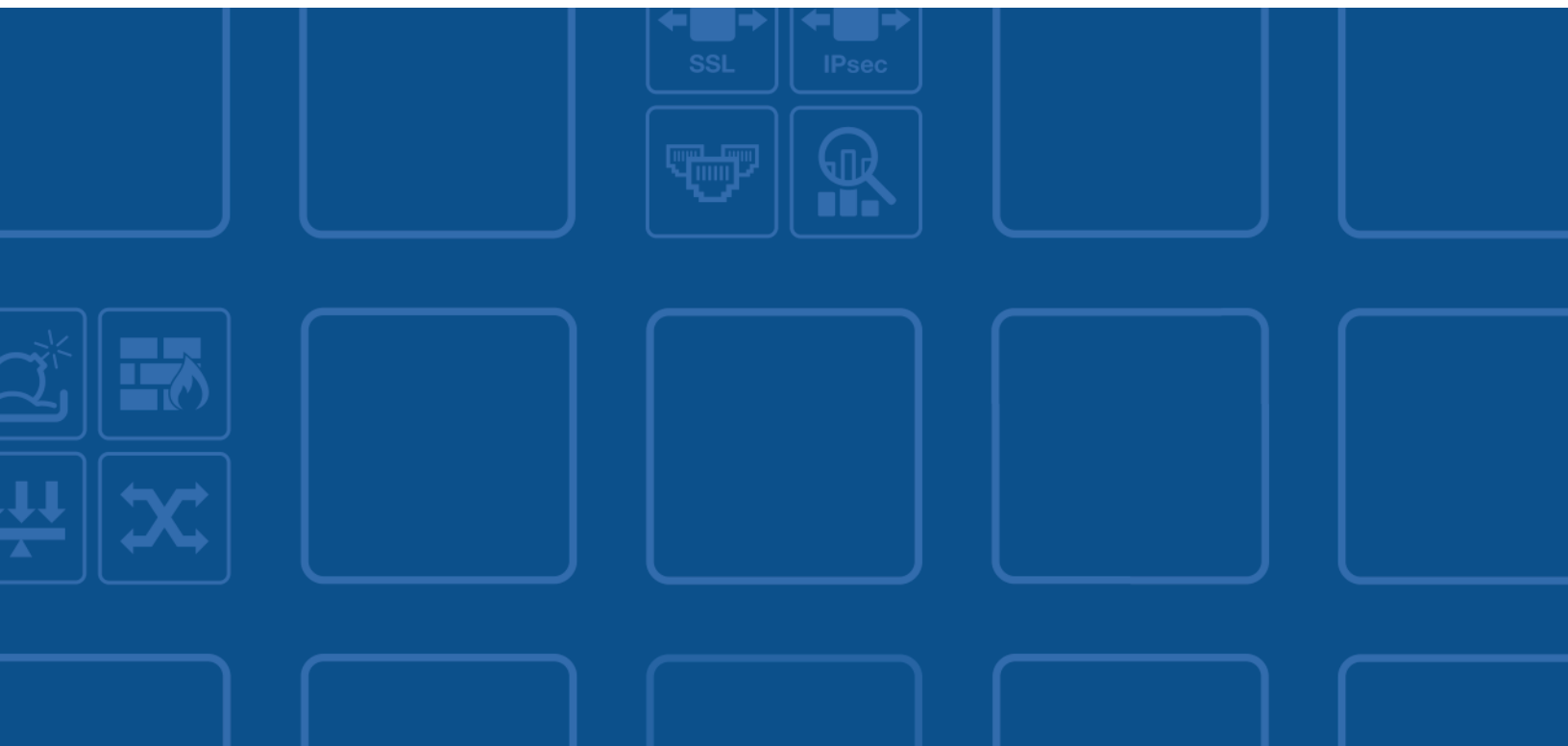
FORTINET
High Performance Network Security

FortiManager - Upgrade Guide

VERSION 5.4.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February 17, 2016

FortiManager 5.4.0 Upgrade Guide

02-540-308706-20160217

Change Log

Date	Change Description
2016-02-17	Initial Release.

FortiManager Firmware

This document provides an overview of FortiManager firmware and highlights general information you should be aware of prior to upgrading your device. This guide is intended to supplement the *FortiManager Release Notes* documentation.

The following topics are included in this section:

Best practices

Before any firmware upgrade complete the following:

- Download the firmware image and Release Notes document from the Fortinet Customer Service & Support portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your device for upgrade. Install any pending configurations, ensure your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file. 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.

In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

- 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.
- Once the upgrade is complete, test your device to ensure that the upgrade was successful and that all managed devices are listed.

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* or contact Fortinet Technical Support.

Upgrading the device firmware can trigger an SQL database rebuild. During this time, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Firmware image naming convention

Firmware images on the Fortinet Customer Service & Support portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the folders follow a specific naming convention and each firmware image is specific to the device model. For example, the FMG_300D-v500-build0310-FORTINET.out image found in the */FortiManager/v5.00.5.0/5.0.6/* file folder is specific to the FortiManager 300D device model.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

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

Citrix XenServer and Open Source XenServer

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

Linux KVM

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

Microsoft Hyper-V Server

- `.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.

VMware ESX/ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 32-bit or 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 product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

SNMP MIB download

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 v5.00 file folder.

Build numbers

Firmware images are generally documented as build numbers. New models may be released on a branch based off of the regular firmware release. As such, the build number found in the *System Settings* > *General* > *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.

Firmware upgrade and support information

Please also refer to the applicable releases notes for more details before upgrading your device.

Upgrade and support information

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.4.0	1019	5.2.0–5.2.4	5.4.0 5.2.0–5.2.6 5.0.4–5.0.12
Supported models: FMG-200D, FMG-300D, FMG-300E, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMG-VM64-KVM, FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.4	0738	5.2.0–5.2.3 5.0.6–5.0.10	5.2.0–5.2.4 5.0.4–5.0.10 4.3.2–4.3.8
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E,FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.3	0724	5.2.0–5.2.2 5.0.6–5.0.10	5.2.0–5.2.4 5.0.4–5.0.10 4.3.2–4.3.8
Supported models:FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.2	0706	5.2.0–5.2.2 5.0.6–5.0.10	5.2.0–5.2.3 5.0.4–5.0.10 4.3.2–4.3.8
Supported models: FMG-100C, FMG-200D, FMG-200E, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D,FMG-4000E, FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMGVM64-KVM. FMG-VM64-AWS, and FMG-VM64-HV.			
5.2.1	0662	5.2.0 5.0.8, 5.0.9	5.2.0–5.2.2 5.0.4–5.0.10 4.3.2–4.3.8
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.2.0	0618	5.0.6– 5.0.9	5.2.0, 5.2.1 5.0.4–5.0.9 4.3.2–4.3.8
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-4000D, FMG-4000E, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.9	0345	5.0.6–5.0.8	5.2.0, 5.2.1 5.0.4–5.0.10 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.8	0329	5.0.6, 5.0.7	5.2.0, 5.2.1 5.0.4–5.0.10 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.7	0321	5.0.6	5.2.0, 5.2.1 5.0.4–5.0.9 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.6	0310	5.0. or later 4.3.0 or later	5.0.4–5.0.7 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-4000E is released on build 4046.			

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.0.	0266	5.0. or later 4.3.0 or later	5.0.4, 5.0. 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.4	0232	5.0. or later 4.3.0 or later	5.0.4 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.3	0200	5.0. or later 4.3.0 or later	5.0.3 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D,FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-VM64-HV is released on build 0200. FMG-1000D is released on build 4035.			
5.0.2	0151	5.0. or 5.0.1 4.3.0 or later	5.0.2 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-400D, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4020. FMG-4000D is released on build 4019.			
5.0.1	0121	5.0.0 4.3.0 or later	5.0.1 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4009.			

Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.0.0	0076	4.3.0 or later	5.0.0 4.3.2–4.3.8 4.2.0–4.2.15
Supported models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			

In version 5.0, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS version 5.0. or later.

For more information, see the *Device and Client Reputation for FortiOS 5.0 Handbook* available in the Fortinet Document Library.

FortiManager version 5.0. introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to version 5.0. or later, a backup must be made and then the disk must be reformatted with following command:

```
execute format {disk | disk-ext4 | disk-ext3}
```

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The device will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services.

Upgrade Information

Upgrading to FortiManager 5.4.0

You can upgrade FortiManager 5.2.0 or later directly to FortiManager 5.4.0.

If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiManager 5.2 first (we recommend that you upgrade to 5.2.4, the latest version of FortiManager 5.2). For information about upgrading to FortiManager 5.2, see FortiManager 5.2.4 upgrade guide.

Upgrading FortiManager Firmware

The following table lists the firmware upgrade steps.

Upgrade steps

Step 1	Prepare your device for upgrade.
Step 2	Backup your system configuration.
Step 3	Transfer the firmware image to your device.
Step 4	Log into the GUI to verify the upgrade was successful.

Step 1: Prepare your device for upgrade

1. Install any pending configurations.
2. Make sure all managed devices are running the supported firmware versions as stated in the *Firmware Release Notes*.
3. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
4. Select *Download* from the toolbar and select *Firmware Images* from the drop-down list.
5. Select *FortiManager* from the drop-down list and select the *HTTPS Download* tab. Alternatively, you can select *FTP Download*. FTP is not an encrypted file transferring protocol and HTTPS download is recommended. The image folders are displayed.
6. Browse to the appropriate file folder to download the firmware image (`.out`) and Release Notes document.
7. Select an image in the list to download the firmware image to your management computer.
8. To verify the integrity of the download, select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.
9. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Backup your system configuration

1. Go to *System Settings* > *Dashboard*.
2. Select *Backup* in the *System Information* widget. The *Backup* dialog box opens.
3. Select the check box to encrypt the backup file and enter a password.
4. Select *OK* and save the backup file on your local computer.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the device.

Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename save to the
    server> <username on server> < password> <crptpasswd>

execute backup all-settings scp <ip> <path/filename save to the server>
    <SSH certificate> <crptpasswd>
```

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

Step 3: Transfer the firmware image to your device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*. The *Firmware Upgrade* dialog box opens.
3. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK*. Your device will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.

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*.

Step 4: Log into the Web-based Manager to verify the upgrade was successful.

1. Refresh the browser and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings* > *All ADOM*s.
4. Launch other functional modules and make sure they work properly.

Upgrading the firmware for an operating cluster

You can upgrade the firmware of an operating cluster through the Web-based Manager or CLI of the primary unit.

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 a HA cluster:

1. Log into the Web-based Manager 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.

Administrators may not be able to connect to the Web-based Manager 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.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

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

FORTINET®

High Performance Network Security