FortiSIEM - Upgrade Guide

Version 6.1.2

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

01/31/2022
FortiSIEM 6.1.2 Upgrade Guide

TABLE OF CONTENTS

Change Log **4**
Upgrading to FortiSIEM 6.1.2 ..... **5**
Pre-Upgrade Steps 5
Upgrade Single Node Deployment 5
Upgrade Cluster Deployment 9
Overview 10
Detailed Steps - Local Disk or NFS Storage 10
Detailed steps – Elasticsearch Storage 13
Upgrade via Proxy 15

Change Log

Date	Change Description
11/05/2020	Initial version of the 6.1.2 Upgrade Guide.
12/01/2021	Updated Pre-Upgrade Steps section.

Upgrading to FortiSIEM 6.1.2

If you are running FortiSIEM 6.x then use these instructions to upgrade to the latest FortiSIEM 6.x version.

- Pre-Upgrade Steps
- Upgrade Single Node Deployment
- Upgrade Cluster Deployment
- Upgrade via Proxy on page 15

Pre-Upgrade Steps

If you are running FortiSIEM 6.1.0, then you will need a simple step before you proceed to upgrade. This involves copying a file into a specific location on the Supervisor node. Please complete this step before you proceed to upgrade to the latest FortiSIEM version.

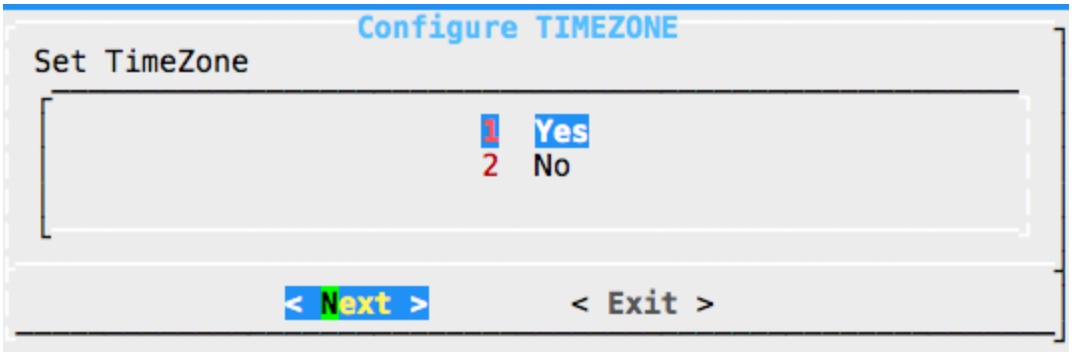
1. Carefully consider the known issues, if any, in the Release Notes.
2. Download the file `FSM_Upgrade_Script_Patch_6.1.2_build0119.zip` from the Fortinet Support website.
3. Login to the Supervisor as `root`.
4. Extract the `upgrade.py` script.
5. Copy it to `/usr/local/syslib/`.
6. Continue with the upgrade instructions below.

Upgrade Single Node Deployment

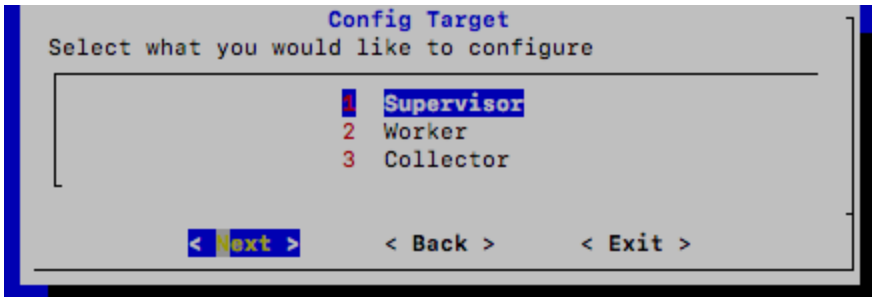
These instructions cover the upgrade process for the FortiSIEM deployment consisting of a single Supervisor node.

1. Download the upgrade image `FSM_Upgrade_All_6.1.2_build0119.zip` from Fortinet Support website.
2. Copy the file to Supervisor:
   a. Login as `root`.
   b. Run `mkdir -p /opt/upgrade`.
   c. Run `cd /opt/upgrade`.
   d. Copy `FSM_Upgrade_All_6.1.2_build0119.zip` to `/opt/upgrade`.
3. To avoid issues with SSH connection timeouts, disconnects etc.:
   a. Run the upgrade using the following command:
   ```
   screen -S upgrade
   ```
   b. To connect the screen after failure, run:
   ```
   run screen -r
   ```

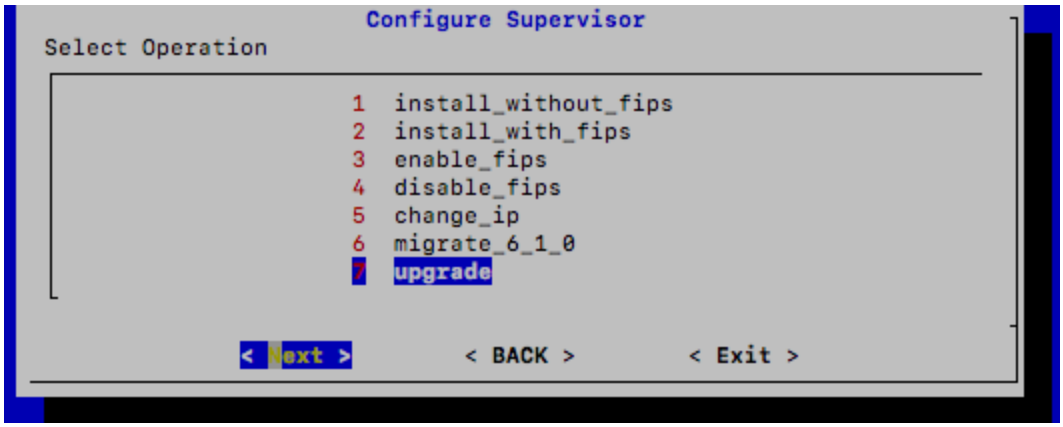
4. Upgrade by running `configFSM.sh`:
   a. Setup **Timezone** with **Country** and **Region** and click **Next**.



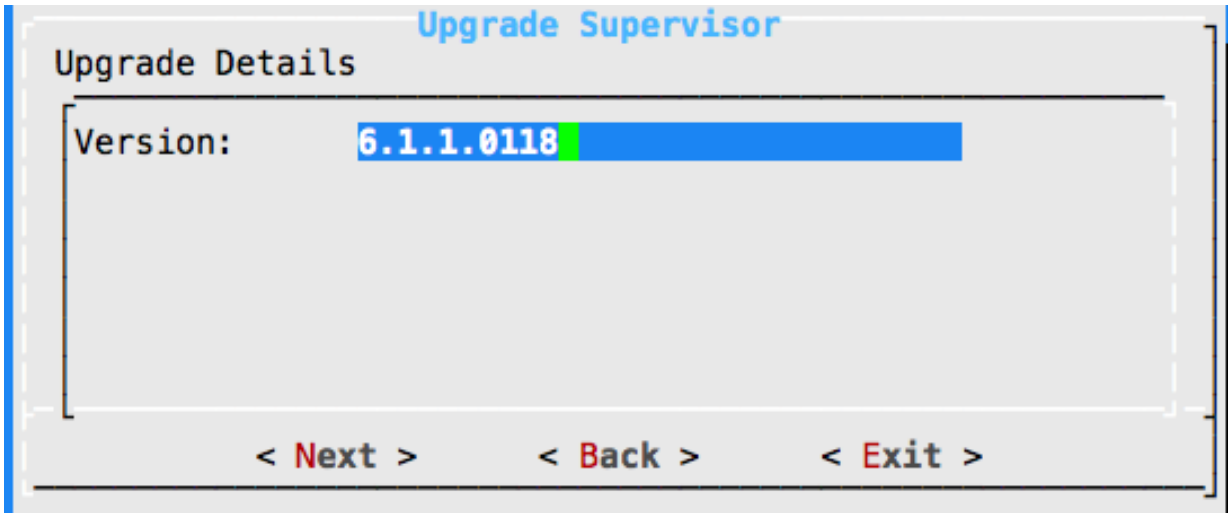
   b. Select **Supervisor** and click **Next**.



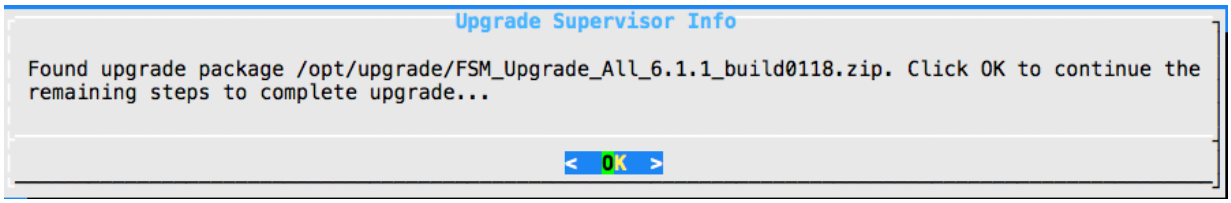
   c. Select **Upgrade** operation and click **Next**.



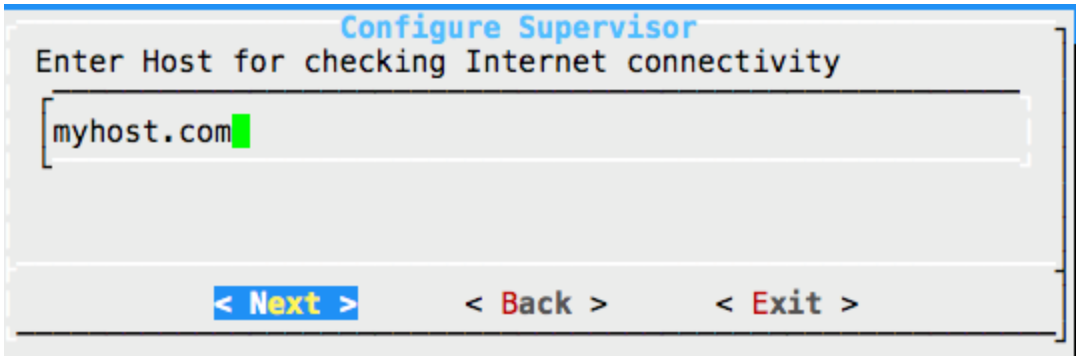
   d. Enter the version you want to upgrade to and click **Next**.



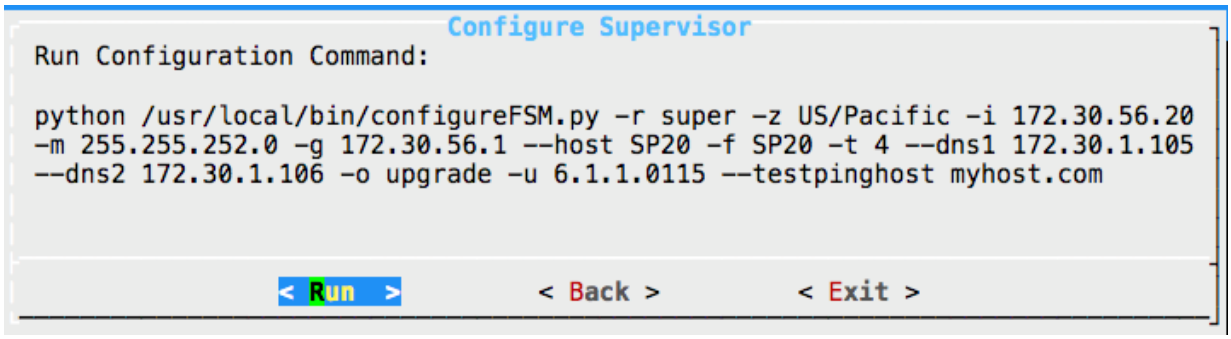
e. Once FortiSIEM finds the matching upgrade package, click **OK**.



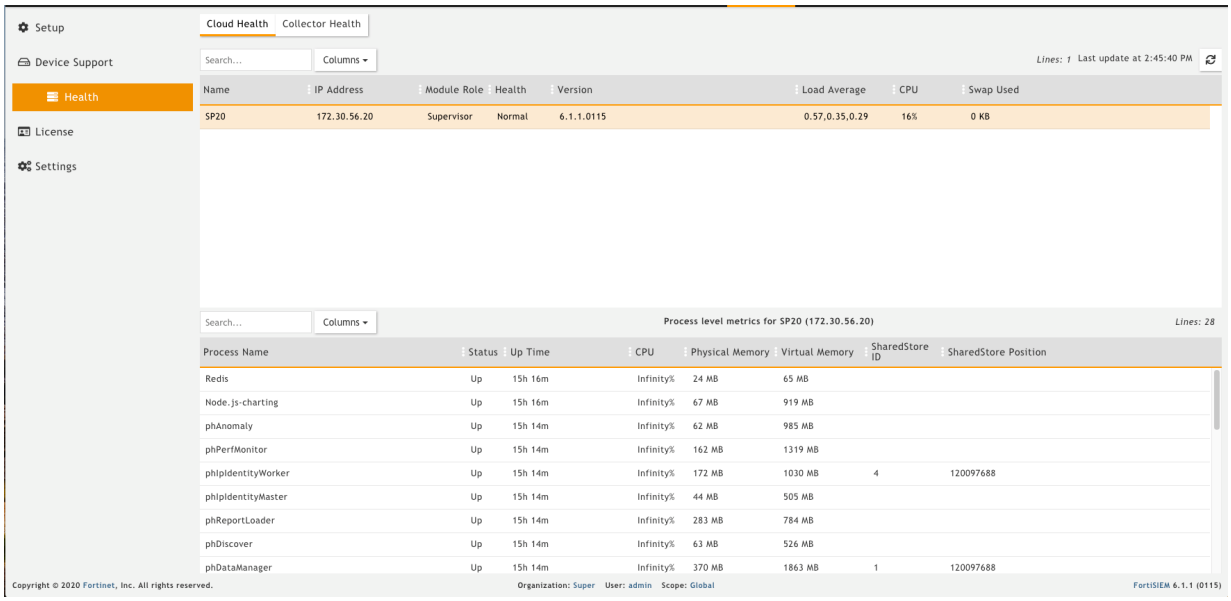
f. Enter a host name (`myhost.com` as an example) that can be resolved from the **Supervisor**, then click **Next**.
Note: Internet connectivity is the same as network connectivity.



g. Click **Run**.



5. Login to the Supervisor and make sure the upgrade succeeded.
   a. In the GUI, go to **Admin > Health > Cloud Health** to make sure it is running the upgraded version and that all processes are up and running.



b. Login via SSH and run `phstatus` to make sure that all processes are up and running.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  14:41:33 up 15:12,  1 user,  load average: 0.41, 0.30, 0.29
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 1.4%us, 0.6%sy, 0.0%ni, 97.5%id, 0.0%wa, 0.2%hi, 0.2%si, 0.0%st
Mem: 32768968k total, 17164828k used, 15604140k free, 5916k buffers
Swap: 26058744k total, 0k used, 26058744k free, 8642272k cached


PROCESS                 UPTIME          CPU%            VIRT_MEM        RES_MEM

phParser                15:10:07        0               2241m           793m
phQueryMaster           15:10:24        0               1073m           127m
phRuleMaster            15:10:24        0               1307m           689m
phRuleWorker            15:10:24        0               1378m           296m
phQueryWorker           15:10:24        0               1398m           189m
phDataManager           15:10:24        0               1863m           327m
phDiscover              15:10:24        0               524m            62m
phReportWorker          15:10:24        0               1440m           196m
phReportMaster          15:10:24        0               679m            151m
phIpIdentityWorker      15:10:24        0               1030m           157m
phIpIdentityMaster      15:10:24        0               505m            44m
phAgentManager          15:10:24        0               1476m           80m
phCheckpoint            15:10:24        0               333m            50m
phPerfMonitor           15:10:24        0               794m            71m
phReportLoader          15:10:24        0               784m            283m
phBeaconEventPackager   15:10:24        0               1129m           168m
phDataPurger            15:10:24        0               627m            86m
phEventForwarder        15:10:24        0               554m            53m
phMonitor               15:10:29        0               1283m           600m
Apache                  15:12:04        0               311m            16m
Node.js-charting        15:11:58        0               919m            67m
Node.js-pm2             15:11:57        0               0               9328
AppSvr                  15:11:55        0               11118m          3200m
DBSvr                   15:12:06        0               327m            33m
phAnomaly               15:10:27        0               985m            62m
phFortiInsightAI        15:12:06        0               13791m          354m
Redis                   15:11:58        0               65m             24m
```

Upgrade Cluster Deployment

- Overview
- Detailed Steps - Local Disk or NFS Storage
- Detailed Steps - Elasticsearch Storage

These instructions cover the upgrade process for FortiSIEM cluster deployment consisting the Supervisor, Workers and Collectors.

Overview

It is important to be aware of these steps while upgrading the FortiSIEM cluster. This is a general overview only; detailed steps will follow.

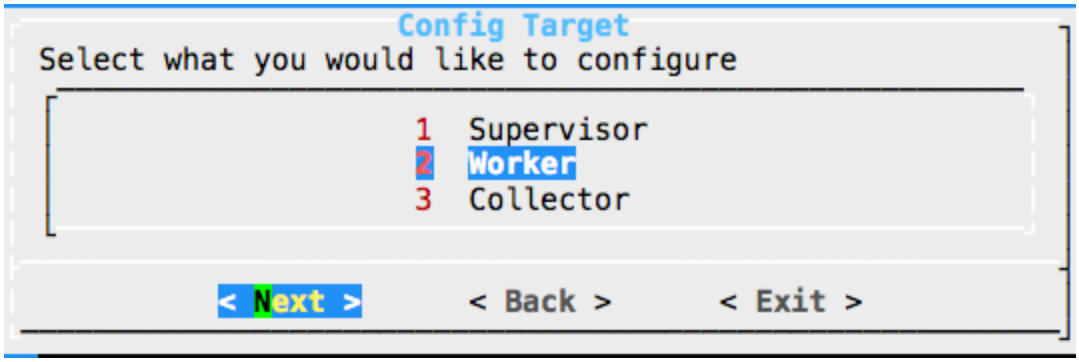
1. Shut down all Workers. Collectors can be up and running.
2. Upgrade Supervisor first (while all Workers are shutdown).
3. After Supervisor is up and running, upgrade Workers one by one.
4. Upgrade Collectors.

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

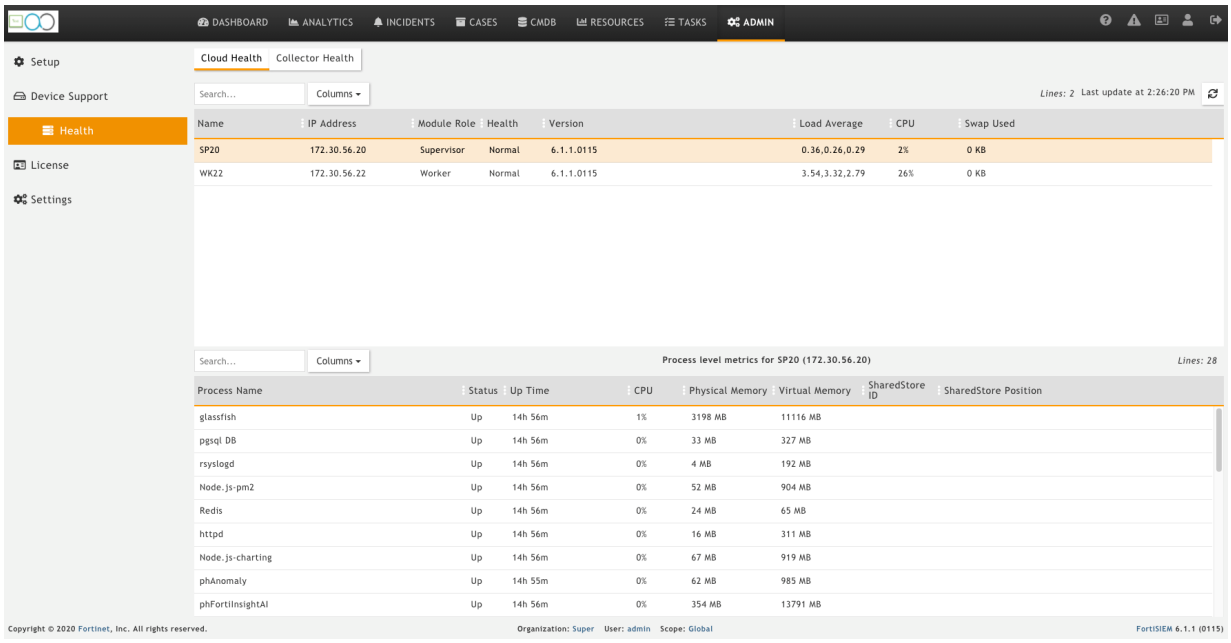
Note: Both the Supervisor and the Worker must be on the same FortiSIEM version, or else various software modules may not work properly. However, Collectors can be in an older version (one version older) - they will work, however they may not have the latest discovery and performance monitoring features in the Supervisor/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.

Detailed Steps - Local Disk or NFS Storage

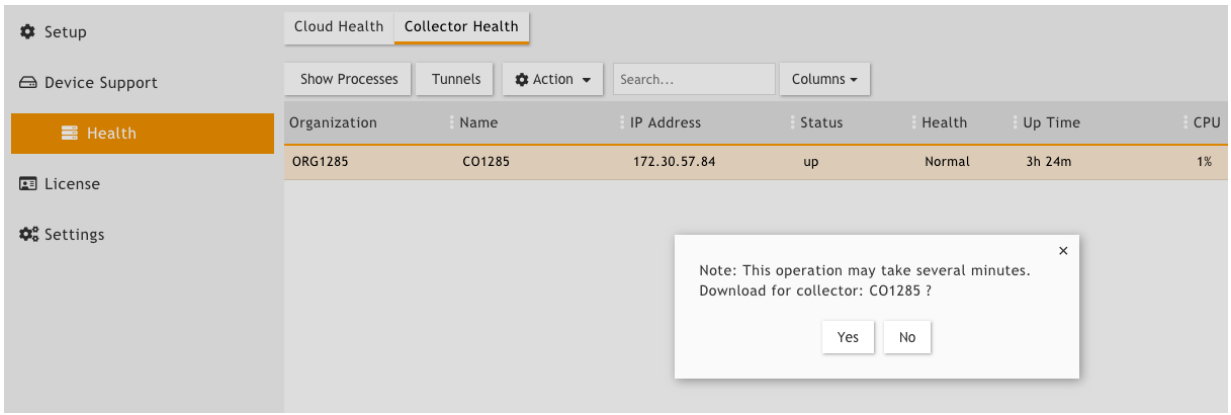
1. Shutdown all Worker nodes.
2. Upgrade Supervisor using the previous step. Make sure the Supervisor is running the version you have upgraded to and that all processes are up and running.
3. After upgrading the Supervisor, you can upgrade Workers one by one, the same way as the Supervisor. In this case, choose **Worker**.



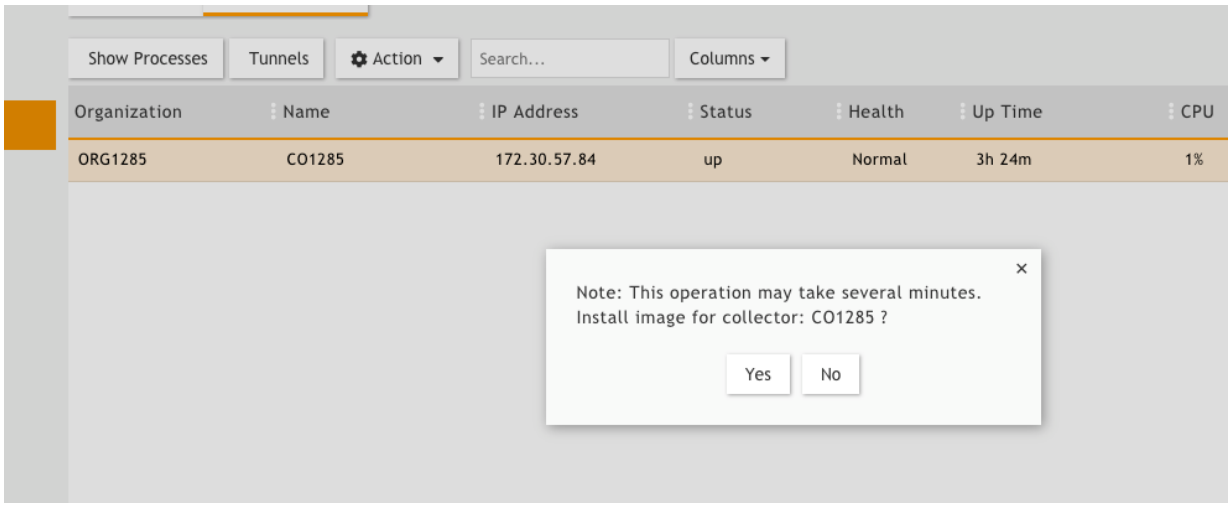
4. After you have upgraded all of the Workers, login to the Supervisor. Go to **Admin > Health > Cloud health** and make sure that all Workers are running the version you have upgraded to and that all processes are up and running. Note: Supervisor and Workers must be on the same version.



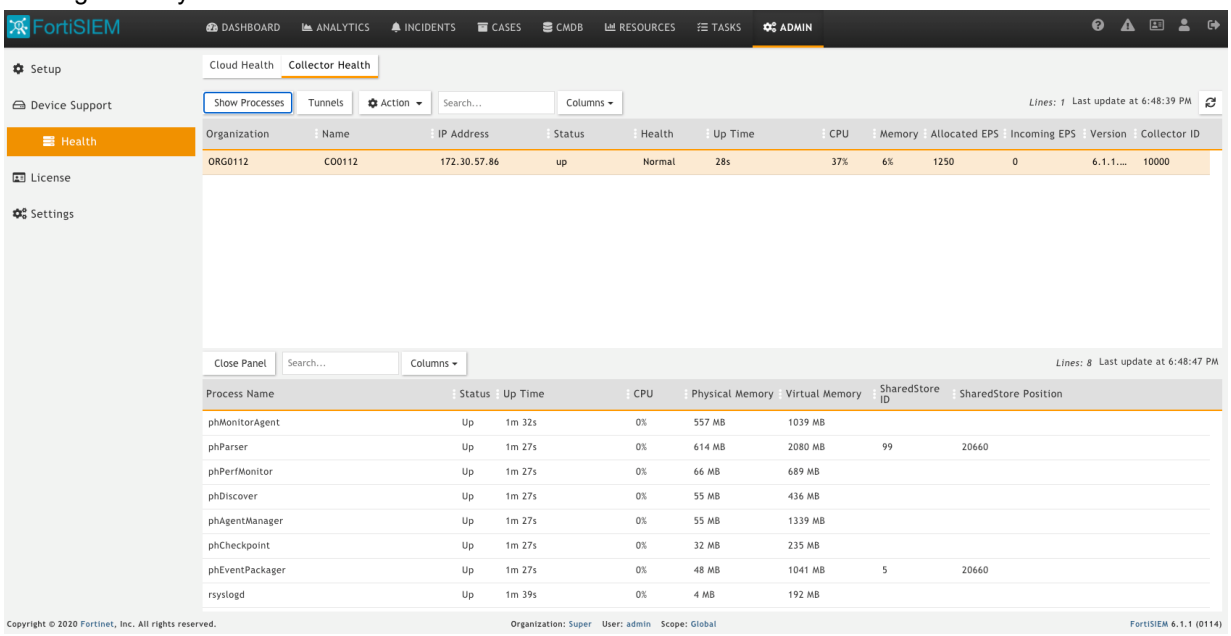
5. Upgrade Collectors running 6.1.0 or later.
   a. Login to the Supervisor via SSH as `root`.
   b. Setup upgrade by running `phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.1.2_build0119.zip <superIP>`.The command will copy the upgrade files to the right location and prepare collector download:
   c. Login to the FortiSIEM GUI.
   d. Go to the **ADMIN > Health > Collector Health** page.
   e. Select a Collector, then choose **Actions > Download Image**, then wait for completion.



   f. Select a Collector, then choose **Actions > Install Image**, then wait for completion.



g. Collector will upgrade, reboot and re-connect to the Supervisor. Check Collector Health to make sure it is running normally.



6. For pre-6.1.0 Collectors, FortiSIEM does not support Collector migration to 6.1.0 for VM based collectors. You will need to install new 6.1.2 Collectors and register them to 6.1.2 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. To do this follow these steps:

a. Preparation steps:

i. Copy the http hashed password file `/etc/httpd/accounts/passwds` from the old Collector.

ii. Disconnect the pre-6.1.0 Collector.

iii. Install the 6.1 Collector with the old IP address by the following the steps in **Cluster Installation > Install Collectors**.

iv. Copy the saved http hashed password file `/etc/httpd/accounts/passwds` from the old Collector to the 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.

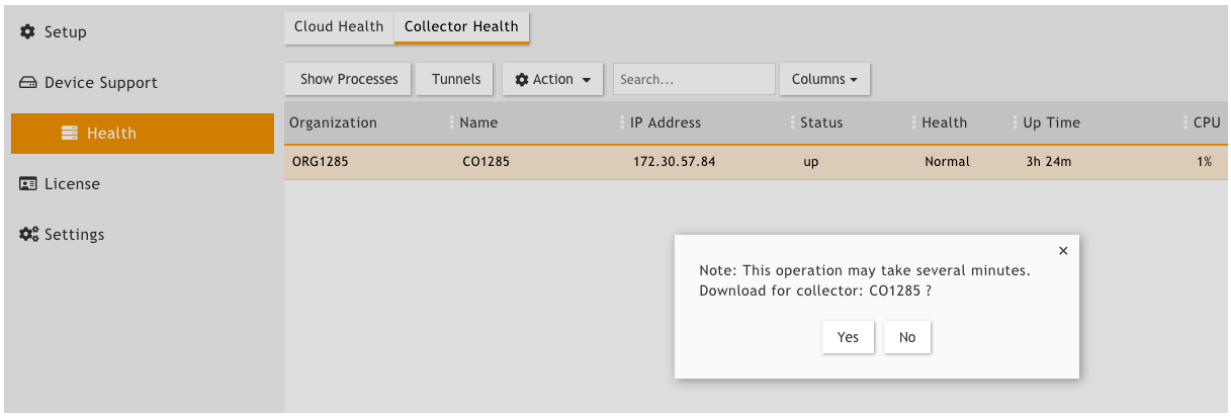
b. Register Collectors steps:
   i. Follow the steps in **Cluster Installation > Register Collectors**, with the following difference: in the `phProvisionCollector` command, use `--update` option instead of `--add`. Other than this, use the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use the `phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations: `# /opt/phoenix/bin/phProvisionCollector --update <user> <password> <Super IP or Host> <Organization> <CollectorName>`. Then, re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.

7. Follow steps in the 500F Collector Configuration Guide to upgrade 500F hardware based Collectors to 6.1.2.

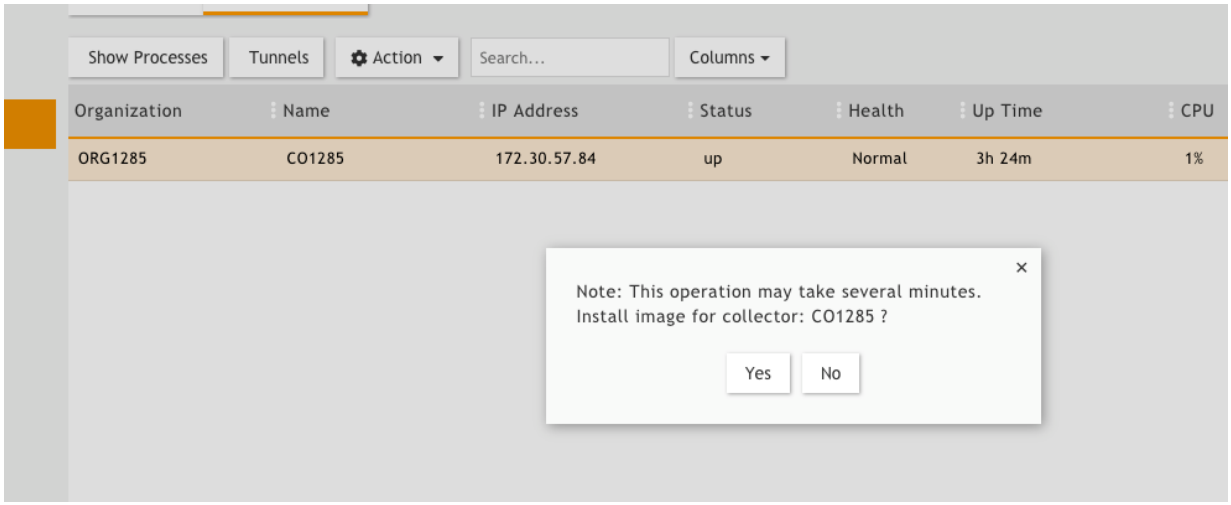
Detailed steps – Elasticsearch Storage

For Elasticsearch, 6.1.0 Workers cannot be upgraded to 6.1.2. You must delete the Workers from the Supervisor, upgrade the Supervisor, and then add back the Workers.

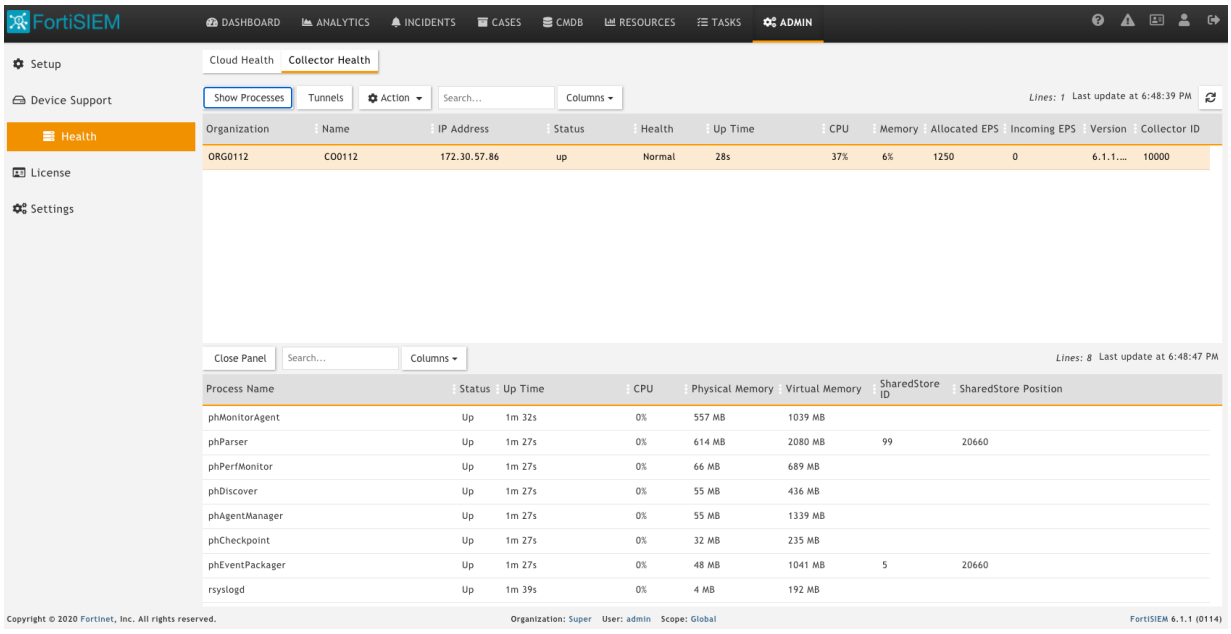
1. Delete the Workers as follows:
   a. Login to Supervisor.
   b. Go to **Admin > License > Nodes** and delete Workers one by one.
   c. Go to **Admin > Health > Cloud health** and make sure Workers do not appear.
   d. Go to **Admin > Event Worker** and delete the Workers.
   e. Shutdown the Workers.
2. Upgrade the Supervisor as in the Single node install. Then go to **Admin > Storage > Online > Elasticsearch** and click **Test and Save**. This important step pushes the latest event attribute definitions to Elasticsearch.
3. Install fresh Worker nodes based on your platform. See the appropriate Installation and Migration Guide for your platform here.
4. Add back the Workers to the Supervisor as follows:
   a. Login to Supervisor.
   b. Go to **Admin > License > Nodes** and add Workers one by one.
   c. Go to **Admin > Health > Cloud health** and make sure Workers appear.
   d. Go to **Admin > Event Worker** and add the Workers.
5. At this point, both Super and Worker must be running 6.1.0. Collectors must be sending events. Verify this from **Admin > Health > Cloud health**, **Admin > Health > Collector health**, and by running some reports.
6. Upgrade Collectors running 6.1.0 or later.
   a. Login to the Supervisor via SSH as `root`.
   b. Setup upgrade by running `phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.1.2_build0119.zip <superIP>`.The command will copy the upgrade files to the right location and prepare collector download:
   c. Login to the FortiSIEM GUI.
   d. Go to the **ADMIN > Health > Collector Health** page.
   e. Select a Collector, then choose **Actions > Download Image**, then wait for completion.



f. Select a Collector, then choose **Actions > Install Image**, then wait for completion.



g. Collector will upgrade, reboot and re-connect to the Supervisor. Check Collector Health to make sure it is running normally.



7. For pre-6.1.0 Collectors, FortiSIEM does not support Collector migration to 6.1.0 for VM based collectors. You will need to install new 6.1.2 Collectors and register them to 6.1.2 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. To do this follow these steps:
   a. Preparation steps:
      i. Copy the http hashed password file `/etc/httpd/accounts/passwds` from the old Collector.
      ii. Disconnect the pre-6.1.0 Collector.
      iii. Install the 6.1 Collector with the old IP address by the following the steps in **Cluster Installation > Install Collectors**.
      iv. Copy the saved http hashed password file `/etc/httpd/accounts/passwds` from the old Collector to the 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.
   b. Register Collectors steps:
      i. Follow the steps in **Cluster Installation > Register Collectors**, with the following difference: in the `phProvisionCollector` command, use `--update option instead of --add`. Other than this, use the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use the `phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations: `# /opt/phoenix/bin/phProvisionCollector --update <user> <password> <Super IP or Host> <Organization> <CollectorName>`. Then, re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.
8. Follow the steps in the 500F Collector Configuration Guide to upgrade 500F hardware based Collectors to 6.1.2.

Upgrade via Proxy

During upgrade, Super/Worker and Hardware appliances FSM-2000F and 3500F must be able to communicate with CentOS OS repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com`) hosted by Fortinet, to get the latest OS packages. Follow these steps to set up this communication via proxy, before initiating the upgrade.

1. SSH to the node.
2. Edit `/etc/yum.conf` as follows:
   - If your proxy does not require authentication, then add a line like this:
     - `proxy=http://<proxy-ip-or-hostname>:<proxy-port>`
   - If your proxy requires authentication, then add `proxy_username=` and `proxy_password=` entries as well. For example, for squid proxy:
     - `proxy_username=<user>`
     - `proxy_password=<pwd>`
3. Test that you can use the proxy to successfully communicate with the two sites: `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com`.
4. Begin the upgrade.