

配置基于Radius和TACACS的用户身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[vEdge和控制器基于RADIUS的用户身份验证和授权](#)

[vEdge和控制器基于TACACS的用户身份验证和授权](#)

[相关信息](#)

简介

本文档介绍如何使用ISE为vEdge和控制器配置基于RADIUS和TACACS的用户身份验证和授权。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本演示使用ISE版本2.6。vEdge云和运行19.2.1的控制器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

Viptela软件提供三个固定用户组名称：basic、netadmin和operator。您必须将用户分配到至少一个组。默认TACACS/Radius用户自动置于基本组中。

vEdge和控制器基于RADIUS的用户身份验证和授权

步骤1:为ISE创建虚拟RADIUS字典。为此，请创建包含以下内容的文本文件：

```
# -*- text -*-  
#  
# dictionary.viptela  
#
```

```

#
# Version:      $Id$
#

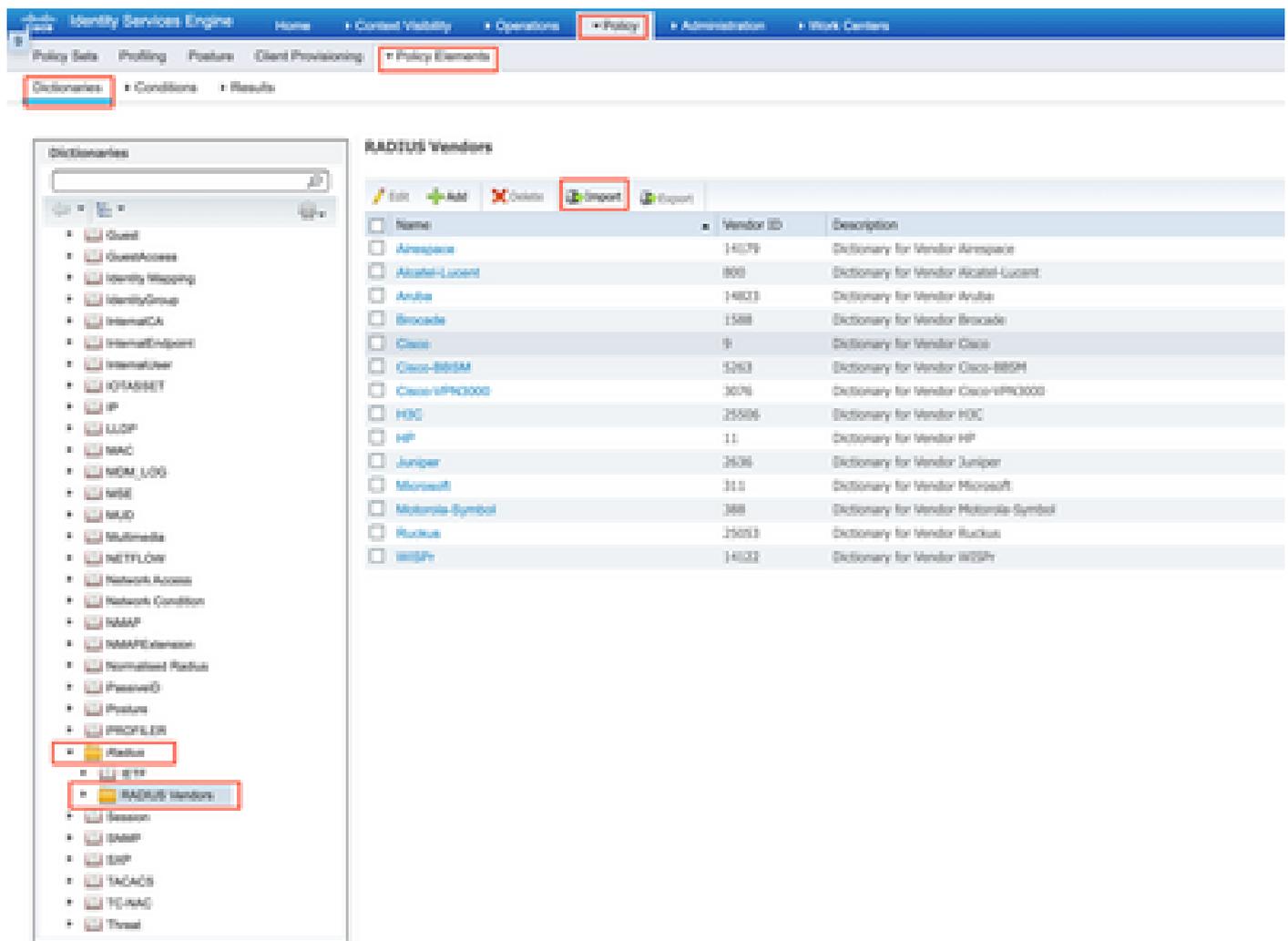
VENDOR          Viptela          41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name 1    string

```

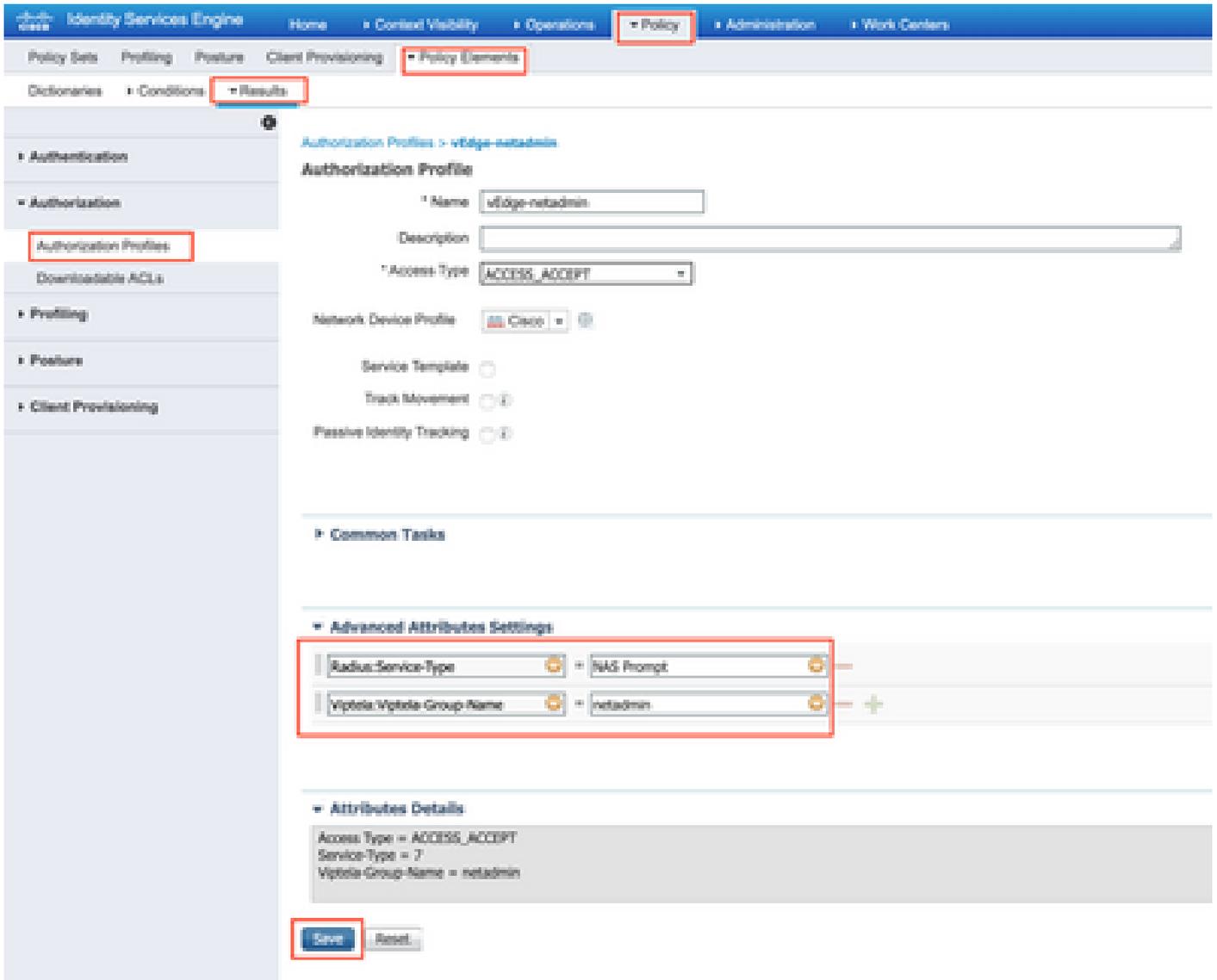
第二步：将词典上传到ISE。为此，请导航到策略>Policy元素>词典。从字典列表中，导航到Radius > Radius Vendors，然后单击Import，如下所示。



上传您在第1步中创建的文件。

The screenshot shows the 'Dictionaries' management interface. On the left, a tree view lists various dictionaries, with 'RADIUS Vendors' highlighted. On the right, an 'Import' dialog is open, prompting the user to select a vendor file. The 'Vendor file' field contains the text 'dictionary.viptelia'. Below the field are 'Import' and 'Cancel' buttons. Above the field, there is a 'Choose file' button. A note at the top of the dialog reads: 'Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".'

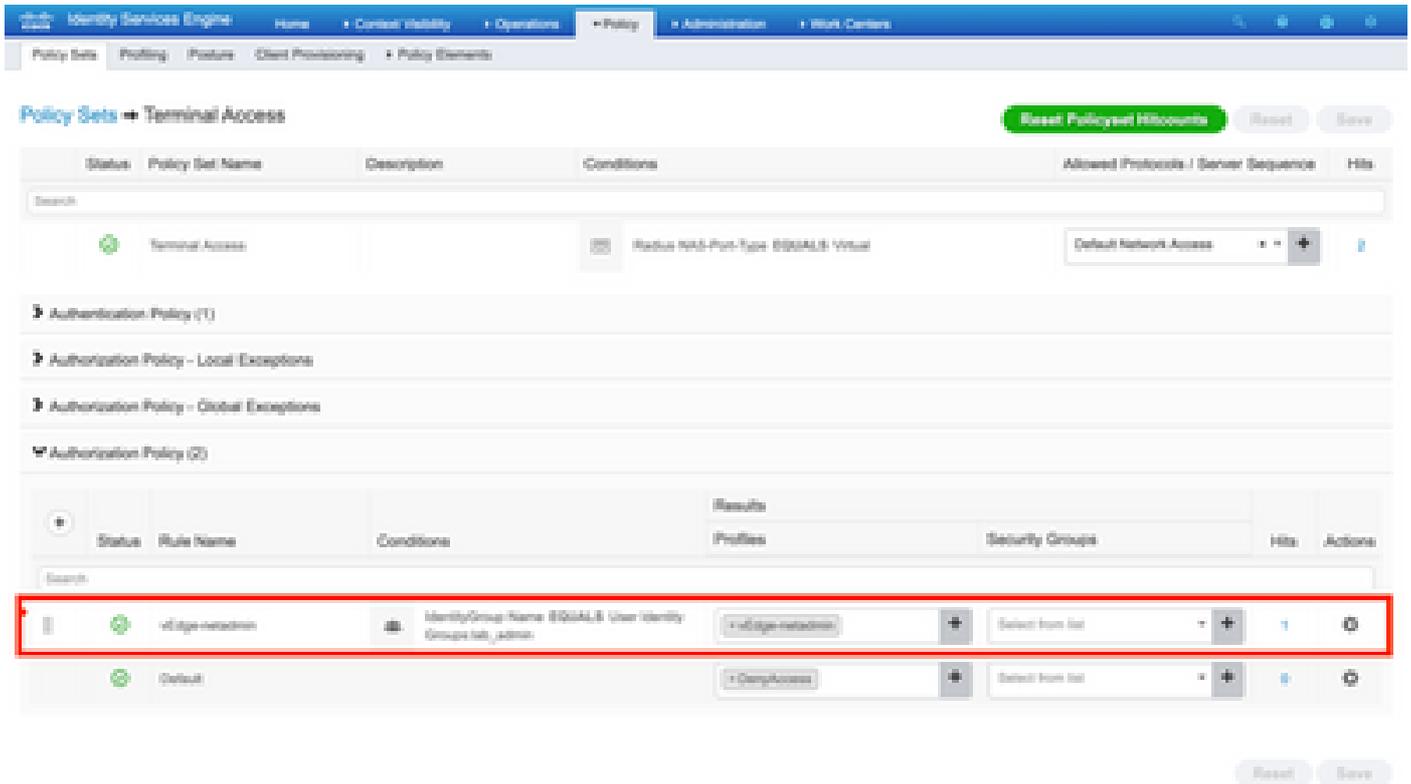
第三步：创建授权配置文件。在此步骤中，Radius授权配置文件将（例如）netadmin权限级别分配给经过身份验证的用户。为此，请导航到策略>策略元素>授权配置文件，并指定两个高级属性（如图所示）。



第四步：根据实际设置，策略集的外观可能会有所不同。出于本文演示的目的，我们创建了称为终端访问的策略条目，如图所示。



单击>，此时将显示下一个屏幕，如图所示。



此策略根据用户组lab_admin进行匹配并分配在步骤3中创建的授权配置文件。

第五步：定义NAS（vEdge路由器或控制器），如图所示。

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 configuration page is titled "Network Devices List > vEdge-01". The "Network Devices" section shows the following fields:

- * 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 and shows:

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

第六步：配置vEdge/控制器。

```

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

```

步骤 7.验证。登录到vEdge并确保将netadmin组分配给远程用户。

```
vEdgeCloud1# show users
```

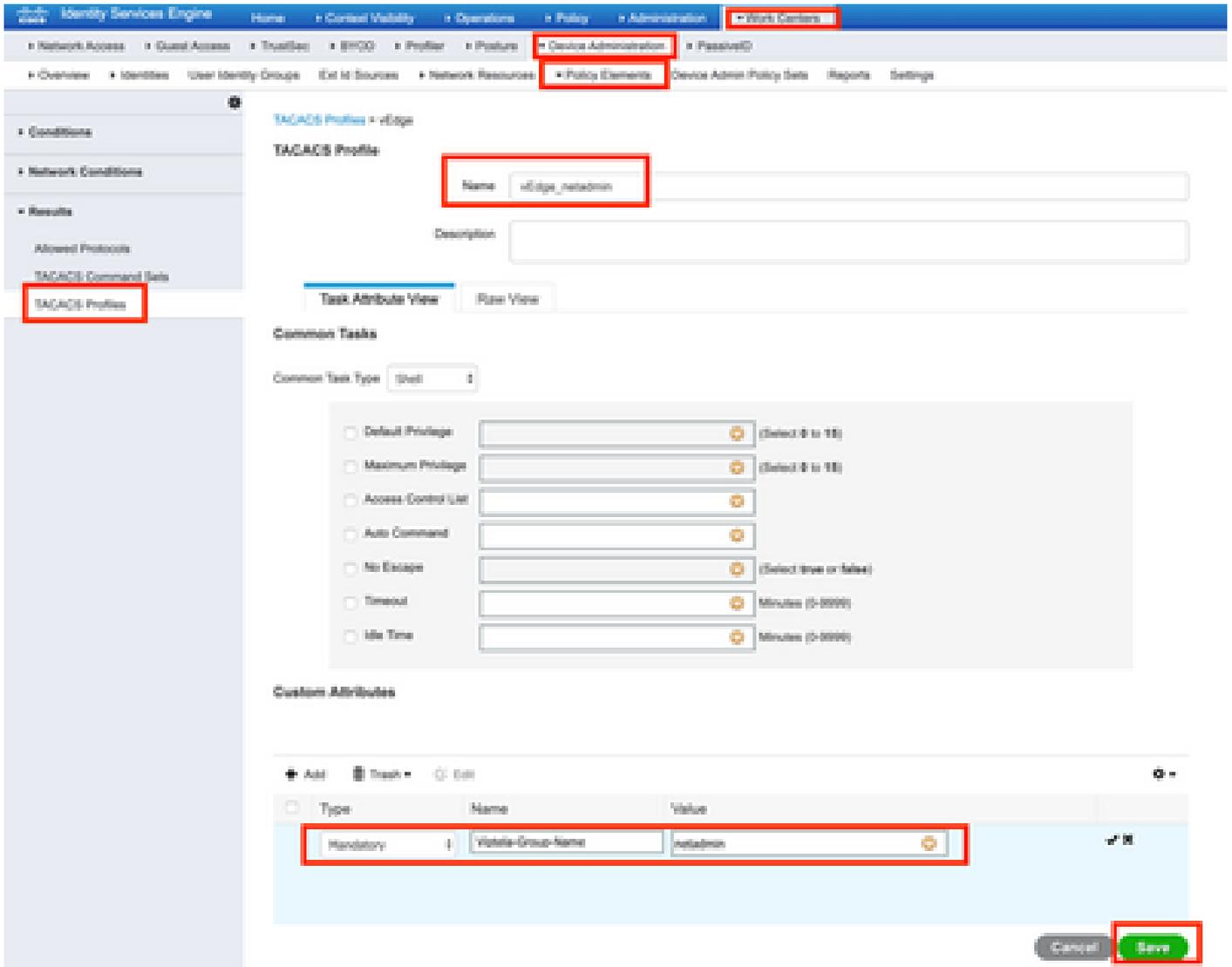
```
SESSION  USER      CONTEXT  FROM          PROTO  AUTH
-----  -
33472    ekhabaro  cli      10.149.4.155  ssh    netadmin  2020-03-09T18:39:40+00:00
```

vEdge和控制器基于TACACS的用户身份验证和授权

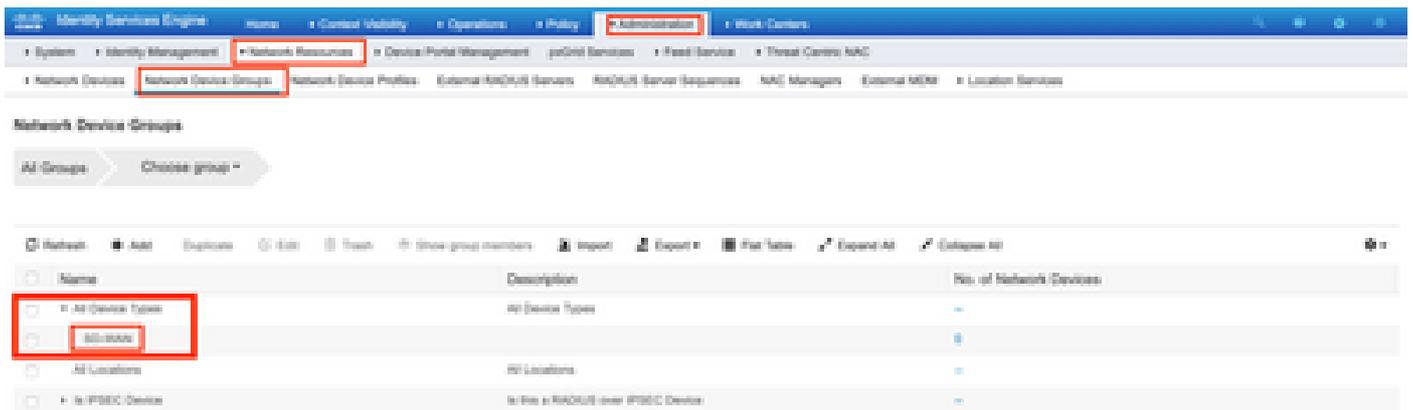
步骤1:创建TACACS配置文件。在此步骤中，将创建的TACACS配置文件分配给经过身份验证的用户，例如netadmin权限级别。

- 从自定义属性部分选择必填，将属性添加为：

类型	名称	价值
必需	Viptela-Group-Name	网络管理员



第二步：为SD-WAN创建设备组。



Add Group



Name

Description

Parent Group

Cancel

Save

第三步：配置设备并将其分配给SD-WAN设备组：

Network Devices List > vEdge-01

Network Devices

Name

Description

IP Address /

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

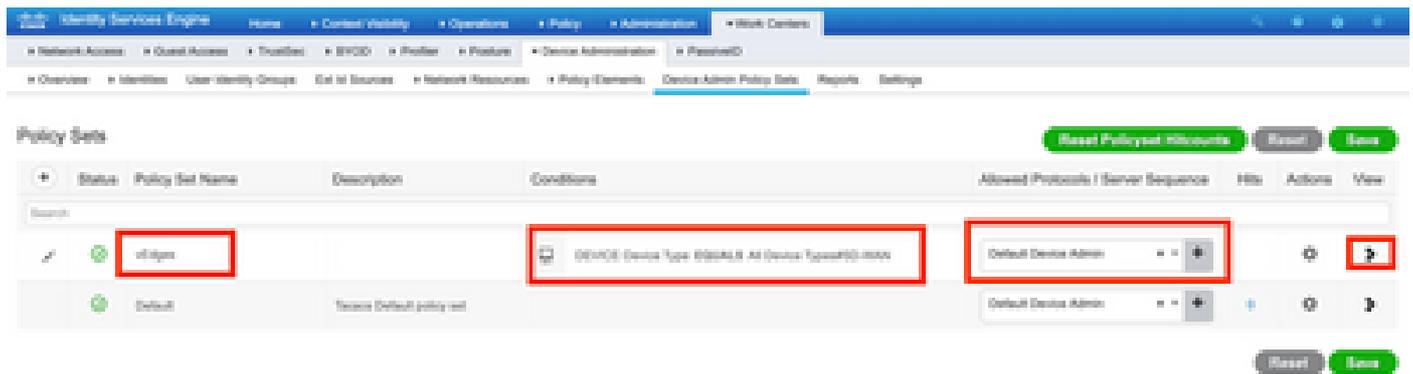
Advanced Truflow Settings

Save

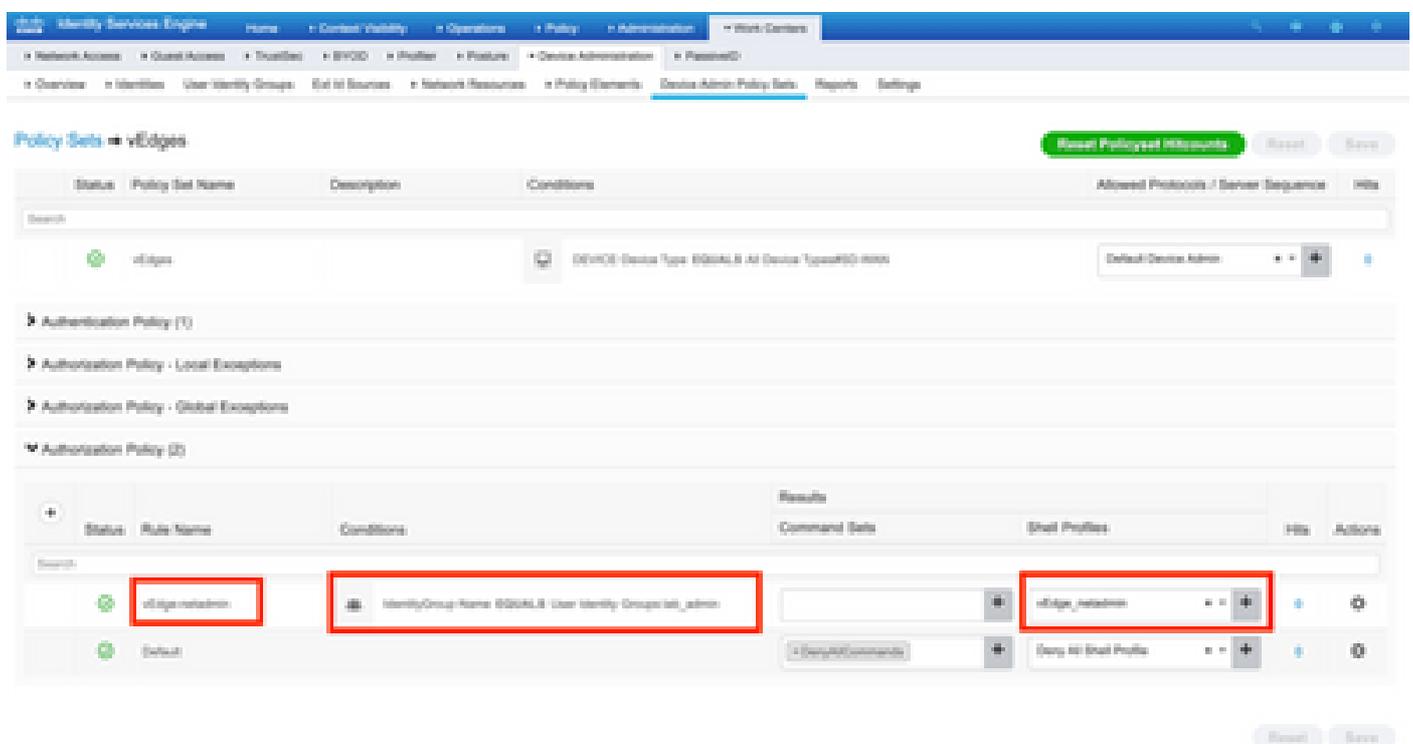
Reset

第四步：定义设备管理策略。

根据实际设置，策略集的外观可能会有所不同。出于本文档演示的目的，将创建策略。



点击>，系统将显示如下图所示的下一个屏幕。此策略根据名为SD-WAN的设备类型进行匹配，并分配在步骤1中创建的外壳配置文件。



第五步：配置vEdge：

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

第六步：验证。登录vEdge并确保将netadmin组分配给远程用户：

```
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

相关信息

- 思科ISE设备管理规范部署指南：<https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- 配置用户访问和身份验证：https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。