在DNA Center和ISE 3.1上配置RADIUS外部身份驗證

目錄

簡介

本文檔介紹如何使用運行3.1版的Cisco ISE伺服器在Cisco DNA Center上配置RADIUS外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco DNA Center和Cisco ISE已經整合，並且整合處於活動狀態。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

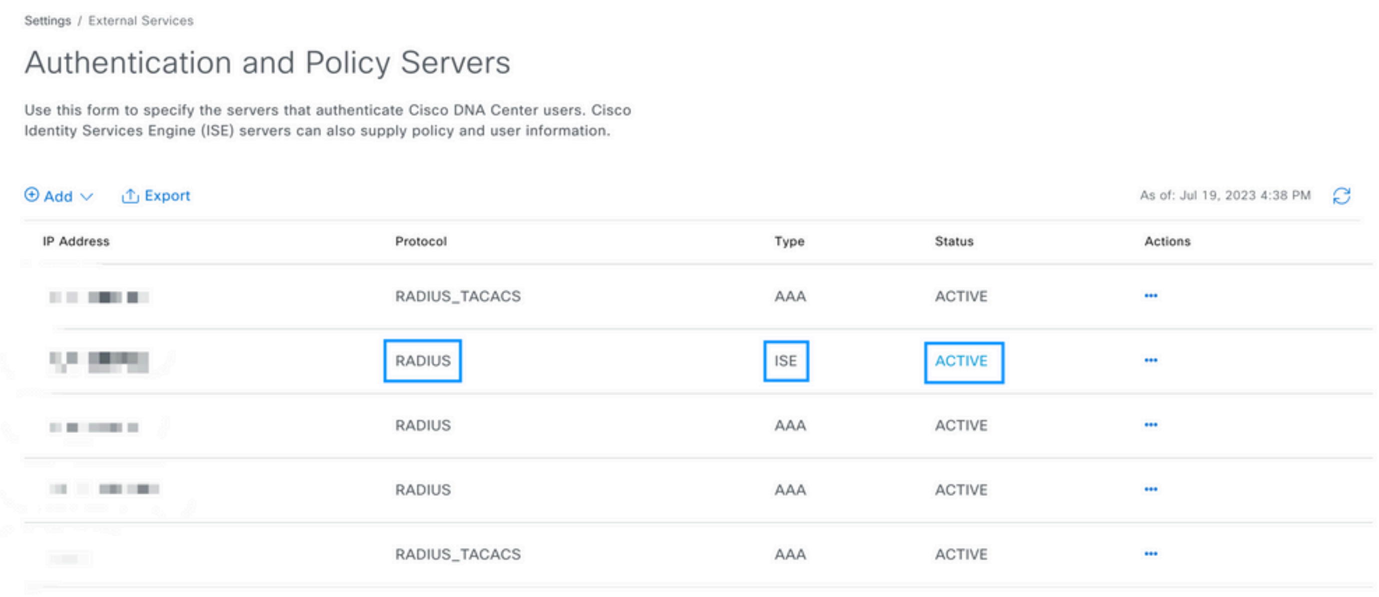
- Cisco DNA Center 2.3.5.x版本。
- Cisco ISE 3.1版本。

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

步驟 1. 登入Cisco DNA Center GUI 並導航至System > Settings > Authentication and Policy Servers。

驗證是否已配置RADIUS協定以及ISE狀態是否為Active(對於ISE型別伺服器)。



Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

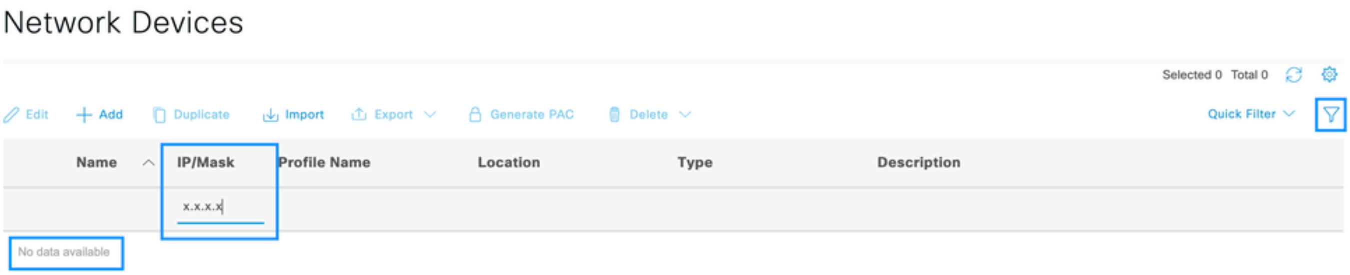
IP Address	Protocol	Type	Status	Actions
[redacted]	RADIUS_TACACS	AAA	ACTIVE	•••
[redacted]	RADIUS	ISE	ACTIVE	•••
[redacted]	RADIUS	AAA	ACTIVE	•••
[redacted]	RADIUS	AAA	ACTIVE	•••
[redacted]	RADIUS_TACACS	AAA	ACTIVE	•••

注意：RADIUS_TACACS協定型別適用於此文檔。

警告：如果ISE伺服器未處於活動狀態，則必須首先修復該整合。

步驟 2.在ISE伺服器導航到管理>網路資源>網路裝置，點選過濾器圖示，寫入Cisco DNA中心IP地址，確認條目是否存在。如果是，請繼續執行步驟3。

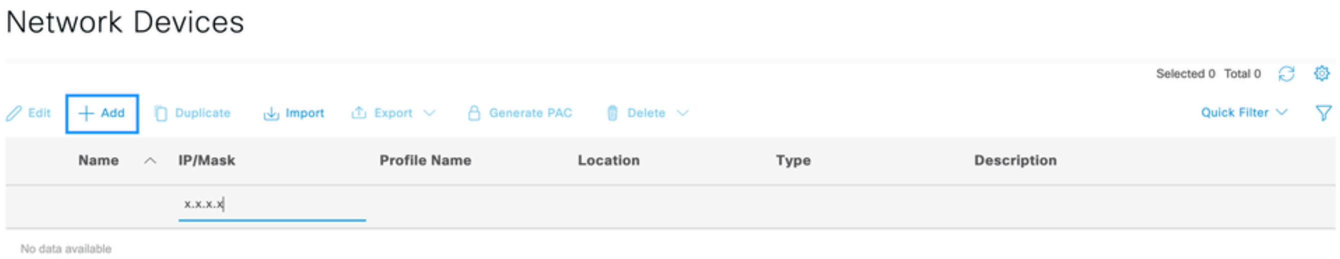
如果缺少條目，您必須看到無可用資料消息。



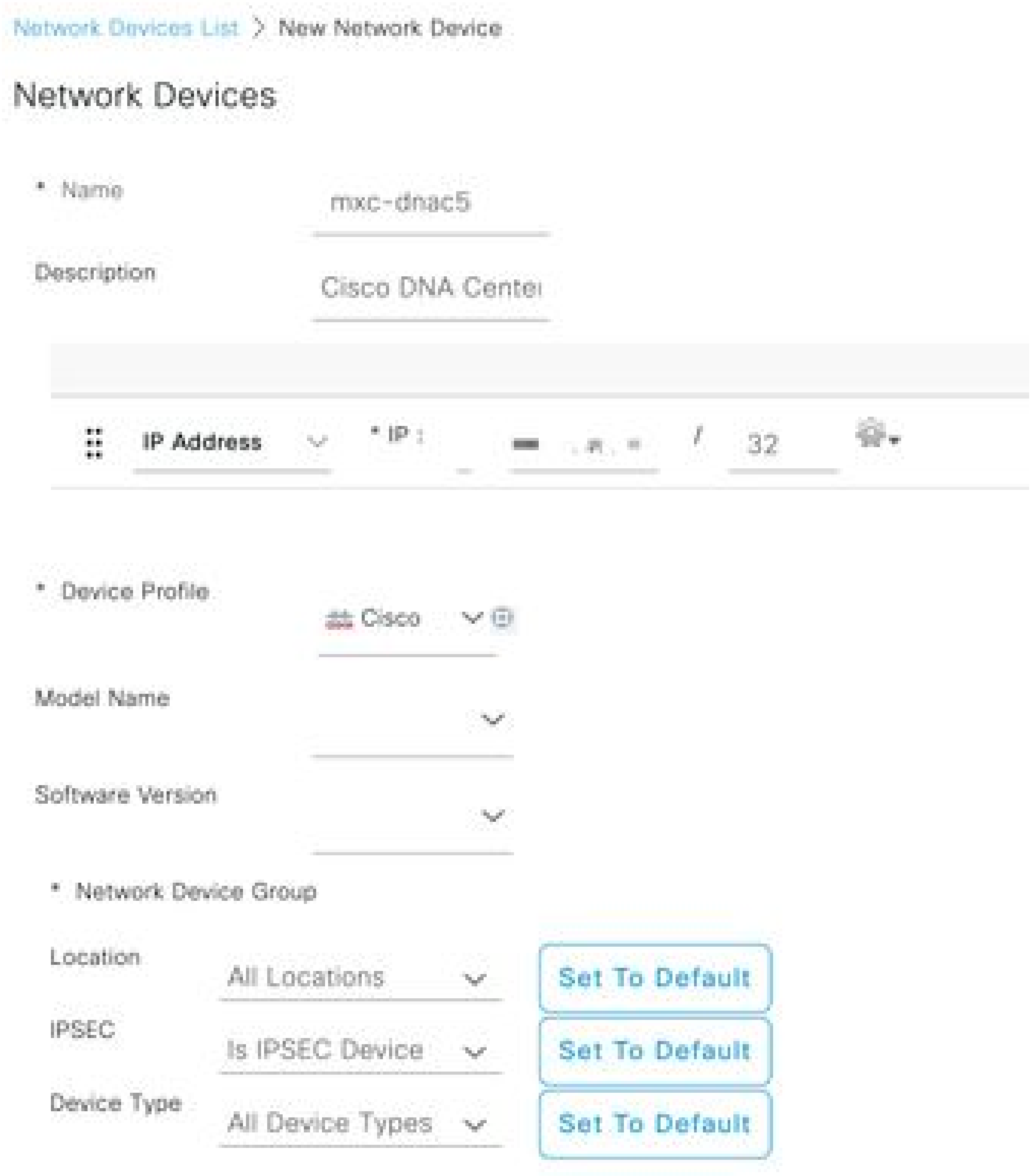
Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

在這種情況下，您必須為Cisco DNA Center建立一個網路裝置，然後按一下Add按鈕。



在Cisco DNA Center中配置名稱、描述和IP地址（或地址），所有其他設定均設定為預設值，本文檔中不需要這些設定。



Network Devices List > New Network Device

Network Devices

* Name: mxc-dnac5

Description: Cisco DNA Cente

IP Address * IP : [redacted] / 32

* Device Profile: Cisco

Model Name

Software Version

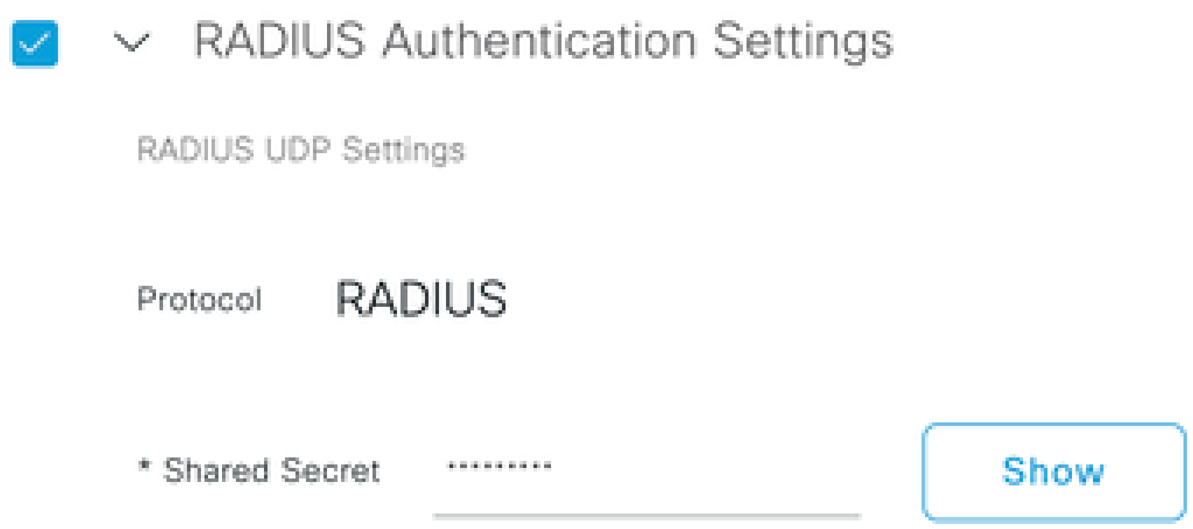
* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

向下滾動並透過按一下RADIUS Authentication Settings覈取方塊並配置Shared Secret來啟用它。



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

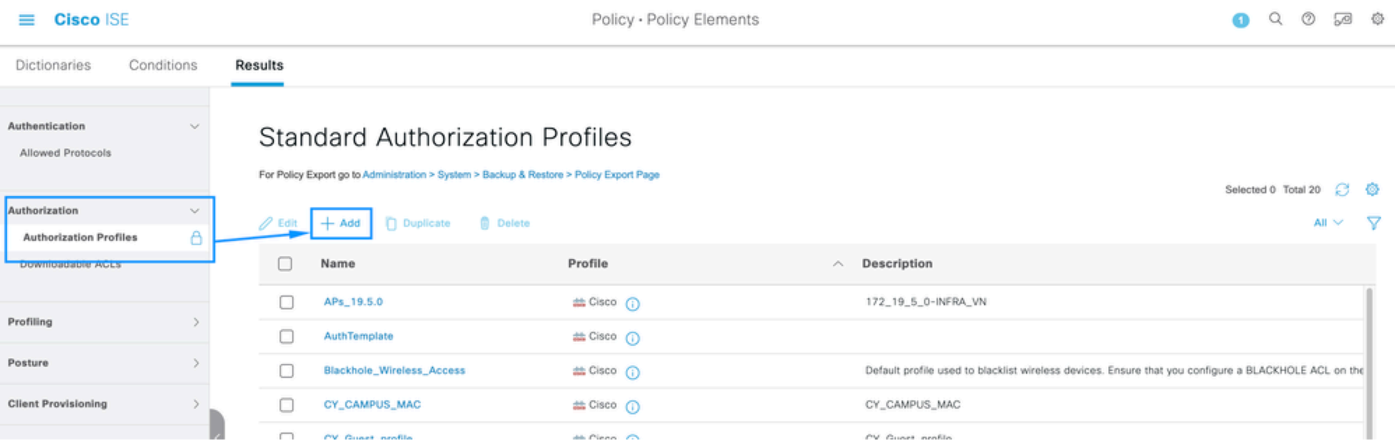
* Shared Secret ··········

提示：此共用金鑰將在以後需要，因此請將其儲存到其他位置。

然後，按一下Submit。

步驟 3.在ISE伺服器上，導航到策略>策略元素>結果，建立授權配置檔案。

確保您處於Authorization > Authorization Profiles下，然後選擇Add選項。

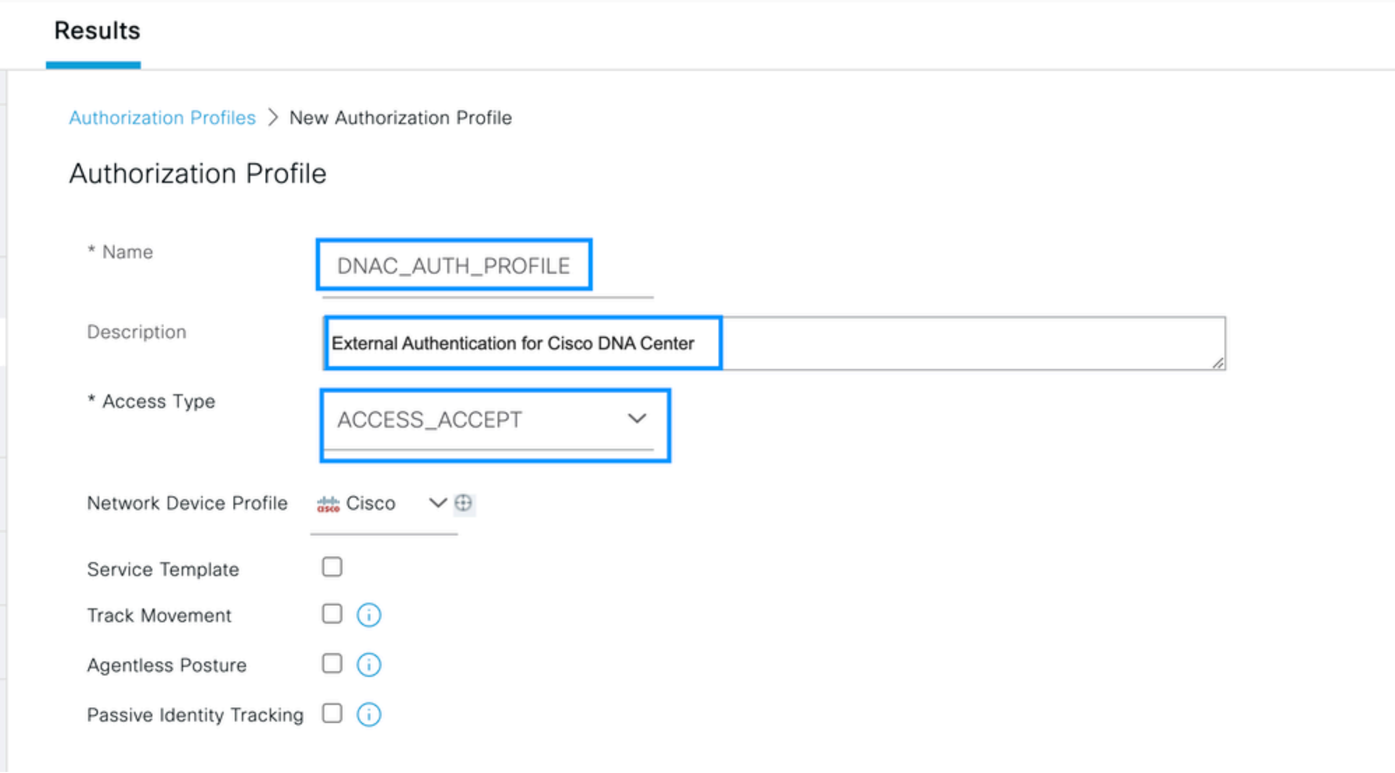


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Profile	Description
□	APs_19.5.0	Cisco	172_19_5_0-INFRA_VN
□	AuthTemplate	Cisco	
□	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the
□	CY_CAMPUS_MAC	Cisco	CY_CAMPUS_MAC
□	CY_Guest_profile	Cisco	CY_Guest_profile

配置Name，增加Description以保留新配置檔案的記錄，並確保Access Type設定為ACCESSES_ACCEPT。



Authorization Profile

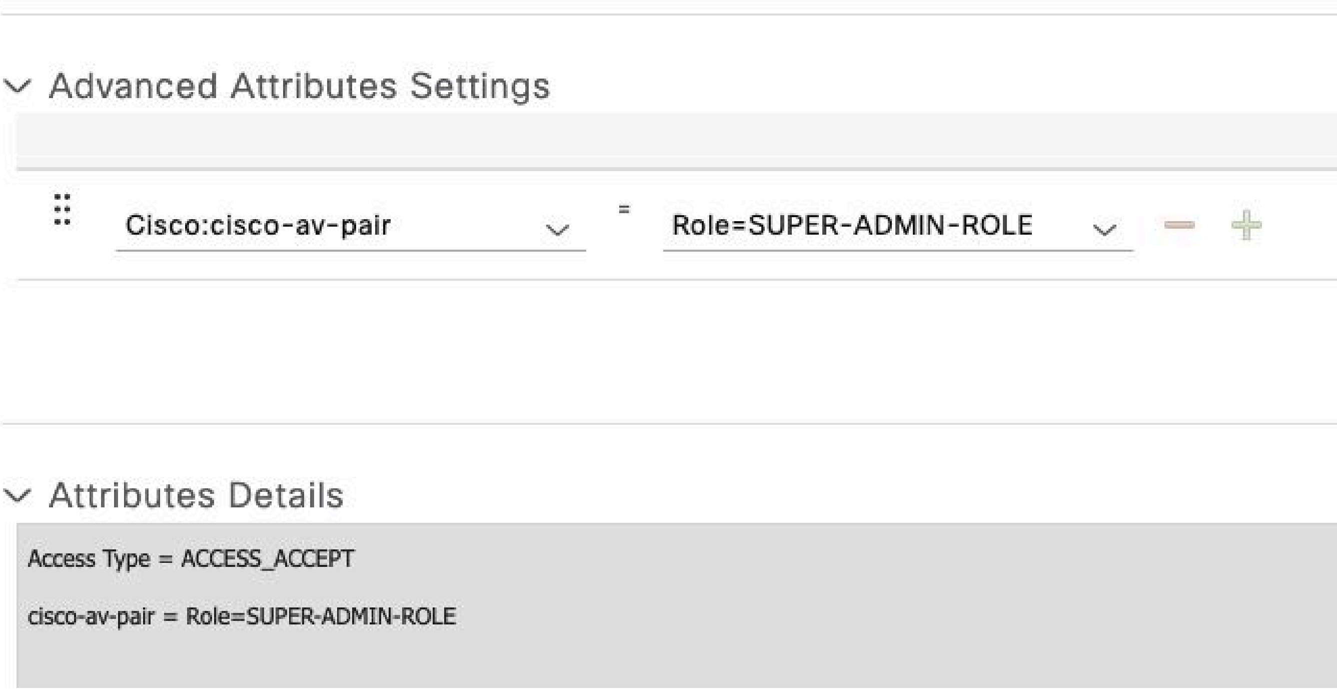
* Name	DNAC_AUTH_PROFILE
Description	External Authentication for Cisco DNA Center
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Agentless Posture	□
Passive Identity Tracking	□

向下滾動並配置高級屬性設定。

在左側列中搜尋cisco-av-pair選項並將其選中。

在右列手動鍵入Role=SUPER-ADMIN-ROLE。

一旦它看起來像以下映像，請按一下Submit。



Advanced Attributes Settings

Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE

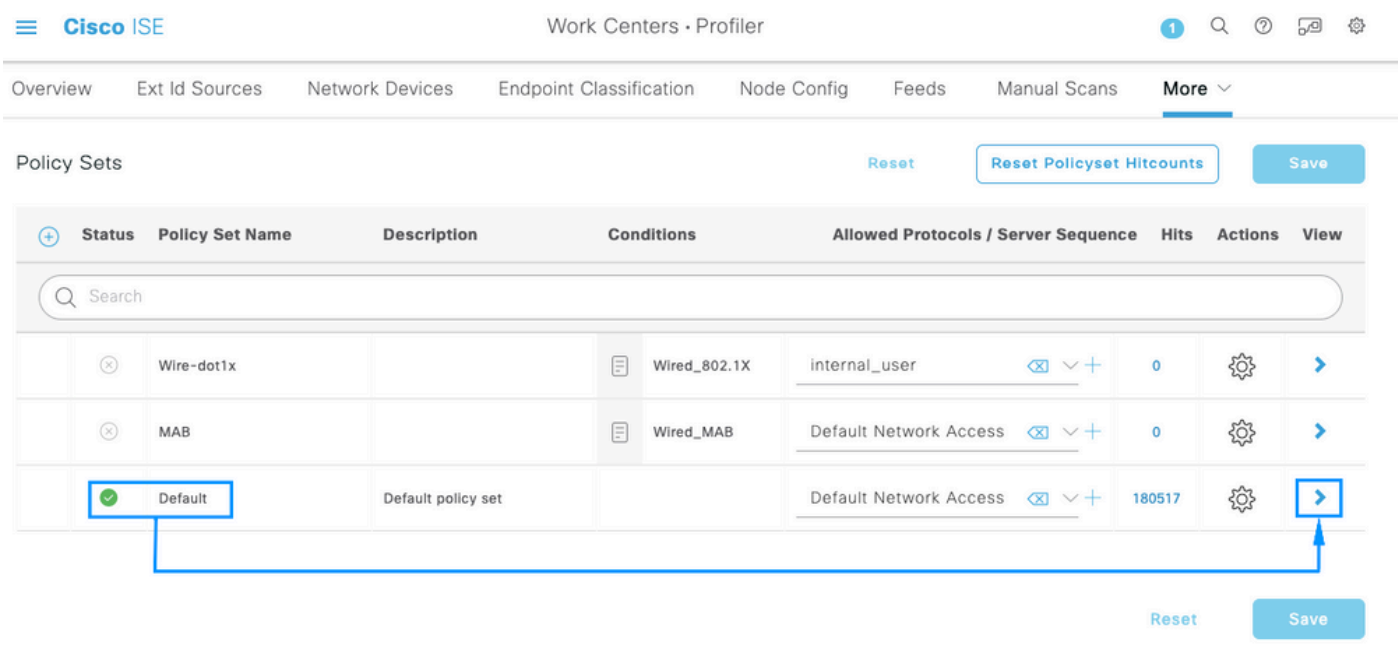
Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = Role=SUPER-ADMIN-ROLE

步驟 4.在ISE伺服器上，導航到工作中心>分析器>策略集，配置身份驗證和授權策略。

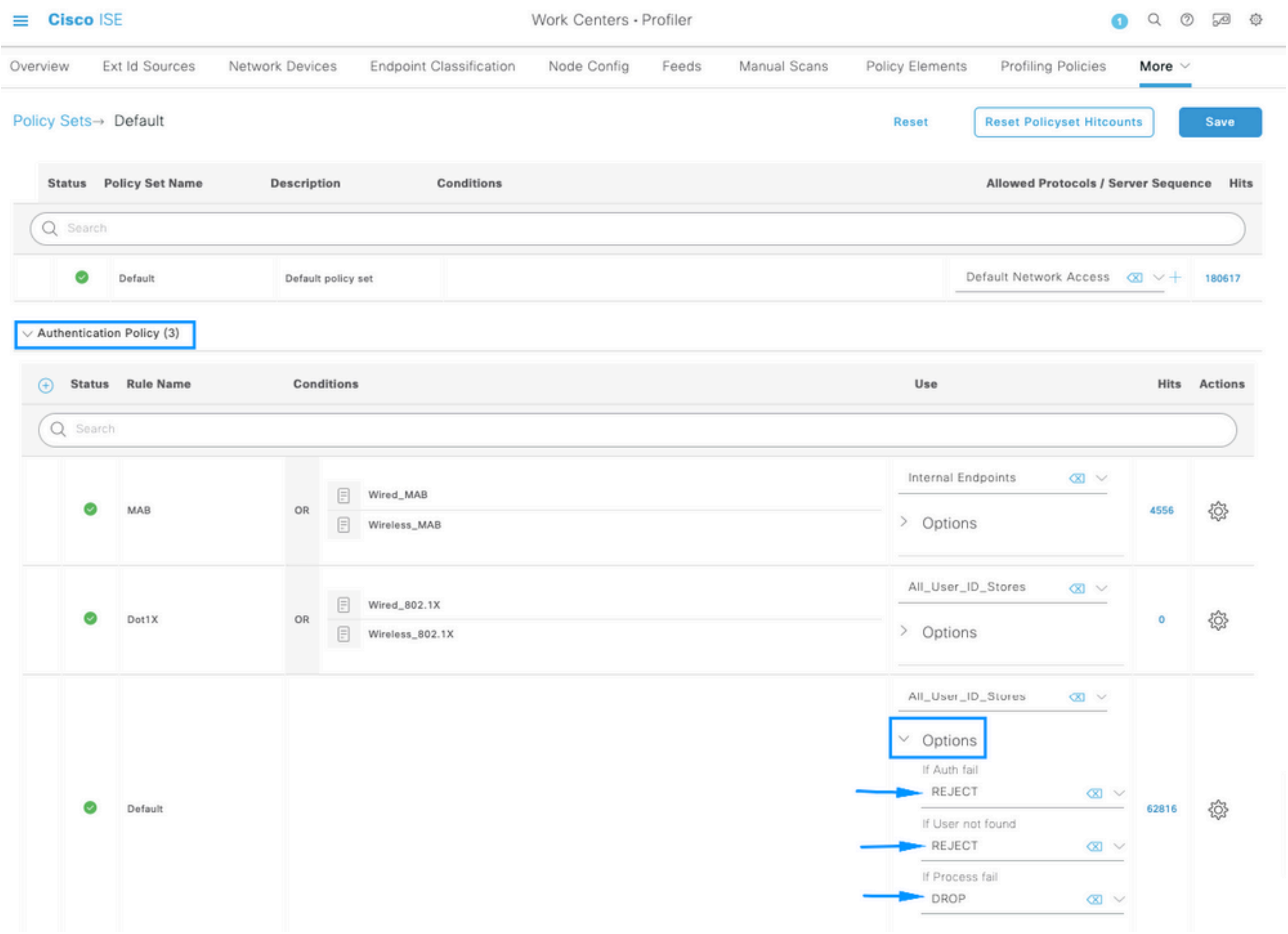
確定預設策略並按一下藍色箭頭進行配置。



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙	>
⊗	MAB		Wired_MAB	Default Network Access	0	⚙	>
✓	Default	Default policy set		Default Network Access	180517	⚙	>

在Default Policy Set內部，展開Authentication Policy，並在Default部分下展開Options，並確保它們與下面的配置匹配。

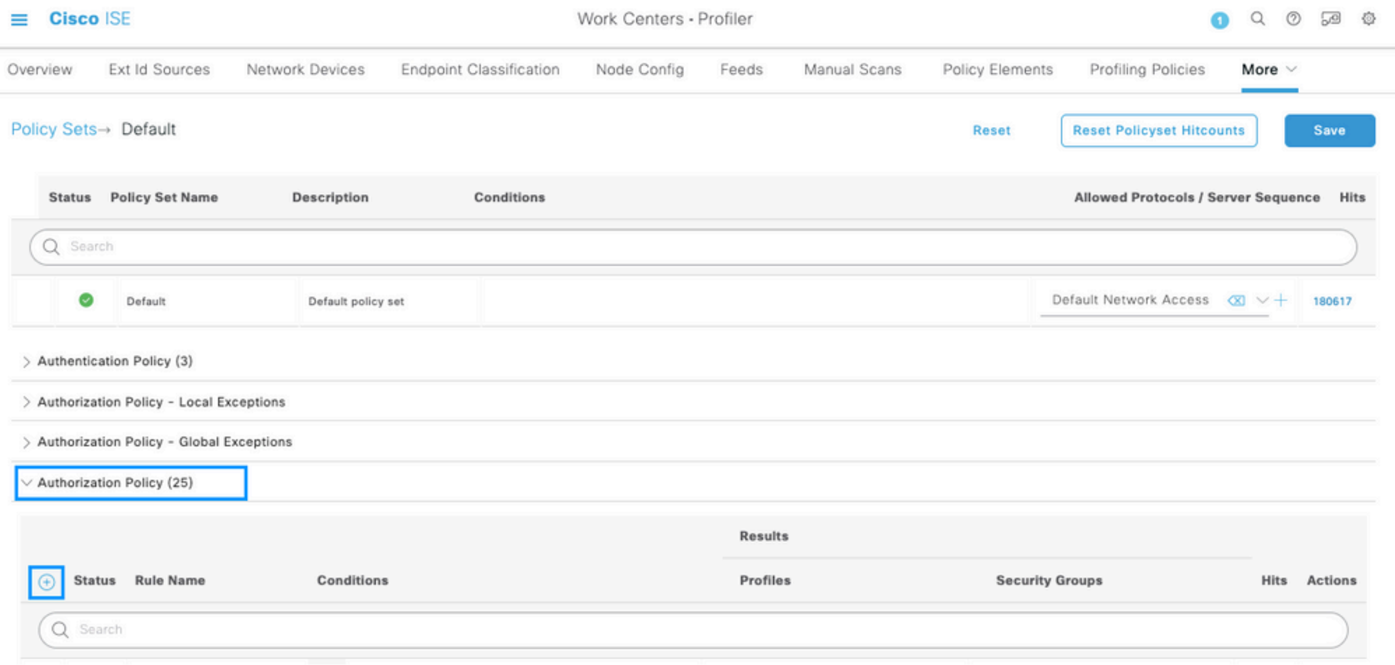


Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options	4556	⚙
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	0	⚙
✓	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙

提示：在3個選項上配置的「拒絕」也有效

在預設策略集中，展開Authorization Policy，並選擇Add圖示以建立新的Authorization Condition。

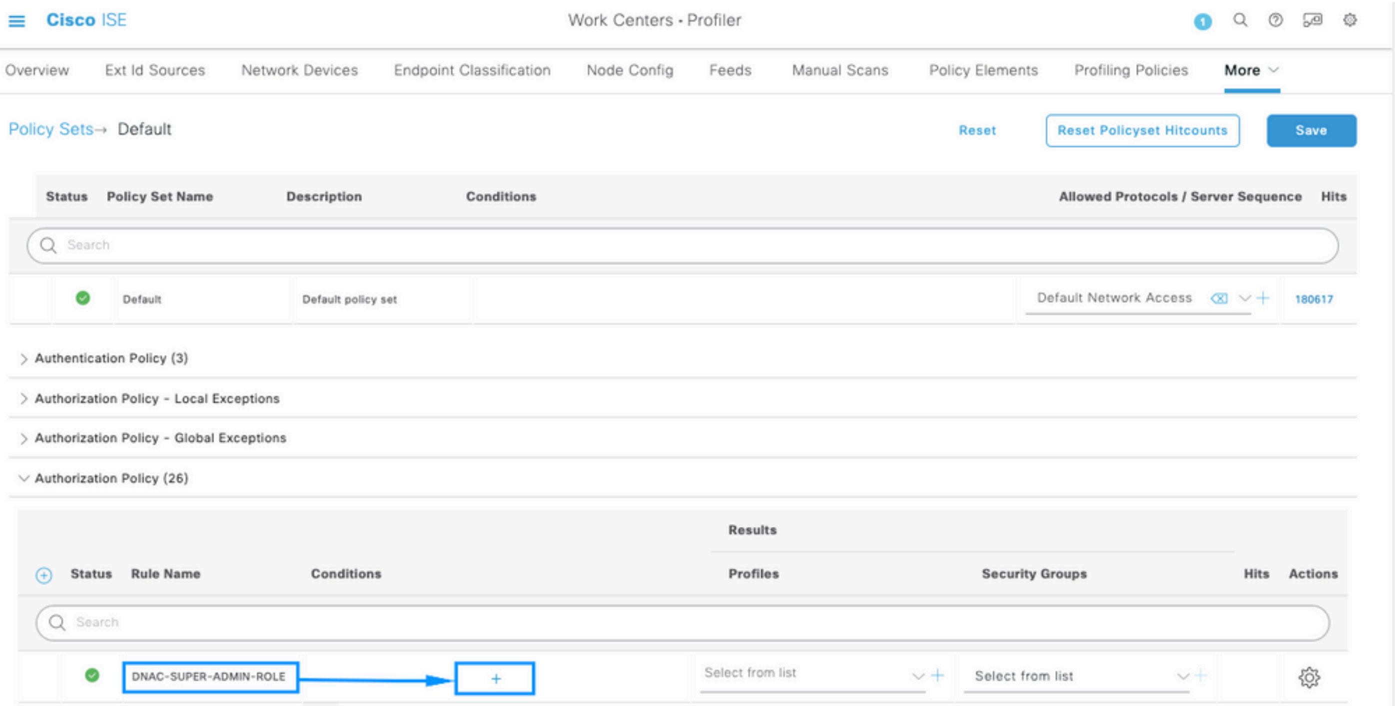


Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (25)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

配置Rule Name，然後按一下Add圖示配置Condition。

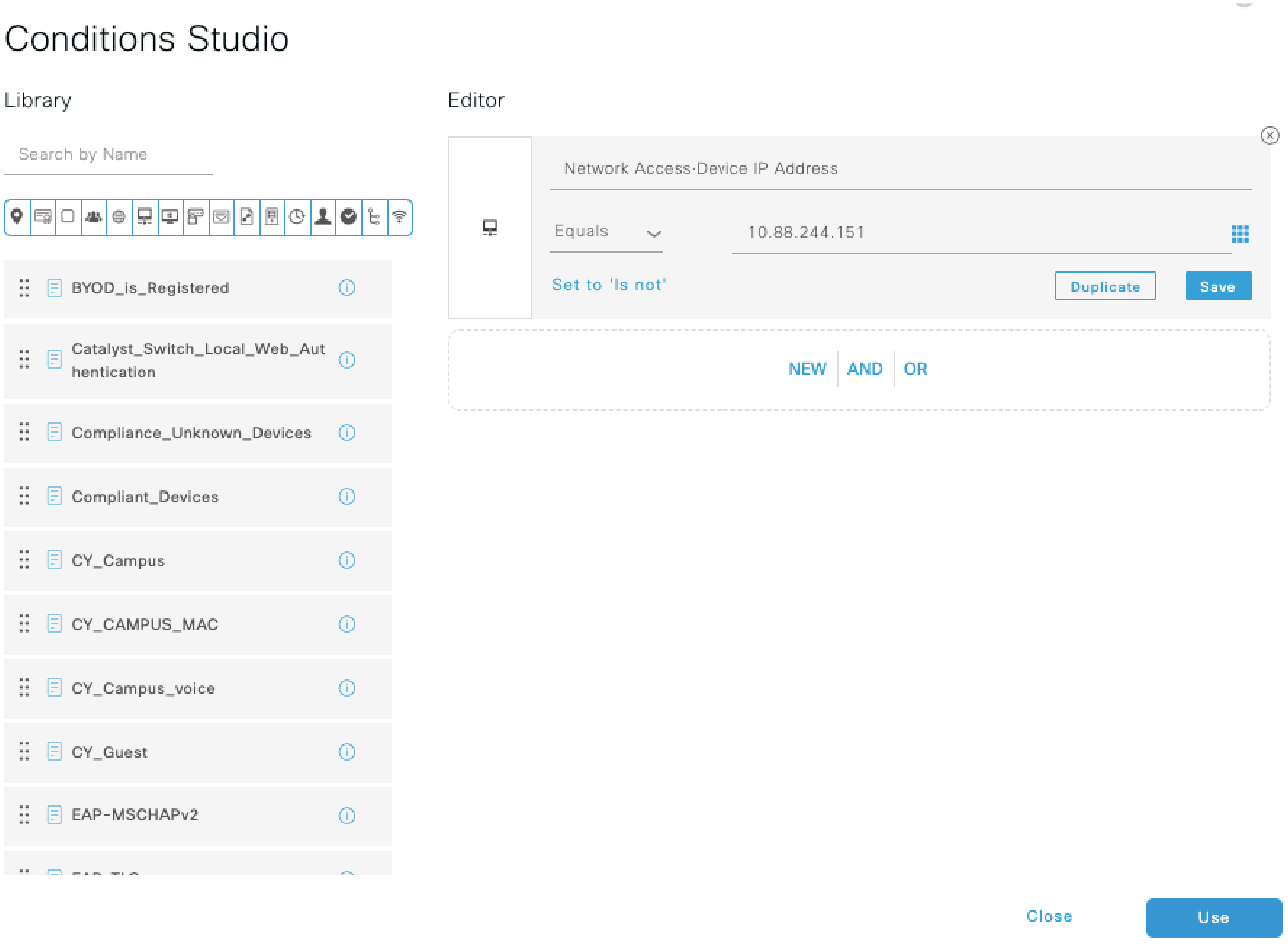


Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (26)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	DNAC-SUPER-ADMIN-ROLE	+	Select from list	Select from list		⚙

作為情況的一部分，請將其與步驟2中配置的網路裝置IP地址關聯。



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CY_Campus
- CY_CAMPUS_MAC
- CY_Campus_voice
- CY_Guest
- EAP-MSCHAPv2

Editor

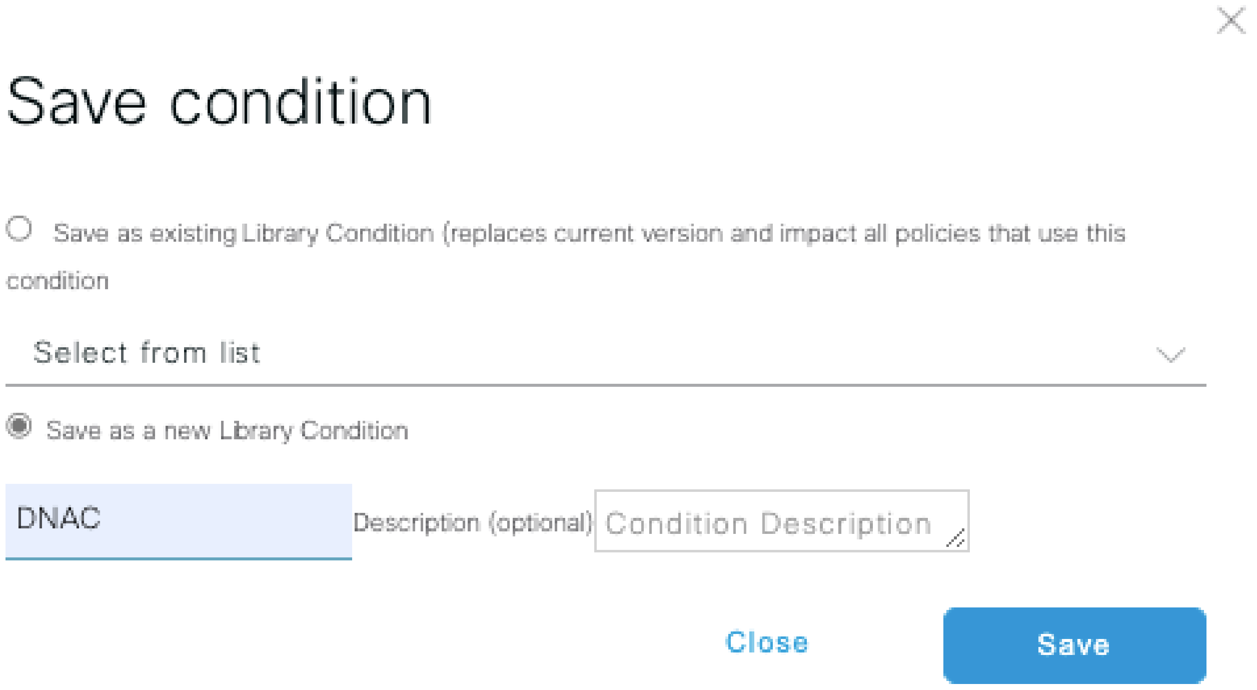
Network Access·Device IP Address

Equals 10.88.244.151

Set to 'Is not'

點選儲存。

將它另存為新的庫條件，並根據需要為其命名，在這種情況下，命名為DNAC。



Save condition

○ Save as existing Library Condition (replaces current version and impact all policies that use this condition

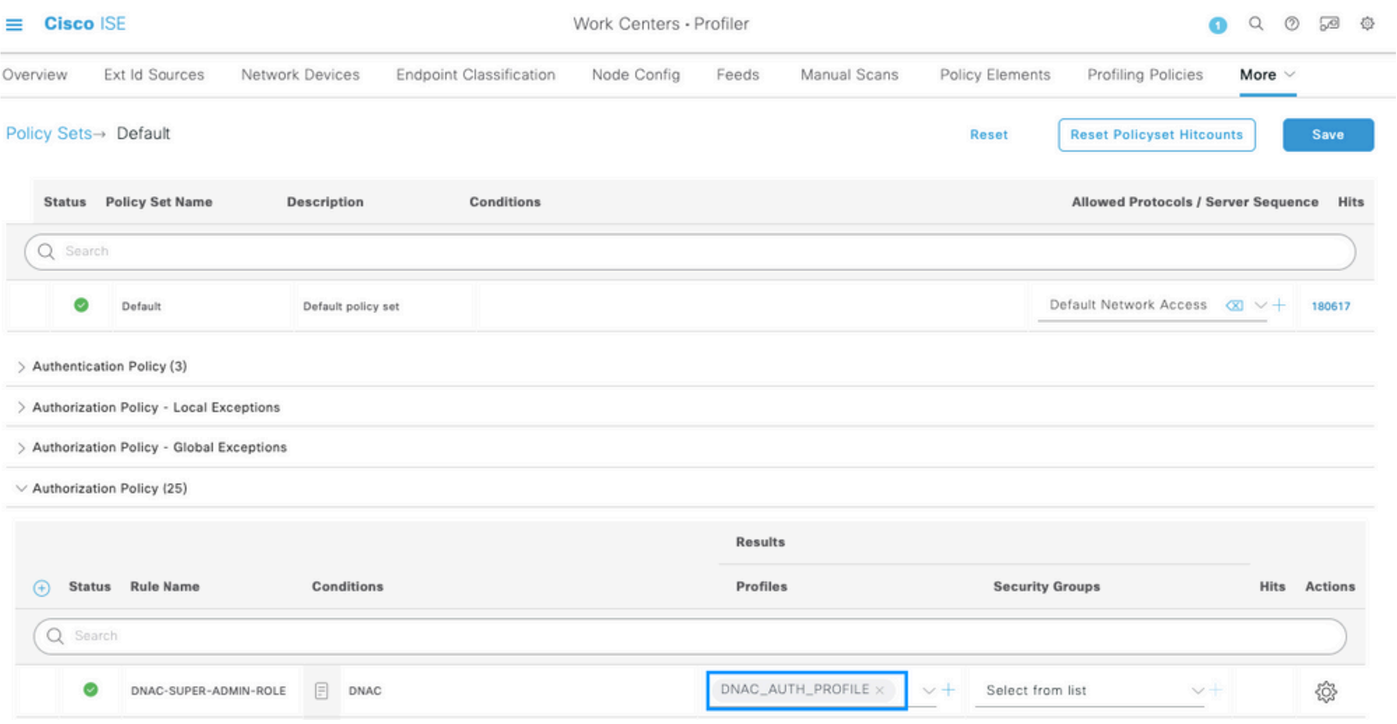
Select from list

● Save as a new Library Condition

DNAC

Description (optional) Condition Description

最後，配置在步驟3中建立的配置檔案。



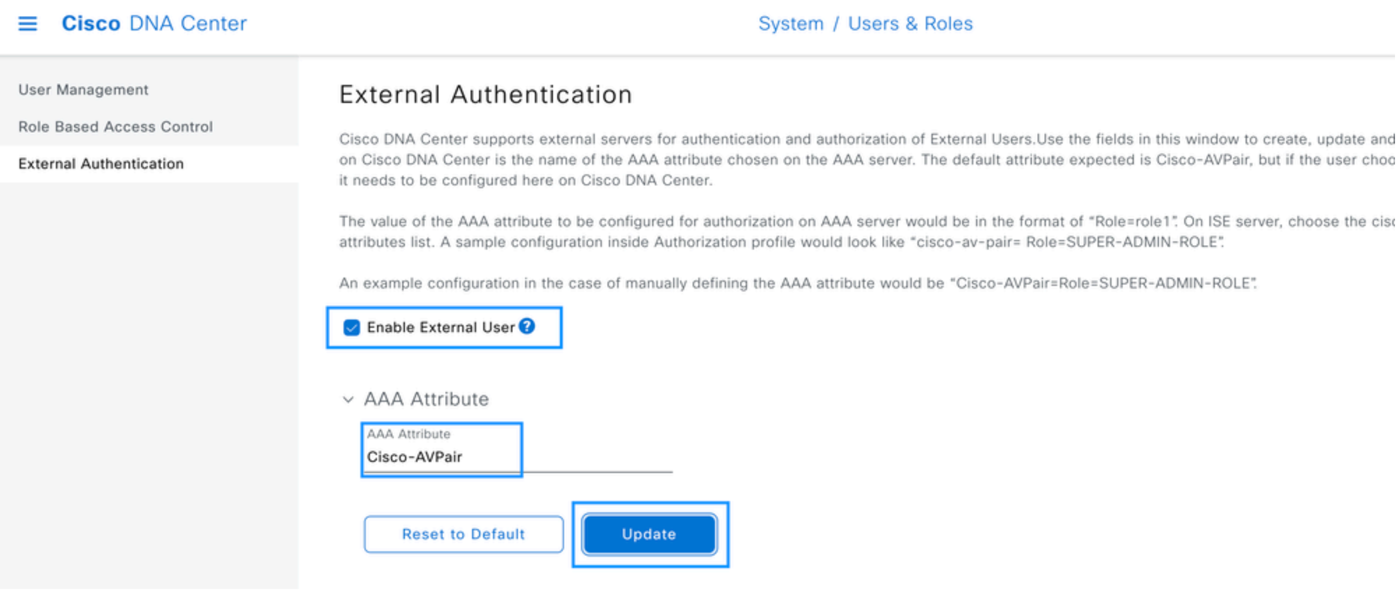
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	180617

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	DNAC-SUPER-ADMIN-ROLE	DNAC	DNAC_AUTH_PROFILE	Select from list		

按一下Save。

步驟 5. 登入到Cisco DNA Center GUI，然後導航到System > Users & Roles > External Authentication。

按一下Enable External User選項，並將AAA Attribute設定為Cisco-AVPair。



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 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 choo 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 cisc 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

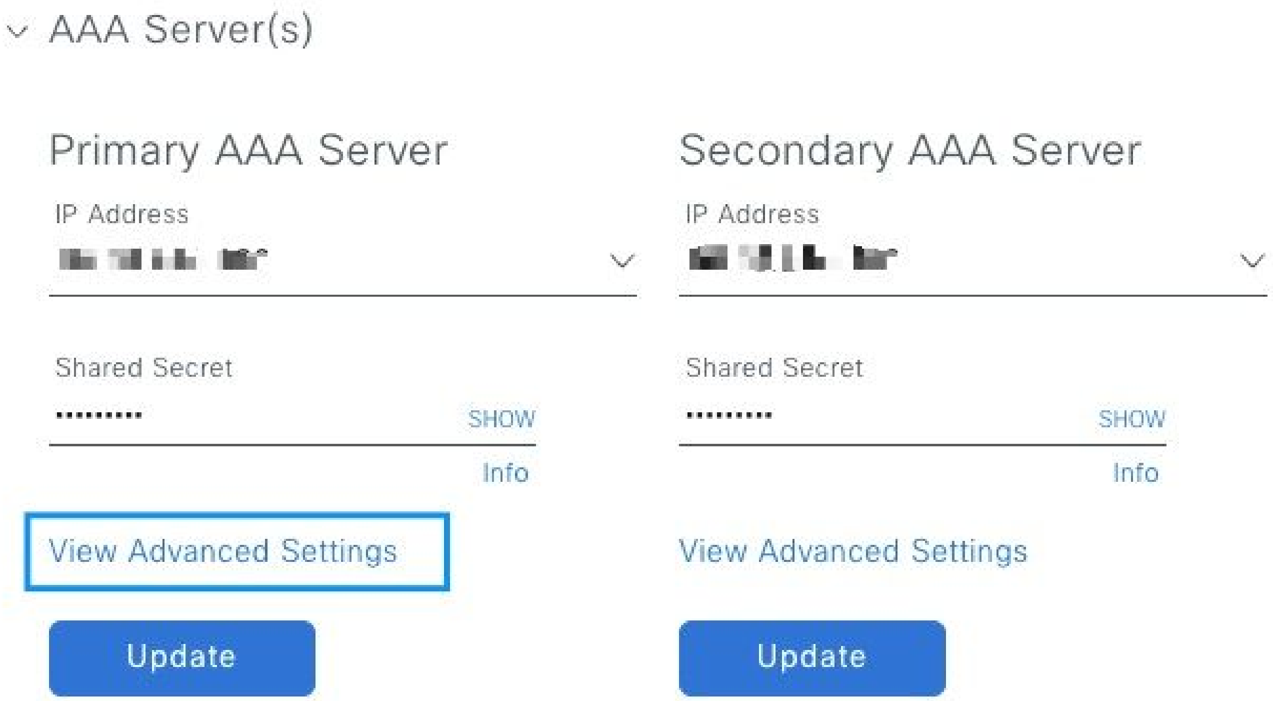
AAA Attribute

AAA Attribute: Cisco-AVPair

注意：ISE伺服器在後端使用Cisco-AVPair屬性，因此第3步中的配置有效。

向下滾動檢視AAA伺服器配置部分。在步驟1中配置ISE伺服器的IP地址，並在步驟3中配置共用金鑰。

然後按一下檢視高級設定。



AAA Server(s)

Primary AAA Server

IP Address
[redacted]

Shared Secret
•••••••••• SHOW

Info

View Advanced Settings

Update

Secondary AAA Server

IP Address
[redacted]

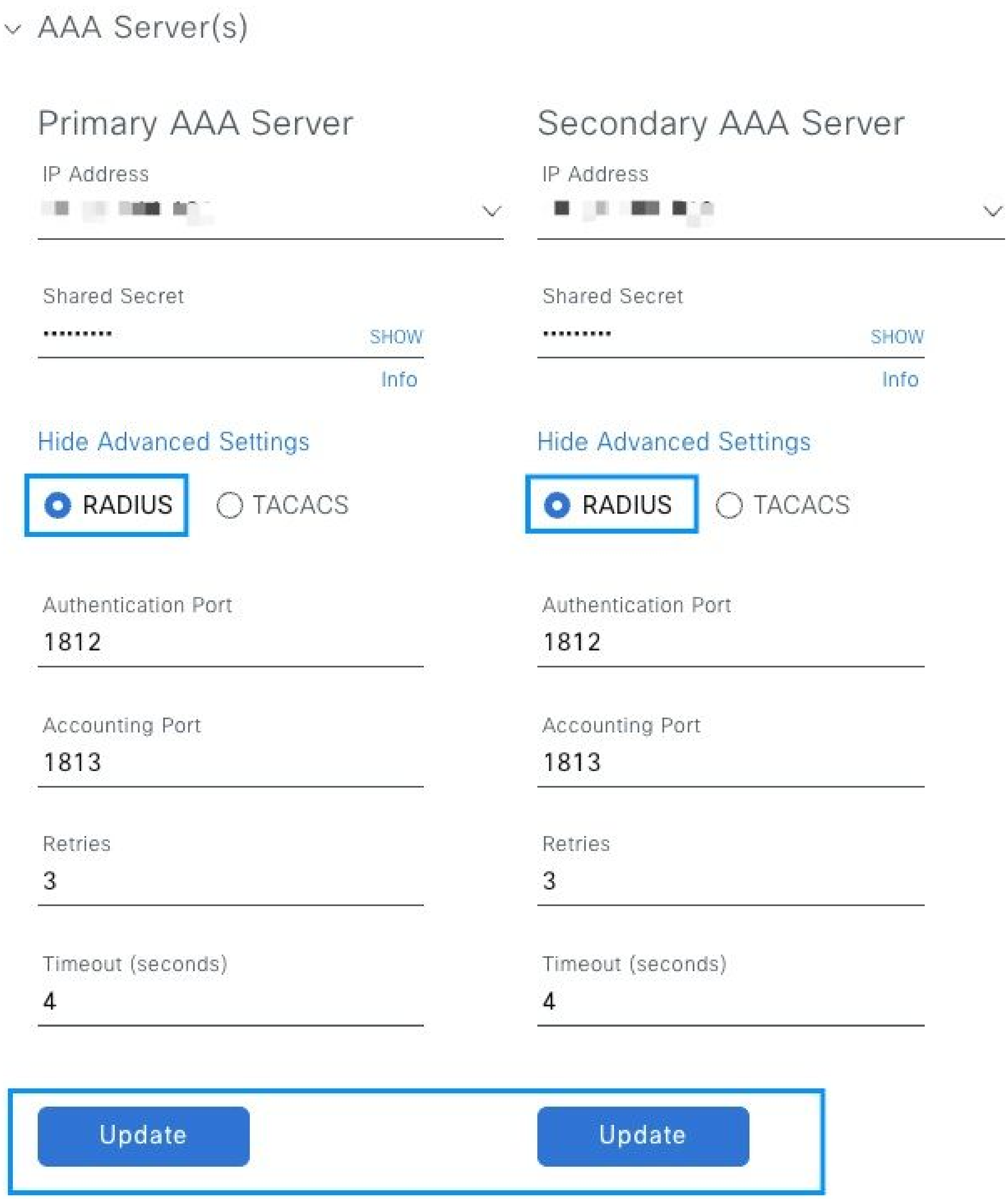
Shared Secret
•••••••••• SHOW

Info

View Advanced Settings

Update

確認已選取RADIUS選項，然後按一下兩個伺服器上的「更新」按鈕。



AAA Server(s)

Primary AAA Server

IP Address
[redacted]

Shared Secret
••••••••••

● RADIUS ○ TACACS

Authentication Port
1812

Accounting Port
1813

Retries
3

Timeout (seconds)
4

Secondary AAA Server

IP Address
[redacted]

Shared Secret
••••••••••

● RADIUS ○ TACACS

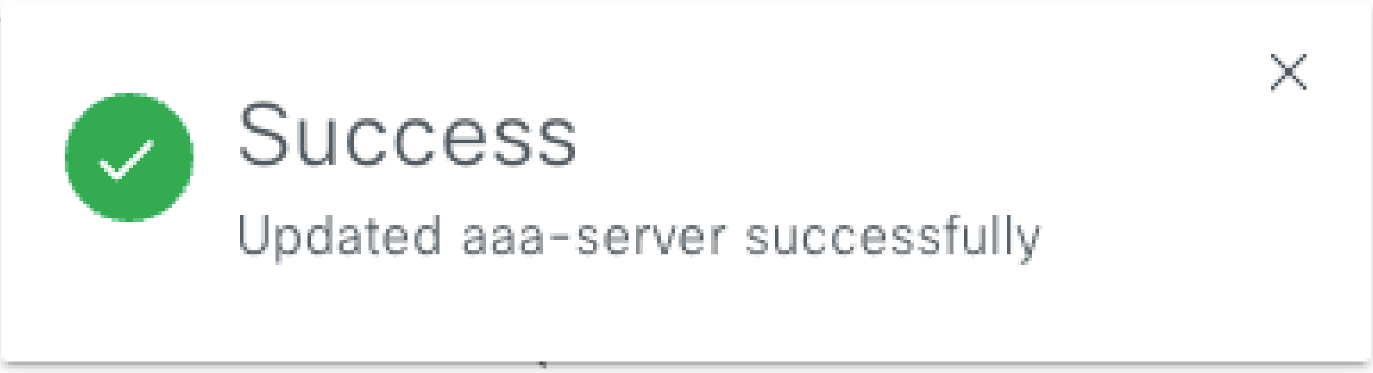
Authentication Port
1812

Accounting Port
1813

Retries
3

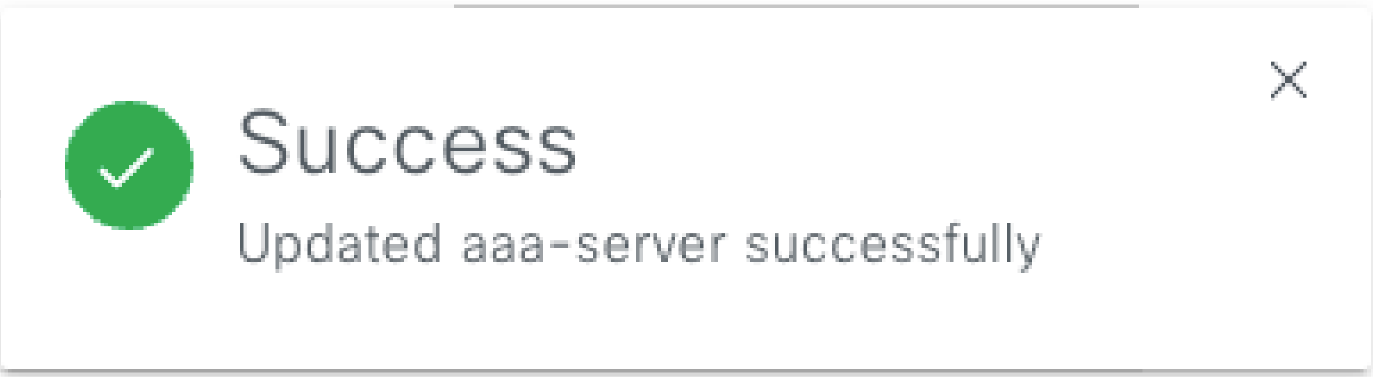
Timeout (seconds)
4

您必須看到每條成功消息。



Success

Updated aaa-server successfully

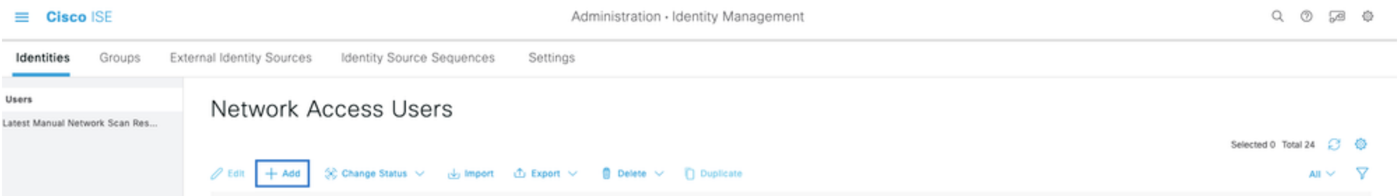


Success

Updated aaa-server successfully

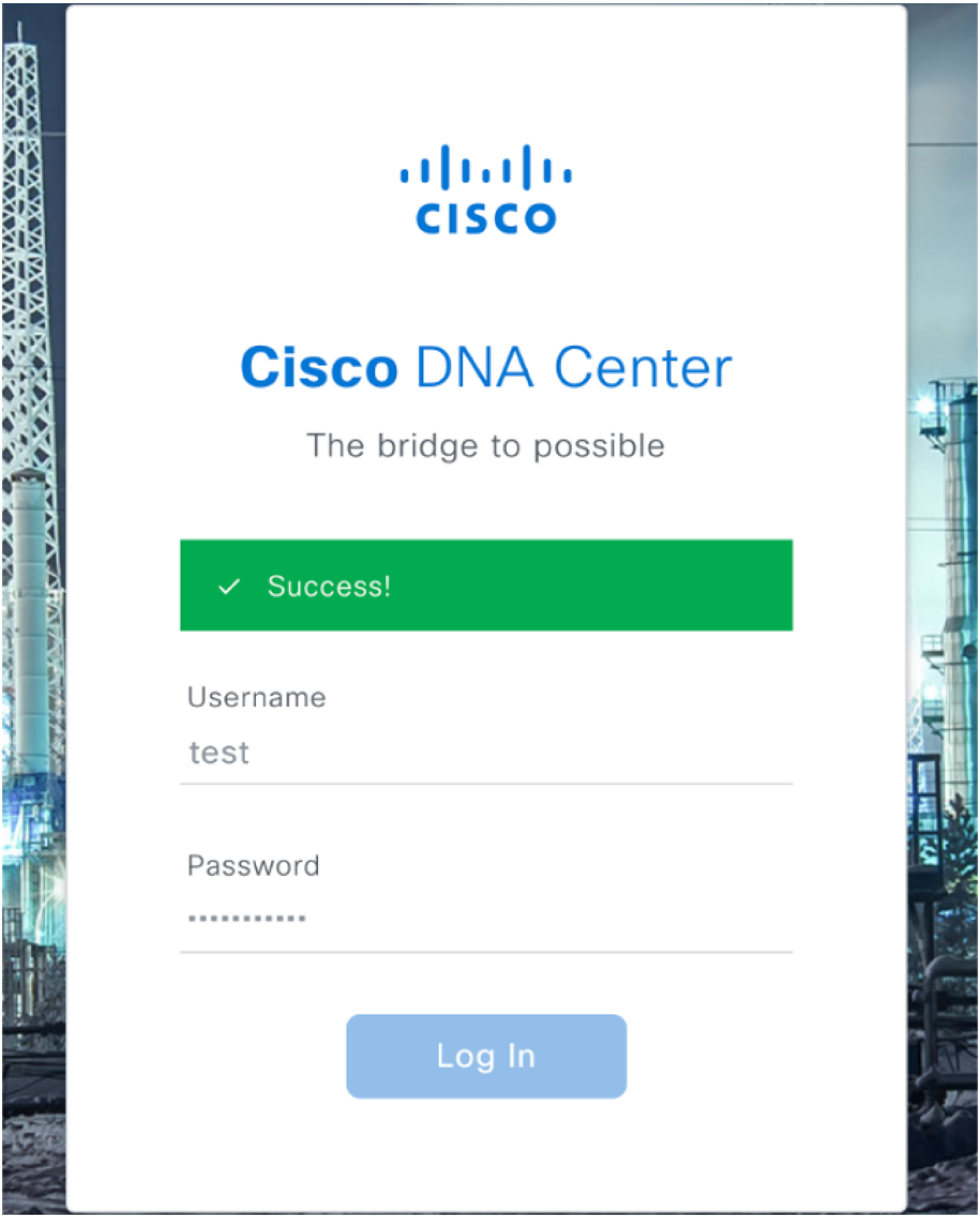
現在您可以使用在ISE選單>管理>身份管理>身份>使用者下建立的任何ISE身份登入。

如果沒有任何建立，請登入ISE，導航到上面的路徑，然後增加新的網路訪問使用者。



驗證

載入Cisco DNA Center GUI 和從ISE身份以使用者登入。



Cisco DNA Center

The bridge to possible

✓ Success!

Username

test

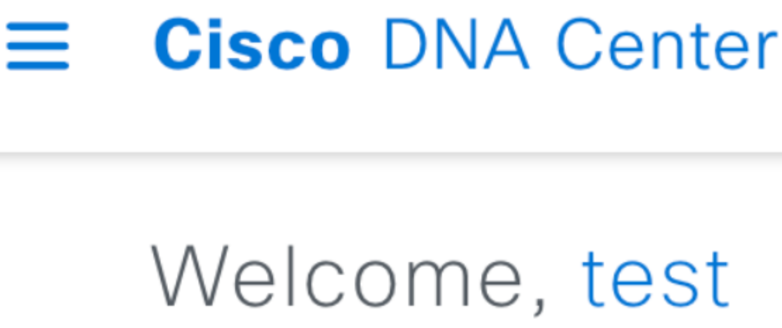
Password

••••••••••

DNA Center登入

注意：ISE標識上的任何使用者現在都可以登入。您可以為ISE伺服器上的身份驗證規則增加更精細的粒度。

登入成功後，使用者名稱顯示在Cisco DNA Center GUI上



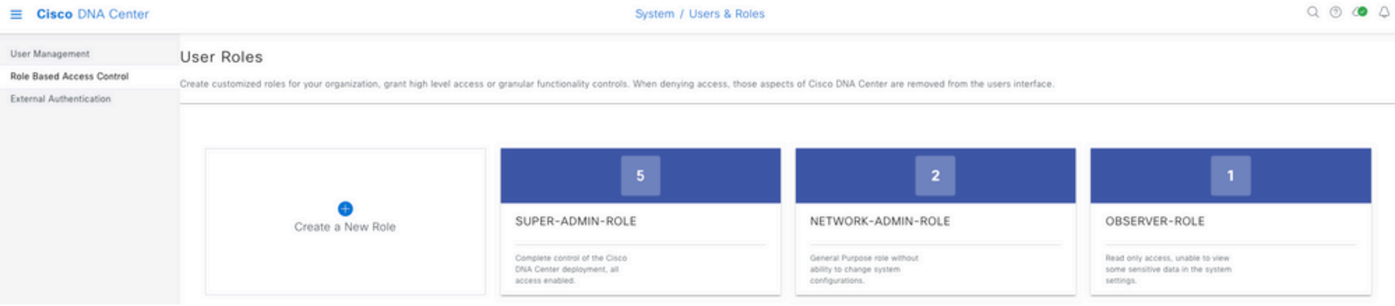
Cisco DNA Center

Welcome, test

歡迎畫面

更多角色

預設情況下，您可以對Cisco DNA Center上的每個角色重複這些步驟：SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE和OBSERVER-ROLE。



Cisco DNA Center

System / Users & Roles

User Management

Role Based Access Control

External Authentication

User Roles

Create customized roles for your organization, grant high level access or granular functionality controls. When denying access, those aspects of Cisco DNA Center are removed from the users interface.

Create a New Role

5

SUPER-ADMIN-ROLE

Complete control of the Cisco DNA Center deployment, all access enabled.

2

NETWORK-ADMIN-ROLE

General Purpose role without ability to change system configurations.

1

OBSERVER-ROLE

Read only access, unable to view some sensitive data in the system settings.

在本文檔中，我們使用SUPER-ADMIN-ROLE角色示例，但是，您可以在ISE上為思科DNA中心上的每個角色配置一個授權配置檔案，唯一的考慮是在步驟3上配置的角色需要與思科DNA中心上的角色名稱完全匹配（區分大小寫）。

關於此翻譯