



# Release Notes

**FortiManager 8.0.0**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



April 21, 2026

FortiManager 8.0.0 Release Notes

02-800-1168460-20260421

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>6</b>
<b>FortiManager 8.0.0 Release</b> .....	<b>7</b>
Supported models .....	7
FortiManager VM subscription license .....	7
<b>Special Notices</b> .....	<b>8</b>
FortiSwitch-VLAN with per-device mapping enabled .....	9
FortiCare Elite or FortiCare Premium required to download FortiGuard objects .....	9
FortiManager instances deployed on the Azure platform .....	9
Script creation API endpoint has changed starting in FortiManager 7.6.5 .....	10
The FortiManager XML API is no longer supported .....	10
New Admin Profile permissions added in 7.6.4 .....	11
Upgrading FortiGate devices on FOS 7.6.1 and 7.6.2 from FortiManager .....	11
Default password policy for local users .....	12
MEAs removed in FortiManager 7.6.4 .....	12
New CLI option for managing FortiGate HA clusters .....	12
SSL VPN tunnel mode no longer supported in FortiOS 7.6.3 .....	13
Adding VM devices to FortiManager .....	13
The system interface speed is read-only in FortiManager .....	14
HA synchronization of FortiGuard package management receive status .....	14
The names of policies derived from policy blocks no longer automatically include the policy block name .....	14
FortiManager support for updated FortiOS private data encryption key .....	15
Shell access has been removed .....	16
Enable fcp-cfg-service for Backup Mode ADOMs .....	16
System Templates include new fields .....	17
Custom certificate name verification for FortiGate connection .....	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 .....	18
FortiGuard web filtering category v10 update .....	18
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
Option to enable permission check when copying policies .....	20
View Mode is disabled in policies when policy blocks are used .....	20
Reconfiguring Virtual Wire Pairs (VWP) .....	21
Hyper-V FortiManager-VM running on an AMD CPU .....	21
<b>New features</b> .....	<b>22</b>
<b>Upgrade Information</b> .....	<b>23</b>
Downgrading to previous firmware versions .....	23

Firmware image checksums .....	23
FortiManager VM firmware .....	24
SNMP MIB files .....	25
<b>Product Integration and Support .....</b>	<b>26</b>
Supported software .....	26
Web browsers .....	27
FortiOS and FortiOS Carrier .....	27
FortiADC .....	27
FortiAnalyzer .....	28
FortiAnalyzer-BigData .....	28
FortiAP .....	28
FortiAuthenticator .....	28
FortiCache .....	29
FortiCASB .....	29
FortiClient .....	29
FortiDDoS .....	29
FortiDeceptor .....	30
FortiFirewall and FortiFirewallCarrier .....	30
FortiMail .....	30
FortiPAM .....	30
FortiPortal .....	31
FortiProxy .....	31
FortiSandbox .....	32
FortiSASE .....	32
FortiSOAR .....	32
FortiSRA .....	32
FortiSwitch .....	32
FortiTester .....	33
FortiToken .....	33
FortiWeb .....	33
Virtualization .....	33
Feature support .....	34
Language support .....	35
Supported models .....	36
FortiGate models .....	36
FortiGate special branch models .....	42
FortiCarrier models .....	44
FortiCarrier special branch models .....	47
FortiADC models .....	48
FortiAnalyzer models .....	49
FortiAnalyzer-BigData models .....	50
FortiAuthenticator models .....	50
FortiCache models .....	51
FortiDDoS models .....	51
FortiDeceptor models .....	52
FortiFirewall models .....	52
FortiFirewallCarrier models .....	53
FortiMail models .....	54

FortiPAM models .....	54
FortiProxy models .....	55
FortiSandbox models .....	55
FortiSOAR models .....	56
FortiSRA models .....	56
FortiTester models .....	56
FortiWeb models .....	56
FortiExtender MODEM firmware compatibility .....	58
<b>Resolved issues .....</b>	<b>59</b>
AP Manager .....	59
Device Manager .....	59
FortiSwitch Manager .....	61
Global ADOM .....	61
Others .....	62
Policy and Objects .....	63
Revision History .....	65
System Settings .....	65
VPN Manager .....	66
<b>Known issues .....</b>	<b>67</b>
New known issues .....	67
Others .....	67
Policy and Objects .....	67
Existing known issues .....	67
Device Manager .....	68
Others .....	68
Policy and Objects .....	68
System Settings .....	68
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>69</b>
FortiGuard Center update support .....	69
<b>Appendix B - Default and maximum number of ADOMs supported .....</b>	<b>70</b>
Hardware models .....	70
Virtual Machines .....	70

# Change Log

Date	Change Description
2026-04-21	Initial release of 8.0.0.

# FortiManager 8.0.0 Release

This document provides information about FortiManager version 8.0.0 build 0105.



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

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)

## Supported models

FortiManager version 8.0.0 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300F, FMG-400G, FMG-410G, FMG-1000F, FMG-1000G, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3100G, FMG-3700F, FMG-3700G, and FMG-3750G.
<b>FortiManager VM</b>	FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_IBM, FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).



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 24](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 70](#).

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 8.0.0.

- [FortiSwitch-VLAN with per-device mapping enabled on page 9](#)
- [FortiCare Elite or FortiCare Premium required to download FortiGuard objects on page 9](#)
- [FortiManager instances deployed on the Azure platform on page 9](#)
- [Script creation API endpoint has changed starting in FortiManager 7.6.5 on page 10](#)
- [The FortiManager XML API is no longer supported on page 10](#)
- [New Admin Profile permissions added in 7.6.4 on page 11](#)
- [Upgrading FortiGate devices on FOS 7.6.1 and 7.6.2 from FortiManager on page 11](#)
- [Default password policy for local users on page 12](#)
- [MEAs removed in FortiManager 7.6.4 on page 12](#)
- [New CLI option for managing FortiGate HA clusters on page 12](#)
- [SSL VPN tunnel mode no longer supported in FortiOS 7.6.3 on page 13](#)
- [Adding VM devices to FortiManager on page 13](#)
- [The system interface speed is read-only in FortiManager on page 14](#)
- [HA synchronization of FortiGuard package management receive status on page 14](#)
- [The names of policies derived from policy blocks no longer automatically include the policy block name on page 14](#)
- [FortiManager support for updated FortiOS private data encryption key on page 15](#)
- [Shell access has been removed on page 16](#)
- [Enable fcp-cfg-service for Backup Mode ADOMs on page 16](#)
- [System Templates include new fields on page 17](#)
- [Custom certificate name verification for FortiGate connection on page 17](#)
- [Additional configuration required for SSO users on page 17](#)
- [When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade on page 18](#)
- [FortiGuard web filtering category v10 update on page 18](#)
- [Configuration backup requires a password on page 19](#)
- [FortiManager-400E support on page 19](#)
- [Serial console has changed for FortiManager deployments on Xen on page 20](#)
- [OpenXen in PV mode is not supported in FortiManager 7.4.1 on page 20](#)
- [Option to enable permission check when copying policies on page 20](#)
- [View Mode is disabled in policies when policy blocks are used on page 20](#)
- [Reconfiguring Virtual Wire Pairs \(VWP\) on page 21](#)
- [Hyper-V FortiManager-VM running on an AMD CPU on page 21](#)

## FortiSwitch-VLAN with per-device mapping enabled

For customers upgrading from a version prior to FortiManager 7.4.9 or 7.6.5 with a FortiSwitch-VLAN with per-device mapping enabled, FortiManager may unset the interface configuration. Specifically, it may "unset allowaccess" on each VLAN interface.

To correct this issue, run the following command after upgrading FortiManager:

```
diagnose cdb manual-fix adom <adom name> fspvlan-dyn-ipv4allowaccess
```

The dynamic mappings will inherit allowaccess settings from the parent entry.

## FortiCare Elite or FortiCare Premium required to download FortiGuard objects

Starting in 7.2.12, 7.4.9, and 7.6.5, FortiManager requires a valid FortiCare Elite or FortiCare Premium support contract registered in FortiCloud in order to get object updates from FortiGuard.

## FortiManager instances deployed on the Azure platform

FortiManager instances deployed on the Azure platform (regardless of version) may lose all data—including configuration, logs, and reports—if the VM is deallocated and subsequently reallocated.

This issue can occur when the VM is deallocated through Azure-level operations (e.g., Azure portal, CLI, or automation). For example, this may happen when an Azure administrator changes the VM SKU (e.g., from Standard\_D16\_v3 to Standard\_D32a\_v4), or when the VM is manually stopped (deallocated) from the Azure portal.

To minimize the risk of data loss, it is strongly recommended to:

- Perform regular backups of configuration and data via the GUI or native CLI commands on FortiManager.
- Shut down the FortiManager instance, if required, only from within the FortiManager system itself rather than through Azure-level controls.
- Before performing any upgrade or modification:

Run `execute lvm info` to verify disk composition and ensure no Azure temporary disk is included in LVM, For example:

```
Disk 1: 10 TB, Disk 2: 6 TB, ...
```

If all listed disks were explicitly added by the FortiManager admin, this indicates that no temporary disk is part of LVM and the upgrade is considered safe.

If an unexpected disk is detected (e.g., smaller system disk such as ~128 GB), it is likely the Azure temporary disk. In this case, perform a full backup before proceeding with the upgrade.

If issues occur after the upgrade:

- Run `execute format disk` to rebuild LVM,
- Use `execute restore` to recover data from backup.

The possible root cause may be as follows:

Prior to version 7.4.2, the system assumed `sdb` was always the Azure temporary disk and excluded it from LVM. In certain corner cases, a different device (e.g., `sda`) may have been incorrectly added to LVM. After upgrading, the existing LVM metadata persists on disk. When the VM is later deallocated and reallocated, Azure replaces the temporary disk, causing LVM initialization to fail due to stale metadata. As a result, any data previously stored on the temporary disk is lost.

## Script creation API endpoint has changed starting in FortiManager 7.6.5

The endpoint used to create scripts through the FortiManager API has changed starting in FortiManager 7.6.5.

### Previous endpoints:

```
dvmdb/script
dvmdb/adom/{adom}/script
dvmdb/global/script
```

### New endpoints:

```
pm/config/adom/{adom}/obj/fmg/script
pm/config/global/obj/fmg/script
```

If you are using this endpoint in any automation, it should be updated following your upgrade to FortiManager 7.6.5 or later. For more information on this change, see [Revision control for scripts and script groups with View Diff function in the CLI format](#).

## The FortiManager XML API is no longer supported

The XML API is removed as of FortiManager 7.6.5 and 8.0.0.

## New Admin Profile permissions added in 7.6.4

In FortiManager 7.6.4, the following permissions are added for Admin Profiles:

- *Firmware Upgrades* (*device-fwm-profile*): set permissions for device firmware profiles.
- *Assign Templates to Device* (*device-assignment*): set permissions to assign provisioning templates.
- *Execute Script* (*script-run*): set permissions to execute scripts.

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

For existing custom Admin Profiles created prior to upgrading to FortiManager 7.6.4 or later, the new permissions will be set to None. You must update these settings according to your needs in the custom Admin Profiles.

## Upgrading FortiGate devices on FOS 7.6.1 and 7.6.2 from FortiManager

Due to FortiOS issue 1106072, image file transfers between FortiManager and FortiGate devices on FortiOS 7.6.1 and 7.6.2 may fail when the upgrade is initiated from the FortiManager acting as the Local FDS Server. This issue is resolved in FortiOS 7.6.3 and later.

If you select an multi-step upgrade path for FortiGate which contains FortiOS 7.6.1 or 7.6.2, the upgrade process may stop once the devices have been upgraded to these affected versions.

### Workarounds:

When managed devices have access to public FortiGuard:

- If FortiGate devices have internet connectivity, you can enable the “Let Device Download Firmware From FortiGuard” option in FortiManager. This allows FortiGate devices to retrieve the firmware image directly from FortiGuard during the upgrade process, reducing load on FortiManager.

When managed devices do NOT have access to public FortiGuard (air-gapped or restricted environments):

- Firmware upgrades may require using the following CLI command on the FortiGate:

```
execute restore image management-station <Image-ID> <Version>
```

With this approach, the FortiGate pulls the firmware image from FortiManager, which acts as a Local FDS server.

If multiple managed devices are affected, this CLI command can be deployed via a FortiManager script and installed across the FortiGate devices to streamline the upgrade process.

## Default password policy for local users

Beginning in FortiManager 7.6.4, a password policy for local users is enabled and configured by default. If you are setting up FortiManager 7.6.4 or later, the password created at setup must be at least 8 characters and must contain uppercase letter(s), lowercase letter(s), number(s), and special character(s).

Note that existing password policy settings are maintained after upgrading. For example, if the password policy is disabled prior to upgrading to FortiManager 7.6.4 or later, it will remain disabled after the upgrade.

## MEAs removed in FortiManager 7.6.4

As of FortiManager 7.6.4, there is no support for management extension applications (MEAs) in FortiManager.

## 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 7.6.3:

```
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.

## SSL VPN tunnel mode no longer supported in FortiOS 7.6.3

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is no longer available in the GUI and CLI. Settings will not be upgraded from previous versions. This applies to all FortiGate models.

To ensure uninterrupted remote access, customers must migrate their SSL VPN tunnel mode configuration to IPsec VPN before upgrading to FortiOS 7.6.3.

See [Migration from SSL VPN tunnel mode to IPsec VPN](#) in the FortiOS 7.6 *New Feature* guide for detailed steps on migrating to IPsec VPN before upgrade.

A complete migration guide can be found in the following links:

- For FortiOS 7.6, see [SSL VPN to IPsec VPN Migration](#).
- For FortiOS 7.4, see [SSL VPN to IPsec VPN Migration](#).

## Adding VM devices to FortiManager

As of FortiManager 7.6.3, 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.

## HA synchronization of FortiGuard package management receive status

Starting in FortiManager 7.6.2, the *To Be Deployed Version* configured in *FortiGuard > Packages > Receive Status* is synchronized in an HA cluster. This means that the package version selected for deployment on the primary device will persist during a failover event. For more information on the *To Be Deployed Version* setting, see the FortiManager Administration Guide.

When upgrading an operating FortiManager cluster to version 7.6.2, please review *To Be Deployed Version* settings for each cluster member before proceeding with the upgrade to ensure there is no unintended impact when the settings are synchronized. If the *To Be Deployed Version* package is not available on the secondary FortiManager, the secondary FortiManager will stay at the latest package to be installed.

## 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.

# FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal private-data-encryption key. Instead administrators simply enable the command, and a random private-data-encryption key is generated.

## Previous FortiOS CLI behavior

```
config system global
  set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
12345678901234567890123456789abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
12345678901234567890123456789abc
Your private data encryption key is accepted.
```

## New FortiOS CLI behavior

```
config system global
  set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y

Private data encryption key generation succeeded!
```

## FortiManager behavior

Support for the FortiGate private-data-encryption key by the *Device Manager* in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate private-data-encryption key status and prompts the administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random private-data-encryption key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.

**Warning** ✖

The following managed devices were detected having 'private-data-encryption' enabled. You are required to enter the encryption key as well on FortiManager side. Otherwise, configuration changes can not be installed successfully.

Status	Device Name	IP Address	Platform	Private Data Encryption K
<span style="color: #4285f4;">?</span>	FGVM02TM24009410	172.18.36.216	FortiGate-VM64	<input type="text"/>
				1

Verify
Close

### FortiOS upgrade behavior

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal private-data-encryption key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal private-data-encryption key and can continue to manage the FortiGate device. However, if the private-data-encryption key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

## Shell access has been removed

As of FortiManager 7.6.0, shell access has been removed.

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

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

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

```
execute shell
```

## Enable fcp-cfg-service for Backup Mode ADOMs

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

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

## System Templates include new fields

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

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

## Custom certificate name verification for FortiGate connection



In FortiManager 7.6.2, 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.

## Additional configuration required for SSO users

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

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

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

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

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

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

### **Workaround:**

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

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

## FortiGuard web filtering category v10 update

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

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

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

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

## Configuration backup requires a password

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

In previous versions, the encryption and password were optional.

For more information, see the [FortiManager Administration Guide](#).

## FortiManager-400E support

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

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

```
FMG400E # conf sys certificate local
(local)# ed Fortinet_Local
(Fortinet_Local)# get
name : Fortinet_Local
password : *
comment : Default local certificate
private-key :
certificate :
Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN =
        FL3K5E3M1500074, emailAddress = support@fortinet.com
Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority,
        CN = support, emailAddress = support@fortinet.com
Valid from: 2015-03-06 16:22:10 GMT
Valid to: 2038-01-19 03:14:07 GMT
Fingerprint: FC:D0:0C:8D:DC:57:B6:16:58:DF:90:22:77:6F:2C:1B
Public key: rsaEncryption (1024 bits)
Signature: sha1WithRSAEncryption
Root CA: No
Version: 3
Serial Num:
1e:07:7a
Extension 1: X509v3 Basic Constraints:
CA:FALSE
...
(Fortinet_Local)#
```

## Serial console has changed for FortiManager deployments on Xen

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

## OpenXen in PV mode is not supported in FortiManager 7.4.1

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

## 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.

## 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*.

## Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FortiManager-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

# New features

For information about what's new in FortiManager 8.0.0, see the [FortiManager 8.0 New Features Guide](#). The [index](#) in the New Features Guide lists new features by release.

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

This section contains the following topics:

- Downgrading to previous firmware versions on page 23
- Firmware image checksums on page 23
- FortiManager VM firmware on page 24
- SNMP MIB files on page 25

## Downgrading to previous firmware versions

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

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

## Firmware image checksums

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

# FortiManager VM firmware

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

## Amazon Web Services

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

## Citrix XenServer and Open Source XenServer

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

## Google Cloud Platform

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

## Linux KVM

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

## Microsoft Azure

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

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

## Microsoft Hyper-V Server

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

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

### Oracle Private Cloud

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

### VMware ESX/ESXi

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



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

## SNMP MIB files

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

# Product Integration and Support

This section lists FortiManager 8.0.0 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [Supported software on page 26](#)
- [Feature support on page 34](#)
- [Language support on page 35](#)
- [Supported models on page 36](#)
- [FortiExtender MODEM firmware compatibility on page 58](#)

## Supported software

FortiManager 8.0.0 supports the following software:

- [Web browsers on page 27](#)
- [FortiOS and FortiOS Carrier on page 27](#)
- [FortiADC on page 27](#)
- [FortiAnalyzer on page 28](#)
- [FortiAnalyzer-BigData on page 28](#)
- [FortiAP on page 28](#)
- [FortiAuthenticator on page 28](#)
- [FortiCache on page 29](#)
- [FortiCASB on page 29](#)
- [FortiClient on page 29](#)
- [FortiDDoS on page 29](#)
- [FortiDeceptor on page 30](#)
- [FortiFirewall and FortiFirewallCarrier on page 30](#)
- [FortiMail on page 30](#)
- [FortiPAM on page 30](#)
- [FortiPortal on page 31](#)
- [FortiProxy on page 31](#)
- [FortiSandbox on page 32](#)
- [FortiSOAR on page 32](#)
- [FortiSwitch on page 32](#)
- [FortiTester on page 33](#)
- [FortiToken on page 33](#)

- [FortiWeb on page 33](#)
- [Virtualization on page 33](#)



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 8.0.0 supports the following web browsers:

- Google Chrome version 147
- Microsoft Edge version 147
- Mozilla Firefox 149

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

See [FortiManager compatibility with FortiOS](#).

FortiManager 8.0.0 supports the following versions of FortiOS and FortiOS Carrier:

- 8.0.0
- 7.6.0 to 7.6.6
- 7.4.0 to 7.4.11
- 7.2.0 to 7.2.13

## FortiADC

FortiManager 8.0.0 supports the following versions of FortiADC:

- 8.0.0 and later
- 7.6.0 and later
- 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 8.0.0 supports the following versions of FortiAnalyzer:

- 8.0.0
- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

## FortiAnalyzer-BigData

FortiManager 8.0.0 supports the following versions of FortiAnalyzer-BigData:

- 7.4.0 and later
- 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 8.0.0 supports the following versions of FortiAuthenticator:

- 8.0.0 and later
- 7.0.0 and later
- 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 8.0.0 supports the following versions of FortiCache:

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

## FortiCASB

FortiManager 8.0.0 supports the following versions of FortiCASB:

- 23.2.0 and later

## FortiClient

FortiManager 8.0.0 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 8.0.0 supports the following versions of FortiDDoS:

- 7.2.0 and later
- 7.0.0 and later
- 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
- 5.7.0 and later
- 5.6.0 and later

Limited support. For more information, see [Feature support on page 34](#).

## FortiDeceptor

FortiManager 8.0.0 supports the following versions of FortiDeceptor:

- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later
- 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 8.0.0 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 8.0.0 and later
- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later

## FortiMail

FortiManager 8.0.0 supports the following versions of FortiMail:

- 7.6.0 and later
- 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 8.0.0 supports the following versions of FortiPAM:

- 1.8.0 and later
- 1.7.0 and later
- 1.6.0 and later

- 1.5.0 and later
- 1.4.0 and later
- 1.3.0 and later
- 1.2.0 and later
- 1.1.0 and later
- 1.0.0 and later

## FortiPortal

For more information about compatibility with FortiPortal, see *FortiPortal Compatibility* in the [Fortinet Document Library](#).

## FortiProxy



The *FortiManager Release Notes* communicate support for FortiProxy versions that are available at the time of the FortiManager 8.0.0 release. For additional information about other supported FortiProxy versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiProxy](#).

FortiManager 8.0.0 supports configuration management for the following versions of FortiProxy:

- 7.6.2 to 7.6.4
- 7.4.0 to 7.4.3, 7.4.5 to 7.4.9, and 7.4.11 to 7.4.13
- 7.2.2, 7.2.3, 7.2.7, and 7.2.9 to 7.2.13
- 7.0.7 to 7.0.21



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 34](#).

FortiManager 8.0.0 supports logs from the following versions of FortiProxy:

- 7.6.0 to 7.6.4
- 7.4.0 to 7.4.13
- 7.2.0 to 7.2.16
- 7.0.0 to 7.0.23
- 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 8.0.0 supports the following versions of FortiSandbox:

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

## FortiSASE

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

## FortiSOAR

FortiManager 8.0.0 supports the following versions of FortiSOAR:

- 7.6.0 and later
- 7.5.0 and later
- 7.4.0 and later
- 7.3.0 and later
- 7.2.0 and later

## FortiSRA

FortiManager 8.0.0 supports the following versions of FortiSRA:

- 1.7.0 and later
- 1.6.0 and later
- 1.5.0 and later
- 1.4.0 and later
- 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 27](#).

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

## FortiTester

FortiManager 8.0.0 supports the following versions of FortiTester:

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

## FortiToken

FortiManager 8.0.0 supports the following versions of FortiToken:

- 3.0.0 and later

## FortiWeb

FortiManager 8.0.0 supports the following versions of FortiWeb:

- 8.0.0 and later
- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

## Virtualization

FortiManager 8.0.0 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			✓	✓	✓	✓
FortiProxy	✓	✓**	✓	✓	✓	✓
FortiSandbox			✓	✓	✓	✓
FortiSOAR			✓	✓		
FortiSwitch	✓*	✓				

Platform	Configuration Management	Firmware Management	FortiGuard Update Services	VM License Activation	Reports	Logging
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 8.0.0.



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

This section contains the following topics:

- [FortiGate models on page 36](#)
- [FortiGate special branch models on page 42](#)
- [FortiCarrier models on page 44](#)
- [FortiCarrier special branch models on page 47](#)
- [FortiADC models on page 48](#)
- [FortiAnalyzer models on page 49](#)
- [FortiAnalyzer-BigData models on page 50](#)
- [FortiAuthenticator models on page 50](#)
- [FortiCache models on page 51](#)
- [FortiDDoS models on page 51](#)
- [FortiDeceptor models on page 52](#)
- [FortiFirewall models on page 52](#)
- [FortiFirewallCarrier models on page 53](#)
- [FortiMail models on page 54](#)
- [FortiPAM models on page 54](#)
- [FortiProxy models on page 55](#)
- [FortiSandbox models on page 55](#)
- [FortiSOAR models on page 56](#)
- [FortiTester models on page 56](#)
- [FortiWeb models on page 56](#)

## 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 42](#).

Model	Firmware Version
<p><b>FortiGate:</b> FortiGate-30G, FortiGate-31G, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60F, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-200E, FortiGate-200F, FortiGate-200G, FortiGate-201E, FortiGate-201F, FortiGate-201G, 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-700G, FortiGate-701G, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate 6000 Series:</b> 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><b>FortiGate 7000 Series:</b> 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><b>FortiGate DC:</b> FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-ACDC, FortiGate-3000F-DC, FortiGate-3001F-ACDC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS, FortiGate-4801F-NEBS</p> <p><b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP, FortiWiFi-51G, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE</p>	8.0

Model	Firmware Version
<p><b>FortiGate VM:</b> FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen</p>	
<p><b>FortiGate Rugged:</b> FortiGateRugged-50G-5G, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGateRugged-70G, FortiGateRugged-70G-5G-Dual</p>	
<p><b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60F, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-71F, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, 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-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate 6000 Series:</b> 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><b>FortiGate 7000 Series:</b> 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>	7.6

Model	Firmware Version
<p><b>FortiGate DC:</b> FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-ACDC, FortiGate-3000F-DC, FortiGate-3001F-ACDC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS</p>	
<p><b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP, FortiWiFi-51G, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE</p>	
<p><b>FortiGate VM:</b> FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen</p>	
<p><b>FortiGate Rugged:</b> FortiGateRugged-50G-5G, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGateRugged-70G, FortiGateRugged-70G-5G-Dual</p>	

Model	Firmware Version
<p><b>FortiGate:</b> FortiGate-30G, FortiGate-31G, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-200G, FortiGate-201E, FortiGate-201F, FortiGate-201G, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-700G, FortiGate-701G, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate 6000 Series:</b> 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><b>FortiGate 7000 Series:</b> 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><b>FortiGate DC:</b> FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4801F-DC-NEBS</p>	7.4

Model	Firmware Version
<p><b>FortiWiFi:</b> FortiWiFi-30G, FortiWiFi-31G, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP, FortiWiFi-51G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE</p> <p><b>FortiGate VM:</b> 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><b>FortiGate Rugged:</b> FortiGateRugged-50G-5G, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGateRugged-70G, FortiGateRugged-70G-5G, FortiGateRugged-70G-5G-Dual</p>	
<p><b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate 6000 Series:</b> 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><b>FortiGate 7000 Series:</b> 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>	7.2

Model	Firmware Version
<b>FortiGate DC:</b> FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS	
<b>FortiWiFi:</b> FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE	
<b>FortiGate VM:</b> 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	
<b>FortiOS-VM:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGate Rugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G	

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 8.0.0 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 36](#).

### FortiOS 7.4

FortiGate Model	FortiOS Version
FortiGate-70G-POE-5G, FortiGate-71G-POE-5G	7.4.8
FortiGate-3800G, FortiGate-3801G	7.4.8
FortiGateRugged-60G, FortiGateRugged-60G-5G, FortiGateRugged-60G-5G-M12, FortiGateRugged-60G-M12	7.4.8

## FortiOS 7.2

FortiGate Model	FortiOS Version
FortiGate-30G, FortiGate-31G	7.2.12
FortiGate-70G	7.2.11
FortiGate-71G	7.2.12
FortiGate-70G-POE	7.2.12
FortiGate-71G-POE	7.2.11
FortiGate-200G, FortiGate-201G	7.2.12
FortiGate-700G, FortiGate-701G	7.2.11
FortiWiFi-30G, FortiWiFi-31G	7.2.12
FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G	7.2.11

## FortiOS 7.0

FortiGate Model	FortiOS Version
FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE	7.0.17
FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE	7.0.17
FortiGate-80F-DSL	7.0.17
FortiGate-90G, FortiGate-91G	7.0.17
FortiGate-120G, FortiGate-121G	7.0.16
FortiGate-900G, FortiGate-900G-DC FortiGate-901G, FortiGate-901G-DC	7.0.17
FortiGate-1000F, FortiGate-1001F	7.0.17
FortiGate-3200F, FortiGate-3201F	7.0.17
FortiGate-3700F, FortiGate-3701F	7.0.17
FortiGate-4800F, FortiGate-4800F-DC FortiGate-4801F, FortiGate-4801F-DC, FortiGate-4801F-NEBS, FortiGate-4801F-DC-NEBS	7.0.17
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
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.16

FortiGate Model	FortiOS Version
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
FortiGateRugged-50G-5G	7.0.17
FortiGateRugged-70F, FortiGateRugged-70F-3G4G	7.0.17
FortiGateRugged-70G	7.0.15
FortiGateRugged-70G-5G-Dual	7.0.16
FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP	7.0.17
FortiWiFi-51G	7.0.17
FortiWiFi-51G-5G	7.0.15
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL	7.0.17

## 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 47](#).

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS <b>FortiCarrier 5000 Series:</b> FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier 6000 Series:</b> FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC <b>FortiCarrier 7000 Series:</b> 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	8.0

Model	Firmware Version
<p><b>FortiCarrier-DC:</b> FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4801F-DC-NEBS</p> <p><b>FortiCarrier-VM:</b> 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</p>	
<p><b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS</p> <p><b>FortiCarrier 5000 Series:</b> FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier 6000 Series:</b> 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><b>FortiCarrier 7000 Series:</b> 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><b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3000F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4800F-DC, FortiCarrier-4801F-DC, FortiCarrier-4801F-DC-NEBS</p> <p><b>FortiCarrier-VM:</b> FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen</p>	7.6

Model	Firmware Version
<p><b>FortiCarrier:</b> FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS</p> <p><b>FortiCarrier 5000 Series:</b> FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier 6000 Series:</b> 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><b>FortiCarrier 7000 Series:</b> 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><b>FortiCarrier-DC:</b> FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4801F-DC-NEBS</p> <p><b>FortiCarrier-VM:</b> 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</p>	7.4
<p><b>FortiCarrier:</b> FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS</p> <p><b>FortiCarrier 5000 Series:</b> FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier 6000 Series:</b> 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><b>FortiCarrier 7000 Series:</b> 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>	7.2

Model	Firmware Version
<b>FortiCarrier-DC:</b> FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4801F-DC-NEBS	
<b>FortiCarrier-VM:</b> FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 8.0.0 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see [FortiCarrier models on page 44](#).

### FortiCarrier 7.4

FortiCarrier Model	FortiCarrier Version
FortiCarrier-3800G, FortiCarrier-3801G	7.4.8

### FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version
FortiCarrier-3200F, FortiCarrier-3201F	7.0.17
FortiCarrier-3700F, FortiCarrier-3701F	7.0.17
FortiCarrier-4800F, FortiCarrier-4800F-DC FortiCarrier-4801F, FortiCarrier-4801F-DC, FortiCarrier-4801F-NEBS, FortiCarrier-4801F-DC-NEBS	7.0.17
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
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.16

FortiCarrier Model	FortiCarrier Version
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

## FortiADC models

Model	Firmware Version
<p><b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-320F, FortiADC-400F, FortiADC-420F, FortiADC-1000F, FortiADC-1000G, FortiADC-1200F, FortiADC-2000F, FortiADC-2000G, FortiADC-2200F, FortiADC-4000F, FortiADC-4000G, FortiADC-4200F, FortiADC-5000F, FortiADC-5000G</p> <p><b>FortiADC VM:</b> FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVERT, FortiADC-VM</p>	7.6
<p><b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-320F, FortiADC-400F, FortiADC-420F, FortiADC-1000F, FortiADC-1200F, FortiADC-2000F, FortiADC-2200F, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F</p> <p><b>FortiADC VM:</b> FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVERT, FortiADC-VM</p>	7.6
<p><b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-320F, 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</p> <p><b>FortiADC VM:</b> FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVERT, FortiADC-VM</p>	7.4
<p><b>FortiADC:</b> 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</p> <p><b>FortiADC VM:</b> FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVERT, FortiADC-VM</p>	6.2, 7.0, 7.1, 7.2

## FortiAnalyzer models

Model	Firmware Version
<p><b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3750G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD</p> <p><b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, 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-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen</p>	8.0
<p><b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3750G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD</p> <p><b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen</p>	7.6
<p><b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3750G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD</p> <p><b>FortiAnalyzer VM:</b> 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-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen</p>	7.4

Model	Firmware Version
<p><b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD</p> <p><b>FortiAnalyzer VM:</b> 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-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen</p>	7.2
<p><b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD</p> <p><b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-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-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen</p>	7.0

## FortiAnalyzer-BigData models

Model	Firmware Version
<p><b>FortiAnalyzer-BigData:</b> FortiAnalyzer-BigData-4500F</p> <p><b>FortiAnalyzer-BigData VM:</b> FortiAnalyzer-BigData-VM64</p>	7.2
<p><b>FortiAnalyzer-BigData:</b> FortiAnalyzer-BigData-4500F</p> <p><b>FortiAnalyzer-BigData VM:</b> FortiAnalyzer-BigData-VM64</p>	7.0

## FortiAuthenticator models

Model	Firmware Version
<p><b>FortiAuthenticator:</b> FAC-300F, FAC-800F</p>	7.0, 8.0

Model	Firmware Version
<b>FortiAuthenticator VM:</b> FAC-VM	
<b>FortiAuthenticator:</b> FAC-200E, FAC-300F, FAC-400E, FAC-800F, FAC-2000E, FAC-3000E, FAC-3000F <b>FortiAuthenticator VM:</b> FAC-VM	6.5, 6.6
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E, FAC-3000F <b>FortiAuthenticator VM:</b> FAC-VM	6.4
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	6.0, 6.1, 6.2, 6.3

## FortiCache models

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

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-1500G, FortiDDoS-1500G-LR, FortiDDoS-2000F, FortiDDoS-2000G, FortiDDoS-3000F, FortiDDoS-3000G, FortiDDoS-4000G <b>FortiDDoS VM:</b> FortiDDoS-VM	7.2
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-1500G, FortiDDoS-1500G-LR, FortiDDoS-2000F, FortiDDoS-2000G, FortiDDoS-3000F, FortiDDoS-3000G <b>FortiDDoS VM:</b> FortiDDoS-VM	7.0
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.4, 6.5, 6.6
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.3

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.2
<b>FortiDDoS:</b> 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
<b>FortiDeceptor:</b> FDC-100G, FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	5.0, 5.1, 5.2, 5.3, 6.0, 6.1, 6.2
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.3

## FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 8.0.0 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version
<b>FortiFirewall:</b> FortiFirewall-1801F, FortiFirewall-2600F, FortiFirewall-3001F, FortiFirewall-3501F, FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F, FortiFirewall-4801F-NEBS <b>FortiFirewall DC:</b> FortiFirewall-3001F-DC, FortiFirewall-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC, FortiFirewall-4801F-DC-NEBS <b>FortiFirewall-VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.4, 7.6, 8.0
<b>FortiFirewall:</b> FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F, FortiFirewall-4801F-NEBS <b>FortiFirewall DC:</b> FortiFirewall-4200F-DC, FortiFirewall-4401F-DC, FortiFirewall-4801F-DC-NEBS <b>FortiFirewall-VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2

## FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 8.0.0 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS <b>FortiFirewallCarrier DC:</b> FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC, FortiFirewallCarrier-4801F-DC-NEBS <b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.6, 8.0
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-1801F, FortiFirewallCarrier-2600F, FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS <b>FortiFirewallCarrier DC:</b> FortiFirewallCarrier-1801F-DC, FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC, FortiFirewallCarrier-4801F-DC-NEBS <b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.4
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-2600F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS <b>FortiFirewallCarrier DC:</b> FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4801F-DC-NEBS <b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.2
<b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.0

## FortiFirewall special branch models

Model	Firmware Version	Firmware Build
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-1801F, FortiFirewallCarrier-4401F	7.2.6	4609

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-900G, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E <b>FortiMail VM:</b> 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	7.6
<b>FortiMail:</b> FE-60D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E <b>FortiMail VM:</b> 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	7.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E <b>FortiMail VM:</b> 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	7.2
<b>FortiMail:</b> 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 <b>FortiMail VM:</b> 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	7.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E <b>FortiMail VM:</b> 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, <b>FortiMail Cloud</b>	6.2, 6.4

## FortiPAM models

Model	Firmware Version
<b>FortiPAM:</b> FortiPAM-100G, FortiPAM-400G, FortiPAM-1000G, FortiPAM-1100G, FortiPAM-3000G, FortiPAM-3100G <b>FortiPAM VM:</b> FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.8
<b>FortiPAM:</b> FortiPAM-1000G, FortiPAM-3000G <b>FortiPAM VM:</b> FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	7.6
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	7.4
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2
<b>FortiProxy:</b> FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G <b>FortiProxy VM:</b> FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	7.0
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E <b>FortiProxy VM:</b> FortiProxy-KVM, FortiProxy-VM64	1.0, 1.1, 1.2, 2.0

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, FSA-3000F <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FSA-AliCloud, FSA-AliCloud-Nested, FSA-AWS, FSA-AWS-Nested, FSA-Azure, FSA-Azure-Nested, FSA-Cloud, FSA-GCP, FSA-GCP-Nested, FSA-HYPERV, FSA-KVM, FSA-OCI-Nested, FSA-VM	5.0
<b>FortiSandbox:</b> FSA-500F, FSA-500G, FSA-1000D, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FSA-AWS, FSA-Cloud, FSA-VM	4.2, 4.4
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FSA-AWS, FSA-Cloud, FSA-VM	4.0
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.2

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FortiSOAR-VM	7.2, 7.3, 7.4, 7.5, 7.6

## FortiSRA models

Model	Firmware Version
<b>FortiSRA-VM:</b> FortiSRA-Azure, FortiSRA-HyperV, FortiSRA-KVM, FortiSRA-VM64	1.4, 1.5, 1.6, 1.7
<b>FortiSRA:</b> FortiSRA-1000G, FortiSRA-3000G	1.0, 1.1
<b>FortiSRA-VM:</b> FortiSRA-Azure, FortiSRA-HyperV, FortiSRA-KVM, FortiSRA-VM64	

## FortiTester models

Model	Firmware Version
<b>FortiTester:</b> FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F	7.1, 7.2, 7.3, 7.4
<b>FortiTester VM:</b> 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	

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-100E, FortiWeb-100F, FortiWeb-400D, FortiWeb-400E, FortiWeb-400F, FortiWeb-600D, FortiWeb-600E, FortiWeb-600F, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000E, FortiWeb-4000F	8.0
<b>FortiWeb VM:</b> FortiWeb-AWS, FortiWeb-AWS_OnDemand, FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
<b>FortiWeb Cloud</b> , including FortiAppSec Cloud.	

Model	Firmware Version
<p><b>FortiWeb:</b> 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><b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p><b>FortiWeb Cloud</b>, including FortiAppSec Cloud.</p>	7.6
<p><b>FortiWeb:</b> 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><b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p><b>FortiWeb Cloud</b>, including FortiAppSec Cloud.</p>	7.4
<p><b>FortiWeb:</b> 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> <p><b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p><b>FortiWeb Cloud</b>, including FortiAppSec Cloud.</p>	7.2
<p><b>FortiWeb:</b> 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><b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p> <p><b>FortiWeb Cloud</b>, 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.

# Resolved issues

The following issues have been fixed in 8.0.0. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
1172122	During policy installation, SSID configurations may be unintentionally removed from the radio interfaces of FortiAPs.
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, FortiManager may suggest to "set ddscan enable" during the 1st installation, and this may create some issue on FortiAPs connected to the FortiGate.
1198357	AP Manager encounters issues with central AP management because some channels may not be supported.
1204035	FortiAP-231K is not supported by FortiManager.
1218302	FortiAP status becomes Unknown shortly after refreshing the AP table.
1239191	When SSID configured with per-device mapping, during the installation, the FortiManager will report error: Commit failed: ssid fortinet is used by vap.

## Device Manager

Bug ID	Description
970157	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.
989507	The visibility (eye) icon is not displayed in the Pre-shared Key field within IPsec template configurations. Furthermore, FortiManager does not support the use of metadata variables for the "Pre-shared Key" and "XAUTH" parameters.
1001557	Metadata variables are not supported for the "XAUTH" field in IPsec tunnel provisioning templates.
1015138	Unable to edit interface with dhcp reservation.

Bug ID	Description
1102790	FortiManager pushes the unset auto-connect command to config system lte-modem, where the default value is disabled on FortiOS but still enabled on FortiManager.
1155534	An error occurs when disabling the IP Range Managed by IPAM option on the VLAN interface.
1167831	Security-mode configuration is removed when FortiManager installs interface configuration on aggregate interfaces Workaround: Enable security mode on the FGT locally, then retrieve the config to sync the status back on FMG
1173182	CLI Template Installation Fails with error message "SSID rename not allowed".
1176593	Install Wizard hangs with no display for install preview window after making changes to device settings under a VDOM.
1176785	Getting error while importing certificate "no write permission to do this operation".
1191558	Changes to SD-WAN performance SLA values are not reflected in the device database or the install preview when the detect-mode is set to remote.
1198163	When installing an SD-WAN static route via a template, the push fails with a duplicated route error.
1201252	The static route template triggers duplicate-route errors during installation because duplicate routes, including those using blackhole interfaces, are not allowed.
1202467	ADOM 7.4 converts SD-WAN rules route-tags into empty route-tag address objects, breaking compatibility with FortiOS 7.2 devices
1202695	FortiGate 90G/91G Gen2 are not supported in Device Model.
1204427	Script log results do not display logs from the most recent script execution; only logs from previous executions are shown.
1208974	Device count is not correct.
1215090	Unable to retrieve correct setting of device-identification in system interface.
1215217	The install preview does not load if a device in the device group is offline, but it works fine if all the devices are online.
1218504	The Replacement Message page may fail to load when ADOM mode is set to Advanced. This issue occurs when the VDOM used to edit the replacement message group is not located in the same ADOM as the management (root) VDOM.
1219062	"sla-compare-method" still available on SDWAN rules when load balance is enabled.
1240231	After upgrading FortiManager, remote access to FortiGate devices may fail with the error Error reading from remote server when using non-standard ports.
1244586	Installation failure occurs when unsetting the "allow-traffic-redirect" under the system global.
1246821	FortiManager retrieval may fail when an admin's remote-group exists only in the root VDOM and the VDOM order starts with a non-root VDOM, causing invalid reference detection during device addition.

Bug ID	Description
1251613	Registration of FortiGate-VM64-KVM as Device model to FortiManager may fail due to incorrect platform identification.
1254998	Incorrect Interface Syntax Selection for FGT90G/91G Gen1/Gen2 During Model Device (ZTP) Creation has been observed.

## FortiSwitch Manager

Bug ID	Description
1193285	When changing the name of a FortiSwitch from FortiSwitch Manager, the next Installation will reset the ports configuration of the switch to default configuration.
1227473	FortiManager attempts to install set poe-status disable on FortiSwitch ports that already have PoE disabled. The issue persists and reoccurs after configuration installation and synchronization.
1118271	FortiSwitch Device information is not displayed when FortiSwitch version is 7.4.3.
1244165	When centrally managing switches via FortiManager, the "Switch-id" is limited to 16 characters. Configuring a hostname exceeding this limit triggers the error: "Switch-id: Value too long."

## Global ADOM

Bug ID	Description
1177672	When global policy package assignment fails, it may impacts the policy packages on the ADOM.
1182076	Renamed global objects are not reflected with their new names in associated policies.
1183101	Not able to delete firewall objects from the global database after upgrading FortiManager from 7.2 (7.2.10).
1201449	Global policy assignment configured with Automatically Install Policies to ADOM Devices may get stuck during deployment.
1232811	Unassigning a Global Policy Package may fail when it is referenced by SSL inspection profiles in the root ADOM.

## Others

Bug ID	Description
1077126	The FortiExtender API connection status is returning incorrect value for the FortiExtender device when in an "unknown" state.
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is enabled.
1099753	Insertion of empty policy rules is not possible when FortiProxy 7.2 ADOM is configured in FortiManager.
1099773	FortiExtender page 'Data Usage' value does not display the updated values.
1146320	After creating the SSID and assigning it to the FortiExtender profile, the configuration is not pushing to the FortiGate, resulting in an installation failure.
1158842	The FortiManager dashboard FortiGuard license status does not display the same data as shown on the FortiGuard page.
1177268	FortiFirewall license validation fails on FortiManager configured as local FDS.
1185269	The local log syslog feature set facility is not functioning properly.
1194429	FortiGuard Query Services displays an incorrect date for the Query Status when viewing the Number of Queries graph.
1199504	When Workspace is in Workflow mode, the fmg-admin may observe "You have no write permission to do this operation" error message when attempting to modify an interface.
1201751	Unable to add managed FortiAnalyzer to FortiManager.
1203535	FortiManager does not support the diagnose fdsm fap-fsw-contract-download request, so the fgdhttpd daemon rejects FortiGate attempts to retrieve FortiAP/FortiSwitch registration status.
1210519	Central-management settings are deleted on the primary unit when adding a FortiProxy HA cluster via Device Discover. This issue may occur when the FortiManager ADOM is configured in backup mode and the FortiProxy central-management setting is also set to the backup mode. Refreshing the device may trigger the issue.
1211261	Users might experience "Attempting to reconnect" messages every few minutes while logged in to the GUI.
1216181	GUI access may fail when FGT default fds port is 443, FMG does not have secondary IP, and Apache is in event mode.
1217534	During an upgrade of an FortiGate-HA cluster via FortiManager, if the disk-check feature is enabled, it may cause all cluster members to reboot simultaneously. This can result in an unexpected traffic interruption.
1217951	FortiManager may not recognize the 1000F serial number as valid for applying the corresponding Device Blueprint, preventing the CSV file from being loaded.

Bug ID	Description
1224258	The new EMS version has upgraded its communication protocol from HTTP/1.0 to HTTP/2. Unlike HTTP/1.x, HTTP/2 does not return a traditional 200 OK text response, so older FortiManager versions that expect this format cannot interpret the new HTTP/2 replies. Because of this, older FortiManager builds will not be compatible with the latest EMS version.
1224460	After the upgrade, policy installation fails with a normalized interface error. The issue appears to be related to dynamic mapping validation failures.
1228166	Running <code>diagnose dvm check-integrity</code> on already corrupt DB may cause unintended behavior.
1230277	If the ADOM in an earlier FortiManager version contains DLP dictionary entries named <code>fg-*</code> which are reserved in FortiManager 7.6 the upgrade from ADOM 7.4 to 7.6 will fail. The upgrade process attempts to copy these reserved-name objects, but ADOM 7.6 does not allow them to be created or modified.
1234093	Time discrepancy occurs between formatted and raw logs when using GMT timezone.
1244008	When FortiAnalyzer is added as a managed device in FortiManager, executing any of the "diagnose cdb upgrade check" commands may result in an unexpected behavior in the CLI.
1246091	FortiOS 7.4.10 is partially supported by FortiManager 7.6.5/7.6.6.
1247597	FortiManager is unable to sync user information from the pxGrid connector.
1251516	Installation failure occurs when pushing primus HSM ( on-premises Hardware Security Module) settings via provisioning templates to FortiProxy.

## Policy and Objects

Bug ID	Description
1083504	FortiManager attempts to configure the service in the ISDB6 policy (IPv6), but FortiOS rejects it, causing the installation to fail.
1101351	Unable to create ZTNA Server with SAML SSO server.
1139663	When using the Install Object(s) function after renaming an object, FortiManager pushes the old object name to the firewall policy.
1156437	No interface mapping listed when importing config for a device (device mapping undefined).
1169058	Installation might fail to these devices "FGT/FWF-30G/31G" due to some unsupported syntax.
1170381	Unable to create new section "Add Section" in policy after upgrade FortiManager while using interface pair view mode. Operation "Add Section" triggers nothing. Field "label" or "global-label" are empty.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager.

Bug ID	Description
1174618	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.
1181585	"Where Used" feature does not function.
1185738	During the auto-linking process, FortiManager attempts to push a policy package containing Internet-Service based rules, but the FortiGates outdated ISDB causes the installation to fail.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1194560	Missing CASB applications occur when FortiManager fetches casb application data without the 'get reserved' option.
1196308	EMS server security posture tags are not fully synchronized with FortiManager; ZTNA tags comment are missing.
1198075	Upon any modification, policy installation will result in attempt to purge dns-database even though no changes are made to dns database.
1202792	The installation may fail with a Current passphrase is invalid error. This can occur when installing an SSID with an MPSK profile, where the MPSK passphrase is not inherited during copy operations or after a FortiManager upgrade.
1203219	A Security Posture Tag installation issue may occur when configuring IP/MAC-based ZTNA rules on lower-end devices such as the FortiGate-60F.
1209756	Policy package installation fails for FGT-30G due to SSL VPN settings not supported by this FortiGate model.
1211860	Existing Objects shown as "Not found" in "Where Used".
1212118	Reinstalling policy packages for more than three devices may cause the Application Security Console to crash.
1215309	Installation hang when pushing configurations to firewall groups.
1215335	Redundant policy sub-sections are displayed in the UI after the upgrade.
1215349	FortiManager may delete policies or settings during device installation due to concurrent database interactions from tasks like auto-updates, policy installs, or HA-related updates running simultaneously.
1216601	When attempting to merge duplicate objects, a Minified React error is observed.
1218648	Alternative Resources setting under AWS connector is not pushed to FortiGate.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.
1224598	The Policy Package Diff does not display any differences and throws an error.
1230592	An error condition in the security console occurs when reinstalling a previous policy package after upgrading ADOM from v7.4 to v7.6.
1235065	When loading an ssh cert, there is no password option and encrypted keys are not accepted.

Bug ID	Description
1240260	When the Policy Package setting "Policy Offload Level" is set to Default mode, the Copy Policy Validation may fail and display an error log "COMMIT FAIL - invalid value".
1240764	Users may experience slowness when loading large policy packages while switching between Interface Pair views.
1242707	Policy package status does not change to "Out of Sync" on FMG when local changes are made on FortiGate.
1245964	In FortiOS 7.4.10, CLI syntax changes can cause install failures on low-memory (2GB) models when pushing configuration for: <ul style="list-style-type: none"> <li>web-proxy global proxy-fqdn</li> <li>firewall ssl-ssh-profile ssh</li> </ul>
1247668	Importing firewall policies may fail when adding an FortiGate with a large number of policies (e.g., over 60K).
1252128	Firewall Policy object lists are auto-compressed when more than 3 objects per rule are present.
1255176	Policy package installation may stuck when dynamic mapping member of a "firewall addrgrp" is empty.
1257115	Policy package installation may fail on hardware devices when policy-offload-level is set to default.
1257828	Searching in Policy Packages/Policies with certain keywords may result in an unexpected error.

## Revision History

Bug ID	Description
1248791	ADOM revision history may be lost when upgrading the ADOM to version 7.6.

## System Settings

Bug ID	Description
1008397	An fmg-admin with root ADOM access and RW/RO permissions for system settings can execute CLI commands to view data from other ADOMs.
1086386	Unable to save changes for SNMP users in FortiManager if more than one notification host is configured.

Bug ID	Description
1196401	SAML authentication fails to process all multi-valued groupmatch attributes and does not follow the FortiManager configuration order.
1238985	In a VRRP HA setup, the 3rd and 4th HA members may not properly synchronize with the primary.
1259170	When running version 8.0.0 BETA 2, the GUI may display a red message at the top of the page indicating that the image is not certified for virtual or hardware platforms.

## VPN Manager

Bug ID	Description
1256324	Installation may fail after creating VPN communities of any type.

# 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 8.0.0.

### Others

Bug ID	Description
1283931	When FortiManager operates in Workflow mode, changes to the global ADOM database may not be reflected in local ADOMs after assigning a Global Policy Package. A session is created; however, the View Diff function returns "No Difference."

### Policy and Objects

Bug ID	Description
1282087	FortiManager for each policy Installation consistently pushes "config endpoint-control fctems" to configure out-of-sync-threshold 180. While this does not cause an installation failure, the change is reapplied during every install operation.

## Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 8.0.0.

## Device Manager

Bug ID	Description
980362	The Firmware Version column in Device Manager incorrectly shows "Upgrading FortiGate from V1 to V2" even after a successful upgrade has been completed.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1136726	Enabling the Power Supply Failure option in an SNMP v2 configuration applied via a System Template results in the following installation error: multi-option(power-blade-down) not exist".

## Others

Bug ID	Description
1169450	When Backup ADOM is enabled and auto-sync is configured, FortiManager is not able to automatically retrieve the changes from FortiGate devices. Devices should remain in sync without the need for manual retrieval.
1196043	Failed to create Alert Handlers or Reports on FortiManager when a Fortinet Fabric Connection is established on FortiAnalyzer to connect to the FortiManager device. <b>Workaround:</b> Go back to the specific ADOM on FortiAnalyzer and create the Alert Handlers or Reports there. After synchronization, the new entries should become available on FortiManager.

## Policy and Objects

Bug ID	Description
1160047	Application control category "GenAI" is missing in FortiManager, but present in FortiGate. <b>Workaround:</b> 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.

## System Settings

Bug ID	Description
1158131	The GUI permits configuring the management port to a port number already in use, resulting in loss of access to the GUI.

# 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	✓	✓	✓
FortiProxy	✓	✓	✓
FortiSandbox	✓	✓	✓
FortiSOAR	✓		
FortiTester	✓		✓
FortiWeb	✓		✓
FortiPAM	✓		✓

# 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](http://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.