Radius- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit ISE

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie RADIUS- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit Identity Service Engine (ISE) konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Für die Demonstration wurde ISE Version 2.6 verwendet. vEdge-Cloud und Controller mit 19.2.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

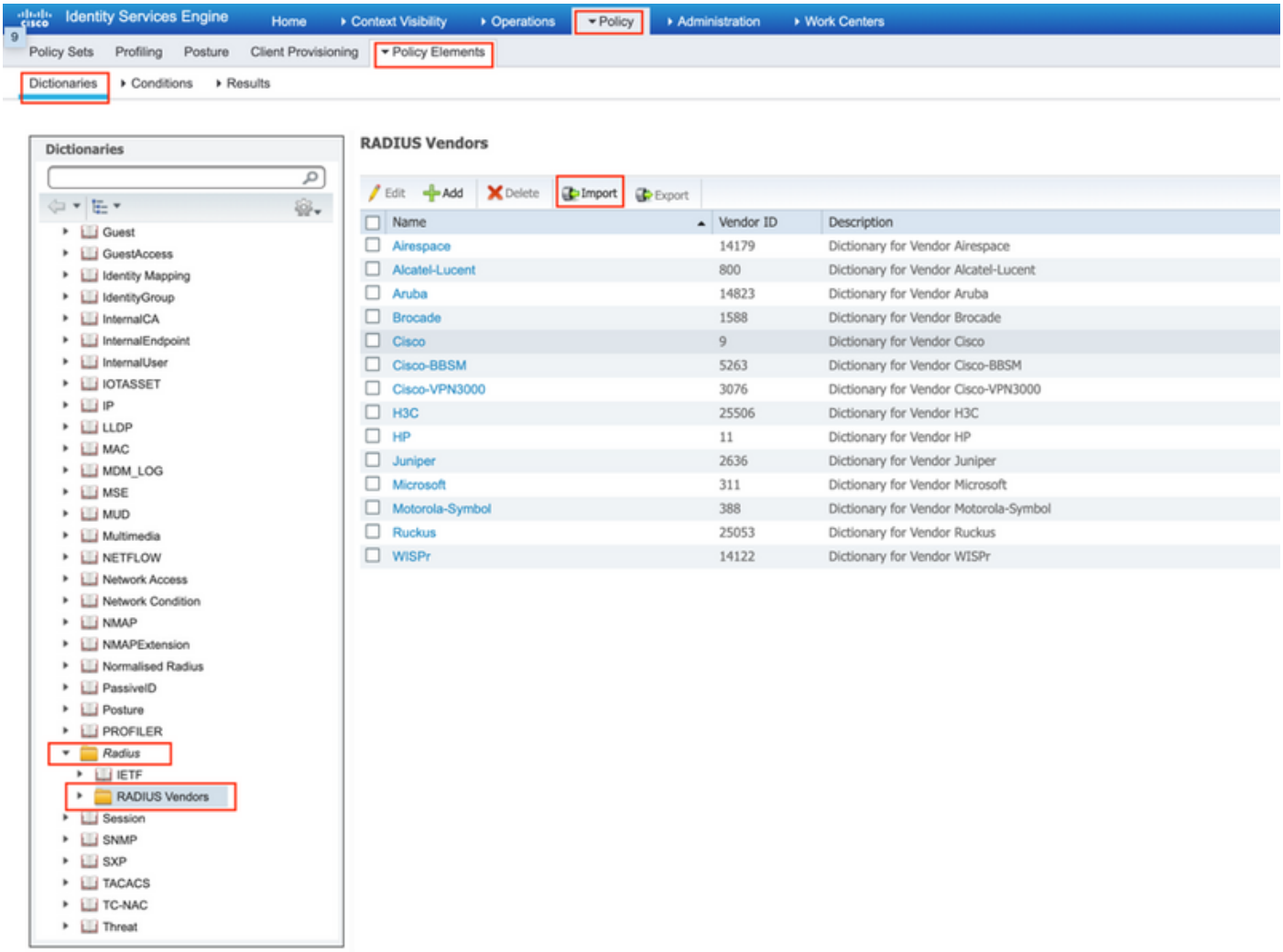
Die Viptela-Software enthält drei feste Benutzergruppennamen: **Basic**, **netadmin** und **operator**. Sie müssen den Benutzer mindestens einer Gruppe zuweisen. Der Benutzer Default TACACS/Radius wird automatisch in die Grundgruppe eingefügt.

Radius-Based User Authentication and Authorization for vEdge and Controllers

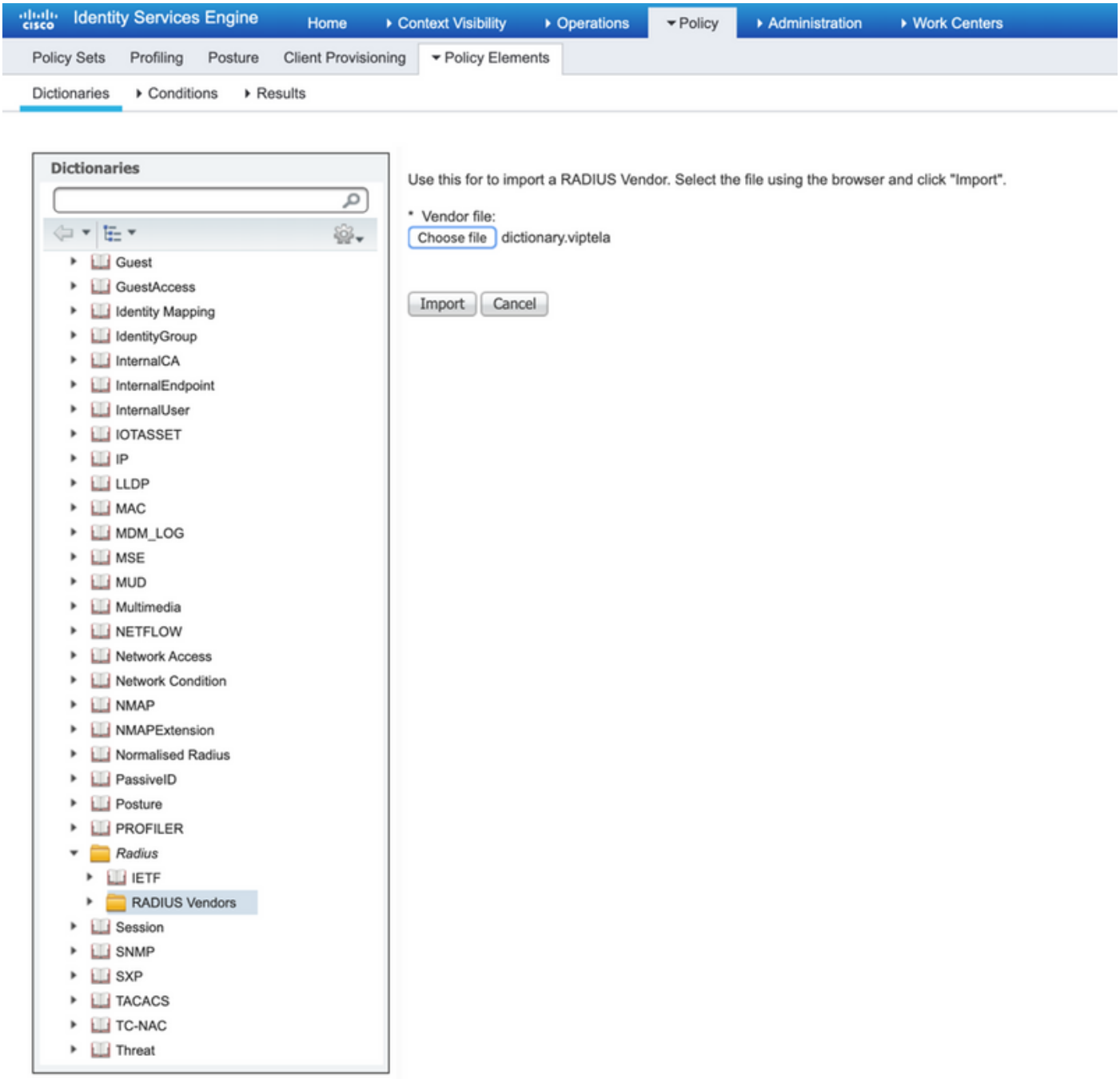
Schritt 1: Erstellen Sie ein Viptela-Radius-Wörterbuch für die ISE. Erstellen Sie dazu eine Textdatei mit dem Inhalt:

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

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1    string
```

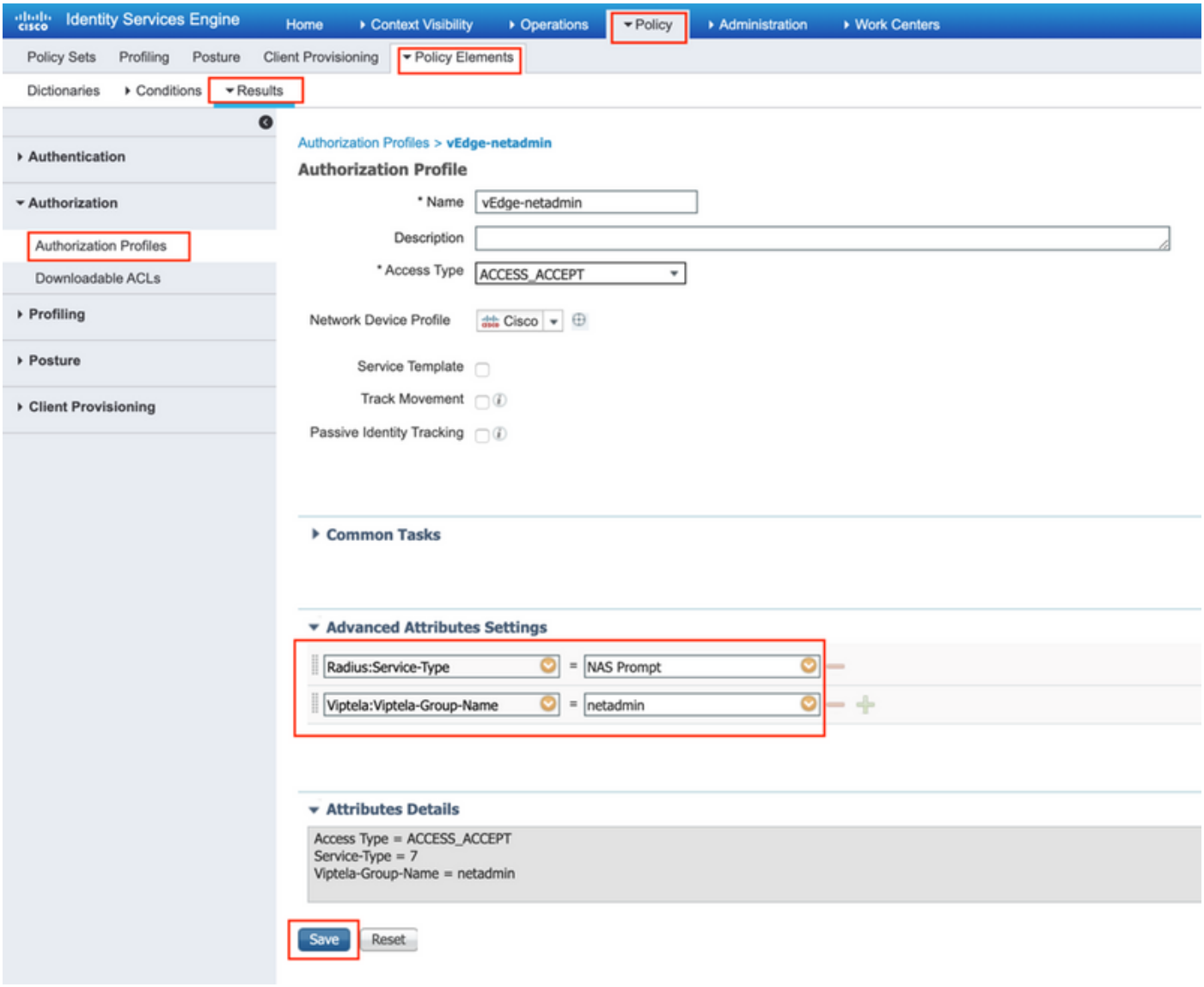
Schritt 2: Wörterbuch auf ISE hochladen Navigieren Sie zu **Richtlinien > Richtlinienelemente > Wörterbücher**. Navigieren Sie in der Liste der Wörterbücher zu **Radius > Radius Vendors** und klicken Sie dann auf **Importieren**, wie im Bild gezeigt.



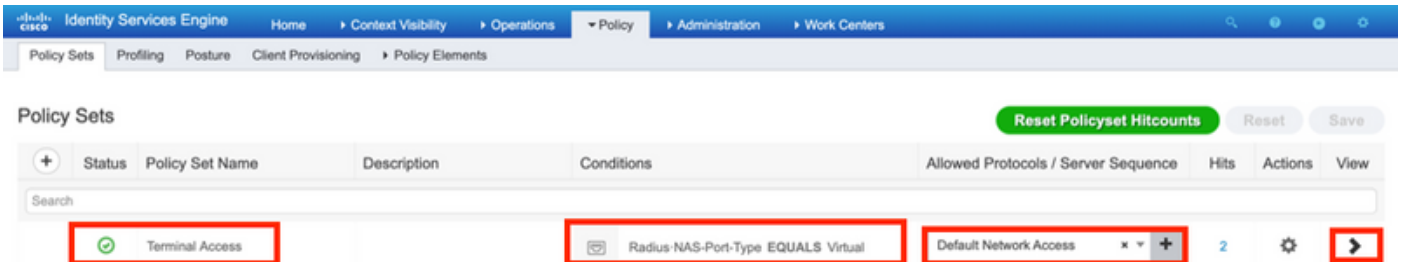
Laden Sie jetzt die Datei hoch, die Sie in Schritt 1 erstellt haben.



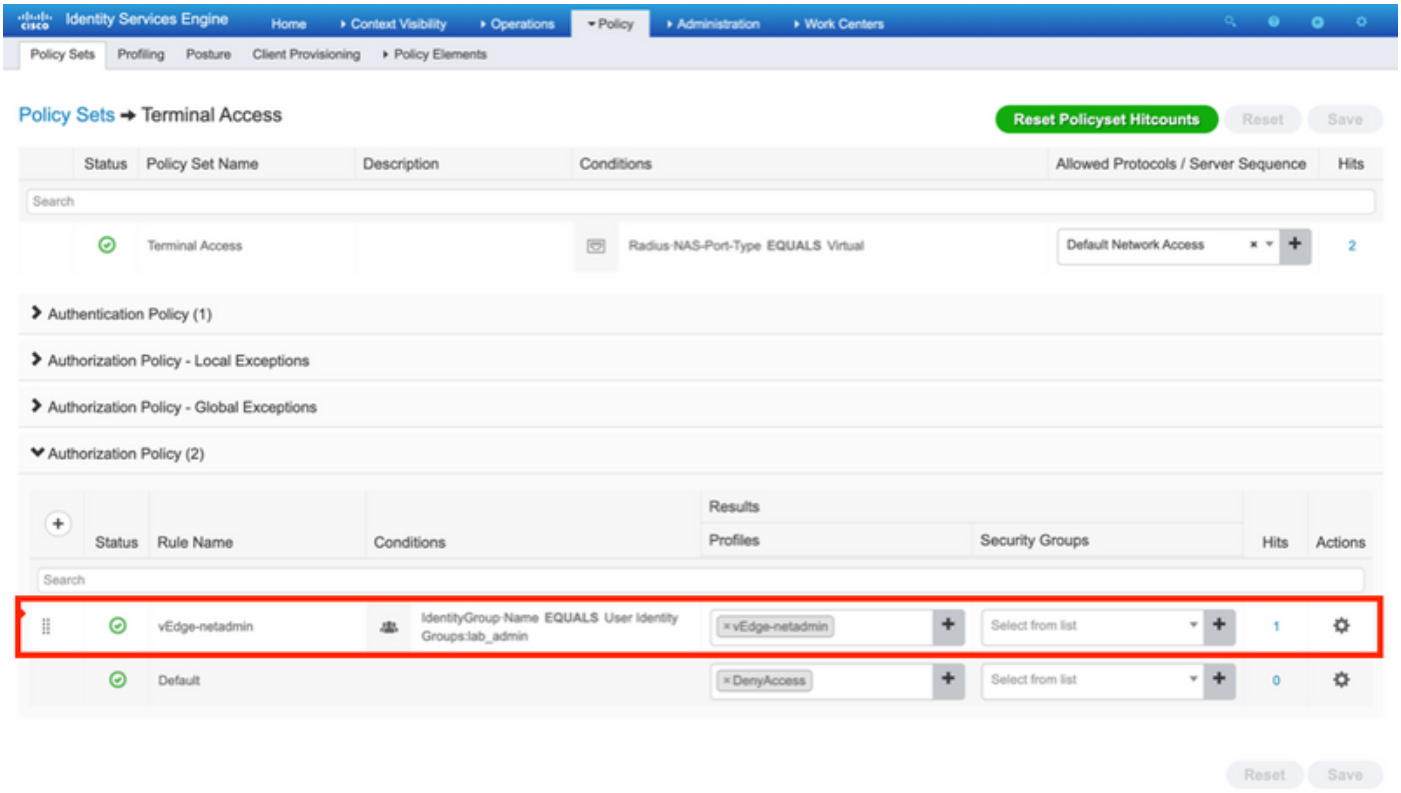
Schritt 3: Erstellen eines Autorisierungsprofils In diesem Schritt weist das Radius-Autorisierungsprofil einem authentifizierten Benutzer beispielsweise die Ebene der Netadmin-Berechtigungen zu. Navigieren Sie hierzu zu **Richtlinien > Richtlinienelemente > Autorisierungsprofile,** und geben Sie zwei erweiterte Attribute an, wie im Bild gezeigt.



Schritt 4: Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtliniensatz möglicherweise anders aus. Für die Demonstration in diesem Artikel wird der Richtlinieneintrag **"Terminalzugriff"** wie im Bild gezeigt erstellt.

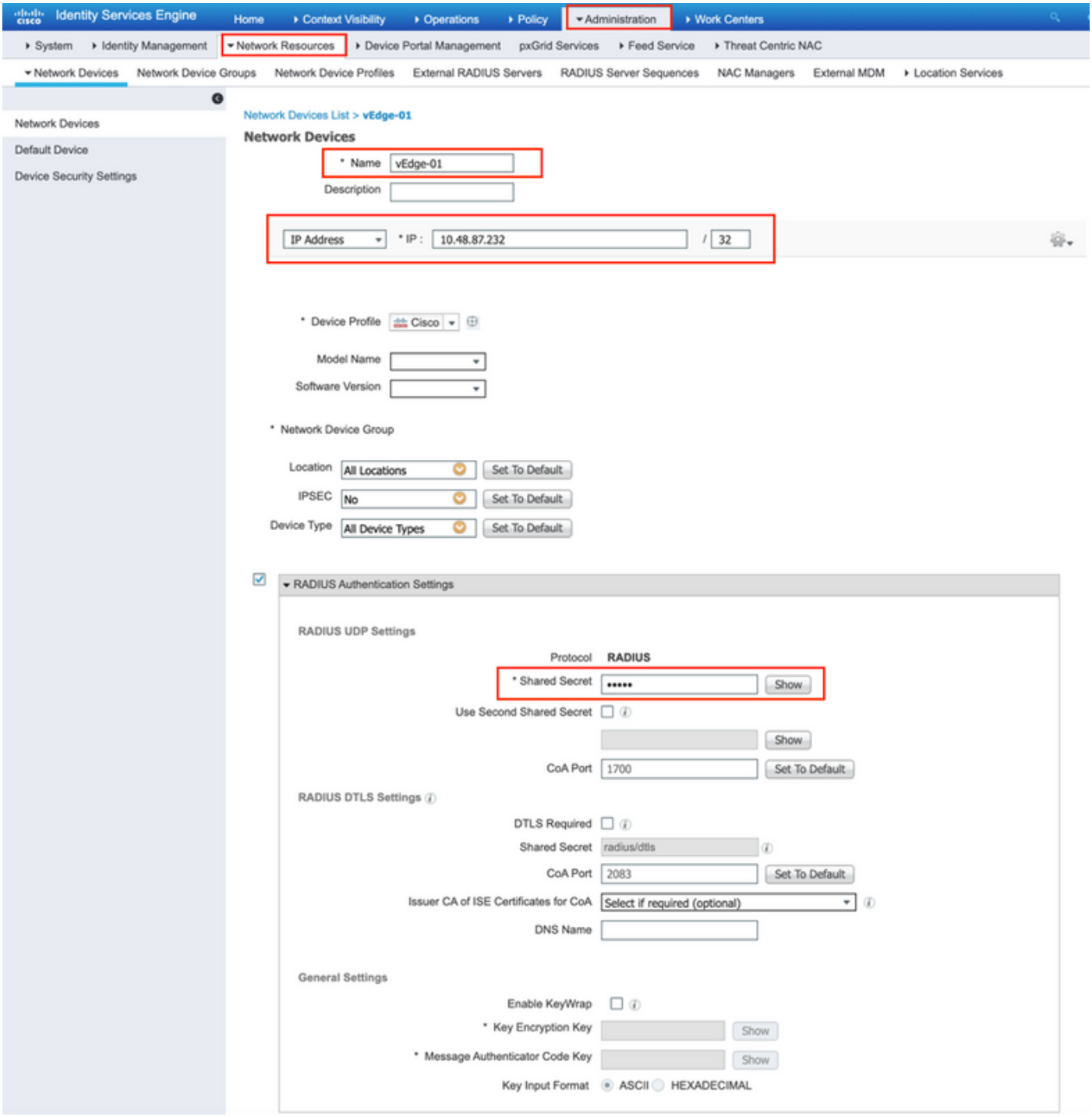


Klicken Sie **>** und der nächste Bildschirm wird angezeigt, wie im Bild gezeigt.



Diese Richtlinie stimmt mit der Benutzergruppe "lab_admin" überein und weist ein in Schritt 3 erstelltes Autorisierungsprofil zu.

Schritt 5: Definieren Sie NAS (vEdge-Router oder Controller), wie im Image gezeigt.



Schritt 6: Konfigurieren Sie vEdge/Controller.

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

Schritt 7: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass dem Remote-Benutzer die Netadmin-Gruppe zugewiesen ist.

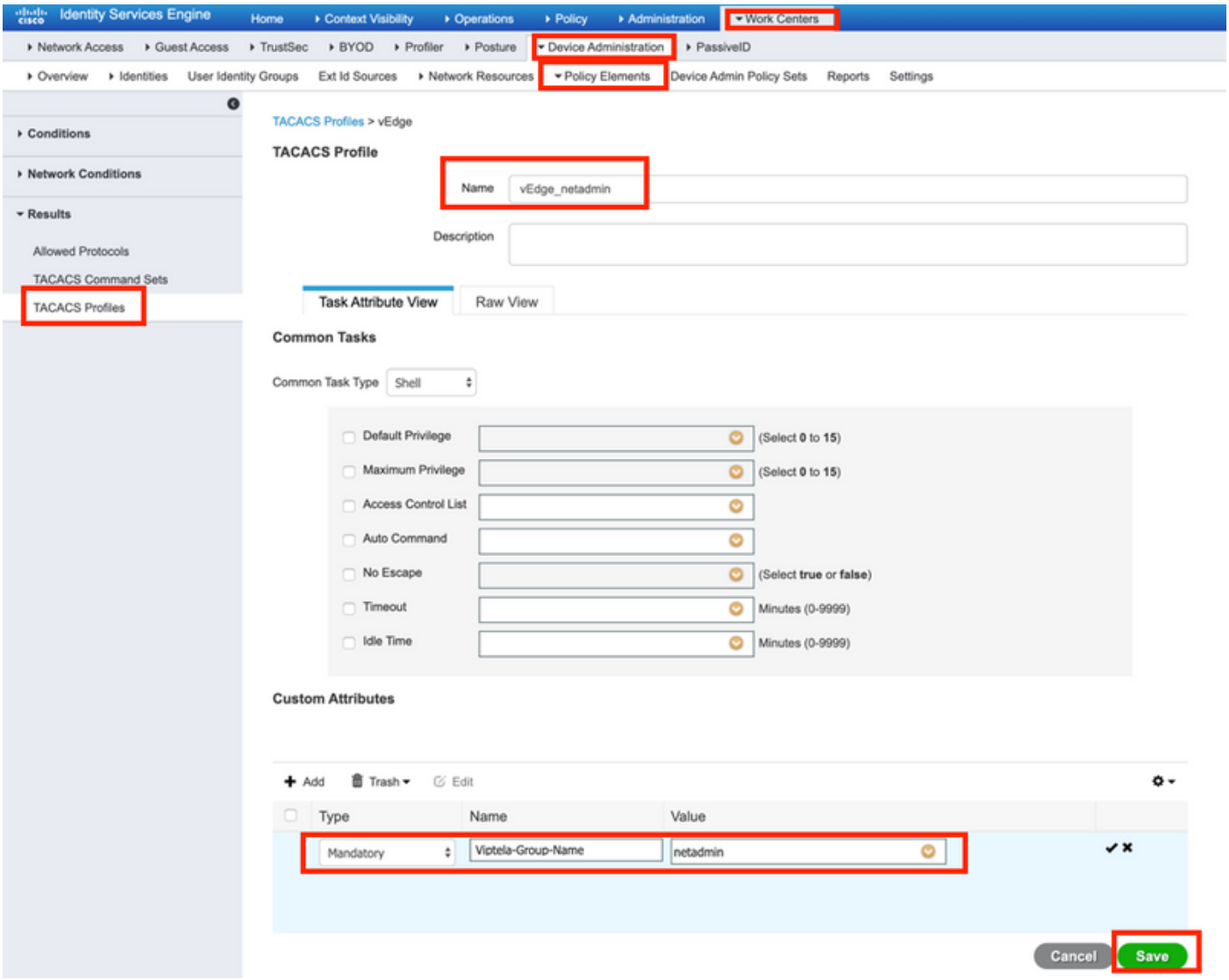
```
vEdgeCloud1# show users

                                                        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
```

TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller

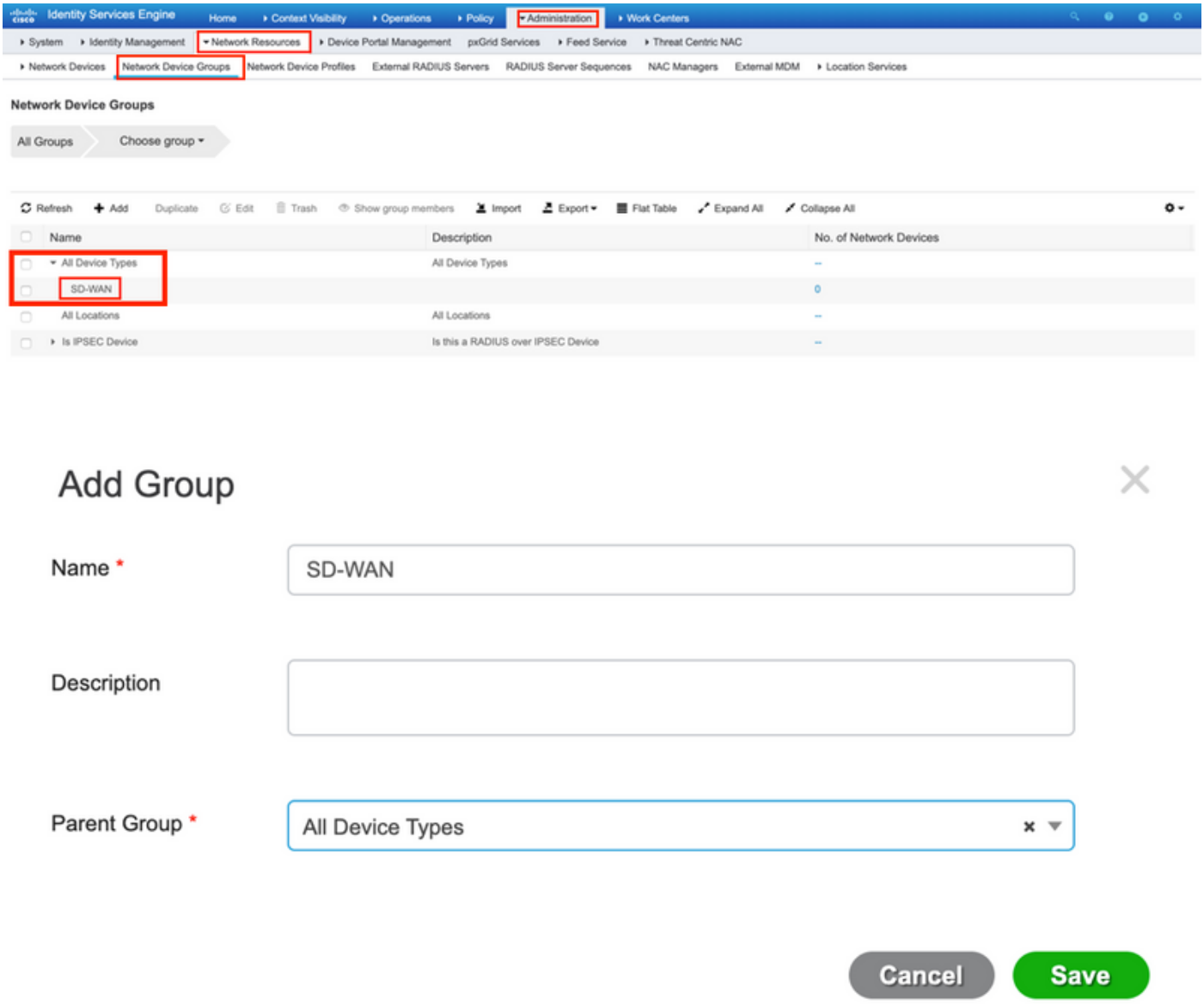
Schritt 1: Erstellen Sie ein TACACS-Profil. In diesem Schritt wird das erstellte TACACS-Profil einem authentifizierten Benutzer zugewiesen, z. B. der Ebene der Netadmin-Berechtigungen.

- Wählen Sie **Obligatorisch** im **Custom-Attribut-**Abschnitt aus, um das Attribut wie folgt hinzuzufügen:

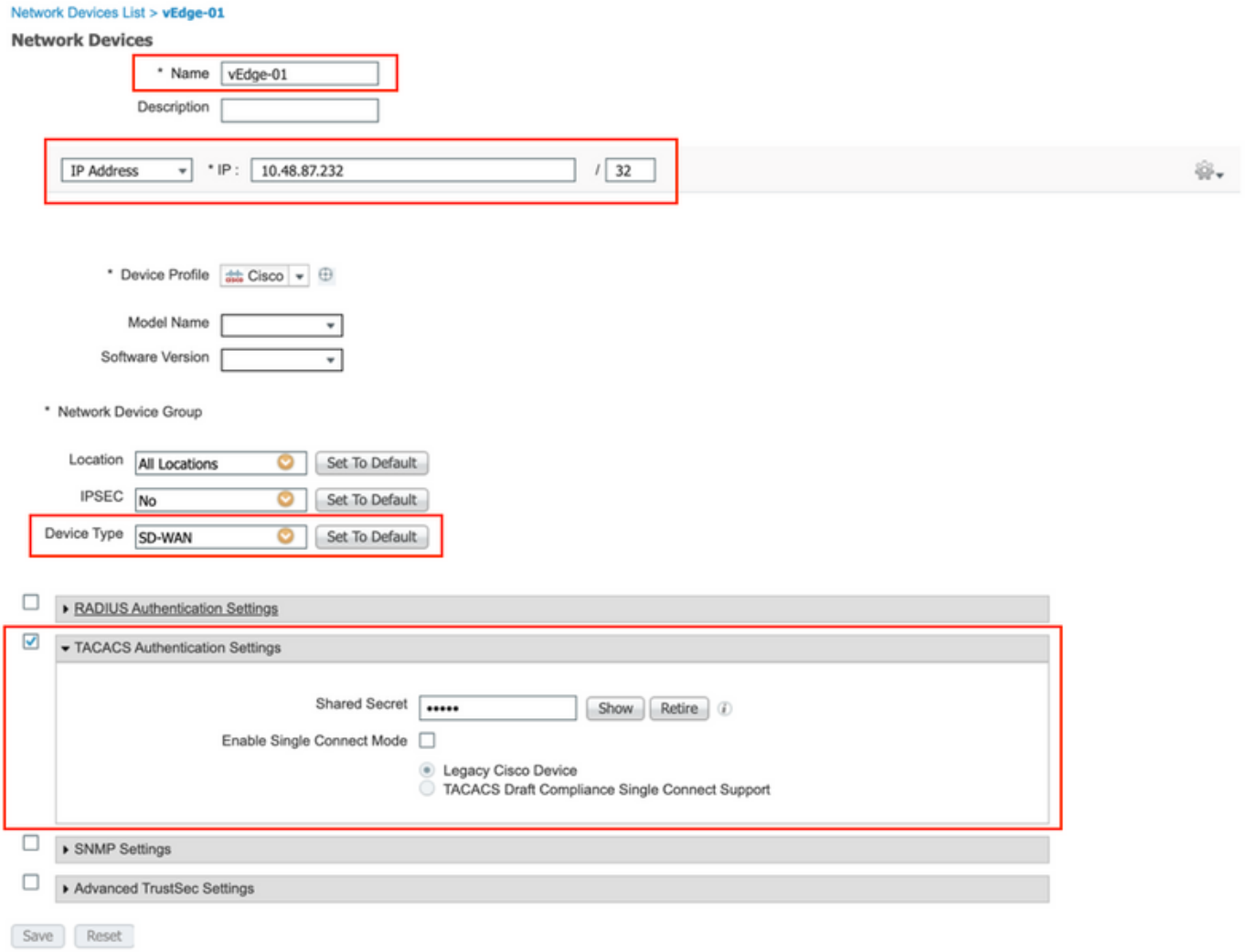
Typ	Name	Wert
Obligatorisch	Viptela-Gruppenname	netadmin



Schritt 2: Erstellen Sie eine Gerätegruppe für SD-WAN.

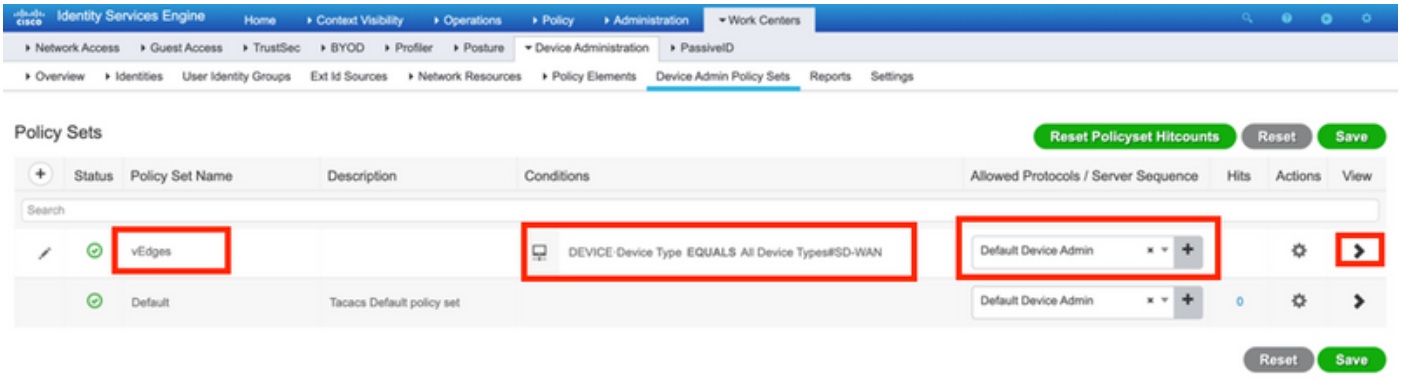


Schritt 3: Konfigurieren Sie das Gerät, und weisen Sie es der SD-WAN-Gerätegruppe zu:

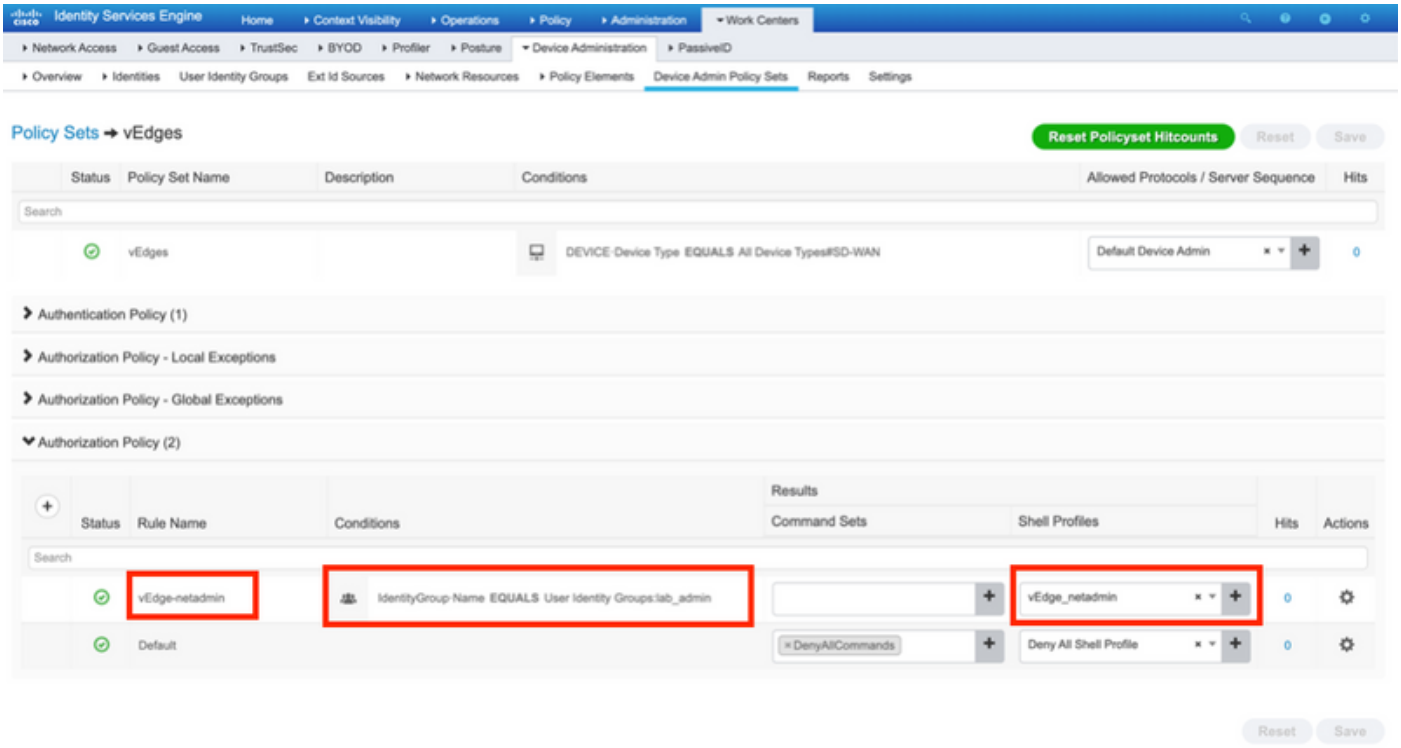


Schritt 4: Definieren Sie die Gerätemanagement-Richtlinie.

Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtliniensatz möglicherweise anders aus. Für die Demonstration in diesem Dokument wird die Richtlinie erstellt.



Klicken Sie auf **>** und der nächste Bildschirm wird angezeigt, wie in diesem Bild gezeigt. Diese Richtlinie stimmt mit dem Gerätetyp **SD-WAN** überein und weist dem in Schritt 1 erstellten Shell-Profil das entsprechende Shell-Profil zu.



Schritt 5: Konfigurieren Sie vEdge:

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

Schritt 6: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass der Remote-Benutzer zugewiesene Netadmin-Gruppe:

```
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
```

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

Zugehörige Informationen

- Cisco ISE Device Administration-Prescriptive Deployment-Guide: https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973
- Konfigurieren von Benutzerzugriff und Authentifizierung: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication