Sensors

Sensor Explorer

The Sensor Explorer page allows you to install, manage, and obtain information about the sensors monitoring your industrial network.

First, you need to know that sensors can be used in two modes, and for different purposes:

- Online mode: A sensor in online mode is placed at a particular and strategic point of the industrial network and will continually capture traffic.

  Applicable to: Cisco IE3400, IE3300 10G, Cisco IC3000, Catalyst 9300 and Cisco IR1101.

- Offline mode: A sensor in offline mode allows you to easily connect it at different points of the industrial network that may be isolated or difficult to access to occasionally make traffic captures. Traffic is captured on a USB drive. The file will then be imported in Cisco Cyber Vision.

  Only applicable to Cisco IC3000.

On the Sensor Explorer page, you will see a list of your folders and sensors (when installed) and buttons that will allow you to perform several actions.

Installation modes, features, and information will be available depending on the sensor model and the mode in which it's being used.

Additional information and actions are available as you click a sensor in the list. A right side panel will appear allowing you to see this information such as the serial number, and buttons to perform other actions.

Filter and sort the sensor list

Filtering

Clicking the Filter button allows you to filter the folders and sensors in the list by label, IP address, version, location, health and processing status.

The folders and sensors list without filtering:

Folders and sensors (5)

	Label ▲	IP Address	Version	Location	Health status ⓘ	Processing status ⓘ
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected

(Filter | 0 Selected | Move selection to | More Actions ⌄ | As o)

Type in the field or select from the drop down menu to reach the folder(s) or sensor(s) and click the Apply button:

The folders and sensors list after filtering by label:

Sorting

Sort icons allow you to sort sensors by label, IP address, version, location, health and processing status by alphabetical or by ascending/descending order. Sort icons appear when applied or as you hover over them.

Folders and sensors (5)

☐	Label ▾	IP Address ▲	Version	Location	Health status ⓘ	Processing status ⓘ
☐	📁 FOLDER2			Paris		
☐	📁 FOLDER1			Lyon		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

☐ Filter   0 Selected   Move selection to   More Actions ∨

Sensors status

There are two types of sensor status:

- The health status, which indicates at which step of the enrollment process the sensor is.

- The processing status, which indicates the network connection state between the sensor and the Center.

☐	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ	Active Discovery	Uptime
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected	Disabled	N/A
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data	Enabled	3 days
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	6 hours

Health status:

- **New**

This is the sensor's first status when it is detected by the Center. The sensor is asking the DHCP server for an IP address.

- **Request Pending**

The sensor has asked the Center for a certificate and is waiting for the authorization to be enrolled.

- **Authorized**

The sensor has just been authorized by the Admin or the Product user. The sensor remains as "Authorized" for only a few seconds before displaying as "Enrolled".

- **Enrolled**

The sensor has successfully connected with the Center. It has a certificate and a private key.

- **Disconnected**

The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

Processing status:

- **Disconnected**

  The sensor is enrolled but isn't connected to the Center. The sensor may be shut down, encountering a problem, or there is a problem on the network.

- **Not enrolled**

  The sensor is not enrolled. The health status is New or Request Pending. The user must enroll the sensor for it to operate.

- **Normally processing**

  The sensor is connected to the Center. Data are being sent and processed by the Center.

- **Waiting for data**

  The sensor is connected to the Center. The Center has treated all data sent by the sensor and is waiting for more data.

- **Pending data**

  The sensor is connected to the Center. The sensor is trying to send data to the Center but the Center is busy with other data treatment.

Sensors features

You will find in the Sensor Explorer page several features to manage and use your sensors. Some buttons are accessible from the Sensor Explorer page itself to manage one or more sensors. Other buttons are available when clicking a sensor in the list. A right side panel opens with additional sensor information and actions that are available or not depending on the sensor model, mode (online or offline) and the installation type performed.

- The **Start recording** button records a traffic capture on the sensor. Records can be used for traffic analysis and may be requested by Cisco support in case of malfunctions. You can download the recording clicking the link below.

  ✎

  Note This feature is targeted for short captures only. Performing long captures may cause the sensor overload and packets loss.

- The **Move to** button is to move the sensor through different folders. For more information, refer to Organize sensors, on page 9.

- The **Download package** button provides a configuration file to be deployed on the sensor when installing the sensor manually (online mode). Only applicable to the Cisco IC3000. Refer to its Installation Guide.

- The **Capture Mode** button can be used to set a filter on a sensor sending data to the Center. Refer to the procedure for Set a capture mode.

- The **Redeploy** button can be used to partly reconfigure the sensor, for example to change its parameters such as its IP address.

- The **Enable IDS** button can be used to enable the SNORT engine embedded in some sensors to analyze traffic by using SNORT rules. SNORT rules management is available on the SNORT administration page.

- The **Reboot** button can be used to reboot the sensor in case of a malfunction.

- The **Shutdown** button triggers a clean shutdown of the sensor from the GUI.

> **Note**   After performing a shutdown, you must switch the sensor ON directly and manually on the hardware.

- The **Uninstall** button can be used to remove an uninstalled sensor from the list or to fully uninstall a sensor. Diverse options are available according to the sensor model or deployment mode. In the case of a sensor deployed through the management extension, the IOx app can be removed from the device, whereas a reset to factory defaults can be performed in other cases. In any case, the sensor will be removed from the Center.

Install sensor

From the Sensor Explorer page, you can:

- Install a sensor manually.

- Install a sensor via the IOx extension. To use the Install via extension button you must first install the sensor management extension via the Extensions page.

- Capture traffic with an offline sensor (only applicable to Cisco IC3000).

For more information about how to install a sensor, refer to the corresponding Sensor Installation Guide.

Manage credentials

The Manage credentials button, which you can have access by clicking Manage Cisco devices in the Sensor Explorer page, is to register your global credentials if configured before in the Local Manager.
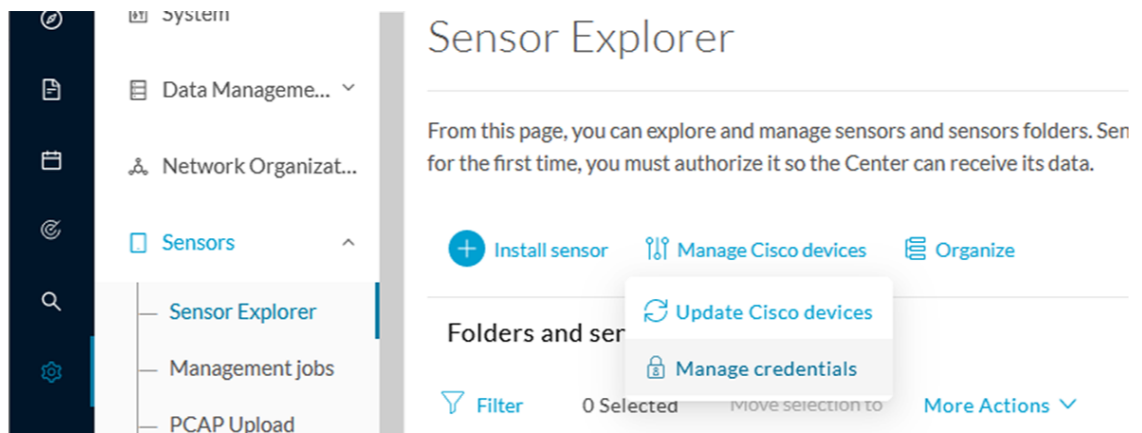
This feature can be used to register your global credentials in Cisco Cyber Vision. This will allow you to enter these credentials only once and they will be used when performing actions that require these credentials, that is installing and updating sensors via the IOx extension.

Only one set of global credentials can be used per Cisco Cyber Vision instance, which means that you cannot have several set of sensors accessible by different global credentials in a single instance. If there are several sensor administrators, they must use the same global credentials registered in Cisco Cyber Vision. However, you can have a set of sensors using a single global credentials and other sensors with their own single credentials.

Global credentials are stored in Cisco Cyber Vision but are set at the switch level in the Local Manager. Consequently, if you lose your global credentials, you must refer to the switch customer support and documentation.

The Manage credentials button can be used the first time you register your global credentials and each time global credentials are changed in the Local Manager. To do so, enter the login and password and click Save.

Once the global credentials are registered, the feature will be enabled in the Install via extension procedure. Select the Use global credentials option to use your global credentials.

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

☑ Use global credentials

Capture mode

◉ Optimal (default): analyze the most relevant flows

Organize sensors

You can create folders and move your sensors into the folders for more clarity. Folders can correspond to a location, a person in charge, a set of disconnected sensors, etc.

To create a folder and move a sensor in it:

1. Click the Organize button and click Create folder.

2. Write a folder name, and, if needed, a location and a description.

The new folder is displayed in the sensor list.

Folders and sensors (5)

	Label	IP Address	Version	Location	Health status	Processing status
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☐	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

Filter · 0 Selected · Move selection to · More Actions ⌄

3. Select a sensor in the list and click the button Move selection to.

Folders and sensors (5)

	Label	IP Address	Version	Location	Health status	Processing status
☐	📁 FOLDER1			Lyon		
☐	📁 FOLDER2			Paris		
☐	▭ FCY014567	192.168.49.41			Disconnected	Disconnected
☑	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
☐	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

Filter · 1 Selected · **Move selection to** · More Actions ⌄

4. Select the folder you want to place the sensor in or create a new folder. Root can be used to move sensors back into the primary list.
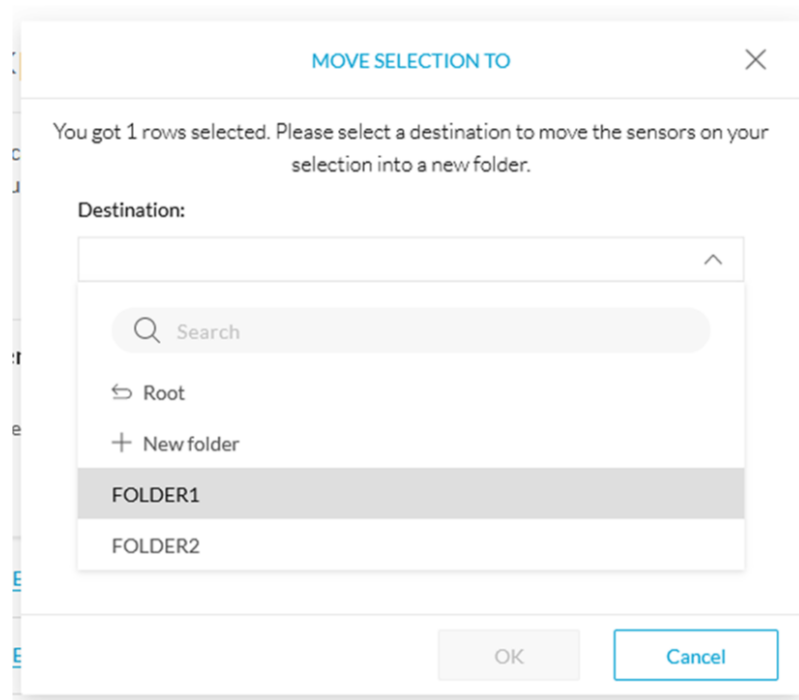
The sensor is moved into the folder. The sensor version, health status and processing status are displayed in the folder line.

If you move a sensor in a disconnected state inside this same folder, then its information will be displayed in the folder line rather than the sensor in connected state. Less secure sensor status are showcased in priority to drag your attention.

Folders and sensors (3)

	Label	IP Address	Version	Location	Health status	Processing status
	📁 FOLDER1		– 4.1.0	Lyon	Disconnected	Disconnected
	📁 FOLDER2			Paris		
	▭ FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data

The sensors inside a folder:

FOLDER1

📍 Lyon

✏️ Edit   🗑 Delete

Folders and sensors (2)

	Label	IP Address	Version	Health status	Processing status
	▭ FCY014567	192.168.49.41		Disconnected	Disconnected
	▭ FCH2309Y01Z	192.168.49.23	4.1.0+202202151504	Connected	Pending data

Set a capture mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. You can set it by clicking an online sensor in the sensors list of the Sensor Explorer page or during a sensor installation.

Setting the capture mode on a sensor from the right side panel:

Capture modes:

The aim is mainly to focus the monitoring on relevant traffic but also to reduce the load on the Center.

For example, a common filter in a firewall can consist of removing the network management flows (SNMP). This can be done by setting a filter like "not (port 161 and host 10.10.10.10)" where "10.10.10.10" is the network management platform.

Using Capture mode Cisco Cyber Vision performance can be improved on large networks.

Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

You can set the capture mode in the installation wizard when enrolling the sensors during the Center installation. This option is recommended if you already know which filter to set. Otherwise, you can change it at any time through the Sensor Explorer page in the GUI (provided that the SSH connection is allowed from the Center to the sensors).

Note You can set a capture mode to offline sensors from a file containing the filter and registered on the USB drive. This will be then plugged on the Offline USB port of the device. For more information about setting a capture mode on an offline sensor contact the support.

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.

- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.

- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.

- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.

Templates

This page allows you to create and set templates with protocol configurations and assign them to specific sensors.

Sensor templates contain protocol configurations which allow you:

- To enable or disable protocol DPI (Deep Packet Inspection) engines.

- To map UDP and TCP ports for each protocol's packet received by the sensor.

By enabling/disabling a protocol DPI engine you can decide which protocols will be analyzed.

Disabling a protocol DPI engine avoid false positives in Cisco Cyber Vision, that is when a protocol appears on the user interface when it's actually not the case because same UDP/TCP ports can be used by other non-standardized protocols.

Some protocols are disabled in the Default template because they are not commonly used or used in specific fields such as transportation. The Default template is applied on all compatible sensors.

As previously mentioned, UDP/TCP ports default configurations are mostly standardized, but conflicts still exist among field-specific protocols or with limited usage. Mapping UDP/TCP port numbers will allow packets to be sent to the correct DPI engine so they can be accurately analyzed and correctly represented in the user interface.

If the protocol's packet is sent to the wrong port, related information will end up in Security Insights/Flows with no tag.
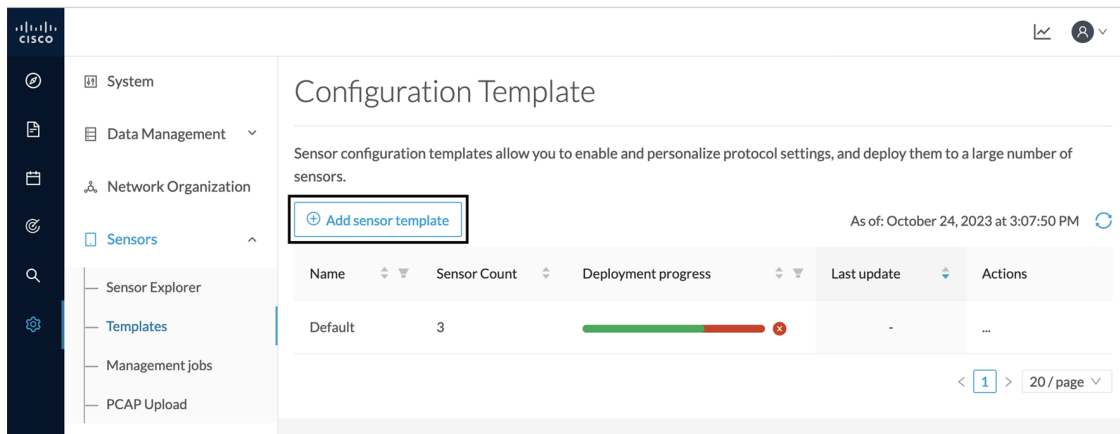
A sensor can be associated with a single template only. Deployment of the template can fail:

• if the sensor is disconnected,

• if there is connection issues,

• if the sensor version is too old.

Create templates

Step 1   In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.

Step 2   Click **Add sensor template**.

The Create sensor template window pops up.

Step 3   Add a name to the template. You can also add a description.

Step 4   Click **Next**.

The list of protocol DPI engines with their basic configurations appears.
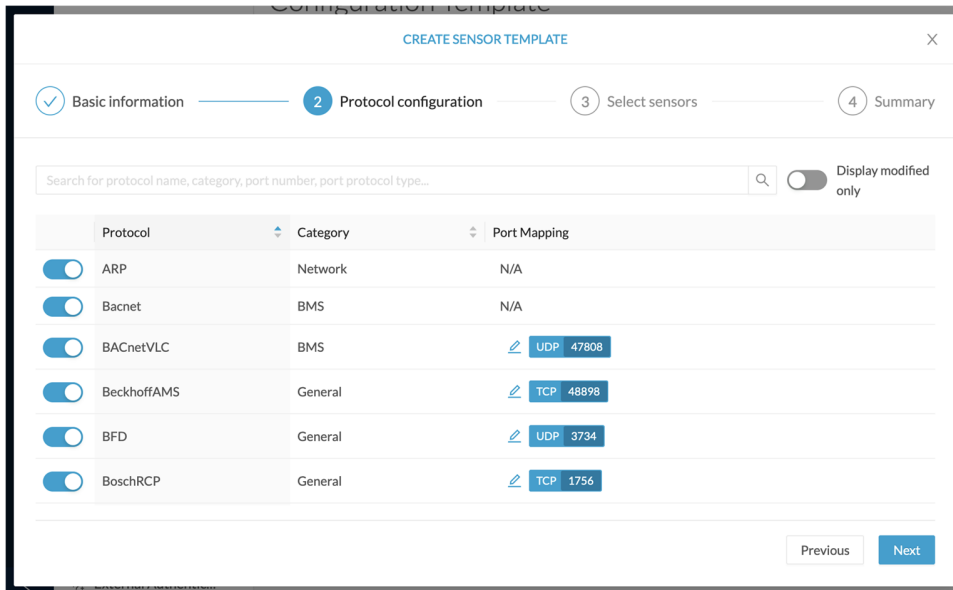
Step 5 In the search bar, type the protocol you want to configure.

In our example, we will add a port to the OPCUA default settings.
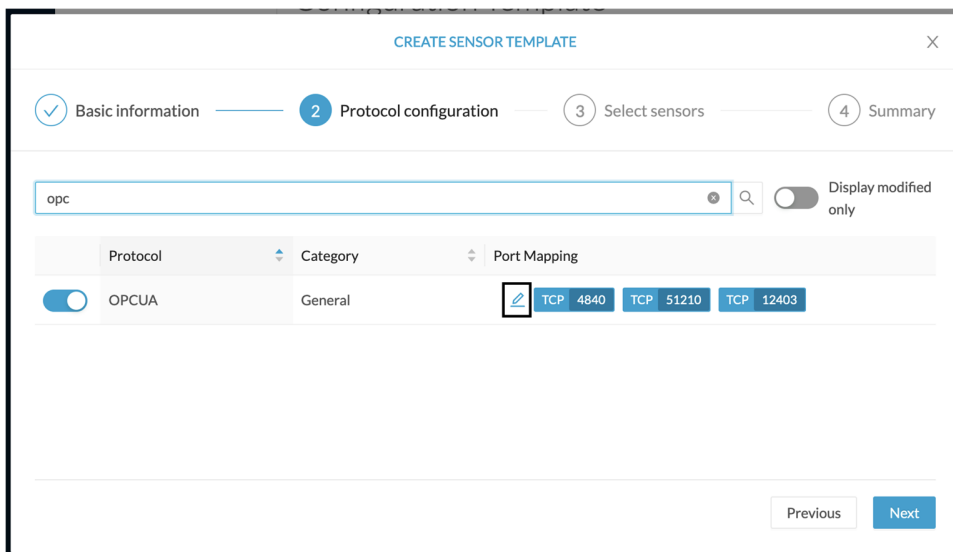
Step 6 Under the Port Mapping column, click the **pen** button to edit its settings.

The protocol's port mapping window pops up.

Step 7 Write down the port number you want to add and hit enter.

Step 8   Click **OK**.

The port number is added to the protocol's default settings.

Toggling ON the **Displayed modified only** button allows you to quickly find this protocol.
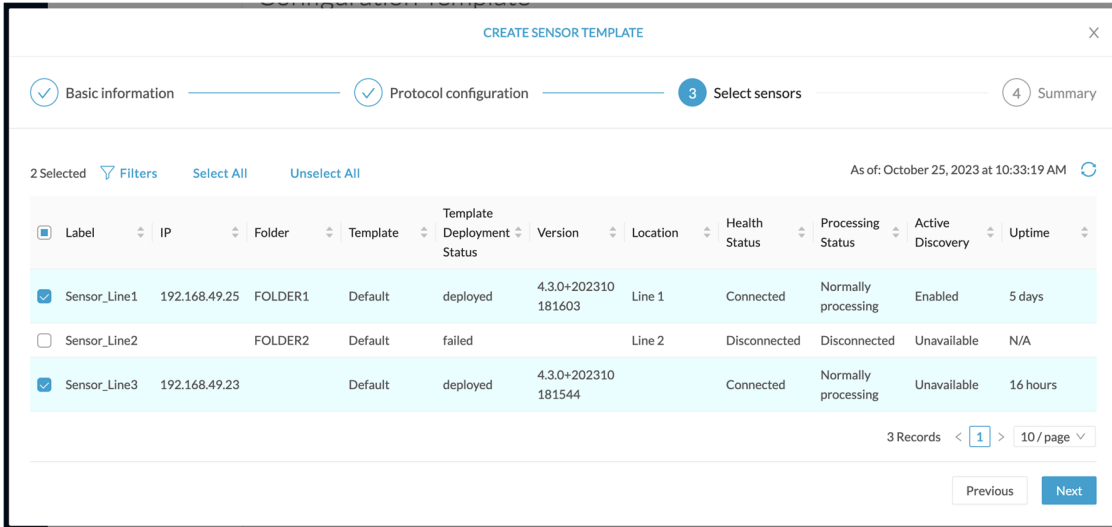
Step 9   Click **Next**.

Step 10   Select the sensor(s) you want to apply the template to.

Step 11   Click **Next**.

Step 12   Check the template configurations and **Confirm** its creation.

The configuration is sent to the sensors. Configuration deployment will take a few moments.

The OPCUA template appears in the template list with its two assigned sensors.

Configuration Template

Sensor configuration templates allow you to enable and personalize protocol settings, and deploy them to a large number of sensors.

⊕ Add sensor template   As of: October 24, 2023 at 3:06:55 PM ⟳

Name	Sensor Count	Deployment progress	Last update	Actions
Default	1	⬤	-	...
OPCUA	2	✓	Today	...

‹ 1 ›   20 / 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.

PCAP Upload

This page allows you to upload pcaps to view their data in Cisco Cyber Vision.

When selecting a pcap, two options are available:

- You can choose to use the timestamp of the pcap or the current timestamp instead. Choosing the current timestamp can be useful if the pcap timestamp is old and searching for its data in Cisco Cyber Vision is thus easier.

- You can define a preset from the pcap. Once the pcap is uploaded you'll just have to click the pcap link to be redirected to its preset.
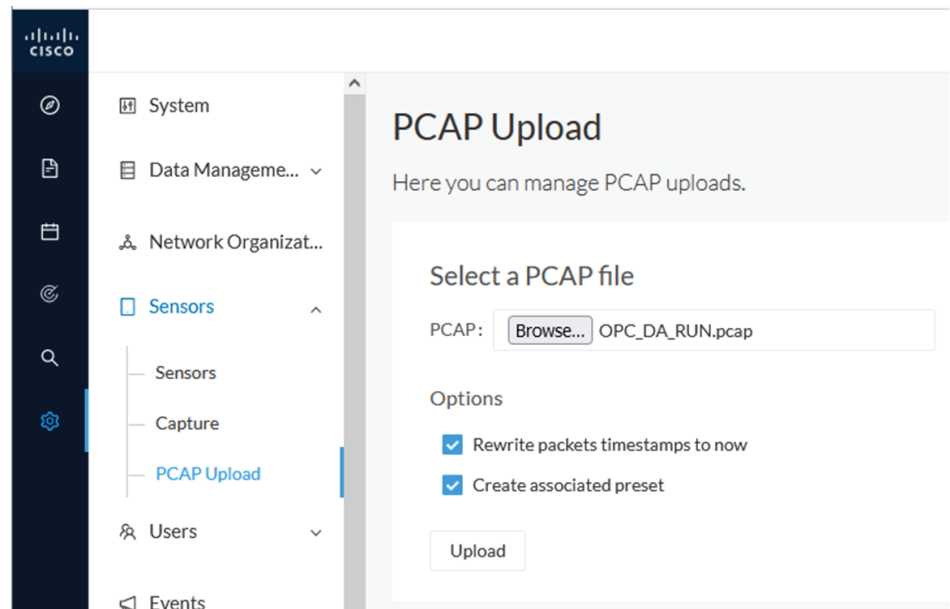
Note that during the upload that the status for the DPI and Snort are displayed.

If uploading a large file, you have the possibility to pause it. To relaunch the upload, you just need to select the same pcap again with the browse button and click Resume.

Note   pcap data cannot be erased individually from Cisco Cyber Vision. You will need to use the Clear data button and it will affect the whole database. Upload pcaps with caution.