

# 將ISE配置為DNAC GUI的外部身份驗證

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

#### [開始之前](#)

### [設定](#)

#### [\(選項1\) 使用RADIUS配置DNAC外部身份驗證](#)

#### [\(選項1\) 為RADIUS配置ISE](#)

#### [\(選項2\) 使用TACACS+配置DNAC外部身份驗證](#)

#### [\(選項2\) 為TACACS+配置ISE](#)

### [驗證](#)

#### [驗證RADIUS設定](#)

#### [驗證TACACS+配置](#)

### [疑難排解](#)

### [參考資料](#)

---

## 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

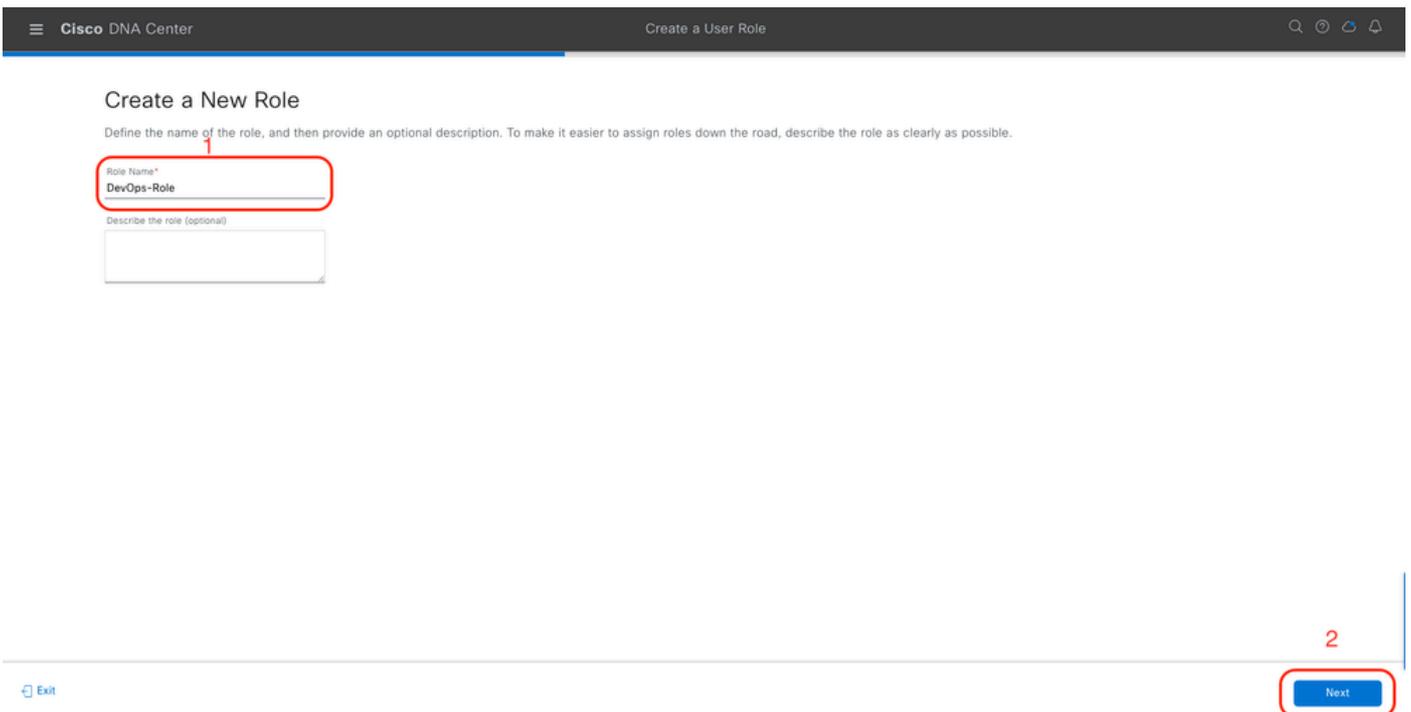
### ( 選項1 ) 使用RADIUS配置DNAC外部身份驗證

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。



Cisco DNA Center Create a User Role

### Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name\*  
DevOps-Role

Describe the role (optional)

Exit Next 2

## DevOps角色名稱

### b. 定義訪問。

Define the Access

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

Exit Review Back **Next**

## DevOps角色訪問

### c. 建立新角色。

Summary

Review the **DevOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section

Role Name & Description [Edit](#)

Role Name DevOps-Role

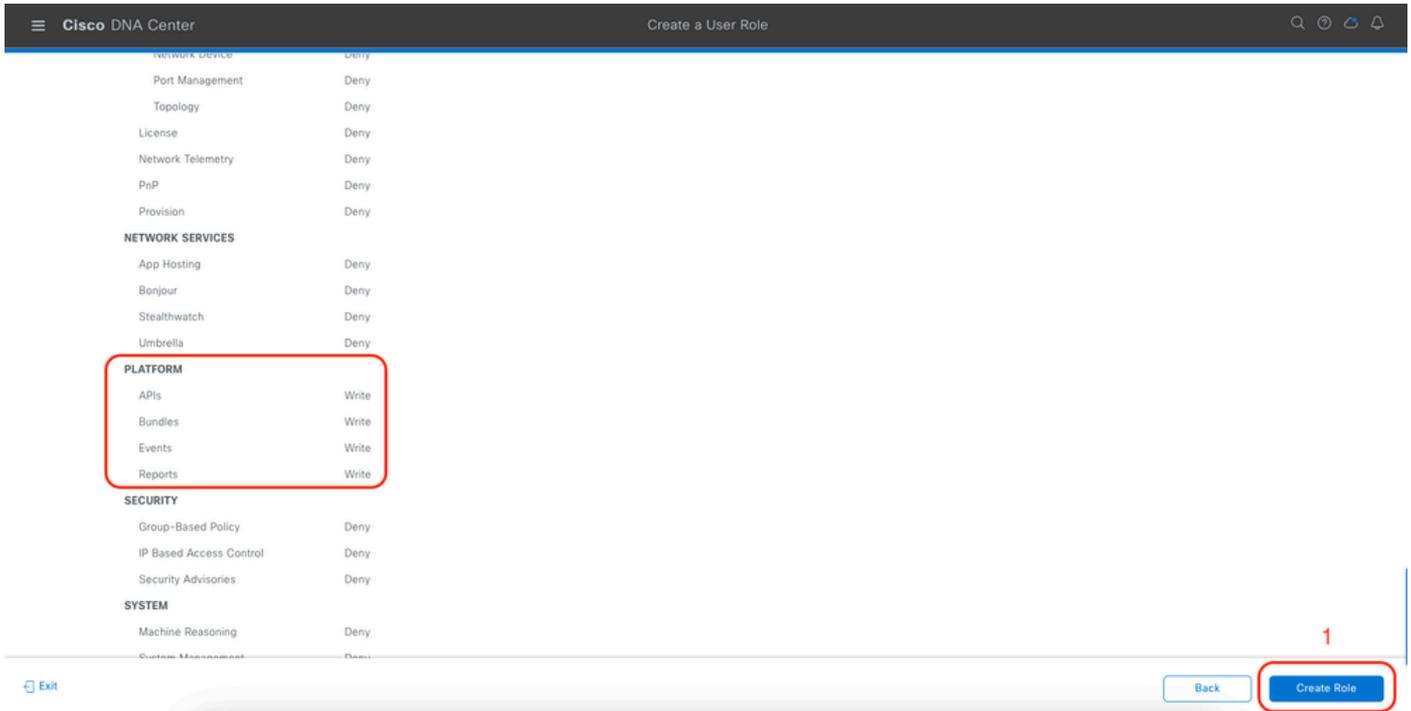
Role Description

Role Capability [Edit](#)

Capability	Permission
<b>ASSURANCE</b>	
Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny
<b>NETWORK ANALYTICS</b>	
Data Access	Read
<b>NETWORK DESIGN</b>	
Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

Exit Back **Create Role**

## 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。

User Management  
Role Based Access Control  
External Authentication

### External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

**a**  Enable External User ?

**b** AAA Attribute  
Cisco-AVPair

Reset to Default Update

**c** AAA Server(s)

Primary AAA Server	Secondary AAA Server
IP Address ISE Server 1 IP	IP Address ISE Server 2 IP
Shared Secret *****	Shared Secret *****
Hide Advanced Settings <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS	Hide Advanced Settings <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS
Authentication Port 1812	Authentication Port 1812

(RADIUS)外部身份驗證配置步驟

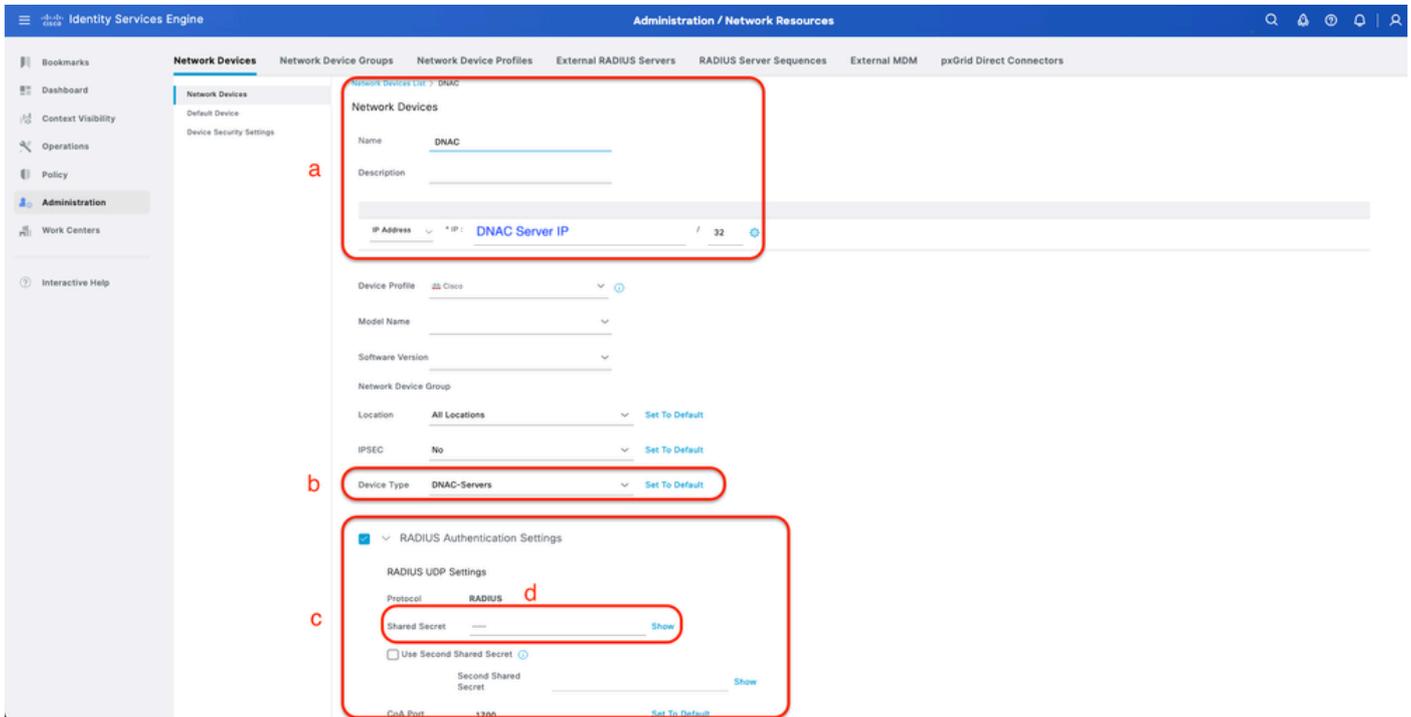
## ( 選項1 ) 為RADIUS配置ISE

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

- 定義(DNAC)網路裝置名稱和IP。
- ( 可選 ) 為策略集條件對裝置型別進行分類。
- 啟用RADIUS身份驗證設定。
- 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

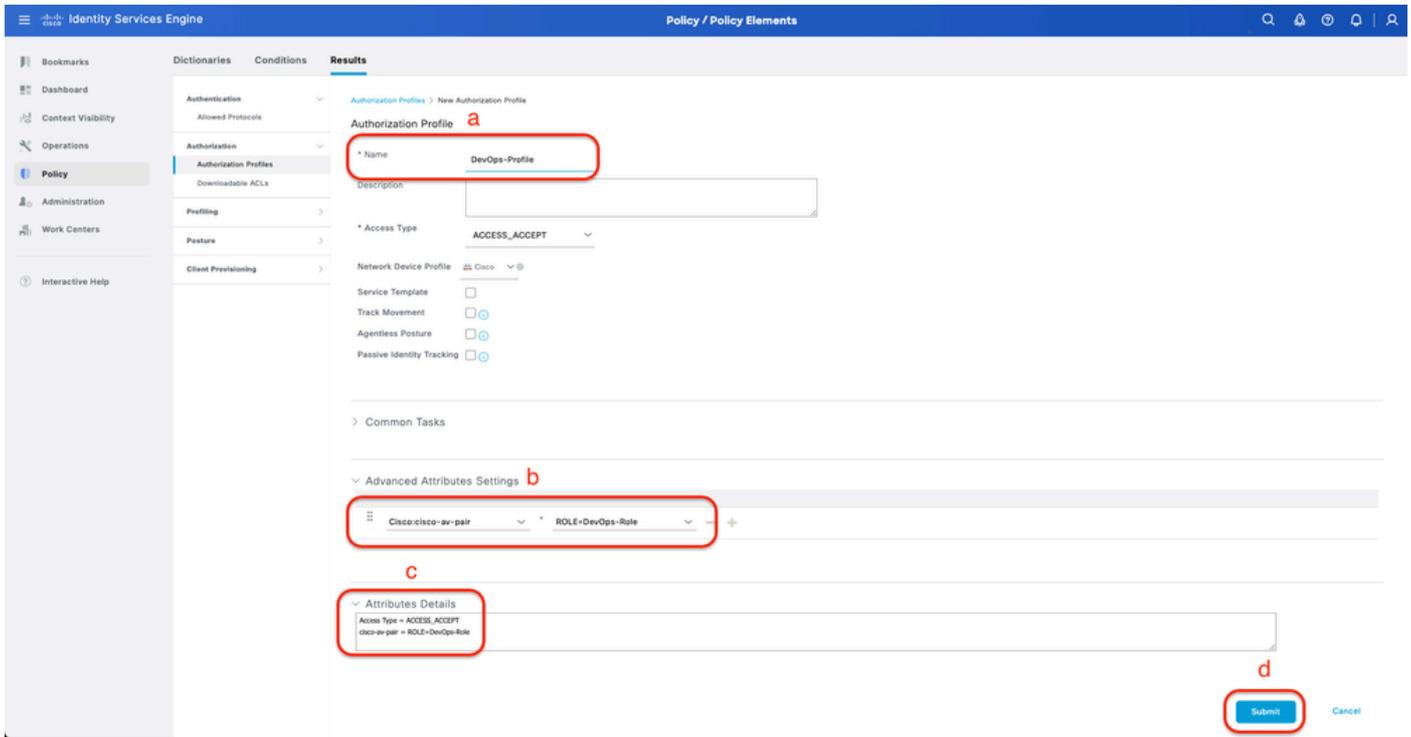
a. 單擊Add並定義RADIUS授權配置檔名稱。

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。

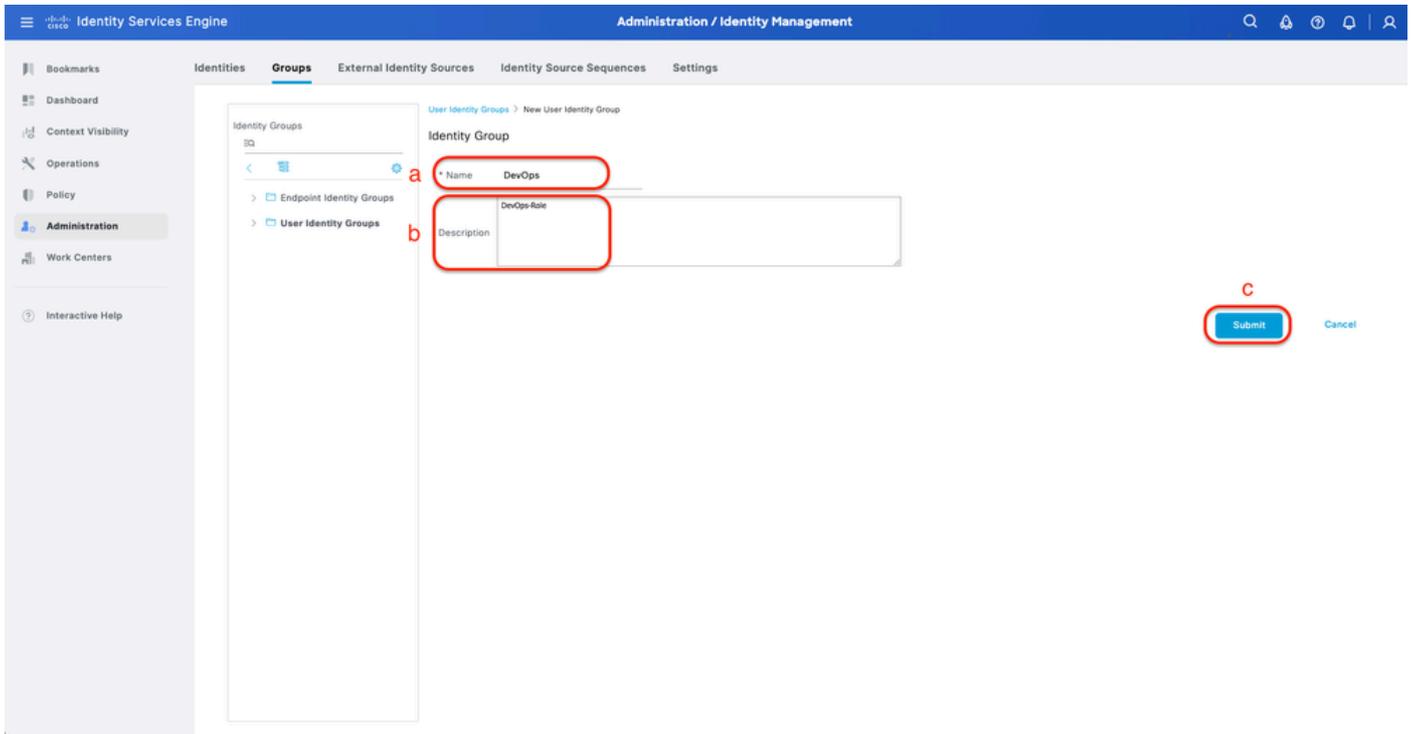
可從管理>身份管理>組>使用者身份組頁籤完成此操作。

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。



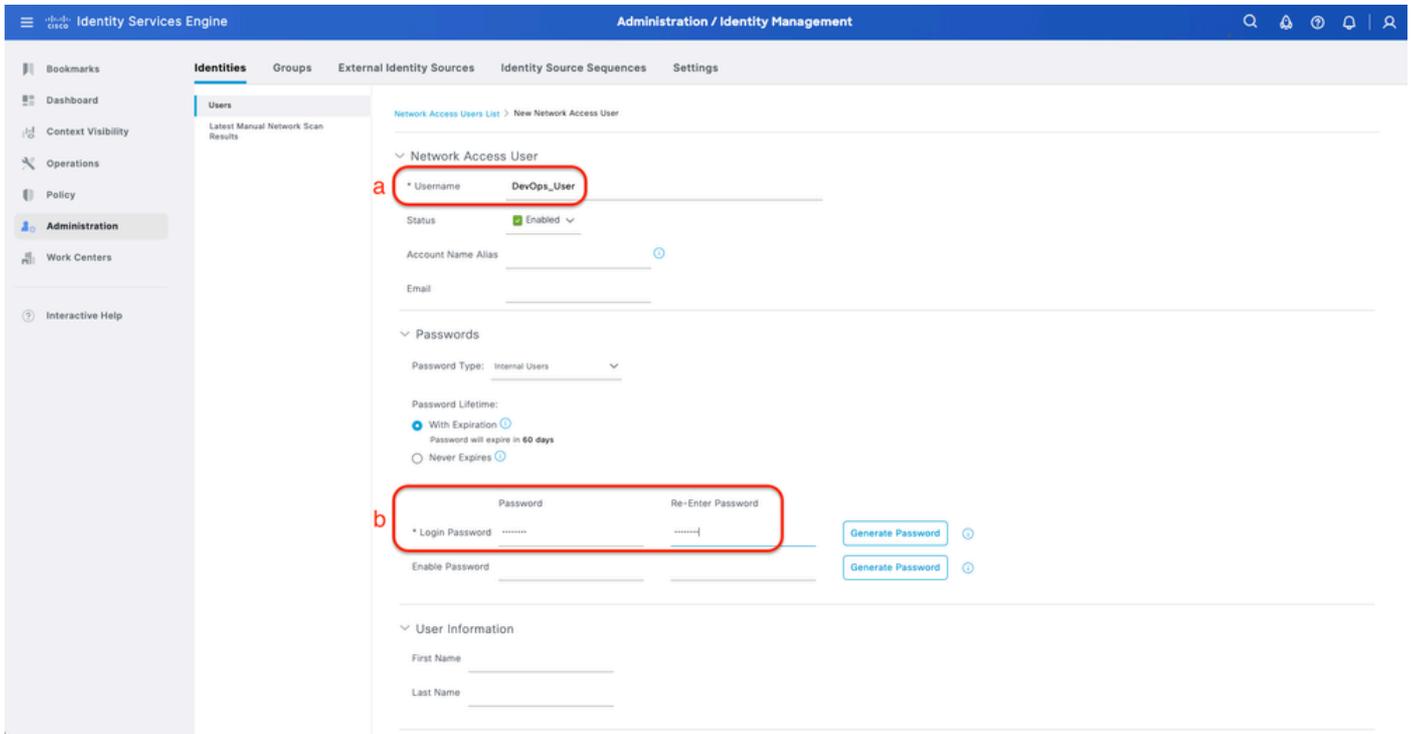
建立使用者身份組

步驟4. 建立本地使用者。

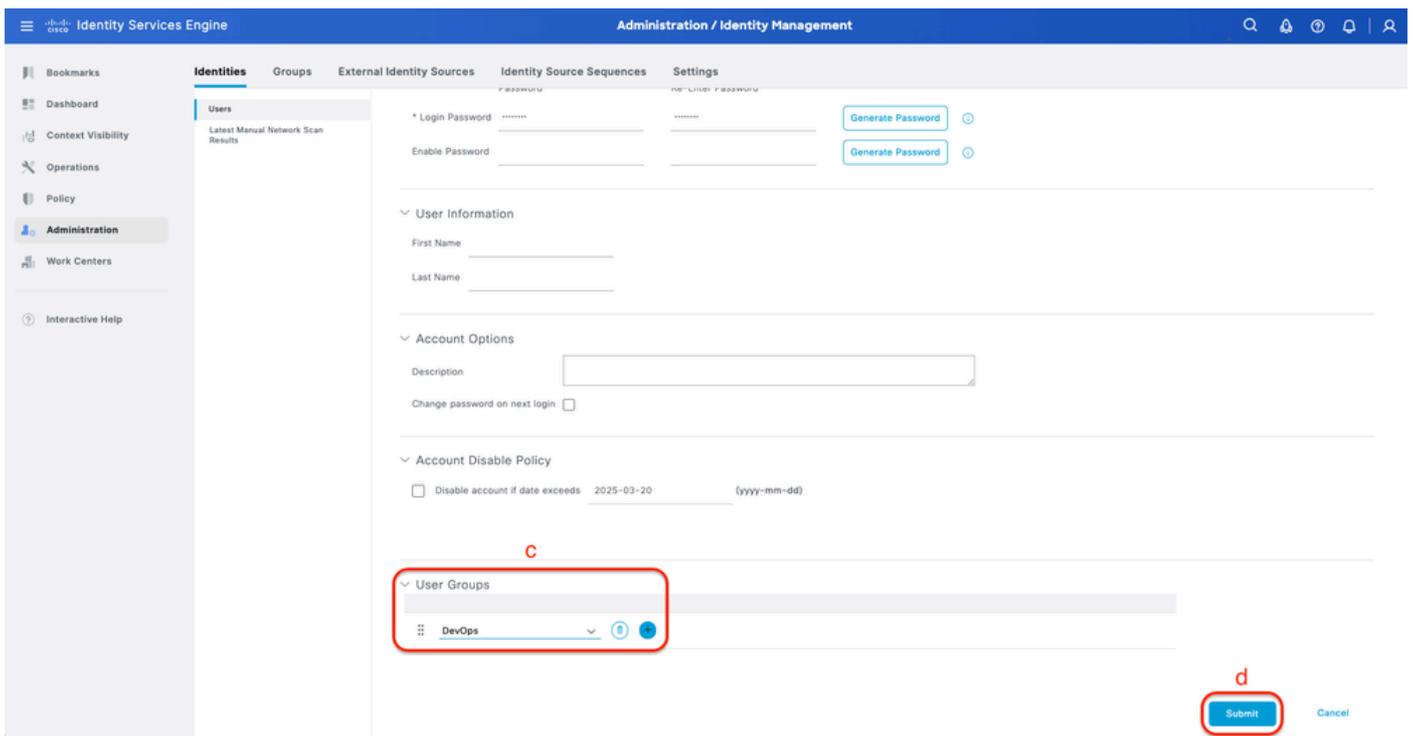
可從Administration > Identity Management > Identities > Users頁籤執行此操作。

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)。

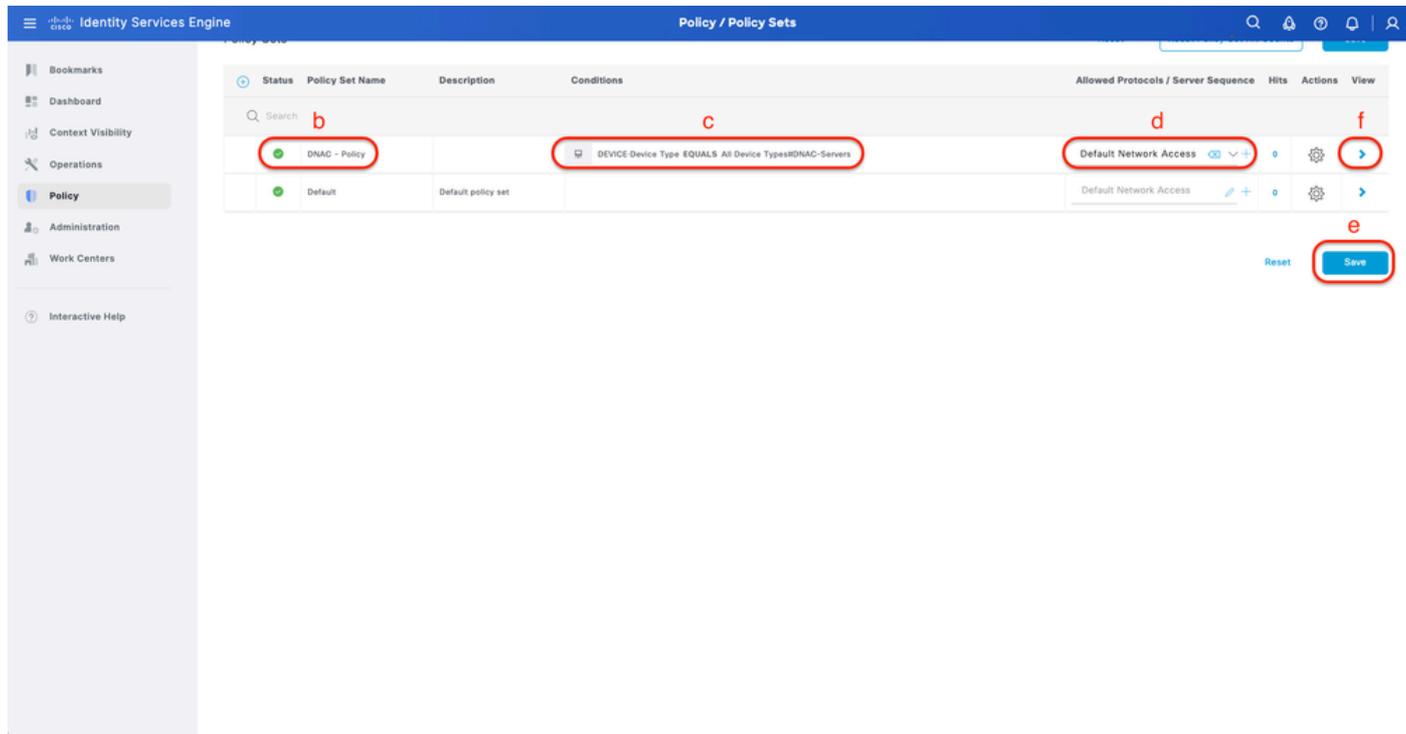
b.定義策略集名稱。

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

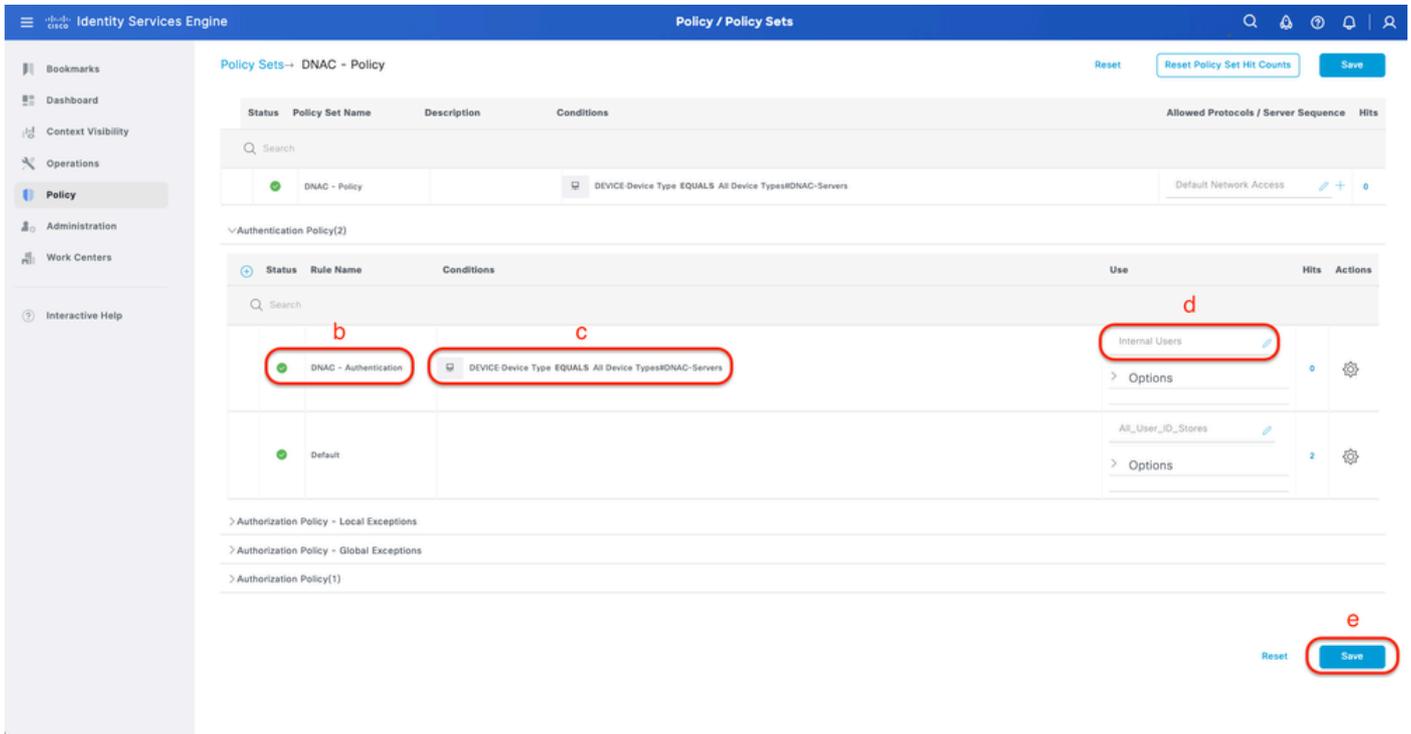
a.按一下Actions並選擇(在上面插入新行)。

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」。

Policy Sets -> DNAC - Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	DNAC - Policy		DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0

> Authentication Policy(2)  
> Authorization Policy - Local Exceptions  
> Authorization Policy - Global Exceptions  
▼ Authorization Policy(4)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr...	Select from list	0	⚙️
●	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role_...	Select from list	0	⚙️
●	DevOps	IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile	Select from list	0	⚙️
●	Default		DenyAccess	Select from list	0	⚙️

Reset 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。

Cisco DNA Center Create a User Role

### Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name\*  
SecOps-Role

Describe the role (optional)

2

Exit Next

## SecOps角色名稱

### b. 定義訪問。

The screenshot shows the 'Define the Access' step in the Cisco DNA Center 'Create a User Role' wizard. A red box labeled '1' highlights the list of capabilities and their permissions. A red box labeled '2' highlights the 'Next' button at the bottom right.

Capability	Deny	Read	Write	Description
Network Analytics	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Access to Network Analytics related components.
Network Design	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
Network Provision	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Configure, upgrade, provision and manage your network devices.
Network Services	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Configure additional capabilities on the network beyond basic network connectivity and access.
Platform	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
Security	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Manage and control secure access to the network.
System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
Utilities	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.

## SecOps角色訪問

### c. 建立新角色。

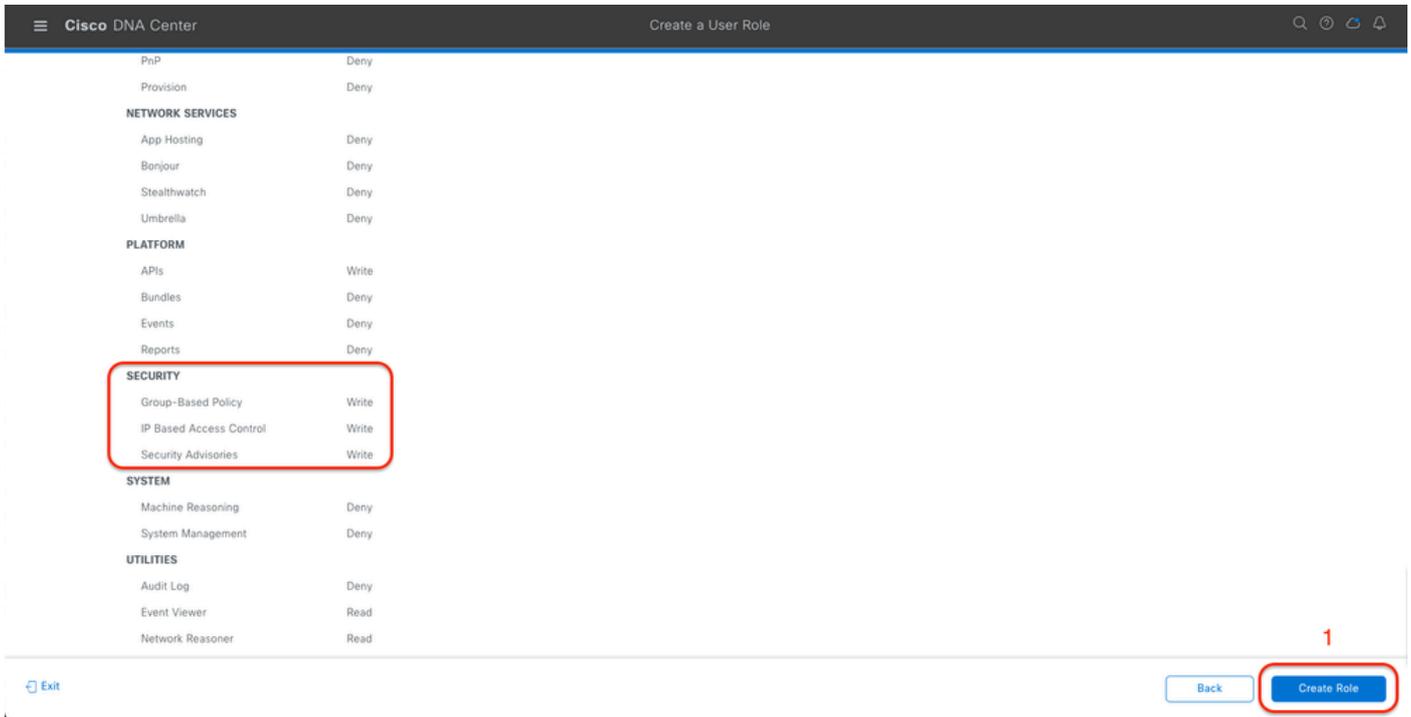
The screenshot shows the 'Summary' step in the Cisco DNA Center 'Create a User Role' wizard. A red box highlights the 'Summary' header. The page displays the role name 'SecOps-Role' and a detailed list of role capabilities and their permissions.

Role Name	Role Description
SecOps-Role	

Capability	Permission
<strong>ASSURANCE</strong>	
Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny
<strong>NETWORK ANALYTICS</strong>	
Data Access	Write
<strong>NETWORK DESIGN</strong>	
Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

## 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。

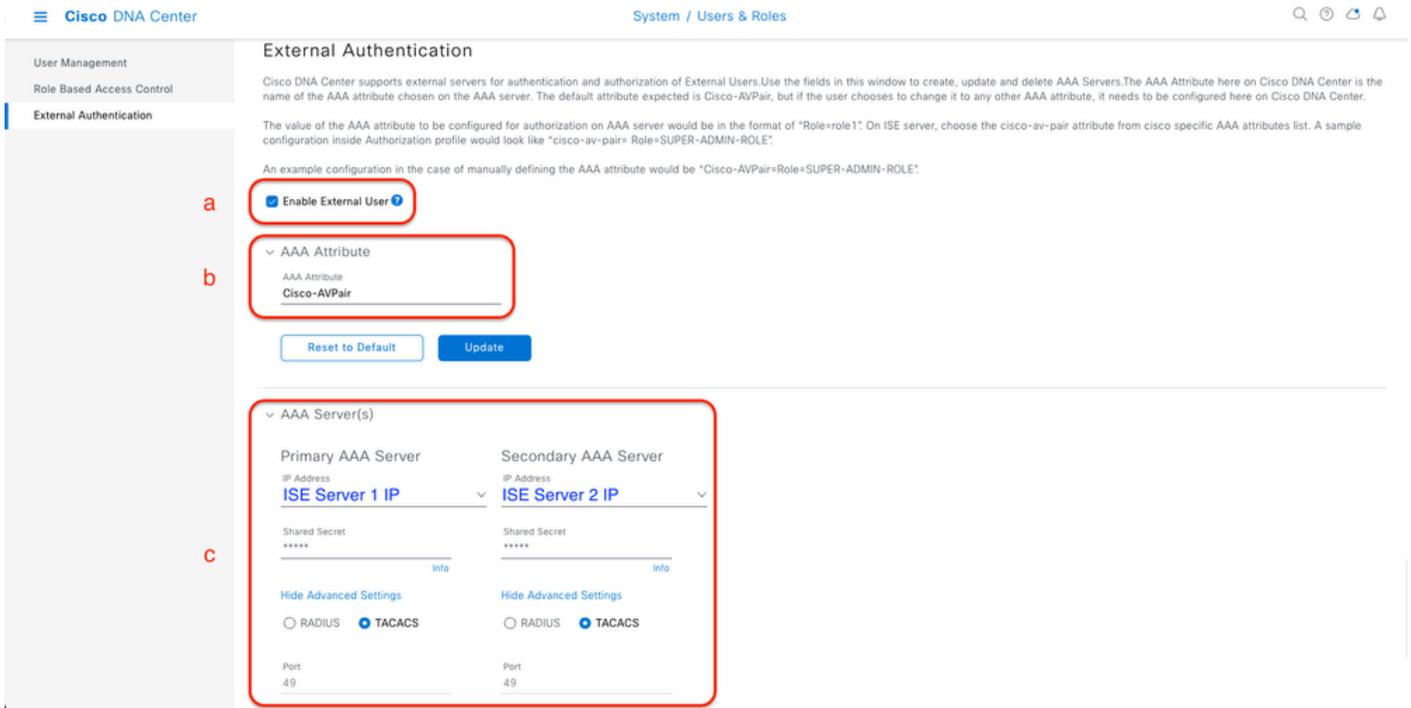
a. 要在Cisco DNA Center中啟用外部身份驗證，請選中啟用外部使用者覈取方塊。

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。

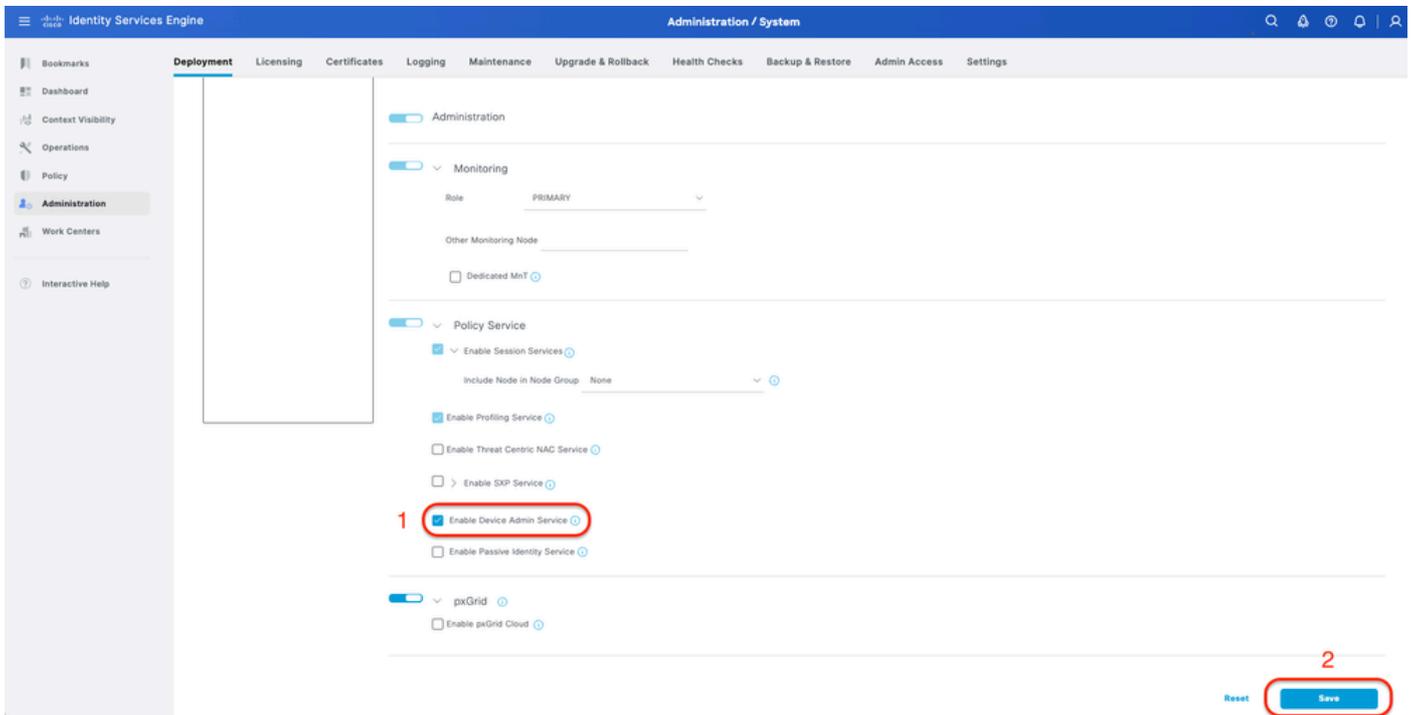


(TACACS+)外部身份驗證配置步驟

## ( 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。



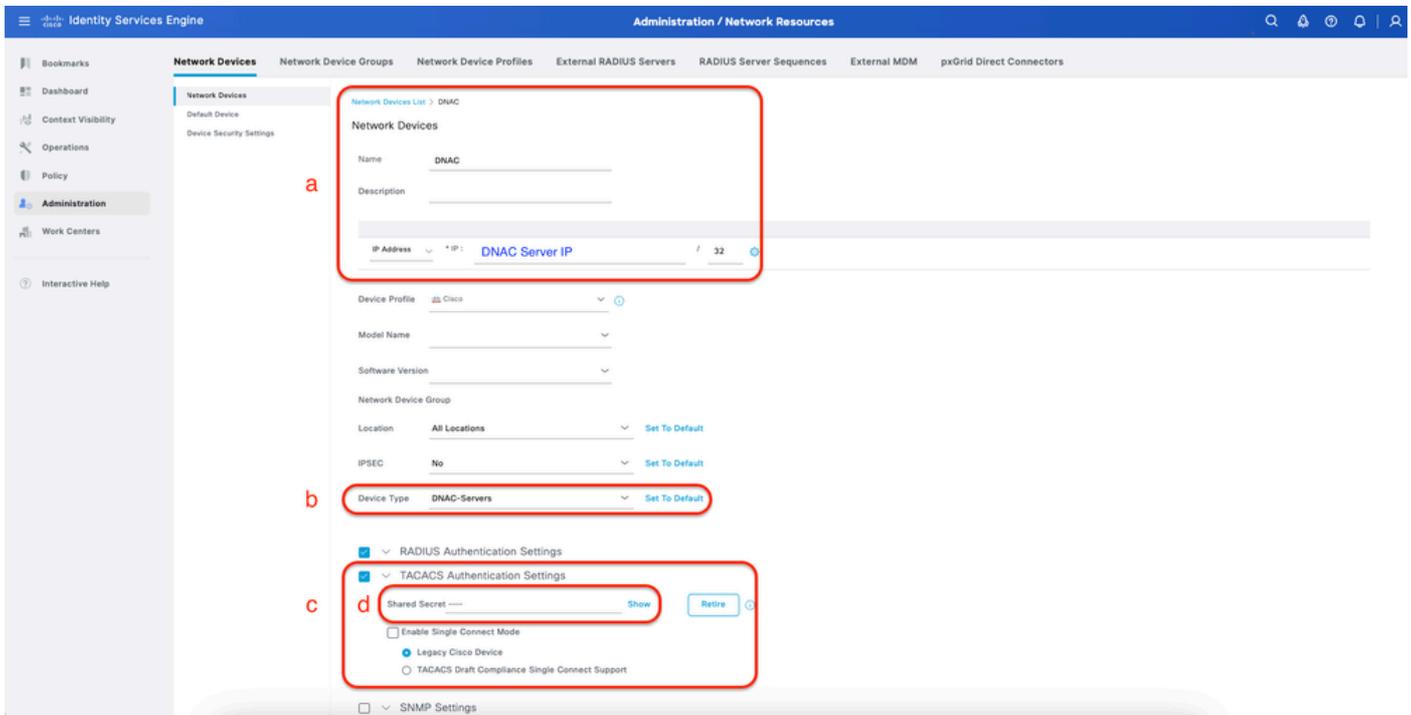
啟用裝置管理服務

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。



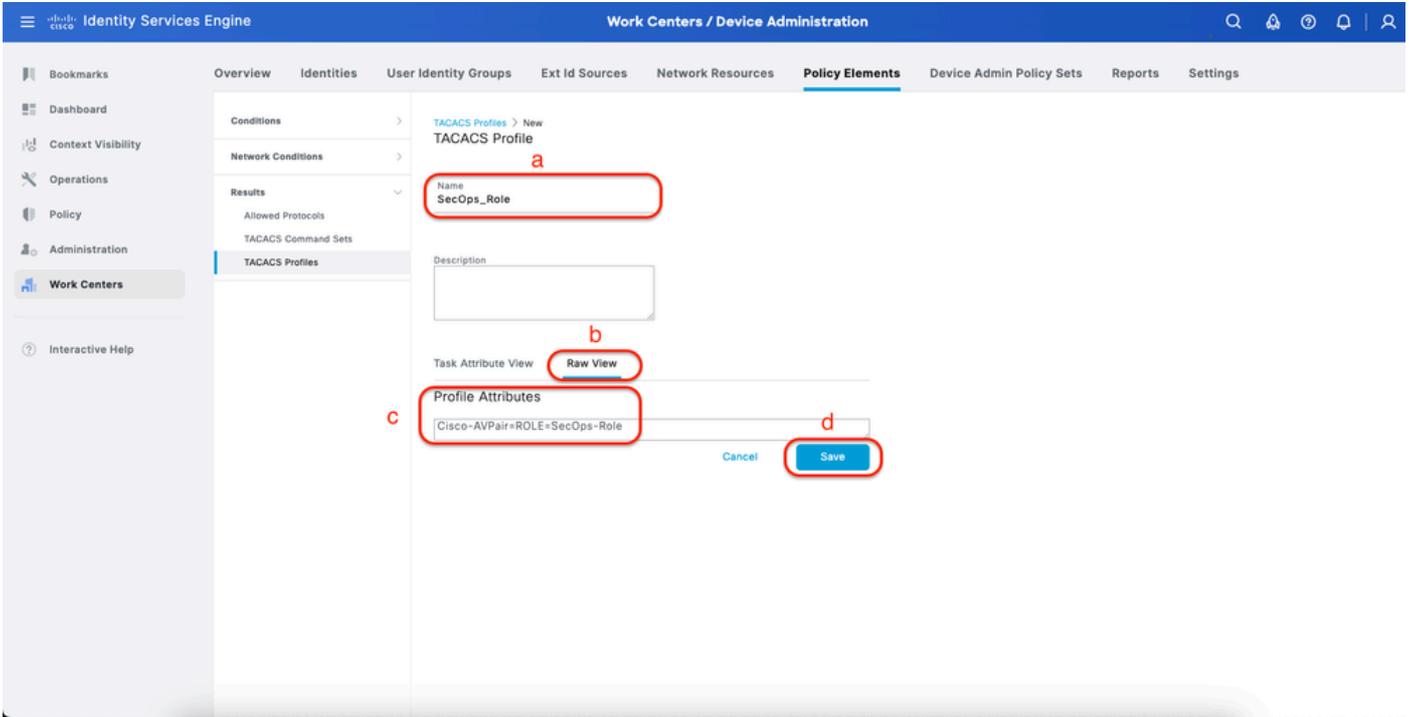
附註：建立3個TACACS+配置檔案，每個使用者角色一個。

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。

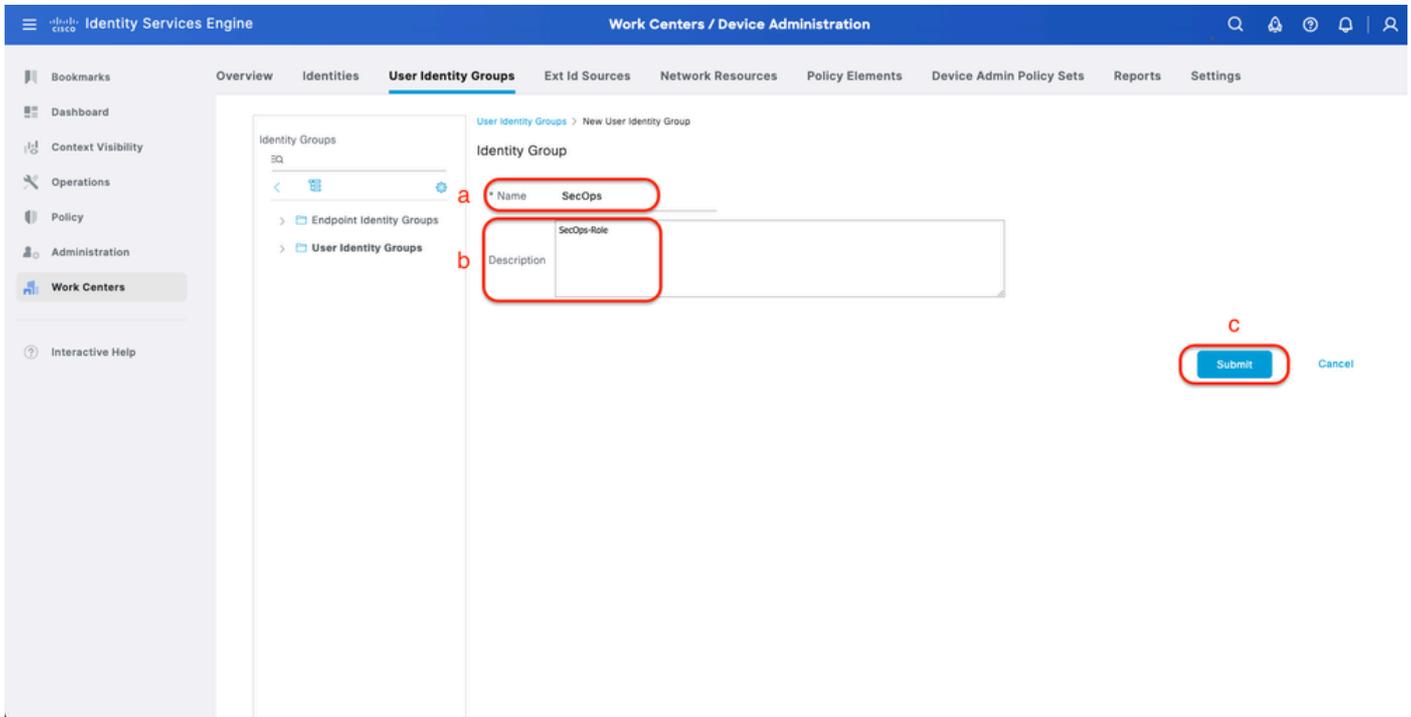
可從工作中心>裝置管理>使用者身份組頁籤完成此操作。

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。



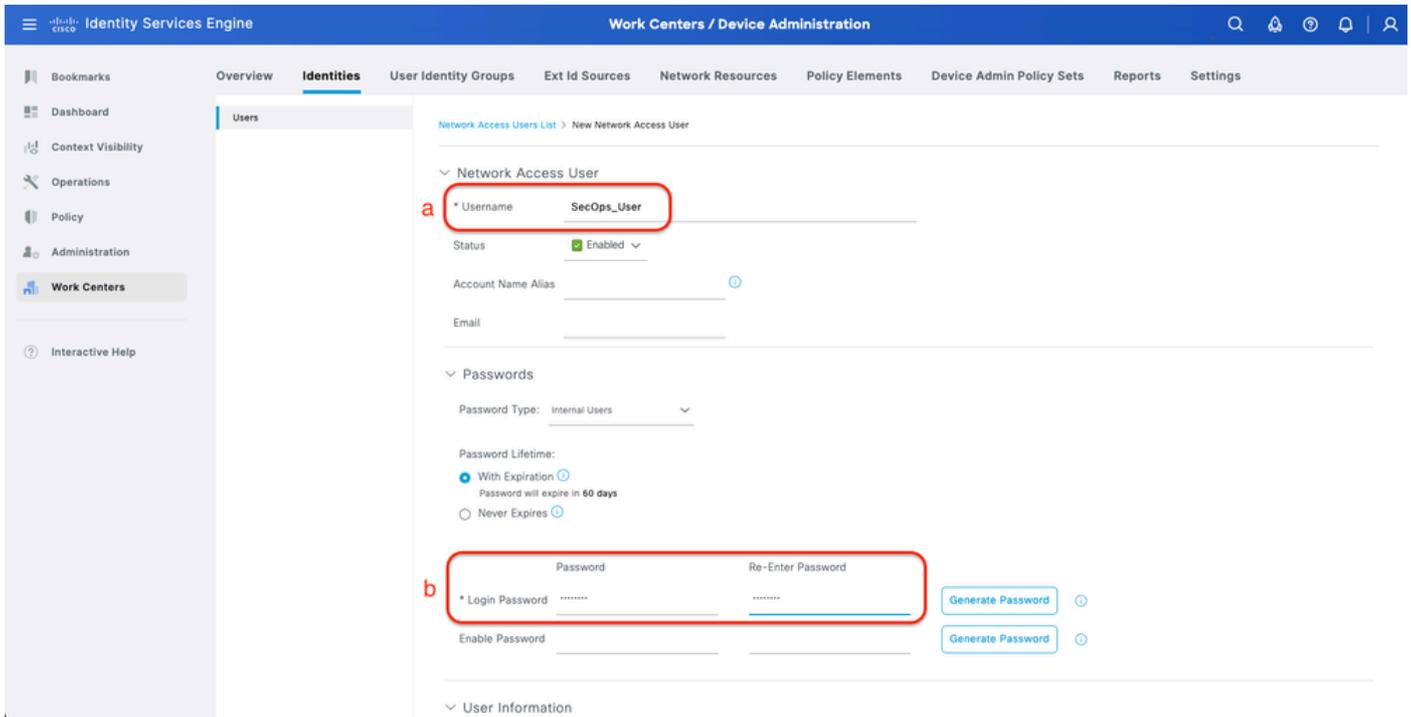
建立使用者身份組

步驟5.建立本地使用者。

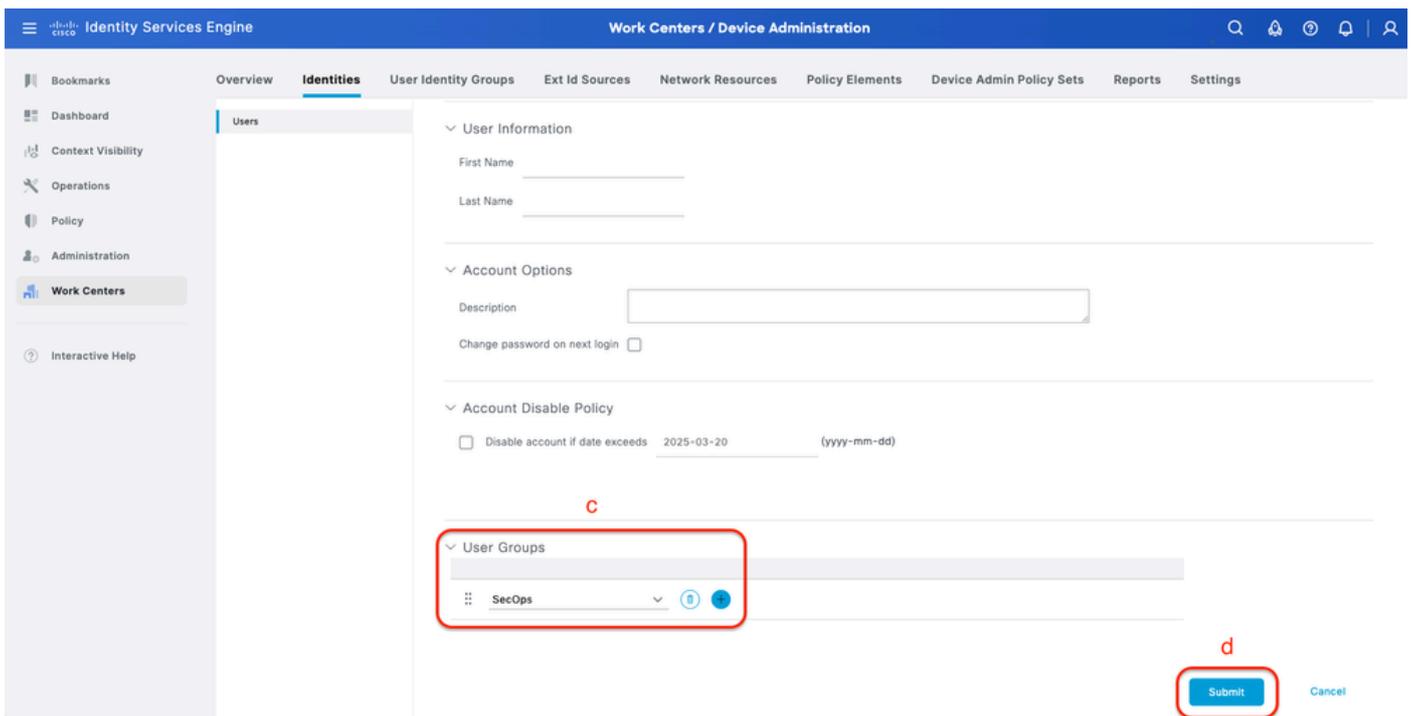
可從工作中心(Work Centers)>裝置管理(Device Administration)>身份(Identities)>使用者(Users)頁籤執行此操作。

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。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	DNAC - Policy		DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0	⚙️ >	>
●	Default	Default policy set		Default Network Access	0	⚙️ >	>

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」。

The screenshot displays the Cisco ISE Work Centers / Device Administration interface. The main content area shows 'Policy Sets -> DNAC - Policy'. A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A 'Save' button is circled in red and labeled 'e'. Below this, the 'Authentication Policy(2)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A new policy 'DNAC - Authentication' is highlighted with a red box labeled 'b'. Its conditions are 'DEVICE-Device Type EQUALS All Device Types#DNAC-Servers', also highlighted with a red box labeled 'c'. The 'Use' column for this policy is set to 'Internal Users', highlighted with a red box labeled 'd'. Other policies like 'Default' and 'All\_User\_ID\_Stores' are also visible.

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」。

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)  
> Authorization Policy - Local Exceptions  
> Authorization Policy - Global Exceptions  
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
+	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	+
+	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	+
+	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	+
+	Default		DenyAllCommands	Deny All Shell Profile	0	+

Reset 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。

Cisco DNA Center System / Users & Roles

User Management  
Role Based Access Control  
External Authentication

### External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role!". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

Enable External User

AAA Attribute  
Cisco-AVPair

Reset to Default Update

AAA Server(s)

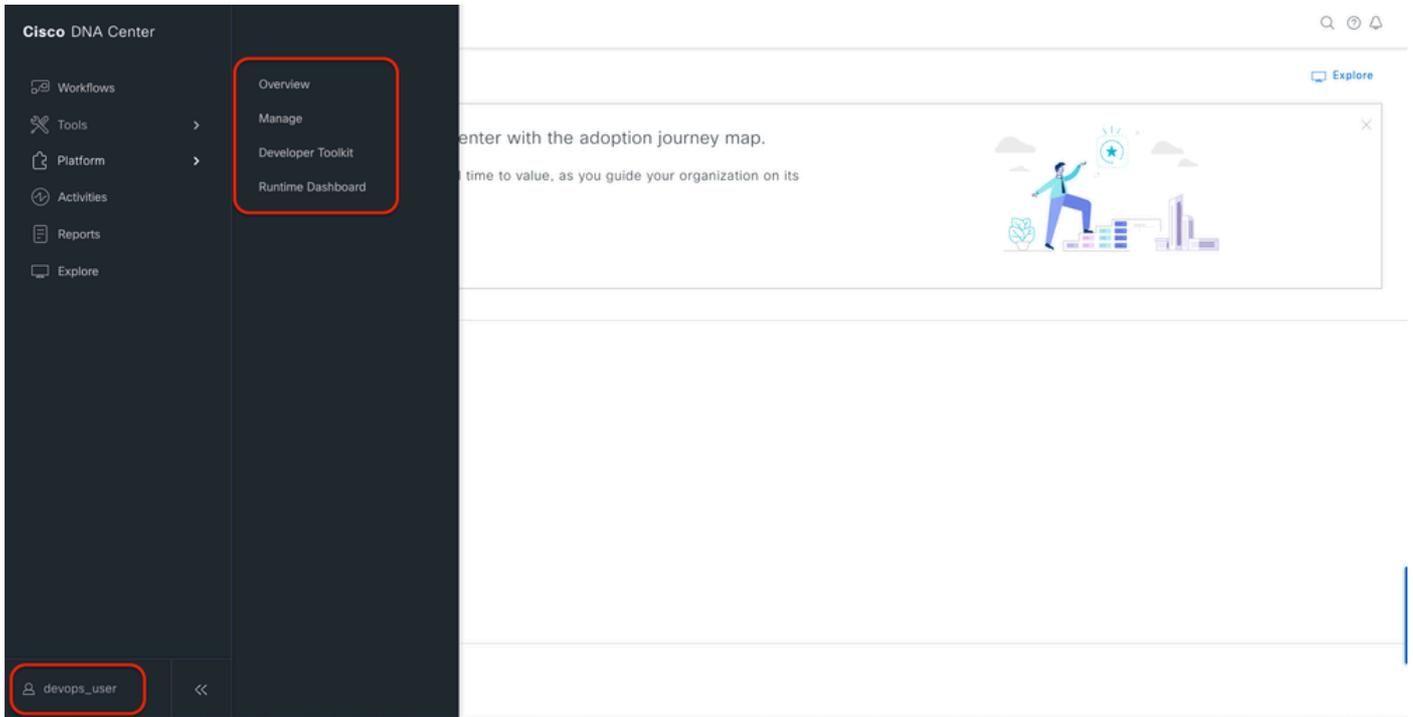
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

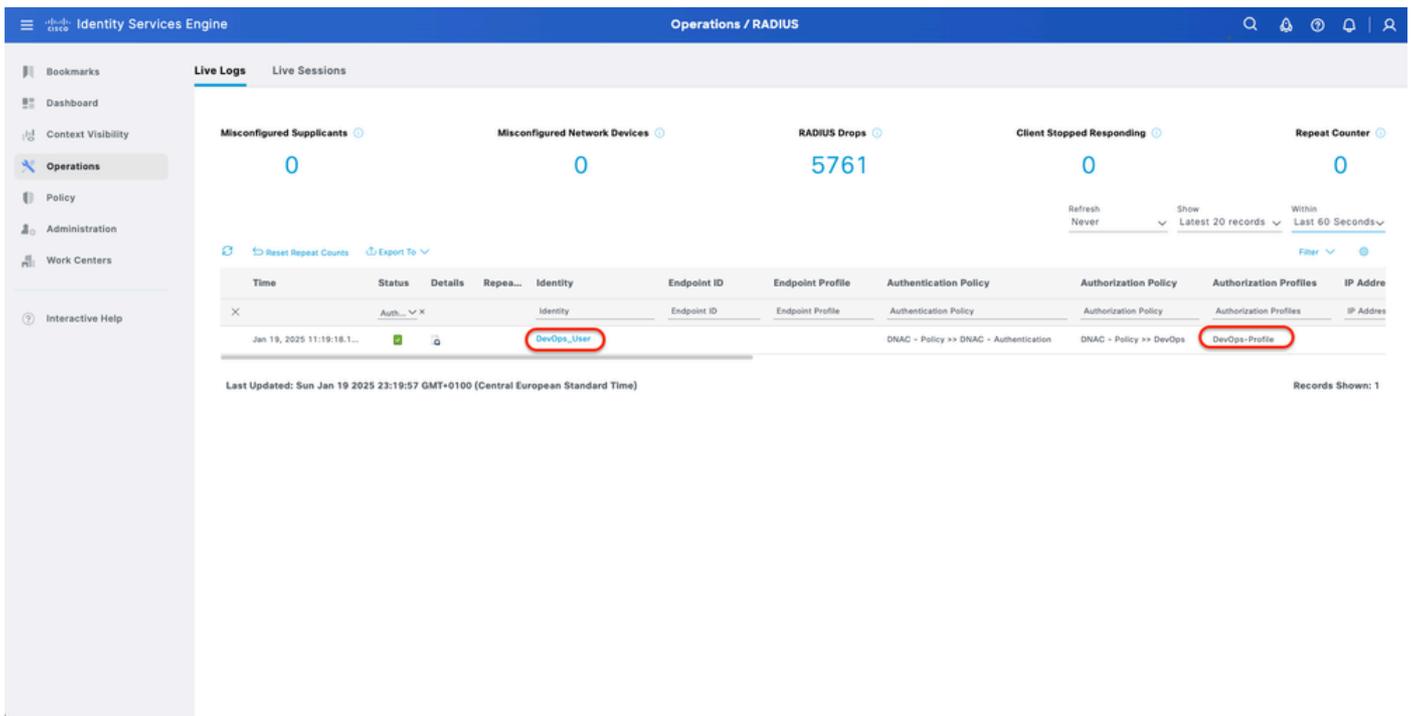
外部使用者

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。

**Cisco ISE**

**Overview**

Event: 5200 Authentication succeeded

Username: DevOps\_User

Endpoint Id:

Endpoint Profile:

Authentication Policy: DNAC - Policy >> DNAC - Authentication

Authorization Policy: DNAC - Policy >> DevOps

**Authorization Result: DevOps-Profile**

**Steps**

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
<b>22037</b>	<b>Authentication Passed</b>	<b>1</b>
15036	Evaluating Authorization Policy	1
<b>15016</b>	<b>Selected Authorization Profile - DevOps-Profile</b>	<b>5</b>
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
<b>11002</b>	<b>Returned RADIUS Access-Accept</b>	<b>0</b>

**Authentication Details**

Source Timestamp: 2025-01-19 23:19:18.156

Received Timestamp: 2025-01-19 23:19:18.156

Policy Server: ise34

Event: 5200 Authentication succeeded

Username: DevOps\_User

User Type: User

Authentication Identity Store: Internal Users

Identity Group: User Identity Groups:DevOps

Authentication Method: PAP\_ASCII

Authentication Protocol: PAP\_ASCII

Network Device: DNAC

Device Type: All Device Types#DNAC-Servers

Location: All Locations

RADIUS詳細即時日誌1-2

**Cisco ISE**

IdentityPolicyMatchedRule: DNAC - Authentication

AuthorizationPolicyMatchedRule: DevOps

ISEPolicySetName: DNAC - Policy

IdentitySelectionMatchedRule: DNAC - Authentication

TotalAuthnLatency: 35

ClientLatency: 0

DTLSSupport: Unknown

Network Device Profile: Cisco

Location: Location#All Locations

Device Type: Device Type#All Device Types#DNAC-Servers

IPSEC: IPSEC#Is IPSEC Device#No

Name: User Identity Groups:DevOps

EnableFlag: Enabled

RADIUS Username: DevOps\_User

Device IP Address:

CPMSessionID: 0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPPrRtG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=92731e30-8c01-11e6-996c-525400b48521rdevops\_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5dedf467

**Result**

Class: CACS:0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPPrRtG/WY:ise34/528427220/15433

**cisco-av-pair** ROLE=DevOps-Role

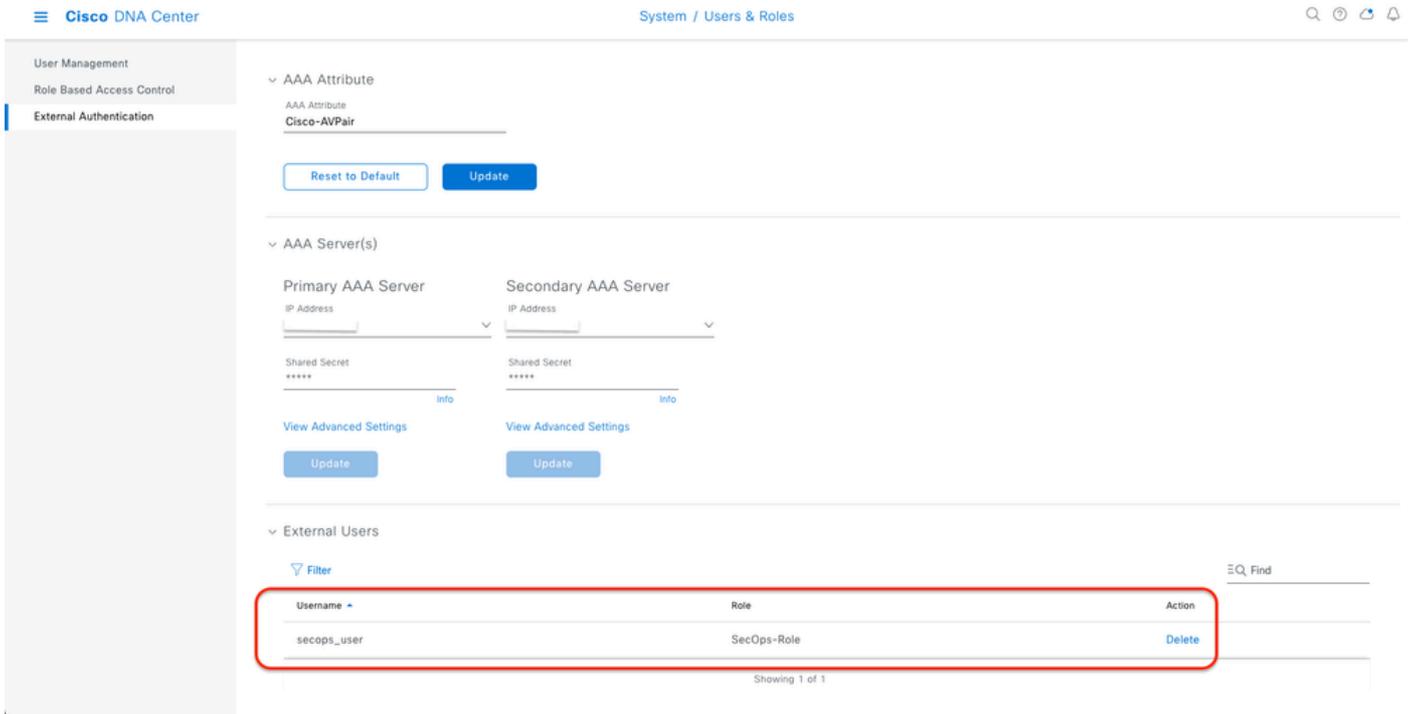
RADIUS詳細即時日誌2-2

## 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。

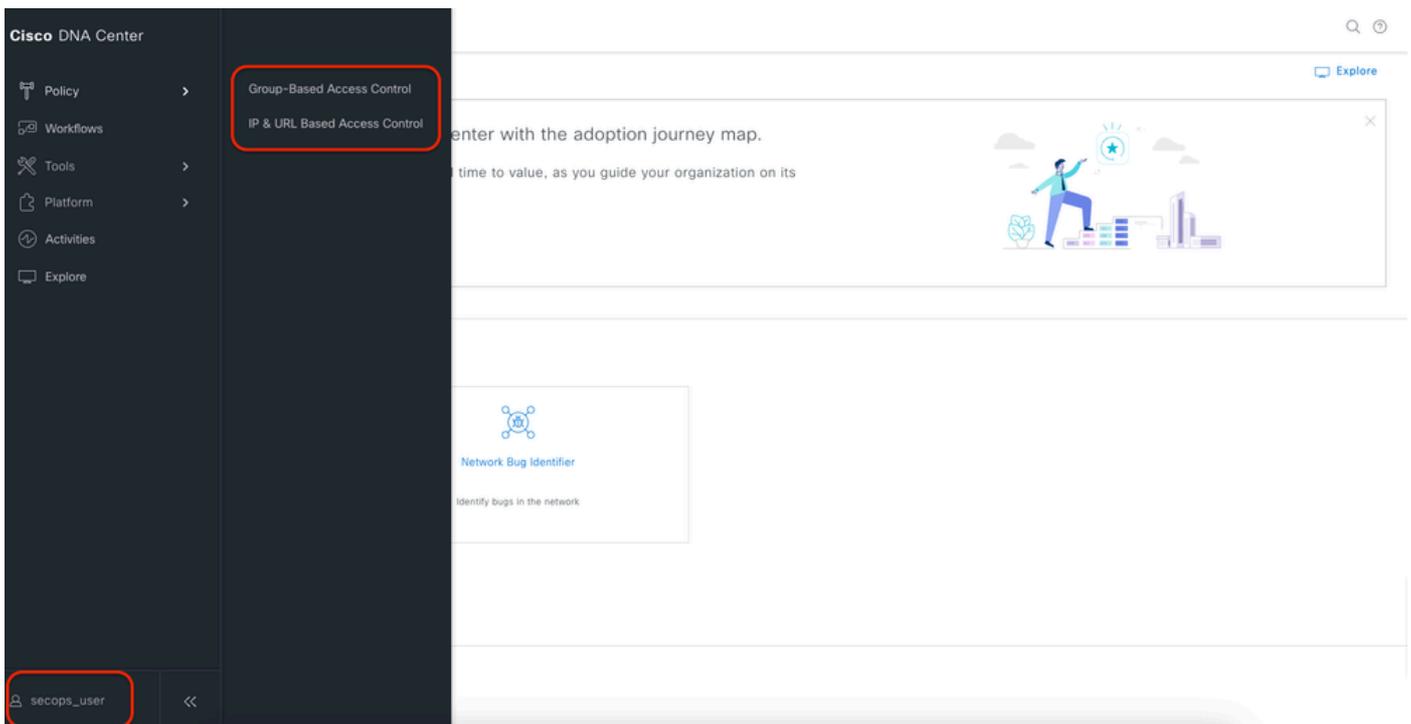
您可以檢視首次通過TACACS+登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色

o



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。

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

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。

Cisco ISE

**Overview**

Request Type: Authorization

Status: Pass

Session Key: ise34/526427220/13958

Message Text: Device-Administration: Session Authorization succeeded

Username: SecOps\_User

Authorization Policy: DNAC - Policy >> SecOps

Shell Profile: SecOps\_Role

Matched Command Set

Command From Device

**Steps**

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">22037</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">Authentication Passed</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">0</span>
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">15017</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">Selected Shell Profile</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">2</span>
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">13034</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">Returned TACACS+ Authorization Reply</span>	<span style="border: 1px solid red; border-radius: 5px; padding: 2px;">0</span>

**Authorization Details**

Generated Time: 2025-01-19 17:12:43.368 +1:00

Logged Time: 2025-01-19 17:12:43.368

Epoch Time (sec): 1737303163

ISE Node: ise34

Message Text: Device-Administration: Session Authorization succeeded

Failure Reason

Resolution

Root Cause

Username: SecOps\_User

Network Device Name: DNAC

TACACS+詳細即時日誌1-2

Type	Value
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;13=1;14=0;15=0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=ROLE+SecOps-Role; }

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）。