

Release Notes

FortiManager 7.0.5



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



Janaury 5th, 2024

FortiManager 7.0.5 Release Notes

02-705-839057-20240105

TABLE OF CONTENTS

Change Log	6
FortiManager 7.0.5 Release	7
Supported models	7
FortiManager VM subscription license	7
Management extension applications	7
Supported models for MEA	8
Minimum system requirements	8
Special Notices	10
FortiManager 7.2.3 and later firmware on FortiGuard	10
FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix	10
FortiManager creates faulty dynamic mapping for VPN manager interface during PP import	11
FortiManager 7.0.5 is not selectable when upgrading from FortiGuard	11
Route-map issue with BGP deployments	11
FAP-831F not yet supported by AP Manager	11
Installing policy packages with 80K rules	12
Authorizing FortiGate with FortiClient EMS connected	12
View Mode is disabled in policies when policy blocks are used	12
FortiManager upgrades from 7.0.0	12
Fortinet verified publisher docker image	12
Scheduling firmware upgrades for managed devices	14
Modifying the interface status with the CLI	14
SD-WAN with upgrade to 7.0	14
Citrix XenServer default limits and upgrade	14
Multi-step firmware upgrades	15
Hyper-V FortiManager-VM running on an AMD CPU	15
SSLv3 on FortiManager-VM64-AWS	15
Upgrade Information	16
Downgrading to previous firmware versions	16
Firmware image checksums	17
FortiManager VM firmware	17
SNMP MIB files	18
Product Integration and Support	19
Supported software	19
Web browsers	20
FortiOS and FortiOS Carrier	20
FortiADC	20
FortiAnalyzer	20
FortiAuthenticator	20
FortiCache	21
FortiClient	21

FortiDDoS	21
FortiDeceptor	21
FortiFirewall and FortiFirewallCarrier	21
FortiMail	21
FortiProxy	22
FortiSandbox	22
FortiSOAR	22
FortiSwitch ATCA	22
FortiTester	23
FortiWeb	23
Virtualization	23
Feature support	23
Language support	24
Supported models	25
FortiGate models	25
FortiGate special branch models	28
FortiCarrier models	31
FortiCarrier special branch models	32
FortiADC models	32
FortiAnalyzer models	33
FortiAuthenticator models	34
FortiCache models	34
FortiDDoS models	34
FortiDeceptor models	34
FortiFirewall models	35
FortiFirewallCarrier models	35
FortiMail models	36
FortiProxy models	36
FortiSandbox models	36
FortiSOAR models	36
FortiSwitch ATCA models	37
FortiTester models	37
FortiWeb models	37
Compatibility with FortiOS Versions	39
FortiManager 7.0.5 and FortiOS 6.2.13 compatibility issues	39
FortiManager 7.0.5 and FortiOS 6.2.14 compatibility issues	39
FortiManager 7.0.5 and FortiOS 6.4.12 compatibility issues	39
FortiManager 7.0.5 and FortiOS 7.0.8 compatibility issues	40
FortiManager 7.0.5 and FortiOS 7.0.9 compatibility issues	40
FortiManager 7.0.5 and FortiOS 7.0.10 compatibility issues	40
Resolved Issues	41
AP Manager	41
Device Manager	41
FortiSwitch Manager	43
Global ADOM	44
Others	44
Policy and Objects	46

Revision History	49
Script	49
Services	50
System Settings	50
VPN Manager	51
Known Issues	52
Device Manager	52
Others	52
Policy & Objects	52
VPN Manager	53
Appendix A - FortiGuard Distribution Servers (FDS)	54
FortiGuard Center update support	54
Appendix B - Default and maximum number of ADOMs supported	55
Hardware models	55
Virtual Machines	55

Change Log

Date	Change Description
2022-10-13	Initial release.
2022-10-17	Updated Resolved Issues on page 41 and Known Issues on page 52 .
2022-10-21	Updated Special Notices on page 10 .
2022-10-27	Updated FortiProxy on page 22 .
2022-10-31	Updated Resolved Issues on page 41 and Known Issues on page 52 .
2022-11-01	Updated FortiOS and FortiOS Carrier on page 20 .
2022-11-08	Added 850548 to Known Issues on page 52 .
2022-11-10	Updated Known Issues on page 52 .
2022-11-16	Updated FortiSandbox on page 22 .
2022-11-30	Updated Appendix A - FortiGuard Distribution Servers (FDS) on page 54 .
2023-02-08	Updated Known Issues on page 52 .
2023-02-16	Updated Special Notices on page 10 .
2023-02-21	Added FortiManager 7.0.5 and FortiOS 7.0.8 compatibility issues on page 40 and FortiManager 7.0.5 and FortiOS 7.0.9 compatibility issues on page 40 . Updated Virtualization on page 23 .
2023-02-23	Updated 784385 in Known Issues on page 52 . Added the workaround in Special Notices on page 10 .
2023-03-03	Added FortiManager 7.0.5 and FortiOS 7.0.10 compatibility issues on page 40 .
2023-03-08	Updated FortiOS and FortiOS Carrier on page 20 .
2023-03-15	Added FortiManager 7.0.5 and FortiOS 6.2.13 compatibility issues on page 39 and FortiManager 7.0.5 and FortiOS 6.4.12 compatibility issues on page 39 .
2023-04-14	Updated FortiOS and FortiOS Carrier on page 20 .
2023-06-08	Updated Special Notices on page 10 and Known Issues on page 52 .
2023-06-23	Updated Special Notices on page 10 and Known Issues on page 52 .
2023-07-12	Updated Special Notices on page 10 and Known Issues on page 52 .
2024-01-05	Updated Special Notices on page 10 .

FortiManager 7.0.5 Release

This document provides information about FortiManager version 7.0.5 build 0365.



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

This section includes the following topics:

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

Supported models

FortiManager version 7.0.5 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_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

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 17](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 55](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.0.5.



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

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

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG_VM64_ALI, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-IBM, 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
- 8 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*
FortiAIOps	<ul style="list-style-type: none"> • 8 vCPU • 32 GB RAM • 500 GB disk storage 	No change
FortiPortal	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
FortiSigConverter	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
FortiSOAR	<ul style="list-style-type: none"> • 4 vCPU 	<ul style="list-style-type: none"> • 16 vCPU

Management Extension Application	Minimum system requirements	Recommended system resources for production*
	<ul style="list-style-type: none"> 8 GB RAM 500 GB disk storage 	<ul style="list-style-type: none"> 64 GB RAM No change for disk storage
Policy Analyzer	<ul style="list-style-type: none"> 4 vCPU 8 GB RAM 	No change
SD-WAN Orchestrator	<ul style="list-style-type: none"> 4 vCPU 8 GB RAM 	<ul style="list-style-type: none"> 4 vCPU 12 GB RAM
Universal Connector	<ul style="list-style-type: none"> 1 GHZ vCPU 2 GB RAM 1 GB disk storage 	No change
Wireless Manager (FortiWLM)	<ul style="list-style-type: none"> 4 vCPU 8 GB RAM 	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 7.0.5.

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>.

FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix

Scenario: Multi-VDOM is enabled on FGTs version 6.4 and external-resource objects are created globally; these objects are being used in webfilter and firewall policies. After upgarding the FGTs to v7.0, the FGTs automatically add a "g-" prefix to the global external-resource. However, FMG has not supported this prefix yet, so FMG fails to retrieve FGT's configuration to DB.

Workaround: There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes.

First workaround approach:

1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed.
2. Delete the global threat feed objects.

Second workaround approach:

1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.
2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.
3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.
4. Retrieve the FGT configuration from FMG.

5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.

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.

FortiManager 7.0.5 is not selectable when upgrading from FortiGuard

Due to known issue 845656, FortiManager 7.0.5 is not listed as an option to upgrade when performing an upgrade from FortiGuard in *System Settings > Firmware Management*.

You can perform an upgrade to FortiManager 7.0.5 using an image downloaded from the Customer Service & Support portal, however, if you are using BGP on FortiGates, an alternative special branch build is available to use. See [Route-map issue with BGP deployments on page 11](#).

Route-map issue with BGP deployments

When using BGP on FortiGates, a special branch build of FortiManager 7.0.5 is available to fix bug 845656. See [Known Issues on page 52](#).

For more information about the special branch build, contact [Customer Service & Support](#).

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

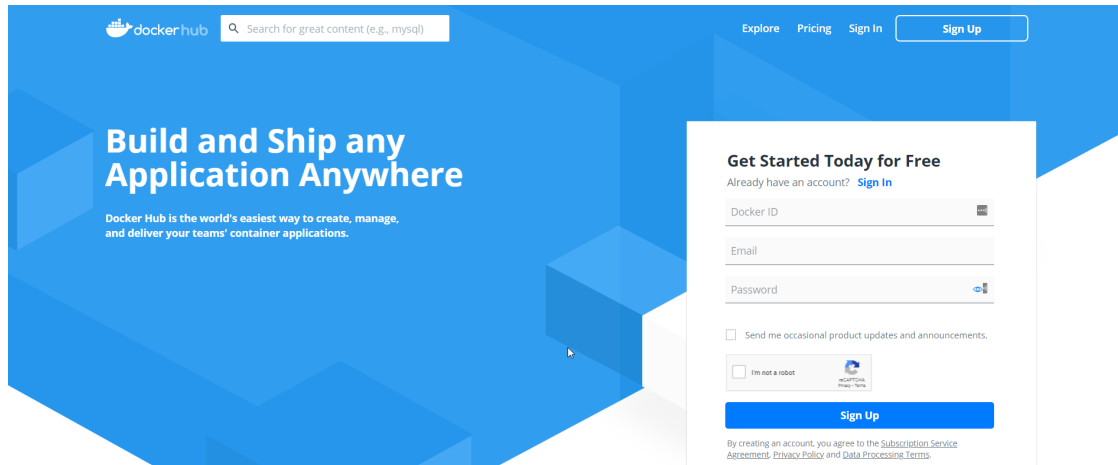
When upgrading from FortiManager 7.0.0, you must first upgrade to 7.0.1 before going to 7.0.2 and later. This is required to correct an issue that causes FortiManager to download unnecessary objects from FortiGuard. Please contact [FortiManager support](#) for more information if required.

Fortinet verified publisher docker image

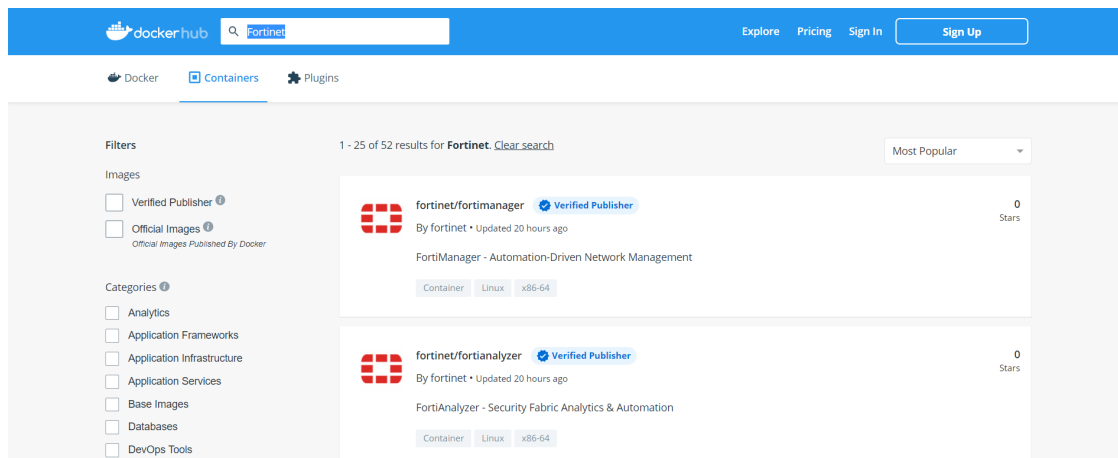
FortiManager docker images are available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

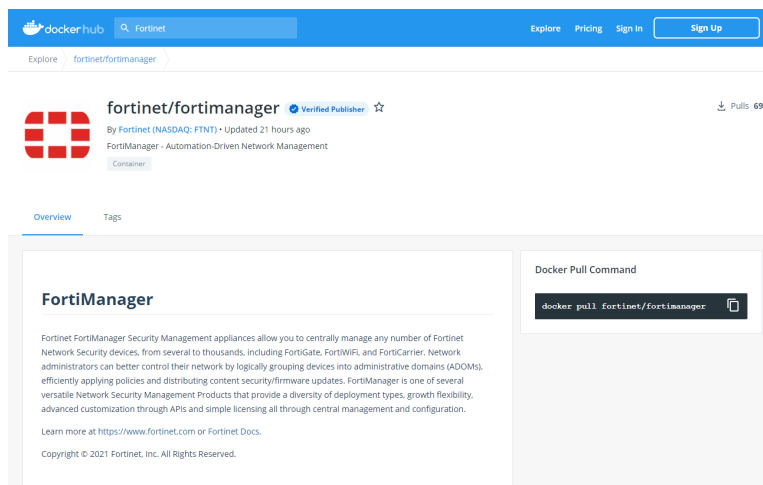
1. Go to dockerhub at <https://hub.docker.com/>.
The dockerhub home page is displayed.



2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortimanager*.
The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the *Overview* tab, copy the docker pull command, and use it to download the image.
The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

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 7.0.5 Upgrade Guide](#).

You can upgrade to FortiManager 7.0.5 from the following versions:

- FortiManager 6.4.0 to 6.4.x
- FortiManager 7.0.1 to 7.0.x

See also [FortiManager upgrades from 7.0.0 on page 12](#).



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 7.0.5 Upgrade Guide](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 16](#)
- [Firmware image checksums on page 17](#)
- [FortiManager VM firmware on page 17](#)
- [SNMP MIB files on page 18](#)

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 7.0.5 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 19](#)
- [Feature support on page 23](#)
- [Language support on page 24](#)
- [Supported models on page 25](#)

Supported software

FortiManager 7.0.5 supports the following software:

- [Web browsers on page 20](#)
- [FortiOS and FortiOS Carrier on page 20](#)
- [FortiADC on page 20](#)
- [FortiAnalyzer on page 20](#)
- [FortiAuthenticator on page 20](#)
- [FortiCache on page 21](#)
- [FortiClient on page 21](#)
- [FortiDDoS on page 21](#)
- [FortiDeceptor on page 21](#)
- [FortiFirewall and FortiFirewallCarrier on page 21](#)
- [FortiMail on page 21](#)
- [FortiProxy on page 22](#)
- [FortiSandbox on page 22](#)
- [FortiSOAR on page 22](#)
- [FortiSwitch ATCA on page 22](#)
- [FortiTester on page 23](#)
- [FortiWeb on page 23](#)
- [Virtualization on page 23](#)



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 7.0.5 supports the following web browsers:

- Microsoft Edge 102 (102.0.1245.33 or later)
- Mozilla Firefox version 101
- Google Chrome version 102 (102.0.5005.63 or later)

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 7.0.5 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 7.0.5 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.10
- 6.4.0 to 6.4.12
- 6.2.0 to 6.2.14

FortiADC

FortiManager 7.0.5 supports the following versions of FortiADC:

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

FortiAnalyzer

FortiManager 7.0.5 supports the following versions of FortiAnalyzer:

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

FortiAuthenticator

FortiManager 7.0.5 supports the following versions of FortiAuthenticator:

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

FortiCache

FortiManager 7.0.5 supports the following versions of FortiCache:

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

FortiClient

FortiManager 7.0.5 supports the following versions of FortiClient:

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

FortiDDoS

FortiManager 7.0.5 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 7.0.5 supports the following versions of FortiDeceptor:

- 4.1 and later
- 4.0 and later
- 3.3 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.5 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 7.0.5 supports the following versions of FortiMail:

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

FortiProxy

FortiManager 7.0.5 supports configuration management for the following versions of FortiProxy:

- 7.0.6
- 7.0.5



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

FortiManager 7.0.5 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.7
- 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 7.0.5 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 7.0.5 supports the following versions of FortiSOAR:

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

FortiSwitch ATCA

FortiManager 7.0.5 supports the following versions of FortiSwitch ATCA:

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

FortiTester

FortiManager 7.0.5 supports the following versions of FortiTester:

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

FortiWeb

FortiManager 7.0.5 supports the following versions of FortiWeb:

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

Virtualization

FortiManager 7.0.5 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- 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			✓	✓	✓

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
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 7.0.5.



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 25](#)
- [FortiGate special branch models on page 28](#)
- [FortiCarrier models on page 31](#)
- [FortiCarrier special branch models on page 32](#)
- [FortiADC models on page 32](#)
- [FortiAnalyzer models on page 33](#)
- [FortiAuthenticator models on page 34](#)
- [FortiCache models on page 34](#)
- [FortiDDoS models on page 34](#)
- [FortiDeceptor models on page 34](#)
- [FortiFirewall models on page 35](#)
- [FortiFirewallCarrier models on page 35](#)
- [FortiMail models on page 36](#)
- [FortiProxy models on page 36](#)
- [FortiSandbox models on page 36](#)
- [FortiSOAR models on page 36](#)
- [FortiSwitch ATCA models on page 37](#)
- [FortiTester models on page 37](#)
- [FortiWeb models on page 37](#)

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
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, 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-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, 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, FortiGate2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, 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	7.0
FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
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-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	
FortiGate ACDC: FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
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	
FortiGate VM: 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, FortiGateVM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI,	
FortiOS VM: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
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, FortiGate-80E-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	6.4
FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
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	
FortiGate ACDC: FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
FortiGate Hardware Low Encryption: FortiGate-100D-LENC	
FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F,	
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	
FortiOS VM: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
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 FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 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 FortiGate Hardware Low Encryption: FortiGate-80C-LENC, FortiGate-100D-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC 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, 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 FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen FortiGate Rugged: FortiGateRugged-30D, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-90D	6.2

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.5 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 25](#).

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-70F	7.0.5	4530
FortiGate-71F		
FortiGate-3000F	7.0.5	4451
FortiGate-3001F	7.0.5	4436
FortiGate-3700F	7.0.5	6066
FortiGate-3701F		

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F	6.4.8	5206
FortiGate-401F		
FortiGate-600F	6.4.8	5306
FortiGate-601F	6.4.8	5301
FortiWiFi-80F-2R	6.4.8	5033
FortiWiFi-81F-2R		
FortiWiFi-81F-2R-3G4G-POE		
FortiWiFi-81F-2R-POE		
FortiWiFi-80F-2R-3G4G-DSL		
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132
FortiGate-6000F	6.4.8	1823
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E	6.4.8	1823
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7000F	6.4.8	1823
FortiGate-7121F		
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80D	6.2.10	5168
FortiGate-1800F, FortiGate-1800F-DC	6.2.9	7197
FortiGate-1801F, FortiGate-1801F-DC		
FortiGate-2600F, FortiGate-2600F-DC	6.2.9	7197
FortiGate-2601F, FortiGate-2601F-DC		
FortiGate-4200F, FortiGate-4200F-DC	6.2.9	7197
FortiGate-4201F, FortiGate-4201F-DC		
FortiGate-4400F, FortiGate-4400F-DC	6.2.9	7197
FortiGate-4401F, FortiGate-4401F-DC	6.2.9	7197
FortiGate-6000F	6.2.10	1211
FortiGate-6300F		
FortiGate-6300F-DC		
FortiGate-6301F		
FortiGate-6301F-DC		
FortiGate-6500F		
FortiGate-6500F-DC		
FortiGate-6501F		
FortiGate-6501F-DC		
FortiGate-7000E		
FortiGate-7030E	6.2.10	1211
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F		
FortiGate-7121F	6.2.10	1211
FortiGate-7121F-2		
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		

FortiGate Model	FortiOS Version	FortiOS Build
FortiWiFi-80F-2R-3G4G-DSL	6.2.6	7219
FortiWiFi-81F-2R-3G4G-DSL		
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099

FortiCarrier models

Model	Firmware Version
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 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 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	7.0
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 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 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	6.4
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	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-ALL, 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 FortiCarrier. FortiManager version 7.0.5 supports these models on the identified FortiCarrier version and build number.

FortiCarrier 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiCarrier-3700F	7.0	Build 304 and special branch 6066.
FortiCarrier-3701F	7.0	Build 304 and special branch 6070.
FortiCarrier-3000F FortiCarrier-3001F	7.0	Build 304 and special branch 4451.

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	

Model	Firmware Version
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-DOCKER, 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
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 FortiAnalyzer VM: FortiAnalyzer-DOCKER, 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: 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. FortiAnalyzer VM: FortiAnalyzer-DOCKER, 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).	6.2

FortiAuthenticator models

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

FortiCache models

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-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 7.0.5 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewall: FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F FortiFirewall DC: FortiFirewall-3980E-DC FortiFirewall VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	1999
FortiFirewall: FortiFirewall-4401F FortiFirewall DC: FortiFirewall-4401F-DC	6.4	5318
FortiFirewall: FortiFirewall-2600F FortiFirewall DC: FortiFirewall-2600F-DC	6.4	5305
FortiFirewall: FortiFirewall-1801F FortiFirewall DC: FortiFirewall-1801F-DC	6.4	5334
FortiFirewall: FortiFirewall-3980E FortiFirewall DC: FortiFirewall-3980E-DC	6.2	1262
FortiFirewall: FortiFirewall-4200F	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 7.0.5 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	1999
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4	5318
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	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	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	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-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
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	6.4, 7.0

Model	Firmware Version
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
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	6.3
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, 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 7.0.5. Compatibility issues have been identified for the following FortiOS releases:

FortiOS 6.2	<ul style="list-style-type: none">• FortiManager 7.0.5 and FortiOS 6.2.13 compatibility issues on page 39• FortiManager 7.0.5 and FortiOS 6.2.14 compatibility issues on page 39
FortiOS 6.4	<ul style="list-style-type: none">• FortiManager 7.0.5 and FortiOS 6.4.12 compatibility issues on page 39
FortiOS 7.0	<ul style="list-style-type: none">• FortiManager 7.0.5 and FortiOS 7.0.8 compatibility issues on page 40• FortiManager 7.0.5 and FortiOS 7.0.9 compatibility issues on page 40• FortiManager 7.0.5 and FortiOS 7.0.10 compatibility issues on page 40

FortiManager 7.0.5 and FortiOS 6.2.13 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 6.2.13. FortiOS 6.2.13 includes syntax changes not supported by FortiManager 7.0.5.

The following objects were added:

```
(attr) system global http-request-limit
(attr) system global http-unauthenticated-request-limit
```

FortiManager 7.0.5 and FortiOS 6.2.14 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 6.2.14. FortiOS 6.2.14 includes syntax changes not supported by FortiManager 7.0.5.

The following objects were added:

```
(attr) system global http-request-limit
(attr) system global http-unauthenticated-request-limit
```

FortiManager 7.0.5 and FortiOS 6.4.12 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 6.4.12. FortiOS 6.4.12 includes syntax changes not supported by FortiManager 7.0.5.

The following objects were added:

```
(attr) system global http-request-limit
(attr) system global http-unauthenticated-request-limit
```

FortiManager 7.0.5 and FortiOS 7.0.8 compatibility issues

The following table lists interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 7.0.8.

Bug ID	Description
827602	[EMS Connector] Unable to import EMS Tags from EMS Server.

FortiManager 7.0.5 and FortiOS 7.0.9 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 7.0.9 in mantis 861815. FortiOS 7.0.9 includes syntax changes not supported by FortiManager 7.0.5.

The following default values changed:

`system global internet-service-database` changed from `full` to `standard`.

The following objects were added:

```
(attr) system speed-test-server host distance
(attr) system speed-test-server host latitude
(attr) system speed-test-server host longitude
```

FortiManager 7.0.5 and FortiOS 7.0.10 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.0.5 and FortiOS 7.0.10. FortiOS 7.0.10 includes syntax changes not supported by FortiManager 7.0.5.

The following objects were removed:

- (attr) system global http-request-limit
- (attr) system global http-unauthenticated-request-limit
- (attr) system speed-test-server host distance
- (attr) system speed-test-server host latitude
- (attr) system speed-test-server host longitude

Additional option changes:

- wireless-controller vap radius-mac-mpsk-timeout
int-range (tag|lmt): 300,864000 -> 1800,864000

Resolved Issues

The following issues have been fixed in 7.0.5. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
661938	FortiManager displays an error when trying to edit and save managed APs.
755815	The "local-standalone" and "local-authentication" features are inconsistent with FortiOS/FortiGate.
794836	Protected Management Frames (PMF) feature always gets disabled when security mode is set to WPA2 (Enterprise or Personal).
819137	Installation failed if Distributed Automatic Radio Resource Provisioning (DARRP) is disabled on AP Profile.

Device Manager

Bug ID	Description
723006	FortiManager does not support creating the "DHCP Reservation" under the <i>Network Monitors</i> widget.
738276	FortiManager's GUI does not display the "Routing Objects" under "Router".
745122	FortiManager unsets the IPv6 configuration during the installation to the FortiGate.
745586	Local firmware images are duplicated under the <i>Device Manager</i> .
746697	Not able to delete the phase2-interface within the IPsec template.
748579	CLI configurations for SD WAN template is not working properly.
752754	Interface Edit button is grayed out, but double-clicking on the interface still lets the users modify and save the new configuration.
757045	Installation failed with "invalid ip address" error when configuring the multiple IPs for system dns-database's forwarder as the meta field.
759264	Applied system template does not apply properly on "Install Wizard" mode after modifying config on device level.

Bug ID	Description
763234	Installation failed due to the syntax's difference between FortiGate and FortiManager in setting log-disk-quota for VDOMs.
770600	Comma between IP address and subnet causes saving problem on Prefix List Rule under BGP Templates.
771417	Cannot override system template settings.
778131	FortiManager did not support the per device mapping for user SAML configurations.
780395	FortiManager displays a blank page when creating the rules under the "distribute access list" for the <i>BGP Templates</i> .
786264	Unable to delete default "wireless-controller" "vap" configuration from the device DB.
787905	PM/AM feature for AV&IPS Scheduled Updates under the FortiGuard's <i>Device Manager</i> cannot be set correctly.
788923	SD-WAN template does not change the value of "service-sla-tie-break" for an SD-WAN Zone.
796447	FortiManager shows CLI Provisioning templates even after removing association of Provisioning template.
801022	Config status gets modified even though the installation preview is empty.
801415	FortiManager adds quotations to IP addresses when configuring trusted hosts for "switch-controller snmp-community" under the GUI's CLI Configuration.
803289	The "Routing - Static & Dynamic" widget gets added successfully, but disappears after a page refresh.
804142	Creating the "EMACVLAN" type interface on FortiManager displays an error: "VLAN ID is required".
804502	Installation fails due to pushing the previous password expiration date to FortiGates.
805208	The forwarder IP in the DNS database is set to "[object Object]".
806622	Installation failed after configuring the link-monitor.
809793	Unable to create vdom link with vcluster.
812213	Default factory setting on FortiGate does not match with its default factory setting on FortiManager's DB. This causes status conflict if FortiGate added to the FortiManager using the "Add Model Device" method.
812687	Unable to add FortiGate WiFi-80F-2R to FortiManager when Trusted Platform Module (TPM) is enabled.
813339	First install after adding a FortiGate to the FortiManager failed due to FortiManager's attempt for installing a new SSID passphrase for the Virtual Access Point (VAP).
819710	FortiManager does not display the VDOMs optmode correctly.
820436	FortiManager displays an error "Failed to update device management data.", when adding a model device based on ZTP approach.

Bug ID	Description
820990	IPSec VPN deployment via ZTP creates some issues on the FortiGate routing.
821866	For FortiGates with FGSP (FortiGate Session Life Support Protocol) configuration, the "ipsec-tunnel-sync" feature under the cluster-sync cannot be disabled.
823092	Not able to add multiple OU (Organization Unit) fields in the <i>Certificate Templates</i> .
823281	Changing Time/Schedule for scripts under the <i>Device Manager</i> makes the "OK" button grayed out.
826141	VLAN interface cannot be created and mapped to a hardware switch interface on the FortiManager.
828122	"Device Detection" gets enabled by FortiManager during the installation.
830105	FortiManager attempts to install 1.0.0.0 as the remote-gw for all the phase1-interfaces when 2 or more IPsec phase1-interfaces have same remote-gw IP.
830727	FortiManager-DOCKER platform does not support adding the FortiAnalyzer-DOCKER device.
832321	Configuration changes on the AP/Switch/Extender settings do not apply on the device DB when these changes are created from the system template.
832753	FortiManager does not install configurations from CLI Template group to FortiGates.
834947	"Resource-limits" proxy default value is missing under the Device Manager's CLI Configurations.
835451	Editing SD-WAN/IPSec template (with no actual changes) removes all assigned devices.
842923	Auto-update fails to sync FortiManager's device DB when interfaces are modified directly in the root VDOM of the FortiGates.
847631	Failed to reload the FortiGate's configuration.

FortiSwitch Manager

Bug ID	Description
755444	Failed to import <i>FortiSwitch Template</i> due to the datasrc invalid error message.
803175	<i>FortiSwitch Template</i> does not enable all the POE interfaces.
817436	LLDP profile cannot be changed when Access Mode has been set to nac in <i>Fortiswitch Template</i> .
829700	FortiManager shows errors while installing FortiSwitch configuration.
830099	<i>FortiSwitch Manager</i> displays the "Missing Switch ID or Platform Info" error.
833262	<i>FortiSwitch Manager</i> does not display the list of firmware images for the FSW 108F-FPOE model.

Global ADOM

Bug ID	Description
767325	Failed to assign global ADOM v6.2 policy to local ADOM v6.4 due to policy IPv6 changed duplicate object.
811660	Global Database object assignment to ADOMs fails.
815130	Global Policy Assignment in FortiManager displays the "TCL error - dstintf in policy cannot be empty" error.
835172	Global ADOM Assignment fails when assigning some profile groups.
835439	Global Policy assignment is not completed successfully due to some missing objects on Global ADOM.
838174	FortiManager does not provide a clear error message when Global IPS Header/Footer profile assignment fails.
842934	Global address group cannot be modified from FortiManager GUI.
847533	Unassigned Policy Package cannot be removed from Global ADOM.

Others

Bug ID	Description
739219	FortiManager's timeout parameters cannot be set by users as it is hardcoded.
742819	Promote to global feature should not be possible since GLOBAL ADOM are not accessible in FortiManager Cloud.
747648	FortiManager does not support some of the FortiExtender models and versions under the <i>FortiExtender Profiles</i> .
750242	FortiManager's DB in HA clusters are not properly synced together.
757524	FortiManager displays many "duplicate license for [FGT devices SN Number] copy AVDB to AVEN" error messages.
759333	After upgrading ADOM 6.2 to 6.4, status of all Policy Packages changed to modified.
770040	FortiManager's web interface and especially API calls are very slow if object-revision-status feature is enabled.
784037	FortiManager offers low encryption cipher Suite in TLS 1.2.
786281	During the installation, FortiManager displays Policy Consistency Check failure without any clear reason.
793085	Sub Type Filter on Event Log search does not show any results, even if logs are present.

Bug ID	Description
795624	FortiManager does not let users to copy the contents of the "View Progress Report".
799378	FortiManager's admins are not able to run FortiManager's CLI scripts/commands from remote stations.
801871	Unable to finish the ZTP installation process successfully.
806109	After ADOM upgrade, log-all is disabled for all protocols under Email Filter profile.
806522	Application websocket crashes and makes FortiManager's GUI unresponsive.
808822	Changing the HTTPS port used for Administrative Web Access will cause FortiManager to stop listening to port 443 for FortiGate update requests.
811018	FortiManager does not support coping of the objects from the Policy Packages and pasting them to the search field.
811379	Users cannot tick any of the checkboxes for individual interfaces under the "speed-test-schedule" under the Device Manager's CLI-Configuration.
815875	After FortiManager's upgrade, device level status has been modified and Install preview shows that pdf-report and fortiview features will be enabled on the FortiGates even if these are already enabled on the FortiGates before.
816444	<i>Extender Manager</i> doesn't display RSSI/RSRP/RSRQ/SINR info.
816834	FortiManager does not support FortiWeb and activate its license.
817667	FortiManager cannot upgrade the ADOM to v7.0 due to several cdb crashes during the upgrade.
820071	Upgrading the FortiOS/FortiGate firmware version via FortiManager did not complete successfully.
820248	Cloning same ADOM multiple times fails with error "Unknown DVM error".
820578	The "svc authd" process is consuming 100% of CPU.
820656	FortiGate 7.2.1 failed to fetch the FortiGuard rating from FortiManager without raw DB Flags.
822286	Adding FortiExtender to <i>FortiExtender Manager</i> using name field causes device settings installation failure.
823111	After upgraded to 7.0.4, FortiManager removes the dev-obj data upon rebooting.
823278	Unable to manually import Query Category FortiGuard package.
823294	SSH connection between FortiGate and FortiAnalyzer/FortiManager v7.0.4/7.2.1 or later fails due to server_host_key_algorithms mismatch.
823547	In Advanced ADOM mode, it is not possible to create a new VDOM in a new ADOM via JSON API request.
823872	FortiManager lost its access to GUI, if a same IP makes more than 250 connections to https admin port.
824316	FortiManager displays an error when "adom-integrity" is performed.

Bug ID	Description
825052	Not able to add the FortiProxy to the FortiProxy ADOM.
826718	Failed to delete the hanging task from task monitor.
826881	FortiManager attempts to apply some changes to voice, video, and interface configurations.
829726	Already existing CLI Templates cannot be modified after the upgrade.
830881	ADOM upgrade fails due to the ID of the sdwan applications; they are larger than the initial defined values.
831453	FortiManager shows an error message when multiple FortiGates are selected to be upgraded to the new version.
833162	FortiManager does not support the FortiProxy 7.0.6.
833623	Estimated Bandwidth for Upstream & Downstream under the interfaces and Upload & Download values under the SD-WAN Monitor's table-view are displayed differently.
835313	FortiManager displays many "duplicate licence" messages for "copy AVDB to AVEN".
835748	FortiManager's GUI takes a very noticeable time to load properly when navigating to <i>Policy & Objects</i> tab.
836489	Firmware Images under the FortiGuard for "All" or "Managed" devices display same list.
839035	"Check License" under the FortiGuard's Licensing Status does not Keep the changes.
840068	Unable to export device stored FortiGuard signatures through TFTP.

Policy and Objects

Bug ID	Description
620680	FortiManager does not support the geographic fields data for firewall internet-service Objects.
686150	FortiManager cannot import NSX-T dynamic IP when VPN Objects are presented in NSX-T Manager.
688586	Exporting Policy Package to "CSV" shows "certificate-inspection" in the "ssl-ssh-profile" column even when the profile is not in use.
703408	FortiManager does not display the interface type Geneve for interface mapping.
704354	"Blocked Certificates" and "Server certificate SNI check" features cannot be configured on SSL/SSH profile.
707481	Deleting DNS filter profile does not deletes the associated Domain filter.
716943	FortiManager's GUI shows so many blank areas after adding the IPS Signatures and Filters.
724011	FortiManager needs to support multiple server certificate list in ssl/ssh profile.

Bug ID	Description
731961	When FortiManager is working in the workspace mode, the installation for those FortiManagers with larger DB may take a longer time to be completed.
762392	The rating lookups does not return the correct category for the URL when it ends with "/" character.
765154	Installation fails when trying to disable the "safe search" on existing DNS filter from FortiManager.
768125	Default configurations of the Potentially Liable category under the Webfilter are different from their corresponding ones on FortiGate.
778171	After the upgrade, FortiManager is changing the "config antivirus quarantine" setting; this fails the installation.
783195	FortiManager changes the "cert-validation-timeout" value to "block" when installing to the FortiGates.
787195	FortiManager skips the zone interface policy without displaying copy fail error message.
789238	Installation error occurs when configuring a VIP with per-device mapping and setting an External IP Range to an IPv4 Range.
793603	Registering a service under the connector configuration displays an error "Failed to run script."
794731	The Policy package counter field does not display the number of modified policy packages.
798955	Traffic shaping policy changes does not trigger any changes/updates on the Policy Packages status.
805178	Installation failed due to the unnecessary setting changes of logtraffic feature in proxy policy.
805211	Installation failed due to the wrong fsw vlan type for the default nac and nac_segment vlans.
805642	New policies created in policy package do not inherit "global-label" section.
805649	Any modification on the "peer group" object within <i>VPN Manager</i> pane, makes all devices' policy status "Modified" even though spoke devices have different policy packages than Hub devices.
807287	Unable to change virtual server objects on FortiManager's <i>Policy & Objects</i> .
808900	Incorrect error message is displayed when re-installing the same policy to FortiGate immediately after the first installation.
809888	Replacement Message Group under Security profiles gets removed by FortiManager during the installation.
811715	FSSO dynamic addresses were visible on two address groups.
812886	On FortiManager, an internet-service-custom objects without protocol number or port-range can be configured on firewall proxy-policy; however, FortiGate/FortiOS does not support this.
812909	FortiManager unsets the "bypass-watchdog" setting on FGT400E-Bypass.

Bug ID	Description
813237	ViewMode feature does not work properly when workspace mode is enabled on FortiManager.
814468	FortiManager purges 'gcp-project-list' and unsets several values from GCP sdn-connector.
814970	EMS Connector is not able to import Tags when Multi-Site is enabled on EMS Server.
815281	SDN Dynamic Address object filter does not display the list properly.
815812	Installation failed because FortiManager tried removing the credentials for Amazon Web Services (AWS) type SDN Connector and enabling the "use-metadata-iam" feature.
816108	The "group-poll-interval" value for FSSO fabric connector cannot configured properly.
816121	FortiManager displays an improper error message when importing the policy package.
816347	Objects Field search under the "Add Object(s)" feature does not properly locate any firewall object addresses for Source & Destination.
818512	In WorkFlow Mode, adding a single policy removes and re-adds the entire policies.
819665	Installation Preview does not display the DNS-Filter configuration changes.
819713	FortiManager in task manager does not show the specific admin name who refreshes the hit-count.
820939	"Firewall Users" does not populate the user authenticated via explicit proxy authentication method.
820993	For Proxy-Policy, FortiManager unsets the "PROFILE-PROTOCOL-OPTION" when installing to the FortiGates.
821412	The Policy Block's name cannot be edited if "/" character is being used.
822843	FortiManager displays an error when using the access-proxy type VIP and normal VIP in firewall policies as they are both using the same external IP.
825411	Installation fails when an application group with category 32 (unknown applications) is configured on FortiManager, even though this category is accepted on the FortiGate.
825530	Explicit web proxy policy does not allow selecting any source address objects.
826928	During the installation, FortiManager attempts to remove the physical ports which are members of the virtual-switch config.
826946	FortiManager does not show anything to install on FortiGates even though the Policy Package has been modified.
827242	For Policies under the Advanced Options, "custom-log-field" uses Names instead of IDs.
827800	When creating the address group on FortiManager, the "Exclude Members" field is not available.
828492	Policy installation fails when using "sdn-addr-type all".
830043	Creating the Custom ipv6 service where icmpcode is not configured causes the Policy Package to get into a conflict state.

Bug ID	Description
830502	FortiManager fails to create the CSV for Policy Package.
831225	Cloning a policy with VIP referencing SDWAN member causes subsequent installs to fail.
831273	FortiManager does not allow deleting the entries for "server-info" under the log "npu-server".
831407	NSX-T connector configuration does not display "VM16" and "VMUL" types.
831484	FortiManager was not able to connect to the "NSX-T Connector" and several "Application connector" failures have been observed.
832962	If Firmware Template status is "Unknown", FortiManager allows installing the Policy & Packages repeatedly to the FortiGates.
834447	Objects are not visible in the <i>Addresses</i> tab when the per-device mapping feature is enabled.
835079	Detail of the "Firewall Security Policy" when running the Policy Package Diff does not display data for all fields.
836783	FortiManager changes the "use-metadata-iam" value for the SDN connectors.
837555	Connector's Service Name, after FortiManager's upgrade, does not display the correct name.
838533	SASE zone cannot be removed from SDWAN Template.
841966	When inserting "Above" or "Below" to add policy, the policy is added to the wrong section/place.
849470	When creating a new firewall policy via API Request, the "global-label" option is skipped.

Revision History

Bug ID	Description
722332	For AP Profile change, installation preview may show No Entry.
809191	Configuration change of HA-logs setting is not reflected into the revision history.

Script

Bug ID	Description
808398	"View script executing history" displays scripts related to other ADOMs.
817172	Running scripts to add static route has been failed due to the "duplicate of static route" error.
821778	Using scripts does not create the ssl-ssh-profile with certificate inspection mode; instead it sets the value to deep-inspection mode.

Services

Bug ID	Description
779997	When upgrading the multiple FortiGates at the same time from the "Firmware Upgrade" feature does not let users to click "OK".
827982	Downstream FortiManagers cannot get all the FDS/FGD packages from upstream FortiManagers in cascade mode network design.

System Settings

Bug ID	Description
687223	Users may not be able to upgrade ADOM because of profile-protocol-options.
777153	FortiManager displays an error when setting up a "Remote Authentication Server" with "No Certificate" option.
780245	Install Wizard shows all devices are selected even-though "Default Device Selection for Install" is set to "Deselect All".
796058	Search box in the "Edit Meta Fields" page under the <i>System Settings</i> does not work.
799519	If Management Extension Applications (MEA) are enabled, all system settings may be lost after upgrading the FortiManager.
807983	FortiManager doesn't display "NTP daemon change time" event log when it synchronizes with the NTP server at booting.
809276	Cloning administrators doesn't copy the specified ADOMs for the cloned administrator and wrongly display "All ADOMs".
815728	FortiManager takes very long hours to rebuild the HA Cluster back to synchronization status.
817244	Sorting function feature does not work properly based on the "Device" column in the "Meta Fields" under the system settings.
818969	Unable to poll SNMP with SNMP Engine ID.
819383	FortiManager disk usage rises to 100% due to traffic-shaping-history enabled.
822316	For RADIUS wildcard config, if "ext-auth-adom-override" feature is enabled, the APIs access are not allowed.
822776	Query Distinguished Name does not display the LDAP users in FortiManager when Secure connection is enabled.
823898	FortiManager does not use all of the configured "ssl-cipher-suites" under its "system global" settings.
825078	New admins with ADOM only access cannot see the previously assigned header and footer policies on that ADOM.

Bug ID	Description
827854	Installation target disappears in workflow mode if session is approved via email.
829751	Installation tasks got stuck at 0% and failed to start any new installation tasks.
830242	FortiManager in Advanced Mode does not show the number of allowed VDOMs correctly.
839715	Any changes on the Admin Setting page alter the FortiManager's Themes.
841931	When FortiManager works in Workspace Mode, users are able to disable "Per-Device Mapping" without locking the ADOMs.

VPN Manager

Bug ID	Description
810027	FortiManager Spoke IP setting for vpn configuration sets properly but the policy package does not change on the Hub phase1.
831076	Static Route (Protected Subnet of the HUB) is not installed to Spoke during install, with HUB and Spoke Dial-up VPN setup.

Known Issues

The following issues have been identified in 7.0.5. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
817346	Editing interface with normalized interface mapping displays some unnecessary messages for mapping change.
845656	When BGP is enabled and no IP address is defined for <code>set-ip-nexthop</code> under the <code>route-map</code> config, FortiManager tries to set the IP to <code>0.0.0.0</code> , and this may break the BGP network.

Others

Bug ID	Description
729175	FortiManager should highlight device consisting of specific IP address under <i>Fabric View</i> .
777831	When FortAnalyzer is added as a managed device to FortiManager, "Incident & Event" Tile will be displayed instead of the "FortiSoC".
822263	Service Status under FortiGuard does not display the secondary Service status of the FortiGate's cluster correctly.

Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
698838	"Download Conflict File" does not display all of the firewall objects conflicts when importing policy packages from FortiGate to FortiManager.
751443	FortiManager displays policy installation copy failures error when ipsec template gets unassigned.
774058	Rule list order may not be saved under File Filter Profile.

Bug ID	Description
793240	<p>FortiManager fails to retrieve FortiGate's configuration when external-resource objects include a "g-" prefix.</p> <p>There are two workarounds; use the approach that works best for your environment. If it is possible, create a new backup of your FMG and FGT(s) before making any changes:</p> <p>First workaround approach:</p> <ol style="list-style-type: none"> 1. Re-create all threat feeds locally in VDOM configuration and update policies and security profiles that reference them to the local threat feed vs. the global feed. 2. Delete the global threat feed objects. <p>Second workaround approach:</p> <ol style="list-style-type: none"> 1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix. 2. FMG reports 'install OK/verify FAIL' at the end of the policy installation. 3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT. 4. Retrieve the FGT configuration from FMG. 5. Perform another policy installation to update the configuration synchronization status between the FGT and FMG. No commands are pushed during this stage according to the install wizard.
803460	"User Definitions" entries under the "User & Authentication" cannot be removed from FortiManager.
827602	[EMS Connector] Unable to import EMS Tags from EMS Server.
834806	Installation fails due to extra back slashes when installing the custom IPS signatures to the FortiGates.

VPN Manager

Bug ID	Description
784385	<p>If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager.</p> <p>Workaround:</p> <p>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:</p> <pre>diagnose cdb check policy-packages <adom></pre> <p>After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.</p>
798995	It's not possible to delete an SSL VPN portal profile from FortiManager GUI if the profile has been already installed.

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 and perpetual licenses are stackable.



www.fortinet.com

Copyright© 2024 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 General Counsel, 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.