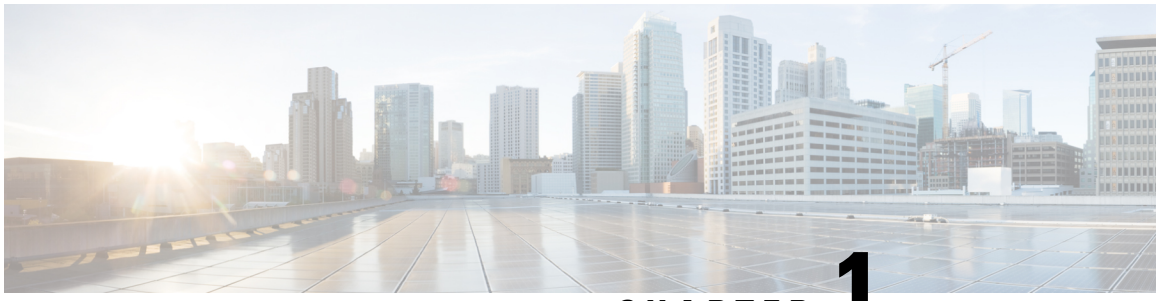
Cisco Cyber Vision Network Sensor Installation Guide for Cisco IC3000, Release 4.4.1

First Published: 2021-01-01

Last Modified: 2023-12-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

About this documentation

Document purpose

This installation guide describes how to perform a clean installation of Cisco Cyber Vision on a Cisco IC3000 Industrial Compute Gateway.

This documentation is applicable to **system version 4.4.1**.

Warnings and notices

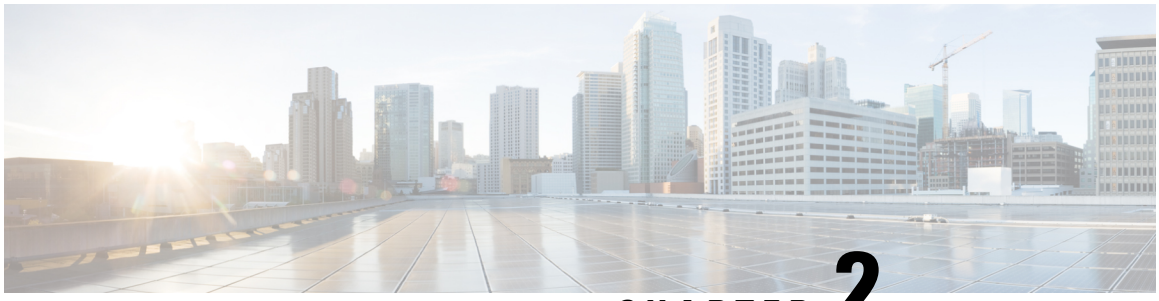
This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.

Warning Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

Important Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

Note Indicates important information on the product described in the documentation to which attention should be paid.



CHAPTER 2

Overview

Overview

The Cisco IC3000 Industrial Compute Gateway is an edge computing platform which extends the cloud computing paradigm to the edge of the network. The Cisco IC3000 captures traffic in SPAN mode. It contains two RJ45 10/100/1000 BaseT connectors ports and two SFP fiber ports to connect switches in port mirroring.

To deploy the Cisco Cyber Vision sensor application in the Cisco IC3000, follow the initial configuration:

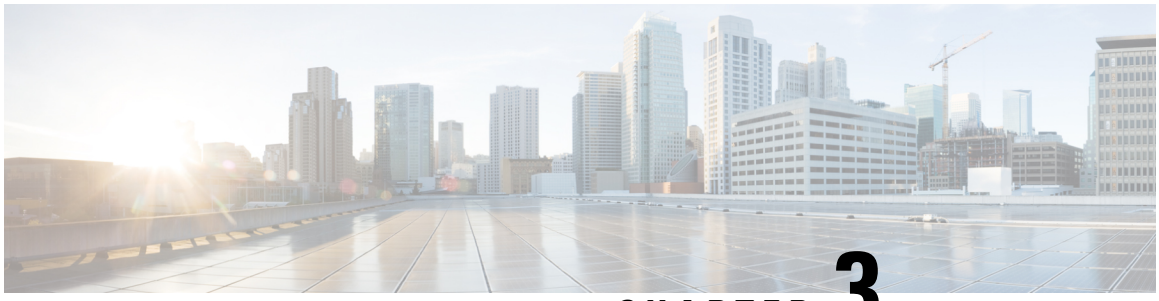
Take a moment to look at the Cisco IC3000 front view and Connect the Cisco IC3000. Proceed with the Cisco IC3000 platform initial configuration if it has never been done to configure a Local Manager IP and admin account. Eventually, Configure date and time.

Then, proceed with one of the installation methods available:

- Procedure with the Sensor management extension, on page 13. The file is available on cisco.com (recommended).
- Procedure with the Local Manager, on page 23.

To upgrade the sensor hosted in the Cisco IC3000, refer to one of the methods available:

- If the sensor management was used to deploy the sensor, Upgrade through the Cisco Cyber Vision sensor management extension.
- Upgrade through the Local Manager.

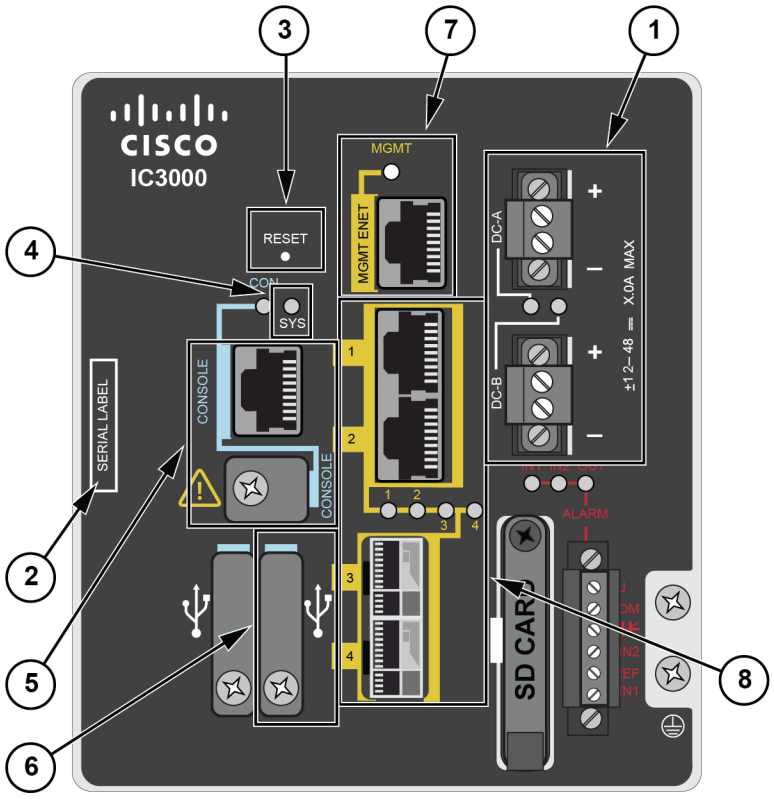


CHAPTER 3

Initial configuration

Cisco IC3000 front view

Before starting, take a moment to note and unscrew the following parts you're going to use during the procedure.



- DC-in connectors **(1)**
- Serial number **(2)**
- Reset pinhole **(3)**
- SYS LED **(4)**
- Console connectors **(5)**: RJ-45 and mini-USB
- USB port 2 **(6)**
- MGMT Ethernet port **(7)**: Local Manager and Collection network interfaces
- Industrial Network Interfaces **(8)**: 2x RJ45 10/100/1000 BaseT connectors and 2x SFP fiber ports

Connect the Cisco IC3000

The Cisco IC3000 contains 4 independent ports which can be used to capture in SPAN mode or to do active scanning on the network. Depending on the port usage the corresponding switch port must have the right configuration (SPAN or access).

The Cisco IC3000's Industrial network interface to do the dPI is to be connected to **switches configured in port mirroring only**.

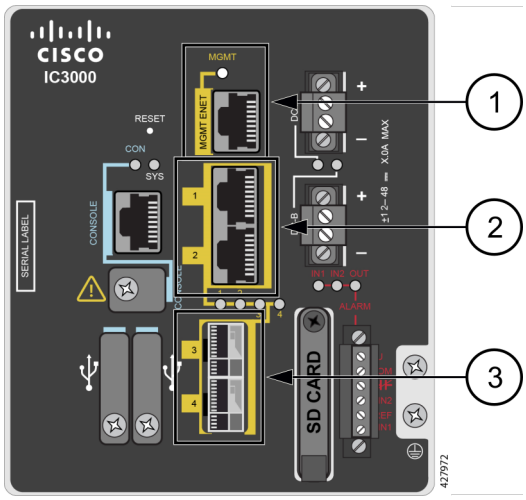
To connect the network interfaces to the Cisco IC3000:

Procedure

Step 1 Connect the Collection network interface (IC3000 to Center) to the MGMT ENET port **(1)**.

Step 2 Connect the Industrial network interface (IC3000 to on-site switches) to ports 1, 2, 3, 4 (up to 4 switches configured in port mirroring or access depending on the port usage).

Step 3
- Ports 1 and 2 are RJ45 10/100/1000 BaseT Connectors **(2)**.
- Ports 3 and 4 are SFP fiber ports **(3)**.



Connect to the Cisco IC3000 with the serial console

This section describes how to establish a connection to the Cisco IC3000 from Windows 10 using PuTTY. It is required to perform a sensor management extension installation and to enable Active Discovery (optional) when performing a manual installation.

Note This procedure will also work for other versions of Windows.

Requirements:

- A RJ45 or mini USB console cable.
- A serial console emulator, like PuTTY.

To connect a console to the Cisco IC3000:

Procedure

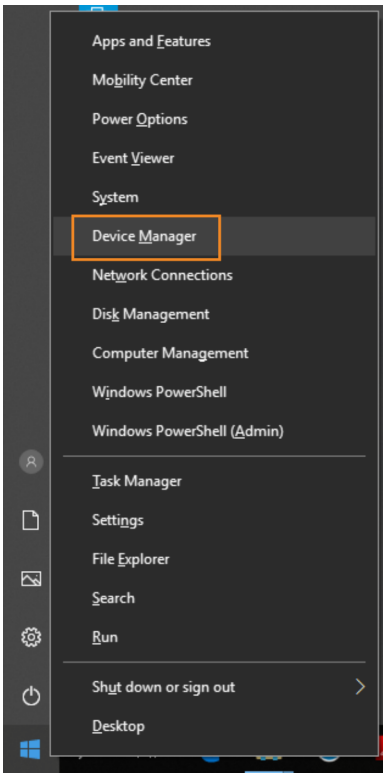
Step 1 Download and install on your computer a serial console emulator like PuTTY. Refer to its own documentation to use it.

Step 2 Connect your computer to the Cisco IC3000 through its serial port using the RJ45 or mini USB console cable.

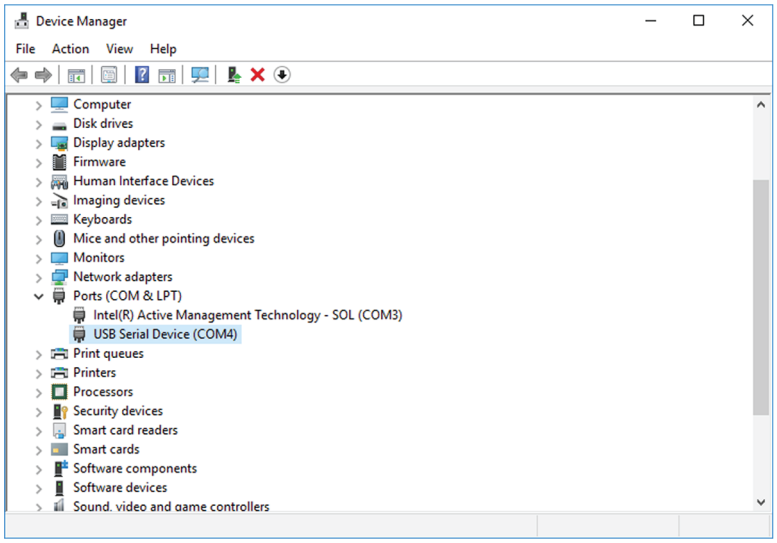
If you are using **Windows**, you need to identify to which COM port the console is connected.

To identify the COM port:

Step 3 Right click on the Windows Start icon and select "Device Manager".



Step 4 Scroll down and click "Ports (COM & LPT)" menu. The COM number appears.



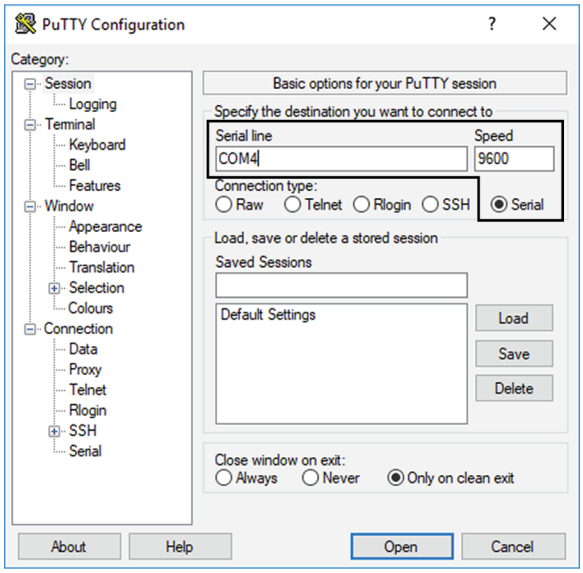
To start a connection to the Cisco IC3000:

Step 5 Make sure there is no USB drive plugged into the Cisco IC3000.

Step 6 Disconnect the Cisco IC3000 from the DC Current source.

Step 7 Open PuTTY.

The following screen appears:



Step 8 Select Serial for the Connection type.

Step 9 Enter "COM<number>" into the serial line field.

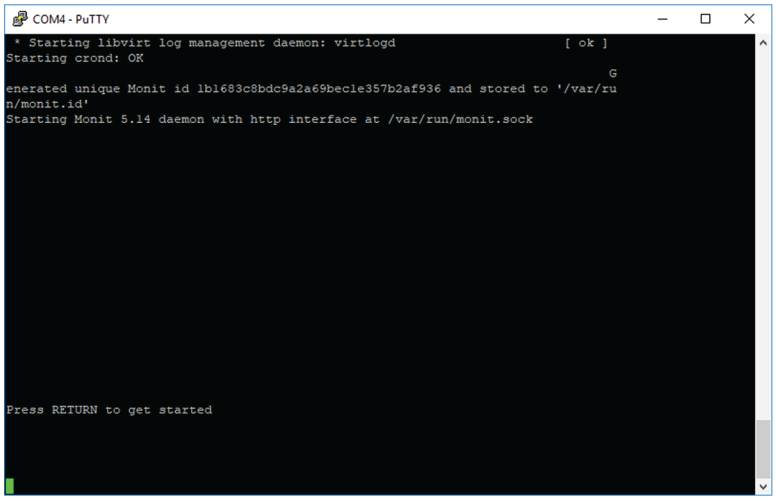
Set speed at 9600.

Step 10 Click Open to display the shell prompt for PuTTY.

Step 11 Connect the Cisco IC3000 to the DC current source.

Wait a few moments. When booting is complete, the shell prompt will ask you to press return to start.

The connection has established with success.



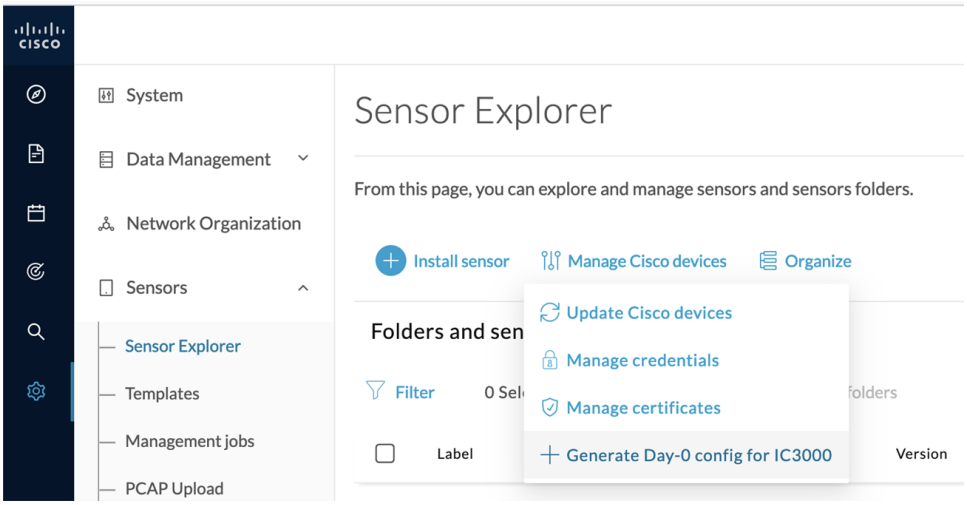
Cisco IC3000 platform initial configuration

Perform the following procedure if it's the first time the Cisco IC3000 device is installed in Cisco Cyber Vision.

Set Cisco IC3000 for Local Manager

Procedure

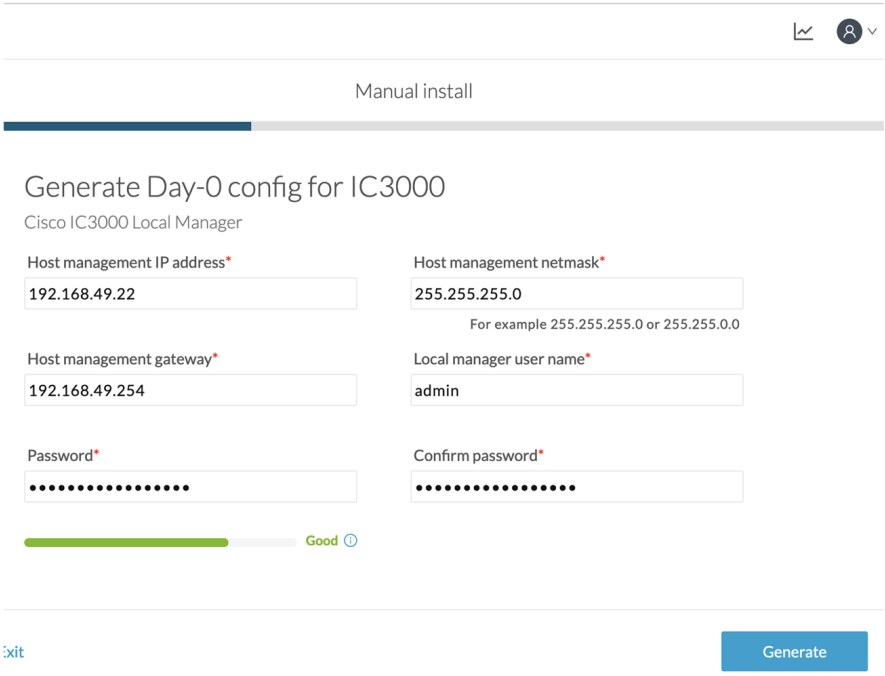
Step 1 Click **Manage Cisco devices**, then **Generate Day-0 config for IC3000**.



Step 2 Fill the following fields to set the Local Manager's network parameters and login:

- The Host Management's IP address, netmask and gateway. They must be set to access the Local Manager of the Cisco IC3000 device.
- The Local Manager admin user name. The login is "admin" by default. You must use the default login in case a factory reset is performed and thus to avoid starting the whole procedure again.

  The user name will be asked later to log in to IOx Local Manager and in case of troubleshooting and configuration. Therefore, make sure to keep this piece of information stored.



Step 3 Click **Generate**.

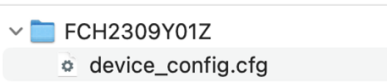
The file **device_config.cfg** is downloaded.

Prepare and import the Local Manager configuration file

After generating and downloading the file **device_config.cfg** you must prepare and import it in the Cisco IC3000.

Procedure

Step 1 Copy the file in a folder named as the serial number of the Cisco IC3000 (e.g. FCH2309Y01Z). The folder must be placed at the root directory of a USB drive formatted as FAT32.



Step 2 Disconnect the Cisco IC3000 from the DC Current source. The USB drive must be plugged at the Cisco IC3000 boot.

Step 3 Plug the USB drive on port 2 of the Cisco IC3000.

Step 4 Connect the sensor to the DC Current source.

Wait a few moments. The Cisco IC3000 status changes to Enrolled on the Cisco Cyber Vision GUI.

Step 5 Unplug the USB drive from port 2.

The Local Manager should become available on the IP address defined during this procedure.

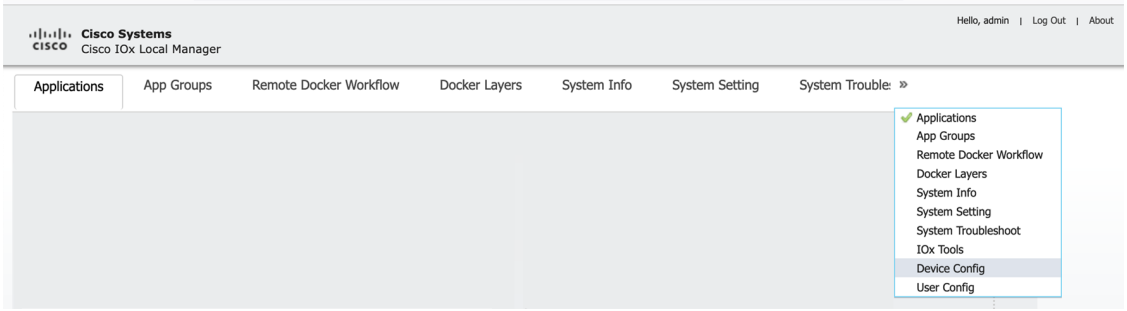
Configure date and time

Before proceeding to the installation, you must set the correct date and time and on the IC3000 through the Local Manager for its proper functioning.

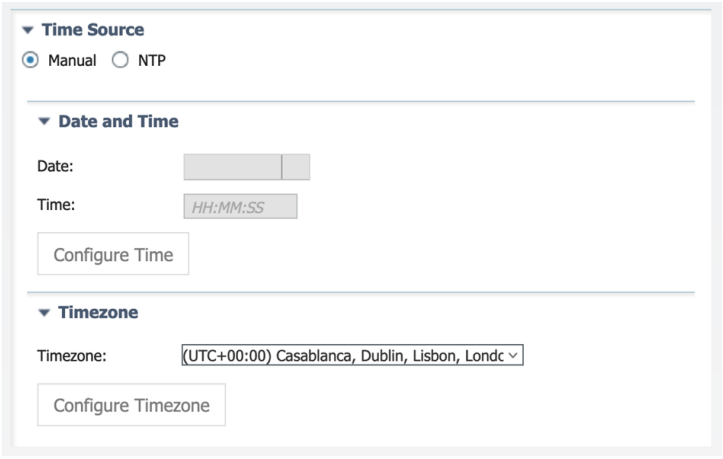
Procedure

Step 1 Access the Local Manager.

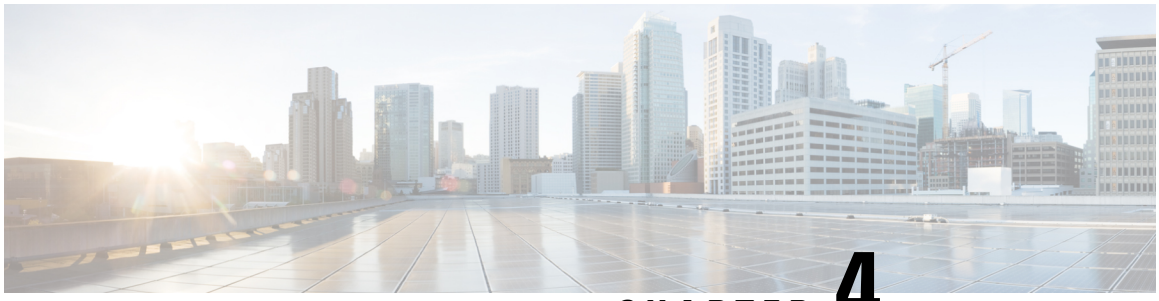
Step 2 Navigate to **Device Config**.



Step 3 Slide down to Time Source and configure the date and time according to your network settings.



For more information, check the Cisco IC3000 user documentation available on cisco.com.



CHAPTER 4

Installation procedures

Procedure with the Sensor management extension

This section explains how to install the Cisco IC3000 thanks to the sensor management extension. You will:

1. Retrieve the sensor management extension on cisco.com.
2. Install the sensor management extension on Cisco Cyber Vision.
3. Connect to the Cisco IC3000 with the serial console and check its firmware version and management interface IP address.
4. Create a new sensor on Cisco Cyber Vision through the Cisco device deployment and proceed to its configuration.

Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

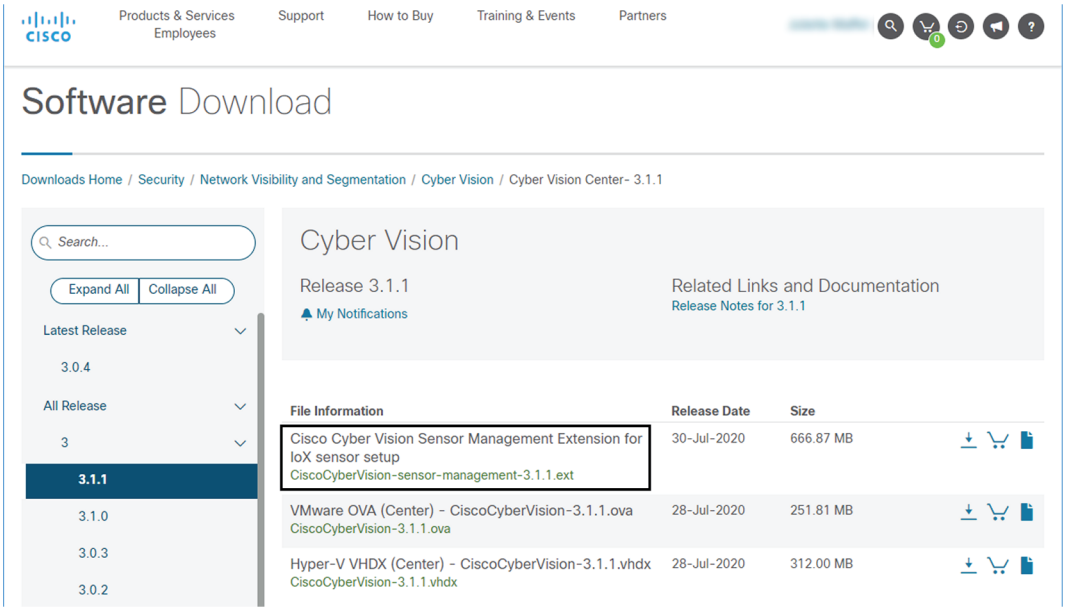
Required material and information:

- An Admin or Product access to Cisco Cyber Vision.
- The network information of the Collection network interface (IP address, subnet mask and gateway).
- A RJ45 or mini USB console cable.
- A serial console emulator, like PuTTY.

Note To be able to use the Cisco Cyber Vision sensor management extension, an IP address reachable by the Center Collection interface must be set on the Collection VLAN.

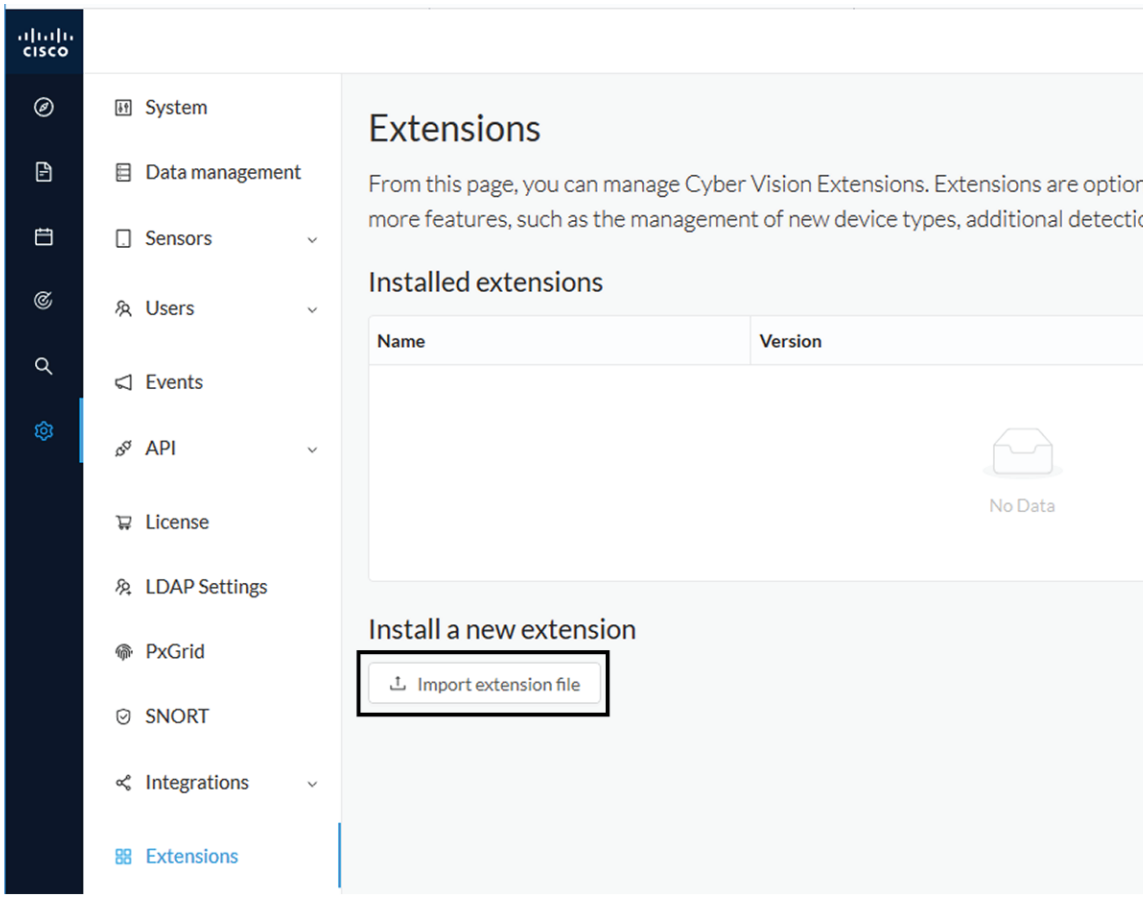
Retrieve the sensor management extension file

1. On cisco.com, navigate to Cisco Cyber Vision's Software Download page.
2. Download Cisco Cyber Vision Sensor Management Extension for IoX sensor setup. Version of the extension must be the same as the version of the center.

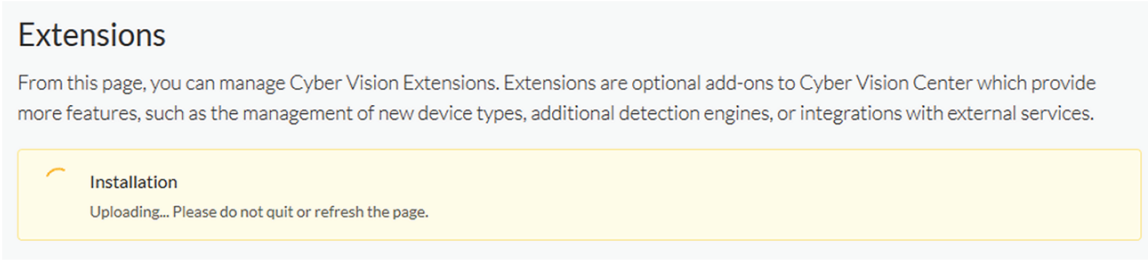


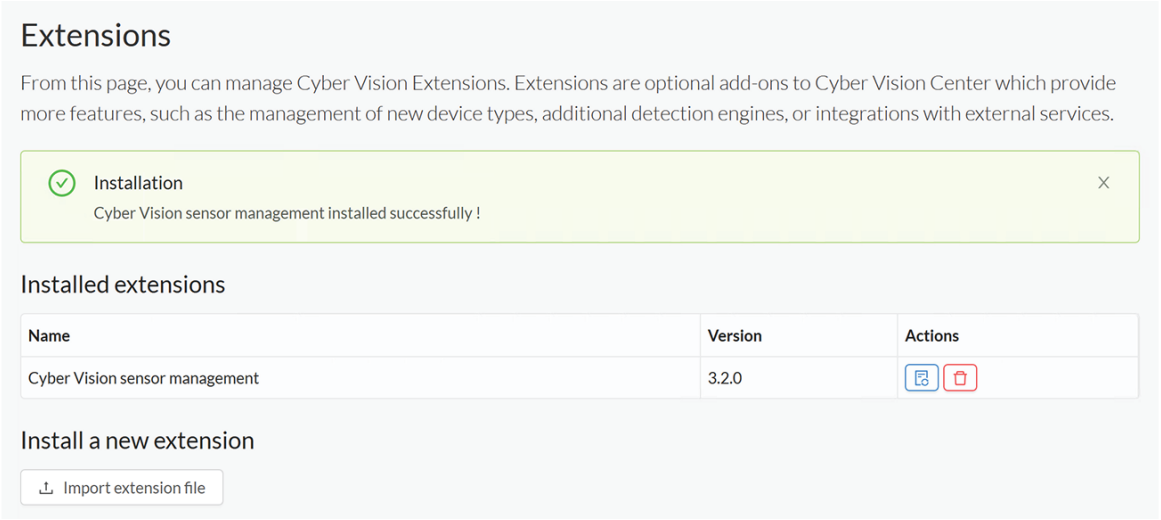
Install the sensor management extension

1. In Cisco Cyber Vision, navigate to Admin > Extensions.
2. Click Import extension file and select CiscoCyberVision-sensor-management-<version>.ext.



The file upload takes a few minutes.





Check the Cisco IC3000 firmware version

To ensure a proper installation of the Cisco IC3000, you must check its firmware version.

It is recommended to use the newest firmware version available. The lowest version used should be 1.2.1 for a classic installation or 1.5.1 for an installation with Active Discovery.

Procedure

Step 1 To check the version:

Step 2
- Use the following command in the Cisco IC3000 shell prompt:

```
ic3k>show version
```

Example:

```
ic3k>show version
Version: 1.2.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FCH2312Y04M
ic3k>
```

Check the MGMT interface IP address

Check that the IP address set on the MGMT network is the one you've configured on the Cisco Cyber Vision GUI.

To check the MGMT network interface:

Procedure

Step 1 Use the following command in the Cisco IC3000 shell prompt:

```
ic3k>show interfaces
```

Step 2 Search for the reference "svcbr_0" which corresponds to the MGMT interface.

The IP address you've set as Host Management on Cisco Cyber Vision GUI should follow the mention "inet addr: <IP ADDRESS>".

Example:

```
svcbr_0   Link encap:Ethernet  HWaddr d0:ec:35:ca:99:a0
          inet addr:192.168.71.22  Bcast:192.168.71.255  Mask:255.255.255.0
          inet6 addr: fe80::d2ec:35ff:feca:99a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12676 (12.3 KiB)  TX bytes:1980 (1.9 KiB)
```

Step 3

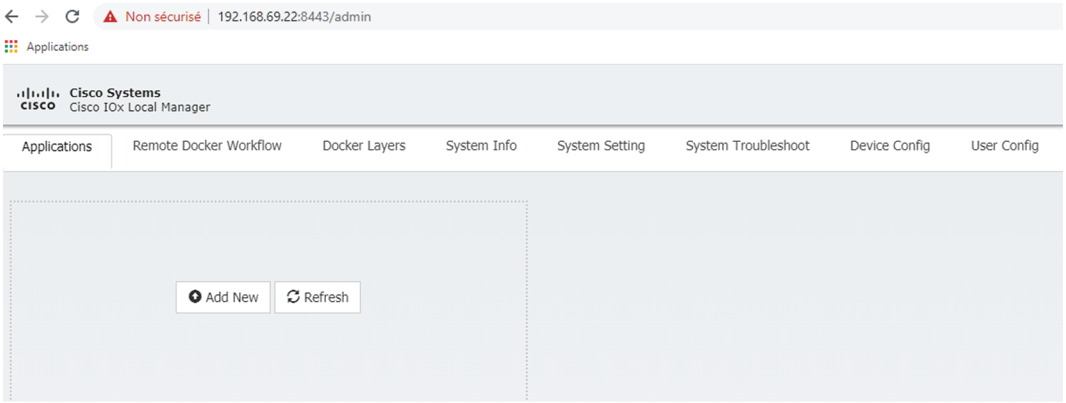
Test connectivity between Cisco IC3000 and IOx Local Manager

To proceed with the installation, you must first test if you have access to the Cisco IC3000's Cisco IOx Local Manager. To do so:

1. Open Chrome.
2. Access Cisco Iox Local Manager using the Cisco IC3000's MGMT IP address and the MGMT port number, which is 8443:

   https://Management_Address:8443

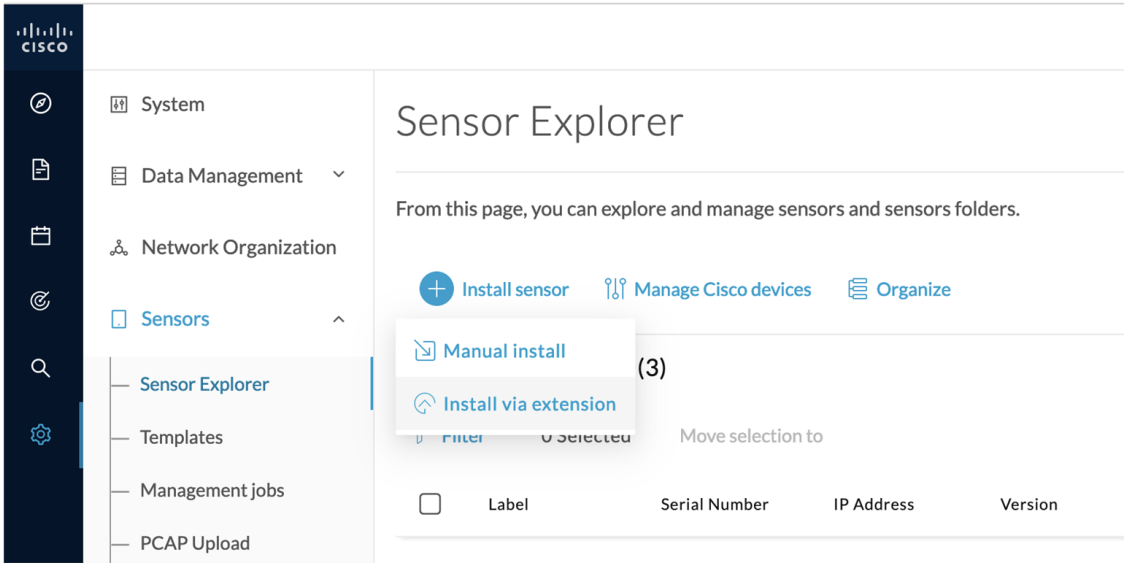
   ex: https://192.168.71.22:8443
3. If you're able to see the following screen it means that the connectivity between the Cisco IC3000 and IOx Local Manager is on.



Create a sensor in Cisco Cyber Vision

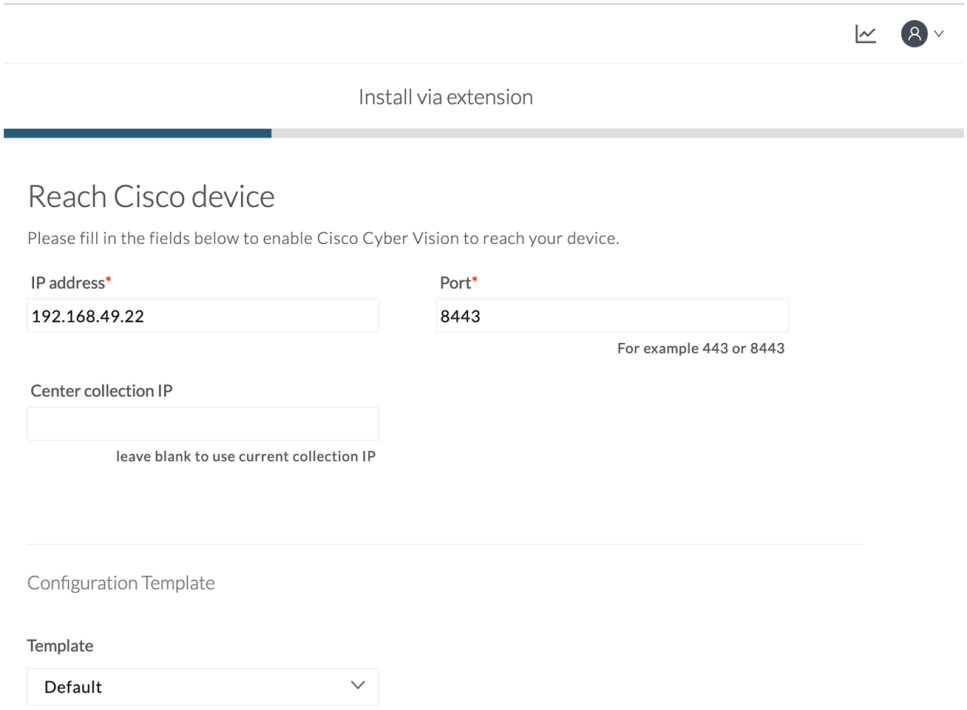
Procedure

Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Install via extension**.



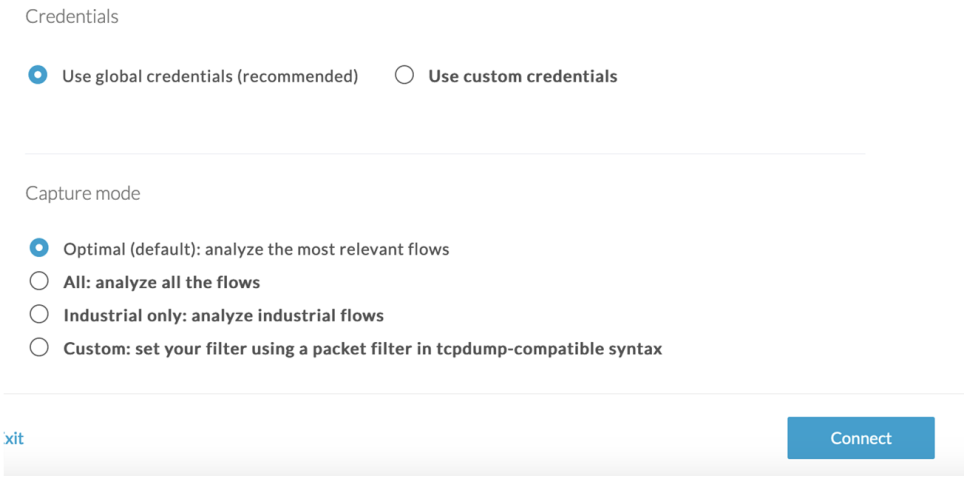
Step 2 Fill in the requested fields so Cisco Cyber Vision can reach the equipment:

- IP Address: admin address of the equipment
- Port: management port (8443)



Step 3 Select a configuration template if required. For more information, refer to Configure sensor configuration template, on page 37.

Step 4 Select the credential mode used. For more information, refer to Cisco Cyber Vision GUI Administration Guide available on cisco.com.



Step 5 Optionally, select a capture mode.

Step 6 Click **Connect**.

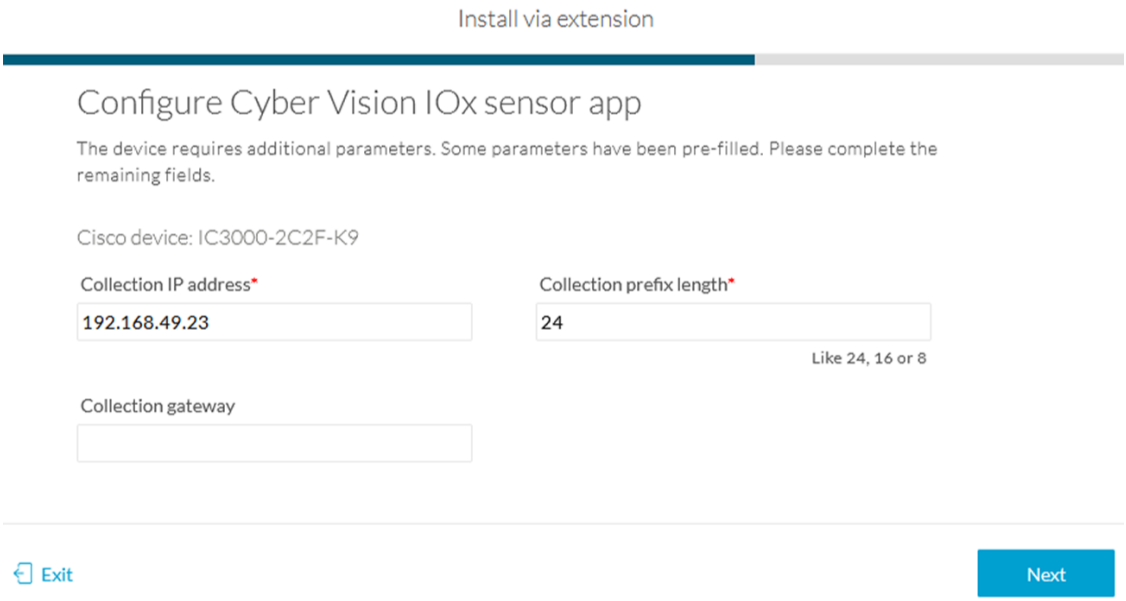
The Center will join the equipment and display the second parameter list. For this step to succeed, the equipment needs to be reachable by the Center on its eth0 connection for a Center with single interface or eth1 for a Center with dual interface.

Configure the sensor

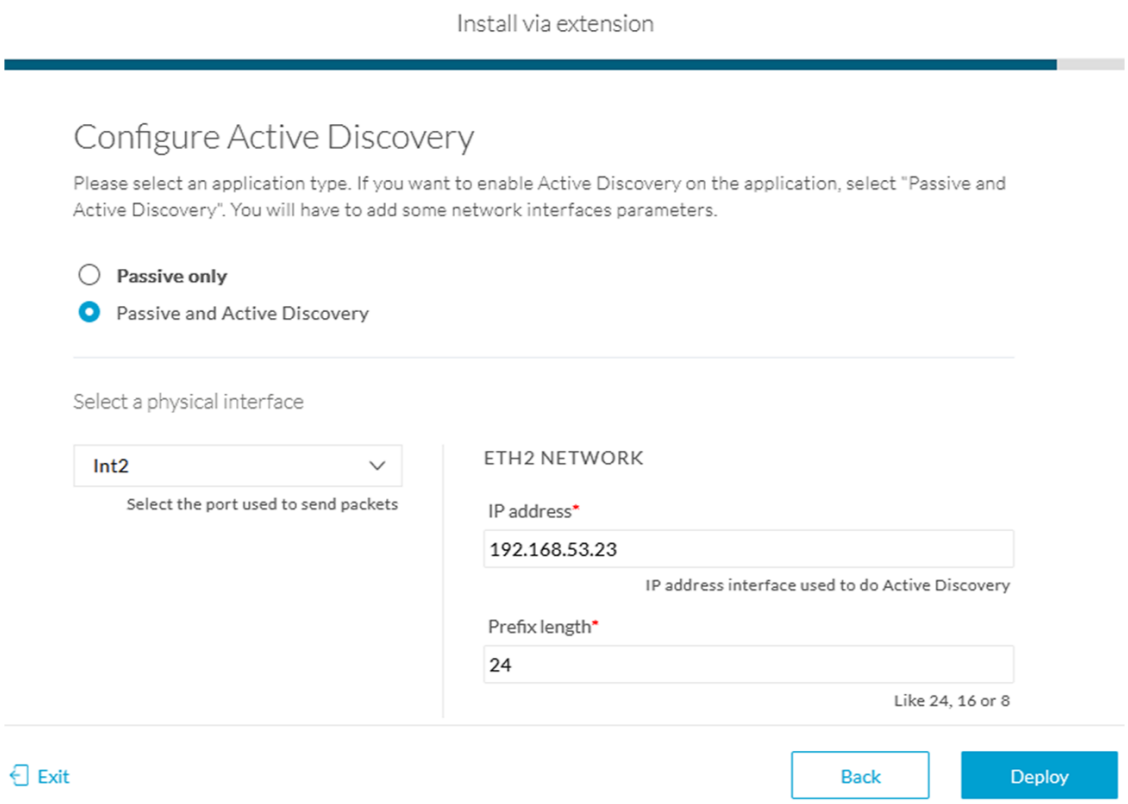
Once the Center can join the equipment, you will have to configure the Cisco Cyber Vision IOx sensor app by setting the Collection interface and, if needed, Active Discovery.

While some parameters are filled automatically, you can still change them if necessary.

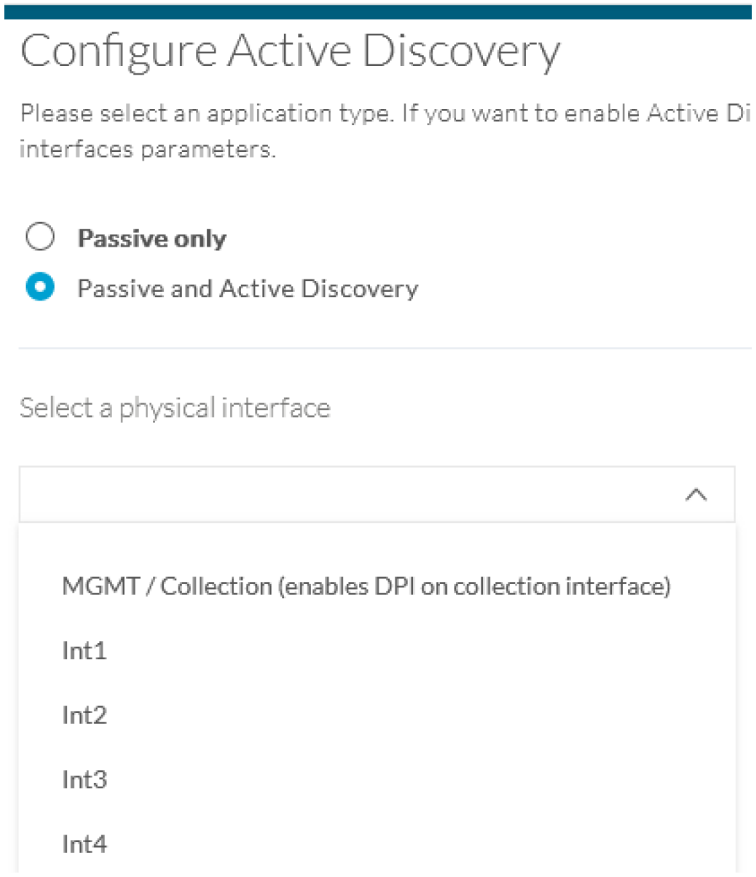
1. Fill the following parameters for the Collection interface:
   - Collection IP address: IP address of the sensor in the sensor (must be different than the ip address of the device)
   - Collection subnet mask: mask of the Collection IP address
   - Collection gateway: gateway of the Collection IP address (optional)



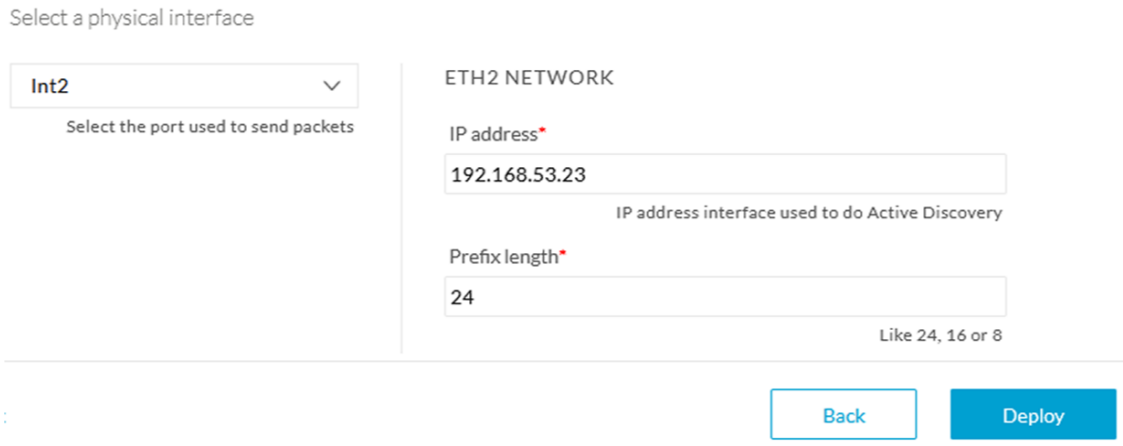
2. Select the Application type (passive only or passive and Active Discovery).
3. If selecting Passive and Active Discovery, the following fields will appear to set its interface:



- Physical interface: port that will be used to send packets.



- IP address of the interface dedicated to Active Discovery.
- Prefix lenght: subnet mask of the interface.



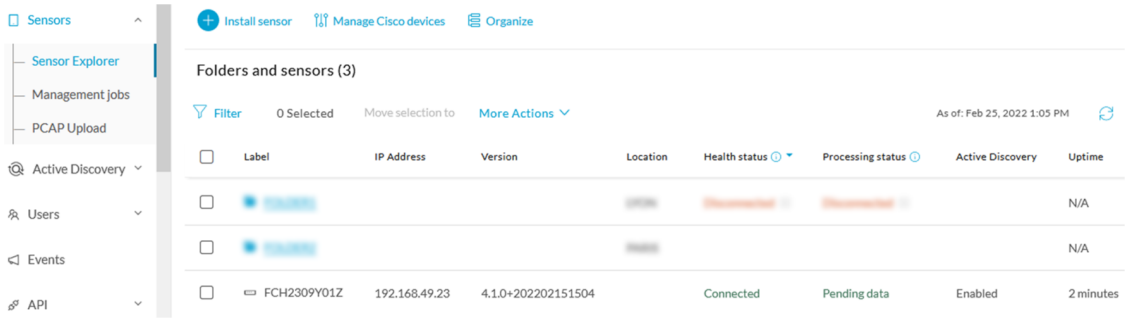
4. Click the Deploy button.

   The Center starts deploying the sensor application on the target equipment. This can take a few minutes.

   Once the deployment is finished, a new sensor appears in the sensors list.

If Active Discovery has been enabled, the Active Discovery status will switch to Available and the Active Discovery button will be displayed in the right side panel as you click the sensor in the list.

The sensor status will turn to connected.



Note You can change the Active Discovery configuration by clicking the Active Discovery button. However, for changes to be applied, you will have to download a new provisioning package and deploy it on the hardware.

Procedure with the Local Manager

This section explains how to install the Cisco IC3000 with the Local Manager. You will:

1. Create and configure a new sensor on Cisco Cyber Vision to retrieve its provisioning package.
2. Install and configure the virtual sensor application on the Local Manager to deploy the provisioning package on the Cisco IC3000.
3. The last step, which is optional, consists in enabling Active Discovery on the Cisco IC3000.

Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

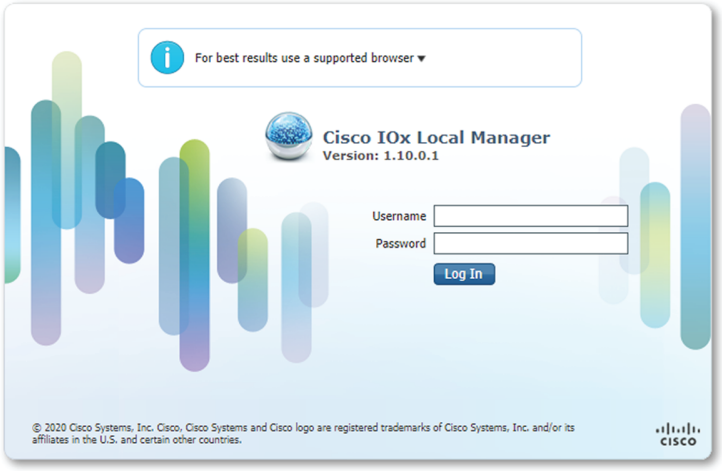
If it's the first time the Cisco IC3000 device is installed with the Local Manager you must first proceed to a Cisco IC3000 platform initial configuration.

Required material and information:

- An Admin or Product access to Cisco Cyber Vision.
- A Local Manager user account and password.
- The serial number of the Cisco IC3000 to be configured (located on the hardware's front view).
- An IP addressing scheme for the Local Manager and the Collection Network Interfaces.
- The Cisco Cyber Vision Sensor application to collect from cisco.com, i.e. CiscoCyberVision-IOx-IC3000-<version>.tar.

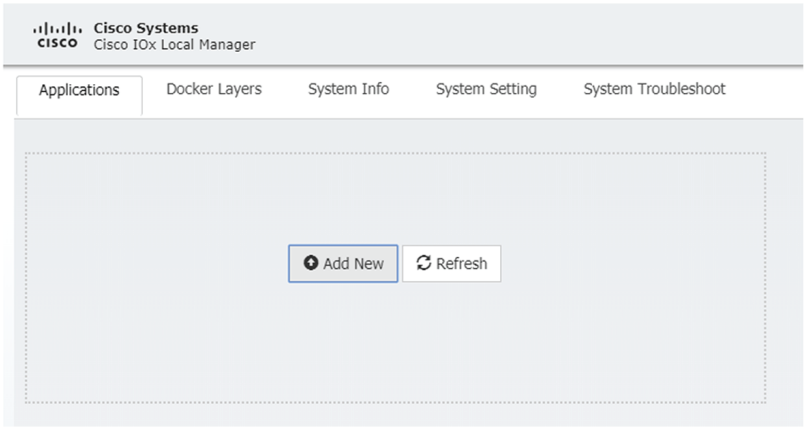
Access the Local Manager

1. Open a browser and navigate to the IP address you configured on the interface you are connected to.
2. Log in using the user account and password.



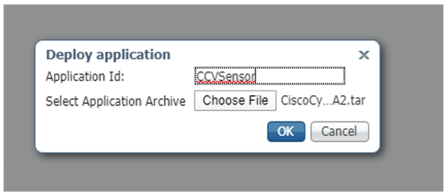
Install the sensor virtual application

Once logged in, the following menu appears:



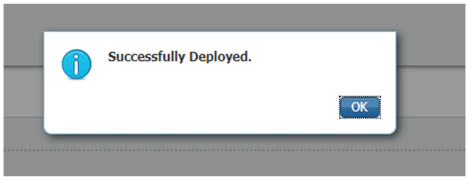
1. Click **Add New**.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file
   (i.e. "CiscoCyberVision-IOx-IC3000-<version>.tar").

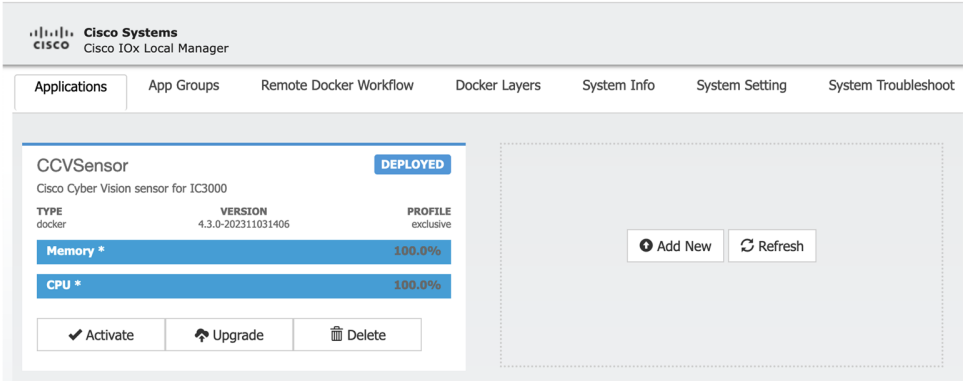
Note If you aim to install a sensor with **Active Discovery**, select the required application archive file (i.e. "CiscoCyberVision-IOx-Active-Discovery-IC3000-<version>.tar").



The installation takes a few minutes.

When the application is installed, the following message is displayed and the sensor application appears:

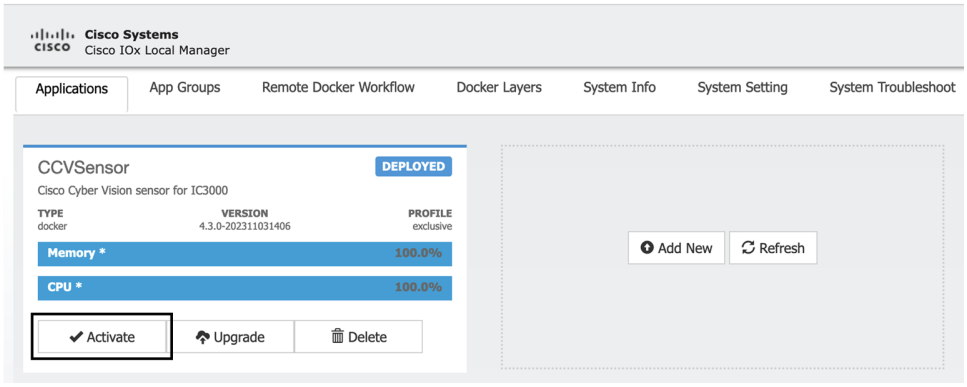




Configure the sensor virtual application

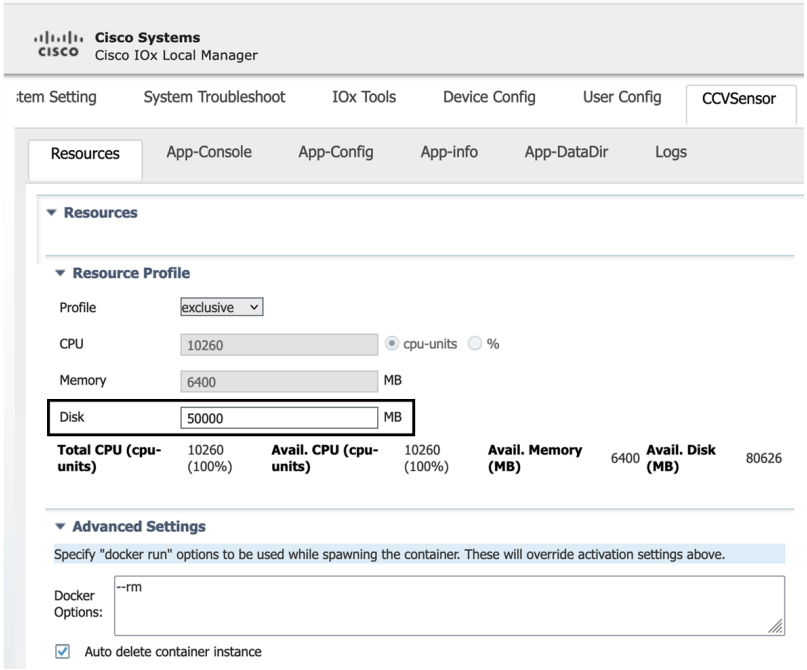
Procedure

Step 1 Click **Activate** to launch the configuration of the sensor application.



Step 2 Access Applications > Resources.

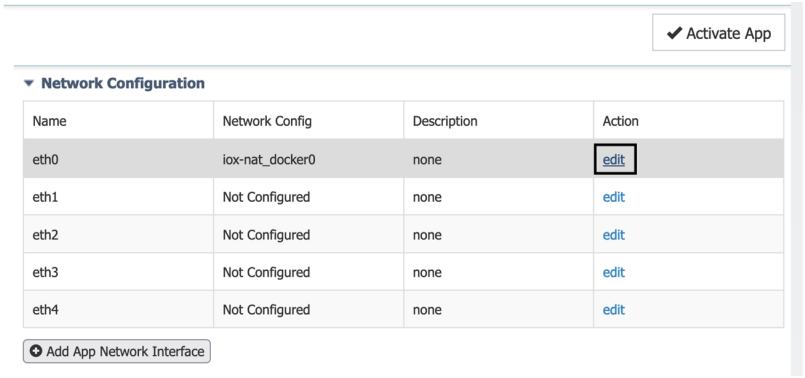
Step 3 Under Resource Profile, change the disk size to 50,000 MB.



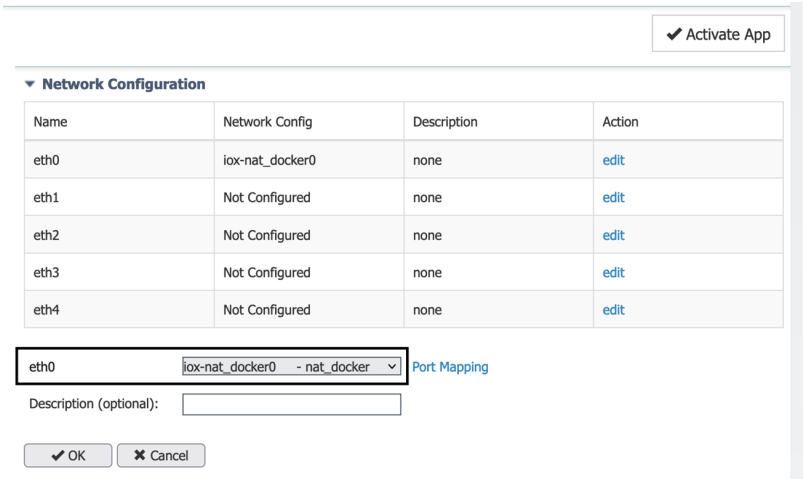
Note Disk size shouldn't be lower than 1,000 MB.

To map the Sensor network interfaces:

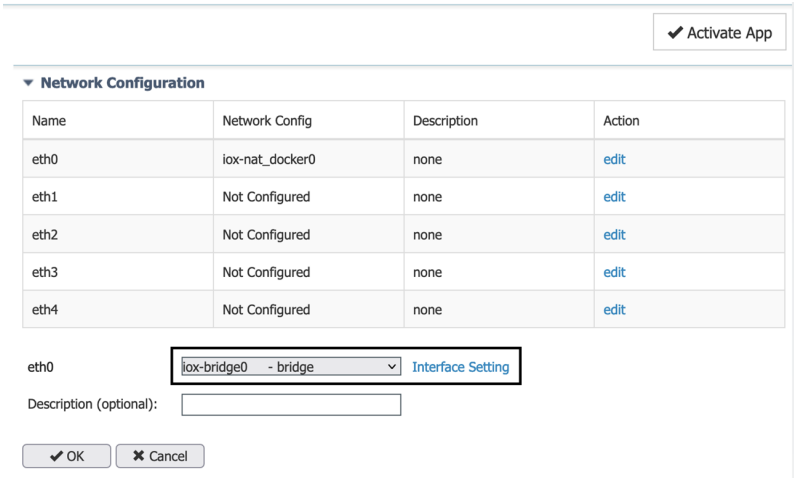
Step 4 Under Network Configuration, click **edit** in the eth0 line.

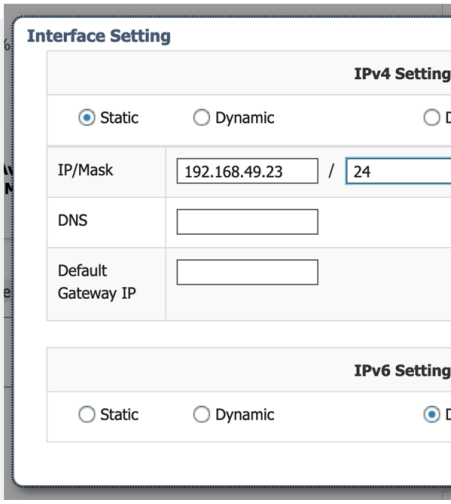


Step 5 Set eth0 to "iox-bridge0" using the dropdown menu.



Step 6 Click **Interface Setting**.





Step 7 Apply the following settings:

- Set IPV4 as **Static**.
- Set the Sensor Collection IP and mask.

- If needed set a default gateway IP.
- **Disable** IPV6.

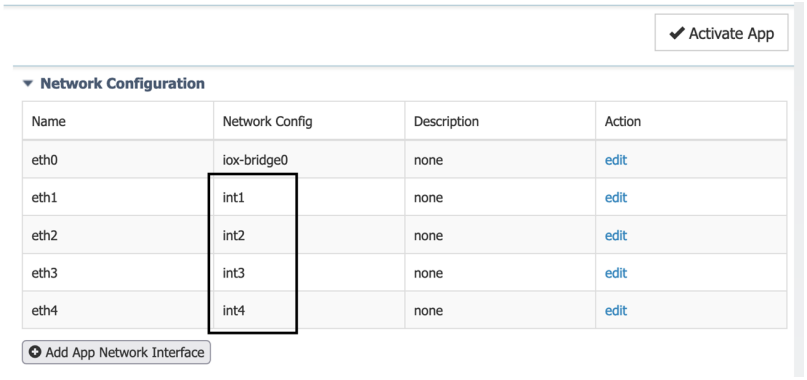
Step 8 Click **OK** to close the Interface Setting window and **OK** again to confirm Network Configurations.

Step 9 A message saying that the network interface has been changed appears. Click **OK**.

Step 10 Set the network interfaces eth1, eth2, eth3 and eth4 by repeating the previous steps and using the table below. You must click **OK** each time you map a new interface for changes to be taken into consideration.

Each network interface must be mapped like below:

Name	Network Configuration
eth0	iox-bridge0
eth1	int1
eth2	int2
eth3	int3
eth4	int4



To set eth1, eth2, eth3 and eth4 as mirrored ports:

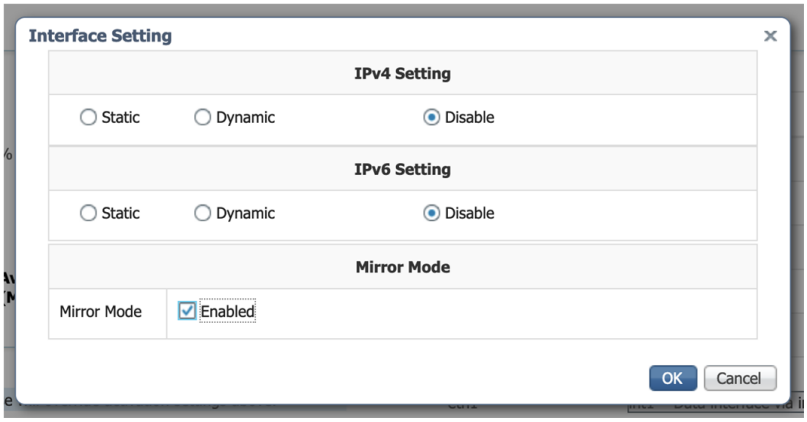
Step 11 Click **Edit** beside eth.

Step 12 Click **Interface Setting**.

Step 13 **Disable** IPv4 and IPv6.

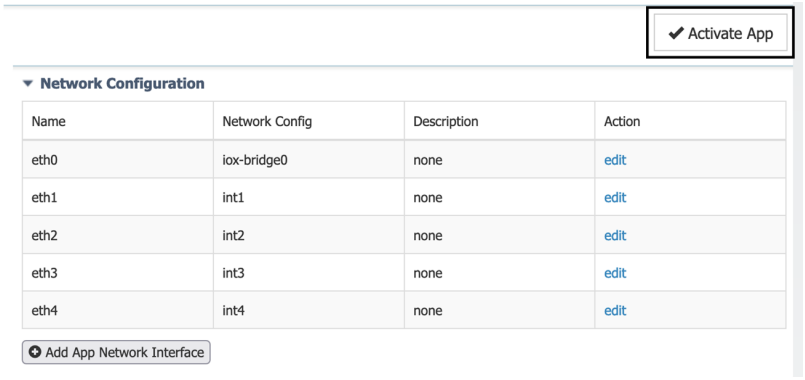
Step 14 Tick **Enabled** for Mirror Mode.

Step 15 Click **OK**.



Step 16 Repeat the above steps for eth2, eth3 and eth4.

Step 17 Click **Activate App** on the page top right corner.

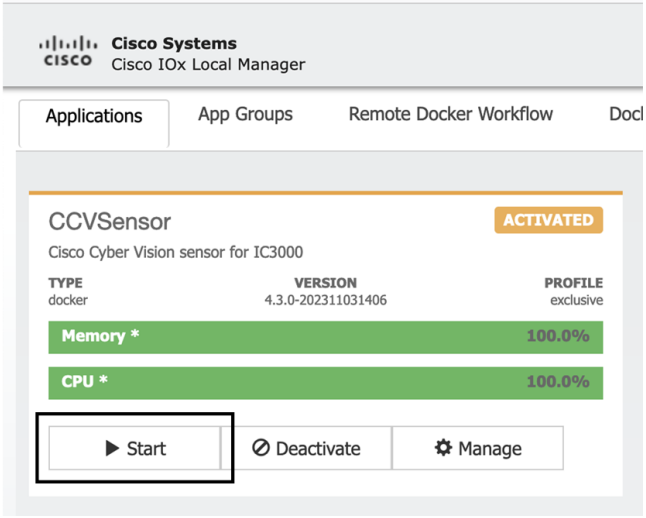


The following message appears:

To start the Sensor Application:

Step 18 Access the Applications tab again.

Step 19 Click **Start**.

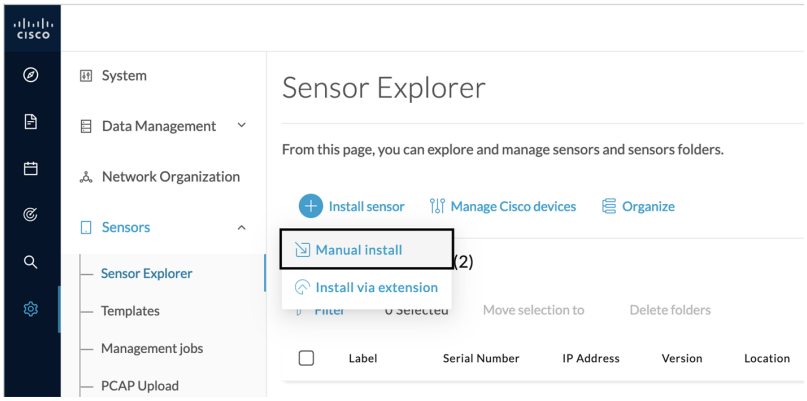


The application moves from Activated to Running state.

Create a sensor and generate the provisioning package

Procedure

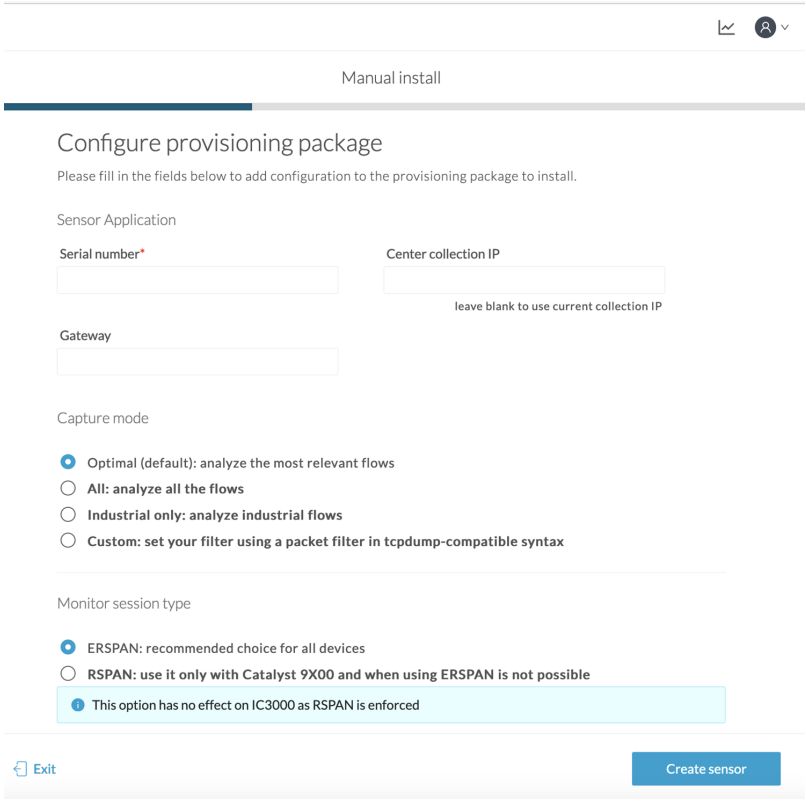
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Manual install**.



Step 2 Fill in the fields to configure the sensor provisioning package:

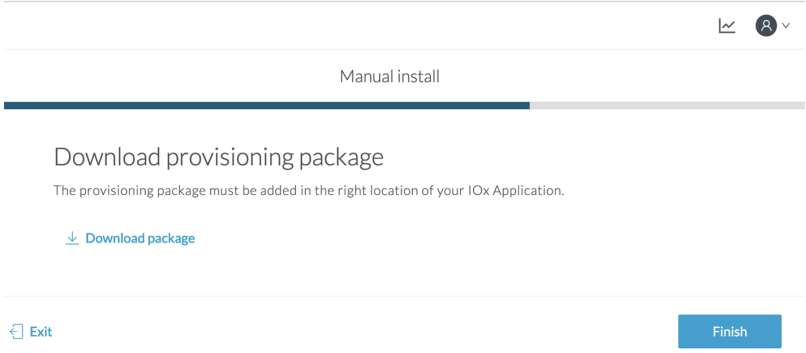
- The serial number of the hardware (e.g. FCH2309Y01Z).
- Center IP: leave blank.
- Gateway: add if necessary.
- Optionally, select a capture mode.

- Leave the Monitor session type setup as it is as RSPAN is already enforced on Cisco IC3000. Changing this setup will have no effect.



Step 3 Click **Create sensor**.

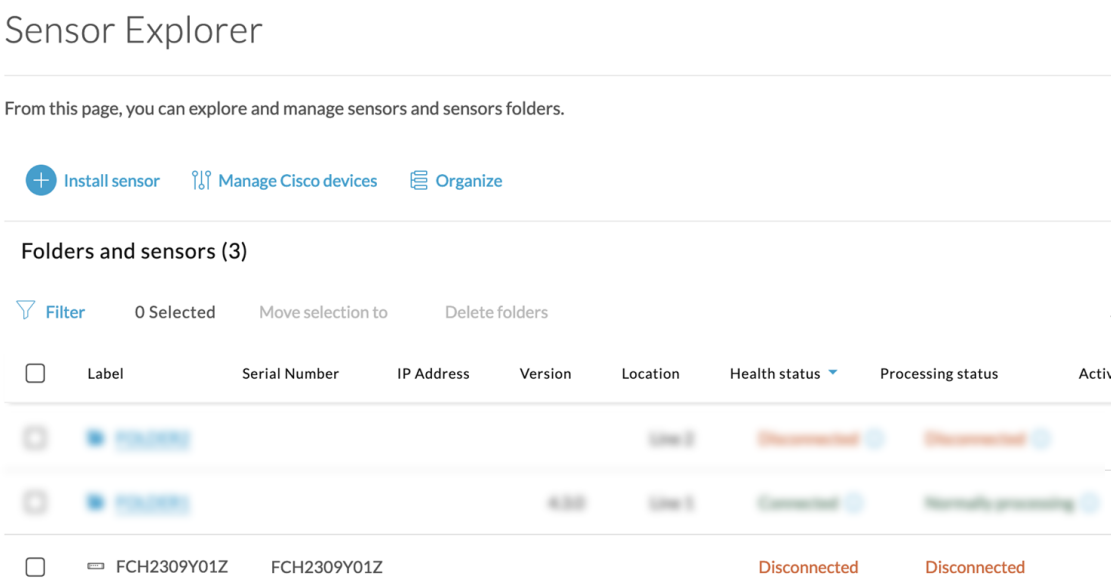
Step 4 Click **Download package**.



The provisioning package will be downloaded. It is a zip archive file with the following name structure: sbs-sensor-config-<serialnumber>.zip (e.g. "sbs-sensor-configFCH2309Y01Z.zip").

Step 5 Click **Finish**.

A new sensor appears in the Sensor Explorer list with the Disconnected status.



What to do next

The provisioning package must be imported in the Local Manager.

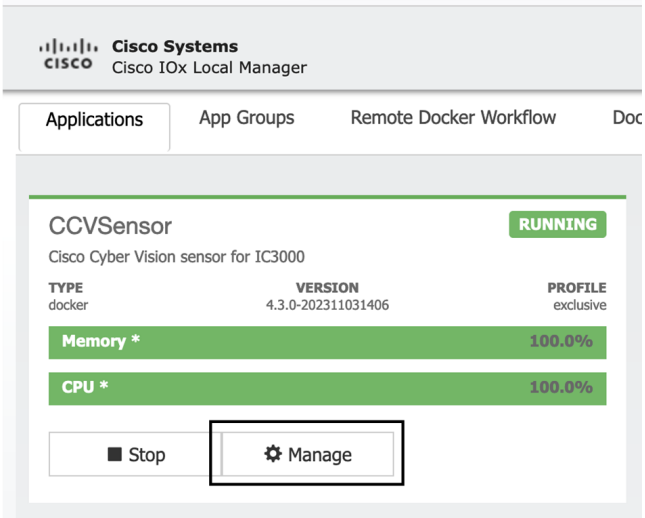
Import the provisioning package

After generating the provisioning package in Cisco Cyber Vision application, you must import it in the Local Manager so the sensor can be enrolled to Cisco Cyber Vision.

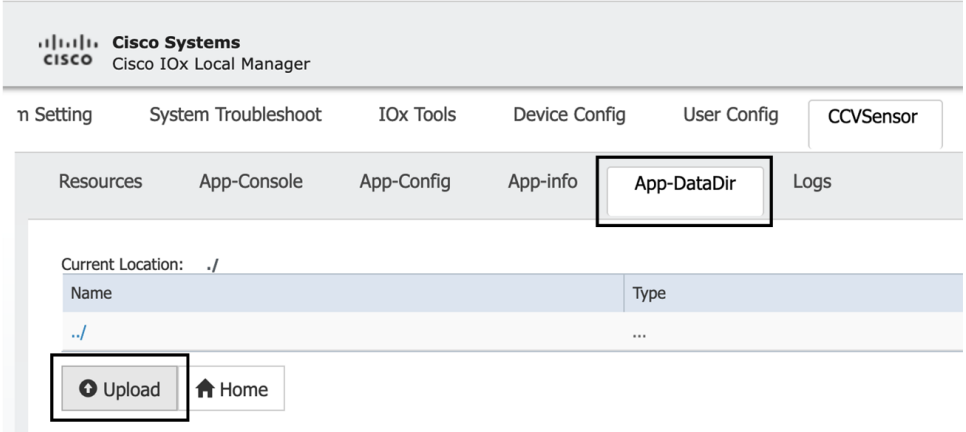
Before you begin

Procedure

Step 1 In the Local Manager, click **Manage** on the sensor application.

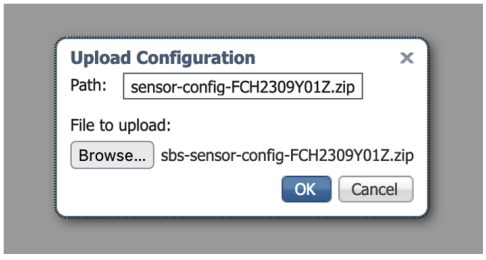


Step 2 Navigate to **App-DataDir**.



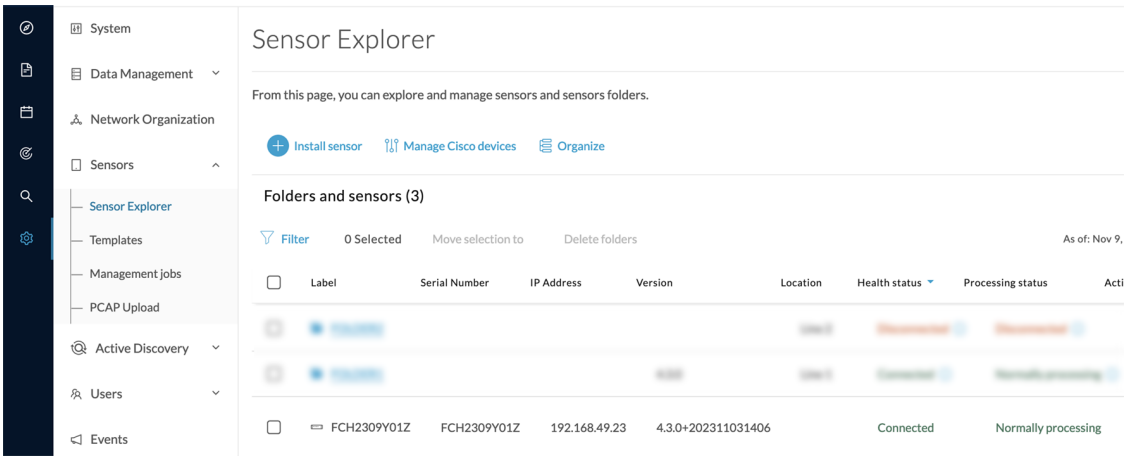
Step 3 Click **Upload**.

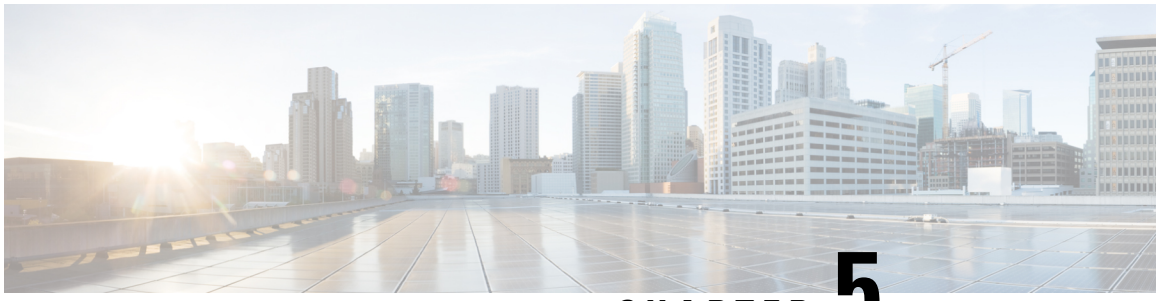
Step 4 Select the provisioning package (i.e. "sbs-sensor-config-<serialnumber>.zip"), and add the exact file name, extension included, in the path field (i.e. "sbs-sensor-config-<serialnumber>.zip").



Step 5 Click **OK**.

After a few seconds, a message saying that the upload went successfully will be displayed and the sensor will appear as Connected in Cisco Cyber Vision.


System
Data Management
Network Organization
Sensors
Sensor Explorer
Templates
Management jobs
PCAP Upload
Active Discovery
Users
Events
Sensor Explorer
From this page, you can explore and manage sensors and sensors folders.
Install sensor
Manage Cisco devices
Organize
Folders and sensors (3)
Filter
0 Selected
Move selection to
Delete folders
As of: Nov 9,
Label
Serial Number
IP Address
Version
Location
Health status
Processing status
Acti
FCH2309Y01Z
FCH2309Y01Z
192.168.49.23
4.3.0+202311031406
Connected
Normally processing



CHAPTER 5

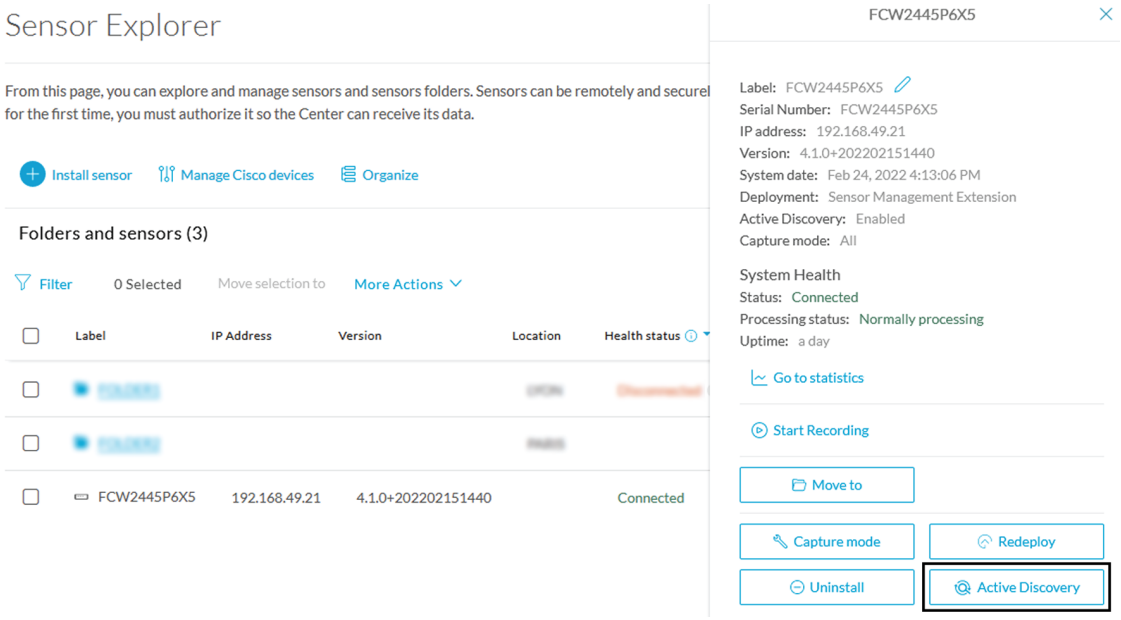
Configuration

Configure Active Discovery

Once the sensor is connected, you can change the Active Discovery's network interface so it uses the Collection network interface instead, and add several network interfaces for the sensor to perform Active Discovery on several subnetworks at the same time.

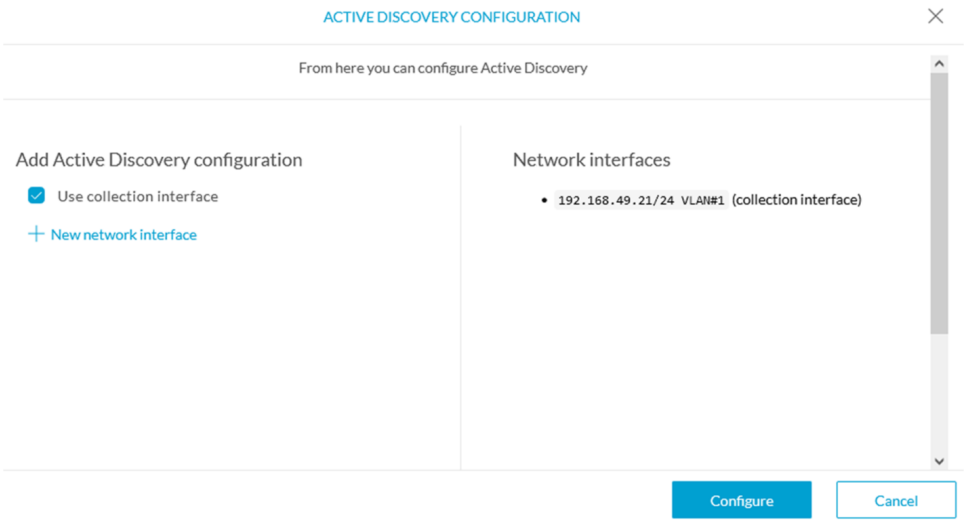
Procedure

Step 1 Click the sensor to configure and click the **Active Discovery** button on its right side panel.



The Active Discovery configuration appears with the interface currently set.

Step 2 Select **Use collection interface** for the Active Discovery to use the Collection network interface.



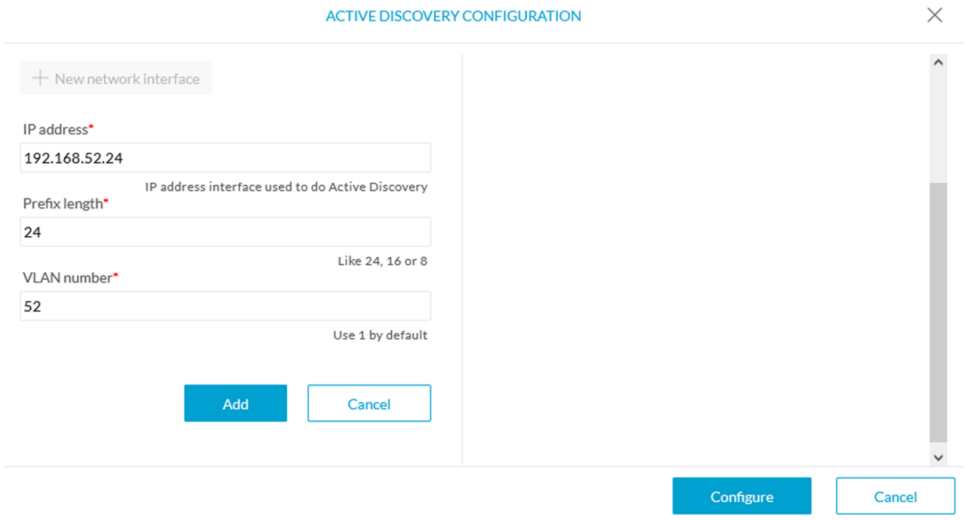
To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

Step 3 Add a new network interface by clicking the corresponding button.

Step 4 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number

Step 5 Click **Add**.



You can add as many network interfaces as needed.

Step 6 When you are done, click **Configure**.

A message saying that the configuration has been applied successfully appears.

Configure sensor configuration template

Templates

This page allows you to create and set templates with protocol configurations and assign them to specific sensors.

Sensor templates contain protocol configurations which allow you:

- To enable or disable protocol DPI (Deep Packet Inspection) engines.
- To map UDP and TCP ports for each protocol's packet received by the sensor.

By enabling/disabling a protocol DPI engine you can decide which protocols will be analyzed.

Disabling a protocol DPI engine avoid false positives in Cisco Cyber Vision, that is when a protocol appears on the user interface when it's actually not the case because same UDP/TCP ports can be used by other non-standardized protocols.

Some protocols are disabled in the Default template because they are not commonly used or used in specific fields such as transportation. The Default template is applied on all compatible sensors.

As previously mentioned, UDP/TCP ports default configurations are mostly standardized, but conflicts still exist among field-specific protocols or with limited usage. Mapping UDP/TCP port numbers will allow packets to be sent to the correct DPI engine so they can be accurately analyzed and correctly represented in the user interface.

If the protocol's packet is sent to the wrong port, related information will end up in Security Insights/Flows with no tag.

A sensor can be associated with a single template only. Deployment of the template can fail:

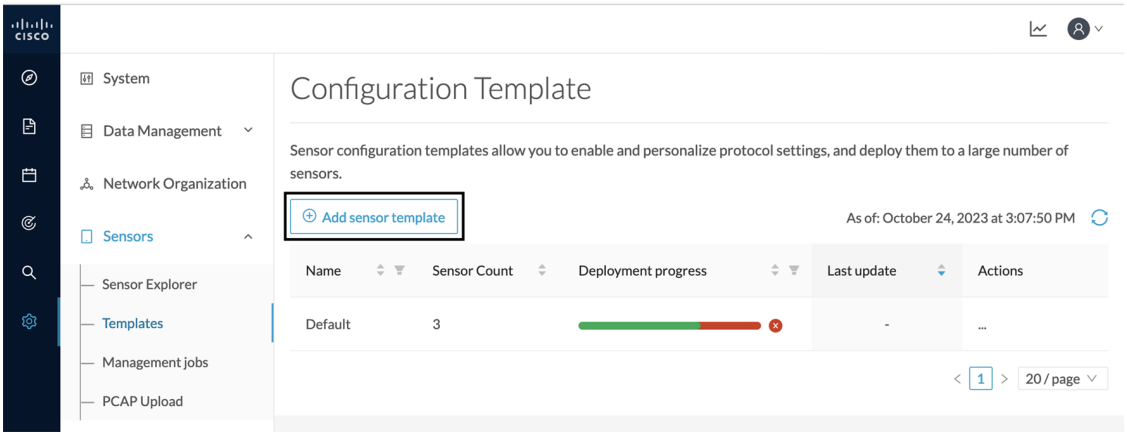
- if the sensor is disconnected,
- if there is connection issues,
- if the sensor version is too old.

Create templates

Procedure

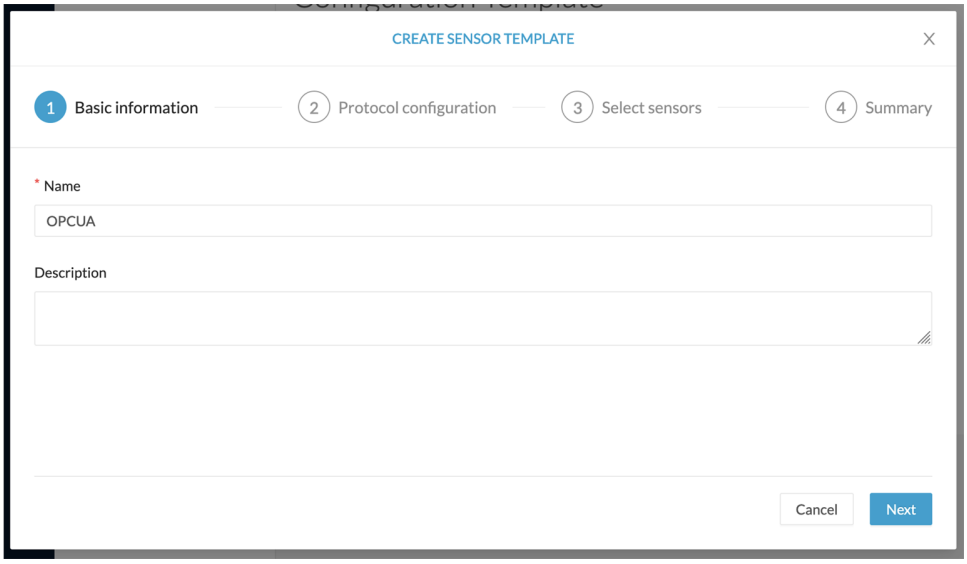
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.

Step 2 Click **Add sensor template**.



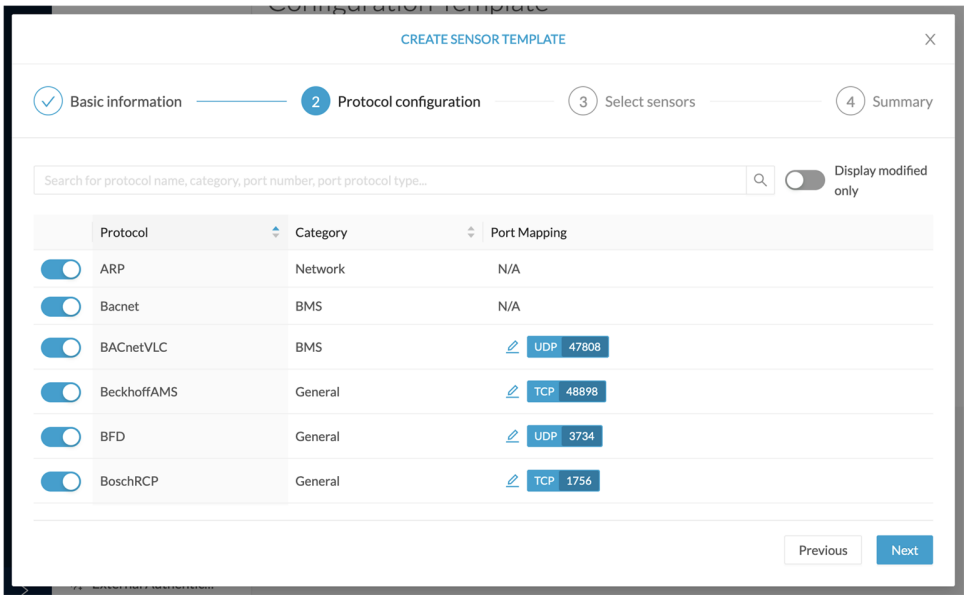
The Create sensor template window pops up.

Step 3 Add a name to the template. You can also add a description.



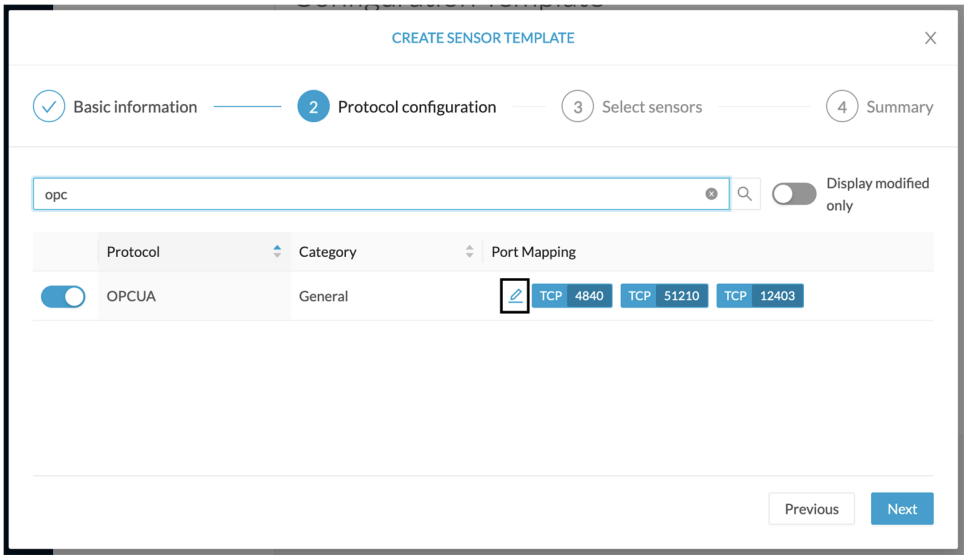
Step 4 Click **Next**.

The list of protocol DPI engines with their basic configurations appears.



Step 5 In the search bar, type the protocol you want to configure.

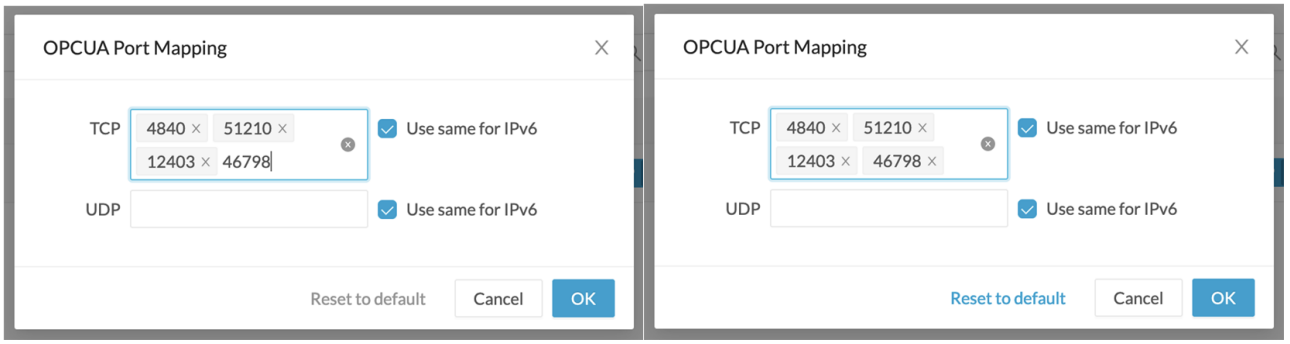
In our example, we will add a port to the OPCUA default settings.



Step 6 Under the Port Mapping column, click the **pen** button to edit its settings.

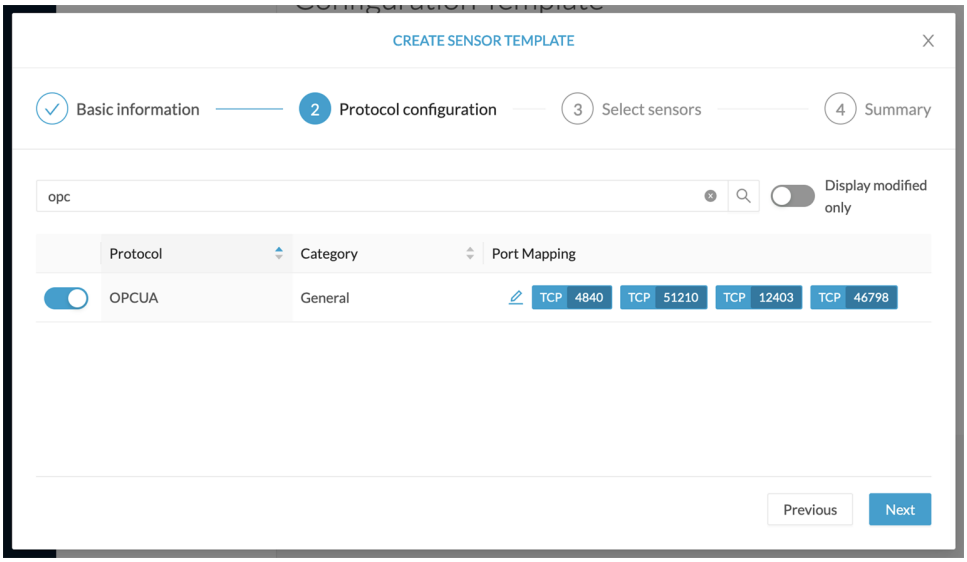
The protocol's port mapping window pops up.

Step 7 Write down the port number you want to add and hit enter.

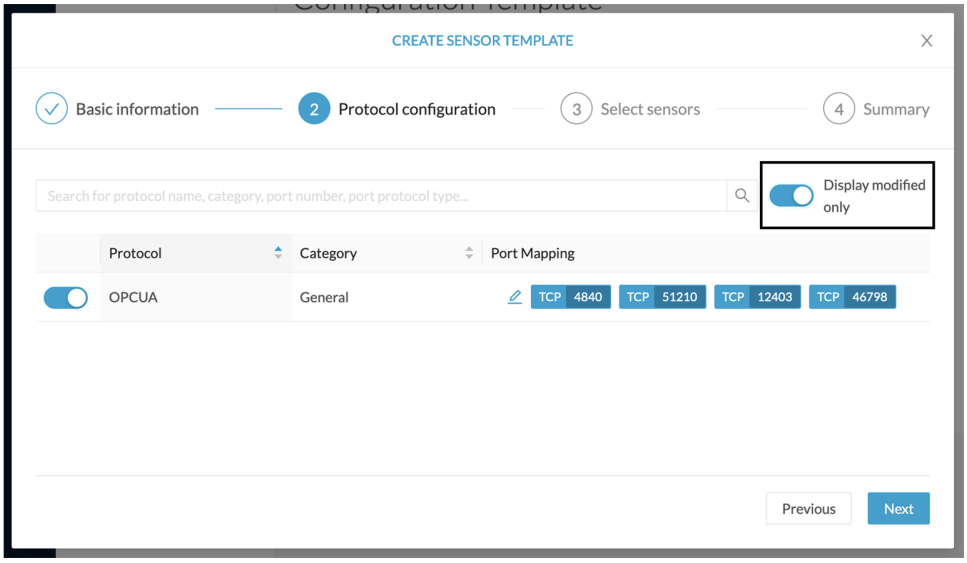


Step 8 Click **OK**.

The port number is added to the protocol's default settings.

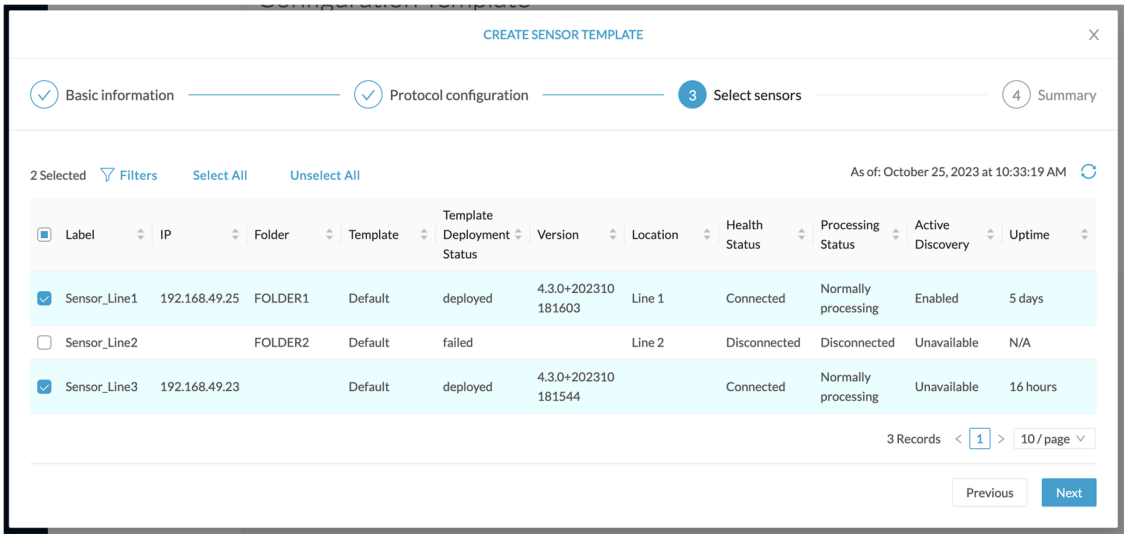


Toggling ON the **Displayed modified only** button allows you to quickly find this protocol.



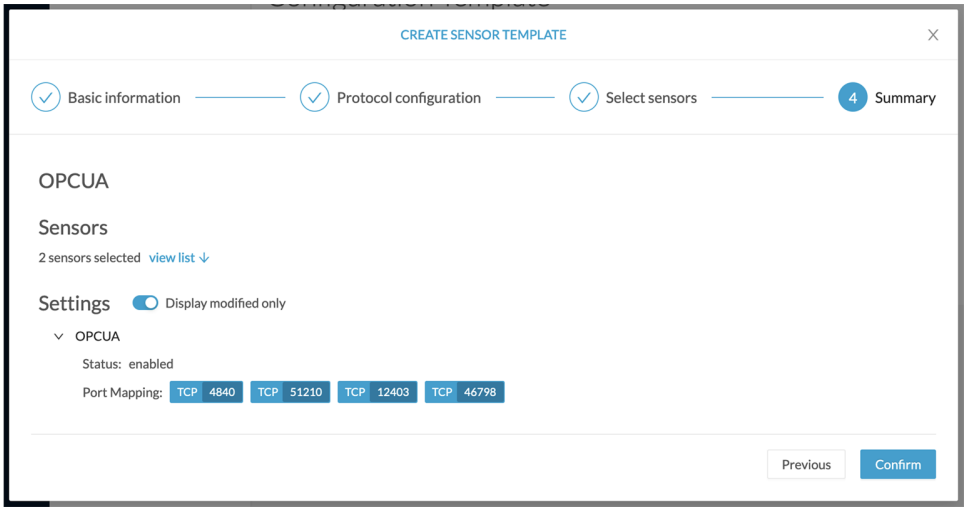
Step 9 Click **Next**.

Step 10 Select the sensor(s) you want to apply the template to.



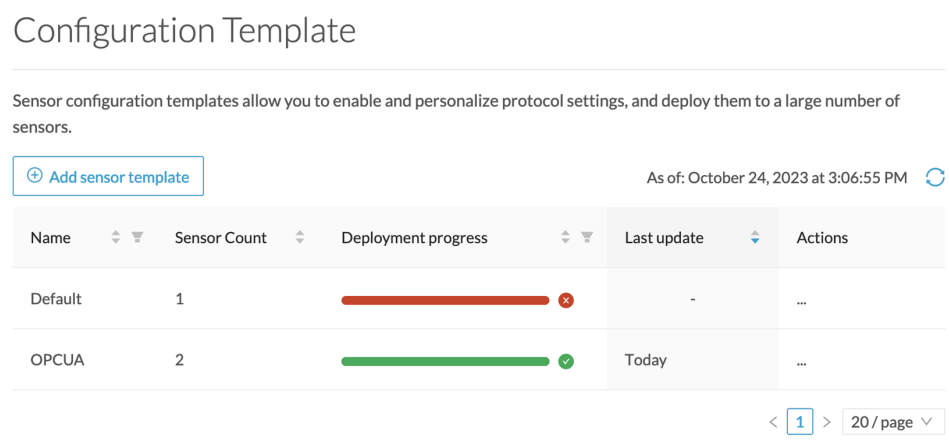
Step 11 Click **Next**.

Step 12 Check the template configurations and **Confirm** its creation.



The configuration is sent to the sensors. Configuration deployment will take a few moments.

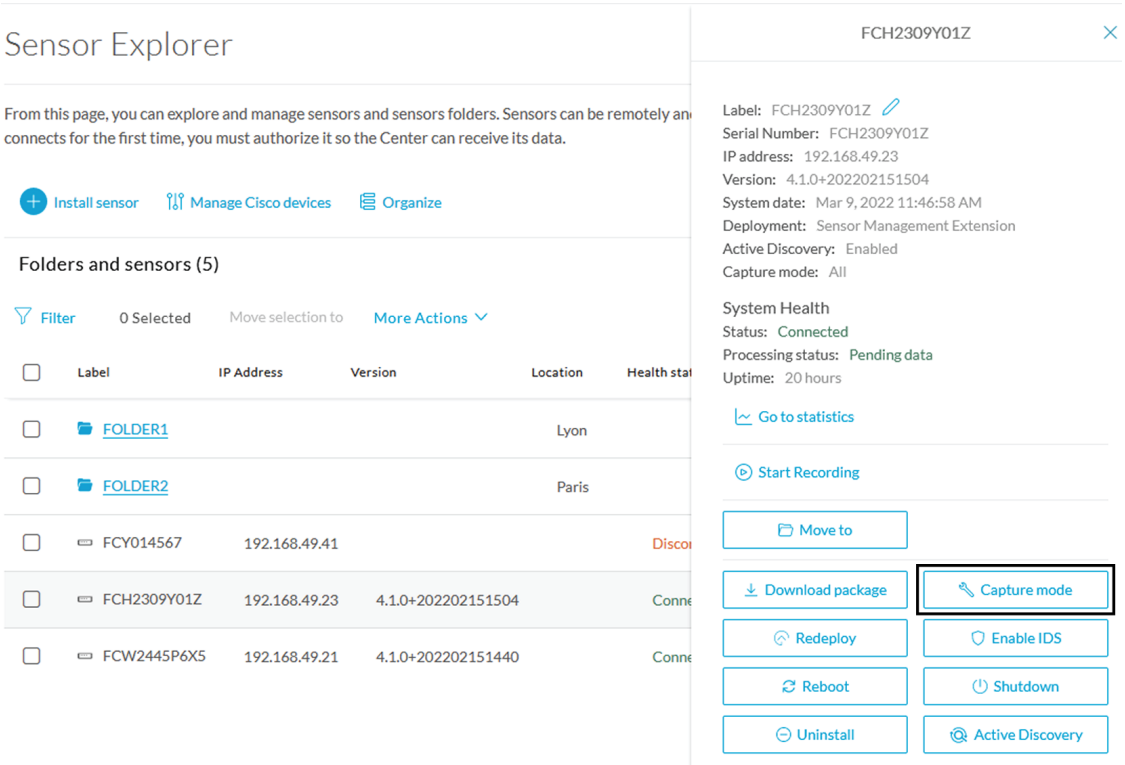
The OPCUA template appears in the template list with its two assigned sensors.



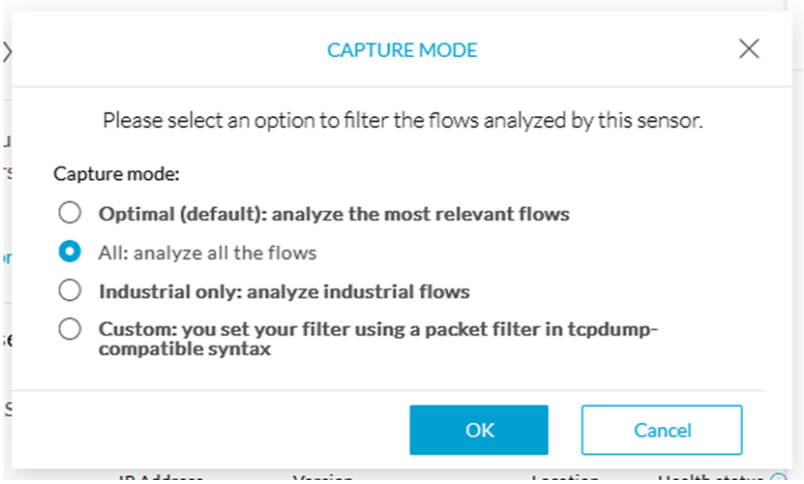
Set a capture mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. You can set it by clicking an online sensor in the sensors list of the Sensor Explorer page or during a sensor installation.

Setting the capture mode on a sensor from the right side panel:



Capture modes:



The aim is mainly to focus the monitoring on relevant traffic but also to reduce the load on the Center.

For example, a common filter in a firewall can consist of removing the network management flows (SNMP). This can be done by setting a filter like "not (port 161 and host 10.10.10.10)" where "10.10.10.10" is the network management platform.

Using Capture mode Cisco Cyber Vision performance can be improved on large networks.

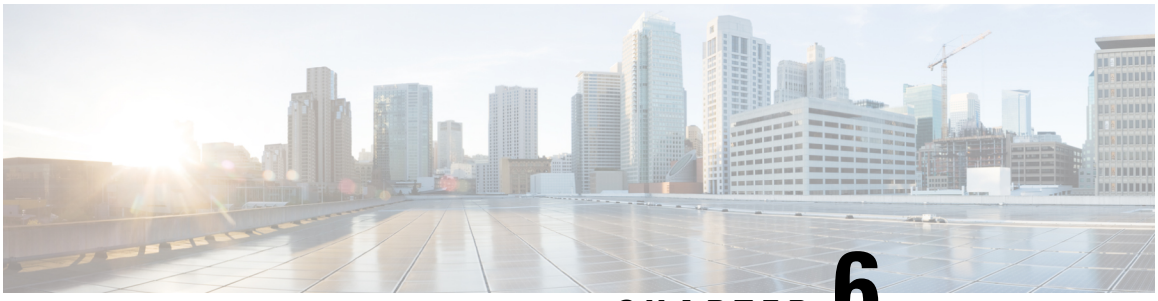
Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

You can set the capture mode in the installation wizard when enrolling the sensors during the Center installation. This option is recommended if you already know which filter to set. Otherwise, you can change it at any time through the Sensor Explorer page in the GUI (provided that the SSH connection is allowed from the Center to the sensors).

Note You can set a capture mode to offline sensors from a file containing the filter and registered on the USB drive. This will be then plugged on the Offline USB port of the device. For more information about setting a capture mode on an offline sensor contact the support.

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.
- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.
- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.
- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.



CHAPTER 6

Maintenance

Upgrade procedures

Sensor Self Update

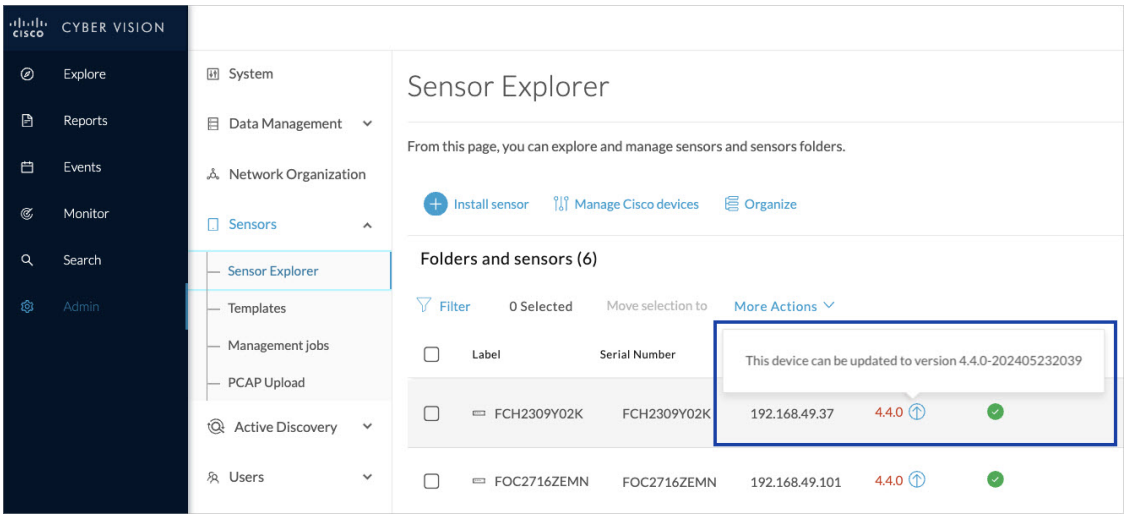
Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.1 provides the necessary foundation for sensor self-updates. However, the self-update feature will only be functional in future releases.

Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

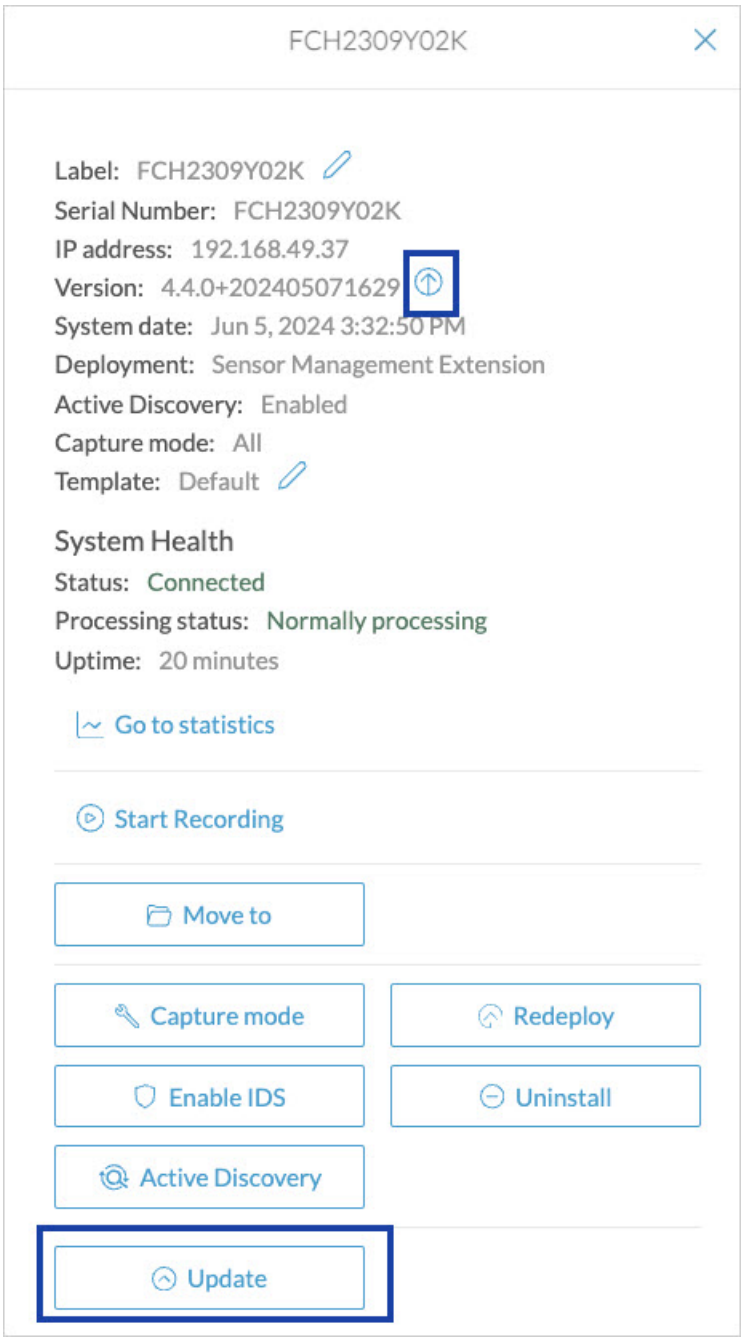
- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

Update Warnings

In the Cisco Cyber Vision center on the Sensor Explorer page (Admin – Sensors – Sensor Explorer), users receive an alert to update the sensor. When this happens, the version number turns red, and a blue arrow with a tooltip indicates the sensor is upgradeable.



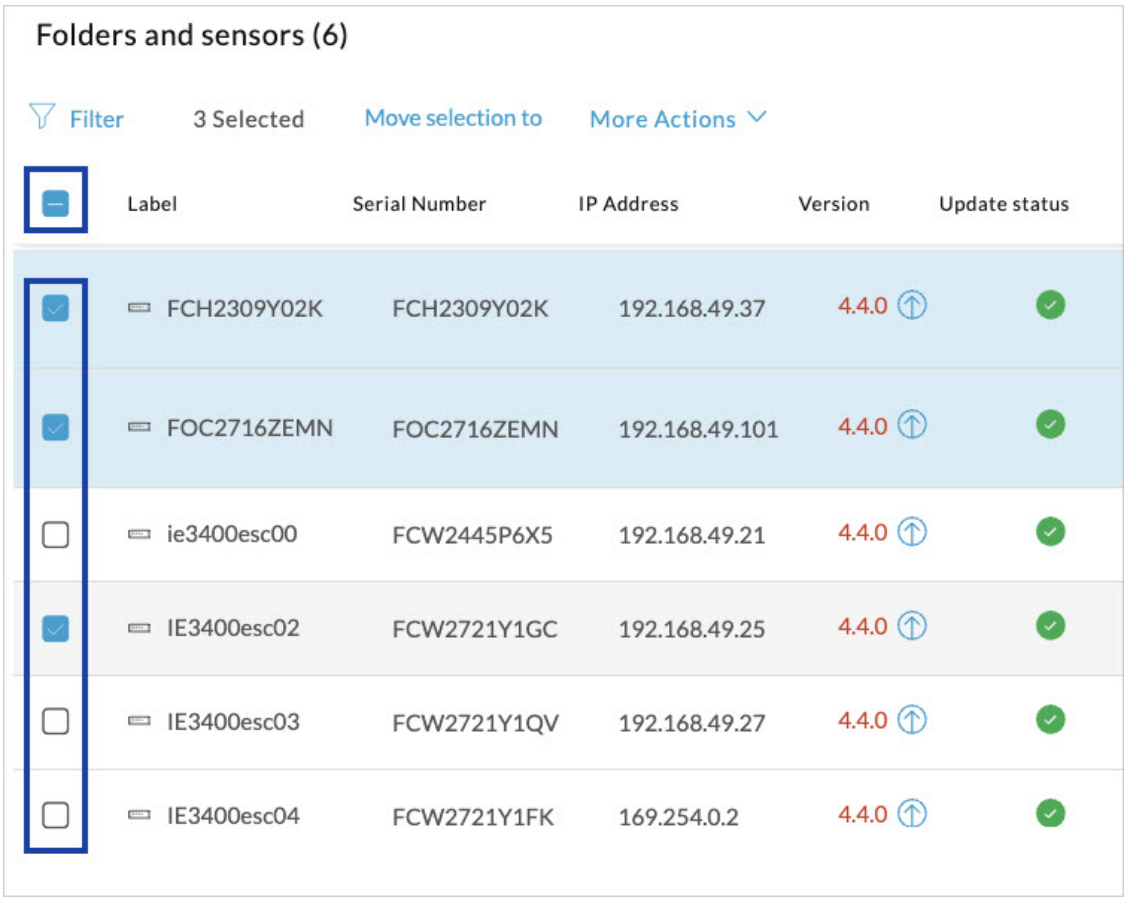
On the sensor's right-side, the same blue arrow and an **Update** button is visible.



Update Procedure

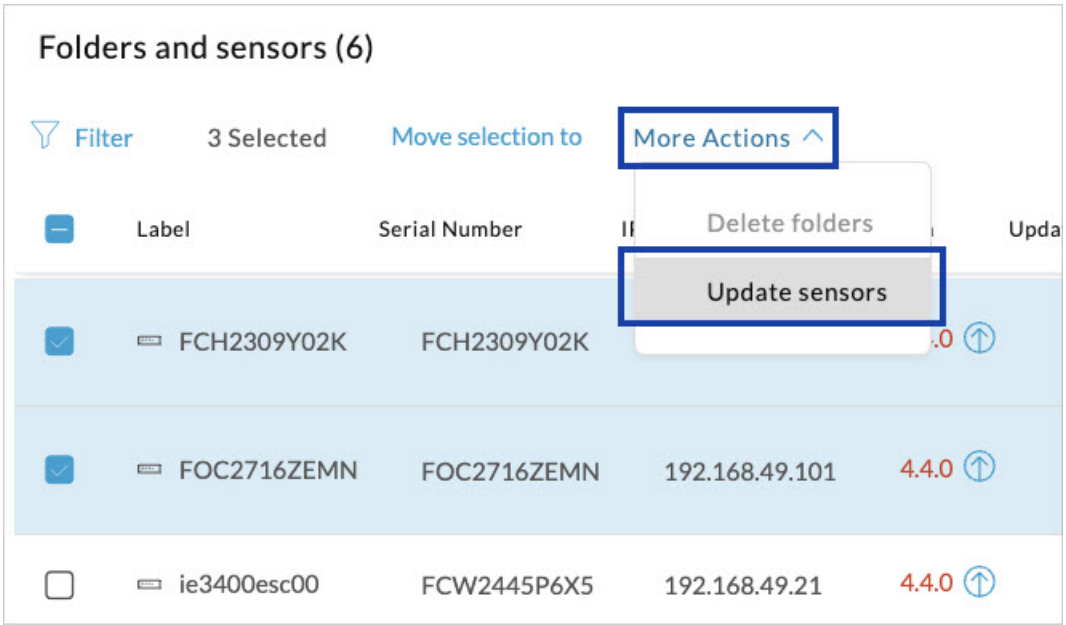
Procedure

Step 1 Use the checkboxes on the left to select multiple sensors.

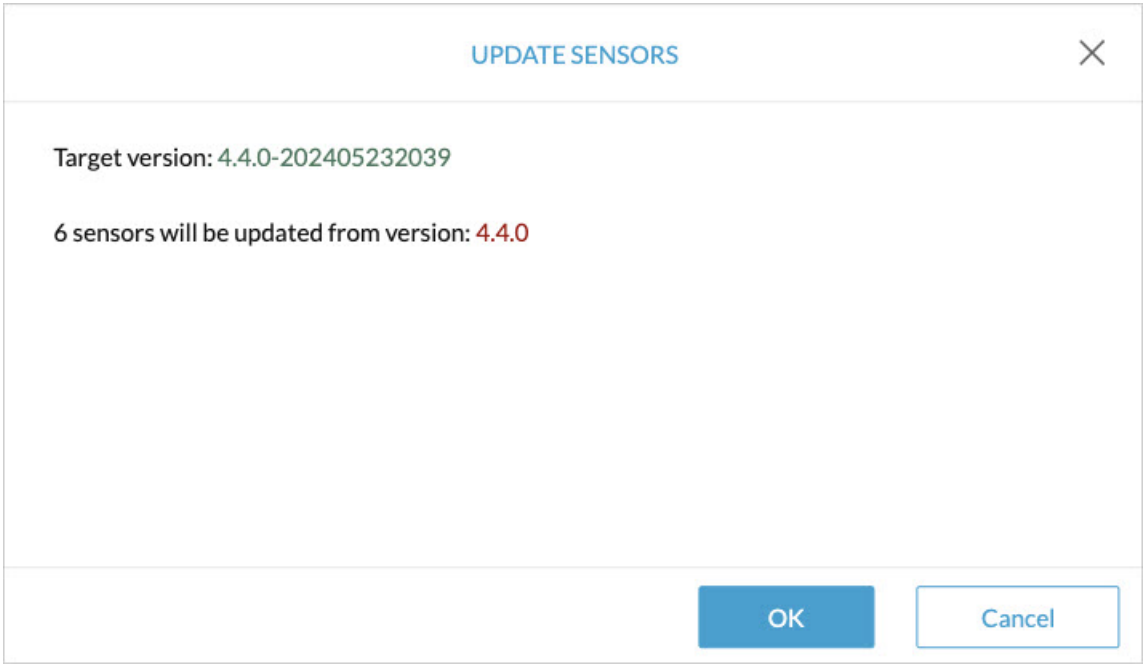


Step 2 Go to the **More Actions** and click **Update sensors**.

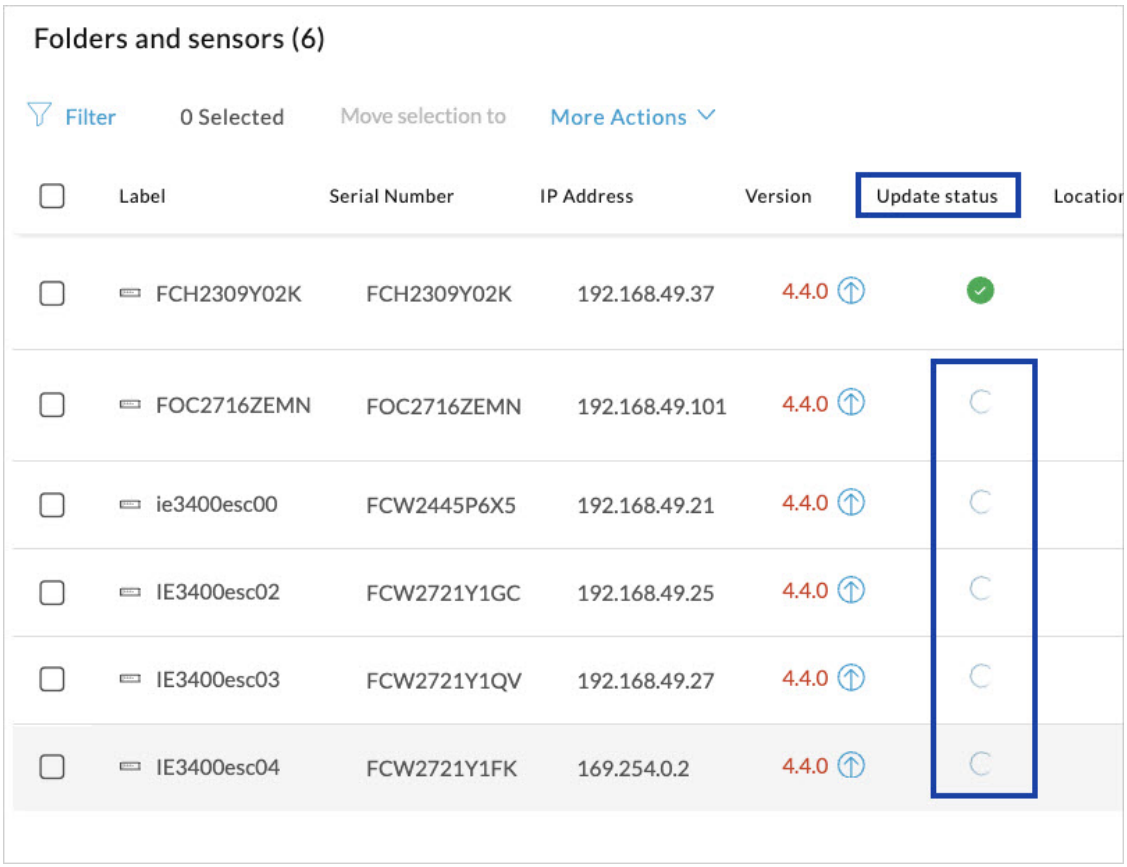
The sensor self-update menu appears.



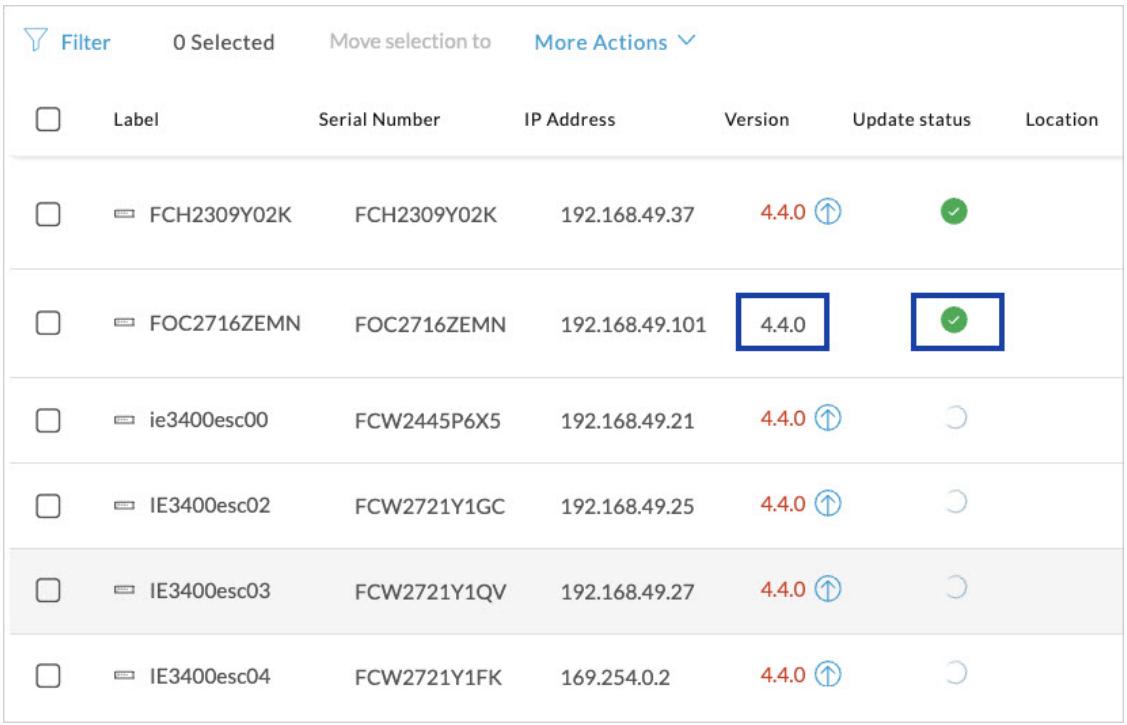
Step 3 Click **OK**.



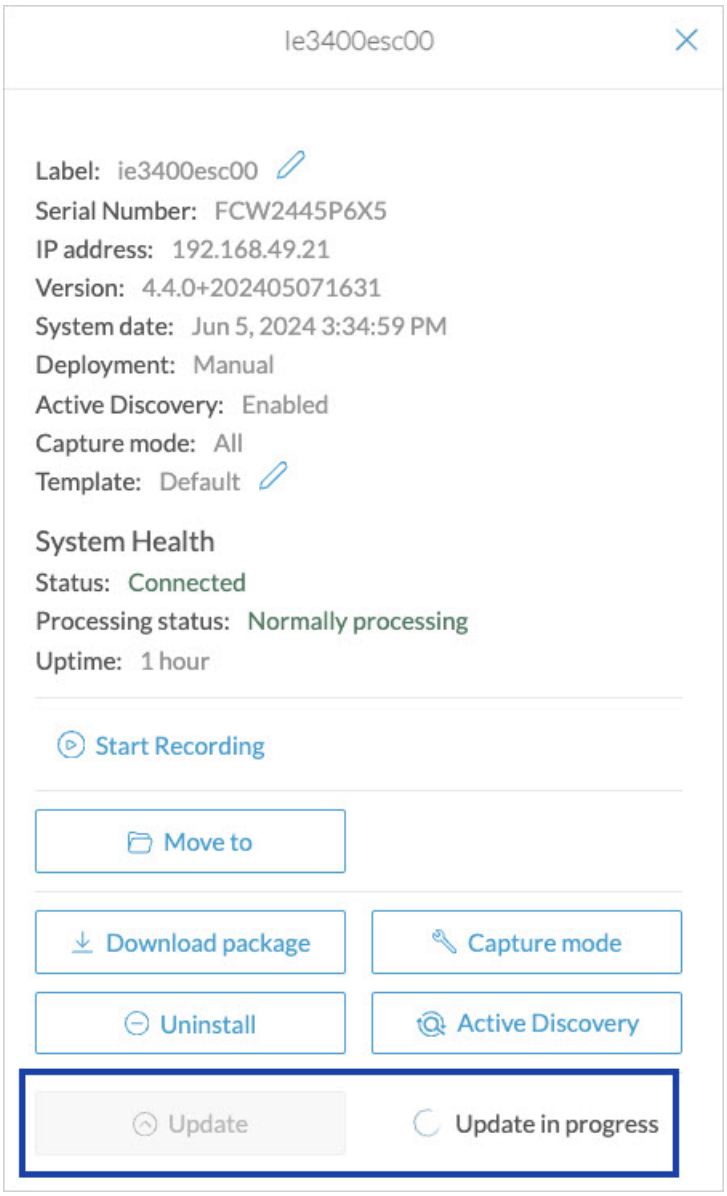
Step 4 During the update, a blue circle appears in the **Update status** column.



Step 5 After the update, the version number turns black, and a green symbol appears in the **Update status** column.

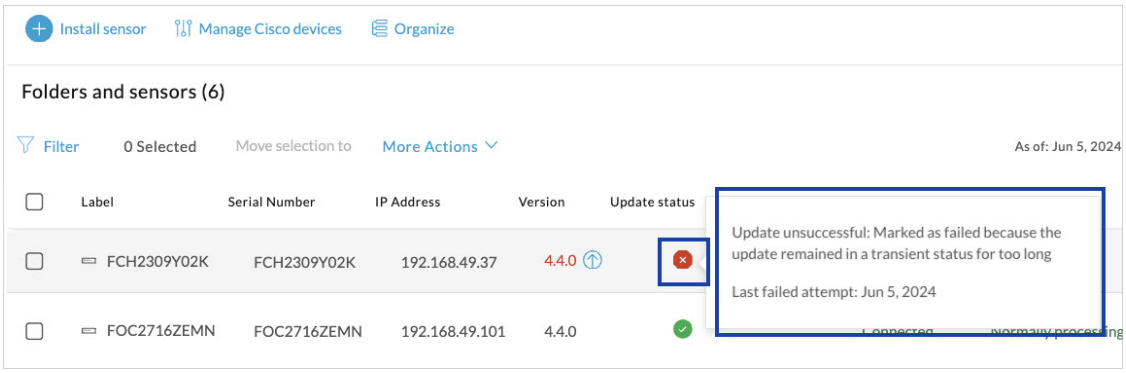


Step 6 The **Update in progress** status is visible.



Update Failure

If the update is unsuccessful, the **Update status** column displays a red cross and a message that provides the details.



Upgrade through the Cisco Cyber Vision sensor management extension

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

Update the sensor management extension

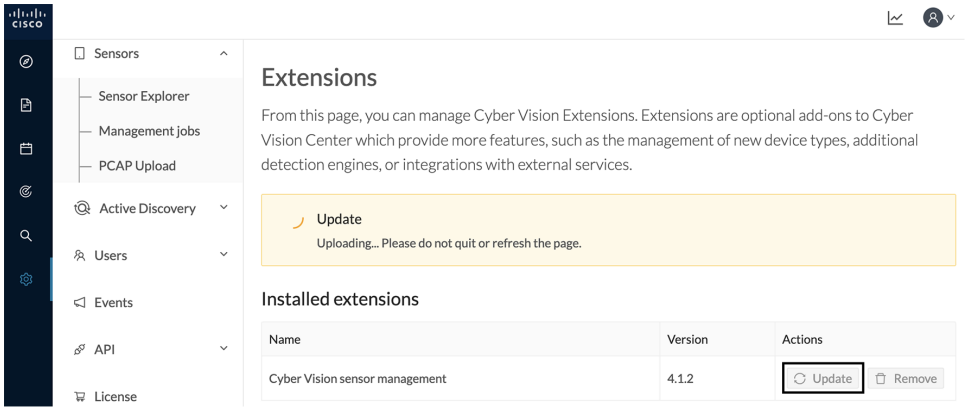
The Cisco Cyber Vision sensor management extension must be up-to-date to update IOx sensors.

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.



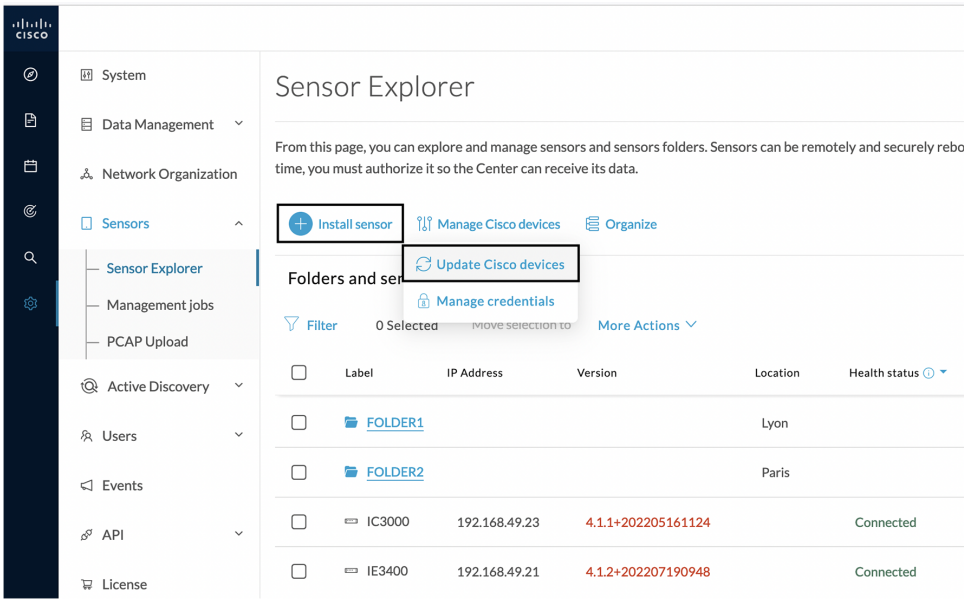
Update the sensors

Procedure

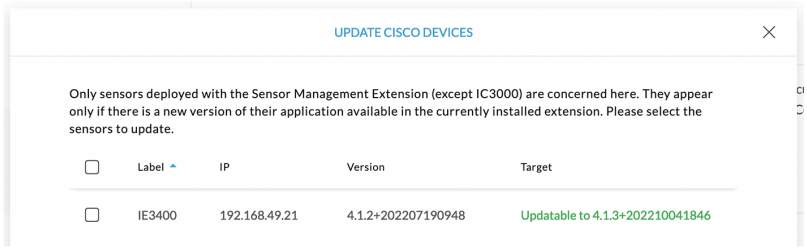
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

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

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



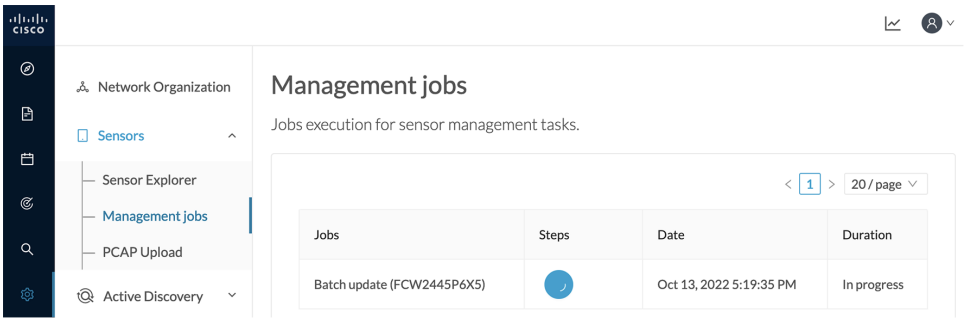
The update Cisco devices window pops up listing all sensors that have been deployed with the sensor management extension.



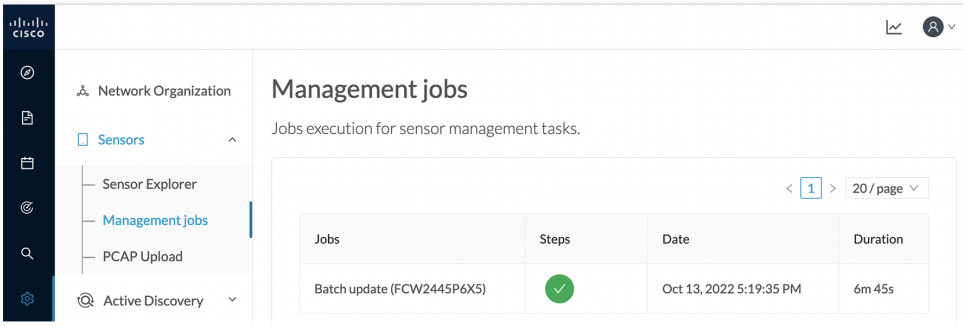
Step 3 Select the sensors you want to update.

Step 4 Click **Update**.

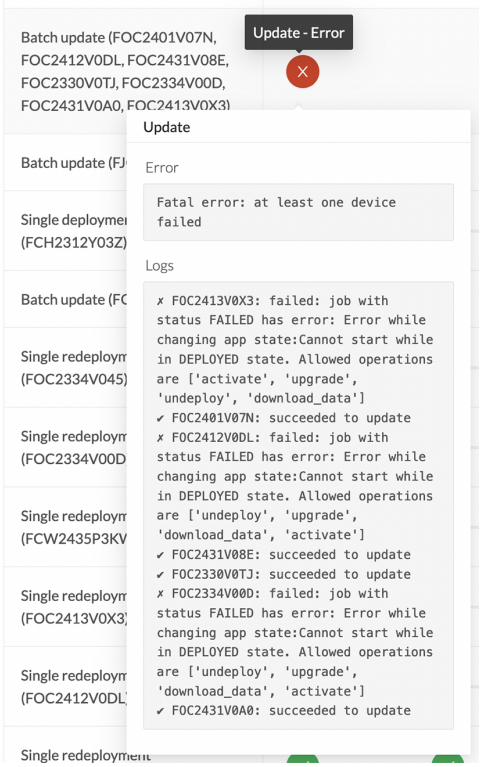
The sensors' update status appear in the Management jobs page in batches per sensor type and of maximum ten sensors per batch.



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



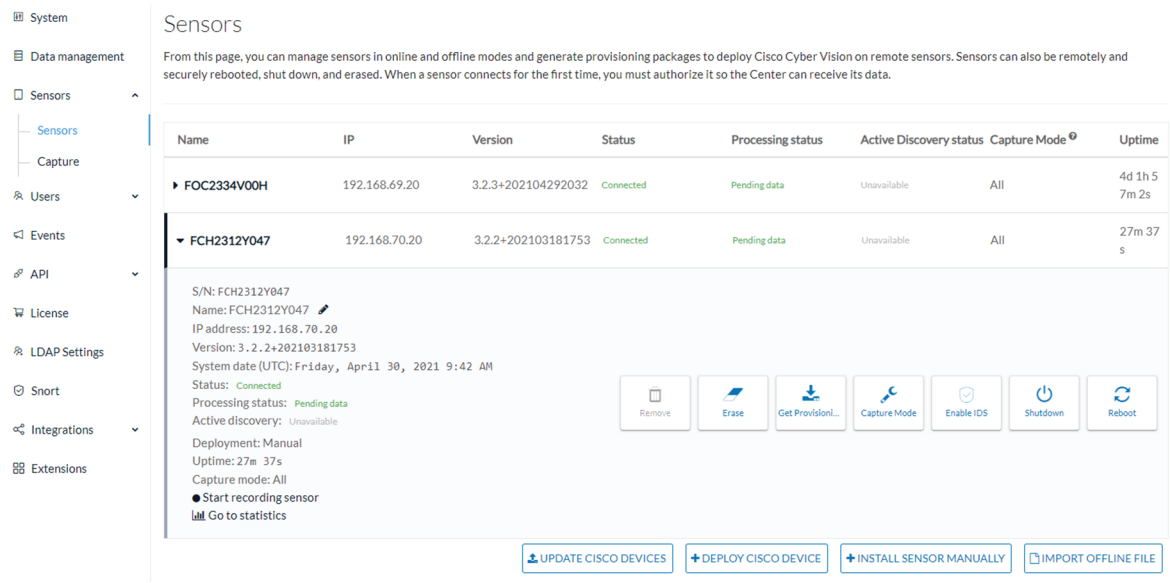
If the batch update fails, click the red update error icon to see logs.



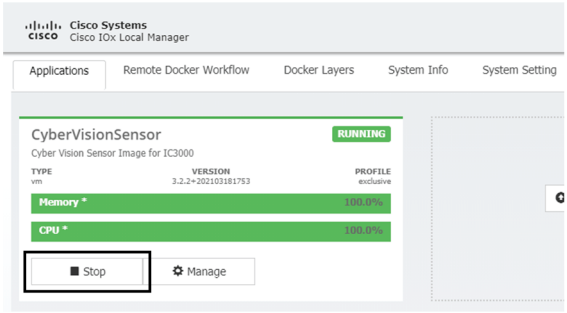
Upgrade through the Local Manager

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

In the Cisco Cyber Vision sensor administration page, the sensor is in 3.2.2. In the example below, we will upgrade the sensor to Cisco Cyber Vision version 3.2.3.

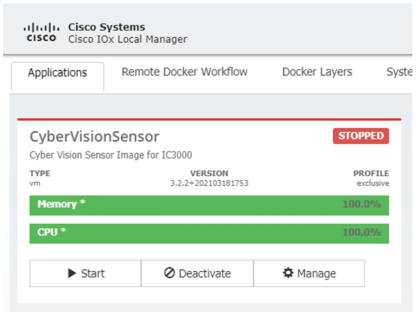


1. Access the Local Manager.
2. Stop the application.

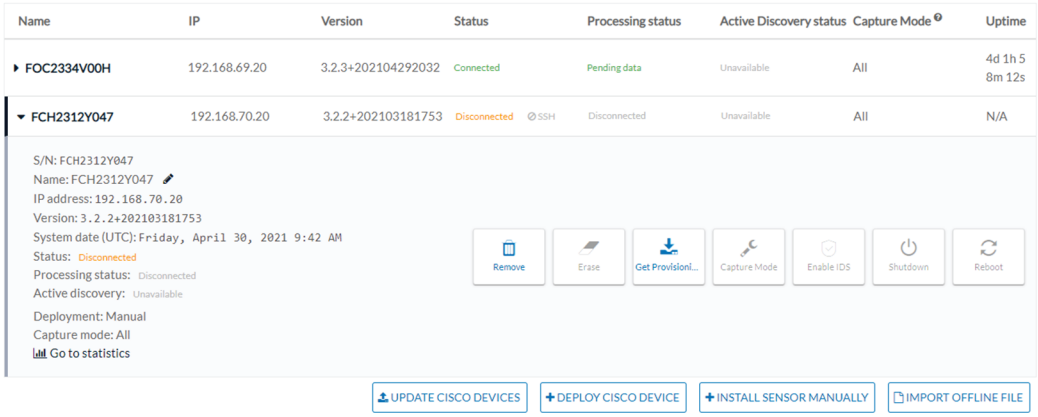


The operation takes a few moments.

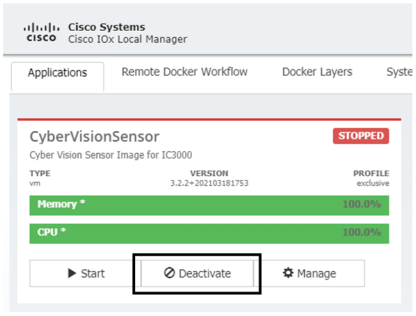
The application status switches to STOPPED.



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

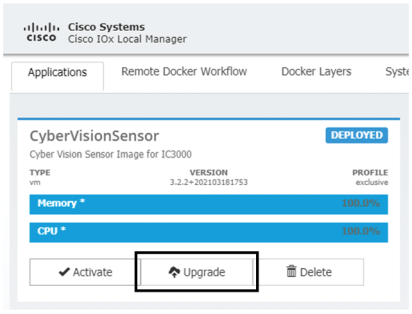


3. In the Local Manager, click the Deactivate button.

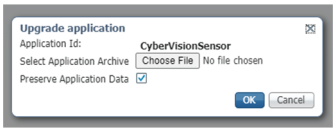


The application status moves to "DEPLOYED".

4. Click Upgrade.

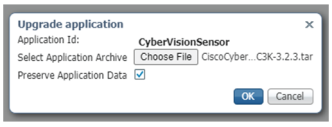


The pop up Upgrade application appears.



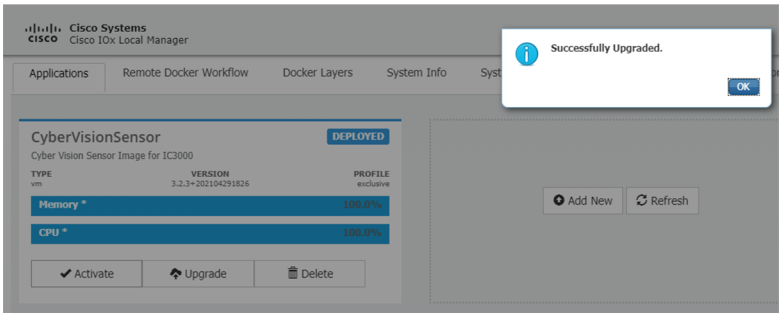
5. Select the option Preserve Application Data.
6. Select the new version of the application archive file.

   e.g. Cisco-Cyber-Vision-IOx-IC3K-3.2.3.tar



The operation takes a few moments.

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



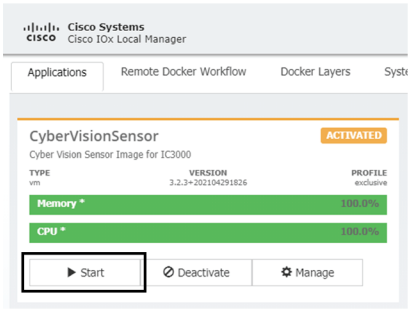
7. Check the number of the new version.
8. Click Activate.
9. Check configurations.

   It can happen that network configurations are lost during the upgrade. If they are, refer to Configure the sensor virtual application, on page 26 **and do as explained.**

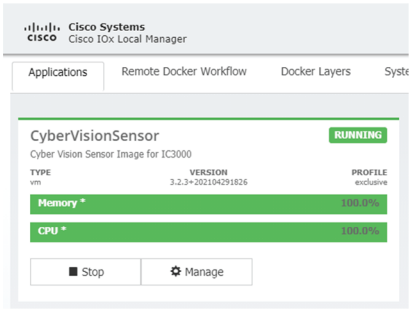
10. Click the Activate App button.

    The application status moves to ACTIVATED.

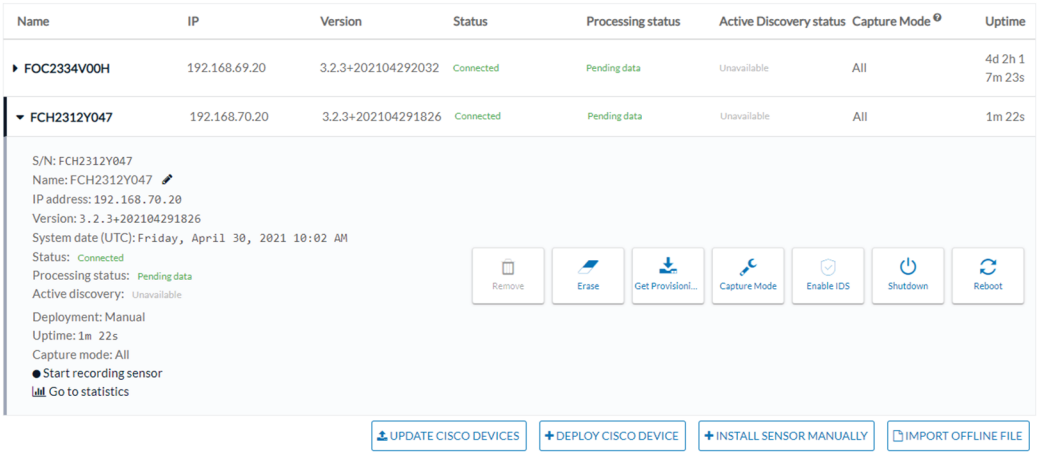
11. Click the Start button.



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.



Certificate renewal

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

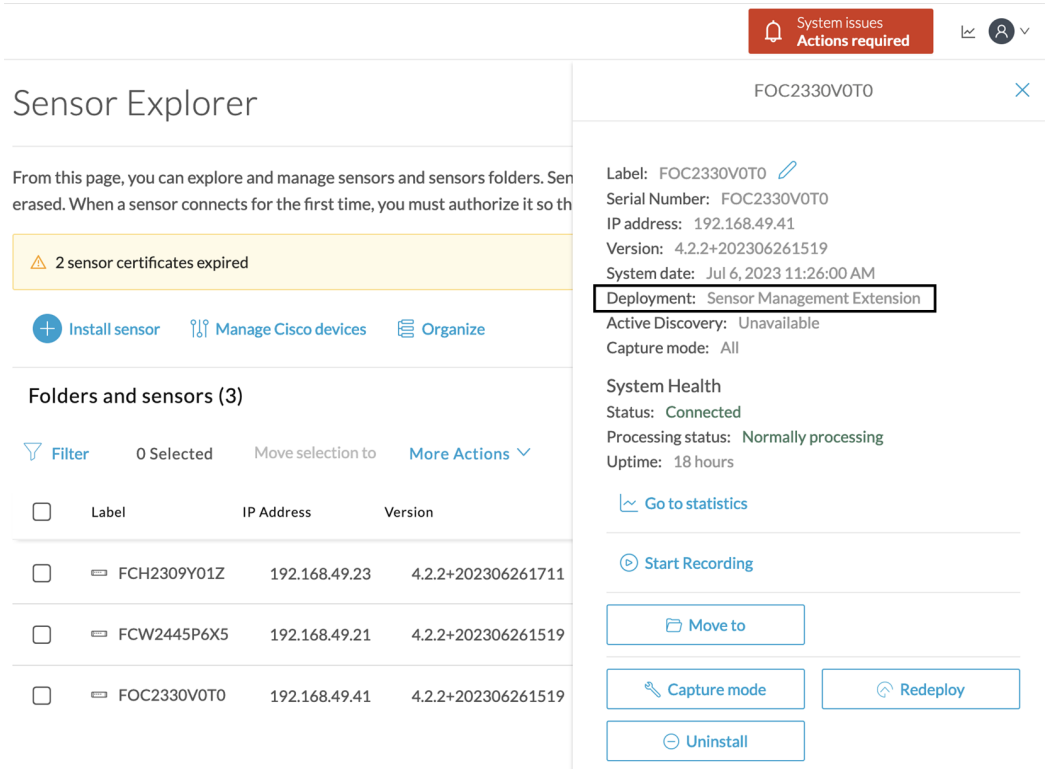
Sensor certificates must be renewed manually. The procedure used differs whether the certificate is already expired or not and whether the sensor has been deployed using the sensor management extension.

- If the certificate is still valid, refer to Sensor certificate renewal, on page 60.
- If the sensor was deployed with the sensor management extension, refer to Sensor certificate renewal, on page 60.
- If the certificate is outdated, and was deployed manually, refer to Sensor certificate renewal through the Local Manager, on page 63.

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).

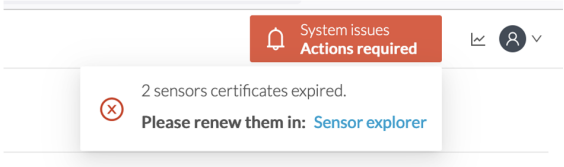


- In the case of sensors deployed manually, it only applies if the sensors certificate have not expired yet (i.e. the sensor certificate status is Expire Soon).

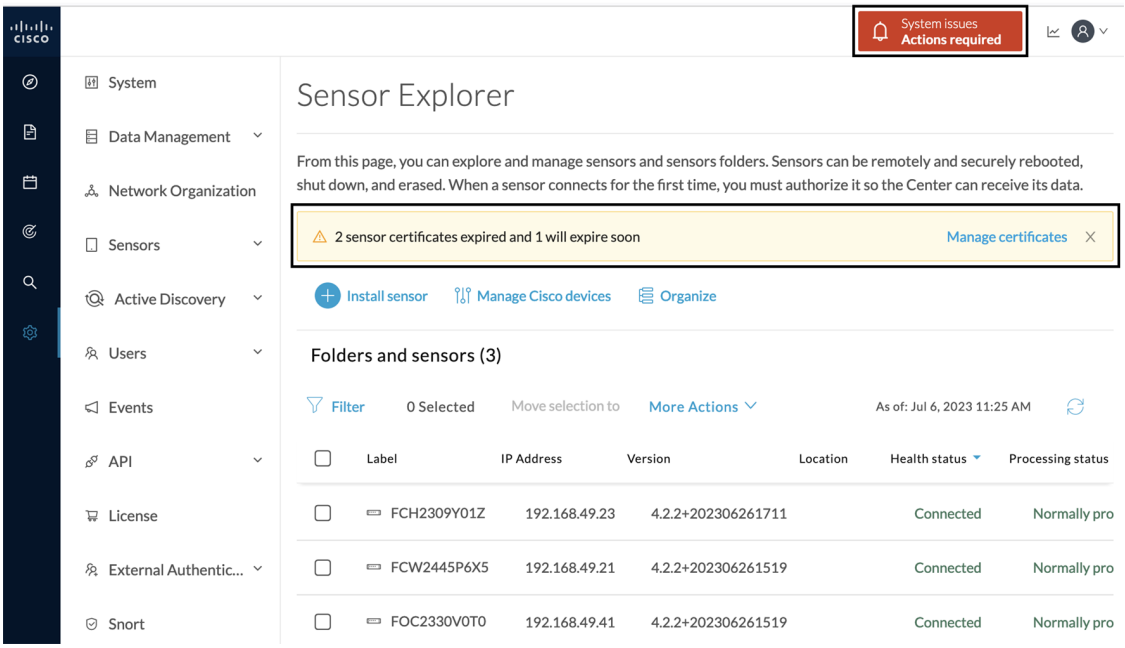
If sensors have been deployed manually and the certificate expiration date is exceeded, refer to Sensor certificate renewal through the Local Manager, on page 63.

Procedure

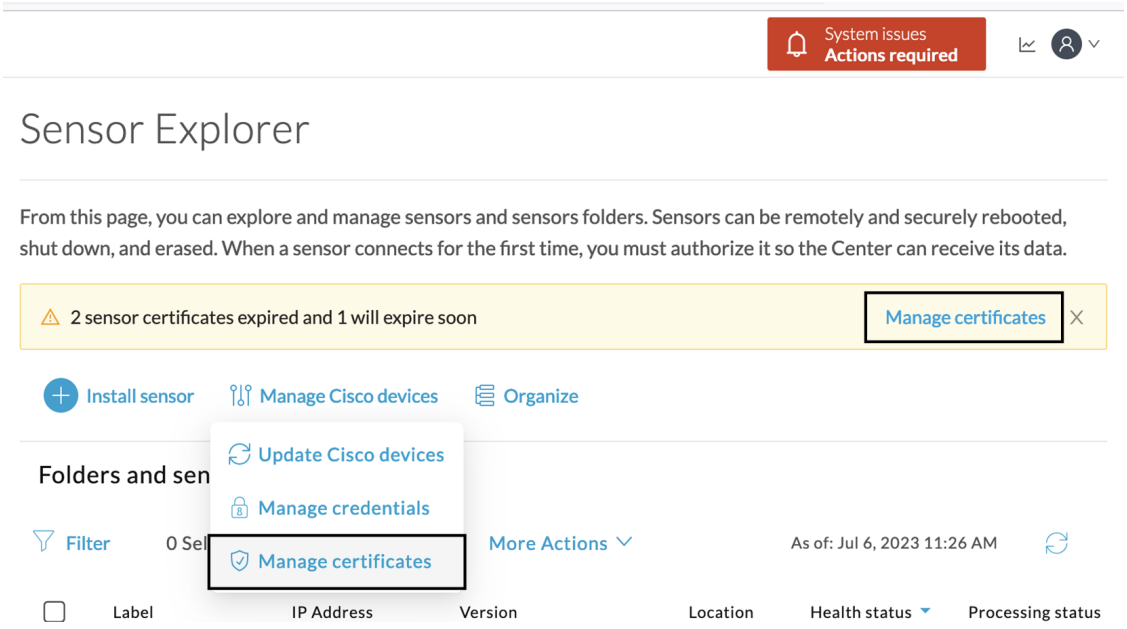
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer or click the top banner alert to access the Sensor Explorer page directly.



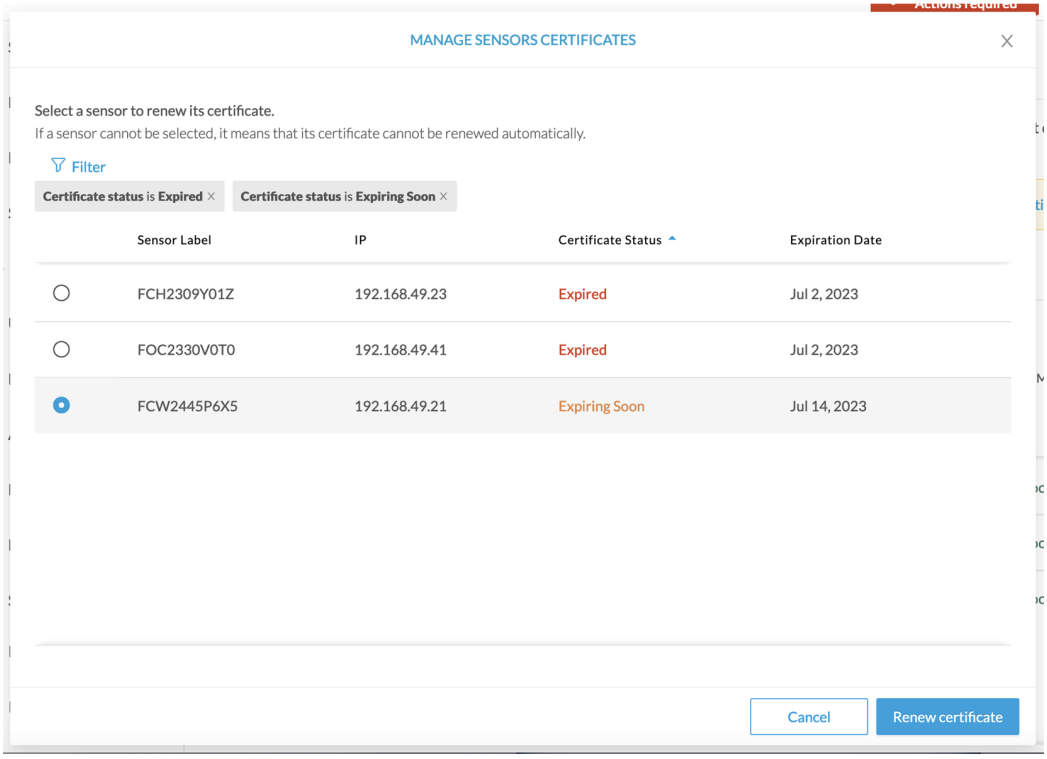
Another alert is displayed.



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

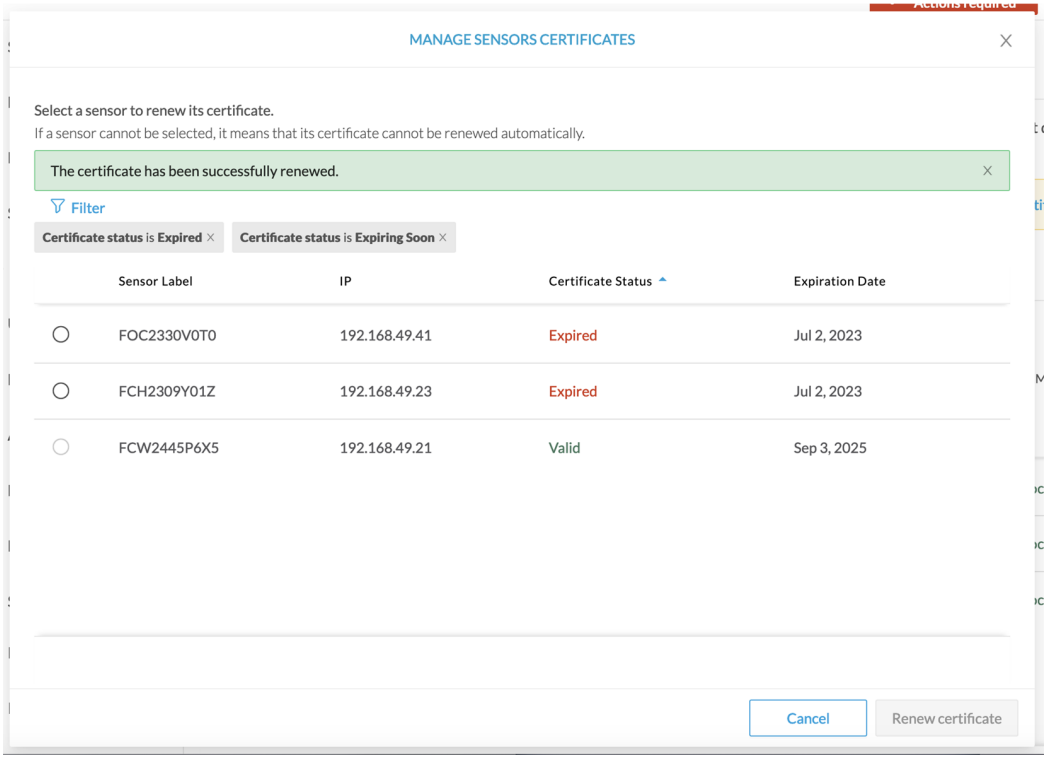


The **Manage sensors certificates** window opens.



Step 3 Select the sensor with the status Expiring Soon.

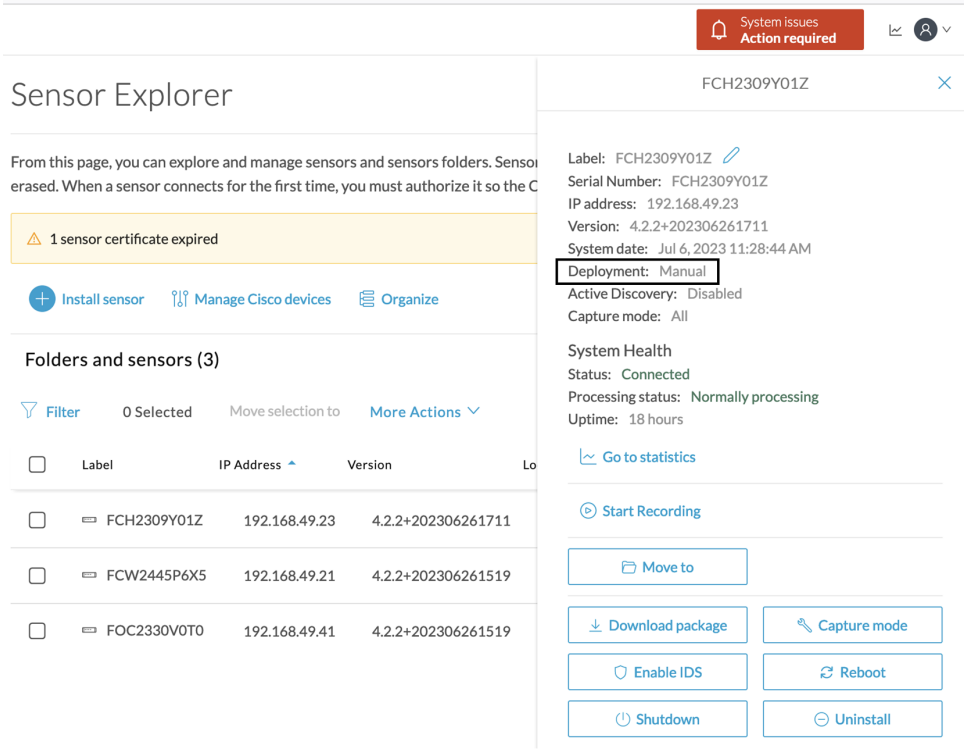
Step 4 Click **Renew certificate**.



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.

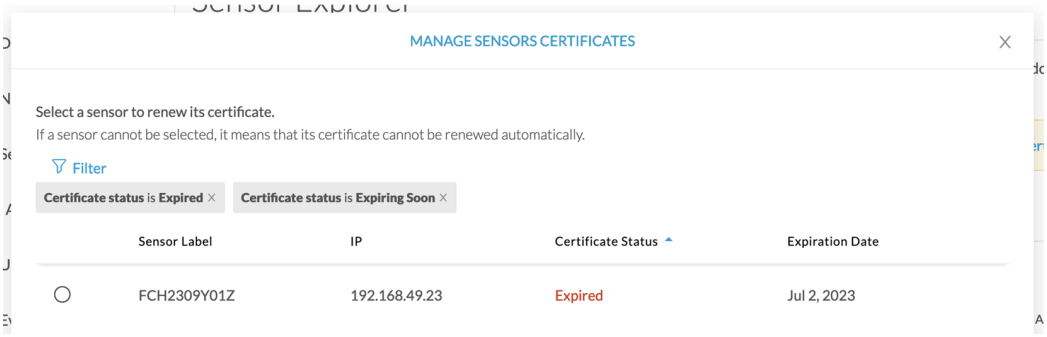


Procedure

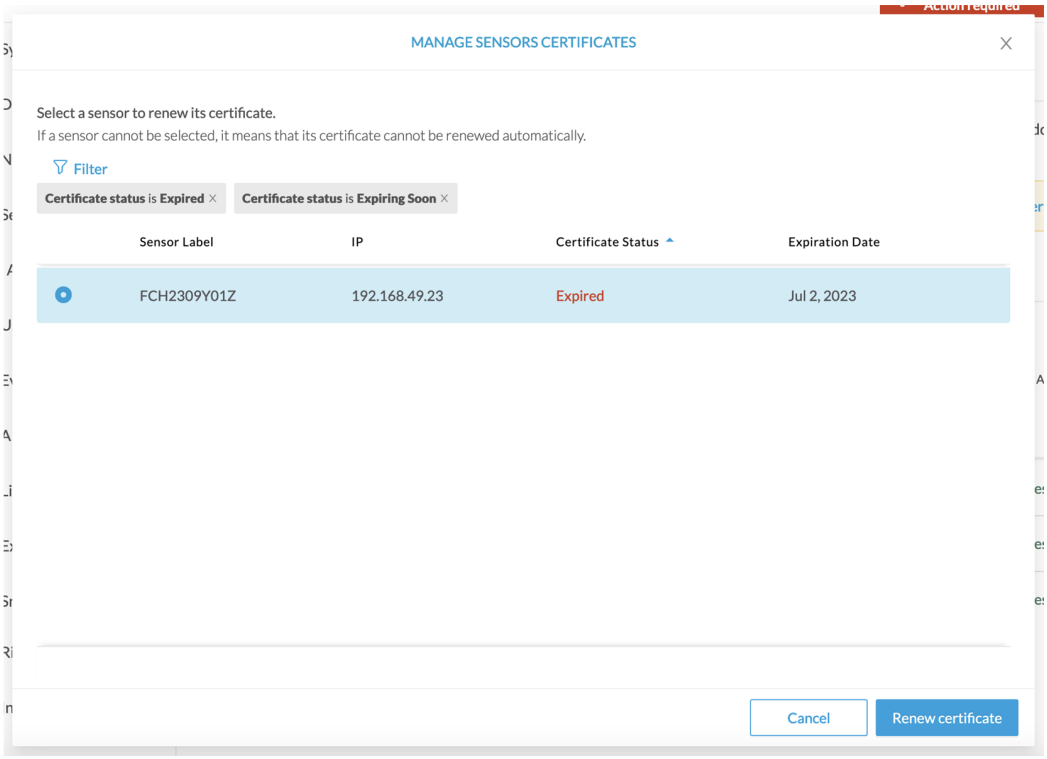
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

Step 2 Click **Manage Certificates**.

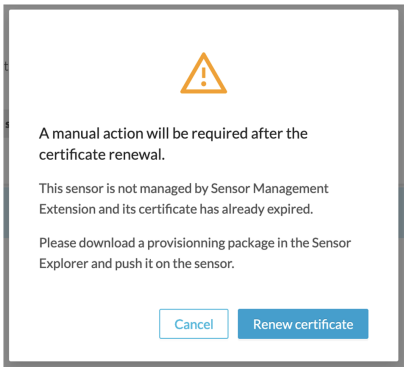
The Manage sensors certificates window appears.



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

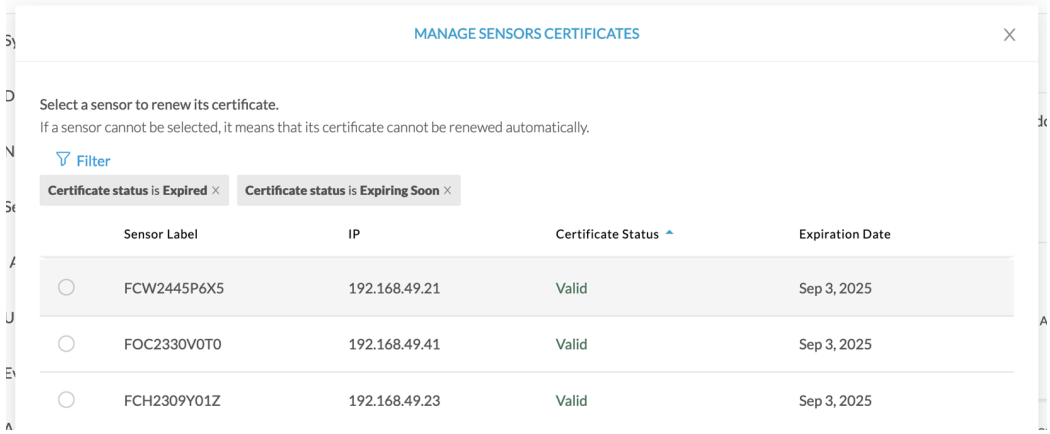


A message is displayed.



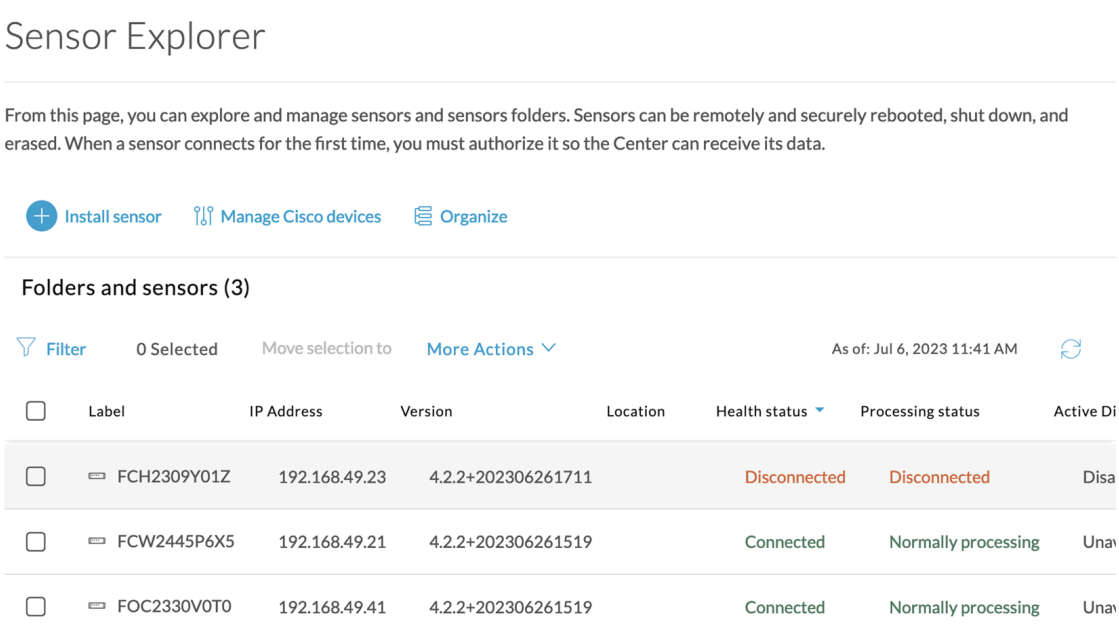
Step 4 Click **Renew certificate** again.

The sensor certificate status appears as valid.



Step 5 Close the Manage sensors certificates window.

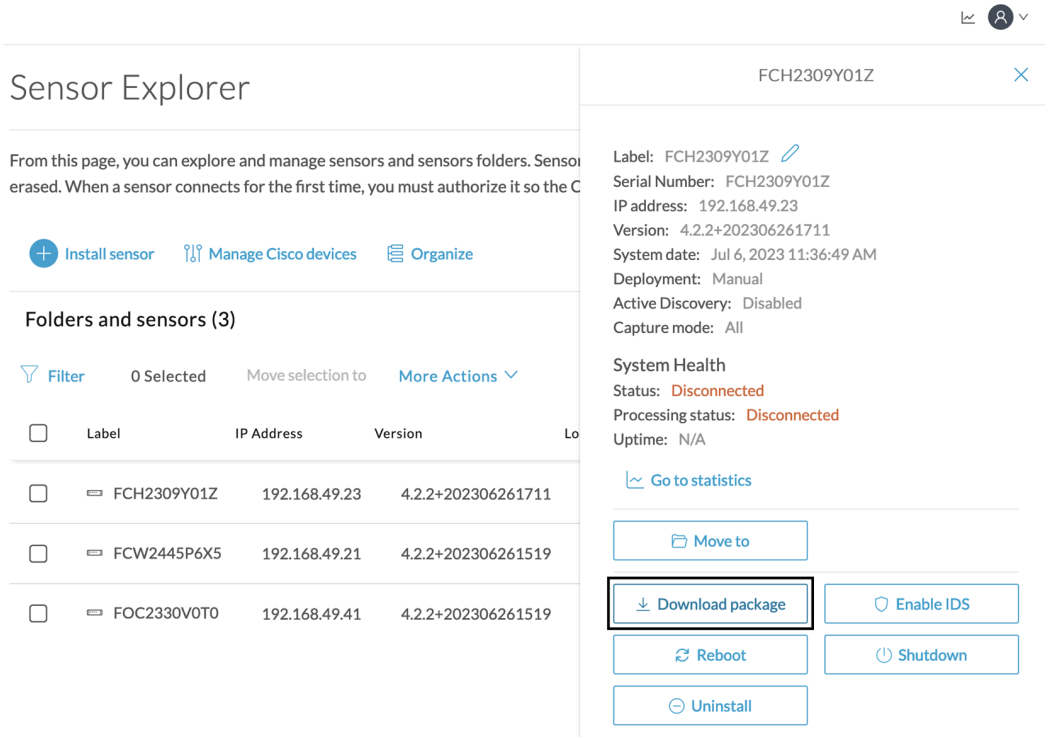
The sensor's health and processing status appear as Disconnected.



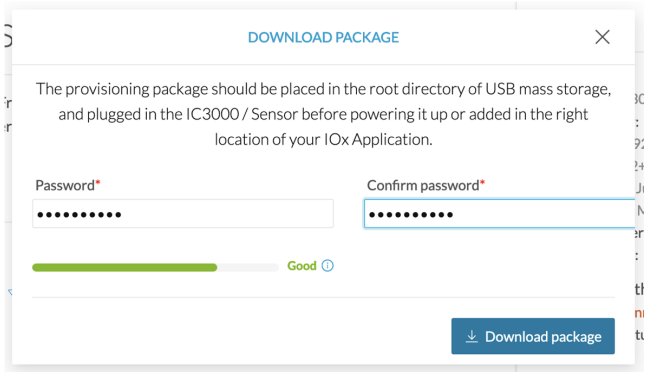
Step 6 Click the sensor in the list.

Its right side panel opens.

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



Step 8 Type the Local Manager's password or set it if not already done. Make sure to keep this piece of information stored as it will be asked to access IOx Local Manager and for further troubleshooting and configuration purposes.



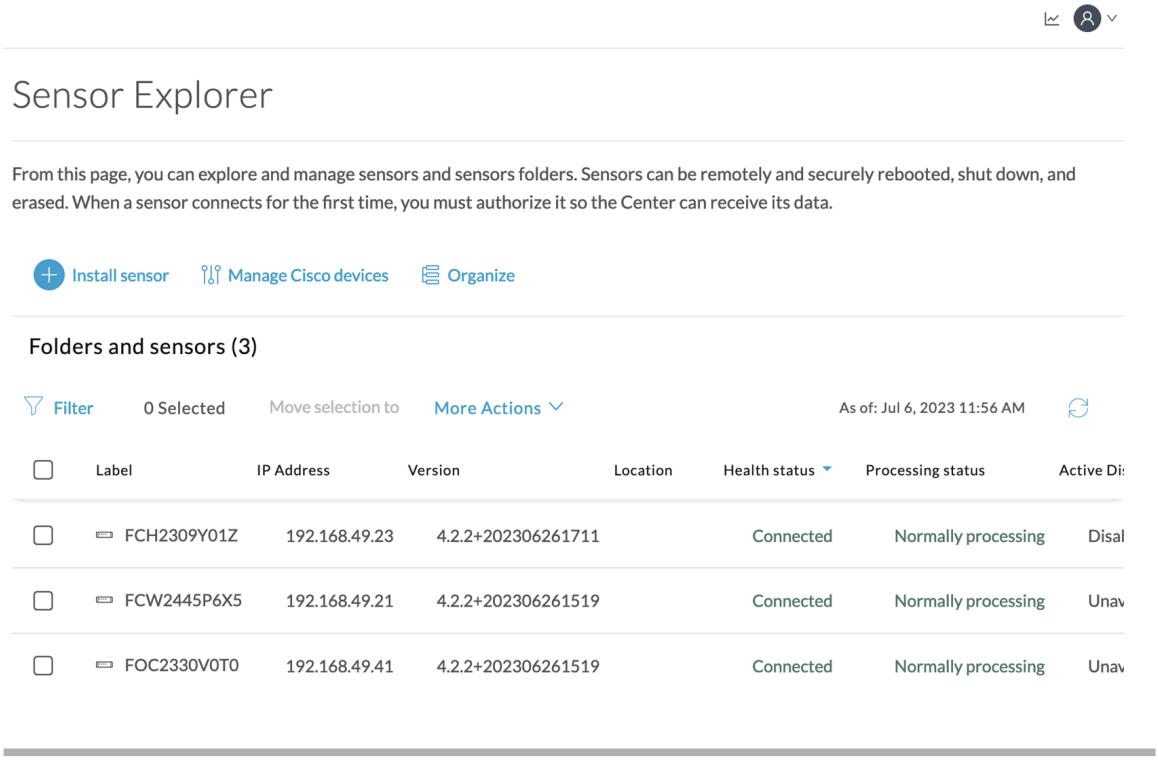
Step 9 Click **Download package**.

Step 10 Import the provisioning package in the Local Manager. To do so, refer to Import the provisioning package, on page 32 .

Step 11 In the sensor's CLI, type the following command to enroll the sensor:

```
sbs-sensor-enroll-offline -fp /data/iox/appdata/cybervision-sensor-config.zip
```

Step 12 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
Label
IP Address
Version
Location
Health status
Processing status
Active Di
FCH2309Y01Z
192.168.49.23
4.2.2+202306261711
Connected
Normally processing
Disal
FCW2445P6X5
192.168.49.21
4.2.2+202306261519
Connected
Normally processing
Unav
FOC2330V0T0
192.168.49.41
4.2.2+202306261519
Connected
Normally processing
Unav