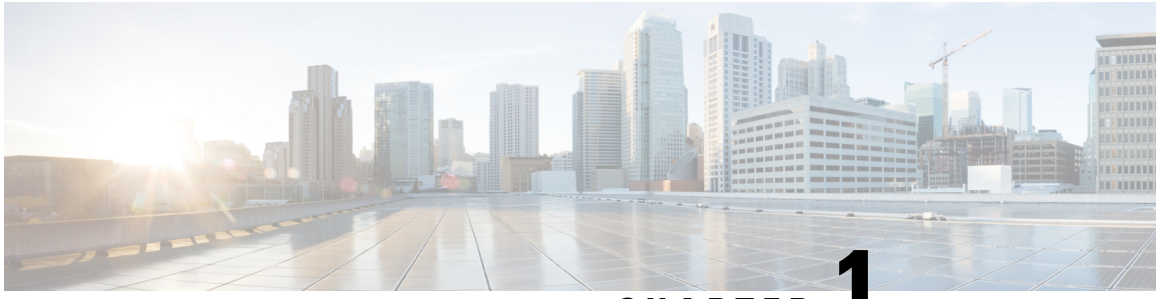
Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.4.0

First Published: 2021-01-01

Last Modified: 2024-04-30

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



CHAPTER 1

About this documentation

Document purpose

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

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst IE3400 Heavy Duty Series Switch

Note The manual refers to these devices as "IE3x00".

- Cisco Catalyst IE9300 Rugged Series Switch

Note The manual refers to this device as "IE9x00".

- Cisco Catalyst 9300 Series Switch
- Cisco Catalyst 9300X Series Switch
- Cisco Catalyst 9400 Series Switch

Note The manual refers to these devices as "Catalyst 9x00".

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

This documentation is applicable to **system version 4.3.0**.

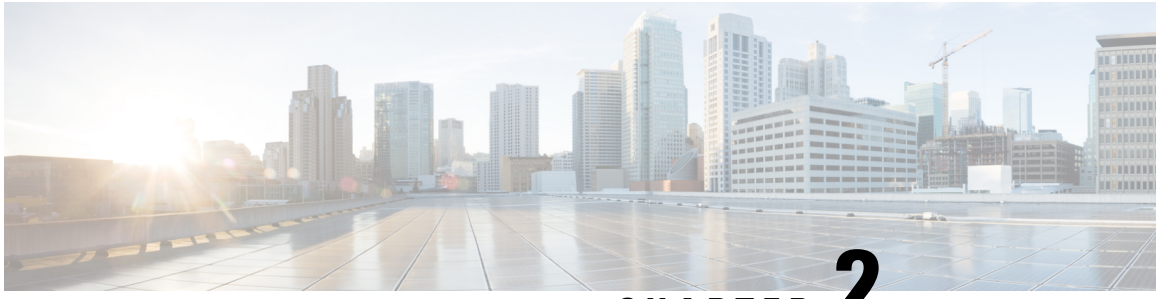
Warnings and notices

To ensure your personal safety and to prevent damage to property, observe the following: Warnings and notices and Safety Alert symbols. 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. Take precautions.

Important Indicates risks that could involve property or Cisco equipment damage and minor personal injury. Take precautions.

Note Indicates important information on the product described in the documentation.



CHAPTER 2

Overview

Overview

Proposed architecture:

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 switch 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 blue on the schema. Mirrored OT traffic is represented in yellow.

The architecture in this document is meant for a switch with an embedded sensor directly connected to the Cisco Cyber Vision Center. The schema presents two types of architecture:

- one with a direct connection to the Center (link="switchport access vlan 507").
- the other with a trunk to another switch or router which is connected to the Center (link="switch mode trunk").

Several types of installation are explained. One of them is the installation with the Sensor Management extension. This method requires an access for the Cisco Cyber Vision Center to the switch's Local Manager. Several solutions exist:

having the Center on the same subnet than the switch's Local Manager (<admin_VLAN> and <collection_VLAN> are the same).

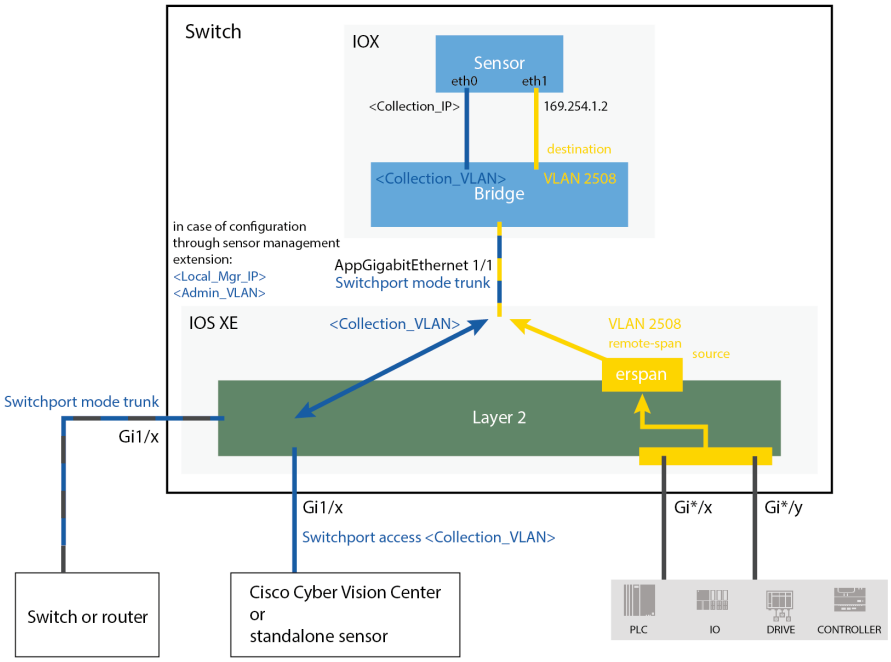
having a route path from the Center to an <admin_VLAN> that is different from <collection_VLAN>.

Any port of the switch can be used for the communication with the Center or for OT traffic.

Architecture diagram for:

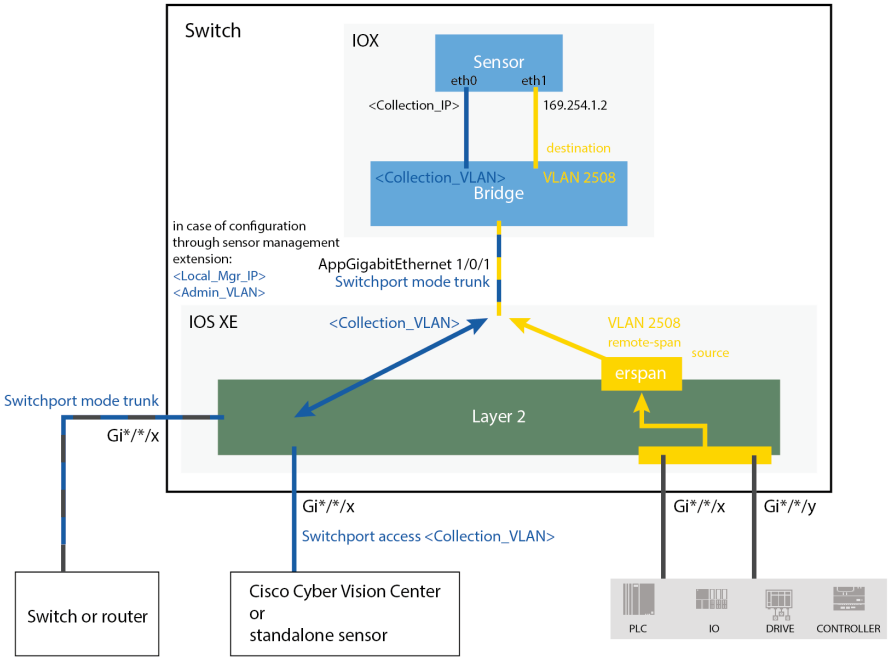
- **Cisco Catalyst IE3300 10G Rugged Series Switch**
- **Cisco Catalyst IE3400 Rugged Series Switch**

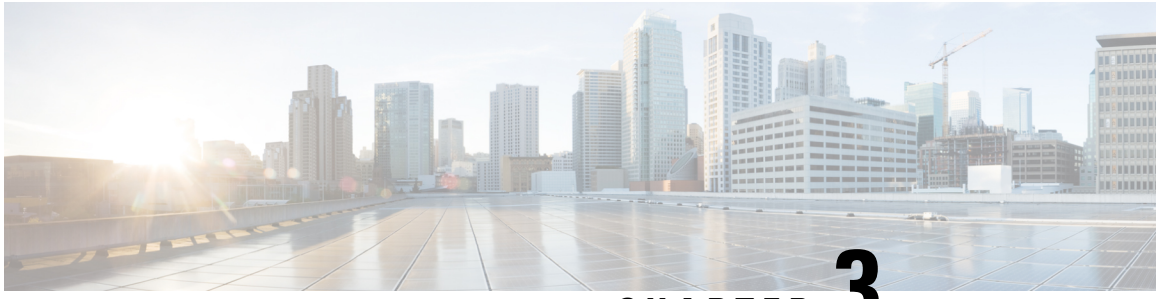
- **Cisco Catalyst IE3400 Heavy Duty Series Switch**



Architecture diagram for:

- **Cisco Catalyst 9300 Series Switch**
- **Cisco Catalyst 9300X Series Switch**
- **Cisco Catalyst 9400 Series Switch**
- **Cisco Catalyst IE9300 Rugged Series Switch**


Switch
IOX
Sensor
eth0
eth1
<Collection_IP>
169.254.1.2
destination
<Collection_VLAN>
VLAN 2508
Bridge
in case of configuration
through sensor management
extension:
<Local_Mgr_IP>
<Admin_VLAN>
AppGigabitEthernet 1/0/1
Switchport mode trunk
IOS XE
<Collection_VLAN>
VLAN 2508
remote-span
source
erspan
Switchport mode trunk
Gi*/*/x
Layer 2
Gi*/*/x
Switchport access <Collection_VLAN>
Gi*/*/x
Gi*/*/y
Switch or router
Cisco Cyber Vision Center
or
standalone sensor
PLC
IO
DRIVE
CONTROLLER



CHAPTER 3

Requirements

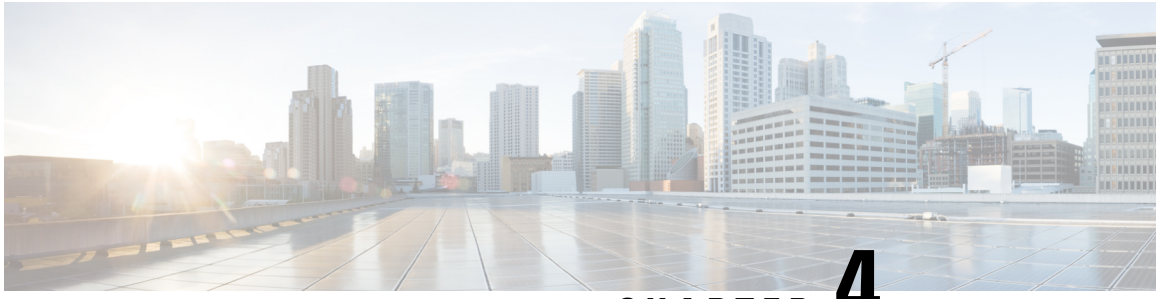
Requirements

The hardware must have an access set to the Local Manager and to the CLI (ssh or console port).

Elements to collect

- The Cisco Cyber Vision Sensor application to collect from Cisco.com, i.e.
  - CiscoCyberVision-IOx-aarch64-<version>.tar (Cisco IE3300 10G, Cisco IE3400, Cisco IE9300)
  - CiscoCyberVision-IOx-x86-64-<version>.tar (Cisco Catalyst 9300)
  - CiscoCyberVision-IOx-Active-Discovery-aarch64-<version>.tar (Cisco IE3300 10G, Cisco IE3400, Cisco IE9300 with Active Discovery)
  - CiscoCyberVision-IOx-Active-Discovery-x86-64-<version>.tar (Cisco Catalyst 9300 with Active Discovery)
- A console cable, for the connection to the hardware's console port.

  OR
- An Ethernet cable, for the connection to one of the hardware's port.



CHAPTER 4

Additional remarks

Additional remarks

About the IE3400 and IE3300 10G platforms:

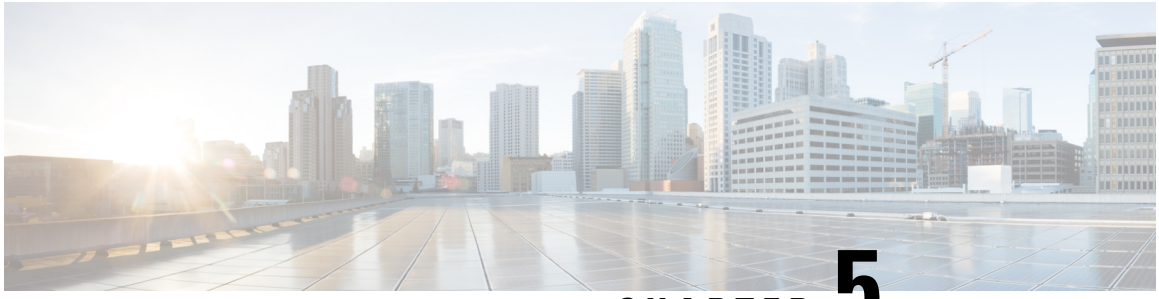
Cisco Cyber Vision Sensor application will receive ERSPAN traffic. Due to ERSPAN overhead it is recommended to not update the MTU of the platform (switch IE3x00) above 1940 bytes. Otherwise, large packets above 1940 will not be received by the sensor application.

About the initial configuration:

Configurations described in the initial configuration are given as examples to use a Cisco Cyber Vision sensor embedded in a switch.

However, in case a more complex installation is required, a trained user will have to configure the switch with all the necessary VLAN and port settings.

Additional remarks

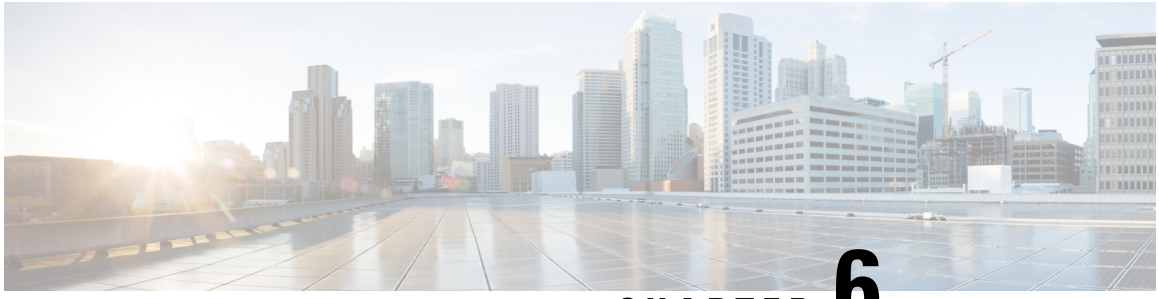


CHAPTER 5

Known issues

Known issues

- The deployment procedure with the Local Manager is not supported by firmware version 17.3.x. Perform the Procedure with the Cisco Cyber Vision sensor management extension, on page 29 instead.
- Cisco Catalyst 9300: deployments will be possible for sensors on firmware version 17.6.x as of Cisco Cyber Vision version 4.0.1.
- IOx redundancy is not supported: sensors will not persist after a failover. This applies in particular to stacks of Cisco Catalyst 9300, stacks of Cisco Catalyst 9300X, stacks of Cisco IE9300 and Cisco Catalyst 9400 with redundant processor boards.
- The sensor application supports RSPAN on Catalyst 9x00 in addition to ERSPAN in Cisco Cyber Vision version 4.1.3. In case of RSPAN usage, multicast packets and packet VLAN information are not transferred to the sensor application.



CHAPTER 6

Initial configuration

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

Configure the switch access

To configure each Cisco switch access refer to its corresponding installation guide available through the following links:

- Cisco Catalyst IE3x00:

  https://www.cisco.com/c/en/us/support/switches/catalyst-ie3300-rugged-series/series.html#~tab-documents

  https://www.cisco.com/c/en/us/support/switches/catalyst-ie3400-rugged-series/series.html#~tab-documents

  https://www.cisco.com/c/en/us/support/switches/catalyst-ie3400-heavy-duty-series/series.html

- Cisco Catalyst IE9x00:

  https://www.cisco.com/c/en/us/support/switches/catalyst-ie9300-rugged-series/series.html

- Cisco Catalyst 9x00:

  https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/series.html#~tab-documents

  https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/series.html#~tab-documents

Check the software version

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

```
Show version
```

To be compatible with the Cisco Cyber Vision Sensor Application:

- the displayed version for Cisco IE3x00 and Cisco Catalyst 9x00 must be 17.02.01 or higher.
- the displayed version for Cisco IE9x00 must be 17.09.01 or higher.

For example: Cisco IE3400

```
IE340CCV#
IE340CCV#show version
Cisco IOS XE Software, Version 17.02.01
Cisco IOS Software [Amsterdam], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.2.1, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 26-Mar-20 01:42 by mcpre
```

If the version is lower, you must update the switch firmware. To do so, follow the links to the products page in Configure the switch access.

SD Card (IE3x00/IE9x00)

If not already done, insert a 4GB Cisco SD card minimum into the switch SD card slot.

Then, you format or partition the SD card.

- You can format the SD card for Ie3x00 using following command:

```
format sdflash: ext4
```

```
IE340CCV#format sdflash: ext4
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:".  Continue? [confirm]
format completed with no errors

Format of sdflash: complete
IE340CCV#
```

Partition command is not supported on Ie9x00.

- You can partition the SD card for Ie3x00 and Ie9x00 with following command:

```
partition sdflash: iox
```

```
IE3400PERF#partition sdflash: iox
Partitioning IOS:IOX(34%:66%) Default
Partition command reloads the switch, Continue?[confirm]
Please make sure to back-up "sdflash:" contents
Partition operation will destroy all data in "sdflash:". Continue?[confirm]
```

Partition is intended for SD swap drive usage. For more information, refer to the corresponding switch user manual.

- You can check the file system using the following command (check for ext4 and Read/Write):

```
show sdflash: filesys
```

```
IE340CCV#show sdflash: filesys
Filesystem: sdflash
Filesystem Path: /flash11
Filesystem Type: ext4
Mounted: Read/Write
```

SSD Disk (Catalyst 9x00)

When a deploying a sensor on a Catalyst 9x00, you have the option to include an SSD or not. If you choose to use an SSD, follow the steps below. Otherwise, proceed to the next step: Check the date and time.

If not already done, insert a 120GB Cisco SSD disk minimum in the SSD slot.

- You can format the SSD disk using the following command:

  ```
  format usbflash1: ext4
  ```

  ```
  CAT9KCCV#
  CAT9KCCV#format usbflash1: ext4
  Format operation may take a while. Continue? [confirm]
  Format operation will destroy all data in "usbflash1:".  Continue? [confirm]
  Format of usbflash1: complete
  CAT9KCCV#
  ```

- You can check the file system using the following command (check for ext4 and Read/Write):

  ```
  show usbflash1: filesys
  ```

  ```
  CAT9KCCV#show usbflash1: filesys
  Filesystem: usbflash1
  Filesystem Path: /vol/usb1
  Filesystem Type: ext4
  Mounted: Read/Write

  CAT9KCCV#
  ```

Check date and time

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

Note Unlike hardware sensors (i.e. Cisco IC3000) that fetch their time from the Center, the Cyber Vision IOX application sensor gets the time from the host (switch platform). Therefore, it is critical that the host synchronizes its time with the Center or a valid NTP server if it's synchronized with the Center. If the time difference is large (hours or more), the user should adjust the Cisco IE3400 time using the Local Manager 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
   ```

   For examples:

Cisco IE3400:

```
IE340CCV#
IE340CCV#show clock
*13:48:03.650 UTC Wed Apr 8 2020
IE340CCV#
```

Cisco Catalyst 9300:

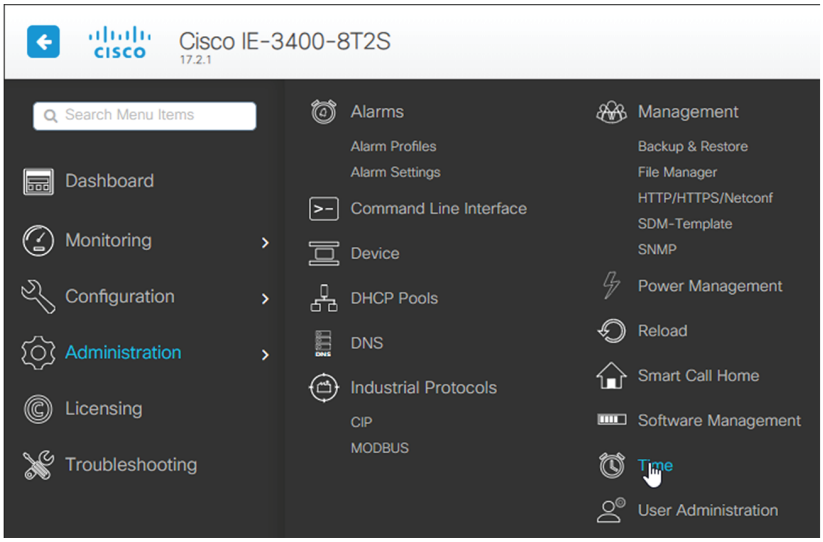
```
CAT9KCCV#
CAT9KCCV#show clock
*16:02:57.900 UTC Thu Apr 30 2020
CAT9KCCV#
```

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

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

   Or go to the Local Manager:

   For example: Cisco IE3400



Enable IOx

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

1. Enable IOx using the following command:

   ```
   configure terminal
   iox
   ```

   For examples:

   Cisco IE3400:

```
IE340CCV#
IE340CCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE340CCV(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device could occur.

IE340CCV(config)#
```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT9KCCV(config)#iox
CAT9KCCV(config)#
```

2. Check the IOx service status using the following command:

```
exit
show iox
```

For examples:

Cisco IE3400:

```
IE340CCV#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
```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 1.10.0.1 : Running
IOx service (HA)           : Running
IOx service (IOxman)       : Running
IOx service (Sec storage)  : Not Running
Libvirtd   1.3.4           : Running
Dockerd    18.03.0         : Running
Application DB Sync Info : Available
Sync Status : Disabled


CAT9KCCV#
```

Add the necessary configuration parameters (IE3x00)

In industrial networking environments, efficient communication between internal applications and external servers is essential for seamless operations. However, the requirement for each application to have a public routable IP address, in addition to the IP address for switch management, poses challenges for network administrators. IOS version 17.14 introduces a new feature called “L3NAT for IOx Applications” to avoid to create a dedicated IP address for a Cyber Vision sensor embedded in a IE3x00 switches. 2 solutions are available to deploy a Cyber Vision sensor:

- The usage of a dedicated IP address for the Cyber Vision sensor
- The new feature in IOS 17.14, "L3NAT for IOx Applications," allows you to use the switch's management IP as a proxy for all network applications.

Sensor Configuration with an External IP Address

The example of configuration given below is a simple one. This configuration is only valid if a direct link exists between the Center and the switch with the embedded sensor. In this case, the dedicated port is configured with the Collection VLAN (for example, 507). In many other cases, the port used for communication between the Center and the sensor will have to be configured as trunk.

Procedure

Step 1 Open the Cisco IE3300 10G/IE3400 CLI through ssh or via the console terminal.

Step 2 Configure a VLAN for traffic mirroring using the following commands:

```
configure terminal
vtp mode off
vlan 2508
remote-span
exit
```

```
IE34ERIC(config)#vtp mode off
Setting device to VTP Off mode for VLANS.
IE34ERIC(config)#vlan 2508
IE34ERIC(config-vlan)#remote-span
IE34ERIC(config-vlan)#exit
IE34ERIC(config)#
```

The VTP off command is performed here since VTP is enabled by default and is not compatible with a high VLAN number.

If needed, select another VLAN number and use the VTP configuration requested by the network.

Step 3 Configure the AppgigabitEthernet port for communications to reach the IOx virtual application.

If communication with the sensor is done on VLAN1, the native VLAN of the Appgigabit interface must be changed to a different value, where "xxx" is the existing VLAN in the switch.

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

```
switchport trunk native vlan xxx
exit
```

```
IE340CCV(config)#
IE340CCV(config)#interface AppGigabitEthernet 1/1
IE340CCV(config-if)#switchport mode trunk
IE340CCV(config-if)#exit
IE340CCV(config)#
```

Step 4 Configure the SPAN session and add to the session the interfaces to monitor:

```
monitor session 1 source interface Gi1/10 both
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
```

```
IE340CCV(config)#monitor session 1 source interface Gi1/10 both
IE340CCV(config)#monitor session 1 destination remote vlan 508
IE340CCV(config)#monitor session 1 destination format-erspan 169.254.1.2
```

Step 5 Configure one of the switch's ports to enable the communication between the virtual sensor and the Center:

```
int gi1/3
switchport access vlan 507
no shutdown
```

```
IE340CCV(config)#
IE340CCV(config)#int gi1/3
IE340CCV(config-if)#switchport access vlan 507
% Access VLAN does not exist. Creating vlan 507
IE340CCV(config-if)#no shutdown
IE340CCV(config-if)#exit
```

Step 6 Save the configuration using the following commands:

```
exit
write mem
```

```
IE340CCV(config)#exit
IE340CCV#write mem
Building configuration...
[OK]
IE340CCV#
```

What to do next

Once you are done with the initial configuration, proceed with the application installation and deployment following one of the procedures below with in mind the IP used in the system with the l3nat_iox feature enabled:

- Procedure with the Cisco Cyber Vision sensor management extension, on page 29
- Procedure with the Local Manager, on page 39
- Procedure with the CLI, on page 57

Sensor Configuration with Layer 3 Network Address Translation

Overview

The Layer3 Network Address Translation (L3NAT) for IOx applications is supported starting with IOS-XE release 17.14.1. This feature uses the management IP of the switch as a proxy for all applications within the routed network. The complexity and overhead associated with managing multiple public IP addresses are reduced. The IE3x00 platform supports the L3NAT feature with the Cisco Cyber Vision (CCV) IOx application. However, it cannot be used to NAT other Ethernet traffic from hosts connected to its physical Ethernet ports.

L3NAT-IOx

L3NAT is a networking technique used to translate private IP addresses in an internal network to a public IP address before packets are sent to an external network at the network layer of the OSI model. The L3NAT-IOx feature utilizes hardware components such as Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) for implementation.

When a Cyber Sensor application communicates with the external CCV server, the NAT protocol translates the source private IP address of the Cyber Sensor Application to the public IP address of the Management Switched Virtual Interface (SVI) of the switch. This translation allows the packets to navigate through the external network, gives the impression that they originate from the switch management SVI IP address.

When the external CCV server communicates with the Cyber Sensor Application, the NAT protocol reverses the translation. Incoming packets addressed to the public IP address of the switch management SVI are translated to the private IP address of the destination Cyber Sensor Application. This ensures seamless communication between the application and external servers.

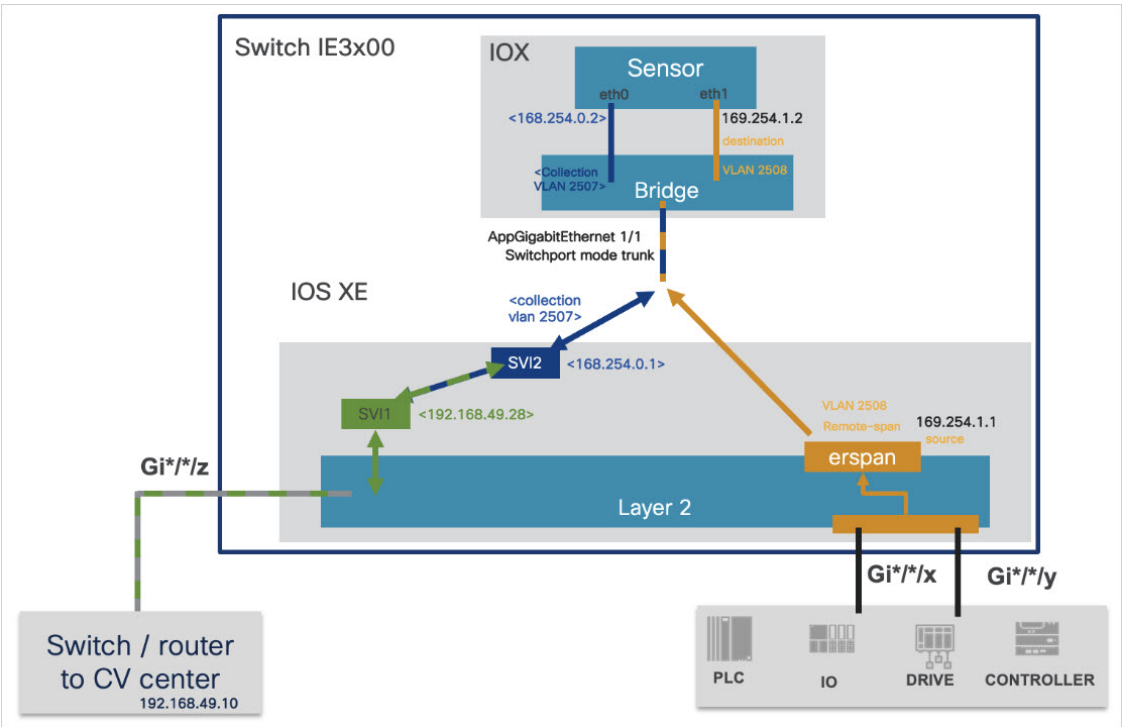
Guidelines and Restrictions

The guidelines and restrictions for L3NAT-IOx are as follows:

- This feature only works with the CCV application and doesn't support any other IOx applications.
- Only static translation is supported.
- Translation is restricted to TCP and UDP packets exclusively.
- Users need to set up an extra SVI on IE for the private network used by the application. The IP assigned to this SVI will act as the default gateway for the application.
- This feature requires a Network Advantage license.
- You can not retrieve L3NAT-IOx statistics using YANG with Network Configuration Protocol (NETCONF).

Configuring L3NAT-IOx

The configuration example is based on the following topology:



The above diagram shows application hosting on the switch using a Private IP address. The CCV sensor application is installed on the access devices connected to hosts. Devices located in the 192.168.49.0/24 network are assigned management IP addresses. The CCV sensor is installed using the private IP network 169.254.0.1/30.

Procedure

Step 1 Set up the SVI for the 169.254.0.x network with an IP address to be the default gateway for the application.

```
Switch(config)# int vlan 2507

Switch(config-if)# ip address 169.254.0.1 255.255.255.252
```

Step 2 Set up the SVI for the 192.168.49.10/24 network with an IP address acting as the public IP to access the CCV center.

```
Switch(config)# int vlan 49

Switch(config-if)# ip address 192.168.49.28 255.255.255.0
```

Step 3 Configure the L3NAT-IOx.

```
Switch# configure terminal

Switch(config)# l3nat-iox

Switch(config-iox-nat)# app-ip 169.254.0.2 svi-ip 192.168.49.28 app-name CCV-ONPREM server-ip
 192.168.49.10
```

```
IE3400esc04#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400esc04(config)#l3
IE3400esc04(config)#l3nat-iox
IE3400esc04(config-l3nat-iox)#$pp-name CCV-ONPREM server-ip 192.168.49.10
IE3400esc04(config-l3nat-iox)#exit
IE3400esc04(config)#exit
IE3400esc04#write mem
Building configuration...
[OK]
IE3400esc04#
```

```
IE3400esc04#show conf | section l3nat
l3nat-iox
 app-ip 169.254.0.2 svi-ip 192.168.49.28 app-name CCV-ONPREM server-ip 192.168.49.10
IE3400esc04#
```

What to do next

Once you are done with the initial configuration, proceed with the application installation and deployment following one of the procedures below with in mind the IP used in the system with the l3nat_iox feature enabled:

- Procedure with the Cisco Cyber Vision sensor management extension, on page 29
- Procedure with the Local Manager, on page 39
- Procedure with the CLI, on page 57

Configuring the Other Necessary Parameters

Procedure

Step 1 Set up a VLAN for mirroring traffic with these commands:

```
configure terminal
vtp mode off
vlan 2508
remote-span
exit
```

```
IE34ERIC(config)#vtp mode off
Setting device to VTP Off mode for VLANS.
IE34ERIC(config)#vlan 2508
IE34ERIC(config-vlan)#remote-span
IE34ERIC(config-vlan)#exit
IE34ERIC(config)#
```

The VTP off command is performed here since VTP is enabled by default and is not compatible with a high VLAN number.

If needed, select another VLAN number and use the VTP configuration requested by the network.

Step 2 Configure the AppgigabitEthernet port for communications to reach the IOx virtual application.

```
interface AppGigabitEthernet 1/1

switchport mode trunk

exit
```

```
IE340CCV(config)#
IE340CCV(config)#interface AppGigabitEthernet 1/1
IE340CCV(config-if)#switchport mode trunk
IE340CCV(config-if)#exit
IE340CCV(config)#
```

Step 3 Configure the SPAN session and add to the monitor:

```
monitor session 1 source interface Gi1/10 both

monitor session 1 destination remote vlan 2508

monitor session 1 destination format-erspan 169.254.1.2
```

```
IE340CCV(config)#monitor session 1 source interface Gi1/10 both
IE340CCV(config)#monitor session 1 destination remote vlan 508
IE340CCV(config)#monitor session 1 destination format-erspan 169.254.1.2
```

Step 4 Save the configuration using the following commands:

```
exit

write mem
```

```
IE340CCV(config)#exit
IE340CCV#write mem
Building configuration...
[OK]
IE340CCV#
```

What to do next

Once you are done with the initial configuration, proceed with the application installation and deployment following one of the procedures below with in mind the IP used in the system with the l3nat_iox feature enabled:

- Procedure with the Cisco Cyber Vision sensor management extension, on page 29
- Procedure with the Local Manager, on page 39
- Procedure with the CLI, on page 57

Add the necessary configuration parameters (Catalyst 9x00/IE9x00)

The configuration examples given in this section are simple ones. They are only valid if a direct link exists between the Center and the switch with the embedded sensor. In this case, the dedicated port is configured with the Collection VLAN (for example, 507). In many other cases, the port used for communication between the Center and the sensor will have to be configured as trunk.

Configuration with ERSPAN is recommended but requires routing to be enabled on the switch. If this is not possible, RSPAN is available on the Catalyst 9x00. However, note that Multicast and VLAN information will be missing with this configuration.

Configure with ERSPAN

Procedure

Step 1 Open the switch's CLI through ssh or via the console terminal.

Step 2 Configure a VLAN for traffic mirroring using the following commands:

```
configure terminal
ip routing
vlan 2508
exit
int vlan 2508
ip address 169.254.1.1 255.255.255.252
no shutdown
exit
```

Step 3 Configure the AppGigabitEthernet port which will enable the communication to the IOx virtual application.

If communication with the sensor is done on VLAN1, the native VLAN of the Appgigabit interface must be changed to a different value, where "xxx" is the existing VLAN in the switch.

```
interface AppGigabitEthernet 1/0/1
switchport mode trunk
switchport trunk native vlan xxx
exit
```

```
CAT9KCCV(config)#
CAT9KCCV(config)#interface AppGigabitEthernet 1/0/1
CAT9KCCV(config-if)#switchport mode trunk
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

Step 4 Configure the SPAN session and add to the session the interfaces to monitor:

Note Disabling the ip routing command for IPv4 connections and ipv6 unicast-routing command for IPv6 connections stops ERSPAN traffic flow to the destination port. Link to Catalyst 9300 manual.

```
monitor session 1 type erspan-source
source interface Gi1/0/2 - 24 both
no shutdown
destination
```

```
erspan-id 2
mtu 9000
ip address 169.254.1.2
origin ip address 169.254.1.1
exit
exit
```

```
CAT9KCCV(config)#
CAT9KCCV(config)#monitor session 1 type erspan-source
CAT9KCCV(config-mon-erspan-src)#source interface Gi1/0/2 - 24 both
CAT9KCCV(config-mon-erspan-src)#no shutdown
CAT9KCCV(config-mon-erspan-src)#destination
CAT9KCCV(config-mon-erspan-src-dst)#erspan-id 2
CAT9KCCV(config-mon-erspan-src-dst)#mtu 9000
CAT9KCCV(config-mon-erspan-src-dst)#ip address 169.254.1.2
CAT9KCCV(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
CAT9KCCV(config-mon-erspan-src-dst)#exit
CAT9KCCV(config-mon-erspan-src)#exit
CAT9KCCV(config)#
```

Step 5 Configure one of the switch's ports to enable the communication between the virtual sensor and the Center:

```
interface GigabitEthernet1/0/1
switchport access vlan 507
no shutdown
exit
```

```
CAT9KCCV(config)#interface GigabitEthernet1/0/1
CAT9KCCV(config-if)#switchport access vlan 507
% Access VLAN does not exist. Creating vlan 507
CAT9KCCV(config-if)#no shutdown
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

Step 6 Save the configuration:

```
exit
write mem
```

```
CAT9KCCV(config)#
CAT9KCCV(config)#exit
CAT9KCCV#write mem
Building configuration...
[OK]
CAT9KCCV#
```

What to do next

The initial configuration is now complete. Proceed with the application installation and deployment following one of the procedures below:

- Procedure with the Cisco Cyber Vision sensor management extension, on page 29
- Procedure with the Local Manager, on page 39
- Procedure with the CLI, on page 57

Configure with RSPAN (Catalyst 9x00 only)

Before you begin

The VLAN configured for RSPAN (here 2508) must be filtered on all trunk ports except for the AppGigabitEthernet interface.

Procedure

Step 1 Open the switch's CLI through ssh or via the console terminal.

Step 2 Configure a VLAN for traffic mirroring using the following commands:

```
configure terminal
vlan 2508
exit
int vlan 2508
remote-span
exit
```

Step 3 Configure the AppGigabitEthernet port which will enable the communication to the IOx virtual application.

If communication with the sensor is done on VLAN1, the native VLAN of the Appgigabit interface must be changed to a different value, where "xxx" is the existing VLAN in the switch.

```
interface AppGigabitEthernet 1/0/1
switchport mode trunk
switchport trunk native vlan xxx
exit
```

```
CAT9KCCV(config)#
CAT9KCCV(config)#interface AppGigabitEthernet 1/0/1
CAT9KCCV(config-if)#switchport mode trunk
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

Step 4 Configure the SPAN session and add to the session the interfaces to monitor:

```
monitor session 1 source interface Gi1/0/2 - 24 both
monitor session 1 destination remote vlan 2508
```

Step 5 Configure one of the switch's ports to enable the communication between the virtual sensor and the Center:

```
interface GigabitEthernet1/0/1
switchport access vlan 507
no shutdown
exit
```

```
CAT9KCCV(config)#interface GigabitEthernet1/0/1
CAT9KCCV(config-if)#switchport access vlan 507
% Access VLAN does not exist. Creating vlan 507
CAT9KCCV(config-if)#no shutdown
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

Step 6 Save the configuration:

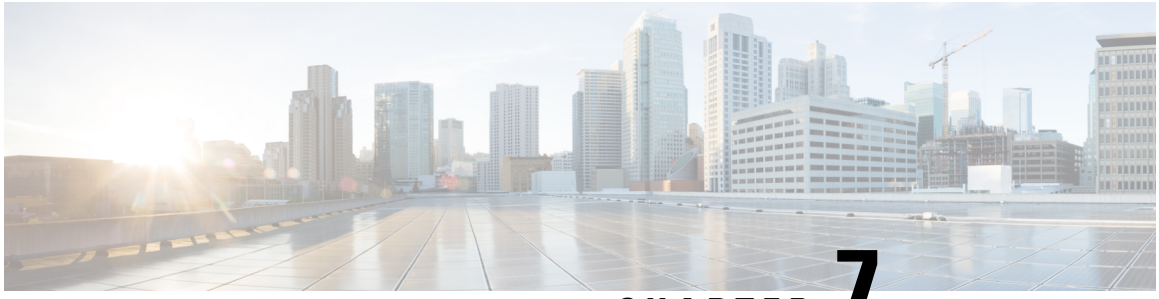
```
exit
write mem
```

```
CAT9KCCV(config)#
CAT9KCCV(config)#exit
CAT9KCCV#write mem
Building configuration...
[OK]
CAT9KCCV#
```

What to do next

The initial configuration is now complete. Proceed with the application installation and deployment following one of the procedures below:

- Procedure with the Cisco Cyber Vision sensor management extension, on page 29
- Procedure with the Local Manager, on page 39
- Procedure with the CLI, on page 57



CHAPTER 7

Installation

Procedure with the Cisco Cyber Vision sensor management extension

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

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.

Note Since the extension deployment based on HTTPS, we should allow the flow to proceed as follows:

- For IEXxxx/CAT9k /IRxx : port TCP 443
- For IC3k : port TCP 8443

We can use an Access Control List (ACL) on IOS XE devices to limit access from the Cyber Vision.

Configuration example for IOS XE devices: Filter Traffic Destined to Cisco IOS XE Devices WebUI Using an Access List - Cisco

```
ip http access-class SOME_ID

ip http secure-server

!

access-list SOME_ID permit CENTER_ETH0_IP CENTER_ETH0_WILDCARDMASK
```

Where CENTER_ETH0_IP is the administration IP address of your Cyber Vision center (eth0).

Install the sensor management extension

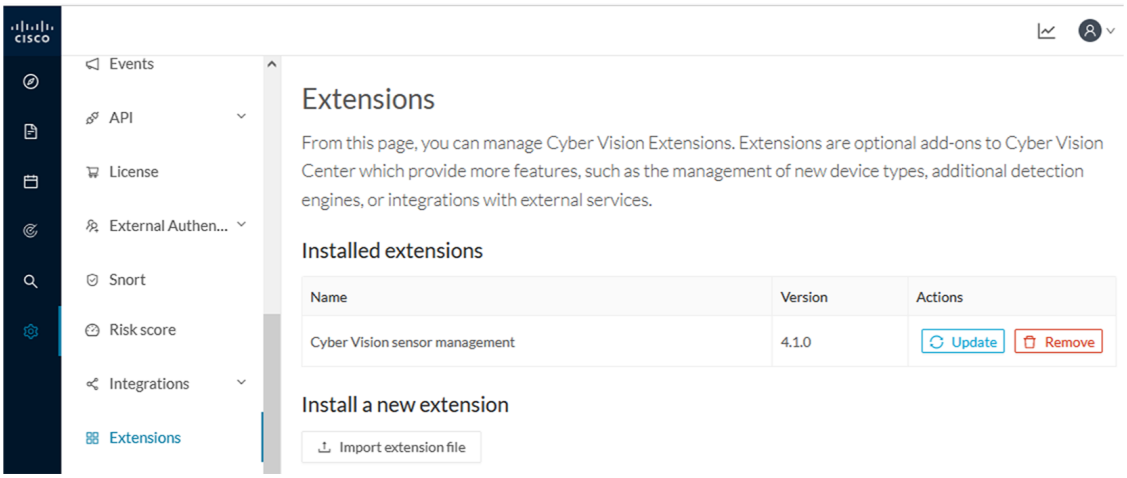
To install the sensor management extension, you must:

Procedure

Step 1 Retrieve the extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) from cisco.com.

Step 2 Access the Extension administration page in Cisco Cyber Vision.

Step 3 Import the extension file.

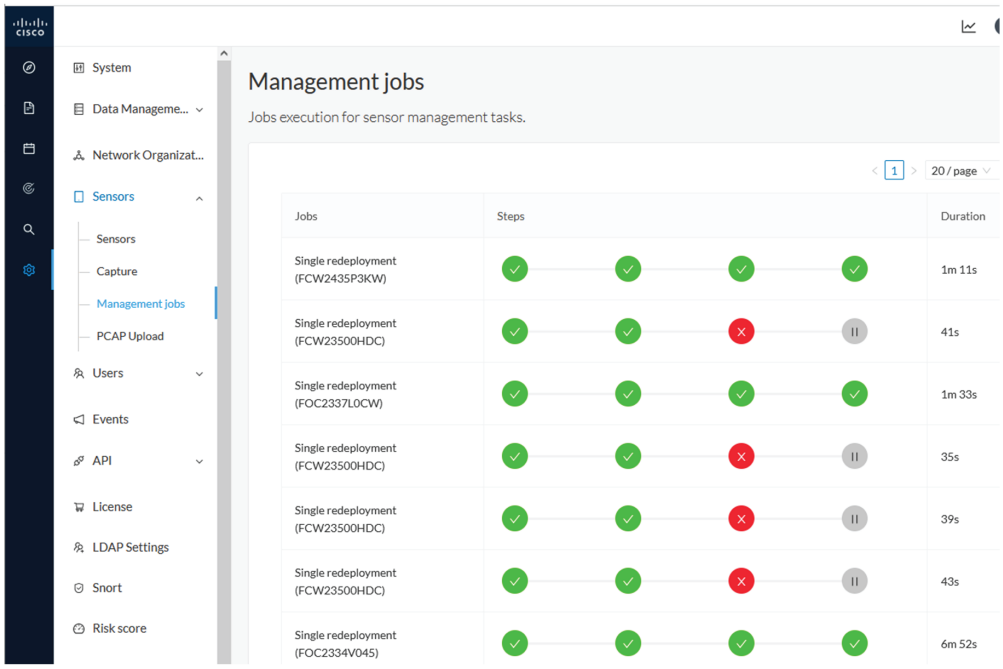


Once the sensor management extension is installed, you will find a new management job under the sensor administration menu (Management jobs, on page 30), and the **Install via extension** button will be enabled in the Sensor Explorer page.

Management jobs

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

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



You will find the following jobs:

- Single deployment

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

- Single redeployment

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

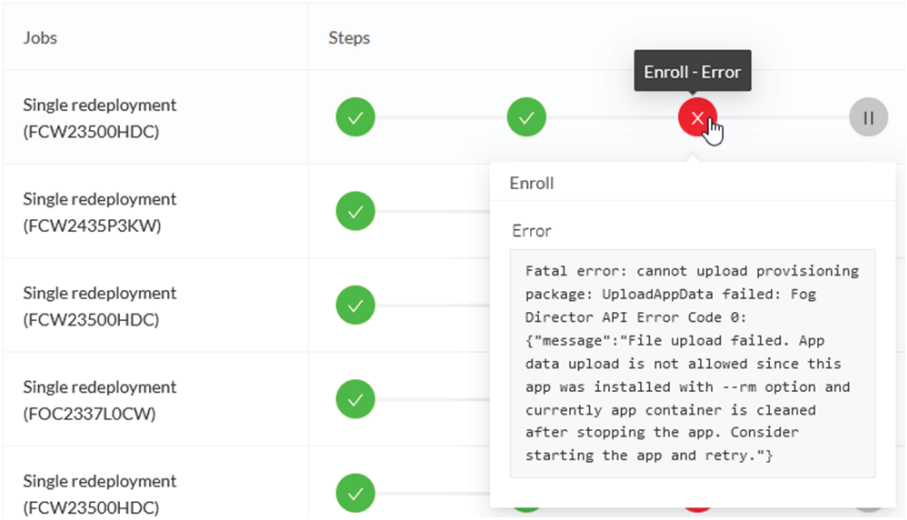
- Single removal

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

- Update all devices

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

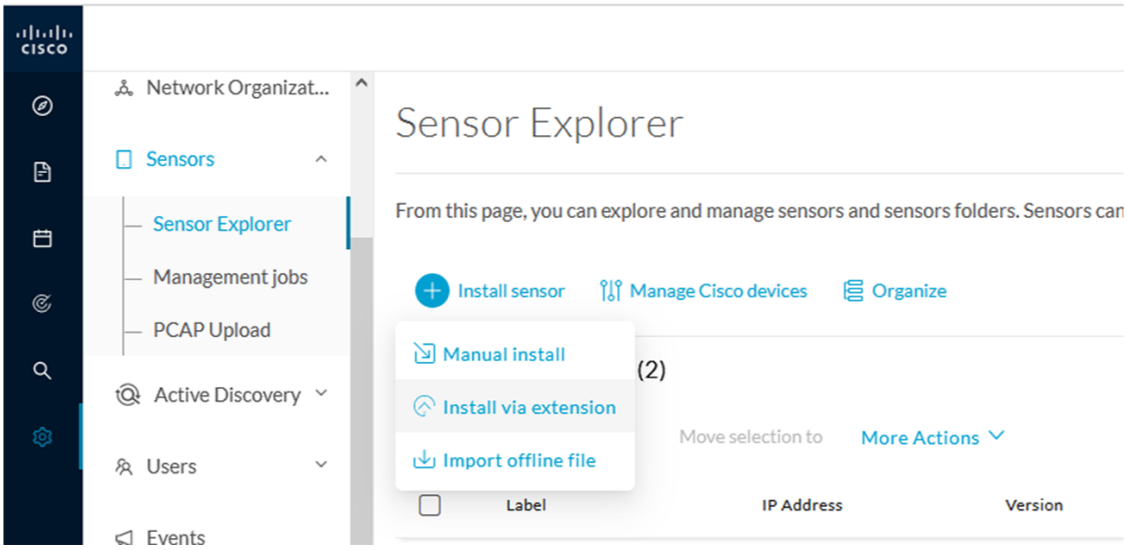
If a job fails, you can click on the error icon to view detailed logs.



Create a sensor in the sensor management extension

Procedure

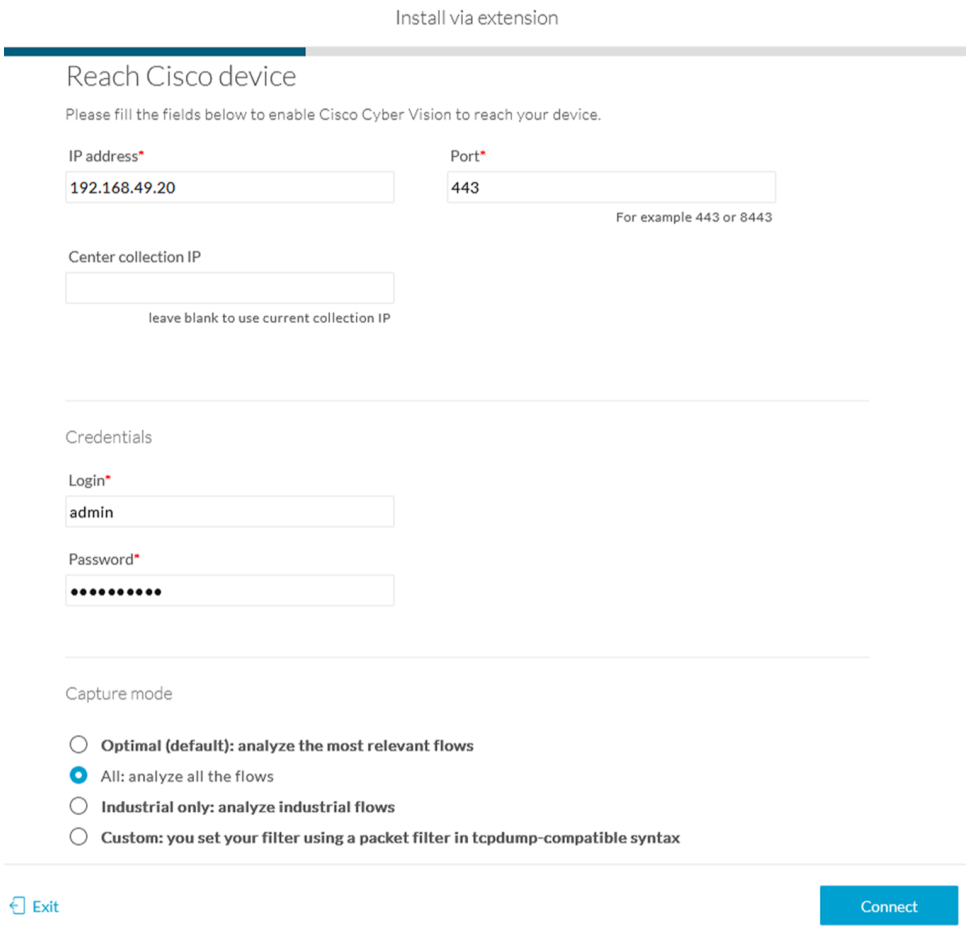
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Install via extension**.



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.



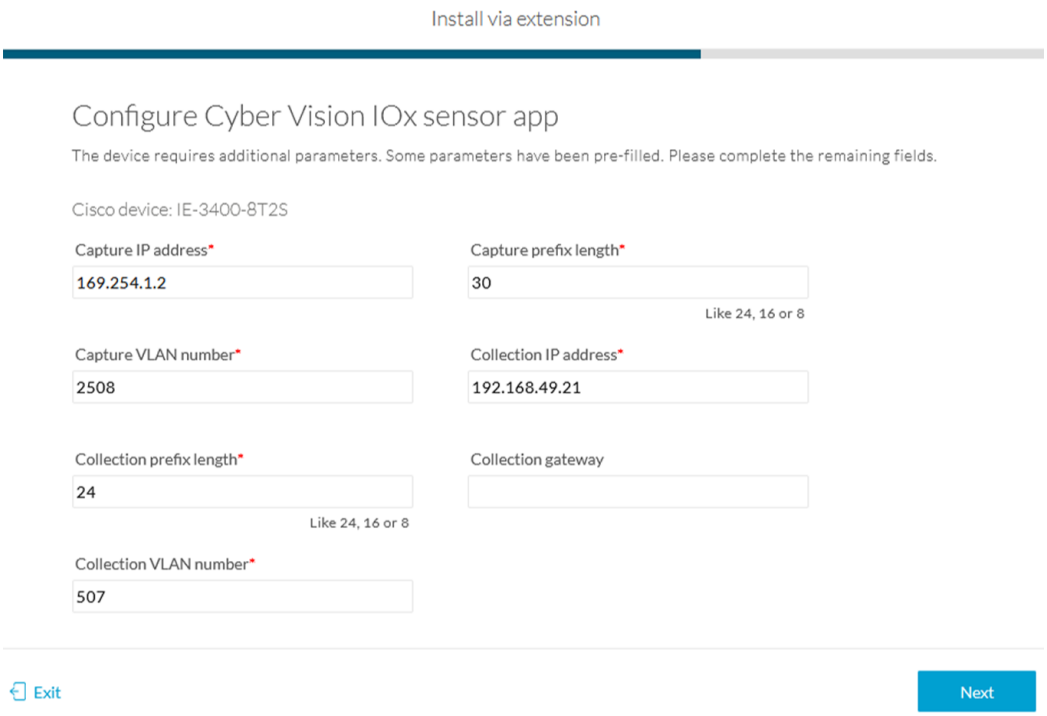
Step 3 Click **Connect**.

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.

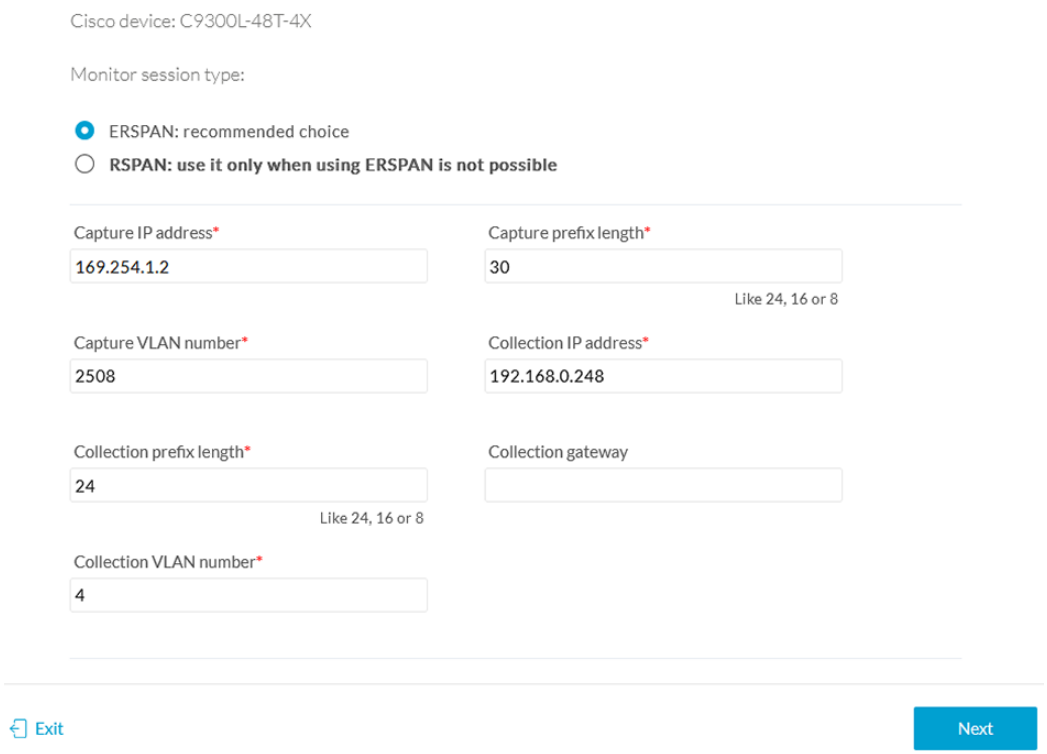
Configure a sensor in the sensor management extension

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

Form for the Cisco IE3x00 and the Cisco IE9x00:



Form for the Cisco Catalyst 9x00 with RSPAN configuration available:



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 sensor
- Capture prefix length: mask of the capture IP address
- Capture VLAN number: VLAN of the monitor session in the sensor
- Collection IP address: IP address of the sensor in the device
- Collection prefix length: mask of the Collection IP address
- Collection gateway: gateway of the Collection IP address
- Collection VLAN number: VLAN of the sensor

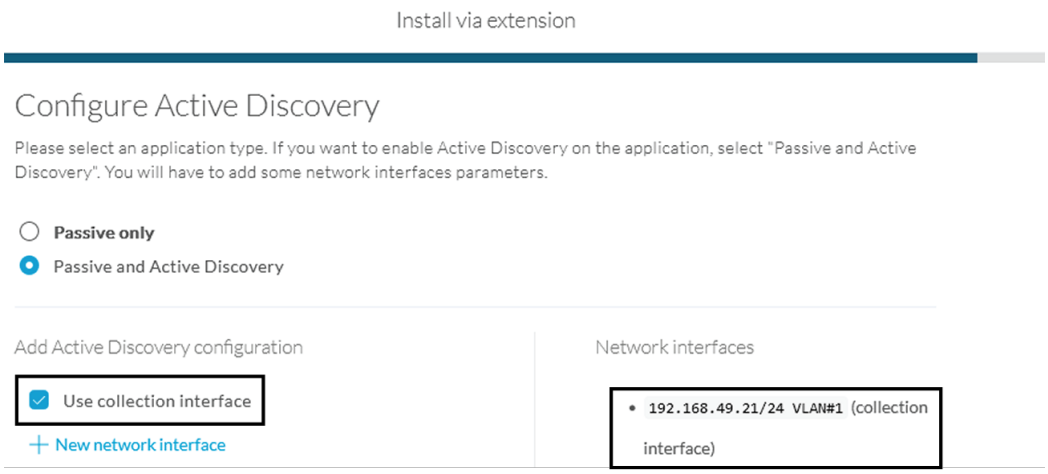
Step 2 Click **Next**.

Step 3 **Active Discovery:**

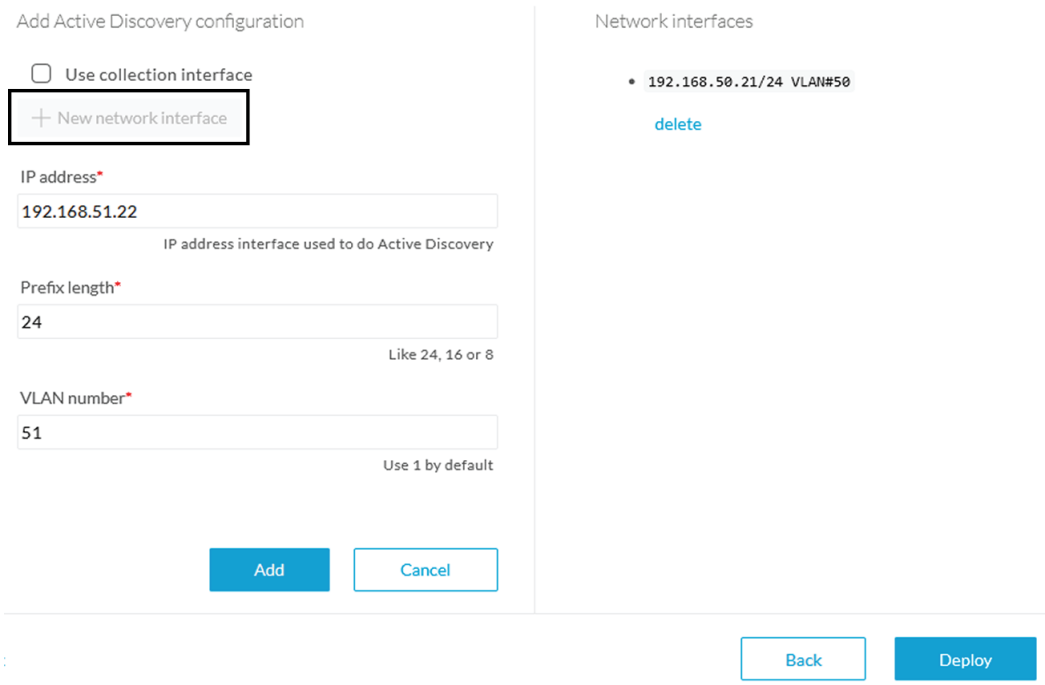
If you want to enable Active Discovery on the sensor, select **Passive and Active Discovery**.

You can:

- use the sensor Collection interface by selecting it:

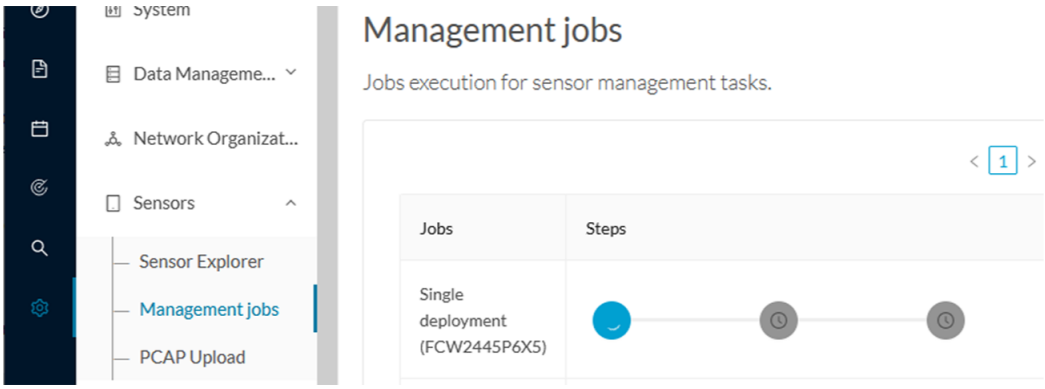


- add new network interfaces filling the following parameters to set dedicated network interfaces and clicking Add:
  - IP address
  - Prefix length
  - VLAN number



Step 4 Click **Deploy**.

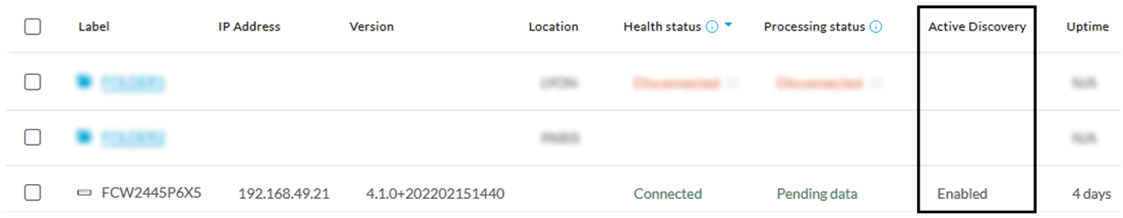
The Center starts deploying the sensor application on the target equipment. This can take a few minutes. You can go to the Management jobs page to check the deployment advancements.



Once the deployment is finished, a new sensor appears in the sensors list.

The sensor's status will eventually turn to connected.

If the Active Discovery has been enabled and set -that is if the option **Passive and Active Discovery** was selected when configuring the sensor in the sensor management extension- the sensor is displayed as below with Active Discovery's status as Enabled.

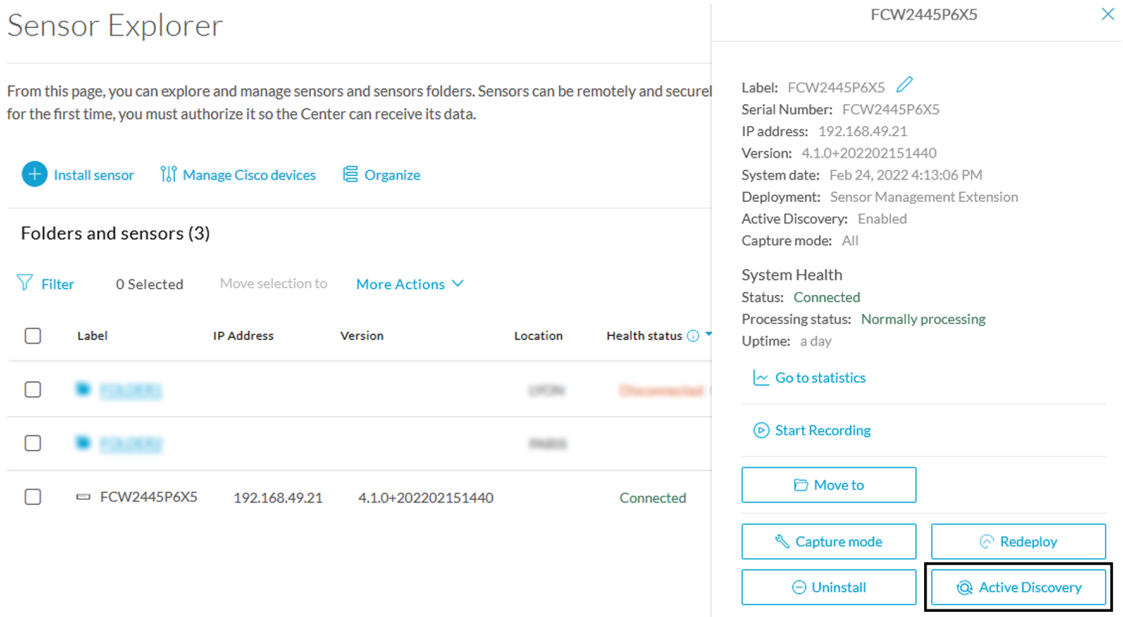


Configure Active Discovery

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.

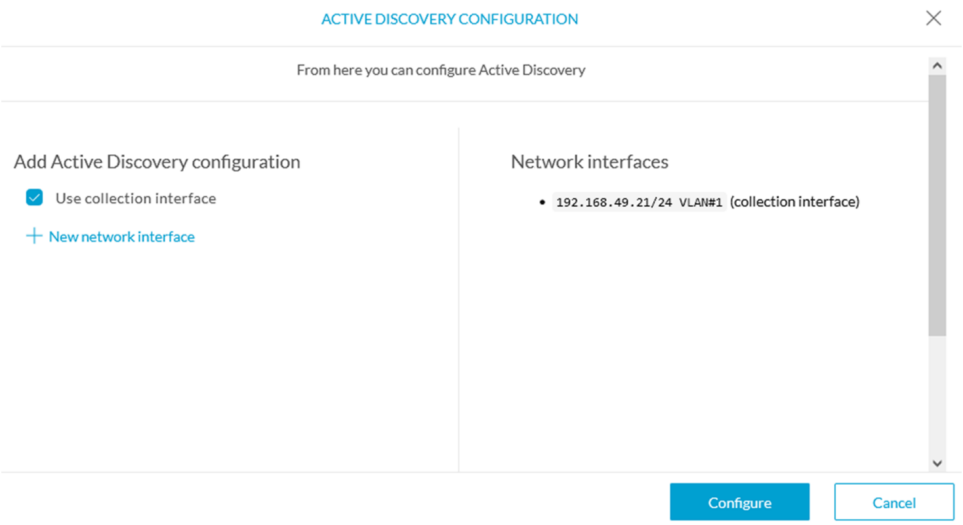
Procedure

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



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.



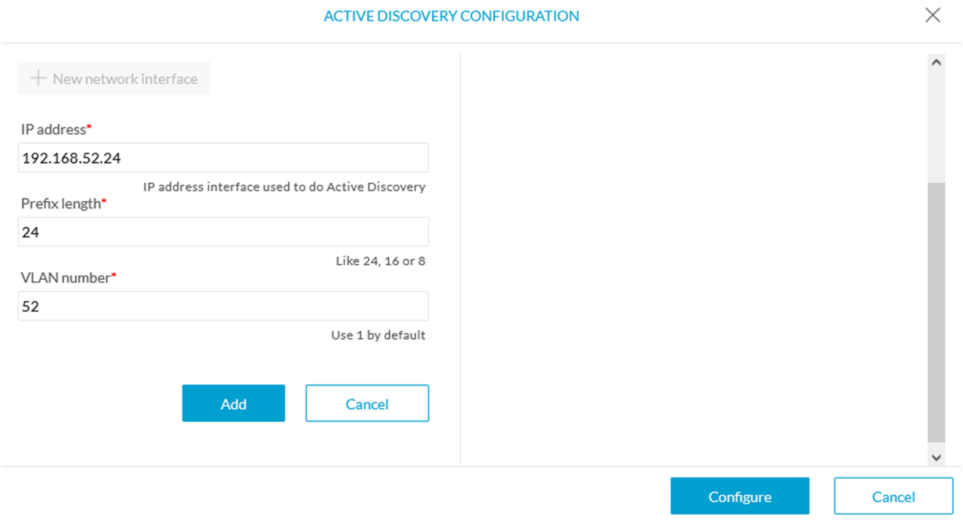
To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

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**.



You can add as many network interfaces as needed.

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

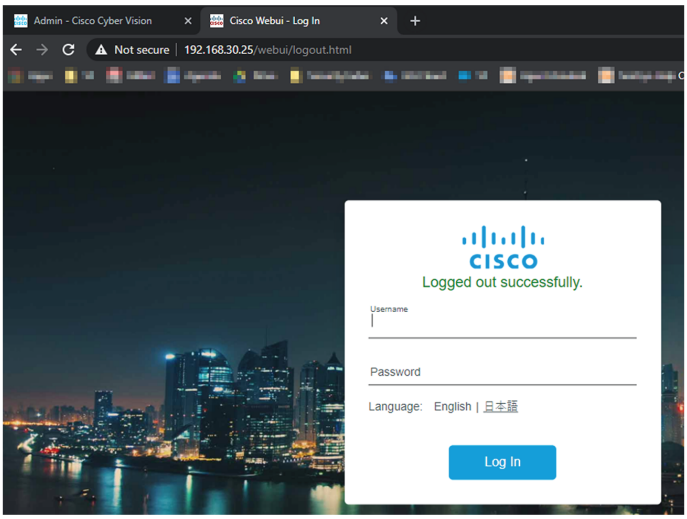
A message saying that the configuration has been applied successfully appears.

Procedure with the Local Manager

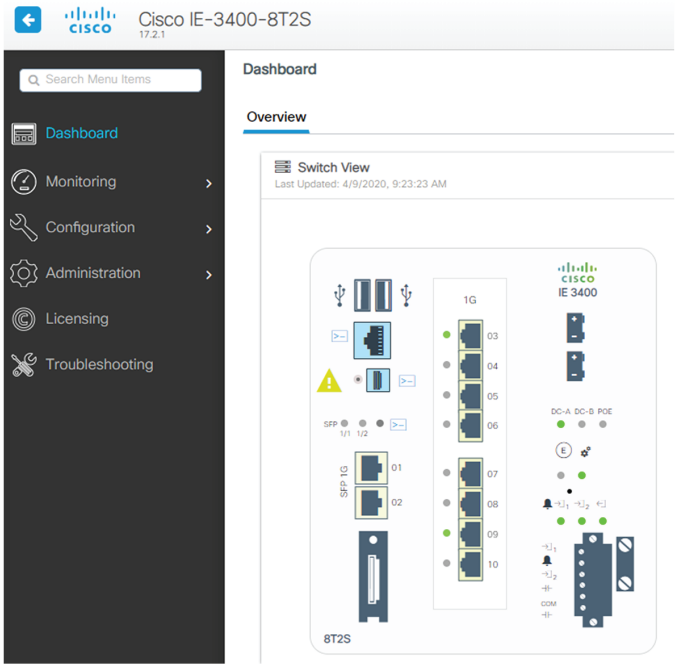
After the Initial configuration, on page 13, proceed to the steps described in this section.

Access the 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 Local Manager user account and password.

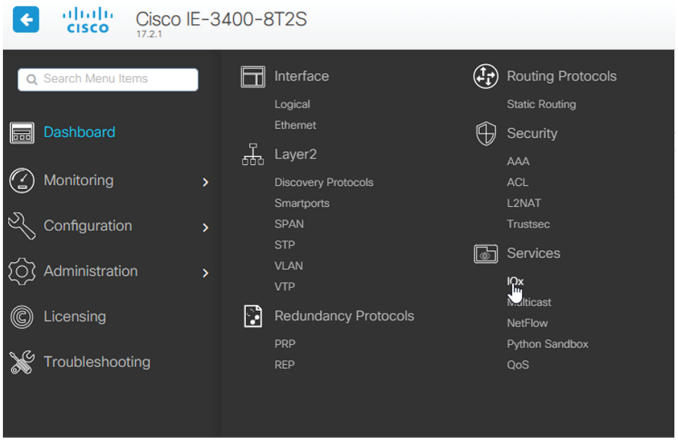


For example: Cisco IE3300 10G/IE3400

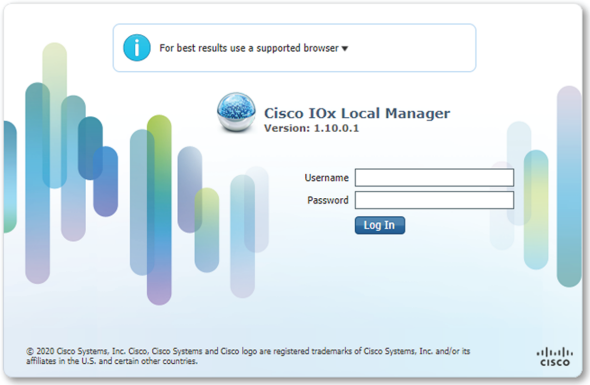


3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.

   For example: Cisco IE3300 10G/IE3400

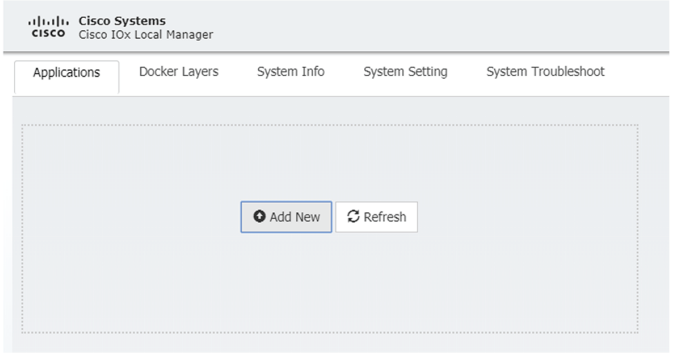


4. Log in using the user account and password.

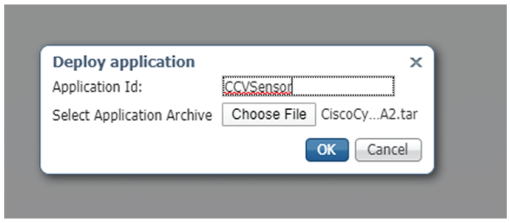


Install the sensor virtual application

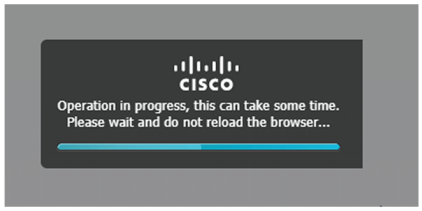
Once logged in, the following menu appears:



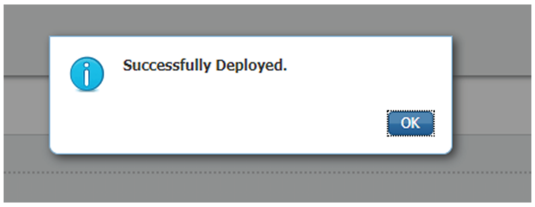
1. Click **Add New**.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file
   - "CiscoCyberVision-IOx-aarch64-xxx.tar" for the Cisco IE3300/IE3400/IE9300
   - "CiscoCyberVision-IOx-Active-Discovery-aarch64.tar" for the Cisco IE3300/IE3400/IE9300 with Active Discovery
   - "CiscoCyberVision-IOx-x86-64-xxx.tar" for the Cisco Catalyst 9300
   - "CiscoCyberVision-IOx-Active-Discovery-x86-64.tar" for the Cisco Catalyst 9300



The installation takes a few minutes.

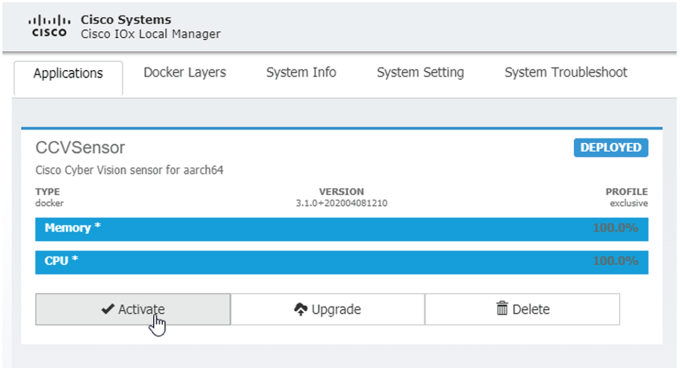


When the application is installed, the following message is displayed:

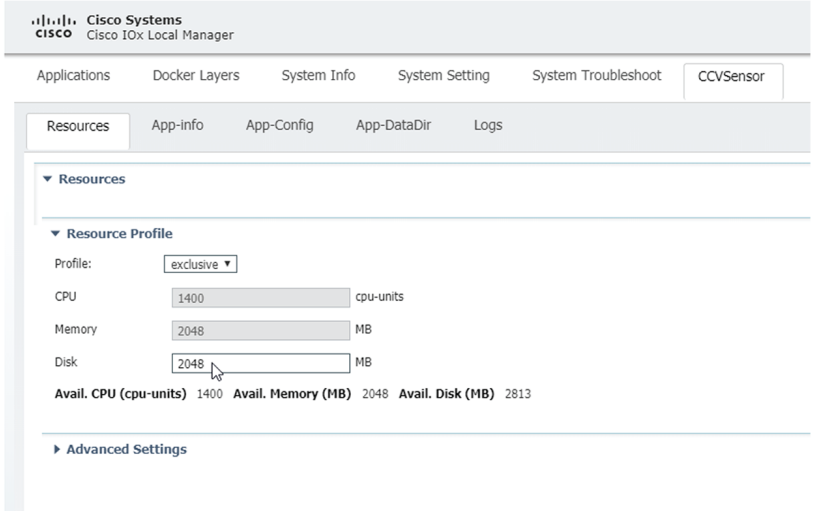


Configure the sensor virtual application (IE3x00/IE9x00)

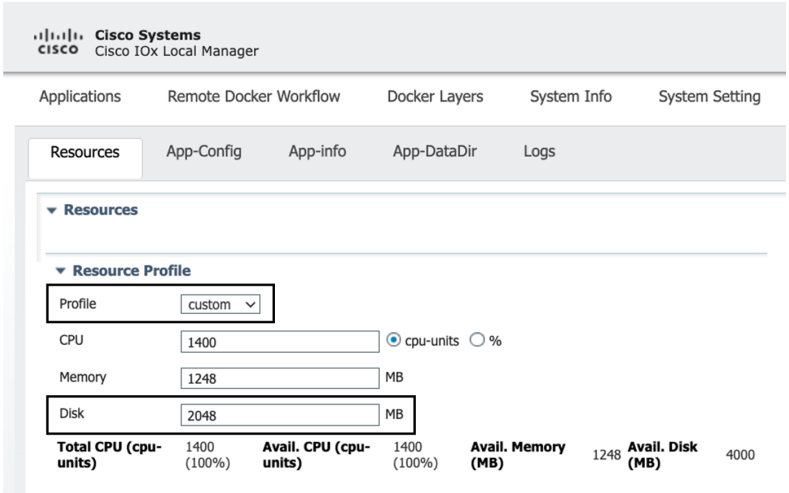
1. Click **Activate** to launch the configuration of the sensor application.



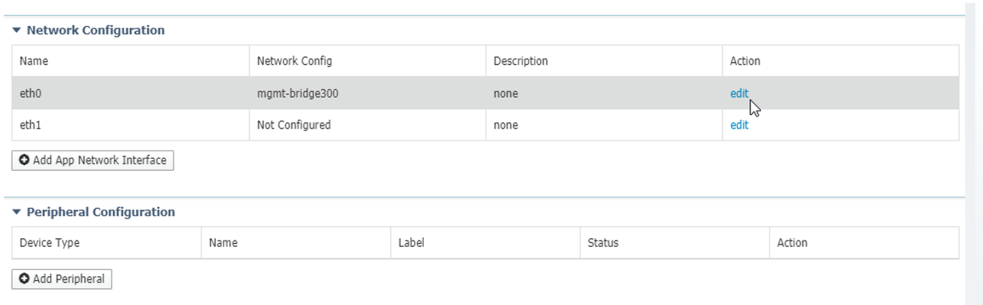
2. Change the disk size from the default size to **1248 MB**. The disk size must **not** be larger than this.



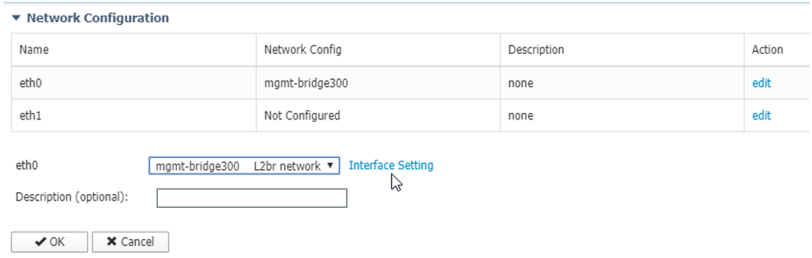
If the field is grayed out, change the profile to **custom** to change the disk value.



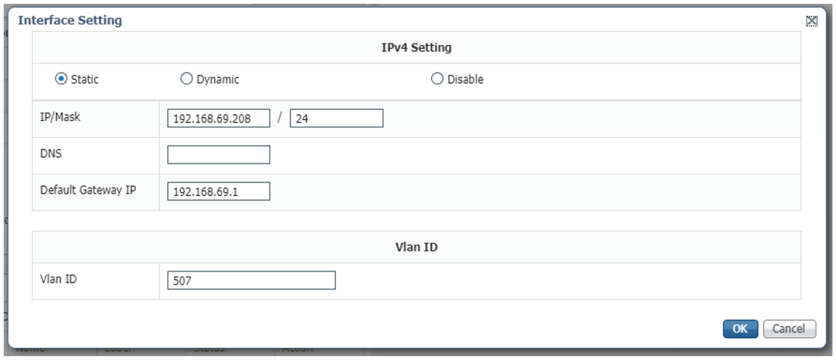
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking **edit** in the eth0 line.



4. Click **Interface Setting**.

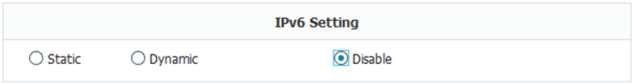


5. Apply the following configurations:
   - Select **Static**
   - IP/Mask: IP and mask of the sensor
   - Default gateway: IP address of the Center
   - Vlan ID, which is defined below, is the VLAN in the Cisco IE3300 10G/IE3400 dedicated to the Collection network interface (link between the Center and the sensors), e.g. 507.

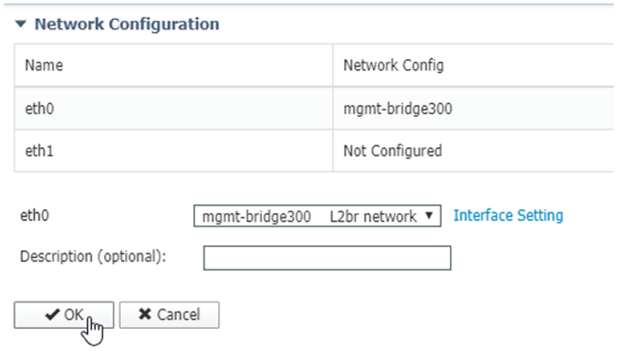


When using l3nat-iox, you need to fill in the collection information with L3 NAT details, and the default gateway IP is the switch SVI address on the collection VLAN.

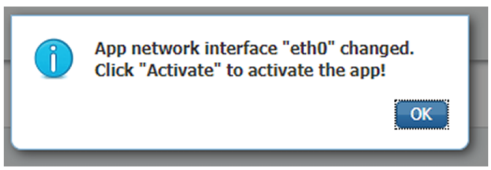
6. IPV6 must be set to Disable.



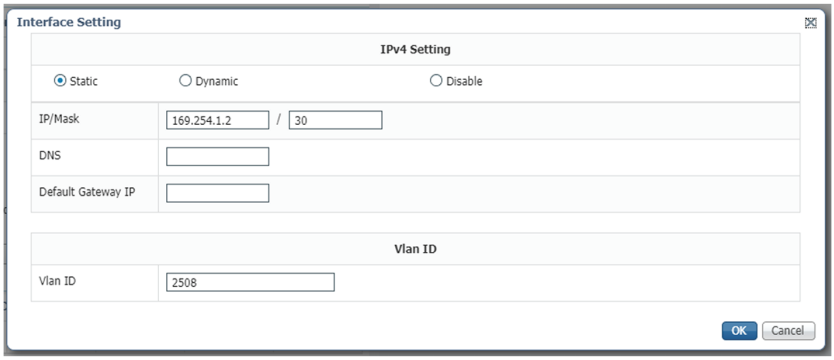
7. Click **OK** twice.



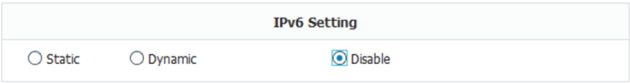
8. Click **OK** again on the popup.



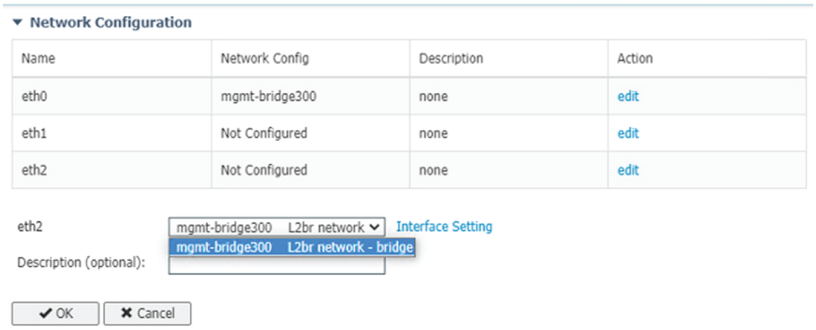
9. Then, apply the following parameters to eth1:
   - Select **Static**.
   - IP/Mask: the IP and mask of the sensor for the mirrored traffic.
   - Vlan ID, which is defined below, is the VLAN in the Cisco IE3300 10G/IE3400/IE9300 dedicated to traffic mirroring.



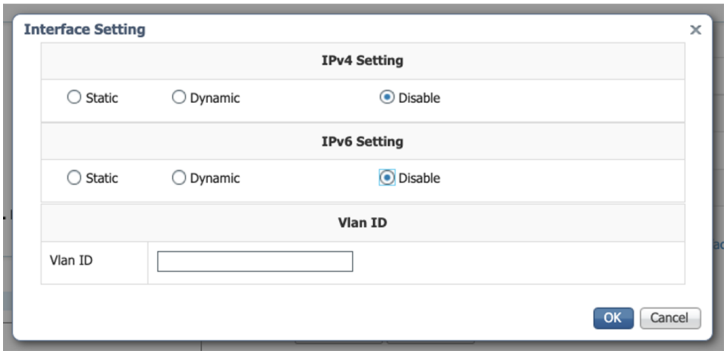
10. IPV6 must be set to **Disable**.



11. If configuring a sensor with **Active Discovery**, you must set an additional interface (eth2 without IP address) dedicated to this feature.

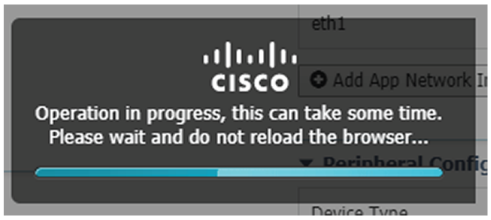


12. Click **Interface Setting** for eth2 and set IPV4 and IPV6 as Disable. Click **OK** to confirm.

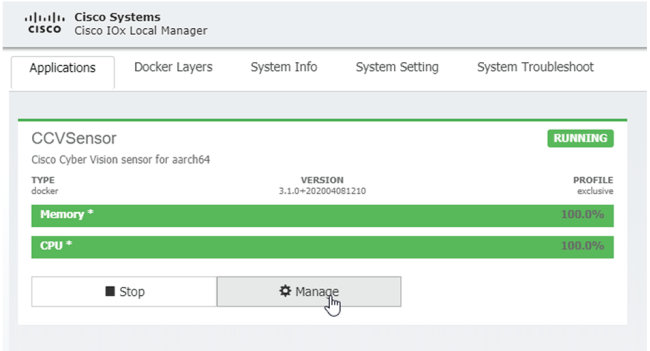


13. Click the **Activate App** button.

The operation takes several minutes.

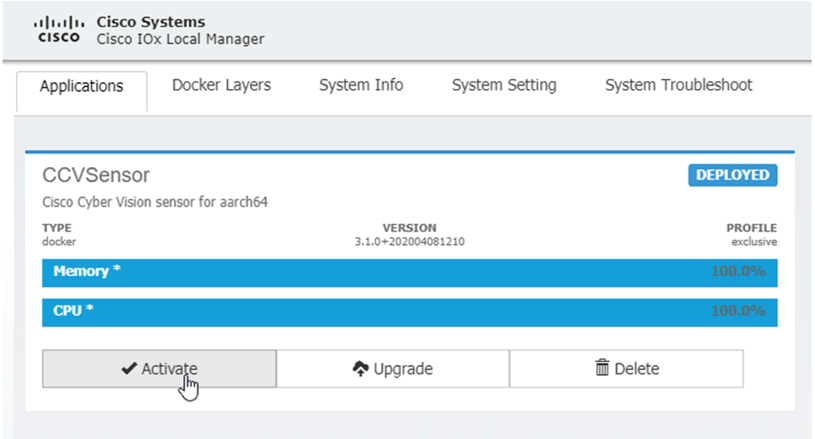


The application status changes to "RUNNING":

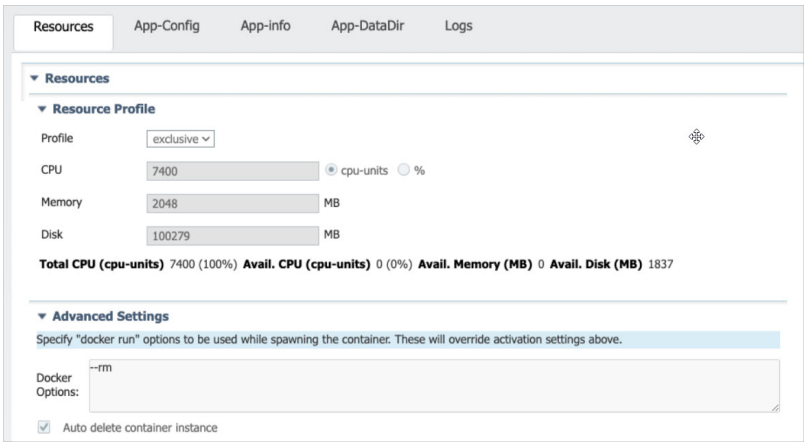


Configure the sensor virtual application (Catalyst 9x00)

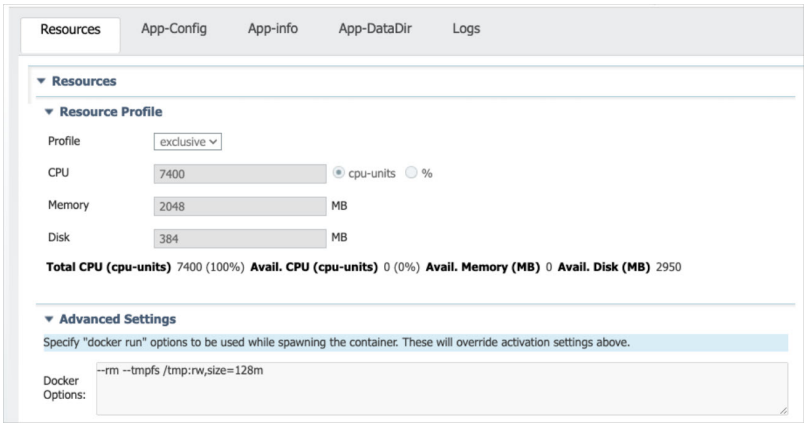
1. Click **Activate** to launch the configuration of the sensor application.



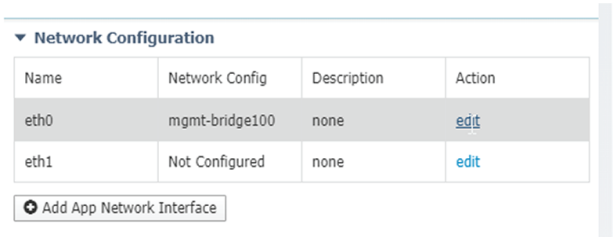
2. Change the resource profile and advanced setting:
   - If you are using SSD:
     a. Change the disk size to at least 80,000 MB and it should not be smaller than that.
     b. Add "--rm" in advanced settings - Docker options.



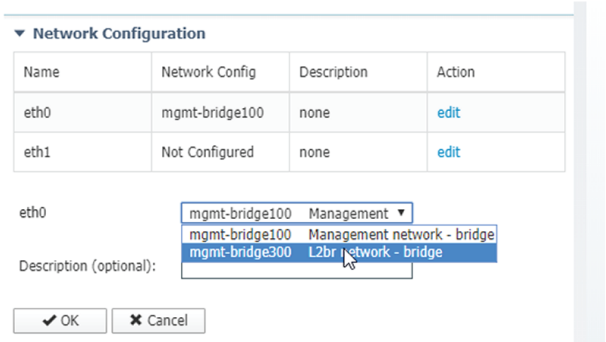
- If you are not using SSD:
  a. Change the disk size from the default size to 384 MB.
  b. Add “--rm --tmpfs /tmp:rw,size=128m” in Advanced Settings – Docker Options.



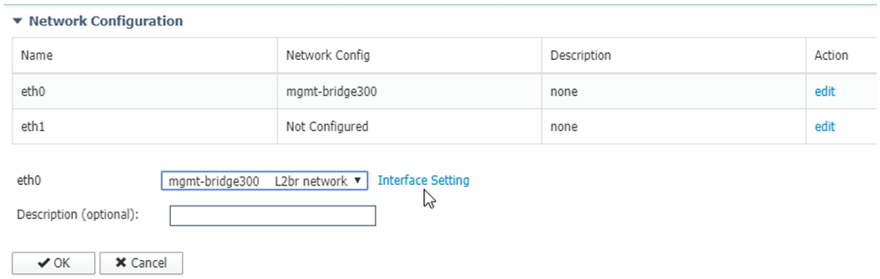
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking **edit** in the eth0 line.



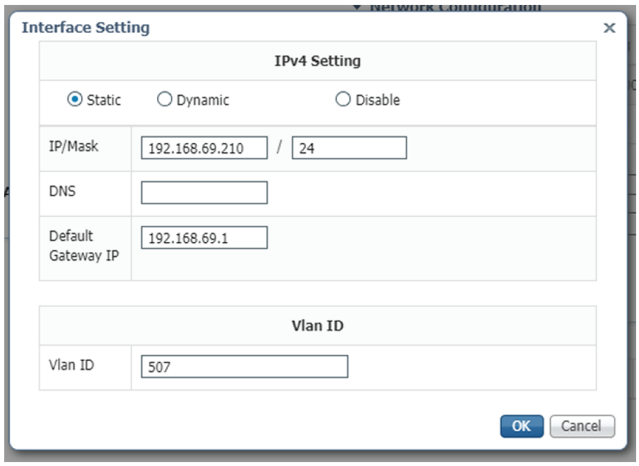
4. Select the mgmt-bridge300 entry in the interface list.



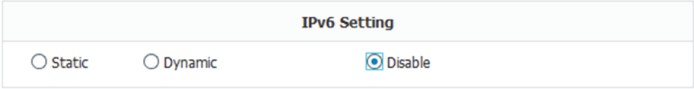
5. Click **Interface Setting**.



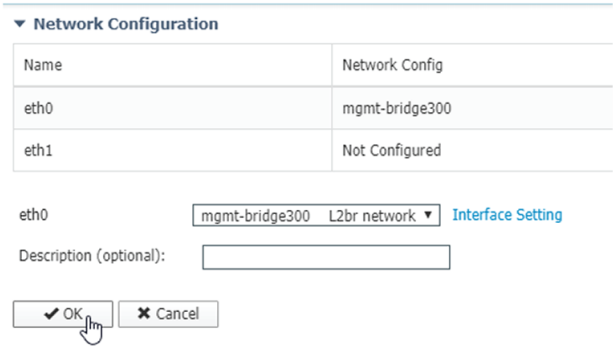
6. Apply the following configurations:
   - Select **Static**
   - IP/Mask: the IP and mask of the sensor
   - Default gateway: the IP address of the Center
   - Vlan ID, which is defined below, is the VLAN in the Cisco Catalyst 9300 dedicated to the Collection network interface (link between the Center and the sensors), e.g. 507.



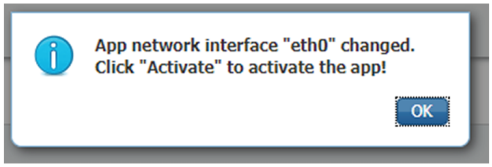
7. IPV6 must be set to **Disable**.



8. Click **OK** twice.



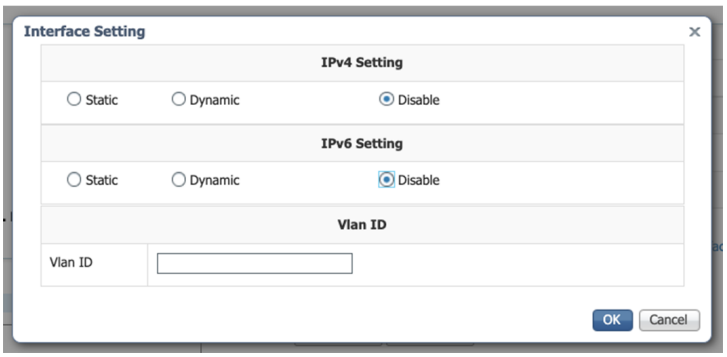
9. Click **OK** again on the following popup.



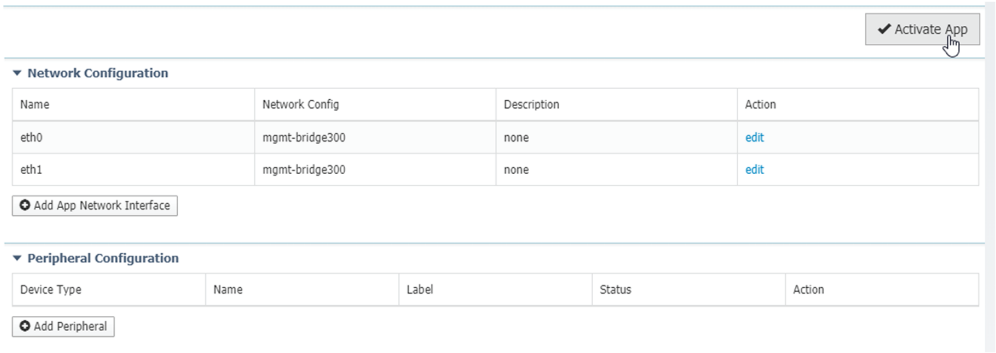
10. Apply the following configurations to eth1:
    - Set IPv4 as **Static** and the IP and mask of the sensor for mirrored traffic.
    - Disable IPv6.
    - Set the VLAN id.
    - **Set the mirror mode as enabled**.

11. Click **OK** until you come back to the screen below.

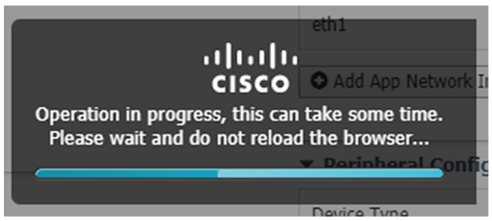
12. If configuring a sensor with **Active Discovery**, you must set an additional interface (eth2 without IP address) dedicated to this feature. Then, click **Interface Setting** for eth2 and set IPV4 and IPV6 as Disable. Click **OK** to confirm.



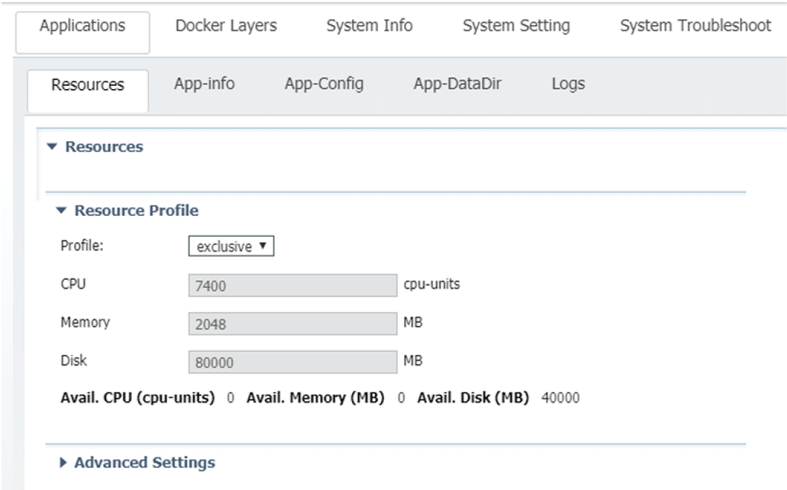
13. Click the **Activate App** button.



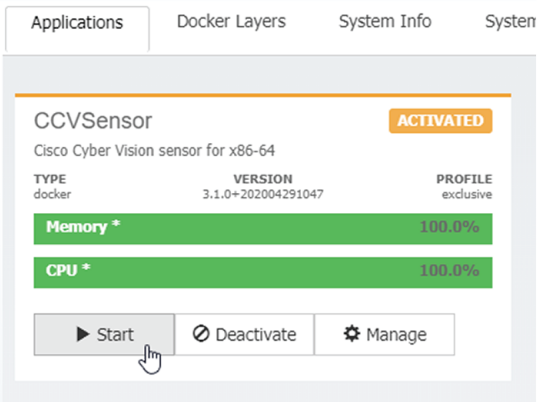
The operation takes several seconds.



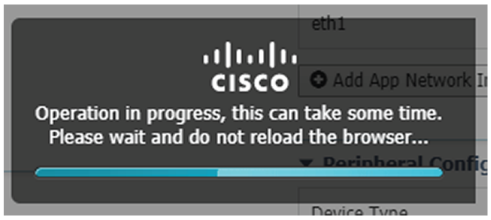
14. Click **Applications** to display the application status:



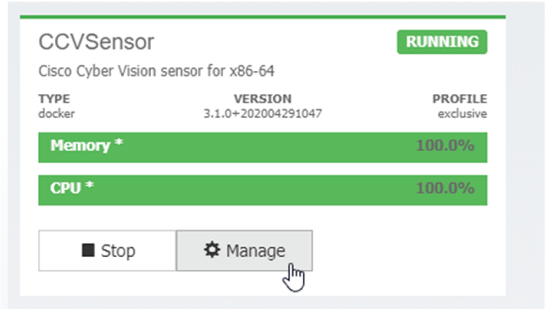
15. The application is activated and needs to be started. To do so, click the **Start** button.



The operation takes several seconds.

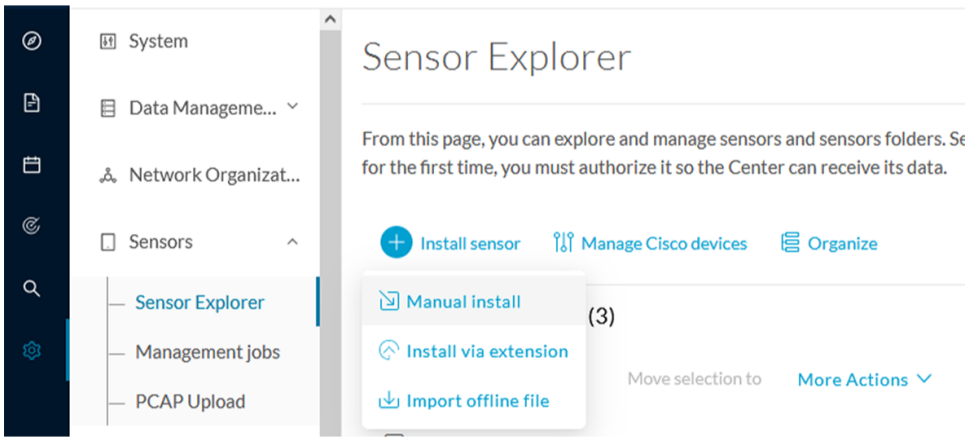


The application status changes to "RUNNING".



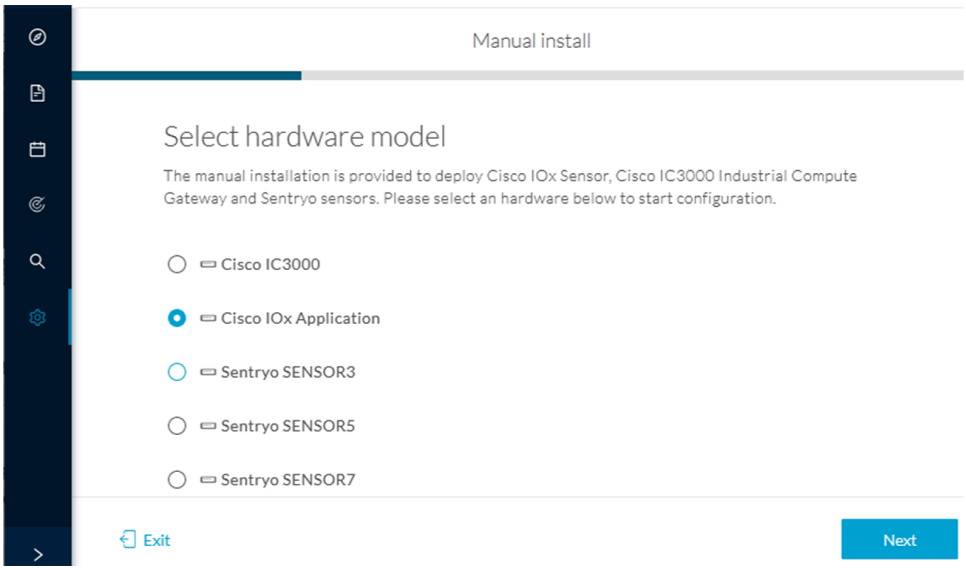
Generate the provisioning package

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

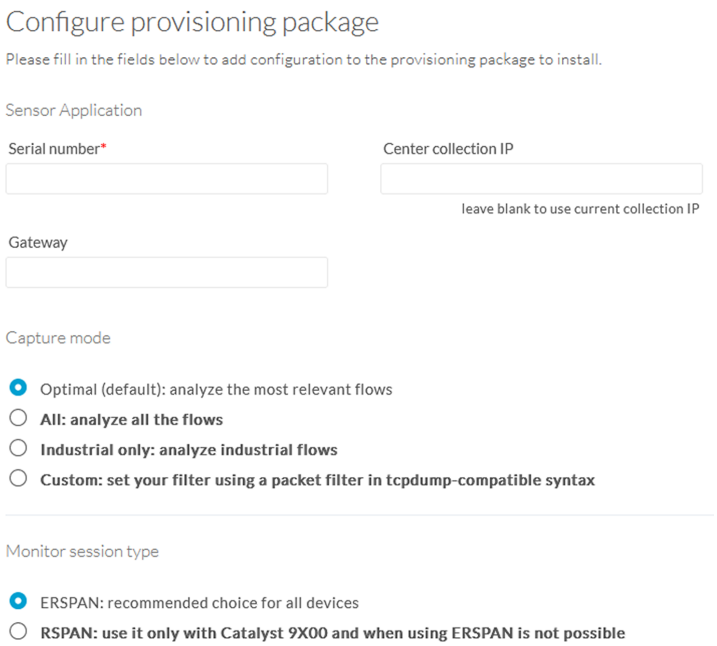


   The manual install wizard appears.

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

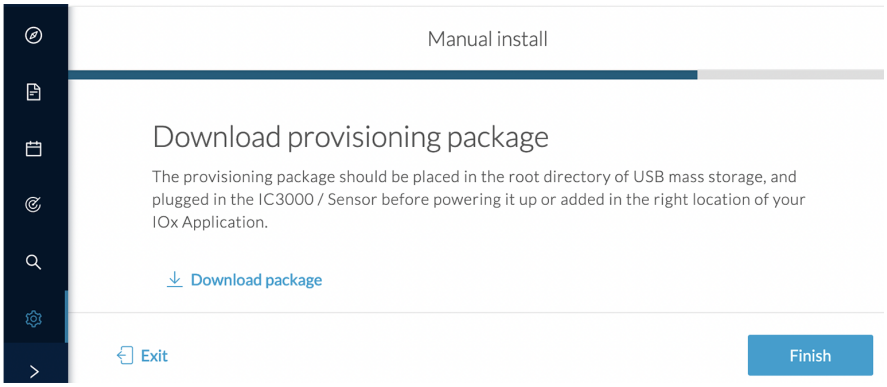


3. Fill the fields to configure the sensor provisioning package:
   - The serial number of the hardware.
   - Center IP: leave blank.
   - Gateway: add if necessary.
   - Optionally, select a capture mode.
   - Optionally, select RSPAN (only with Catalyst 9x00 and if using ERSPAN is not possible).



4. Click **Create sensor**.

5. Click the link to download the provisioning package.

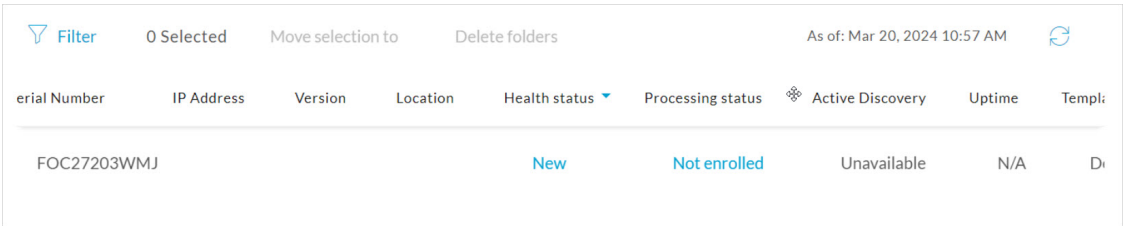


This will download the provisioning package which is a zip archive file with the following name structure: sbs-sensor-config-<serialnumber>.zip (e.g. "sbs-sensor-configFCW23500HDC.zip").

6. Click **Finish**.

7. A new entry for the sensor appears in the Sensor Explorer list.

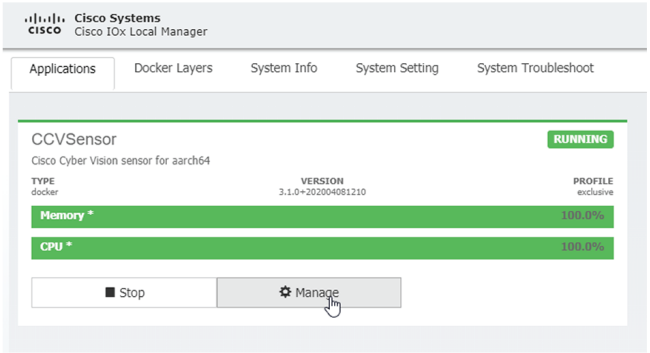
   The sensor status will switch from Disconnected to New.



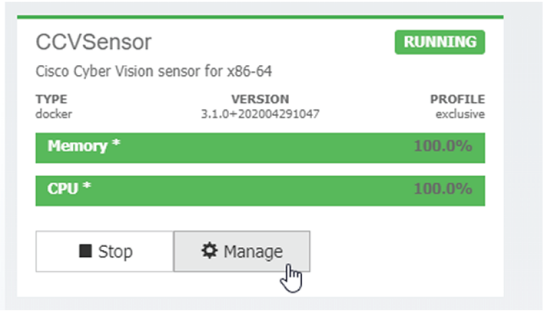
Import the provisioning package

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

   Cisco IE3400:

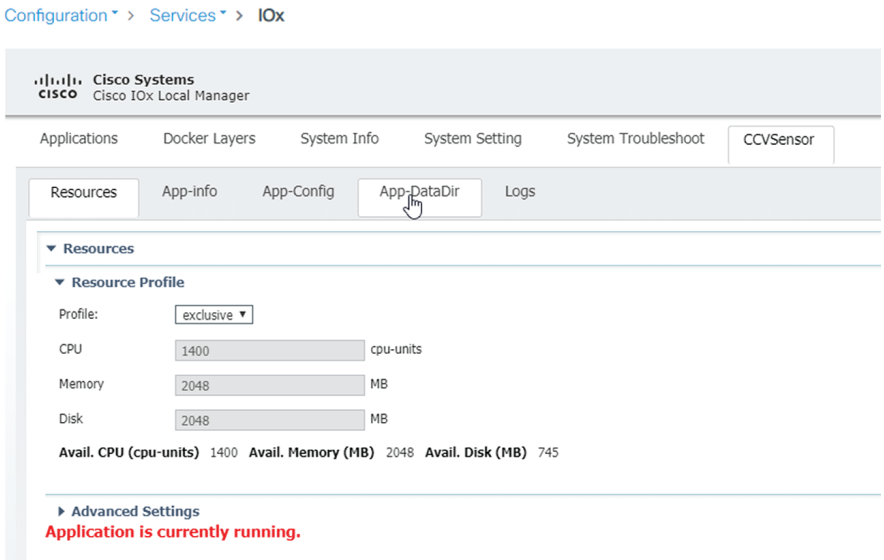


   Cisco Catalyst 9300:

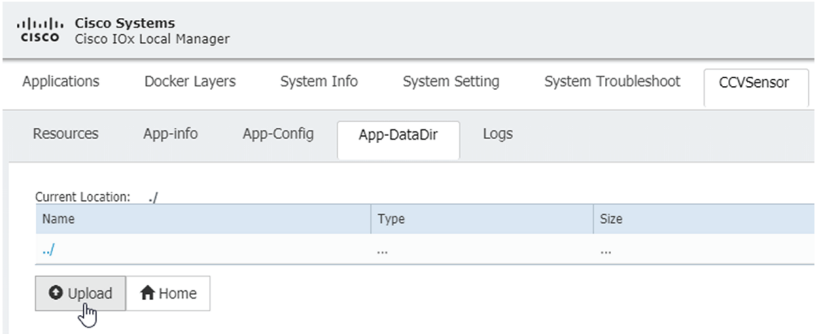


2. Navigate to **App_DataDir**.

   For example Cisco IE3400:

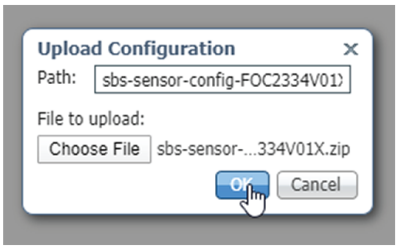


3. Click **Upload**.



4. Choose the provisioning package downloaded (i.e. "sbs-sensor-config-FOC2334V01X.zip") and add the exact file name in the path field (i.e. "sbs-sensor-config-FOC2334V01X.zip").

5. Click **OK**.



A popup indicating that Cisco Cyber Vision has been deployed successfully appears.

6. Click **OK**.

Procedure with the CLI

After the Initial configuration, on page 13, proceed to the steps described in this section.

Configure the sensor application

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

1. Connect to the device through SSH or a console.
2. Configure the application payload by typing the following commands.

   To enable **Active Discovery**, you must add `guest-interface 2` (in bold in the examples below).

   Cisco IE3300 10G/IE3400:

```
enable
configure terminal
app-hosting appid CCVSensor
app-vnic AppGigabitEthernet trunk
guest-interface 2
vlan 507 guest-interface 0
guest-ipaddress 192.168.69.208 netmask 255.255.255.0
vlan 2508 guest-interface 1
guest-ipaddress 169.254.1.2 netmask 255.255.255.0
app-default-gateway 192.168.69.1 guest-interface 0
app-resource profile custom
persist-disk 2048
cpu 1400
memory 1248
vcpu 2
end
```

```
IE3400esc00#
IE3400esc00#enable
IE3400esc00#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE3400esc00(config)#app-hosting appid CCVSensor
IE3400esc00(config-app-hosting)#app-vnic AppGigabitEthernet trunk
IE3400esc00(config-config-app-hosting-trunk)#guest-interface 2
IE3400esc00(config-config-app-hosting-trunk-mode-guest)#vlan 507 guest-interface 0
IE3400esc00(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 192.168.69.208 netmask 255.255.255.0
IE3400esc00(config-config-app-hosting-vlan-access-ip)#vlan 2508 guest-interface 1
IE3400esc00(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 169.254.1.2 netmask 255.255.255.0
IE3400esc00(config-config-app-hosting-vlan-access-ip)#app-default-gateway 192.168.69.1 guest-interface 0
IE3400esc00(config-app-hosting)#app-resource profile custom
IE3400esc00(config-app-resource-profile-custom)#persist-disk 2048
IE3400esc00(config-app-resource-profile-custom)#cpu 1400
IE3400esc00(config-app-resource-profile-custom)#memory 1248
IE3400esc00(config-app-resource-profile-custom)#vcpu 2
IE3400esc00(config-app-resource-profile-custom)#end
IE3400esc00#
IE3400esc00#
IE3400esc00#
```

When using l3nat-iox you need to fill in collection information with L3 NAT information, and the **app-default-gateway** is the switch SVI address on the collection vlan. For example,

```
app-default-gateway 169.254.0.1 guest-interface 0
```

Cisco IE9300:

```
enable
configure terminal
app-hosting appid CCVSensor
 app-vnic AppGigabitEthernet trunk
guest-interface 2
  vlan 507 guest-interface 0
   guest-ipaddress 192.168.69.90 netmask 255.255.255.0
  vlan 2508 guest-interface 1
   guest-ipaddress 169.254.1.2 netmask 255.255.255.252
 app-default-gateway 192.168.69.190 guest-interface 0
 app-resource docker
  run-opts 1 --rm
 app-resource profile custom
  cpu 1000
  memory 862
  persist-disk 4000
end
```

```
IE9300_1#
IE9300_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE9300_1(config)#app-hosting appid CCVSensor
IE9300_1(config-app-hosting)#app-vnic AppGigabitEthernet trunk
IE9300_1(config-config-app-hosting-trunk)#vlan 507 guest-interface 0
IE9300_1(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 192.168.69.90 netmask 255.255.255.0
IE9300_1(config-config-app-hosting-vlan-access-ip)#vlan 2508 guest-interface 1
IE9300_1(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 169.254.1.2 netmask 255.255.255.252
IE9300_1(config-config-app-hosting-vlan-access-ip)#app-default-gateway 192.168.69.190 guest-interface 0
IE9300_1(config-app-hosting)#app-resource docker
IE9300_1(config-app-hosting-docker)#run-opts 1 "--rm"
IE9300_1(config-app-hosting-docker)#app-resource profile custom
IE9300_1(config-app-resource-profile-custom)#cpu 1000
IE9300_1(config-app-resource-profile-custom)#memory 862
IE9300_1(config-app-resource-profile-custom)#persist-disk 4000
IE9300_1(config-app-resource-profile-custom)#end
IE9300_1#
```

Cisco Catalyst 9300:

```
enable
configure terminal
app-hosting appid CCVSensor
app-vnic AppGigabitEthernet trunk
guest-interface 2
```

```
vlan 507 guest-interface 0
guest-ipaddress 192.168.69.210 netmask 255.255.255.0
vlan 2508 guest-interface 1
mirroring
guest-ipaddress 169.254.1.2 netmask 255.255.255.0
app-default-gateway 192.168.69.1 guest-interface 0
app-resource profile custom
persist-disk 8192
cpu 7400
memory 2048
vcpu 2
end
```

```
CAT9KCCV#
CAT9KCCV#enable
CAT9KCCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT9KCCV(config)#app-hosting appid CCVSensor
CAT9KCCV(config-app-hosting)#app-vnic AppGigabitEthernet trunk
CAT9KCCV(config-config-app-hosting-trunk)#vlan 507 guest-interface 0
CAT9KCCV(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 192.168.69.210 netmask 255.255.255.0
CAT9KCCV(config-config-app-hosting-vlan-access-ip)#vlan 2508 guest-interface 1
CAT9KCCV(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 169.254.1.2 netmask 255.255.255.0
CAT9KCCV(config-config-app-hosting-vlan-access-ip)#app-default-gateway 192.168.69.1 guest-interface 0
CAT9KCCV(config-app-hosting)#app-resource profile custom
CAT9KCCV(config-app-resource-profile-custom)#persist-disk 8192
CAT9KCCV(config-app-resource-profile-custom)#cpu 7400
CAT9KCCV(config-app-resource-profile-custom)#memory 2048
CAT9KCCV(config-app-resource-profile-custom)#vcpu 2
CAT9KCCV(config-app-resource-profile-custom)#end
CAT9KCCV#
```

For the app-resource profile's custom values, refer to the result of the show app-hosting resource command.

In this example, all maximum values are used for:

- the CPU (CPU available units, here 1400 for the Cisco IE3300 10G/IE3400, 1000 for the Cisco IE9300, and 7400 for the Cisco Catalyst 9300)
- the VCPU (here 2), the memory (Memory available, here 2048)
- the disk (only 2048 MB and 8192 MB respectively are used to let space for application updates)

Install the sensor application

The sensor package is to be retrieved on cisco.com. The file has the following name structure:

- CiscoCyberVision-IOx-aarch64-<VERSION>.tar (Cisco IE3300 10G/IE3400/IE9300).
- CiscoCyberVision-IOx-x86-64-<VERSION>.tar (Cisco Catalyst 9300).

1. Copy the package to a USB key or in the flash memory.
2. Type the following commands on the CLI:

   ```
   enable
   app-hosting install appid CCVSensor package usbflash0:<FILENAME>.tar
   ```

   Cisco IE3300 10G/IE3400/IE9300:

   ```
   IE340CCV#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.

   IE340CCV#
   ```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#enable
CAT9KCCV#app-hosting install appid CCVSensor package usbflash0:CiscoCyberVision-IOx-x86-64-3.1.0-RC4.tar
Installing package 'usbflash0:CiscoCyberVision-IOx-x86-64-3.1.0-RC4.tar' for 'CCVSensor'. Use 'show app-hosting list' fo
r progress.

CAT9KCCV#
```

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

Note Replace "CiscoCyberVision-IOx-aarch64-<VERSION>.tar" with the right filename.

3. Check that the application is in "DEPLOYED" state:

   `show app-hosting list`

   For example: Cisco IE3400

```
IE340CCV#
IE340CCV#show app-hosting list
App id                                    State
---------------------------------------------------------
CCVSensor                                 DEPLOYED

IE340CCV#
```

4. Activate the application using the following command:

   `app-hosting activate appid CCVSensor`

   For example: Cisco IE3400

```
IE340CCV#app-hosting activate appid CCVSensor
CCVSensor activated successfully
Current state is: ACTIVATED

IE340CCV#
```

5. Start the application using the following command:

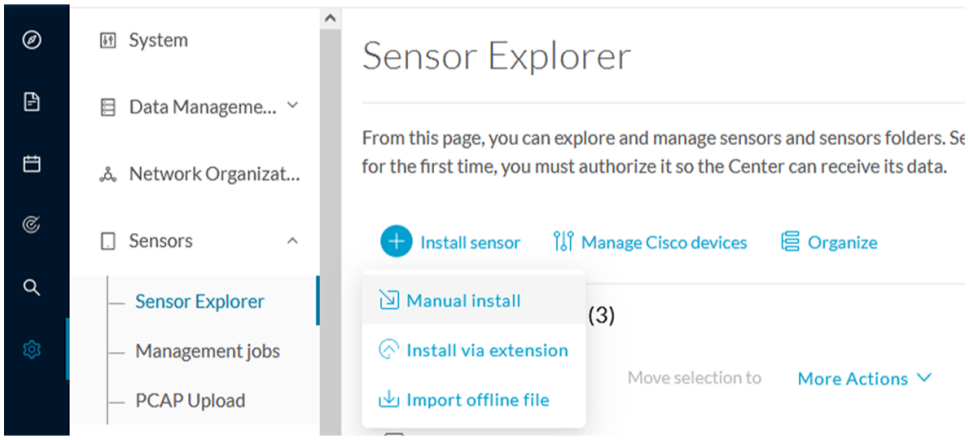
   `app-hosting start appid CCVSensor`

   For example: Cisco IE3400:

```
IE340CCV#
IE340CCV#app-hosting start appid CCVSensor
CCVSensor started successfully
Current state is: RUNNING
IE340CCV#
```

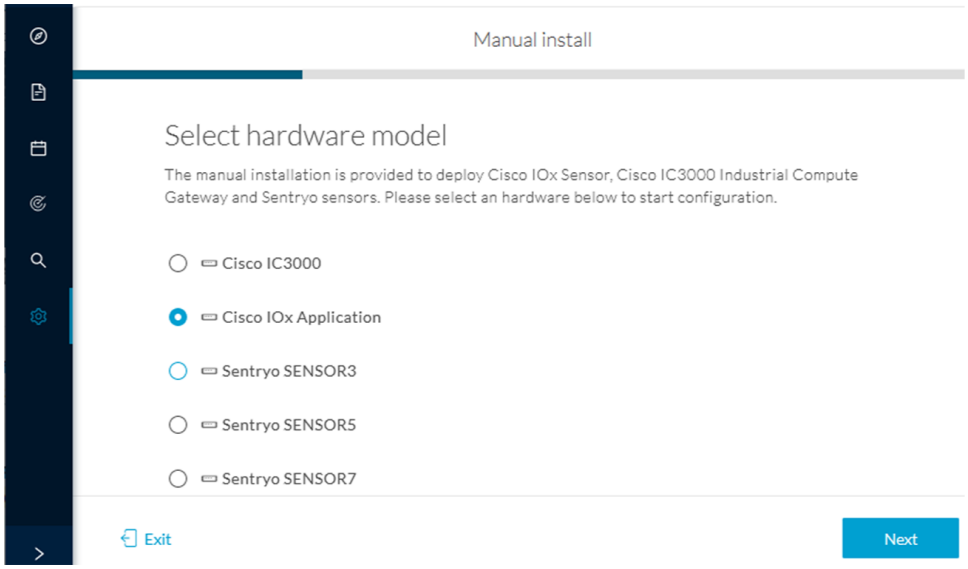
Generate the provisioning package

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

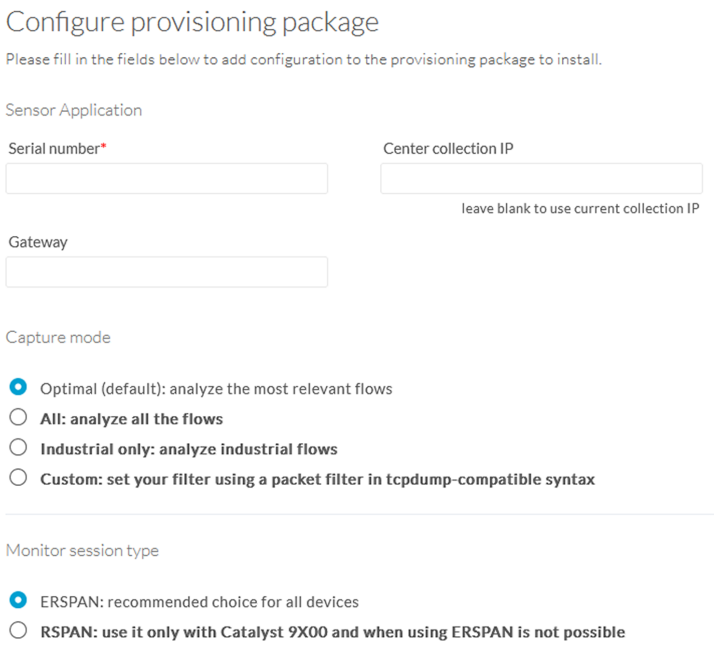


The manual install wizard appears.

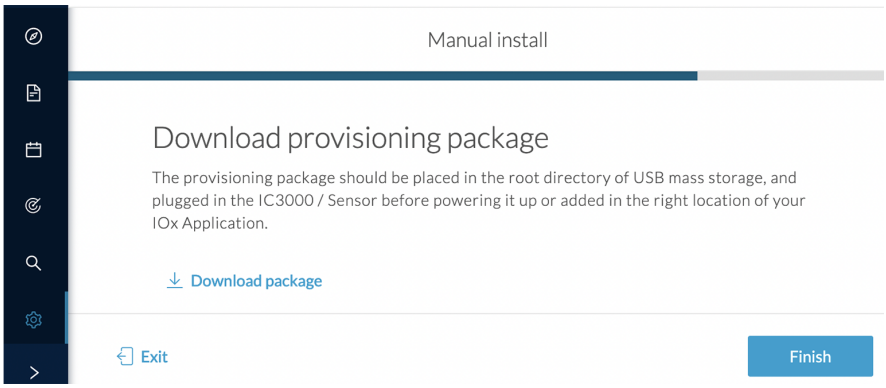
2. Select **Cisco IOx Application** and click **Next**.



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).



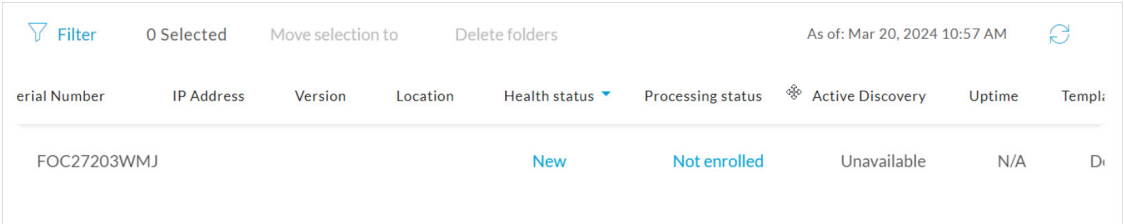
4. Click **Create sensor**.
5. Click the link to download the provisioning package.



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 New.



Copy the sensor application provisioning package

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

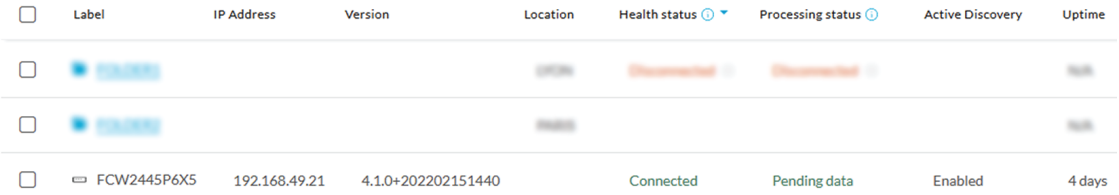
  ```
  app-hosting data appid CCVSensor copy usbflash0:sbs-sensor-config-<SERIAL-NUMBER>.zip
  sbs-sensor-config-<SERIAL-NUMBER>.zip
  ```

  For example: Cisco IE3400

  ```
  IE340CCV#
  IE340CCV#$ data appid CCVSensor copy usbflash0:sbs-sensor-config-FOC2334V01X.zip sbs-sensor-config-FOC2334V01X.zip
  Successfully copied file /usbflash0/sbs-sensor-config-FOC2334V01X.zip to CCVSensor as sbs-sensor-config-FOC2334V01X.zip
  IE340CCV#
  ```

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

  The sensor status will switch from Disconnected to Connected.

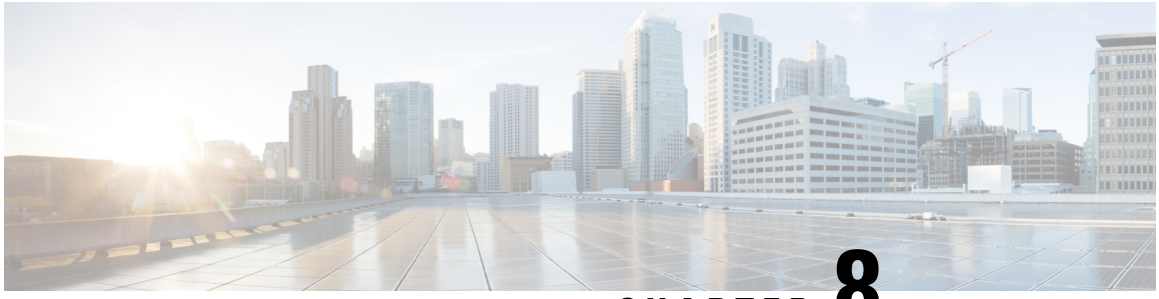


Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
[illegible]			[illegible]	[illegible]	[illegible]		[illegible]
[illegible]			[illegible]				[illegible]
FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days

Final step

In the sensor's CLI save the product's configuration by typing the following command:

```
write mem
```



CHAPTER 8

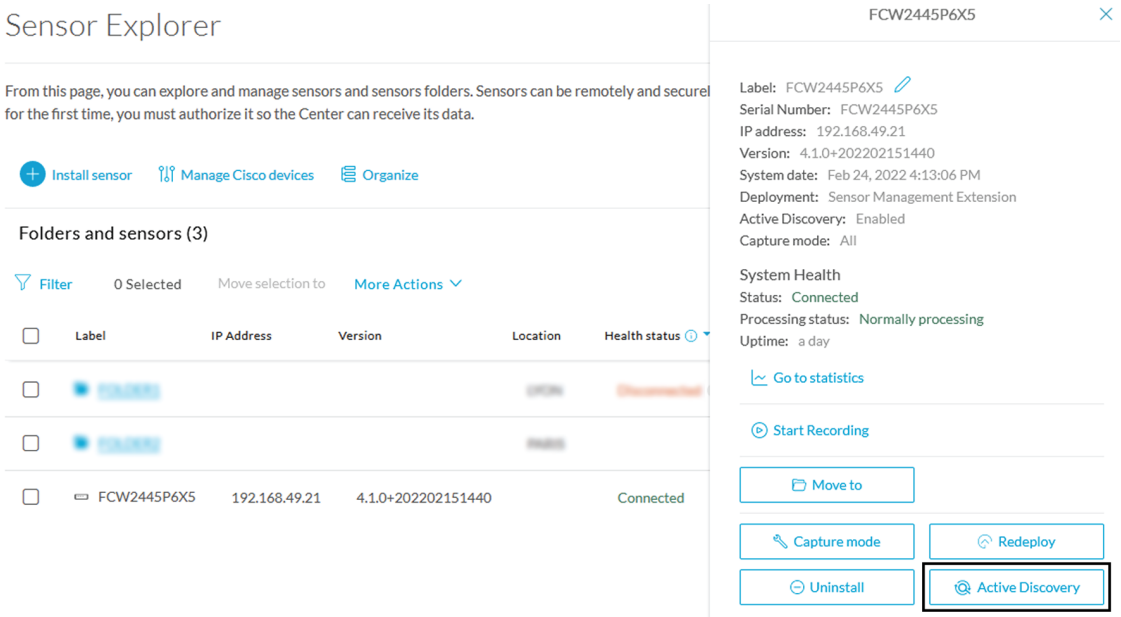
Configuration

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.

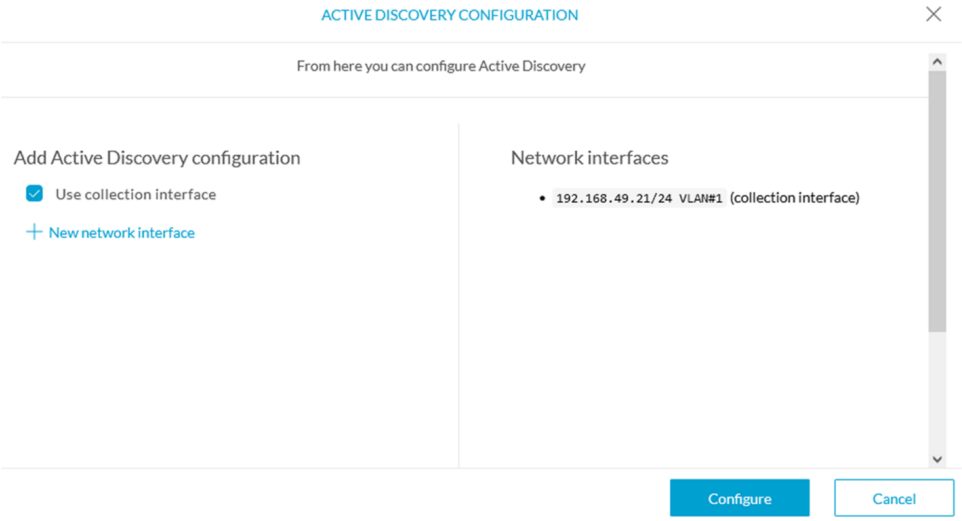
Procedure

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



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.



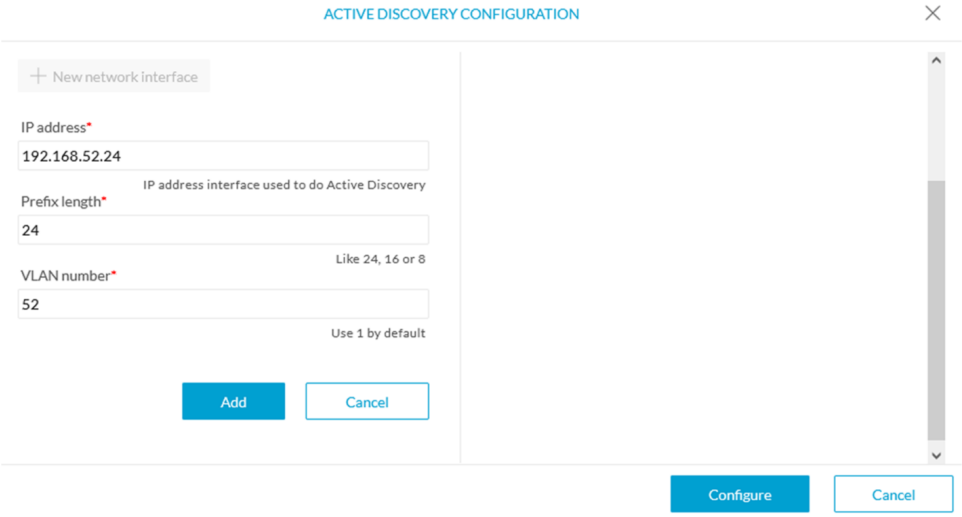
To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

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**.



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:

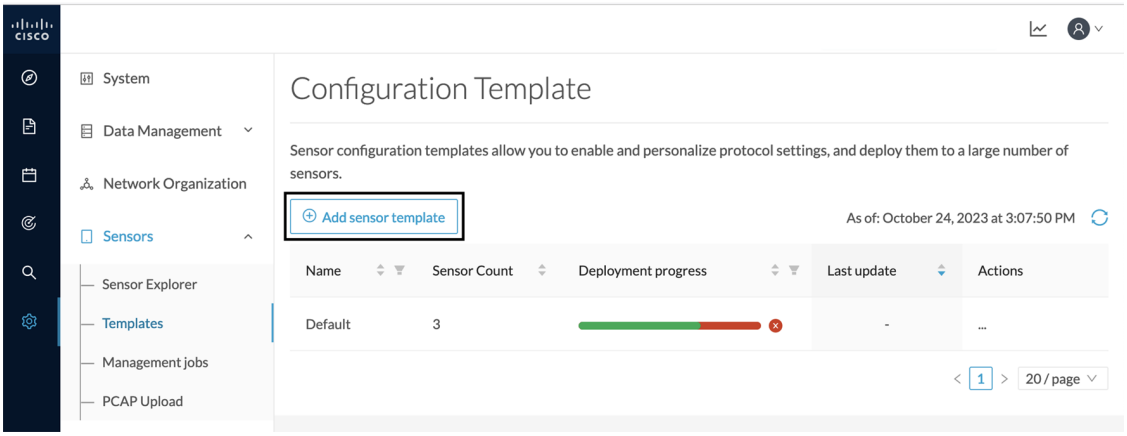
- if the sensor is disconnected,
- if there is connection issues,
- if the sensor version is too old.

Create templates

Procedure

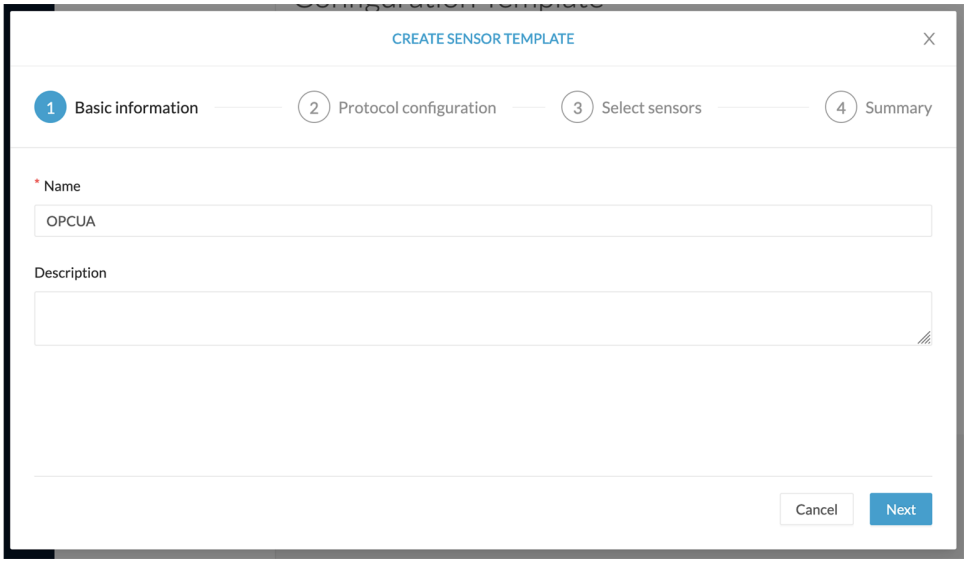
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.

Step 2 Click **Add sensor template**.



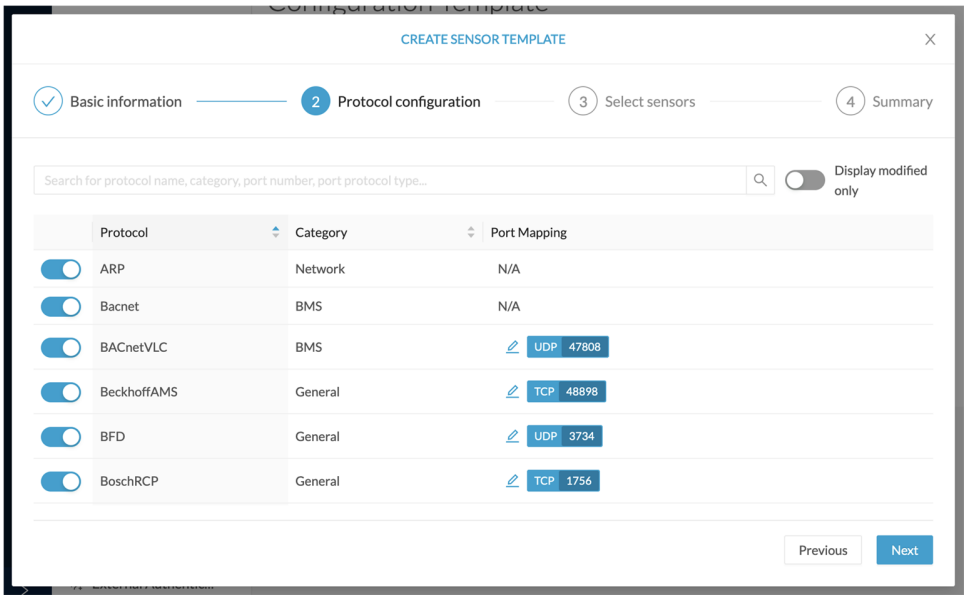
The Create sensor template window pops up.

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



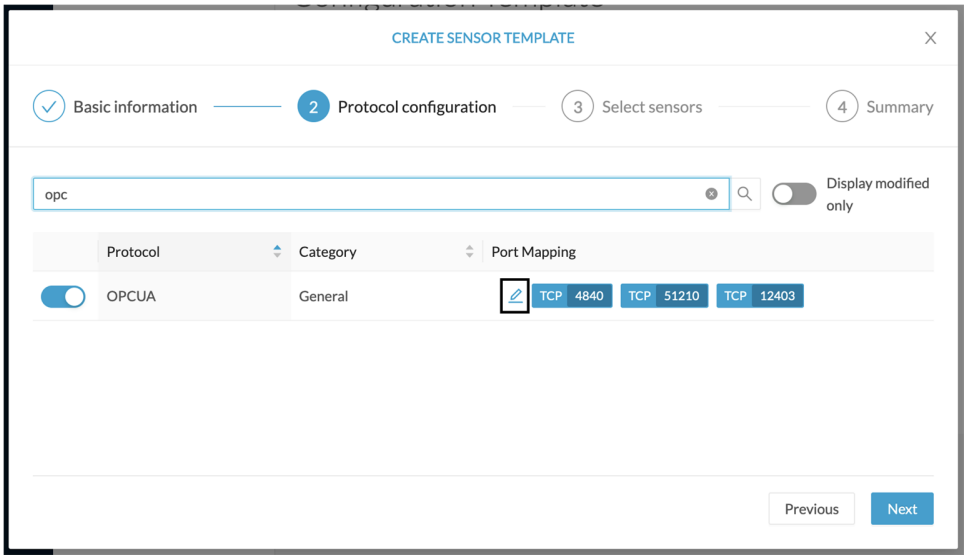
Step 4 Click **Next**.

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



Step 5 In the search bar, type the protocol you want to configure.

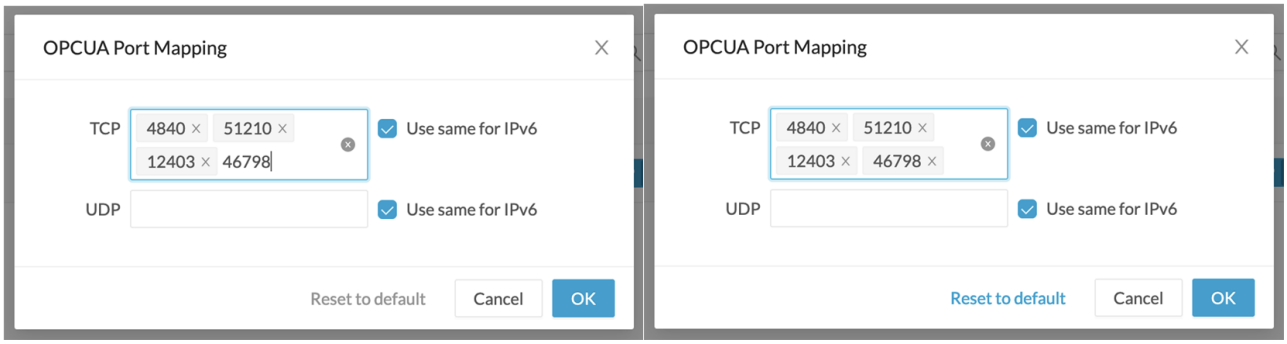
In our example, we will add a port to the OPCUA default settings.



Step 6 Under the Port Mapping column, click the **pen** button to edit its settings.

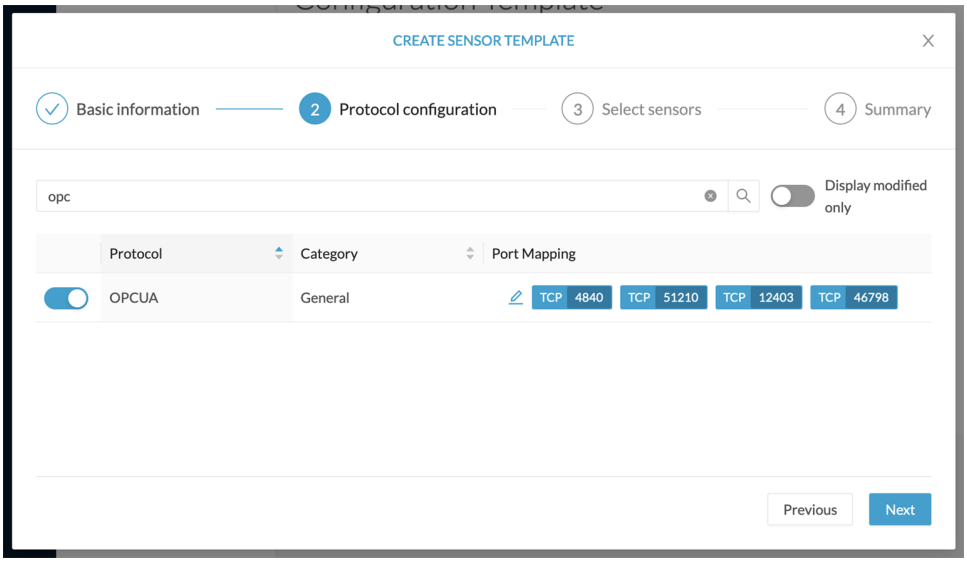
The protocol's port mapping window pops up.

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

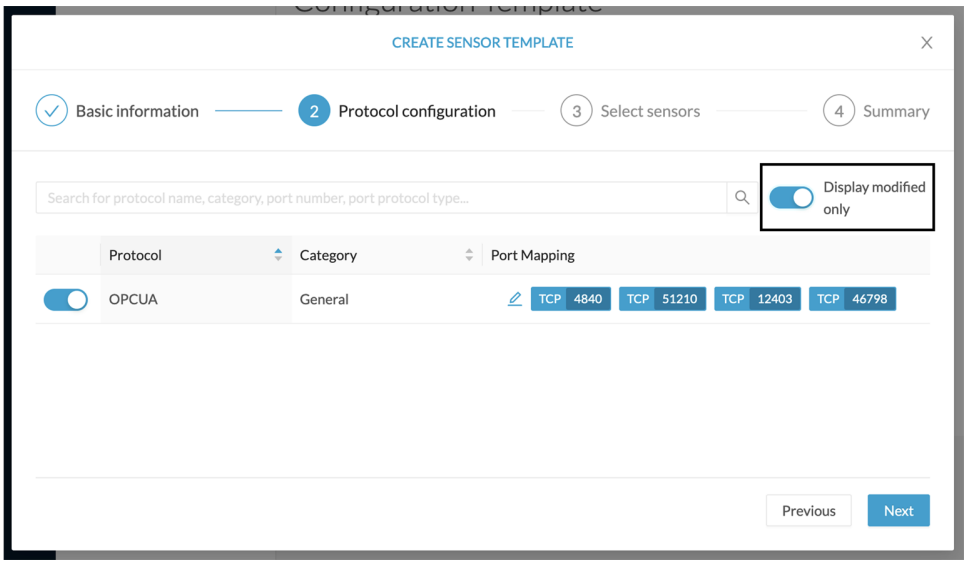


Step 8 Click **OK**.

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

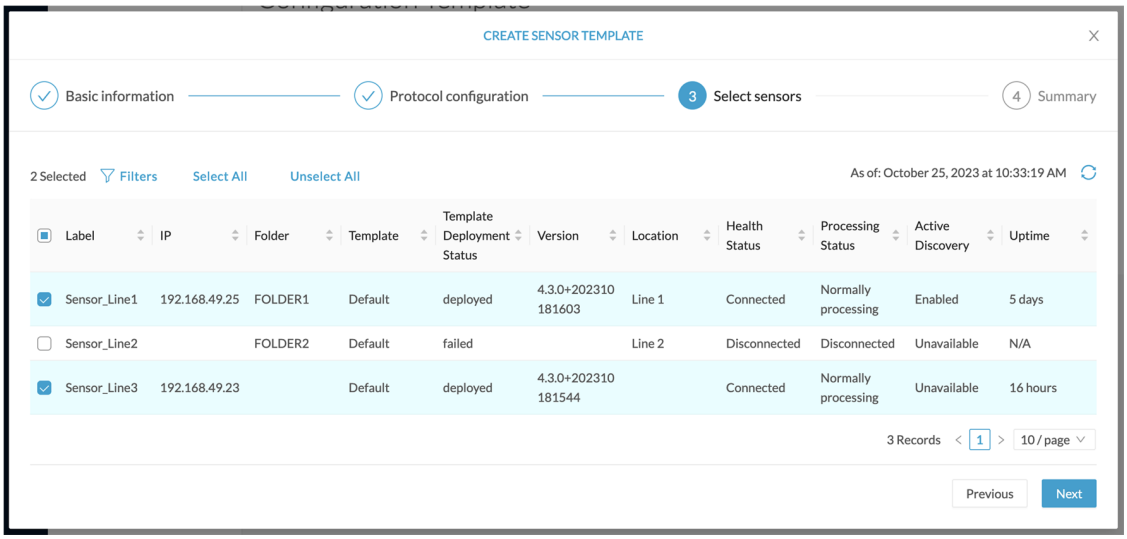


Toggling ON the **Displayed modified only** button allows you to quickly find this protocol.



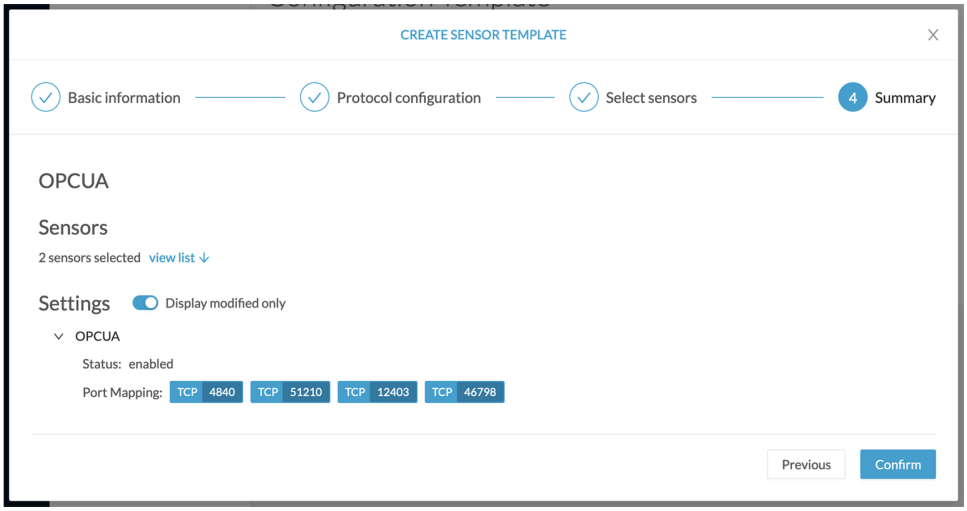
Step 9 Click **Next**.

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



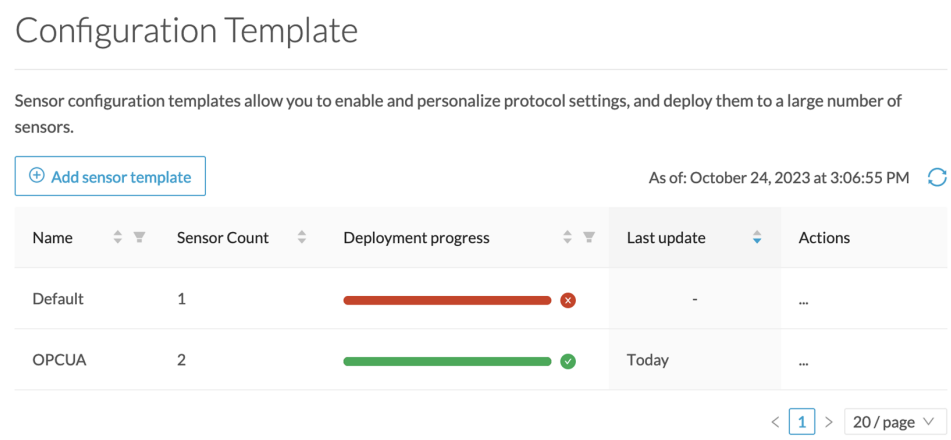
Step 11 Click **Next**.

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



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

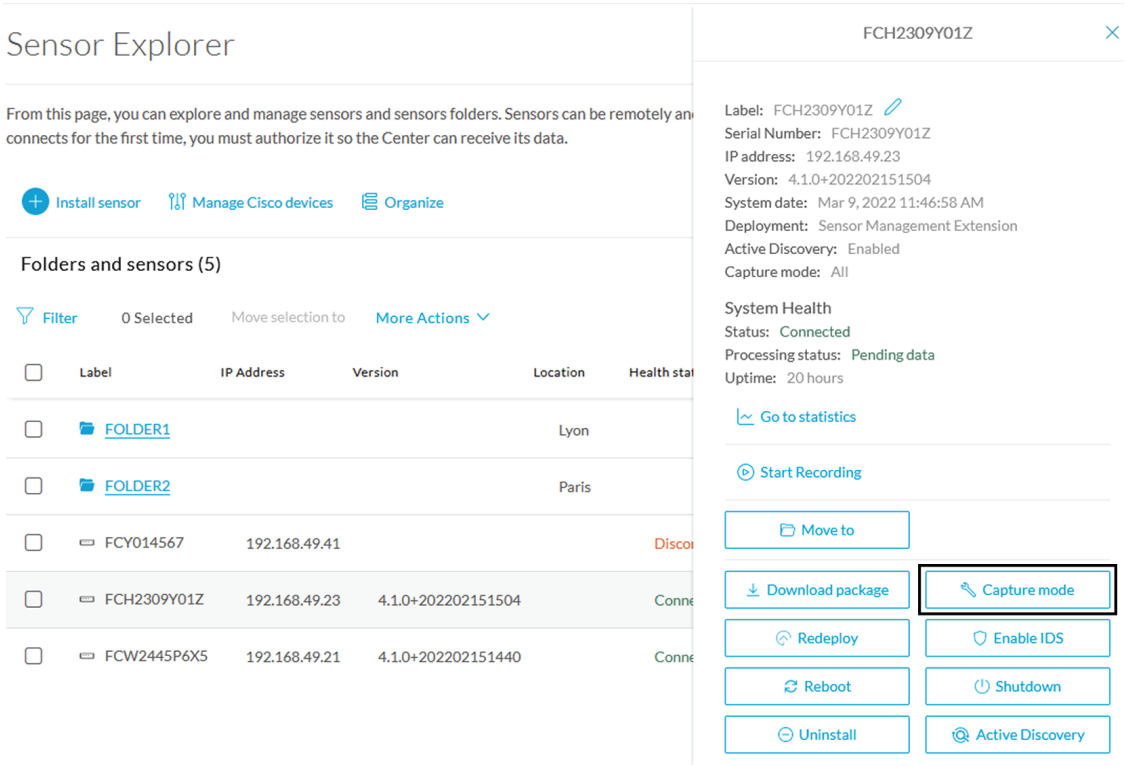
The OPCUA template appears in the template list with its two assigned sensors.



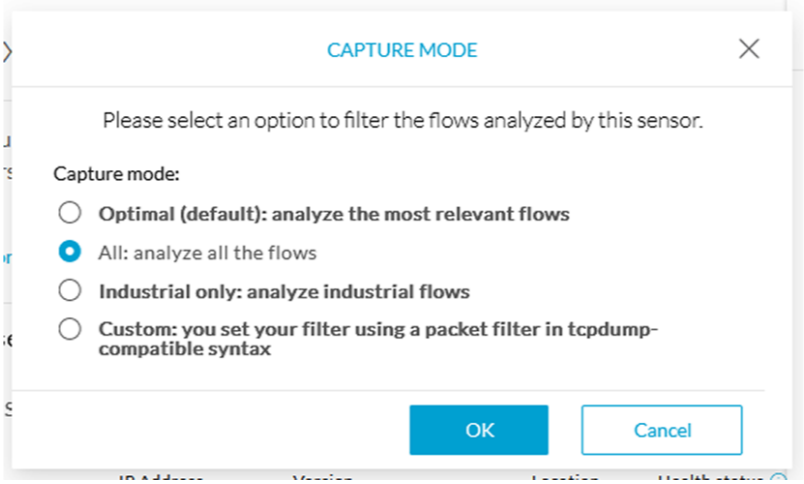
Set a capture mode

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

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



Capture modes:



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

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

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

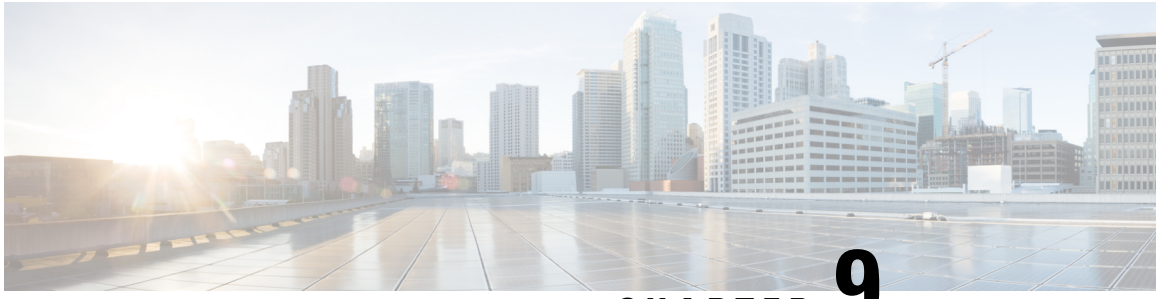
Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

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

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

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.
- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.
- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.
- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.



CHAPTER 9

Maintenance

Upgrade procedures

Upgrade through the Cisco Cyber Vision sensor management extension

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

Update the sensor management extension

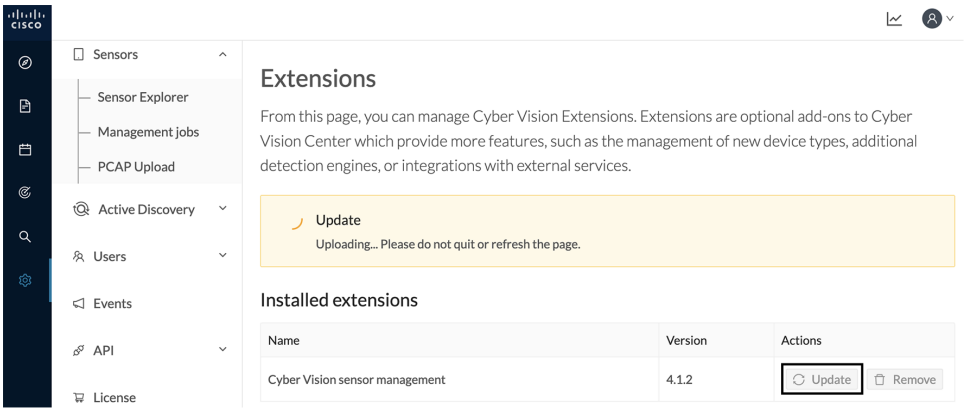
The Cisco Cyber Vision sensor management extension must be up-to-date to update IOx sensors.

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.



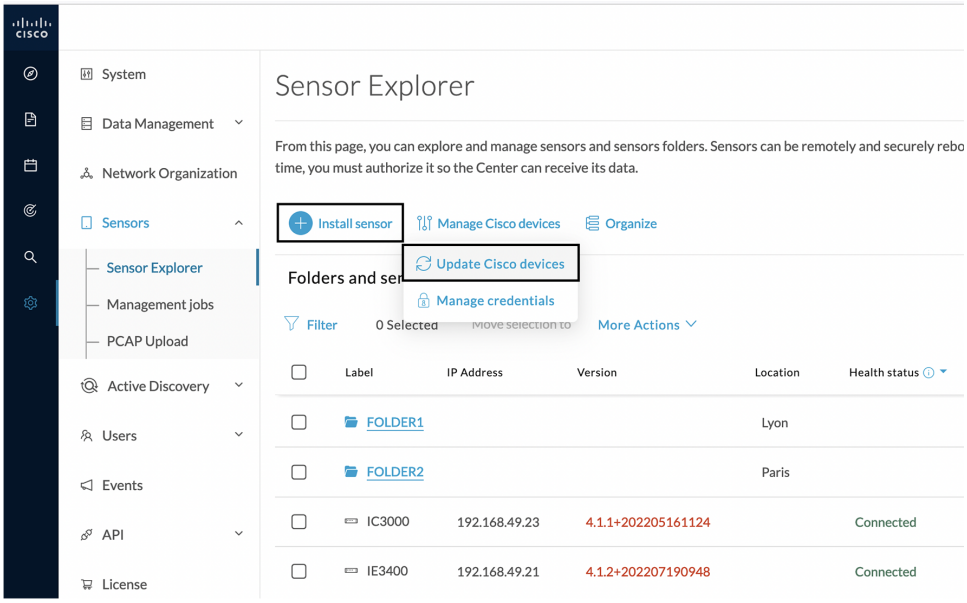
Update the sensors

Procedure

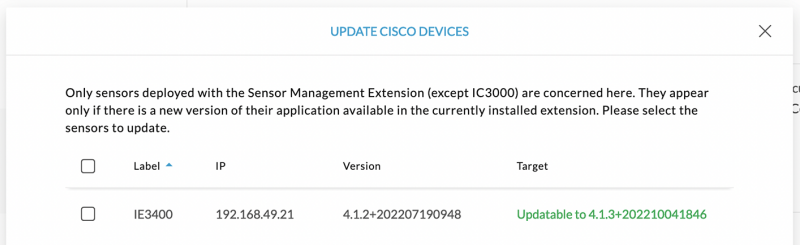
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

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

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



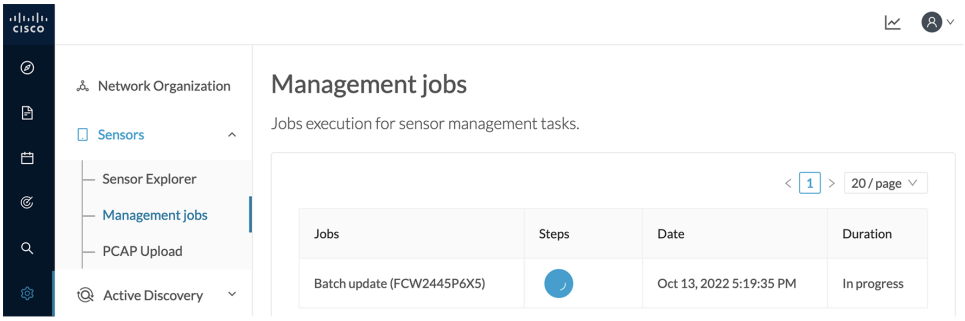
The update Cisco devices window pops up listing all sensors that have been deployed with the sensor management extension.



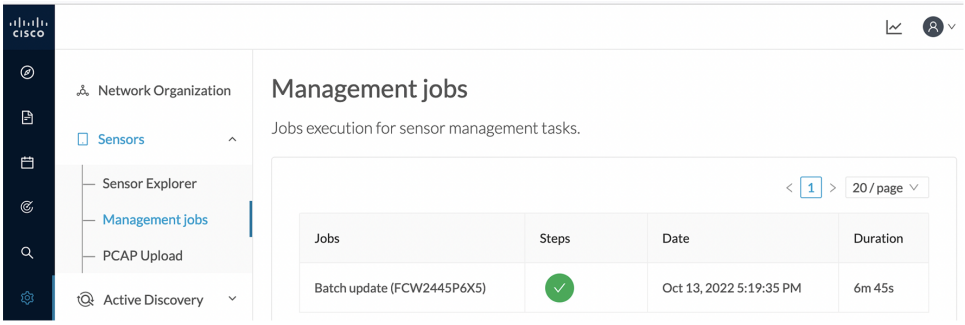
Step 3 Select the sensors you want to update.

Step 4 Click **Update**.

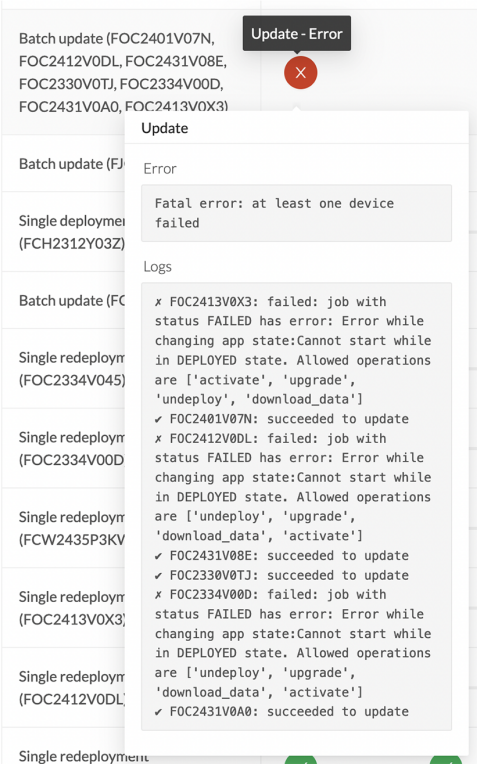
The sensors' update status appear in the Management jobs page in batches per sensor type and of maximum ten sensors per batch.



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



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

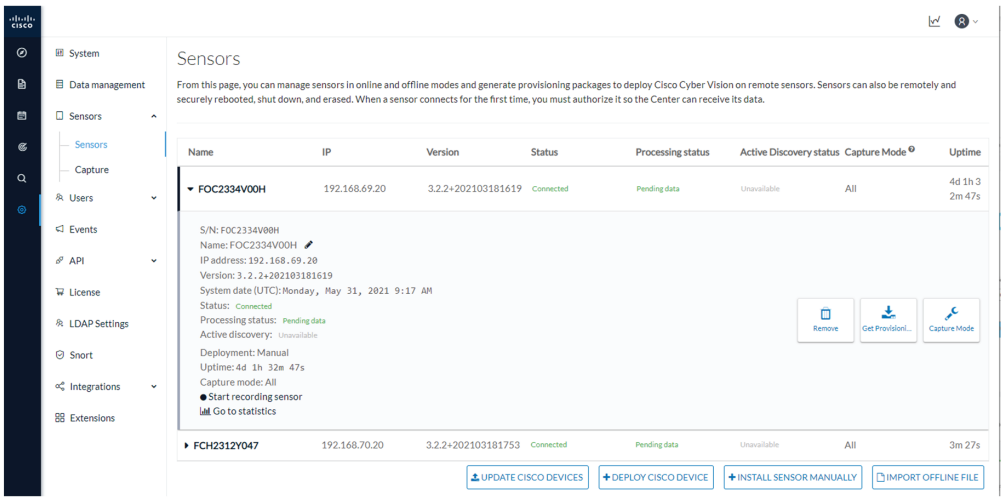


Upgrade through the IOx Local Manager

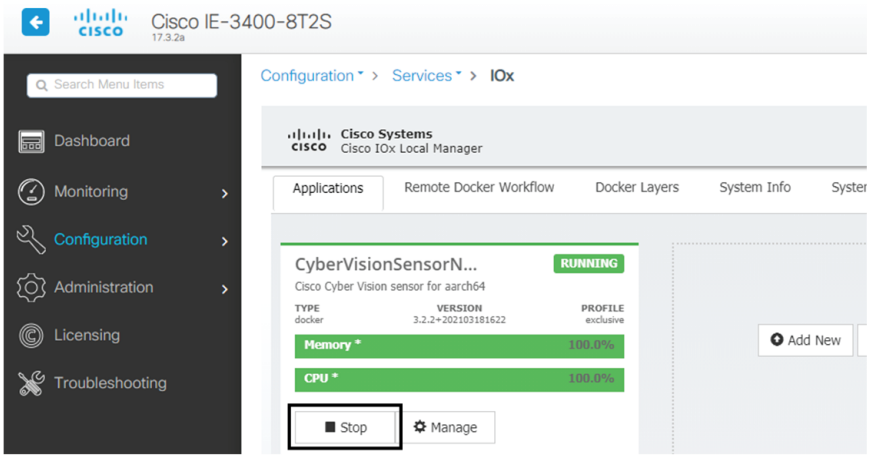
The following section explains how to upgrade the sensor through the IOx Local Manager.

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

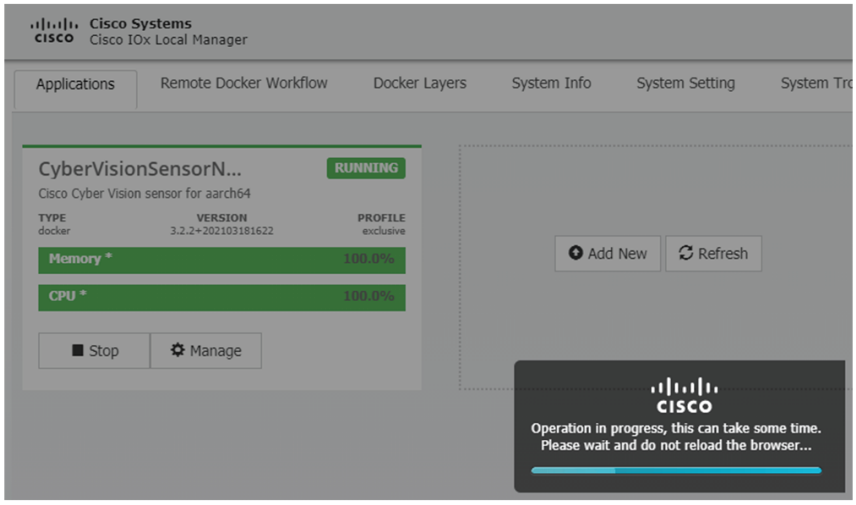
Figure 1: The sensor in version 3.2.2 in the Sensors administration page of Cisco Cyber Vision



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

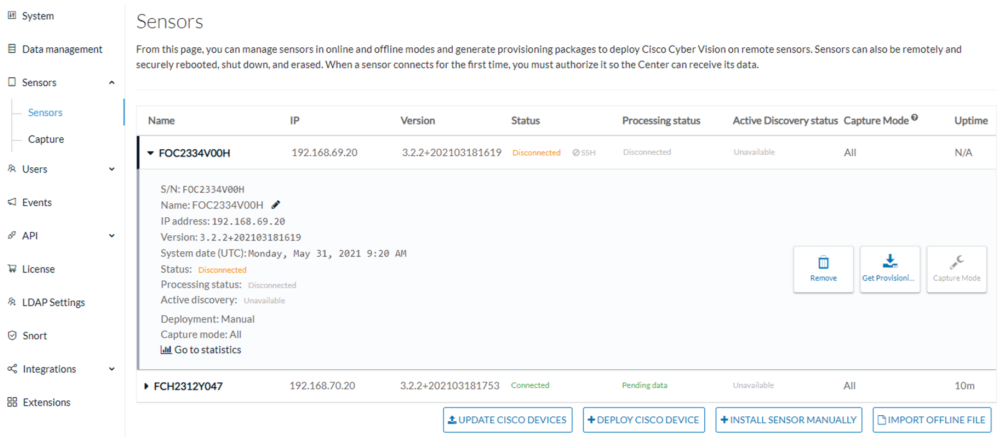


The operation takes a few moments.



The application status switches to STOPPED.

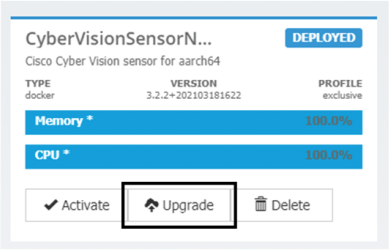
In Cisco Cyber Vision, the sensor status switches to Disconnected.



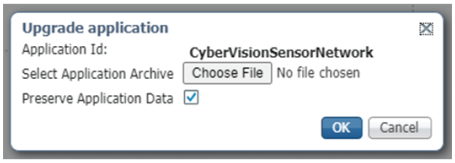
3. In the IOx Local Manager, click the **Deactivate** button.

   The application status moves to DEPLOYED.

4. Click **Upgrade**.



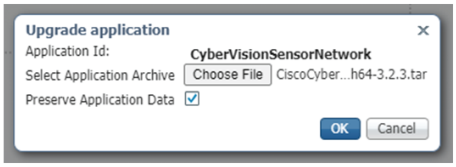
The pop up Upgrade application appears.



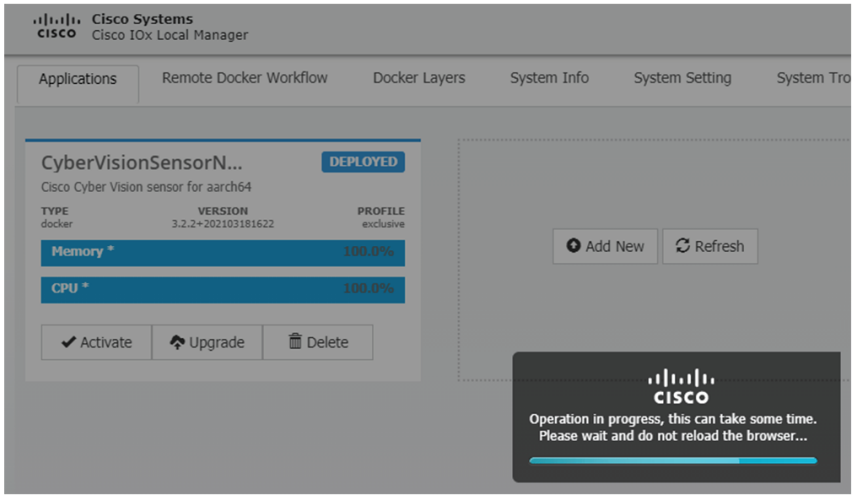
5. Select the **Preserve Application Data** option.

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

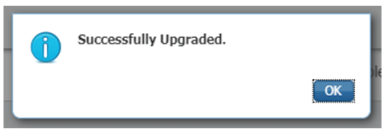
   e.g. CiscoCyberVision-IOx-aarch64-3.2.3.tar



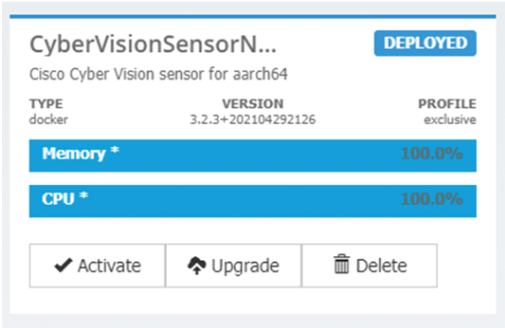
The operation takes a few moments.



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



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

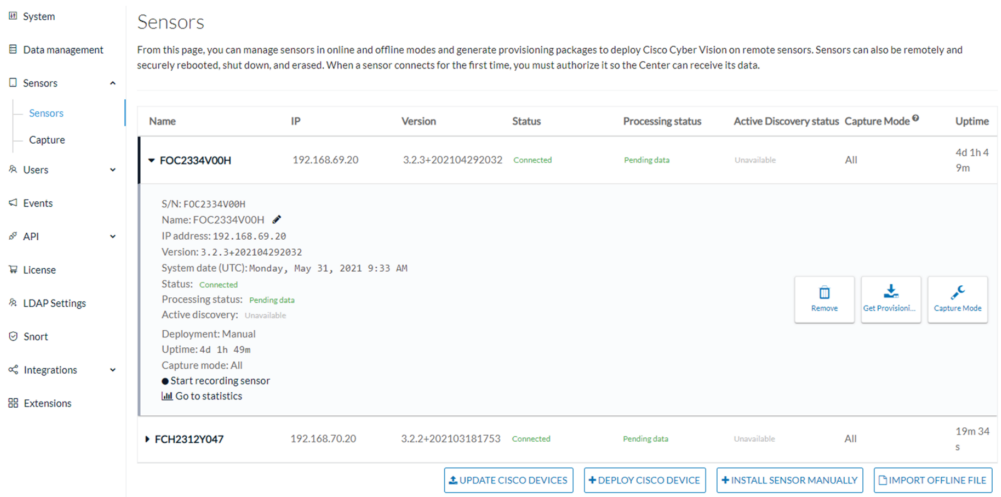


9. Check configurations.
10. Click the **Activate App** button.

    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.



Replace SD card

This section explains how to replace a SD card on a Cisco IE3x00.

Procedure

Step 1 Connect to the device CLI and use the following commands to disable IoX:

```
configure terminal
no iox
exit
```

Step 2 Replace the SD card.

Step 3 Format the SD card using the following command:

```
format sdflash: ext4
```

```
IE340CCV#format sdflash: ext4
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:".  Continue? [confirm]
format completed with no errors

Format of sdflash: complete
IE340CCV#
```

Step 4 Enable IOx using the following command:

```
configure terminal
iox
```

```
IE340CCV#
IE340CCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE340CCV(config)#iox
Warning: Do not remove SD flash card when IOx is enabled or errors on SD device could occur.

IE340CCV(config)#
```

Step 5 Follow the instructions described in the following section to redeploy the sensor.

What to do next

Reconfigure/Redeploy a sensor, on page 83

Reconfigure/Redeploy a sensor

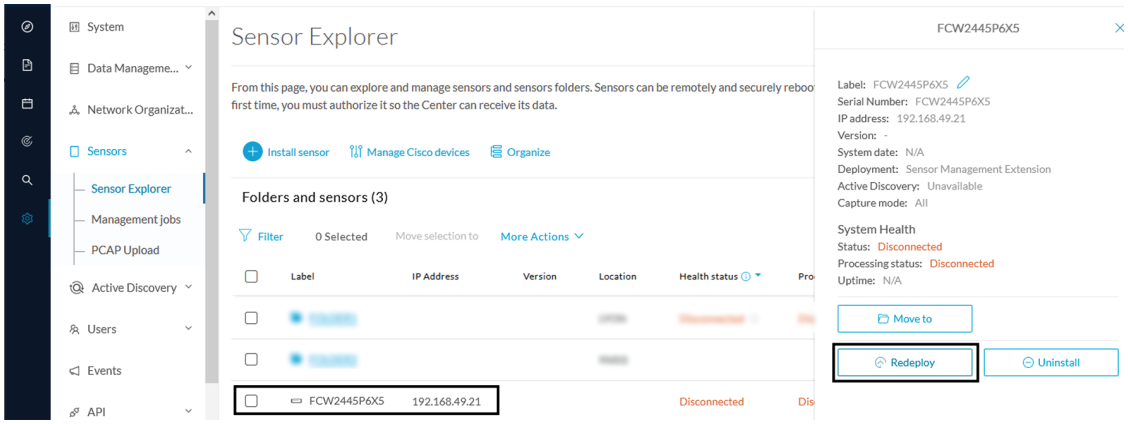
The Redeploy button is used when you need to replace a sensor model with another one keeping the same network configurations (e.g. replacing a Cisco IE3400 with a Cat 9300), change configurations, or if you need to reconfigure the sensor (e.g. to enable Active Discovery).

To do so:

Procedure

Step 1 On the Sensor Explorer page, click the sensor to reconfigure/redeploy. The sensor right side panel appears.

Step 2 Click **Redeploy**.

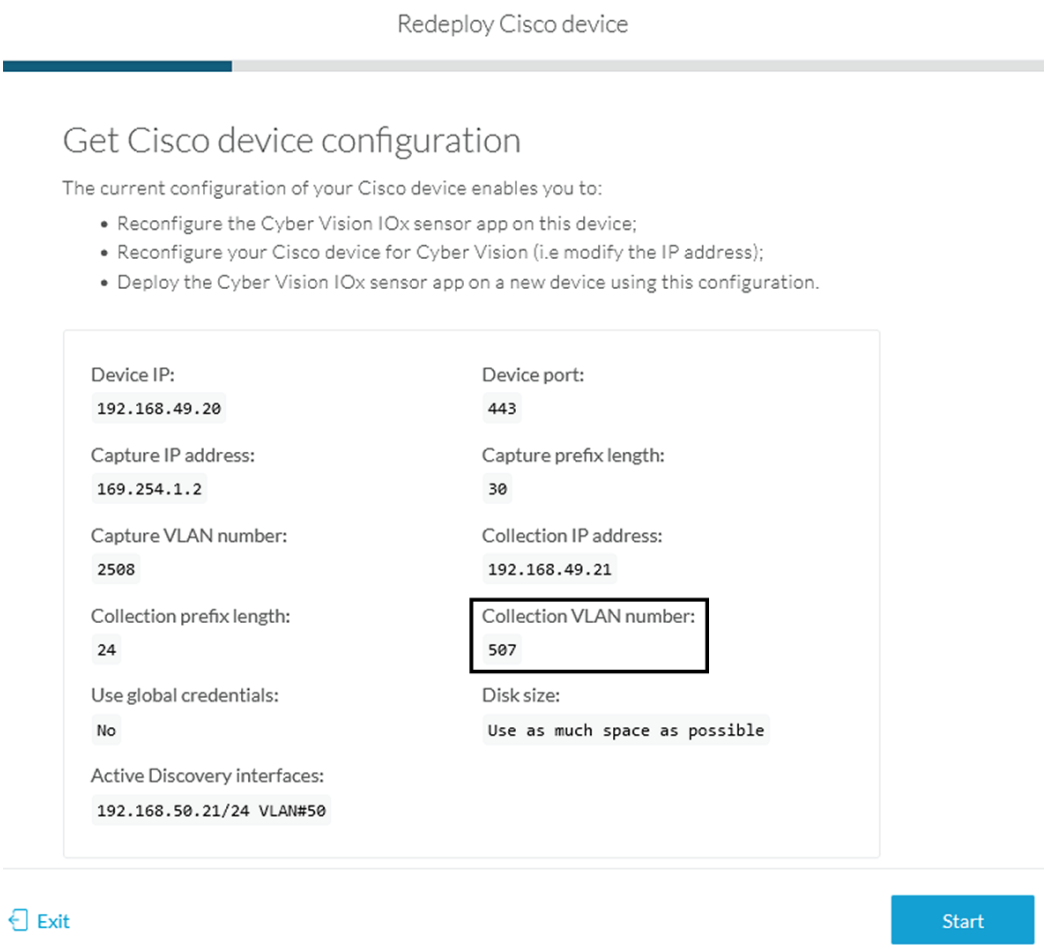


A pop up asking to confirm the redeployment of the sensor appears.

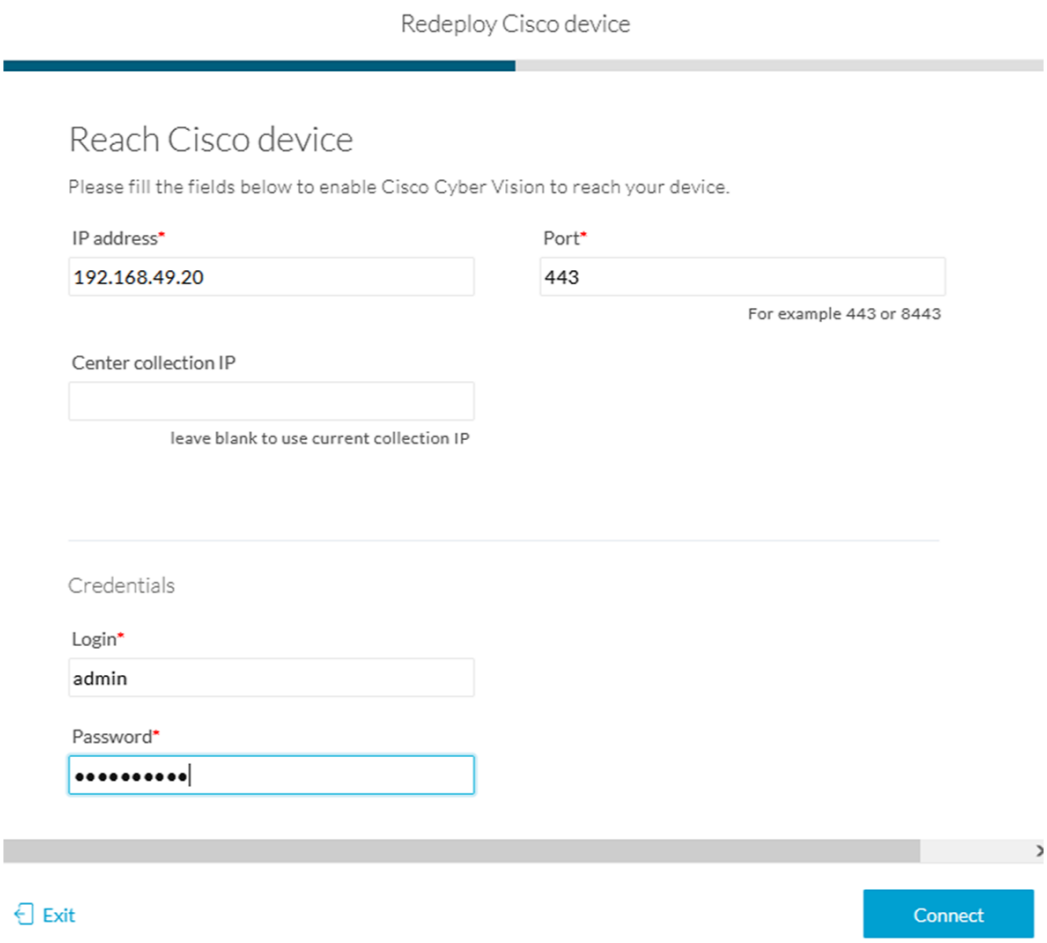
Step 3 Click **OK** to proceed.

A summary of the sensor configuration is displayed. In this example, we're going to change the Collection VLAN number.

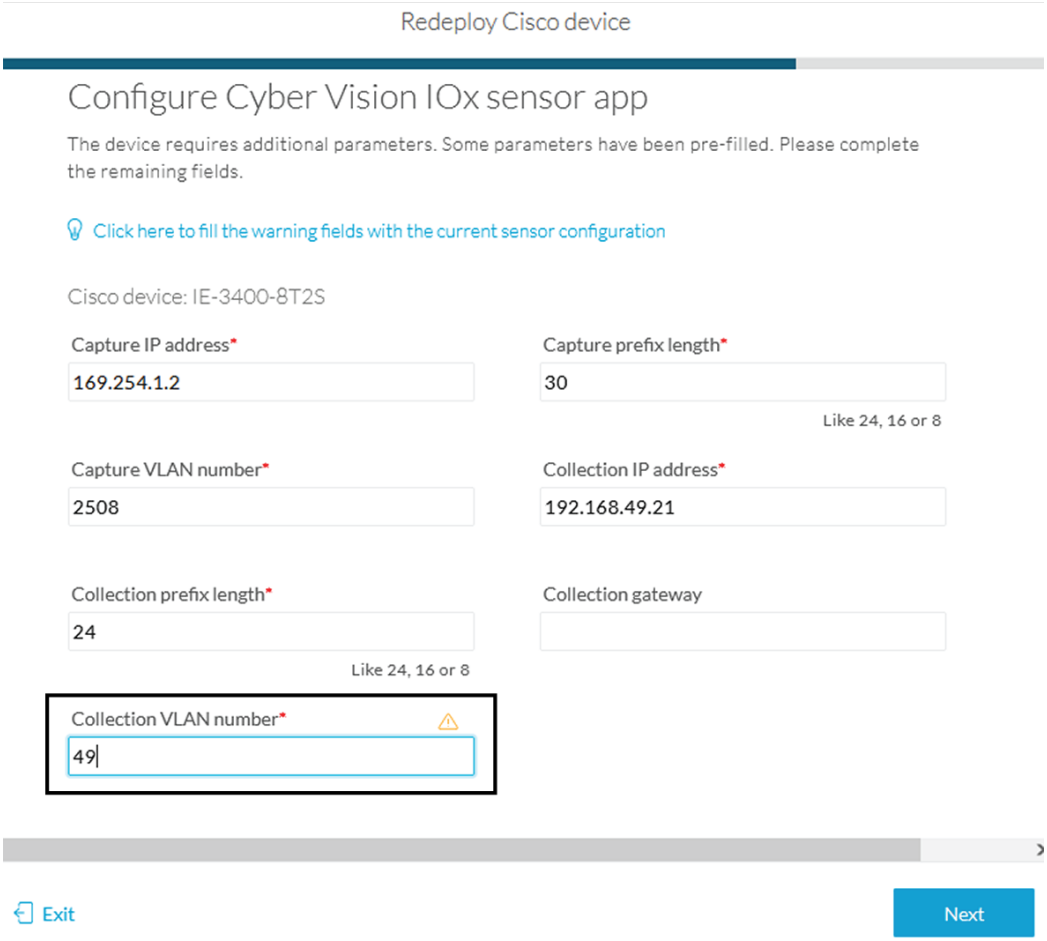
Step 4 Click **Start**.



Step 5 Enter the credentials to reach the sensor to redeploy and click **Connect**.



Step 6 Click the blue link to fill the warning fields with the current sensor configuration. We change the Collection VLAN number value to 49.



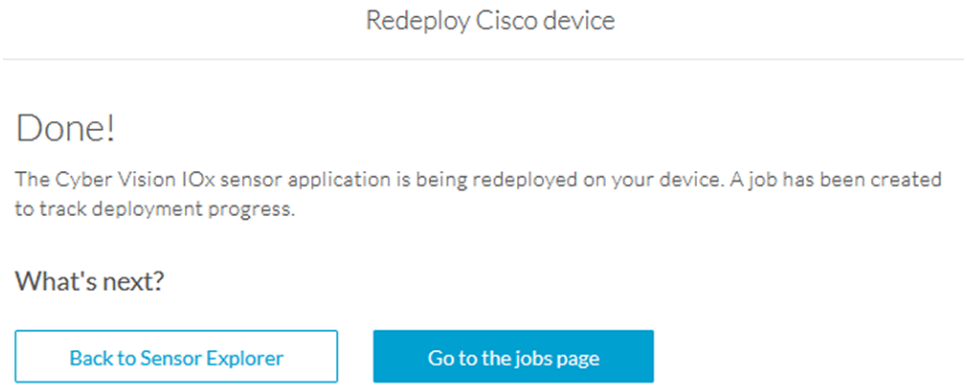
Step 7 Click **Next**.

Step 8 You can enable Active Discovery selecting Passive and Active Discovery.

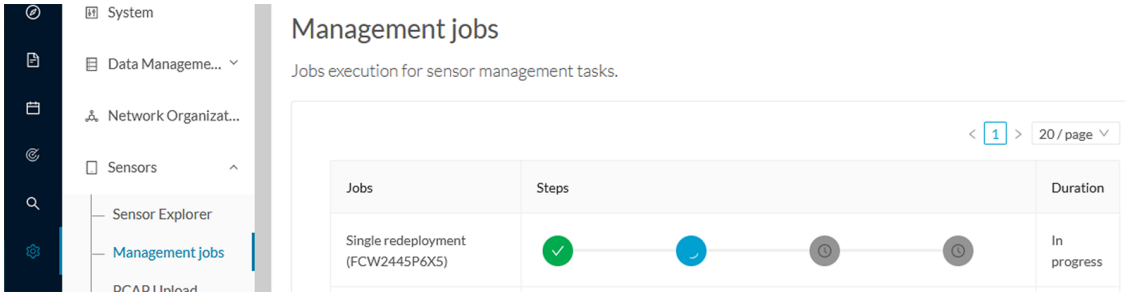
Step 9 Click Deploy.

A message saying that the sensor is being redeployed appears. You can either go the jobs page or go back to the Sensor Explorer page.

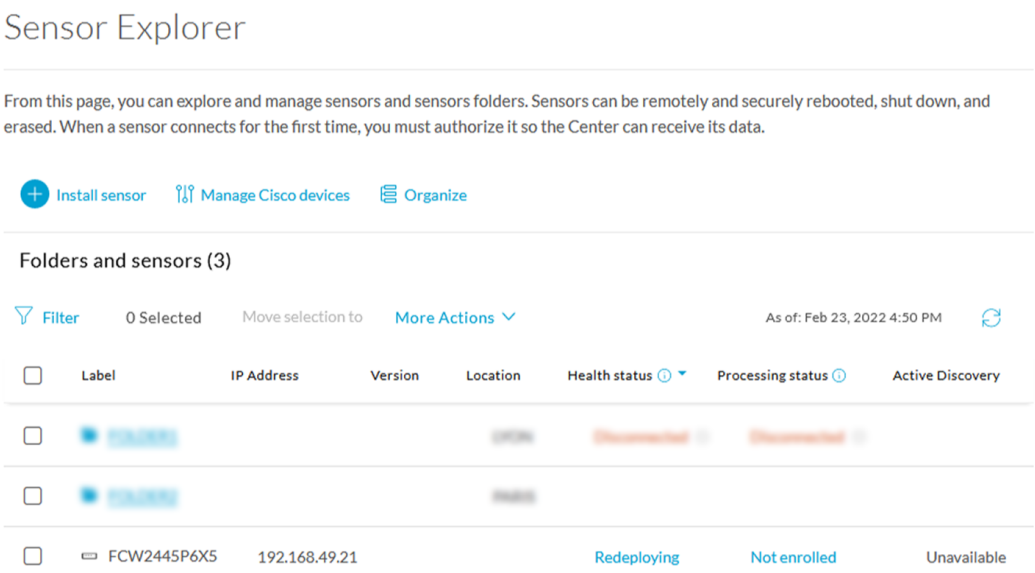
Step 10 Click **Go to the jobs page**.



You are redirected to the Management jobs to see the redeployment advancement. This can take several minutes.



If you go back to the Sensor Explorer page, you will see that the sensor is in Redeploying status.



Once the redeployment is finished, the sensor will switch status to connected and the Active Discovery to Enabled.

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.

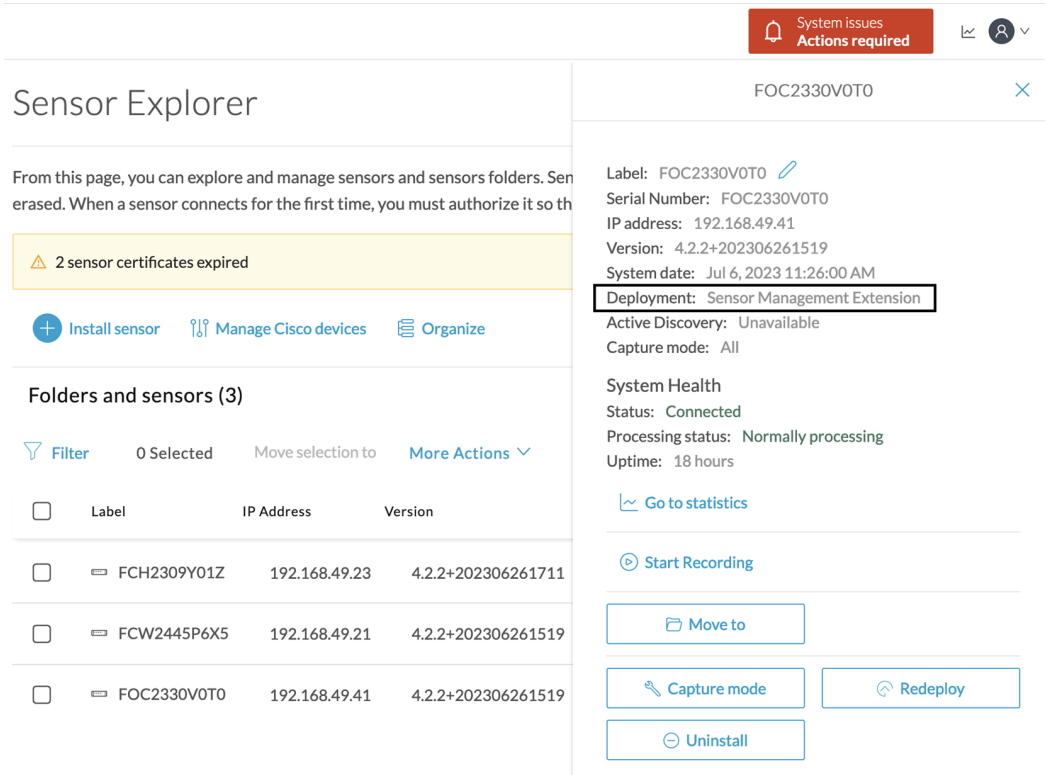
- If the certificate is still valid, refer to Sensor certificate renewal, on page 88.
- If the sensor was deployed with the sensor management extension, refer to Sensor certificate renewal, on page 88.

- If the certificate is outdated, and was deployed manually, refer to Sensor certificate renewal through the Local Manager, on page 91.

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).

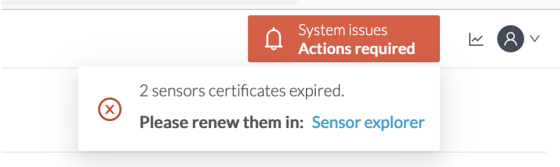


- In the case of sensors deployed manually, it only applies if the sensors certificate have not expired yet (i.e. the sensor certificate status is Expire Soon).

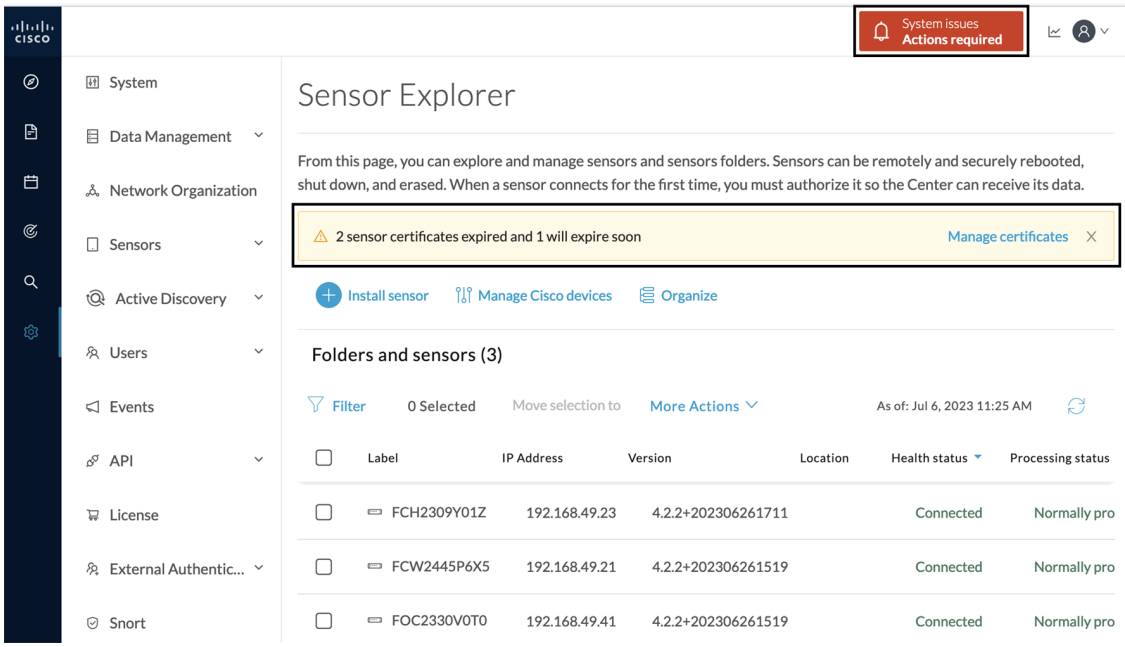
If sensors have been deployed manually and the certificate expiration date is exceeded, refer to Sensor certificate renewal through the Local Manager, on page 91.

Procedure

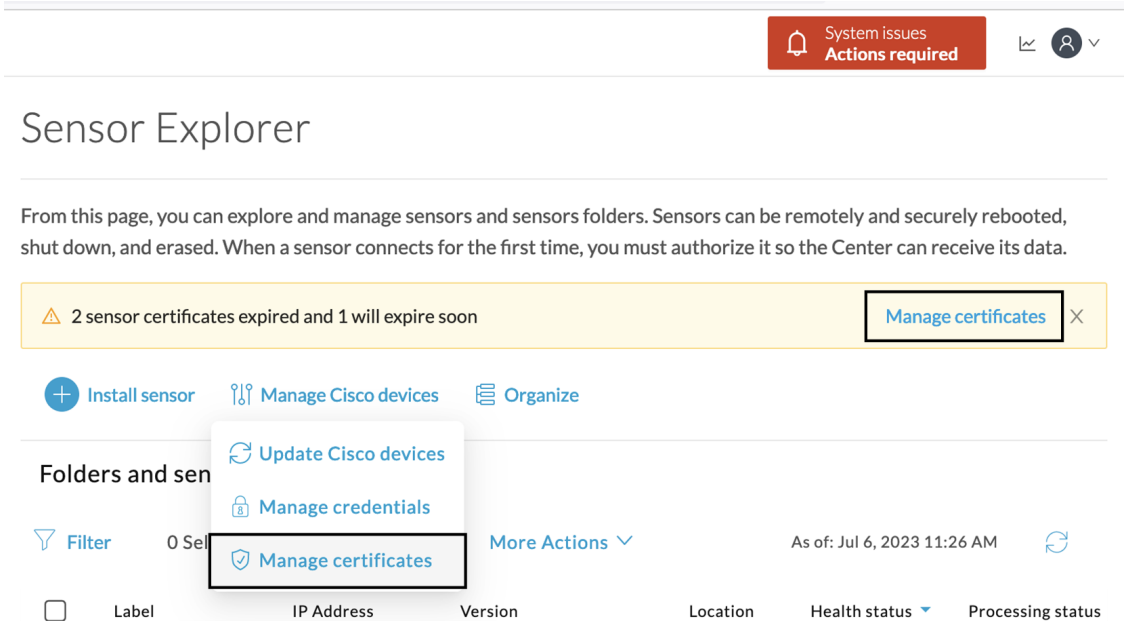
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer or click the top banner alert to access the Sensor Explorer page directly.



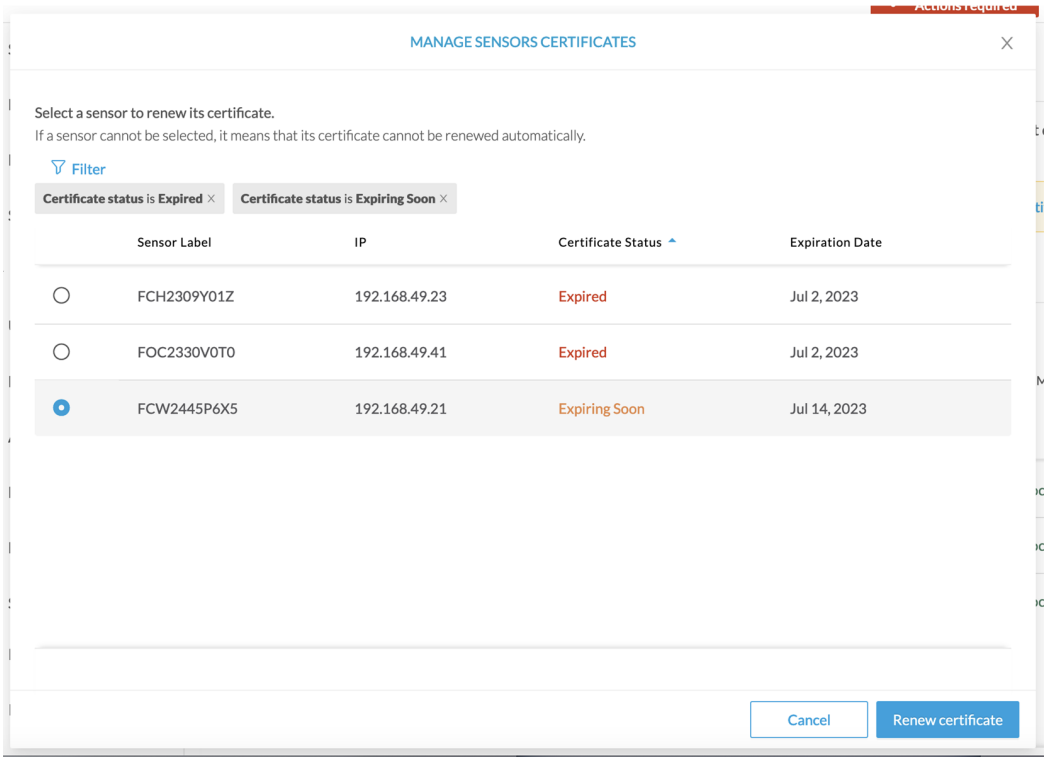
Another alert is displayed.



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

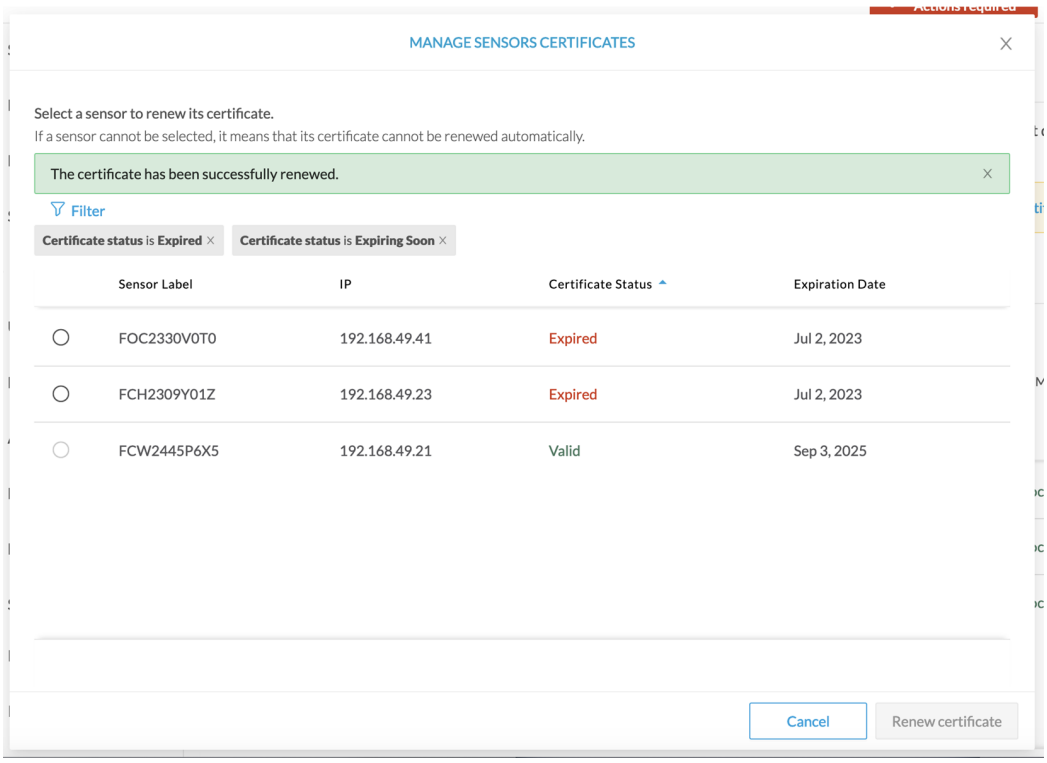


The **Manage sensors certificates** window opens.



Step 3 Select the sensor with the status Expiring Soon.

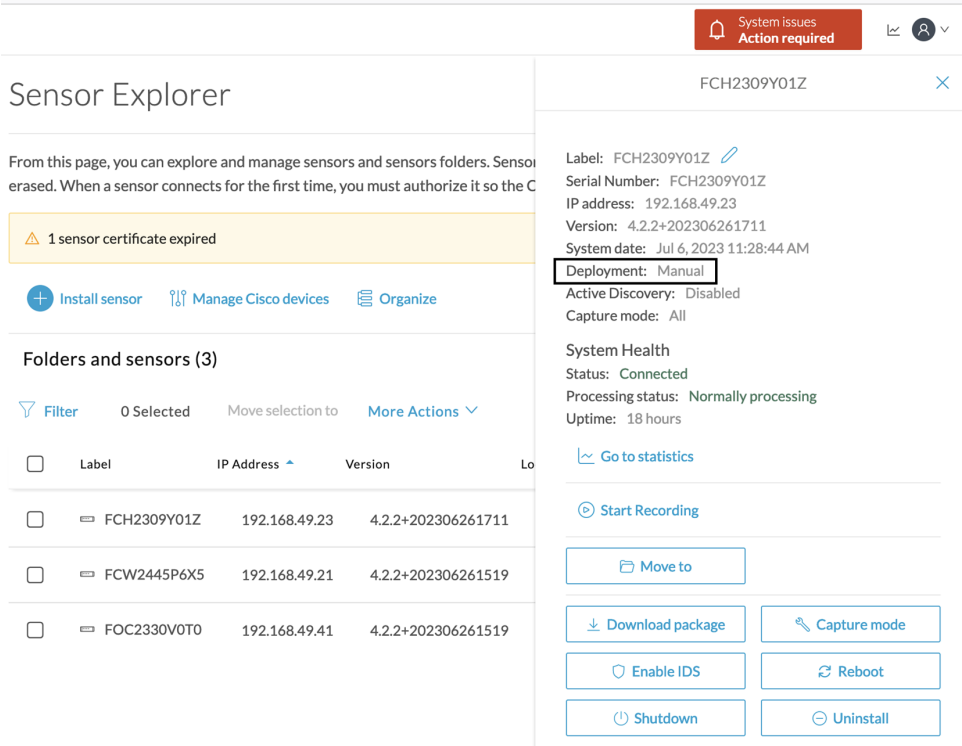
Step 4 Click **Renew certificate**.



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.

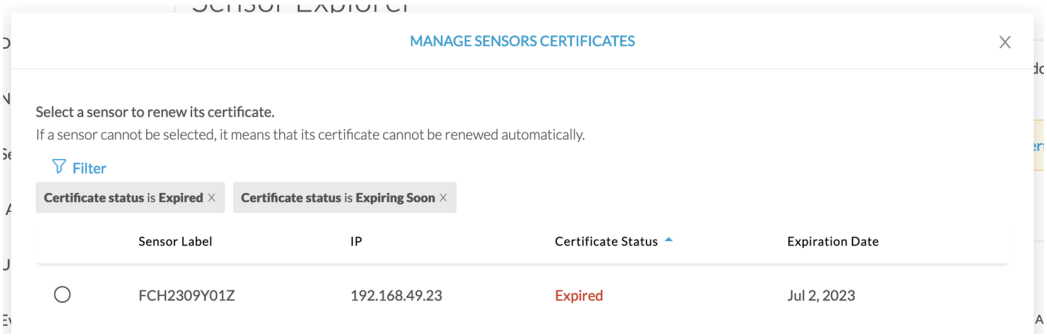


Procedure

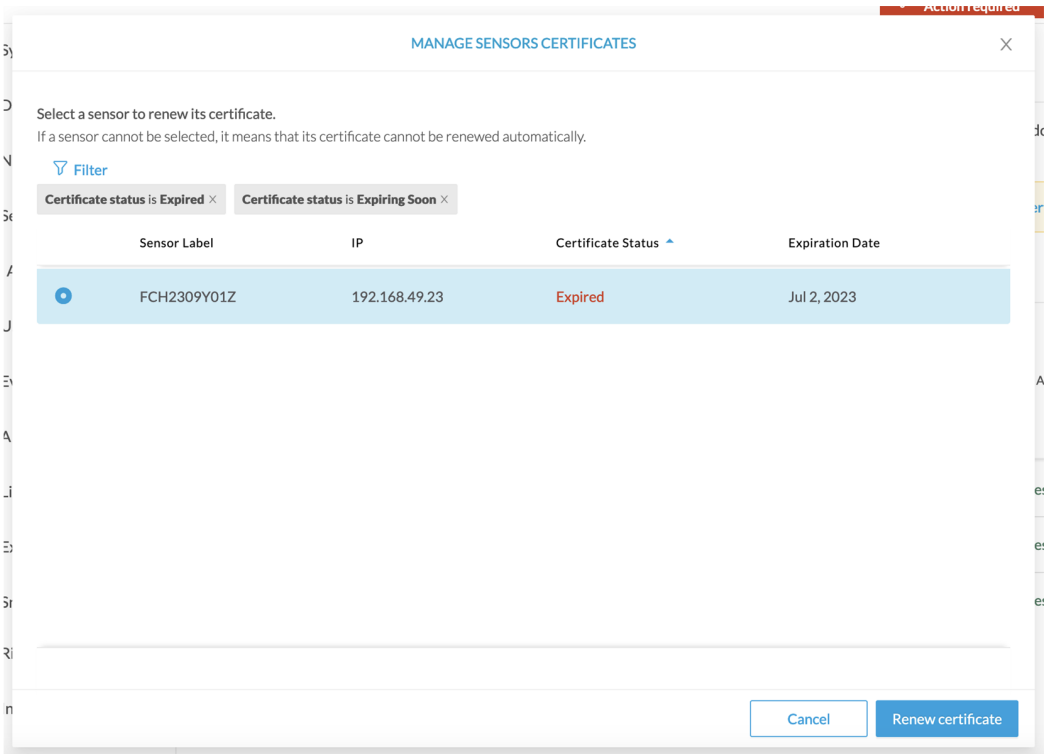
Step 1 In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer.

Step 2 Click **Manage Certificates**.

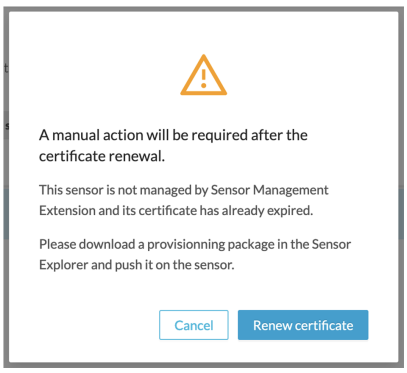
The Manage sensors certificates window appears.



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

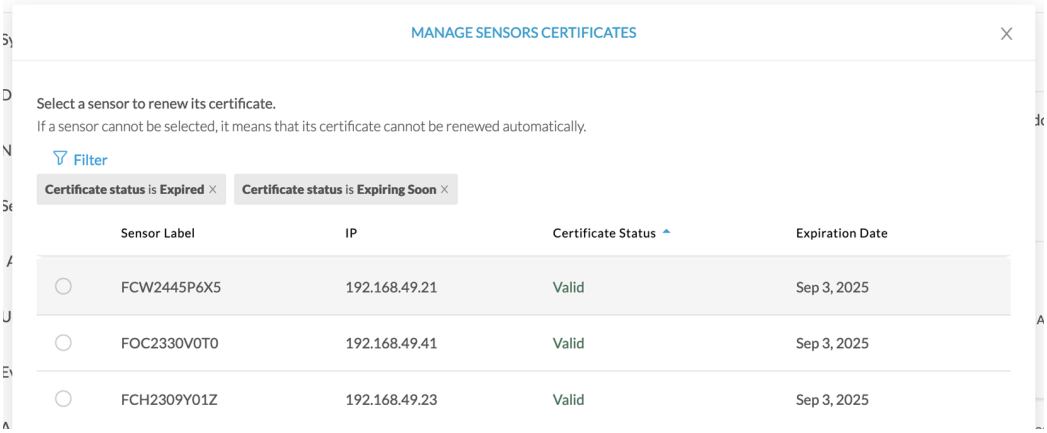


A message is displayed.



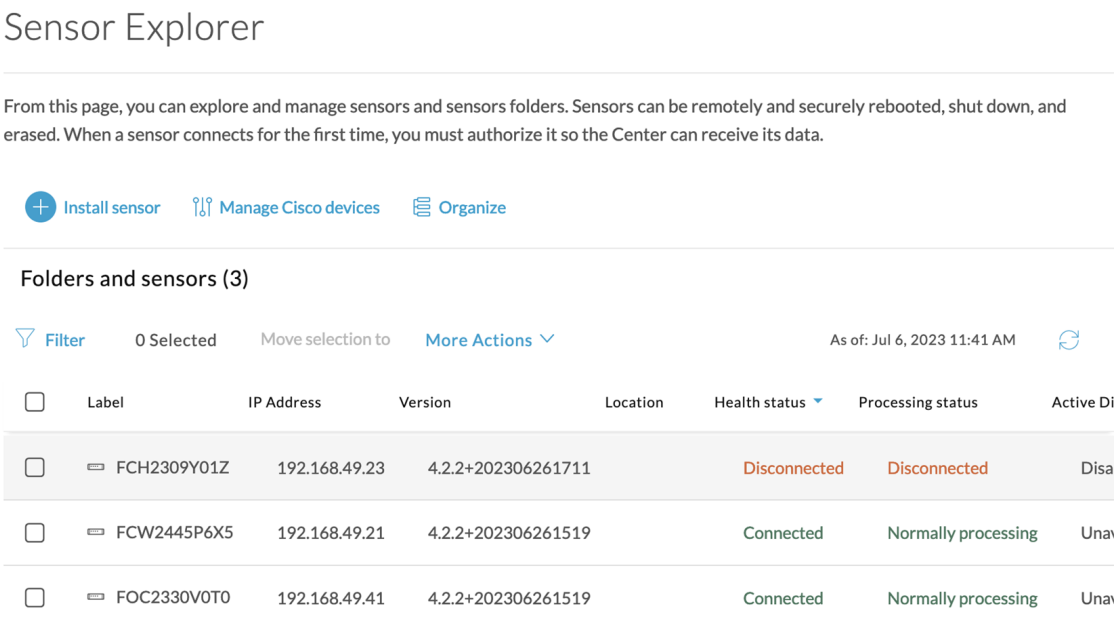
Step 4 Click **Renew certificate** again.

The sensor certificate status appears as valid.



Step 5 Close the Manage sensors certificates window.

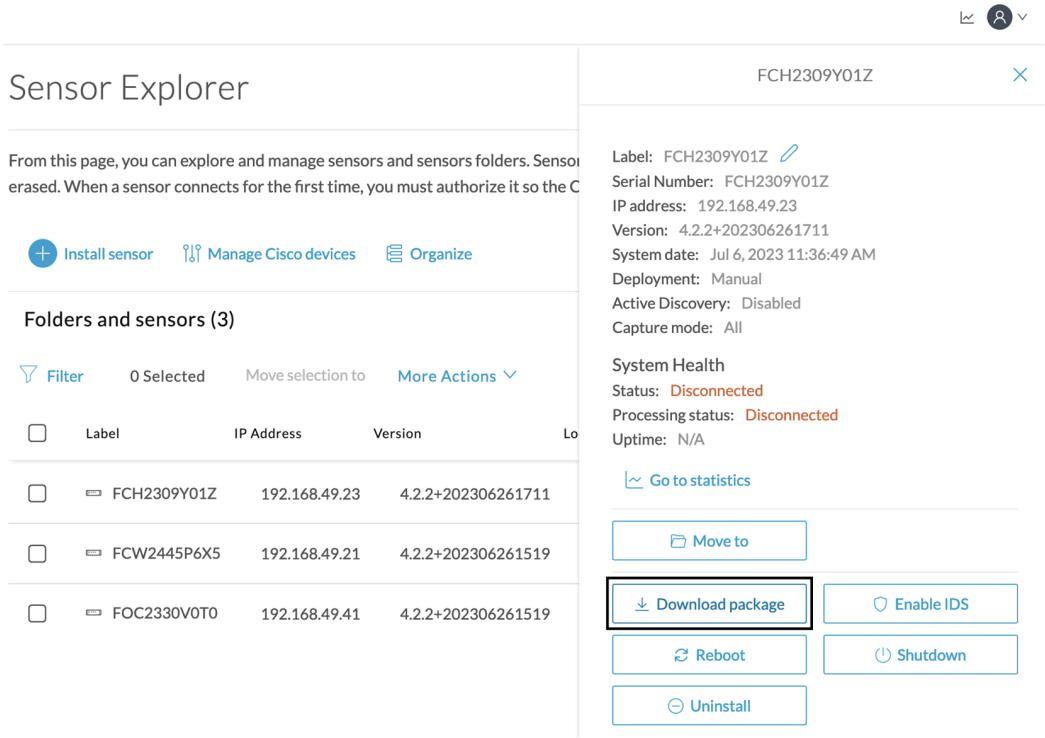
The sensor's health and processing status appear as Disconnected.



Step 6 Click the sensor in the list.

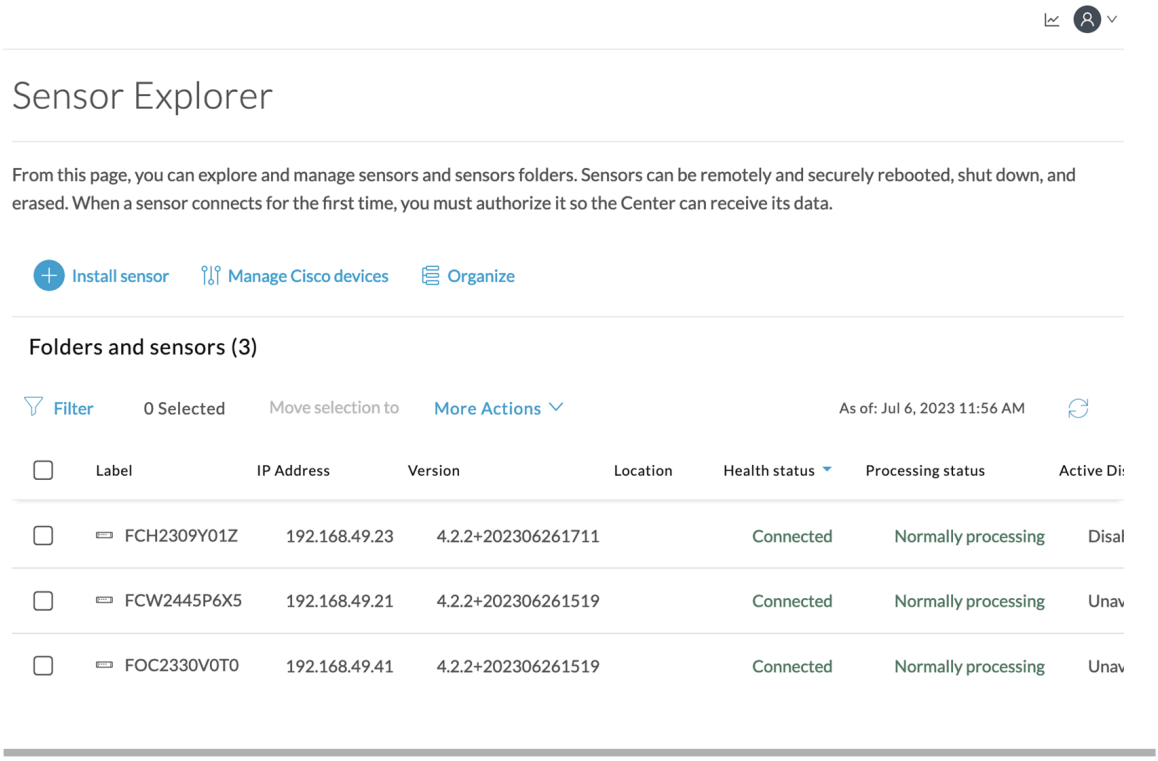
Its right side panel opens.

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



Step 8

Step 9 The sensor's health status switches to Connected and its processing status to Normally processing.



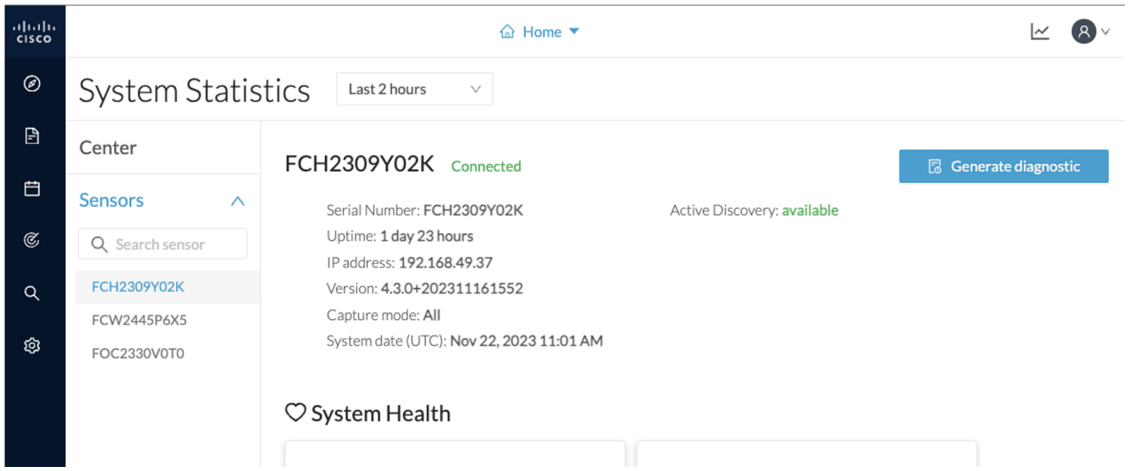
CHAPTER 10

Troubleshooting

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 VisionGUI to generate the sensor diagnostic from the sensor statistics page.



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

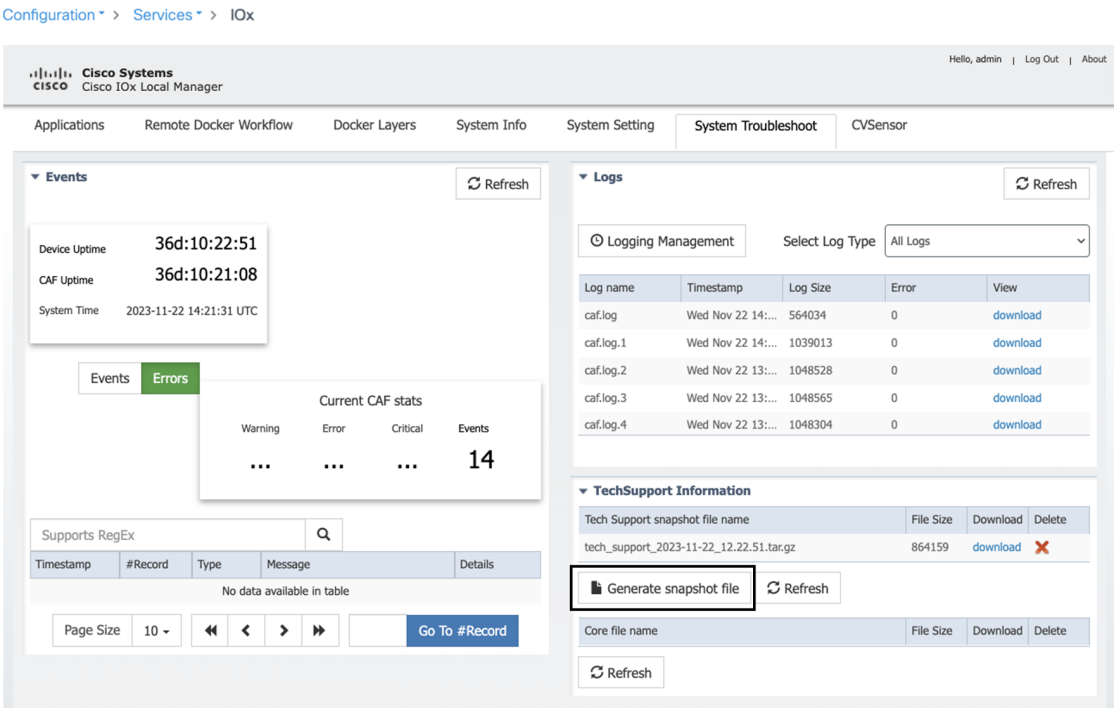
In case of sensor issues Cisco Cyber Vision support can ask you to retrieve IOx sensor logs. You can retrieve them through the IOx Local Manager.

Procedure

Step 1 Access the sensor's IOx Local Manager.

Step 2 Click the **System Troubleshoot** tab.

Step 3 Click the **Generate snaptshot 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
Supports RegEx
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 download
caf.log.1 Wed Nov 22 14:... 1039013 0 download
caf.log.2 Wed Nov 22 13:... 1048528 0 download
caf.log.3 Wed Nov 22 13:... 1048565 0 download
caf.log.4 Wed Nov 22 13:... 1048304 0 download
TechSupport Information
Tech Support snapshot file name File Size Download Delete
tech_support_2023-11-22_12.22.51.tar.gz 864159 download
Generate snapshot file
Refresh
Core file name File Size Download Delete
Refresh