



Maintenance

- [Upgrade procedures, on page 1](#)
- [Replace SD card, on page 8](#)
- [Reconfigure/Redeploy a sensor, on page 9](#)
- [Certificate renewal, on page 13](#)

Upgrade procedures

Upgrade through the Cisco Cyber Vision sensor management extension

Before updating sensors, the Cisco Cyber Vision sensor management extension must be up-to-date.

It is possible to select which sensors to update. The update status will be visible in the [Management jobs](#) page.

Update the sensor management extension

The Cisco Cyber Vision sensor management extension must be up-to-date to update IOx sensors.

Procedure

- Step 1** Retrieve the sensor management extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) on cisco.com.
- Step 2** In Cisco Cyber Vision, navigate to Admin > Extensions.
- Step 3** Click **Update** to browse the new version of the extension file.

Extensions

From this page, you can manage Cyber Vision Extensions. Extensions are optional add-ons to Cyber Vision Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services.

Update
Uploading... Please do not quit or refresh the page.

Installed extensions

Name	Version	Actions
Cyber Vision sensor management	4.1.2	Update Remove

Update the sensors

Procedure

Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

Sensors that are not up-to-date have their version displayed in red.

Step 2 Click **Install sensor**, then **Update Cisco devices**.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebo time, you must authorize it so the Center can receive its data.

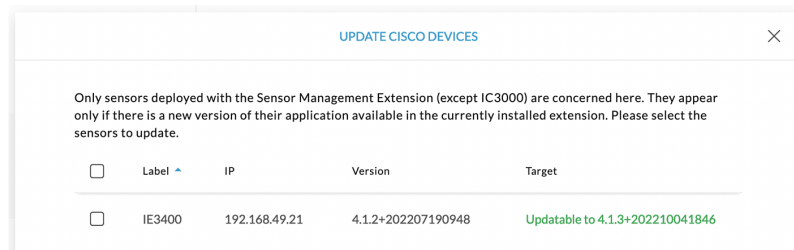
[Install sensor](#) [Manage Cisco devices](#) [Organize](#)
[Update Cisco devices](#) [Manage credentials](#)

Folders and sensors

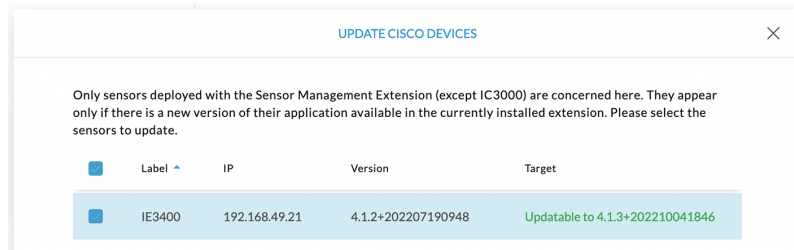
Filter 0 Selected MOVE SELECTION TO More Actions

	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FOLDER1			Lyon	
<input type="checkbox"/>	FOLDER2			Paris	
<input type="checkbox"/>	IC3000	192.168.49.23	4.1.1+202205161124		Connected
<input type="checkbox"/>	IE3400	192.168.49.21	4.1.2+202207190948		Connected

The update Cisco devices window pops up listing all sensors that have been deployed with the sensor management extension.

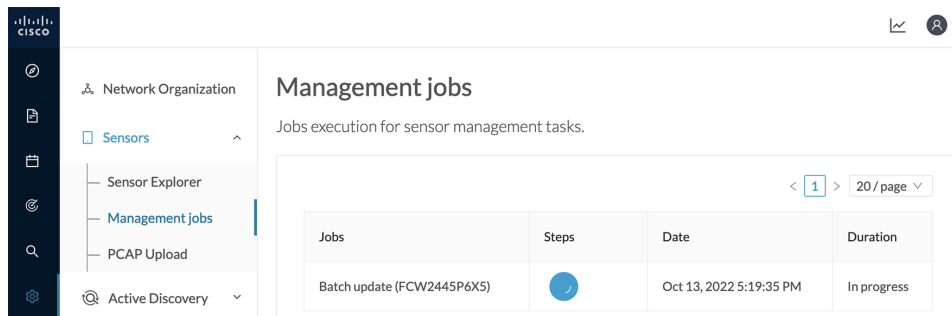


Step 3 Select the sensors you want to update.

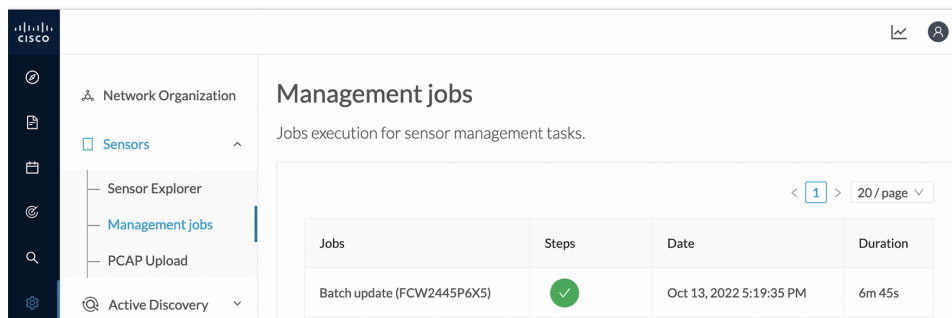


Step 4 Click **Update**.

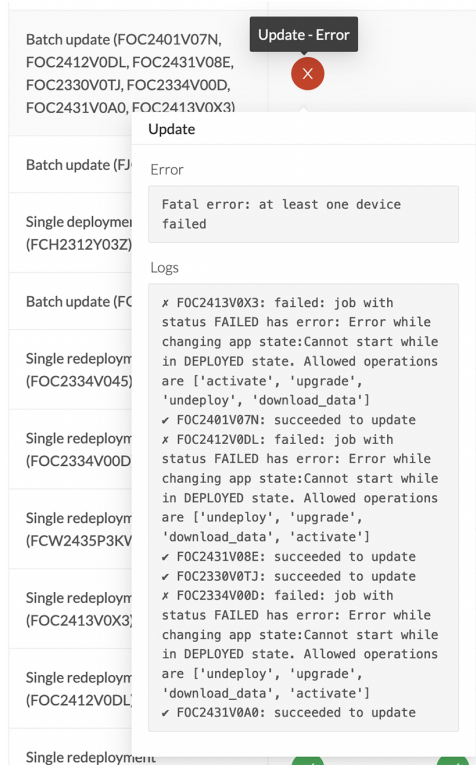
The sensors' update status appear in the Management jobs page in batches per sensor type and of maximum ten sensors per batch.



Herebelow the management jobs indicate that the batch of sensors updated successfully.



If the batch update fails, click the red update error icon to see logs.



Batch update (FOC2401V07N, FOC2412V0DL, FOC2431V08E, FOC2330V0TJ, FOC2334V00D, FOC2431V0A0, FOC2413V0X3)

Update - Error

Update

Error

Fatal error: at least one device failed

Logs

```
x FOC2413V0X3: failed: job with status FAILED has error: Error while changing app state:Cannot start while in DEPLOYED state. Allowed operations are ['activate', 'upgrade', 'undeploy', 'download_data']
✓ FOC2401V07N: succeeded to update
x FOC2412V0DL: failed: job with status FAILED has error: Error while changing app state:Cannot start while in DEPLOYED state. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate']
✓ FOC2431V08E: succeeded to update
✓ FOC2330V0TJ: succeeded to update
x FOC2334V00D: failed: job with status FAILED has error: Error while changing app state:Cannot start while in DEPLOYED state. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate']
✓ FOC2431V0A0: succeeded to update
```

Upgrade through the IOx Local Manager

The following section explains how to upgrade the sensor through the IOx Local Manager.



Note In the case of Cisco Cyber Vision upgrade for a Catalyst 9x00 from a release 4.1.2 or lower to a release 4.1.3, the update will fail due to the addition of the RSPAN option. The sensor application must be removed and deployed again.

In the example below, the sensor is upgraded from Cisco Cyber Vision version 3.2.2 to version 3.2.3.

Figure 1: The sensor in version 3.2.2 in the Sensors administration page of Cisco Cyber Vision

The screenshot displays the 'Sensors' administration page in Cisco Cyber Vision. The left sidebar contains navigation options: System, Data management, Sensors, Capture, Users, Events, API, License, LDAP Settings, Snort, Integrations, and Extensions. The main content area shows a table of sensors:

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.2+202103181619	Connected	Pending data	Unavailable	All	4d 1h 3m 47s
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	3m 27s

Below the table are action buttons: UPDATE CISCO DEVICES, DEPLOY CISCO DEVICE, INSTALL SENSOR MANUALLY, and IMPORT OFFLINE FILE. The details for the selected sensor (FOC2334V00H) are shown below:

- S/N: FOC2334V00H
- Name: FOC2334V00H
- IP address: 192.168.69.20
- Version: 3.2.2+202103181619
- System date (UTC): Monday, May 31, 2021 9:17 AM
- Status: Connected
- Processing status: Pending data
- Active discovery: Unavailable
- Deployment: Manual
- Uptime: 4d 1h 32m 47s
- Capture mode: All
- Start recording sensor
- Go to statistics

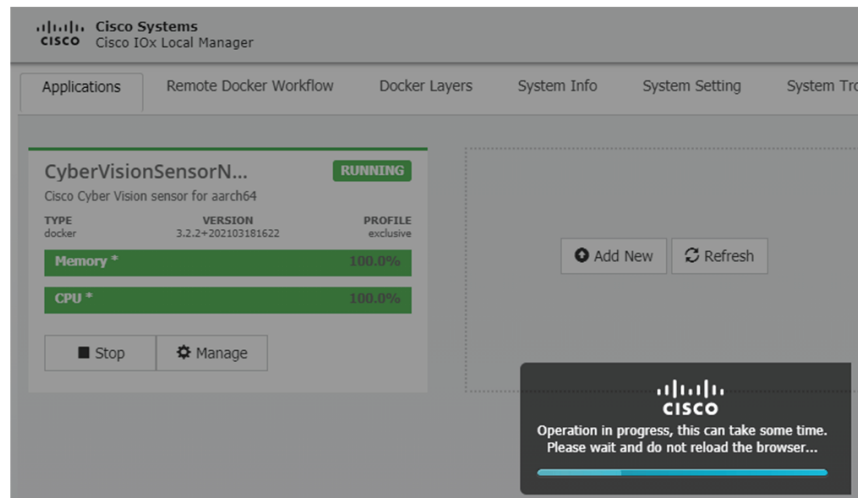
1. Access the IOx Local Manager.
2. Stop the application.

The screenshot shows the Cisco IOx Local Manager interface. The breadcrumb navigation is 'Configuration > Services > IOx'. The main content area displays the status of the 'CyberVisionSensorN...' application, which is currently 'RUNNING'. The application details include:

- TYPE: docker
- VERSION: 3.2.2+202103181622
- PROFILE: exclusive
- Memory *: 100.0%
- CPU *: 100.0%

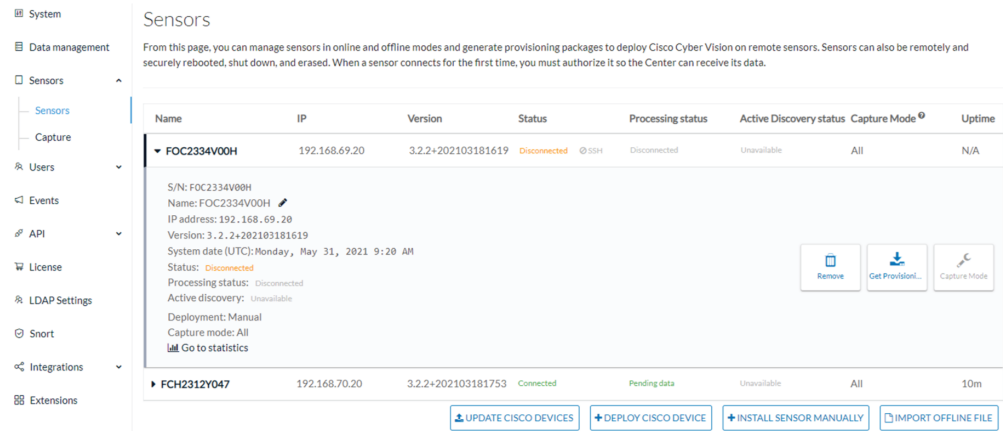
At the bottom of the application card, there is a 'Stop' button (highlighted with a red box) and a 'Manage' button.

The operation takes a few moments.



The application status switches to STOPPED.

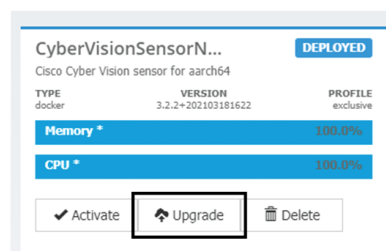
In Cisco Cyber Vision, the sensor status switches to Disconnected.



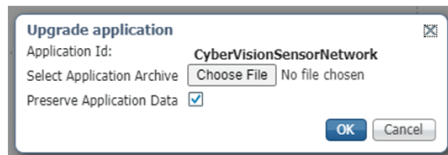
3. In the IOx Local Manager, click the **Deactivate** button.

The application status moves to DEPLOYED.

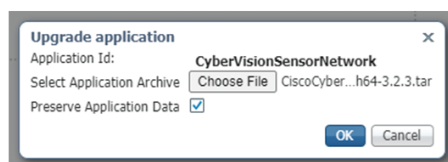
4. Click **Upgrade**.



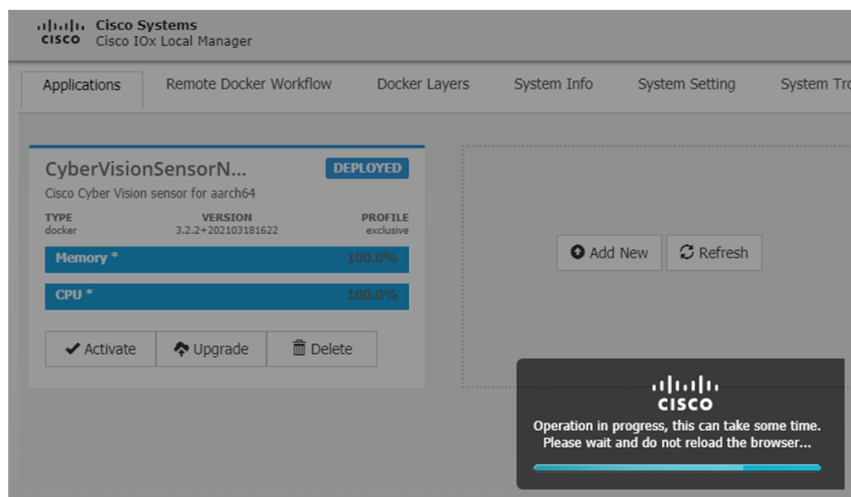
The pop up Upgrade application appears.



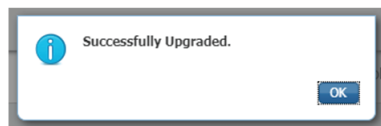
5. Select the **Preserve Application Data** option.
6. Select the new version of the application archive file.
e.g. CiscoCyberVision-IOx-aarch64-3.2.3.tar



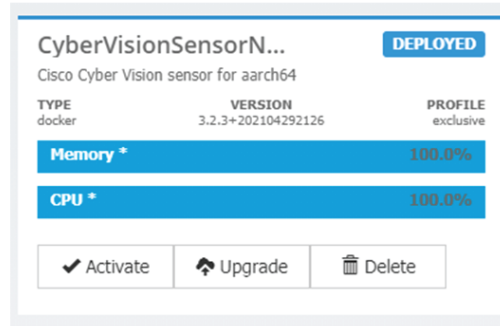
The operation takes a few moments.



A message indicating that the sensor has been successfully upgraded is displayed.



7. Check the number of the new version.
8. Click **Activate**.



9. Check configurations.

It can happen that network configurations are lost during the upgrade. If they are, refer to Configure the sensor virtual application in the [procedure with the Local Manager](#) corresponding to the switch used and do as explained.

10. Click the **Activate App** button.

The application status moves to ACTIVATED.

11. Click the **Start** button.

The application status changes to RUNNING.

In Cisco Cyber Vision, the sensor is upgraded from version 3.2.2 to 3.2.3 and its status moves to Connected.

Replace SD card

This section explains how to replace a SD card on a Cisco IE3x00.

Procedure

Step 1 Connect to the device CLI and use the following commands to disable IoX:

```
configure terminal
no iox
exit
```

Step 2 Replace the SD card.

Step 3 Format the SD card using the following command:

```
format sdflash: ext4
```

```
IE340CCV#format sdflash: ext4
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:". Continue? [confirm]
format completed with no errors

Format of sdflash: complete
IE340CCV#
```

Step 4 Enable IOx using the following command:

```
configure terminal
iox
```

```
IE340CCV#
IE340CCV#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IE340CCV(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device could occur.
IE340CCV(config)#
```

Step 5 Follow the instructions described in the following section to redeploy the sensor.

What to do next

[Reconfigure/Redeploy a sensor, on page 9](#)

Reconfigure/Redeploy a sensor

The Redeploy button is used when you need to replace a sensor model with another one keeping the same network configurations (e.g. replacing a Cisco IE3400 with a Cat 9300), change configurations, or if you need to reconfigure the sensor (e.g. to enable Active Discovery).

To do so:

Procedure

Step 1 On the Sensor Explorer page, click the sensor to reconfigure/redeploy. The sensor right side panel appears.

Step 2 Click **Redeploy**.

The screenshot shows the 'Sensor Explorer' interface. On the left is a navigation pane with 'Sensors' selected. The main area displays a table of sensors under 'Folders and sensors (3)'. The table has columns for Label, IP Address, Version, Location, Health status, and Pro. The sensor 'FCW2445P6X5' with IP '192.168.49.21' is highlighted. To the right, a details pane for this sensor shows its configuration and system health. At the bottom of the details pane, the 'Redeploy' button is circled in red.

A pop up asking to confirm the redeployment of the sensor appears.

Step 3 Click **OK** to proceed.

A summary of the sensor configuration is displayed. In this example, we're going to change the Collection VLAN number.

Step 4 Click **Start**.

Redeploy Cisco device

Get Cisco device configuration

The current configuration of your Cisco device enables you to:

- Reconfigure the Cyber Vision IOx sensor app on this device;
- Reconfigure your Cisco device for Cyber Vision (i.e modify the IP address);
- Deploy the Cyber Vision IOx sensor app on a new device using this configuration.

Device IP: 192.168.49.20	Device port: 443
Capture IP address: 169.254.1.2	Capture prefix length: 30
Capture VLAN number: 2508	Collection IP address: 192.168.49.21
Collection prefix length: 24	Collection VLAN number: 507
Use global credentials: No	Disk size: Use as much space as possible
Active Discovery interfaces: 192.168.50.21/24 VLAN#50	

Exit

Start

Step 5 Enter the credentials to reach the sensor to redeploy and click **Connect**.

Redeploy Cisco device

Reach Cisco device

Please fill the fields below to enable Cisco Cyber Vision to reach your device.

IP address*

Port*

For example 443 or 8443

Center collection IP

leave blank to use current collection IP

Credentials

Login*

Password*

[Exit](#)

[Connect](#)

Step 6 Click the blue link to fill the warning fields with the current sensor configuration. We change the Collection VLAN number value to 49.

Redeploy Cisco device

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

[Click here to fill the warning fields with the current sensor configuration](#)

Cisco device: IE-3400-8T2S

Capture IP address*

Capture prefix length*

Like 24, 16 or 8

Capture VLAN number*

Collection IP address*

Collection prefix length*

Like 24, 16 or 8

Collection gateway

Collection VLAN number*



[Exit](#)

[Next](#)

Step 7

Click **Next**.

Step 8

You can enable Active Discovery selecting Passive and Active Discovery.

Step 9

Click **Deploy**.

A message saying that the sensor is being redeployed appears. You can either go the jobs page or go back to the Sensor Explorer page.

Step 10

Click **Go to the jobs page**.

Redeploy Cisco device

Done!

The Cyber Vision IOx sensor application is being redeployed on your device. A job has been created to track deployment progress.

What's next?

[Back to Sensor Explorer](#)

[Go to the jobs page](#)

You are redirected to the [Management jobs page](#) to see the redeployment advancement. This can take several minutes.

The screenshot shows the 'Management jobs' page with a sidebar on the left containing navigation options like System, Data Management, Network Organization, Sensors, Sensor Explorer, and Management jobs. The main content area displays a table of jobs. A single job, 'Single redeployment (FCW2445P6X5)', is shown with a progress bar consisting of four steps. The first step is completed (green checkmark), and the second step is in progress (blue circle). The third and fourth steps are not yet started (grey circles). The duration is listed as 'In progress'.

Jobs	Steps	Duration
Single redeployment (FCW2445P6X5)		In progress

If you go back to the Sensor Explorer page, you will see that the sensor is in Redeploying status.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors (3)

[Filter](#) 0 Selected Move selection to [More Actions](#) As of: Feb 23, 2022 4:50 PM [Refresh](#)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery
<input type="checkbox"/>					Disconnected	Disconnected	
<input type="checkbox"/>					Disconnected	Disconnected	
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21			Redeploying	Not enrolled	Unavailable

Once the redeployment is finished, the sensor will switch status to connected and the Active Discovery to Enabled.

<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	a minute
--------------------------	-------------	---------------	--------------------	--	-----------	--------------	---------	----------

Certificate renewal

The certificates generated by Cisco Cyber Vision have a validity of two years.

Sensor certificates must be renewed manually. The procedure used differs whether the certificate is already expired or not and whether the sensor has been deployed using the sensor management extension.

- If the certificate is still valid, refer to [Sensor certificate renewal, on page 14](#).
- If the sensor was deployed with the sensor management extension, refer to [Sensor certificate renewal, on page 14](#).

- If the certificate is outdated, and was deployed manually, refer to [Sensor certificate renewal through the Local Manager, on page 17](#).

Sensor certificate renewal

The following procedure applies to:

- Sensors deployed with the sensor management extension, whether the certificate expiration date is exceeded or not (i.e. the deployment method is indicated in the sensor's right side panel).

The screenshot shows the 'Sensor Explorer' interface. At the top right, there is a notification for 'System issues Actions required'. The main area is divided into two panels. The left panel shows a list of sensors under 'Folders and sensors (3)'. A yellow alert box indicates '2 sensor certificates expired'. The right panel shows details for sensor 'FOC2330V0T0', including its label, serial number, IP address, version, and system date. The 'Deployment' method is highlighted as 'Sensor Management Extension'. Below the details are buttons for 'Move to', 'Capture mode', 'Redeploy', and 'Uninstall'.

Label	IP Address	Version
FCH2309Y01Z	192.168.49.23	4.2.2+202306261711
FCW2445P6X5	192.168.49.21	4.2.2+202306261519
FOC2330V0T0	192.168.49.41	4.2.2+202306261519

Details for FOC2330V0T0:

- Label: FOC2330V0T0
- Serial Number: FOC2330V0T0
- IP address: 192.168.49.41
- Version: 4.2.2+202306261519
- System date: Jul 6, 2023 11:26:00 AM
- Deployment: **Sensor Management Extension**
- Active Discovery: Unavailable
- Capture mode: All
- System Health: Status: Connected
- Processing status: Normally processing
- Uptime: 18 hours

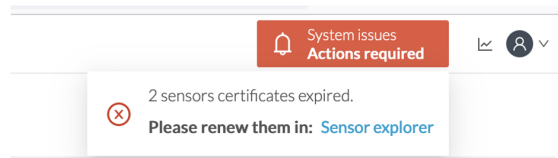
- In the case of sensors deployed manually, it only applies if the sensors certificate have not expired yet (i.e. the sensor certificate status is Expire Soon).

If sensors have been deployed manually and the certificate expiration date is exceeded, refer to [Sensor certificate renewal through the Local Manager, on page 17](#).

Procedure

Step 1

In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer or click the top banner alert to access the Sensor Explorer page directly.



Another alert is displayed.

System issues
Actions required

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

2 sensor certificates expired and 1 will expire soon [Manage certificates](#)

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors (3)

Filter 0 Selected Move selection to [More Actions](#) As of: Jul 6, 2023 11:25 AM

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Connected	Normally pro
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally pro
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally pro

Step 2 Click **Manage certificates** in the alert or **Manage Cisco devices > Manage certificates**.

System issues
Actions required

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

2 sensor certificates expired and 1 will expire soon [Manage certificates](#)

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors

Update Cisco devices
Manage credentials
Manage certificates

Filter 0 Selected [More Actions](#) As of: Jul 6, 2023 11:26 AM

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
--------------------------	-------	------------	---------	----------	---------------	-------------------

The **Manage sensors certificates** window opens.

MANAGE SENSORS CERTIFICATES

Select a sensor to renew its certificate.
If a sensor cannot be selected, it means that its certificate cannot be renewed automatically.

Filter

Certificate status is Expired × Certificate status is Expiring Soon ×

	Sensor Label	IP	Certificate Status	Expiration Date
<input type="radio"/>	FCH2309Y01Z	192.168.49.23	Expired	Jul 2, 2023
<input type="radio"/>	FOC2330V0T0	192.168.49.41	Expired	Jul 2, 2023
<input checked="" type="radio"/>	FCW2445P6X5	192.168.49.21	Expiring Soon	Jul 14, 2023

Cancel Renew certificate

Step 3 Select the sensor with the status Expiring Soon.

Step 4 Click **Renew certificate**.

MANAGE SENSORS CERTIFICATES

Select a sensor to renew its certificate.
If a sensor cannot be selected, it means that its certificate cannot be renewed automatically.

The certificate has been successfully renewed. ×

Filter

Certificate status is Expired × Certificate status is Expiring Soon ×

	Sensor Label	IP	Certificate Status	Expiration Date
<input type="radio"/>	FOC2330V0T0	192.168.49.41	Expired	Jul 2, 2023
<input type="radio"/>	FCH2309Y01Z	192.168.49.23	Expired	Jul 2, 2023
<input type="radio"/>	FCW2445P6X5	192.168.49.21	Valid	Sep 3, 2025

Cancel Renew certificate

The certificate is renewed and automatically sent to the sensor. Its status switches to Valid and the new expiration date appears.

Sensor certificate renewal through the Local Manager

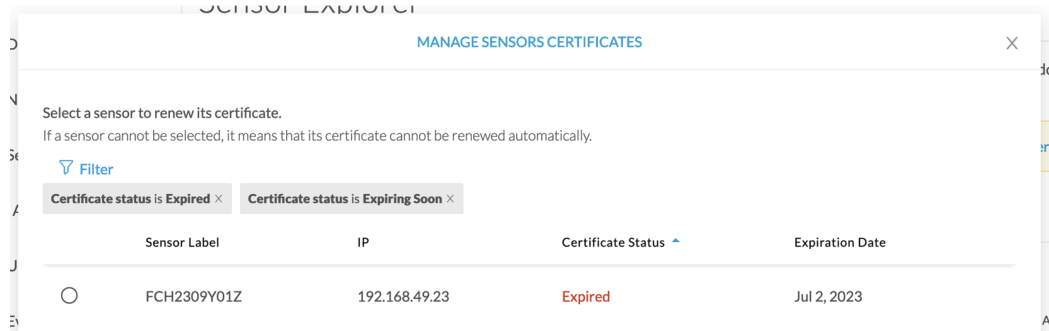
In case of certificate expiration, communication with the sensor is no longer possible if it was deployed manually (i.e. without the sensor management extension). In this case, the certificate is renewed by sending it to the sensor manually. As the certificate is part of the provisioning package, the action consists in generating the provisioning package and sending it to the sensor application through the Local Manager.

The screenshot shows the Cisco Sensor Explorer interface. At the top right, there is a red notification banner that says "System issues Action required". Below this, the "Sensor Explorer" page is displayed. A yellow warning box indicates "1 sensor certificate expired". Below the warning, there are three buttons: "Install sensor", "Manage Cisco devices", and "Organize". A table titled "Folders and sensors (3)" lists three sensors. The first sensor, FCH2309Y01Z, is highlighted. To the right of the table, a detailed view for the selected sensor is shown, including its label, serial number, IP address, version, system date, and deployment method (Manual). Below the details, there are several action buttons: "Go to statistics", "Start Recording", "Move to", "Download package", "Capture mode", "Enable IDS", "Reboot", "Shutdown", and "Uninstall".

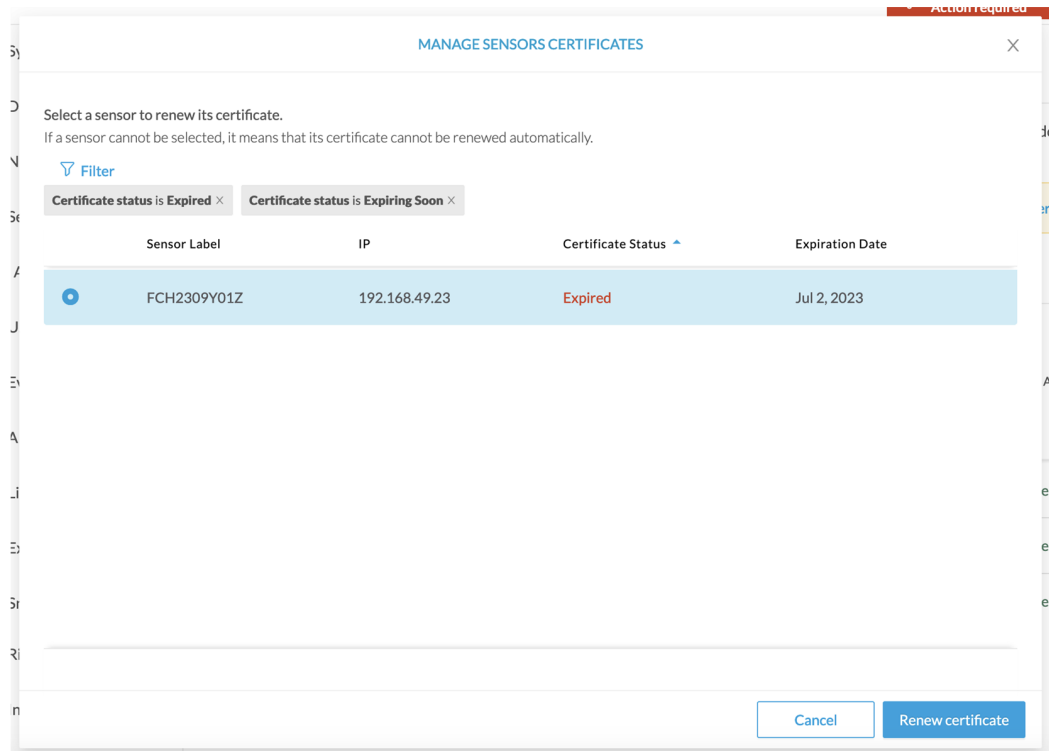
Label	IP Address	Version
FCH2309Y01Z	192.168.49.23	4.2.2+202306261711
FCW2445P6X5	192.168.49.21	4.2.2+202306261519
FOC2330V0T0	192.168.49.41	4.2.2+202306261519

Procedure

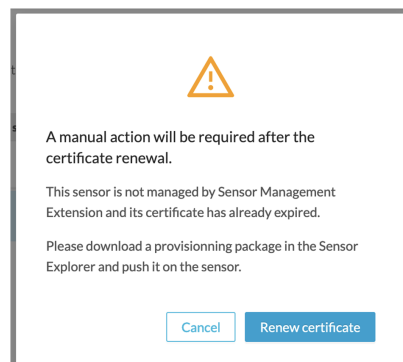
- Step 1** In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.
- Step 2** Click **Manage Certificates**.
- The Manage sensors certificates window appears.



Step 3 Select the sensor and click **Renew Certificate**.



A message is displayed.



Step 4 Click **Renew certificate** again.

The sensor certificate status appears as valid.

Sensor Label	IP	Certificate Status	Expiration Date
FCW2445P6X5	192.168.49.21	Valid	Sep 3, 2025
FOC2330V0T0	192.168.49.41	Valid	Sep 3, 2025
FCH2309Y01Z	192.168.49.23	Valid	Sep 3, 2025

Step 5 Close the Manage sensors certificates window.

The sensor's health and processing status appear as Disconnected.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors (3)

[Filter](#) 0 Selected Move selection to [More Actions](#) As of: Jul 6, 2023 11:41 AM [Refresh](#)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Di
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Disconnected	Disconnected	Disa
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally processing	Unav
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally processing	Unav

Step 6 Click the sensor in the list.

Its right side panel opens.

Step 7 Click the **Download package** button.

The screenshot shows the 'Sensor Explorer' interface. On the left, there's a list of 'Folders and sensors (3)'. The table below shows three sensors:

<input type="checkbox"/>	Label	IP Address	Version	Lo
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711	
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519	
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519	

On the right, the detailed view for sensor 'FCH2309Y01Z' is shown. It includes the following information:

- Label: FCH2309Y01Z
- Serial Number: FCH2309Y01Z
- IP address: 192.168.49.23
- Version: 4.2.2+202306261711
- System date: Jul 6, 2023 11:36:49 AM
- Deployment: Manual
- Active Discovery: Disabled
- Capture mode: All
- System Health: Status: **Disconnected**, Processing status: **Disconnected**, Uptime: N/A

Below the system health, there are several action buttons: 'Go to statistics', 'Move to', 'Download package' (highlighted with a red box), 'Enable IDS', 'Reboot', 'Shutdown', and 'Uninstall'.

Step 8**Step 9**

Import the provisioning package in the Local Manager. To do so, refer to [Import the provisioning package](#).

Step 10

The sensor's health status switches to Connected and its processing status to Normally processing.



Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#)
[🔗 Manage Cisco devices](#)
[📁 Organize](#)

Folders and sensors (3)

[Filter](#)
0 Selected
Move selection to
[More Actions](#)
As of: Jul 6, 2023 11:56 AM

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Di
<input type="checkbox"/>	⇒ FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Connected	Normally processing	Disal
<input type="checkbox"/>	⇒ FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally processing	Unav
<input type="checkbox"/>	⇒ FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally processing	Unav

