

RADIUS- en TACACS-gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Radius-gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers](#)

[Op TACACS gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u op Radius en TACACS gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers met Identity Services Engine (ISE) kunt configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Voor de demonstratie werd ISE versie 2.6 gebruikt. vEdge-cloud en controllers die lopen 19.2.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

De Viptela-software biedt drie vaste gebruikersgroepnamen: **basis**, **netadmin** en **operator**. U moet de gebruiker aan ten minste één groep toewijzen. De standaardgebruiker TACACS/Straal wordt automatisch in de basisgroep geplaatst.

Radius-gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers

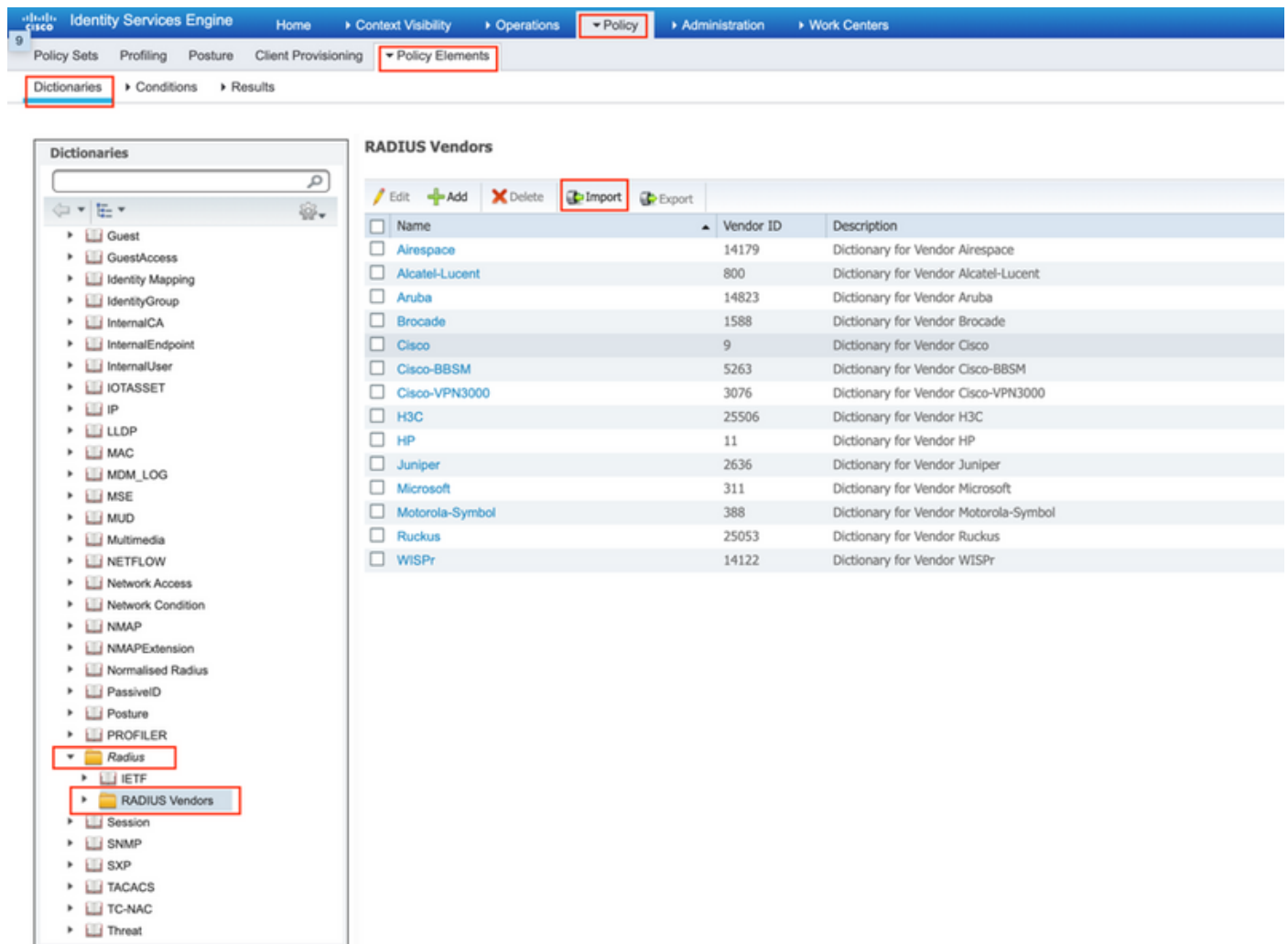
Stap 1. Maak een Straalwoordenboek van Viptela voor ISE. U maakt daarom een tekstbestand met de inhoud:

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

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name          1      string
```

Stap 2. Upload woordenboek op ISE. navigeren in dit geval naar **Beleids-elementen > Beleids-elementen > Woordenboeken**. In de lijst met woordenboeken navigeren we nu naar **Straal > Straal verkopers** en vervolgens klikt u op **Importeren**, zoals in de afbeelding.



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' sidebar on the left is expanded to show 'RADIUS' and 'RADIUS Vendors'. The 'RADIUS Vendors' table is displayed with the following data:

| 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 |

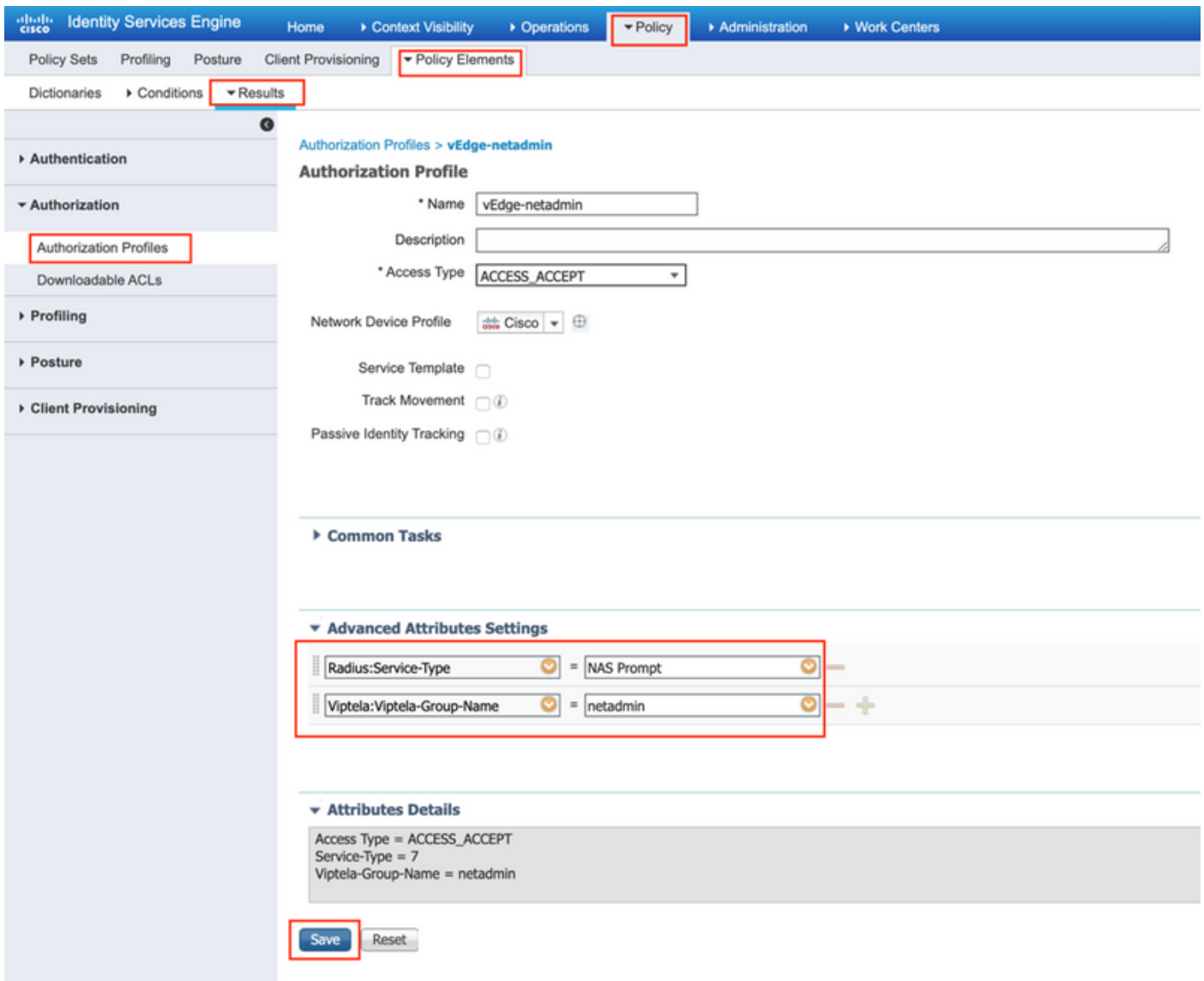
Upload nu het bestand dat u op stap 1 hebt gemaakt.



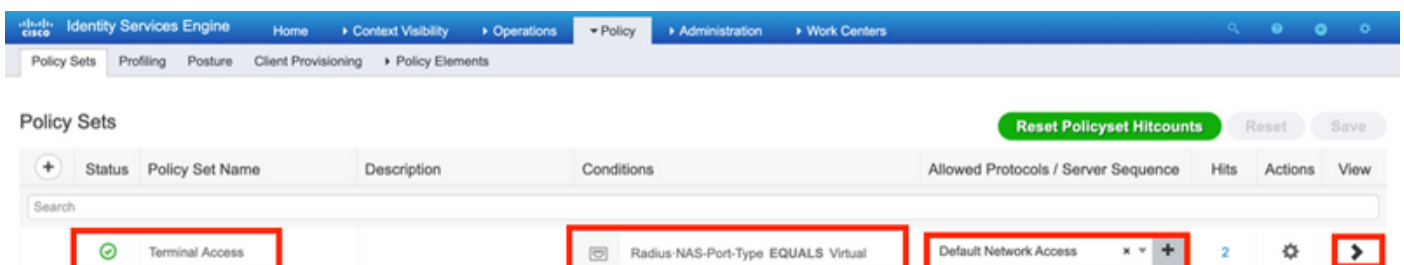
Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

* Vendor file:
 dictionary.viptela

Stap 3. Maak een vergunningsprofiel. In deze stap wijst het Radius autorisatieprofiel bijvoorbeeld het niveau van de netadmin-bevoorrechte rechten toe aan een geauthentiseerde gebruiker. Blader hiervoor naar **Beleidselementen > Gegevens over autorisatie** en specificeer twee geavanceerde eigenschappen zoals in de afbeelding.



Stap 4. Afhankelijk van uw eigenlijke instellingen kan uw beleidsset er anders uitzien. Ten behoeve van de demonstratie in dit artikel wordt het beleidsonderdeel **Terminaltoegang** gecreëerd zoals in de afbeelding.



Klik op > en het volgende scherm verschijnt zoals in de afbeelding.

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

Dit beleid komt overeen op basis van gebruikersgroep lab_admin en wijst een autorisatieprofiel toe dat in Stap 3 werd gemaakt.

Stap 5. Definieer NAS (vEdge-router of controller) zoals in de afbeelding.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources (highlighted), Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The sub-menu includes Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services.

The 'Network Devices' section is active, showing a list with 'vEdge-01'. The configuration form for 'vEdge-01' includes:

- Name: vEdge-01
- Description: (empty)
- IP Address: 10.48.87.232 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)

The 'RADIUS Authentication Settings' section is expanded, showing:

- RADIUS UDP Settings:** Protocol: RADIUS; Shared Secret: (masked); Use Second Shared Secret: (unchecked); CoA Port: 1700 (Set To Default).
- RADIUS DTLS Settings:** DTLS Required: (unchecked); Shared Secret: radius/dtls; CoA Port: 2083 (Set To Default); Issuer CA of ISE Certificates for CoA: Select if required (optional); DNS Name: (empty).
- General Settings:** Enable KeyWrap: (unchecked); Key Encryption Key: (masked); Message Authenticator Code Key: (masked); Key Input Format: ASCII (selected).

Stap 6. Configureer vEdge/controller.

```

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

```

Stap 7. Verificatie. Meld u aan bij vEdge en controleer of er een netwerkbeheergroep is toegewezen aan de externe gebruiker.

```
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 |

Op TACACS gebaseerde gebruikersverificatie en -autorisatie voor vEdge en controllers

Stap 1. Maak een TACACS-profiel. In deze stap wordt het TACACS-profiel dat is gemaakt, bijvoorbeeld een netadmin-voorkeursniveau toegewezen aan een geauthentiseerde gebruiker.

- Selecteer **Verplicht** uit het gedeelte **Aangepaste eigenschap** om de eigenschap toe te voegen als:

| Type | Name | Waarde |
|-----------|--------------------|--------------|
| Verplicht | Viptela-groepsnaam | netbeheerder |

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a TACACS profile. The interface is divided into several sections:

- Navigation:** The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' menu is expanded, showing 'Device Administration' and 'PassiveID'. The 'Policy Elements' sub-menu is also expanded, showing 'Device Admin Policy Sets', 'Reports', and 'Settings'.
- Left Sidebar:** The sidebar shows 'Conditions', 'Network Conditions', 'Results', 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles' (highlighted).
- Main Content Area:**
 - TACACS Profile:** The 'Name' field is set to 'vEdge_netadmin'.
 - Task Attribute View:** The 'Common Task Type' is set to 'Shell'.
 - Common Tasks:** A list of tasks with checkboxes and dropdown menus for configuration, including 'Default Privilege', 'Maximum Privilege', 'Access Control List', 'Auto Command', 'No Escape', 'Timeout', and 'Idle Time'.
 - Custom Attributes:** A table with columns for 'Type', 'Name', and 'Value'. A new attribute is added with 'Type' set to 'Mandatory', 'Name' set to 'Viptela-Group-Name', and 'Value' set to 'netadmin'.
- Buttons:** 'Cancel' and 'Save' buttons are located at the bottom right.

Stap 2. Maak een apparaatgroep voor 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 |
|--|------------------------------------|------------------------|
| ▾ 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

Stap 3. Configureer het apparaat en verdeel het aan het SD-WAN apparaatgroep:

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

Stap 4. Bepaal het beleid voor apparaatbeheer.

Afhankelijk van uw eigenlijke instelling kan uw beleidsset er anders uitzien. Met het oog op de demonstratie in dit document wordt het beleid opgericht.

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"/> | |

Klik op > en het volgende scherm verschijnt zoals in deze afbeelding. Dit beleid past op apparaat type aan dat **SD-WAN** heet en wijst het Shell profiel toe dat in stap 1 wordt gemaakt.

Policy Sets → vEdges

Reset Policyset Hitcounts Reset Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | |
|---|-----------------|----------------|--|-------------------------------------|------|---------|
| ✓ | vEdges | | DEVICE Device Type EQUALS All Device Types#SO-WAN | Default Device Admin | 0 | |
| <p>Authentication Policy (1)</p> <p>Authorization Policy - Local Exceptions</p> <p>Authorization Policy - Global Exceptions</p> <p>Authorization Policy (2)</p> | | | | | | |
| + | Status | Rule Name | Conditions | Results | Hits | Actions |
| | ✓ | vEdge-netadmin | IdentityGroup Name EQUALS User Identity Groups:lab_admin | vEdge_netadmin | 0 | ⚙️ |
| | ✓ | Default | | Deny All Shell Profile | 0 | ⚙️ |

Reset Save

Stap 5. Configuratie vEdge:

```

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

```

Stap 6. Verificatie. Meld u aan bij vEdge en controleer of er een netwerkbeheergroep is toegewezen aan een externe gebruiker:

```
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 |

Stap 5. Configuratie vEdge:

Stap 5. Configuratie vEdge:

Stap 5. Configuratie vEdge:

Gerelateerde informatie

- Cisco ISE-handleiding voor adaptieve implementatie van apparaat: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- Gebruikerstoegang en -verificatie configureren: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication