



## Installation procedures

---

- [Procedure with the Sensor management extension, on page 1](#)
- [Procedure with the Local Manager, on page 11](#)

### 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](http://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.

The screenshot shows the Cisco Cyber Vision Software Download page for release 3.1.1. The page includes a search bar, a version selection menu, and a table of download files. The file 'Cisco Cyber Vision Sensor Management Extension for IoX sensor setup' is highlighted with a red box.

File Information	Release Date	Size	
Cisco Cyber Vision Sensor Management Extension for IoX sensor setup CiscoCyberVision-sensor-management-3.1.1.ext	30-Jul-2020	666.87 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
VMware OVA (Center) - CiscoCyberVision-3.1.1.ova CiscoCyberVision-3.1.1.ova	28-Jul-2020	251.81 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Hyper-V VHDX (Center) - CiscoCyberVision-3.1.1.vhdx CiscoCyberVision-3.1.1.vhdx	28-Jul-2020	312.00 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>

## 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.

**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.

**Installed extensions**

Name	Version
No Data	

**Install a new extension**

[Import extension file](#)

The file upload takes a few minutes.

## 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.



### Installation

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

## 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.

✓ Installation  
Cyber Vision sensor management installed successfully!

### Installed extensions

Name	Version	Actions
Cyber Vision sensor management	3.2.0	 

### Install a new extension

 Import extension file

## 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

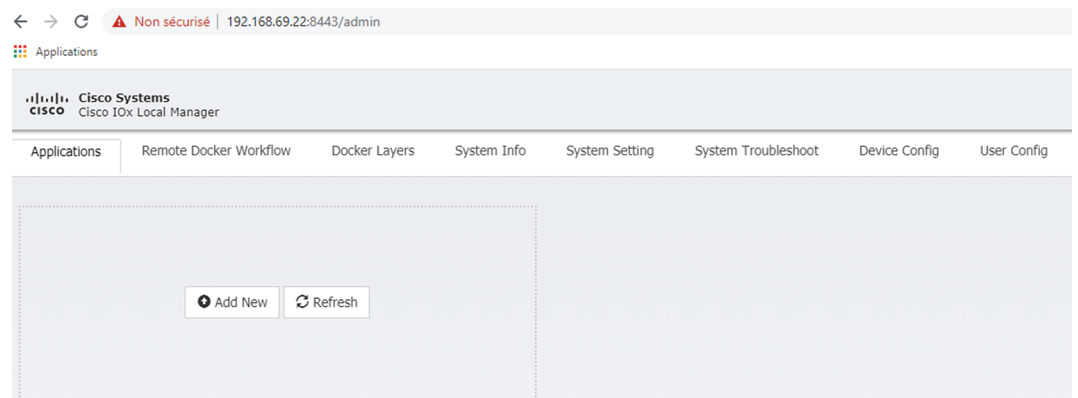
To proceed with the installation, you must first test if you have access to the Cisco IC3000's Cisco IOx Local Manager. To do so:

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`

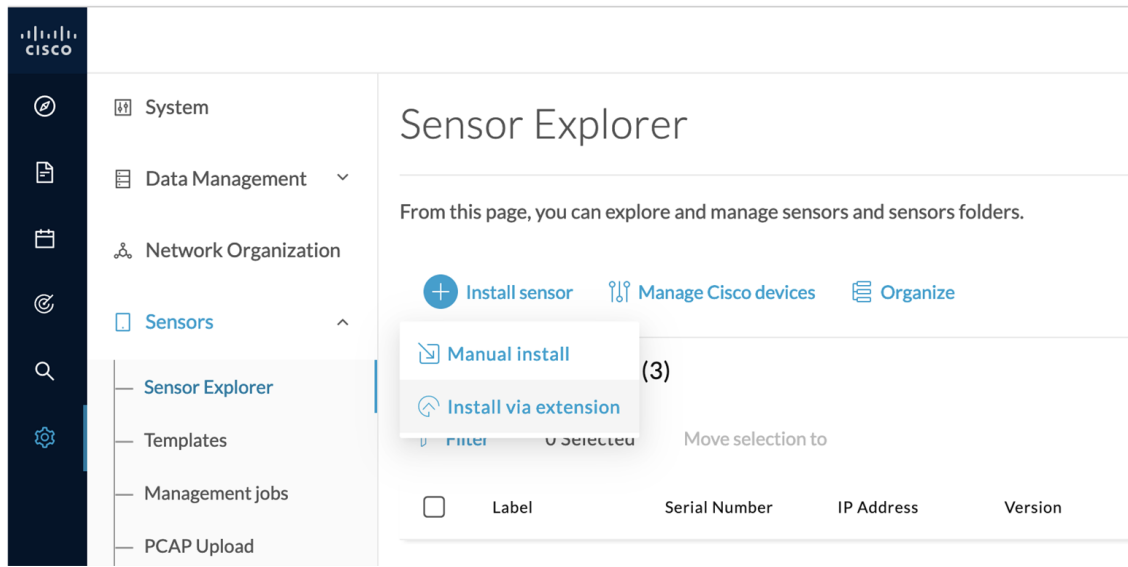
3. If you're able to see the following screen it means that the connectivity between the Cisco IC3000 and IOx Local Manager is on.



# 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)

---

Install via extension

---

### Reach Cisco device

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

<p>IP address*</p> <input type="text" value="192.168.49.22"/>	<p>Port*</p> <input type="text" value="8443"/> <p style="font-size: small; text-align: right;">For example 443 or 8443</p>
---	--

Center collection IP

leave blank to use current collection IP

---

Configuration Template

Template

Default
 ▼

- Step 3** Select a configuration template if required. For more information, refer to [Configure sensor configuration template](#).
- Step 4** Select the credential mode used. For more information, refer to Cisco Cyber Vision GUI Administration Guide available on [cisco.com](http://cisco.com).

Credentials

- Use global credentials (recommended)
- Use custom credentials

Capture mode

- Optimal (default): analyze the most relevant flows
- All: analyze all the flows
- Industrial only: analyze industrial flows
- Custom: set your filter using a packet filter in tcpdump-compatible syntax

xit

Connect

- 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)

Install via extension

### Configure Cyber Vision IOx sensor app

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

Cisco device: IC3000-2C2F-K9

Collection IP address\*

192.168.49.23

Collection prefix length\*

24

Like 24, 16 or 8

Collection gateway

 Exit

Next

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:



Install via extension

## Configure Active Discovery

Please select an application type. If you want to enable Active Discovery on the application, select "Passive and Active Discovery". You will have to add some network interfaces parameters.

- Passive only
- Passive and Active Discovery

Select a physical interface

Int2

Select the port used to send packets

ETH2 NETWORK

IP address\*

192.168.53.23

IP address interface used to do Active Discovery

Prefix length\*

24

Like 24, 16 or 8

[Exit](#)

[Back](#)

[Deploy](#)

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

## Configure Active Discovery

Please select an application type. If you want to enable Active Discovery, select the physical interface parameters.

- Passive only**  
 **Passive and Active Discovery**

Select a physical interface

^

MGMT / Collection (enables DPI on collection interface)

Int1

Int2

Int3

Int4

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

Select a physical interface

Int2
v

Select the port used to send packets

**ETH2 NETWORK**

IP address\*

192.168.53.23

IP address interface used to do Active Discovery

Prefix length\*

24

Like 24, 16 or 8

Back

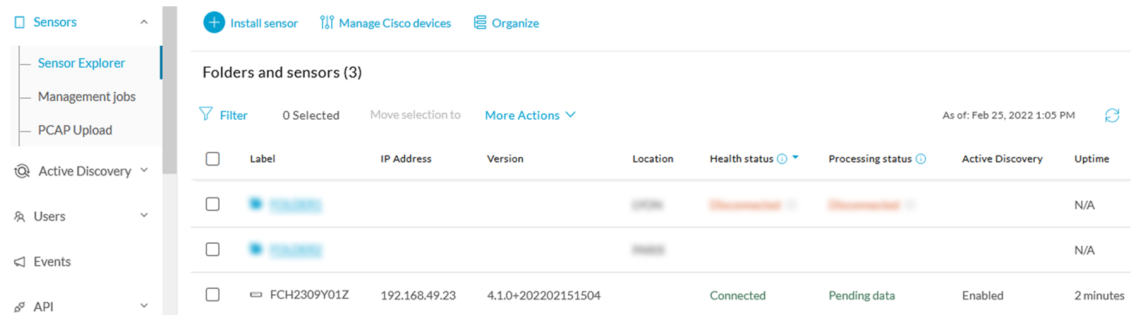
Deploy

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.



Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
							N/A
							N/A
FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data	Enabled	2 minutes



**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).

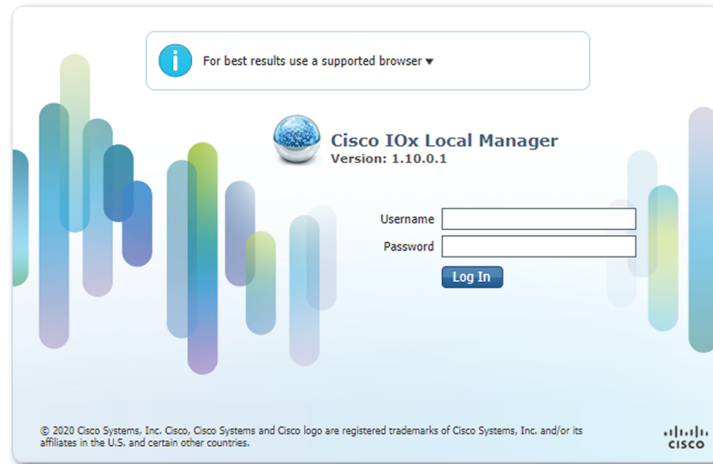
If it's the first time the Cisco IC3000 device is installed with the Local Manager you must first proceed to a [Cisco IC3000 platform initial configuration](#).

### 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](http://cisco.com), i.e. `CiscoCyberVision-IOx-IC3000-<version>.tar`.

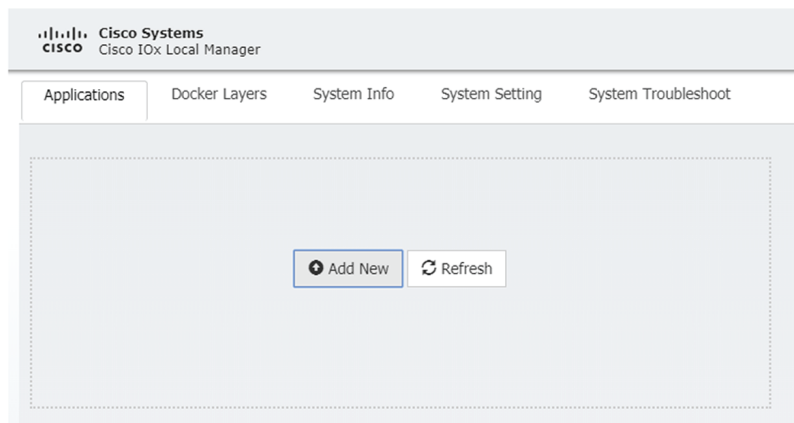
## Access the Local Manager

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:

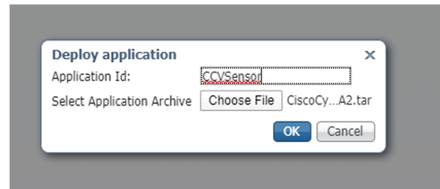


1. Click **Add New**.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file  
(i.e. "CiscoCyberVision-IOx-IC3000-<version>.tar").

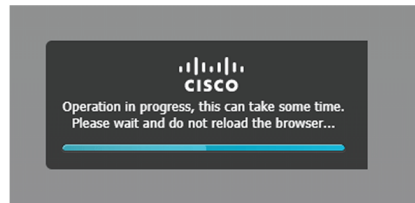


**Note** If you aim to install a sensor with **Active Discovery**, select the required application archive file

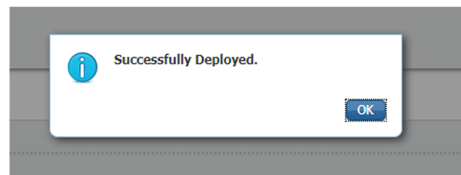
(i.e. "CiscoCyberVision-IOx-Active-Discovery-IC3000-<version>.tar").



The installation takes a few minutes.



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



TYPE	VERSION	PROFILE
docker	4.3.0-202311031406	exclusive

Resource	Usage
Memory *	100.0%
CPU *	100.0%

Buttons:  Activate, Upgrade, Delete

# Configure the sensor virtual application

## Procedure

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

The screenshot shows the Cisco IOx Local Manager interface. The top navigation bar includes 'Applications', 'App Groups', 'Remote Docker Workflow', 'Docker Layers', 'System Info', 'System Setting', and 'System Troubleshoot'. The main content area displays the 'CCVSensor' application, which is in a 'DEPLOYED' state. Below the application name, there is a table with columns for 'TYPE', 'VERSION', and 'PROFILE'. The 'TYPE' is 'docker', 'VERSION' is '4.3.0-202311031406', and 'PROFILE' is 'exclusive'. Below this table, there are two progress bars: 'Memory \*' at 100.0% and 'CPU \*' at 100.0%. At the bottom of the application card, there are three buttons: 'Activate' (with a checkmark), 'Upgrade', and 'Delete'. To the right of the application card, there is a dashed box containing 'Add New' and 'Refresh' buttons.

**Step 2** Access Applications > Resources.

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

The screenshot shows the Cisco IOx Local Manager interface for the 'CCVSensor' application. The top navigation bar includes 'System Setting', 'System Troubleshoot', 'IOx Tools', 'Device Config', 'User Config', and 'CCVSensor'. The main content area displays the 'Resources' configuration for the application. The 'Resource Profile' section is expanded, showing the following settings: Profile: 'exclusive', CPU: '10260' (with 'cpu-units' selected), Memory: '6400' MB, and Disk: '50000' MB. Below these settings, there is a summary table:

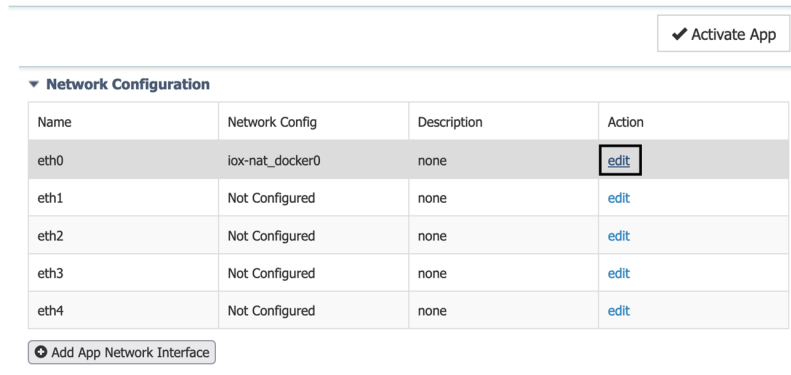
	Total CPU (cpu-units)	Avail. CPU (cpu-units)	Avail. Memory (MB)	Avail. Disk (MB)
	10260 (100%)	10260 (100%)	6400	80626

The 'Advanced Settings' section is also expanded, showing a text area for 'Docker Options' with the value '--rm' and a checked checkbox for 'Auto delete container instance'.

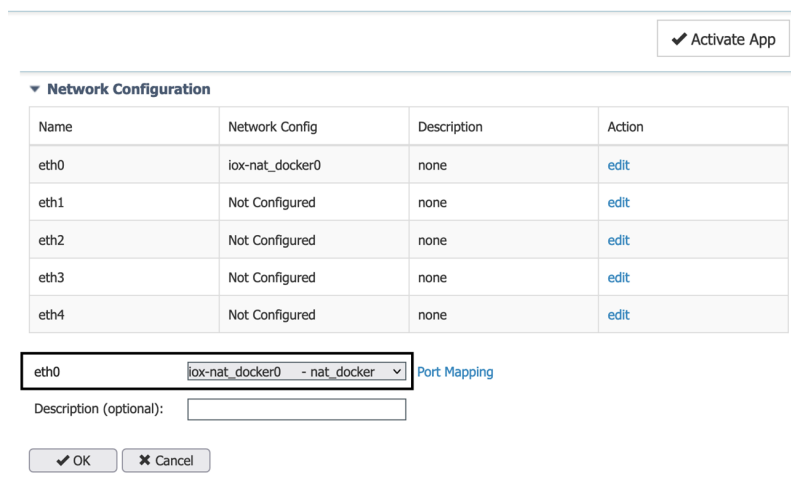
**Note** Disk size shouldn't be lower than 1,000 MB.

To map the Sensor network interfaces:

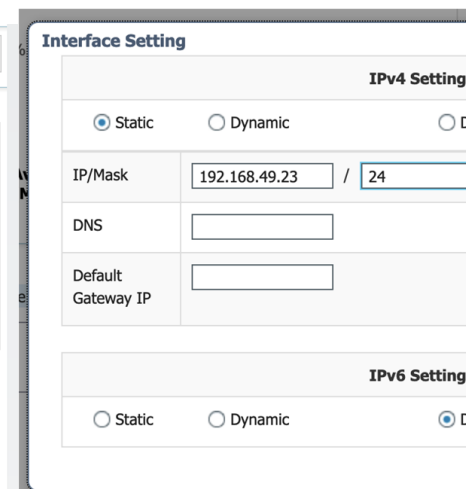
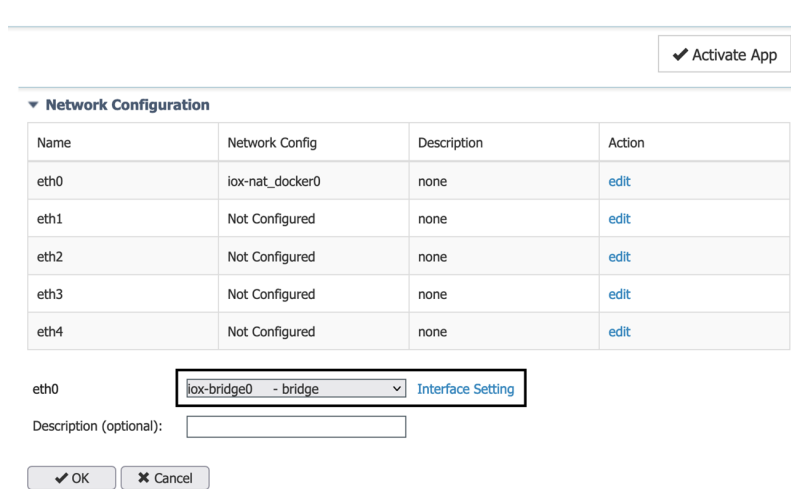
**Step 4** Under Network Configuration, click **edit** in the eth0 line.



**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

Name	Network Config	Description	Action
eth0	iox-bridge0	none	<a href="#">edit</a>
eth1	int1	none	<a href="#">edit</a>
eth2	int2	none	<a href="#">edit</a>
eth3	int3	none	<a href="#">edit</a>
eth4	int4	none	<a href="#">edit</a>

[Add App Network Interface](#)

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

**Step 11** Click **Edit** beside eth.

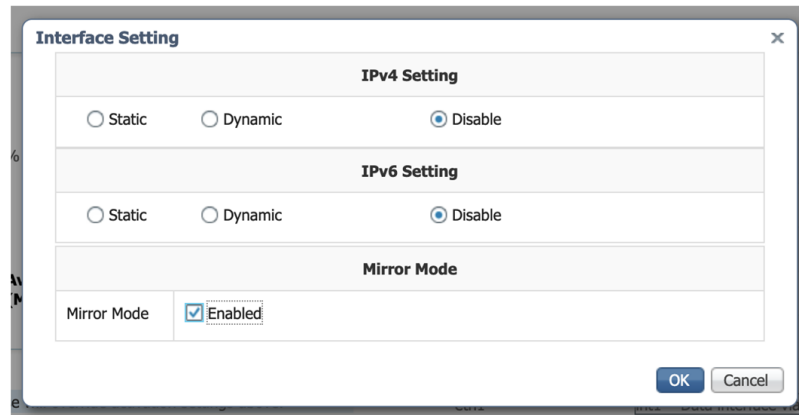
**Step 12** Click **Interface Setting**.

**Step 13** **Disable** IPv4 and IPv6.

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

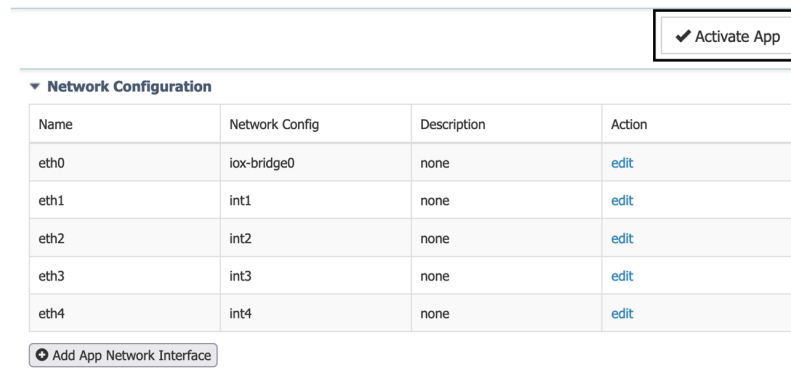
**Step 15** Click **OK**.



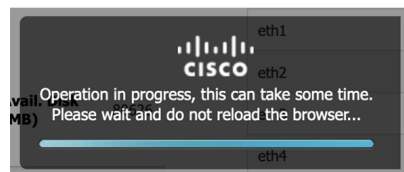


**Step 16** Repeat the above steps for eth2, eth3 and eth4.

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



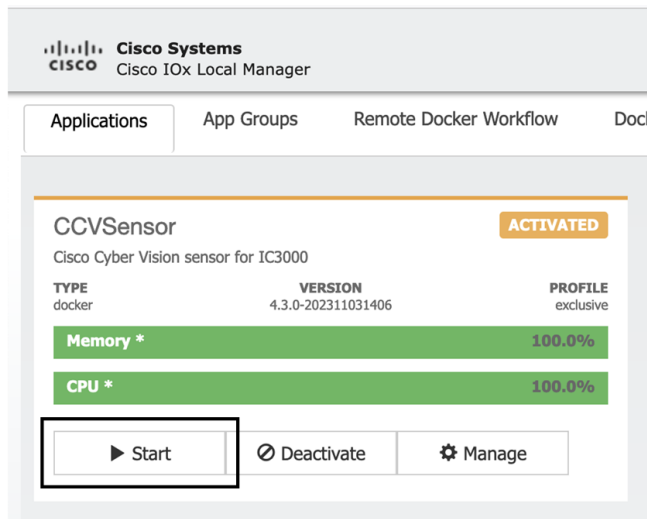
The following message appears:



To start the Sensor Application:

**Step 18** Access the Applications tab again.

**Step 19** Click **Start**.

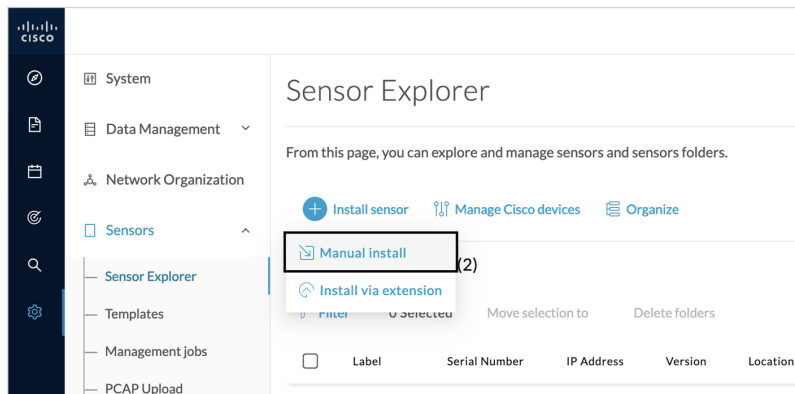


The application moves from Activated to Running state.

## 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.

---

Manual install

---

### Configure provisioning package

Please fill in the fields below to add configuration to the provisioning package to install.

Sensor Application

Serial number\*

Center collection IP

leave blank to use current collection IP

Gateway


Capture mode

Optimal (default): analyze the most relevant flows  
 All: analyze all the flows  
 Industrial only: analyze industrial flows  
 Custom: set your filter using a packet filter in tcpdump-compatible syntax



Monitor session type

ERSPAN: recommended choice for all devices  
 RSPAN: use it only with Catalyst 9X00 and when using ERSPAN is not possible

ⓘ This option has no effect on IC3000 as RSPAN is enforced

 Exit
Create sensor

**Step 3**Click **Create sensor**.**Step 4**Click **Download package**.

---


Manual install

---

### Download provisioning package

The provisioning package must be added in the right location of your IOx Application.

[↓ Download package](#)

 Exit
Finish

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.

## 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

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Location	Health status	Processing status	Activ
<input type="checkbox"/>	<a href="#">FCH2309Y01Z</a>				Line 2	Disconnected	Disconnected	
<input type="checkbox"/>	<a href="#">FCH2309Y01Z</a>			4.00	Line 1	Connected	Normally processing	
<input type="checkbox"/>	<a href="#">FCH2309Y01Z</a>	FCH2309Y01Z				Disconnected	Disconnected	

### What to do next

The provisioning package must be imported in the Local Manager.

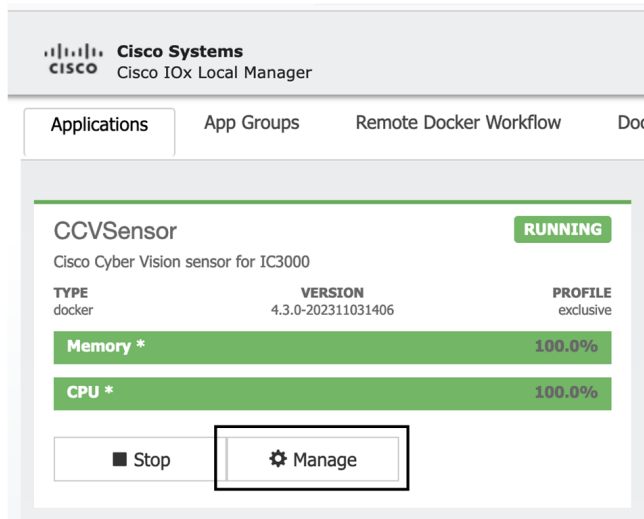
## Import the provisioning package

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.

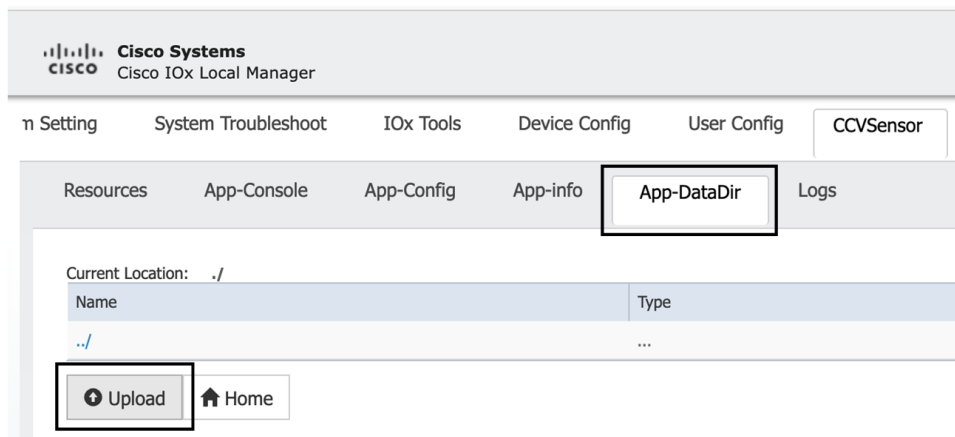
### Before you begin

### Procedure

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

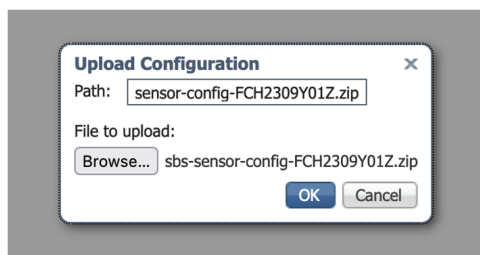


**Step 2** Navigate to **App-DataDir**.



**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,

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Location	Health status	Processing status	Acti
<input type="checkbox"/>						Connected	Normally processing	
<input type="checkbox"/>	FCH2309Y01Z	FCH2309Y01Z	192.168.49.23	4.3.0+202311031406		Connected	Normally processing	