

Cisco Cyber Vision Active Discovery Configuration Guide, Release 5.2.x

First Published: 2022-05-06

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

Short Description ?

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

Set Active Discovery Broadcast 5

CHAPTER 3 **Sensor configuration** 7

Configure Active Discovery on a Cisco switch or router 7

Configure Active Discovery on a Cisco IC3000 11

Configure Active Discovery on a Docker Sensor 15

Configure Active Discovery on a Center Interface 15

CHAPTER 4 **Policies configuration** 17

Create a Policy 17

Set Active Discovery Broadcast 17

Set Active Discovery Unicast 18

Set Active Discovery Unicast BACnet 19

Set Active Discovery Unicast Beckhoff 19

Set Active Discovery Unicast DNP3 20

Set Active Discovery Unicast EtherNet/IP 20

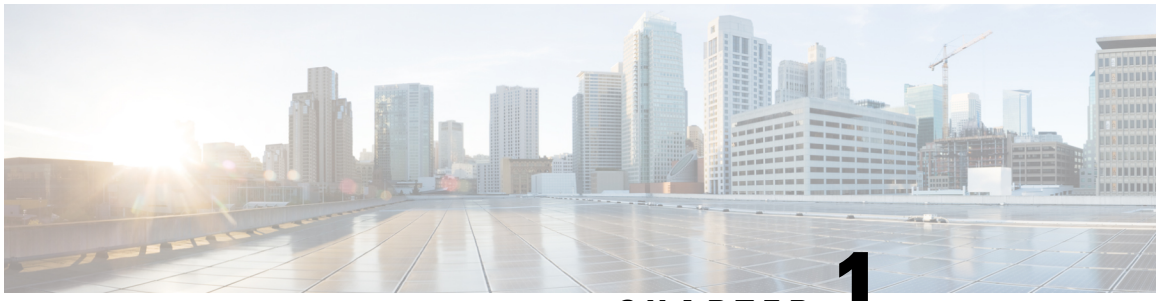
Set Active Discovery Unicast GESRTP 21
Set Active Discovery Unicast HTTP or HTTPS 21
Set Active Discovery Unicast Melsoft 21
Set Active Discovery Unicast MMS 22
Set Active Discovery Unicast Modbus 22
Set Active Discovery Unicast OMRON 23
Set Active Discovery Unicast SiemensS7 23
Set Active Discovery Unicast SiemensS7plus 24
Set Active Discovery Unicast SNMPv2c 24
Set Active Discovery Unicast SNMPv3 25
Set Active Discovery Unicast WMI 26
Edit, Duplicate, and Delete Policy 26

CHAPTER 5 **Profiles configuration** 29
Set an Active Discovery profile 29

CHAPTER 6 **Launch Active Discovery** 31
Launch Active Discovery 31

CHAPTER 7 **Annex: Active Discovery protocols** 35
BACnet 36
Beckhoff 36
DNP3 37
EtherNet/IP 38
EtherNet/IP Broadcast or Unicast 39
Ethernet/IP backplane discovery 40
GESRTP 42
HTTP-HTTPS 42
Melsoft 43
Modbus 44
OMRON 45
Profinet Multicast 45
S7 Broadcast 46
S7 Unicast 47

S7Plus 48
ICMPv6 Multicast 49
SNMP Unicast 49
AD SNMP with Schneider PLC 50
AD SNMP with Siemens PLC 51
AD SNMP with Rockwell PLC 52
AD SNMP with Moxa switches 52
AD SNMP with Siemens Switches 53
AD SNMP with Hirschmann hardware 54
AD SNMP with Cisco hardware 55
AD SNMP with Microsoft Windows OS 56
WMI 57



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 **Cisco Cyber Vision Center Sensor/Center, Release 5.2.x**.

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
- Cisco Center Active Discovery Interface

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.



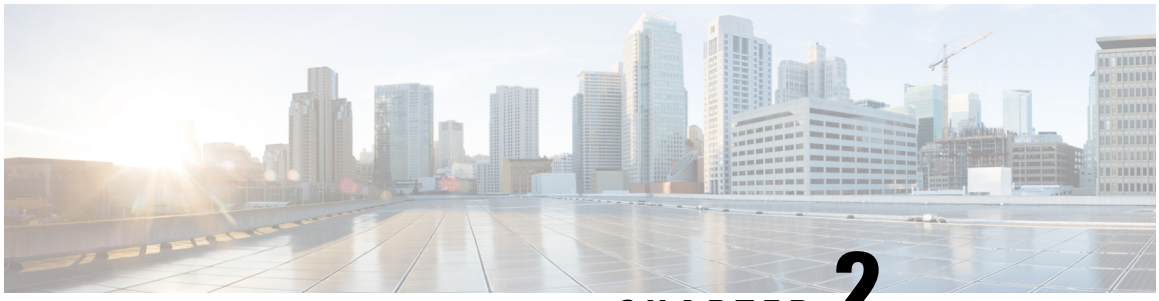
Warning Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.



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
- Set Active Discovery Broadcast, on page 5

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
  - Beckhoff
  - EtherNet/IP
  - Profinet
  - SiemensS7
  - ICMPv6
- Unicast
  - BacNet
  - Beckhoff
  - DNP3

- EtherNet/IP
- GESRTP
- HTTP-HTTPS
- Melsoft
- Modbus
- Omron
- SiemensS7
- SiemensS7Plus
- SNMPv2c
- SNMPv3
- WMI

For more information about discoverable properties, refer to Annex: Active Discovery protocols, on page 35.

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.

Set Active Discovery Broadcast

Before you begin

Active Discovery works with the following Broadcast protocols:

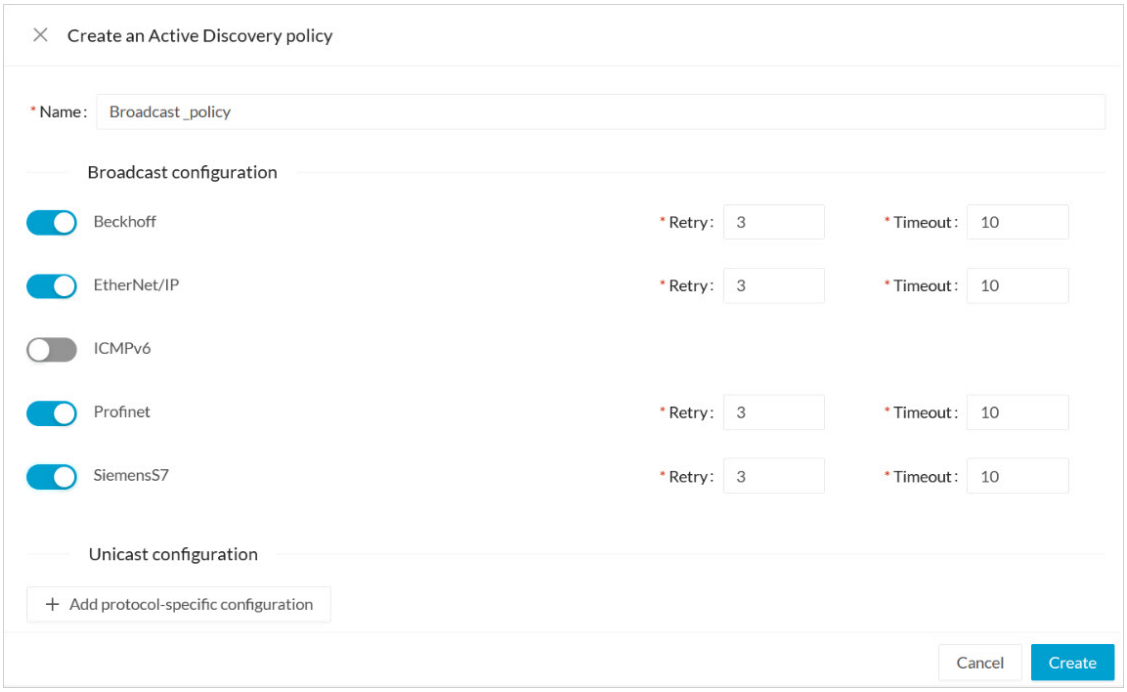
- Beckhoff
- EtherNet/IP
- ICMPv6
- Profinet
- Siemens S7

The sensor will send requests on all specified interfaces.

Procedure

Step 1 Add a policy name in Name field.

Step 2 Toggle the Broadcast protocol ON to enable Active Discory on these protocols.

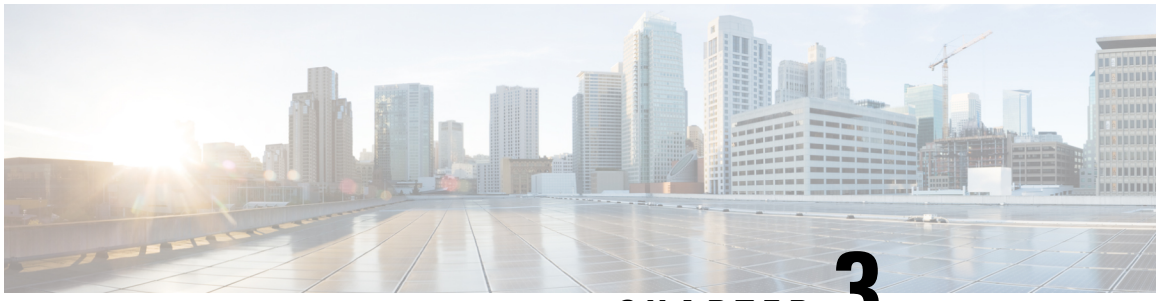


Step 3 Keep the Retry and Timeout settings at their default values (3 and 10).

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.



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 7
- Configure Active Discovery on a Cisco IC3000, on page 11
- Configure Active Discovery on a Docker Sensor, on page 15
- Configure Active Discovery on a Center Interface, on page 15

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

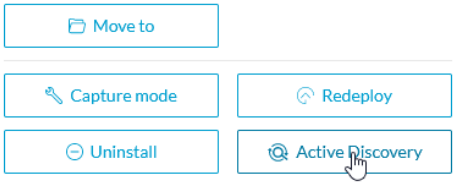
Step 1 Navigate to **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

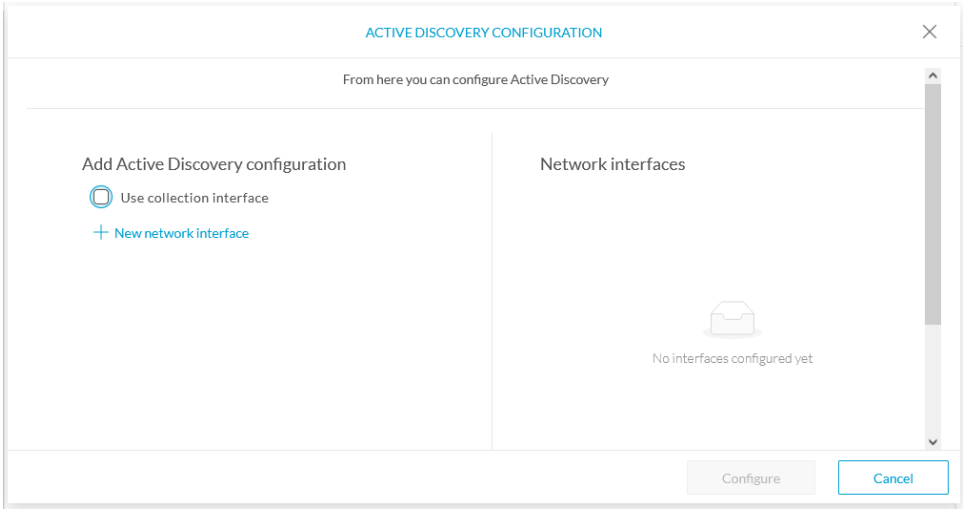
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

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.

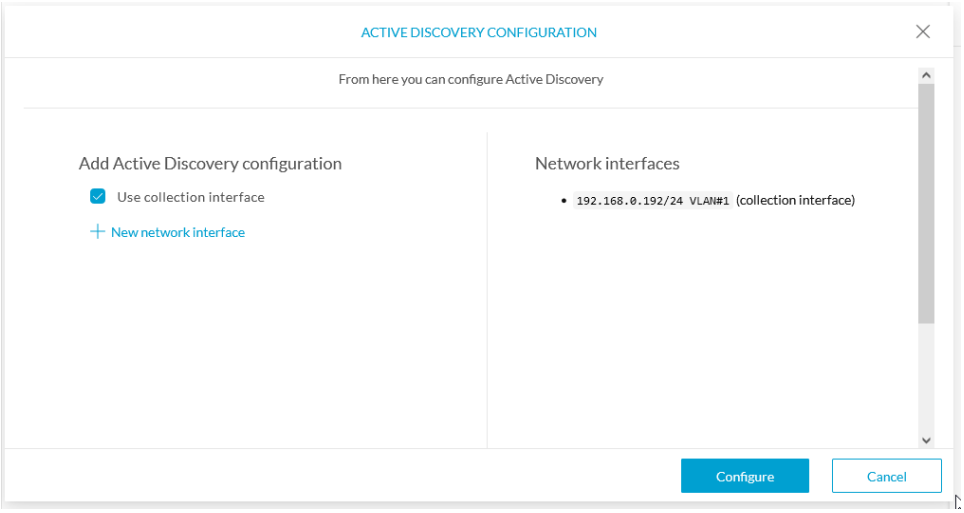


The Active Discovery Configuration window pops up:



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.

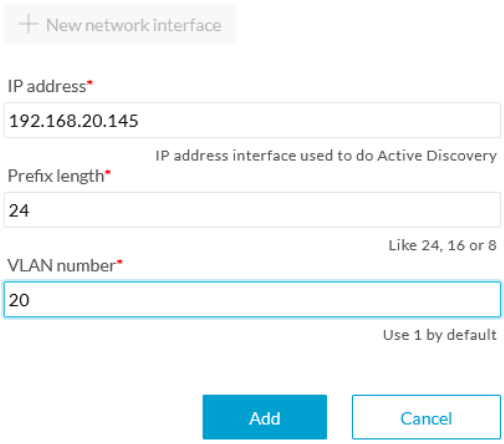
The Collection network interface is added in the list on the right.



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

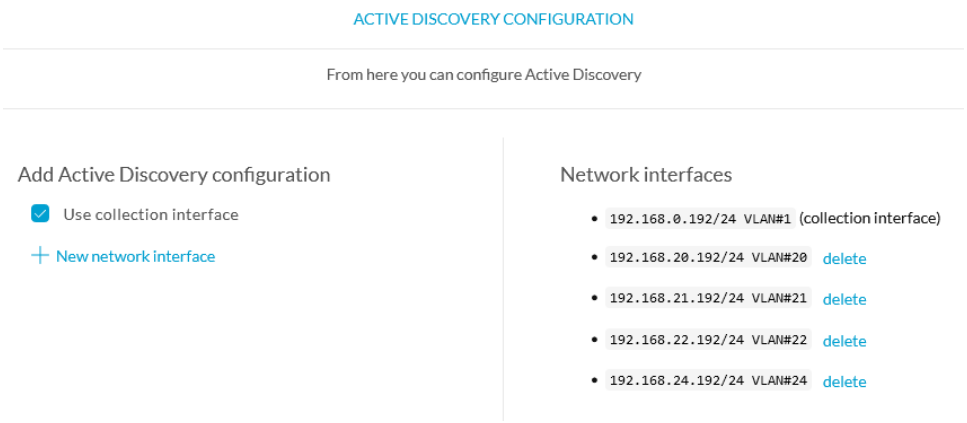
Step 6 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number



Step 7 Click **Add**.

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



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:

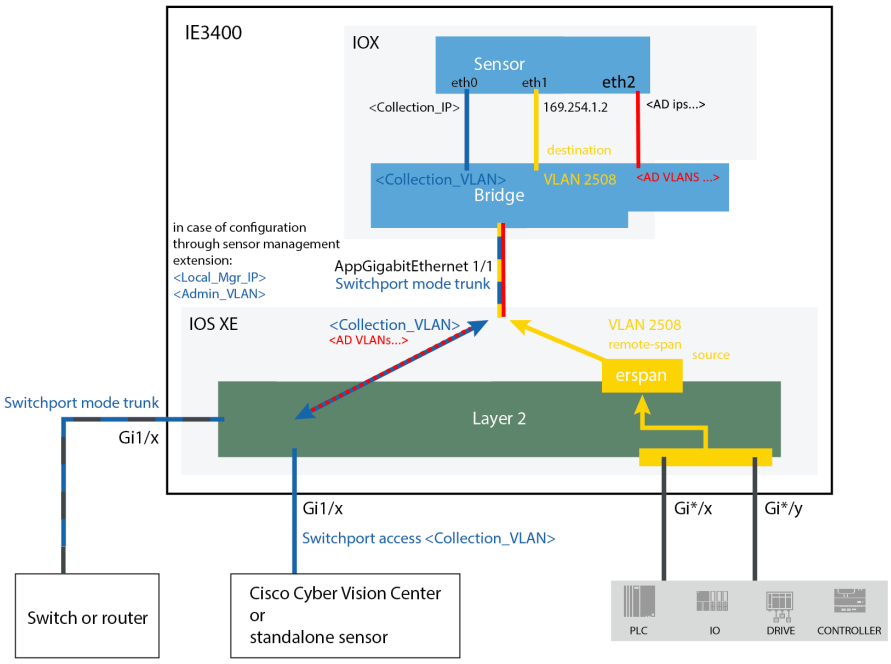


Figure 2: Catalyst 9300 and Catalyst 9400:

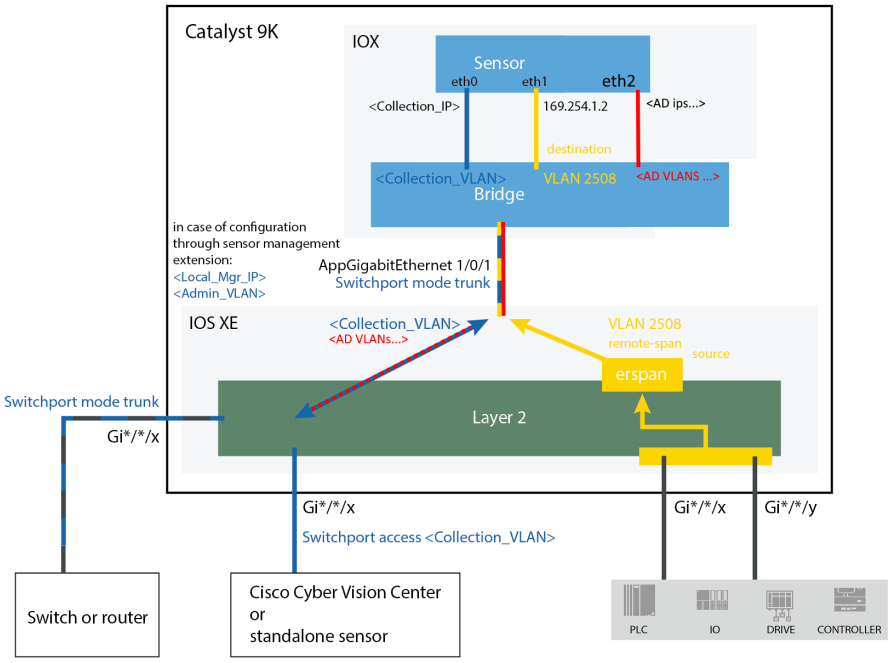
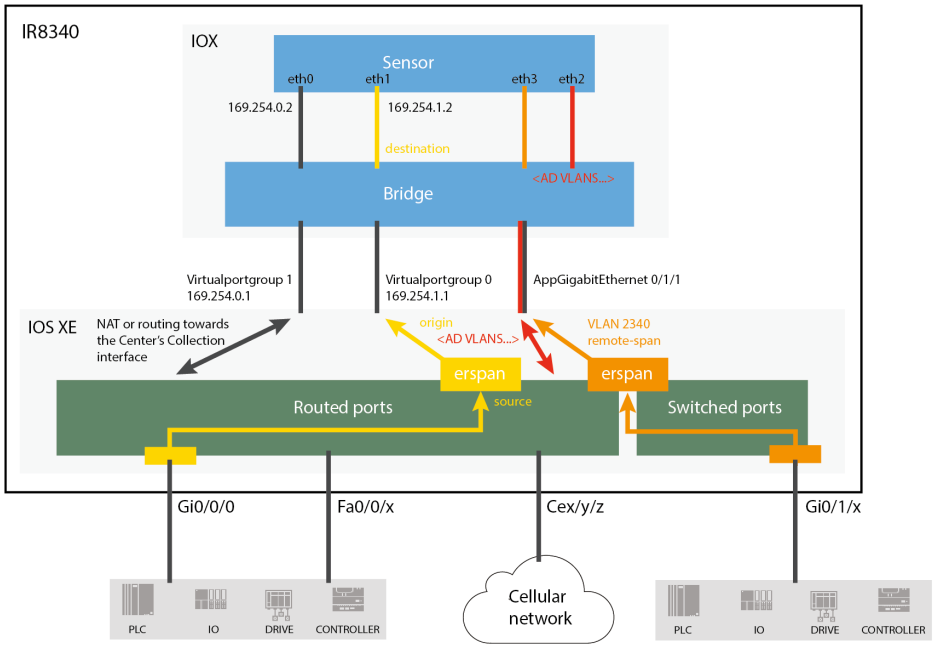


Figure 3: IR8340:



What to do next

Proceed to Policies configuration, on page 17.

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

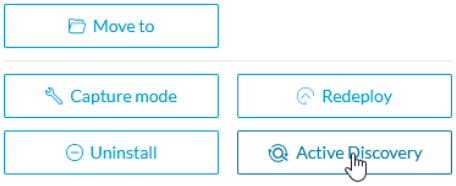
Step 1 Navigate to **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

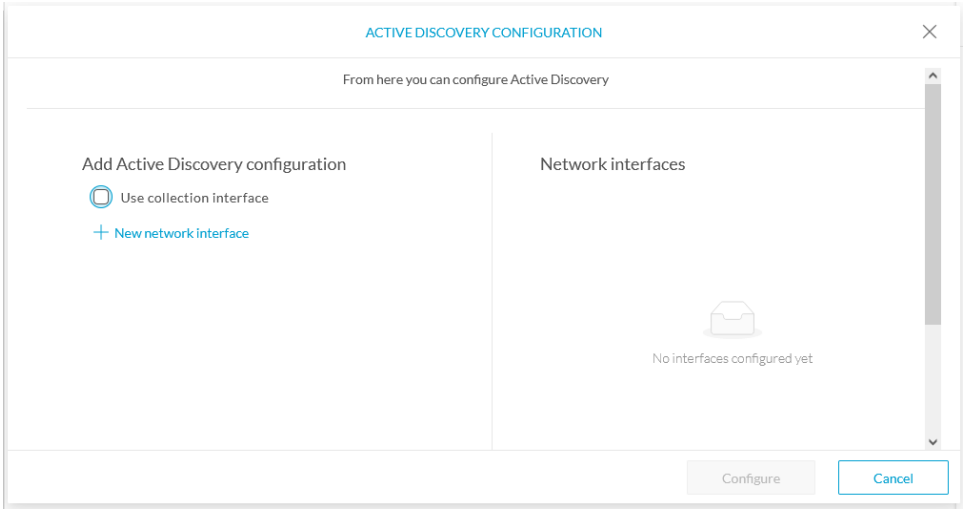
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

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.

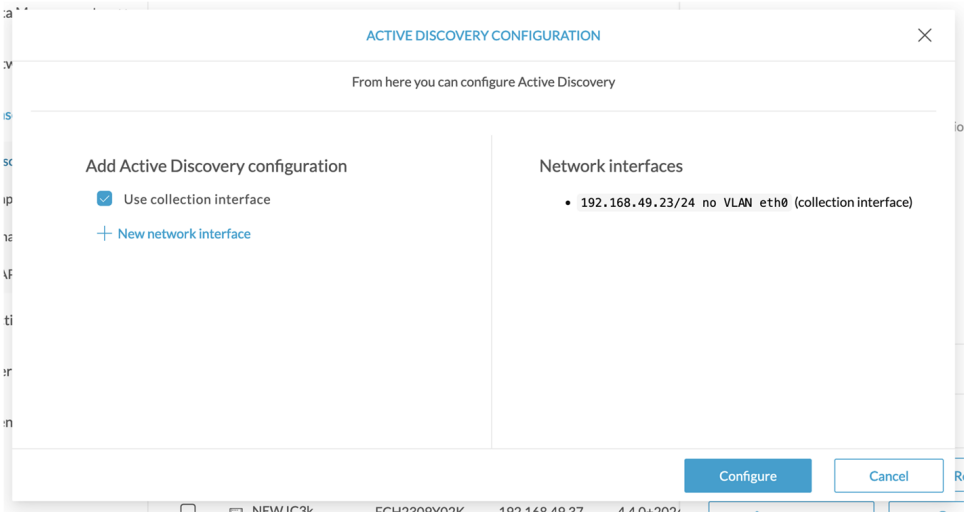


The Active Discovery Configuration window pops up:



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.

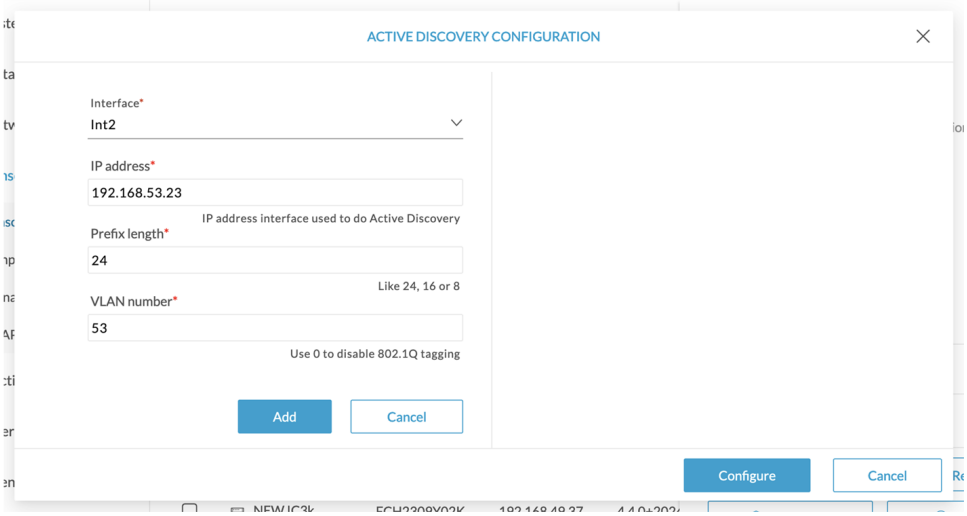


Step 5 Click **+ New network interface** for the sensor to perform Active Discovery on additional subnetworks.

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

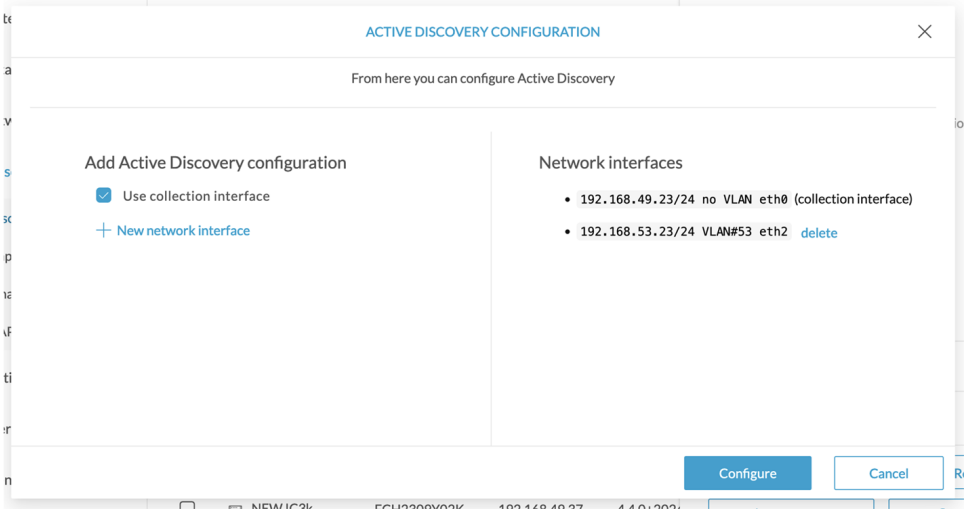
- IP address

- Prefix length
- VLAN number



Step 7 Click **Add**.

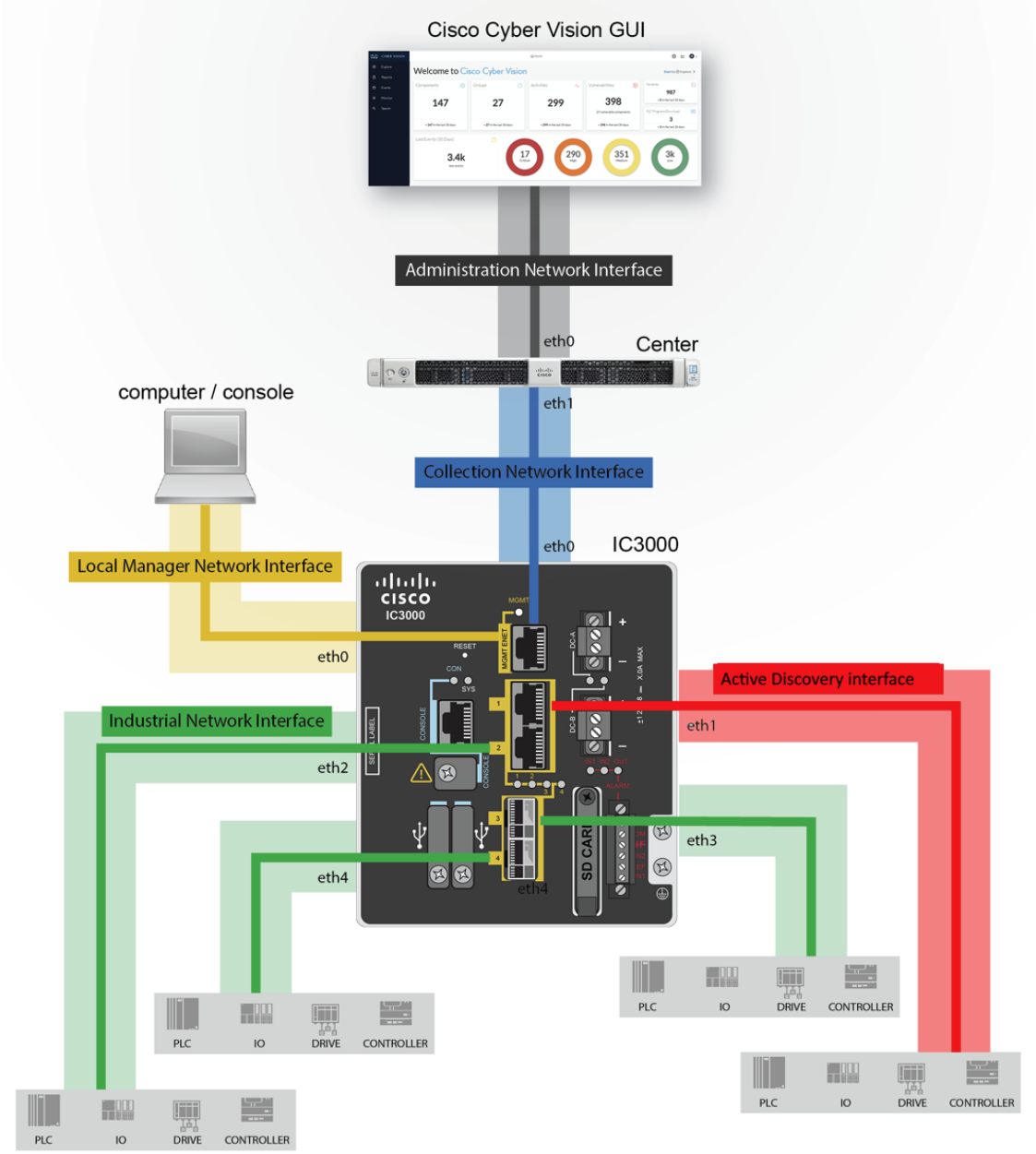
The network interfaces appears on the right.



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 17.

Configure Active Discovery on a Docker Sensor

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

The sensor's right-side panel appears.

The **Active Discovery** button is displayed if the sensor is compatible.

Note
If there is no **Active Discovery** button in the panel, the selected Docker sensor is not an Active Discovery sensor. Select a sensor that supports Active Discovery.

Step 3 Click **Active Discovery**.

The **ACTIVE DISCOVERY CONFIGURATION** window appears.

Step 4 Click **+ New network interface** for the sensor to perform Active Discovery on additional subnetworks.

Step 5 Fill in the following parameters to set a dedicated network interface:

- IP address
- Prefix length
- VLAN number

Step 6 Click **Add**.

The network interfaces appears on the right under **Network interfaces**.

You can add as many network interfaces as needed.

Step 7 Click **Configure**.

Configure Active Discovery on a Center Interface

Configure Active Discovery on a center interface to transform it into an active probe. This setup allows the center to send packets based on user-configured protocols and frequencies and discovers network devices that sensors might not detect. It is especially useful for identifying silent devices, like certain PLCs, by prompting them to respond to the center. The responses provide detailed information about the devices, including model references and vendor details, helping you identify more vulnerabilities.

Note Active discovery exclusively uses the interface. If there is any IP address that attached to the interface, it creates a conflict.

Before you begin

- In the CLI, type the **sudo sbs-netconf** command.
- From the **Network configuration** window, select the new interface. Click **OK**.
- Choose the **Active Discovery** configuration type. Click **OK**.

Procedure

Step 1 From the main menu, choose **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select the corresponding center interface from the sensor list.

The right-side panel appears and shows the Active Discovery status as **Enabled**.

Step 3 Click **Active Discovery**.

The **ACTIVE DISCOVERY CONFIGURATION** window pops up.

Step 4 Click **+ New network interfaces** for the center to perform Active Discovery on additional subnetworks.

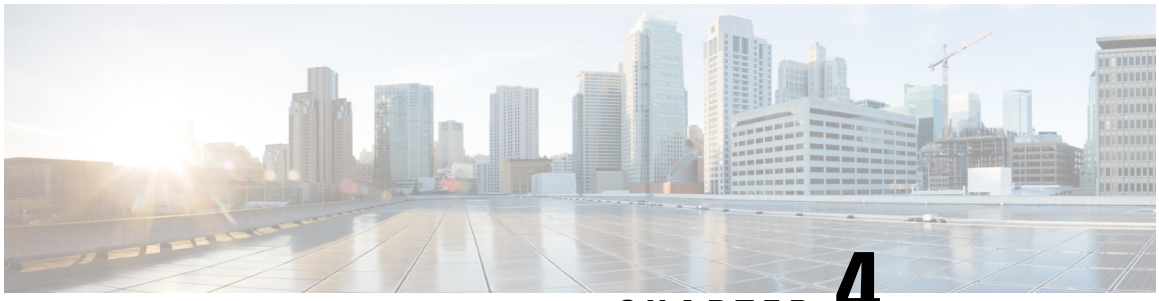
Step 5 Fill the following parameters to set dedicated network interfaces:

- IP address
- Prefix length
- VLAN number

Step 6 Click **Add**.

You can add as many network interfaces as needed.

Step 7 Click **OK**.



CHAPTER 4

Policies configuration

- Create a Policy, on page 17
- Set Active Discovery Broadcast, on page 17
- Set Active Discovery Unicast, on page 18
- Edit, Duplicate, and Delete Policy, on page 26

Create a Policy

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

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies** .

Step 2 Click **+ Create policy**.

What to do next

- Set Active Discovery Broadcast, on page 17
- Set Active Discovery Unicast, on page 18

Set Active Discovery Broadcast

Before you begin

Active Discovery is compatible with the following Broadcast protocols:

- Beckhoff
- BACnet

- EtherNet/IP
- Siemens S7
- Profinet
- ICMPv6

The sensor will send requests on all defined interfaces.

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies** .

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 In the **Broadcast Configuration** field, enable the toggle switch for the required fields.

Step 5 The **Broadcast retry** and **Unicast timeout (in seconds)** are listed under **Advanced settings**.

a) Leave the **Broadcast retry** and **Unicast timeout (in seconds)** at their default values (3 and 10).

Broadcast retry: number of request attempts.

Unicast timeout (in seconds): waiting time in seconds for a response.

Step 6 Click **Create**.

What to do next

Set Active Discovery Unicast, on page 18

Set Active Discovery Unicast

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select a protocol.

Step 5 Update **Advanced settings**.

Step 6 Click **Create**.

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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **BACnet**.

Step 5 Enable the toggle switch.

Step 6 Click **Create**.

Set Active Discovery Unicast Beckhoff

Enable Active Discovery Unicast Beckhoff to search for devices and components using AMS requests. It will check all components with an IPV4 address.

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **Beckhoff**.

Step 5 Enable the toggle switch.

Step 6 (Optional) Enable Authentication and enter a Beckhoff user account and password.

Without authentication, Cyber Vision will only be able to provide the device name and firmware version.

Step 7 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **DNP3**.

Step 5 Enable the toggle switch.

Step 6 Leave the **Source Address** and **Max Destination Address** at their default values (0 and 16).

Step 7 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **EtherNet/IP**.

Step 5 Enable the toggle switch.

Step 6 Check the checkbox to enable the **Backplane discovery** button.

Active Discovery will look for different module details within the discovered chassis.

Step 7 Click **Create**.

Set Active Discovery Unicast GESRTP

Configure Active Discovery Unicast GESRTP to search for devices and components using GESRTP requests. It will check all components with an IPV4 address.

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **GESRTP**.

Step 5 Enable the toggle switch.

Step 6 Click **Create**.

Set Active Discovery Unicast HTTP or HTTPS

Configure Active Discovery Unicast HTTP/HTTPS to find devices and components with HTTP/HTTPS requests. It will check all components with an IPV4 address.

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **HTTP/HTTPS**.

Step 5 Enable the toggle switch.

Step 6 Add **HTTP** or **HTTPS** port details to scan.

Step 7 Click **Create**.

Set Active Discovery Unicast Melsoft

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

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **Melsoft**.

Step 5 Enable the toggle switch.

Step 6 Click **Create**.

Set Active Discovery Unicast MMS

Set Active Discovery Unicast MMS to search for devices and components using MMS requests. The Manufacturing Message Specification (MMS) is used between IEDs and SCADA devices.

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **MMS**.

Step 5 Enable the toggle switch.

Step 6 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **Modbus**.

Step 5 Enable the toggle switch.

Step 6 Add the **Unit Id** code (0-255), (usually 0).

Step 7 Select the **Force UMAS Function Codes** option to discover with UMAS.

In this case, Modbus discovery performs UMAS commands even if it does not detect the device as a Schneider Electric PLC.

Step 8 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **OMRON**.

Step 5 Enable the toggle switch.

Step 6 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **SiemensS7**.

Step 5 Enable the toggle switch.

Step 6 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **SiemensS7plus**.

Step 5 Enable the toggle switch.

Step 6 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **SNMPv2c**.

Step 5 Enable the toggle switch.

Step 6 Enter a **Community** string for authentication.

IT or network administrators define the **Community** string. The value 'public' is often used by default

Step 7 Check the checkbox to enable the **Enable SNMPv1 fallback** option.

In case of failure with SNMPv2, SNMPv1 will be used.

Step 8 Click **Create**.

Refer to the annex appended at the end of this document to see the 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **SNMPv3**.

Step 5 Enable the toggle switch.

Step 6 Type a community string for authentication.

IT or network administrators define community string. The value "public" is often used by default.

Step 7 Select the appropriate security and privacy level based on information provided by IT or network administrators.

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

- **Disable both authentication and privacy.**

  Only a username is requested for authentication.

- **Enable authentication and disable privacy.**

  Authentication uses HMAC-MD5 or HMAC-SHA algorithms.

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

- **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.

Step 8 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 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click **+ Create policy**.

The **Create a policy** side panel appears.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Unicast configuration**, click the drop-down arrow next to **Add a new protocol** and select **WMI**.

Step 5 Enable the toggle switch.

Step 6 Enter the **Username** and **Password** with appropriate WMI rights.

You can also use an Active Directory user account for authentication across multiple hosts with a single set of login credentials.

Step 7 Click **Create**.

Edit, Duplicate, and Delete Policy

Procedure

Step 1 From the main menu, choose **Admin** > **Active Discovery** > **Policies**.

Step 2 Click the policy name under the **Name** column that you want to modify.

The policy panel appears with the configurations and the **Edit**, **Duplicate**, and **Delete** buttons.

Step 3 If you click **Edit**, an **Edit a policy** panel appears.

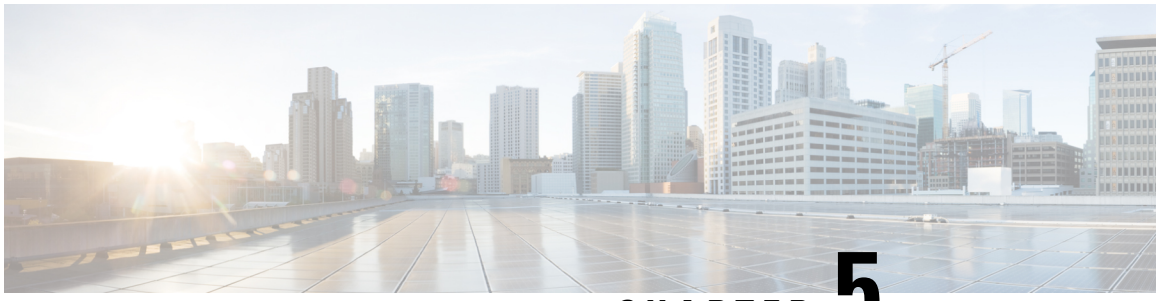
a) Edit the policy name in the **Name** field.
b) Under the **Broadcast configuration** field, you can toggle the buttons ON/OFF to enable/disable broadcast protocols.
c) Under **Unicast configuration**, click the drop-down arrow next to Add a new protocol field and select a protocol.
d) Update **Advanced settings**.
e) Click **Update**.

Step 4 If you click **Duplicate**, a **Create a policy** panel appears.

a) Edit the policy name in the **Name** field.
b) Under the **Broadcast configuration** field, you can toggle the buttons ON/OFF to enable/disable broadcast protocols.
c) Under **Unicast configuration**, click the drop-down arrow next to Add a new protocol field and select a protocol.
d) Update **Advanced settings**.
e) Click **Create**.

Step 5 If you click **Delete**, a **DELETE POLICY** pop-up appears.

a) Click **Ok**.



CHAPTER 5

Profiles configuration

• Set an Active Discovery profile, on page 29

Set an Active Discovery profile

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

Procedure

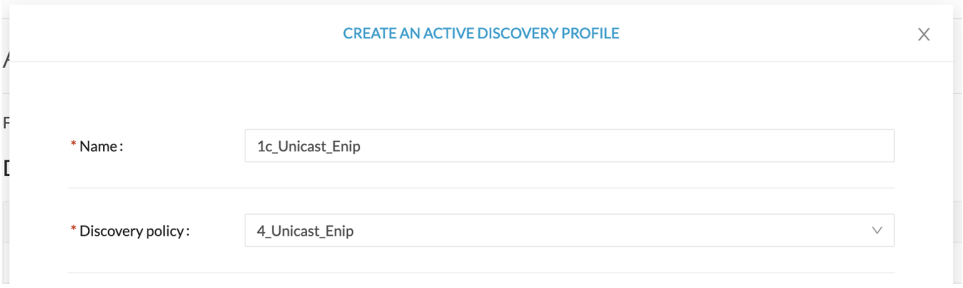
Step 1 On , navigate to Admin > Active Discovery > Profiles.

Step 2 Click the **Create profile** button.

A form to create an Active Discovery profile pops up.

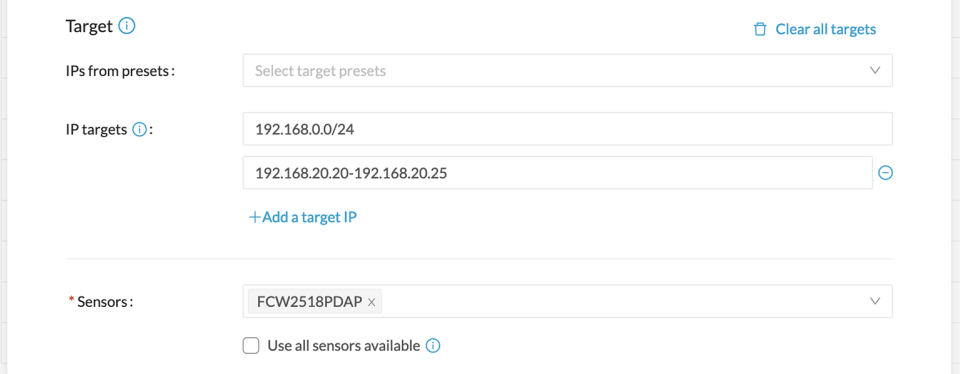
Step 3 Give the profile a name.

Step 4 Select a policy to base the profile on.



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 adresses, IP ranges and subnets you want to be queried.
- selecting sensors: all IP adresses detected by a sensor will be queried. You can also tick the **Use all sensors available** option.



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

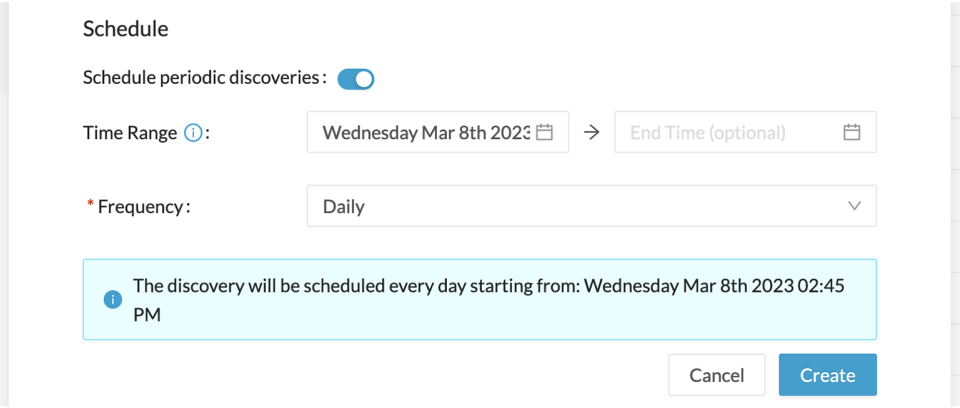
a) Toggle ON the **Schedule periodic discoveries** button.

Additional options to setup appear:

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

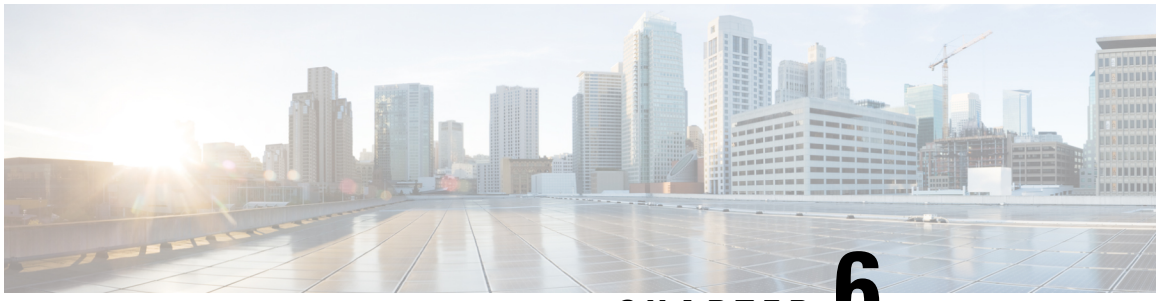
The end date and time is optional. If you don't set it, Active Discovery will be launched endlessly.

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 31

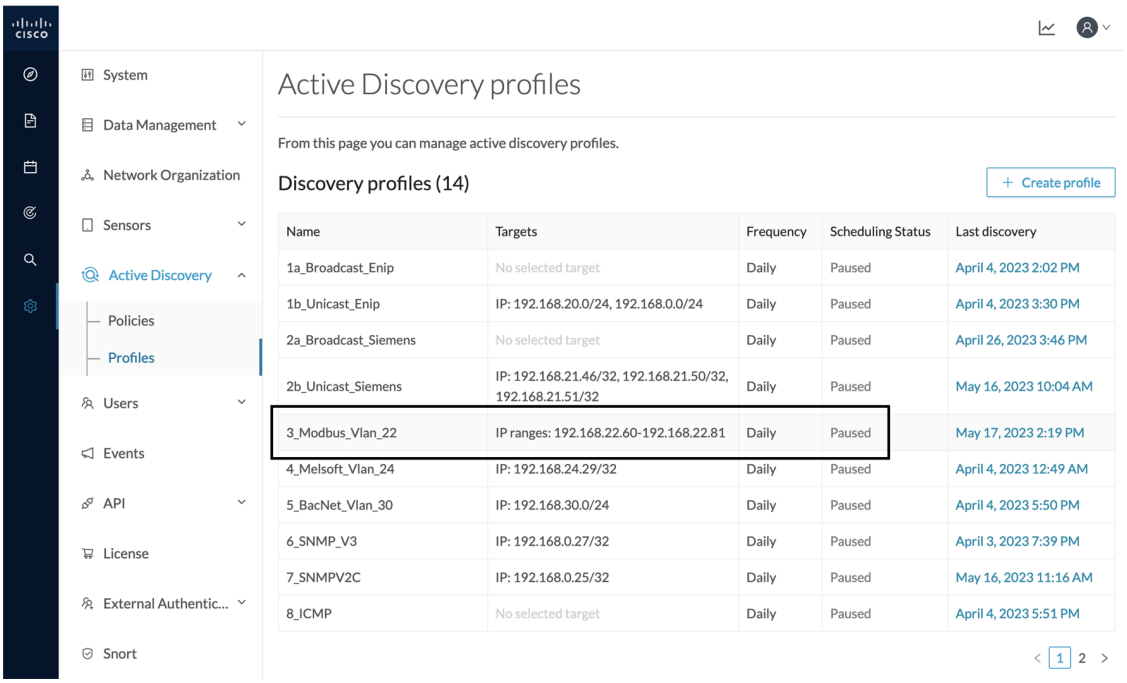
Launch Active Discovery

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

Procedure

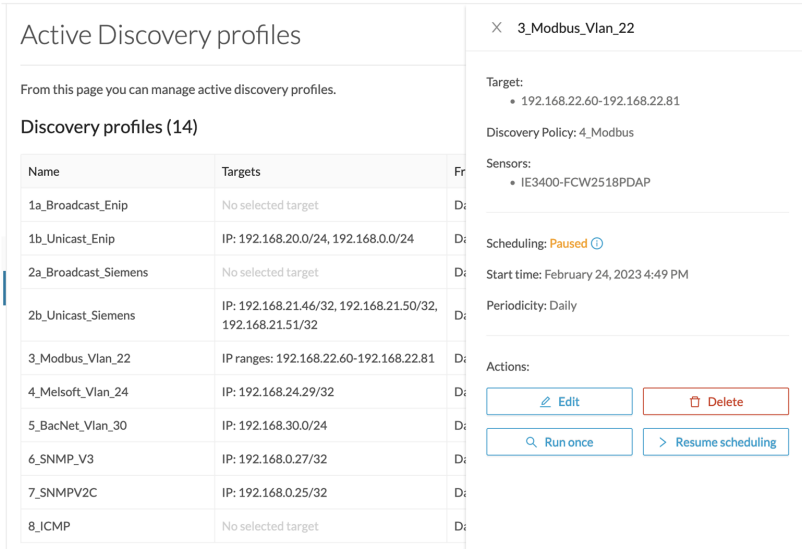
Step 1 On , navigate to Admin > Active Discovery > Profiles.

Step 2 Click a profile in the list.



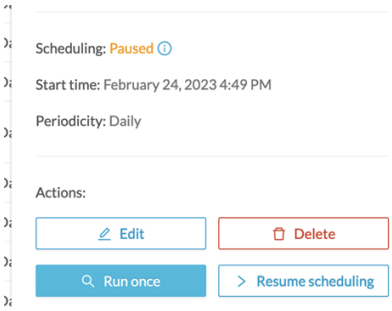
Its right side panel opens.

Launch Active Discovery

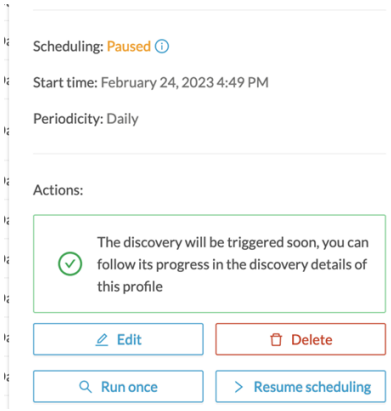


Step 3 You can run the discovery once or resume scheduling.

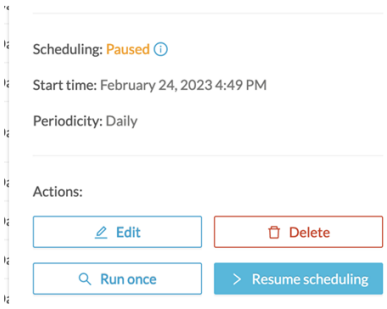
- Click **Run once**.



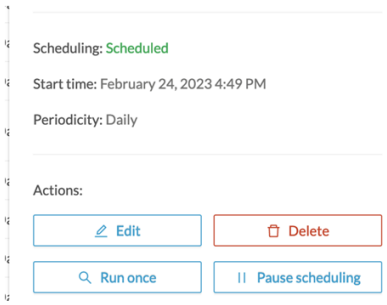
A message indicating that Active Discovery will be launched soon appears.



- Click **Resume scheduling**.



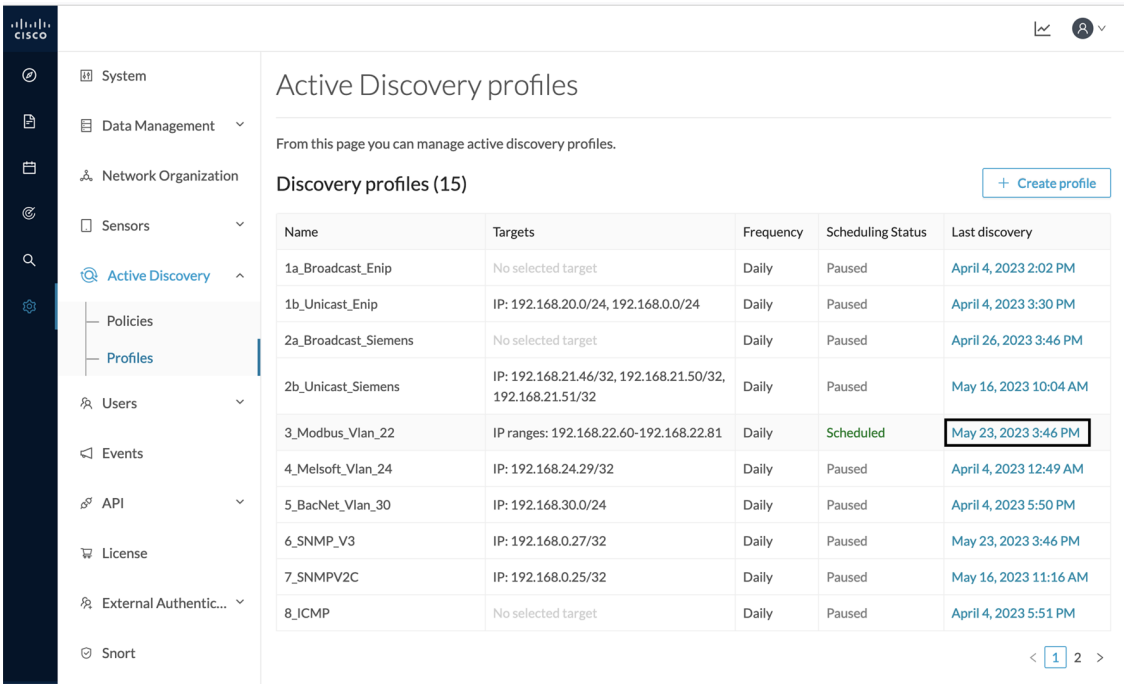
The scheduling status switches from paused to scheduled.



The discovery will be launched as configured.

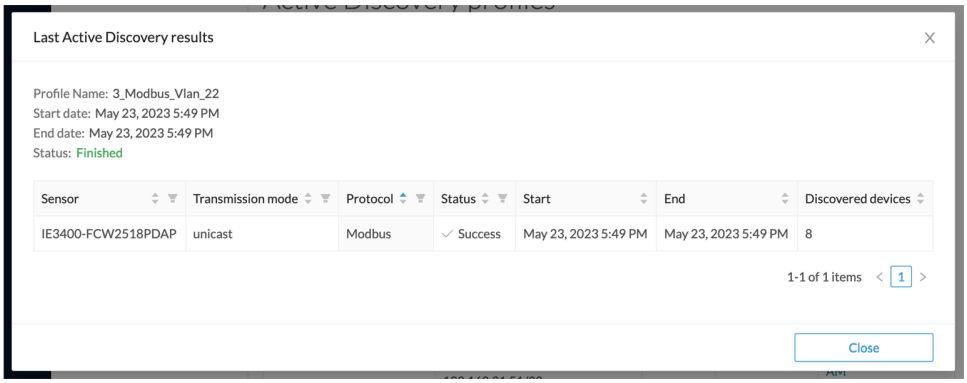
You can change these configurations clicking **Edit**.

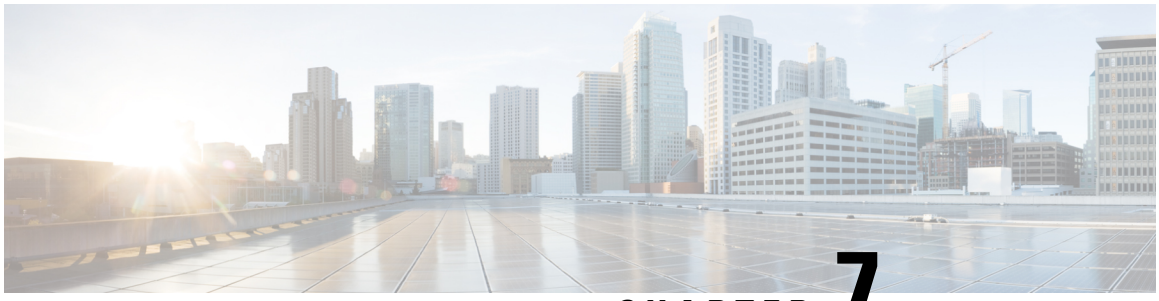
Step 4 You can click the link in the last discovery column to see a profile's Active Discovery results.



A window opens with the result details.

Launch Active Discovery





CHAPTER 7

Annex: Active Discovery protocols

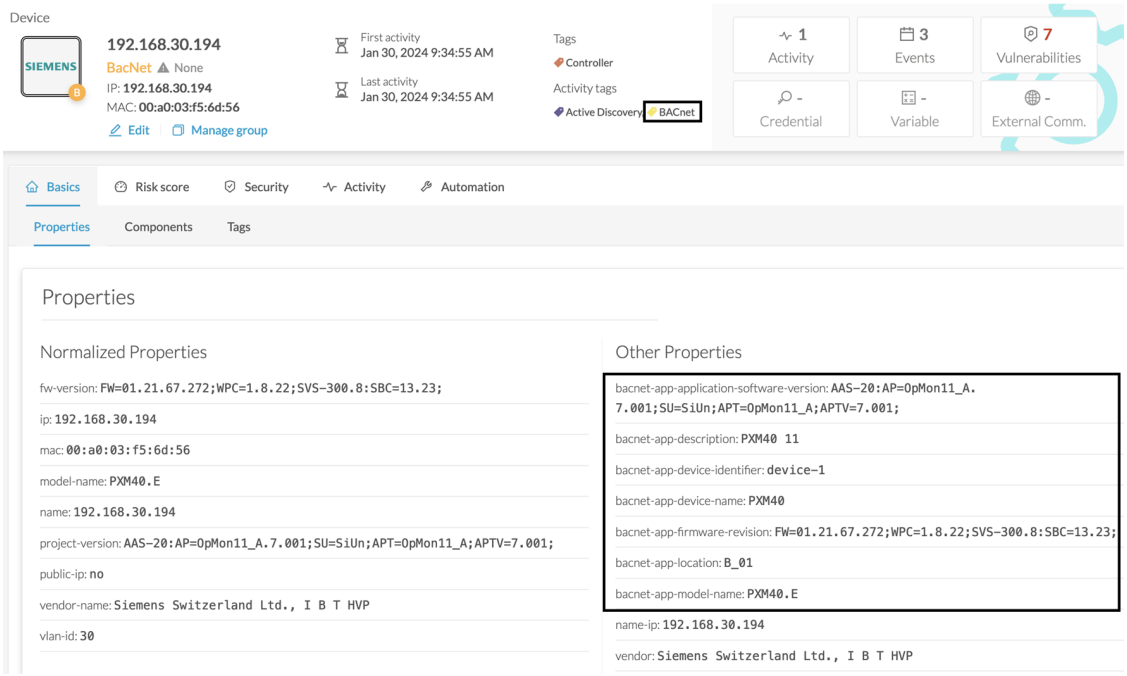
All protocols implemented in the Active Discovery feature use standard packets commonly used by vendors. The system will never send requests on the network without a clear configuration made by the user. It is possible to schedule requests at a pre-defined frequency.

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.

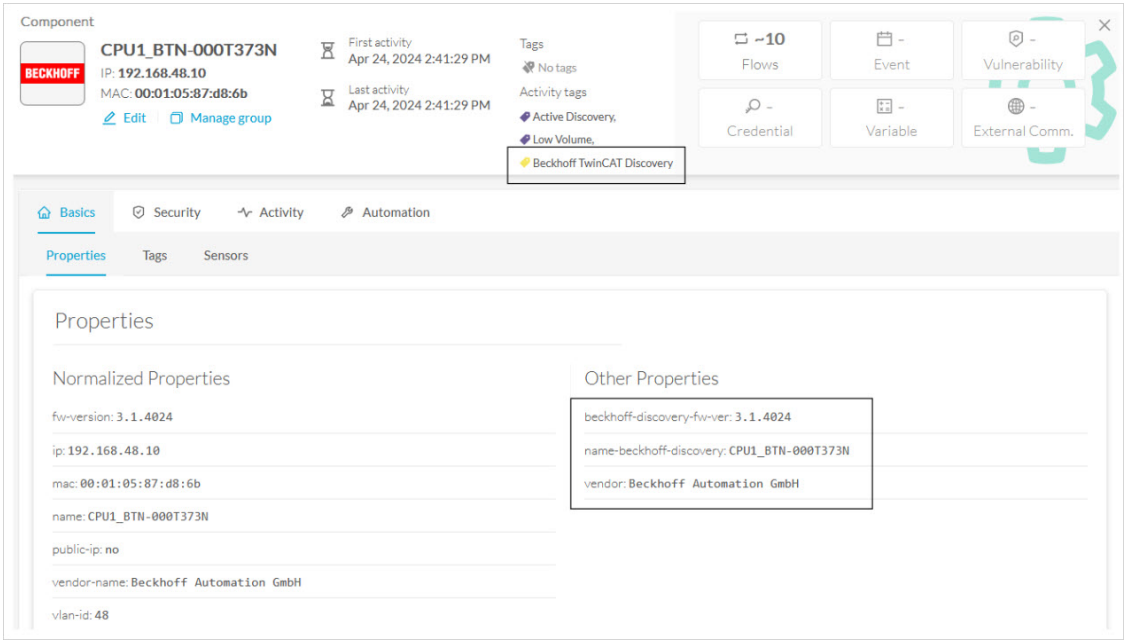
- BACnet, on page 36
- Beckhoff, on page 36
- DNP3, on page 37
- EtherNet/IP, on page 38
- GESRTP, on page 42
- HTTP-HTTPS, on page 42
- Melsoft, on page 43
- Modbus, on page 44
- OMRON, on page 45
- Profinet Multicast, on page 45
- S7 Broadcast, on page 46
- S7 Unicast, on page 47
- S7Plus, on page 48
- ICMPv6 Multicast, on page 49
- SNMP Unicast, on page 49
- WMI, on page 57

BACnet

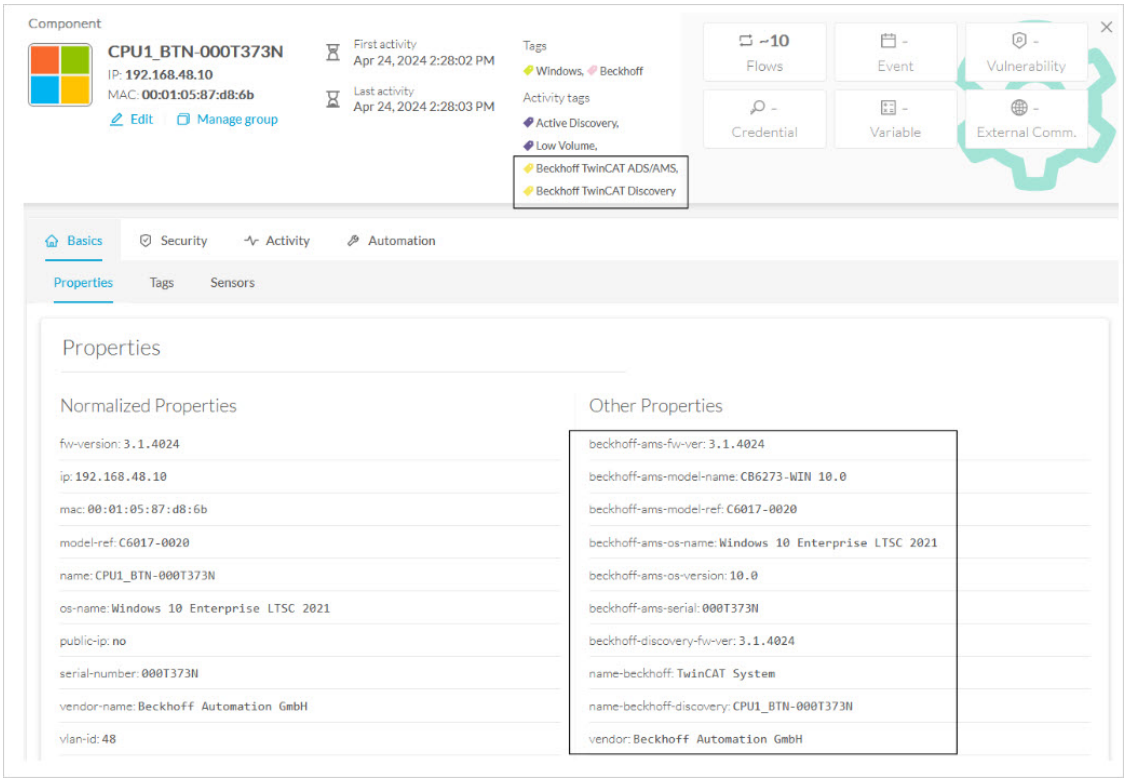


Beckhoff

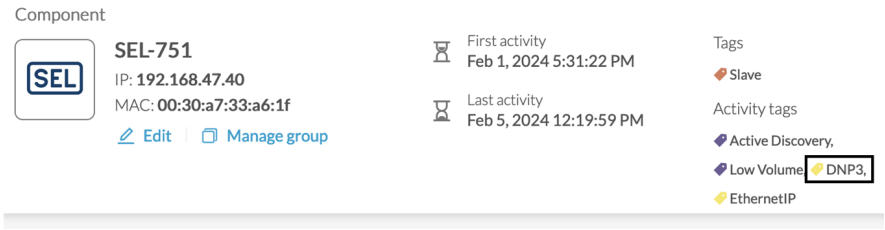
Without User



With User



DNP3





EtherNet/IP

Ethernet/IP Active Discovery can be performed by 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 direclty 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):

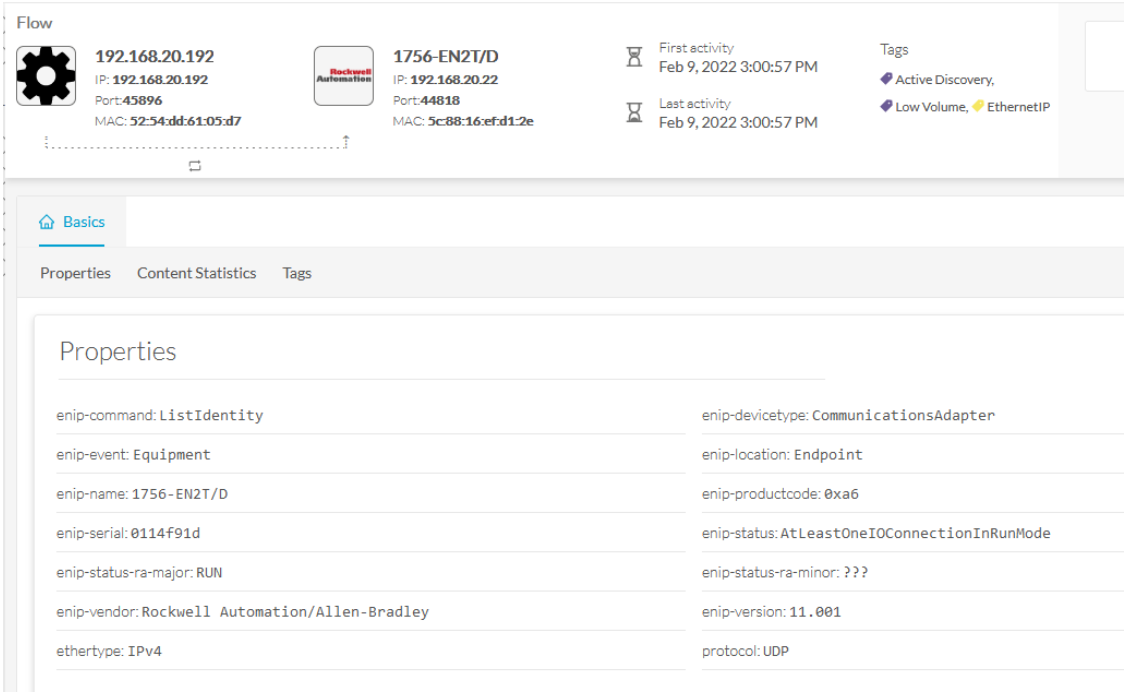


Figure 5: Example of properties received from a Rockwell Automation EtherNet/IP safety controller (1756-L81ES):

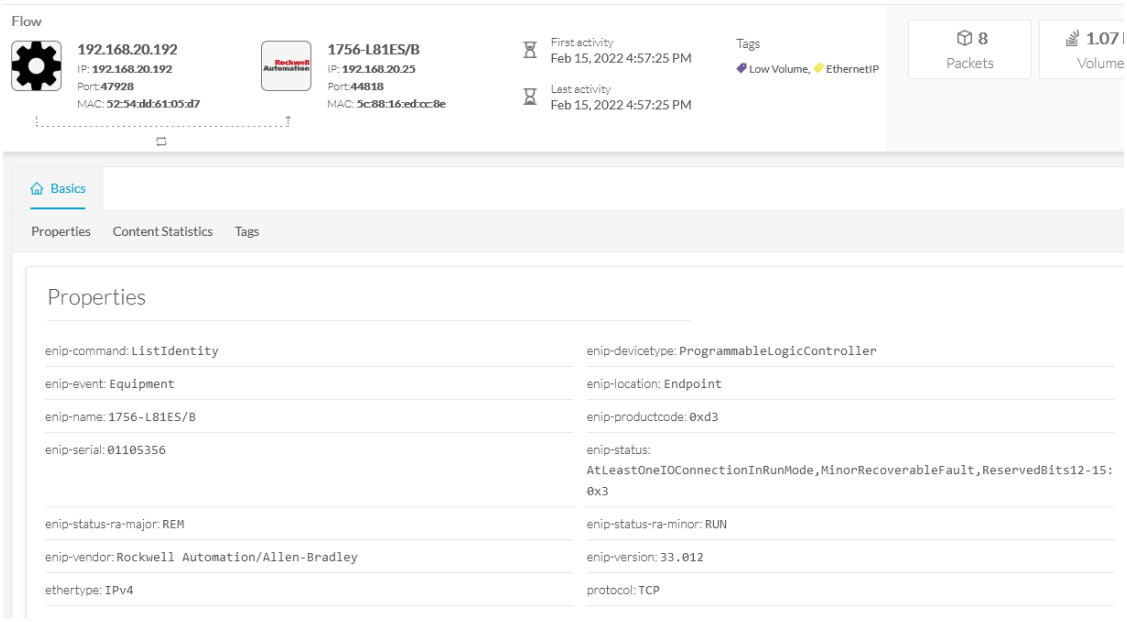
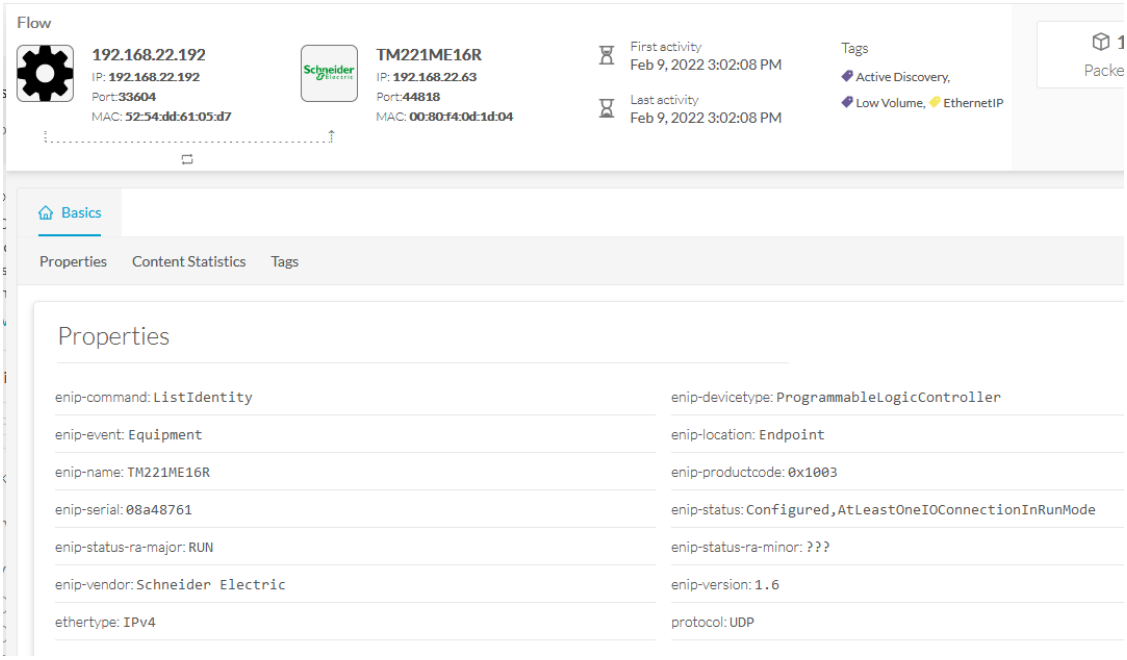


Figure 6: Example of properties received from a Schneider Eletric EtherNet/IP controller (TM221ME16R):

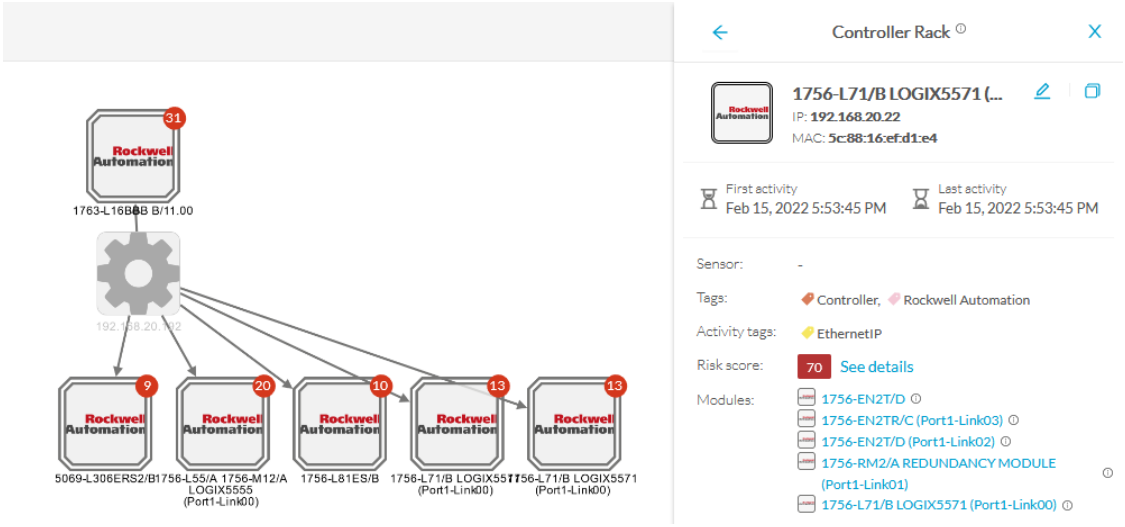


Ethernet/IP backplane discovery

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 form 0 to the chassis size). All modules will then send their properties such as the product reference and the firmware version.

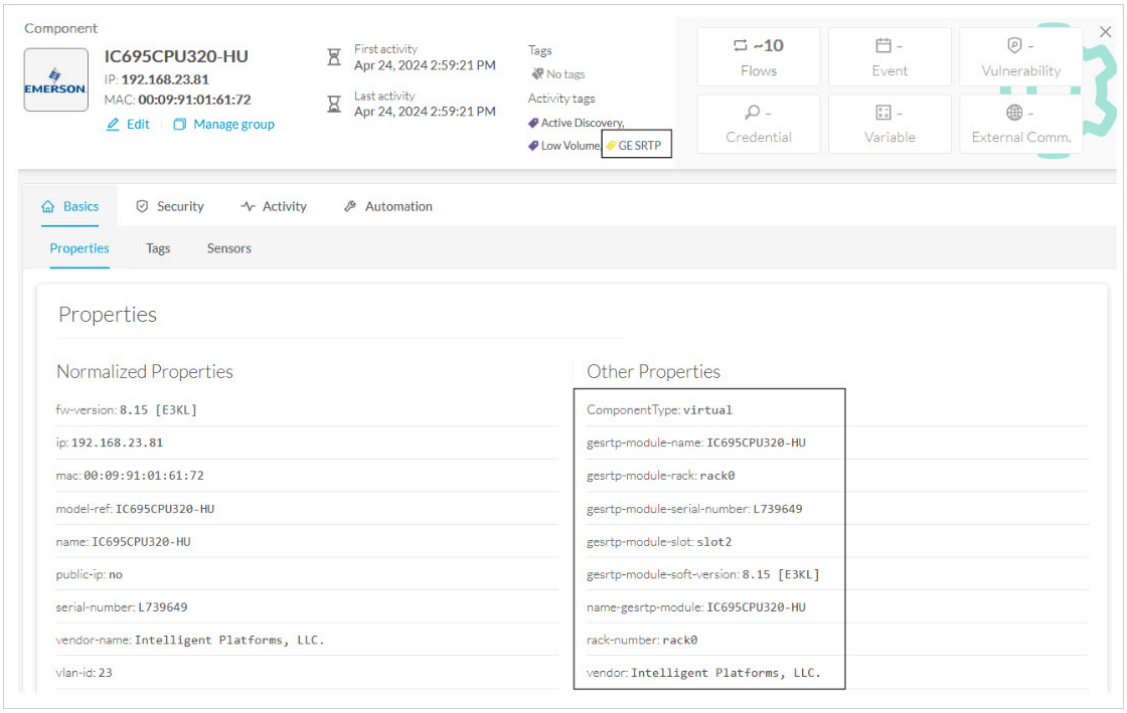
For example, an Ethernet/IP communication adapter with the IPv4 192.168.20.22 was first discovered. Then, all seven slots of the chassis backplane were queried. Four of them have answered back, which allowed to build a Controller Rack:



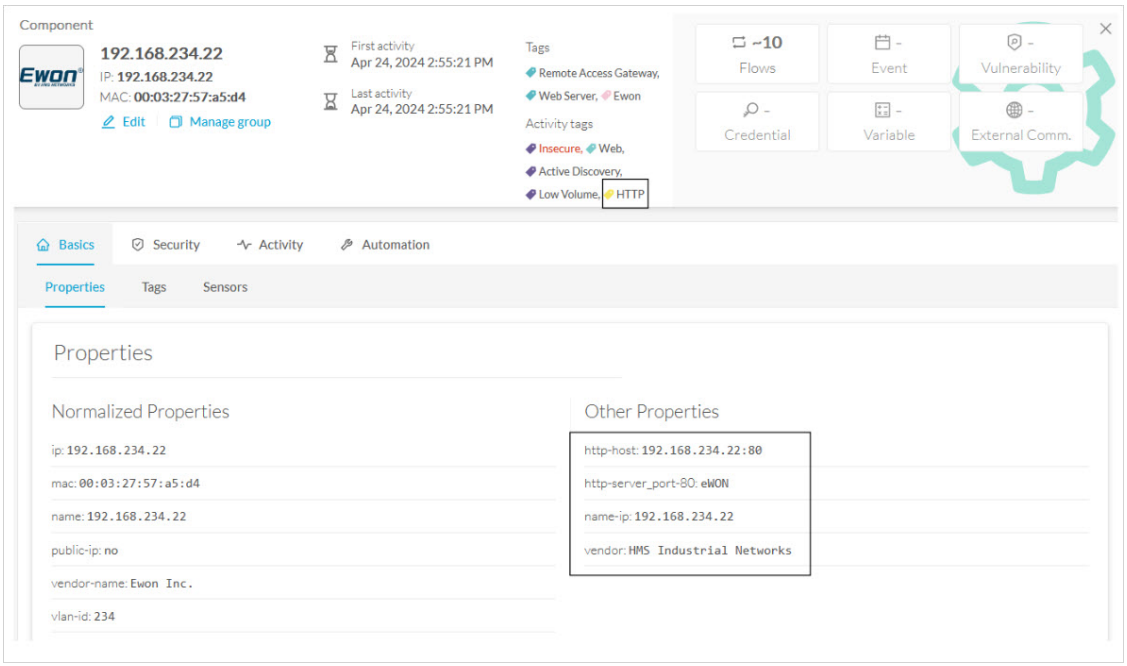
A controller and a firmware version were discovered in the slot 0 of this backplane thanks to Active Discovery:



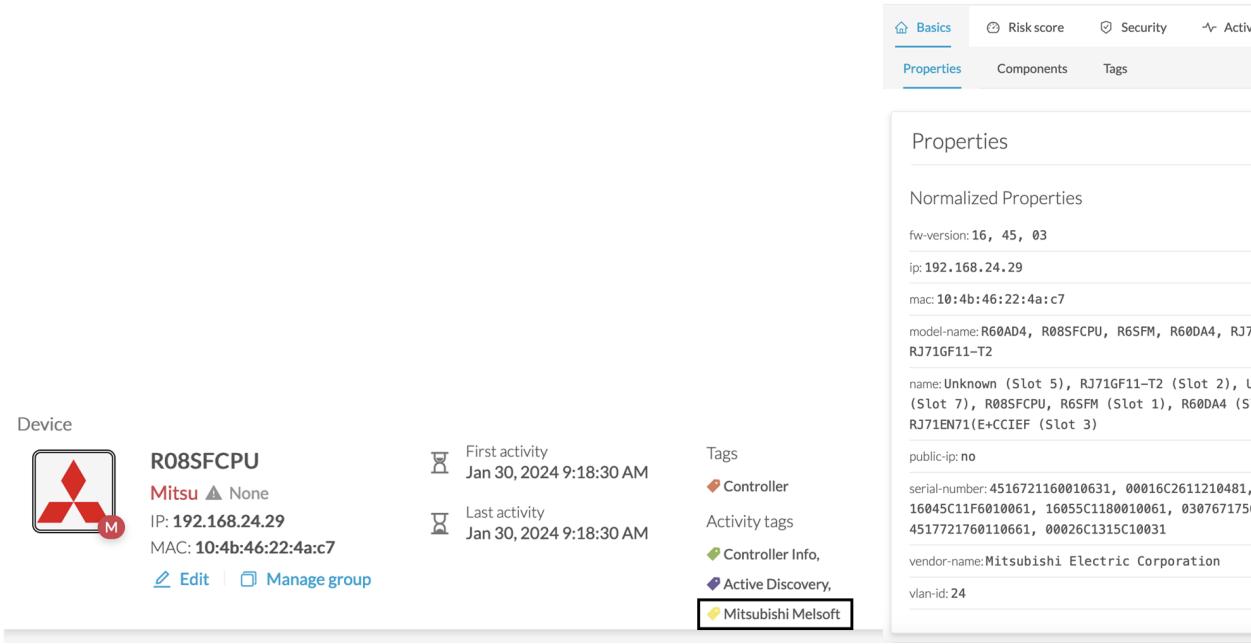
GESRTP



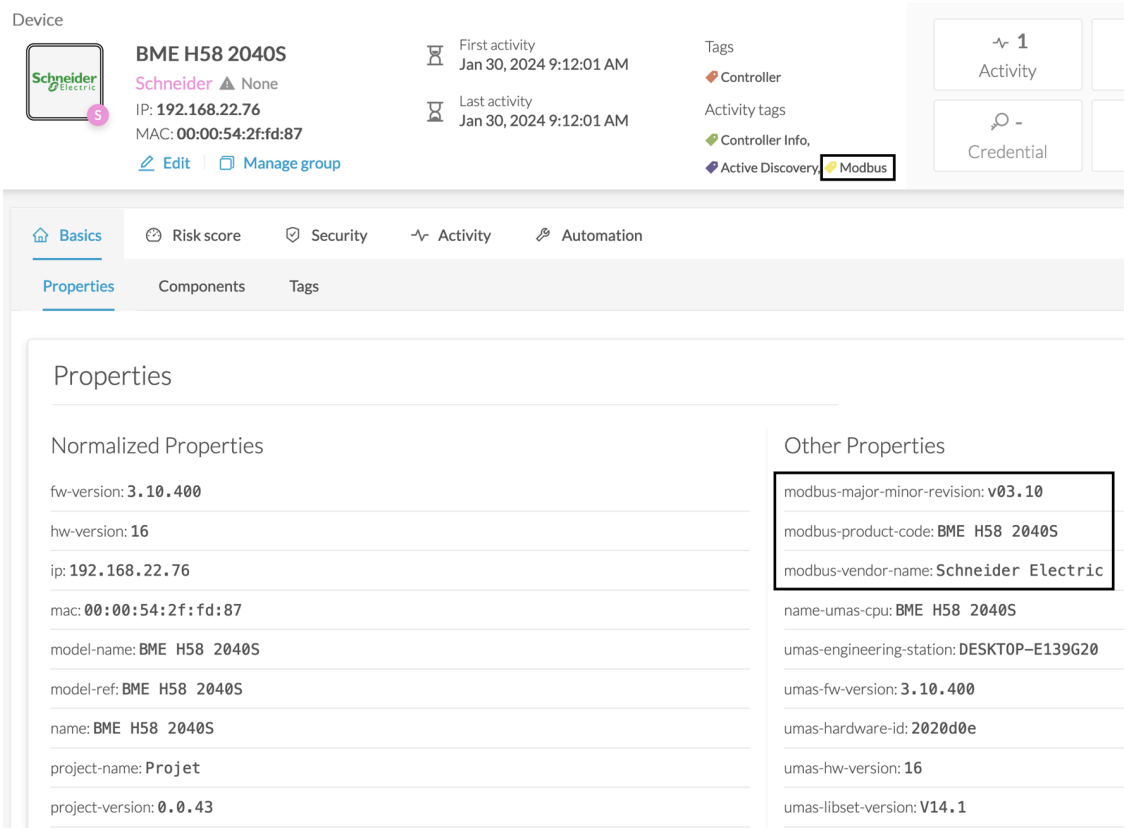
HTTP-HTTPS



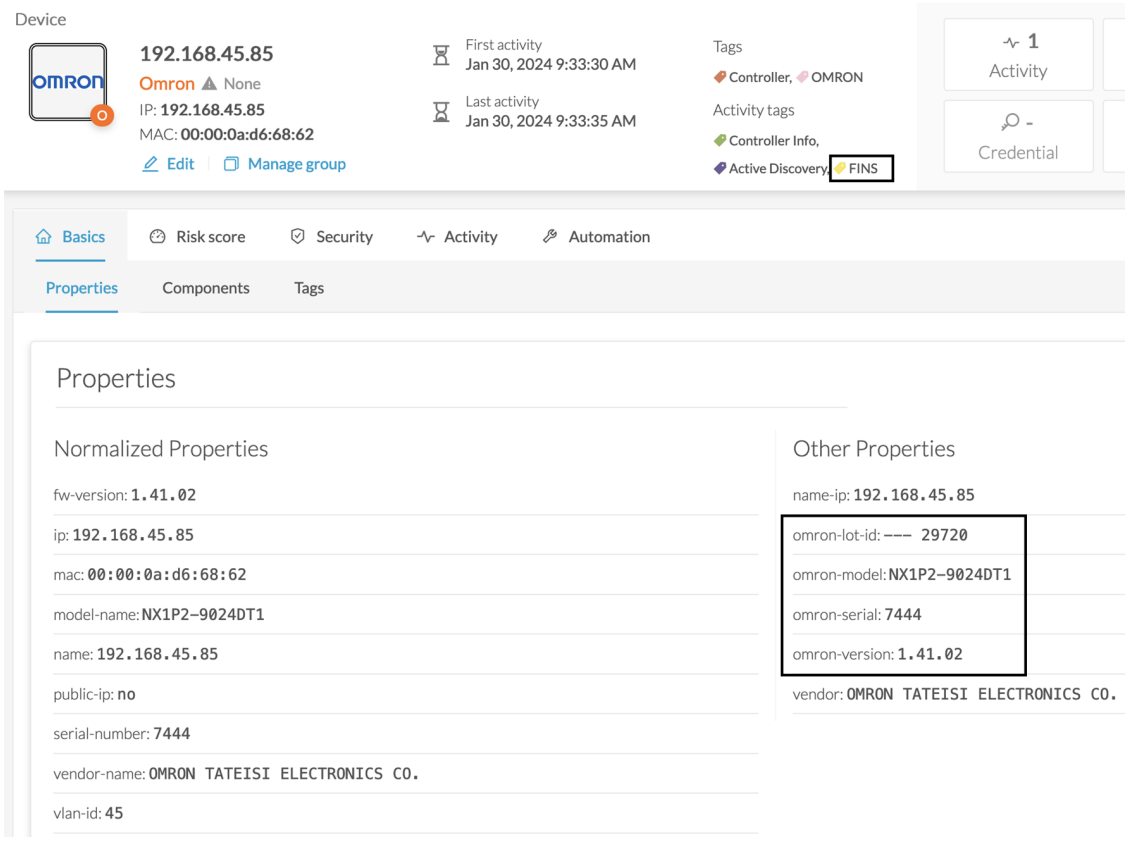
Melsoft


Basics
Risk score
Security
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, R6SFM, R60DA4, RJ71GF11-T2
name: Unknown (Slot 5), RJ71GF11-T2 (Slot 2), (Slot 7), R08SFCPU, R6SFM (Slot 1), R60DA4 (S RJ71EN71(E+CCIEF (Slot 3)
public-ip: no
serial-number: 4516721160010631, 00016C2611210481, 16045C11F6010061, 16055C1180010061, 030767175 4517721760110661, 00026C1315C10031
vendor-name: Mitsubishi Electric Corporation
vlan-id: 24
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

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
Activity tags
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



Profinet Multicast

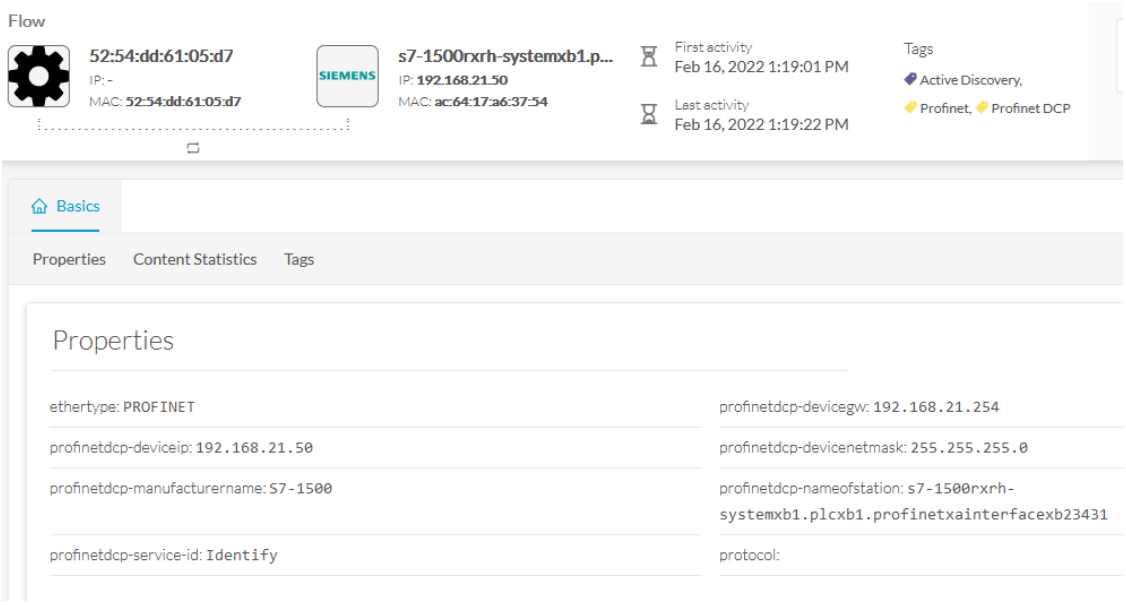
Cisco Cyber Vision Active Discovery can use a Profinet DCP service called Identify Request. This request will be sent by the sensor interfaces defined for Active Discovery. All Profinet devices will answer with a specific Profinet DCP identify response packet.

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:



S7 Broadcast

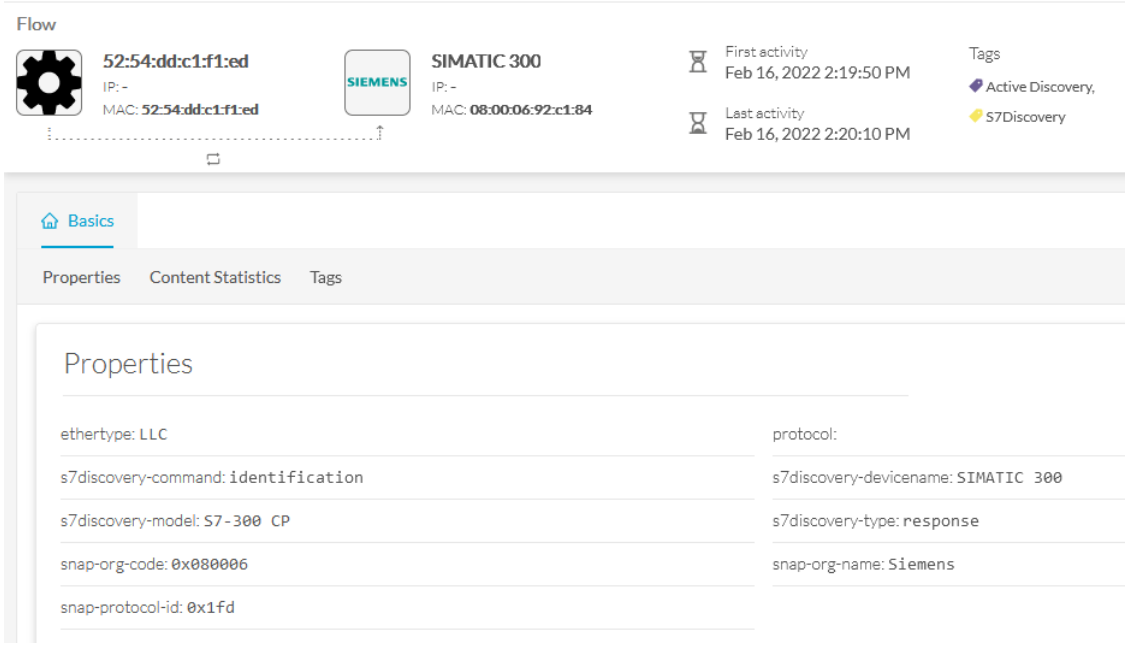
Cyber Vision Active Discovery can use a request on the protocol S7 discovery with a command: "identification". This request will be sent by the sensor interfaces defined for Active Discovery. All S7 devices will answer with a specific S7 Discovery identification response packet.

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.

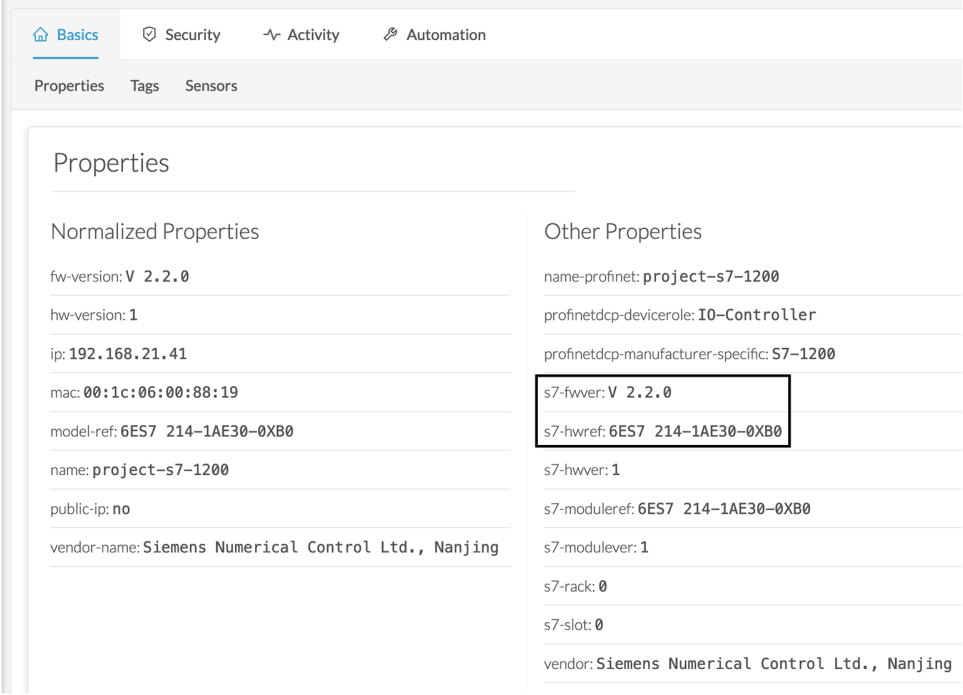
Figure 8: For example, a Siemens S7-300 controller:



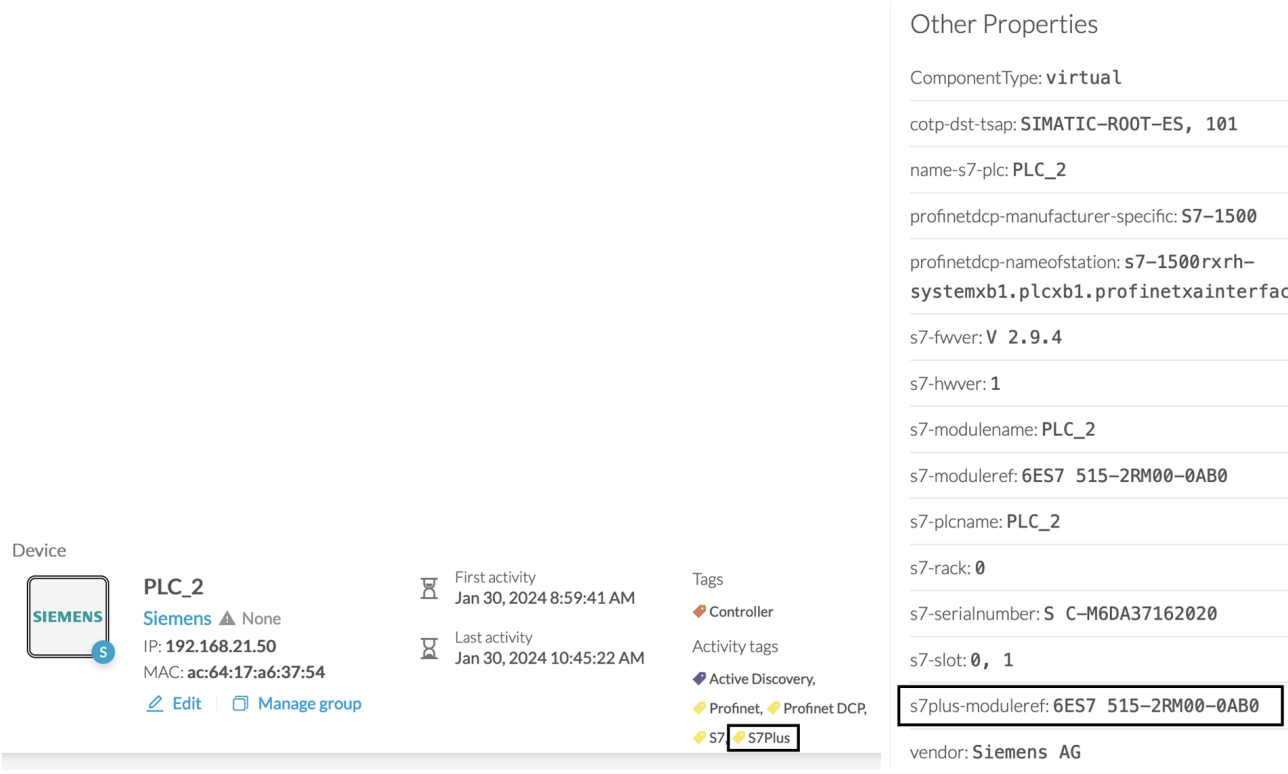
S7 Unicast

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

S7Plus


Device
SIEMENS
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.profinetxainterfac
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

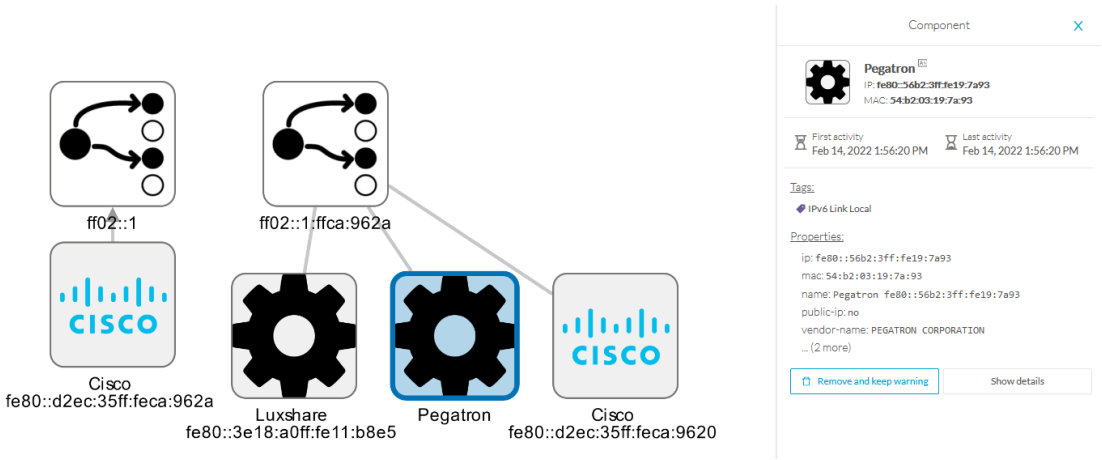
ICMPv6 Multicast

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 ff:02::1. Three different devices are answering back:



SNMP Unicast

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 sensor Active Discovery supports:

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

- SNMP Version 3 (SNMPv3).

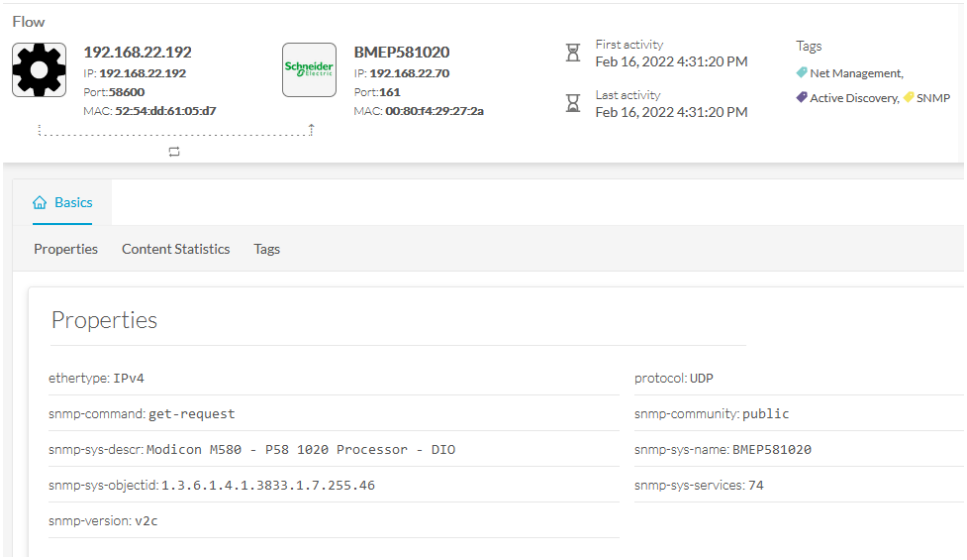
SNMPv3 Active Discovery is able to provide authentication and encryption.

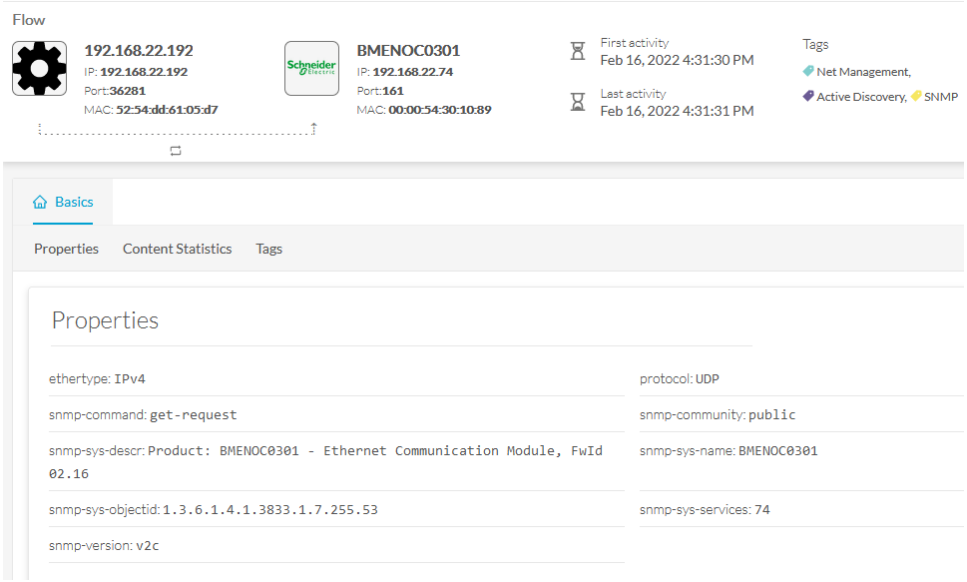
All SNMP versions will give the same results in the application. They are important regarding data access. The subsequent section describes the SNMP results with different types of network devices.

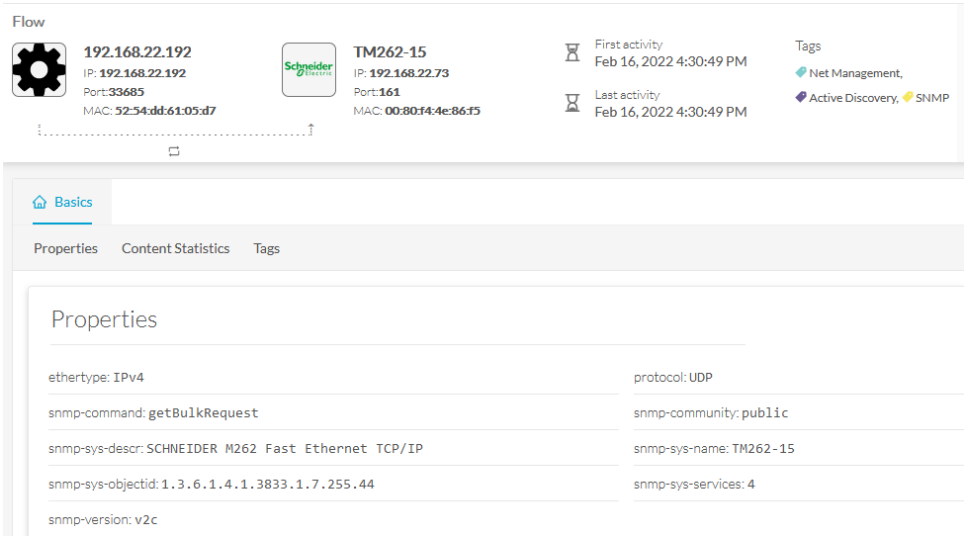
AD SNMP with Schneider PLC

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

Typcical results with nodes where SNMP is enabled by defaut are:



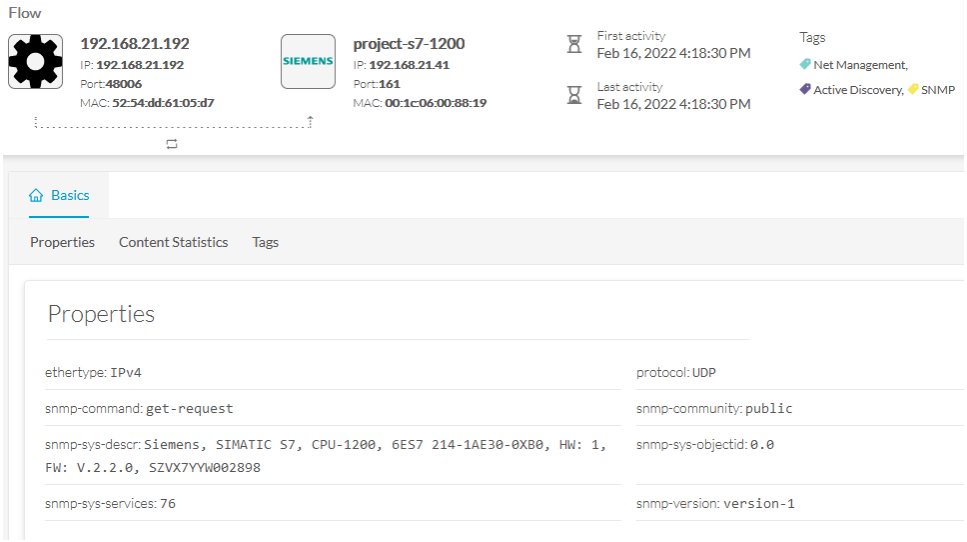


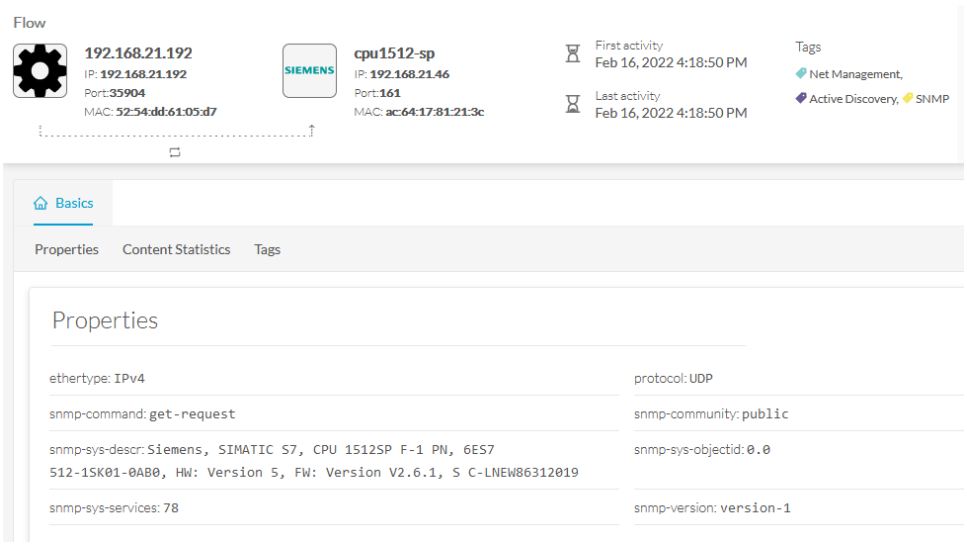


AD SNMP with Siemens PLC

The 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 defaut are:

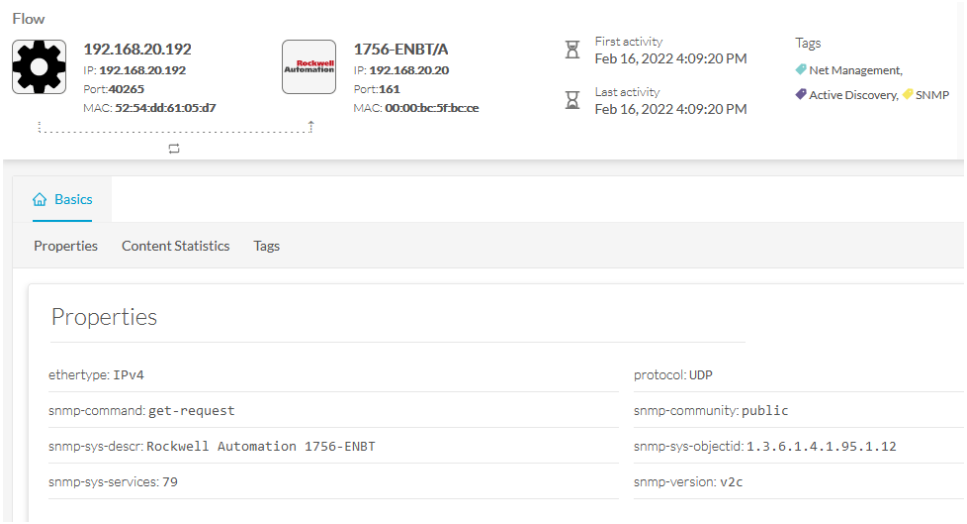




AD SNMP with Rockwell PLC

The 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 defaut are:



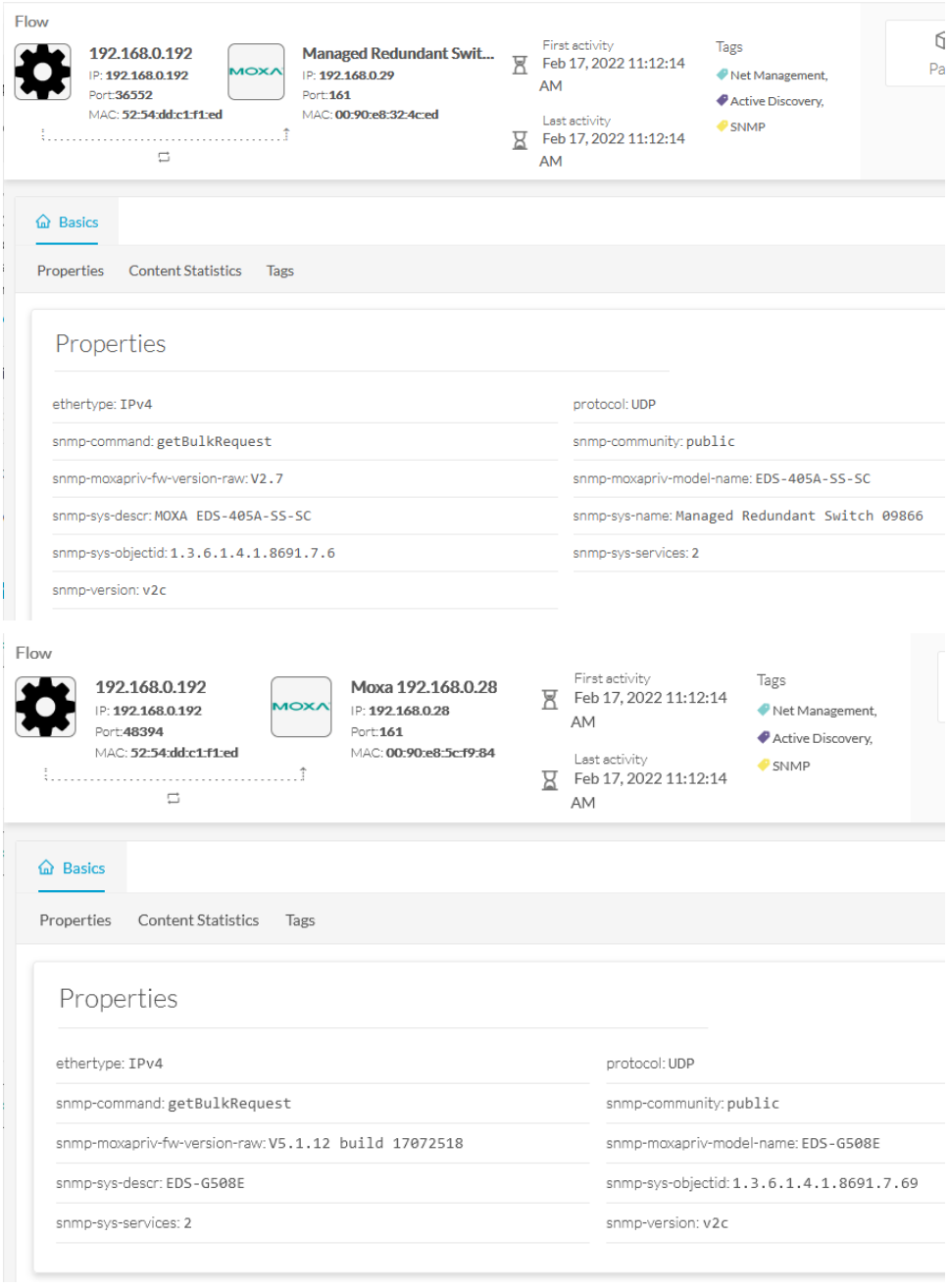
AD SNMP with Moxa switches

The 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 defaut are:

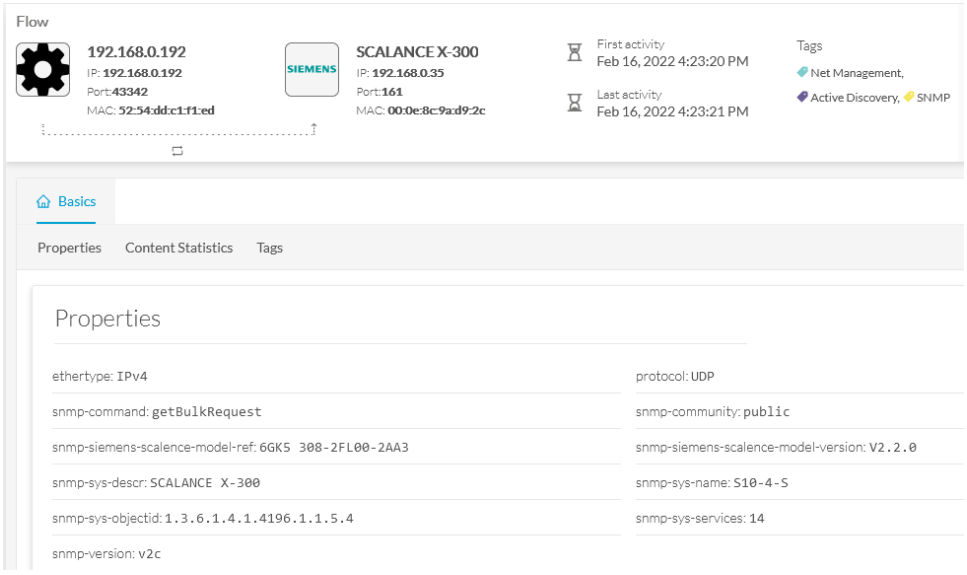


AD SNMP with Siemens Switches

The 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 defaut are:

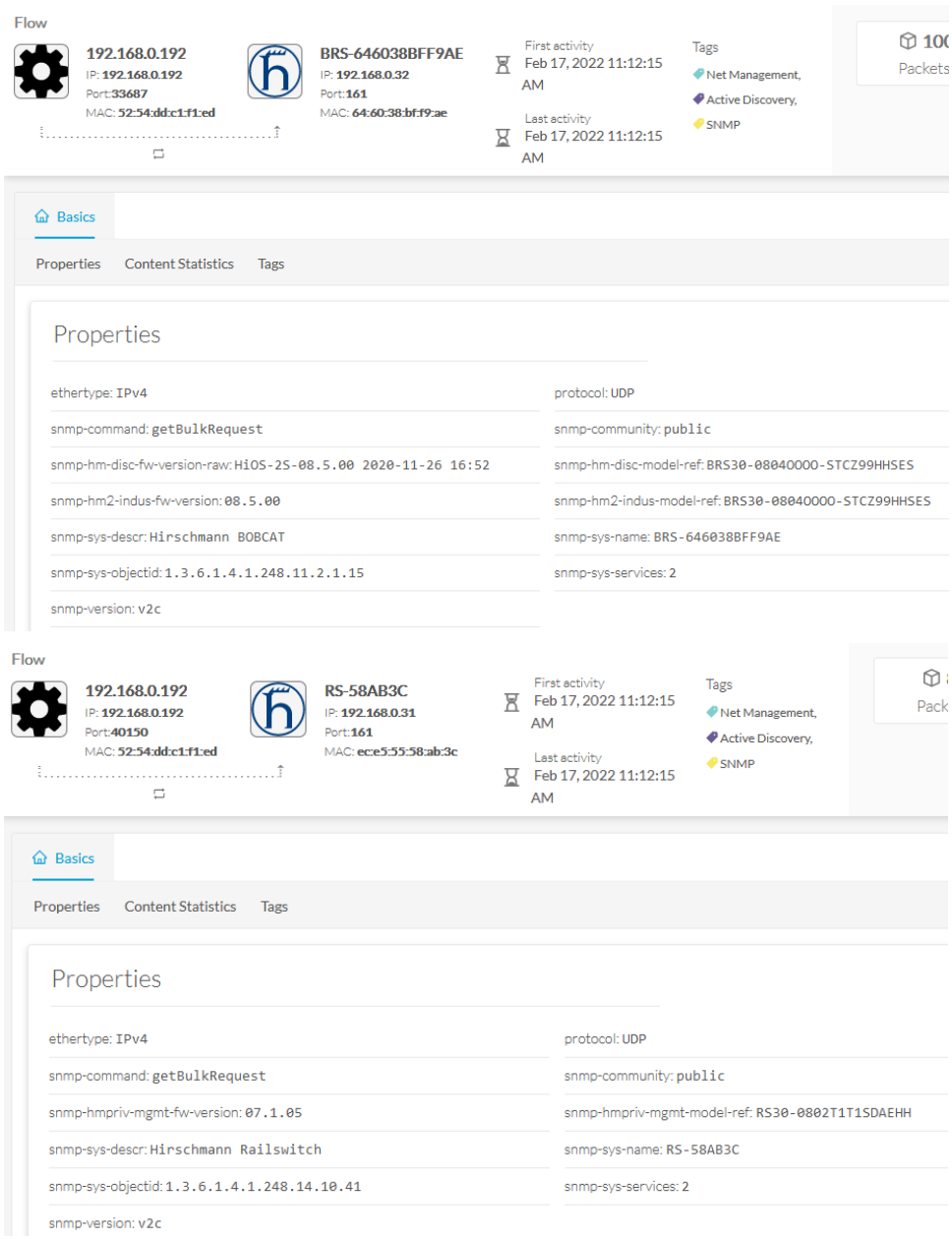


AD SNMP with Hirschmann hardware

The 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 defaut are:



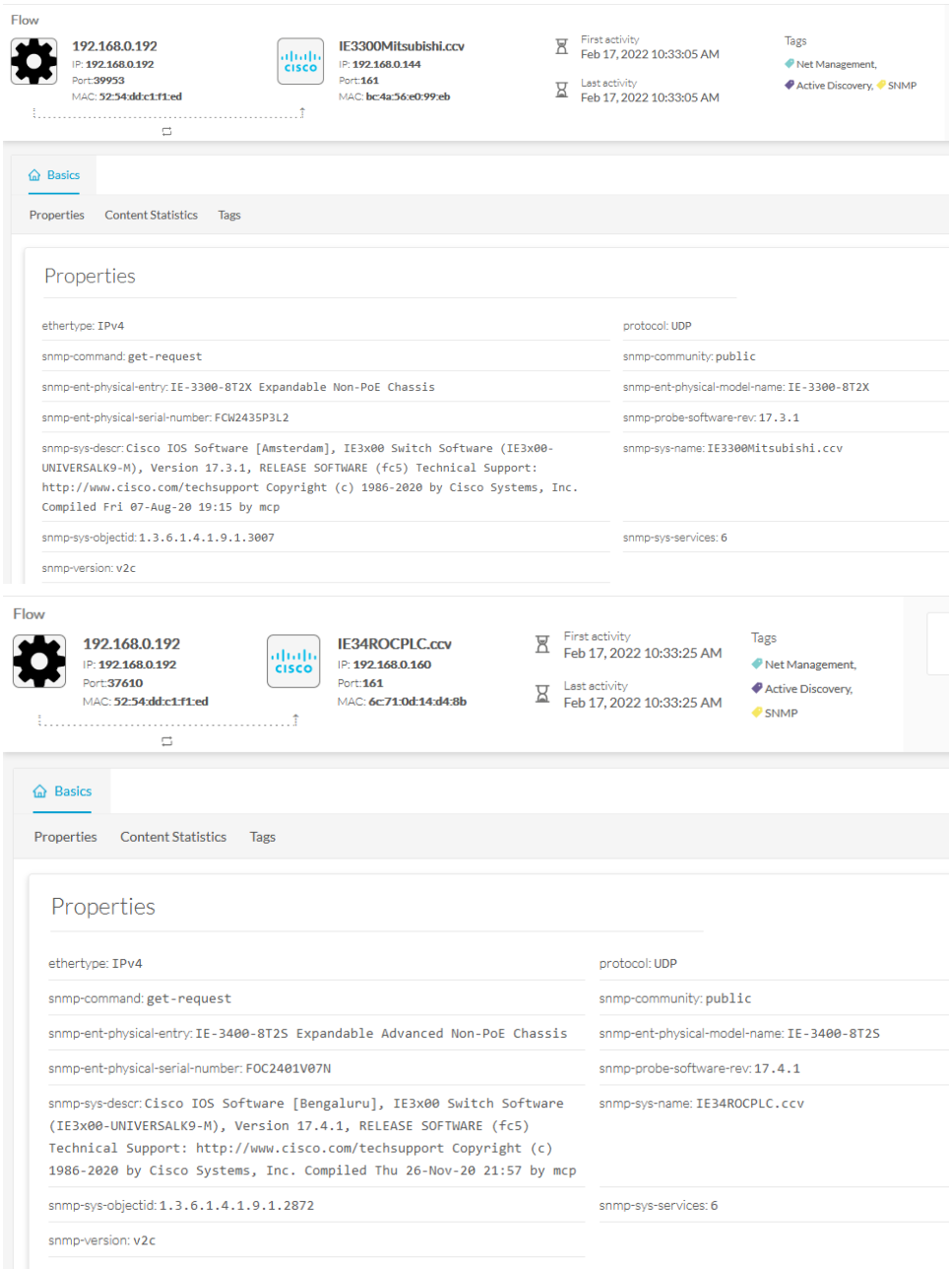
AD SNMP with Cisco hardware

The 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 defaut are:

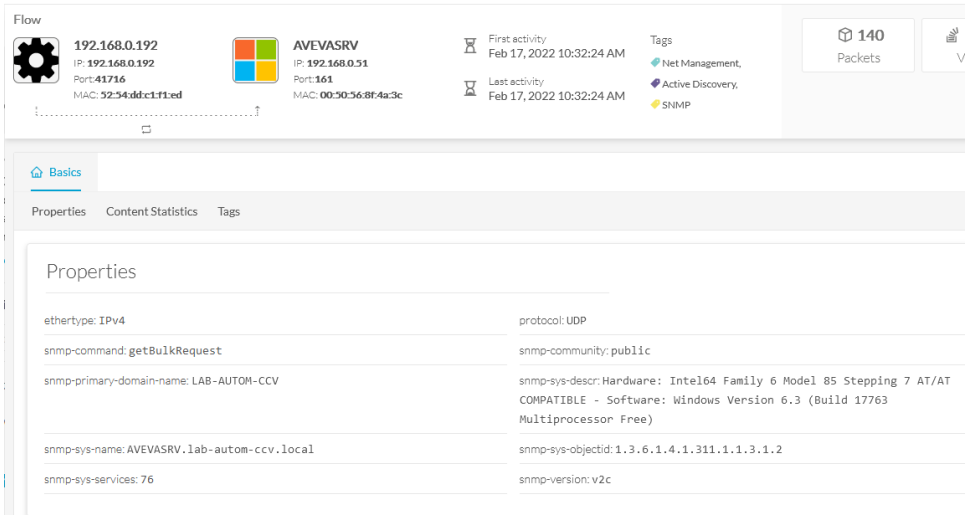


AD SNMP with Microsoft Windows OS

The 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

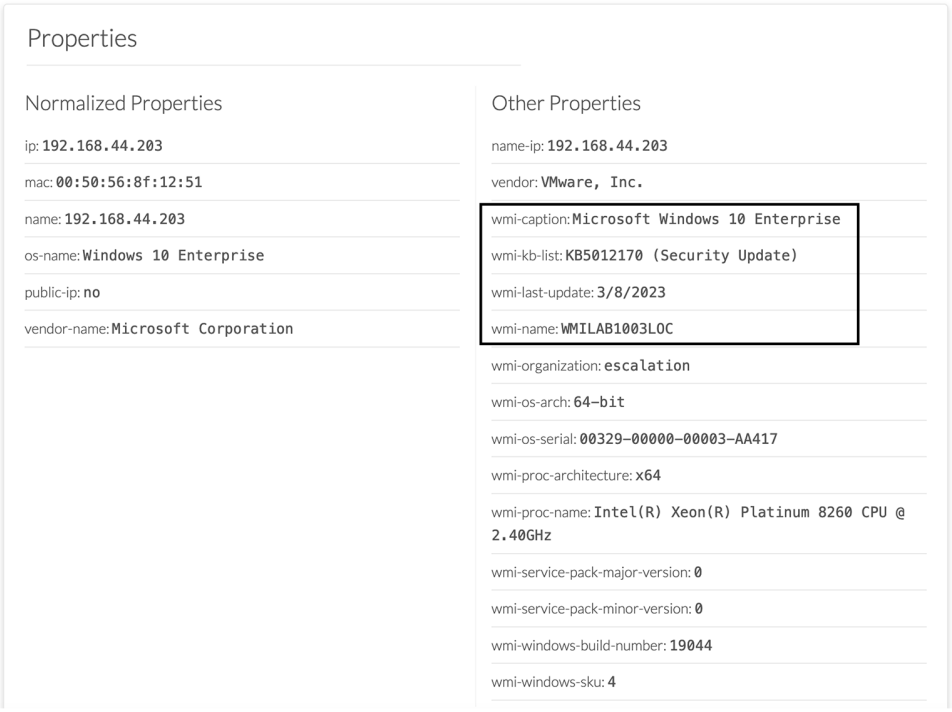
Typical results with nodes where SNMP is enabled by defaut are:



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
ip: 192.168.44.203
mac: 00:50:56:8f:12:51
name: 192.168.44.203
os-name: Windows 10 Enterprise
public-ip: no
vendor-name: Microsoft Corporation
Other Properties
name-ip: 192.168.44.203
vendor: VMware, Inc.
wmi-caption: Microsoft Windows 10 Enterprise
wmi-kb-list: KB5012170 (Security Update)
wmi-last-update: 3/8/2023
wmi-name: WMILAB1003LOC
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