

# 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.

Identity Services Engine Home | Content Visibility | Operations | **Policy** | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | **Policy Elements**

**Dictionaries** | Conditions | Results

### Dictionaries

- Guest
- GuestAccess
- Identity Mapping
- IdentityGroup
- InternalCA
- InternalEndpoint
- InternalUser
- iPSANSET
- IP
- LLDP
- MAC
- NDM\_LOG
- NIS
- NSD
- Multimedia
- NETFLIX
- Network Access
- Network Condition
- NMAP
- NMAPExtension
- Normalized Radius
- Presence
- Posture
- PROFILE
- Radius**
- RTT
- RADIUS Vendors**
- Session
- SMB
- SNP
- TACACS
- TCNAC
- Threat

### RADIUS Vendors

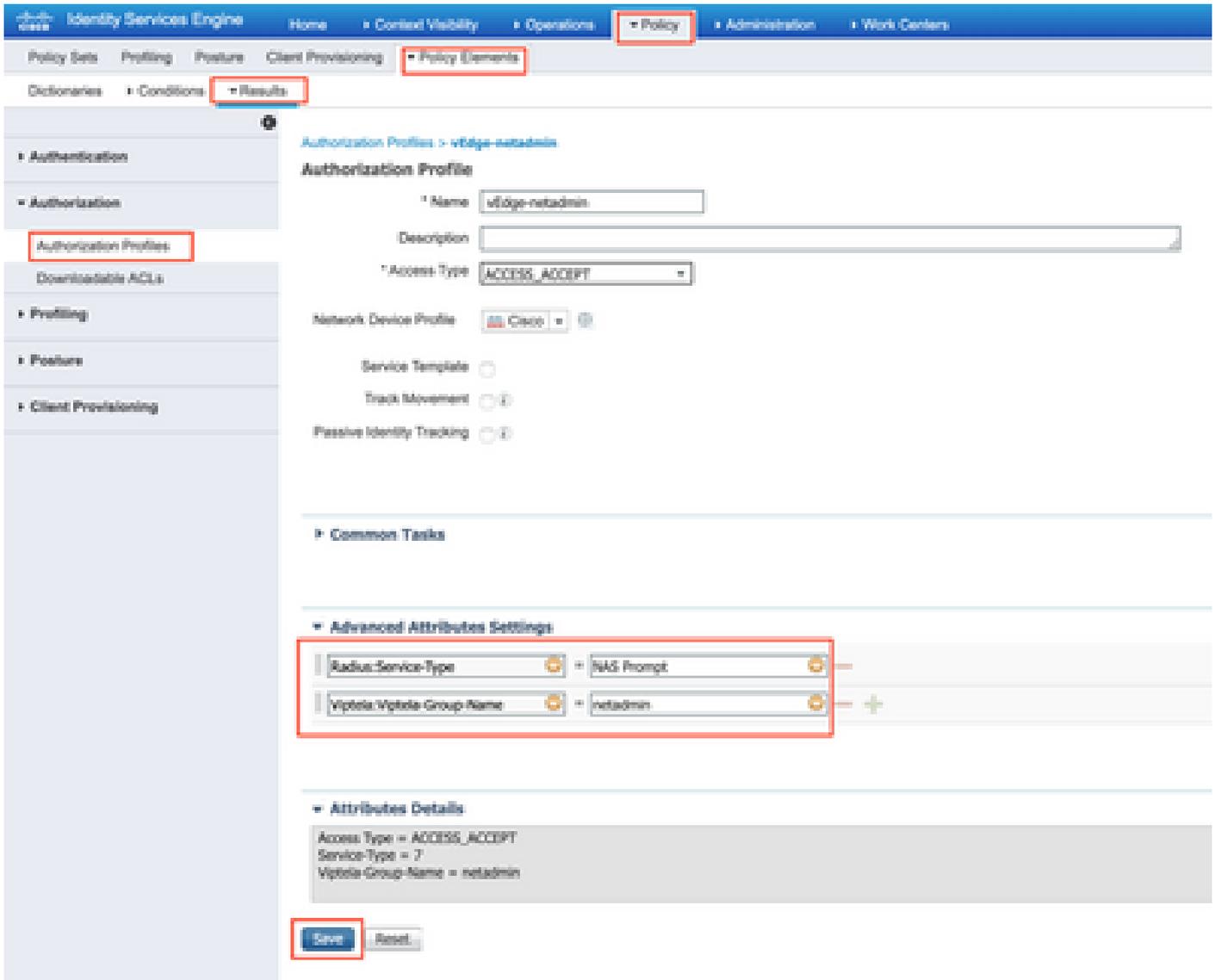
Edit + Add Delete Import Export

| Name                                     | Vendor ID | Description                           |
|--|-----------|---------------------------------------|
| <input type="checkbox"/> Airespace       | 14079     | Dictionary for Vendor Airespace       |
| <input type="checkbox"/> Alcatel-Lucent  | 800       | Dictionary for Vendor Alcatel-Lucent  |
| <input type="checkbox"/> Aruba           | 14823     | Dictionary for Vendor Aruba           |
| <input type="checkbox"/> Brocade         | 1588      | Dictionary for Vendor Brocade         |
| <input type="checkbox"/> Cisco           | 9         | Dictionary for Vendor Cisco           |
| <input type="checkbox"/> Cisco-BSSM      | 3263      | Dictionary for Vendor Cisco-BSSM      |
| <input type="checkbox"/> Cisco-IPN3000   | 3076      | Dictionary for Vendor Cisco-IPN3000   |
| <input type="checkbox"/> H3C             | 25506     | Dictionary for Vendor H3C             |
| <input type="checkbox"/> HP              | 11        | Dictionary for Vendor HP              |
| <input type="checkbox"/> Juniper         | 2626      | Dictionary for Vendor Juniper         |
| <input type="checkbox"/> Microsoft       | 311       | Dictionary for Vendor Microsoft       |
| <input type="checkbox"/> Motorola-Symbol | 368       | Dictionary for Vendor Motorola-Symbol |
| <input type="checkbox"/> Ruckus          | 25053     | Dictionary for Vendor Ruckus          |
| <input type="checkbox"/> WISH            | 14032     | Dictionary for Vendor WISH            |

Carregue o arquivo criado na etapa 1.

The screenshot displays the 'Dictionaries' management interface. On the left, a tree view lists various dictionary types, including Guest, GuestAccess, Identity Mapping, IdentityGroup, InternalCA, InternalEndpoint, InternalUser, InternalUser, iCTASSET, IP, LLDP, MAC, MDM\_LOG, MSE, MUD, Multimedia, NETFLOW, Network Access, Network Condition, NMAP, NMAPExtension, Normalised Radius, PassiveID, Posture, PROFILER, Radius, RADIUS Vendors (highlighted), Session, SNMP, SXP, TACACS, TC-MAC, and Threat. On the right, a dialog box titled 'Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".' contains a 'Vendor file:' field with a 'Choose file' button and the text 'dictionary.viptelia'. Below this are 'Import' and 'Cancel' buttons.

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.

The screenshot displays the 'Policy Sets' configuration page for 'Terminal Access' in the Identity Services Engine. The main table lists policy sets, and a detailed view of the 'vEdge-remote' policy set is shown below. The highlighted row in the detailed view is as follows:

| Status | Rule Name    | Conditions   | Profiles     | Security Groups  | Hits | Actions  |
|--------|--------------|--|--------------|------------------|------|----------|
| Active | vEdge-remote | IdentityGroup Name ISGALB User Identity Group: lab_admin | vEdge-remote | Select from list | 1    | Settings |

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.

Identity Services Engine Administration Work Centers

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > vEdge-01

### Network Devices

\* Name

Description

IP Address  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

## 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
```

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

Identity Services Engine

Home > Context 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\_nstadmin

Description: [Empty]

Task Attribute View | Rule View

Common Tasks

Common Task Type: [Shell]

Default Privilege: [ ] (Select 0 to 15)  
 Maximum Privilege: [ ] (Select 0 to 15)  
 Access Control List: [ ]  
 Auto Comment: [ ]  
 No Escape: [ ] (Select true or false)  
 Timeout: [ ] Minutes (0-9999)  
 Idle Time: [ ] Minutes (0-9999)

Custom Attributes

+ Add | Trash | Edit

| Type      | Name               | Value     |
|-----------|--------------------|-----------|
| Mandatory | Violate-Group-Name | !nstadmin |

Cancel | Save

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

Identity Services Engine

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

System > Identity Management > **Network Resources** > Device Profile Management > p2GSM Services > Post Service > Threat Control NAC

Network Devices > **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                | -                      |
| <b>Bluetooth</b> |                                 | 0                      |
| 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

Etapa 3. Configure o dispositivo e atribua-o ao 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

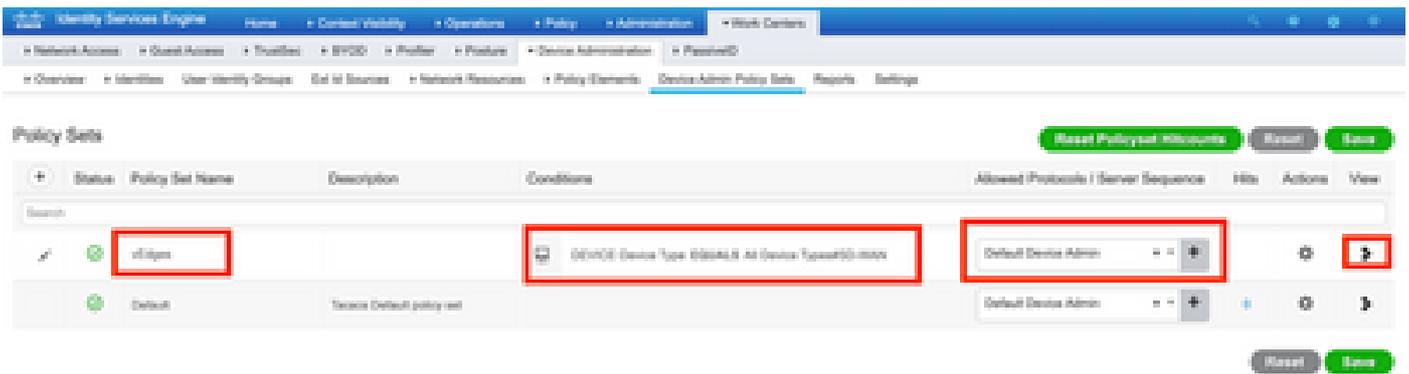
Advanced TrustSec Settings

Save

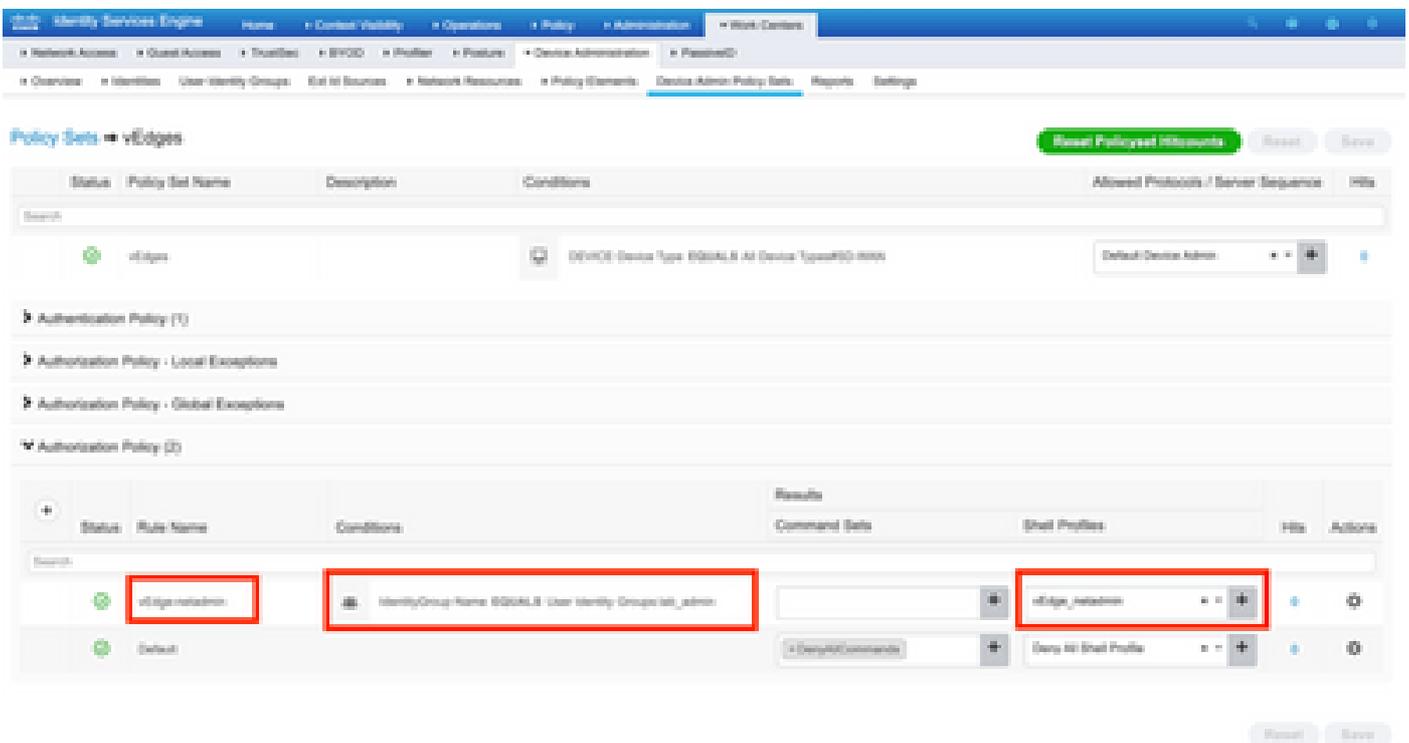
Reset

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
```

| 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 |

## 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](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.