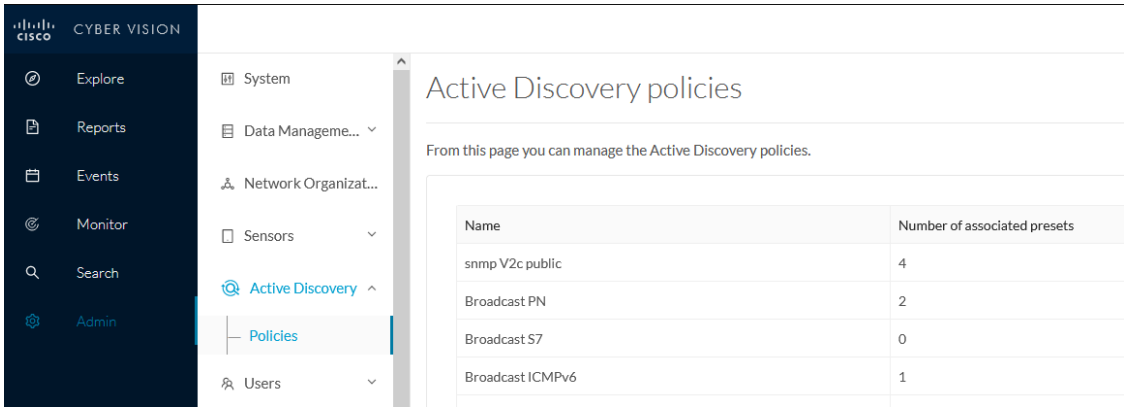
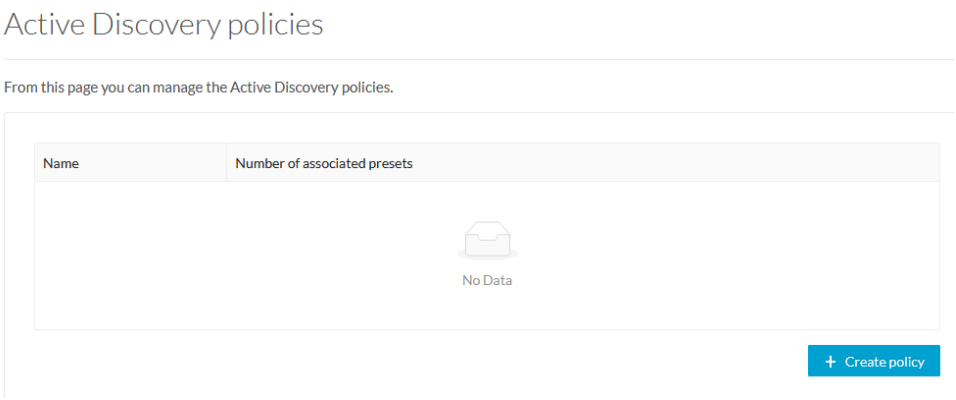
Policies configuration

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.

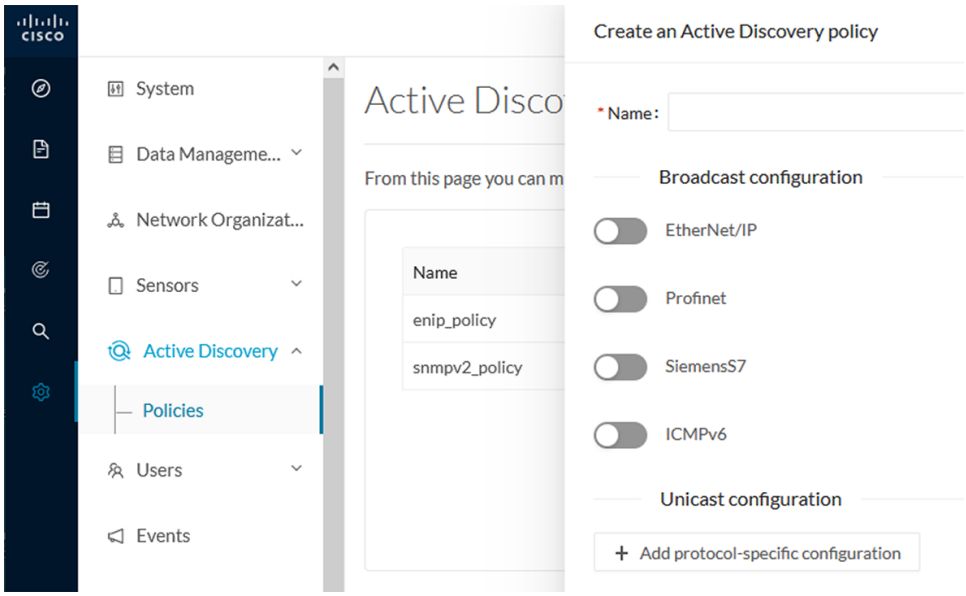


Step 1 Navigate to **Admin** > **Active Discovery** > **Policies** .



Step 2 Click + **Create policy**.

A Create an Active Discovery policy overlay appears.



What to do next

- Set Active Discovery Broadcast, on page 3
- Set Active Discovery Unicast Ethernet/IP, on page 4
- Set Active Discovery Unicast SiemensS7, on page 5
- Set Active Discovery Unicast SNMPv2c, on page 7
- Set Active Discovery Unicast SNMPv3, on page 9
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Broadcast

Before you begin

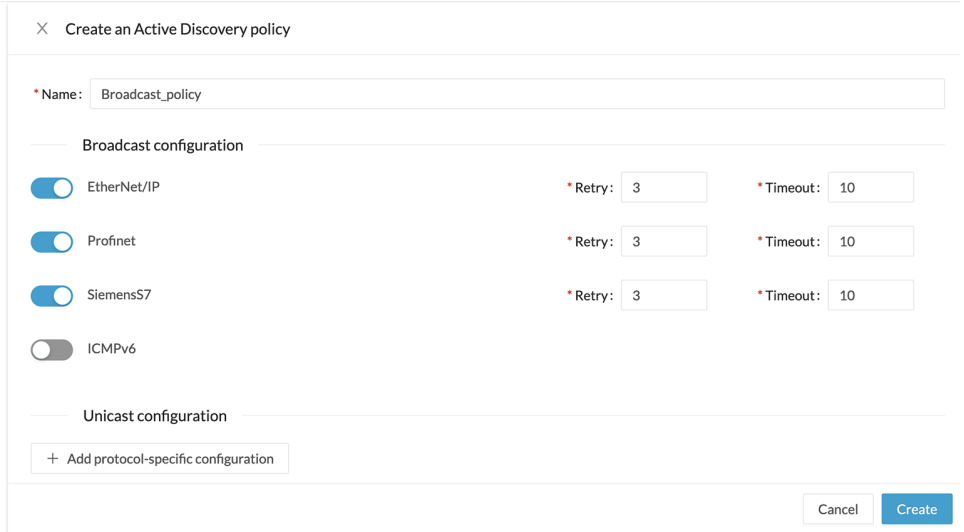
Active Discovery is compatible with the following Broadcast protocols:

- 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 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

Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast Ethernet/IP, on page 4.
- Set Active Discovery Unicast SiemensS7, on page 5

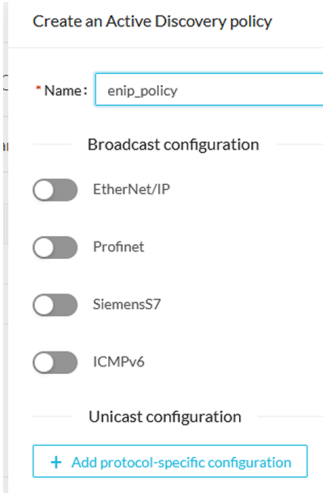
- Set Active Discovery Unicast SNMPv2c, on page 7.
- Set Active Discovery Unicast SNMPv3, on page 9.
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Unicast Ethernet/IP

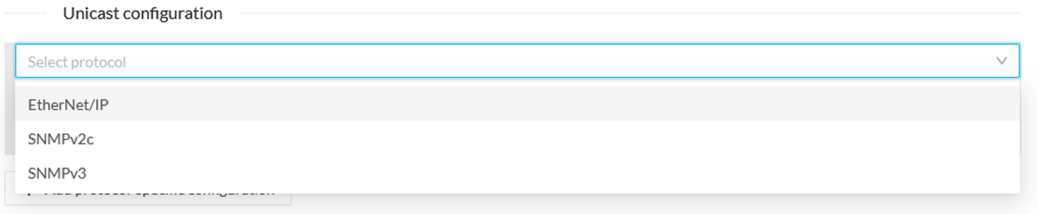
Set Active Discovery Unicast Ethernet/IP to search for devices and components with Ethernet/IP requests. All components with an IPV4 address will be queried.

Step 1 Give the policy a name.

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



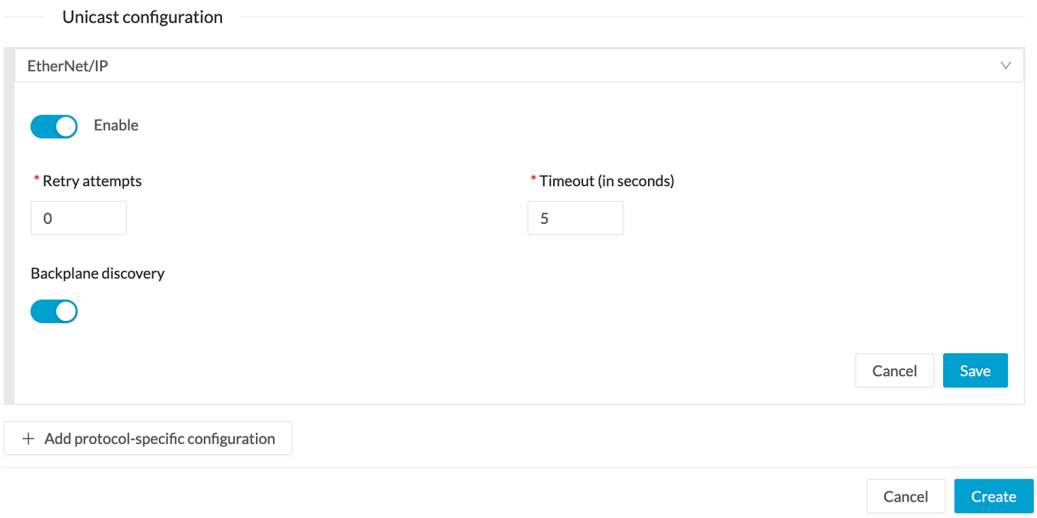
Step 3 Click the **Select protocol** dropdown menu and select **EtherNet/IP**.



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 discovery** button ON. Active Discovery will look for the different module details within the discovered chassis.



Step 7 Click **Save**.

The menu closes.

Step 8 Click **Create**.

What to do next

Add an Active Discovery Unicast configuration:

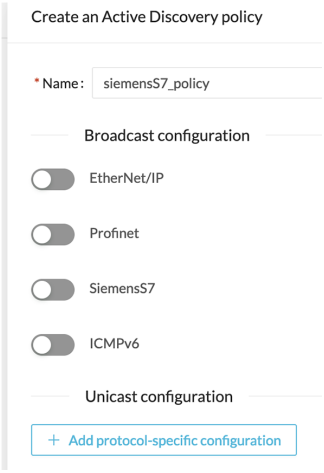
- Set Active Discovery Unicast SiemensS7, on page 5
- Set Active Discovery Unicast SNMPv2c, on page 7.
- Set Active Discovery Unicast SNMPv3, on page 9.
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Unicast SiemensS7

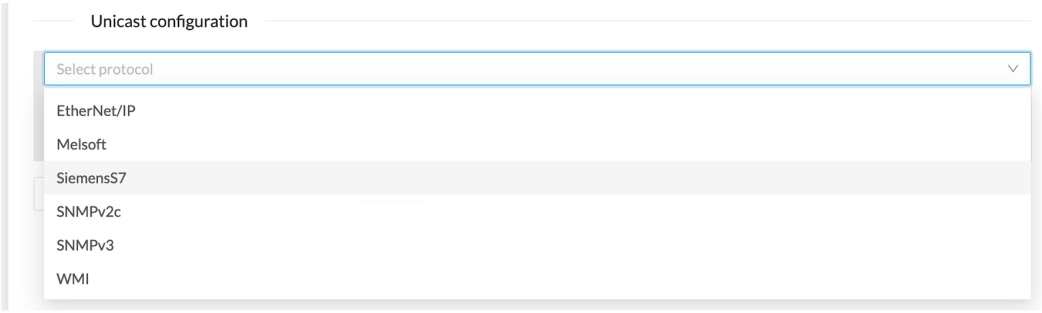
Set Active Discovery Unicast SiemensS7 to search for devices and components with SiemensS7 requests. SiemensS7 is a communication protocol used on Siemens PLCs. Siemens PLCs with an IPV4 address will be queried.

Step 1 Give the policy a name.

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

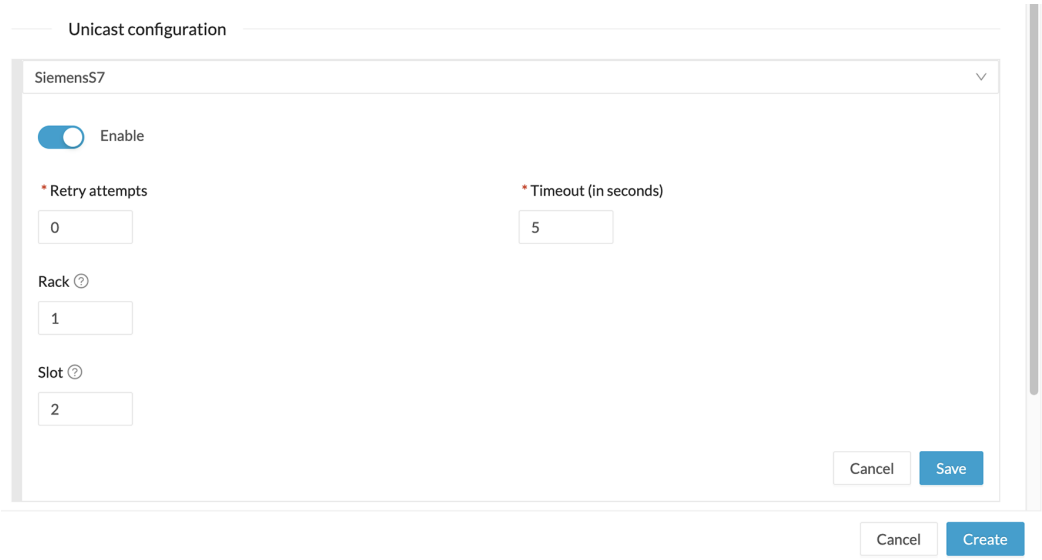


Step 3 Click the **Select protocol** dropdown menu and select **SiemensS7**.



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 Enter a number of racks and slots to be queried.

Slot: number of modules to search for within a chassis.

Step 7 Click **Save**.

The menu closes.

Step 8 Click **Create**.

What to do next

Add an Active Discovery Unicast configuration:

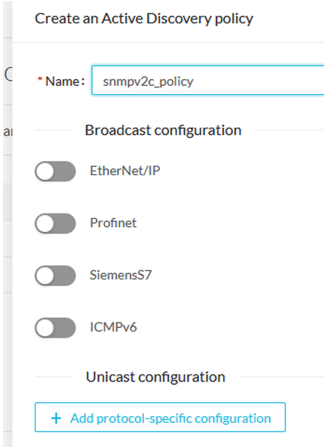
- Set Active Discovery Unicast Ethernet/IP, on page 4
- Set Active Discovery Unicast SNMPv2c, on page 7.
- Set Active Discovery Unicast SNMPv3, on page 9.
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Unicast SNMPv2c

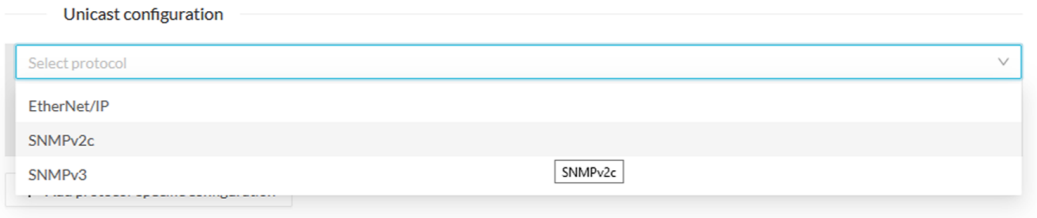
Set Active Discovery Unicast SNMPv2c to search for devices and components with SNMPv2c requests. All components with an IPV4 address will be queried. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

Step 1 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**.



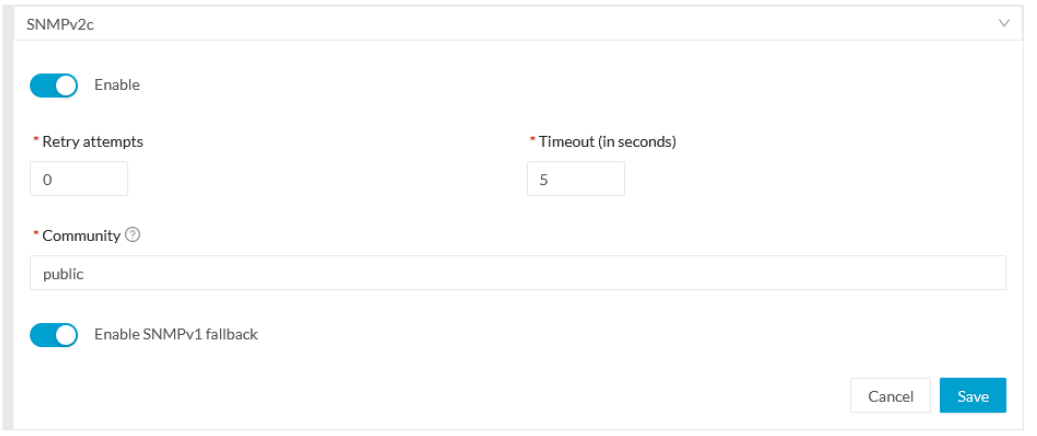
Step 4 Toggle the **Enable** button ON.

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:

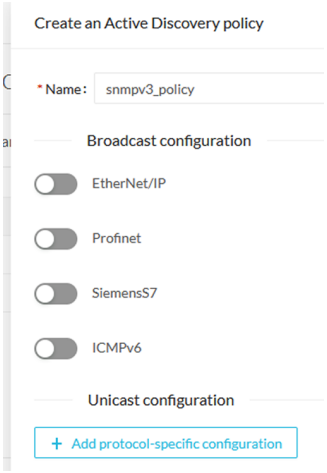
- Set Active Discovery Unicast Ethernet/IP, on page 4
- Set Active Discovery Unicast SiemensS7, on page 5
- Set Active Discovery Unicast SNMPv3, on page 9.
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Unicast SNMPv3

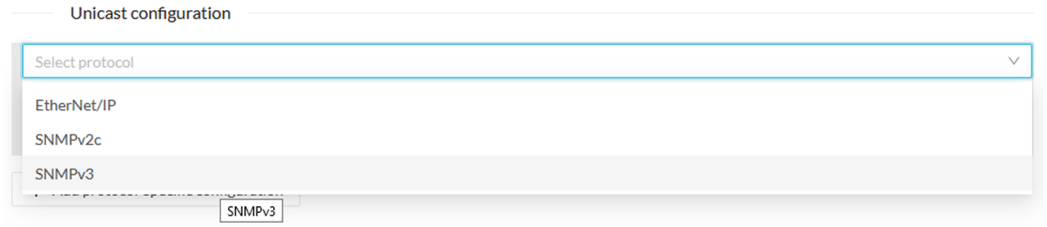
Set Active Discovery Unicast SNMPv3 to search for devices and components with SNMPv3 requests. All components with an IPV4 address will be queried. Default OIDs are requested for all devices and some specific OIDs are requested based on the vendor and the type of components.

Step 1 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.

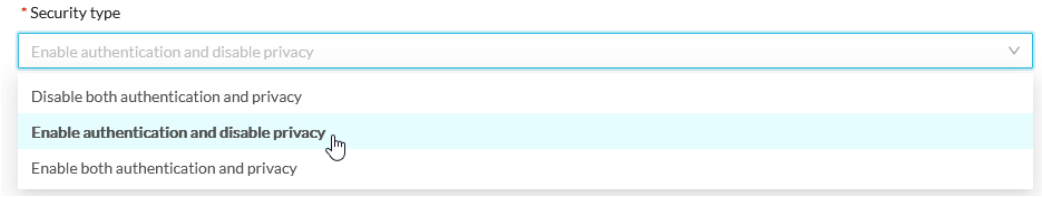
The community string is defined by IT or network administrators. The value "public" is often used by default.

Step 7 Select the proper security and 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.**

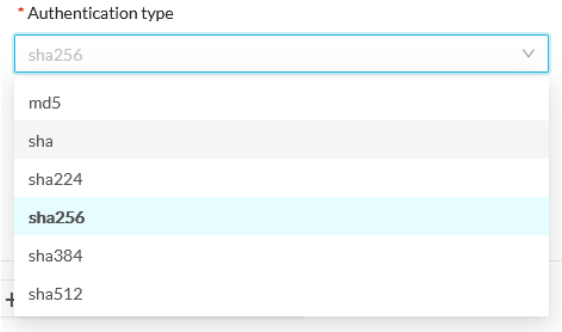
  Only a username is requested for authentication.



- **Enable authentication and disable privacy.**

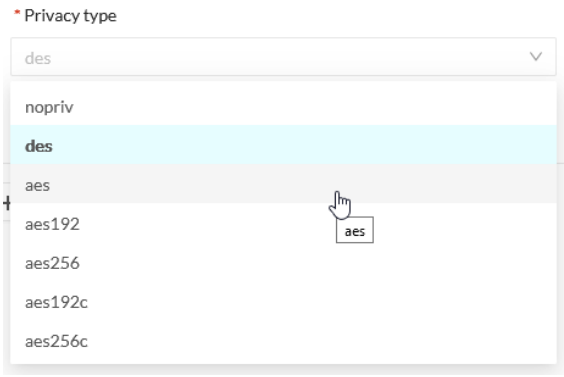
  Authentication will be based on HMAC-MD5 or HMAC-SHA algorithms.

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

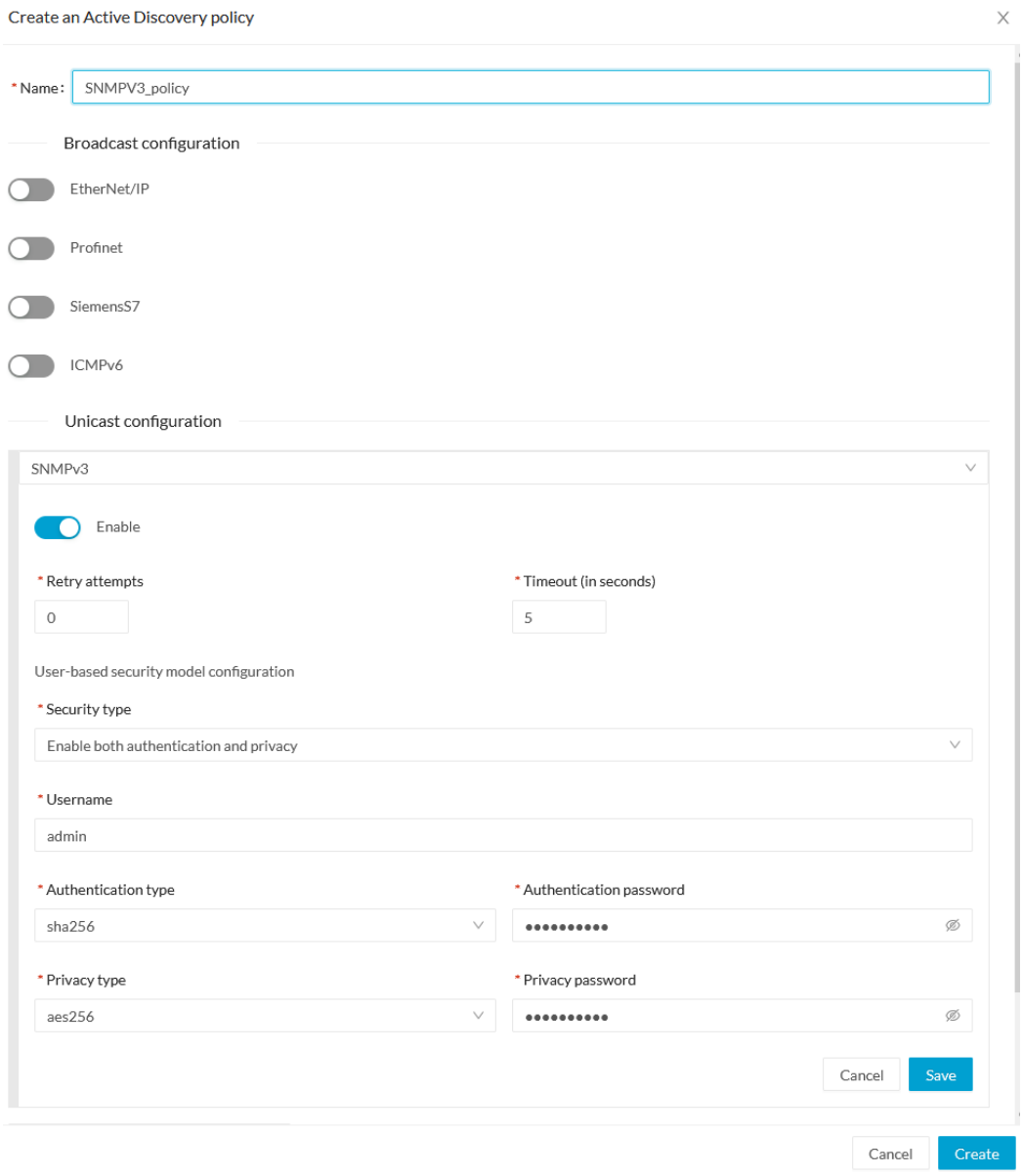


- **Enable both authentication and privacy.**

  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**.



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

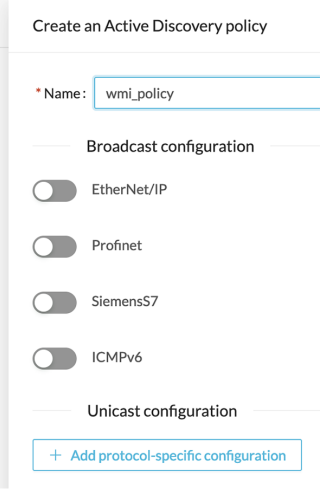
- Set Active Discovery Unicast SiemensS7, on page 5
- Set Active Discovery Unicast SNMPv2c, on page 7.
- Set Active Discovery Unicast WMI, on page 12

Set Active Discovery Unicast WMI

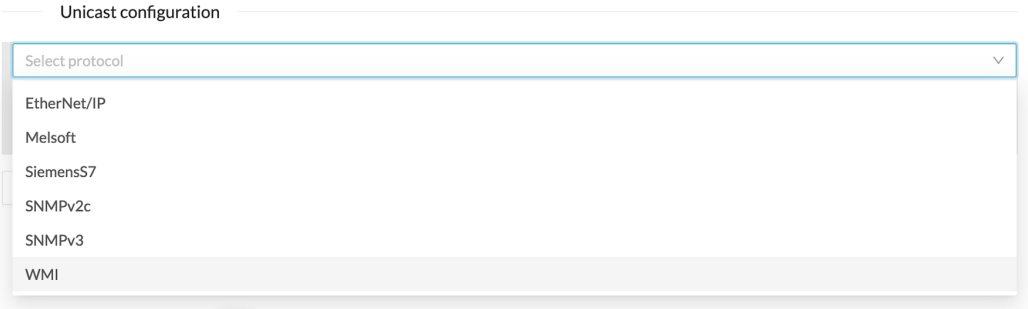
Set Active Discovery Unicast WMI (Windows Management Instrumentation) to collect Windows information like local-host names and operating system versions.

Step 1 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 **WMI**.

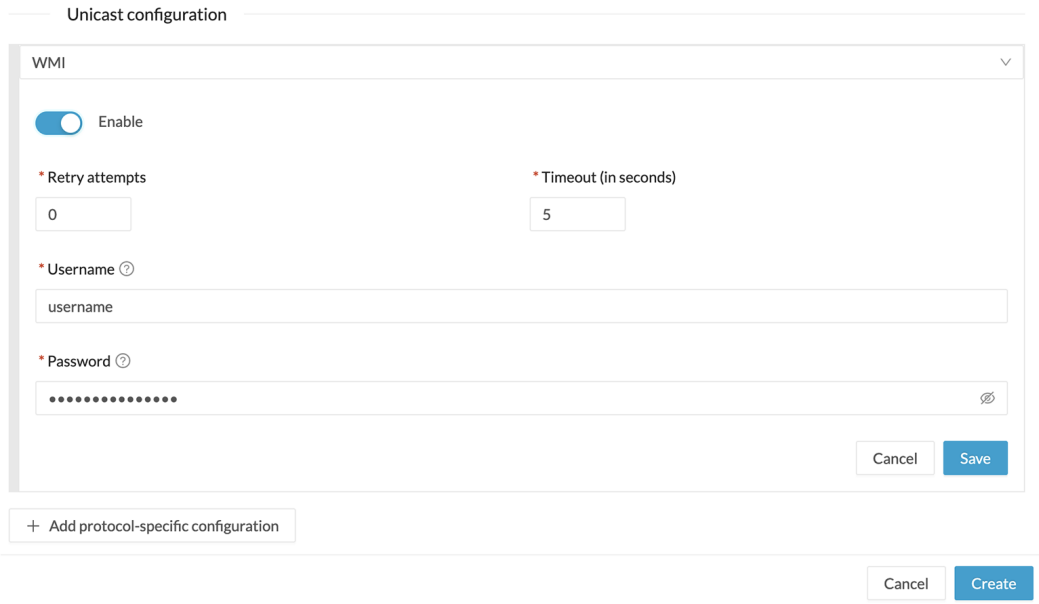


Step 4 Toggle the **Enable** button ON.

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

Step 6 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.



Step 7 Click **Save**.

The menu closes.

Step 8 Click **Create**.

What to do next

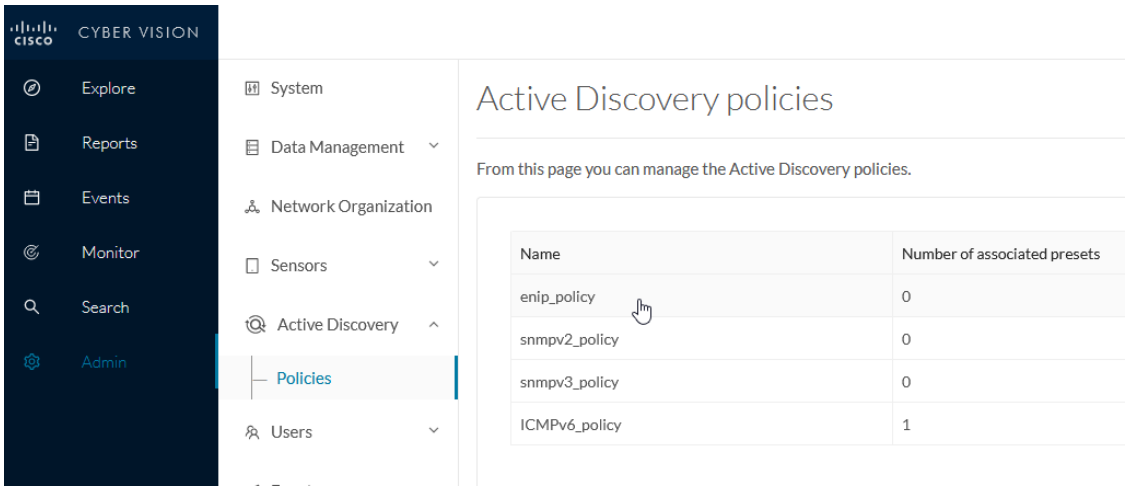
Add an Active Discovery Unicast configuration:

- Set Active Discovery Unicast Ethernet/IP, on page 4
- Set Active Discovery Unicast SiemensS7, on page 5
- Set Active Discovery Unicast SNMPv2c, on page 7.
- Set Active Discovery Unicast SNMPv3, on page 9.

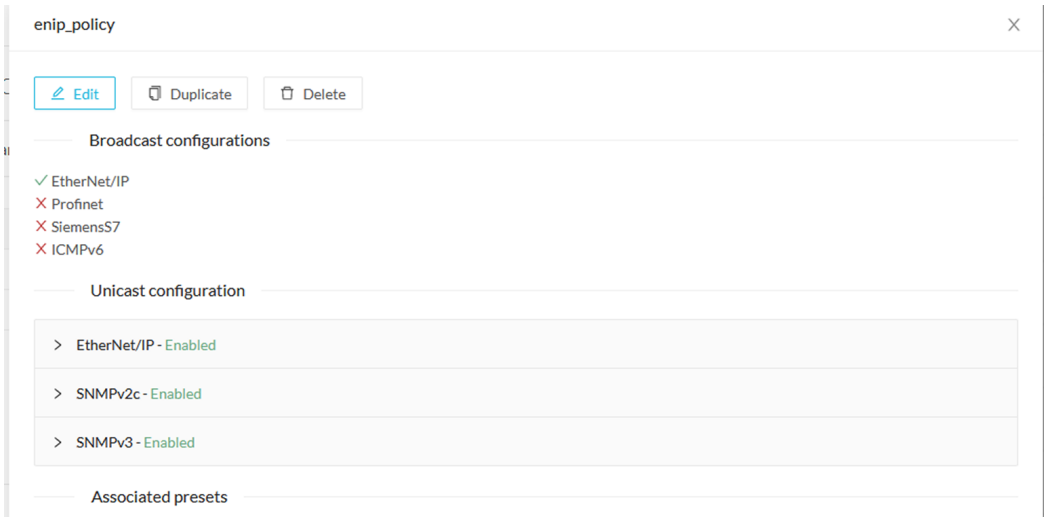
Modify a policy

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

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

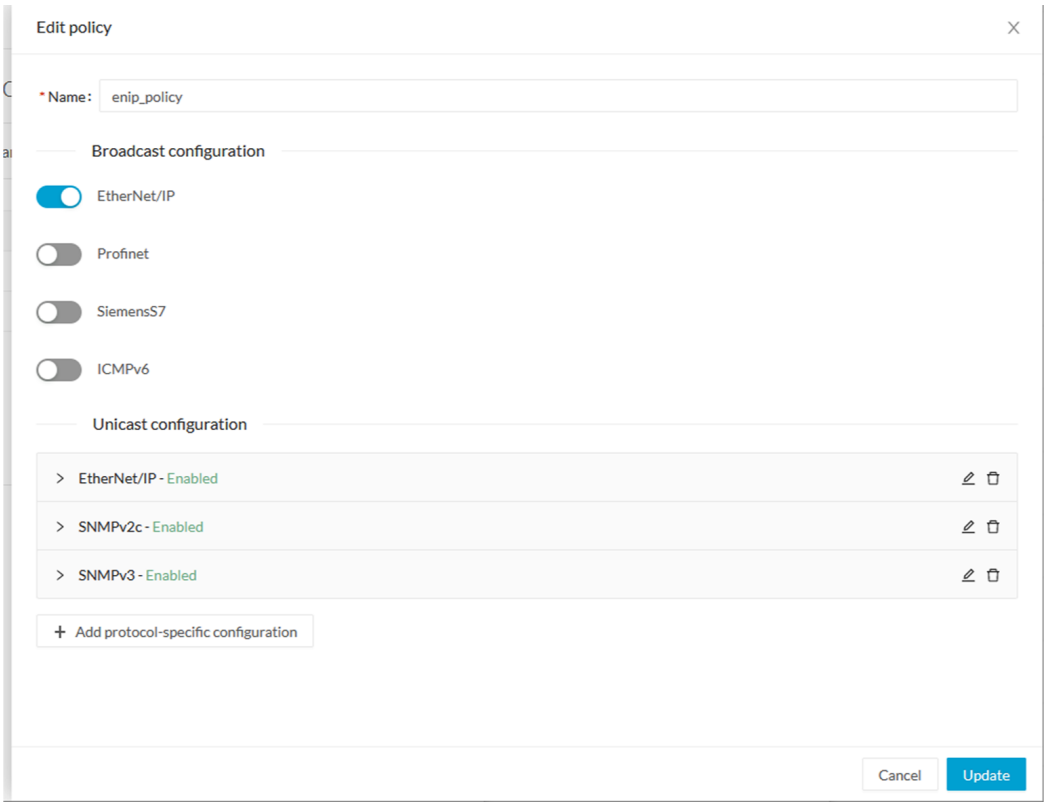


An overlay appears with the policy's configurations.



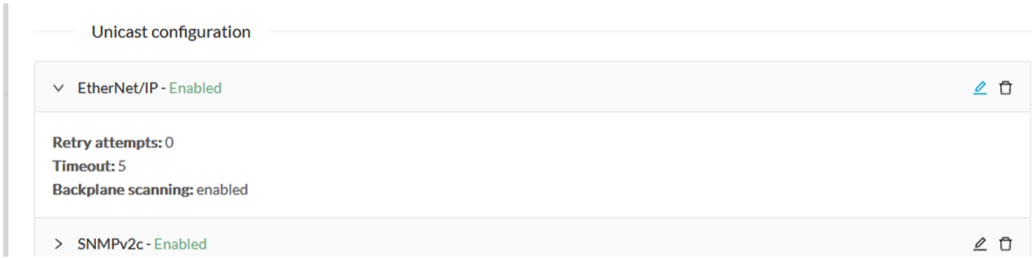
Step 3 Click **Edit**, **Duplicate** or **Delete**.

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

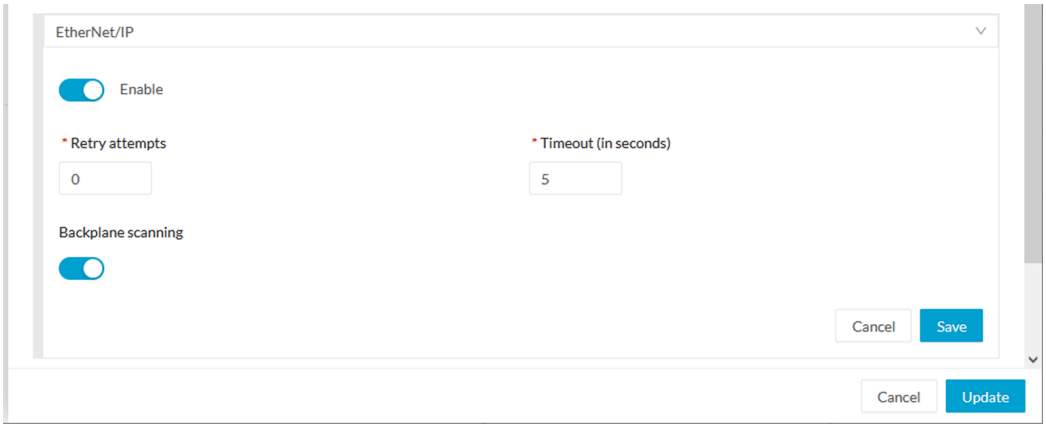


Step 4 You can toggle the buttons ON/OFF to enable/disable broadcast protocols.

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**.