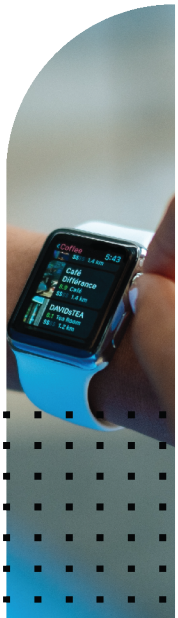
Release Notes

FortiManager 7.0.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 5, 2024
FortiManager 7.0.1 Release Notes
02-701-729157-20240105

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-15	Initial release.
2021-07-20	Updated Special Notices on page 9.
2021-07-21	Updated FortiClient on page 18.
2021-07-28	Added *Configuring Static Route with SD-WAN* to Special Notices on page 9. Updated description of 732144 in Known Issues on page 40. Removed 681006 and 711964 from Known Issues on page 40.
2021-07-29	Added *Scheduling firmware upgrades for managed devices* to Special Notices on page 9. Added 713714 to Known Issues on page 40.
2021-08-04	Updated Special Notices on page 9.
2021-08-30	Updated FortiAuthenticator models on page 27.
2021-09-01	Added FortiTester models on page 29.
2021-09-10	Added 744766 to Known Issues on page 40.
2021-09-15	Added *Fortinet verified publisher docker image* to Special Notices on page 9.
2021-09-29	Updated format of FortiGate special branch models on page 24.
2021-10-18	Updated 704637 in Resolved Issues on page 32.
2021-11-26	Added Microsoft Hyper-V Server 2019 to Virtualization on page 19, and removed 695782 from Resolved Issues on page 32.
2024-01-05	Updated Special Notices on page 9.

FortiManager 7.0.1 Release

This document provides information about FortiManager version 7.0.1 build 0113.

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

FortiManager version 7.0.1 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), 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 13.

See also Appendix B - Default and maximum number of ADOMs supported on page 46.

You can use the FortiManager VM subscription license with new FMG-VM installations.

For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.0.1.

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, and FMG-3900E.
FortiManager VM	FMG_DOCKER, FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), 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	• 8 vCPU • 32 GB RAM • 500 GB disk storage	No change
FortiAuthenticator	• 4 vCPU	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
	• 8 GB RAM	
FortiPortal	• 4 vCPU • 8 GB RAM	No change
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage
SD-WAN Orchestrator	• 4 vCPU • 8 GB RAM	• 4 vCPU • 12 GB RAM
Universal Connector	• 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage	No change
Wireless Manager (FortiWLM)	• 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 7.0.1.

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
```

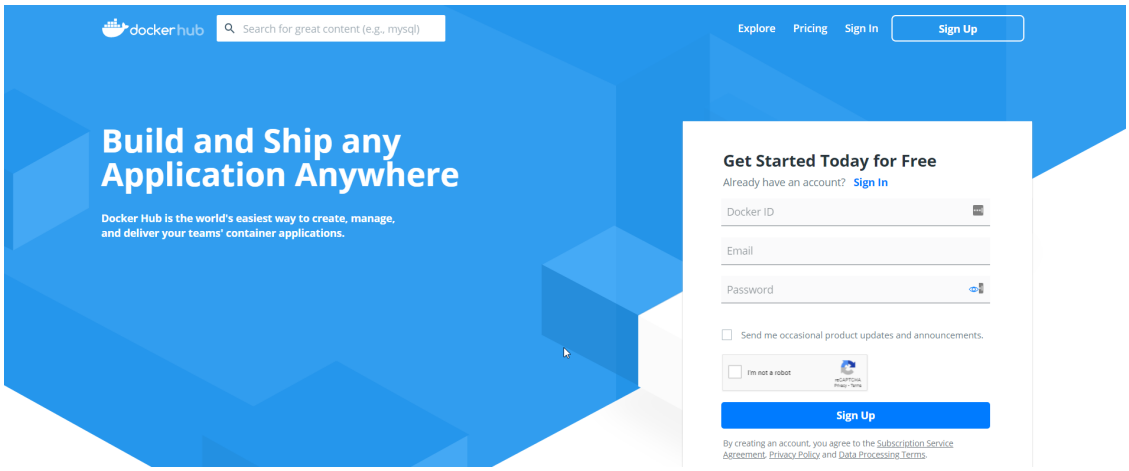
Fortinet has not uploaded FortiManager 7.2.3 and later firmware to FortiGuard in order to work around the GUI bug, however, the firmware is available for download from the Fortinet Support web site https://support.fortinet.com.

Fortinet verified publisher docker image

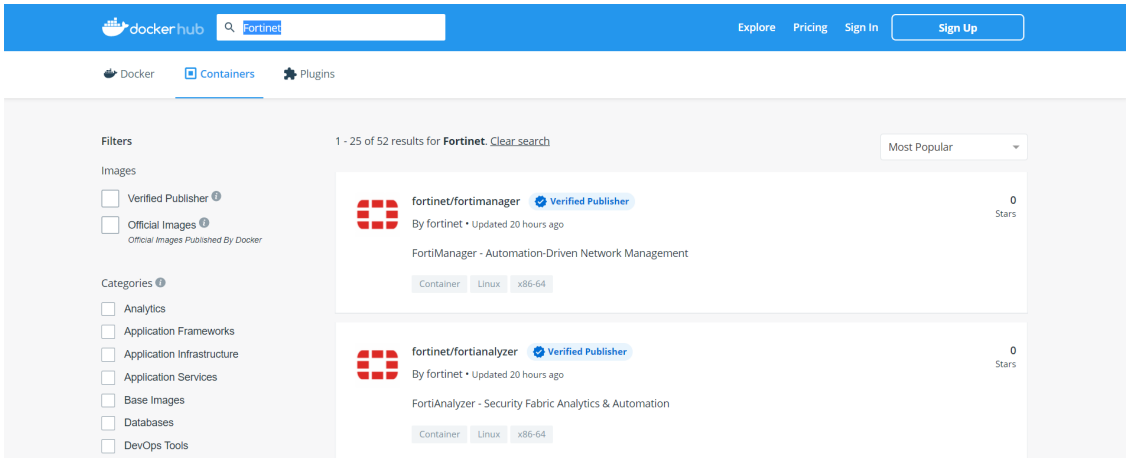
FortiManager 7.0.1 docker image is available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

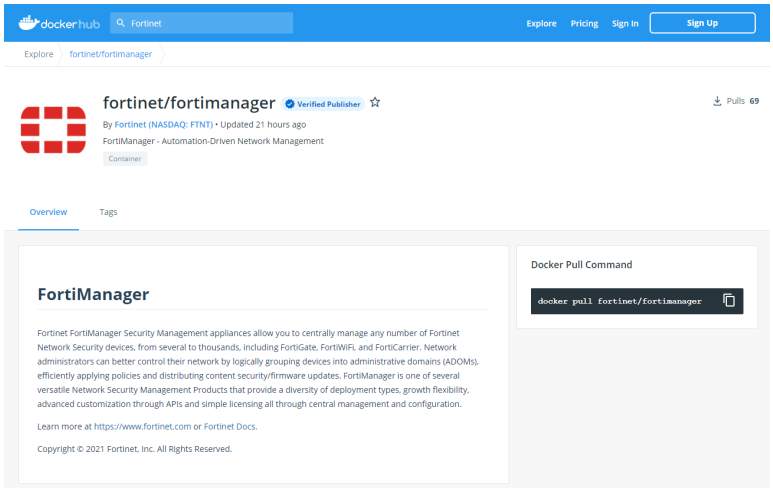
1. Go to dockerhub at https://hub.docker.com/.
   The dockerhub home page is displayed.



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.

Configuring static route with SD-WAN

Due to known CLI changes on FortiOS 7.0.1 or later, FortiManager cannot configure static route with SD-WAN by using the GUI or script. Please configure static route with SD-WAN on FortiGate, and then retrieve the configuration to FortiManager.

Modifying the interface status with the CLI

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

For example:

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

SD-WAN with upgrade to 7.0

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

Citrix XenServer default limits and upgrade

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

To increase the size of the ramdisk setting:

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

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

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

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

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

Hyper-V FortiManager-VM running on an AMD CPU

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

SSLv3 on FortiManager-VM64-AWS

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

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

Upgrade Information

You can upgrade FortiManager 6.4.0 or later directly to 7.0.1.

For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading 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 select *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 `FMG_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, `FMG_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 7.0.1 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:

FortiManager 7.0.1 support

This section identifies FortiManager 7.0.1 product integration and support information:

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

This section lists FortiManager 7.0.1 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 89
- Google Chrome version 91

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

FortiOS/FortiOS Carrier

This section lists FortiManager 7.0.1 product integration and support for FortiOS/FortiOS Carrier:

- 7.0.0 to 7.0.1
- 6.4.0 to 6.4.6
- 6.2.0 to 6.2.9

FortiADC

This section lists FortiManager 7.0.1 product integration and support for FortiADC:

- 6.0.1
- 5.4.5

FortiAnalyzer

This section lists FortiManager 7.0.1 product integration and support for FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiManager 7.0.1 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiManager 7.0.1 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiManager 7.0.1 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later

FortiDDoS

This section lists FortiManager 7.0.1 product integration and support for FortiDDoS:

- 5.4.2
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see Feature support on page 20.

FortiMail

This section lists FortiManager 7.0.1 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

FortiSandbox

This section lists FortiManager 7.0.1 product integration and support for FortiSandbox:

- 4.0.0
- 3.2.3
- 3.1.4

- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiManager 7.0.1 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

FortiSwitch ATCA

This section lists FortiManager 7.0.1 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

FortiTester

This section lists FortiManager 7.0.1 product integration and support for FortiTester:

- 3.9
- 3.8
- 3.7

FortiWeb

This section lists FortiManager 7.0.1 product integration and support for FortiWeb:

- 6.3.13
- 6.2.4
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.3
- 5.6.2
- 5.5.7
- 5.4.1

Virtualization

This section lists FortiManager 7.0.1 product integration and support for virtualization:

- 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	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
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 *FortiAnalyzer 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 7.0.1.

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

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-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, 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-2000E, FortiGate-2200E, FortiGate2201E, 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, FortiGate3960E, FortiGate-3980E **FortiGate 5000 Series**: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC**: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-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 **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-GCP, FortiGate-VM64-HV,FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS**: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged**: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0
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-81E, FortiGate-81E-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-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, 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-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E	6.4

Model	Firmware Version
FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:**FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-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 Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, 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-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGateRugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, 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-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D,FortiGate-2200E, FortiGate-2201E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate 7000 Series:** FortiGate-7000F **FortiGate DC:** FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, RortiGate-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-3600C-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-600C-LENC, FortiGate-1000C-LENC **FortiWiFi:** FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM, FortiWiFi-60F, FortiWiFi-61F	6.2

Model	Firmware Version
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-Xen, FortiGate-VMX-Service-Manager **FortiGate Rugged:** FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G **FortiOS:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.0.1 supports these models on the identified FortiOS version and build number.

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-200F	6.4.6	5785
FortiGate-6000F	6.4.2	1749
FortiGate-7000E	6.4.2	1749

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-POE, FortiGate-81F-POE	6.2.6	7097
FortiGate-1800F, FortiGate-1800F-DC FortiGate-1801F, FortiGate-1801F-DC	6.2.7	7104
FortiGate-2600F, FortiGate-2600F-DC FortiGate-2601F, FortiGate-2601F-DC	6.2.7	7104
FortiGate-4200F, FortiGate-4200F-DC FortiGate-4201F, FortiGate-4201F-DC	6.2.7	7104
FortiGate-4400F, FortiGate-4400F-DC	6.2.7	7105
FortiGate-4401F, FortiGate-4401F-DC	6.2.7	7104
FortiWiFi-80F-2R FortiWiFi-81F-2R	6.2.6	6997

FortiGate Model	FortiOS Version	FortiOS Build
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-POE	6.2.6	7032
FortiGate-6000F	6.2.6	1158
FortiGate-7000E	6.2.6	1158

FortiCarrier models

Model	Firmware Version
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, FotiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, 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-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	7.0
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzerVM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0.0
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand,FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.0 to 6.2
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	5.0 to 5.5
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	4.3

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-VM64, FCH-KVM	4.0, 4.1, 4.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3

Model	Firmware Version
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.3, 4.4, 4.5, 4.7

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E **FortiMail Low Encryption:** FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

FortiSandbox models

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

Model	Firmware Version
FortiSandbox-VM: FSA-AWS, FSA-VM	
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FSR-VM	6.4
FortiSOAR VM: FSR-VM	6.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.9
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.8
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL	3.7

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D **FortiWeb VM:** FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1

Resolved Issues

The following issues have been fixed in 7.0.1. For inquires about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
513324	Users should be able to delete multiple APs in AP Manager.
674636	SSID may be empty in the *AP Manager> WiFi Profiles> SSID* column.
677419	FortiManager may show installation error on dual-5G radio band while pushing wireless-controller configuration.
689325	FortiManager may not be able to configure Channel 13 for Germany AP profile.
698004	When installing to a 6.4 FortiGate device from a 6.2 ADOM, there may be issue with `set vap-all manual` within the AP Profile.
706233	FortiManager may not detect changes in `AP Manager > SSID > Pre-shared Key Password` and display the message *No record found*.
712669	FortiManager may set `darrp` as `enable` when the Radio mode is set to monitor causing the installation to fail.
716135	There may be verification error when trying to install FortiAP with 2.4GHZ *Radio 1* channel disabled.

Device Manager

Bug ID	Description
521976	Users may not be able to enable *CSV format* within a system template.
603820	FortiManager fails to import a policy when `reputation-minimum` and *reputation-direction* are set.
615044	Configuration status may be shown modified after adding FortiGate to FortiManager.
640907	FortiManager is unable to configure FortiSwitch port mirroring.
649260	*Device Manager* may return an error when deleting *VPN phase1*.
664120	When FortiGate HA secondary unit is down, action is displayed as *promote* in *Device*

Bug ID	Description
	Manager.
672344	If a managed FortiAnalyzer is in HA, setting *Send Logs to "Managed FortiAnalyzer"* in the system template may cause an install error.
690493	License check setting may not be saved.
692200	FortiManager may return conflict after a zero-touch-provisioning cluster deployment.
694713	When *Workspace* mode is enabled, the SD-WAN template may sporadically disappear.
696576	The available Explicit FTP proxy certificates are not consistent with the ones available in the FortiGate.
697596	*Advanced Options* is not displayed when creating a new interface.
701348	Once VRPP instance is created, the user should be able to edit or delete it.
702906	*DHCP Relay Service* may not be deleted when it is configured on VLAN interface.
708937	FortiManager may randomly update the geographical coordinates of a FortiGate device.
709214	System template should allow source interface to be selected when *Specify* is activated as `interface-select-method`.
709302	SD-WAN monitor search function on the table view does not actually search but highlight.
711005	Under backup ADOM, FortiManager should hide the selection for *Provisioning Templates* and *Policy Packages* in add device wizard, device dashboard, and device edit page.
711713	DHCP relay is displayed as DHCP server when *Workspace* is unlocked.
711888	FortiManager is not retrieving and saving the `vdom-exception` configuration.
713267	Searching for FortiGate name when editing a device group should display FortiGate device name with all the VDOMs.
714036	SD-WAN widget cannot be loaded when a rule uses a specific SLA target.
714208	*Device Manager* may not be able to save `scan-botnet-connections` option in interface settings page.
714710	Secondary interface configuration may not show on *Device Manager*.
719028	FortiManager may not update FortiGate's VDOM license information when it is changed.
719568	There should be *Has Log Disk* in editing device page.
726990	When an administrator has access to a specified device group, FortiManager may remove devices that do not belong to the group when synchronizing device list to FortiAnalyzer.

FortiSwitch Manager

Bug ID	Description
700023	Install may fail with switch-controller `managed-switch:poe-pre-standard-detection` after upgrade.
713492	In the per-device mapping of the VLANs in FortiSwitch Manager, the *Specify* option for the gateway is not saved in the database.
713553	FortiSwitch Template sflow counter interval value variance between 6.0 and 6.2 ADOMs.

Global ADOM

Bug ID	Description
680798	FortiManager may return an error, *Could not read zone validation results*, when assigning global ADOM changes with *Automatically Install Policies to ADOM Devices*.
693510	*Display Options* for *Object Config* will reset to default after some time.
710963	FortiManager may show unclear error message when trying to promote an object from an ADOM to Global database in Workspace or Workflow mode.
722562	Users may not be able to filter when assigning global policy.
724229	Global ADOM display options may be reset to default after reboot.

Others

Bug ID	Description
669191	The `fdssvd` daemon may randomly crash.
704545	FortiManager may stop responding when there is a lot of *Workflow* sessions and users try to disable the *Workflow* mode with the GUI.
706516	`Securityconsole` may crash when there are quotes around group name.
715601	Under some conditions, disk usage may reach 100% after a few days.
728375	JSON API may return `runtime error 0: invalid value` error when getting dynamic mapping with the *fields* attribute.
724470	The `dmworker` may crash on device retrieve or revision import.

Policy and Objects

Bug ID	Description
487186	FortiManager may install a different local category ID to FortiGate causing a conflict with custom URL rating list.
569446	Interface subnet address object may show *any* as interface instead of the selected interface.
580880	FortiManager is unable to see dynamic mapping for *Local Certificate* if a *Workflow* session is created.
636537	*CLI Only Objects* > *user* > *peergrp* is not able to delete *peergrp*.
642708	*View Mode* may unexpectedly change from *Interface Pair View* to *By Sequence* mode.
654172	There may be webfilter local category ID mismatch between FortiManager and FortiGate causing incorrect action when using *Custom URL List*.
659543	FortiManager is not allowing reorder between *Policy Blocks*.
663109	FortiManager should not allow the user to select a profile group in a flow-based policy that uses a proxy-based feature.
666091	After cloning a policy package, the cloned policy package loses the installation targets.
672035	There may be an error when importing AWS credential from FortiGate to FortiManager.
675501	Policy check may show negative values.
679282	Editing a global object in an ADOM is not possible generating error, *Undefined is not iterable*.
684728	FortiManager and FortiGate should have equivalent filter list entries.
696367	*Hit count*, *First used*, and *Last used* may not get updated on FortiManager.
696489	The *URL Filter* in a *Web Filter* profile may not be enabled properly.
701526	There may be issue when scrolling down to view policy consistency results.
702621	When adding a remote usergroup when the LDAP service is unreachable, the *Manually specify* option is only available after a timeout.
704148	FortiManager is missing some IPS signatures while they are available on FortiGate.
704637	FortiManager allows VIP to be configured without default value or dynamic mapping.
705025	*Find Unused Policies* may report incorrect session data for security policy.
707953	IPS sensor may incorrectly set the action to *pass* instead *block* when quarantine is set.
708877	FortiManager 6.0 ADOM should not allow users to set ISDB objects that are not supported on FortiOS 6.0.
709435	FortiManager may not be able to import existing *Azure SDN Connector* from FortiGate.
711121	Enabling *FortiGuard Outbreak Prevention* database does not match FortiGate's behavior.
712150	The Search function in *Address* may not work after upgrading FortiManager to 6.4.5.

Bug ID	Description
712213	Users may not be able to filter a policy using the *Inspection Mode* field.
712900	When new folders are created and the default policy package is deleted, then the new policy package cannot be created.
713216	When the policy package is large, it is slow to load the policy package, install the policy package, or view sessions revision diff in Workflow mode.
713682	FortiManager changes the *Web URL Filter* name on its own when saving a *Web Filter Profile*.
715275	FortiManager may not be able to show specific signature.
715722	Users may not be able to delete global object.
719700	FortiManager may have incorrect IPS default action entries in the database.
719981	The *Where Used* function may return no result for *Internet Service* objects.
725274	GUI may be slow when filtering many entries with DNS filter.
726424	IPS signature list may be empty after upgrade.
727329	FortiManager may fail to identify case sensitivity with interface having similar name for the *Normalized Interfac*" settings.
729287	User may not be able to edit DNAT.

Revision History

Bug ID	Description
638060	Installing an existing revision or renaming a revision should be allowed in backup ADOM.
685509	FortiManager may unset `authmethod-remote` causing the install to fail.
691240	FortiManager should not unset the value `forward-error-correction` with certain FortiGate platforms.
693225	FortiManager may install `unset inspection-mode` to FortiGate 6.2 device in 6.0 ADOM.
694380	Installation may fail when `set whitelist enable` in ssl-ssh-profile is pushed to FortiGate 6.2 from a in 6.0 ADOM.
697642	Connecting unauthorized FortiSwitch to a managed FortiGate may cause issues on FortiManager when `auto-update` is disabled.
708913	FortiManager may try to set `sflow-counter-interval` and unset `trunk-member` resulting in installation failure.
715313	FortiManager may not enable the option `FortiGuard Category Based Filter` after FortiManager is synchronized with FortiGate.
724976	In a Zero Touch Provisioning deployment, the device database may get wiped by an *AutoRetreive* task.

Bug ID	Description
728422	Policy validation may fail due to dynamic mapping for global object that is for FortiGate 6.2 device but it is in 6.0 ADOM.
728447	Installation may fail due to VIP's mapped IP as a range with two identical IP addresses.

Script

Bug ID	Description
645684	Users may not be able to run TCL script in *Workflow* mode.
668876	Using CLI script to create SD-WAN with auto-numbering, `edit 0`, may not work.
689775	Users may not be able to edit an empty *CLI Script Group*.
701777	*Application ID* is not being configured after policy script execution.
707952	Copying a *CLI Script Group* from one ADOM to another ADOM may not work.
715305	When changing the system setting `opmode` from `nat` to `transparent` via a script, FortiManager may return failure to commit to database stating that there is no interface.
715623	Running a script on the device database may not update the *Save* status.
715632	Script configuring AntiVirus quarantine may fail.
721740	FortiManager may fail to run CLI script on Device DB after `dmworker` rash.

Services

Bug ID	Description
567664	HA secondary unit does not update FortiMeter license.
673302	FDS updates may fail with TLS v1.3.
688498	FortiSwitch version shown in the FortiGuard package page is not seen on FortiGate.
695685	FortiGate HA firmware upgrade may fail when both HA units need disk check.
712062	FortiSwitch and FortiAP upgrades may fail with *Response with errors* by using FortiGuard image.
714596	For web filter query, FortiManager should support *category 9* mapping data.
714787	FortiManager should have a `diagnose` command to force web filtering database merge.

System Settings

Bug ID	Description
598194	FortiManager two-factor authentication admin login is missing the option for *FTK Mobile* push notification authentication.
625683	Changes made by ADOM upgrade may not update *Last Modified* date/time and user admin.
637377	If *Manage Device Configurations* is set to none in the admin profile, the user may not be able to see interface in policy.
667284	FortiManager should have a better log message when aborting device upgrade.
687171	Users may not be able to assign devices to the ADOMs which they have full access to.
687968	FortiManager should not change to `ipv6-autoconf` to `disable`when management access is changed to the `ipv6-autoconf` enable state.
697082	Schedule SCP backup may fail due to incorrect default port number.
700142	FortiManager should allow the user to configure more than eight hosts per SNMP community.
702165	Wildcard search may not work for *Event* logs.
705185	ADOM upgrade may cause per device mapping of VLANs in FortiSwitch Manager change to *0*.
708939	*Dashboard* is showing incorrect GB per day and Device Quota information when FortiManager is enabled.
709873	Global task assignment time may not be accurate.
711446	Copy may fail due to invalid protocol options when both FortiGate and ADOM are upgraded to v6.2.
713233	FortiManager may fail to upgrade firmware resulting in `cdbupgrade` task error on console and process crashes.
714210	LDAP admin group search should be done with the service or administrator bind account.
714635	FortiManager backup file size may increase gradually when the IPS package is updated.
723117	Admin user may not be able to see who has locked an ADOM.
726138	After upgrade, *FortiSwitch Template* setting `poe-pre-standard-detection` may cause the installation to fail.
727458	FortiManager may not allow users to access all the VDOMs within an ADOM.

VPN Manager

Bug ID	Description
695879	Edit community may not be able to set *VPN zone* to *Off* via the GUI.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
716350	FortiManager 7.0.1 is no longer vulnerable to the following CVE-Reference: • CVE-2021-32589

Known Issues

The following issues have been identified in 7.0.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
673020	Creating SSID interface with central AP Manager automatically generates normalized interface name that has no default mapping configuration.

Device Manager

Bug ID	Description
545239	After adding FortiAnalyzer fabric ADOM to FortiManager, Device Manager's *Log Status*, *Log Rate*, or *Device Storage* column cannot get data from FortiAnalyzer.
554241	FortiManager cannot delete and reassign ports to VDOM when split VDOM is enabled.
563690	Device Manager fails to add a FortiAnalyzer which contains a FortiGate HA device with the error: *serial number does not match database*.
596711	FortiManager CLI Configuration shows incorrect default wildcard value for `router access-list`.
610568	FortiManager may not follow the order in CLI Script template.
636638	*Fabric View* may stall at loading.
651560	SD-WAN monitor may get stuck loading when the admin user belongs to device group.
660491	Device Manager system interface should not allow a duplicate secondary IP address.
665207	FortiManager needs IPv6 support on *Syslog server* setting.
670577	When creating an API admin from a CLI Configuration, the *Trusted Host* section is missing.
673548	FortiManager may not be able to make any change to the FortiGate interface settings when the interface type is *Software Switch*.
674904	FortiManager may not be able to import policy with interface binding contradiction on `srcintf` error.
689721	When changing FortiGuard related settings via CLI Configuration, FortiManager shows

Bug ID	Description
	changes are reverted back, and it also shows the message: *Successfully updated*.
696730	FortiManager is unable to promote Secondary FortiGate as Primary in a HA Cluster.
710570	The *Any* statement is not accepted by FortiManager in the `perfix-list` configuration.
713714	Legacy device and group schedule firmware upgrade will be ignored. FortiGates are upgraded immediately.
728687	Policy package status may change to *Modified* on all FortiGate devices when a dynamic address group changes.
729301	A managed FortiGate with assigned CLI template remains in *Modified* state following a successful device configure installation.
729606	FortiManager should show where a *Device Zone* is used under *Device Manager*.

FortiSwitch Manager

Bug ID	Description
674539	FortiManager may fail to upgrade two FortiSwitch devices at the same time.

Global ADOM

Bug ID	Description
667197	User should not be able to delete a Global object when the ADOM is not locked.

Others

Bug ID	Description
510508	FortiManager cannot assign multiple ADOMs to an admin user via JSON API.
657997	Assigning a device to a system template may not work via JSON when FortiManager is in *Workspace* mode.
677304	the `diagnose` command cannot filer download objects by `objid`.
697361	FortiExtender status may not display correctly.

Bug ID	Description
732144	A CA certificate may be missing from some older FortiManager platforms causing failure to login with FortiCloud SSO.
744766	Unable to retrieve Group/IP address for NSX-T v3.1.2.

Policy & Objects

Bug ID	Description
538057	The *OR*" button in column filter may not work.
584288	FortiManager may not be able to load configuration of virtual server on the policy page.
585177	FortiManager is unable to create VIPv6 virtual server objects.
644822	Imported *SDN Connector Objects* may change to random names.
646329	*Policy Check* may claim that different IPS profiles are duplicate.
652753	Wen an obsolete internet service is selected, FortiManager may show entries IDs instead of names.
655601	FortiManager may be slow to add or remove a URL entry on Web Filter with a large list.
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
659296	FortiManager may take a lot of time to update Web Filter URL filter list.
666258	A user should not be able to create a firewall policy with an *Internet Service* with *Destination* direction in *Source* using drag and drop.
670061	FortiManager does not report error when an unsupported FQDN address format is created.
682356	FortiManager may not be able to map normalized interface.
688586	Exporting Policy Package to *CSV* shows `certificate-inspection` in the `ssl-ssh-profile` column even when the profile is not in use.
713692	*Web Filter Profile* install may fail when using pre-defined URL filter.
716114	FortiManager should push changes in `ssl-ssh-profile` with *Untrusted SSL Certificates* setting reverted from *Block* to *Allow*.
719774	IP reputation for the policies are not working without *Source* or *Destination*.
725024	*Proxy Policy* page shows empty when the *View Mode* is selected as *Interface Pair View*.
725427	Policy package install skips the policy where destination interface is set as *SD-WAN zone* and policy is *IPSEC* policy.
731053	FortiManager may miss some *Internet Service* entries.

Revision History

Bug ID	Description
618305	FortiManager changes configuration system `csf` settings.
635957	Install fails for subnet overlap IP between two interfaces.
672609	After import, FortiManager may prompt a password error to administrator during install.
674094	FortiManager may unset explicit proxy's *HTTPS* and *PAC* ports and change the value to *0* instead.
724447	When managing a dual chassis SLBC cluster, install may fail when private data encryption is enabled and cluster was previously failed-over.
728117	After upgrade, install may fail due to *set pri-type-max 1000000*.
729587	FortiManager may create an already deleted admin account on FortiGate when installing changes for a new VDOM.

Script

Bug ID	Description
630016	A FortiGate user can see scripts from all ADOMs.
679313	Meta variables used in CLI template should work with both *Device* and *Device VDOM* types.
729571	TCL script commands run on device no longer show in the script log.

Services

Bug ID	Description
725118	FortiManager may not logging FortiGuard connectivity failures.

System Settings

Bug ID	Description
616703	GUI CLI Console may not respond.
617601	Sort by *Time Used* in task monitor may not be correct.

Bug ID	Description
652417	FortiManager HA may go out of synchronization periodically based on the logs.
690926	FortiManager is removing SD-WAN field description upon ADOM upgrading from 6.2 to 6.4.
723447	After ADOM upgrade, install may fail due to wildcard FQDN type firewall address for Microsoft update.
726007	Admin User systematically gets access to *Root* ADOM in case of RADIUS authentication and "Fortinet-Vdom-Name" VSA not set.
729280	Admin User with no access to management ADOM or VDOM can create a new VDOM from non-management ADOM > VDOM.

VPN Manager

Bug ID	Description
615890	IPSec VPN `Authusergrp` option *Inherit from Policy* is missing when setting *xauthtype* as auto server.
699759	When installing a policy package, per device mapped objects used in SSL VPN cannot be installed.
712633	VPN Manager pushes default `dpd-retrycount` and `dpd-retryinterval`, but it cannot display them.
721783	Applying Authentication or Portal Mapping changes may take several minutes.
722924	FortiManager may not be able to edit `skip-check-for-unsupported-os enable` under SSL portal profile.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- 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 via 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/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
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

The following table identifies the default number of ADOMs supported for FortiManager hardware models G series and later. It also identifies the hardware models that support the ADOM subscription license and the maximum number of ADOMs supported.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
3000G Series	500	✓	1200

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

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. 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.