Cisco Cyber Vision Network Sensor Installation Guide for Cisco IR8340, Release 4.1.2

First Published: 2022-08-25

Last Modified: 2022-08-25

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

© 2022–2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **About this documentation** 1

Document purpose 1

Warnings and notices 1

CHAPTER 2 **Overview** 3

CHAPTER 3 **Requirements** 5

CHAPTER 4 **Hardware front view** 7

Hardware front view 7

CHAPTER 5 **Initial configuration** 9

Check the software version 9

Check date and time 9

Enable IOx 10

Setup ERSPAN 11

Setup ERSPAN for routed ports 11

Setup ERSPAN for switched ports 12

Setup NAT 13

CHAPTER 6 **Procedure with the Cisco Cyber Vision sensor management extension** 15

Install the sensor management extension 15

Management jobs 16

IOx APP sensor creation 17

IOx APP sensor configuration 18

CHAPTER 7 **Procedure with the Local Manager** 23

Access the IOx Local Manager 23

Install the sensor virtual application 26

Configure the sensor virtual application 27

Generate the provisioning package 34

Import the provisioning package 37

CHAPTER 8 **Procedure with the CLI** 39

Configure the sensor application 39

without SSD 39

with SSD 40

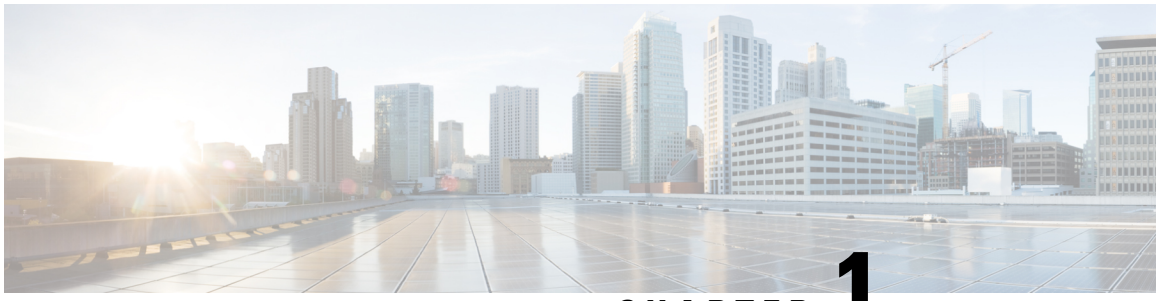
Install the sensor application 40

Copy the sensor application's provisioning package 41

CHAPTER 9 **Upgrade procedures** 43

Upgrade through the Cisco Cyber Vision sensor management extension 43

Upgrade through the IOx Local Manager 44



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 a Cisco IR8340 and how to upgrade a Cisco IR8340 sensor through different methods.

This documentation is applicable to **system version 4.1.0** or later.

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

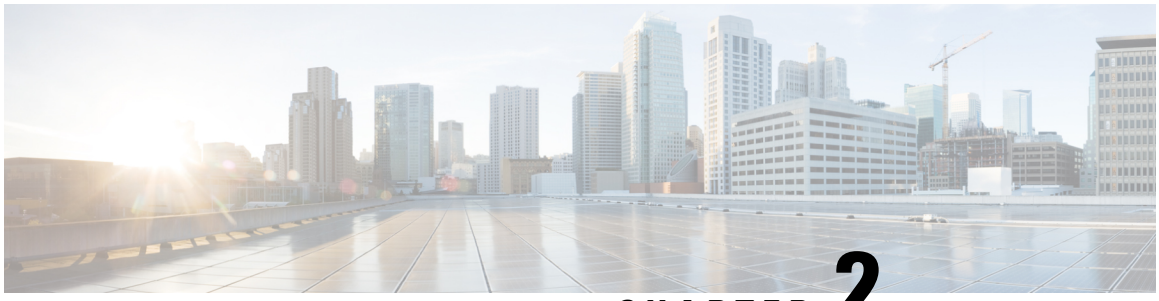
This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

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.

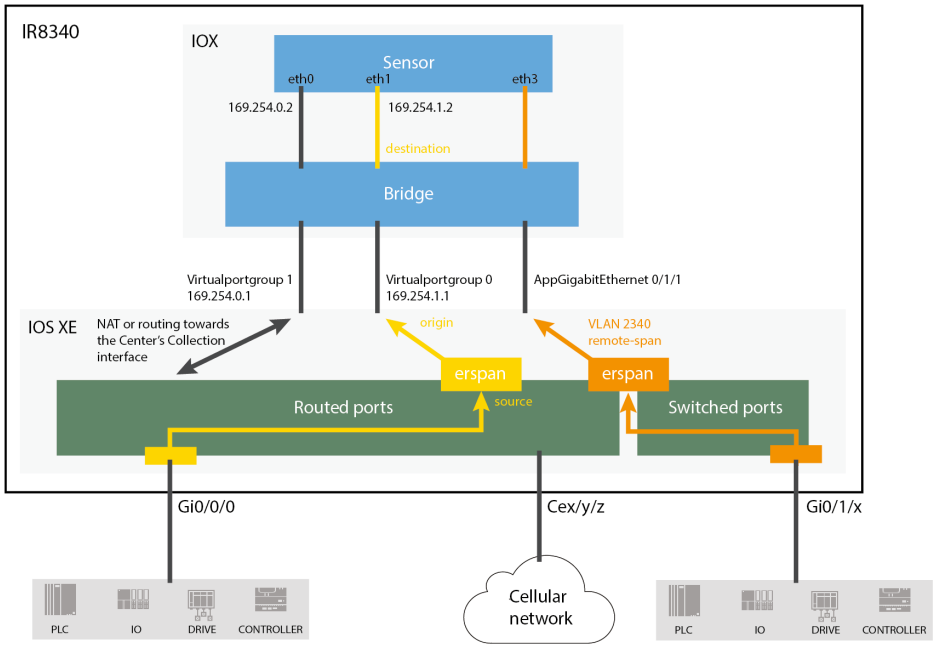
The schema below explains the architecture virtually deployed in the router to embed the sensor application. VLAN and physical ports configuration will allow OT traffic to be copied and communication with the Cisco Cyber Vision Center to be established.

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.

Overview

Figure 1: Cisco IR8340 Integrated Services Router Rugged:

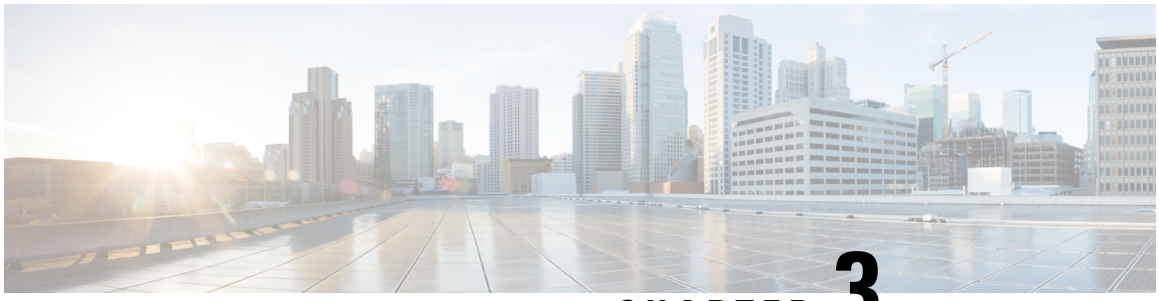


The sensor can be installed on the Cisco IR8340 with different disk configurations: on a SSD, or on the flash if there is no SSD.

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

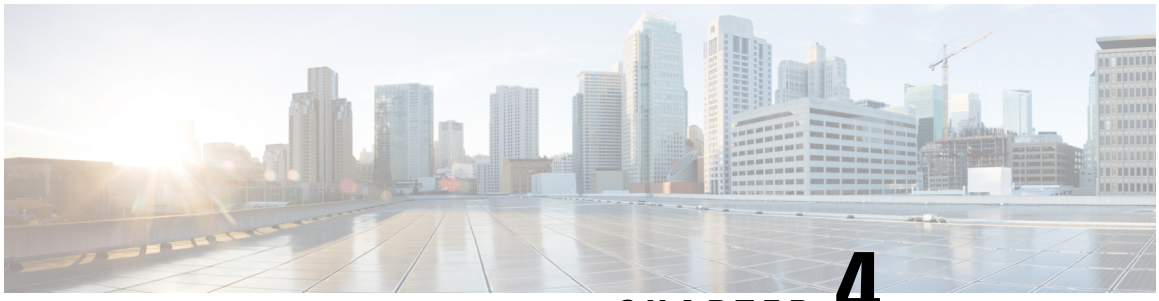
The Cisco IR8340 needs to be configured with access to the CLI (ssh or console port). An access to the IOx Local Manager could be necessary depending on the installation procedure chosen.

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-IOx-Active-Discovery-x86-64-<VERSION>.tar

Requirements



CHAPTER 4

Hardware front view

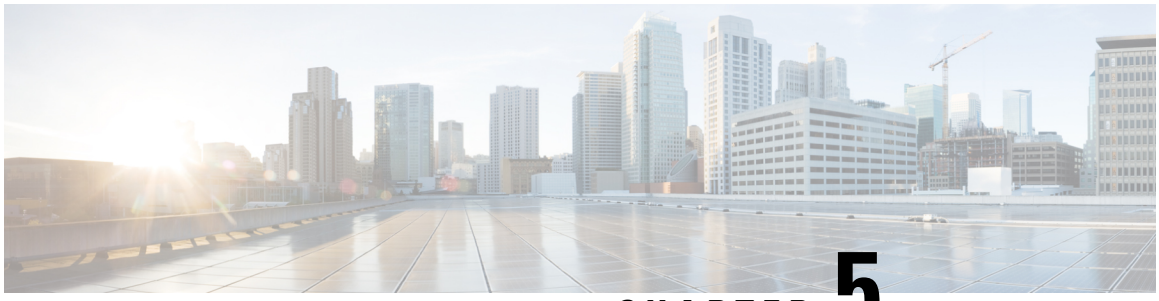
• Hardware front view, on page 7

Hardware front view

Cisco IR8340 Integrated Services Router Rugged:

For more information, refer to the Hardware Installation Guide available in cisco.com.

Hardware front view



CHAPTER 5

Initial configuration

To install Cisco Cyber Vision on the Cisco IR8340, you must perform the Initial configuration which steps are described in this section.

- Check the software version, on page 9
- Check date and time, on page 9
- Enable IOx, on page 10
- Setup ERSPAN, on page 11
- Setup NAT, on page 13

Check the software version

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

  ```
  Show version
  ```

  The displayed version must be 17.8.1 or higher to be compatible with the Cisco Cyber Vision Sensor Application.

  If the version is lower, you must update the router firmware. To do so, go to cisco.com and refer to the Cisco IR8340'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 IR8340 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:

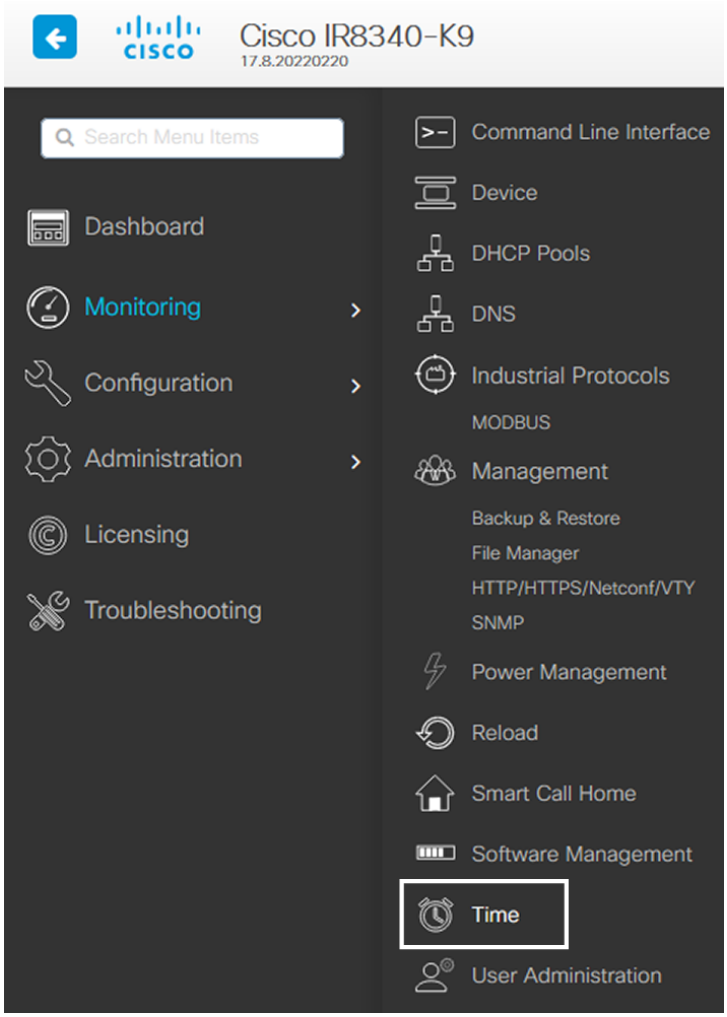
   ```
   Show clock
   ```

```
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 Monitoring > Time.



Enable IOx

Before installing the Cisco Cyber Vision sensor on the Cisco IR8340, 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
```

```
IR8340#
IR8340#
IR8340#sh iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

IR8340#
```

Setup ERSPAN

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

- must be connected to a VirtualPortGroup and the Appgigabit interface,
- must have the correct IP address assigned (do not use the same IP subnet for the VPG interface and the VLAN interface),
- must have one or two monitor sessions created:
  - one to capture traffic on routed ports,
  - and a different one to capture traffic on switched ports.

Setup ERSPAN for routed ports

Procedure

Step 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
```

Step 2 Create the monitor session using the following commands. The monitor session number must be 5 or higher.

```
monitor session 5 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
```

Setup ERSPAN for switched ports

Procedure

Step 1 Configure a VLAN for traffic mirroring using the following commands. The VLAN number must be between 2340 and 2349.

```
configure terminal
vlan 2340
exit
int vlan 2340
ip address 169.254.2.1 255.255.255.252
no shutdown
exit
```

Step 2 Configure the AppGigabitEthernet port which will enable the communication to the IOx virtual application.

```
interface AppGigabitEthernet 0/1/1
switchport mode trunk
exit
```

Step 3 Configure the SPAN session and add to the session the interfaces to monitor. The monitor session number must be between 1 and 4.

```
monitor session 1 type erspan-source
source interface Gi0/1/0 - 10 both
no shutdown
destination
erspan-id 2
mtu 9000
ip address 169.254.2.2
origin ip address 169.254.2.1
exit
exit
```

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
```

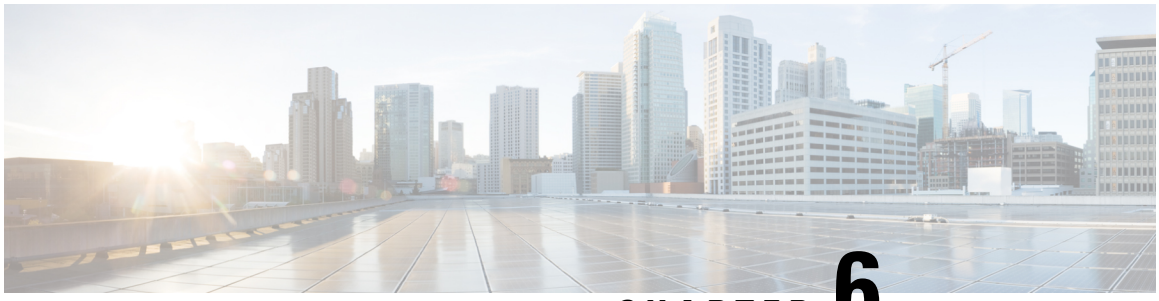
```
IR110CCV#
IR110CCV#write mem
Building configuration...

[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 15
- Procedure with the Local Manager, on page 23
- Procedure with the CLI, on page 39



CHAPTER 6

Procedure with the Cisco Cyber Vision sensor management extension

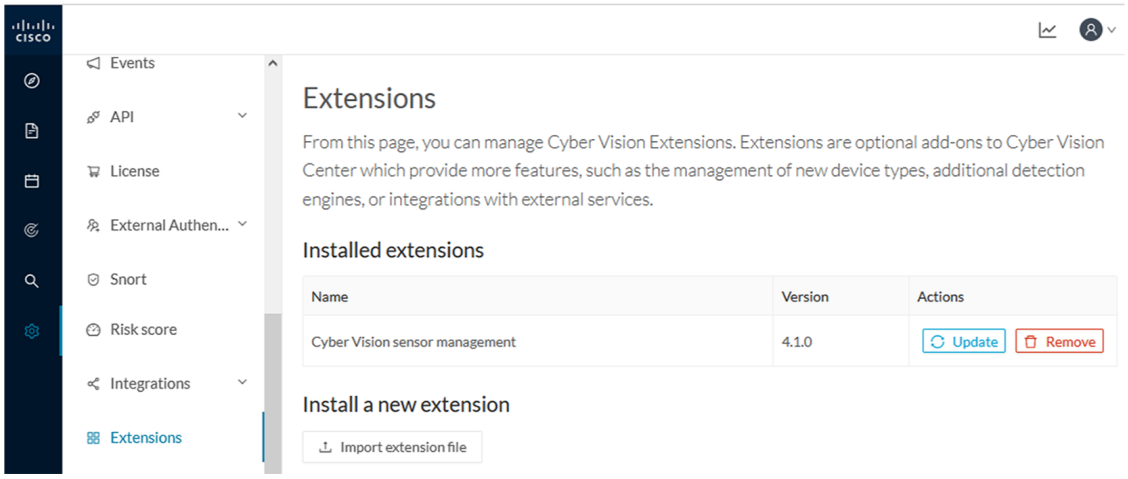
After the Initial configuration, proceed to the steps described in this section.

- Install the sensor management extension, on page 15
- IOx APP sensor creation, on page 17
- IOx APP sensor configuration, on page 18

Install the sensor management extension

To install the Sensor Management extension, you must:

1. Retrieve the extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) from cisco.com.
2. Access the Extension administration page in Cisco Cyber Vision.
3. Import the extension file.

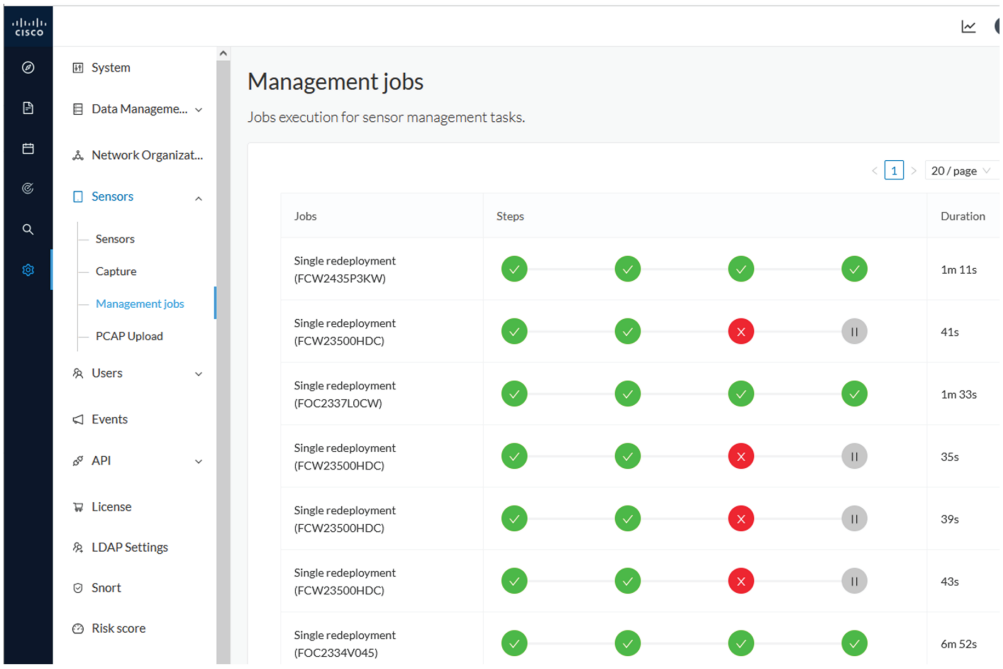


Once the sensor management extension is installed, you will find a new management job under the sensor administration menu (Management jobs), and the Install via extension button will be enabled in the Sensor Explorer page.

Management jobs

As some deployment tasks on sensors can take several minutes, this page shows the jobs execution status and advancement for each sensor deployed with the sensor management extension.

This page is only visible when the sensor management extension is installed in Cisco Cyber Vision.



You will find the following jobs:

- Single deployment

  This job is launched when clicking the Deploy Cisco device button in the sensor administration page, that is when a new IOx sensor is deployed.

- Single redeployment

  This job is launched when clicking the Reconfigure Redeploy button in the sensor administration page, that is when deploying on a sensor that has already been deployed. This option is used for example to change the sensor's parameters like enabling active discovery.

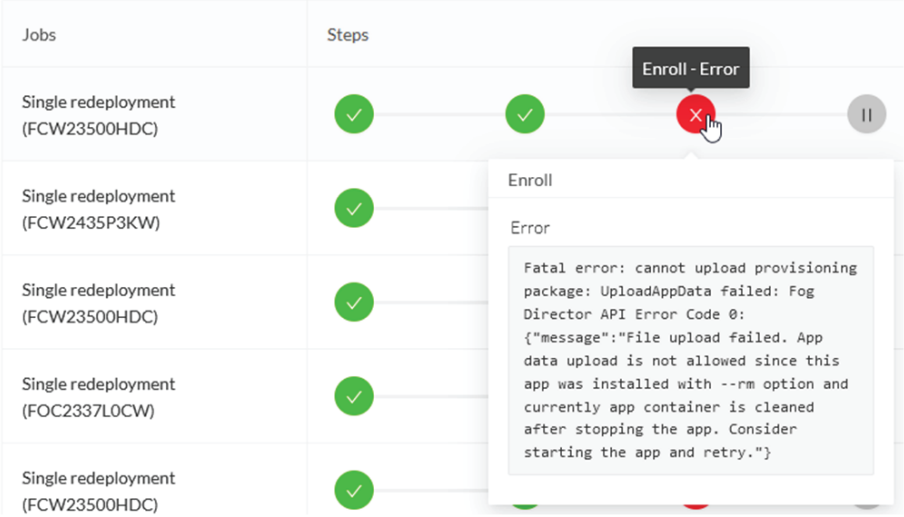
- Single removal

  This job is launched when clicking the Remove button from the sensor administration page.

- Update all devices

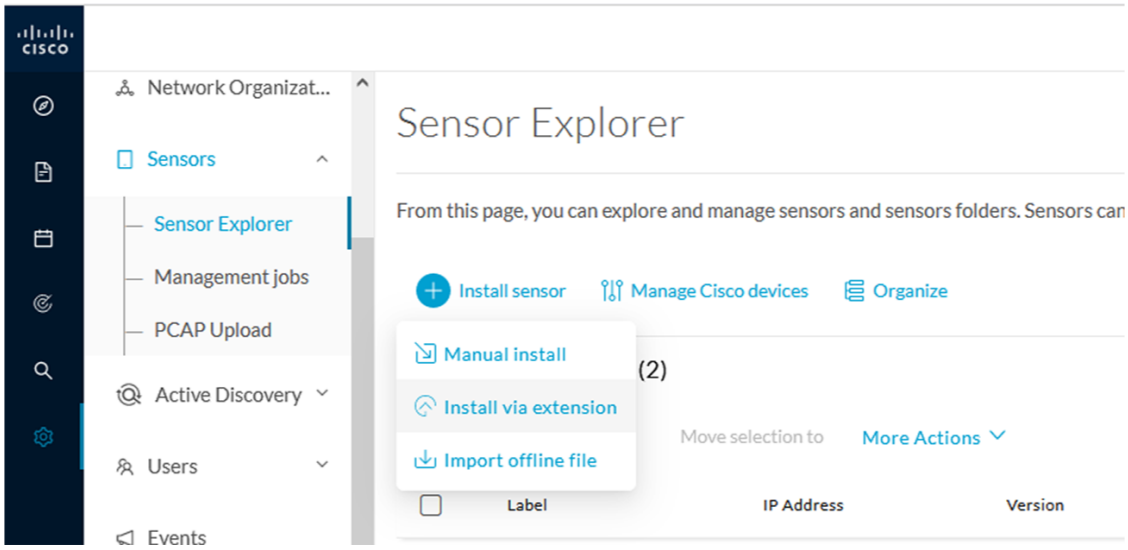
  This job is launched when clicking the Update Cisco devices button from the sensor administration page. A unique job is created for all managed sensors that are being updated.

If a job fails, you can click on the error icon to view detailed logs.

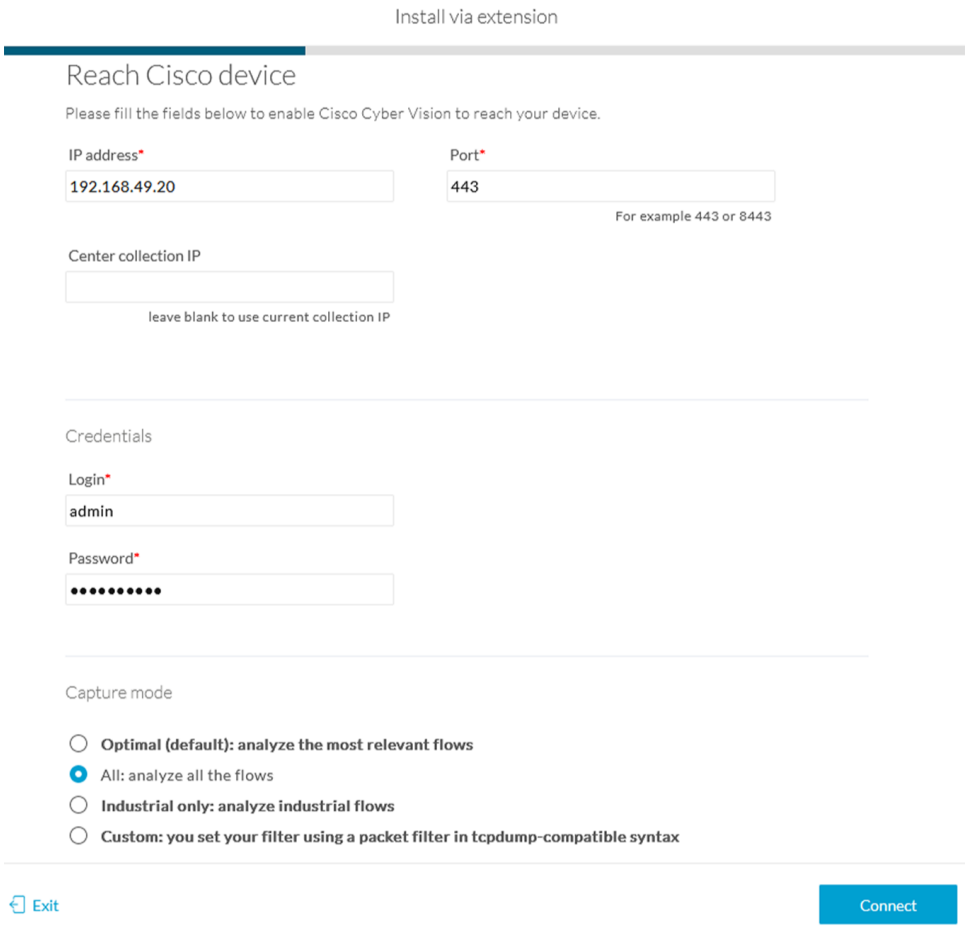


IOx APP sensor creation

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



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.

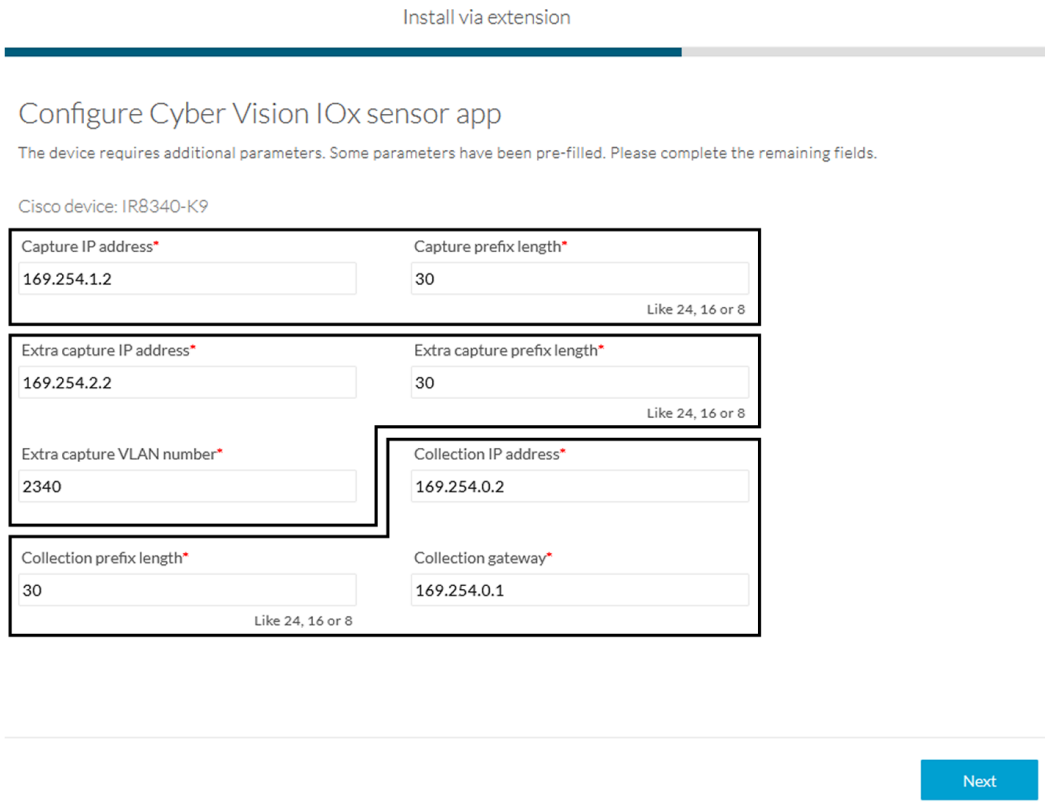


3. Click **Connect**.

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.

IOx APP sensor configuration

If the Center can join the device, the following form appears:



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

Procedure

Step 1 Fill the following parameters for the Collection interface:

a. Capture interface: traffic capture from routed ports

- Capture IP address: IP address destination of the monitor session in the sensor
- Capture prefix length: mask of the capture IP address

b. Extra capture interface: traffic capture from switched ports

- Extra capture IP address
- Extra capture prefix length
- Extra capture VLAN number

c. Collection interface: capture traffic to the Center

- Collection IP address: IP address of the sensor in the device
- Collection prefix length: mask of the Collection IP address
- Collection gateway: IP address of the interface VirtualPortGroup 1

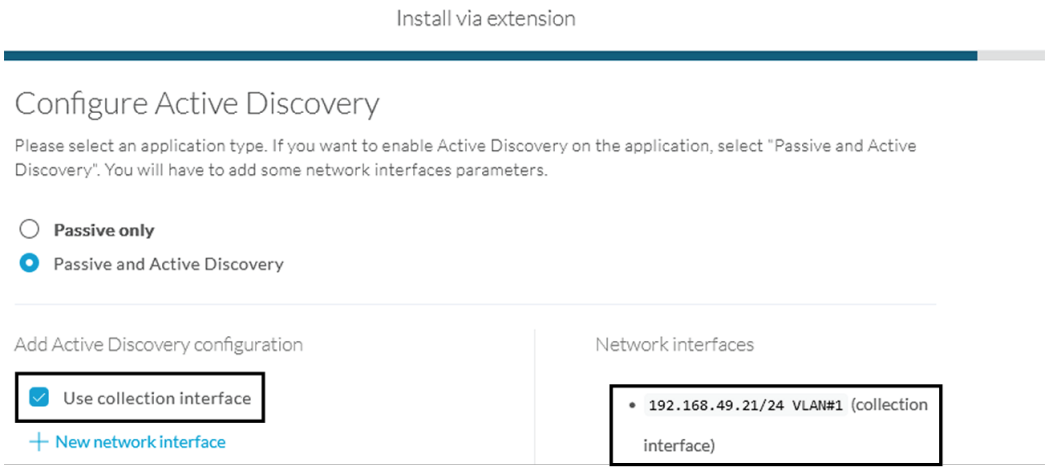
Step 2 Click **Next**.

Step 3 **Active Discovery:**

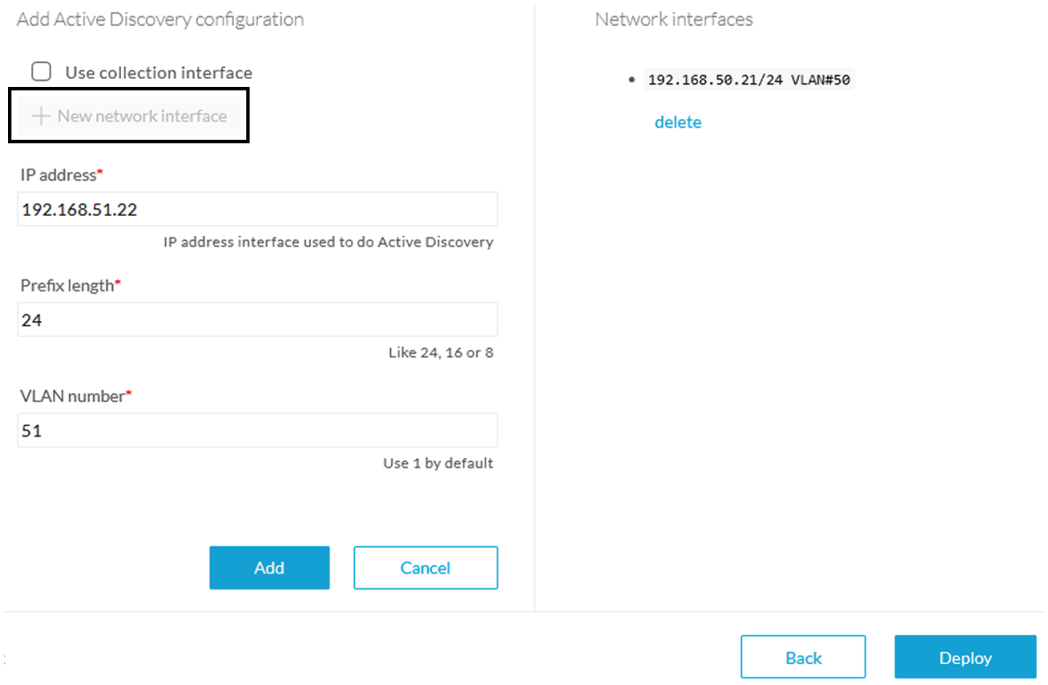
If you want to enable Active Discovery on the sensor, select **Passive and Active Discovery**.

You can:

- use the sensor Collection interface by selecting it:

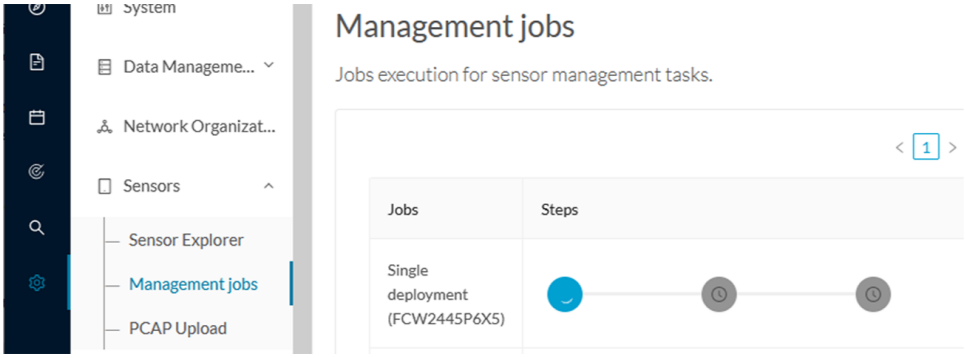


- add new network interfaces filling the following parameters to set dedicated network interfaces and clicking **Add**.
  - IP address
  - Prefix length
  - VLAN number



Step 4 Click **Deploy**.

The Center starts deploying the sensor application on the target equipment. This can take a few minutes. You can go to the Management jobs page to check the deployment advancements.

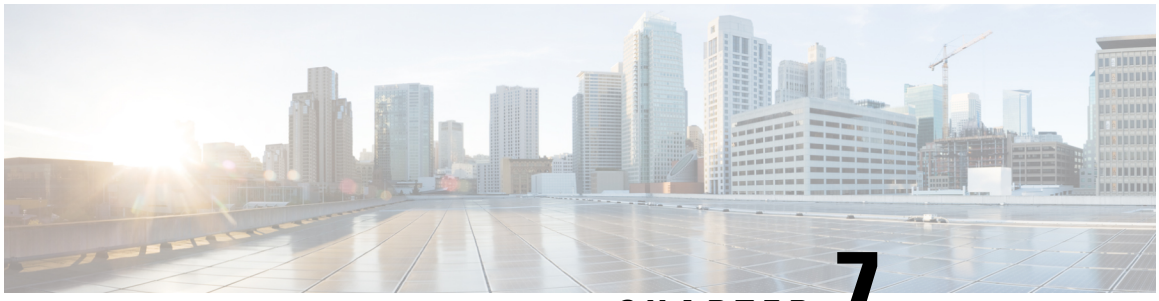


Once the deployment is finished, a new sensor appears in the sensors list of the Sensor Explorer page.

The sensor's status will eventually turn to Connected.

If the Active Discovery has been enabled and set -that is if the **Passive and Active Discovery** option was selected during the IOX App sensor configuration- the sensor is displayed as below with Active Discovery's status as Enabled.

	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
☐	[redacted]			[redacted]	[redacted]	[redacted]		[redacted]
☐	[redacted]			[redacted]				[redacted]
☐	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days



CHAPTER 7

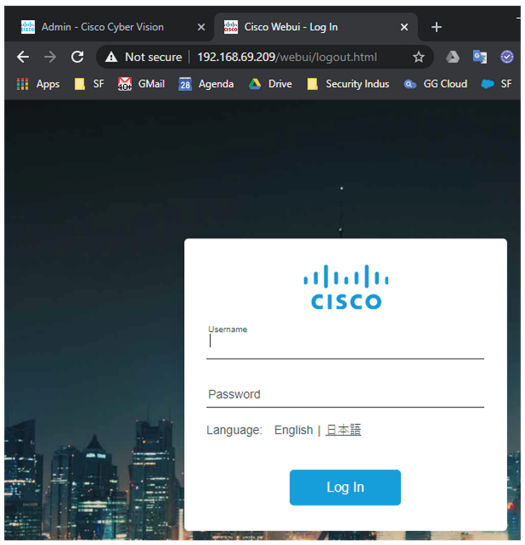
Procedure with the Local Manager

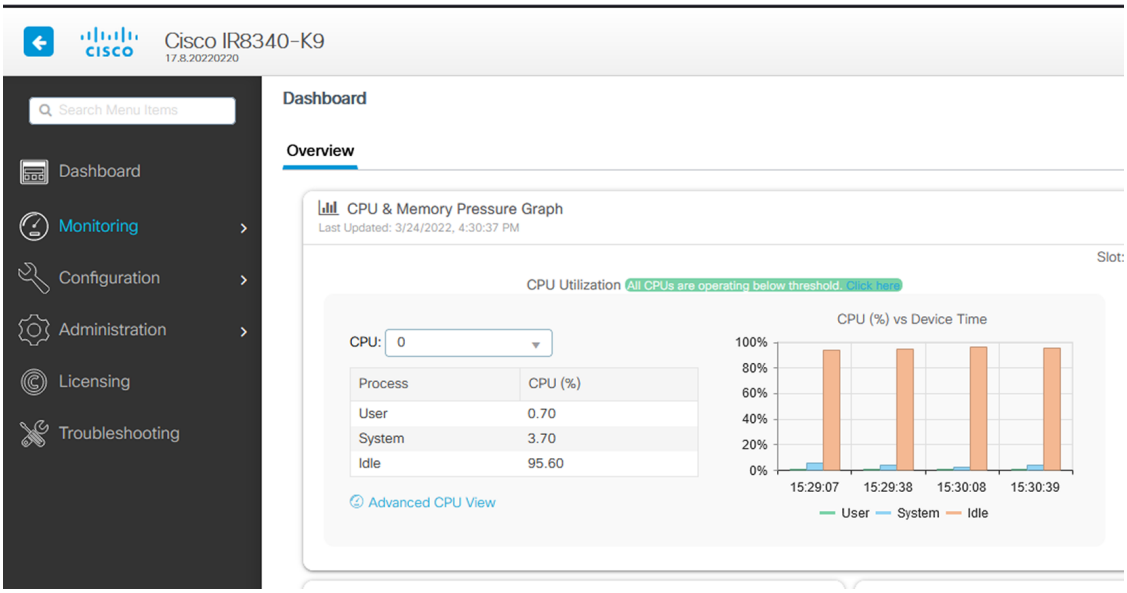
After the Initial configuration, proceed to the steps described in this section.

- Access the IOx Local Manager, on page 23
- Install the sensor virtual application, on page 26
- Configure the sensor virtual application, on page 27
- Generate the provisioning package, on page 34
- Import the provisioning package, on page 37

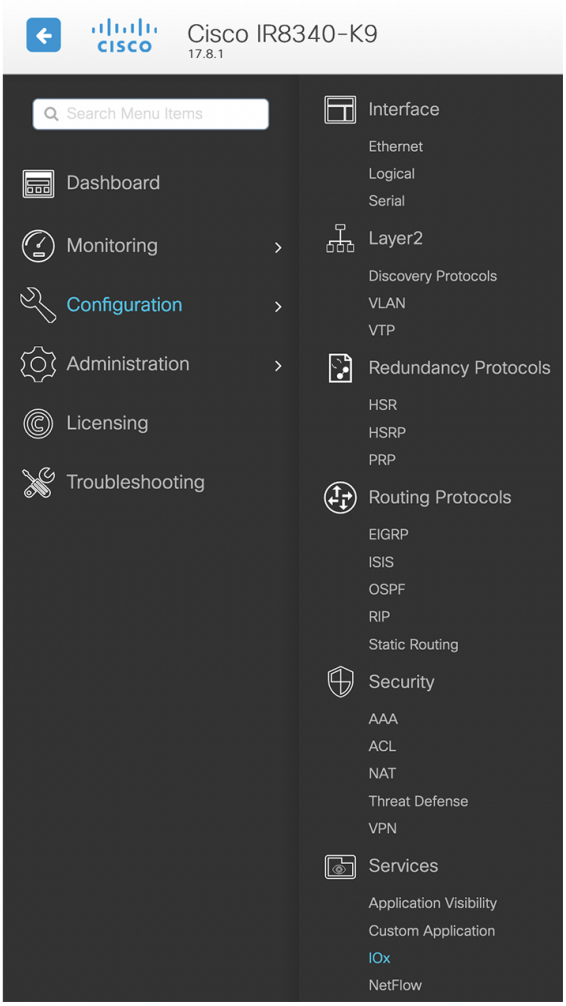
Access the IOx Local Manager

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 IR8340 admin user account and password.

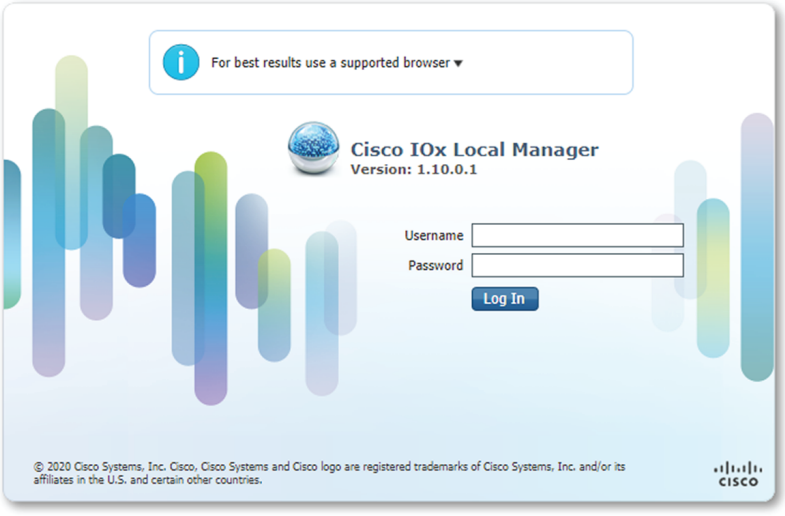




3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.

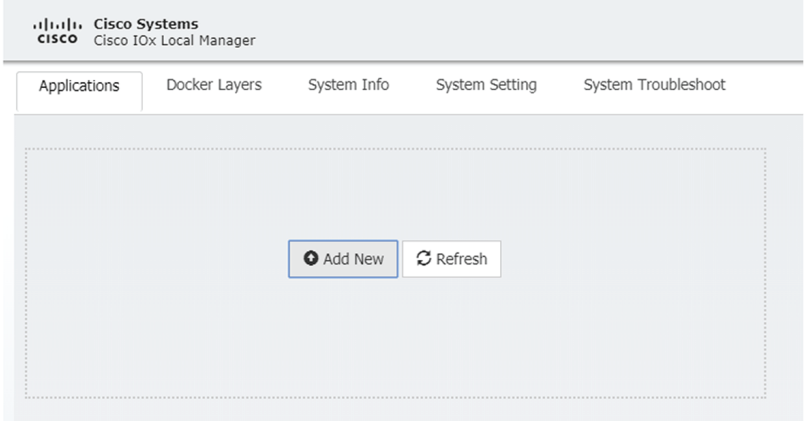


4. Log in using the user account and password.



Install the sensor virtual application

Once logged in, the following menu appears:

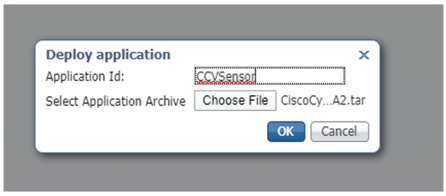


1. Click **Add New**.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file

   (i.e. "CiscoCyberVision-IOx-x86-64-<version>.tar").

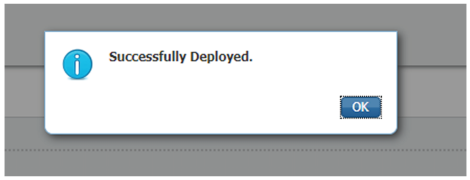
Note If you aim to install a sensor with **Active Discovery**, select the required application archive file

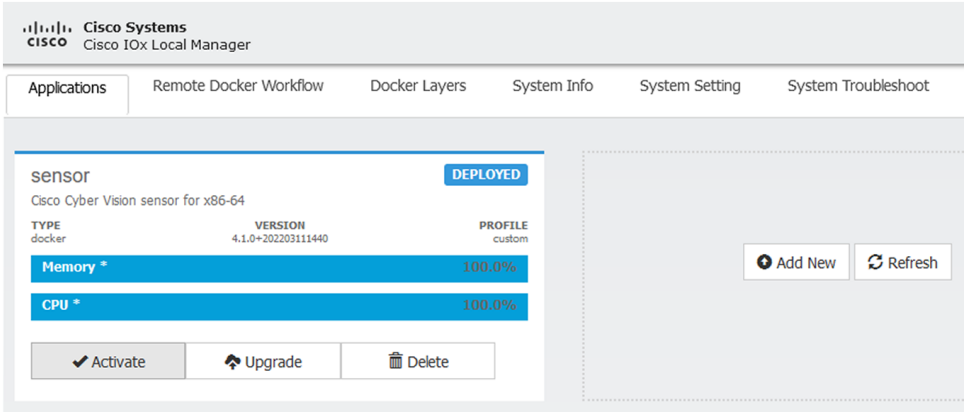
(i.e. "CiscoCyberVision-IOx-Active-Discovery-x86-64-<version>.tar").



The installation takes a few minutes.

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

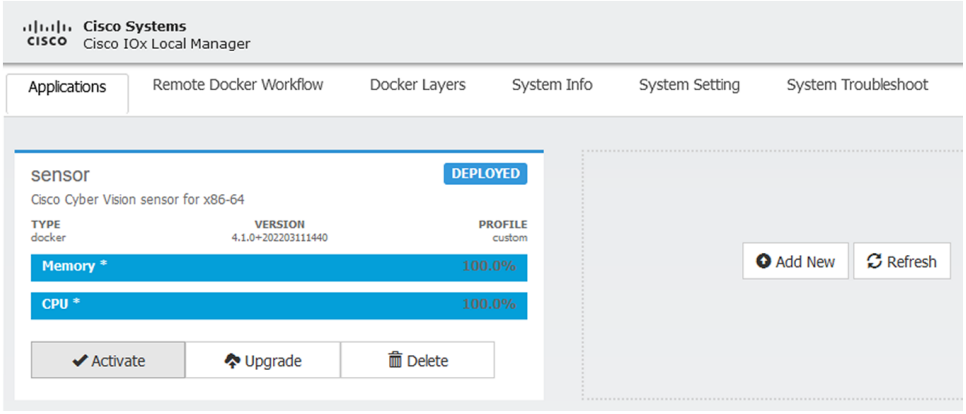




Configure the sensor virtual application

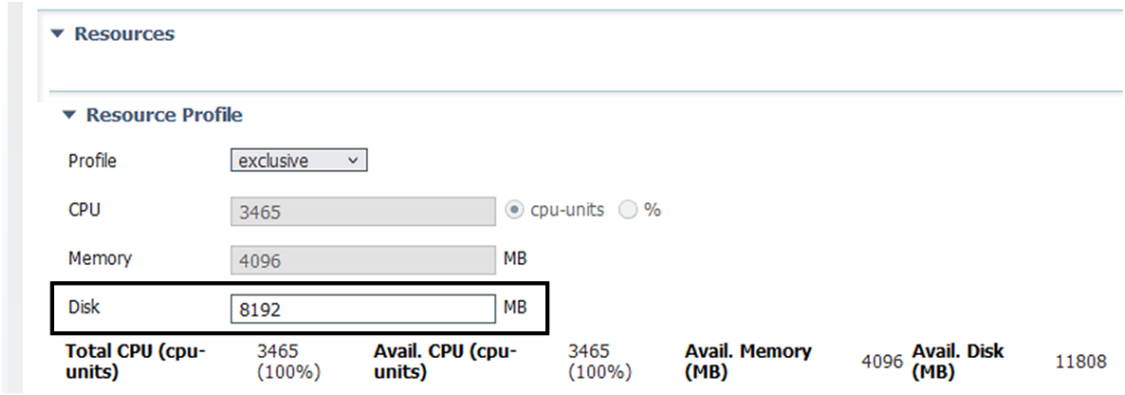
Procedure

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



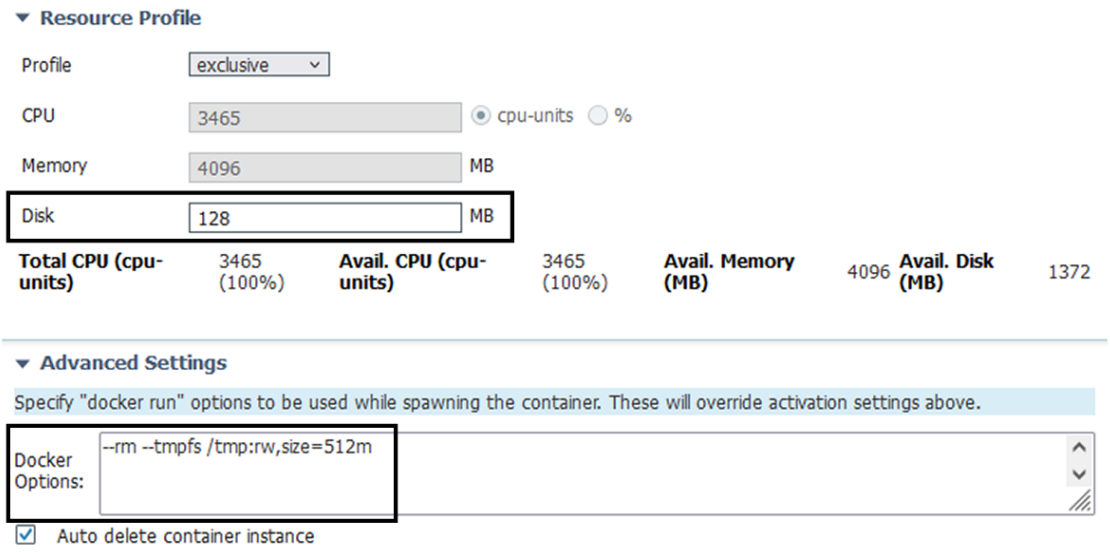
Step 2 Deploy the Resource Profile menu and set the disk size. The procedure differs whether the device has a SSD or not:

- 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 128MB, then deploy the Advanced Settings menu and configure tmpfs by filling the docker options text area with:

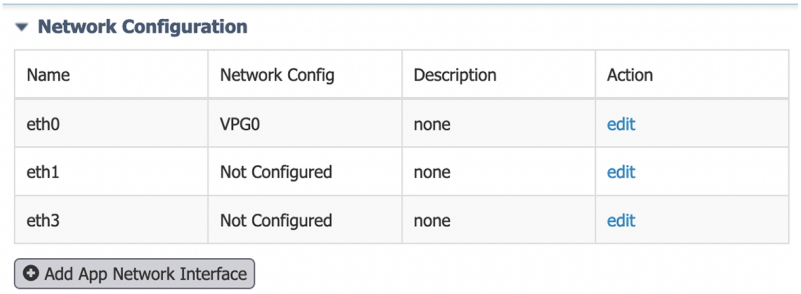
```
--tmpfs /tmp:rw,size=512m
```



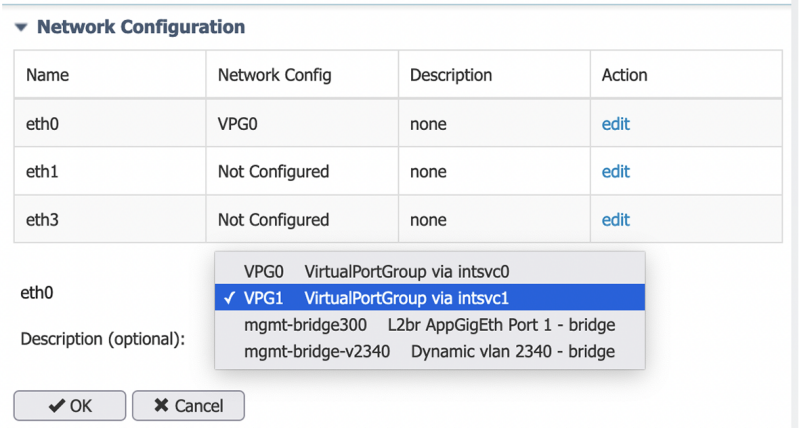
Step 3 Bind the eth0, eth1 and eth3 interfaces in the container to an interface on the host in the Network Configuration menu.

eth0:

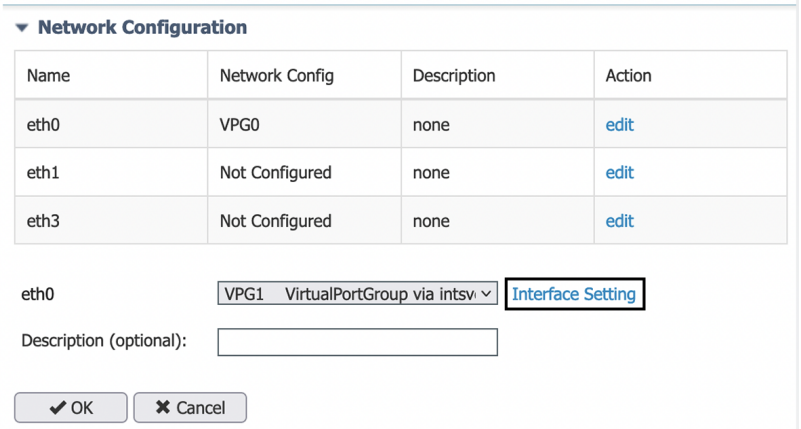
a) Click **edit** in the eth0 line.



b) Select the **VPG1** interface.



c) Click **Interface Setting**.



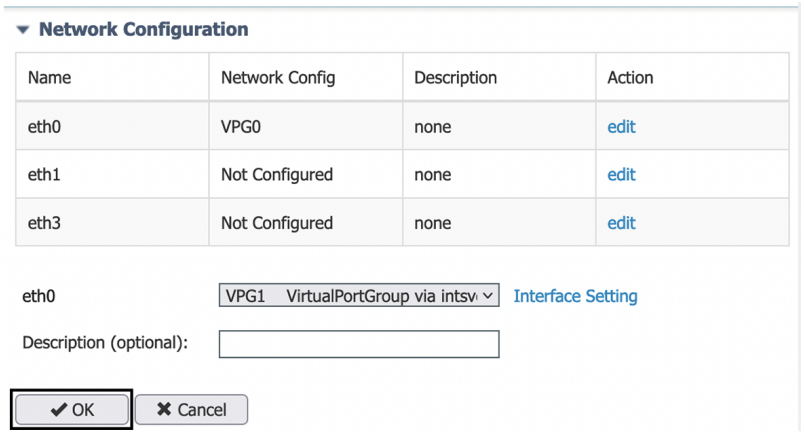
The Interface Setting window pops up.

d) Apply the following configurations:

- Set IPv4 as **Static**.
- IP/Mask: 169.254.0.2 / 30
- Default gateway: 169.254.0.1
- **Disable** IPv6.

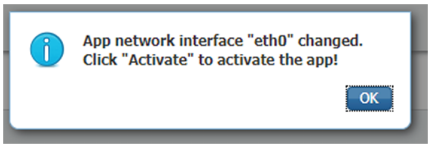
e) Click **OK** to save the interface settings.

You're back to the Network Configuration menu.



f) Click **OK** to save the network configurations.

A popup that confirms changes appears.

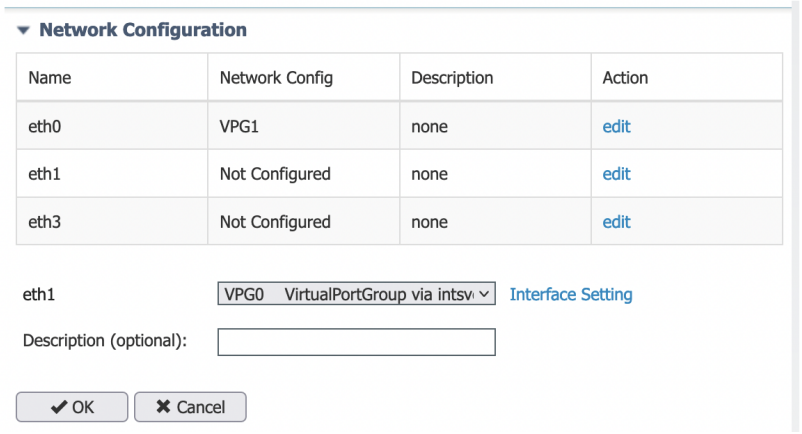


g) Click **OK**.

Step 4 **eth1:**

a) Click **edit** in the eth1 line.

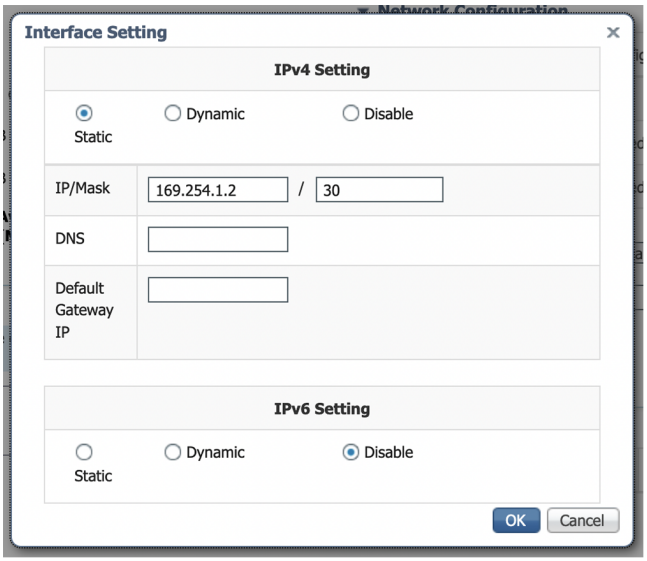
b) Select the **VPG0** interface.



c) Click **Interface setting**.

d) Apply the following configurations:

- Set IPv4 as **Static**.
- IP/Mask: 169.254.1.2 / 30
- **Disable** IPv6.

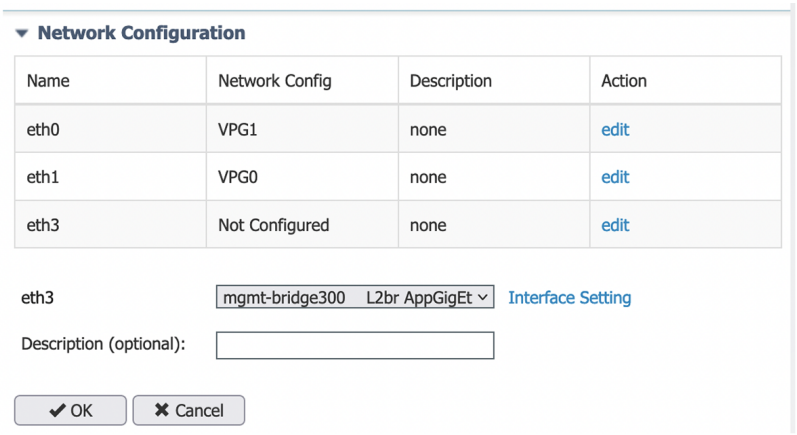


e) Click **OK**, and click **OK** again when you're back to the Network Configuration menu to save the interface settings.

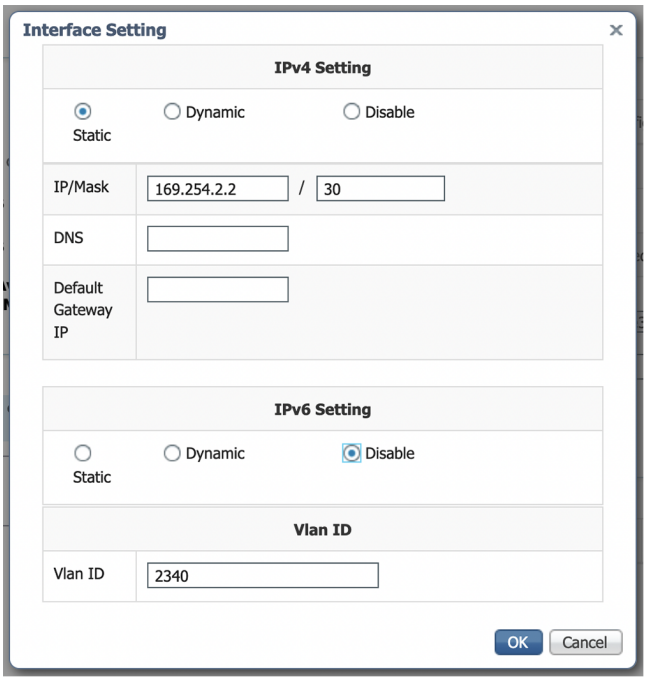
Step 5 **eth3:**

a) Apply the following configurations to eth3:

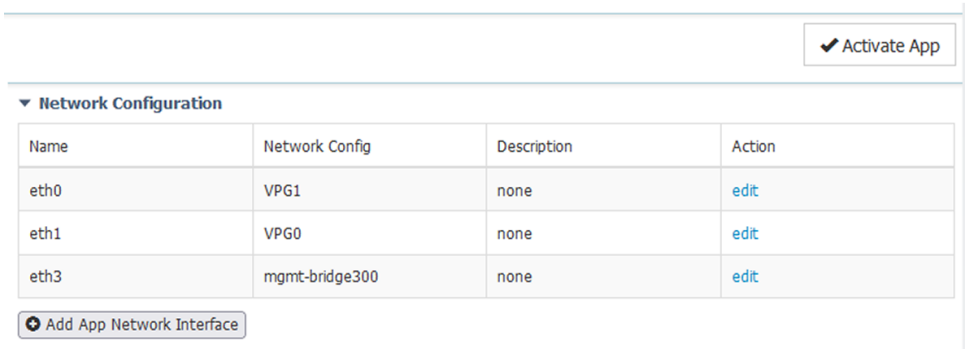
- Select **mgmt-bridge300**.



- Select **Static**.
- IP/Mask: 169.254.2.2/30.
- **Disable** IPv6.
- Vlan ID: VLAN in the Cisco IR8340 dedicated to traffic mirroring for the switched ports (e.g. 2340).



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

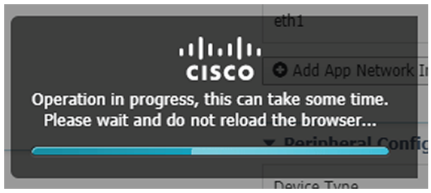


Step 6 If installing a sensor with **Active Discovery**, an additional eth2 interface appears in the Network Configuration menu. To configure this interface:

- Bind eth2 with mgmt-bridge300.
- Make sure IPv4 and IPv6 are set to Dynamic.

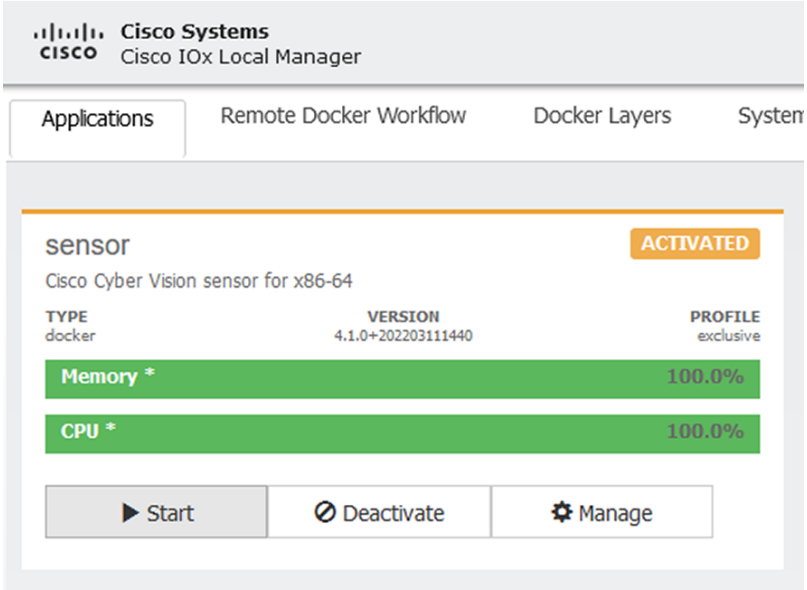
Step 7 Click the **Activate App** button.

The operation takes several seconds.



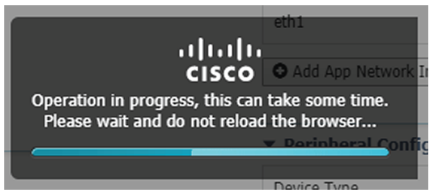
Step 8 Go to the Applications menu to see the application's status.

The application is activated and needs to be started.



Step 9 Click the **Start** button.

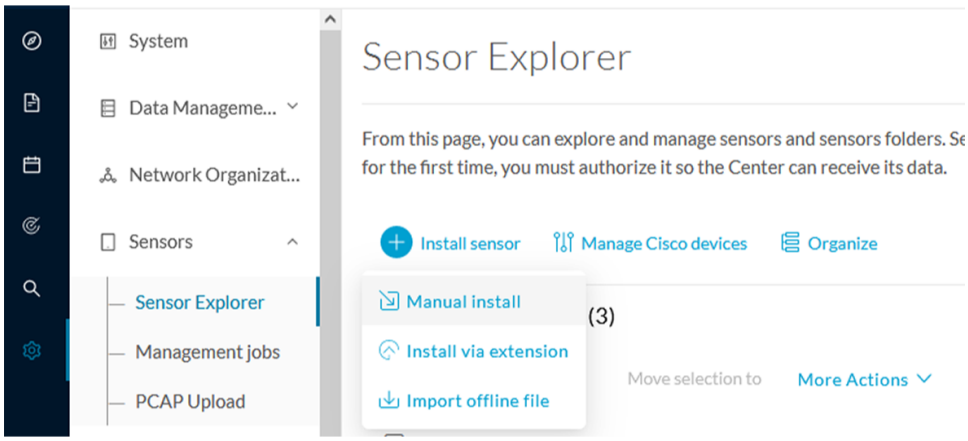
The operation takes several seconds.



The applications' status changes to RUNNING.

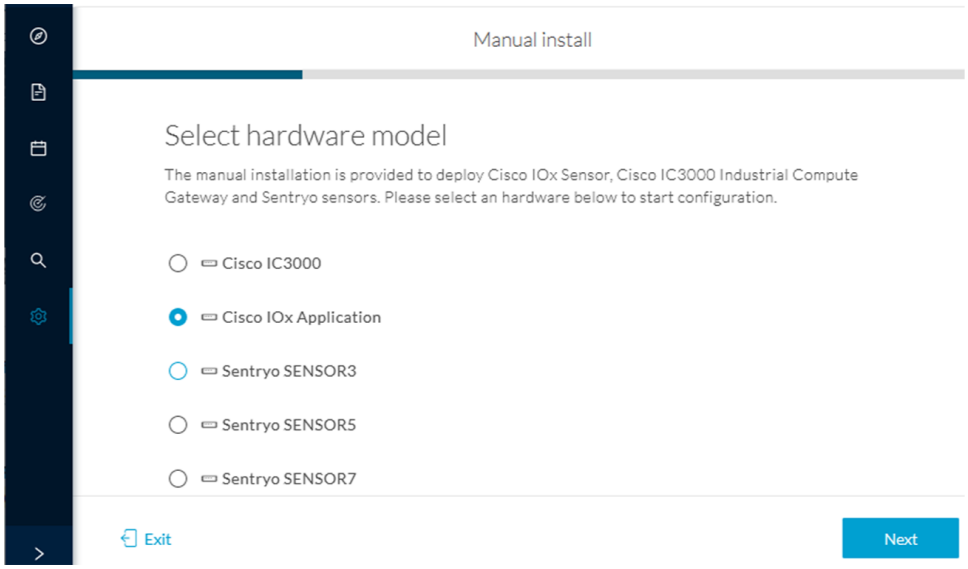
Generate the provisioning package

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

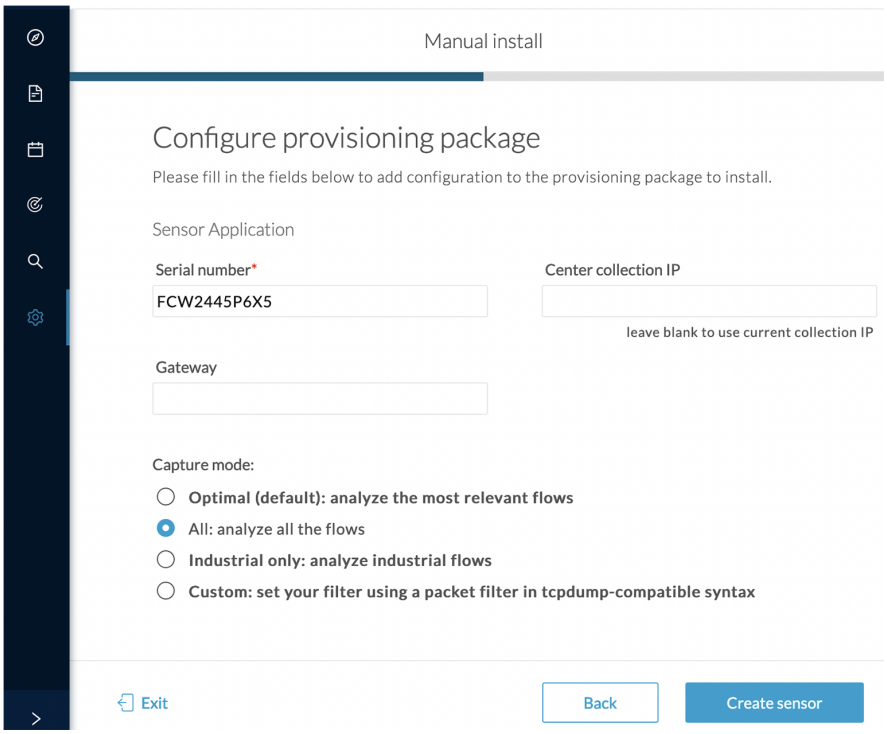


The manual install wizard appears.

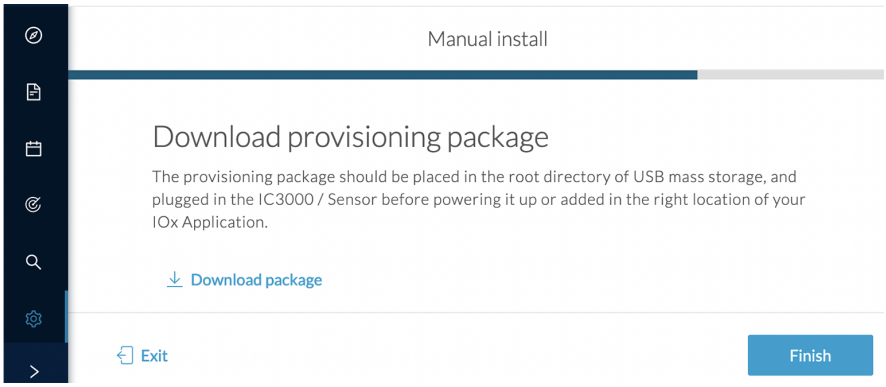
2. Select **Cisco IOx Application** and click **Next**.



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.



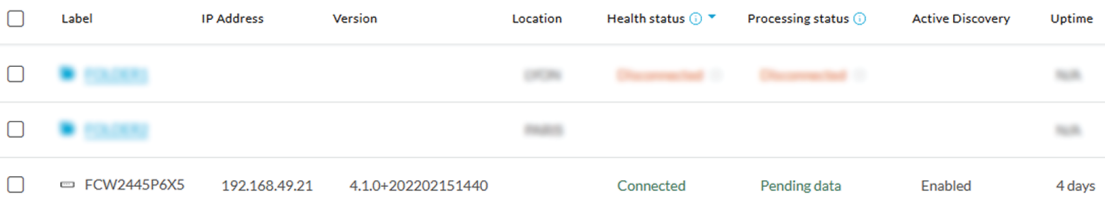
4. Click **Create sensor**.
5. Click the link to download the provisioning package.



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").

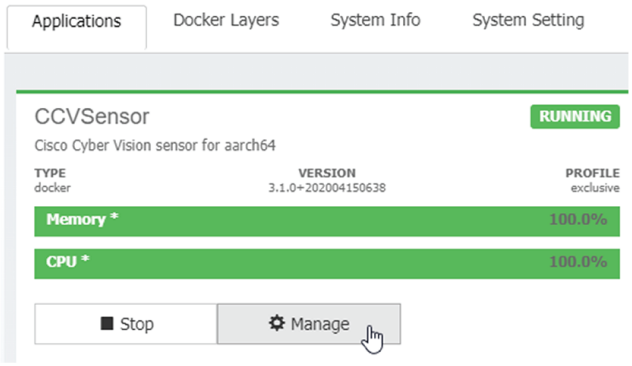
6. Click **Finish**.
7. A new entry for the sensor appears in the Sensor Explorer list.

   The sensor status will switch from Disconnected to Connected.

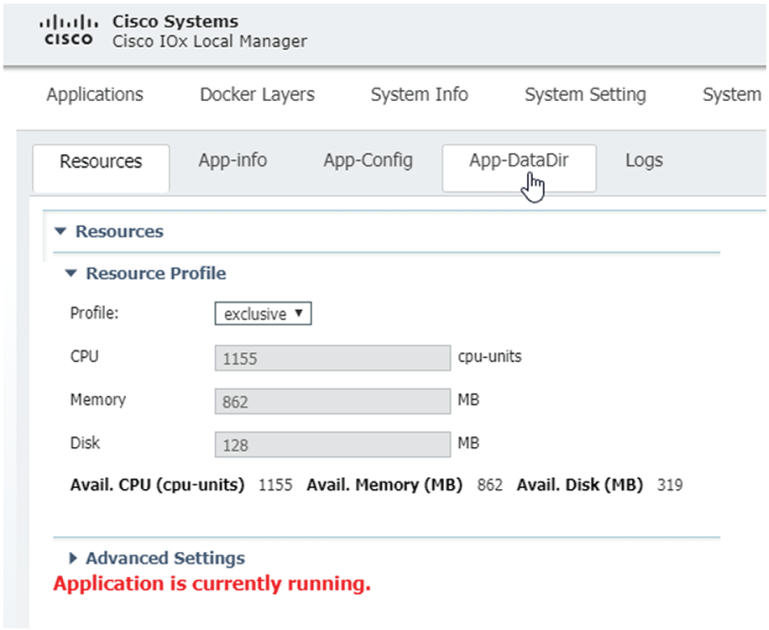


Import the provisioning package

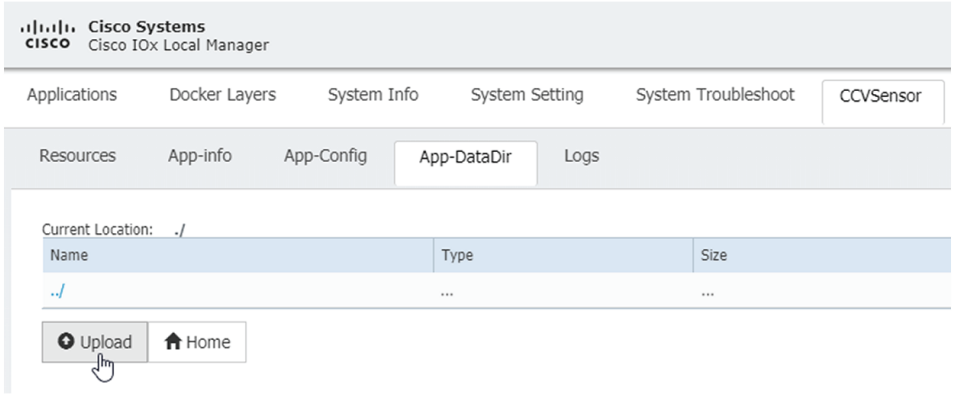
1. In the Local Manager, in the IOx configuration menu, click **Manage**.



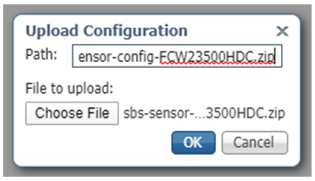
2. Navigate to **App-DataDir**.



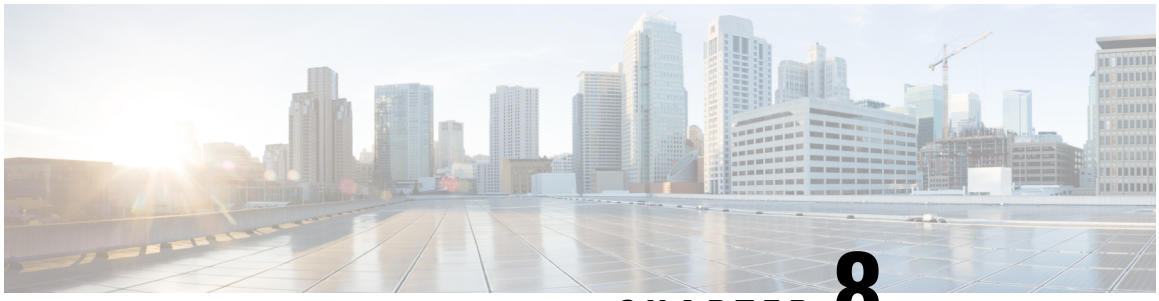
3. Click **Upload**.



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.



CHAPTER 8

Procedure with the CLI

After the Initial configuration, proceed to the steps described in this section.

- Configure the sensor application, on page 39
- Install the sensor application, on page 40
- Copy the sensor application's provisioning package, on page 41

Configure the sensor application

without SSD

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

Procedure

Step 1 Connect to the Cisco IR8340 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-vnic AppGigabitEthernet trunk
      vlan 2340 guest-interface 3
        guest-ipaddress 169.254.2.2 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=512m"
end
```

with SSD

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

Procedure

Step 1 Connect to the Cisco IR8340 through SSH or a console.

Step 2 Configure the application payload by typing the following commands:

```
enable
configure terminal
app-hosting appid sensor
  app-vnic AppGigabitEthernet trunk
    vlan 2340 guest-interface 3
     guest-ipaddress 169.254.2.2 netmask 255.255.255.252
  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 -rm
  app-resource profile custom
    cpu 3465
    memory 4096
    persist-disk 8192
    vcpu 2
end
```

Install the sensor application

The sensor package needs to be collected from cisco.com. The file has the following name structure:

CiscoCyberVision-IOx-x86-64-<version>.tar.

1. Copy the package to a USB key or in the flash memory.
2. Type the following command on the Cisco IR8340's CLI:

   ```
   app-hosting install appid CCVSensor package
   usbflash0:CiscoCyberVision-IOx-x86-64-4.1.0.tar
   ```

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

Note Replace "CiscoCyberVision-IOx-x86-64-4.1.0.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

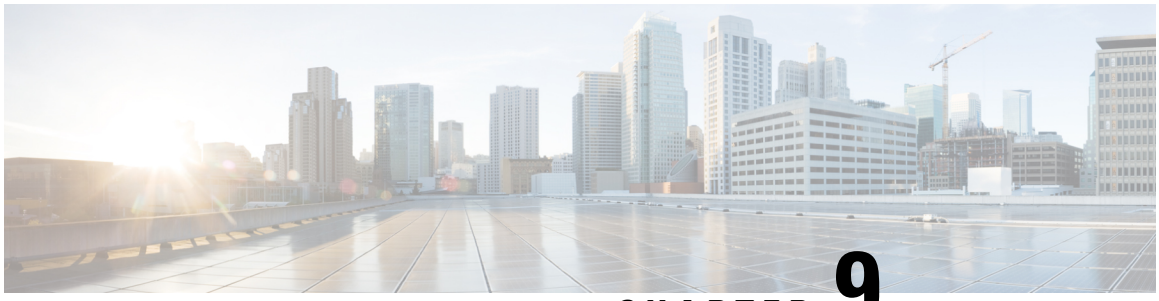
- Copy the provisioning package from the USB key to the application by typing the following command:

```
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.

FCW2445P6X5
192.168.49.21
4.1.0+202202151440
Connected
Pending data
Enabled
4 days



CHAPTER 9

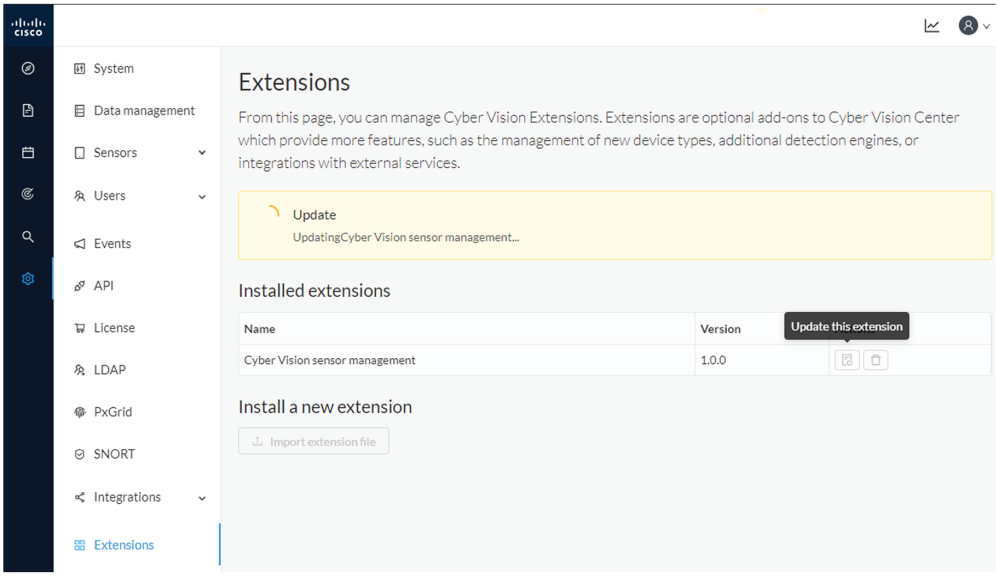
Upgrade procedures

- Upgrade through the Cisco Cyber Vision sensor management extension, on page 43
- Upgrade through the IOx Local Manager, on page 44

Upgrade through the Cisco Cyber Vision sensor management extension

To update IOx sensors, you just need to update the Cisco Cyber Vision sensor management extension.

To do so, navigate to the Extensions administration page and click the **Update this extension** button to browse the new version of the extension file.



Cisco Cyber Vision will attempt to update all IOx sensors. This will take a moment. Update advancements are visible in the Management jobs, on page 16. A job will be created for each sensor.

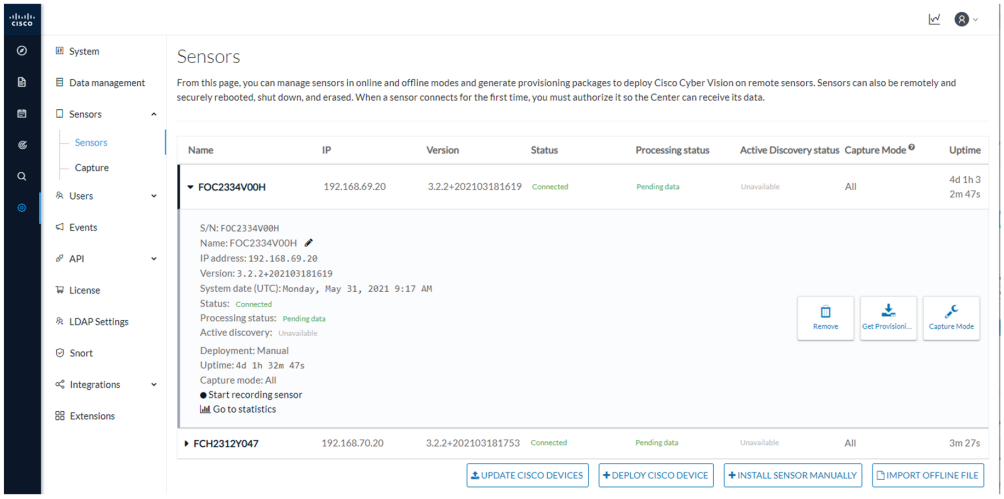
If a sensor update fails, check the management jobs error messages to have more information, and use the **Update Cisco Devices** button.

Upgrade through the IOx Local Manager

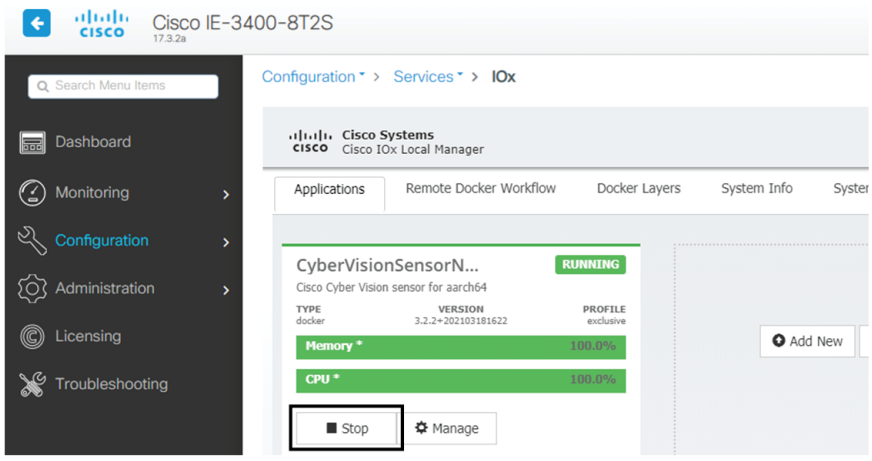
The following section explains how to upgrade the sensor through the IOx Local Manager.

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

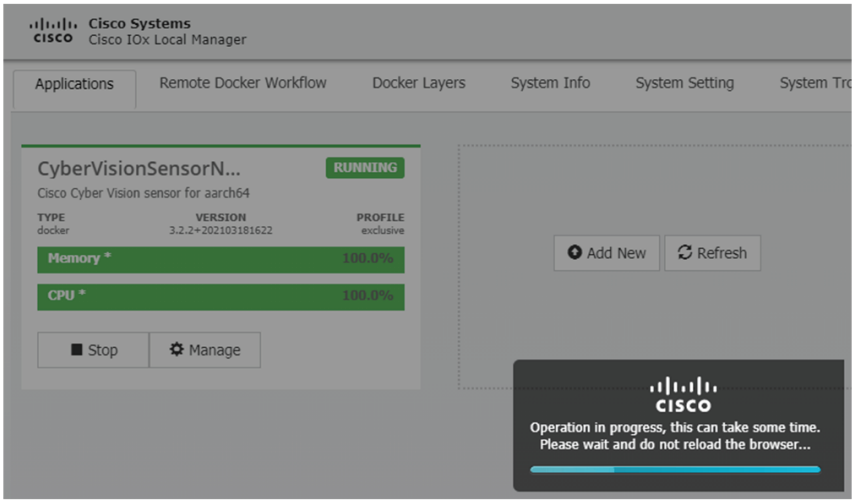
Figure 2: The sensor in version 3.2.2 in the Sensors administration page of Cisco Cyber Vision



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

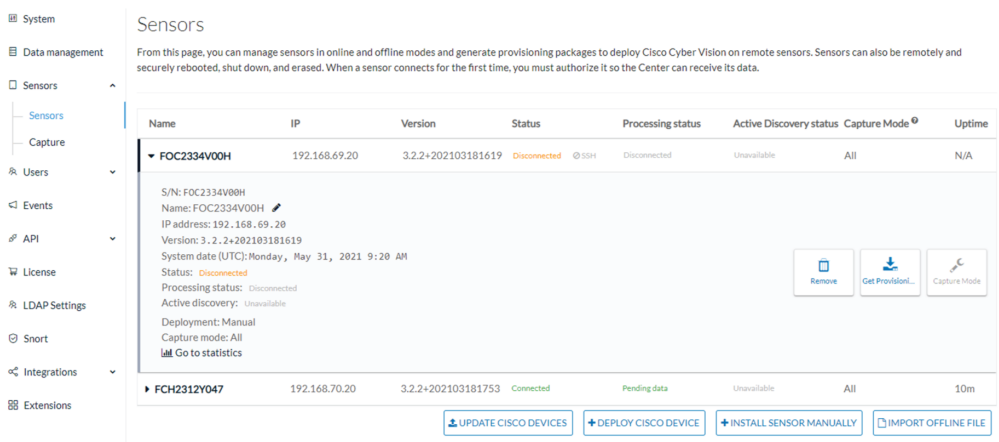


The operation takes a few moments.



The application status switches to STOPPED.

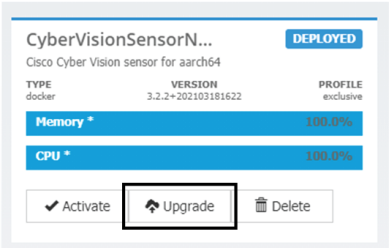
In Cisco Cyber Vision, the sensor status switches to Disconnected.



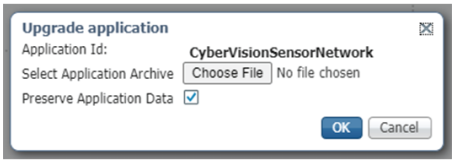
3. In the IOx Local Manager, click the **Deactivate** button.

   The application status moves to DEPLOYED.

4. Click **Upgrade**.

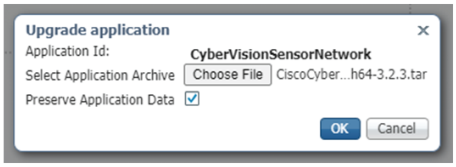


The pop up Upgrade application appears.

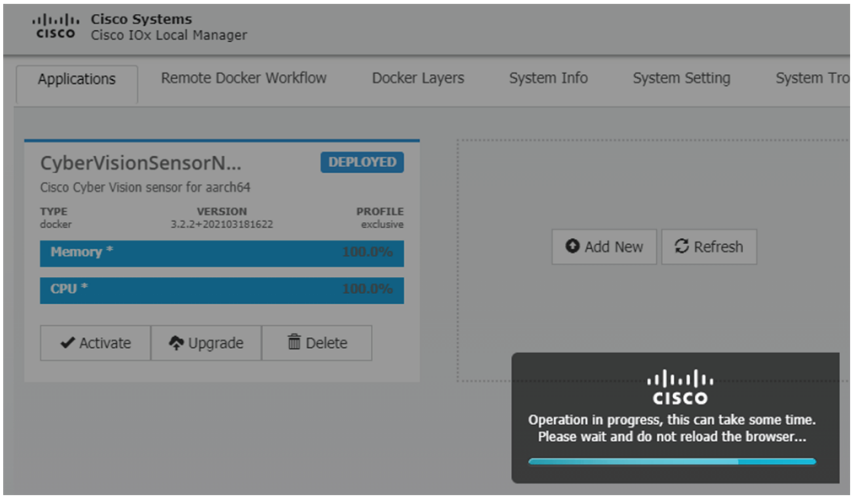


5. Select the **Preserve Application Data** option.
6. Select the new version of the application archive file.

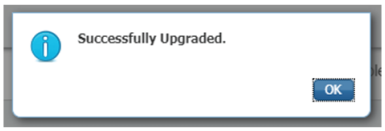
   e.g. CiscoCyberVision-IOx-aarch64-3.2.3.tar



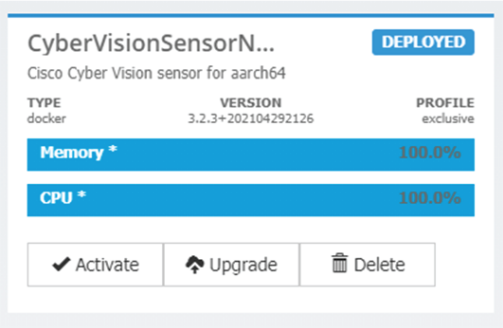
The operation takes a few moments.



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



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



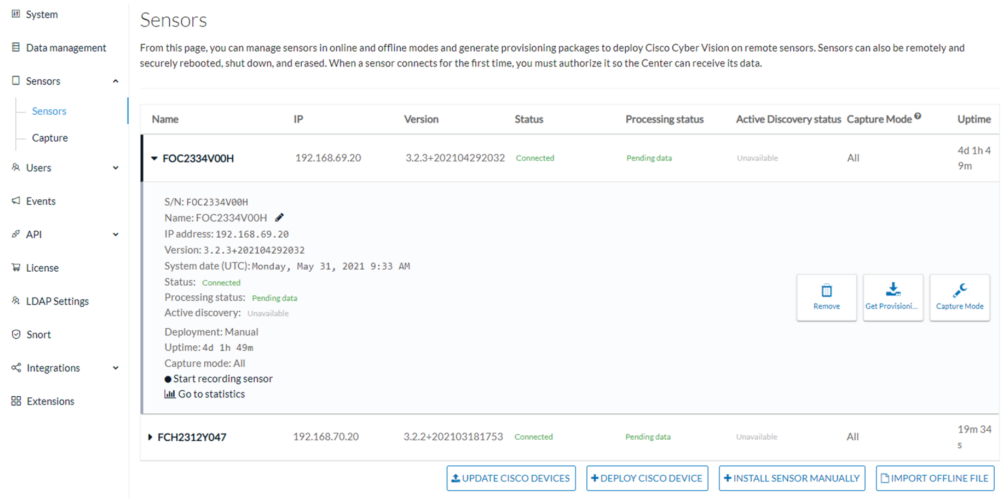
9. Check configurations.

   It can happen that network configurations are lost during the upgrade. If they are, refer to Configure the sensor virtual application (IE3x00 or Catalyst 9300) and do as explained.

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.