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

Sommario

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

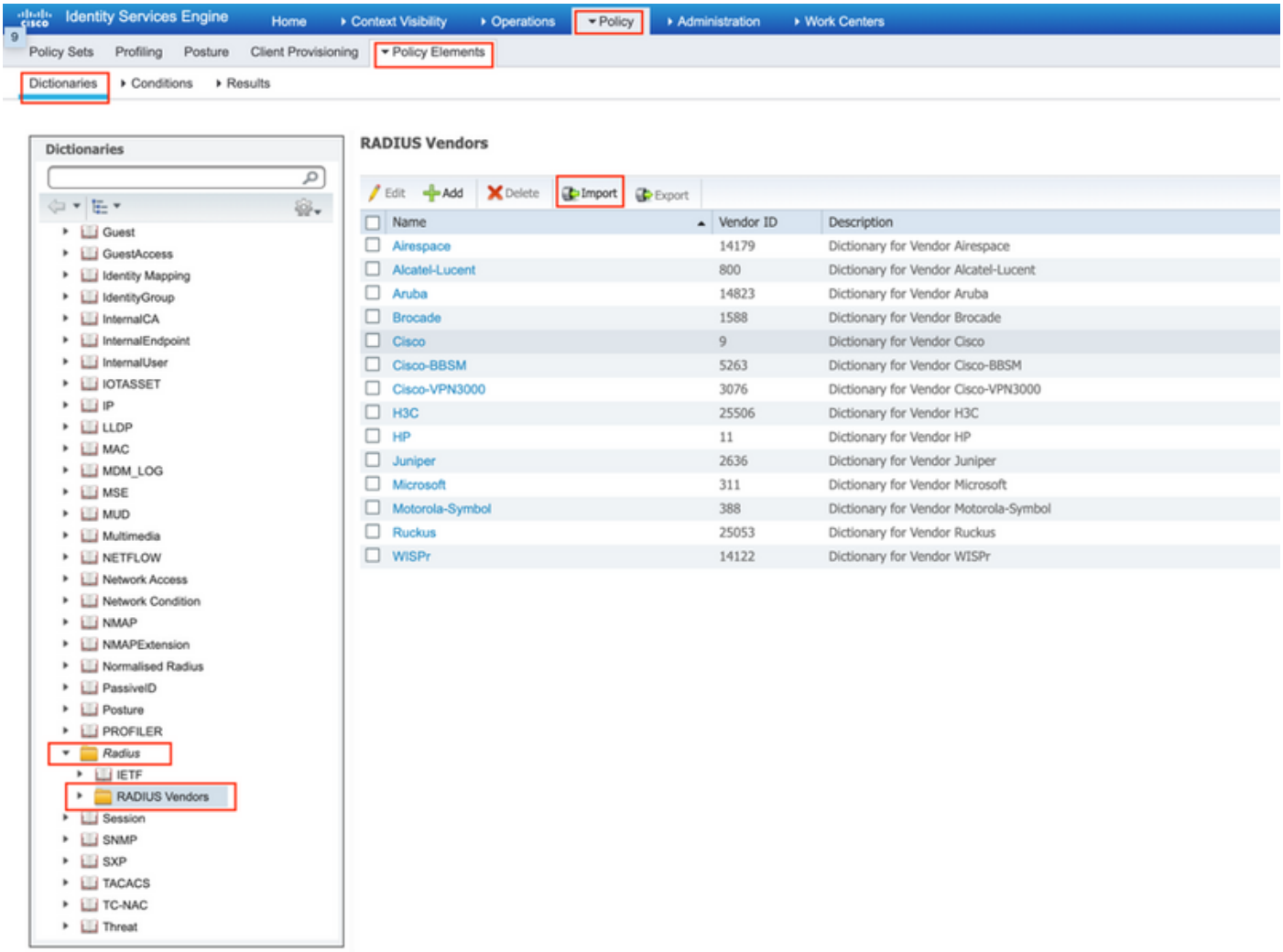
Il software Viptela fornisce tre nomi di gruppi di utenti fissi: **basic**, **netadmin** e **operator**. È necessario assegnare l'utente ad almeno un gruppo. L'utente TACACS/Radius di default viene inserito automaticamente nel gruppo di base.

Autenticazione e autorizzazione utente basate su Radius per vEdge e controller

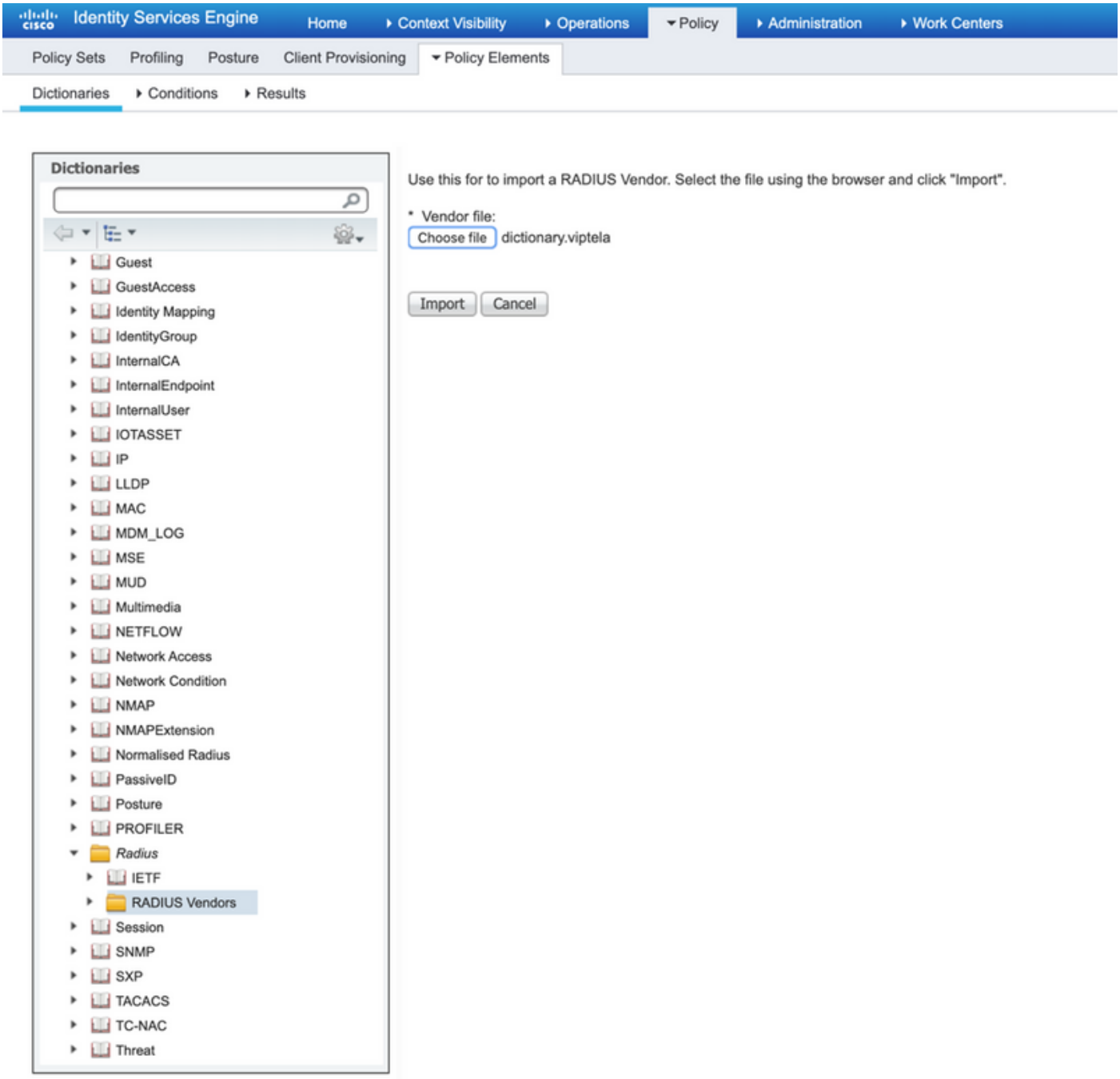
Passaggio 1. Creare un dizionario Viptela radius per ISE. A tale scopo, creare un file di testo con il contenuto:

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

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

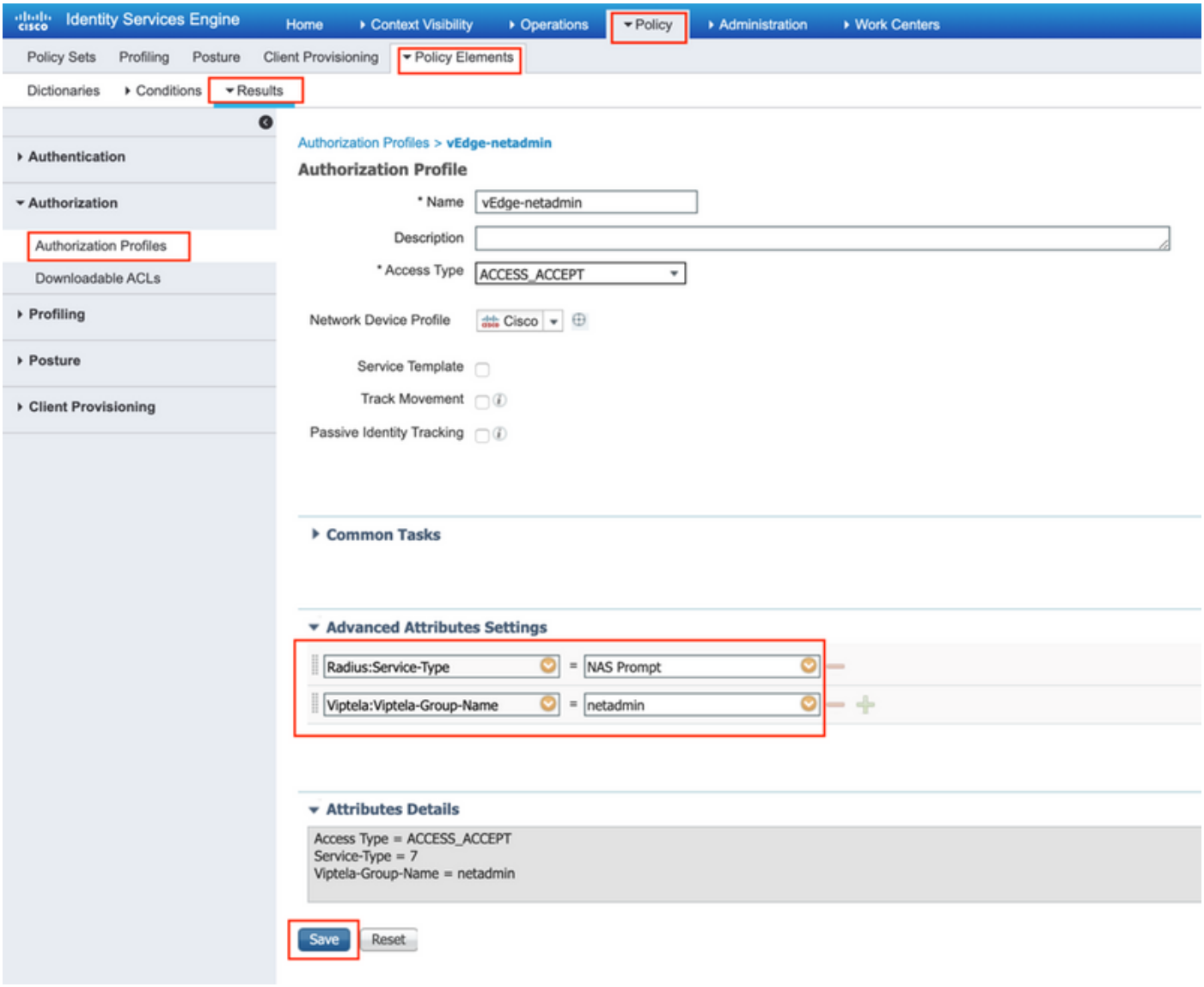
Passaggio 2. Caricare il dizionario su ISE. A tale scopo, selezionare **Criteri > Elementi dei criteri > Dizionari**. Dall'elenco dei dizionari, selezionare **Raggio > Fornitori Raggio**, quindi fare clic su **Importa**, come mostrato nell'immagine.



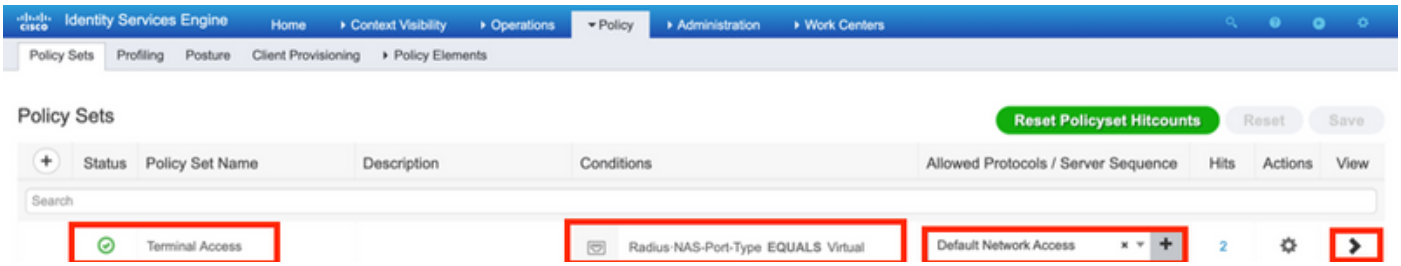
Caricare il file creato al punto 1.



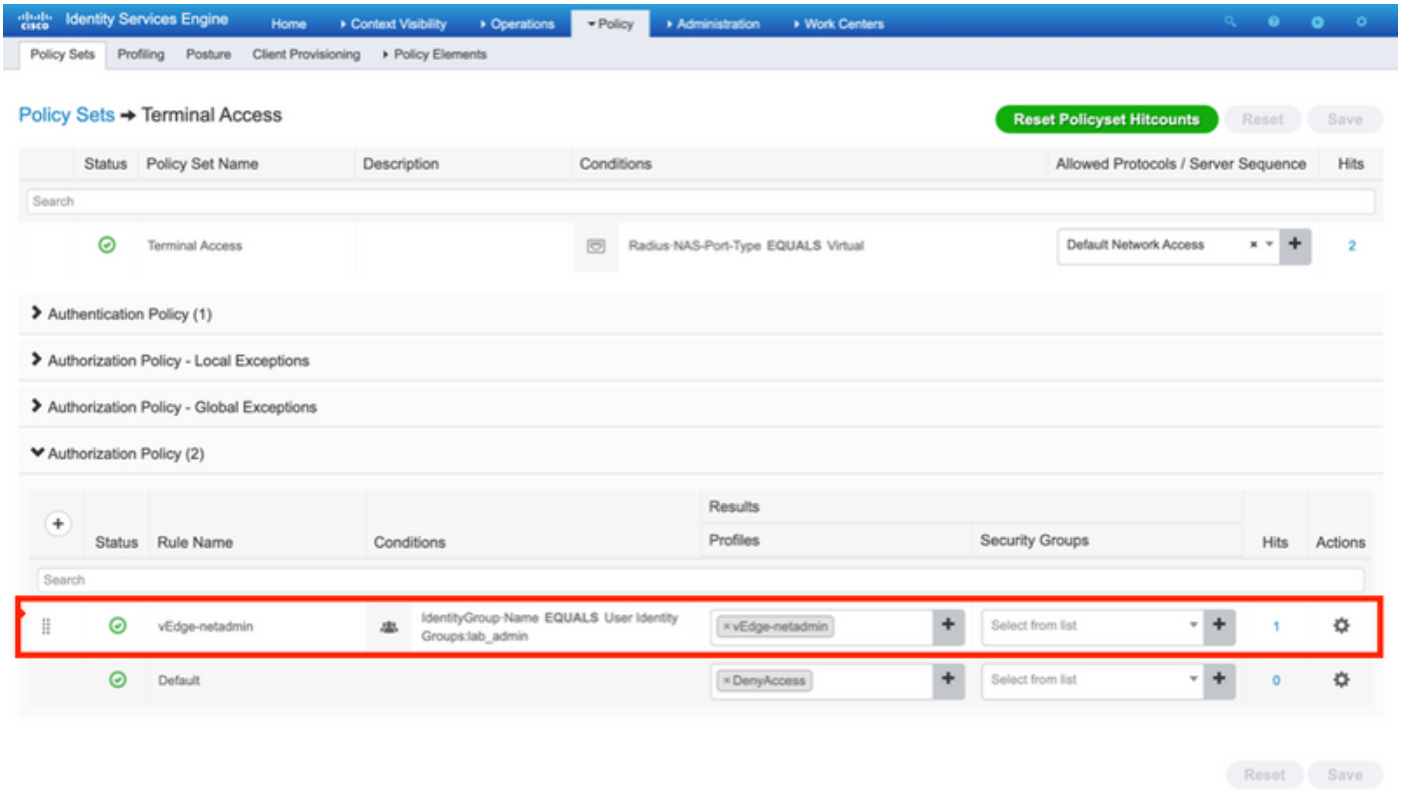
Passaggio 3. Creare un profilo di autorizzazione. In questo passaggio il profilo di autorizzazione Radius assegna, ad esempio, il livello di privilegio netadmin a un utente autenticato. A tale scopo, selezionare **Policy > Policy Elements > Authorization Profiles** (Criteri > Elementi criteri > Profili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



Passaggio 4. A seconda 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.

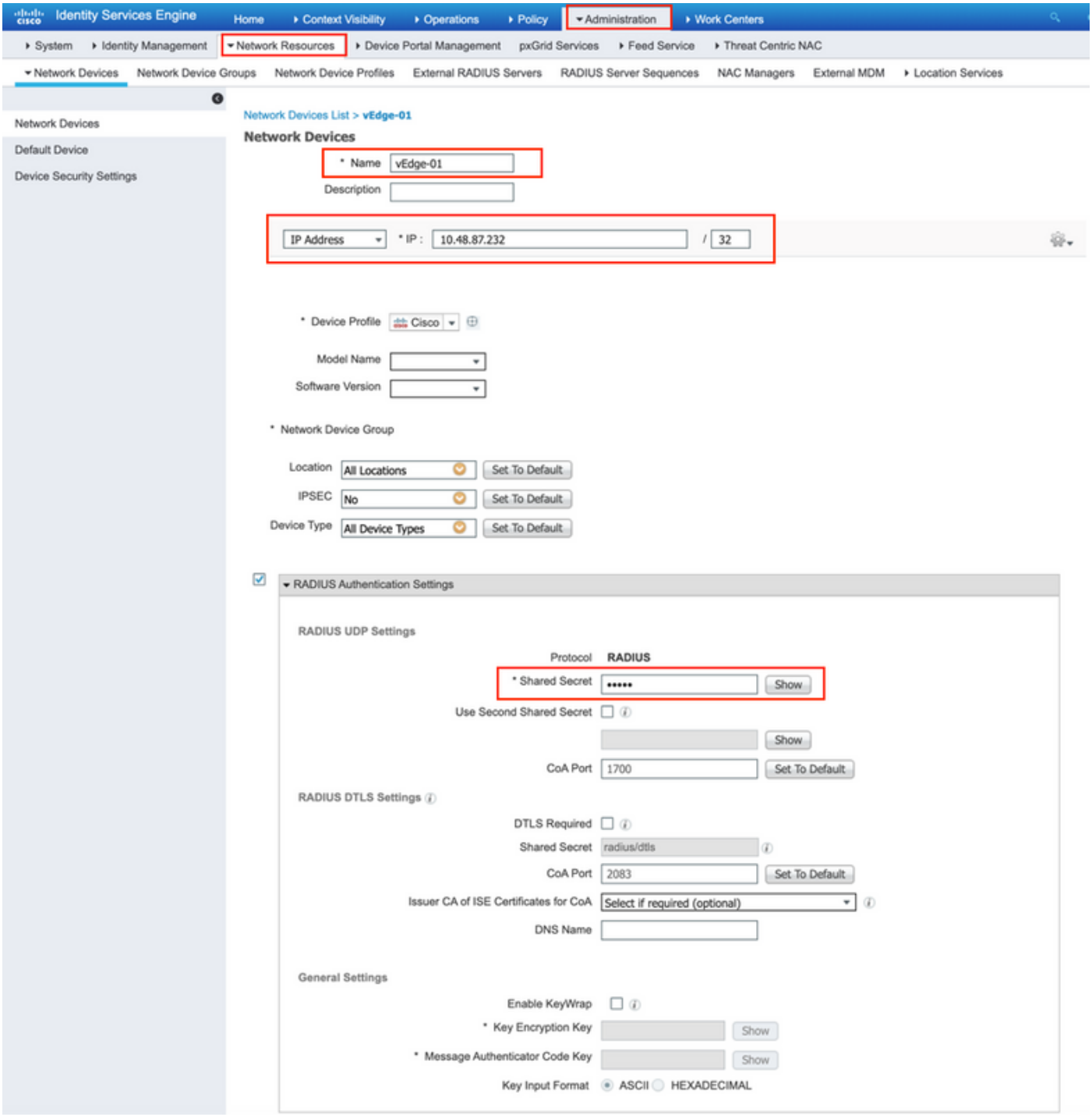


Fare clic su **>** e viene visualizzata la schermata successiva come illustrato nell'immagine.



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.



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.

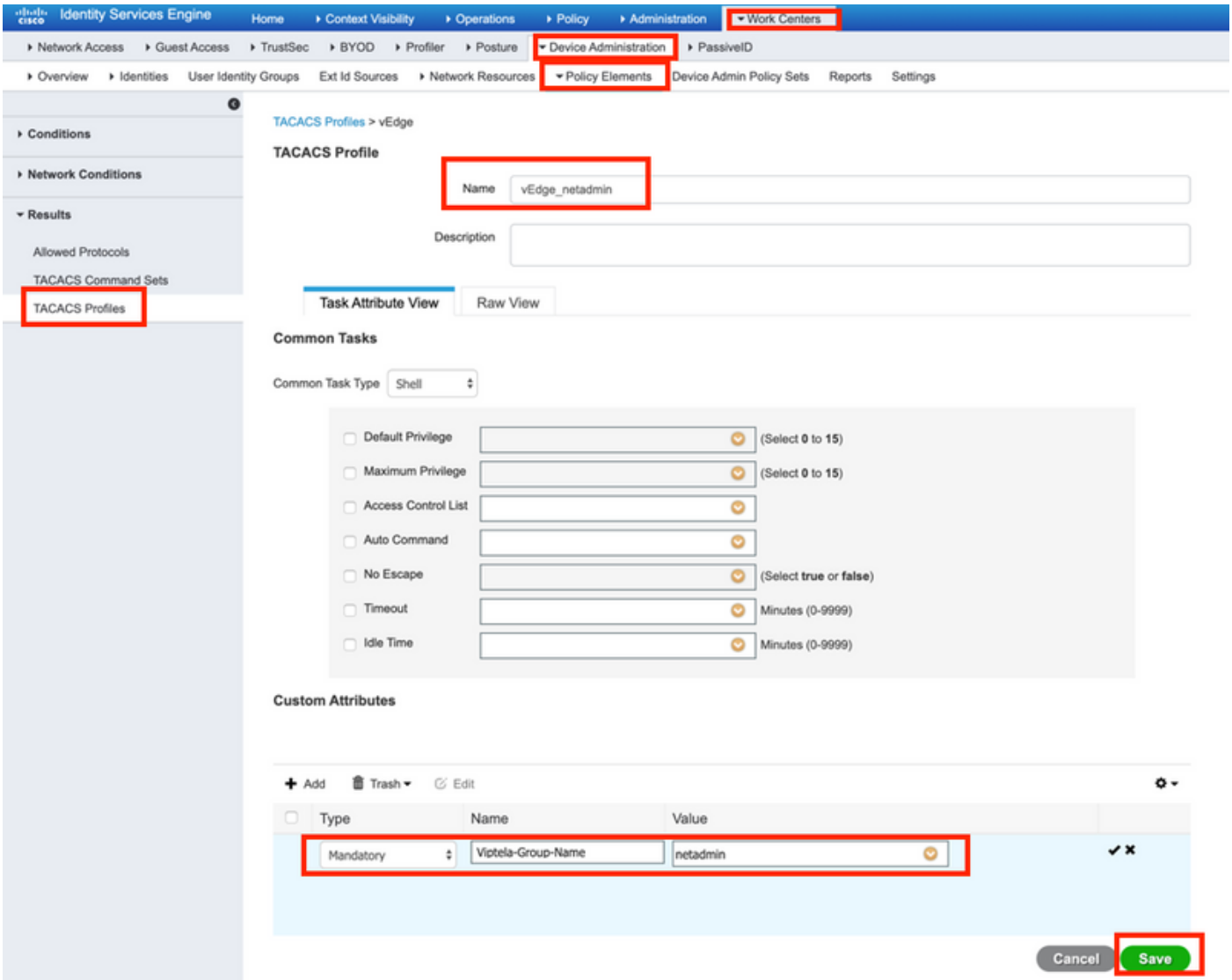
```
vEdgeCloud1# show users

                                                    AUTH
SESSION  USER      CONTEXT  FROM          PROTO  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

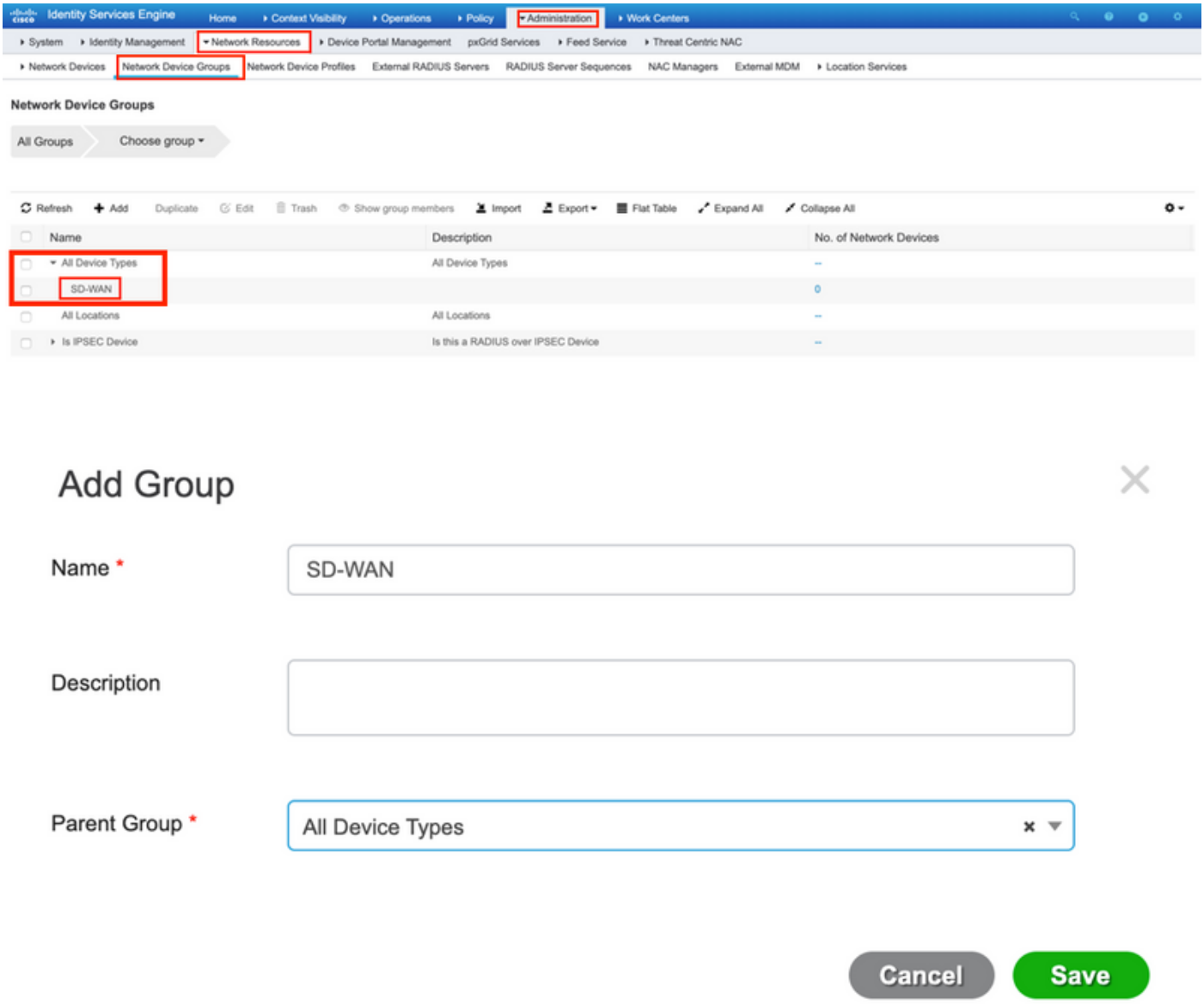
Passaggio 1. Creare un profilo TACACS. In questo passaggio, il profilo TACACS creato viene assegnato, ad esempio, il livello di privilegio netadmin a un utente autenticato.

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

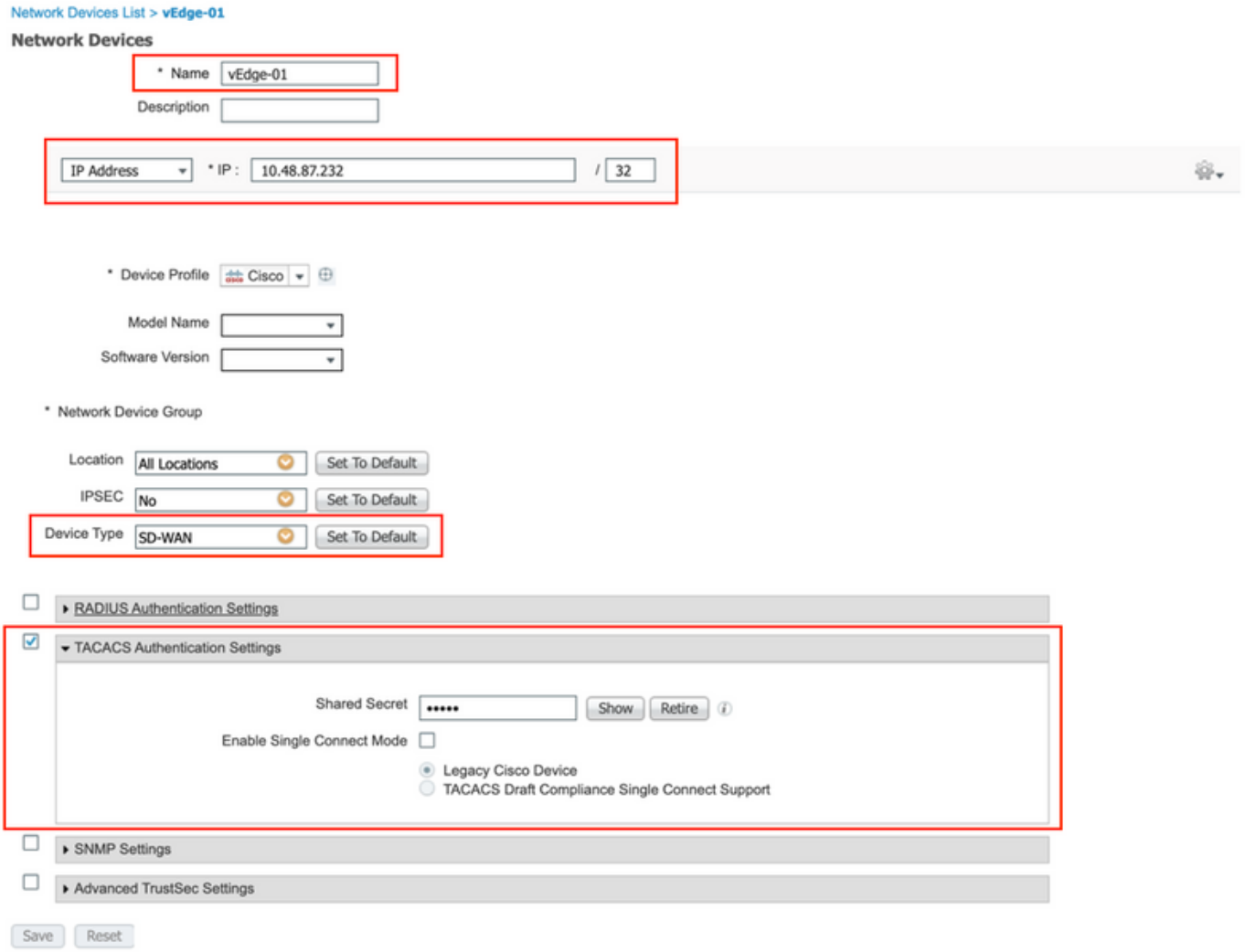
Tipo	Nome	Valore
Obbligatorio	Viptela-Group-Name	netadmin



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

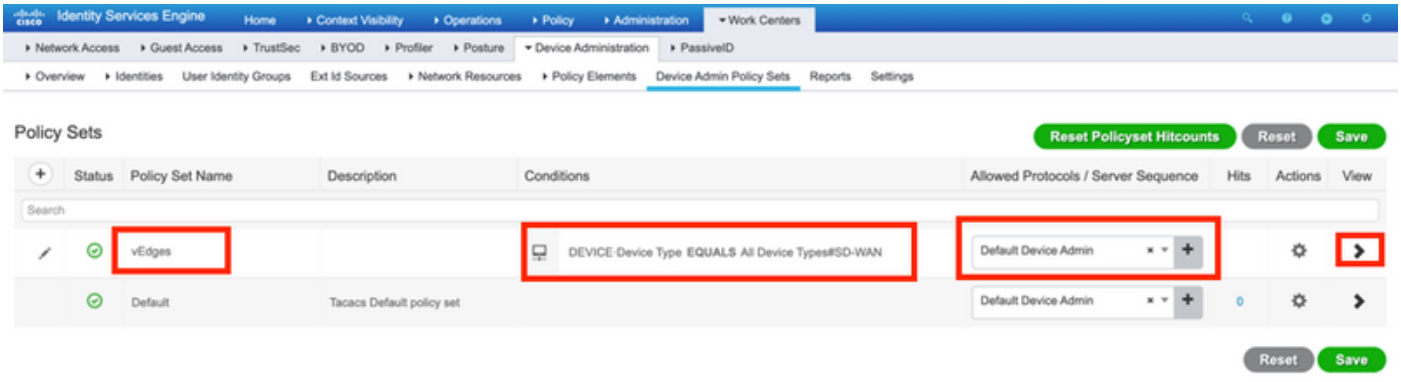


Passaggio 3. Configurare il dispositivo e assegnarlo al gruppo di dispositivi SD-WAN:

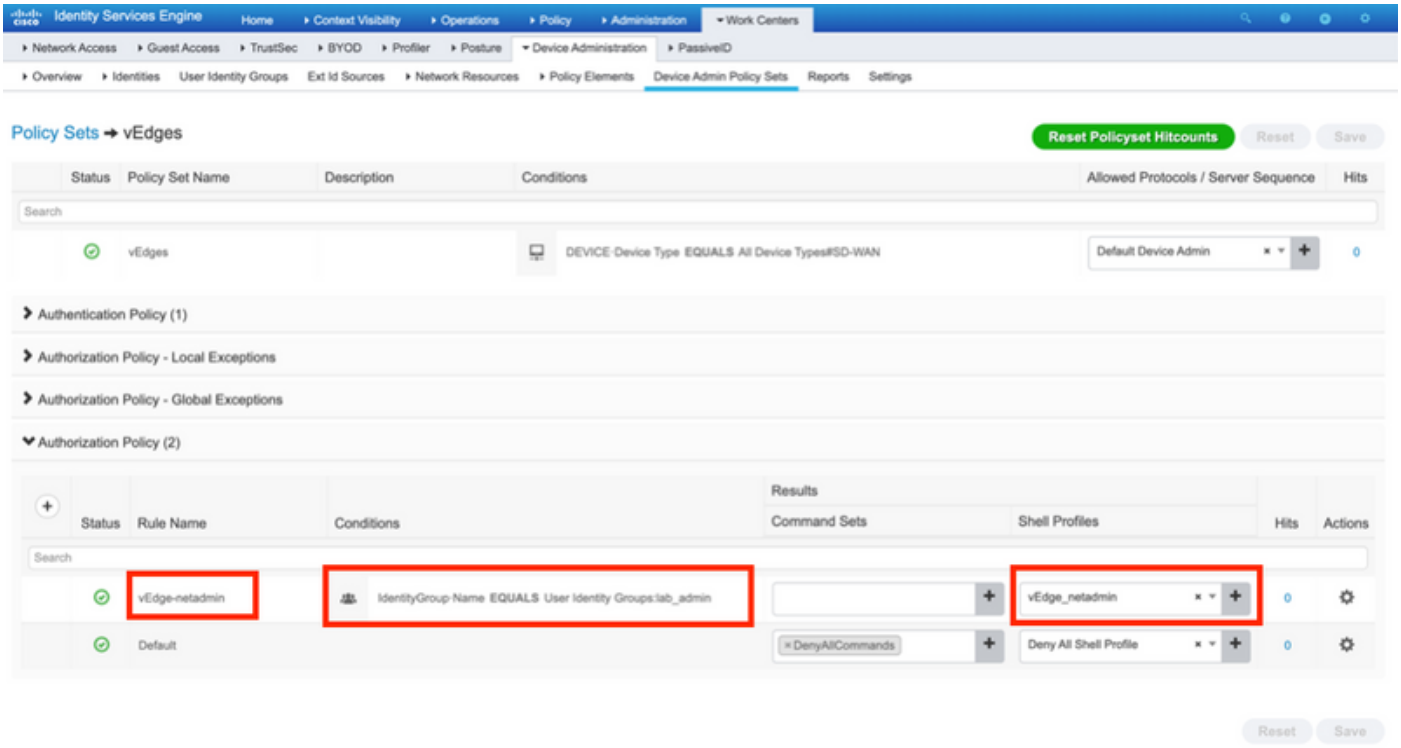


Passaggio 4. Definizione dei criteri di amministrazione dei dispositivi.

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.



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

                                                    AUTH
SESSION  USER      CONTEXT  FROM           PROTO   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