FORTINET

High Performance Network Securit

FortiAnalyzer Upgrade Guide

Version 5.4.1

Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 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.

1

Overview

STEP 1: Before you begin

Make sure FortiAnalyzer 5.4.1 can run on your FortiAnalyzer model. Back up your device configuration and logs. Wait until all the running reports are completed.

STEP 2: Download

Download upgrade images from Fortinet Customer Service & Support portal.

STEP 3: Upgrade and monitor

Install the new firmware and monitor if a rebuild occurs.

STEP 4: Verify

Verify the upgrade has been completed successfully.

More Information

Upgrading from 5.2 to 5.4: Disk space allocation policy

Upgrading from 5.2 to 5.4: Data retention policy

Supported Models

2

Upgrade Paths

You can upgrade FortiAnalyzer 5.2.0 or later directly to FortiAnalyzer 5.4.1.

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

Upgrade paths

Initial Version	Upgrade To	Log Database Rebuild Occurs?
5.4.0	5.4.1	No
5.2.0 or later	5.4.1	Yes
5.0.6 or later	5.2	Yes for 5.0.6, No for the rest

3

Detailed Upgrade Instructions

Step 1. Before you begin

- Make sure FortiAnalyzer 5.4.1 can run on your FortiAnalyzer model. For a list of FortiAnalyzer models that support FortiAnalyzer 5.4.1, see “Supported Models” on page 14.
- Back up your device configuration and logs. See “To back up device configuration” on page 8.
- 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
```

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

To back up device configuration:

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

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

Step 2. Download

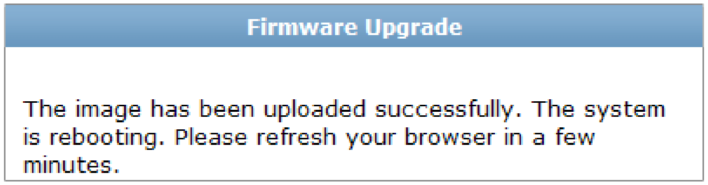
You can download the firmware image and Release Notes from Fortinet Customer Service & Support portal at https://support.fortinet.com.

Step 3. Upgrade and monitor

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

To install the firmware upgrade:

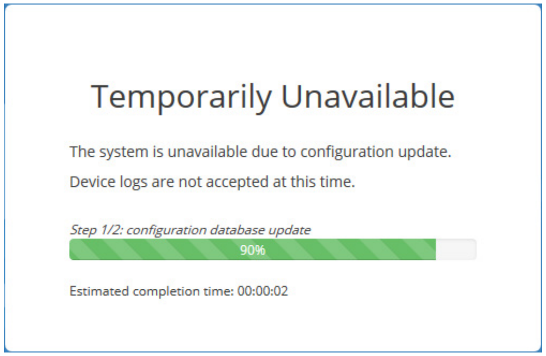
1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, go to the *Firmware Version* field, and click the *Upgrade Firmware* icon.
3. In the *Firmware Upload* dialog box that opens, click *Browse* and browse to the firmware package (.out file) that you downloaded to the management computer.
4. Click *OK*. Your device will start uploading the firmware image.
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.

You will then see the FortiAnalyzer user interface and the system temporarily unavailable message.



Temporarily Unavailable

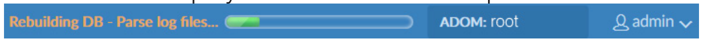
The system is unavailable due to configuration update.

Device logs are not accepted at this time.

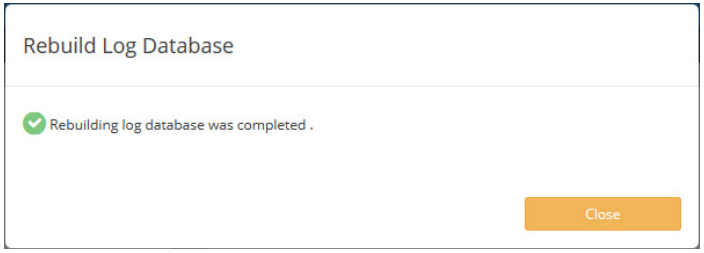
Step 1/2: configuration database update

Estimated completion time: 00:00:02

6. Once the Login window is displayed, log into FortiAnalyzer.
7. Select an ADOM if ADOM is enabled.
8. If the database is rebuilding, double-click the *Rebuilding DB* status that is displayed on the toolbar to open it.

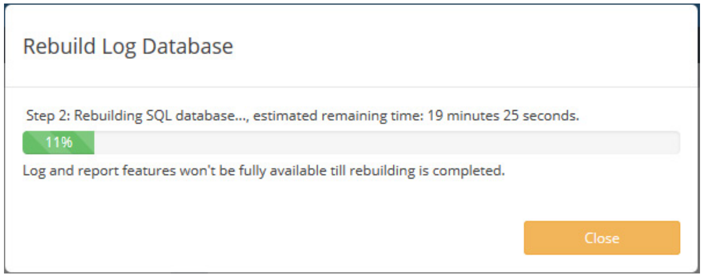


9. Monitor the rebuild status. The rebuild process consists of two steps. Eventually, you will see the “Rebuilding log database was completed“ message.



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.

Step 4. Verify

Verify the following to make sure the upgrade has been completed successfully.

1. Database rebuild is successful, if a rebuild occurred. Use this CLI command to check database rebuild:

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

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

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

By default, the SQL database is disabled for the Collector mode in 5.4 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
```

Upgrading from 5.2 to 5.4: Disk space allocation policy

For FortiAnalyzer 5.2 and earlier, disk space is allocated per device. Starting in 5.4, disk space is allocated per ADOM.

Here is the policy governing disk space allocation when FortiAnalyzer is upgraded from 5.2 to 5.4.

- For FortiAnalyzer working in the *Normal ADOM mode*: After upgrade to 5.4, 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 5.4, 33G (30G + 10% of 30G) will be allocated to the ADOM of this FortiGate device.
- For FortiAnalyzer working in the *Advanced ADOM mode*: After upgrade to 5.4, 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.
- 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, the ADOM quota for the device will be adjusted to 1GB after upgrade to 5.4.
  Note: 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.

Upgrading from 5.2 to 5.4: Data retention policy

- 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 is 67-day old, and the oldest Analytics logs is 38-day old. After upgrade to 5.4, FortiAnalyzer will keep the Archive logs for 365+67=432 days, and keep the Analytics logs for 365+38=403 days.
- For *newly created ADOMs*, Archive logs are kept for *365* days, and Analytics logs are kept for *60* days.

Supported Models

FortiAnalyzer 5.4.1 can run on the following FortiAnalyzer models:

Table 2: FortiAnalyzer 5.4.1 supported models

FortiAnalyzer	FortiAnalyzer VM
FAZ-200D	FAZ-VM64
FAZ-300D	FAZ-VM64-AWS
FAZ-400E	FMG-VM64-Azure
FAZ-1000D	FAZ-VM64-HV
FAZ-1000E	FAZ-VM64-KVM
FAZ-2000B	FAZ-VM64-XEN (Citrix XenServer and Open Source Xen)
FAZ-2000E	
FAZ-3000D	
FAZ-3000E	
FAZ-3000F	
FAZ-3500E	
FAZ-3500F	
FAZ-3900E	
FAZ-4000B	

FORTINET®

High Performance Network Security

05-541-370663-20161025