



Sensors

- [Sensor Explorer, on page 1](#)
- [Templates, on page 22](#)
- [Management jobs, on page 27](#)
- [PCAP Upload, on page 28](#)

Sensor Explorer

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

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 the 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: Feb 15, 2022 10:41 AM

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
<input type="checkbox"/>	FOLDER1			LYON				
<input type="checkbox"/>	FOLDER2			PARIS				
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected	Disabled	0
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202021832		Connected	Pending data	Disabled	6 days
<input type="checkbox"/>	FCW2445P6XS	192.168.49.21	4.1.0+202202021803		Connected	Pending data	Unavailable	6 days

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)

<input type="checkbox"/>	Filter	0 Selected	Move selection to	More Actions	As o	
<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	 FOLDER1			Lyon		
<input type="checkbox"/>	 FOLDER2			Paris		
<input type="checkbox"/>	 FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	 FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing
<input type="checkbox"/>	 FCY014567	192.168.49.41			Disconnected	Disconnected

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

Folders and sensors (5)

Filter 0 Selected Move selection to More Actions ▾

Label	IP Address	Version	Location	Health status ⓘ	Processing status ⓘ
FCH			Lyon		
			Paris		
		4.1.0+202202151504		Connected	Pending data
		4.1.0+202202151440		Connected	Pending data
				Disconnected	Disconnected

Filter dialog box:

- Label: FCH
- IP Address: _____
- Version: _____
- Location: _____
- Health status: ▾

Buttons: Cancel, Apply

The folders and sensors list after filtering by label:

Folders and sensors (1)

Filter 0 Selected Move selection to More Actions ▾

Label is FCH ✕

<input type="checkbox"/>	Label ▲	IP Address	Version	Location	Health status ⓘ	Processing status ⓘ
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

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)

Filter 0 Selected Move selection to More Actions ▾

<input type="checkbox"/>	Label ▾	IP Address ▾	Version	Location	Health status ⓘ	Processing status ⓘ
<input type="checkbox"/>	FOLDER2			Paris		
<input type="checkbox"/>	FOLDER1			Lyon		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data

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.

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status ⓘ	Processing status ⓘ	Active Discovery	Uptime
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected	Disabled	N/A
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data	Enabled	3 days
<input type="checkbox"/>	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.

FCH2309Y01Z

Label: FCH2309Y01Z [✎](#)
 Serial Number: FCH2309Y01Z
 IP address: 192.168.49.23
 Version: 4.1.0+202202151504
 System date: Feb 16, 2022 10:07:45 AM
 Deployment: Sensor Management Extension
 Active Discovery: Disabled
 Capture mode: All

System Health
 Status: Connected
 Processing status: Pending data
 Uptime: 7 minutes

[Go to statistics](#)

Start Recording

Last recording: Feb 10, 2022 3:36:54 PM
[Download \(49 bytes\)](#)

[Move to](#)

[Download package](#) [Capture mode](#)

[Redeploy](#) [Enable IDS](#)

[Reboot](#) [Shutdown](#)

[Uninstall](#)

- 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 16](#).
- 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.

Sensor Self Update

Cisco Cyber Vision now allows sensor updates regardless of the install method (i.e., without the extension). Release 4.4.1 provides the necessary foundation for sensor self-updates. However, the self-update feature will only be functional in future releases.

Starting with Cisco Cyber Vision release 4.4.1, you can update all sensors automatically. The required steps are:

- Select sensors to update.
- The Center adds a new job to the sensor queue.
- The sensor automatically collects and validates the update file.
- The sensor restarts with the new version.

Update Warnings

In the Cisco Cyber Vision center on the Sensor Explorer page (Admin – Sensors – Sensor Explorer), users receive an alert to update the sensor. When this happens, the version number turns red, and a blue arrow with a tooltip indicates the sensor is upgradeable.

The screenshot shows the Cisco Cyber Vision interface. On the left is a navigation menu with options like Explore, Reports, Events, Monitor, Search, and Admin. The main content area is titled 'Sensor Explorer' and contains a table of sensors. A tooltip is visible over the first sensor, indicating it can be updated to version 4.4.0-202405232039.

Label	Serial Number	IP Address	Version	Status	
<input type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	
<input type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	

On the sensor's right-side, the same blue arrow and an **Update** button is visible.

FCH2309Y02K ✕

Label: FCH2309Y02K ✎
Serial Number: FCH2309Y02K
IP address: 192.168.49.37
Version: 4.4.0+202405071629 ⬆️
System date: Jun 5, 2024 3:32:50 PM
Deployment: Sensor Management Extension
Active Discovery: Enabled
Capture mode: All
Template: Default ✎

System Health
Status: Connected
Processing status: Normally processing
Uptime: 20 minutes

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

[Capture mode](#) [Redeploy](#)

[Enable IDS](#) [Uninstall](#)

[Active Discovery](#)

[Update](#)

Update Procedure

Step 1 Use the checkboxes on the left to select multiple sensors.

Folders and sensors (6)

Filter 3 Selected Move selection to More Actions ▾

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status
<input checked="" type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	
<input checked="" type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	
<input type="checkbox"/>	ie3400esc00	FCW2445P6X5	192.168.49.21	4.4.0	
<input checked="" type="checkbox"/>	IE3400esc02	FCW2721Y1GC	192.168.49.25	4.4.0	
<input type="checkbox"/>	IE3400esc03	FCW2721Y1QV	192.168.49.27	4.4.0	
<input type="checkbox"/>	IE3400esc04	FCW2721Y1FK	169.254.0.2	4.4.0	

Step 2 Go to the **More Actions** and click **Update sensors**.

The sensor self-update menu appears.

Folders and sensors (6)

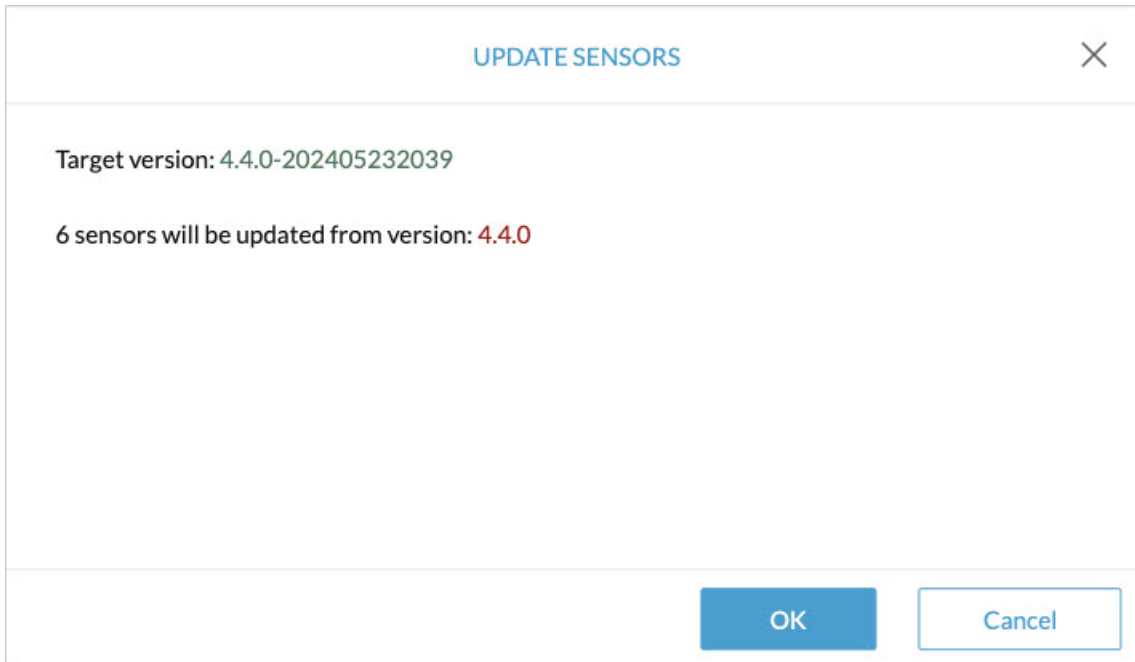
Filter 3 Selected Move selection to More Actions ^

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status
<input checked="" type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	
<input checked="" type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	
<input type="checkbox"/>	ie3400esc00	FCW2445P6X5	192.168.49.21	4.4.0	

More Actions menu:

- Delete folders
- Update sensors

Step 3 Click **OK**.



Step 4 During the update, a blue circle appears in the **Update status** column.

Folders and sensors (6)

Filter 0 Selected Move selection to More Actions

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status	Location
<input type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0		
<input type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0		
<input type="checkbox"/>	ie3400esc00	FCW2445P6X5	192.168.49.21	4.4.0		
<input type="checkbox"/>	IE3400esc02	FCW2721Y1GC	192.168.49.25	4.4.0		
<input type="checkbox"/>	IE3400esc03	FCW2721Y1QV	192.168.49.27	4.4.0		
<input type="checkbox"/>	IE3400esc04	FCW2721Y1FK	169.254.0.2	4.4.0		

Step 5 After the update, the version number turns black, and a green symbol appears in the **Update status** column.

<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status	Location
<input type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0		
<input type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0		
<input type="checkbox"/>	ie3400esc00	FCW2445P6X5	192.168.49.21	4.4.0		
<input type="checkbox"/>	IE3400esc02	FCW2721Y1GC	192.168.49.25	4.4.0		
<input type="checkbox"/>	IE3400esc03	FCW2721Y1QV	192.168.49.27	4.4.0		
<input type="checkbox"/>	IE3400esc04	FCW2721Y1FK	169.254.0.2	4.4.0		

Step 6 The **Update in progress** status is visible.

ie3400esc00 ✕

Label: ie3400esc00 ✎
Serial Number: FCW2445P6X5
IP address: 192.168.49.21
Version: 4.4.0+202405071631
System date: Jun 5, 2024 3:34:59 PM
Deployment: Manual
Active Discovery: Enabled
Capture mode: All
Template: Default ✎

System Health
Status: Connected
Processing status: Normally processing
Uptime: 1 hour

▶ Start Recording

📁 Move to

↓ Download package 🔑 Capture mode

⊖ Uninstall 🔍 Active Discovery

↻ Update 🔄 Update in progress

Update Failure

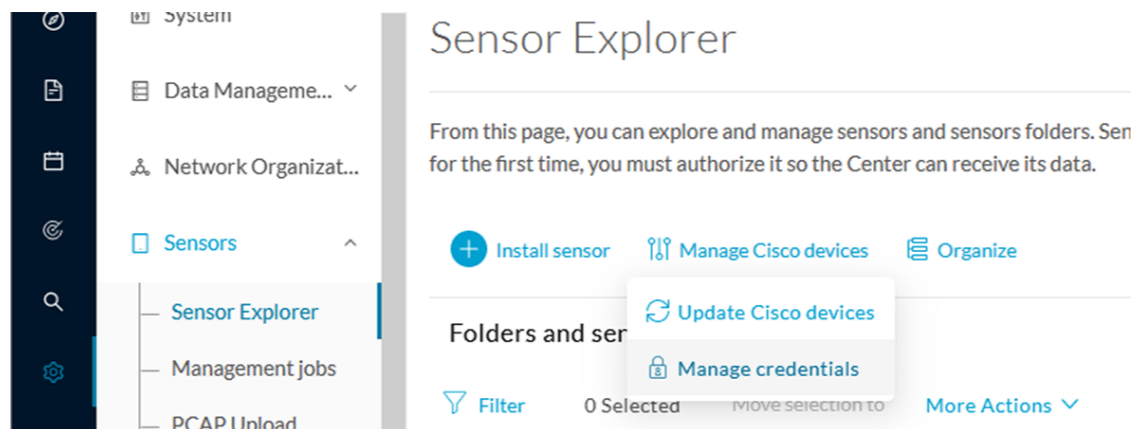
If the update is unsuccessful, the **Update status** column displays a red cross and a message that provides the details.

The screenshot shows the 'Folders and sensors (6)' section of the Sensor Explorer. A table lists sensors with columns for Label, Serial Number, IP Address, Version, and Update status. A tooltip is displayed over the 'Update status' column for the sensor FCH2309Y02K, indicating an update failure.

Label	Serial Number	IP Address	Version	Update status
FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	Update unsuccessful: Marked as failed because the update remained in a transient status for too long Last failed attempt: Jun 5, 2024
FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	Connected normally processing

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.

SET GLOBAL CREDENTIALS

You can define "global credentials" which can be used as default credentials when deploying a new Cisco device. When you update these "global credentials" it affects both new and deployed sensors.

Login *

Password *

Save Cancel

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

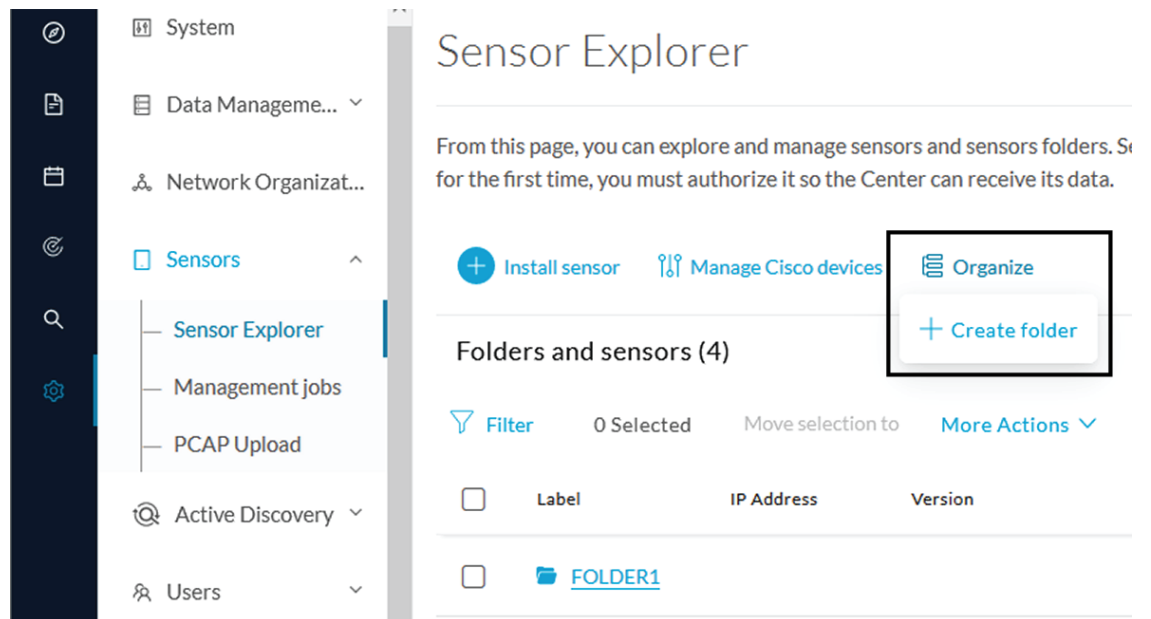
- Optimal (default): analyze the most relevant flows

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.

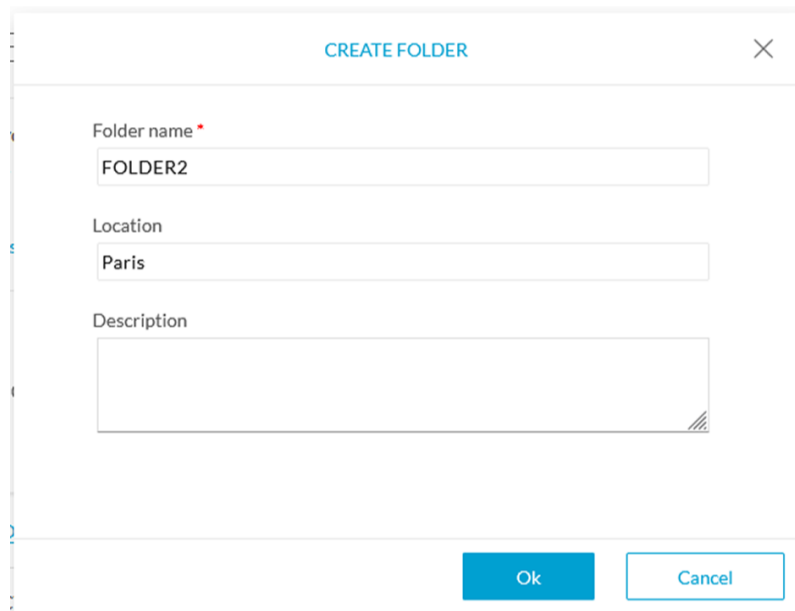
To create a folder and move a sensor in it:

1. Click the Organize button and click Create folder.



The screenshot shows the 'Sensor Explorer' interface. On the left is a navigation sidebar with a 'Sensors' section expanded to show 'Sensor Explorer', 'Management jobs', and 'PCAP Upload'. The main content area has a title 'Sensor Explorer' and a sub-header 'Folders and sensors (4)'. Below this is a table with columns 'Label', 'IP Address', and 'Version'. The table contains one entry: 'FOLDER1'. A 'More Actions' dropdown menu is open, showing 'Organize' and '+ Create folder' options. The '+ Create folder' option is highlighted with a black box.

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








The 'CREATE FOLDER' dialog box is shown. It has a title bar with 'CREATE FOLDER' and a close button. The form contains three fields: 'Folder name' with the value 'FOLDER2', 'Location' with the value 'Paris', and 'Description' which is empty. At the bottom are 'Ok' and 'Cancel' buttons.

The new folder is displayed in the sensor list.

Folders and sensors (5)


Filter 0 Selected Move selection to More Actions ▾ As

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
<input type="checkbox"/>	 FOLDER1			Lyon		
<input type="checkbox"/>	 FOLDER2			Paris		
<input type="checkbox"/>	 FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	 FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	 FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

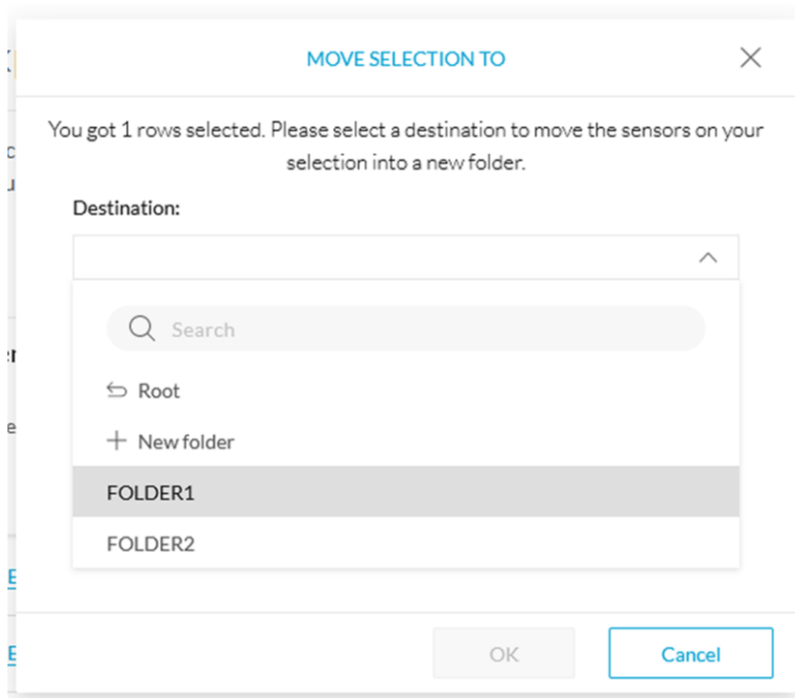
- Select a sensor in the list and click the button Move selection to.

Folders and sensors (5)

Filter 1 Selected Move selection to More Actions ▾ As

<input checked="" type="checkbox"/>	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
<input type="checkbox"/>	 FOLDER1			Lyon		
<input type="checkbox"/>	 FOLDER2			Paris		
<input type="checkbox"/>	 FCY014567	192.168.49.41			Disconnected	Disconnected
<input checked="" type="checkbox"/>	 FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Connected	Pending data
<input type="checkbox"/>	 FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Normally processing

- 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.

Folders and sensors (4)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	FOLDER1		4.1.0+202202151504	Lyon	Connected	Pending data
<input type="checkbox"/>	FOLDER2			Paris		
<input type="checkbox"/>	FCY014567	192.168.49.41			Disconnected	Disconnected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data

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)

Filter 0 Selected Move selection to More Actions ▾

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status ⓘ ▾	Processing status ⓘ
<input type="checkbox"/>	 FOLDER1		- 4.1.0	Lyon	Disconnected	Disconnected
<input type="checkbox"/>	 FOLDER2			Paris		
<input type="checkbox"/>	 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)

Filter 0 Selected Move selection to More Actions ▾

<input type="checkbox"/>	Label	IP Address	Version	Health status ⓘ ▾	Processing status ⓘ
<input type="checkbox"/>	 FCY014567	192.168.49.41		Disconnected	Disconnected
<input type="checkbox"/>	 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:

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and connects for the 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](#) ▾

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FOLDER1			Lyon	
<input type="checkbox"/>	FOLDER2			Paris	
<input type="checkbox"/>	FCY014567	192.168.49.41			Discon
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.1.0+202202151504		Conne
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Conne

FCH2309Y01Z

Label: FCH2309Y01Z [✎](#)
 Serial Number: FCH2309Y01Z
 IP address: 192.168.49.23
 Version: 4.1.0+202202151504
 System date: Mar 9, 2022 11:46:58 AM
 Deployment: Sensor Management Extension
 Active Discovery: Enabled
 Capture mode: All

System Health
 Status: Connected
 Processing status: Pending data
 Uptime: 20 hours

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

[Download package](#) **[Capture mode](#)**

[Redeploy](#) [Enable IDS](#)

[Reboot](#) [Shutdown](#)

[Uninstall](#) [Active Discovery](#)

Capture modes:

CAPTURE MODE

Please select an option to filter the flows analyzed by this sensor.

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**

[OK](#) [Cancel](#)

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.

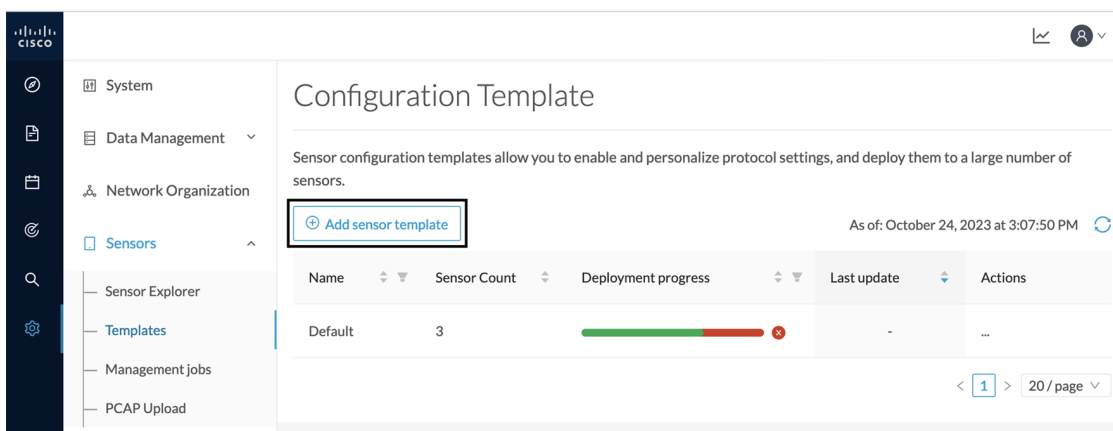
A sensor can be associated with a single template only. Deployment of the template can fail:

- 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**.

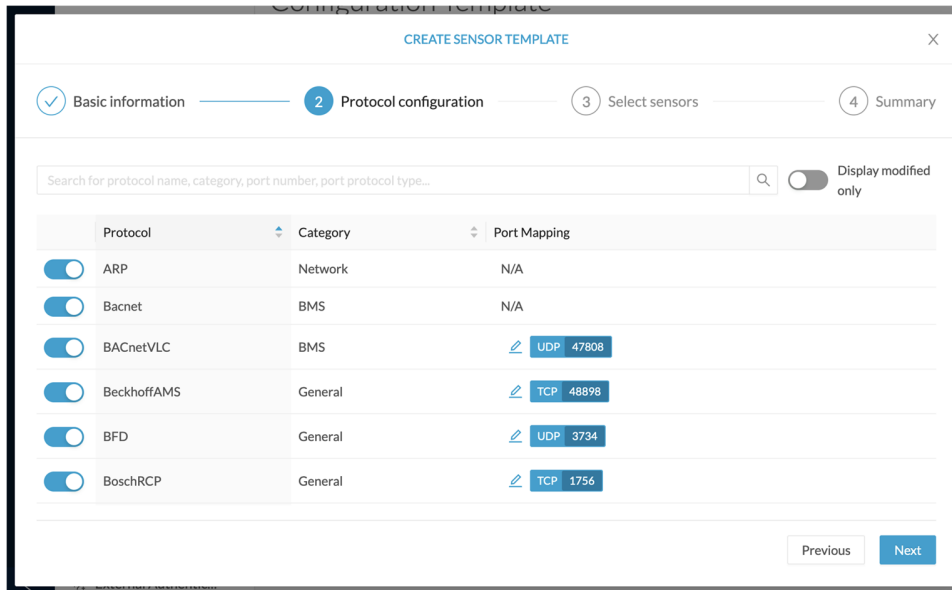


The Create sensor template window pops up.

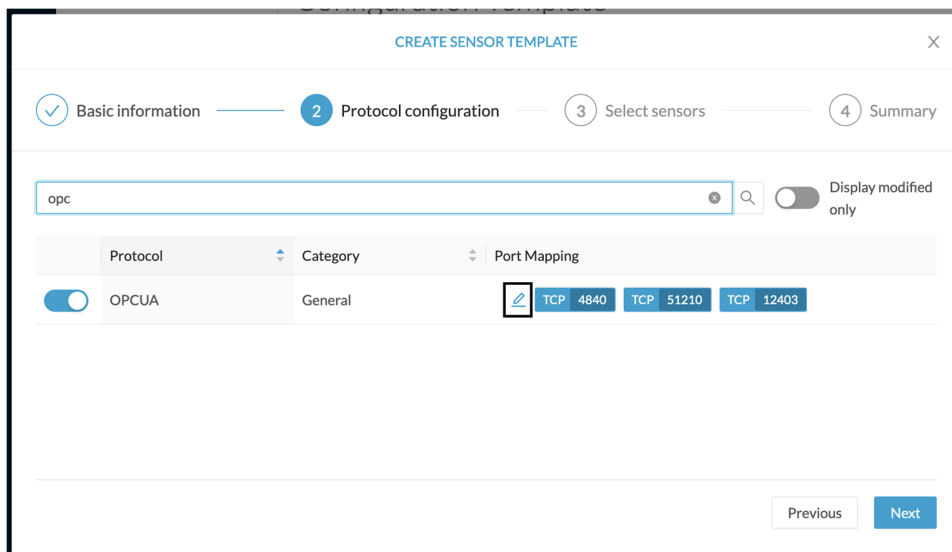
Step 3 Add a name to the template. You can also add a description.

Step 4 Click **Next**.

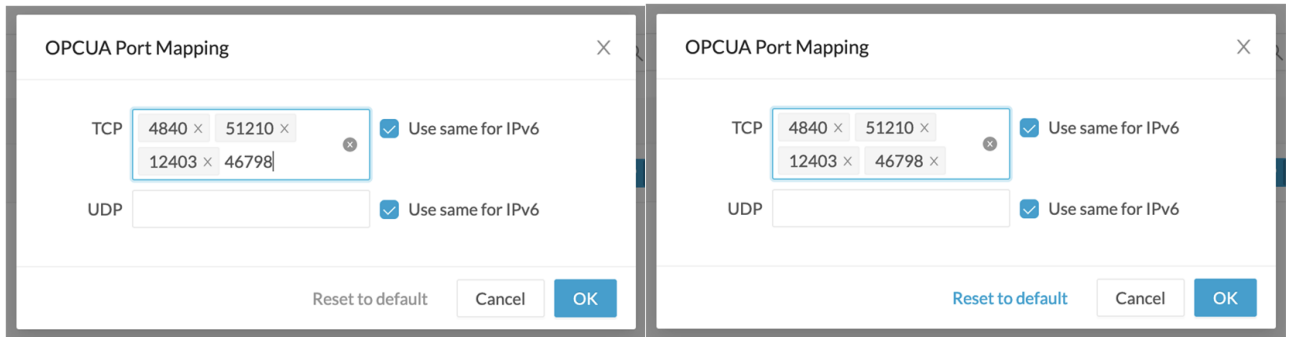
The list of protocol DPI engines with their basic configurations appears.



- 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.

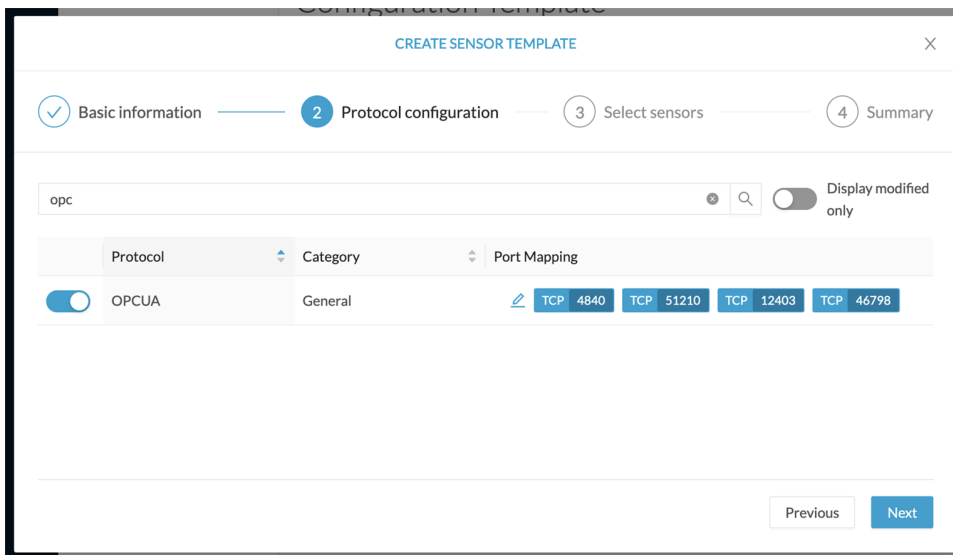


- Step 6** Under the Port Mapping column, click the **pen** button to edit its settings.
The protocol's port mapping window pops up.
- Step 7** Write down the port number you want to add and hit enter.

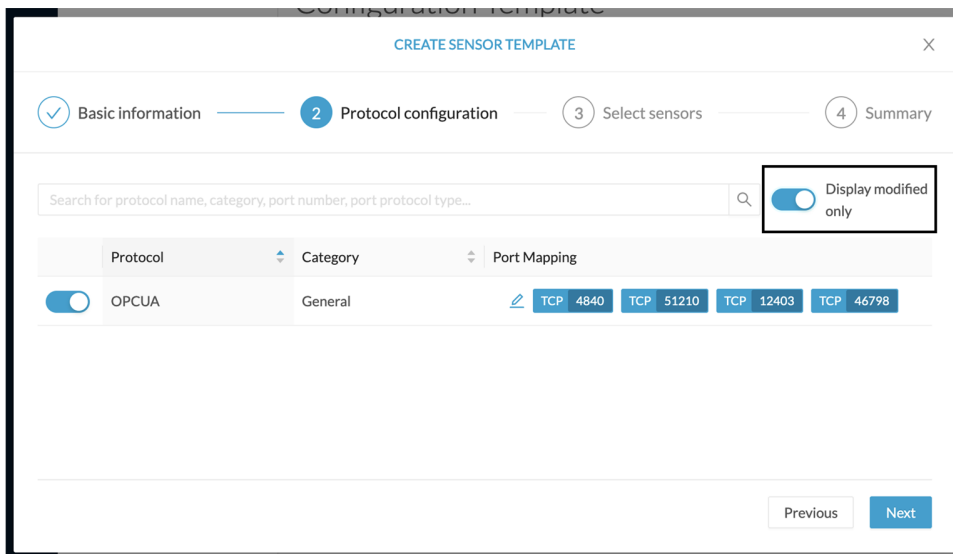
**Step 8**

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.

CREATE SENSOR TEMPLATE

Basic information Protocol configuration **3 Select sensors** 4 Summary

2 Selected Filters Select All Unselect All As of: October 25, 2023 at 10:33:19 AM

Label	IP	Folder	Template	Template Deployment Status	Version	Location	Health Status	Processing Status	Active Discovery	Uptime
<input checked="" type="checkbox"/> Sensor_Line1	192.168.49.25	FOLDER1	Default	deployed	4.3.0+202310181603	Line 1	Connected	Normally processing	Enabled	5 days
<input type="checkbox"/> Sensor_Line2		FOLDER2	Default	failed		Line 2	Disconnected	Disconnected	Unavailable	N/A
<input checked="" type="checkbox"/> Sensor_Line3	192.168.49.23		Default	deployed	4.3.0+202310181544		Connected	Normally processing	Unavailable	16 hours

3 Records < 1 > 10/page

Previous Next

Step 11 Click **Next**.

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

CREATE SENSOR TEMPLATE

Basic information Protocol configuration Select sensors **4 Summary**

OPCUA

Sensors

2 sensors selected [view list](#)

Settings Display modified only

OPCUA

Status: enabled

Port Mapping: TCP 4840 TCP 51210 TCP 12403 TCP 46798

Previous Confirm

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	<div style="width: 100%; height: 10px; background-color: red;"></div>	-	...
OPCUA	2	<div style="width: 100%; height: 10px; background-color: green;"></div>	Today	...

< 1 > 20 / page v

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.

Jobs	Steps	Duration
Single redeployment (FCW2435P3KW)		1m 11s
Single redeployment (FCW23500HDC)		41s
Single redeployment (FOC2337LOCW)		1m 33s
Single redeployment (FCW23500HDC)		35s
Single redeployment (FCW23500HDC)		39s
Single redeployment (FCW23500HDC)		43s
Single redeployment (FOC2334V045)		6m 52s

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.

Jobs	Steps
Single redeployment (FCW23500HDC)	
Single redeployment (FCW2435P3KW)	
Single redeployment (FCW23500HDC)	
Single redeployment (FOC2337L0CW)	
Single redeployment (FCW23500HDC)	

Enroll

Error

```
Fatal error: cannot upload provisioning package: UploadAppData failed: Fog Director API Error Code 0: {"message": "File upload failed. App data upload is not allowed since this app was installed with --rm option and currently app container is cleaned after stopping the app. Consider starting the app and retry."}
```

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.

Name	Size	Upload status	Processing status	Packets first timestamp
OPC_DA_RUN.pcap	7.3 MB	<div style="width: 100%;"><div style="width: 100%;"></div></div> ✓	DPI: ✓ Snort: ✓	Jul 5, 2021 5:42:20 PM
smb_putty_xfer.pcap	726.5 kB	<div style="width: 100%;"><div style="width: 100%;"></div></div> ✓	DPI: ✓ Snort: ✓	Jun 30, 2021 4:23:24 PM
MergedFile.pcapng	815 MB	<div style="width: 3%;"><div style="width: 3%;"></div></div> 3%	DPI: ○ Snort: ○	
DAN_Rockwell_With_Variables.pcap	1.5 MB	<div style="width: 100%;"><div style="width: 100%;"></div></div> ✓	DPI: ✓ Snort: ✓	Jun 30, 2021 11:28:37 AM

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.

