FortiAnalyzer - Upgrade Guide

VERSION 5.6.0

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

August 01, 2017

FortiAnalyzer - Upgrade Guide

05-560-404544-20170801

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-27	Initial release.
2017-08-01	Added a caution to *Upgrade Instructions* > *Preparing FortiAnalyzer for upgrade* > *ESX VM networks*.

Upgrade Paths

You can upgrade FortiAnalyzer 5.4.0 or later directly to FortiAnalyzer 5.6.0.

If you are upgrading from versions earlier than 5.4.0, you must upgrade to FortiAnalyzer 5.4 first. (We recommend that you upgrade to the latest version of FortiAnalyzer 5.4.) For information about upgrading to FortiAnalyzer 5.4, see the corresponding *FortiAnalyzer 5.4.x Upgrade Guide*.

The following table identifies the supported FortiAnalyzer upgrade paths and whether the upgrade requires a rebuild of the log database.

Initial Version	Upgrade To	Log Database Rebuild Occurs?
5.4.0 or later	5.6.0	Yes
5.2.0 or later	5.4.0 or later	Yes
5.0.6 or later	5.2	Yes for 5.0.6, No for the rest

FortiGate units with logdisk will buffer log data while FortiAnalyzer units are rebooting. In most circumstances, the amount of buffering is sufficient to cover the time need for FortiAnalyzer to reboot. However, Fortinet still recommends configuring multiple log destinations to help ensure that no logs are lost.

See also:

- Upgrade Policies for Log Storage on page 10
- Supported Models on page 12.

Fortinet Security Fabric

If you are upgrading the firmware for a FortiAnalyzer unit that is part of a FortiOS Security Fabric, you should be aware of how the FortiOS Security Fabric upgrade affects the FortiAnalyzer upgrade. You must upgrade the products in the Security Fabric in a specific order. For details, see the *FortiOS 5.6.0 Security Fabric Upgrade Guide* posted on the Document Library at http://docs.fortinet.com/fortigate/release-information.

Upgrade Instructions

This section provides an overview of how to upgrade a FortiAnalyzer unit followed by the detailed upgrade instructions.

Overview

To upgrade FortiAnalyzer (overview):

1. Prepare FortiAnalyzer for upgrade:
    - **a.** Ensure that FortiAnalyzer 5.6.0 can run on your FortiAnalyzer model.
    - **b.** Back up your device configuration and logs.
    - **c.** Wait until all the running reports are completed.
    - **d.** If you are upgrading a FortiAnalyzer VM, ensure that your VM partition has enough space and your VM server is update to date.

    For details, see Preparing FortiAnalyzer for upgrade on page 6.

2. Download upgrade images from Fortinet Customer Service & Support portal at https://support.fortinet.com. See Downloading upgrade images on page 7.
3. Upgrade FortiAnalyzer and monitor the upgrade. See Upgrading FortiAnalyzer and monitoring the upgrade on page 7.
4. Verify the upgrade has been completed successfully. See Verifying upgrade success on page 8.

Preparing FortiAnalyzer for upgrade

⚠

In FortiAnalyzer 5.6.0 and later, Fortinet changed the network interface mapping for ESX VM networks as shown below. After upgrading to FortiAnalyzer 5.6.0, you must edit ESX VM network mapping in order to preserve network connectivity.

- port1 -> Network Adapter 1
- port2 -> Network Adapter 2
- port3 -> Network Adapter 3
- port4 -> Network Adapter 4

New FortiAnalyzer 5.6.0 VM installations use the correct mapping with ESX 5.5 and later.

To prepare FortiAnalyzer for upgrade:

1. Ensure that FortiAnalyzer 5.6.0 can run on your FortiAnalyzer model.

    For a list of FortiAnalyzer models that support FortiAnalyzer 5.6.0, see Supported Models on page 12.

2. Back up your device configuration and logs:

   a. Go to *System Settings > Dashboard*.
   b. In the *System Information* widget, go to *System Configuration*, and click the *Backup* link.
   c. In the *Backup* dialog box that opens, select the *Encryption* check box to enable encryption; enter and confirm the password.
   d. Click *OK* and save the backup file to your management computer.

   If you have a FortiAnalyzer VM, you can take a VM snapshot instead.

3. Wait until all the running reports are completed. Use the following CLI commands to check for running and pending reports.

   ```
   FAZ1000D # dia report status running
   ```

   ```
   FAZ1000D # dia report status pending
   ```

4. If you are upgrading a FortiAnalyzer VM, make sure your VM partition has more than 512MB*, and your VM server is up to date.

   * We recommend that you allocate 1024MB for the FortiAnalyzer VM partition.

Downloading upgrade images

You can download the firmware image and Release Notes for FortiAnalyzer 5.6.0 from Fortinet Customer Service & Support portal at https://support.fortinet.com.

It is recommended to run an MD5 checksum on the file.

Upgrading FortiAnalyzer and monitoring the upgrade

For the Collector-Analyzer architecture upgrade, Fortinet recommends upgrading the Analyzer first. Upgrading the Collector first could impact the Analyzer’s performance.

When upgrading from FortiAnalyzer 5.4.0 or 5.4.1 to 5.6.0, reboot FortiAnalyzer 5.4.0 or 5.4.1 before installing the firmware image for FortiAnalyzer 5.6.0.

To install the firmware upgrade:

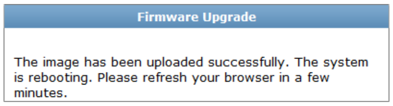
1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, go to the *Firmware Version* field, and click the *Upgrade Firmware* icon.

   The *Firmware Upload* dialog box is displayed.

3. Click *Browse* and browse to the firmware package (.out file) that you downloaded to the management computer.
4. Click *OK*.

   The firmware image is uploaded.

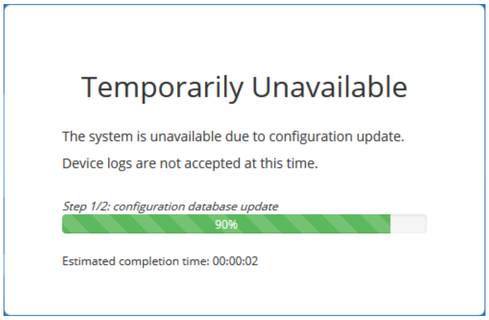
5. When you see the following system message, clear the cache of your web browser and keep refreshing the web page.



Firmware Upgrade

The image has been uploaded successfully. The system is rebooting. Please refresh your browser in a few minutes.

The FortiAnalyzer GUI and the system temporarily unavailable message are displayed.



Temporarily Unavailable

The system is unavailable due to configuration update.

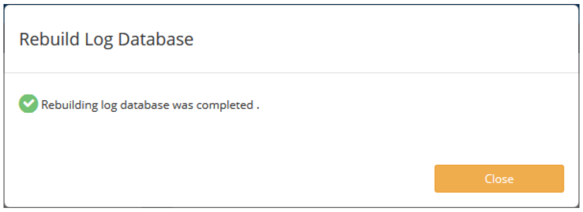
Device logs are not accepted at this time.

Step 1/2: configuration database update

Estimated completion time: 00:00:02

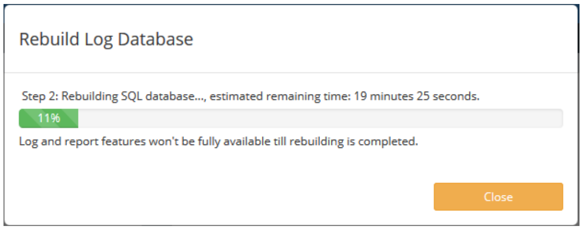
6. When the *Login* window is displayed, log into FortiAnalyzer.
7. Select an ADOM if ADOMs are enabled.
8. If the database is rebuilding, double-click the *Rebuilding DB* status that is displayed on the toolbar to open it.
9. Monitor the rebuild status. The rebuild process consists of two steps.

   Eventually, the *Rebuilding log database was completed* message is displayed.



Rebuild Log Database

✓ Rebuilding log database was completed .



Rebuild Log Database

Step 2: Rebuilding SQL database..., estimated remaining time: 19 minutes 25 seconds.

Log and report features won't be fully available till rebuilding is completed.

Not all the features are available while the SQL database is being rebuilt.

Verifying upgrade success

You can use the following procedure to verify that the FortiAnalyzer upgrade to 5.6.0 was completed successfully.

To verify the upgrade process:

1. If a database rebuild occurred, verify that database rebuild was successful by using the following CLI command:

```
diag sql status rebuild-db
```

2. Verify that configurations were not lost.
3. Launch the *Device Manager* pane and ensure that all the log devices that were previously added are still listed.
4. Launch other functional modules and make sure they work properly.

By default, the SQL database is disabled for the Collector mode in 5.4 and later to optimize performance. For a Collector with the SQL database enabled, the SQL database will be disabled after upgrade. You can re-enable the SQL storage settings to view logs and analytics with the following CLI command:

```
config system sql
set status local
end
```

Upgrade Policies for Log Storage

This section describes how the upgrade from FortiAnalyzer 5.2.x to 5.4.0 and later affects the disk allocation policy and the data retention policy.

This section applies only when upgrading FortiAnalyzer 5.2.x to 5.4.0 and later because log storage policies changed in FortiAnalyzer 5.4.0.

Disk space allocation policy

For FortiAnalyzer 5.2 and earlier, disk space is allocated per device. Starting in FortiAnalyzer 5.4, disk space can be allocated per ADOM. Following is the policy governing disk space allocation when FortiAnalyzer is upgraded from 5.2 to 5.4.0 and later.

Normal ADOM mode

For FortiAnalyzer working in the Normal ADOM mode, after upgrade to 5.4.0 and later, the ADOM for each managed device (with or without VDOMs) will get the disk space of the device before upgrade, plus 10% extra.

For example, a FortiGate device was allotted 30 GB in 5.2. After upgrade to FortiAnalyzer 5.4.0 and later, 33G (30G + 10% of 30G) will be allocated to the ADOM of this FortiGate device.

Advanced ADOM mode

For FortiAnalyzer working in the Advanced ADOM mode, after upgrade to 5.4.0 and later, the disk space of the device will be split among its VDOMs of different ADOMs, proportional to the log distribution across the VDOMs. Each ADOM will also get 10% extra.

For example, the disk quota for Device-A is 10GB in 5.2. Device-A consists of three VDOMs: root VDOM (the management VDOM), VDOM1, and VDOM2, which are assigned to ADOM root, ADOM1, and ADOM2 respectively.

During the upgrade, FortiAnalyzer calculates that 10% of Device-A log files are from root VDOM, 30% from VDOM1, and 60% from VDOM2. Accordingly, FortiAnalyzer will assign 1.1GB (1GB + 10% of 1GB) to ADOM root, 3.3GB (3GB + 10% of 3GB) to ADOM1, and 6.6GB (6GB+ 10% of 6GB) to ADOM2.

Additional policies

When the content files of the device, including DLP (data leak prevention) files, antivirus quarantine files, and IPS (intrusion prevention system) packet captures, use more than 40% of its disk quota, FortiAnalyzer will add some extra space to the device.

ADOM disk quota is recommended to be at least 1GB in 5.4. If the disk quota of a device is smaller than 1GB before upgrade to 5.4.x, the ADOM quota for the device will be adjusted to 1GB after upgrade to 5.4.x.

This adjustment could cause the total allocated disk space to oversize the actual device disk space. You can use the CLI command `diag log dev` to verify. You can always adjust the disk space back to smaller than 1GB if necessary.

Data retention policy

This section describes how the upgrade from FortiAnalyzer 5.2.x to 5.4.0 and later affects the data retention policy for existing and new ADOMs.

Existing ADOMs

For existing ADOMs, both Archive logs and Analytics logs are kept for 365 days + the age in days of the oldest Archive/Analytics logs respectively. For example, the oldest Archive logs of a device were generated on February 1st, 2016, and the oldest Analytics logs were generated on March 1st, 2016. Today is April 7th. So the oldest Archive logs are 67-days old, and the oldest Analytics logs are 38-days old. After upgrade to 5.4.0 and later, FortiAnalyzer will keep the Archive logs for 365+67=432 days, and keep the Analytics logs for 365+38=403 days.

New ADOMs

For newly created ADOMs, Archive logs are kept for 365 days, and Analytics logs are kept for 60 days.

Supported Models

FortiAnalyzer version 5.6.0 supports the following models:

FortiAnalyzer	FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.
FortiAnalyzer VM	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.