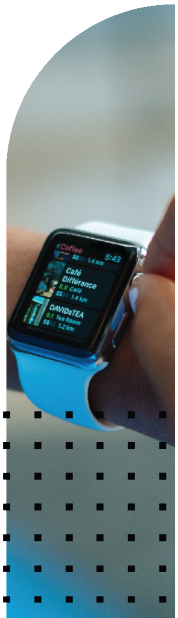
Upgrade Guide

FortiAnalyzer 7.0.11



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 7th, 2024
FortiAnalyzer 7.0.11 Upgrade Guide
05-7011-990567-20240207

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-02-07	Initial release of 7.0.11.

Introduction

This document describes how to upgrade FortiAnalyzer to 7.0.11. This guide is intended to supplement the *FortiAnalyzer Release Notes*, and it includes the following sections:

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 *FortiAnalyzer Release Notes* on the Fortinet Document Library (https://docs.fortinet.com/), or contact Fortinet Customer Service & Support (https://support.fortinet.com/).
- Upgrade FortiAnalyzer before upgrading FortiOS, and be sure to maintain release version compatibility at all times.

Preparing to Upgrade FortiAnalyzer

We recommend performing the following tasks to prepare for a successful upgrade of a FortiAnalyzer unit. Following is a summary of the preparation tasks and a link to the details for each task.

To prepare for upgrading FortiAnalyzer (summary):

1. Download release notes, firmware images, and SNMP MIB files. See Downloading files from Customer Service & Support on page 6.
2. Review release notes. See Reviewing FortiAnalyzer 7.0.11 Release Notes on page 9.
3. Plan when to perform the upgrade. See Planning when to upgrade on page 9.
4. Review the status of managed devices. See Reviewing status of managed devices on page 9.
5. Review FortiAnalyzer system resources and license information. See Reviewing FortiAnalyzer system resources and license information on page 11.
6. Back up configuration files and databases. See Backing up configuration files and databases on page 12.
7. Back up logs. See Backing up logs on page 13.
8. Check reports. See Checking reports on page 13
9. Clone VM instances. See Creating a snapshot of VM instances on page 13.

Downloading files from Customer Service & Support

You can download release notes and firmware images from the Fortinet Customer Service & Support portal at https://support.fortinet.com. If you are using SNMP to monitor equipment, you can also download MIB files from the Fortinet Customer Service & Support portal.

This section contains the following topics:

Downloading release notes and firmware images

Release notes are available for download from the Fortinet Customer Service & Support portal (https://support.fortinet.com/).

Firmware images can be downloaded from the following locations:

- FortiGuard: From FortiAnalyzer GUI, you can view the recommended firmware upgrade path, download the firmware from FortiGuard, and upgrade the firmware.

- Fortinet Customer Service & Support portal: Firmware images are organized by firmware version, major release, and patch release. You can download the firmware image, and then upload the firmware image to FortiAnalyzer GUI.

This section describes how to download firmware images from the Fortinet Customer Service & Support portal. For information about downloading firmware images from FortiGuard, see Upgrading FortiAnalyzer Firmware on page 14.

For information about the naming convention of firmware images and VM firmware images, see FortiAnalyzer firmware images on page 8, FortiAnalyzer VM firmware images on page 8, and Build numbers on page 9.

We recommend running an MD5 checksum on the firmware image file.

To download release notes and firmware images for hardware:

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiAnalyzer*.
4. Download the release notes for the 7.0.11 build:
   a. On the *Release Notes* tab, click the *7.0.11 Build <number>* link.
   The Document Library is displayed.
   b. Download the release notes.
5. Download the firmware image:
   a. Return to the Fortinet Customer Service & Support portal, and click the *Download* tab.
   b. Go to the *v7.00* > *7.0* > *7.0.11* folder, and locate the firmware image for your device or VM.
   c. Download the firmware image by clicking the *HTTPS* link.
   An HTTPS connection is used to download the firmware image.
   d. Click the *Checksum* link for the image that you downloaded.
   The image file name and checksum code are displayed in the *Get Checksum Code* dialog box.
   e. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

To download firmware images for VM environments:

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *VM Images*.
3. In the *Select Product* dropdown list, select *FortiAnalyzer*.
4. In the *Select Platform* list, select the platform.
5. Click the version.
   The firmware images for the selected product, platform, and version are displayed in the content pane.
6. Click *Download* for the *.out* file.
   The firmware image is downloaded to your computer.

Downloading MIB files for SNMP

If you are not using SNMP to monitor equipment, you can skip this procedure.

If you are using SNMP to monitor equipment, download the following MIB file from the Fortinet Customer Service & Support portal:

- *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib*, which is used with both FortiManager and FortiAnalyzer

To download SNMP MIB files:

1. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* dropdown list, select *FortiAnalyzer*.
4. Download the MIB file for the FortiAnalyzer 7.0.11 release:
   a. On the *Download* tab, go to the *v7.00* > *7.0* > *7.0.11* > *MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
   An HTTPS connection is used to download the file.

FortiAnalyzer firmware images

The firmware images in the folders follow a specific naming convention, and each firmware image is specific to the device model or VM.

For example, the `FAZ_2000E-v7.0.3-build0254-FORTINET.out` image found in the */FortiAnalyzer/v7.00/7.0/7.0.0/* folder is specific to the FortiAnalyzer 2000E device model.

FortiAnalyzer VM firmware images

Fortinet provides FortiAnalyzer VM firmware images for a number of virtualization environments.

Firmware images follow a specific naming convention, and each firmware image is specific to the VM environment. All firmware images for VM upgrades have filenames that end with `.out`.

For example, the `FAZ_VM64_HV-v6-build2201-FORTINET.out` image is specific to upgrade for the Hyper-V platform.

For more information, see the FortiAnalyzer data sheet at https://www.fortinet.com/products/management/fortianalyzer.html.

VM installation guides are available in the Fortinet Document Library.

FortiAnalyzer 5.6.0 and later uses a different network interface mapping for ESX VM networks. After upgrading to FortiAnalyzer 7.0.11, edit the ESX VM network mapping to preserve network connectivity.

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

New FortiAnalyzer 7.0.11 VM installations use the correct mapping with ESX 5.5 and later.

Build numbers

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

Ensure that FortiAnalyzer 7.0.11 can run on your FortiAnalyzer model. See Supported Models on page 22.

Reviewing FortiAnalyzer 7.0.11 Release Notes

After you download the release notes for FortiAnalyzer 7.0.11, review the special notices, upgrade information, product integration and support, resolved issues, and known issues.

Planning when to upgrade

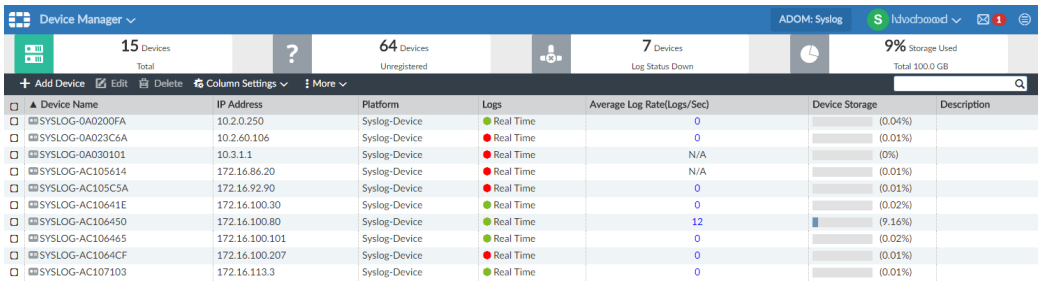
Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.

Reviewing status of managed devices

Before starting an upgrade, use the *Device Manager* pane to review the status of all logging devices to ensure 0 devices have a status of *Log Status Down*.

Either correct devices with a *Log Status Down* status or make note of them prior to starting the upgrade.

Following is an example of the *Device Manager* pane with 7 devices that have a status of *Log Status Down*.



You can use the following CLI commands to review the status of managed devices. Use this command to check that device and ADOM disk quota are correct before and after the upgrade.

- `diagnose log device`

This section contains the following topics:

- CLI example of diagnose log device on page 10

CLI example of diagnose log device

Run this command before the upgrade and keep the output. After the upgrade, run this command again and check that device and ADOM disk quota are correct.

Following is an example of the CLI output for the `diagnose log device` command:

```
FAZ1000E # diagnose log device
Device Name  Device ID   Used Space(logs/quarantine/content/IPS) Allocated Space Used%
CSF-81E-HA   FGHA0815848309_CID 163.4MB( 163.4MB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
   |- HA cluster member: FG81EP4Q16000393
   |- HA cluster member: FG81EP4Q16001954
FG101E-L2    FG101E4Q17001425     0.0KB(   0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
FG101E-L3    FG101E4Q17001278     0.0KB(   0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
FG280DPOE-L3 FG280P4614800182    18.0MB(  18.0MB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
FGT100D-HA   FGHA000879790946_CID 0.0KB(   0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
   |- HA cluster member: FG100D3G13802934
   |- HA cluster member: FG100D3G14811667
FGT200DPOE-L1-root FGP2046148316 10.6MB(  10.6MB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
FGVM-076-L2  FGVM020000069046     4.7MB(   4.7MB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
vm1          FGVM021111111111     0.0KB(   0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) unlimited n/a
Total: 8 log devices, used=196.7MB quota=unlimited

AdomName AdomOID Type Logs Database
           [Retention Quota UsedSpace(logs/quarantine/content/IPS) Used%]    [Retention
                Quota Used Used%]
FortiAnalyzer 108 FAZ 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiAuthenticator 124 FAC 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days
     700.0MB 0.0KB 0.0%
FortiCache   112 FCH 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiCarrier 104 FGT 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiClient  114 FCT 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiDDoS    122 FDD 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
```

```
FortiMail    106 FML 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiManager 118 FMG 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiSandbox 120 FSA 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
FortiWeb     110 FWB 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
Syslog       116 SYS 365days 300.0MB 0.0KB( 0.0KB/ 0.0KB/ 0.0KB/ 0.0KB) 0.0% 60days 700.0MB
     0.0KB 0.0%
root         3 FGT 365days 15.0GB 196.7MB( 196.7MB/ 0.0KB/ 0.0KB/ 0.0KB) 1.3% 60days 35.0GB
     264.5MB 0.7%

Total usage: 12 ADOMs, logs=196.7MB database=331.3MB(ADOMs usage:264.5MB + Internal
     Usage:66.8MB)

Total Quota Summary:
   Total Quota Allocated Available Allocate%
   10700.4GB 110.7GB 10589.7GB 1.0 %

System Storage Summary:
   Total Used Available Use%
   11000.4GB 17.5GB 10982.9GB 0.2 %

Reserved space: 300.0GB ( 2.7% of total space).
```

Reviewing FortiAnalyzer system resources and license information

Before starting an upgrade, go to *System Settings* to review the following widgets:

- License Information widget
- System Resources widget to check for high memory and CPU usage

It is also recommended to check the Alert Message Console widget in *System Settings* and the notifications in the toolbar.

If you are upgrading a FortiAnalyzer VM:

Make sure your VM partition has more than 1024MB and your VM server is up to date.

To view the flash disk size of your VM, enter the following command in the FortiAnalyzer CLI and review the value for the first hard disk (SDA):

```
diagnose system print partitions
```

For example:

```
dia sys print partitions
   major minor #blocks name fstype
   1 0 4096 ram0
   1 1 4096 ram1
   1 2 4096 ram2
   1 3 4096 ram3
   7 0 10240 loop0 ext2
   8 0 4199424 sda
   8 1 1048576 sda1 ext3
```

```
8 16 524288000 sdb
8 48 1048576 sdd
8 32 1048576 sdc
8 80 1048576 sdf
8 64 1048576 sde
8 96 1048576 sdg
8 160 1048576 sdk
8 128 1048576 sdi
8 144 1048576 sdj
8 208 1048576 sdn
8 192 1048576 sdm
8 176 1048576 sdl
8 224 1048576 sdo
8 112 1048576 sdh
253 0 524283904 dm-0
```

You can increase the size by shutting down the VM, editing the VM hardware to increase the size of the first hard disk, and then restarting the VM.

For more information about FortiAnalyzer VM, see documentation for FortiAnalyzer Private Cloud and FortiAnalyzer Public Cloud.

Backing up configuration files and databases

Back up the FortiAnalyzer configuration file and databases.

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.

It is also recommended that you verify the integrity of your backup file.

When the database is larger than 2.8 GB, back up the configuration file to an FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename of
    server> <username on server> <password> <crptpasswd>
execute backup all-settings scp <ip> <path/filename of server> <SSH
    certificate> <crptpasswd>
```

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

To back up your system configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, locate *System Configuration* and click *Backup*. The *Backup System* dialog opens.
3. Click the *Backup Now* tab.
4. Enter and confirm the password you want to use for encryption. The password can be a maximum of 63 characters.
5. Click *OK* and save the backup file on your local computer.

To verify the integrity of a backup file:

1. Back up your system configuration and save the backup file on your local computer.
2. Go to *System Settings* > *Event Log*.

3. Locate the system event that was logged as a result of the backup operation from the *Event Log* table. You may use the *Add Filter* button from the toolbar above to simplify locating the logged event entry.
4. In the *Changes* column for the event log, note the MD5 checksum.

If the checksums match, then the backup process was successful.

Before restoring a configuration with private data encryption enabled, you must first enable this setting on the FortiAnalyzer where the restore is to be performed.

Private data encryption can be enabled in the CLI using command `set private-data-encryption enable`.

If private data encryption is not enabled, local certificates may not be restored which will prevent remote users from being able to successfully log in.

Backing up logs

It is recommended to back up logs before an upgrade.

```
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd> <directory>
     [vdlist]
```

It is also recommended to send logs to a temporary FortiAnalyzer or syslog server during the upgrade.

Checking reports

Wait until all the running reports are completed, and ensure that no reports are scheduled to run during the upgrade.

You can use the following CLI commands to check for running and pending reports:

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

Creating a snapshot of VM instances

In VM environments, it is recommended to stop the VM instance and take a snapshot or clone of the VM instance before the upgrade. If there are issues with the upgrade, you can revert to the VM snapshot or clone.

Avoid taking snapshots when applications in the virtual machine are communicating with other computers.

Upgrading FortiAnalyzer

If you are upgrading from versions earlier than 6.4.0, you must upgrade to FortiAnalyzer 6.4.0 first, and then to 7.0.11. We recommend that you upgrade to the latest version of FortiAnalyzer 6.4.

When upgrading to FortiAnalyzer 7.0.11 from FortiAnalyzer 6.4.0 and later, you are not required to wait for a database rebuild before upgrading to the next firmware release in your upgrade path, if your upgrade path involves multiple steps.

For other upgrade paths, see Firmware Upgrade Paths on page 23.

This section contains the following topics:

Upgrading the device firmware can trigger an SQL database rebuild. During the database rebuild, new logs are inserted into the database and can be viewed, but existing logs are not available until the rebuild is complete. The time required to rebuild the database depends on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

For more information, see Verifying database rebuild success on page 20.

Upgrading FortiAnalyzer Firmware

This section describes how to upgrade FortiAnalyzer firmware. You can use the following methods to upgrade firmware:

- From the FortiAnalyzer GUI, download the firmware from FortiGuard and upgrade the unit.
- From the FortiAnalyzer GUI, upload the firmware that you previously downloaded from the Customer Service & Support portal.

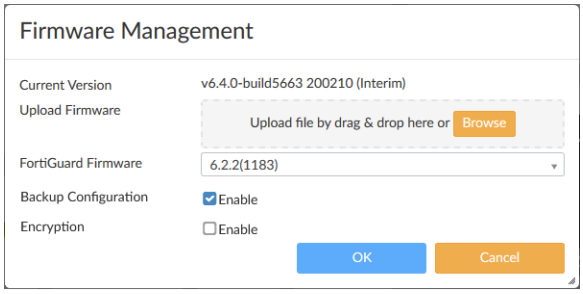
Fortinet recommends uploading firmware to FortiAnalyzer by using a server that is in the same location as the FortiAnalyzer. This helps avoid timeouts.

For the Collector-Analyzer architecture upgrade, Fortinet recommends upgrading the Analyzer first. Upgrading the Collector first might affect the Analyzer's performance.

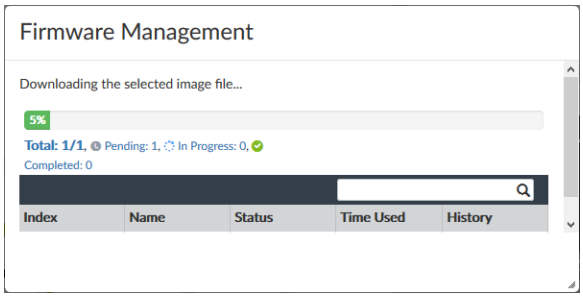
To upgrade firmware for a cluster, Fortinet recommends upgrading the HA secondary units first, followed by the HA primary unit last. To avoid losing log information, wait until each FAZ upgrade has finished before proceeding to the next. See Upgrading the firmware for an operating cluster on page 17.

To upgrade firmware using FortiGuard:

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



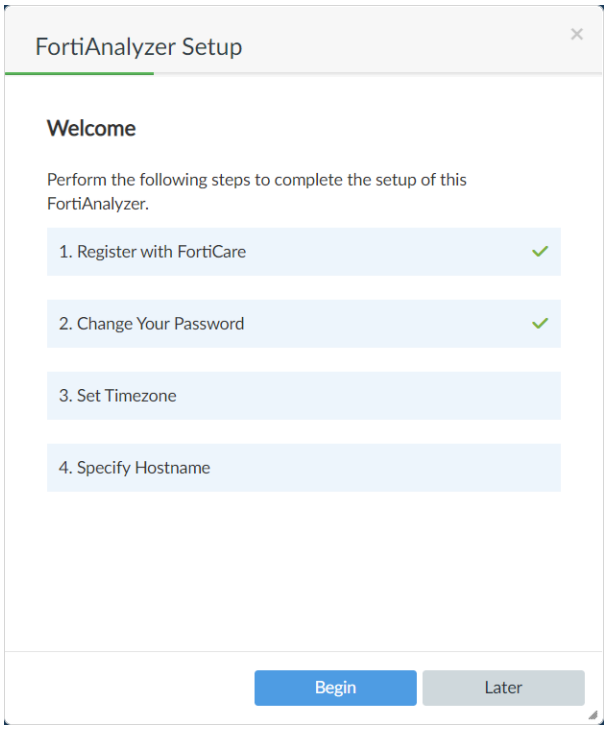
3. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiAnalyzer configuration when performing a firmware upgrade. If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. In the *FortiGuard Firmware* list, select the version of FortiAnalyzer for upgrade, and click *OK*.
   The *FortiGuard Firmware* box displays all FortiManager firmware images available for upgrade. A green checkmark displays beside the recommended image for FortiAnalyzer upgrade.
   If you select an image without a green checkmark, a confirmation dialog box is displayed. Click *OK* to continue.
   FortiAnalyzer downloads the firmware image from FortiGuard.



   FortiAnalyzer uses the downloaded image to update its firmware, and then restarts.
   It is recommended to view the console log output during upgrade. See Checking FortiAnalyzer log output on page 18.
5. When the login window displays, log into FortiAnalyzer.

When the upgrade completes, you might have to refresh your web browser to see the login window.

The *FortiAnalyzer Setup* wizard is displayed.



6. Click *Begin* to start the *FortiAnalyzer Setup* wizard.
   Alternately, you can click *Later* to complete the wizard later.
7. If the database needs rebuilding, you can monitor the rebuild status by double-clicking the *Rebuilding DB* status in the toolbar.

   The rebuild process includes two steps. When it's done, you see the *Rebuilding log database was completed* message.

   Some features are unavailable while the SQL database is rebuilding.

8. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiAnalyzer events on page 19.

To upgrade firmware using an image downloaded from the Customer Service & Support portal:

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. Before upgrading your firmware, you can choose to enable or disable *Backup Configuration*. When this setting is enabled, you will automatically download a backup copy of your FortiAnalyzer configuration when performing a firmware upgrade. If you want to encrypt the backup file, enable *Encryption*, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. In the *Firmware Upload* dialog box, click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal, and click *Open*.
5. Click *OK*.
   The firmware image is uploaded. When the upgrade completes, a message confirms a successful upgrade.

It is recommended to view the console log output during upgrade. See Checking FortiAnalyzer log output on page 18.

6. When the login window displays, log into FortiAnalyzer.

When the upgrade completes, you might have to refresh your web browser to see the login window.

The *FortiAnalyzer Setup* wizard is displayed.

7. Click *Begin* to start the *FortiAnalyzer Setup* wizard.
Alternately, you can click *Later* to complete the wizard later.
8. If the database needs rebuilding, you can monitor the rebuild status by double-clicking the *Rebuilding DB* status in the toolbar.

The rebuild process includes two steps. When it's done, you see the *Rebuilding log database was completed* message.

Some features are unavailable while the SQL database is rebuilding.

9. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiAnalyzer events on page 19.

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 *FortiAnalyzer CLI Reference*.

Upgrading the firmware for an operating cluster

You can upgrade the firmware of an operating FortiAnalyzer cluster in the same way as upgrading the firmware of a standalone FortiAnalyzer unit.

Upgrade the secondary units first. Upgrade the primary unit last, after all secondary units have been upgraded and have synchronized with the primary unit.

When you upgrade the primary unit, one of the secondary units is automatically selected to be the primary unit following the rules configured in FortiAnalyzer. This allows the HA cluster to continue operating through the upgrade process with primary and secondary units. See the *FortiAnalyzer Administration Guide* in the Fortinet Document Library for more information.

During the upgrade, you might see messages about firmware version mismatch. This is to be expected. When the upgrade is completed and all cluster members are at the same firmware version, you should not see this message.

To upgrade FortiAnalyzer HA cluster firmware:

1. Log into each secondary unit and upgrade the firmware.
   See Upgrading FortiAnalyzer Firmware on page 14 and the *FortiAnalyzer Release Notes* in the Fortinet Document Library for more information.
2. Wait for the upgrades to complete and check that the secondary units have joined the HA cluster as secondary units.
3. Ensure that logs are synchronized with the primary unit.
4. Upgrade the primary unit.
   When the primary unit is upgraded, it automatically becomes a secondary unit and one of the secondary units is automatically selected to be the primary unit following the rules. This allows the HA cluster to continue operating through the upgrade process with primary and secondary units.

If firmware versions between cluster members do not match, configuration synchronization is disabled. Other synchronization operations continue to function.

You might not be able to connect to the FortiAnalyzer GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI might be slow. If necessary, use the console to connect to the CLI.

Checking FortiAnalyzer log output

While upgrading a FortiAnalyzer unit, use the console to check the log output in real-time. Check for any errors or warnings.

Following is a sample console output of an upgrade:

```
Serial number:FAZ-VM0000000001
Upgrading geography IP data...Done.
Initialize file systems...
Old version: v5.4.3-build1187 branchpt1187 170518 (GA)
New version: v5.4.4-build1220 branchpt1220 170928 (GA)
Global DB running version is 429, built-in DB schema version is 429
Upgrading report config from version:5. patch:3, branch point:1187
   Exporting existing config... (step 1/4)
      export (13/13) adoms. took 14 sec.
   Initializing default config... (step 2/4)
      init (13/13) adoms. took 12 sec.
   Upgrading existing config... (step 3/4)
      Upgrading V5.4.2->V5.4.3...
         process (13/13) adoms. took 19 sec.
   Importing upgraded config... (step 4/4)
      import (13/13) adoms. took 10 sec.
Upgrade report config completed. took 55 sec.
```

Checking FortiAnalyzer events

After upgrading, it is recommended to check all messages logged to the FortiAnalyzer Event Log. If you find any errors, you can fix the errors before continuing.

Following is an example of messages in the FortiAnalyzer Event Log:

Date Time	Level	User	Sub Type	Message
2017-09-17 20:00:07	warning	system	FortiAnalyzer event	Dropped 2 log database tables before 2017-07-19 20:00:00 from Adom root due to Adom retention policy.
2017-09-17 20:00:00	warning	system	FortiAnalyzer event	Requested to trim database tables older than 60 days to enforce the retention policy of Adom root.
2017-09-17 12:11:37	information	system	FortiAnalyzer event	fazcfgd update webfilter categories files: status='successful'.
2017-09-17 12:11:37	information	system	FortiAnalyzer event	fazcfgd update link prefixes file: status='successful'.
2017-09-12 18:06:18	information	system	FortiAnalyzer event	Received new version 00012.00222-1709122344 for object '05004000NIDS02300'.
2017-09-12 18:06:18	information	system	FortiAnalyzer event	Received new version 00012.00222-1709122344 for object '05004000NIDS02200'.

Downgrading to previous firmware versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release using the GUI or CLI, but this causes configuration loss. A system reset is required after the firmware downgrade. 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}
```

Verifying FortiAnalyzer Upgrade Success

Once the upgrade is complete, check the FortiAnalyzer unit to ensure that the upgrade was successful. This section describes items you should check.

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 is disabled after upgrade. You can re-enable the SQL storage settings to view logs and analytics with the following CLI commands:

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

This section contains the following topics:

Verifying database rebuild success

Upgrade automatically triggers an SQL rebuild post upgrade to 6.0, which must complete for FortiAnalyzer to function normally. Verify the database rebuild status using the following CLI command:

```
diagnose sql status rebuild-db
```

FortiAnalyzer's database rebuild is performed using Archive logs. Analytic logs will not be restored if FortiAnalyzer Archive logs are trimmed before performing a device database rebuild, therefore, it is important to review your storage data policy before upgrading and performing a database rebuild.

See the FortiAnalyzer Administration Guide for more information on Analytic vs Archive logs.

Verifying device and ADOM disk quota

Run the `diagnose log device` CLI command after the upgrade and compare it to the output before the upgrade. Check that the device and ADOM disk quota allocations are correct. See CLI example of diagnose log device on page 10.

Verifying required daemons are running

Use the following CLI commands to check that the following daemons are running:

- `diagnose test application fortilogd 1`
- `diagnose test application sqllogd 2`
- `diagnose test application oftpd 2`
- `diagnose test application oftpd 3`
- `diagnose test application fazcfgd 2`

Checking Alert Message Console and notifications

After the FortiAnalyzer upgrade completes, check the *Alert Message Console* and list of notifications for any messages that might indicate problems with the upgrade.

- In *System Settings* > *Dashboard*, check the *Alert Message Console* widget.
- Click the Notification icon and review any notifications.

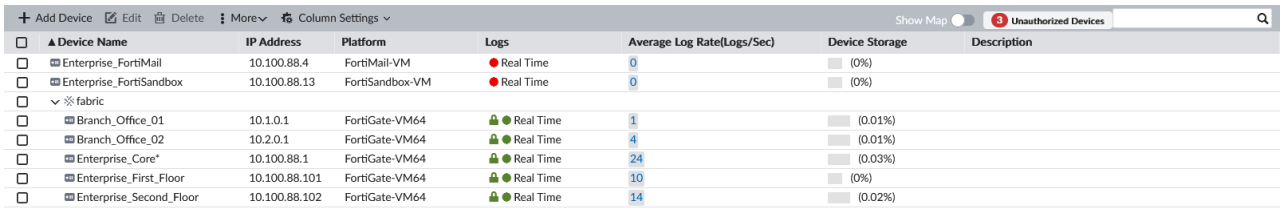
For information on accessing system settings, see Reviewing FortiAnalyzer system resources and license information on page 11.

Checking managed devices

After the FortiAnalyzer upgrade completes, check the managed devices in the GUI.

To check managed devices:

1. Refresh the browser and log back into the device GUI.
2. Go to *Device Manager*, and ensure that all formerly added devices are still listed.
3. In *Device Manager*, select each ADOM and ensure that managed devices reflect the appropriate connectivity state. It might take some time for FortiAnalyzer to establish connectivity after the upgrade.



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
Enterprise_FortiMail	10.100.88.4	FortiMail-VM	Real Time	0	(0%)	
Enterprise_FortiSandbox	10.100.88.13	FortiSandbox-VM	Real Time	0	(0%)	
fabric						
Branch_Office_01	10.1.0.1	FortiGate-VM64	Real Time	1	(0.01%)	
Branch_Office_02	10.2.0.1	FortiGate-VM64	Real Time	4	(0.01%)	
Enterprise_Core*	10.100.88.1	FortiGate-VM64	Real Time	24	(0.03%)	
Enterprise_First_Floor	10.100.88.101	FortiGate-VM64	Real Time	10	(0%)	
Enterprise_Second_Floor	10.100.88.102	FortiGate-VM64	Real Time	14	(0.02%)	

4. Launch other functional modules and make sure they work properly.

Supported Models

FortiAnalyzer version 7.0.11 supports the following models:

FortiAnalyzer	FortiAnalyzer VM
FAZ-150G	FAZ_DOCKER
FAZ-200F	FAZ-VM64
FAZ-300F	FAZ_VM64_ALI
FAZ-300G	FAZ-VM64-AWS
FAZ-400E	FAZ-VM64-Azure
FAZ-800F	FAZ-VM64-GCP
FAZ-800G	FAZ-VM64-HV (including Hyper-V 2016, 2019)
FAZ-1000F	FAZ-VM64-IBM
FAZ-2000E	FAZ-VM64-KVM
FAZ-3000F	FAZ-VM64-OPC
FAZ-3000G	FAZ-VM64-XEN (Citrix XenServer and Open Source Xen)
FAZ-3500E	
FAZ-3500F	
FAZ-3500G	
FAZ-3700F	
FAZ-3700G	
FAZ-3900E	

Firmware Upgrade Paths

The following table identifies the supported FortiAnalyzer upgrade paths and whether the upgrade requires a rebuild of the log database. If you need information about upgrading to FortiAnalyzer 6.0, 6.2, or 6.4, see the corresponding *FortiAnalyzer Upgrade Guide*.

Initial Version	Upgrade to	Log Database Rebuild
7.0.0 or later	7.0.11	No
6.4.0 or later	Latest 6.4 version, then to version 7.0.11	No
6.2.0 or later	Latest 6.4 version	Yes if upgrading from a previous maintenance release
6.0.3 or later	Latest 6.2 version, then to latest 6.4 version	Yes

FortiGate units with logdisk buffer log data while FortiAnalyzer units are rebooting. In most cases, the buffer is enough to cover the time needed for FortiAnalyzer to reboot. However, Fortinet still recommends configuring multiple log destinations to ensure no logs are lost.

Fortinet Security Fabric

If you are upgrading the firmware for a FortiAnalyzer unit that is part of a FortiOS Security Fabric, 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 example, you must upgrade FortiAnalyzer to 7.0.0 or later before you upgrade FortiOS to 7.0.0 or later.

www.fortinet.com