

Configurazione dell'autenticazione utente Radius e TACACS

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 ISE.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la dimostrazione, viene utilizzata la versione 2.6 di ISE. 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

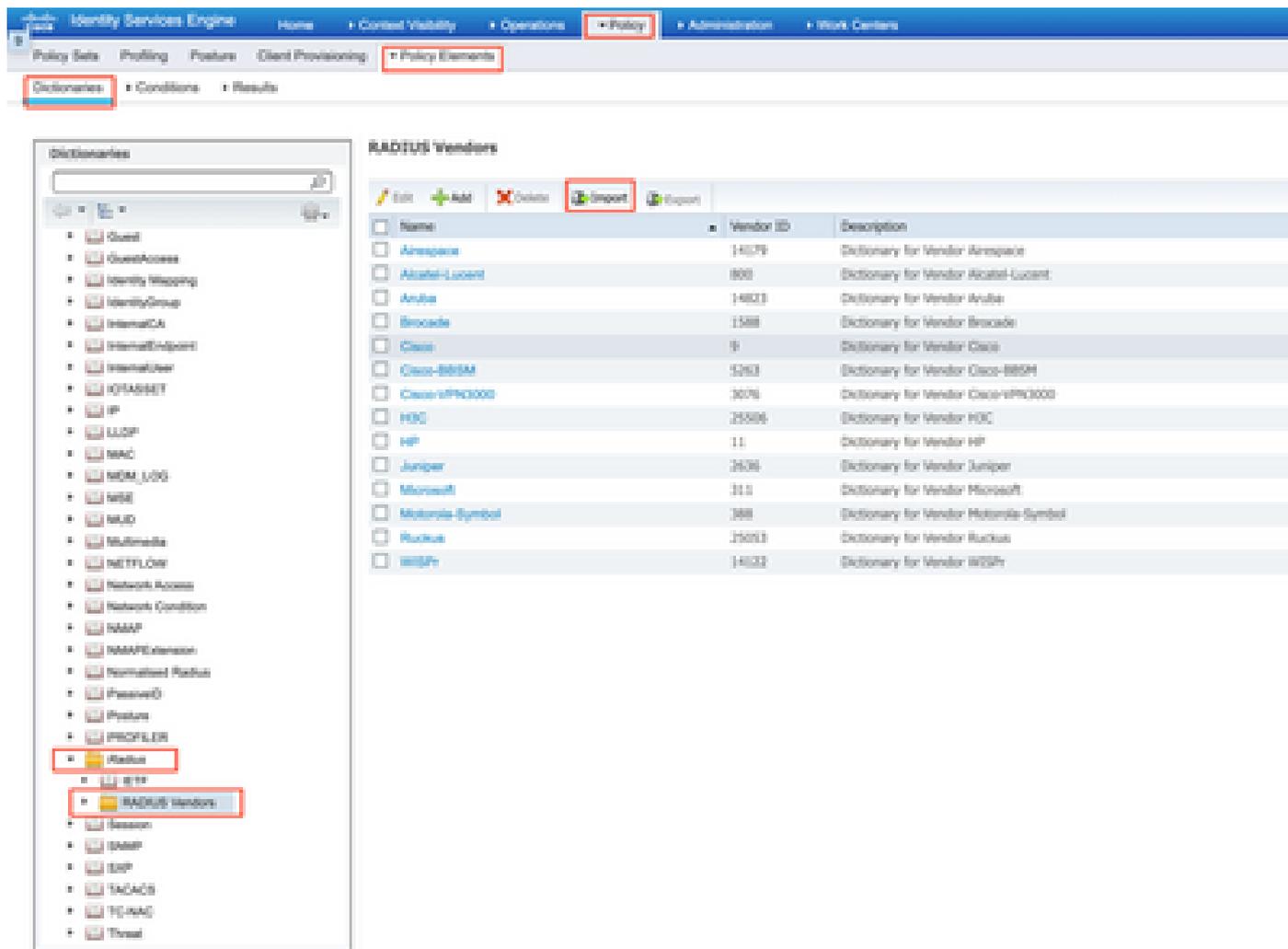
Passaggio 1. Creare un dizionario Viptela radius per ISE. A tale scopo, creare un file di testo con il contenuto:

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

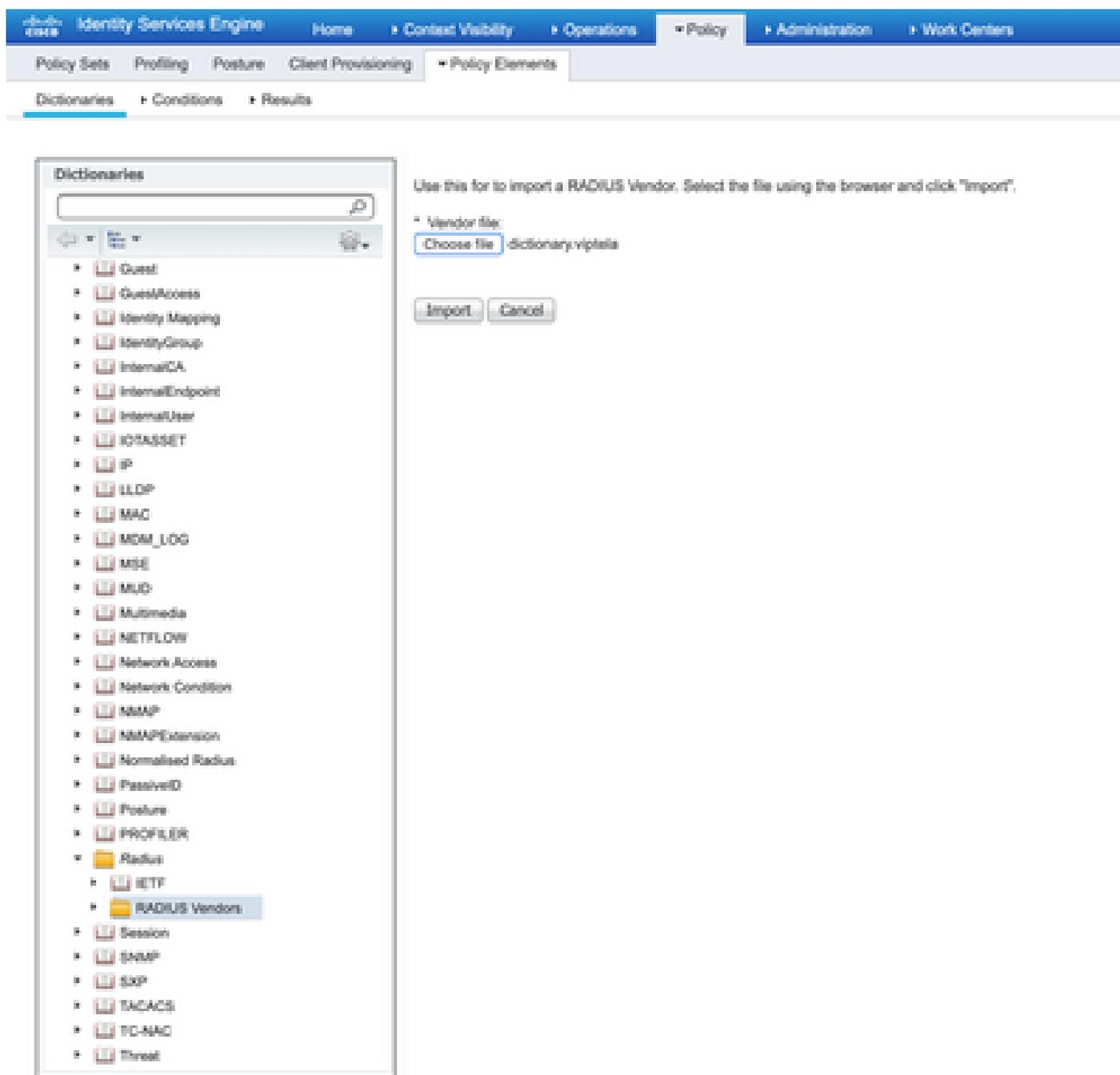
BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name 1 string
```

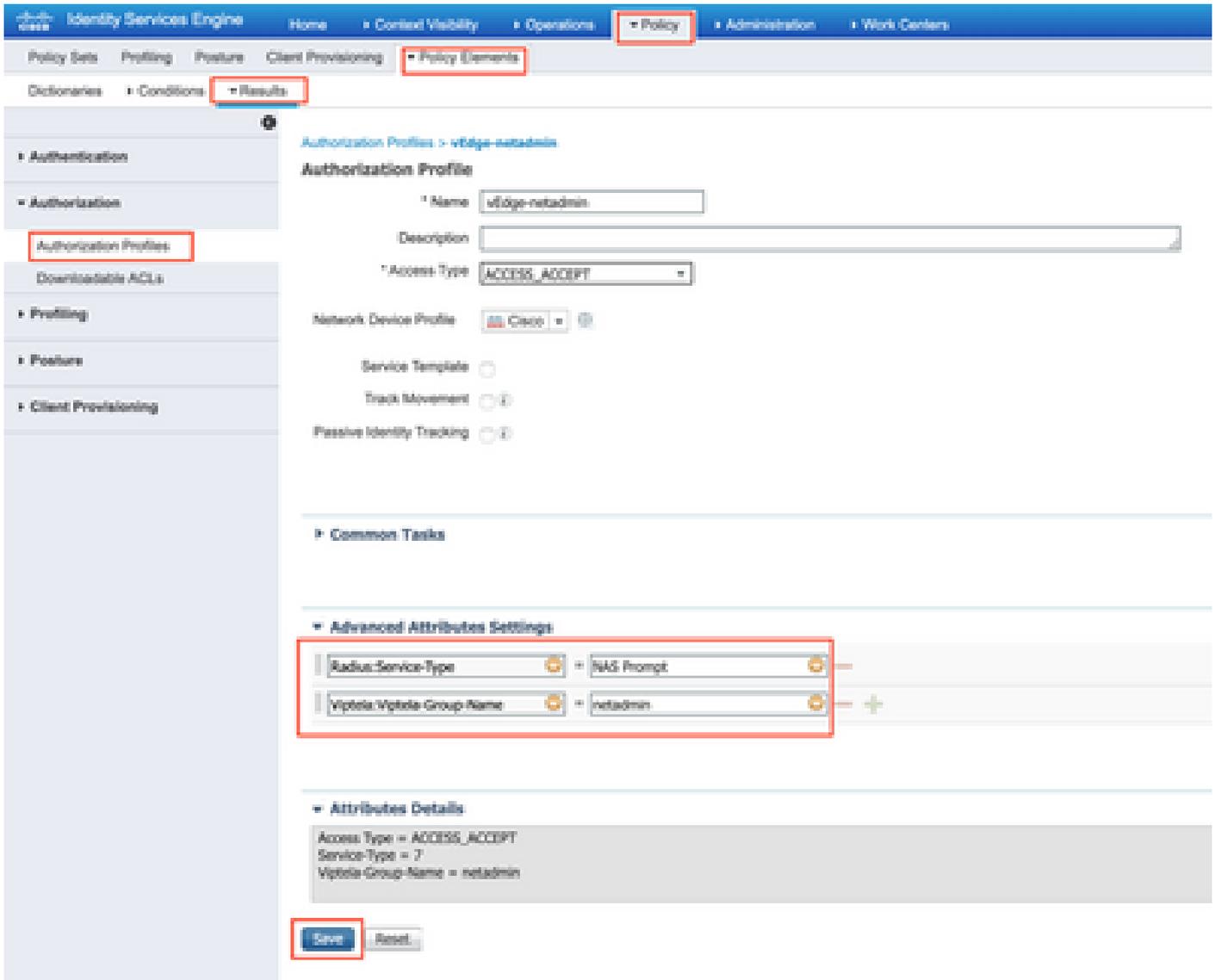
Passaggio 2. Caricare il dizionario su ISE. A tale scopo, selezionare Criteri > Elementi dei criteri > Dizionari. Dall'elenco dei dizionari, selezionare Raggio > Fornitori Raggio, quindi fare clic su Importa come mostrato.



Caricare il file creato nel passaggio 1.



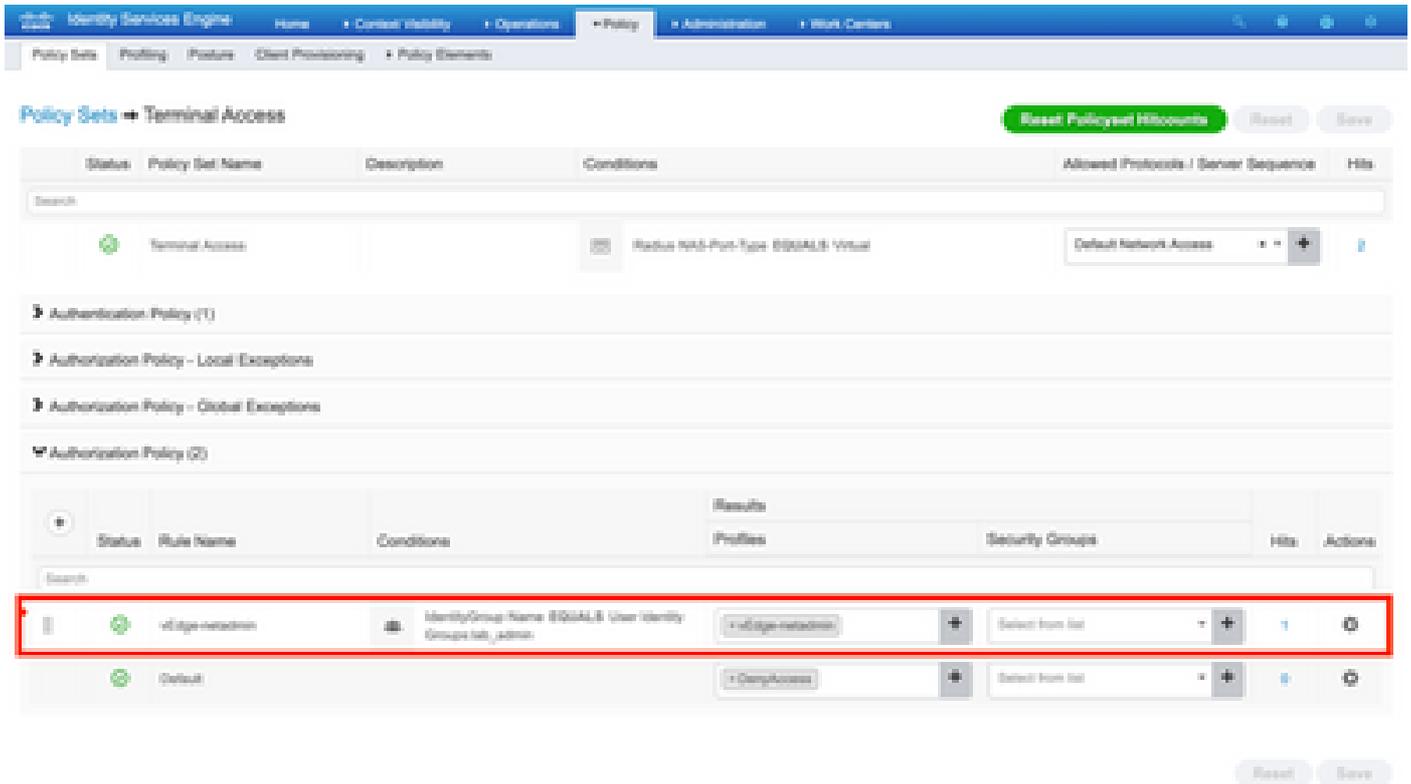
Passaggio 3. Creare un profilo di autorizzazione. In questo passaggio, il profilo di autorizzazione Radius assegna, ad esempio, il livello di privilegio netadmin a un utente autenticato. A tale scopo, selezionare Policy > Policy Elements > Authorization Profiles (Criteri > Elementi criteri > Profili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



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



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



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

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

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  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

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: [Empty] (Select 0 to 15)
 Maximum Privilege: [Empty] (Select 0 to 15)
 Access Control List: [Empty]
 Auto Command: [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	!nstadmin

Cancel | Save

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 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 MDM > 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	-
Standalone		0
All Locations	All Locations	-
All IPSEC Device	Standalone RADIUS user 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 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

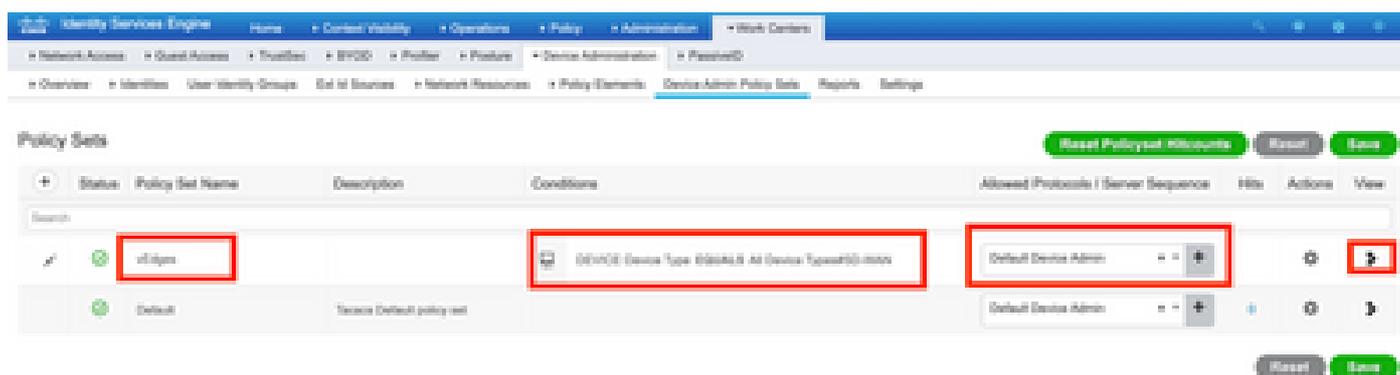
Advanced Tracer Settings

Save

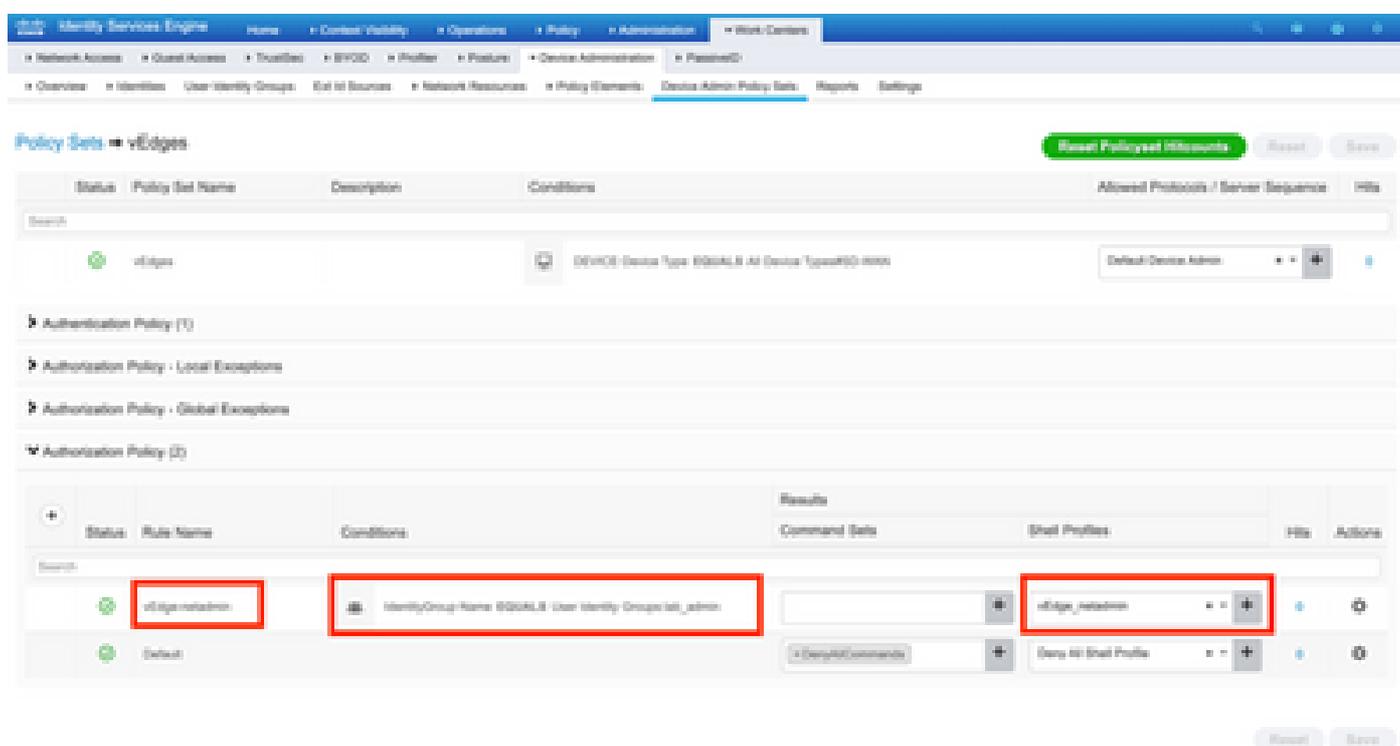
Reset

Passaggio 4. Definire i criteri di amministrazione del dispositivo.

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



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.



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

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_Interface

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).