Configurar a autenticação de usuário baseada em Radius e TACACS

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Configurar

- Autenticação e autorização de usuário com base em Radius para vEdge e controladores
- Autenticação e autorização de usuário com base em TACACS para vEdge e controladores

Informações Relacionadas

Introdução

Este documento descreve como configurar a autenticação e autorização de usuário com base em Radius e TACACS para vEdge e controladores com ISE.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Para fins de demonstração, é usado o ISE versão 2.6. vEdge-nuvem e controladores executando 19.2.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

O software Viptela fornece três nomes de grupo de usuários fixos: basic, netadmin e operator. Você deve atribuir o usuário a pelo menos um grupo. O usuário TACACS/Radius padrão é colocado automaticamente no grupo básico.

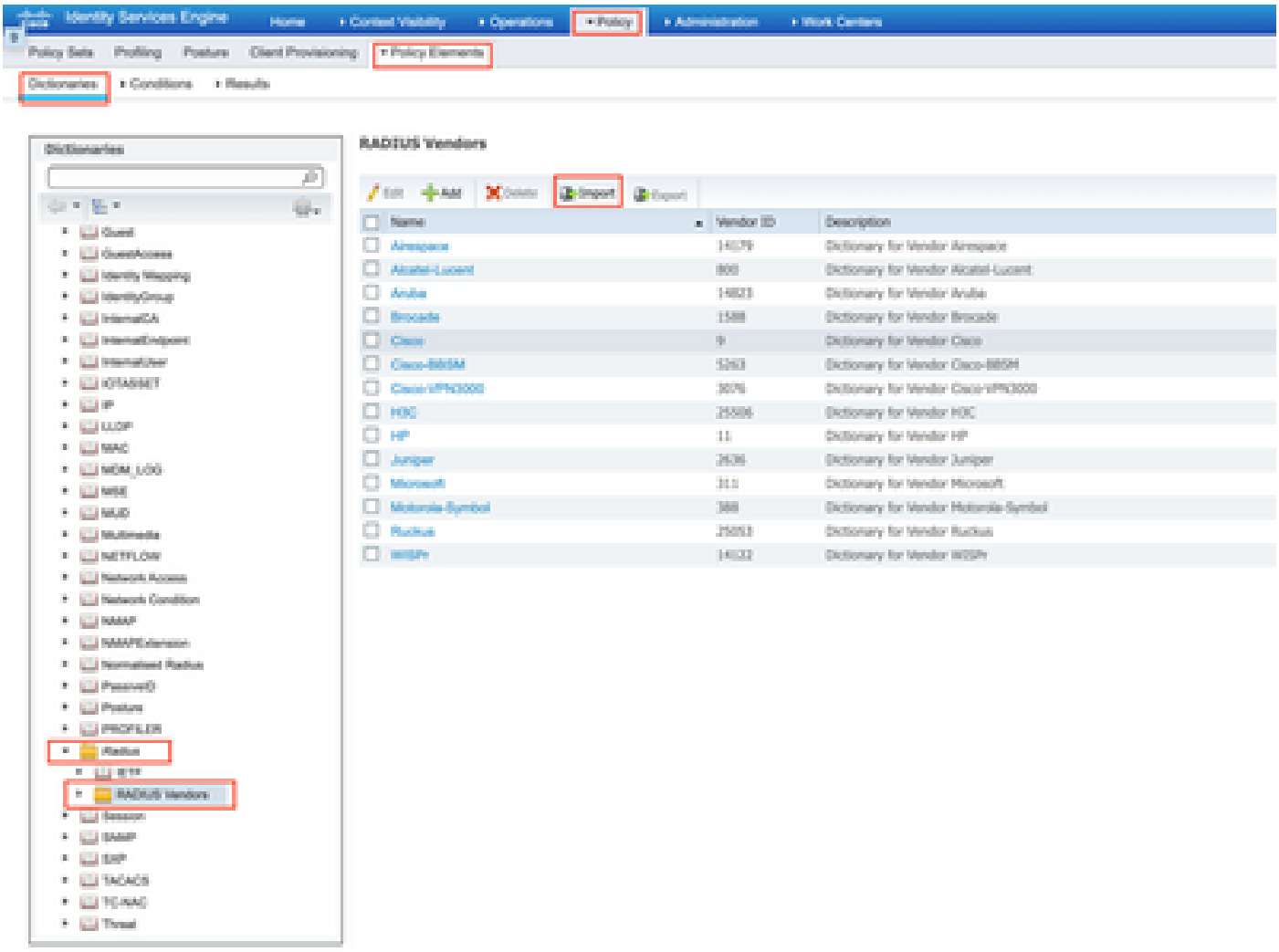
Autenticação e autorização de usuário com base em Radius para vEdge e

controladores

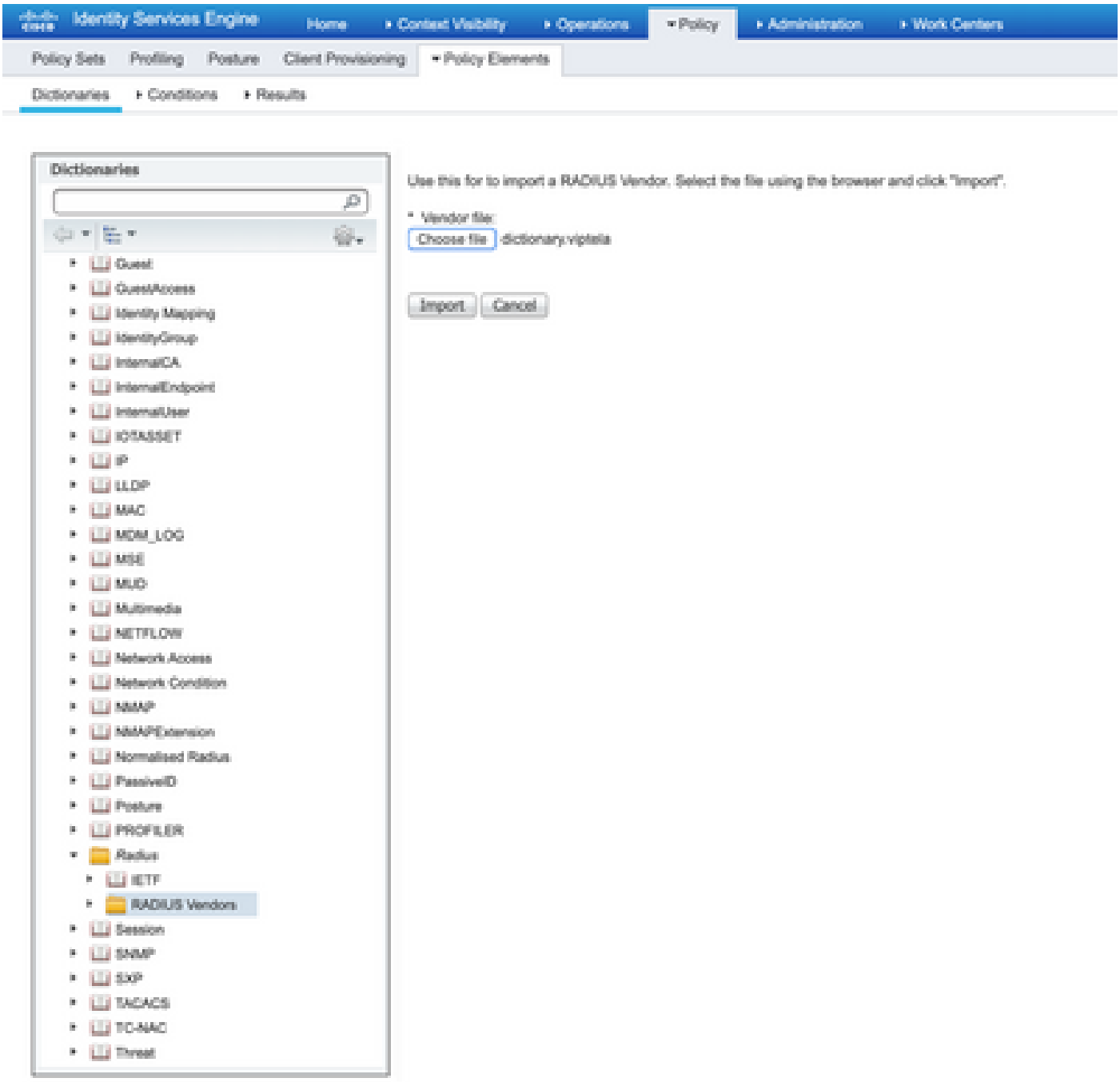
Etapa 1. Crie um dicionário do Viptela radius para o ISE. Para fazer isso, crie um arquivo de texto com o conteúdo:

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

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

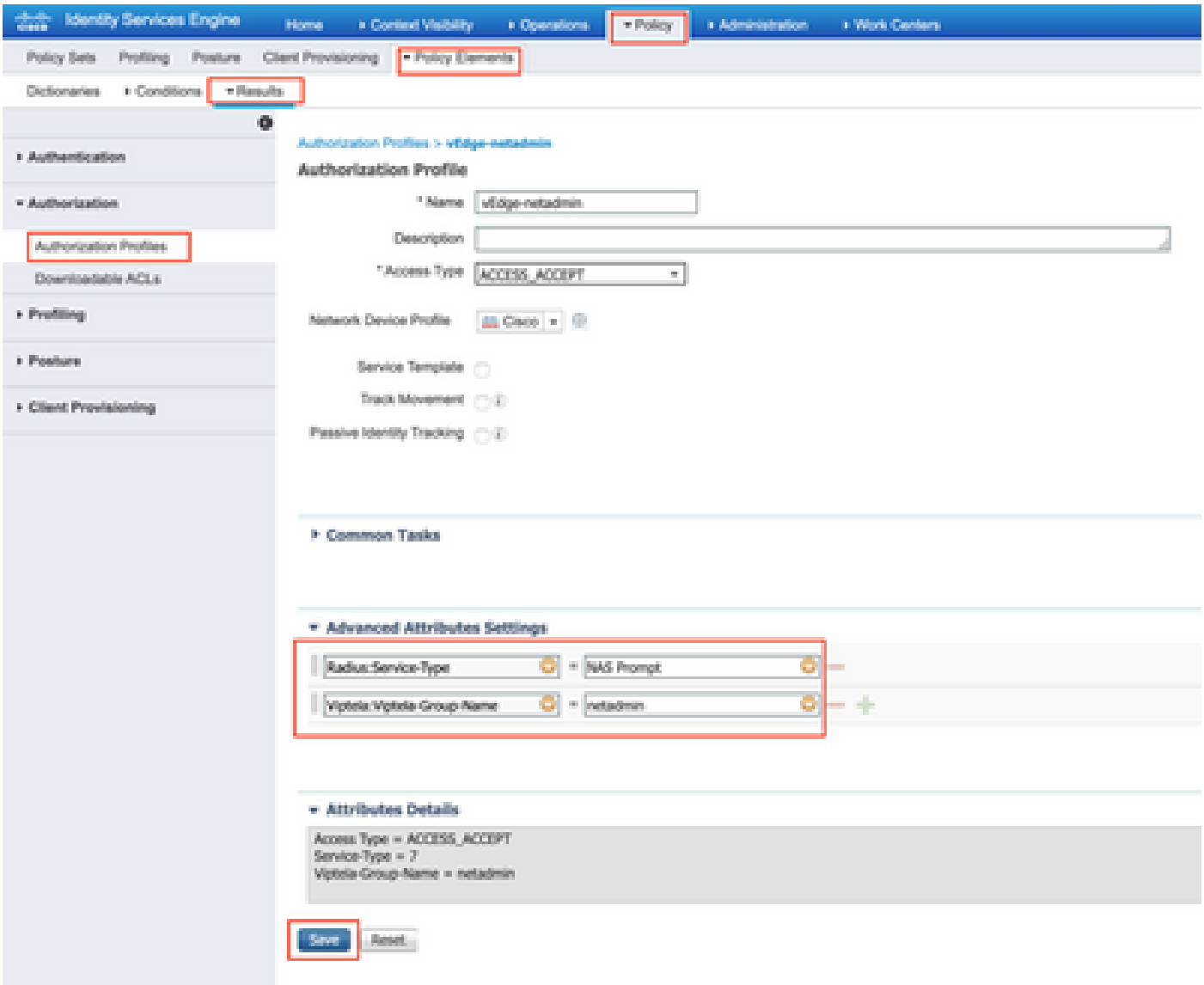
Etapa 2. Carregue o dicionário no ISE. Para isso, navegue até Política > Elementos de política > Dicionários. Na lista de dicionários, navegue até Radius > Radius Vendors e clique em Import conforme mostrado.



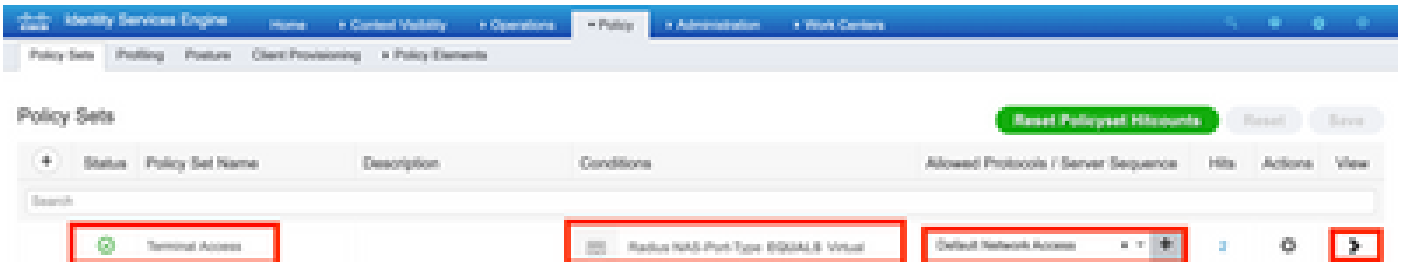
Carregue o arquivo criado na etapa 1.



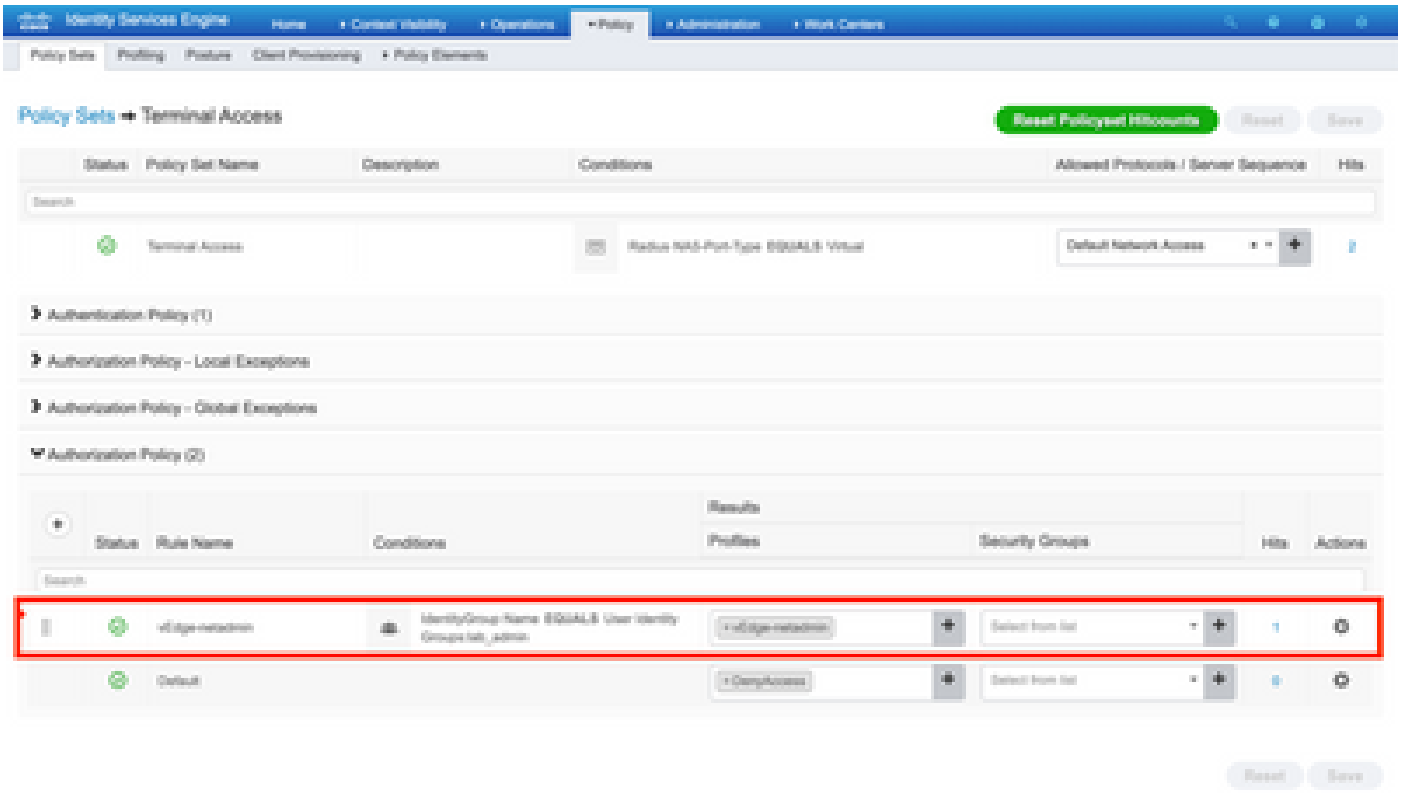
Etapa 3. Crie um perfil de autorização. Nesta etapa, o perfil de autorização Radius atribui, por exemplo, o nível de privilégio netadmin a um usuário autenticado. Para isso, navegue para Política > Elementos de política > Perfis de autorização e especifique dois atributos avançados como mostrado na imagem.



Etapa 4. Dependendo da configuração real, o seu conjunto de políticas pode ter uma aparência diferente. Para a finalidade da demonstração neste artigo, a entrada de política chamada Terminal Access é criada conforme mostrado na imagem.

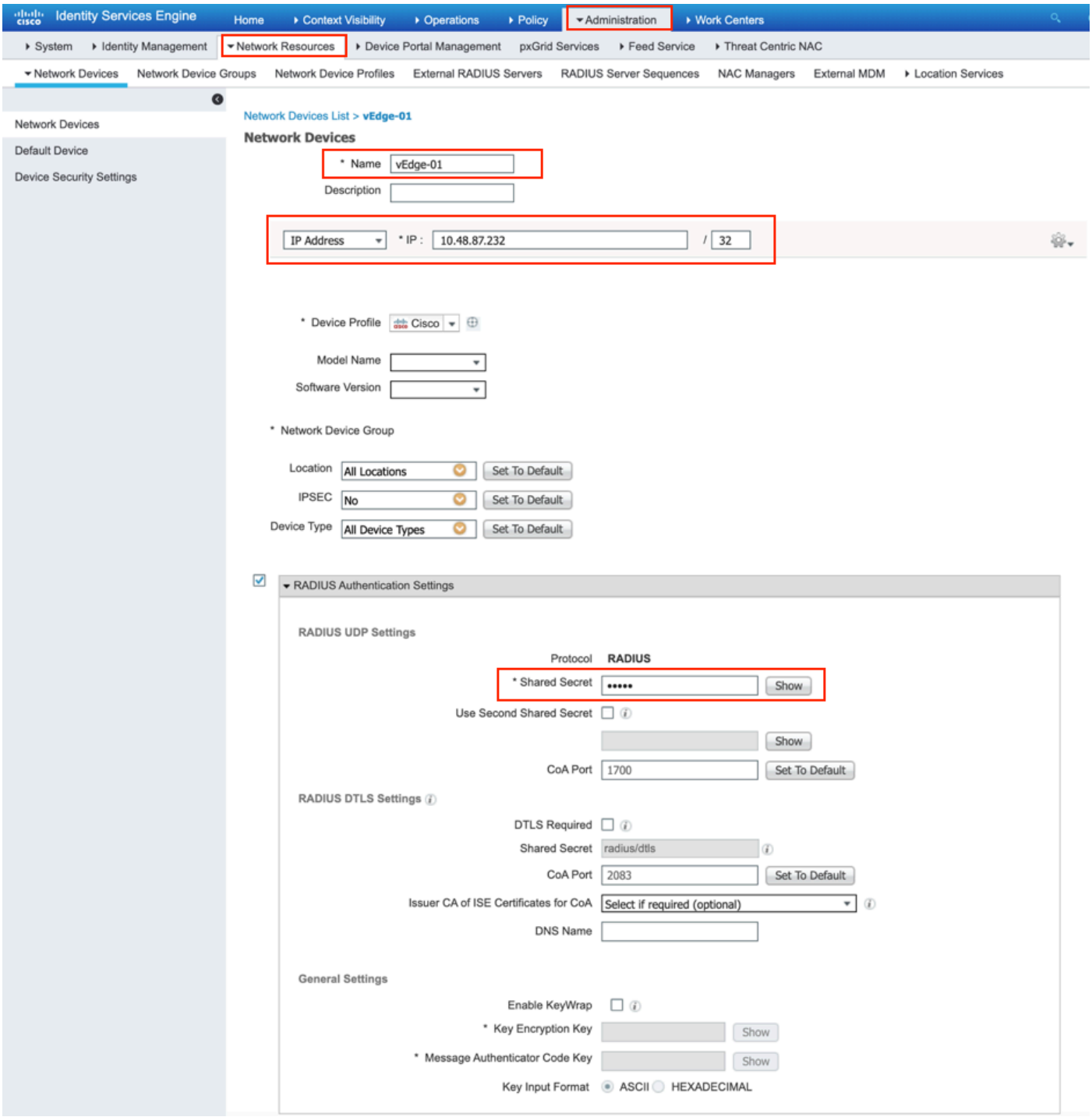


Clique em > e a próxima tela será exibida conforme mostrado na imagem.



Essa política corresponde com base no grupo de usuários lab_admin e atribui um perfil de autorização que foi criado na Etapa 3.

Etapa 5. Defina NAS (roteador ou controlador vEdge) como mostrado na imagem.



Etapa 6. Configure o vEdge/Controller.

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

Passo 7. Verificação. Faça login no vEdge e verifique se o grupo netadmin foi atribuído ao usuário remoto.

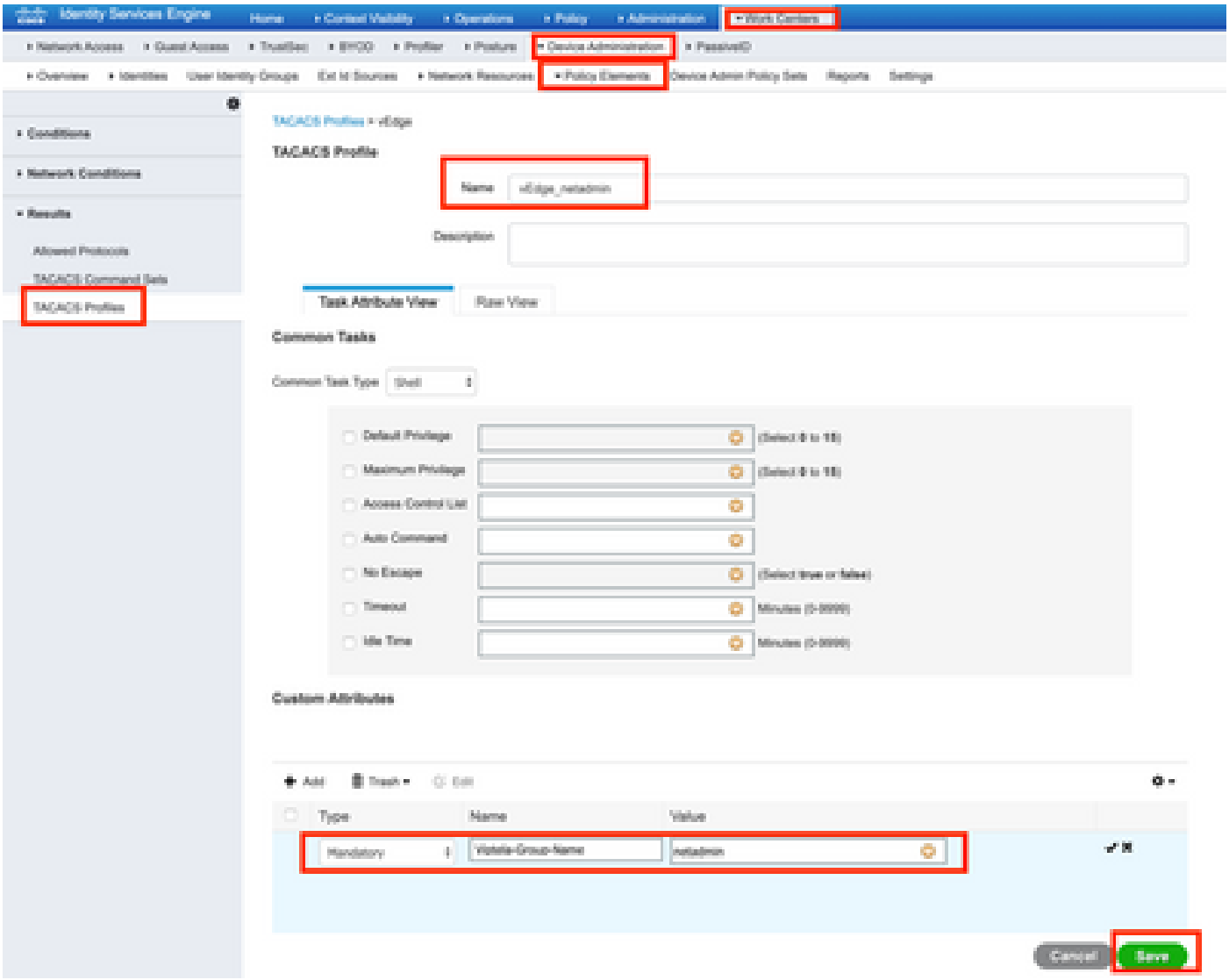
```
vEdgeCloud1# show users

                                                    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
```

Autenticação e autorização de usuário com base em TACACS para vEdge e controladores

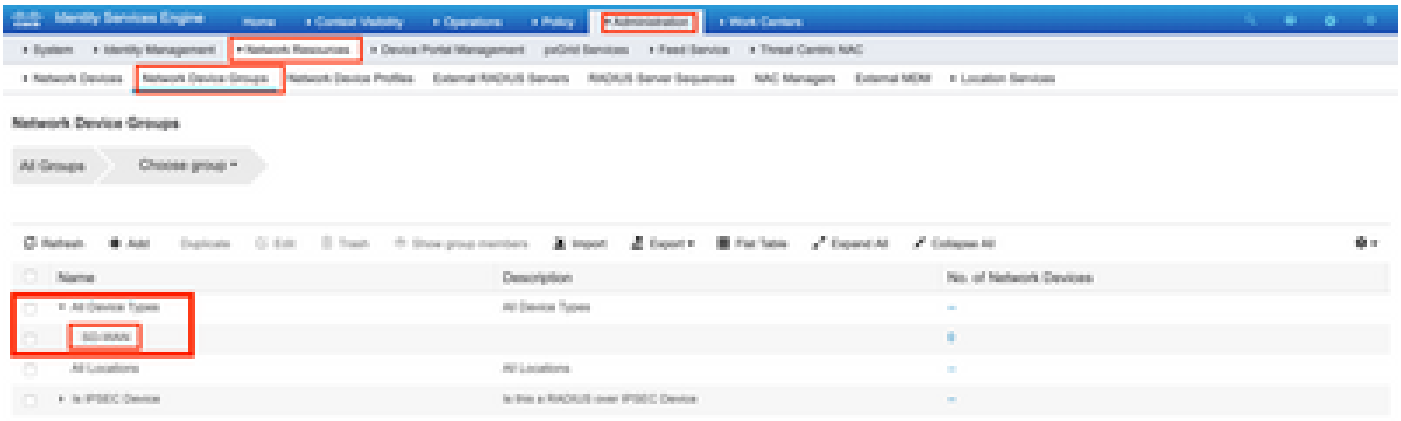
Etapa 1. Crie um perfil TACACS. Nesta etapa, o perfil TACACS criado é atribuído, por exemplo, o nível de privilégio netadmin a um usuário autenticado.

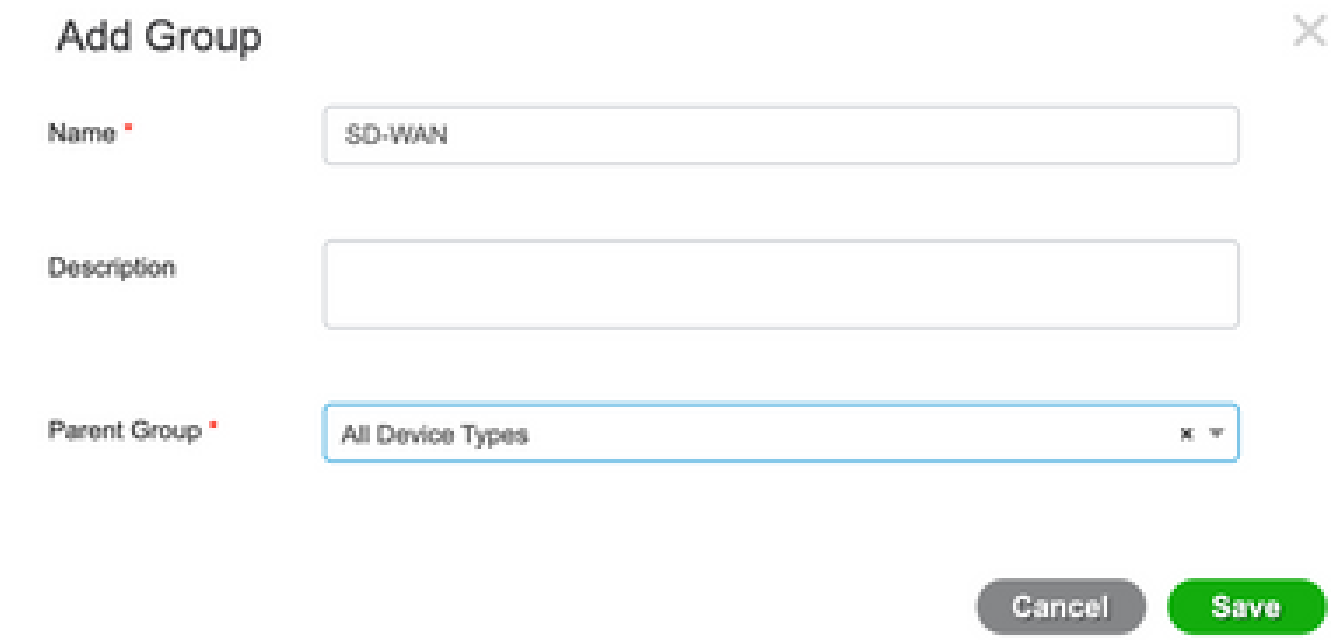
- Selecione Obrigatório na seção Atributo personalizado para adicionar o atributo como:

Tipo	Nome	Valor
Obrigatório	Viptela-Group-Name	netadmin

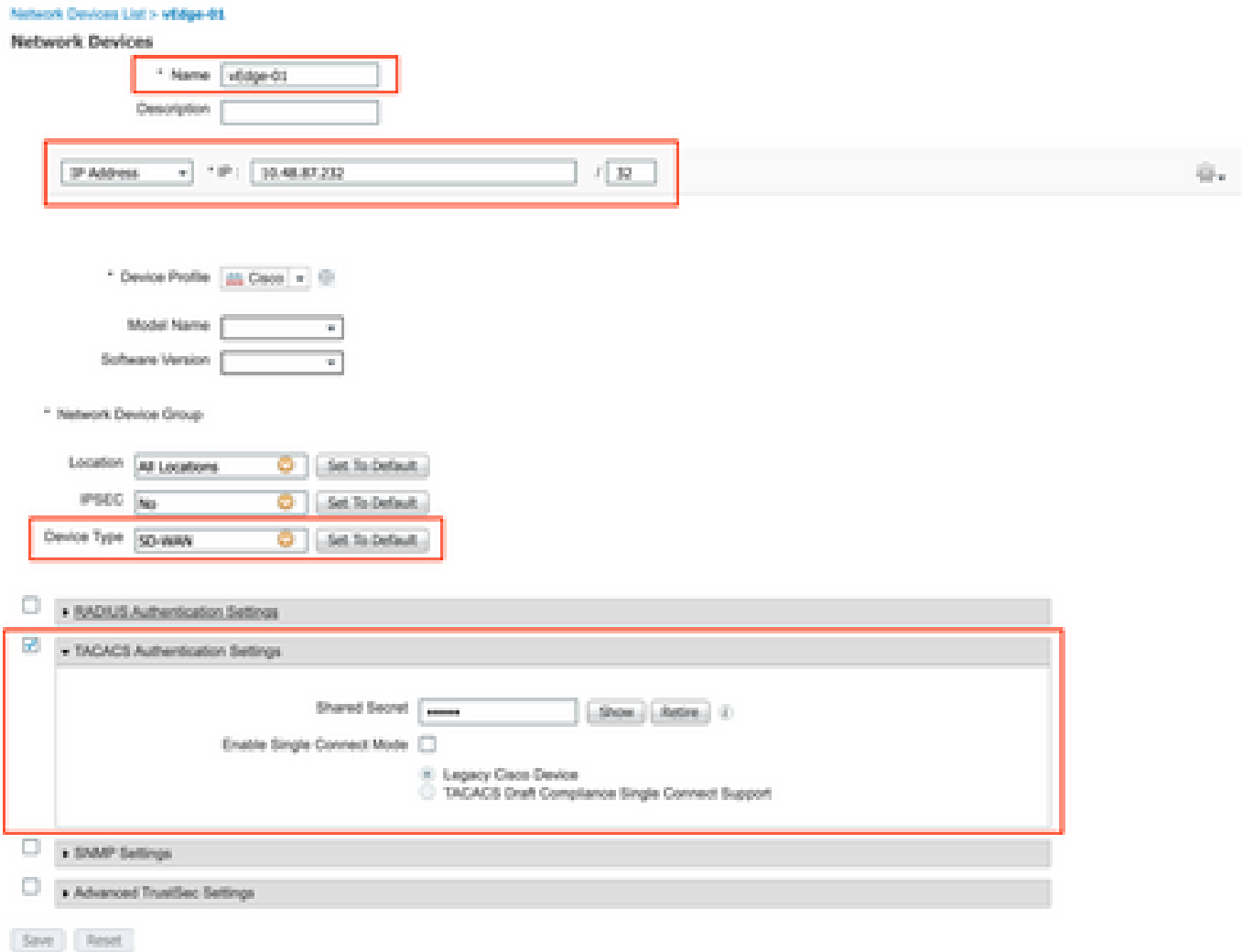


Etapa 2. Crie um grupo de dispositivos para SD-WAN.



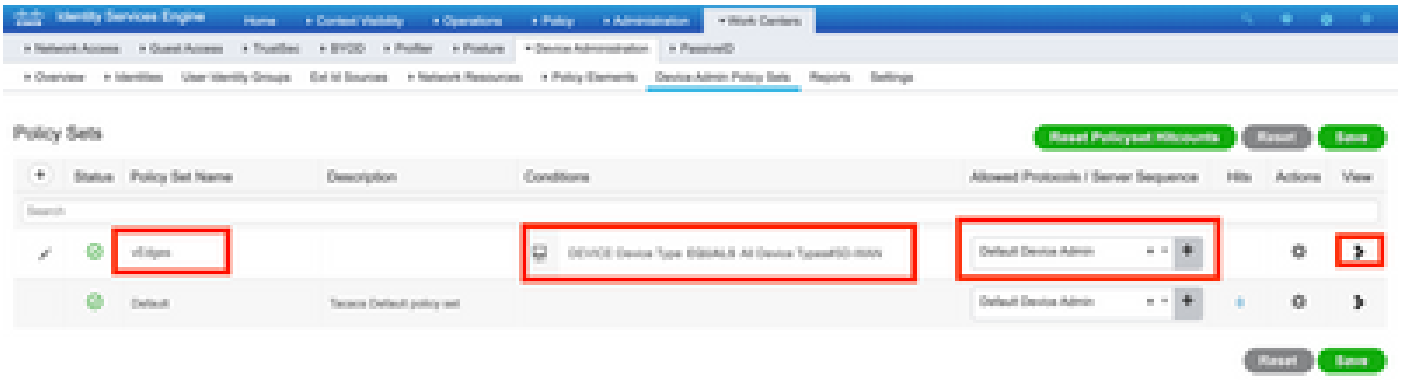


Etapa 3. Configure o dispositivo e atribua-o ao grupo de dispositivos SD-WAN:

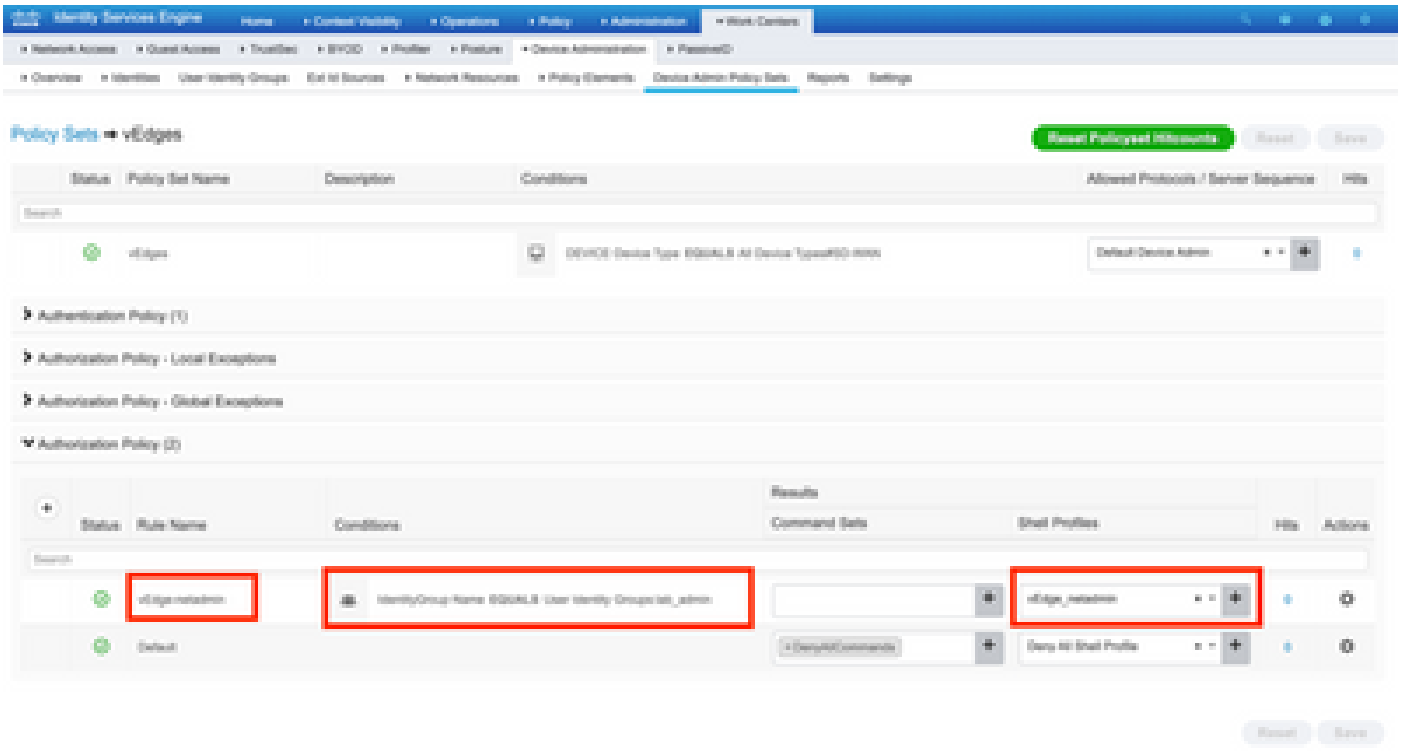


Etapa 4. Defina a Política de Administração do Dispositivo.

Dependendo da configuração real, o seu conjunto de políticas pode ter uma aparência diferente. Para a finalidade da demonstração neste documento, a Política é criada.



Clique em > e a próxima tela será exibida conforme mostrado nesta imagem. Essa política corresponde com base no tipo de dispositivo chamado SD-WAN e atribui o perfil Shell criado na etapa 1.



Etapa 5. Configurar vEdge:

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

Etapa 6. Verificação. Faça login no vEdge e verifique se o grupo netadmin foi atribuído ao usuário 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
```

Informações Relacionadas

- Guia de implantação prescritiva da administração de dispositivos do Cisco ISE: https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973
- Configuração de acesso e autenticação de usuário: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.