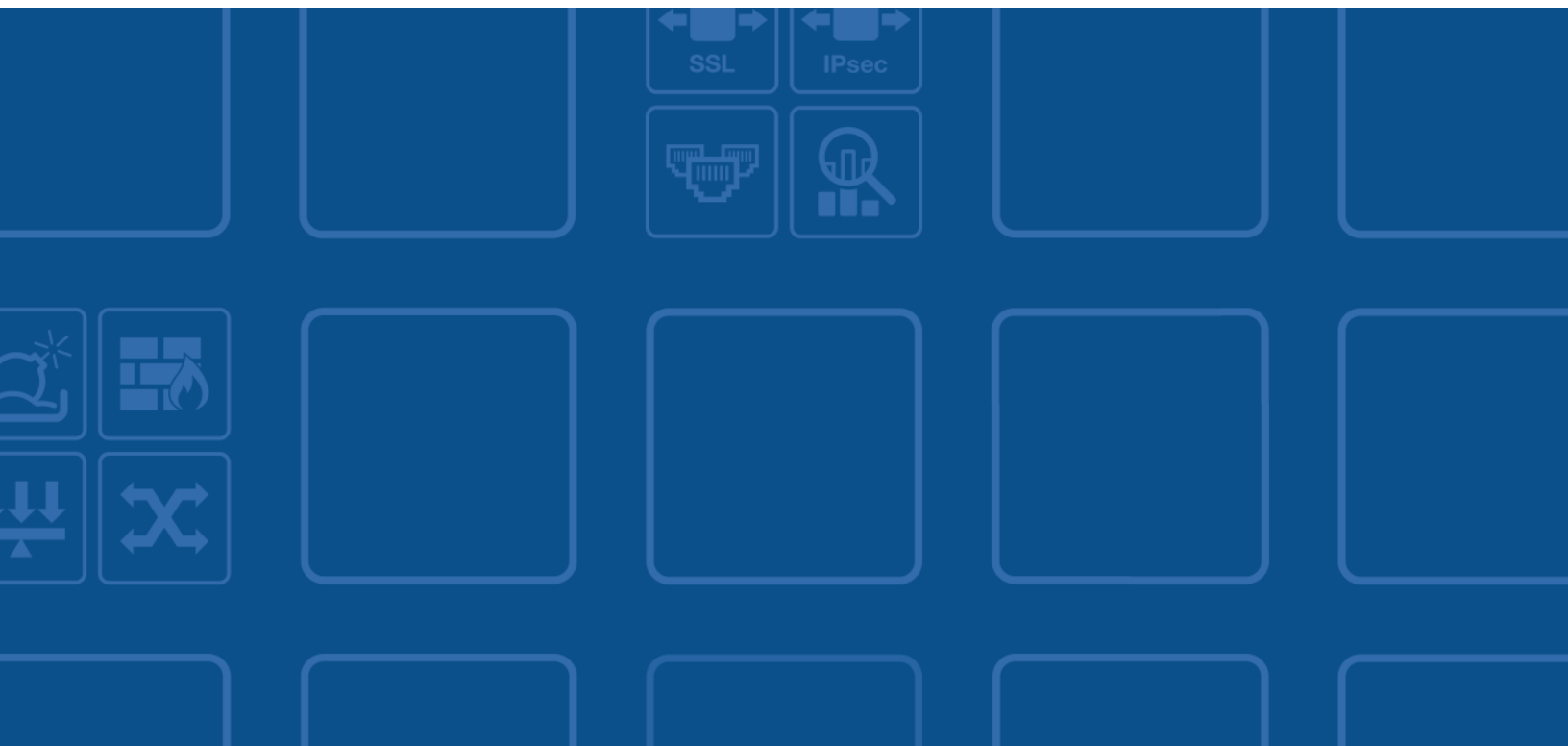
FortiAnalyzer - Upgrade Guide

VERSION 5.4.4



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

July 25, 2017

FortiAnalyzer 5.4.4 Upgrade Guide

05-544-451339-20170725

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Preparing to Upgrade FortiAnalyzer **7**
Summary of preparation tasks 7
Downloading files from Customer Service & Support 7
Downloading release notes and firmware images 7
Downloading MIB files 8
FortiAnalyzer firmware images 9
FortiAnalyzer VM firmware images 9
Build numbers 10
Reviewing FortiAnalyzer 5.4.4 Release Notes 10
Planning when to upgrade 10
Reviewing status of managed devices 10
CLI example of diagnose log device 11
Reviewing FortiAnalyzer System Settings 12
Backing up configuration files and databases 13
Backing up logs 14
Checking reports 14
Creating a snapshot of VM instances 14
Upgrading FortiAnalyzer **15**
Upgrading FortiAnalyzer Firmware 15
Checking FortiAnalyzer log output 16
Checking FortiAnalyzer events 17
Downgrading to previous firmware versions 17
Verifying FortiAnalyzer Upgrade Success **18**
Verifying database rebuild success 18
Verifying device and ADOM disk quota 18
Verifying required daemons are running 18
Checking Alert Message Console and notifications 18
Checking managed devices 19
Upgrade Policies for Log Storage **20**
Disk space allocation policy 20
Normal ADOM mode 20

Advanced ADOM mode 20
Additional policies 20
Data retention policy 21
Existing ADOMs 21
New ADOMs 21
Supported Models **22**
Firmware Upgrade Paths **23**

Change Log

Date	Change Description
2017-10-05	Initial Release.
2017-07-25	Added FAZ-800F to *Supported Models*.

Introduction

This document describes how to upgrade FortiAnalyzer to 5.4.4. This guide is intended to supplement the *FortiAnalyzer Release Notes*, and it includes the following sections:

- Preparing to Upgrade FortiAnalyzer on page 7
- Upgrading FortiAnalyzer on page 15
- Verifying FortiAnalyzer Upgrade Success on page 18
- Upgrade Policies for Log Storage on page 20
- Supported Models on page 22
- Firmware Upgrade Paths on page 23

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*, or contact Fortinet Customer Service & Support (https://support.fortinet.com/).

Preparing to Upgrade FortiAnalyzer

This section describes how to prepare FortiAnalyzer for upgrade. It includes a summary and details of each preparation task.

Summary of preparation tasks

We recommend performing the following tasks to prepare for a successful upgrade of a FortiAnalyzer unit. This section provides a summary of the tasks and includes links 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 7.
2. Review release notes. See Reviewing FortiAnalyzer 5.4.4 Release Notes on page 10.
3. Plan when to perform the upgrade. See Planning when to upgrade on page 10.
4. Review the status of managed devices. See Reviewing status of managed devices on page 10.
5. Review FortiAnalyzer System Settings pane. See Reviewing FortiAnalyzer System Settings on page 12.
6. Back up configuration files and databases. See Backing up configuration files and databases on page 13.
7. Back up logs. See Backing up logs on page 14.
8. Check reports. See Checking reports on page 14
9. Clone VM instances. See Creating a snapshot of VM instances on page 14.

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 also describes the VM firmware images available for FortiAnalyzer.

Downloading release notes and firmware images

Firmware images are located on the Fortinet Customer Service & Support portal, and they are organized by firmware version, major release, and patch release.

For information about the naming convention of firmware images and VM firmware images, see FortiAnalyzer firmware images on page 9, FortiAnalyzer VM firmware images on page 9, and Build numbers on page 10.

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

To download release notes and firmware images:

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 5.4.4 build:
   a. On the *Release Notes* tab, click the *5.4.4 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 *v5.00* > *5.4* > *5.4.4* 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.

Downloading MIB files

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 files from the Fortinet Customer Service & Support portal:

- *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib*, which is used with both FortiManager and FortiAnalyzer
- Fortinet Core MIB file, which is used with all Fortinet products

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 5.4.4 release:
   a. On the *Download* tab, go to the *v5.00* > *5.4* > *5.4.4* > *MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
      An HTTPS connection is used to download the firmware image.
   c. 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.
   d. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

5. Download the Fortinet Core MIB file:
   a. On the *Download* tab, go to the *v5.00* > *Core MIB* folder.
   b. Download the MIB file by clicking the *HTTPS* link.
      An HTTPS connection is used to download the firmware image.
   c. 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.
   d. Confirm that the checksum of the downloaded image file matches the checksum provided on the download site.

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_1000C-v5-build1187-FORTINET.out image found in the */FortiAnalyzer/v5.00/5.4/5.4.3/* file folder is specific to the FortiAnalyzer 1000C device model.

FortiAnalyzer VM firmware images

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available in the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit 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-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: For a new FortiAnalyzer VM installation, also download the Hyper-V package as it contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.ovf.zip`: Download the 64-bit package for a new FortiAnalyzer 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 FortiAnalyzer data sheet at https://www.fortinet.com/products/management/fortianalyzer.html.

VM installation guides are available in the Fortinet Document Library.

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 > 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 build number.

Ensure that FortiAnalyzer 5.4.4 can run on your FortiAnalyzer model. See Supported Models on page 22.

Reviewing FortiAnalyzer 5.4.4 Release Notes

After you download the release notes for FortiAnalyzer 5.4.4, review the special notices, upgrade information, product integration and support, resolved issues, and known issues.

Planning when to upgrade

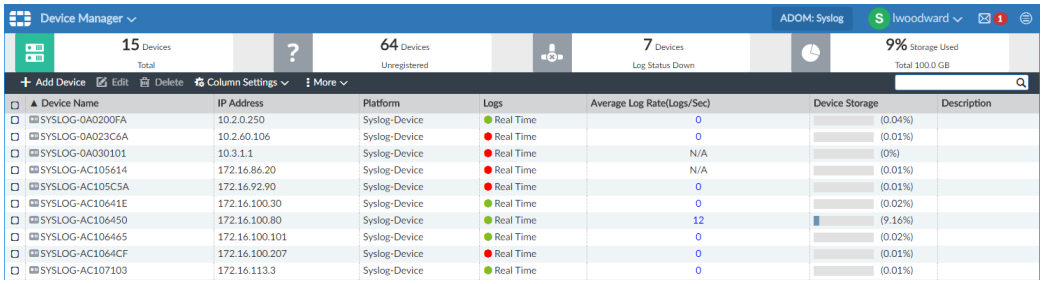
Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.

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`

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).
```

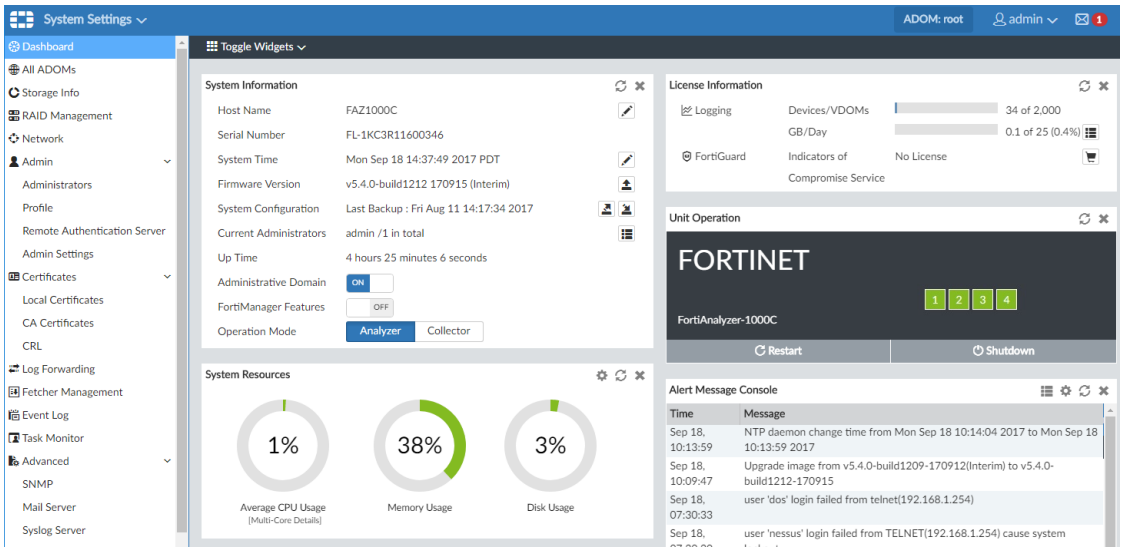
Reviewing FortiAnalyzer System Settings

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

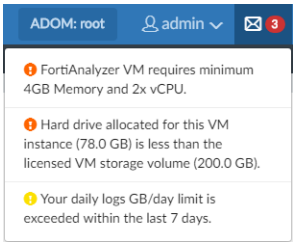
- License Information widget
- System Resources widget to check for high memory and CPU usage

It is also recommended to check the Alert Message Console and the list of notifications.

Following is an example of the *System Settings Dashboard* with the *License Information* and *System Resources* widgets:



Following is an example of the Notification list:



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 verify the integrity of a backup file:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click *Backup*. The *Backup* dialog box opens.
3. In the `Encryption` line, deselect the checkbox so that the backup is not encrypted.
4. Click *OK* and save the backup file on your local computer.
5. Locate the backup file and change the file extension from `.dat` to `.tgz`.
6. Decompress the backup file and verify that the decompression is successful.

If the decompression fails, then the backup process has likely also failed.

Ensure the backup is not encrypted because an encrypted backup always fails to decompress.

To back up your system configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click *Backup*. The *Backup* dialog box opens.
3. If you wish, select the checkbox to encrypt the backup file, and enter a password.
4. Click *OK* and save the backup file on your local computer.

If you encrypt the backup file, you must use the same password to restore this backup file.

Backing up logs

It is recommended to back up logs before an upgrade.

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 take a snapshot or clone of the VM instance before the upgrade. In the event of an issue with the upgrade, you can revert to the VM snapshot or clone.

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

Upgrading FortiAnalyzer

You can upgrade FortiAnalyzer 5.2.0 or later directly to FortiAnalyzer 5.4.4.

If you are upgrading from versions earlier than 5.2.0, you must upgrade to FortiAnalyzer 5.2 first. We recommend that you upgrade to the latest version of FortiAnalyzer 5.2.

Upgrading the device firmware can trigger an SQL database rebuild. New logs are not be 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.

The following features are available until the SQL database rebuild is complete: FortiView, Log View, Event Management, and Reports.

Upgrading FortiAnalyzer Firmware

This section describes how to upgrade FortiAnalyzer firmware.

It is recommended to upload 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 could impact the Analyzer's performance.

When upgrading from FortiAnalyzer 5.4.0 to 5.4.4, reboot FortiAnalyzer 5.4.0 before installing the firmware image for FortiAnalyzer 5.4.4.

To upgrade firmware:

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 displays.
3. Click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal, and click *Open*.
4. Click *OK*.
   The firmware image is uploaded. When the upgrade completes, a confirmation message is displayed that communicates a successful upgrade.

   It is recommended to view the console log output during upgrade. See Checking FortiAnalyzer log output on page 16.
5. Once the login window is displayed, log into FortiAnalyzer.

6. If the database needs rebuilding, you can monitor the rebuild status by double-clicking the *Rebuilding DB* status in the toolbar.

The rebuild process consists of 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.

7. Review the *System Settings* > *Event Log* for any additional errors. See Checking FortiAnalyzer events on page 17.

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*.

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 via the Web-based Manager 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 | 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
```

Verifying database rebuild success

If a database rebuild occurred during the FortiAnalyzer upgrade, verify that database rebuild was successful using the following CLI command:

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

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 11.

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 Settings on page 12.

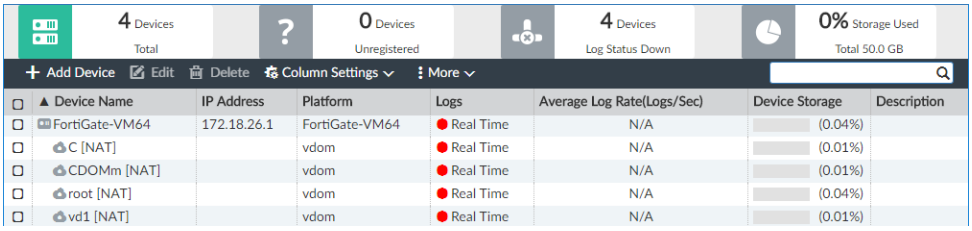
Checking managed devices

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.

   Following is an example of the quick status bar in *Device Manager* where you can check the connectivity status of managed devices. It might take some time for FortiAnalyzer to establish connectivity after the upgrade.



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

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) is allocated the disk space of the device before upgrade plus 10%.

For example, a FortiGate device allotted 30GB in 5.2 gets 33GB (30GB + 10%) to the ADOM of this FortiGate device after the upgrade to FortiAnalyzer 5.4.0 and later.

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 is split among the VDOMs of different ADOMs proportional to the log distribution across the VDOMs. Each ADOM also gets 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 assigns 1.1GB (1GB + 10%) to ADOM root, 3.3GB (3GB + 10%) to ADOM1, and 6.6GB (6GB+ 10%) 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 adds 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 less than 1GB before upgrading to 5.4.x, the ADOM quota for the device is adjusted to 1GB after upgrading to 5.4.x.

This adjustment might cause the total allocated disk space to go over the actual device disk space. Verify using the `diagnose log device` CLI command. If necessary, you can adjust the disk space back to less than 1GB.

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 1, 2016, and the oldest Analytics logs were generated on March 1, 2016. Today is April 7. 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 5.4.4 supports the following models:

FortiAnalyzer	FortiAnalyzer VM
FAZ-200D FAZ-300D FAZ-400E FAZ-800F FAZ 1000C FAZ-1000D FAZ-1000E FAZ-2000B FAZ-2000E FAZ-3000D FAZ-3000E FAZ-3000F FAZ-3500E FAZ-3500F FAZ-3700F FAZ-3900E FAZ-4000B	FAZ-VM64 FAZ-AWSOnDemand FAZ-VM64-AWS FAZ-VM64-Azure FAZ-VM64-HV FAZ-VM64-KVM FAZ-VM64-XEN (Citrix XenServer and Open Source Xen)

Firmware Upgrade Paths

You can upgrade FortiAnalyzer 5.2.0 or later directly to FortiAnalyzer 5.4.4.

If you are upgrading from versions earlier than 5.2.0, you must 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 5.2.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
5.4.2 or 5.4.3	5.4.4	No
5.4.0 or 5.4.1	5.4.4	Yes
5.2.x	5.4.4	Yes
5.0.6 or later	5.2	Yes for 5.0.6, no for the rest

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.

Copyright© 2018 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.