Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide, Release 4.1.3

First Published: 2021-01-01

Last Modified: 2022-10-20

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

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

This documentation is applicable to **system version 4.1.3**.

Warnings and notices

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

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

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

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

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

CHAPTER 2

Overview

Overview

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).

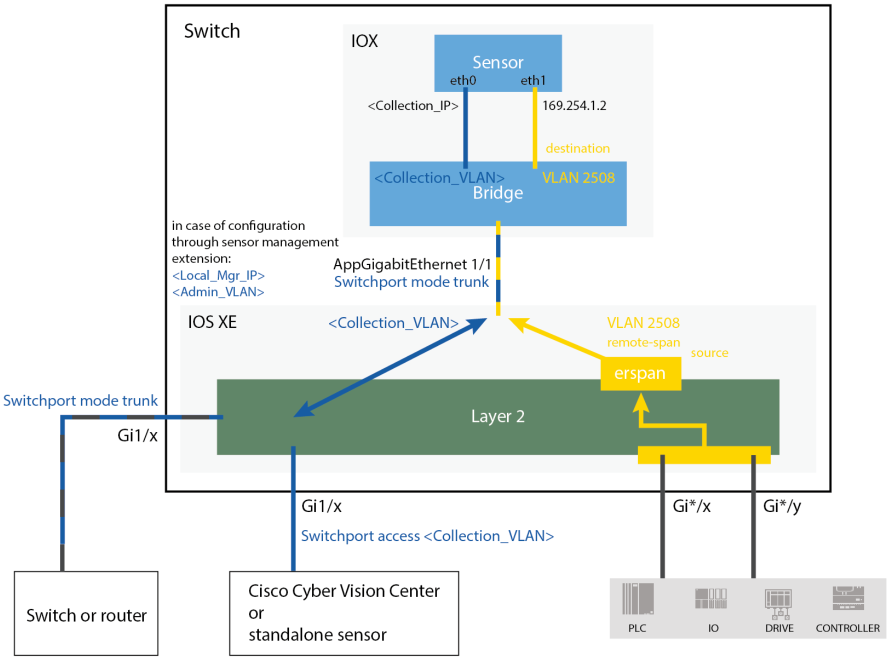
having a route path from the Center to an <admin_VLAN> that is different from <collection_VLAN>.

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

Architecture diagram for:

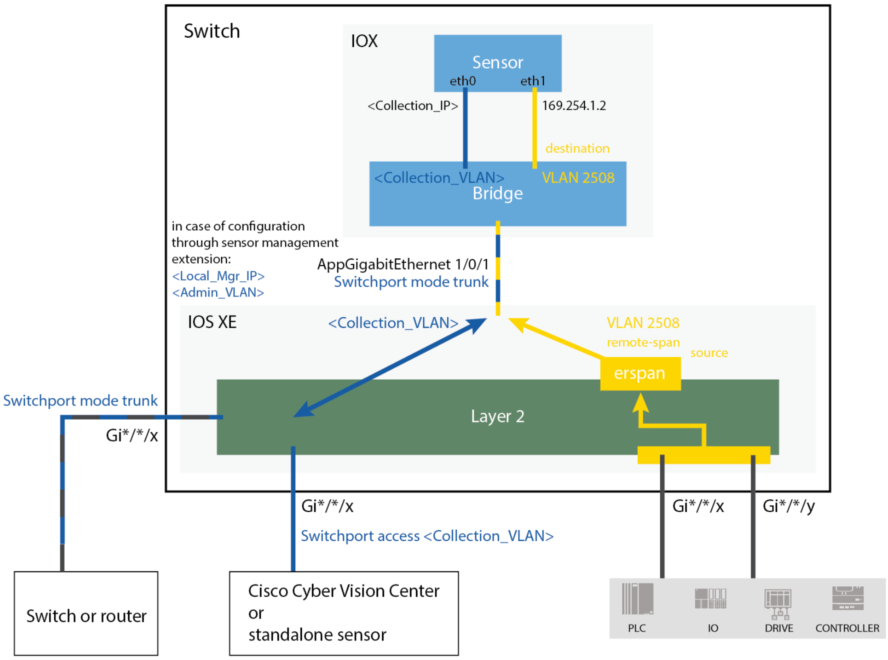
- **Cisco Catalyst IE3300 10G Rugged Series Switch**
- **Cisco Catalyst IE3400 Rugged Series Switch**

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



Architecture diagram for:

- **Cisco Catalyst 9300 Series Switch**
- **Cisco Catalyst 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

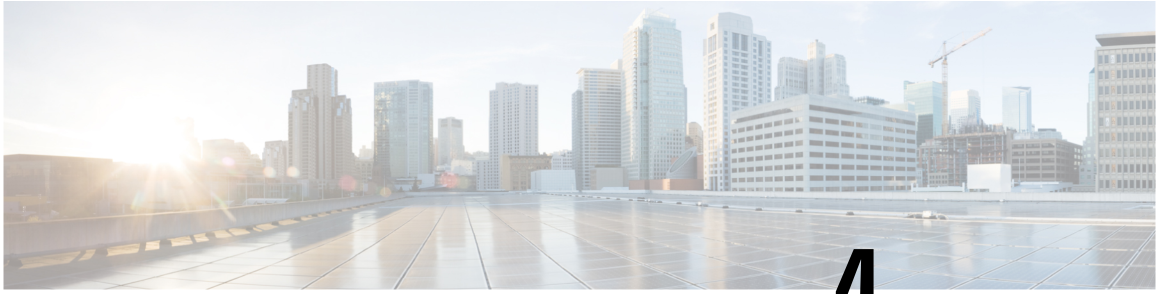
Requirements

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.

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 23 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 IE9300 and Cisco Catalyst 9400 with redundant processor boards.
- The sensor application supports RSPAN on Catalyst 9300 and Catalyst 9400 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

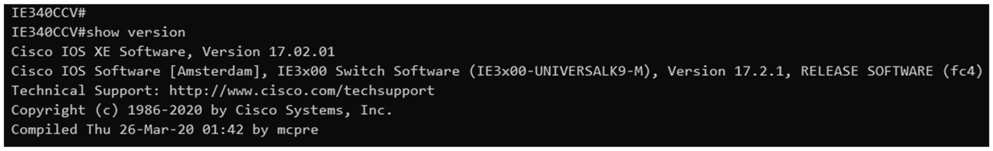
- Check the software version using the following command in the switch's CLI:

```
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
```

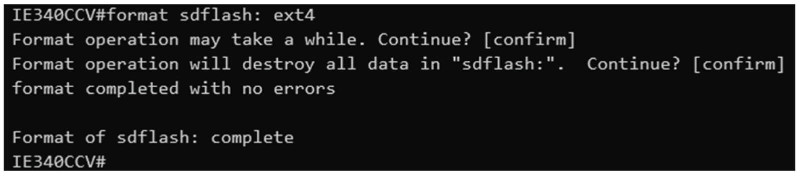
If the version is lower, you must update the switch firmware. To do so, follow the links to the products page in Configure the switch access.

SD Card (IE3x00/IE9x00)

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

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

```
format sdflash: ext4
```

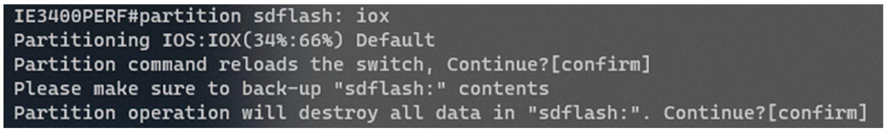


```
IE340CCV#format sdflash: ext4
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "sdflash:".  Continue? [confirm]
format completed with no errors

Format of sdflash: complete
IE340CCV#
```

- You can partition the SD card using the following command:

```
partition sdflash: iox
```

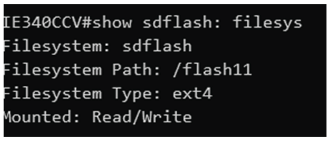


```
IE3400PERF#partition sdflash: iox
Partitioning IOS:IOX(34%:66%) Default
Partition command reloads the switch, Continue?[confirm]
Please make sure to back-up "sdflash:" contents
Partition operation will destroy all data in "sdflash:". Continue?[confirm]
```

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
```



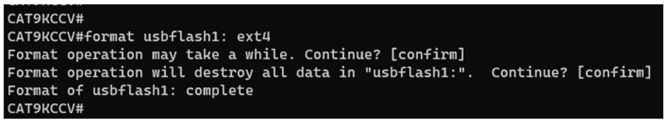
```
IE340CCV#show sdflash: filesys
Filesystem: sdflash
Filesystem Path: /flash11
Filesystem Type: ext4
Mounted: Read/Write
```

SSD Disk (Catalyst 9x00)

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

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

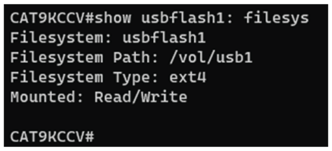
  ```
  format usbflash1: ext4
  ```



```
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.

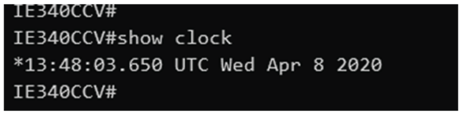
Note Unlike hardware sensors (i.e. Cisco IC3000) that fetch their time from the Center, the Cyber Vision IOX application sensor gets the time from the host (switch platform). Therefore, it is critical that the host synchronizes its time with the Center or a valid NTP server if it's synchronized with 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
   ```

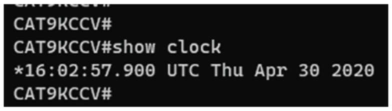
   For examples:

   Cisco IE3400:



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

   Cisco Catalyst 9300:



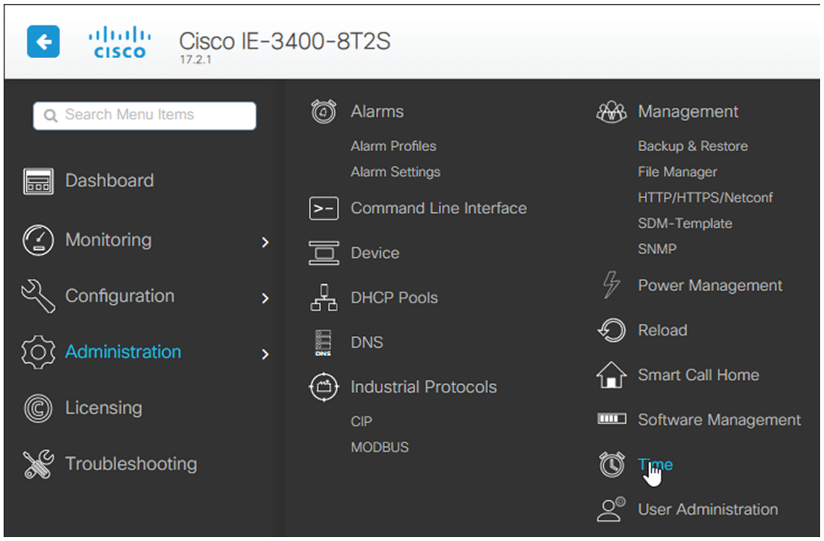
```
CAT9KCCV#
CAT9KCCV#show clock
*16:02:57.900 UTC Thu Apr 30 2020
CAT9KCCV#
```

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

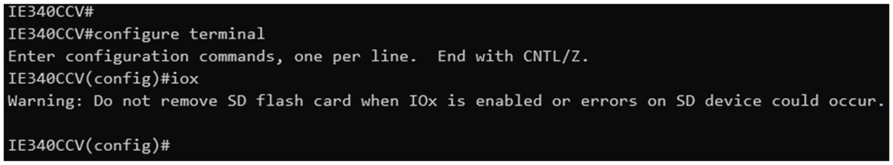
Before installing the Cisco Cyber Vision sensor on the hardware, you must enable IOx.

1. Enable IOx using the following command:

   ```
   configure terminal
   iox
   ```

   For examples:

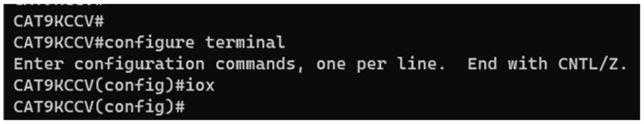
   Cisco IE3400:



```
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:



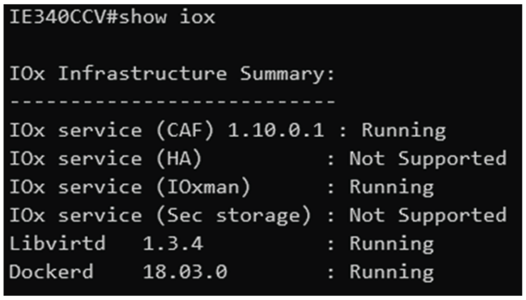
```
CAT9KCCV#
CAT9KCCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT9KCCV(config)#iox
CAT9KCCV(config)#
```

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

```
exit
show iox
```

For examples:

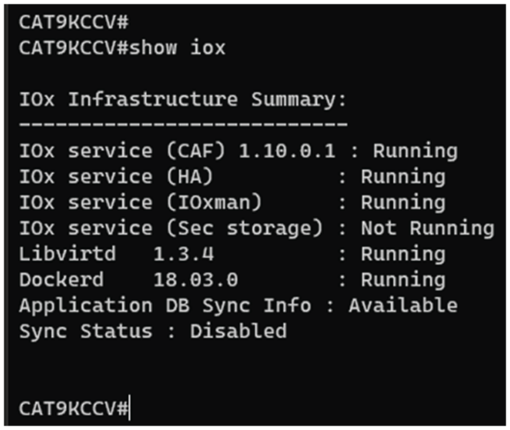
Cisco IE3400:



```
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#
```

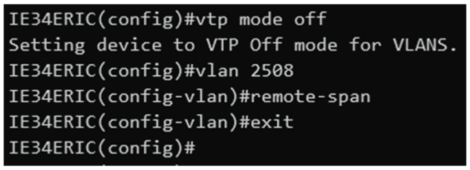
Add the necessary configuration parameters (IE3x00)

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.

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

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

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



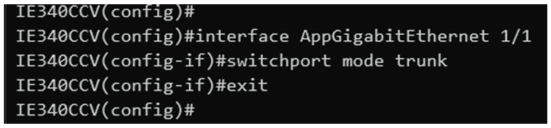
```
IE34ERIC(config)#vtp mode off
Setting device to VTP Off mode for VLANS.
IE34ERIC(config)#vlan 2508
IE34ERIC(config-vlan)#remote-span
IE34ERIC(config-vlan)#exit
IE34ERIC(config)#
```

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.

3. Configure the AppgigabitEthernet port for communications to reach the IOx virtual application using the following commands:

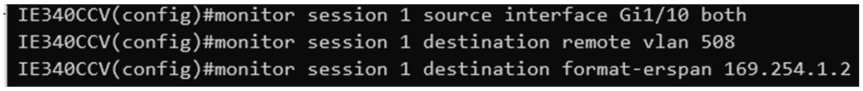
```
interface AppGigabitEthernet 1/1
switchport mode trunk
exit
```



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

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

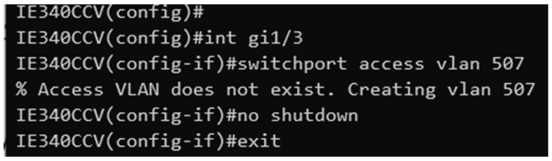
```
monitor session 1 source interface Gi1/10 both
monitor session 1 destination remote vlan 2508
monitor session 1 destination format-erspan 169.254.1.2
```



```
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
```

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

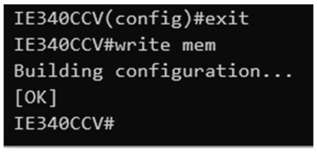
```
int gi1/3
switchport access vlan 507
no shutdown
```



```
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
```

6. Save the configuration using the following commands:

```
exit
write mem
```



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

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 23
- Procedure with the Local Manager, on page 35
- Procedure with the CLI, on page 53

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

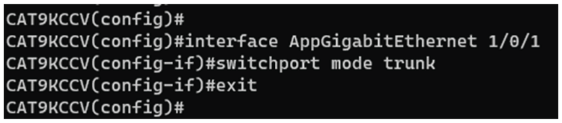
Step 1 Open the switch's CLI through ssh or via the console terminal.

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:

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

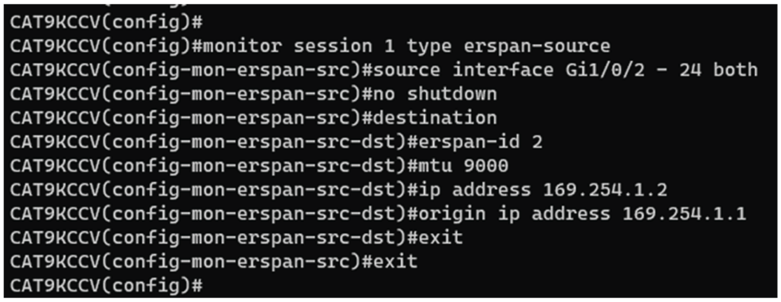


```
CAT9KCCV(config)#
CAT9KCCV(config)#interface AppGigabitEthernet 1/0/1
CAT9KCCV(config-if)#switchport mode trunk
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

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.

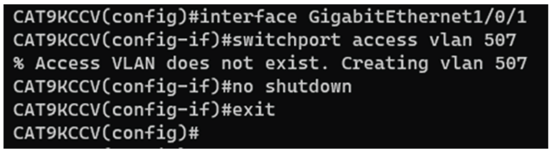
```
monitor session 1 type erspan-source
source interface Gi1/0/2 - 24 both
no shutdown
destination
erspan-id 2
mtu 9000
ip address 169.254.1.2
origin ip address 169.254.1.1
exit
exit
```



```
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:

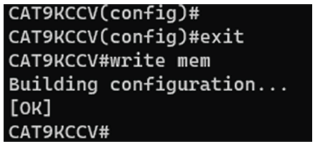
```
interface GigabitEthernet1/0/1
switchport access vlan 507
no shutdown
exit
```



```
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 23
- Procedure with the Local Manager, on page 35
- Procedure with the CLI, on page 53

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

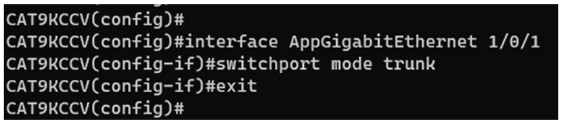
Step 1 Open the switch's CLI through ssh or via the console terminal.

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:

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



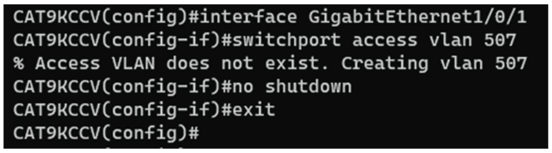
```
CAT9KCCV(config)#
CAT9KCCV(config)#interface AppGigabitEthernet 1/0/1
CAT9KCCV(config-if)#switchport mode trunk
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

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:

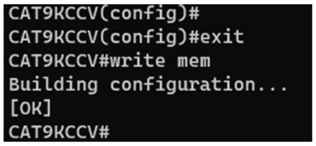
```
interface GigabitEthernet1/0/1
switchport access vlan 507
no shutdown
exit
```



```
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 23
- Procedure with the Local Manager, on page 35
- Procedure with the CLI, on page 53

CHAPTER 7

Procedure with the Cisco Cyber Vision sensor management extension

After the Initial configuration, proceed to the steps described in this section. This section also describes the steps to configure Active Discovery.

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.

Install the sensor management extension

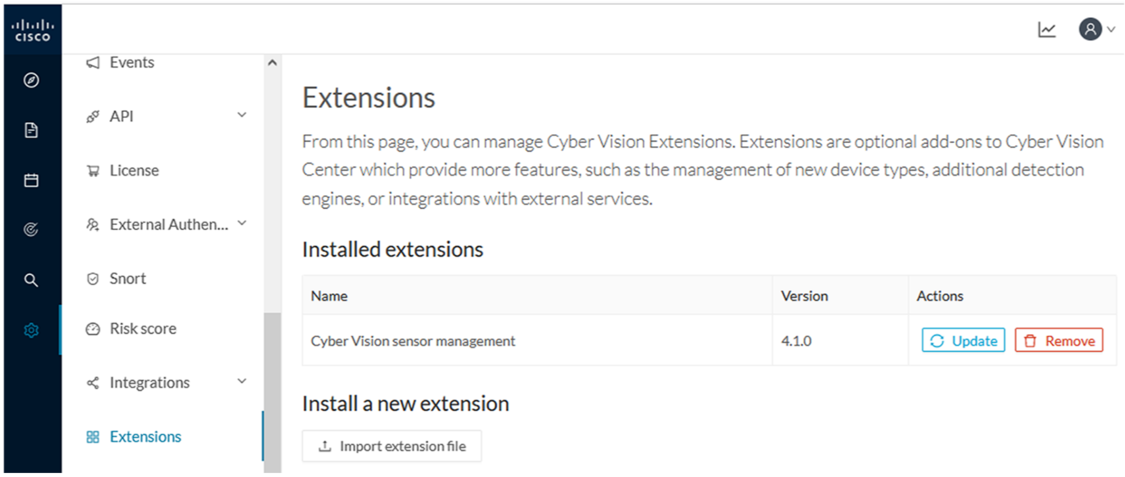
To install the sensor management extension, you must:

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.



Extensions

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

Installed extensions

Name	Version	Actions
Cyber Vision sensor management	4.1.0	Update Remove

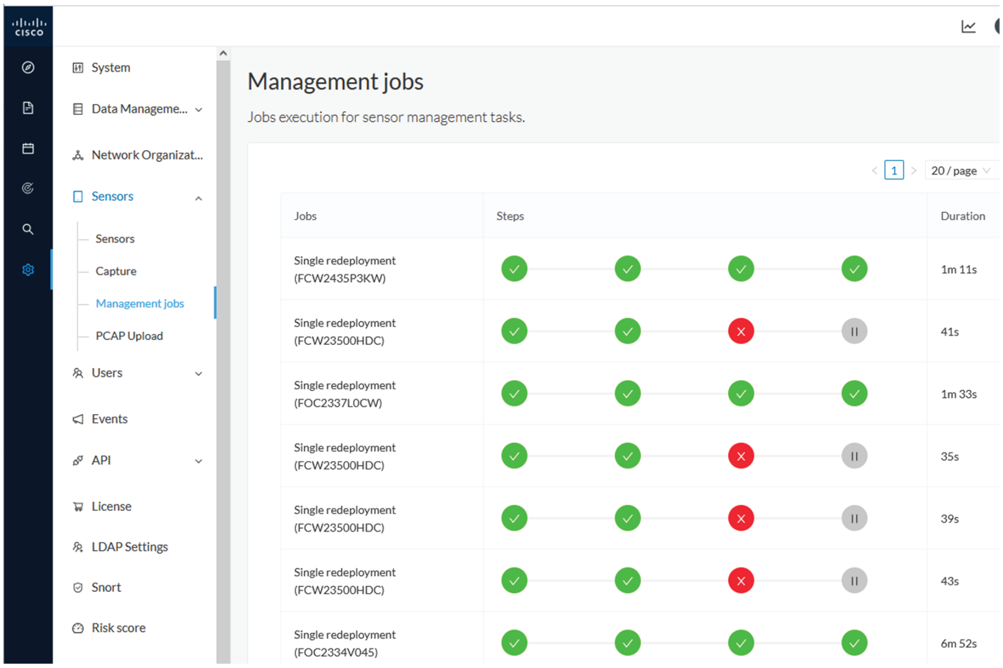
Install a new extension

Once the sensor management extension is installed, you will find a new management job under the sensor administration menu (Management jobs, on page 24), 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.



Management jobs

Jobs execution for sensor management tasks.

Jobs	Steps				Duration
Single redeployment (FCW2435P3KW)	✓	✓	✓	✓	1m 11s
Single redeployment (FCW23500HDC)	✓	✓	✗	⏸	41s
Single redeployment (FOC2337L0CW)	✓	✓	✓	✓	1m 33s
Single redeployment (FCW23500HDC)	✓	✓	✗	⏸	35s
Single redeployment (FCW23500HDC)	✓	✓	✗	⏸	39s
Single redeployment (FCW23500HDC)	✓	✓	✗	⏸	43s
Single redeployment (FOC2334V045)	✓	✓	✓	✓	6m 52s

You will find the following jobs:

- Single deployment

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

- Single redeployment

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

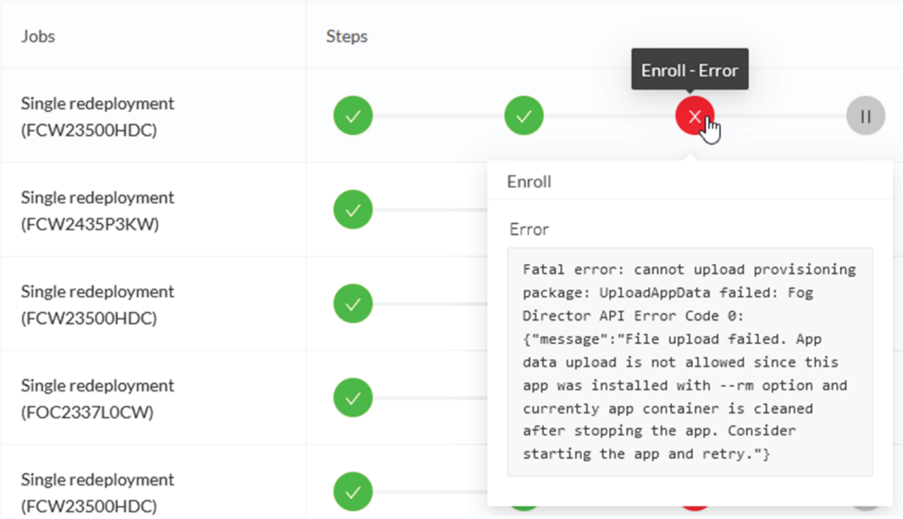
- Single removal

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

- Update all devices

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

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



Jobs	Steps
Single redeployment (FCW23500HDC)	✓ ✓ ✕ ⏸
Single redeployment (FCW2435P3KW)	✓
Single redeployment (FCW23500HDC)	✓
Single redeployment (FOC2337L0CW)	✓
Single redeployment (FCW23500HDC)	✓

Enroll

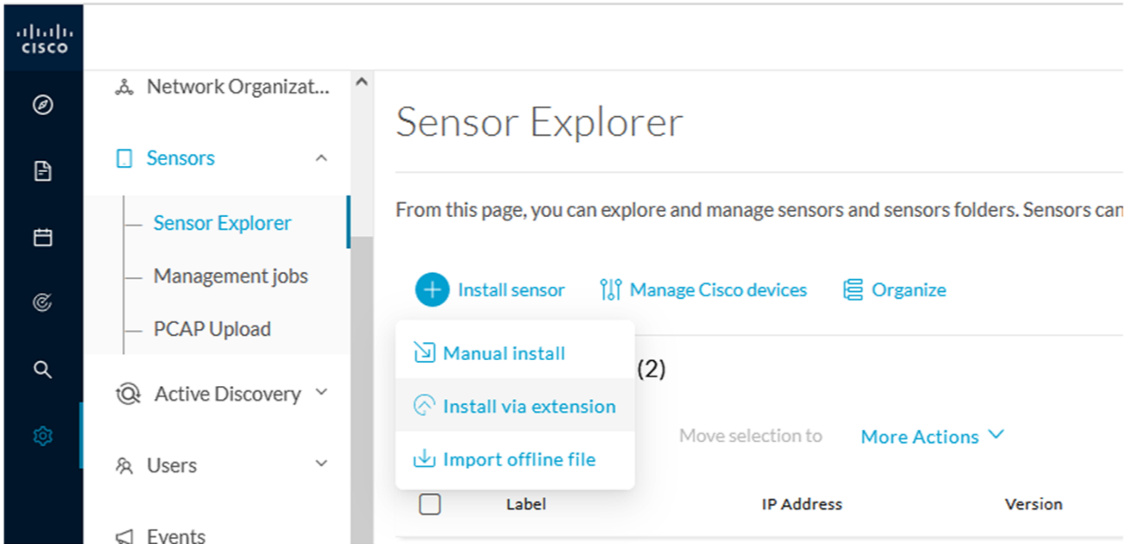
Error

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

Create a sensor in the sensor management extension

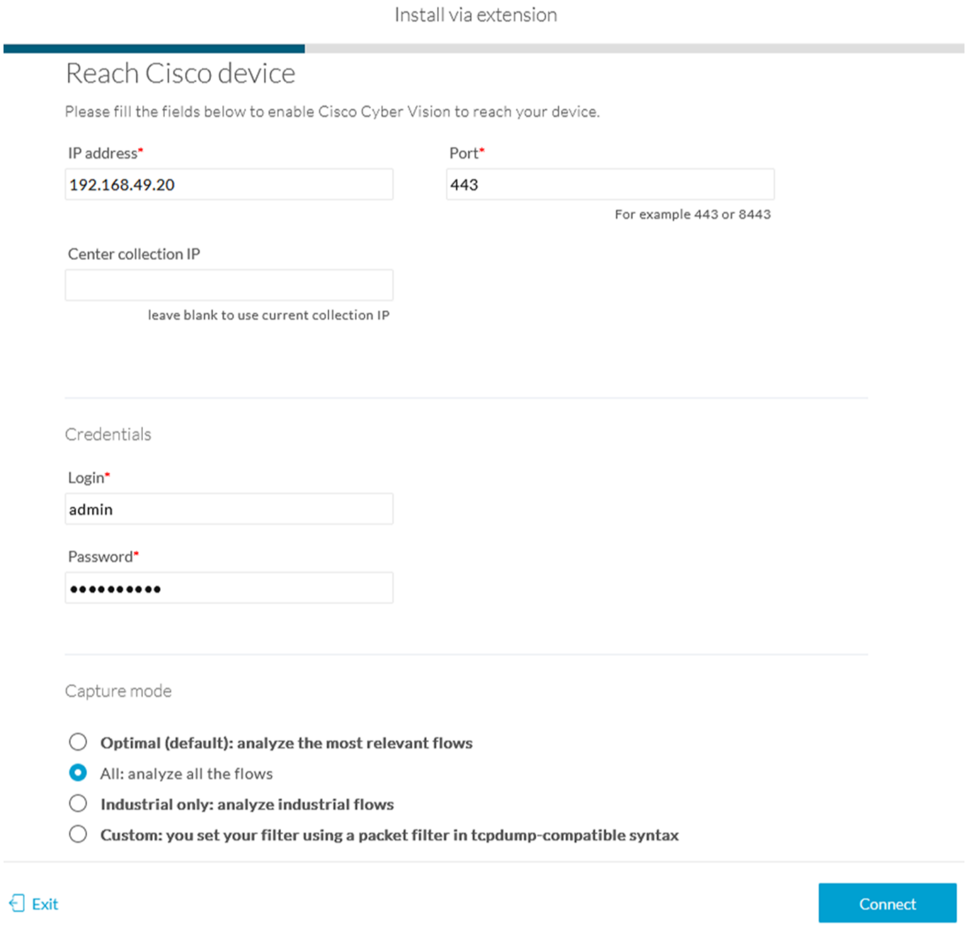
Procedure

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.



Install via extension

Reach Cisco device

Please fill the fields below to enable Cisco Cyber Vision to reach your device.

IP address*: 192.168.49.20

Port*: 443

For example 443 or 8443

Center collection IP:

leave blank to use current collection IP

Credentials

Login*: admin

Password*: ●●●●●●●●●●

Capture mode

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

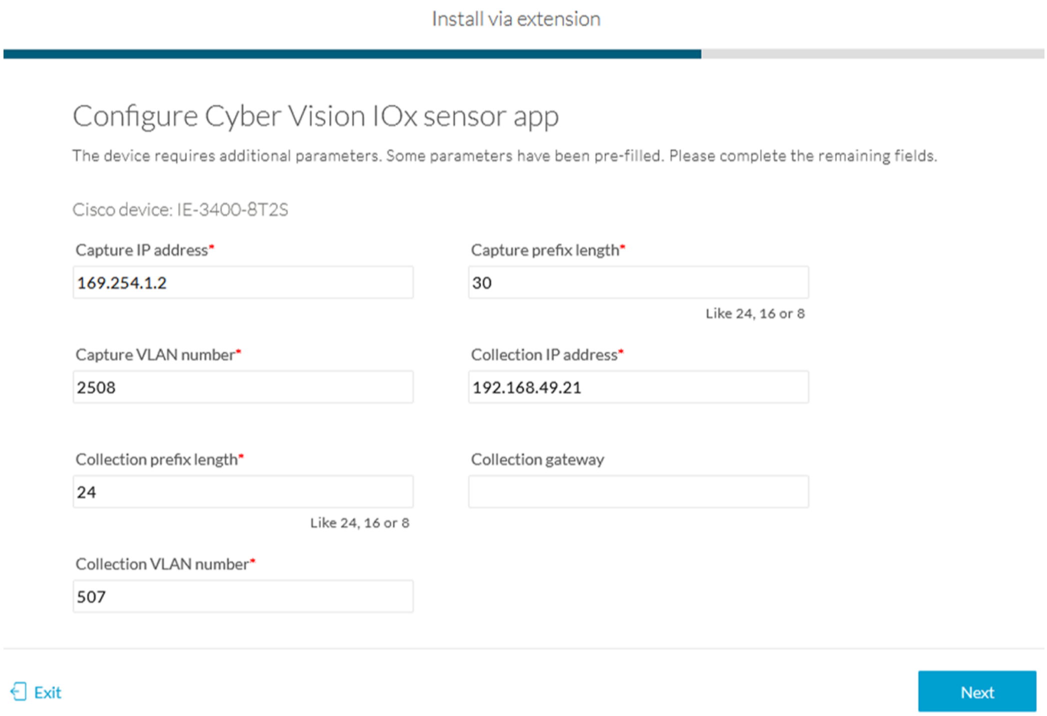
Step 3 Click **Connect**.

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:



Install via extension

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

Cisco device: IE-3400-8T2S

Capture IP address*: 169.254.1.2

Capture prefix length*: 30 (Like 24, 16 or 8)

Capture VLAN number*: 2508

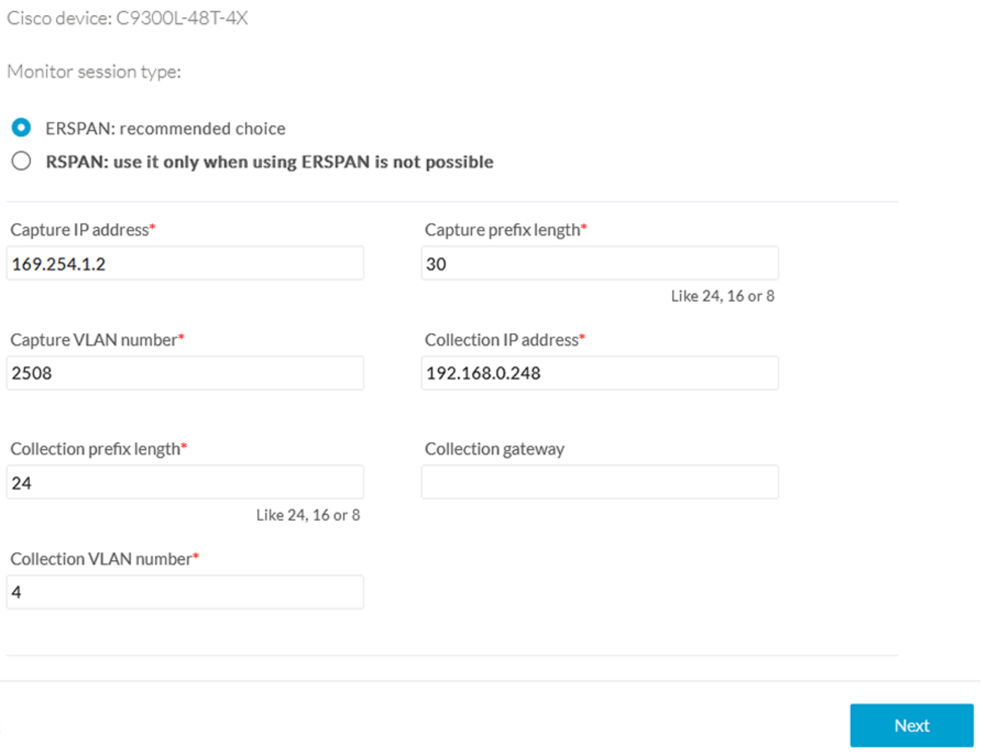
Collection IP address*: 192.168.49.21

Collection prefix length*: 24 (Like 24, 16 or 8)

Collection gateway:

Collection VLAN number*: 507

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



Cisco device: C9300L-48T-4X

Monitor session type:

● ERSPAN: recommended choice

○ **RSPAN: use it only when using ERSPAN is not possible**

Capture IP address*: 169.254.1.2

Capture prefix length*: 30 (Like 24, 16 or 8)

Capture VLAN number*: 2508

Collection IP address*: 192.168.0.248

Collection prefix length*: 24 (Like 24, 16 or 8)

Collection gateway:

Collection VLAN number*: 4

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

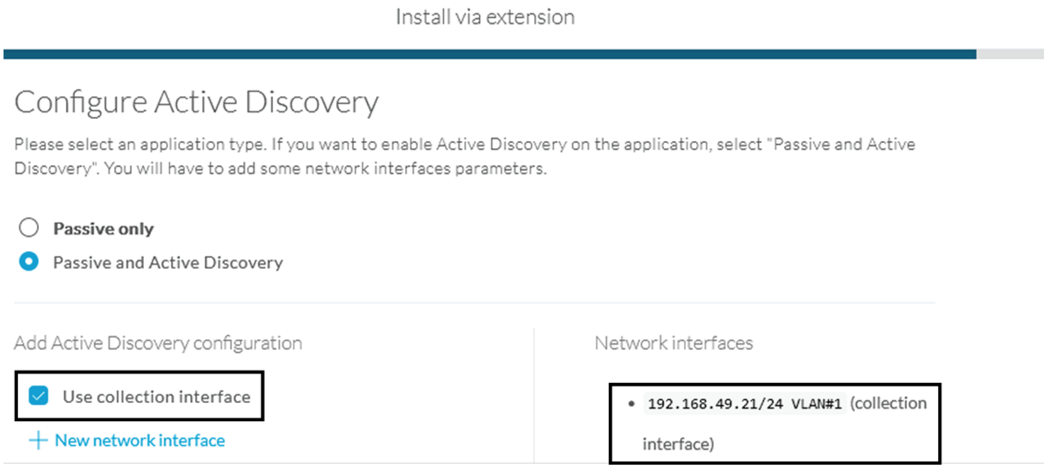
Step 2 Click **Next**.

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:



Install via extension

Configure Active Discovery

Please select an application type. If you want to enable Active Discovery on the application, select "Passive and Active Discovery". You will have to add some network interfaces parameters.

○ Passive only
● Passive and Active Discovery

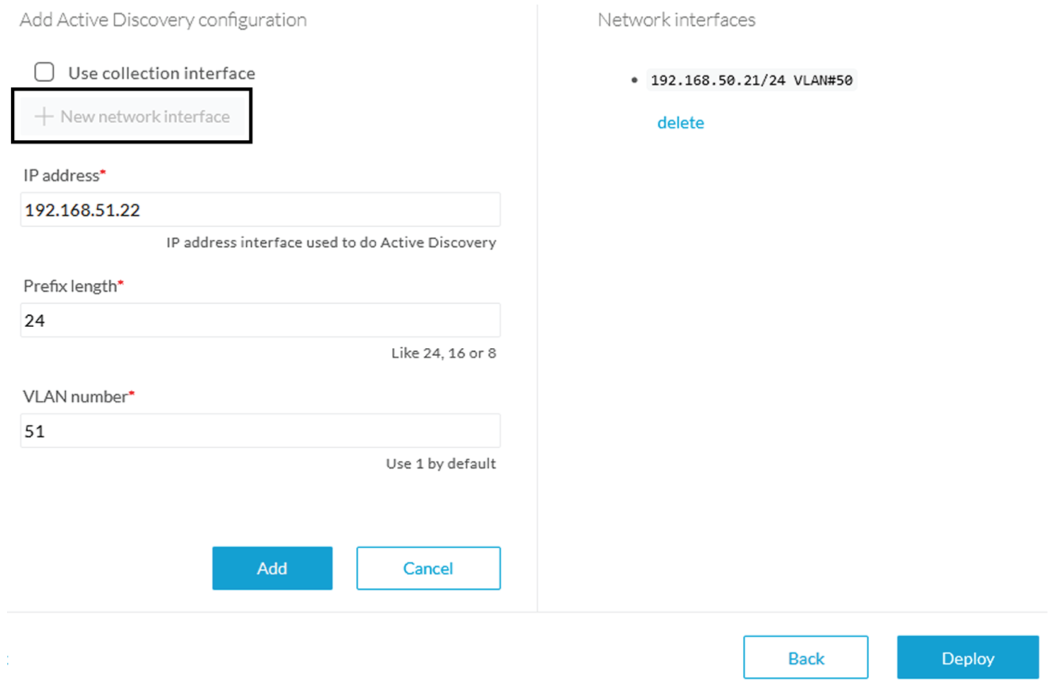
Add Active Discovery configuration

☑ Use collection interface

Network interfaces

- 192.168.49.21/24 VLAN#1 (collection interface)

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



Add Active Discovery configuration

☐ Use collection interface

IP address*

192.168.51.22

IP address interface used to do Active Discovery

Prefix length*

24

Like 24, 16 or 8

VLAN number*

51

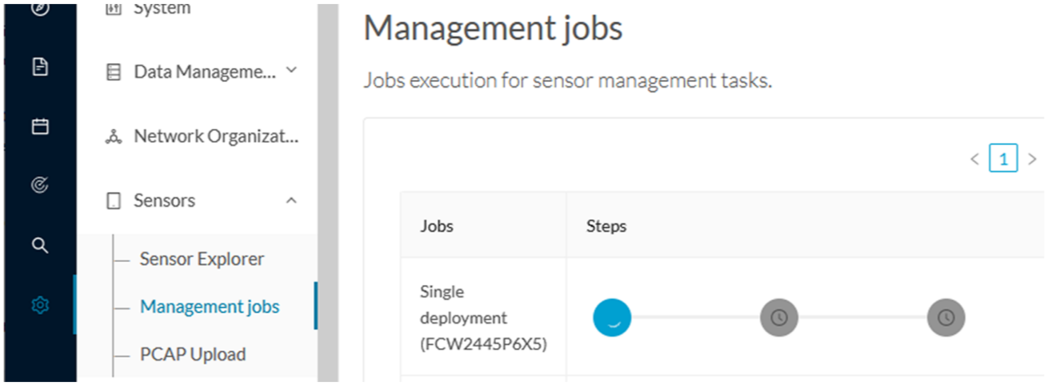
Use 1 by default

Network interfaces

- `192.168.50.21/24 VLAN#50`

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.



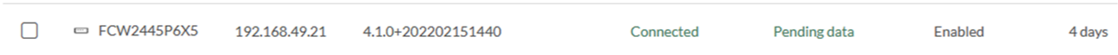
Management jobs

Jobs execution for sensor management tasks.

Jobs	Steps
Single deployment (FCW2445P6X5)	

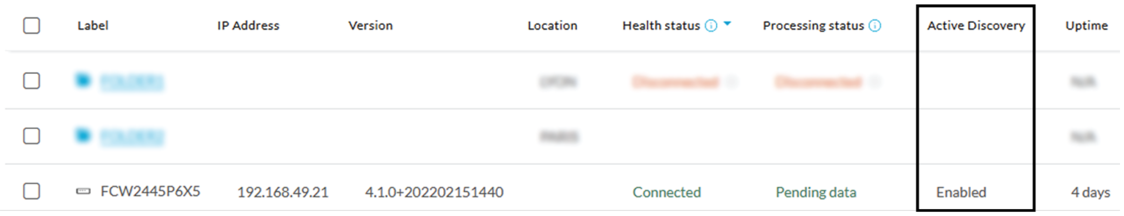
Once the deployment is finished, a new sensor appears in the sensors list.

The sensor's status will eventually turn to connected.



☐	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	4 days

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.



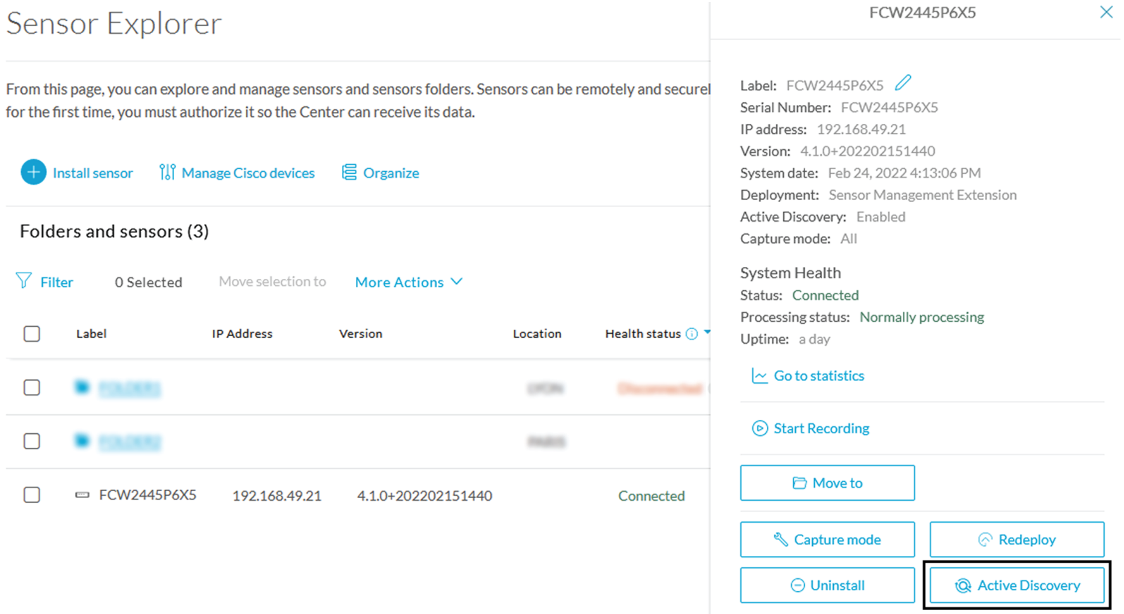
□	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
□	FOLDER1			LYON	Disconnected	Disconnected		N/A
□	FOLDER2			PARIS				N/A
□	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days

Configure Active Discovery

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

Procedure

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



Sensor Explorer

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

Folders and sensors (3)

□	Label	IP Address	Version	Location	Health status
□	FOLDER1			LYON	Disconnected
□	FOLDER2			PARIS	
□	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected

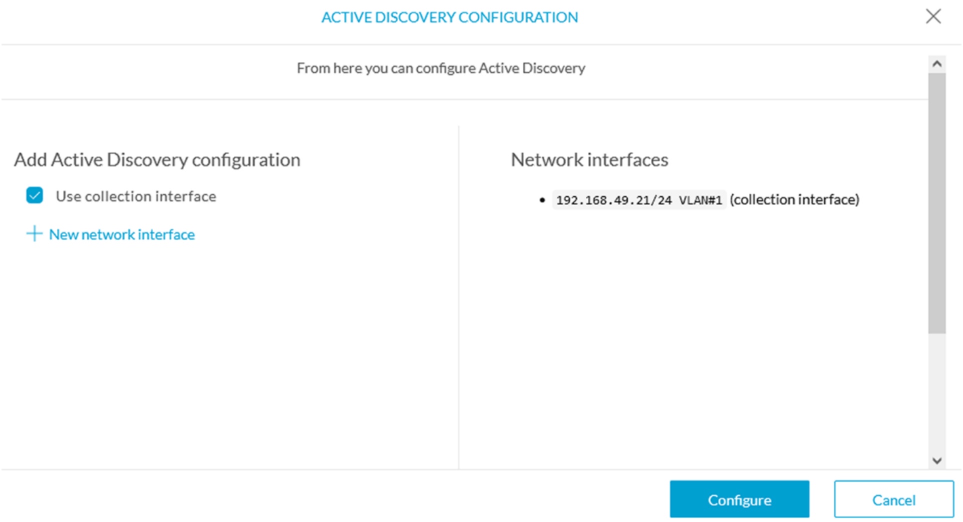
FCW2445P6X5

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

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

The Active Discovery configuration appears with the interface currently set.

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



ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

☑ Use collection interface

Network interfaces

- `192.168.49.21/24 VLAN#1` (collection interface)

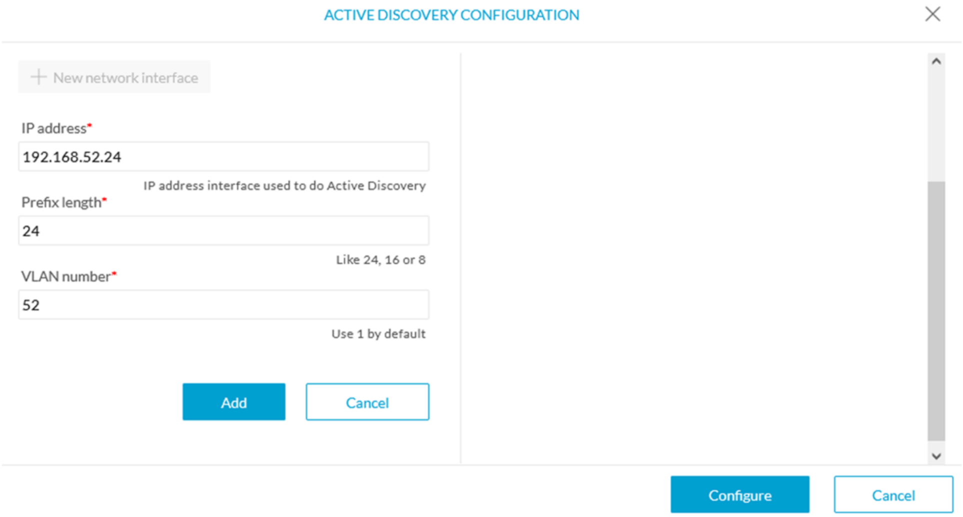
To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

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**.



ACTIVE DISCOVERY CONFIGURATION

IP address*: 192.168.52.24
IP address interface used to do Active Discovery

Prefix length*: 24
Like 24, 16 or 8

VLAN number*: 52
Use 1 by default

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.

CHAPTER 8

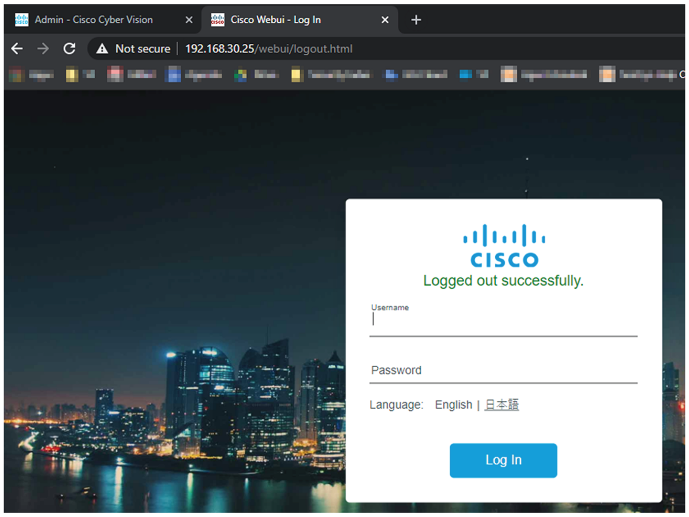
Procedure with the Local Manager

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.

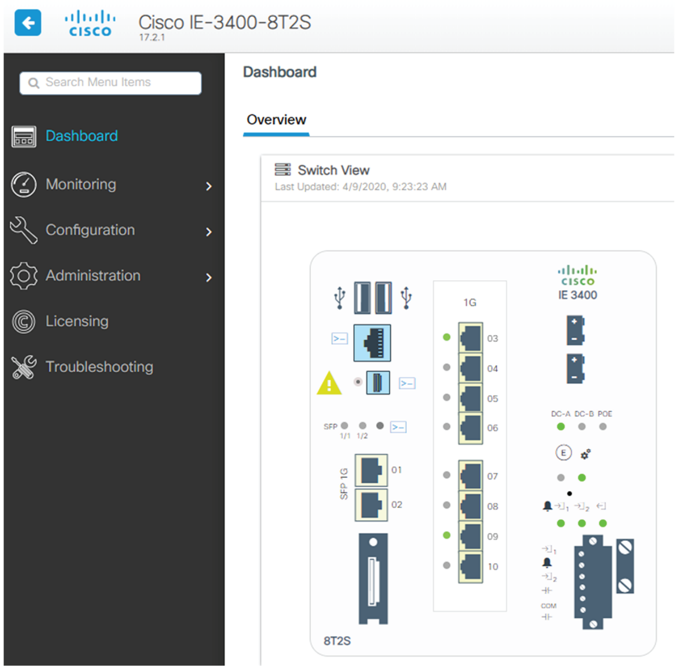
2. Log in using the Local Manager user account and password.



Not secure | 192.168.30.25/webui/logout.html

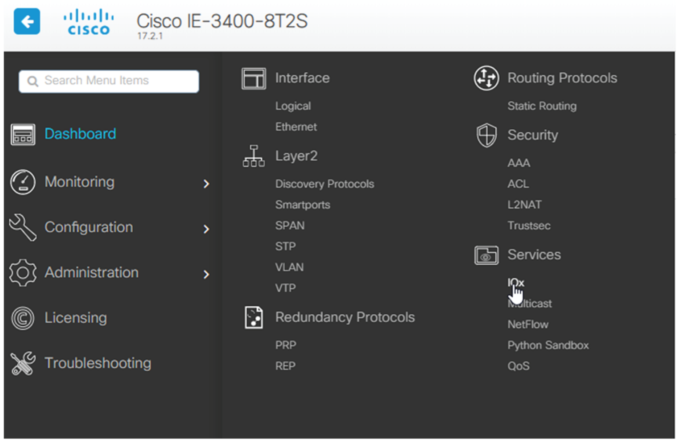
Logged out successfully.

For example: Cisco IE3300 10G/IE3400

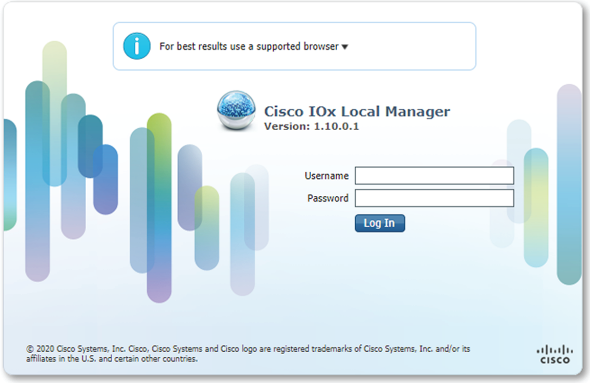


3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.

   For example: Cisco IE3300 10G/IE3400



4. Log in using the user account and password.



For best results use a supported browser ▾

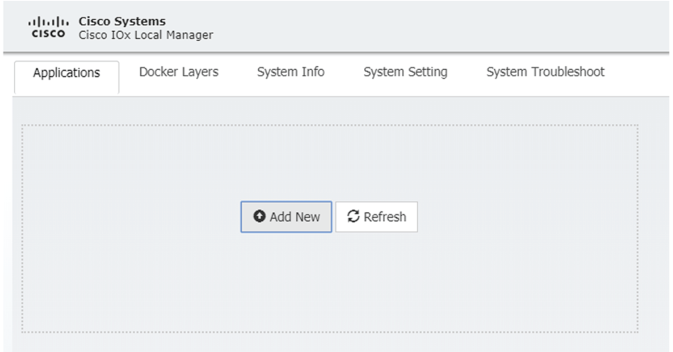
Cisco IOx Local Manager
Version: 1.10.0.1

Username
Password
Log In

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

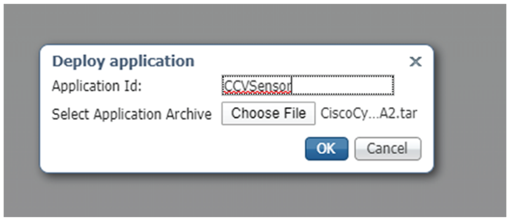
Install the sensor virtual application

Once logged in, the following menu appears:



Cisco Systems
Cisco IOx Local Manager

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

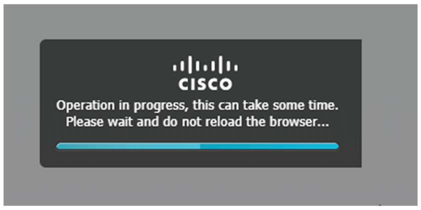


Deploy application

Application Id: CCVSensor

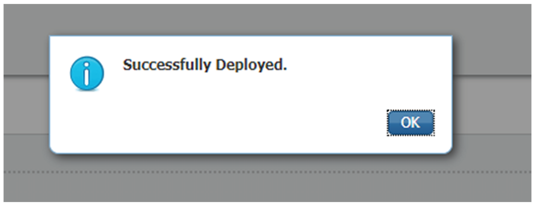
Select Application Archive: CiscoCy...A2.tar

The installation takes a few minutes.



Operation in progress, this can take some time.
Please wait and do not reload the browser...

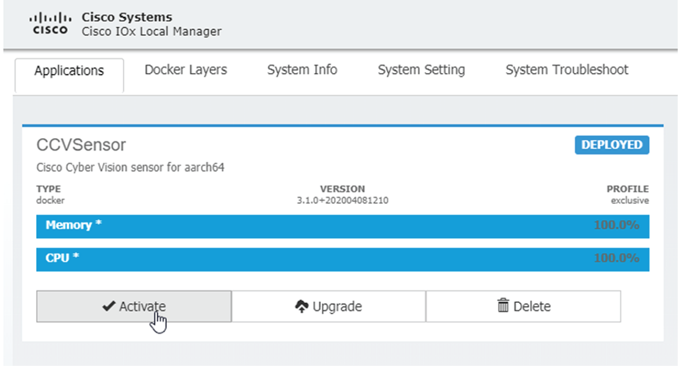
When the application is installed, the following message is displayed:



Successfully Deployed.

Configure the sensor virtual application (IE3x00/IE9x00)

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



Cisco Systems
Cisco IOx Local Manager

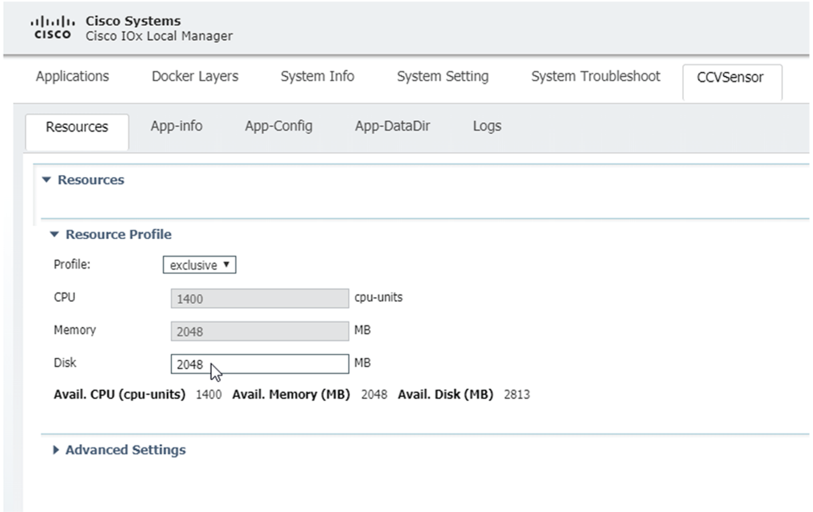
CCVSensor — DEPLOYED

Cisco Cyber Vision sensor for aarch64

TYPE: docker
VERSION: 3.1.0+202004081210
PROFILE: exclusive

Memory * 100.0%
CPU * 100.0%

2. Change the disk size from the default size to 2048 MB. The disk size must not be larger than this.



Profile: exclusive

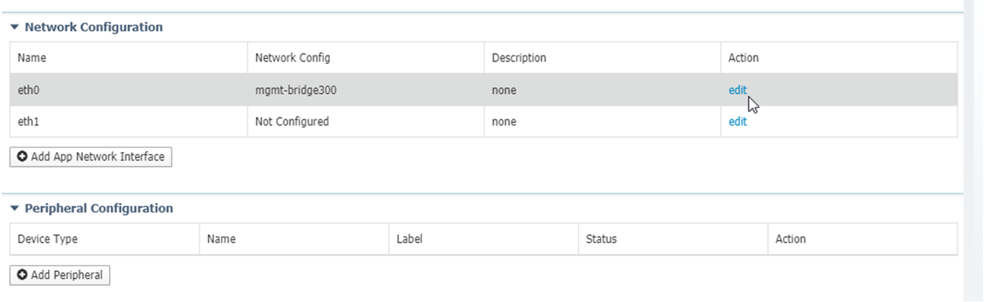
CPU 1400 cpu-units

Memory 2048 MB

Disk 2048 MB

Avail. CPU (cpu-units) 1400 Avail. Memory (MB) 2048 Avail. Disk (MB) 2813

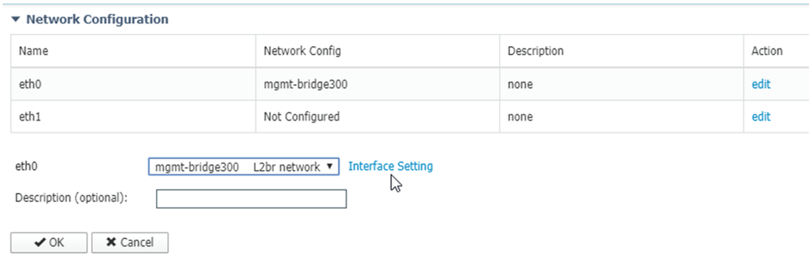
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking **edit** in the eth0 line.



Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	Not Configured	none	edit

Device Type	Name	Label	Status	Action

4. Click **Interface Setting**.



Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	Not Configured	none	edit

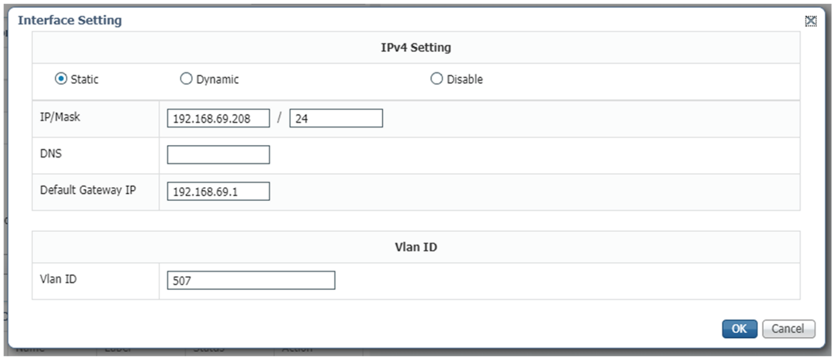
eth0 mgmt-bridge300 L2br network

Description (optional):

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.



Interface Setting

IPv4 Setting

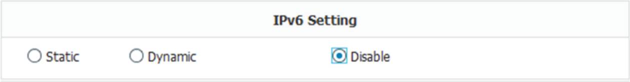
● Static ○ Dynamic ○ Disable

IP/Mask	192.168.69.208 / 24
DNS	
Default Gateway IP	192.168.69.1

Vlan ID

Vlan ID	507

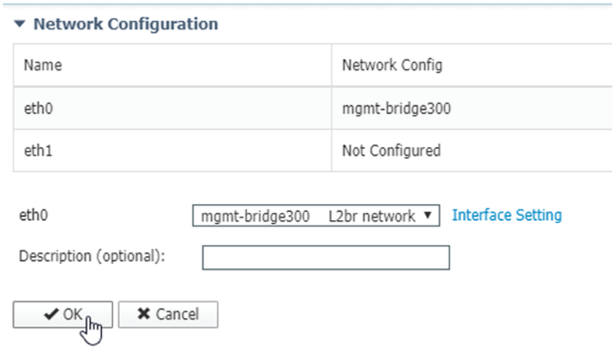
6. IPV6 must be set to Disable.



IPv6 Setting

○ Static ○ Dynamic ● Disable

7. Click **OK** twice.



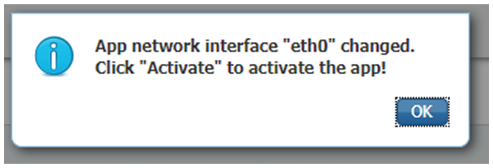
Network Configuration

Name	Network Config
eth0	mgmt-bridge300
eth1	Not Configured

eth0 mgmt-bridge300 L2br network ▾ Interface Setting

Description (optional):

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



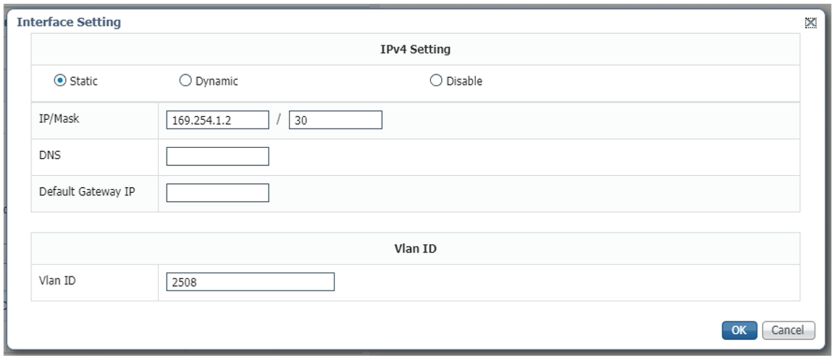
App network interface "eth0" changed.
Click "Activate" to activate the app!

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.



Interface Setting

IPv4 Setting

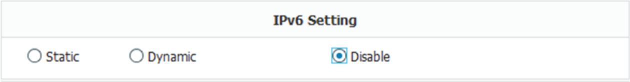
● Static ○ Dynamic ○ Disable

IP/Mask	169.254.1.2 / 30
DNS	
Default Gateway IP	

Vlan ID

Vlan ID	2508

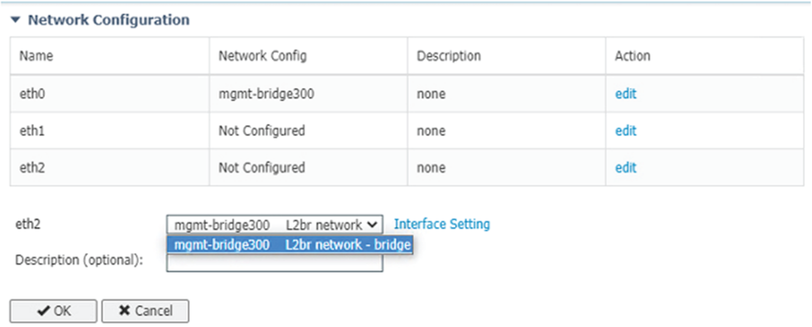
10. IPV6 must be set to **Disable**.



IPv6 Setting

○ Static ○ Dynamic ● Disable

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



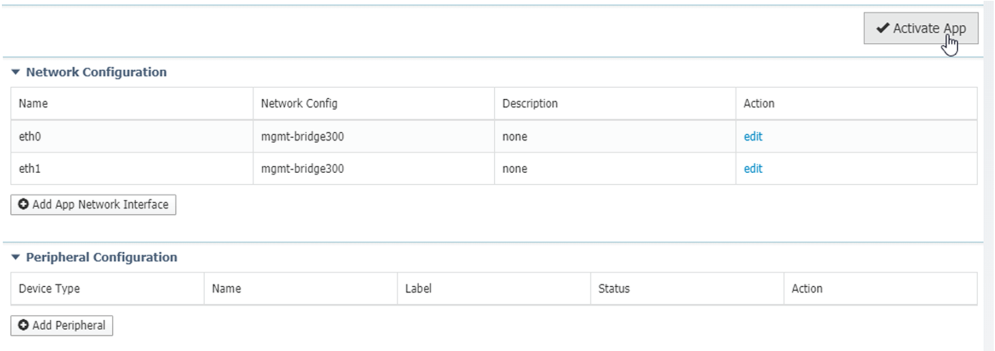
Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	Not Configured	none	edit
eth2	Not Configured	none	edit

eth2: mgmt-bridge300 L2br network (selected: mgmt-bridge300 L2br network - bridge) Interface Setting

Description (optional):

12. Click the **Activate App** button.



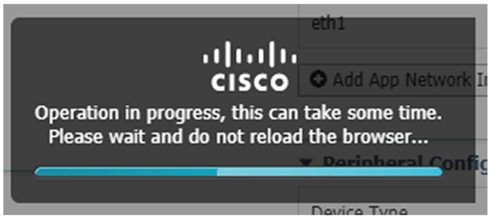
Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	mgmt-bridge300	none	edit

Peripheral Configuration

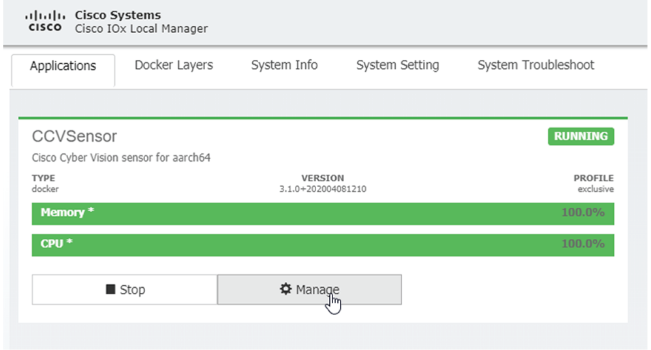
Device Type	Name	Label	Status	Action

The operation takes several minutes.



Operation in progress, this can take some time.
Please wait and do not reload the browser...

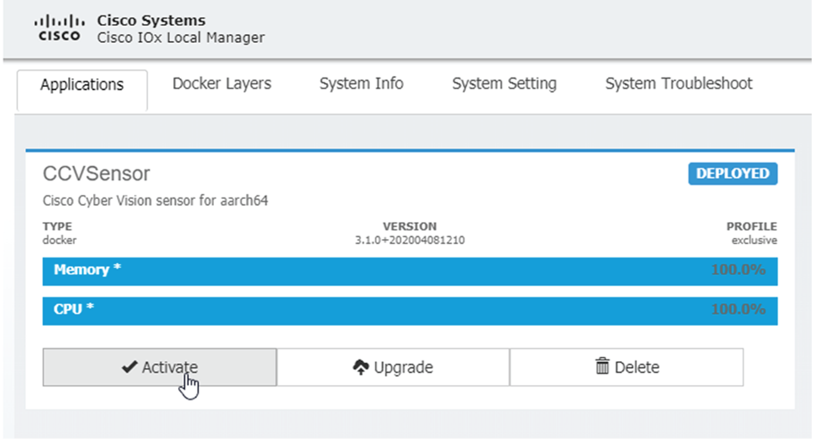
The application status changes to "RUNNING":



CCVSensor RUNNING
Cisco Cyber Vision sensor for aarch64
TYPE docker
VERSION 3.1.0+202004081210
PROFILE exclusive
Memory * 100.0%
CPU * 100.0%

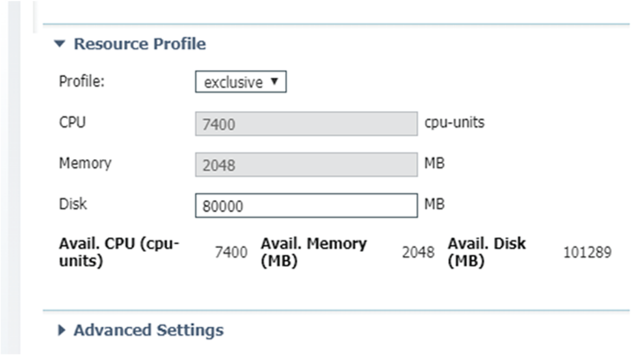
Configure the sensor virtual application (Catalyst 9x00)

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



CCVSensor DEPLOYED
Cisco Cyber Vision sensor for aarch64
TYPE docker
VERSION 3.1.0+202004081210
PROFILE exclusive
Memory * 100.0%
CPU * 100.0%

2. Change the disk size from the default size to 80,000 MB. The disk size must not be smaller than this.



▼ Resource Profile

Profile: exclusive ▼

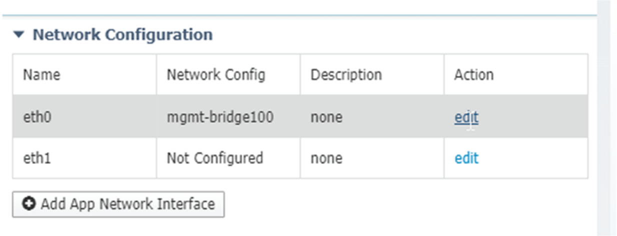
CPU 7400 cpu-units

Memory 2048 MB

Disk 80000 MB

Avail. CPU (cpu-units)	7400	Avail. Memory (MB)	2048	Avail. Disk (MB)	101289

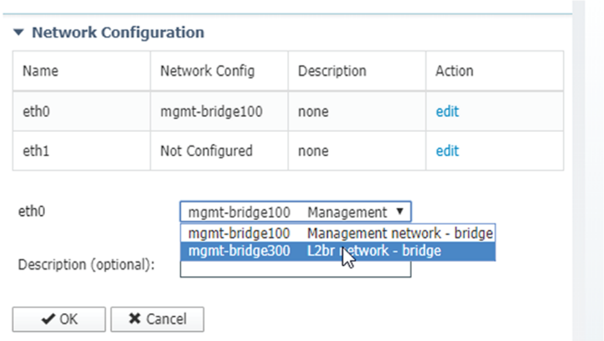
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking **edit** in the eth0 line.



▼ Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge100	none	edit
eth1	Not Configured	none	edit

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



▼ Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge100	none	edit
eth1	Not Configured	none	edit

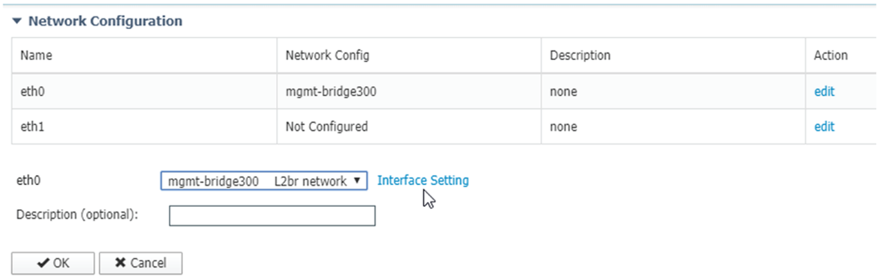
eth0 mgmt-bridge100 Management ▼

mgmt-bridge100 Management network - bridge

mgmt-bridge300 L2br network - bridge

Description (optional):

5. Click **Interface Setting**.



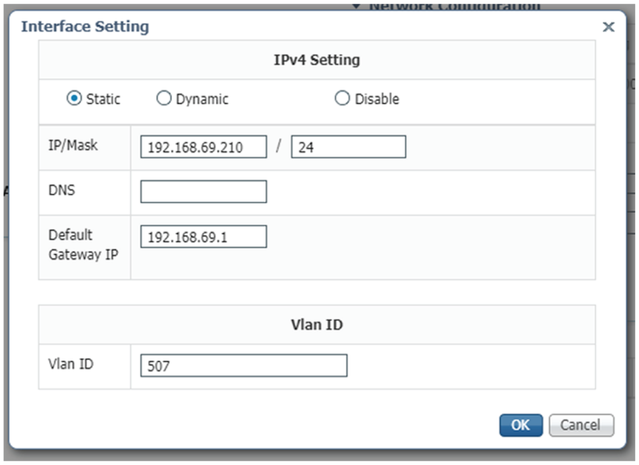
▼ Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	Not Configured	none	edit

eth0 mgmt-bridge300 L2br network ▾ Interface Setting

Description (optional):

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.



Interface Setting

IPv4 Setting

● Static ○ Dynamic ○ Disable

IP/Mask: 192.168.69.210 / 24

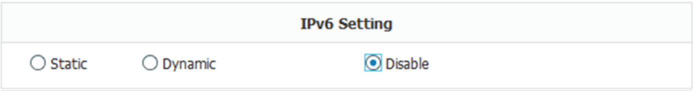
DNS:

Default Gateway IP: 192.168.69.1

Vlan ID

Vlan ID: 507

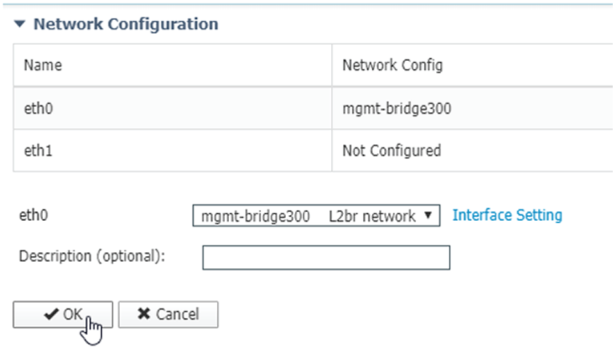
7. IPV6 must be set to **Disable**.



IPv6 Setting

○ Static ○ Dynamic ● Disable

8. Click **OK** twice.



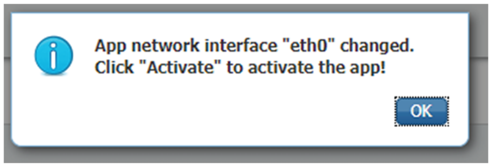
▼ Network Configuration

Name	Network Config
eth0	mgmt-bridge300
eth1	Not Configured

eth0 mgmt-bridge300 L2br network ▼ Interface Setting

Description (optional):

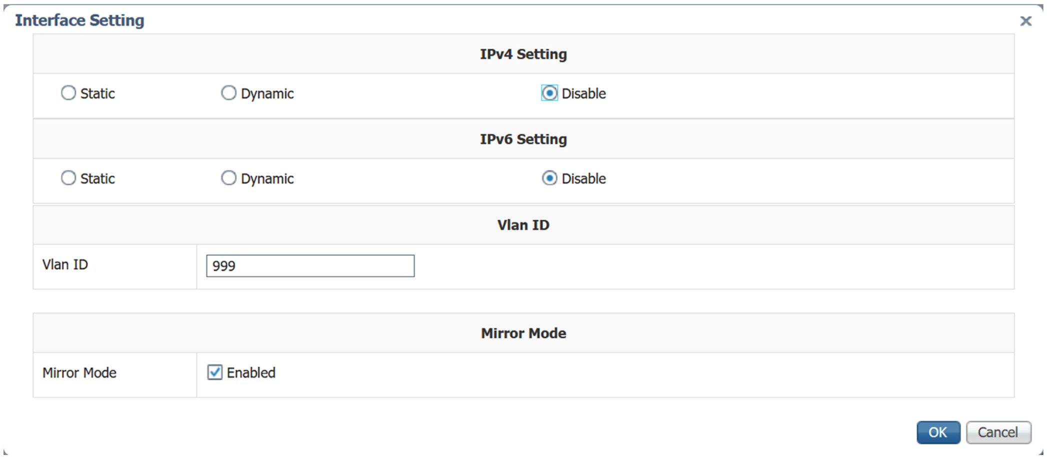
9. Click **OK** again on the following popup.



App network interface "eth0" changed.
Click "Activate" to activate the app!

10. Apply the following configurations to eth1:

    - Disable IPv4.
    - Disable IPv6.
    - Set the VLAN id.
    - **Set the mirror mode as enabled**.



Interface Setting

IPv4 Setting

○ Static ○ Dynamic ● Disable

IPv6 Setting

○ Static ○ Dynamic ● Disable

Vlan ID

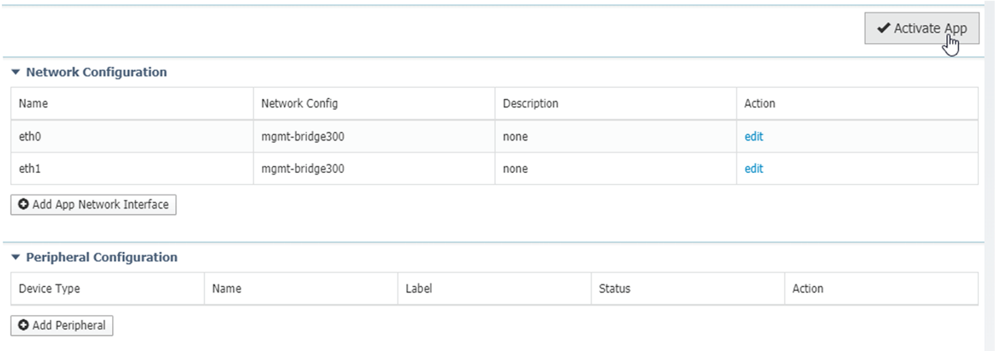
Vlan ID: 999

Mirror Mode

Mirror Mode: ☑ Enabled

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

12. Click the **Activate App** button.



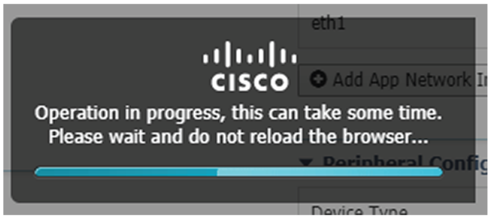
▾ Network Configuration

Name	Network Config	Description	Action
eth0	mgmt-bridge300	none	edit
eth1	mgmt-bridge300	none	edit

▾ Peripheral Configuration

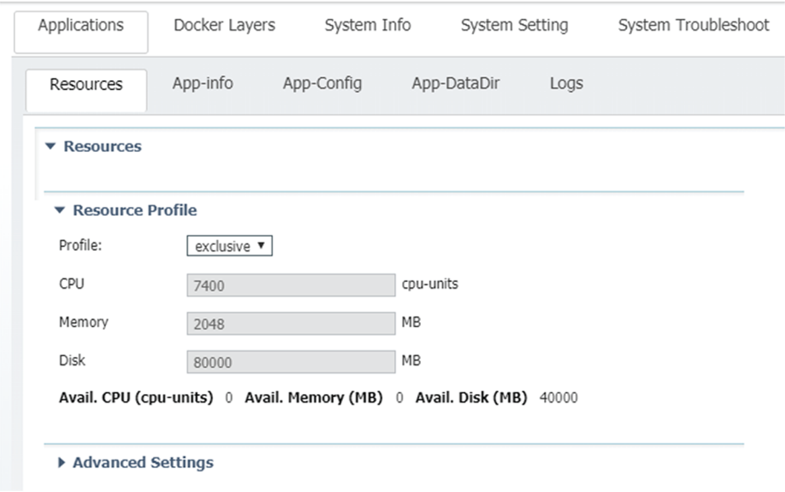
Device Type	Name	Label	Status	Action

The operation takes several seconds.



Operation in progress, this can take some time.
Please wait and do not reload the browser...

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



▾ Resources

▾ Resource Profile

Profile: exclusive ▾

CPU 7400 cpu-units

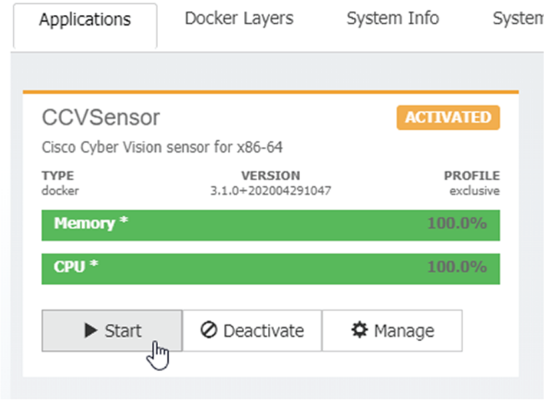
Memory 2048 MB

Disk 80000 MB

Avail. CPU (cpu-units) 0 **Avail. Memory (MB)** 0 **Avail. Disk (MB)** 40000

▸ Advanced Settings

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



CCVSensor ACTIVATED

Cisco Cyber Vision sensor for x86-64

TYPE docker

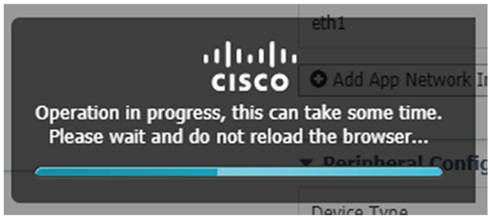
VERSION 3.1.0+202004291047

PROFILE exclusive

Memory * 100.0%

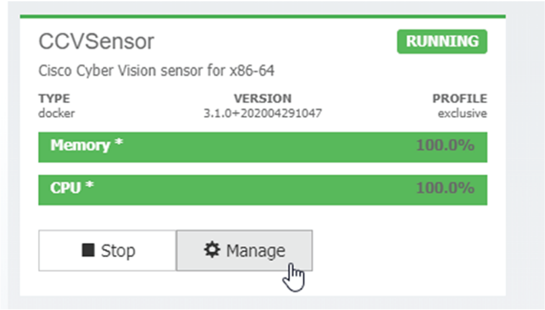
CPU * 100.0%

The operation takes several seconds.



Operation in progress, this can take some time.
Please wait and do not reload the browser...

The application status changes to "RUNNING".



CCVSensor RUNNING

Cisco Cyber Vision sensor for x86-64

TYPE docker

VERSION 3.1.0+202004291047

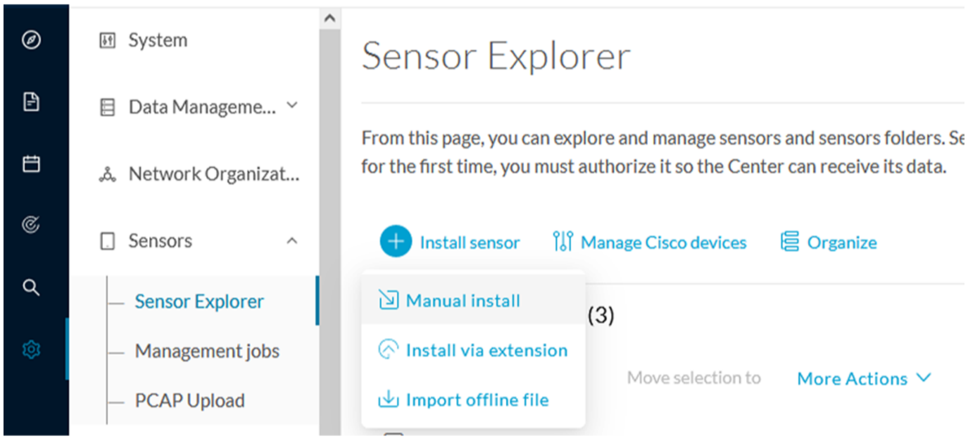
PROFILE exclusive

Memory * 100.0%

CPU * 100.0%

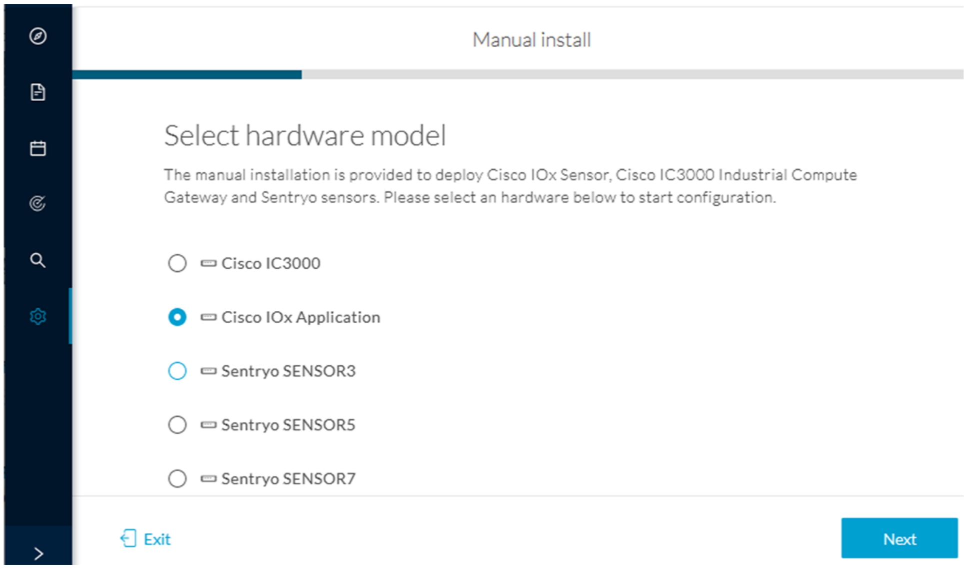
Generate the provisioning package

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

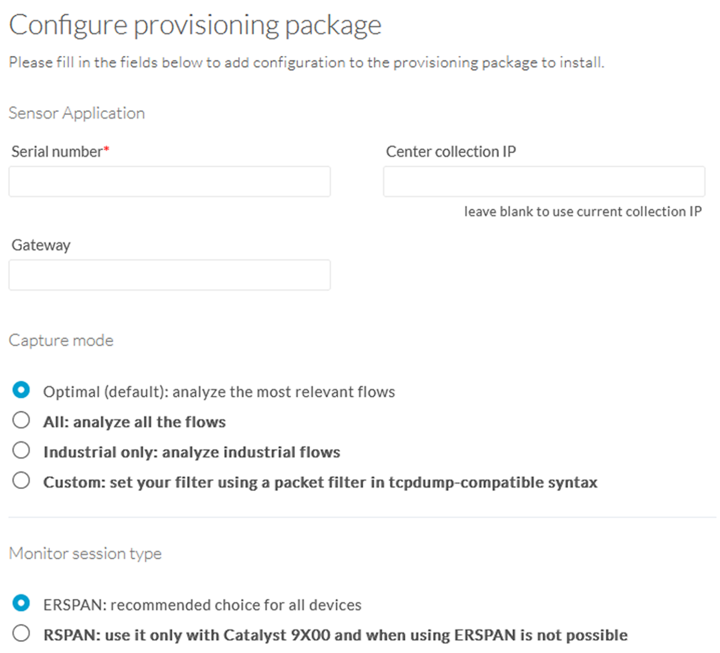


The manual install wizard appears.

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


Manual install
Select hardware model
The manual installation is provided to deploy Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and Sentryo sensors. Please select an hardware below to start configuration.
○ Cisco IC3000
● Cisco IOx Application
○ Sentryo SENSOR3
○ Sentryo SENSOR5
○ Sentryo SENSOR7
Exit
Next

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



Configure provisioning package

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

Sensor Application

Serial number*

Center collection IP

leave blank to use current collection IP

Gateway

Capture mode

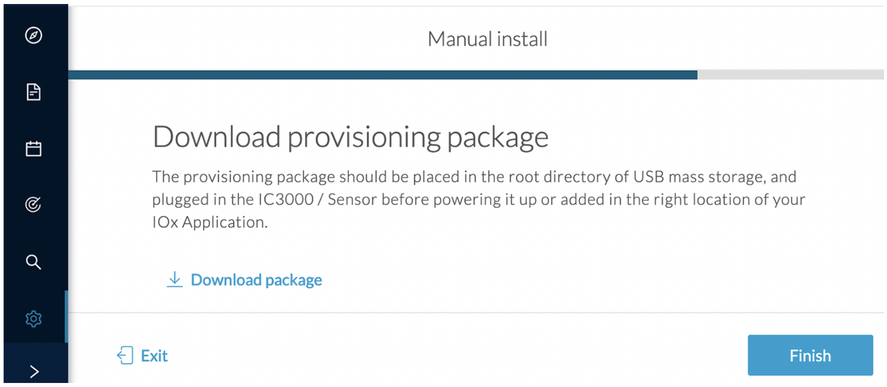
● Optimal (default): analyze the most relevant flows
○ All: analyze all the flows
○ Industrial only: analyze industrial flows
○ Custom: set your filter using a packet filter in tcpdump-compatible syntax

Monitor session type

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

4. Click **Create sensor**.

5. Click the link to download the provisioning package.



Manual install

Download provisioning package

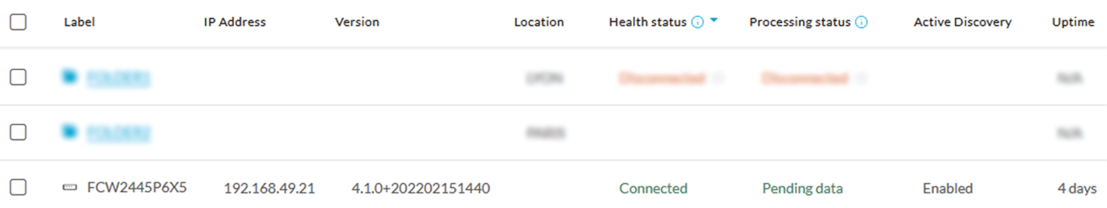
The provisioning package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or added in the right location of your IOx Application.

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

6. Click **Finish**.

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

The sensor status will switch from Disconnected to Connected.

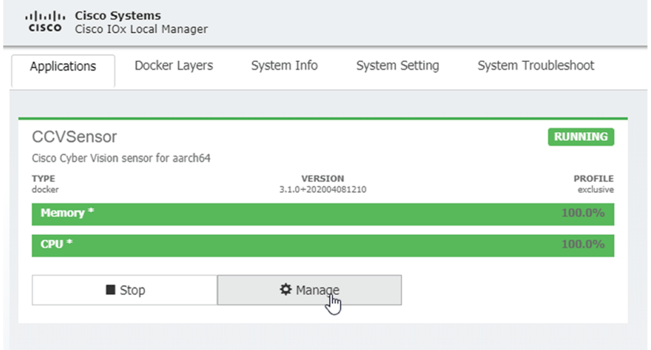


□	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
□	[illegible]			[illegible]	[illegible]	[illegible]		[illegible]
□	[illegible]			[illegible]				[illegible]
□	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days

Import the provisioning package

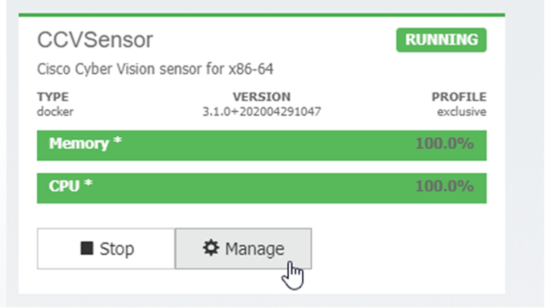
1. In the Local manager, in the IOx configuration menu, click **Manage**.

   Cisco IE3400:



CCVSensor
Cisco Cyber Vision sensor for aarch64
TYPE docker
VERSION 3.1.0+202004081210
PROFILE exclusive
Memory * 100.0%
CPU * 100.0%

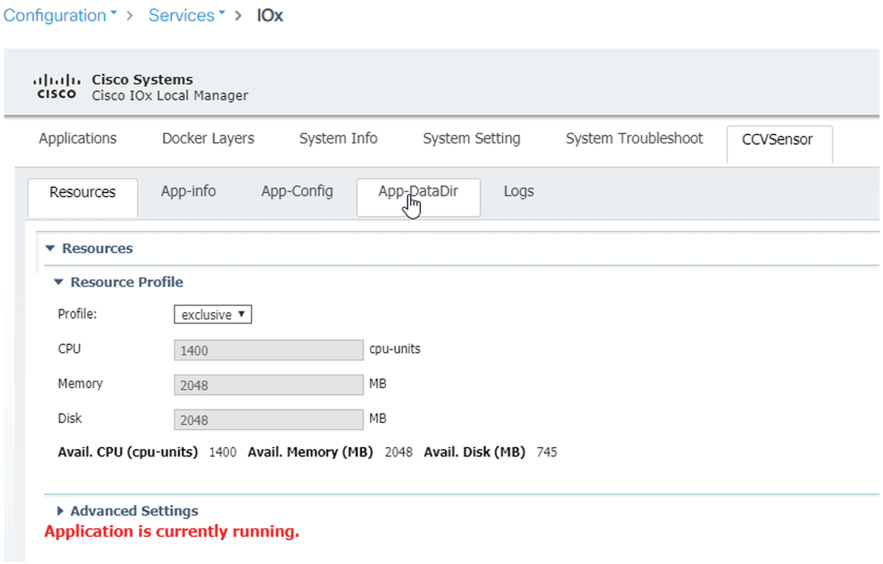
   Cisco Catalyst 9300:



CCVSensor
Cisco Cyber Vision sensor for x86-64
TYPE docker
VERSION 3.1.0+202004291047
PROFILE exclusive
Memory * 100.0%
CPU * 100.0%

2. Navigate to **App_DataDir**.

   For example Cisco IE3400:



Profile: exclusive

CPU 1400 cpu-units

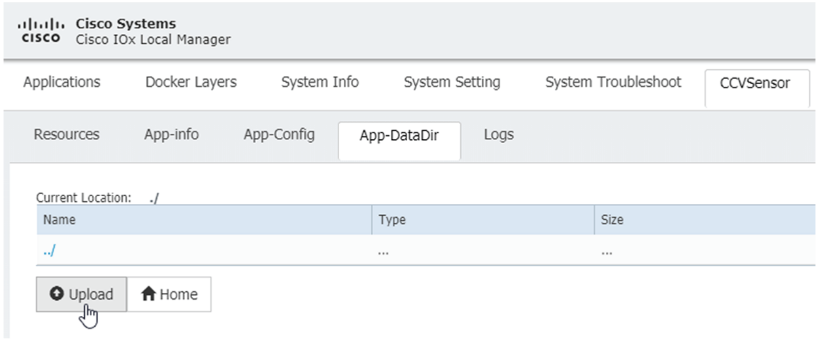
Memory 2048 MB

Disk 2048 MB

Avail. CPU (cpu-units) 1400 Avail. Memory (MB) 2048 Avail. Disk (MB) 745

Application is currently running.

3. Click **Upload**.

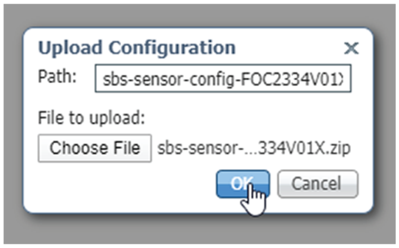


Current Location: ./

Name	Type	Size
../	...	...

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**.



Path: sbs-sensor-config-FOC2334V01)

File to upload: sbs-sensor-...334V01X.zip

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

6. Click **OK**.

CHAPTER 9

Procedure with the CLI

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

Configure the sensor application

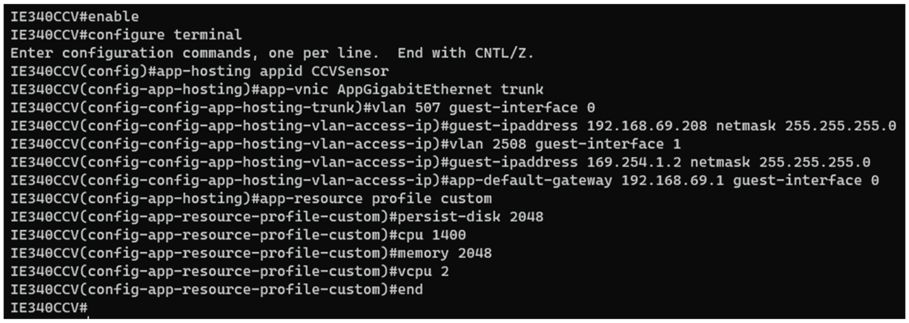
Note In this section, "CCVSensor" is used as the appid.

1. Connect to the device through SSH or a console.

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

   Cisco IE3300 10G/IE3400:

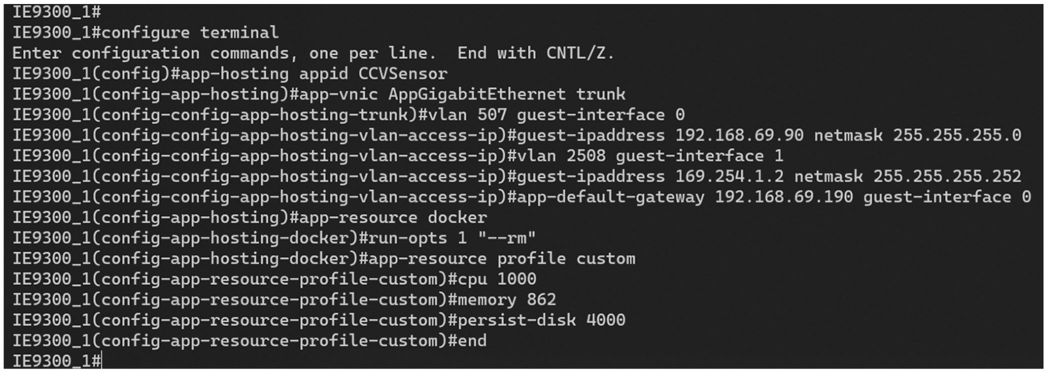
   ```
   enable
   configure terminal
   app-hosting appid CCVSensor
   app-vnic AppGigabitEthernet trunk
   vlan 507 guest-interface 0
   guest-ipaddress 192.168.69.208 netmask 255.255.255.0
   vlan 2508 guest-interface 1
   guest-ipaddress 169.254.1.2 netmask 255.255.255.0
   app-default-gateway 192.168.69.1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



```
IE340CCV#enable
IE340CCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE340CCV(config)#app-hosting appid CCVSensor
IE340CCV(config-app-hosting)#app-vnic AppGigabitEthernet trunk
IE340CCV(config-config-app-hosting-trunk)#vlan 507 guest-interface 0
IE340CCV(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 192.168.69.208 netmask 255.255.255.0
IE340CCV(config-config-app-hosting-vlan-access-ip)#vlan 2508 guest-interface 1
IE340CCV(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 169.254.1.2 netmask 255.255.255.0
IE340CCV(config-config-app-hosting-vlan-access-ip)#app-default-gateway 192.168.69.1 guest-interface 0
IE340CCV(config-app-hosting)#app-resource profile custom
IE340CCV(config-app-resource-profile-custom)#persist-disk 2048
IE340CCV(config-app-resource-profile-custom)#cpu 1400
IE340CCV(config-app-resource-profile-custom)#memory 2048
IE340CCV(config-app-resource-profile-custom)#vcpu 2
IE340CCV(config-app-resource-profile-custom)#end
IE340CCV#
```

Cisco IE9300:

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

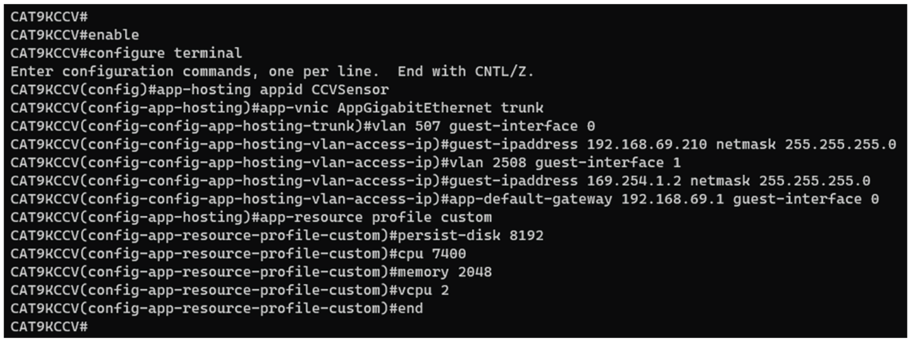


```
IE9300_1#
IE9300_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IE9300_1(config)#app-hosting appid CCVSensor
IE9300_1(config-app-hosting)#app-vnic AppGigabitEthernet trunk
IE9300_1(config-config-app-hosting-trunk)#vlan 507 guest-interface 0
IE9300_1(config-config-app-hosting-vlan-access-ip)#guest-ipaddress 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
vlan 507 guest-interface 0
guest-ipaddress 192.168.69.210 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 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

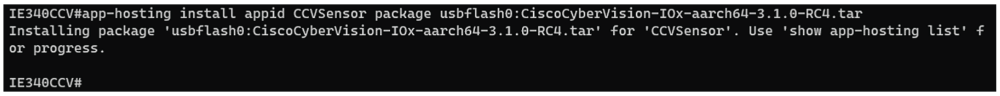
The sensor package is to be retrieved on cisco.com. The file has the following name structure:

- 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
   ```

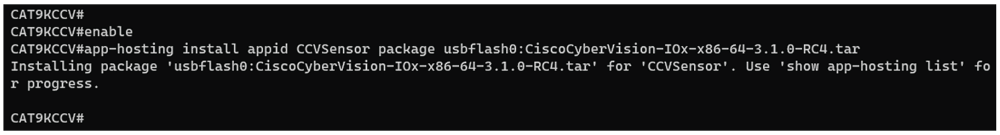
   Cisco IE3300 10G/IE3400/IE9300:

   ```
   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#
   ```

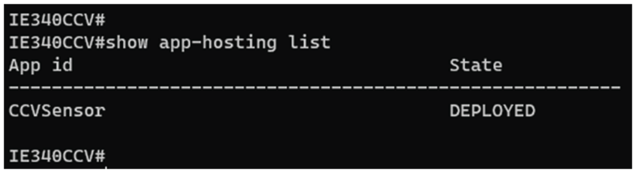
Note Adjust "usbflash0:" in accordance with the sensor package's localization (USB port or flash memory).

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



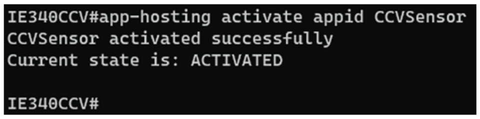
```
IE340CCV#
IE340CCV#show app-hosting list
App id                                   State
---------------------------------------------------------
CCVSensor                                DEPLOYED

IE340CCV#
```

4. Activate the application using the following command:

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

   For example: Cisco IE3400



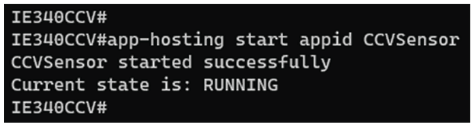
```
IE340CCV#app-hosting activate appid CCVSensor
CCVSensor activated successfully
Current state is: ACTIVATED

IE340CCV#
```

5. Start the application using the following command:

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

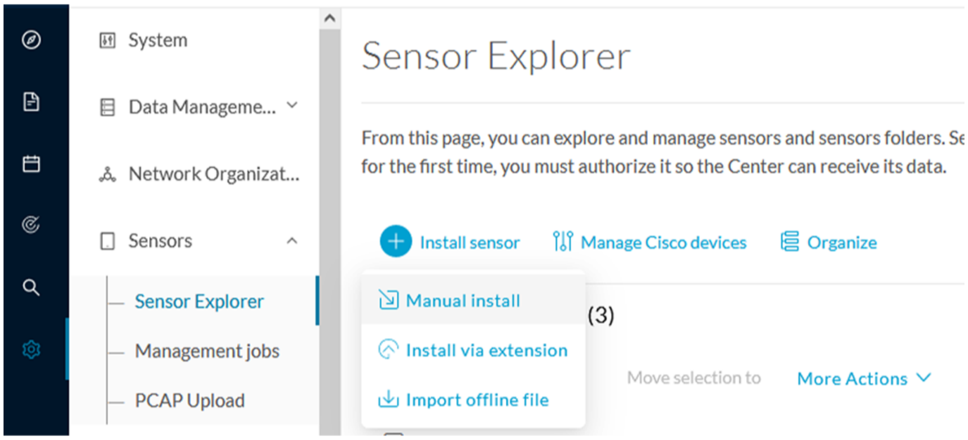
   For example: Cisco IE3400:



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

Generate the provisioning package

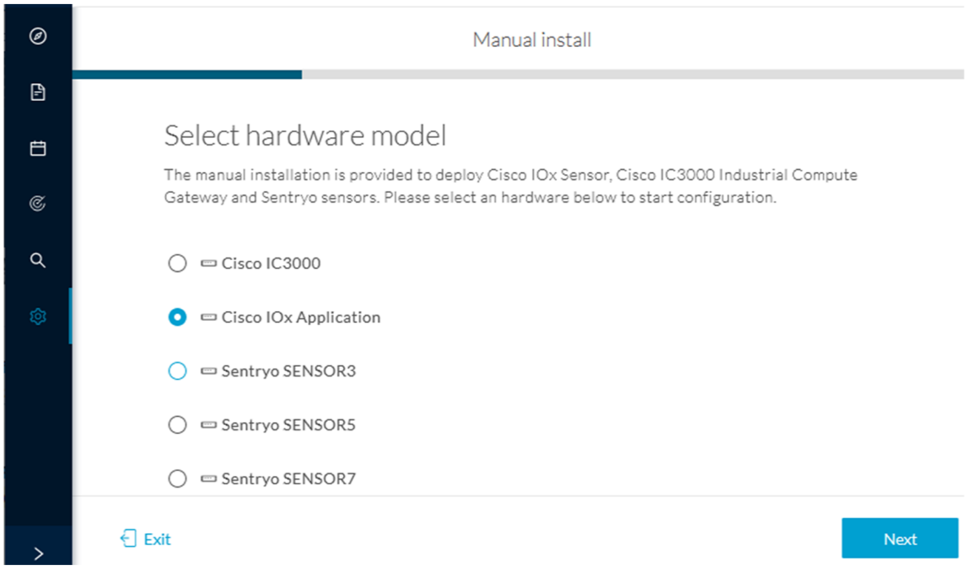
1. In Cisco Cyber Vision, navigate to Admin > Sensors > Sensor Explorer and click **Install sensor**, then **Manual install**.



From this page, you can explore and manage sensors and sensors folders. Se
for the first time, you must authorize it so the Center can receive its data.

The manual install wizard appears.

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



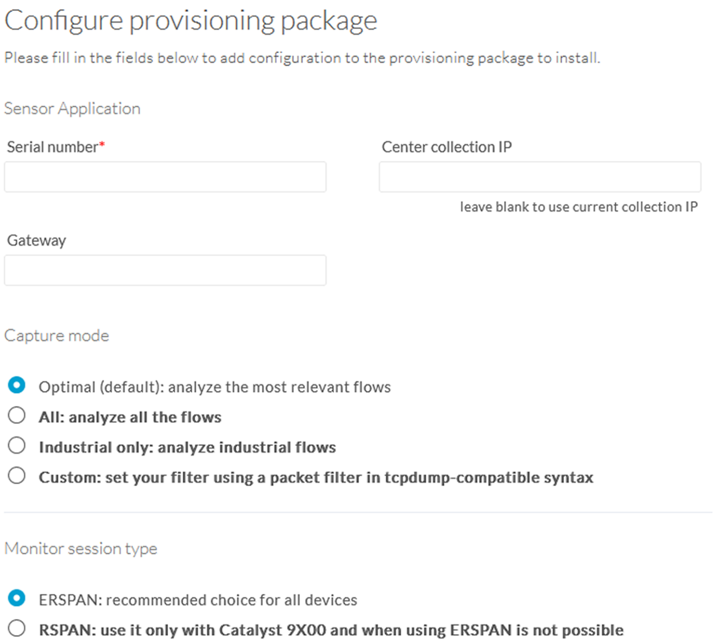
Select hardware model

The manual installation is provided to deploy Cisco IOx Sensor, Cisco IC3000 Industrial Compute Gateway and Sentryo sensors. Please select an hardware below to start configuration.

○ Cisco IC3000
● Cisco IOx Application
○ Sentryo SENSOR3
○ Sentryo SENSOR5
○ Sentryo SENSOR7

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

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



Configure provisioning package

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

Sensor Application

Serial number*

Center collection IP

leave blank to use current collection IP

Gateway

Capture mode

● Optimal (default): analyze the most relevant flows

○ All: analyze all the flows

○ Industrial only: analyze industrial flows

○ Custom: set your filter using a packet filter in tcpdump-compatible syntax

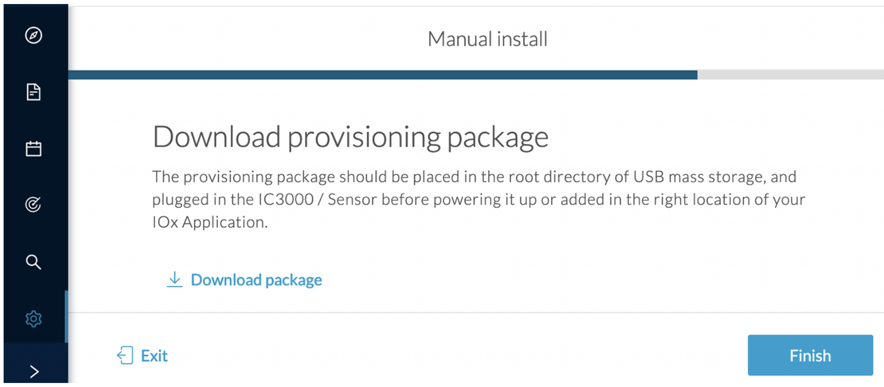
Monitor session type

● ERSPAN: recommended choice for all devices

○ RSPAN: use it only with Catalyst 9X00 and when using ERSPAN is not possible

4. Click **Create sensor**.

5. Click the link to download the provisioning package.



Manual install

Download provisioning package

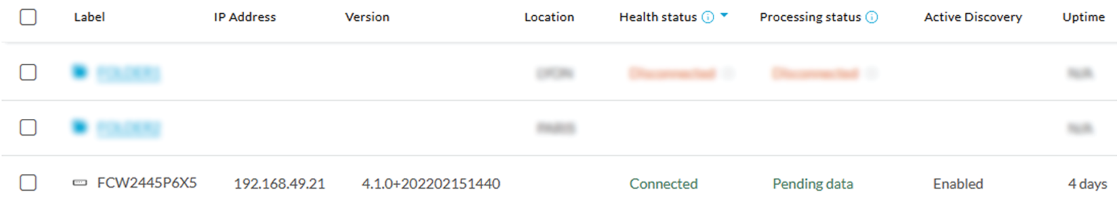
The provisioning package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up or added in the right location of your IOx Application.

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

6. Click **Finish**.

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

The sensor status will switch from Disconnected to Connected.



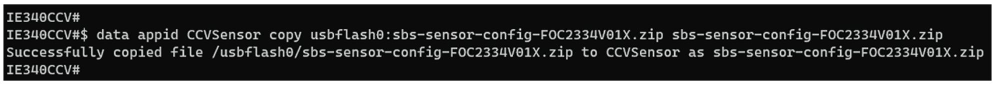
□	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery	Uptime
□	[redacted]			[redacted]	[redacted]	[redacted]		[redacted]
□	[redacted]			[redacted]				[redacted]
□	FCW2445P6X5	192.168.49.21	4.1.0+202202151440		Connected	Pending data	Enabled	4 days

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#
```

Final step

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

```
write mem
```

CHAPTER 10

Upgrade procedures

Upgrade through the Cisco Cyber Vision sensor management extension

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

It is possible to select which sensors to update. The update status will be visible in the Management jobs, on page 24 page.

Update the sensor management extension

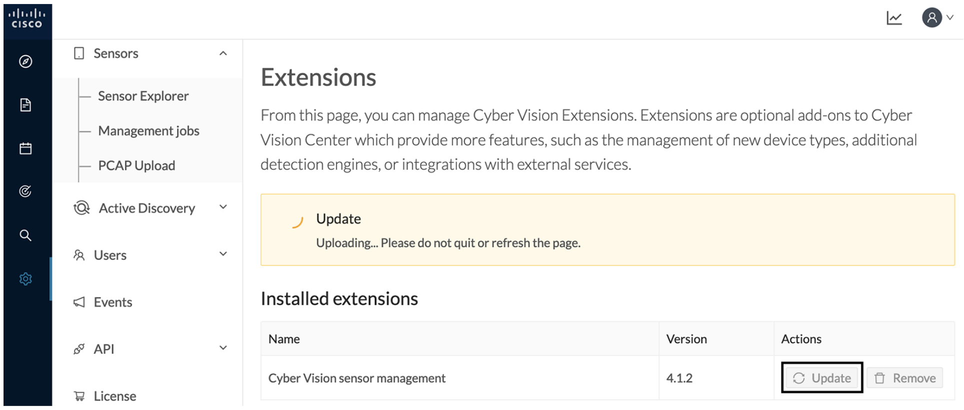
The Cisco Cyber Vision sensor management extension must be up-to-date to update IOx sensors.

Procedure

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

Step 2 In Cisco Cyber Vision, navigate to Admin > Extensions.

Step 3 Click **Update** to browse the new version of the extension file.



Extensions

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

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

Installed extensions

Name	Version	Actions
Cyber Vision sensor management	4.1.2	Update Remove

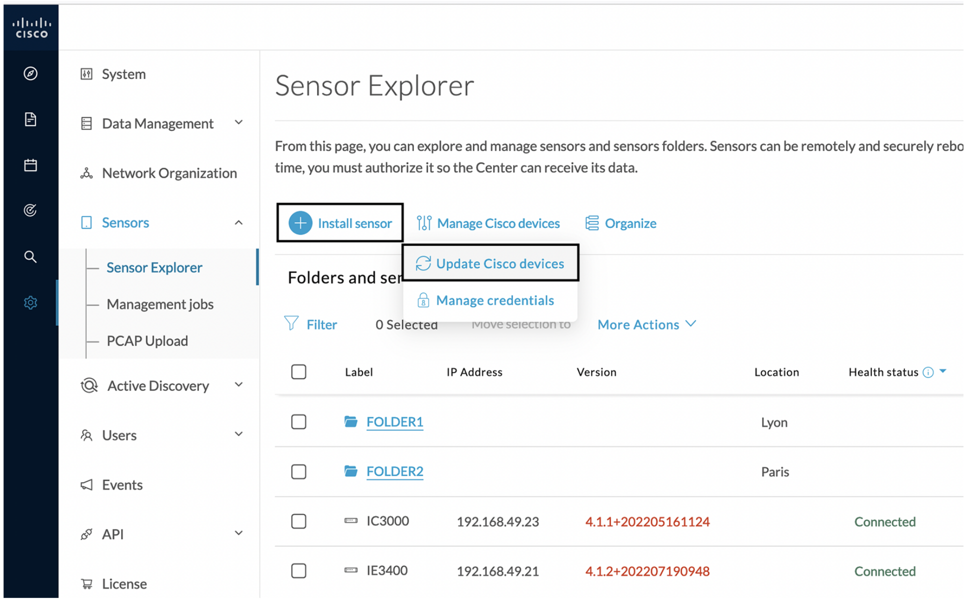
Update the sensors

Procedure

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

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

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



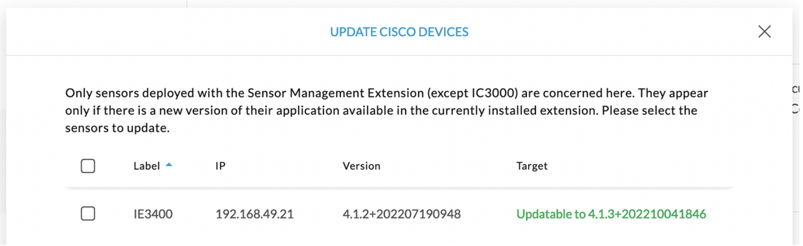
Sensor Explorer

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

Folders and ser

Label	IP Address	Version	Location	Health status
FOLDER1			Lyon	
FOLDER2			Paris	
IC3000	192.168.49.23	4.1.1+202205161124		Connected
IE3400	192.168.49.21	4.1.2+202207190948		Connected

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

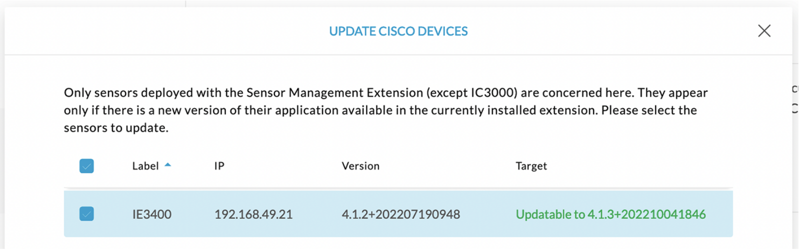


UPDATE CISCO DEVICES

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

□	Label	IP	Version	Target
□	IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846

Step 3 Select the sensors you want to update.



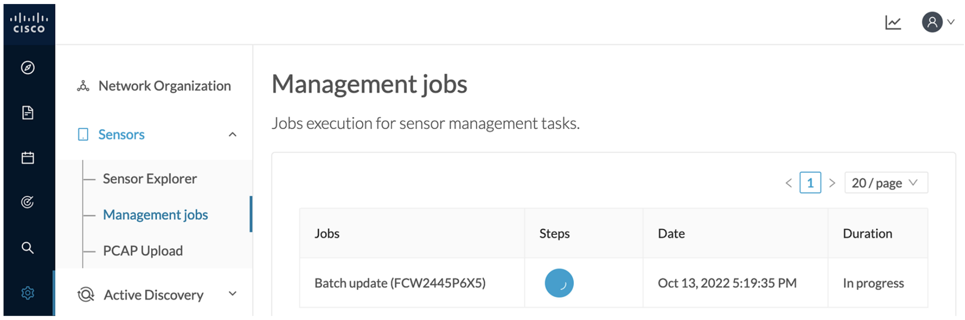
UPDATE CISCO DEVICES

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

☑	Label	IP	Version	Target
☑	IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846

Step 4 Click **Update**.

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

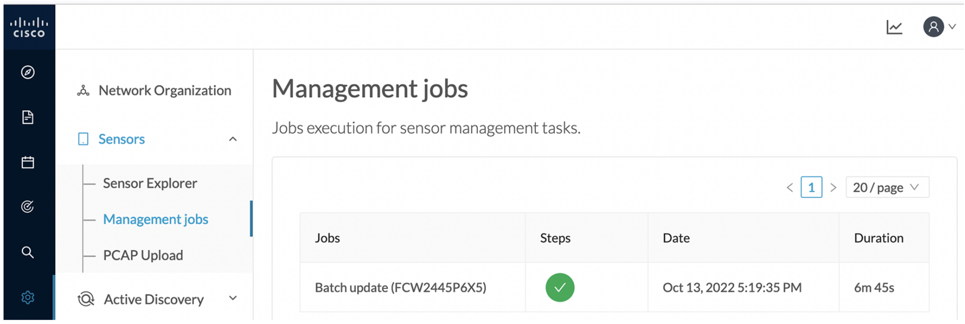


Management jobs

Jobs execution for sensor management tasks.

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

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

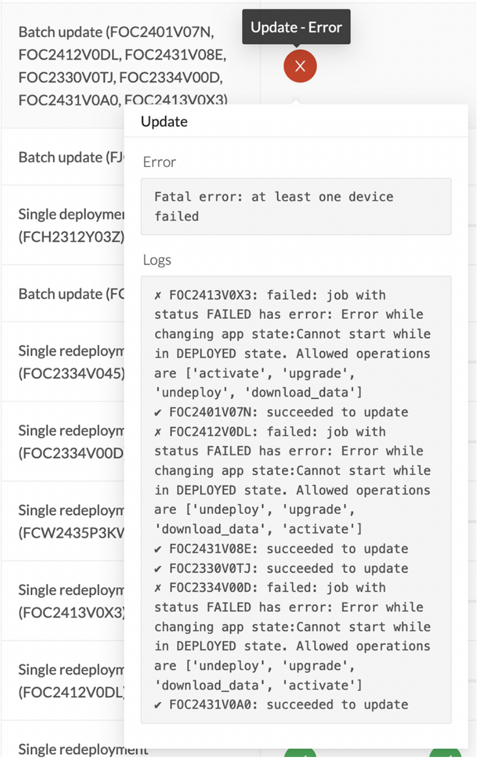


Management jobs

Jobs execution for sensor management tasks.

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

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



Batch update (FOC2401V07N, FOC2412V0DL, FOC2431V08E, FOC2330V0TJ, FOC2334V00D, FOC2431V0A0, FOC2413V0X3)

Update

Error

```
Fatal error: at least one device
failed
```

Logs

```
✗ FOC2413V0X3: failed: job with
status FAILED has error: Error while
changing app state:Cannot start while
in DEPLOYED state. Allowed operations
are ['activate', 'upgrade',
'undeploy', 'download_data']
✔ FOC2401V07N: succeeded to update
✗ FOC2412V0DL: failed: job with
status FAILED has error: Error while
changing app state:Cannot start while
in DEPLOYED state. Allowed operations
are ['undeploy', 'upgrade',
'download_data', 'activate']
✔ FOC2431V08E: succeeded to update
✔ FOC2330V0TJ: succeeded to update
✗ FOC2334V00D: failed: job with
status FAILED has error: Error while
changing app state:Cannot start while
in DEPLOYED state. Allowed operations
are ['undeploy', 'upgrade',
'download_data', 'activate']
✔ FOC2431V0A0: succeeded to update
```

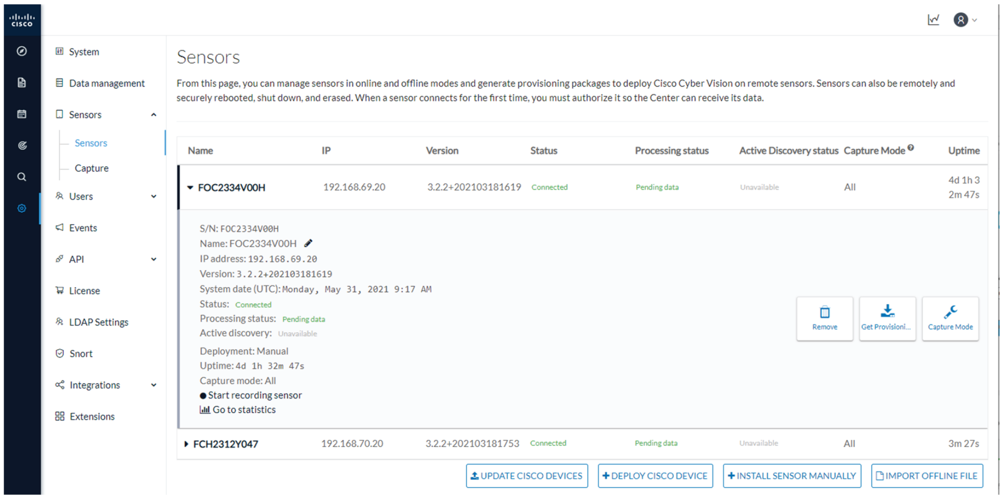
Upgrade through the IOx Local Manager

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

Note In the case of Cisco Cyber Vision upgrade for a Catalyst 9x00 from a release 4.1.2 or lower to a release 4.1.3, the update will fail due to the addition of the RSPAN option. The sensor application must be removed and deployed again.

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



Sensors

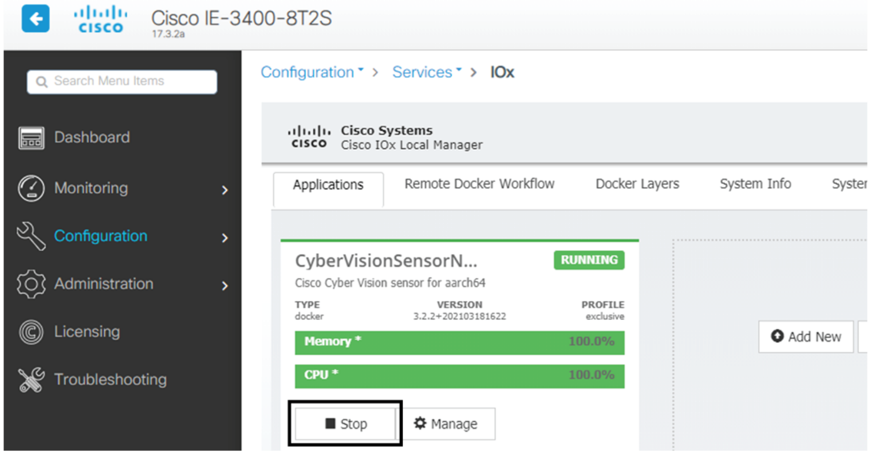
From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.2+202103181619	Connected	Pending data	Unavailable	All	4d 1h 32m 47s
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	3m 27s

S/N: FOC2334V00H
Name: FOC2334V00H
IP address: 192.168.69.20
Version: 3.2.2+202103181619
System date (UTC): Monday, May 31, 2021 9:17 AM
Status: Connected
Processing status: Pending data
Active discovery: Unavailable
Deployment: Manual
Uptime: 4d 1h 32m 47s
Capture mode: All
● Start recording sensor
Go to statistics

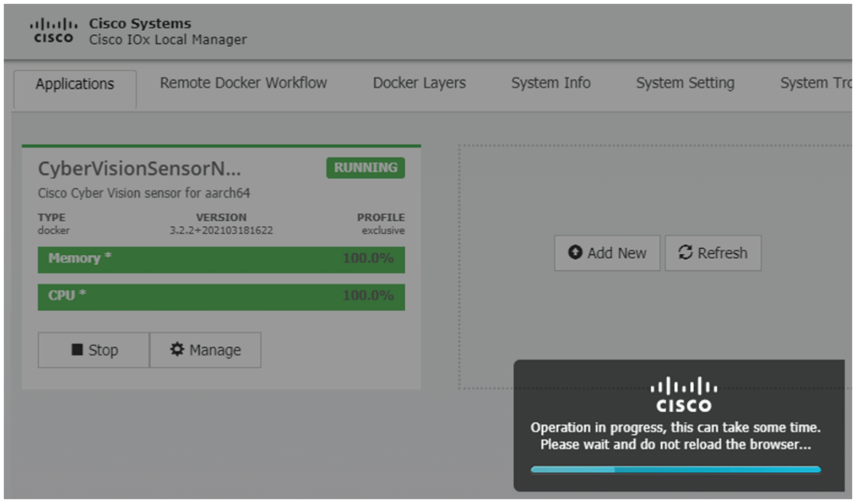
1. Access the IOx Local Manager.

2. Stop the application.



CyberVisionSensorN... RUNNING
Cisco Cyber Vision sensor for aarch64
TYPE docker
VERSION 3.2.2+202103181622
PROFILE exclusive
Memory * 100.0%
CPU * 100.0%

The operation takes a few moments.



CyberVisionSensorN... RUNNING
Cisco Cyber Vision sensor for aarch64

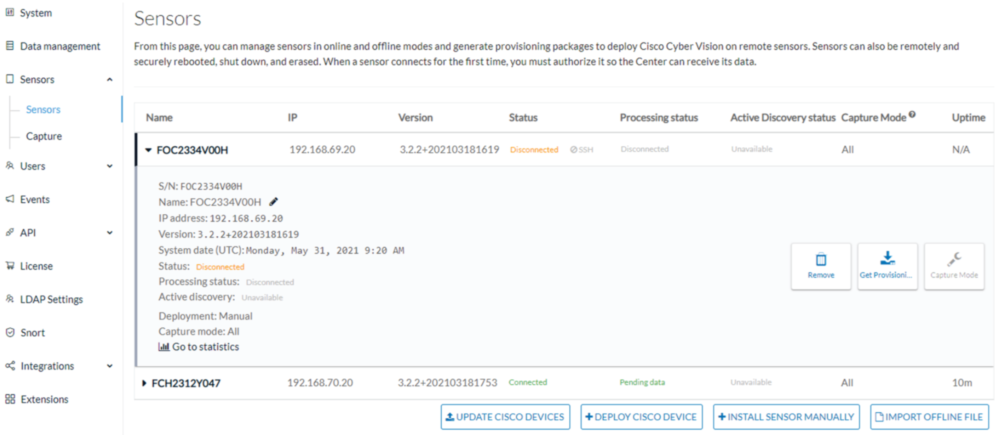
TYPE	VERSION	PROFILE
docker	3.2.2+202103181622	exclusive

Memory * 100.0%
CPU * 100.0%

Operation in progress, this can take some time.
Please wait and do not reload the browser...

The application status switches to STOPPED.

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



Sensors

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

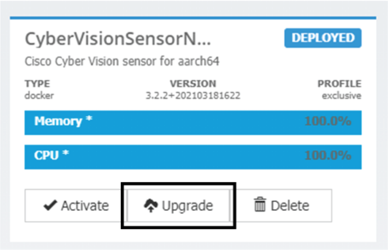
Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.2+202103181619	Disconnected ⊘SSH	Disconnected	Unavailable	All	N/A
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	10m

S/N: FOC2334V00H
Name: FOC2334V00H
IP address: 192.168.69.20
Version: 3.2.2+202103181619
System date (UTC): Monday, May 31, 2021 9:20 AM
Status: Disconnected
Processing status: Disconnected
Active discovery: Unavailable
Deployment: Manual
Capture mode: All
Go to statistics

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

   The application status moves to DEPLOYED.

4. Click **Upgrade**.

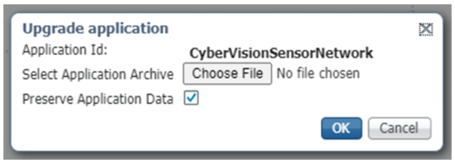


CyberVisionSensorN... DEPLOYED
Cisco Cyber Vision sensor for aarch64

TYPE	VERSION	PROFILE
docker	3.2.2+202103181622	exclusive

Memory * 100.0%
CPU * 100.0%

The pop up Upgrade application appears.



Upgrade application

Application Id: CyberVisionSensorNetwork

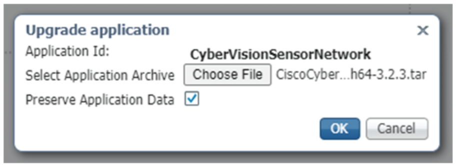
Select Application Archive Choose File No file chosen

Preserve Application Data ☑

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

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

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



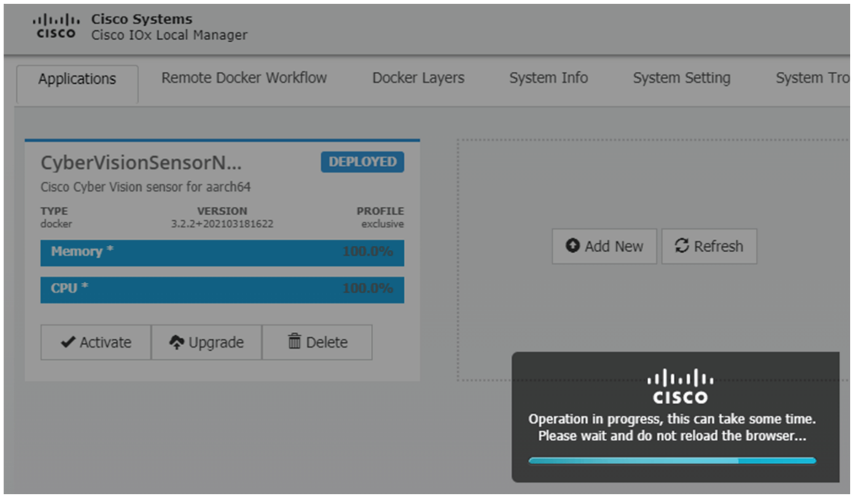
Upgrade application

Application Id: CyberVisionSensorNetwork

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

Preserve Application Data ☑

The operation takes a few moments.



CyberVisionSensorN... DEPLOYED

Cisco Cyber Vision sensor for aarch64

TYPE docker

VERSION 3.2.2+202103181622

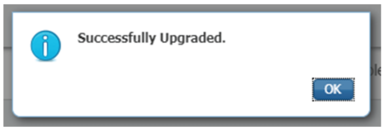
PROFILE exclusive

Memory * 100.0%

CPU * 100.0%

Operation in progress, this can take some time. Please wait and do not reload the browser...

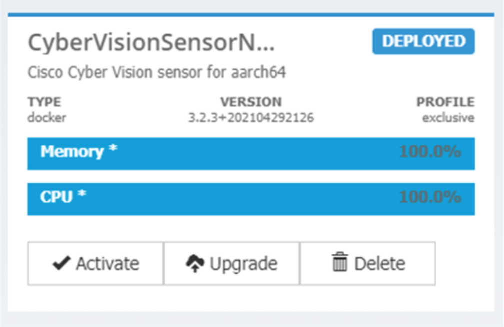
A message indicating that the sensor has been successfully upgraded is displayed.



Successfully Upgraded.

7. Check the number of the new version.

8. Click **Activate**.



CyberVisionSensorN... DEPLOYED

Cisco Cyber Vision sensor for aarch64

TYPE	VERSION	PROFILE
docker	3.2.3+202104292126	exclusive

Memory * 100.0%

CPU * 100.0%

9. Check configurations.

   It can happen that network configurations are lost during the upgrade. If they are, refer to Configure the sensor virtual application in the Procedure with the Local Manager **corresponding to the switch used and do as explained.**

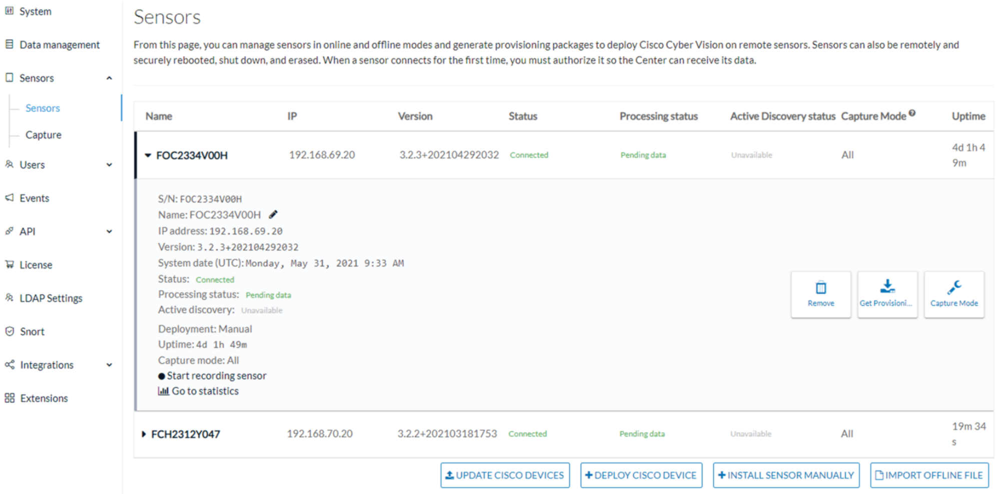
10. Click the **Activate App** button.

    The application status moves to ACTIVATED.

11. Click the **Start** button.

    The application status changes to RUNNING.

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

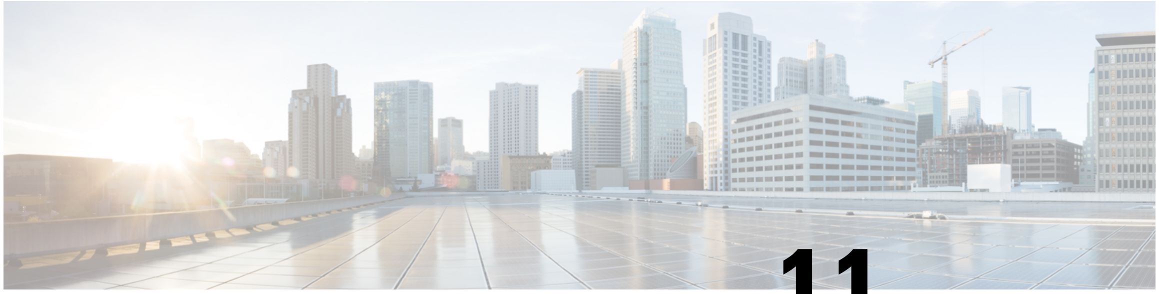


Sensors

From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

Name	IP	Version	Status	Processing status	Active Discovery status	Capture Mode	Uptime
FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data	Unavailable	All	4d 1h 49m
FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	19m 34 s

S/N: FOC2334V00H
Name: FOC2334V00H
IP address: 192.168.69.20
Version: 3.2.3+202104292032
System date (UTC): Monday, May 31, 2021 9:33 AM
Status: Connected
Processing status: Pending data
Active discovery: Unavailable
Deployment: Manual
Uptime: 4d 1h 49m
Capture mode: All
● Start recording sensor
Go to statistics



CHAPTER 11

Reconfigure/Redeploy a sensor

Reconfigure/Redeploy a sensor

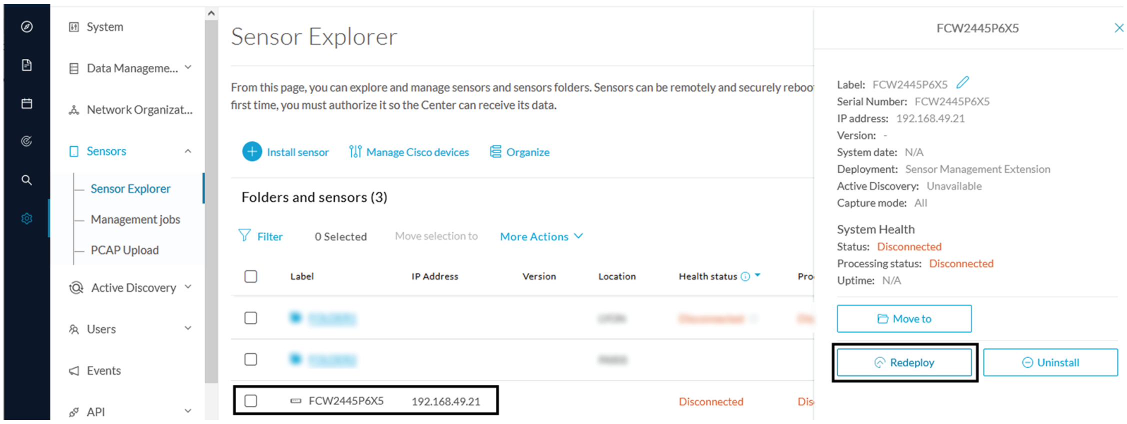
The Redeploy button is used when you need to replace a sensor model with another one keeping the same network configurations (e.g. replacing a Cisco IE3400 with a Cat 9300), change configurations, or if you need to reconfigure the sensor (e.g. to enable Active Discovery).

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**.



Sensor Explorer

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

Folders and sensors (3)

0 Selected

	Label	IP Address	Version	Location	Health status	Pro
□						
□						
□	FCW2445P6X5	192.168.49.21			Disconnected	Dis

FCW2445P6X5

Label: FCW2445P6X5
Serial Number: FCW2445P6X5
IP address: 192.168.49.21
Version: -
System date: N/A
Deployment: Sensor Management Extension
Active Discovery: Unavailable
Capture mode: All

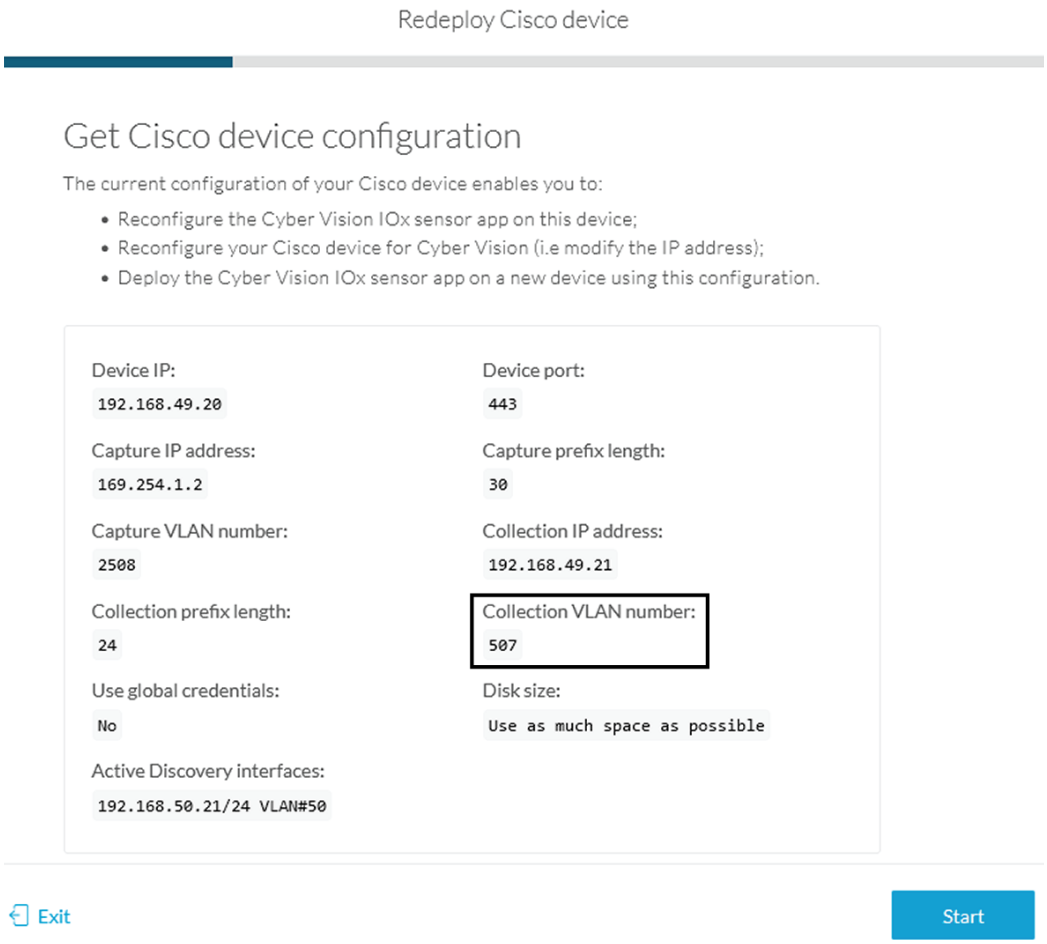
System Health
Status: Disconnected
Processing status: Disconnected
Uptime: N/A

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**.



Redeploy Cisco device

Get Cisco device configuration

The current configuration of your Cisco device enables you to:

- Reconfigure the Cyber Vision IOx sensor app on this device;
- Reconfigure your Cisco device for Cyber Vision (i.e modify the IP address);
- Deploy the Cyber Vision IOx sensor app on a new device using this configuration.

Device IP: 192.168.49.20

Device port: 443

Capture IP address: 169.254.1.2

Capture prefix length: 30

Capture VLAN number: 2508

Collection IP address: 192.168.49.21

Collection prefix length: 24

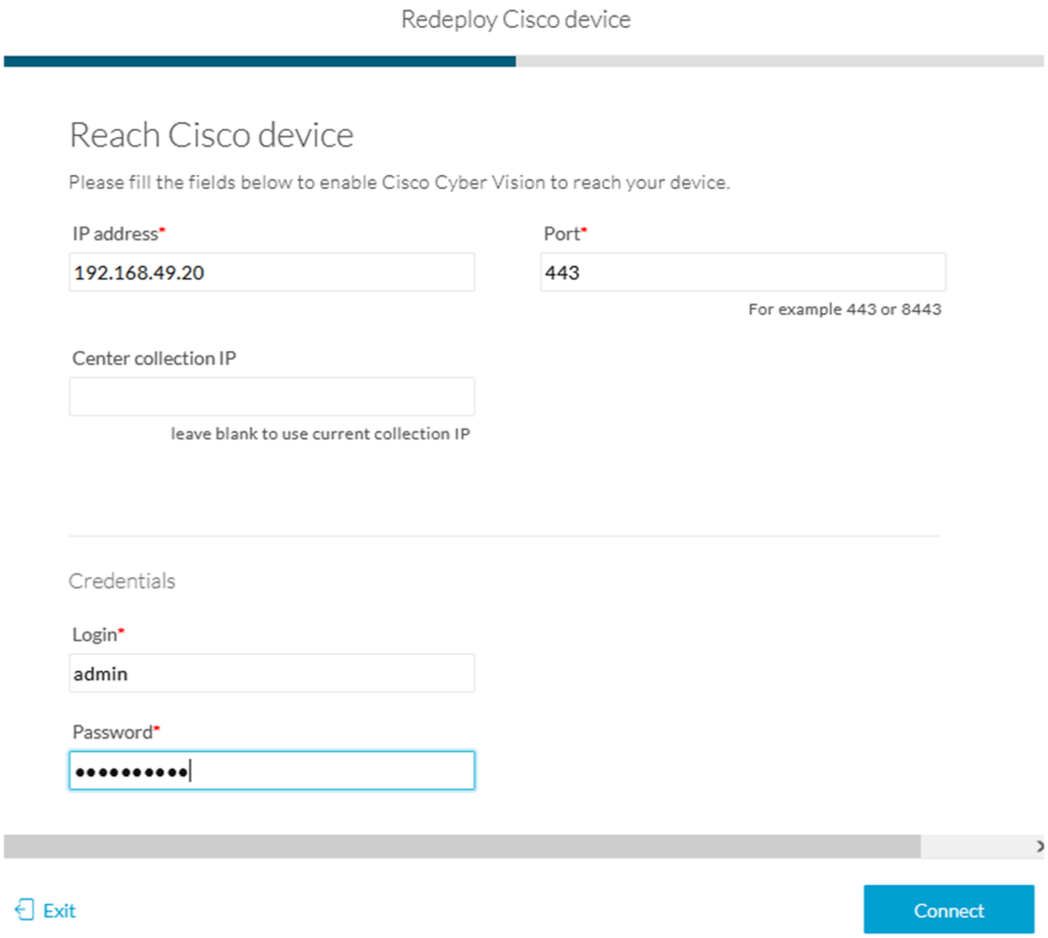
Collection VLAN number: 507

Use global credentials: No

Disk size: Use as much space as possible

Active Discovery interfaces: 192.168.50.21/24 VLAN#50

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



Redeploy Cisco device

Reach Cisco device

Please fill the fields below to enable Cisco Cyber Vision to reach your device.

IP address*: 192.168.49.20

Port*: 443

For example 443 or 8443

Center collection IP:

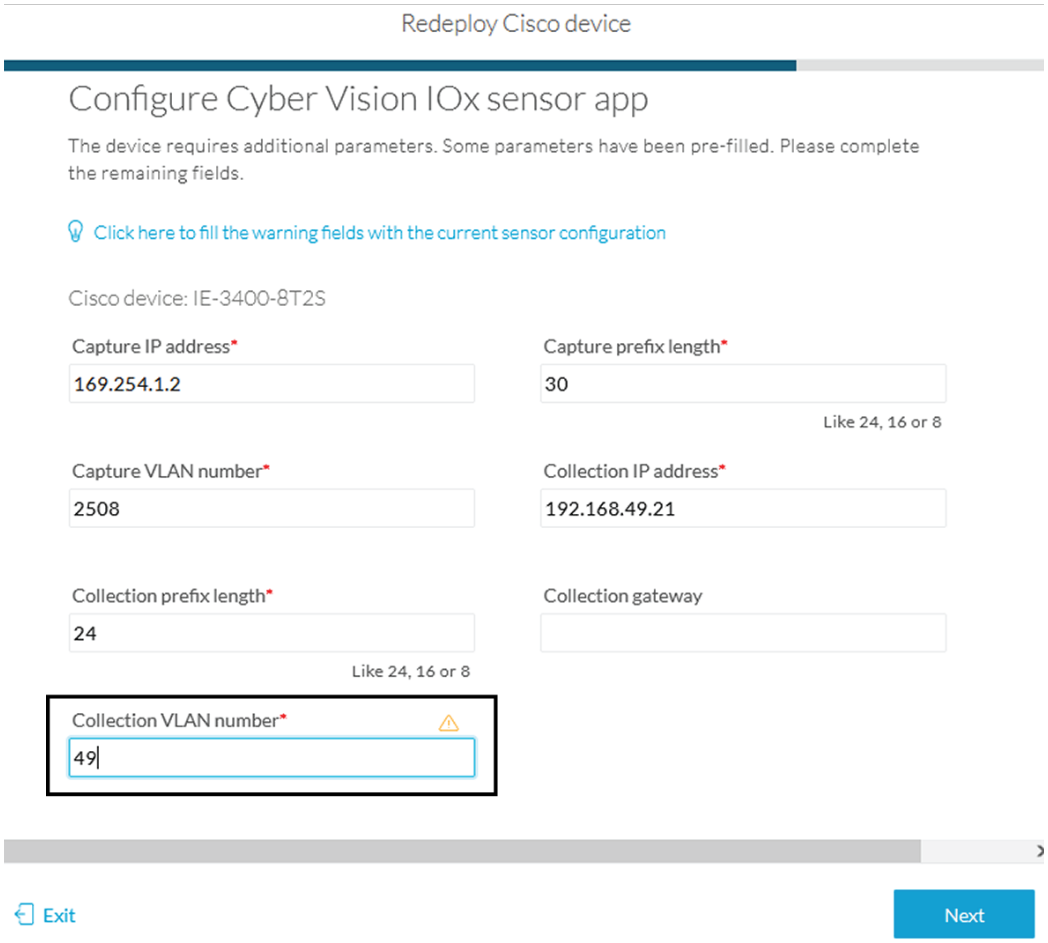
leave blank to use current collection IP

Credentials

Login*: admin

Password*: ●●●●●●●●●●

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.



Redeploy Cisco device

Configure Cyber Vision IOx sensor app

The device requires additional parameters. Some parameters have been pre-filled. Please complete the remaining fields.

Click here to fill the warning fields with the current sensor configuration

Cisco device: IE-3400-8T2S

Capture IP address*: 169.254.1.2

Capture prefix length*: 30 (Like 24, 16 or 8)

Capture VLAN number*: 2508

Collection IP address*: 192.168.49.21

Collection prefix length*: 24 (Like 24, 16 or 8)

Collection gateway:

Collection VLAN number*: 49

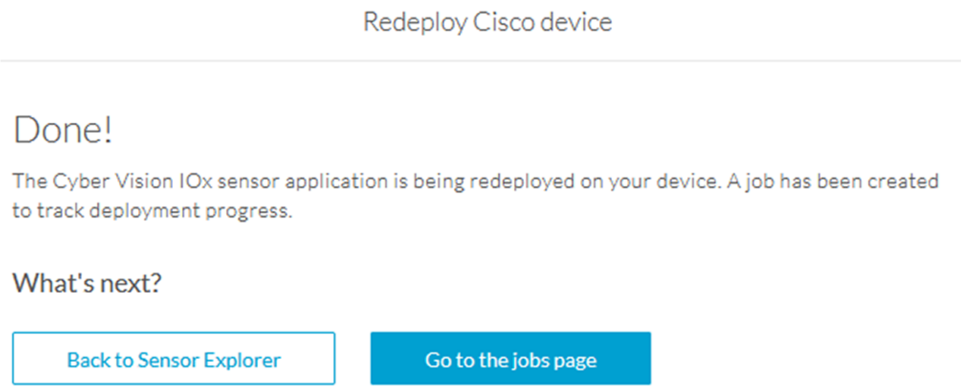
Step 7 Click **Next**.

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**.



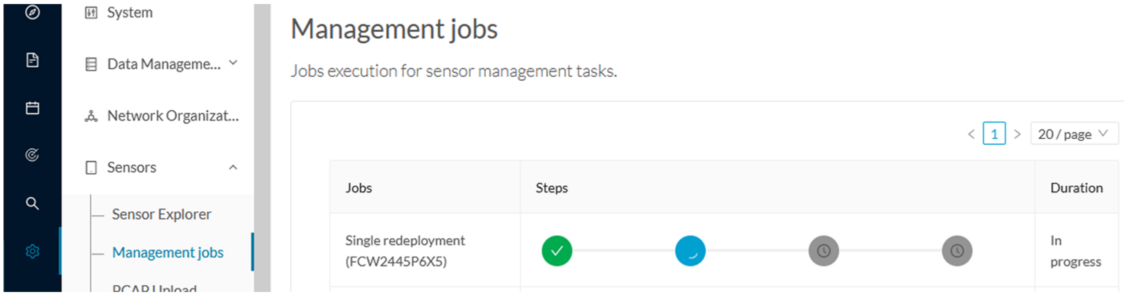
Redeploy Cisco device

Done!

The Cyber Vision IOx sensor application is being redeployed on your device. A job has been created to track deployment progress.

What's next?

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

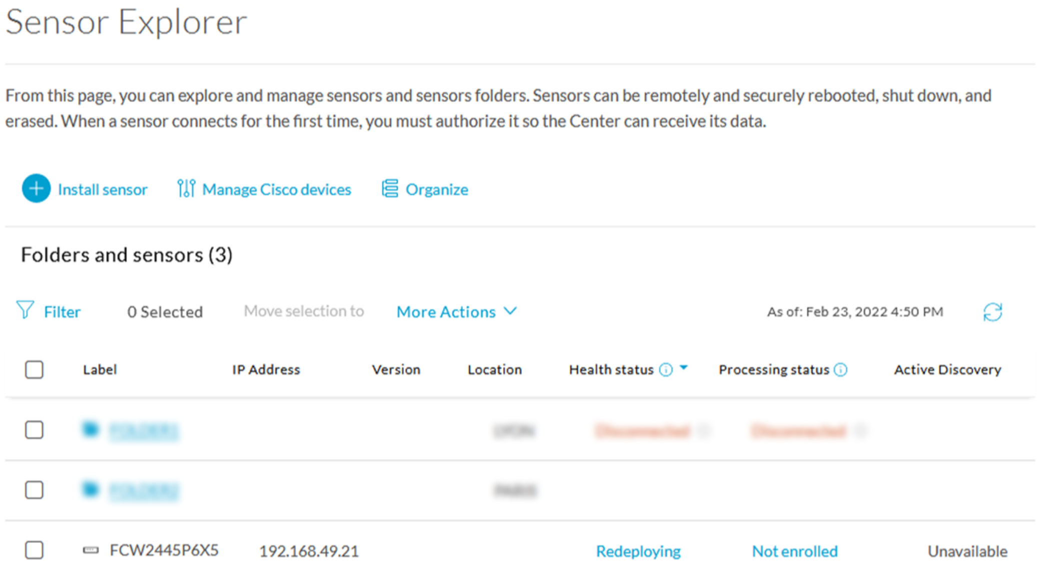


Management jobs

Jobs execution for sensor management tasks.

Jobs	Steps	Duration
Single redeployment (FCW2445P6X5)	✓ ● ● ●	In progress

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



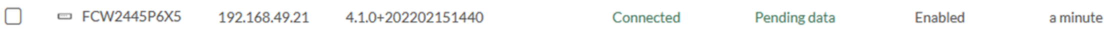
Sensor Explorer

From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data.

Folders and sensors (3)

□	Label	IP Address	Version	Location	Health status	Processing status	Active Discovery
□	[redacted]			[redacted]	[redacted]	[redacted]	
□	[redacted]			[redacted]			
□	FCW2445P6X5	192.168.49.21			Redeploying	Not enrolled	Unavailable

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



□	FCW2445P6X5	192.168.49.21	4.1.0+202202151440	Connected	Pending data	Enabled	a minute