Configuración de SNMP CoA en Identity Services Engine 2.1 y posteriores

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configuración de ISE](#)
[Configuración de los parámetros SNMP de NAD](#)
[Configuración de los parámetros de SNMP CoA del perfil de dispositivo de red](#)
[OID compatibles con ISE](#)
[Reautenticar](#)
[Rebote de puerto](#)
[Port Shutdown](#)
[Verificación](#)
[Troubleshoot](#)

Introducción

Este documento describe la función de cambio de autorización (CoA) con el uso del protocolo simple de administración de red (SNMP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del protocolo SNMP
- Conocimiento previo de expresiones regulares
- Conocimiento previo de Cisco Identity Service Engine (ISE)
- Identity Service Engine 2.1.
- Switches admitidos por SNMP

Componentes Utilizados

La información de este documento se basa en la versión 2.1 de ISE.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Esta es una nueva función introducida en ISE 2.1. Esta función complementa otra nueva función de ISE, es decir, la redirección por parte del propio ISE y no depende de los dispositivos de red. Incluso si ISE envía una URL de redirección directamente al cliente final, el terminal debe aplicarse con una política diferente después de la autenticación en el portal para el acceso adecuado a la red. Para que esto sucediera, en versiones anteriores, ISE envió una CoA RADIUS. Algunos de los dispositivos de red no entienden una CoA RADIUS enviada por ISE. Dado que SNMP es compatible con casi todos los dispositivos de acceso a la red (NAD), la CoA que utiliza SNMP se ha convertido en una opción viable en este escenario. Una CoA SNMP se realiza mediante una petición SetRequest SNMP enviada desde ISE a un NAD para establecer determinados identificadores de objeto (OID) que administran el estado operativo de un puerto.

Configuración de ISE

Hay dos configuraciones en ISE que deben configurarse para que la CoA SNMP funcione.

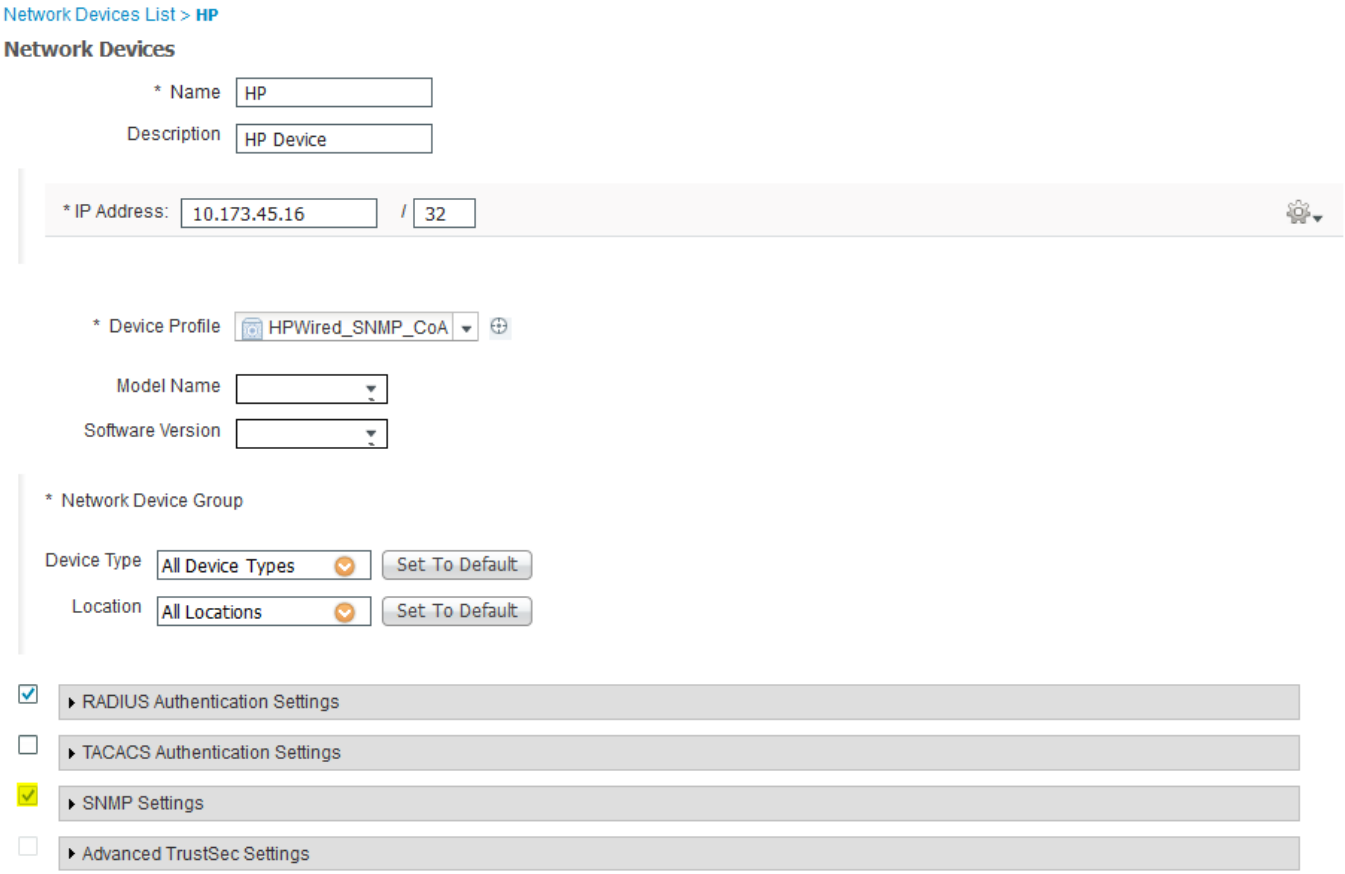
1. Configuración del servidor SNMP de un NAD.

2. Configuración de SNMP CoA de un perfil NAD.

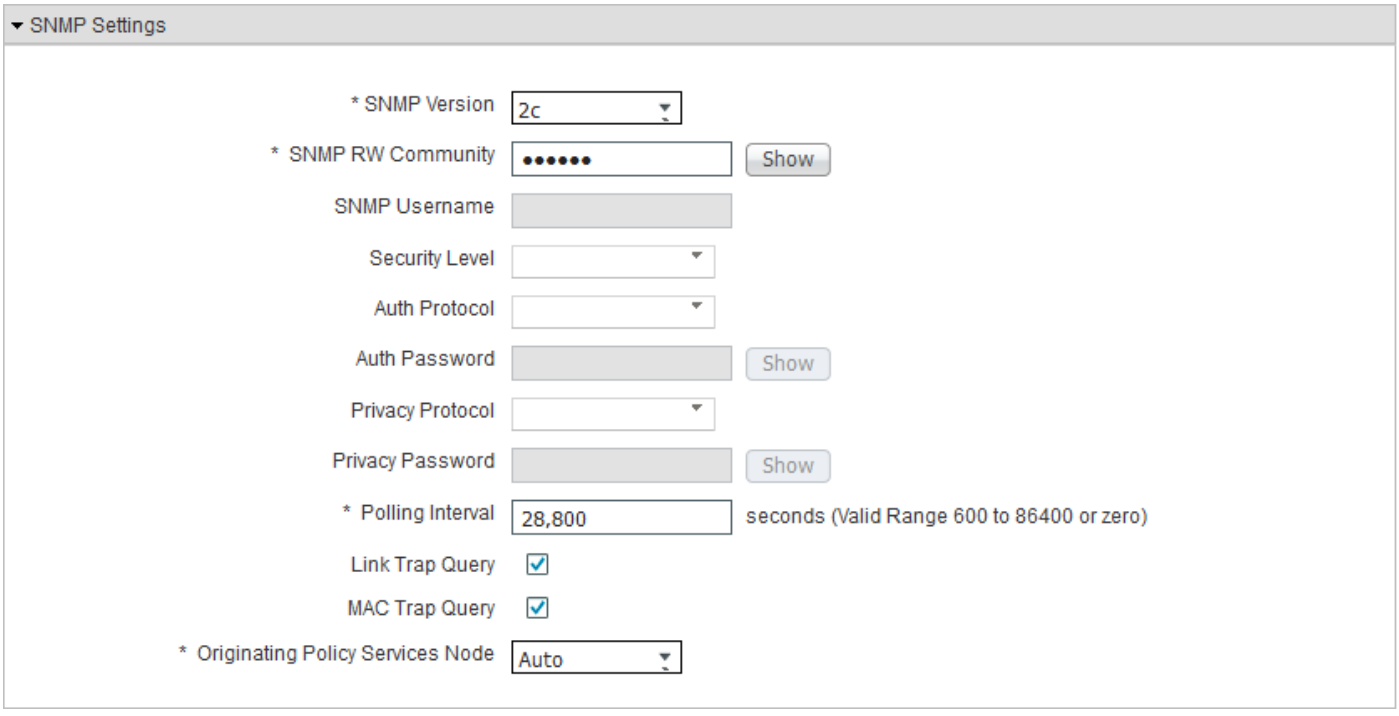
Para configurar la configuración del servidor SNMP en ISE para un NAD, navegue hasta **Administration> Network Resources > Network Devices.**

Configuración de los parámetros SNMP de NAD

Seleccione un NAD. Debajo de la configuración de autenticación TACACS habrá disponible una casilla de verificación para editar la configuración SNMP, como se muestra en la imagen.



Rellene los parámetros según los requisitos. Se muestra un ejemplo en la imagen.

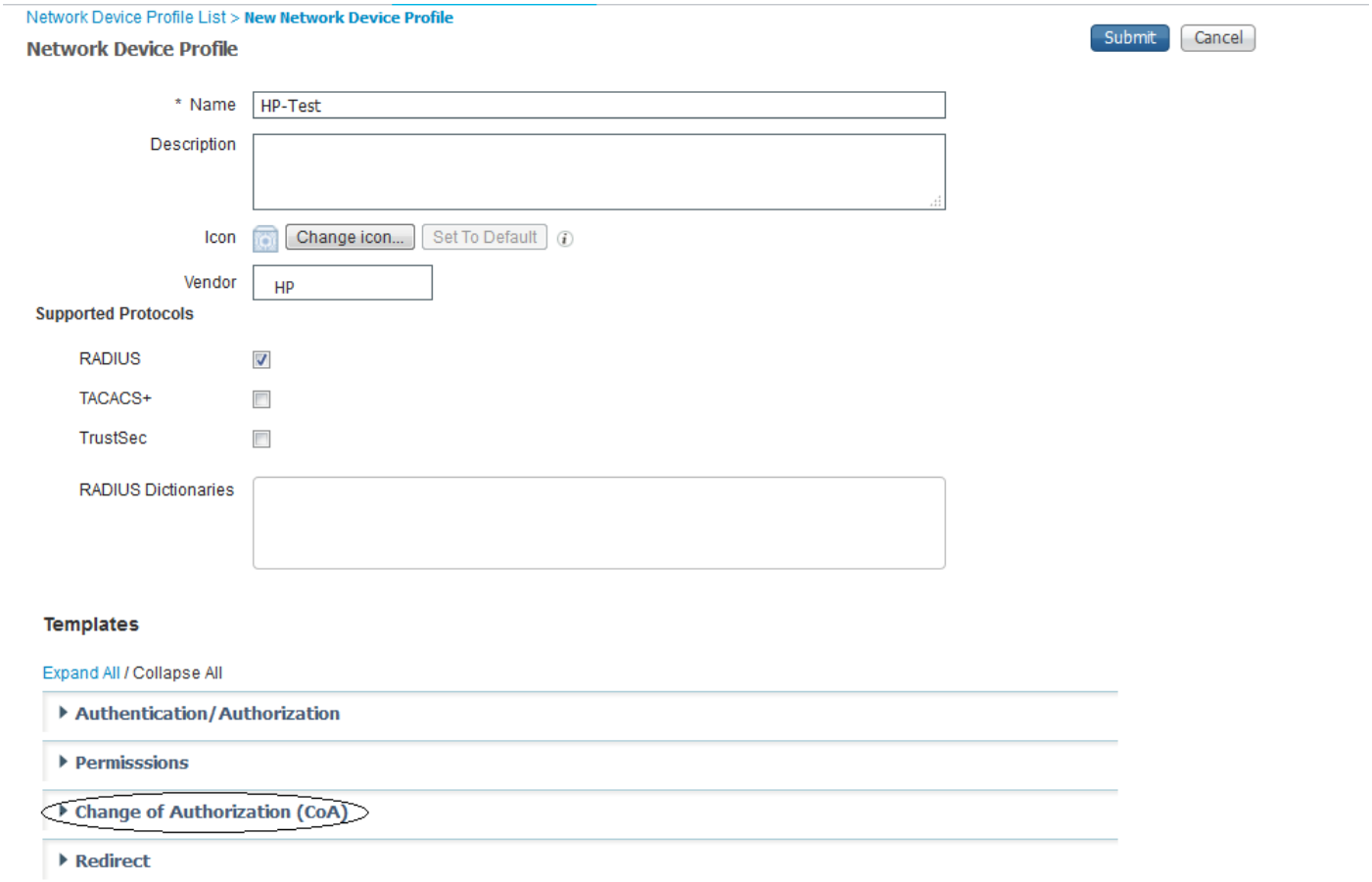


Configuración de los parámetros de SNMP CoA del perfil de dispositivo de red

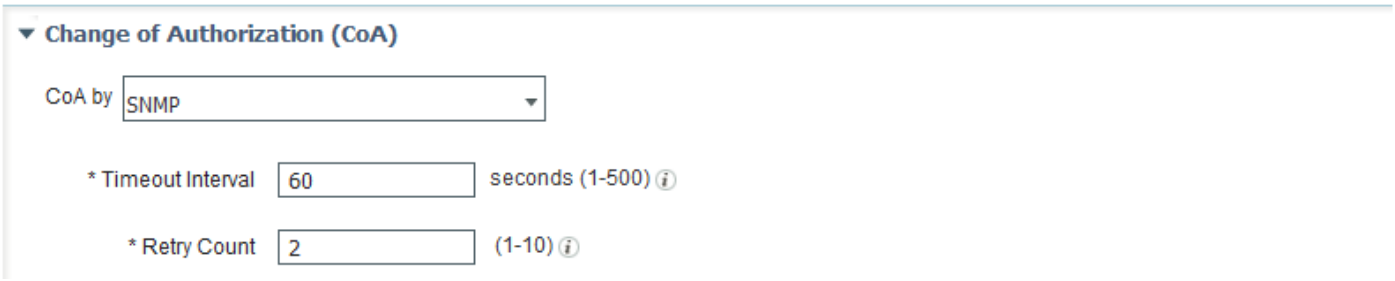
Para configurar los parámetros de SNMP CoA para un perfil de dispositivo de red, navegue hasta **Administration> Network Resources> Network Device Profiles .**

Seleccione el perfil del dispositivo de red para el cual debe configurarse SNMP CoA y expanda la pestaña **Cambio de autorización** como se muestra en la imagen.

Nota: No se puede editar la configuración SNMP de los perfiles de dispositivo de red predeterminados.



Seleccione el tipo CoA como **SNMP** y edite los parámetros SNMP Timeout y Retry. Estos parámetros se pueden establecer según los requisitos. En esta imagen se muestra un ejemplo.

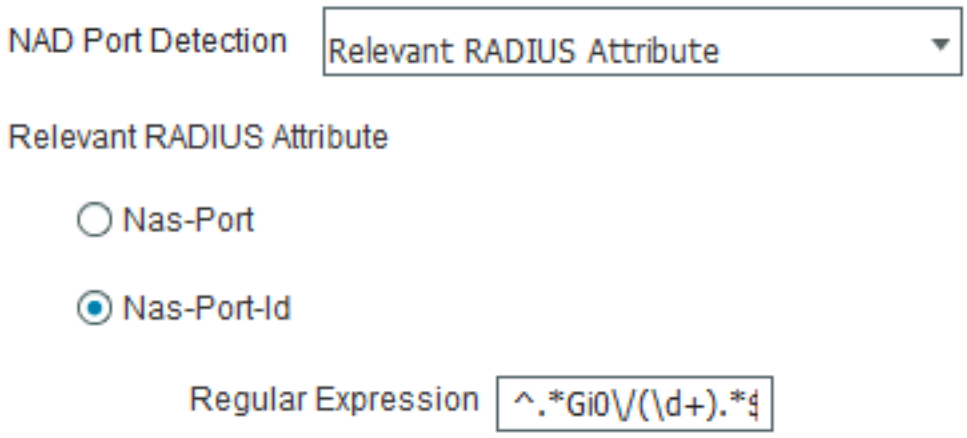


Ahora, configure el método NAD Port Detection mediante el cual ISE conocería el puerto para el que se deben establecer los OID. Hasta ahora, el único método disponible es recuperar esa información del atributo RADIUS relevante de la información de contabilidad.

Los atributos RADIUS disponibles actuales que proporcionan dicha información son NAS-Port y NAS-Port-Id. Cualquiera de ellos se puede elegir en función del atributo soportado por el NAD. La mayoría de los NAD soportan NAS-Port-Id. Los diferentes proveedores tienen diferentes maneras de representar las interfaces disponibles en el NAD. Es posible que no sea posible una forma estándar de extraer la información. Por lo tanto, las expresiones regulares se utilizan en ISE para personalizar las cadenas que se van a hacer coincidir con el valor del atributo NAS-Port-Id. Aquí se da un ejemplo para hacer coincidir los puertos que se encuentran en la forma de Gi0/x.

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

Esta expresión significa esencialmente que (^)el patrón de inicio (.*)coincide con cualquier número de instancias de cualquier carácter (Gi0)coincide con 'Gi0' (\/)coincidencia '/' (\d+)coincide con una o más instancias de cualquier dígito (.)coincidencia con cualquier carácter (*) (.*)coincidencia con cualquier número de instancias de cualquier patrón de fin de carácter ($). Este ejemplo se puede configurar como se muestra en esta imagen.



OID compatibles con ISE

De forma predeterminada, ISE proporciona opciones para configurar tres tipos de OID para realizar una operación en los puertos identificados por el valor del atributo NAS-Port-Id.

1. Reautenticar

2. Rebote de puerto

3. Port Shutdown

Reautenticar

Es posible que la mayoría de los proveedores no admita la reautenticación de OID en las MIB estándar. La información de este OID puede variar de proveedor a proveedor.

> **Nota:** Esta opción se proporciona para una posible mejora futura si cualquier dispositivo comienza a soportar un OID para administrar sesiones de usuario basadas en la dirección MAC.

Rebote de puerto

El rebote de puerto utiliza un OID operacional de puerto que tiene dos valores, uno para apagar el puerto y el otro para descerrar el puerto. Se trata de OID estándar que utilizan la mayoría de los proveedores.

1.3.6.1.2.1.2.2.1.7.$port es el OID

Si el valor se establece en 2, el puerto se apaga y si el valor se establece en 1, el puerto se desconecta.

Port Shutdown

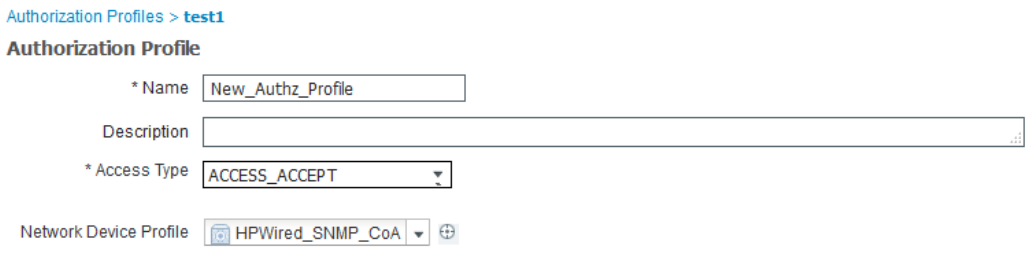
Seleccione la operación deseada que se debe realizar en ese puerto específico como se muestra en la imagen.

> **Precaución:** El orden en el que se envían los valores OID es muy importante. Porque, el orden en el que se configuran los valores OID es el orden en el que se realizan las operaciones en el puerto. Si se configuran en un orden inverso, digamos 1 y luego 2, un puerto se descerraría primero y luego se apagaría, lo que esencialmente está cerrando el puerto.

Envíe los cambios al perfil del dispositivo.

Este perfil de dispositivo se puede utilizar en cualquier perfil de autorización que se tenga en cuenta. Cualquier operación de CoA que deba realizarse para un punto final se enviará como petición de configuración SNMP al switch con los OID configurados para configurarse en el puerto en el que está conectado el punto final. Este es un ejemplo para configurar el perfil NAD en el perfil de autorización.

Para crear una nueva política de autorización o editar la que ya existe, navegue hasta **Política > Elementos de política > Resultados > Autorización > Perfiles de autorización** como se muestra en la imagen.



> **Nota:** El switch debe configurarse con ISE como servidor SNMP y debe utilizar la misma cadena de comunidad configurada en ISE. La configuración del switch está fuera del alcance de este documento.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.