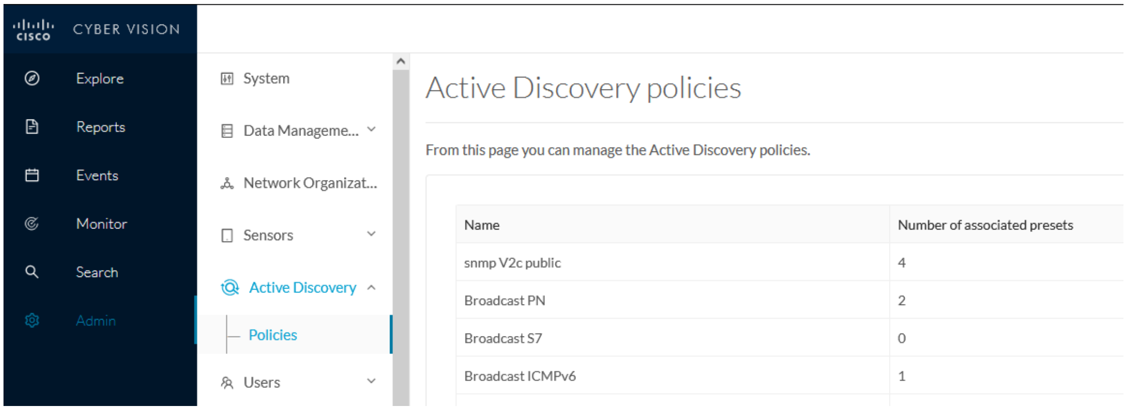
Policies configuration

Create a policy

An Active Discovery policy is a list of settings which define protocols and their parameters that will be used to 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.

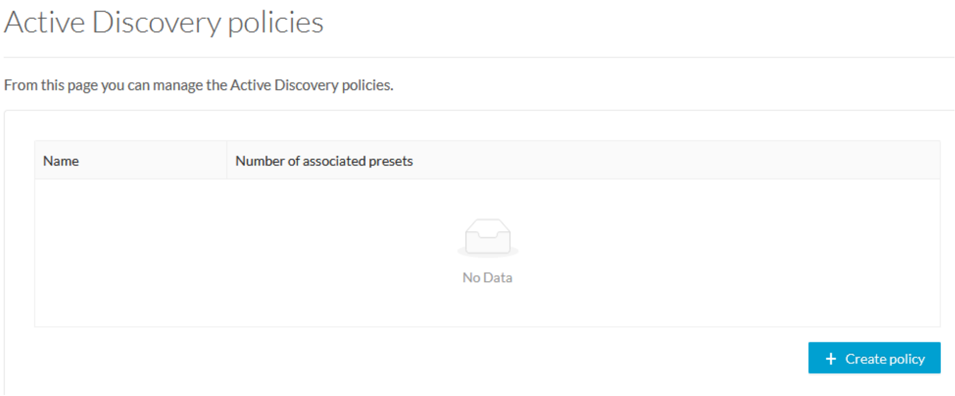


Active Discovery policies

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

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



Active Discovery policies

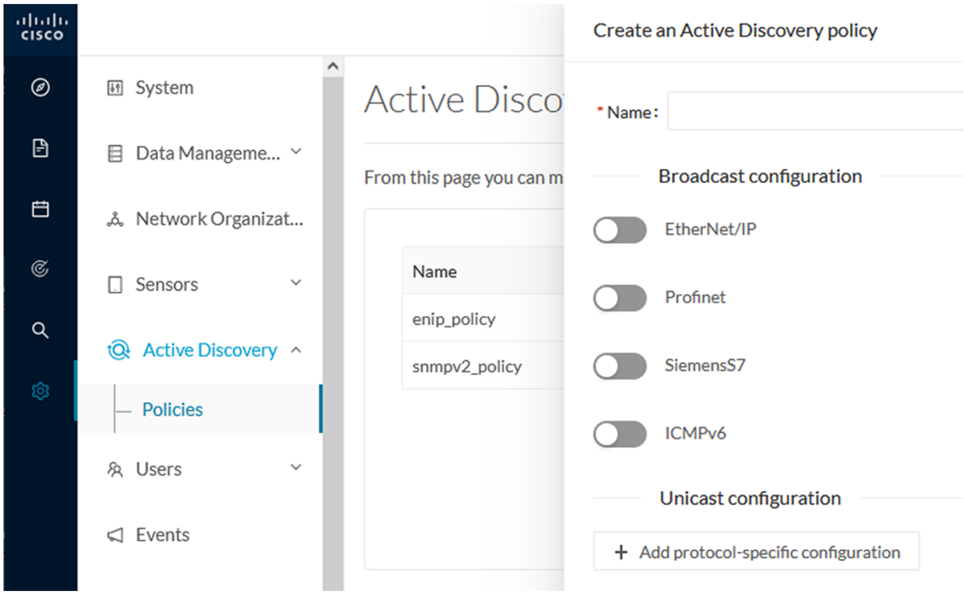
From this page you can manage the Active Discovery policies.

Name	Number of associated presets

No Data

Step 2 Click **+ Create policy**.

A Create an Active Discovery policy overlay appears.



Create an Active Discovery policy

* Name:

Broadcast configuration

- EtherNet/IP
- Profinet
- SiemensS7
- ICMPv6

Unicast configuration

What to do next

- Set Active Discovery Broadcast, on page 2
- Set Active Discovery Unicast, on page 3

Set Active Discovery Broadcast

Before you begin

Active Discovery is compatible with the following Broadcast protocols:

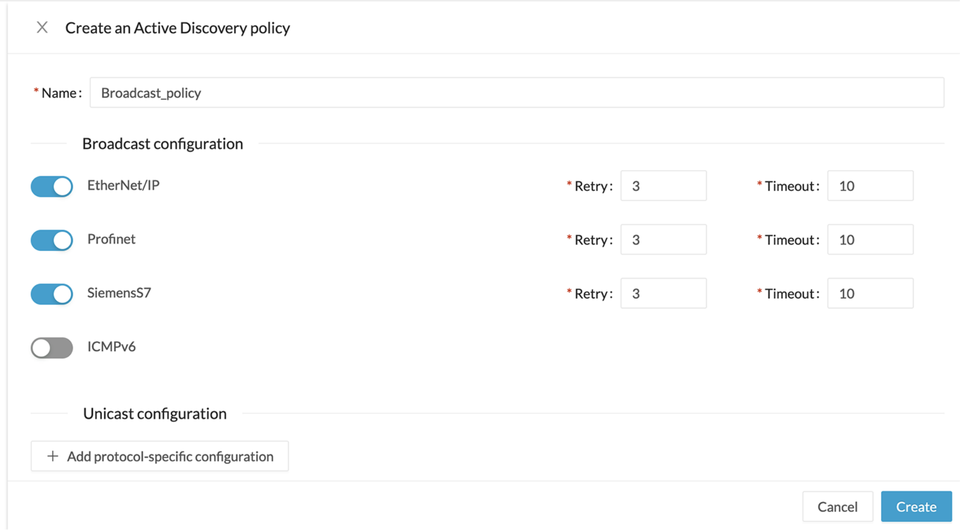
- EtherNet/IP

- 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	* Retry: 3	* Timeout: 10
● Profinet	* Retry: 3	* Timeout: 10
● SiemensS7	* Retry: 3	* Timeout: 10
○ ICMPv6		

Unicast configuration

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

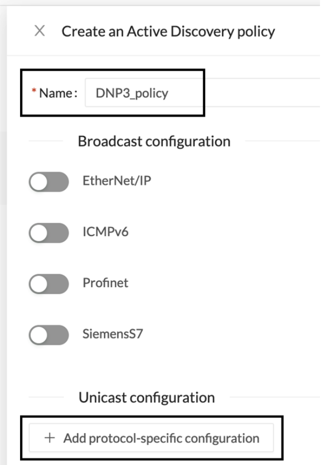
Set Active Discovery Unicast, on page 3

Set Active Discovery Unicast

Before you begin

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

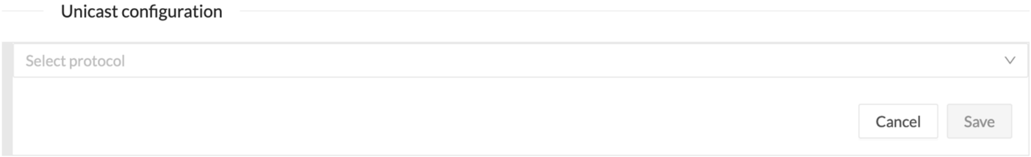
○ Profinet

○ SiemensS7

Unicast configuration

+ Add protocol-specific configuration

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



Unicast configuration

Select protocol

What to do next

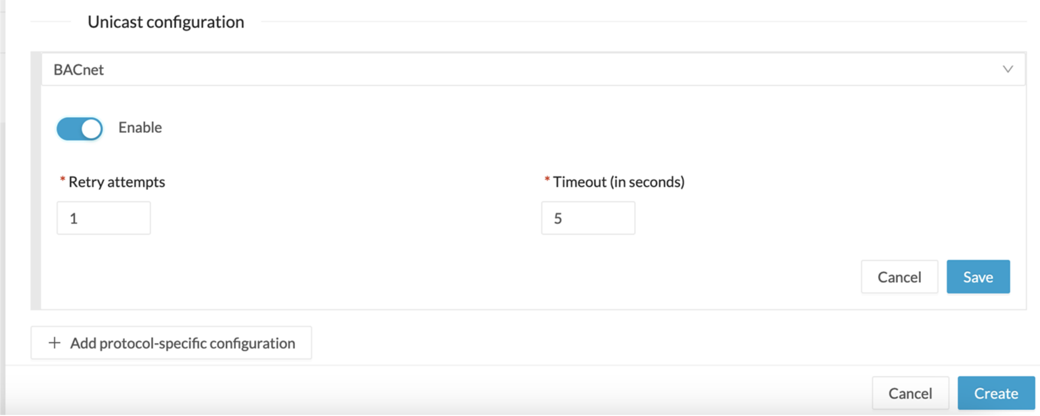
See herebelow configurations per protocol.

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.

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

BACnet

● Enable

* Retry attempts: 1

* Timeout (in seconds): 5

Step 3 Click **Save**.

The menu closes.

Step 4 Click **Create**.

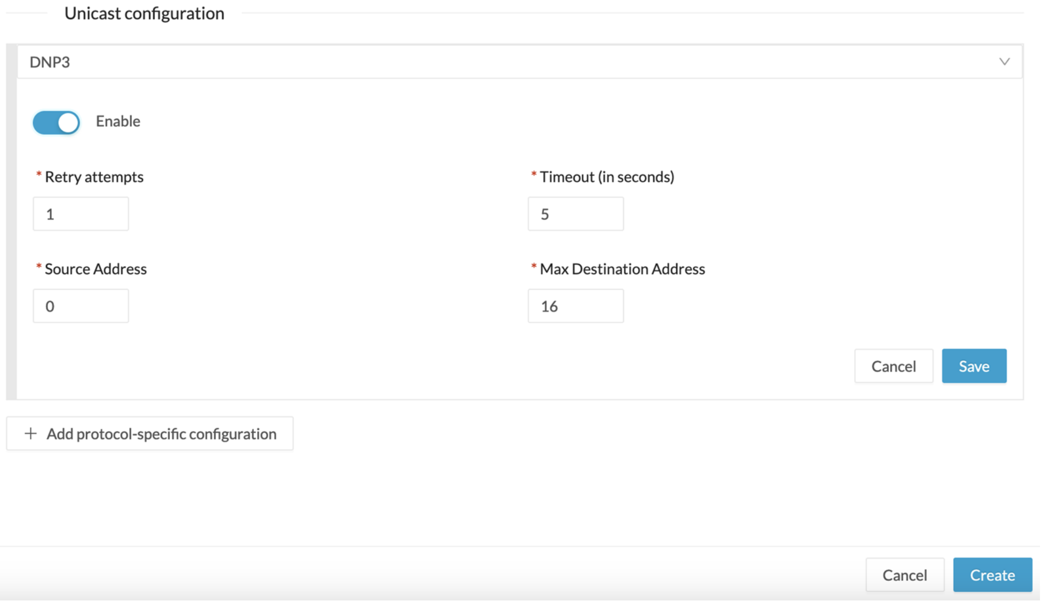
Set Active Discovery Unicast DNP3

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

Before you begin

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: 1

* Timeout (in seconds): 5

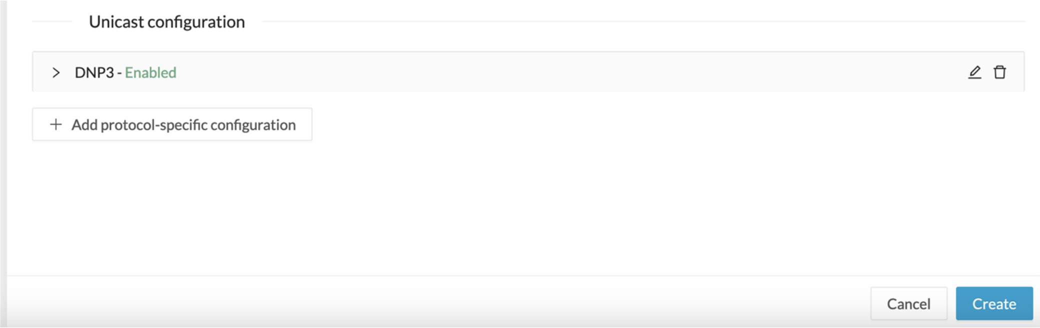
* Source Address: 0

* Max Destination Address: 16

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

Step 5 Click **Create**.

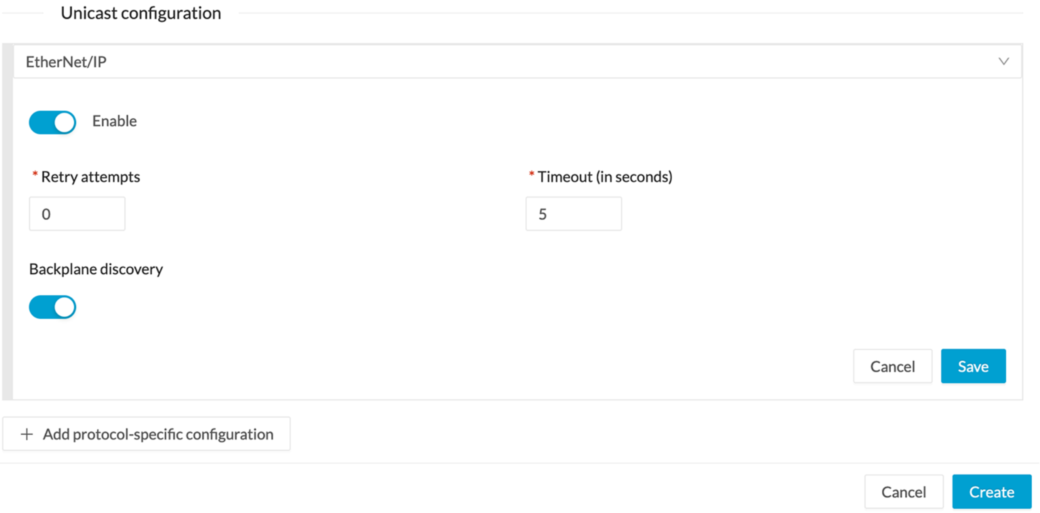
Set Active Discovery Unicast Ethernet/IP

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.

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

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

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



Unicast configuration

EtherNet/IP

Enable: ON

* Retry attempts: 0

* Timeout (in seconds): 5

Backplane discovery: ON

Step 4 Click **Save**.

The menu closes.

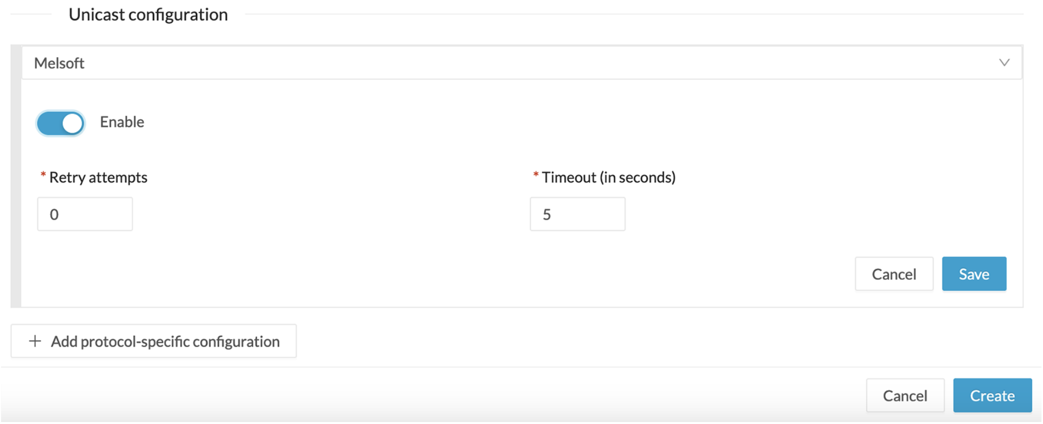
Step 5 Click **Create**.

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.

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: 0

* Timeout (in seconds): 5

Step 3 Click **Save**.

The menu closes.

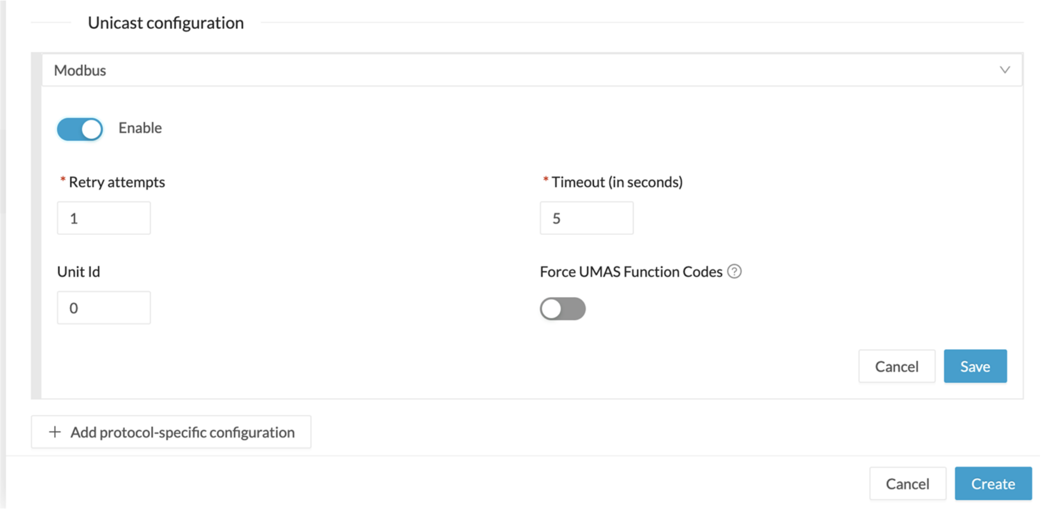
Step 4 Click **Create**.

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.

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: ON

* Retry attempts: 1

* Timeout (in seconds): 5

Unit Id: 0

Force UMAS Function Codes: OFF

Step 3 Click **Save**.

The menu closes.

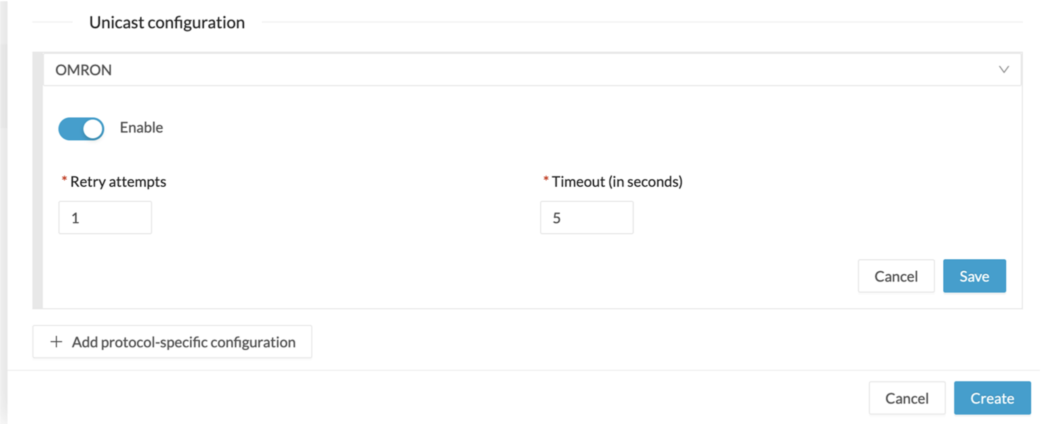
Step 4 Click **Create**.

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.

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

OMRON

Enable: ON

* Retry attempts: 1

* Timeout (in seconds): 5

Step 3 Click **Save**.

The menu closes.

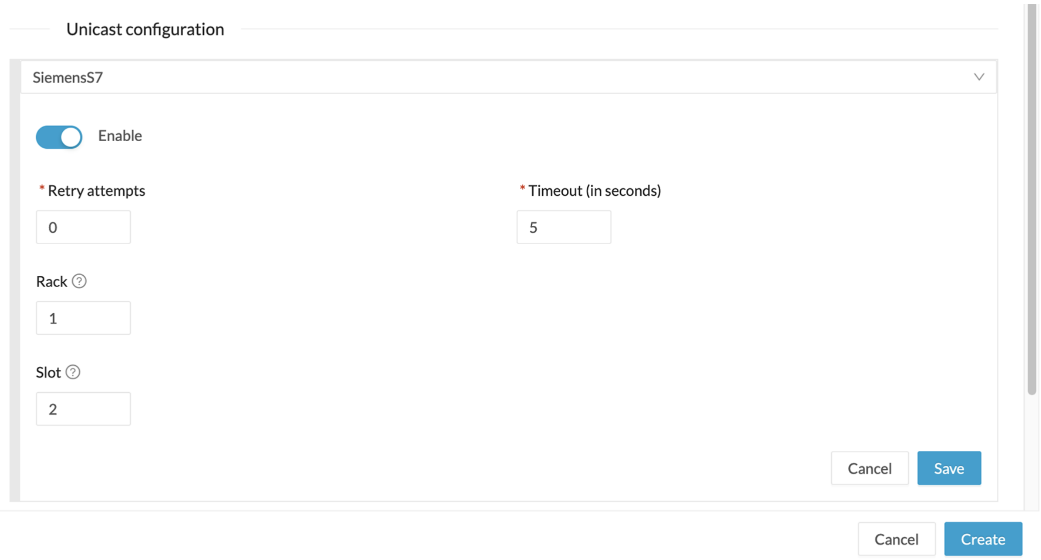
Step 4 Click **Create**.

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.

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

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.

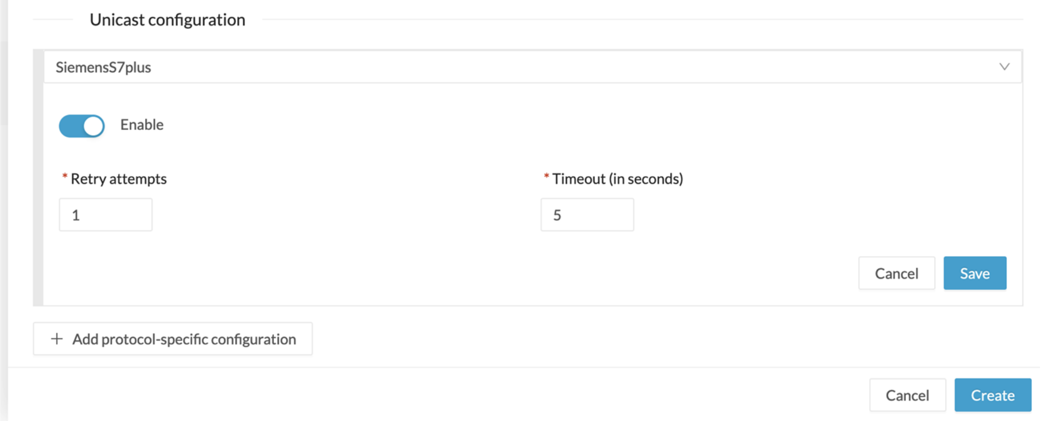
Step 5 Click **Create**.

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.

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

SiemensS7plus

Enable: ON

* Retry attempts: 1

* Timeout (in seconds): 5

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.

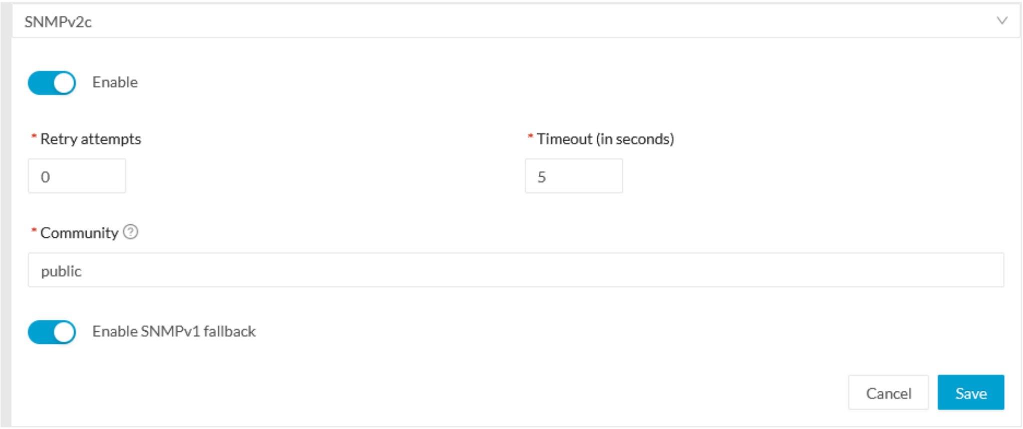
Step 1 Toggle the **Enable** button ON.

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.



SNMPv2c

Enable

* Retry attempts: 0

* Timeout (in seconds): 5

* Community: public

Enable SNMPv1 fallback

Step 5 Click **Save**.

The menu closes.

Step 6 Click **Create**.

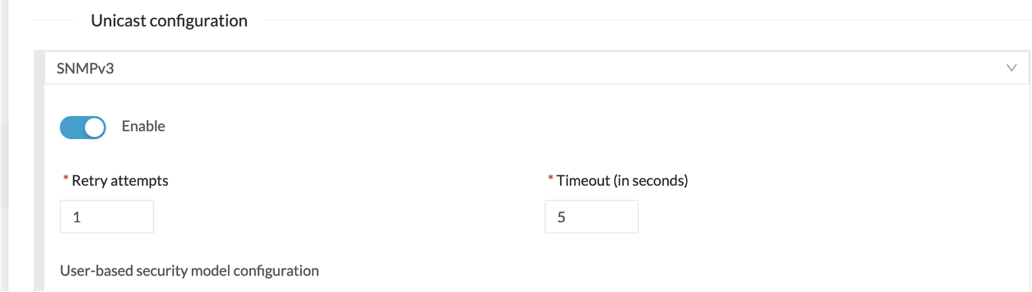
Refer to the Annex appended at the end of this document to see examples of Unicast SNMPv2c results and detailed information about packets.

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.

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

SNMPv3

Enable

* Retry attempts: 1

* Timeout (in seconds): 5

User-based security model configuration

Step 3 Type a community string for authentication.

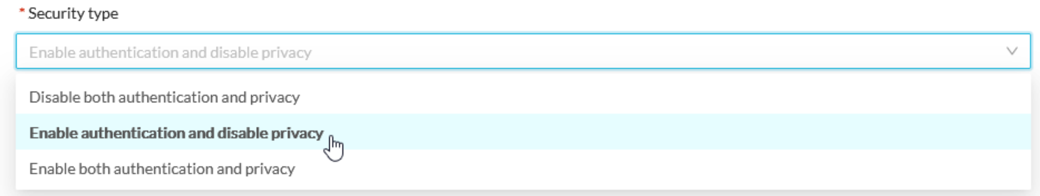
The community string is defined by IT or network administrators. The value "public" is often used by default.

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

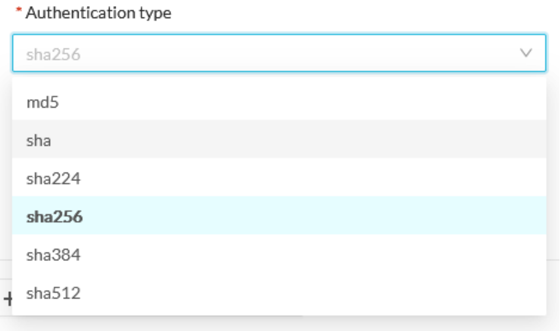
Enable authentication and disable privacy

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.

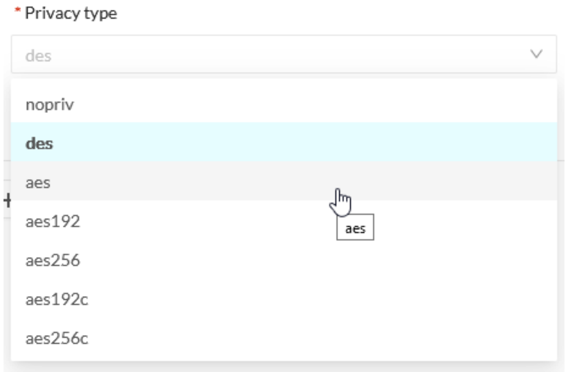


* Authentication type

sha256

- **Enable both authentication and privacy.**

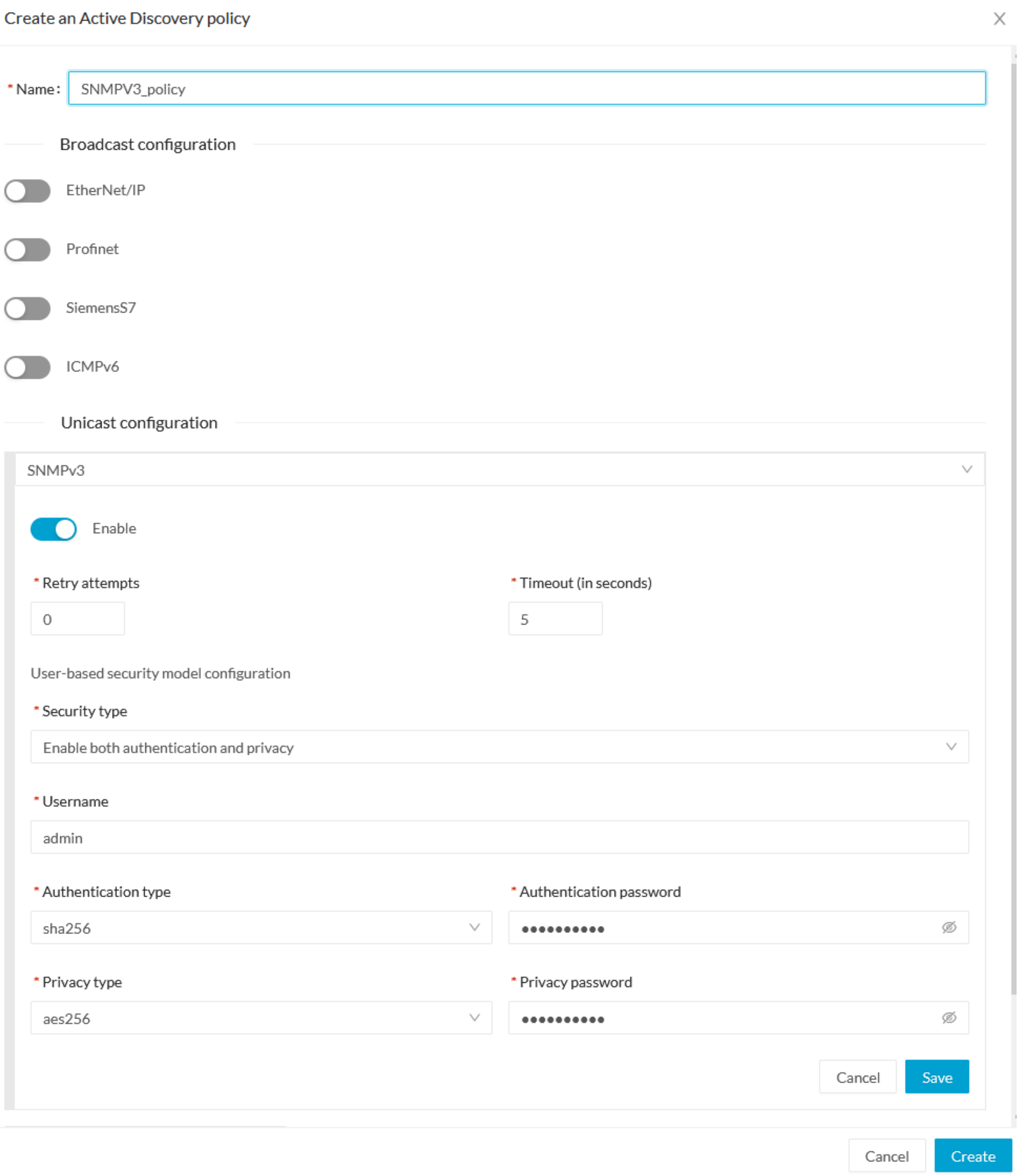
  In addition to the previous level, a DES or AES encryption of the content is requested. Select the level of encryption to use and provide a username and an authentication password. In addition, you must provide a password used for the encryption.



* Privacy type

des

Step 5 Click **Save**.



Create an Active Discovery policy

* Name: SNMPV3_policy

Broadcast configuration

- EtherNet/IP: off
- Profinet: off
- SiemensS7: off
- ICMPv6: off

Unicast configuration

SNMPv3

Enable: on

* Retry attempts: 0

* Timeout (in seconds): 5

User-based security model configuration

* Security type: Enable both authentication and privacy

* Username: admin

* Authentication type: sha256

* Authentication password: ●●●●●●●●●●

* Privacy type: aes256

* 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

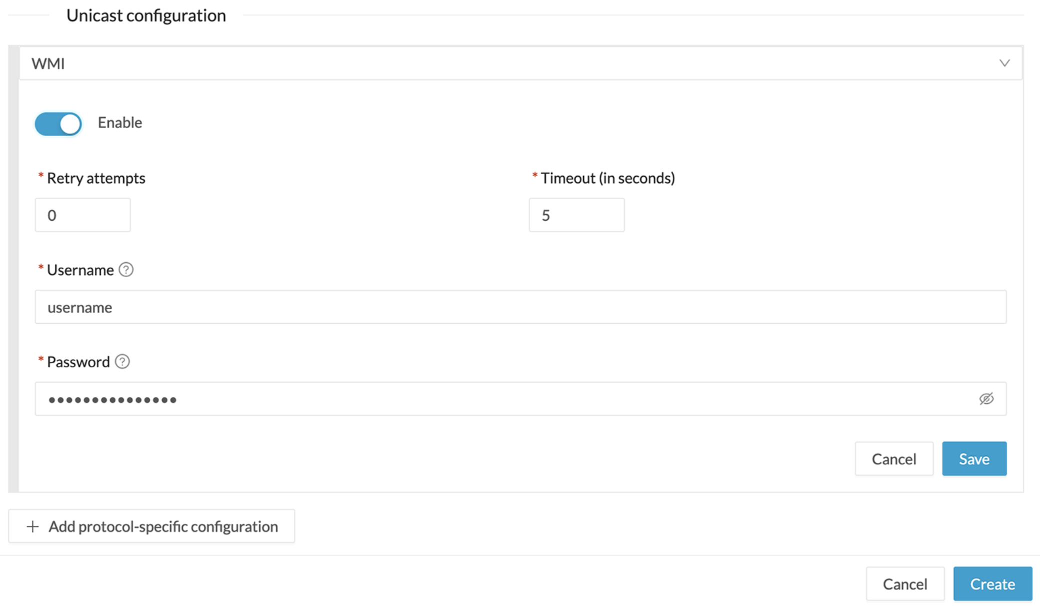
Set Active Discovery Unicast WMI (Windows Management Instrumentation) to collect Windows information like local-host names and operating system versions.

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: ON

* Retry attempts: 0

* Timeout (in seconds): 5

* Username: username

* Password: •••••••••••••••

Step 4 Click **Save**.

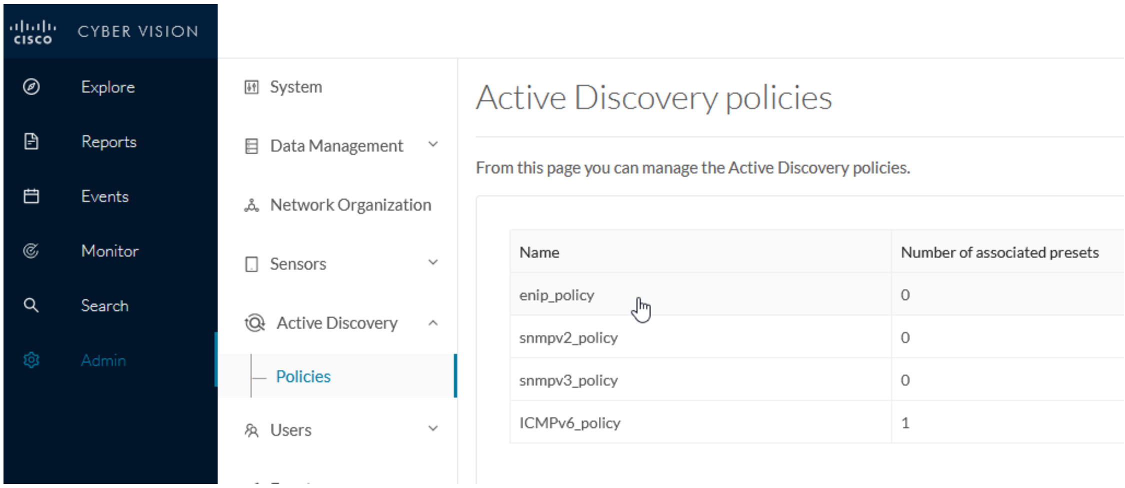
The menu closes.

Step 5 Click **Create**.

Modify a policy

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

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

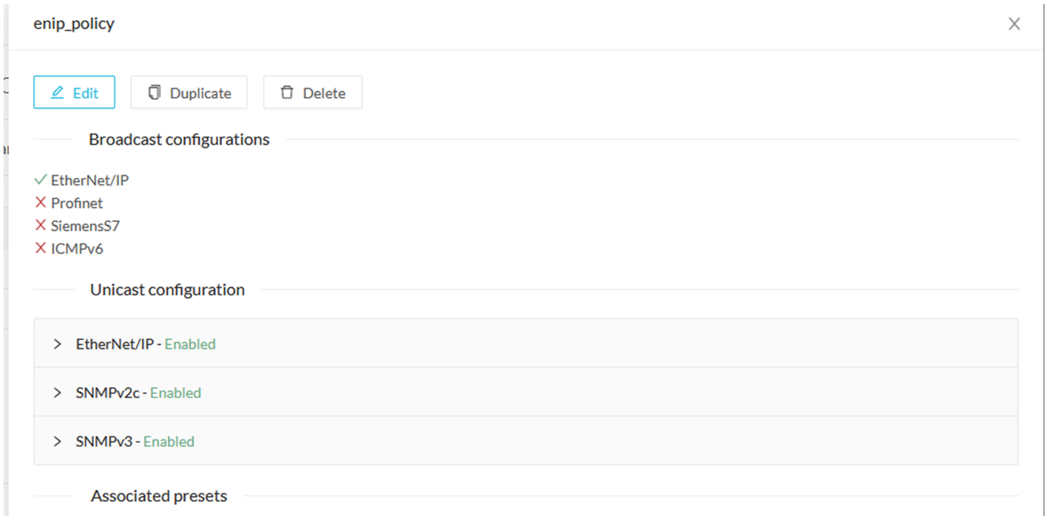


Active Discovery policies

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

Broadcast configurations

✓ EtherNet/IP
✗ Profinet
✗ SiemensS7
✗ ICMPv6

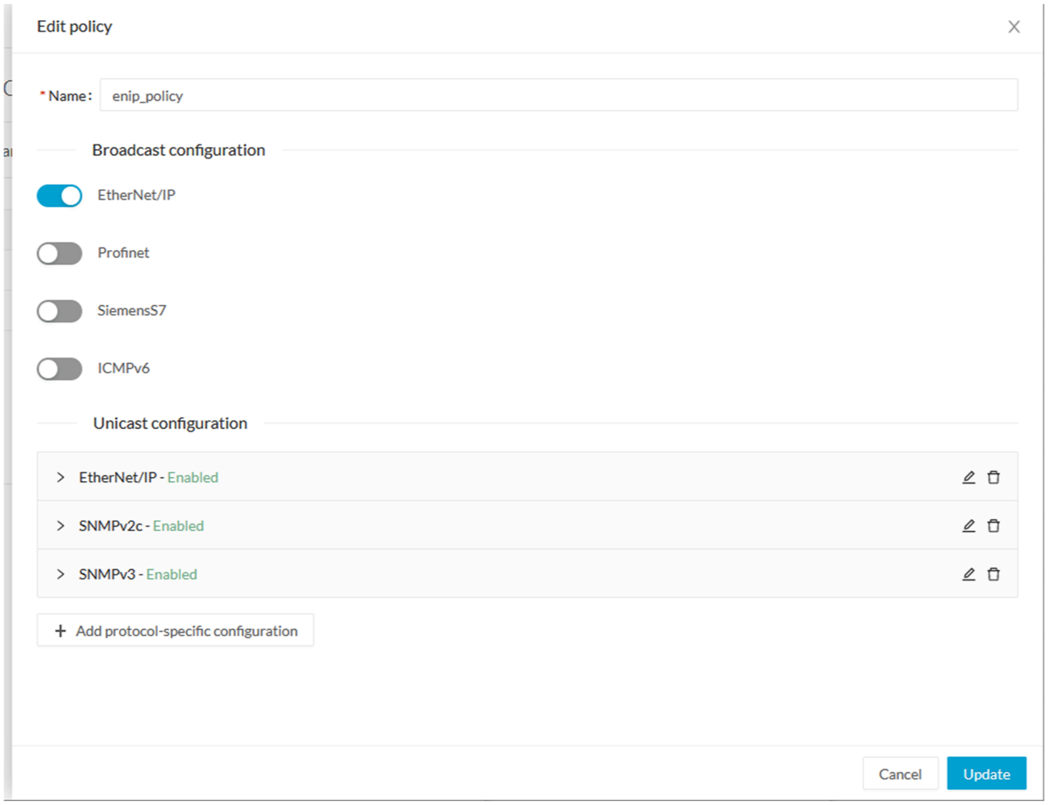
Unicast configuration

> 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.



Edit policy

* Name: enip_policy

Broadcast configuration

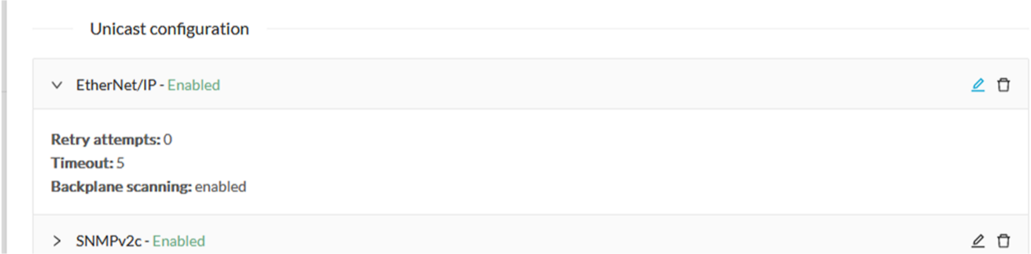
- ● EtherNet/IP
- ○ Profinet
- ○ SiemensS7
- ○ ICMPv6

Unicast configuration

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

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.



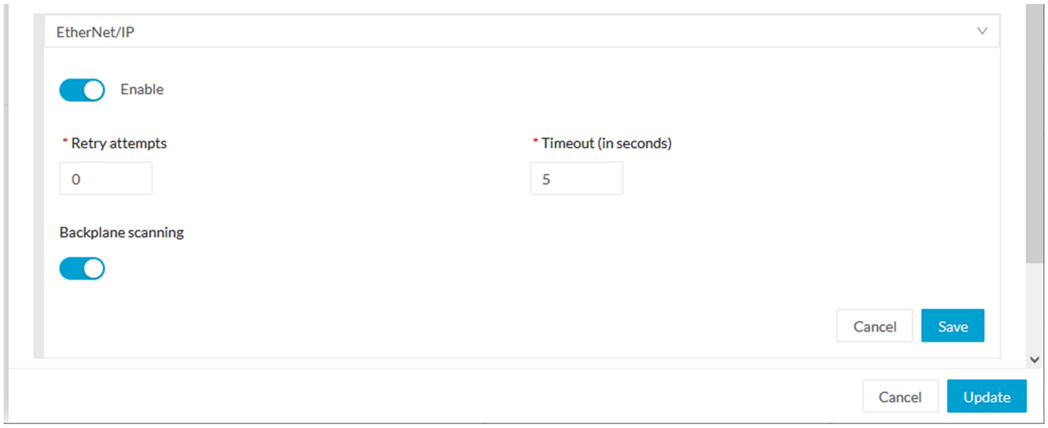
Unicast configuration

EtherNet/IP - Enabled

Retry attempts: 0
Timeout: 5
Backplane scanning: enabled

SNMPv2c - Enabled

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



EtherNet/IP

Enable

* Retry attempts

0

* Timeout (in seconds)

5

Backplane scanning

Step 6 Make the necessary modifications.

Step 7 Click **Save**.

The overlay closes.

Step 8 Click **Update**.