



Cisco Cyber Vision Active Discovery Configuration Guide, Release 4.3.0

First Published: 2022-05-06

Last Modified: 2024-03-05

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1	About this documentation	1
	Document purpose	1
	Warnings and notices	1

CHAPTER 2	Overview	3
	General principles	3
	Design considerations	4
	Basic configuration workflow	4

CHAPTER 3	Sensor configuration	5
	Configure Active Discovery on a Cisco switch or router	5
	Configure Active Discovery on a Cisco IC3000	9

CHAPTER 4	Policies configuration	13
	Create a policy	13
	Set Active Discovery Broadcast	14
	Set Active Discovery Unicast	16
	Set Active Discovery Unicast BACnet	16
	Set Active Discovery Unicast DNP3	17
	Set Active Discovery Unicast Ethernet/IP	18
	Set Active Discovery Unicast Melsoft	19
	Set Active Discovery Unicast Modbus	20
	Set Active Discovery Unicast OMRON	21
	Set Active Discovery Unicast SiemensS7	21
	Set Active Discovery Unicast SiemensS7plus	22
	Set Active Discovery Unicast SNMPv2c	23

Set Active Discovery Unicast SNMPv3 24
 Set Active Discovery Unicast WMI 26
 Modify a policy 27

CHAPTER 5 Profiles configuration 31
 Set an Active Discovery profile 31

CHAPTER 6 Launch Active Discovery 33
 Launch Active Discovery 33

CHAPTER 7 Annex: Active Discovery protocols 37

- BACnet 38
- DNP3 39
- EtherNet/IP 39
 - EtherNet/IP Broadcast or Unicast 40
 - Ethernet/IP backplane discovery 42
- Melsoft 44
- Modbus 45
- OMRON 46
- Profinet Multicast 46
- S7 Broadcast 47
- S7 Unicast 48
- S7Plus 49
- ICMPv6 Multicast 50
- SNMP Unicast 50
 - AD SNMP with Schneider PLC 51
 - AD SNMP with Siemens PLC 52
 - AD SNMP with Rockwell PLC 53
 - AD SNMP with Moxa switches 53
 - AD SNMP with Siemens Switches 54
 - AD SNMP with Hirschmann hardware 55
 - AD SNMP with Cisco hardware 56
 - AD SNMP with Microsoft Windows OS 57
- WMI 58



CHAPTER 1

About this documentation

- [Document purpose, on page 1](#)
- [Warnings and notices, on page 1](#)

Document purpose

This configuration guide explains how to configure Active Discovery in Cisco Cyber Vision and gives details on expected results.

This documentation is applicable to **system version 4.3.0**.

Active Discovery is **available on** the following devices:

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 Rugged Series Switch
- Cisco Catalyst IE9300 Rugged Series Switch
- Cisco Catalyst 9300 Series Switch
- Cisco Catalyst 9400 Series Switch
- Cisco IC3000 Industrial Compute Gateway
- Cisco IR8340 Integrated Services Router Rugged

Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.



Warning

Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.



Important Indicates risks that could involve property or equipment damage and minor personal injury if proper precautions are not taken.



Note Indicates important information on the product described in the documentation to which attention should be paid.



CHAPTER 2

Overview

- [General principles, on page 3](#)
- [Design considerations, on page 4](#)
- [Basic configuration workflow, on page 4](#)

General principles

Active Discovery allows the sensor to send packets to the network to discover previously unseen devices and gather additional properties for known devices.

There are two different types of Active Discovery operations:

- Broadcast

The sensor sends Broadcast packets targeting all the devices in the subnet. Devices that support the protocol will give a response back and appear in Cisco Cyber Vision.

- Unicast

The sensor sends Unicast packets to known components and analyses the responses received.

The protocols supported for Active Discovery operations are:

- Broadcast:

- EtherNet/IP
- Profinet
- SiemensS7
- ICMPv6

- Unicast:

- EtherNet/IP
- SiemensS7
- SNMPv2c
- SNMPv3

- WMI

For more information about discoverable properties, refer to [Annex: Active Discovery protocols, on page 37](#).

Design considerations

Several requirements must be met when deploying and configuring Active Discovery on a sensor:

- The sensor must have access to the required subnet:
 - For Broadcast discovery, the target subnet/VLAN must be directly accessible from the sensor, meaning the sensor must have an IP address set in this subnet.

On IOx sensors, the AppGigabit interface must be in trunk mode, and the VLAN must be allowed on this port.

On the Cisco IC3000, one of the interfaces must be connected to a port on the VLAN, with no span configured on this port.
 - For Unicast discovery, the target subnet/VLAN must be either directly accessible from the sensor, or the sensor must have the required gateway or route to reach the targeted devices.
- The list of nodes targeted in Unicast discovery comes from the device list of the preset which launch the discovery. A preset configured with sensors in its filter will trigger Active Discovery on these sensors. It means that only the components that have been filtered by this particular preset will be scanned.

Basic configuration workflow

To configure Active Discovery, you must perform the following steps:

- Deploy a sensor with the required configuration: IP address, VLAN, gateway or routes.
- Create an Active Discovery policy containing the protocols needed and their respective parameters.
- Create an Active Discovery profile with a policy, target IP addresses and and set an execution time or run it once.



CHAPTER 3

Sensor configuration

The Active Discovery configuration procedure will vary depending on the sensor model, whether it is a switch, a router or a Cisco IC3000.

To configure Active Discovery on a switch or a router, the sensors must have been previously deployed using the IOx sensor application file with Active Discovery. In this case, the Active Discovery button should appear in the sensor right side panel in Cisco Cyber Vision's Sensor Explorer page.

On a Cisco IC3000, you can configure Active Discovery performing a manual configuration or redeploying the sensor via the sensor extension.

- [Configure Active Discovery on a Cisco switch or router, on page 5](#)
- [Configure Active Discovery on a Cisco IC3000, on page 9](#)

Configure Active Discovery on a Cisco switch or router

Before you begin

This procedure is applicable to:

- Cisco IE3300 10G, Cisco IE3400 and Cisco IE9300.
- Cisco Catalyst 9300, Cisco Catalyst 9300X and Cisco Catalyst 9400.
- Cisco IR1101 and Cisco IR8340 Integrated Services Router Rugged

The sensors must have been deployed using the IOx sensor application file with Active Discovery.

Procedure

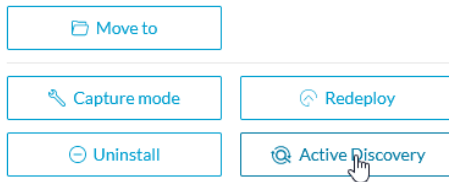
Step 1 Navigate to **Admin > Sensors > Sensor Explorer**.

Step 2 Select a sensor in the list.

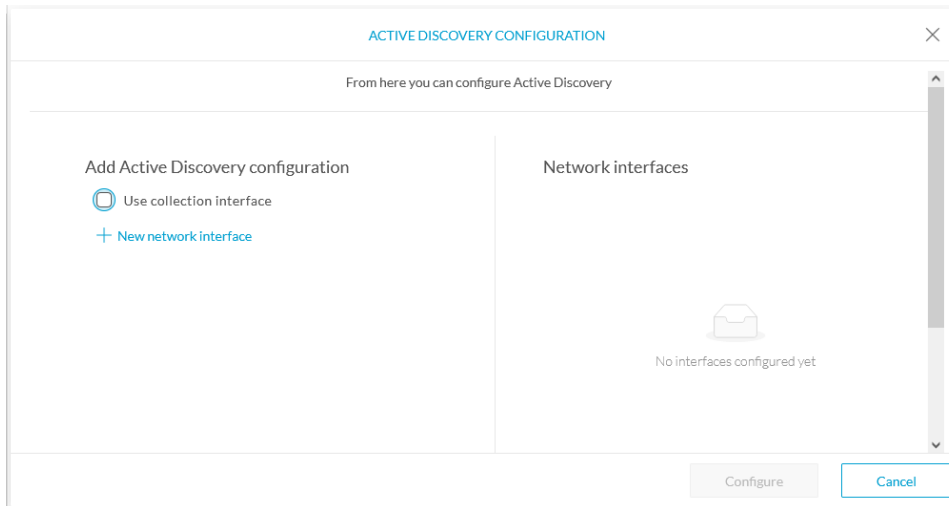
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

If there is no Active Discovery button in the panel, you must redeploy the sensor using the IOx application file with Active Discovery.

Step 3 Click the **Active Discovery** button.

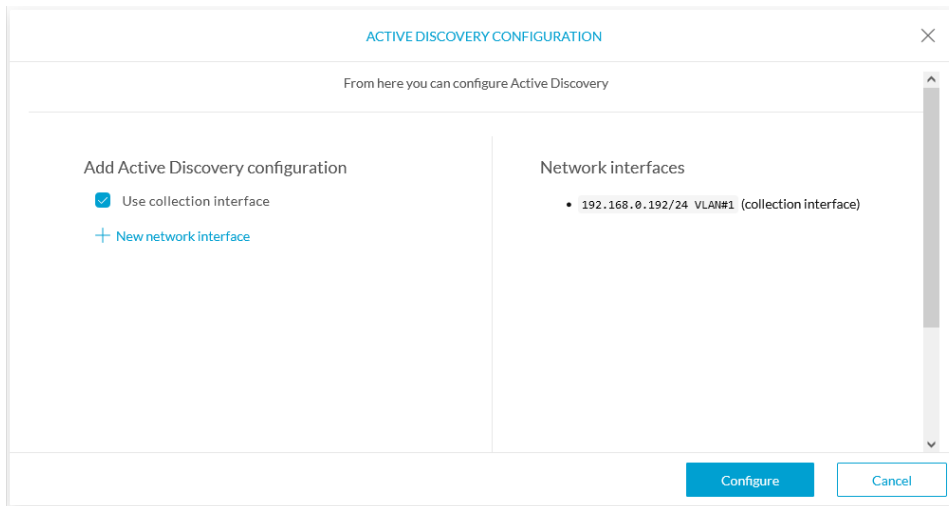


The Active Discovery Configuration window pops up:



Step 4 If necessary, tick the **Use collection interface** check box for Active Discovery to use the Collection network interface to do discovery on the same subnet as the sensor IP, or using the sensor Collection gateway.

The Collection network interface is added in the list on the right.



Step 5 Click + **New network interfaces** for the sensor to perform Active Discovery on additional subnetworks.

Step 6 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length

• VLAN number

+ New network interface

IP address*
192.168.20.145
IP address interface used to do Active Discovery

Prefix length*
24
Like 24, 16 or 8

VLAN number*
20
Use 1 by default

Add Cancel

Step 7 Click **Add**.

You can add as many network interfaces as needed, like below.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

Use collection interface

+ New network interface

Network interfaces

- 192.168.0.192/24 VLAN#1 (collection interface)
- 192.168.20.192/24 VLAN#20 delete
- 192.168.21.192/24 VLAN#21 delete
- 192.168.22.192/24 VLAN#22 delete
- 192.168.24.192/24 VLAN#24 delete

Step 8 Click **OK**.

The following schemas show how Active Discovery is created and how packets navigate inside the switch (in red).

Figure 1: IE3300 10G and IE3400:

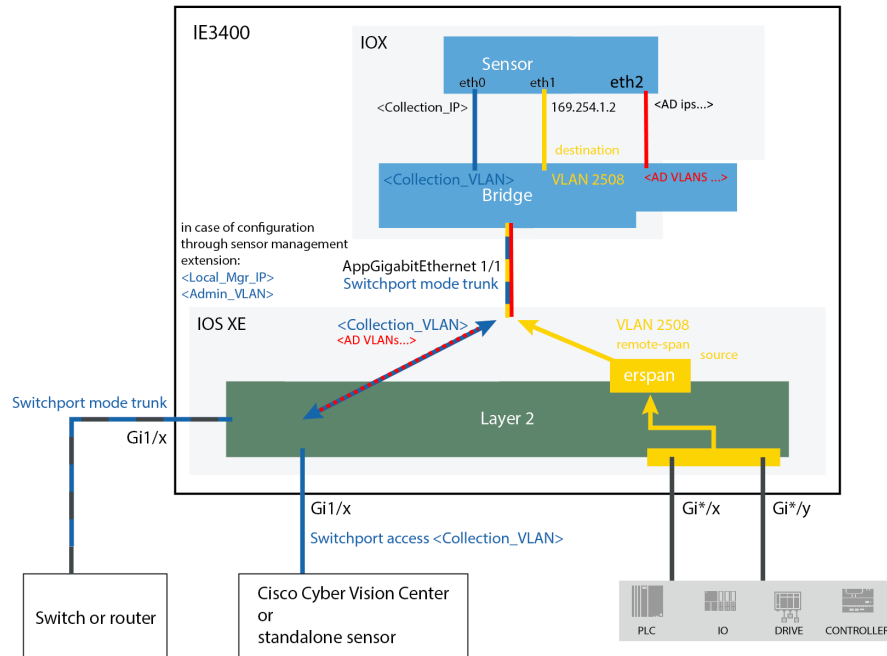


Figure 2: Catalyst 9300 and Catalyst 9400:

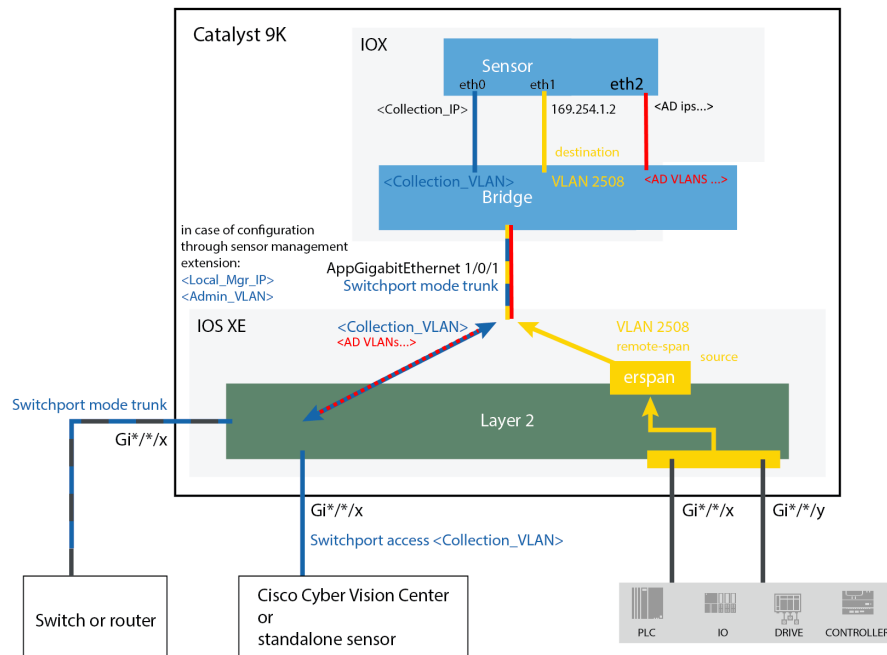
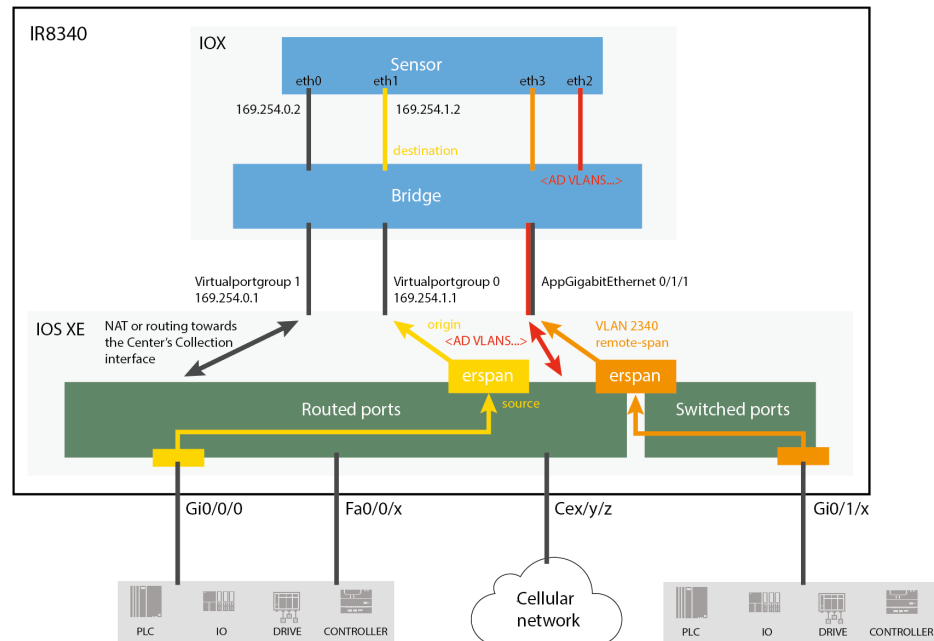


Figure 3: IR8340:

**What to do next**

Proceed to [Policies configuration](#), on page 13.

Configure Active Discovery on a Cisco IC3000

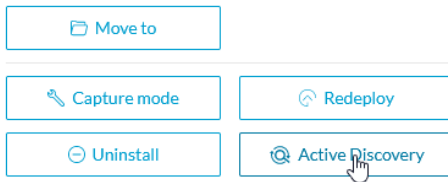
Before you begin

This procedure is applicable to the Cisco IC3000 Industrial Compute Gateway.

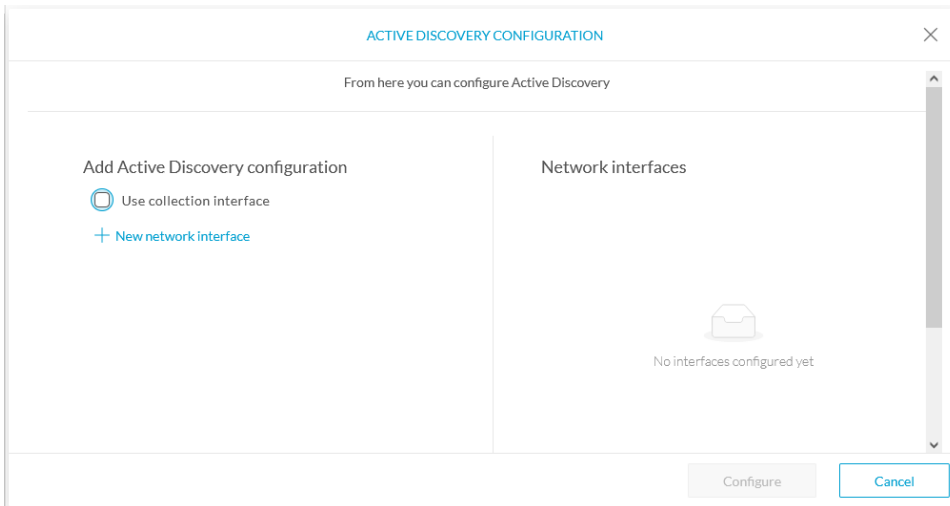
The sensors must have been deployed using the IOx sensor application file with Active Discovery.

Procedure

-
- Step 1** Navigate to **Admin > Sensors > Sensor Explorer**.
- Step 2** Select a sensor in the list.
- The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.
- If there is no Active Discovery button in the panel, you must redeploy the sensor using the IOx application file with Active Discovery.
- Step 3** Click the **Active Discovery** button.

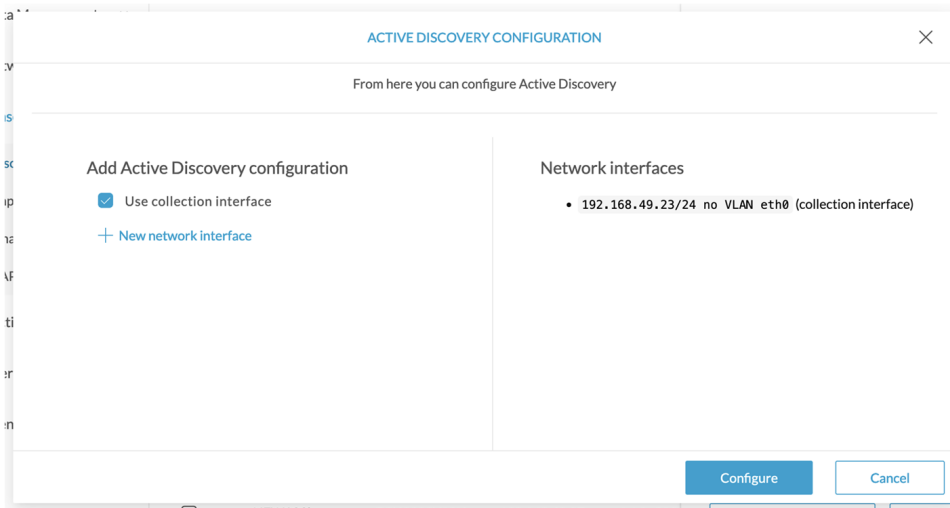


The Active Discovery Configuration window pops up:



Step 4 If necessary, tick the **Use collection interface** check box for Active Discovery to use the Collection network interface to do discovery on the same subnet as the sensor IP, or using the sensor Collection gateway.

The Collection network interface is added in the list on the right.



Step 5 Click + **New network interface** for the sensor to perform Active Discovery on additional subnetworks.

Step 6 Select a physical interface and fill the following parameters to set a dedicated network interface:

- IP address

- Prefix length
- VLAN number

ACTIVE DISCOVERY CONFIGURATION

Interface*
Int2

IP address*
192.168.53.23

Prefix length*
24

VLAN number*
53

Add Cancel

Step 7 Click **Add**.

The network interfaces appears on the right.

ACTIVE DISCOVERY CONFIGURATION

From here you can configure Active Discovery

Add Active Discovery configuration

Use collection interface

+ New network interface

Network interfaces

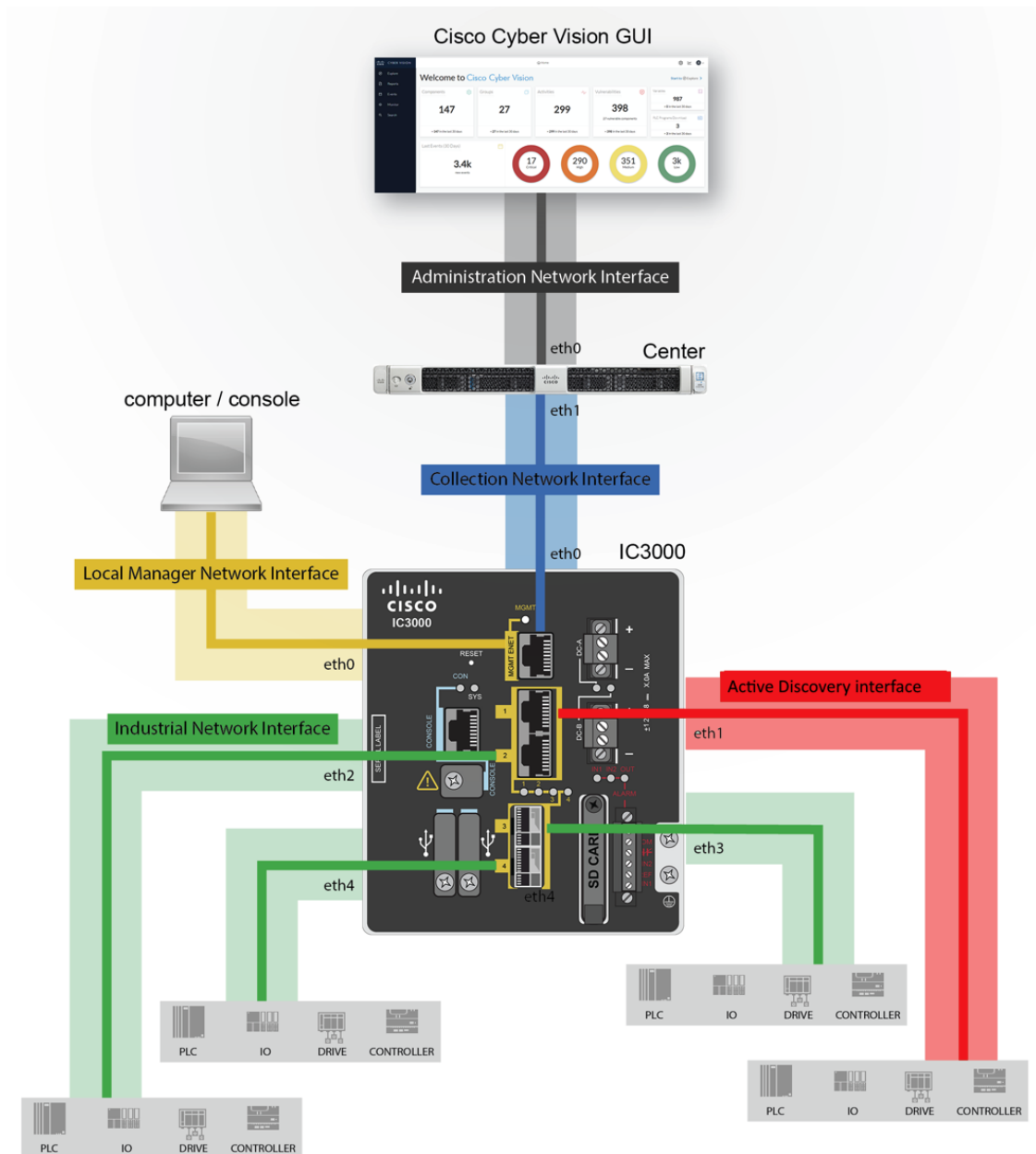
- 192.168.49.23/24 no VLAN eth0 (collection interface)
- 192.168.53.23/24 VLAN#53 eth2 delete

Configure Cancel

You can add as many network interfaces as needed.

Step 8 Click **Configure**.

The following schema shows how Active Discovery is created and how packets navigate inside the Cisco IC3000 (in red).



What to do next

Proceed to [Policies configuration](#), on page 13.



CHAPTER 4

Policies configuration

- [Create a policy, on page 13](#)
- [Set Active Discovery Broadcast, on page 14](#)
- [Set Active Discovery Unicast, on page 16](#)
- [Modify a policy, on page 27](#)

Create a policy

An Active Discovery policy is a list of settings which define protocols and their parameters that will be used to inspect the industrial network. The policy will be applied to an IP address, an IP range and/or a preset and used on a list of sensors and components.

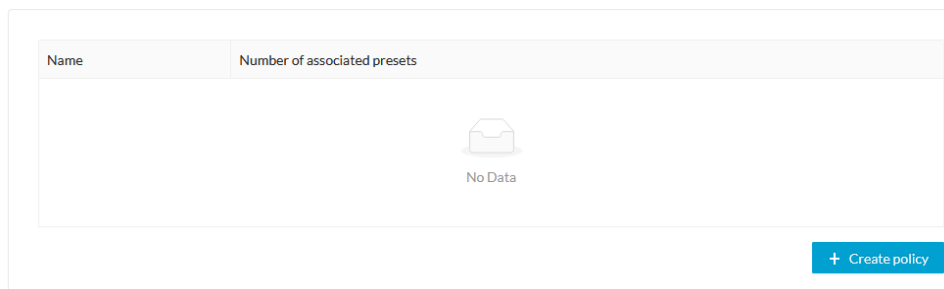
Name	Number of associated presets
snmp V2c public	4
Broadcast PN	2
Broadcast S7	0
Broadcast ICMPv6	1

Procedure

Step 1 Navigate to **Admin > Active Discovery > Policies** .

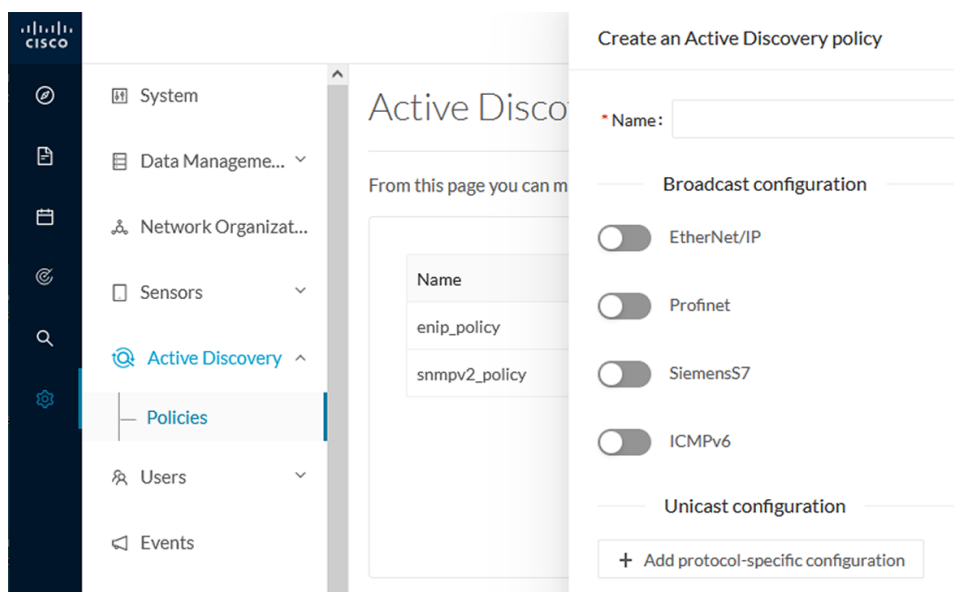
Active Discovery policies

From this page you can manage the Active Discovery policies.



Step 2 Click **+ Create policy**.

A Create an Active Discovery policy overlay appears.



What to do next

- [Set Active Discovery Broadcast, on page 14](#)
- [Set Active Discovery Unicast, on page 16](#)

Set Active Discovery Broadcast

Before you begin

Active Discovery is compatible with the following Broadcast protocols:

- EtherNet/IP

- Siemens S7
- Profinet
- ICMPv6

The sensor will send requests on all defined interfaces.

Procedure

Step 1

Type a policy name.

Step 2

Toggle the Broadcast protocol buttons ON to enable Active Discovery on these protocols.

× Create an Active Discovery policy

* Name: Broadcast_policy

Broadcast configuration

<input checked="" type="checkbox"/> EtherNet/IP	* Retry: 3	* Timeout: 10
<input checked="" type="checkbox"/> Profinet	* Retry: 3	* Timeout: 10
<input checked="" type="checkbox"/> SiemensS7	* Retry: 3	* Timeout: 10
<input type="checkbox"/> ICMPv6		

Unicast configuration

+ Add protocol-specific configuration

Cancel Create

Step 3

Leave the Retry and Timeout settings with the default values (3 and 10).

Retry: number of request attempts.

Timeout: waiting time in seconds for a response.

Step 4

Click **Create** to finish or add Unicast configurations to the policy.

What to do next

[Set Active Discovery Unicast, on page 16](#)

Set Active Discovery Unicast

Before you begin

Procedure

Step 1 Give the policy a name.

Step 2 Under Unicast configuration, click + **Add protocol-specific configuration**.

Step 3 Click the **Select protocol** dropdown menu and select a protocol.

What to do next

See herebelow configurations per protocol.

Set Active Discovery Unicast BACnet

Set Active Discovery Unicast BacNet to search for devices and components with BacNet requests. All components with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

The screenshot shows a configuration window titled "Unicast configuration". Inside, there is a dropdown menu set to "BACnet". Below it, an "Enable" toggle switch is turned on. There are two input fields: "Retry attempts" with the value "1" and "Timeout (in seconds)" with the value "5". At the bottom right of the dialog box are "Cancel" and "Save" buttons. Below the dialog box is a button labeled "+ Add protocol-specific configuration". At the bottom right of the main configuration area are "Cancel" and "Create" buttons.

Step 3 Click **Save**.

The menu closes.

Step 4 Click **Create**.

Set Active Discovery Unicast DNP3

Set Active Discovery Unicast DNP3 to search for devices and components with DNP3 requests. All components with an IPV4 address will be queried.

Before you begin

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

Unicast configuration

DNP3

Enable

* Retry attempts:

* Timeout (in seconds):

* Source Address:

* Max Destination Address:

Cancel Save

+ Add protocol-specific configuration

Cancel Create

Step 3 Leave the Source Address and Max Destination Address with the default values (0 and 16).

Step 4 Click **Save**.

The menu closes.

Unicast configuration

> DNP3 - Enabled ✎ ✕

+ Add protocol-specific configuration

Cancel Create

Step 5 Click **Create**.

Set Active Discovery Unicast Ethernet/IP

Set Active Discovery Unicast Ethernet/IP to search for devices and components with Ethernet/IP requests. All components with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

- Step 3** You can toggle the **Backplane discovery** button ON. Active Discovery will look for the different module details within the discovered chassis.

Unicast configuration

EtherNet/IP

Enable

* Retry attempts * Timeout (in seconds)

Backplane discovery

Cancel Save

+ Add protocol-specific configuration

Cancel Create

- Step 4** Click **Save**.
The menu closes.

- Step 5** Click **Create**.

Set Active Discovery Unicast Melsoft

Set Active Discovery Unicast Melsoft to search for devices and components with Melsoft requests. All Mitsubishi components with an IPV4 address will be queried.

Procedure

- Step 1** Toggle the **Enable** button ON.
- Step 2** Leave the Retry attempts and Timeout settings with the default values (0 and 5).

Unicast configuration

Melsoft

Enable

* Retry attempts

* Timeout (in seconds)

Cancel Save

+ Add protocol-specific configuration

Cancel Create

Step 3 Click **Save**.
The menu closes.

Step 4 Click **Create**.

Set Active Discovery Unicast Modbus

Set Active Discovery Unicast Modbus to search for devices and components with Modbus requests. All components with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (1 and 5).

Unicast configuration

Modbus

Enable

* Retry attempts

* Timeout (in seconds)

Unit Id

Force UMAS Function Codes

Cancel Save

+ Add protocol-specific configuration

Cancel Create

Step 3 Click **Save**.

The menu closes.

Step 4 Click **Create**.

Set Active Discovery Unicast OMRON

Set Active Discovery Unicast OMRON to search for devices and components with FINS requests. All components with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (1 and 5).

The screenshot shows a configuration window titled "Unicast configuration". Inside, there is a section for "OMRON" with a dropdown arrow. Below this, there is an "Enable" toggle switch which is turned on. There are two input fields: "Retry attempts" with the value "1" and "Timeout (in seconds)" with the value "5". At the bottom right of the configuration area are "Cancel" and "Save" buttons. Below the configuration area is a button labeled "+ Add protocol-specific configuration". At the very bottom of the window are "Cancel" and "Create" buttons.

Step 3 Click **Save**.

The menu closes.

Step 4 Click **Create**.

Set Active Discovery Unicast SiemensS7

Set Active Discovery Unicast SiemensS7 to search for devices and components with SiemensS7 requests. SiemensS7 is a communication protocol used on Siemens PLCs. Siemens PLCs with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

Unicast configuration

SiemensS7

Enable

* Retry attempts:

* Timeout (in seconds):

Rack [?]:

Slot [?]:

Cancel Save

Cancel Create

Step 3 Enter a number of racks and slots to be queried.
Slot: number of modules to search for within a chassis.

Step 4 Click **Save**.
The menu closes.

Step 5 Click **Create**.

Set Active Discovery Unicast SiemensS7plus

Set Active Discovery Unicast SiemensS7plus to search for devices and components with SiemensS7plus requests. SiemensS7plus is a communication protocol used on the latest Siemens PLCs. Siemens PLCs with an IPV4 address will be queried.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (1 and 5).

Unicast configuration

Siemens57plus

Enable

* Retry attempts: 1

* Timeout (in seconds): 5

Cancel Save

+ Add protocol-specific configuration

Cancel Create

Step 3 Click **Save**.
The menu closes.

Step 4 Click **Create**.

Set Active Discovery Unicast SNMPv2c

Set Active Discovery Unicast SNMPv2c to search for devices and components with SNMPv2c requests. All components with an IPV4 address will be queried. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

Procedure

- Step 1** Toggle the **Enable** button ON.
- Step 2** Leave the Retry attempts and Timeout settings with the default values (0 and 5).
- Step 3** Type a community string for authentication.
The community string is defined by IT or network administrators. The value "public" is often used by default.
- Step 4** You can toggle the **Enable SNMPv1 fallback** button ON. Active Discovery will look for PLCs and I/O chassis with module details.

Step 5 Click **Save**.
The menu closes.

Step 6 Click **Create**.

Refer to the Annex appended at the end of this document to see examples of Unicast SNMPv2c results and detailed information about packets.

Set Active Discovery Unicast SNMPv3

Set Active Discovery Unicast SNMPv3 to search for devices and components with SNMPv3 requests. All components with an IPV4 address will be queried. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

Procedure

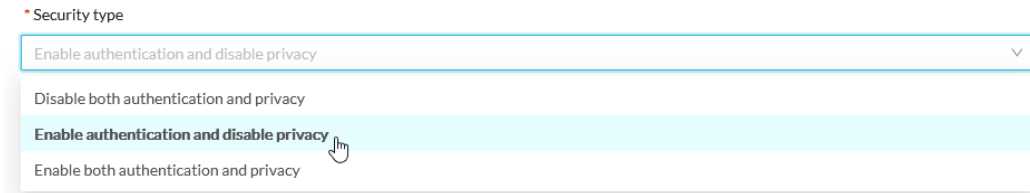
Step 1 Toggle the **Enable** button ON.
Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

Step 3 Type a community string for authentication.
The community string is defined by IT or network administrators. The value "public" is often used by default.
Step 4 Select the proper security and privacy level based on the information provided by the IT or network administrators.

All options available on SNMPv3 are implemented in Cisco Cyber Vision. Three security levels are available:

- **Disable both authentication and privacy.**

Only a username is requested for authentication.



* Security type

Enable authentication and disable privacy

Disable both authentication and privacy

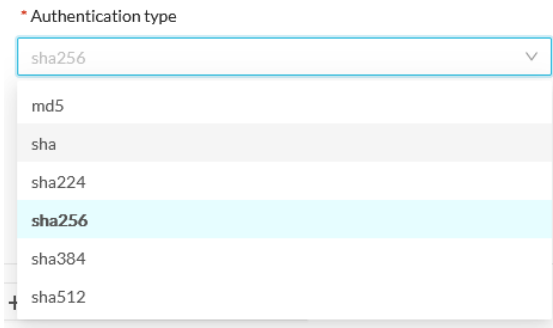
Enable authentication and disable privacy

Enable both authentication and privacy

- **Enable authentication and disable privacy.**

Authentication will be based on HMAC-MD5 or HMAC-SHA algorithms.

Select the algorithm to use and provide a username and an authentication password.



* Authentication type

sha256

md5

sha

sha224

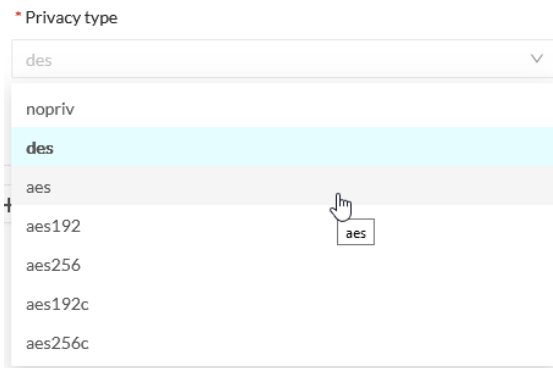
sha256

sha384

sha512

- **Enable both authentication and privacy.**

In addition to the previous level, a DES or AES encryption of the content is requested. Select the level of encryption to use and provide a username and an authentication password. In addition, you must provide a password used for the encryption.



* Privacy type

des

nopriv

des

aes

aes192

aes256

aes192c

aes256c

Step 5 Click **Save**.

Create an Active Discovery policy X

* Name:

Broadcast configuration

EtherNet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

SNMPv3 v

Enable

* Retry attempts * Timeout (in seconds)

User-based security model configuration

* Security type

* Username

* Authentication type * Authentication password

* Privacy type * Privacy password

The menu closes.

Step 6 Click **Create**.

Refer to the Annex appended at the end of this document to see examples of Unicast SNMPv3 results and detailed information about packets.

Set Active Discovery Unicast WMI

Set Active Discovery Unicast WMI (Windows Management Instrumentation) to collect Windows information like local-host names and operating system versions.

Procedure

Step 1 Toggle the **Enable** button ON.

Step 2 Leave the Retry attempts and Timeout settings with the default values (0 and 5).

Step 3 Enter a Windows user account and password with the suitable WMI rights.

An Active Directory user account for authentication on multiple hosts with single login credentials can also be used.

Unicast configuration

WMI

Enable

* Retry attempts * Timeout (in seconds)

* Username

* Password

+ Add protocol-specific configuration

Step 4 Click **Save**.

The menu closes.

Step 5 Click **Create**.

Modify a policy

Procedure

Step 1 Navigate to **Admin > Active Discovery > Policies**.

Step 2 Click the policy in the list you want to modify.

Name	Number of associated presets
enip_policy	0
snmpv2_policy	0
snmpv3_policy	0
ICMPv6_policy	1

An overlay appears with the policy's configurations.

Step 3 Click **Edit**, **Duplicate** or **Delete**.

If you clicked **Edit**, an Edit policy overlay appears.

Edit policy

Name: enip_policy

Broadcast configuration

EtherNet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

- > EtherNet/IP - Enabled ✎ 🗑
- > SNMPv2c - Enabled ✎ 🗑
- > SNMPv3 - Enabled ✎ 🗑

+ Add protocol-specific configuration

Cancel Update

Step 4 You can toggle the buttons ON/OFF to enable/disable broadcast protocols.

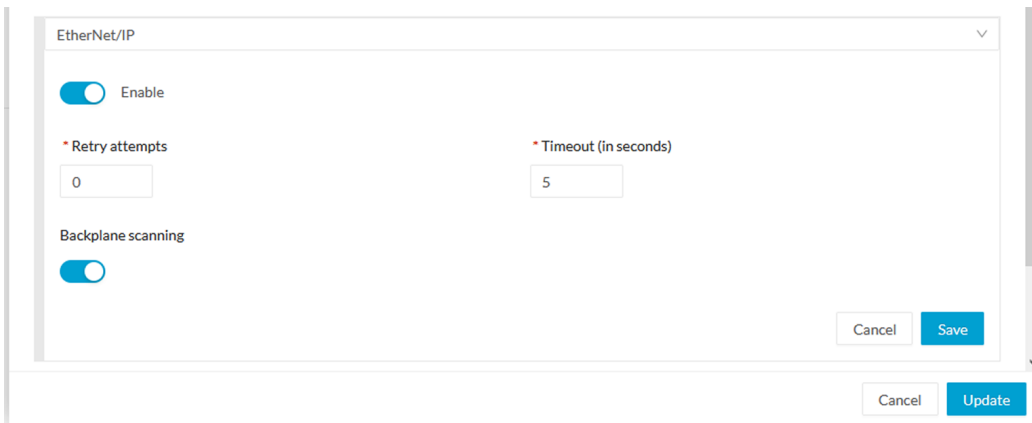
Step 5 Click the pencil button to edit Unicast protocols settings.

Unicast configuration

- Retry attempts: 0
 - Timeout: 5
 - Backplane scanning: enabled
- > SNMPv2c - Enabled ✎ 🗑

The Unicast configuration panels appears below the list of Unicast protocols.

Modify a policy



The screenshot shows a configuration dialog box titled "EtherNet/IP". It contains the following settings:

- Enable:** A toggle switch that is currently turned on.
- Retry attempts:** A text input field containing the value "0".
- Timeout (in seconds):** A text input field containing the value "5".
- Backplane scanning:** A toggle switch that is currently turned on.

At the bottom right of the dialog, there are two buttons: "Cancel" and "Save". Below the dialog box, there are two more buttons: "Cancel" and "Update".

Step 6 Make the necessary modifications.

Step 7 Click **Save**.

The overlay closes.

Step 8 Click **Update**.



CHAPTER 5

Profiles configuration

- [Set an Active Discovery profile, on page 31](#)

Set an Active Discovery profile

Set an Active Discovery profile by adding a policy, targeting IP addresses and arranging a schedule.

Procedure

- Step 1** On Cisco Cyber Vision, navigate to Admin > Active Discovery > Profiles.
- Step 2** Click the **Create profile** button.
- A form to create an Active Discovery profile pops up.
- Step 3** Give the profile a name.
- Step 4** Select a policy to base the profile on.

CREATE AN ACTIVE DISCOVERY PROFILE

* Name:

* Discovery policy:

- Step 5** Set target IP addresses: different options are available, such as:
- selecting a preset: the preset's device list will be used to list the IP addresses to be queried. In other words, the Active Discovery engine will use the IPv4 inside a component list to build its own list of components to check. You can use default and custom presets.
 - setting IP targets: you can directly add the IP addresses, IP ranges and subnets you want to be queried.
 - selecting sensors: all IP addresses detected by a sensor will be queried. You can also tick the **Use all sensors available** option.

Set an Active Discovery profile

Step 6 Optionally, you can arrange a schedule for Active Discovery to be launched. To do so:

- a) Toggle ON the **Schedule periodic discoveries** button.

Additional options to setup appear:

- b) Set a time range by selecting a start and end date and time.

The end date and time is optional. If you don't set it, Active Discovery will be launched endlessly.

- c) Set a frequency. You can set it to hourly, daily, weekly and monthly.

Step 7 Click **Create**.

The profile is added to the list and discovery is enabled by default if scheduling is set.



CHAPTER 6

Launch Active Discovery

- [Launch Active Discovery, on page 33](#)

Launch Active Discovery

Enable Active Discovery on the profiles created. You can run it once or launch the scheduling if it's paused.

Procedure

Step 1 On Cisco Cyber Vision, navigate to Admin > Active Discovery > Profiles.

Step 2 Click a profile in the list.

Name	Targets	Frequency	Scheduling Status	Last discovery
1a_Broadcast_Enip	No selected target	Daily	Paused	April 4, 2023 2:02 PM
1b_Unicast_Enip	IP: 192.168.20.0/24, 192.168.0.0/24	Daily	Paused	April 4, 2023 3:30 PM
2a_Broadcast_Siemens	No selected target	Daily	Paused	April 26, 2023 3:46 PM
2b_Unicast_Siemens	IP: 192.168.21.46/32, 192.168.21.50/32, 192.168.21.51/32	Daily	Paused	May 16, 2023 10:04 AM
3_Modbus_Vlan_22	IP ranges: 192.168.22.60-192.168.22.81	Daily	Paused	May 17, 2023 2:19 PM
4_Melsoft_Vlan_24	IP: 192.168.24.29/32	Daily	Paused	April 4, 2023 12:49 AM
5_BacNet_Vlan_30	IP: 192.168.30.0/24	Daily	Paused	April 4, 2023 5:50 PM
6_SNMP_V3	IP: 192.168.0.27/32	Daily	Paused	April 3, 2023 7:39 PM
7_SNMPV2C	IP: 192.168.0.25/32	Daily	Paused	May 16, 2023 11:16 AM
8_ICMP	No selected target	Daily	Paused	April 4, 2023 5:51 PM

Its right side panel opens.

Active Discovery profiles

From this page you can manage active discovery profiles.

Discovery profiles (14)

Name	Targets	Fr
1a_Broadcast_Enip	No selected target	D:
1b_Unicast_Enip	IP: 192.168.20.0/24, 192.168.0.0/24	D:
2a_Broadcast_Siemens	No selected target	D:
2b_Unicast_Siemens	IP: 192.168.21.46/32, 192.168.21.50/32, 192.168.21.51/32	D:
3_Modbus_Vlan_22	IP ranges: 192.168.22.60-192.168.22.81	D:
4_Melsoft_Vlan_24	IP: 192.168.24.29/32	D:
5_BacNet_Vlan_30	IP: 192.168.30.0/24	D:
6_SNMP_V3	IP: 192.168.0.27/32	D:
7_SNMPV2C	IP: 192.168.0.25/32	D:
8_ICMP	No selected target	D:

× 3_Modbus_Vlan_22

Target:

- 192.168.22.60-192.168.22.81

Discovery Policy: 4_Modbus

Sensors:

- IE3400-FCW2518PDAP

Scheduling: Paused ⓘ

Start time: February 24, 2023 4:49 PM

Periodicity: Daily

Actions:

[Edit](#)
[Delete](#)

[Run once](#)
[Resume scheduling](#)

Step 3 You can run the discovery once or resume scheduling.

- Click **Run once**.

Scheduling: Paused ⓘ

Start time: February 24, 2023 4:49 PM

Periodicity: Daily

Actions:

[Edit](#)
[Delete](#)

[Run once](#)
[Resume scheduling](#)

A message indicating that Active Discovery will be launched soon appears.

Scheduling: Paused ⓘ

Start time: February 24, 2023 4:49 PM

Periodicity: Daily

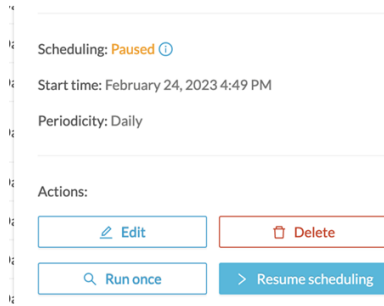
Actions:

✓ The discovery will be triggered soon, you can follow its progress in the discovery details of this profile

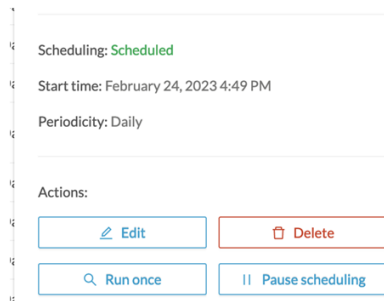
[Edit](#)
[Delete](#)

[Run once](#)
[Resume scheduling](#)

- Click **Resume scheduling**.



The scheduling status switches from paused to scheduled.

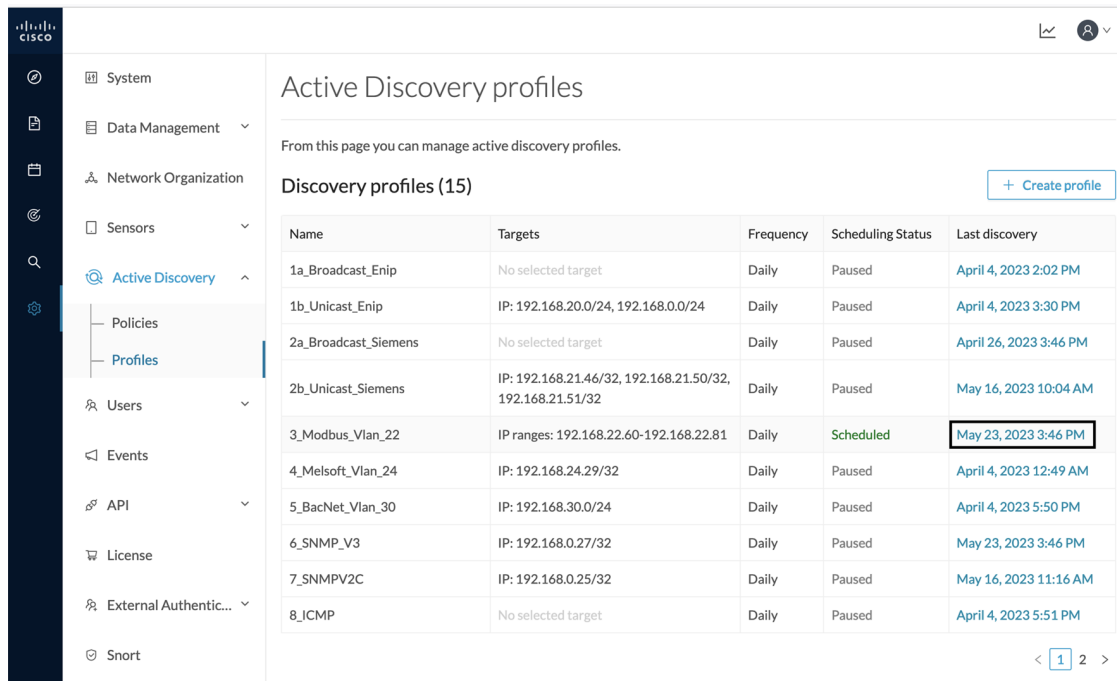


The discovery will be launched as configured.

You can change these configurations clicking **Edit**.

Step 4

You can click the link in the last discovery column to see a profile's Active Discovery results.



A window opens with the result details.

Last Active Discovery results ✕

Profile Name: 3_Modbus_Vlan_22
Start date: May 23, 2023 5:49 PM
End date: May 23, 2023 5:49 PM
Status: Finished

Sensor	Transmission mode	Protocol	Status	Start	End	Discovered devices
IE3400-FCW2518PDAP	unicast	Modbus	✓ Success	May 23, 2023 5:49 PM	May 23, 2023 5:49 PM	8

1-1 of 1 items < 1 >

Close



CHAPTER 7

Annex: Active Discovery protocols

All protocols implemented in the Active Discovery feature use standard packets commonly used by vendors. The system will never send requests on the network without a clear configuration made by the user. It is possible to schedule requests at a pre-defined frequency.


Discovered devices' responses will depend on the protocol implemented by the manufacturer and the user configuration. Except for what is clearly stated in this documentation, no specific configuration is required on discovered devices. Devices may give an answer by default, but it can vary in the field depending on the configuration.

This annex gives examples of the packets used by Cisco Cyber Vision to discover devices and of typical answers the user can expect.

- [BACnet, on page 38](#)
- [DNP3, on page 39](#)
- [EtherNet/IP, on page 39](#)
- [Melsec, on page 44](#)
- [Modbus, on page 45](#)
- [OMRON, on page 46](#)
- [Profinet Multicast, on page 46](#)
- [S7 Broadcast, on page 47](#)
- [S7 Unicast, on page 48](#)
- [S7Plus, on page 49](#)
- [ICMPv6 Multicast, on page 50](#)
- [SNMP Unicast, on page 50](#)
- [WMI, on page 58](#)

BACnet

Device



192.168.30.194
BacNet ▲ None
IP: 192.168.30.194
MAC: 00:a0:03:f5:6d:56

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:34:55 AM

Last activity
Jan 30, 2024 9:34:55 AM

Tags

- Controller
- Active Discovery BACnet

1
Activity

3
Events

7
Vulnerabilities

-
Credential

-
Variable

-
External Comm.

Basics
Risk score
Security
Activity
Automation

Properties
Components
Tags

Properties

Normalized Properties

fw-version: FW=01.21.67.272;WPC=1.8.22;SVS=300.8;SBC=13.23;

ip: 192.168.30.194

mac: 00:a0:03:f5:6d:56

model-name: PXM40.E

name: 192.168.30.194

project-version: AAS-20:AP=OpMon11_A.7.001;SU=SiUn;APT=OpMon11_A;APTV=7.001;

public-ip: no

vendor-name: Siemens Switzerland Ltd., I B T HVP

vlan-id: 30

Other Properties

bacnet-app-application-software-version: AAS-20:AP=OpMon11_A.7.001;SU=SiUn;APT=OpMon11_A;APTV=7.001;

bacnet-app-description: PXM40 11

bacnet-app-device-identifier: device-1

bacnet-app-device-name: PXM40

bacnet-app-firmware-revision: FW=01.21.67.272;WPC=1.8.22;SVS=300.8;SBC=13.23;

bacnet-app-location: B_01


bacnet-app-model-name: PXM40.E

name-ip: 192.168.30.194

vendor: Siemens Switzerland Ltd., I B T HVP

DNP3

Component



SEL-751
IP: 192.168.47.40
MAC: 00:30:a7:33:a6:1f
[Edit](#) | [Manage group](#)

First activity
Feb 1, 2024 5:31:22 PM

Last activity
Feb 5, 2024 12:19:59 PM

Tags

- ▶ Slave
- Activity tags**
- ▶ Active Discovery,
- ▶ Low Volume DNP3,
- ▶ EthernetIP

Other Properties

```

dnp3-device-hw-version: 751001G0X0X0
dnp3-device-id: SEL-751
dnp3-device-location: FEEDER RELAY
dnp3-device-manufacturer: SEL
dnp3-device-product-name-model: SEL751
dnp3-device-serial-number: 3230405000
dnp3-device-sw-version: 751-R302-V0-
enip-devicetype: CipDeviceTypeGene
enip-name: SEL-751-0
enip-serial: a733a61f
enip-status: SelfTesting/Unknwon
enip-vendor: Schweitzer Engineering
enip-version: 1.1
name-dnp3-device: SEL-751
name-enip: SEL-751-0
vendor: SCHWEITZER ENGINEERING

```

EtherNet/IP

Ethernet/IP Active Discovery can be performed by Cisco Cyber Vision using Broadcast or Unicast mode. In any case, requests sent and component properties collected in return will be the same. The main differences will be:

- Broadcast will discover all devices in the local LAN.
- Unicast will only discover the devices and components which have an IPv4 address.
- Unicast will search for, once an EtherNet/IP node is discovered, the devices' content. If a device is a chassis with a backplane, it will be queried and all modules will send their properties.

The EtherNet/IP command used is the List Identity request (0x00063). This command will be sent to the IPv4 broadcast address or directly to an IPv4 address or to a module inside a backplane behind an IPv4 address. The result whether in Broadcast or Unicast will always be the same CIP Identity response (0x000c) with the following properties:

#	Name	Cyber Vision Properties	Example
---	------	-------------------------	---------

1	Vendor ID	enip-vendor	Rockwell Automation/Allen-Bradley
2	Device Type	enip-devicetype	ProgrammableLogicController
3	Product Code	enip-productcode	235
4	Revision	enip-version	33.012
5	Status	enip-status	AtLeastOneIOConnectionInRunMode, MinorRecoverableFault, ReservedBits12-15:0x3
6	Serial Number	enip-serial	01105356
7	Product Name	enip-name	1756-L81ES/B

EtherNet/IP Broadcast or Unicast

A Broadcast Ethernet/IP Active Discovery consists of a packet sent by the sensor which requests EtherNet/IP identities to all devices in the local LAN. For example, a sensor with an Active Discovery IPv4 address 192.168.20.192/24 will send this EtherNet/IP request to the Broadcast address, here 192.168.20.255. All devices in the IPv4 range 192.168.20.0 to 192.168.20.254 will answer with the packet described above (CIP Identity response (0x000c)).

A direct Unicast Ethernet/IP (i.e. no backplane) will consist of the same request but sent directly to the device. When a preset is configured to query EtherNet/IP devices, the system will take the list of components of this preset which have an IPv4 address. Then, the Active Discovery engine will try to reach each IPv4 with this EtherNet/IP identities request. All reachable EtherNet/IP nodes of this list will answer with the packet described above (CIP Identity response (0x000c)).

In both cases (Broadcast and Unicast), the answer will be sent by the discovered devices to the sensor's Active Discovery network interface. The answer will be a UDP packet for the Broadcast request and some TCP packets for the Unicast request.

Figure 4: Example of properties received from a Rockwell Automation EtherNet/IP communication adapter (1756-EN2T):

The screenshot displays the 'Flow' view for a Rockwell Automation device. The device details include IP: 192.168.20.192, Port: 45896, MAC: 52:54:dd:61:05:d7, and device name 1756-EN2T/D with IP: 192.168.20.22, Port: 44818, and MAC: 5c:88:16:efd1:2e. Activity logs show first and last activity on Feb 9, 2022 at 3:00:57 PM. Tags include Active Discovery and Low Volume. The 'Properties' section is expanded, showing the following details:

enip-command: ListIdentity	enip-devicetype: CommunicationsAdapter
enip-event: Equipment	enip-location: Endpoint
enip-name: 1756-EN2T/D	enip-productcode: 0xa6
enip-serial: 0114f91d	enip-status: AtLeastOneIOConnectionInRunMode
enip-status-ra-major: RUN	enip-status-ra-minor: ???
enip-vendor: Rockwell Automation/Allen-Bradley	enip-version: 11.001
etherstype: IPv4	protocol: UDP

Figure 5: Example of properties received from a Rockwell Automation EtherNet/IP safety controller (1756-L81ES):

The screenshot displays the 'Flow' view for a Rockwell Automation device. The device details include IP: 192.168.20.192, Port: 47928, MAC: 52:54:dd:61:05:d7, and device name 1756-L81ES/B with IP: 192.168.20.25, Port: 44818, and MAC: 5c:88:16:edcc:8e. Activity logs show first and last activity on Feb 15, 2022 at 4:57:25 PM. Tags include Low Volume and EthernetIP. Summary statistics show 8 Packets and 1.071 Volume. The 'Properties' section is expanded, showing the following details:

enip-command: ListIdentity	enip-devicetype: ProgrammableLogicController
enip-event: Equipment	enip-location: Endpoint
enip-name: 1756-L81ES/B	enip-productcode: 0xd3
enip-serial: 01105356	enip-status: AtLeastOneIOConnectionInRunMode, MinorRecoverableFault, ReservedBits12-15: 0x3
enip-status-ra-major: REM	enip-status-ra-minor: RUN
enip-vendor: Rockwell Automation/Allen-Bradley	enip-version: 33.012
etherstype: IPv4	protocol: TCP

Figure 6: Example of properties received from a Schneider Electric EtherNet/IP controller (TM221ME16R):

The screenshot displays a network management interface for a device. The header section includes a gear icon, the IP address 192.168.22.192, and the device name TM221ME16R. It also shows the first and last activity times as Feb 9, 2022 3:02:08 PM. Tags include Active Discovery, Low Volume, and EthernetIP. The main section, titled 'Properties', contains the following table:

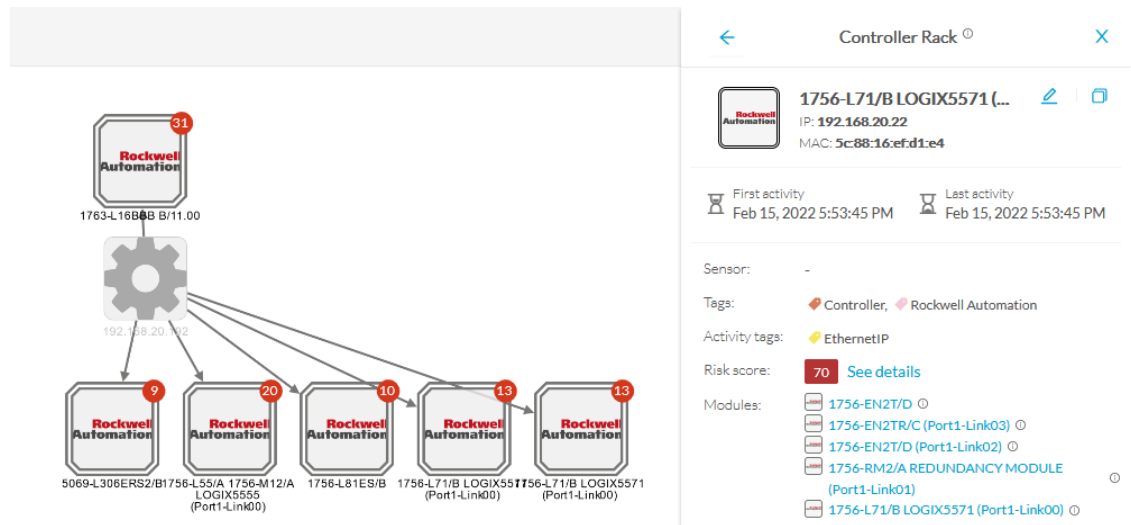
enip-command: ListIdentity	enip-devicetype: ProgrammableLogicController
enip-event: Equipment	enip-location: Endpoint
enip-name: TM221ME16R	enip-productcode: 0x1003
enip-serial: 08a48761	enip-status: Configured, AtLeastOneIOConnectionInRunMode
enip-status-ra-major: RUN	enip-status-ra-minor: ???
enip-vendor: Schneider Electric	enip-version: 1.6
etherstype: IPv4	protocol: UDP

Ethernet/IP backplane discovery

To browse backplanes, the Active Discovery policy with the Unicast EtherNet/IP protocol enabled needs to have the backplane discovery option set to enabled.

In such case, all EtherNet/IP nodes detected by Active Discovery Ethernet/IP Unicast will be queried again by the sensor. The sensor will try to know the backplane size and then send a request to the different modules (link addresses from 0 to the chassis size). All modules will then send their properties such as the product reference and the firmware version.

For example, an Ethernet/IP communication adapter with the IPv4 192.168.20.22 was first discovered. Then, all seven slots of the chassis backplane were queried. Four of them have answered back, which allowed Cisco Cyber Vision to build a Controller Rack:



A controller and a firmware version were discovered in the slot 0 of this backplane thanks to Active Discovery:

Properties

enip-cip-class: Connection Manager Object	enip-cip-request: true
enip-devicetype: ProgrammableLogicController	enip-event: Equipment
enip-location: Port1-Link00	enip-name: 1756-L71/B LOGIX5571
enip-productcode: 0x5c	enip-serial: 0115289b
enip-status: AtLeastOneIOConnectionInRunMode,ReservedBits12-15:0x3	enip-status-ra-major: REM
enip-status-ra-minor: RUN	enip-vendor: Rockwell Automation/Allen-Bradley
enip-version: 32.051	ethertype: IPv4
protocol: TCP	

Melsoft

Device



R08SFCPU

Mitsu ▲ None

IP: **192.168.24.29**

MAC: **10:4b:46:22:4a:c7**

[Edit](#) | [Manage group](#)



First activity
Jan 30, 2024 9:18:30 AM



Last activity
Jan 30, 2024 9:18:30 AM

Tags

◆ Controller

Activity tags

◆ Controller Info,

◆ Active Discovery,

◆ Mitsubishi Melsoft

- [Basics](#) [Risk score](#) [Security](#) [Activity](#)
- [Properties](#) [Components](#) [Tags](#)

Properties

Normalized Properties

fw-version: **16, 45, 03**

ip: **192.168.24.29**

mac: **10:4b:46:22:4a:c7**

model-name: **R60AD4, R08SFCPU, R65FM, R60DA4, RJ71EN71 RJ71GF11-T2**

name: **Unknown (Slot 5), RJ71GF11-T2 (Slot 2), Unknown (Slot 7), R08SFCPU, R65FM (Slot 1), R60DA4 (Slot 6), RJ71EN71(E+CCIEF (Slot 3)**

public-ip: **no**


serial-number: **4516721160010631, 00016C2611210481, 030616045C11F6010061, 16055C1180010061, 030767175021054517721760110661, 00026C1315C10031**

vendor-name: **Mitsubishi Electric Corporation**

vlan-id: **24**

Modbus

Device



BME H58 2040S
 Schneider ▲ None
 IP: **192.168.22.76**
 MAC: **00:00:54:2f:fd:87**
[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:12:01 AM

Last activity
Jan 30, 2024 9:12:01 AM

Tags

- Controller
- Controller Info,
- Active Discovery Modbus

~ 1
Activity

-
Credential

[Basics](#)
[Risk score](#)
[Security](#)
[Activity](#)
[Automation](#)

[Properties](#)
[Components](#)
[Tags](#)

Properties

Normalized Properties

fw-version: **3.10.400**

hw-version: **16**

ip: **192.168.22.76**

mac: **00:00:54:2f:fd:87**

model-name: **BME H58 2040S**

model-ref: **BME H58 2040S**

name: **BME H58 2040S**

project-name: **Projet**

project-version: **0.0.43**

Other Properties

modbus-major-minor-revision: **v03.10**

modbus-product-code: **BME H58 2040S**

modbus-vendor-name: **Schneider Electric**

name-umas-cpu: **BME H58 2040S**

umas-engineering-station: **DESKTOP-E139G20**

umas-fw-version: **3.10.400**

umas-hardware-id: **2020d0e**

umas-hw-version: **16**

umas-libset-version: **V14.1**

OMRON

Device

192.168.45.85

Omron ▲ None

IP: **192.168.45.85**

MAC: **00:00:0a:d6:68:62**

[Edit](#) | [Manage group](#)

First activity
Jan 30, 2024 9:33:30 AM

Last activity
Jan 30, 2024 9:33:35 AM

Tags

Controller, OMRON

Activity tags

Controller Info, Active Discovery **FINS**

Activity 1

Credential -

Basics Risk score Security Activity Automation

Properties Components Tags

Properties

Normalized Properties

fw-version: 1.41.02

ip: 192.168.45.85

mac: 00:00:0a:d6:68:62

model-name: NX1P2-9024DT1

name: 192.168.45.85

public-ip: no

serial-number: 7444

vendor-name: OMRON TATEISI ELECTRONICS CO.

vlan-id: 45

Other Properties

name-ip: 192.168.45.85

omron-lot-id: --- 29720

omron-model: NX1P2-9024DT1

omron-serial: 7444

omron-version: 1.41.02

vendor: OMRON TATEISI ELECTRONICS CO.

Profinet Multicast

Cisco Cyber Vision Active Discovery can use a Profinet DCP service called Identify Request. This request will be sent by the sensor interfaces defined for Active Discovery. All Profinet devices will answer with a specific Profinet DCP identify response packet.

The request is sent by the sensor MAC address to a specific Ethernet Multicast address: 01:0e:cf:00:00:00. This Profinet DCP Multicast address will allow Cisco Cyber Vision to join all Profinet nodes on the local LAN. The answer of each node will be a specific Profinet DCP packet sent to the sensor MAC address.

The information collected are:

- The IP address + mask.
- The Manufacturer name.
- The name of the station.

Figure 7: For example, a Siemens S7-1500 controller:

Flow

52:54:dd:61:05:d7
IP: -
MAC: 52:54:dd:61:05:d7

SIEMENS

s7-1500rxrh-systemxb1.p...
IP: 192.168.21.50
MAC: ac:64:17:a6:37:54

First activity
Feb 16, 2022 1:19:01 PM

Last activity
Feb 16, 2022 1:19:22 PM

Tags
Active Discovery,
Profinet, Profinet DCP

Basics

Properties Content Statistics Tags

Properties

ethertype: PROFINET	profinetdcp-devicegw: 192.168.21.254
profinetdcp-deviceip: 192.168.21.50	profinetdcp-devicenetmask: 255.255.255.0
profinetdcp-manufacturername: S7-1500	profinetdcp-nameofstation: s7-1500rxrh-systemxb1.plcxb1.profinetxinterfacexb23431
profinetdcp-service-id: Identify	protocol:

S7 Broadcast

Cyber Vision Active Discovery can use a request on the protocol S7 discovery with a command: "identification". This request will be sent by the sensor interfaces defined for Active Discovery. All S7 devices will answer with a specific S7 Discovery identification response packet.

The request is sent by the sensor MAC address to the Ethernet broadcast address: ff:ff:ff:ff:ff:ff. The answer of each S7 protocol capable node will be a specific S7 discovery packet sent by the device MAC address to the sensor MAC address.

The information collected are:

- The model name.
- The name of the device.

Figure 8: For example, a Siemens S7-300 controller:

Flow

52:54:dd:c1:f1:ed
IP: -
MAC: 52:54:dd:c1:f1:ed

SIMATIC 300
IP: -
MAC: 08:00:06:92:c1:84

First activity
Feb 16, 2022 2:19:50 PM

Last activity
Feb 16, 2022 2:20:10 PM

Tags
Active Discovery
S7Discovery

Basics
Properties Content Statistics Tags

Properties

ethertype: LLC	protocol:
s7discovery-command: identification	s7discovery-devicename: SIMATIC 300
s7discovery-model: S7-300 CP	s7discovery-type: response
snap-org-code: 0x080006	snap-org-name: Siemens
snap-protocol-id: 0x1fd	

S7 Unicast

The Active Discovery engine uses a specific S7 Unicast command to request properties from S7-compatible devices, such as:

- Hardware reference
- Firmware version

Basics Security Activity Automation

Properties Tags Sensors

Properties

Normalized Properties	Other Properties
fw-version: V 2.2.0	name-profinet: project-s7-1200
hw-version: 1	profinetdcp-devicerole: IO-Controller
ip: 192.168.21.41	profinetdcp-manufacturer-specific: S7-1200
mac: 00:1c:06:00:88:19	s7-fwver: V 2.2.0
model-ref: 6ES7 214-1AE30-0XB0	s7-hwref: 6ES7 214-1AE30-0XB0
name: project-s7-1200	s7-hwver: 1
public-ip: no	s7-moduleref: 6ES7 214-1AE30-0XB0
vendor-name: Siemens Numerical Control Ltd., Nanjing	s7-modulever: 1
	s7-rack: 0
	s7-slot: 0
	vendor: Siemens Numerical Control Ltd., Nanjing

S7Plus

Device

PLC_2

Siemens ▲ None

IP: 192.168.21.50

MAC: ac:64:17:a6:37:54

[Edit](#) | [Manage group](#)

🕒 First activity
Jan 30, 2024 8:59:41 AM

🕒 Last activity
Jan 30, 2024 10:45:22 AM

Tags

- 🔗 Controller
- Activity tags
- 🔗 Active Discovery,
- 🔗 Profinet, 🔗 Profinet DCP,
- 🔗 S7 S7Plus

Other Properties

ComponentType: virtual

cotp-dst-tsap: SIMATIC-ROOT-ES, 101

name-s7-plc: PLC_2

profinetdcp-manufacturer-specific: S7-1500

profinetdcp-nameofstation: s7-1500rxrh-systemxb1.plcxb1.profinetxainte

s7-fwver: V 2.9.4

s7-hwver: 1

s7-modulename: PLC_2

s7-moduleref: 6ES7 515-2RM00-0AB0

s7-plcname: PLC_2

s7-rack: 0

s7-serialnumber: S C-M6DA37162020

s7-slot: 0, 1

s7plus-moduleref: 6ES7 515-2RM00-0AB0

vendor: Siemens AG

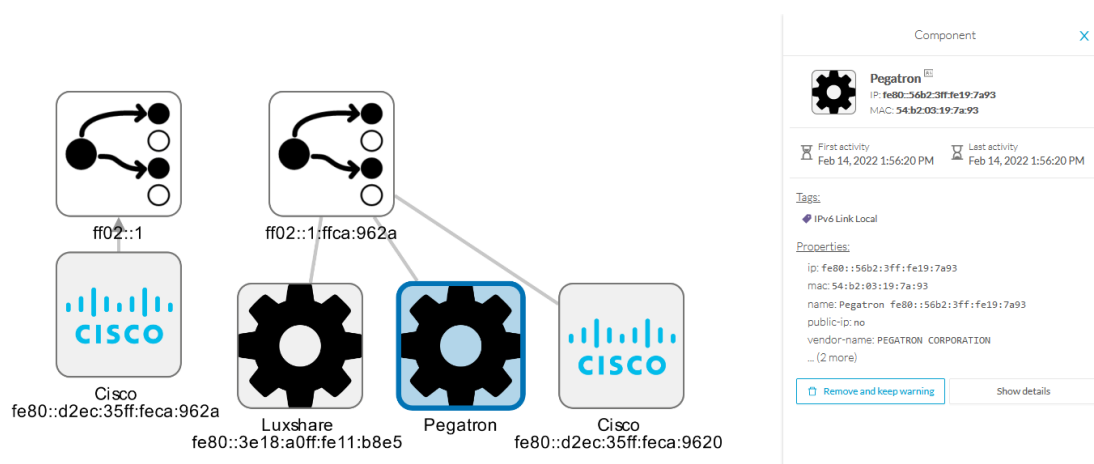
ICMPv6 Multicast

For the ICMPv6 Active Discovery protocol, the Cisco Cyber Vision sensor will use an ICMPv6 Echo request (ping) to the all-nodes link-local scope multicast address. The sensor will thus ping all IPv6 nodes on the local link. All reachable nodes will answer back with their link-local IPv6 address and their MAC address.

Cisco Cyber Vision sensors use a specific ICMPv6 packet, echo request (type 128) to the address `ff02::1` (All nodes on the local network segment) with a hop limit of 1.

The different nodes will answer with a ICMPv6 Neighbor solicitation (type 135) to the Solicited-Node Multicast address which has the form `ff02::1::ff` with the least-significant 24 bits of the sensor IPv6 Unicast address.

Figure 9: For example, a sensor with IPv6: `fe80::d2ec:35ff:feca:962a` is requesting `ff02::1`. Three different devices are answering back:



SNMP Unicast

Cisco Cyber Vision sensor can use the SNMP protocol to collect network devices information.

SNMP Active Discovery results highly depend on the configuration, type and version of the queried devices. Some devices might respond without any specific configuration, others might need complex configurations, and others not respond at all.

While doing SNMP Active Discovery, the sensor will try to read some generic and vendor-specific values. The generic values will be used by the sensor to build extra queries based on vendors and hardware models.

Generic values collected are:

Property	Description
snmp-sys-descr	Description
snmp-sys-name	Name

The Cisco Cyber Vision sensor Active Discovery supports:

- SNMP Version 2c (SNMPv2c) with a fallback in SNMP Version 1 (SNMPv1).

- SNMP Version 3 (SNMPv3).

SNMPv3 Active Discovery is able to provide authentication and encryption.

All SNMP versions will give the same results in the Cisco Cyber Vision application. They are important regarding data access. The subsequent section describes the SNMP results with different types of network devices.

AD SNMP with Schneider PLC

The Cisco Cyber Vision SNMP Active Discovery with Schneider Electric PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two network nodes discovered by Cisco Cyber Vision. Each node's details are shown in a 'Flow' view and a 'Properties' view.


Node 1: BMEP581020

- IP: 192.168.22.192
- Port: 58600
- MAC: 52:54:00:61:05:d7
- First activity: Feb 16, 2022 4:31:20 PM
- Last activity: Feb 16, 2022 4:31:20 PM
- Tags: Net Management, Active Discovery, SNMP
- Properties:
 - ethertype: IPv4
 - protocol: UDP
 - snmp-command: get-request
 - snmp-community: public
 - snmp-sys-descr: Modicon M580 - P58 1020 Processor - DIO
 - snmp-sys-name: BMEP581020
 - snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.46
 - snmp-sys-services: 74
 - snmp-version: v2c


Node 2: BMENOC0301

- IP: 192.168.22.192
- Port: 36281
- MAC: 52:54:00:61:05:d7
- First activity: Feb 16, 2022 4:31:30 PM
- Last activity: Feb 16, 2022 4:31:31 PM
- Tags: Net Management, Active Discovery, SNMP
- Properties:
 - ethertype: IPv4
 - protocol: UDP
 - snmp-command: get-request
 - snmp-community: public
 - snmp-sys-descr: Product: BMENOC0301 - Ethernet Communication Module, FwId 02.16
 - snmp-sys-name: BMENOC0301
 - snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.53
 - snmp-sys-services: 74
 - snmp-version: v2c

Flow



192.168.22.192
IP: 192.168.22.192
Port: 33685
MAC: 52:54:00:61:05:d7



TM262-15
IP: 192.168.22.73
Port: 161
MAC: 00:80:14:4e:86:f5

First activity
Feb 16, 2022 4:30:49 PM

Last activity
Feb 16, 2022 4:30:49 PM

Tags

- Net Management,
- Active Discovery, SNMP

Basics

Properties Content Statistics Tags

Properties


ethertype: IPv4	protocol: UDP
snmp-command: getBulkRequest	snmp-community: public
snmp-sys-descr: SCHNEIDER M262 Fast Ethernet TCP/IP	snmp-sys-name: TM262-15
snmp-sys-objectid: 1.3.6.1.4.1.3833.1.7.255.44	snmp-sys-services: 4
snmp-version: v2c	

AD SNMP with Siemens PLC


The Cisco Cyber Vision SNMP Active Discovery with Siemens PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

Flow



192.168.21.192
IP: 192.168.21.192
Port: 48006
MAC: 52:54:00:61:05:d7



project-s7-1200
IP: 192.168.21.41
Port: 161
MAC: 00:1c:06:00:88:19

First activity
Feb 16, 2022 4:18:30 PM

Last activity
Feb 16, 2022 4:18:30 PM

Tags

- Net Management,
- Active Discovery, SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Siemens, SIMATIC S7, CPU-1200, 6ES7 214-1AE30-0XB0, HW: 1, FW: V.2.2.0, SZVX7YYW002898	snmp-sys-objectid: 0.0
snmp-sys-services: 76	snmp-version: version-1

Flow



192.168.21.192
IP: 192.168.21.192
Port: 35904
MAC: 52:54:00:61:05:d7



cpu1512-sp
IP: 192.168.21.46
Port: 161
MAC: ac:64:17:81:21:3c

First activity
Feb 16, 2022 4:18:50 PM

Last activity
Feb 16, 2022 4:18:50 PM

Tags

- ◆ Net Management,
- ◆ Active Discovery, ◆ SNMP

Basics

Properties Content Statistics Tags

Properties


ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019	snmp-sys-objectid: 0.0
snmp-sys-services: 78	snmp-version: version-1

AD SNMP with Rockwell PLC


The Cisco Cyber Vision SNMP Active Discovery with Rockwell Automation PLC requests generic values (snmp-sys-descr and snmp-sys-name).

Typical results with nodes where SNMP is enabled by default are:

Flow



192.168.20.192
IP: 192.168.20.192
Port: 40265
MAC: 52:54:00:61:05:d7



1756-ENBT/A
IP: 192.168.20.20
Port: 161
MAC: 00:00:bc:5f:bc:ce

First activity
Feb 16, 2022 4:09:20 PM

Last activity
Feb 16, 2022 4:09:20 PM

Tags

- ◆ Net Management,
- ◆ Active Discovery, ◆ SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4	protocol: UDP
snmp-command: get-request	snmp-community: public
snmp-sys-descr: Rockwell Automation 1756-ENBT	snmp-sys-objectid: 1.3.6.1.4.1.95.1.12
snmp-sys-services: 79	snmp-version: v2c

AD SNMP with Moxa switches

The Cisco Cyber Vision SNMP Active Discovery with Moxa switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-moxapriv-model-name	Model

snmp-moxapriv-fw-version	Firmware version
--------------------------	------------------

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two nodes in a network management interface. Each node has a 'Flow' header and a 'Properties' section. The first node is a 'Managed Redundant Switch' with IP 192.168.0.192 and port 36532. The second node is a 'Moxa' switch with IP 192.168.0.28 and port 48394. Both nodes show their respective SNMP properties, including community name, model name, and system description.

Node 1: Managed Redundant Switch

- IP: 192.168.0.192
- Port: 36532
- MAC: 52:54:dd:c1:f1:ed
- SNMP Community: public
- SNMP Model Name: EDS-405A-SS-SC
- SNMP System Name: Managed Redundant Switch 09866
- SNMP System Description: MOXA EDS-405A-SS-SC
- SNMP System Object ID: 1.3.6.1.4.1.8691.7.6
- SNMP Version: v2c

Node 2: Moxa 192.168.0.28

- IP: 192.168.0.28
- Port: 48394
- MAC: 00:90:e8:5c:f9:84
- SNMP Community: public
- SNMP Model Name: EDS-G508E
- SNMP System Name: EDS-G508E
- SNMP System Description: EDS-G508E
- SNMP System Object ID: 1.3.6.1.4.1.8691.7.69
- SNMP Version: v2c

AD SNMP with Siemens Switches

The Cisco Cyber Vision SNMP Active Discovery with Siemens switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-siemens-scalence-model-ref	Model
snmp-siemens-scalence-model-version	Firmware version

Typical results with nodes where SNMP is enabled by default are:

Flow

192.168.0.192
IP: 192.168.0.192
Port: 43342
MAC: 52:54:dd:c1:f1:ed

SIEMENS SCALANCE X-300
IP: 192.168.0.35
Port: 161
MAC: 00:0e:8c:9a:d9:2c

First activity
Feb 16, 2022 4:23:20 PM

Last activity
Feb 16, 2022 4:23:21 PM

Tags
Net Management, Active Discovery, SNMP

Basics

Properties Content Statistics Tags

Properties

ethertype: IPv4 protocol: UDP

snmp-command: getBulkRequest snmp-community: public

snmp-siemens-scalence-model-ref: 6GK5 308-2FL00-2AA3 snmp-siemens-scalence-model-version: V2.2.0

snmp-sys-descr: SCALANCE X-300 snmp-sys-name: S10-4-S

snmp-sys-objectid: 1.3.6.1.4.1.4196.1.1.5.4 snmp-sys-services: 14

snmp-version: v2c

AD SNMP with Hirschmann hardware

The Cisco Cyber Vision SNMP Active Discovery with Hirschmann switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-hmpriv-mgmt-model-ref	Model
snmp-hmpriv-mgmt-fw-version	Firmware version
snmp-hm2-indus-model-ref	Model
snmp-hm2-indus-fw-version	Firmware version
snmp-hm-disc-fw-version	Model
snmp-hm-disc-model-ref	Firmware version

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two flow details for SNMP requests. Each flow includes a gear icon, IP address (192.168.0.192), port, MAC address, a host icon, device name, IP, port, MAC, activity timestamps, and tags (Net Management, Active Discovery, SNMP). Below each flow is a 'Properties' section with tabs for Basics, Properties, Content Statistics, and Tags. The 'Properties' section lists various SNMP-related attributes.

Flow 1: BRS-646038BF9AE

- IP: 192.168.0.192, Port: 33687, MAC: 52:54:00:1c:1f:1e
- Device: BRS-646038BF9AE, IP: 192.168.0.32, Port: 161, MAC: 64:60:38:bf:f9:ae
- First activity: Feb 17, 2022 11:12:15 AM
- Last activity: Feb 17, 2022 11:12:15 AM
- Tags: Net Management, Active Discovery, SNMP
- Properties:
 - ethertype: IPv4, protocol: UDP
 - snmp-command: getBulkRequest, snmp-community: public
 - snmp-hm-disc-fw-version-raw: H105-25-08.5.00 2020-11-26 16:52, snmp-hm-disc-model-ref: BRS30-08040000-STCZ99HHSES
 - snmp-hm2-indus-fw-version: 08.5.00, snmp-hm2-indus-model-ref: BRS30-08040000-STCZ99HHSES
 - snmp-sys-descr: Hirschmann BOBCAT, snmp-sys-name: BRS-646038BF9AE
 - snmp-sys-objectid: 1.3.6.1.4.1.248.11.2.1.15, snmp-sys-services: 2
 - snmp-version: v2c

Flow 2: RS-58AB3C

- IP: 192.168.0.192, Port: 40150, MAC: 52:54:00:1c:1f:1e
- Device: RS-58AB3C, IP: 192.168.0.31, Port: 161, MAC: ece:55:58:ab:3c
- First activity: Feb 17, 2022 11:12:15 AM
- Last activity: Feb 17, 2022 11:12:15 AM
- Tags: Net Management, Active Discovery, SNMP
- Properties:
 - ethertype: IPv4, protocol: UDP
 - snmp-command: getBulkRequest, snmp-community: public
 - snmp-hmpriv-mgmt-fw-version: 07.1.05, snmp-hmpriv-mgmt-model-ref: RS30-08021T1SDAEHH
 - snmp-sys-descr: Hirschmann Railswitch, snmp-sys-name: RS-58AB3C
 - snmp-sys-objectid: 1.3.6.1.4.1.248.14.10.41, snmp-sys-services: 2
 - snmp-version: v2c

AD SNMP with Cisco hardware

The Cisco Cyber Vision SNMP Active Discovery with Cisco Hardware demands some specific configurations on the device side and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-ent-physical-model-name	Model
snmp-ent-physical-entry	Description
snmp-ent-physical-serial-number	Serial number

snmp-probe-software-rev	Firmware version
-------------------------	------------------

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays two nodes in the Cisco Cyber Vision Active Discovery interface. Each node card shows a gear icon, IP address (192.168.0.192), port (39933), MAC address (52:54:00:11:11:11), and a Cisco logo with model name (IE3300Mitsubishi.ccv). Activity logs show first and last activity on Feb 17, 2022 at 10:33:05 AM. Tags include Net Management, Active Discovery, and SNMP.

Below each node card is a 'Basics' tab with a 'Properties' section. The properties are as follows:

Node 1 (IE3300Mitsubishi.ccv)	Node 2 (IE34R0CPLC.ccv)
ether-type: IPv4	ether-type: IPv4
protocol: UDP	protocol: UDP
snmp-command: get-request	snmp-command: get-request
snmp-community: public	snmp-community: public
snmp-ent-physical-entry: IE-3300-8T2X Expandable Non-PoE Chassis	snmp-ent-physical-entry: IE-3400-8T2S Expandable Advanced Non-PoE Chassis
snmp-ent-physical-model-name: IE-3300-8T2X	snmp-ent-physical-model-name: IE-3400-8T2S
snmp-ent-physical-serial-number: FCW2435P3L2	snmp-ent-physical-serial-number: FOC2401V07N
snmp-probe-software-rev: 17.3.1	snmp-probe-software-rev: 17.4.1
snmp-sys-descr: Cisco IOS Software [Amsterdam], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.3.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Fri 07-Aug-20 19:15 by mcp	snmp-sys-descr: Cisco IOS Software [Bengaluru], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.4.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Thu 26-Nov-20 21:57 by mcp
snmp-sys-name: IE3300Mitsubishi.ccv	snmp-sys-name: IE34R0CPLC.ccv
snmp-sys-objectid: 1.3.6.1.4.1.9.1.3007	snmp-sys-objectid: 1.3.6.1.4.1.9.1.2872
snmp-sys-services: 6	snmp-sys-services: 6
snmp-version: v2c	snmp-version: v2c

AD SNMP with Microsoft Windows OS

The Cisco Cyber Vision SNMP Active Discovery with Microsoft Windows stations demands a specific operating system configuration and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-primary-domain-name	Domain name of the machine

Typical results with nodes where SNMP is enabled by default are:

The screenshot displays a network flow analysis interface. At the top, it shows a flow between two hosts: 192.168.0.192 (Port: 41716, MAC: 52:54:00:11:11:11) and AVEVASRV (IP: 192.168.0.51, Port: 161, MAC: 00:50:56:8F:4a:3c). The flow is tagged with 'Net Management', 'Active Discovery', and 'SNMP'. The 'Properties' section is expanded, showing the following details:

ethertype: IPv4	protocol: UDP
snmp-command: getBulkRequest	snmp-community: public
snmp-primary-domain-name: LAB-AUTOM-CCV	snmp-sys-descr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)
snmp-sys-name: AVEVASRV.lab-autom-ccv.local	snmp-sys-objectid: 1.3.6.1.4.1.311.1.1.3.1.2
snmp-sys-services: 76	snmp-version: v2c

WMI

WMI is used to collect the following Windows hosts' properties.

- wmi-caption: operating system's name and version
- wmi-kb-list: security updates installed in the host
- wmi-last-update: latest update date
- wmi-name: host name

Properties	
Normalized Properties	Other Properties
ip: 192.168.44.203	name-ip: 192.168.44.203
mac: 00:50:56:8f:12:51	vendor: VMware, Inc.
name: 192.168.44.203	wmi-caption: Microsoft Windows 10 Enterprise
os-name: Windows 10 Enterprise	wmi-kb-list: KB5012170 (Security Update)
public-ip: no	wmi-last-update: 3/8/2023
vendor-name: Microsoft Corporation	wmi-name: WMLAB1003LOC
	wmi-organization: escalation
	wmi-os-arch: 64-bit
	wmi-os-serial: 00329-00000-00003-AA417
	wmi-proc-architecture: x64
	wmi-proc-name: Intel(R) Xeon(R) Platinum 8260 CPU @ 2.40GHz
	wmi-service-pack-major-version: 0
	wmi-service-pack-minor-version: 0
	wmi-windows-build-number: 19044
	wmi-windows-sku: 4

