Configure SNMP CoA in Identity Services Engine 2.1 and Above

Contents

Introduction

This document describes Change of Authorization (CoA) feature with the use of Simple Network Management Protocol (SNMP).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of SNMP Protocol
- Prior knowledge of regular expressions
- Prior knowledge of Cisco Identity Service Engine (ISE)
- Identity Service Engine 2.1.
- SNMP Supported Switches

Components Used

The information in this document is based on ISE Version 2.1.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This is a new feature introduced in ISE 2.1. This feature compliments another new feature in ISE viz., redirection by ISE itself and does not depend on Network Devices. Even if ISE sends a redirection URL directly to the end client, the endpoint should be applied with different policy after the authentication in the portal for appropriate network access. For this to happen, in previous versions, ISE sent a RADIUS CoA. Some of the network devices do not understand a RADIUS CoA sent by ISE. Since SNMP is supported by almost all Network Access Devices (NADs), CoA that uses SNMP became a viable option in such a scenario. An SNMP CoA is performed by an SNMP SetRequest sent from ISE to a NAD in order to set certain Object Identifoers (OIDs) which manage the operational status of a port.

Configure ISE

There are two settings on ISE which need to be configured in order for the SNMP CoA to work.

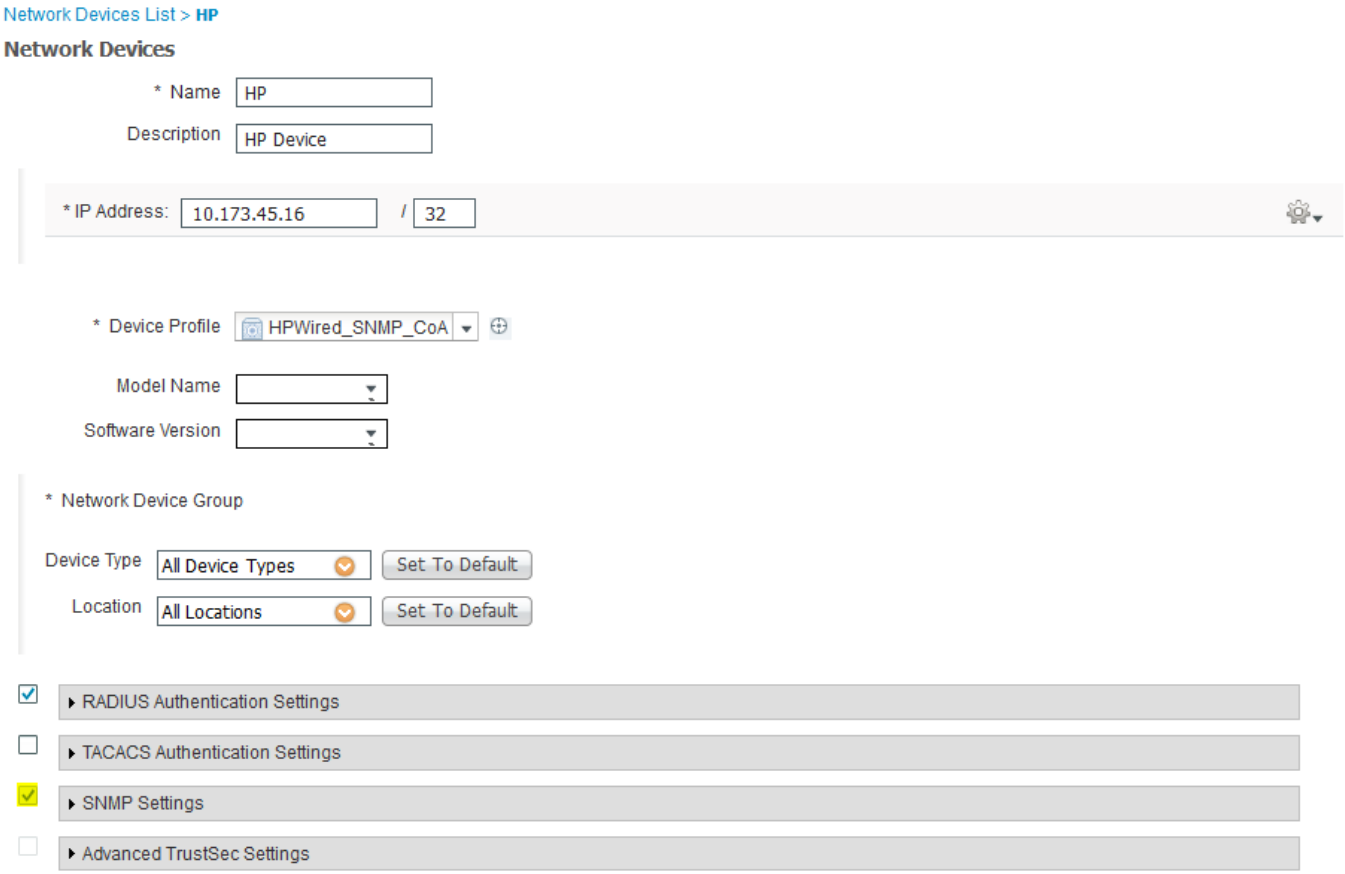
1. SNMP server settings of a NAD.

2. SNMP CoA settings of a NAD Profile.

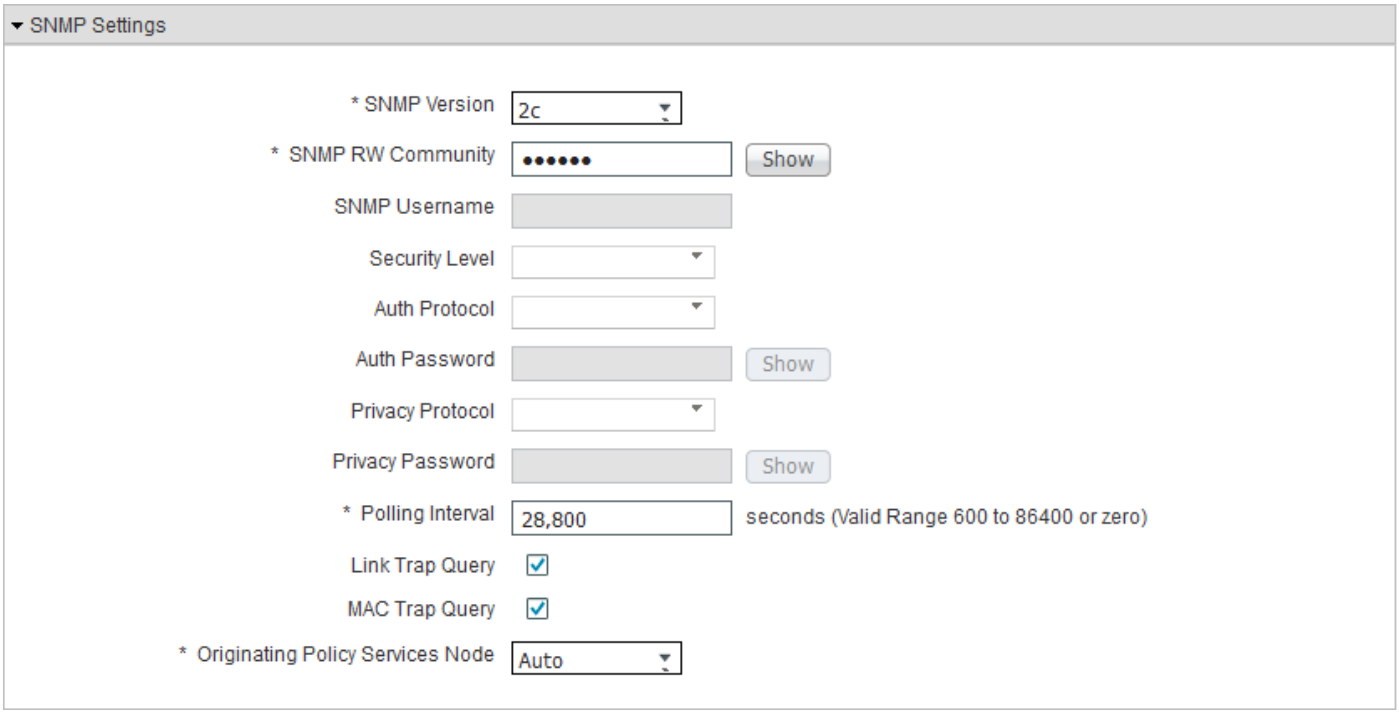
In order to configure SNMP server settings on ISE for a NAD, navigate to **Administration> Network Resources > Network Devices.**

Configure SNMP Settings of NAD

Select a NAD. A checkbox will be available underneath the TACACS Authentication Settings in order to edit the SNMP Settings as shown in the image.



Populate the settings as per the requirement. An example is shown in the image.

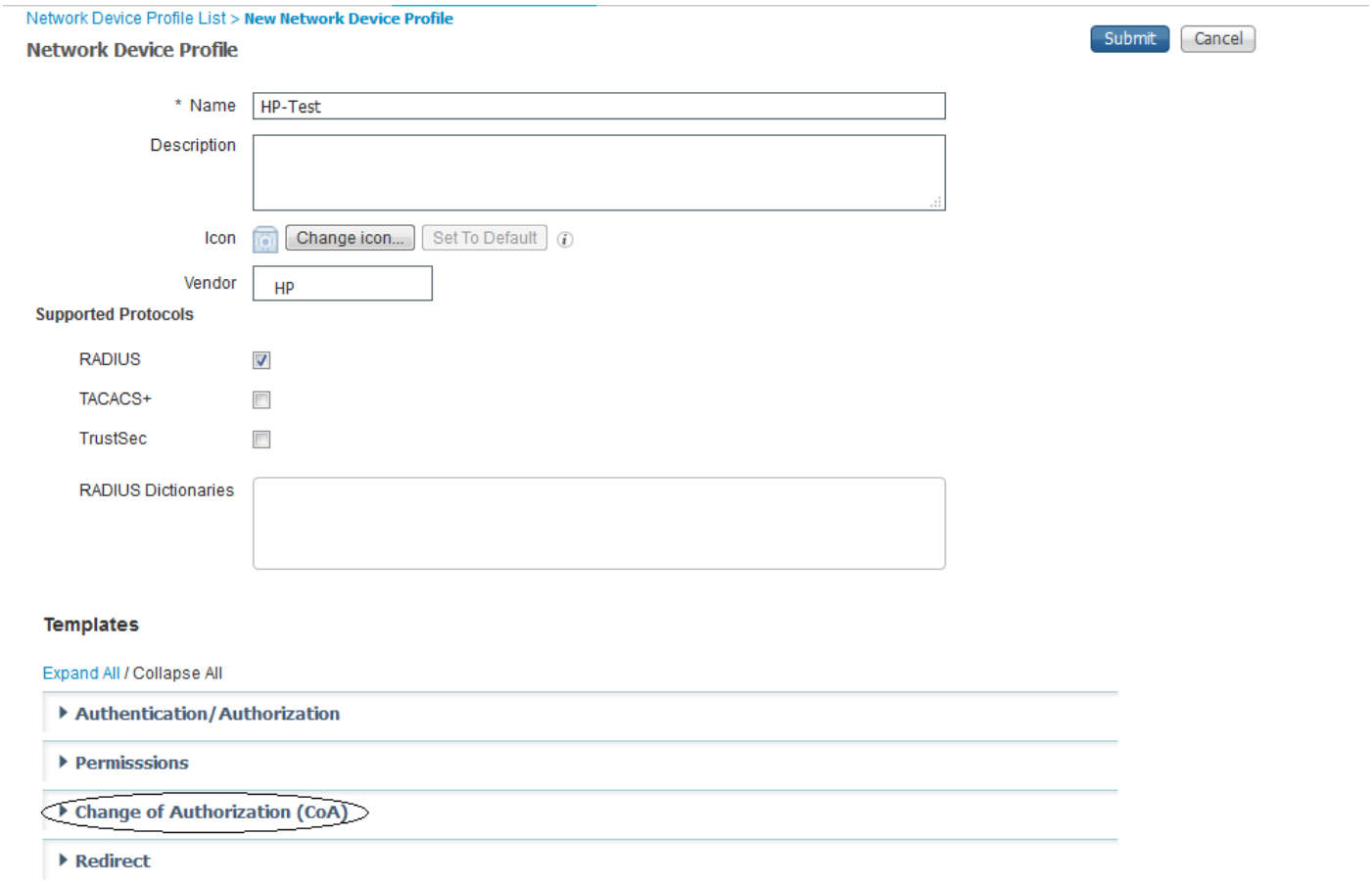


Configure SNMP CoA Settings of Network Device Profile

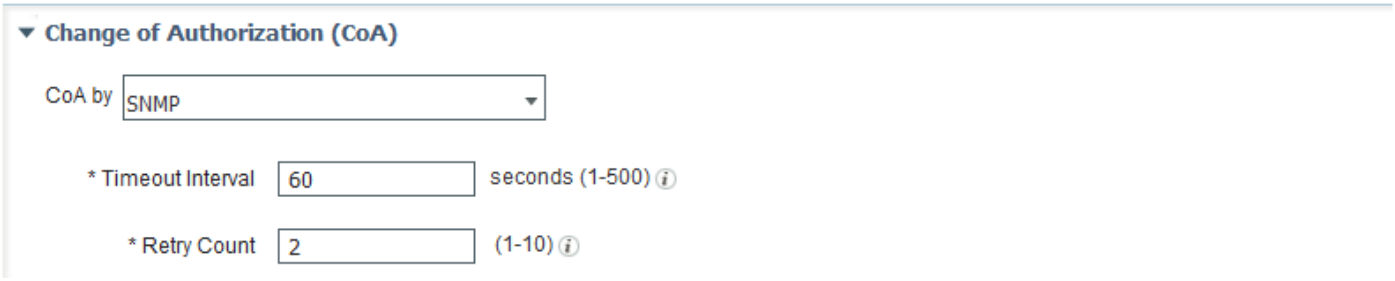
In order to configure the SNMP CoA settings for a Network Device Profile, navigate to **Administration> Network Resources> Network Device Profiles.**

Select the network device profile for which SNMP CoA needs to be configured and expand **Change of Authorization** tab as shown in the image.

Note: SNMP settings of Default Network Device Profiles cannot be edited.



Select the CoA type as **SNMP** and edit the SNMP Timeout and Retry settings. These settings can be set as per the requirement. An example is shown in this image.



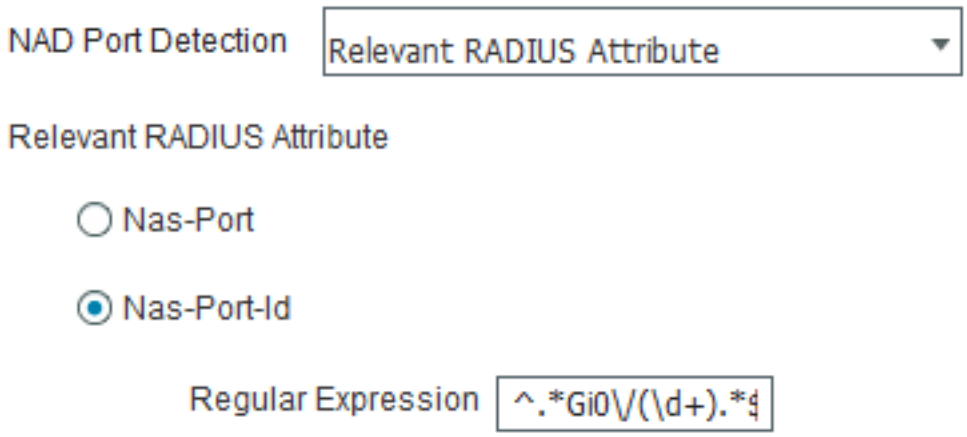
Now, configure NAD Port Detection method by which ISE would know the port for which the OIDs should be set. As of now, the only available method is to retrieve that information from the relevant RADIUS attribute from the accounting information.

The current available RADIUS attributes that give such information are NAS-Port and NAS-Port-Id. Any one of them can be chosen based on the attribute supported by the NAD. Most of the NADs do support NAS-Port-Id. Different vendors have different ways to represent the interfaces available on the NAD. A standard way to extract the information might not be possible. Hence regular expressions are used in ISE to custom the strings to be matched from the NAS-Port-Id attribute value. An example is given here in order to match the ports which are in the form of Gi0/x.

^.*Gi0\/(\d+).*$

This expression essentially means (^)start pattern (.*)match any number of instances of any

charecter (Gi0)match 'Gi0' (\/)match '/' (\d+)match one or more than one instances of any digit (.)match any charecter (*) (.*)match any number of instances of any charecter ($)end pattern. This example can be configured as shown in this image.



OIDs Supported by ISE

By default, ISE provides options in order to configure three types of OIDs in order to perform an operation on the ports identified by the NAS-Port-Id attribute value.

1. Reauthenticate

2. Port Bounce

3. Port Shutdown

Reauthenticate

Reauthenticate OID might not be supported in standard MIBs used by most of the vendors. Information of this OID might vary from vendor to vendor.

> **Note**: This option is provided for possible future enhancement if any device starts to support an OID to manage user sessions based on MAC-Address.

Port Bounce

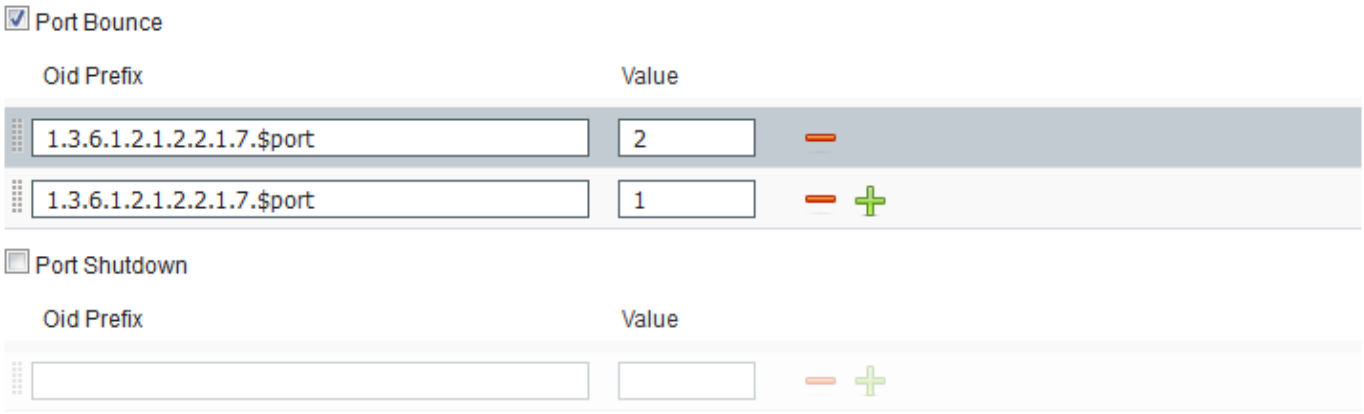
Port bounce uses a port operational OID which has two values, one for Shutting the port down and the other one for Unshutting the port. These are standard OIDs used by most of the vendors.

1.3.6.1.2.1.2.2.1.7.$port is the OID

If the value is set to 2, the port is shutdown and if the value is set to 1, the port is unshut.

Port Shutdown

Select the desired operation that has to be performed on that specific port as shown in the image.

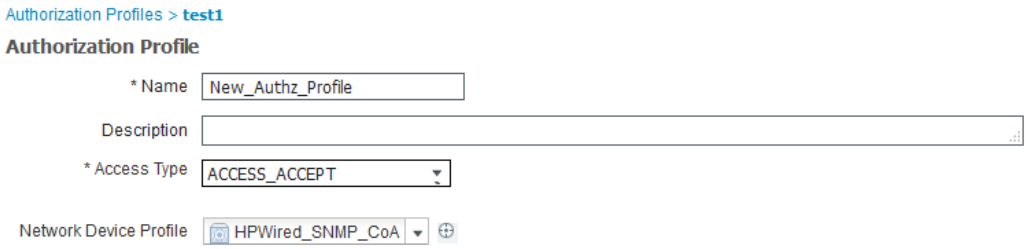


> **Caution**: The order in which the OID values are sent is very important. Because, the order in which the OID values are set is the order in which the operations are performed on the port. If they are set in a reverse order, say 1 and then 2, a port would be unshut first and then shutdown which essentially is shutting down the port.

Submit the changes to the device profile.

This device profile can be used in any authorization profile to be taken into affect. Any CoA operation that has to be performed for an endpoint will be sent as an SNMP SetRequest to the switch with the configured OIDs to be set on the port on which the endpoint is connected. Here is an example in order to configure NAD Profile in Authorization Profile.

To create a new authorization policy or to edit the one that already exists, navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** as shown in the image.



> **Note**: Switch must be configured with ISE as the SNMP Server and should use the same community string that is configured on ISE. Configuration of Switch is out of scope of this document.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.