

為9800 WLC上的GUI & CLI Auth配置RADIUS & TACACS+

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[唯讀使用者限制](#)

[為WLC配置RADIUS身份驗證](#)

[為RADIUS配置ISE](#)

[配置TACACS+ WLC](#)

[TACACS+ ISE配置](#)

[疑難排解](#)

[排除WLC GUI或透過WLC CLI訪問CLI RADIUS/TACACS+的故障](#)

[透過ISE GUI排除WLC GUI或CLITACACS+訪問故障](#)

簡介

本文說明如何配置Catalyst 9800進行RADIUS或TACACS+外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- Catalyst無線9800組態型號
- AAA、RADIUS和TACACS+概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C9800-CL v17.9.2
- ISE 3.2.0

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。

背景資訊

當使用者嘗試存取WLC的CLI或GUI時，系統會提示使用者輸入使用者名稱和密碼。預設情況下，這些憑證會與本地使用者資料庫（裝置本身就有）進行比較。或者，可以指示WLC將輸入憑據與遠端AAA伺服器進行比較：WLC可以使用RADIUS或TACACS+與伺服器通訊。

設定

在本示例中，在AAA伺服器(ISE)上配置了兩種型別的使用者，分別為adminuser和helpdeskuser。這些使用者分別是admin-group和helpdesk-group組的一部分。使用者adminuser是admin-group的一部分，應該被授予對WLC的完全訪問許可權。另一方面，helpdeskuser是helpdesk-group的一部分，用於僅向WLC授予監控許可權。因此，沒有配置訪問許可權。

本文首先配置WLC和ISE進行RADIUS身份驗證，然後對TACACS+執行相同操作。

唯讀使用者限制

使用TACACS+或RADIUS進行9800 WebUI驗證時，存在以下限制：

- 許可權級別為0的使用者存在，但無權訪問GUI
- 許可權級別為1-14的使用者只能檢視Monitor頁籤（這相當於本地身份驗證的只讀使用者的許可權級別）
- 許可權級別為15的使用者具有完全訪問許可權
- 不支援許可權等級為15的使用者，以及僅允許特定命令的命令集。使用者仍可透過WebUI執行組態變更

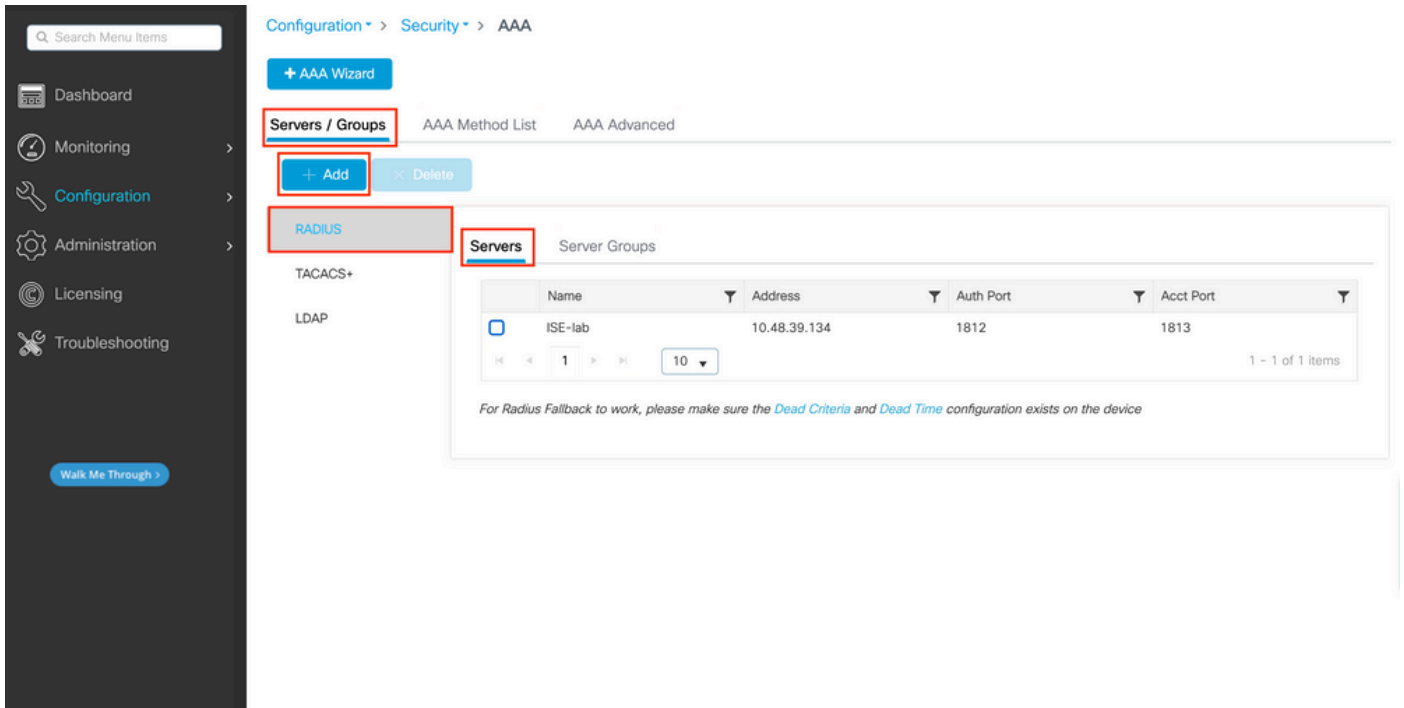
這些考量無法變更或修改。

為WLC配置RADIUS身份驗證

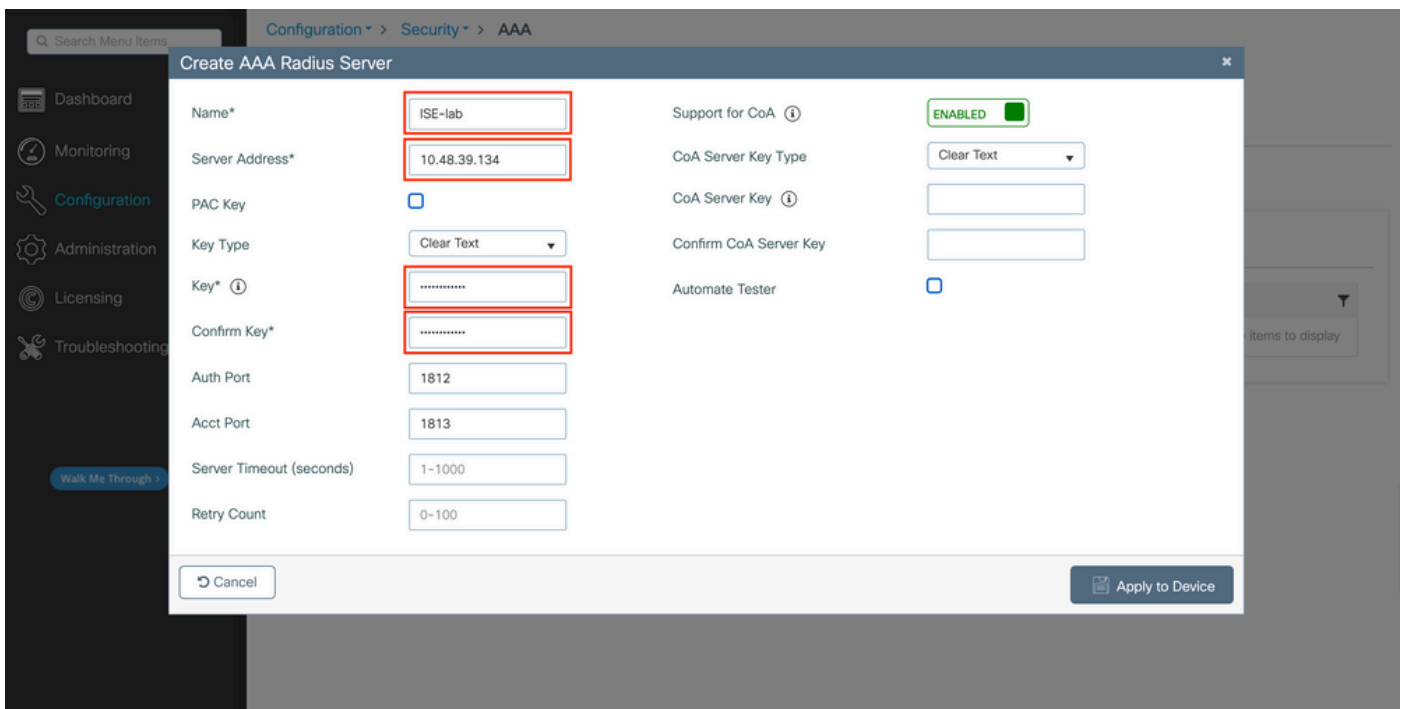
步驟 1.宣告RADIUS伺服器。

在 GUI 上：

首先，在WLC上建立ISE RADIUS伺服器。這可以在<https://<WLC-IP>/webui/#/aaa>中訪問的GUI WLC頁面的Servers/Groups > RADIUS > Servers頁籤中完成，或者導航到Configuration > Security > AAA([Webex](#)或[Webex](#))進行（如圖所示）。



要在WLC上增加RADIUS伺服器，請按一下映像中以紅色框住的「增加」按鈕。這會開啟螢幕擷取畫面中描繪的躍現式視窗。



在此彈出窗口中，必須提供：

- 伺服器名稱（請注意，它不必與ISE系統名稱匹配）
- 伺服器IP地址
- WLC和RADIUS伺服器之間的共用金鑰

可以配置其他引數，例如用於身份驗證和記帳的埠，但這些引數不是必需的，保留為本文檔的預設設定。

在 CLI 上：

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-lab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

步驟 2.將RADIUS伺服器對映到伺服器組。

在 GUI 上：

如果有多個可用於身份驗證的RADIUS伺服器，建議將所有這些伺服器對映到同一個伺服器組。WLC負責對伺服器組中伺服器之間的不同身份驗證進行負載均衡。RADIUS伺服器組在與步驟1.中所提到的GUI頁面的Servers/Groups > RADIUS > Server Groups頁籤上配置，如圖所示。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

TACACS+

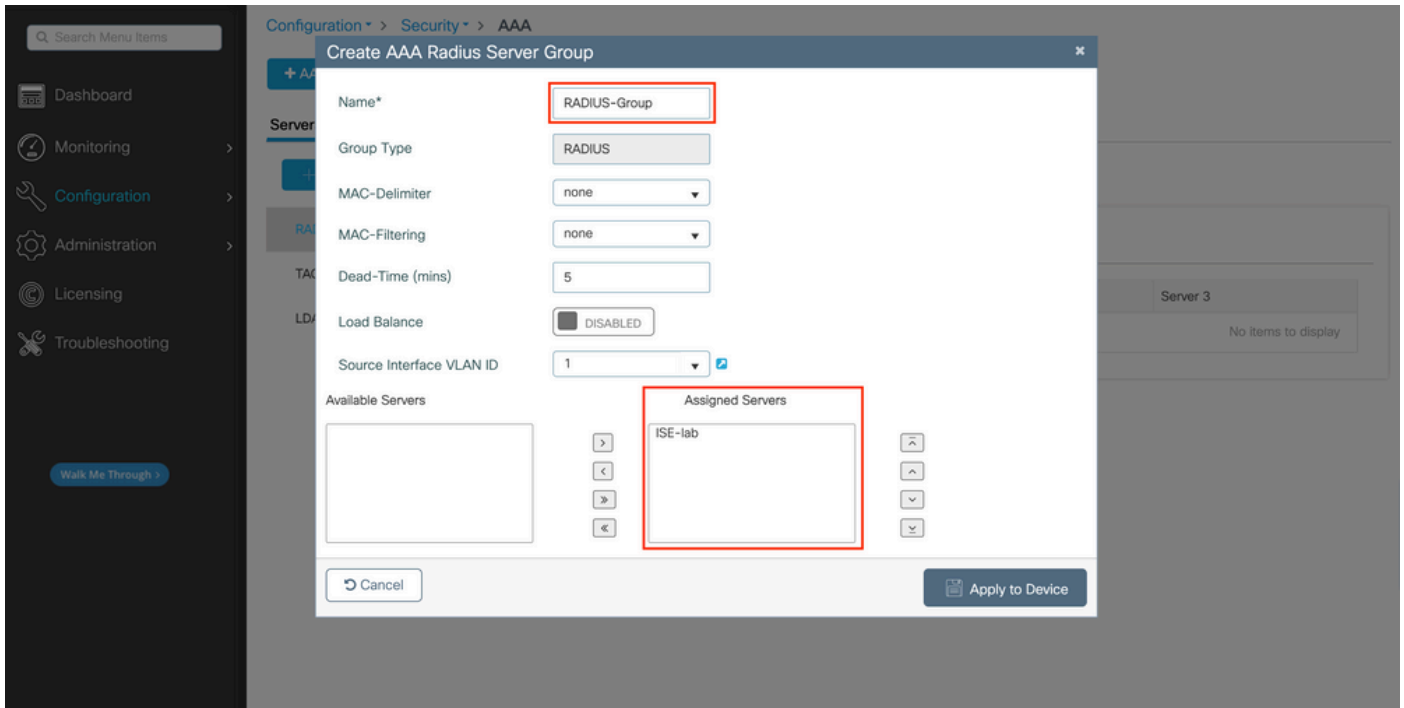
LDAP

Servers Server Groups

Name	Server 1	Server 2	Server 3
<input type="checkbox"/> RADIUS-Group	ISE-lab	N/A	N/A

1 - 1 of 1 items

至於伺服器的建立，當您按一下「新增」(Add)按鈕時，會出現一個躍現式視窗（上一個影像中的架構），如下圖所示。



在彈出窗口中，為組提供一個名稱，並將所需的伺服器移到Assigned Servers清單中。

在 CLI 上：

```
.  
.  
.  
_<#root>
```

```
WLC-9800(config)# aaa group server radius
```

```
.  
.  
.  
RADIUS-Group
```

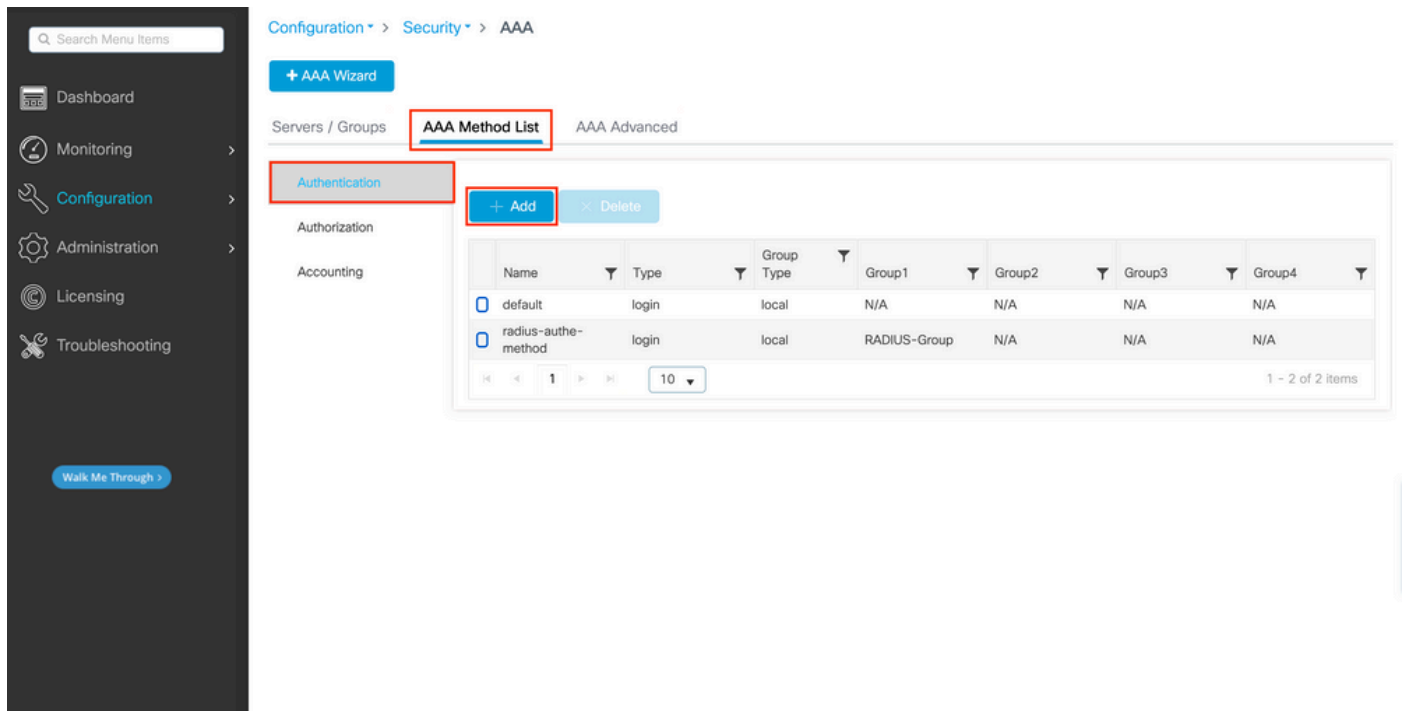
```
.  
.  
.  
WLC-9800(config-sg-radius)# server name
```

```
.  
.  
.  
ISE-lab  
.
```

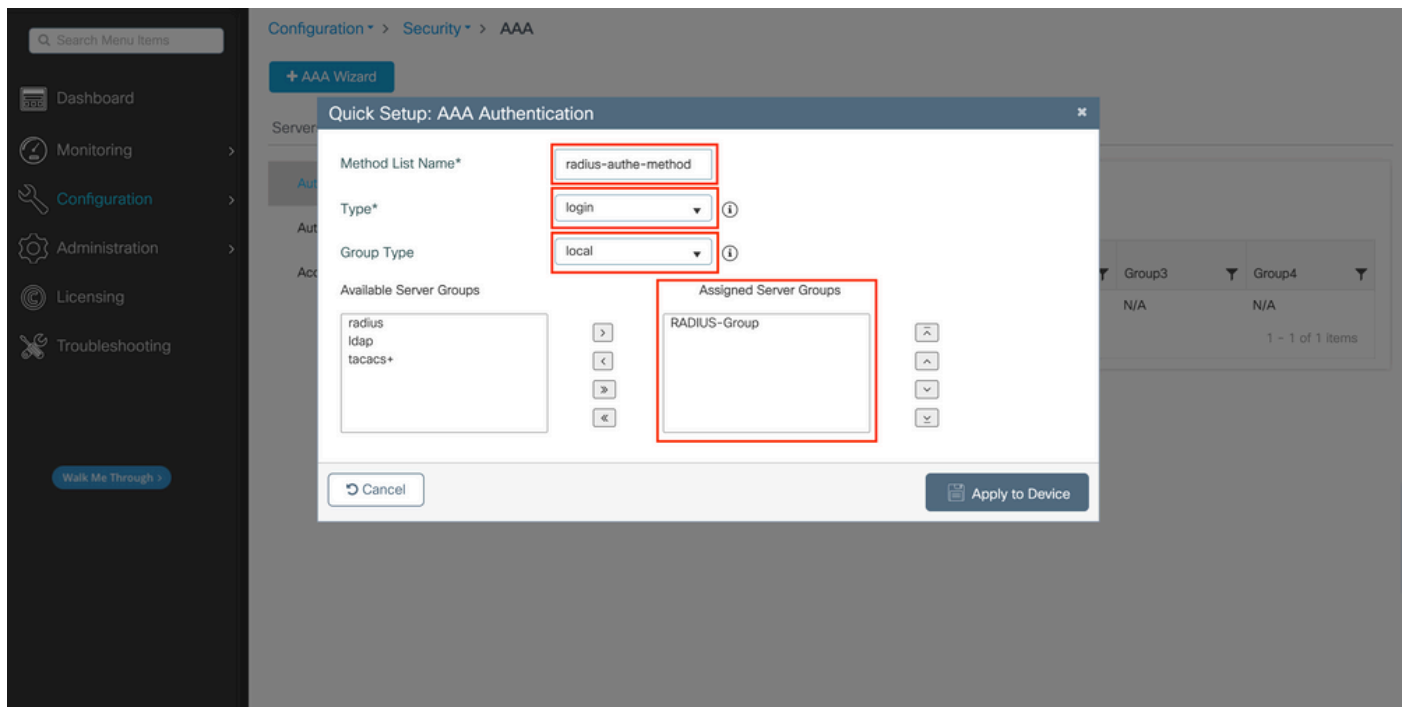
步驟 3. 建立指向RADIUS伺服器組的AAA身份驗證登入方法。

在 GUI 上：

仍在GUI頁面<https://<WLC-IP>/webui/#/aaa>中，導覽至AAA Method List > Authentication索引標籤，然後建立驗證方法，如下圖所示。



通常，當您使用「增加」按鈕建立身份驗證方法時，會出現配置彈出窗口，類似於本圖中所示的窗口。



在此彈出窗口中，提供方法的名稱。選擇Type作為登入，並且將在上一步中建立的組伺服器增加到Assigned Server Groups清單中。對於Group Type欄位，可以進行若干配置。

- 如果您選擇「群組型別」作為「本機」，WLC會先檢查使用者身份證明是否在本機存在，然後回到伺服器群組。

- 如果您選擇「群組型別」作為群組且未核取「轉至本機」選項，WLC只會檢查伺服器群組的使用者認證。
- 如果選擇組型別作為組並選中回退到本地選項，則WLC將根據伺服器組檢查使用者憑據，並且僅當伺服器未響應時才查詢本地資料庫。如果伺服器傳送拒絕訊息，則使用者必須經過驗證，即使該使用者可以存在於本機資料庫上。

在 CLI 上：

如果您希望只有在本機找不到使用者身份證明時，才使用伺服器群組來檢查使用者身份證明，請使用：

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

```
local group
```

```
RADIUS-Group
```

如果您希望僅對伺服器群組檢查使用者身份證明，請使用：

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
radius-auth-method
```

group

RADIUS-Group

如果您想要使用伺服器群組檢查使用者身份證明，而且如果最後未使用本機專案回應，請使用：

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

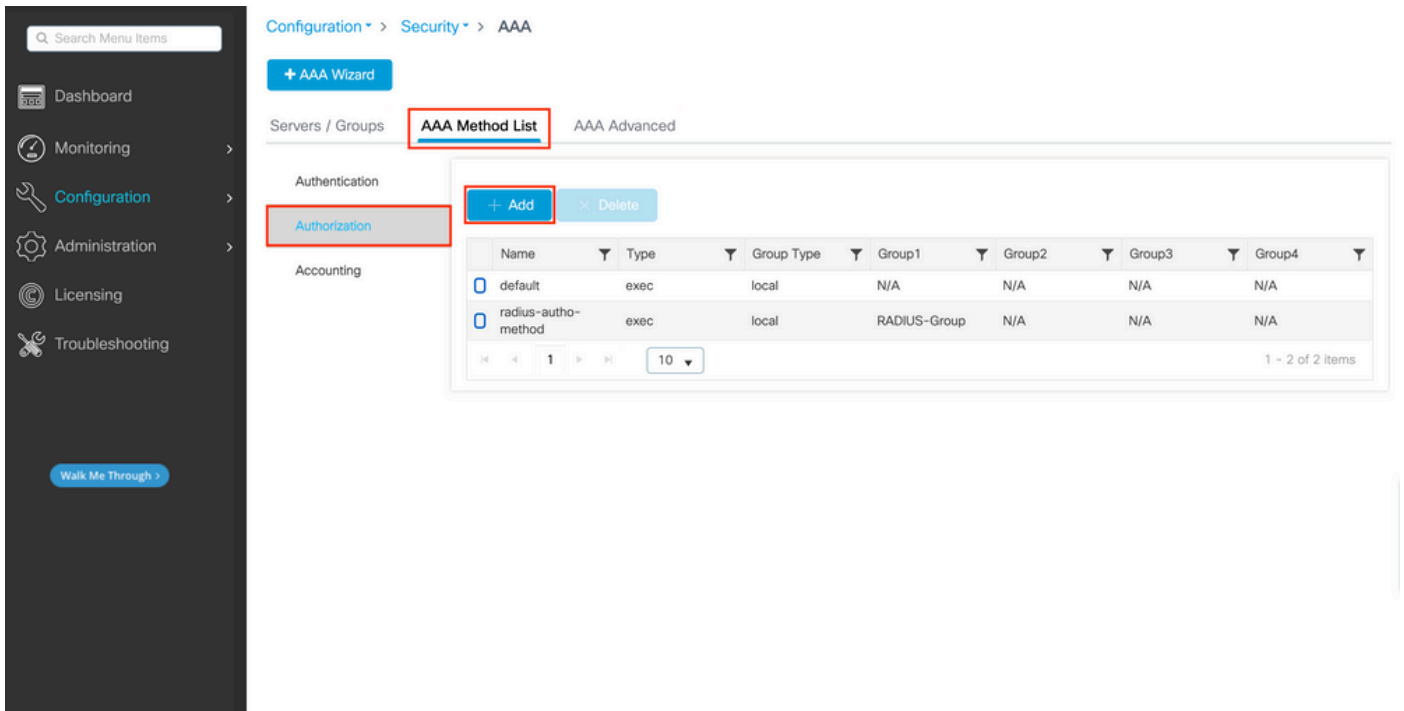
local

在此示例設定中，有些使用者僅在本機建立，而有些使用者僅在ISE伺服器上，因此，使用第一個選項。

步驟 4. 建立指向RADIUS伺服器組的AAA授權exec方法。

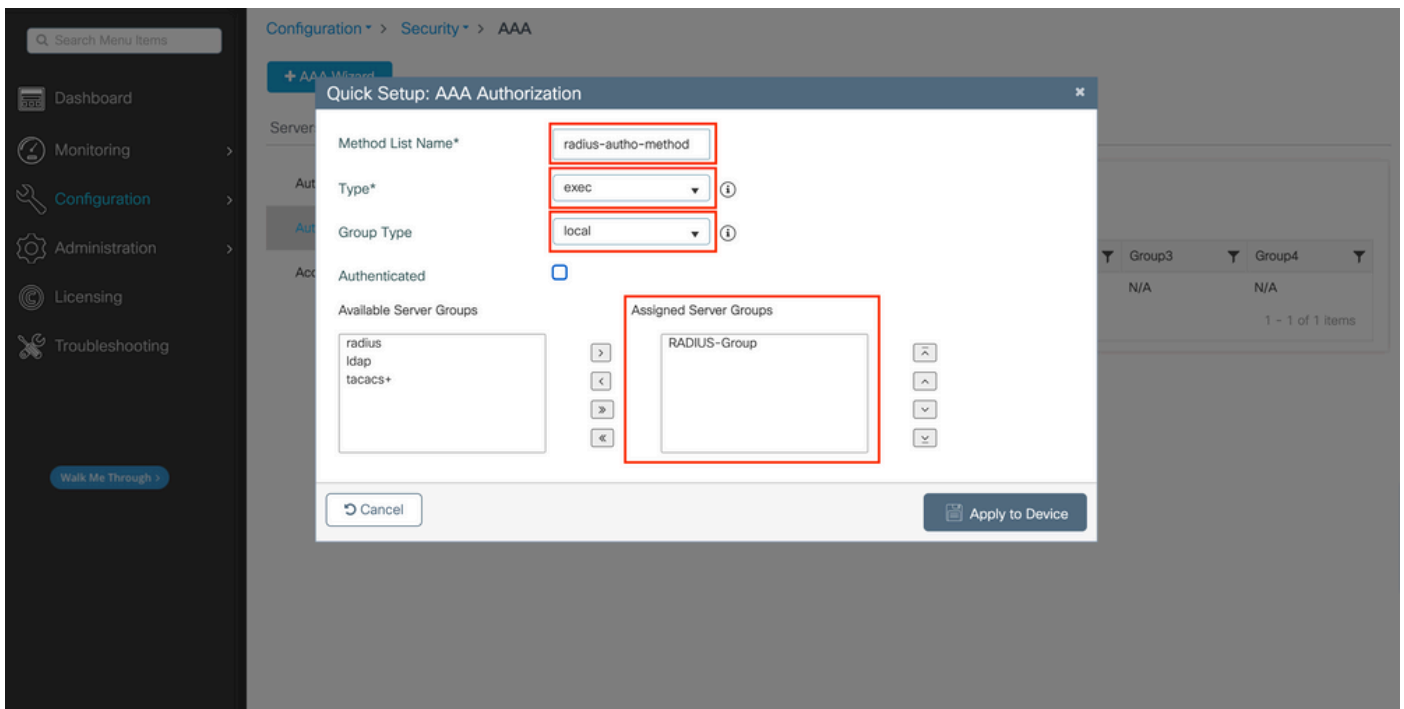
在 GUI 上：

使用者還必須獲得授權才能獲得訪問許可權。仍在GUI Page Configuration > Security > AAA頁籤中，導航到AAA Method List > Authorization頁籤，然後建立授權方法（如圖所示）。



授權方法建立

當您使用Add按鈕增加新授權方法時，會出現與所描述配置類似的授權方法配置彈出窗口。



在此配置彈出窗口中，為授權方法提供一個名稱，選擇Type作為exec，並使用Group Type與步驟3中用於身份驗證方法的順序相同的順序。

在 CLI 上：

對於身份驗證方法，首先分配授權以根據本地條目檢查使用者，然後根據伺服器組中的條目檢查使用者。

<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

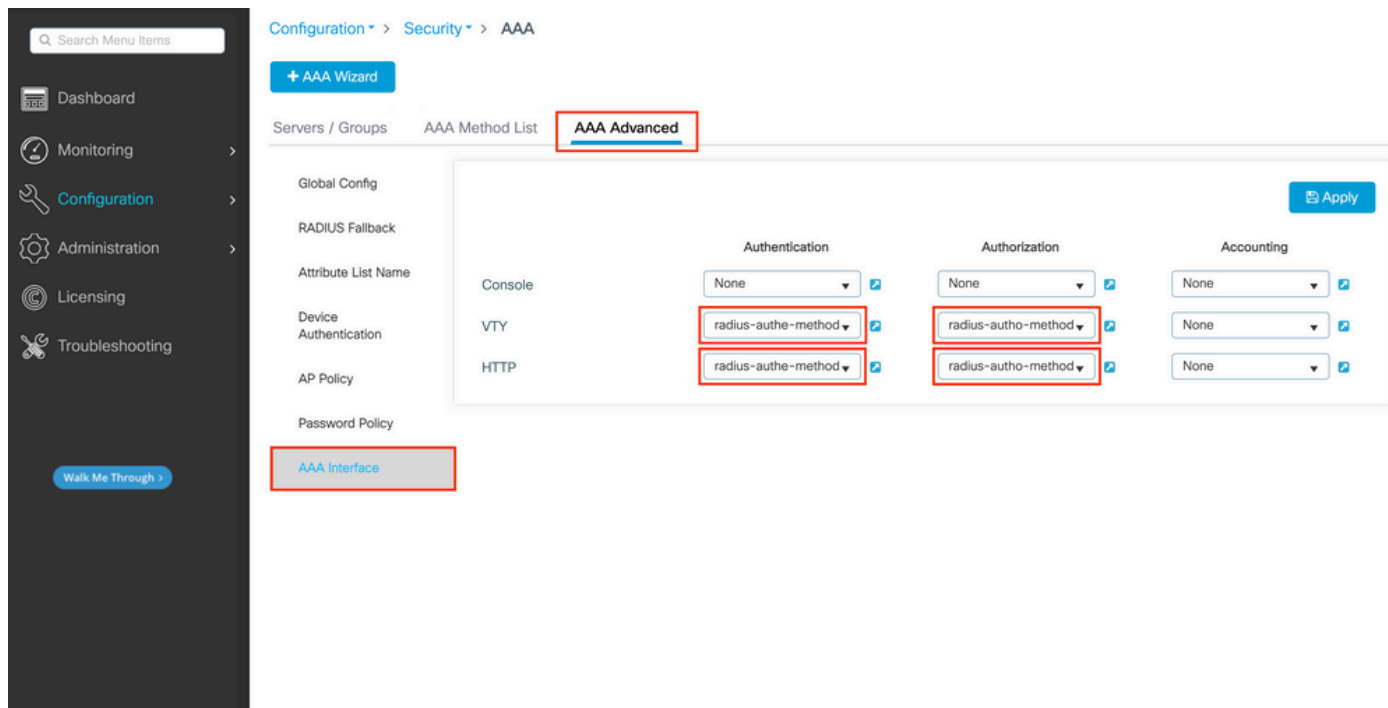
local group

RADIUS-Group

步驟 5.將方法分配給HTTP配置和用於Telnet/SSH的VTY線路。

在 GUI 上：

建立的身份驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連線，您可以從AAA Advanced > AAA Interface頁籤上的GUI WLC頁進行配置(可透過<https://<WLC-IP>/webui/#/aaa>訪問)，如下圖所示：



用於GUI身份驗證的CLI：

<#root>

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

```
radius-auth-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

```
radius-auth-method
```

用於Telnet/SSH身份驗證的CLI：

```
<#root>
```

```
WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication
```

```
radius-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
radius-auth-method
```

請注意，當對HTTP配置執行更改時，最好重新啟動HTTP和HTTPS服務。這可以透過以下命令來實現：

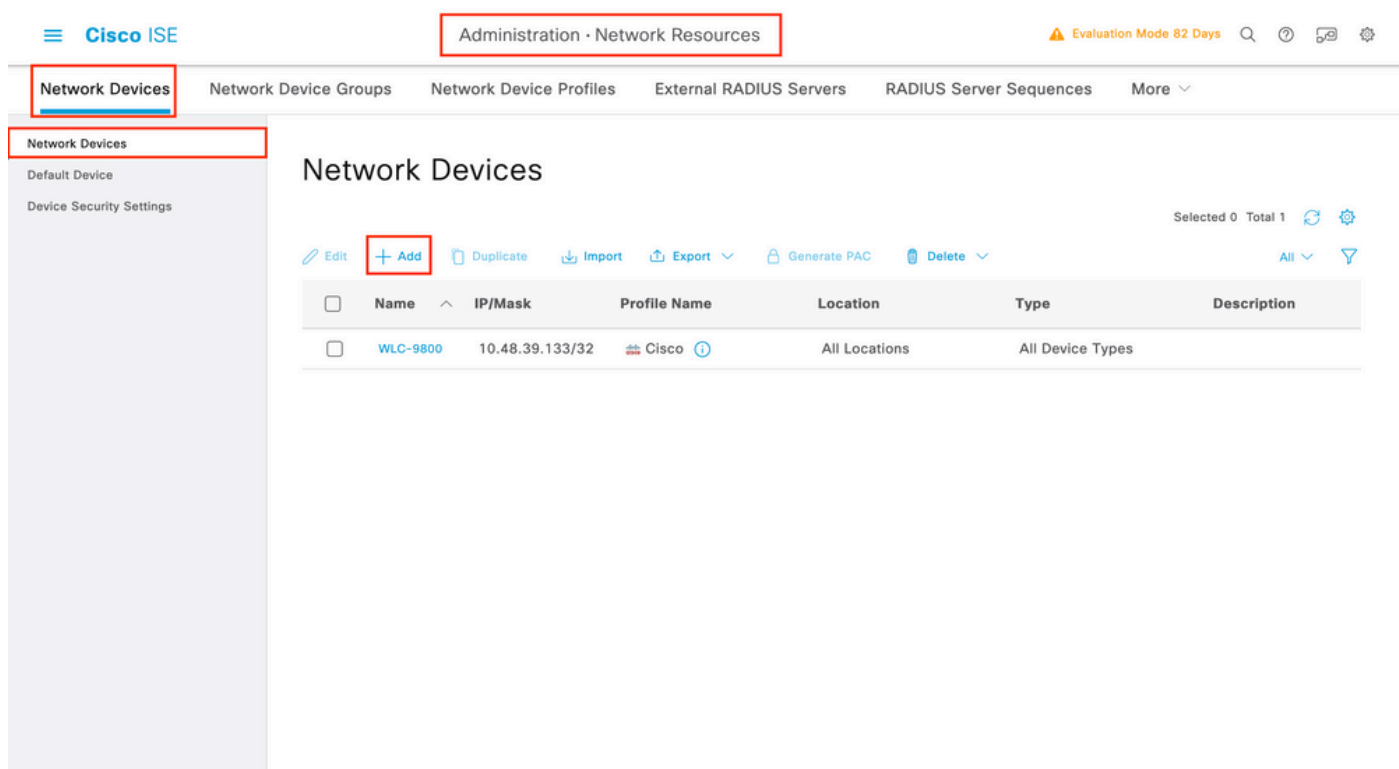
```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

為RADIUS配置ISE

步驟 1.將WLC配置為RADIUS的網路裝置。

在 GUI 上：

要將上一部分中使用的WLC宣告為ISE中RADIUS的網路裝置，請導航到Administration > Network Resources > Network Devices並打開Network devices頁籤，如下圖所示。



要增加網路裝置，請使用Add按鈕，該按鈕將打開新的網路裝置配置表單。

Network Devices List > New Network Device

Network Devices

Name **WLC-9800**

Description

IP Address * IP: **10.48.39.133 / 32**

Device Profile **Cisco**

Model Name

Software Version

Network Device Group

Location **All Locations** [Set To Default](#)

IPSEC **Is IPSEC Device** [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 [?](#)

Second Shared Secret [Show](#)

CoA Port **1700** [Set To Default](#)

RADIUS DTLS Settings [?](#)

DTLS Required [?](#)

Shared Secret **radius/dtls** [?](#)

在新窗口中，為網路裝置提供一個名稱，並增加其IP地址。選擇RADIUS身份驗證設定並配置與WLC上使用的RADIUS共用金鑰相同的RADIUS共用金鑰。

步驟 2. 建立授權結果以返回許可權。

在 GUI 上：

要具有管理員訪問許可權，adminuser需要具有15級的特權，它允許訪問exec提示符shell。另一方面，helpdeskuser不需要exec提示符訪問，因此可以為它分配低於15的特權級別。為了將適當的許可權級別分配給使用者，可以使用授權配置檔案。這些可以從ISE GUI Page Policy > Policy Elements > Results頁籤下配置，下圖顯示了Authorization > Authorization Profiles。

- Dictionarys
- Conditions
- Results**
- Authentication
- Authorization
- Authorization Profiles**
- Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All [Filter](#)

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	9800-admin-priv	Cisco	
<input type="checkbox"/>	9800-helpdesk-priv	Cisco	
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure th
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess	Cisco	Default Profile with access type as Access-Reject

要配置新的授權配置檔案，請使用Add按鈕，打開新的授權配置檔案配置表。要配置分配給adminuser的配置檔案，此表單尤其必須如下所示。

Dictionarys Conditions **Results**

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name 9800-admin-priv

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

Advanced Attributes Settings

⋮ Cisco:cisco-av-pair = shell:priv-lvl=15

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:priv-lvl=15

Submit Cancel

配置顯示將許可權級別15授予與其關聯的任何使用者。如前所述，這是下一步建立的adminuser的預期行為。但是，helpdeskuser必須具有較低的許可權級別，因此必須建立第二個策略元素。

helpdeskuser的策略元素類似於上面建立的策略元素，不同之處在於字串shell:priv-lvl=15 須更改為shell:priv-lvl=X，然後將X替換為所需的許可權級別。在本例中，使用1。

步驟 3. 在ISE上建立使用者組。

在 GUI 上：

Administration > Identity Management > Groups GUI Page ISE使用者組是從的使用者身份組頁籤（如螢幕截圖所示）中建立的。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is "Administration > Identity Management". The "Groups" tab is selected. On the left, the "User Identity Groups" folder is highlighted in red. The main area displays a table of existing groups:

Name	Description
helpdesk-group	This is the group containing all users with read-only privileges.
admin-group	This is the group containing all users with administrator privileges.
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
GuestType_Weekly (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_Contractor (default)	Identity group mirroring the guest type
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
Employee	Default Employee User Group
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

The "+ Add" button is highlighted in red.

要建立新使用者，請使用「增加」按鈕，該按鈕將打開新的使用者身份組配置表單，如下所示。

The screenshot shows the "New User Identity Group" configuration form. The breadcrumb navigation is "User Identity Groups > New User Identity Group". The "Name" field is highlighted in red and contains the text "admin-group". The "Description" field contains the text "This is the group containing all users with administrator privileges." The "Submit" and "Cancel" buttons are visible at the bottom.

提供所建立群組的名稱。建立上面討論的兩個使用者組，即admin-group 和helpdesk-group。

步驟 4. 在ISE上建立使用者。

在 GUI 上：

ISE使用者透過Administration > Identity Management > Identities GUI Page的使用者頁籤建立，如螢幕截圖所示。

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit **+ Add** Change Status Import Export Delete Duplicate

All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled	adminuser				admin-group	
<input type="checkbox"/>	Enabled	helpdeskus...				helpdesk-group	

要建立新使用者，請使用Add按鈕打開新的網路訪問使用者配置表單，如下所示。

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username **adminuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in 60 days

Never Expires

Password Re-Enter Password

* Login Password

Generate Password

Enable Password

Generate Password

User Information

Account Options

Account Disable Policy

User Groups

admin-group

向使用者提供憑證，即使用者名稱和密碼，用於在WLC上進行驗證。並且，確保使用者的狀態為Enabled。最後，將使用者增加到其相關組(已在步驟4.中建立)，表單末尾的User Groups下拉選單。

建立上面討論的兩個使用者，即adminuser和helpdeskuser。

步驟 5.驗證使用者。

在 GUI 上：

在此場景中，已預配置的ISE預設策略集的身份驗證策略允許預設網路訪問。此策略集可從ISE GUI頁面的Policy > Policy Sets檢視，如下圖所示。因此，沒有必要對其進行更改。

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

步驟 6. 授權使用者。

在 GUI 上：

登入嘗試透過身份驗證策略後，需要授權該策略，並且ISE需要返回之前建立的授權配置檔案（允許接受，以及許可權級別）。

在本示例中，登入嘗試是根據裝置IP地址（即WLC IP地址）過濾的，並根據使用者所屬的組區分要授予的許可權級別。另一個有效的方法是根據使用者的使用者名稱過濾使用者，因為在本示例中，每個組只包含一個使用者。

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	9800 Helpdesk Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙️
✓	9800 Admin Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙️

> Authorization Policy (12)

Reset

Save

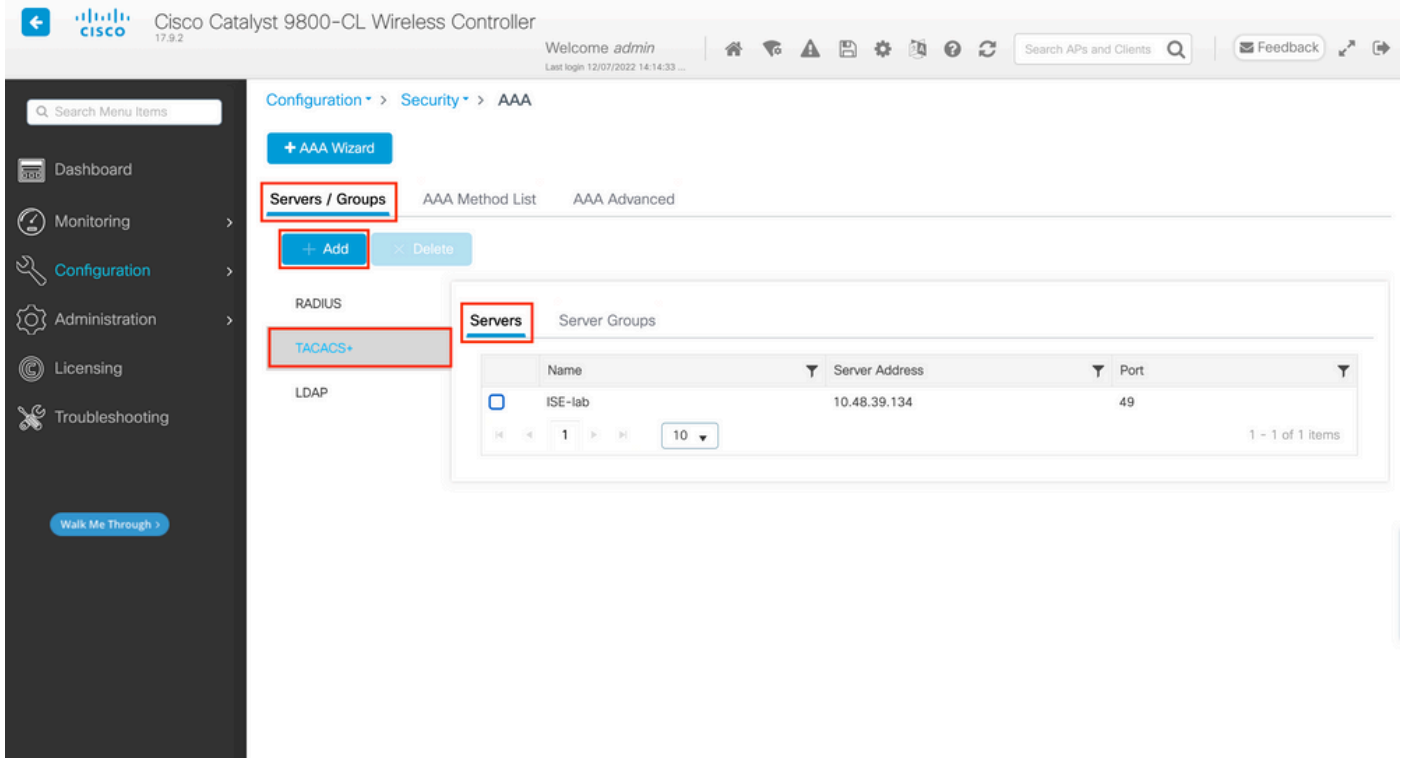
完成此步驟後，為adminuser 和helpdesk使用者配置的憑據可用於透過GUI或Telnet/SSH在WLC中進行身份驗證。

配置TACACS+ WLC

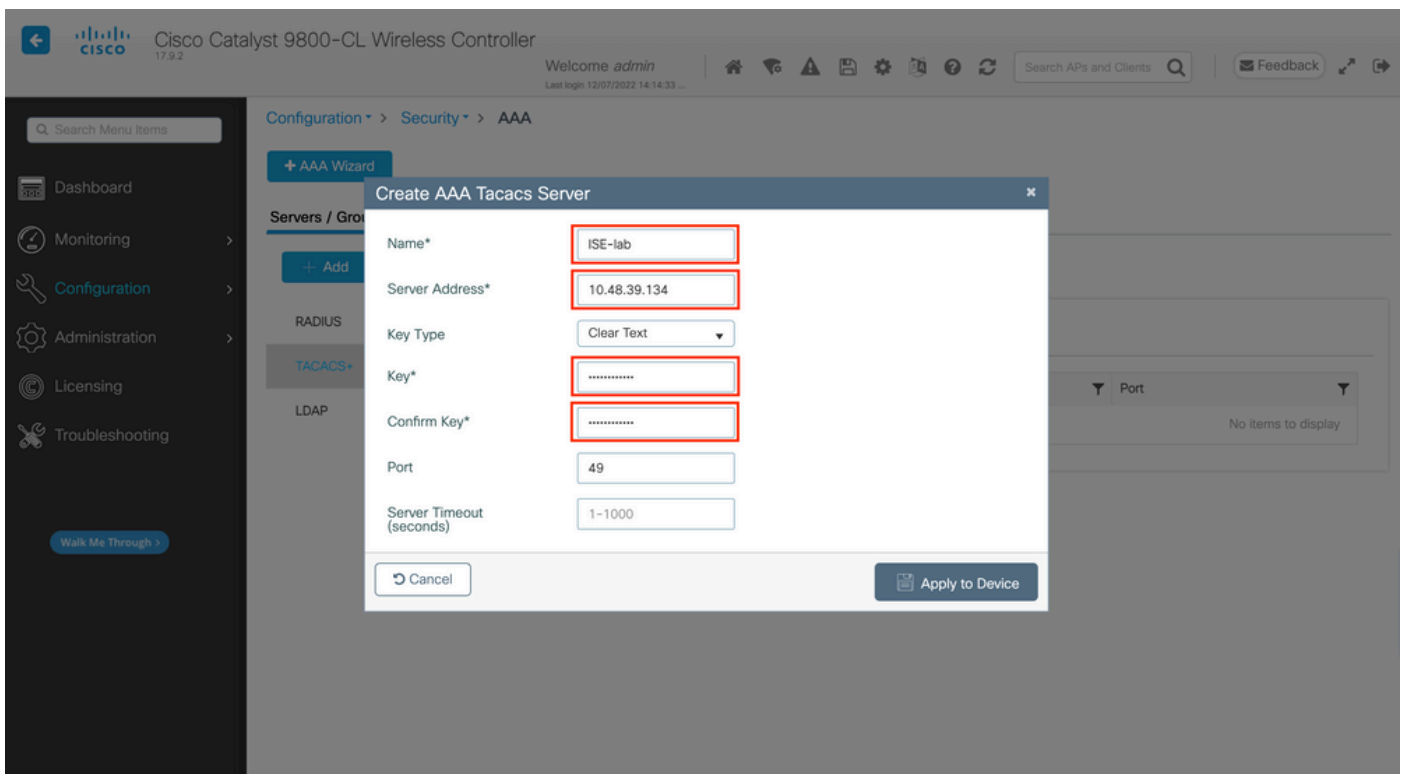
步驟 1.宣告TACACS+伺服器。

在 GUI 上：

首先，在WLC上建立Tacacs+伺服器ISE。可以在<https://<WLC-IP>/webui/#/aaa>中的GUI WLC頁面上的頁籤Servers/Groups > TACACS+ > Servers中執行此操作，或者在導航到Configuration > Security > AAA時執行此操作，如下圖所示。



要在WLC上增加TACACS伺服器，請按一下上圖中以紅色框住的「增加」按鈕。這樣會開啟描繪的躍現式視窗。



當彈出窗口打開時，提供伺服器名稱（它不必與ISE系統名稱匹配）、其IP地址、共用金鑰、使用的埠和超時。

在此彈出窗口中，必須提供：

- 伺服器名稱（請注意，它不必與ISE系統名稱匹配）
-

伺服器IP地址

- WLC和TACACS+伺服器之間的共用金鑰

可以配置其他引數，例如用於身份驗證和記賬的埠，但這些不是必需的，保留為本文檔的預設設定。

在 CLI 上：

```
<#root>
```

```
WLC-9800(config)#tacacs server
```

```
ISE-lab
```

```
WLC-9800(config-server-tacacs)#address ipv4
```

```
10.48.39.134
```

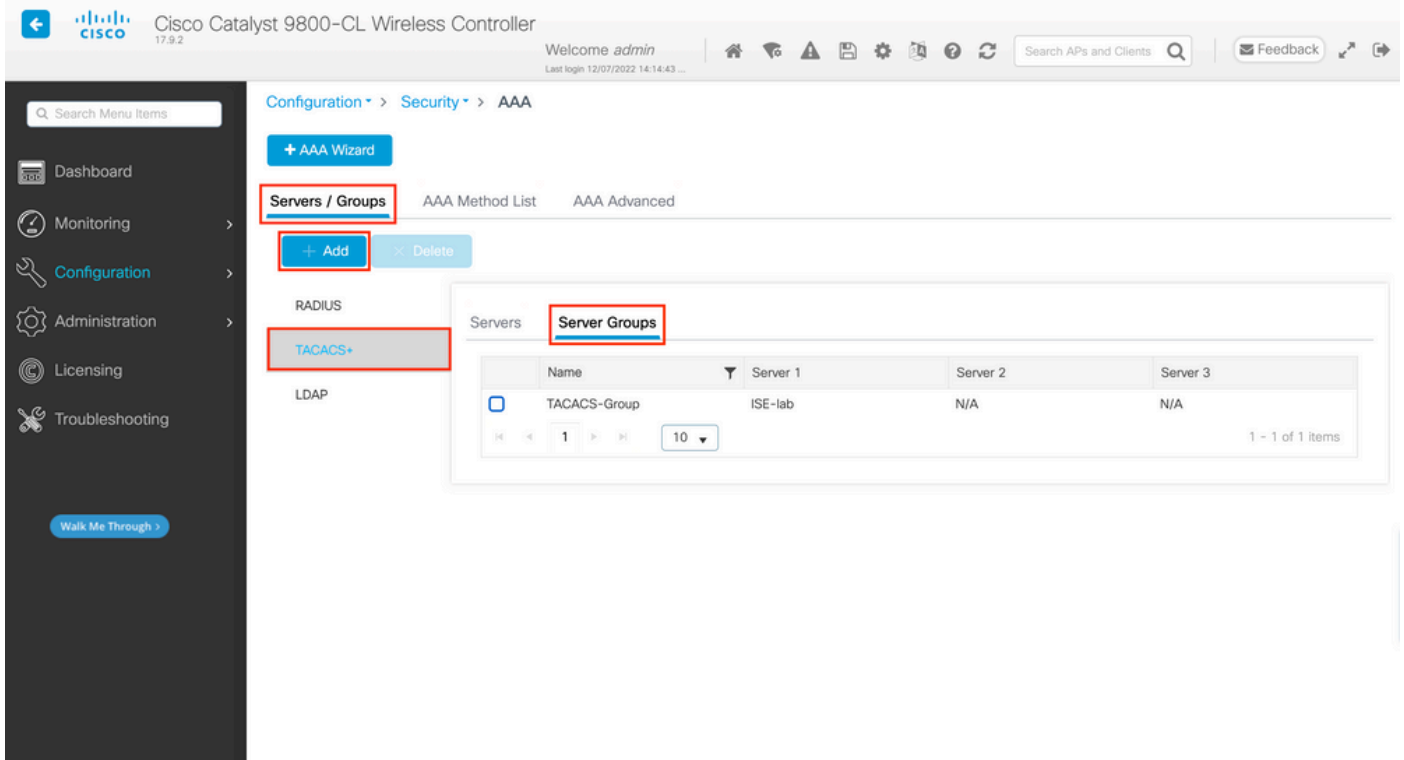
```
WLC-9800(config-server-tacacs)#key
```

```
Cisco123
```

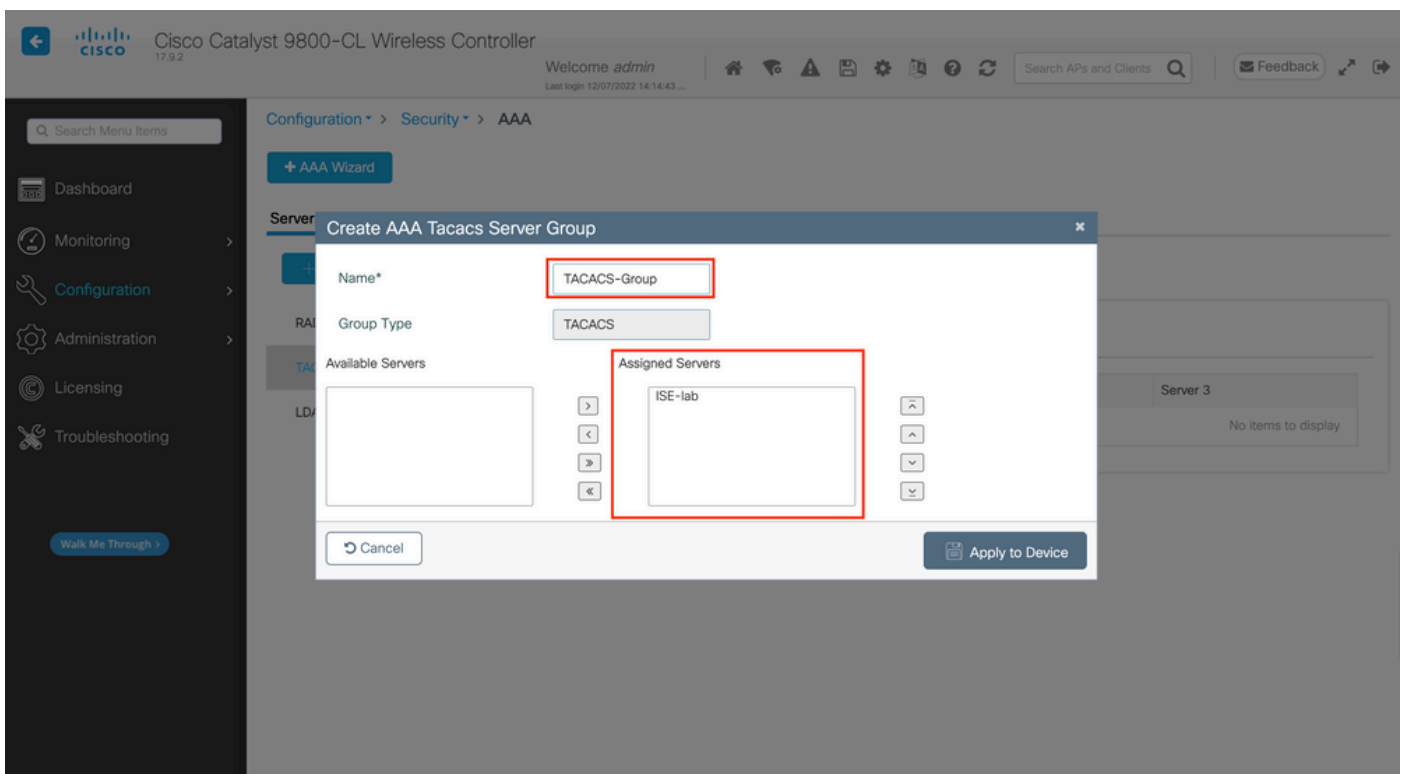
步驟 2.將TACACS+伺服器對映到伺服器組。

在 GUI 上：

如果您有多個可用於驗證的TACACS+伺服器，建議將這些伺服器對應到同一個伺服器群組。然後，WLC會處理伺服器群組中伺服器之間不同驗證作業的負載平衡。TACACS+伺服器組是在第1步中提及的相同GUI頁面的Servers/Groups > TACACS > Server Groups頁籤上配置的，如下圖所示。



至於伺服器的建立，當您按一下先前影像（如該影像所示）中的「新增」按鈕架構時，會出現一個躍現式視窗。



在彈出窗口中，為組指定名稱，並將所需伺服器移至Assigned Servers清單。

在 CLI 上：

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

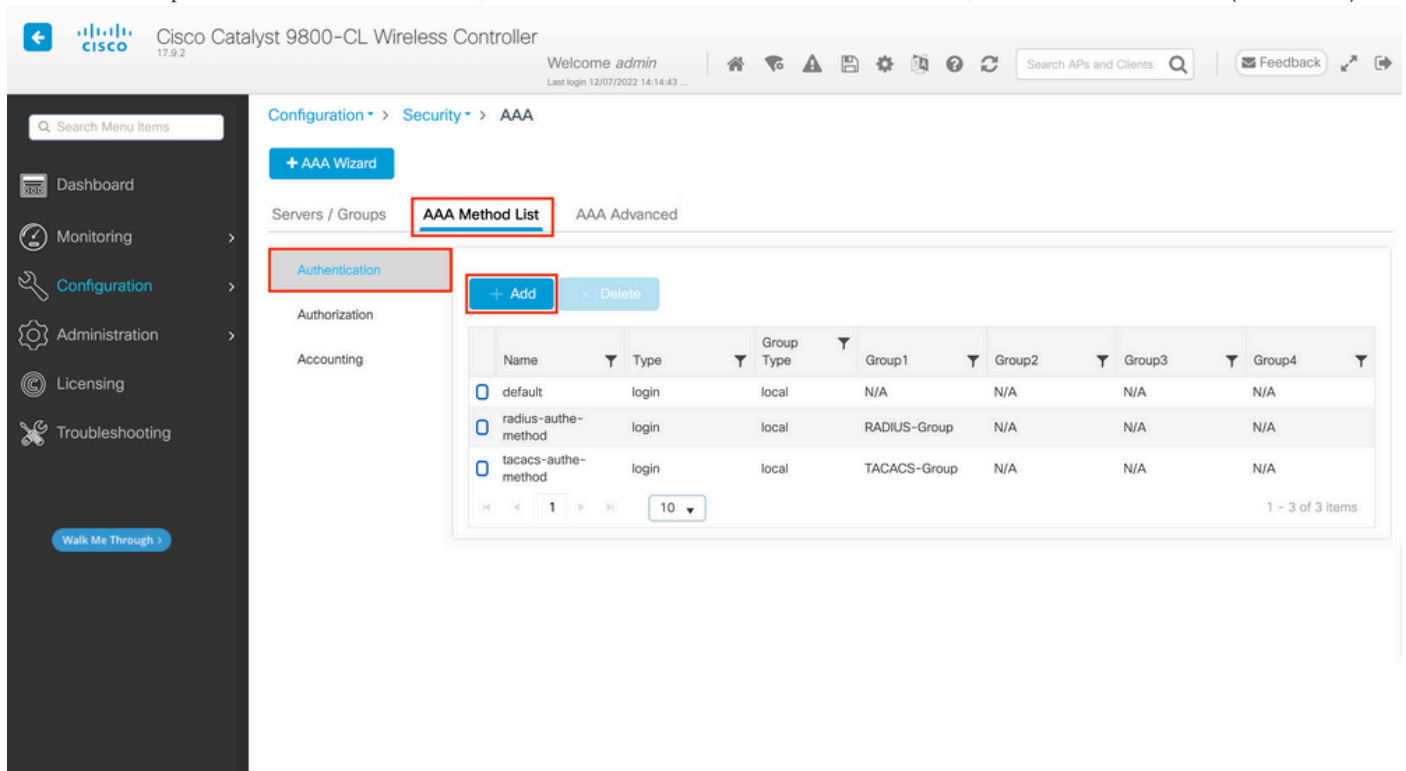
WLC-9800(config-sg-tacacs+)#server name

ISE-lab

步驟 3. 建立指向TACACS+伺服器組的AAA身份驗證登入方法。

在 GUI 上：

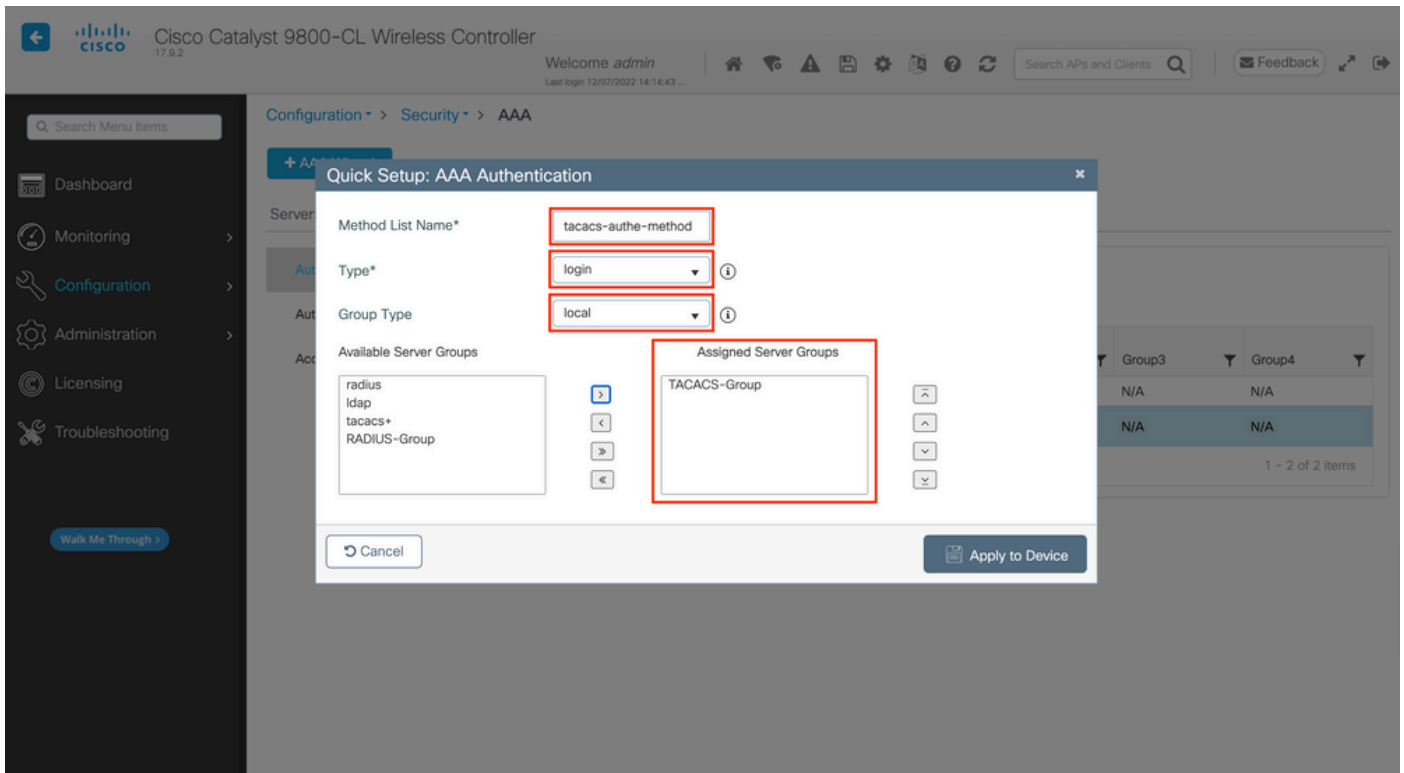
仍在GUI頁面https://<WLC-IP>/webui/#/aaa中，導航到AAA Method List > Authentication頁籤，然後建立身份驗證方法（如圖所示）。



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is active, and the 'Authentication' sub-tab is selected. A table displays the current AAA methods:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
radius-auth-method	login	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	login	local	TACACS-Group	N/A	N/A	N/A

通常，當您使用「增加」按鈕建立身份驗證方法時，會出現配置彈出窗口，類似於本圖中所示的窗口。



在此彈出窗口中，提供方法的名稱，選擇login型別，並將上一步中建立的組伺服器增加到Assigned Server Groups清單中。對於Group Type欄位，可以進行若干配置。

- 如果您選擇「群組型別」作為「本機」，WLC會先檢查使用者身份證明是否在本機存在，然後回到伺服器群組。
- 如果您選擇「群組型別」作為群組且未核取「轉至本機」選項，WLC只會檢查伺服器群組的使用者認證。
- 如果選擇組型別作為組並選中回退到本地選項，則WLC將根據伺服器組檢查使用者憑據，並且僅當伺服器未響應時才查詢本地資料庫。如果伺服器傳送拒絕訊息，則使用者必須經過驗證，即使該使用者可以存在於本機資料庫上。

在 CLI 上：

如果您希望只有在本機找不到使用者身份證明時，才使用伺服器群組來檢查使用者身份證明，請使用：

```
<#root>
```

```
WLC-9800(config)#aaa authentication login
```

```
tacacs-auth-method
```

local group

TACACS-Group

如果您希望僅對伺服器群組檢查使用者身份證明，請使用：

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

如果您想要使用伺服器群組檢查使用者身份證明，而且如果最後未使用本機專案回應，請使用：

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

local

在此示例設定中，有些使用者僅在本機建立，而有些使用者僅在ISE伺服器上，因此使用第一個選項。

步驟 4. 建立指向TACACS+伺服器組的AAA授權exec方法。

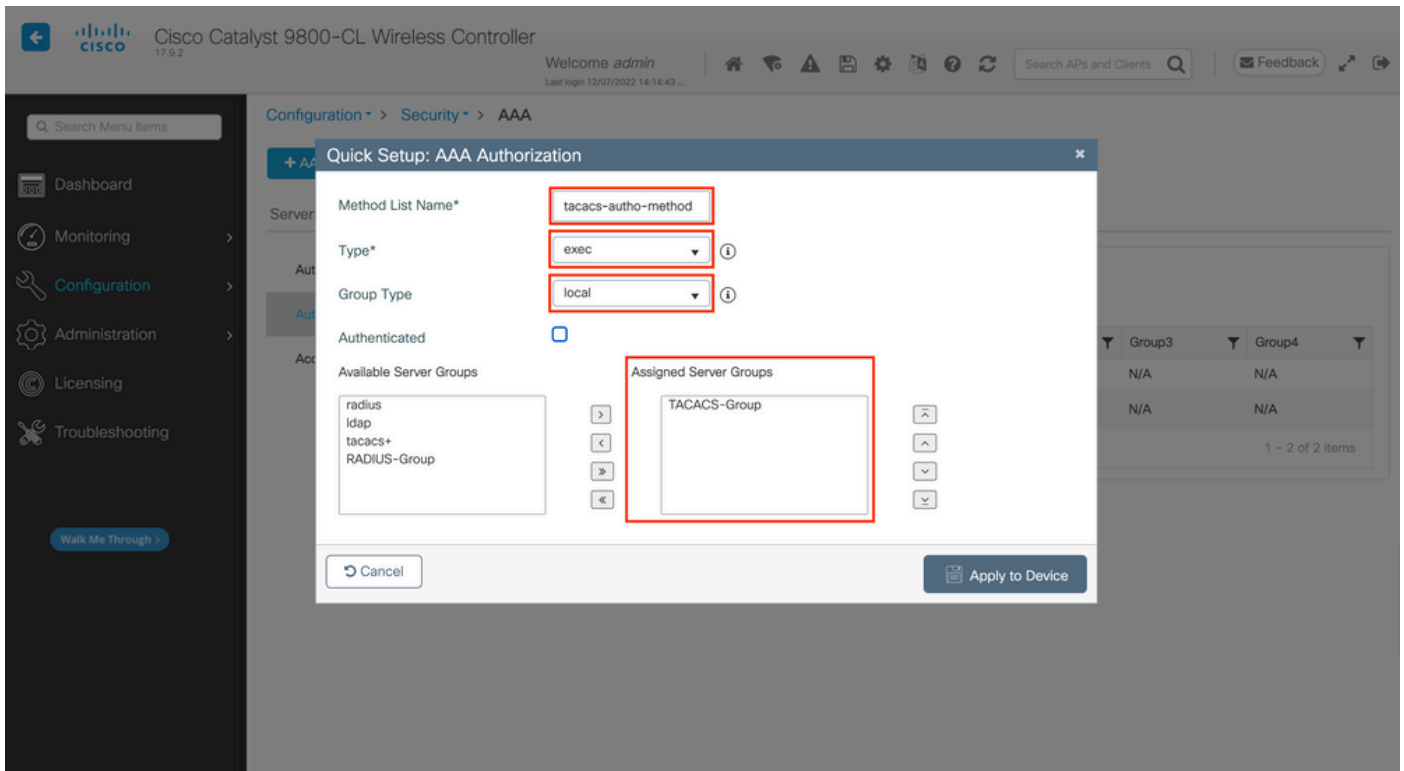
在 GUI 上：

使用者還必須獲得授權才能獲得訪問許可權。 Configuration > Security > AAA 仍在GUI頁面中，導航到AAA Method List > Authorization頁籤，然後建立授權方法（如圖所示）。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is active. The 'Authorization' sub-tab is selected, and the '+ Add' button is highlighted with a red box. Below the sub-tabs is a table with the following data:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	exec	local	N/A	N/A	N/A	N/A
radius-auth-method	exec	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	exec	local	TACACS-Group	N/A	N/A	N/A

當您使用Add按鈕增加新授權方法時，會出現與所描述配置類似的授權方法配置彈出窗口。



在此配置彈出窗口中，為授權方法提供一個名稱，選擇Type作為exec，並使用Group Type的順序與上一步中用於身份驗證方法的順序相同。

在 CLI 上：

```
<#root>
```

```
WLC-9800(config)#aaa authorization exec
```

```
tacacs-autho-method
```

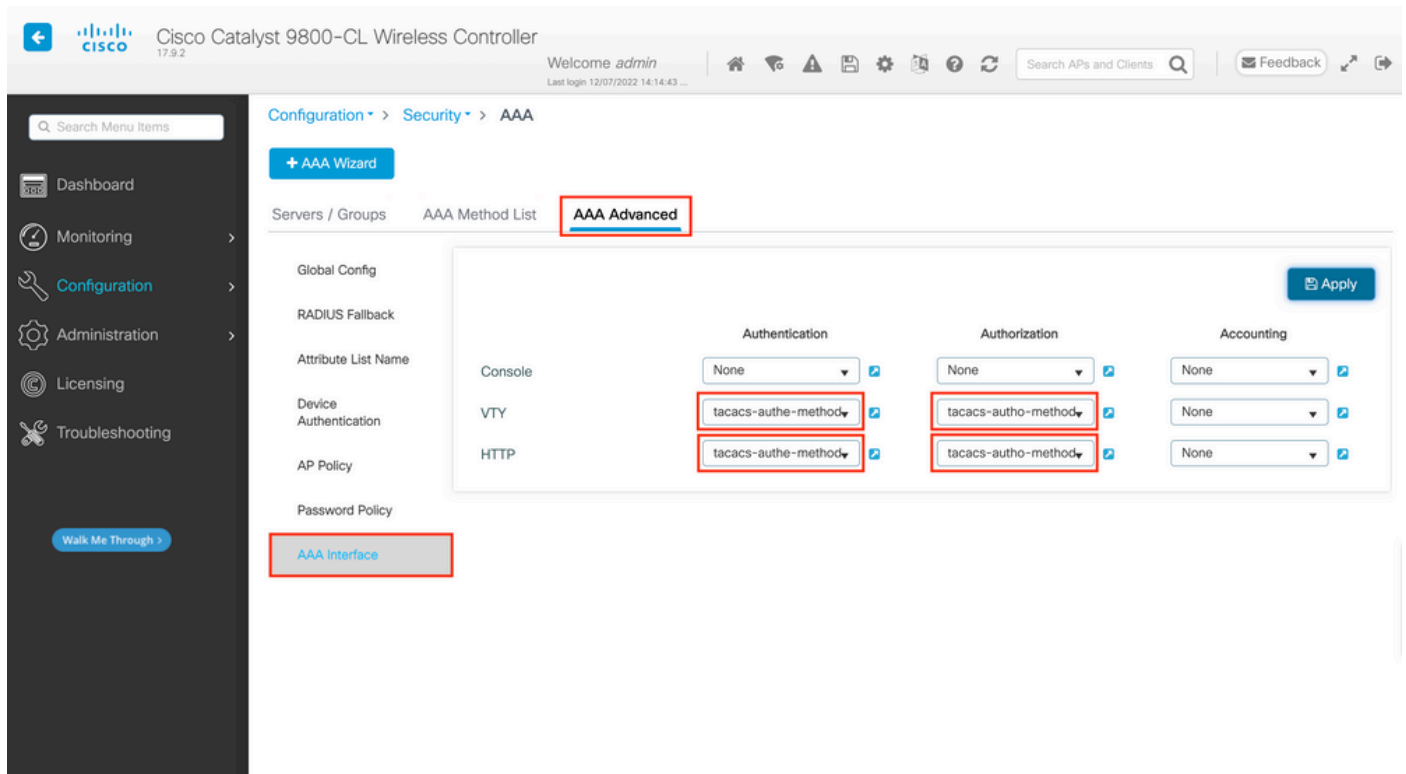
```
local group
```

```
TACACS-Group
```

步驟 5.將方法分配給HTTP配置和用於Telnet/SSH的VTY線路。

在 GUI 上：

建立的身份驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連線，您可以從AAA Advanced > AAA Interface頁籤上的GUI WLC頁進行配置(可透過https://<WLC-IP>/webui/#/aaa訪問)，如圖所示。



在 CLI 上：

對於GUI身份驗證：

```
<#root>
```

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

```
tacacs-authe-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

```
tacacs-autho-method
```

對於Telnet/SSH身份驗證：

```
<#root>
```

```
WLC-9800(config)#line vty 0 15  
WLC-9800(config-line)#login authentication
```

tacacs-authe-method

```
WLC-9800(config-line)#authorization exec
```

tacacs-autho-method

請注意，當對HTTP配置執行更改時，最好重新啟動HTTP和HTTPS服務。這可以透過這些命令來實現。

```
WLC-9800(config)#no ip http server  
WLC-9800(config)#no ip http secure-server  
WLC-9800(config)#ip http server  
WLC-9800(config)#ip http secure-server
```

TACACS+ ISE配置

步驟 1.將WLC配置為TACACS+的網路裝置。

在 GUI 上：

要將上一部分中使用的WLC宣告為ISE中RADIUS的網路裝置，請導航到Administration > Network Resources > Network Devices並打開「網路裝置」頁籤，如此圖中所示。

The screenshot shows the Cisco ISE Administration console. At the top, the navigation bar includes 'Cisco ISE', 'Administration · Network Resources', and 'Evaluation Mode 82 Days'. Below this, a menu bar contains 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'More'. The left sidebar has 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and shows a table with one entry: 'WLC-9800' with IP/Mask '10.48.39...', Profile Name 'Cisco', Location 'All Locations', and Type 'All Device Types'. The 'Edit' button and the checkbox for the 'WLC-9800' entry are highlighted with red boxes.

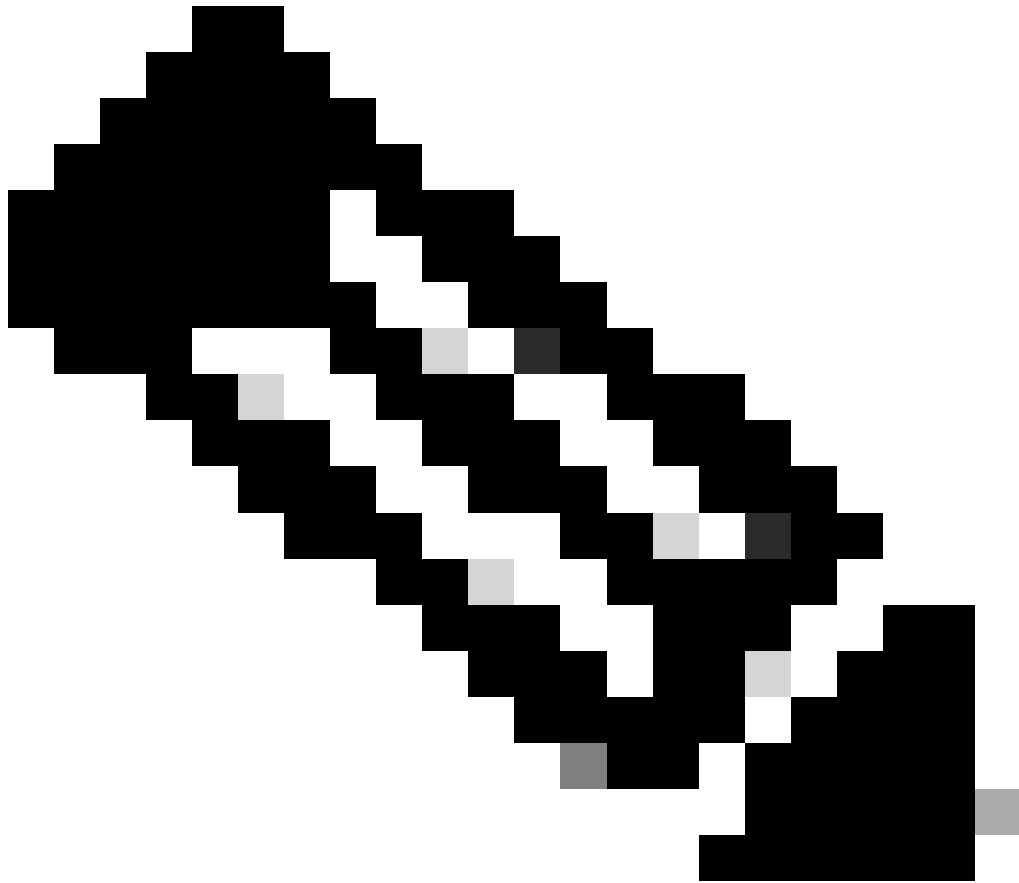
<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input checked="" type="checkbox"/>	WLC-9800	10.48.39....	Cisco	All Locations	All Device Types	

在本示例中，已為RADIUS身份驗證增加了WLC(請參閱[配置RADIUS ISE](#)部分的步驟1。)因此，只需修改其配置即可配置TACACS身份驗證，只需在網路裝置清單中選擇WLC並按一下Edit按鈕即可。這將打開網路裝置配置表，如下圖所示。

The screenshot shows the configuration page for a Network Device in Cisco ISE. The navigation bar and menu bar are the same as in the previous screenshot. The left sidebar is the same. The main content area is titled 'General Settings' and includes several sections: 'Enable KeyWrap' (disabled), 'Key Encryption Key' (with a 'Show' link), 'Message Authenticator Code Key' (with a 'Show' link), 'Key Input Format' (radio buttons for ASCII and HEXADECIMAL, with ASCII selected), 'TACACS Authentication Settings' (checked), 'Shared Secret' (with a 'Show' link), 'Enable Single Connect Mode' (disabled, with radio buttons for Legacy Cisco Device and TACACS Draft Compliance Single Connect Support, with Legacy Cisco Device selected), 'SNMP Settings' (disabled), and 'Advanced TrustSec Settings' (disabled). The 'TACACS Authentication Settings' section and the 'Shared Secret' field are highlighted with red boxes.

打開新窗口後，向下滾動到「TACACS Authentication Settings」部分，啟用這些設定，並增加在[Configure TACACS+ WLC](#)部分的步驟1中輸入的共用金鑰。

步驟 2. 啟用節點的裝置管理功能。



注意：要將ISE用作TACACS+伺服器，您必須擁有裝置管理許可證軟體套件和基礎許可證或移動許可證。

在 GUI 上：

安裝裝置管理許可證後，必須啟用節點的裝置管理功能，才能將ISE用作TACACS+伺服器。為此，請編輯所用ISE部署節點的配置(可以在Administrator > Deployment下找到)，然後按一下其名稱或藉助Edit按鈕執行此操作。

Deployment

- Deployment
- PAN Failover

Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	<input checked="" type="checkbox"/>

打開節點配置窗口後，請選中Policy Service部分下的Enable Device Admin Service選項，如下圖所示。

Deployment Nodes List > ise

Edit Node

General Settings Profiling Configuration

Hostname **ise**

FQDN **ise.cisco.com**

IP Address **10.48.39.134**

Node Type **Identity Services Engine (ISE)**

Role **STANDALONE** [Make Primary](#)

Administration

Monitoring

Role **PRIMARY**

Other Monitoring Node _____

Dedicated MnT ⓘ

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **None**

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

[Reset](#) [Save](#)

步驟 3. 建立TACACS設定檔，以傳回許可權。

在 GUI 上：

要具有管理員訪問許可權，adminuser需要具有15級的特權，它允許訪問exec提示符shell。另一方面，helpdeskuser不需要exec提示外殼訪問，因此可以為它分配低於15的特權級別。為了將適當的許可權級別分配給使用者，可以使用授權配置檔案。這些可以從ISE GUI頁面Work Centers > Device Administration > Policy Elements的Results > TACACS Profiles頁籤下配置，如下圖所示。

- Conditions
 - Library Conditions
 - Smart Conditions
- Network Conditions
- Results
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles**

TACACS Profiles

Rows/Page 6 / 1 / 1 > > Go 6 Total Rows

Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	IOS Admin	Shell	Assigned to each user in the group admin-group
<input type="checkbox"/>	IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

要配置新的TACACS配置檔案，請使用Add按鈕，打開與圖中所示類似的新配置檔案配置表。此表單在配置分配給adminuser(即，具有shell許可權級別15)的配置檔案時，必須特別像這樣。

Cisco ISE Work Centers - Device Administration Evaluation Mode 82 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets More

TACACS Profiles > IOS Admin
TACACS Profile

Name: **IOS Admin**

Description: Assigned to each user in the group admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type: **Shell**

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

對輪廓重複操作helpdesk。對於最後一個，Default Privilege和Maximum Privilege均設定為1。

步驟 4.在ISE上建立使用者組。

這與本文檔[配置RADIUS ISE](#)部分的步驟3中的說明相同。

步驟 5.在ISE上建立使用者。

這與本文檔[配置RADIUS ISE](#)部分的步驟4中的說明相同。

步驟 6.建立裝置管理策略集。

在 GUI 上：

對於RADIUS訪問，使用者建立後，仍需要在ISE上定義其身份驗證和授權策略以授予其正確的訪問許可權。TACACS身份驗證為此，使用裝置管理策略集，可從Work Centers > Device Administration > Device Admin Policy Sets GUI Page進行配置，如下所示。

Policy Sets

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0		
	Default	Tacacs Default policy set		Default Device Admin	0		

[Reset](#) [Save](#)

若要建立裝置管理原則集，請使用上一個影像中以紅色框住的「新增」按鈕，這樣會將專案新增至原則集清單。為新建立的組提供一個名稱、必須應用該組的條件以及允許的協定/伺服器序列(此處，Default Device Admin為足夠)。使用Save按鈕完成增加策略集，並使用其右邊的箭頭來訪問其配置頁 (如圖中所示)。

Policy Sets → **WLC TACACS Authentication**

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		All_User_ID_Stores	0	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Helpdesk users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0		
✓	Admin users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset

Save

此示例中的特定策略集「WLC TACACS Authentication」過濾IP地址等於示例C9800 WLC IP地址的請求。

作為身份驗證策略，預設規則已保留，因為它滿足使用需要。已設定兩個授權規則：

- 當使用者屬於定義的群組admin-group時，會觸發第一個動作。它允許所有命令(透過預設Permit_all規則)並分配許可權15(透過定義的IOS_Admin TACACS配置檔案)。
- 當使用者屬於定義的組helpdesk-group時，將觸發第二個。它允許所有命令(透過預設Permit_all規則)並分配許可權1(透過定義的IOS_Helpdesk TACACS配置檔案)。

完成此步驟後，為adminuser和helpdesk使用者配置的憑據可用於透過GUI或Telnet/SSH在WLC中執行身份驗證。

疑難排解

如果您的RADIUS伺服器預期會傳送服務型別RADIUS屬性，您可以新增WLC：

```
radius-server attribute 6 on-for-login-auth
```

透過WLC CLI排除WLC GUI或CLI RADIUS/TACACS+訪問故障

要排除TACACS+對WLC GUI或CLI的訪問故障，請發出debug tacacs命令以及terminal monitor one，並在嘗試登入時檢視即時輸出。

例如，成功登入後註銷adminuser使用者，即可生成以下輸出。

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

從這些記錄中可以看到，TACACS+伺服器傳回正確的許可權(即AV priv-lvl=15)。

執行RADIUS驗證時，會顯示類似的偵錯輸出，其中涉及RADIUS流量。

而命令debug aaa authentication和debug aaa authorization會顯示WLC在使用者嘗試登入時選擇的方法清單。

透過ISE GUI排除WLC GUI或CLI TACACS+訪問故障

在第Operations > TACACS > Live Logs頁中，可以檢視過去24小時內透過TACACS+進行的每個使用者身份驗證。要展開TACACS+授權或身份驗證的詳細資訊，請使用與此事件相關的「詳細資訊」按鈕。

The screenshot shows the Cisco ISE interface with the following elements:

- Page Header: Cisco ISE, Operations · TACACS, Evaluation Mode 82 Days.
- Navigation: Live Logs (highlighted).
- Controls: Refresh (Never), Show (Latest 20 records), Within (Last 3 hours), Filter, Export To.
- Table with columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, N.
- Table Content (6 records):

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	✓		helpdeskuser	Authorization	Authentication Policy	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	✓		helpdeskuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:38:38.2...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W
Dec 08, 2022 06:34:54.0...	✓		adminuser	Authorization		WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	✓		adminuser	Authentication	WLC TACACS Authentication >...		ise	W

Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time) Records Shown: 6

展開時，helpdeskuser的身份驗證成功嘗試如下所示：

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

```

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global
TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (
🚫 Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

```

從這裡可以看出，使用者helpdeskuser已經在驗證原則WLC TACACS Authentication > Default的幫助下成功地透過驗證到網路裝置WLC-9800。此外，授權配置檔案IOS Helpdesk已分配給此使用者，並授予許可權級別1。

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）。