

Autenticazione e autorizzazione utente basata su Radius e TACACS per vEdge e controller con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Autenticazione e autorizzazione utente basate su Radius per vEdge e controller](#)

[Autenticazione e autorizzazione utente basate su TACACS per vEdge e controller](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione e l'autorizzazione utente basate su Radius e TACACS per vEdge e i controller con Identity Service Engine (ISE).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la dimostrazione, è stato usato ISE versione 2.6. vEdge-cloud e controller con versione 19.2.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Il software Viptela fornisce tre nomi di gruppi di utenti fissi: **basic**, **netadmin** e **operator**. È necessario assegnare l'utente ad almeno un gruppo. L'utente TACACS/Radius di default viene inserito automaticamente nel gruppo di base.

Autenticazione e autorizzazione utente basate su Radius per vEdge e controller

Passaggio 1. Creare un dizionario Viptela radius per ISE. A tale scopo, creare un file di testo con il contenuto:

```
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela                41916

BEGIN-VENDOR    Viptela

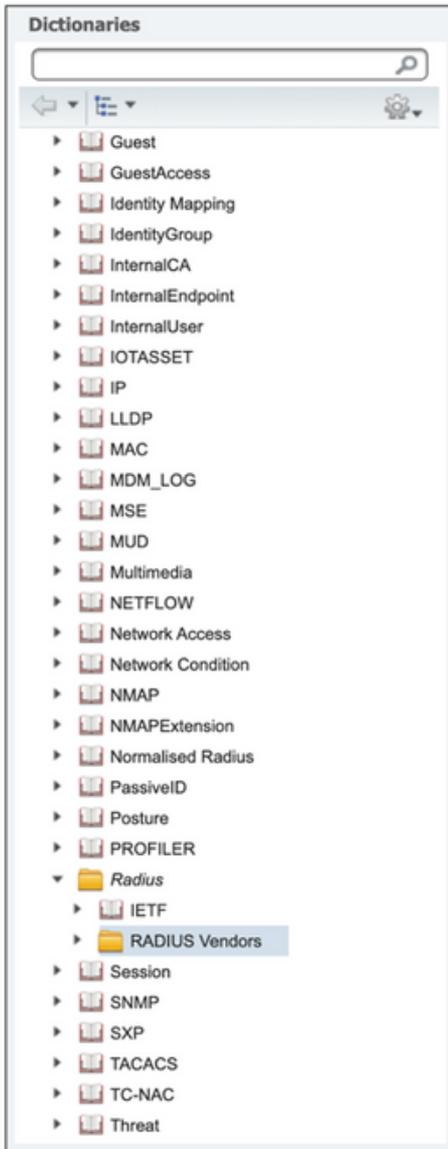
ATTRIBUTE       Viptela-Group-Name     1      string
```

Passaggio 2. Caricare il dizionario su ISE. A tale scopo, selezionare **Criteri > Elementi dei criteri > Dizionari**. Dall'elenco dei dizionari, selezionare **Raggio > Fornitori Raggio**, quindi fare clic su **Importa**, come mostrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded, showing 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded to show 'Dictionaries', 'Conditions', and 'Results'. The 'Dictionaries' section is active, displaying a tree view of various dictionary categories. The 'RADIUS Vendors' section is also active, showing a table of vendors and their IDs. The 'Import' button is highlighted in red.

| Name | Vendor ID | Description |
|-----------------|-----------|---------------------------------------|
| Airspace | 14179 | Dictionary for Vendor Airspace |
| Alcatel-Lucent | 800 | Dictionary for Vendor Alcatel-Lucent |
| Aruba | 14823 | Dictionary for Vendor Aruba |
| Brocade | 1588 | Dictionary for Vendor Brocade |
| Cisco | 9 | Dictionary for Vendor Cisco |
| Cisco-BBSM | 5263 | Dictionary for Vendor Cisco-BBSM |
| Cisco-VPN3000 | 3076 | Dictionary for Vendor Cisco-VPN3000 |
| H3C | 25506 | Dictionary for Vendor H3C |
| HP | 11 | Dictionary for Vendor HP |
| Juniper | 2636 | Dictionary for Vendor Juniper |
| Microsoft | 311 | Dictionary for Vendor Microsoft |
| Motorola-Symbol | 388 | Dictionary for Vendor Motorola-Symbol |
| Ruckus | 25053 | Dictionary for Vendor Ruckus |
| WISPr | 14122 | Dictionary for Vendor WISPr |

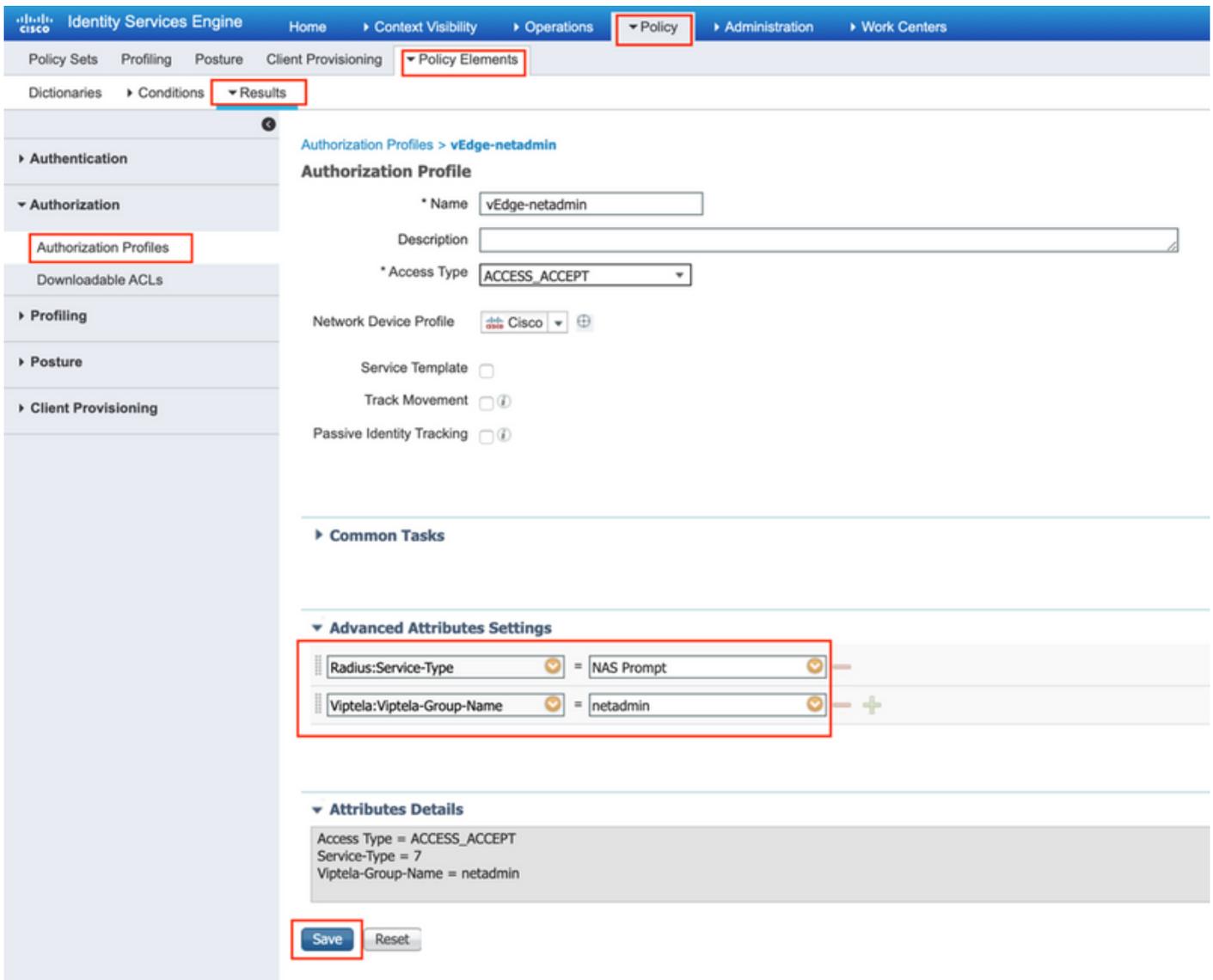
Caricare il file creato al punto 1.



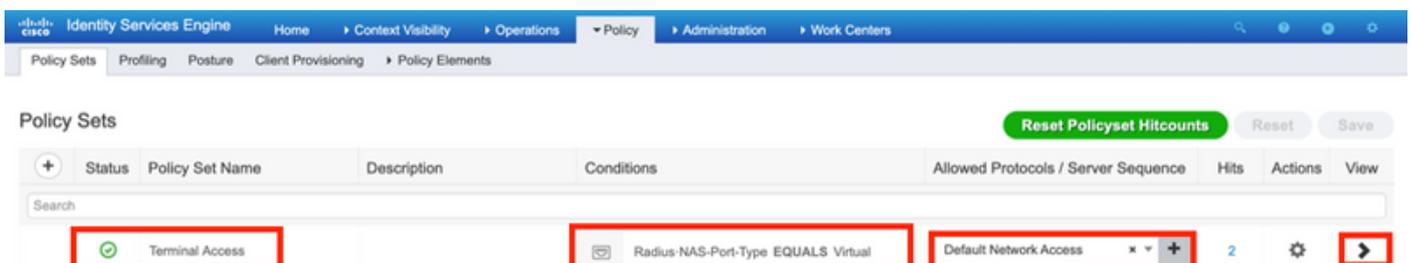
Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

* Vendor file:
 dictionary.viptela

Passaggio 3. Creare un profilo di autorizzazione. In questo passaggio il profilo di autorizzazione Radius assegna, ad esempio, il livello di privilegio netadmin a un utente autenticato. A tale scopo, selezionare **Policy > Policy Elements > Authorization Profiles** (Criteri > Elementi criteri > Profili di autorizzazione) e specificare due attributi avanzati, come mostrato nell'immagine.



Passaggio 4. A seconda della configurazione effettiva, il set di criteri potrebbe avere un aspetto diverso. Ai fini della dimostrazione in questo articolo, la voce Policy denominata **Terminal Access** (Accesso terminale) viene creata come mostrato nell'immagine.



Fare clic su > e viene visualizzata la schermata successiva come illustrato nell'immagine.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Terminal Access Reset Pollicyset Hitcounts Reset Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|-----------------|-------------|-------------------------------------|-------------------------------------|------|
| ✓ | Terminal Access | | Radius-NAS-Port-Type EQUALS Virtual | Default Network Access | 2 |

Authentication Policy (1)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (2)

| + | Status | Rule Name | Conditions | Results | | Hits | Actions |
|---|--------|----------------|---|----------------|------------------|------|---------|
| | | | | Profiles | Security Groups | | |
| ⋮ | ✓ | vEdge-netadmin | IdentityGroup-Name EQUALS User Identity Groups:lab_admin | vEdge-netadmin | Select from list | 1 | ⚙️ |
| | ✓ | Default | | DenyAccess | Select from list | 0 | ⚙️ |

Reset Save

Questo criterio corrisponde in base al gruppo di utenti lab_admin e assegna un profilo di autorizzazione creato nel passaggio 3.

Passaggio 5. Definire NAS (vEdge router o controller) come mostrato nell'immagine.

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 * IP: /

* 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

Passaggio 6. Configurare vEdge/Controller.

```

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

```

Passaggio 7. Verifica. Accedere a vEdge e verificare che il gruppo netadmin sia assegnato all'utente 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
```

Autenticazione e autorizzazione utente basate su TACACS per vEdge e controller

Passaggio 1. Creare un profilo TACACS. In questo passaggio, il profilo TACACS creato viene assegnato, ad esempio, il livello di privilegio netadmin a un utente autenticato.

- Selezionare **Obbligatorio** dalla sezione **Attributo personalizzato** per aggiungere l'attributo come:

| Tipo | Nome | Valore |
|--------------|--------------------|----------|
| Obbligatorio | Viptela-Group-Name | netadmin |

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a TACACS Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The main content area is titled 'TACACS Profile' and shows the following configuration:

- Name:** vEdge_netadmin
- Description:** (empty)
- Task Attribute View:** Selected
- Common Task Type:** Shell
- Common Tasks:**
 - Default Privilege: (Select 0 to 15)
 - Maximum Privilege: (Select 0 to 15)
 - Access Control List: (empty)
 - Auto Command: (empty)
 - No Escape: (Select true or false)
 - Timeout: (empty) Minutes (0-9999)
 - Idle Time: (empty) Minutes (0-9999)
- Custom Attributes:**
 - Type: Mandatory
 - Name: Viptela-Group-Name
 - Value: netadmin

Buttons for 'Cancel' and 'Save' are visible at the bottom right.

Passaggio 2. Creare un gruppo di dispositivi per SD-WAN.

Identity Services Engine Home Context Visibility Operations Policy 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 Device Groups

All Groups Choose group ▾

Refresh + Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

| Name | Description | No. of Network Devices |
|---|------------------------------------|------------------------|
| <input type="checkbox"/> All Device Types | All Device Types | -- |
| <input type="checkbox"/> SD-WAN | | 0 |
| <input type="checkbox"/> All Locations | All Locations | -- |
| <input type="checkbox"/> Is IPSEC Device | Is this a RADIUS over IPSEC Device | -- |

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types



Cancel

Save

Passaggio 3. Configurare il dispositivo e assegnarlo al gruppo di dispositivi SD-WAN:

Network Devices

* Name

Description

IP Address * IP : /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

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

Passaggio 4. Definizione dei criteri di amministrazione dei dispositivi.

A seconda della configurazione effettiva, il set di criteri potrebbe avere un aspetto diverso. Ai fini della dimostrazione in questo documento, viene creato il criterio.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

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

Policy Sets

| + | Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|-------------------------------------|-------------------------------------|-----------------|---------------------------|---|-------------------------------------|------|--|------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | vEdges | | DEVICE Device Type EQUALS All Device Types#SD-WAN | Default Device Admin | | <input type="button" value="Settings"/> <input checked="" type="button" value="View"/> | |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Default | Tacacs Default policy set | | Default Device Admin | 0 | <input type="button" value="Settings"/> <input type="button" value="View"/> | |

Fare clic su > e viene visualizzata la schermata successiva, come mostrato nell'immagine. Questo criterio corrisponde in base al tipo di dispositivo denominato **SD-WAN** e assegna il profilo Shell creato nel passaggio 1.

The screenshot shows the Cisco ISE web interface for configuring vEdge policy sets. The main navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The breadcrumb trail is 'Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Device Admin Policy Sets'. The current page is 'Policy Sets -> vEdges'. A table lists policy sets, with 'vEdges' selected. Below, the configuration for 'vEdge-netadmin' is shown, with red boxes highlighting the rule name, condition, and result. The condition is 'IdentityGroup Name EQUALS User Identity Groups:lab_admin' and the result is 'vEdge_netadmin'. There are also buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'.

Passaggio 5. Configurare vEdge:

```

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

```

Passaggio 6. Verifica. Accedere a vEdge e verificare che il gruppo netadmin sia assegnato all'utente 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 |

Passaggio 5. Configurare vEdge:

Passaggio 5. Configurare vEdge:

Passaggio 5. Configurare vEdge:

Informazioni correlate

- Guida all'implementazione prescrittiva di Cisco ISE Device Administration: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- Configurazione dell'accesso e dell'autenticazione utente: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication