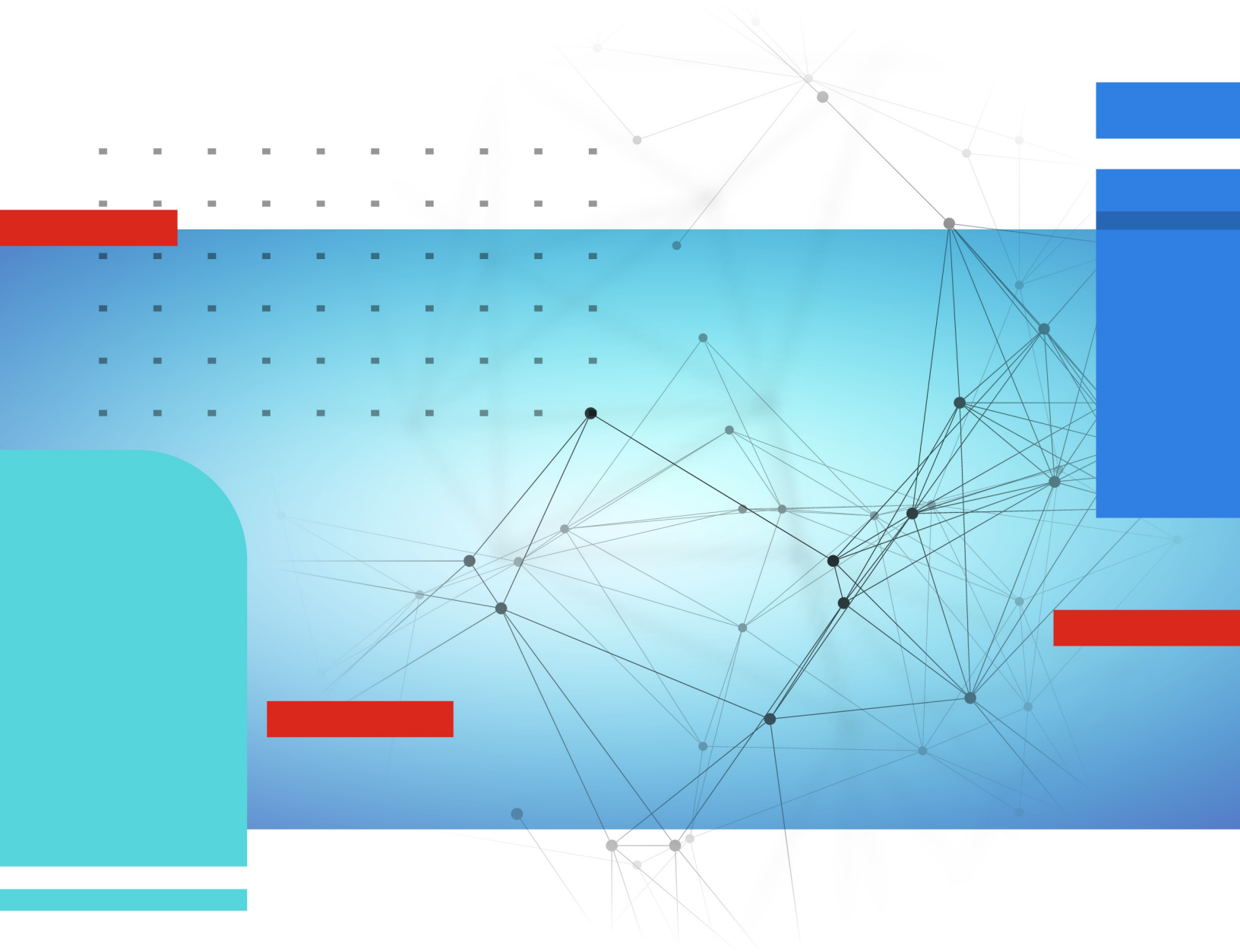
Release Notes

FortiManager 7.6.7



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

June 2, 2026
FortiManager 7.6.7 Release Notes
02-767-1296362-20260602

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-06-02	Initial release of 7.6.7.

FortiManager 7.6.7 Release

This document provides information about FortiManager version 7.6.7 build 3737.

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 7.6.7 supports the following models:

FortiManager	FMG-200G, FMG-400G, FMG-410G, FMG-1000F, FMG-1000G, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3100G, FMG-3700F, and FMG-3700G, FMG-3750G.
FortiManager VM	FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022), FMG_VM64_IBM, FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

For access to container versions of FortiManager, contact Fortinet Support.

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 24.

See also Appendix B - Default and maximum number of ADOMs supported on page 67.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.6.7.

FortiSwitch-VLAN with per-device mapping enabled

For customers upgrading from a version prior to FortiManager 7.4.9 or 7.6.5 with a FortiSwitch-VLAN with per-device mapping enabled, FortiManager may unset the interface configuration. Specifically, it may "unset allowaccess" on each VLAN interface.

To correct this issue, run the following command after upgrading FortiManager:

```
diagnose cdb manual-fix adom <adom name> fspvlan-dyn-ipv4allowaccess
```

The dynamic mappings will inherit allowaccess settings from the parent entry.

FortiCare Elite or FortiCare Premium required to download FortiGuard objects

Starting in 7.2.12, 7.4.9, and 7.6.5, FortiManager requires a valid FortiCare Elite or FortiCare Premium support contract registered in FortiCloud in order to get object updates from FortiGuard.

FortiManager instances deployed on the Azure platform

FortiManager instances deployed on the Azure platform (regardless of version) may lose all data—including configuration, logs, and reports—if the VM is deallocated and subsequently reallocated.

This issue can occur when the VM is deallocated through Azure-level operations (e.g., Azure portal, CLI, or automation). For example, this may happen when an Azure administrator changes the VM SKU (e.g., from Standard_D16_v3 to Standard_D32a_v4), or when the VM is manually stopped (deallocated) from the Azure portal.

To minimize the risk of data loss, it is strongly recommended to:

- Perform regular backups of configuration and data via the GUI or native CLI commands on FortiManager.
- Shut down the FortiManager instance, if required, only from within the FortiManager system itself rather than through Azure-level controls.
- Before performing any upgrade or modification:

Run `execute lvm info` to verify disk composition and ensure no Azure temporary disk is included in LVM, For example:

```
Disk 1: 10 TB, Disk 2: 6 TB, ...
```

If all listed disks were explicitly added by the fmg-admin, this indicates that no temporary disk is part of LVM and the upgrade is considered safe.

If an unexpected disk is detected (e.g., smaller system disk such as ~128 GB), it is likely the Azure temporary disk. In this case, perform a full backup before proceeding with the upgrade.

If issues occur after the upgrade:

- Run `execute format disk` to rebuild LVM,
- Use `execute restore` to recover data from backup.

The possible root cause may be as follows:

Prior to version 7.4.2, the system assumed sdb was always the Azure temporary disk and excluded it from LVM. In certain corner cases, a different device (e.g., sda) may have been incorrectly added to LVM. After upgrading, the existing LVM metadata persists on disk. When the VM is later deallocated and reallocated, Azure replaces the temporary disk, causing LVM initialization to fail due to stale metadata. As a result, any data previously stored on the temporary disk is lost.

Script creation API endpoint has changed starting in FortiManager 7.6.5

The endpoint used to create scripts through the FortiManager API has changed starting in FortiManager 7.6.5.

Previous endpoints:

```
dvmdb/script
dvmdb/adom/{adom}/script
dvmdb/global/script
```

New endpoints:

```
pm/config/adom/{adom}/obj/fmg/script
pm/config/global/obj/fmg/script
```

If you are using this endpoint in any automation, it should be updated following your upgrade to FortiManager 7.6.5 or later. For more information on this change, see Revision control for scripts and script groups with View Diff function in the CLI format.

Upgrading FortiGate devices on FOS 7.6.1 and 7.6.2 from FortiManager

Due to FortiOS issue 1106072, image file transfers between FortiManager and FortiGate devices on FortiOS 7.6.1 and 7.6.2 may fail when the upgrade is initiated from the FortiManager acting as the Local FDS Server. This issue is resolved in FortiOS 7.6.3 and later.

If you select an multi-step upgrade path for FortiGate which contains FortiOS 7.6.1 or 7.6.2, the upgrade process may stop once the devices have been upgraded to these affected versions.

Workarounds:

When managed devices have access to public FortiGuard:

- If FortiGate devices have internet connectivity, you can enable the “Let Device Download Firmware From FortiGuard” option in FortiManager. This allows FortiGate devices to retrieve the firmware image directly from FortiGuard during the upgrade process, reducing load on FortiManager.

When managed devices do NOT have access to public FortiGuard (air-gapped or restricted environments):

- Firmware upgrades may require using the following CLI command on the FortiGate:

  ```
  execute restore image management-station <Image-ID> <Version>
  ```

  With this approach, the FortiGate pulls the firmware image from FortiManager, which acts as a Local FDS server.

  If multiple managed devices are affected, this CLI command can be deployed via a FortiManager script and installed across the FortiGate devices to streamline the upgrade process.

The FortiManager XML API is no longer supported

The XML API is removed as of FortiManager 7.6.5.

New Admin Profile permissions

In FortiManager 7.6.4, the following permissions are added for Admin Profiles:

- *Firmware Upgrades* (`device-fwm-profile`): set permissions for device firmware profiles.
- *Assign Templates to Device* (`device-assignment`): set permissions to assign provisioning templates.
- *Execute Script* (`script-run`): set permissions to execute scripts.

To review the default settings for these permissions in predefined Admin Profiles, see the FortiManager Administration Guide.

For existing custom Admin Profiles created prior to upgrading to FortiManager 7.6.4 or later, the new permissions will be set to `None`. You must update these settings according to your needs in the custom Admin Profiles.

Default password policy for local users

Beginning in FortiManager 7.6.4, a password policy for local users is enabled and configured by default. If you are setting up FortiManager 7.6.4 or later, the password created at setup must be at least 8 characters and must contain uppercase letter(s), lowercase letter(s), number(s), and special character(s).

Note that existing password policy settings are maintained after upgrading. For example, if the password policy is disabled prior to upgrading to FortiManager 7.6.4 or later, it will remain disabled after the upgrade.

MEAs removed in FortiManager 7.6.4

As of FortiManager 7.6.4, there is no support for management extension applications (MEAs) in FortiManager.

New CLI option for managing FortiGate HA clusters

By default, FortiManager no longer installs HA-related configurations to FortiGate clusters unless explicitly configured to do so.

The following CLI option has been added in FortiManager 7.6.3:

```
config system dm
   set handle-nonhasync-config {enable | disable}
end
```

Previously, there was no CLI option like `handle-nonhasync-config`. This caused issues during installations to FortiGate HA clusters. For example, FortiManager could push FortiGate A's IP to FortiGate B, leading to partial or failed policy package (PP) installations.

Now, with the introduction of the `handle-nonhasync-config` CLI setting:

- Disabled (default): FortiManager will skip any configuration items marked as nonhasync when installing to the FortiGate. This avoids pushing HA-related or member-specific configurations that might break HA sync.
- Enabled: FortiManager will include nonhasync configuration items during installation, allowing updates to HA settings, vdom-exception configs, and other per-platform objects.

This change makes FortiManager behavior safer by default and gives admins more control over what gets pushed to HA clusters.

SSL VPN tunnel mode no longer supported in FortiOS 7.6.3

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is no longer available in the GUI and CLI. Settings will not be upgraded from previous versions. This applies to all FortiGate models.

To ensure uninterrupted remote access, customers must migrate their SSL VPN tunnel mode configuration to IPsec VPN before upgrading to FortiOS 7.6.3.

See Migration from SSL VPN tunnel mode to IPsec VPN in the FortiOS *7.6 New Feature* guide for detailed steps on migrating to IPsec VPN before upgrade.

A complete migration guide can be found in the following links:

- For FortiOS 7.6, see SSL VPN to IPsec VPN Migration.
- For FortiOS 7.4, see SSL VPN to IPsec VPN Migration.

Adding VM devices to FortiManager

As of FortiManager 7.6.3, connection between VM devices and FortiManager is restricted for security. By default, FortiManager will not allow VM platform connection in FGFM.

This applies to the following products:

- FortiGate-VM
- FortiCarrier-VM
- FortiProxy-VM
- FortiFirewall-VM

When upgrading from an earlier version of FortiManager, VM devices already managed by FortiManager will continue to be supported without interruption, but you must enable `fgfm-allow-vm` in global settings before adding additional VM devices.

To allow VM platform connection in FGFM, enter the following command in the FortiManager CLI:

```
config system global
   set fgfm-allow-vm enable
end
```

The system interface speed is read-only in FortiManager

The default value for `system interface speed` in FortiOS depends on the FortiGate platform, specified interface, and config. This attribute is read-only in FortiManager, and can only be edited in the FortiGate.

HA synchronization of FortiGuard package management receive status

Starting in FortiManager 7.6.2, the *To Be Deployed Version* configured in *FortiGuard > Packages > Receive Status* is synchronized in an HA cluster. This means that the package version selected for deployment on the primary device will persist during a failover event. For more information on the *To Be Deployed Version* setting, see the FortiManager Administration Guide.

When upgrading an operating FortiManager cluster to version 7.6.2, please review *To Be Deployed Version* settings for each cluster member before proceeding with the upgrade to ensure there is no unintended impact when the settings are synchronized. If the *To Be Deployed Version* package is not available on the secondary FortiManager, the secondary FortiManager will stay at the latest package to be installed.

The names of policies derived from policy blocks no longer automatically include the policy block name

Previously, when a policy was derived from a "policy block," its name was automatically prefixed with the policy block name, ensuring unique names but sometimes exceeding the 35-character limit in the policy package. To address this, the renaming behavior has been removed, and policies now retain their original names without policy block prefixes, avoiding the character limit issue.

After the fix, FortiManager may encounter duplicate policy names if multiple policy blocks previously contained policies with the same base name. Since FortiManager requires unique policy names for proper management, this duplication can break the installation or functionality of policies. To resolve this, customers may need to manually identify and rename all conflicting policies after upgrading.

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the `private-data-encryption` key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
123456789012345678901234567890abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
123456789012345678901234567890abc
Your private data encryption key is accepted.
```

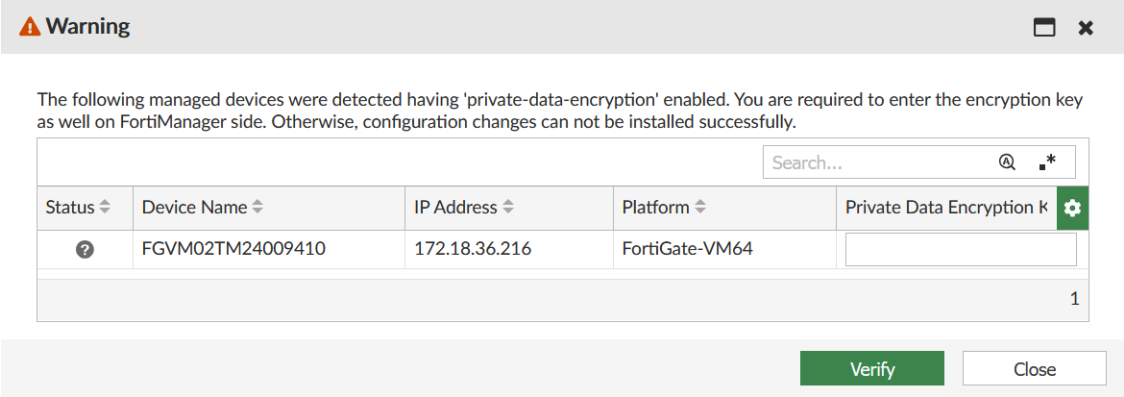
New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y

Private data encryption key generation succeeded!
```

FortiManager behavior

Support for the FortiGate `private-data-encryption` key by the *Device Manager* in FortiManager 7.6.2 and earlier is unchanged. It automatically detects the remote FortiGate `private-data-encryption` key status and prompts the administrator to manually type the private key (see picture below). FortiManager 7.6.2 and earlier does not support the updated, random `private-data-encryption` key as the administrator will have no knowledge of the key generated in the FortiOS CLI command above. It will be supported in a later version of FortiManager.



FortiOS upgrade behavior

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal `private-data-encryption` key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal `private-data-encryption` key and can continue to manage the FortiGate device. However, if the `private-data-encryption` key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

Shell access has been removed

As of FortiManager 7.6.0, shell access has been removed.

The following CLI variables have been removed, which were previously used to enable shell access:

```
config system admin setting
   set shell-access {enable | disable}
   set shell-password <passwd>
```

The following CLI command has been removed, which was previously used to access shell when enabled:

```
execute shell
```

Enable fcp-cfg-service for Backup Mode ADOMs

When performing a configuration backup from the CLI of FortiGates managed by FortiManager in Backup Mode ADOMs, you must enable the "`fcp-cfg-service`" using the following command on the FortiManager:

```
config system global
   set fcp-cfg-service enable
end
```

System Templates include new fields

Beginning in FortiManager 7.4.3, the *Hostname*, *Timezone*, *gui-device-latitude*, and *gui-device-longitude* fields have been added to System Templates.

System Templates created before upgrading to 7.4.3 must be reconfigured to specify these fields following the upgrade. If these fields are not specified in a System Template, the default settings will be applied the next time an install is performed which may result in preferred settings being overwritten on the managed device.

Custom certificate name verification for FortiGate connection

In FortiManager 7.6.2, the `fgfm-peercert-withoutsn` setting has been removed, so there is no method to disable this verification. The FortiGate certificate must contain the FortiGate serial number in either the CN or SAN.

FortiManager 7.4.3 introduces a new verification of the CN or SAN of a custom certificate uploaded by the FortiGate admin. This custom certificate is used when a FortiGate device connects to a FortiManager unit. The FortiGate and FortiManager administrators may configure the use of a custom certificate with the following CLI commands:

FortiGate-related CLI:

```
config system central-management
   local-cert Certificate to be used by FGFM protocol.
   ca-cert CA certificate to be used by FGFM protocol.
```

FortiManager-related CLI:

```
config system global
   fgfm-ca-cert set the extra fgfm CA certificates.
   fgfm-cert-exclusive set if the local or CA certificates should be used exclusively.
   fgfm-local-cert set the fgfm local certificate.
```

Upon upgrading to FortiManager 7.4.3, FortiManager will request that the FortiGate certificate must contain the FortiGate serial number either in the CN or SAN. The tunnel connection may fail if a matching serial number is not found. If the tunnel connection fails, the administrator may need to re-generate the custom certificates to include serial number.

Additional configuration required for SSO users

Beginning in 7.4.3, additional configuration is needed for FortiManager Users declared as wildcard SSO users.

When configuring Administrators as wildcard SSO users, the `ext-auth-accprofile-override` and/or `ext-auth-adom-override` features, under *Advanced Options*, should be enabled if the intent is to obtain the ADOMs list and/or permission profile from the SAML IdP.

When using VPN Manager, IPSEC VPN CA certificates must be re-issued to all devices after upgrade

When FortiManager is upgraded to 7.4.2/7.6.0 or later, it creates a new CA <ADOM Name>_CA3 certificate as part of a fix for resolved issue 796858. See Resolved Issues in the FortiManager 7.4.2 Release Notes. These certificates are installed to the FortiGate devices on the next policy push. As a result, the next time any IPSEC VPNs which use FortiManager certificates rekey, they will fail authentication and be unable to re-establish.

The old CA <ADOM Name>_CA2 cannot be deleted, as existing certificates rely on it for validation. Similarly, the new CA <ADOM Name>_CA3 cannot be deleted as it is required for the fix. Therefore, customers affected by this change must follow the below workaround after upgrading FortiManager to v7.4.2/7.6.0 or later.

A maintenance period is advised to avoid IPSEC VPN service disruption.

Workaround:

Re-issue *all* certificates again to *all* devices, and then delete the old CA <ADOM Name>_CA2 from all devices. Next, regenerate the VPN certificates.

To remove CA2 from FortiManager, *Policy & Objects > Advanced > CA Certificates* must be enabled in feature visibility.

FortiGuard web filtering category v10 update

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

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

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

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

FortiManager 7.2.3 and later firmware on FortiGuard

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

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

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

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

Configuration backup requires a password

As of FortiManager 7.4.2, configuration backup files are automatically encrypted and require you to set a password. The password is required for scheduled backups as well.

In previous versions, the encryption and password were optional.

For more information, see the FortiManager Administration Guide.

FortiManager-400E support

FortiManager 7.4.2 and later does not support the FortiManager-400E device.

FortiManager 7.4.2 introduces an upgrade of the OpenSSL library to address known vulnerabilities in the library. As a result, the SSL connection that is setup between the FortiManager-400E device and the Google Map server hosted by Fortinet uses a SHA2 (2048) public key length. The certificate stored on the BIOS that is used during the setup of the SSL connection contains a SHA1 public key length, which causes the connection setup to fail. Running the following command shows the key length.

```
FMG400E # conf sys certificate local
   (local)# ed Fortinet_Local
      (Fortinet_Local)# get
      name : Fortinet_Local
      password : *
      comment : Default local certificate
      private-key :
      certificate :
```

```
        Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN =
              FL3K5E3M15000074, emailAddress = support@fortinet.com
        Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority,
              CN = support, emailAddress = support@fortinet.com
        Valid from: 2015-03-06 16:22:10 GMT
        Valid to: 2038-01-19 03:14:07 GMT
        Fingerprint: FC:D0:0C:8D:DC:57:B6:16:58:DF:90:22:77:6F:2C:1B
        Public key: rsaEncryption (1024 bits)
        Signature: sha1WithRSAEncryption
        Root CA: No
        Version: 3
        Serial Num:
        1e:07:7a
        Extension 1: X509v3 Basic Constraints:
        CA:FALSE
        ...
(Fortinet_Local)#
```

Serial console has changed for FortiManager deployments on Xen

As of FortiManager 7.4.1, the serial console for Xen deployments has changed from hvc0 (Xen specific) to ttyS0 (standard).

OpenXen in PV mode is not supported in FortiManager 7.4.1

As of FortiManager 7.4.1, kernel and rootfs are encrypted. OpenXen in PV mode tries to unzip the kernel and rootfs, but it will fail. Therefore, OpenXen in PV mode cannot be used when deploying or upgrading to FortiManager 7.4.1. Only HVM (hardware virtual machine) mode is supported for OpenXen in FortiManager 7.4.1.

Option to enable permission check when copying policies

As of 7.4.0, a new command is added in the CLI:

```
config system global
   set no-copy-permission-check {enable | disable}
end
```

By default, this is set to `disable`. When set to `enable`, a check is performed when copying policies to prevent changing global device objects if the user does not have permission.

Install On column for policies

Prior to version 7.2.3, the 'Install-on' column for policies in the policy block had no effect. However, starting from version 7.2.3, the 'Install-on' column is operational and significantly impacts the behavior and installation process of policies. It's important to note that using 'Install-on' on policies in the policy block is not recommended. If required, this setting can only be configured through a script or JSON APIs.

Changes to FortiManager meta fields

Beginning in 7.2.0, FortiManager supports policy object metadata variables.

When upgrading from FortiManager 7.0 to 7.2.0 and later, FortiManager will automatically create ADOM-level metadata variable policy objects for meta fields previously configured in System Settings that have per-device mapping configurations detected. Objects using the meta field, for example CLI templates, are automatically updated to use the new metadata variable policy objects.

Meta fields in *System Settings* can continue to be used as comments/tags for configurations.

For more information, see ADOM-level meta variables for general use in scripts, templates, and model devices.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain policies with multiple interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

Reconfiguring Virtual Wire Pairs (VWP)

A conflict can occur between the ADOM database and device database when a Virtual Wire Pair (VWP) is installed on a managed FortiGate that already has a configured VWP in the device database. This can happen when an existing VWP has been reconfigured or replaced.

Before installing the VWP, you must first remove the old VWP from the device's database, otherwise a policy and object validation error may occur during installation. You can remove the VWP from the device database by

going to *Device Manager* > *Device & Groups*, selecting the managed device, and removing the VWP from *System* > *Interface*.

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.

New features

For information about what's new in FortiManager 7.6.7, see the FortiManager 7.6 New Features Guide. The index in the New Features Guide lists new features by release.

Upgrade Information

Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM, including recommended upgrade paths.
See the *FortiManager Upgrade Guide* in the Fortinet Document Library.

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. See the *FortiManager Upgrade Guide* in the Fortinet Document Library.

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 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
```

Firmware image checksums

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

FortiManager VM firmware

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

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Google Cloud Platform

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

Linux KVM

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

Microsoft Azure

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

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

Microsoft Hyper-V Server

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

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

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 7.6.7 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

FortiManager 7.6.7 supports the following software:

- FortiWeb on page 33
- Virtualization on page 33

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 7.6.7 supports the following web browsers:

- Google Chrome version 144
- Microsoft Edge version 144
- Mozilla Firefox 147

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 7.6.7 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility tool in the Fortinet Document Library.

See FortiManager compatibility with FortiOS.

FortiManager 7.6.7 supports the following versions of FortiOS and FortiOS Carrier:

- 7.6.0 to 7.6.7
- 7.4.0 to 7.4.12
- 7.2.0 to 7.2.13
- 7.0.0 to 7.0.19

FortiADC

FortiManager 7.6.7 supports the following versions of FortiADC:

- 8.0.0 and later
- 7.6.0 and later
- 7.4.0 and later

- 7.2.0 and later
- 7.1.0 and later
- 7.0.0 and later
- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later

FortiAnalyzer

FortiManager 7.6.7 supports the following versions of FortiAnalyzer:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiAnalyzer-BigData

FortiManager 7.6.7 supports the following versions of FortiAnalyzer-BigData:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiAP

FortiAP devices are controlled by the FortiGate devices managed by FortiManager. Thus, support for FortiAP firmware is dependent on supported FortiOS versions.

For FortiManager compatibility with FortiOS, see FortiOS and FortiOS Carrier.

For FortiOS compatibility with FortiAP, see the FortiAP and FortiOS Compatibility Matrix.

FortiAuthenticator

FortiManager 7.6.7 supports the following versions of FortiAuthenticator:

- 8.0.0 and later
- 7.0.0 and later
- 6.6.0 and later
- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later

- 6.2.0 and later
- 6.1.0 and later
- 6.0.0 and later

FortiCache

FortiManager 7.6.7 supports the following versions of FortiCache:

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

FortiCASB

FortiManager 7.6.7 supports the following versions of FortiCASB:

- 23.2.0 and later

FortiClient

FortiManager 7.6.7 supports the following versions of FortiClient:

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

FortiDDoS

FortiManager 7.6.7 supports the following versions of FortiDDoS:

- 7.2.0 and later
- 7.0.0 and later
- 6.6.0 and later
- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later
- 6.1.0 and later
- 5.7.0 and later
- 5.6.0 and later

Limited support. For more information, see Feature support on page 33.

FortiDeceptor

FortiManager 7.6.7 supports the following versions of FortiDeceptor:

- 6.1.0 and later
- 6.0.0 and later
- 5.3.0 and later
- 5.2.0 and later
- 5.1.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.6.7 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiMail

FortiManager 7.6.7 supports the following versions of FortiMail:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later

FortiPAM

FortiManager 7.6.7 supports the following versions of FortiPAM:

- 1.8.0 and later
- 1.7.0 and later
- 1.6.0 and later
- 1.5.0 and later
- 1.4.0 and later
- 1.3.0 and later
- 1.2.0 and later

- 1.1.0 and later
- 1.0.0 and later

FortiPortal

For more information about compatibility with FortiPortal, see *FortiPortal Compatibility* in the Fortinet Document Library.

FortiProxy

FortiManager 7.6.7 supports configuration management for the following versions of FortiProxy:

- 7.6.2 to 7.6.4
- 7.4.0 to 7.4.3, and 7.4.5 to 7.4.13
- 7.2.2, 7.2.3, 7.2.7, and 7.2.9 to 7.2.13
- 7.0.7 to 7.0.21

Configuration management support is identified as *Management Features* in these release notes. See Feature support on page 33.

FortiManager 7.6.7 supports logs from the following versions of FortiProxy:

- 7.6.0 to 7.6.4
- 7.4.0 to 7.4.13
- 7.2.0 to 7.2.15
- 7.0.0 to 7.0.22
- 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 7.6.7 supports the following versions of FortiSandbox:

- 5.0.0 and later
- 4.4.0 and later
- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later

FortiSASE

For more information about compatibility, see the FortiSASE Release Notes.

FortiSOAR

FortiManager 7.6.7 supports the following versions of FortiSOAR:

- 7.6.0 and later
- 7.5.0 and later
- 7.4.0 and later
- 7.3.0 and later
- 7.2.0 and later

FortiSRA

FortiManager 7.6.7 supports the following versions of FortiSRA:

- 1.1.0 and later
- 1.0.0 and later

FortiSwitch

FortiSwitch devices are controlled by the FortiGate devices managed by FortiManager. Thus, support for FortiSwitchOS is dependent on supported FortiOS versions.

For FortiManager compatibility with FortiOS, see FortiOS and FortiOS Carrier on page 27.

For FortiOS Compatibility with FortiSwitchOS, see FortiLink Compatibility.

FortiTester

FortiManager 7.6.7 supports the following versions of FortiTester:

- 7.4.0 and later
- 7.3.0 and later
- 7.2.0 and later
- 7.1.0 and later

FortiToken

FortiManager 7.6.7 supports the following versions of FortiToken:

- 3.0.0 and later

FortiWeb

FortiManager 7.6.7 supports the following versions of FortiWeb:

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

Virtualization

FortiManager 7.6.7 supports the following virtualization software:

Public Cloud

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

Private Cloud

- Citrix XenServer 8.2 and later
- OpenSource XenServer 4.2.5
- Microsoft Hyper-V Server 2016, 2019, and 2022
- Nutanix
  - AHV 20220304 and later
  - AOS 6.5 and later
  - NCC 4.6 and later
  - LCM 3.0 and later
- RedHat 9.1
  - Other versions and Linux KVM distributions are also supported
- VMware ESXi versions 6.5 and later

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Configuration Management	Firmware Management	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓	✓
FortiADC			✓	✓		
FortiAnalyzer				✓	✓	✓
FortiAP	✓*	✓				
FortiAuthenticator						✓
FortiCache				✓	✓	✓
FortiClient			✓		✓	✓
FortiDDoS				✓	✓	✓
FortiDeceptor			✓			
FortiExtender	✓*	✓				
FortiFirewall	✓					✓
FortiFirewall Carrier	✓					✓
FortiMail			✓	✓	✓	✓
FortiProxy	✓	✓**	✓	✓	✓	✓
FortiSandbox			✓	✓	✓	✓
FortiSOAR			✓	✓		
FortiSwitch	✓*	✓				
FortiTester			✓			
FortiWeb			✓	✓	✓	✓
Syslog						✓

*FortiManager can push FortiAP, FortiSwitch, and FortiExtender configuration to FortiGate. FortiGate then manages the FortiAP, FortiSwitch, or FortiExtender; they will not be directly managed by FortiManager.

**Only upgrades performed directly on an individual device from *Device Manager* are supported. Firmware management templates are not supported for these devices.

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, FortiWeb, FortiCache, FortiProxy, FortiAuthenticator, and other Fortinet product models and firmware versions can be managed by a FortiManager or send logs to a FortiManager running version 7.6.7.

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

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 41.

Model	Firmware Version
FortiGate: FortiGate-30G, FortiGate-31G, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60F, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71G, FortiGate-71G-POE, FortiGate-71F, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-200E, FortiGate-200F, FortiGate-200G, FortiGate-201E, FortiGate-201F, FortiGate-201G, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-700G, FortiGate-701G, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.6

Model	Firmware Version
FortiGate 7000 Series: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC **FortiGate DC:** FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-ACDC, FortiGate-3000F-DC, FortiGate-3001F-ACDC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS **FortiWiFi:** FortiWiFi-30G, FortiWiFi-31G, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP, FortiWiFi-51G, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen **FortiGate Rugged:** FortiGateRugged-50G-5G, FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGateRugged-70G, FortiGateRugged-70G-5G-Dual	

Model	Firmware Version
FortiGate: FortiGate-30G, FortiGate-31G, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE, FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-70G, FortiGate-70G-POE, FortiGate-71F, FortiGate-71G, FortiGate-71G-POE, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100F, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-200G, FortiGate-201E, FortiGate-201F, FortiGate-201G, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-700G, FortiGate-701G, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC **FortiGate 7000 Series**: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC **FortiGate DC:** FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4801F-DC-NEBS	7.4

Model	Firmware Version
FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP, FortiWiFi-51G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen **FortiGate Rugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G, FortiGateRugged-70G, FortiGateRugged-70G-5G-Dual	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-DSL, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90G, FortiGate-91E, FortiGate-91G, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-120G, FortiGate-121G, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-900G, FortiGate-901G, FortiGate-1000D, FortiGate-1000F, FortiGate-1001F, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3200F, FortiGate-3201F, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3700F, FortiGate-3701F, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate-4800F, FortiGate-4801F, FortiGate-4801F-NEBS **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate 6000 Series**: FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC **FortiGate 7000 Series**: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.2

Model	Firmware Version
FortiGate DC: FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-900G-DC, FortiGate-901G-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC, FortiGate-4800F-DC, FortiGate-4801F-DC, FortiGate-4801F-DC-NEBS **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-70G, FortiWiFi-71G, FortiWiFi-80F-2R, FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGate Rugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G, FortiGateRugged-70F, FortiGateRugged-70F-3G4G	
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	7.0

Model	Firmware Version
FortiGate DC: FortiGate-400F-DC, FortiGate-401E-DC, FortiGate-401F-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3000F-ACDC, FortiGate-3001F-DC, FortiGate-3001F-ACDC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC **FortiWiFi:** FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen **FortiGate Rugged:** FortiGateRugged-60F, FortiGateRugged-60F-3G4G	

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.6.7 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 36.

FortiGate Model	FortiOS Version
FortiGate-400G	7.6.5
FortiGate-401G	7.6.6
FortiGate-3000G, FortiGate-3001G	7.6.5

FortiOS 7.4

FortiGate Model	FortiOS Version
FortiGate-70G-POE-5G, FortiGate-71G-POE-5G	7.4.8

FortiGate Model	FortiOS Version
FortiGate-3800G, FortiGate-3801G FortiGate-3800G-DC, FortiGate-3801G-DC	7.4.11
FortiGateRugged-50G-5G	7.4.8
FortiGateRugged-60G, FortiGateRugged-60G-5G, FortiGateRugged-60G-5G-M12, FortiGateRugged-60G-M12	7.4.11
FortiGateRugged-70G-5G	7.4.11

FortiOS 7.2

FortiGate Model	FortiOS Version
FortiGate-30G, FortiGate-31G	7.2.12
FortiGate-70G	7.2.11
FortiGate-71G	7.2.12
FortiGate-70G-POE	7.2.12
FortiGate-71G-POE	7.2.11
FortiGate-200G, FortiGate-201G	7.2.12
FortiGate-700G, FortiGate-701G	7.2.11
FortiWiFi-30G, FortiWiFi-31G	7.2.12
FortiWiFi-70G, FortiWiFi-70G-POE, FortiWiFi-71G	7.2.11

FortiOS 7.0

FortiGate Model	FortiOS Version
FortiGate-50G, FortiGate-50G-5G, FortiGate-50G-DSL, FortiGate-50G-SFP, FortiGate-50G-SFP-POE	7.0.17
FortiGate-51G, FortiGate-51G-5G, FortiGate-51G-SFP-POE	7.0.17
FortiGate-80F-DSL	7.0.17
FortiGate-90G, FortiGate-91G	7.0.17
FortiGate-120G, FortiGate-121G	7.0.16
FortiGate-900G, FortiGate-900G-DC FortiGate-901G, FortiGate-901G-DC	7.0.17
FortiGate-1000F, FortiGate-1001F	7.0.17

FortiGate Model	FortiOS Version
FortiGate-3200F, FortiGate-3201F	7.0.17
FortiGate-3700F, FortiGate-3701F	7.0.17
FortiGate-4800F, FortiGate-4800F-DC FortiGate-4801F, FortiGate-4801F-DC, FortiGate-4801F-NEBS, FortiGate-4801F-DC-NEBS	7.0.17
FortiGate-6000F, FortiGate-6001F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.16
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.16
FortiGate-7000F, FortiGate-7081F, FortiGate-7081F-DC, FortiGate-7081F-2-DC, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.16
FortiGateRugged-50G-5G	7.0.17
FortiGateRugged-70F, FortiGateRugged-70F-3G4G	7.0.17
FortiGateRugged-70G	7.0.15
FortiGateRugged-70G-5G-Dual	7.0.16
FortiWiFi-50G, FortiWiFi-50G-5G, FortiWiFi-50G-DSL, FortiWiFi-50G-SFP	7.0.17
FortiWiFi-51G	7.0.17
FortiWiFi-51G-5G	7.0.15
FortiWiFi-80F-2R-3G4G-DSL, FortiWiFi-81F-2R-3G4G-DSL	7.0.17

FortiCarrier models

The following FortiCarrier models are released with FortiCarrier firmware.

For information about supported FortiCarrier models on special branch releases of FortiCarrier firmware, see FortiCarrier special branch models on page 45.

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1	7.6

Model	Firmware Version
FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC **FortiCarrier 7000 Series**: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3000F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4800F-DC, FortiCarrier-4801F-DC, FortiCarrier-4801F-DC-NEBS **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC **FortiCarrier 7000 Series**: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **FortiCarrier-DC**: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4801F-DC-NEBS	7.4

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-IBM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3200F, FortiCarrier-3201F, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3700F, FortiCarrier-3701F, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-4800F, FortiCarrier-4801F, FortiCarrier-4801F-NEBS **FortiCarrier 5000 Series**: FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier 6000 Series**: FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC **FortiCarrier 7000 Series**: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC **FortiCarrier-DC**: FortiCarrier-2600F-DC, FortiCarrier-2601F-DC, FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3000F-ACDC, FortiCarrier-3001F-DC, FortiCarrier-3001F-ACDC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC, FortiCarrier-4801F-DC-NEBS **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.2

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.6.7 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see FortiCarrier models on page 43.

FortiCarrier 7.4

FortiCarrier Model	FortiCarrier Version
FortiCarrier-3800G, FortiCarrier-3801G FortiCarrier-3800G-DC, FortiCarrier-3801G-DC	7.4.11

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version
FortiCarrier-3200F, FortiCarrier-3201F	7.0.17
FortiCarrier-3700F, FortiCarrier-3701F	7.0.17
FortiCarrier-4800F, FortiCarrier-4800F-DC FortiCarrier-4801F, FortiCarrier-4801F-DC, FortiCarrier-4801F-NEBS, FortiCarrier-4801F-DC-NEBS	7.0.17
FortiCarrier-6000F, FortiCarrier-6001F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.16
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.16
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7081F-DC, FortiCarrier-7081F-2-DC, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	7.0.16

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-1000G, FortiADC-2000G, FortiADC-4000G, FortiADC-5000G	8.0
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-320F, FortiADC-400F, FortiADC-420F, FortiADC-1000F, FortiADC-1200F, FortiADC-2000F, FortiADC-2200F, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVER, FortiADC-VM	7.6

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-320F, FortiADC-400D, FortiADC-400F, FortiADC-420F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVER, FortiADC-VM	7.4
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-ALI, FortiADC-ALI_ONDEMAND, FortiADC-AZURE, FortiADC-AZURE_ONDEMAND, FortiADC-GCP, FortiADC-GCP_ONDEMAND, FortiADC-HYV, FortiADC-IBM, FortiADC-KVM, FortiADC-OCI, FortiADC-XENAWS, FortiADC-XENAWS_ONDEMAND, FortiADC-XENOPEN, FortiADC-XENSERVER, FortiADC-VM	6.2, 7.0, 7.1, 7.2

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-300G, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3750G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD **FortiAnalyzer VM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen	7.6
FortiAnalyzer: FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3750G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD	7.4

Model	Firmware Version
FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen	
FortiAnalyzer: FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3510G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD **FortiAnalyzer VM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen	7.2
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-810G, FortiAnalyzer-1000F, FortiAnalyzer-1000G, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3100G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E, FortiAnalyzer-K8S-CLOUD **FortiAnalyzer VM**: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-VIO-CLOUD, FortiAnalyzer-VM64-Xen	7.0

FortiAnalyzer-BigData models

Model	Firmware Version
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F **FortiAnalyzer-BigData VM**: FortiAnalyzer-BigData-VM64	7.2
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F **FortiAnalyzer-BigData VM**: FortiAnalyzer-BigData-VM64	7.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator VM: FAC-VM	7.0, 8.0
FortiAuthenticator: FAC-200E, FAC-300F, FAC-400E, FAC-800F, FAC-2000E, FAC-3000E, FAC-3000F **FortiAuthenticator VM:** FAC-VM	6.5, 6.6
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E, FAC-3000F **FortiAuthenticator VM:** FAC-VM	6.4
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.0, 6.1, 6.2, 6.3

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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-3000G, FortiDDoS-4000G	7.2
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-1500G, FortiDDoS-1500G-LR, FortiDDoS-2000F, FortiDDoS-2000G, FortiDDoS-3000F, FortiDDoS-3000G **FortiDDoS VM**: FortiDDoS-VM	7.0
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F **FortiDDoS VM**: FortiDDoS-VM	6.4, 6.5, 6.6
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F **FortiDDoS VM**: FortiDDoS-VM	6.3
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F	6.2

Model	Firmware Version
FortiDDoS VM: FortiDDoS-VM	
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.6, 5.7

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-100G, FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	5.0, 5.1, 5.2, 5.3, 6.0, 6.1
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.6.7 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version
FortiFirewall: FortiFirewall-1801F, FortiFirewall-2600F, FortiFirewall-3001F, FortiFirewall-3501F, FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F, FortiFirewall-4801F-NEBS **FortiFirewall DC**: FortiFirewall-3001F-DC, FortiFirewall-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC, FortiFirewall-4801F-DC-NEBS **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.6
FortiFirewall: FortiFirewall-1801F, FortiFirewall-2600F, FortiFirewall-3001F, FortiFirewall-3501F, FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F, FortiFirewall-4801F-NEBS **FortiFirewall DC**: FortiFirewall-3001F-DC, FortiFirewall-3980E-DC, FortiFirewall-4200F-DC, FortiFirewall-4400F-DC, FortiFirewall-4401F-DC, FortiFirewall-4801F-DC-NEBS **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.4

Model	Firmware Version
FortiFirewall: FortiFirewall-3980E, FortiFirewall-4200F, FortiFirewall-4400F, FortiFirewall-4401F, FortiFirewall-4801F, FortiFirewall-4801F-NEBS **FortiFirewall DC**: FortiFirewall-4200F-DC, FortiFirewall-4401F-DC, FortiFirewall-4801F-DC-NEBS **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC **FortiFirewall-VM**: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.0

FortiFirewall special branch models

Model	Firmware Version	Firmware Build (for special branch)
FortiFirewall: FortiFirewall-3001F **FortiFirewall DC**: FortiFirewall-3001F-DC,	7.0.10	4955
FortiFirewall: FortiFirewall-3501F **FortiFirewall DC**: FortiFirewall-3001F-DC,	7.0.10	4955

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.6.7 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version
FortiFirewallCarrier: FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS **FortiFirewallCarrier DC**: FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC, FortiFirewallCarrier-4801F-DC-NEBS **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.6
FortiFirewallCarrier: FortiFirewallCarrier-1801F, FortiFirewallCarrier-2600F, FortiFirewallCarrier-3001F, FortiFirewallCarrier-3501F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4401F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS	7.4

Model	Firmware Version
FortiFirewallCarrier DC: FortiFirewallCarrier-1801F-DC, FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4401F-DC, FortiFirewallCarrier-4801F-DC-NEBS **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	
FortiFirewallCarrier: FortiFirewallCarrier-2600F, FortiFirewallCarrier-3980E, FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F, FortiFirewallCarrier-4801F, FortiFirewallCarrier-4801F-NEBS **FortiFirewallCarrier DC**: FortiFirewallCarrier-4200F-DC, FortiFirewallCarrier-4801F-DC-NEBS **FortiFirewallCarrier-VM**: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.2
FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.0

FortiFirewall special branch models

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-1801F, FortiFirewallCarrier-4401F	7.2.6	4609
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0.10	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0.10	4940

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-900G, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCP, FML-VM-XEN, FortiMail Cloud	7.6
FortiMail: FE-60D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCP, FML-VM-XEN	7.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCP, FML-VM-XEN	7.2

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCP, FML-VM-XEN	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FML-VM, FML-VM-ALI, FML-VM-AWS, FML-VM-Azure, FML-VM-DK, FML-VM-GCP, FML-VM-HV, FML-VM-KVM, FML-VM-OCP, FML-VM-XEN, **FortiMail Cloud**	6.2, 6.4

FortiPAM models

Model	Firmware Version
FortiPAM: FortiPAM-100G, FortiPAM-400G, FortiPAM-1000G, FortiPAM-1100G, FortiPAM-3000G, FortiPAM-3100G **FortiPAM VM:** FortiPAM-Azure, FortiPAM-KVM	1.7, 1.8
FortiPAM: FortiPAM-1000G, FortiPAM-3000G **FortiPAM VM:** FortiPAM-Azure, FortiPAM-KVM	1.5, 1.6
FortiPAM: FortiPAM-1000G, FortiPAM-3000G **FortiPAM VM:** FortiPAM-AWS, FortiPAM-Azure, FortiPAM-GCP, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1, 1.2, 1.3, 1.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	7.6
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	7.4
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G	7.0

Model	Firmware Version
FortiProxy VM: FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-OPC, FortiProxy-VM64	
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FortiProxy-KVM, FortiProxy-VM64	1.0, 1.1, 1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-500G, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000E, FSA-3000F **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FSA-AliCloud, FSA-AliCloud-Nested, FSA-AWS, FSA-AWS-Nested, FSA-Azure, FSA-Azure-Nested, FSA-Cloud, FSA-GCP, FSA-GCP-Nested, FSA-HYPERV, FSA-KVM, FSA-OCI-Nested, FSA-VM	5.0
FortiSandbox: FSA-500F, FSA-500G, FSA-1000D, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FSA-AWS, FSA-Cloud, FSA-VM	4.2, 4.4
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FSA-AWS, FSA-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FSA-AWS, FSA-VM	3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	7.2, 7.3, 7.4, 7.5, 7.6

FortiSRA models

Model	Firmware Version
FortiSRA: FortiSRA-1000G, FortiSRA-3000G **FortiSRA-VM**: FortiSRA-Azure, FortiSRA-HyperV, FortiSRA-KVM, FortiSRA-VM64	1.0, 1.1

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-BYOL, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.1, 7.2, 7.3, 7.4

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-100F, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-400F, FortiWeb-600D, FortiWeb-600E, FortiWeb-600F, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer **FortiWeb Cloud**, including FortiAppSec Cloud.	7.6
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-100F, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-400F, FortiWeb-600D, FortiWeb-600E, FortiWeb-600F, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	7.4

Model	Firmware Version
FortiWeb Cloud, including FortiAppSec Cloud.	
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000F, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer **FortiWeb Cloud**, including FortiAppSec Cloud.	7.2
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer **FortiWeb Cloud**, including FortiAppSec Cloud.	7.0

FortiExtender MODEM firmware compatibility

See the FortiOS Release Notes for a list of MODEM firmware filename and version for each FortiExtender model and where in the world the MODEMs are compatible.

Resolved issues

The following issues have been fixed in 7.6.7. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
1239191	When SSID configured with per-device mapping, during the installation, the FortiManager will report error: Commit failed: ssid fortinet is used by vap.
1239368	Duplicate SSID occurs when accented character is used at the end of the SSID name.

Device Manager

Bug ID	Description
894948	FortiManager fails to push the FortiAnalyzer override settings to the FortiGate.
895994	When using the 'where used' feature in Phase 2 quick mode selector, objects do not appear, and they can be removed.
1001557	Metadata variables are not supported for the "XAUTH" field in IPsec tunnel provisioning templates.
1015138	Unable to edit interface with dhcp reservation.
1028515	The Greenwich time zone on FortiGate does not supported on the FortiManager.
1189821	Failure to add FortiAnalyzer occurs when using the HA cluster's virtual IP in FortiManager.
1191558	Changes to SD-WAN performance SLA values are not reflected in the device database or the install preview when the detect-mode is set to remote.
1194361	Installation fails when device description contains single quote characters.
1204427	Script log results do not display logs from the most recent script execution; only logs from previous executions are shown.
1215217	The install preview does not load if a device in the device group is offline, but it works fine if all the devices are online.
1224965	Device identification is disabled when changing interface role from LAN to undefined.

Bug ID	Description
1240231	After upgrading FortiManager to version 7.6.5, remote access to FortiGate devices may fail with the error Error reading from remote server when using non-standard ports.
1244586	Installation failure occurs when unsetting the "`allow-traffic-redirect`" under the system global.
1246821	FortiManager retrieve may fail when an admins remote-group exists only in the root VDOM and the VDOM order starts with a non-root VDOM, causing invalid reference detection during device addition.
1247501	Installation error occurs when using metadata variables on IP range field in system template.
1251613	Registration of FortiGate-VM64-KVM as Device model to FortiManager may fail due to incorrect platform identification.
1254998	Incorrect Interface Syntax Selection for FGT90G/91G Gen1/Gen2 During Model Device (ZTP) Creation has been observed.
1269401	Performing device deletion may appear very slow. While the deletion process is still ongoing, clients performing policy package installation tasks may experience delays before the task starts or completes. This behavior has been observed in some cases where FortiManager manages more than 6,000 device groups.

FortiSwitch Manager

Bug ID	Description
1118271	FortiSwitch Device information is not displayed when FortiSwitch version is 7.4.3.
1227473	FortiManager attempts to install set poe-status disable on FortiSwitch ports that already have PoE disabled. The issue persists and reoccurs after configuration installation and synchronization.
1244165	When centrally managing switches via FortiManager, the "Switch-id" is limited to 16 characters. Configuring a hostname exceeding this limit triggers the error: "Switch-id: Value too long."
1246204	Firmware upgrade tasks stall when multiple upgrades for the same FortiSwitch are run concurrently.
1268279	Deleting custom-command from FortiSwitch Manager template is not deleting it from device.

Global ADOM

Bug ID	Description
1150670	Installation failure occurs when upgrading global ADOM from v7.2 to v7.4 due to gno-inspection settings.
1163223	A global object loses its global status when transferred from a local ADOM to an FortiGate device and then re-imported into another local ADOM, resulting in a duplicate object error.
1177672	When global policy package assignment fails, it may impacts the policy packages on the ADOM.
1201449	Global policy assignment configured with Automatically Install Policies to ADOM Devices may get stuck during deployment.
1232811	Unassigning a Global Policy Package may fail when it is referenced by SSL inspection profiles in the root ADOM.
1244194	Global Policy Block appended to Global Policy Package is not visible under root ADOM PP when assigned.
1245741	The Promote to Global feature for objects created in an ADOM may fail if the object name contains a forward slash (/) character.

Others

Bug ID	Description
1081121	The syslog server is unable to receive FortiManager event logs when the reliable option is enabled.
1179653	The API interface performance in version 7.6 may appear slower compared to previous versions.
1180920	After the installation, an event alert was received indicating that the FGFM tunnel is flapping.
1185269	The local log syslog feature set facility is not functioning properly.
1189184	Copy Policy Package operations may take longer than usual and remain stuck for an extended duration, even for small changes. This issue may occur when FortiOS does not return a response to FGFM requests from FortiManager.
1194429	FortiGuard Query Services displays an incorrect date for the Query Status when viewing the Number of Queries graph.
1201248	Historical logs are not displayed when FortiAnalyzer feature is enabled.

Bug ID	Description
1203535	FortiManager does not support the `diagnose fdsm fap-fsw-contract-download` request, so the fgdhttpd daemon rejects FortiGate attempts to retrieve FortiAP/FortiSwitch registration status.
1210519	Central-management settings are deleted on the primary unit when adding a FortiProxy HA cluster via Device Discover. This issue may occur when the FortiManager ADOM is configured in backup mode and the FortiProxy central-management setting is also set to the backup mode. Refreshing the device may trigger the issue.
1230277	If the ADOM in an earlier FortiManager version contains DLP dictionary entries named fg-*, which are reserved in FortiManager 7.6, the upgrade from ADOM 7.4 to 7.6 will fail. The upgrade process attempts to copy these reserved-name objects, but ADOM 7.6 does not allow them to be created or modified.
1234093	Time discrepancy occurs between formatted and raw logs when using GMT timezone.
1239748	Unable to delete Meta Variables with the following Error: The data is invalid for selected url.
1241163	After upgrading from 7.6.4 or earlier, users may encounter a blank GUI screen upon login if the ADOM flag value (flags) contains an incorrect value.
1241561	ADOM integrity check fails when running `diagnose cdb check adom-integrity`.
1244008	When FortiAnalyzer is added as a managed device in FortiManager, executing any of the "`diagnose cdb upgrade check`" commands may result in an unexpected behavior in the CLI.
1246091	FortiOS 7.4.10 partially supported by FortiManager 7.6.5/7.6.6. See the FortiManager 7.6.5/7.6.6 Release Notes for Compatibility Issues.
1247597	FortiManager is unable to sync user information from the pxGrid connector.
1251516	Installation failure occurs when pushing primus HSM (on-premises Hardware Security Module) settings via provisioning templates to FortiProxy.
1252855	ADOM upgrade from 7.4 to 7.6 may fail repeatedly during the dynamic_mapping copy phase with the error message: "unexpected input."
1255147	The fmg-admin is able to click both the text label and the toggle.
1256462	FortiClient fails to pull AV signatures from FortiManager acting as FDS server when receiving UM objects over HTTP.
1257065	FortiGuard subscription status shows unknown when trial license has expired.
1257789	Root ADOM upgrade fails when duplicate policy package names exist within a policy block.
1266515	When importing a custom firewall service definition through a FortiManager script that mixes the set protocol TCP/UDP/SCTP parameter with `set protocol-number <value>`, FortiManager allows the configuration without validation errors.
1268146	An error occurs when upgrading FortiManager due to password length limitations.
1284743	In an FortiGate HA setup running on a public cloud platform and managed by FortiManager, FortiManager may attempt to install or modify `vdom-exception` configurations, such as static routes. This may lead to issues during a failover event, including routes being deleted or other unexpected behavior.

Policy and Objects

Bug ID	Description
1101351	Unable to create ZTNA Server with SAML SSO Server.
1171027	NAT64 policy and CNAT cannot be created or modified in FortiManager.
1182465	Installation fails when FortiManager creates a default shaping-profile and binds it to an interface.
1189177	The FortiManager configuration attempted to change the order of custom service objects, but this returned an "Unknown action 0" error.
1194560	Missing CASB applications occur when FortiManager fetches casb application data without the 'get reserved' option.
1202792	The installation may fail with a "Current passphrase is invalid" error. This can occur when installing an SSID with an MPSK profile, where the MPSK passphrase is not inherited during copy operations or after a FortiManager upgrade.
1209756	Policy package installation fails for FGT-30G due to SSL VPN settings not supported by this FortiGate model.
1224582	FortiManager tries to delete access-proxy and all ZTNA-related configuration from the firewall.
1224598	The Policy Package Diff does not display any differences and throws an error.
1227209	Insert above or insert below fails when using ISDB objects in the policies.
1232760	Permit-stun-host configuration is not applied during installation when NAT is disabled.
1234646	FortiManager fails to display installation preview info. Preview stays blank with just a special character.
1235065	When loading an ssh cert, there is no password option and encrypted keys are not accepted.
1240260	When the Policy Package setting "Policy Offload Level" is set to Default mode, the Copy Policy Validation may fail and display an error log "COMMIT FAIL - invalid value".
1240764	Users may experience slowness when loading large policy packages while switching between Interface Pair views.
1242292	When configuring ISDB entries through the GUI, the default port value may be incorrectly applied, resulting in inaccurate port assignments within the configuration.
1242707	Policy package status does not change to "Out of Sync" on FortiManager when local changes are made on FortiGate.

1245964	In FortiOS 7.4.10, CLI syntax changes can cause install failures on low-memory (2GB) models when pushing configuration for:
	`web-proxy global proxy-fqdn`
	`firewall ssl-ssh-profile ssh`

Bug ID	Description
	For more details, please review the Special Notices in the FortiManager 7.6.5/7.6.6 Release Notes.
1247668	Importing firewall policies may fail when adding an FortiGate with a large number of policies (e.g., over 60K).
1249297	Policies disappear from policy block GUI when policy block name contains '/' character.
1252128	Firewall Policy object lists are auto-compressed when more than 3 objects per rule are present.
1255176	Policy package installation may stuck when dynamic mapping member of a "firewall addrgrp" is empty.
1257115	Policy package installation may fail on hardware devices when policy-offload-level is set to default.
1257828	Searching in Policy Packages/Policies with certain keywords may result in an unexpected error.
1258985	When disabling the HTTPS protocol under "Protocol Port Mapping" of any "SSL/SSH Inspection" profile, FortiManager tries to push the command "unset ports" which is not recognized by the FortiGate. As a result, the error "Must set at least one port or enable ssl inspect-all. ..."is generated during the Policy Package Installation.
1265850	When attempting to view "Where Used" for a url-filter list, the GUI continuously loads and does not return any results, even after several minutes.
1270583	Installation fails when FortiManager pushes an invalid limit for policing type shaping-profile.
1287157	GUI may crash when clicking Next in the Import Wizard before the Conflict Configuration table has fully loaded.
1287203	When attempting to view "Where Used" for a Web Content Filter, the GUI continuously loads and does not return any results, even after several minutes.

Revision History

Bug ID	Description
1248791	ADOM revision history may be lost when upgrading the ADOM to version 7.6.

Services

Bug ID	Description
1180123	FortiManager downloads and pushes full-version objects between FDS and FortiGate, which can result in high traffic usage.

System Settings

Bug ID	Description
1158131	The GUI permits configuring the management port to a port number already in use, resulting in loss of access to the GUI.
1235915	Trusted host configuration is not enforced when administrator accounts use SSH key authentication.
1238985	In a VRRP HA setup, the 3rd and 4th HA members may not properly synchronize with the master.
1257096	Policy package changes are unavailable to FortiManager-admins authenticated by Radius with ADOM scope and ext-auth-adom-override enabled.

VPN Manager

Bug ID	Description
1256324	Installation may fail after creating VPN communities of any type.
1262311	In a FortiManager 7.4 ADOM, attempts to create or retrieve SSL VPN web portal settings for FortiOS 7.4 devices may fail due to per-VDOM limit validation errors.

Known issues

Known issues are organized into the following categories:

- New known issues
- Existing known issues

To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

New known issues

The following issues have been identified in version 7.6.7.

Existing known issues

The following issues have been identified in a previous version of FortiManager and remain in FortiManager 7.6.7.

AP Manager

Bug ID	Description
1086946	The FortiAP upgrade via FortiManager may fail (on FortiGate 7.6.1). The process could stop at the controller_download_image step or experience a prolonged stall, eventually resulting in a timeout.

Others

Bug ID	Description
1143100	Unable to add physical FortiProxy to FortiManager.
1196043	Failed to create *Event Handlers* or *Reports* on FortiManager when a Fortinet Fabric Connection is established on FortiAnalyzer to connect to the FortiManager device. **Workaround**:

Bug ID	Description
	Go back to the specific ADOM on FortiAnalyzer and create the *Event Handlers* or *Reports* there. After synchronization, the new entries should become available on FortiManager.

1217534	During an upgrade of an FortiGate-HA cluster via FortiManager, if the disk-check feature is enabled, it may cause all cluster members to reboot simultaneously. This can result in an unexpected traffic interruption.
	Workaround:
	To prevent this issue, disable the disk check before performing the upgrade:
	`config fmupdate fwm-setting`
	`set check-fgt-disk disable`
	`end`

Policy and Objects

Bug ID	Description
1160047	Application control category "GenAI" is missing in FortiManager, but present in FortiGate. **Workaround**: Copy a FortiGate application list (Applist) from the CLI that includes Category 36, and insert it into a CLI template in FortiManager. Assign CLI template to FortiGate.
1200063	Failed to update EMS tags from EMS cloud server on FortiManager v7.6.x.

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 443 to communicate with the proxy server in *tunnel* mode by default. Alternatively, you can configure web proxy to use *proxy* mode using port 80. For more information, see the FortiManager Administration Guide.

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	VM License Activation
FortiGate	✓	✓	✓
FortiADC	✓		✓
FortiCache	✓		✓
FortiCarrier	✓	✓	✓
FortiClient	✓		
FortiDeceptor	✓	✓	✓
FortiDDoS	✓		✓
FortiEMS	✓		
FortiMail	✓	✓	✓
FortiProxy	✓	✓	✓
FortiSandbox	✓	✓	✓
FortiSOAR	✓		
FortiTester	✓		✓
FortiWeb	✓		✓
FortiPAM	✓		✓

Appendix B - Default and maximum number of ADOMs supported

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

Hardware models

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

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

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

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

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

Virtual Machines

For FortiManager VM, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.

- FortiManager-VM subscription licenses are fully stackable.

www.fortinet.com