier	29
FortiMail	29
FortiPAM	29
FortiProxy	29
FortiSandbox	30
FortiSASE	30
FortiSOAR	30
FortiSRA	30
FortiSwitch	31
FortiTester	31
FortiToken	31
FortiWeb	31
Virtualization	31
Feature support	32
Language support	33
Supported models	34
FortiGate models	34
FortiGate special branch models	38
FortiCarrier models	40
FortiCarrier special branch models	42
FortiADC models	43

FortiAnalyzer models	44
FortiAnalyzer-BigData models	45
FortiAuthenticator models	45
FortiCache models	45
FortiDDoS models	46
FortiDeceptor models	46
FortiFirewall models	47
FortiFirewallCarrier models	48
FortiMail models	48
FortiPAM models	49
FortiProxy models	49
FortiSandbox models	50
FortiSOAR models	50
FortiSRA models	50
FortiTester models	51
FortiWeb models	51
FortiExtender MODEM firmware compatibility	52
Resolved issues	53
Device Manager	53
Others	53
Common Vulnerabilities and Exposures	53
Known issues	54
New known issues	54
Existing known issues	54
AP Manager	54
Device Manager	54
FortiSwitch Manager	55
Others	55
Policy and Objects	56
Services	56
Appendix A - FortiGuard Distribution Servers (FDS)	57
FortiGuard Center update support	57
Appendix B - Default and maximum number of ADOMs supported	59
Hardware models	59
Virtual Machines	59

Change Log

Date	Change Description
2026-01-27	Initial release.
2026-01-28	Updated Web browsers on page 26.
2026-02-05	Updated Supported models on page 7.
2026-02-09	Updated Known issues on page 54 and Special Notices on page 9.
2026-02-20	Updated FortiProxy on page 29.
2026-02-23	Updated Known issues on page 54

FortiManager 7.4.10 Release

This document provides information about FortiManager version 7.4.10 build 2778.



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 8](#)

Supported models

FortiManager version 7.4.10 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_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

Special branch supported models

The following models are released on a special branch of FortiManager 7.4.10. To confirm that you are running the correct build, run the CLI command `get system status` and check that the Branch point field shows 2778.

FMG-3750G	is released on build 6143.
------------------	----------------------------



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

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 23](#).

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

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.4.10.

Device database enters an incorrect state

In FortiManager 7.4.8 during the installation process of a configuration to a FortiGate device running in HA, the process may result in the inadvertent deletion of configuration settings. Although the root cause of the issue has been corrected in FortiManager 7.4.9 and later, upgrade by itself does not correct the database. Those upgrading from 7.4.8 may have been affected. For steps to correct, see support bulletin CSB-260116-1.

MEAs removed in FortiManager 7.4.8

As of FortiManager 7.4.8, there is no support for management extension applications (MEAs) in FortiManager.

New Admin Profile permission

In FortiManager 7.4.7, the following permission was added for Admin Profiles:

- *Firmware Upgrades* (device-fwm-profile): set permissions for device firmware profiles.

To review the default settings for this permission in predefined Admin Profiles, see the [FortiManager Administration Guide](#).

For existing custom Admin Profiles created prior to upgrading to FortiManager 7.4.7 or later, the new permission will be set to None. You must update this setting according to your needs in the custom Admin Profiles.

FortiSwitch 110G support

Pre-provisioning on FortiManager for the FortiSwitch 110G is unavailable, as this functionality might not yet be supported on the FortiOS. If this is the case, then it is recommended to perform FortiLink discovery on the FortiGate, retrieve the configuration to FortiManager, and import it into a template. If adding and managing a new switch from FortiManager without discovery/retrieve is required, an upgrade to an FortiOS version that supports pre-provisioning must be performed.

Unauthorized devices appearing in Device Manager despite having fgfm-deny-unknown enabled

Despite having the fgfm-deny-unknown setting enabled, unauthorized devices can still appear in the *Device Manager*.

This happens due to FDS request sent by FortiGate when FortiManager IP is configured under central management config. The fgfm connection will still be blocked as long fgfm-deny-unknown option is enabled. To prevent the devices to show up unauthorized for FDS request, following setting can be done on FortiManager.

```
config system admin setting
    set unreg_dev_opt ignore
end
```

New CLI option for managing FortiGate HA clusters

By default, FortiManager no longer installs HA-related configurations to FortiGate clusters unless explicitly configured to do so.

The following CLI option has been added in FortiManager 7.4.7:

```
config system dm
    set handle-nonhasync-config {enable | disable}
end
```

Previously, there was no CLI option like handle-nonhasync-config. This caused issues during installations to FortiGate HA clusters. For example, FortiManager could push FortiGate A's IP to FortiGate B, leading to partial or failed policy package (PP) installations.

Now, with the introduction of the handle-nonhasync-config CLI setting:

- Disabled (default): FortiManager will skip any configuration items marked as nonhasync when installing to the FortiGate. This avoids pushing HA-related or member-specific configurations that might break HA sync.
- Enabled: FortiManager will include nonhasync configuration items during installation, allowing updates to HA settings, vdom-exception configs, and other per-platform objects.

This change makes FortiManager behavior safer by default and gives admins more control over what gets pushed to HA clusters.

Adding VM devices to FortiManager

As of FortiManager 7.4.7, connection between VM devices and FortiManager is restricted for security. By default, FortiManager will not allow VM platform connection in FGFM.

This applies to the following products:

- FortiGate-VM
- FortiCarrier-VM
- FortiProxy-VM
- FortiFirewall-VM

When upgrading from an earlier version of FortiManager, VM devices already managed by FortiManager will continue to be supported without interruption, but you must enable `fgfm-allow-vm` in global settings before adding additional VM devices.

To allow VM platform connection in FGFM, enter the following command in the FortiManager CLI:

```
config system global
    set fgfm-allow-vm enable
end
```

The system interface speed is read-only in FortiManager

The default value for `system interface speed` in FortiOS depends on the FortiGate platform, specified interface, and config. This attribute is read-only in FortiManager, and can only be edited in the FortiGate.

Custom certificate name verification for FortiGate connection



In FortiManager 7.4.6, the `fgfm-peercert-withoutsan` setting has been removed, so there is no method to disable this verification. The FortiGate certificate must contain the FortiGate serial number in either the CN or SAN.

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.

The names of policies derived from policy blocks no longer automatically include the policy block name

Previously, when a policy was derived from a "policy block," its name was automatically prefixed with the policy block name, ensuring unique names but sometimes exceeding the 35-character limit in the policy package. To address this, the renaming behavior has been removed, and policies now retain their original names without policy block prefixes, avoiding the character limit issue.

After the fix, FortiManager may encounter duplicate policy names if multiple policy blocks previously contained policies with the same base name. Since FortiManager requires unique policy names for proper management, this duplication can break the installation or functionality of policies. To resolve this, customers may need to manually identify and rename all conflicting policies after upgrading.

Upgrading from 7.4.3 to 7.4.8 with FIPS mode enabled

When FIPS mode is enabled, upgrading from 7.4.3 to 7.4.8 might fail due to the following error message: "FIPS firmware signature verification failed". The following steps should be taken as workaround:

1. Backup FortiManager-v7.4.3-fips-cc mode DB.
2. Disable FortiManager-v7.4.3-fips mode to normal mode.
3. Upgrade FortiManager-v7.4.3 normal mode to v7.4.8.
4. FortiManager-v7.4.8 enable fips-cc mode.
5. Restore FortiManager-v7.4.3-fips DB on FortiManager-v7.4.8-fips.

Note that you do not need to follow this workaround if upgrading from 7.4.4 or later to 7.4.8.

Device blueprint header

The device blueprint header is updated in FortiManager 7.4.4, and the new format is required when importing model devices from a CSV file. If you have existing CSV files that are used as a template to import model devices, the header must be updated to use the new format.

To update the header for an existing CSV file:

1. In the FortiManager 7.4.4 or later GUI, go to *Device Manager > Device & Groups*.
2. From the *Add Device* dropdown, select *Device Blueprint*.
3. Select an existing blueprint and click *Generate CSV*.
4. Open the new CSV file and copy the header.
5. Open the existing CSV file and paste the new header, replacing the old header from previous versions.

Shell access has been removed

As of FortiManager 7.4.4, 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
```

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.

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 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 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.

Apache-mode changed from prefork to event

Before version 7.4.0, the default "apache-mode" utilized the "prefork" mode. However, starting from version 7.4.1, the default configuration switches to the "event" mode.

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

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

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

FortiGuard web filtering category v10 update

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

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

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

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

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 =
        FL3K5E3M1500074, 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.

Default GUI theme changed

As of FortiManager 7.4.1, the default GUI theme is *Jade*. The default theme can be changed from *System Settings > Settings*.

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.

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*.

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, 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 7.2 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 22](#)
- [Firmware image checksums on page 22](#)
- [FortiManager VM firmware on page 23](#)
- [SNMP MIB files on page 24](#)

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
```

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.

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 7.4.10 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 25](#)
- [Feature support on page 32](#)
- [Language support on page 33](#)
- [Supported models on page 34](#)
- [FortiExtender MODEM firmware compatibility on page 52](#)

Supported software

FortiManager 7.4.10 supports the following software:

- [Web browsers on page 26](#)
- [FortiOS and FortiOS Carrier on page 26](#)
- [FortiADC on page 26](#)
- [FortiAnalyzer on page 27](#)
- [FortiAnalyzer-BigData on page 27](#)
- [FortiAP on page 27](#)
- [FortiAuthenticator on page 27](#)
- [FortiCache on page 28](#)
- [FortiCASB on page 28](#)
- [FortiClient on page 28](#)
- [FortiDDoS on page 28](#)
- [FortiDeceptor on page 28](#)
- [FortiFirewall and FortiFirewallCarrier on page 29](#)
- [FortiMail on page 29](#)
- [FortiPAM on page 29](#)
- [FortiProxy on page 29](#)
- [FortiSandbox on page 30](#)
- [FortiSASE on page 30](#)
- [FortiSOAR on page 30](#)
- [FortiSRA on page 30](#)
- [FortiSwitch on page 31](#)
- [FortiTester on page 31](#)

- [FortiToken on page 31](#)
- [FortiWeb on page 31](#)
- [Virtualization on page 31](#)



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 7.4.10 supports the following web browsers:

- Google Chrome version 144
- Microsoft Edge version 144
- Mozilla Firefox 147

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 7.4.10 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 7.4.10 supports the following versions of FortiOS and FortiOS Carrier:

- 7.4.0 to 7.4.11
- 7.2.0 to 7.2.13
- 7.0.0 to 7.0.19

FortiADC

FortiManager 7.4.10 supports the following versions of FortiADC:

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

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

FortiAnalyzer

FortiManager 7.4.10 supports the following versions of FortiAnalyzer:

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

FortiAnalyzer-BigData

FortiManager 7.4.10 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAP

FortiAP devices are controlled by the FortiGate devices managed by FortiManager. Thus, support for FortiAP firmware is dependent on supported FortiOS versions.

For FortiManager compatibility with FortiOS, see [FortiOS and FortiOS Carrier](#).

For FortiOS compatibility with FortiAP, see the [FortiAP and FortiOS Compatibility Matrix](#).

FortiAuthenticator

FortiManager 7.4.10 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
- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later

FortiCache

FortiManager 7.4.10 supports the following versions of FortiCache:

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

FortiCASB

FortiManager 7.4.10 supports the following versions of FortiCASB:

- 23.2.0 and later

FortiClient

FortiManager 7.4.10 supports the following versions of FortiClient:

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

FortiDDoS

FortiManager 7.4.10 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
- 5.7.0 and later
- 5.6.0 and later

Limited support. For more information, see [Feature support on page 32](#).

FortiDeceptor

FortiManager 7.4.10 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 7.4.10 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 7.4.10 supports the following versions of FortiMail:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiPAM

FortiManager 7.4.10 supports the following versions of FortiPAM:

- 1.8.0 and later
- 1.7.0 and later
- 1.6.0 and later
- 1.5.0 and later
- 1.4.0 and later
- 1.3.0 and later
- 1.2.0 and later
- 1.1.0 and later
- 1.0.0 and later

FortiProxy

FortiManager 7.4.10 supports configuration management for the following versions of FortiProxy:

- 7.4.0 to 7.4.13
- 7.2.2, 7.2.3, 7.2.7, and 7.2.9 to 7.2.13
- 7.0.7 to 7.0.21



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 32](#).

FortiManager 7.4.10 supports logs from the following versions of FortiProxy:

- 7.4.0 to 7.4.13
- 7.2.0 to 7.2.15
- 7.0.0 to 7.0.22
- 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 7.4.10 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

For more information about compatibility, see the [FortiSASE Release Notes](#).

FortiSOAR

FortiManager 7.4.10 supports the following versions of FortiSOAR:

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

FortiSRA

FortiManager 7.4.10 supports the following versions of FortiSRA:

- 1.1.0 and later
- 1.0.0 and later

FortiSwitch

FortiSwitch devices are controlled by the FortiGate devices managed by FortiManager. Thus, support for FortiSwitchOS is dependent on supported FortiOS versions.

For FortiManager compatibility with FortiOS, see [FortiOS and FortiOS Carrier on page 26](#).

For FortiOS Compatibility with FortiSwitchOS, see [FortiLink Compatibility](#).

FortiTester

FortiManager 7.4.10 supports the following versions of FortiTester:

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

FortiToken

FortiManager 7.4.10 supports the following versions of FortiToken:

- 3.0.0 and later

FortiWeb

FortiManager 7.4.10 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.4.10 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 8.2 and later
- 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	Configuration Management	Firmware Management	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓	✓
FortiADC			✓	✓		
FortiAnalyzer				✓	✓	✓
FortiAP	✓*	✓				
FortiAuthenticator						✓
FortiCache				✓	✓	✓
FortiClient			✓		✓	✓
FortiDDoS				✓	✓	✓
FortiDeceptor			✓			
FortiExtender	✓*	✓				
FortiFirewall	✓					✓
FortiFirewall Carrier	✓					✓
FortiMail			✓	✓	✓	✓

Platform	Configuration Management	Firmware Management	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiProxy	✓	✓**	✓	✓	✓	✓
FortiSandbox			✓	✓	✓	✓
FortiSOAR			✓	✓		
FortiSwitch	✓*	✓				
FortiTester			✓			
FortiWeb			✓	✓	✓	✓
Syslog						✓

*FortiManager can push FortiAP, FortiSwitch, and FortiExtender configuration to FortiGate. FortiGate then manages the FortiAP, FortiSwitch, or FortiExtender; they will not be directly managed by FortiManager.

**Only upgrades performed directly on an individual device from *Device Manager* are supported. Firmware management templates are not supported for these devices.

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, FortiWeb, FortiCache, FortiProxy, FortiAuthenticator, and other Fortinet product models and firmware versions can be managed by a FortiManager or send logs to a FortiManager running version 7.4.10.



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 34](#)
- [FortiGate special branch models on page 38](#)
- [FortiCarrier models on page 40](#)
- [FortiCarrier special branch models on page 42](#)
- [FortiADC models on page 43](#)
- [FortiAnalyzer models on page 44](#)
- [FortiAnalyzer-BigData models on page 45](#)
- [FortiAuthenticator models on page 45](#)
- [FortiCache models on page 45](#)
- [FortiDDoS models on page 46](#)
- [FortiDeceptor models on page 46](#)
- [FortiFirewall models on page 47](#)
- [FortiFirewallCarrier models on page 48](#)
- [FortiMail models on page 48](#)
- [FortiPAM models on page 49](#)
- [FortiProxy models on page 49](#)
- [FortiSandbox models on page 50](#)
- [FortiSOAR models on page 50](#)
- [FortiSRA models on page 50](#)
- [FortiTester models on page 51](#)
- [FortiWeb models on page 51](#)

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 38](#).

Model	Firmware Version
FortiGate: FortiGate-30G, FortiGate-31G, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, 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-90G, FortiGate-91E, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-200G, FortiGate-201E, FortiGate-201F, FortiGate-201G, 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-700G, FortiGate-701G, 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-4801F-NEBS 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 FortiGate DC: FortiGate-400F-DC, FortiGate-401F-DC, FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-900G-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, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS	7.4

Model	Firmware Version
FortiWiFi: FWF-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-DSL, FWF-50G-SFP, FWF-51G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-70G, FWF-70G-POE, FWF-71G, 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-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G, FGR-70G, FGR-70G-5G-Dual	
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-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, 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-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-4801F-NEBS	7.2
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	

Model	Firmware Version
FortiGate DC: FortiGate-400F-DC, FortiGate-401F-DC, FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-900G-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, FortiGate-4801F-DC-NEBS FortiWiFi: FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-70G, FWF-71G, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, 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-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-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	7.0

Model	Firmware Version
FortiGate DC: FortiGate-400F-DC, FortiGate-401F-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-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	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.4.10 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 34](#).

FortiOS 7.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-70G-POE-5G, FortiGate-71G-POE-5G	7.4.8	6345
FortiGate-3800G	7.4.8	6564
FortiGate-3801G	7.4.8	6438
FortiGateRugged-60G	7.4.8	6300
FortiGateRugged-70G-5G	7.4.8	6340

FortiOS 7.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-30G, FortiGate-31G	7.2.12	6666
FortiGate-70G, FortiGate-70G-POE	7.2.12	6659
FortiGate-71G	7.2.11	6570
FortiGate-71G-POE	7.2.11	6559
FortiGate-200G, FortiGate-201G	7.2.12	6660
FortiGate-700G, FortiGate-701G	7.2.11	6531
FortiWiFi-30G, FortiWiFi-31G	7.2.12	6662
FortiWiFi-70G, FortiWiFi-70G-POE FortiWiFi-71G	7.2.11	6566

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE	7.0.17	7592
FortiGate-80F-DSL	7.0.17	7558
FortiGate-90G, FortiGate-91G	7.0.17	7558
FortiGate-120G, FortiGate-121G	7.0.16	7534
FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC	7.0.17	7551
FortiGate-1000F, FortiGate-1001F	7.0.17	7552
FortiGate-3200F, FortiGate-3201F	7.0.17	7553
FortiGate-3700F, FortiGate-3701F	7.0.17	7553
FortiGate-4800F, FortiGate-4800F-DC FortiGate-4801F, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS, FortiGate- 4801F-NEBS	7.0.17	7553
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.16	0280

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.16	0280
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.16	0280
FortiGateRugged-50G-5G	7.0.17	7577
FortiGateRugged-70F, FortiGateRugged-70F-3G4G	7.0.17	7557
FortiGateRugged-70G	7.0.15	7496
FortiGateRugged-70G-5G-Dual	7.0.16	7550
FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP	7.0.17	7592
FortiWiFi-51G	7.0.17	7592
FortiWiFi-51G-5G	7.0.17	7537
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL	7.0.17	7558

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 42](#).

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-4801F-NEBS 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	7.4

Model	Firmware Version
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-4801F-DC, FortiCarrier-4801F-DC-NEBS 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	
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-4801F-NEBS 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-4801F-DC, FortiCarrier-4801F-DC-NEBS 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	7.2

Model	Firmware Version
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, 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 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-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	7.0

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.4.10 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 40](#).

FortiCarrier 7.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3800G	7.4.8	6564
FortiCarrier-3801G	7.4.8	6438

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.17	7553
FortiCarrier-3700F, FortiCarrier-3701F	7.0.17	7553
FortiCarrier-4800F, FortiCarrier-4800F-DC	7.0.17	7553

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-4801F, FortiCarrier-4801F-DC, FortiCarrier-4801F-DC-NEBS, FortiCarrier-4801F-NEBS		
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.16	0280
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.16	0280
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.16	0280

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-420F, 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-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-VM, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVR	7.4
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-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-VM, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVR	6.2, 7.0, 7.1, 7.2

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-VM, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVEN	6.0, 6.1

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-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-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	7.0

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

FortiAnalyzer-BigData models

Model	Firmware Version
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500G	7.4
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F, FortiAnalyzer-BigData-4500G FortiAnalyzer-BigData VM: FortiAnalyzer-BigData-VM64	7.2
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F, FortiAnalyzer-BigData-4500G 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, 6.6
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	6.0, 6.1, 6.2, 6.3

FortiCache models

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

Model	Firmware Version
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-1500G, FortiDDoS-1500G-LR, FortiDDoS-2000F, FortiDDoS-2000G, FortiDDoS-3000F, FortiDDoS-3000G 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
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.6, 5.7

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, 6.0
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 7.4.10 supports these models on the identified FortiFirewall firmware version and build number.

FortiFirewall 7.4

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

FortiFirewall 7.2

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

FortiFirewall 7.0

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

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.4.10 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version
FortiFirewallCarrier: FortiFirewallCarrier-1801F, FortiFirewallCarrier-2600F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS, FortiFirewallCarrier-4801F-DC-NEBS 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, FortiFirewallCarrier-4801F-NEBS, FortiFirewallCarrier-4801F-DC-NEBS FortiFirewallCarrier DC: FortiFirewallCarrier-4200F-DC FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.2
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, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCF, FML-VM-XEN, FortiMail Cloud	7.4

Model	Firmware Version
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, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCF, FML-VM-XEN, 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, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCF, FML-VM-XEN, 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, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCF, FML-VM-XEN, FortiMail Cloud	6.2, 6.4

FortiPAM models

Model	Firmware Version
FortiPAM: FortiPAM-100G, FortiPAM-400G, FortiPAM-1100G, FortiPAM-3100G	1.8
FortiPAM: FortiPAM-1000G, FortiPAM-3000G FortiPAM VM: FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1, 1.2, 1.3, 1.4

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-OPC, FortiProxy-VM64	7.4
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	7.2
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-OPC, FortiProxy-VM64	7.0

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E	1.0, 1.1, 1.2, 2.0
FortiProxy VM: FortiProxy-KVM, FortiProxy-VM64	

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	4.2, 4.4
FortiSandbox DC: FSA-1000F-DC	
FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D	4.0
FortiSandbox DC: FSA-1000F-DC	
FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	3.2
FortiSandbox DC: FSA-1000F-DC	
FortiSandbox-VM: FortiSandbox-AWS, FSA-VM	

FortiSOAR models

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

FortiSRA models

Model	Firmware Version
FortiSRA: FortiSRA-1000G, FortiSRA-3000G	1.0, 1.1
FortiSRA-VM: FortiSRA-Azure, FortiSRA-HyperV, FortiSRA-KVM, FortiSRA-VM64	

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-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer FortiWeb Cloud , including FortiAppSec Cloud.	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-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer FortiWeb Cloud , including FortiAppSec Cloud.	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-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer FortiWeb Cloud , including FortiAppSec Cloud.	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.

Resolved issues

The following issues have been fixed in 7.4.10. To inquire about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
1246821	FMG retrieve may fail when an admins remote-group exists only in the root VDOM and the VDOM order starts with a non-root VDOM, causing invalid reference detection during device addition.

Others

Bug ID	Description
1247597	FortiManager is unable to sync user information from the pxGrid connector.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1247736	FortiManager 7.4.10 is no longer vulnerable to the following CVE Reference: • CVE-2026-24858

Known issues

Known issues are organized into the following categories:

- [New known issues](#)
- [Existing known issues](#)

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 7.4.10.

Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.4.10.

AP Manager

Bug ID	Description
1032762	Since FortiOS 7.4.4 now supports the selection of multiple 802.11 protocols and has trimmed the band options, importing FortiOS 7.4.3 AP profiles may result in some bands and channels being un-matched or unset.

Device Manager

Bug ID	Description
974925	The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FortiOS version lower than 7.4.2. Workaround: Edit NTP server setting under CLI configuration.
1015138	Unable to edit interface with dhcp reservation.

Bug ID	Description
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1112389	FortiView & LogView fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager.
1215090	Unable to retrieve correct setting of device-identification in system interface.

FortiSwitch Manager

Bug ID	Description
1227473	FortiManager attempts to install set poe-status disable on FSW ports that already have PoE disabled. The issue persists and reoccurs after configuration installation and synchronization.

Others

Bug ID	Description
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: <pre>config webfilter profile edit "g-default" config web unset urlfilter-table end next end</pre>
1217534	During an upgrade of an FortiGate-HA cluster via FortiManager, if the disk-check feature is enabled, it may cause all cluster members to reboot simultaneously. This can result in an unexpected traffic interruption. Workaround: To prevent this issue, disable the disk check before performing the upgrade:

Bug ID	Description
	<pre>config fmupdate fwm-setting set check-fgt-disk disable end</pre>

Policy and Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
1199272	Imported certificate does not show details.
1217455	FortiManager is not able to retrieve "usergroup" from "Cisco 3.3 Path7 Pxgrid" using FortiManager connector. Workaround: Add the appropriate DNS entry under System Settings Network.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.
1242707	Policy package status does not change to "Out of Sync" on FortiManager when local changes are made on FortiGate.

Services

Bug ID	Description
1167362	Despite having the "fgfm-deny-unknown" setting enabled, unauthorized devices might still be appearing in the <i>Device Manager</i> . For more details, see Special Notices on page 9 .

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	VM License Activation
FortiGate	✓	✓	✓
FortiADC	✓		✓
FortiCache	✓		✓
FortiCarrier	✓	✓	✓
FortiClient	✓		
FortiDeceptor	✓	✓	✓
FortiDDoS	✓		✓
FortiEMS	✓		
FortiMail	✓	✓	✓
FortiPAM	✓		✓
FortiProxy	✓	✓	✓
FortiSandbox	✓	✓	✓
FortiSOAR	✓		
FortiSRA	✓		✓
FortiTester	✓		✓

Platform	Update Service	Query Service	VM License Activation
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© 2026 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.