配置基於Radius和TACACS的使用者身份驗證

目錄

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。

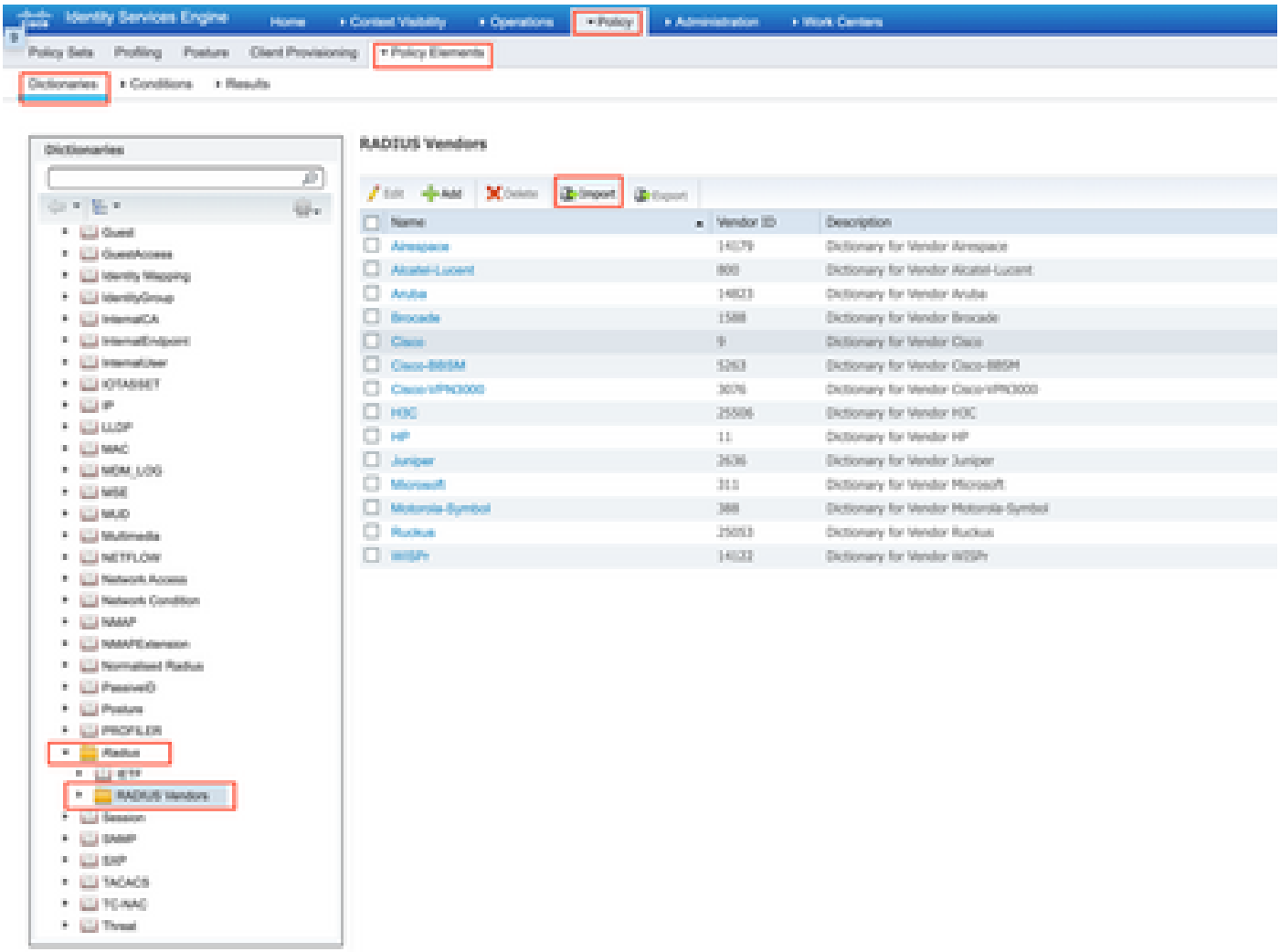
適用於vEdge和控制器的基於RADIUS的使用者身份驗證和授權

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：

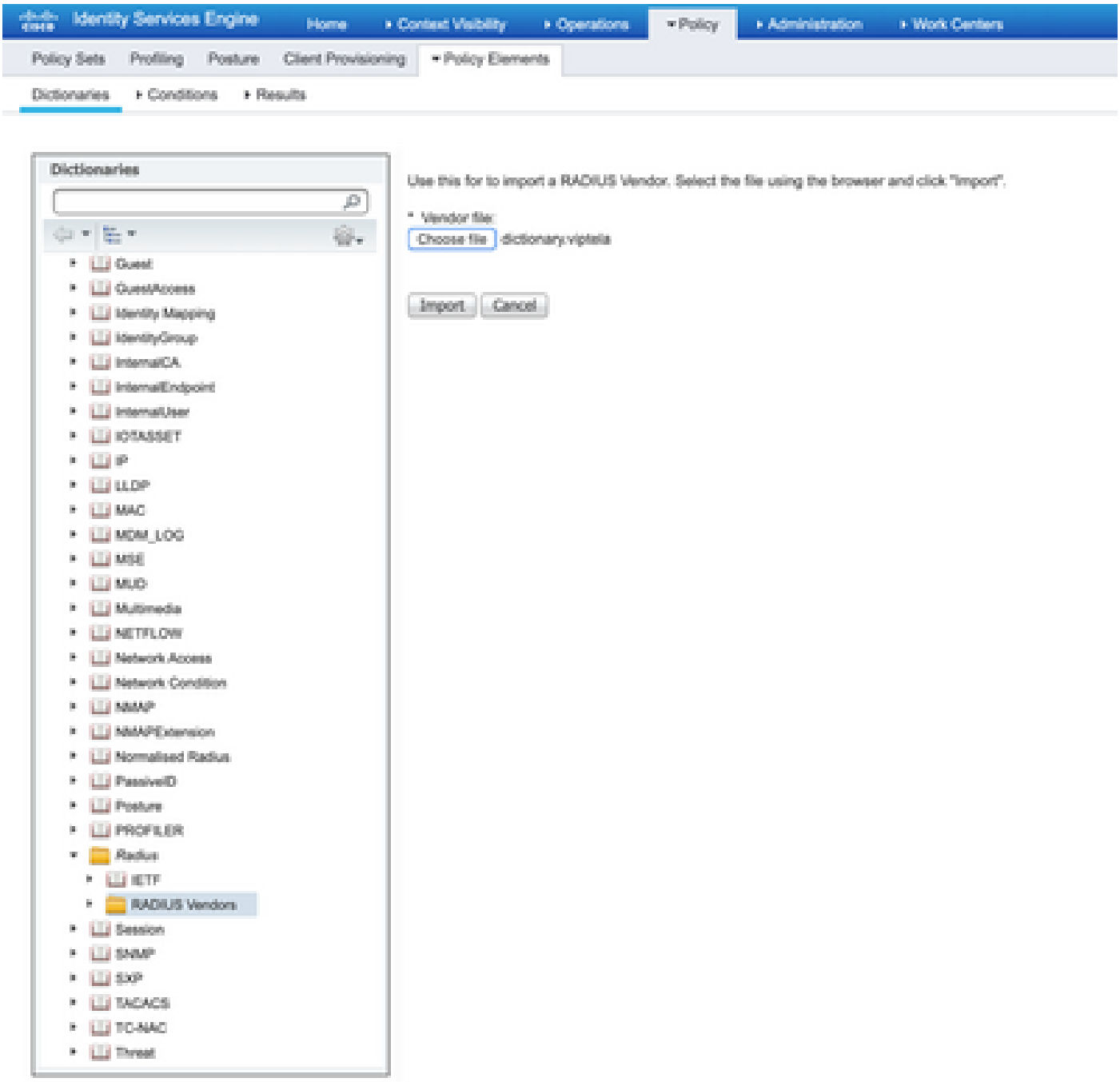
```
# -*- text -*-
#
#  dictionary.viptela
```

```
#
#
# Version:      $Id$
#

VENDOR          Viptela                         41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name              1     string
```

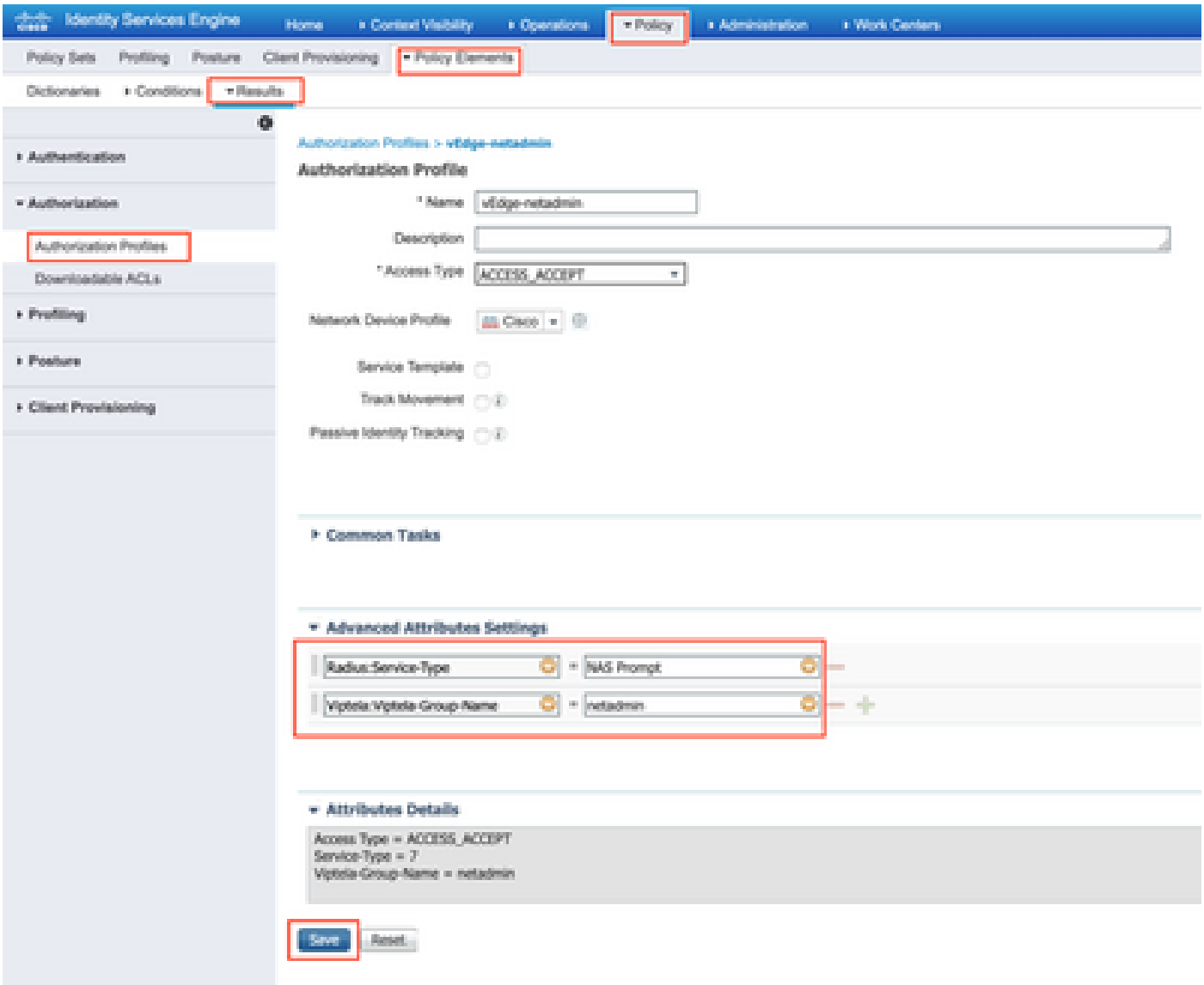
步驟 2.將詞典上傳到ISE。為此，請導航到策略>策略元素>詞典。從詞典清單中，導航到Radius > Radius Vendors，然後按一下Import（如圖所示）。



上傳您在步驟1中建立的檔案。

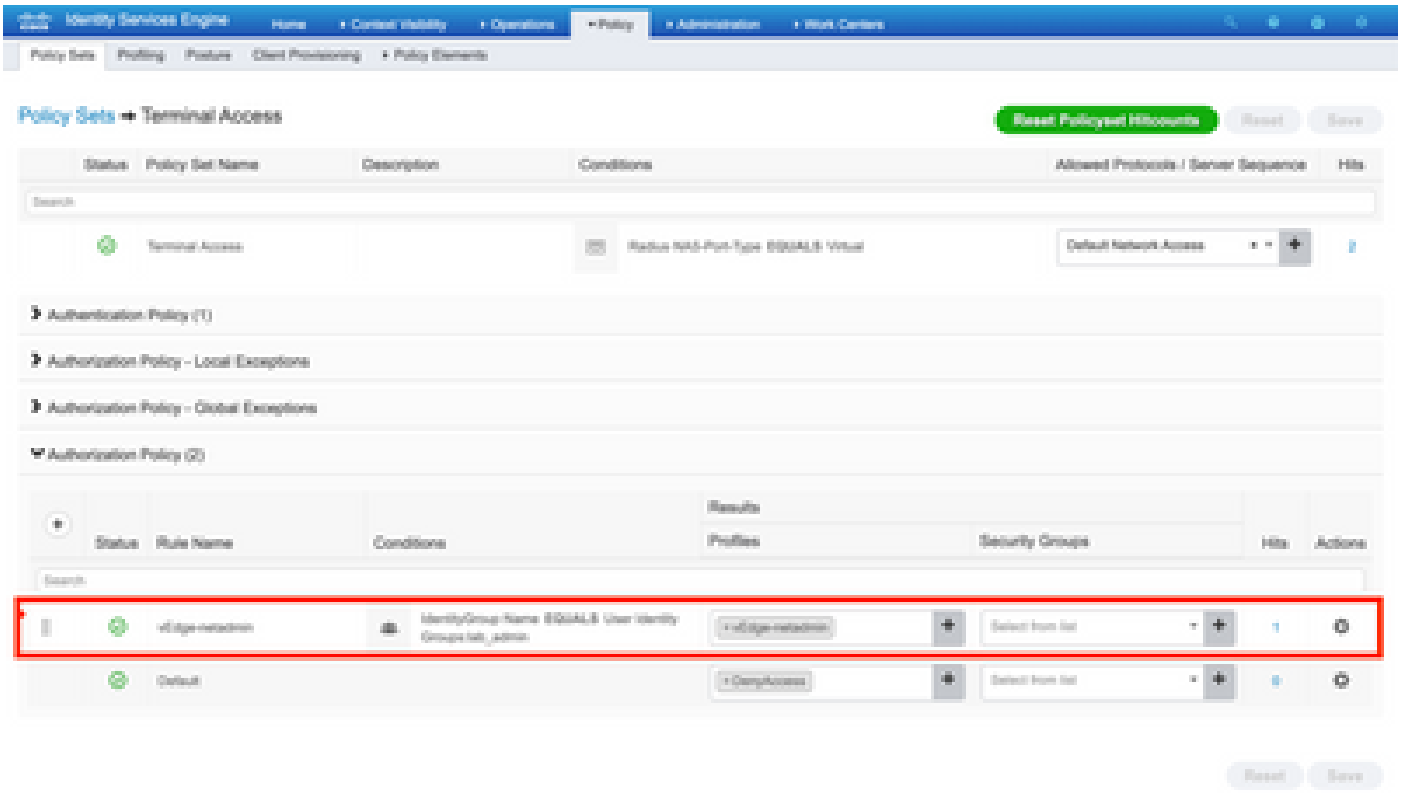


步驟 3.建立授權配置檔案。在此步驟中，Radius授權配置檔案將（例如）netadmin許可權級別分配給經過身份驗證的使用者。為此，請導航到策略>策略元素>授權配置檔案，並指定兩個高級屬性，如下圖所示。



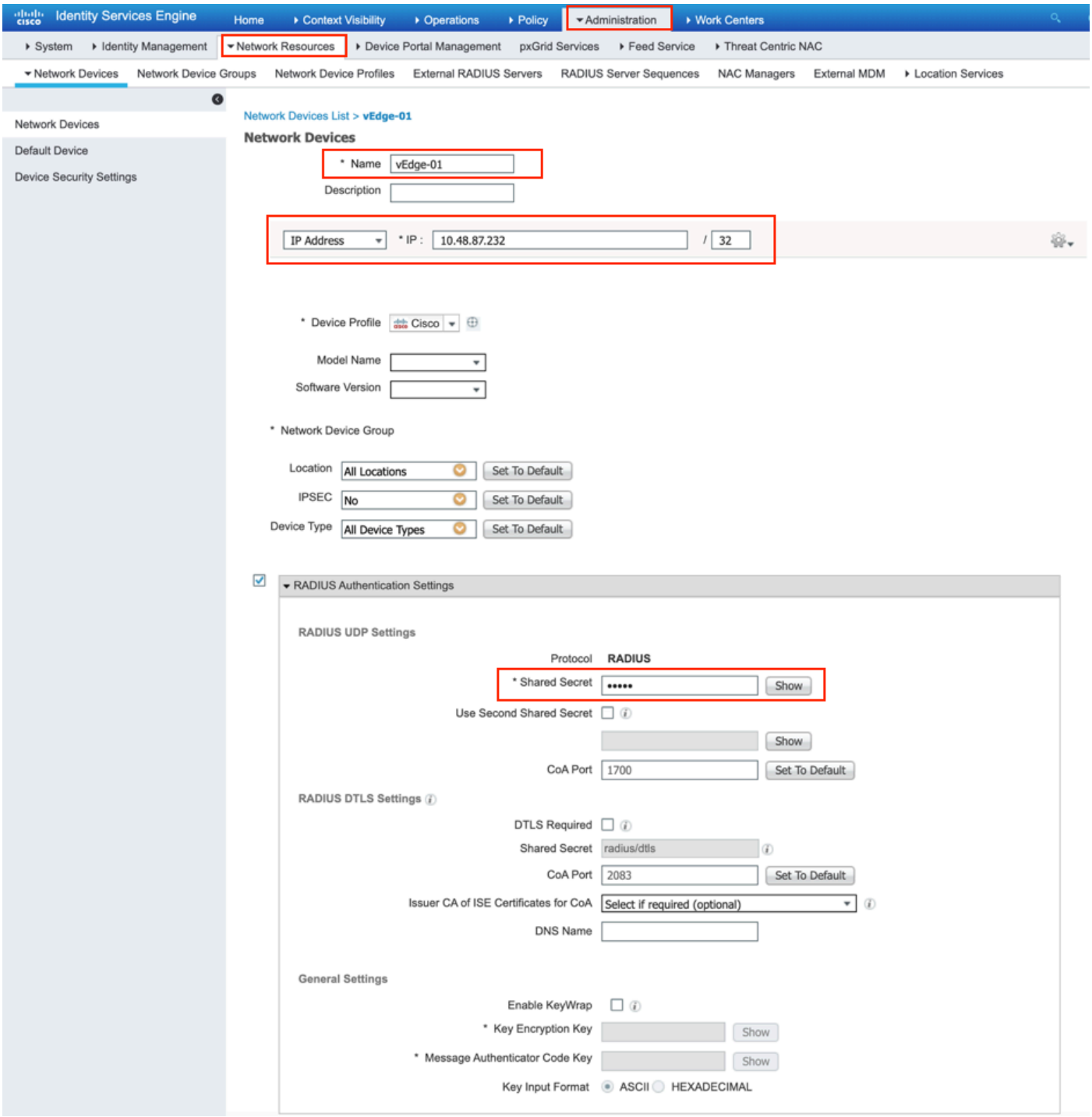
步驟 4.根據您的實際設定，策略集的外觀可能有所不同。出於本文演示的目的，我們建立了稱為終端訪問的策略條目，如下圖所示。

點選>，下一個螢幕會出現，如下圖所示。



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。



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。

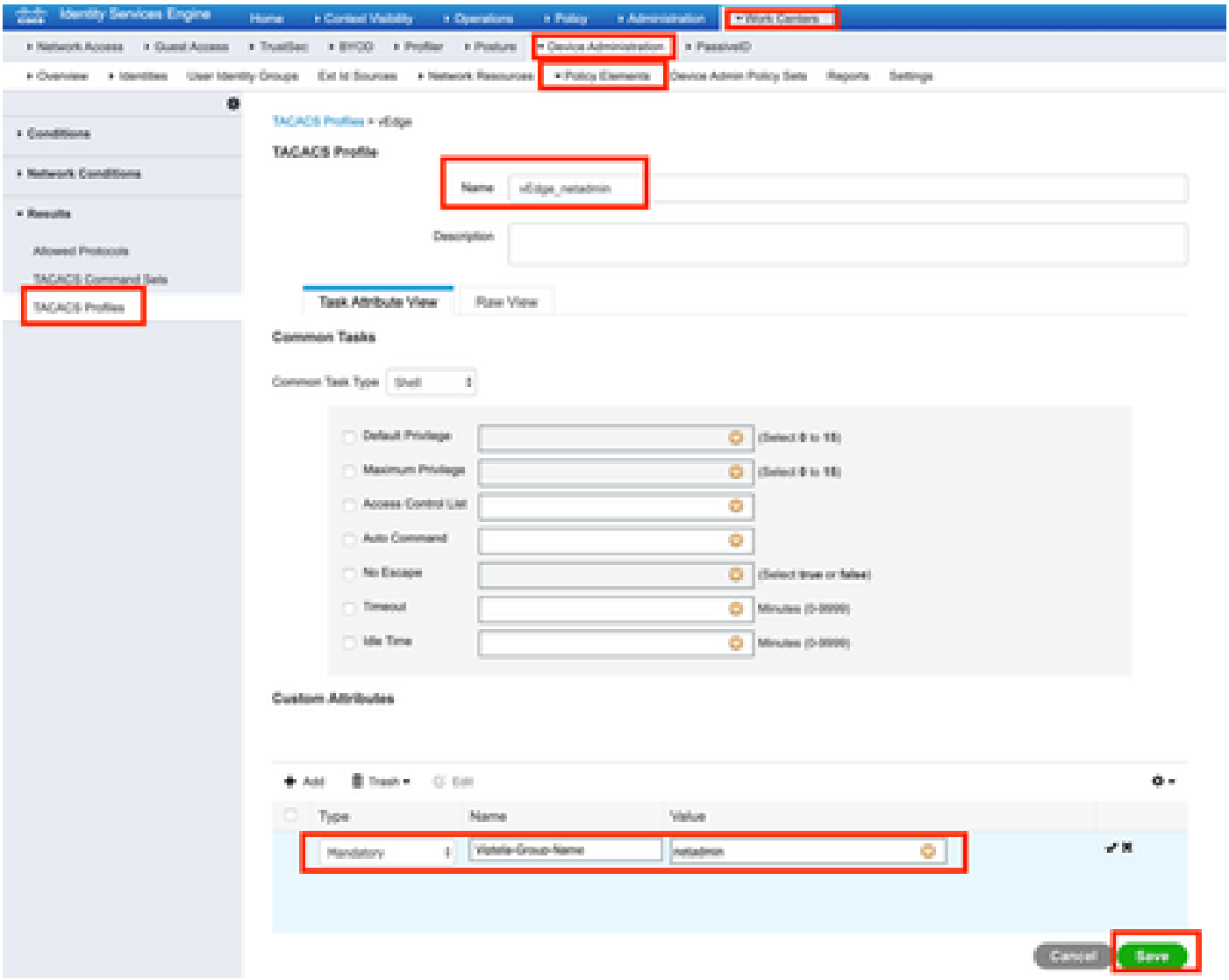
```
vEdgeCloud1# show users

                                                    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

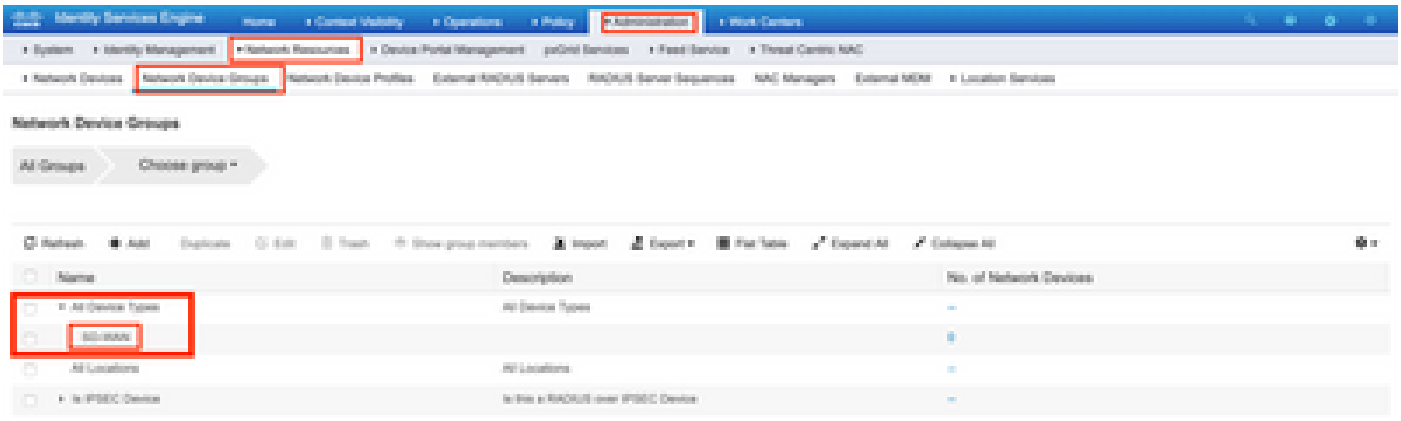
步驟 1.建立TACACS配置檔案。在此步驟中，會將建立的TACACS設定檔指派給已驗證的使用者，例如netadmin許可權層級。

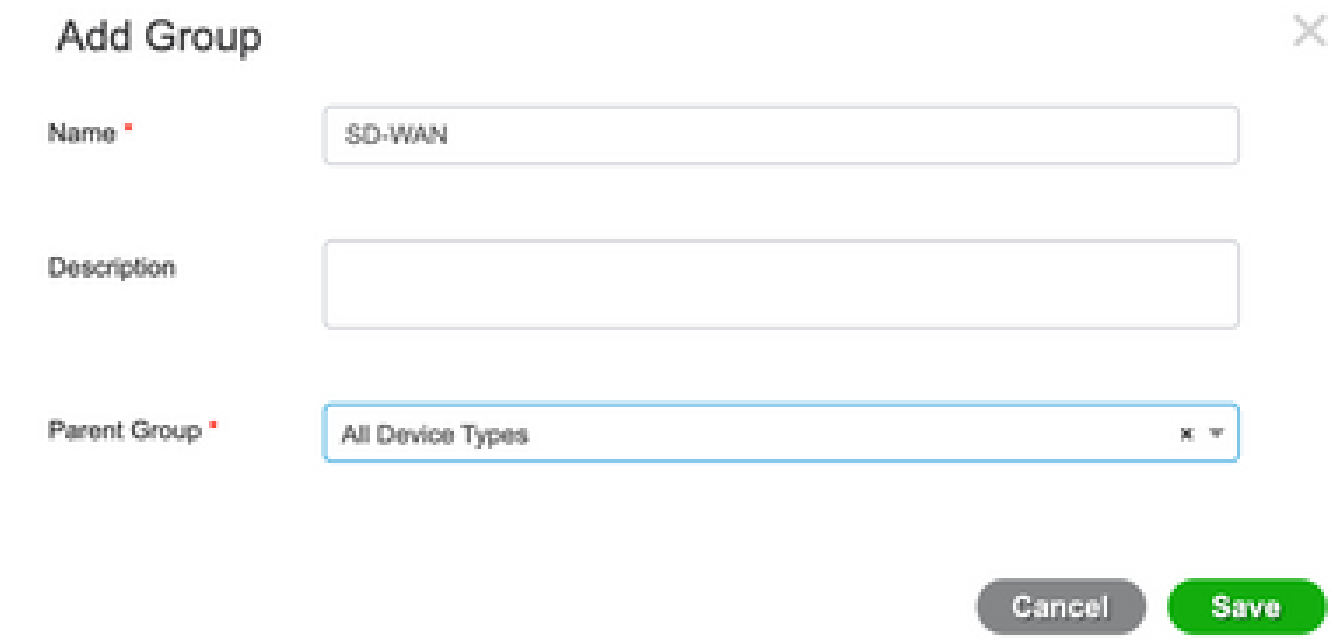
- 從Custom attribute部分選擇Mandatory以增加屬性：

類型	名稱	價值
必填	Viptela-Group-Name	netadmin

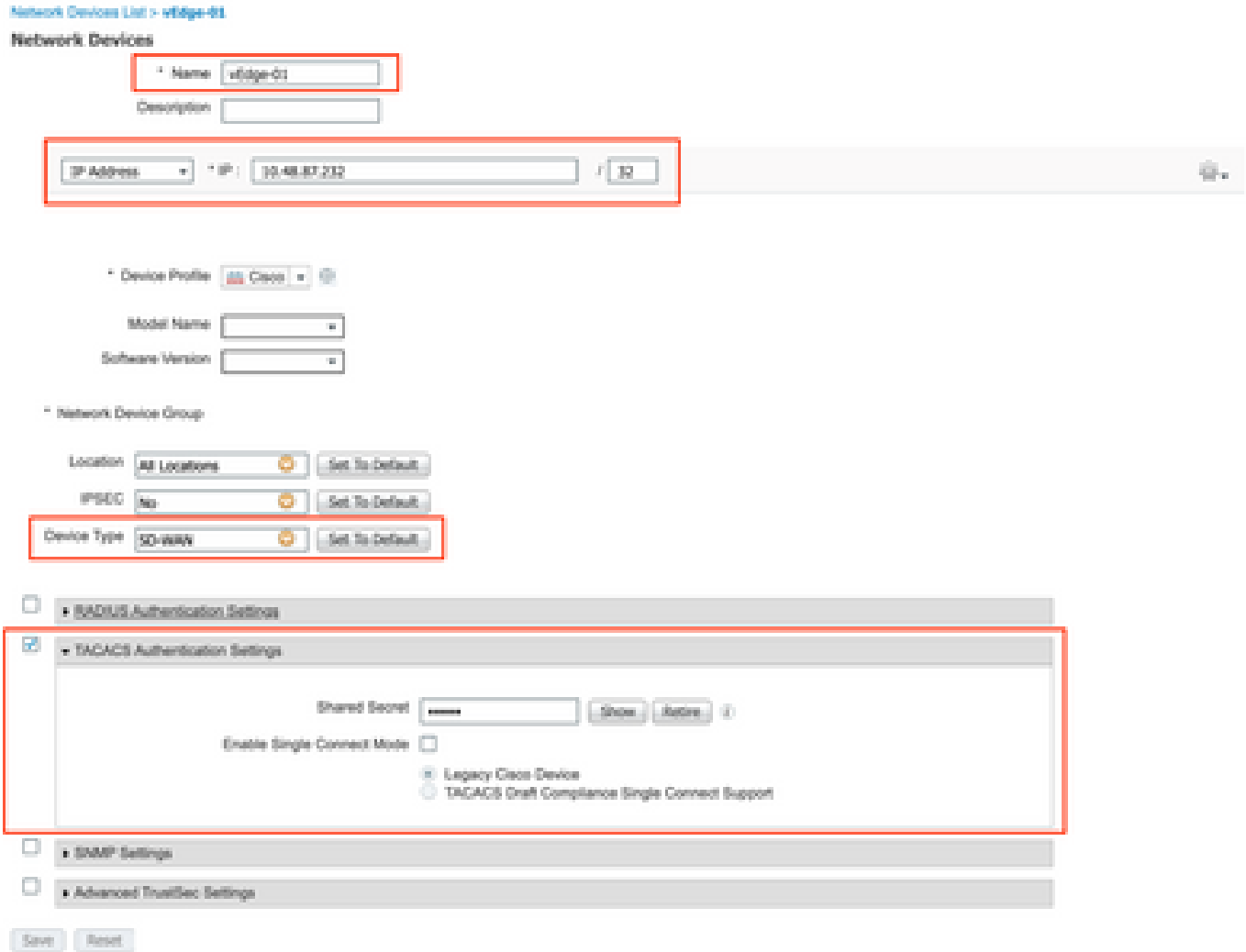


步驟 2.為SD-WAN建立裝置組。



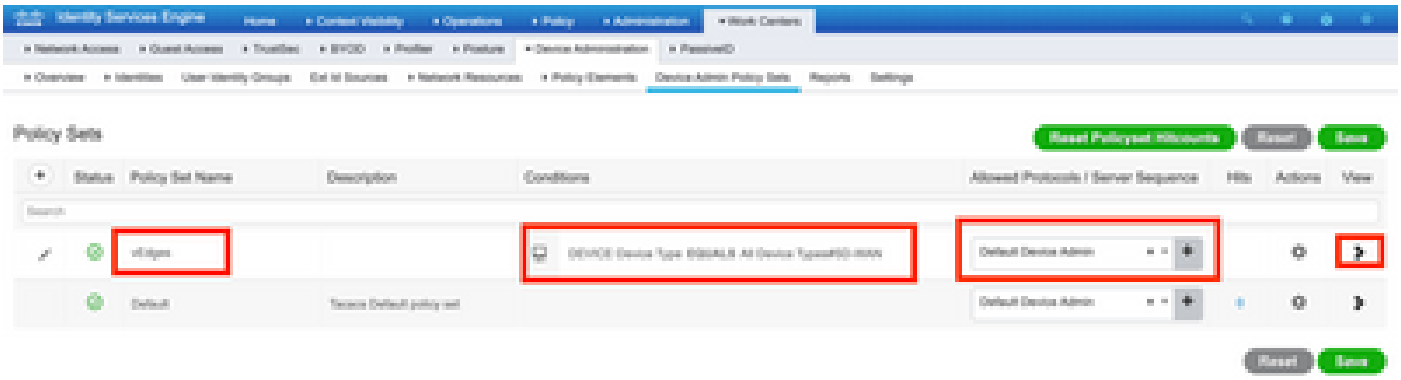


步驟 3.配置裝置並將其分配給SD-WAN裝置組：

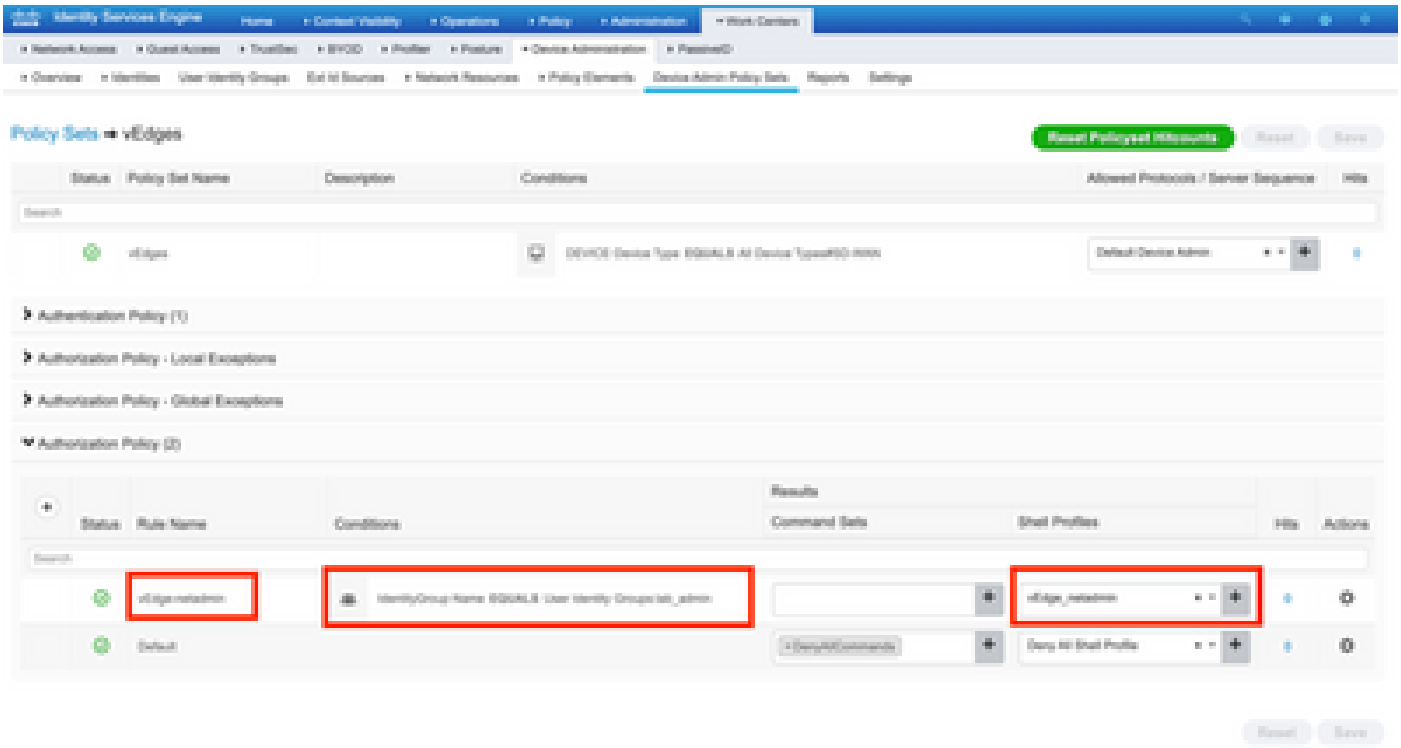


步驟 4.定義裝置管理策略。

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

                                                    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
```

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）。