

Release Notes

FortiManager 7.0.15



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



November 14, 2025

FortiManager 7.0.15 Release Notes

02-7015-1222478-20251114

TABLE OF CONTENTS

Change Log	5
FortiManager 7.0.15 Release	6
Supported models	6
Special branch supported models	6
FortiManager VM subscription license	7
Special Notices	8
MEAs removed in FortiManager 7.0.14	8
Custom certificate name verification for FortiGate connection	8
FortiGuard web filtering category v10 update	9
FortiManager 7.2.3 and later firmware on FortiGuard	9
Configuration backup requires a password	10
FortiClient EMS Cloud connectors must be authorized on the EMS Cloud server	10
Option to enable permission check when copying policies	10
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	10
FAP-831F not yet supported by AP Manager	11
Installing policy packages with 80K rules	11
Authorizing FortiGate with FortiClient EMS connected	11
View Mode is disabled in policies when policy blocks are used	11
FortiManager upgrades from 7.0.0	12
Scheduling firmware upgrades for managed devices	12
Modifying the interface status with the CLI	12
SD-WAN with upgrade to 7.0	12
Citrix XenServer default limits and upgrade	13
Multi-step firmware upgrades	13
Hyper-V FortiManager-VM running on an AMD CPU	13
SSLv3 on FortiManager-VM64-AWS	14
Upgrade Information	15
Downgrading to previous firmware versions	15
Firmware image checksums	15
FortiManager VM firmware	16
SNMP MIB files	17
Product Integration and Support	18
Supported software	18
Web browsers	19
FortiOS and FortiOS Carrier	19
FortiADC	19
FortiAnalyzer	19
FortiAuthenticator	20
FortiCache	20
FortiClient	20
FortiDDoS	20

FortiDeceptor	20
FortiFirewall and FortiFirewallCarrier	21
FortiMail	21
FortiProxy	21
FortiSandbox	21
FortiSOAR	22
FortiSwitch ATCA	22
FortiTester	22
FortiWeb	22
Virtualization	22
Feature support	23
Language support	24
Supported models	25
FortiGate models	25
FortiGate special branch models	28
FortiCarrier models	33
FortiCarrier special branch models	34
FortiADC models	36
FortiAnalyzer models	36
FortiAuthenticator models	37
FortiCache models	37
FortiDDoS models	38
FortiDeceptor models	38
FortiFirewall models	38
FortiFirewallCarrier models	39
FortiMail models	40
FortiProxy models	40
FortiSandbox models	40
FortiSOAR models	40
FortiSwitch ATCA models	41
FortiTester models	41
FortiWeb models	42
Resolved Issues	43
Others	43
Known issues	44
New known issues	44
Existing known issues	44
Device Manager	44
Others	44
Policy and Objects	45
Revision History	45
VPN Manager	45
Appendix A - FortiGuard Distribution Servers (FDS)	47
FortiGuard Center update support	47
Appendix B - Default and maximum number of ADOMs supported	48
Hardware models	48
Virtual Machines	48

Change Log

Date	Change Description
2025-11-06	Initial release.
2025-11-14	Updated Supported models on page 6 .

FortiManager 7.0.15 Release

This document provides information about FortiManager version 7.0.15 build 0697.



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 6](#)
- [FortiManager VM subscription license on page 7](#)

Supported models

FortiManager version 7.0.15 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
FortiManager VM	FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019, and 2022), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

Special branch supported models

The following models are released on a special branch of FortiManager 7.0.15. To confirm that you are running the correct build, run the CLI command `get system status` and check that the Branch point field shows 0697.

FMG-410G	is released on build 6122.
-----------------	----------------------------



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 16](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 48](#).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.15.

MEAs removed in FortiManager 7.0.14

There is no support for MEAs in FortiManager 7.0.14 and later.

The following management extension applications (MEAs) are removed in FortiManager 7.0.14:

- FortiAIOps
- FortiSigConverter
- FortiSOAR
- Policy Analyzer
- Universal Connector
- Wireless Manager (FortiWLM)

Custom certificate name verification for FortiGate connection

FortiManager 7.0.12 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 7.0.12, 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 7.0.12 provides a new CLI command to disable this verification. Fortinet recommends to keep the verification enabled.

```
config system global
  fgfm-peercert-withoutsn 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-withoutsn` 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-withoutsn` is enabled, the FortiManager unit does not perform the verification serial number in subject CN or SAN.

FortiGuard web filtering category v10 update

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

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

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

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

FortiManager 7.2.3 and later firmware on FortiGuard

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

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

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

Fortinet has not uploaded FortiManager 7.2.3 and later firmware to FortiGuard in order to work around the GUI bug, however, the firmware is available for download from the Fortinet Support web site

<https://support.fortinet.com>.

Configuration backup requires a password

As of FortiManager 7.0.11, configuration backup files are automatically encrypted and require you to set a password. The password is required for scheduled backups as well.

In previous versions, the encryption and password were optional.

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

FortiClient EMS Cloud connectors must be authorized on the EMS Cloud server

Prior to FortiManager 7.0.9, it was required to provide a username and password when creating EMS Cloud connectors. However, starting from FortiManager 7.0.9, similar to versions 7.2 and 7.4, FortiManager offers the capability to connect to the FortiClient EMS Cloud without the necessity of entering a username and password. With this enhancement, once the connector is configured, FortiManager will automatically appear on the EMS Cloud server under *Administration > Fabric Devices*. Users are required to authorize the FortiManager on the EMS Cloud server before FortiManager can retrieve the EMS tags.

Option to enable permission check when copying policies

As of 7.0.8, 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.

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.

FAP-831F not yet supported by AP Manager

The AP Manager module does not yet support the FAP-831F model.

Installing policy packages with 80K rules

A minimum of 32 GB of memory is required on FortiManager to support the installation of 80K rules to managed FortiGates.

Authorizing FortiGate with FortiClient EMS connected

Please follow the steps below when managing FortiClient EMS Connector's configuration via FortiManager:

1. Add a FortiGate device to FortiManager.
2. Create FortiClient EMS Connector's configuration on FortiManager.
3. Install the configuration onto the FortiGate device.

If the order of the steps is not followed, FortiClient EMS may not authorize the FortiGate device.

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 multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

FortiManager upgrades from 7.0.0

When upgrading from FortiManager 7.0.0, you must first upgrade to 7.0.1 before going to 7.0.2 and later. This is required to correct an issue that causes FortiManager to download unnecessary objects from FortiGuard. Please contact [FortiManager support](#) for more information if required.

Scheduling firmware upgrades for managed devices

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

Modifying the interface status with the CLI

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

For example:

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

SD-WAN with upgrade to 7.0

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

Citrix XenServer default limits and upgrade

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

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
`xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912`
2. Confirm the setting is in effect by running `xenstore-ls`.

`limits = ""`
`pv-kernel-max-size = "33554432"`
`pv-ramdisk-max-size = "536,870,912"`
`boot-time = ""`

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

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

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

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

Hyper-V FortiManager-VM running on an AMD CPU

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

SSLv3 on FortiManager-VM64-AWS

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

```
config system global
set ssl-protocol t1sv1
end
```

Upgrade Information



Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM, including recommended upgrade paths. See [FortiManager 7.0.15 Upgrade Guide](#).



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 6.4 supports ADOM versions 6.0, 6.2, and 6.4, but FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0. Before you upgrade FortiManager 6.4 to 7.0, ensure that all ADOM 6.0 versions have been upgraded to ADOM version 6.2 or later. See [FortiManager 7.0.15 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 15](#)
- [Firmware image checksums on page 15](#)
- [FortiManager VM firmware on page 16](#)
- [SNMP MIB files on page 17](#)

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, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Google Cloud Platform

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

Linux KVM

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

Microsoft Azure

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

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

Microsoft Hyper-V Server

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

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



Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

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

VMware ESX/ESXi

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



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

SNMP MIB files

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

Product Integration and Support

This section lists FortiManager 7.0.15 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 18](#)
- [Feature support on page 23](#)
- [Language support on page 24](#)
- [Supported models on page 25](#)

Supported software

FortiManager 7.0.15 supports the following software:

- [Web browsers on page 19](#)
- [FortiOS and FortiOS Carrier on page 19](#)
- [FortiADC on page 19](#)
- [FortiAnalyzer on page 19](#)
- [FortiAuthenticator on page 20](#)
- [FortiCache on page 20](#)
- [FortiClient on page 20](#)
- [FortiDDoS on page 20](#)
- [FortiDeceptor on page 20](#)
- [FortiFirewall and FortiFirewallCarrier on page 21](#)
- [FortiMail on page 21](#)
- [FortiProxy on page 21](#)
- [FortiSandbox on page 21](#)
- [FortiSOAR on page 22](#)
- [FortiSwitch ATCA on page 22](#)
- [FortiTester on page 22](#)
- [FortiWeb on page 22](#)
- [Virtualization on page 22](#)



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 7.0.15 supports the following web browsers:

- Google Chrome version 142
- Microsoft Edge version 142
- Mozilla Firefox version 144

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 7.0.15 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 7.0.15 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.18
- 6.4.0 to 6.4.16
- 6.2.0 to 6.2.17

FortiADC

FortiManager 7.0.15 supports the following versions of FortiADC:

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

FortiAnalyzer

FortiManager 7.0.15 supports the following versions of FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later

- 6.2.0 and later

FortiAuthenticator

FortiManager 7.0.15 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

FortiCache

FortiManager 7.0.15 supports the following versions of FortiCache:

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

FortiClient

FortiManager 7.0.15 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 7.0.15 supports the following versions of FortiDDoS:

- 6.3.0 and later
- 6.2.0 and later
- 6.1.0 and later

Limited support. For more information, see [Feature support on page 23](#).

FortiDeceptor

FortiManager 7.0.15 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later

- 3.3 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.15 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiMail

FortiManager 7.0.15 supports the following versions of FortiMail:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiProxy

FortiManager 7.0.15 supports configuration management for the following versions of FortiProxy:

- 7.0.14 to 7.0.21
- 7.0.12
- 7.0.5 to 7.0.7



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 23](#).

FortiManager 7.0.15 supports logs from the following versions of FortiProxy:

- 7.0.14 to 7.0.21
- 7.0.12
- 7.0.0 to 7.0.8
- 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 7.0.15 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later
- 3.1.0 and later

FortiSOAR

FortiManager 7.0.15 supports the following versions of FortiSOAR:

- 7.0.0 and later
- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

FortiManager 7.0.15 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.0.15 supports the following versions of FortiTester:

- 7.0.0 and later
- 4.2.0 and later
- 4.1.0 and later

FortiWeb

FortiManager 7.0.15 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

Virtualization

FortiManager 7.0.15 supports the following virtualization software:

Public Cloud

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Alibaba Cloud
- Google Cloud Platform
- 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		✓			

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

Language support

The following table lists FortiManager language support information.

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

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

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

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch 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 7.0.15.



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 25](#)
- [FortiGate special branch models on page 28](#)
- [FortiCarrier models on page 33](#)
- [FortiCarrier special branch models on page 34](#)
- [FortiADC models on page 36](#)
- [FortiAnalyzer models on page 36](#)
- [FortiAuthenticator models on page 37](#)
- [FortiCache models on page 37](#)
- [FortiDDoS models on page 38](#)
- [FortiDeceptor models on page 38](#)
- [FortiFirewall models on page 38](#)
- [FortiFirewallCarrier models on page 39](#)
- [FortiMail models on page 40](#)
- [FortiProxy models on page 40](#)
- [FortiSandbox models on page 40](#)
- [FortiSOAR models on page 40](#)
- [FortiSwitch ATCA models on page 41](#)
- [FortiTester models on page 41](#)
- [FortiWeb models on page 42](#)

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 28](#).

Model	Firmware Version
<p>FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate80E-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, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, 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, FortiGate2201E, 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, FortiGate3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F</p> <p>FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p>FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC</p> <p>FortiGate ACDC: FortiGate-2201E-ACDC, FortiGate-3000F-ACDC, FortiGate-3001F-ACDC, FortiGate-3960E-ACDC</p> <p>FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE</p> <p>FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALL, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI,</p> <p>FortiOS VM: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p> <p>FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G</p>	7.0

Model	Firmware Version
<p>FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-80F-POE, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F</p> <p>FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p>FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, 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-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC</p> <p>FortiGate ACDC: FortiGate-2201E-ACDC, FortiGate-3960E-ACDC</p> <p>FortiGate Hardware Low Encryption: FortiGate-100D-LENC</p> <p>FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F,</p> <p>FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM</p> <p>FortiOS VM: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p> <p>FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G</p>	6.4

Model	Firmware Version
<p>FortiGate: FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FG-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, 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-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-400E-Bypass, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000C, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, 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</p> <p>FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p>FortiGate DC: FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC</p> <p>FortiGate Hardware Low Encryption: FortiGate-80C-LENC, FortiGate-100D-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC</p> <p>FortiWiFi: FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-POE,</p> <p>FortiGate-VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager</p> <p>FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p> <p>FortiGate Rugged: FortiGateRugged-30D, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-90D</p>	6.2

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.15 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 25](#).

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-50G	7.0.17	7592
FortiGate-50G-5G		
FortiGate-50G-DSL		
FortiGate-50G-SFP		
FortiGate-51G		
FortiGate-51G-5G		
FortiGate-51G-SFP-POE		
FortiGate-80F-DSL	7.0.17	7558
FortiGate-90G	7.0.17	7556
FortiGate-91G		
FortiGate-120G	7.0.16	7534
FortiGate-121G		
FortiGate-900G	7.0.17	7551
FortiGate-901G		
FortiGate-1000F	7.0.17	7552
FortiGate-1001F		
FortiGate-3200F	7.0.17	7553
FortiGate-3201F		
FortiGate-3700F	7.0.17	7553
FortiGate-3701F		
FortiGate-4800F	7.0.17	7553
FortiGate-4800F-DC		
FortiGate-4801F		
FortiGate-4801F-DC		
FortiGate-4801F-DC-NEBS		
FortiGate-4801F-NEBS		
FortiGate-6000F	7.0.16	0280
FortiGate-6001F		
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	7.0.16	0280
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	7.0.16	0280
FortiGate-7081F		
FortiGate-7081F-DC		
FortiGate-7081F-2		
FortiGate-7081F-2-DC		
FortiGate-7121F		
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		
FortiGateRugged-50G-5G	7.0.17	7577
FortiGateRugged-70F	7.0.17	7557
FortiGateRugged-70F-3G4G		
FortiGateRugged-70G	7.0.15	7496
FortiGateRugged-70G-5G-Dual	7.0.16	7550
FortiWiFi-50G	7.0.17	7592
FortiWiFi-50G-5G		
FortiWiFi-50G-DSL		
FortiWiFi-50G-SFP		
FortiWiFi-51G		
FortiWiFi-51G-5G	7.0.17	7537
FortiWiFi-80F-2R-3G4G-DSL	7.0.17	7558
FortiWiFi-81F-2R-3G4G-DSL		

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F	6.4.13	5455
FortiGate-401F		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-600F FortiGate-601F	6.4.13	5455
FortiGate-3500F FortiGate-3501F	6.4.6	5886 6132
FortiGate-6000F 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-7121F FortiGate-7121F-2 FortiGate-7121F-2-DC FortiGate-7121F-DC	6.4.13	1926
FortiWiFi-80F-2R FortiWiFi-81F-2R FortiWiFi-81F-2R-3G4G-POE FortiWiFi-81F-2R-POE FortiWiFi-80F-2R-3G4G-DSL	6.4.8	5033

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.13	5238
FortiGate-200F, FortiGate-201F	6.2.13	7249
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.9	7197

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.9	7197
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.9	7197
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiGate-6000F FortiGate-6300F FortiGate-6300F-DC FortiGate-6301F FortiGate-6301F-DC FortiGate-6500F FortiGate-6500F-DC FortiGate-6501F FortiGate-6501F-DC	6.2.13	1271
FortiGate-7000E FortiGate-7030E FortiGate-7040E FortiGate-7060E FortiGate-7060E-8-DC	6.2.13	1271
FortiGate-7000F FortiGate-7081F FortiGate-7121F FortiGate-7121F-2 FortiGate-7121F-2-DC FortiGate-7121F-DC	6.2.13	1271
FortiWiFi-80F-2R-3G4G-DSL FortiWiFi-81F-2R-3G4G-DSL	6.2.6	7219
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

FortiCarrier models

Model	Firmware Version
<p>FortiCarrier: 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-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p>FortiCarrier-ACDC: FortiCarrier-3000F-ACDC, FortiCarrier-3001F-ACDC</p> <p>FortiCarrier-DC: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, 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, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC</p> <p>FortiCarrier-VM: 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-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI</p>	7.0
<p>FortiCarrier: 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-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p>FortiCarrier-DC: FortiCarrier-3000D-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, FortiCarrier-4400F-DC, FortiCarrier-4400F-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC</p> <p>FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen</p>	6.4
<p>FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p>	6.2

Model	Firmware Version
FortiCarrier-DC: FortiCarrier-3000D-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	
FortiCarrier 6K and 7K: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7000F, FortiCarrier-7121F, FortiCarrier-7121F-2	
FortiCarrier 6K and 7K DC: FortiCarrier-6000F-DC, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC, FortiCarrier-7060E-8-DC, FortiCarrier-7121F-DC, FortiCarrier-7121F-2-DC	
FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.0.15 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 33](#).

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F FortiCarrier-3201F	7.0.17	7553
FortiCarrier-3700F FortiCarrier-3701F	7.0.17	7553
FortiCarrier-4800F FortiCarrier-4800F-DC FortiCarrier-4801F FortiCarrier-4801F-DC FortiCarrier-4801F-DC-NEBS FortiCarrier-4801F-NEBS	7.0.17	7553
FortiCarrier-6000F FortiCarrier-6001F FortiCarrier-6300F FortiCarrier-6300F-DC	7.0.16	0280

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-6301F		
FortiCarrier-6301F-DC		
FortiCarrier-6500F		
FortiCarrier-6500F-DC		
FortiCarrier-65001F		
FortiCarrier-6501F-DC		
FortiCarrier-7000E	7.0.16	0280
FortiCarrier-7030E		
FortiCarrier-7040E		
FortiCarrier-7060E		
FortiCarrier-7060E-8-DC		
FortiCarrier-7000F	7.0.16	0280
FortiCarrier-7081F		
FortiCarrier-7081F-DC		
FortiCarrier-7081F-2		
FortiCarrier-7081F-2-DC		
FortiCarrier-7121F		
FortiCarrier-7121F-DC		
FortiCarrier-7121F-2		
FortiCarrier-7121F-2-DC		

FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F	6.4.13	1926
FortiCarrier-6300F		
FortiCarrier-6300F-DC		
FortiCarrier-6301F		
FortiCarrier-6301F-DC		
FortiCarrier-6500F		
FortiCarrier-6500F-DC		
FortiCarrier-65001F		
FortiCarrier-6501F-DC		
FortiCarrier-7000E	6.4.13	1926
FortiCarrier-7030E		
FortiCarrier-7040E		

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

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	6.2, 7.0
FortiADC: FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	6.0, 6.1

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: 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-3900E FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0

Model	Firmware Version
<p>FortiAnalyzer: 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</p> <p>FortiAnalyzer VM: 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</p>	6.4
<p>FortiAnalyzer: FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-1000F, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F and FAZ-3900E.</p> <p>FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).</p>	6.2

FortiAuthenticator models

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

FortiCache models

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-2000F	6.3
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F FortiDDoS VM: FortiDDoS-VM	6.1, 6.2, 6.3

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.1
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.0
FortiDeceptor: FDC-1000F, FDC-3000D FortiDeceptor VM: FDC-VM	3.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.0.15 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewall: FortiFirewall-3001F	7.0	4955
FortiFirewall: FortiFirewall-3501F	7.0	4940
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	7.0	487
FortiFirewall VM: FortiFirewall-VM64	7.0	486
FortiFirewall: FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F FortiFirewall DC: FortiFirewall-3980E-DC, FortiFirewall-4200F-DC	6.4	1999

Model	Firmware Version	Firmware Build
FortiFirewall VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM		
FortiFirewall: FortiFirewall-4401F FortiFirewall DC: FortiFirewall-4401F-DC	6.4	5423
FortiFirewall: FortiFirewall-2600F FortiFirewall DC: FortiFirewall-2600F-DC	6.4	5423
FortiFirewall: FortiFirewall-1801F FortiFirewall DC: FortiFirewall-1801F-DC	6.4	5423
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	6.2	1262
FortiFirewall: FortiFirewall-4200F FortiFirewall DC: FortiFirewall-4200F-DC	6.2.7	5141
FortiFirewall: FortiFirewall-4400F	6.2.7	5148

FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.0.15 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version
FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.0

FortiFirewall special branch models

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0	4940
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F FortiFirewallCarrier-DC: FortiFirewallCarrier-4200F-DC	6.4	1999
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4	5423
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F FortiFirewallCarrier-DC: FortiFirewallCarrier-4200F-DC	6.2.7	5148

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E FortiMail VM: FML-VM, FortiMail Cloud	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E FortiMail VM: FML-VM, FortiMail Cloud	6.2, 6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G FortiProxy VM: FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FortiProxy-KVM, FortiProxy-VM64	1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0, 4.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FSA-VM	3.1, 3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	6.0, 6.4, 7.0

FortiSwitch ATCA models

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

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.1

FortiWeb models

Model	Firmware Version
<p>FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F</p> <p>FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p>	6.4, 7.0
<p>FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E</p> <p>FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer</p>	6.3

Resolved Issues

The following issues have been fixed in 7.0.15. To inquire about a particular bug, please contact [Customer Service & Support](#).

Others

Bug ID	Description
1161082	FortiManager HA cluster status mismatch between GUI and CLI during force-resync.

Known issues

Known issues are organized into the following categories:

- [New known issues on page 44](#)
- [Existing known issues on page 44](#)

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

New known issues

There are no new issues identified in 7.0.15.

Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.0.15.

Device Manager

Bug ID	Description
752443	Vertical scroll bar is missing in SD-WAN configuration.
997344	FortiManager is missing the "set members 0" feature when creating SDWAN Performance SLA.
1102790	FortiManager pushes the unset auto-connect command to config system lte-modem, where the default value is disabled on FortiOS but still enabled on FortiManager.

Others

Bug ID	Description
777831	When FortiAnalyzer is added as a managed device to FortiManager, the "Incident & Event" tile will be displayed instead of "FortiSoC".

Bug ID	Description
988477	There is no detail output information when executing "diagnose cdb check policy-packages".
1080463	An admin with access to a specific ADOM can view the database and clone objects to another ADOM, even if they do not have direct access to it.

Policy and Objects

Bug ID	Description
751443	FortiManager displays policy installation copy failures error when ipsec template gets unassigned. Workaround: Instead of unassigning IPSec template, modify IPSec template, replace the reference to IPSec tunnel interface with another interface. Please ensure a fresh FortiManager backup is created prior to any changes.
845022	SDN Connector failed to import objects from VMware VSphere.
851331	Cloning Firewall Addresses under the Firewall Objects does not clone the "Add To Groups" entries.
925609	Unused firewall shaping-profile is copied to device db and will be installed to devices.

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.

VPN Manager

Bug ID	Description
784385	If policy changes are made directly on the FortiGates, the subsequent policy package import creates faulty dynamic mappings for <i>VPN Manager</i> . Workaround: It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to the workaround. Perform the following command to check & repair the FortiManager's configuration database. <code>diagnose cdb check policy-packages <adom></code>

Bug ID	Description
	After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

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	✓	

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



- FortiManager-VM subscription licenses are fully stackable.
 - For FortiManager-VM perpetual licenses, only the number of managed devices is stackable.
-



www.fortinet.com

Copyright© 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.