將ISE配置為DNAC GUI的外部身份驗證

目錄

簡介

本文檔介紹如何將思科身份服務引擎(ISE)配置為用於Cisco DNA Center GUI管理的外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- TACACS+和RADIUS通訊協定。
- 思科ISE與思科DNA中心整合。
- Cisco ISE策略評估。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎(ISE)版本3.4補丁1。
- Cisco DNA中心版本2.3.5.5。

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。

開始之前

- 請確保在System > Settings > External Services > Authentication and Policy Servers上至少配置了一個RADIUS身份驗證伺服器。
- 只有對DNAC具有超級管理員角色許可權的使用者可以執行此過程。
- 啟用外部身份驗證回退。

⚠ 注意：在低於2.1.x的版本中，當啟用外部身份驗證時，如果AAA伺服器無法訪問或AAA伺服器拒絕未知使用者名稱，Cisco DNA Center將回退到本地使用者。在當前版本中，如果AAA伺服器無法訪問或AAA伺服器拒絕未知使用者名稱，Cisco DNA Center不會回退到本地使用者。啟用外部身份驗證回退後，外部使用者和本地管理員可以登入到Cisco DNA Center。

要啟用外部身份驗證回退，請通過SSH連線到Cisco DNA Center例項並輸入此CLI命令(magctl rbac external_auth_fallback enable)。

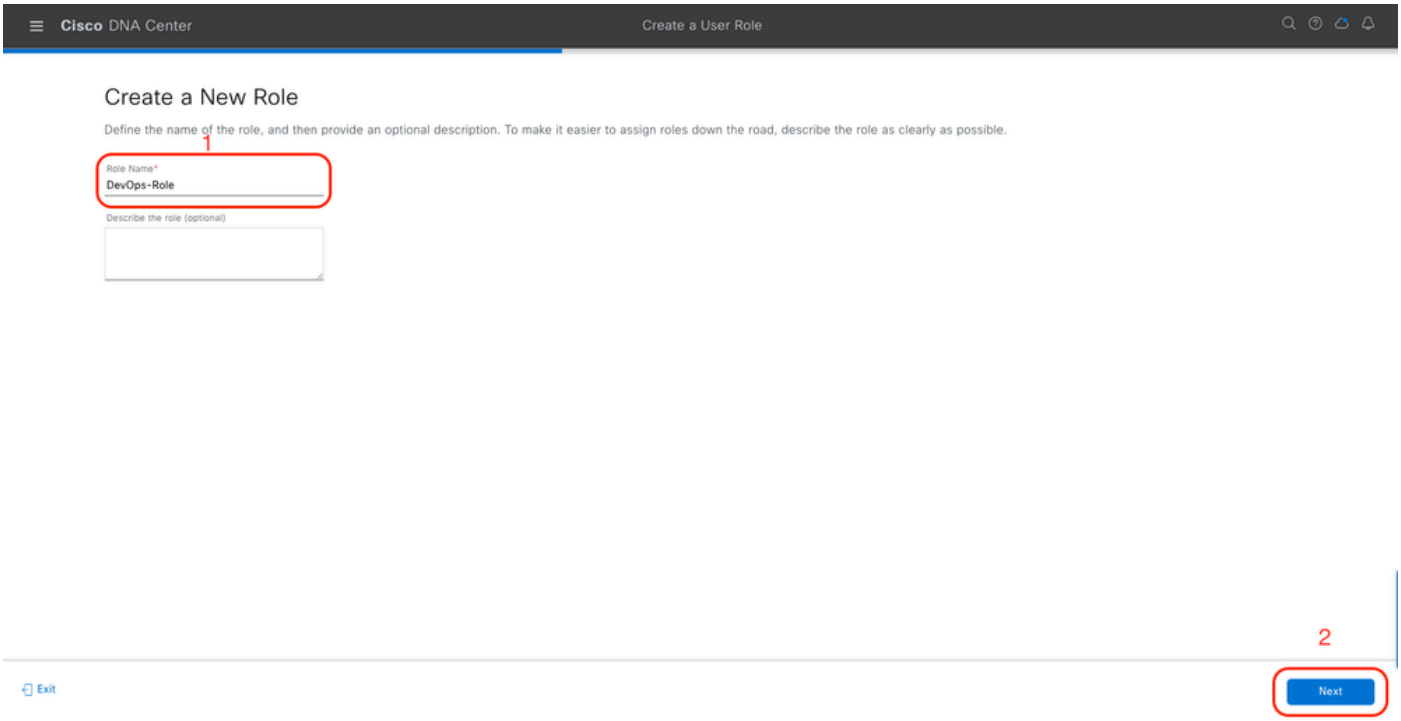
設定

（選項1）使用RADIUS配置DNAC外部身份驗證

步驟1.（可選）定義自定義角色。
配置滿足要求的自定義角色，而您可以使用預設的使用者角色。可從System > Users & Roles > Role Based Access Control頁籤執行此操作。

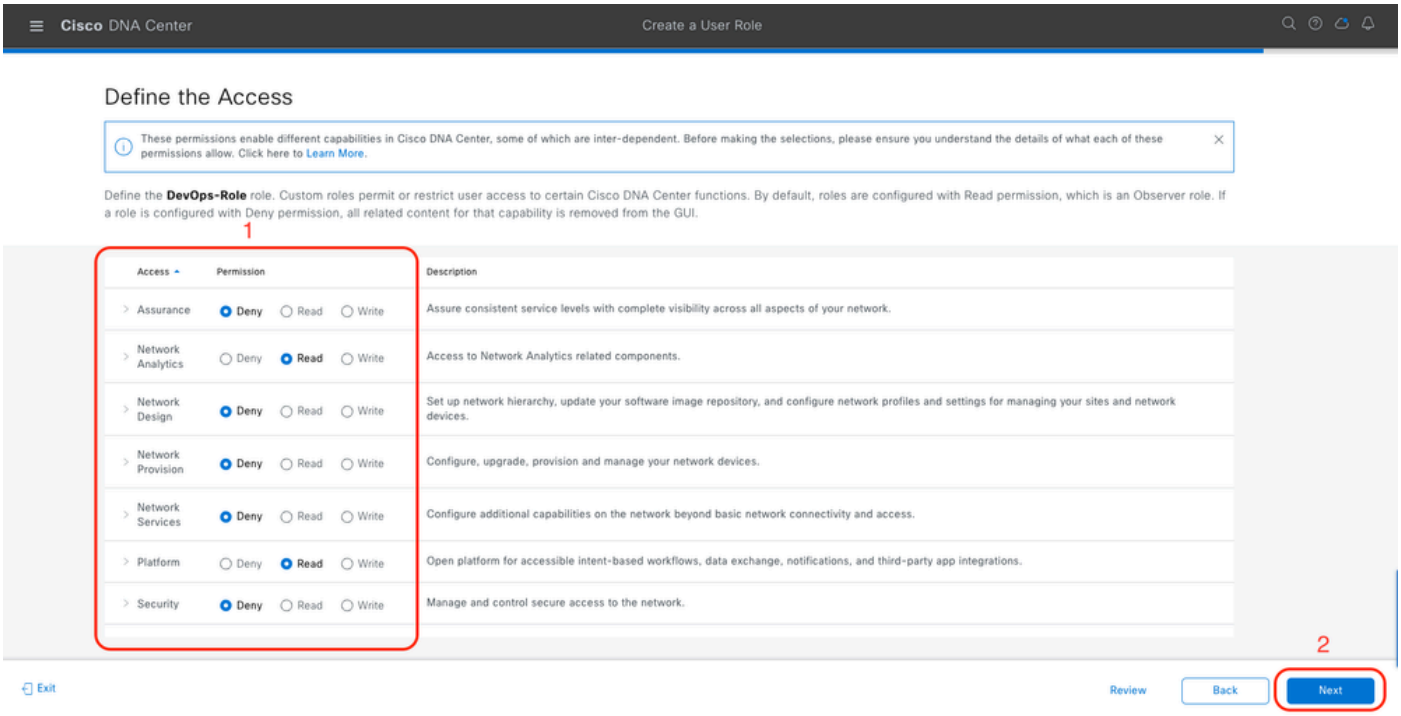
程式

a.建立新角色。



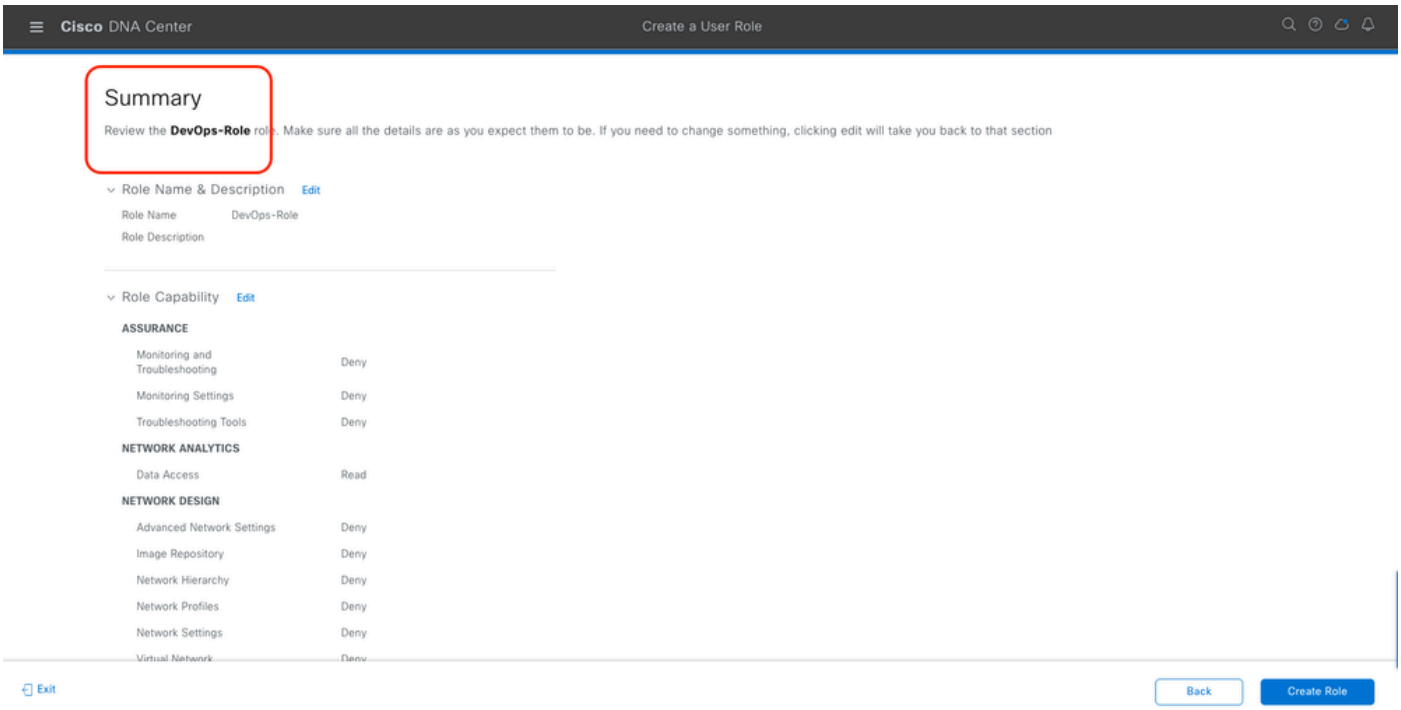
DevOps角色名稱

b.定義訪問。

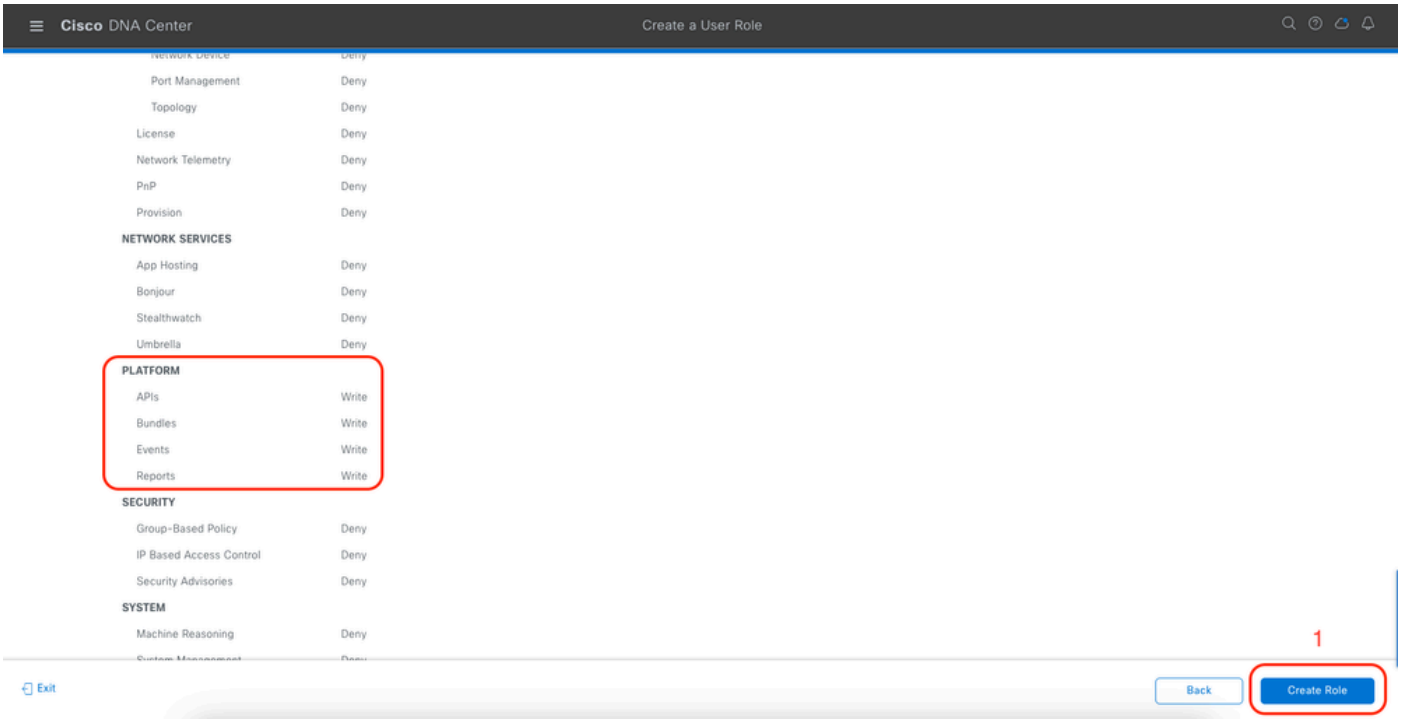


DevOps角色訪問

c.建立新角色。



DevOps角色摘要



稽核和建立DevOps角色

步驟2.使用RADIUS配置外部身份驗證。
可從System > Users & Roles > External Authentication頁籤執行此操作。

程式

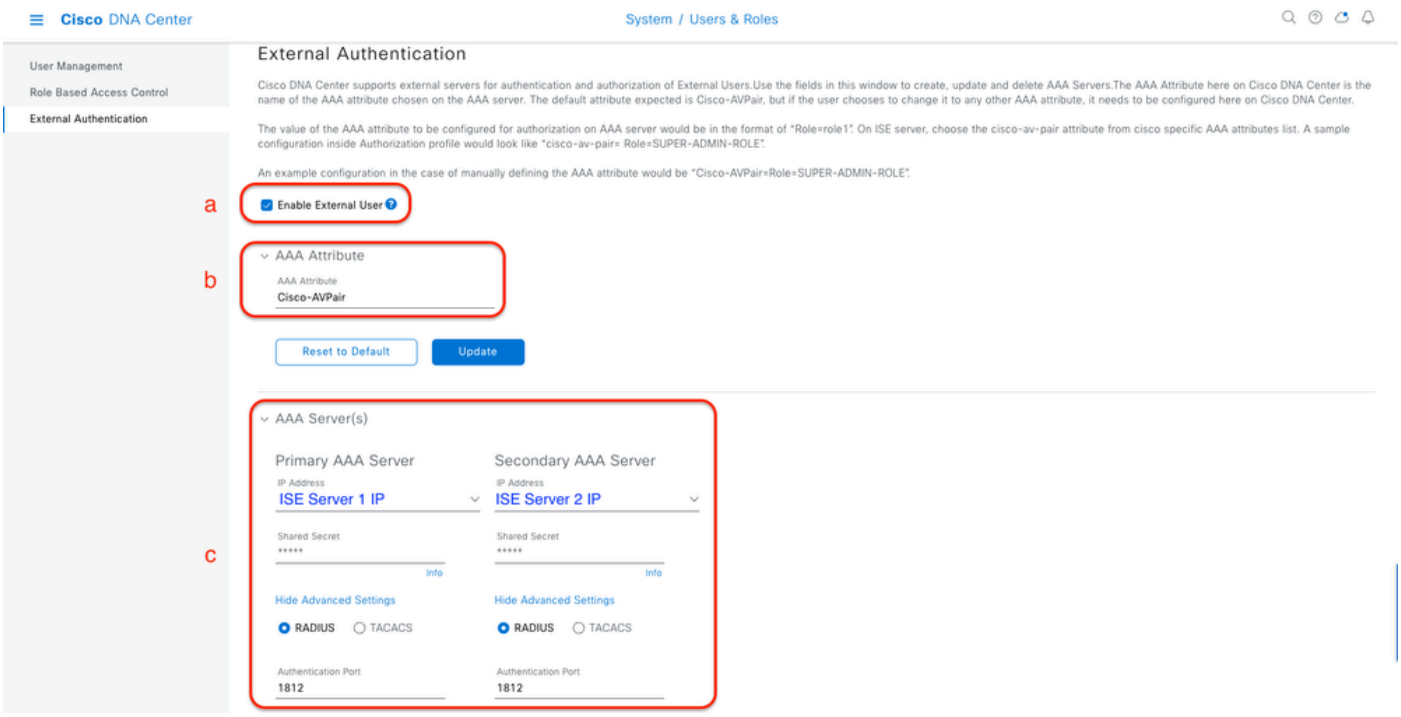
a.要在Cisco DNA Center中啟用外部身份驗證，請選中啟用外部使用者覈取方塊。

b.設定AAA屬性。

在AAA attributes欄位中輸入Cisco-AVPair。

c.（可選）配置主要和輔助AAA伺服器。

確保至少在主AAA伺服器上，或者在主伺服器和輔助伺服器上都啟用了RADIUS協定。



(RADIUS)外部身份驗證配置步驟

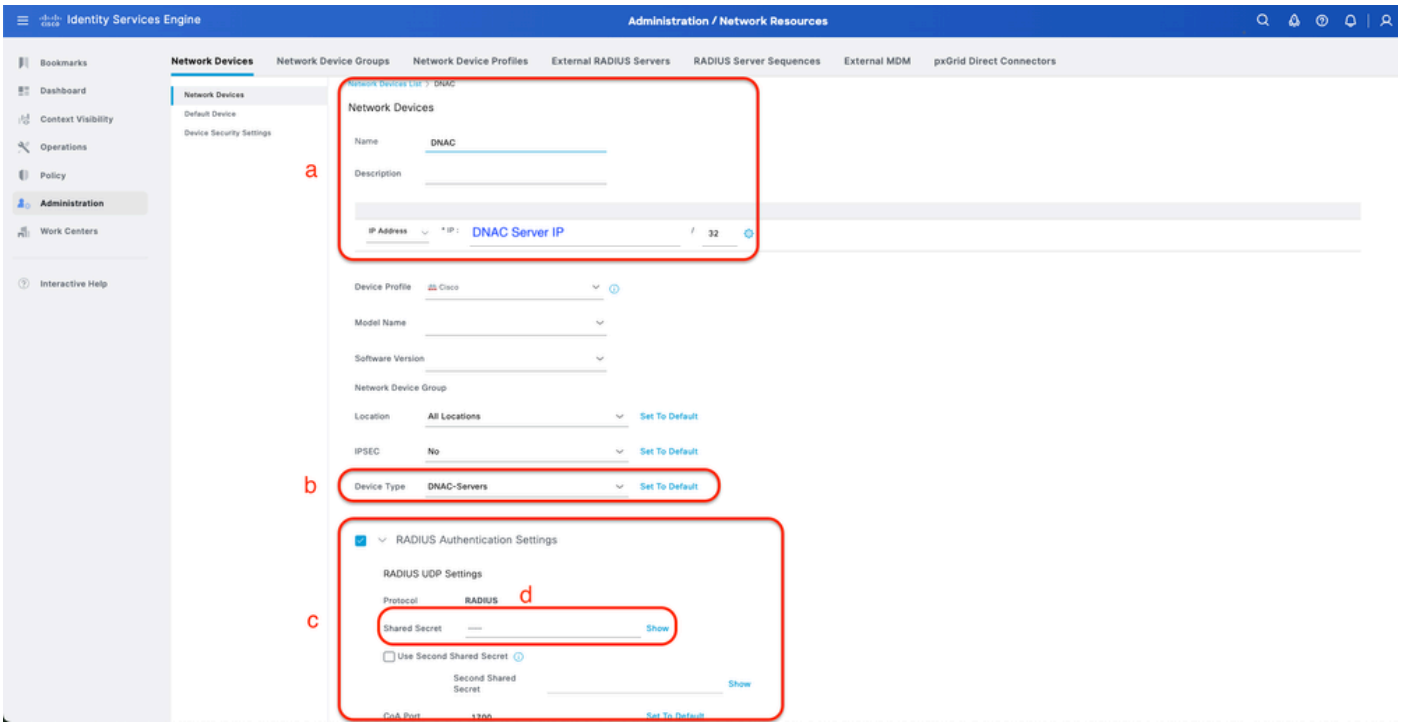
（選項1）為RADIUS配置ISE

步驟1.將DNAC伺服器新增為ISE上的網路裝置。

可從管理>網路資源>網路裝置索引標籤完成此操作。

程式

a.定義(DNAC)網路裝置名稱和IP。
b.（可選）為策略集條件對裝置型別進行分類。
c.啟用RADIUS身份驗證設定。
d.設定RADIUS共用金鑰。



適用於RADIUS的ISE網路裝置(DNAC)

步驟2.建立RADIUS授權設定檔。

這可通過頁籤完成 Policy > Policy Elements > Results > Authorization > 授權配置檔案。

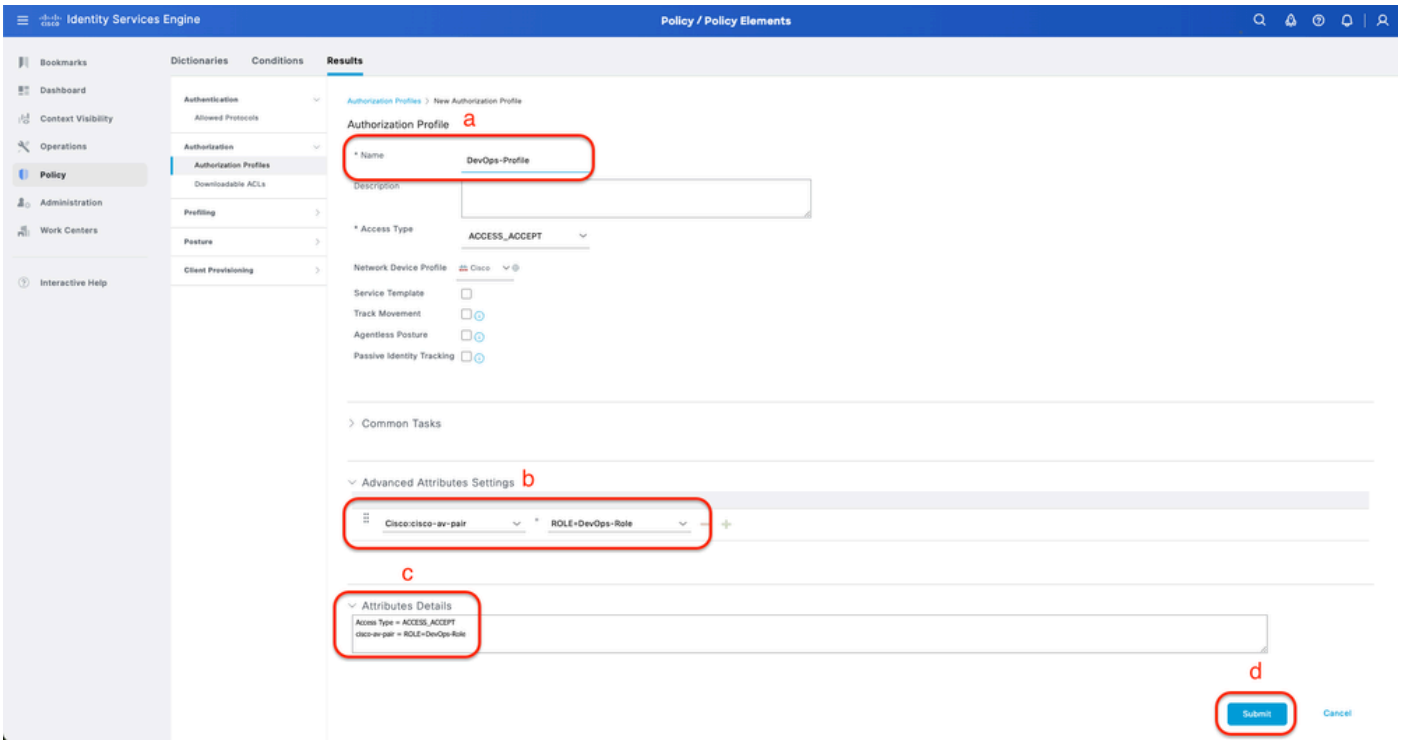
✎ 附註：建立3個RADIUS授權配置檔案，每個使用者角色一個。

程式
a.單擊Add並定義RADIUS授權配置檔名稱。

b.在「高級屬性設定」中輸入Cisco:cisco-av-pair，並填充正確的「使用者」角色。

- 對於(DecOps-Role)使用者角色，請輸入ROLE=DevOps-Role。
- 對於(NETWORK-ADMIN-ROLE)使用者角色，輸入ROLE=NETWORK-ADMIN-ROLE。
- 對於(SUPER-ADMIN-ROLE)使用者角色，輸入ROLE=SUPER-ADMIN-ROLE。

c.複查屬性詳細資訊。
d.按一下「Save」。



建立授權設定檔

步驟3.建立使用者組。

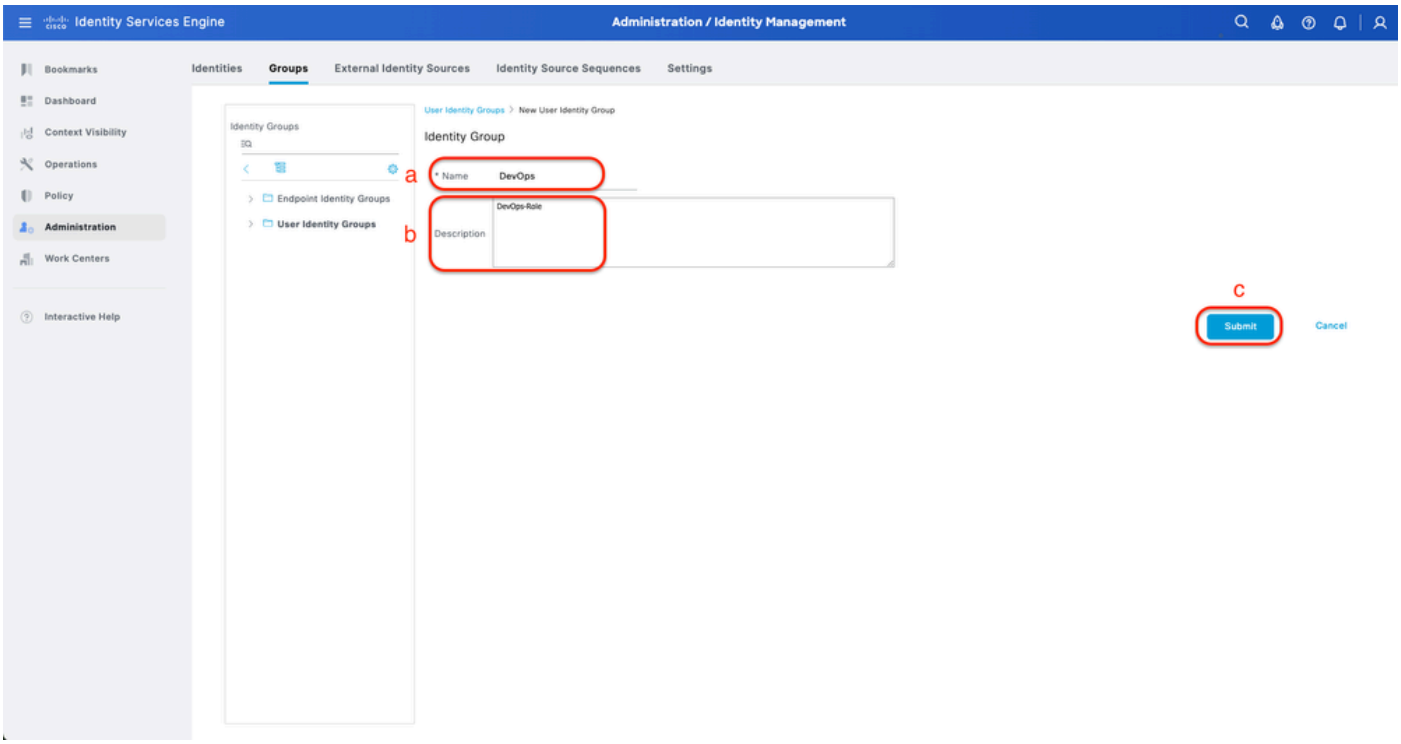
可從管理>身份管理>組>使用者身份組頁籤完成此操作。

程式

a.按一下Add並定義身份組名稱

b.（可選）定義說明。

c.按一下提交。



建立使用者身份組

步驟4.建立本地使用者。

可從Administration > Identity Management > Identities > Users頁籤執行此操作。

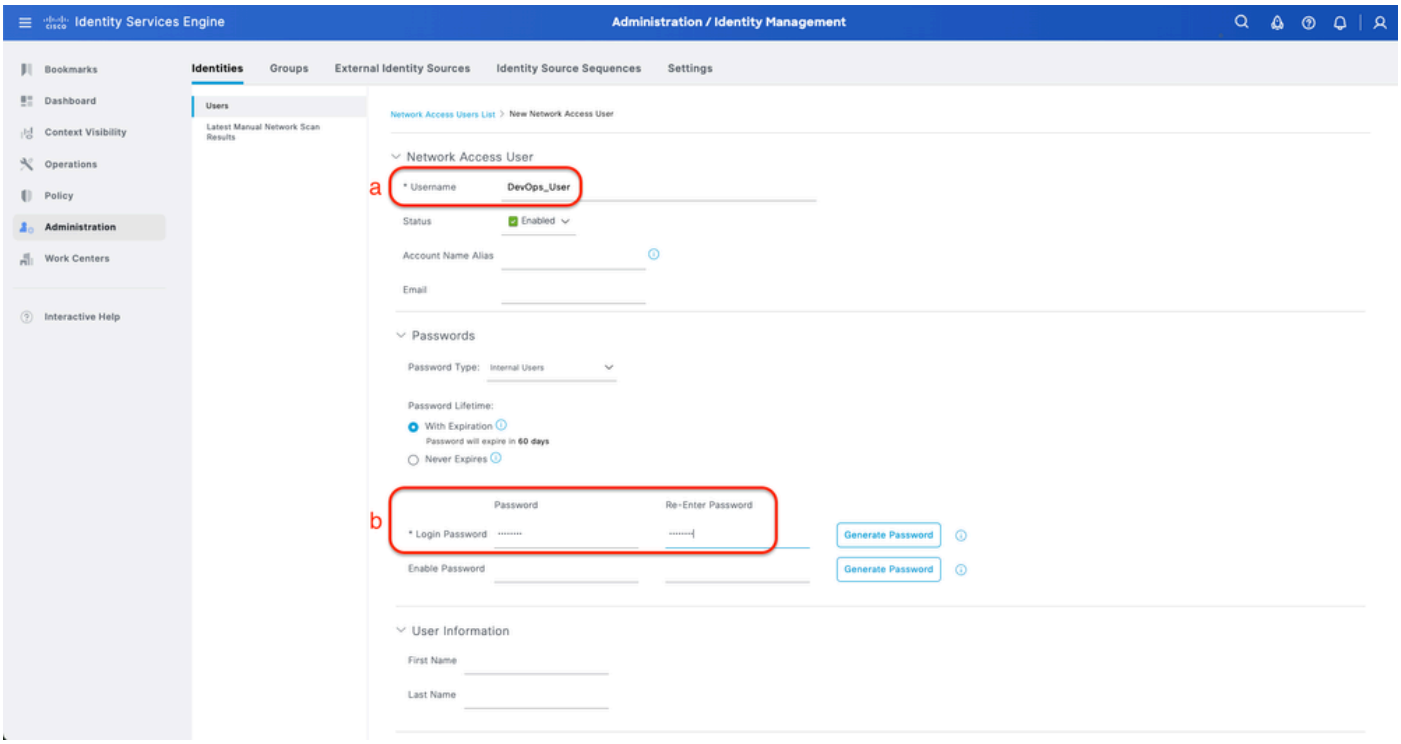
程式

a.按一下Add並定義使用者名稱。

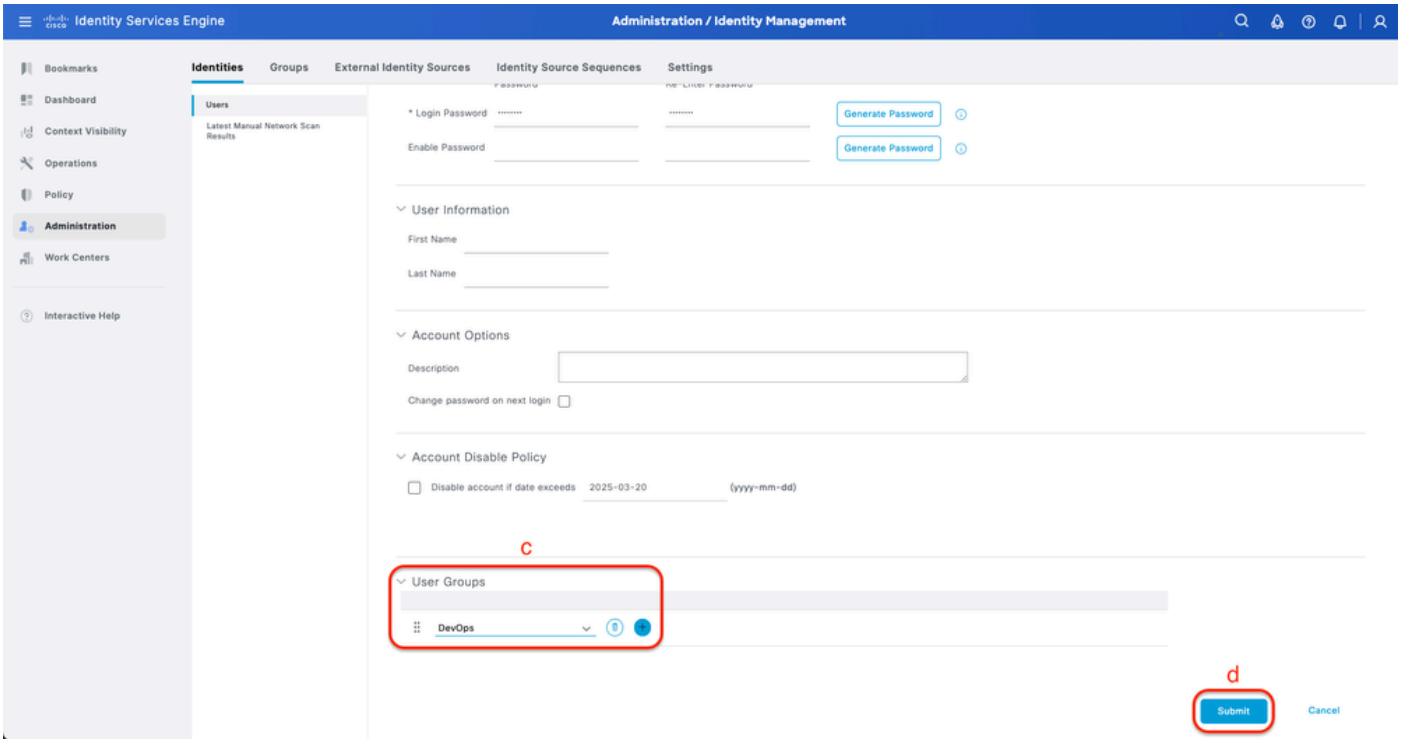
b.設定登入密碼。

c.將使用者新增到相關使用者組。

d.按一下「Submit」。



建立本地使用者1-2



建立本地使用者2-2

步驟5.（可選）新增RADIUS策略集。

可從Policy > Policy Sets頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

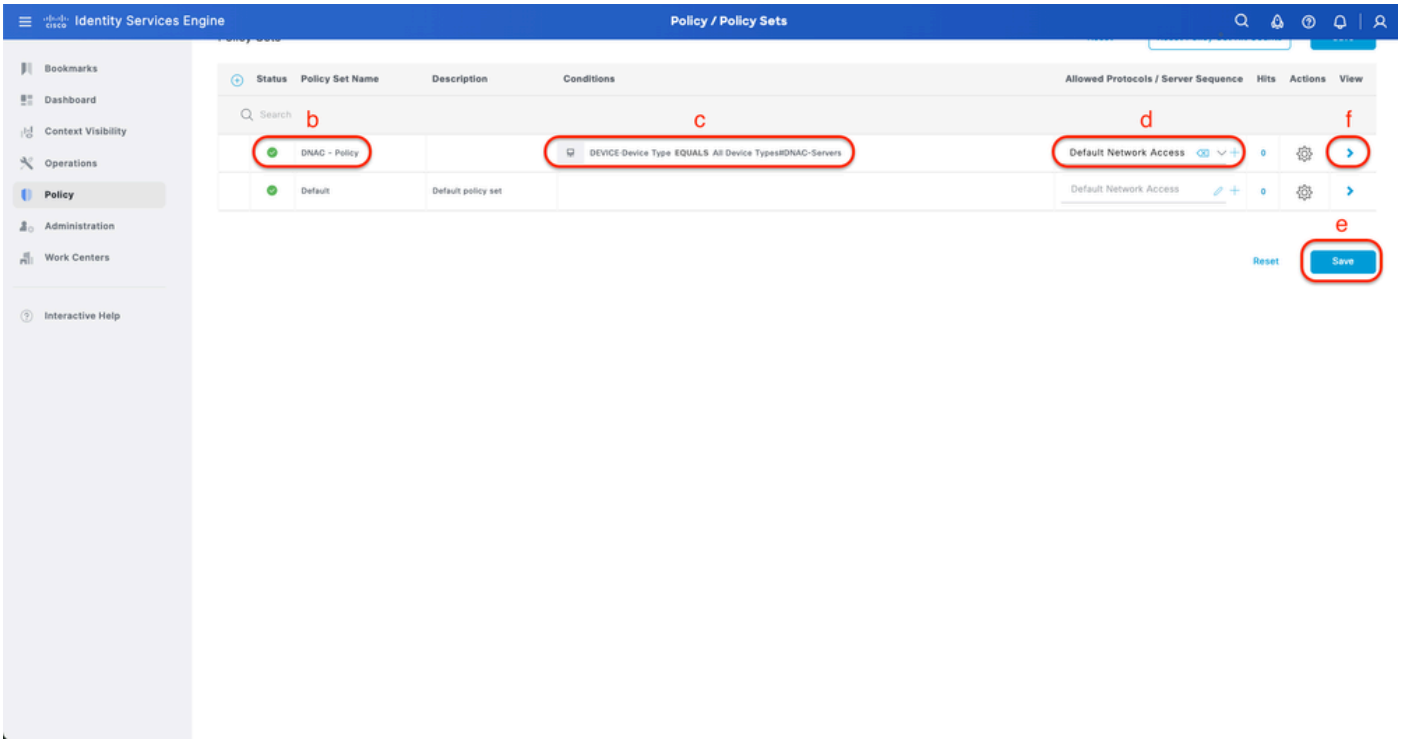
b.定義策略集名稱。

c.將Policy Set Condition設定為Select Device Type，您之前是在上建立的（步驟1 > b）。

d.設定Allowed協定。

e.按一下「Save」。

f.按一下(>)策略集檢視配置身份驗證和授權規則。



新增RADIUS策略集

步驟6.配置RADIUS身份驗證策略。

可從Policy > Policy Sets >按一下(>)頁籤完成此操作。

程式

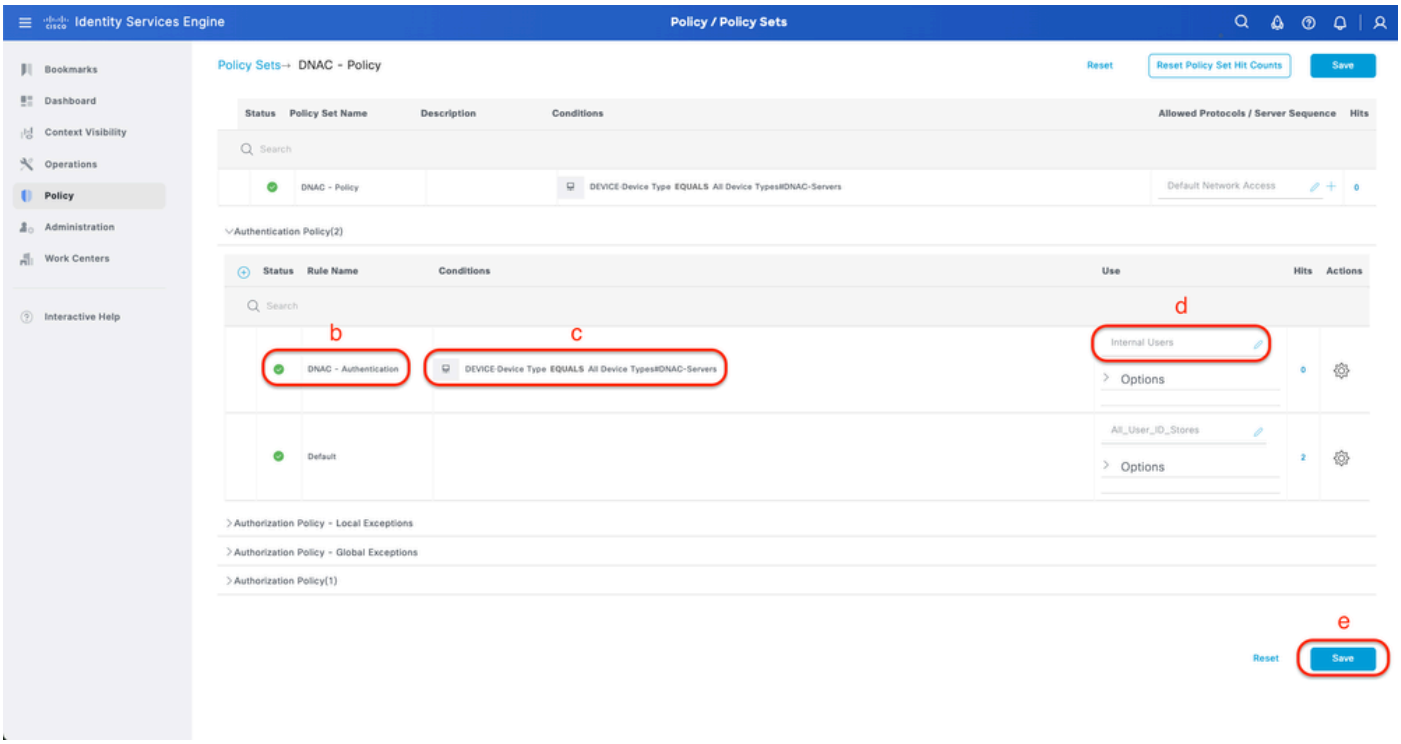
a.按一下Actions並選擇(在上面插入新行)。

b.定義身份驗證策略名稱。

c.設定身份驗證策略條件並選擇先前在上建立的裝置型別（步驟1 > b）。

d.設定Authentication Policy Use for Identity源。

e.按一下「Save」。



新增RADIUS身份驗證策略

步驟7.配置RADIUS授權策略。

可從Policy > Policy Sets>按一下(>)頁籤完成此操作。

此步驟用於為每個用戶角色建立授權策略：

- 超級管理員角色
- NETWORK-ADMIN-ROLE
- DevOps — 角色

程式

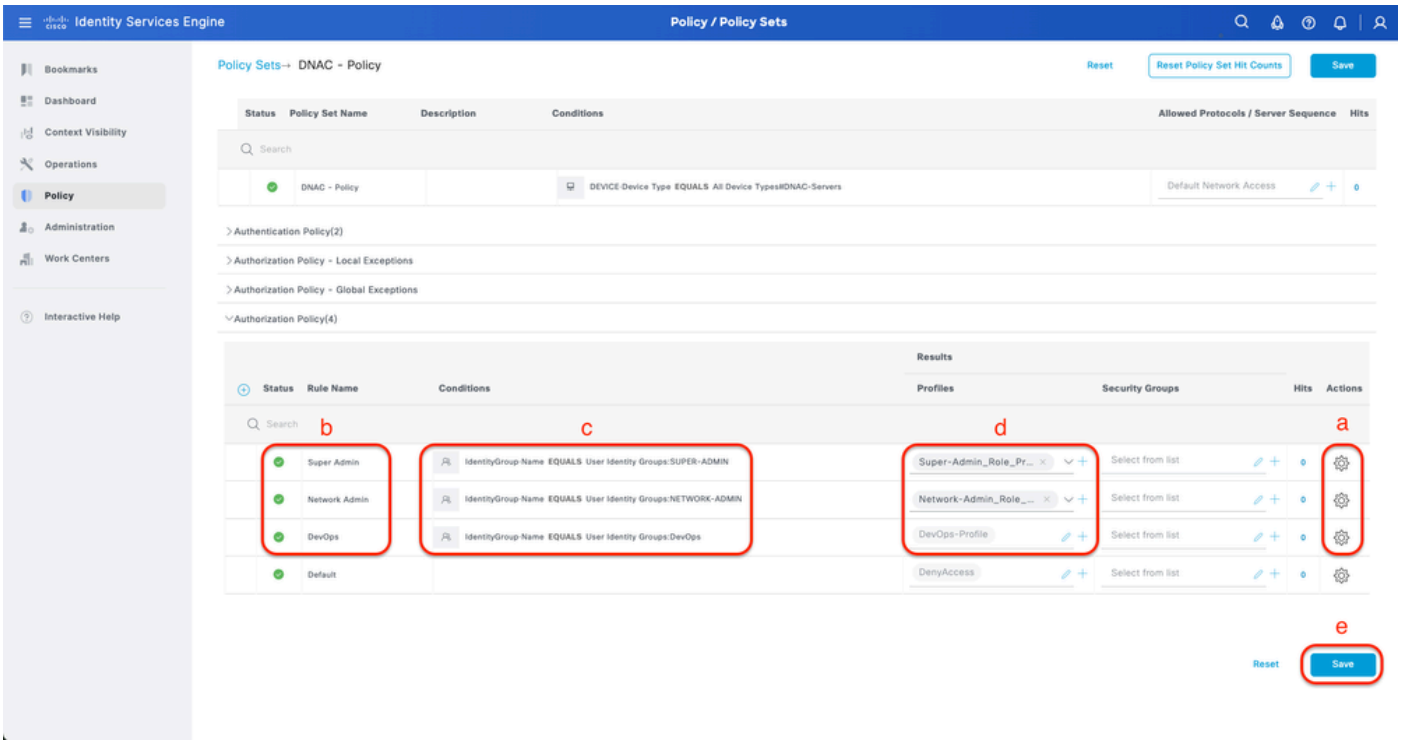
a.按一下Actions並選擇(在上面插入新行)。

b.定義授權策略名稱。

c.設定授權策略條件並選擇在中建立的使用者組（步驟3）。

d.設定授權策略結果/配置檔案並選擇您在(Step2)中建立的授權配置檔案。

e.按一下「Save」。



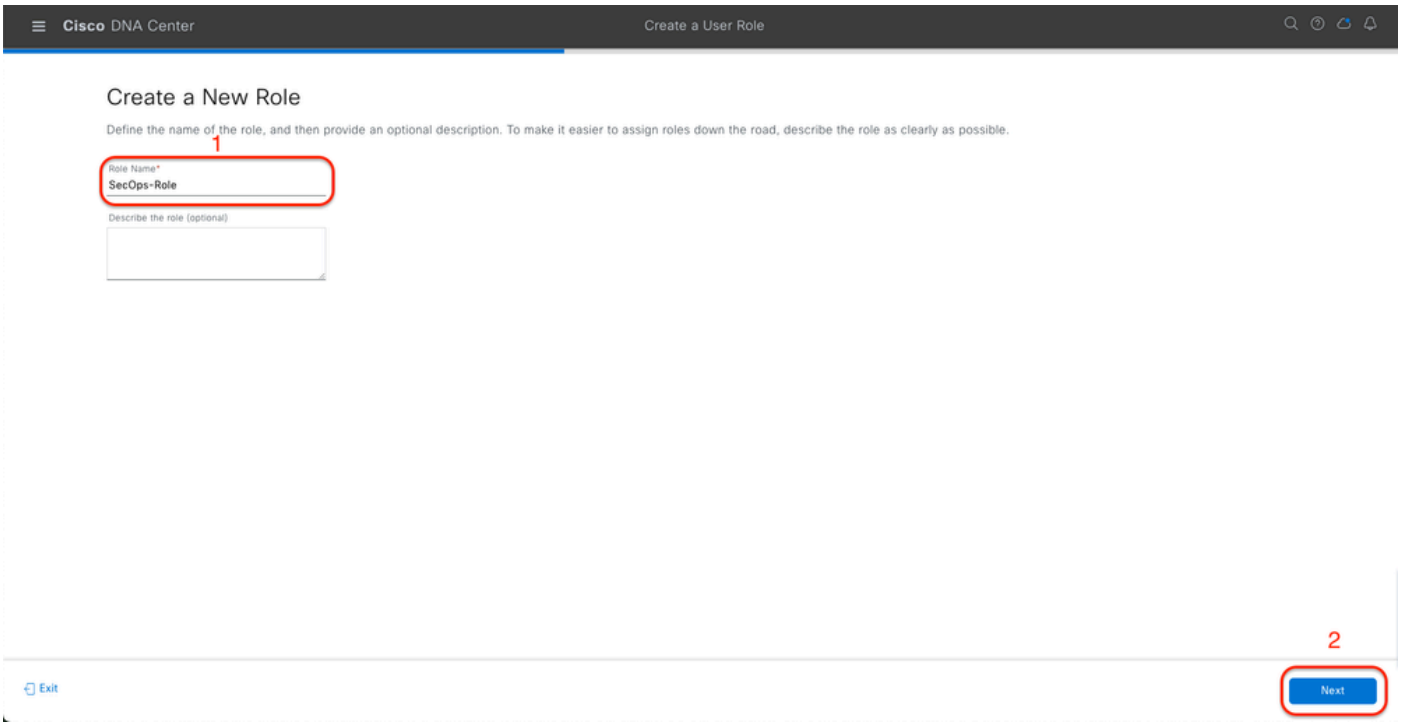
新增授權策略

（選項2）使用TACACS+配置DNAC外部身份驗證

步驟1.（可選）定義自定義角色。
配置滿足要求的自定義角色，而您可以使用預設的使用者角色。可從System > Users & Roles > Role Based Access Control頁籤執行此操作。

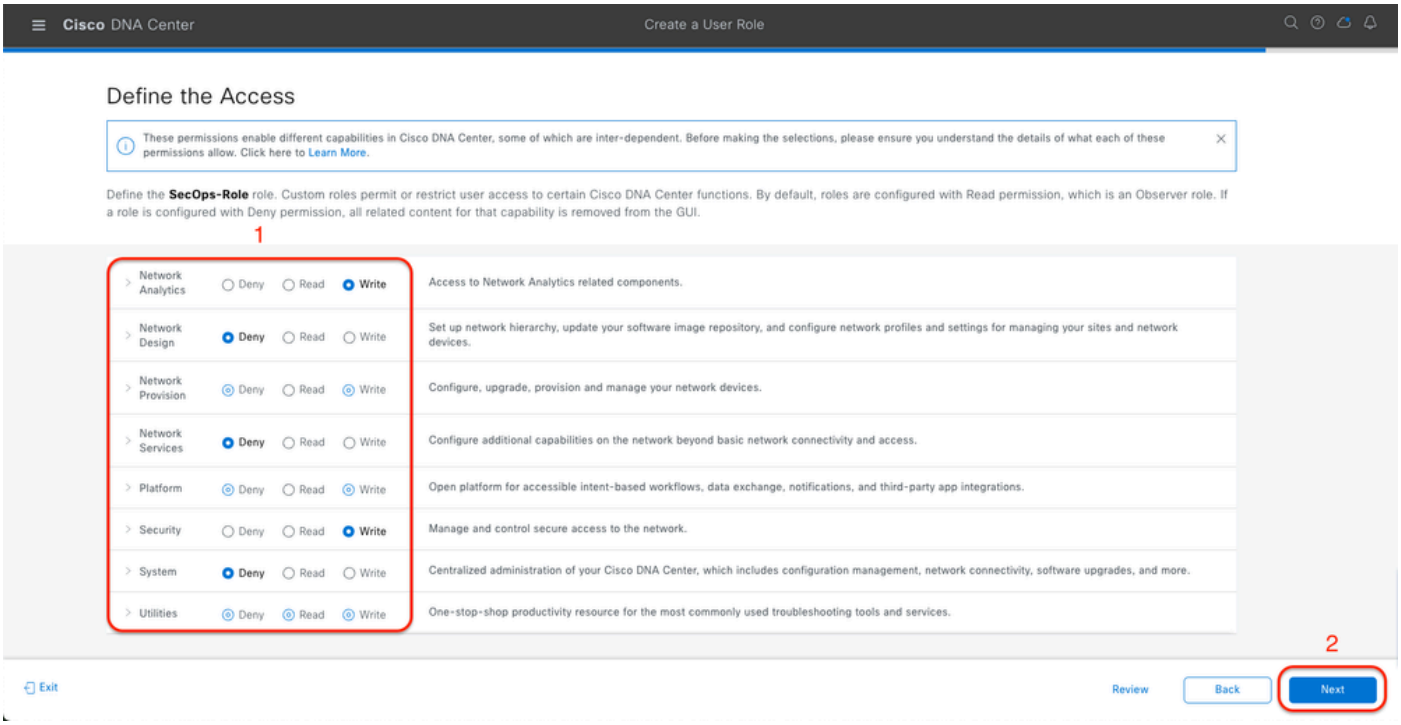
程式

a.建立新角色。



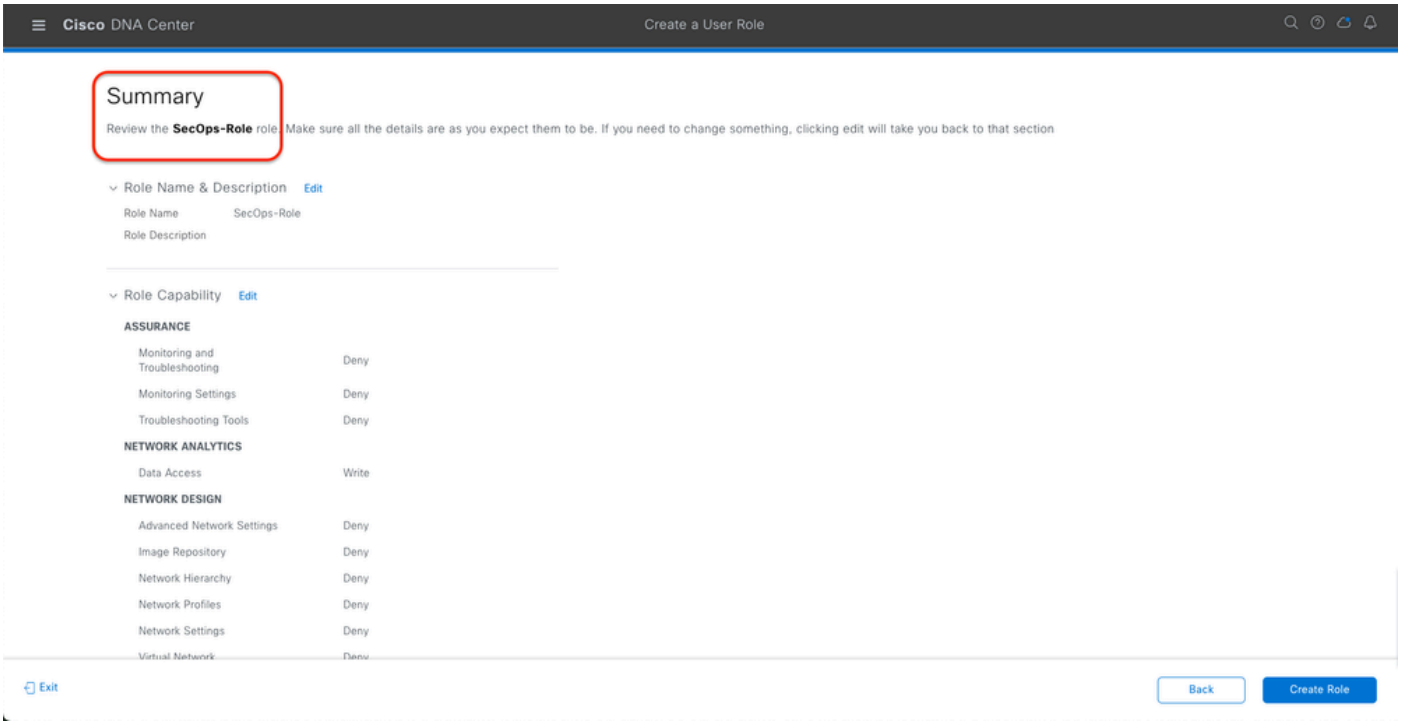
SecOps角色名稱

b.定義訪問。

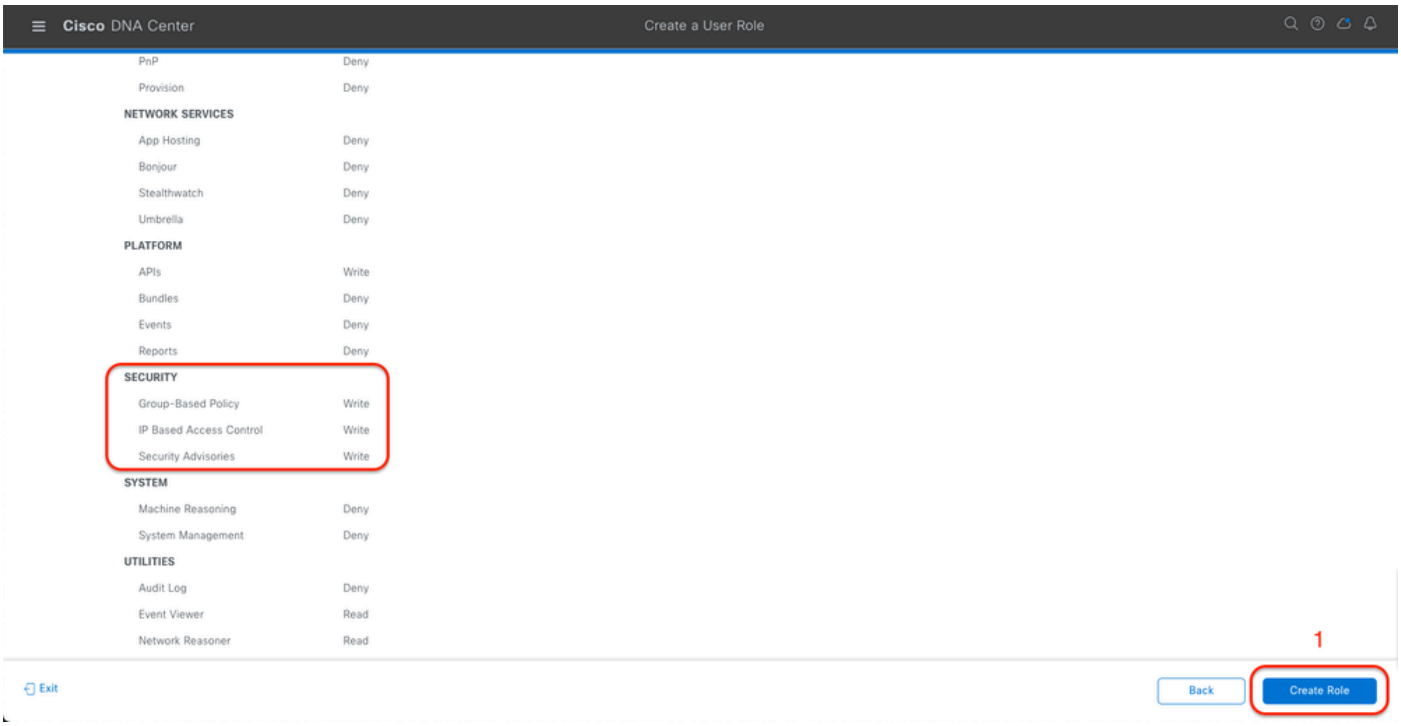


SecOps角色訪問

c.建立新角色。



SecOps角色摘要



檢視和建立SecOps角色

步驟2.使用TACACS+配置外部身份驗證。
可從System > Users & Roles > External Authentication頁籤執行此操作。

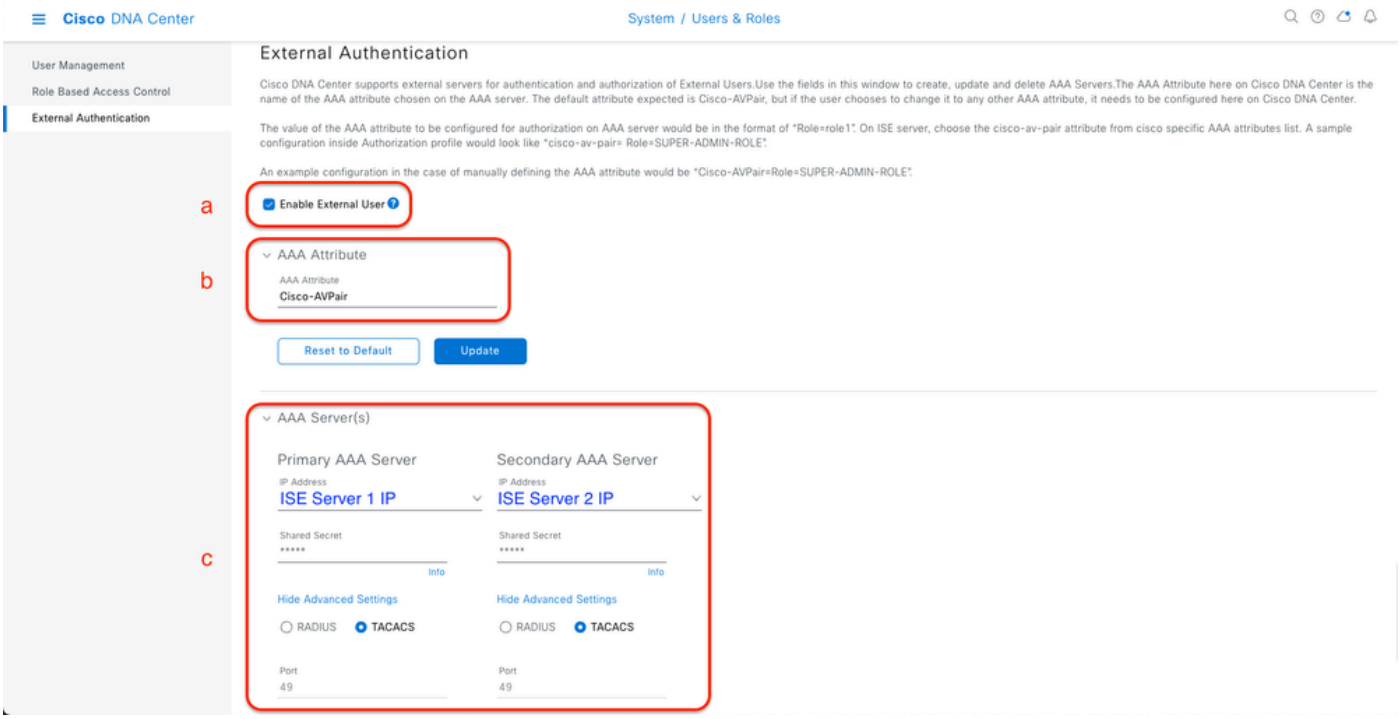
a.要在Cisco DNA Center中啟用外部身份驗證，請選中啟用外部使用者覈取方塊。

b.設定AAA屬性。

在AAA attributes欄位中輸入Cisco-AVPair。

c.（可選）配置主要和輔助AAA伺服器。

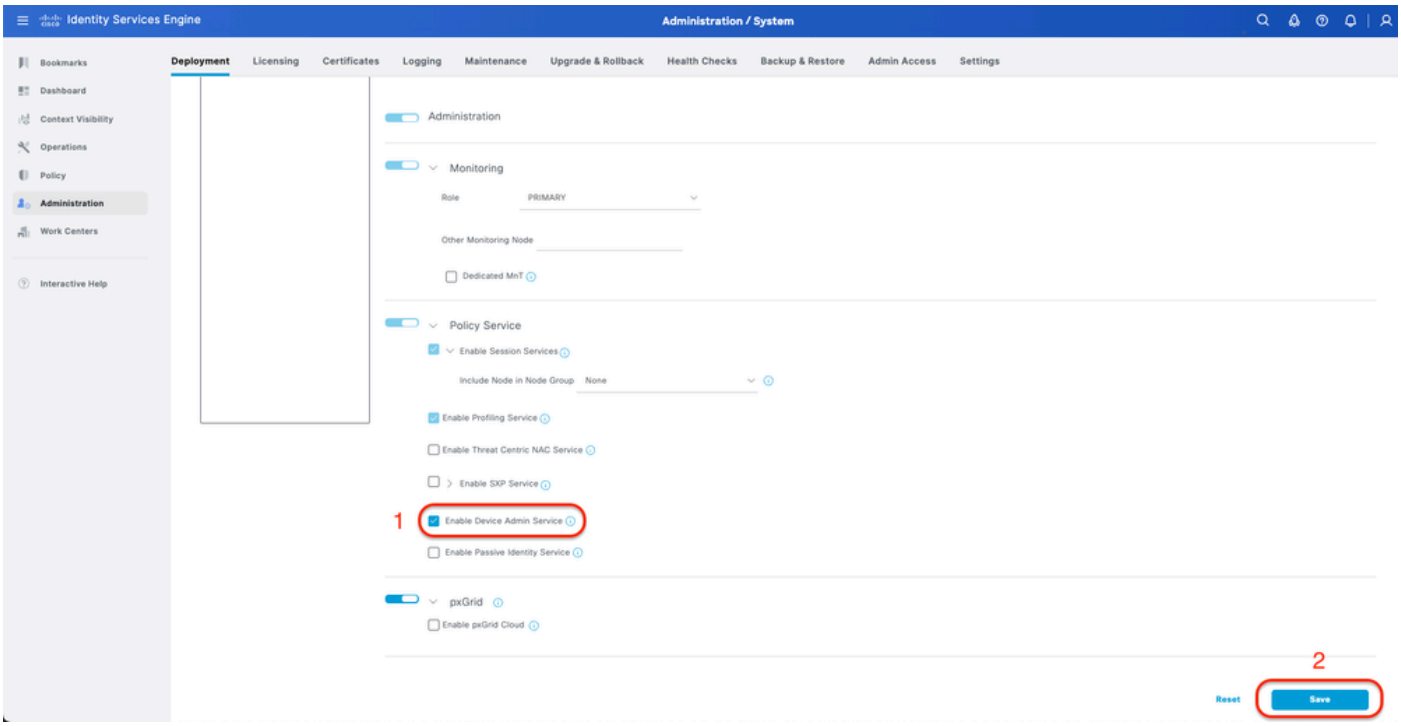
確保至少在主AAA伺服器上，或者在主伺服器和輔助伺服器上都啟用了TACACS+協定。



(TACACS+)外部身份驗證配置步驟

（選項2）為TACACS+配置ISE

步驟1.啟用Device Admin Service。
可從Administration > System > Deployment > Edit(ISE PSN Node)> Check Enable Device Admin Service頁籤完成此操作。



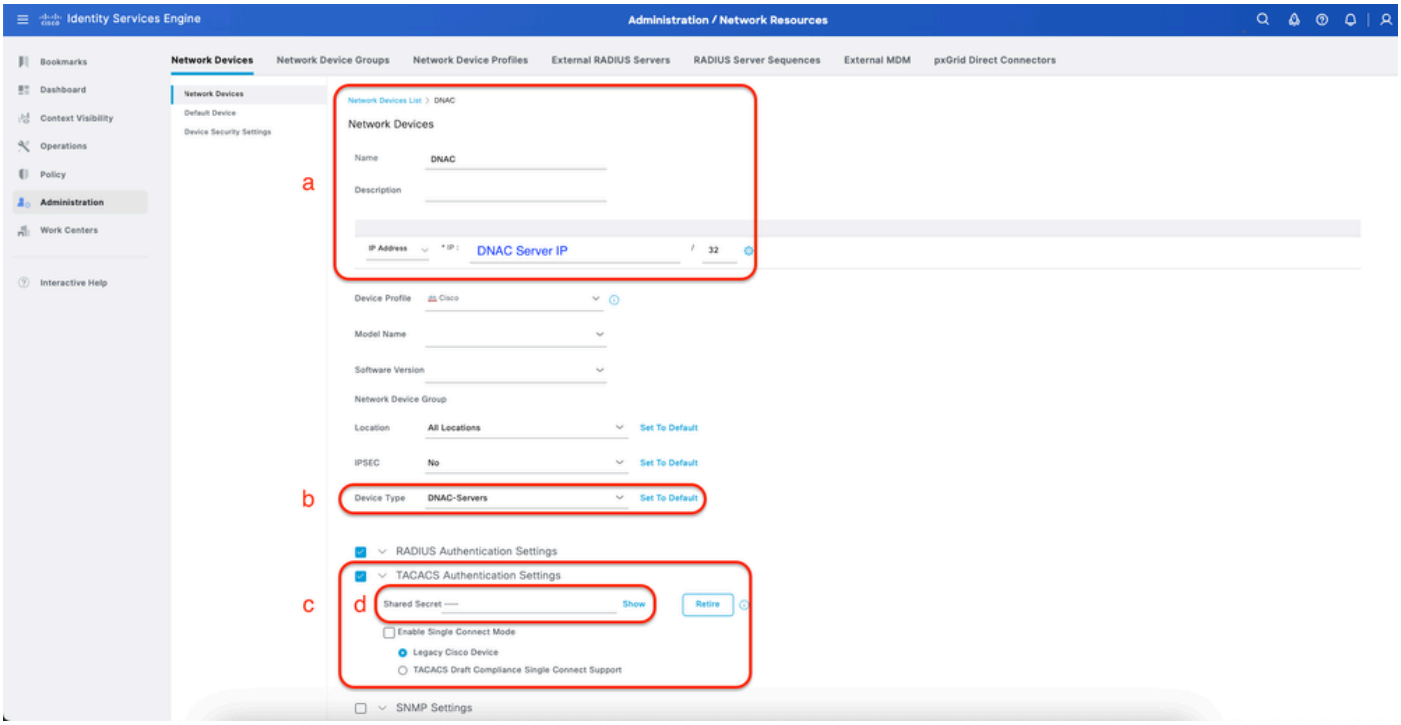
啟用裝置管理服務

步驟2.將DNAC伺服器新增為ISE上的網路裝置。

可從管理>網路資源>網路裝置索引標籤完成此操作。

程式

a.定義(DNAC)網路裝置名稱和IP。
b.（可選）為策略集條件對裝置型別進行分類。
c.啟用TACACS+身份驗證設定。
d.設定TACACS+共用金鑰。



適用於TACACS+的ISE網路裝置(DNAC)

步驟3.為每個DNAC角色建立TACACS+配置檔案。

可從工作中心>裝置管理>原則元素>結果> TACACS設定檔索引標籤完成此操作。

附註：建立3個TACACS+配置檔案，每個使用者角色一個。

程式

a.按一下「Add」，定義TACACS設定檔名稱。

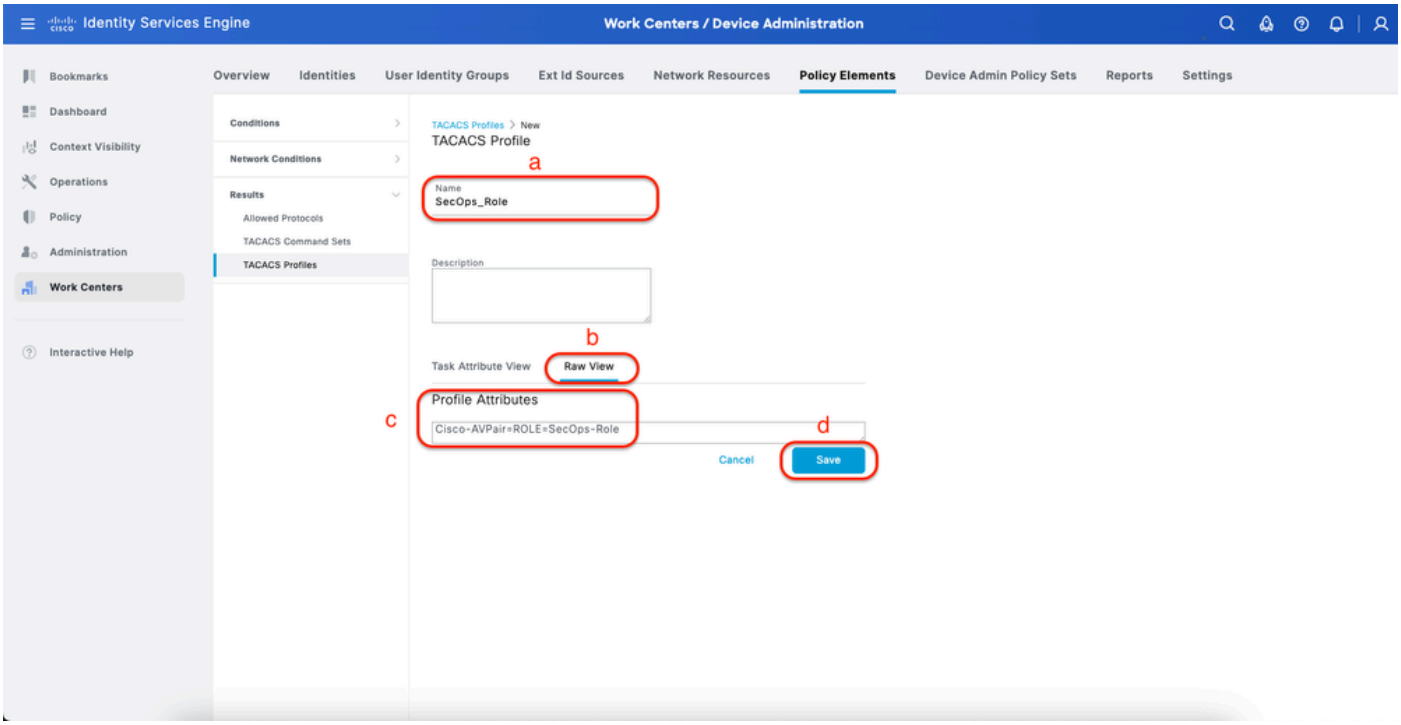
b.按一下Raw View選項卡。

c.輸入Cisco-AVPair=ROLE=並填寫正確的使用者角色。

- 對於(SecOps-Role)使用者角色，請輸入Cisco-AVPair=ROLE=SecOps-Role。
- 對於(NETWORK-ADMIN-ROLE)使用者角色，輸入Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE。
- 對於(SUPER-ADMIN-ROLE)使用者角色，輸入Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE。

附註：請記住，AVPair值(Cisco-AVPair=ROLE=)區分大小寫，並確保其與DNAC使用者角色匹配。

d.按一下「Save」。



建立TACACS配置檔案(SecOps_Role)

步驟4.建立使用者組。

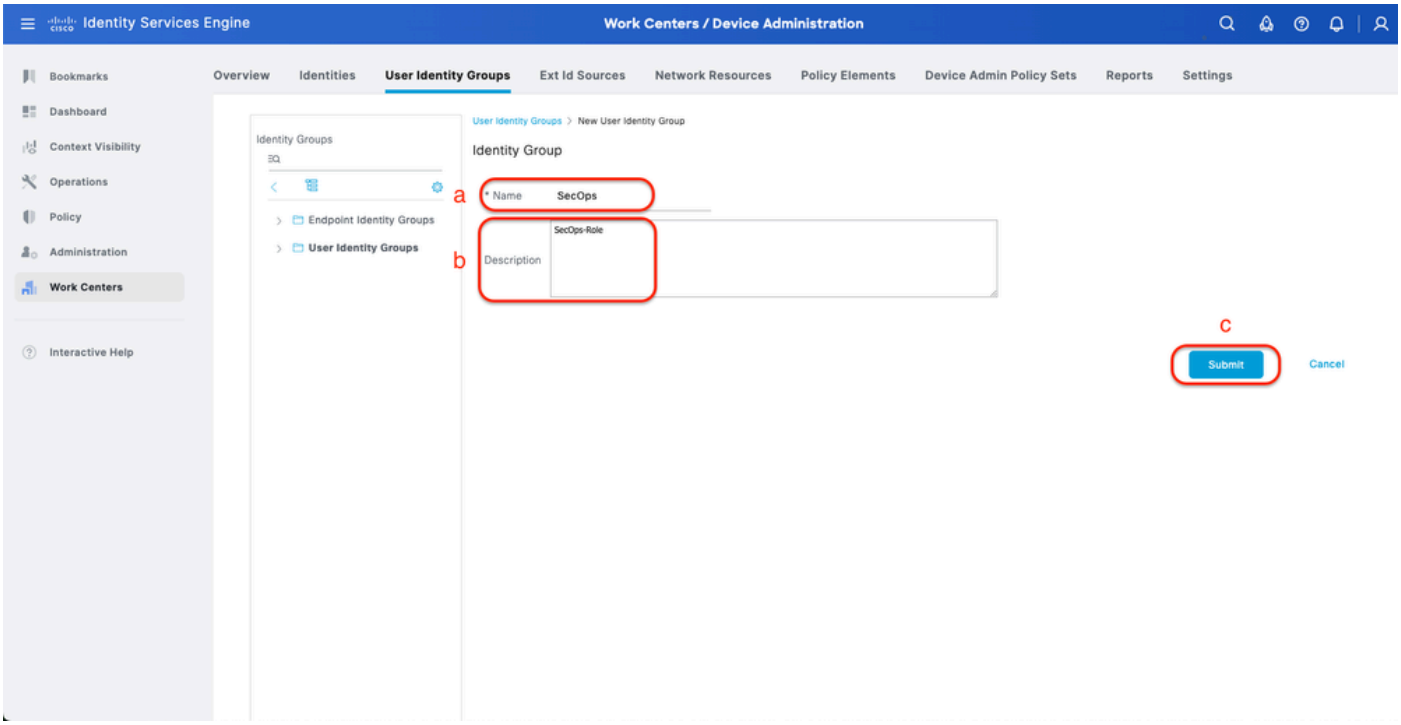
可從工作中心>裝置管理>使用者身份組頁籤完成此操作。

程式

a.按一下Add並定義身份組名稱。

b.（可選）定義說明。

c.按一下提交。



建立使用者身份組

步驟5.建立本地使用者。

可從工作中心(Work Centers)>裝置管理(Device Administration)>身份(Identities)>使用者(Users)頁籤執行此操作。

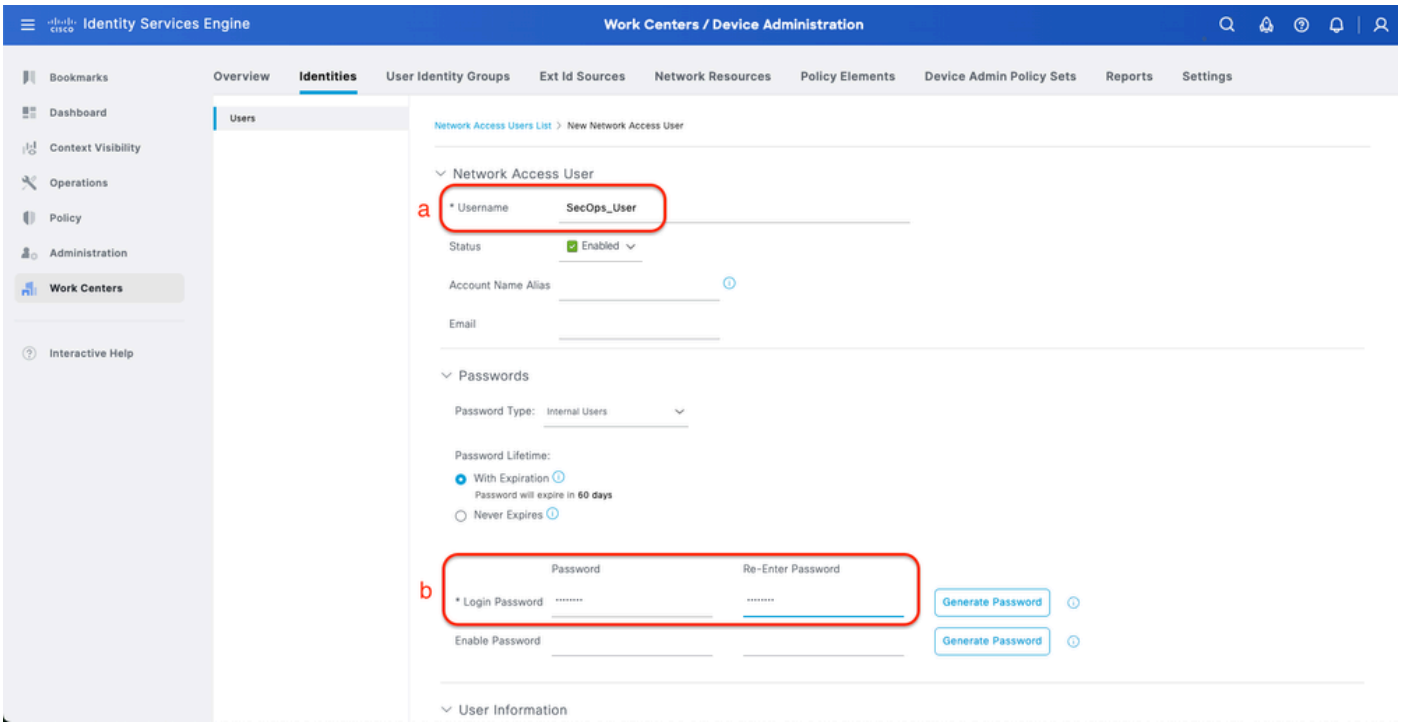
程式

a.按一下Add並定義使用者名稱。

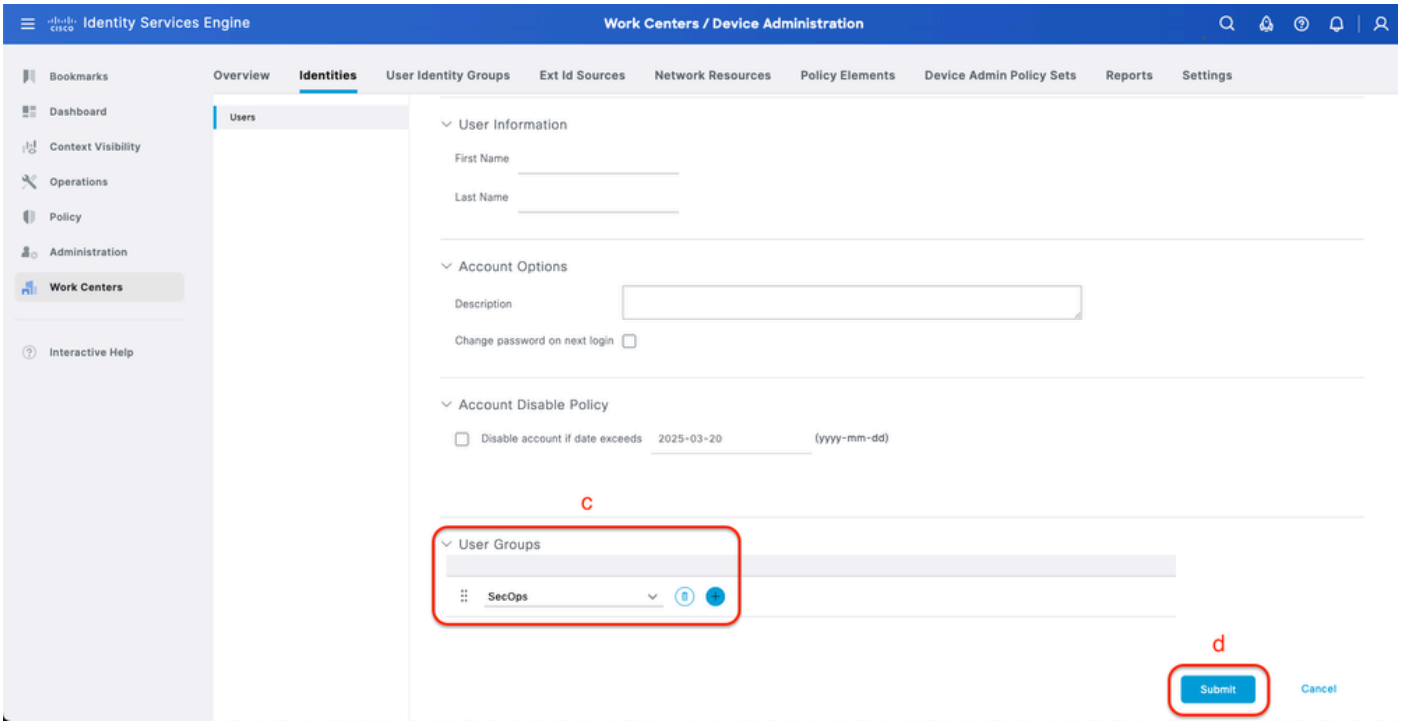
b.設定登入密碼。

c.將使用者新增到相關使用者組。

d.按一下「Submit」。



建立本地使用者1-2



建立本地使用者2-2

步驟6.（可選）新增TACACS+策略集。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

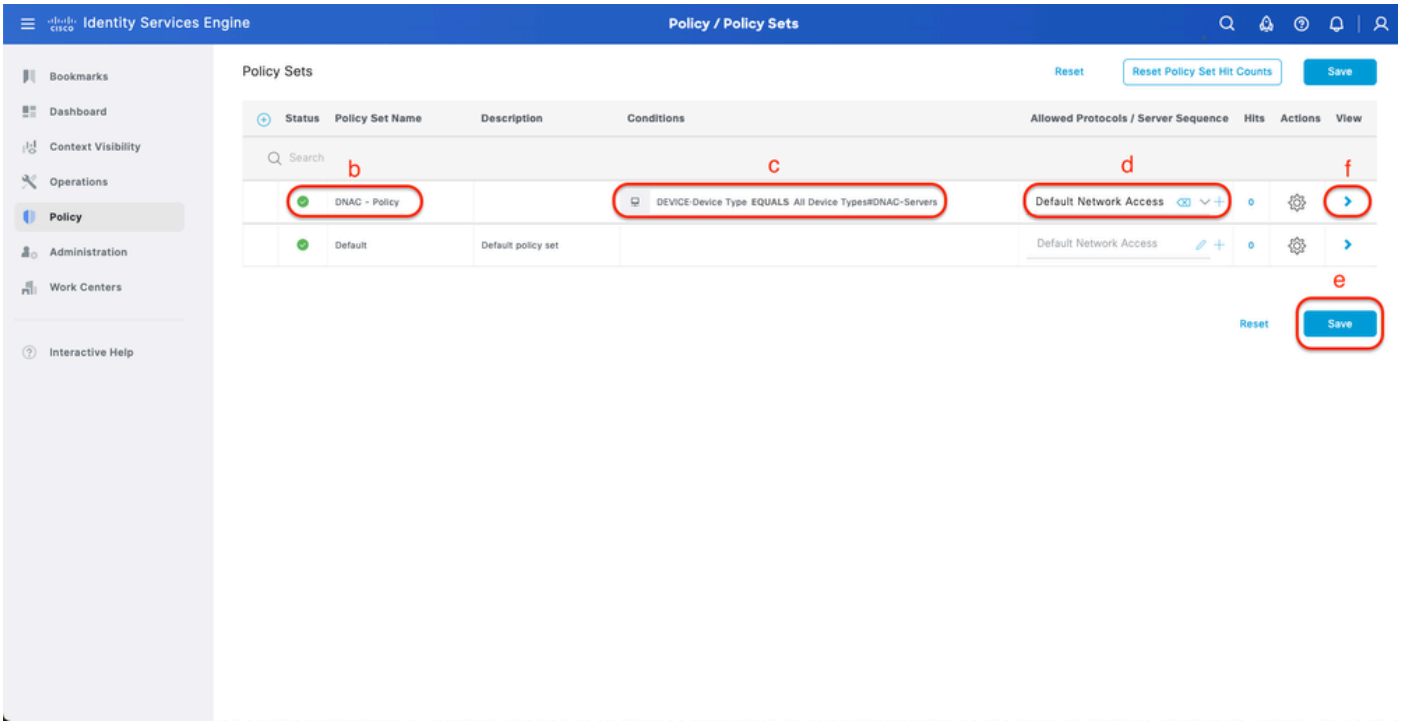
b.定義策略集名稱。

c.將Policy Set Condition設定為Select Device Type，您之前是在上建立的（步驟2 > b）。

d.設定Allowed協定。

e.按一下「Save」。

f.按一下(>)策略集檢視配置身份驗證和授權規則。



新增TACACS+策略集

步驟7.配置TACACS+身份驗證策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

程式

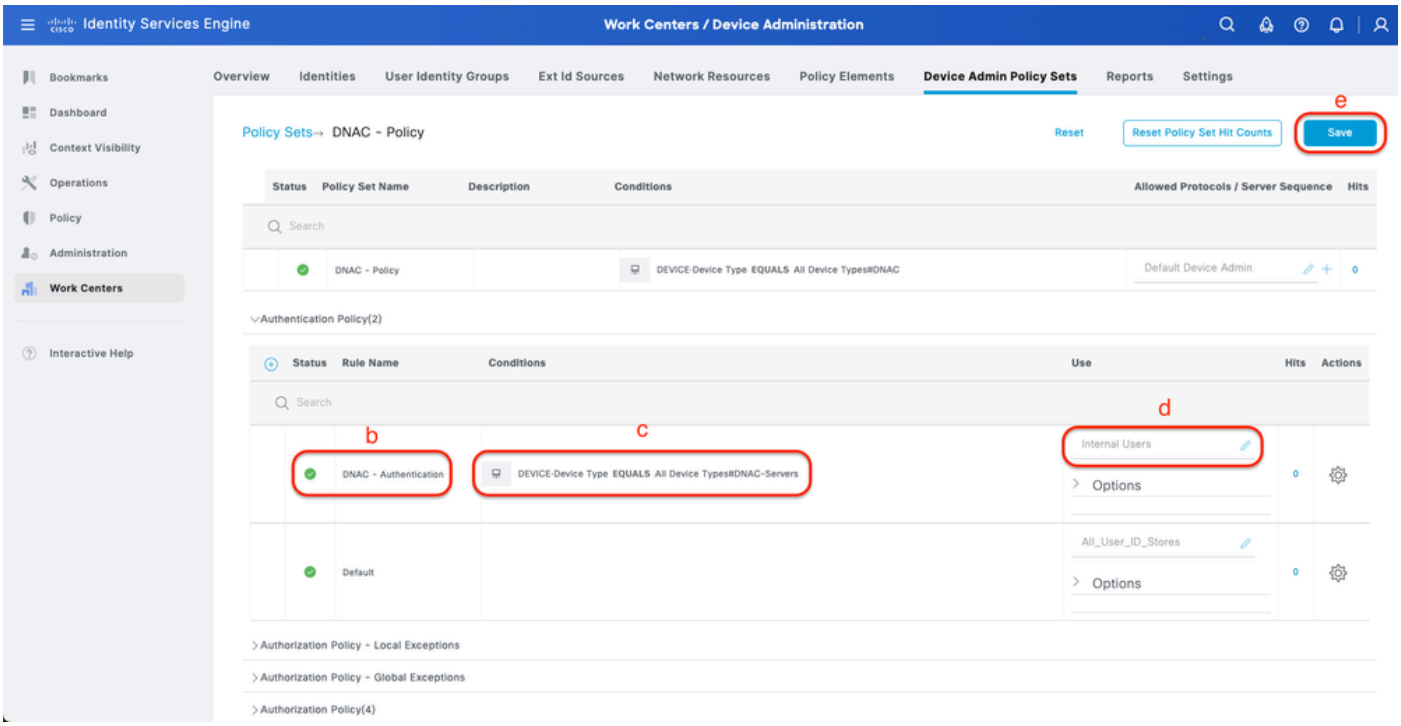
a.按一下Actions並選擇(在上面插入新行)。

b.定義身份驗證策略名稱。

c.設定身份驗證策略條件並選擇先前在上建立的裝置型別（步驟2 > b）。

d.設定Authentication Policy Use for Identity源。

e.按一下「Save」。



新增TACACS+身份驗證策略

步驟8.配置TACACS+授權策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

此步驟用於為每個用戶角色建立授權策略：

- 超級管理員角色
- NETWORK-ADMIN-ROLE
- SecOps角色

程式

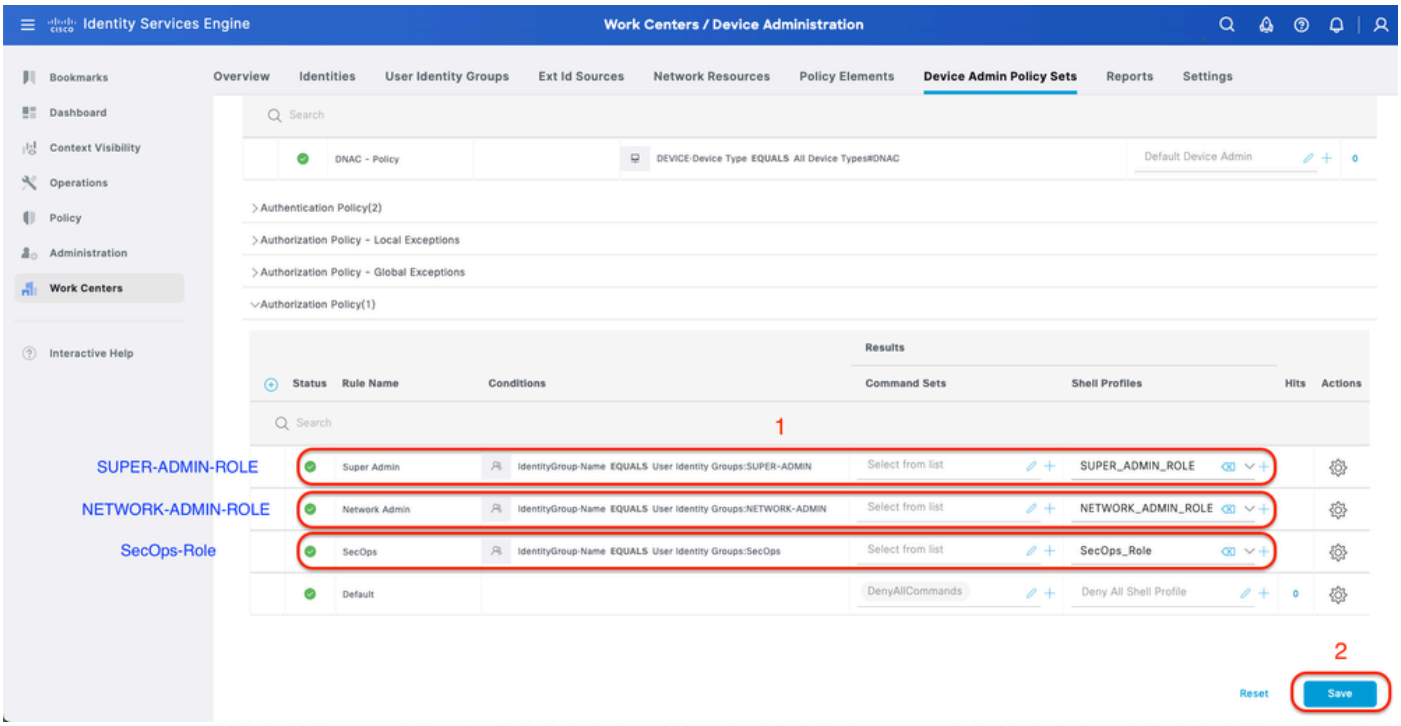
a.按一下Actions並選擇(在上面插入新行)。

b.定義授權策略名稱。

c.設定授權策略條件並選擇在中建立的使用者組（步驟4）。

d.設定授權策略Shell Profiles並選擇您在中建立的TACACS配置檔案（步驟3）。

e.按一下「Save」。

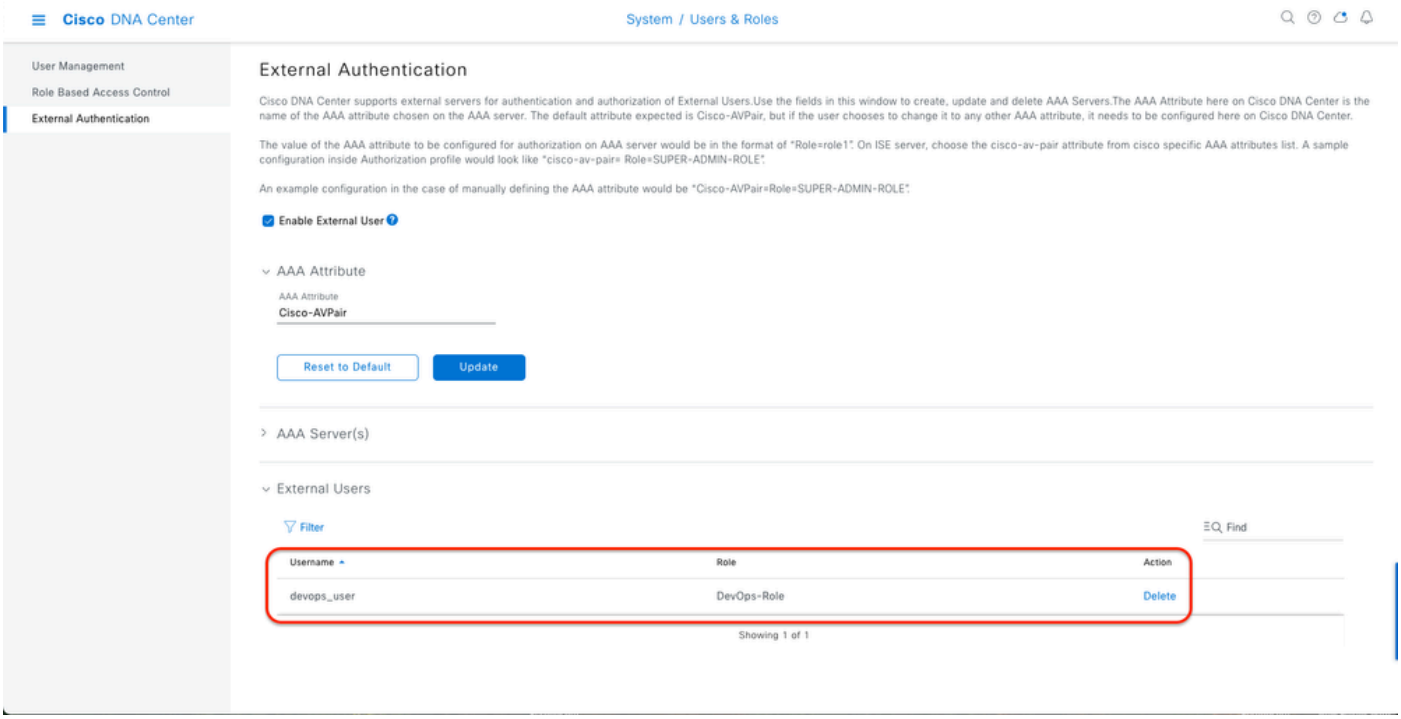


新增授權策略

驗證

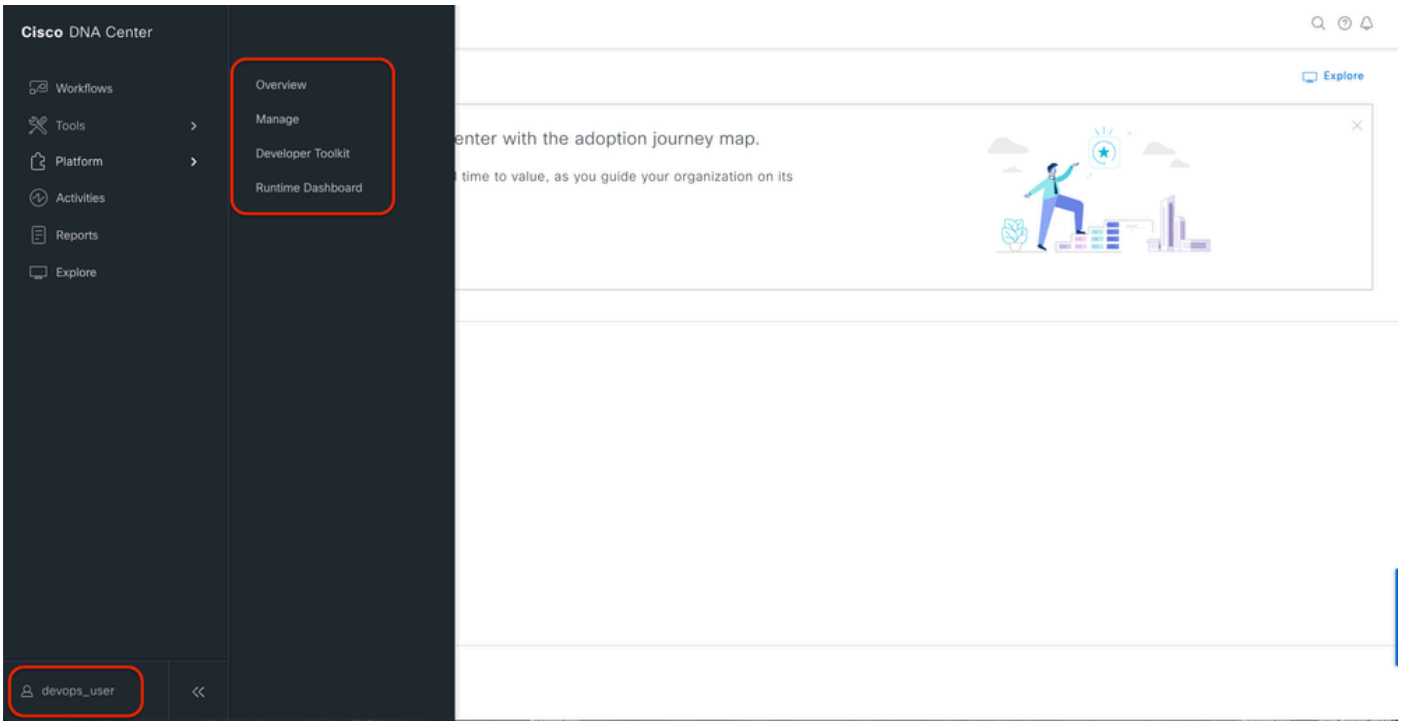
驗證RADIUS設定

1- DNAC — 顯示外部使用者系統>使用者和角色>外部身份驗證>外部使用者。
您可以檢視首次透過RADIUS登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色。



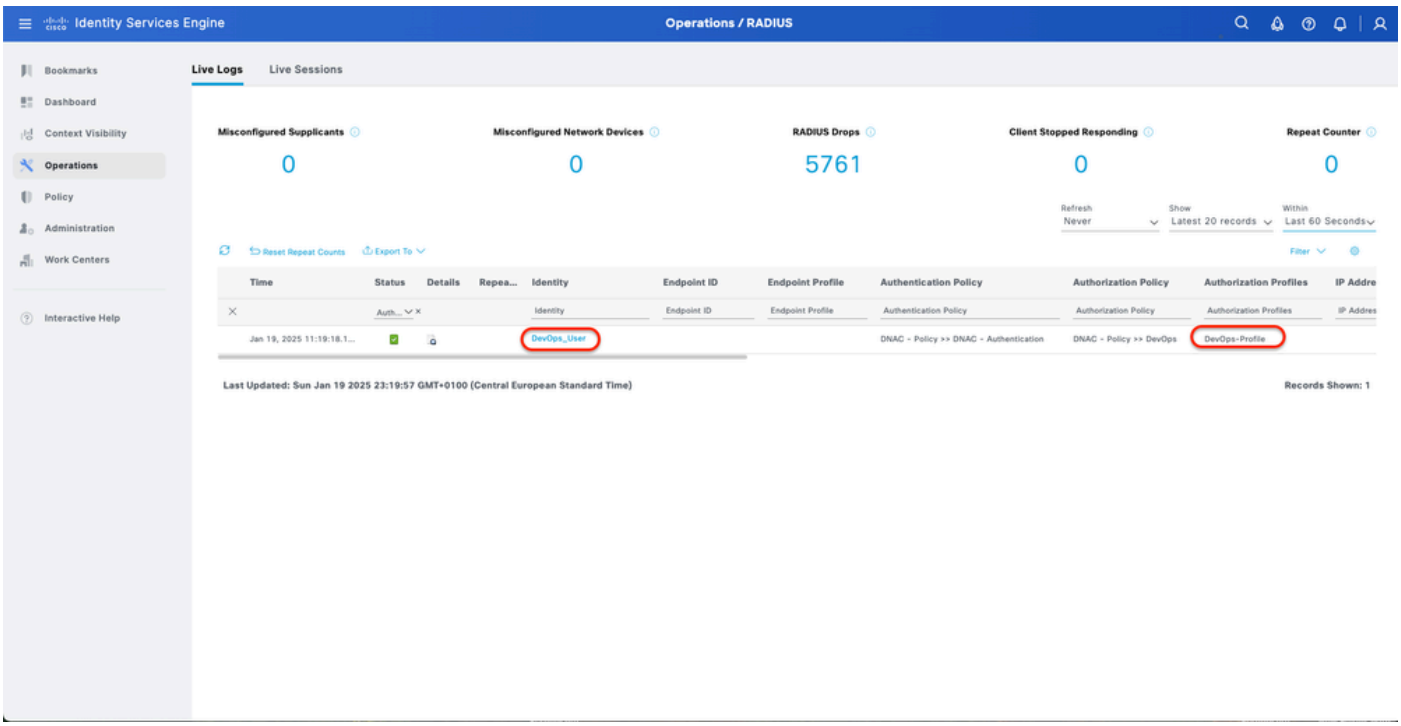
外部使用者

2. DNAC — 確認使用者訪問許可權。



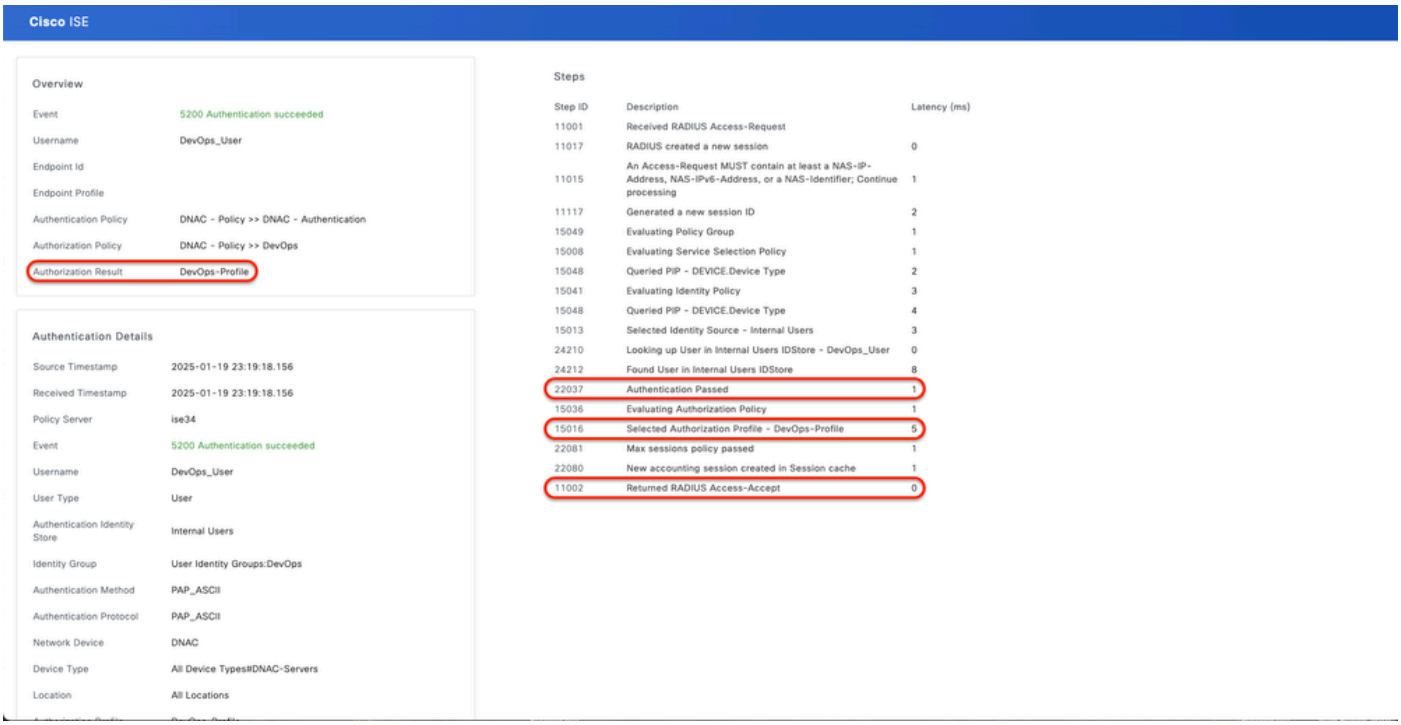
有限的使用者訪問

3.a ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs。

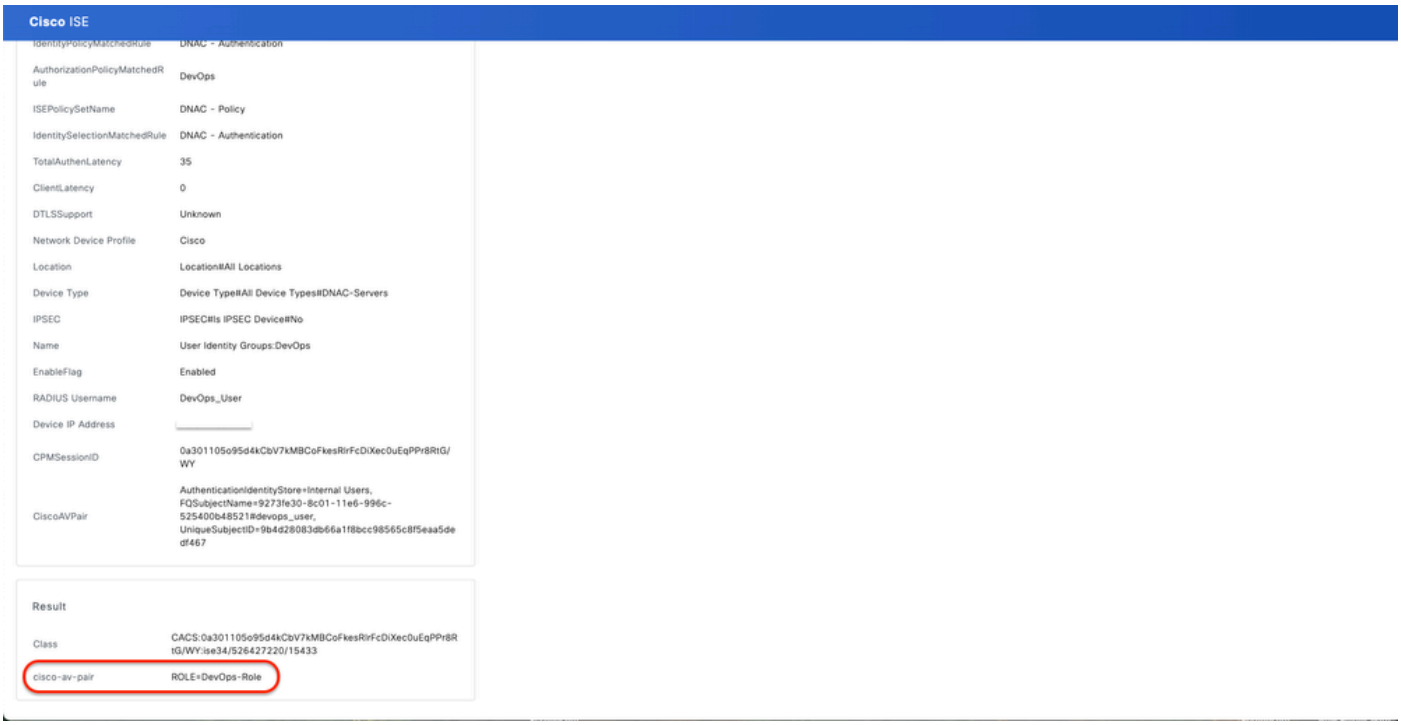


RADIUS即時日誌

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click(Details)for Authorization log。



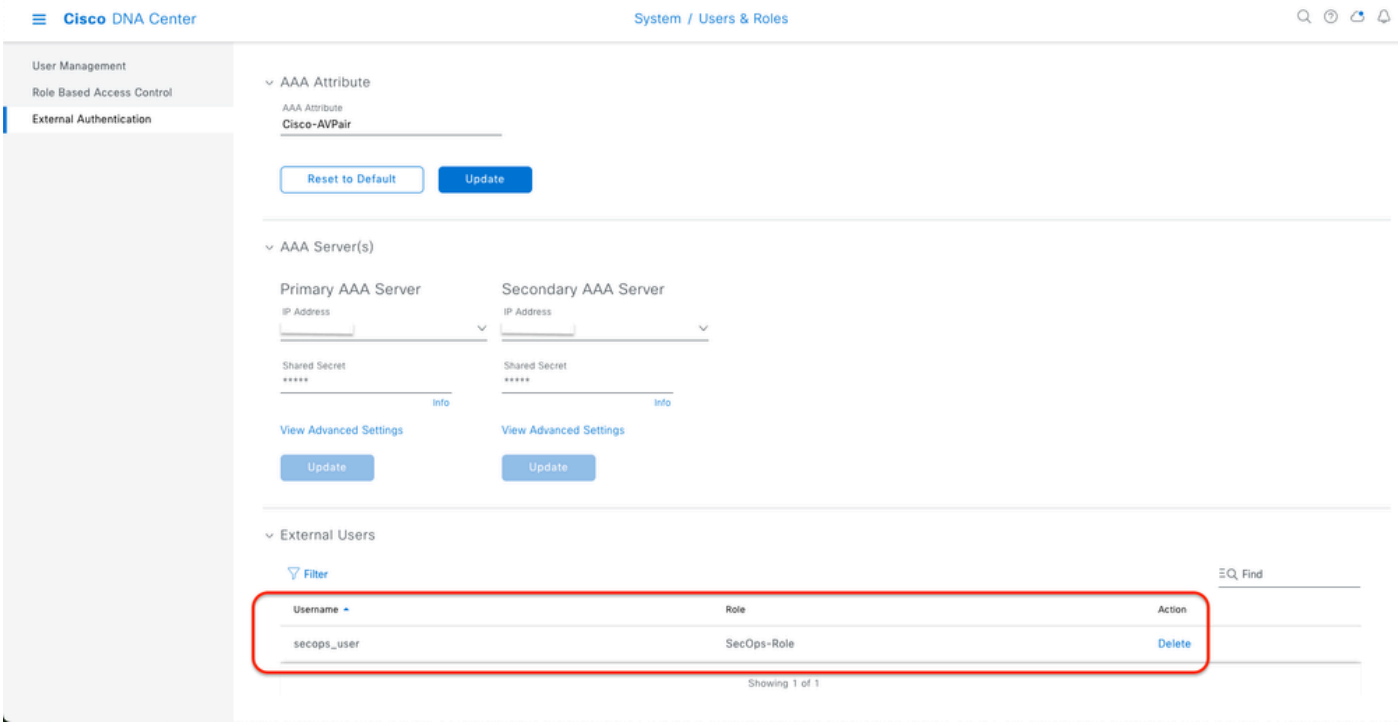
RADIUS詳細即時日誌1-2



RADIUS詳細即時日誌2-2

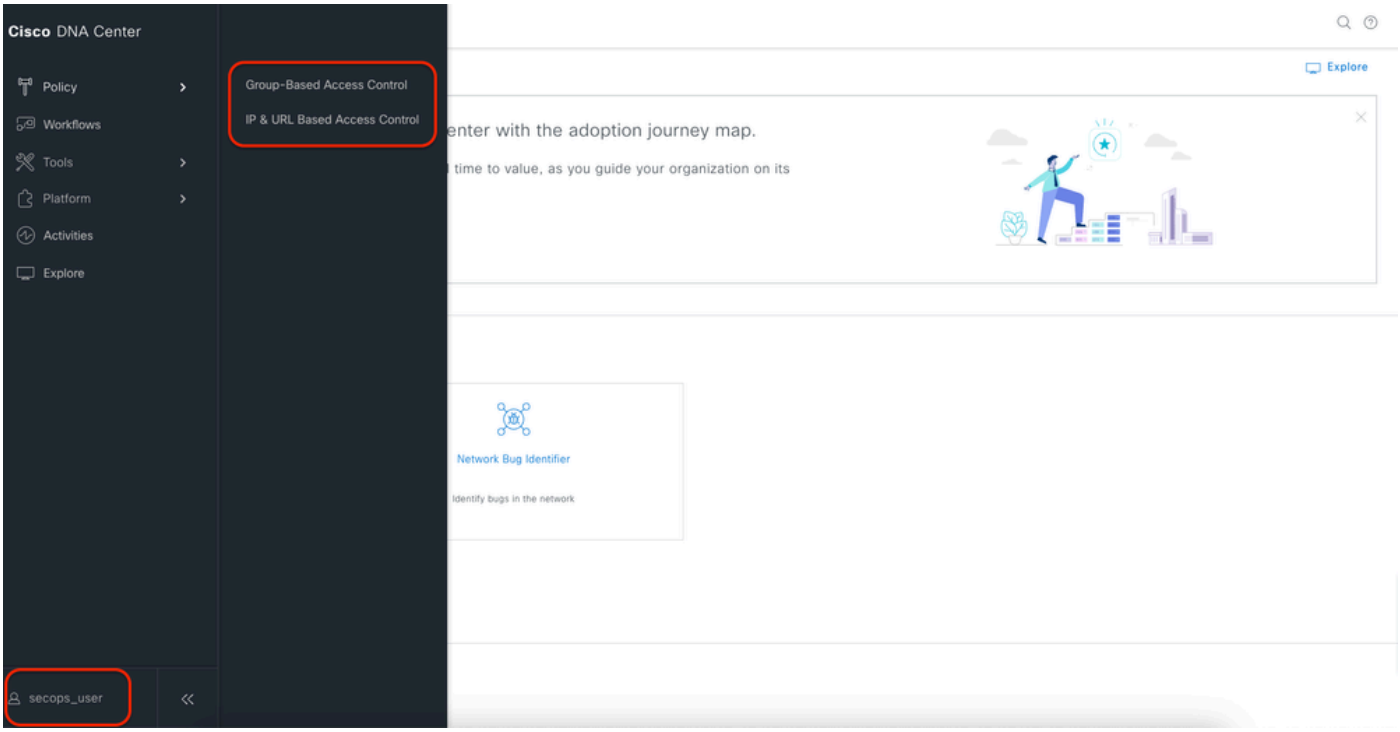
驗證TACACS+配置

1- DNAC — 顯示外部使用者系統>使用者和角色>外部身份驗證>外部使用者。
您可以檢視首次通過TACACS+登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色。



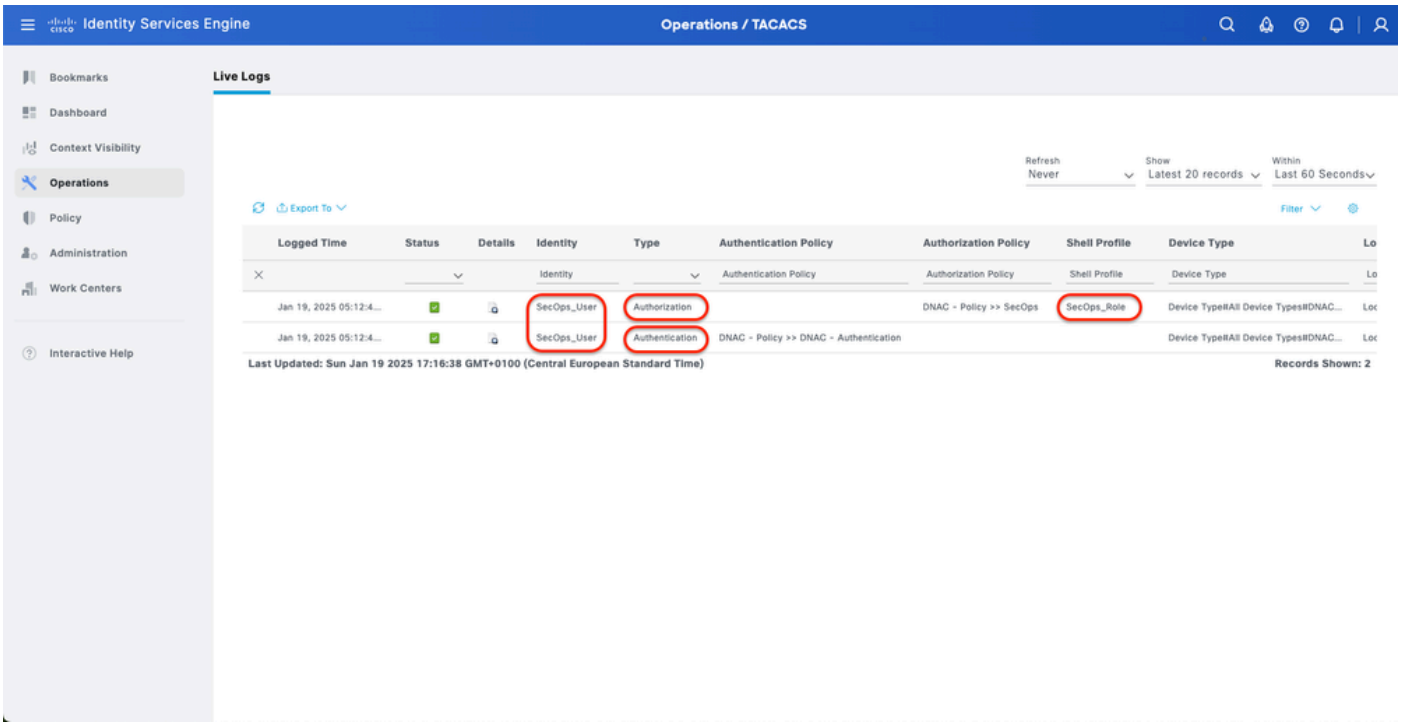
外部使用者

2. DNAC — 確認使用者訪問許可權。



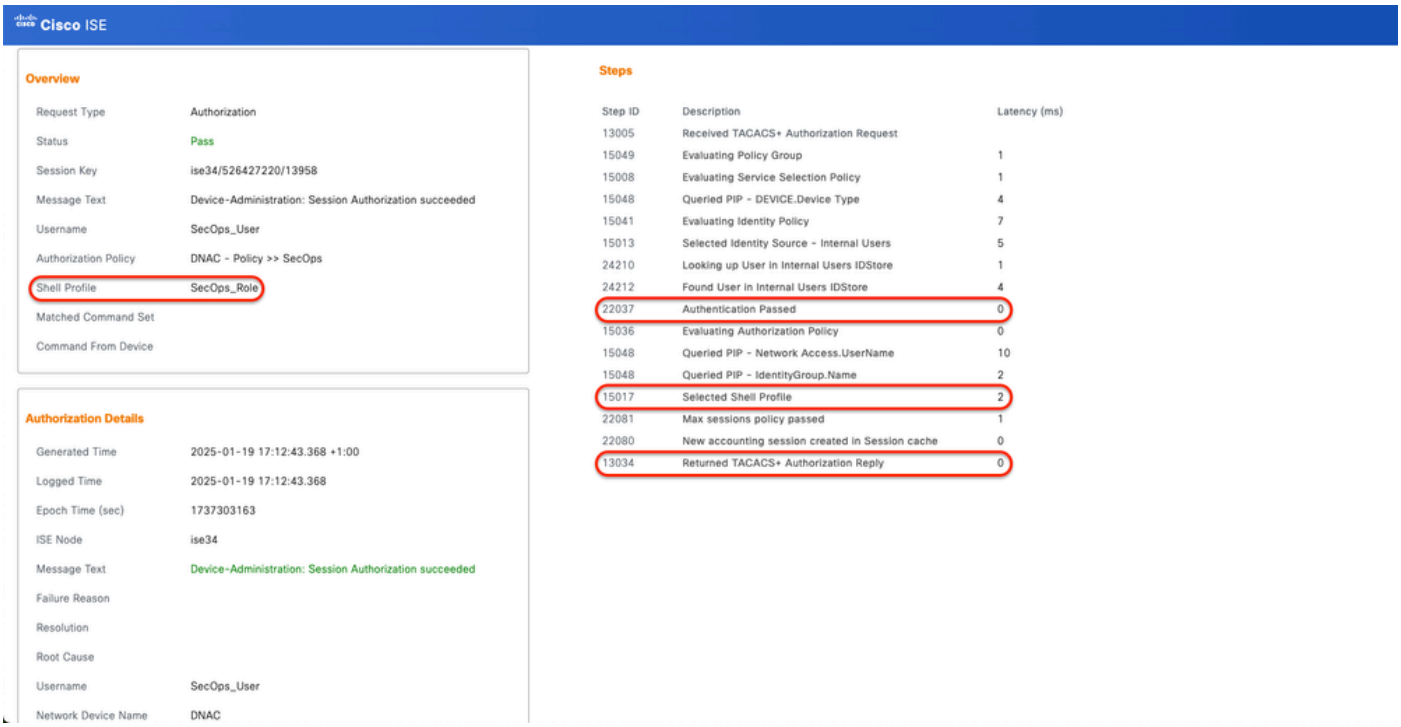
有限的使用者訪問

3.a ISE - TACACS+即時日誌工作中心>裝置管理>概述> TACACS即時日誌。

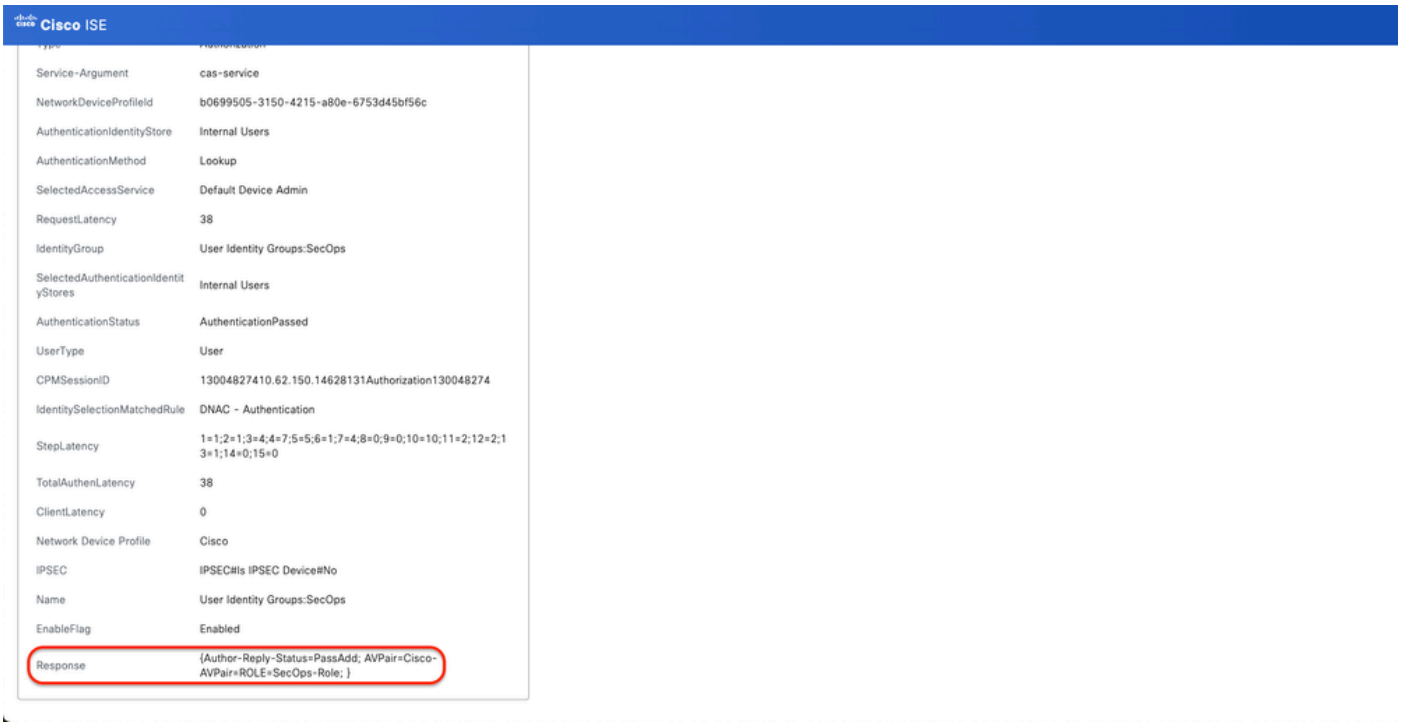


TACACS即時日誌

3.b ISE — 詳細的TACACS+即時日誌工作中心(Work Centers)>裝置管理(Device Administration)>概述(Overview)> TACACS即時日誌(TACACS Livelog)>按一下（詳細資訊）獲取授權日誌。



TACACS+詳細即時日誌1-2



TACACS+詳細即時日誌2-2

疑難排解

目前尚無適用於此組態的具體診斷資訊。

參考資料

- Cisco Identity Services Engine管理員指南，版本3.4 >裝置管理
- Cisco DNA Center管理員指南2.3.5版

- Cisco DNA Center：具有外部驗證的基於角色的存取控制

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）。