

Upgrade procedures

- Upgrade through the Cisco Cyber Vision sensor management extension, on page 1
- Upgrade through the IOx Local Manager, on page 4

Upgrade through the Cisco Cyber Vision sensor management extension

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

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

Update the sensor management extension

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

Procedure

- **Step 1** Retrieve the sensor management extension file (i.e. CiscoCyberVision-sensor-management-<version>.ext) on cisco.com.
- **Step 2** In Cisco Cyber Vision, navigate to Admin > Extensions.
- **Step 3** Click **Update** to browse the new version of the extension file.

				<u>~</u> 8
. Sensors	^	Extensions		
 Sensor Explore Management j PCAP Upload 		From this page, you can manage Cyber Visio Vision Center which provide more features detection engines, or integrations with exte	, such as the management of ne	
Q Active Discove	ery ~	/ Update		
冬 Users	~	Uploading Please do not quit or refresh th	e page.	
⊂ ⊑vents		Installed extensions		
o ^g API	~	Name	Version	Actions
무 License		Cyber Vision sensor management	4.1.2	⊖ Update 📋 Remove

Update the sensors

	nstall sensor, the	to-date have their version displayed in red. en Update Cisco devices . Sensor Explorer
elisto Cisco	∄ System	
 CISCO Ø B 		Sensor Explorer
		Sensor Explorer
F F		
	🗄 Data Management 🛛 🗡	
Ë "s	δ。 Network Organization	From this page, you can explore and manage sensors and sensors folders. Sensors can be remotely and securel time, you must authorize it so the Center can receive its data.
¢.	. Sensors	🕂 Install sensor 👫 Manage Cisco devices 🕫 Organize
۹	 — Sensor Explorer 	Folders and ser
¢	 Management jobs 	B Manage credentials
	— PCAP Upload	Filter 0 Selected Move selection to More Actions Y
te	& Active Discovery 🗸	Label IP Address Version Location Health status
	à lleare 🗸	EVEN EVEN EVEN
1	à Users 🗸 🗸	FoldER2 Paris

Step 1

📼 IC3000

📼 IE3400

Step 2

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

4.1.1+202205161124

4.1.2+202207190948

Connected

Connected

I

192.168.49.23

192.168.49.21

o^g API

'⊒ License

			UPDATE CISCO DEVICES		×
	ere is a new ve			3000) are concerned here. They appear installed extension. Please select the	0
	Label 🔷	IP	Version	Target	
	IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846	

Step 3 Select the sensors you want to update.

		UPDATE CISCO DEVICES		×
nere is a new ve			3000) are concerned here. They appear installed extension. Please select the	
ee apaaro.				
Label 🔦	IP	Version	Target	

Step 4 Click Update.

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

uluilu cisco					<u>⊢</u> ⊗ √	
Ø	& Network Organization	Management jobs				
Ē	Sensors ^	Jobs execution for sensor management tasks.				
¢	 Sensor Explorer 			< 1	$>$ 20/page \vee	
	 Management jobs 	Jobs	Steps	Date	Duration	
۹	— PCAP Upload					
¢	Q Active Discovery ~	Batch update (FCW2445P6X5)	\bigcirc	Oct 13, 2022 5:19:35 PM	In progress	

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

uluulu cisco					<u>⊬</u> 8×
Ø	& Network Organization	Management jobs			
Ê	Sensors ^	Jobs execution for sensor managem	ent tasks.		
	 — Sensor Explorer 			< 1	20/page ∨
¢	— Management jobs	Jobs	Steps	Date	Duration
Q	— PCAP Upload	JODS	Steps	Date	Duration
¢	Q Active Discovery ×	Batch update (FCW2445P6X5)	\checkmark	Oct 13, 2022 5:19:35 PM	6m 45s

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

Batch update (FOC2401V07N, FOC2412V0DL, FOC2431V08E, FOC2330V0TJ, FOC2334V00D, FOC2431V0A0, FOC2413V0X3) Update					
Batch update (FJ	Error				
Single deploymeı (FCH2312Y03Z)	Fatal error: at least one device failed				
	Logs				
Batch update (FC	x FOC2413V0X3: failed: job with status FAILED has error: Error while				
Single redeploym (FOC2334V045)	<pre>changing app state:Cannot start while in DEPLOYED state. Allowed operations are ['activate', 'upgrade', 'undeploy', 'download_data']</pre>				
Single redeploym (FOC2334V00D	 F0C2401V07N: succeeded to update F0C2412V0DL: failed: job with status FAILED has error: Error while changing app state:Cannot start while 				
Single redeploym (FCW2435P3KV	<pre>in DEPLOYED state. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate']</pre>				
Single redeploym (FOC2413V0X3)	 FOC2330V07J: succeeded to update x FOC2334V00D: failed: job with status FAILED has error: Error while changing app state:Cannot start while 				
Single redeploym (FOC2412V0DL)	<pre>in DEPLOYED state. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate'] ✓ F0C2431V0A0: succeeded to update</pre>				
Single redeploym	HIL .				

Upgrade through the IOx Local Manager

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



Note In the case of Cisco Cyber Vision upgrade for an IR8340 from a release 4.1.2 or lower to a release 4.1.3, the update will fail due to the addition of the RSPAN option. The sensor application must be removed and deployed again.

In the example below, the sensor is upgraded from Cisco Cyber Vision version 3.2.2 to version 3.2.3.

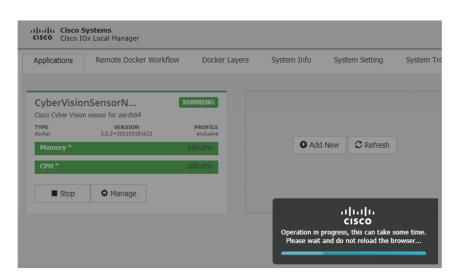
<u>⊮</u> ⊗. cisco E Systen Sensors ß Data management From this page, you can manage sensors in online and offline modes and generate provisioning packages to deploy Cisco Cyber Vision on remote sensors. Sensors can also be remotely and securely rebooted, shut down, and erased. When a sensor connects for the first time, you must authorize it so the Center can receive its data. Ē Sensors ~ Sensors Name IP Version Status Processing status Active Discovery status Capture Mode [©] Uptime Capture 4d 1h 3 2m 47s ▼ FOC2334V00H 192.168.69.20 3.2.2+202103181619 Con Per All • A Users S/N:F0C2334V00H Name:F0C2334V00H IP address:192.168.69.20 Version:3.2.2.242013181619 System date(UTC):Monday, May 31, 2021 9:17 AM Status: Commette Processing status: rending data Active discovery: Unsublate Dendorment: Manual Events & API ~ ₩ License Get Provisioni... Capture Mode Û A LDAP Settings Deployment: Manual Uptime: 4d 1h 32m 47s Capture mode: All • Start recording sensor Lift Go to statistics ⊘ Snort BB Extensions • FCH2312Y047 192.168.70.20 3.2.2+202103181753 Connected Pending data All 3m 27s LUPDATE CISCO DEVICES + DEPLOY CISCO DEVICE + INSTALL SENSOR MANUALLY

Figure 1: The sensor in version 3.2.2 in the Sensors administration page of Cisco Cyber Vision

- 1. Access the IOx Local Manager.
- 2. Stop the application.

Cisco Cis Cisco 17.3.2	co IE-340	0-8T2S				
Q Search Menu Items		Configuration * >	Services > IOx			
📰 Dashboard		cisco Cisco I	Systems Dx Local Manager			
Monitoring	>	Applications	Remote Docker Workflow	Docker Layers	System Info	Syster
Configuration	>					
() Administration	>	Cisco Cyber Visio	n sensor for aarch64	RUNNING		
C Licensing		TYPE docker Memory *	VERSION 3.2.2+202103181622	PROFILE exclusive	• Add	New
X Troubleshooting		CPU *		100.0%		
		Stop	🌣 Manage			

The operation takes a few moments.



The application status switches to STOPPED.

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

III System		Sensors							
Data managemen	t	From this page, you can manage securely rebooted, shut down, a						ors. Sensors can also be remo	tely and
Sensors	^								
- Sensors		Name	IP	Version	Status	Processing status	Active Discove	ry status Capture Mode €	Uptime
 Capture 		▼ FOC2334V00H	192.168.69.20	3.2.2+202103181619	Disconnected @SSH	Disconnected	Unavailable	All	N/A
A Users	ř	S/N: F0C2334V00H							
S Events		Name: FOC2334V00H							
ø ^g API	~	Version: 3.2.2+20210318 System date (UTC): Monda	1619	20. 44					
₩ License		Status: Disconnected Processing status: Disconnected		20 API				Remove Get Provisioni	Capture Mode
条 LDAP Settings		Active discovery: Unavailab Deployment: Manual	le						
⊖ Snort		Capture mode: All							
≪ Integrations	~	▶ FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data		All	10m
B Extensions		FCH23121047	172.100./0.20	3.2.2+202103181/53	connected	Penoing data	onavallable	All	10m
				🕹 UPDATE C	ISCO DEVICES	DEPLOY CISCO DEVICE	+ INSTALL SENSO	R MANUALLY	OFFLINE FILE

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

The application status moves to DEPLOYED.

4. Click Upgrade.

CyberVisio Cisco Cyber Visio	DEPLOYED	
TYPE docker	VERSION 3.2.2+202103181622	PROFILE exclusive
Memory *		100.0%
CPU *		100.0%
✓ Activate	Upgrade	💼 Delete

The pop up Upgrade application appears.

Upgrade application		×
Application Id:	CyberVisionSensorNetwork	
Select Application Archive	Choose File No file chosen	
Preserve Application Data	\checkmark	
	OK Cancel	

- 5. Select the **Preserve Application Data** option.
- 6. Select the new version of the application archive file.

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

Upgrade application		×
Application Id:	CyberVision	SensorNetwork
Select Application Archive	Choose File	CiscoCyberh64-3.2.3.tar
Preserve Application Data	✓	
		OK Cancel

The operation takes a few moments.

Applications	Remote Docker Workflo	w Docker Layers	System Info Sy	stem Setting	Syste
3	nSensorN	DEPLOYED			
TYPE docker	VERSION 3.2.2+202103181622	PROFILE exclusive			
Memory *		100.0%	O Add New	C Refresh	
CPU *		100.0%			
✓ Activate	💠 Upgrade 🗂 D	elete			
				ılıılı. cısco	

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



- 7. Check the number of the new version.
- 8. Click Activate.

3	onSensorN ion sensor for aarch64	
TYPE docker	VERSION 3.2.3+2021042921	26 PROFILI
Memory *		100.0%
CPU *		100.0%
✓ Activate	e 🔷 Upgrade	💼 Delete

- 9. Check configurations.
- **10.** Click the **Activate App** button.

The application status moves to ACTIVATED.

11. Click the Start button.

The application status changes to RUNNING.

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

Data management		From this page, you can manage s securely rebooted, shut down, an						ors. Sensors can also be r	emotely and
Sensors	^	securely rebooted, shut down, an	u eraseu. writerra senso	connects for the first tim	e, you must autho	size it so the Center can receive	ve its data.		
- Sensors	- 1	Name	IP	Version	Status	Processing status	Active Discove	ery status Capture Mod	• Uptime
 Capture 									4d 1h 4
冬 Users	~	▼ FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data	Unavailable	All	9m
		S/N: F0C2334V00H Name: F0C2334V00H							
& API	~	IP address: 192.168.69.20 Version: 3.2.3+202104292							
	Ť		032	АМ					
₽ License	*	Version: 3 . 2 . 3+202104292 System date (UTC): Monday	032 , May 31, 2021 9:33	АМ				Cate Provision	iL Capture Mode
₩ License % LDAP Settings	*	Version: 3.2.3+202104292 System date (UTC): Monday Status: Connected Processing status: Pending di	032 , May 31, 2021 9:33	АМ					•
와 API License LDAP Settings Snort Integrations	*	Version: 3. 2. 3+202104292 System date (UTC): Monday, Status: Connected Processing status: Pending d Active discovery: Unavailable Deployment: Manual	032 , May 31, 2021 9:33	АМ			[
		Version: 3.2.3+202104292 System date (UTC): Monday, Status: Connected Processing status: Pending di Active discovery: Unavailable Deployment: Manual Uptime: 4d 1h. 49m Capture mode: All	032 , May 31, 2021 9:33	АМ					
		Version: 3. 2. 3+202104292 System date (UTC): Monday, Status: Connected Processing status: Preding d Active discovery: Unavailable Deployment: Manual Uptime: 4d 1h 49= Capture mode: All • Stat recording sensor	032 , May 31, 2021 9:33	AM 3.2.2+202103181753	Connected	Pending data	Unavailable		•