

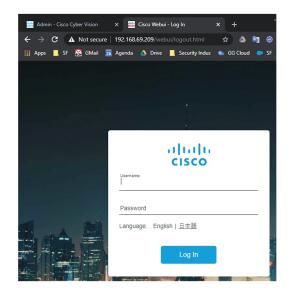
Procedure with the Local Manager

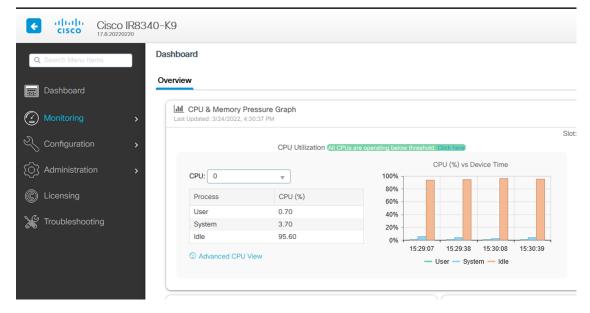
After the Initial configuration, proceed to the steps described in this section.

- Access the IOx Local Manager, on page 1
- Install the sensor virtual application, on page 4
- Configure the sensor virtual application, on page 5
- Generate the provisioning package, on page 12
- Import the provisioning package, on page 15

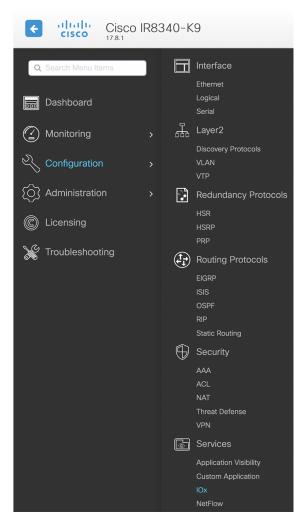
Access the IOx Local Manager

- 1. Open a browser and navigate to the IP address you configured on the interface you are connected to.
- 2. Log in using the Cisco IR8340 admin user account and password.





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



4. Log in using the user account and password.

For best results use a supported browser	
© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its	altalta
affiliates in the U.S. and certain other countries.	cisco

Install the sensor virtual application

Once logged in, the following menu appears:

cisco Cisc	co Systems co IOx Local Manager			
Applications	Docker Layers	System Info	System Setting	System Troubleshoot
		Add New	${\cal C}$ Refresh	

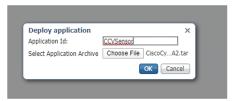
- 1. Click Add New.
- 2. Add an Application id name (e.g. CCVSensor).
- 3. Select the application archive file

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



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

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



The installation takes a few minutes.



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

	Successfully Deployed.	ОК				
cisco S Cisco I	Systems Dx Local Manager					
Applications	Remote Docker Workflow	Docker Layers	System Info	System Setting	System Ti	oubleshoot
sensor		DEPLO	YED			
Cisco Cyber Vision	n sensor for x86-64					
TYPE docker	VERSION 4.1.0+202203111440		COFILE custom			
Memory *		100.	0%		Add New	C Refresh
CPU *		100.	0%			
✓ Activa	te 🔷 Upgrade	💼 Delete				

Configure the sensor virtual application

Procedure

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

cisco Cisco I	Systems IOx Local Manager					
Applications	Remote Docker Workflow	Docker Layers	System Info	System Setting	System Tro	oubleshoot
sensor		DEPI	LOYED			
Cisco Cyber Visio	on sensor for x86-64					
TYPE docker	VERSION 4.1.0+20220311144		PROFILE			
Memory *		10	0.0%		O Add New	C Refresh
CPU *		10	0.0%			
			_			
🖌 Activa	ate 🔷 🔷 Upgrade	💼 Delete				

- **Step 2** Deploy the Resource Profile menu and set the disk size. The procedure differs whether the device has a SSD or not:
 - If the device has a SSD, set the necessary disk size. It should be at least 4GB.

Resources						
 Resource Pro 	file					
Profile	exclusive	~				
CPU	3465	• ct	ou-units 🔵 %			
Memory	4096	MB				
Disk	8192	МВ				
Total CPU (cpu- units)	3465 (100%)	Avail. CPU (cpu- units)	3465 (100%)	Avail. Memory (MB)	4096 <mark>Avail. Disk</mark> (MB)	11808

• If the device has no SSD, set the disk size to 128MB, then deploy the Advanced Settings menu and configure tmpfs by filling the docker options text area with:

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

 Resource Prof 	ile						
Profile	exclusive	~					
CPU	3465		💿 сри	u-units 🔵 %			
Memory	4096		MB				
Disk	128		MB				
Total CPU (cpu- units)	3465 (100%)	Avail. CPU (c units)	pu-	3465 (100%)	Avail. Memory (MB)	4096 Avail. Disk (MB)	1372
 Advanced Set 	tings						
Specify "docker run	" options to be i	used while spawn	ing the	container. The	se will override activat	tion settings above.	
Docker Options:	pfs /tmp:rw,size	=512m					^ ~ ///

Auto delete container instance

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

eth0:

a) Click edit in the eth0 line.

Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit
eth3	Not Configured	none	edit

b) Select the VPG1 interface.

tion		
cion		
Network Config	Description	Action
VPG0	none	edit
Not Configured	none	edit
Not Configured	none	edit
VPG0 VirtualPortGr	oup via intsvc0	
✓ VPG1 VirtualPortGr	oup via intsvc1	
0 0	11 5	
	Network Config VPG0 Not Configured Not Configured VPG0 VirtualPortGr ✓ VPG1 VirtualPortGr mgmt-bridge300 L	Network Config Description VPG0 none Not Configured none Not Configured none

c) Click Interface Setting.

 Network Configur 	ation		
Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit
eth3	Not Configured	none	edit
eth0 Description (optional):	VPG1 VirtualPortGrou	Interface S	Setting
✓ OK X Car	icel		

The Interface Setting window pops up.

- d) Apply the following configurations:
 - Set IPv4 as Static.
 - IP/Mask: 169.254.0.2 / 30
 - Default gateway: 169.254.0.1
 - Disable IPv6.

Interface Set	ting			×
	:	IPv4 Setting		
 Static 	O Dynamic	O Disable		
IP/Mask	169.254.0.2	/ 30]	
DNS				
Default Gateway IP	169.254.0.1			
	:	IPv6 Setting		
) Static	O Dynamic	💽 Disable		
			OK Cancel	

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

You're back to the Network Configuration menu.

I

 Network Configuration 	ation		
Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit
eth3	Not Configured	none	edit
eth0 Description (optional):	VPG1 VirtualPortG	roup via intsv Interface	Setting
✓ OK 🛛 🗶 Car	ncel		

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

A popup that confirms changes appears.



g) Click OK.

Step 4 eth1:

- a) Click edit in the eth1 line.
- b) Select mgmt-bridge300.

Name	Network Config	Description	Action
eth0	VPG0	none	edit
eth1	Not Configured	none	edit
eth3	Not Configured	none	edit

etn1	mgmt-bridge300	L2br AppGigEtr ~	Interface
Description (optional):			

✓ OK X Cancel

- c) Click Interface setting.
- d) Apply the following configurations:
 - Set IPv4 as Static.
 - IP/Mask: 169.254.2.2 / 30
 - Set IPv6 as **Dynamic**.
 - Vlan ID: VLAN in the Cisco IR8340 dedicated to traffic mirroring for the switched ports (e.g. 2340).
 - Set Mirror mode as Enabled.

		IPv4 Setting	
		IPv4 Setting	
 Static 	O Dynamic	○ Disable	
IP/Mask	169.254.2.2 / 30		
DNS			
Default Gateway IP			
		IPv6 Setting	
◯ Static	 Dynamic 	◯ Disable	
		Vian ID	
Vlan ID	2340		
		Mirror Mode	
Mirror Mode	✓ Enabled		

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

Step 5 eth3:

- a) Apply the following configurations to eth3:
 - Select the VPG0 interface.

 Network Configuration 						
Name	Network Config	Description	Action			
eth0	VPG0	none	edit			
eth1	mgmt-bridge300	none	edit			
eth3	Not Configured	none	edit			
eth3 VPG0 VirtualPortGroup via intsvc > Interface Setting Description (optional):						
✓ OK X Cancel						

- Set IPv4 as Static.
- IP/Mask: 169.254.1.2/30.
- Set IPv6 as Dynamic.
- Leave the DNS and default gateway IP fields blank.

I

		IPv4 Setting	
 Static 	O Dynamic	○ Disable	
IP/Mask	169.254.1.2 / 3)	
DNS			
Default Gateway IP			
		IPv6 Setting	
◯ Static	 Dynamic 		

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

✓ Network Configuration					
Name	Network Config	Description	Action		
eth0	VPG1	none	edit		
eth1	mgmt-bridge300	none	edit		
eth3	VPG0	none	edit		

O Add App Network Interface

- **Step 6** If installing a sensor with **Active Discovery**, an additional eth2 interface appears in the Network Configuration menu. To configure this interface:
 - Bind eth2 with mgmt-bridge300.
 - Make sure IPv4 and IPv6 are set to Dynamic.

Step 7 Click the Activate App button.

The operation takes several seconds.



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

The application is activated and needs to be started.

Cisco Systems Cisco IOx Local Manager							
Applications	Remote Docker Workflow	Docker Layers	System				
sensor		ACTIVATE	D				
Cisco Cyber Vision	sensor for x86-64						
TYPE docker	VERSION 4.1.0+202203111440	PROF exclu					
Memory *		100.0%	/o				
CPU *		100.0%	/o				
► Start	Ø Deactivate	🌣 Manage					

Step 9 Click the **Start** button.

The operation takes several seconds.

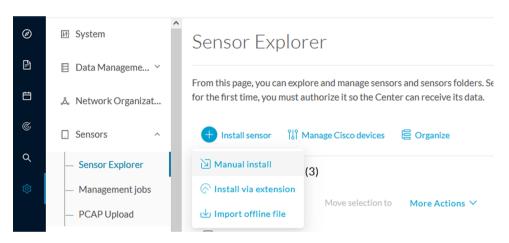


The applications' status changes to RUNNING.

Generate the provisioning package

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

L



The manual install wizard appears.

2. Select Cisco IOx Application and click Next.

Ø	Manual install
Ē	
Ë	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.
۹	◯
\$	O
	◯
	🔿 📼 Sentryo SENSOR5
	🔘 📼 Sentryo SENSOR7
>	Exit Next

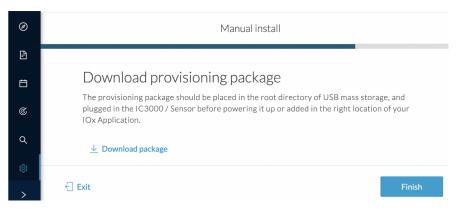
- 3. Fill the fields to configure the sensor provisioning package:
 - The serial number of the hardware.
 - Center IP: leave blank.
 - Gateway: add if necessary.
 - Optionally, select a capture mode.
 - Optionally, select RSPAN (only with Catalyst 9x00 and if using ERSPAN is not possible).

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 relevan	it flows
 All: analyze all the flows 	
$\bigcirc~$ Industrial only: analyze industrial flows	
O Custom: set your filter using a packet fil	ter in tcpdump-compatible syntax
Monitor session type	
• ERSPAN: recommended choice for all device	ces
O RSPAN: use it only with Catalyst 9X00 a	nd when using ERSPAN is not possible

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



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

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

The sensor status will switch from Disconnected to Connected.

Label	IP Address	Version	Location	Health status 🗊 🔻	Processing status 🕕	Active Discovery	Uptime
•			0128	Descended 1	Descended 1		10.0
•			*****				110
□ 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.

Applications	Docker Layers	System Info	System Setting
CCVSensor Cisco Cyber Vision	sensor for aarch64		RUNNING
TYPE docker		ERSION 202004150638	PROFILE exclusive
Memory *			100.0%
CPU *			100.0%
Stop	о 🌣 м	anage 📠	

2. Navigate to App-DataDir.

Applications	Docker Layers	System Info	System S	Setting	Syste
Resources	App-info Ap	op-Config App	-DataDir	Logs	
 Resources 					
▼ Resource P	Profile				
Profile:	exclusive 🔻				
CPU	1155	cpu-u	nits		
Memory	862	MB			
Disk	128	MB			
	ou-units) 1155 Avai				

3. Click Upload.

Cisco Systems Cisco IOx Local Manager								
Applications	Docker Layers	System I	nfo	System S	etting	System	Troubleshoot	CCVSensor
Resources	App-info	App-Config	App-Da	ataDir	Logs			
Current Location:	./							
Name			Туре				Size	
/								
O Upload	A Home							

- **4.** Choose the provisioning package downloaded (i.e. "sbs-sensor-config-FCW23500HDC.zip"), and add the exact file name in the path field (i.e. "sbs-sensor-config-FCW23500HDC.zip").
- 5. Click OK.



6. After a few seconds, the sensor appears as Connected in Cisco Cyber Vision.

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