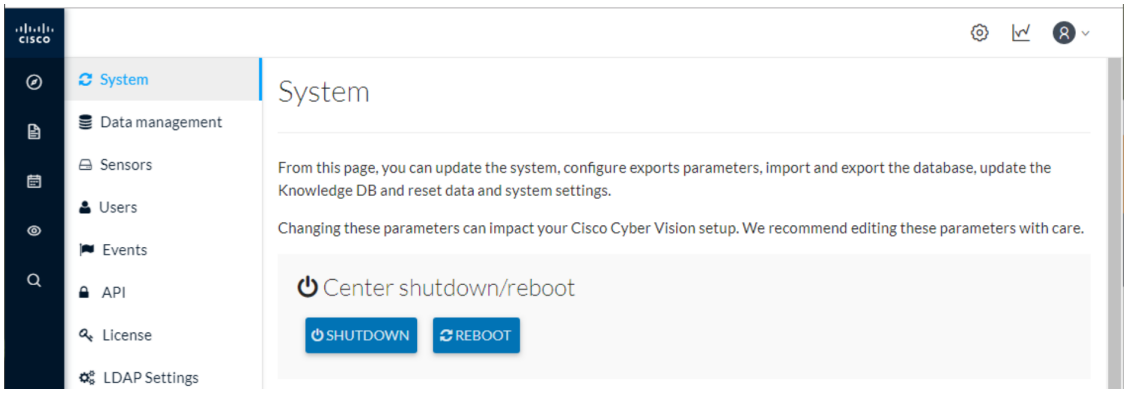
System

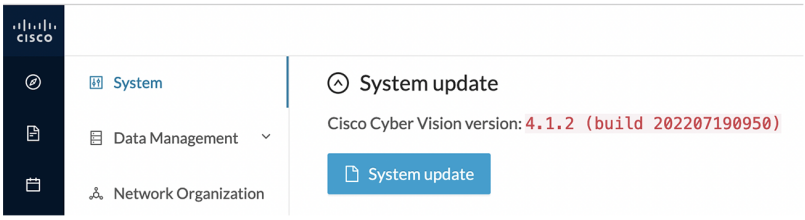
Center shutdown/reboot



You can trigger a safe shutdown and reboot of the Center from the System administration page.

The reboot can be used in case of a minor bug. For example, in case of a system overload.

Upgrade with a combined update file



Version releases include a combined update file for the Center, the SENSOR3, SENSOR5, SENSOR7 and the Cisco IC3000 Industrial Compute Gateway. If operating conditions make it possible, you can update the Center and these sensors at once from the GUI.

Note Make sure that all your sensors are connected by accessing the Sensor Explorer page, and SSH is authorized between the Center and the sensors before proceeding to a combined update.

Important Rolling back to an older Cisco Cyber Vision version is not possible.

Requirements:

- A combined update to retrieve from cisco.com.

To verify that the file you just downloaded is healthy, it is recommended to use the SHA512 checksum provided by Cisco.

To do so (Windows users):

Step 1 Retrieve the Cisco Cyber Vision combined update from cisco.com.

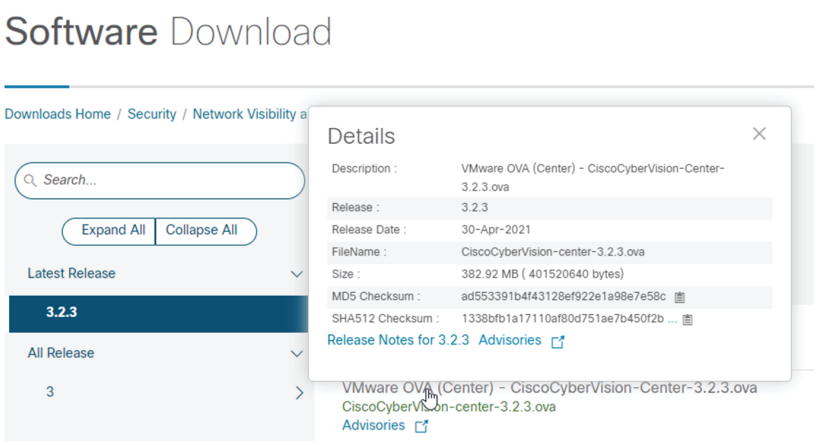
Step 2 Open a shell prompt such as Windows Powershell and use the following command to retrieve the file checksum:

Get-FileHash .\CiscoCyberVision-<TYPE>-<VERSION>.<EXT> -Algorithm SHA512 | Format-List

```
PS C:\Users\[redacted]> Get-FileHash .\Downloads\CiscoCyberVision-center-3.2.3.ova -Algorithm SHA512 | Format-List

Algorithm : SHA512
Hash      : 1338BFB1A17110AF80D751AE7B450F2B29CCB4CB54F550F38B8E6B4236865EC9EDF7773FD05D1055C7F1EF76E68C2B8A96CFE69AB
            1B622E4B0B88EBB9E94DB16
Path      : C:\Users\[redacted]\Downloads\CiscoCyberVision-center-3.2.3.ova
```

Step 3 In cisco.com, mouse over the file and copy the SHA512 checksum.



Step 4 Compare both checksums.

- If both checksums are identical it means the file is healthy.
- If the checksums do not match try to download the file again.
- If, after downloading the file again the checksums still don't match, please contact the support.

To update the Center and all applicable sensors:

Step 5 Access Cisco Cyber Vision's GUI.

Step 6 Navigate to Admin > System and use the System update button.

Step 7 Select the update file CiscoCyberVision-update-combined-<VERSION>.dat

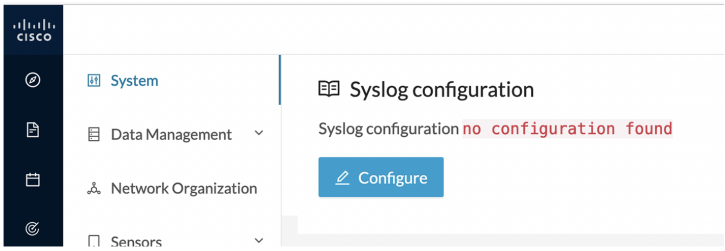
Step 8 Confirm the update.

As the Center and sensors updates proceed, you are redirected to a holding page. Once the update is finished the Center and the sensors need to reboot and you will be logged out from the user interface.

Step 9 Log in again.

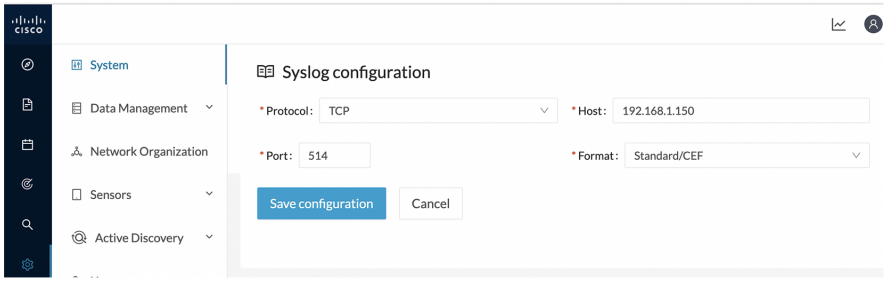
If sensors were offline when the update occurred, the same procedure can be used as many times as necessary to update all sensors.

Syslog configuration



Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. To configure which machine syslogs will be sent to:

Step 1 Click **Configure**.



Step 2 Select a protocol.

If you select TCP + TLS connection an additional "set certificate" button is displayed to import a p12 file. This file is to be provided by the administrator of your SIEM solution to secure communications between the Center and the syslog collector.

Step 3 Enter the IP address of the SIEM reachable from the Administration network interface (i.e. eth0) of the Center.

Step 4 Enter the port on the SIEM that will receive syslogs.

Step 5 Select the variant of syslog format:

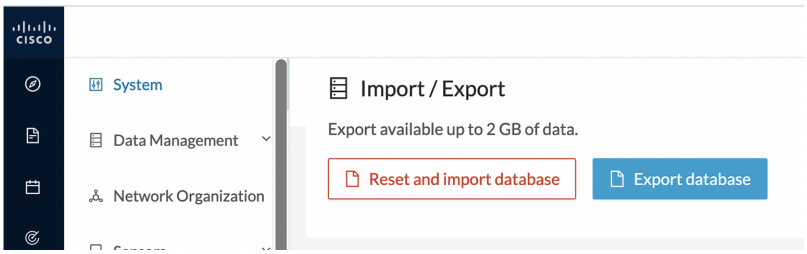
- Standard: event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).
- CEF: industry standard ("Common Event Format") which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.
- RFC3164: extended syslog header format with microsecond precision for timestamps.

Step 6 Click **Save configuration**.

Import/Export

You can import and export the Cisco Cyber Vision database from the System administration page.

This can be used on a regular basis to back up the industrial network data on Cisco Cyber Vision or if you need to transfer the database to a different Center.



Exports are possible up to 2 GB of data to avoid side effects related to slow database exports. If the database is larger than 2 GB, you will get an error message. In this case, you must connect to the Center using SSH and perform a data dump using the command `sbs db dump`.

Network data, events, users will be kept as well as all customizations (e.g. groups, component names).

As for configurations, only those made in Cisco Cyber Vision's GUI will be kept. Thus, if you change Center you will have to perform a basic configuration of the Center and then configure Cisco Cyber Vision again (refer to the corresponding Center Installation Guide).

Note Import can last up to one hour for big databases. However, you can refresh the page from time to time to check that the import keeps going on normally (i.e. no error message).

Knowledge DB

Cisco Cyber Vision uses an internal database which contains the list of recognized vulnerabilities, icons, threats, etc.

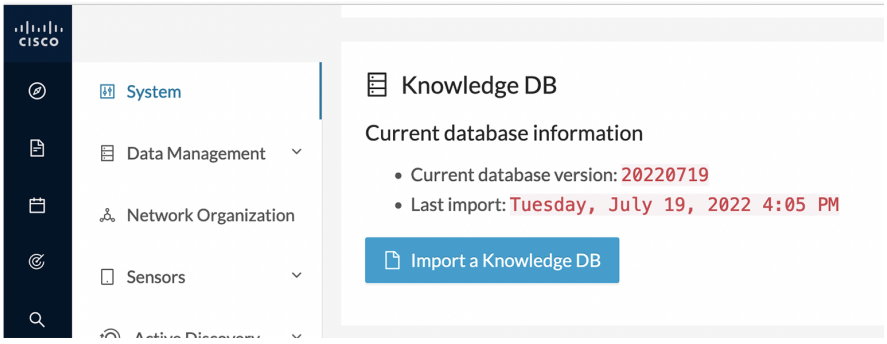
Important It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities.

To update the Knowledge DB:

Step 1 Download the latest.db file available from cisco.com.

Step 2 From the Cisco Cyber Vision system administration page click the **Import a knowledge DB** button to upload the file.

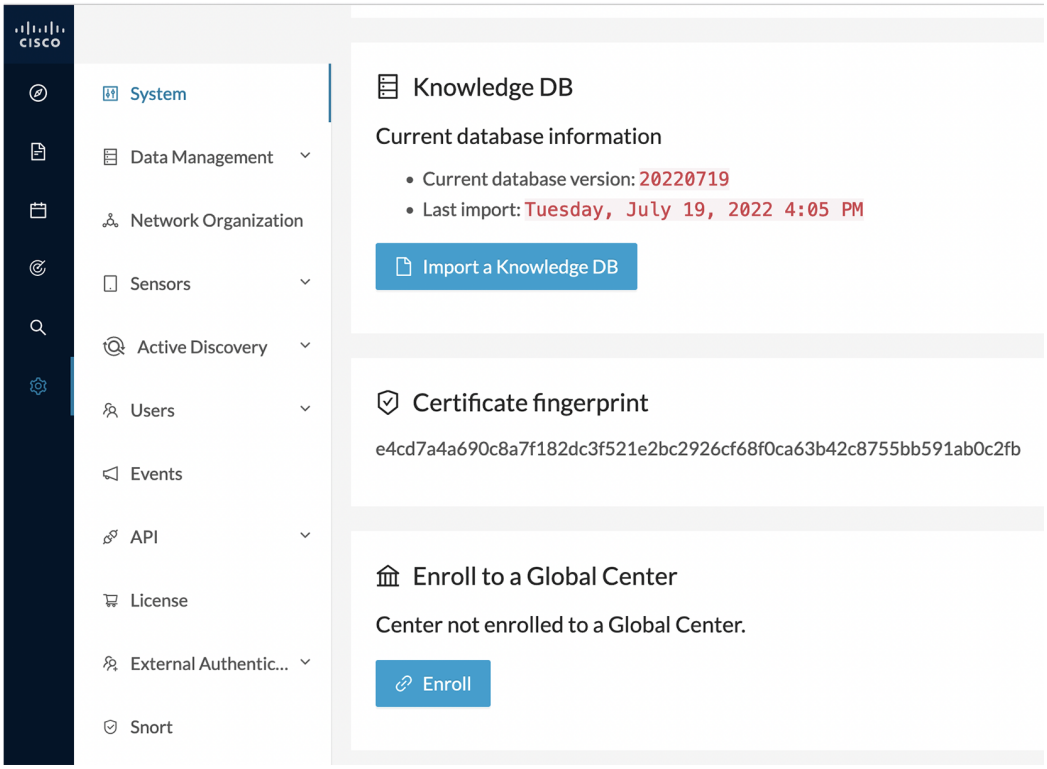
Importing the new database will rematch your existing components against any new vulnerabilities and update network data.



Certificate fingerprint

The certificate fingerprint is used to register a Global Center with its synchronized Centers and vice versa.

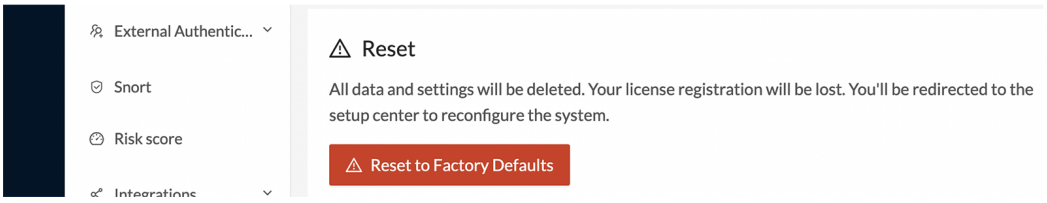
The Enroll button is used to enroll a Global Center with its synchronized Centers.



For more information, refer the Centers Installation Guides.

Reset to factory defaults

Resetting the system to factory defaults should be performed carefully with the help of Cisco product support and be used only as a last resort when all other troubleshooting attempts have failed. Please read below all implications of taking this action.



Reset to Factory Defaults is to be used as a last resort to clear all existing data from the Center.

Proceeding to a Reset to Factory Defaults will lead to the deletion of:

- Some Center configuration data elements.

- The GUI configuration (such as user accounts, the setup of event severities, etc.).
- Data collected by the sensors.
- The configuration of all known sensors (such as IP addresses, capture modes, etc.).

Root password, certificates and configurations from the Basic Center configuration will be kept.

Once a Reset to Factory Defaults has been performed, the GUI page refreshes with the Cisco Cyber Vision installation wizard (refer to the corresponding Center Installation Guides).