Configuración de Radius y Autenticación de Usuario Basada en TACACS

Contenido

Introducción

Este documento describe cómo configurar la autenticación de usuarios y la autorización basadas en Radius y TACACS para vEdge y los controladores con ISE.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Para la demostración, se utiliza ISE versión 2.6. vEdge-cloud y controladores que ejecutan 19.2.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

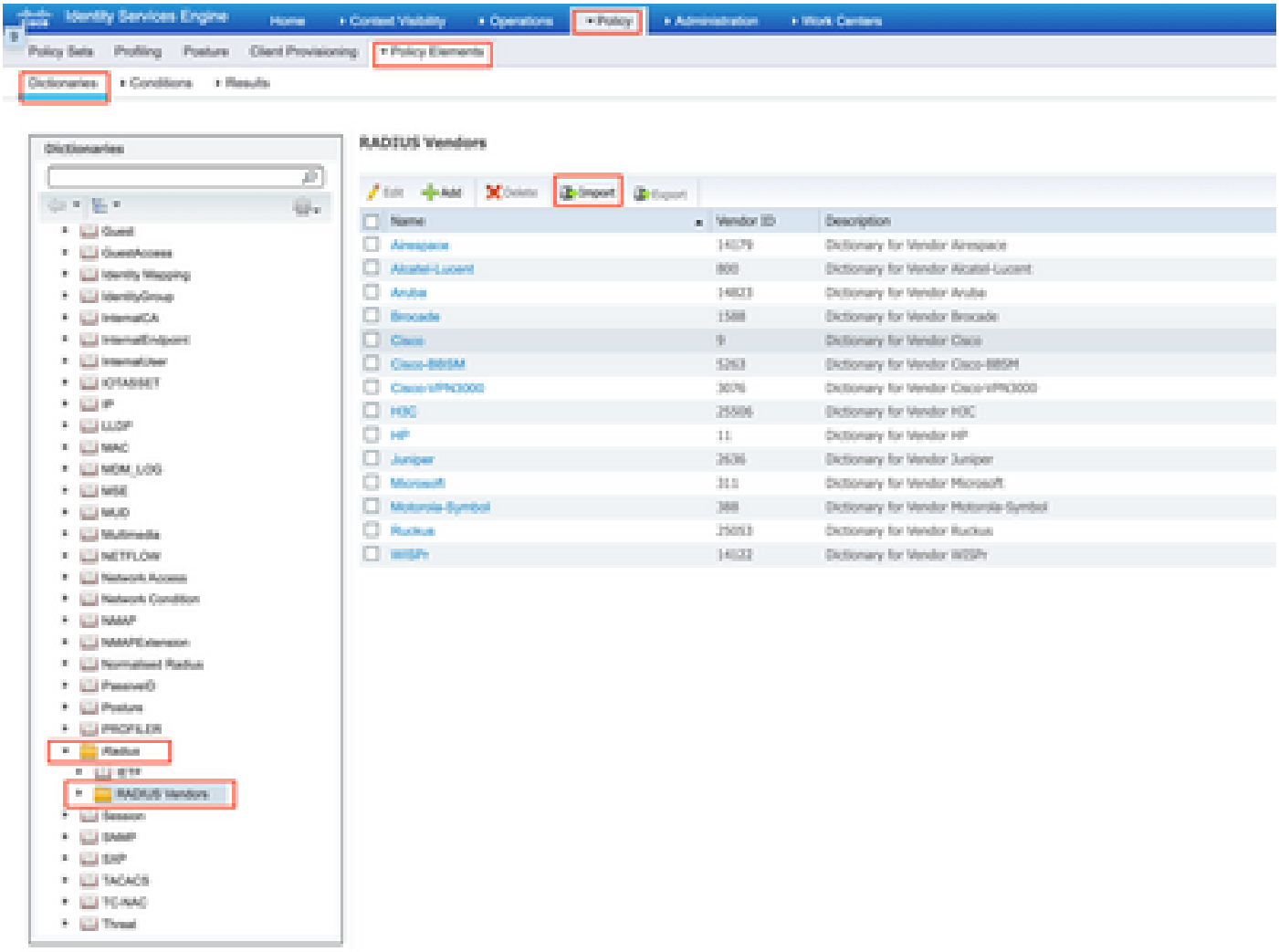
El software Viptela proporciona tres nombres de grupos de usuarios fijos: basic, netadmin y operator. Debe asignar el usuario al menos a un grupo. El usuario TACACS/Radius predeterminado se coloca automáticamente en el grupo básico.

Autenticación de usuario y autorización basadas en Radius para vEdge y controladores

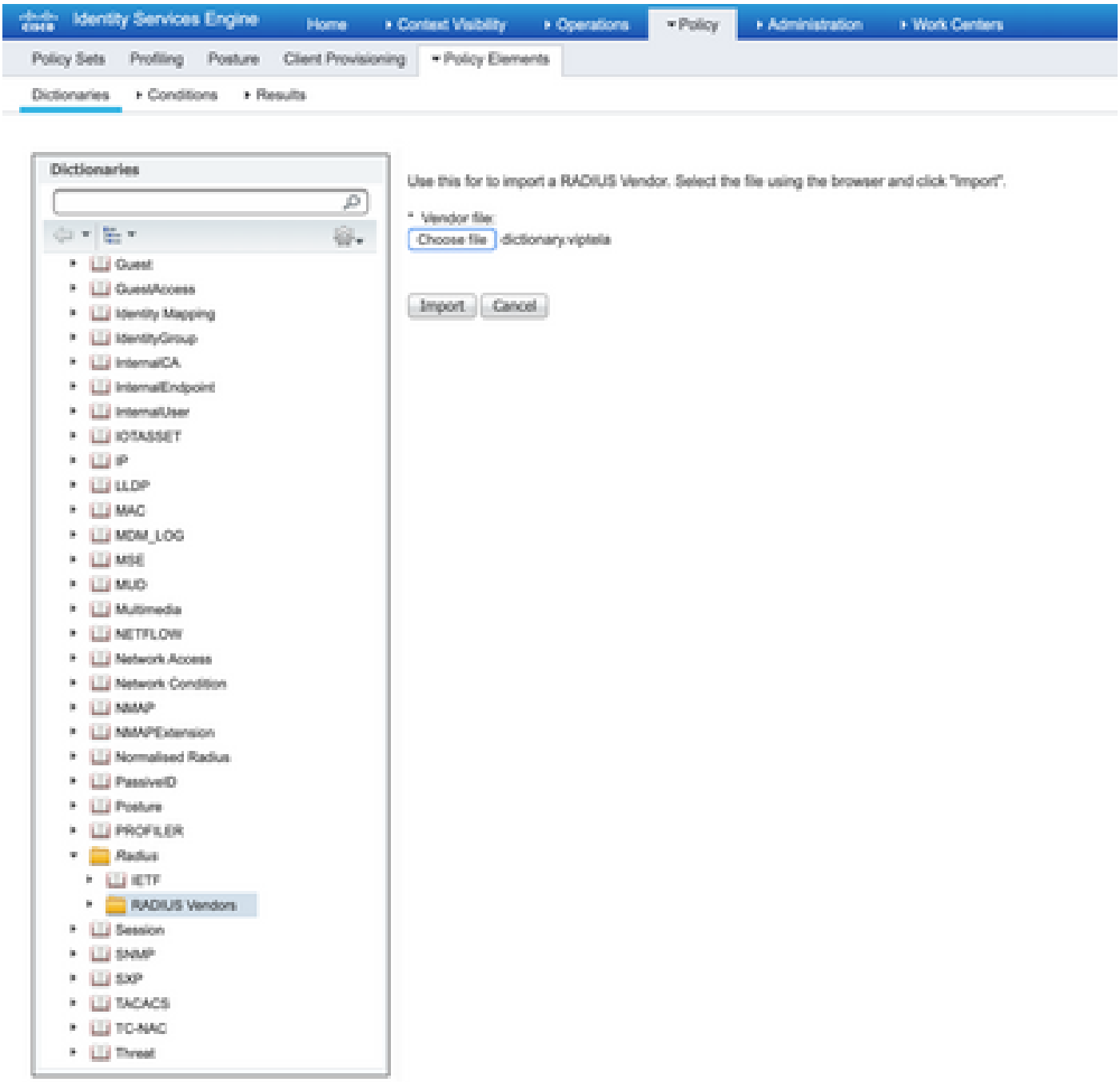
Paso 1. Cree un diccionario Viptela radius para ISE. Para ello, cree un archivo de texto con el contenido:

```
# -*- text -*-
#
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

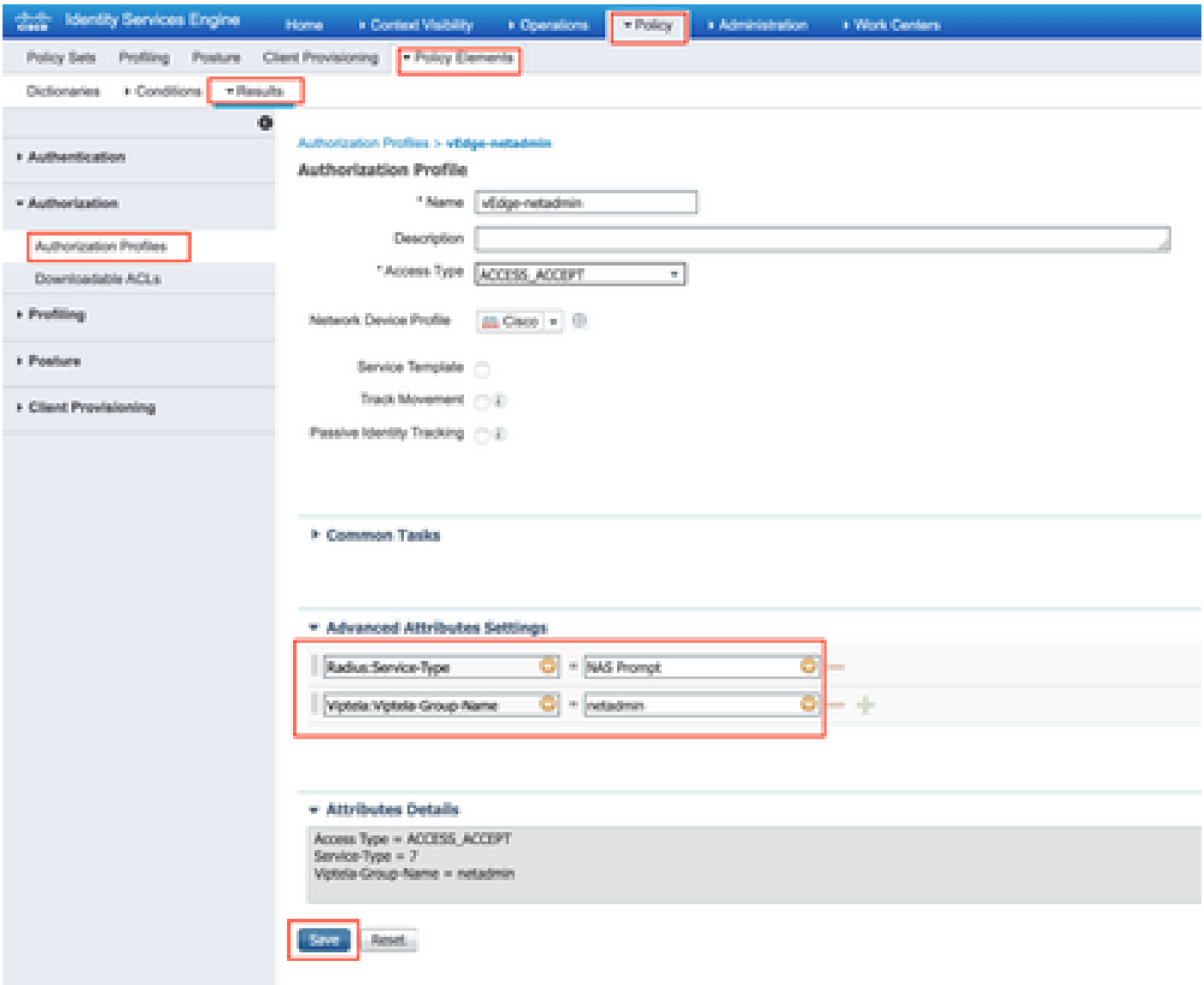
Paso 2. Cargue el diccionario en ISE. Para esto, navegue hasta Política > Elementos de Política > Diccionarios. En la lista de diccionarios, navegue hasta Radius > Radius Vendors y luego haga clic en Import como se muestra.



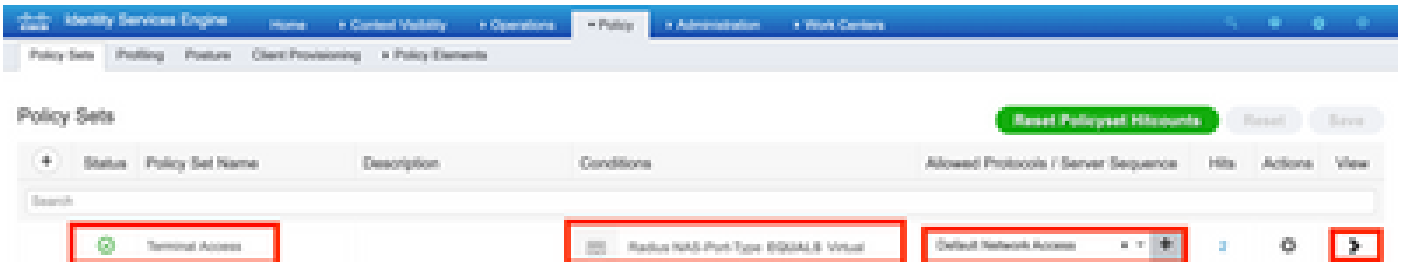
Cargue el archivo creado en el paso 1.



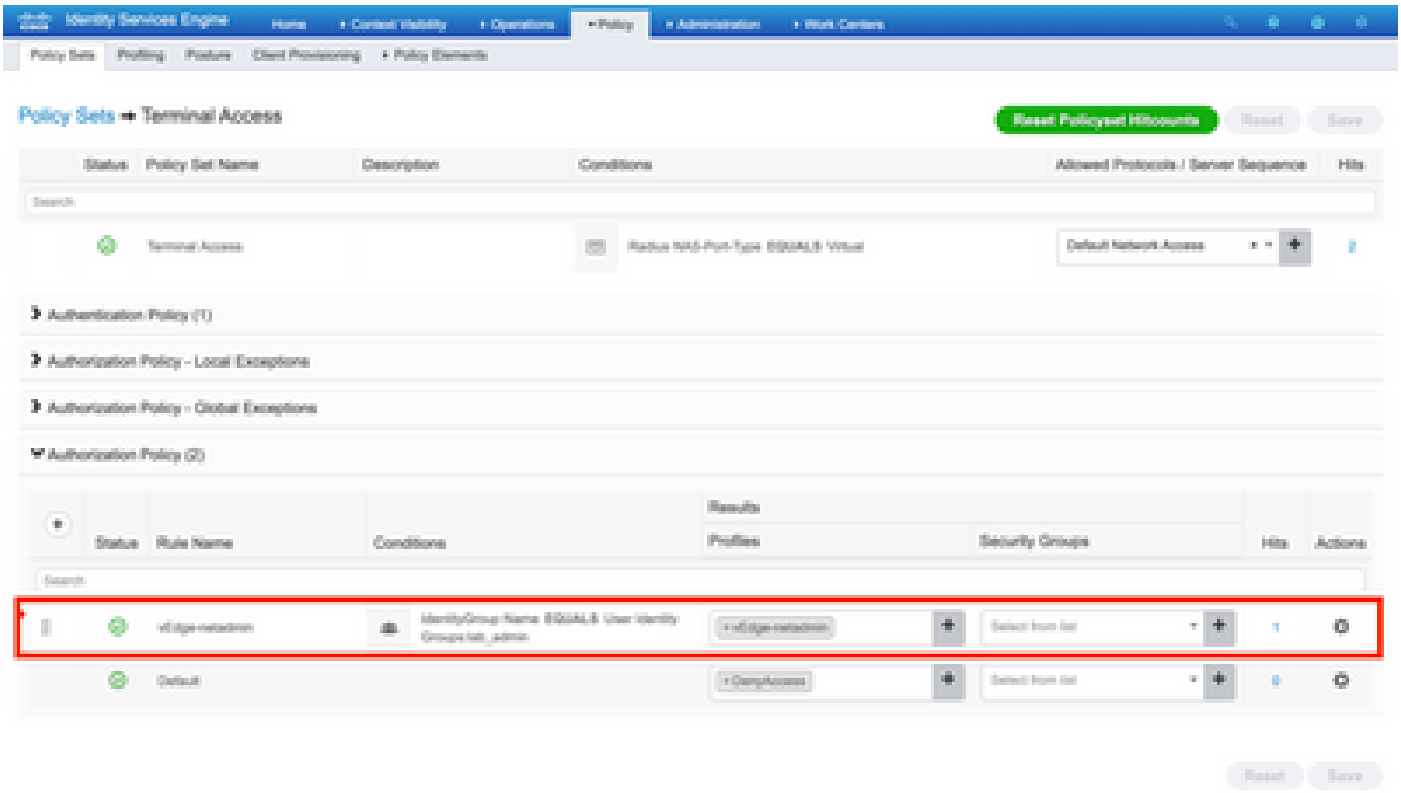
Paso 3. Cree un perfil de autorización. En este paso, el perfil de autorización de Radius asigna, por ejemplo, el nivel de privilegio netadmin a un usuario autenticado. Para esto, navegue hasta Policy > Policy Elements > Authorization Profiles y especifique dos atributos avanzados como se muestra en la imagen.



Paso 4. Dependiendo de su configuración real, su conjunto de políticas puede tener un aspecto diferente. Para la demostración de este artículo, se crea la entrada de política llamada Terminal Access como se muestra en la imagen.

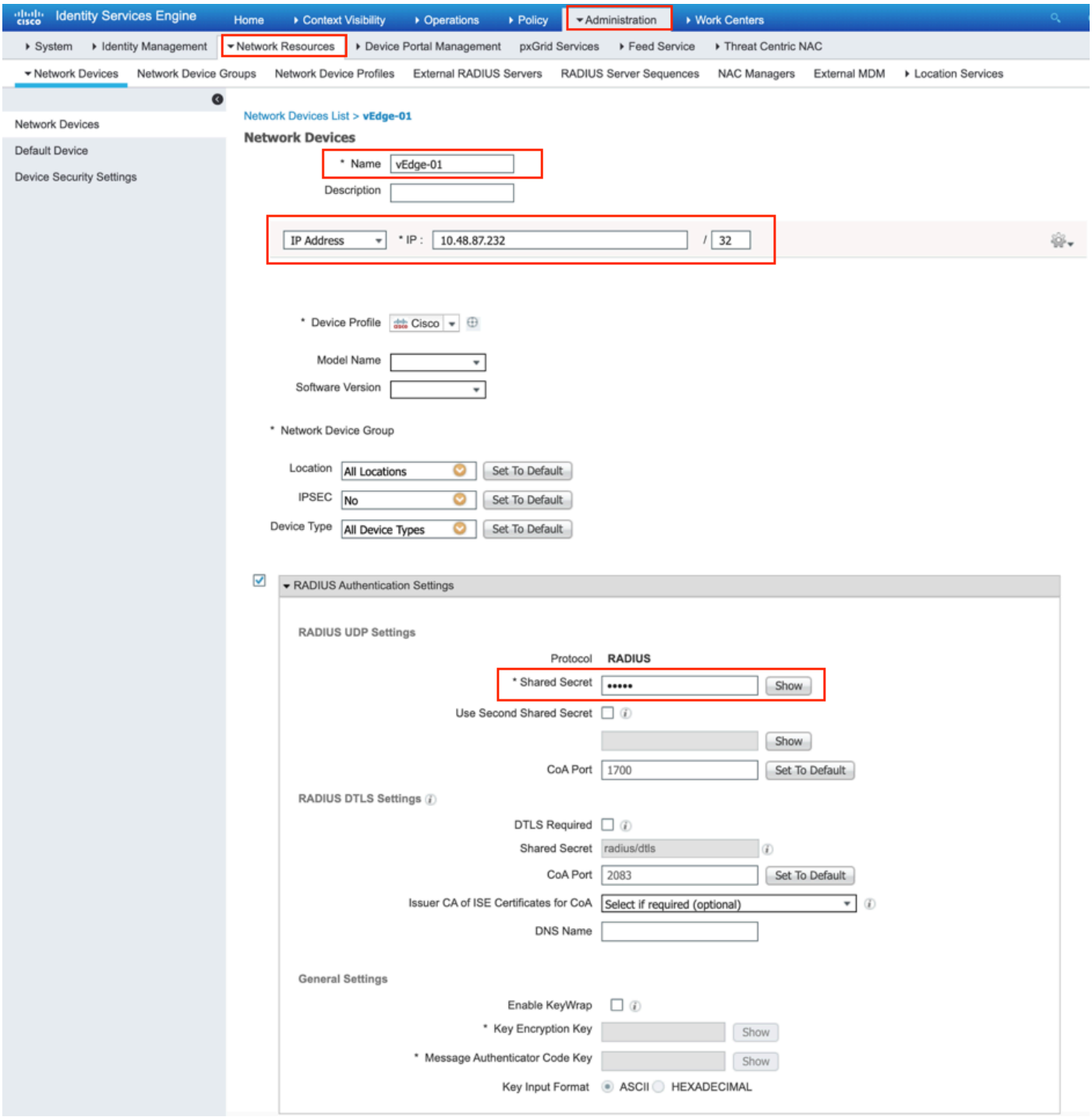


Haga clic en > y aparecerá la siguiente pantalla como se muestra en la imagen.



Esta política coincide según el grupo de usuarios lab_admin y asigna un perfil de autorización que se creó en el paso 3.

Paso 5. Defina el NAS (router o controlador vEdge) como se muestra en la imagen.



Paso 6. Configuración de vEdge/Controller.

```
system
 aaa
  auth-order       radius local
  radius
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

Paso 7. Verificación. Inicie sesión en vEdge y asegúrese de asignar el grupo netadmin al usuario remoto.

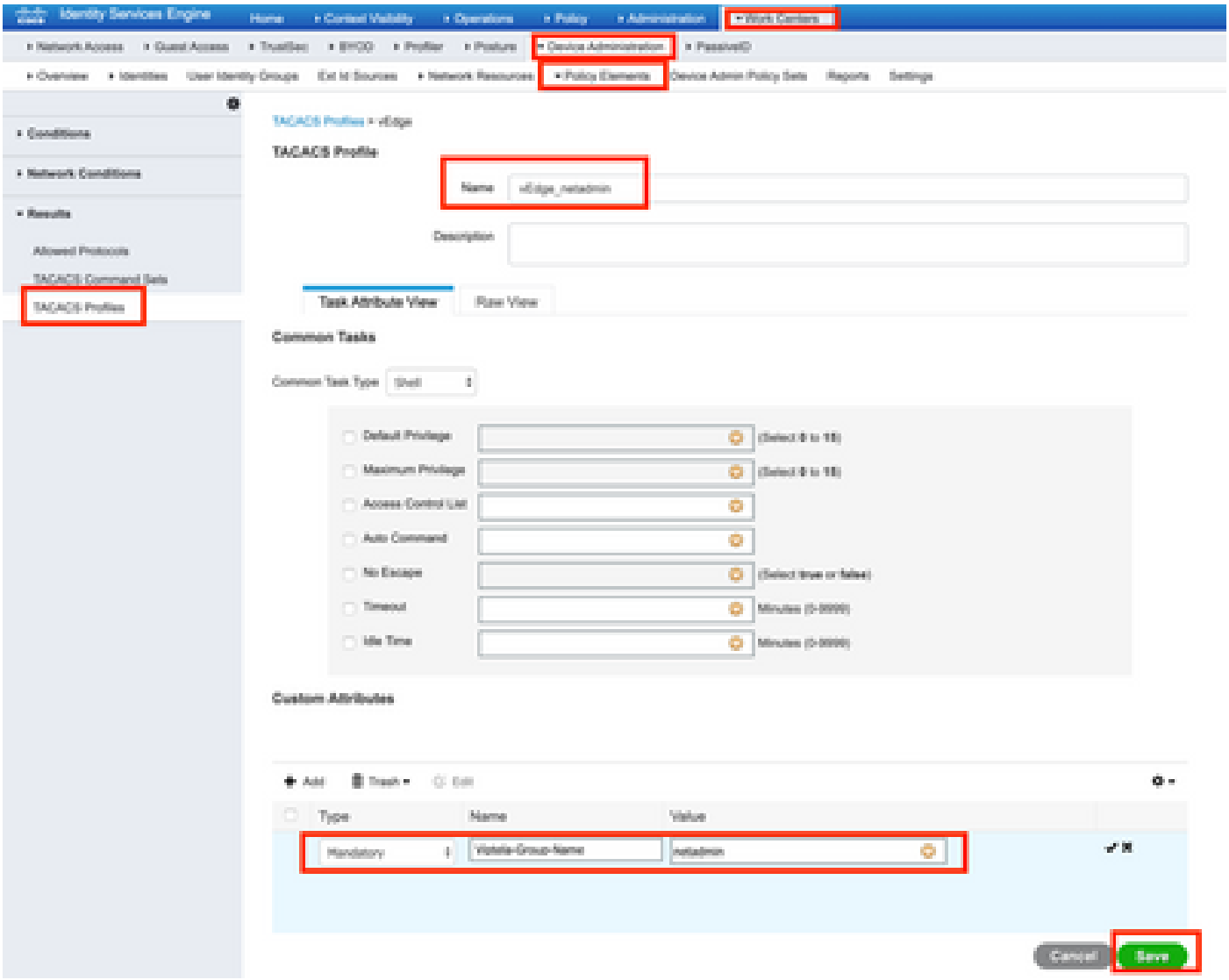
```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

Autenticación y autorización de usuarios basadas en TACACS para vEdge y controladores

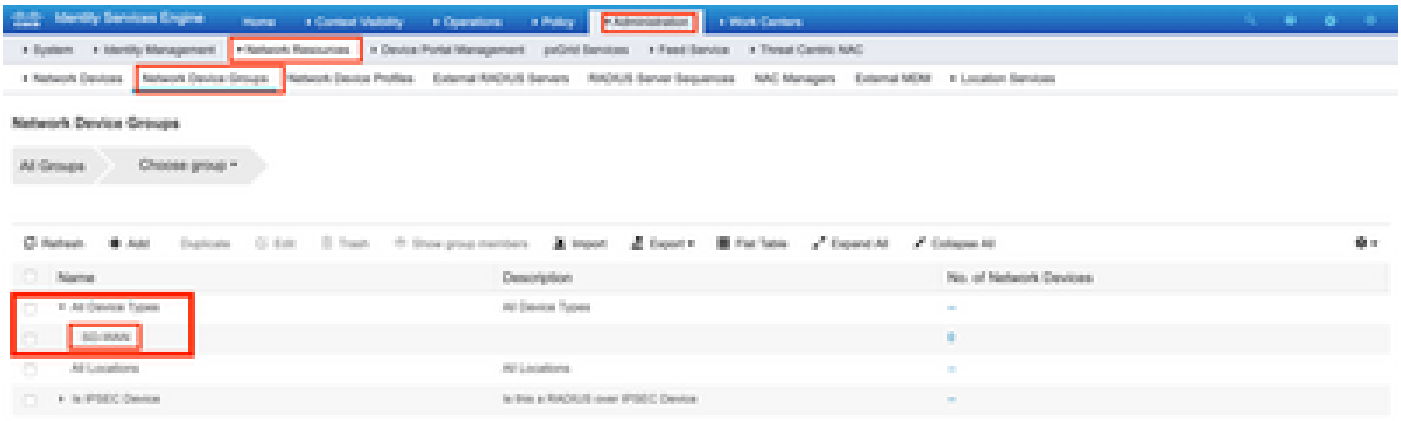
Paso 1. Cree un perfil TACACS. En este paso, el perfil TACACS creado se asigna, por ejemplo, el nivel de privilegio netadmin a un usuario autenticado.

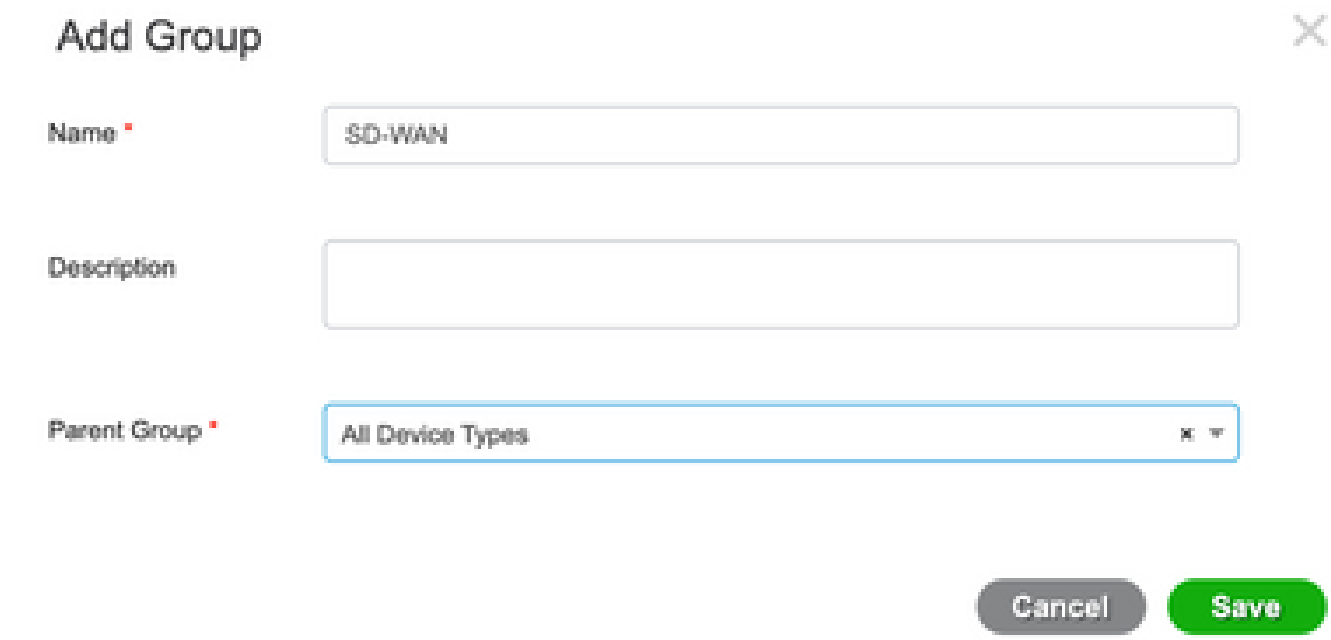
- Seleccione Obligatorio en la sección Atributo personalizado para agregar el atributo como:

Tipo	Nombre	Valor
Obligatoria	Viptela-Group-Name	netadmin

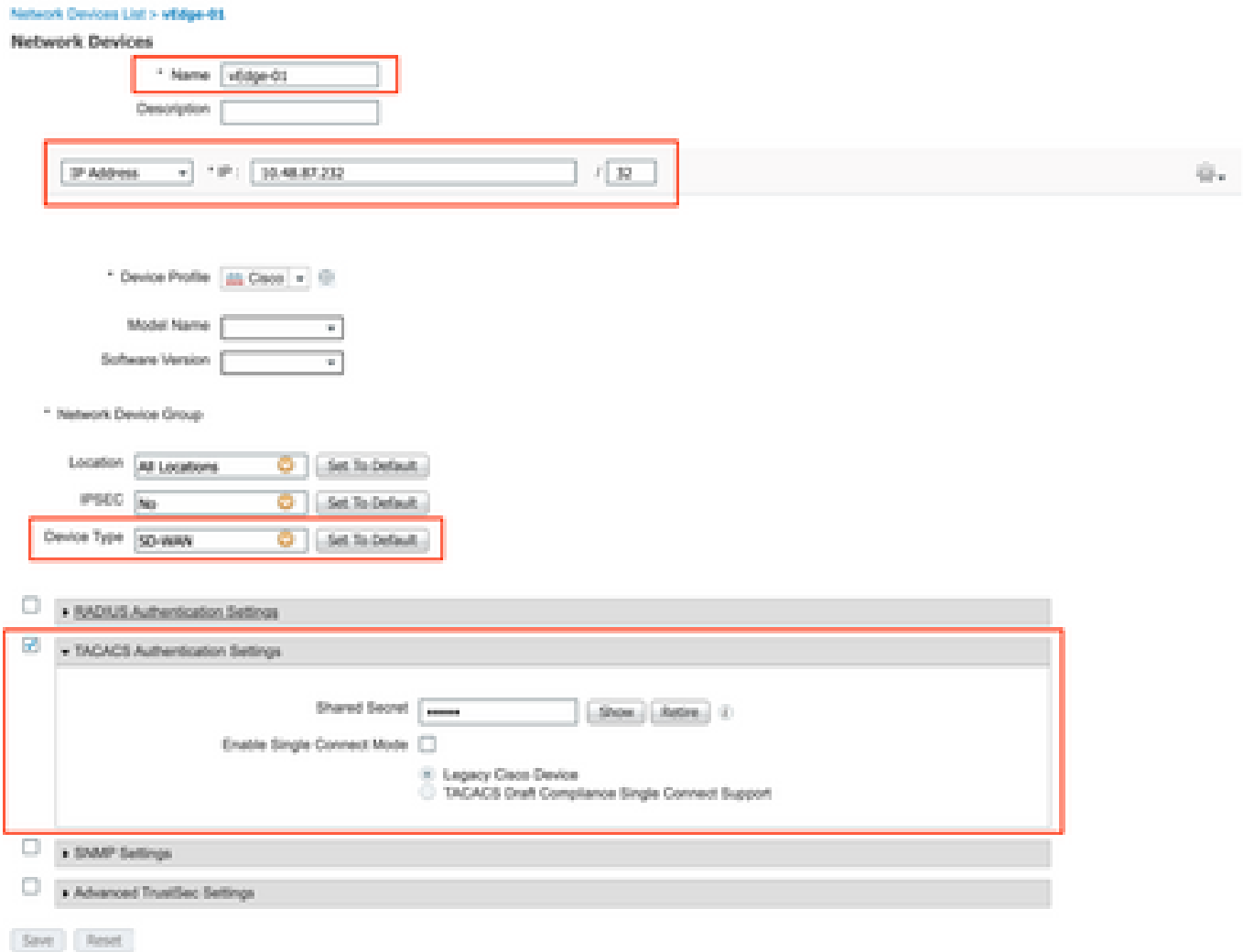


Paso 2. Cree un grupo de dispositivos para SD-WAN.



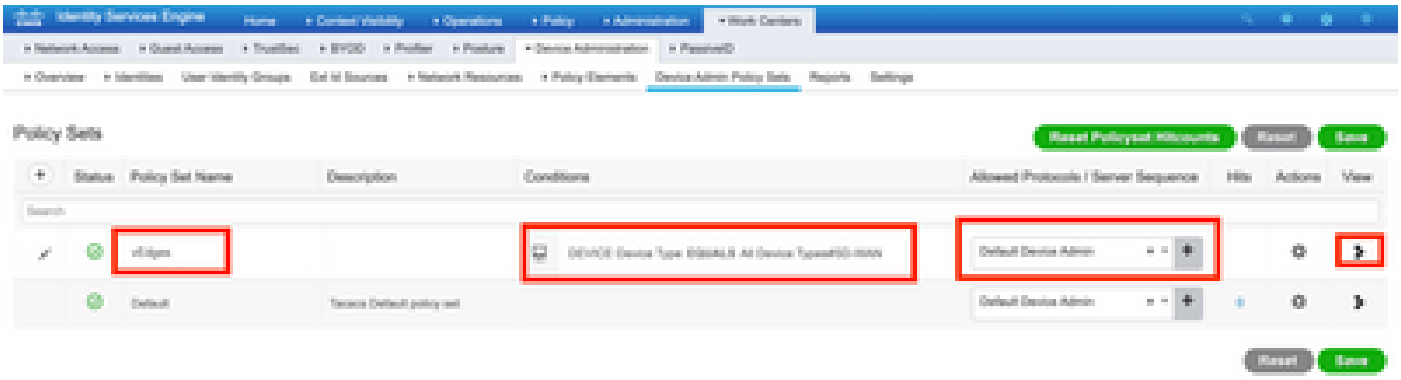


Paso 3. Configure el dispositivo y asígnelo al grupo de dispositivos SD-WAN:

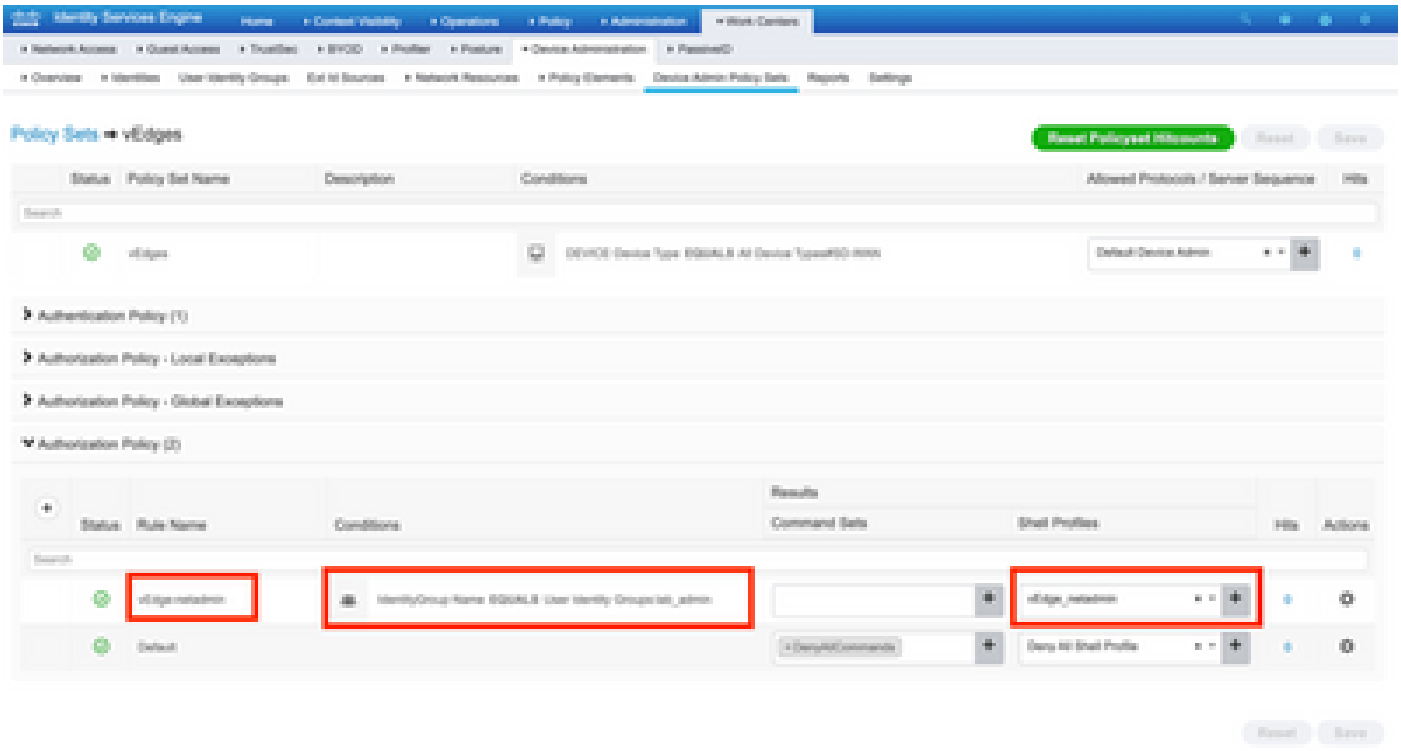


Paso 4. Defina la política de administración de dispositivos.

Dependiendo de su configuración real, su conjunto de políticas puede tener un aspecto diferente. Para la demostración de este documento, se crea la directiva.



Haga clic en > y aparecerá la siguiente pantalla como se muestra en esta imagen. Esta política coincide en función del tipo de dispositivo denominado SD-WAN y asigna el perfil de shell que se crea en el paso 1.



Paso 5. Configurar vEdge:

```
system
 aaa
  auth-order tacacs local
 !
 tacacs
  server 10.48.87.210
   vpn 512
   key cisco
  exit
 !
!
```

Paso 6. Verificación. Inicie sesión en vEdge y asegúrese de que el grupo netadmin esté asignado al usuario remoto:

```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

Información Relacionada

- Guía de implementación prescriptiva de Cisco ISE Device Administration: https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973
- Configuración del acceso y la autenticación de usuarios: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).