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

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.

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.

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

Procedure

Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Install via extension**.
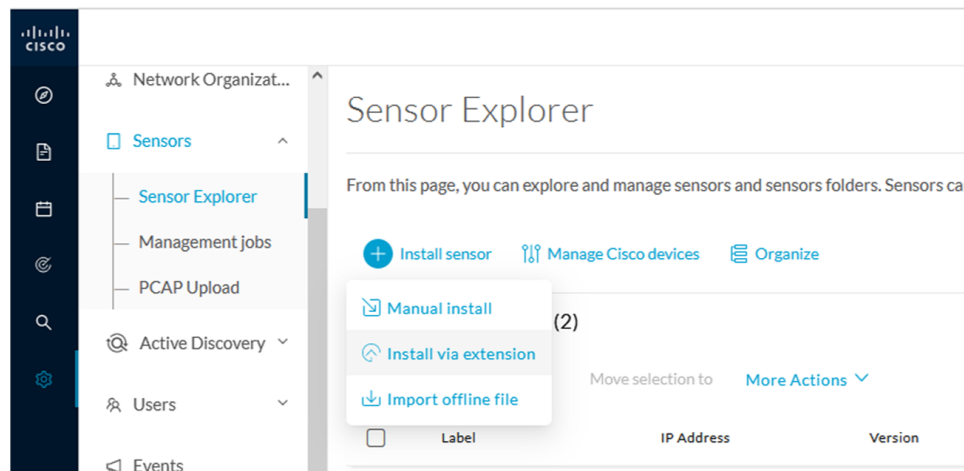
Step 2 Fill the requested fields so Cisco Cyber Vision can reach the device:

• 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*
192.168.49.20

Port*
443
For example 443 or 8443

Center collection IP

leave blank to use current collection IP

Credentials

Login*
admin

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: IR1101-K9

Capture IP address*

169.254.1.2

Capture prefix length*

30

Like 24, 16 or 8

Collection IP address*

169.254.0.2

Collection prefix length*

30

Like 24, 16 or 8

Collection gateway*

169.254.0.1

Exit

Deploy

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 Cisco IR1101

- Capture prefix length: mask of the capture IP address

- Collection IP address: IP address of the sensor in the Cisco IR1101

- Collection prefix length: mask of the Collection IP address

- Collection gateway: gateway of the Collection IP address

Step 2 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.
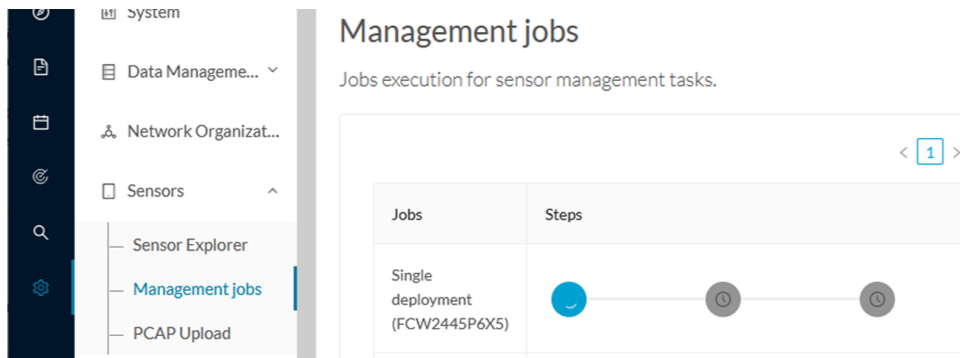
Once the deployment is finished, a new sensor appears in the sensors list of the Sensor Explorer page.

The sensor's status will eventually turn to Connected.