

配置基於Radius和TACACS的使用者身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[適用於vEdge和控制器的基於RADIUS的使用者身份驗證和授權](#)

[vEdge和控制器的TACACS型使用者驗證和授權](#)

[相關資訊](#)

簡介

本文檔介紹如何為使用ISE的vEdge和控制器配置基於RADIUS和TACACS的使用者身份驗證和授權。

必要條件

需求

本文件沒有特定需求。

採用元件

本演示使用ISE 2.6版。vEdge雲和控制器運行19.2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

Viptela軟體提供三個固定使用者群組名稱：basic、netadmin和operator。您必須將使用者指派給至少一個群組。預設TACACS/Radius使用者自動置於基本組中。

適用於vEdge和控制器的基於RADIUS的使用者身份驗證和授權

步驟 1. 為ISE建立影片半徑詞典。若要這麼做，請建立包含下列內容的文字檔案：

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

```

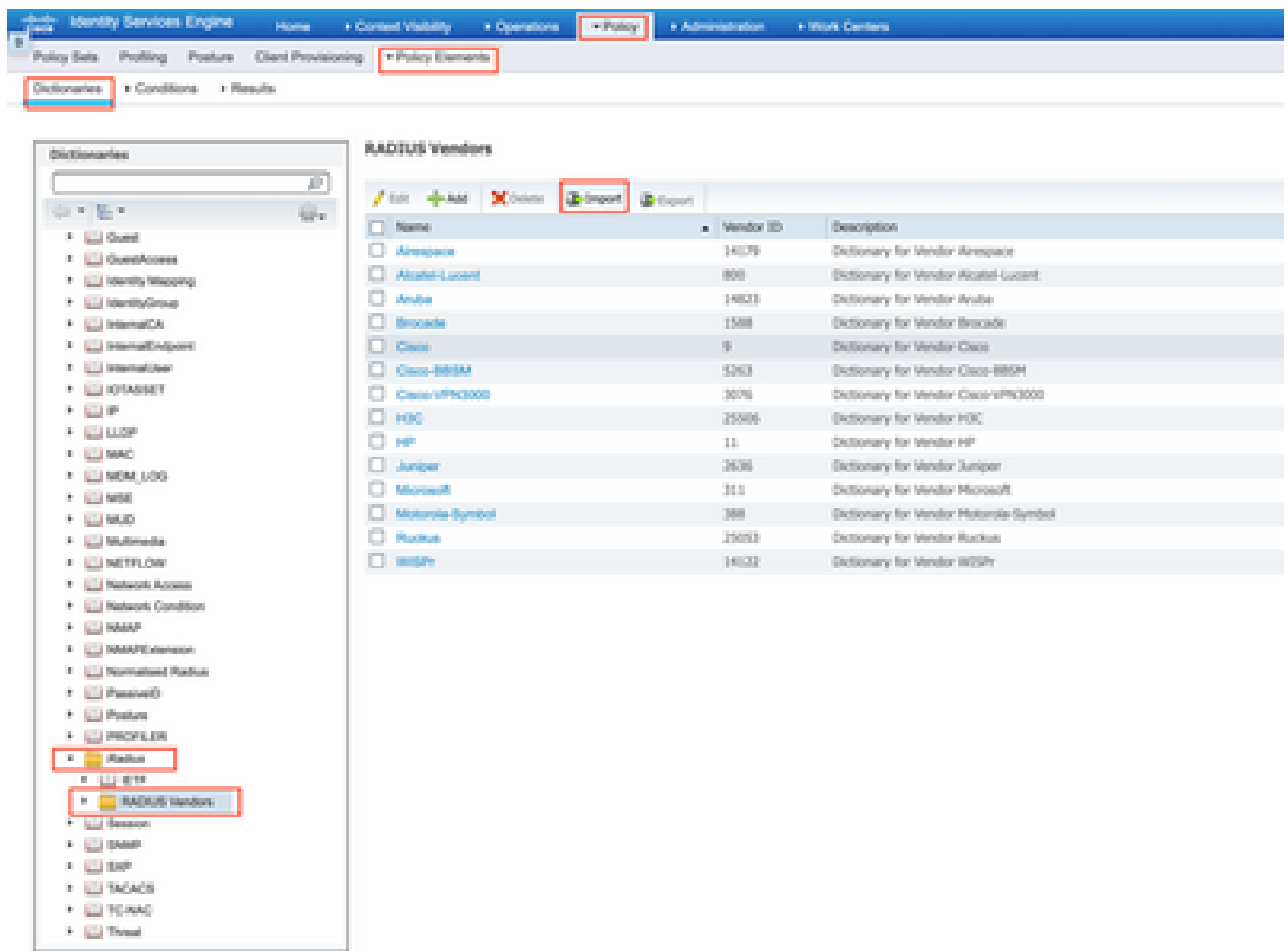
#
#
# Version:      $Id$
#
VENDOR          Viptela          41916

BEGIN-VENDOR    Viptela

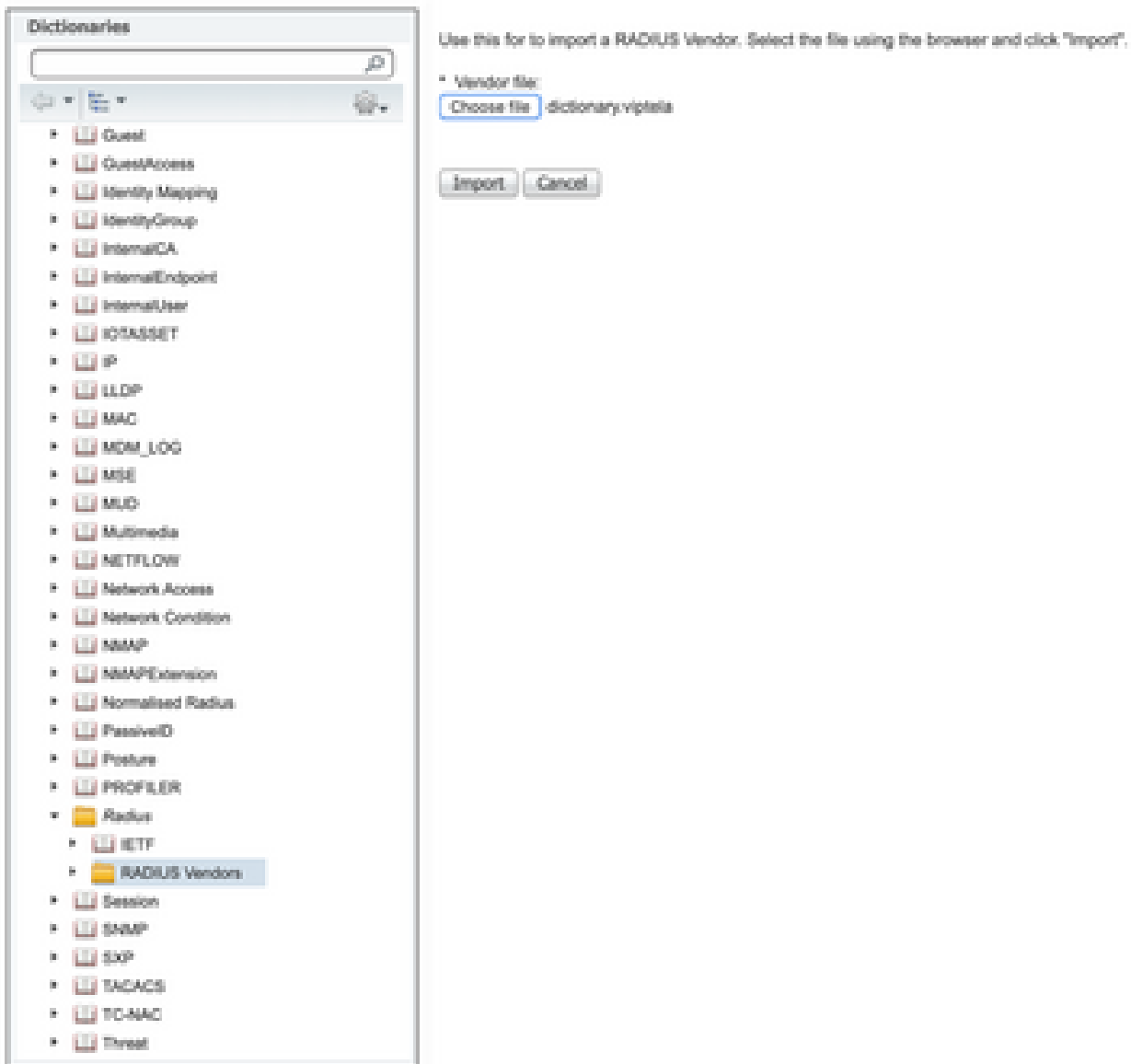
ATTRIBUTE       Viptela-Group-Name 1 string

```

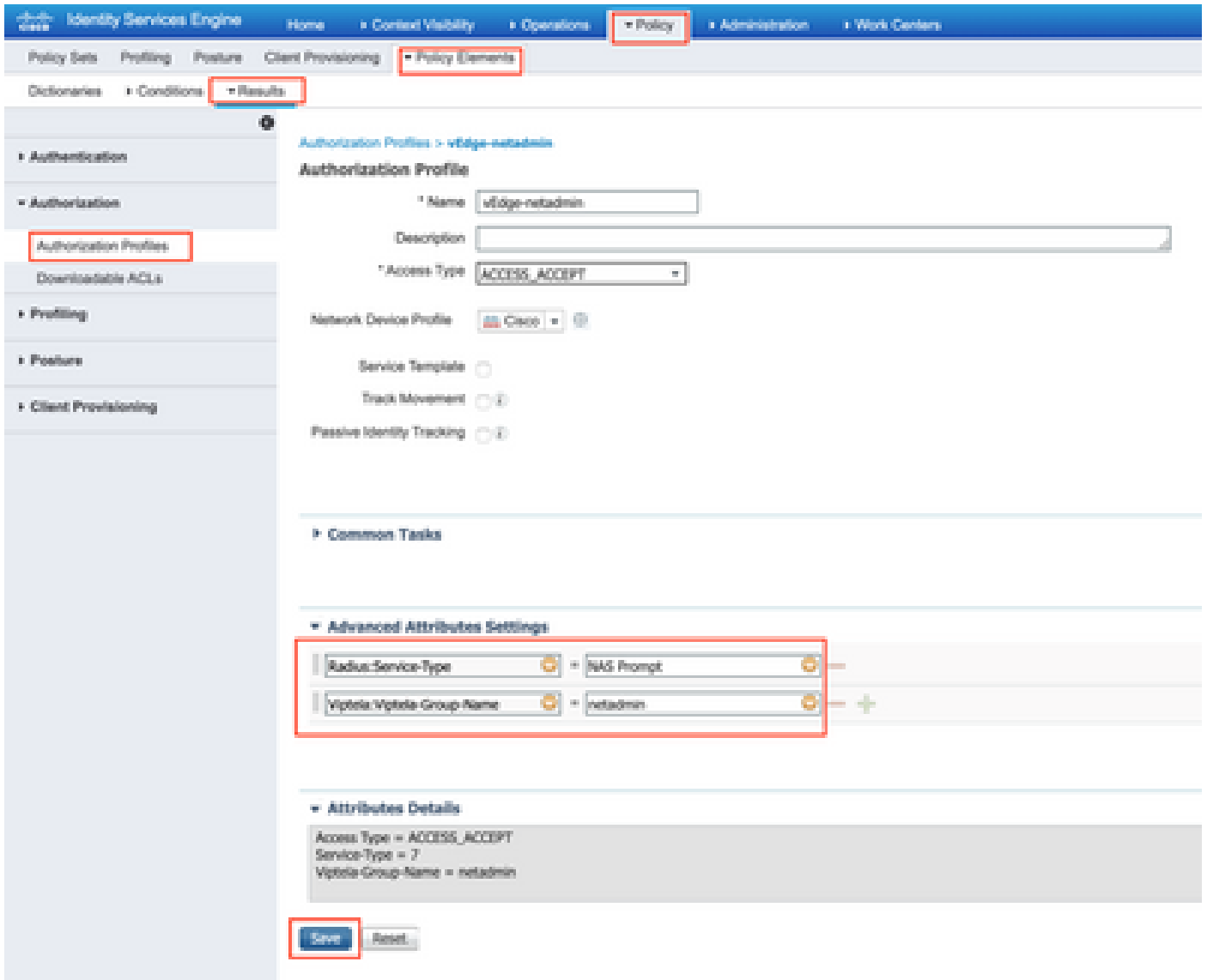
步驟 2. 將詞典上傳到ISE。為此，請導航到策略>策略元素>詞典。從詞典清單中，導航到Radius > Radius Vendors，然後按一下Import (如圖所示)。



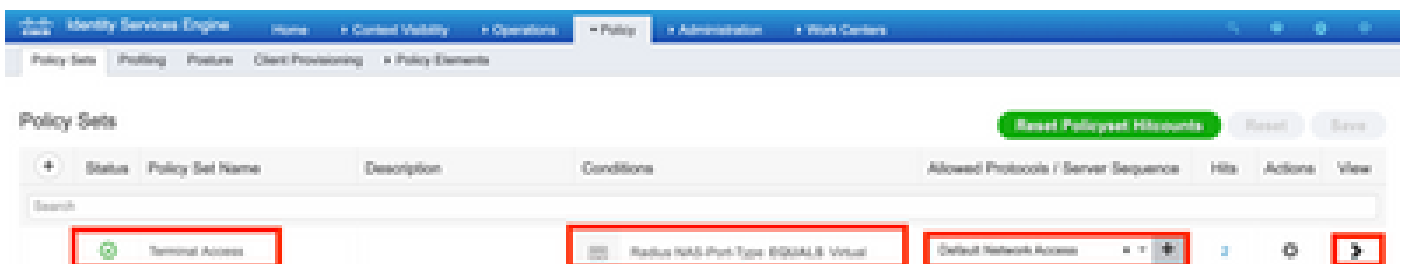
上傳您在步驟1中建立的檔案。



步驟 3. 建立授權配置檔案。在此步驟中，Radius授權配置檔案將（例如）netadmin許可權級別分配給經過身份驗證的使用者。為此，請導航到策略>策略元素>授權配置檔案，並指定兩個高級屬性，如下圖所示。



步驟 4. 根據您的實際設定，策略集的外觀可能有所不同。出於本文演示的目的，我們建立了稱為終端訪問的策略條目，如下圖所示。



點選>，下一個螢幕會出現，如下圖所示。

The screenshot displays the 'Policy Sets' configuration for 'Terminal Access'. At the top, there are navigation tabs: Home, Control Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation, there are sub-tabs: Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The main content area shows a table of policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is located above the table. Below the table, there are expandable sections for 'Authentication Policy (1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. The 'Authorization Policy (2)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The first row in this table, representing the 'vEdge-remediation' rule, is highlighted with a red box. The details for this rule are: Status: Enabled, Rule Name: vEdge-remediation, Conditions: IdentityGroup Name ISDA&L User Identity Group: lab_admin, Profiles: vEdge-remediation, Security Groups: Select from list, Hits: 1, and Actions: [gear icon].

此策略根據使用者組lab_admin進行匹配並分配在第3步中建立的授權配置檔案。

步驟 5. 定義NAS（vEdge路由器或控制器），如下圖所示。

Identity Services Engine Administration

Network Resources

Network Devices List > 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: [i]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings [i]

DTLS Required: [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: []

General Settings

Enable KeyWrap: [i]

* Key Encryption Key: [] [Show]

* Message Authenticator Code Key: [] [Show]

Key Input Format: ASCII HEXADECIMAL

步驟 6. 配置vEdge/控制器。

```

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

```

步驟 7.驗證。登入到vEdge並確保將netadmin組分配給遠端使用者。

```
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和控制器的TACACS型使用者驗證和授權

步驟 1.建立TACACS配置檔案。在此步驟中，會將建立的TACACS設定檔指派給已驗證的使用者，例如netadmin許可權層級。

- 從Custom attribute部分選擇Mandatory以增加屬性：

類型	名稱	價值
必填	Viptela-Group-Name	netadmin

Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > **Device Settings**

Network Access > Guest Access > TrustSec > EPOD > Profiles > Posture > **Device Administration** > Privileged

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: [] (Select 0 to 15)
 Maximum Privilege: [] (Select 0 to 15)
 Access Control List: []
 Auto Comment: []
 No Escape: [] (Select true or false)
 Timeout: [] Minutes (0-9999)
 Idle Time: [] Minutes (0-9999)

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
Mandatory	Violate-Group-Name	netadmin

Cancel | Save

步驟 2. 為SD-WAN建立裝置組。

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

System > Identity Management > **Network Resources** > Device Profile Management > yGSM Services > Post Service > Threat Control NAC

Network Device > **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

Description

Parent Group

Cancel

Save

步驟 3. 配置裝置並將其分配給SD-WAN裝置組：

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

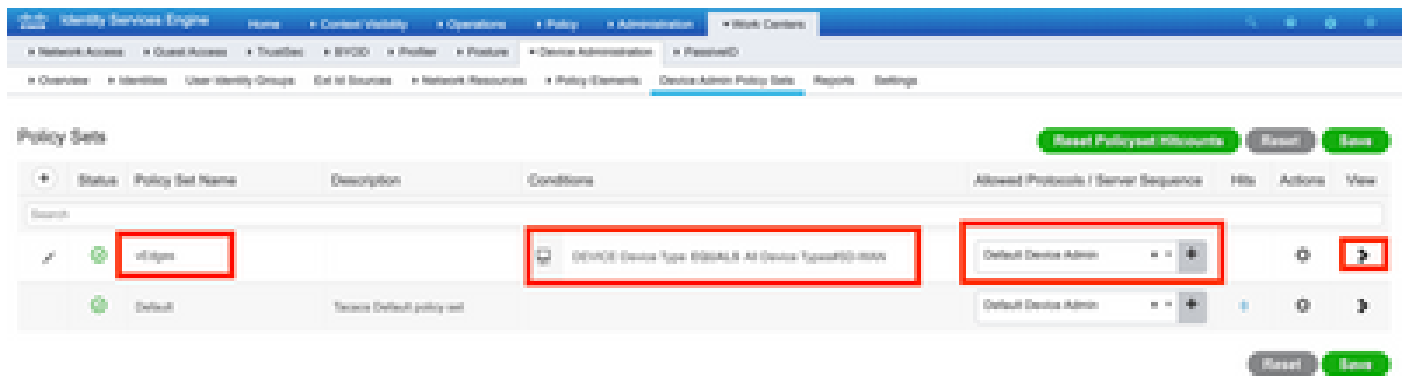
Advanced Truflow Settings

Save

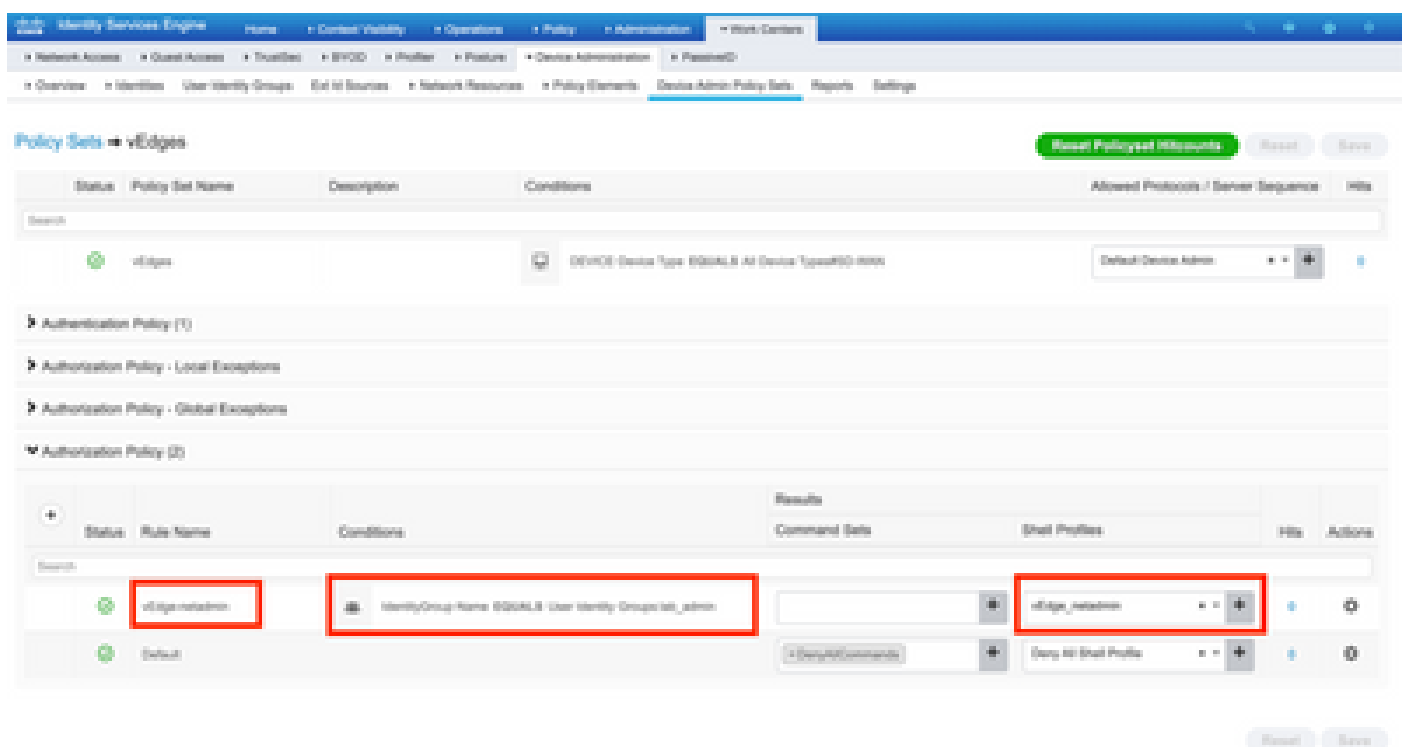
Reset

步驟 4. 定義裝置管理策略。

根據您的實際設定，策略集的外觀可能有所不同。出於本文檔中演示的目的，將建立策略。



按一下>，下一個螢幕將會顯示，如下圖所示。此策略根據名為SD-WAN的裝置型別進行匹配，並分配在步驟1中建立的Shell配置檔案。



步驟 5.配置vEdge：

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

步驟 6. 驗證。登入到vEdge並確保將netadmin組分配給遠端使用者：

```
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

相關資訊

- 思科ISE裝置管理規範部署指南：<https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- 配置使用者訪問和身份驗證：https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interface

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。