



## Active Discovery policies configuration

- [Create a policy, on page 1](#)
- [Set Active Discovery Broadcast, on page 3](#)
- [Set Active Discovery Unicast Ethernet/IP, on page 4](#)
- [Set Active Discovery Unicast SNMPv2c, on page 5](#)
- [Set Active Discovery Unicast SNMPv3, on page 7](#)
- [Modify a policy, on page 10](#)

### 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.

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

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

## Active Discovery policies

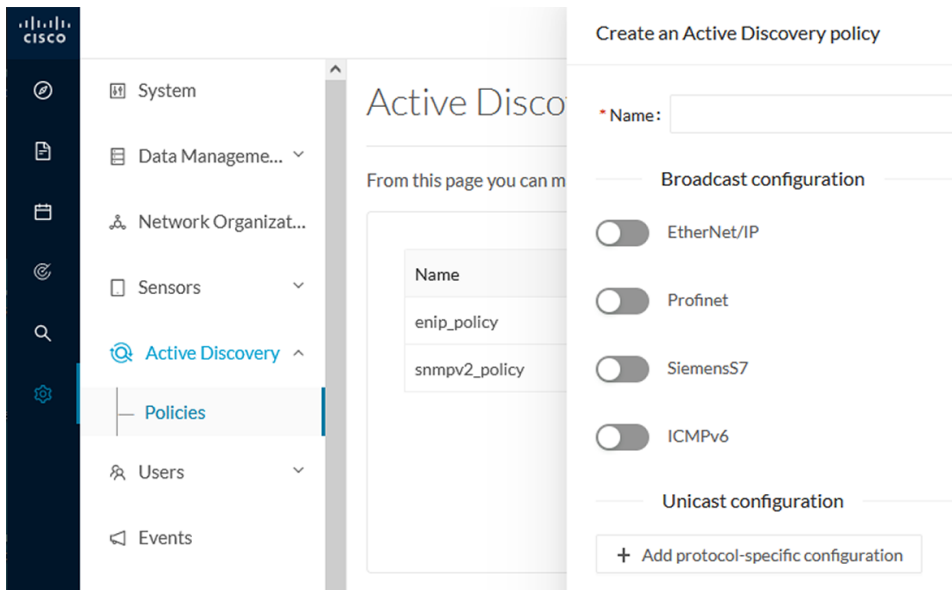
From this page you can manage the Active Discovery policies.

Name	Number of associated presets
 No Data	

[+ Create policy](#)

**Step 2** Click **+ Create policy**.

A Create an Active Discovery policy overlay appears.



The screenshot shows the Cisco Active Discovery configuration interface. On the left is a navigation sidebar with the following menu items: System, Data Management..., Network Organization..., Sensors, Active Discovery (selected), Policies (highlighted), Users, and Events. The main content area is titled 'Create an Active Discovery policy' and contains the following elements:

- A text input field for 'Name' with a red asterisk indicating it is required.
- A section for 'Broadcast configuration' with four toggle switches:
  - EtherNet/IP (disabled)
  - Profinet (disabled)
  - SiemensS7 (disabled)
  - ICMPv6 (disabled)
- A section for 'Unicast configuration' with a button labeled '+ Add protocol-specific configuration'.

In the background, a table titled 'Active Discovery' is visible, showing a list of policies: 'enip\_policy' and 'snmpv2\_policy'.

### What to do next

- [Set Active Discovery Broadcast, on page 3](#)
- [Set Active Discovery Unicast Ethernet/IP, on page 4](#)
- [Set Active Discovery Unicast SNMPv2c, on page 5](#)
- [Set Active Discovery Unicast SNMPv3, on page 7](#)

# 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.

Create an Active Discovery policy

Name: Broadcast\_policy

Broadcast configuration

- EtherNet/IP
- Profinet
- SiemensS7
- ICMPv6

Unicast configuration

+ Add protocol-specific configuration

Cancel Create

**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 4.](#)

- [Set Active Discovery Unicast SNMPv2c, on page 5.](#)
- [Set Active Discovery Unicast SNMPv3, on page 7.](#)

[Configure Active Discovery on a preset.](#)

## 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.

Unicast configuration

EtherNet/IP

Enable

\* Retry attempts: 0

\* Timeout (in seconds): 5

Backplane scanning:

Cancel Save

+ Add protocol-specific configuration

Cancel Create

**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 5.](#)
- [Set Active Discovery Unicast SNMPv3, on page 7.](#)

[Configure Active Discovery on a preset.](#)

## 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**.

Create an Active Discovery policy

\*Name:

Broadcast configuration

EtherNet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

[+ Add protocol-specific configuration](#)

**Step 3** Click the **Select protocol** dropdown menu and select **SNMPv2c**.

Unicast configuration

Select protocol ▼

EtherNet/IP

SNMPv2c

SNMPv3

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.

SNMPv2c ▼

Enable

\*Retry attempts

\*Timeout (in seconds)

\*Community ⓘ

Enable SNMPv1 fallback

**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 4](#)
- [Set Active Discovery Unicast SNMPv3, on page 7.](#)

[Configure Active Discovery on a preset.](#)

## 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**.

Create an Active Discovery policy

Name:

Broadcast configuration

Ethernet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

[+ Add protocol-specific configuration](#)

**Step 3** Click the **Select protocol** dropdown menu and select **SNMPv3**.

Unicast configuration

Select protocol

EtherNet/IP

SNMPv2c

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.

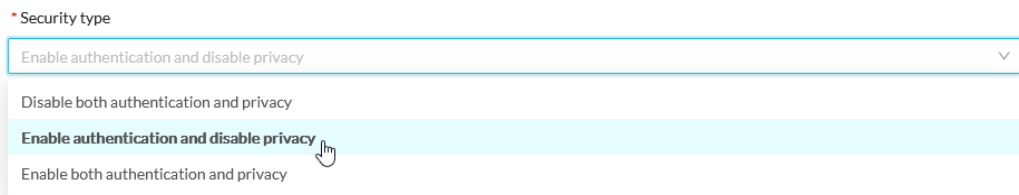
The community string is defined by IT or network administrators. The value "public" is often used by default.

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

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

- **Disable both authentication and privacy.**

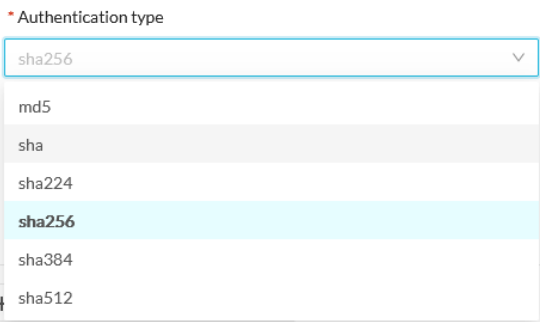
Only a username is requested for authentication.



- **Enable authentication and disable privacy.**

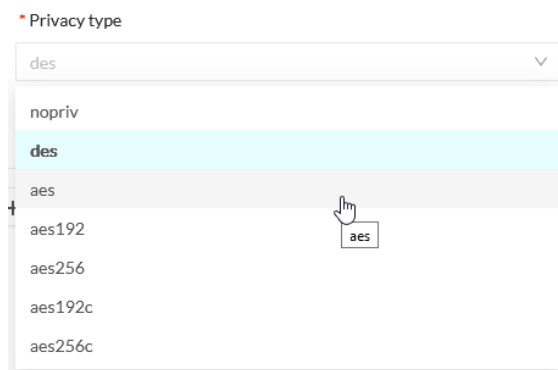
Authentication will be based on HMAC-MD5 or HMAC-SHA algorithms.

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**.

Create an Active Discovery policy X

\* Name:

Broadcast configuration

EtherNet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

SNMPv3 v

Enable

\* Retry attempts  \* Timeout (in seconds)

User-based security model configuration

\* Security type  v

\* Username

\* Authentication type  v \* Authentication password  🔗

\* Privacy type  v \* Privacy password  🔗

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 4](#)

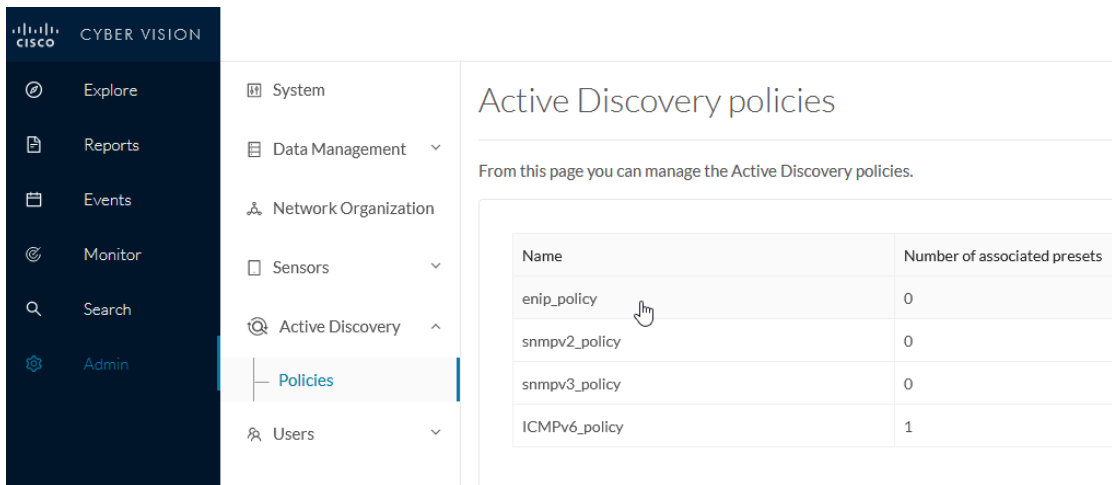
- Set Active Discovery Unicast SNMPv2c, on page 5.

Configure Active Discovery on a preset.

## Modify a policy

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

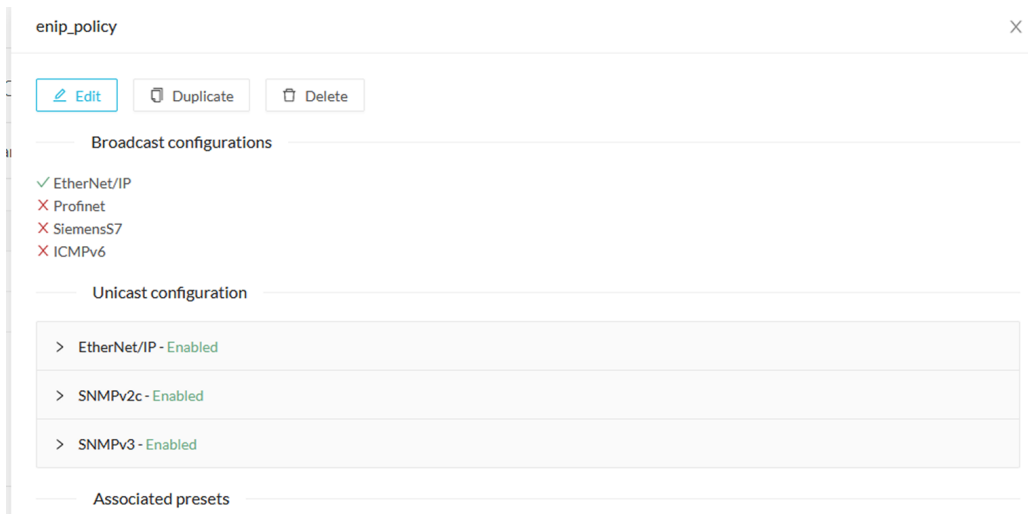
**Step 2** Click the policy in the list you want to modify.



The screenshot shows the Cisco Cyber Vision interface. The left sidebar contains a navigation menu with the following items: Explore, Reports, Events, Monitor, Search, and Admin (highlighted). The main content area is titled 'Active Discovery policies' and includes a sub-header 'From this page you can manage the Active Discovery policies.' Below this is a table with the following data:

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

An overlay appears with the policy's configurations.



The screenshot shows the configuration overlay for the 'enip\_policy'. At the top, there are three buttons: Edit, Duplicate, and Delete. Below these are two sections: 'Broadcast configurations' and 'Unicast configuration'. In the 'Broadcast configurations' section, 'EtherNet/IP' is checked (green), while 'Profinet', 'SiemensS7', and 'ICMPv6' are unchecked (red). In the 'Unicast configuration' section, 'EtherNet/IP - Enabled', 'SNMPv2c - Enabled', and 'SNMPv3 - Enabled' are all shown as enabled (green).

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

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

Edit policy ×  
 \* Name:   


---

 Broadcast configuration  
 EtherNet/IP  
 Profinet  
 SiemensS7  
 ICMPv6  


---

 Unicast configuration  

> EtherNet/IP - Enabled ✎ 🗑

> SNMPv2c - Enabled ✎ 🗑

> SNMPv3 - Enabled ✎ 🗑

+ Add protocol-specific configuration

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

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

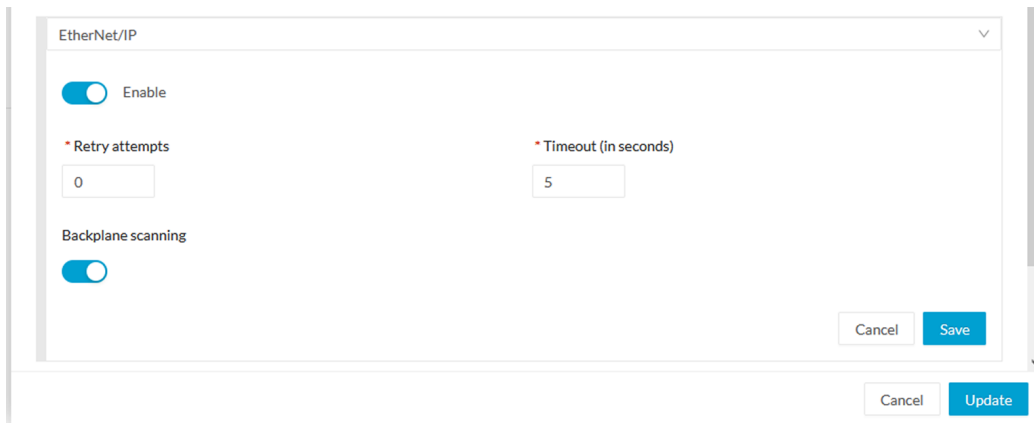
Unicast configuration  

v EtherNet/IP - Enabled ✎ 🗑  
 Retry attempts: 0  
 Timeout: 5  
 Backplane scanning: enabled

> SNMPv2c - Enabled ✎ 🗑

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

## Modify a policy



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

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

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

**Step 6** Make the necessary modifications.

**Step 7** Click **Save**.

The overlay closes.

**Step 8** Click **Update**.

---