



Active Discovery sensor configuration

The Active Discovery configuration procedure will vary depending on the sensor model, whether it is a switch, a router or a Cisco IC3000.

To configure Active Discovery on a switch or a router, the sensors must have been previously deployed using the IOx sensor application file with Active Discovery. In this case, the Active Discovery button should appear in the sensor right side panel in Cisco Cyber Vision's Sensor Explorer page.

On a Cisco IC3000, you can configure Active Discovery performing a manual configuration or redeploying the sensor via the sensor extension.

- [Configure Active Discovery on a Cisco switch or router, on page 1](#)
- [Configure Active Discovery on a Cisco IC3000, on page 5](#)

Configure Active Discovery on a Cisco switch or router

Before you begin

This procedure is applicable to:

- Cisco IE3300 10G and Cisco IE3400.
- Cisco Catalyst 9300 and Cisco Catalyst 9400.
- Cisco IR8340 Integrated Services Router Rugged

The sensors must have been deployed using the IOx sensor application file with Active Discovery.

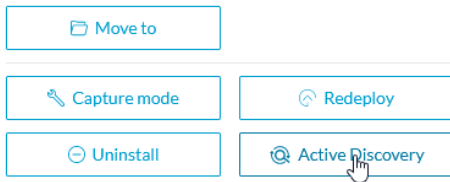
Step 1 Navigate to **Admin > Sensors > Sensor Explorer**.

Step 2 Select a sensor in the list.

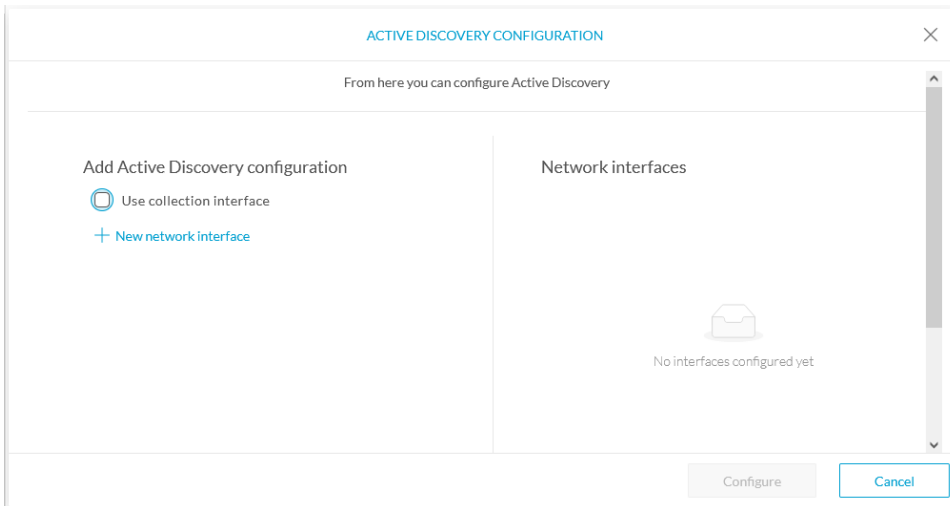
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

If there is no Active Discovery button in the panel, you must redeploy the sensor using the IOx application file with Active Discovery.

Step 3 Click the **Active Discovery** button.

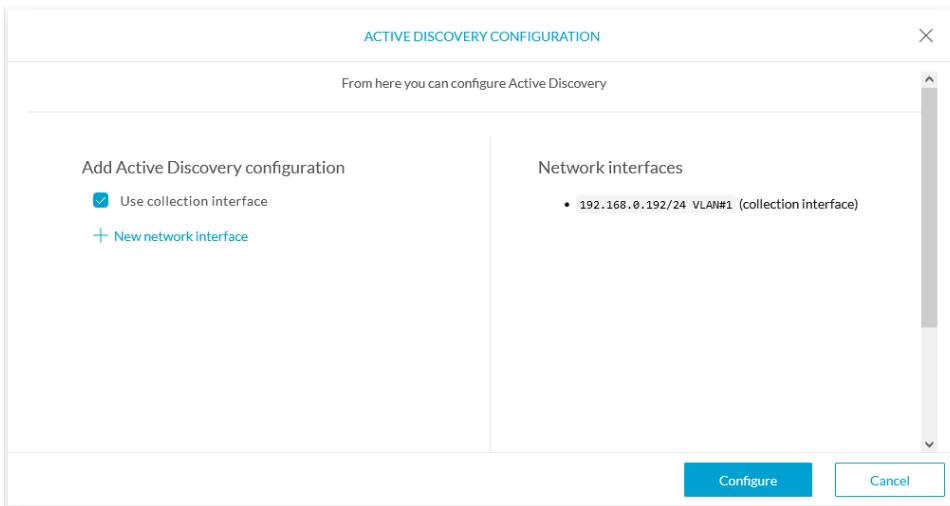


The Active Discovery Configuration window pops up:



Step 4 If necessary, tick the **Use collection interface** check box for Active Discovery to use the Collection network interface to do discovery on the same subnet as the sensor IP, or using the sensor Collection gateway.

The Collection network interface is added in the list on the right.



Step 5 Click + **New network interfaces** for the sensor to perform Active Discovery on additional subnetworks.

Step 6 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length

• VLAN number

+ New network interface

IP address*
192.168.20.145
IP address interface used to do Active Discovery

Prefix length*
24
Like 24, 16 or 8

VLAN number*
20
Use 1 by default

Add Cancel

Step 7 Click **Add**.

You can add as many network interfaces as needed, like below.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

Use collection interface

+ New network interface

Network interfaces

- 192.168.0.192/24 VLAN#1 (collection interface)
- 192.168.20.192/24 VLAN#20 delete
- 192.168.21.192/24 VLAN#21 delete
- 192.168.22.192/24 VLAN#22 delete
- 192.168.24.192/24 VLAN#24 delete

Step 8 Click **OK**.

The following schemas show how Active Discovery is created and how packets navigate inside the switch (in red).

Figure 1: IE3300 10G and IE3400:

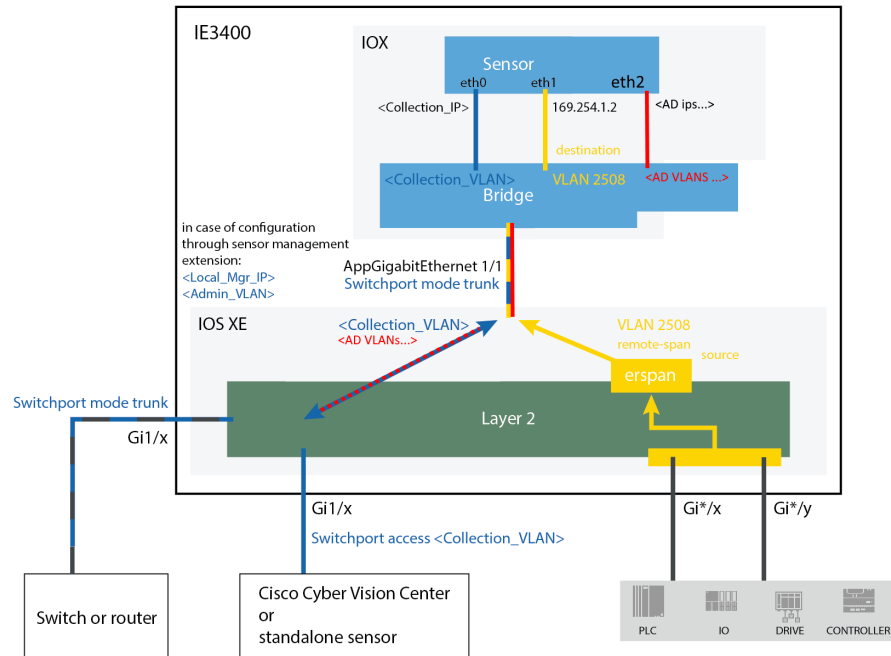


Figure 2: Catalyst 9300 and Catalyst 9400:

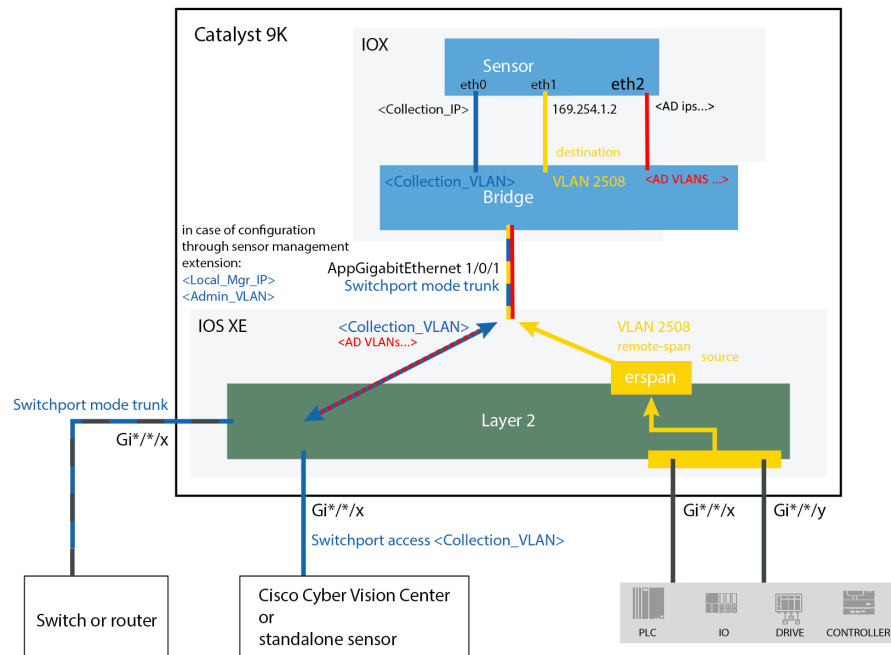
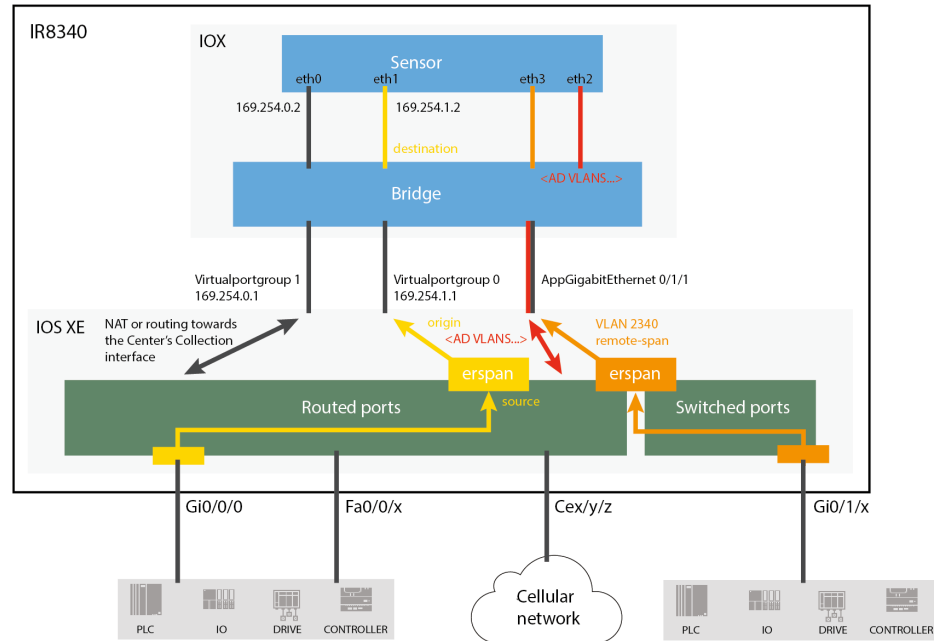


Figure 3: IR8340:

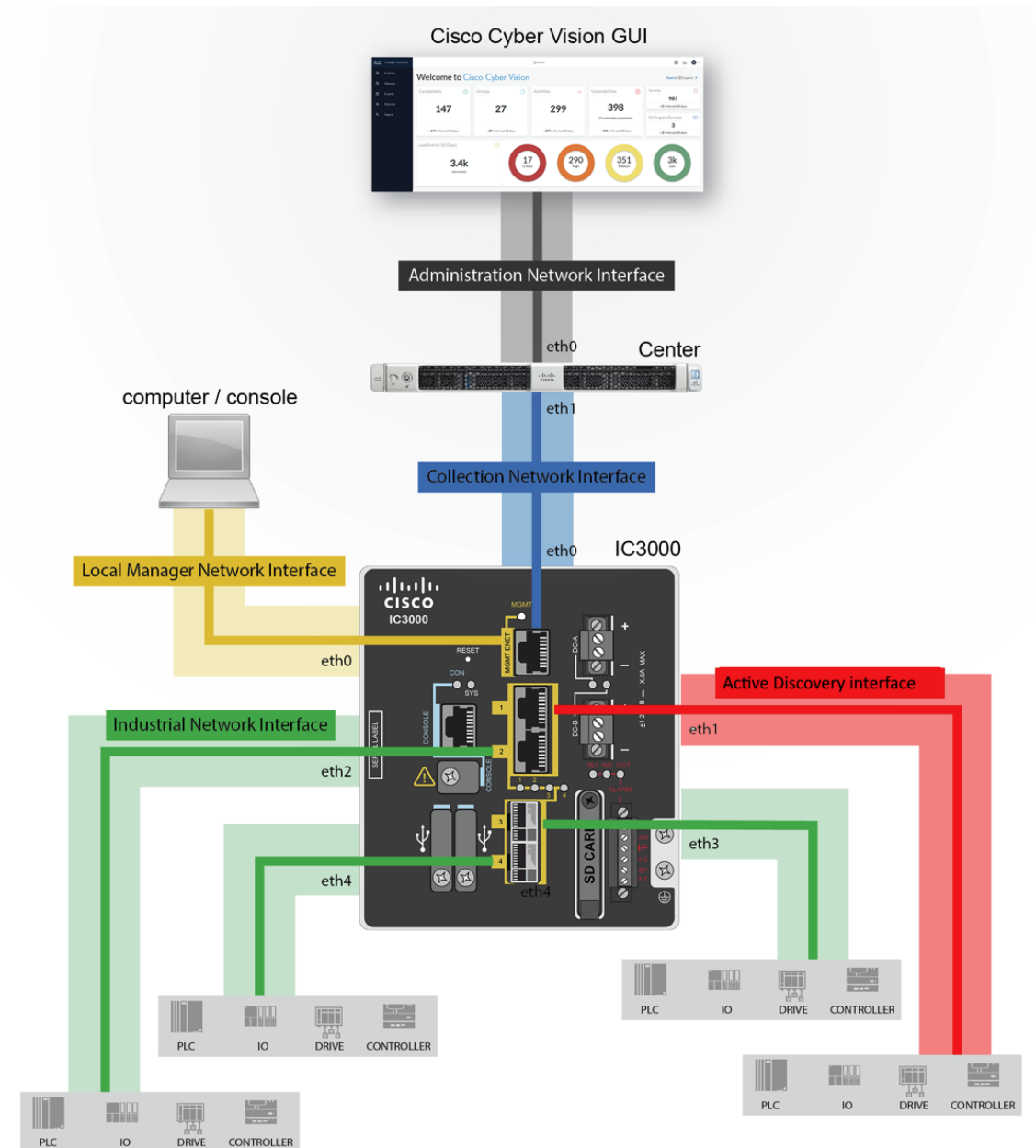
**What to do next**

Proceed to [Active Discovery policies configuration](#).

Configure Active Discovery on a Cisco IC3000

An interface must be defined on the Cisco IC3000 for Active Discovery to be enabled. Active Discovery can be set on the Collection network interface (i.e. the management port), or one of the four other interfaces of the Cisco IC3000 (i.e. int 1 to int 4).

Example: Active Discovery set on int1 (in red):



In any case, to configure Active Discovery on a Cisco IC3000, you have two options:

- To redeploy the Cisco IC3000 sensor with Active Discovery through the sensor management extension on Cisco Cyber Vision.
- To set up Active Discovery on the sensor, retrieve the provisioning package and deploy it on the device through the Local Manager.

Redeploy the Cisco IC3000 with Active Discovery

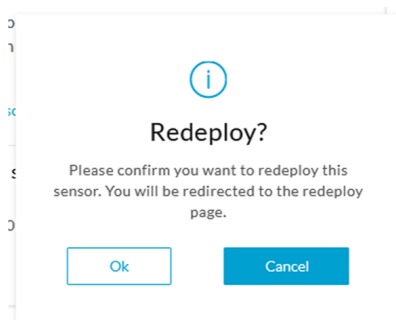
Redeploy the sensor to enable and configure Active Discovery on the Cisco IC3000.

- Step 1** On the Sensor Explorer page, click the sensor to reconfigure/redeploy. The sensor right side panel appears.
- Step 2** Click **Redeploy**.

The screenshot shows the Cisco Sensor Explorer interface. On the left is a navigation sidebar with categories like System, Data Management, Network Organization, Sensors, Management jobs, PCAP Upload, Active Discovery, Users, Events, API, License, External Authentication, and Snort. The 'Sensors' category is expanded, and 'Sensor Explorer' is selected. The main area displays 'Sensor Explorer' with a sub-header: 'From this page, you can explore and manage sensors and sensors folders, and erased. When a sensor connects for the first time, you must authorize...'. Below this are buttons for 'Install sensor', 'Manage Cisco devices', and 'Organize'. A table titled 'Folders and sensors (5)' lists sensors with columns for Label, IP Address, and Version. The sensor 'FCH2309Y01Z' is highlighted. To the right of the table is a detailed view for this sensor, including fields for Label, Serial Number, IP address, Version, System date, Deployment, Active Discovery, and Capture mode. Below these fields is a 'System Health' section with status 'Connected' and 'Uptime: 2 days'. At the bottom of the right panel, a 'Redeploy' button is highlighted with a red box.

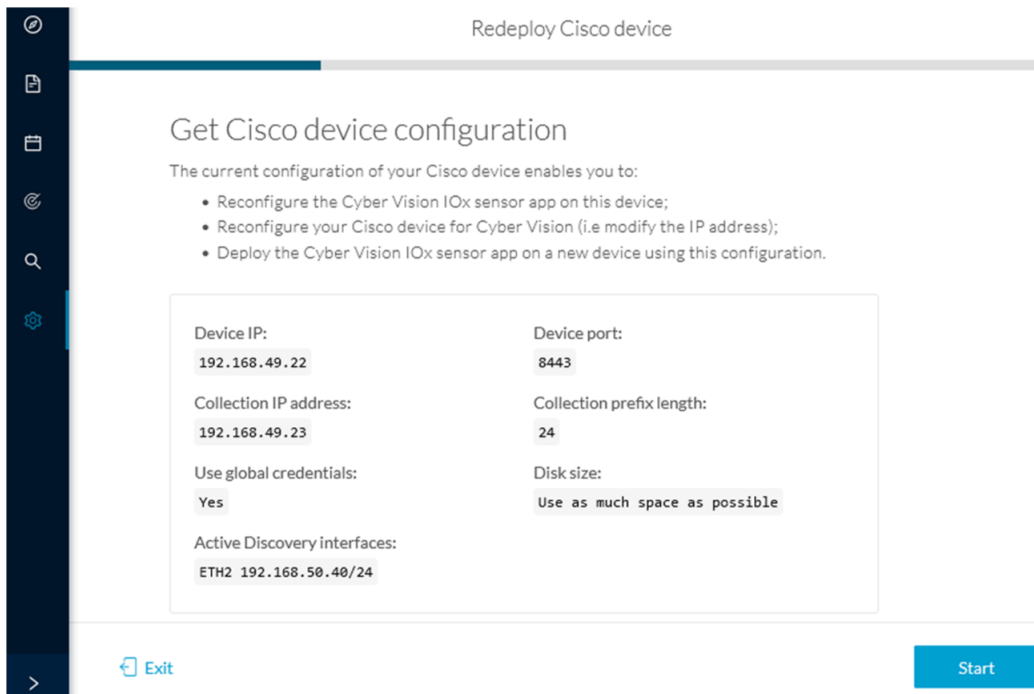
A pop up asking to confirm the redeployment of the sensor appears.

- Step 3** Click **OK** to proceed.

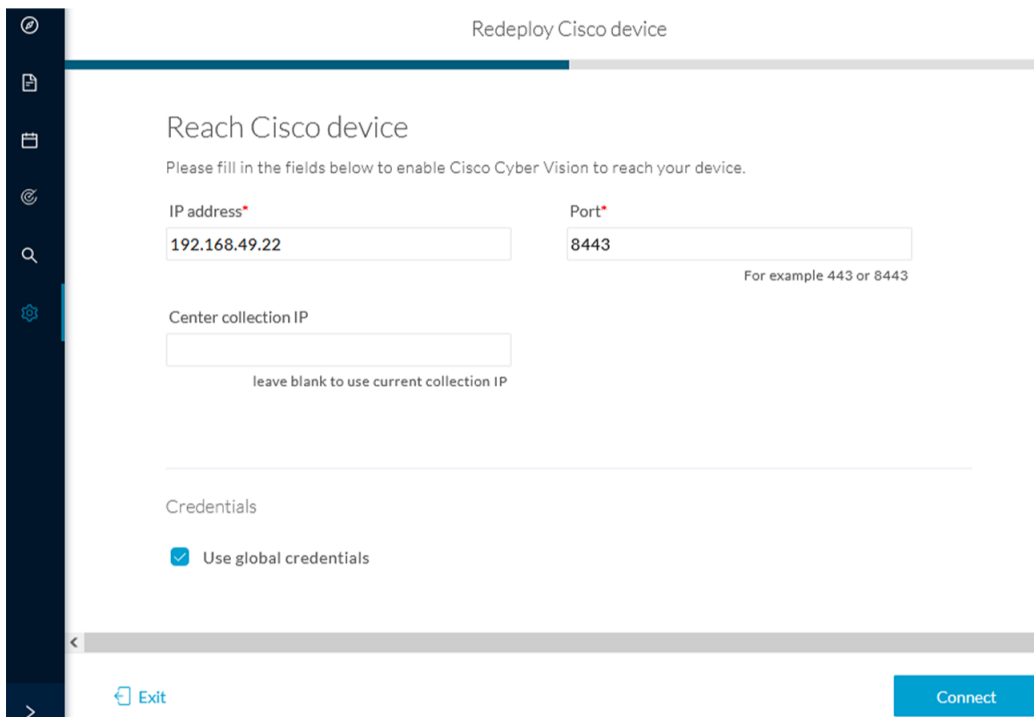


A summary of the sensor configuration is displayed.

- Step 4** Click **Start**.



The reach Cisco device window appears. The device's IP address and port are displayed.



Step 5 Enter the credentials to reach the device or tick **Use global credentials**.

Step 6 Click **Connect**.

The Configure Cyber Vision IOx sensor app window appears.

Redeploy Cisco device

Configure Cyber Vision IOx sensor app

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

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

Cisco device: IC3000-2C2F-K9

Collection IP address* ⚠

Collection prefix length* ⚠

Like 24, 16 or 8

Collection gateway

Step 7 Click the blue link to fill the warning fields with the current sensor configuration.

The Collection IP address and Collection prefix length are automatically filled.

Configure Cyber Vision IOx sensor app

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

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

Cisco device: IC3000-2C2F-K9

Collection IP address*

Collection prefix length*

Like 24, 16 or 8

Collection gateway

it

Next

Step 8 Click **Next**.

The Configure Active Discovery window appears.

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.

[Click here to add the current Active Discovery configuration on this sensor](#)

- Passive only
 Passive and Active Discovery

Select a physical interface

MGMT / Collection (enables DPI on collection inte... ▼

Select the port used to send packets

it

Back

Deploy

Step 9 Select **Passive and Active Discovery**.

Step 10 Select a physical interface.

Step 11 Click **Deploy**.

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

Redeploy Cisco device

Done!

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

What's next?

[Back to Sensor Explorer](#)

[Go to the jobs page](#)

If you click **Go to the jobs page** you are redirected to the Management jobs page.

Management jobs
Jobs execution for sensor management tasks.

Jobs	Steps	Duration
Single redeployment (FCH2309Y01Z)		In progress
Single redeployment (FCH2309Y01Z)		1m 10s

You can see the redeployment advancement. This can take several minutes.

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

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

Install sensor Manage Cisco devices Organize

Folders and sensors (5)

Filter 0 Selected Move selection to More Actions As of: Apr 8, 2022 7:04 PM

Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
				Disconnected	Disconnected	Disabled	0s
FCH2309Y01Z	192.168.49.23	4.1.0+202203111515		Redeploying	Not enrolled	Scanning	N/A
				Connected	Healthy	Enabled	0s

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

Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
				Disconnected	Disconnected	Disabled	0s
FCH2309Y01Z	192.168.49.23	4.1.0+202203111515		Connected	Pending data	Enabled	2 minutes
				Connected	Healthy	Enabled	0s

What to do next

Proceed to [Active Discovery policies configuration](#).

Manually configure Active Discovery on the Cisco IC3000

To do so, you will:

1. Set up the Cisco IC3000 sensor with Active Discovery on Cisco Cyber Vision and download the provisioning package.
2. Deploy the provisioning package on the Cisco IC3000 device through the Local Manager.

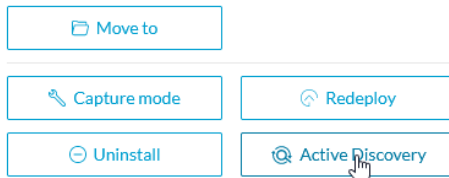
Set up Active Discovery on Cisco Cyber Vision

Step 1 Navigate to **Admin > Sensors > Sensor Explorer**.

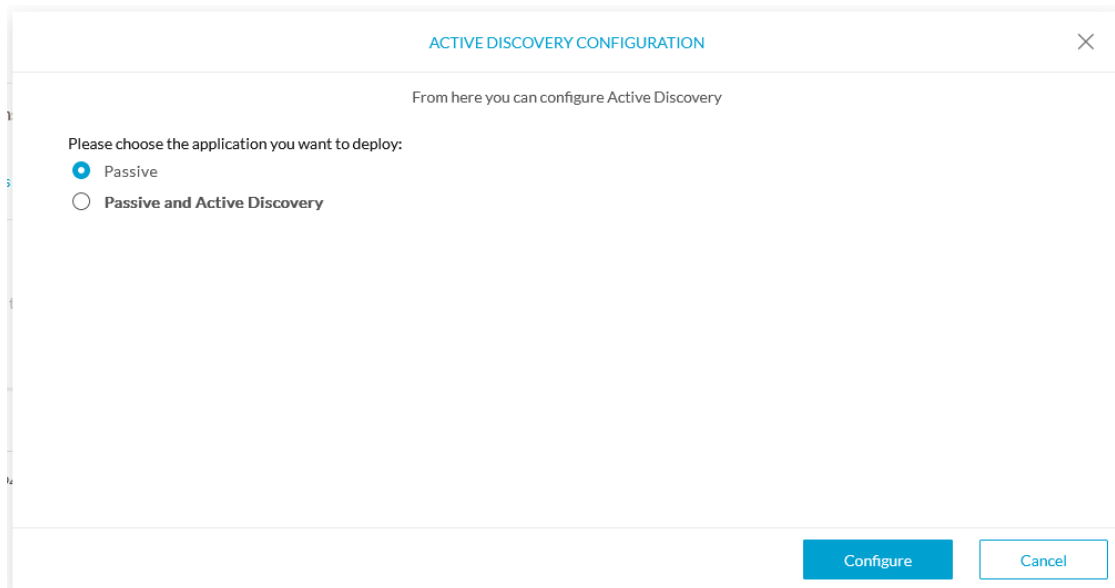
Step 2 Select a sensor in the list.

The sensor right side panel appears.

Step 3 Click the **Active Discovery** button.



The Active Discovery configuration window pops up.



Step 4 Select the **Passive and Active Discovery** option.

A list of network interfaces appears.

ACTIVE DISCOVERY CONFIGURATION ×

From here you can configure Active Discovery

Please choose the application you want to deploy:

Passive

Passive and Active Discovery

int1 ^

MGMT / Collection (enables DPI on collection interface)

int1

int2 ☞

int3

int4

Configure
Cancel

Step 5 Select the network interface dedicated to Active Discovery, i.e. the management port or one of the four interfaces.

The following fields appears:


- IP address
- Prefix length

Step 6 Fill them with the proper network information.

Step 7 Click **Configure**.

The following message appears:

ACTIVE DISCOVERY CONFIGURATION ×



The configuration has been saved successfully. Please download a new provisioning package to apply the configuration to your sensor.

OK

Step 8 Click **OK**.

Step 9 In the sensor list, click the Cisco IC3000 you just set with Active Discovery. Its right side panel appears.

Step 10 Click **Download package**.

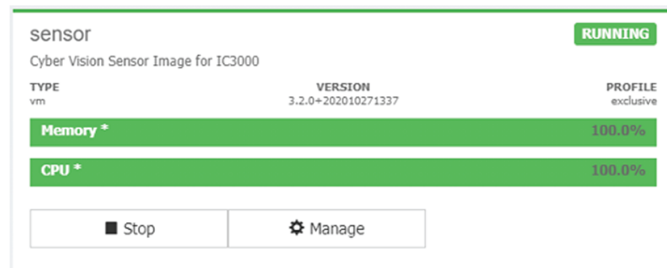
The provisioning package including the Active Discovery configuration is downloaded.

What to do next

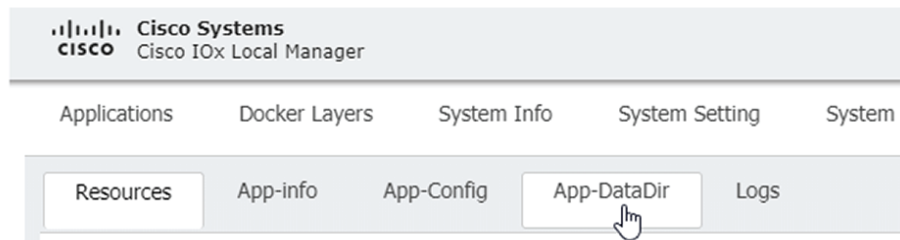
Import the provisioning package in the Cisco IC3000 device through the Local Manager.

Import the provisioning package

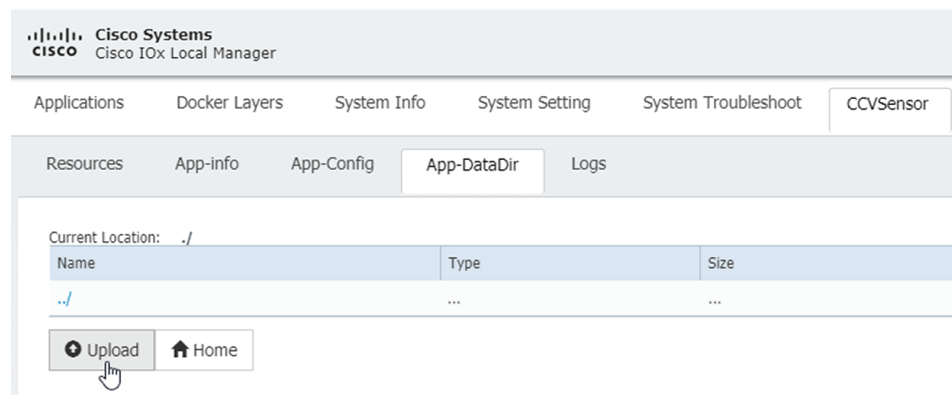
1. In the Local Manager, in the IOx configuration menu, click **Manage**.



2. Navigate to **App_DataDir**.



3. Before browsing the file, you must unzip the provisioning package.
4. Click **Upload**.



5. Navigate to the folder with the sensor serial name (i.e. FCH2312Y03F) > appconfigs, and select cybervision-sensor-config.zip.



6. Make sure the path contains the entire file name (with .zip).



7. Click **OK**.

