

RADIUSおよびTACACSベースのユーザ認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[vEdgeおよびコントローラに対するRADIUSベースのユーザ認証および許可](#)

[vEdgeおよびコントローラ用のTACACSベースのユーザ認証および許可](#)

[関連情報](#)

はじめに

このドキュメントでは、ISEを使用してvEdgeおよびコントローラのRADIUSベースおよびTACACSベースのユーザ認証および許可を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

デモンストレーションでは、ISEバージョン2.6を使用します。vEdge-cloudおよび19.2.1を実行するコントローラを使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Viptelaソフトウェアには、basic、netadmin、およびoperatorの3つの固定ユーザグループ名があります。ユーザを少なくとも1つのグループに割り当てる必要があります。デフォルトのTACACS/RADIUSユーザは、自動的に基本グループに配置されます。

vEdgeおよびコントローラに対するRADIUSベースのユーザ認証および許可

ステップ 1 : ISE用のViptela radiusディクショナリを作成します。これを行うには、次の内容を含むテキストファイルを作成します。

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

BEGIN-VENDOR    Viptela

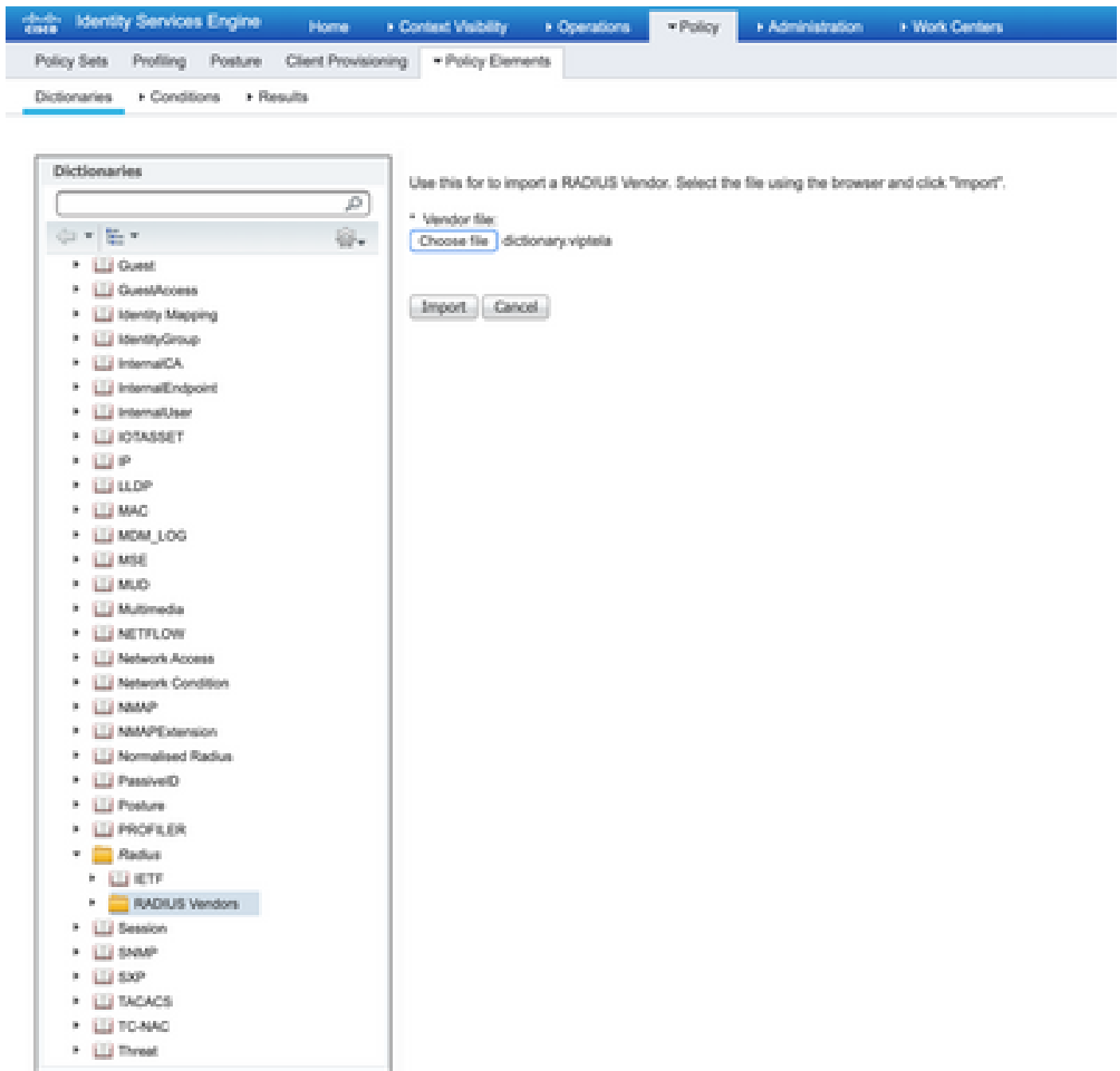
ATTRIBUTE       Viptela-Group-Name 1 string
```

ステップ 2 : ISEにディクショナリをアップロードします。それには、Policy > Policy Elements > Dictionariesの順に移動します。ディクショナリのリストから、Radius > Radius Vendorsの順に移動し、次に示すようにImportをクリックします。

The screenshot shows the Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Content Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is selected, and the 'Policy Elements' sub-tab is active. The 'Dictionaries' sub-tab is also selected. The left sidebar shows a tree view of dictionaries, with 'Radius' and 'RADIUS Vendors' highlighted. The main content area displays the 'RADIUS Vendors' table, which includes columns for Name, Vendor ID, and Description. The 'Import' button is highlighted in the table's toolbar.

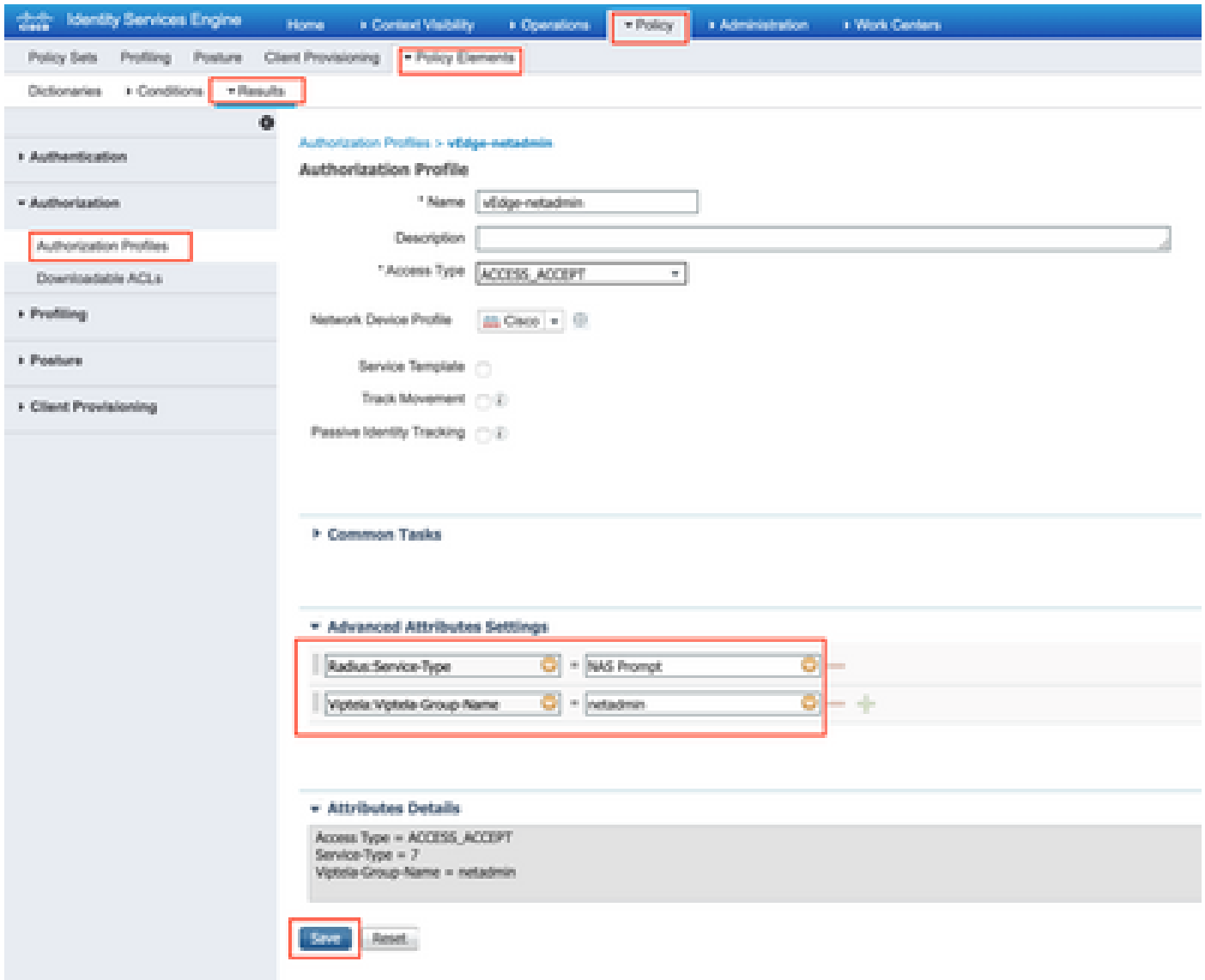
Name	Vendor ID	Description
Airspace	14079	Dictionary for Vendor Airspace
Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
Aruba	14803	Dictionary for Vendor Aruba
Brocade	1588	Dictionary for Vendor Brocade
Cisco	9	Dictionary for Vendor Cisco
Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
Cisco-IPAC0000	3076	Dictionary for Vendor Cisco-IPAC0000
H3C	25506	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2626	Dictionary for Vendor Juniper
Microsoft	315	Dictionary for Vendor Microsoft
Motolora-Symbol	388	Dictionary for Vendor Motorola-Symbol
Ruckus	25013	Dictionary for Vendor Ruckus
WSPH	14032	Dictionary for Vendor WSPH

手順1で作成したファイルをアップロードします。



The screenshot shows the Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' tab is active, and the 'Policy Elements' sub-tab is selected. The 'Dictionaries' section is open, displaying a list of dictionary categories. The 'RADIUS Vendors' category is highlighted. A dialog box is open, titled 'Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import"'. It contains a 'Vendor file:' label, a 'Choose file' button, and the file path 'dictionary.viptela'. Below the dialog are 'Import' and 'Cancel' buttons.

ステップ 3 : 許可プロファイルを作成します。この手順では、Radius認可プロファイルは、たとえば、netadmin特権レベルを認証されたユーザに割り当てます。このためには、Policy > Policy Elements > Authorization Profilesの順に移動し、図に示すように2つの高度な属性を指定します。



ステップ 4：実際の設定によっては、ポリシーセットの外観が異なる場合があります。この記事のデモンストレーションでは、図に示すように、Terminal Accessという名前のポリシーエントリが作成されます。



> をクリックすると、次の画面が次の図のように表示されます。

The screenshot shows the Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Control Visibility, Operations, Policy, Administration, and Work Centers. Below this, there are sub-tabs: Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The main heading is 'Policy Sets → Terminal Access'. There are buttons for 'Reset Policyset Hitcounts', 'Reset', and 'Save'.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	
✓	Terminal Access		Radius NAS-Port-Type ISDNALB Virtual	Default Network Access		
<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	Profiles	Security Groups	Hits	Actions
✓	vEdge-remote	IdentityGroup Name ISDNALB User Identity Group:lab_admin	vEdge-remote	Select from list	1	
✓	Default		CompAccess	Select from list		

Buttons for 'Reset' and 'Save' are located at the bottom right of the table.

このポリシーは、ユーザグループlab_adminに基づいて照合され、手順3で作成した許可プロファイルを割り当てます。

ステップ 5 : 図に示すように、NAS (vEdgeルータまたはコントローラ) を定義します。

Identity Services Engine Administration

Network Resources > 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

手順 6 : vEdge/コントローラを設定します。

```

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

```

手順 7 : 検証.vEdgeにログインし、リモートユーザにnetadminグループが割り当てられていることを確認します。

```
vEdgeCloud1# show users
```

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

vEdgeおよびコントローラ用のTACACSベースのユーザ認証および許可

ステップ 1 : TACACSプロファイルを作成します。この手順では、作成されたTACACSプロファイルが、たとえばnetadmin特権レベルを認証されたユーザに割り当てられます。

- Custom attributeセクションでMandatoryを選択し、次のように属性を追加します。

Type	[名前(Name)]	値
Mandatory	Viptelaグループ名	netadmin

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > **Custom 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_netadmin

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 Comment: [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	netadmin

Cancel | Save

ステップ 2 : SD-WANのデバイスグループを作成します。

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > **Network Resources** > Device Profile Management > yuGest Services > Feed Service > Threat Control NAC

Network Devices > **Network Device Groups** > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External NEM > 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	-
Blindfish		5
All Locations	All Locations	-
All IPSEC Device	With a RADIUS user IPSEC Device	-

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types

Cancel

Save

ステップ 3 : デバイスを設定し、SD-WANデバイスグループに割り当てます。

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

TACACS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

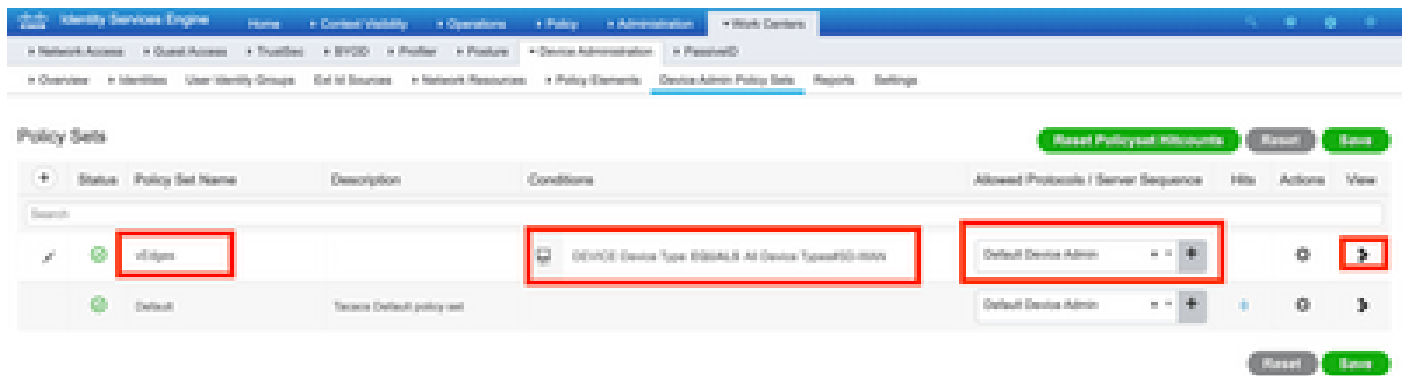
Advanced Tracer Settings

Save

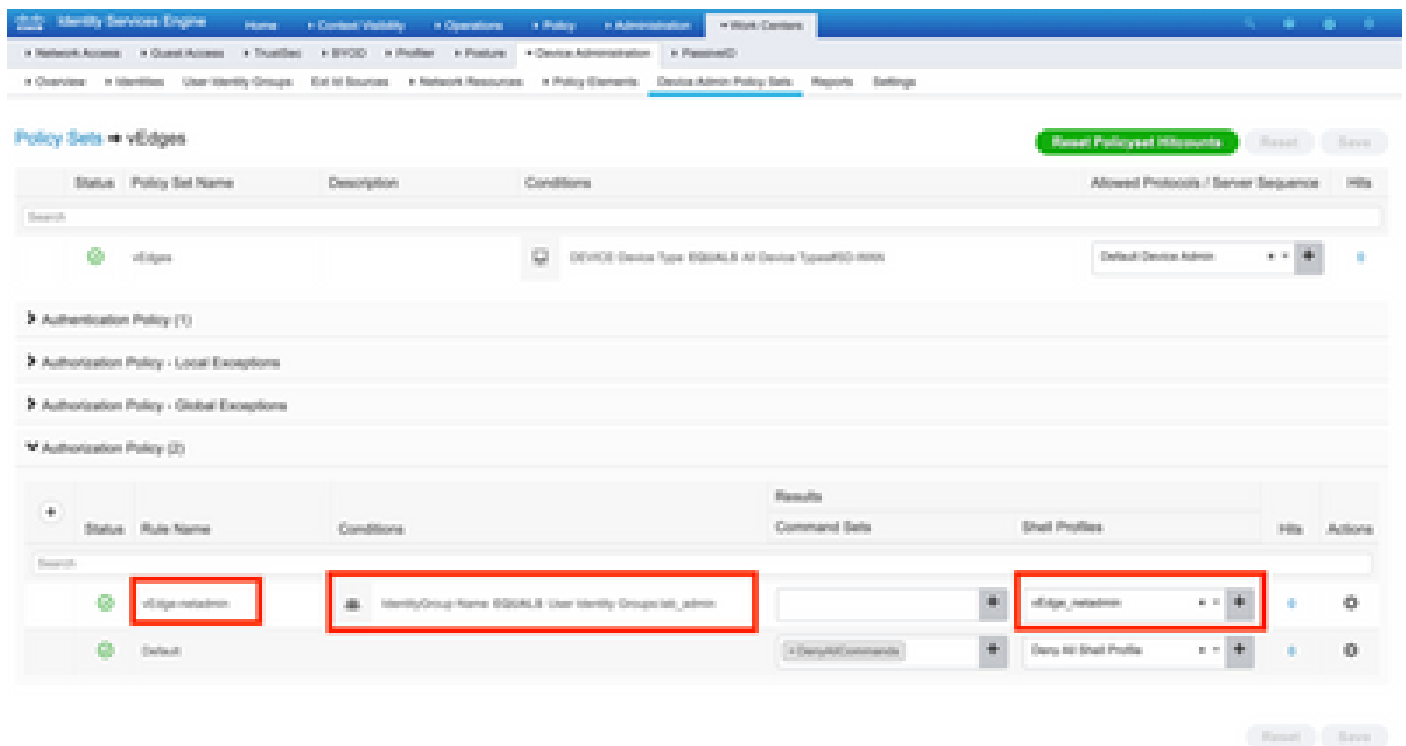
Reset

ステップ 4 : デバイス管理ポリシーを定義します。

実際の設定によっては、ポリシーセットの外観が異なる場合があります。このドキュメントのデモでは、ポリシーを作成します。



>をクリックすると、次の図に示す画面が表示されます。このポリシーは、SD-WANという名前のデバイスタイプに基づいて照合され、ステップ1で作成したシェルプロファイル割り当てます。



ステップ 5 : vEdgeの設定 :

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

手順 6 : 検証.vEdgeにログインし、リモートユーザにnetadminグループが割り当てられていることを確認します。

```
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

関連情報

- Cisco ISE Device Administration規範的導入ガイド : <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- ユーザアクセスおよび認証の設定 : https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。