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 Docker Sensor, on page 9
- Configure Active Discovery on a Center Interface, on page 9

Configure Active Discovery on a Cisco switch or router

Before you begin

This procedure is applicable to:

- Cisco IE3300, Cisco IE3400, and Cisco IE9300.
- Cisco Catalyst 9300, Cisco Catalyst 9300X and Cisco Catalyst 9400.
- Cisco IR8340 Integrated Services Rugged Router.

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

Procedure

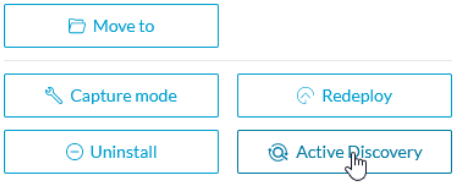
Step 1 Navigate to **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

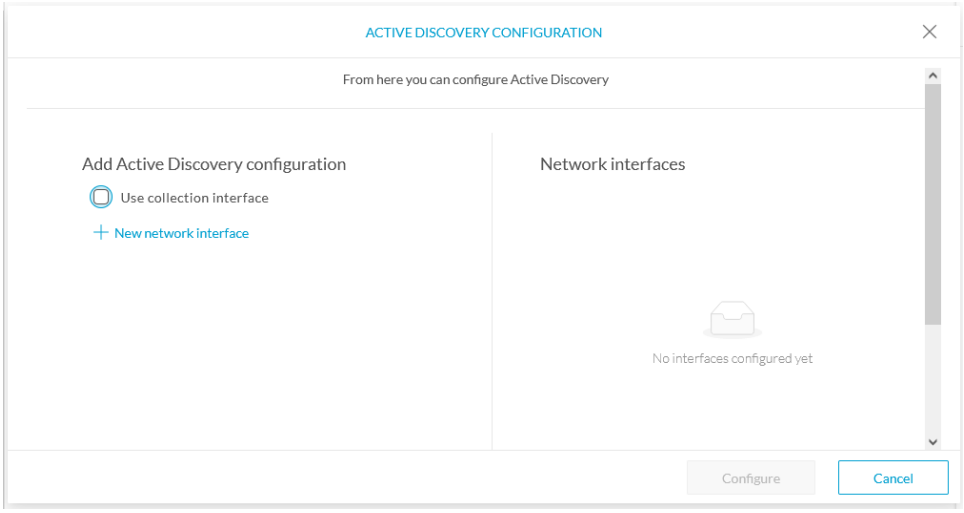
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

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.

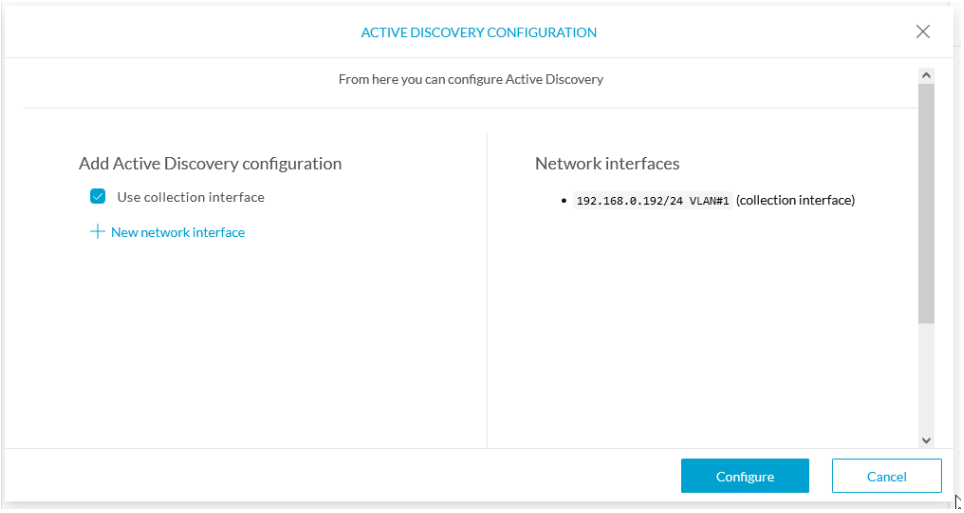


The Active Discovery Configuration window pops up:



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.

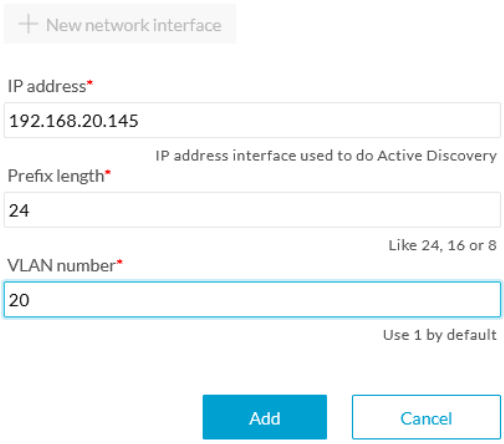
The Collection network interface is added in the list on the right.



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

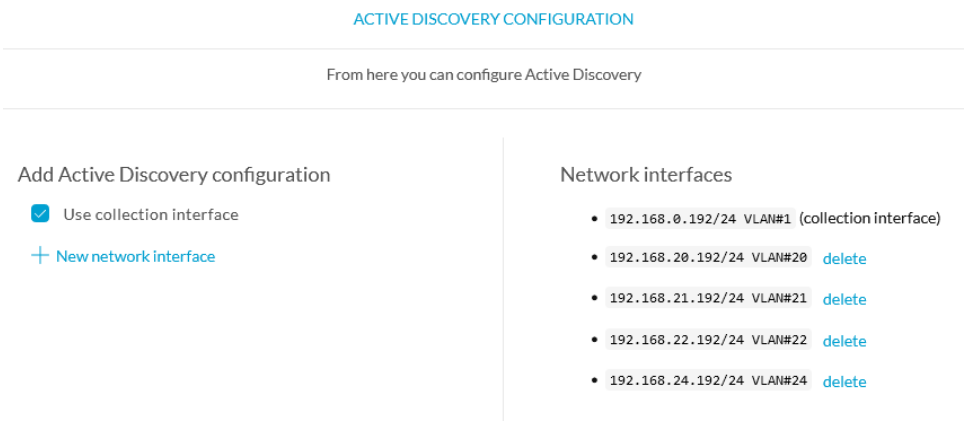
Step 6 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number



Step 7 Click **Add**.

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



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:

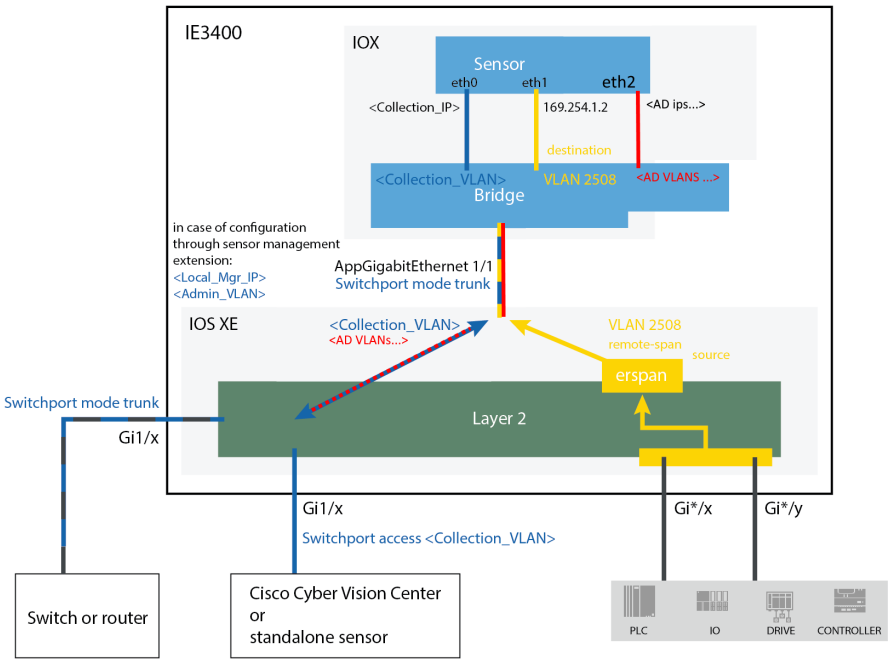


Figure 2: Catalyst 9300 and Catalyst 9400:

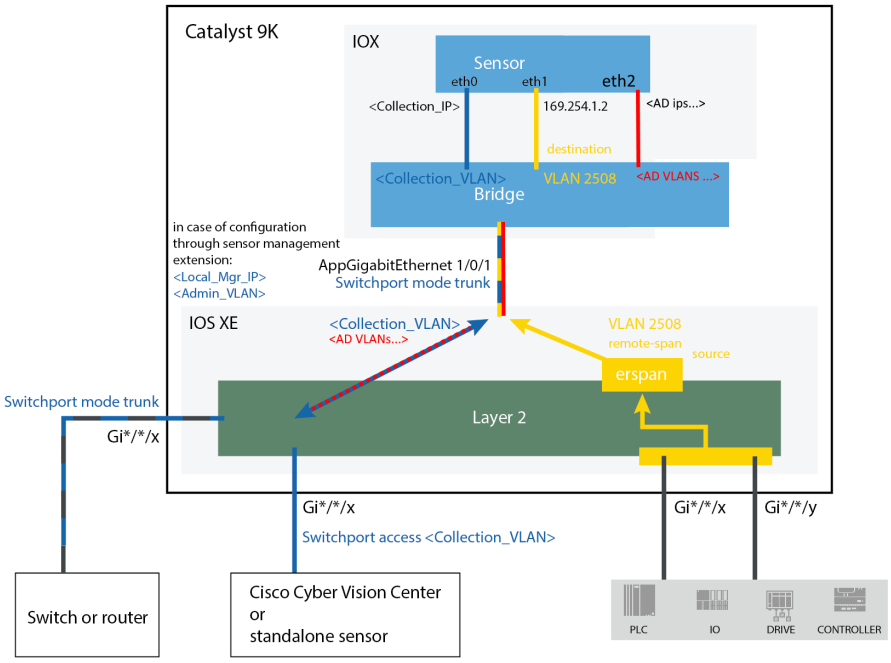
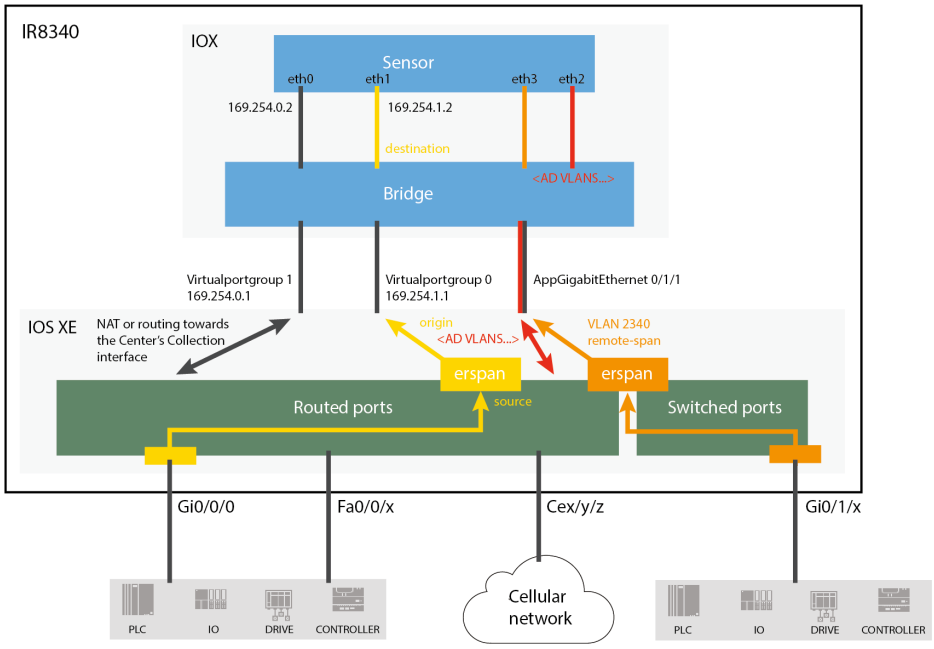


Figure 3: IR8340:



What to do next

Proceed to Policies configuration.

Configure Active Discovery on a Cisco IC3000

Before you begin

This procedure is applicable to the Cisco IC3000 Industrial Compute Gateway.

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

Procedure

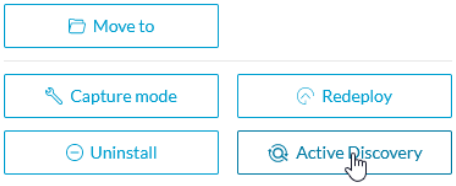
Step 1 Navigate to **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

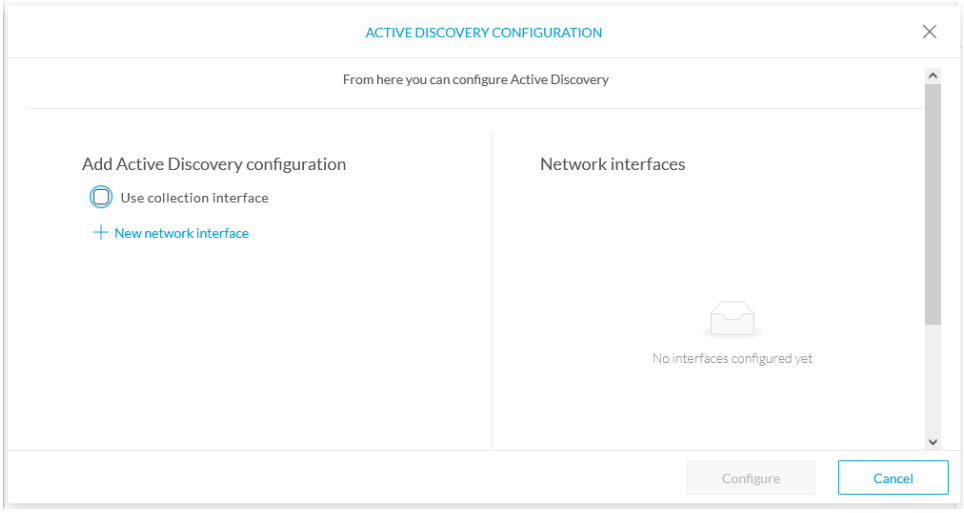
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

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.

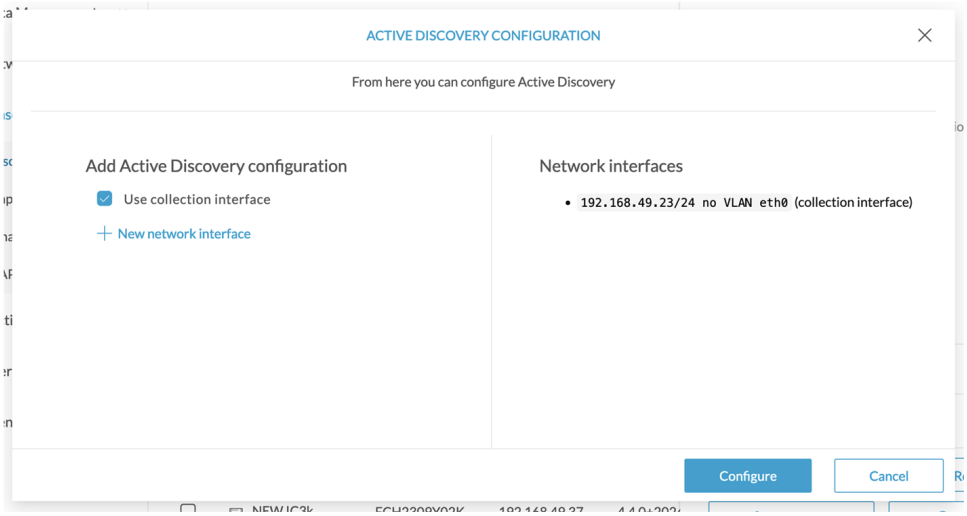


The Active Discovery Configuration window pops up:



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.

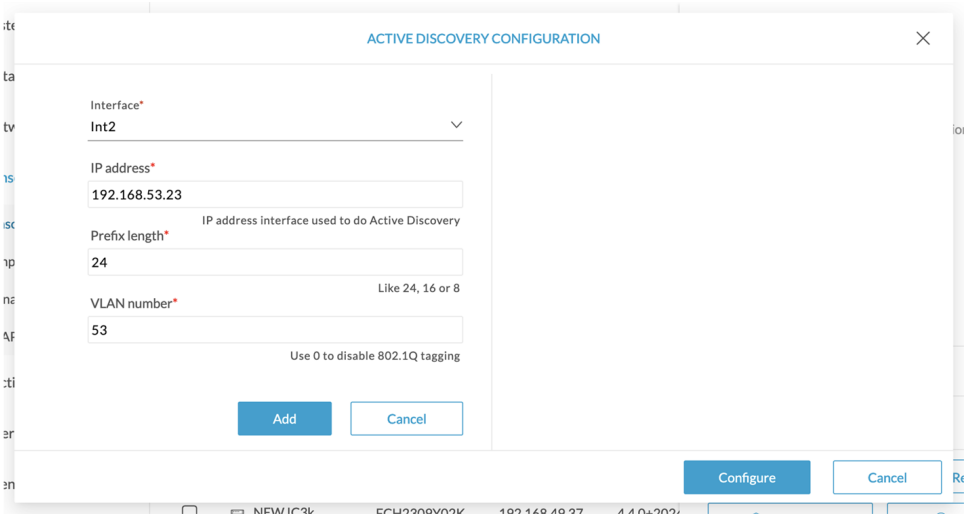


Step 5 Click **+ New network interface** for the sensor to perform Active Discovery on additional subnetworks.

Step 6 Select a physical interface and fill the following parameters to set a dedicated network interface:

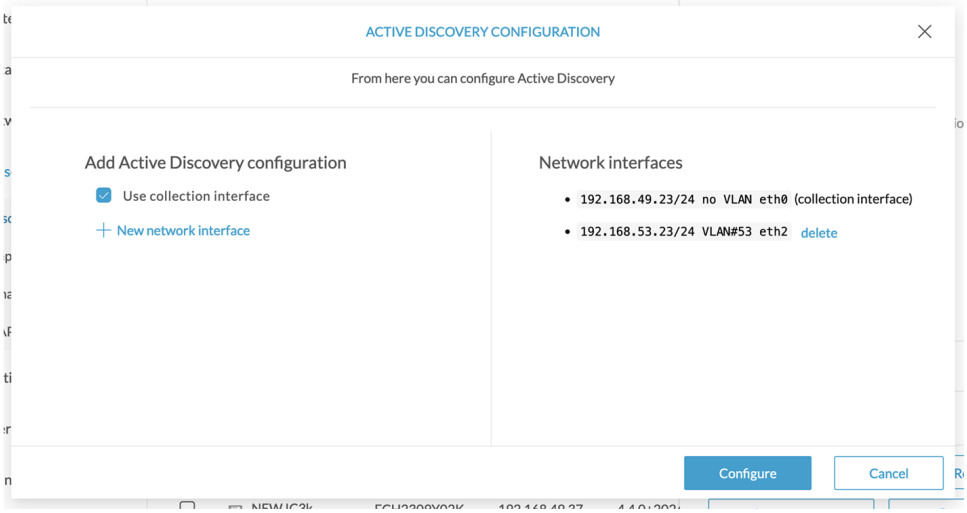
- IP address

- Prefix length
- VLAN number



Step 7 Click **Add**.

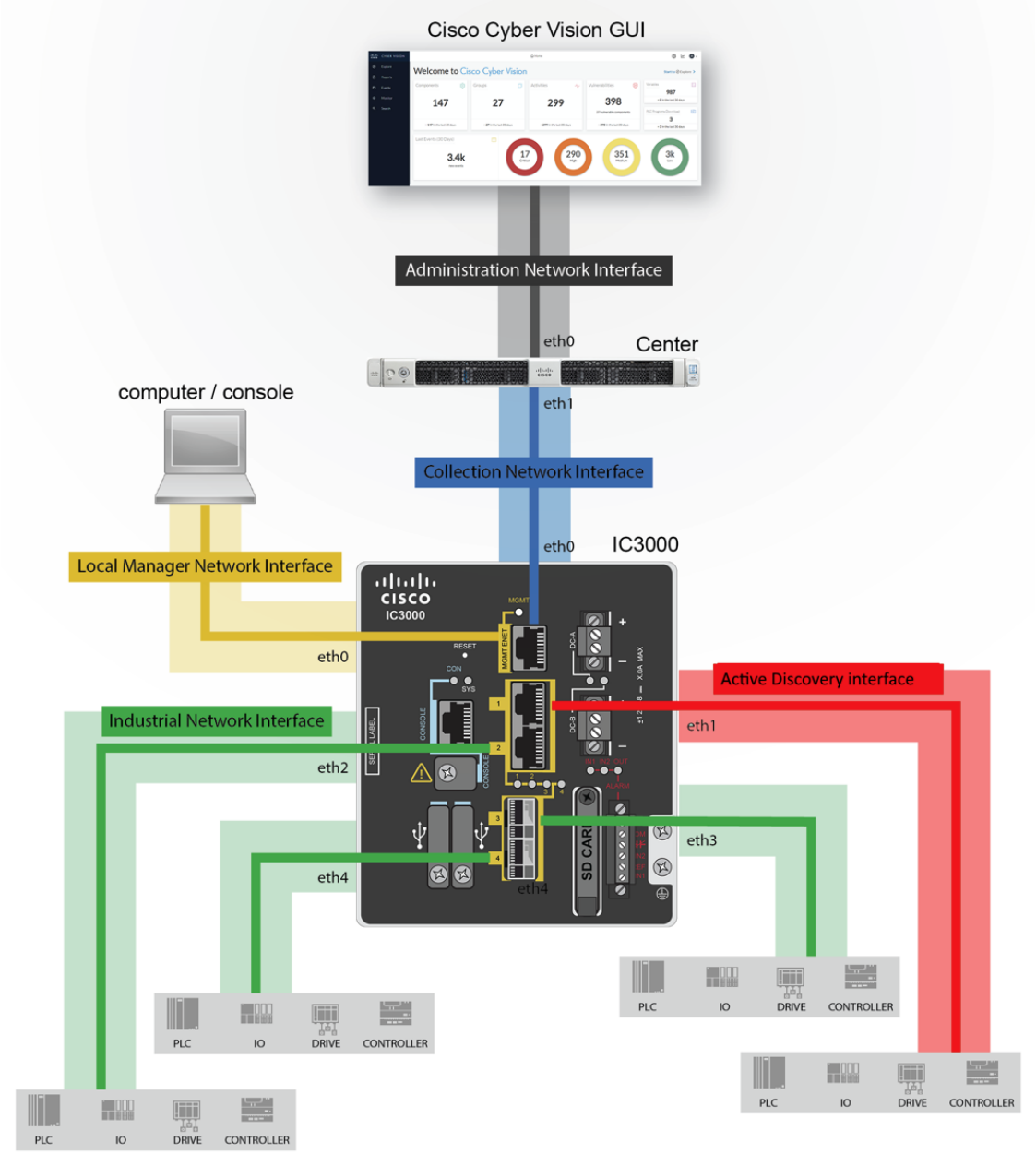
The network interfaces appears on the right.



You can add as many network interfaces as needed.

Step 8 Click **Configure**.

The following schema shows how Active Discovery is created and how packets navigate inside the Cisco IC3000 (in red).



What to do next

Proceed to Policies configuration.

Configure Active Discovery on a Docker Sensor

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

The sensor's right-side panel appears.

The **Active Discovery** button is displayed if the sensor is compatible.

Note
If there is no **Active Discovery** button in the panel, the selected Docker sensor is not an Active Discovery sensor. Select a sensor that supports Active Discovery.

Step 3 Click **Active Discovery**.

The **ACTIVE DISCOVERY CONFIGURATION** window appears.

Step 4 Click **+ New network interface** for the sensor to perform Active Discovery on additional subnetworks.

Step 5 Fill in the following parameters to set a dedicated network interface:

- IP address
- Prefix length
- VLAN number

Step 6 Click **Add**.

The network interfaces appears on the right under **Network interfaces**.

You can add as many network interfaces as needed.

Step 7 Click **Configure**.

Configure Active Discovery on a Center Interface

Configure Active Discovery on a center interface to transform it into an active probe. This setup allows the center to send packets based on user-configured protocols and frequencies and discovers network devices that sensors might not detect. It is especially useful for identifying silent devices, like certain PLCs, by prompting them to respond to the center. The responses provide detailed information about the devices, including model references and vendor details, helping you identify more vulnerabilities.

Note Active discovery exclusively uses the interface. If there is any IP address that attached to the interface, it creates a conflict.

Before you begin

- In the CLI, type the **sudo sbs-netconf** command.
- From the **Network configuration** window, select the new interface. Click **OK**.
- Choose the **Active Discovery** configuration type. Click **OK**.

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select the corresponding center interface from the sensor list.

The right-side panel appears and shows the Active Discovery status as **Enabled**.

Step 3 Click **Active Discovery**.

The **ACTIVE DISCOVERY CONFIGURATION** window pops up.

Step 4 Click **+ New network interfaces** for the center to perform Active Discovery on additional subnetworks.

Step 5 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number

Step 6 Click **Add**.

You can add as many network interfaces as needed.

Step 7 Click **OK**.