

Configuración de Radius y Autenticación de Usuario Basada en TACACS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Autenticación de usuario y autorización basadas en Radius para vEdge y controladores](#)

[Autenticación y autorización de usuarios basadas en TACACS para vEdge y controladores](#)

[Información Relacionada](#)

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

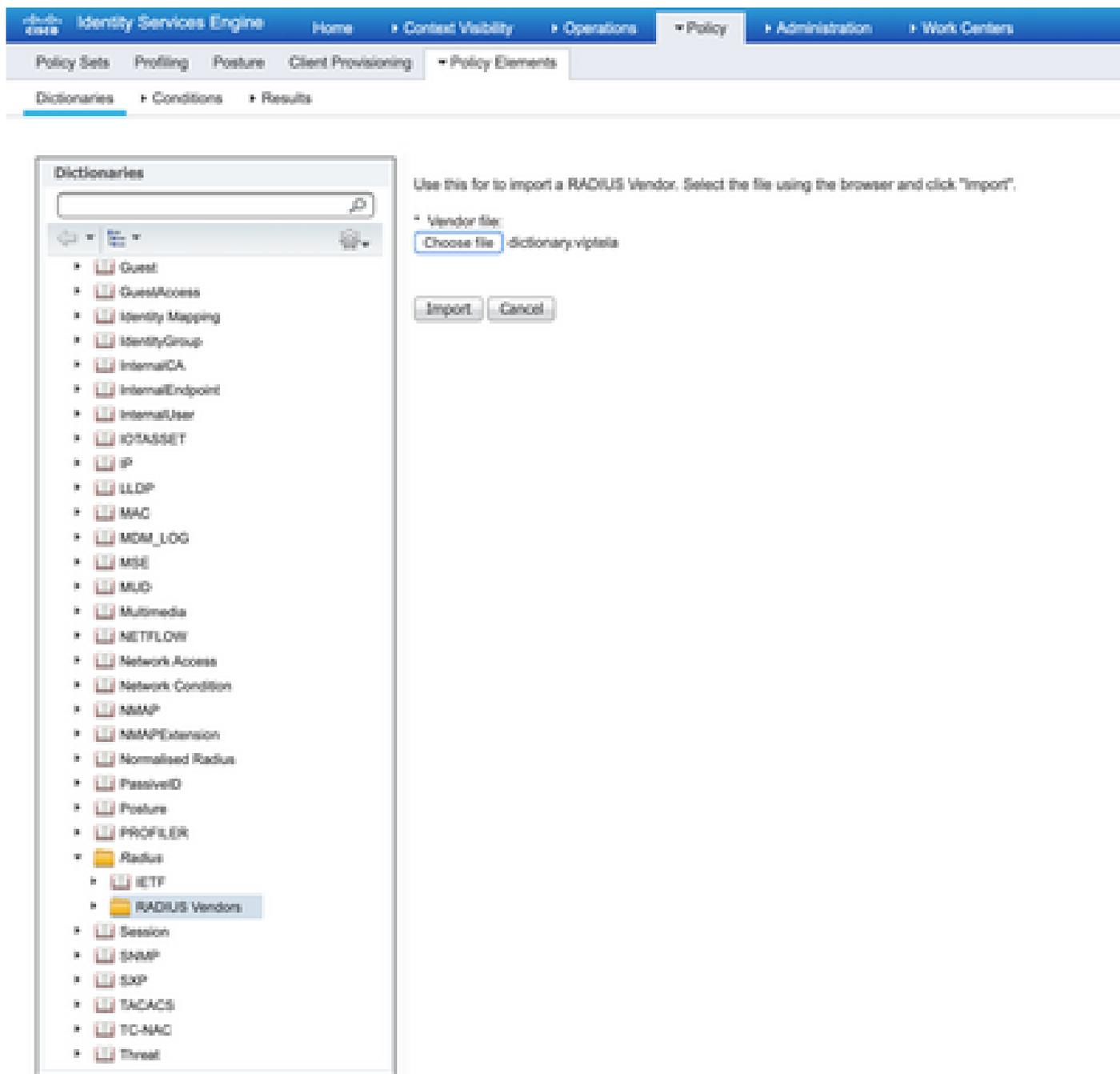
ATTRIBUTE       Viptela-Group-Name 1 string
```

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.

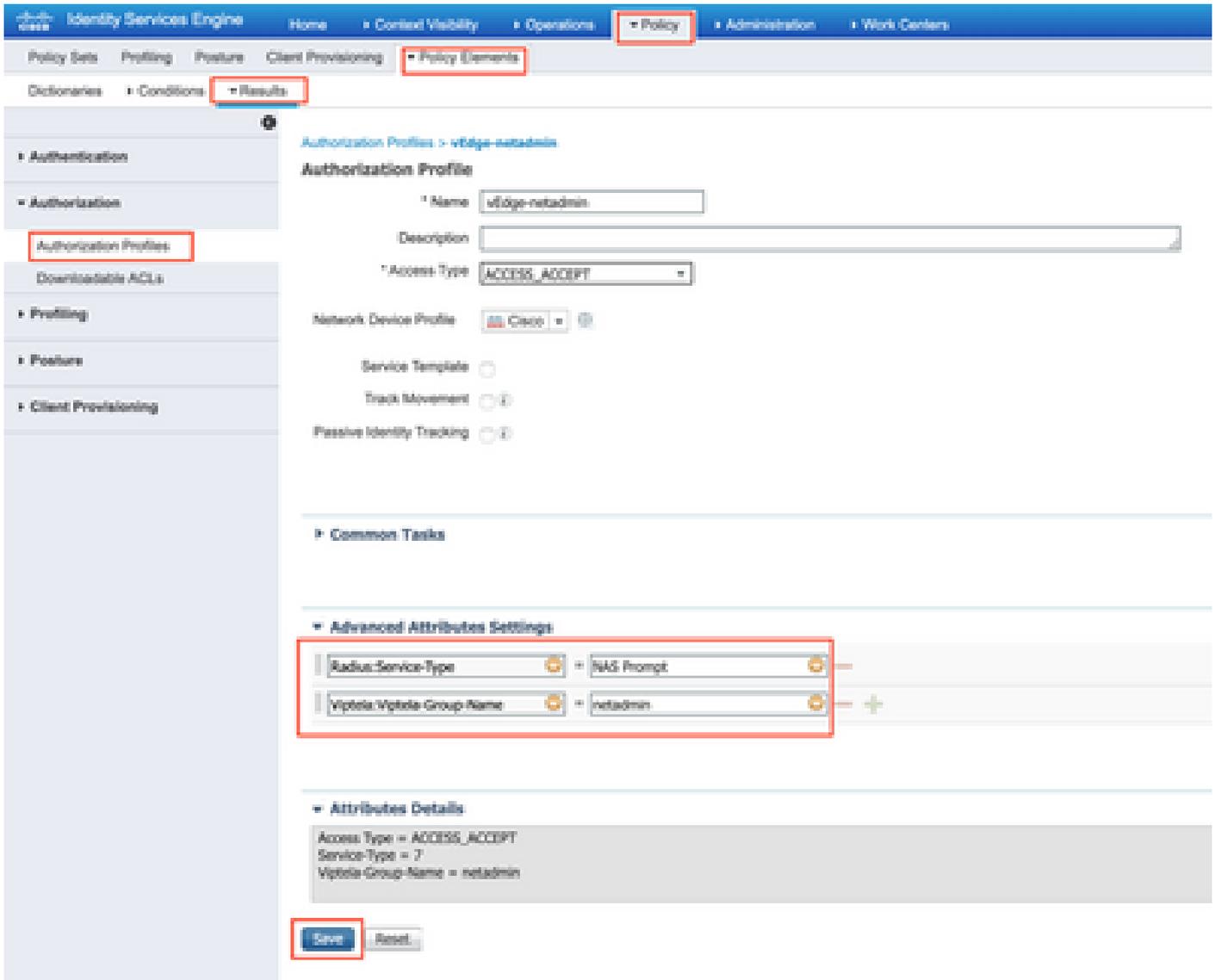
The screenshot shows the Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Content Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Features', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded to show 'Dictionaryes', 'Conditions', and 'Results'. The 'Dictionaryes' menu is selected, and the 'RADIUS Vendors' sub-menu is highlighted. The 'RADIUS Vendors' page displays a table of vendors with columns for Name, Vendor ID, and Description. The 'Import' button is highlighted in red.

Name	Vendor ID	Description
Airspace	14079	Dictionary for Vendor Airspace
Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
Aruba	14833	Dictionary for Vendor Aruba
Brocade	1588	Dictionary for Vendor Brocade
Cisco	9	Dictionary for Vendor Cisco
Cisco-BSSM	5263	Dictionary for Vendor Cisco-BSSM
Cisco-vPro3000	3076	Dictionary for Vendor Cisco-vPro3000
H3C	25586	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2626	Dictionary for Vendor Juniper
Microsoft	315	Dictionary for Vendor Microsoft
Motorsola-Symbol	388	Dictionary for Vendor Motorsola-Symbol
Ruckus	25033	Dictionary for Vendor Ruckus
WSPH	14032	Dictionary for Vendor WSPH

Cargue el archivo creado en el paso 1.



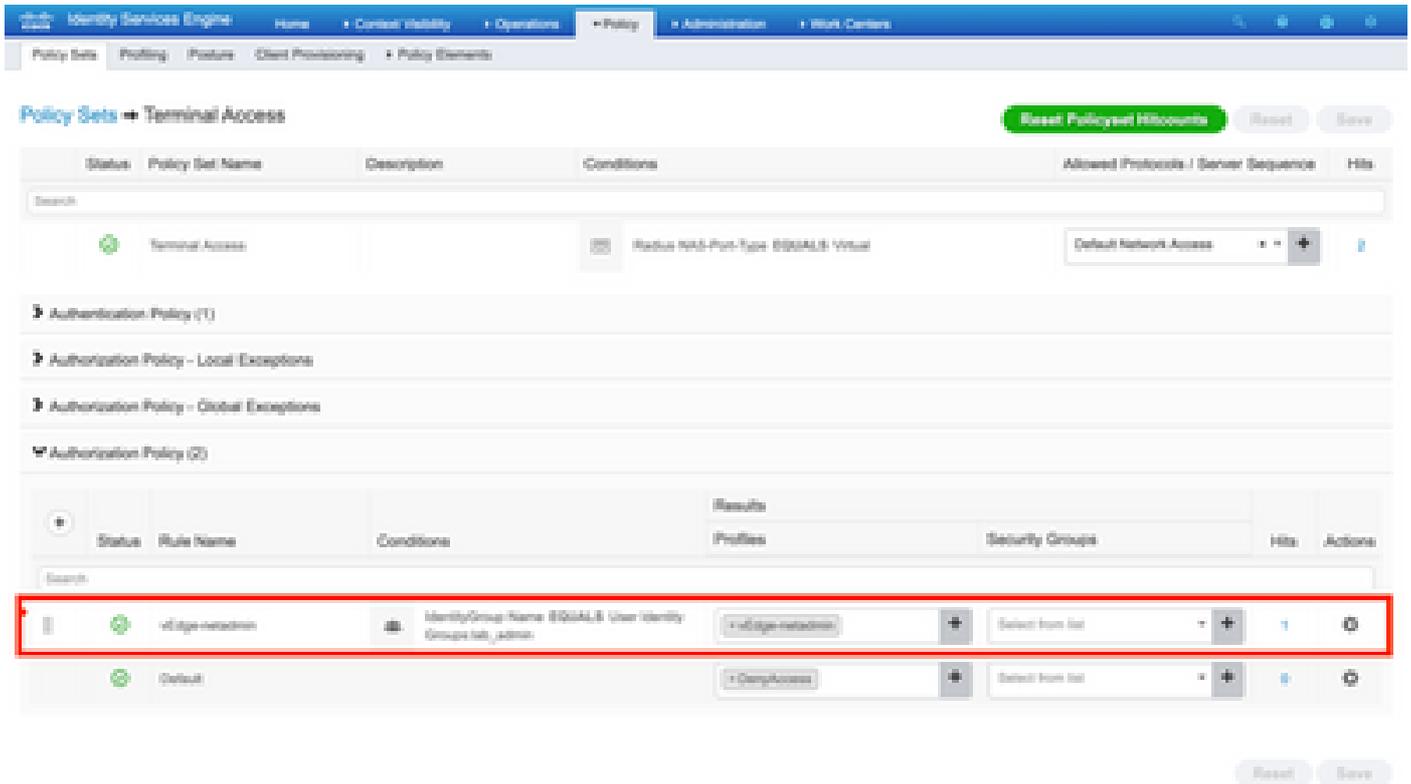
Paso 3. Cree un perfil de autorización. En este paso, el perfil de autorización de Radius asigna, por ejemplo, el nivel de privilegio netadmin a un usuario autenticado. Para esto, navegue hasta Policy > Policy Elements > Authorization Profiles y especifique dos atributos avanzados como se muestra en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

Identity Services Engine Administration

Network Resources

Network Devices List > vEdge-01

Network Devices

* Name: vEdge-01

Description: []

IP Address: [10.48.87.232 / 32]

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: No [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: [*****] [Show]

Use Second Shared Secret: [Show]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings

DTLS Required: [?]

Shared Secret: radius/dtls [?]

CoA Port: 2083 [Set To Default]

Issuer CA of ISE Certificates for CoA: Select if required (optional) [?]

DNS Name: []

General Settings

Enable KeyWrap: [?]

* Key Encryption Key: [] [Show]

* Message Authenticator Code Key: [] [Show]

Key Input Format: ASCII HEXADECIMAL

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
```

```
SESSION  USER      CONTEXT  FROM          PROTO  AUTH
-----  -
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

Identity Services Engine

Home > Control Visibility > Operations > Policy > Administration > **Device Settings**

Network Access > Guest Access > TrustSec > EPOD > Profiles > Posture > **Device Administration** > Password

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > **Policy Elements** > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > vEdge

TACACS Profile

Name: vEdge_netadmin

Description: [Empty]

Task Attribute View | Rule View

Common Tasks

Common Task Type: [Shell]

Default Privilege: [Empty] (Select 0 to 15)
 Maximum Privilege: [Empty] (Select 0 to 15)
 Access Control List: [Empty]
 Auto Comment: [Empty]
 No Escape: [Empty] (Select true or false)
 Timeout: [Empty] Minutes (0-6000)
 Idle Time: [Empty] Minutes (0-6000)

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
Mandatory	Violate-Group-Name	netadmin

Cancel | Save

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

Identity Services Engine

Home > Control Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > **Network Resources** > Device Profile Management > uGent Services > Feed Service > Threat Center NAC

Network Device > **Network Device Groups** > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External NEM > Location Services

Network Device Groups

All Groups > Choose group

Network | Add | Edit | Show group members | Import | Export | Pin Table | Expand All | Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	-
Blindfish		5
All Locations	All Locations	-
All IPSEC Device	With a RADIUS user IPSEC Device	-

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types

Cancel

Save

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

Network Devices List > vEdge-01

Network Devices

Name vEdge-01

Description

IP Address

IP: 10.48.87.232

/ 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations

IPSEC No

Device Type SD-WAN

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance (Single Connect Support)

SNMP Settings

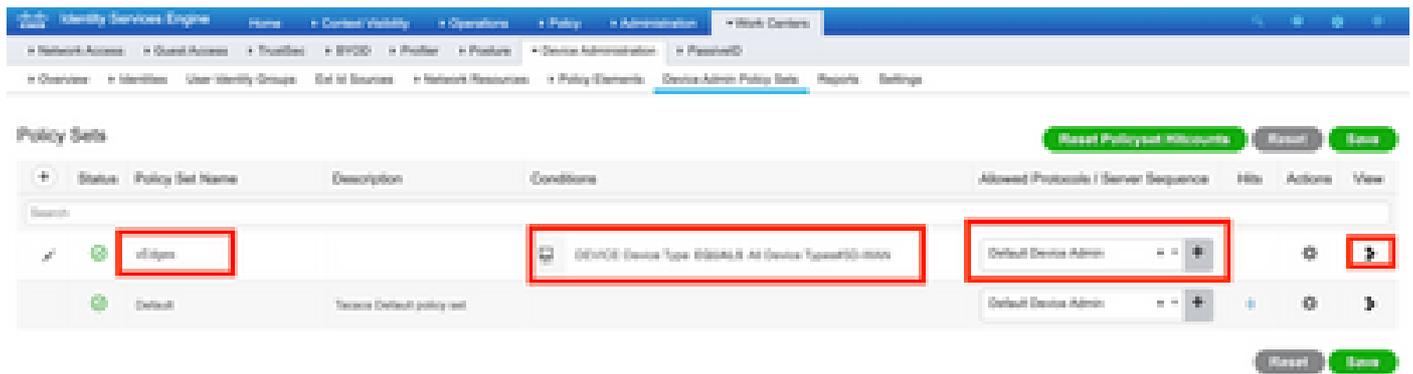
Advanced TrustSec Settings

Save

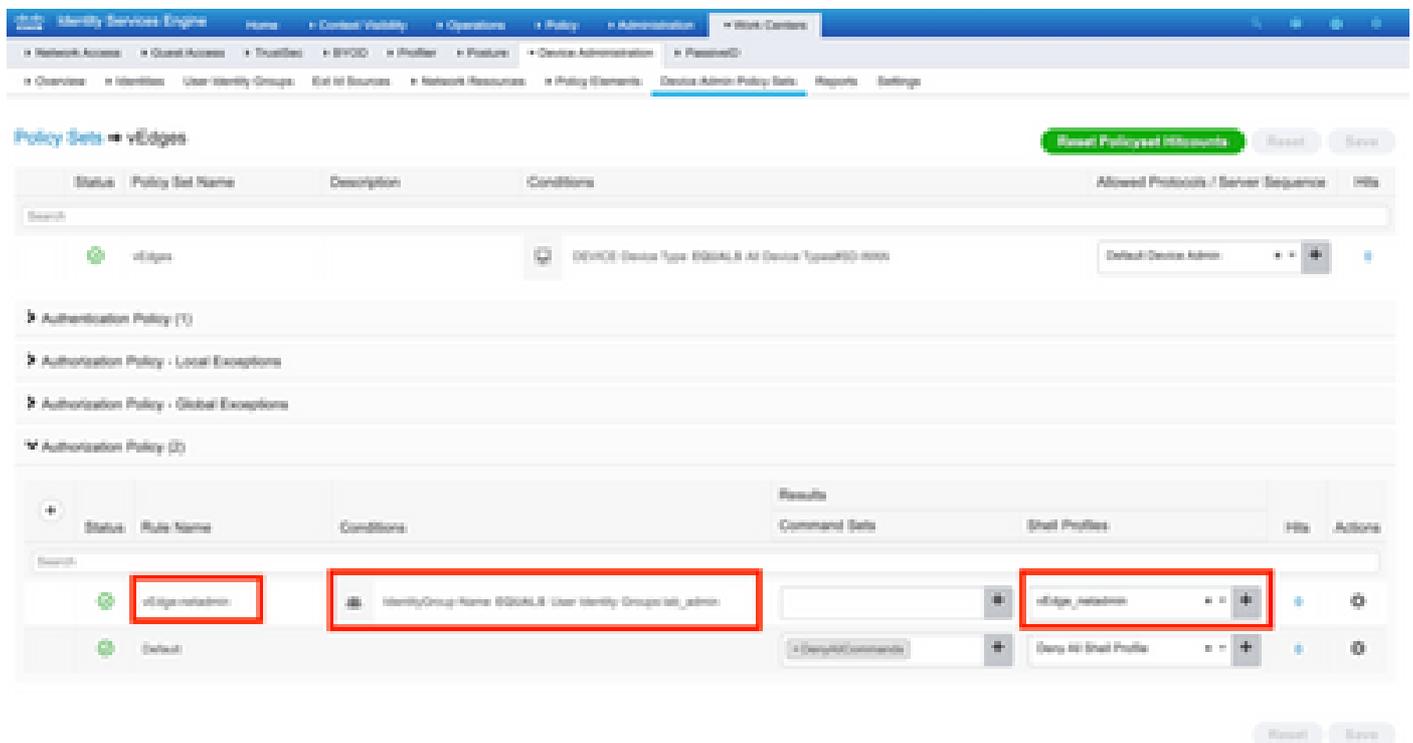
Reset

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
```

SESSION	USER	CONTEXT	FROM	PROTO	AUTH 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).