



Cyber Vision Center

- [Cyber Vision Support, on page 1](#)
- [Installing CVC Sensor using LM GUI, on page 8](#)

Cyber Vision Support

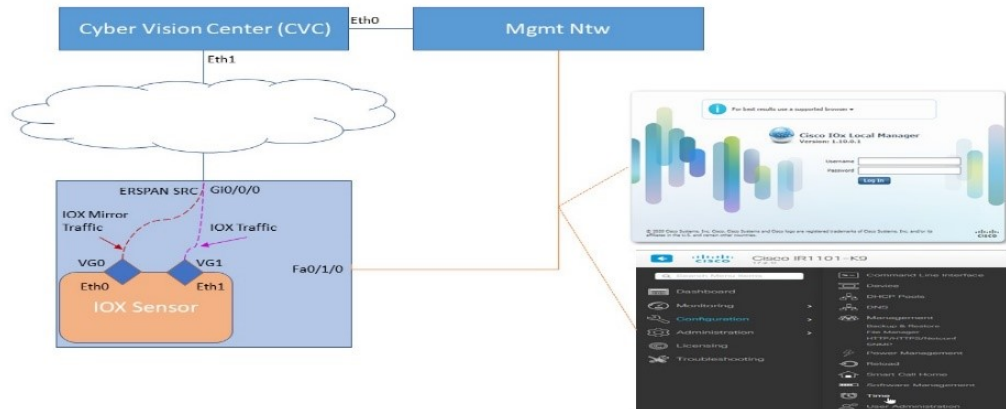
Cisco Cyber Vision Center (CVC) gives more visibility into Industrial IoT networks across Industrial Control Systems (ICS) with real-time monitoring of control and data networks. On IoT IOS-XE platforms beginning with release 17.4, integration of CVC is supported by deploying IOX Cyber Vision sensor. With this sensor deployed on IoT Routers, the platform can forward the traffic from IOX applications to Cyber Vision Center for real-time monitoring and we can forward any captured PCAP files to Vision center from IOX application.

Deployment of Cyber Vision Center (CVC) on IOS-XE platform

Procedure

- Step 1** Download Cisco supported Cyber Vision IOX application from the following location:
<https://software.cisco.com/download/home/286325414/type/286325316/release/3.1.1?catid=268438162>
Select **Cisco Cyber Vision Sensor IOx Application 3.1.1 for IE3400 and IR1101**.
- Step 2** Install CVC version 3.1.1 on Virtual Machine or on any Hypervisor. The following location is the download link for different versions of CVC:
<https://software.cisco.com/download/home/286325414/type>
Release Notes for Cisco Cyber Vision Release 3.1.1:
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco-Cyber-Vision_Release-Note-3-1-1.pdf
- Step 3** The CVC sensor requires two VirtualPort Group interfaces. One on the platform where one interface is used for IOX traffic, and the other for mirror traffic which is forwarded to physical, SVI or Tunnel interface which ERSPAN source. Refer to the following illustration:

Figure 1: CVC over L3 interface



Step 4 The CVC Sensor deployment can be installed from either the LMGUI or CLI.

Example Configuration for ERSPAN over L3 configuration along with Virtual Port Groups

Physical and Virtual Port Configuration:

```
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
interface virtualportgroup 1
ip nat inside
ip address 169.254.0.1 255.255.255.252
interface gi0/0/0
ip address 101.0.0.151 255.255.255.0
ip nat outside
no shut
```

ERSPAN Configuration:

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

NAT Configuration with Access-list:

```
ip nat inside source list NAT_ACL interface Gi0/0/0 overload
ip access-list standard NAT_ACL
10 permit 169.254.0.0 0.0.0.3
```

CLI Installation

To install the app through the CLI, copy the CVC sensor to bootflash, USB, or mSATA. Then install the app using the app-hosting CLI, and provide the docker options before activating the app.

For example:

```
Router(config-if)#iox
Router# app-hosting install app-id <app-id> package {bootflash:|usbflash0:|msata:}
app-hosting appid <app-id>
app-vnic gateway0 virtualportgroup 0 guest-interface 0
    guest-ipaddress 169.254.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
    guest-ipaddress 169.254.0.2 netmask 255.255.255.252
app-default-gateway 169.254.0.1 guest-interface 1
app-resource docker
    run-opts 1 "--rm --tmpfs /tmp:rw,size=128m"
Router# app-hosting {activate|start|stop|deactivate|uninstall} app-id <app-id>
```

LMGUI Installation

Configure the following to reach the LMGUI:

```
iox
ip http server
ip http secure-server
ip http authentication local
Username cisco privilege 15 password cisco
Login URL: http://<Mgmt_IP>/iox/login
```

Additional details can be found in [Installing CVC Sensor using LM GUI, on page 8](#)

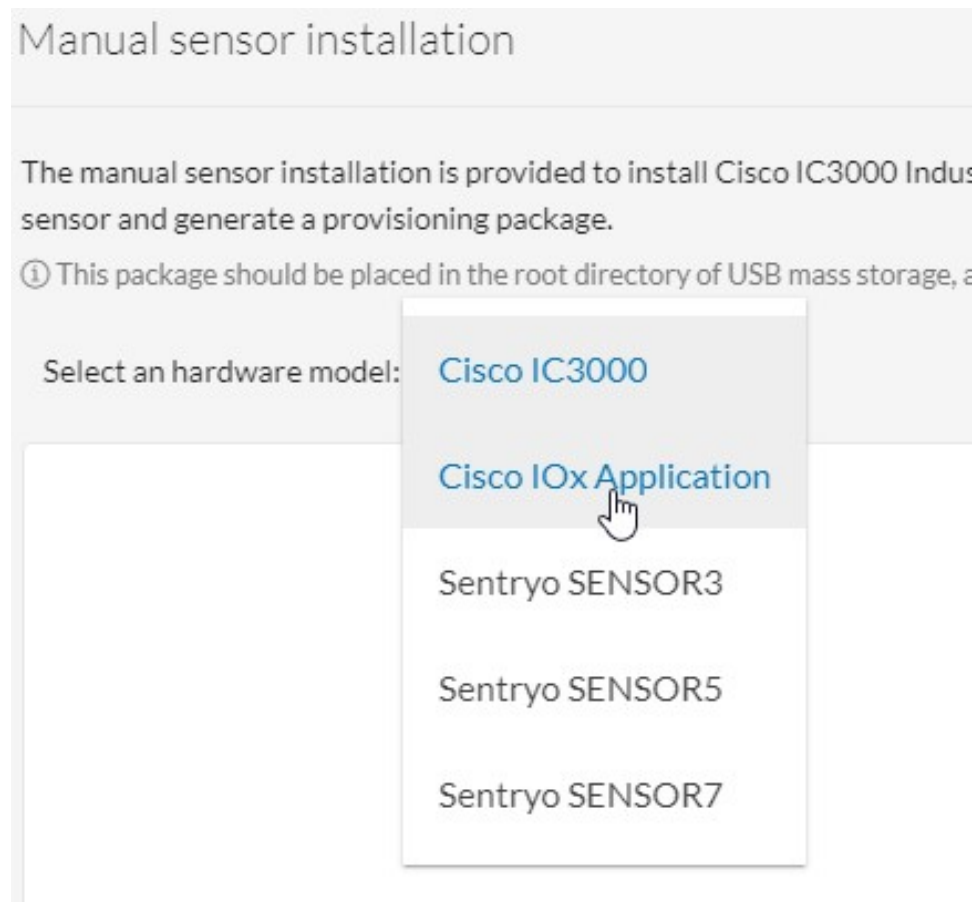
Register the Router Details

Procedure

Step 1 Register the IOS-XE Router details on CVC by logging in and navigating to:

Admin > Sensors > Install Sensor Manually

Then click on Cisco IOx Application. Refer to the following:

Figure 2: Sensor install

- Step 2** Provide the serial number of the Router. It should be an exact match from the output of **show inventory**, and then click on **Create Sensor**. Refer to the following:

Figure 3: Router Serial Number

Manual sensor installation

The manual sensor installation is provided to install Cisco IC3000 Industrial Compute Gateway and sensors that are not allowed to access the Center's DHCP server for automatic configuration. Please fill the fields below to configure your sensor and generate a provisioning package.

① This package should be placed in the root directory of USB mass storage, and plugged in the IC3000 / Sensor before powering it up.

Select an hardware model: Cisco IOx Application ▼

Sensor configuration

Serial number: *
Sensor's serial number as printed on the side panel

FCW23500HDC

Center IP:
Optional, leave blank to use current Center IP address

Gateway:
Optional

Capture mode:
Optional

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

Create Sensor Cancel

Step 3 Generate the Provisioning file from CVC by clicking on Get Provisioning File. Refer to the following:

Figure 4: Generate Provisioning File

FCW23500HDC	N/A	N/A	New	SSH
S/N: FCW23500HDC Name: FCW23500HDC ✎ Status: New Processing status: Not enrolled Capture mode: All				

Step 4 Download the provisioning file to a local directory. The file comes as a zip file with a file name like the following:

Example:

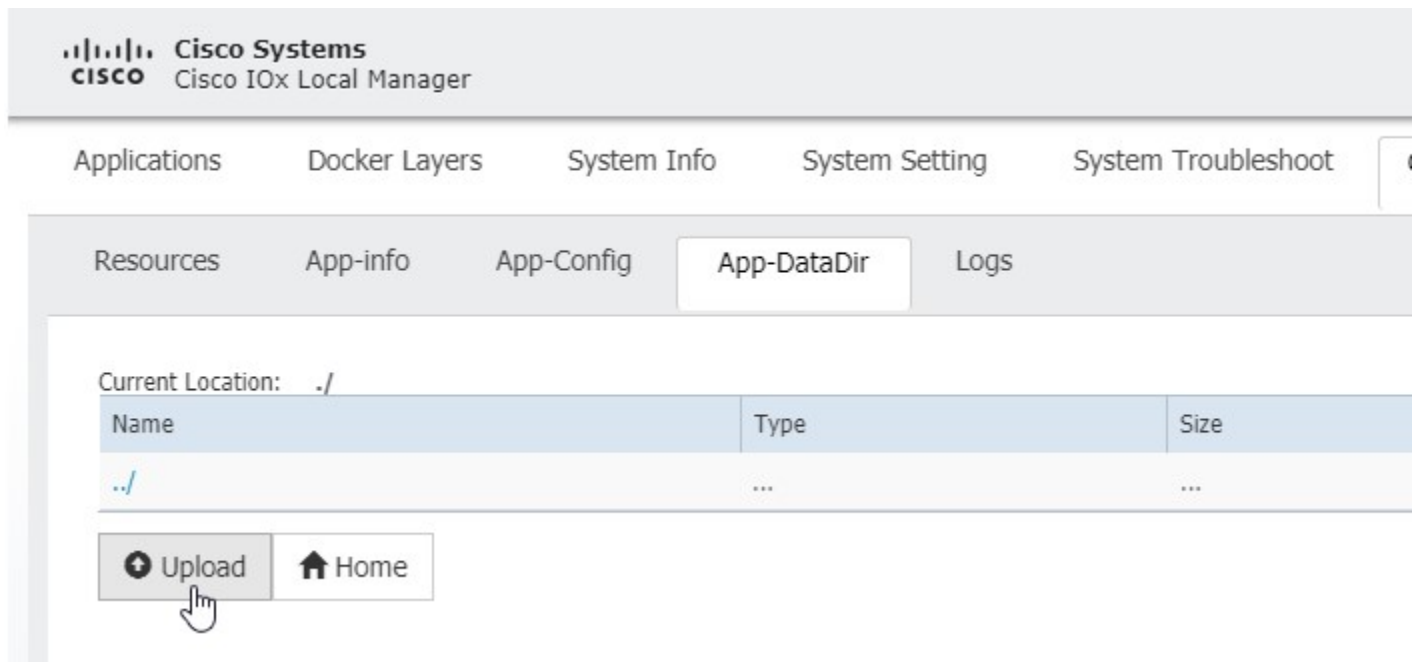
sbs-sensor-config-*<S/N of Router>*.zip

Step 5 Import the Provisioning file to Router through the LM GUI. From the LM GUI Applications, navigate to:

Applications > CVC App (Application Name) > Manage > App-DataDir

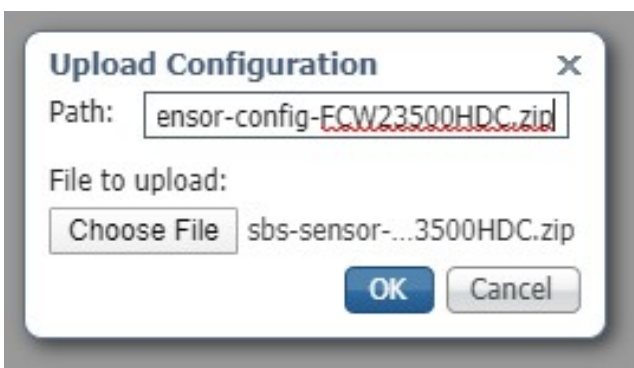
Refer to the following:

Figure 5: Upload Provision File



Step 6 Click **Upload**. The Upload Configuration window appears. Upload the downloaded provisioned file from CVC with the same name. Refer to the following:

Figure 6: Upload Configuration



Step 7 Verify the Authentication on CVC. Validate if the installed sensor Status changed to **Connected** or **Waiting for Data**. Refer to the following:

Figure 7: Sensor Status



Capture Live Traffic

Procedure

- Step 1** Sync the date and time between CVC and Router. To capture the live traffic there should be exact clock sync between Router and CVC.
- Step 2** Simulate IOX Traffic or play captured PCAP files. The CVC Sensor installed on the Router is a docker app. To login to the console of the App, perform the following command:

Example:

```
app-hosting connect app-id <app-name> session
```

- Step 3** Upload the PCAP Files to the App from LM-GUI. Navigate to:
Applications > CVC App (Application Name) > Manage > App-Dir
- The following commands show how to play the PCAP file:

Example:

```
Router# show app-hosting list
App id      State
```

```
-----
CVC Sensor    RUNNING
```

```
Router# app-hosting connect appid CVCSensor session
```

```
sh-5.0#
```

```
*Jul 14 08:45:05.603: %SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(15! in/busybox.nosuid"
dev="overlay" ino=72930 scontext=system_u:system_r: polaris_bexecute_*
```

```
sh-5.0# flowctl read-capture-file /iox_data/appdata/tl04
```

```
OK
```

```
sh-5.0#
```

Step 4 Monitor the traffic on CVC. Navigate to **Explore > Essential Data > Activity List**

Refer to the following:

Figure 8: Activity List

Explore / Essential data / Activity list

Sep 24, 2020 1:17:04 PM - Sep 24, 2020 1:27:04 PM (10 mins) LIVE

4 Activities Export to CSV

< 1 > 20 / page

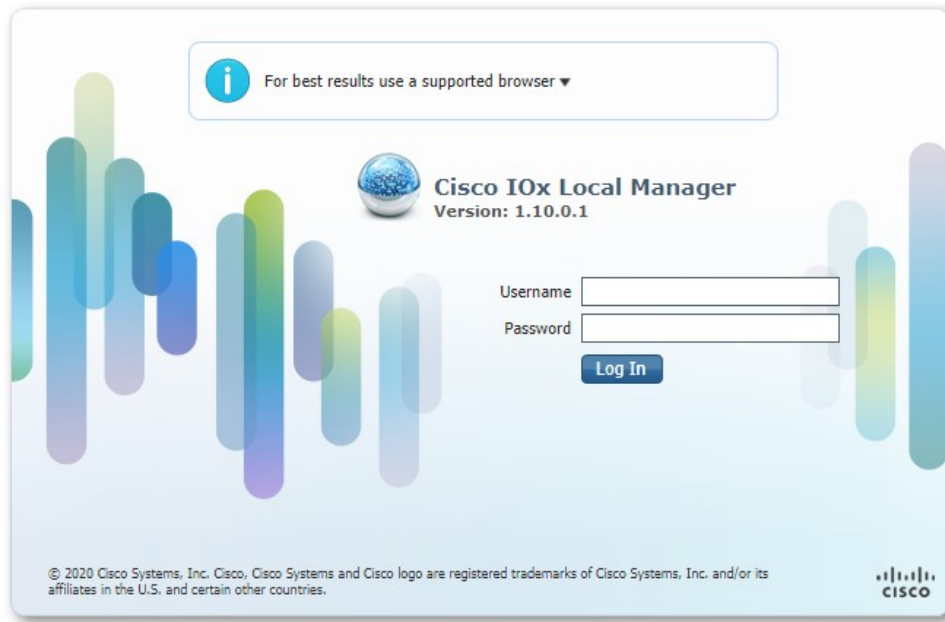
Component	Component	First activity	Last activity	Tags
169.254.1.2	Cisco 169.254.1.1	Sep 12, 2020 3:00:29 PM	Sep 24, 2020 1:26:33 PM	Tunneling , ARP
105.0.0.1	101.0.0.151	Sep 14, 2020 7:44:21 AM	Sep 24, 2020 1:26:33 PM	Unestablished , Ping , Web , ARP
101.0.0.3	255.255.255.255	Jul 14, 2020 12:59:47 AM	Sep 24, 2020 1:25:51 PM	Time Management , Broadcast
SIT-DC	101.0.0.255	Jul 14, 2020 1:07:50 AM	Sep 24, 2020 1:22:02 PM	Insecure , Broadcast , Netbios , SMB

Installing CVC Sensor using LM GUI

Procedure

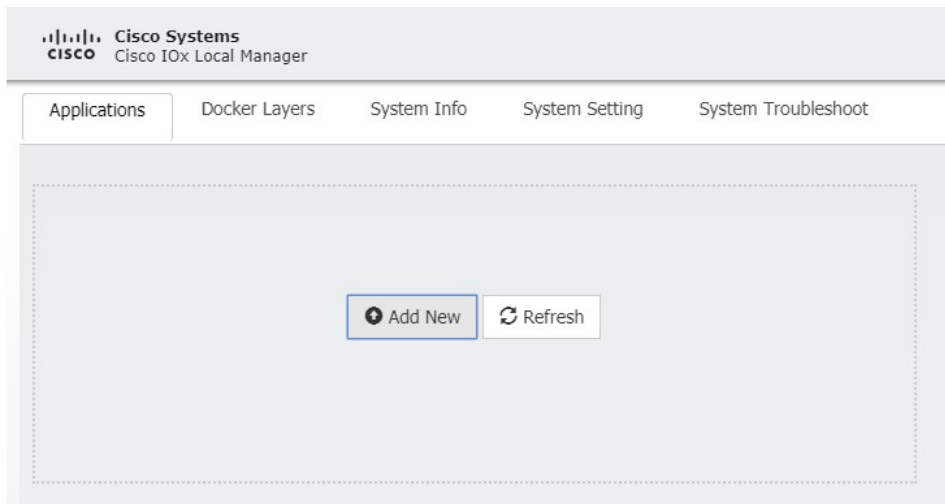
Step 1 Login using user account and password.

Figure 9: Local Manager Login



Step 2 Install the sensor virtual application. Once you are logged in, the following menu will appear:

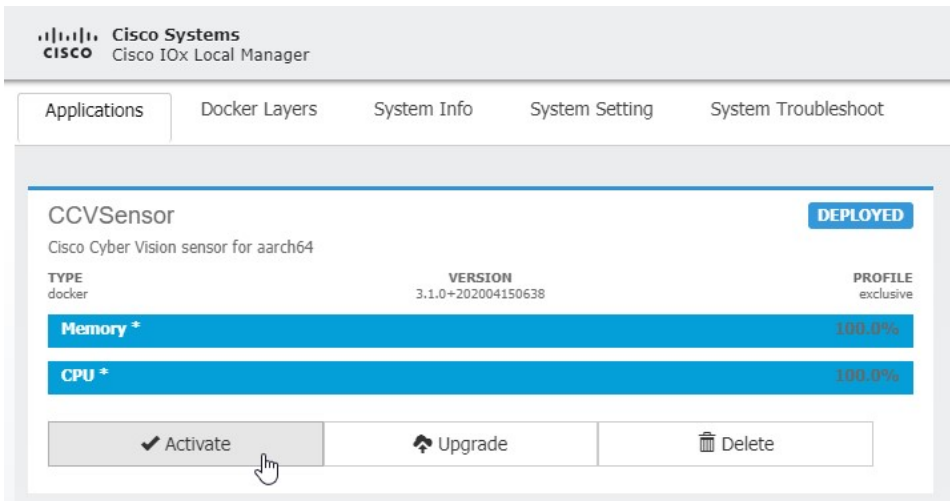
Figure 10: LM GUI Application Install



Step 3 Click on **Add New**. Navigate to the app file, for example, CiscoCyberVision-IOx-aarch64-xxx.tar. Add the name of the app, for example, **CCVSensor**.

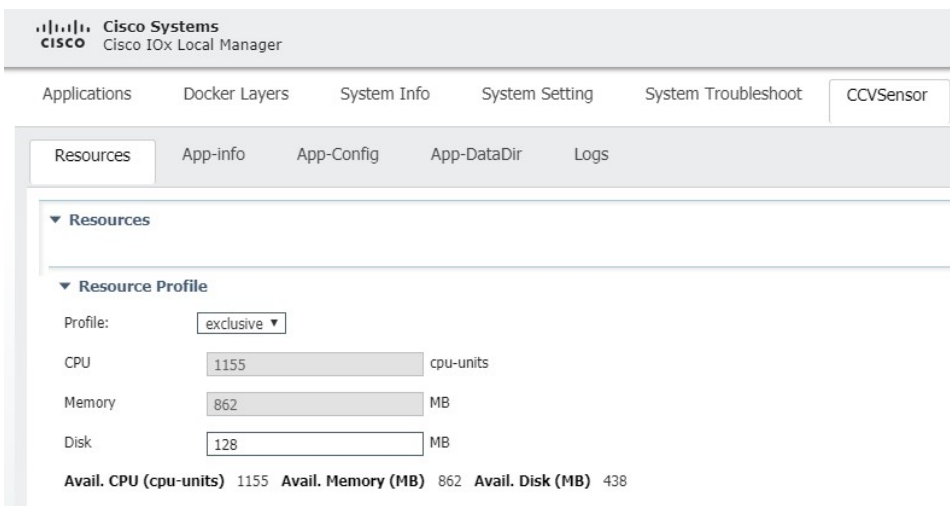
Configure the sensor virtual application. Refer to the following:

Figure 11: CCVSensor Activation



Step 4 Click on **Activate** to launch the configuration of the sensor application. Click on the **CCVSensor** Tab, and click on **Resources**. Refer to the following:

Figure 12: Setup Sensor LM IOXAppDisk



Change the disk size to 128MB.

Note

Do not use more space than that.

Step 5 Navigate to **Advanced Settings**. In advanced options, configure the tmpfs by adding the following in the text area beside Docker Options:

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

Figure 13: Advanced Settings

Resource Profile

Profile: exclusive ▾

CPU: 1155 cpu-units

Memory: 862 MB

Disk: 128 MB

Avail. CPU (cpu-units) 1155 Avail. Memory (MB) 862 Avail. Disk (MB) 438

Advanced Settings

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

Docker Options: --rm --tmpfs /tmp:rw,size=128m

☒ Auto delete container instance

Step 6 Bind interfaces in the container to an interface on the host in the **Network Configuration** section.

What to do next

Move to the next sections Binding eth0 and Binding eth1.

Binding eth0

To configure eth0:

Procedure

Step 1 Select interface eth0, and then click on **edit**.

Figure 14: eth0

Network Configuration			
Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit

[Add App Network Interface](#)

Step 2 Select the Interface **VPG1**.

Figure 15: VPG1

▼ Network Configuration

Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0 VPG1 VirtualPortGroup via intsv1 ▼ [Interface Setting](#)

Description (optional): VPG0 VirtualPortGroup via intsv0
VPG1 VirtualPortGroup via intsv1

Step 3 Click on **Interface Setting**.

Figure 16: Interface Setting

▼ Network Configuration

Name	Network Config
eth0	VPG0
eth1	Not Configured

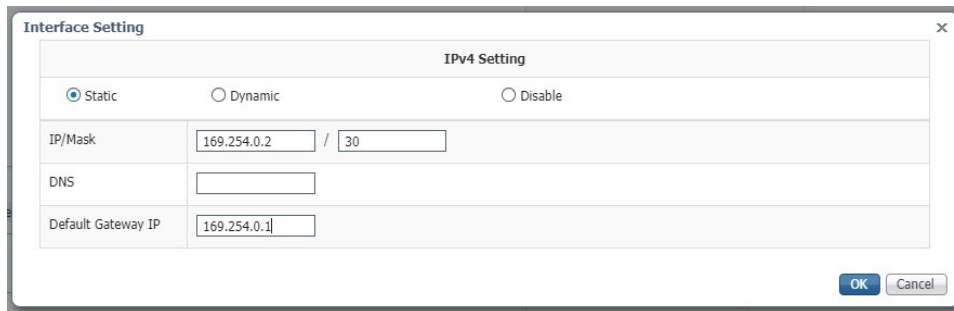
eth0 VPG1 VirtualPortGroup via intsv1 ▼ [Interface Setting](#)

Description (optional):

Step 4 Apply the following configuration:

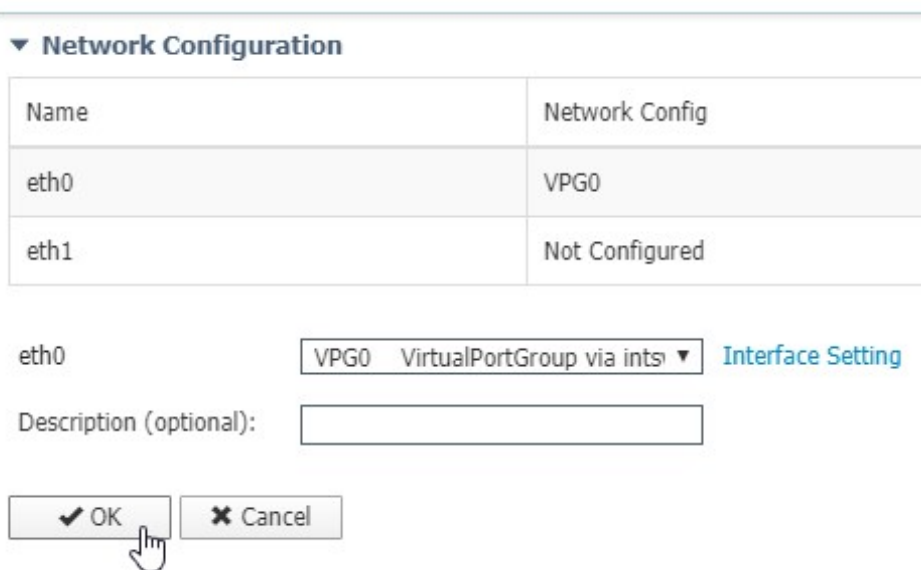
- Choose the **Static** option
- IP/Mask add **169.254.0.2 / 30**
- Default Gateway IP is **169.254.0.1**

Then click on **OK**.

Figure 17: IPv4 Setting

The 'Interface Setting' dialog box is shown with the 'IPv4 Setting' tab selected. The 'Static' radio button is chosen. The IP/Mask field is set to '169.254.0.2 / 30'. The DNS field is empty. The Default Gateway IP field is set to '169.254.0.1'. The 'OK' and 'Cancel' buttons are at the bottom right.

Step 5 Click on **OK** again.



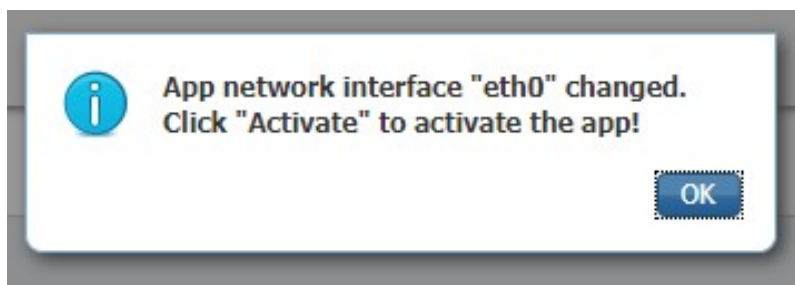
Network Configuration

Name	Network Config
eth0	VPG0
eth1	Not Configured

eth0 VPG0 VirtualPortGroup via intsr [Interface Setting](#)

Description (optional):

Step 6 The **Activate** window appears. Click on **OK**.

Figure 18: Activate Window

Binding eth1

To configure the eth1 interface:

Procedure

Step 1 Select VPG0.

Figure 19: VPG0

The screenshot shows a 'Network Configuration' dialog box. It contains a table with two columns: 'Name' and 'Network Config'. The table has three rows: 'eth0' with 'VPG1', and 'eth1' with 'Not Configured'. Below the table, there is a section for 'eth1' with a dropdown menu set to 'VPG0 VirtualPortGroup via ints' and a link labeled 'Interface Setting'. Below this is a text input field for 'Description (optional):'. At the bottom are 'OK' and 'Cancel' buttons.

Name	Network Config
eth0	VPG1
eth1	Not Configured

eth1 VPG0 VirtualPortGroup via ints ▼ [Interface Setting](#)

Description (optional):

Step 2 Click **Interface Setting** and apply the following configuration:

- Choose the **Static** option
- IP/Mask add **169.254.1.2 / 30**

Figure 20: IPv4 Setting

Interface Setting

IPv4 Setting

☒ Static
 ☐ Dynamic
 ☐ Disable

IP/Mask: 169.254.1.2 / 30

DNS:

Default Gateway IP:

Activate the Application

Now the sensor application should be activated.

Procedure

Step 1 Click on **Activate App**. Refer to the following:

Figure 21: Activate the Application

✓ Activate App

▼ Network Configuration

Name	Network Config	Description	Action
eth0	VP01	none	edit
eth1	VP00	none	edit

➤ Add App Network Interface

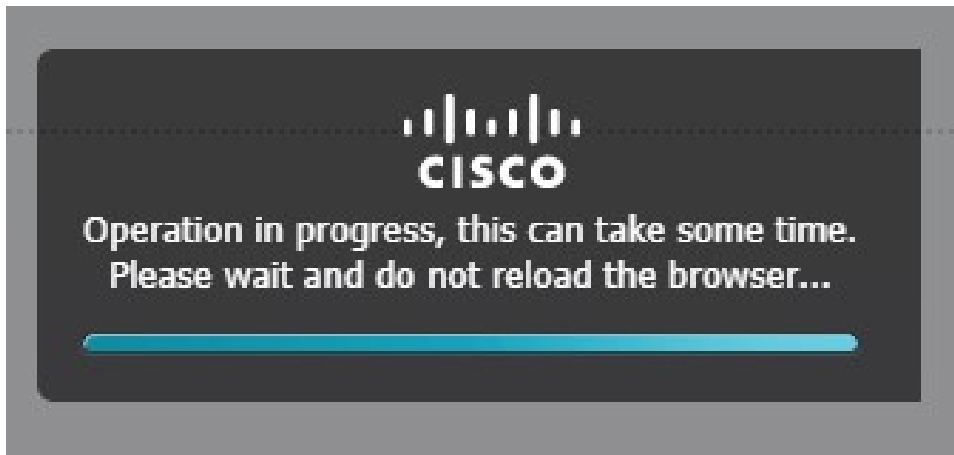
▼ Peripheral Configuration

Device Type	Name	Label	Status	Action
-------------	------	-------	--------	--------

➤ Add Peripheral

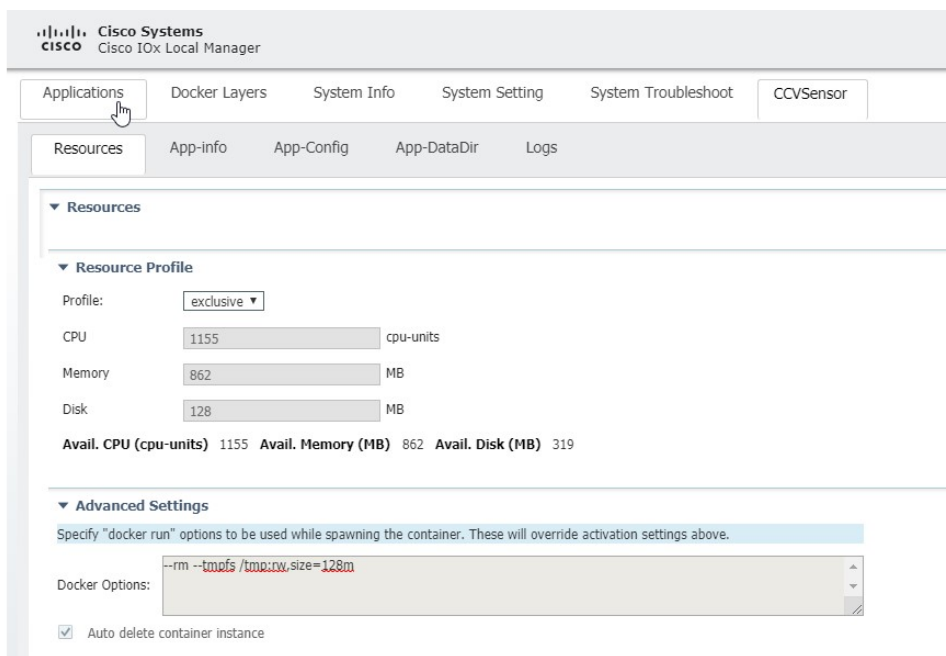
Step 2 The progress window appears. This may take several seconds to finish.

Figure 22: Activation Progress



Step 3 Click on **Applications** to display the app status. Refer to the following:

Figure 23: Applications Resources



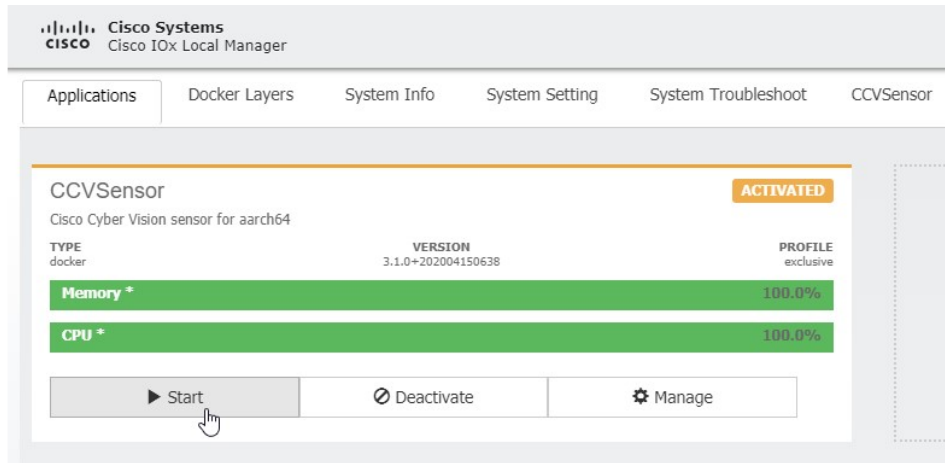
Step 4 The application is activated and needs to be started.

Starting the Application

Procedure

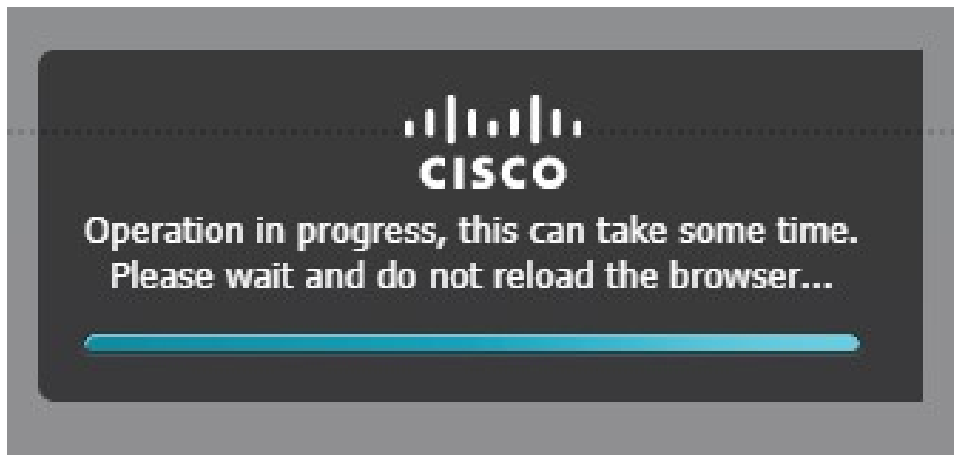
Step 1 Click on **Start**. Refer to the following:

Figure 24: Start Application



Step 2 The progress window appears. This may take several seconds to finish.

Figure 25: Progress Window



Step 3 After some time, the app status will change to running.

Figure 26: Application Running