配置RADIUS &適用於GUI的TACACS+ &9800 WLC上的CLI驗證

目錄

簡介

本文說明如何為RADIUS或TACACS+外部驗證設定Catalyst 9800。

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

使用者嘗試存取WLC的CLI或GUI時，系統會提示其輸入使用者名稱和密碼。預設情況下，會將這些憑證與裝置本身存在的使用者本地資料庫進行比較。或者，可指示WLC將輸入憑證與遠端AAA伺服器進行比較：wlc可以使用RADIUS或TACACS+與伺服器通訊。這些是管理員使用者僅有的兩種外部身份驗證方法（例如，無LDAP）。

設定

在本示例中，配置了AAA伺服器(ISE)上的兩種使用者adminuser，分別為helpdeskuser和。這些使用者分別是admin-group和helpdesk-group組的一部分。使用者adminuser(屬於admin-group)預期會獲得對WLC的完整存取許可權。另一方面helpdeskuser,的一部分helpdesk-group，僅被授予WLC的監控器許可權。因此，沒有配置訪問許可權。

本文先將WLC和ISE配置為RADIUS身份驗證，然後對TACACS+執行相同操作。

只讀使用者限制

將TACACS+或RADIUS用於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（這相當於本地通過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
- 不支援許可權級別為15的使用者以及僅允許特定命令的命令集。使用者仍可以通過WebUI執行配置更改

不能更改或修改這些注意事項。

設定WLC的RADIUS驗證

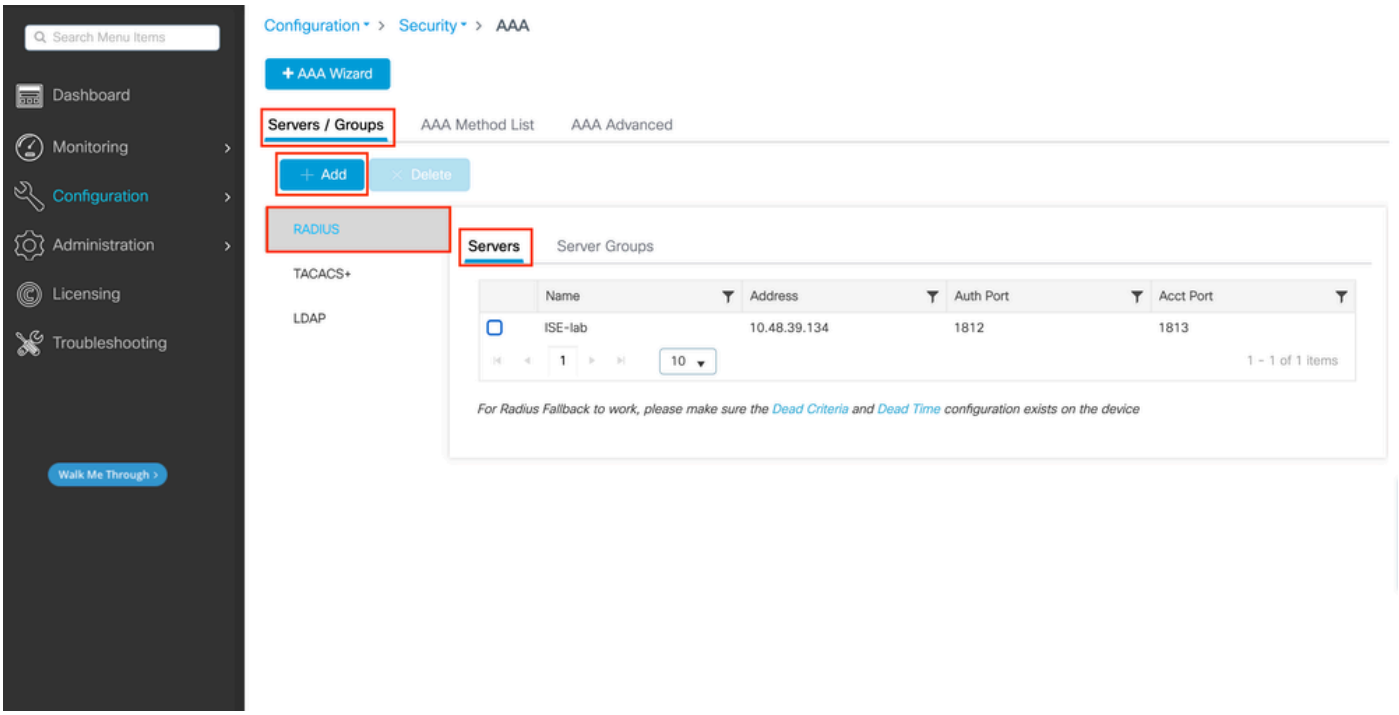
步驟1.宣告RADIUS伺服器。

在 GUI 上：

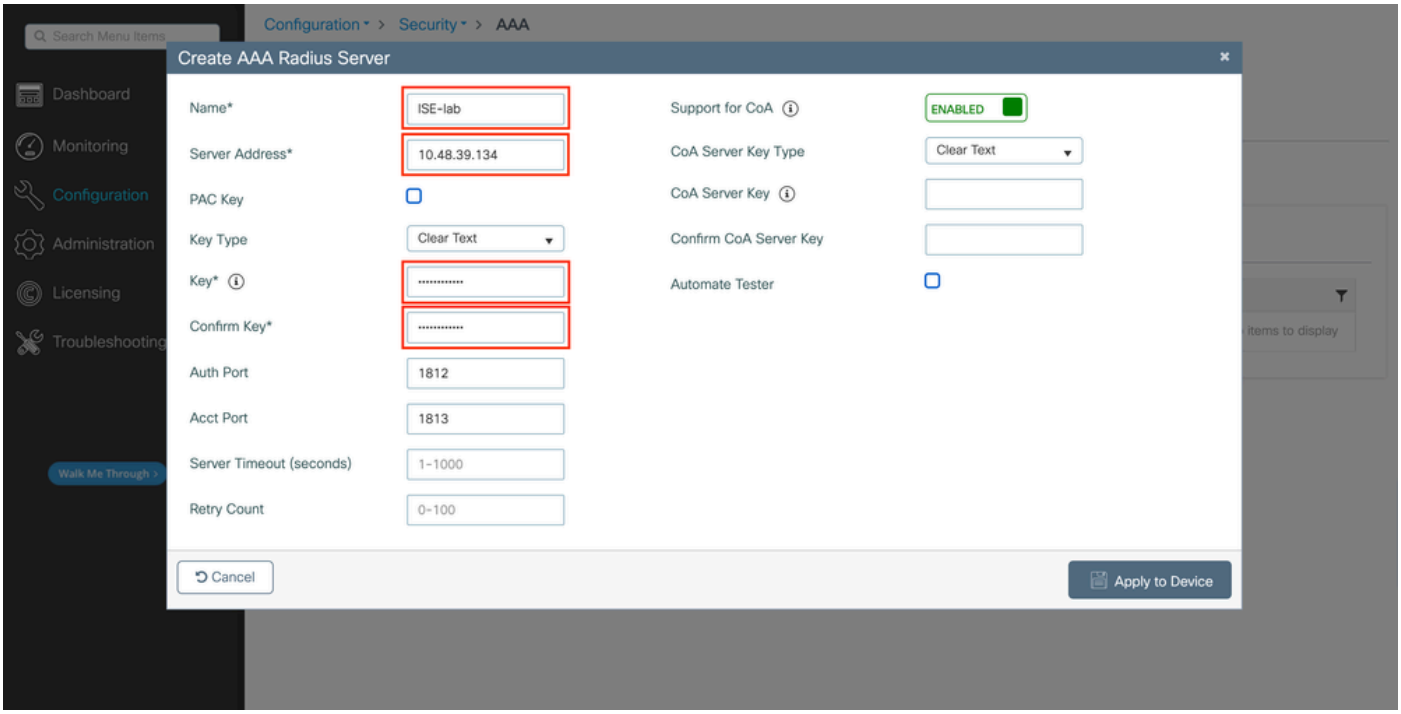
首先，在WLC上建立ISE RADIUS伺服器。這可以通過https://

/webui/#/aaa

的GUI WLC頁面中的頁籤Servers/Groups > RADIUS > Servers(如果導航到Configuration > Security > AAA)，如本圖所示。



若要在WLC上新增RADIUS伺服器，請按一下映像中紅色框架的「Add」按鈕。這將開啟螢幕截圖中所示的彈出視窗。



在此彈出視窗中，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伺服器之間的共用密碼

可以配置其他引數，例如用於身份驗證和記帳的埠，但這些引數不是強制引數，保留為本文檔的預設引數。

在 CLI 上：

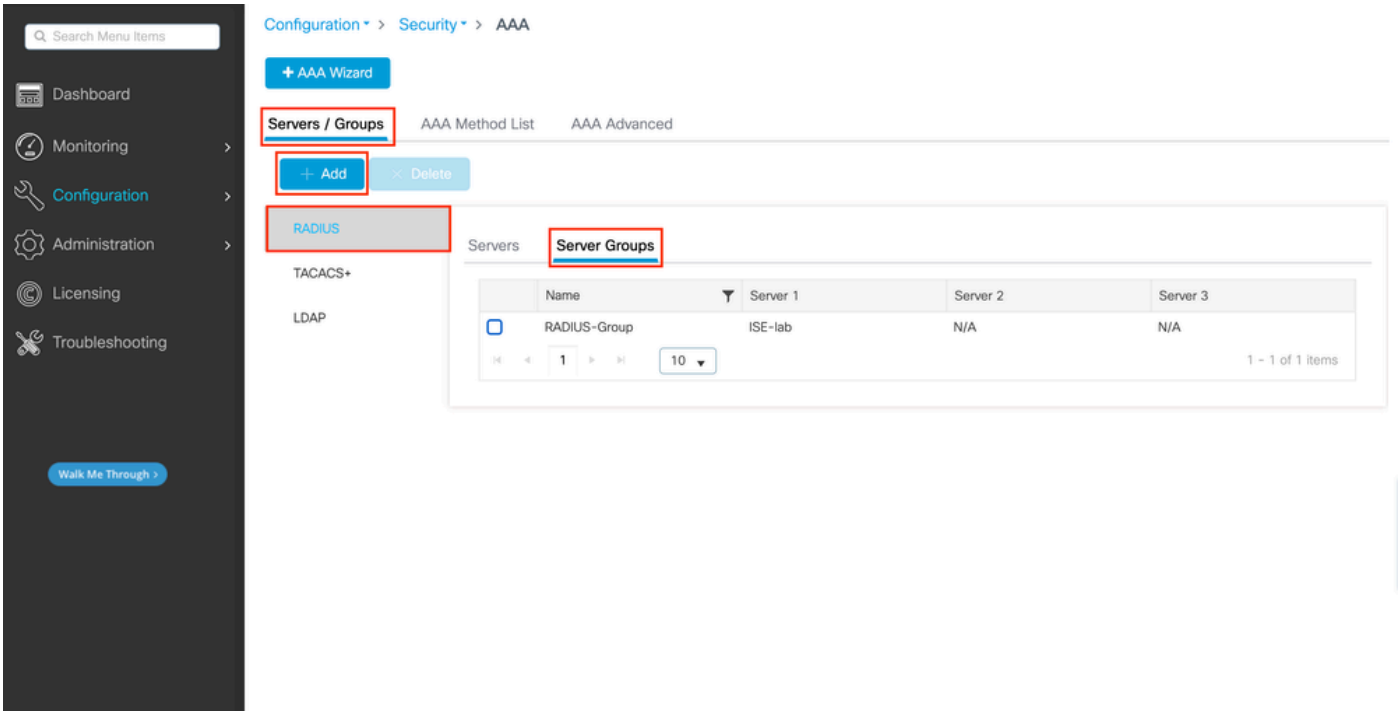
<#root>

```
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
```

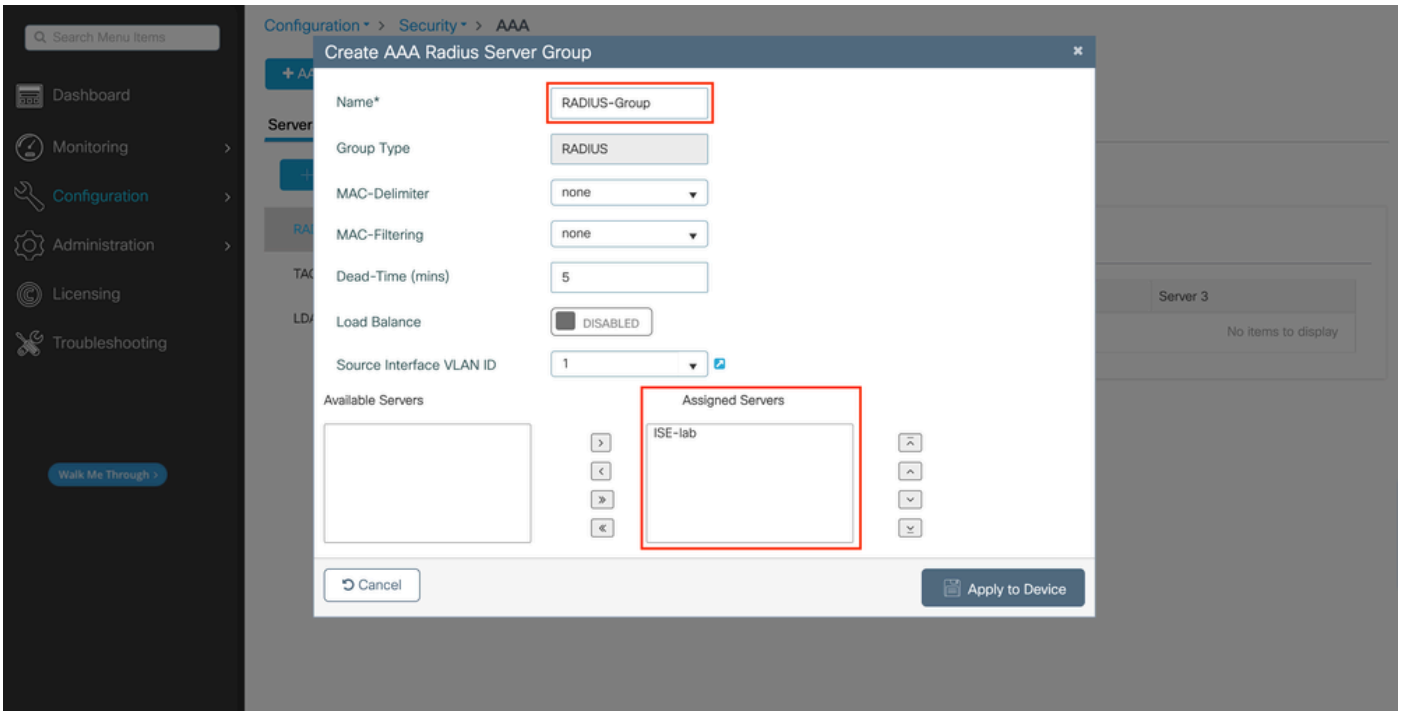
步驟2.將RADIUS伺服器對映到伺服器組。

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負責在伺服器組中的伺服器之間平衡不同身份驗證的負載。RADIUS伺服器群組是從「Servers/Groups > RADIUS > Server Groups」索引標籤中，從與步驟1中提到的GUI頁面進行設定，如下圖所示。



對於伺服器建立，當您按一下Add按鈕（框定在上一個影象中）時，將出現一個彈出視窗，如下圖所示。



在彈出視窗中，為組提供一個名稱，並將所需的伺服器移動到「分配的伺服器」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
```

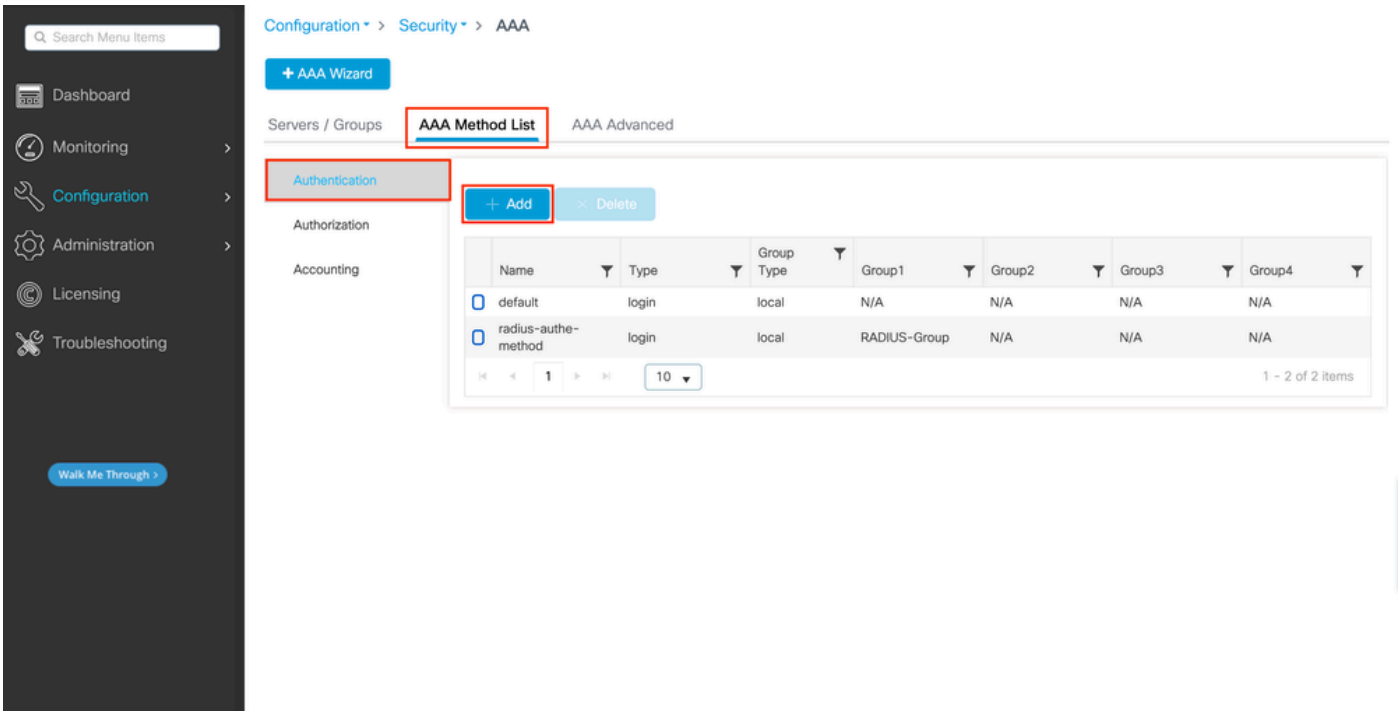
步驟3.建立指向RADIUS伺服器組的AAA身份驗證登入方法。

在 GUI 上：

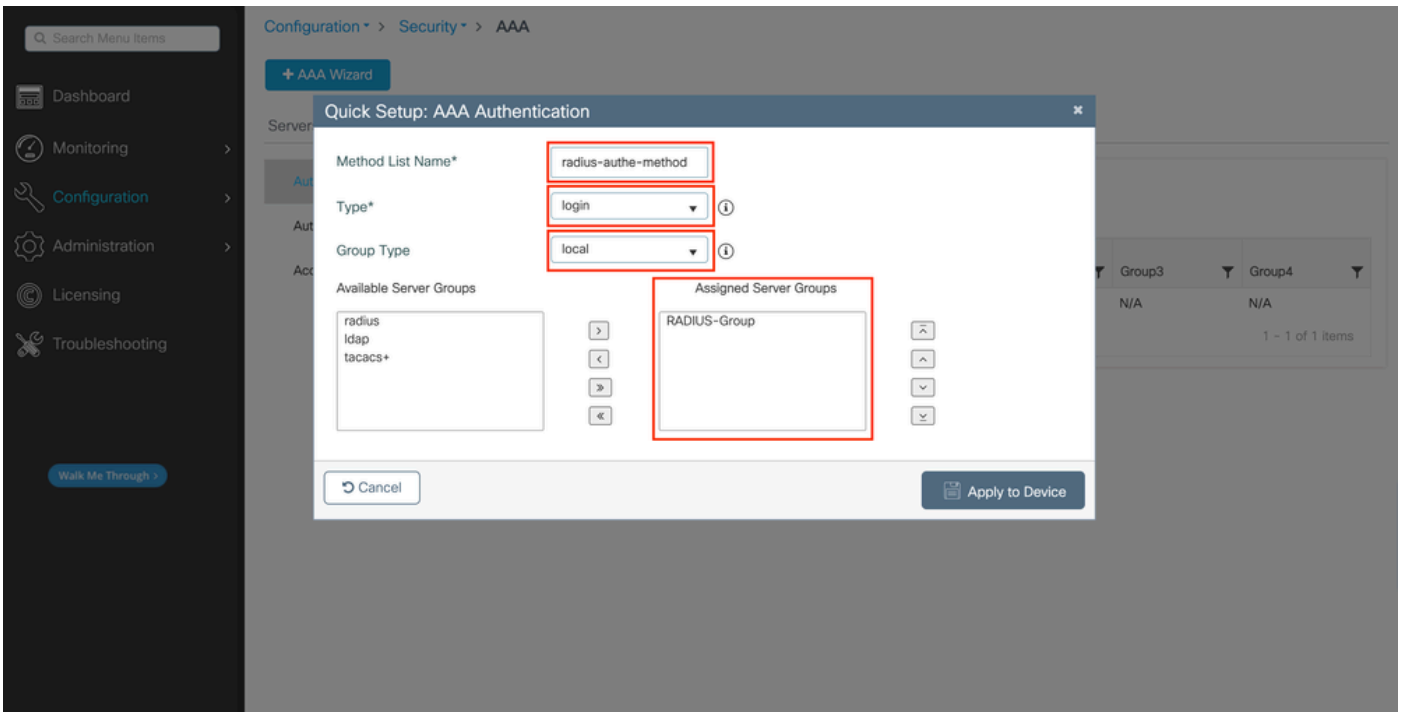
仍可在GUI頁面上https://

/webui/#/aaa

，導覽至AAA Method List > Authentication頁籤並建立一個驗證方法，如下圖所示。



通常，當您使用Add按鈕建立身份驗證方法時，會出現一個配置彈出視窗，類似於本圖中所示的視窗。



在此彈出視窗中，提供方法的名稱。選擇Type「作為登入」，將在上一步中建立的組伺服器新增到列表Assigned Server Groups。對於Group Type欄位，可能有幾種配置。

- 如果您選擇「組型別」作為「本地」，WLC會首先檢查使用者憑證是否存在於本地，然後回退到伺服器組。
- 如果您選擇「組型別」作為組並且沒有選中「回退到本地」選項，WLC只會針對伺服器組檢查使用者憑據。
- 如果選擇「組型別」作為組並選中「回退到本地」選項，則WLC會針對伺服器組檢查使用者憑據，並僅在伺服器沒有響應時才查詢本地資料庫。如果伺服器傳送拒絕消息，則使用者將被

驗證，即使該使用者可能存在於本地資料庫中。

在 CLI 上：

如果希望只有在首先在本地找不到使用者憑據時，才使用伺服器組檢查使用者憑據，請使用：

```
<#root>
WLC-9800(config)#aaa authentication login
radius-authe-method
 local group
RADIUS-Group
```

如果希望僅對伺服器組檢查使用者憑據，請使用：

```
<#root>
WLC-9800(config)#aaa authentication login
radius-authe-method
 group
RADIUS-Group
```

如果希望對伺服器組檢查使用者憑據，並且最後未對本地條目作出響應，請使用：

```
<#root>
WLC-9800(config)#aaa authentication login
radius-authe-method
 group
RADIUS-Group
 local
```

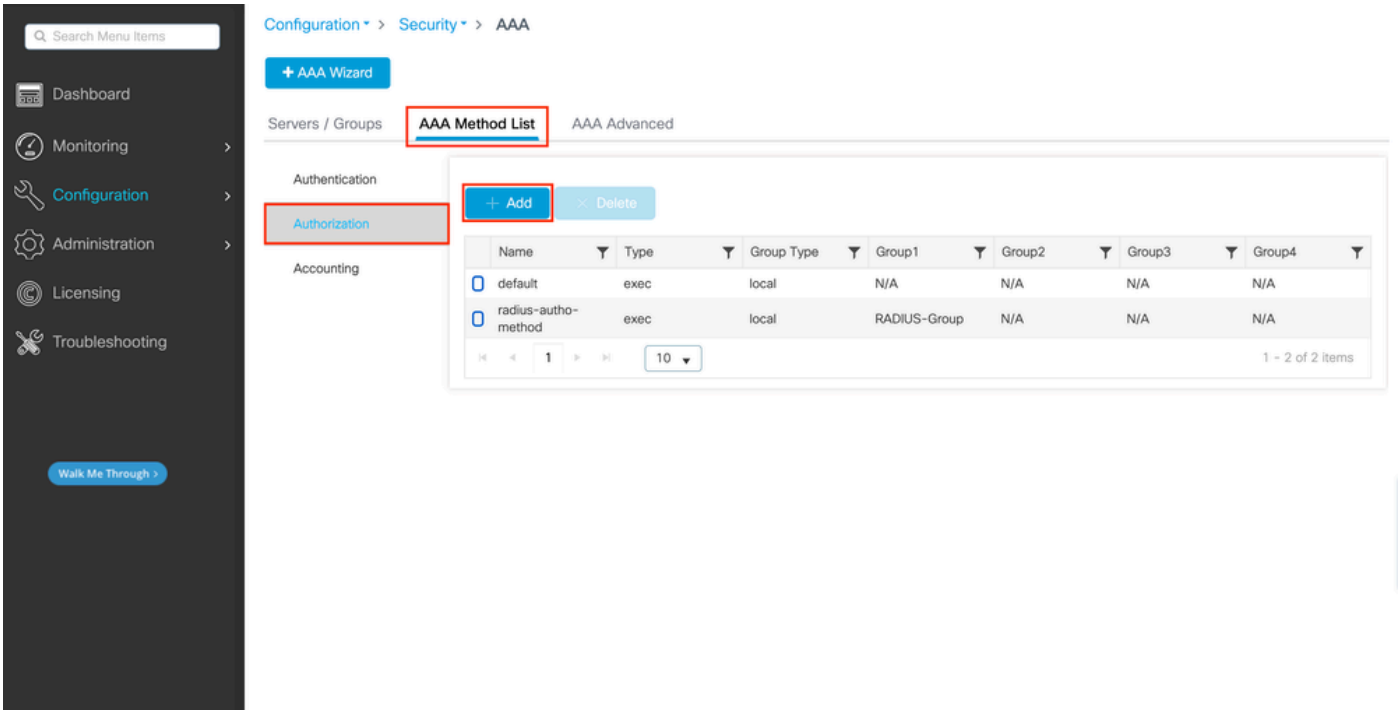
在此示例設定中，有些使用者僅在本機建立，而有些使用者僅在ISE伺服器上建立，因此使用第一

個選項。

步驟4.建立指向RADIUS伺服器組的AAA授權執行方法。

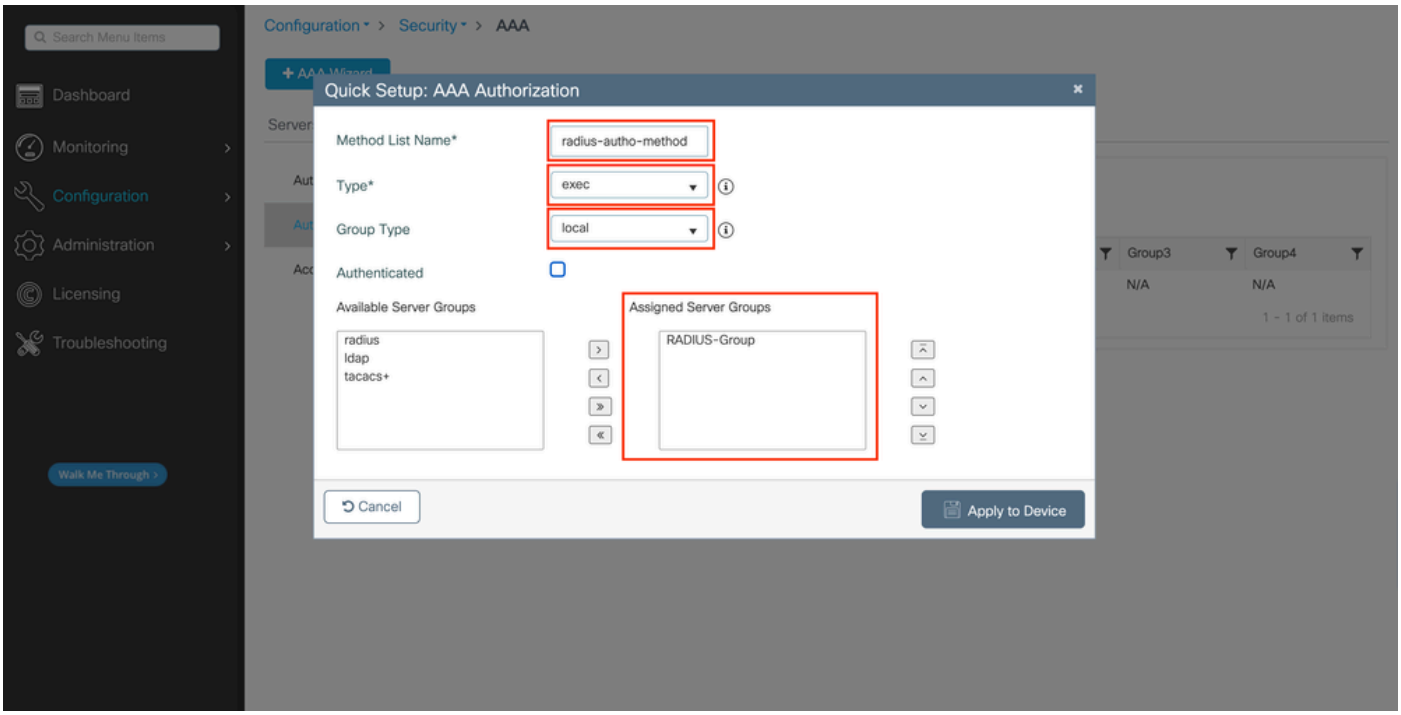
在 GUI 上：

使用者還必須獲得授權才能獲得訪問許可權。仍可從GUI Page Configuration > Security > AAA，導覽至AAA Method List > Authorization頁籤，然後建立授權方法，如下圖所示。



授權方法建立

當您使用「新增」按鈕新增新授權方法時，將出現一個與所示的授權方法配置類似的彈出式視窗。



在此配置彈出視窗中，提供授權方法的名稱，選擇型別為exec，並使用與步驟3中身份驗證方法相同的組型別順序。

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
```

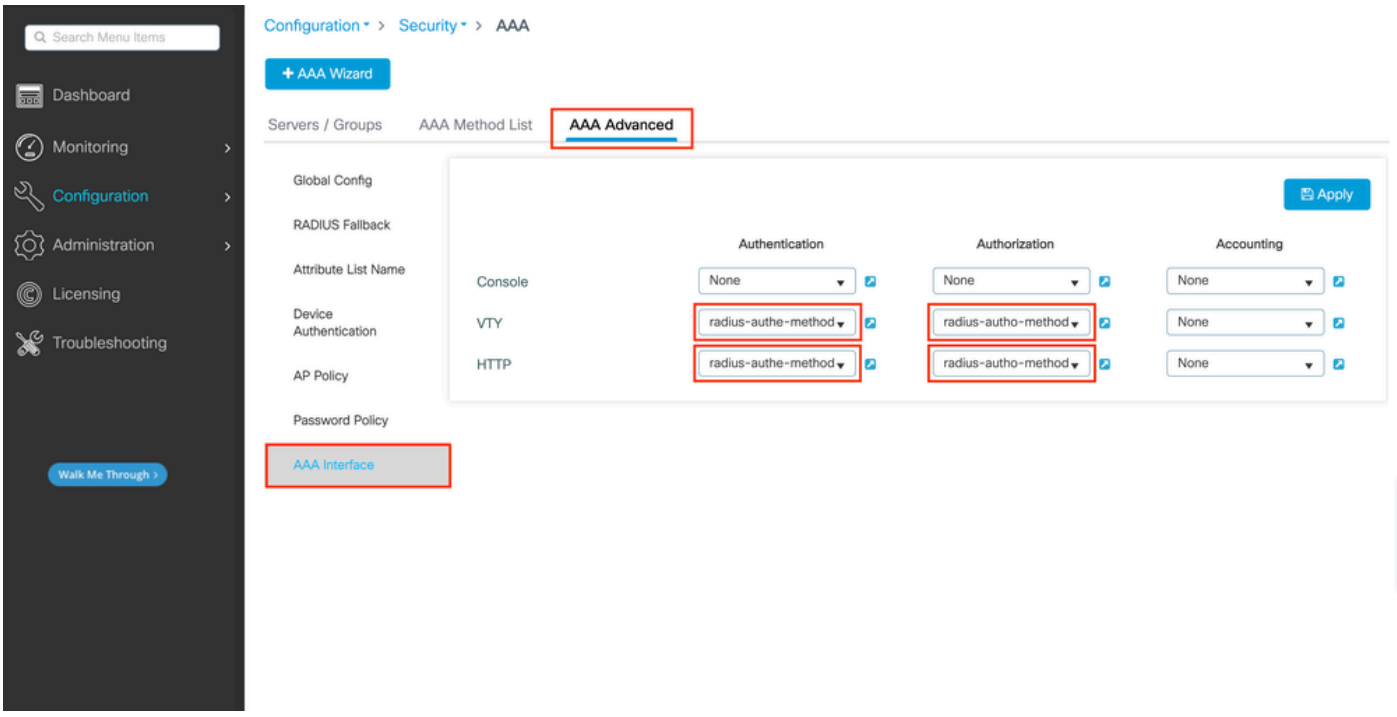
步驟5.將方法分配給HTTP配置以及用於Telnet/SSH的VTY線路。

在 GUI 上：

建立的驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連接，可在GUI WLC頁面的AAA Advanced > AAA Interface https://

/webui/#/aaa

(仍可在GUI WLC頁面上設定)，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-authe-method

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

radius-autho-method
```

Telnet/SSH身份驗證的CLI:

```
<#root>

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

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-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。這可通過以下命令實現：

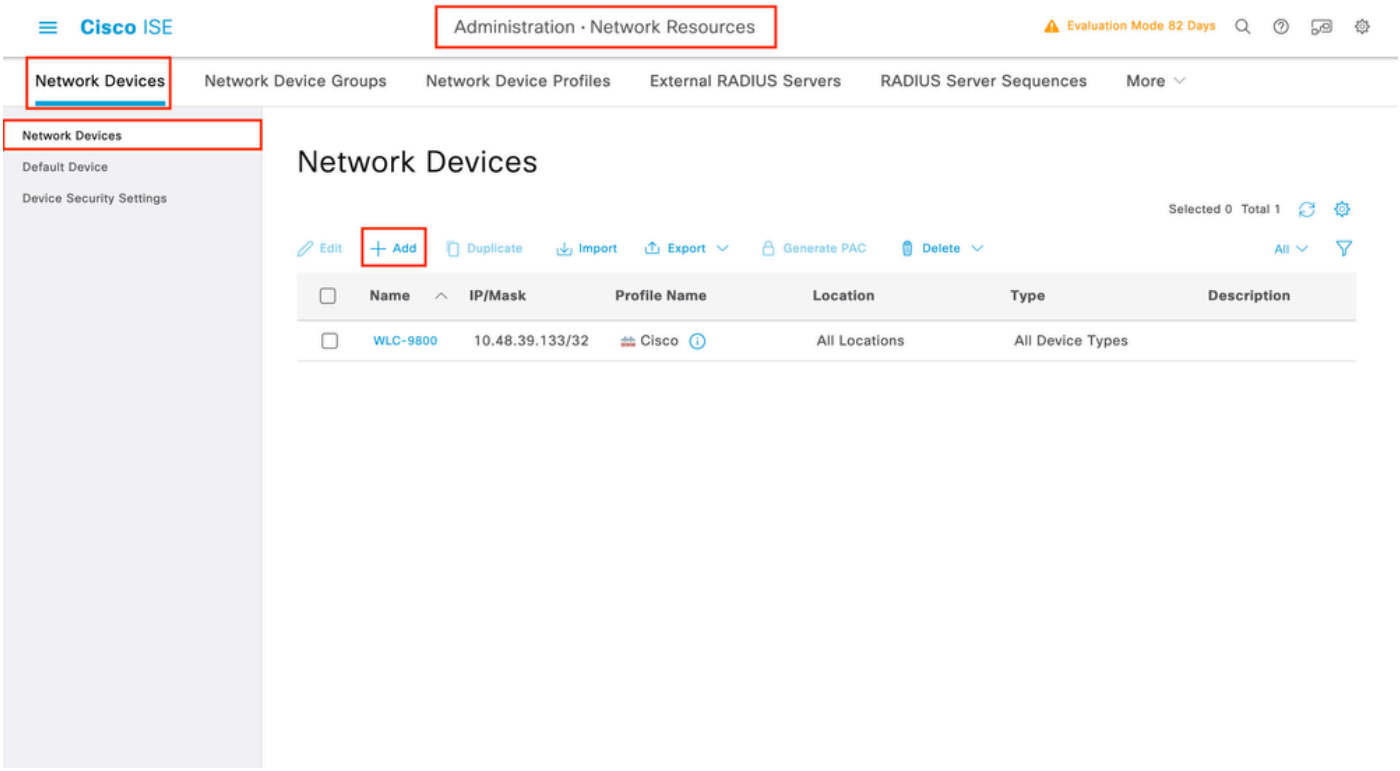
```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

為RADIUS配置ISE

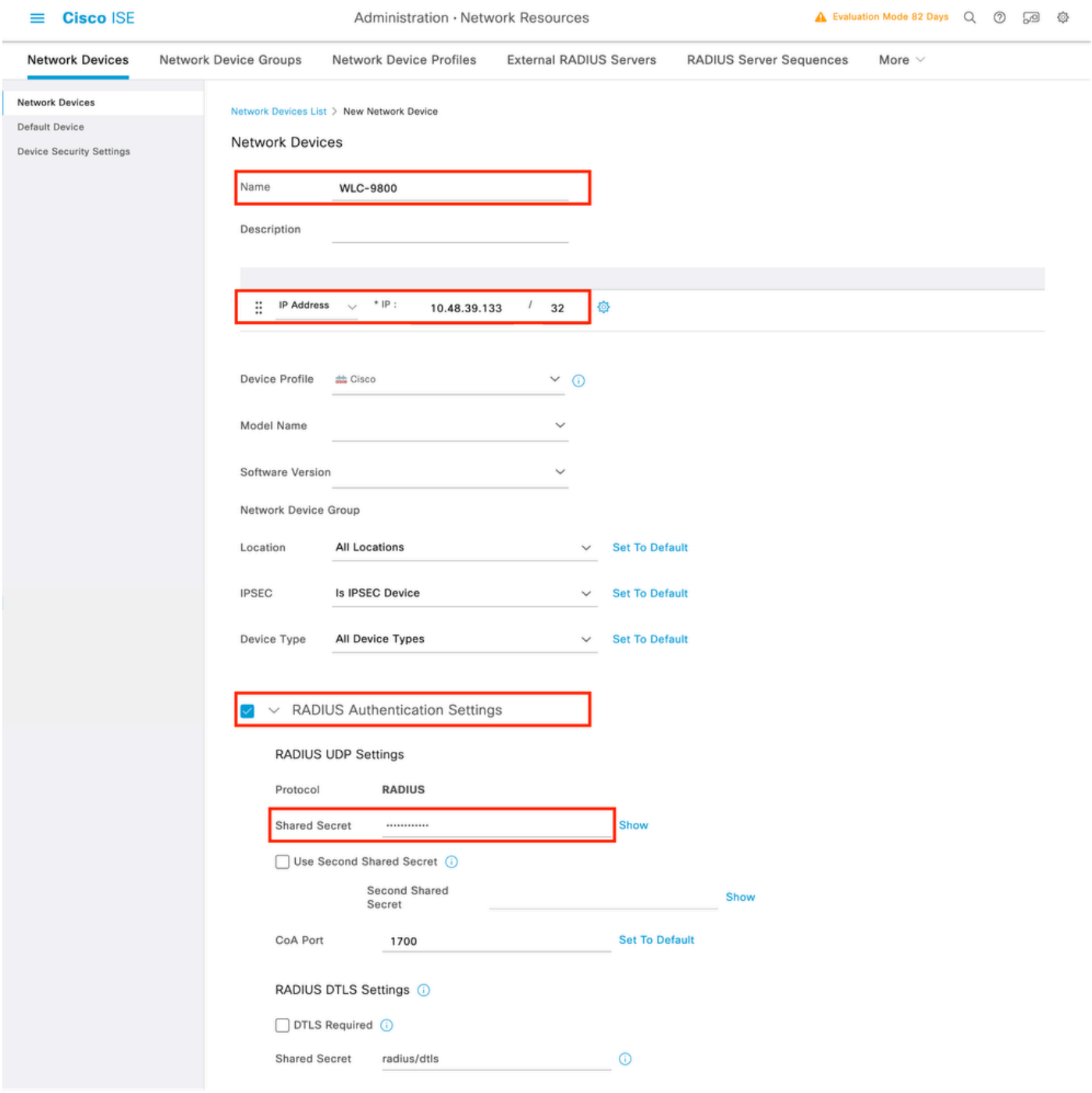
步驟1.將WLC配置為RADIUS的網路裝置。

在 GUI 上：

若要將上一節中使用的WLC宣告為ISE中RADIUS的網路裝置，請導覽至Administration > Network Ressources > Network Devices，然後開啟Network devices頁籤，如下圖所示。



要新增網路裝置，請使用Add按鈕，該按鈕將開啟新的網路裝置配置表單。

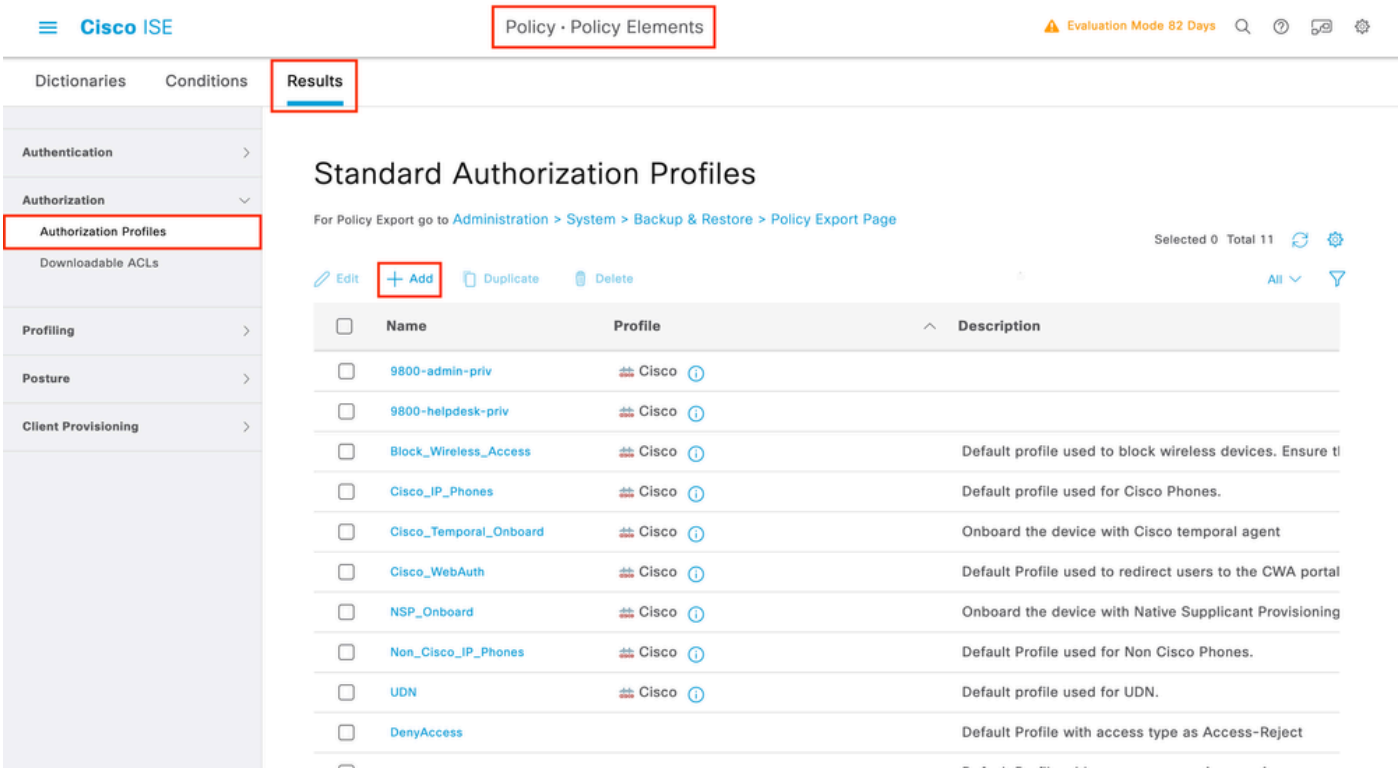


在新視窗中，提供網路裝置的名稱，並新增其IP地址。選擇RADIUS驗證設定，並設定與WLC上使用的同一RADIUS共用密碼。

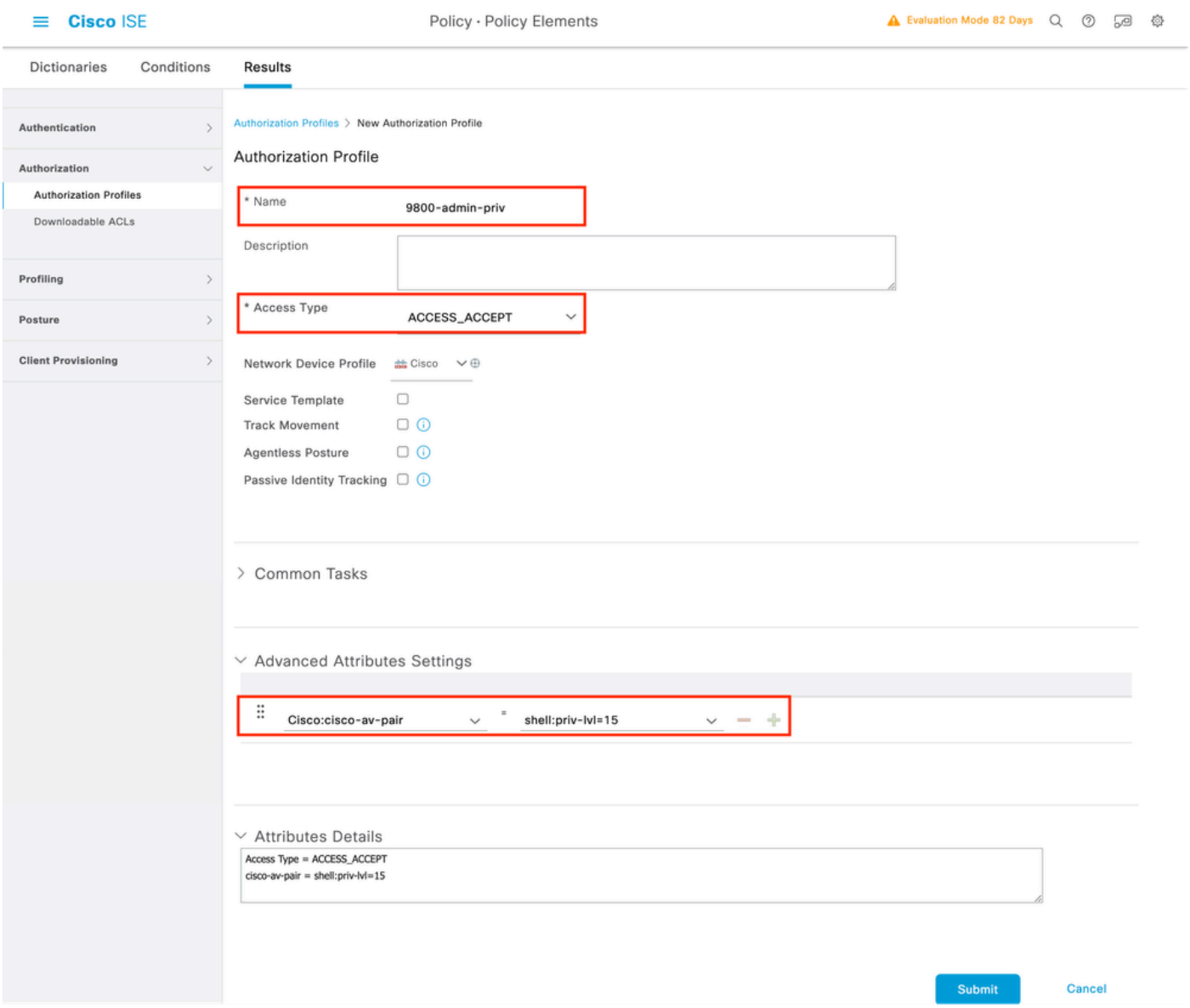
步驟2.建立授權結果以返回許可權。

在 GUI 上：

要具有管理員訪問許可權，需要具有adminuser15的許可權級別，該級別允許訪問exec提示外殼。另一方面，不需要exec提示外殼訪問，因此可以分配許可權級別低於helpdeskuser15的許可權級別。為了向使用者分配正確的許可權級別，可以使用授權配置檔案。可以從下一張圖ISE GUI Page Policy > Policy Elements > Results所示頁籤下的Authorization > Authorization Profiles，配置這些選項。



要配置新的授權配置檔案，請使用Add按鈕，該按鈕將開啟新的授權配置檔案配置表。要配置分配給的配置檔案，此表單必須特別像這樣adminuser。



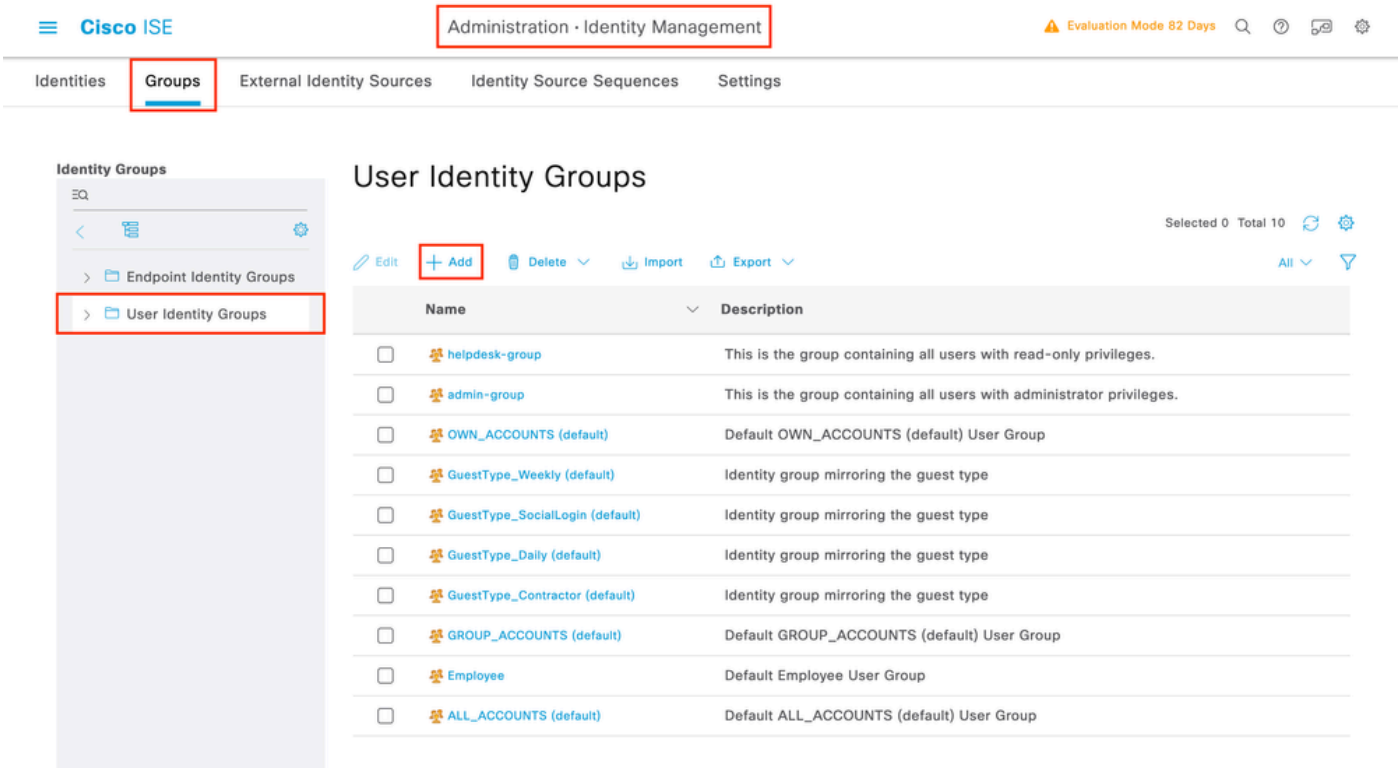
配置顯示將許可權級別15授予與其關聯的任何使用者。如前所述，這是下一個步驟中建立的的預期行為adminuser。但是，必helpdeskuser須具有較低的許可權級別，因此必須建立第二個策略元素。

helpdeskuser 的策略元素類似於上面建立的元素，不同之處在shell:priv-lvl=15是，必須將字串更改為shell:priv-lvl=X，並用所需的許可權級別替換X。在此示例中，使用1。

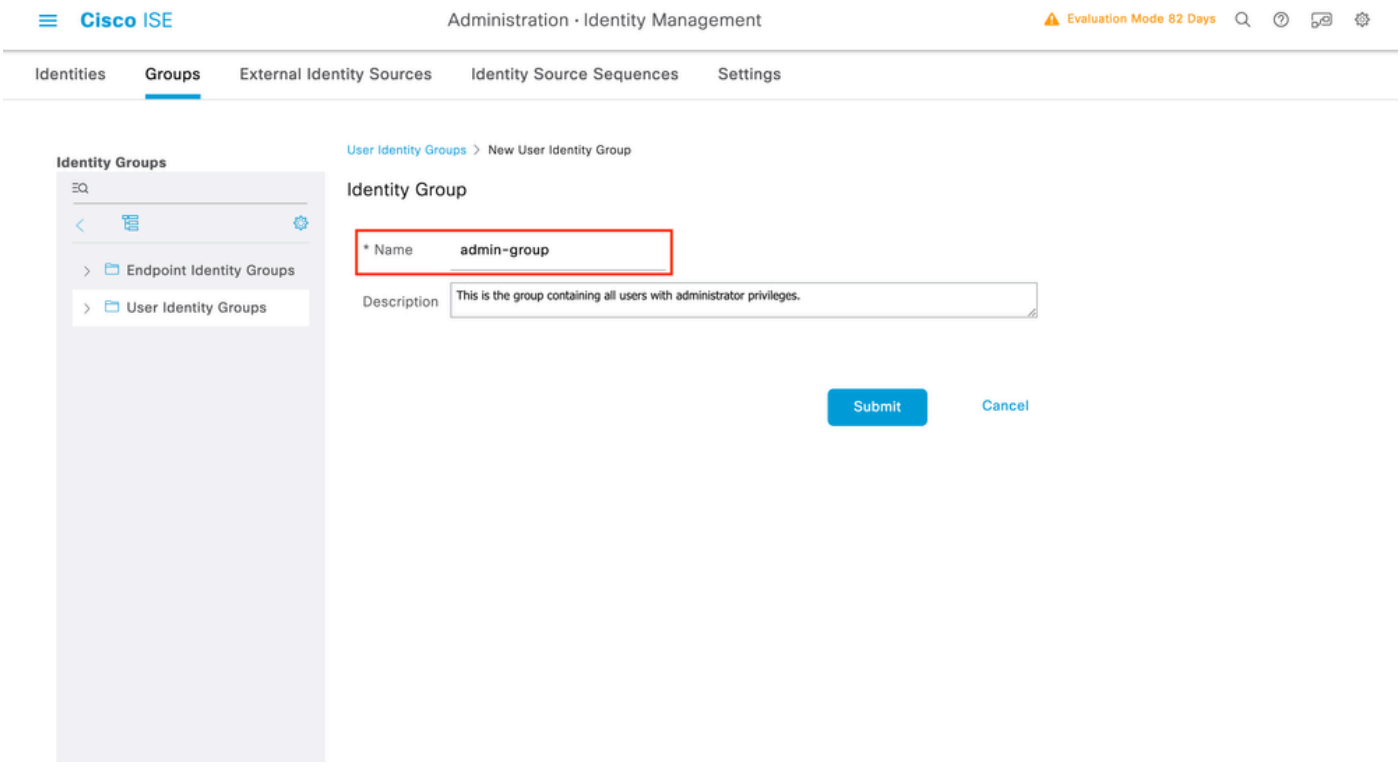
步驟3.在ISE上建立使用者組。

在 GUI 上：

ISE使用者組通過的使用者身份組頁籤建立Administration > Identity Management > Groups GUI Page，該頁籤顯示在螢幕捕獲中。



要建立新使用者，請使用「新增」按鈕，該按鈕將開啟新的使用者身份組配置表單，如圖所示。



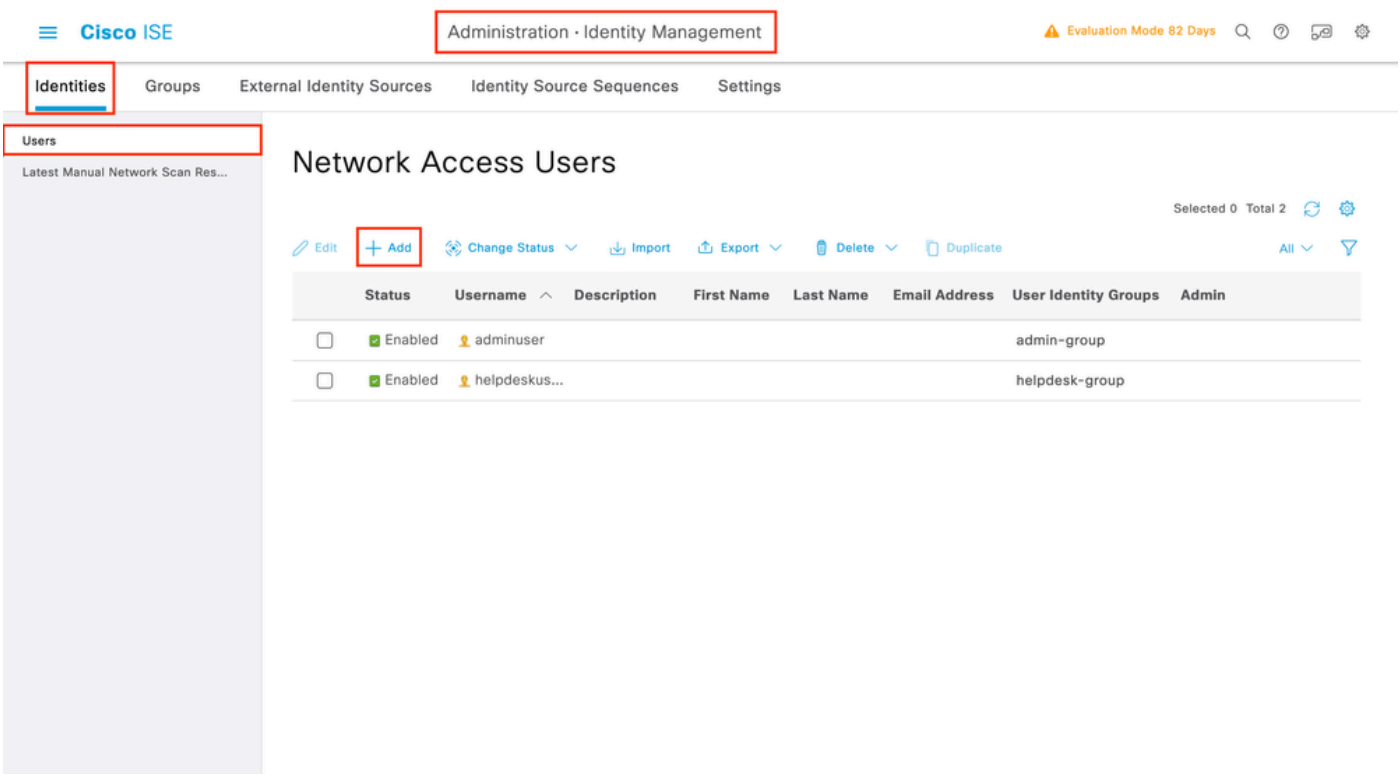
提供所建立的組的名稱。建立上述兩個使用者組，即admin-group 和helpdesk-group。

步驟4.在ISE上建立使用者。

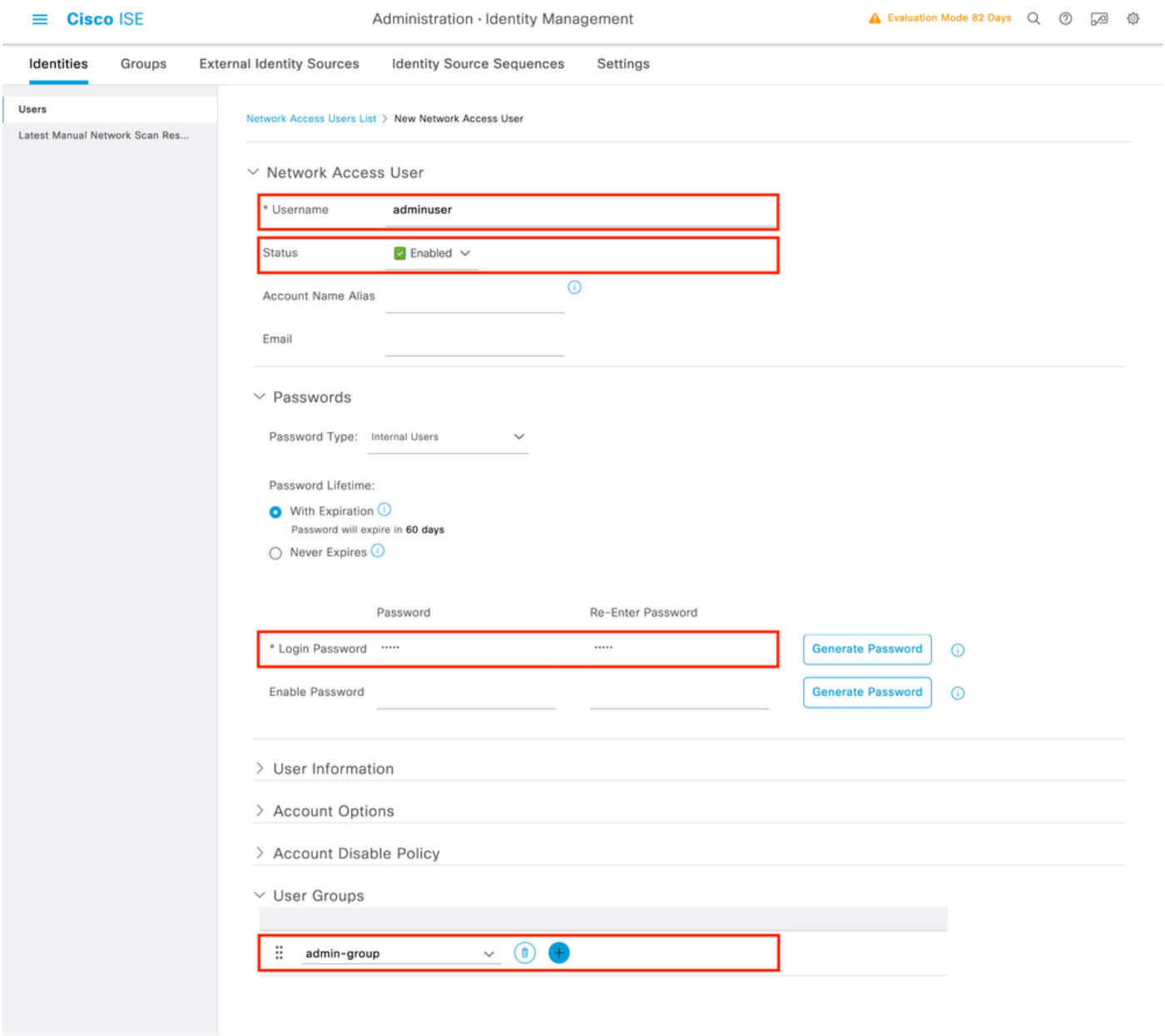
在 GUI 上：

ISE使用者從的Users頁籤建立Administration > Identity Management > Identities GUI Page，該頁籤顯示在螢幕捕獲

中。



要建立新使用者，請使用Add按鈕開啟新的網路訪問使用者配置表單，如圖所示。



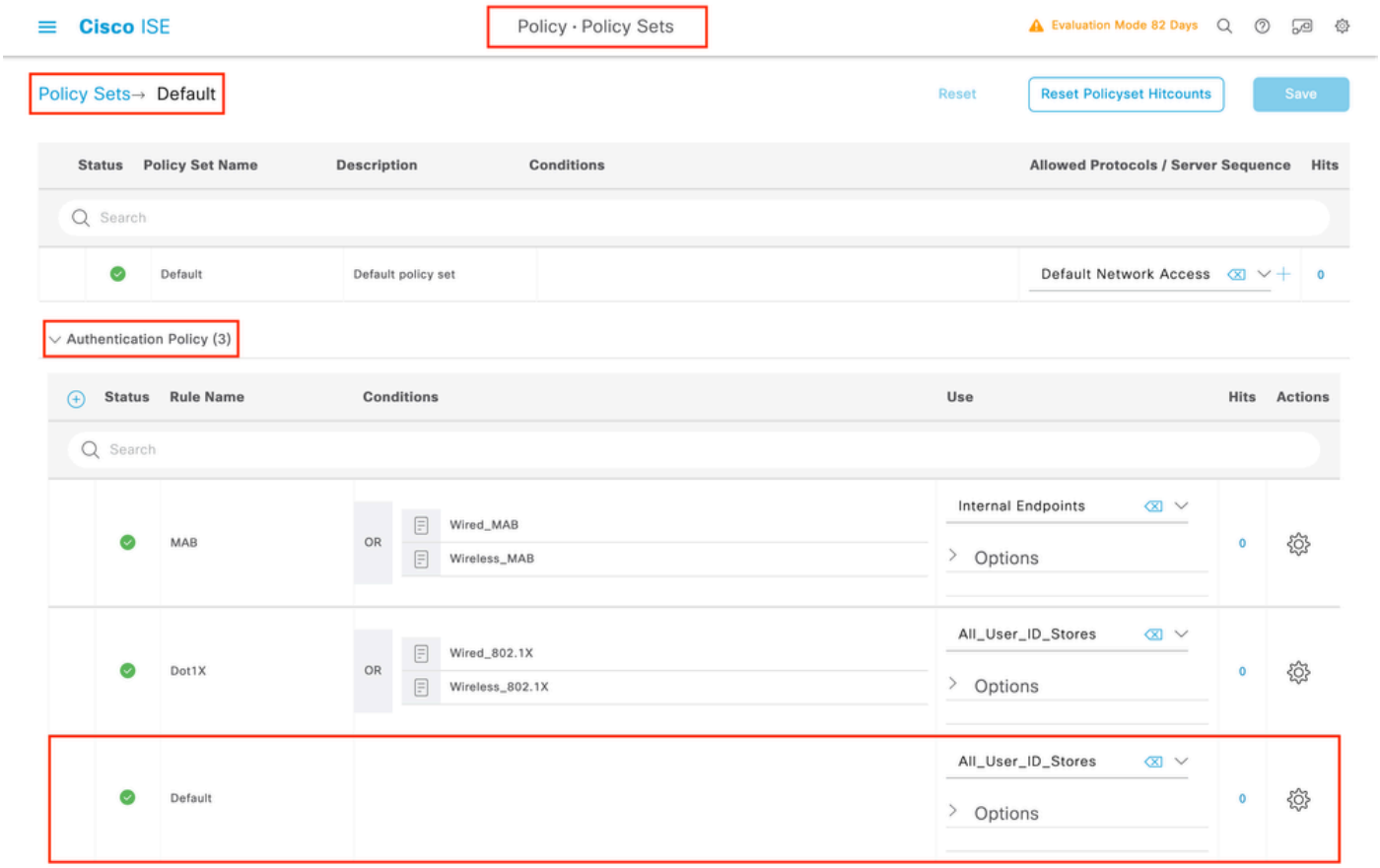
向使用者提供憑證，即使用者名稱和密碼，這些使用者名稱和密碼用於在WLC上進行驗證。此外，請確保使用者狀態為Enabled。最後，將使用者新增到其相關組（已在步驟4中建立），並在表單末尾使用User Groups下拉選單。

建立上述兩個使用者，即adminuser和helpdeskuser。

步驟5.驗證使用者身分。

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。可以從ISE GUI頁面的Policy > Policy Sets（如圖所示）檢視此策略集。因此，沒有必要對其進行更改。

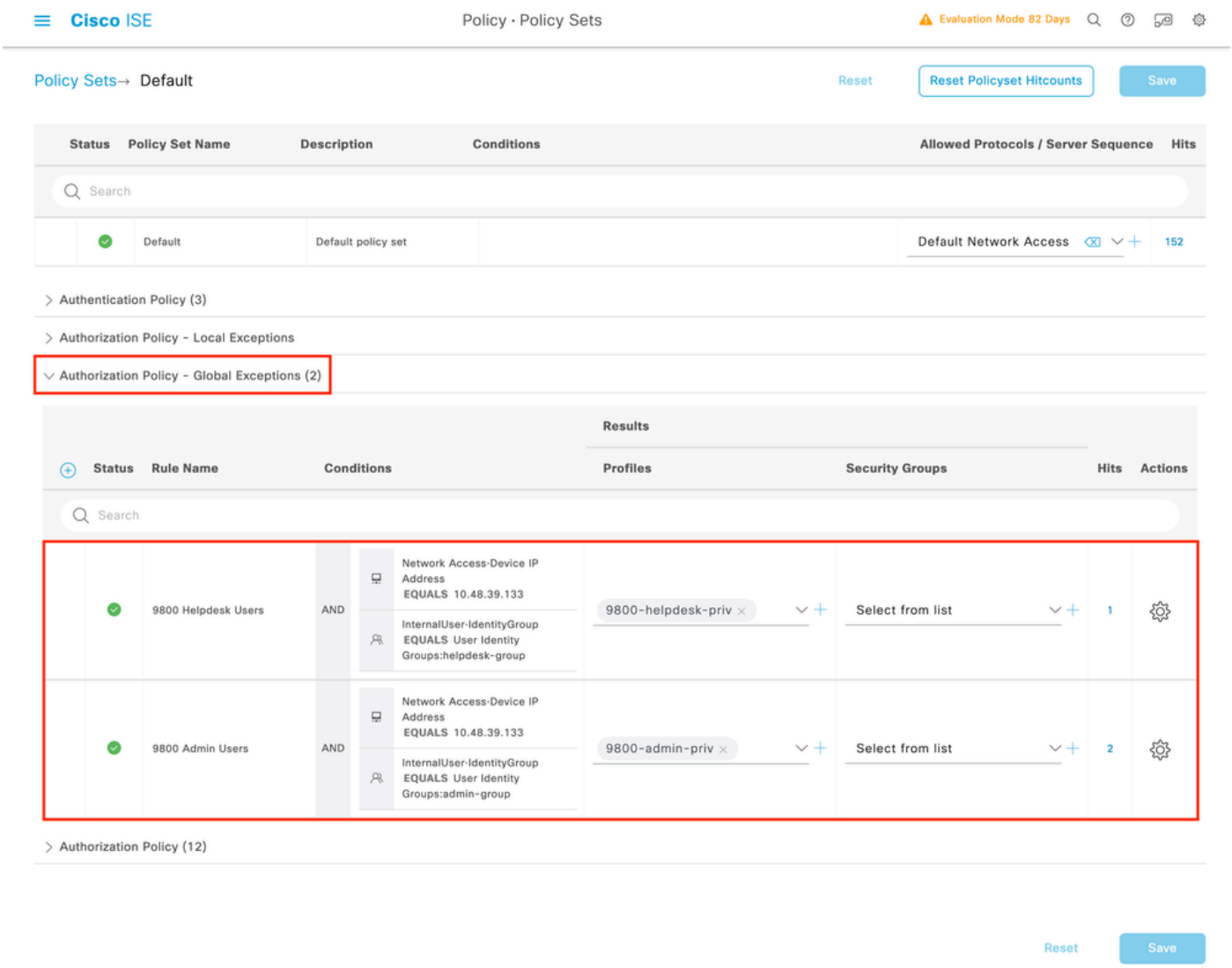


步驟6.授權使用者。

在 GUI 上：

在登入嘗試通過身份驗證策略後，需要對其進行授權，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）。

在此範例中，登入嘗試會根據裝置的IP位址（即WLC IP位址）進行過濾，並根據使用者所屬的群組區分要授予的許可權層級。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，每個組只包含單個使用者。



完成此步驟後，可用於在WLC中通過GUI或Telnet/SSH驗證為adminuser 和helpdesk（使用者）配置的憑證。

設定TACACS+ WLC

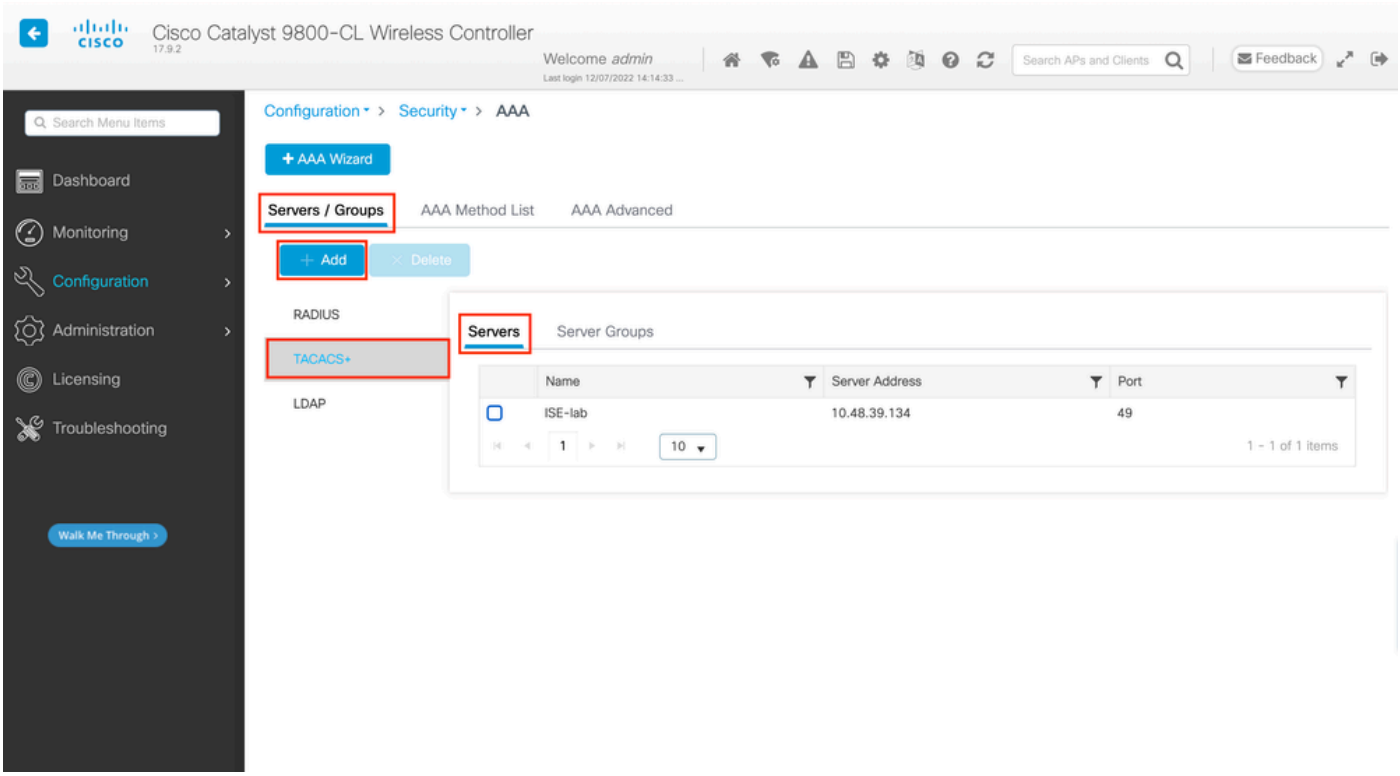
步驟1.宣告TACACS+伺服器。

在 GUI 上：

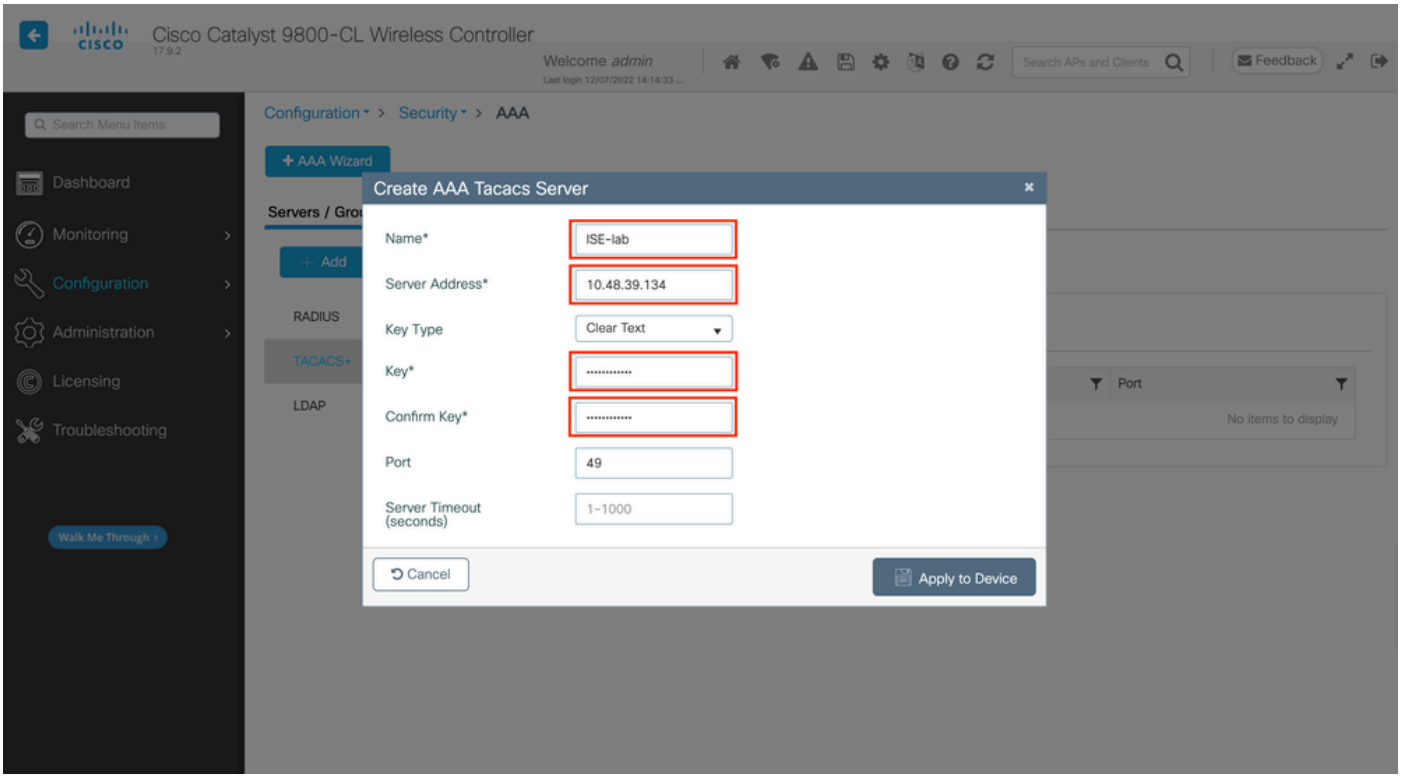
首先，在WLC上建立Tacacs+伺服器ISE。這可以從GUI WLC頁面(可在https://

/webui/#/aaa

中存取)的選項卡Servers/Groups > TACACS+ > Servers(Tab)中完成，如果您導航到Configuration > Security > AAA，如下圖所示。



要在WLC上新增TACACS伺服器，請按一下上圖中以紅色框示的Add按鈕。這將開啟所示的彈出視窗。



當彈出視窗開啟時，請提供伺服器名稱（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。

在此彈出視窗中，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帳的埠，但這些引數不是必填項，保留為本文檔的預設設定。

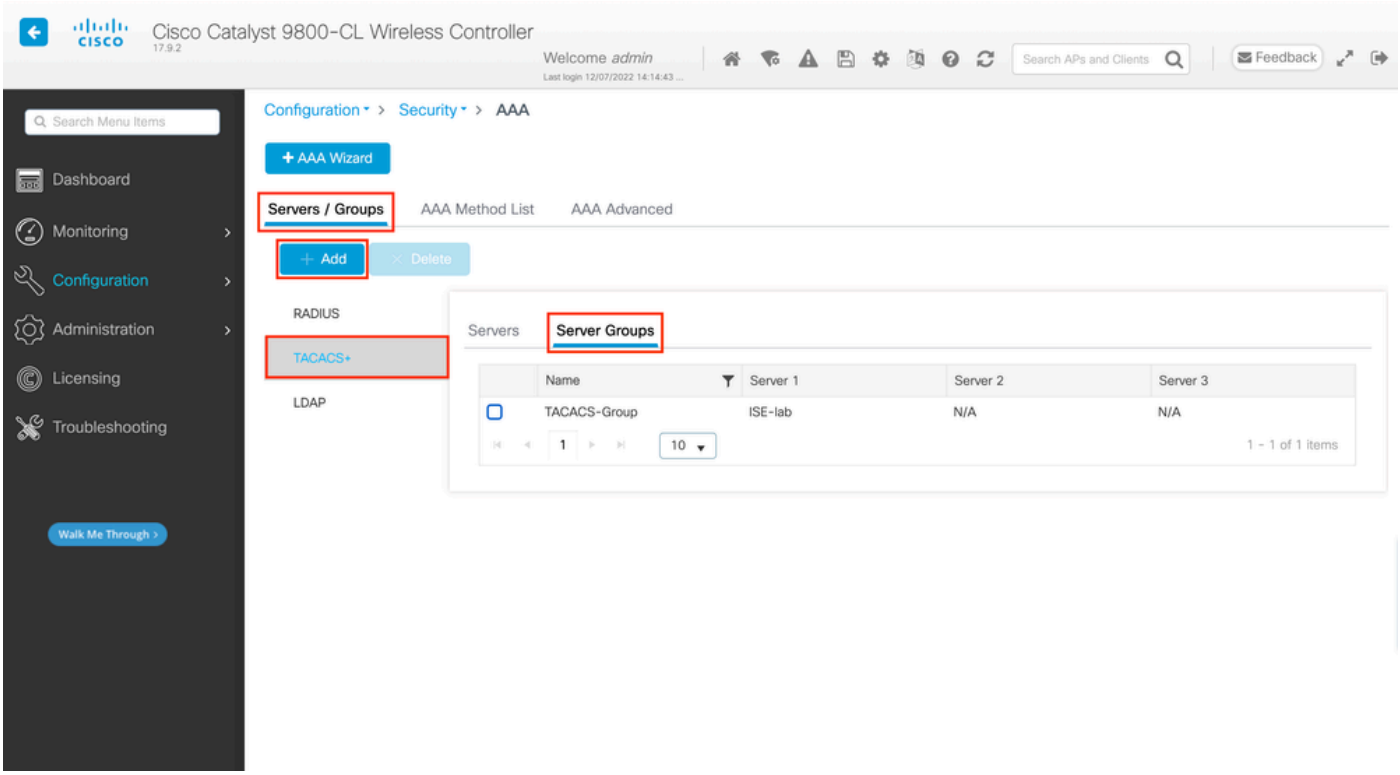
在 CLI 上：

```
<#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
```

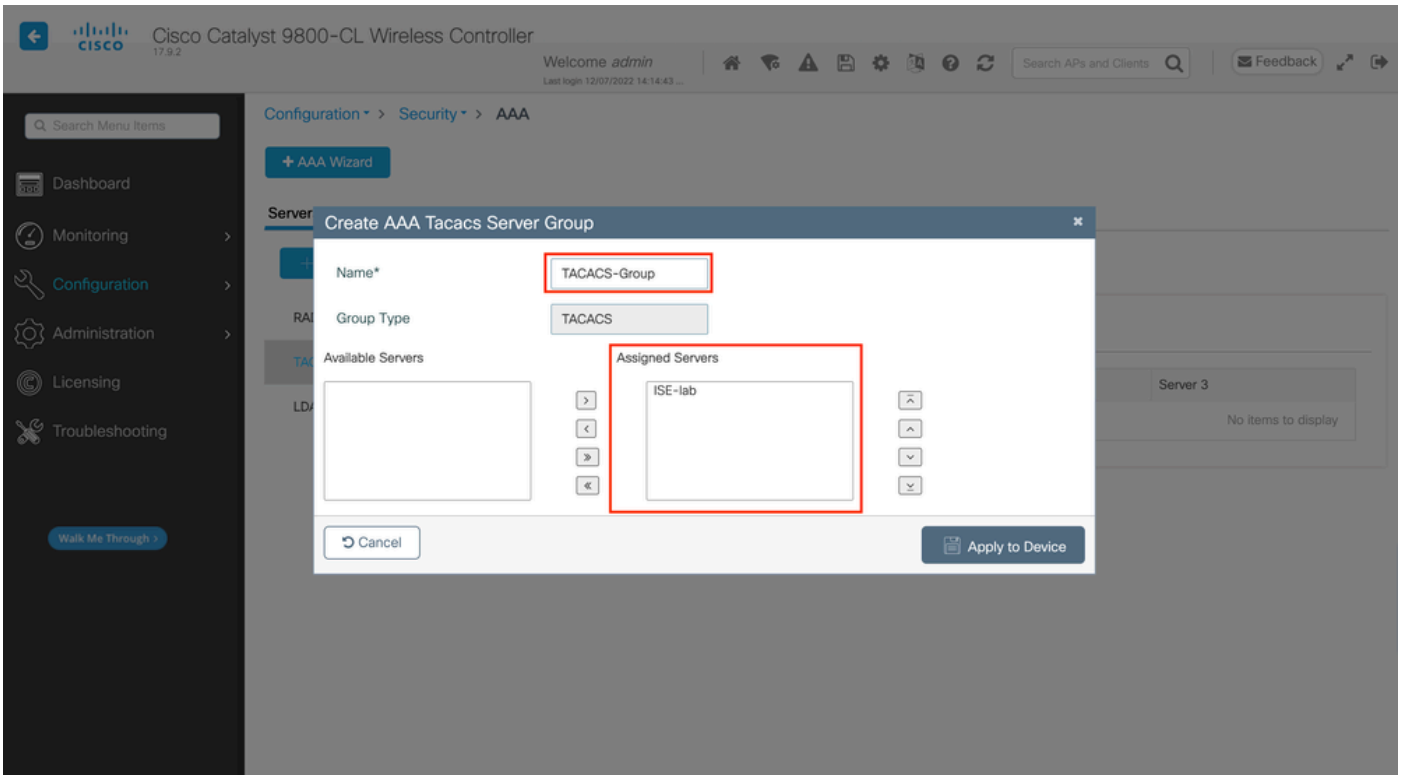
步驟2.將TACACS+伺服器對映到伺服器組。

在 GUI 上：

如果您有多台可用於身份驗證的TACACS+伺服器，建議將所有這些伺服器對映到同一個伺服器組。然後，WLC負責在伺服器組中的伺服器之間平衡不同身份驗證的負載。TACACS+服務器組是在與步驟1中提到的GUI頁面相同Servers/Groups > TACACS > Server Groups（如下圖所示）的GUI頁面上從標籤中設定。



對於伺服器建立，當您按一下前面影象（如圖所示）中框的Add按鈕時，將出現一個彈出視窗。



在彈出視窗中，為組指定一個名稱，並將所需的伺服器移動到「分配的伺服器」清單中。

在 CLI 上：

```
<#root>

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

TACACS-Group

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

ISE-lab
```

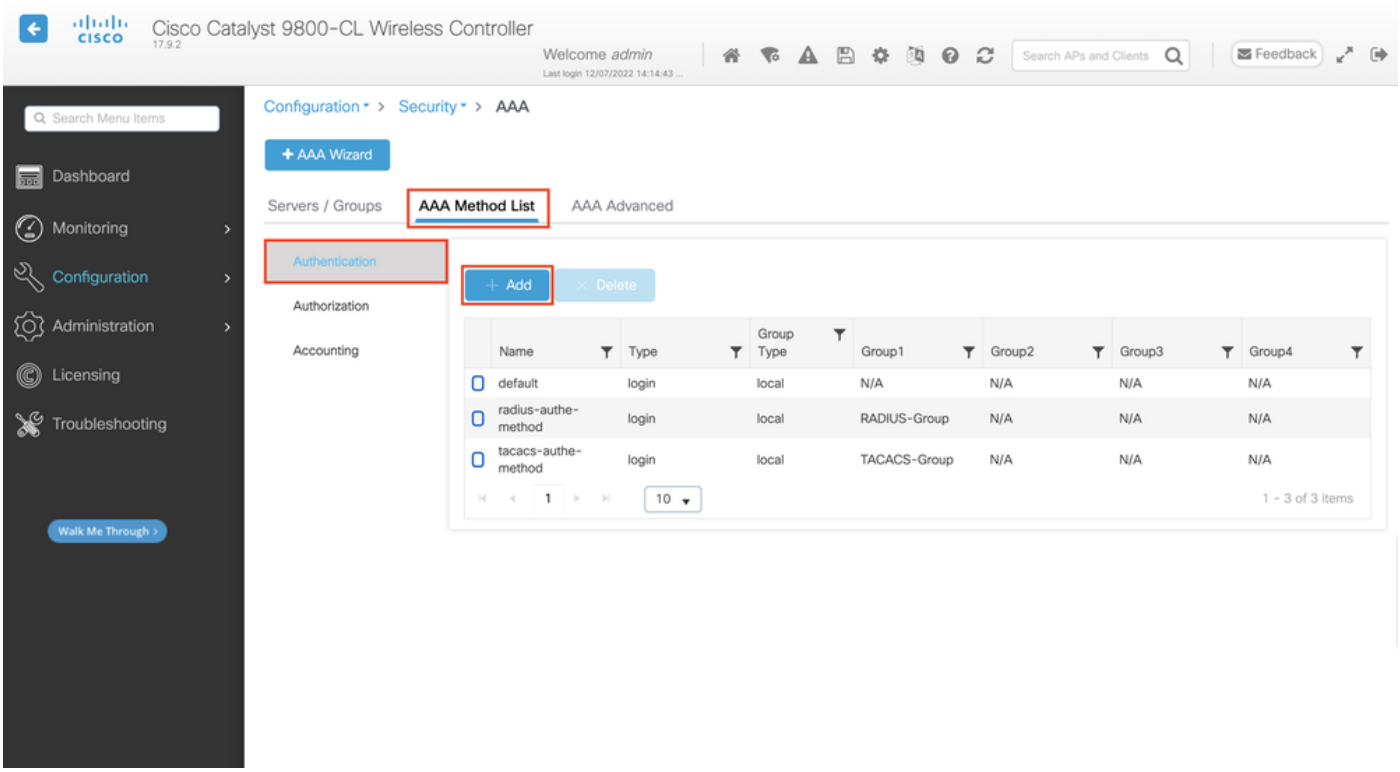
步驟3.建立指向TACACS+伺服器組的AAA身份驗證登入方法。

在 GUI 上：

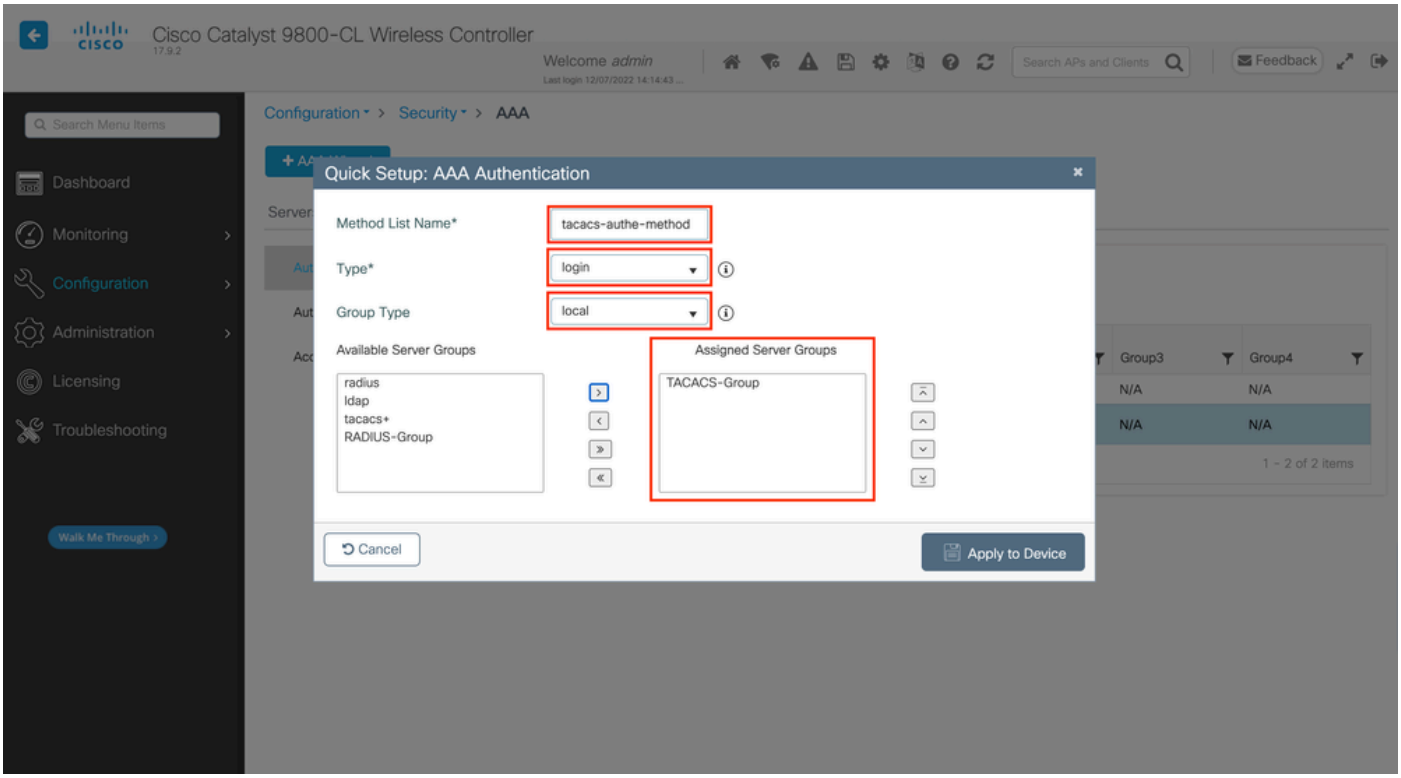
仍可在GUI頁面https://

/webui/#/aaa

，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Add按鈕建立身份驗證方法時，會出現一個配置彈出視窗，類似於本圖中所示的視窗。



在此彈出視窗中，提供方法的名稱，選擇Type aslogin，並將上一步中建立的組伺服器新增到Assigned Server Groups清單中。對於Group Type欄位，可能有幾種配置。

- 如果您選擇「組型別」作為「本地」，WLC會首先檢查使用者憑證是否存在於本地，然後回退到伺服器組。
- 如果您選擇「組型別」作為組並且沒有選中「回退到本地」選項，WLC只會針對伺服器組檢查使用者憑據。
- 如果選擇「組型別」作為組並選中「回退到本地」選項，則WLC會針對伺服器組檢查使用者

憑據，並僅在伺服器沒有響應時才查詢本地資料庫。如果伺服器傳送拒絕消息，則使用者將被驗證，即使該使用者可能存在於本地資料庫中。

在 CLI 上：

如果希望只有在首先在本地找不到使用者憑據時，才使用伺服器組檢查使用者憑據，請使用：

```
<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

 local group

TACACS-Group
```

如果希望僅對伺服器組檢查使用者憑據，請使用：

```
<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

 group

TACACS-Group
```

如果希望對伺服器組檢查使用者憑據，並且最後未對本地條目作出響應，請使用：

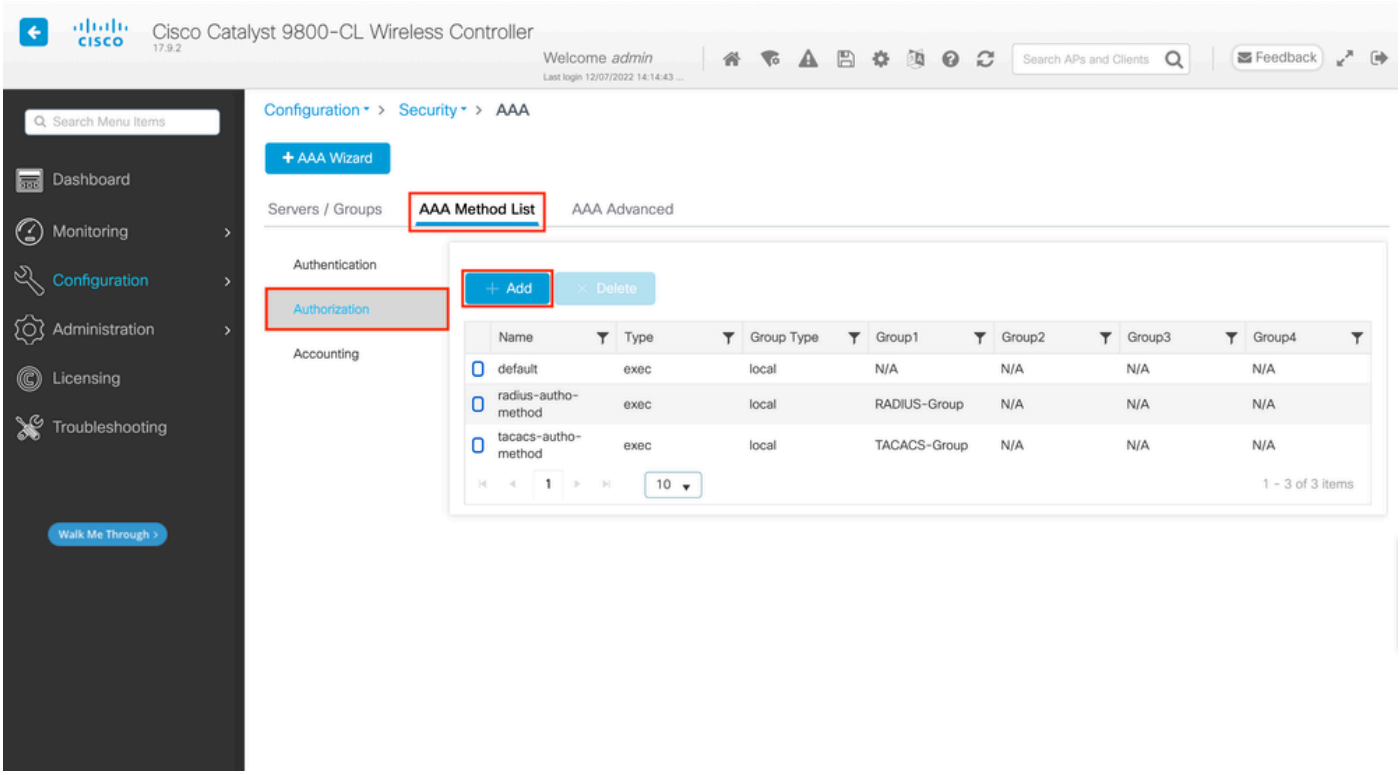
```
<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-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。

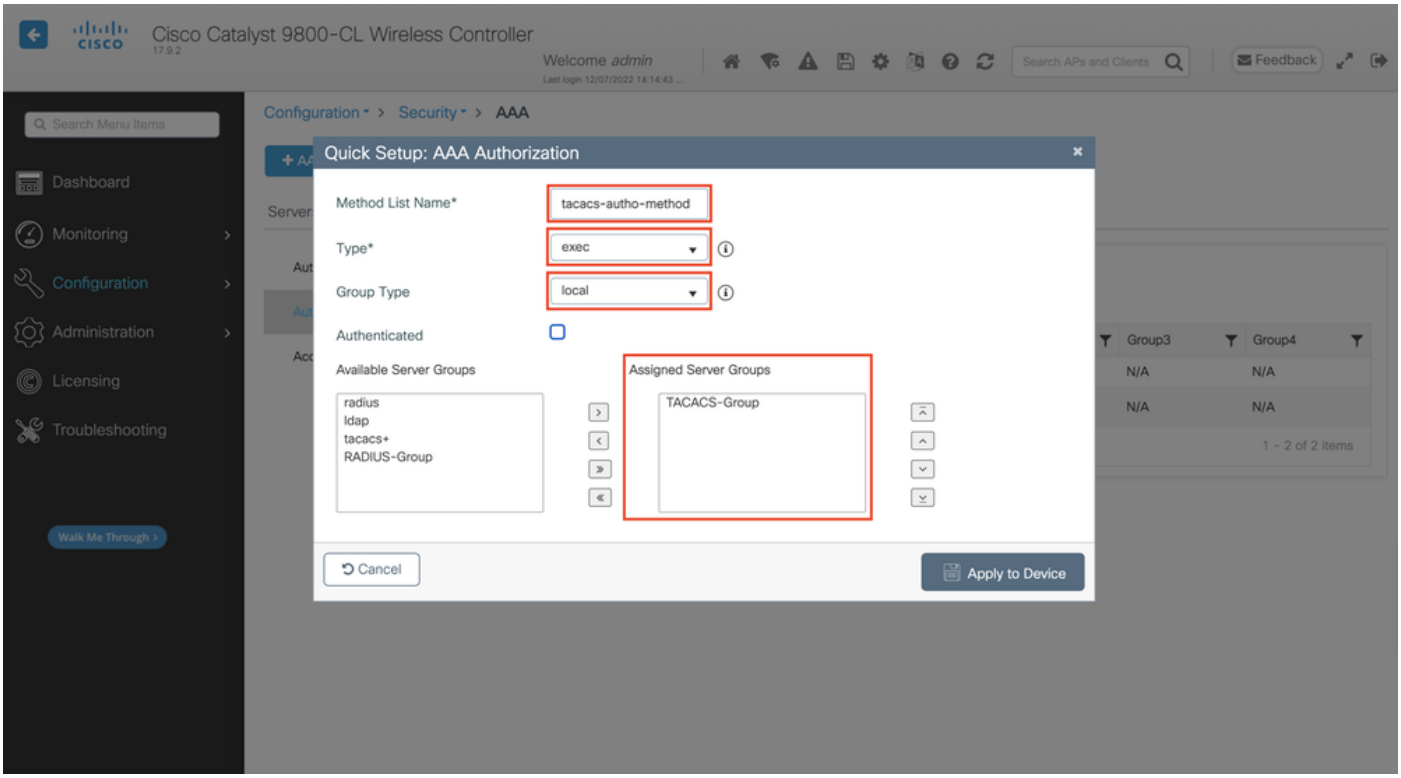
步驟4.建立指向TACACS+伺服器群組的AAA授權exec方法。

在 GUI 上：

使用者還必須獲得授權才能獲得訪問許可權。仍然在GUI頁面Configuration > Security > AAA，導航到「AAA Method List > Authorization」頁籤，然後建立授權方法，如下圖所示。



當您使用「新增」按鈕新增新授權方法時，將出現一個與所示的授權方法配置類似的彈出式視窗。



在此配置彈出視窗中，提供授權方法的名稱，選擇exec「型別」作為，並使用與上一步中身份驗證方法相同的組型別順序。

在 CLI 上：

```
<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

 local group

TACACS-Group
```

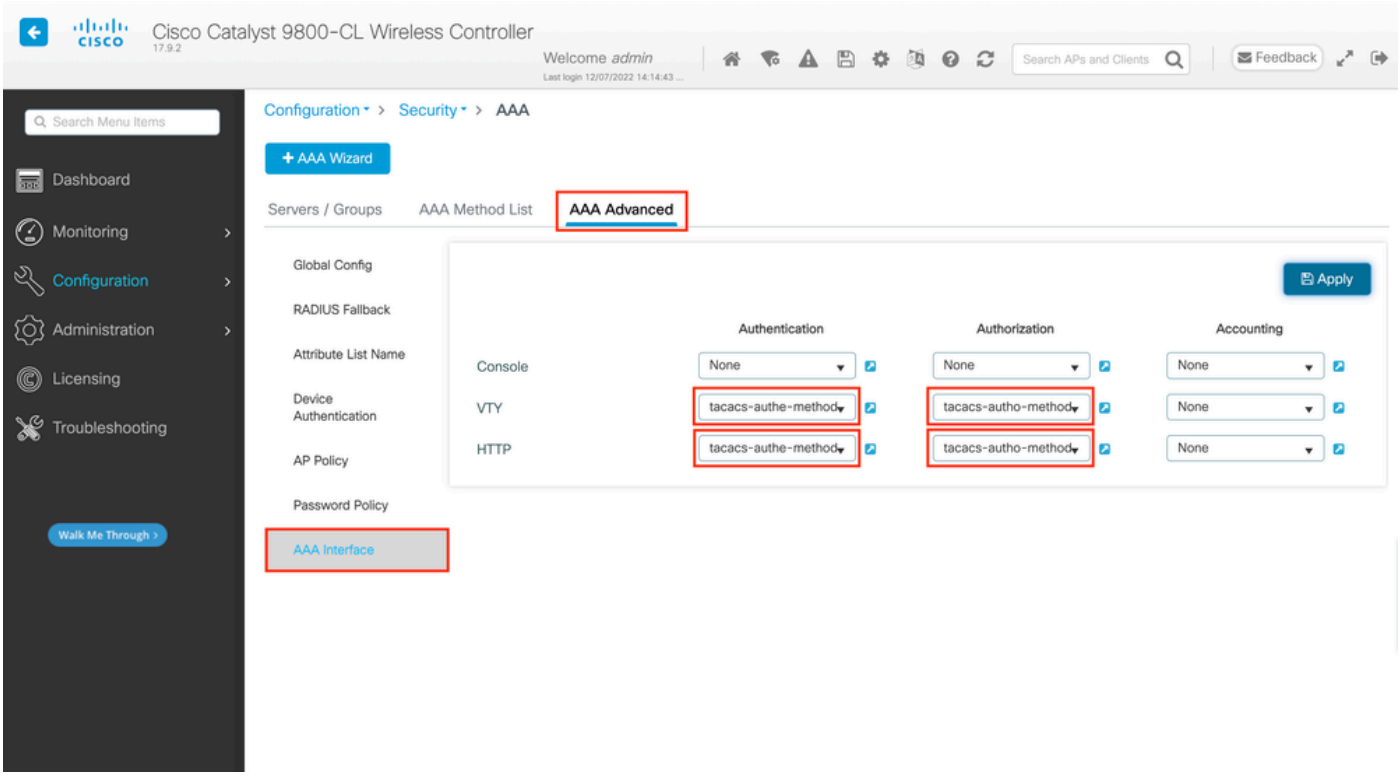
步驟5.將方法分配給HTTP配置以及用於Telnet/SSH的VTY線路。

在 GUI 上：

建立的驗證和授權方法可用於HTTP和/或Telnet/SSH使用者連接，可在GUI WLC頁面的AAA Advanced > AAA Interface https://

/webui/#/aaa

(仍可在GUI WLC頁面上設定，如下圖所示。



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。可以使用這些命令實現這一點。

```
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
```

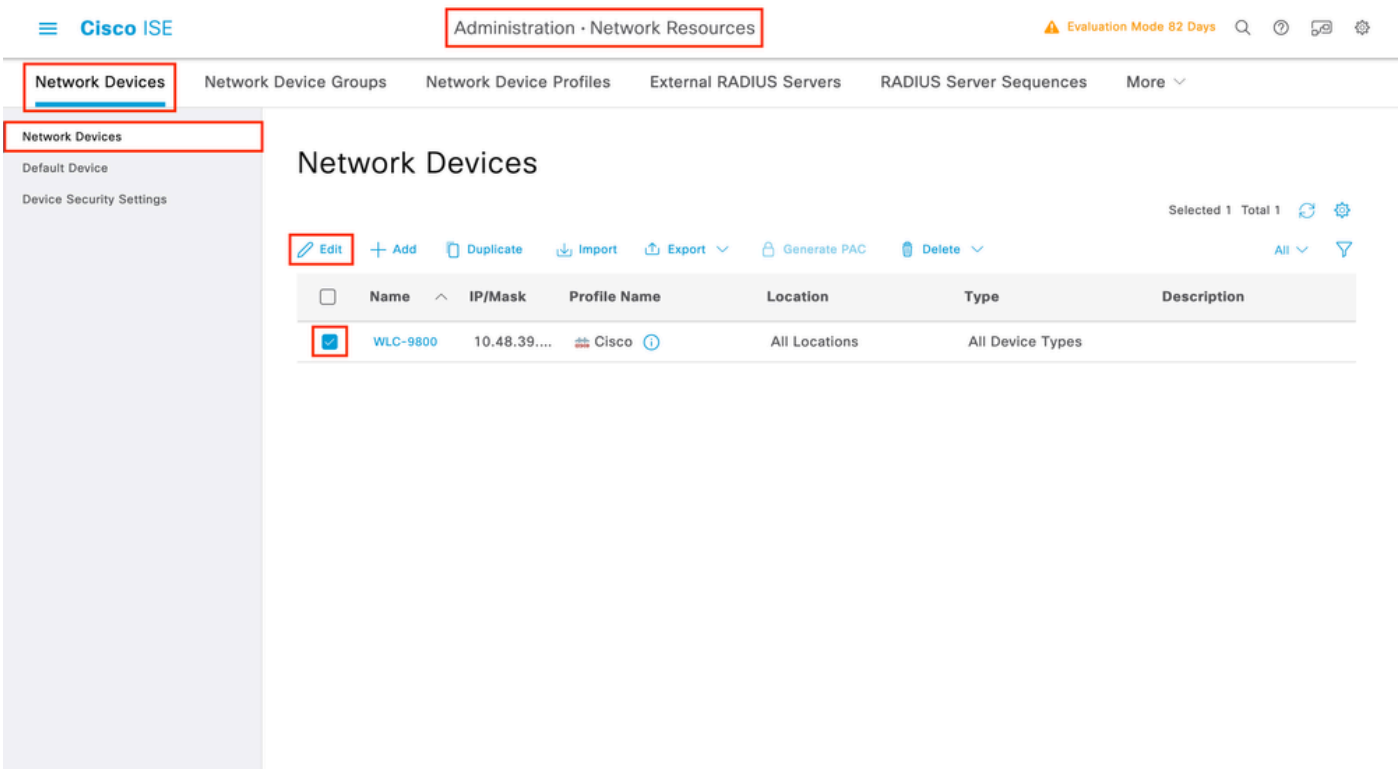
TACACS+ ISE配置

步驟1.將WLC配置為TACACS+的網路裝置。

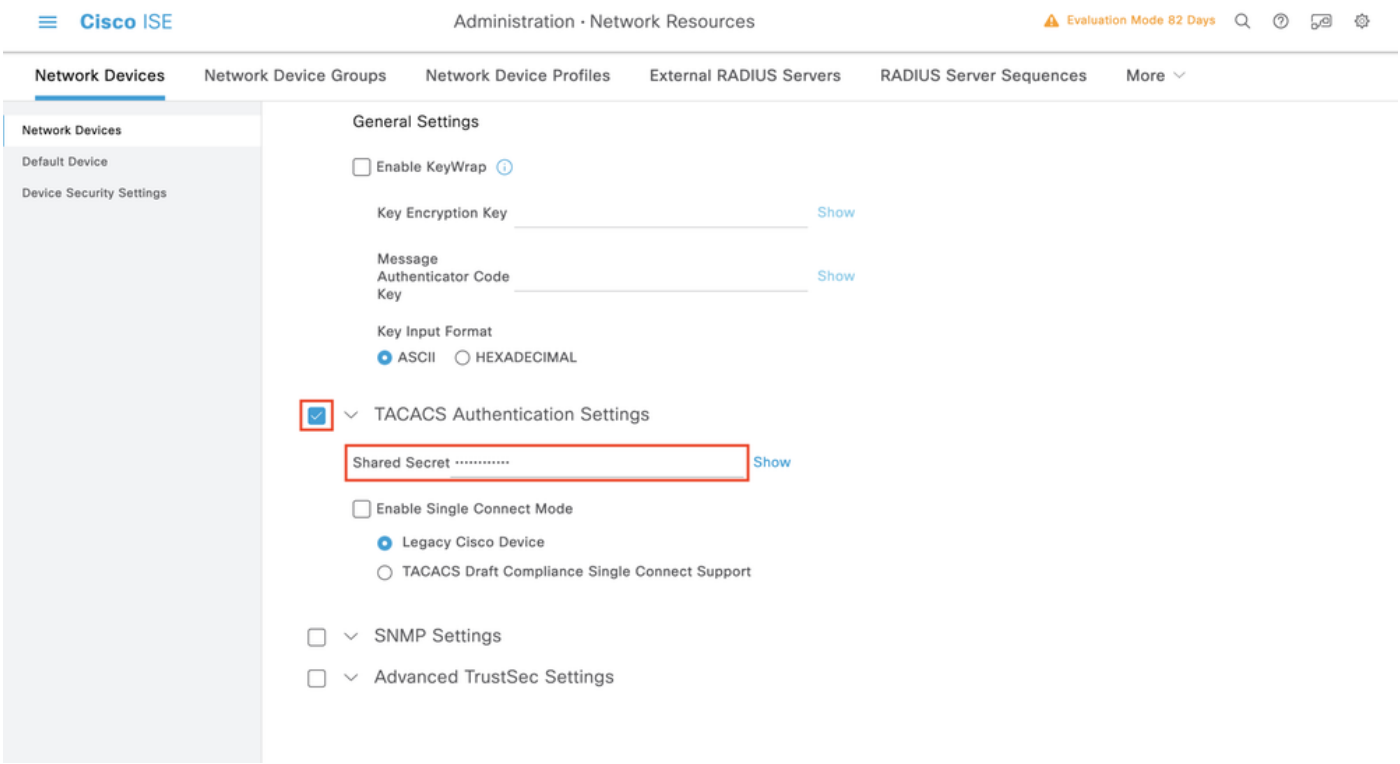
在 GUI 上：

若要將上節中使用的WLC宣告為ISE中RADIUS的網路裝置，請導覽至Administration > Network Resources > Network

Devices，然後開啟Network devices頁籤，如下圖所示。

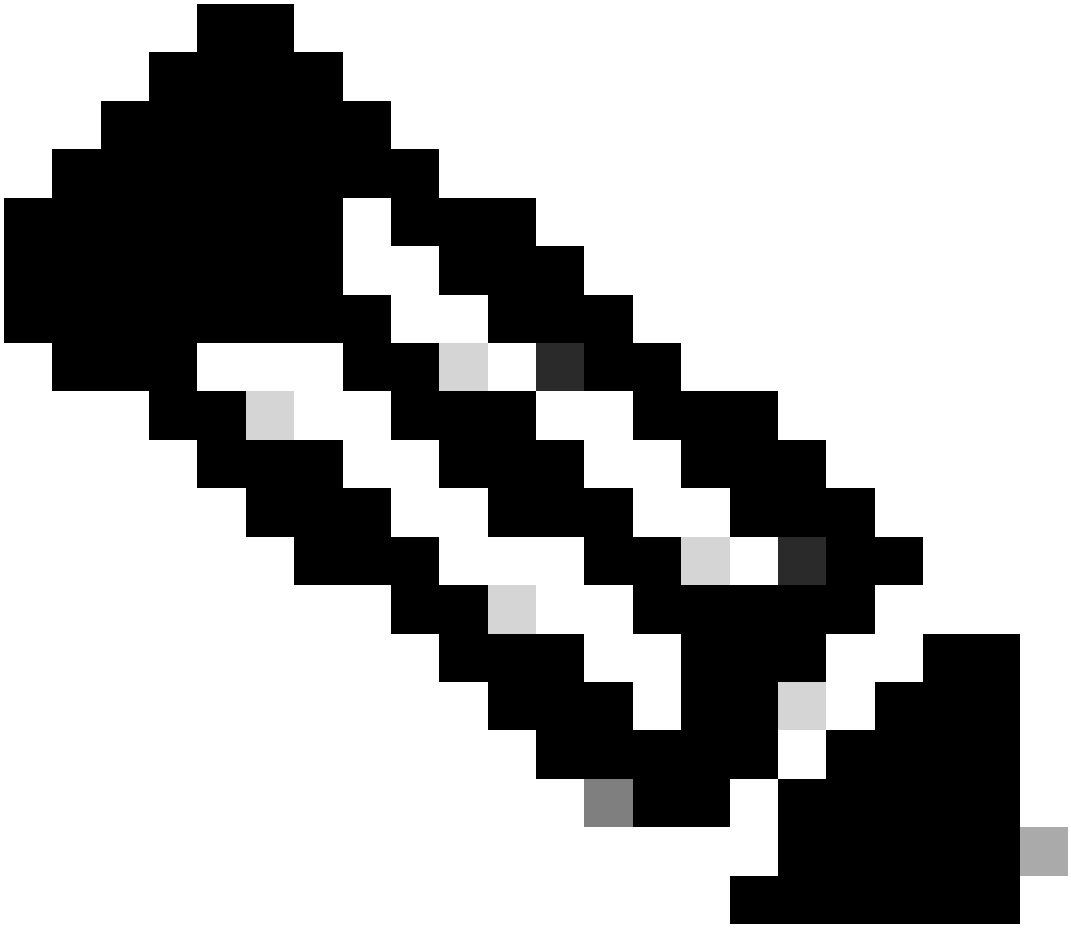


在本示例中，已為RADIUS身份驗證新增了WLC(請參閱配置RADIUS ISE一節的步驟1。) 因此，只需修改其配置即可配置TACACS身份驗證，當您在網路裝置清單中選擇WLC並點選Edit按鈕時，即可完成此操作。這將開啟網路裝置配置表單，如下圖所示。



開啟新視窗後，向下滾動到配置TACACS+ WLC部分的「TACACS身份驗證設定」部分，啟用這些設定，並新增在步驟1中輸入的共用金鑰。

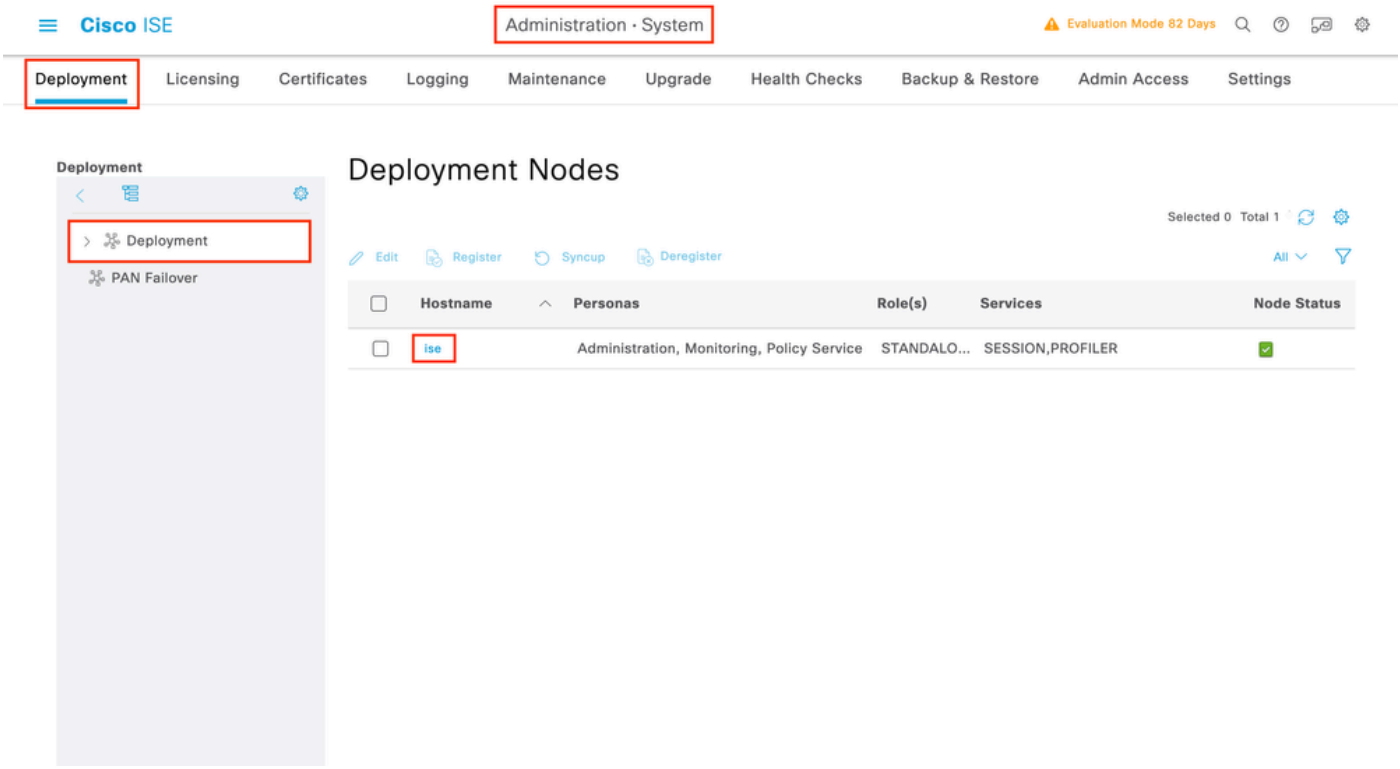
步驟2.為節點啟用Device Admin功能。



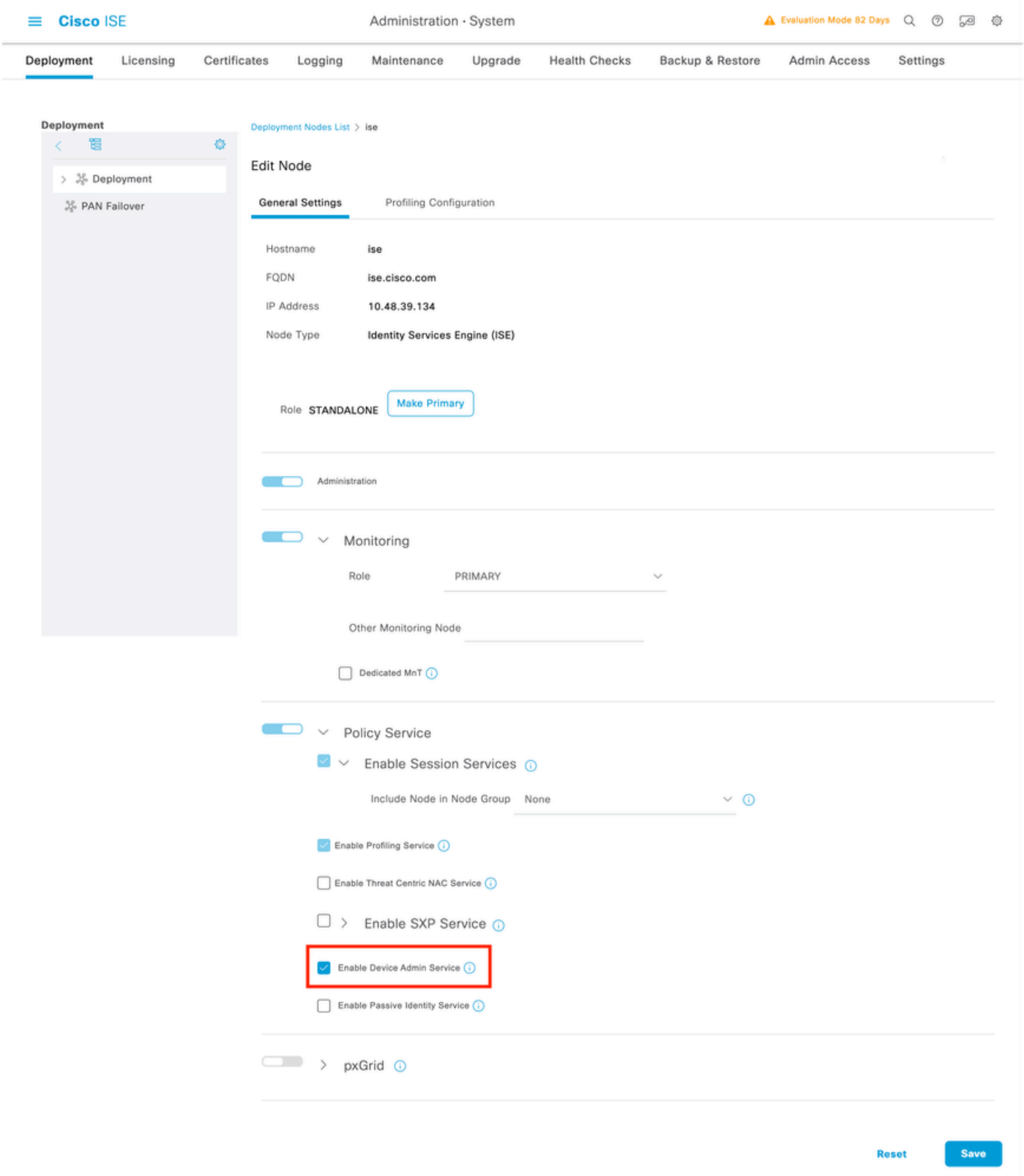
附註：要使用ISE作為TACACS+伺服器，您必須擁有裝置管理許可證包以及基本許可證或移動許可證。

在 GUI 上：

安裝裝置管理許可證後，必須為節點啟用Device Admin功能，才能使用ISE作為TACACS+伺服器。為此，請編輯使用的ISE部署節點的配置(可在Administrator > Deployment下找到)，然後按一下其名稱或使用Edit「幫助」按鈕。



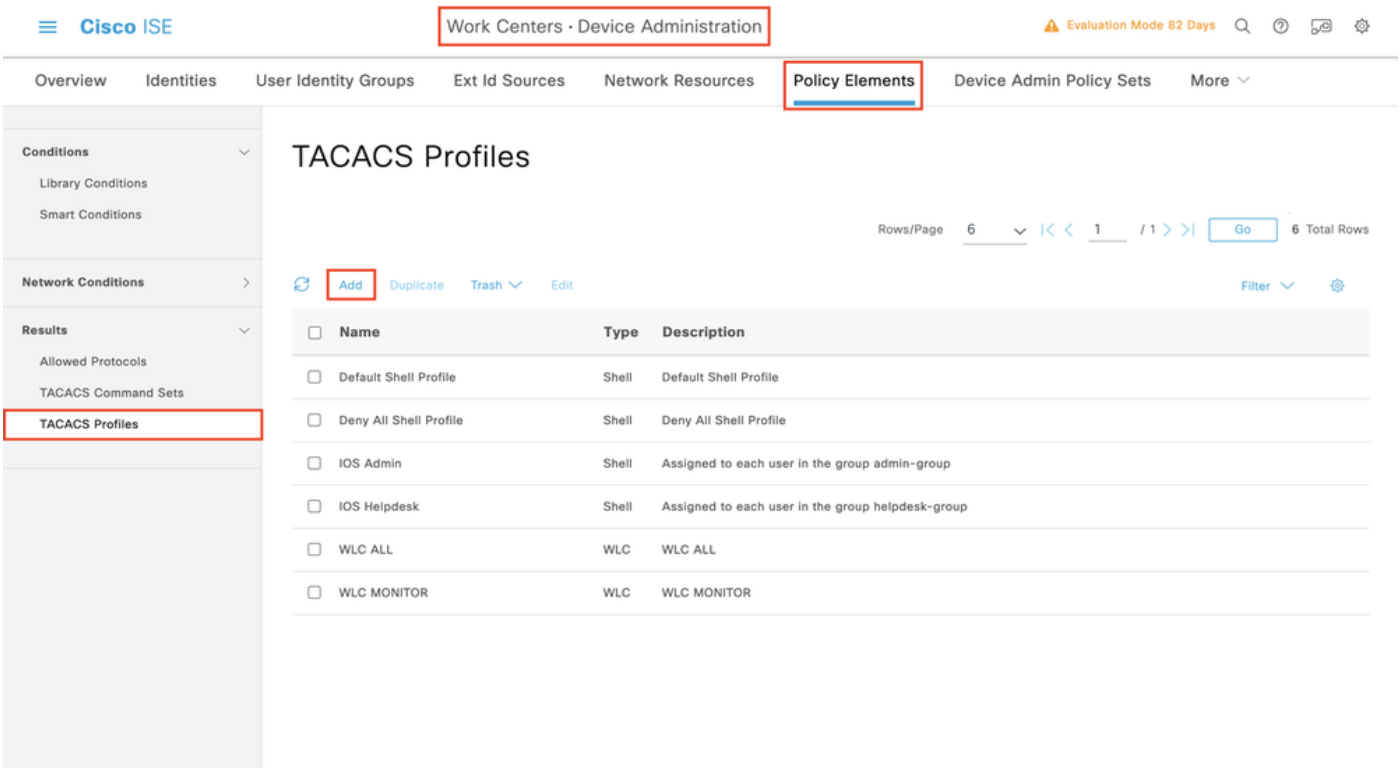
開啟節點配置視窗後，選中Policy Service部分下的Enable Device Admin Service選項，如下圖所示。



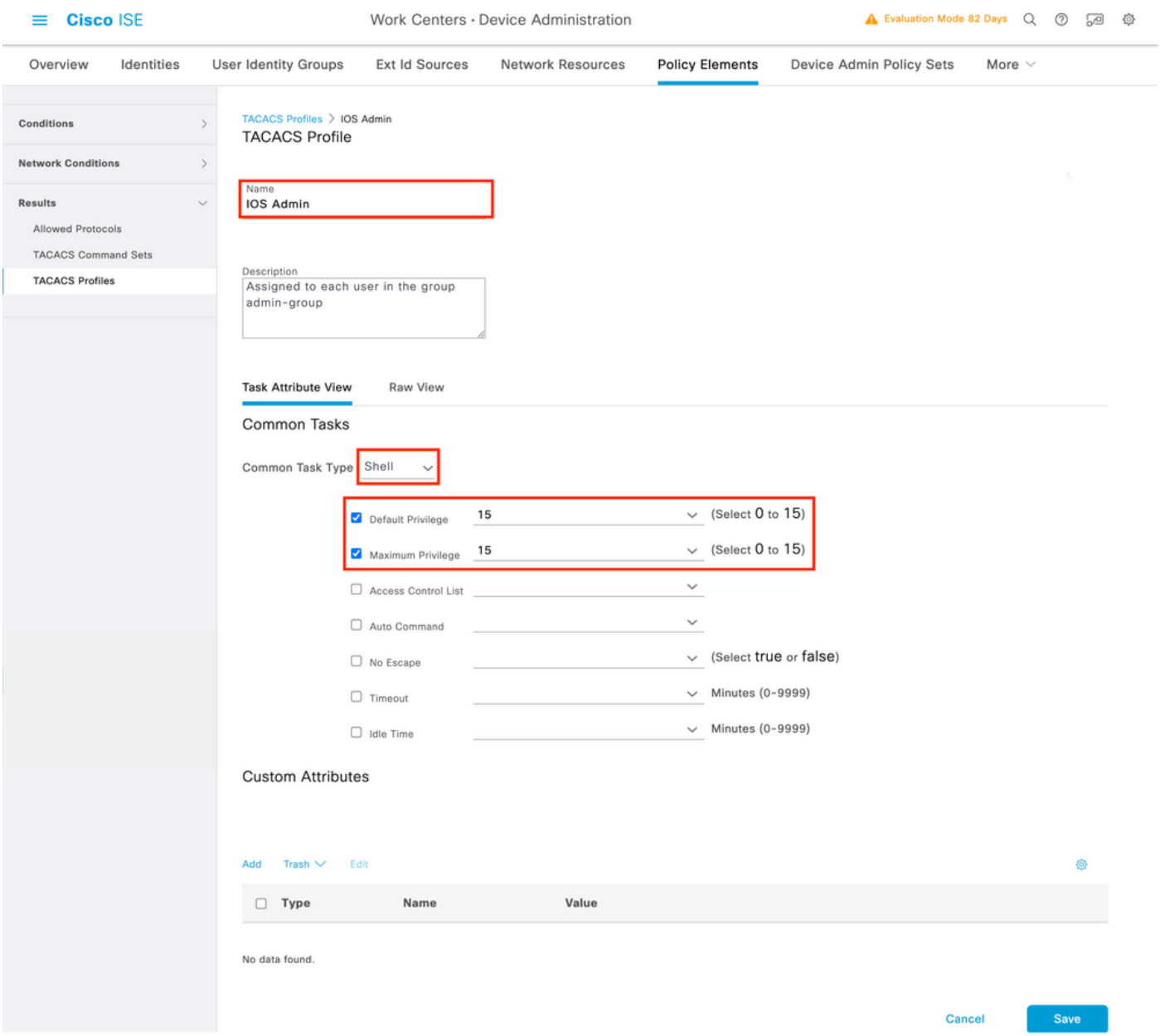
步驟3.建立TACACS配置檔案，以返回許可權。

在 GUI 上：

要具有管理員訪問許可權，需要具有adminuser15的許可權級別，該級別允許訪問exec提示外殼。另一方面，不需要exec提示外殼訪問，因此可以分配許可權級別低於helpdeskuser15的許可權級別。為了向使用者分配正確的許可權級別，可以使用授權配置檔案。可從ISE GUI頁面(頁籤下Work Centers > Device Administration > Policy Elements)配置Results > TACACS Profiles，如下圖所示。



若要設定新的TACACS設定檔，請使用「Add」按鈕，此按鈕會開啟與圖中所示設定表單類似的新設定檔設定表單。此表單在配置分配給的配置檔案(即，外殼許可權級別為adminuser15)時，必須特別如下所示。



對配置檔案重複該操作helpdesk。對於最後一個，預設許可權和最大許可權都設定為1。

步驟4.在ISE上建立使用者組。

這與本文檔的配置RADIUS ISE一節的步驟3中提供的相同。

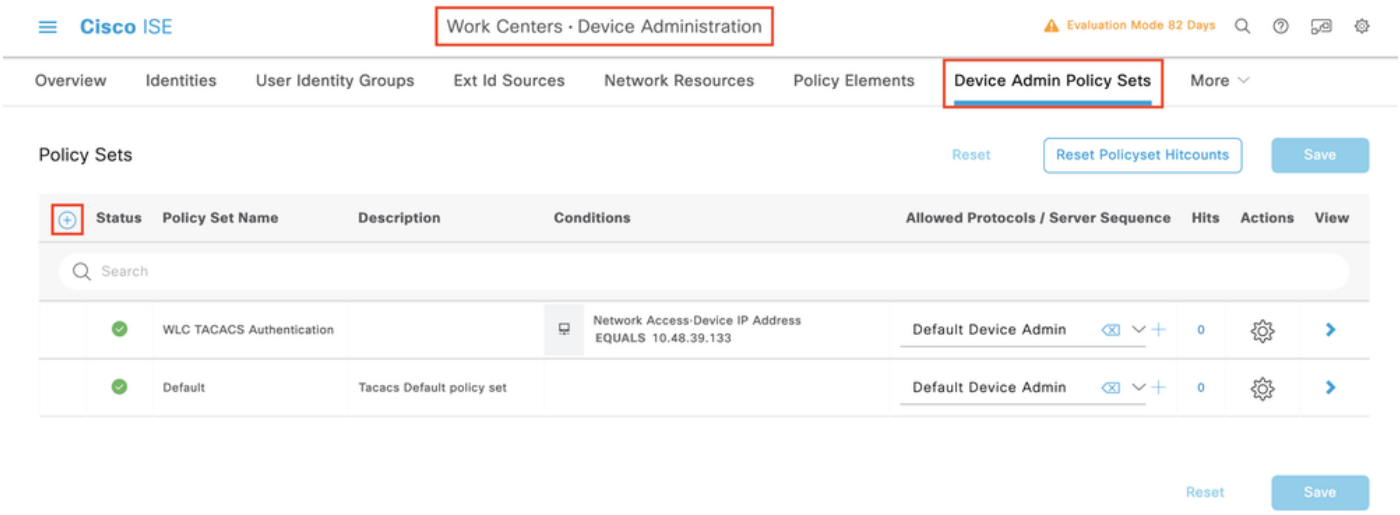
步驟5.在ISE上建立使用者。

這與本文檔的配置RADIUS ISE一節的步驟4中提供的相同。

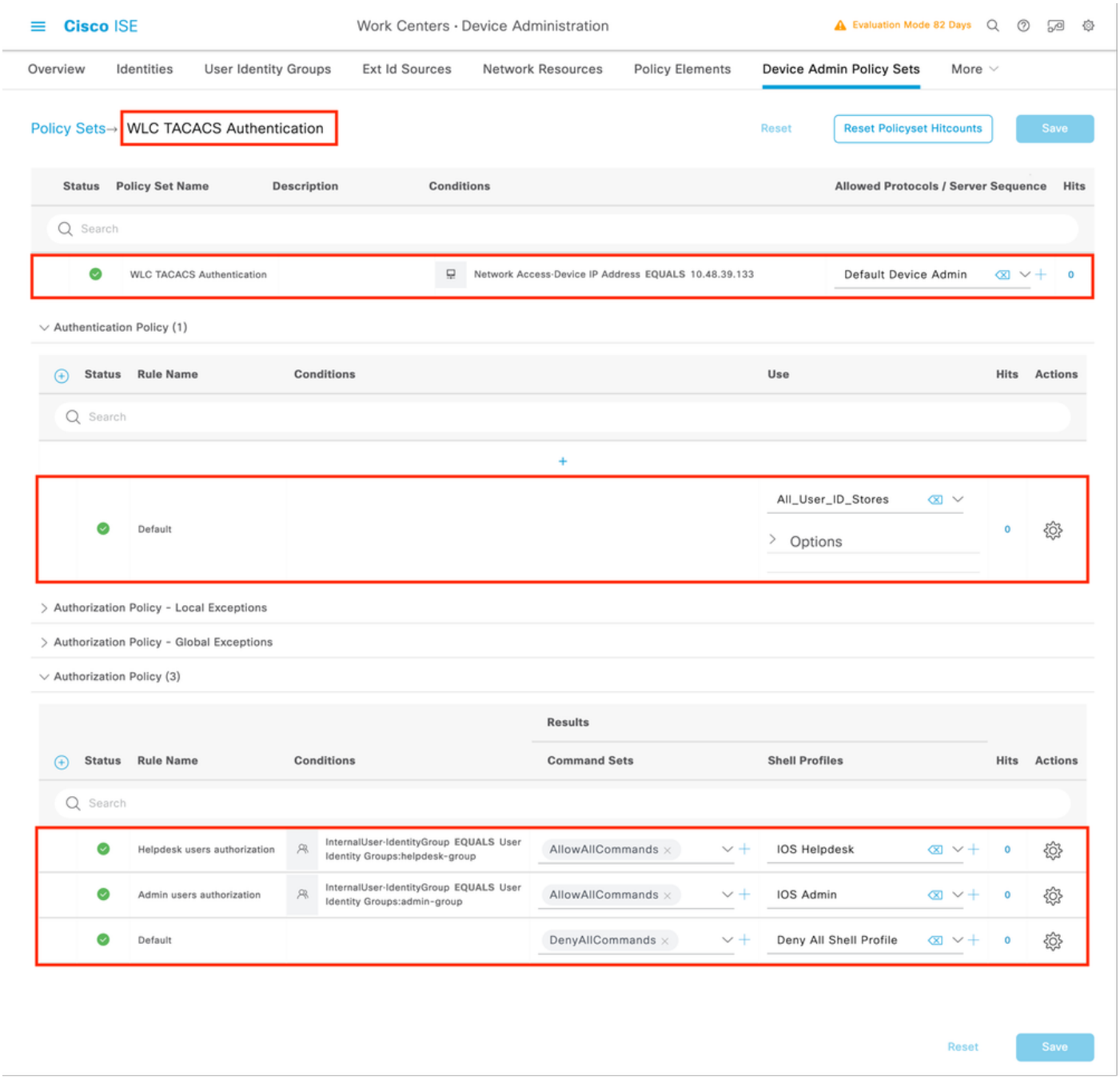
步驟6.建立裝置管理策略集。

在 GUI 上：

對於RADIUS訪問，使用者一旦建立，其身份驗證和授權策略仍需要在ISE上定義，以便授予其正確的訪問許可權。TACACS身份驗證使用裝置管理策略集來達到該目的，可以從進行配置Work Centers > Device Administration > Device Admin Policy Sets GUI Page，如下所示。



要建立裝置管理策略集，請使用上一映像中紅色框架的「新增」按鈕，這會將專案新增到策略集清單中。為新建立的集提供一個名稱、必須應用該集的條件以及允許的協定/伺服器序列(此處，Default Device Admin足)。 使用Save按鈕完成策略集的新增，並使用其右側的箭頭來訪問其配置頁面（如圖中所示）。



本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，因為它滿足了使用者的需求。已設定兩個授權規則：

- 當使用者屬於定義的組時，會觸發第一個選項admin-group。它允許所有命令(通過預設規則Permit_all)並分配許可權15(通過定義的IOS_Admin TACACS配置檔案)。
- 第二個選項在使用者屬於定義的組helpdesk-group(通過預設規Permit_all IOS_Helpdesk則)時觸發。它允許所有命令，並分配許可權1(通過定義的TACACS配置檔案)。

完成此步驟後，可用於在WLC中透過GUI或Telnet/SSH驗證為adminuser和helpdesk(US)設定的憑證。

疑難排解

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

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

通過WLC CLI對WLC GUI或CLI RADIUS/TACACS+訪問進行故障排除

若要疑難排解對WLC GUI或CLI的TACACS+存取問題，請發出debug tacacs命令以及終端監控器1，並在嘗試登入時檢視實際輸出。

例如，成功登入後註銷使用者會生成adminuser此輸出。

```
<#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: processing authentication start request id 15465
Dec 8 11:38:34.685: TPLUS: Authentication start packet created for 15465(adminuser)
Dec 8 11:38:34.685: TPLUS: Using server 10.48.39.134
Dec 8 11:38:34.685: TPLUS(00003C69)/0/NB_WAIT/7FD29013CA68: Started 5 sec timeout
Dec 8 11:38:34.687: TPLUS(00003C69)/0/NB_WAIT: socket event 2
Dec 8 11:38:34.688: TPLUS(00003C69)/0/NB_WAIT: wrote entire 45 bytes request
Dec 8 11:38:34.688: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:34.688: TPLUS(00003C69)/0/READ: Would block while reading
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 15 bytes data)
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: read entire 27 bytes response
Dec 8 11:38:34.701: TPLUS(00003C69)/0/7FD29013CA68: Processing the reply packet
Dec 8 11:38:34.701: TPLUS: Received authen response status GET_PASSWORD (8)
Dec 8 11:38:38.156: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:38.156: TPLUS(00003C69) login timer started 1020 sec timeout
Dec 8 11:38:38.156: TPLUS: processing authentication continue request id 15465
Dec 8 11:38:38.156: TPLUS: Authentication continue packet generated for 15465
Dec 8 11:38:38.156: TPLUS(00003C69)/0/WRITE/7FD3796079D8: Started 5 sec timeout
Dec 8 11:38:38.156: TPLUS(00003C69)/0/WRITE: wrote entire 29 bytes request
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 6 bytes data)
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: read entire 18 bytes response
Dec 8 11:38:38.183: TPLUS(00003C69)/0/7FD3796079D8: Processing the reply packet
Dec 8 11:38:38.183: TPLUS: Received authen response status PASS (2)
Dec 8 11:38:38.184: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: adminuser] [Source: 10.61.80.151]
```

```
Dec 8 11:38:38.259: TPLUS: Queuing AAA Authorization request 15465 for processing
Dec 8 11:38:38.260: TPLUS(00003C69) login timer started 1020 sec timeout
Dec 8 11:38:38.260: TPLUS: processing authorization request id 15465
Dec 8 11:38:38.260: TPLUS: Protocol set to None .....Skipping
Dec 8 11:38:38.260: TPLUS: Sending AV service=shell
Dec 8 11:38:38.260: TPLUS: Sending AV cmd*
Dec 8 11:38:38.260: TPLUS: Authorization request created for 15465(adminuser)
Dec 8 11:38:38.260: TPLUS: using previously set server 10.48.39.134 from group TACACS-Group
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT/7FD3796079D8: Started 5 sec timeout
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT: socket event 2
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT: wrote entire 64 bytes request
Dec 8 11:38:38.260: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.260: TPLUS(00003C69)/0/READ: Would block while reading
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 18 bytes data)
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: read entire 30 bytes response
Dec 8 11:38:38.285: TPLUS(00003C69)/0/7FD3796079D8: Processing the reply packet
Dec 8 11:38:38.285: TPLUS: Processed AV priv-lvl=15
Dec 8 11:38:38.285: TPLUS: received authorization response for 15465: PASS
Dec 8 11:38:44.225: %SYS-6-LOGOUT: User adminuser has exited tty session 7(10.61.80.151)
Dec 8 11:38:44.225:Socket I/O cleanup message sent to TACACS
TPLUS Proc:SOCKET IO CLEANUP EVENT
Dec 8 11:38:44.226: %HA_EM-6-LOG: catchall: logout
Dec 8 11:39:18.689: %SYS-6-LOGOUT: User admin has exited tty session 5(10.61.80.151)
Dec 8 11:39:18.690:Socket I/O cleanup message sent to TACACS
TPLUS Proc:SOCKET IO CLEANUP EVENT
```

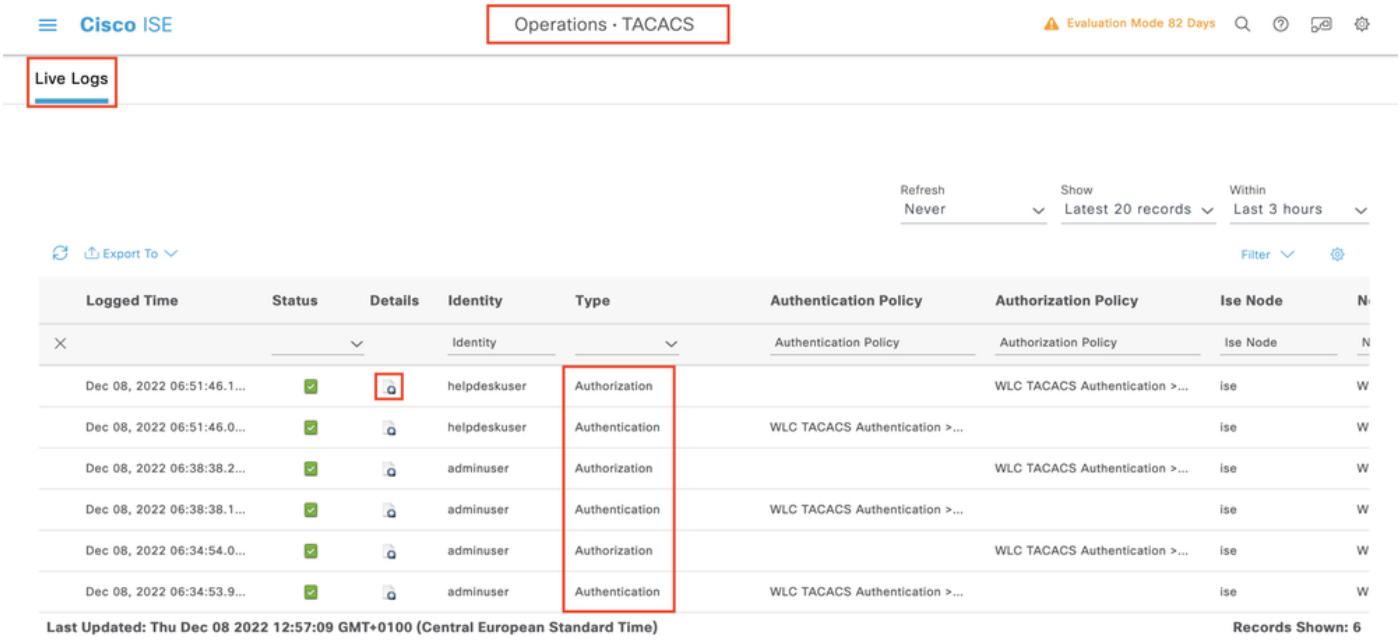
從這些日誌中可以看到，TACACS+伺服器傳回正確的特權(即AV priv-lvl=15)。

執行RADIUS驗證時，會顯示類似的偵錯輸出，與RADIUS流量相關。

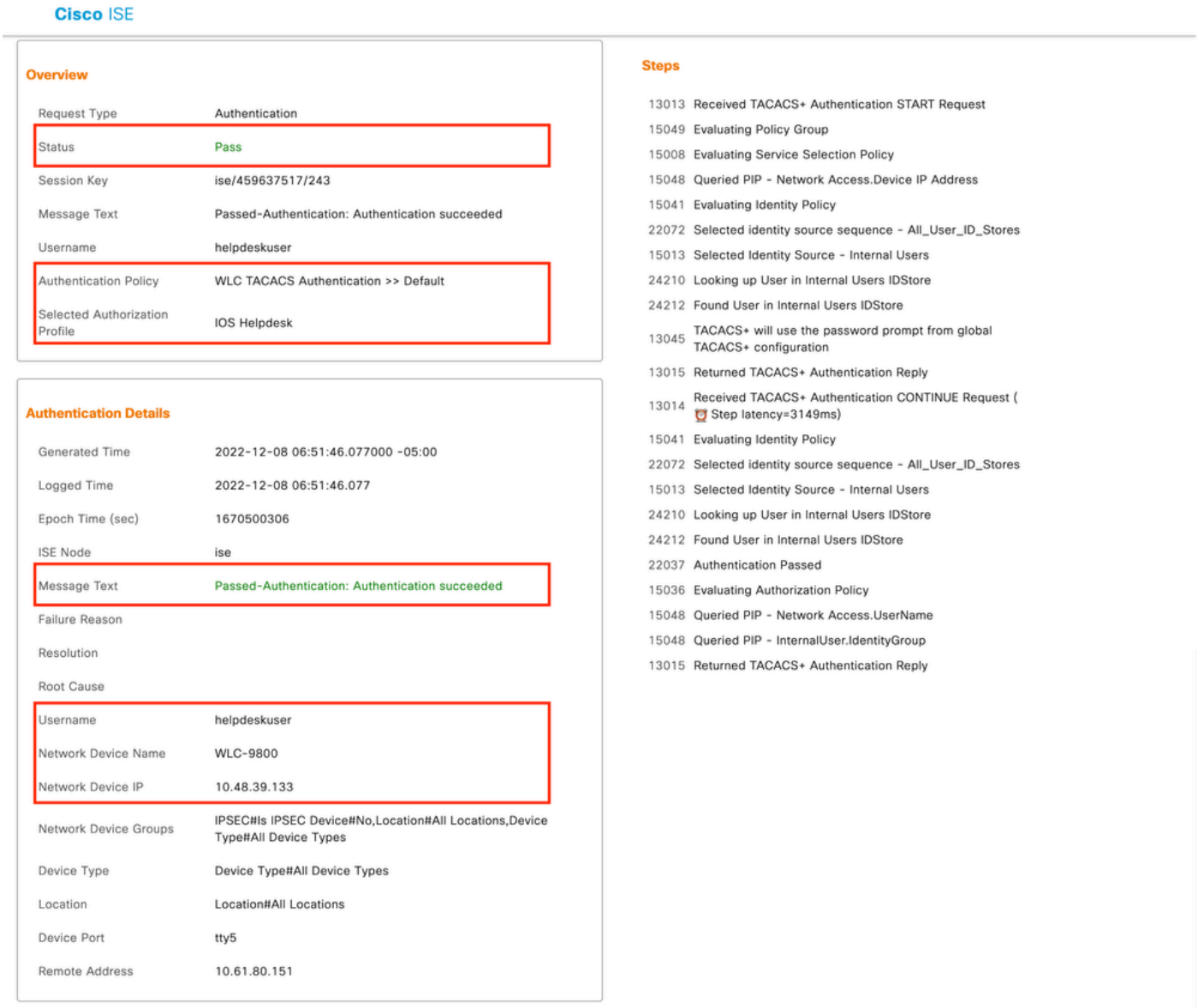
命令debug aaa authentication和debug aaa authorization會顯示使用者嘗試登入時WLC選擇了哪一方法清單。

通過ISE GUI排除WLC GUI或CLI TACACS+訪問故障

從第頁Operations > TACACS > Live Logs ，可以檢視使用TACACS+進行直到最近24小時內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Details按鈕。



展開後，成功的身份驗證嘗試helpdeskuser如下所示：



從這裡可以看到，使用者已helpdeskuser成功透過驗證原則的協助WLC-9800，通過網路裝置的驗證WLC TACACS Authentication > Default。此外，授權配置IOS Helpdesk已分配給此使用者，並且已授予許可權級別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）。