

# Release Notes

**FortiManager 7.2.5**



**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 8th, 2025

FortiManager 7.2.5 Release Notes

02-725-999335-20250408

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 7.2.5 Release</b>	<b>8</b>
Supported models	8
Special branch supported models	8
FortiManager VM subscription license	9
Management extension applications	9
Supported models for MEA	9
Minimum system requirements	9
<b>Special Notices</b>	<b>11</b>
FortiManager & FortiGate: handling of auto-firmware-upgrade setting	11
Custom certificate name verification for FortiGate connection	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	14
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	16
SD-WAN with upgrade to 7.0	17
Citrix XenServer default limits and upgrade	17
Multi-step firmware upgrades	17
Hyper-V FortiManager-VM running on an AMD CPU	18
SSLv3 on FortiManager-VM64-AWS	18
<b>Upgrade Information</b>	<b>19</b>
Downgrading to previous firmware versions	19
Firmware image checksums	19
FortiManager VM firmware	20
SNMP MIB files	21

FortiManager instances on Azure Stack .....	21
<b>Product Integration and Support .....</b>	<b>22</b>
Supported software .....	22
Web browsers .....	23
FortiOS and FortiOS Carrier .....	23
FortiADC .....	23
FortiAnalyzer .....	23
FortiAnalyzer-BigData .....	24
FortiAuthenticator .....	24
FortiCache .....	24
FortiClient .....	24
FortiDDoS .....	24
FortiDeceptor .....	25
FortiFirewall and FortiFirewallCarrier .....	25
FortiMail .....	25
FortiPAM .....	25
FortiProxy .....	25
FortiSandbox .....	26
FortiSOAR .....	26
FortiSwitch ATCA .....	26
FortiTester .....	26
FortiWeb .....	27
Virtualization .....	27
Feature support .....	28
Language support .....	28
Supported models .....	29
FortiGate models .....	30
FortiGate special branch models .....	33
FortiCarrier models .....	34
FortiCarrier special branch models .....	35
FortiADC models .....	37
FortiAnalyzer models .....	37
FortiAnalyzer-BigData models .....	38
FortiAuthenticator models .....	38
FortiCache models .....	38
FortiDDoS models .....	39
FortiDeceptor models .....	39
FortiFirewall models .....	39
FortiFirewallCarrier models .....	40
FortiMail models .....	42
FortiPAM models .....	42
FortiProxy models .....	42
FortiSandbox models .....	43
FortiSOAR models .....	43
FortiSwitch ATCA models .....	43
FortiTester models .....	44
FortiWeb models .....	44

---

<b>Compatibility with FortiOS Versions</b>	<b>46</b>
FortiManager 7.2.5 and FortiOS 7.0.15 compatibility issues	46
<b>Resolved Issues</b>	<b>47</b>
AP Manager	47
Device Manager	47
FortiSwitch Manager	49
Global ADOM	49
Others	50
Policy and Objects	51
Revision History	53
Script	54
Services	54
System Settings	54
VPN Manager	55
Common Vulnerabilities and Exposures	55
<b>Known Issues</b>	<b>56</b>
AP Manager	56
Device Manager	56
FortiSwitch Manager	57
Others	58
Policy & Objects	59
Revision History	61
Script	61
System Settings	62
VPN Manager	62
<b>Appendix A - FortiGuard Distribution Servers (FDS)</b>	<b>63</b>
FortiGuard Center update support	63
<b>Appendix B - Default and maximum number of ADOMs supported</b>	<b>64</b>
Hardware models	64
Virtual Machines	64

# Change Log

Date	Change Description
2024-03-14	Initial release.
2024-03-18	Updated <a href="#">FortiGate special branch models on page 33</a> .
2024-04-02	Updated <a href="#">Resolved Issues on page 47</a> .
2024-04-03	Updated <a href="#">Supported models on page 8</a> .
2024-04-08	Updated <a href="#">Special Notices on page 11</a> , <a href="#">Resolved Issues on page 47</a> , and <a href="#">Known Issues on page 56</a>
2024-04-09	Updated <a href="#">Resolved Issues on page 47</a> .
2024-04-10	Updated <a href="#">Known Issues on page 56</a> .
2024-04-12	Updated <a href="#">Resolved Issues on page 47</a> and <a href="#">Known Issues on page 56</a> .
2024-04-22	Updated <a href="#">Known Issues on page 56</a> .
2024-04-24	Updated <a href="#">Resolved Issues on page 47</a> and <a href="#">Known Issues on page 56</a> .
2024-04-30	Updated <a href="#">Known Issues on page 56</a> .
2024-05-06	Added "Apache-mode changed from prefork to event" to <a href="#">Special Notices on page 11</a> . Updated <a href="#">Resolved Issues on page 47</a> . Updated <a href="#">Known Issues on page 56</a> .
2024-05-13	Updated <a href="#">Known Issues on page 56</a> .
2024-05-23	Updated <a href="#">Supported models on page 8</a> and <a href="#">Known Issues on page 56</a> .
2024-05-29	Added "FortiManager & FortiGate: handling of auto-firmware-upgrade setting" to <a href="#">Special Notices on page 11</a> .
2024-05-31	Updated "IPSEC VPN CA certificates must be re-issued to all devices after upgrade" in <a href="#">Special Notices on page 11</a> .
2024-06-04	Updated <a href="#">FortiGate special branch models on page 33</a> .
2024-06-10	Add 1012413 to <a href="#">Known Issues on page 56</a> .
2024-06-12	Updated <a href="#">Known Issues on page 56</a> .
2024-06-19	Updated <a href="#">Known Issues on page 56</a> and <a href="#">Supported models on page 8</a> .
2024-06-20	Added <a href="#">FortiManager 7.2.5 and FortiOS 7.0.15 compatibility issues on page 46</a> .
2024-06-26	Updated <a href="#">Feature support on page 28</a> .
2024-07-11	Updated <a href="#">Management extension applications on page 9</a> .
2024-07-29	Updated <a href="#">Virtualization on page 27</a> .

Date	Change Description
2024-08-09	Updated <a href="#">Resolved Issues on page 47</a> and <a href="#">Known Issues on page 56</a> .
2024-08-13	Updated <a href="#">Resolved Issues on page 47</a> .
2024-08-19	Updated <a href="#">Resolved Issues on page 47</a> .
2024-08-22	Updated <a href="#">Known Issues on page 56</a> .
2024-09-10	Updated <a href="#">Resolved Issues on page 47</a> .
2024-11-14	Updated <a href="#">Resolved Issues on page 47</a> . Updated <a href="#">FortiGate models on page 30</a> and <a href="#">Known Issues on page 56</a> .
2024-12-03	Updated <a href="#">Special Notices on page 11</a> .
2024-12-10	Updated <a href="#">Supported models on page 8</a> with information about access to FortiManager container versions.
2025-01-07	Updated <a href="#">Known Issues on page 56</a> .
2025-01-14	Updated <a href="#">Appendix A - FortiGuard Distribution Servers (FDS) on page 63</a>
2025-02-11	Updated <a href="#">Known Issues on page 56</a> .
2025-04-08	Updated <a href="#">Resolved Issues on page 47</a> .

# FortiManager 7.2.5 Release

This document provides information about FortiManager version 7.2.5 build 1574.



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 8](#)
- [FortiManager VM subscription license on page 9](#)
- [Management extension applications on page 9](#)

## Supported models

FortiManager version 7.2.5 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, 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).

## Special branch supported models

The following models are released on a special branch of FortiManager 7.2.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1574.

<b>FMG-410G</b>	is released on build 6054.
<b>FMG-1000G</b>	is released on build 6054.
<b>FMG-3100G</b>	is released on build 6054.



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 20](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 64](#).

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.2.5.



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-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 7.2.5.

## FortiManager & FortiGate: handling of auto-firmware-upgrade setting

Normally, the following `auto-firmware-upgrade` setting controls whether the FortiGate automatically upgrades firmware once available:

```
FortiGate # config system fortiguard
FortiGate (fortiguard) # set auto-firmware-upgrade disable
FortiGate (fortiguard) # end
```

By design, when a FortiGate is managed by a FortiManager, the `auto-firmware-upgrade` feature is disabled regardless of the configuration setting. For more information, see the [FortiManager Administration Guide](#).

To check `auto-firmware-upgrade` state:

```
FGT # diagnose test application forticldd 13
<snip>
Automatic image upgrade: Disabled.
```

Two issues can arise:

1. During install, FortiManager may attempt to enable this configuration setting when that setting is disabled on the FortiGate.  
To prevent this, after disabling the setting on the FortiGate via FortiManager CLI script, be sure to perform a Retrieve to update the FortiManager.
2. Due to a known FortiOS issue (bug id 1017519), the FortiGate may not automatically disable the `auto-firmware-upgrade` feature when the "`set fmg <IP>`" setting is empty.

```
config system central-management
  set type fortimanager
  set fmg "" -----> IP address is missing
end
```

For this second scenario, to ensure that `auto-firmware-upgrade` is disabled, either make sure the `auto-firmware-upgrade` configuration setting is set to disable (mid-range models and above), or make sure that "`set fmg`" is configured with an IP address.

## Custom certificate name verification for FortiGate connection

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.

Alternatively, FortiManager 7.2.5 provides a new CLI command to disable this verification. Fortinet recommends to keep the verification enabled.

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

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

## Configuration backup requires a password

As of FortiManager 7.2.5, configuration backup files are automatically encrypted and require you to set a password. 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 7.4.2, it creates a new CA <ADOM Name>\_CA3 certificate as part of a fix for resolved issue 796858. See [Resolved Issues on page 47](#). 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 v7.4.2.

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
```

# 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 7.2.5 Upgrade Guide](#).

You can upgrade FortiManager 7.0.1 or later directly to 7.2.5.



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 7.2.5 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 19](#)
- [Firmware image checksums on page 19](#)
- [FortiManager VM firmware on page 20](#)
- [SNMP MIB files on page 21](#)
- [FortiManager instances on Azure Stack on page 21](#)

## Downgrading to previous firmware versions

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

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

## Firmware image checksums

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

## FortiManager VM firmware

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

### Amazon Web Services

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

### Citrix XenServer and Open Source XenServer

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

### Google Cloud Platform

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

### Linux KVM

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

### Microsoft Azure

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

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

### Microsoft Hyper-V Server

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

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



Microsoft Hyper-V 2016 is supported.

---

### Oracle Private Cloud

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

### VMware ESX/ESXi

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



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

---

## SNMP MIB files

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

## 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 7.2.5 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 22](#)
- [Feature support on page 28](#)
- [Language support on page 28](#)
- [Supported models on page 29](#)

## Supported software

FortiManager 7.2.5 supports the following software:

- [Web browsers on page 23](#)
- [FortiOS and FortiOS Carrier on page 23](#)
- [FortiADC on page 23](#)
- [FortiAnalyzer on page 23](#)
- [FortiAnalyzer-BigData on page 24](#)
- [FortiAuthenticator on page 24](#)
- [FortiCache on page 24](#)
- [FortiClient on page 24](#)
- [FortiDDoS on page 24](#)
- [FortiDeceptor on page 25](#)
- [FortiFirewall and FortiFirewallCarrier on page 25](#)
- [FortiMail on page 25](#)
- [FortiPAM on page 25](#)
- [FortiProxy on page 25](#)
- [FortiSandbox on page 26](#)
- [FortiSOAR on page 26](#)
- [FortiSwitch ATCA on page 26](#)
- [FortiTester on page 26](#)
- [FortiWeb on page 27](#)
- [Virtualization on page 27](#)



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 7.2.5 supports the following web browsers:

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

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

## FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.2.5 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 7.2.5 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0 to 7.2.8
  - 7.0.0 to 7.0.15
  - 6.4.0 to 6.4.16
- 



Some FortiOS versions are supported with compatibility issues. For more details, see [Compatibility with FortiOS Versions on page 46](#).

---

## FortiADC

FortiManager 7.2.5 supports the following versions of FortiADC:

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

## FortiAnalyzer

FortiManager 7.2.5 supports the following versions of FortiAnalyzer:

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

## FortiAnalyzer-BigData

FortiManager 7.2.5 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

## FortiAuthenticator

FortiManager 7.2.5 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 7.2.5 supports the following versions of FortiCache:

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

## FortiClient

FortiManager 7.2.5 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 7.2.5 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 28](#).

## FortiDeceptor

FortiManager 7.2.5 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 7.2.5 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 7.2.5 supports the following versions of FortiMail:

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

## FortiPAM

FortiManager 7.2.5 supports the following versions of FortiPAM:

- 1.1.0 and later
- 1.0.0 and later

## FortiProxy

FortiManager 7.2.5 supports configuration management for the following versions of FortiProxy:

- 7.2.9
- 7.2.7
- 7.2.6

- 7.2.3
- 7.2.2
- 7.0.12 to 7.0.14
- 7.0.7 to 7.0.10



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 28](#).

---

FortiManager 7.2.5 supports logs from the following versions of FortiProxy:

- 7.2.0 to 7.2.9
- 7.0.0 to 7.0.14
- 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 7.2.5 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 7.2.5 supports the following versions of FortiSOAR:

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

## FortiSwitch ATCA

FortiManager 7.2.5 supports the following versions of FortiSwitch ATCA:

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

## FortiTester

FortiManager 7.2.5 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 7.2.5 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 7.2.5 supports the following virtualization software:

### Public Cloud

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

### Private Cloud

- Citrix XenServer 7.2
- OpenSource XenServer 4.2.5
- Microsoft Hyper-V Server 2016, 2019, and 2022
- Nutanix
  - AHV 20220304 and later
  - AOS 6.5 and later
  - NCC 4.6 and later
  - LCM 3.0 and later
- RedHat 9.1
  - Other versions and Linux KVM distributions are also supported
- VMware ESXi versions 6.5 and later

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiPAM		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

## Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓

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

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

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

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.2.5.



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 30](#)
- [FortiGate special branch models on page 33](#)
- [FortiCarrier models on page 34](#)
- [FortiCarrier special branch models on page 35](#)
- [FortiADC models on page 37](#)
- [FortiAnalyzer models on page 37](#)
- [FortiAnalyzer-BigData models on page 38](#)
- [FortiAuthenticator models on page 38](#)
- [FortiCache models on page 38](#)
- [FortiDDoS models on page 39](#)
- [FortiDeceptor models on page 39](#)
- [FortiFirewall models on page 39](#)
- [FortiFirewallCarrier models on page 40](#)
- [FortiMail models on page 42](#)

- [FortiPAM models on page 42](#)
- [FortiProxy models on page 42](#)
- [FortiSandbox models on page 43](#)
- [FortiSOAR models on page 43](#)
- [FortiSwitch ATCA models on page 43](#)
- [FortiTester models on page 44](#)
- [FortiWeb models on page 44](#)

## 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 33](#).

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-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-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 <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	7.2

Model	Firmware Version
<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-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-80F-2R, FWF-81F-2R, 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 <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-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	

Model	Firmware Version
<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 <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 <b>FortiOS-VM:</b> FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-60F, FGR-60F-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-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, <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <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 <b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC <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	6.4

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.2.5 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 30](#).

### FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.14	7132
FortiGate-90G	7.0.13	6984
FortiGate-91G	7.0.13	7017
FortiGate-120G, FortiGate-121G	7.0.12	5334
FortiGate-900G, FortiGate-901G	7.0.14	7119
FortiGate-1000F, FortiGate-1001F	7.0.14	7115
FortiGate-3200F, FortiGate-3201F	7.0.14	7120
FortiGate-3700F, FortiGate-3701F	7.0.14	7120
FortiGate-4800F, FortiGate-4800F-DC	7.0.14	7137
FortiGate-4801F, FortiGate-4801F-DC	7.0.14	7120
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.14	0220
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.14	0220
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-2-DC, FortiGate-7081F-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.14	0220
FortiGateRugged-70F, FortiGateRugged- 70F-3G4G	7.0.14	7146
FortiGateRugged-70G-5G-Dual	7.0.12	7151
FortiWiFi-50G-5G	7.0.12	7192
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F- 2R-3G4G-DSL	7.0.14	7132

## FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F, FortiGate-401F	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 35](#).

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 <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	7.2

Model	Firmware Version
<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 <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	
<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 <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 <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	7.0
<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 <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 <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	6.4

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.2.5 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 34](#).

## FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.14	7120
FortiCarrier-3700F, FortiCarrier-3701F	7.0.14	7120
FortiCarrier-4800F, FortiCarrier-4800F-DC	7.0.14	7137
FortiCarrier-4801F, FortiCarrier-4801F-DC	7.0.14	7120
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.14	0220
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.14	0220
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	7.0.14	0220

## 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-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	6.4.13	1926

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
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-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, 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-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E <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	7.0

Model	Firmware Version
<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 <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	6.4

## FortiAnalyzer-BigData models

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

## 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 <b>FortiAuthenticator VM:</b> FAC-VM	6.4, 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 <b>FortiAuthenticator VM:</b> FAC-VM	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-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 7.2.5 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 <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	7.2

## 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	7.0	
<b>FortiFirewall DC:</b> FortiFirewall-3980E-DC		
<b>FortiFirewall-VM:</b> FortiFirewall-VM64, FortiFirewall-VM64-KVM		

## FortiFirewall 6.4

Model	Firmware Version	Firmware Build (for special branch)
<b>FortiFirewall:</b> FortiFirewall-1801F, FortiFirewall-2600F	6.4.12	5423
<b>FortiFirewall DC:</b> FortiFirewall-1801F-DC, FortiFirewall-2600F-DC		
<b>FortiFirewall:</b> FortiFirewall-3980E	6.4	
<b>FortiFirewall DC:</b> FortiFirewall-3980E-DC		
<b>FortiFirewall:</b> FortiFirewall-4200F, FortiFirewall-4400F	6.4	1999
<b>FortiFirewall:</b> FortiFirewall-4401F	6.4.12	5423
<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 7.2.5 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 <b>FortiFirewallCarrier-DC:</b> FortiFirewallCarrier-1801F-DC	7.2.6	4609
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-2600F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F <b>FortiFirewallCarrier-DC:</b> FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC <b>FortiFirewallCarrier-VM:</b> FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.2	

## 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
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4401F	6.4.9	5318

## 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 <b>FortiPAM VM:</b> FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1

## 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-VM64	7.0, 7.2
<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-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D <b>FortiSandbox DC:</b> FSA-1000F-DC <b>FortiSandbox-VM:</b> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	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> FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.2
<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> FortiSandbox-AWS, FortiSandbox-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> FortiSandbox-AWS, FSA-VM	3.2

## FortiSOAR models

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

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B	5.0
<b>FortiSwitch-ATCA:</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
<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	7.2, 7.4

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

# Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.2.5.

## FortiManager 7.2.5 and FortiOS 7.0.15 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.5 and FortiOS 7.0.15. FortiOS 7.0.15 includes syntax changes not supported by FortiManager 7.2.5.



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

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

The following objects were added:

```
(attr) system global npu-neighbor-update (119 platforms: excludes 91E,90E)
(attr) system npu background-sse-scan scan-stale (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu background-sse-scan scan-vt (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu background-sse-scan stats-qual-access (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu background-sse-scan stats-qual-duration (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu background-sse-scan udp-qual-access (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu background-sse-scan udp-qual-duration (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu default-tcp-refresh-dir (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu default-udp-refresh-dir (22 platforms:
3500F,4400F,2601F,3001F,4200F,3501F,1800F,3000F,4401F,1801F,4201F,2600F)
(attr) system npu nss-threads-option (16 platforms:
3500F,4400F,3001F,4200F,3501F,3000F,4401F,4201F)
```

The following default value changed:

```
system npu sse-ha-scan gap (6000 -> 200)
```

# Resolved Issues

The following issues have been fixed in 7.2.5. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
736930	FortiManager is unable to efficiently display rogue AP lists for FortiGates with a high volume of rogue APs.
861941	FortiManager attempts to install "arp-profile" even if "darp" is disabled.
884233	FortiManager may display FortiAP critical security vulnerability information even after FortiAPs have been upgraded. This could be because the FortiAP does not provide their patch numbers to the FortiGate, and therefore this information is not transferred to the FortiManager for proper vulnerability checking. Please follow up with the FortiAP team for more information.
906061	It takes a significant amount of time to assign a profile to each FortiAPs.
974444	DNS server for SSIDs gets resets after Importing AP Profile.
982548	FortiGate configuration install may fail with a reason "Need to unset channel list in radio-1 first."
987111	Unable to save the SSID configuration changes under the <i>AP Manager</i> .
1002043	<i>AP Manager</i> view does not show SSIDs and Radio Channels.

## Device Manager

Bug ID	Description
723720	The "strong-crypto" feature change under the CLI configuration cannot be installed to FortiGate.
751612	After upgrading to 7.2.4 version, Read/Write Access level profile for SD-WAN and provisioning template is not properly set.
778131	FortiManager did not support the per device mapping for user SAML configurations.
811104	Import policy package fails after installing web-proxy through CLI configurations
838462	Adding device using "Add Model HA Cluster" feature failed as FortiManager does not allow

Bug ID	Description
	"virtual switch interfaces" being used as "heartbeat interfaces".
871334 973064	Installation to FortiGate with NP7 Acceleration feature enabled might fail when FortiManager attempted to modify the QoS settings. Changing the "default-qos-type" to values other than its default may result in a FortiGate reboot (FOS Behavior).
880934	FortiManager reverts Syslog mode settings on local FortiGates (when FortiGates are in FIPS mode).
902577	The status of the FortiLink split-interface radio button under FortiManager's <i>Device Manager</i> does not match the configuration in FortiGates.
920394	Installation failed due to the incorrect install order during ZTP.
923808	Even with the "set dhcp-relay-request-all-server enable" option enabled, FortiManager does not keep the DHCP server & relay configurations on the same interface.
935586	When managed devices go down/appear offline, not all FGFM tunnels are automatically recovered by FortiManager.
936168	Unable to assign Device Group to the Firmware Template.
936544	When importing CLI Templates, GUI displays a blank page.
939804	Creating/Modifying the IPSEC Phase1 Interface Mode might trigger the following error message: "The string contains XSS vulnerability characters." This ONLY occurs when <code>devicid = ''</code> .
939921	The firmware upgrade in ADOM mode backup is not allowed.
949546	When zones have identical names except for case, only 1 of the zones may be visible in <i>Device Manager</i> .
949612	The SD-WAN monitor table-view takes too long to load/display information.
950391	FortiManager attempts to unset the "peervd" parameter under the system "cluster-sync", resulting in installation failure.
952404	FortiManager cannot install the Static Route config under the Provisioning Template due to a static route template error after upgrading to FortiManager 7.2.4/7.4.1.
954610	FortiManager does not show objects under the "named address" options in IPsec VPN Phase 2 definitions.
956567	Not able to edit/delete Logging Devices Group.
956920	Monitor Health Check graphs return incomplete or no value.
960315	Unable to create/edit "ssh-public-key1" with "sh-ed25519" for admin users from FortiManager's <i>Device Manager</i> ; it displays an "invalid value" error message.
961447	After upgrading FortiManager (VMs & FortiManager Cloud) to versions 7.2.4 or 7.4.1, devices may not be able to be retrieved or refreshed.
966118	FortiManager tries to purge all entries under table "system global split-port-mode" for its System Template .

Bug ID	Description
967611	<i>Device Manager</i> interface link status is blank for various Interface type (Tunnel, Aggregate, VDOM Link, Software Switch).
969542	Sometimes IPsec Tunnel Template displaying "Response with errors" message when editing the template.
969698	FortiManager allows the creation of an empty service value for Internet Service routes.
971432	<i>SD-WAN Monitor</i> in the FortiManager doesn't show up data for more than one hour.
975310	Unable to unset interface IP for a VLAN interface in <i>Device Manager</i> .
984868	<i>Device Manager</i> page turns blank after right-clicking on a device.
986466	When modifying the BGP template with a new route map rule, a failure error message may be displayed.
988964	FortiManager tries to push <code>switch-controller</code> command to devices that do not have this command.
1009883	Unable to set the Radius-Server addresses as FQDN.

## FortiSwitch Manager

Bug ID	Description
940419	When adding FortiSwitch on FortiManager Error message, "Import error - invalid port number" is displayed.
947651	<i>Per Device</i> under the <i>FortiSwitch Manager</i> cannot edit FortiSwitch name and GUI returns error "invalid value".
967213	While attempting to deploy a FortiSwitch template to a model device, FortiManager generates the following error message: "VLAN interface does not match FortiLink."

## Global ADOM

Bug ID	Description
906058	Firewall address cannot be deleted from Global ADOM; it displays an error message indicating that the object is being used in ADOM root.
925188	The per-device mapping for any assigned global objects cannot be modified.
969182	Under the Global ADOM, the assignment of specific policy packages does not function properly.

## Others

Bug ID	Description
583349	FortiManager does not provide support for image upgrades on "ONDEMAND" devices.
796858	Subject Key Identifier extension is missing on FortiManager ADOM CA certificate.
862651	Even after enabling all MEAs, the warning to enable the application is displayed.
874052	After upgrade ADOM from v7.0 to v7.2, when installing a policy package to FGT-v7.2 device, FortiManager tries to change "match-vip" from "disabled" to "enabled".
875584	FortiManager cannot upgrade ADOMs to 7.2 due to error, "copy system replacemsg spam.smtp-spam-emailblock".
891253	The firmware upgrade is successful; however, the task line does not get updated for the retrieve action when device names exceed the predefined character limit.
897157	Unexpected changes in existing static routes, created by static route template after upgrade to 7.0.7, 7.2.2, 7.4.0.
900512	FortiManager ADOM Upgrade fails with the error message, "Peer type cannot be peer when authentication method is pre-share key".
922957	The "fmgd" process may crash while loading the ADOM when multiple Policy Packages are locked.
924201	Jinja templates does not identify new variables automatically when a new variable is added.
930305	Firmware template upgrade preview shows incorrect versions for the upgrade.
935430	When FortiAnalyzer is managed by FortiManager and FortiManager's local logs are being sent to FortiAnalyzer, installing PP to FortiGates may display the message, "Confirm Deletion FortiManager is going to sync the following device deletion to FortiAnalyzer,...".
941203	FortiManager does not support the use of Certificate Templates to create certificates with a "range=global" setting for FortiGates operating in multi-vdom mode.
956335	Unable to upgrade root ADOM from v6.4 to v7.0 with "med-location-service" object error.
960796	FortiExtenders are not displayed under the <i>FortiExtender Manager</i> for all FortiGates.
961155	Event Logs cannot be downloaded via GUI.
961249	Significant CPU utilization has been detected in the miglogd process upon enabling the locallog FortiAnalyzer feature.
963490	Installation fails as FortiManager attempts to "set role primary" feature for the "lan-extension backhaul" under the "extender-controller"
963744	FortiManager's HA status becomes unsynchronized when the "private-data-encryption" feature is enabled.
971122	FortiManager does not support all authentication types that are supported by FortiOS, leading to a certificate error in the FortiClient EMS connector.
976448	Unable to login FortiManager Cloud.

Bug ID	Description
982564	When upgrading the root ADOM, the process might fail with the following error message: "...The string contains XSS vulnerability characters...".

## Policy and Objects

Bug ID	Description
630648	A FortiManager instance running on Microsoft Azure is unable to import the SDN connector for a dynamic firewall address and is displaying an error message stating, "wrong input parameter."
696367	Hit count, first used, and last used may not get updated on FortiManager.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
751443	FortiManager displays policy installation copy failures error when IPsec template gets unassigned.
804160	FortiManager does not remove "Radius Server" on the FortiGate when it becomes unused.
817289	FortiManager only accepts IPv6 Compressed Notation format for the <i>Policy &amp; Objects</i> .
830640	"Send files to FortiSandbox for inspection" option is being enabled when creating an antivirus profile.
854359	An installation error occurs when FortiManager attempts to install wildcard FQDN addresses "mzstatic-apple" and "cdn-apple" within the "custom-deep-inspection" SSL-SSH profile.
855073	The "where used" feature (under the Source & Destination objects) incorrectly displays "No Record Found" even when these objects are in use.
875103	Local categories gets purged if used in Profile Mode Security Profiles.
888798	Changing deep inspection ssl-ssh-profile to "inspect all ports" may cause installation error.
894597	Default value for "unsupported-ssl-version" in ssl-ssh-profile gets modified during the installation.
899226	Unable to create Central SNAT explicit port translations on FortiManager.
900229	In policy-based policy packaged, application IDs are displayed instead of their names.
901324	Change entries in FortiGuard Category Based Filter table from "Monitor" to "Allow" cannot be saved.
904751	WebRating overrides can't be deployed or deleted via FortiManager.
905377	Threat Feeds with name starting with "g-" do not get installed to FortiGates without VDOM enabled.

Bug ID	Description
907925	IPS profile/Signature tab is not visible for admins with non-default admin profile.
908353	When ISDB name changed, FortiManager is not automatically updating the new ISDB object name.
908445	FortiManager does not display correct edit page for virtual server VIP when edit object in policy table.
917225	FortiManager is unable to install policy packages to multiple devices due to "security console" crashes.
920983	The policy blocks using a group object do not get updated when the objects within the group are modified.
924680	Policy packages containing geo-based ISDB objects may not be successfully installed to the FortiGates.
924900	Wrong date format is displayed for " <i>first used</i> " and " <i>last used</i> " column.
938019	Policy Package Status not changed on modification of nested group used in policy block.
939979	After editing authentication-rule/portal mapping, FortiManager installs unexpected changes to these rules.
942659	Syncing EMS tags from FortiManager fails when the EMS Connector is configured in multi-site mode.
945632	Modifying the Policy Installation Target does not trigger a status change in the Policy Package when adding an "install on" to a single policy.
945853	FortiManager doesn't sync previously deleted EMS tags.
948559	Policy blocks doesn't load properly.
949515	Security Policy Installation Verification fails because the " <i>internet-service-negate</i> " feature gets enabled every time after modifying the policy.
954399	Cloning Webfilter profiles does not save the FortiGuard Category Based Filter action.
955010	Comments on policies may be cleared when a blank area within the text field is clicked.
957225	ADOM admin users not able to view the managed FortiGate in the policy push wizard
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."
959116	The timestamps displayed for 'First/Last Used' under the Hit Count for Firewall Policies within the Policy & Objects section are invalid.
959166	Export to Excel does not work.
959877	The timestamps displayed for "First/Last Used" under the <i>Hit Count</i> for Firewall Policies within the <i>Policy &amp; Objects</i> section are invalid.
959890	Per-device mapping search for VDOMs is not possible for users.
960660	The Clone Reverse feature is not functioning when the firewall policy includes an Internet

Bug ID	Description
	service address object.
960778	Installation failed because FortiManager attempts to remove a static entry, "QuarantinedDevices."
963008	Impossible to merge duplicate objects.
963536	The policy package feature "Export to Excel" is not functioning.
965670	Creating a new interface type "vlan"; changing VDOM results in the removal of the selected interface.
965719	FortiManager is unable to enable the log setting for implicit deny rule under the policy package.
972392	Users do not receive a proper warning when creating a firewall address with the IP address "0.0.0.0/0."
978814	When attempting to use the "Export to Excel" feature under the Firewall Policy with extensive rules, GUI may slow down and become unresponsive for some time.
979554	EMS connectors are randomly getting disabled on FortiManager, despite no changes being made to EMS settings on either FortiManager or FortiGate.
982638	Invalid IPS signature breaks the GUI when users are trying to edit the IPS profile in the FortiManager.
984935	The "view mode" and "Routing Object" options are not displayed on the GUI.
986262	EMS Cloud tags are not updated on FortiManager.
989423	FortiManager SD-WAN interfaces are not available as Normalized interfaces.
1002551	FortiManager is pushing the web-proxy profile configuration without space between domains.

## Revision History

Bug ID	Description
513317	FortiManager may fail to install policy after FortiGate failover on Azure.
894523	Object revision timestamp is taken from previous revision.
904710	Restoring a revision of a policy removes the information of all the SD-WAN rules.

## Script

Bug ID	Description
923966	When FortiManager is operating in Workspace mode, there are no options to save changes after executing a CLI script.
937528	Unable to send DHCP options "set value" using CLI template and using Script.

## Services

Bug ID	Description
863094	The query status is not functioning correctly, and the "Top 10 Unrated Sites" section actually displays ratings.
938365	FortiManager's GUI does not display an option under FortiGuard Settings to support the 7.2 version for FortiClient and FortiMail.
980334	"Download to Excel" option on Licensing Status under the FortiGuard does not work.
985074	Changing the FortiGuard Server Location under the license info widget results in a blank page popup.

## System Settings

Bug ID	Description
733279	After changing the http or https port, FortiManager displays an "Unknown Error." error message.
842732	FortiManager does not display the Secondary HA member's status correctly.
853429	Creating FortiManager's configuration backup via scp cannot be done.
871633	The configuration that is not synchronized among HA members cannot be modified on secondary devices.
881309	In SSO configuration, whether the settings for "ext-auth-accprofile-override" and "ext-auth-adom-override" are enabled or disabled, the users are granted an adom/accprofile override, if the IdP sends valid ADOMs and "profilename" attributes.
930200	Unable to change the time and timezone from the GUI.
930449	Testing the syslog server displays the message, "Failed to send a test log to syslog server".
936694	After removing a device, FortiManager generates repeated "sync dvmdb to faz" tasks for all logged-in administrative users.

Bug ID	Description
941082	A password prompt is consistently requested with each new login attempt when applying password policies to a local account linked to FortiToken Cloud Mobile for multi-factor authentication (MFA).
957308	After enabling FortiAnalyzer features, the new Event Logs are not displayed in Event Log under the system settings.
966148	RADIUS remote users are unable to successfully install changes to FortiGates.

## VPN Manager

Bug ID	Description
678319	Once "os-check" option is enabled, "os-check-list" table is not loaded.
897574	Address Objects with Meta Variables do not function correctly when creating Static routes using the <i>VPN Manager</i> .
906097	<i>VPN Manager</i> IPsec community Phase 2 encryption setting can't be changed to AES256GCM from the GUI.
923221	Provision Template - IPsec Tunnel: cannot Activate IPsec_Fortinet_Recommended; GUI returns error.
942222	The configuration settings for the "peergroup" are not being retained properly.

## Common Vulnerabilities and Exposures

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

Bug ID	CVE references
934161	FortiManager 7.2.5 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2023-44254</li></ul>
968793	FortiManager 7.2.5 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2023-47542</li></ul>
977283	FortiManager 7.2.5 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-21757</li></ul>
998721	FortiManager 7.2.5 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-26011</li></ul>
1003216	FortiManager 7.2.5 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2024-26013</li></ul>

# Known Issues

The following issues have been identified in 7.2.5. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
977726	SSID config changes cannot be installed when SSID mode selected as Tunnel under AP.
1010485	Under the <i>AP Manager</i> , WiFi map view cannot load the AP Information.
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.
895994	When using the 'where used' feature in Phase 2 quick mode selector, objects do not appear, and they can be removed.
955058	Changes on Address groups only referenced in phase2 selectors are not installed
960363	<i>Traffic Shaping</i> widgets keep loading on Dashboard page of the <i>Device Manager</i> .
961508	<i>SD-WAN Monitor</i> table-view does not load.
966546	Unable to disable the "Create Address Object Matching Subnet" feature when the interfaces role is LAN.
976887	Unable to set non-HEX values for <i>DHCP Option</i> ; it displays an error message: "...enter a valid Hexadecimal number...".
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.
980659	When adding FortiGates (FWF-80F, FWF-80F-2R-3G4G-DSL, FWF-81F-2R-3G4G-DSL) as model devices, FortiManager may attempt to create a duplicate DHCP server. Consequently, this installation fails due to the duplicate configuration.
981031	<i>Device Inventory</i> widget shows wrong date for "last seen".
993094	Firmware image for Azure FortiGate (PAYGO) is not available from ( <i>Device Manager</i> >

Bug ID	Description
	<i>Firmware upgrade).</i>
997344	FortiManager is missing the "set members 0" feature when creating SDWAN Performance SLA.
1000686	HA autolink failure occurs when LAN interfaces do not exist.
1002289	Unable to delete default <code>wireless-controller vap</code> configuration with pre-run CLI templates.
1006838	"Admin User" settings get modified if username is more than 37 characters.
1011744	Autoupdate will not update the Device DB with FortiGate's ssh local-key details.
1015064	Disabling the "auto-firmware-update" in FortiManager device db does not disable it on the FortiGate. Please review "FortiManager & FortiGate: handling of auto-firmware-upgrade setting" in <a href="#">Special Notices on page 11</a> .
1016654	<p>FortiManager fails to add FortiAnalyzer as a managed device.</p> <p><b>Workaround:</b></p> <p>Configure the following on the FortiManager to allow FortiAnalyzer to connect:</p> <pre>config system global   set fgfm-peercert-withoutsn enable end</pre>
1016987	<p>FGFM's tunnel went down after upgrade because the device's SN doesn't match the expected certificate.</p> <p><b>Workaround:</b></p> <p>This check can be manually disabled globally on FortiManager side by the following CLI:</p> <pre>config system global   set fgfm-peercert-withoutsn enable end</pre>
1021087	<p>The out-of-sync notification is missing in FortiManager after upgrading to version 7.2.5.</p> <p><b>Workaround:</b></p> <ul style="list-style-type: none"> <li>• Reboot the FortiManager, or</li> <li>• Find the process IDs (PIDs) of "webworker", "websocket", and "webevent", then terminate them using the following command: <code>diag sys process kill 11 &lt;pid&gt;</code></li> </ul>
1063635	FortiManager does not support the "FortiWiFi-80F-2R-3G4G-DSL".

## FortiSwitch Manager

Bug ID	Description
995984	Cannot create MC-LAG in <i>FortiSwitch Manager</i> .

## 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, the "Incident & Event" tile will display instead of the "FortiSoC" tile.
894219	The log filter does not function correctly when filtering by FortiGate HA cluster ID instead of the device ID for individual FortiGate units.
954564	FortiManager attempts to change FEX serial number and returns an installation error.
967214	Unable to set up metadata variables using CSV file when Workspace mode is enabled on ALL ADOMs.
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.
983359	The "40F-3G-4G LTE" modem is not listed on the FortiManager's <i>Extender Manager</i> .
986753	Policy installation may stuck on the validation due to recurrent Segmentation Fault errors on the webevent / webworker processes. <b>Workaround:</b> FortiManager may be rebooted.
988422	The installation fails to FortiProxys when FortiManager attempts to set the firewall address object with the associated-interface value of "any". FortiProxy does not support the "any" value key.
991052	FortiManager AWS is not able to form geo-redundant cluster as VRRP HA fails to sync.
1003261	FortiManager displays the Vulnerability notification alert but the device list is blank.
1015415	When FortiAnalyzer is added as a managed device to FortiManager, filtered logs will not be displayed under <i>Log View</i> .
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>
1022997	When devices are vulnerable, the table view freezes, resulting in the section not loading properly and the GUI continuously spinning.

Bug ID	Description
1023512	FortiManager fails to install policies to FortiProxy if number of local users are more than 1000.
1025097	The GUI crashes with "Uncaught TypeError: Cannot read properties..." as soon as the first dot of an IP address is entered in the generic search of the <i>Firewall Addresses</i> table. This occurs when there is an address object with a <NULL> subnet.
1034511	<p>Unable to upgrade ADOM from v7.2 to v7.4 due to a crash occurring with the assigned FortiSwitch template.</p> <p><b>Workaround:</b></p> <p>Unassign all FortiSwitch templates and upgrade the ADOM, then create a new model switch.</p>

## Policy & Objects

Bug ID	Description
843716	FortiManager tries to unset url-map for TCP forwarding ZTNA virtual server.
845022	SDN Connector failed to import objects from VMware VSphere.
852603	Per device mapping feature is not available for EMS connector under the <i>Policy &amp; Objects</i> on the FortiManager.
925609	Unused firewall shaping-profile is copied to device db and will be installed to devices.
958206	Policy package import fails due to a certificate error in the SSL VPN web realm configuration for the virtual host server.
967271	Installation failed when trying to remove firewall <code>internet-service-name</code> objects.
970056	The policy installation fails when FortiManager attempts to apply changes related to the "management address" on the interface of the FortiGates.
976795	When attempting to utilize the "Unused Policies" tool in FortiManager (Find Unused Policies), FortiManager fails to present the policies and instead shows an empty window.
993263	Filters in Policy Packages do not function correctly.
997752	<p>Install preview randomly hangs and doesn't return any data on next screen.</p> <p><b>Workaround:</b></p> <p>Close the install preview window and re-run the install.</p>
998850	<p>Modification to Policy with install target does not update the policy package status.</p> <p><b>Workaround:</b></p> <p>Remove the Installation Target and re-add to the policy, which will trigger Policy Package Modification and the install preview will also show the changes made.</p>
1001027	<p>If using Static Route template, FortiManager may become unresponsive when trying to install multiple devices simultaneously.</p> <p><b>Workaround:</b></p>

Bug ID	Description
	Disassociate device from static route template.
1001165	Installation failure while installing the Fortinet_GUI_Server Certificate.
1002787	User external-identity-provider can't be created in the User Definition or CLI configuration under the <i>Policy &amp; Objects</i> .
1002794	<p>FortiManager attempts to remove the existing external-resource when "set external-blocklist-enable-all enable" in AV profile.</p> <p><b>Workaround:</b> Use "set external-blocklist &lt;external-profile-name&gt; &lt;external-profile-name2&gt;".</p>
1003295	"Install On" field in FortiManager does not exist anymore.
1003309	<p>When an address object is cloned, it is not automatically included in the original address group.</p> <p><b>Workaround:</b></p> <p>Manually add the cloned address to the original address group after cloning.</p>
1004056	The installation may encounter an error related to Syntax support for the "ssh-enc-algo" command.
1004929	<p>FortiManager removes the Web Filter Profile from the Profile Group for Policy-Based FortiGates.</p> <p><b>Workaround:</b></p> <p>Use individual profiles in the policy instead of the profile group.</p>
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.
1008729	EMS tags fail to import upon clicking <i>Apply &amp; Refresh</i> .
1009296	"Fork error (out of memory?)" message has been observed when installing Policy Package on multiple targets simultaneously.
1012389	"Negate Source" and "Negate Destination" options are missing.
1012400	<p>The policy package installation is hanging due to a crash in the "securityconsole" application. This is more likely to happen when installing to more than 5 devices.</p> <p><b>Workaround:</b></p> <p>Avoid using static route templates OR template groups.</p>
1012413	Searching for an address object by its IP address does not display the related address groups; instead, it only shows the address object.
1012435	<p>When editing an address group in a firewall policy, the members do not display correctly.</p> <p><b>Workaround:</b></p> <p>First edit the policy, and then edit the address group.</p>
1013434	Unable to add VIP/VIP group in the destination address field of policies, as they are not visible when trying to add them in ADOM 6.4.
1013459	FortiManager fails to load address object in SSL/SSH inspection.

Bug ID	Description
1013948	After upgrading to FortiManager versions 7.2.5 or 7.4.3, the installation preview may hang. However, the installation process itself can be completed successfully.
1013990	There are no commands available for installing source or destination interfaces when adding them to a firewall policy or SNAT rule.
1014499	FortiManager Azure SDN connector is unable to pull K8s label from AKS.
1020917	When "partial-install" feature is enabled, clicking on "Install Objects" can sometimes freeze the GUI, preventing any modifications until it refreshes and also installation may not completed.
1024070	Policy package might not be installed due to the following error message: "unassign template object vpn ipsec phase1-interface <...> fail: Do not delete fortitoken during ADOM to device copy." This case is still under investigation for the root cause analysis (RCA).
1027238	Unable to install when using vlan interfaces within a Virtual Wire Pair Policy

## Revision History

Bug ID	Description
801614	FortiManager might display an error message "Failed to create a new revision." for some FortiGates when retrieving their configurations.

## Script

Bug ID	Description
1008268	The FortiManager script installation process hangs and does not complete.
1011730	FortiManager does not load scripts instantly; it takes a noticeable number of seconds for each script to open.
1012336	Pre-installation from CLI Template fails with the error message "Attribute source-IP check error for RADIUS users."
1020938	After the image upgrade, users may encounter a "Temporarily Unavailable" page message. This problem specifically occurs when special characters, like "\$ ( . . ) ", are used within a TCL script in an ADOM. The Meta variable parsing function incorrectly identifies these characters as meta variable delimiters.

## System Settings

Bug ID	Description
987173	The "ext-auth-group-match" feature doesn't work for SAML SSO users.
1034076	Admin Profile with no access to provisioning template can view provisioning templates by using direct URLs.

## 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 <i>VPN Manager</i>.</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>

## 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 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

### FortiGuard Center update support

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

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