

# Release Notes

**FortiManager 7.2.10**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



May 9, 2025

FortiManager 7.2.10 Release Notes

02-7210-1115714-20250509

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 7.2.10 Release</b>	<b>7</b>
Supported models	7
FortiManager VM subscription license	7
Management extension applications	8
Supported models for MEA	8
Minimum system requirements	8
<b>Special Notices</b>	<b>10</b>
Adding VM devices to FortiManager	10
The names of policies derived from policy blocks no longer automatically include the policy block name	10
Custom certificate name verification for FortiGate connection	11
Shell access has been removed	11
Enable fcp-cfg-service for Backup Mode ADOMs	11
Configuration backup requires a password	12
Additional configuration required for SSO users	12
When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade	12
Apache-mode changed from prefork to event	13
FortiGuard web filtering category v10 update	13
Install On column for policies	13
FortiManager 7.2.3 and later firmware on FortiGuard	14
Option to enable permission check when copying policies	14
Management Extensions visibility in the GUI	14
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	15
SD-WAN Orchestrator removed in 7.2	15
Changes to FortiManager meta fields	15
Setup wizard requires FortiCare registration	15
Access lists as ADOM-level objects	16
View Mode is disabled in policies when policy blocks are used	16
Reconfiguring Virtual Wire Pairs (VWP)	16
Scheduling firmware upgrades for managed devices	16
Modifying the interface status with the CLI	17
SD-WAN with upgrade to 7.0	17
Citrix XenServer default limits and upgrade	17
Multi-step firmware upgrades	18
Hyper-V FortiManager-VM running on an AMD CPU	18
SSLv3 on FortiManager-VM64-AWS	18

<b>New features</b>	<b>19</b>
<b>Upgrade Information</b>	<b>20</b>
Downgrading to previous firmware versions	20
Firmware image checksums	21
FortiManager VM firmware	21
SNMP MIB files	22
FortiManager instances on Azure Stack	22
<b>Product Integration and Support</b>	<b>23</b>
Supported software	23
Web browsers	24
FortiOS and FortiOS Carrier	24
FortiADC	24
FortiAnalyzer	24
FortiAnalyzer-BigData	25
FortiAuthenticator	25
FortiCache	25
FortiClient	25
FortiDDoS	25
FortiDeceptor	26
FortiFirewall and FortiFirewallCarrier	26
FortiMail	26
FortiPAM	26
FortiProxy	26
FortiSandbox	27
FortiSOAR	27
FortiSwitch	27
FortiTester	27
FortiWeb	28
Virtualization	28
Feature support	29
Language support	30
Supported models	30
FortiGate models	31
FortiGate special branch models	34
FortiCarrier models	36
FortiCarrier special branch models	38
FortiADC models	39
FortiAnalyzer models	39
FortiAnalyzer-BigData models	40
FortiAuthenticator models	40
FortiCache models	41
FortiDDoS models	41
FortiDeceptor models	41
FortiFirewall models	42
FortiFirewallCarrier models	43
FortiMail models	44
FortiPAM models	45
FortiProxy models	45

FortiSandbox models .....	45
FortiSOAR models .....	46
FortiSwitch models .....	46
FortiTester models .....	46
FortiWeb models .....	47
<b>Resolved Issues .....</b>	<b>48</b>
AP Manager .....	48
Device Manager .....	48
FortiSwitch Manager .....	49
Others .....	49
Policy and Objects .....	50
Script .....	51
Services .....	51
System Settings .....	52
VPN Manager .....	52
Common Vulnerabilities and Exposures .....	52
<b>Known issues .....</b>	<b>53</b>
New known issues .....	53
Device Manager .....	53
Others .....	53
Existing known issues .....	53
AP Manager .....	53
Device Manager .....	54
Others .....	54
Policy & Objects .....	55
VPN Manager .....	55
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>56</b>
FortiGuard Center update support .....	56
<b>Appendix B - Default and maximum number of ADOMs supported .....</b>	<b>57</b>
Hardware models .....	57
Virtual Machines .....	57

# Change Log

Date	Change Description
2025-02-12	Initial release.
2025-02-18	Added information to "Custom certificate name verification for FortiGate connection" in <a href="#">Special Notices on page 10</a> . Updated <a href="#">Resolved Issues on page 48</a> and <a href="#">Known issues on page 53</a> . Updated <a href="#">Virtualization on page 28</a> .
2025-02-25	Updated <a href="#">Known issues on page 53</a> .
2025-03-05	Updated <a href="#">Known issues on page 53</a> .
2025-03-13	Updated <a href="#">Resolved Issues on page 48</a> .
2025-04-09	Updated <a href="#">FortiProxy on page 26</a> .
2025-04-14	Updated <a href="#">Known issues on page 53</a> .
2025-04-21	Updated <a href="#">Resolved Issues on page 48</a> .
2025-04-29	Updated <a href="#">Web browsers on page 24</a> .
2025-05-01	Added <a href="#">New features on page 19</a> .
2025-05-09	Updated <a href="#">Feature support on page 29</a> .

# FortiManager 7.2.10 Release

This document provides information about FortiManager version 7.2.10 build 1682.



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

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 8](#)

## Supported models

FortiManager version 7.2.10 supports the following models:

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



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

## FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 21](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 57](#).

# Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.2.10.



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

## Supported models for MEA

As of FortiManager 7.2.3, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one MEA is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

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

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

## Minimum system requirements

By default FortiManager VMs use the following system resource settings:

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

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

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

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

Management Extension Application	Minimum system requirements	Recommended system resources for production*
<b>FortiAIOps</b>	<ul style="list-style-type: none"> <li>• 8 vCPU</li> <li>• 32 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	No change
<b>FortiSigConverter</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSOAR</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	<ul style="list-style-type: none"> <li>• 16 vCPU</li> <li>• 64 GB RAM</li> <li>• No change for disk storage</li> </ul>
<b>Policy Analyzer</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>Universal Connector</b>	<ul style="list-style-type: none"> <li>• 1 GHZ vCPU</li> <li>• 2 GB RAM</li> <li>• 1 GB disk storage</li> </ul>	No change
<b>Wireless Manager (FortiWLM)</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change

\*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.2.10.

## Adding VM devices to FortiManager

As of FortiManager 7.2.10, 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 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.

## Custom certificate name verification for FortiGate connection



In FortiManager 7.2.10, the `fgfm-peer-cert-without-sn` 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 7.2.5 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 7.2.5, 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.

## Shell access has been removed

As of FortiManager 7.2.6, 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
```

## Configuration backup requires a password

As of FortiManager 7.2.5, 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](#).

## Additional configuration required for SSO users

Beginning in 7.2.5, 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 7.2.5 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 7.2.5 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 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 v7.2.5 or later.

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

### **Workaround:**

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

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

## Apache-mode changed from prefork to event

Before version 7.2.3, the default "apache-mode" utilized the "prefork" mode. However, starting from version 7.2.4, the default configuration switches to the "event" mode.

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

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

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

## FortiGuard web filtering category v10 update

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

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

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

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

## Install On column for policies

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

## FortiManager 7.2.3 and later firmware on FortiGuard

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

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

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

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

## Option to enable permission check when copying policies

As of 7.2.3, a new command is added in the CLI:

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

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

## Management Extensions visibility in the GUI

As of FortiManager 7.2.3, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one management extension application (MEA) is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

## FortiManager creates faulty dynamic mapping for VPN manager interface during PP import

If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for *VPN Manager*.

It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database:

```
diagnose cdb check policy-packages <adom>
```

After executing this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

## SD-WAN Orchestrator removed in 7.2

Starting in 7.2.0, the SD-WAN Orchestrator is no longer available in FortiManager. Instead, you can use the *SD-WAN Overlay Template* wizard to configure your SD-WAN overlay network.

For more information, see [SD-WAN Overlay Templates](#) in the FortiManager Administration Guide.

## Changes to FortiManager meta fields

Beginning in 7.2.0, FortiManager supports policy object metadata variables.

When upgrading from FortiManager 7.0 to 7.2.0 and later, FortiManager will automatically create ADOM-level metadata variable policy objects for meta fields previously configured in System Settings that have per-device mapping configurations detected. Objects using the meta field, for example CLI templates, are automatically updated to use the new metadata variable policy objects.

Meta fields in *System Settings* can continue to be used as comments/tags for configurations.

For more information, see [ADOM-level meta variables for general use in scripts, templates, and model devices](#).

## Setup wizard requires FortiCare registration

Starting in FortiManager 7.2.1, the FortiManager Setup wizard requires you to complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM. Previously the step was optional.

For FortiManager units operating in a closed environment, contact customer service to receive an entitlement file, and then load the entitlement file to FortiManager by using the CLI.

## Access lists as ADOM-level objects

Starting in 7.2.0, FortiManager supports IPv4 and IPv6 access list firewall policies as ADOM-level object configurations from FortiGate. Previously, these access lists were controlled by the device database/FortiGate configuration.

After upgrading to 7.2.0 from an earlier release, the next time you install changes to a FortiGate device with an IPv4 or IPv6 access list firewall policy (`config firewall acl/acl6`), FortiManager will purge the device database/FortiGate configuration which may have previously contained the access list.

To address this, administrators can re-import the FortiGate policy configuration to an ADOM's policy package or re-create the IPv4/IPv6 access list firewall policy in the original package.

## View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain policies with multiple interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

## Reconfiguring Virtual Wire Pairs (VWP)

A conflict can occur between the ADOM database and device database when a Virtual Wire Pair (VWP) is installed on a managed FortiGate that already has a configured VWP in the device database. This can happen when an existing VWP has been reconfigured or replaced.

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

## Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

## Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from `up/down` to `enable/disable`.

For example:

```
config system interface
  edit port2
    set status <enable/disable>
  next
end
```

## SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

**To increase the size of the ramdisk setting:**

1. On Citrix XenServer, run the following command:  
`xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912`
2. Confirm the setting is in effect by running `xenstore-ls`.  
-----  
`limits = ""`  
`pv-kernel-max-size = "33554432"`  
`pv-ramdisk-max-size = "536,870,912"`  
`boot-time = ""`  
-----
3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

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

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

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol tlsv1
end
```

# New features

For information about what's new in FortiManager 7.2.10, see the [FortiManager 7.2 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.

See [FortiManager 7.2.10 Upgrade Guide](#).

---

You can upgrade FortiManager 7.0.1 or later directly to 7.2.10.

---



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

For example, FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0, but FortiManager 7.2 supports ADOM versions 6.4, 7.0, and 7.2. Before you upgrade FortiManager 7.0 to 7.2, ensure that all ADOM 6.2 versions have been upgraded to ADOM version 6.4 or later. See [FortiManager 7.2.10 Upgrade Guide](#).

---

This section contains the following topics:

- [Downgrading to previous firmware versions on page 20](#)
- [Firmware image checksums on page 21](#)
- [FortiManager VM firmware on page 21](#)
- [SNMP MIB files on page 22](#)
- [FortiManager instances on Azure Stack on page 22](#)

## Downgrading to previous firmware versions

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

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

# Firmware image checksums

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

## FortiManager VM firmware

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

### Amazon Web Services

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

### Citrix XenServer and Open Source XenServer

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

### Google Cloud Platform

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

### Linux KVM

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

### Microsoft Azure

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

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

### Microsoft Hyper-V Server

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

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



Microsoft Hyper-V 2016 is supported.

---

### Oracle Private Cloud

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

### VMware ESX/ESXi

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



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

---

## SNMP MIB files

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

## FortiManager instances on Azure Stack

After upgrading FortiManager on Azure Stack from version 7.2.3 to 7.2.4, the instance will become unreachable. To re-establish connectivity, dissociate the Public IP of the instance and then re-associate it via the Azure Stack client portal.

# Product Integration and Support

This section lists FortiManager 7.2.10 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [Supported software on page 23](#)
- [Feature support on page 29](#)
- [Language support on page 30](#)
- [Supported models on page 30](#)

## Supported software

FortiManager 7.2.10 supports the following software:

- [Web browsers on page 24](#)
- [FortiOS and FortiOS Carrier on page 24](#)
- [FortiADC on page 24](#)
- [FortiAnalyzer on page 24](#)
- [FortiAnalyzer-BigData on page 25](#)
- [FortiAuthenticator on page 25](#)
- [FortiCache on page 25](#)
- [FortiClient on page 25](#)
- [FortiDDoS on page 25](#)
- [FortiDeceptor on page 26](#)
- [FortiFirewall and FortiFirewallCarrier on page 26](#)
- [FortiMail on page 26](#)
- [FortiPAM on page 26](#)
- [FortiProxy on page 26](#)
- [FortiSandbox on page 27](#)
- [FortiSOAR on page 27](#)
- [FortiSwitch on page 27](#)
- [FortiTester on page 27](#)
- [FortiWeb on page 28](#)
- [Virtualization on page 28](#)



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

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

---



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

---

## Web browsers

FortiManager 7.2.10 supports the following web browsers:

- Google Chrome version 135
- Microsoft Edge version 135
- Mozilla Firefox 138

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

## FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.2.10 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiOS](#).

---

FortiManager 7.2.10 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0 to 7.2.11
- 7.0.0 to 7.0.17
- 6.4.0 to 6.4.16

## FortiADC

FortiManager 7.2.10 supports the following versions of FortiADC:

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

## FortiAnalyzer

FortiManager 7.2.10 supports the following versions of FortiAnalyzer:

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

## FortiAnalyzer-BigData

FortiManager 7.2.10 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

## FortiAuthenticator

FortiManager 7.2.10 supports the following versions of FortiAuthenticator:

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

## FortiCache

FortiManager 7.2.10 supports the following versions of FortiCache:

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

## FortiClient

FortiManager 7.2.10 supports the following versions of FortiClient:

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

## FortiDDoS

FortiManager 7.2.10 supports the following versions of FortiDDoS:

- 7.0.0 and later
- 6.6.0 and later
- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

Limited support. For more information, see [Feature support on page 29](#).

## FortiDeceptor

FortiManager 7.2.10 supports the following versions of FortiDeceptor:

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

## FortiFirewall and FortiFirewallCarrier

FortiManager 7.2.10 supports the following versions of FortiFirewall and FortiFirewallCarrier:

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

## FortiMail

FortiManager 7.2.10 supports the following versions of FortiMail:

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

## FortiPAM

FortiManager 7.2.10 supports the following versions of FortiPAM:

- 1.1.0 and later
- 1.0.0 and later

## FortiProxy

FortiManager 7.2.10 supports configuration management for the following versions of FortiProxy:

- 7.2.9 to 7.2.13
- 7.2.6 to 7.2.7
- 7.2.2 to 7.2.3

- 7.0.12 to 7.0.20
- 7.0.7 to 7.0.10



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 29](#).

---

FortiManager 7.2.10 supports logs from the following versions of FortiProxy:

- 7.2.0 to 7.2.13
- 7.0.0 to 7.0.20
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

## FortiSandbox

FortiManager 7.2.10 supports the following versions of FortiSandbox:

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

## FortiSOAR

FortiManager 7.2.10 supports the following versions of FortiSOAR:

- 7.3.0 and later
- 7.2.0 and later
- 7.0.0 and later

## FortiSwitch

FortiManager 7.2.10 supports the following versions of FortiSwitch:

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

## FortiTester

FortiManager 7.2.10 supports the following versions of FortiTester:

- 7.3.0 and later
- 7.2.0 and later
- 7.1.0 and later
- 7.0.0 and later
- 4.2.0 and later

## FortiWeb

FortiManager 7.2.10 supports the following versions of FortiWeb:

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

## Virtualization

FortiManager 7.2.10 supports the following virtualization software:

### Public Cloud

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

### Private Cloud

- Citrix XenServer 8.2 and later
- OpenSource XenServer 4.2.5
- Microsoft Hyper-V Server 2016, 2019, and 2022
- Nutanix
  - AHV 20220304 and later
  - AOS 6.5 and later
  - NCC 4.6 and later
  - LCM 3.0 and later
- RedHat 9.1
  - Other versions and Linux KVM distributions are also supported
- VMware ESXi versions 6.5 and later

## Feature support

The following table lists FortiManager feature support for managed platforms.

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

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

## Language support

The following table lists FortiManager language support information.

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

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

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

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch, FortiWeb, FortiCache, FortiProxy, FortiAuthenticator, and other Fortinet product models and firmware versions can be managed by a FortiManager or send logs to a FortiManager running version 7.2.10.



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

This section contains the following topics:

- [FortiGate models on page 31](#)
- [FortiGate special branch models on page 34](#)
- [FortiCarrier models on page 36](#)
- [FortiCarrier special branch models on page 38](#)
- [FortiADC models on page 39](#)
- [FortiAnalyzer models on page 39](#)

- [FortiAnalyzer-BigData models on page 40](#)
- [FortiAuthenticator models on page 40](#)
- [FortiCache models on page 41](#)
- [FortiDDoS models on page 41](#)
- [FortiDeceptor models on page 41](#)
- [FortiFirewall models on page 42](#)
- [FortiFirewallCarrier models on page 43](#)
- [FortiMail models on page 44](#)
- [FortiPAM models on page 45](#)
- [FortiProxy models on page 45](#)
- [FortiSandbox models on page 45](#)
- [FortiSOAR models on page 46](#)
- [FortiSwitch models on page 46](#)
- [FortiTester models on page 46](#)
- [FortiWeb models on page 47](#)

## 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 34](#).

Model	Firmware Version
<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-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-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 <b>FortiGate 5000 Series:</b> FortiGate-5001E, FortiGate-5001E1	7.2

Model	Firmware Version
<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 <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-2-DC, FortiGate-7081F-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC <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-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-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 <b>FortiWiFi:</b> FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-70G, FWF-71G, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE <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> FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G	
<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-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F,	7.0
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	

Model	Firmware Version
<p><b>FortiGate DC:</b> FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-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-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC</p> <p><b>FortiWiFi:</b> FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE</p> <p><b>FortiGate VM:</b> FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager</p> <p><b>FortiOS-VM:</b> FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen</p> <p><b>FortiGate Rugged:</b> FGR-60F, FGR-60F-3G4G</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-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F,</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC</p>	6.4

Model	Firmware Version
<b>FortiWiFi:</b> FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, VM64-GCPONDEMAND, 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> FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-60F, FGR-60F-3G4G	

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.2.10 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 31](#).

### FortiOS 7.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-30G	7.2.8	6390
FortiGate-31G	7.2.8	6464
FortiGate-70G, FortiGate-71G	7.2.8	6403
FortiGate-200G, FortiGate-201G	7.2.8	6397
FortiWiFi-30G	7.2.8	6390
FortiWiFi-31G	7.2.8	6464
FortiWiFi-70G, FortiWiFi-71G	7.2.8	6403

### FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE	7.0.17	7592
FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE	7.0.17	7592

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.17	7569
FortiGate-90G, FortiGate-91G	7.0.17	7571
FortiGate-120G, FortiGate-121G	7.0.16	7534
FortiGate-900G, FortiGate-900G-DC, FortiGate-901G, FortiGate-901G-DC	7.0.17	7573
FortiGate-1000F, FortiGate-1001F	7.0.17	7574
FortiGate-3200F, FortiGate-3201F	7.0.17	7575
FortiGate-3700F, FortiGate-3701F	7.0.17	7575
FortiGate-4800F, FortiGate-4800F-DC	7.0.17	7575
FortiGate-4801F, FortiGate-4801F-DC	7.0.17	7575
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.16	0280
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.16	0280
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-2-DC, FortiGate-7081F-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.16	0280
FortiGateRugged-50G-5G	7.0.17	7577
FortiGateRugged-70F, FortiGateRugged- 70F-3G4G	7.0.17	7570
FortiGateRugged-70G	7.0.15	7496
FortiGateRugged-70G-5G-Dual	7.0.16	7515
FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi- 50G-DSL, FortiWiFi-50G-SFP	7.0.17	7592
FortiWiFi-51G	7.0.17	7592
FortiWiFi-51G-5G	7.0.15	7537
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F- 2R-3G4G-DSL	7.0.17	7569

## FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F, FortiGate-400F-DC, FortiGate-401F, FortiGate-401F-DC	6.4.13	5455
FortiGate-600F, FortiGate-601F	6.4.13	5455
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	6.4.13	1926
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	6.4.13	1926
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-2-DC, FortiGate-7081F-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	6.4.13	1926
FortiWiFi-80F-2R-3G4G-DSL	6.4.7	5003

## 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 38](#).

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-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	7.2

Model	Firmware Version
<p><b>FortiCarrier 7000 Series:</b> FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7081F-2, FortiCarrier-7081F-2-DC, FortiCarrier-7081F-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-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-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC</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-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen</p>	
<p><b>FortiCarrier:</b> FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier-DC:</b> FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3000F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC</p> <p><b>FortiCarrier-VM:</b> FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM</p>	7.0
<p><b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC</p> <p><b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen</p>	6.4

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.2.10 supports these models on the identified FortiOS Carrier version and build number.

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

### FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.17	7575
FortiCarrier-3700F, FortiCarrier-3701F	7.0.17	7575
FortiCarrier-4800F, FortiCarrier-4800F-DC	7.0.17	7575
FortiCarrier-4801F, FortiCarrier-4801F-DC	7.0.17	7575
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.16	0280
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.16	0280
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7081F-2, FortiCarrier-7081F-2-DC, FortiCarrier-7081F-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.16	0280

### FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	6.4.13	1926

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	6.4.13	1926
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7081F-2, FortiCarrier-7081F-2-DC, FortiCarrier-7081F-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	6.4.13	1926

## FortiADC models

Model	Firmware Version
<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 <b>FortiADC VM:</b> FortiADC-VM	7.0, 7.1, 7.2

## FortiAnalyzer models

Model	Firmware Version
<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 <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-OPC, FortiAnalyzer-VM64-Xen	7.2
<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-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E	7.0

Model	Firmware Version
<b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E	6.4
<b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	

## FortiAnalyzer-BigData models

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

## FortiAuthenticator models

Model	Firmware Version
<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	6.4, 6.5, 6.6
<b>FortiAuthenticator VM:</b> FAC-VM	
<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	6.2, 6.3
<b>FortiAuthenticator VM:</b> FAC-VM	

## 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-2000F, FortiDDoS-3000F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.4, 6.5, 6.6, 7.0
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.3
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.2

## 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
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.3
<b>FortiDeceptor:</b> FDC-1000F, FDC-1000G <b>FortiDeceptor Rugged:</b> FDCR-100G <b>FortiDeceptor VM:</b> FDC-VM	4.2

## FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.2.10 supports these models on the identified FortiFirewall firmware version and build number.

### FortiFirewall 7.2

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

### FortiFirewall 7.0

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewall:</b> FortiFirewall-3001F	7.0.10	4955
<b>FortiFirewall:</b> FortiFirewall-3501F	7.0.10	4940
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC <b>FortiFirewall-VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.0	

### FortiFirewall 6.4

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewall:</b> FortiFirewall-1801F, FortiFirewall-2600F <b>FortiFirewall DC:</b> FortiFirewall-1801F-DC, FortiFirewall-2600F-DC	6.4.12	5423
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC	6.4	
<b>FortiFirewall:</b> FortiFirewall-4200F, FortiFirewall-4400F	6.4	1999
<b>FortiFirewall:</b> FortiFirewall-4401F	6.4.12	5423

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewall DC:</b> FortiFirewall-4401F-DC		
<b>FortiFirewall-VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	

## FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.2.10 supports these models on the identified FortiFirewallCarrier firmware version and build number.

### FortiFirewallCarrier 7.2

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-1801F	7.2.6	4609
<b>FortiFirewallCarrier-DC:</b> FortiFirewallCarrier-1801F-DC		
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-2600F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F	7.2	
<b>FortiFirewallCarrier-DC:</b> FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC		
<b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM		

### FortiFirewallCarrier 7.0

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-3001F	7.0.10	4955
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-3501F	7.0.10	4940
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4401F	6.4.9	5318
<b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.0	

## FortiFirewallCarrier 6.4

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4401F	6.4.9	5318

## FortiFirewallCarrier 6.2

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000F, FE-3000F	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, FortiMail Cloud	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, FortiMail Cloud	6.4

## FortiPAM models

Model	Firmware Version
<b>FortiPAM:</b> FortiPAM-1000G, FortiPAM-3000G	1.0, 1.1
<b>FortiPAM VM:</b> FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	

## FortiProxy models

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

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D	4.4
<b>FortiSandbox DC:</b> FSA-1000F-DC	
<b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D	4.2
<b>FortiSandbox DC:</b> FSA-1000F-DC	
<b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D	4.0
<b>FortiSandbox DC:</b> FSA-1000F-DC	
<b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	3.2
<b>FortiSandbox DC:</b> FSA-1000F-DC	
<b>FortiSandbox-VM:</b> FortiSandbox-AWS, FSA-VM	

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FortiSOAR-VM	7.0, 7.2, 7.3

## FortiSwitch models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
<b>FortiSwitch:</b> FS-5003A, FS-5003B	5.0
<b>FortiController:</b> FTCL-5103B	
<b>FortiSwitch:</b> FS-5003A, FS-5003B	4.3

## FortiTester models

Model	Firmware Version
<b>FortiTester:</b> FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E, <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	7.2, 7.3
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <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-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.1
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <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-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0

Model	Firmware Version
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F <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-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2

## FortiWeb models

Model	Firmware Version
<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 <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	7.2, 7.4
<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 <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0

# Resolved Issues

The following issues have been fixed in FortiManager version 7.2.10. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
1040365	FortiManager is generating false vulnerability reports for certain FortiAPs: <ul style="list-style-type: none"><li>• U431F</li><li>• U231F</li></ul>
1076200	Policy install fails due to FortiManager installs unexpected changes related to "<wifi_intf> address".

## Device Manager

Bug ID	Description
973365	FortiManager does not display the IP addresses of FortiGate interfaces configured with DHCP addressing mode.
1015138	Unable to edit interface with dhcp reservation.
1030539	Managed FortiAnalyzer shown as managed FortiGate in <i>Device Manager</i> .
1030685	Unable to export metadata variables if the metadata's per-device-mapping value is empty.
1050126	Setting up a FortiGate-HA with ZTP fails because the FortiLink is not deleted during the "HA config pushed to FGT" process.
1051889	When downloading the FortiGate config through <i>Device Manager &gt; Managed Devices &gt; Device Configuration DB</i> , the downloaded file contains line breaks in middle of commands, which prevents it to be installed on FortiGate.
1053194	If the "system interface speed" attribute is changed from the FortiManager, it may potentially cause an installation failure. Modifying the "system interface speed" is not currently supported on the FortiManager and must be done on the FortiGate side.
1063635	FortiManager does not support the "FortiWiFi-80F-2R-3G4G-DSL".

Bug ID	Description
1063835	FortiManager ZTP installation to FortiGate versions 7.2.8 and lower may fail due to differing default "ssh-kex-algo" settings between FortiManager and FortiGate.
1063850	FortiManager is attempting to install a "PRIVATE KEY" with every installation, even after retrieving the config.
1067706	Metadata variables cannot be used in the firewall address objects.
1070943	Unable to upgrade the devices via Device Group Upgrade Firmware feature.
1074717	An error might be observed when the SD-WAN template health check name contains a space, displaying the following message: "Bad health check name...".
1075052	Occasionally, installations may fail on FortiGates in HA mode due to a "Serial number does NOT match" error. This can happen if the HA device's serial number on FortiManager does not immediately update after a failover.
1075281	Unable to add FortiAnalyzer to FortiManager, when "fgfm-peercert-withoutsu" is enabled.
1099270	Unable to upgrade of FortiGate HA devices via Firmware Templates.

## FortiSwitch Manager

Bug ID	Description
1061315	Device DB FortiLink config changes when authorizing or deauthorizing FortiSwitch from either <i>FortiSwitch Manager</i> or local FortiGate.

## Others

Bug ID	Description
998198	When upgrading ADOM, the upgrade process fails with the following error: "invalid value - can not find import template 'XYZ' ".
1003711	During the FortiGate HA upgrade, both the primary and secondary FortiGates may reboot simultaneously, which can disrupt the network. This issue is more likely to occur in FortiGates that require disk checks, leading to longer boot times.
1020787	ZTP Enforce firmware Version doesn't upgrade the secondary cluster member.
1058185	FortiProxy policies not imported if the policies have either internet service or IPv6 used in the source or destination.

Bug ID	Description
1078947	Repeatedly testing the URL rating on FortiManager ( <code>diagnose fmupdate test fgd-url-rating...</code> ) may cause the "fgdsvr daemon" to crash.
1081941	When UTM-Profile gets added to a FortiProxy policy FortiManager generates invalid config.

## Policy and Objects

Bug ID	Description
958923	Installing policy packages that utilize an SSL/SSH Inspection profile may fail with the error message "Server certificate replace mode cannot support category exempt."
978136	Occasionally, installation may fail due to an error message, "Waiting for another session", which prevents policies from being installed from FortiManager. During this issue, the following message may also appear: "Blocked by session id(XYZ) username(n/a)". This issue may be caused by a signal loss between the child and parent security console processes, leading the parent process to continue waiting for a copy result.
983591	In the Firewall section, when attempting to add a note to the policy, the comment window shifts towards the left corner.
991720	FortiManager still has an option to enable the "match-vip" through the policy package for "allow" policies. However, this is not supported anymore on the FortiGates.
1004929	FortiManager removes the Web Filter Profile from the Profile Group for Policy-Based FortiGates.
1005161	The policy package status changes for all devices even when an address object is opened and saved without any modifications. This issue is particularly observed in objects utilizing the per-device mapping feature.
1008413	FortiManager fails to load IPS signatures in the profile. This may only occur when the number of signatures listed in the profile is larger than 80.
1014025 1087922	While attempting to access the Application Signatures list on FortiManager, an error message: "a.foreach is not a function" might be displayed.
1029787	The Firewall Policy pane in the FortiManager GUI may occasionally display both "Standard Security Profiles" (SSL no-inspection and protocol default profiles) and "Security Profile Groups" simultaneously.
1046002	Policy Package status does not display "unknown" status immediately following retrieve.
1055795	During device import via multiple CSV files at same time, some devices were imported successfully, while others encountered errors and had missing metadata variables. Additionally, FortiManager forced the admin to log out. When attempting to log back in, the following error message appeared: "ADOM not found".
1068736	Best Quality SDWAN rules installation may fail with the following error message: "Commit

Bug ID	Description
	failed: Bad health check name".
1069285	Using TAB button while creating firewall address object creates error Invalid IP address.
1070800	FortiManager is attempting to install the " <code>cli-cmd-audit</code> " command on a FortiGate running version 7.2.8, which does not support this command, leading to an installation error.
1071226	Policy Lookup is not showing result as highlighted when the sections are not expended.
1076659	When policy package configured with policy block, installation to multiple devices may have copy fail errors if combined length of the Policy Block name and Policy name is greater than 35 characters and if the total number of such policies exceeds 1000. - <OLD>There is not any Workaround for now.
1079037	The " <code>internet-service-id</code> " attribute is configurable in the FortiManager, whereas this attribute cannot be modified on the FortiGate.
1079128	ZTNA Server Per-Device Mapping may display a copy error failure if a new per-device mapping is created without specifying the object interface.
1082548	Address type FQDN is missing DNS resolve domain name function feature.
1109061	FortiManager tries to set the inspection mode for the deny policies.

## Script

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

## Services

Bug ID	Description
1034102	Unable to upgrade FortiGates from FortiManager due to a "no valid FMWR license" error, despite the FortiGates being licensed. This issue is reported when the "FMG Authorization table" on the FDS server is empty.
1060509	When updating query service packages from the global anycast server ( <a href="http://globalupdate.fortinet.net">globalupdate.fortinet.net</a> ), larger-sized IoT packages may encounter checksum errors. These errors can prevent the proper updating of SPAM and URL databases, potentially impacting the FortiManager's FortiGuard Services.

## System Settings

Bug ID	Description
1081463	The encrypted backup file cannot be easily correlated with the backup details, as the date and time are not included.

## VPN Manager

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

## Common Vulnerabilities and Exposures

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

Bug ID	CVE references
1020280	FortiManager 7.2.10 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-33504</li></ul>
1055002	FortiManager 7.2.10 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-3596</li></ul>

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 53](#)
- [Existing known issues on page 53](#)

To inquire about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## New known issues

The following issues have been identified in version 7.2.10.

### Device Manager

Bug ID	Description
1128094	After upgrading to v7.2.10, the entries under <i>Network Monitor &gt; Routing</i> (Static & Dynamic) no longer appear.

### Others

Bug ID	Description
1093040	SDWAN template import failed when meta variable has the default value set.

## Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.2.10.

### AP Manager

Bug ID	Description
1010632	Floor Map shows wrong AP status and does not show the rest of APs when adding a new AP.

## Device Manager

Bug ID	Description
894948	FortiManager fails to push the FortiAnalyzer override settings to the FortiGate.
980362	The Firmware Version column in <i>Device Manager</i> incorrectly shows 'Upgrading FortiGate from V1 to V2' even after a successful upgrade has been completed.
1004220	The SD-WAN Overlay template creates route-map names that exceed the 35-character limit.
1122481	When a FortiGate HA failover occurs, making any changes to the SD-WAN configuration on the FortiGate HA may cause FortiManager to attempt to purge the firewall policies on the device during the installation (Install Device Settings (only)).
1124171	FortiManager retrieves the device configuration from the ZTP FortiGate after the image upgrade is performed, due to the 'Enforce Firmware' feature. This action erases all settings in the device database on the FortiManager side, and as a result, AutoLink installation will not be completed successfully.

## Others

Bug ID	Description
703585	FortiManager may return 'Connection aborted' error with JSON API request.
777831	When FortiAnalyzer is added as a managed device to FortiManager, "Incident & Event" Tile will be displayed instead of the "FortiSoC".
968647	On the <i>Log View</i> (when FortiAnalyzer is added to FortiManager) changing time filters, first request always fails but second one is successful. <b>Workaround:</b> Use FortiAnalyzer's <i>Log View</i> to view logs.
1019261	Unable to upgrade ADOM from 7.0 to 7.2, due to the error "Do not support urlfilter-table for global scope webfilter profile". <b>Workaround:</b> Run the following script against the ADOM DB: <pre>config webfilter profile   edit "g-default"     config web       unset urlfilter-table     end   next end</pre>
1029677	Unable to upgrade ADOM from v6.4 to v7.0 due to global scope error in webfilter profile. <b>Workaround:</b>

Bug ID	Description
	Rename the "g-default" to "g-test" > save. It can be deleted after that. Once ADOM upgraded, new g-default is created.
1052341	Not able to select Address type MAC in SD-WAN rule source address.

## Policy & Objects

Bug ID	Description
971065	When the number of Custom Internet Services exceeds 256, installation fails due to this limitation.
967271	Installation failed when trying to remove firewall internet-service-name objects.
1029921	Under the "Web Application Firewall" security profiles, users are unable to disable the signatures via GUI.
1030914	Copy and paste function in GUI removes name of the policy rule and adds unwanted default security profiles (SSL-SSH no-inspection and default PROTOCOL OPTIONS).
845022	SDN Connector failed to import objects from VMware VSphere.

## VPN Manager

Bug ID	Description
784385	<p>If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager.</p> <p><b>Workaround:</b></p> <p>It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to the workaround. Perform the following command to check &amp; repair the FortiManager's configuration database.</p> <pre>diagnose cdb check policy-packages &lt;adom&gt;</pre> <p>After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.</p>
1042701	The traffic view page for the full mesh does not display the FortiGate and the external gateway.

# 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© 2025 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.