FortiManager - Upgrade Guide

VERSION 5.2.9

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

September 21, 2016

FortiManager 5.2.9 Upgrade Guide

02-529-388410-20160921

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-09-21	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.
- Back up 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 a three-digit build number. 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 three-digit build number.

Supported models

FortiManager version 5.2.9 supports the following models:

FortiManager	FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).

For more information about supported versions and models as well as product integration, refer to the *FortiManager5.2.9 Release Notes*.dled. Note bulb icon - text middled. Note bulb icon - text middled. Note bulb icon - text middled. Note bulb icon - text middled.

Upgrade Information

Upgrading to FortiManager 5.2.9

You can upgrade FortiManager 5.0.6 or later and 5.2.0 or later directly to FortiManager 5.2.9.

If you upgrade from versions earlier than FortiManager 5.0.6, you need to upgrade to 5.0.6 first.

FortiManager 5.0.7 or later has resized the flash partition storing system firmware. If your FortiManager is running 5.0.6, you will need to change the hard disk provisioned size to more than 512 MB in your VM environment before powering on the FortiManager VM. The secondary firmware and System Settings stored in the partition is lost after upgrade. Please reconfigure System Settings as needed.

Firmware upgrade steps

The following table lists the firmware upgrade steps.

Upgrade steps

Step 1	Prepare your device for upgrade.
Step 2	Back up 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. In the toolbar, click *Download* > *Firmware Images*.
5. From the *Select a Product* list, select *FortiManager*, and click the *Download* tab.
6. Click the *5.00* folder, and browse to the folder for version 5.2.9.
7. From the list, click the HTTPS link beside the image for your FortiManager model to download the firmware image to your management computer.

You can verify the integrity of the download by clicking *Download* in the toolbar, then select *Firmware Image Checksums* from the drop-down menu.

8. Enter the file name of your firmware image file, then click *Get Checksum Code*.

Step 2: Back up your system configuration

1. Go to *System Settings* > *Dashboard*.
2. Click *Backup* in the *System Information* widget. The *Backup* dialog box opens.
3. Select the checkbox to encrypt the backup file and enter a password.
4. Click *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 back up 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, go to the *Firmware Version* field, and click *Update*. The *Firmware Upgrade* dialog box opens.
3. Click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal, then select *Open*.
4. Click *OK*. The firmware image will be downloaded to your device 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 back in to FortiManager GUI and verify the following:

1. Database rebuild is successful. Use this CLI command to check database rebuild:
   `diag sql status rebuild-db`
2. Configurations are not lost.
3. Go to *Device Manager* of each ADOM, and make sure all the devices that were added before upgrade are still listed. You can also get an overview of the status of all the devices under *System Settings* > *All ADOMs*.
4. Check 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 in the same way as upgrading the firmware of a standalone unit. During the firmware upgrade procedure, you connect to the primary unit GUI or CLI to upgrade the firmware.

Similar to upgrading the firmware of a standalone unit, normal operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a maintenance window.

To upgrade an HA cluster:

1. Log into the primary unit GUI using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is synchronized between the primary device and backup devices.
3. Administrators may not be able to connect to the Web-based Manager until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

Downgrading to previous firmware versions

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

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