Radius and TACACS-Based User Authentication and Authorization for vEdge and Controllers with ISE

Contents

Introduction

This document describes how to configure Radius- and TACACS-based user authentication and authorization for vEdge and controllers with Identity Service Engine (ISE).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

For the purpose of the demonstration, ISE version 2.6 was used. vEdge-cloud and controllers running 19.2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

The Viptela software provides three fixed user group names: **basic**, **netadmin**, and **operator**. You must assign the user to at least one group. The Default TACACS/Radius user is automatically placed in the basic group.

Radius-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a Viptela radius dictionary for ISE. To do so, create a text file with the content:

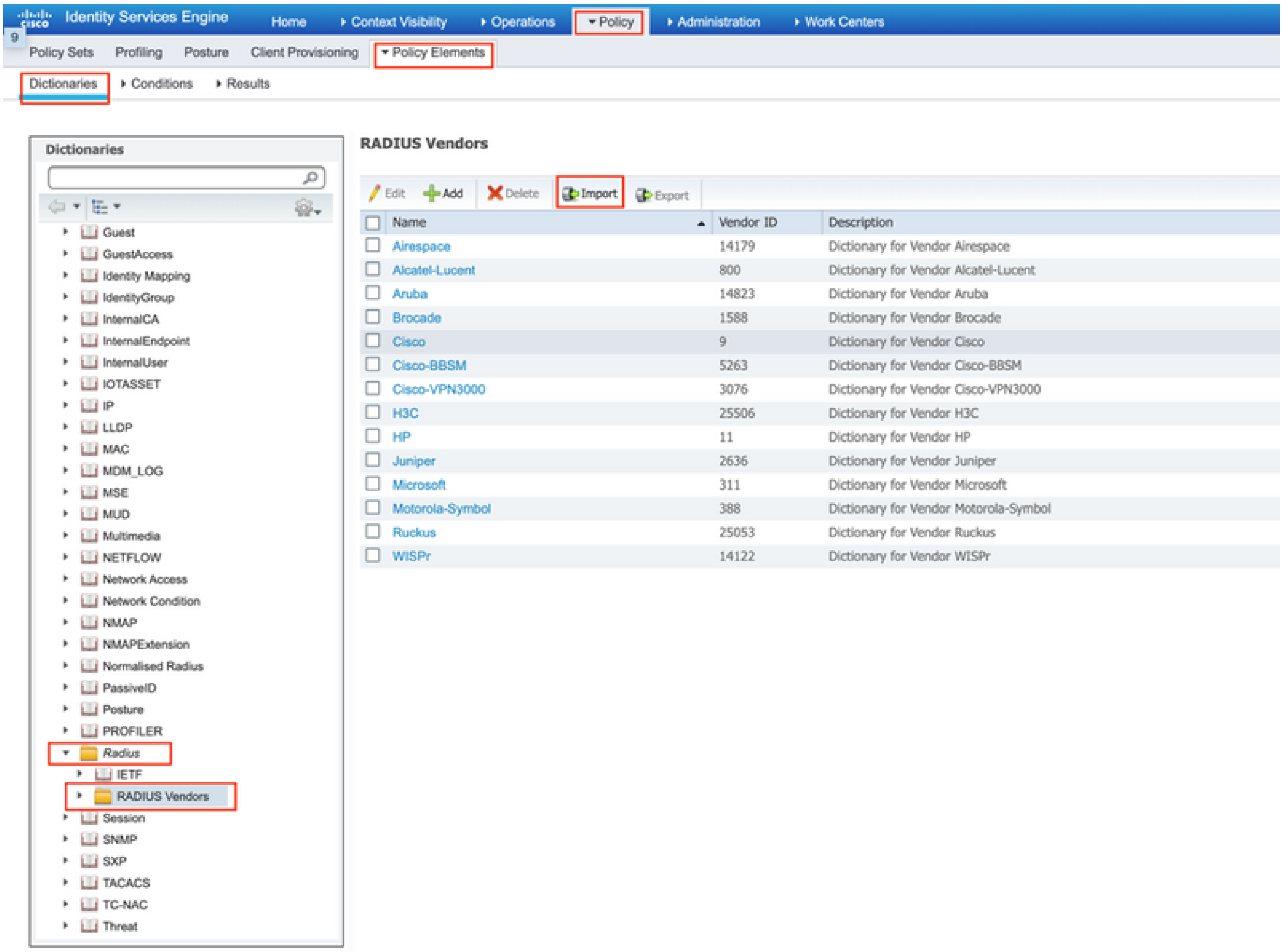
```
# -*- text -*-
#
#  dictionary.viptela
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

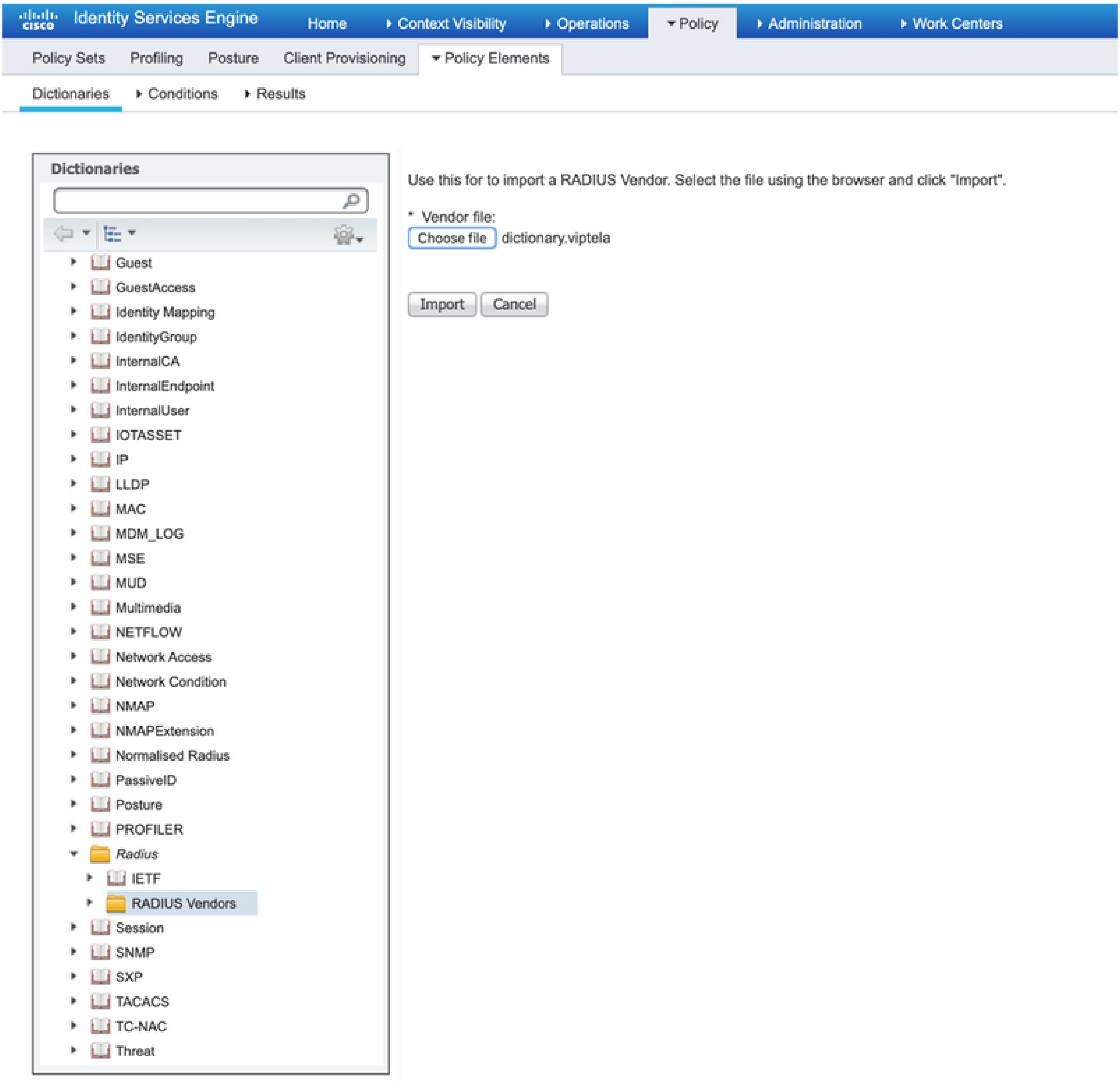
Step 2. Upload dictionary to ISE. For this, navigate to **Policy > Policy Elements > Dictionaries**. From the list of Dictionaries, now navigate to **Radius > Radius Vendors** and then click **Import**, as shown image.



RADIUS Vendors

□	Name	Vendor ID	Description
□	Airespace	14179	Dictionary for Vendor Airespace
□	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

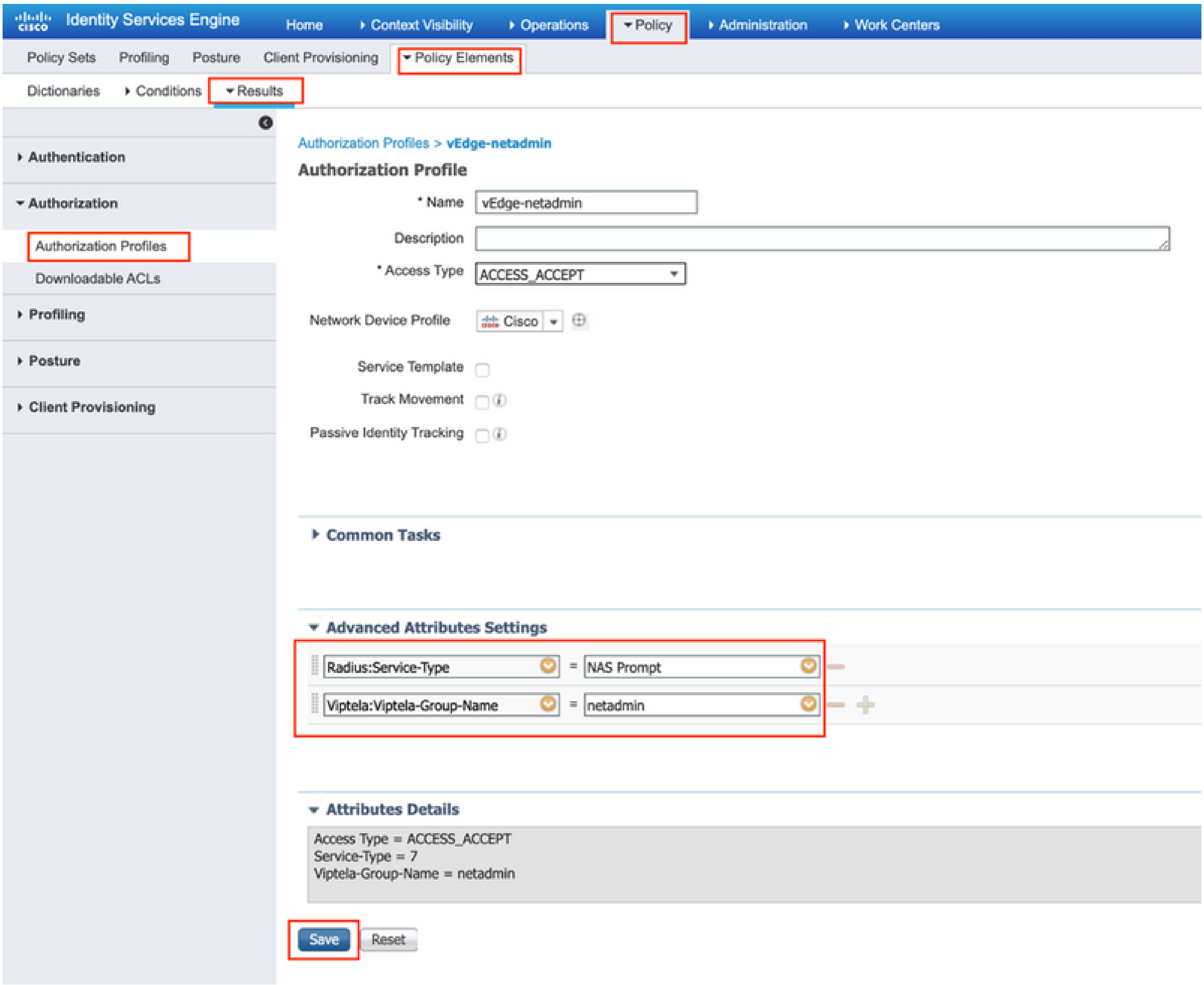
Now upload the file you created on step 1.



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

* Vendor file: dictionary.viptela

Step 3. Create an Authorization Profile. In this step Radius authorization profile assigns, for example, netadmin privilege level to an authenticated user. For this, navigate to **Policy > Policy Elements > Authorization Profiles** and specify two advanced attributes as shown in the image.



Authorization Profiles > vEdge-netadmin

Authorization Profile

* Name: vEdge-netadmin

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Advanced Attributes Settings

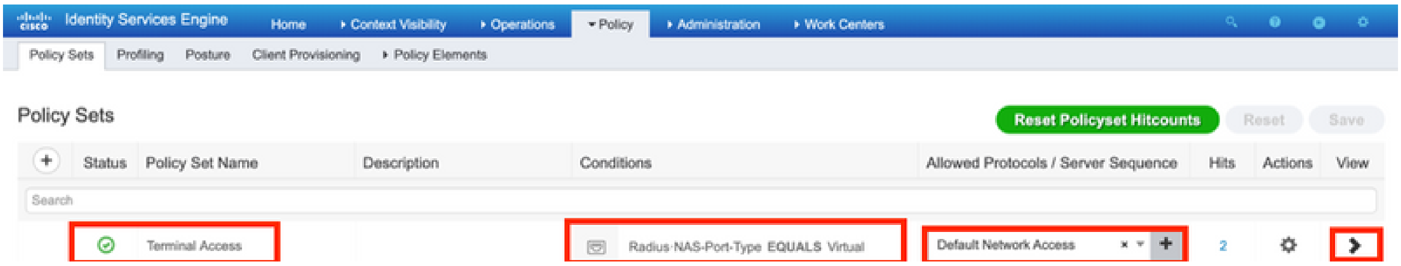
Radius:Service-Type = NAS Prompt

Viptela:Viptela-Group-Name = netadmin

Attributes Details

```
Access Type = ACCESS_ACCEPT
Service-Type = 7
Viptela-Group-Name = netadmin
```

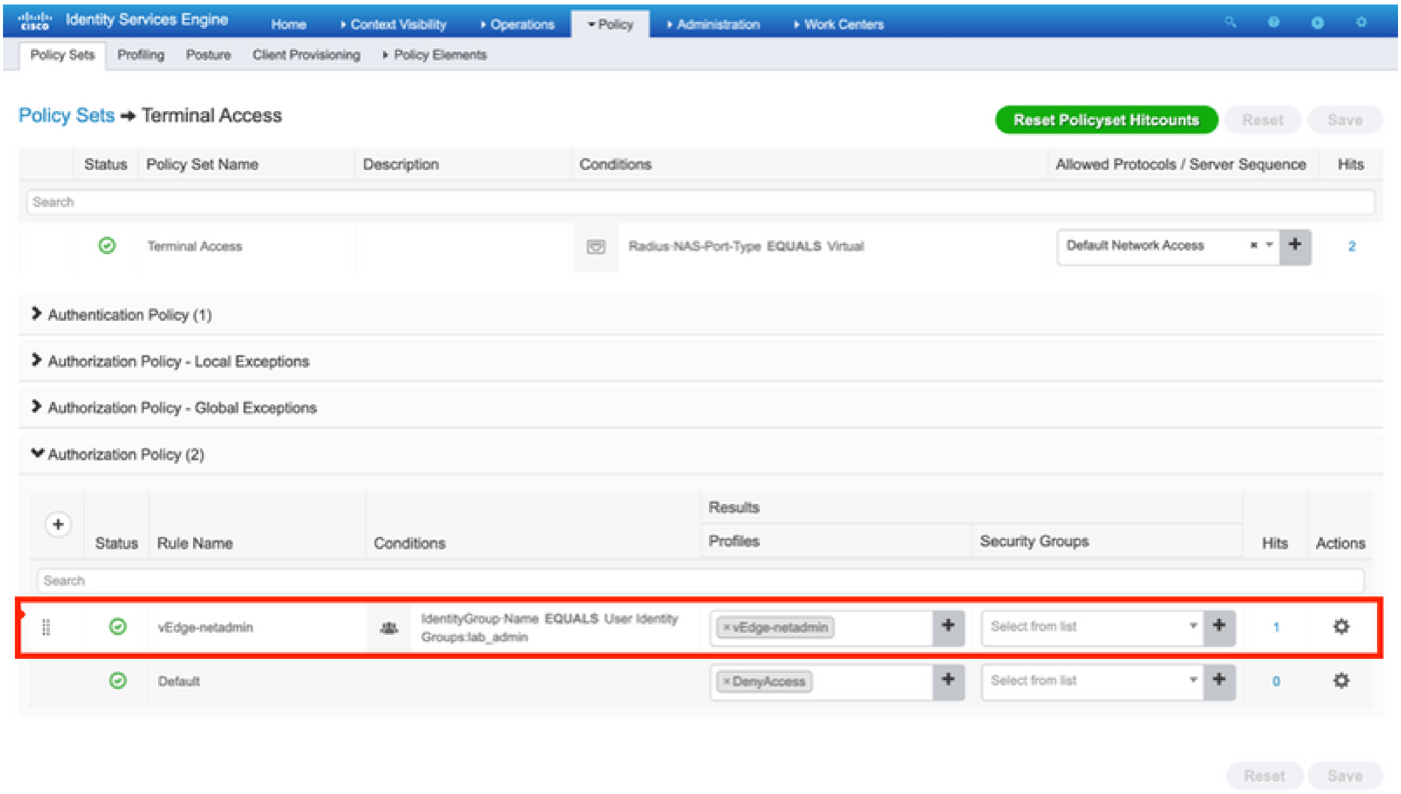
Step 4. Depends on your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this article, the Policy entry called **Terminal Access i**s created as shown in the image.



Policy Sets

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

Click **>** and the next screen appears as shown in the image.



Policy Sets → Terminal Access

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

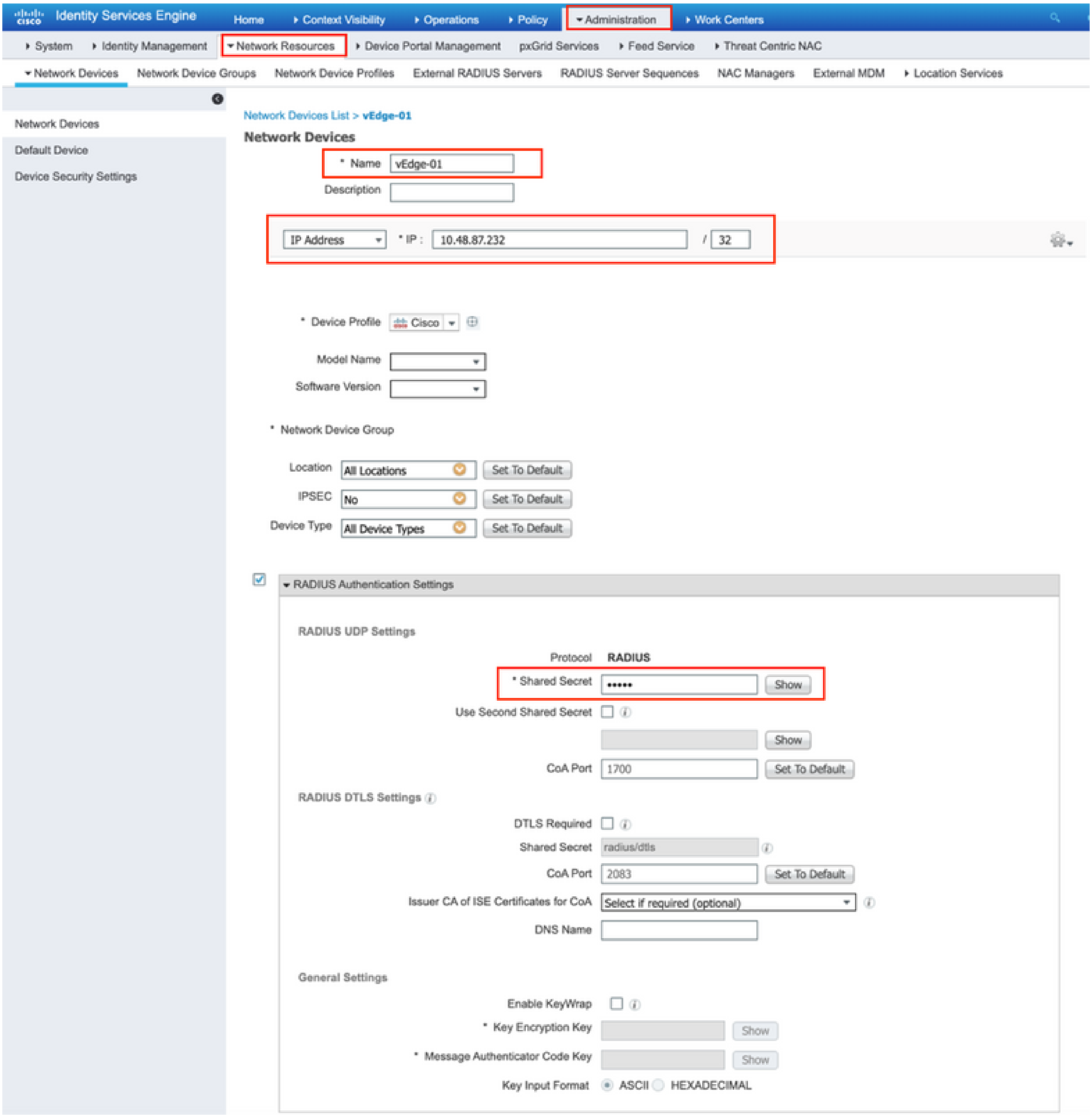
> Authorization Policy - Global Exceptions

⌄ Authorization Policy (2)

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

This policy matches based on user group lab_admin and assigns an authorization profile that was created in Step 3.

Step 5. Define NAS (vEdge router or controller) as shown in the image.



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 All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret •••••

Use Second Shared Secret □

CoA Port 1700

RADIUS DTLS Settings

DTLS Required □

Shared Secret radius/dtls

CoA Port 2083

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

General Settings

Enable KeyWrap □

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

Step 6. Configure vEdge/Controller.

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

Step 7. Verification. Login to vEdge and ensure netadmin group assigned to the remote user.

```
vEdgeCloud1# show users
```

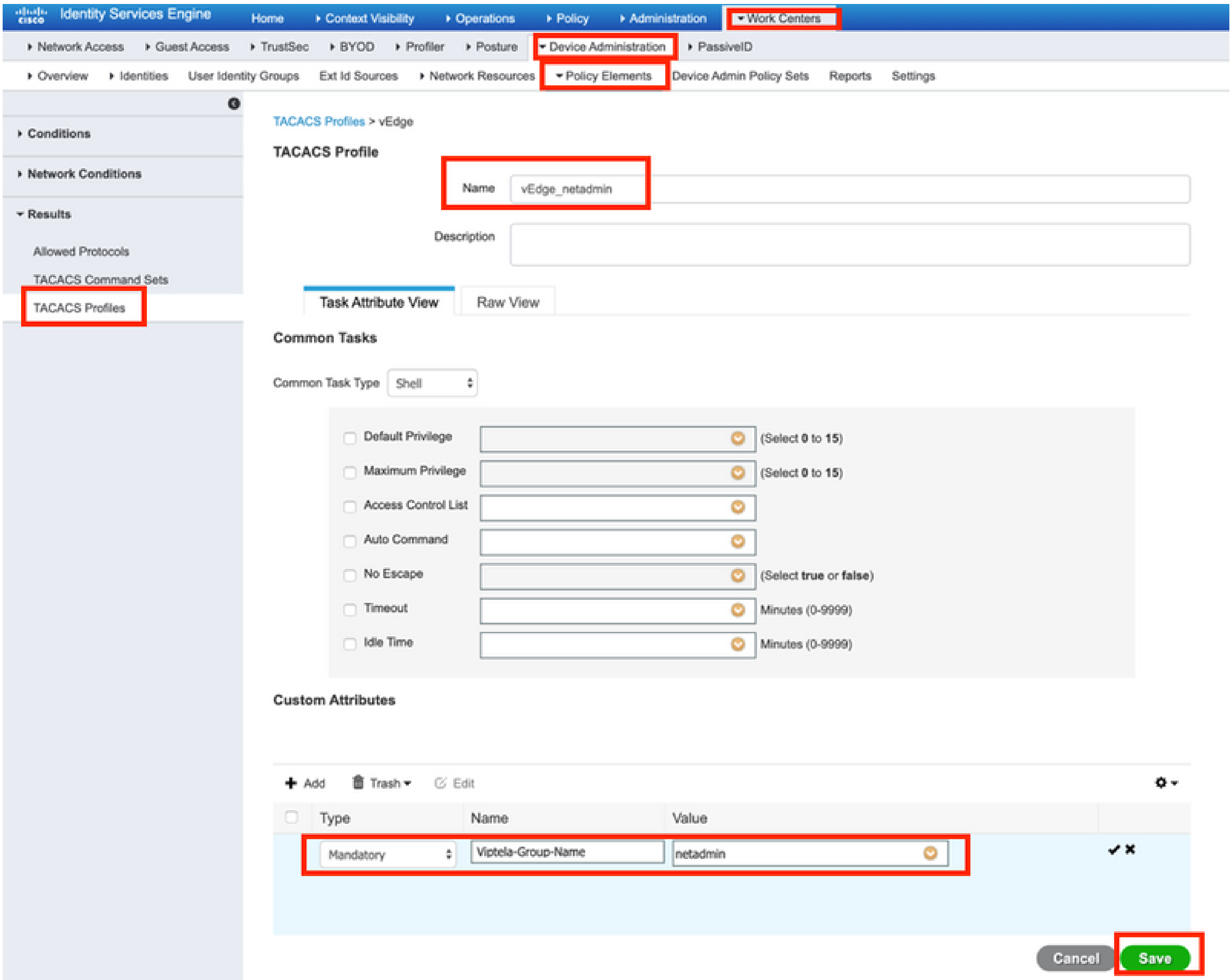
```
                                               AUTH
SESSION  USER      CONTEXT  FROM          PROTO  GROUP      LOGIN TIME
-------------------------------------------------------------------------------------
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin   2020-03-09T18:39:40+00:00
```

TACACS-Based User Authentication and Authorization for vEdge and Controllers

Step 1. Create a TACACS profile. In this step, the TACACS profile created is assigned, for example, netadmin privilege level to an authenticated user.

- Select **Mandatory** from the **Custom attribute** section to add the attribute as:

Type	**Name**	**Value**
Mandatory	Viptela-Group-Name	netadmin



TACACS Profile

Name: vEdge_netadmin

Description:

Common Tasks

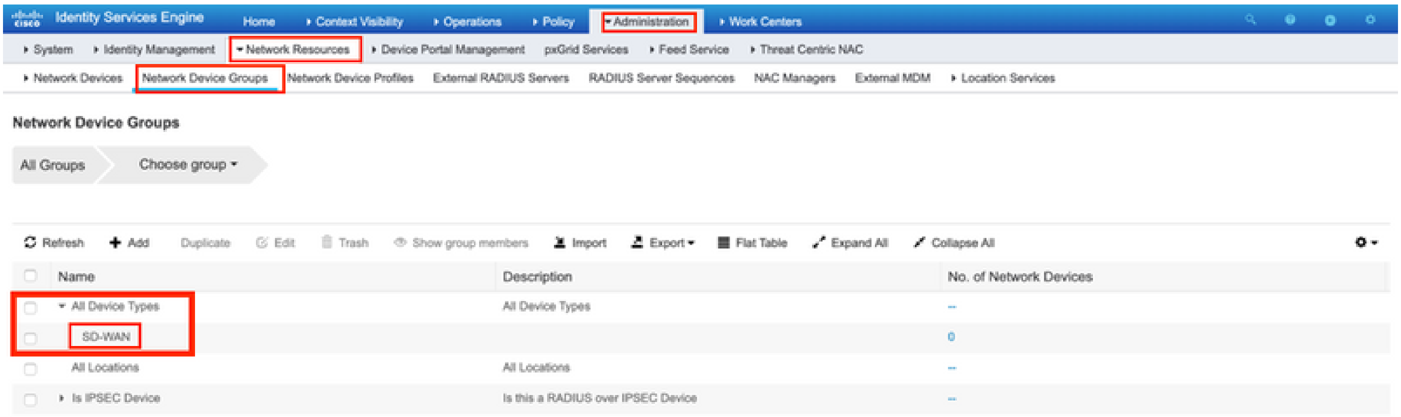
Common Task Type: Shell

□	Default Privilege		(Select 0 to 15)
□	Maximum Privilege		(Select 0 to 15)
□	Access Control List		
□	Auto Command		
□	No Escape		(Select true or false)
□	Timeout		Minutes (0-9999)
□	Idle Time		Minutes (0-9999)

Custom Attributes

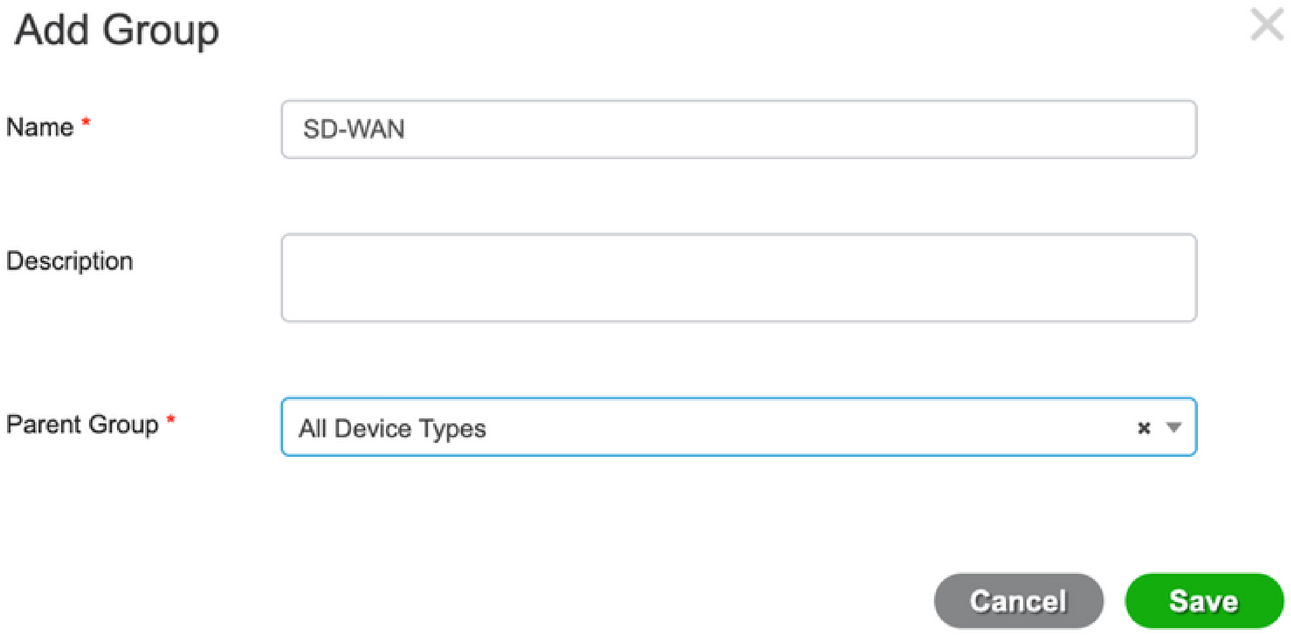
□	Type	Name	Value
	Mandatory	Viptela-Group-Name	netadmin

Step 2. Create a device group for SD-WAN.



Network Device Groups

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
SD-WAN		0
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--



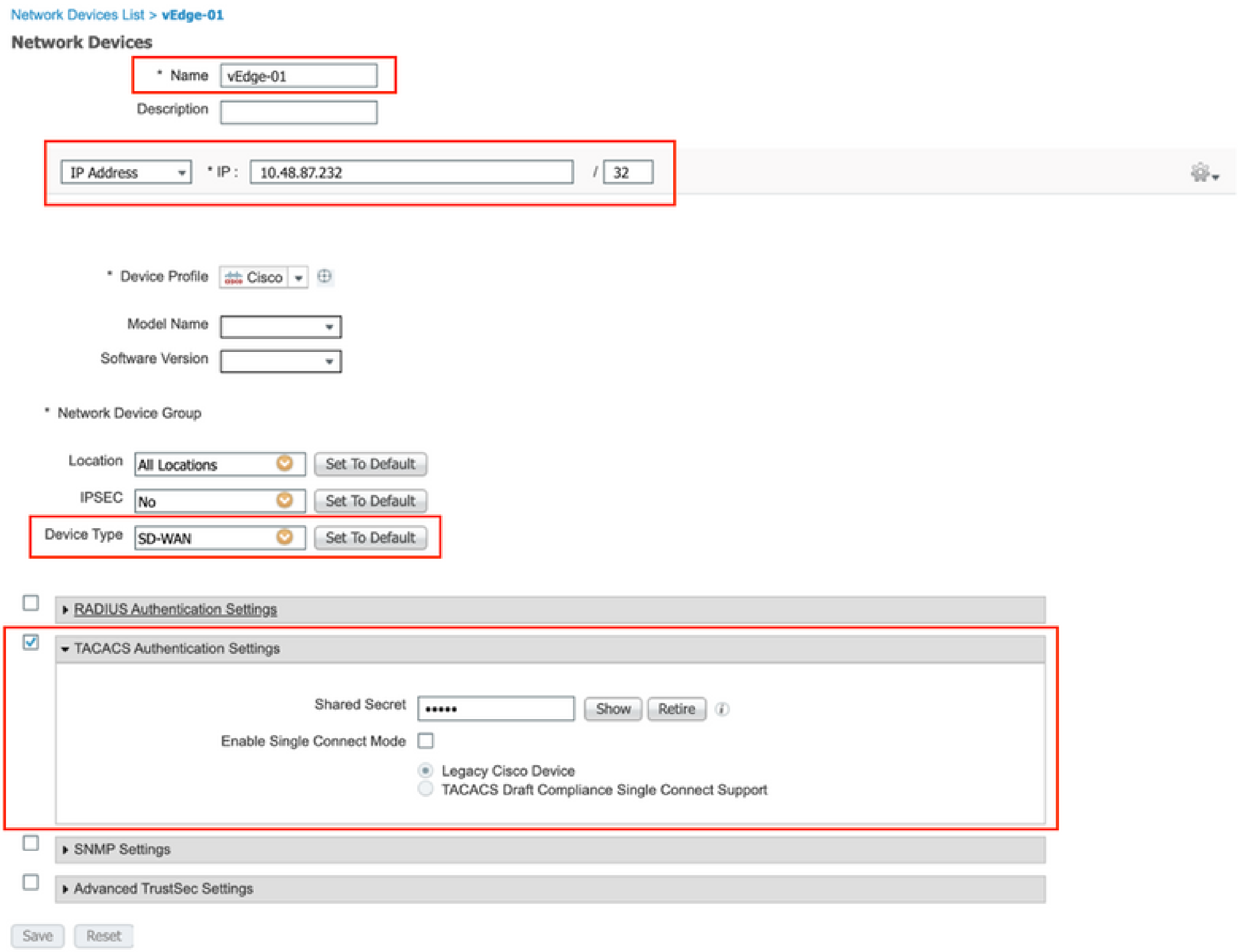
Add Group

Name * SD-WAN

Description

Parent Group * All Device Types

Step 3. Configure the device and assign it to the SD-WAN device group:



* 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 | Set To Default

IPSEC: No | Set To Default

Device Type: SD-WAN | Set To Default

□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: ••••• | Show | Retire

Enable Single Connect Mode □

● Legacy Cisco Device

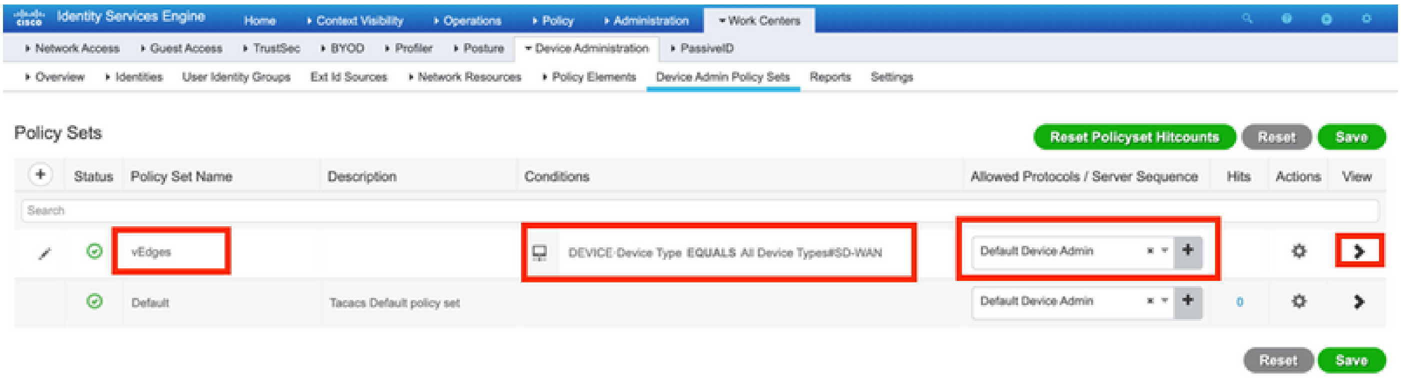
○ TACACS Draft Compliance Single Connect Support

□ SNMP Settings

□ Advanced TrustSec Settings

Step 4. Define Device Administration Policy.

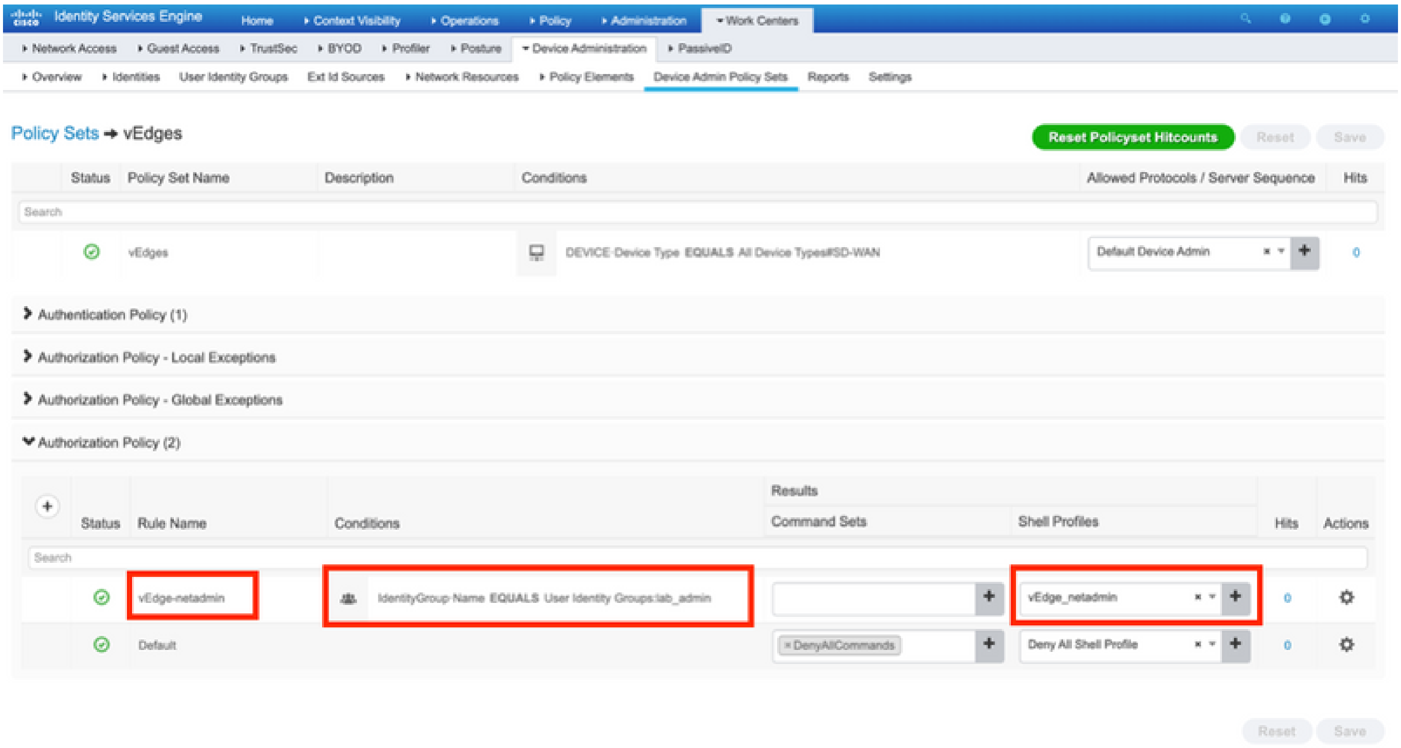
Depends upon your actual setup, your Policy Set may look differently. For the purpose of the demonstration in this document, the Policy is created.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	vEdges		DEVICE·Device Type EQUALS All Device Types#SD-WAN	Default Device Admin		⚙	>
✓	Default	Tacacs Default policy set		Default Device Admin	0	⚙	>

Click **>** and the next screen appears as shown in this image. This policy matches based on device type named **SD-WAN** and assigns the Shell profile that is created in step 1.



Policy Sets → vEdges

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	vEdges		DEVICE·Device Type EQUALS All Device Types#SD-WAN	Default Device Admin	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results Command Sets	 Shell Profiles	Hits	Actions
✓	vEdge-netadmin	IdentityGroup·Name EQUALS User Identity Groups:lab_admin		vEdge_netadmin	0	⚙
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙

Step 5. Configure vEdge:

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

Step 6. Verification. Login to vEdge and ensure netadmin group assigned to remote user:

```
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
```

Step 5. Configure vEdge:

Step 5. Configure vEdge:

Step 5. Configure vEdge:

Related Information

- **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

- Configuring User Access and Authentication: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication