

FortiAnalyzer Upgrade Guide

VERSION 5.2.5

FORTINET®

Copyright© 2015 Fortinet, Inc. All rights reserved.

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

How to Upgrade

STEP 1: Backup Your Device.

Backup your device and its configuration.

STEP 2: Download.

Upgrade images are available from the Customer Support website.

STEP 3: Upgrade and Monitor.

Install the new firmware.

STEP 4: Verify and Validate.

Use the GUI to verify that the upgrade succeeded, and run the dataset validation tool to verify your datasets.

2

Upgrade Paths

You can upgrade FortiAnalyzer 5.0.6 or later directly to FortiAnalyzer 5.2.5. If you are upgrading from 5.0.5 or earlier, you will need to upgrade to FortiAnalyzer 5.0.6 first.

Table 1: FortiAnalyzer V5.2.5 upgrade paths

Initial Version	Upgrade To	Log Database Rebuild Required?
5.0.6–5.0.11	5.2.5	Yes for 5.0.6, No for the rest
5.2.0 or later	5.2.5	No

**If you are running v5.0.6, 5.0.7, 5.0.8, 5.0.9, 5.0.10, during the firmware upgrade, your FortiAnalyzer will temporarily disconnect. When complete, you will be able to login and access your FortiAnalyzer, Not all features will be available immediately while the SQL database is rebuilt. View Step 3 Upgrade and Monitor for details.*

3

Detailed Upgrade Instructions

Step 1. Back Up Your Device.

Backup your device configuration from the Systems Settings tab.

Step 2. Download.

Download your firmware image.

1. Use the CLI command to check for current reports. Allow them to complete prior to upgrading.

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

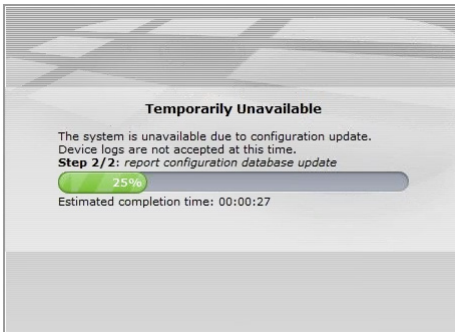
2. If you are upgrading a FortiAnalyzer VM, make sure your VM partition has more than 512MB*, and your VM server is up to date.

**It is recommended to allocate 1024MB for the FortiAnalyzer VM partition.*

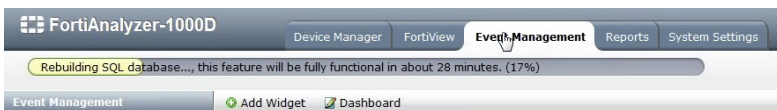
Step 3. Upgrade and Monitor

Install the downloaded firmware image.

During a firmware upgrade, you will temporarily disconnect to your FortiAnalyzer. When the firmware has been installed, you can reconnect to your device.

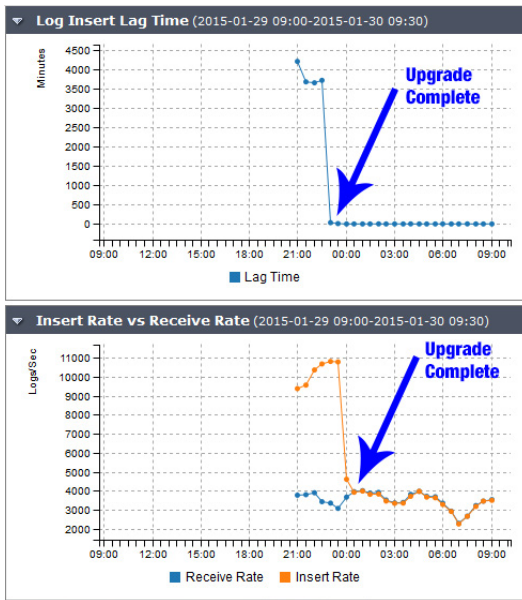


When complete, you will be able to log in and access your FortiAnalyzer. Not all features will be available immediately while the SQL database is rebuilt. A status bar will keep you up to date on the rebuild status:



Step 3. Upgrade and Monitor

Monitor the rebuild progress with the *Log Insert Lag Time* and *Insert Rate vs Receive Rate* widgets. These widgets will show you the gap between logs being received and logs being inserted after the upgrade. You can customize this widget to show data every 60 to 240 seconds. As shown below, you will notice an initial delay in logs being inserted, but that will resolve itself as time passes. You can add these widgets in the same way you add other widgets in the Dashboard.



Step 4. Verify and Validate

After using GUI to verify that the upgrade succeeded, run dataset validation tool to verify your datasets.

1. Select the *Reports* tab.
2. Select *Advanced* in the left pane.
3. Select *Dataset*.
4. Right-click any report and select *Validate All Custom*.

The screenshot shows the FortiAnalyzer-3000D interface. The top navigation bar includes 'Device Manager', 'FortiView', 'Event Management', and 'Reports'. The left sidebar shows a tree view with 'Reports' expanded, and 'Dataset' selected under the 'Advanced' category. The main content area displays a list of reports. A context menu is open over the 'App-Risk-High-Risk-Application' report, with the 'Validate All Custom' option highlighted in a red box.

Dataset	Message
1111	ERROR: inet types text and inet cannot be matched LINE 1: ... (select ... as ...
2222	ERROR: inet types text and inet cannot be matched LINE 1: ... (select ... as ...
3333	ERROR: inet types text and inet cannot be matched LINE 1: select * from (... as ...)

Supported Models

The following models support upgrading to FortiAnalyzer v5.2.5:

FAZ-100C

FAZ-200D

FAZ-300D

FAZ-400C

FAZ-1000C

FAZ-1000D

FAZ-2000B

FAZ-3000D

FAZ-3000E

FAZ-3500E

FAZ-3900E

FAZ-4000B

FAZ-VM32

FAZ-VM64

FAZ-VM64-AWS

FAZ-VM64-HV

FAZ-VM64-KVM

FAZ-VM64-XEN

FORTINET®

05-525-307321-20160120