



Procedure with the Cisco Cyber Vision sensor management extension

After the [Initial configuration](#), proceed to the steps described in this section. This section also describes the steps to configure Active Discovery.



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.

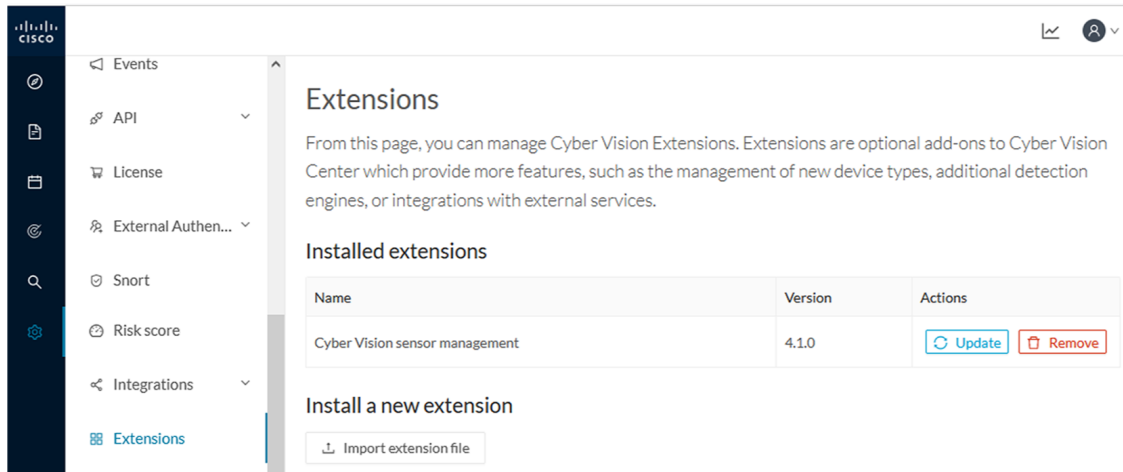
- [Install the sensor management extension, on page 1](#)
- [Create a sensor in the sensor management extension, on page 3](#)
- [Configure a sensor in the sensor management extension, on page 5](#)
- [Configure Active Discovery, on page 9](#)

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 Extension administration page in Cisco Cyber Vision.
- Step 3** Import the extension file.

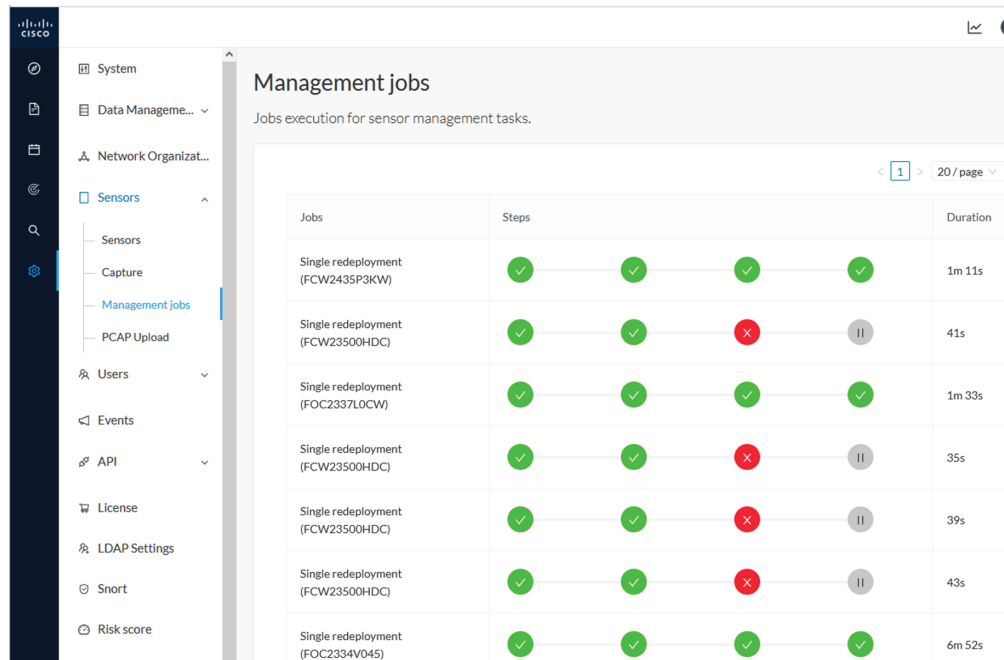


Once the sensor management extension is installed, you will find a new management job under the sensor administration menu ([Management jobs, on page 2](#)), and the **Install via extension** button will be enabled in the Sensor Explorer page.

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.



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.

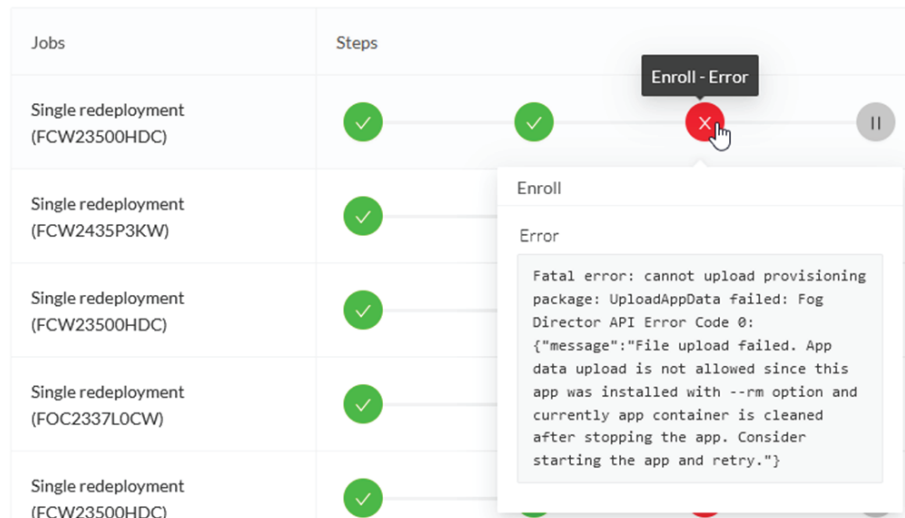
- Single removal

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.

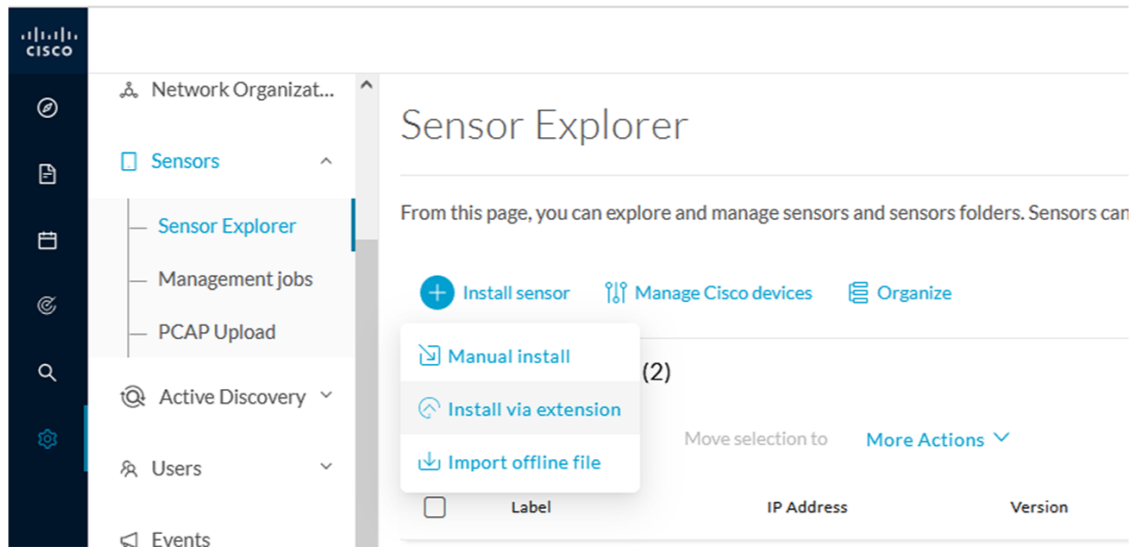
If a job fails, you can click on the error icon to view detailed logs.



Create a sensor in the sensor management extension

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*
<input type="text" value="192.168.49.20"/>	<input type="text" value="443"/>
	<small>For example 443 or 8443</small>

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 a sensor in the sensor management extension

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

Form for the Cisco IE3x00 and the Cisco IE9x00:

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: IE-3400-8T2S

Capture IP address*	Capture prefix length*
<input type="text" value="169.254.1.2"/>	<input type="text" value="30"/>
	<small>Like 24, 16 or 8</small>
Capture VLAN number*	Collection IP address*
<input type="text" value="2508"/>	<input type="text" value="192.168.49.21"/>
Collection prefix length*	Collection gateway
<input type="text" value="24"/>	<input type="text"/>
<small>Like 24, 16 or 8</small>	
Collection VLAN number*	
<input type="text" value="507"/>	

[Exit](#)

[Next](#)

Form for the Cisco Catalyst 9x00 with RSPAN configuration available:

Cisco device: C9300L-48T-4X

Monitor session type:

- ERSPAN: recommended choice
- RSPAN: use it only when using ERSPAN is not possible

Capture IP address*	Capture prefix length*
<input type="text" value="169.254.1.2"/>	<input type="text" value="30"/>
	<small>Like 24, 16 or 8</small>
Capture VLAN number*	Collection IP address*
<input type="text" value="2508"/>	<input type="text" value="192.168.0.248"/>
Collection prefix length*	Collection gateway
<input type="text" value="24"/>	<input type="text"/>
<small>Like 24, 16 or 8</small>	
Collection VLAN number*	
<input type="text" value="4"/>	

[Exit](#)

[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:

- Capture IP address: IP address destination of the monitor session in the sensor
- Capture prefix length: mask of the capture IP address
- Capture VLAN number: VLAN of the monitor session in the sensor
- Collection IP address: IP address of the sensor in the device
- Collection prefix length: mask of the Collection IP address
- Collection gateway: gateway of the Collection IP address
- Collection VLAN number: VLAN of the sensor

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 + New network interface	<ul style="list-style-type: none">• 192.168.49.21/24 VLAN#1 (collection interface)

- add new network interfaces filling the following parameters to set dedicated network interfaces and clicking Add:

- IP address
- Prefix length
- VLAN number

Configure a sensor in the sensor management extension

Add Active Discovery configuration

Use collection interface

+ New network interface

IP address*

IP address interface used to do Active Discovery

Prefix length*

Like 24, 16 or 8

VLAN number*

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.

The screenshot shows the 'Management jobs' page in the Cisco Cyber Vision interface. The left sidebar contains navigation options: System, Data Management, Network Organization, Sensors (expanded to show Sensor Explorer, Management jobs, and PCAP Upload), and a search icon. The main content area is titled 'Management jobs' and includes the subtitle 'Jobs execution for sensor management tasks.' Below this is a table with two columns: 'Jobs' and 'Steps'. The 'Jobs' column contains a single entry: 'Single deployment (FCW2445P6X5)'. The 'Steps' column shows a progress bar with three circular indicators: the first is blue with a white checkmark, and the other two are grey with a white power symbol. A page indicator '< 1 >' is visible in the top right corner of the table area.

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

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 option **Passive and Active Discovery** was selected when configuring the sensor in the sensor management extension- the sensor is displayed as below with Active Discovery's status as Enabled.

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

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 screenshot shows the 'Sensor Explorer' interface. On the left, there is a list of sensors under 'Folders and sensors (3)'. The sensor 'FCW2445P6X5' is selected. On the right, the configuration panel for this sensor is displayed. The 'Active Discovery' button is highlighted with a red box.

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.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

- Use collection interface
- [+ New network interface](#)

Network interfaces

- 192.168.49.21/24 VLAN#1 (collection interface)

Configure Cancel

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**.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

+ New network interface

IP address*
192.168.52.24

Prefix length*
24

VLAN number*
52

IP address interface used to do Active Discovery
Like 24, 16 or 8
Use 1 by default

Add Cancel

Configure Cancel

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.
