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

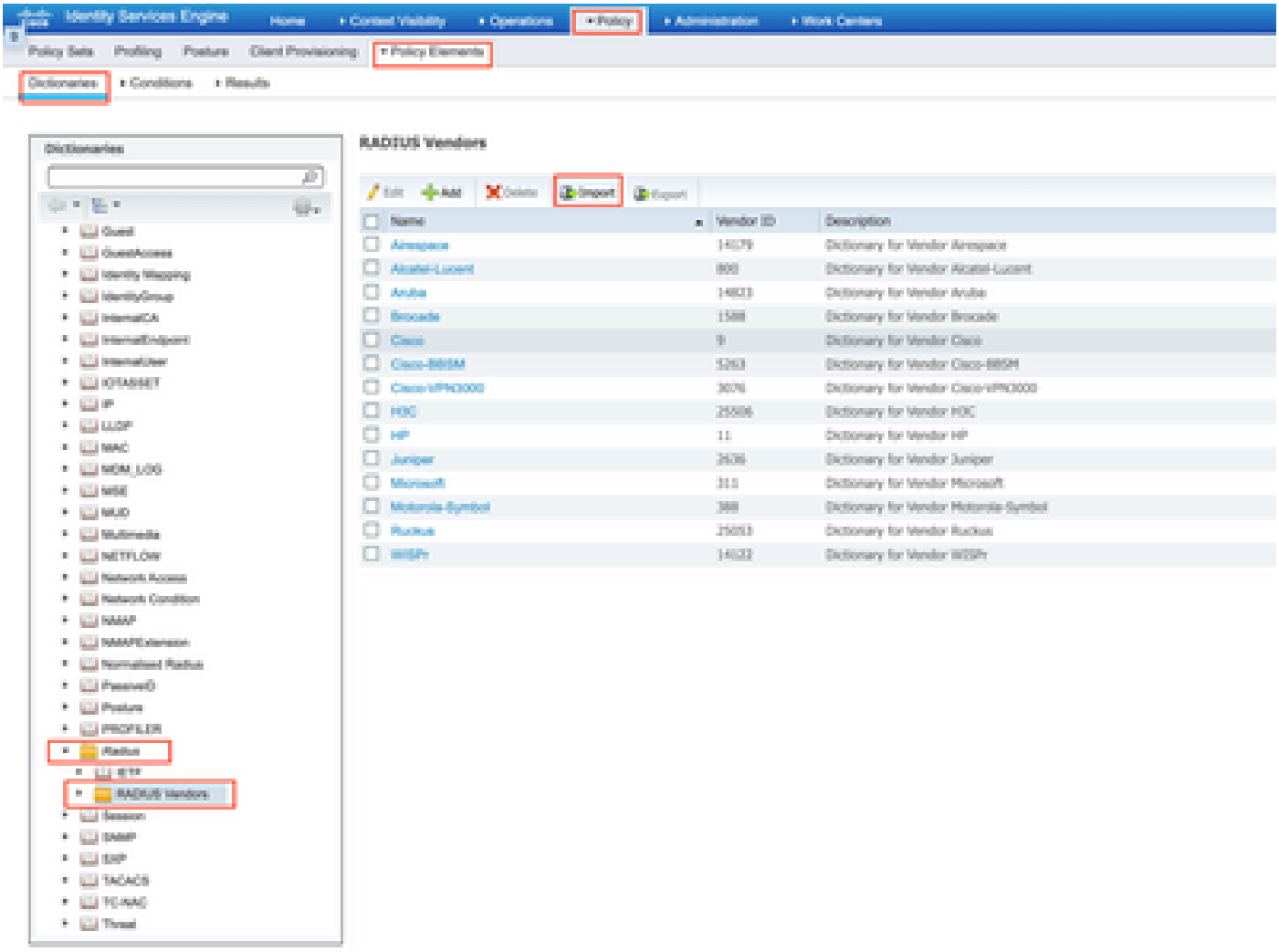
Viptelaソフトウェアには、basic、netadmin、およびoperatorの3つの固定ユーザグループ名があります。 ユーザを少なくとも1つのグループに割り当てる必要があります。デフォルトのTACACS/RADIUSユーザは、自動的に基本グループに配置されます。

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

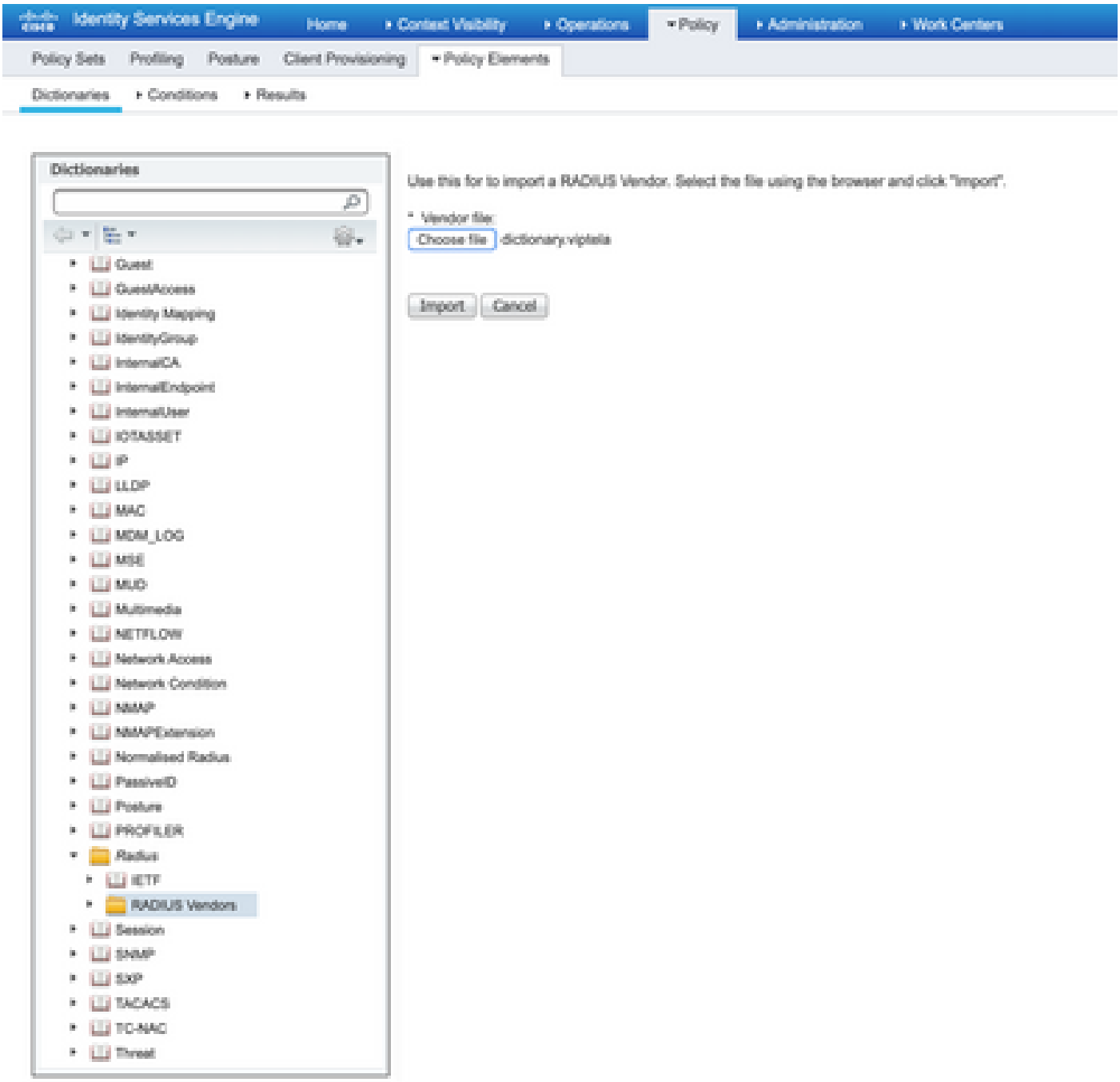
ステップ 1：ISE用のViptela radiusディクショナリを作成します。これを行うには、次の内容を含むテキストファイルを作成します。

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

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

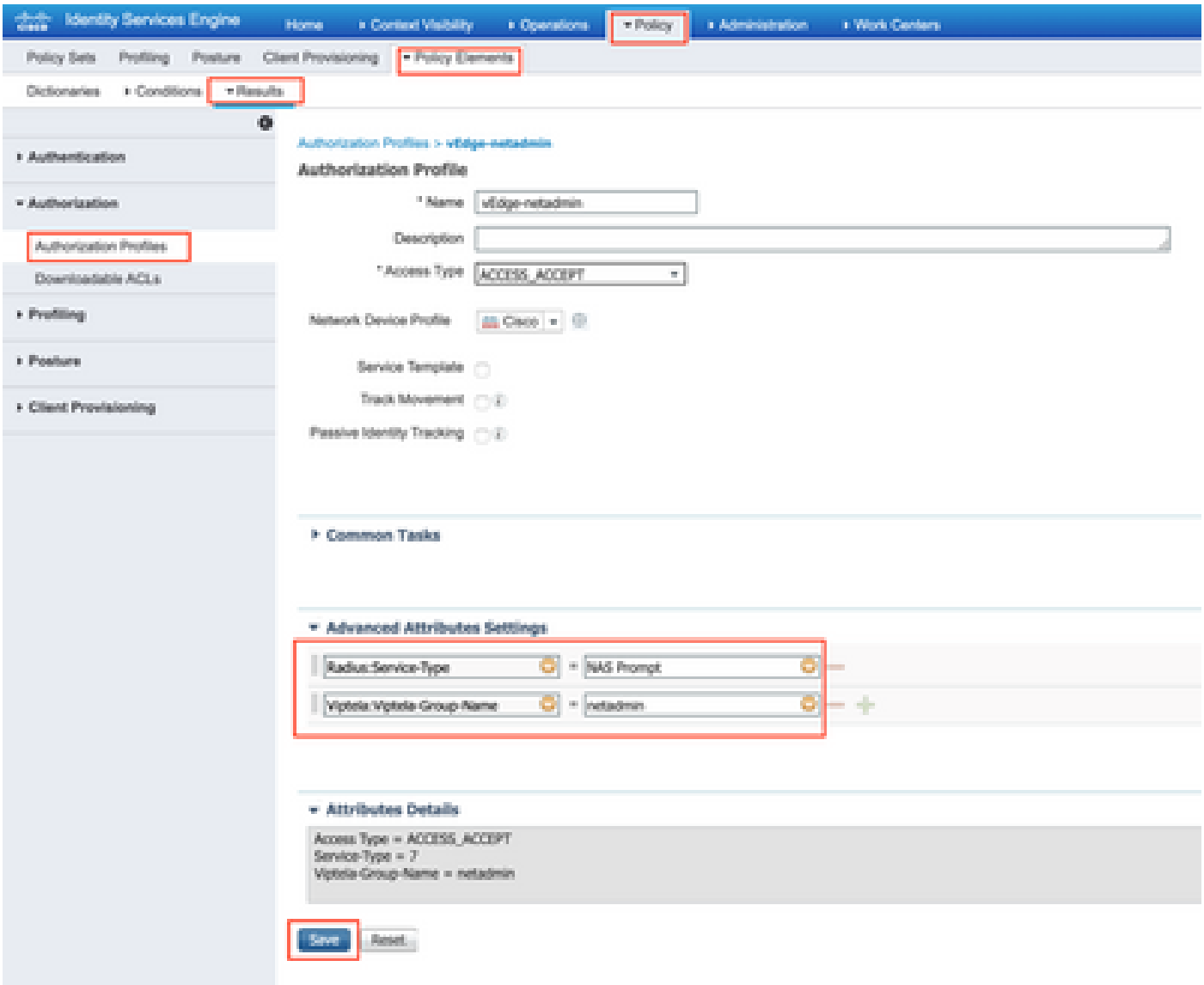
ステップ 2：ISEにディクショナリをアップロードします。それには、Policy > Policy Elements > Dictionariesの順に移動します。ディクショナリのリストから、Radius > Radius Vendorsの順に移動し、次に示すようにImportをクリックします。



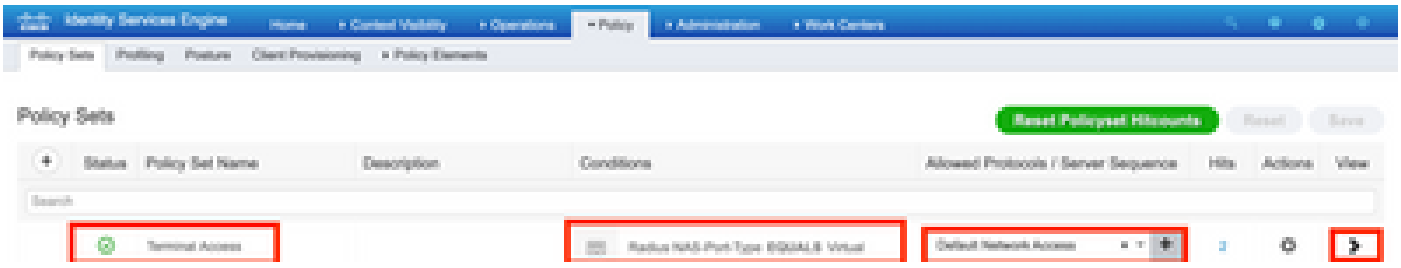
手順1で作成したファイルをアップロードします。



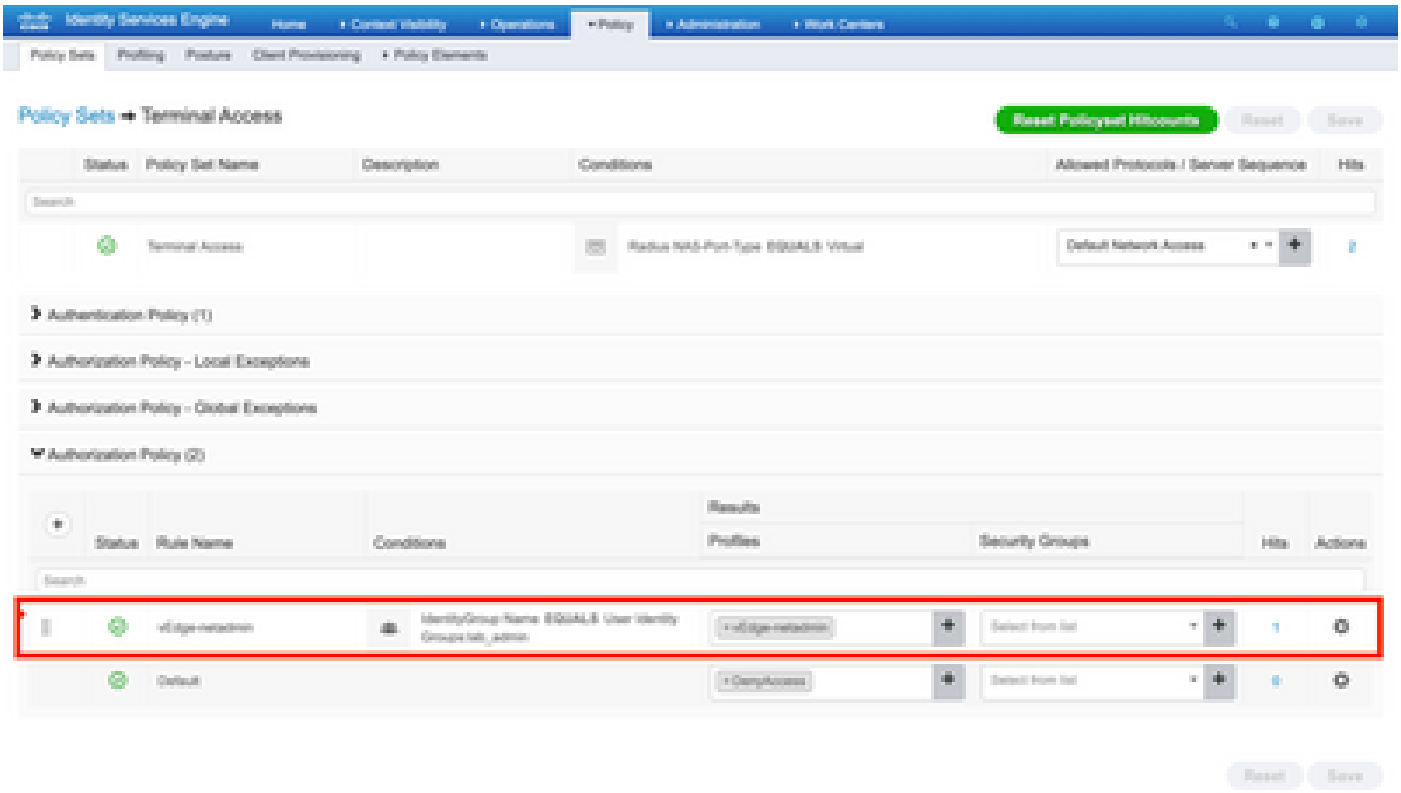
ステップ 3：許可プロファイルを作成します。この手順では、Radius認可プロファイルは、たとえば、netadmin特権レベルを認証されたユーザに割り当てます。このためには、Policy > Policy Elements > Authorization Profilesの順に移動し、図に示すように2つの高度な属性を指定します。



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。

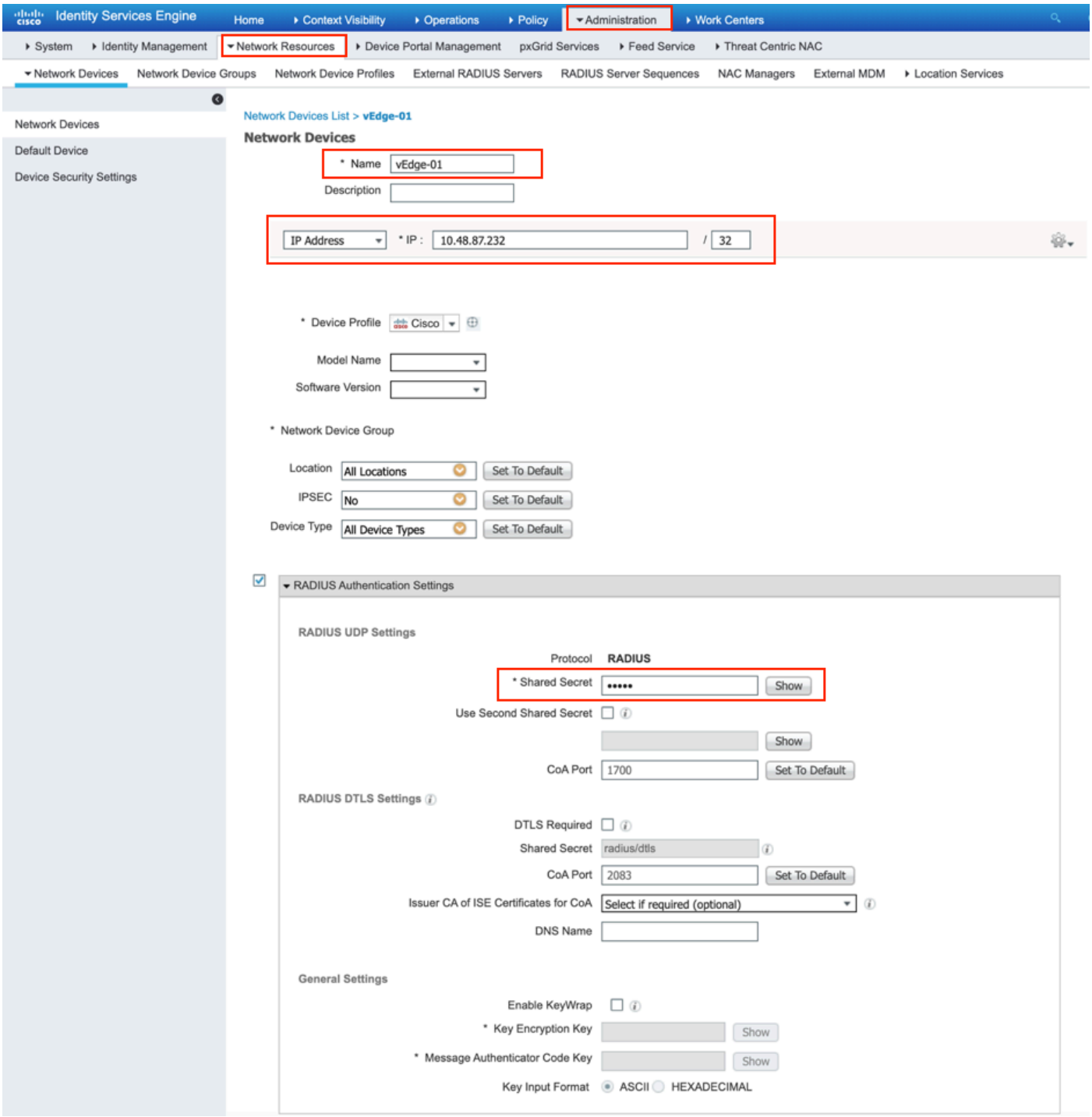


> をクリックすると、次の画面が次の図のように表示されます。



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。



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。

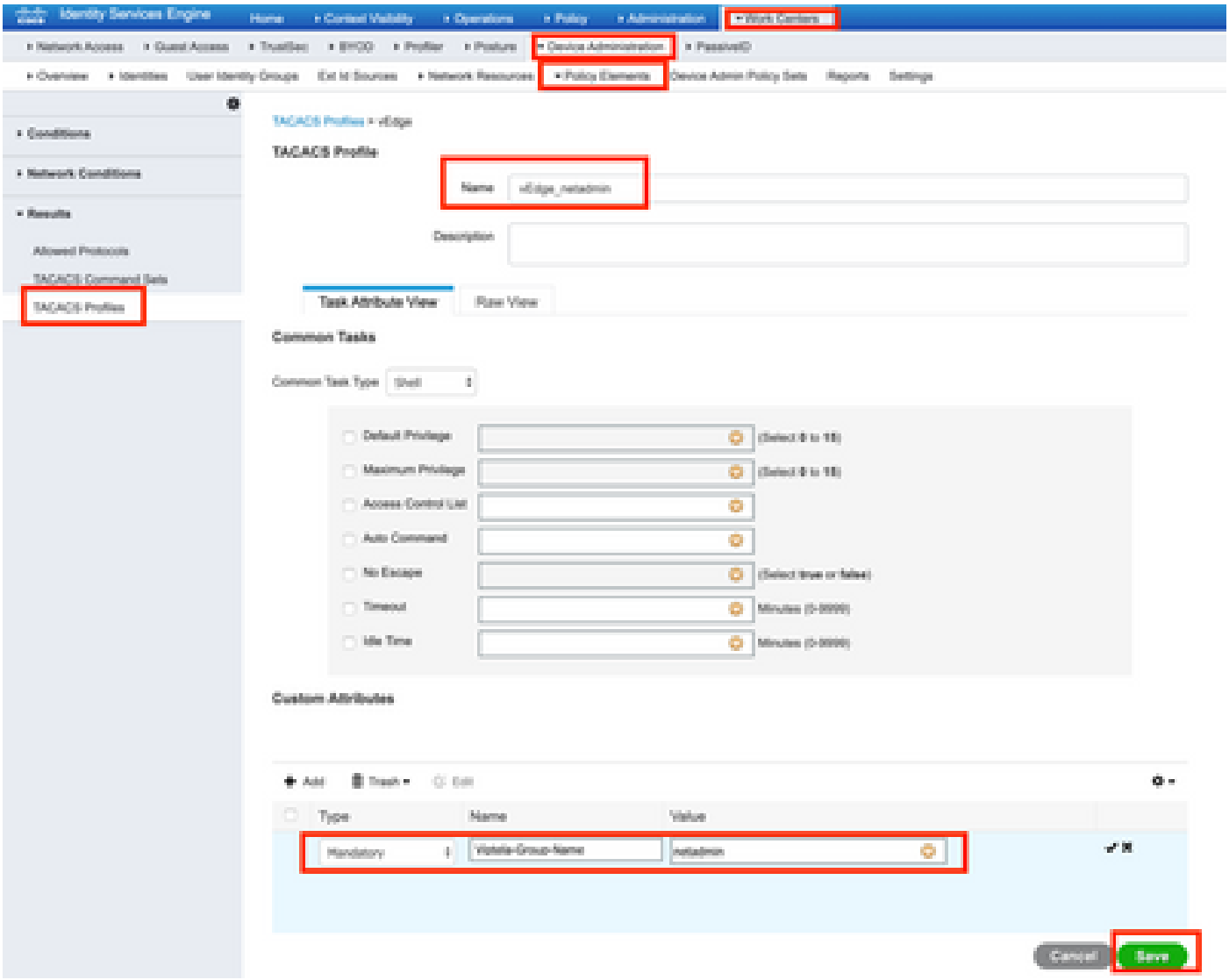
```
vEdgeCloud1# show users

                                                    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
```

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

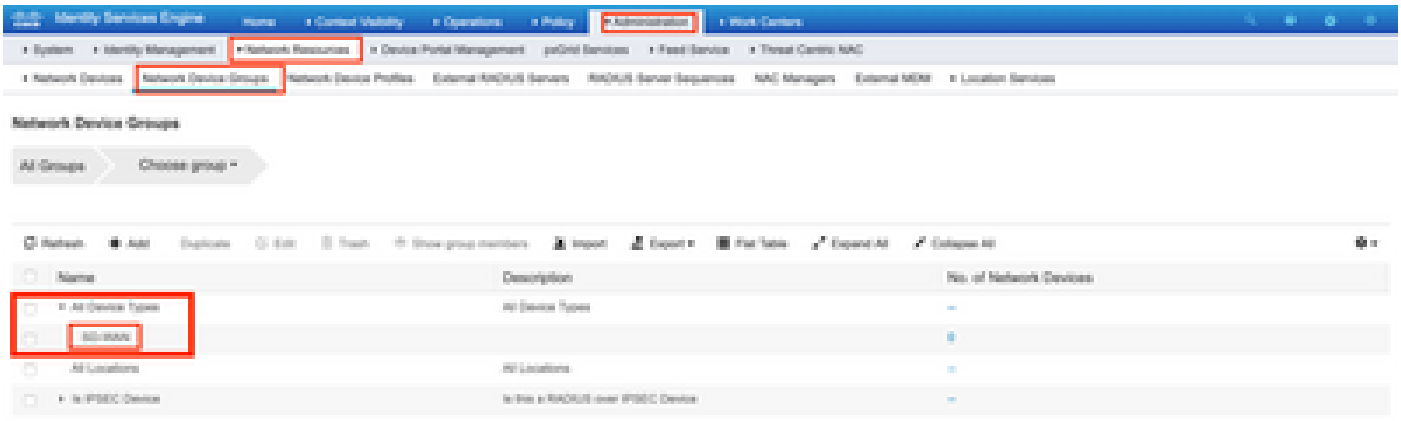
ステップ 1：TACACSプロファイルを作成します。この手順では、作成されたTACACSプロファイルが、たとえばnetadmin特権レベルを認証されたユーザに割り当てられます。

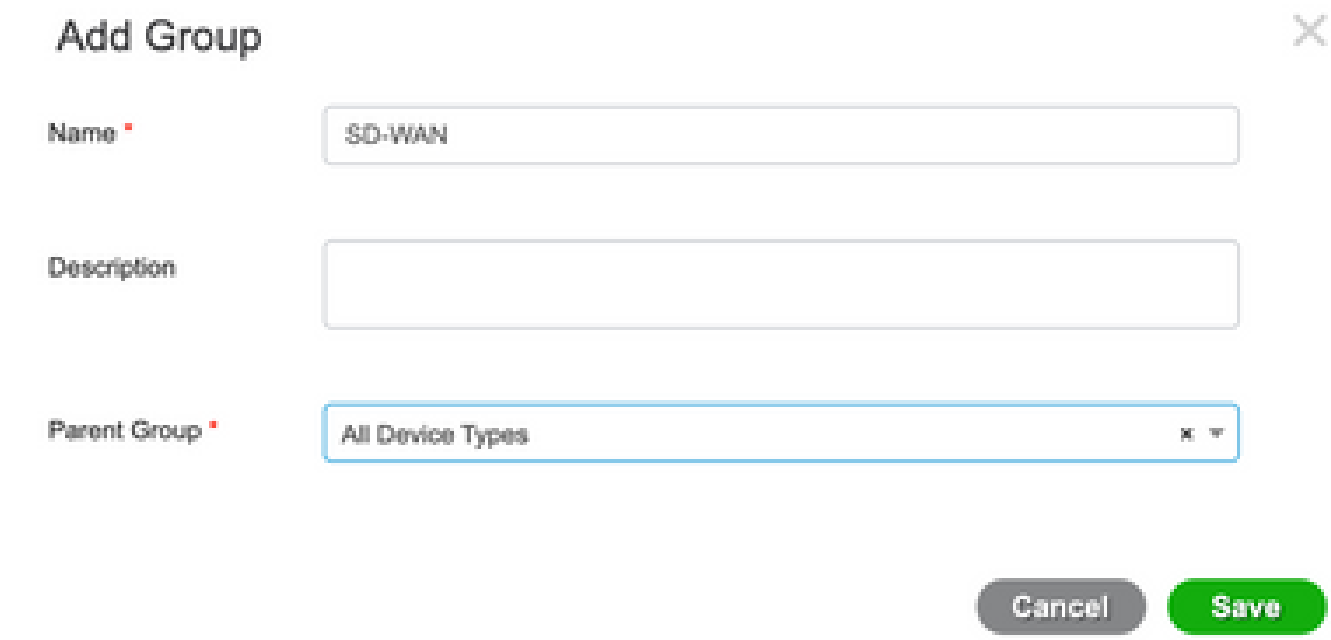
- Custom attributeセクションでMandatoryを選択し、次のように属性を追加します。

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

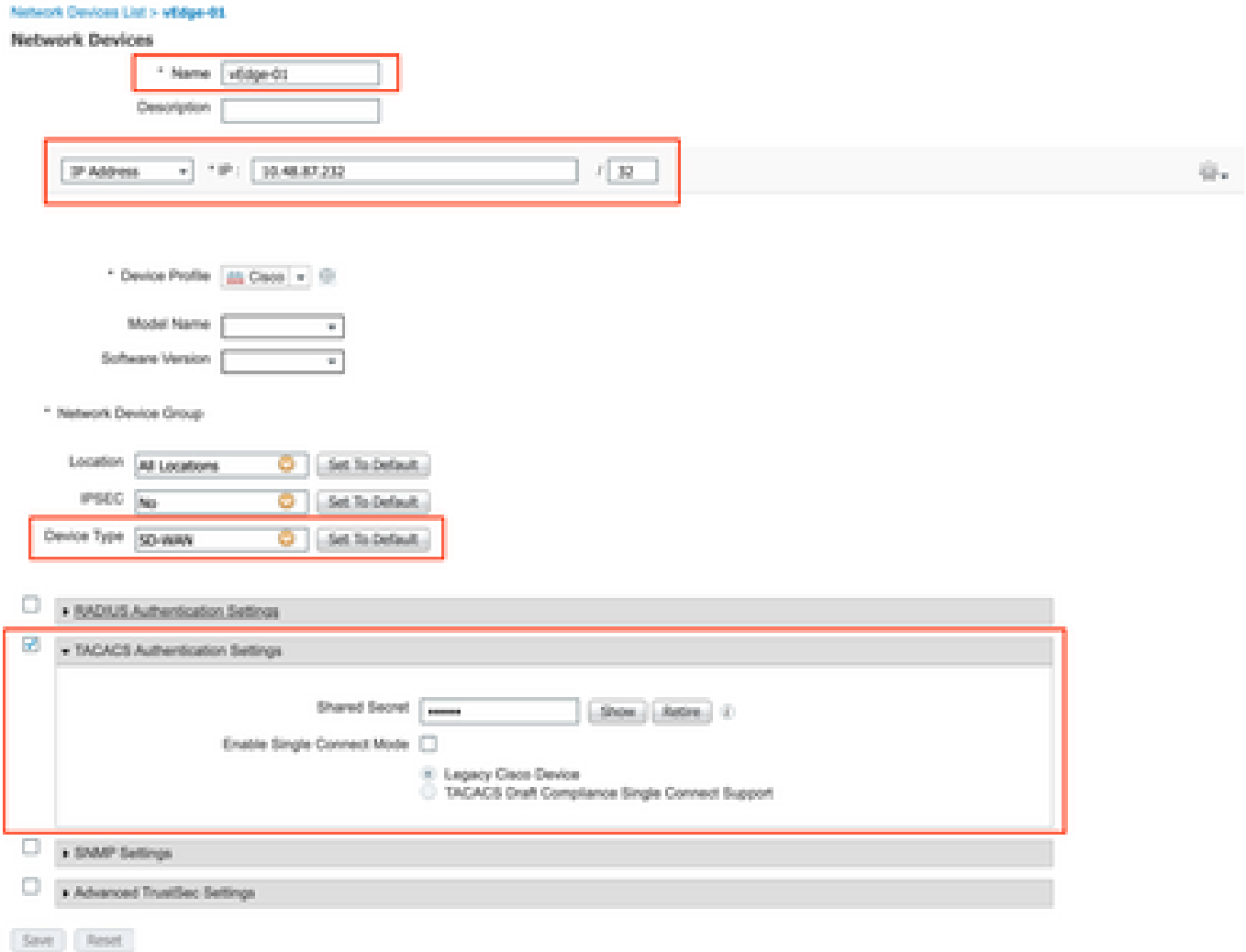


ステップ 2：SD-WANのデバイスグループを作成します。



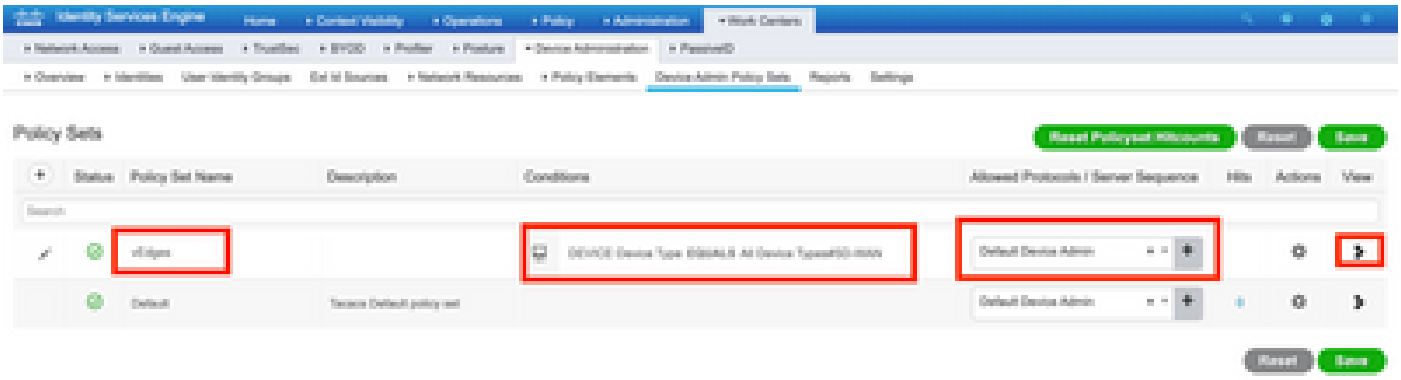


ステップ 3：デバイスを設定し、SD-WANデバイスグループに割り当てます。

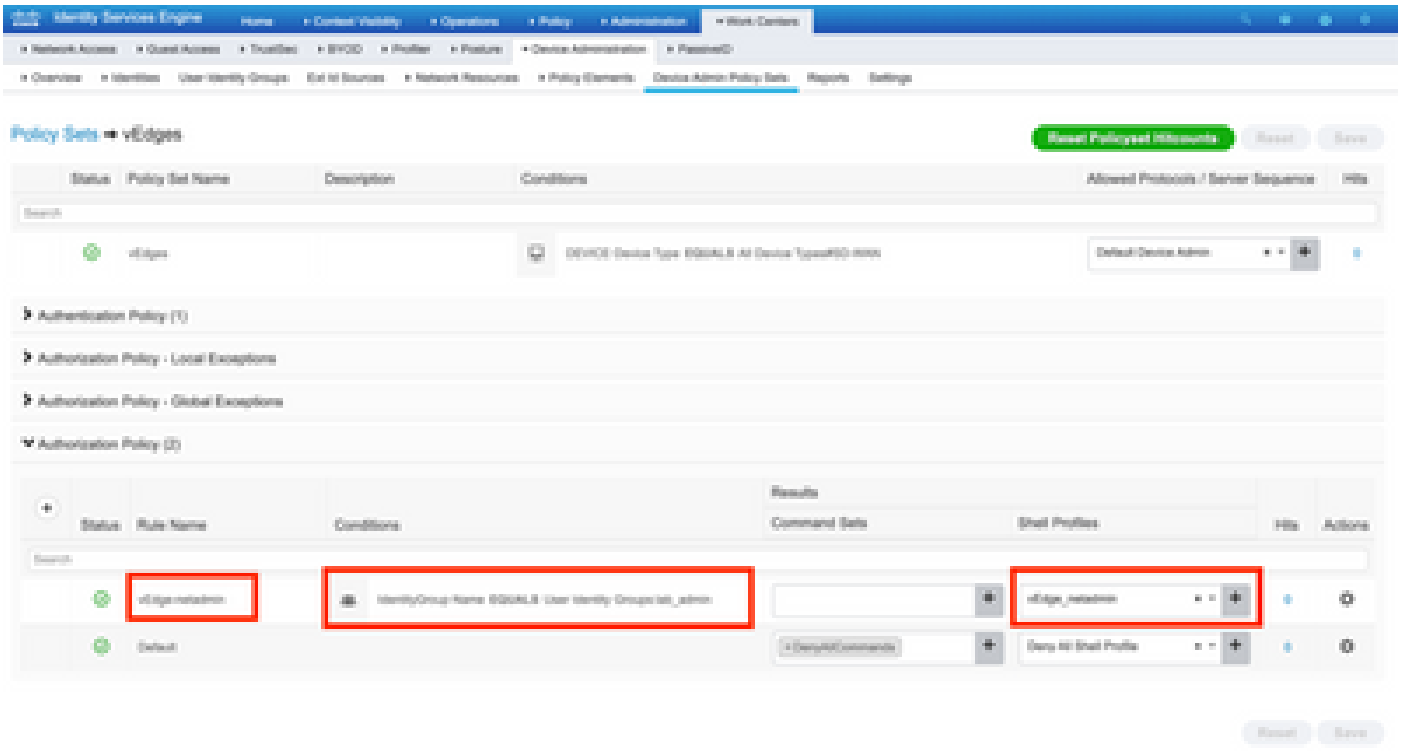


ステップ 4：デバイス管理ポリシーを定義します。

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を割り当てます。



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

                                                    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
```

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。