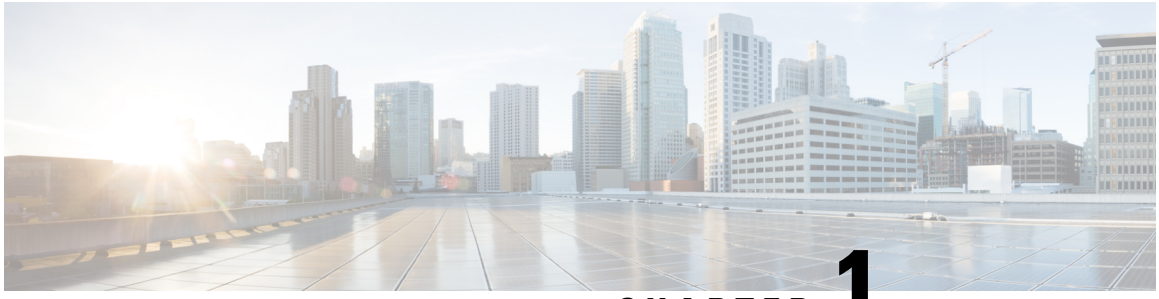
Cisco Cyber Vision Active Discovery Configuration Guide, Release 4.1.0

First Published: 2022-05-06

Last Modified: 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

CONTENTS



CHAPTER 1

About this documentation

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 4.1.0**.

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

- Cisco Catalyst IE3300 10G Rugged Series Switch
- Cisco Catalyst IE3400 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

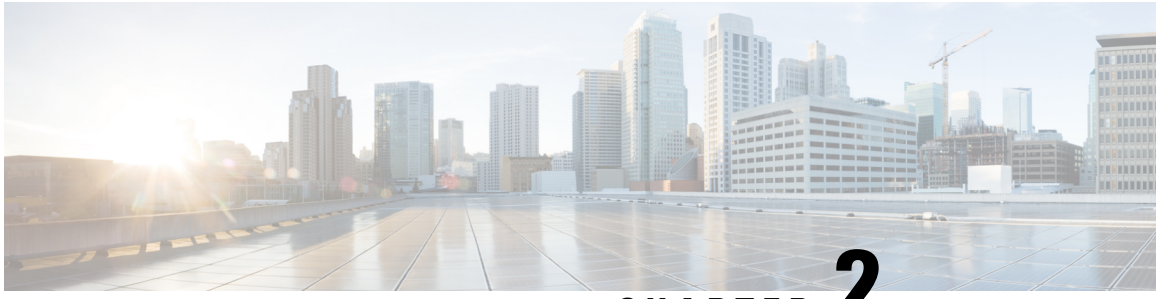
This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

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

Active Discovery overview

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
  - Siemens S7
  - Profinet
  - ICMPv6
- Unicast:
  - EtherNet/IP
  - SNMP

For more information about discoverable properties, refer to Active Discovery protocol details, on page 39.

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.

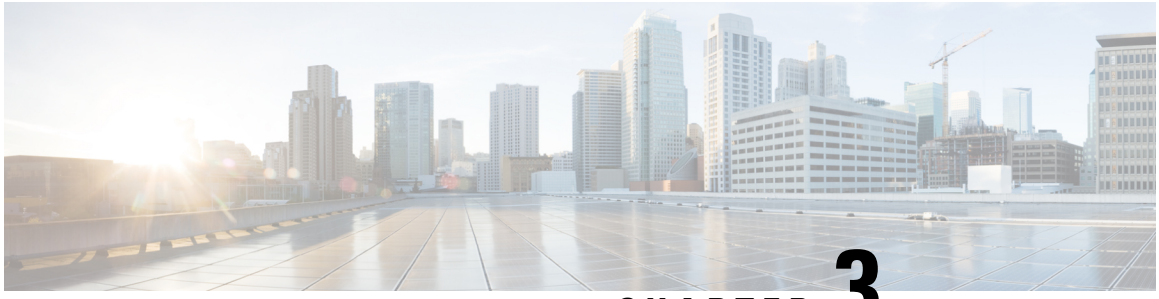
    On IOx sensors, the AppGigabit interface must be in trunk mode, and the VLAN must be allowed on this port.

    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 a preset with at least one sensor.
- Set the policy on the preset and set an execution time or run it once.



CHAPTER 3

Active Discovery 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 and Cisco IE3400.
- Cisco Catalyst 9300 and Cisco Catalyst 9400.
- Cisco IR8340 Integrated Services Router Rugged

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

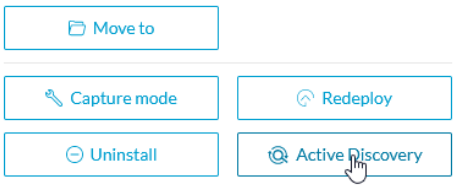
Step 1 Navigate to **Admin** > **Sensors** > **Sensor Explorer**.

Step 2 Select a sensor in the list.

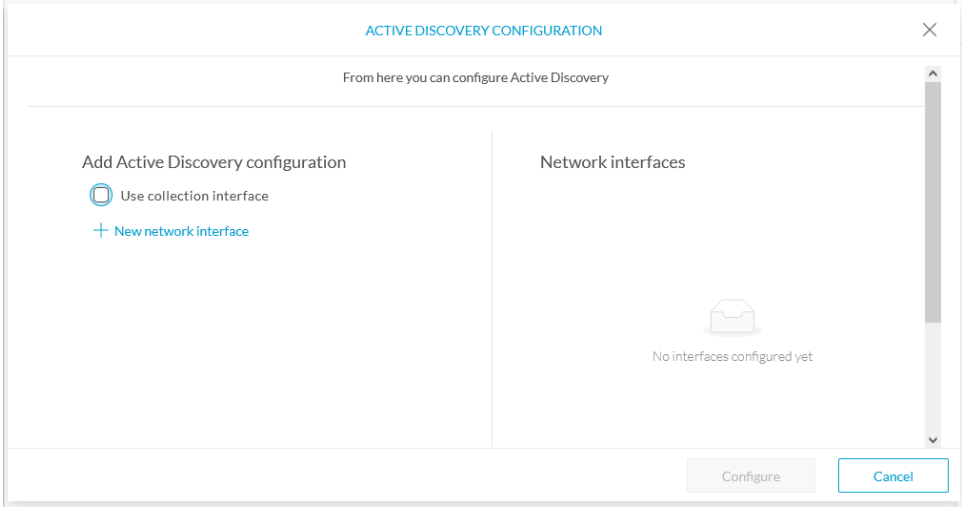
The sensor right side panel appears. The Active Discovery button is displayed if the sensor is compatible.

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.

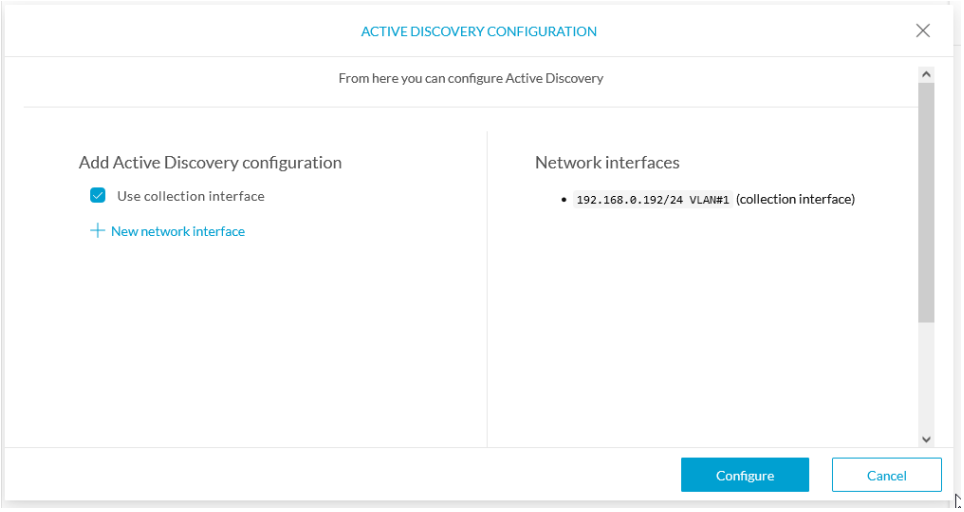


The Active Discovery Configuration window pops up:



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.

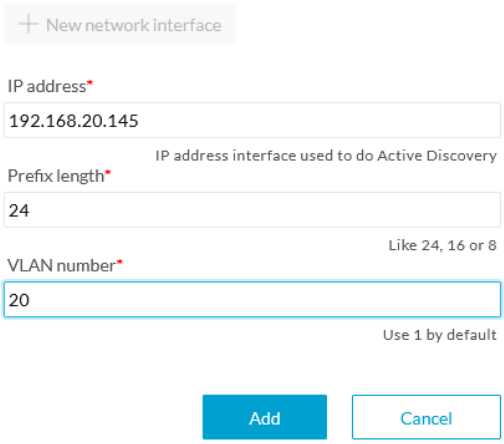


Step 5 Click + **New network interfaces** for the sensor to perform Active Discovery on additional subnetworks.

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

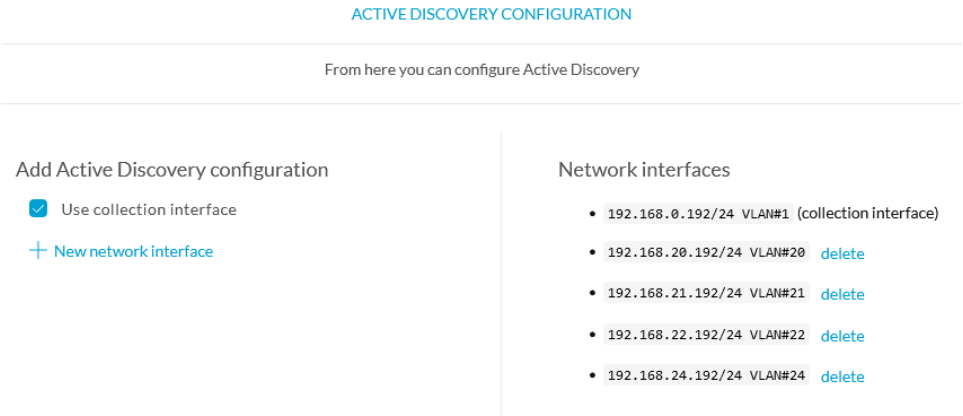
- IP address
- Prefix length

- 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:

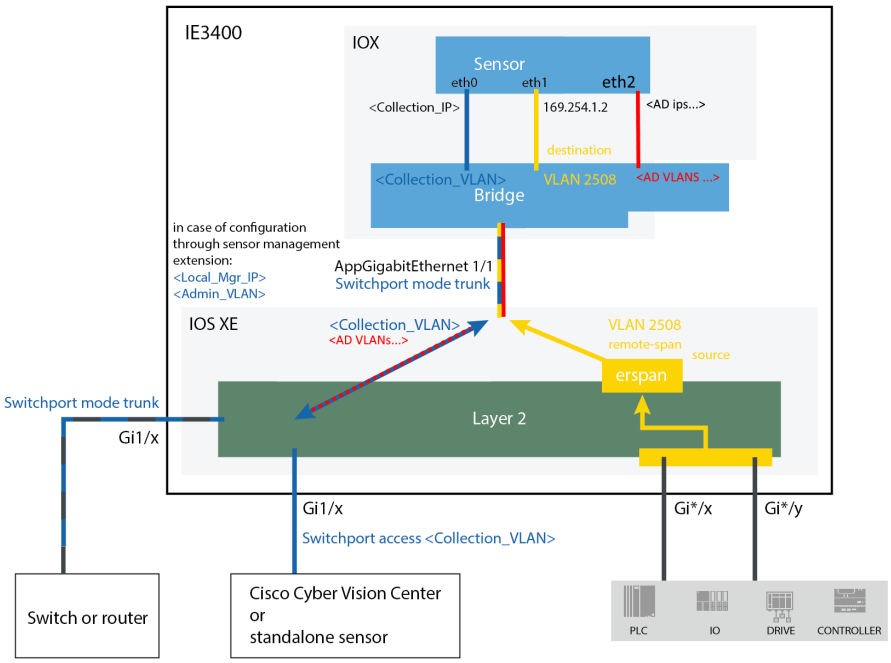


Figure 2: Catalyst 9300 and Catalyst 9400:

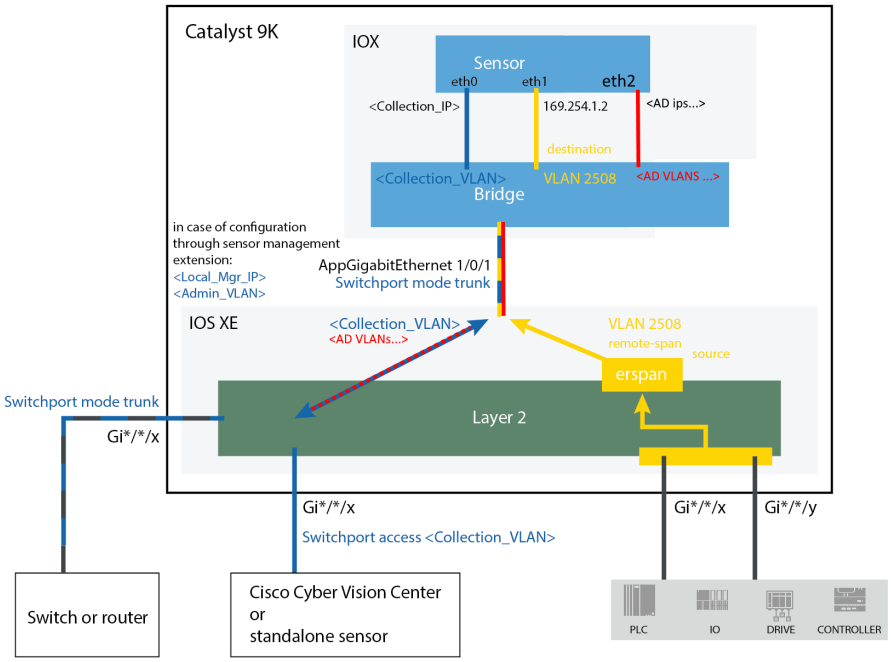
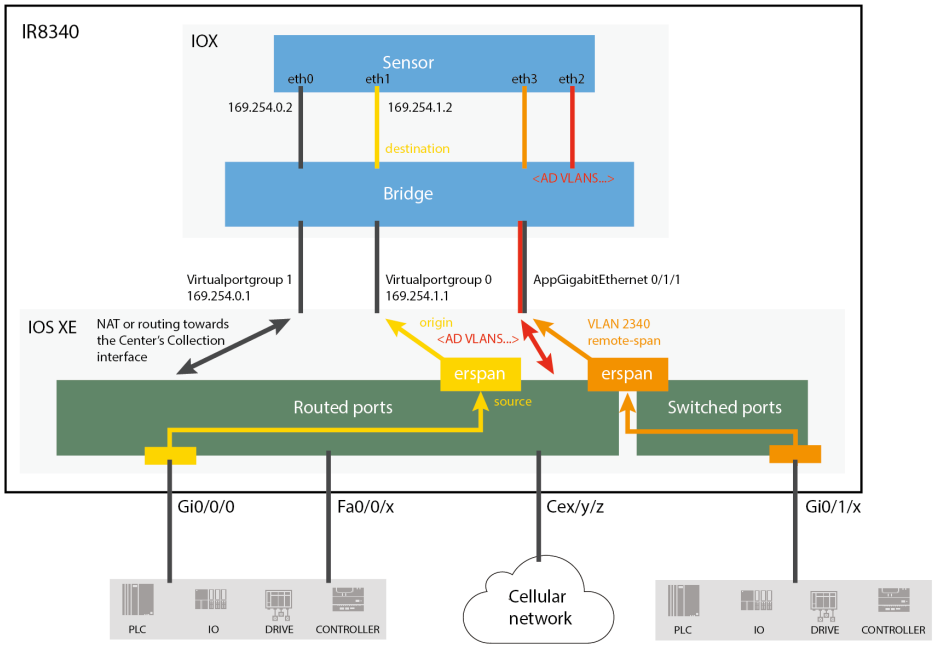


Figure 3: IR8340:



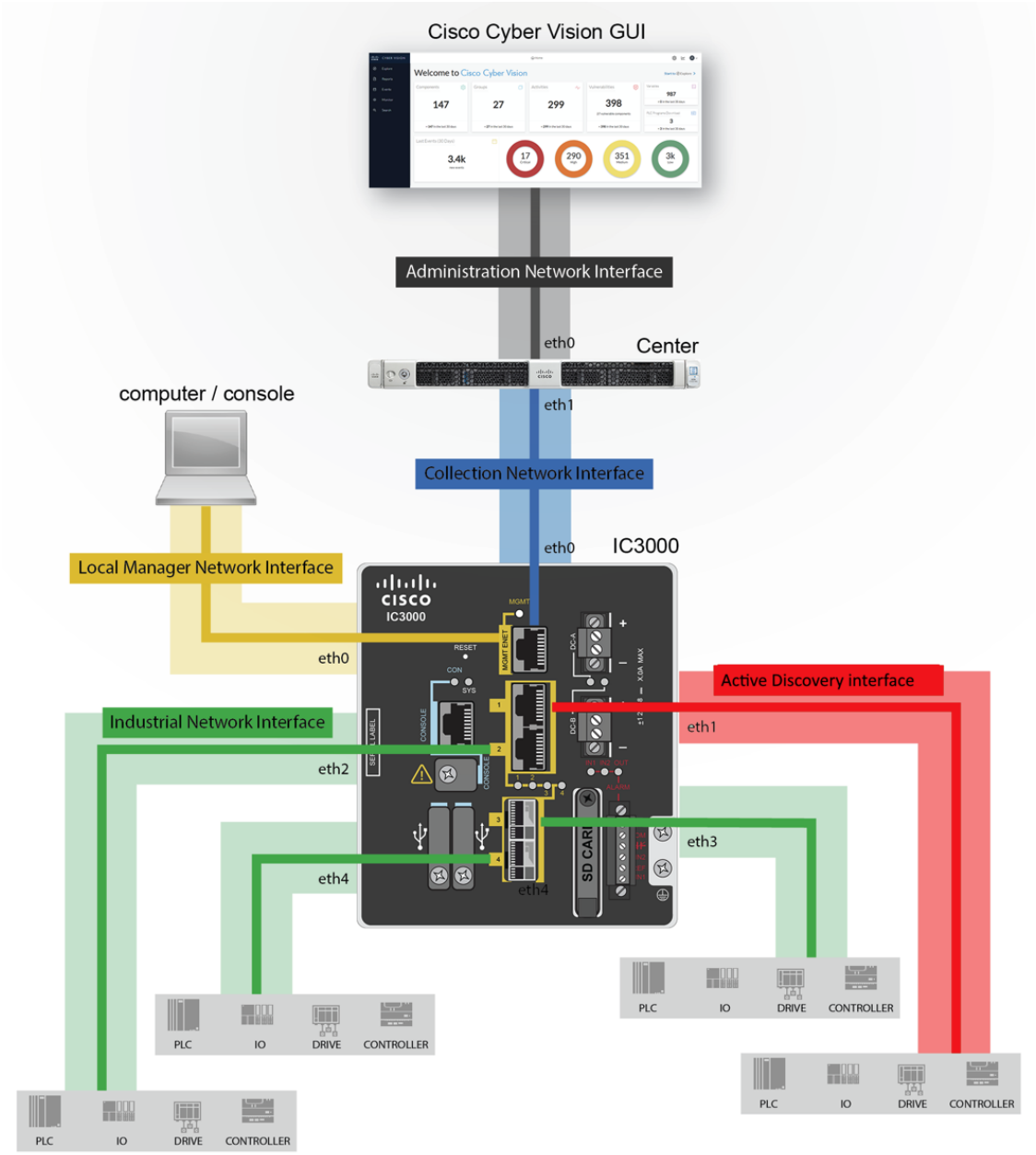
What to do next

Proceed to Active Discovery policies configuration, on page 21.

Configure Active Discovery on a Cisco IC3000

An interface must be defined on the Cisco IC3000 for Active Discovery to be enabled. Active Discovery can be set on the Collection network interface (i.e. the management port), or one of the four other interfaces of the Cisco IC3000 (i.e. int 1 to int 4).

Example: Active Discovery set on int1 (in red):



In any case, to configure Active Discovery on a Cisco IC3000, you have two options:

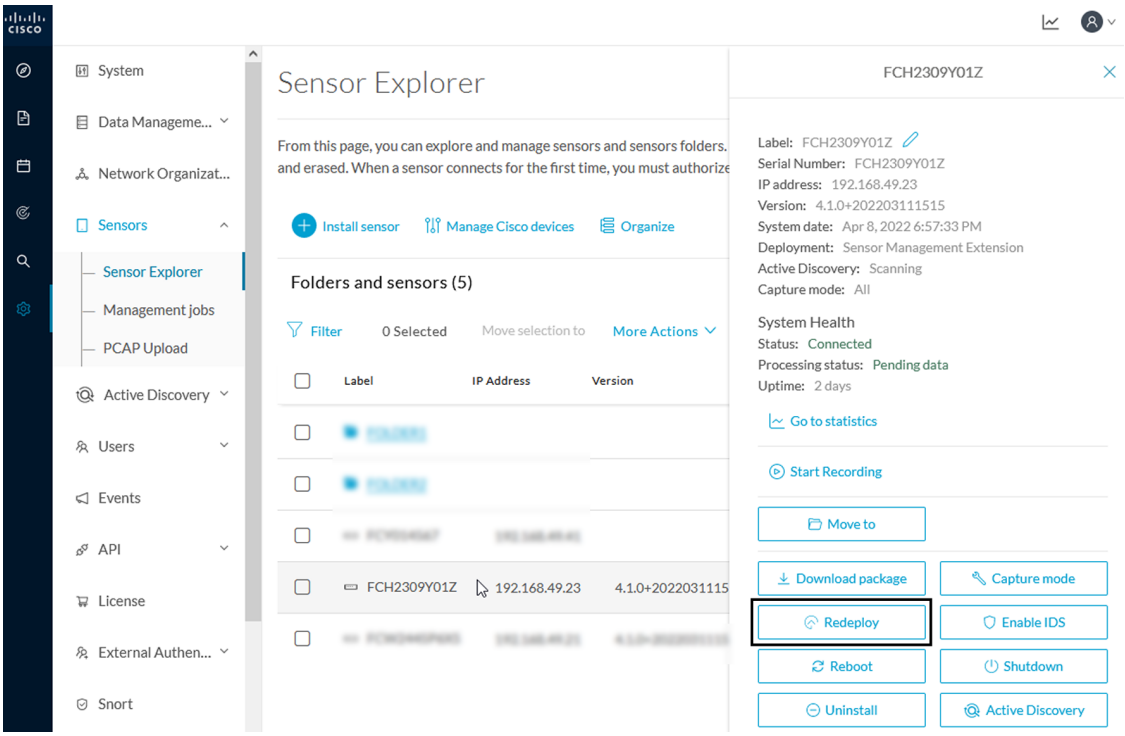
- To redeploy the Cisco IC3000 sensor with Active Discovery through the sensor management extension on Cisco Cyber Vision.
- To set up Active Discovery on the sensor, retrieve the provisioning package and deploy it on the device through the Local Manager.

Redeploy the Cisco IC3000 with Active Discovery

Redeploy the sensor to enable and configure Active Discovery on the Cisco IC3000.

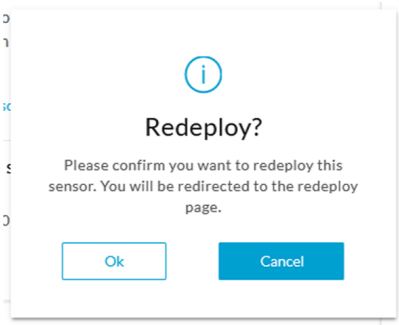
Step 1 On the Sensor Explorer page, click the sensor to reconfigure/redeploy. The sensor right side panel appears.

Step 2 Click **Redeploy**.



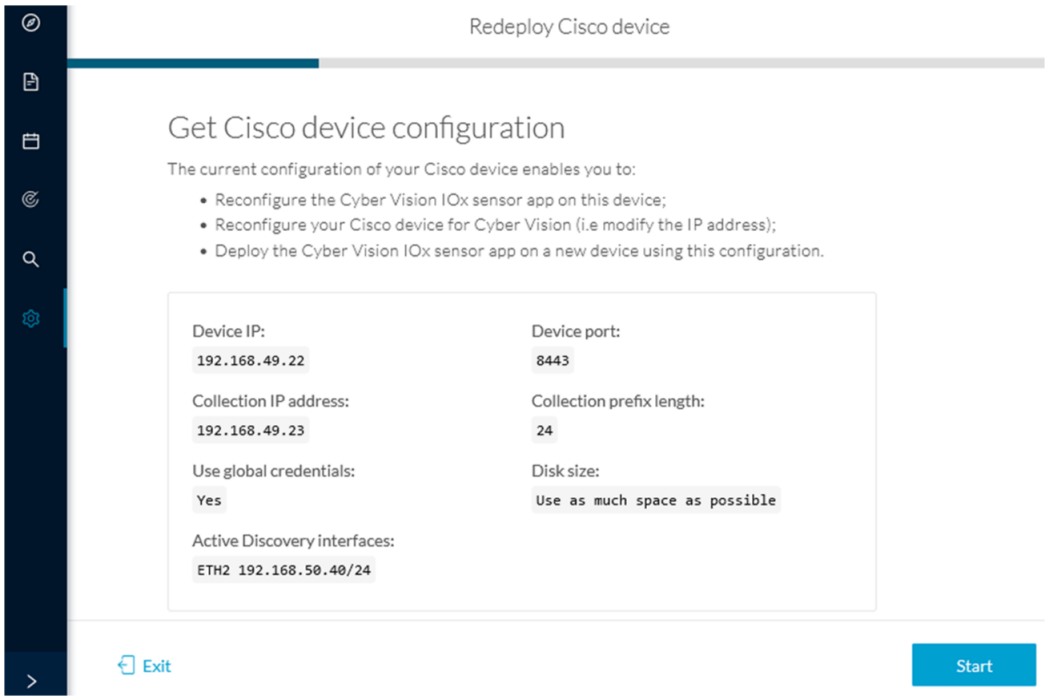
A pop up asking to confirm the redeployment of the sensor appears.

Step 3 Click **OK** to proceed.

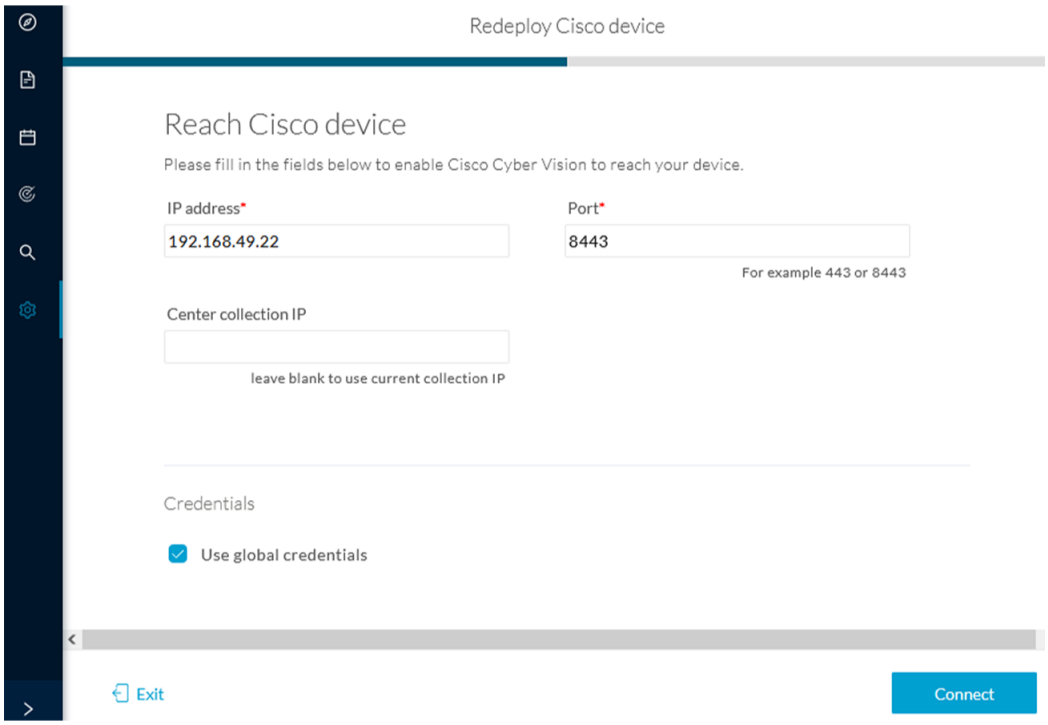


A summary of the sensor configuration is displayed.

Step 4 Click **Start**.



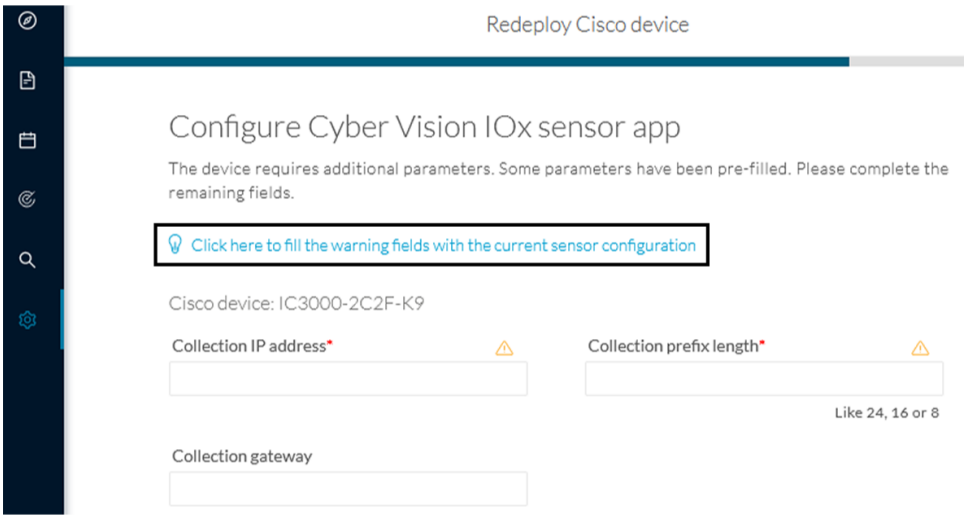
The reach Cisco device window appears. The device's IP address and port are displayed.



Step 5 Enter the credentials to reach the device or tick **Use global credentials**.

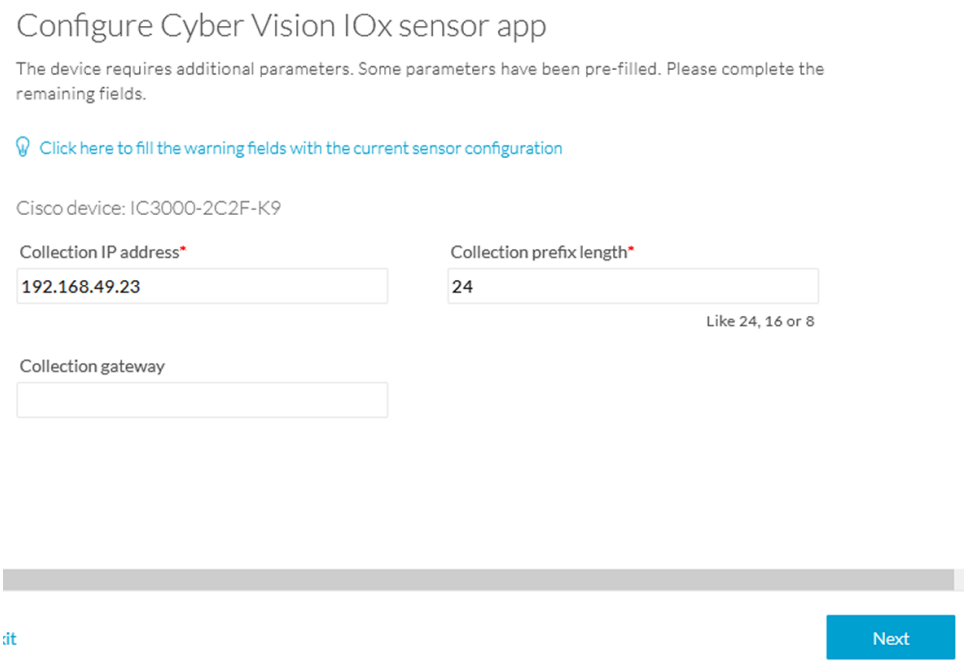
Step 6 Click **Connect**.

The Configure Cyber Vision IOx sensor app window appears.



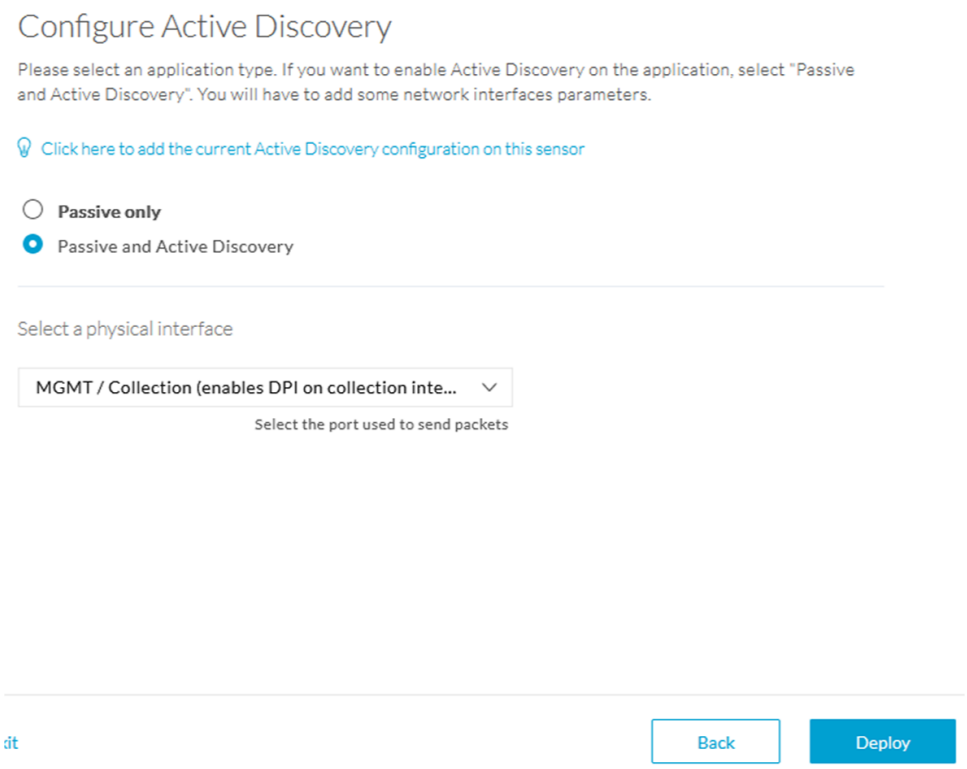
Step 7 Click the blue link to fill the warning fields with the current sensor configuration.

The Collection IP address and Collection prefix length are automatically filled.



Step 8 Click **Next**.

The Configure Active Discovery window appears.

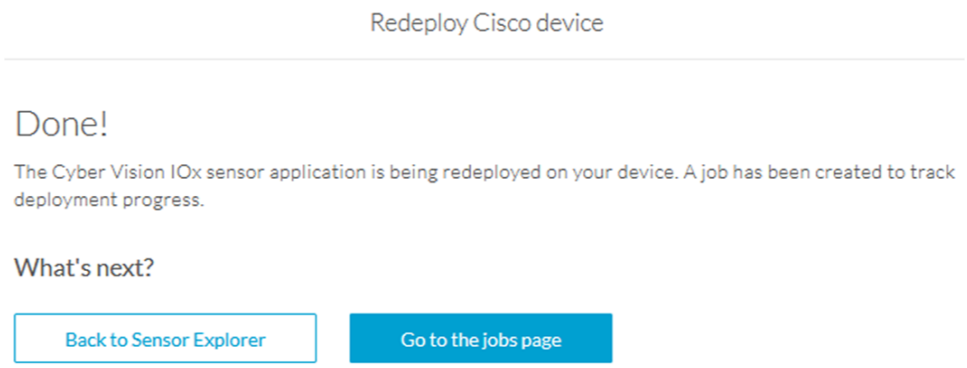


Step 9 Select **Passive and Active Discovery**.

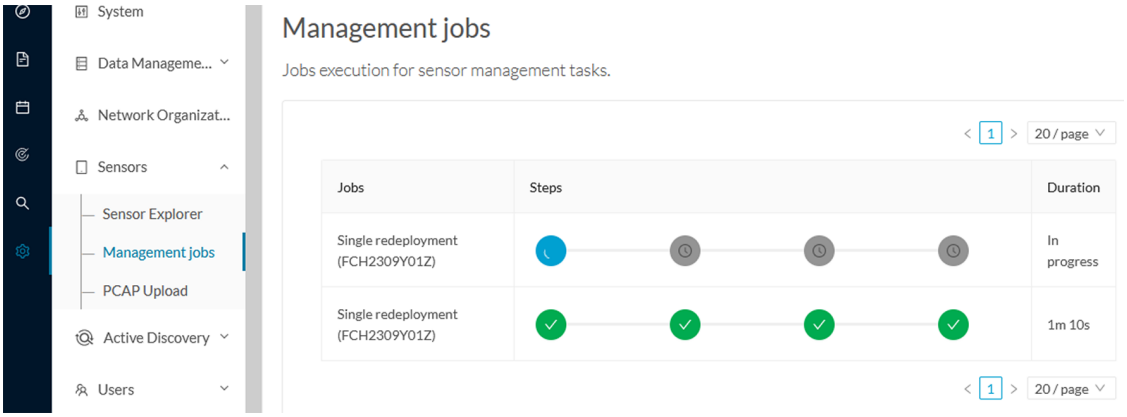
Step 10 Select a physical interface.

Step 11 Click **Deploy**.

A message saying that the sensor is being redeployed appears. You can either go the jobs page or go back to the Sensor Explorer page.

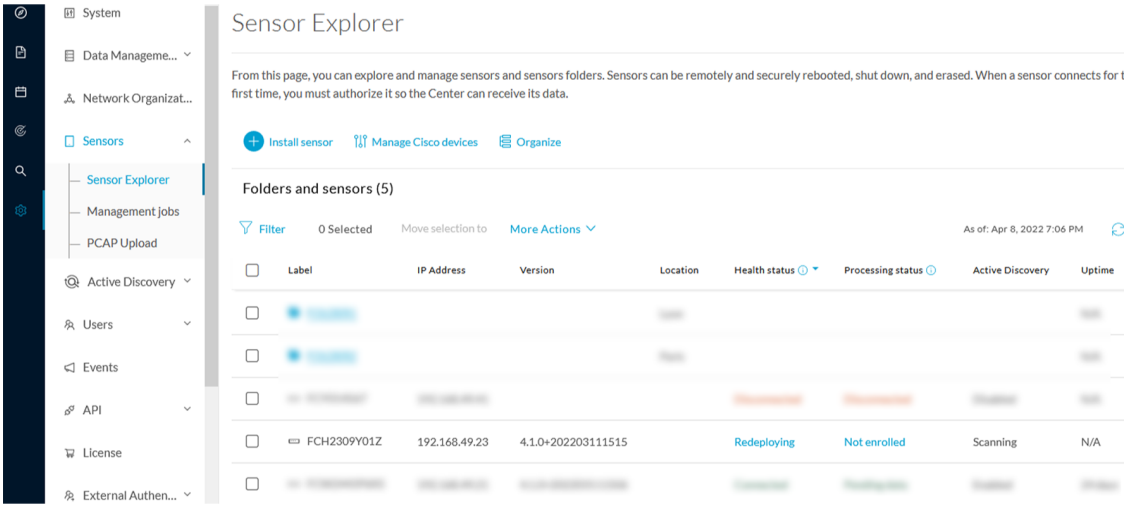


If you click **Go to the jobs page** you are redirected to the Management jobs page.

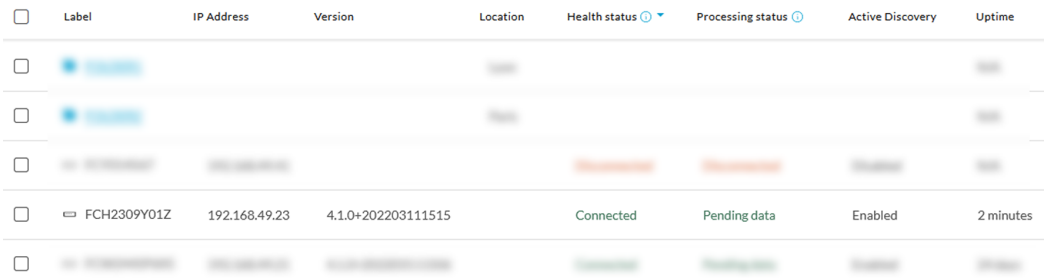


You can see the redeployment advancement. This can take several minutes.

If you go back to the Sensor Explorer page, you will see that the sensor is in Redeploying status.



Once the redeployment is finished, the sensor will switch status to Connected and Active Discovery to Enabled.



What to do next

Proceed to Active Discovery policies configuration, on page 21.

Manually configure Active Discovery on the Cisco IC3000

To do so, you will:

1. Set up the Cisco IC3000 sensor with Active Discovery on Cisco Cyber Vision and download the provisioning package.
2. Deploy the provisioning package on the Cisco IC3000 device through the Local Manager.

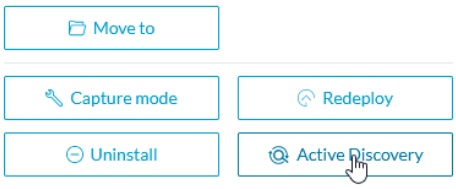
Set up Active Discovery on Cisco Cyber Vision

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

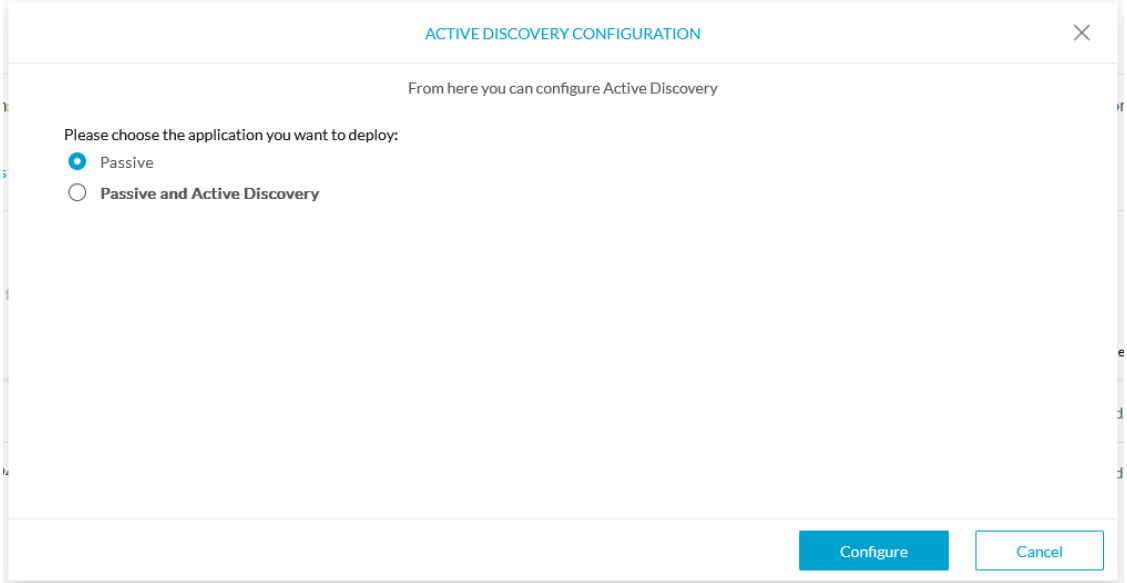
Step 2 Select a sensor in the list.

The sensor right side panel appears.

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

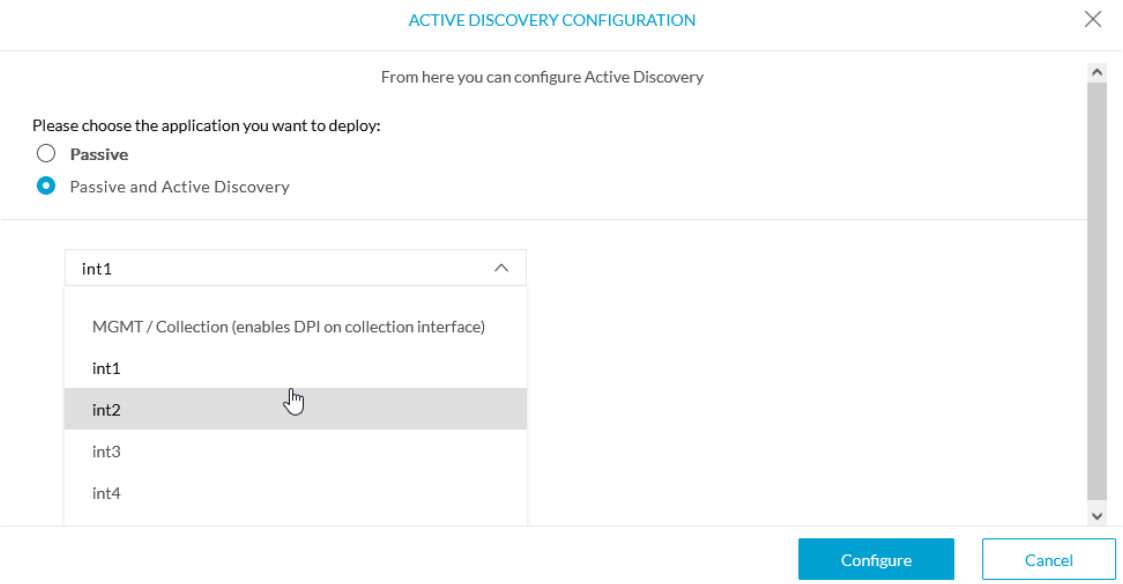


The Active Discovery configuration window pops up.



Step 4 Select the **Passive and Active Discovery** option.

A list of network interfaces appears.



Step 5 Select the network interface dedicated to Active Discovery, i.e. the management port or one of the four interfaces.

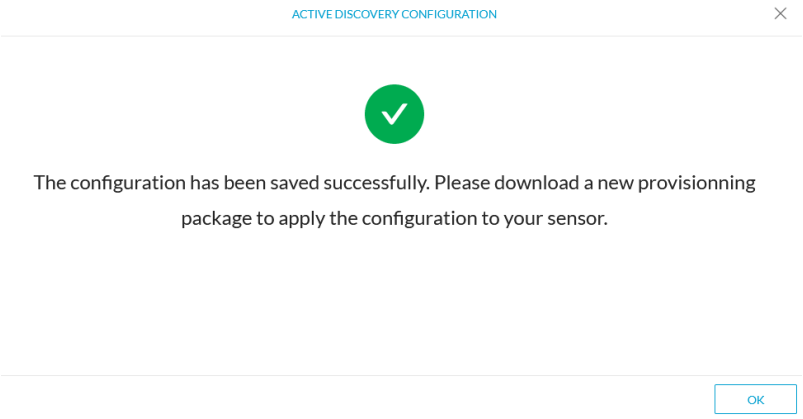
The following fields appears:

- IP address
- Prefix length

Step 6 Fill them with the proper network information.

Step 7 Click **Configure**.

The following message appears:



Step 8 Click **OK**.

Step 9 In the sensor list, click the Cisco IC3000 you just set with Active Discovery.

Its right side panel appears.

Step 10 Click **Download package**.

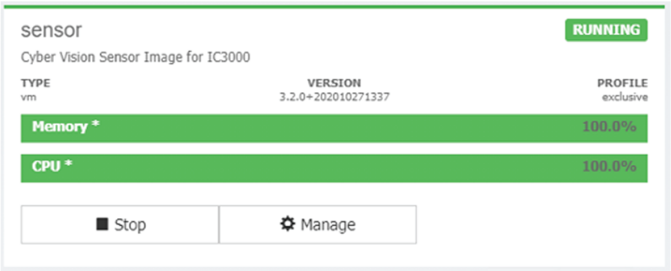
The provisioning package including the Active Discovery configuration is downloaded.

What to do next

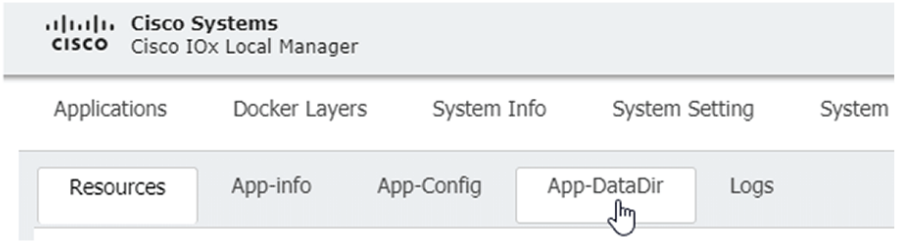
Import the provisioning package in the Cisco IC3000 device through the Local Manager.

Import the provisioning package

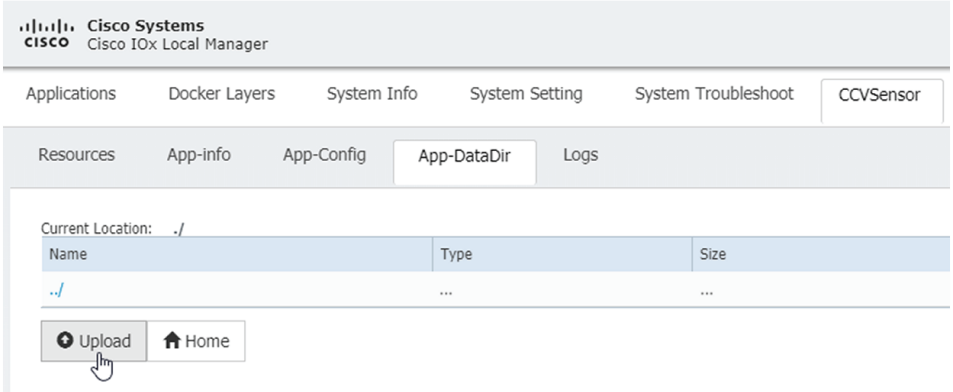
1. In the Local Manager, in the IOx configuration menu, click **Manage**.



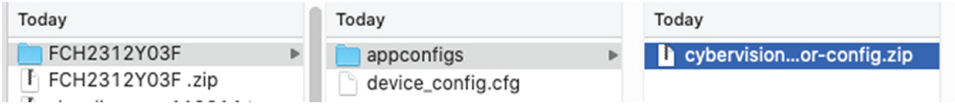
2. Navigate to **App_DataDir**.



3. Before browsing the file, you must unzip the provisioning package.
4. Click **Upload**.

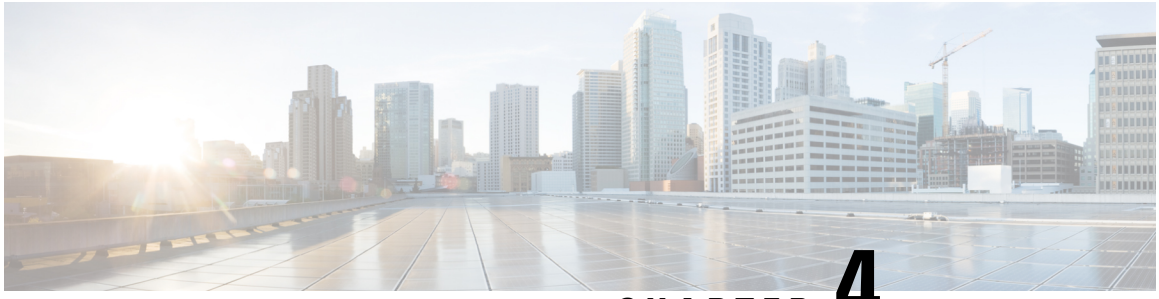


5. Navigate to the folder with the sensor serial name (i.e. FCH2312Y03F) > appconfigs, and select cybervision-sensor-config.zip.



6. Make sure the path contains the entire file name (with .zip).

7. Click **OK**.

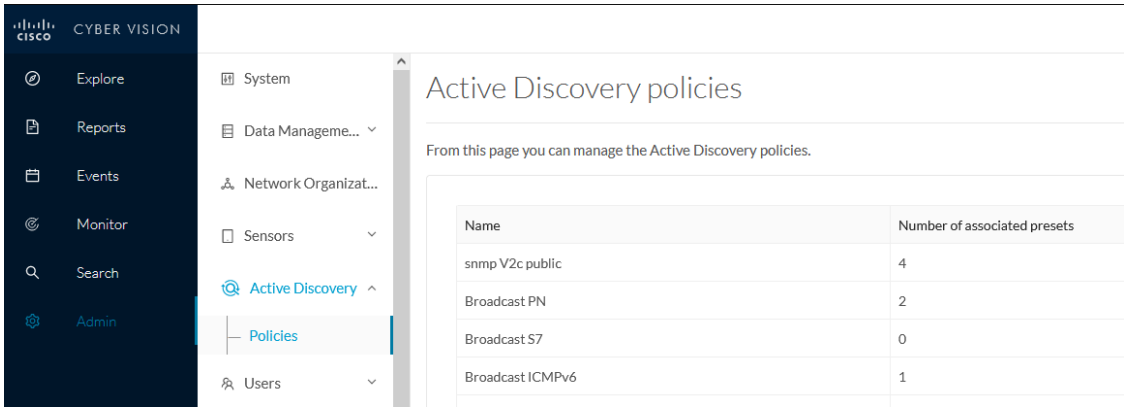


CHAPTER 4

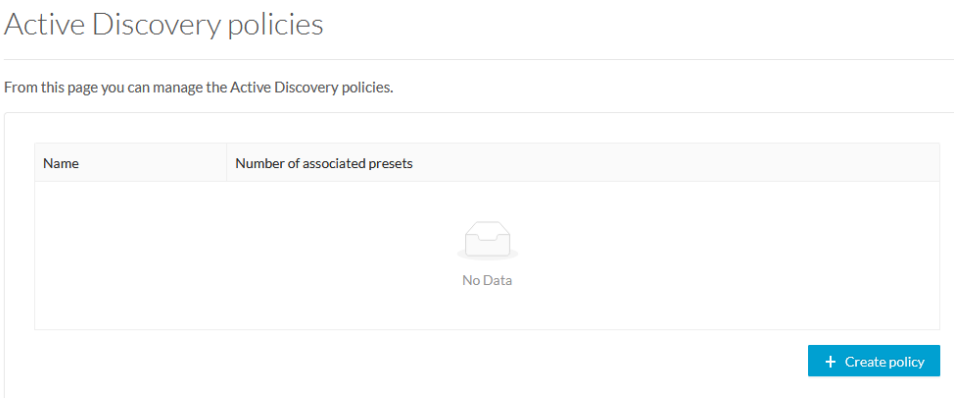
Active Discovery policies configuration

Create a policy

An Active Discovery policy is a list of settings which define protocols and their parameters that will be used to scan the industrial network. The policy will be used in a preset and be applied on a list of sensors and components.

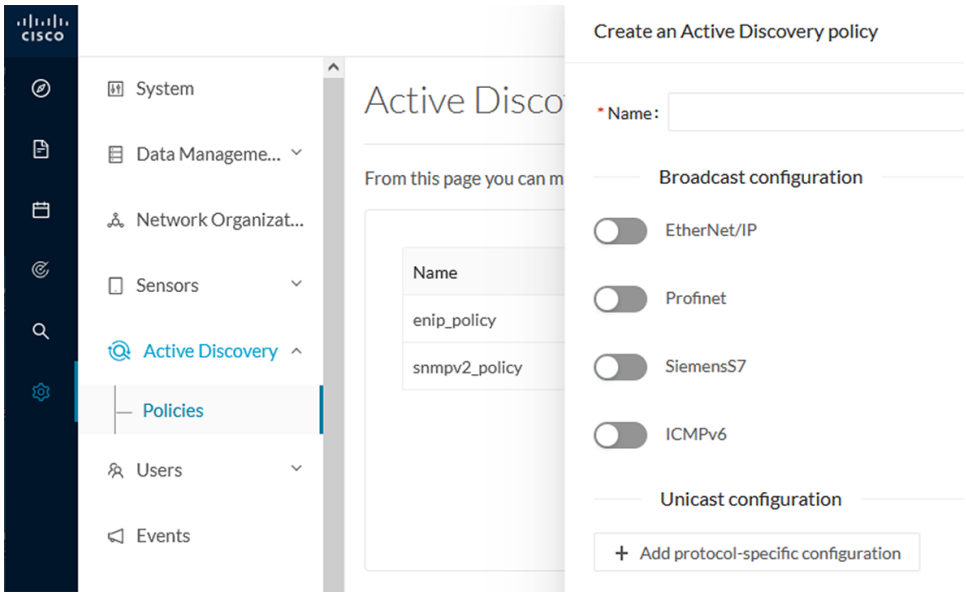


Step 1 Navigate to **Admin** > **Active Discovery** > **Policies** .



Step 2 Click + **Create policy**.

A Create an Active Discovery policy overlay appears.



What to do next

- Set Active Discovery Broadcast, on page 23
- Set Active Discovery Unicast Ethernet/IP, on page 24
- Set Active Discovery Unicast SNMPv2c, on page 25
- Set Active Discovery Unicast SNMPv3, on page 27

Set Active Discovery Broadcast

Before you begin

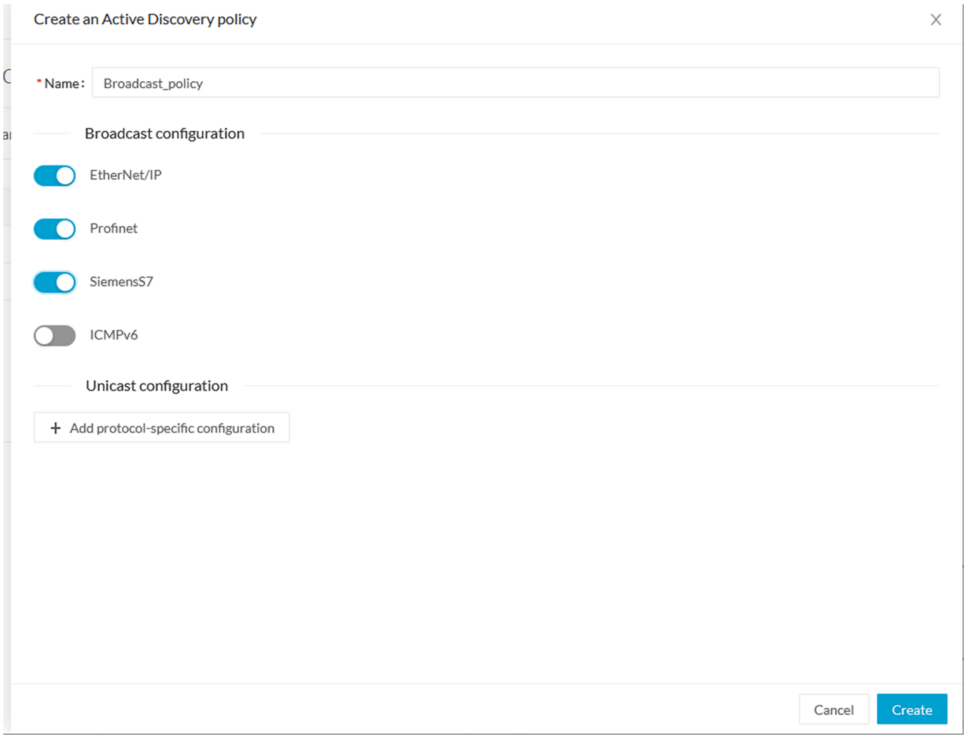
Active Discovery is compatible with the following Broadcast protocols:

- EtherNet/IP
- Siemens S7
- Profinet
- ICMPv6

The sensor will send requests on all defined interfaces.

Step 1 Type a policy name.

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



Step 3 Click **Create** to finish or add Unicast configurations to the policy.

What to do next

Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast Ethernet/IP, on page 24.

- Set Active Discovery Unicast SNMPv2c, on page 25.
- Set Active Discovery Unicast SNMPv3, on page 27.

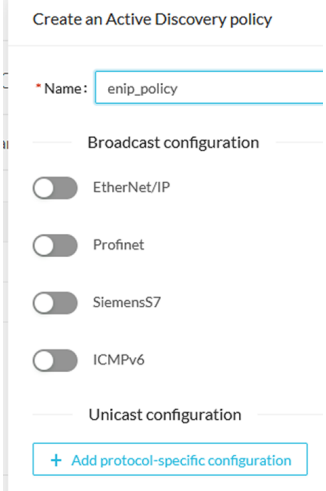
Active Discovery preset configuration.

Set Active Discovery Unicast Ethernet/IP

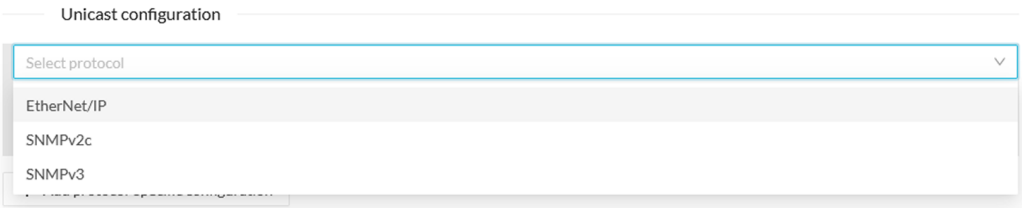
Set Active Discovery Unicast Ethernet/IP to scan all the devices and components in a preset with Ethernet/IP requests. All components with an IPV4 address will be scanned.

Step 1 Give the policy a name.

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



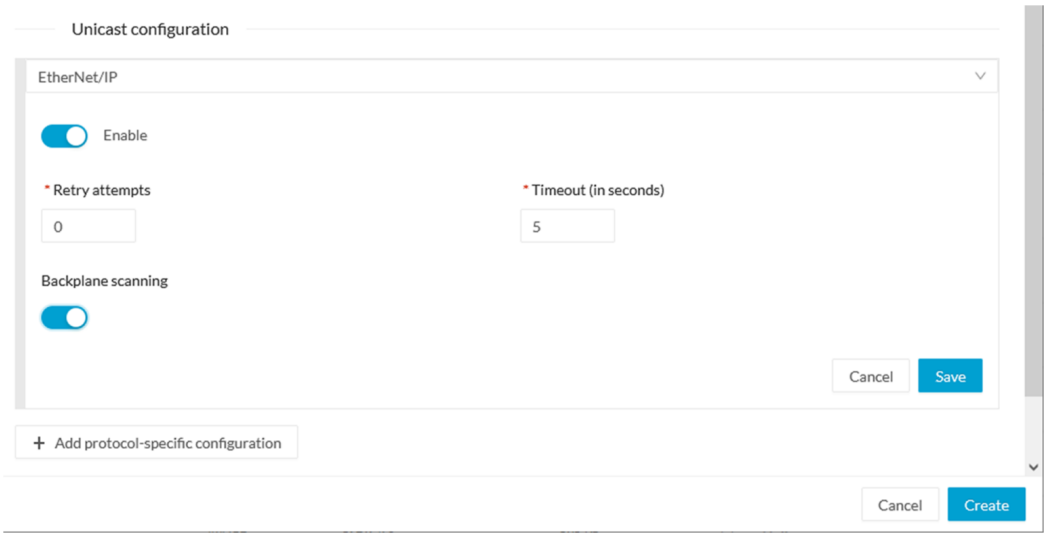
Step 3 Click the **Select protocol** dropdown menu and select **EtherNet/IP**.



Step 4 Toggle the **Enable** button ON.

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

Step 6 You can toggle the **Backplane scanning** button ON. Active Discovery will look for PLCs and I/O chassis with module details.



Step 7 Click **Save**.

The menu closes.

Step 8 Click **Create**.

What to do next

Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast SNMPv2c, on page 25.
- Set Active Discovery Unicast SNMPv3, on page 27.

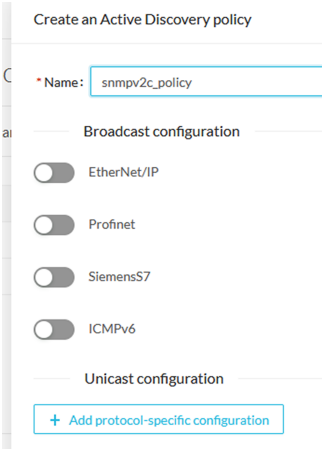
Active Discovery preset configuration.

Set Active Discovery Unicast SNMPv2c

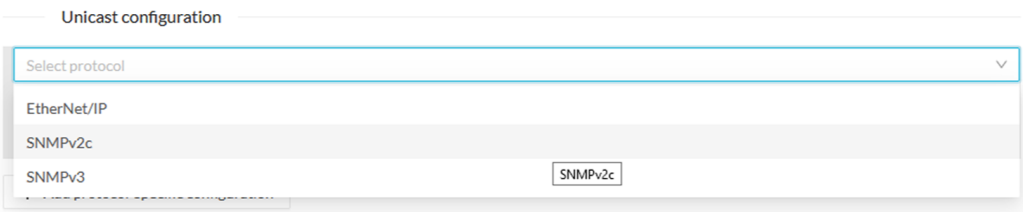
Set Active Discovery Unicast SNMPv2c to scan all the devices and components in a preset with SNMPv2c requests. All components with an IPV4 address will be scanned. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

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 **SNMPv2c**.



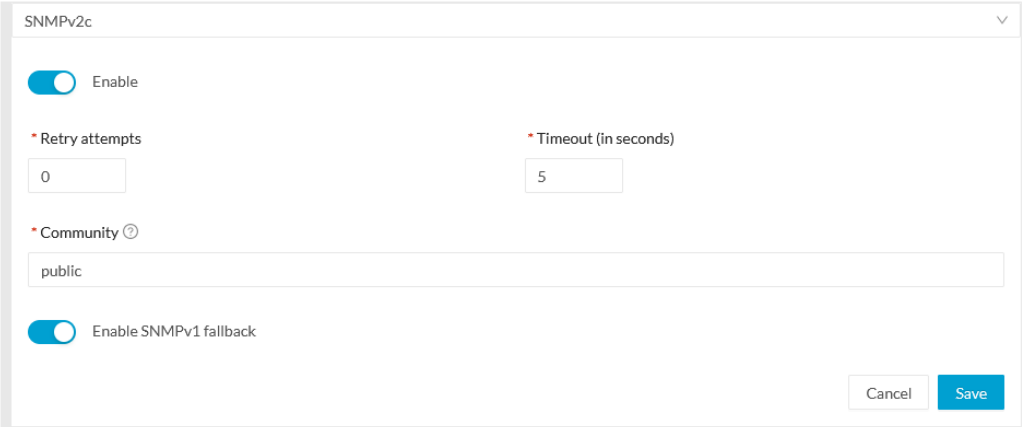
Step 4 Toggle the **Enable** button ON.

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

Step 6 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 7 You can toggle the **Enable SNMPv1 fallback** button ON. Active Discovery will look for PLCs and I/O chassis with module details.



Step 8 Click **Save**.

The menu closes.

Step 9 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.

What to do next

Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast Ethernet/IP, on page 24
- Set Active Discovery Unicast SNMPv3, on page 27.

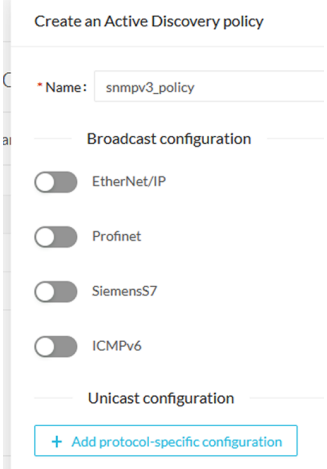
Active Discovery preset configuration.

Set Active Discovery Unicast SNMPv3

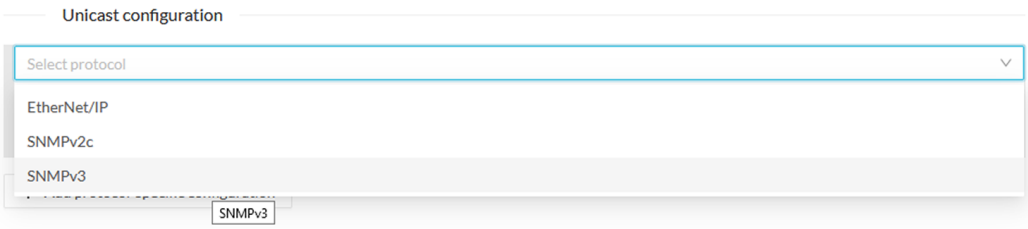
Set Active Discovery Unicast SNMPv3 to scan all the devices and components in a preset with SNMPv3 requests. All components with an IPV4 address will be scanned. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

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 **SNMPv3**.



Step 4 Toggle the **Enable** button ON.

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

Step 6 Type a community string for authentication.

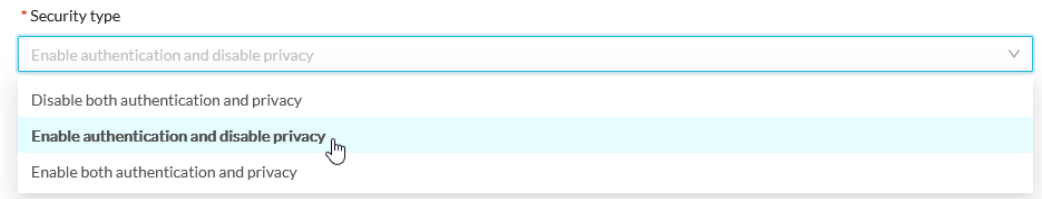
The community string is defined by IT or network administrators. The value "public" is often used by default.

Step 7 Select the proper security and privary 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.**

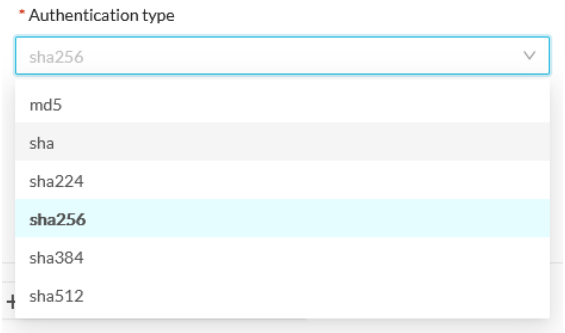
  Only a username is requested for authentication.



- **Enable authentication and disable privacy.**

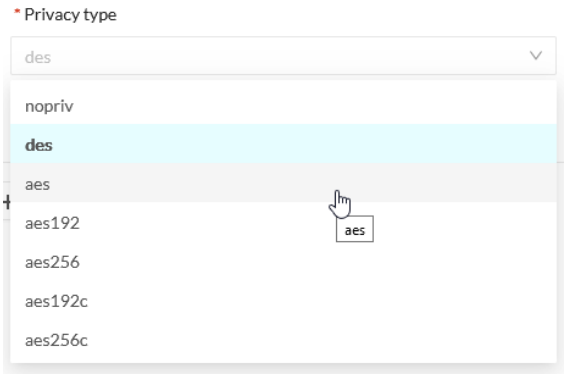
  Authentication will be based on HMAC-MD5 or HMAC-SHA algorithms.

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

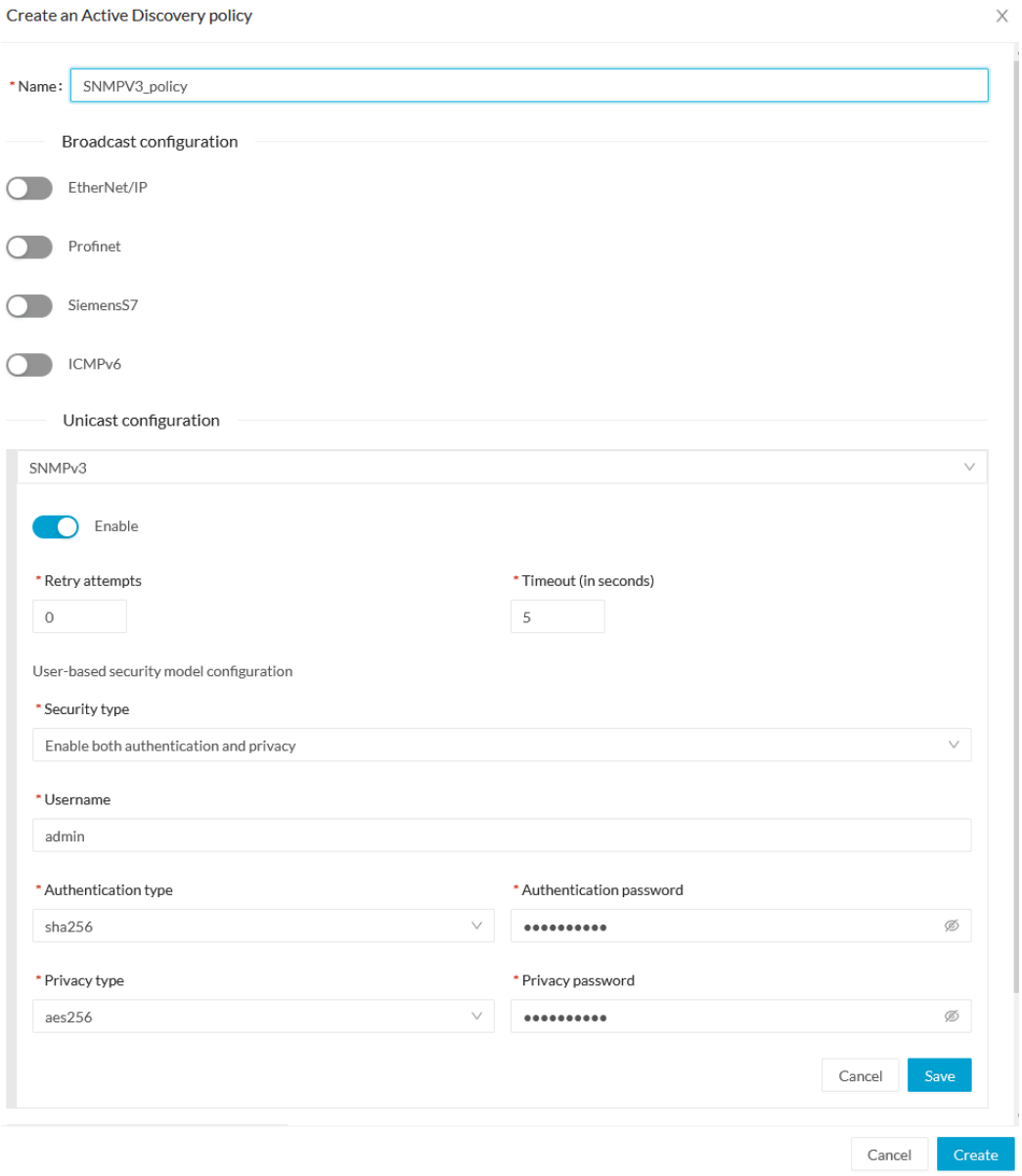


- **Enable both authentication and privacy.**

  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 **Save**.



The menu closes.

Step 9 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.

What to do next

Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast Ethernet/IP, on page 24

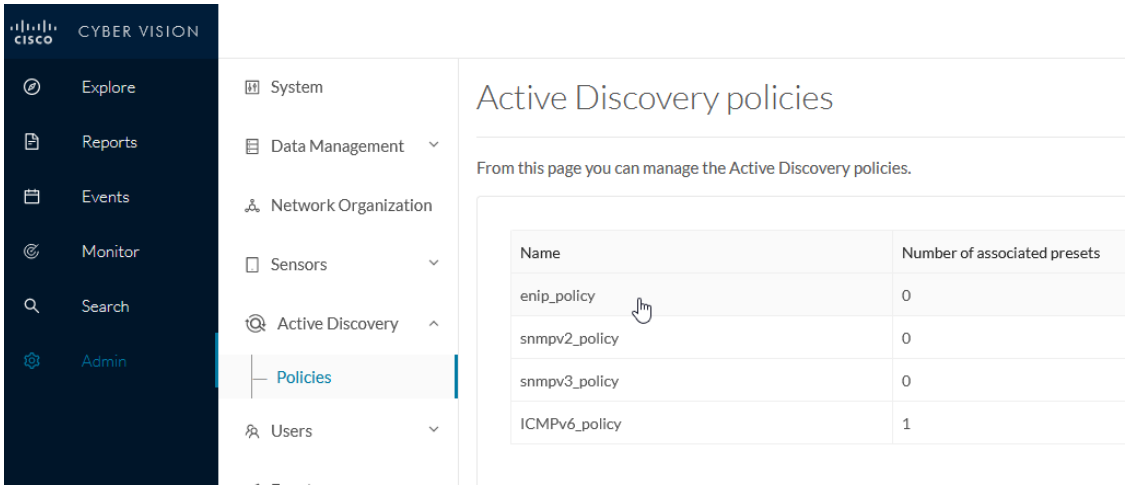
- Set Active Discovery Unicast SNMPv2c, on page 25.

Active Discovery preset configuration.

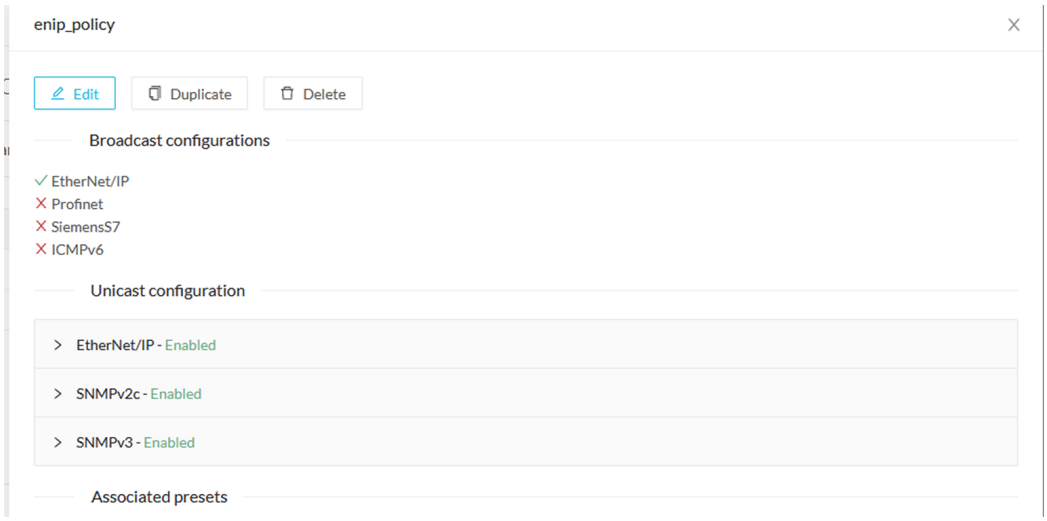
Modify a policy

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

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

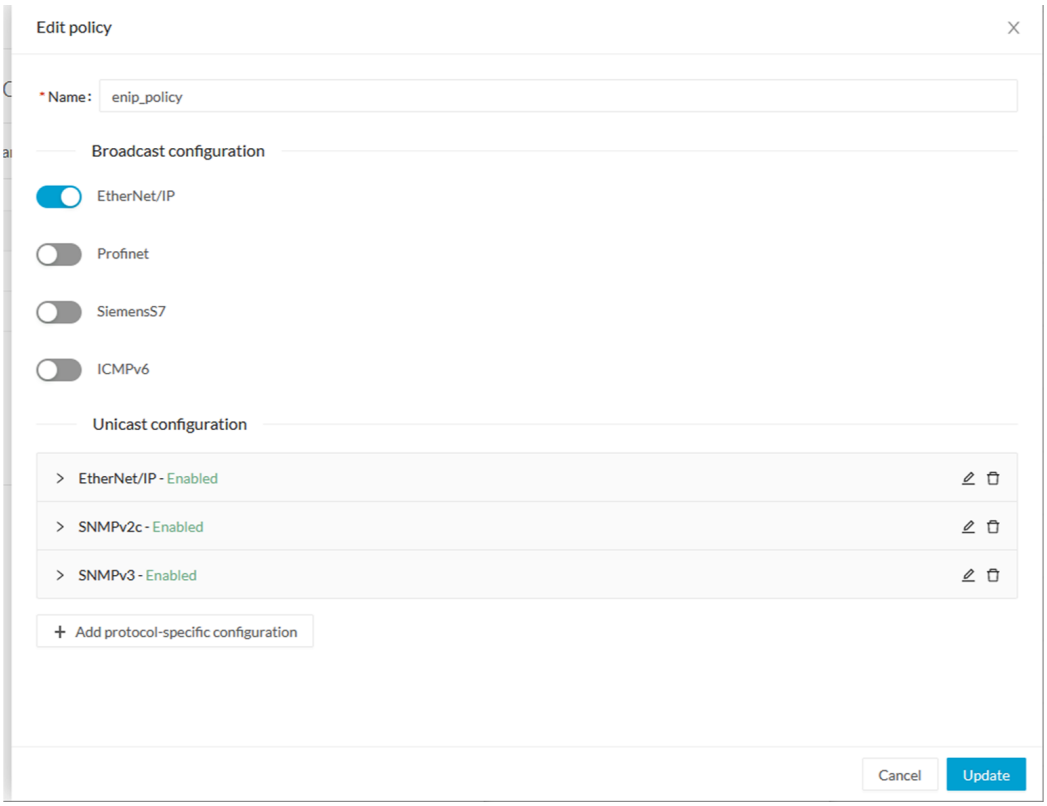


An overlay appears with the policy's configurations.



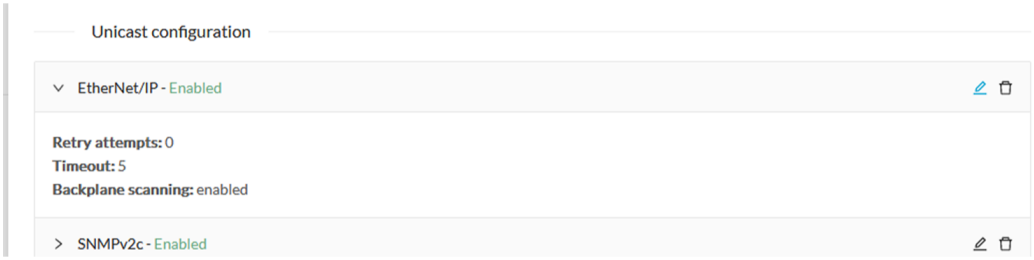
Step 3 Click **Edit**, **Duplicate** or **Delete**.

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

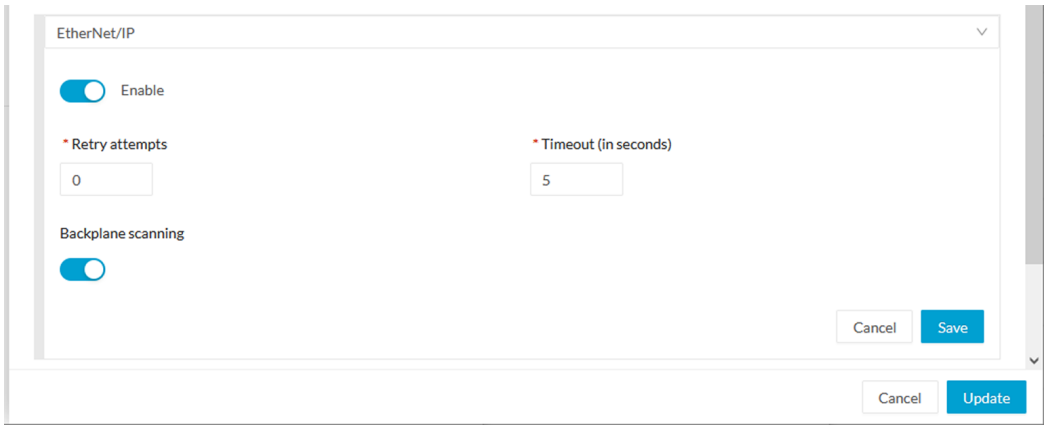


Step 4 You can toggle the buttons ON/OFF to enable/disable broadcast protocols.

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



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

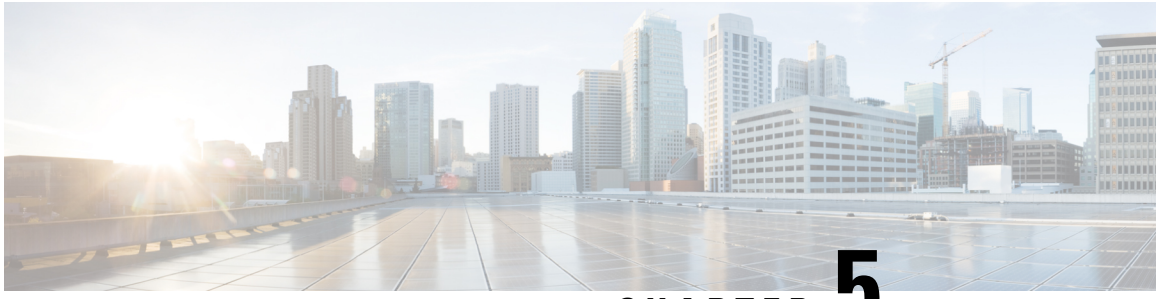


Step 6 Make the necessary modifications.

Step 7 Click **Save**.

The overlay closes.

Step 8 Click **Update**.



CHAPTER 5

Active Discovery preset configuration

Configure Active Discovery in a preset

Policies that have been created will be used in a preset. Configuring Active Discovery in a preset consists in selecting a policy and configuring a schedule for Unicast and/or Broadcast scans. In the example, a preset Broadcast Enip is used.

To configure Active Discovery on a preset:

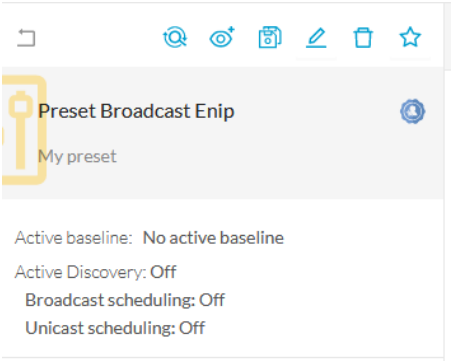
Before you begin

A preset can be used for Active Discovery if at least one sensor is selected in the filter preset criteria. The selected sensors will be used to execute the policy selected in the preset. Those sensors need to have access to the different networks to scan. For Unicast Active Discovery, the preset device list will be used to list the IP addresses to scan. In other words, the Active Discovery engine will use the IPv4 inside a component list to build its own list of components to scan.

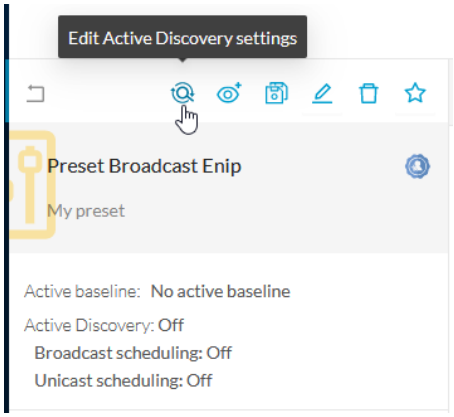
Step 1 Open the preset in the Explorer menu.

The presets' settings are displayed on the left:

- the usage of a Baseline in the preset
- the usage of Active Discovery
- the usage of Active Discovery schedule (Broadcast or Unicast)

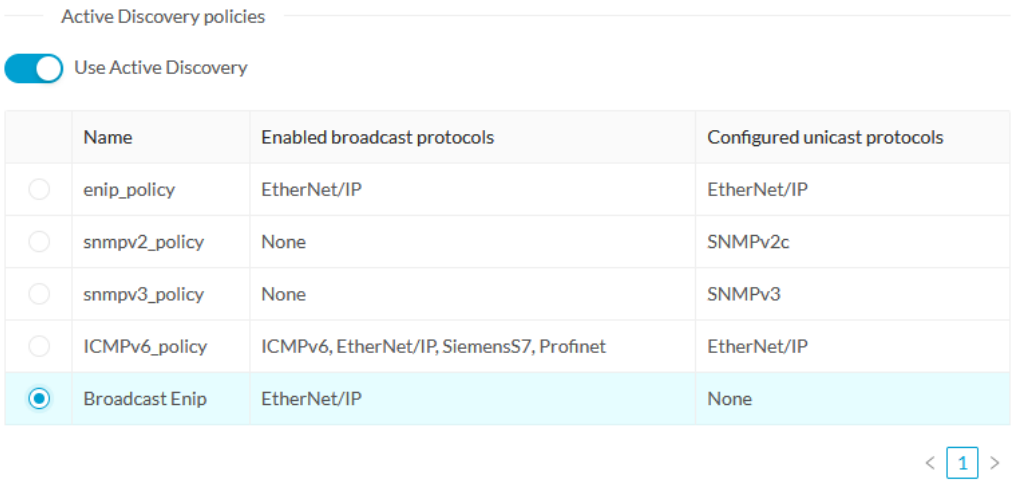


Step 2 Click the **Edit Active Discovery settings** icon.



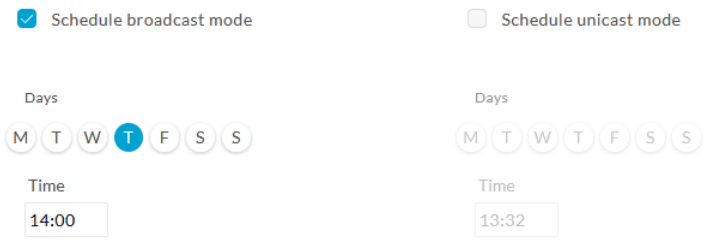
Step 3 Toggle the **Use Active Discovery** button ON.

Step 4 Select a Policy.



Step 5 To run Active Discovery, you have two options:

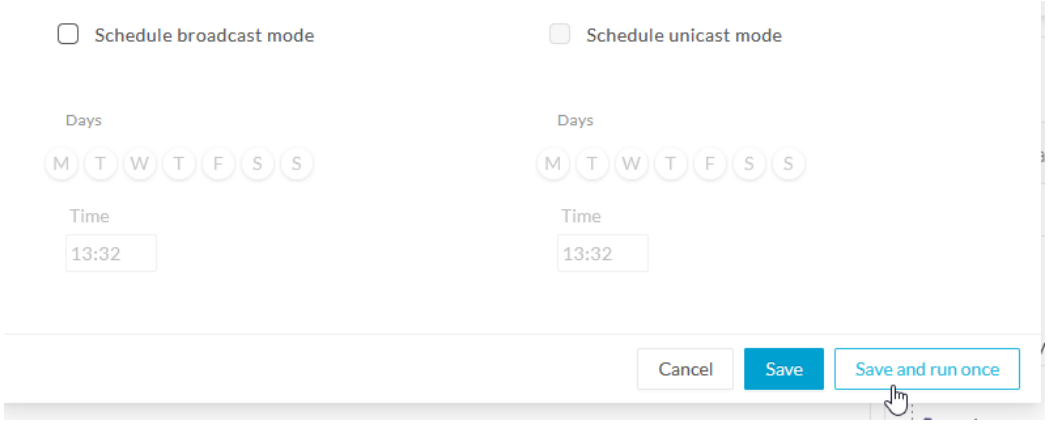
a) Schedule Active Discovery with the **Schedule Broadcast mode** and/or the **Schedule Unicast mode** by defining the days and times for scannings to be launched. Click **Save**.



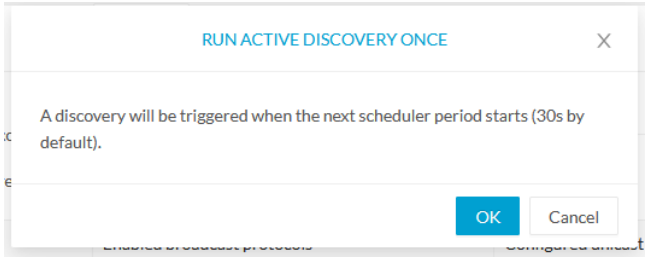
Scans will start automatically on the defined days and times.

Note A policy can have a Broadcast and Unicast mode.

b) Click **Save and run once** for the scan to be launched immediately without scheduling any.



A pop up appears. Launch the scan by clicking **OK**.

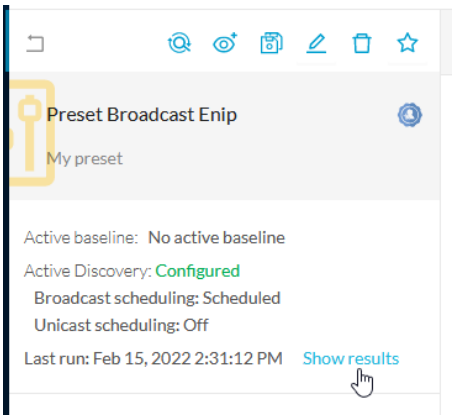


The scan may take a moment depending on the network.

Step 6 You can modify these settings as you like.

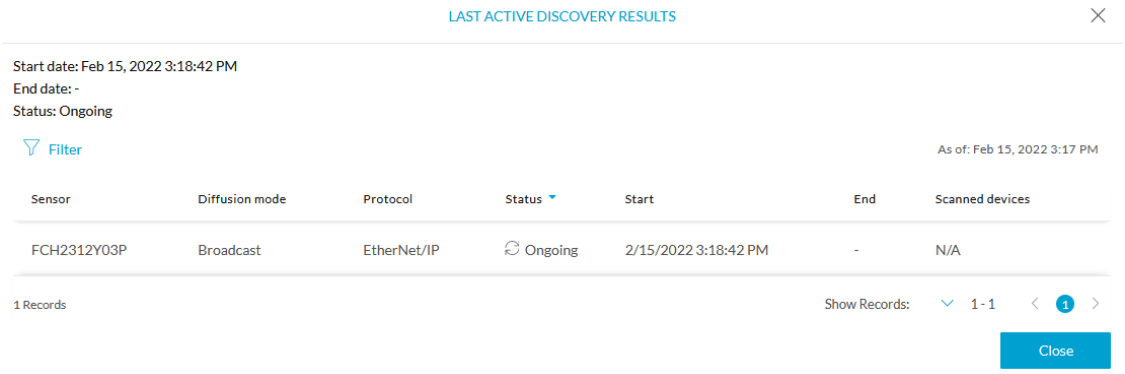
Active Discovery preset status

When the first scan starts, a **Show results** link appears to view Active Discovery results.



You will find the following information:

- Start date and time of the scan.
- The sensor used.
- The diffusion mode and the protocol used.
- The scanning status to Ongoing.



Once the scan is done, more information are displayed:

- The scanning status:
  - Success: All Broadcast scans ran without enduring problem. All Unicast components available were scanned.
  - Warning: A Unicast scan has at least one device which had a communication failure.
  - Fail: The scan failed. For example the IP to scan didn't send any response.
- The quantity of devices scanned for Unicast scans. N/A will be displayed for broadcast scans.

A successful scan:

LAST ACTIVE DISCOVERY RESULTS

Start date: Feb 15, 2022 2:31:12 PM
End date: Feb 15, 2022 2:31:42 PM
Status: Finished

Filter

Refreshing...

Sensor	Diffusion mode	Protocol	Status	Start	End	Scanned devices
FCH2312Y03P	Broadcast	EtherNet/IP	Success	2/15/2022 2:31:12 PM	2/15/2022 2:31:42 PM	N/A

1 Records

Show Records: 1 - 1

Close

A warning scan:

LAST ACTIVE DISCOVERY RESULTS

Start date: Feb 7, 2022 2:43:25 PM
End date: Feb 7, 2022 2:43:26 PM
Status: Finished

Filter

As of: Feb 15, 2022 3:11 PM

Sensor	Diffusion mode	Protocol	Status	Start	End	Scanned devices
IE3400	Unicast	EtherNet/IP	Warning	FAIL: IP scan succeed for 6, failed for 4, over a total of 10	M	10

1 Records

Show Records: 1 - 1

Close

A list of scans with one failed scan:

LAST ACTIVE DISCOVERY RESULTS

Start date: Feb 14, 2022 7:30:11 PM
End date: Feb 14, 2022 7:32:22 PM
Status: Failure

Filter

As of: Feb 15, 2022 3:12 PM

Sensor	Diffusion mode	Protocol	Status	Start	End	Scanned devices
FCH2312Y03P	Unicast	EtherNet/IP	Fail	2/14/2022 7:30:11 PM	2/14/2022 7:32:22 PM	3
FCH2312Y03P	Broadcast	Profinet	Success	2/14/2022 7:30:11 PM	2/14/2022 7:31:13 PM	N/A
FCH2312Y03P	Broadcast	EtherNet/IP	Success	2/14/2022 7:30:11 PM	2/14/2022 7:31:11 PM	N/A
FCH2312Y03P	Broadcast	SiemensS7	Success	2/14/2022 7:30:11 PM	2/14/2022 7:30:43 PM	N/A
FCH2312Y03P	Broadcast	ICMPv6	Success	2/14/2022 7:30:11 PM	2/14/2022 7:30:41 PM	N/A

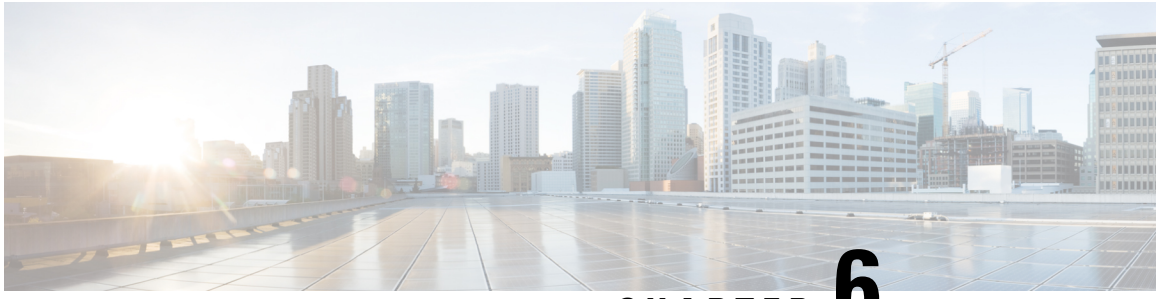
5 Records

Show Records: 1 - 5

Close

If the scan is successful, its status will eventually switch to Finished.

Refresh the preset to see the new information.



CHAPTER 6

Annex: Active Discovery protocols

Active Discovery protocol details

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.

Active Discovery EtherNet/IP details

Ethernet/IP active scanning 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 scan the preset components which have an IPv4 address.
- Unicast will scan, once an EtherNet/IP node is discovered, the devices' content. If a device is a chassis with a backplane, it will be scanned 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

Active Discovery EtherNet/IP Broadcast or Unicast

A Broadcast Ethernet/IP scan 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 (not backplane scan) will consist of the same request but sent directly to the device. When a preset is configured to scan 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):

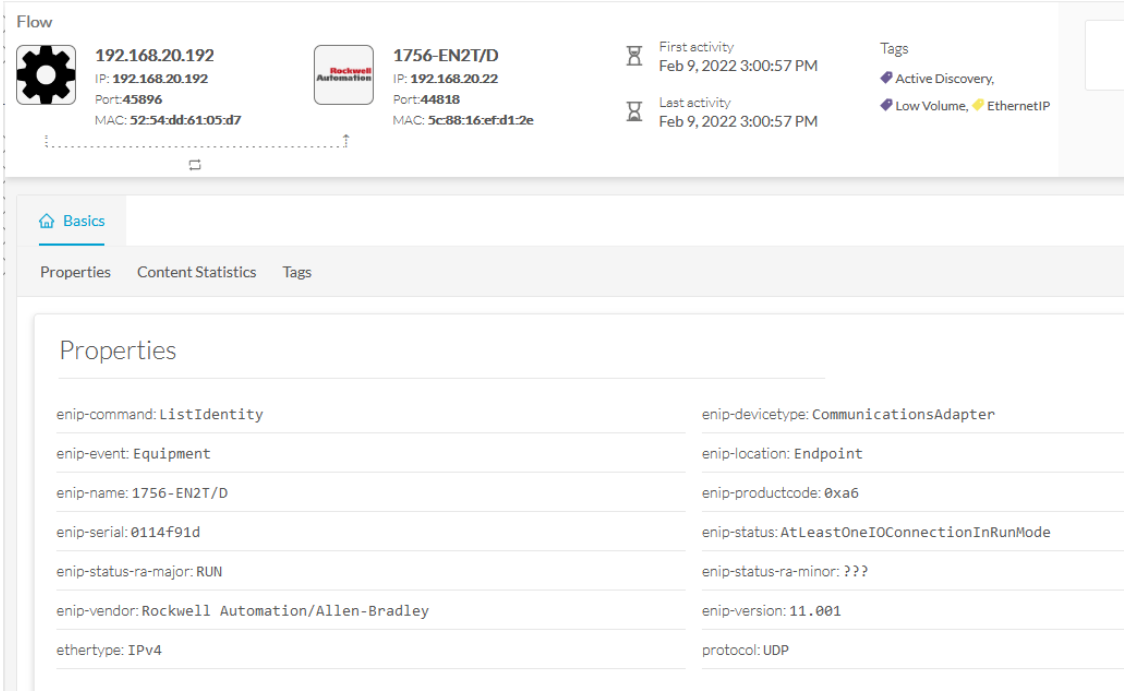


Figure 5: Example of properties received from a Rockwell Automation EtherNet/IP safety controller (1756-L81ES):

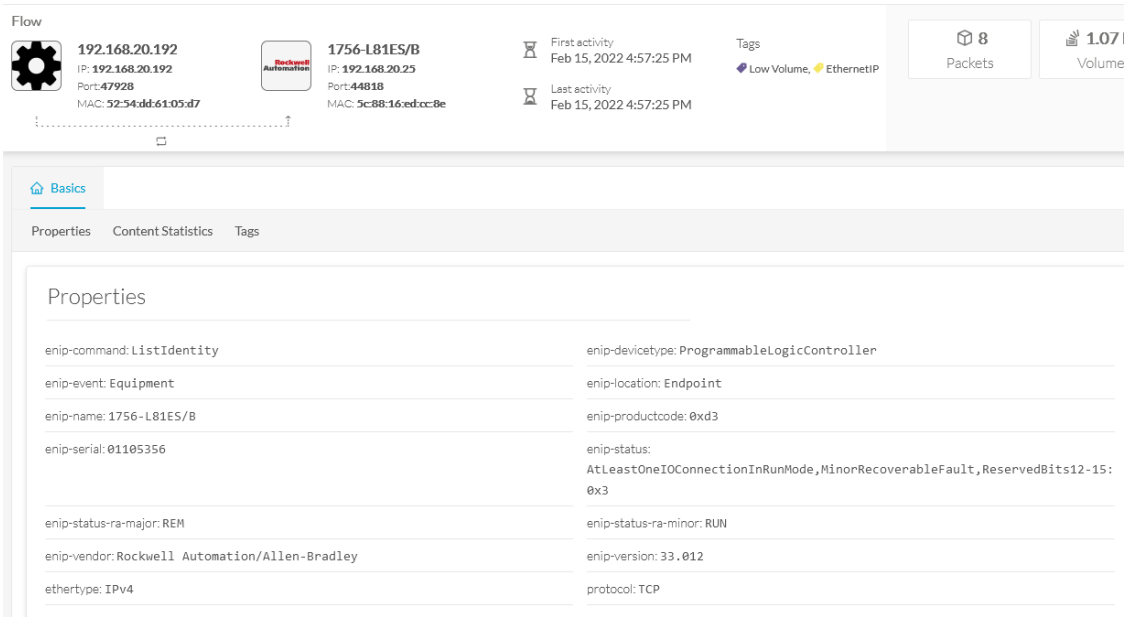
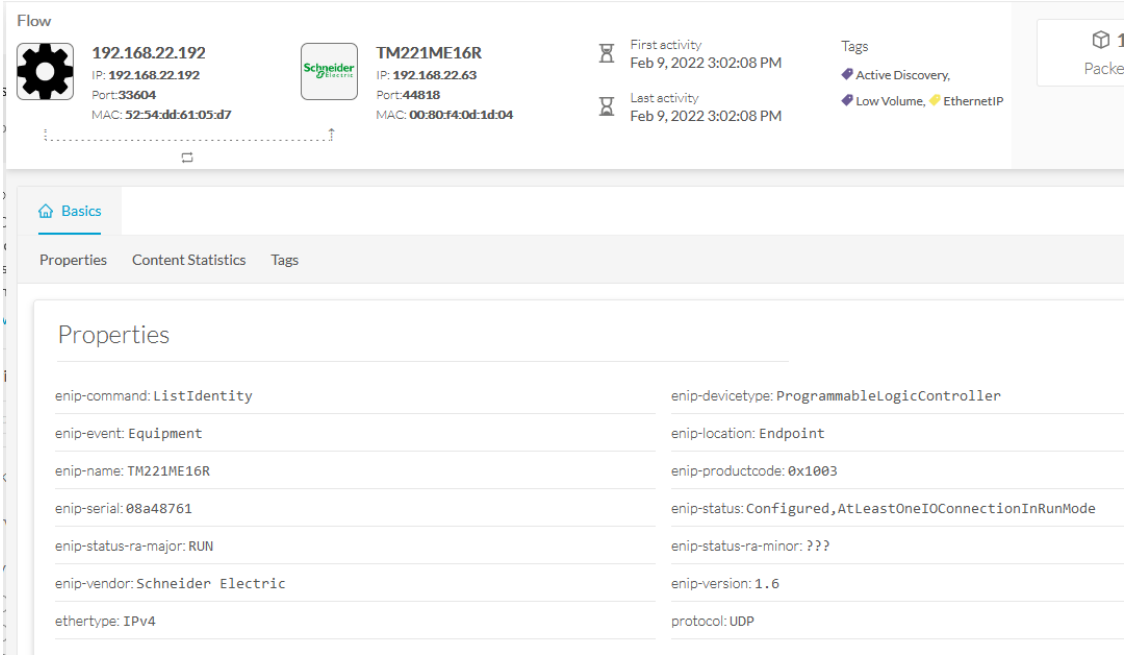


Figure 6: Example of properties received from a Schneider Eletric EtherNet/IP controller (TM221ME16R):

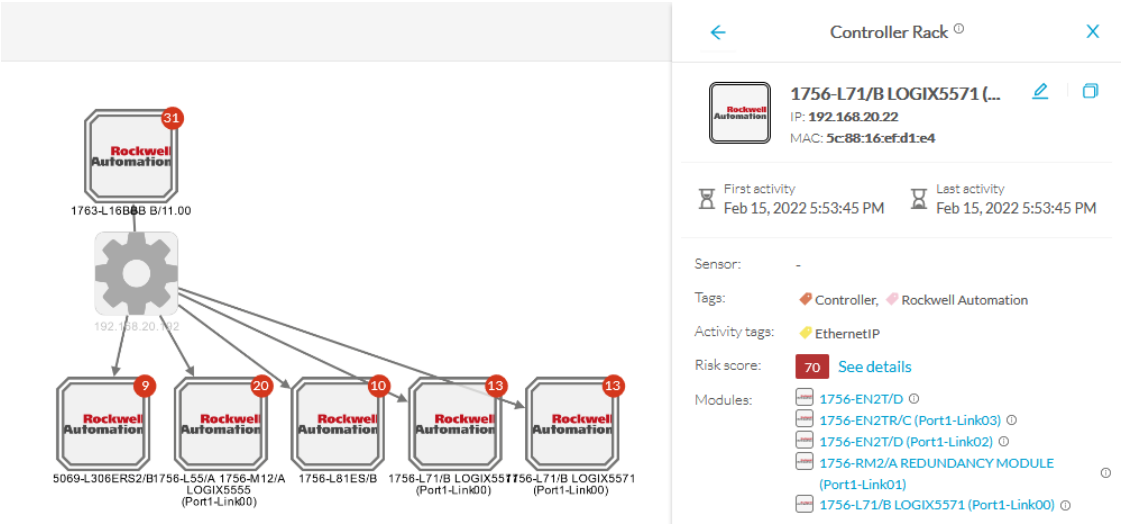


Active Discovery Ethernet/IP backplane scanning

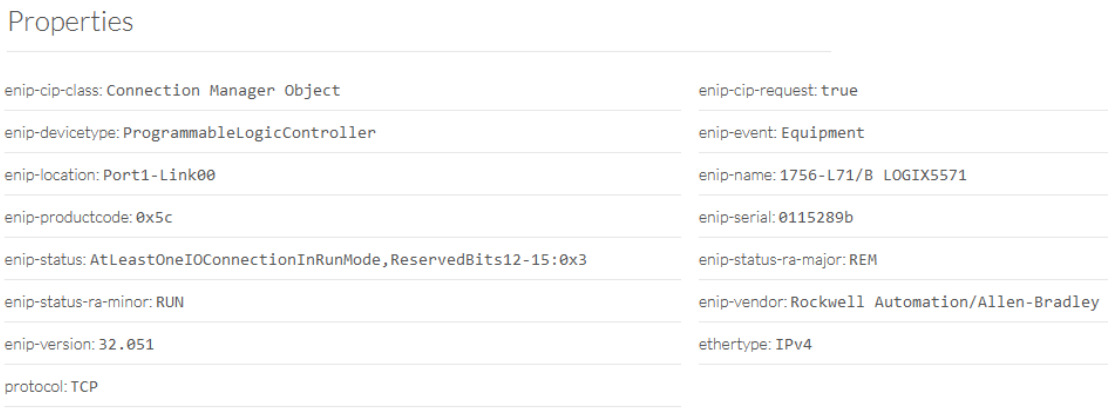
To browse backplanes, the Active Discovery policy with the Unicast EtherNet/IP protocol enabled needs to have the Backplane scanning option set to enabled.

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 scanned. Then, all seven slots of the chassis backplane were scanned. 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:



Active Discovery Profinet Multicast

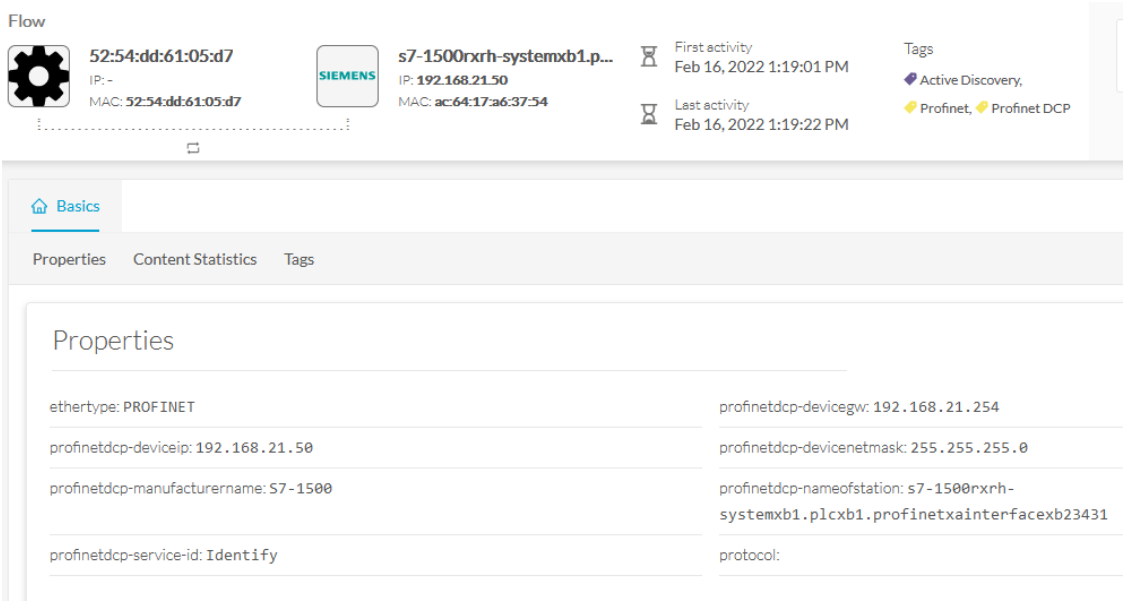
Cisco Cyber Vision Active Discovery can use a Profinet DCP service called Identify Request. This request will be sent by the sensor interfaces defined for Active Discovery. All Profinet devices will answer with a specific Profinet DCP identify response packet.

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:



Active Discovery S7 Broadcast

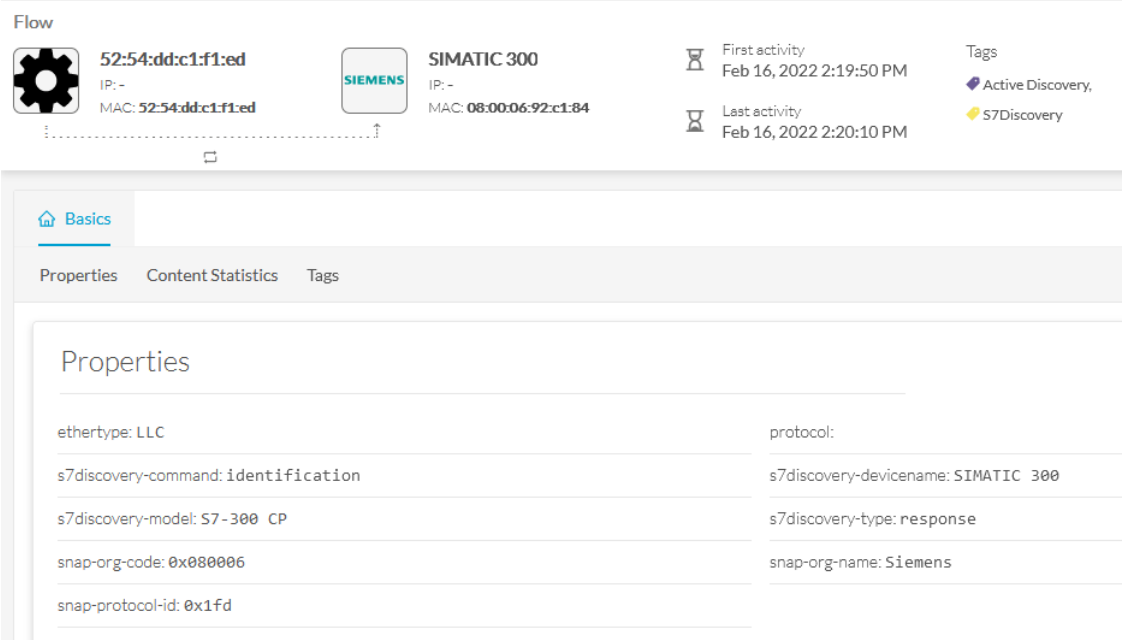
Cyber Vision Active Discovery can use a request on the protocol S7 discovery with a command: "identification". This request will be sent by the sensor interfaces defined for Active Discovery. All S7 devices will answer with a specific S7 Discovery identification response packet.

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:



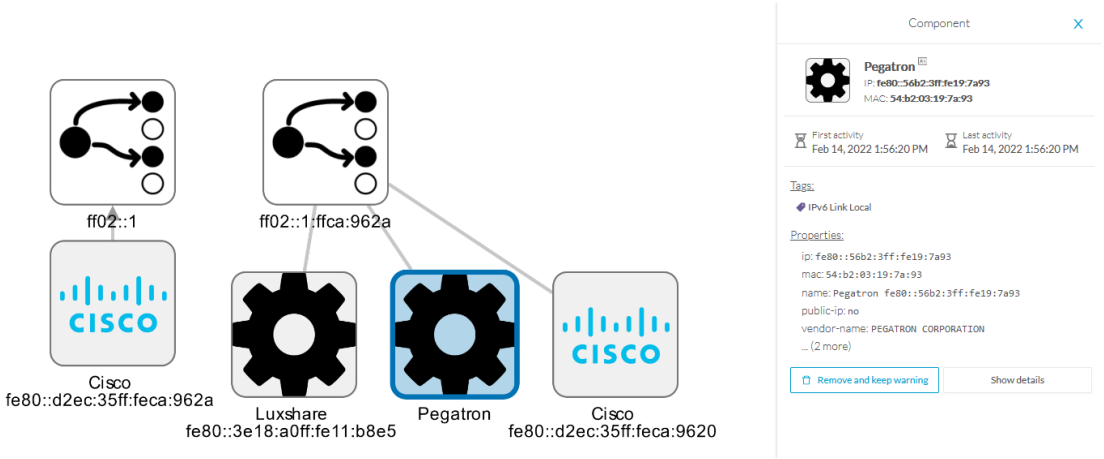
Active Discovery ICMPv6 Multicast

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:



Active Discovery SNMP Unicast

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

SNMP Active Discovery scan results highly depend on the configuration, type and version of the devices scanned. Some devices might respond without any specific configuration, but others might need complex configurations, or 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).

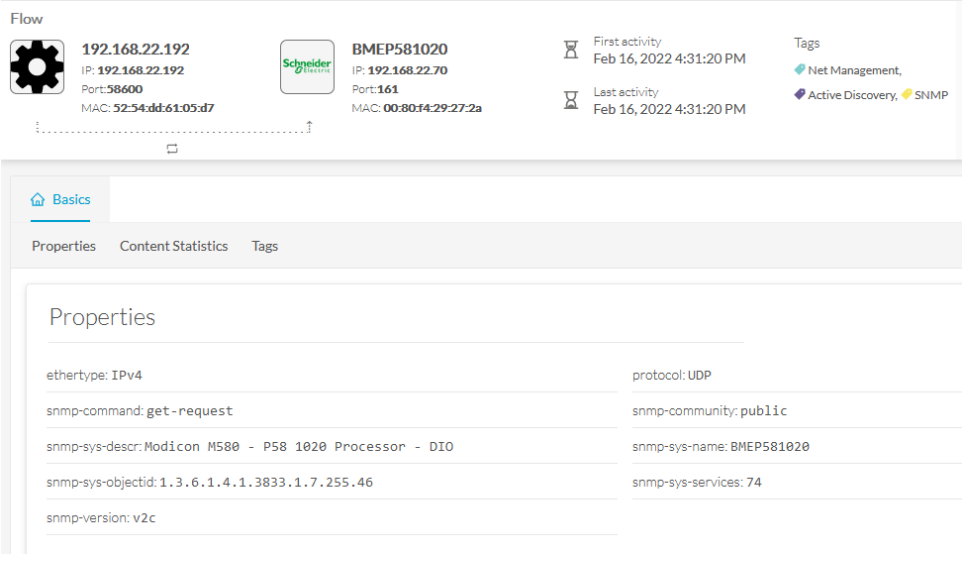
SNMPv3 Active Discovery is able to provide authentication and encryption.

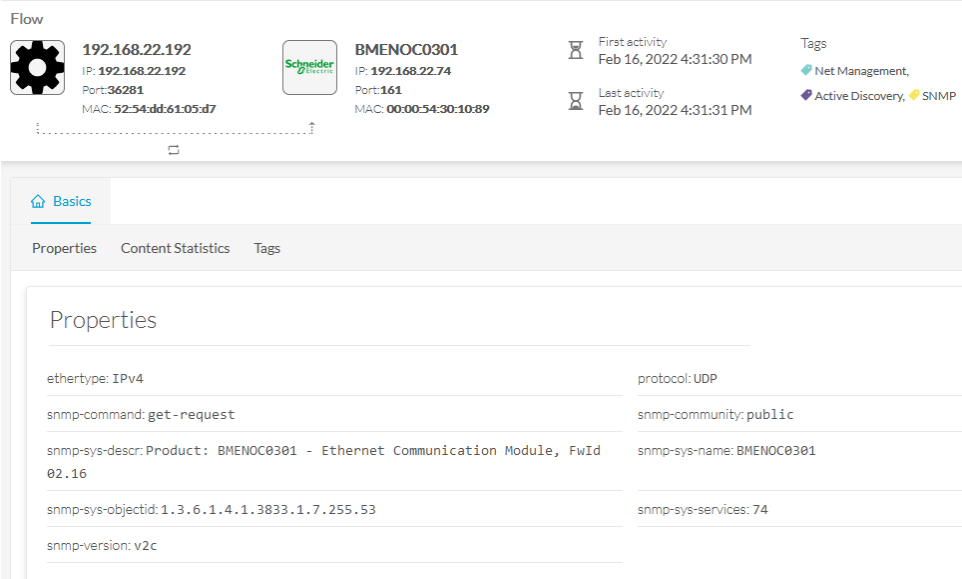
All SNMP versions will give the same results in the Cisco Cyber Vision application. They are important regarding data access. The subsequent section describes the SNMP results with different types of network devices.

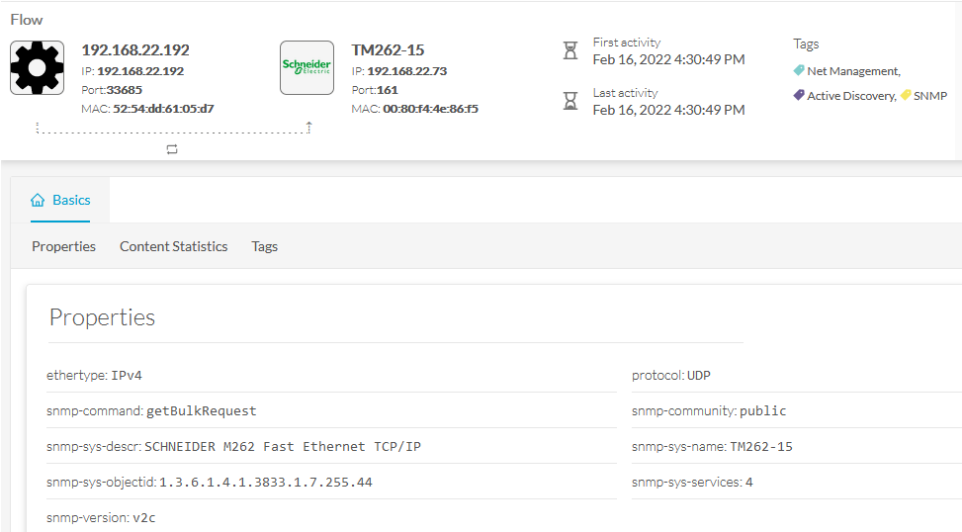
Active Discovery SNMP with Schneider PLC

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

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


Flow
192.168.22.192
IP: 192.168.22.192
Port:58600
MAC: 52:54:dd:61:05:d7
BMEP581020
IP: 192.168.22.70
Port:161
MAC: 00:80:f4:29:27:2a
First activity
Feb 16, 2022 4:31:20 PM
Last activity
Feb 16, 2022 4:31:20 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: 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

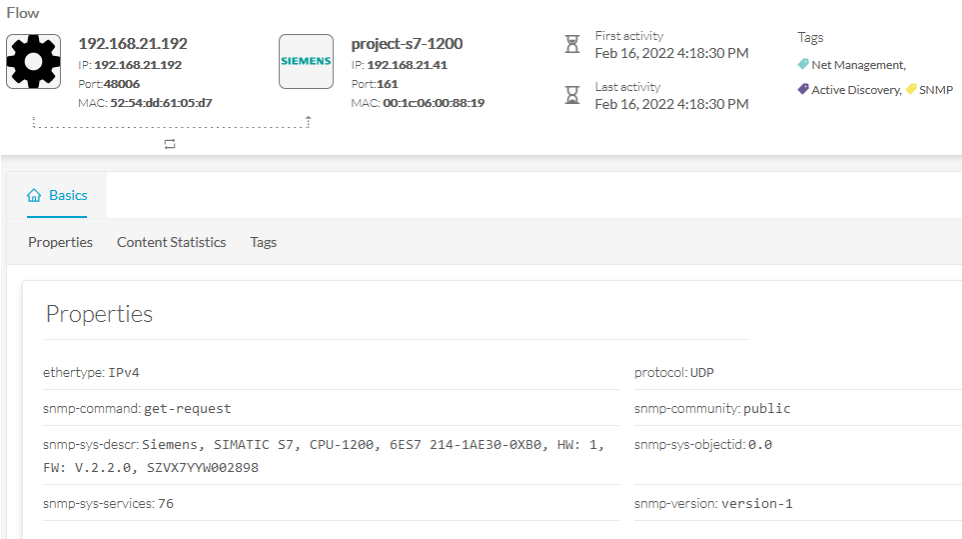

Flow
192.168.22.192
IP: 192.168.22.192
Port:36281
MAC: 52:54:dd:61:05:d7
BMENOC0301
IP: 192.168.22.74
Port:161
MAC: 00:00:54:30:10:89
First activity
Feb 16, 2022 4:31:30 PM
Last activity
Feb 16, 2022 4:31:31 PM
Tags
Net Management,
Active Discovery, SNMP
Basics
Properties
Content Statistics
Tags
Properties
ethertype: IPv4
protocol: UDP
snmp-command: get-request
snmp-community: public
snmp-sys-descr: 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

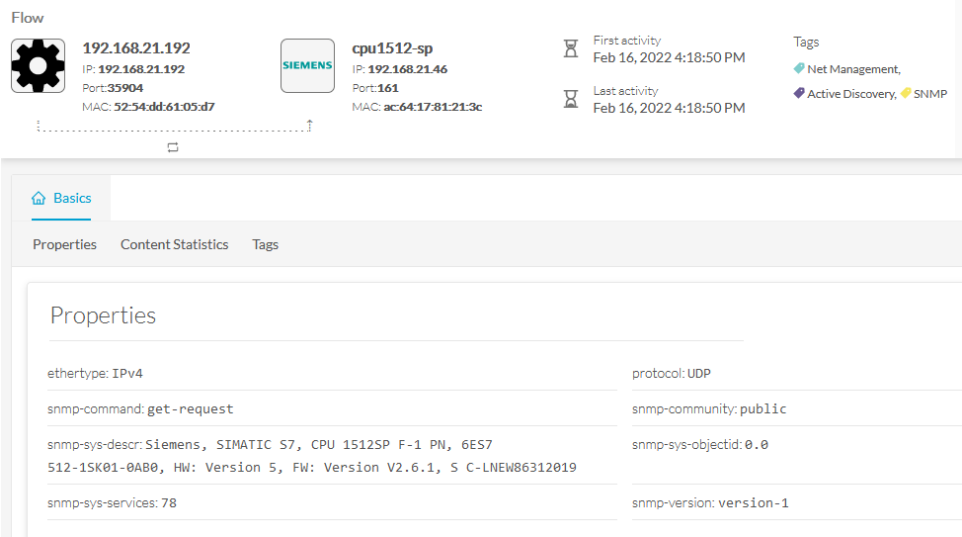


Active Discovery SNMP with Siemens PLC

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 defaut are:

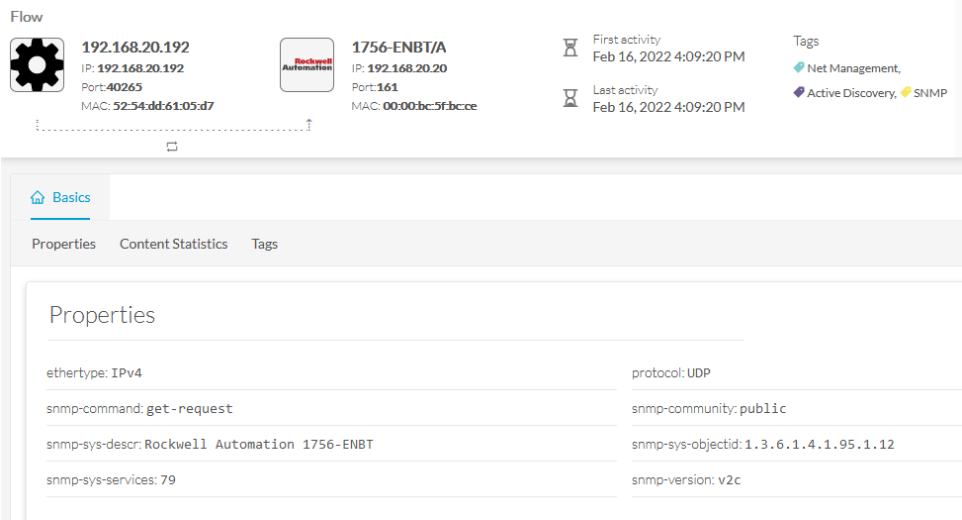




Active Discovery SNMP with Rockwell PLC

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 defaut are:



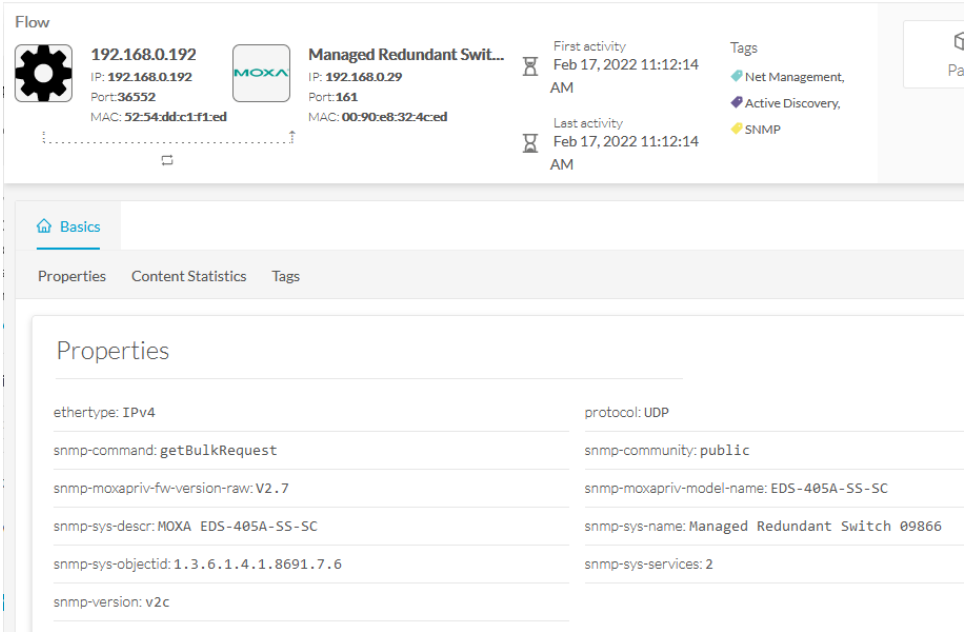
Active Discovery SNMP with Moxa switches

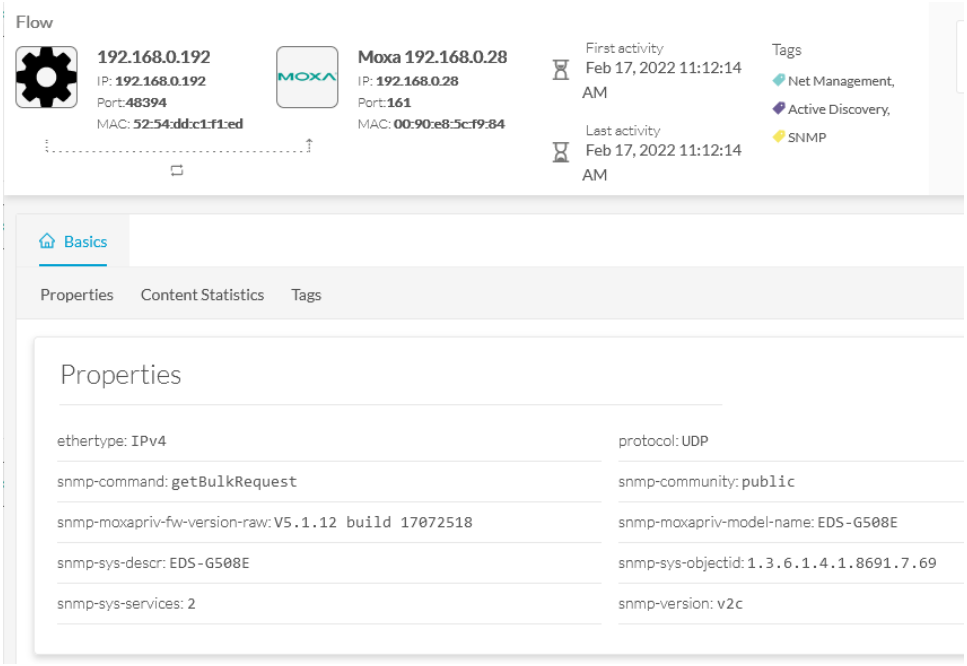
The Cisco Cyber Vision SNMP Active Discovery with Moxa switches requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

Property	Description
snmp-moxapriv-model-name	Model

snmp-moxapriv-fw-version	Firmware version

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



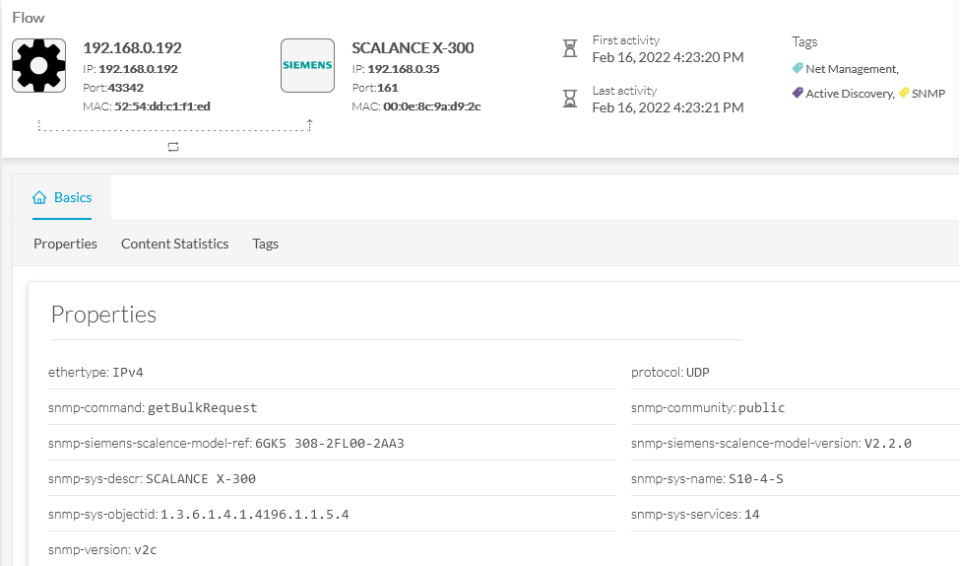


Active Discovery SNMP with Siemens Switches

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 defaut are:

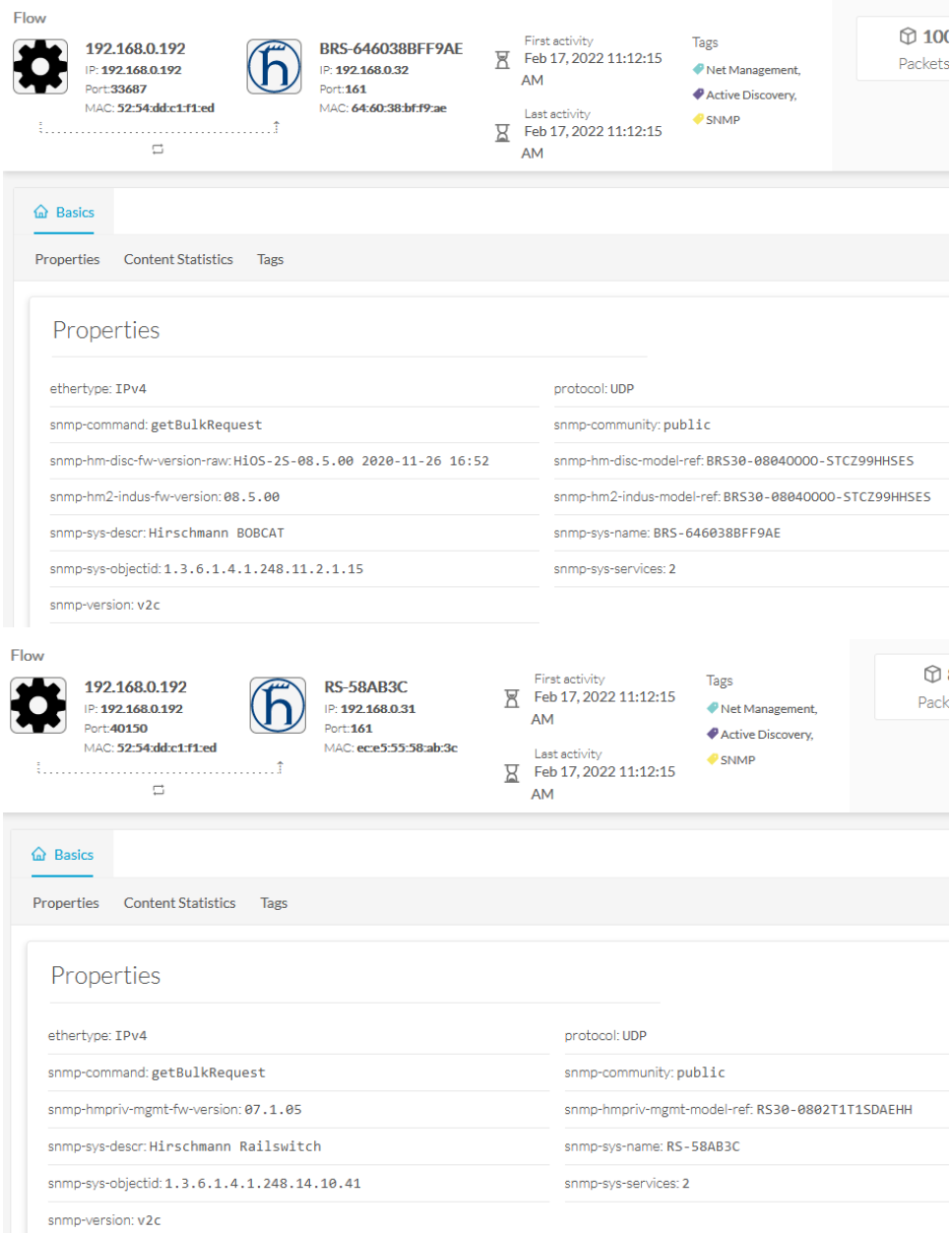


Active Discovery SNMP with Hirschmann hardware

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 defaut are:



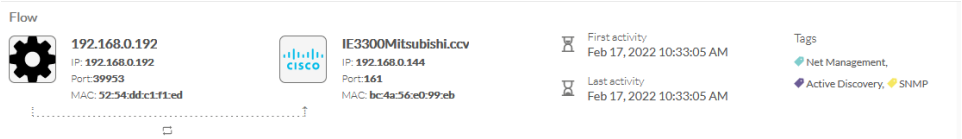
Active Discovery SNMP with Cisco hardware

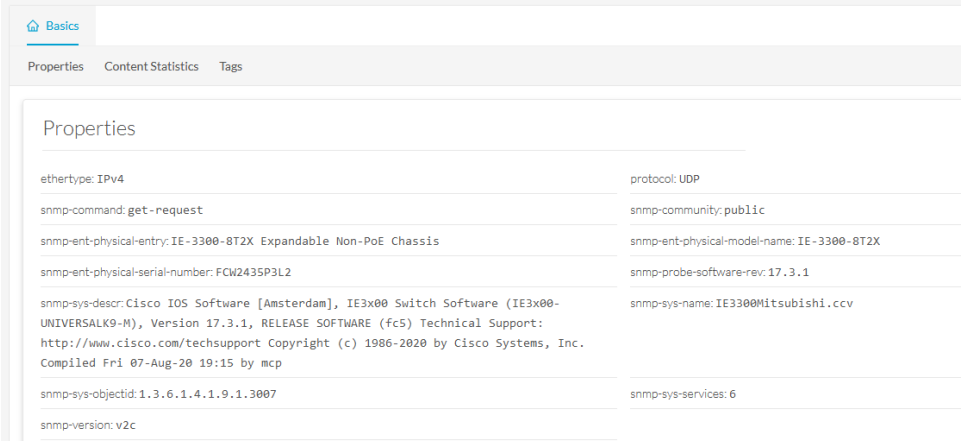
The Cisco Cyber Vision SNMP Active Discovery with Cisco Hardware demands some specific configurations on the device side and requests generic values (snmp-sys-descr and snmp-sys-name) with the addition of:

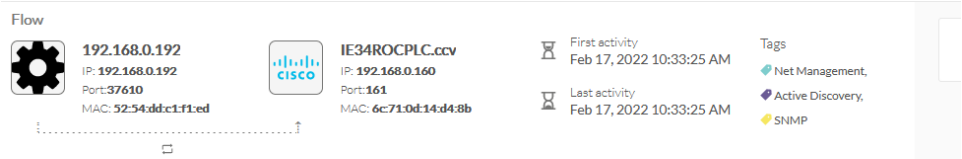
Property	Description
snmp-ent-physical-model-name	Model
snmp-ent-physical-entry	Description
snmp-ent-physical-serial-number	Serial number

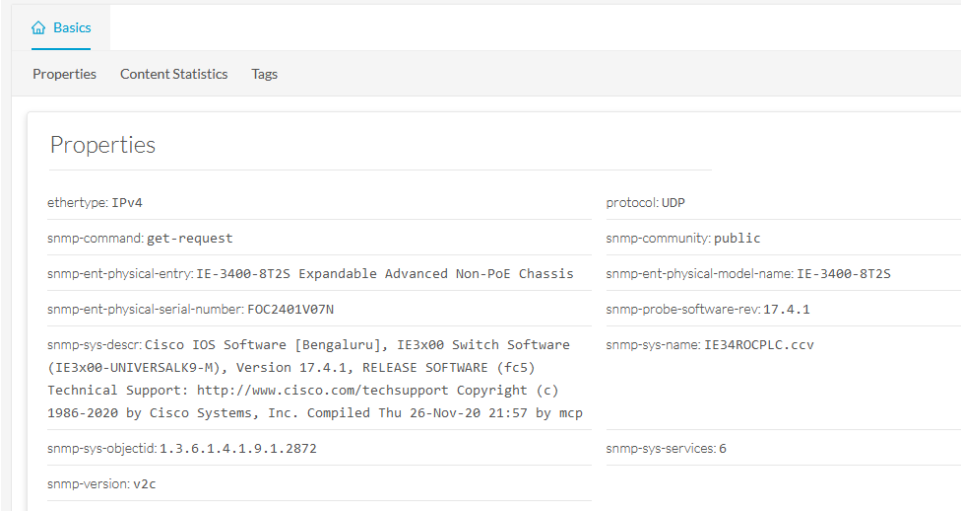
snmp-probe-software-rev	Firmware version

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









Active Discovery 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 defaut are: