

# Release Notes

## FortiManager 7.0.4



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



January 5th, 2024

FortiManager 7.0.4 Release Notes

02-704-806193-20240105

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 7.0.4 Release</b>	<b>7</b>
Supported models	7
FortiManager VM subscription license	7
Management extension applications	7
Supported models for MEA	8
Minimum system requirements	8
<b>Special Notices</b>	<b>10</b>
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
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	11
Fortinet verified publisher docker image	12
Scheduling firmware upgrades for managed devices	13
Modifying the interface status with the CLI	13
SD-WAN with upgrade to 7.0	13
Citrix XenServer default limits and upgrade	14
Multi-step firmware upgrades	14
Hyper-V FortiManager-VM running on an AMD CPU	14
SSLv3 on FortiManager-VM64-AWS	14
<b>Upgrade Information</b>	<b>16</b>
Downgrading to previous firmware versions	16
Firmware image checksums	17
FortiManager VM firmware	17
SNMP MIB files	18
<b>Product Integration and Support</b>	<b>19</b>
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 .....	33
FortiAnalyzer models .....	33
FortiAuthenticator models .....	34
FortiCache models .....	34
FortiDDoS models .....	34
FortiDeceptor models .....	34
FortiFirewall models .....	35
FortiFirewallCarrier models .....	35
FortiMail models .....	35
FortiProxy models .....	35
FortiSandbox models .....	36
FortiSOAR models .....	36
FortiSwitch ATCA models .....	36
FortiTester models .....	36
FortiWeb models .....	37
<b>Resolved Issues .....</b>	<b>38</b>
AP Manager .....	38
Device Manager .....	38
Global ADOM .....	39
Others .....	39
Policy and Objects .....	40
Revision History .....	42
Script .....	42
Services .....	42
System Settings .....	43
VPN Manager .....	43
<b>Known Issues .....</b>	<b>44</b>
Device Manager .....	44
Others .....	44
Policy & Objects .....	44
System Settings .....	45

---

<b>Appendix A - FortiGuard Distribution Servers (FDS)</b>	<b>46</b>
FortiGuard Center update support	46
<b>Appendix B - Default and maximum number of ADOMs supported</b>	<b>47</b>
Hardware models	47
Virtual Machines	47

# Change Log

Date	Change Description
2022-06-08	Initial release.
2022-06-09	Updated <a href="#">Resolved Issues on page 38</a> , <a href="#">FortiGate models on page 25</a> , and <a href="#">FortiGate special branch models on page 28</a> .
2022-06-17	Updated <a href="#">Special Notices on page 10</a> .
2022-07-07	Updated <a href="#">Upgrade Information on page 16</a> .
2022-07-19	Updated <a href="#">Upgrade Information on page 16</a> .
2022-07-25	Updated <a href="#">Known Issues on page 44</a> .
2022-08-05	Removed <i>SDN fabric connectors</i> special notice because 496870 is resolved.
2022-08-26	Updated <a href="#">Upgrade Information on page 16</a> .
2022-09-06	Added 830105 to <a href="#">Known Issues on page 44</a> .
2022-09-12	Updated <a href="#">FortiOS and FortiOS Carrier on page 20</a>
2022-10-06	Updated <a href="#">Known Issues on page 44</a> .
2022-10-11	Updated <a href="#">FortiOS and FortiOS Carrier on page 20</a> .
2022-10-12	Updated <a href="#">Known Issues on page 44</a> .
2022-10-27	Updated <a href="#">FortiProxy on page 22</a> .
2022-11-16	Updated <a href="#">FortiSandbox on page 22</a> .
2022-11-21	Updated <a href="#">Known Issues on page 44</a> .
2023-04-25	Updated <a href="#">Known Issues on page 44</a> .
2023-06-08	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 44</a> .
2023-06-23	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 44</a> .
2023-07-12	Updated <a href="#">Special Notices on page 10</a> and <a href="#">Known Issues on page 44</a> .
2024-01-05	Updated <a href="#">Special Notices on page 10</a> .

# FortiManager 7.0.4 Release

This document provides information about FortiManager version 7.0.4 build 0306.



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 7.0.4 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, 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 47](#).

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.0.4.



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:

<b>FortiManager</b>	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, and FMG-3900E.
<b>FortiManager VM</b>	FMG_DOCKER, FMG-VM64, 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*
<b>FortiAIOps</b>	<ul style="list-style-type: none"> <li>• 8 vCPU</li> <li>• 32 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	No change
<b>FortiPortal</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSigConverter</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> </ul>	No change
<b>FortiSOAR</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> </ul>	<ul style="list-style-type: none"> <li>• 16 vCPU</li> </ul>



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

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

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.0.4.

## 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 upgrading 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.

## 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

Starting in FortiManager 7.0.4, policy packages containing a large number of rules (for example, 80K) can be installed on managed FortiGate devices. Prior to 7.0.4, installing policy packages that contained a large number of rules would result in a copy failure.

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.

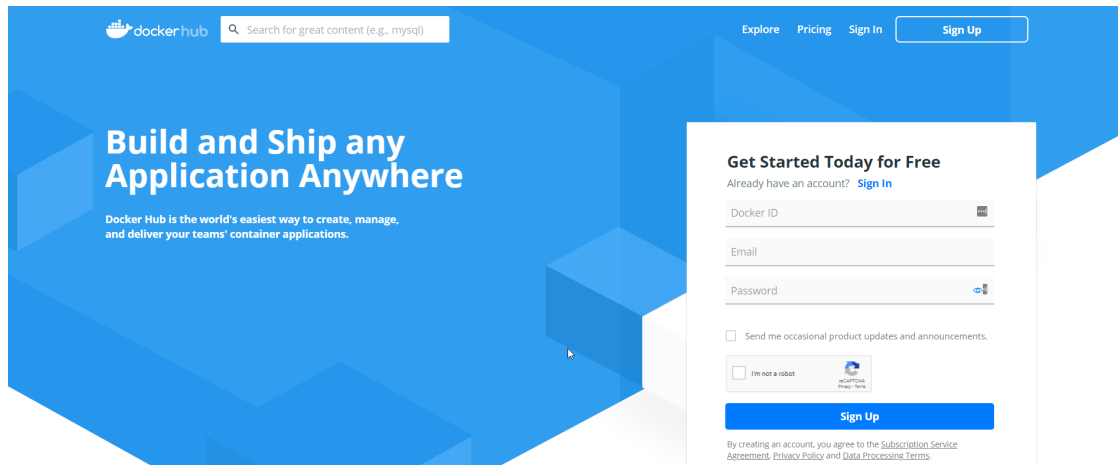
## Fortinet verified publisher docker image

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/>.

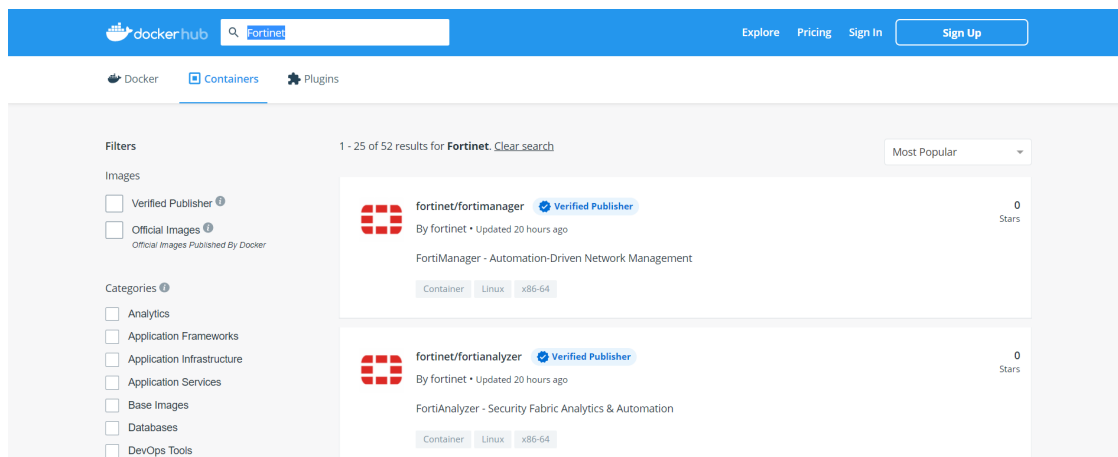
The dockerhub home page is displayed.



2. In the banner, click *Explore*.

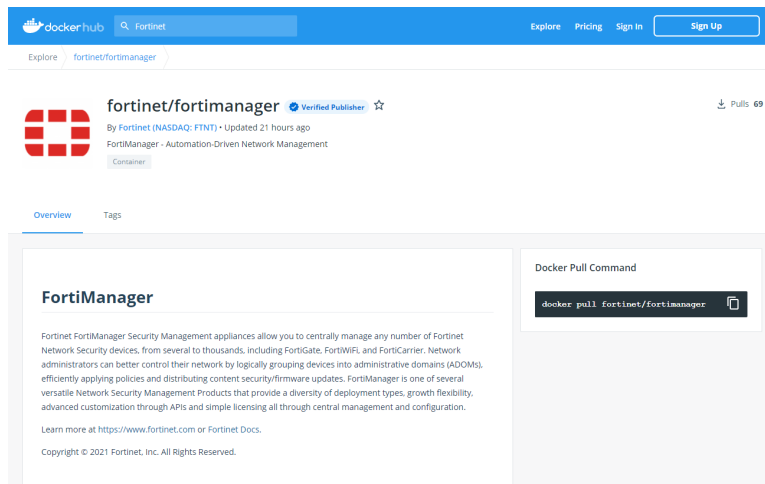
3. In the search box, type *Fortinet*, and press *Enter*.

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 7.0.4 Upgrade Guide](#).

You can upgrade to FortiManager 7.0.4 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 11](#).



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 7.0.4 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 7.0.4 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 7.0.4 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 7.0.4 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 7.0.4 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 7.0.4 supports the following versions of FortiOS and FortiOS Carrier:

- 7.0.0 to 7.0.7
- 6.4.0 to 6.4.10
- 6.2.0 to 6.2.11

## FortiADC

FortiManager 7.0.4 supports the following versions of FortiADC:

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

## FortiAnalyzer

FortiManager 7.0.4 supports the following versions of FortiAnalyzer:

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

## FortiAuthenticator

FortiManager 7.0.4 supports the following versions of FortiAuthenticator:

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

## FortiCache

FortiManager 7.0.4 supports the following versions of FortiCache:

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

## FortiClient

FortiManager 7.0.4 supports the following versions of FortiClient:

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

## FortiDDoS

FortiManager 7.0.4 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 7.0.4 supports the following versions of FortiDeceptor:

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

## FortiFirewall and FortiFirewallCarrier

FortiManager 7.0.4 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 7.0.4 supports the following versions of FortiMail:

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

## FortiProxy

FortiManager 7.0.4 supports configuration management for the following versions of FortiProxy:

- 7.0.2



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

---

FortiManager 7.0.4 supports logs from the following versions of FortiProxy:

- 7.0.0 to 7.0.5
- 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 7.0.4 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 7.0.4 supports the following versions of FortiSOAR:

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

## FortiSwitch ATCA

FortiManager 7.0.4 supports the following versions of FortiSwitch ATCA:

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

## FortiTester

FortiManager 7.0.4 supports the following versions of FortiTester:

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

## FortiWeb

FortiManager 7.0.4 supports the following versions of FortiWeb:

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

## Virtualization

FortiManager 7.0.4 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 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
<b>FortiGate</b>	✓	✓	✓	✓	✓
<b>FortiCarrier</b>	✓	✓	✓	✓	✓
<b>FortiADC</b>		✓	✓		
<b>FortiAnalyzer</b>			✓	✓	✓

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 7.0.4.



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 33](#)
- [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 35](#)
- [FortiProxy models on page 35](#)
- [FortiSandbox models on page 36](#)
- [FortiSOAR models on page 36](#)
- [FortiSwitch ATCA models on page 36](#)
- [FortiTester models on page 36](#)
- [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
<b>FortiGate:</b> 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
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
<b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, 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	
<b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
<b>FortiWiFi:</b> 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	
<b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-ARM64-KVM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM	
<b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-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
<b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	
<b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-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	
<b>FortiGate ACDC:</b> FortiGate-2201E-ACDC, FortiGate-3960E-ACDC	
<b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC	
<b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F,	
<b>FortiGate VM:</b> 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	
<b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

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

## FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.4 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 FortiGate-71F	7.0	Build 304 and special branch 4530.
FortiGate-3000F	7.0	Build 304 and special branch 4451.
FortiGate-3001F	7.0	Build 304 and special branch 4436.
FortiGate-3700F FortiGate-3701F	7.0	Build 304 and special branch 6066.

## FortiOS 6.4

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

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7060E	6.4.8	1823
FortiGate-7060E-8-DC		
FortiGate-7000F		
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	6.2.10	1211
FortiGate-7030E		
FortiGate-7040E		
FortiGate-7060E		
FortiGate-7060E-8-DC		
FortiGate-7000F	6.2.10	1211
FortiGate-7121F		
FortiGate-7121F-2		

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-7121F-2-DC		
FortiGate-7121F-DC		
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
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> 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 <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	7.0
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> 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 <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4

Model	Firmware Version
<b>FortiCarrier:</b> 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 <b>FortiCarrier-DC:</b> 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 <b>FortiCarrier 6K and 7K:</b> 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 <b>FortiCarrier 6K and 7K DC:</b> 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 <b>FortiCarrier-VM:</b> 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	6.2

## FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiCarrier. FortiManager version 7.0.4 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
<b>FortiADC:</b> FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F <b>FortiADC VM:</b> FortiADC-VM	6.2, 7.0
<b>FortiADC:</b> 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 <b>FortiADC VM:</b> FortiADC-VM	6.0, 6.1

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> 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
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-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
<b>FortiAnalyzer:</b> 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. <b>FortiAnalyzer VM:</b> 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
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	6.2, 6.3, 6.4

## FortiCache models

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

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-2000F	6.3
<b>FortiDDoS:</b> FortiDDoS-200F, FortiDDoS-1500F <b>FortiDDoS VM:</b> FortiDDoS-VM	6.1, 6.2, 6.3

## FortiDeceptor models

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

## FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.0.4 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewall:</b> FortiFirewall-3980E <b>FortiFirewall DC:</b> FortiFirewall-3980E-DC	6.2	1262
<b>FortiFirewall:</b> FortiFirewall-4200F	6.2.7	5141
<b>FortiFirewall:</b> FortiFirewall-4400F	6.2.7	5148

## FortiFirewallCarrier models

The following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.0.4 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
<b>FortiFirewallCarrier:</b> FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148

## FortiMail models

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

## FortiProxy models

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

## FortiSandbox models

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

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FortiSOAR-VM	6.0, 6.4, 7.0

## FortiSwitch ATCA models

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

## FortiTester models

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

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

## FortiWeb models

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

# Resolved Issues

The following issues have been fixed in 7.0.4. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
755815	"local-standalone" and "local-authentication" features are inconsistent with FortiOS/FortiGate.
810804	FortiManager does not support configuration for wireless-controller nac-profile.

## Device Manager

Bug ID	Description
676415	SAML account with remote certificate not getting imported to FortiManager-Cloud.
704106	Certificate enrollment fails using SCEP on Microsoft server with sub-ca certificate chains.
736990	System Template cannot be assigned to a device as a member of a device group when the required meta-fields are used.
739746	When VDOM is enabled, FortiManager shows multiple firmware templates on Device Manager with different status.
753548	Error message <i>peer must be set</i> can be seen when configuring the IPSec Tunnel Templates.
764491	Unable to configure more than one IP addresses for "vrdst" under the "interface vrrp" setting.
767185	Unable to create route map rule using 'match-interface' when using the BGP Templates under the Provisioning Templates.
770699	Speedtest and speedtest-bypass-routing under SD-WAN templates configuration cannot be set on FortiManager.
773147	Installation fails due to the unexpected system interface config changes for "pvc" related settings.
775552	The view device revision under <i>Revision History</i> does not display the full and complete device's configuration.
777925	Several unregistered FortiGates consume FortiManager's resources thus FortiManager becomes very slow and unresponsive.

Bug ID	Description
782752	FortiManager does not update its Fortigate's IP address in case the IP gets modified on the FortiGate.
791117	Unable to create simultaneous static routes with named address objects.
792553	Removing VLANs from zones and adding a new VLAN to the same zone deletes that Zone.
793021	Creating the interface type <i>Software Switch</i> throws an error when adding a VLAN interface as a member.
793495	It is not possible to select all objects filtered by the search under Device Manager.
793510	Special characters in Meta fields are displayed in HTML Numeric Code.
793941	Unable to install VPN psk with special characters through CLI template.
796842	Failed to reload the configuration due to the "datasrc invalid" error message.
796920	"OPEN" mode is missing from the System Template's WIFI SSID.
799259	Duplicate CSF groups for 7.0 FGTs (7.0.2+) due to syntax returning upstream-ip instead of upstream.
800773	FortiManager doesn't show the filter configuration for syslogd correctly.
803683	Installation failed due to the config wireless-controller SNMP settings.
804237	Unable to modify the firmware templates under the <i>Device &amp; Groups</i> .

## Global ADOM

Bug ID	Description
743734	Cannot remove objects from Global Database.
768527	After upgrading the global ADOM, installation failed due to the custom ssl-ssh-profile config.
794206	Policy installation fails due to Global Object adding prefix g- in threat feed.

## Others

Bug ID	Description
763635	Unable to upgrade an ADOM from 6.2 to 6.4.
766874	FortiManager holds the wrong value for AP limit of the FG-80F.
780548	"Push Update" does not work for pending device under the <i>FortiGuard &gt; License Status</i> .

Bug ID	Description
781530	FortiManager does not sent the proper response for SNMP request to the <i>fmDeviceEntSupportState</i> query.
784034	HA Configuration in Zero-touch provisioning (ZTP) does not synchronize to the secondary FortiGate.
785797	<i>diag cdb upgrade force-retry del-invalid-ref</i> never stops.
792296	ADOM upgrade fails due to the virtual wire pair policy.
794256	Unable to export update manager log files for the sftp fdssvr.
794304	"Interface Bandwidth" widget is displayed in ADOM 6.2 in 6.4 FortiManager's version.
794633	FortiManager configured in closed network was unable to fetch the FGD DBs which was previously manually saved on another closed network FortiManager.
795111	Unable to add/modify a FPX 'Explicit Proxy' policy from a FortiProxy ADOM in FortiManager.
796200	Extremely slow performance when fetching all the devices from DVM via JSON API.
796506	Upgrading HA cluster via FortiManager stays members into a restart loop.
797165	FortiManager has some unsupported commands for the fortitoken user definition.
804244	ADOMs created by XML API cannot be locked or unlocked.
805226	ADOM upgrade uses too much memory and this makes the upgrade process too slow.

## Policy and Objects

Bug ID	Description
701750	The App Control set to <i>Monitor</i> in FortiManager causes the app to disappear from FortiGate.
705302	Remote VPN certificate installation failed and cert disappeared from FortiManager however on the FortiGate the certificate installed successfully.
706809	Policy Check export does not have the last hit count details anymore.
714375	There is not any warning messages when assigning already in used normalized interface.
721253	FortiManager may not import all the roles and address groups from ClearPass.
724154	Installation fails when <i>Any</i> has been set as incoming interface and VIP is being used on the IPV4 firewall policy.
725132	When modifying the IP address of the default VPN interface of a spoke in Device Manager, hub remote gateway should be modified to reflect that change.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
737424	Policy package import fails due to the 'Device mapping::"query failed."' error.



Bug ID	Description
755891	Copy procedure fails without any proper and clear error messages.
758494	Searching members inside an address group does not work.
758680	Unable to complete the Cisco pxGrid fabric connector's configuration on FortiManager.
760918	Unable to change the action field for the default IPS profile and their clones.
767255	FortiManager fails to install the custom signature because it is too long.
773403	FortiManager may now differentiate between the ISDB objects "Predefined Internet Services" and "IP Reputation Database".
775128	Unable to create more than 20 SAML users in policy package object.
775806	In workspace mode, locking and unlocking ADOMs displays a blank page when classic dual pane is enabled.
777017	FortiManager purges the "arrp-profile" when installing the v6.2 policy packages to v6.4 FortiGates.
781118	6.4 version ADOM policy package failed to enable policy NAT from GUI.
791357	Installation failed when using custom-deep-inspection.
791797	Installation failed after upgrading ADOM from 6.2 to 6.4.
792980	Installation fails when trying to install SAML user configuration.
794731	The Policy package counter field does not display the number of modified policy packages.
796505	Modifying the "Sections" under the Policy&Objects leads to some unexpected changes/behavior.
796512	Wrong direction definition has been displayed for "Tor-Relay.Node" ISDB object.
797091	"Synchronize Firewall Addresses" under the FortiClient EMS Connector does not automatically create and synchronize addresses for all EMS tags.
798094	Re-assignment of tokens in FortiManager policy and objects, deletes and re-adds the firewall policies that are used those objects.
798958	Policy Consistency Check fails due to the firewall service's name.
799538	The export policy feature displays limited numbers of the group objects.
801876	Installation failed due to "Copy global shared objects" failure.
802072	<i>Auto-asic-offload</i> cannot be disabled for the first time in the policy.
802934	FortiManager's Policy Package diff displays policy objects change even though there is not any changes.
805211	Installation failed due to the wrong FortiSwitch VLAN type for the default NAC and nac_ segment VLANs.

Bug ID	Description
805783	After the 6.0 ADOM upgrade, installing the same v6.0 policy package got "unset webfilter-profile" in wanopt proxy policy.
805966	Verification fails due to the "resource-limits.proxy".
811450	Installation preparation step for installing the PP to the FortiGate takes very long time.

## Revision History

Bug ID	Description
496870	Fabric SDN Connector is installed on FortiGate even if it is not in use.
691240	FortiManager should not unset the value forward-error-correction with certain FortiGate platforms.

## Script

Bug ID	Description
766019	Failed to run the Post-Run CLI Template due to the "datasrc invalid" error.
793407	Installation fails if one of the BGP network prefix entry is a supernet.
800149	FortiManager reorders the <ID>s with ascending order for BGP and static settings.

## Services

Bug ID	Description
752849	FortiManager doesn't have the proper version string of FortiGate's IPGeo information.
796345	FortiManager does not recognize the entitlement file for some FortiGates.
798979	FortiManager cannot download the latest IPS DB.
808121	FortiManager ignores <i>add_no_service</i> setting for the <i>Unauthorized Devices</i> .

## System Settings

Bug ID	Description
728972	"fmDeviceEntSupportState" OID returns incorrect value for some devices.
732949	FortiManager displays wrong admin name under task monitor for firmware upgrade task.
752916	FortiManager should be able to set desired permissions for Extender Manager in administrator profile settings.
753690	SNMPv3 security option configuration has discrepancy between GUI and CLI.
784978	The <i>Mode</i> option is not always available for root ADOM in all GUI-based root ADOM properties editing methods.
787588	Webfiltering HTTPS 8888 is not working after FortiManager upgraded from 6.4.7 to 7.0.4.
795655	FortiManager loads the "Administrator" list under the System Setting very slowly.
799619	When Advanced ADOM Mode is enabled, FortiManager under the <i>Device Inventory</i> displays all devices from all VDOMs.
803200	FortiManager does not synchronize with NTP server.
807788	Not able to disable the trusted hosts from the GUI.
811633	Restricted Administrators using the API requests have full Read-Write access.

## VPN Manager

Bug ID	Description
615890	IPSec VPN Authusergrp option "Inherit from Policy" is missing when setting xauthtype as auto server.
774040	keyboard-layout configuration in VPN SSL web portal predefined RDP bookmark generates incorrect commands.
791421	Bookmark setting under the SSLVPN portal has some missing screen/color configuration.
794168	Installation becomes very slow when FortiManager acts as CA server.
796104	FortiManager deletes and re-creates VPN routes with different ID's on every install.

# Known Issues

The following issues have been identified in 7.0.4. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
771417	Cannot overriding system template settings.
764369	FortiManager tries to install Security Fabric trusted list to all downstream FGs when a new one is added.
830105	When two or more IPsec <code>phase1-interfaces</code> have same <code>remote-gw</code> IP address, FMG tries to install 1.0.0.0 as <code>remote-gw</code> .

## Others

Bug ID	Description
823294	SSH connection between FortiGate and FortiManager v7.0.4 fails due to <code>server_host_key_algorithms</code> mismatch.

## Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
724011	FortiManager needs to support multiple server certificate list in <code>ssl/ssh</code> profile.
751168	Installation to FortiGate may fail when installing some specific applications.
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"><li>1. Re-create all threat feeds locally in VDOM configuration and update policies and security</li></ol>

Bug ID	Description
	<p>profiles that reference them to the local threat feed vs. the global feed.</p> <ol style="list-style-type: none"><li>2. Delete the global threat feed objects.</li></ol> <p>Second workaround approach:</p> <ol style="list-style-type: none"><li>1. Perform policy reinstallation. FMG adds original threat feed objects within the VDOM configuration without the 'g' prefix.</li><li>2. FMG reports 'install OK/verify FAIL' at the end of the policy installation.</li><li>3. Run scripts to delete the global threat feed objects (objects with the 'g' prefix) from the FGT.</li><li>4. Retrieve the FGT configuration from FMG.</li><li>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.</li></ol>
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.
838648	"Rename objects to import" inconsistency with "datasrc duplicate" error.

## System Settings

Bug ID	Description
780245	Install Wizard shows all devices are selected even-though "Default Device Selection for Install" is set to "Deselect All".

## 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	✓	✓
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
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. Licenses are non-stackable. 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](#).



[www.fortinet.com](http://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.