

Configuration de l'authentification utilisateur basée sur Radius et TACACS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Authentification et autorisation utilisateur basées sur Radius pour vEdge et les contrôleurs](#)

[Authentification et autorisation des utilisateurs basées sur TACACS pour vEdge et les contrôleurs](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation des utilisateurs basées sur Radius et TACACS pour vEdge et les contrôleurs avec ISE.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Pour les besoins de la démonstration, la version 2.6 d'ISE est utilisée. vEdge-cloud et les contrôleurs exécutant 19.2.1

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Le logiciel Viptela fournit trois noms de groupes d'utilisateurs fixes : basic, netadmin, et operator. Vous devez affecter l'utilisateur à au moins un groupe. L'utilisateur TACACS/Radius par défaut est automatiquement placé dans le groupe de base.

Authentification et autorisation utilisateur basées sur Radius pour vEdge et les

contrôleurs

Étape 1. Créez un dictionnaire de rayons Viptela pour ISE. Pour ce faire, créez un fichier texte avec le contenu suivant :

```
# -*- text -*-  
#  
# dictionary.viptela  
#  
#  
# Version:      $Id$  
#  
  
VENDOR          Viptela                41916  
  
BEGIN-VENDOR    Viptela  
  
ATTRIBUTE       Viptela-Group-Name     1    string
```

Étape 2. Téléchargez le dictionnaire vers ISE. Pour cela, accédez à Policy > Policy Elements > Dictionaries. Dans la liste des dictionnaires, accédez à Radius > Fournisseurs Radius, puis cliquez sur Importer comme indiqué.

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
- NAD
- Multimedia
- NETFLOW
- Network Access
- Network Condition
- NMAP
- NMAPExtension
- Normalized Radius
- Presence
- Posture
- PROFILES
- Radius**
- RTT
- RADIUS Vendors**
- Session
- SANAP
- SNP
- TACACS
- TCNAD
- Threat

RADIUS Vendors

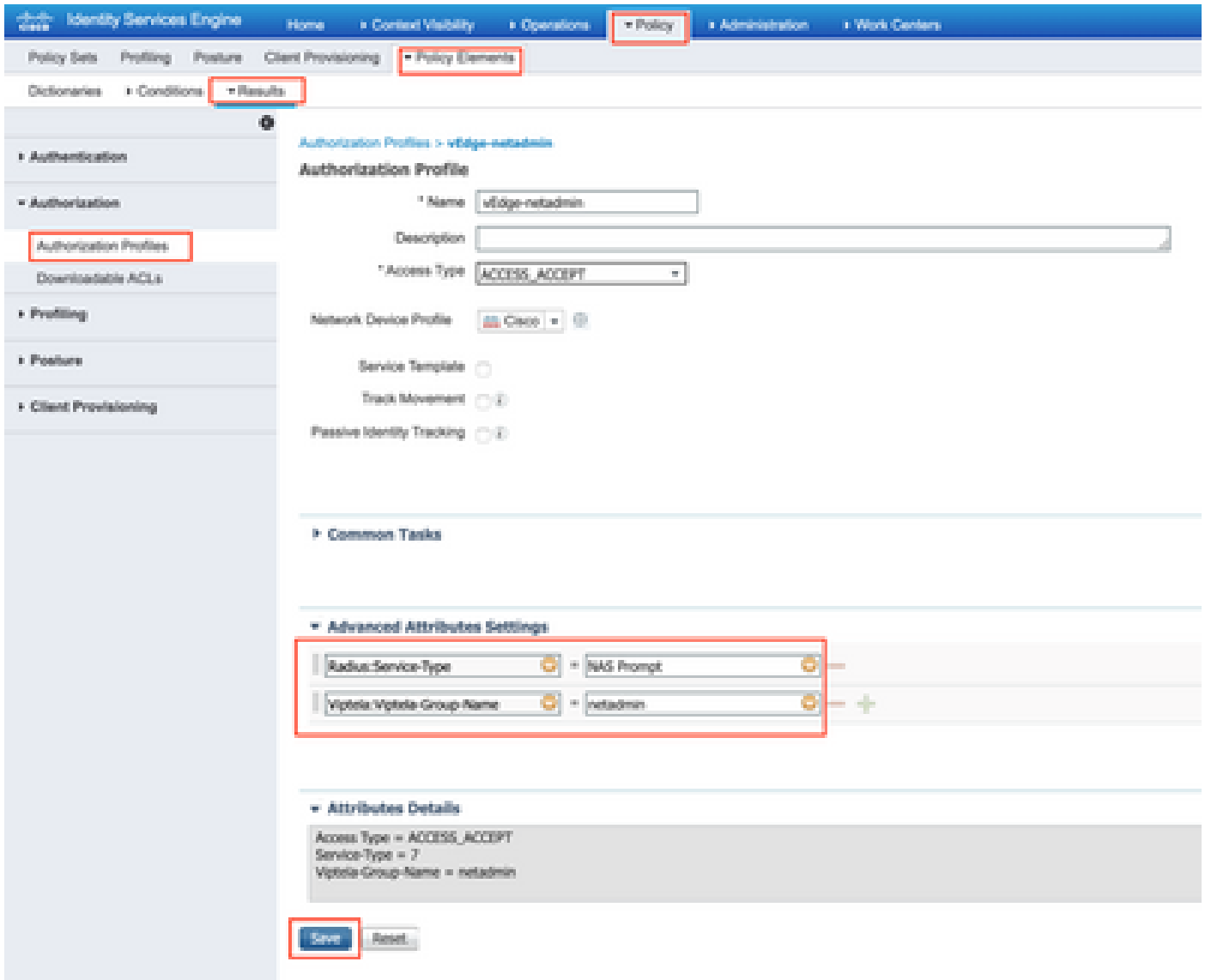
Edit + Add Delete Import Export

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"/> WISPR	14032	Dictionary for Vendor WISPR

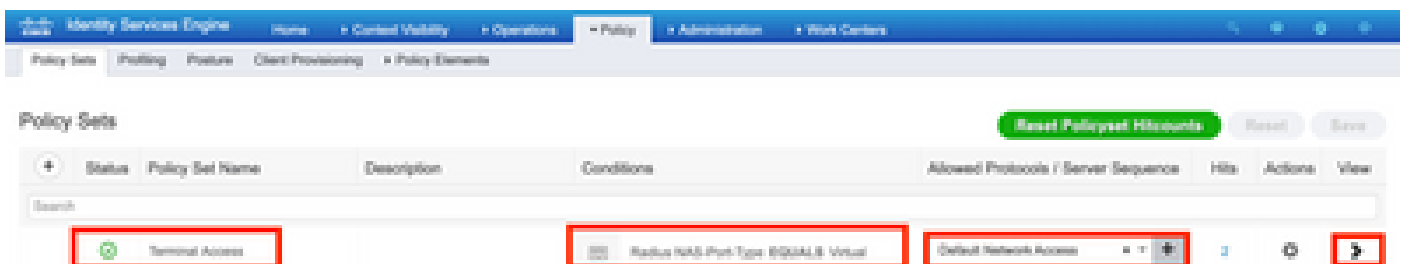
Téléchargez le fichier que vous avez créé à l'étape 1.

The screenshot shows the 'Dictionaries' section of the Identity Services Engine. On the left, a tree view lists various dictionaries, with 'RADIUS Vendors' highlighted. On the right, an 'Import' dialog is open, prompting the user to select a RADIUS vendor file. The file 'dictionary.viptelia' is selected, and the 'Import' button is visible.

Étape 3. Créer un profil d'autorisation. Dans cette étape, le profil d'autorisation Radius attribue, par exemple, le niveau de privilège netadmin à un utilisateur authentifié. Pour cela, accédez à Policy > Policy Elements > Authorization Profiles et spécifiez deux attributs avancés comme indiqué dans l'image.



Étape 4. En fonction de votre configuration réelle, votre jeu de stratégies peut avoir un aspect différent. Pour les besoins de la démonstration dans cet article, l'entrée de stratégie appelée Terminal Access est créée comme illustré dans l'image.



Cliquez sur > et l'écran suivant apparaît comme illustré dans l'image.

The screenshot shows the Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Policy Sets' selected. Below it, the 'Terminal Access' policy set is displayed. A table lists the policy sets, with the 'vEdge-remote' row highlighted by a red box. The table has columns for Status, Rule Name, Conditions, Results (Profiles and Security Groups), Hits, and Actions.

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
Enabled	vEdge-remote	IdentityGroup Name ISG:Lab User Identity Group:lab_admin	vEdge-remote	Select from list	1	Settings	
Enabled	Default		CompAccess	Select from list		Settings	

Cette stratégie correspond au groupe d'utilisateurs lab_admin et attribue un profil d'autorisation créé à l'étape 3.

Étape 5. Définissez NAS (routeur ou contrôleur vEdge) comme indiqué dans l'image.

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

Étape 6. Configurez vEdge/Controller.

```

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

```

Étape 7. Vérification . Connectez-vous à vEdge et assurez-vous que le groupe netadmin est attribué à l'utilisateur distant.

```
vEdgeCloud1# show users
```

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

Authentification et autorisation des utilisateurs basées sur TACACS pour vEdge et les contrôleurs

Étape 1. Créez un profil TACACS. Dans cette étape, le profil TACACS créé est affecté, par exemple, au niveau de privilège netadmin à un utilisateur authentifié.

- Sélectionnez Obligatoire dans la section Attribut personnalisé pour ajouter l'attribut comme suit :

Type	Nom	Valeur
Obligatoire	Nom-Groupe-Viptela	netadmin

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > **Custom Systems**

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:

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	netadmin

Cancel | Save

Étape 2. Créez un groupe de périphériques pour SD-WAN.

Identity Services Engine

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

System > Identity Management > **Network Resources** > Device Profile Management > uGSM 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	-
SD-WAN		0
All Locations	All Locations	-
All IPSEC Device	SD-WAN & RADIUS over IPSEC Device	-

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types

Cancel

Save

Étape 3. Configurez le périphérique et attribuez-le au groupe de périphériques 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

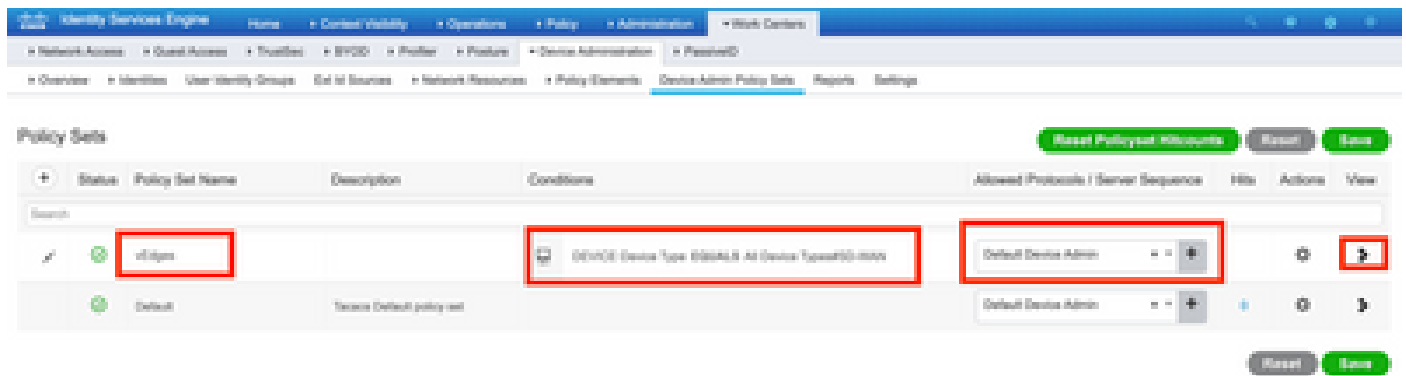
Advanced TrustSec Settings

Save

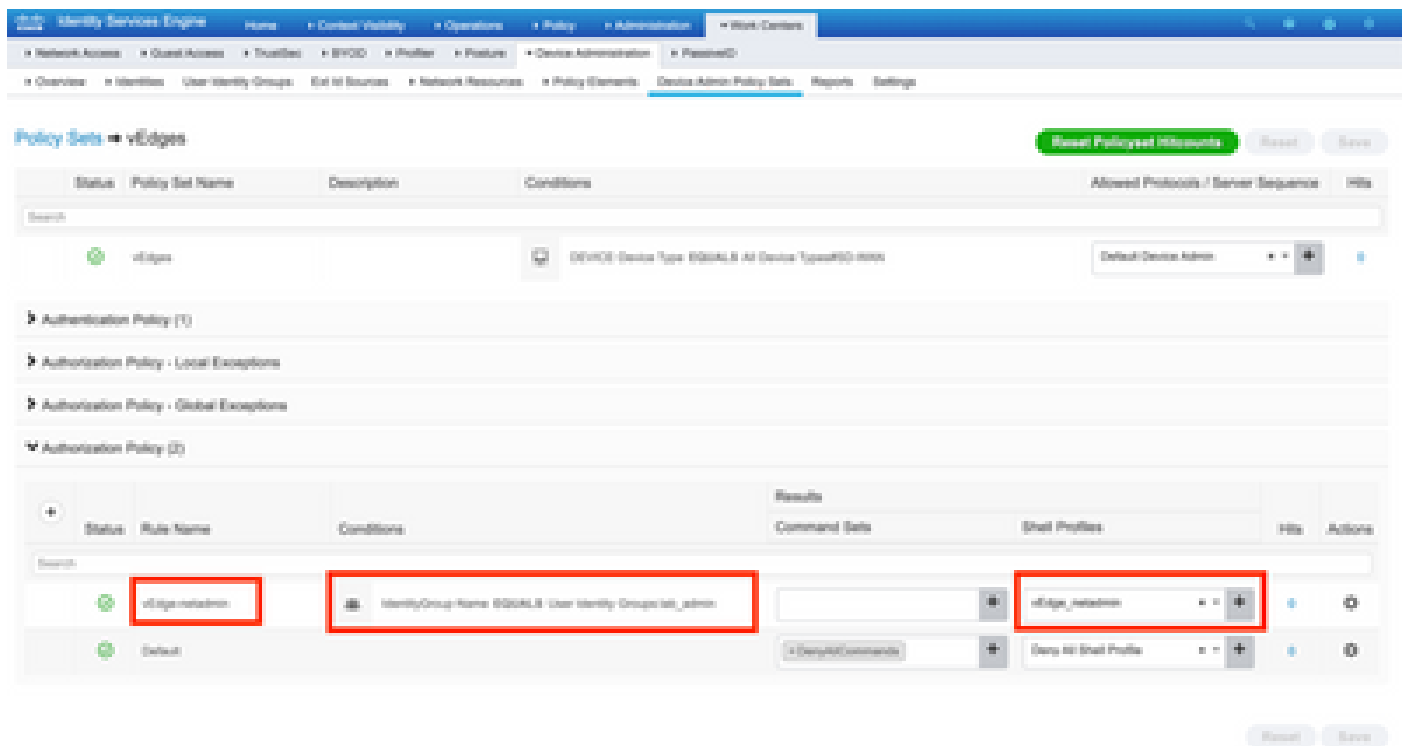
Reset

Étape 4. Définissez la politique d'administration des périphériques.

En fonction de votre configuration réelle, votre jeu de stratégies peut avoir un aspect différent. Pour les besoins de la démonstration dans ce document, la politique est créée.



Cliquez sur > et l'écran suivant apparaît comme illustré dans cette image. Cette stratégie correspond en fonction du type de périphérique nommé SD-WAN et attribue le profil Shell qui est créé à l'étape 1.



Étape 5. Configurer vEdge :

```

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

```

Étape 6. Vérification . Connectez-vous à vEdge et assurez-vous que le groupe netadmin est attribué à l'utilisateur distant :

```
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

Informations connexes

- Guide de déploiement prescriptif 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>
- Configuration de l'accès et de l'authentification des utilisateurs : https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.