

Release Notes

FortiManager 7.4.7



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 9, 2026

FortiManager 7.4.7 Release Notes

02-747-1152859-20260209

TABLE OF CONTENTS

Change Log	7
FortiManager 7.4.7 Release	9
Supported models	9
FortiManager VM subscription license	9
Management extension applications	10
Supported models for MEA	10
Minimum system requirements	10
Special Notices	12
FortiManager and FortiClient EMS compatibility	12
New Admin Profile permission	12
FortiAP support in 7.2 and 7.4 ADOMs	12
FortiSwitch 110G support	12
Unauthorized devices appearing in Device Manager despite having fgfm-deny-unknown enabled	13
New CLI option for managing FortiGate HA clusters	13
MEAs removed in FortiManager 7.4.7	14
Adding VM devices to FortiManager	14
The system interface speed is read-only in FortiManager	14
Custom certificate name verification for FortiGate connection	15
The names of policies derived from policy blocks no longer automatically include the policy block name	15
Upgrading from 7.4.3 to 7.4.7 with FIPS mode enabled	16
Device blueprint header	16
Shell access has been removed	16
Enable fcp-cfg-service for Backup Mode ADOMs	17
System Templates include new fields	17
Additional configuration required for SSO users	17
When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade	17
Apache-mode changed from prefork to event	18
FortiGuard web filtering category v10 update	18
FortiManager 7.2.3 and later firmware on FortiGuard	19
Configuration backup requires a password	19
FortiManager-400E support	19
Serial console has changed for FortiManager deployments on Xen	20
OpenXen in PV mode is not supported in FortiManager 7.4.1	20
Default GUI theme changed	20
Option to enable permission check when copying policies	21
Management Extensions visibility in the GUI	21
Install On column for policies	21
SD-WAN Orchestrator removed in 7.2	21
Changes to FortiManager meta fields	21

Setup wizard requires FortiCare registration	22
Access lists as ADOM-level objects	22
View Mode is disabled in policies when policy blocks are used	22
Reconfiguring Virtual Wire Pairs (VWP)	22
Scheduling firmware upgrades for managed devices	23
Modifying the interface status with the CLI	23
SD-WAN with upgrade to 7.0	23
Citrix XenServer default limits and upgrade	23
Multi-step firmware upgrades	24
Hyper-V FortiManager-VM running on an AMD CPU	24
SSLv3 on FortiManager-VM64-AWS	24
Upgrade Information	25
Downgrading to previous firmware versions	25
Firmware image checksums	25
FortiManager VM firmware	26
SNMP MIB files	27
Product Integration and Support	28
Supported software	28
Web browsers	29
FortiOS and FortiOS Carrier	29
FortiADC	29
FortiAnalyzer	30
FortiAnalyzer-BigData	30
FortiAP	30
FortiAuthenticator	30
FortiCache	31
FortiCASB	31
FortiClient	31
FortiDDoS	31
FortiDeceptor	31
FortiFirewall and FortiFirewallCarrier	32
FortiMail	32
FortiPAM	32
FortiProxy	32
FortiSandbox	33
FortiSASE	33
FortiSOAR	33
FortiSRA	33
FortiSwitch	34
FortiTester	34
FortiToken	34
FortiWeb	34
Virtualization	34
Feature support	35
Language support	36
Supported models	37

FortiGate models	37
FortiGate special branch models	41
FortiCarrier models	43
FortiCarrier special branch models	45
FortiADC models	45
FortiAnalyzer models	46
FortiAnalyzer-BigData models	47
FortiAuthenticator models	47
FortiCache models	48
FortiDDoS models	48
FortiDeceptor models	48
FortiFirewall models	49
FortiFirewallCarrier models	50
FortiMail models	50
FortiPAM models	51
FortiProxy models	51
FortiSandbox models	52
FortiSOAR models	52
FortiSRA models	52
FortiTester models	52
FortiWeb models	53
FortiExtender MODEM firmware compatibility	54
Compatibility with FortiOS Versions	55
FortiManager 7.4.7 and FortiOS 7.2.12 compatibility issues	55
FortiManager 7.4.7 and FortiOS 7.4.9 compatibility issues	56
Resolved issues	58
AP Manager	58
Device Manager	58
FortiSwitch Manager	61
Others	61
Policy and Objects	63
Script	65
Services	65
System Settings	66
VPN Manager	66
Common Vulnerabilities and Exposures	67
Known issues	68
New known issues	68
AP Manager	68
Device Manager	68
FortiSwitch Manager	69
Others	69
Policy & Objects	70
Services	70
System Settings	71
VPN Manager	71
Existing known issues	71

AP Manager	71
Device Manager	71
Global ADOM	72
Others	72
Policy & Objects	73
Services	74
Appendix A - FortiGuard Distribution Servers (FDS)	75
FortiGuard Center update support	75
Appendix B - Default and maximum number of ADOMs supported	77
Hardware models	77
Virtual Machines	77

Change Log

Date	Change Description
2025-05-28	Initial release.
2025-05-29	Updated Resolved issues on page 58 and Known issues on page 68 .
2025-05-30	Updated Resolved issues on page 58 .
2025-06-11	Updated Known issues on page 68 .
2025-06-16	Updated Resolved issues on page 58 .
2025-06-19	Updated Known issues on page 68 .
2025-06-23	Updated Known issues on page 68 .
2025-06-24	Added "Unauthorized devices appearing in Device Manager despite having fgfm-deny-unknown enabled" to Special Notices on page 12 . Updated Resolved issues on page 58 . Updated Known issues on page 68 .
2025-06-25	Updated FortiGate special branch models on page 41 .
2025-06-26	Updated Resolved issues on page 58 . Updated Known issues on page 68 .
2025-07-08	Updated Resolved issues on page 58 .
2025-07-09	Updated Special Notices on page 12 and Known issues on page 68 .
2025-07-10	Added FortiAP on page 30 . Updated FortiSwitch on page 34 . Updated Known issues on page 68 .
2025-07-14	Updated Known issues on page 68 .
2025-07-15	Updated Known issues on page 68 .
2025-07-21	Updated Resolved issues on page 58 and Known issues on page 68 . Updated FortiGate special branch models on page 41 .
2025-07-28	Updated Known issues on page 68 .
2025-08-07	Updated Resolved issues on page 58 and Known issues on page 68 .
2025-08-13	Updated Resolved issues on page 58 .
2025-08-14	Added FortiSwitch 110G support to Special Notices on page 12 .
2025-08-20	Updated Known issues on page 68 .
2025-08-25	Updated Feature support on page 35 .

Date	Change Description
2025-09-03	Added "Apache-mode changed from prefork to event" to Special Notices on page 12 . Updated Web browsers on page 29 .
2025-09-08	Updated Known issues on page 68 .
2025-09-10	Updated Known issues on page 68 . Added FortiManager 7.4.7 and FortiOS 7.2.12 compatibility issues on page 55 .
2025-09-12	Updated Resolved issues on page 58 .
2025-09-16	Updated Resolved issues on page 58 and Known issues on page 68 .
2025-09-19	Updated Known issues on page 68 .
2025-09-26	Updated Known issues on page 68 .
2025-09-29	Added FortiManager 7.4.7 and FortiOS 7.4.9 compatibility issues on page 56 . Added "FortiAP support in 7.2 and 7.4 ADOMs" to Special Notices on page 12 .
2025-10-02	Updated Known issues on page 68 .
2025-10-24	Updated Known issues on page 68 .
2025-10-31	Updated Known issues on page 68 .
2025-12-09	Updated Resolved issues on page 58 .
2025-12-11	Updated Special Notices on page 12 .
2025-12-19	Updated Special Notices on page 12 .
2025-02-09	Updated Known issues on page 68 .

FortiManager 7.4.7 Release

This document provides information about FortiManager version 7.4.7 build 2685.



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 9](#)
- [FortiManager VM subscription license on page 9](#)
- [Management extension applications on page 10](#)

Supported models

FortiManager version 7.4.7 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).



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 26](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 77](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.4.7.



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

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

Supported models for MEA

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

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

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

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

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA.

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
FortiSigConverter	<ul style="list-style-type: none">• 4 vCPU• 8 GB RAM
Universal Connector	<ul style="list-style-type: none">• 1 GHZ vCPU• 2 GB RAM• 1 GB disk storage

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.4.7.

FortiManager and FortiClient EMS compatibility

In FortiClient EMS 7.4.5, the communication protocol has been upgraded from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, HTTP/2 does not return a traditional "200 OK" text response, so previous versions of FortiManager that expect this format cannot interpret the new HTTP/2 replies. Because of this, versions prior to FortiManager 7.4.9 and 7.6.5 are not compatible with the EMS version 7.4.5 and later.

New Admin Profile permission

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

- *Firmware Upgrades (device-fw-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.

FortiAP support in 7.2 and 7.4 ADOMs

In FortiOS 7.4.4, the available radio band format options used in FortiAP configurations has changed. This updated syntax is reflected in FortiManager 7.4.3 and later in version 7.4 ADOMs. As a result of this syntax difference, FortiManager 7.4.3 and later does not support installing FortiAP profile configurations from a 7.4 ADOM to a 7.2 FortiAP device (downgrade installation), or configurations from a 7.2 ADOM on a 7.4 FortiAP device (upgrade installation).

FortiSwitch 110G support

Pre-provisioning on FortiManager for the FortiSwitch 110G is unavailable, as this functionality might not yet 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.

MEAs removed in FortiManager 7.4.7

The following management extension applications (MEAs) are removed in FortiManager 7.4.7:

- FortiAIOps
- FortiSOAR
- Policy Analyzer
- Wireless Manager (FortiWLM)

The following MEAs are still supported in FortiManager 7.4.7:

- FortiSigConverter
- Universal Connector

For more information about the supported MEAs, see [Management extension applications on page 10](#).

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-withoutsn` 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 7.4.7 with FIPS mode enabled

When FIPS mode is enabled, upgrading from 7.4.3 to 7.4.7 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 v7.4.7.
4. FortiManager-v7.4.7 enable fips-cc mode.
5. Restore FortiManager-v7.4.3-fips DB on FortiManager-v7.4.7-fips.

Note that you do not need to follow this workaround if upgrading from 7.4.4, 7.4.5, or 7.4.6 to 7.4.7.

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 =
        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.

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.

Management Extensions visibility in the GUI

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

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 25](#)
- [Firmware image checksums on page 25](#)
- [FortiManager VM firmware on page 26](#)
- [SNMP MIB files on page 27](#)

Downgrading to previous firmware versions

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

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

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, go to *Download > Firmware Image Checksums*,

enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Google Cloud Platform

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

Linux KVM

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

Microsoft Azure

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

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

Microsoft Hyper-V Server

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

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



Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

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

VMware ESX/ESXi

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



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 7.4.7 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 28](#)
- [Feature support on page 35](#)
- [Language support on page 36](#)
- [Supported models on page 37](#)
- [FortiExtender MODEM firmware compatibility on page 54](#)

Supported software

FortiManager 7.4.7 supports the following software:

- [Web browsers on page 29](#)
- [FortiOS and FortiOS Carrier on page 29](#)
- [FortiADC on page 29](#)
- [FortiAnalyzer on page 30](#)
- [FortiAnalyzer-BigData on page 30](#)
- [FortiAP on page 30](#)
- [FortiAuthenticator on page 30](#)
- [FortiCache on page 31](#)
- [FortiCASB on page 31](#)
- [FortiClient on page 31](#)
- [FortiDDoS on page 31](#)
- [FortiDeceptor on page 31](#)
- [FortiFirewall and FortiFirewallCarrier on page 32](#)
- [FortiMail on page 32](#)
- [FortiPAM on page 32](#)
- [FortiProxy on page 32](#)
- [FortiSandbox on page 33](#)
- [FortiSASE on page 33](#)
- [FortiSOAR on page 33](#)
- [FortiSRA on page 33](#)
- [FortiSwitch on page 34](#)
- [FortiTester on page 34](#)

- [FortiToken on page 34](#)
- [FortiWeb on page 34](#)
- [Virtualization on page 34](#)



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 7.4.7 supports the following web browsers:

- Google Chrome version 139.0.7258.155
- Microsoft Edge version 139.0.3405.119
- Mozilla Firefox 142.0.1

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 7.4.7 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 7.4.7 supports the following versions of FortiOS and FortiOS Carrier:

- 7.4.0 to 7.4.9
- 7.2.0 to 7.2.11
- 7.0.0 to 7.0.17



Some FortiOS versions are supported with compatibility issues. For more details, see [Compatibility with FortiOS Versions on page 55](#).

FortiADC

FortiManager 7.4.7 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 7.4.7 supports the following versions of FortiAnalyzer:

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

FortiAnalyzer-BigData

FortiManager 7.4.7 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 7.4.7 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 7.4.7 supports the following versions of FortiCache:

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

FortiCASB

FortiManager 7.4.7 supports the following versions of FortiCASB:

- 23.2.0 and later

FortiClient

FortiManager 7.4.7 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 7.4.7 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 35](#).

FortiDeceptor

FortiManager 7.4.7 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 7.4.7 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 7.4.7 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 7.4.7 supports the following versions of FortiPAM:

- 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 7.4.7 supports configuration management for the following versions of FortiProxy:

- 7.4.0 to 7.4.9
- 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 35](#).

FortiManager 7.4.7 supports logs from the following versions of FortiProxy:

- 7.4.0 to 7.4.9
- 7.2.0 to 7.2.13
- 7.0.0 to 7.0.21
- 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 7.4.7 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

The FortiSASE connector is only supported on FortiManager VM platforms, not FortiManager hardware models.

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

FortiSOAR

FortiManager 7.4.7 supports the following versions of FortiSOAR:

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

FortiSRA

FortiManager 7.4.7 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 29](#).

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

FortiTester

FortiManager 7.4.7 supports the following versions of FortiTester:

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

FortiToken

FortiManager 7.4.7 supports the following versions of FortiToken:

- 3.0.0 and later

FortiWeb

FortiManager 7.4.7 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.4.7 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 7.4.7.



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 37](#)
- [FortiGate special branch models on page 41](#)
- [FortiCarrier models on page 43](#)
- [FortiCarrier special branch models on page 45](#)
- [FortiADC models on page 45](#)
- [FortiAnalyzer models on page 46](#)
- [FortiAnalyzer-BigData models on page 47](#)
- [FortiAuthenticator models on page 47](#)
- [FortiCache models on page 48](#)
- [FortiDDoS models on page 48](#)
- [FortiDeceptor models on page 48](#)
- [FortiFirewall models on page 49](#)
- [FortiFirewallCarrier models on page 50](#)
- [FortiMail models on page 50](#)
- [FortiPAM models on page 51](#)
- [FortiProxy models on page 51](#)
- [FortiSandbox models on page 52](#)
- [FortiSOAR models on page 52](#)
- [FortiSRA models on page 52](#)
- [FortiTester models on page 52](#)
- [FortiWeb models on page 53](#)

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 41](#).

Model	Firmware Version
<p>FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-51G, 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-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-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</p> <p>FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1</p> <p>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</p> <p>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</p> <p>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</p> <p>FortiWiFi: FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-DSL, FWF-50G-SFP, 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</p>	7.4

Model	Firmware Version
<p>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</p>	
<p>FortiGate Rugged: FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G</p>	
<p>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</p> <p>FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1</p> <p>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</p> <p>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</p> <p>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</p>	7.2

Model	Firmware Version
<p>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</p> <p>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</p> <p>FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen</p> <p>FortiGate Rugged: FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G</p>	
<p>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,</p> <p>FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p>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</p> <p>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</p>	7.0

Model	Firmware Version
FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager	
FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen	
FortiGate Rugged: FGR-60F, FGR-60F-3G4G	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.4.7 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 37](#).

FortiOS 7.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-30G, FortiGate-31G	7.4.8	5164
FortiGate-70G, FortiGate-71G FortiGate-70G-POE, FortiGate-71G-POE FortiGate-70G-POE-5G, FortiGate-71G-POE-5G	7.4.8	6345
FortiGateRugged-50G-5G	7.4.8	6345

FortiOS 7.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-30G, FortiGate-31G	7.2.11	6542
FortiGate-70G, FortiGate-71G	7.2.11	6570
FortiGate-70G-POE, FortiGate-71G-POE	7.2.11	6559
FortiGate-200G, FortiGate-201G	7.2.11	6561
FortiGate-700G, FortiGate-701G	7.2.11	6531
FortiWiFi-30G, FortiWiFi-31G	7.2.11	6534
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	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-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

FortiGate Model	FortiOS Version	FortiOS Build
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 45](#).

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

Model	Firmware Version
<p>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</p> <p>FortiCarrier 5000 Series: FortiCarrier-5001E, FortiCarrier-5001E1</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p>	7.2
<p>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</p> <p>FortiCarrier 5000 Series: FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p>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</p> <p>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</p>	7.0

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.4.7 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 43](#).

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 FortiCarrier-4801F, FortiCarrier-4801F-DC	7.0.17	7553
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	7.4

Model	Firmware Version
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-XENSERVER	
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	6.2, 7.0, 7.1, 7.2
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-XENSERVER	
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	6.0, 6.1
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-XENSERVER	

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	7.4
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	
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	7.2

Model	Firmware Version
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	
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
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
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
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 7.4.7 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-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC	7.4
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	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 7.4.7 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-OCP, 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-OCP, 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-OCP, 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-OCP, FML-VM-XEN, FortiMail Cloud	6.2, 6.4

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, 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
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

FortiSRA models

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

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F	7.3

Model	Firmware Version
<p>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</p>	
<p>FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F</p> <p>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</p>	7.2
<p>FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F</p> <p>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</p>	7.1

FortiWeb models

Model	Firmware Version
<p>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</p> <p>FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p>FortiWeb Cloud, including FortiAppSec Cloud.</p>	7.4
<p>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</p>	7.2

Model	Firmware Version
<p>FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p>FortiWeb Cloud, including FortiAppSec Cloud.</p>	
<p>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</p> <p>FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p>FortiWeb Cloud, including FortiAppSec Cloud.</p>	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 7.4.7. This includes providing the syntax diff between the fully supported versions of FortiOS and the newly released versions that may have objects changed, added, or removed. The differences listed apply to FortiOS, but not to FortiManager 7.4.7. Thus, administrators should be aware if they are using the related FortiOS version(s), platform(s), and object(s) listed in this section.

FortiOS versions will be added to this section as the syntax diff becomes available after the FortiOS release. For current support, see the [FortiOS Compatibility Tool on the Fortinet Document Library](#).

FortiManager 7.4.7 and FortiOS 7.2.12 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.4.7 and FortiOS 7.2.12.

The following objects were added in FortiOS 7.2.12. These objects can only be configured on the FortiOS device, and they cannot be configured from FortiManager 7.4.7.

- (attr) vpn ipsec phase1 cert-trust-store
- (attr) vpn ipsec phase1 dev-id
- (attr) vpn ipsec phase1 dev-id-notification
- (attr) vpn ipsec phase1 ems-sn-check
- (attr) vpn ipsec phase1 exchange-fgt-device-id
- (attr) vpn ipsec phase1 link-cost
- (attr) vpn ipsec phase1 loopback-asymroute
- (attr) vpn ipsec phase1 network-id
- (attr) vpn ipsec phase1 network-overlay
- (attr) vpn ipsec phase1 remote-gw6-country
- (attr) vpn ipsec phase1 remote-gw6-end-ip
- (attr) vpn ipsec phase1 remote-gw6-match
- (attr) vpn ipsec phase1 remote-gw6-start-ip
- (attr) vpn ipsec phase1 remote-gw6-subnet
- (attr) vpn ipsec phase1 remote-gw-country
- (attr) vpn ipsec phase1 remote-gw-end-ip
- (attr) vpn ipsec phase1 remote-gw-match
- (attr) vpn ipsec phase1 remote-gw-start-ip
- (attr) vpn ipsec phase1 remote-gw-subnet

Other changes in FortiOS 7.2.12.

```
vpn ipsec phase1 fec-mapping-profile
tag: None -> ds
```

FortiManager 7.4.7 and FortiOS 7.4.9 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.4.7 and FortiOS 7.4.9.

The following objects were added in FortiOS 7.4.9. These objects can only be configured on the FortiOS device, and they cannot be configured from FortiManager 7.4.7.

- (attr) firewall access-proxy api-gateway realservers verify-cert
- (attr) firewall access-proxy api-gateway6 realservers verify-cert
- (attr) firewall access-proxy6 api-gateway realservers verify-cert
- (attr) firewall access-proxy6 api-gateway6 realservers verify-cert
- (node) firewall proxy-policy poolname6
- (attr) firewall vip realservers verify-cert
- (attr) log setting rest-api-performance
- (attr) system admin gui-dashboard widget modem
- (attr) system admin gui-dashboard widget temperature-unit
- (attr) system global geoip-full-db
- (attr) system global user-device-store-max-device-mem
- (attr) system settings intree-ses-best-route
- (attr) system sso-admin gui-dashboard widget modem
- (attr) system sso-admin gui-dashboard widget temperature-unit
- (attr) system sso-forticloud-admin gui-dashboard widget modem
- (attr) system sso-forticloud-admin gui-dashboard widget temperature-unit
- (attr) system sso-fortigate-cloud-admin gui-dashboard widget modem
- (attr) system sso-fortigate-cloud-admin gui-dashboard widget temperature-unit

Additional option changes in FortiOS 7.4.9. You must confirm these option changes do not conflict with options that you have set from FortiManager. For example, from FortiManager 7.4.7, you cannot use options that have been removed and you cannot set options that have been added.

```
system admin gui-dashboard widget type
  ++ 2 opts: modem-signal-info sensor-info
system interface speed
  ++ 1 opts: 100auto
system sso-admin gui-dashboard widget type
  ++ 2 opts: modem-signal-info sensor-info
system sso-forticloud-admin gui-dashboard widget type
  ++ 2 opts: modem-signal-info sensor-info
```

```
system sso-fortigate-cloud-admin gui-dashboard widget type
++ 2 opts: modem-signal-info sensor-info
```

Other changes in FortiOS 7.4.9. If a table size or integer range has changed in FortiOS 7.4.9, you are still restricted to the old table size or integer range in FortiManager.

```
system ntp key
tag|sz: 59 -> 64
system ntp ntpserver key
tag|sz: 59 -> 64
```

Resolved issues

The following issues have been fixed in 7.4.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
1041445	The AP attributes do not automatically update in the <i>AP Manager</i> .
1050466	The 802.11ax-5g AP profile is missing for all FortiAPs that support WiFi 6.
1083224	FortiManager attempts to install 'port1-mode > bridge-to-wan' when 'Override LAN Port' is enabled and 'LAN Port Bridge' is set to 'Bridge to LAN'.

Device Manager

Bug ID	Description
932579	Assigning a BGP template is purging the previously existing BGP config from the target FortiGates
973365	FortiManager does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode.
992550	Unable to remove the trusted host for a FortiGate admins under the Device DB from the FortiManager's GUI.
995919	Cannot config system password-policy expire-day for FortiGates.
1000101	FortiManager fails to retrieve certificates that were directly imported into the FortiGate. As a result, FortiManager repeatedly attempts to push a CSR, leading to installation status conflicts.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
1021789	The FortiManager SD-WAN widget's health check status is not functioning as expected.
1039127	Unable to edit the Logs settings under the device management.

Bug ID	Description
1041265	While using a <i>Device Blueprint</i> to apply a pre-run cli template and creating model devices via CSV import, the pre-run does not show applied in <i>Device Manager</i> .
1041440	Some FortiGate platform (FGT-40F & FGT-60F) does not support the <code>ip-managed-by-fortiiipam</code> and FortiGate refuses to take the configuration from FortiManager; hence users will be experiencing the install error.
1053194	If the <code>system interface speed</code> 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.
1063635	FortiManager does not support the FortiWiFi-80F-2R-3G4G-DSL.
1063835	FortiManager ZTP installation to FortiGate versions 7.2.8 and lower may fail due to differing default <code>ssh-kex-algo</code> settings between FortiManager and FortiGate.
1063850	FortiManager is attempting to install a "PRIVATE KEY" with every installation, even after retrieving the config.
1071249	Under <i>Device Manager > Monitors > SD-WAN Monitor</i> , there are some missing data on widgets Bandwidth Overview and Traffic Growth.
1073479	Install preview does not function properly.
1075052	Occasionally, installations may fail on FortiGates in HA mode due to a "Serial number does NOT match" error. This can happen if the HA device's serial number on FortiManager does not immediately update after a failover.
1079654	Firewall address entries are incorrectly generated when creating a bridge/mesh-type SSID.
1080414	CSV import fails to set metadata variables due to old header format ("name").
1080940	In an IPSEC tunnel template, deleting an IPSEC tunnel that is not the last one in the template causes the configuration of the last remaining tunnel to disappear when you revisit the template.
1081105	The "system interface speed" attribute is incorrectly configured on the FortiManager, which may cause the installation to the FortiGate to fail. Workaround: Change the interface speed using CLI script and run directly on the FortiGate using the syntax "set speed auto".
1085385	Importing SD-WAN configuration previously completed on a FortiGate as a provisioning template in FortiManager returns "Response format error" message
1086303	An installation error may occur when binding and installing the created VLAN interface to the software switch due to <code>ip-managed-by-fortiiipam</code> . No issues have been observed with the installation of VLAN interfaces or physical interfaces.
1089102	Metadata variable value cannot be emptied (value deleted) after a value has been set via <i>Edit Variable Mapping</i> for a model device.
1090340	Deleting at least 1 VPN IPsec tunnel from the IPSEC Templates purging other vpn

Bug ID	Description
	phase2-interfaces which are using the same template
1091441	Managed FortiAnalyzer is not available in dropdown menu in <i>System Template</i> in <i>Log Settings</i> .
1094451	If the <i>Timezone</i> field in the <i>System Template</i> is left blank, FortiManager may apply its default timezone and overwrite the existing timezone on the FortiGates.
1099270	Unable to upgrade of FortiGate HA devices via Firmware Templates.
1103166	Installation wizard might stuck at 50% if the device has Jinja CLI template assigned.
1103304	OSPF passive interface settings cannot be set via <i>Device settings > Router > OSPF</i> .
1110780	FortiManager does not allow creating the local-in policy with SD-WAN zone.
1111432	In a BGP template Neighbor Range, set <code>max-neighbor-num 0</code> is not accepted by the GUI.
1115014	FortiManager fails to install SSID configuration in FortiGate when captive portal is enabled with error "Must set selected-usergroups"
1119280	Firmware Template assignment does not work properly.
1122481	When a FortiGate HA failover occurs, making any configuration changes on the FortiGate HA may cause FortiManager to attempt to purge the firewall policies on the device during the installation (Install Device Settings (only)).
1124171	FortiManager retrieves the device configuration from the ZTP FortiGate after the image upgrade is performed, due to the 'Enforce Firmware' feature. This action erases all settings in the device database on the FortiManager side, and as a result, AutoLink installation will not be completed successfully.
1124431	Installation failure due to 'sslvpn os check' syntax error.
1126321	When creating a VLAN with "LAN" Role, an object is created even if "Create Address Object Matching Subnet" is disabled.
1128094	After upgrading to v7.2.10, the entries under Network Monitor > Routing (Static & Dynamic) no longer appear.
1129574	Unable to restrict Firmware upgrade via Admin Profile.
1136080	Starting from version 7.2.11, FortiGate devices use a different password type for the administrator's password field. FortiManager versions released before this change cannot verify the administrator password when installing to an FortiGate, which may result in an installation failure.
1148864	During provisioning, if multiple scripts attempt to modify the aggregate interface, the database installation fails with the following error: [attribute "vdom" check error - runtime error -2: Virtual domain must be same as virtual domain () for all aggregate/redundant interfaces] This issue occurs only with aggregate interfaces.
1152564	Unable to edit route-map due to the following error "rule/2/set-priority is out of range"

Bug ID	Description
	(property: set-priority)".
1153376	If devices are added to FortiManager after SD-WAN is enabled, then Traffic Shaping/SD-WAN may display No Data or No Records Found. If the user enables SD-WAN after the device is already managed by FortiManager, there should be no issue.

FortiSwitch Manager

Bug ID	Description
1026433	When navigating to <i>FortiSwitch Manager</i> > FSW VLAN > "BUILD-VLAN" and enabling the DHCP Server, the Advanced options are missing the <i>filename</i> field.
1077058	IPv4 allow access for VLAN interface over Per-Device Mapping cannot be set.
1089719	Pre-provisioning on FortiManager for the FortiSwitch 110G is unavailable, as this functionality might not yet supported on the FortiOS. Please review <i>FortiSwitch 110G support</i> in Special Notices on page 12 .
1097467	There is a mismatch in the per-VDOM limit between the Managed FortiSwitch on the FortiManager and the actual FortiGate, causing a copy failure error when installing the configuration. So far, this issue has been observed on the FGT-90G.
1110598	Unable to add per device mapping config for FortiSwitch VLAN.
1153287	The maximum number of managed FortiSwitches on FortiManager does not match with the maximum number of managed FortiSwitches by FortiGate, resulting in a copy failure error during installation to FortiGates.

Others

Bug ID	Description
1003711	During the FortiGate HA upgrade, both the primary and secondary FortiGates may reboot simultaneously, which can disrupt the network. This issue is more likely to occur in FortiGates that require disk checks, leading to longer boot times.
1009848	Support ISE distributed deployment: PAN/MnT Nodes up to 2, Pxgrid Nodes up to 4.
1025366	FortiManager does not support the FortiExtender SSID
1049457	Users may encounter an issue in the FortiManager GUI when expanding the log details (when FortiAnalyzer is added as a managed device).

Bug ID	Description
1052341	Not able to select Address type MAC in SD-WAN rule source address.
1065593	Not able upgrade ADOM.
1066240	The FortiSASE Connector is supported only on FortiManager VM platforms and is not supported on FortiManager hardware models.
1067460	Unable to upgrade ADOMs from 6.0 to 6.2, due to the FortiGate's syntax changed.
1075449	Intermittent connection issues have been reported randomly when the FortiManager manages 1000+ FortiGates.
1081941	When UTM-Profile gets added to a FortiProxy policy, FortiManager generates invalid config.
1089725	Progressively slower GUI performance caused by increasing memory usage of the "init" daemon.
1091375	When the install is waiting for a session, it neither updates nor completes the task.
1103008	Not able to edit DNS Filter profile in FortiProxy ADOM.
1111686	FortiManager's GUI may crash with the error "Oops! Sorry, an unexpected error has occurred." when downloading a backup or accessing the <i>Last Script Run</i> option under <i>Device Database</i> .
1113799	Unable to upgrade the FortiAP or FortiSwitch from FortiManager.
1114595	Login authentication fail when using FortiAuthenticator with FortiToken Mobile assigned to the user.
1114809	After upgrading the FortiManager using the "Upgrade Image via FortiGuard" feature, the FortiManager JSON API login may fail, leading to service disruptions. This issue is important for FortiPortal and other FortiManager API clients.
1117603	Some compatibility issues have been encountered with FortiOS 7.4.7, please review the FortiManager 7.4.6 Release Notes.
1119279	Event log for object is generating thousands of Wifi Events.
1124007	'Ok' button does not save the settings; Navigate to Device Manager > Device & Groups > Right click on FortiGate > Firmware upgrade > Schedule > Custom > Define time > Press OK.
1125382	When EMS is added as a Fabric Connector to these FortiGates from FortiManager, all devices appear under FortiManager-managed devices, but only the primary FortiGates serial number is displayed.
1136765	The PxGrid connector should support Fully Qualified Domain Names (FQDN).
1142559	When attempting to upload the firmware image from FortiGuard, FortiManager returns the following error "Code: -1, Invalid image". This issue has primarily been observed on FortiGate hardware platforms running special build firmware versions, where the image contains an encrypted MBR such as on the FortiGateRugged-70G-5G-Dual, FortiGateRugged-70G, FortiGateRugged-50G-5G, FortiWiFi-70G models.

Bug ID	Description
1147636	Universal connector card on <i>Fabric View</i> page is missing under <i>Fabric View > Endpoint/Identity connectors</i> .
1160086	Unable to upgrade ADOM from v7.2 to v7.4 due to HTTP3(QUIC) error in deep-inspection profile.

Policy and Objects

Bug ID	Description
706809	Policy Checkexport does not have the last hit count details anymore.
968149	Unable to export policy package to CSV.
969923	The <i>View Mode</i> button, which is used to check the interface in Pair View, is missing in the Firewall Policy under Policy Packages.
991720	FortiManager still has an option to enable the <code>match-vip</code> through the policy package for "allow" policies. However, this is not supported anymore on the FortiGates.
1011220	FortiManager constantly changes the UUID of some objects.
1025012	Configuring the SSL/SSH inspection profile may result in the following error: "The server certificate replacement mode cannot support category exemptions."
1030914	Copy and paste function in GUI removes name of the policy rule and adds unwanted default security profiles (SSL-SSH no-inspection and default PROTOCOL OPTIONS).
1047850	Error occurs when modifying any route maps: "Cannot save route maps: rule/[id]/set-priority: out of range...".
1054707	FortiManager try to install "unset qos-policy" and installation fails.
1057228	Importing the SDN Objects, with multiple tags, will add multiple entries listed as SDN objects; when clients add anything into the filters section, browser immediately redirects to an error page showing: "Oops! Sorry, an unexpected error has occurred".
1070800	FortiManager is attempting to install the <code>cli-cmd-audit</code> command on a FortiGate running version 7.2.8, which does not support this command, leading to an installation error.
1073463	Installation is failed with error "VIP entry cannot be moved when central-nat is disabled."
1076659	When policy package configured with policy block, installation to multiple devices may have copy fail errors if combined length of the Policy Block name and Policy name is greater than 35 characters and if the total number of such policies exceeds 1000.
1077964	After ZTNA server real server address type changes from FQDN to IP, the policy installation may fail; FortiManager pushes ZTNA server config with wrong order.

Bug ID	Description
1078598	Unable to import policy due to issues related to the protocol-options feature.
1079037	The <code>internet-service-id</code> attribute is configurable in the FortiManager, whereas this attribute cannot be modified on the FortiGate.
1079128	ZTNA Server Per-Device Mapping may display a copy error failure if a new per-device mapping is created without specifying the object interface.
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".
1082548	Address type FQDN is missing DNS resolve domain name function feature.
1086603	Unable to create local-in policy with ISDB objects.
1086705	Multicast policy table Log column shows wrong info and right click update does not work properly.
1089894	The Policy Package import may hang indefinitely on a specific FortiGate VDOM due to recursive object references.
1092581	FortiManager cannot modify <code>rat-timeout-profile</code> in Policy Packages.
1093173	Web-filter rating service returns unrated when the URL does not have 'scheme' part.
1096879	When checking the policy package diff, FortiManager shows that the "system replacemsg spam" entry will be deleted; however, this change is not reflected in the install log.
1097885	Action column is missing in policy package for security policy when NGFW Mode set to policy-based.
1101436	The <code>sni-server-cert-check</code> cannot be disabled on SSL-SSH inspection profile for "ftps", "pop3s", and "smtps".
1101919	Changes to a Virtual IP global settings are not applied when a per-device mapping exists.
1106646	When attempting to configure a local-in policy on FortiManager using ISDB objects as the source, the following error is encountered: "Attribute 'srcaddr' MUST be set when internet-service-src-name is set"
1108159	IP address list for an ISDB object differ between FortiManager and managed FortiGate while both devices have installed the same ISDB definitions.
1109061	FortiManager tries to set the inspection mode for the deny policies.
1112011	When a policy package contains a globally assigned policy, installing a local ADOM policy package (with the "Install On" feature enabled for a specific device) may not function properly. The policy could be installed on all devices instead of the intended one.
1112917	Unable to set or update a security profile group on a policy directly in the firewall or proxy policy view.

Bug ID	Description
1113129	FortiManager is treating <code>implicit-deny local-in</code> policy incorrectly, denying any traffic.
1114832	Any addition/modification in Application and Filter Overrides for Application profile doesn't show up in the install preview.
1116489	The revision history time stamps for custom profiles are all showing the same.
1119299	Installation fails due to syntax compatibility issues between FortiManager and FortiGate version 7.2.10. Specifically, the issue occurs when FortiManager attempts to unset the <code>servercert</code> in the <code>vpn ssl</code> settings.
1130475	FortiManager starts appending an ID to the global-label associated with policies. This can cause a problem if global labels are being used to group policies together.
1131552	Import fails due to an invalid remote certificate, even though the certificate is available on the FortiGate.
1133553	Unused policy tool showing <i>No hit count report</i> for this policy package message when policy block is added to policy package.
1134276	Installation of "config system ddns" configuration fails.
1139220	FortiManager does not prevent users to mix ISDB and destination addresses.

Script

Bug ID	Description
931088	Unable to delete VDOMs using the FortiManager script. Interfaces remain in the device database, causing the installation to fail.
1085374	FortiManager does not support exporting the TCL scripts via CLI.

Services

Bug ID	Description
1104925	FortiManager in Cascade mode may fail to display accurate license information/contracts for FortiGate retrieved from the FDS server, as it is not listed in the FortiGate's authlist.

Bug ID	Description
1108706	When updating query service packages from the global anycast server (globalupdate.fortinet.net), medium-sized IoT packages may encounter checksum errors. These errors can prevent the proper updating of SPAM and URL databases, potentially impacting the FortiManager's FortiGuard Services.
1116120	When the FortiGuard Web Filter and Email Filter services are enabled, the usage of the root filesystem ("rootfs") gradually increases until it reaches 100%. This may affect the performance of other functions on the FortiManager, and it will be more noticeable when the FortiManager is operating with a smaller memory size.
1138715	FortiManager does not auto-download the FortiClient signature from FortiGuard.

System Settings

Bug ID	Description
1047252	Incorrect warning message displayed in FortiManager GUI during upgrade from Feature build to Mature build.
1081463	The encrypted backup file cannot be easily correlated with the backup details, as the date and time are not included.
1088248	When users perform any task, such as installing a policy, the task monitor icon that appears at the top-right of the GUI continuously shows a loading state, and users are unable to view the task progress.
1108205	ADOM lock override does not work even though lock-preempt has been enabled.
1115464	When any interfaces have the service access feature enabled (fgtupdates, fclupdates, and webfilter-antispam), changing the IP address on the desired interfaces may not immediately affect the listing port for that IP. As a result, the user might not be able to access the GUI using the newly configured IP address (assuming default port 443 is being used).
1121608	Under the <i>Dashboard > Sessions</i> widget, the number of current sessions presented in FortiManager does not match the number of sessions in the FortiGate.

VPN Manager

Bug ID	Description
1084434	Unable to rename theaddress objects (either source and/or destination) used in Phase2 quick selectors in IPSec VPN without an installation error.

Bug ID	Description
1084696	If users reopen the IPsec Tunnel template and close it without making any changes, FortiManager might still display the following error message in the install log: "Error: VPN IPsec phase1-interface psksecret...Minimum psksecret length is 6..." .
1090636	Unable to edit VPN community due to the following error message: "vpnmgr/vpntable/: cannot be edited".

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1091672	FortiManager 7.4.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2025-24474
1129438	FortiManager 7.4.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2025-26466

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

The following issues have been identified in version 7.4.7.

AP Manager

Bug ID	Description
1173274	FortiManager is trying to enable ddscan when it is not enabled on ADOM db, device db, and AP Manager profile.
1174004	After FortiManager's upgrade to 7.4.7, FortiManager may suggest to "set ddscan enable" during the first installation, and this may create some issue on FortiAPs connected to the FortiGate.

Device Manager

Bug ID	Description
1166830	FortiGates may be unexpectedly renamed during policy package installation when deploying to multiple devices (more than 5). Workaround: Install to less than 5 devices at the same time or create metadata variable to config hostname in system template.
1167436	FortiManager displays "retrievehaconfail" error when performing retrieve config for FortiGate's HA cluster. Workaround: "diagnose test deploymanager reloadconf " from the CLI does not display any error.

Bug ID	Description
1167958 1175207	<p>After upgrading FortiManager to version 7.4.7, /var may fill up with temporary files. This is most likely to happen with high device count (>100) or heavy use of thread feeds. Possible symptoms include FGFM tunnels to FortiGates not coming up or GUI not functioning correctly. The likelihood of /var filling up increases the longer FortiManager runs on 7.4.7</p> <p>What to look for:</p> <ol style="list-style-type: none"> 1. The inode usage of /var increases rapidly as seen in "diagnose system print df -i", it soars over 30% hours/days after a FortiManager reboot. 2. The fgfm debug output shows many occurrences of "connect error when connect to : Bad file descriptor". 3. If some function/feature is broken, this functionality often recovers if rebooting FortiManager, then after some time, it is broken again.

FortiSwitch Manager

Bug ID	Description
1161320	FortiManager shows an incomplete FortiSwitch Topology compared with FortiGate.

Others

Bug ID	Description
1158842	The FortiManager dashboard <i>FortiGuard license status</i> does not display the same data as shown on the FortiGuard page.
1163922	The <i>FortiView</i> tile is missing after adding FortiAnalyzer as a managed device to FortiManager.
1168422	FortiManager does not properly support the "FortiGate-50G-SFP-POE" platform.
1170281	<p>Not able to create a new VDOM or remove any interfaces from VDOMs when Workspace mode is enabled.</p> <p>Workaround:</p> <p>Use a script like the following and run it against the Device Database CLI:</p> <pre>config vdom edit vdom_name end</pre>
1188452	Downstream FortiManagers in cascade mode does not download the Webfilter database from the Upstream FortiManager.

Policy & Objects

Bug ID	Description
1152640	<p>When no port setting (empty value) has been set for HTTPS on SSL/SSH Inspection Profile, the installation preview shows error "https ... Must set at least one port (default port:443) or enable ssl inspect-all".</p> <p>Workaround:</p> <p>Modify the profile by adding port setting for HTTPS under "Protocol Port Mapping" even they were disabled. (Enable the option first, input port setting, such as "443", then disable the option and save the profile).</p>
1157272	<p>When creating a new entry under the Logical Relationship for a DLP dictionary, the <i>Pattern</i> field must be completed only for the applicable entry types; it should remain blank for those that do not require it.</p>
1160047	<p>Application control category "GenAI" is missing in FortiManager, but present in FortiGate.</p> <p>Workaround:</p> <p>Copy a FortiGate application list (Applist) from the CLI that includes Category 36, and insert it into a CLI template in FortiManager. Assign CLI template to Fortigate.</p>
1162327	<p>Install preview may get stuck if another user is simultaneously pushing an install on a different FortiGate within FortiManager.</p>
1170381	<p>Unable to create new section "Add Section" in policy after upgrading FortiManager to 7.4.7 while using interface pair view mode. Operation "Add Section" triggers nothing. Field "label" or "global-label" are empty.</p>
1173197	<p>Where Used feature is not working for objects that contain a forward slash (/).</p>
1199272	<p>Imported certificate does not show details.</p>
1174618	<p>After importing the policies and objects from the FortiGate, even though the FortiManager settings were selected, the configuration status for all FortiGates changed to 'Modified.'</p>

Services

Bug ID	Description
1167362	<p>Despite having the <code>fgfm-deny-unknown</code> setting enabled, unauthorized devices might still be appearing in the <i>Device Manager</i>. For more information, see Special Notices on page 12.</p>

System Settings

Bug ID	Description
1169081	<p>When clicking on the "Approve this request" link in the Workflow mode, following error message can be observed: "Unable to complete action, failed to 'approve'."</p> <p>Workaround: Log in to FortiManager to approve the task.</p>

VPN Manager

Bug ID	Description
1166323	The <i>VPN Manager > IPsec VPN Communities</i> page no longer displays correctly — the page loads but shows only a blank (white) screen.

Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.4.7.

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
970157	<p>FortiManager is attempting to install SNMP configurations that are not supported by the FortiGate VM, such as power-supply-failure, temperature-high, and voltage-alert.</p> <p>Workaround:</p>

Bug ID	Description
	Create a CLI template for SNMP configuration and assign it to the device(s).
974925	The NTP Server setting may not display the correct configuration. This issue might occur on managed devices running FortiOS versions lower than 7.4.2. Workaround: Edit NTP server setting under CLI configuration.
980362	The Firmware Version column in <i>Device Manager</i> incorrectly shows "Upgrading FortiGate from V1 to V2" even after a successful upgrade has been completed.
1102790	FortiManager pushes the <code>unset auto-connect</code> command to <code>config system lte-modem</code> , where the default value is disabled on FortiOS but still enabled on FortiManager.
1112389	<i>FortiView</i> and <i>Log View</i> fail to display logs when FortiAnalyzer is configured as a managed device in FortiManager.

Global ADOM

Bug ID	Description
1141123	Installing the Global Header Policy fails with the error: "invalid value". This issue has been observed after upgrading FortiManager to v7.2.10. Workaround: <ol style="list-style-type: none"> Unset the uuids of all addresses and address groups in Global. <ul style="list-style-type: none"> # execute fmpolicy print-adom-object Global 140 all # execute fmpolicy print-adom-object Global 142 all <ul style="list-style-type: none"> • copy them to new file in Notepad++ • use regex replace all <code>^set uuid.*\$</code> with <code>unset uuid</code> Clone all used global addresses and services to have different names from the local ones and replace them in the global policies. Assign the changes. Install.

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: <code>config webfilter profile</code>

Bug ID	Description
	<pre> edit "g-default" config web unset urlfilter-table end next end </pre>
1041706	<i>Extender Manager</i> shows the managed Extender as Down even if it is Up and correctly displayed on FortiGate.
1049457	Users may encounter an issue in the FortiManager GUI when expanding the log details (when FortiAnalyzer is added as a managed device).
1071646	Formatted Event logs do not display the correct timestamp.
1113980	In FortiManager operating in Workspace (ALL ADOMs) mode, the Installation Preview may hang, and the GUI displays an infinite loading state. This issue is observed when multiple users initiate installations to their respective devices simultaneously while the Policy Packages (PPs) are locked.
1126662	In an FortiGate HA setup running on the public cloud platform, the FortiManager attempts to install changes on static routes, which may cause routes to be deleted after an HA failover.

Policy & Objects

Bug ID	Description
845022	SDN Connector failed to import objects from VMware VSphere.
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.
1131041	Not able to create ZTNA Server due to the certificate error.
1142983	In FortiManager, creating a threat feed connector and applying it to multiple VDOMs results in the same UUID being assigned across all instances. This behavior may lead to duplicate UUID issues.
1168866	In FortiManager under <i>Policy & Objects > Firewall Objects > Internet Service > IP Reputation Database</i> , most entries show "0" in the Number of Entries column, while the same entries display data on FortiGate devices.

Services

Bug ID	Description
1170893	When FortiManager is acting as Local FortiGuard Servers, FortiClient applications running on Linux machines are not receiving any signature updates.

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.