

# **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.

iliiilii cisco					<u>~</u> 8 ·
Ø	. Sensors	^	Extensions		
Ð	<ul> <li>Sensor Explorer</li> <li>Management jobs</li> <li>PCAP Upload</li> </ul>		From this page, you can manage Cyber Vision Extensions. E: Vision Center which provide more features, such as the mar detection engines, or integrations with external services.	xtensions are opt nagement of new	tional add-ons to Cyber device types, additional
ଞ ପ	<ul> <li>Q Active Discovery</li> <li>&amp; Users</li> </ul>	~ ~	Update     Uploading Please do not quit or refresh the page.		
¢	⊲ Events		Installed extensions		
	o <sup>ợ</sup> API	~	Name	Version	Actions
	꾜 License		Cyber Vision sensor management	4.1.2	C Update 🗇 Remove

## Update the sensors

Proce	edure	
In Cis	sco Cyber Vision, 1	navigate to Admin > Sensors > Sensor Explorer.
Senso	ors that are not up-	o-date have their version displayed in red.
Click	Install sensor, the	en Update Cisco devices.
cisco		
Ø	₩ System	Sensor Explorer
F	🗄 Data Management 🗠	
Ë	& Network Organization	time, you must authorize it so the Center can receive its data.
C	Sensors ^	🕒 Install sensor 👔 🖞 Manage Cisco devices 🗧 Organize
۹	<ul> <li>— Sensor Explorer</li> </ul>	Folders and ser
¢	<ul> <li>Management jobs</li> </ul>	☐ Manage credentials       ✓ Eilter     0 Selecter
	<ul> <li>PCAP Upload</li> </ul>	p File Objected Morescellarity More Activity
	Q Active Discovery ~	Label IP Address Version Location Health status 🔿 🔻
	条 Users ~	Even Lyon
	-1 F	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

⊲ Events

o<sup>g</sup> API

'⊒ License

			UPDATE CISCO DEVICES		×
Only sen only if th sensors t	sors deployed ere is a new ve to update.	with the Sensor Mana ersion of their applica	agement Extension (except IC tion available in the currently	3000) are concerned here. They appear installed extension. Please select the	ci Ci
	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.

			U	JPDATE CISCO DEVICES		×
Onl onl <sup>1</sup> sen	ly senso y if ther isors to i	rs deployed wi e is a new vers update.	th the Sensor Manage ion of their applicatior	ment Extension (except IC300 n available in the currently inst	0) are concerned here. They appear alled extension. Please select the	c 2
		Label 🔦	IP	Version	Target	
		IE3400	192.168.49.21	4.1.2+202207190948	Updatable to 4.1.3+202210041846	

#### 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.

cisco					<u>⊬</u> 8×
Ø	& Network Organization	Management jobs			
Ē	Sensors ^	Jobs execution for sensor manageme	ent tasks.		
	<ul> <li>Sensor Explorer</li> </ul>			< 1	> 20/page ∨
C	<ul> <li>Management jobs</li> </ul>				
Q	<ul> <li>PCAP Upload</li> </ul>	Jobs	Steps	Date	Duration
¢	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.

li.ili. cisco					<b>⊵</b> 8∨
Ø	& Network Organization	Management jobs			
Ē	Sensors ^	Jobs execution for sensor manage	ment tasks.		
	<ul> <li>Sensor Explorer</li> </ul>			< 1 >	20/page $\vee$
© Q	<ul> <li>Management jobs</li> </ul>	Jobs	Steps	Date	Duration
α	— PCAP Upload				
¢	@ Active Discovery ~	Batch update (FCW2445P6X5)		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 (FOC FOC2412V0DL, F FOC2330V0TJ, FC FOC2431V0A0, F	C2401V07N, OC2431V08E, OC2334V00D, OC2413V0X3) Update - Error
Batch update (FJ	Error
Single deploymer (FCH2312Y03Z)	Fatal error: at least one device failed
(, , , , , , , , , , , , , , , , , , ,	Logs
Batch update (FC	<pre>x FOC2413V0X3: failed: job with status FAILED has error: Error while</pre>
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	<ul> <li>F0C2401V07N: succeeded to update</li> <li>F0C2412V0DL: failed: job with</li> <li>status FALED has error: Error while</li> <li>changing app state:Cannot start while</li> </ul>
Single redeploym (FCW2435P3KV	<pre>in DEPLOYED state. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate'] &lt; FOC2431V08E: succeeded to update</pre>
Single redeploym (FOC2413V0X3)	<ul> <li>FOC2330V0TJ: succeeded to update</li> <li>x FOC2334V00D: failed: job with</li> <li>status FAILED has error: Error while</li> <li>changing app state:Cannot start while</li> </ul>
Single redeploym (FOC2412V0DL)	in UFFLUTED State. Allowed operations are ['undeploy', 'upgrade', 'download_data', 'activate'] / F0C2431V0A0: succeeded to update
Single redeployme	iii.

# **Upgrade through the IOx Local Manager**

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

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

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

.ili.ili. cisco											5	8~
0	🖽 System		Sensors									
e	Data management		From this page, you can manage s securely rebooted, shut down, and	ensors in online and offli d erased. When a sensor	ine modes a	nd generate p or the first tim	rovisioning packs	ages to deploy Cisco Cyber Vis orize it so the Center can recei	ion on remote sen ve its data.	sors. Sensors can also	be remotely	and
۲	Sensors	^										
¢	- Sensors		Name	IP	Version		Status	Processing status	Active Discov	ery status Capture I	Mode <sup>©</sup>	Uptime
Q (0)	— Capture 冬 Users	•	▼ FOC2334V00H	192.168.69.20	3.2.2+20	2103181619	Connected	Pending data	Unavailable	All		4d 1h 3 2m 47s
	<1 Events		S/N: F0C2334V00H Name: F0C2334V00H									
	ø API	~	IP address: 192.168.69.20 Version: 3.2.2+202103181	.619								
	₩ License		System date (UTC): Monday Status: Connected	, May 31, 2021 9:17	АМ					n l	+	,c
	糸 LDAP Settings		Active discovery: Unavailable	ata						Remove Get Pro	ovisioni Cap	ture Mode
	⊙ Snort		Deployment: Manual Uptime: 4d 1h 32m 47s									
	∝ Integrations	<b>~</b>	Capture mode: All • Start recording sensor									
	BB Extensions		Go to statistics									
			• FCH2312Y047	192.168.70.20	3.2.2+202	2103181753	Connected	Pending data	Unavailable	All		3m 27s
						🛓 UPDATE C	SCO DEVICES	+ DEPLOY CISCO DEVICE	+ INSTALL SENS	DR MANUALLY	IMPORT OFFI	INE FILE

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

Dashboard		cisco Cisco IC	<b>ystems</b> Ix Local Manager			
Monitoring	>	Applications	Remote Docker Workflow	Docker Layers	System Info	Syster
	>					
O Administration	>	CyberVision Cisco Cyber Vision	sensor for aarch64	RUNNING		
		TYPE docker	VERSION 3.2.2+202103181622	PROFILE exclusive		
C Licensing		Memory *		100.0%	• Add	New
X Troubleshooting		CPU *		100.0%		

The operation takes a few moments.

Applications	Remote Docker Workflow	Docker Layers	System Info	System Setting	Syste
CyberVisio	nSensorN	RUNNING			
TYPE docker	VERSION 3.2.2+202103181622	PROFILE			
Memory *		100.0%	O Add	New C Refresh	
CPU *		100.0%			
Stop	🌣 Manage				
			Operation in p	rogress, this can take s	ome tim

The application status switches to STOPPED.

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

III System		Sensors							
Data management		From this page, you can manage s securely rebooted, shut down, an	ensors in online and offi d erased. When a sensor	ine modes and generate p connects for the first tim	rovisioning packa e, you must autho	ages to deploy Cisco Cyber Vi orize it so the Center can rece	sion on remote sen ive its data.	sors. Sensors can also be rem	otely and
Sensors	^								
- Sensors		Name	IP	Version	Status	Processing status	Active Discov	very status Capture Mode <sup>©</sup>	Uptime
- Capture		▼ FOC2334V00H	192.168.69.20	3.2.2+202103181619	Disconnected @	SSH Disconnected	Unavailable	All	N/A
A Users	Ť	S/N: F0C2334V00H							
S Events		Name: FOC2334V00H IP address: 192.168.69.20	9						
o <sup>g</sup> API	Ĭ	Version: 3.2.2+202103181 System date (UTC): Monday	1619 , May 31, 2021 9:20	АМ				<u> </u>	.c
₩ License		Status: Disconnected Processing status: Disconnected	cted					Remove Get Provisioni	Capture Mode
ℜ LDAP Settings		Active discovery: Unavailable Deployment: Manual							
⊖ Snort		Capture mode: All							
≪ Integrations	~	<ul> <li>FCH2312Y047</li> </ul>	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	10m
B Extensions					ISCO DEVICES	+ DEPLOY CISCO DEVICE	+INSTALL SENS		T OFFLINE FILE

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

The application status moves to DEPLOYED.

4. Click Upgrade.



The pop up Upgrade application appears.



- 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	x
Application Id:	CyberVisionSensorNetwork
Select Application Archive	Choose File CiscoCyberh64-3.2.3.tar
Preserve Application Data	$\checkmark$
	OK Cancel

The operation takes a few moments.

Applications	Remote Docker V	Norkflow	Docker Layers	System Info	System Setting	System Tr
CyberVision	nSensorN sensor for aarch64	DEP	LOYED			
TYPE docker	VERSION 3.2.2+202103181622	2	PROFILE			
Memory *		10	0.0%	O Add	New 🛛 📿 Refresh	
CPU *		10	0.0%			
✓ Activate	💠 Upgrade	💼 Delete				
					cisco	

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



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

CyberVision Cisco Cyber Vision	DEPLOYED			
TYPE docker	VERSION 3.2.3+202104292126	PROFILE exclusive		
Memory *	100.0%			
CPU *	100.0%			
✓ Activate	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.

I

I System	Sensors							
Data management	From this page, you can manag securely rebooted, shut down,	e sensors in online and o and erased. When a sen	offline modes and generate p sor connects for the first tim	rovisioning packa e, you must autho	ges to deploy Cisco Cyber Vis rrize it so the Center can recei	ion on remote sen ve its data.	sors. Sensors can al	so be remotely and
Sensors ^								
- Sensors	Name	IP	Version	Status	Processing status	Active Discov	very status Capture	e Mode <sup>©</sup> Uptime
<ul> <li>Capture</li> </ul>								4d 1h 4
永 Users 🗸	▼ FOC2334V00H	192.168.69.20	3.2.3+202104292032	Connected	Pending data		All	9m
⊲ Events	S/N: F0C2334V00H Name: FOC2334V00H	,						
o <sup>g</sup> API ✓	IP address: 192.168.69. Version: 3.2.3+2021042	.20 192032						
₩ License	System date (UTC): Mond Status: Connected	ay, May 31, 2021 9:	33 AM					
糸 LDAP Settings	Processing status: Pendir Active discovery: Unavail	<b>g data</b> able					Remove Get	Provisioni Capture Mode
⊘ Snort	Deployment: Manual Uptime: 4d 1h 49m							
📽 Integrations 👻	Capture mode: All Start recording sensor							
88 Extensions	Go to statistics							
	▶ FCH2312Y047	192.168.70.20	3.2.2+202103181753	Connected	Pending data	Unavailable	All	19m 34 s
			1 UPDATE C	ISCO DEVICES	+ DEPLOY CISCO DEVICE	+INSTALL SENS	OR MANUALLY	