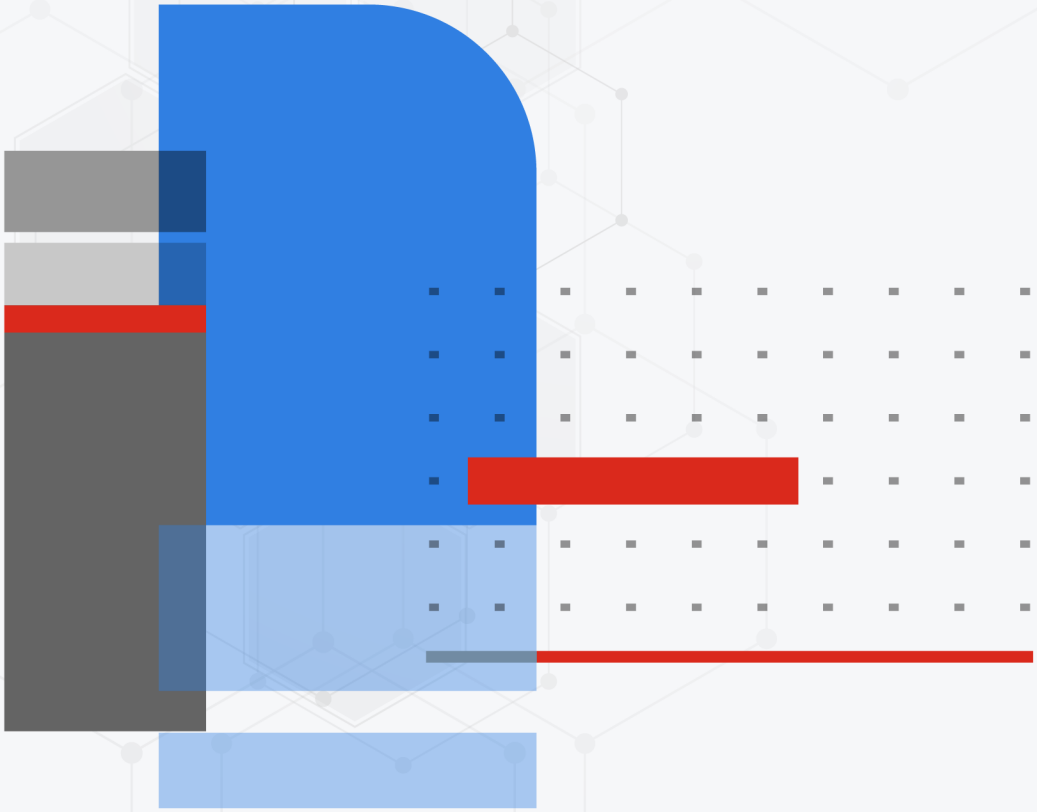
# Upgrade Guide

FortiManager 7.4.4



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

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

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

**FEEDBACK**
Email: techdoc@fortinet.com

September 17, 2024
FortiManager 7.4.4 Upgrade Guide
02-744-1067932-20240917

# TABLE OF CONTENTS


**Change Log** ..... **4**
**Introduction** ..... **5**
**Preparing to Upgrade FortiManager** ..... **6**
Disabling FortiAnalyzer Features ..... 6
Upgrading unsupported ADOMs ..... 7
Downloading files from Customer Service & Support ..... 8
Downloading release notes and firmware images ..... 8
Downloading MIB files for SNMP ..... 9
FortiManager firmware images ..... 10
FortiManager VM firmware images ..... 10
Build numbers ..... 10
Reviewing FortiManager 7.4.4 Release Notes ..... 11
Planning when to upgrade ..... 11
Installing pending configurations ..... 11
Reviewing status of managed devices ..... 11
CLI example of diagnose dvm adom list ..... 12
CLI example of diagnose dvm device list ..... 12
CLI example of diagnose dvm group list ..... 13
Checking FortiManager databases ..... 13
Reviewing FortiManager system resources and license information ..... 16
Backing up configuration files and databases ..... 17
Back up FortiGuard packages ..... 18
Creating a snapshot of VM instances ..... 18
**Upgrading FortiManager** ..... **19**
Upgrading FortiManager Firmware ..... 19
Upgrading the firmware for an operating cluster ..... 22
Checking FortiManager log output ..... 23
Checking FortiManager events ..... 23
Downgrading to previous firmware versions ..... 24
**Verifying FortiManager Upgrade Success** ..... **25**
Checking Alert Message Console and notifications ..... 25
Checking managed devices ..... 25
Previewing changes for a policy package installation ..... 26
**Supported Models** ..... **27**
**FortiManager Firmware Upgrade Paths** ..... **28**

# Change Log

| Date | Change Description |
| --- | --- |
| 2024-09-17 | Initial release of 7.4.4. |
| | |
| | |

# Introduction

This document describes how to upgrade FortiManager to 7.4.4. This guide is intended to supplement the *FortiManager Release Notes*, and it includes the following sections:


- Preparing to Upgrade FortiManager on page 6
- Upgrading FortiManager on page 19
- Verifying FortiManager Upgrade Success on page 25
- Supported Models on page 27
- FortiManager Firmware Upgrade Paths on page 28

Firmware best practice:

- Stay current on patch releases for your current major release.
- Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiManager Release Notes* on the Fortinet Document Library (https://docs.fortinet.com/), or contact Fortinet Customer Service & Support (https://support.fortinet.com/).
- Upgrade FortiManager before upgrading FortiOS, and be sure to maintain release version compatibility at all times.
  It is important to upgrade FortiManager before FortiOS to enable FortiManager to properly parse new FortiOS syntax.

# Preparing to Upgrade FortiManager

We recommend performing the following tasks to prepare for a successful upgrade of a FortiManager unit. Following is a summary of the preparation tasks and a link to the details for each task.

**To prepare for upgrading FortiManager (summary):**

1. If FortiAnalyzer Features are enabled on FortiManager in an HA cluster, you must disable FortiAnalyzer Features before upgrading FortiManager to version 7.4.4. See Disabling FortiAnalyzer Features on page 6.

   All log data is deleted during the upgrade. It is recommended to back up log data before starting the upgrade.
2. If FortiManager has ADOM versions that are unsupported in the target FortiManager version, upgrade all unsupported ADOM versions to 7.0 or higher.

   You cannot upgrade unsupported ADOM versions after upgrading to the target FortiManager version.

   *FortiManager* 7.4.0 and higher supports ADOM versions 7.0, 7.2, and 7.4. See Upgrading unsupported ADOMs on page 7.
3. Download release notes, firmware images, and SNMP MIB files. See Downloading files from Customer Service & Support on page 8.
4. Review release notes. See Reviewing FortiManager 7.4.4 Release Notes on page 11.
5. Plan when to perform the upgrade. See Planning when to upgrade on page 11.
6. Install pending configuration files. See Installing pending configurations on page 11.
7. Review the status of managed devices. See Reviewing status of managed devices on page 11.
8. Check the status of FortiManager databases. See Checking FortiManager databases on page 13.
9. Review FortiManager system resources and license information. See Reviewing FortiManager system resources and license information on page 16.
10. Back up configuration files and databases. See Backing up configuration files and databases on page 17.
11. Optionally, back up FortiGuard packages. See Back up FortiGuard packages on page 18.
12. Clone VM instances. See Creating a snapshot of VM instances on page 18.

## Disabling FortiAnalyzer Features

If FortiManager HA is disabled, you can skip this step by leaving FortiAnalyzer Features enabled.

With FortiManager 7.4.0, you cannot enable FortiAnalyzer Features on FortiManager nodes that are part of an HA cluster. If FortiAnalyzer Features are enabled on FortiManager nodes in an HA cluster before you upgrade to FortiManager 7.4.0, FortiAnalyzer Features are automatically disabled on each FortiManager in the HA cluster during upgrade.

After upgrade to FortiManager 7.4.0 completes, you cannot enable FortiAnalyzer Features on any FortiManager nodes that are part of an HA cluster, and the *FortiAnalyzer Features* option is hidden in the GUI.

This topic describes how to disable FortiAnalyzer Features before starting the upgrade.

**To disable FortiAnalyzer features:**

1. Back up log data.
   All log data is deleted during the upgrade. It is recommended to back up log data.
2. Go to *Dashboard*.
3. In the *System Information* widget, toggle *FortiAnalyzer Features* to *OFF*.
   FortiManager reboots to apply the change.

# Upgrading unsupported ADOMs

FortiManager 7.4.4 supports ADOM versions 7.0, 7.2, and 7.4.

Before upgrading FortiManager to 7.4.4, review what ADOM versions you are using, and compare them to the ADOM versions in following table. The following table identifies whether you must upgrade ADOM versions in FortiManager *before* upgrading FortiManager to 7.4.4:

| ADOM version before upgrade | ADOM version supported in FortiManager 7.4 | Action required before upgrading FortiManager |
|---|---|---|
| 6.4 | Not supported by FortiManager 7.4. | Before upgrading FortiManager to 7.4.4, upgrade ADOMs from 6.4 to 7.0.<br>You cannot upgrade unsupported ADOMs, such as 6.4, *after* upgrading FortiManager to 7.4.4. |
| 7.0 | Supported. ADOM can contain FortiGates running FortiOS 7.0 and 7.2. | No action required before upgrading FortiManager to 7.4.4. |
| 7.2 | Supported. ADOM can contain FortiGates running FortiOS 7.0, 7.2, and 7.4. | |

The global database ADOM supports its own version plus one version. For example, if the global database ADOM version is 7.2, the global database ADOM can manage version 7.2 and 7.4, but not 7.0.

If necessary, you should upgrade the global database ADOM *after* all the ADOMs that are using a global policy package have been upgraded.

See also *FortiManager Administration Guide > Global database version*.

Although each ADOM version supports FortiGates running multiple versions of FortiOS, it is recommended to use the same ADOM and FortiOS versions for optimal syntax support. For example, it is recommended to use ADOM version 7.0 for FortiGates running FortiOS 7.0.

The following procedure describes how to upgrade ADOM 6.4 to 7.0 by first upgrading all FortiGates to FortiOS 7.0 or later. Although this procedure is recommended, it is not required. You can upgrade ADOM 6.4 to 7.0 without first upgrading the FortiGates.

See also *FortiManager Administration Guide > Using mixed versions in ADOMs*.

**To upgrade ADOM version:**

1. In the older version ADOM, upgrade one of the FortiGate units to FortiOS 7.0 or later, and then resynchronize the device.
   All the ADOM objects, including Policy Packages, remain as objects for the earlier version.
2. Upgrade the remaining FortiGate units in the older version ADOMs to FortiOS 7.0 or later.
3. Upgrade the ADOM to version 7.0 or later.
   a. Ensure that you are logged into FortiManager as a super user administrator.
   b. Go to *System Settings* > *All ADOMs*.
   c. Select an ADOM, and then select *More* > *Upgrade* from the toolbar.
   d. Click *OK* in the confirmation dialog box to upgrade the ADOM.
   All the database objects are converted to the new version's format and the GUI content for the ADOM changes to reflect the new version's features and behavior.
4. If necessary, upgrade the Global database ADOM.

# Downloading files from Customer Service & Support

You can download release notes and firmware images from the Fortinet Customer Service & Support portal at https://support.fortinet.com. If you are using SNMP to monitor equipment, you can also download MIB files from the Fortinet Customer Service & Support portal.

This section contains the following topics:


- Downloading release notes and firmware images on page 8
- Downloading MIB files for SNMP on page 9
- FortiManager firmware images on page 10
- FortiManager VM firmware images on page 10
- Build numbers on page 10


## Downloading release notes and firmware images

Release notes are available for download from the Fortinet Customer Service & Support portal (https://support.fortinet.com/).

Firmware images can be downloaded from the following locations:

- FortiGuard: From FortiManager GUI, you can view the recommended firmware upgrade path, download the firmware from FortiGuard, and upgrade the firmware.
- Fortinet Customer Service & Support portal: Firmware images are organized by firmware version, major release, and patch release. You can download the firmware image, and then upload the firmware image to FortiManager GUI.

This section describes how to download firmware images from the Fortinet Customer Service & Support portal. For information about downloading firmware images from FortiGuard, see Upgrading FortiManager Firmware on page 19.

For information about the naming convention of firmware images and VM firmware images, see FortiManager firmware images on page 10, FortiManager VM firmware images on page 10, and Build numbers on page 10.

We recommend running an MD5 checksum on the firmware image file.

**To download release notes and firmware images for hardware:**

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiManager*.
4. Download the release notes for the 7.4.4 build:
   a. On the *Release Notes* tab, click the *7.4.4 Build <number>* link.
   The Document Library is displayed.
   b. Download the release notes.
5. Download the firmware image:
   a. Return to the Fortinet Customer Service & Support portal, and click the *Download* tab.
   b. Go to the *v7.00* > *7.4* > *7.4.4* folder, and locate the firmware image for your device or VM.
   c. Download the firmware image by clicking the *HTTPS* link.
   An HTTPS connection is used to download the firmware image.
   d. Click the *Checksum* link for the image that you downloaded.
   The image file name and checksum code are displayed in the *Get Checksum Code* dialog box.
   e. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

**To download firmware images for VM environments:**

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *VM Images*.
3. In the *Select Product* dropdown list, select *FortiManager*.
4. In the *Select Platform* list, select the platform.
5. Click the version.
   The firmware images for the selected product, platform, and version are displayed in the content pane.
6. Click *Download* for the *.out* file.
   The firmware image is downloaded to your computer.

## Downloading MIB files for SNMP

If you are not using SNMP to monitor equipment, you can skip this procedure.

If you are using SNMP to monitor equipment, download the following MIB file from the Fortinet Customer Service & Support portal:

- *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib*, which is used with both FortiManager and FortiAnalyzer

**To download SNMP MIB files:**

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiManager*.
4. Download the MIB file for the FortiManager 7.4.4 release:
   a. On the *Download* tab, go to the *v7.00* > *7.4* > *7.4.4* > *MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
   An HTTPS connection is used to download the file.

## FortiManager firmware images

The firmware images in the folders follow a specific naming convention, and each firmware image is specific to the device model or VM.

For example, the `FMG_2000E-v7.4.0-build****-FORTINET.out` image found in the */FortiManager/v7.00/7.4/7.4.0/* folder is specific to the FortiManager 2000E device model.

## FortiManager VM firmware images

Fortinet provides FortiManager VM firmware images for a number of virtualization environments.

Firmware images follow a specific naming convention, and each firmware image is specific to the VM environment. All firmware images for VM upgrades have filenames that end with `.out`.

For example, the `FMG_VM64_HV-v7-build2201-FORTINET.out` image is specific to upgrade for the Hyper-V platform.

For more information, see the FortiManager data sheet at https://www.fortinet.com/products/management/fortimanager.html.

VM installation guides are available in the Fortinet Document Library.

## Build numbers

Firmware images are generally documented as build numbers. New models may be released from a branch of the regular firmware release. As such, the build number found in the *Dashboard* > *System Information* widget and the output from the `get system status` CLI command displays this four-digit build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch Point` field that displays the regular build number.

Ensure that FortiManager 7.4.4 can run on your FortiManager model. See Supported Models on page 27.

# Reviewing FortiManager 7.4.4 Release Notes

After you download the release notes for FortiManager 7.4.4, review the special notices, upgrade information, product integration and support, resolved issues, and known issues.

# Planning when to upgrade

Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.

# Installing pending configurations

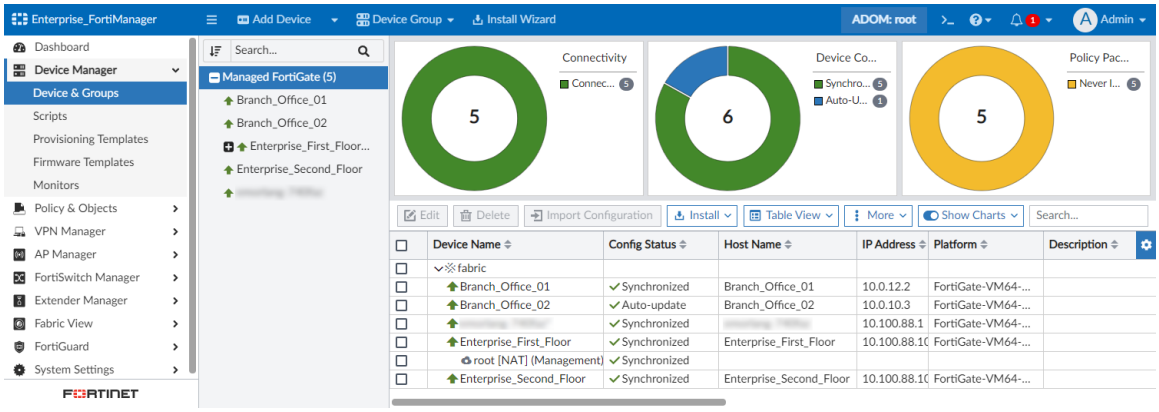
Prepare your device for upgrade by installing any pending configurations, and ensure that your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.

# Reviewing status of managed devices

Before starting an upgrade, use the *Device Manager* pane to review the status of all managed devices to ensure they have a status of *Synchronized*.

Either correct devices without a *Synchronized* status or make note of them prior to starting the upgrade.

Following is an example of the *Device Manager* pane:




Also, you can use the following CLI commands to gather detailed properties of managed devices, device groups, or ADOMs. The example output that follows highlights the important properties and attributes.

- `diagnose dvm adom list`
- `diagnose dvm device list`
- `diagnose dvm group list`

This section contains the following topics:


- CLI example of diagnose dvm adom list on page 12
- CLI example of diagnose dvm device list on page 12
- CLI example of diagnose dvm group list on page 13


## CLI example of diagnose dvm adom list

Following is an example of the CLI output for the `diagnose dvm adom list` command:

```
# diagnose dvm adom list
There are currently 26 ADOMs:
OID STATE PRODUCT OSVER MR NAME MODE VPN MANAGEMENT IPS
...
...
239 enabled FOS 5.0 4 54-ADOM Normal Policy & Device VPNs 10.00032 (regular)
141 enabled FOS 5.0 4 54-VPN Normal Central VPN Console 6.00741 (regular)
...
...
---End ADOM list---
```

The following properties should be the same before and after the upgrade:

- Total number of ADOMs.
- Name of each ADOM.
- VPN management mode. There are two VPN management modes: `Policy & Device VPNs` or `Central VPN Console`.

## CLI example of diagnose dvm device list

Following is an example of the CLI output for the `diagnose dvm device list` command:

```
# diagnose dvm device list
--- There are currently 16 devices/vdoms managed ---
TYPE            OID SN               HA IP         NAME    ADOM    IPS
...
...
fmg/faz enabled 448 FGVM020000058807 - 10.3.121.82 FGVM82 54-VPN 6.00741 (regular)
|- STATUS: db: modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:54-VPN pkg:[modified]pp_vpn_v1
fmg/faz enabled 317 FGVM02Q105060033 - 10.3.121.92 FGVM92 54-ADOM 6.00741 (regular)
|- STATUS: db: not modified; conf: out of sync; cond: unknown; dm: autoupdated; conn: down
|- vdom:[3]root flags:1 adom:54-ADOM pkg:[unknown]VM92_root
...
...
--- End device list ---
```

This command shows the total number of devices or VDOMs, the configuration status of devices and policy packages, and the connection status. The number of managed devices or VDOMs should be the same before and after the upgrade.

- If the device configuration or policy package status (`db`) is `modified`, we recommend installing the changes before upgrading.

- The policy package status (`pkg`) shows if there is any pending package change on a policy package that has been linked to a device or VDOM. This status can be `modified`, `never-installed`, or `unknown`.
- The connection status (`conn`) is either `up` or `down`.

### CLI example of diagnose dvm group list

Following is an example of the CLI output for the `diagnose dvm group list` command:

```
FMG-v54 # diagnose dvm group list
There are 2 groups:
OID  NAME          ADOM
277  FGT_Group1    54-VPN
+DEVICE oid=162 name=FGTVM93
278  FGT_Group2    54-VPN
+DEVICE oid=265 name=FGTVM94
---End group list---
```

The number of groups and their members should be the same before and after the upgrade.

## Checking FortiManager databases

Before upgrading, it is recommended that you check the integrity of FortiManager databases using the following CLI commands. If you find any errors, you can fix the errors before the upgrade.

- If you need to fix database errors, back up before making any changes. See Backing up configuration files and databases on page 17.
- Before running integrity check commands, ensure only one admin is logged in and no objects are locked.
- If workspace mode is enabled, you must unlock all ADOMs before running any integrity commands. For information on workspace mode, see the *FortiManager Administration Guide*.

### diagnose pm2 check-integrity all

Check the integrity of the Policy Manager database by using the following command:

```
diagnose pm2 check-integrity all.
```

The `diagnose pm2 check-integrity all` command only detects errors. It cannot correct errors. If any errors are found, the only option is to restore from the last good backup before upgrading.

**Example 1 with error:**

```
FMG-VM64 # diagnose pm2 check-integrity all
--- pragma integrity_check adom db ---
Error: database disk image is malformed
pragma integrity_check fails: /var/pm2/adom153
>>> total: 10 failed: 1
```

**Example 2 without error:**

```
FMG-VM64 # diagnose pm2 check-integrity all
--- pragma integrity_check adom db ---
--- total: 15 ok.
--- pragma integrity_check device db ---
--- total: 1 ok.
--- pragma integrity_check global db ---
--- total: 2 ok.
--- pragma integrity_check ips db ---
--- total: 3 ok.
--- pragma integrity_check task db ---
--- total: 1 ok.
--- pragma integrity_check ncmdb db ---
--- total: 18 ok.
```

## diagnose dvm check-integrity

Check the integrity of the Device Manager database by using the following command:

```
diagnose dvm check-integrity.
```

**Example 1 with error:**

```
FMG-VM64 # diagnose dvm check-integrity
[1/8] Checking object memberships ... correct
[2/8] Checking device nodes ... 0 change(s) will be made (263 error(s))
[3/8] Checking device vdoms ...
...
The above changes will be made to the database, however it is recommended to perform a
     backup first.
Do you want to continue? (y/n)
```

**Example 2 without error:**

```
FMG-VM64 # diagnose dvm check-integrity
[1/8] Checking object memberships       ... correct
[2/8] Checking device nodes              ... correct
[3/8] Checking device vdoms              ... correct
[4/8] Checking duplicate device vdoms    ... correct
[5/8] Checking device ADOM memberships   ... correct
[6/8] Checking groups                    ... correct
[7/8] Checking group membership          ... correct
[8/8] Checking task database             ... correct
```

## diagnose cdb check adom-integrity

Check the integrity of ADOM configurations in the database by using the following command:

```
diagnose cdb check adom-integrity.
```

This command does not work on version 5.4.3 or versions earlier than 5.2.11.

**Example 1 with error:**

```
FMG-VM64 # diagnose cdb check adom-integrity
General updating - adom FWF_LAB    ... ..100% Ready to update
General updating - adom FWF_Root   ... ..100% Ready to update
General updating - adom root       ... ..100% An error has occured: (errno=33):duplicate
If the update check returns an error, please contact Fortinet Support for assistance.
```

**Example 2 without error:**

```
FMG-VM64 # diagnose cdb check adom-integrity
General updating - adom FWF_Root     ... .......90%..100% Ready to update
General updating - adom FWF_ADOM_50  ... .......90%..100% Ready to update
General updating - adom FWF_ADOM_52  ... ...........90%..100% % Ready to update
General updating - adom root         ... ...100% Ready to update
```

## diagnose cdb check policy-packages

Check the integrity of the policy packages by using the following command:

```
diagnose cdb check policy-packages.
```

**Example 1 with error:**

```
FMG-VM64 # diagnose cdb check policy-packages
Adom VPNConsole
   [1/4] Checking Scope ... correct
   [2/4] Checking Dynamic mappings ... 2 change(s) will be made
   [3/4] Checking Policy package settings ... correct
   [4/4] Checking Undeleted objs ... correct
Adom root
   [1/4] Checking Scope ... correct
   [2/4] Checking Dynamic mappings ... correct
   [3/4] Checking Policy package settings ... correct
   [4/4] Checking Undeleted objs ... correct
The above change(s) will be made to the database, however it is recommended to perform a
     backup first.
Do you want to continue? (y/n)
```

**Example 2 without error:**

```
FMG-VM64 # diagnose cdb check policy-packages
Adom FG54
   [1/4] Checking Scope ... correct
   [2/4] Checking Dynamic mappings ... correct
   [3/4] Checking Policy package settings ... correct
   [4/4] Checking Undeleted objs ... correct
Adom root
   [1/4] Checking Scope ... correct
   [2/4] Checking Dynamic mappings ... correct
   [3/4] Checking Policy package settings ... correct
   [4/4] Checking Undeleted objs ... correct
```

### diagnose cdb upgrade check +all

Check the integrity of object configuration database, reference table, ADOM database, DVM database, and invalid policy package and template installation targets by using the following command:

```
diag cdb upgrade check +all
```

This command does not work on version 5.6.0 or earlier.

**Example**

```
FMG-VM64 # diag cdb upgrade check +all
Checking: Object config database integrity
No error found.

Checking: Reference table integrity
No error found.

Checking: Repair invalid object sequence
No error found.

Checking: Reassign duplicated uuid in ADOM database
No error found.

Checking: Resync and add any missing vdoms from device database to DVM database
No error found.

Checking: Invalid policy package and template install target
No error found.
```

## Reviewing FortiManager system resources and license information

Before starting an upgrade, go to *System Settings* to review the following widgets:

- License Information widget
- System Resources widget to check for high memory and CPU usage

It is also recommended to check the Alert Message Console widget in *System Settings* and the notifications in the toolbar.

**If you are upgrading a FortiManager VM:**

Make sure your VM partition has more than 1024MB and your VM server is up to date.

To view the flash disk size of your VM, enter the following command in the FortiManager CLI and review the value for the first hard disk (SDA):

```
diagnose system print partitions
```

For example:

```
diagnose system print partitions
   major minor #blocks name fstype
   1 0 4096 ram0
   1 1 4096 ram1
   1 2 4096 ram2
   1 3 4096 ram3
   7 0 10240 loop0 ext2
   8 0 2097152 sda
   8 1 1048576 sda1 ext3
   8 16 83886080 sdb
   8 32 1073741824 sdc
   253 0 1157619712 dm-0
```

You can increase the size by shutting down the VM, editing the VM hardware to increase the size of the first hard disk, and then restarting the VM.

For more information about FortiManager VM, see documentation for FortiManager Private Cloud and FortiManager Public Cloud.

# Backing up configuration files and databases

Back up the FortiManager configuration file and databases.

It is recommended that you create a system backup file and save this configuration to your local computer. The device configuration file is saved with a `.dat` extension.

It is also recommended that you verify the integrity of your backup file.

When the database is larger than 2.8 GB, back up the configuration file to an FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename of
     server> <username on server> <password> <crptpasswd>
execute backup all-settings scp <ip> <path/filename of server> <SSH
     certificate> <crptpasswd>
```

For more information, see the *FortiManager CLI Reference*.

**To back up your system configuration:**

1. Go to *Dashboard*.
2. In the *System Information* widget, locate *System Configuration* and click *Backup*. The *Backup System* dialog opens.
3. Click the *Backup Now* tab.
4. Enter and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.
5. Click *OK* and save the backup file on your local computer.

**To verify the integrity of a backup file:**

1. Back up your system configuration and save the backup file on your local computer.
2. Go to *System Settings* > *Event Log*.
3. Locate the system event that was logged as a result of the backup operation from the *Event Log* table. You may use

the *Add Filter* button from the toolbar above to simplify locating the logged event entry.

4. In the *Changes* column for the event log, note the MD5 checksum.

If the checksums match, then the backup process was successful.

# Back up FortiGuard packages

Optionally, you can back up your FortiGuard packages (for example, Web Filter or IPS). Creating a backup of FortiGuard packages allows you to re-import the packages in cases of upgrade failure where the FortiManager needs to be reset/formatted or downgraded to an earlier version. Without a backup, the packages will be downloaded from FortiGuard.

This is recommended in scenarios where FortiManager is acting as the FortiGuard Distribution Server (FDS) for managed devices operating in a closed network.

**To export FortiGuard packages:**

1. Go to *FortiGuard* > *Query Services* > *Receive Status* or *FortiGuard* > *Packages* > *Receive Status*.
2. Select the FortiGuard packages that you want to export.
3. Click *Export* in the toolbar.

You can find more information in exporting and importing FortiGuard packages in the FortiManager Administration Guide.

- Query service receive status
- Exporting packages
- Importing packages example
- Exporting Web Filter databases

# Creating a snapshot of VM instances

In VM environments, it is recommended to stop the VM instance and take a snapshot or clone of the VM instance before the upgrade. If there are issues with the upgrade, you can revert to the VM snapshot or clone.

Avoid taking snapshots when applications in the virtual machine are communicating with other computers.

# Upgrading FortiManager

You can upgrade FortiManager 7.2.0 or later to 7.4.4.

For other upgrade paths, see FortiManager Firmware Upgrade Paths on page 28.

For information about FortiManager support for FortiOS, see the FortiManager Compatibility chart in the Document Library at https://docs.fortinet.com/product/fortimanager/7.4.

It is important to upgrade FortiManager before FortiOS to enable FortiManager to properly parse new FortiOS syntax.

If you upgrade FortiOS before FortiManager, you can still upgrade FortiManager. After upgrading FortiManager, manually synchronize the configuration from the remote FortiGate to the FortiManager device configuration database by using the *Retrieve Config* option on *Device Manager > Device Dashboard > Configuration and Installation* widget. For more information, see the *FortiManager Administration Guide > Viewing configuration revision history* topic.

This section contains the following topics:


- Upgrading FortiManager Firmware on page 19
- Upgrading the firmware for an operating cluster on page 22
- Checking FortiManager log output on page 23
- Checking FortiManager events on page 23
- Downgrading to previous firmware versions on page 24

When upgrading firmware, all ADOMs (and Policy Package Versions, if ADOMs are disabled) remain at the same version after the upgrade. For information about upgrading ADOMs, see the *FortiManager Administration Guide*.

Upgrading the device firmware can trigger an SQL database rebuild. During the database rebuild, new logs are inserted into the database and can be viewed, but existing logs are not available until the rebuild is complete. The time required to rebuild the database depends on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

## Upgrading FortiManager Firmware

This section describes how to upgrade FortiManager firmware. You can use the following methods to upgrade firmware:

- From the FortiManager GUI, download the firmware from FortiGuard and upgrade the unit.
- From the FortiManager GUI, upload the firmware that you previously downloaded from the Customer Service & Support portal.

Fortinet recommends uploading firmware to FortiManager by using a server that is in the same location as the FortiManager. This helps avoid timeouts.

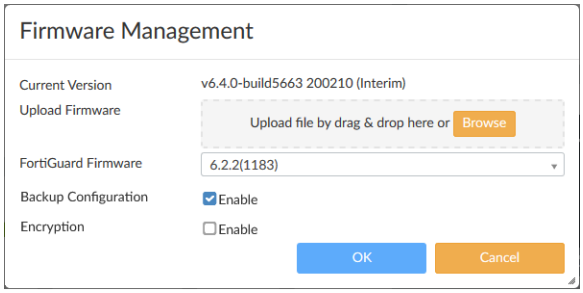
After updating FortiManager firmware, you should update the following items in the following order:

1. Update firmware for managed FortiGates.
2. Upgrade the ADOM version.
3. Upgrade the global ADOM version.

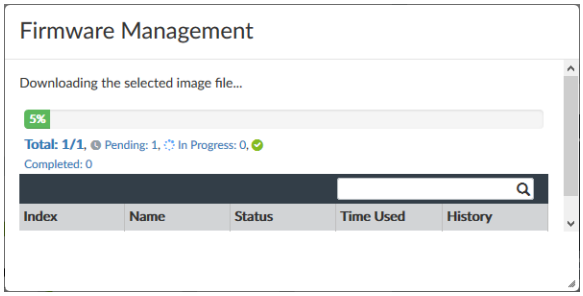
For information about updating firmware for FortiGates and ADOM versions, see the *FortiManager Administration Guide*.

**To upgrade firmware using FortiGuard:**

1. Go to *Dashboard*.
2. In the *System Information* widget, go to the *Firmware Version* field, and click the *Upgrade Firmware* icon.




3. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiManager configuration when performing a firmware upgrade. If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. In the *FortiGuard Firmware* list, select the version of FortiManager for upgrade, and click *OK*.
   The *FortiGuard Firmware* box displays all FortiManager firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiManager upgrade.
   If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.
   FortiManager downloads the firmware image from FortiGuard.

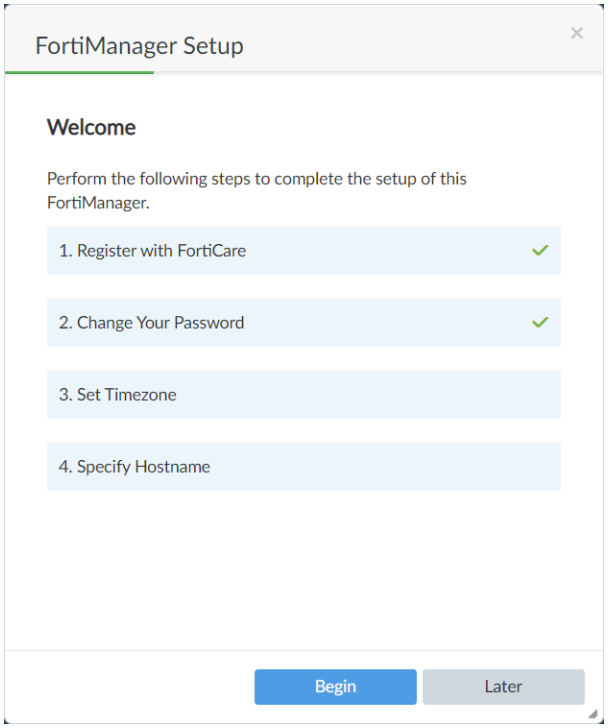



   FortiManager uses the downloaded image to update its firmware, and then restarts.
   It is recommended to view the console log output during upgrade. See Checking FortiManager log output on page 23.

5. When the login window displays, log into FortiManager.

   When the upgrade completes, you might have to refresh your web browser to see the login window.

   The *FortiManager Setup* wizard is displayed.




6. Click *Begin* to start the *FortiManager Setup* wizard.
   Alternately, you can click *Later* to complete the wizard later.
7. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiManager events on page 23.

**To upgrade firmware using an image downloaded from the Customer Service & Support portal:**

1. Go to *Dashboard*.
2. In the *System Information* widget, go to the *Firmware Version* field, and click the *Upgrade Firmware* icon.
3. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiManager configuration when performing a firmware upgrade. If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. In the *Firmware Upload* dialog box, click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal, and click *Open*.
5. Click *OK*.
   The firmware image is uploaded. When the upgrade completes, a message confirms a successful upgrade.
   It is recommended to view the console log output during upgrade. See Checking FortiManager log output on page 23.

6. When the login window displays, log into FortiManager.

When the upgrade completes, you might have to refresh your web browser to see the login window.

The *FortiManager Setup* wizard is displayed.

7. Click *Begin* to start the *FortiManager Setup* wizard.
   Alternately, you can click *Later* to complete the wizard later.
8. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiManager events on page 23.

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of
    server> <username on server> <password>
```

For more information, see the *FortiManager CLI Reference*.

# Upgrading the firmware for an operating cluster

You can upgrade the firmware of an operating cluster using the GUI or CLI of the primary unit.

Starting with FortiManager 7.0.0, FortiAnalyzer Features must be disabled when FortiManager HA is enabled. If you have FortiAnalyzer Features enabled on FortiManager, FortiAnalyzer Features will be automatically disabled during upgrade to FortiManager to 7.0.0 or later.

Similar to upgrading the firmware of a standalone unit, normal operations are temporarily interrupted during the cluster firmware upgrade. Therefore, you should upgrade the firmware during a maintenance window.

**To upgrade an HA cluster:**

1. Log into the GUI of the primary unit using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is automatically synchronized between the primary device and backup devices.
   It is recommended to view the console log output during upgrade. See Checking FortiManager log output on page 23.

Administrators may not be able to connect to the GUI until the upgrade synchronization process is completed. During the upgrade, SSH or telnet connections to the CLI may also be slow. You can still use the console to connect to the CLI of the primary device.

# Checking FortiManager log output

While upgrading a FortiManager unit, use the console to check the log output in real-time. Check for any errors or warnings.

Following is a sample console output with warnings or errors you might encounter during an upgrade:

```
Please stand by while rebooting the system.
Restarting system.
Serial number:FMG-VM0A11000137
Upgrading sample reports...Done.
Upgrading geography IP data...Done.
rebuilding log database (log storage upgrade)...
Prepare log data for SQL database rebuild...Done.
Global DB running version is 222, built-in DB schema version is 432
......
upgrading device ssl-vpn flags...done
upgrading scripts ...
Invalid schedule. The device 10160520 does not belong to script 136's adom
Invalid schedule. The device 33933609 does not belong to script 46's adom
Invalid schedule. The device 10515974 does not belong to script 46's adom
......
Invalid schedule. The device 1709397 does not belong to script 46's adom
Invalid schedule. The device 1709397 does not belong to script 46's adom
Invalid schedule. The device 1407292 does not belong to script 46's adom
upgrading scripts ... done
upgrading script log ...
Failed to upgrade some script logs. Please use "diagnose debug backup-oldformat-script-logs"
     to upload the failed logs into a ftp server
upgrading script log ... done
Upgrading adom vpn certificate ca ...
......
Finish check-upgrade-objects [32923/49325]
Upgrade all DB version ...
Global DB running version is upgraded to 432
Database upgrade finished, using 846m11s
```

# Checking FortiManager events

After upgrading, it is recommended to check all messages logged to the FortiManager Event Log. If you find any errors, you can fix the errors before continuing.

Following is an example of messages in the FortiManager Event Log:

| Date Time | Level | User | Sub Type | Message |
|---|---|---|---|---|
| 2017-09-20 11:37:21 | notice | | System manager event | Upgrade all DB version ... |
| 2017-09-20 11:37:21 | notice | | System manager event | Upgrading: Repair DVM device groups os_type |
| 2017-09-20 11:37:21 | notice | | System manager event | Upgrading: System Template SNMP upgrade |
| 2017-09-20 11:37:21 | notice | | System manager event | Finished, used 0m39s! |
| 2017-09-20 11:36:42 | notice | | System manager event | Upgrading: Refresh controller license count (for 5.6.0) |
| 2017-09-20 11:36:42 | notice | | System manager event | Upgrading: Dual mode support for VPN Manager |
| 2017-09-20 11:36:42 | notice | | System manager event | Upgrading: ADOM wtpid |
| 2017-09-20 11:36:42 | notice | | System manager event | Widget setting changed for Template default in ADOM 7_CMX_Chile. |
| 2017-09-20 11:36:41 | notice | | System manager event | Upgrading System Template widgets... |
| 2017-09-20 11:36:41 | notice | | System manager event | Deleting adomdb max_policy_id ... |

# Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release using the GUI or CLI, but this causes configuration loss. A system reset is required after the firmware downgrade. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

# Verifying FortiManager Upgrade Success

Once the upgrade is complete, check the FortiManager unit to ensure that the upgrade was successful. This section describes items you should check.

This section contains the following topics:


- Checking Alert Message Console and notifications on page 25
- Checking managed devices on page 25
- Previewing changes for a policy package installation on page 26


## Checking Alert Message Console and notifications

After the FortiManager upgrade completes, check the *Alert Message Console* and list of notifications for any messages that might indicate problems with the upgrade.

- In *Dashboard*, check the *Alert Message Console* widget.
- Click the Notification icon and review any notifications.

For information on accessing system settings, see Reviewing FortiManager system resources and license information on page 16.

## Checking managed devices

After the FortiManager upgrade completes, check the managed devices in the GUI.

**To check managed devices:**

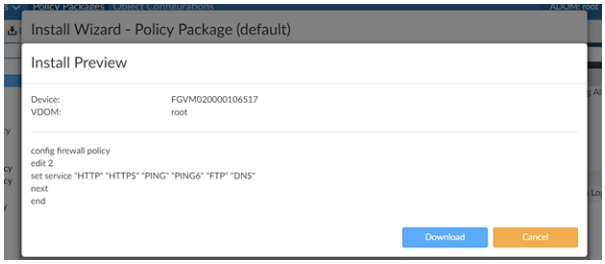
1. Refresh the browser and log back into the device GUI.
2. Go to *Device Manager*, and ensure that all formerly added devices are still listed.
3. In *Device Manager*, select each ADOM and ensure that managed devices reflect the appropriate connectivity state. It might take some time for FortiManager to establish connectivity after the upgrade.
4. Launch other functional modules and make sure they work properly.
   See Previewing changes for a policy package installation on page 26.

# Previewing changes for a policy package installation

The first time that you install a policy package after the upgrade, use the Install Preview feature to ensure that only the desired changes will be installed to the device.

The policy package must include a change to use the Install Preview feature.

Following is an example of the Install Preview pane:



# Supported Models

FortiManager version 7.4.4 supports the following models:

| FortiManager | FortiManager VM |
|---|---|
| FMG-200F | FMG_VM64 |
| FMG-200G | FMG_VM64_ALI |
| FMG-300F | FMG_VM64_AWS |
| FMG-400G | FMG_VM64_AWSOnDemand |
| FMG-410G | FMG_VM64_Azure |
| FMG-1000F | FMG_VM64_GCP |
| FMG-1000G | FMG_VM64_IBM |
| FMG-2000E | FMG_VM64_HV (including Hyper-V 2016, 2019, and 2022) |
| FMG-3000F | FMG_VM64_KVM |
| FMG-3000G | FMG_VM64_OPC |
| FMG-3100G | FMG_VM64_XEN (for both Citrix and Open Source Xen) |
| FMG-3700F | |
| FMG-3700G | |
| FMG-3900E | |

# FortiManager Firmware Upgrade Paths

The following table identifies the supported FortiManager upgrade paths. If you need information about upgrading to 6.4, 7.0, or 7.2 see the corresponding FortiManager Upgrade Guide.

As a best practice, it typically is recommended to upgrade to the latest patch version before upgrading to the next major version. For recommended upgrade paths from a specific version and model, see the Upgrade Path Tool Table on the Fortinet Document Library.

Before upgrading your device, see details in the applicable FortiManager Release Notes.

| Firmware Version | Build Number | Upgrade From |
|---|---|---|
| 7.4.4 | 2550 | 7.4.0-7.4.3<br>7.2.0-7.2.6 |
| **Note**: FortiManager 7.4 does not support ADOM versions 6.4 and earlier. FortiManager 7.4 supports only ADOM versions 7.0, 7.2, and 7.4. | | |
| 7.4.3 | 2487 | 7.4.0-7.4.2<br>7.2.0-7.2.6 |
| 7.4.2 | 2397 | 7.4.0-7.4.1<br>7.2.0-7.2.6 |
| 7.4.1 | 2308 | 7.4.0<br>7.2.0-7.2.6 |
| 7.4.0 | 2223 | 7.2.0-7.2.6 |
| 7.2.6 | 1632 | 7.2.0-7.2.5<br>7.0.1-7.0.12 |
| 7.2.5 | 1574 | 7.2.0-7.2.4<br>7.0.1-7.0.12 |
| 7.2.4 | 1460 | 7.2.0-7.2.3<br>7.0.1-7.0.12 |
| 7.2.3 | 1405 | 7.2.0-7.2.2<br>7.0.1-7.0.12 |
| 7.2.2 | 1334 | 7.2.0-7.2.1<br>7.0.1-7.0.12 |
| 7.2.1 | 1215 | 7.2.0<br>7.0.1-7.0.12 |
| 7.2.0 | 1124 | 7.0.1-7.0.12 |
| 7.0.12 | 0623 | 7.0.1-7.0.11<br>6.4.0-6.4.14 |

| Firmware Version | Build Number | Upgrade From |
|---|---|---|
| 7.0.11 | 0595 | 7.0.1-7.0.10<br>6.4.0-6.4.14 |
| 7.0.10 | 0561 | 7.0.1-7.0.9<br>6.4.0-6.4.14 |
| 7.0.9 | 0489 | 7.0.1-7.0.8<br>6.4.0-6.4.14 |
| 7.0.8 | 0452 | 7.0.1-7.0.7<br>6.4.0-6.4.14 |
| 7.0.7 | 0419 | 7.0.1-7.0.6<br>6.4.0-6.4.14 |
| 7.0.6 | 0372 | 7.0.1-7.0.5<br>6.4.0-6.4.14 |
| 7.0.5 | 0365 | 7.0.1-7.0.4<br>6.4.0-6.4.14 |
| 7.0.4 | 0306 | 7.0.1-7.0.3<br>6.4.0-6.4.14 |
| 7.0.3 | 0254 | 7.0.1-7.0.2<br>6.4.0-6.4.14 |
| 7.0.2 | 0180 | 7.0.1<br>6.4.0-6.4.14 |
| 7.0.1 | 0113 | 7.0.0<br>6.4.0-6.4.14 |
| 7.0.0 | 0047 | 6.4.0-6.4.14 |

See Supported Models on page 27 for the list of models that are supported in FortiManager 7.4.4.

Supported models for previous versions can be found in the FortiManager Release Notes for that version.

For information about FortiManager support for FortiOS, see the FortiManager Compatibility chart in the Document Library at https://docs.fortinet.com/product/fortimanager/7.4.

www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.