



## **Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.1**

**First Published:** 2019-01-01

**Last Modified:** 2023-12-14

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





## CONTENTS

---

<b>CHAPTER 1</b>	<b>About this documentation</b>	<b>1</b>
	Document purpose	1
	Warnings and notices	1

---

<b>CHAPTER 2</b>	<b>Overview</b>	<b>3</b>
	Overview	3

---

<b>CHAPTER 3</b>	<b>Requirements</b>	<b>5</b>
	Requirements	5

---

<b>CHAPTER 4</b>	<b>Hardware front view</b>	<b>7</b>
	Hardware front view	7

---

<b>CHAPTER 5</b>	<b>Known issues</b>	<b>9</b>
------------------	---------------------	----------

---

<b>CHAPTER 6</b>	<b>Initial configuration</b>	<b>11</b>
	Check the software version	11
	Check date and time	11
	Enable IOx	12
	Setup ERSPAN	13
	Setup NAT	14

---

<b>CHAPTER 7</b>	<b>Procedure with the Cisco Cyber Vision sensor management extension</b>	<b>17</b>
	Install the sensor management extension	17
	Management jobs	18
	Create a sensor	19

Configure the sensor 20

---

**CHAPTER 8**

**Procedure with the Local Manager 23**

- Access the IOx Local Manager 23
- Install the sensor virtual application 25
- Configure the sensor virtual application 26
- Generate the provisioning package 32
- Import the provisioning package 34

---

**CHAPTER 9**

**Procedure with the CLI 37**

- Configure the sensor application 37
  - without SSD 37
  - with SSD 38
- Install the sensor application 38
- Copy the sensor application's provisioning package 39

---

**CHAPTER 10**

**Configuration 41**

- Configure Active Discovery 41
- Configure sensor configuration template 43
  - Templates 43
  - Create templates 43
- Set a capture mode 48

---

**CHAPTER 11**

**Maintenance 51**

- Upgrade procedures 51
  - Sensor Self Update 51
    - Update Warnings 51
    - Update Procedure 53
    - Update Failure 58
  - Upgrade through the Cisco Cyber Vision sensor management extension 59
    - Update the sensor management extension 59
    - Update the sensors 60
  - Upgrade through the IOx Local Manager 62
- Certificate renewal 66



Sensor certificate renewal 66

Sensor certificate renewal through the Local Manager 70

---

**CHAPTER 12****Troubleshooting 75**

Collect IOx sensor logs 75

Collect IOx sensor logs from the Local Manager 76





# CHAPTER 1

## About this documentation

---

- [Document purpose, on page 1](#)
- [Warnings and notices, on page 1](#)

### Document purpose

This installation guide describes how to perform a clean installation of Cisco Cyber Vision on the following devices:

- Cisco Catalyst IR1101 Rugged Series Router
- Cisco Catalyst IR1800 Rugged Series Router

Moreover, this document describes how to upgrade sensors through different methods.

This documentation is applicable to **system version 4.4.1**.



---

**Note** To be able to use the Cisco Cyber Vision sensor management extension, an IP address reachable by the Center Collection interface must be set on the Collection VLAN.

---

### Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.



---

**Warning** Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

---



---

**Important** Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

---



---

**Note** Indicates important information on the product described in the documentation to which attention should be paid.

---



## CHAPTER 2

# Overview

---

- [Overview, on page 3](#)

## Overview

The architecture proposed and described in this document is for demonstration. The local network engineer should be consulted before applying the parameters used in this document. IP addresses, port numbers and VLAN IDs used should be verified beforehand as wrong configurations could stop normal exchanges and stop the process.

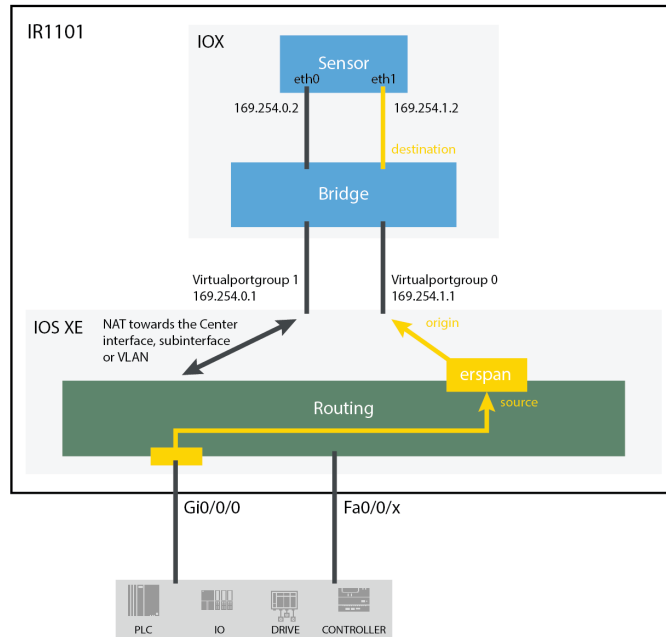
The schema below explains the architecture virtually deployed in the router to embed the sensor application. VLAN and physical ports configuration will allow OT traffic to be copied and communication with the Cisco Cyber Vision Center to be established.

The communication between the Cisco Cyber Vision Center and the sensor is represented in black on the schema. Mirrored OT traffic is represented in yellow.

Any port of the router can be used for the communication with the Center.

Only the routed traffic to the port gi0/0/0 can be spanned to the sensor.

Figure 1: Cisco IR1101 Integrated Services Router Rugged:



The sensor can be installed on the Cisco IR1101 with different disk configurations: on a SSD, or on the flash if there is no SSD.

SD card is not supported and will be ignored.

In case the sensor management extension is used and if a SSD is detected, Cisco Cyber Vision will be automatically deployed on it. If there is none, the application will be installed on the flash memory.

For other deployment modes (IOx Local Manager or CLI), the procedures describe how the installation is done for both cases.



## CHAPTER 3

# Requirements

---

- [Requirements, on page 5](#)

## Requirements

The Cisco IR1101 needs to be configured with access to the CLI (ssh or console port). An access to the IOx Local Manager could be necessary depending on the installation procedure chosen.

To be able to use the Cisco Cyber Vision sensor management extension, it has to be deployed on the Center and an IP address reachable by the Center Collection interface must be set on the device.

In case of manual installation (IOx Local Manager or CLI), the Cisco Cyber Vision Sensor application must be collected from Cisco.com, i.e.

`CiscoCyberVision-sensor-IOx-aarch64-<VERSION>.tar`







## CHAPTER 4

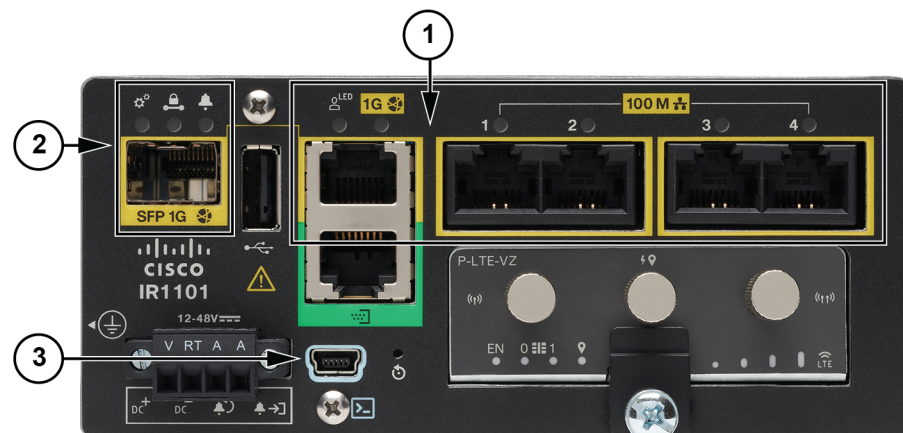
# Hardware front view

- [Hardware front view, on page 7](#)

## Hardware front view

Before starting, take a moment to note the following parts you're going to use during the procedure.

**Cisco Cisco IR1101 Integrated Services Router Rugged:**



- 1x RJ45 10/100/1000 BaseT connector (the one on the left) (1)
- 4x RJ45 10/100 BaseT connector (the ones on the right) (1)
- SFP fiber port (2)
- mini-USB console connector (3)





## CHAPTER 5

### Known issues

---

- [Known issues, on page 9](#)

### Known issues

The deployment procedure with the Local Manager is not supported by firmware version 17.3.x.

Perform the procedure with [Procedure with the Cisco Cyber Vision sensor management extension](#) instead.





## CHAPTER 6

# Initial configuration

To install Cisco Cyber Vision on the Cisco IR1101, you must perform the Initial configuration which steps are described in this section.

- [Check the software version, on page 11](#)
- [Check date and time, on page 11](#)
- [Enable IOx, on page 12](#)
- [Setup ERSPAN, on page 13](#)
- [Setup NAT, on page 14](#)

## Check the software version

- Check the software version using the following command in the router's CLI:

```
Show version
```

The displayed version must be 17.2.1 or higher to be compatible with the Cisco Cyber Vision Sensor Application.

```
IR110CCV#  
IR110CCV#Show version  
Cisco IOS XE Software, Version 17.02.01r  
Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 17.2.1r, RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2020 by Cisco Systems, Inc.  
Compiled Thu 09-Apr-20 22:45 by mcpre
```

If the version is lower, you must update the router firmware. To do so, go to [cisco.com](http://cisco.com) and refer to the Cisco IR1101's documentation.

## Check date and time

The internal clock of the router must be synchronized and configured properly.



**Note** The Cisco Cyber Vision IOx sensor application gets the time from the host. Therefore, it is critical that the host synchronizes its time with the Center or a valid NTP server. If the time difference is large (hours or more), the user should adjust the Cisco IR1101 time using the CLI or the WebUI so it is close to the reference time. If not, the synchronization may take many update cycles.

1. Check the date and time using the following command:

```
Show clock
```

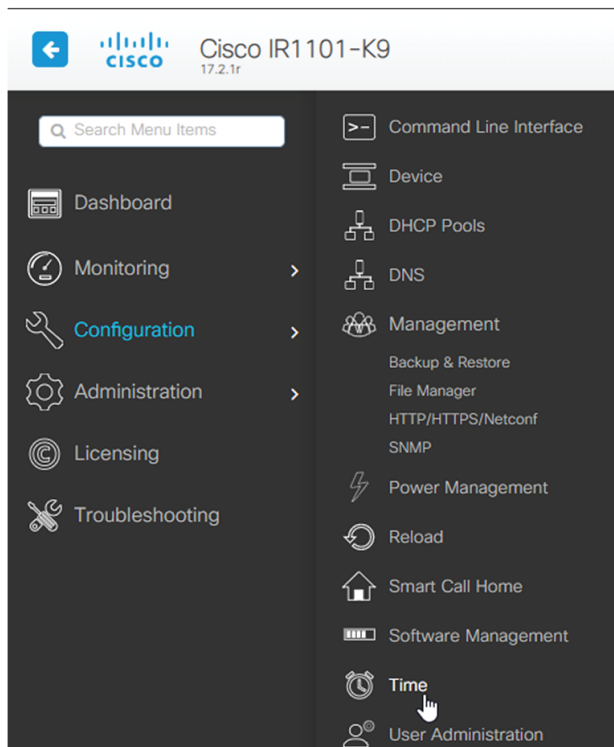
```
IR110CCV#
IR110CCV#Show clock
*14:33:05.354 UTC Fri Apr 17 2020
IR110CCV#
```

- 2.

If needed, adjust to the UTC time using the following command:

```
clock set [hh:mm:ss] [month] [day] [year]
```

Or in the WebUI, navigate to Configuration > Time.



## Enable IOx

Before installing the Cisco Cyber Vision sensor on the Cisco IR1101, you must enable IOx.

## Procedure

---

**Step 1** Enable IOx using the following command.

```
configure terminal
iox
```

**Step 2** Check that the CAF and IOxman services are running using the following command.

```
exit
show iox
```

```
IR110CCV(config)#
IR110CCV(config)#exit
IR110CCV#show iox

IOx Infrastructure Summary:
-----
IOx service (CAF) 1.10.0.1 : Running
IOx service (HA)          : Not Supported
IOx service (IOxman)      : Running
IOx service (Sec storage) : Not Supported
Libvirtd 1.3.4            : Running
Dockerd  18.03.0          : Running

IR110CCV#
```

---

## Setup ERSPAN

In order to receive traffic in the Cisco Cyber Vision IOx application, the application:

- must be connected to a VirtualPortGroup,
- must have the correct IP address assigned,
- must have a monitor session created.

1. Connect the application to a VirtualPortGroup and set an IP address using the following commands:

```
Configure terminal
ip routing
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
exit
```

```

IR110CCV#
IR110CCV#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IR110CCV(config)#ip routing
IR110CCV(config)#interface virtualportgroup 0
IR110CCV(config-if)#ip address 169.254.1.1 255.255.255.252
IR110CCV(config-if)#
IR110CCV(config-if)#
IR110CCV(config-if)#exit
IR110CCV(config)#

```

2. Create the monitor session using the following commands:

```

monitor session 1 type erspan-source
source interface Gi0/0/0
no shutdown
destination
erspan-id 1
mtu 1464
ip address 169.254.1.2
origin ip address 169.254.1.1
end

```

```

IR110CCV(config)#monitor session 1 type erspan-source
IR110CCV(config-mon-erspan-src)#source interface Gi0/0/0
IR110CCV(config-mon-erspan-src)#no shutdown
IR110CCV(config-mon-erspan-src)#destination
IR110CCV(config-mon-erspan-src-dst)#erspan-id 1
IR110CCV(config-mon-erspan-src-dst)#mtu 1464
IR110CCV(config-mon-erspan-src-dst)#ip address 169.254.1.2
IR110CCV(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
IR110CCV(config-mon-erspan-src-dst)#end
IR110CCV#

```

## Setup NAT

You must add NAT rules so that the container can reach the outside. This will be on a different virtual port group from the ERSPAN to separate the traffic.

### Procedure

- Step 1** Type the following commands to achieve this configuration.

```

Configure terminal
interface GigabitEthernet 0/0/0
ip nat outside
media-type rj45
exit
interface VirtualPortGroup 1
ip address 169.254.0.1 255.255.255.252
ip nat inside

```



```
exit
ip nat inside source list NAT_ACL interface GigabitEthernet 0/0/0 overload
ip access-list standard NAT_ACL
10 permit 169.254.0.0 0.0.0.3
exit
```

```
IR110CCV#
IR110CCV#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IR110CCV(config)#interface GigabitEthernet 0/0/0
IR110CCV(config-if)#ip nat outside
IR110CCV(config-if)#media-type rj45
IR110CCV(config-if)#exit
IR110CCV(config)#interface VirtualPortGroup 1
IR110CCV(config-if)#ip address 169.254.0.1 255.255.255.252
IR110CCV(config-if)#ip nat inside
IR110CCV(config-if)#exit
IR110CCV(config)#ip nat inside source list NAT_ACL interface GigabitEthernet 0/0/0 overload
IR110CCV(config)#ip access-list standard NAT_ACL
IR110CCV(config-std-nacl)#10 permit 169.254.0.0 0.0.0.3
IR110CCV(config-std-nacl)#exit
IR110CCV(config)#
```

## Step 2 Save the configuration.

```
exit
write mem
```

```
IR110CCV#
IR110CCV#write mem
Building configuration...

[OK]
IR110CCV#
*Apr 17 16:22:58.709: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
IR110CCV#
```

## What to do next

Proceed with one of the following procedures:

- [Procedure with the Cisco Cyber Vision sensor management extension, on page 17](#)
- [Procedure with the Local Manager, on page 23](#)
- [Procedure with the CLI, on page 37](#)





## CHAPTER 7

# 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, on page 17](#)
- [Create a sensor, on page 19](#)
- [Configure the sensor, on page 20](#)

## 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.

Name	Version	Actions
Cyber Vision sensor management	4.1.0	<a href="#">Update</a> <a href="#">Remove</a>

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.

Jobs	Steps	Duration
Single redeployment (FCW2435P3KW)	✓ — ✓ — ✓ — ✓	1m 11s
Single redeployment (FCW23500HDC)	✓ — ✓ — ✗ —	41s
Single redeployment (FOC2337L0CW)	✓ — ✓ — ✓ — ✓	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)	<div style="position: absolute; top: 0; right: 0; background-color: black; color: white; padding: 2px;">Enroll - Error</div>
Single redeployment (FCW2435P3KW)	
Single redeployment (FCW23500HDC)	
Single redeployment (FOC2337L0CW)	
Single redeployment (FCW23500HDC)	

Enroll

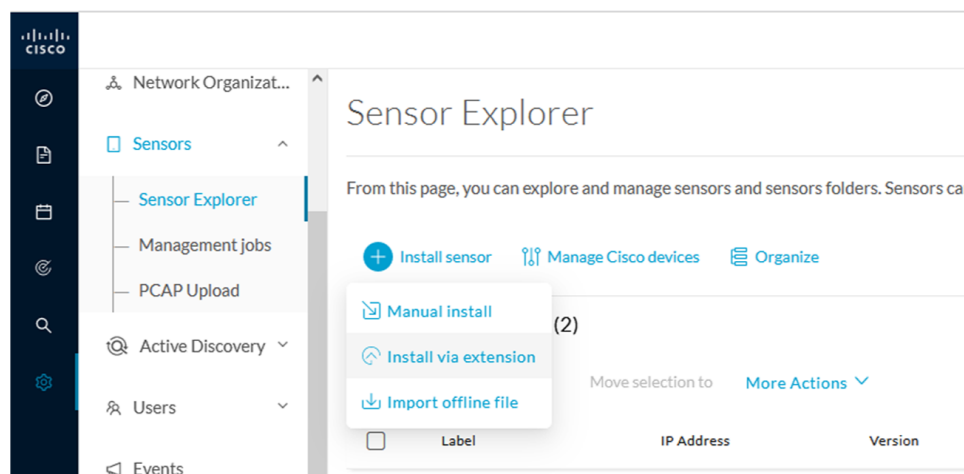
Error

```
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."}
```

## 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\*

Port\*  For example 443 or 8443

Center collection IP

leave blank to use current collection IP

---

Credentials

Login\*

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\*

Capture prefix length\*

Like 24, 16 or 8

Collection IP address\*

Collection prefix length\*

Like 24, 16 or 8

Collection gateway\*

[Exit](#)

[Deploy](#)

While some parameters are filled automatically, you can still change them if necessary.

### Procedure

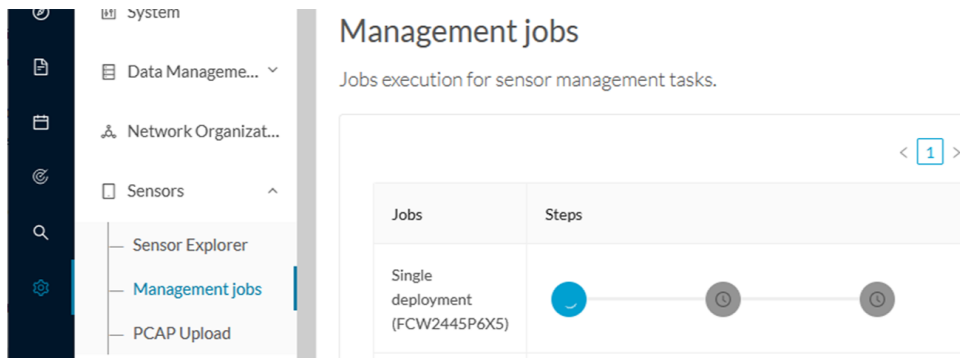
---

- 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.

Configure the sensor



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.

<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	4 days
--------------------------	-------------	---------------	--------------------	-----------	--------------	---------	--------





## CHAPTER 8

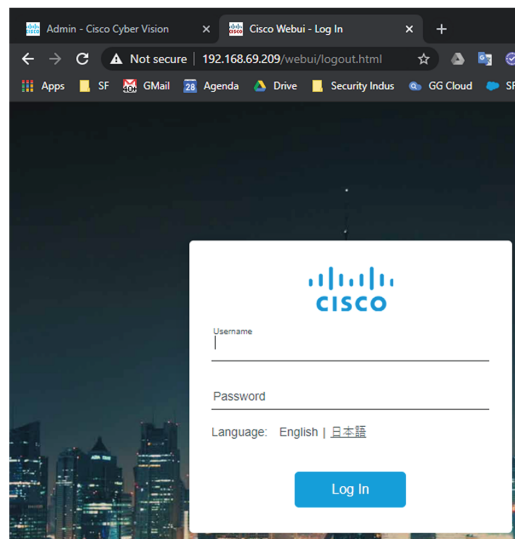
# Procedure with the Local Manager

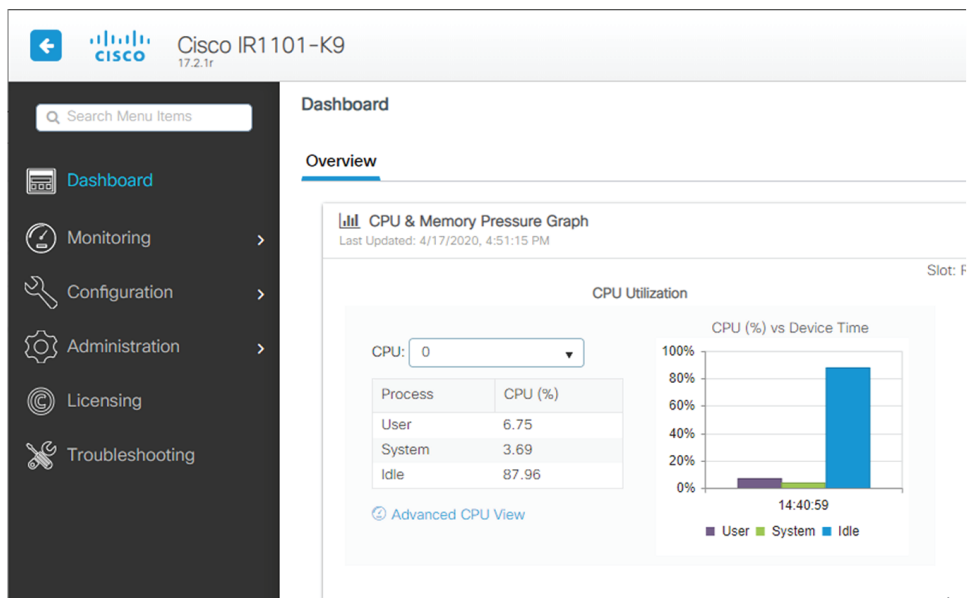
After the [Initial configuration](#), proceed to the steps described in this section.

- [Access the IOx Local Manager, on page 23](#)
- [Install the sensor virtual application, on page 25](#)
- [Configure the sensor virtual application, on page 26](#)
- [Generate the provisioning package, on page 32](#)
- [Import the provisioning package, on page 34](#)

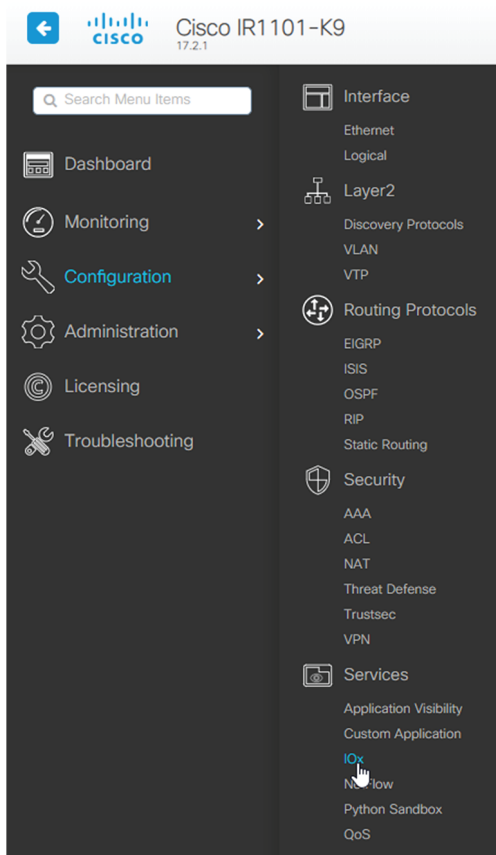
## Access the IOx Local Manager

1. Open a browser and navigate to the IP address you configured on the interface you are connected to.
2. Log in using the Cisco IR1101 admin user account and password.





3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.

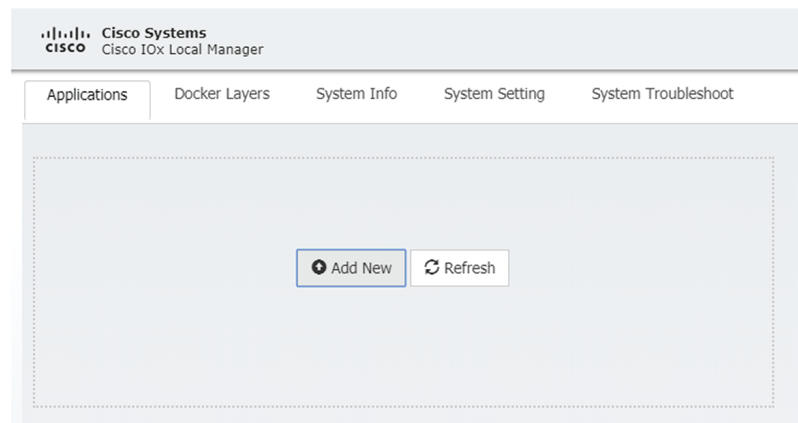


4. Log in using the user account and password.



## Install the sensor virtual application

Once logged in, the following menu appears:

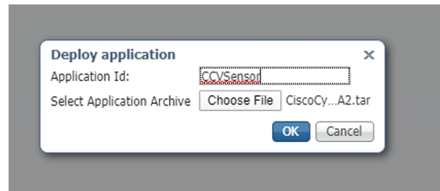


1. Click **Add New**.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file  
(i.e. "CiscoCyberVision-IOx-aarch64-<version>.tar").

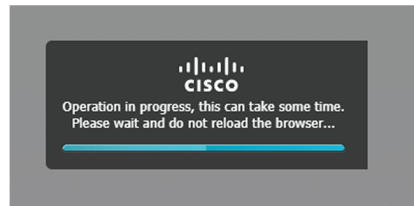


**Note** If you aim to install a sensor with **Active Discovery**, select the required application archive file

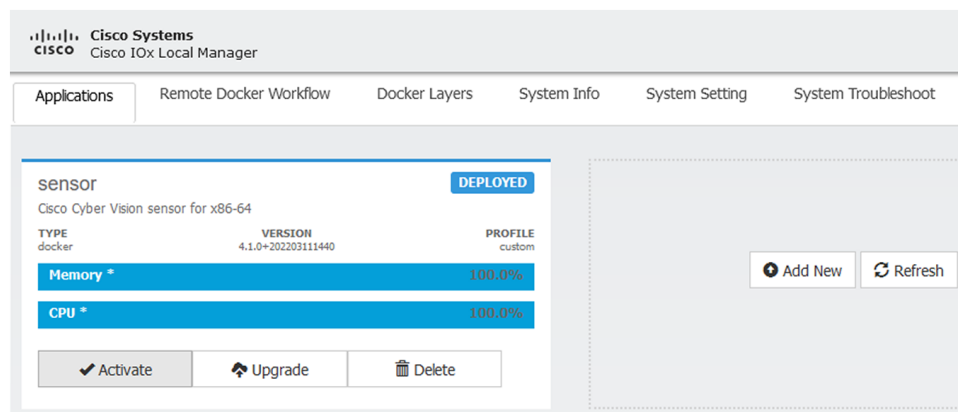
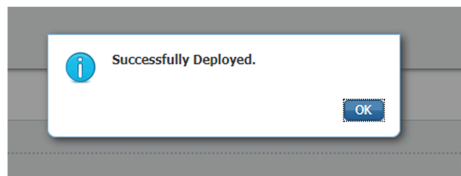
(i.e. "CiscoCyberVision-IOx-Active-Discovery-aarch64-<version>.tar").



The installation takes a few minutes.



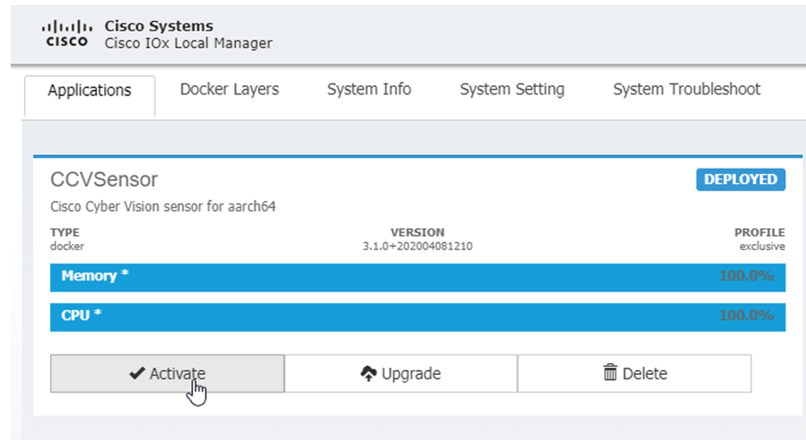
When the application is installed, the following message is displayed and the sensor application appears:



## Configure the sensor virtual application

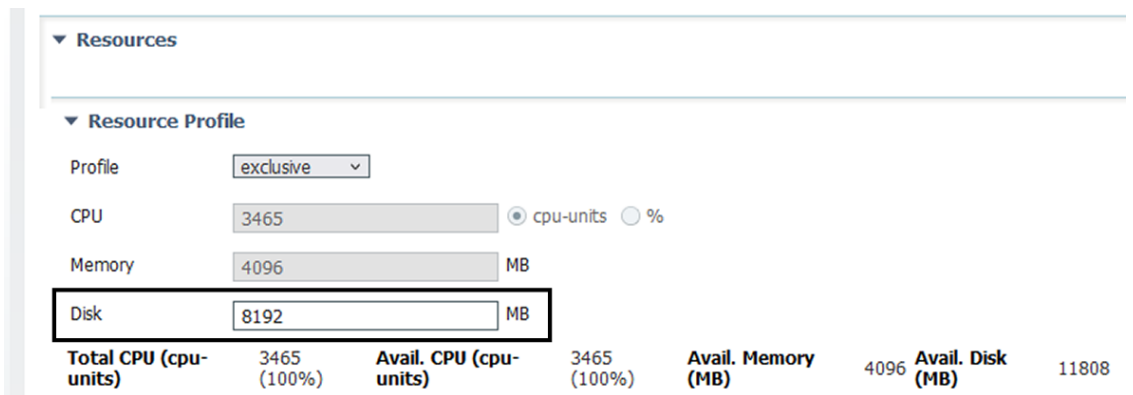
### Procedure

- Step 1** Click **Activate** to launch the configuration of the sensor application.



**Step 2** Deploy the Resource Profile menu and set the disk size. The procedure differs whether the device has a SSD or not:

- If the device has a SSD, set the necessary disk size. It should be at least 4GB.



- If the device has no SSD, set the disk size to 384MB, then deploy the Advanced Settings menu and configure tmpfs by filling the docker options text area with:

```
--tmpfs /tmp:rw,size=128m
```

Configure the sensor virtual application

**Resources**

**Resource Profile**

Profile:

CPU:   cpu-units  %

Memory:  MB

Disk:  MB

**Total CPU (cpu-units) 1155 (100%) Avail. CPU (cpu-units) 1155 (100%) Avail. Memory (MB) 862 Avail. Disk (MB) 181**

**Advanced Settings**

Specify "docker run" options to be used while spawning the container. These will override activation settings above.

Docker Options:

Auto delete container instance

**Step 3** Bind the eth0 and eth1 interfaces in the container to an interface on the host in the Network Configuration menu.

**eth0:**

a) Click **edit** in the eth0 line.

**Network Configuration**

Name	Network Config	Description	Action
eth0	VPG0	none	<a href="#">edit</a>
eth1	Not Configured	none	<a href="#">edit</a>

b) Select the **VPG1** interface.

**Network Configuration**

Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0  [Interface Setting](#)

Description (optional):

c) Click **Interface setting**.

▼ Network Configuration

Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0 VPG1 VirtualPortGroup via ints ▼ [Interface Setting](#)

Description (optional):

The Interface Setting window pops up.

- d) Apply the following configurations:
- Set IPv4 as **Static**.
  - IP/Mask: 169.254.0.2 / 30
  - Default gateway: 169.254.0.1

Interface Setting

IPv4 Setting

Static  Dynamic  Disable

IP/Mask:  /

DNS:

Default Gateway IP:

- e) Check that IPV6 is set to **Disable**.

IPv6 Setting

Static  Dynamic  Disable

- f) Click **OK** to save the interface settings.  
You're back to the Network Configuration menu.

▼ Network Configuration

Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0  [Interface Setting](#)

Description (optional):

- g) Click **OK** to save the network configurations.  
A popup that confirms changes appears.



- h) Click **OK**.

#### Step 4

##### eth1:

- Click **edit** in the eth1 line.
- Select the **VPG0** interface.

▼ Network Configuration

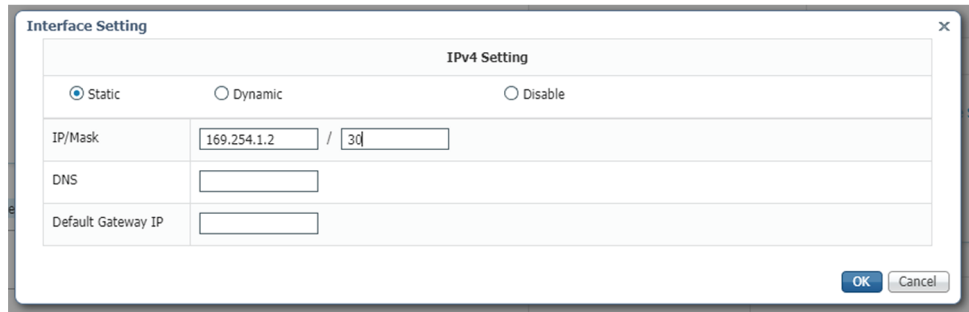
Name	Network Config
eth0	VPG1
eth1	Not Configured

eth1  [Interface Setting](#)

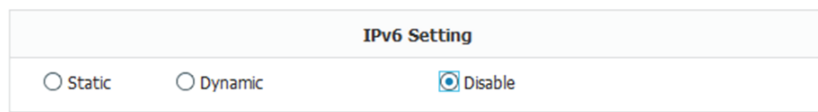
Description (optional):

- Click **Interface setting**.
- Apply the following configurations:
  - Set IPv4 as **Static**.
  - IP/Mask: 169.254.1.2 / 30





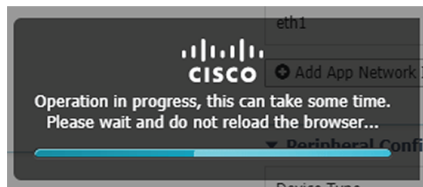
e) **Disable IPv6.**



f) Click **OK**, and click **OK** again when you're back to the Network Configuration menu to save the interface settings.

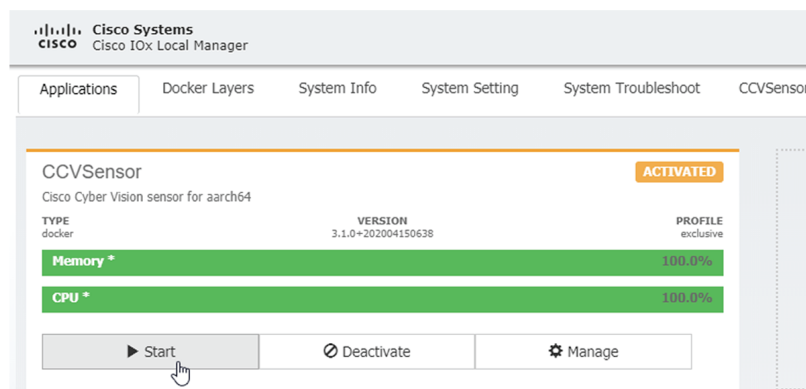
**Step 5** Click the **Activate App** button.

The operation takes several seconds.



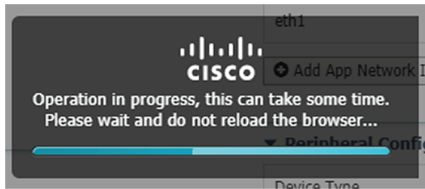
**Step 6** Go to the Applications menu to see the application's status.

The application is activated and needs to be started.

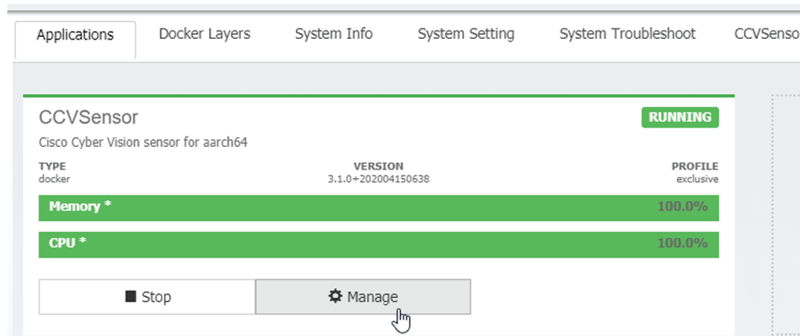


**Step 7** Click the **Start** button.

The operation takes several seconds.

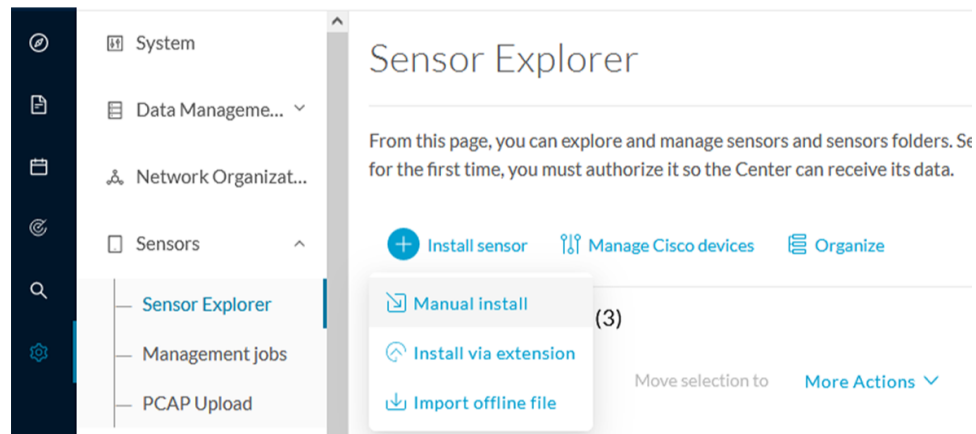


The applications' status changes to RUNNING.



## Generate the provisioning package

1. In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Manual install**.



The manual install wizard appears.

2. Select **Cisco IOx Application** and click **Next**.

3. Fill the fields to configure the sensor provisioning package:

- The serial number of the hardware.
- Center IP: leave blank.
- Gateway: add if necessary.
- Optionally, select a capture mode.
- Optionally, select RSPAN (only with Catalyst 9x00 and if using ERSPAN is not possible).

### Configure provisioning package

Please fill in the fields below to add configuration to the provisioning package to install.

#### Sensor Application

Serial number\*

Center collection IP

leave blank to use current collection IP

Gateway

#### Capture mode

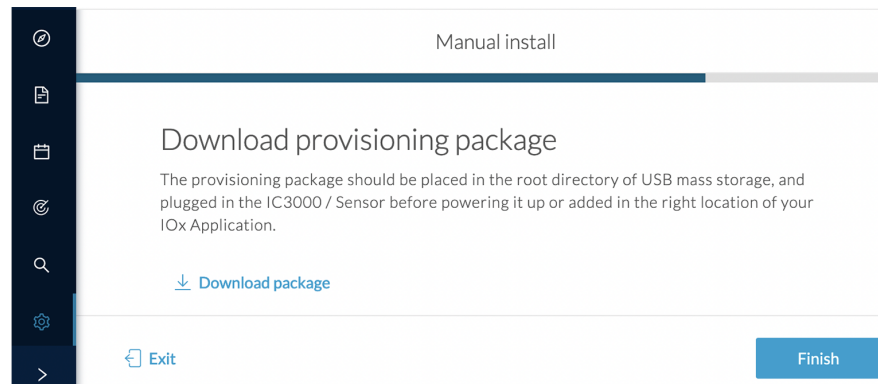
- Optimal (default): analyze the most relevant flows
- All: analyze all the flows
- Industrial only: analyze industrial flows
- Custom: set your filter using a packet filter in tcpdump-compatible syntax

#### Monitor session type

- ERSPAN: recommended choice for all devices
- RSPAN: use it only with Catalyst 9X00 and when using ERSPAN is not possible

4. Click **Create sensor**.

- Click the link to download the provisioning package.



This will download the provisioning package which is a zip archive file with the following name structure: sbs-sensor-config-<serialnumber>.zip (e.g. "sbs-sensor-configFCW23500HDC.zip").

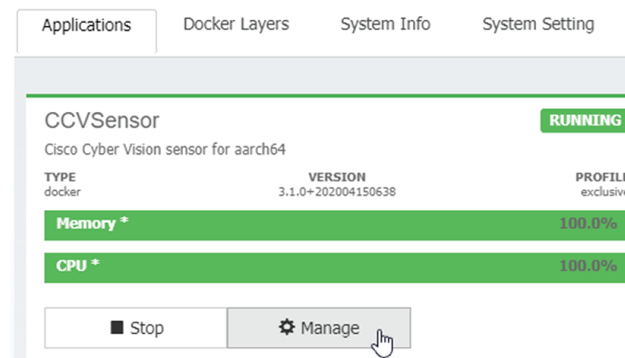
- Click **Finish**.
- A new entry for the sensor appears in the Sensor Explorer list.

The sensor status will switch from Disconnected to New.

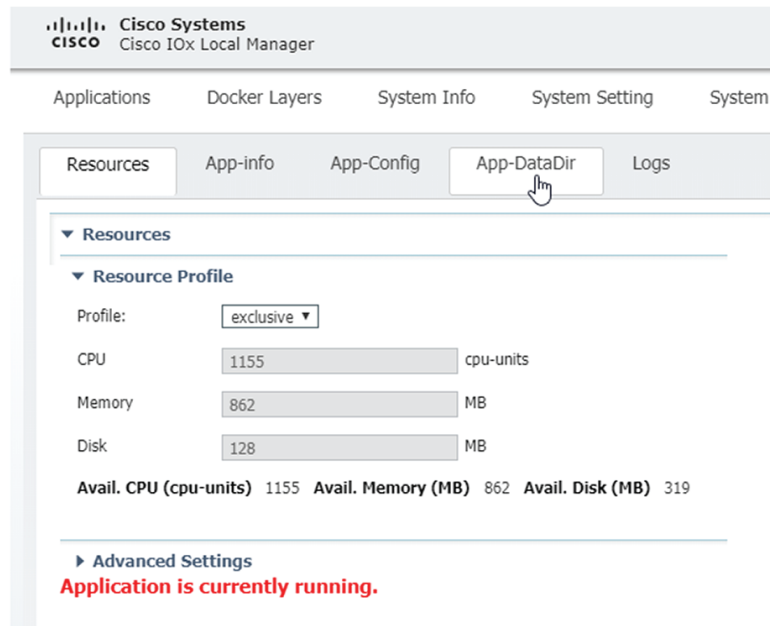
Filter	0 Selected	Move selection to	Delete folders	As of: Mar 20, 2024 10:57 AM	Refresh			
erial Number	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime	Templ
FOC27203WMJ				New	Not enrolled	Unavailable	N/A	Di

## Import the provisioning package

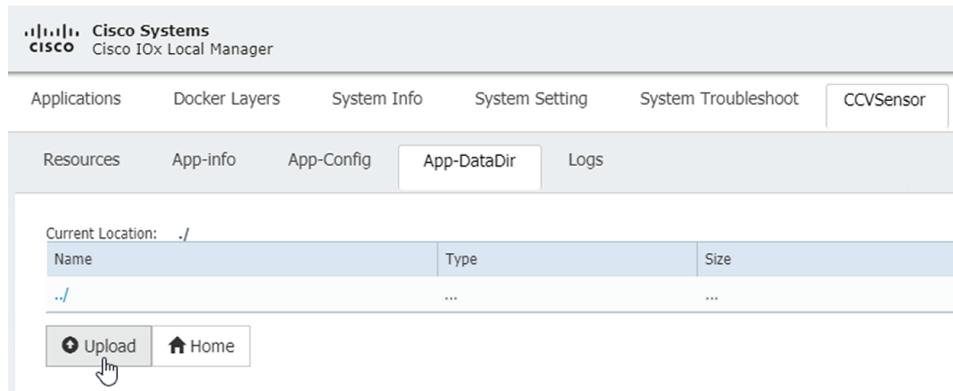
- In the Local Manager, in the IOx configuration menu, click **Manage**.



- Navigate to **App-DataDir**.

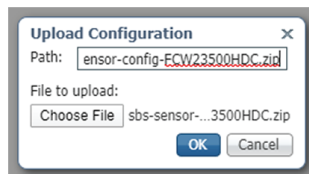


3. Click **Upload**.



4. Choose the provisioning package downloaded (i.e. "sbs-sensor-config-FCW23500HDC.zip"), and add the exact file name in the path field (i.e. "sbs-sensor-config-FCW23500HDC.zip").

5. Click **OK**.



6. After a few seconds, the sensor appears as Connected in Cisco Cyber Vision.

Import the provisioning package

---

<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	4 days
--------------------------	-------------	---------------	--------------------	-----------	--------------	---------	--------



## CHAPTER 9

# Procedure with the CLI

---

After the [Initial configuration](#), proceed to the steps described in this section.

- [Configure the sensor application, on page 37](#)
- [Install the sensor application, on page 38](#)
- [Copy the sensor application's provisioning package, on page 39](#)

## Configure the sensor application

### without SSD



---

**Note** In this section, "CCVSensor" is used as the appid.

---

#### Procedure

---

- Step 1** Connect to the Cisco IR1101 through SSH or a console.
- Step 2** Configure the application payload by typing the following commands:

```
enable
configure terminal
app-hosting appid CCVSensor
  app-vnic gateway0 virtualportgroup 1 guest-interface 0
    guest-ipaddress 169.254.0.2 netmask 255.255.255.252
  app-vnic gateway1 virtualportgroup 0 guest-interface 1
    guest-ipaddress 169.254.1.2 netmask 255.255.255.252
  app-default-gateway 169.254.0.1 guest-interface 0
  app-resource docker
    run-opts 1 "--tmpfs /tmp:rw,size=128m"
end
```

---

## with SSD



**Note** In this section, "CCVSensor" is used as the appid.

### Procedure

- Step 1** Connect to the Cisco IR1101 through SSH or a console.
- Step 2** Configure the application payload by typing the following commands:

```
enable
configure terminal
app-hosting appid CCVSensor
  app-vnic gateway0 virtualportgroup 1 guest-interface 0
    guest-ipaddress 169.254.0.2 netmask 255.255.255.252
  app-vnic gateway1 virtualportgroup 0 guest-interface 1
    guest-ipaddress 169.254.1.2 netmask 255.255.255.252
  app-default-gateway 169.254.0.1 guest-interface 0
  app-resource docker
  run-opts 1
end
```

## Install the sensor application

The sensor package needs to be collected from [cisco.com](http://cisco.com). The file has the following name structure:

CiscoCyberVision-IOx-aarch64-<version>.tar.

1. Copy the package to a USB key or in the flash memory.
2. Type the following command on the Cisco IR1101's CLI:

```
app-hosting install appid CCVSensor package
usbflash0:CiscoCyberVision-IOx-aarch64-4.1.0.tar
```

```
IR110CCV#
IR110CCV#app-hosting install appid CCVSensor package usbflash0:CiscoCyberVision-IOx-aarch64-3.1.0-RC4.tar
Installing package 'usbflash0:CiscoCyberVision-IOx-aarch64-3.1.0-RC4.tar' for 'CCVSensor'. Use 'show app-hosting list' f
or progress.
IR110CCV#
```



**Note** Adjust "usbflash0:" in accordance with the sensor package's localization (USB port or flash memory).



**Note** Replace "CiscoCyberVision-IOx-aarch64-4.1.0.tar" with the right filename.

3. Check that the application is in DEPLOYED state:



```
show app-hosting list
```

```
IR110CCV#
IR110CCV#show app-hosting list
App id                               State
-----
CCVSensor                            DEPLOYED
IR110CCV#
```

4. Activate the application using the following command:

```
app-hosting activate appid CCVSensor
```

```
IR110CCV#
IR110CCV#app-hosting activate appid CCVSensor
CCVSensor activated successfully
Current state is: ACTIVATED
IR110CCV#
```

5. Start the application using the following command:

```
app-hosting start appid CCVSensor
```

```
IR110CCV#
IR110CCV#app-hosting start appid CCVSensor
CCVSensor started successfully
Current state is: RUNNING
IR110CCV#
```

## Copy the sensor application's provisioning package

- Copy the provisioning package from the USB key to the application by typing the following command:

```
app-hosting data appid CCVSensor copy usbflash0:sbs-sensor-config-<serialnumber>.zip
sbs-sensor-config-<serialnumber>.zip
```

```
IR110CCV#
IR110CCV#$ data appid CCVSensor copy usbflash0:sbs-sensor-config-FCW23500HDC.zip sbs-sensor-config-FCW23500HDC.zip
Successfully copied file /usbflash0/sbs-sensor-config-FCW23500HDC.zip to CCVSensor as sbs-sensor-config-FCW23500HDC.zip
IR110CCV#
```

The sensor will appear as Connected in Cisco Cyber Vision's Sensor Explorer page.

<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	4 days
--------------------------	-------------	---------------	--------------------	-----------	--------------	---------	--------

Copy the sensor application's provisioning package



# CHAPTER 10

## Configuration

- [Configure Active Discovery, on page 41](#)
- [Configure sensor configuration template, on page 43](#)
- [Set a capture mode, on page 48](#)

## Configure Active Discovery

Once the sensor is connected, you can change the Active Discovery's network interface so it uses the Collection network interface instead, and add several network interfaces for the sensor to perform Active Discovery on several subnetworks at the same time.

### Procedure

**Step 1** Click the sensor to configure and click the **Active Discovery** button on its right side panel.

Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely installed. For the first time, you must authorize it so the Center can receive its data.

[+ Install sensor](#) [Manage Cisco devices](#) [Organize](#)

Folders and sensors (3)

[Filter](#) 0 Selected [Move selection to](#) [More Actions](#)

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected

FCW2445P6X5

Label: FCW2445P6X5  
Serial Number: FCW2445P6X5  
IP address: 192.168.49.21  
Version: 4.1.0+202202151440  
System date: Feb 24, 2022 4:13:06 PM  
Deployment: Sensor Management Extension  
Active Discovery: Enabled  
Capture mode: All

System Health  
Status: Connected  
Processing status: Normally processing  
Uptime: a day

[Go to statistics](#)

[Start Recording](#)

[Move to](#)

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

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

The Active Discovery configuration appears with the interface currently set.

**Step 2** Select **Use collection interface** for the Active Discovery to use the Collection network interface.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

- Use collection interface
- [+ New network interface](#)

Network interfaces

- 192.168.49.21/24 VLAN#1 (collection interface)

[Configure](#) [Cancel](#)

To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

**Step 3** Add a new network interface by clicking the corresponding button.

**Step 4** Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number

**Step 5** Click **Add**.

ACTIVE DISCOVERY CONFIGURATION

[+ New network interface](#)

IP address\*

192.168.52.24

Prefix length\*

24

VLAN number\*

52

[Add](#) [Cancel](#)

[Configure](#) [Cancel](#)

You can add as many network interfaces as needed.

**Step 6** When you are done, click **Configure**.

A message saying that the configuration has been applied successfully appears.

---

# Configure sensor configuration template

## 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:

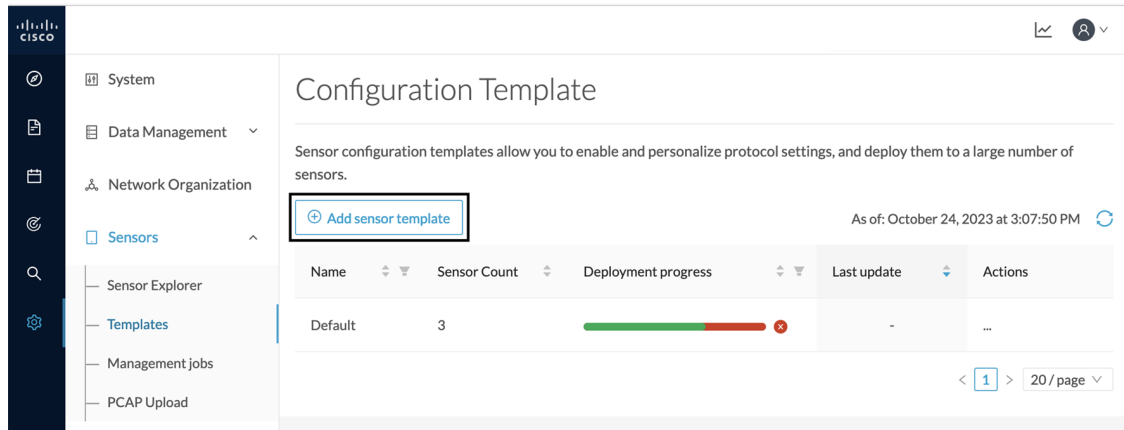
- if the sensor is disconnected,
- if there is connection issues,
- if the sensor version is too old.

## Create templates

### Procedure

---

- Step 1** In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.
- Step 2** Click **Add sensor template**.



The Create sensor template window pops up.

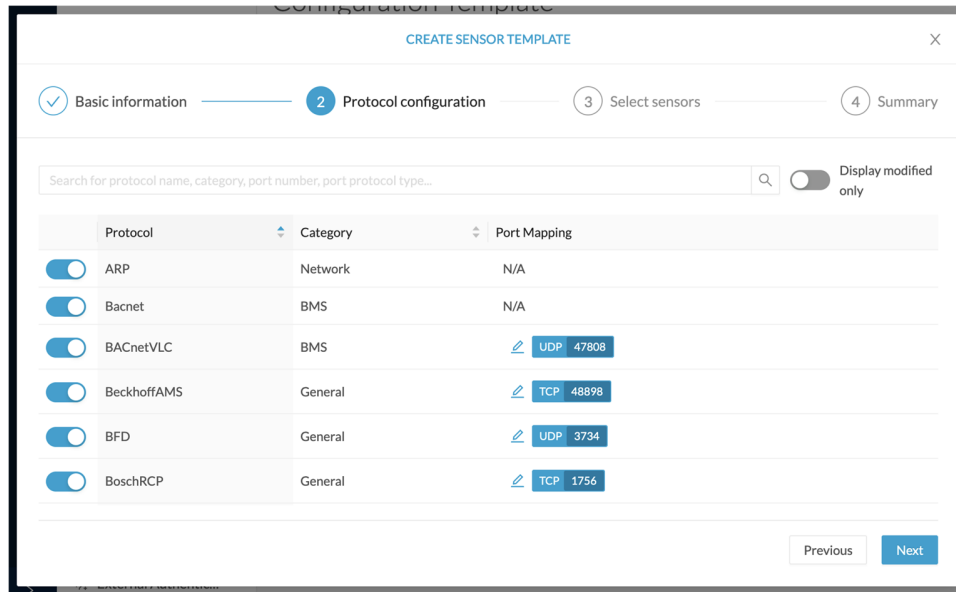
### Step 3

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

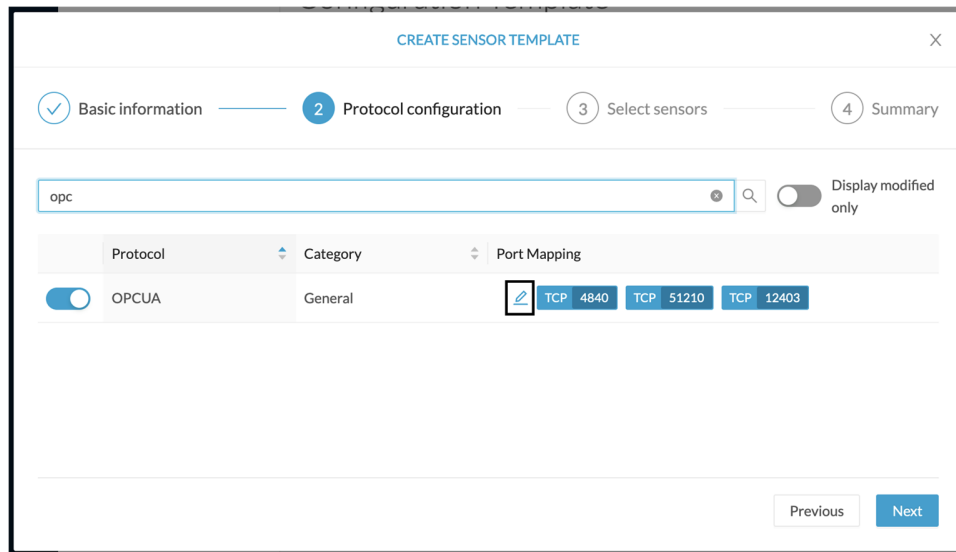
### Step 4

Click **Next**.

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

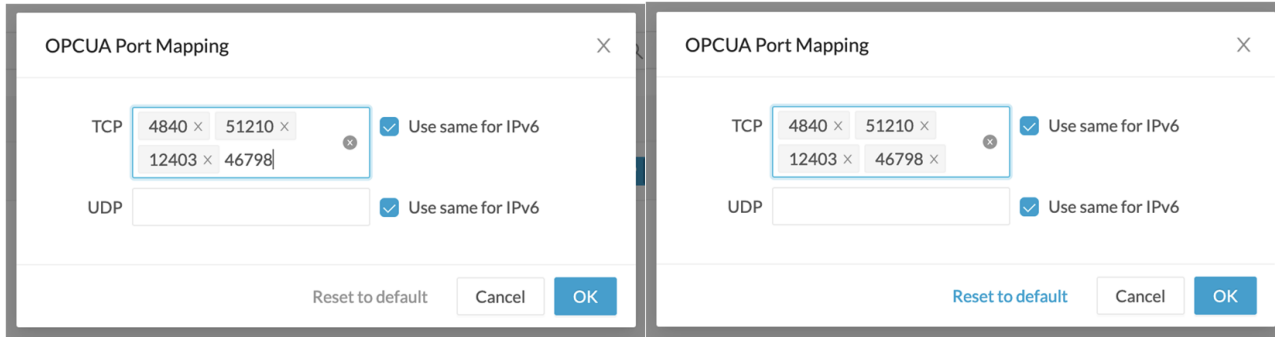


**Step 5** In the search bar, type the protocol you want to configure.  
 In our example, we will add a port to the OPCUA default settings.



**Step 6** Under the Port Mapping column, click the **pen** button to edit its settings.  
 The protocol's port mapping window pops up.

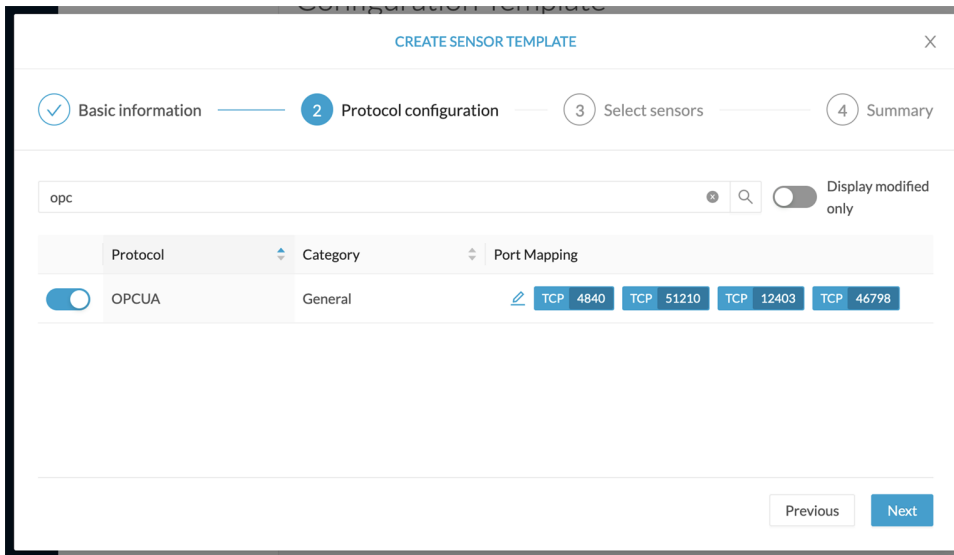
**Step 7** Write down the port number you want to add and hit enter.



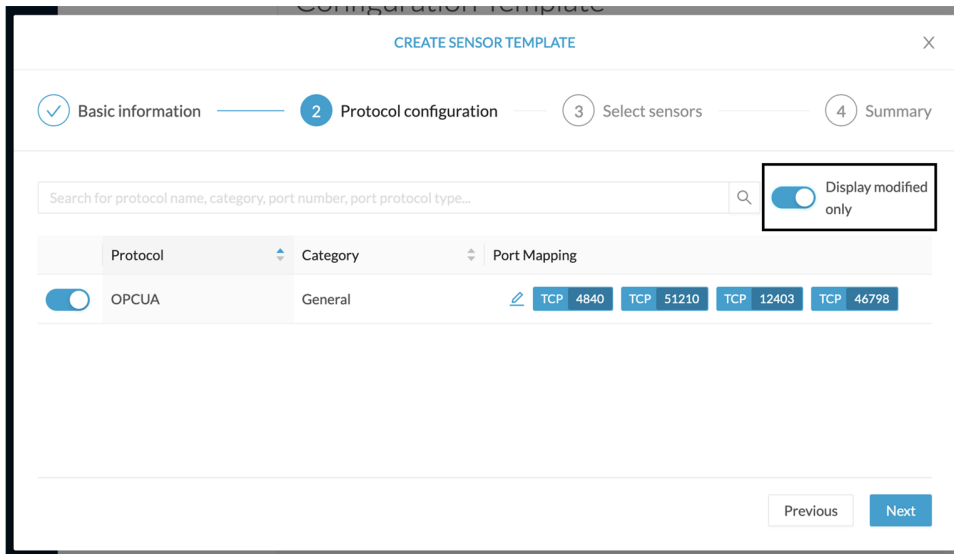
**Step 8**

Click **OK**.

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



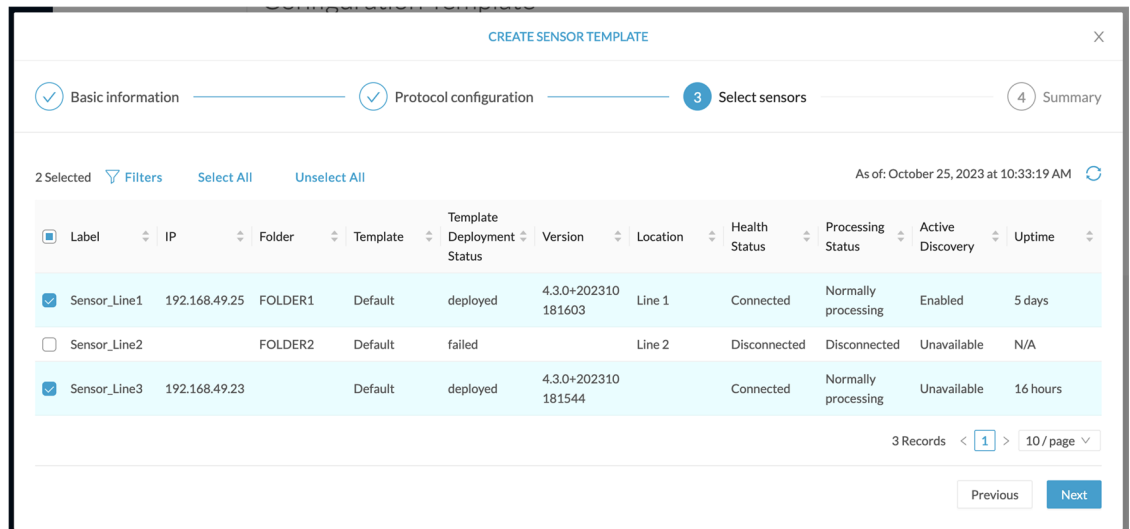
toggling ON the **Displayed modified only** button allows you to quickly find this protocol.





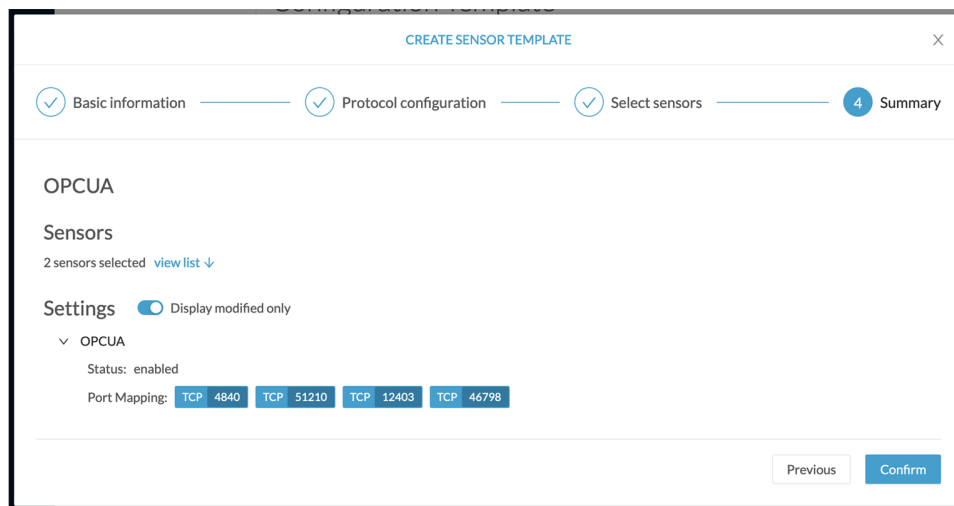
**Step 9** Click **Next**.

**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	<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

## 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 analyzed. 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](#)

<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](#)

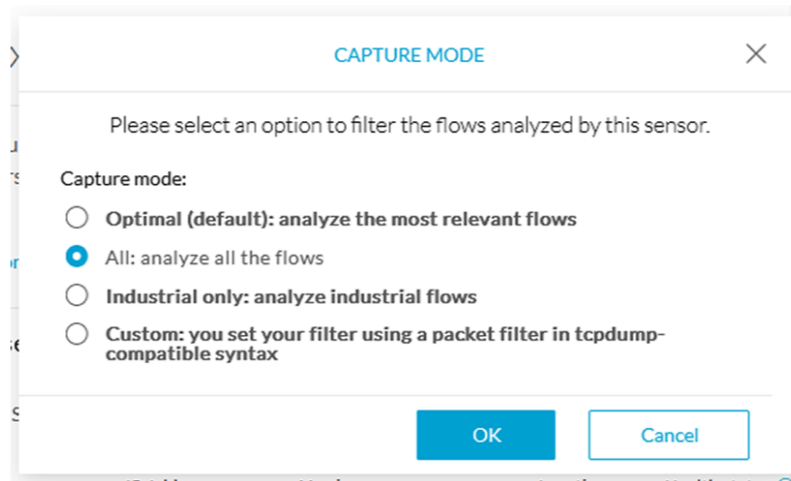
[Download package](#) [Capture mode](#)

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

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

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

*Capture modes:*



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.





## CHAPTER 11

# Maintenance

---

- [Upgrade procedures, on page 51](#)
- [Certificate renewal, on page 66](#)

## Upgrade procedures

### 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 displays the Cisco Cyber Vision interface, specifically the Sensor Explorer section. The left sidebar contains navigation options: Explore, Reports, Events, Monitor, Search, and Admin. The main content area is titled "Sensor Explorer" and includes a sub-menu with options like System, Data Management, Network Organization, Sensors, Templates, Management jobs, PCAP Upload, Active Discovery, and Users. The Sensors section is active, showing a table of "Folders and sensors (6)".

From this page, you can explore and manage sensors and sensors folders.

Install sensor Manage Cisco devices Organize

Filter 0 Selected Move selection to More Actions

Label	Serial Number	IP Address	Version	Status
FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	Update
FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	OK

A tooltip is visible over the "4.4.0" version of the first sensor, stating: "This device can be updated to version 4.4.0-202405232039".

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

### 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 ^

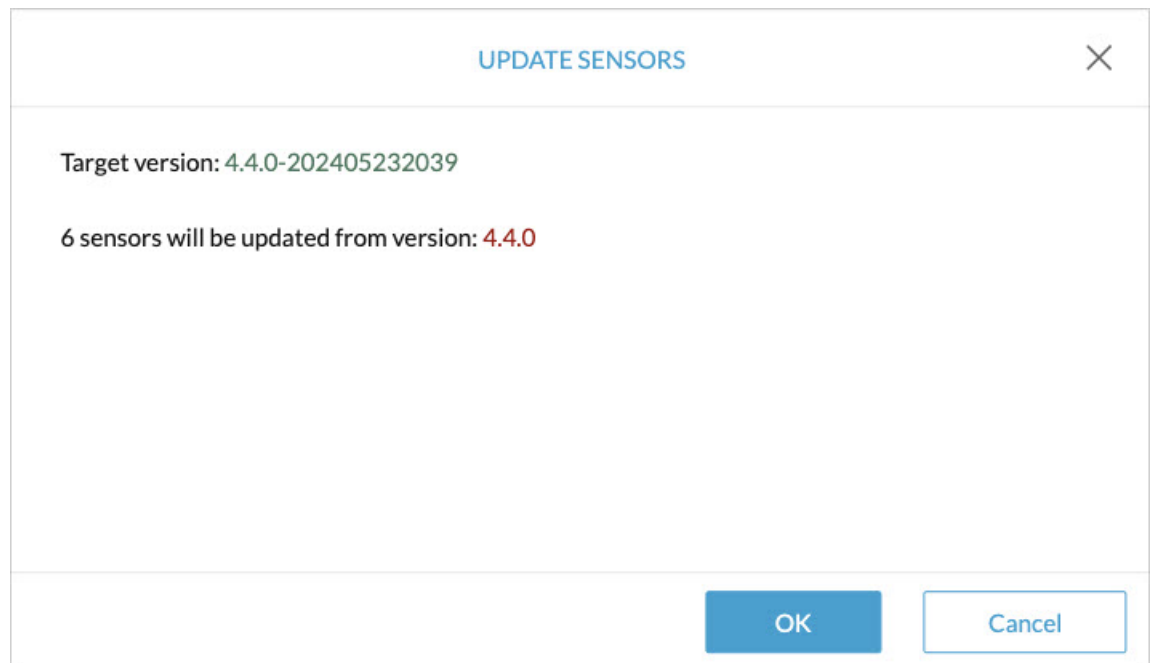
<input type="checkbox"/>	Label	Serial Number	IP Address	Version	Update status
<input checked="" type="checkbox"/>	FCH2309Y02K	FCH2309Y02K	192.168.49.37	4.4.0	
<input checked="" type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	
<input type="checkbox"/>	ie3400esc00	FCW2445P6X5	192.168.49.21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

More Actions ^

- 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.

	Label	Serial Number	IP Address	Version	Update status
<input type="checkbox"/>	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
<input type="checkbox"/>	FOC2716ZEMN	FOC2716ZEMN	192.168.49.101	4.4.0	Connected normally processing

## Upgrade through the Cisco Cyber Vision sensor management extension

Before updating sensors, the Cisco Cyber Vision sensor management extension must be up-to-date.

It is possible to select which sensors to update. The update status will be visible in the [Management jobs](#), on [page 18](#) page.

### Update the sensor management extension

The Cisco Cyber Vision sensor management extension must be up-to-date to update IOx sensors.

#### Procedure

- Step 1** Retrieve the sensor management extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) on [cisco.com](#).
- Step 2** In Cisco Cyber Vision, navigate to Admin > Extensions.
- Step 3** Click **Update** to browse the new version of the extension file.

**Extensions**

From this page, you can manage Cyber Vision Extensions. Extensions are optional add-ons to Cyber Vision Center which provide more features, such as the management of new device types, additional detection engines, or integrations with external services.

**Update**  
Uploading... Please do not quit or refresh the page.

**Installed extensions**

Name	Version	Actions
Cyber Vision sensor management	4.1.2	<input type="button" value="Update"/> <input type="button" value="Remove"/>

## Update the sensors

### Procedure

**Step 1** In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

Sensors that are not up-to-date have their version displayed in red.

**Step 2** Click **Install sensor**, then **Update Cisco devices**.

**Sensor Explorer**

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebo time, you must authorize it so the Center can receive its data.

Buttons: **Install sensor**, **Manage Cisco devices**, **Organize**, **Update Cisco devices**, **Manage credentials**

Filter: 0 Selected

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status
<input type="checkbox"/>	FOLDER1			Lyon	
<input type="checkbox"/>	FOLDER2			Paris	
<input type="checkbox"/>	IC3000	192.168.49.23	4.1.1+202205161124		Connected
<input type="checkbox"/>	IE3400	192.168.49.21	4.1.2+202207190948		Connected

The update Cisco devices window pops up listing all sensors that have been deployed with the sensor management extension.

**UPDATE CISCO DEVICES**

Only sensors deployed with the Sensor Management Extension (except IC3000) are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.

<input type="checkbox"/>	Label	IP	Version	Target
<input type="checkbox"/>	IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846

**Step 3** Select the sensors you want to update.

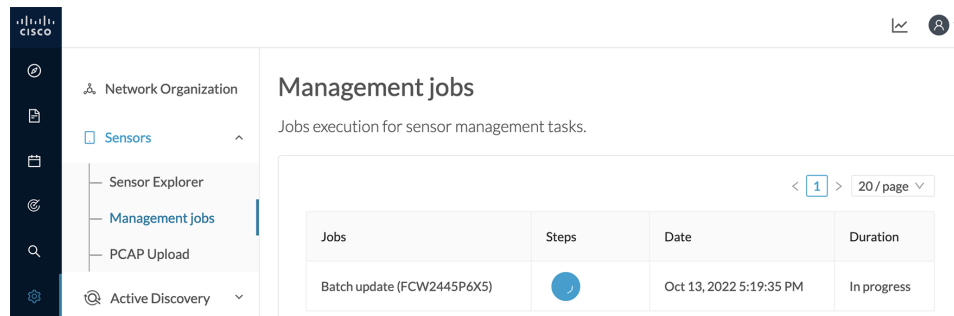
**UPDATE CISCO DEVICES**

Only sensors deployed with the Sensor Management Extension (except IC3000) are concerned here. They appear only if there is a new version of their application available in the currently installed extension. Please select the sensors to update.


<input checked="" type="checkbox"/>	Label	IP	Version	Target
<input checked="" type="checkbox"/>	IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846

**Step 4** Click **Update**.

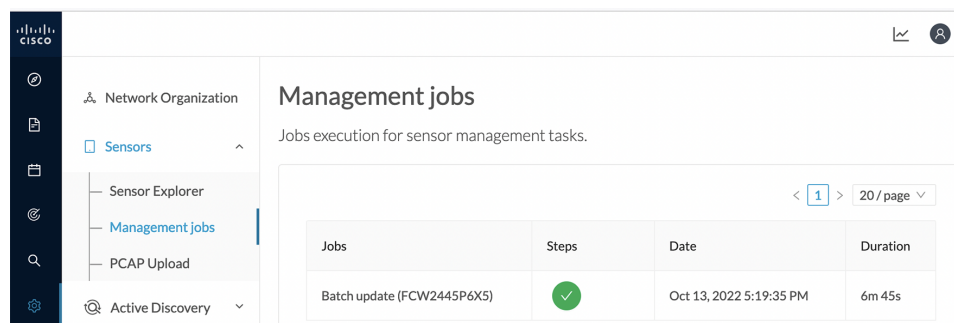
The sensors' update status appear in the Management jobs page in batches per sensor type and of maximum ten sensors per batch.




The screenshot shows the Cisco Management jobs page. The left sidebar contains navigation options: Network Organization, Sensors (expanded), Sensor Explorer, Management jobs (selected), PCAP Upload, and Active Discovery. The main content area is titled "Management jobs" and includes the subtitle "Jobs execution for sensor management tasks." Below this is a table with a pagination control showing page 1 of 20. The table has four columns: Jobs, Steps, Date, and Duration. A single row is visible, representing a batch update for FCW2445P6X5, which is currently in progress, indicated by a blue circular arrow icon in the Steps column.

Jobs	Steps	Date	Duration
Batch update (FCW2445P6X5)		Oct 13, 2022 5:19:35 PM	In progress

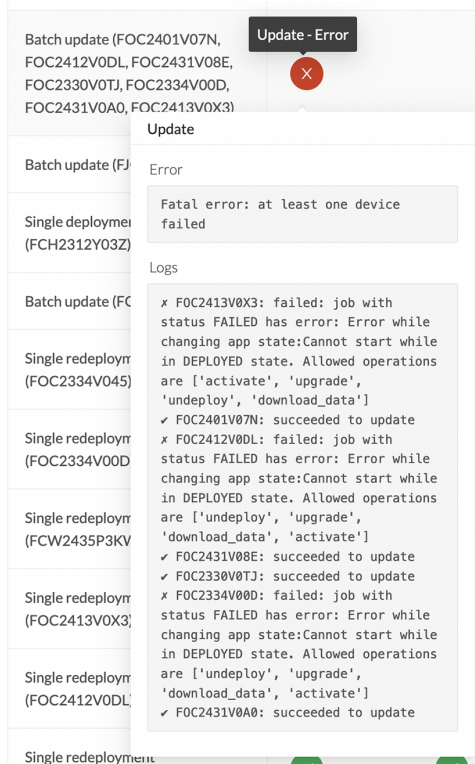
Herebelow the management jobs indicate that the batch of sensors updated successfully.



The screenshot shows the Cisco Management jobs page with the same navigation sidebar. The main content area is titled "Management jobs" and includes the subtitle "Jobs execution for sensor management tasks." Below this is a table with a pagination control showing page 1 of 20. The table has four columns: Jobs, Steps, Date, and Duration. A single row is visible, representing a batch update for FCW2445P6X5, which is now completed successfully, indicated by a green checkmark icon in the Steps column.

Jobs	Steps	Date	Duration
Batch update (FCW2445P6X5)		Oct 13, 2022 5:19:35 PM	6m 45s

If the batch update fails, click the red update error icon to see logs.

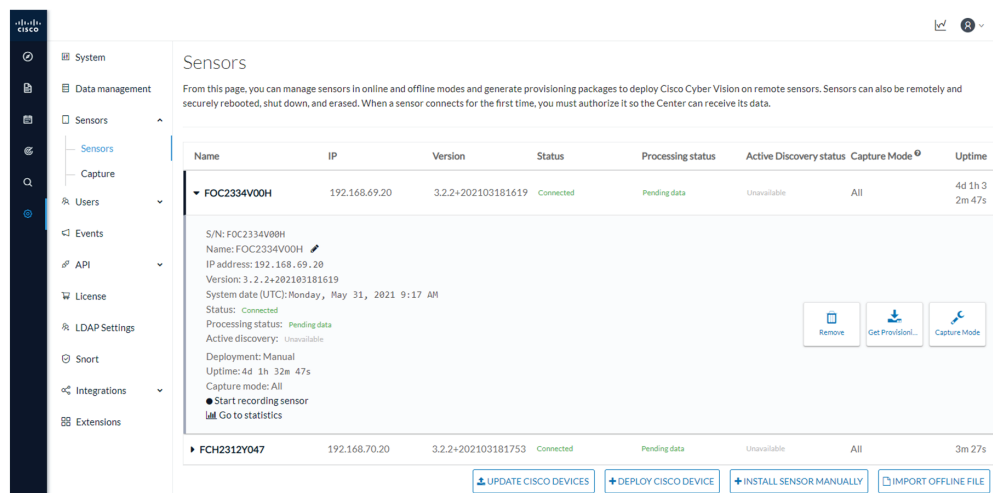


## Upgrade through the IOx Local Manager

The following section explains how to upgrade the sensor through the IOx Local Manager.

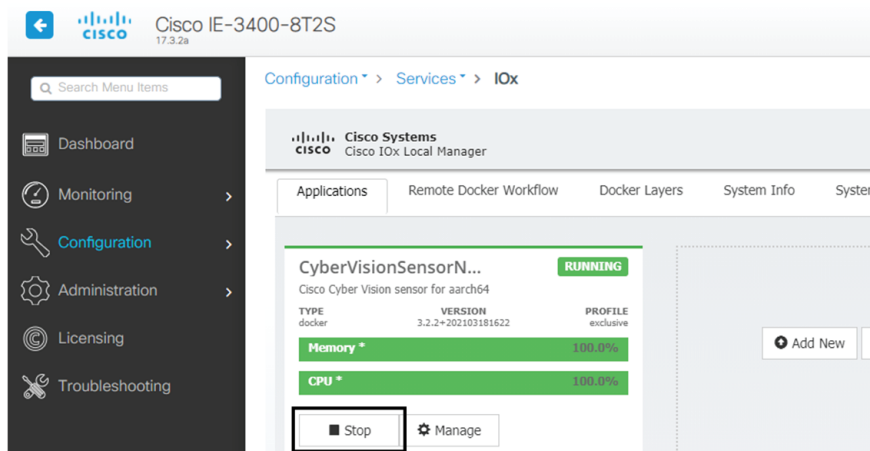
In the example below, the sensor is upgraded from Cisco Cyber Vision version 3.2.2 to version 3.2.3.

**Figure 2: The sensor in version 3.2.2 in the Sensors administration page of Cisco Cyber Vision**

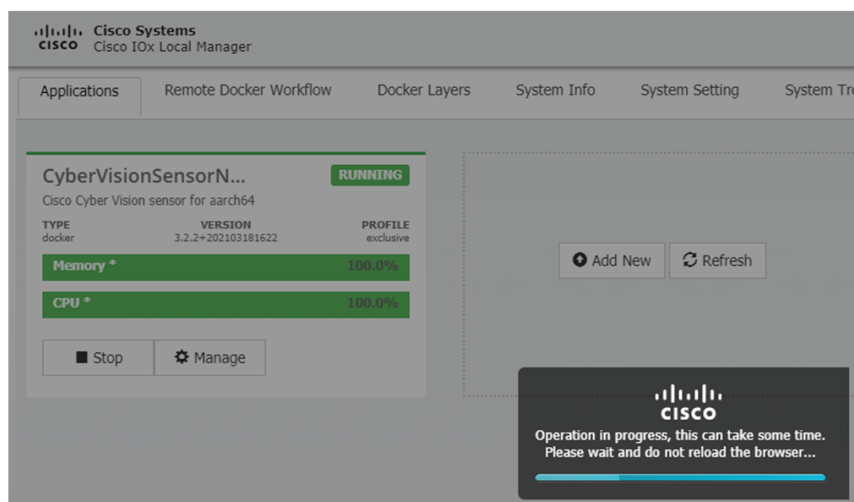




1. Access the IOx Local Manager.
2. Stop the application.



The operation takes a few moments.



The application status switches to STOPPED.

In Cisco Cyber Vision, the sensor status switches to Disconnected.

**Sensors**

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also 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.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.2+202103181619	Disconnected	Disconnected	Unavailable	All	N/A
<p>S/N: FOC2334V00H            Name: FOC2334V00H            IP address: 192.168.69.20            Version: 3.2.2+202103181619            System date (UTC): Monday, May 31, 2021 9:20 AM            Status: <b>Disconnected</b>            Processing status: Disconnected            Active discovery: Unavailable            Deployment: Manual            Capture mode: All            Go to statistics</p>							
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	10m

[UPDATE CISCO DEVICES](#)
[+DEPLOY CISCO DEVICE](#)
[+INSTALL SENSOR MANUALLY](#)
[IMPORT OFFLINE FILE](#)

3. In the IOx Local Manager, click the **Deactivate** button.

The application status moves to **DEPLOYED**.

4. Click **Upgrade**.

CyberVisionSensorN... **DEPLOYED**

Cisco Cyber Vision sensor for aarch64

TYPE	VERSION	PROFILE
docker	3.2.2+202103181622	exclusive

Memory \* 100.0%

CPU \* 100.0%

Activate
  Upgrade
  Delete

The pop up Upgrade application appears.

**Upgrade application**

Application Id: CyberVisionSensorNetwork

Select Application Archive: Choose File No file chosen

Preserve Application Data

OK Cancel

5. Select the **Preserve Application Data** option.

6. Select the new version of the application archive file.

e.g. CiscoCyberVision-IOx-aarch64-3.2.3.tar

**Upgrade application**

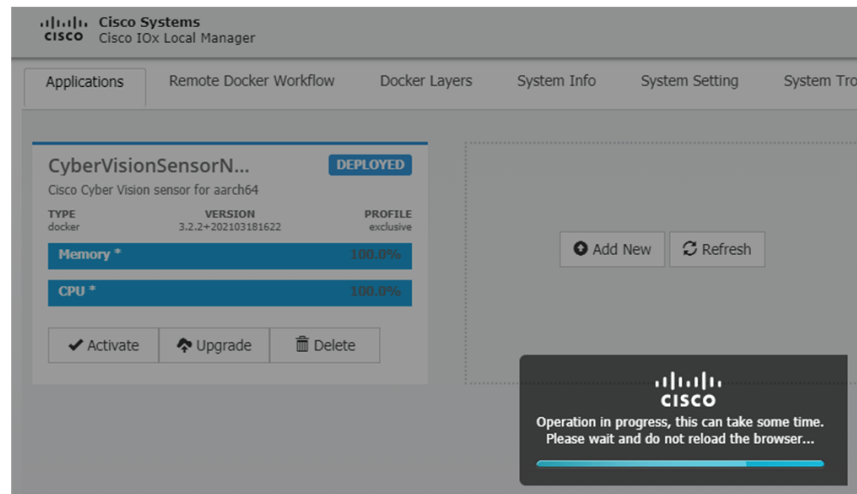
Application Id: CyberVisionSensorNetwork

Select Application Archive: Choose File CiscoCyber...h64-3.2.3.tar

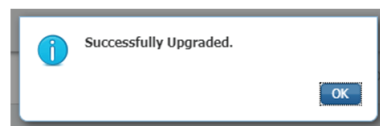
Preserve Application Data

OK Cancel

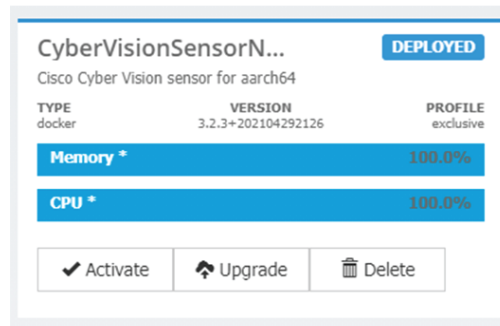
The operation takes a few moments.



A message indicating that the sensor has been successfully upgraded is displayed.



7. Check the number of the new version.
8. Click **Activate**.



9. Check configurations.
10. Click the **Activate App** button.  
The application status moves to **ACTIVATED**.
11. Click the **Start** button.  
The application status changes to **RUNNING**.

In Cisco Cyber Vision, the sensor is upgraded from version 3.2.2 to 3.2.3 and its status moves to Connected.

**Sensors**

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also 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.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode <sup>6</sup>	Uptime
▼ FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data	Unavailable	All	4d 1h 49m
<p>S/N: FOC2334V00H            Name: FOC2334V00H            IP address: 192.168.69.20            Version: 3.2.3+202104292032            System date (UTC): Monday, May 31, 2021 9:33 AM            Status: Connected            Processing status: Pending data            Active discovery: Unavailable            Deployment: Manual            Uptime: 4d 1h 49m            Capture mode: All            ● Start recording sensor            📊 Go to statistics</p>							
▶ FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	19m 34s

## Certificate renewal

The certificates generated by Cisco Cyber Vision have a validity of two years.

Sensor certificates must be renewed manually. The procedure used differs whether the certificate is already expired or not and whether the sensor has been deployed using the sensor management extension.

- If the certificate is still valid, refer to [Sensor certificate renewal, on page 66](#).
- If the sensor was deployed with the sensor management extension, refer to [Sensor certificate renewal, on page 66](#).
- If the certificate is outdated, and was deployed manually, refer to [Sensor certificate renewal through the Local Manager, on page 70](#).

## Sensor certificate renewal

The following procedure applies to:

- Sensors deployed with the sensor management extension, whether the certificate expiration date is exceeded or not (i.e. the deployment method is indicated in the sensor's right side panel).

**Sensor Explorer**

From this page, you can explore and manage sensors and sensors folders. Sensors are automatically discovered. When a sensor connects for the first time, you must authorize it so that it can be managed.

⚠️ 2 sensor certificates expired

[+ Install sensor](#)
[🔧 Manage Cisco devices](#)
[📁 Organize](#)

**Folders and sensors (3)**

🔍 Filter 0 Selected Move selection to [More Actions](#) ▾

<input type="checkbox"/>	Label	IP Address	Version
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519

**FOC2330V0T0**

Label: FOC2330V0T0 [🔗](#)  
 Serial Number: FOC2330V0T0  
 IP address: 192.168.49.41  
 Version: 4.2.2+202306261519  
 System date: Jul 6, 2023 11:26:00 AM  
 Deployment: **Sensor Management Extension**  
 Active Discovery: Unavailable  
 Capture mode: All

**System Health**  
 Status: Connected  
 Processing status: Normally processing  
 Uptime: 18 hours

[📊 Go to statistics](#)  
[🔴 Start Recording](#)

[📁 Move to](#)

[🔧 Capture mode](#)
[🔄 Redeploy](#)

[⊖ Uninstall](#)

- In the case of sensors deployed manually, it only applies if the sensors certificate have not expired yet (i.e. the sensor certificate status is Expire Soon).

If sensors have been deployed manually and the certificate expiration date is exceeded, refer to [Sensor certificate renewal through the Local Manager, on page 70](#).

## Procedure

### Step 1

In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer or click the top banner alert to access the Sensor Explorer page directly.

System Issues  
Actions required

⊗ 2 sensors certificates expired.  
Please renew them in: [Sensor explorer](#)

Another alert is displayed.

The screenshot shows the Cisco Sensor Explorer interface. On the left is a navigation sidebar with options like System, Data Management, Network Organization, Sensors, Active Discovery, Users, Events, API, License, External Authentication, and Snort. The main content area is titled "Sensor Explorer" and includes a description: "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." A yellow alert banner at the top states "2 sensor certificates expired and 1 will expire soon" with a "Manage certificates" link. Below the alert are buttons for "Install sensor", "Manage Cisco devices", and "Organize". A section titled "Folders and sensors (3)" contains a table of sensors.

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Connected	Normally pro
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally pro
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally pro

**Step 2** Click **Manage certificates** in the alert or **Manage Cisco devices > Manage certificates**.

This screenshot shows the same Cisco Sensor Explorer interface as the previous one, but with a dropdown menu open over the "Manage Cisco devices" button. The dropdown menu contains three options: "Update Cisco devices", "Manage credentials", and "Manage certificates". The "Manage certificates" option is highlighted with a blue border. The rest of the interface, including the alert banner and the sensor table, remains visible in the background.

The **Manage sensors certificates** window opens.

MANAGE SENSORS CERTIFICATES

Select a sensor to renew its certificate.  
If a sensor cannot be selected, it means that its certificate cannot be renewed automatically.

Filter

Certificate status is Expired × Certificate status is Expiring Soon ×

	Sensor Label	IP	Certificate Status	Expiration Date
<input type="radio"/>	FCH2309Y01Z	192.168.49.23	Expired	Jul 2, 2023
<input type="radio"/>	FOC2330V0T0	192.168.49.41	Expired	Jul 2, 2023
<input checked="" type="radio"/>	FCW2445P6X5	192.168.49.21	Expiring Soon	Jul 14, 2023

Cancel Renew certificate

**Step 3** Select the sensor with the status Expiring Soon.

**Step 4** Click **Renew certificate**.

MANAGE SENSORS CERTIFICATES

Select a sensor to renew its certificate.  
If a sensor cannot be selected, it means that its certificate cannot be renewed automatically.

The certificate has been successfully renewed.

Filter

Certificate status is Expired × Certificate status is Expiring Soon ×

	Sensor Label	IP	Certificate Status	Expiration Date
<input type="radio"/>	FOC2330V0T0	192.168.49.41	Expired	Jul 2, 2023
<input type="radio"/>	FCH2309Y01Z	192.168.49.23	Expired	Jul 2, 2023
<input type="radio"/>	FCW2445P6X5	192.168.49.21	Valid	Sep 3, 2025

Cancel Renew certificate

The certificate is renewed and automatically sent to the sensor. Its status switches to Valid and the new expiration date appears.

## Sensor certificate renewal through the Local Manager

In case of certificate expiration, communication with the sensor is no longer possible if it was deployed manually (i.e. without the sensor management extension). In this case, the certificate is renewed by sending it to the sensor manually. As the certificate is part of the provisioning package, the action consists in generating the provisioning package and sending it to the sensor application through the Local Manager.

The screenshot displays the Cisco Sensor Explorer interface. At the top right, there is a red notification banner that says "System issues Action required". Below this, the main content area is split into two panels. The left panel, titled "Sensor Explorer", shows a notification: "1 sensor certificate expired". Below the notification are three buttons: "Install sensor", "Manage Cisco devices", and "Organize". A table titled "Folders and sensors (3)" lists three sensors with columns for Label, IP Address, and Version. The first sensor, FCH2309Y01Z, is highlighted. The right panel shows the details for the selected sensor, FCH2309Y01Z. It includes fields for Label, Serial Number, IP address, Version, and System date. The "Deployment" field is highlighted with a red box and contains the value "Manual". Other fields include Active Discovery (Disabled), Capture mode (All), System Health (Connected), Processing status (Normally processing), and Uptime (18 hours). At the bottom of the right panel, there are several action buttons: "Go to statistics", "Start Recording", "Move to", "Download package", "Capture mode", "Enable IDS", "Reboot", "Shutdown", and "Uninstall".

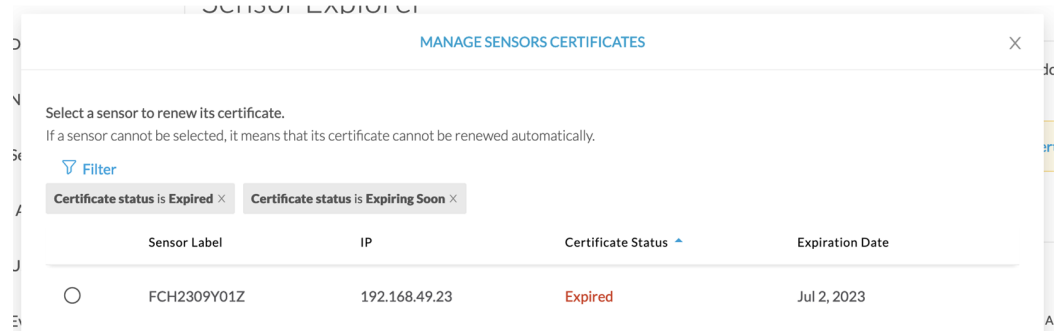
### Procedure

**Step 1** In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

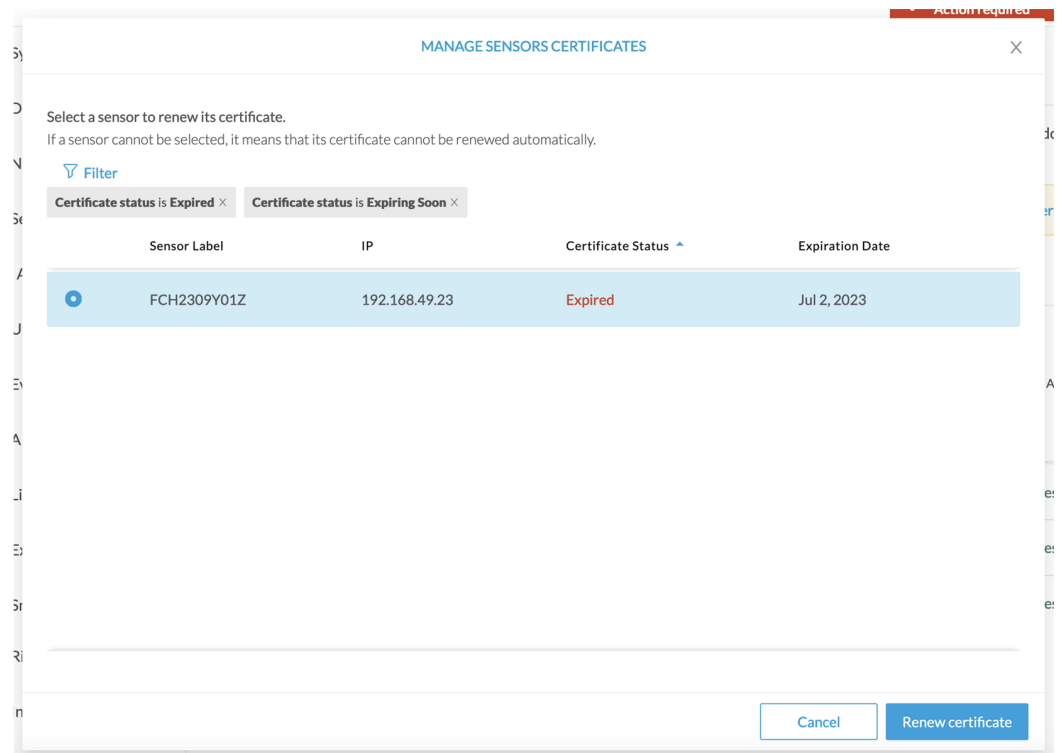
**Step 2** Click **Manage Certificates**.

The Manage sensors certificates window appears.

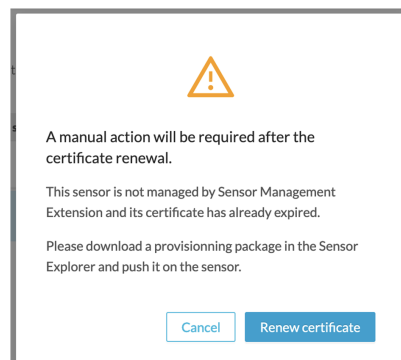




**Step 3** Select the sensor and click **Renew Certificate**.

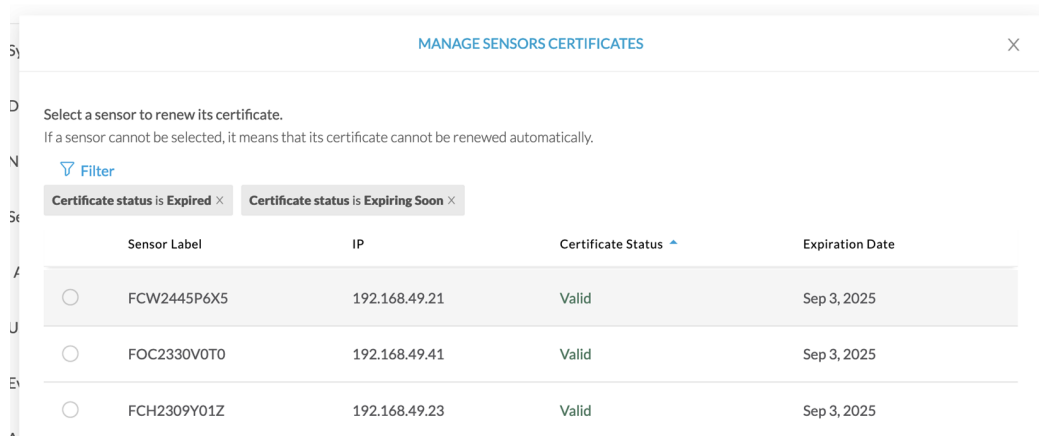


A message is displayed.



**Step 4** Click **Renew certificate** again.

The sensor certificate status appears as valid.



**Step 5** Close the Manage sensors certificates window.

The sensor's health and processing status appear as Disconnected.

## 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.

---

**Folders and sensors (3)**

0 Selected
Move selection to


As of: Jul 6, 2023 11:41 AM

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Di
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Disconnected	Disconnected	Disa
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally processing	Una
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally processing	Una

**Step 6** Click the sensor in the list.




Its right side panel opens.

**Step 7** Click the **Download package** button.





## Sensor Explorer


From this page, you can explore and manage sensors and sensors folders. Sensor erases. When a sensor connects for the first time, you must authorize it so the C

 Install sensor
 Manage Cisco devices
 Organize

### Folders and sensors (3)

 Filter
0 Selected
Move selection to
 More Actions

	Label	IP Address	Version	Lo
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711	
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519	
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519	

Label: FCH2309Y01Z 

Serial Number: FCH2309Y01Z

IP address: 192.168.49.23

Version: 4.2.2+202306261711

System date: Jul 6, 2023 11:36:49 AM

Deployment: Manual

Active Discovery: Disabled

Capture mode: All


**System Health**


Status: Disconnected


Processing status: Disconnected


Uptime: N/A


[Go to statistics](#)


 Move to

 Download package

 Reboot

 Uninstall

 Enable IDS

 Shutdown

**Step 8****Step 9**

Import the provisioning package in the Local Manager. To do so, refer to [Import the provisioning package, on page 34](#)

**Step 10**

The sensor's health status switches to Connected and its processing status to Normally processing.



## 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 (3)

Filter    0 Selected    Move selection to    [More Actions](#)    As of: Jul 6, 2023 11:56 AM   

<input type="checkbox"/>	Label	IP Address	Version	Location	Health status	Processing status	Active Di:
<input type="checkbox"/>	FCH2309Y01Z	192.168.49.23	4.2.2+202306261711		Connected	Normally processing	Disal
<input type="checkbox"/>	FCW2445P6X5	192.168.49.21	4.2.2+202306261519		Connected	Normally processing	Unav
<input type="checkbox"/>	FOC2330V0T0	192.168.49.41	4.2.2+202306261519		Connected	Normally processing	Unav



# CHAPTER 12

## Troubleshooting

- [Collect IOx sensor logs, on page 75](#)
- [Collect IOx sensor logs from the Local Manager, on page 76](#)

### Collect IOx sensor logs

In case of sensor issues Cisco Cyber Vision support can ask you to retrieve IOx sensor logs.

If the sensor is communicating with the Center, use the Cisco Cyber Vision GUI to generate the sensor diagnostic from the sensor statistics page.

The screenshot shows the Cisco Cyber Vision GUI interface. The main content area is titled 'System Statistics' with a dropdown menu set to 'Last 2 hours'. Below this, there's a 'Center' section showing the sensor 'FCH2309Y02K' as 'Connected'. A 'Generate diagnostic' button is present. The sensor details include: Serial Number: FCH2309Y02K, Uptime: 1 day 23 hours, IP address: 192.168.49.37, Version: 4.3.0+202311161552, Capture mode: All, and System date (UTC): Nov 22, 2023 11:01 AM. A 'System Health' section is partially visible at the bottom.

If the sensor is not communicating with the Center, you can collect the logs from the sensor command line. To do so:

#### Procedure

- Step 1** Connect to the sensor in ssh.
- Step 2** Use the following command to get the sensor application id:  

```
show app-hosting list
```

```
IE3400esc00#
IE3400esc00#
IE3400esc00#
IE3400esc00#show app-hosting list
App id                               State
-----
CVSensor                             RUNNING
IE3400esc00#
IE3400esc00#
IE3400esc00#
```

**Step 3** Use the following command to connect to the sensor application:

```
app-hosting connect appid <sensor-app-id> session
```

```
IE3400esc00#
IE3400esc00#
IE3400esc00#app-hosting connect appid CVSensor session
sh-5.0#
sh-5.0#
sh-5.0#
```

**Step 4** Use the following command and copy the results returned in a file to be sent to Cisco Cyber Vision support.

```
flowctl diagnostic
```

```
sh-5.0#
sh-5.0# flowctl diagnostic > iox_data/appdata/sensor-diag.log
sh-5.0#
sh-5.0#
sh-5.0#
```

## Collect IOx sensor logs from the Local Manager

In case of sensor issues Cisco Cyber Vision support can ask you to retrieve IOx sensor logs. You can retrieve them through the IOx Local Manager.

### Procedure

- Step 1** Access the sensor's IOx Local Manager.
- Step 2** Click the **System Troubleshoot** tab.
- Step 3** Click the **Generate snapshot file** button.

Configuration > Services > IOx

**Cisco Systems**  
Cisco IOx Local Manager

Hello, admin | Log Out | About

Applications
Remote Docker Workflow
Docker Layers
System Info
System Setting
System Troubleshoot
CVSensor

▼ Events Refresh

Device Uptime
36d:10:22:51

CAF Uptime
36d:10:21:08

System Time
2023-11-22 14:21:31 UTC

Events
Errors

Current CAF stats

Warning	Error	Critical	Events
...	...	...	14

Timestamp	#Record	Type	Message	Details
No data available in table				

Page Size 10






Go To #Record

▼ Logs Refresh

Logging Management
Select Log Type
All Logs

Log name	Timestamp	Log Size	Error	View
caf.log	Wed Nov 22 14:...	564034	0	<a href="#">download</a>
caf.log.1	Wed Nov 22 14:...	1039013	0	<a href="#">download</a>
caf.log.2	Wed Nov 22 13:...	1048528	0	<a href="#">download</a>
caf.log.3	Wed Nov 22 13:...	1048565	0	<a href="#">download</a>
caf.log.4	Wed Nov 22 13:...	1048304	0	<a href="#">download</a>

▼ TechSupport Information

Tech Support snapshot file name	File Size	Download	Delete
tech_support_2023-11-22_12.22.51.tar.gz	864159	<a href="#">download</a>	<a href="#">✖</a>

Generate snapshot file
Refresh

Core file name	File Size	Download	Delete

Refresh

Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR1101, Release 4.4.1

77

