



# Procedure with the Cisco Cyber Vision sensor management extension

After the [Initial configuration](#), proceed to the steps described in this section.

- [Install the sensor management extension, on page 1](#)
- [Create a sensor, on page 3](#)
- [Configure the sensor, on page 4](#)

## Install the sensor management extension

To install the Sensor Management extension, you must:

### Procedure

- Step 1** Retrieve the extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) from [cisco.com](#).
- Step 2** Access the Extensions administration page in Cisco Cyber Vision.
- Step 3** Import the extension file.

The screenshot shows the Cisco Cyber Vision interface. On the left is a dark sidebar with the Cisco logo and a list of navigation items: Events, API, License, External Authen..., Snort, Risk score, Integrations, and Extensions. The main content area is titled 'Extensions' and includes a brief description: '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.' Below this is a table titled 'Installed extensions' with columns for Name, Version, and Actions. The table contains one entry: 'Cyber Vision sensor management' with version '4.1.0' and actions 'Update' and 'Remove'. At the bottom, there is a section 'Install a new extension' with a button labeled 'Import extension file'.

Once the sensor management extension is installed, you will find a new management job under the sensor administration menu ([Management jobs](#)), and the Install via extension button will be enabled in the Sensor Explorer page.

## Management jobs

As some deployment tasks on sensors can take several minutes, this page shows the jobs execution status and advancement for each sensor deployed with the sensor management extension.

This page is only visible when the sensor management extension is installed in Cisco Cyber Vision.

Jobs	Steps	Duration
Single redeployment (FCW2435P3KW)	✓ — ✓ — ✓ — ✓	1m 11s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	41s
Single redeployment (FOC2337L0CW)	✓ — ✓ — ✓ — ✓	1m 33s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	35s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	39s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	43s
Single redeployment (FOC2334V045)	✓ — ✓ — ✓ — ✓	6m 52s

You will find the following jobs:

- Single deployment

This job is launched when clicking the Deploy Cisco device button in the sensor administration page, that is when a new IOx sensor is deployed.

- Single redeployment

This job is launched when clicking the Reconfigure Redeploy button in the sensor administration page, that is when deploying on a sensor that has already been deployed. This option is used for example to change the sensor's parameters like enabling active discovery.

- Single removal

This job is launched when clicking the Remove button from the sensor administration page.

- Update all devices

This job is launched when clicking the Update Cisco devices button from the sensor administration page. A unique job is created for all managed sensors that are being updated.

If a job fails, you can click on the error icon to view detailed logs.

Jobs	Steps
Single redeployment (FCW23500HDC)	<div style="position: absolute; top: -20px; left: 50%; transform: translate(-50%, -50%); background-color: black; color: white; padding: 2px;">Enroll - Error</div>
Single redeployment (FCW2435P3KW)	
Single redeployment (FCW23500HDC)	
Single redeployment (FOC2337L0CW)	
Single redeployment (FCW23500HDC)	

Enroll

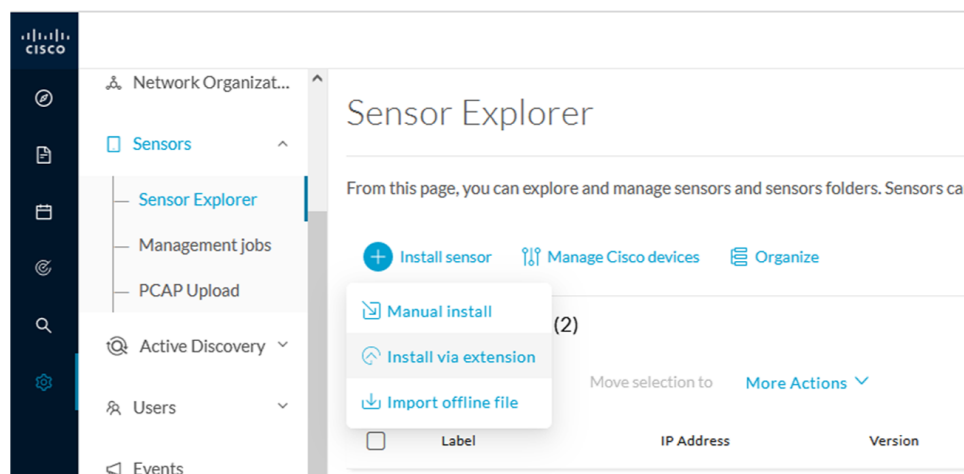
Error

```
Fatal error: cannot upload provisioning package: UploadAppData failed: Fog Director API Error Code 0: {"message": "File upload failed. App data upload is not allowed since this app was installed with --rm option and currently app container is cleaned after stopping the app. Consider starting the app and retry."}
```

## Create a sensor

### Procedure

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



**Step 2** Fill the requested fields so Cisco Cyber Vision can reach the device:

- IP address: admin address of the device.

- Port: management port (443).
- Login: user with the admin rights of the device.
- Password: password of the admin user.
- Capture Mode: Optionally, select a capture mode.

Install via extension

---

### 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\*

---

Capture mode

Optimal (default): analyze the most relevant flows

All: analyze all the flows

Industrial only: analyze industrial flows

Custom: you set your filter using a packet filter in tcpdump-compatible syntax

[Exit](#) [Connect](#)

### Step 3 Click **Connect**.

The Center will join the device and the second parameter list will be displayed. For this step to succeed, the device needs to be reachable by the Center on its eth1 connection.

## Configure the sensor

If the Center can join the device, the following form appears:

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: IR8340-K9

Capture IP address*	Capture prefix length*
169.254.1.2	30
	Like 24, 16 or 8
Extra capture IP address*	Extra capture prefix length*
169.254.2.2	30
	Like 24, 16 or 8
Extra capture VLAN number*	Collection IP address*
2340	169.254.0.2
Collection prefix length*	Collection gateway*
30	169.254.0.1
	Like 24, 16 or 8

Next

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

## Procedure

**Step 1** Fill the following parameters for the Collection interface:

- a. Capture interface: traffic capture from routed ports
  - Capture IP address: IP address destination of the monitor session in the sensor
  - Capture prefix length: mask of the capture IP address
- b. Extra capture interface: traffic capture from switched ports
  - Extra capture IP address
  - Extra capture prefix length
  - Extra capture VLAN number
- c. Collection interface: capture traffic to the Center
  - Collection IP address: IP address of the sensor in the device
  - Collection prefix length: mask of the Collection IP address
  - Collection gateway: IP address of the interface VirtualPortGroup 1

**Step 2** Click **Next**.

**Step 3** **Active Discovery:**

If you want to enable Active Discovery on the sensor, select **Passive and Active Discovery**.

You can:

- use the sensor Collection interface by selecting it:

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**

---

Add Active Discovery configuration	Network interfaces
<input checked="" type="checkbox"/> Use collection interface <a href="#">+ New network interface</a>	<ul style="list-style-type: none"> <li>• 192.168.49.21/24 VLAN#1 (collection interface)</li> </ul>

- add new network interfaces filling the following parameters to set dedicated network interfaces and clicking **Add**.
  - IP address
  - Prefix length
  - VLAN number

Add Active Discovery configuration

Use collection interface

+ New network interface

IP address\*  
192.168.51.22  
IP address interface used to do Active Discovery

Prefix length\*  
24  
Like 24, 16 or 8

VLAN number\*  
51  
Use 1 by default

Add
Cancel

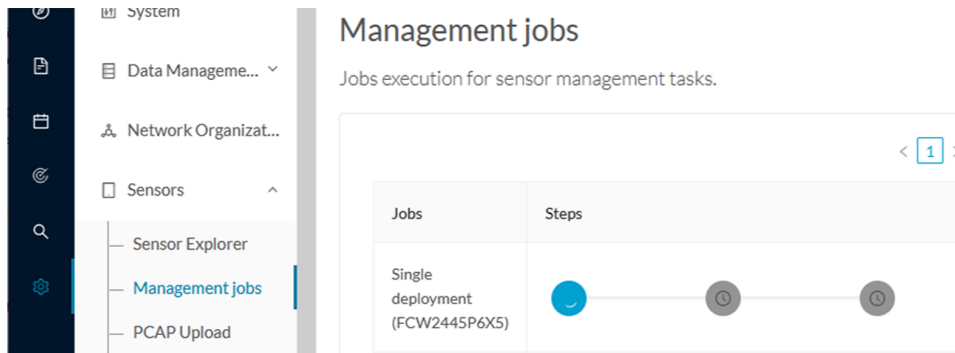
Network interfaces

- 192.168.50.21/24 VLAN#50  
[delete](#)

Back
Deploy

**Step 4** Click **Deploy**.

The Center starts deploying the sensor application on the target equipment. This can take a few minutes. You can go to the Management jobs page to check the deployment advancements.



Once the deployment is finished, a new sensor appears in the sensors list of the Sensor Explorer page. The sensor's status will eventually turn to Connected.

<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	4 days
--------------------------	-------------	---------------	--------------------	-----------	--------------	---------	--------

If the Active Discovery has been enabled and set -that is if the **Passive and Active Discovery** option was selected during the IOX App sensor configuration- the sensor is displayed as below with Active Discovery's status as Enabled.

Configure the sensor

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
<input type="checkbox"/>				FCW2445P6X5	Disconnected	Disconnected		Not
<input type="checkbox"/>				FCW2445P6X5				Not
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days