Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300

Rev. 0.1.1, 11 December 2020

Cisco Systems, Inc.

Total pages: 47

Cisco Cyber Vision Network Sensor Installation Guide for Cisco IE3300 10G, Cisco IE3400 and Cisco Catalyst 9300

Rev. 0.1.1, 11 December 2020

Owner: **Cisco IoT**

Author: **Juliette Maffet**

Cisco Systems, Inc.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents

1 About this documentation

1.1 Document purpose

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

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst 9300 Series Switch.

This documentation is applicable to **system version 3.2.0**.

1.2 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.

2 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:

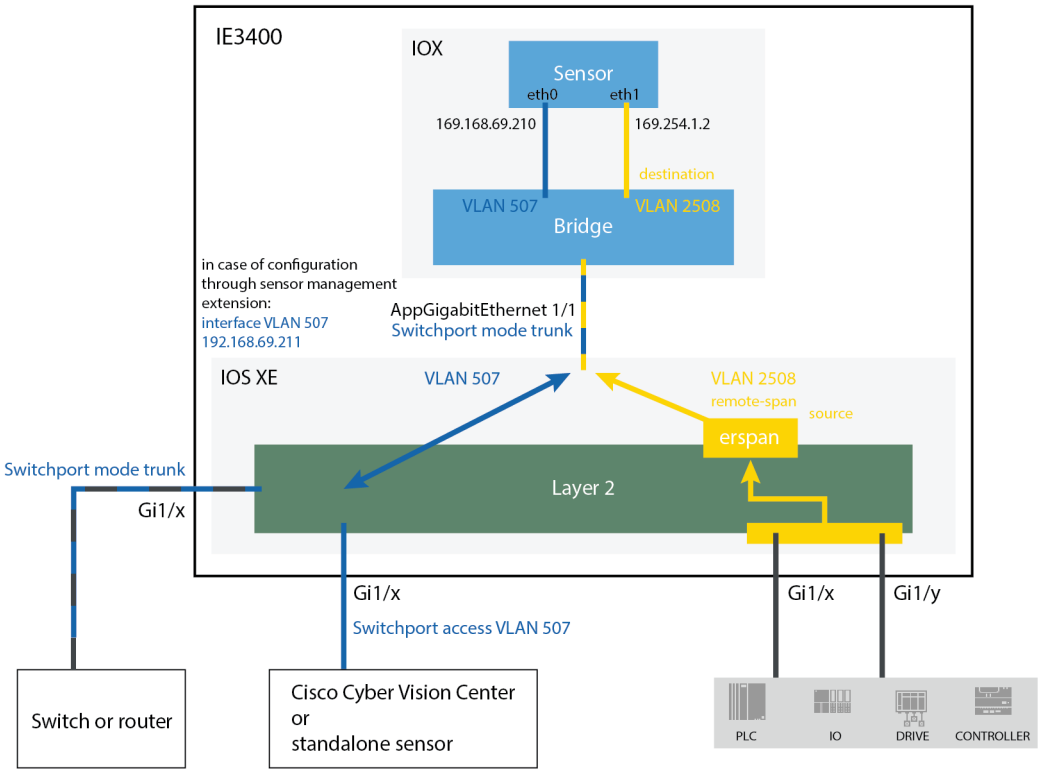
- one with a direct connection to the Center (link="switchport access vlan 507").
- the other with a trunk to another switch or router which is connected to the Center (link="switch mode trunk").

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:

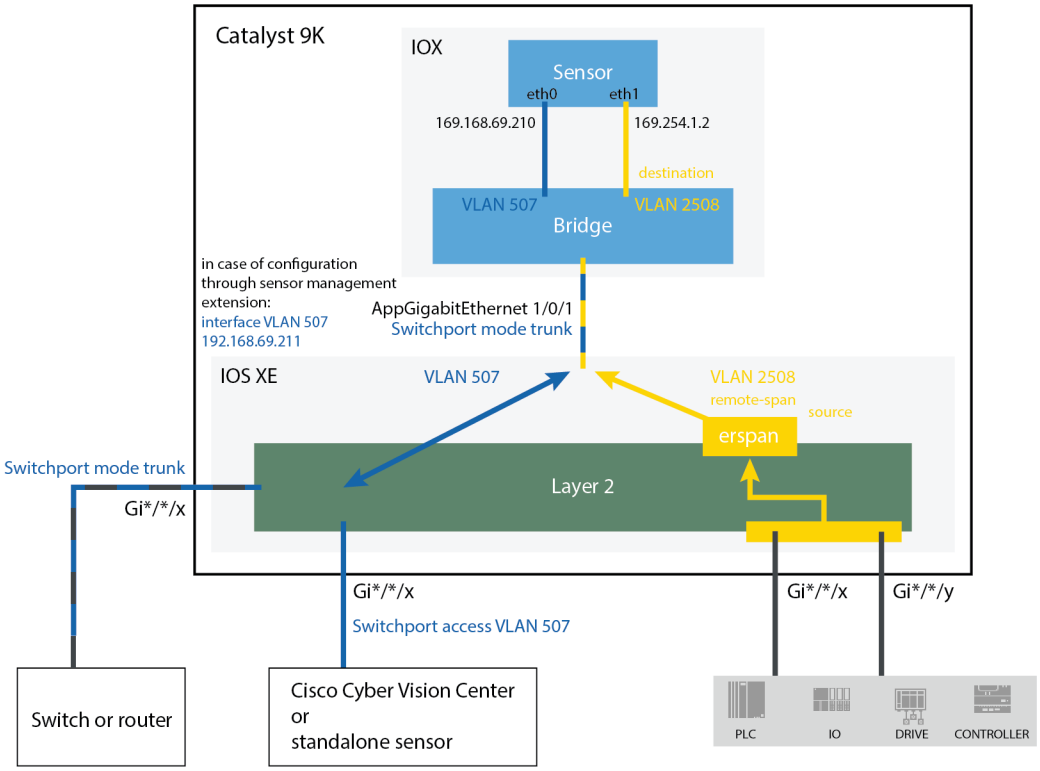
- having the Center on the same subnet than the switch's Local Manager (IP added on VLAN 507).
- having a route path to the Local Manager subnet.

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

Cisco Catalyst IE3300 10G & IE3400 Rugged Series Switch:



Cisco Catalyst 9300 Series switch:



3 Requirements

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

Elements to collect

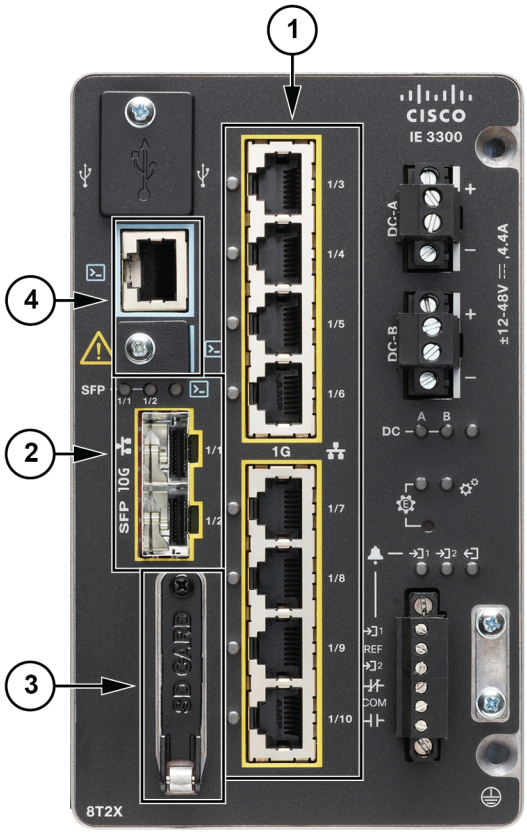
- The Cisco Cyber Vision Sensor application to collect from Cisco.com, i.e. CiscoCyberVision-sensor-IOx-aarch64-3.1.0.tar.
- A console cable, for the connection to the hardware's console port.

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

4 Hardware front view

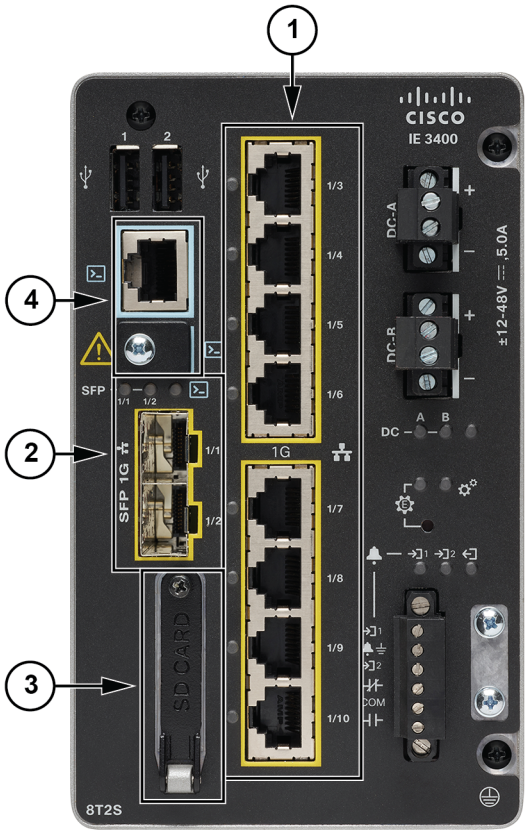
Before starting, take a moment to note and/or unscrew the following parts you're going to use during the procedure.

Cisco Catalyst IE3300 10G Rugged Series Switch:



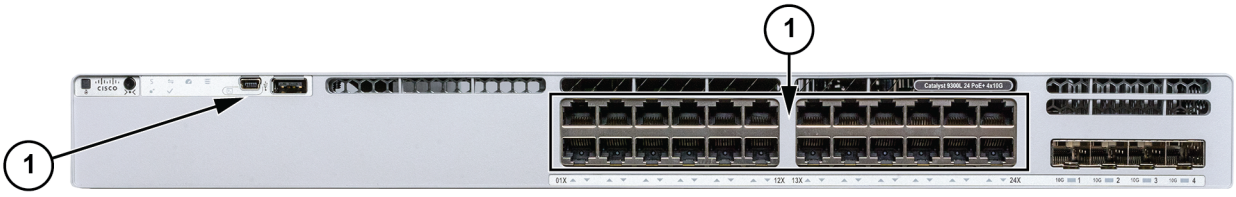
- 8x RJ45 10/100/1000 BaseT connector **(1)**
- 2x SFP 10G fiber port **(2)**
- SD CARD **(3)**
- Console connectors **(4)** RJ-45 and mini-USB

Cisco Catalyst IE3400 Rugged Series Switch:



- 8x RJ45 10/100/1000 BaseT connector **(1)**
- 2x SFP 1G fiber port **(2)**
- SD CARD **(3)**
- Console connectors **(4)** RJ-45 and mini-USB

Cisco Catalyst 9300 Series switch:



- x24 RJ45 10/100/1000 BaseT connector **(1)**
- mini-USB console connector **(2)**

5 Initial configuration

5.1 Check the Hardware version

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

```
Show version
```

The displayed version must be 17.02.01 or higher to be compatible with the CCV Sensor Application.

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
```

Cisco Catalyst 9300:

```
CAT9KCCV#show version
Cisco IOS XE Software, Version 17.02.01
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), 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 03:29 by mcpre
```

5.2 SD Card (IE3300/IE3400)

If not already done, insert a 4 GB ext4 formatted Cisco SD Card in the 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 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
```

5.3 SSD Disk (Catalyst 9300)

If not already done, insert a 12 GB ext4 formatted 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#
```

5.4 Check date and time

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

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

```
Show clock
```

Cisco IE3400:

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

Cisco Catalyst 9300:

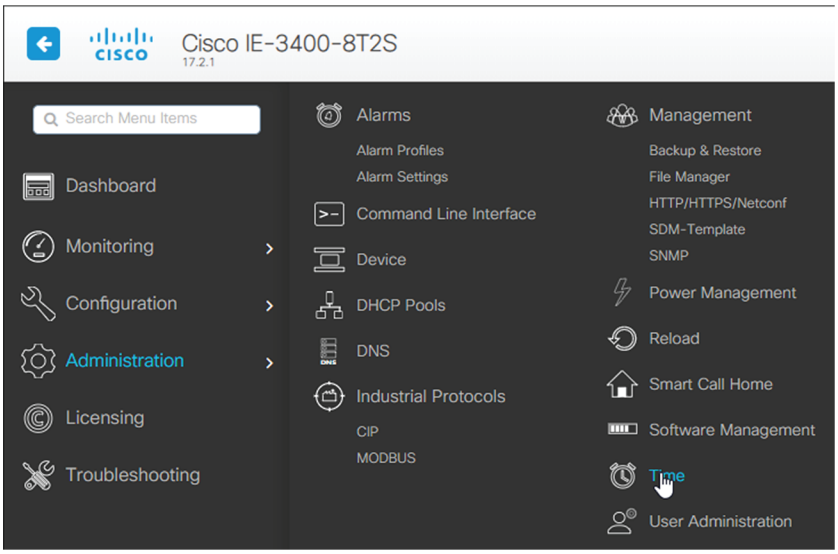
```
CAT9KCCV#
CAT9KCCV#show clock
*16:02:57.900 UTC Thu Apr 30 2020
CAT9KCCV#
```

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

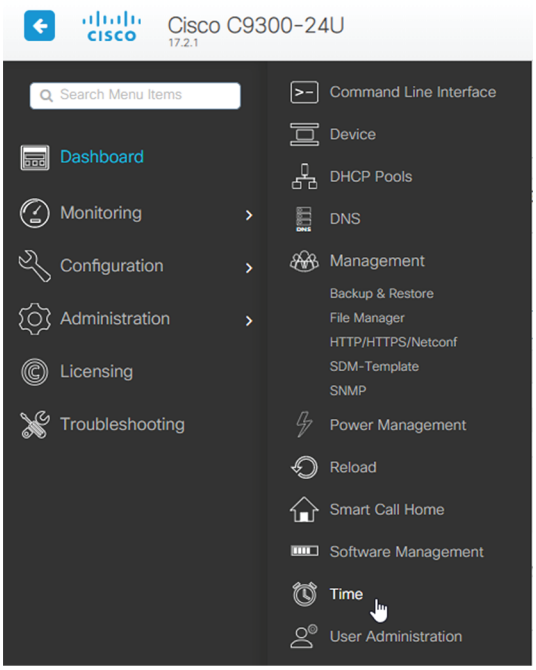
```
clock set [hh:mm:ss] [month] [day] [year]
```

Or go to the Local Manager:

Cisco IE3400:



Cisco Catalyst 9300:



5.5 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
```

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
```

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#
```

5.6 Add the necessary configuration parameters (IE3300/IE3400)

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
```

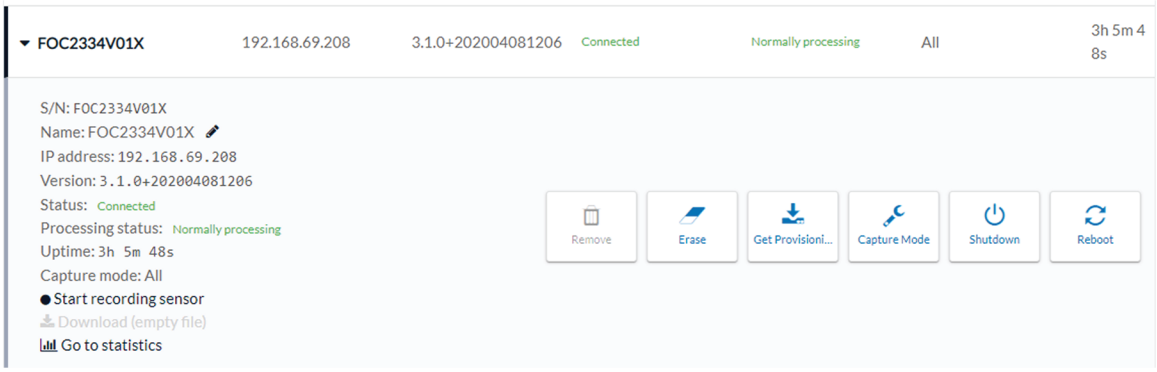
```
IE340CCV(config)#
IE340CCV(config)#int gi1/3
IE340CCV(config-if)#switchport access vlan 507
% Access VLAN does not exist. Creating vlan 507
IE340CCV(config-if)#no shutdown
IE340CCV(config-if)#exit
```

6. Save the configuration using the following commands:

```
exit
write mem
```

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

After a few minutes, the sensor will appear as connected in Cisco Cyber Vision.



5.7 Add the necessary configuration parameters (Catalyst 9300)

1. Open the Cisco Catalyst 9300 CLI through ssh or via the console terminal.
2. Configure a vlan for traffic mirroring using the following commands:

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

```
CAT9KCCV#
CAT9KCCV#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT9KCCV(config)#vlan 2508
CAT9KCCV(config-vlan)#exit
CAT9KCCV(config)#int vlan 2508
CAT9KCCV(config-if)#ip address 169.254.1.1 255.255.255.252
CAT9KCCV(config-if)#no shutdow
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

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)#
```

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

```
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)#
```

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
```

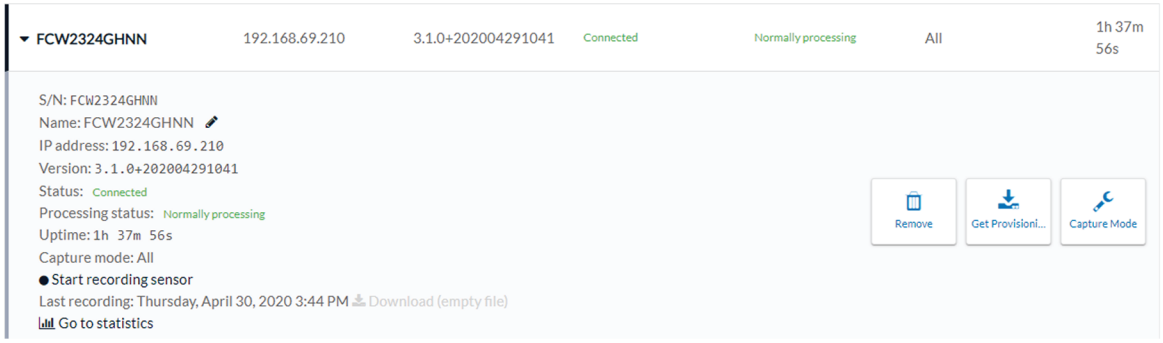
```
CAT9KCCV(config)#interface GigabitEthernet1/0/1
CAT9KCCV(config-if)#switchport access vlan 507
% Access VLAN does not exist. Creating vlan 507
CAT9KCCV(config-if)#no shutdown
CAT9KCCV(config-if)#exit
CAT9KCCV(config)#
```

6. Save the configuration:

```
exit
write mem
```

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

After a few minutes, the sensor will appear as connected in Cisco Cyber Vision.



6 Procedure with the Cyber Vision sensor management extension

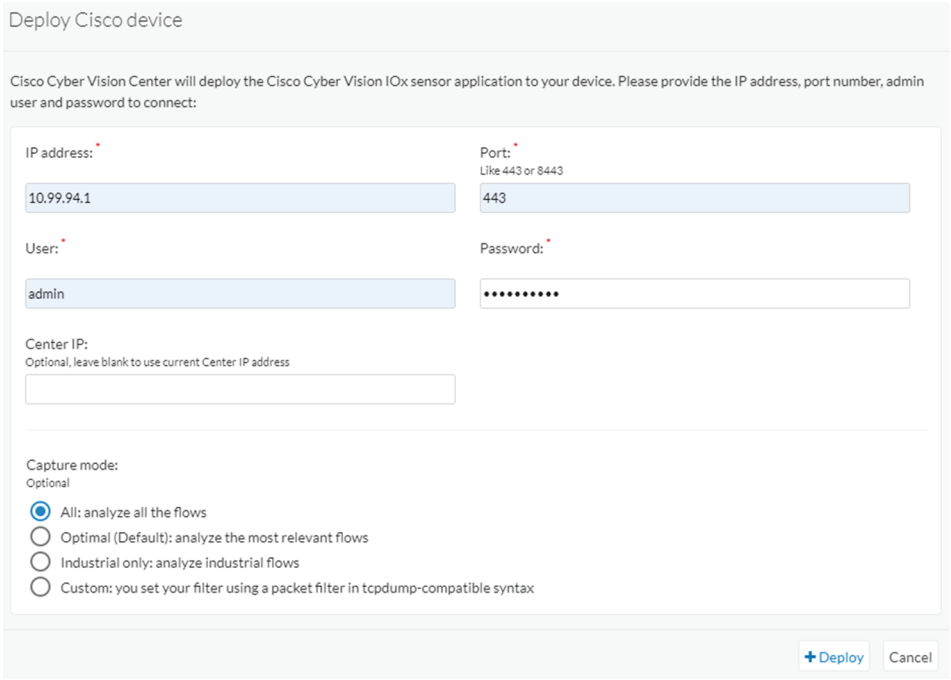
After the Initial configuration (page 11), proceed to the steps described in this section. This section also described the steps to configure Active Discovery on the Cisco IE3300 10G and Cisco IE3400.

> **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.

6.1 IOx APP sensor creation

1. In Cisco Cyber Vision, navigate to Admin > Sensors > Management and click DEPLOY IOX APP.

2. Fill the requested fields so Cisco Cyber Vision can reach the equipment:
   - IP Address: admin address of the equipment
   - Port: management port (443)
   - User: user with the admin rights of the equipment
   - Password: password of the admin user
   - Capture Mode: Optionally, select a capture mode.

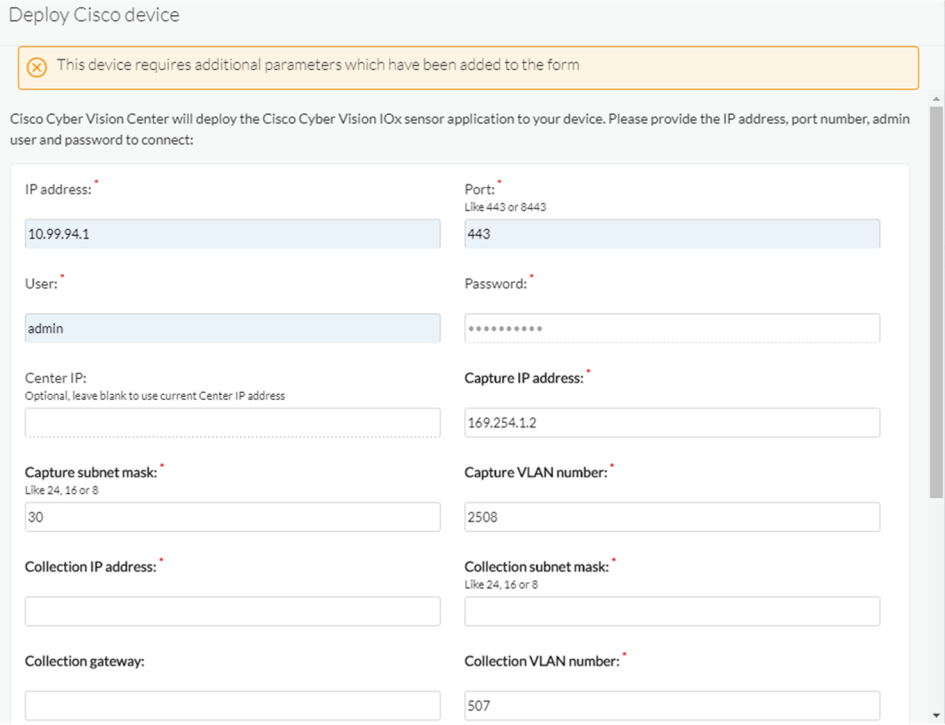


3. Click the Deploy button.

The Center will join the equipment and display the second parameter list. For this step to succeed, the equipment needs to be reachable by the Center on its eth1 connection.

6.2 IOx APP sensor configuration

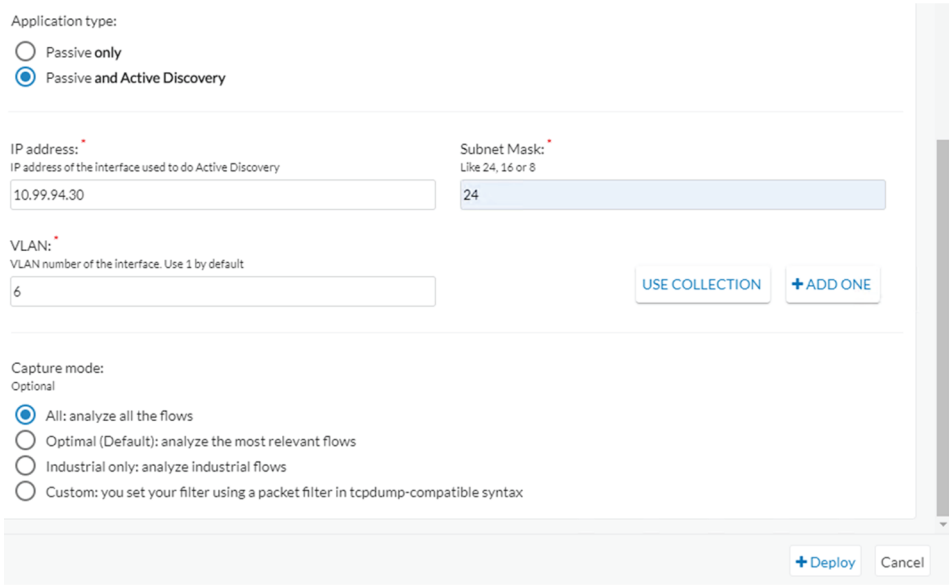
If the Center can join the equipment, the following window appears:



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

1. Fill the following parameters for the Collection interface:
    - Capture IP address: IP address destination of the monitor session in the sensor
    - Capture subnet mask: 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 sensor
    - Collection subnet mask: mask of the Collection IP address
    - Collection gateway: gateway of the Collection IP address
    - Collection VLAN number: VLAN of the sensor
2. **Active Discovery (only available for Cisco IE3300 10G and Cisco IE3400):**
   If you want to enable Active Discovery on the sensor, select Passive and Active Discovery. You must then fill the following parameters to set a dedicated network interface:

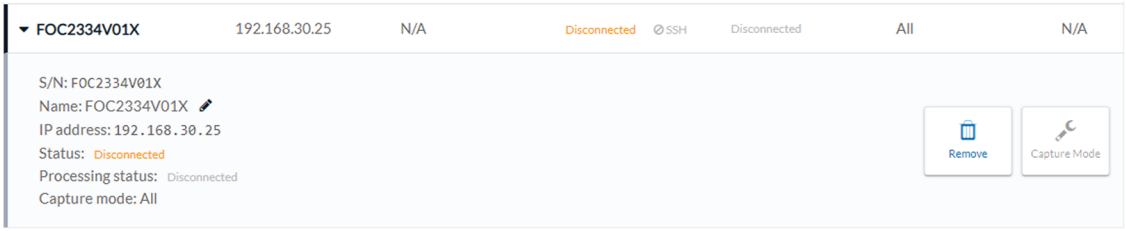
- IP address
- Subnet Mask
- VLAN



1. Click the Deploy button.

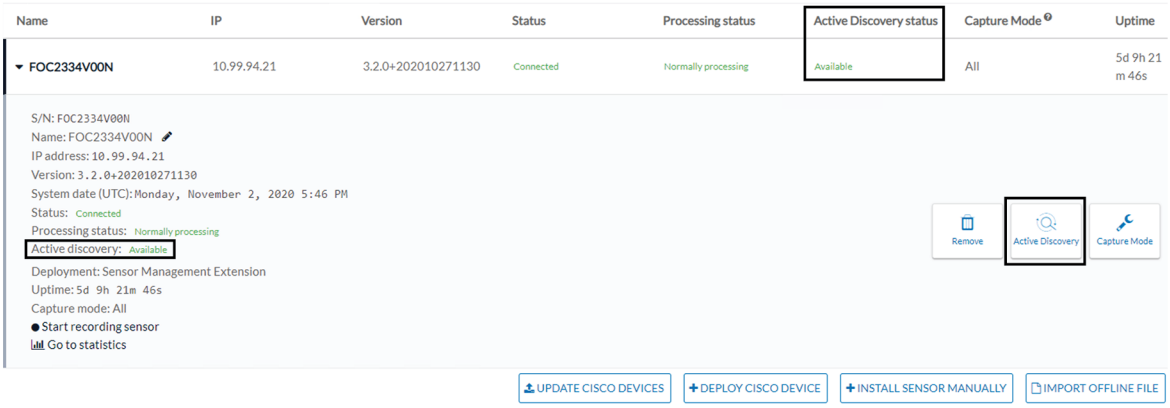
   The Center starts deploying the sensor application on the target equipment. This can take a few minutes.

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



The sensor's status will eventually turn to connected.

If the Active Discovery has been enabled and set, the sensor is displayed as below with Active Discovery's status as Available.

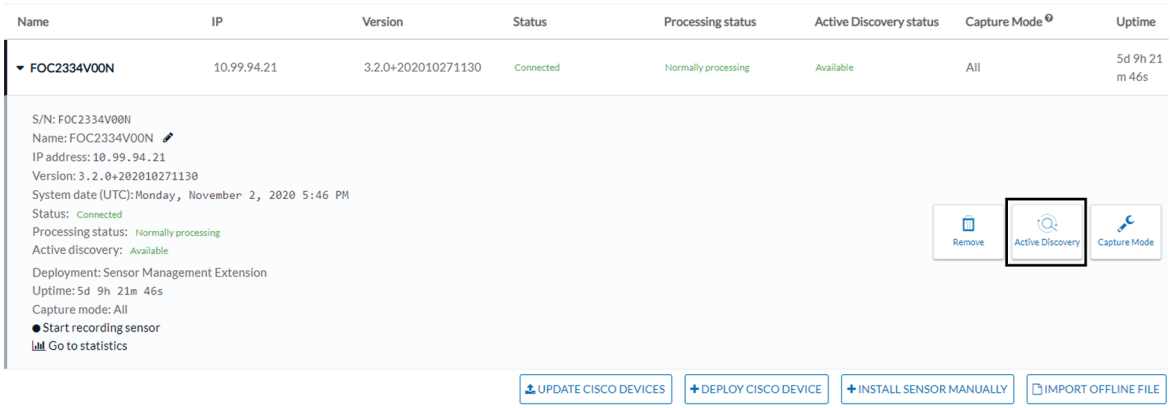


6.3 Configure Active Discovery (IE3300/IE3400 only)

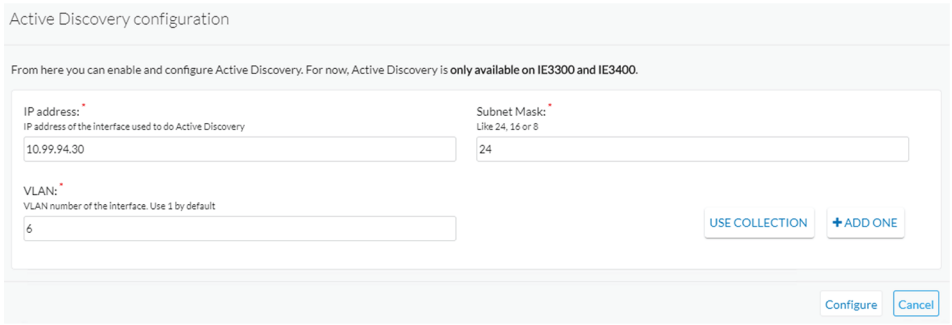
Once the sensor is connected, you can change the Active Discovery's network interface so it uses the Collection network interface instead, and add several network interfaces for the sensor to perform Active Discovery on several subnetworks at the same time.

To set the Active Discovery on the Collection network interface:

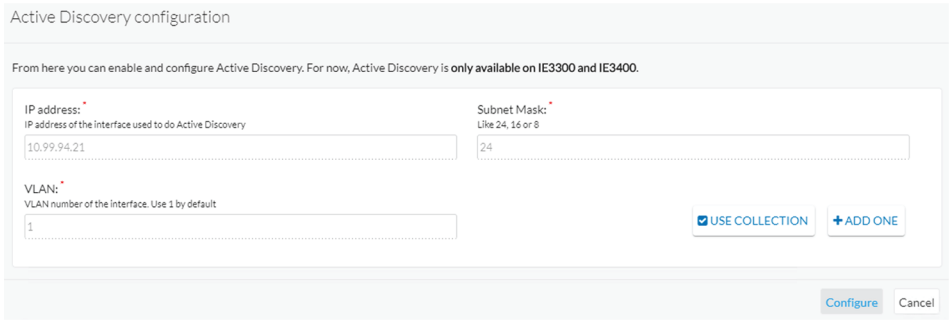
1. Click the Active Discovery button.



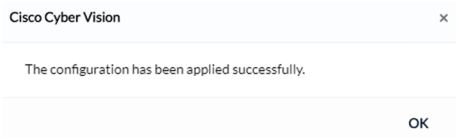
The Active Discovery configuration appears with the interface currently set.



2. Click the Use Collection button for the Active Discovery to use the Collection network interface.

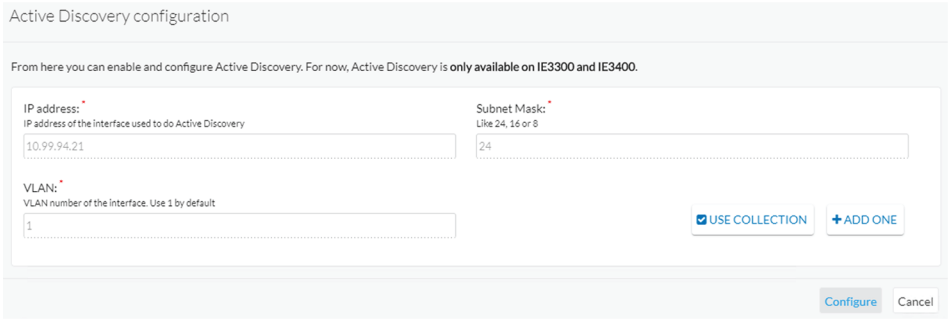


The following message is displayed to show that changes applied successfully.

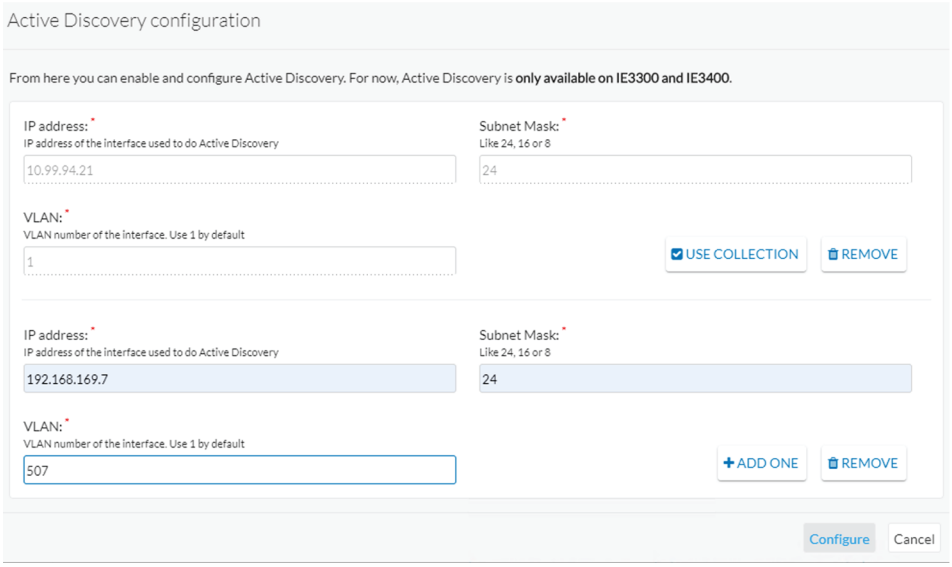


To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

1. Click the Add one button.



2. Fill the required fields with the subnetwork's information.



You can add as many interfaces as needed. The sensor will perform Active Discovery on all network interfaces added here.

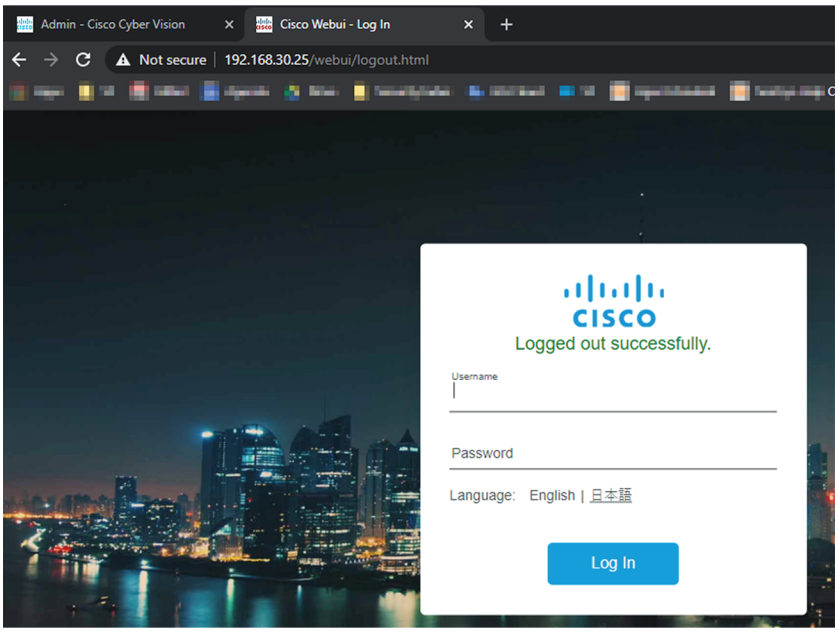
3. When you are done, click Configure.

7 Procedure with the Local Manager

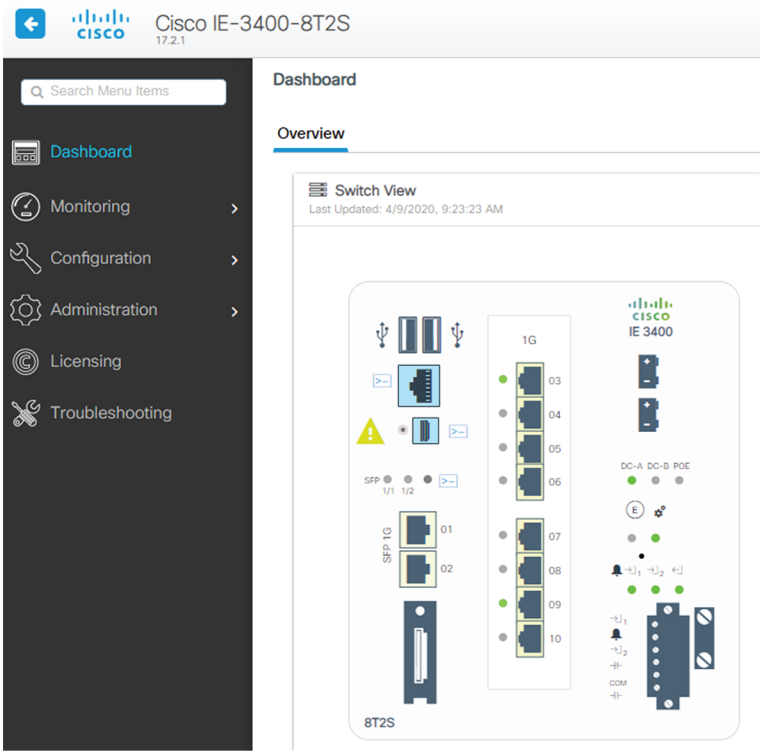
After the Initial configuration (page 11), proceed to the steps described in this section. This section also described the steps to configure Active Discovery on the Cisco IE3300 10G and Cisco IE3400.

7.1 Access the Local manager

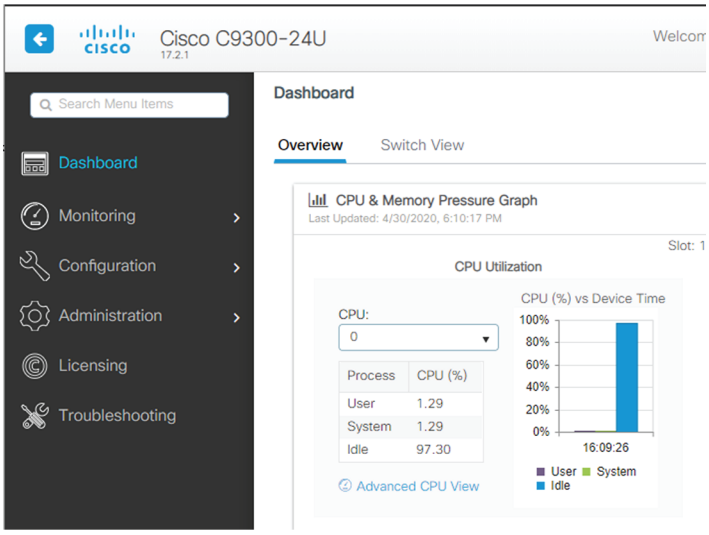
1. Open a browser and navigate to the IP address you configured on the interface you are connected to.
2. Log in using the Local Manager user account and password.



Cisco IE3300 10G/IE3400:

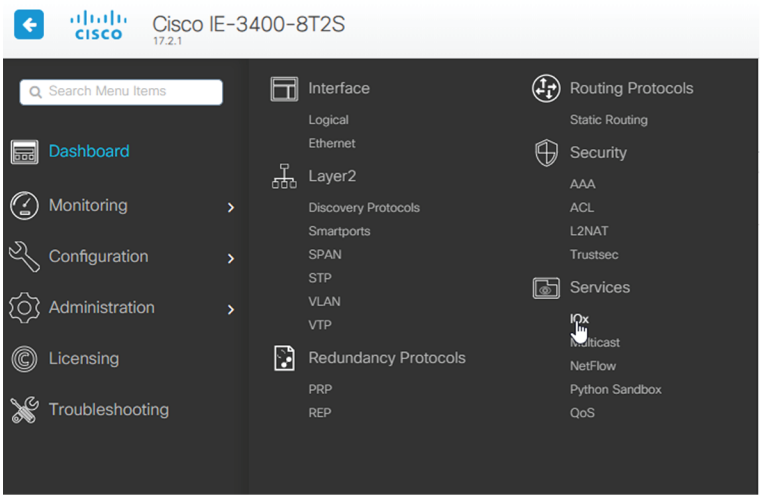


Cisco Catalyst 9300:

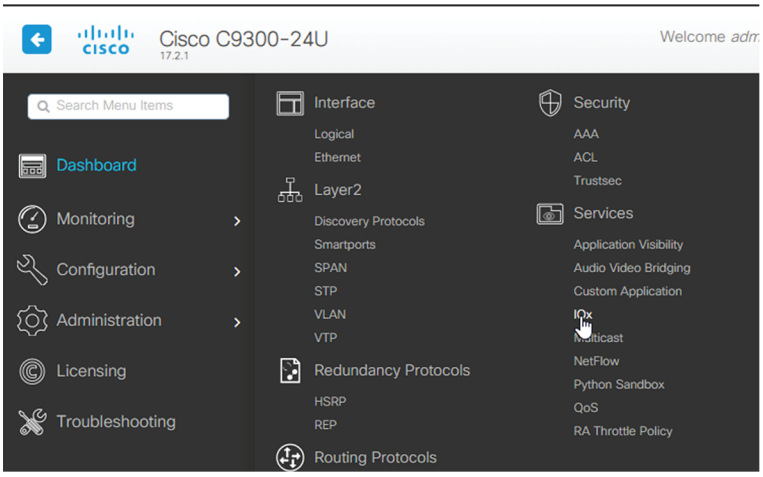


3. Once logged into the Local Manager, navigate to Configuration > Services > IOx.

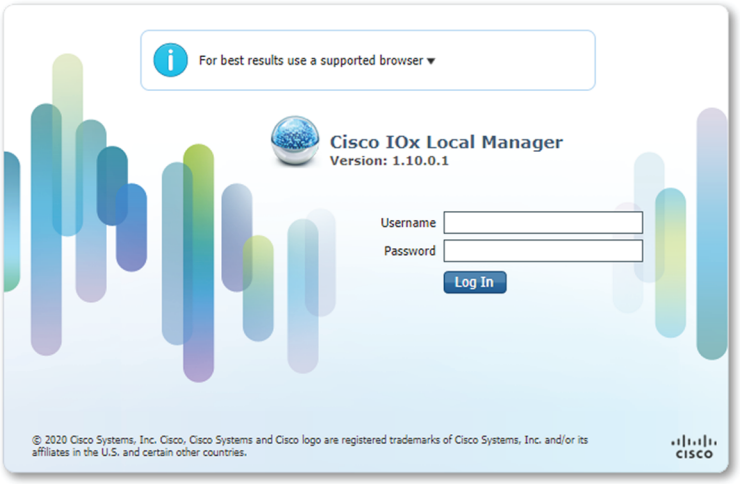
Cisco IE3300 10G/IE3400:



Cisco Catalyst 9300:

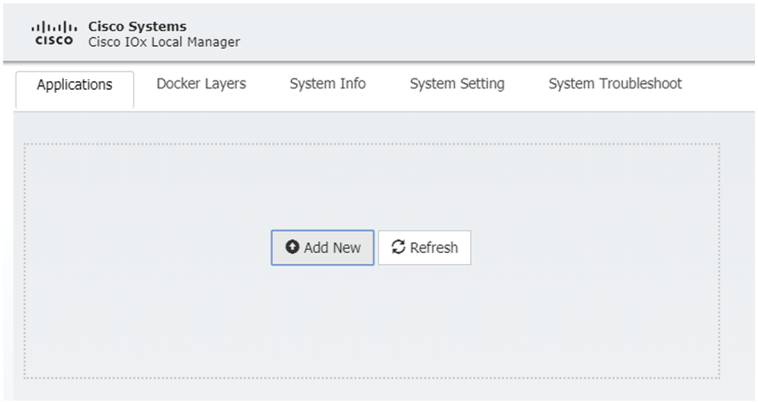


4. Log in using the user account and password.

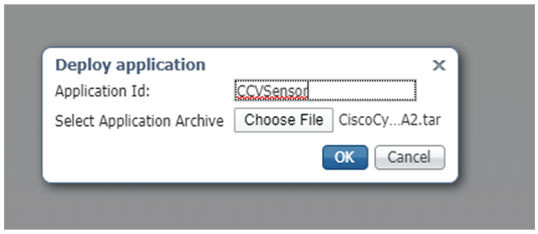


7.2 Install the sensor virtual application

Once logged in, the following menu appears:

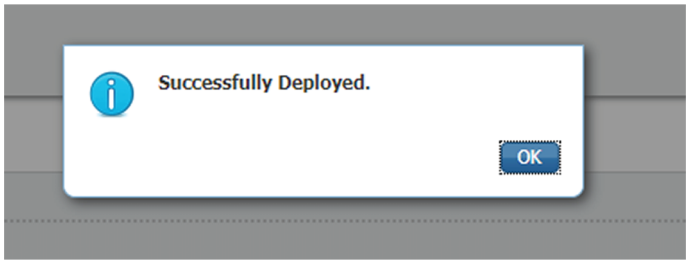


1. Click Add New.
2. Add an Application id name (e.g. CCVSensor).
3. Select the application archive file
    - "CiscoCyberVision-IOx-aarch64-xxx.tar" for the Cisco IE3300/IE3400
    - "CiscoCyberVision-IOx-Active-Discovery-aarch64.tar" for the Cisco IE3300/IE3400 with Active Discovery
    - "CiscoCyberVision-IOx-x86-64-xxx.tar"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



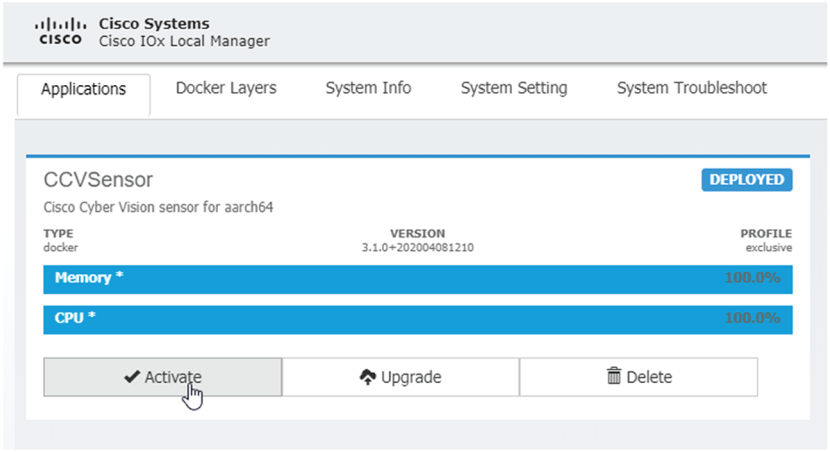
The installation takes a few minutes.

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

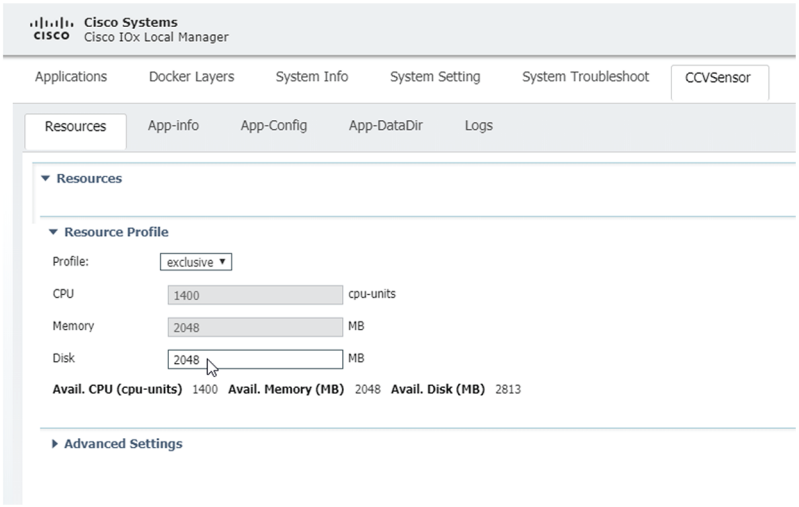


7.3 Configure the sensor virtual application (IE3300/IE3400)

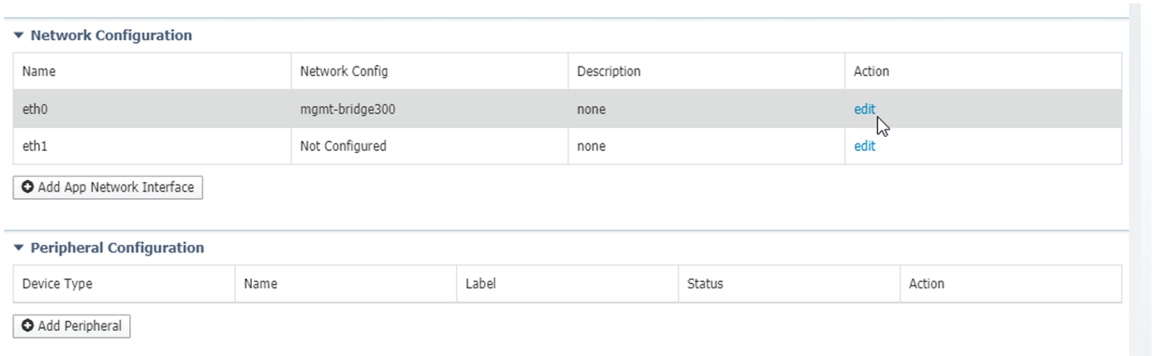
1. Click Activate to launch the configuration of the sensor application.



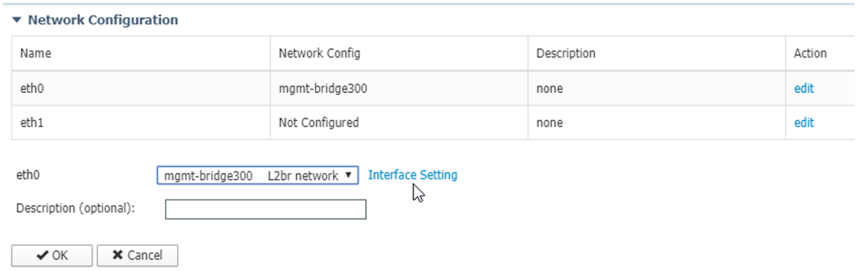
2. Change the disk size from the default size to 2048 MB. The disk size must not be larger than this.



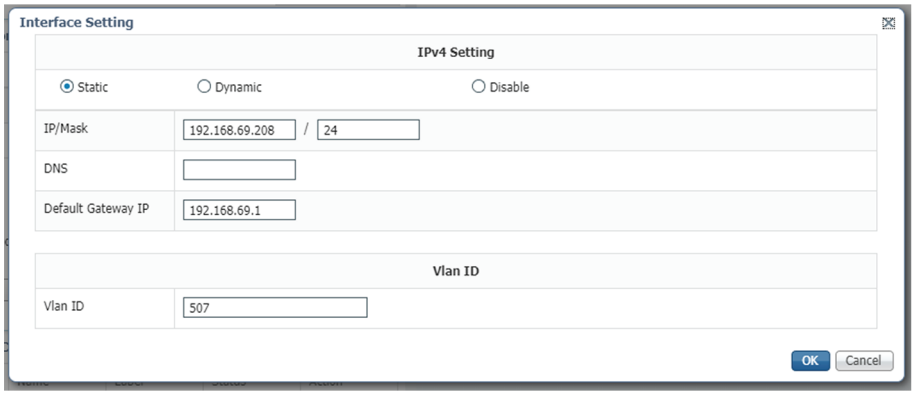
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking edit in the eth0 line.



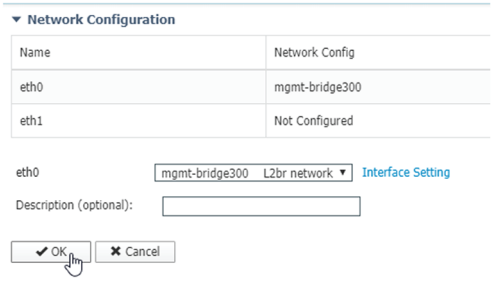
4. Click Interface Setting.



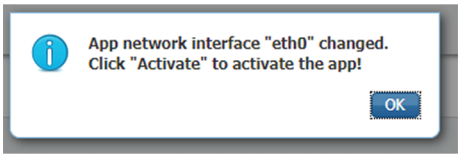
5. Apply the following configurations:
   - Select Static
   - IP/Mask: IP and mask of the sensor
   - Default gateway: IP address of the Center
   - Vlan ID, which is defined below, is the VLAN in the Cisco IE3300 10G/ IE3400 dedicated to the Collection network interface (link between the Center and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



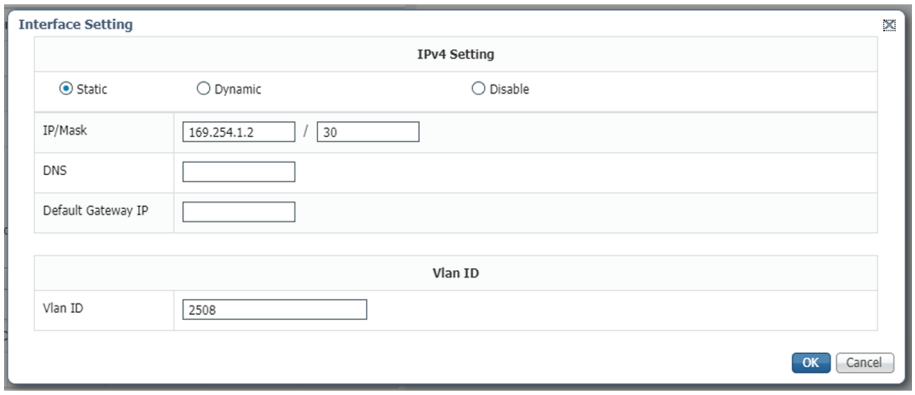
6. Click OK twice.



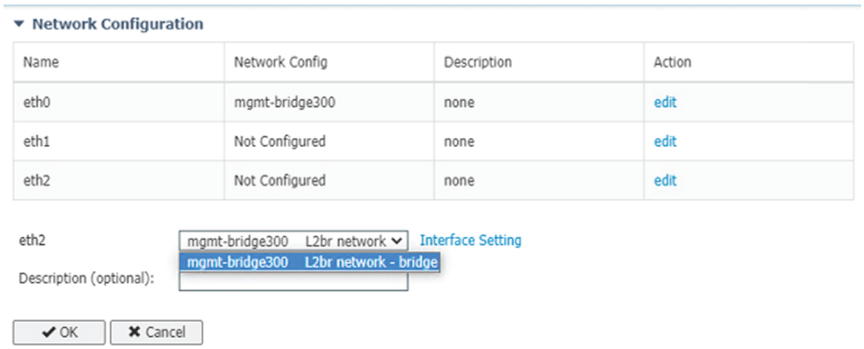
7. Click OK again on the popup.



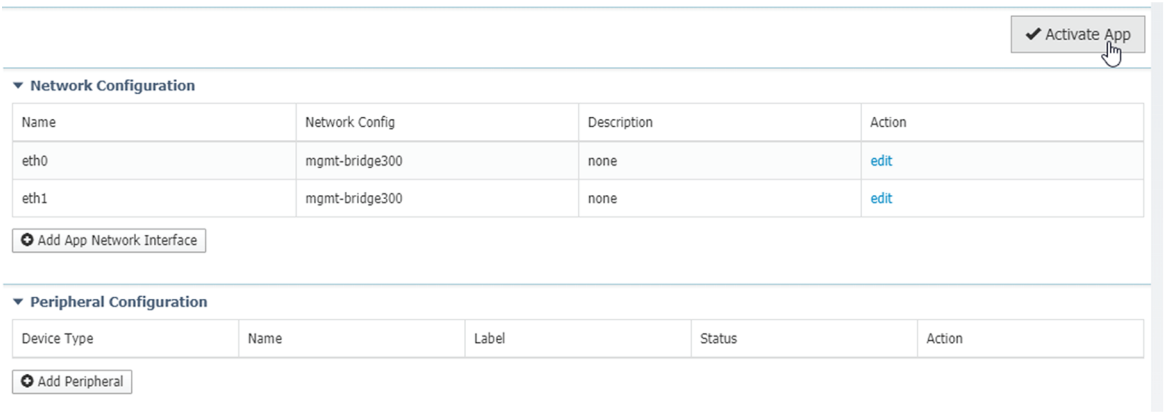
8. Then, apply the following parameters to eth1:
   - Select Static.
   - IP/Mask: the IP and mask of the sensor for the mirrored traffic.
   - Vlan ID, which is defined below, is the VLAN in the Cisco IE3300 10G/ IE3400 dedicated to traffic mirroring.



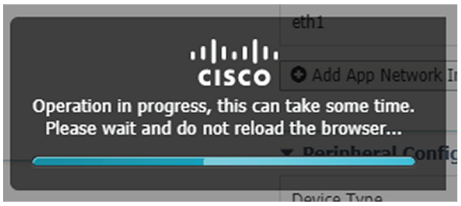
9. If configuring a sensor with **Active Discovery**, you must set an additional interface (eth2 without IP address) dedicated to this feature.



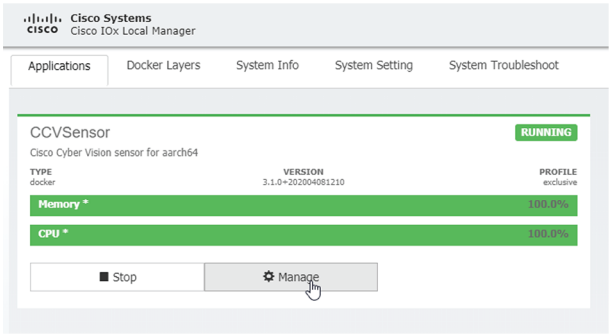
10. Click the Activate App button.



The operation takes several minutes.

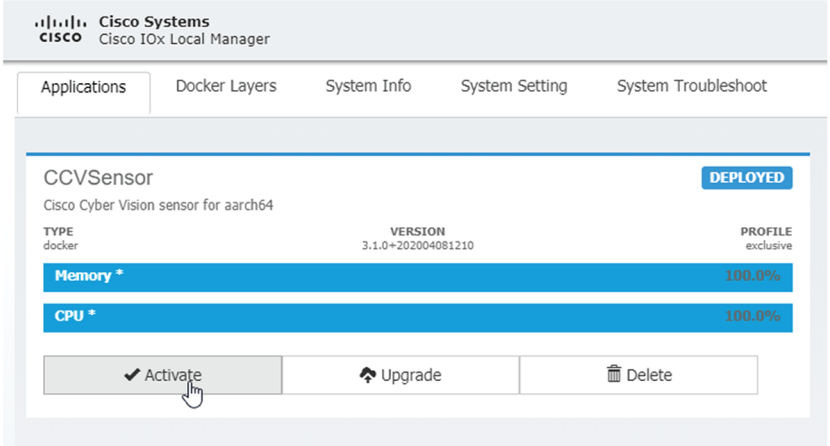


The application status changes to "RUNNING":

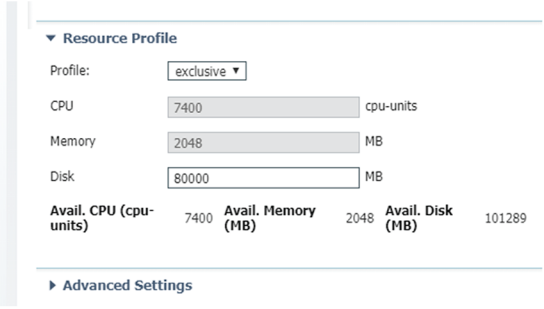


7.4 Configure the sensor virtual application (Catalyst 9300)

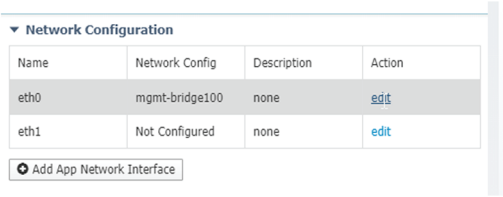
1. Click Activate to launch the configuration of the sensor application.



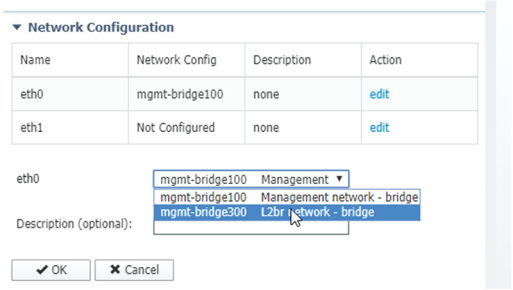
2. Change the disk size from the default size to 2048 MB. The disk size must not be smaller than this.



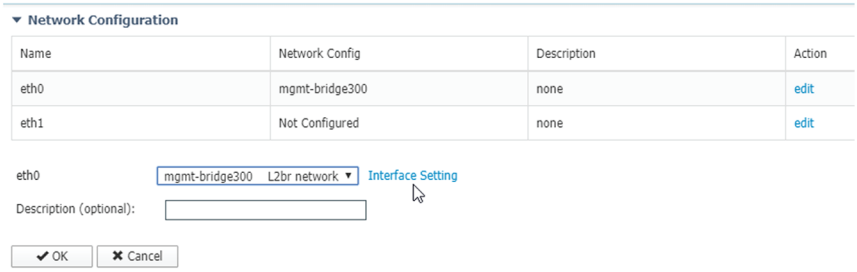
3. Bind the interfaces in the container to an interface on the host in Network Configuration. Start with eth0 by clicking edit in the eth0 line.



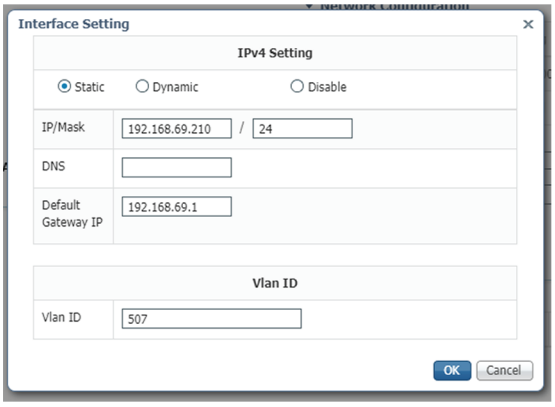
4. Select the mgmt.-bridge300 entry in the interface list.



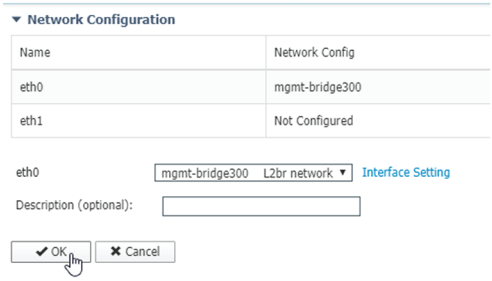
5. Click Interface Setting.



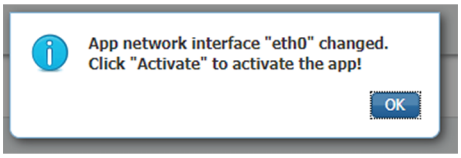
6. Apply the following configurations:
   - Select Static
   - IP/Mask: the IP and mask of the sensor
   - Default gateway: the IP address of the Center
   - Vlan ID, which is defined below, is the VLAN in the Cisco Catalyst 9300 dedicated to the Collection network interface (link between the Center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



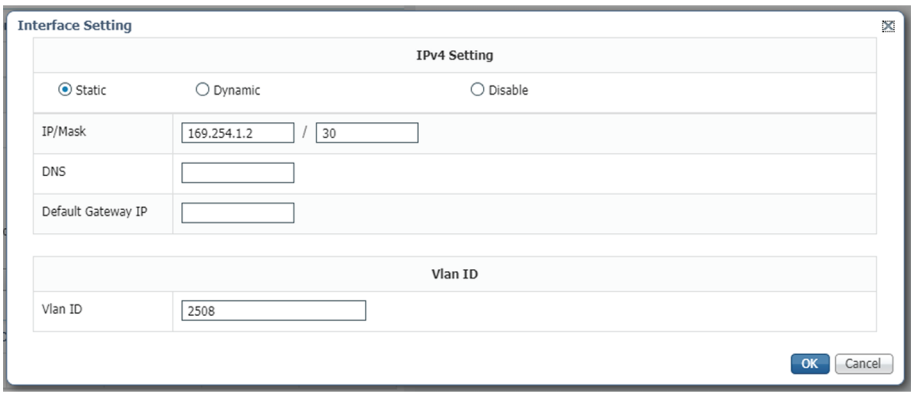
7. Click OK twice.



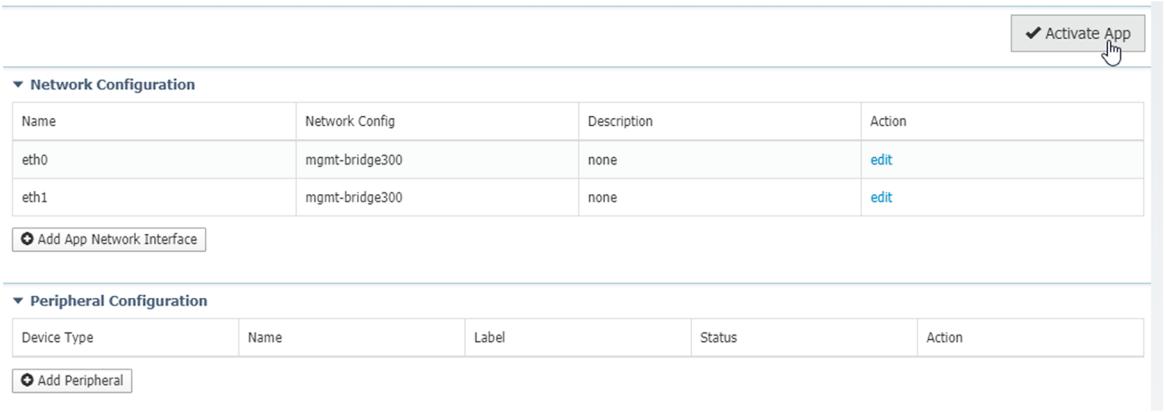
8. Click OK again on the following popup.



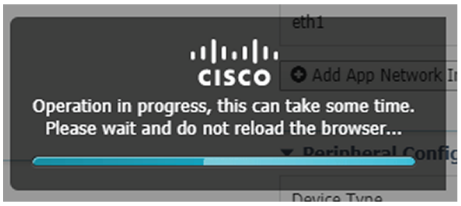
9. Apply the following configurations to eth1:
   - Select the mgmt.-bridge300 entry in the interface list
   - Select Static
   - IP/Mask: the IP and mask of the sensor for mirrored traffic
   - Vlan ID, will be defined below, is the VLAN in the Cisco Catalyst 9300 dedicated to traffic mirroring.



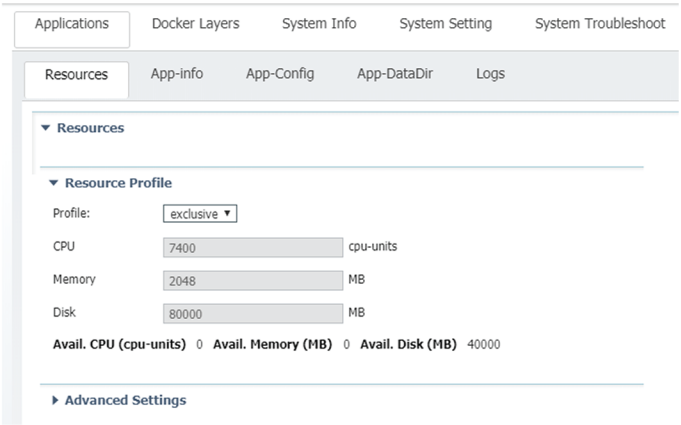
10. Click OK until you come back to the screen below.
11. Click the Activate App button.



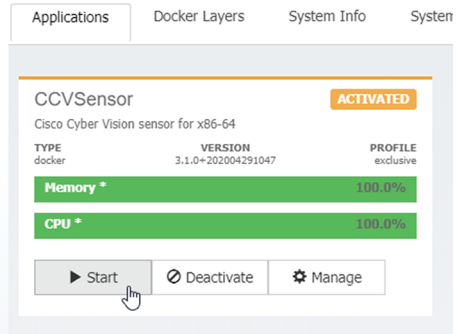
The operation takes several seconds.



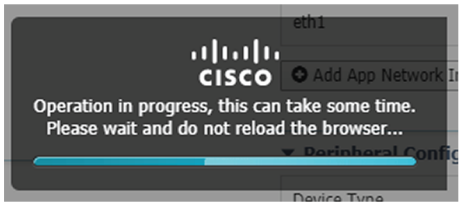
12. Click Applications to display the application status:



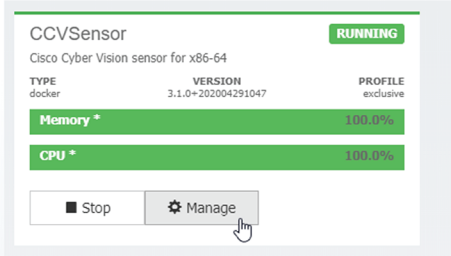
13. The application is activated and needs to be started. To do so, click the Start button.



The operation takes several seconds.

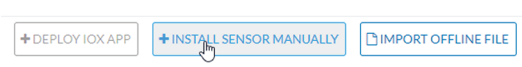


The application status changes to "RUNNING".

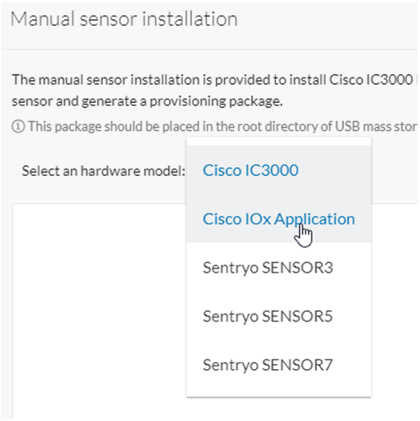


7.5 Generate the provisioning package

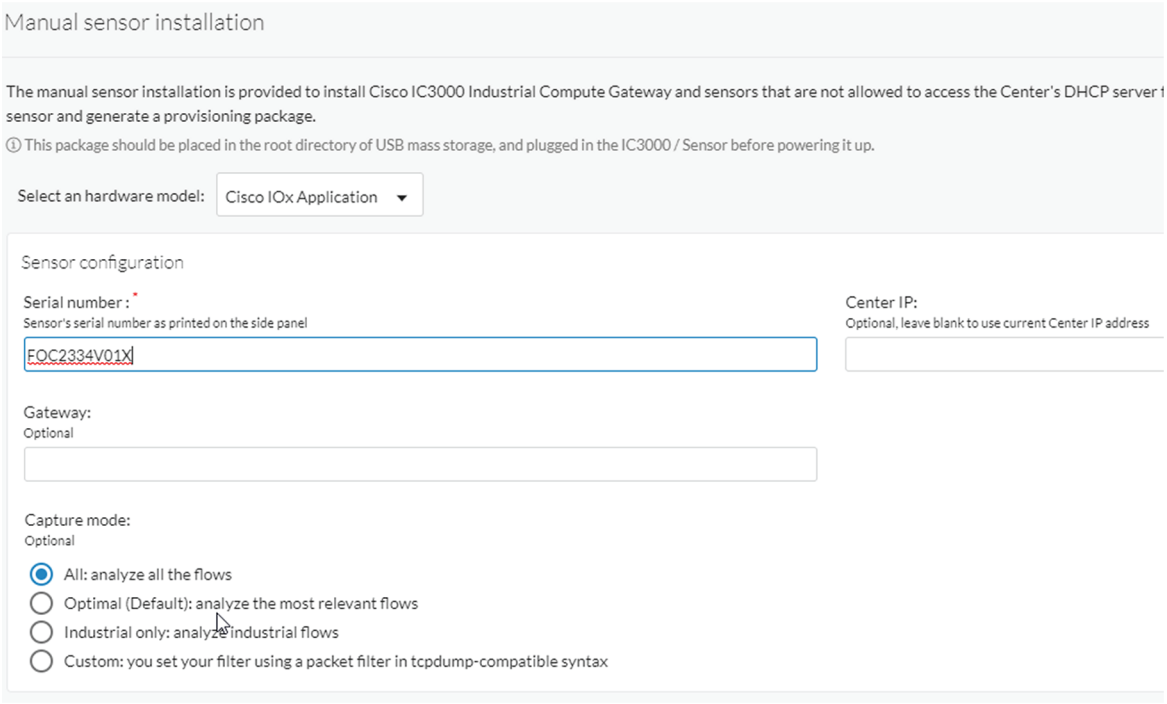
1. In Cisco Cyber Vision, navigate to Admin > Sensors > Management and click INSTALL SENSOR MANUALLY.



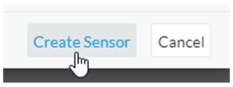
2. Select Cisco IOx Application sensor.



3. Fill the Manual sensor information form:
    - The serial number of the hardware.
    - Center IP: leave blank.
    - Gateway: add if necessary.
    - Optionally, select a capture mode.

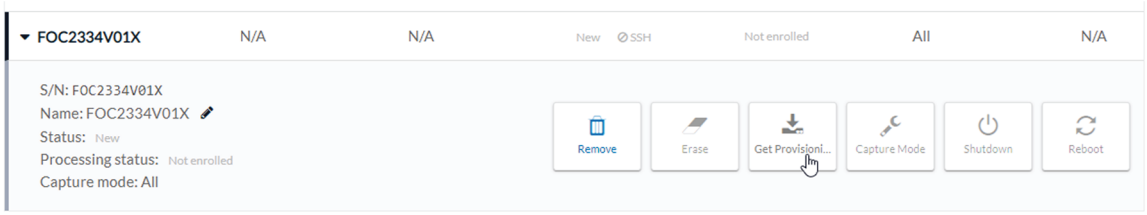


4. Click the Create Sensor button.



At this point, you should have a new entry for the sensor in Cisco Cyber Vision's sensors management page with the status New.

5. Click the entry, then click on the Get Provisioning Package button to download the provisioning package.



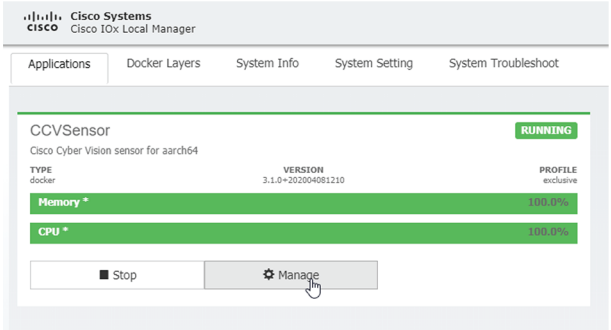
The sensors' status switches to Disconnected.

This will download the provisioning package which is a zip archive file with the following name structure: <sbs-sensor-config-IE3400orCAT9300SN>.zip (e.g. "sbs-sensor-configFCW23500HDC.zip").

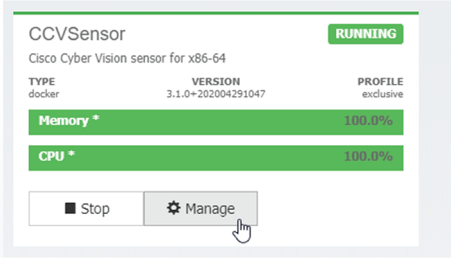
7.6 Import the provisioning package

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

Cisco IE3400:

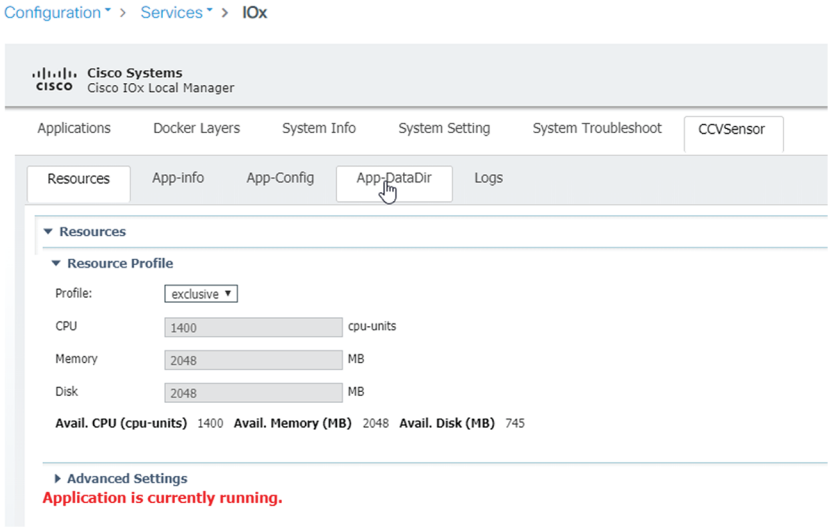


Cisco Catalyst 9300:

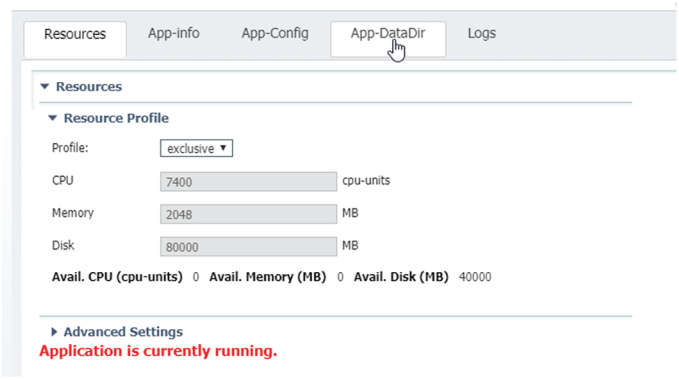


2. Navigate to App_DataDir.

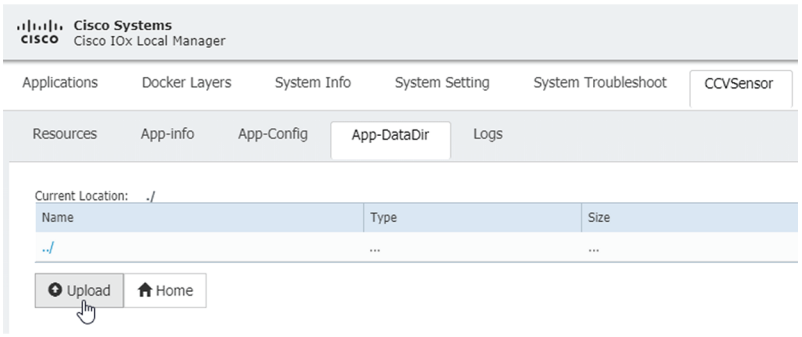
Cisco IE3400:



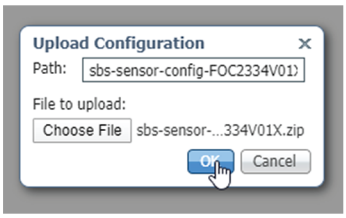
Cisco Catalyst 9300:



3. Click Upload.



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



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

6. Click OK.

8 Procedure with the CLI

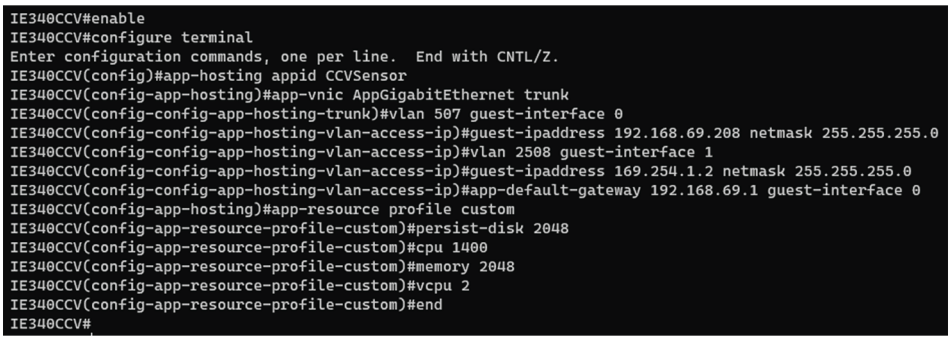
After the Initial configuration (page 11), proceed to the steps described in this section.

8.1 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
```



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, 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).

8.2 Install the sensor application

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

- CiscoCyberVision-IOx-aarch64-3.1.0.tar (Cisco IE3300 10G/IE3400).
- CiscoCyberVision-IOx-x86-64-3.1.0.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:

```
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).
>
> Replace "CiscoCyberVision-IOx-aarch64-3.1.0-RC4.tar" with the right filename.

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

```
show app-hosting list
```

Cisco IE3300 10G/IE3400:

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

IE340CCV#
```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#show app-hosting list
App id                                   State
---------------------------------------------------------
CCVSensor                                DEPLOYED

CAT9KCCV#
```

4. Activate the application using the following command:

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

Cisco IE3300 10G/IE3400:

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

IE340CCV#
```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#app-hosting activate appid CCVSensor
CCVSensor activated successfully
Current state is: ACTIVATED

CAT9KCCV#
```

5. Start the application using the following command:

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

Cisco IE3300 10G/IE3400:

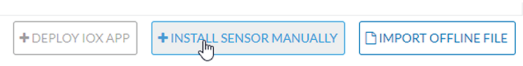
```
IE340CCV#
IE340CCV#app-hosting start appid CCVSensor
CCVSensor started successfully
Current state is: RUNNING
IE340CCV#
```

Cisco Catalyst 9300:

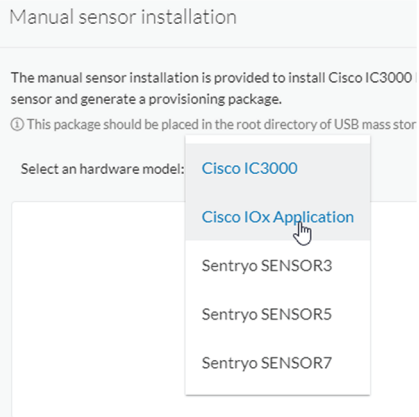
```
CAT9KCCV#
CAT9KCCV#app-hosting start appid CCVSensor
CCVSensor started successfully
Current state is: RUNNING
CAT9KCCV#
```

8.3 Generate the provisioning package

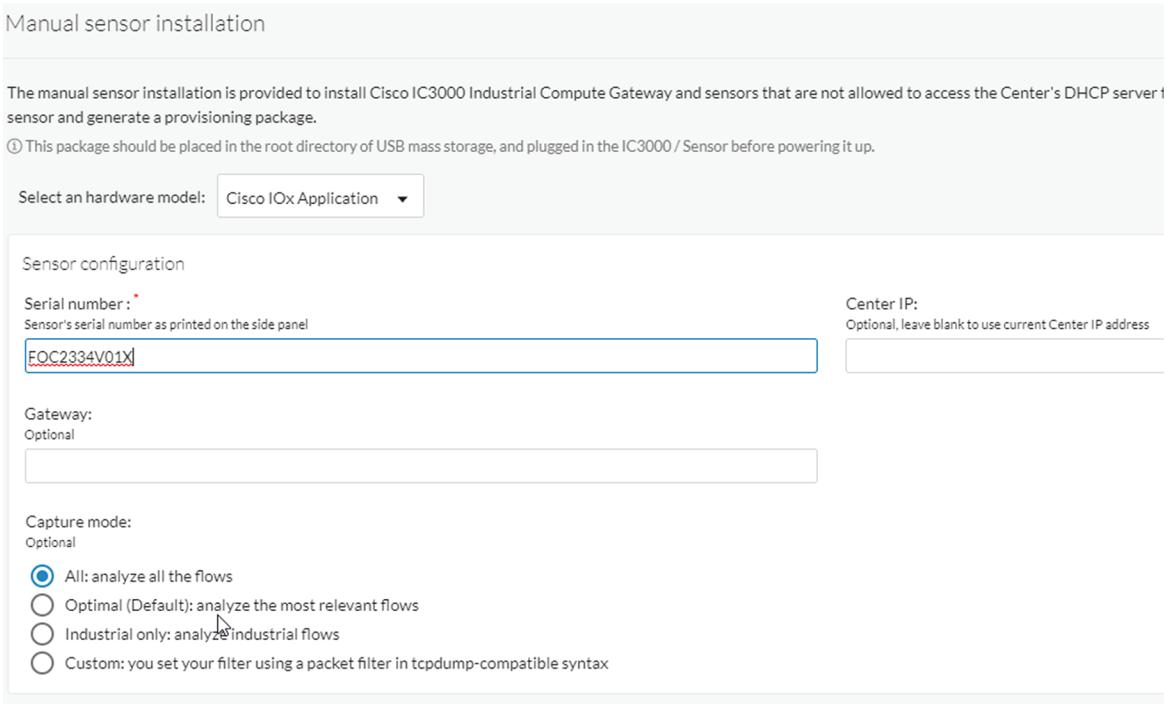
1. In Cisco Cyber Vision, navigate to Admin > Sensors > Management and click INSTALL SENSOR MANUALLY.



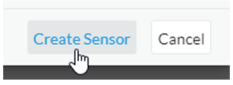
2. Select Cisco IOx Application sensor.



3. Fill the Manual sensor information form:
    - The serial number of the hardware.
    - Center IP: leave blank.
    - Gateway: add if necessary.
    - Optionally, select a capture mode.

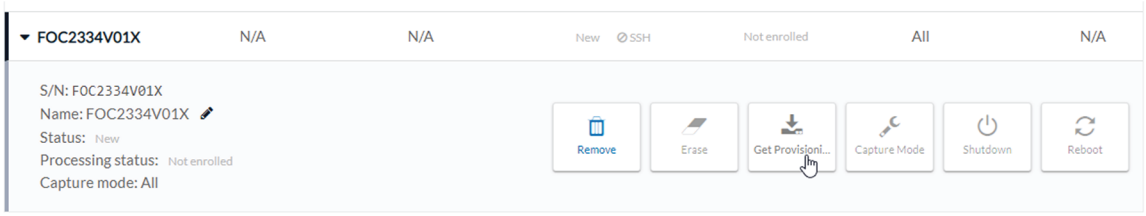


4. Click the Create Sensor button.



At this point, you should have a new entry for the sensor in Cisco Cyber Vision's sensors management page with the status New.

5. Click the entry, then click on the Get Provisioning Package button to download the provisioning package.



The sensors' status switches to Disconnected.

This will download the provisioning package which is a zip archive file with the following name structure: <sbs-sensor-config-IE3400orCAT9300SN>.zip (e.g. "sbs-sensor-configFCW23500HDC.zip").

8.4 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
```

Cisco IE3300 10G/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#
```

Cisco Catalyst 9300:

```
CAT9KCCV#
CAT9KCCV#$ data appid CCVSensor copy usbflash0:sbs-sensor-config-FCW2324GHNN.zip sbs-sensor-config-FCW2324GHNN.zip
Successfully copied file /usbflash0/sbs-sensor-config-FCW2324GHNN.zip to CCVSensor as sbs-sensor-config-FCW2324GHNN.zip
CAT9KCCV#
```

8.5 Final step

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

```
write mem
```