Cisco IC3000 Industrial Compute Gateway with Cisco Cyber Vision

First Published: 2019-12-12

Last Modified: 2019-12-12

Cisco IC3000 Industrial Compute Gateway with Cisco Cyber Vision

The purpose of this document is to describe the procedures to successfully deploy the Cisco Cyber Vision Application on the IC3000.

This guide only discusses the interaction of the Cisco Cyber Vision Application on the IC3000. You must have a working knowledge of installation and deployment of the device, which can be found here:

https://www.cisco.com/c/en/us/support/routers/3000-series-industrial-compute-gateways/tsd-products-support-series-home.html

Introduction

The IC3000 Industrial Compute Gateway (IC3000) is an edge computing platform which extends the cloud computing paradigm to the edge of the network. Instead of hosting applications in a remote data center, applications can now be hosted on the edge itself. Imagine, if we can host specific applications in the field close to the sensors, meters or the things. whatever may be the IOT use case, IC3000 serves the purpose by allowing us to deploy applications that need more cores and memory.

The IC3000 is a mid-range, low-power, fanless, edge server ruggedized for Industrial Applications. It is powered by a 4 core 1.2GHz Intel Rangeley CPU with 8 GB of 1333MHz DDR3 memory, and a 100GB mSATA drive (internal). For connectivity it supports 2x1GbE SFP and 2x10/100/1000Base-T with a management port.



Note

Examples shown in this document use IP addresses that are from a lab environment and should not be used on a typical customer installation.



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Unboxing, Installing and Connecting to the IC3000 Device

Unboxing the IC3000

Complete details for the hardware installation of the product are covered in the IC3000 Hardware Configuration Guide. The following steps are a high level overview.

Installing the IC3000

- 1. Review the general description of the unit in the Product Overview section of the hardware installation guide.
- 2. Check the Equipment, Tools, and Connections section of the hardware installation guide to ensure you have everything you need for the installation.
- **3.** Review the procedures for Mounting, Grounding, Connecting to DC Power and Connecting to the IC3000 in the hardware installation guide.
- 4. If you are installing the device in a Hazloc location, follow the printed instructions that came inside the box with the device.
- 5. Power on the device.

Reset Button Options

The device can be returned to the original factory configuration by using the reset button. The reset button is a small button accessed through a pinhole located on the front of the device. For the location, see the IC3000 Hardware Configuration Guide .

The reset button options are:

- Press 10 to 15 seconds Device is reloaded.
- Press 30 to 35 seconds All user configurations (apps, network details) are removed and device is reloaded.
- Press 60 to 65 seconds All user configurations are removed, all images are cleared except for the factory image, and the device is reloaded with the factory image.

Cisco Cyber Vision Sensor Application

The IC3000 can be ordered with the Cisco Cyber Vision sensor application, which will come pre-installed at manufacturing. The Cisco Cyber Vision sensor app allows traffic from a network to be captured in offline or online mode. This captured data can be viewed from Cisco Cyber Vision. For more information on how to explore the captured data and to navigate the Cisco Cyber Vision GUI please refer to the Cisco Cyber Vision GUI User Guide.

Note: The IC3000 contains 4 independent data capture ports (2 RJ45 copper ports & 2 SFP fiber ports) in SPAN mode, each of which can be connected to an on-site switch. The IC3000's data capture ports are to be connected to switches with SPAN configured.

Cyber Vision Sensor Application in Offline Mode

Cisco Cyber Vision sensor offline mode allows SPAN traffic to be captured from the 4 data ports onto a USB stick. This offline traffic can then be manually added to Cisco Cyber Vision, to provide visibility to the

collected network traffic. To collect SPAN traffic onto a USB, and to manually add it to the CVC, follow the instructions below:

Procedure

Step 1 Step 2	Obtain Plug a	Obtain an IC3000 with Cyber Vision sensor app pre-installed at manufacturing. Plug a USB device in USB slot 1 of the IC3000.						
	Note	Ext2/Ext3/Ext4 and FAT32 formats are supported.						
Step 3	Power	on the unit.						
Step 4	Connee	et any of the 4 data ports to on-site switches you wish to capture SPAN traffic.						
Step 5	Allow	for the SPAN traffic to be collected for a day or two						
Step 6	Unplug	the USB, connect it to a PC and verify that a .dat file is present.						
	Note	Hot plug of a USB device is not supported. In the case where a USB is unplugged, the plugged back into the USB slot 1, the device will not recognize the USB. To resume offline mode capture, the						

Note A new offline capture session will create a new .dat file. See the following graphic.

USB needs to be plugged back in and the device must be rebooted (powered OFF and ON).

Figure 1: Data File on a USB

📼 offline-data-20191106-000608.dat	Yesterday at 1:09 AM	30 KB	Sc
sensor.log	Yesterday at 12:06 AM	230 bytes	Lo
stats.log	Yesterday at 1:09 AM	526 KB	Lo

Step 7 Upload the .dat file to CVC by going to CVC home page > System Administration (cog icon on the top right) > Sensors > Import Offline File.

Figure 2: Import Offline Capture

alialia cisco	CYBER VISION									0	<u>~</u> 8 ~
ø		C System	Se								
		Sensors Management Capture	Fro Sen can	Import an offline capture	file. To capture traffic or	a sensor in offline mode, plug an	USB drive on	ng cor	packages to deploy Cisco C nnects for the first time, you	yber Vision on remo I must authorize it s	ote sensors. o the Center
0		🛎 Users	IMF sen	its Offline USB port. Unpl Capture startir You can	ug the USB drive to stop ng date is embeddo optionally specify a date	the capture. ed in the upload offline of and time to be used to rewrite.	data file.	led	manually. To complete the	installation click the	"Install
Q		API	r	SET DATE AI	ND TIME	KEEP DEFAULT, IMPC	ORT FILE		Processing status	Capture Mode [©]	Uptime
		of LDAP Settings	•				Cance	a as		All	N/A
		@ pxGrid	► FO	C2227Y307	192.168.69.31	N/A	Disconnecto	nd © Si		All	N/A
			► FCI	H2314Y166					Waiting for data	All	7d 2h 4 1m 55s
			► FCI	H2309Y00U					Waiting for data	All	19d 22 h 23m 4s
			♦ OF	FLINE SENSOR	N/A	N/A				N/A	N/A
			► FCI	H2307Y02C	192.168.69.44				Waiting for data	All	4d 22h 17m 3 2s
								•	INSTALL SENSOR MANUAL		

Step 8 If desired, you can manually change the date and time for the offline data file.

Cyber Vision Sensor Application in Online Mode

Before you begin

Cyber Vision sensor online mode allows SPAN traffic to be sent continuously to the Cisco Cyber Vision's Collection Network for real-time visualization of industrial networks. To add a device and pass SPAN traffic to the Collection Network follow the instructions below:

Procedure

Step 1 Login to Cisco Cyber Vision.

Figure 3: Cisco Cyber Vision Login Window



Step 2 Go to the System administration tab by clicking the cog icon on the top right corner. See the following graphic.



Figure 4: System Administration Window



Figure 5: Install Sensor Manually

•	CYBER VISION							© 12	8 -
		System Sensors Management	Sensors From this page, you can mana	ige sensors in online an	d offline modes and gen	erate provisioning pac	kages to deploy Cisco C	yber Vision on remote	sensors.
		Capture	can receive its data.	and securely rebooted	, snut down, and erased.	when a sensor conne	cts for the first time, you	i must authorize it so ti	ne Center
		Lusers Events API	IMPORTANT: the Cisco IC30 sensor manually [®] button belo	00 Industrial Compute	Gateway device should	always be installed ma	anually. To complete the	installation click the "li	nstall
			Name	IP	Version	Status	Processing status	Capture Mode [©]	Uptime
		Clicense	• FCH2307Y02W	192.168.69.37	3.0.0+20191021210	O Connected	Waiting for data	All	6d 1h 1 6m 43s
		@ pxGrid	▶ FCH2314Y166	192.168.69.50	3.0.0+20191021210	O Connected	Waiting for data	All	8d 50m 15s
			▶ FCH2309Y00U	192.168.69.27	3.0.0+20191021210	10 Connected	Waiting for data	All	20d 20 h 31m 24s
			OFFLINE SENSOR	N/A	N/A	Unknown ØSSH	Not enrolled	N/A	N/A
			▶ FCH2307Y02C	192.168.69.44	3.0.0+20191021210	IQ Connected	Waiting for data	All	5d 20h 25m 5 2s
						+ IN	STALL SENSOR MANUAL		LINE FILE



Select Cisco IC3000 as hardware model from the drop-down list.

Figure 6: Select Hardware Model

uluilu cisco	CYBER VISION								0 2	8.
		C System	Carro							
		⊖ Sensors	Manual sensor instal	ation				Cisco Cy	ber Vision on remote s	ensors.
		 Manaj Captu 	The manual sensor installation	n is provided to install Ci	isco IC3000 Industrial	Compute Gateway and sensors tha	t are not allowed to access	ime, you	must authorize it so th	e Center
		🏝 Users	the Center's DHCP server for package.	automatic configuration	n. Please fill the fields b	elow to configure your sensor and	generate a provisioning	ete the i	nstallation click the "In	stall
		🍽 Events	(1) This package should be place	d in the root directory of U	JSB mass storage, and pl	ugged in the IC30007 Sensor before p	oowering it up.			
		API	Select an hardware model:	CISCO IC 3000				tatus	Capture Mode [€]	Uptime
		& License		Sentryo SENSORS						
		S LDAP Se		Sentryo SENSOR5						
		₩ pxGrid		Sentryo SENSOR7					All	
									All	h 36m 4s
			► OFFLI	NE SENSOR N	1/A	N/A Unknown	Create Sensor Cancel		N/A	N/A
			► FCH2:	807Y02C 1	92.168.69.44		ed Waiting for dat		All	
							+INSTALL SENSOR			

Step 5 Fill out the Cisco IC3000 and Sensor configuration fields. Refer to the **Filled Out Form** and the **Sensor Configuration Window**.

Caution: Make sure the network information entered is correct and will not result in a network conflict. Any mistake will require a device reset to be performed, resulting in the device returning to factory defaults. This will lead to a complete deletion of the inner system, which will require a special procedure to install the Cyber Vision Application manually via Local Manager. Refer to Installing the Cyber Vision Sensor Application Using Local Manager after a Configuration Reset, on page 10 for more details if a reset must be performed on the IC3000 device. Refer to Reset Button Options, on page 2 for details.

Figure 7: Filled Out Form

Manual sensor installation	
The manual sensor installation is provided to install Cisco IC3000 Inc the Center's DHCP server for automatic configuration. Please fill the package.	dustrial Compute Gateway and sensors that are not allowed to access fields below to configure your sensor and generate a provisioning
 This package should be placed in the root directory of USB mass storag 	e, and plugged in the IC3000 / Sensor before powering it up.
Select an hardware model: Cisco IC3000 🔻	
Cisco IC3000 configuration	
Serial number:*	Host management IP address: *
FCH2314Y166	10.10.10.7
Host management Netmask: * Like 255.255.255.0 or 255.255.0.0	Host management Gateway:
255.255.255.0	10.10.10.1
Local manager user name:	
admin	

Note: The serial number for the IC3000 device can be found in the front view of the chassis. See **Serial Number Location**. The Local Manager default credentials are (username:admin/password:cisco123) for a device that was shipped from the factory. Enter "admin" for local manager username field.

Figure 8: Serial Number Location



Note The Cisco IC3000 configuration is to be able to access Local Manager for troubleshooting purposes.

Figure 9: Sensor Configuration Window

Sensor configuration	
IP address:	Subnet Mask: Like 24, 16 or 8
192.168.68.77	16
Center IP:	Gateway:
Optional, leave blank to use current Center IP address	Optional
Capture mode:	
All: analyze all the flows	
Optimal (Default): analyze the most relevant flows	
O Industrial only: analyze industrial flows	
O Custom: you set your filter using a packet filter in tcpdump-	compatible syntax

Step 6 Click **Create Sensor**. Once created, the sensor will appear in the sensor list with "New" as its status. Expand the sensor and click the **Get Provisioning Package** icon to download the sensor provisioning zip file. See the following graphic.

Figure 10: Get Provisioning Window

▼ FCH23I4Y166	192.168.69.77	N/A	Ν	√ew ⊘SSH	Not enroll	ed	Optimal	N/A
S/N: FCH23I4Y166								
IP address: 192.168	.69.77		Ĥ		*	,C	Ċ	2
Status: New			Remove	Erase	Get Provisioni	Capture Mode	Shutdown	Reboot
Processing status: No	ot enrolled							
Capture mode: Optim	al							

Step 7 The Get Provisioning Package window opens. You are required to create a password.

Figure 11: Get Provisioning Package

ahah cisco	CYBER VISION						🛆 84 dayse Evalu	remaining	<u>d</u> 😮 -
0		 Ø System Data management 	Serisors	elvece			Cisco Cyber Vision on ro rize it so the Center can	emote sensors. Sensors car receive its data.	also be
		 Gensors Management 	IMP To generate the provisioning pac belo IMPORTANT: the package is a .21p file	LCABE kage, please create your C a. You should unzip it the root dim	isco IC3000 local manager participation of USB mass storage.	assword.	ete the installation click	the "Install sensor manual	y" button
Q		Capture Users Events	Create password N Password must:				Processing status	Capture Mode [©]	Uptime N/A
		API	Be at teast of characters using Not be based upon a dictional Not be a combination of diction Not be composed of common Not be a combination of common	ry word onary words string patterns like "qwerty" non string patterns and dicti	"asdfgh", etc.		Waiting for data	All	3d 2h 5 1m 53s
		OC LDAP Settings	Confirm password						
			Uptime: 3d 2h 51m 53s	_		Ok Cancel	Get ProvisionL Caper	are Mode	C Reboot
			Start recording sensor						
			• FCH2309Y00U 1	92.168.69.36	3.0.0+201911151747		Waiting for data	All	3d 3h 8 m 3s
							+INSTALL SENSOR M		

- **Step 8** Enter a new password. The default password for the admin account will be replaced with this new password. In order to access the Local Manager, you will need to use this new password for the "admin" account. Make sure to keep this information stored and secured. Follow these password rules:
 - Minimum length = 6
 - Must not be based upon a dictionary word
 - · Must not be a combination of dictionary words
 - Must not be composed of common string patterns like "qwerty", "asdfgh" etc...
 - Must not be a combination of common string patterns and dictionary words
- **Step 9** Click **Ok**. A serialNumber.zip file will be generated and downloaded on the laptop. Unzip the .zip file and copy the serialNumber folder to the root directory of the USB.

Figure 12: Example Zip File

V E FCH2314Y166
device_config.cfg
🔻 🛅 appconfigs
Cybervision-sensor-config.zip

Note These next steps are performed on the IC3000 with the Sensor Application installed from manufacturing.

L

- **Step 10** Prepare your IC3000 by making sure you have proper power, console, and data connections available.
- **Step 11** Connect the USB stick you have prepared to USB slot 2, and plug the MGMT cable into the Collection Network. Also, connect any on-site switches that have SPAN configured to data ports 1 4 to pass SPAN traffic. See the following example setup.

Figure 13: Example of an IC3000 Setup



- **Step 12** Power on the device. Once the device powers on the configurations on the USB are copied to the device and application. Cisco Cyber Vision sensor will register to Cisco Cyber Vision. Wait up to 5 min for the Cisco Cyber Vision sensor app to register.
- **Step 13** The Cyber Vision Sensor should show as "connected" under the Sensor status. The IC3000 status should quickly change to connected. The provisioning package has been installed successfully on the IC3000 and traffic starts to appear in Cisco Cyber Vision.

Figure 14: Cyber Vision Sensors

altada cisco	CYBER VISION							© 14	8.
Ø		2 System	Sensors						
ĥ		 Sensors Management 	From this page, you can mana Sensors can also be remotely	ge sensors in online an and securely rebooted	d offline modes and generate , shut down, and erased. Whe	e provisioning pacl en a sensor connec	ages to deploy Cisco Cy ts for the first time, you	ber Vision on remote must authorize it so th	sensors. ne Center
		 Capture 	can receive its data.						
۲		🛎 Users	IMPORTANT: the Cisco IC30 sensor manually" button belo	00 Industrial Compute w.	Gateway device should alwa	iys be installed ma	nually. To complete the i	nstallation click the "Ir	nstall
Q		I■ Events							
		API	Name	IP	Version Sta	atus	Processing status	Capture Mode [©]	Uptime
		a License	N ECH2207V02W	1021606027	200+201910212100 0~	anartad	Waiting for data	All	6d 3h 2
		Contraction Contractic Con	FCH2307T02W	172.100.07.37	3.0.0+201710212100 00	Intected	Watting for data	Aii	3m 53s
		🏶 pxGrid	▶ FCH2314Y166	192.168.69.50	3.0.0+201910212100 Cor	nnected	Normally processing	All	8d 2h 5 7m 25s
			▶ FCH2309Y00U	192.168.69.27	3.0.0+201910212100 Cor	nnected	Waiting for data	All	20d 22 h 38m 34s
			OFFLINE SENSOR	N/A	N/A Uni	known ØSSH	Not enrolled	N/A	N/A
			► FCH2307Y02C	192.168.69.44	3.0.0+201910212100 Cor	nnected	Pending data	All	5d 22h 33m 2s
						+INS	TALL SENSOR MANUALI	Y IMPORT OFFI	INE FILE
	<								

Installing the Cyber Vision Sensor Application Using Local Manager after a Configuration Reset

Performing a reset results in a factory default of the device. When this occurs, the Cisco Cyber Vision Sensor Application will be deleted and needs to be installed by using the LM. Refer to Reset Button Options, on page 2 for details.

To re-install the application, perform the following steps:

Procedure

Step 1	Perform reset. Press the physical reset button on the IC3000 device for 30 - 35 seconds and make sure the MGMT cable is not connected.
Step 2	Follow steps 1- 8 from the Cyber Vision Sensor Application in Online Mode, on page 4 section. Also follow step 10, where you connect the USB stick in USB slot 2.
	Note : Make sure any old sensor installations using this IC3000 device have been erased. Go to Cisco Cyber Vision > System Administration > Sensors > Management to confirm the IC3000 serial number does not appear.
Step 3	Access the LM GUI using the IP address configured in the Host Management IP address field found in step 5 under the Cyber Vision Sensor Application in Online Mode, on page 4 section. Type the following URL in a web browser: https://< <i>Host-MGMT-IP-Address</i> >:8443 Make sure your MGMT cable has access to the Host Management Subnet.
Step 4	Login to the LM GUI using the credentials admin/newPassword, where new password is the password set in step 7 under the Cyber Vision Sensor Application in Online Mode, on page 4 section.
Step 5	Download the latest version of signed Cisco Cyber Vision's Sensor Application from the Cisco download site. Go to Applications > Add New > Browse > OK . See the following graphic.

Figure 15: Add New Application

cisco Cisco IO	/stems x Local Manager							Helio, admin Log Out About
Applications	Remote Docker Workflow	Docker Layers	System Info	System Setting	System Troubleshoot	Device Config	User Config	
	C Add Now							
	• Add New 27 Keiresi							
				Deploy application Application Id:	CiscoCyberVision			
				Select Application Archive	Browse No filelected.			
					_			

Step 6 Press Activate on the Cisco Cyber Vision Sensor Application.

Figure 16: Activate the Application



Step 7 Add the Network Configurations. Click **Edit** on each interface. Each interface name should be mapped exactly in this format, eth0 > iox-bridge0, eth1 > int1, eth2 > int2, eth3 > int3, and eth4 > int4.

 Network Configurat 	ion		
Name	Network Config	Description	Action
eth0	iox-bridge0	none	edit
eth1	int1	none	edit
eth2	int2	none	edit
eth3	int3	none	edit
eth4	int4	none	edit
eth1 [Description (optional): [int1 Data interface via int1	Interface Setting	
✓ OK X Cance	el		

Figure 17: Network Configuration

Step 8Next, eth1 - eth4 should be configured with Mirror mode Enabled. To enable Mirror mode, go to Edit >
Interface Setting > Enable > OK for eth1 - eth4.

Figure 18: Interface Setting

Interface Setti	ng		×					
	IPv4 Setting							
◯ Static	 Dynamic 	◯ Disable						
		IPv6 Setting						
◯ Static	 Dynamic 	◯ Disable						
DHCP Client ID								
		Mirror Mode						
Mirror Mode	Enabled							
			OK Cancel					

Step 9 Add the Peripheral Configuration. Go to **Peripheral Configuration > edit > Port:1usb1 > OK**.

Figure 19: Peripheral Configuration

 Peripheral Col 	nfiguration			
Device Type	Name	Label	Status	Action
USB_port		USB1	Not present	edit
Device Type	LICP port	_		
Port:1usb1		<u> </u>		
Port:1usb1 Label:	USB1	<u>_</u>		
 Port:1usb1 Label: pid: 	USB1 Not available			

The following shows an example of the Added Peripheral Configuration.

Figure 20: Added Peripheral Configuration

Peripheral Configuration								
Device Type	Name	Label	Status	Action				
USB_port	Port:1usb1	USB1	Present	edit				
• Add Peripheral								

Step 10From the Cisco Cyber Vision Resources Tab, click Activate App to activate the application.Figure 21: Activate Application

plications	Remote Docker Workflow	Docker Layers	System Info	System Setting	Syster	m Troubleshoot	Device	Config	User Config	CiscoCyberVision			
Resources	App-info App-Config	App-DataDir	Logs										
Resources												🖌 Activate A	
• Resource I	Profile				,	 Network Configu 	uration						
Profile:	exclusive 💌					Name	,	Vetwork Config		Description	Action		
CPU	10260	cpu-units				eth0	i	ox-nat0		none	edit		
Memory	6400	MB				eth1 Not Configur		Not Configured		none			
Disk	10	MB			eth2 eth3		Not Configured			none	edit	edit	
Vcpu	4						1	Not Configured		none edit		edit	
Avail. CPU (cp	ou-units) 10260 Avail. Memory	(MB) 6400 Avail. Di	sk (MB) 81010			eth4 Not Configured							
						eth1	lint1	Data interface	uia inti	Interface Settion			
						Description (ontional):		Data internate	416 ITL1	Interface occurry			
						beachpaon (opconar).	·						
						√ок ×с	Cancel						
					,	 Peripheral Confi 	iguration						
						Device Type	Name		Label	Status		Action	
						USB_port	Port:1u	ısb1	USB1	Present		edit	
						O Add Peripheral							
						• Add Peripheral							

Step 11 The next step is to start up the application. Go to **Applications > Start App**.

Figure 22: Start Application

cisco _{Cis}	co Systems co IOx Local Manager								Hello, admin	Log Out	About
Application	s Remote Docker Workflow	Docker Layers	System Info	System Setting	System Troubleshoot	Device Config	User Config	CiscoCyberVision			
CiscoCi	ther lision	ACTIVATED									
Cyber Vision	Sensor Image for IC3000										
VTT	VERSION 1.0	PROFILE exclusive									
Memory	•	100.0%		O Add New	C Refresh						
CPU *		100.0%									
▶ 5	tart Ø Deactivate	🌣 Manage									

- **Step 12** The application is now in a running state.
- **Step 13** Plug in the MGMT cable so that it has access to the Collection Network. The Cyber Vision sensor should show as "connected" under the Sensor status.

Figure 23: Cyber Vision Sensors

-ilialia cisco	CYBER VISION							© 12	8 ~
() 19 10 10 10 10 10 10 10 10 10 10 10 10 10	Explore Reports Events Monitor	System System Source Management Capture Users Sustain Events	Sensors From this page, you can manay Sensors can also be remotely a can receive its data. IMPORTANT: the Cisco IC300 sensor manually" button below	te sensors in online anc ind securely rebooted, 0 Industrial Compute 0 v.	l offline modes and gene shut down, and erased. ¹ Gateway device should a	erate provisioning pack When a sensor connec always be installed mar	ages to deploy Cisco Cy ts for the first time, you uually. To complete the in	ber Vision on remote s must authorize it so th nstallation click the "In	ensors. e Center stall
3	Search	 ▲ API ♣ License ✿ LDAP Settings ♥ pxGrid 	Name	IP 192.168.69.37 192.168.69.50	Version 3.0.0+201910212100 3.0.0+201910212100	Status Connected Connected	Processing status Walting for data Normally processing	Capture Mode [©] All All	Uptime 6d 3h 2 3m 53s 8d 2h 5 7m 25s
			FCH2309Y00U OFFLINE SENSOR FCH2307Y02C	192.168.69.27 N/A 192.168.69.44	3.0.0+201910212100 N/A 3.0.0+201910212100) Connected Unknown ©SSH) Connected	Waiting for data Not enrolled Pending data TATL SENSCIP MANULATI		20d 22 h 38m 34s N/A 5d 22h 33m 2s
						+ INS	TALL SENSOR MANUALL		INEFILE

Step 14 Connect any on-site switches that have SPAN configured to data ports 1-4 to begin passing traffic to the Cisco Cyber Vision

 $^{\odot}$ 2019–2021 Cisco Systems, Inc. All rights reserved.