FortiSIEM - Upgrade Guide

Version 5.3.1

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

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/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://fortiguard.com/

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
06/30/2020	Initial version of the 5.3.1 Upgrade Guide.

Known Issues for 5.3.1

FortiSIEM customers running 5.3.1 build 1668 or lower, and having license for the FortiSIEM Indicators Of Compromise (IOC) service may experience a failure to update the IOC. The following error may be received:

```
Update failed: No SSL Connect
```

This is due to a licensing issue that requires an update to be applied to FortiSIEM and a new license key installed. To get the update, please contact Fortinet Support https://support.fortinet.com/.

Upgrade notes

- The location where you pick up FortiSIEM Images has changed—the website https://imagescdn.fortisiem.fortinet.com/ is no longer available. You must obtain FortiSIEM Images from the Fortinet support site: https://support.fortinet.com/.
Follow the instructions in Downloading FortiSIEM Products to get the FortiSIEM images.
- **If you are running Elasticsearch, then the upgrade from 5.2.1 or earlier to 5.3.1 requires special steps – See here. Please read these steps before beginning the upgrade process**.
- The Report Server upgrade to 5.3.1 requires additional steps. See Upgrade Report Server.
- Customers using releases prior to 4.10.0 must first upgrade to 4.10.0 before upgrading to 5.3.1. Customers using release 4.10.0 can directly upgrade to 5.3.1.
- Make sure that Super, Worker, Collector, and Report Server can connect to FortiSIEM hosted CentOS repo on https port 443 under the URLs below. Otherwise, some packages may not install and 5.3.1 binaries will not run.
    - https://os-pkgs-cdn.fortisiem.fortinet.com/centos6/
    - https://os-pkgs.fortisiem.fortinet.com/centos6/
- Collector image upgrades can now be performed from the Supervisor. For more information, see Upgrade the Collector Image From the Supervisor.

- The GUI settings for Archive are lost during the upgrade to 5.3.0. In earlier releases, the user mounted the archive and defined the local mount point in FortiSIEM. In this release, however, the user provides the archive host and exported directory and FortiSIEM performs the mount operation. This action unifies both the online and archive database mounting operations. If you were archiving in version 5.2.8 or earlier, then complete the following steps to recover the archive settings.
    a. Upgrade the Super and all Workers to FortiSIEM version 5.3.0.
    b. Unmount the archive.
    c. Delete the `/etc/fstab` entry of archive setting.
    d. Define the archive in **ADMIN > Setup > > Storage > Archive**. Make sure that the Archive host and exported directories are identical to the settings before the archive.
    e. Click **Test and Save**. FortiSIEM will now archive new events to the same location as before the upgrade.
    f. Delete all of the Workers in **ADMIN > License > Nodes**.
    g. Re-add all of the Workers in **ADMIN > License > Nodes**.

- To remediate a vulnerability in an external module, Flex login via LDAP is disabled.

Upgrade process

- Before upgrading FortiSIEM, you **MUST** read the changes in FortiSIEM licensing documented in the 'Licensing Guide' **here**.
- Customers using releases prior to 4.10.0 must first upgrade to 4.10.0 before upgrading to 5.3.1. Customers in 4.10.0 can directly upgrade to 5.3.1.

UPGRADE HARDWARE REQUIREMENT

Starting with version 4.5, Supervisor requires 24 GB RAM. This is because Supervisor node is caching device monitoring status for faster performance.

If Elasticsearch is chosen as the Event Database, the Supervisor needs an additional 8 GB RAM - in this case, the minimum requirement of the Supervisor is 32 GB RAM.

FortiSIEM SNMP Configuration

If you enabled SNMP on FortiSIEM nodes (Collectors, Workers, Supervisors), it recommended that you modify the snmpd.local.conf file to store special configurations. You should not modify snmpd.conf file since FortiSIEM upgrade will wipe away the changes in snmpd.conf. To prevent changes from being lost, copy the changes to snmpd.local.conf file and then upgrade.

Upgrading a FortiSIEM Single Node Deployment

These instructions cover the upgrade process for FortiSIEM Enterprise deployment with a single Supervisor.

1. Download the image from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Unzip the zip file to get the tar file.
3. Copy the `.tar` file to the Supervisor:
   a. Copy the `va-5.3.1.1668.tar` file, using SCP (for example), from your system to the Supervisor.
   b. Make sure this file is in a directory named 5.3.1.1668.
4. Using SSH, log in to the FortiSIEM virtual appliance as the root user. To avoid issues with SSH connection timeouts, disconnects etc., run the upgrade in screen using the following command:
   ```
   screen -S upgrade
   ```
   To connect the screen after failure:
   ```
   run screen -r
   ```
5. Log in as root to FortiSIEM Supervisor via SSH and run these commands:
   ```
   # mkdir /root/5.3.1.1668
   # mv va-5.3.1.1668.tar /root/5.3.1.1668/
   ```
6. Run the `phdownloadimage` script and point to your directory:
   ```
   # cd /pbin
   # ./phdownloadimage file:///root/5.3.1.1668
   ```
7. Run the `phupgradeimage` script to actually upgrade:
   ```
   # cd /pbin
   # ./phupgradeimage
   ```

Upgrading a FortiSIEM Cluster Deployment

Overview

Follow these steps while upgrading a VA cluster.

1. **Shut down all Workers.** Collectors can be up and running.
2. Upgrade Super first (while all workers are shutdown).
3. After Super is up and running, upgrade worker one by one.
4. Upgrade Collectors.

Step #1 prevents the accumulation of Report files while Super is not available during upgrade (#2). If these steps are not followed, Supervisor may not be able to come up after upgrade because of excessive unprocessed report file accumulation.

Note: Both Super and Worker MUST be on the same FortiSIEM version, else various software modules may not work properly. However, Collectors can be in an older version (one version older) - they will work except that they may not have the latest discovery and performance monitoring features in the Super/Worker versions. So FortiSIEM recommends that you also upgrade Collectors within a short period of time. If you have Collectors in your deployment, make sure you have configured an image server to use as a repository for the Collector.

Upgrade Supervisor

Supervisor must be upgraded first, before Workers and Collectors and Report Server.

Ensure all Workers are shut down before proceeding with the upgrade of the Supervisor.

1. Download the image from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Unzip the zip file to get the tar file.
3. Copy the `.tar` file to the Supervisor:
    a. Copy the `va-5.3.1.1668.tar` file, using SCP (for example), from your system to the Supervisor.
    b. Make sure this file is in a directory named 5.3.1.1668.

4. Using SSH, log in to the FortiSIEM virtual appliance as the root user. To avoid issues with SSH connection timeouts, disconnects etc., run the upgrade in screen using the following command:
   ```
   screen -S upgrade
   ```
   To connect the screen after failure:
   ```
   run screen -r
   ```
5. Run the `phdownloadimage` script and point to your directory:
   ```
   # cd /pbin
   # ./phdownloadimage file:///root/5.3.1.1668
   ```
6. Run the `phupgradeimage` script to actually upgrade:
   ```
   # cd /pbin
   # ./phupgradeimage
   ```

Upgrade Worker

Workers must be upgraded after Super.

1. Download the image from Fortinet Support Site to your system and unzip to get the tar file.
2. Copy the `.tar` file to the Worker:
   a. Copy the `va-5.3.1.1668.tar` file, using SCP (for example), from your system to the Worker.
   b. Make sure this file is in a directory named 5.3.1.1668.
3. Using SSH, log in to the FortiSIEM virtual appliance as the root user. To avoid issues with SSH connection timeouts, disconnects etc., run the upgrade in screen using the following command:
   ```
   screen -S upgrade
   ```
   To connect the screen after failure:
   ```
   run screen -r
   ```
4. Run the `phdownloadimage` script and point to your directory:
   ```
   # cd /pbin
   # ./phdownloadimage file:///root/5.3.1.1668
   ```
5. Run the `phupgradeimage` script:
   ```
   # cd /pbin
   # ./phupgradeimage
   ```

Migrating Elasticsearch data from 5.2.1 or earlier to 5.3.1

In 5.2.4, Elasticsearch query behavior changed from case-sensitive to case-insensitive. Therefore, Elasticsearch event data format has changed. After upgrade, data will be written in the new format starting new day UTC time. FortiSIEM can only query data in the new format. For existing customers that are already running Elasticsearch, older data must be re-indexed for searches to work, after upgrading to 5.3.1. Exact steps are as follows. It is advisable to start the upgrade with a few hours to go before new day in UTC time. Here is a PST example: a new day in UTC time format begins at 5pm PST. The customer can begin the upgrade at 12 PM PST.

1. Upgrade FortiSIEM Supervisor and Workers to 5.3.1.
2. Go to **Admin > Setup > Storage**. Click **Test and Save**.
3. Re-index earlier days – do not re-index today's data as new data is being written.

4. After a new day in UTC time, re-index yesterday's index. See Re-indexing.

5. Delete all old indices. See Delete old index.

6. Create an alias. See Creating alias.

Data will be queryable after steps 4 and 6 are complete.

Re-indexing:

```
curl -X POST "X.X.X.X:9200/_reindex" -H 'Content-Type: application/json' -d'
{
"source": {
"index": "fortisiem-event-2019.04.22"
},
"dest": {
"index": "fortisiem-event-upgrade-2019.04.22"
}
}'
```

Delete old index:

```
curl -XDELETE http://X.X.X.X:9200/fortisiem-event-2019.04.22
```

Creating alias:

```
curl -X POST "X.X.X.X:9200/_aliases" -H 'Content-Type: application/json' -d'
{
"actions" : [
{ "add" : { "index" : "fortisiem-event-upgrade-2019.04.22", "alias" : "fortisiem-event-
2019.04.22" } }
]
}
'
```

Upgrade Report Server

Complete the following steps to upgrade the Report Server. Because the upgrade is not working properly, you will have to complete additional steps here.

1. Download the files from image server to your system and unzip to get the tar file.

2. Copy the `.tar` file to the Report Server.
   a. Copy the `rs-5.3.1.1668.tar` file, using SCP (for example), from your system to the Report Server.
   b. Make sure this file is in a directory named `5.3.1.1668`.

3. Using SSH, log in to the FortiSIEM virtual appliance as the root user. To avoid issues with SSH connection timeouts, disconnects etc., run the upgrade in screen using the following command:

```
screen -S upgrade
```

To connect the screen after failure:

```
run screen -r
```

4. Log in as `root` to Report Server via SSH and move the tar file to that directory and open the tar file:
    ```
    # mkdir /root/5.3.1.1668
    # mv rs-5.3.1.1668.tar /root/5.3.1.1668 /
    # cd 5.3.1.1668 /
    # tar xf rs-5.3.1.1668.tar
    ```

5. Obtain the `phdownloadimage` script. You can do this in either of the following ways:

    a. Upgrade Super to 5.3.1. Then copy the Super's `/pbin/phdownloadimage` and replace the Report Server's `/pbin/phdownloadimage` script.

    b. Contact Fortinet Support: https://support.fortinet.com.

6. Replace the `phdownloadimage` script in the `/opt/phoenix/deployment/jumpbox` folder with the copy you just obtained.

7. Run the `phdownloadimage` script and point to your directory:
    ```
    # cd /pbin
    # ./phdownloadimage file:///root/5.3.1.1668
    ```

8. Run the `phupgradeimage` script.
    ```
    # cd /pbin
    # ./phupgradeimage
    ```

Report Server upgrade to 5.3.1 is not working properly. If you are running Report Server, then complete these steps to upgrade to 5.3.1:

1. Upgrade Super, Worker, Collector, and Report Server as described above.

2. Archive the Report Server event database. Run this command:
    `/opt/phoenix/deployment/reportdb_archiver.sh`

3. The report db backup is under `/data/archive/reportdb/reportdb_2019-09-09T14-33-26`.

4. Delete the Report Server from Super.

5. Add the Report Server back to Super.

6. Restore Report Server event database from Archive. Run this command:
    `/opt/phoenix/deployment/reportdb_restore.sh/data/archive/reportdb/reportdb_2019-09-09T14-33-26`.

Upgrade the Collector Image From the Supervisor

Follow these steps to download the Collector image files from the support site:

1. Download the Collector upgrade file from the Fortinet Support site and copy it to a location on the Supervisor.

2. Check the MD5 checksum with the one published on the Support site to make sure the image is correctly downloaded.

3. Log in to the Supervisor as root user.

4. Check whether the Collector package from a previous upgrade is present in the Supervisor. If it is, delete it.

5. Prepare the upgrade file for Collector download:

    a. Go to `/opt/phoenix/phscripts/bin/`.

    b. Run the command:
        `phSetupCollectorUpgrade.sh <coImageZipFile> <superFQDN/IP>`

where *coImageZipFile* is the full path of the location of the Collector upgrade file in Step 1 and *superFQDN/IP* is the FQDN or IP that must be resolvable from Collectors

6. Go to **Settings > System > Collector Image Server** and make sure that the image download URL is displayed. This value is generated by the system and cannot be edited.

7. Go to **ADMIN > Health > Collector Health**

   a. Select a Collector and click **Action > Download Image**. This will cause the Collectors to download the upgrade images from the Supervisor.

   b. Select a Collector and click **Action > Install Image**. This will cause the Collectors to install the upgrade.

Troubleshooting a FortiSIEM Upgrade

FortiSIEM generates a number of log files to help you diagnose any problems you might encounter during the upgrade process.

Inspect this log file in the `/tmp` folder:

- `dbschemaupgrade_1668x.log`

and this log file in the `/opt/phoenix/log` folder:

- `upgrade-populatedb_1668x.log`