



## Policies configuration

- [Create a policy, on page 1](#)
- [Set Active Discovery Broadcast, on page 2](#)
- [Set Active Discovery Unicast, on page 4](#)
- [Modify a policy, on page 17](#)

### Create a policy

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

Active Discovery policies

From this page you can manage the Active Discovery policies.


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

#### Procedure

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

## Active Discovery policies

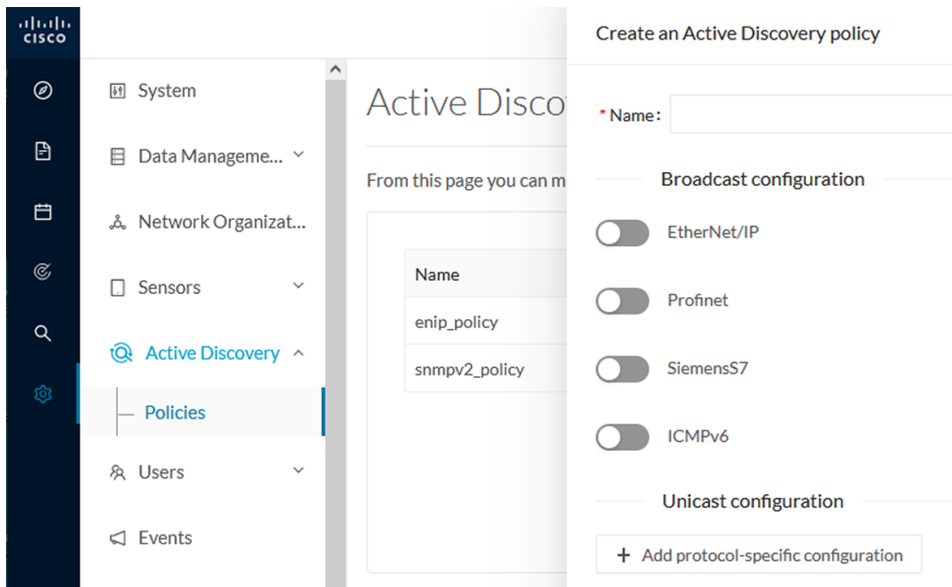
From this page you can manage the Active Discovery policies.

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 'Create an Active Discovery policy' overlay. The 'Name' field is empty. Under 'Broadcast configuration', all four protocols (EtherNet/IP, Profinet, SiemensS7, ICMPv6) are disabled. Under 'Unicast configuration', there is a button to '+ Add protocol-specific configuration'. The background shows the Cisco management interface with the 'Active Discovery' menu open, highlighting 'Policies'.

### What to do next

- [Set Active Discovery Broadcast, on page 2](#)
- [Set Active Discovery Unicast, on page 4](#)

# Set Active Discovery Broadcast

### Before you begin

Active Discovery is compatible with the following Broadcast protocols:

- EtherNet/IP

- Siemens S7
- Profinet
- ICMPv6

The sensor will send requests on all defined interfaces.

## Procedure

**Step 1** Type a policy name.

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

× Create an Active Discovery policy

\* Name:

Broadcast configuration

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

Unicast configuration

+ Add protocol-specific configuration

Cancel Create

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

Retry: number of request attempts.

Timeout: waiting time in seconds for a response.

**Step 4** Click **Create** to finish or add Unicast configurations to the policy.

## What to do next

[Set Active Discovery Unicast, on page 4](#)

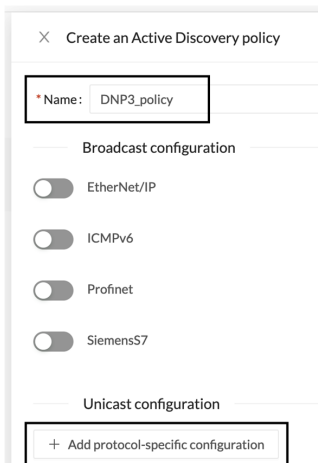
# Set Active Discovery Unicast

## Before you begin

### Procedure

**Step 1** Give the policy a name.

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



× Create an Active Discovery policy

\*Name: DNP3\_policy

Broadcast configuration

EtherNet/IP

ICMPv6

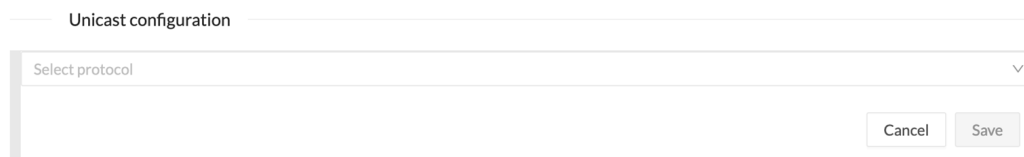
Profinet

SiemensS7

Unicast configuration

+ Add protocol-specific configuration

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



Unicast configuration

Select protocol

Cancel Save

## What to do next

See herebelow configurations per protocol.

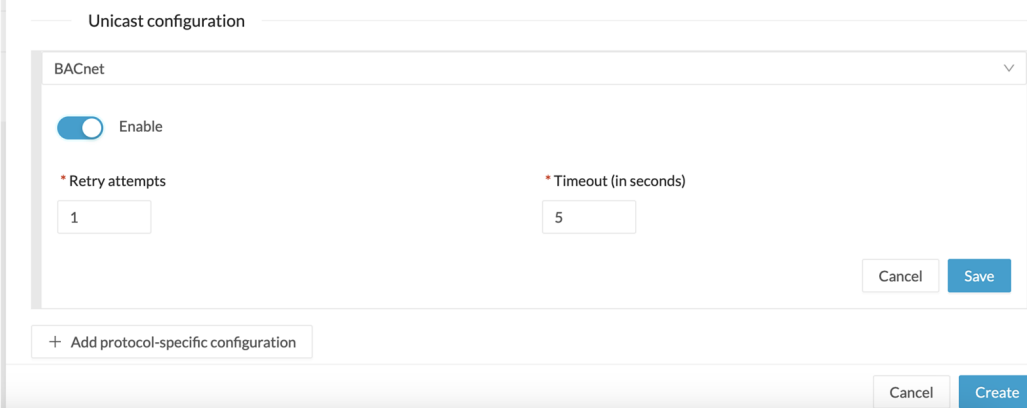
## Set Active Discovery Unicast BACnet

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

## Procedure

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

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



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

**Step 3** Click **Save**.

The menu closes.

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

**Step 2** Add 5 seconds (Default value) to the timeout field.

The screenshot shows a configuration window for Beckhoff. At the top, it says '> Beckhoff - Enabled'. Below that, the title 'Beckhoff' is visible. The settings are as follows:

- Enable:** A blue toggle switch is turned on.
- Timeout (in seconds):** A text input field contains the number '5'.
- Enable authentication:** A blue toggle switch is turned on.
- Username:** An empty text input field.
- Password:** An empty password input field with a small eye icon on the right.

At the bottom right, there are two buttons: 'Cancel' and 'Save'.

**Step 3** Enter a Beckhoff user account and password.

**Step 4** Click **Save**.

The menu closes.

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

## Set Active Discovery Unicast DNP3

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

### Before you begin

### Procedure

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

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

Unicast configuration

DNP3

Enable

\* Retry attempts:

\* Timeout (in seconds):

\* Source Address:

\* Max Destination Address:

Cancel Save

+ Add protocol-specific configuration

Cancel Create

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

**Step 4** Click **Save**.

The menu closes.

Unicast configuration

> DNP3 - Enabled ✎ 🗑

+ Add protocol-specific configuration

Cancel Create

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

## Set Active Discovery Unicast Ethernet/IP

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

### Procedure

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

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

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

Unicast configuration

EtherNet/IP v

Enable

\* Retry attempts       \* Timeout (in seconds)

Backplane discovery

+ Add protocol-specific configuration

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

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

## Set Active Discovery Unicast GES RTP

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

### Procedure

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

**Step 2** Add 5 seconds (default value) to the Timeout field.

GES RTP v

Enable

\* Timeout (in seconds)

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



**Step 4** Click **Create**.

---

## Set Active Discovery Unicast HTTP or HTTPS

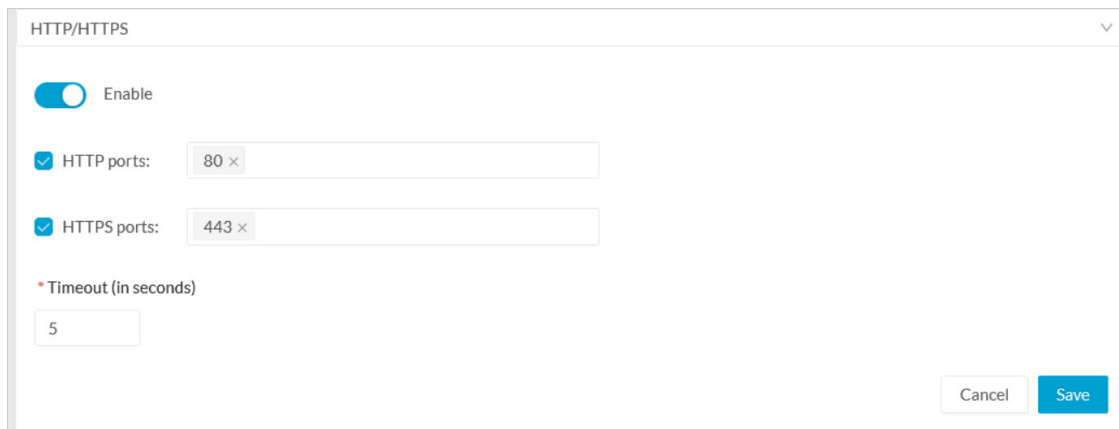
Configure Active Discovery Unicast HTTP/HTTPS to find devices and components with HTTP/HTTPS requests. It will check all components with an IPV4 address.

### Procedure

---

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

**Step 2** Add 5 seconds (default value) to the Timeout field.



The screenshot shows a configuration window titled "HTTP/HTTPS". It contains the following elements:

- An "Enable" toggle switch, which is currently turned ON.
- A checked checkbox for "HTTP ports:" with a text input field containing "80".
- A checked checkbox for "HTTPS ports:" with a text input field containing "443".
- A section labeled "\* Timeout (in seconds)" with a text input field containing "5".
- At the bottom right, there are "Cancel" and "Save" buttons.

**Step 3** Add HTTP and/or HTTPS port details to scan.

**Step 4** Click **Save**.

The menu closes.

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

---

## Set Active Discovery Unicast Melsoft

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

### Procedure

---

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

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

Unicast configuration

Melsoft

Enable

\* Retry attempts

\* Timeout (in seconds)

Cancel Save

+ Add protocol-specific configuration

Cancel Create

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

**Step 4** Click **Create**.

## Set Active Discovery Unicast Modbus

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

### Procedure

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

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

Unicast configuration

Modbus

Enable

\* Retry attempts

\* Timeout (in seconds)

Unit Id

Force UMAS Function Codes

Cancel Save

+ Add protocol-specific configuration

Cancel Create

**Step 3** Click **Save**.

The menu closes.

**Step 4** Click **Create**.

---

## Set Active Discovery Unicast OMRON

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

### Procedure

---

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

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

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

**Step 3** Click **Save**.

The menu closes.

**Step 4** Click **Create**.

---

## Set Active Discovery Unicast SiemensS7

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

### Procedure

---

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

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

Unicast configuration

SiemensS7

Enable

\* Retry attempts: 0

\* Timeout (in seconds): 5

Rack: 1

Slot: 2

Cancel Save

Cancel Create

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

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

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

## Set Active Discovery Unicast SiemensS7plus

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

### Procedure

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

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

Unicast configuration

Siemens57plus

Enable

\*Retry attempts: 1

\*Timeout (in seconds): 5

Cancel Save

+ Add protocol-specific configuration

Cancel Create

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

**Step 4** Click **Create**.

---

## Set Active Discovery Unicast SNMPv2c

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

### Procedure

---

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

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

**Step 3** Type a community string for authentication.

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

**Step 4** You can toggle the **Enable SNMPv1 fallback** button ON. Active Discovery will look for PLCs and I/O chassis with module details.

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

**Step 6** Click **Create**.

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

## Set Active Discovery Unicast SNMPv3

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

### Procedure

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

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

**Step 3** Type a community string for authentication.

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

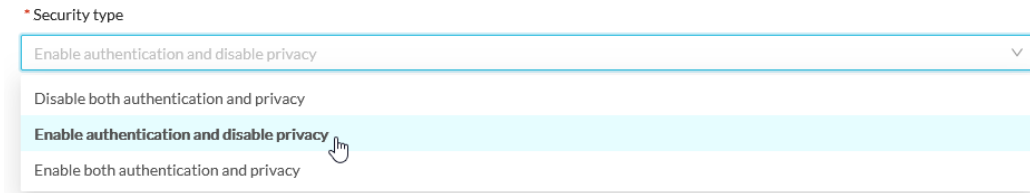
**Step 4** Select the proper security and privacy level based on the information provided by the IT or network administrators.

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

- **Disable both authentication and privacy.**

Only a username is requested for authentication.

\* Security type



Enable authentication and disable privacy

Disable both authentication and privacy

Enable authentication and disable privacy

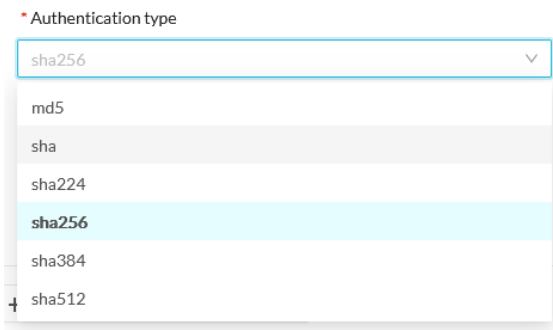
Enable both authentication and privacy

- **Enable authentication and disable privacy.**

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

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

\* Authentication type



sha256

md5

sha

sha224

sha256

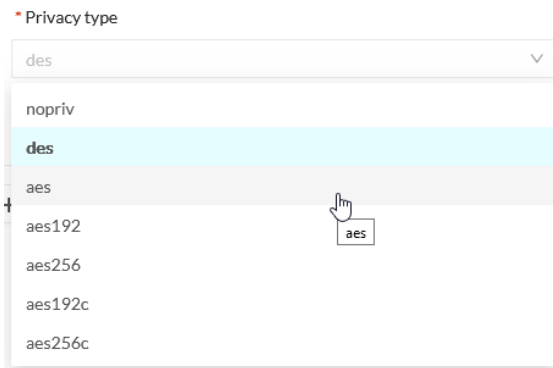
sha384

sha512

- **Enable both authentication and privacy.**

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

\* Privacy type



des

nopriv

des

aes

aes192

aes256

aes192c

aes256c

**Step 5** Click **Save**.

Create an Active Discovery policy X

\* Name:

Broadcast configuration

EtherNet/IP

Profinet

SiemensS7

ICMPv6

Unicast configuration

SNMPv3 v

Enable

\* Retry attempts       \* Timeout (in seconds)

User-based security model configuration

\* Security type

\* Username

\* Authentication type       \* Authentication password

\* Privacy type       \* Privacy password

The menu closes.

**Step 6** Click **Create**.

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

## Set Active Discovery Unicast WMI

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



## Procedure

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

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

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

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

Unicast configuration

WMI

Enable

\* Retry attempts  \* Timeout (in seconds)

\* Username

\* Password

+ Add protocol-specific configuration

**Step 4** Click **Save**.

The menu closes.

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

## Modify a policy

### Procedure

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

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

Active Discovery policies

From this page you can manage the Active Discovery policies.

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.

enip\_policy

Edit Duplicate Delete

Broadcast configurations

- ✓ EtherNet/IP
- ✗ Profinet
- ✗ SiemensS7
- ✗ ICMPv6

Unicast configuration

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

Associated presets

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

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

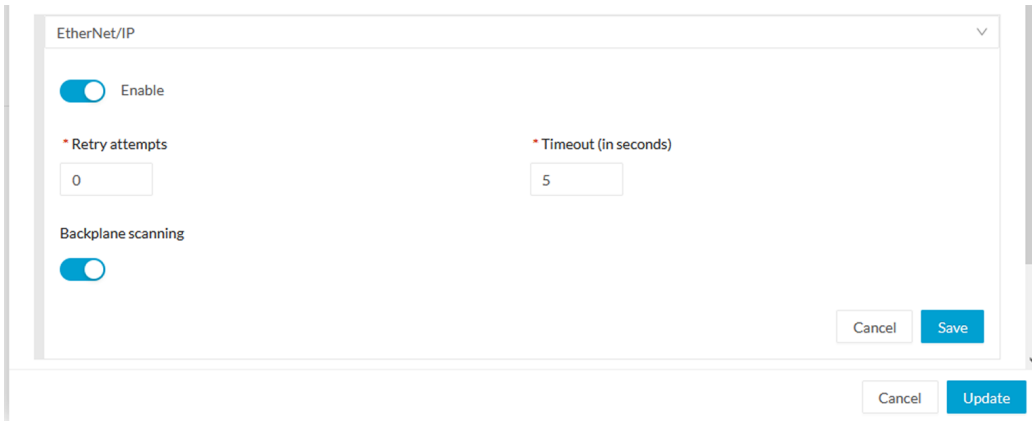
The screenshot shows a dialog box titled "Edit policy" with a close button (X) in the top right corner. The "Name" field contains "enip\_policy". Under the "Broadcast configuration" section, there are four toggle switches: "EtherNet/IP" (checked), "Profinet" (unchecked), "SiemensS7" (unchecked), and "ICMPv6" (unchecked). Under the "Unicast configuration" section, there is a list of three items: "EtherNet/IP - Enabled", "SNMPv2c - Enabled", and "SNMPv3 - Enabled". Each item has a right-pointing chevron on the left and edit (pencil) and delete (trash) icons on the right. Below the list is a button labeled "+ Add protocol-specific configuration". At the bottom right of the dialog are "Cancel" and "Update" buttons.

**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 screenshot shows a close-up of the "Unicast configuration" section. The "EtherNet/IP - Enabled" item is expanded, showing a right-pointing chevron on the left and edit and delete icons on the right. Below the item name, the following settings are displayed: "Retry attempts: 0", "Timeout: 5", and "Backplane scanning: enabled". Below this expanded panel, the "SNMPv2c - Enabled" item is visible with a right-pointing chevron and edit/delete icons.

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



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 box, there are two more buttons: "Cancel" and "Update".

**Step 6** Make the necessary modifications.

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

The overlay closes.

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

---