

# Configuration

- Configure Active Discovery, on page 1
- Configure sensor configuration template, on page 3
- Set a capture mode, on page 8

# **Configure Active Discovery**

Once the sensor is connected, you can change the Active Discovery's network interface so it uses the Collection network interface instead, and add several network interfaces for the sensor to perform Active Discovery on several subnetworks at the same time.

#### Procedure

## Step 1 Click the sensor to configure and click the Active Discovery button on its right side panel.

Sensor Explorer		FCW2445P6X5	×
rom this page, you can explore and manage sensors and sensors folders. Sensors can b or the first time, you must authorize it so the Center can receive its data.	el Label: FCW2445P6X5 Serial Number: FCW2445P6X5 IP address: 192.168.49.21		
+ Install sensor		Version: 4.1.0+202202151440 System date: Feb 24, 2022 4:13:06 PM Deployment: Sensor Management Extension	
Folders and sensors (3)		Active Discovery: Enabled Capture mode: All	
√ Filter 0 Selected Move selection to More Actions  ✓		System Health Status: Connected	
Label IP Address Version Location	Health status 🕕 🔻	Processing status: Normally processing Uptime: a day	
C • 55355 arts	Descented	∠ Go to statistics	
		Start Recording	
□ □ FCW2445P6X5 192.168.49.21 4.1.0+202202151440	Connected	🗇 Move to	
		🔦 Capture mode 🔗 Redeploy	
		⊖ Uninstall @ Active Disco	very

The Active Discovery configuration appears with the interface currently set.

ACTIVE DISCOVERY CONFIGURATION From here you can configure Active Discovery			
Add Active Discovery configuration Use collection interface New network interface	Network interfaces • 192.168.49.21/24 VLAN#1 (collection interface)		

## **Step 2** Select **Use collection interface** for the Active Discovery to use the Collection network interface.

To add a network interface to Active Discovery for the sensor to perform active monitoring on another subnetwork:

<b>Step 3</b> Add a new network interface by clicking the corresponding but
---

**Step 4** Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number

## Step 5 Click Add.

ACTIVE DISCOV	ERY CONFIGURATION
+ New network interface	
IP address*	
192.168.52.24	
IP address interface used to do Active Discovery Prefix length*	
24	
Like 24, 16 or 8	
52	
Use 1 by default	
Add Cancel	
	Colore
	Configure

You can add as many network interfaces as needed.

**Step 6** When you are done, click **Configure**.

A message saying that the configuration has been applied successfully appears.

## **Configure sensor configuration template**

## **Templates**

This page allows you to create and set templates with protocol configurations and assign them to specific sensors.

Sensor templates contain protocol configurations which allow you:

- To enable or disable protocol DPI (Deep Packet Inspection) engines.
- To map UDP and TCP ports for each protocol's packet received by the sensor.

By enabling/disabling a protocol DPI engine you can decide which protocols will be analyzed.

Disabling a protocol DPI engine avoid false positives in Cisco Cyber Vision, that is when a protocol appears on the user interface when it's actually not the case because same UDP/TCP ports can be used by other non-standardized protocols.

Some protocols are disabled in the Default template because they are not commonly used or used in specific fields such as transportation. The Default template is applied on all compatible sensors.

As previously mentioned, UDP/TCP ports default configurations are mostly standardized, but conflicts still exist among field-specific protocols or with limited usage. Mapping UDP/TCP port numbers will allow packets to be sent to the correct DPI engine so they can be accurately analyzed and correctly represented in the user interface.

If the protocol's packet is sent to the wrong port, related information will end up in Security Insights/Flows with no tag.

A sensor can be associated with a single template only. Deployment of the template can fail:

- if the sensor is disconnected,
- if there is connection issues,
- if the sensor version is too old.

## **Create templates**

#### Procedure

Step 1In Cisco Cyber Vision, navigate to Admin > Sensors > Templates.Step 2Click Add sensor template.



The Create sensor template window pops up.



CREATE SENSOR TEMPLATE						
1 Basic information	2 Protocol configuration	3 Select sensors	4 Summary			
* Name OPCUA						
Description						
			h			
			Cancel Next			

Step 4 Click Next.

The list of protocol DPI engines with their basic configurations appears.

		ormgaration ren	ipiace			
	CREATE SENSOR TEMPLATE					
Bas	ic information	2 Protocol configuration	3 Select sensors	(4) So	ummary	
	Search for protocol name, category, port number, port protocol type Q Display modified only					
	Protocol 🗘	Category $\begin{tabular}{c} \end{tabular}$	Port Mapping			
	ARP	Network	N/A			
	Bacnet	BMS	N/A			
	BACnetVLC	BMS	∠ UDP 47808			
	BeckhoffAMS	General	<u>∥</u> TCP 48898			
	BFD	General	<u>⊿</u> UDP 3734			
	BoschRCP	General	<u>∥</u> TCP 1756			
				Previous	Next	

## Step 5

In the search bar, type the protocol you want to configure.

In our example, we will add a port to the OPCUA default settings.

		CREATE SENSOR TEMPLATE	Х
V Bas	ic information	2 Protocol configuration 3 Select sensors	4 Summary
орс		• 9	Display modified only
	Protocol	Category	
	OPCUA	General 2 TCP 4840 TCP 51210 TCP 12403	
		Previo	Next

Step 6Under the Port Mapping column, click the pen button to edit its settings.The protocol's port mapping window pops up.

**Step 7** Write down the port number you want to add and hit enter.

Configuration

OPCUA Por	rt Mapping		×	OPCUA Po	ort Mapping		×
ТСР	4840 × 51210 × 12403 × 46798	Use same for IPv6		ТСР	4840 × 51210 × 12403 × 46798 ×	Use same for IPv6	
UDP		Use same for IPv6		UDP		Use same for IPv6	
L			_	-			
	Reset to	default Cancel	ОК		Reset t	o default Cancel	ОК

## Step 8 Click OK.

The port number is added to the protocol's default settings.

CREATE SENSOR TEMPLATE X						
Basic information	2 Protocol configuration 3 Select sensors	4 Summary				
opc	• Q	Display modified only				
Protocol 🗘	Category					
ΟΡΟΟΑ	General 🖉 TCP 4840 TCP 51210 TCP 12403	TCP 46798				
	Prev	ious Next				

Comparation remplate						
CREATE SENSOR TEMPLATE X						
V Bas	sic information —		2 Protocol c	onfiguration	3 Select sensors	4 Summary
						Q Display modified only
	Protocol	÷	Category	Port Mapp	ing	
	OPCUA		General	тс	P 4840 TCP 51210	TCP 12403 TCP 46798
						Previous Next

Toggling ON the **Displayed modified only** button allows you to quickly find this protocol.

# Step 9Click Next.Step 10Select the sensor(s) you want to apply the template to.

CREATE SENSOR TEMPLATE X						
Basic information	- V Protocol configuration	Select sensors	(4) Summary			
2 Selected 🖓 Filters Select All Unselect All As of: October 25, 2023 at 10:33:19 AM 🔿						
■ Label	<ul> <li>Template</li> <li>Template</li> <li>Deployment <pre></pre></li></ul>	Version	Processing Status ¢ Active Discovery ¢ Uptime ¢			
Sensor_Line1 192.168.49.25 FOLDER1	Default deployed	4.3.0+202310 181603 Line 1 Connected	Normally Enabled 5 days processing			
Sensor_Line2 FOLDER2	Default failed	Line 2 Disconnected	Disconnected Unavailable N/A			
Sensor_Line3 192.168.49.23	Default deployed	4.3.0+202310 Connected 181544	Normally Unavailable 16 hours processing			
			3 Records $<$ 1 $>$ 10/page $\vee$			
			Previous Next			

## Step 11

Click Next.

**Step 12** Check the template configurations and **Confirm** its creation.

CREATE SENSOR TEMPLATE	×
Select sensors	4 Summary
OPCUA Sensors 2 sensors selected view list ↓ Settings   Display modified only	
Status: enabled Port Mapping: TCP 4840 TCP 51210 TCP 12403 TCP 46798	
Previou	Is Confirm

The configuration is sent to the sensors. Configuration deployment will take a few moments. The OPCUA template appears in the template list with its two assigned sensors.

## Configuration Template

Sensor configuration templates allow you to enable and personalize protocol settings, and deploy them to a large number of sensors.

🕀 Add se	nsor temp	plate			As of: Octo	ber 24, 2	2023 at 3:06:55 PM	С
Name	÷ ±	Sensor Count	\$ Deployment progress	÷ Ŧ	Last update	¢	Actions	
Default		1			-			
OPCUA		2		•	Today			
						<	1 > 20/page	e V

# Set a capture mode

The Capture mode feature lets you choose which network communications will be analyzed by the sensors. You can set it by clicking an online sensor in the sensors list of the Sensor Explorer page or during a sensor installation.

Setting the capture mode on a sensor from the right side panel:

Sensor Explorer			FCH2309Y01Z		
From this page, you can explore and n connects for the first time, you must a	nanage sensors and ser authorize it so the Cent	Label: FCH2309Y01Z Serial Number: FCH2309Y01Z IP address: 192.168.49.23 Version: 4.1.0+202202151504			
🕂 Install sensor ျို် Manage Ci	isco devices 🛛 🗟 Orga	nize		System date: Mar 9, 2022 11: Deployment: Sensor Manager	46:58 AM nent Extension
Folders and sensors (5)				Capture mode: All	
<b>Filter</b> 0 Selected Mov	re selection to More	Actions 🗡		System Health Status: Connected Processing status: Bonding da	to
Label IP Add	lress Version	Location	Health stat	Uptime: 20 hours	la
Folder1		Lyor	ı	$\sim$ Go to statistics	
Folder2		Pari	s	Start Recording	
□ □ FCY014567 19	92.168.49.41		Disco	🗁 Move to	
□ □ FCH2309Y01Z 19	92.168.49.23 4.1.04	202202151504	Conne	⊥ Download package	🔧 Capture mode
□ □ FCW2445P6X5 19	92.168.49.21 4.1.0+	202202151440	Conne	Redeploy	C Enable IDS
				€ Reboot	() Shutdown
				⊖ Uninstall	Q Active Discovery

Capture modes:

>	CAPTURE MODE X
L	Please select an option to filter the flows analyzed by this sensor.
	Capture mode:
	Optimal (default): analyze the most relevant flows
ar -	• All: analyze all the flows
Ŀ	O Industrial only: analyze industrial flows
÷€	<ul> <li>Custom: you set your filter using a packet filter in tcpdump- compatible syntax</li> </ul>
5	OK Cancel
	In adding the state of the stat

The aim is mainly to focus the monitoring on relevant traffic but also to reduce the load on the Center.

For example, a common filter in a firewall can consist of removing the network management flows (SNMP). This can be done by setting a filter like "not (port 161 and host 10.10.10.10)" where "10.10.10.10" is the network management platform.

Using Capture mode Cisco Cyber Vision performance can be improved on large networks.

Capture modes operate because of filters applied on each sensor. Filters are set to define which types of incoming packets are to be analyzed by the sensors. You can set a different filter on each sensor according to your needs.

You can set the capture mode in the installation wizard when enrolling the sensors during the Center installation. This option is recommended if you already know which filter to set. Otherwise, you can change it at any time through the Sensor Explorer page in the GUI (provided that the SSH connection is allowed from the Center to the sensors).



Note

You can set a capture mode to offline sensors from a file containing the filter and registered on the USB drive. This will be then plugged on the Offline USB port of the device. For more information about setting a capture mode on an offline sensor contact the support.

The different capture modes are:

- ALL: No filter is applied. The sensor analyzes all incoming flows and they will all be stored inside the Center database.
- OPTIMAL (Default): The applied filter selects the most relevant flows according to Cisco expertise. Multicast flows are not recorded. This capture mode is recommended for long term capture and monitoring.
- INDUSTRIAL ONLY: The filter selects industrial protocols only like modbus, S7, EtherNet/IP, etc. This means that IT flows of the monitored network won't be analyzed by the sensor and won't appear in the GUI.
- CUSTOM (advanced users): Use this capture mode if you want to fully customize the filter to be applied. To do so you will need to use the tcpdump syntax to define the filtering rules.

I