使用RADIUS和TACACS+驗證設定9800 WLC前廳授權大使

目錄

簡介

本檔案介紹如何使用身分識別服務引擎(ISE)為Lobby Ambassador使用者的RADIUS和TACACS+外部驗證設定Catalyst 9800無線LAN控制器。

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：

- Catalyst 9800無線控制器系列(Catalyst 9800-CL)
- Cisco IOS®-XE直布羅陀版16.12.1s
- ISE 2.3.0

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

大堂大使使用者由網路管理員建立。Lobby Ambassador使用者能夠建立訪客使用者的使用者名稱、密碼、說明和生存期。它還可以刪除訪客使用者。訪客使用者可通過GUI或CLI建立。

設定

網路圖表

在此範例中，已設定游說大使「lobby」和「lobbyTac」。大堂大使「大堂」是針對RADIUS伺服器進行驗證，而大堂大使「lobbyTac」是針對TACACS+進行驗證。

此組態將首先為RADIUS大堂大使完成，最後為TACACS+大堂大使完成。RADIUS和TACACS+ ISE配置也共用。

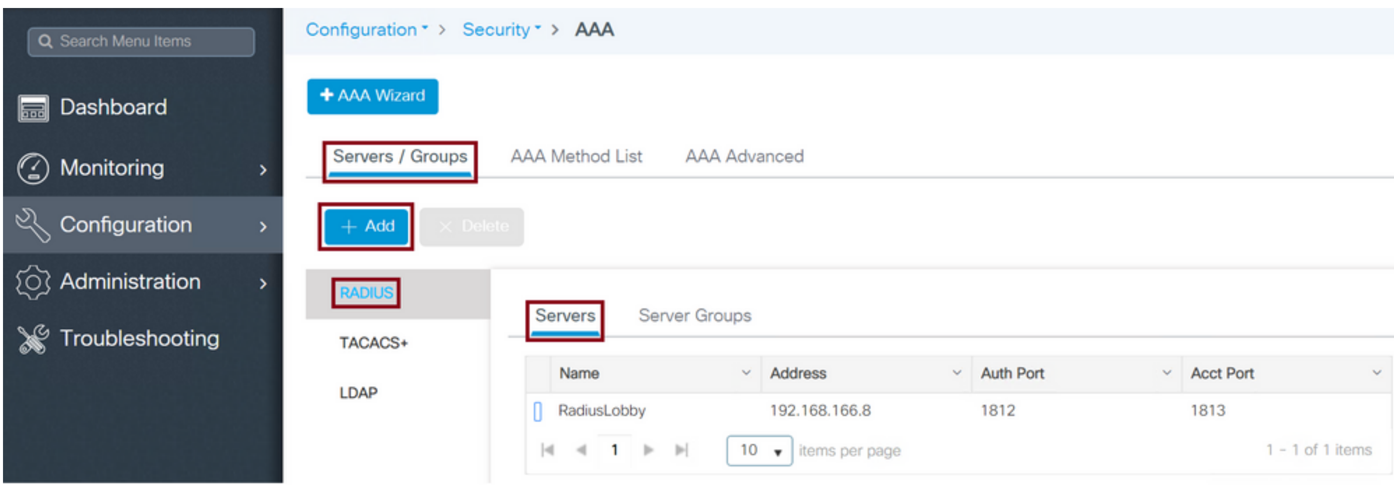
驗證RADIUS

在無線LAN控制器(WLC)上設定RADIUS。

步驟1.宣告RADIUS伺服器。在WLC上建立ISE RADIUS伺服器。

GUI:

導覽至**Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add**，如下圖所示。



當配置視窗開啟時，強制配置引數為RADIUS伺服器名稱（它不必與ISE/AAA系統名稱匹配）、RADIUS伺服器IP地址和共用金鑰。其他任何引數都可以保留為預設值，也可以根據需要進行配置。

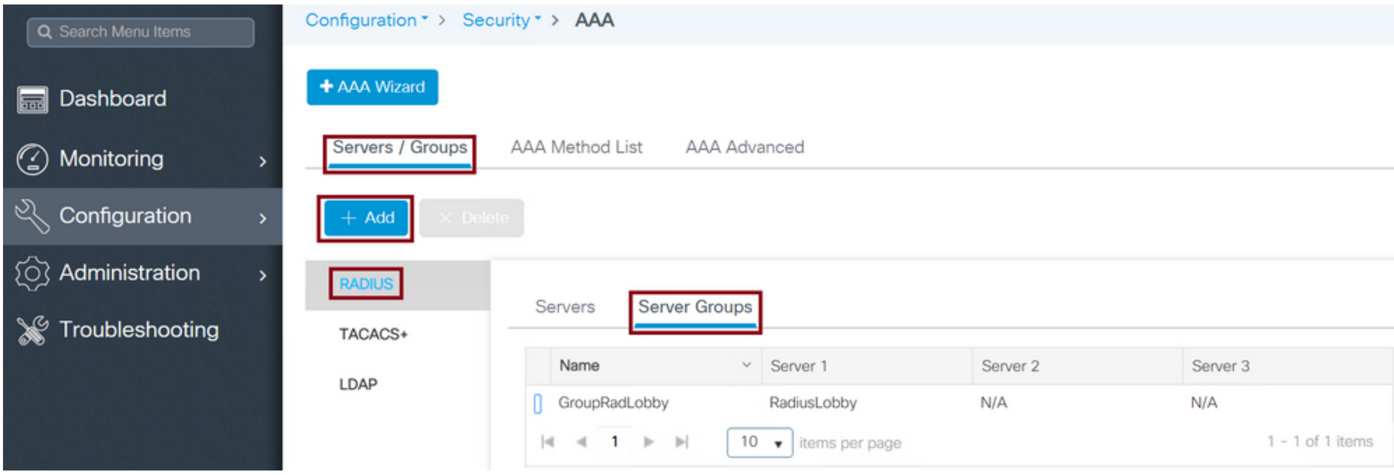
CLI:

```
Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end
```

步驟2.將RADIUS伺服器新增到伺服器組。定義伺服器組並新增配置的RADIUS伺服器。這將是RADIUS伺服器，用於驗證大廳大使使用者。如果WLC中配置了多個可用於身份驗證的RADIUS伺服器，則建議將所有RADIUS伺服器新增到同一個伺服器組。如果這樣做，就會讓WLC在伺服器群組中的RADIUS伺服器之間負載平衡驗證作業。

GUI:

導覽至**Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**，如下圖所示。



開啟配置視窗以為組指定名稱時，將已配置的RADIUS伺服器從「可用伺服器」清單移動到「已分配的伺服器」清單。

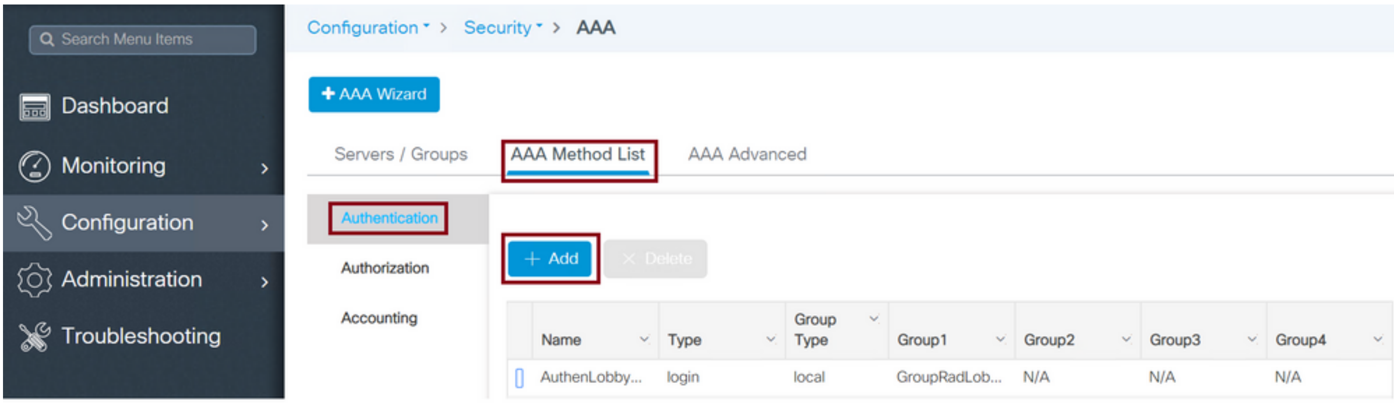
CLI:

```
Tim-eWLC1(config)#aaa group server radius GroupRadLobby
Tim-eWLC1(config-sg-radius)#server name RadiusLobby
Tim-eWLC1(config-sg-radius)#end
```

步驟3.建立身份驗證方法清單。身份驗證方法清單定義您查詢的身份驗證型別，並將將其附加到您定義的伺服器組。您會知道驗證是在WLC本機上進行，還是在RADIUS伺服器外部進行。

GUI:

導覽至**Configuration > Security > AAA > AAA Method List > Authentication > + Add**，如下圖所示。



開啟配置視窗時，提供名稱，選擇型別選項作為**登入**，並分配先前建立的伺服器組。

組型別為本地。

GUI:

如果選擇「Group Type」作為「local」，WLC將首先檢查使用者是否存在於本地資料庫中，然後僅當在本地資料庫中找不到Lobby Ambassador使用者時回退到伺服器組。

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

附註：請注意錯誤CSCvs87163 當您首先使用本地時。這一點在17.3中得到修正。

組型別作為組。

GUI:

如果選擇「組型別」作為「組」，且未選中「回退到本地」選項，則WLC將僅針對伺服器組檢查使用者，而不簽入其本地資料庫。

CLI:

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Group Type（組型別）作為組，並選中fallback to local（回退到本地）選項。

GUI:

如果選擇「組型別」作為「組」並選中「回退到本地」選項，則WLC將針對伺服器組檢查使用者，並且僅當RADIUS伺服器在響應中超時時才查詢本地資料庫。如果伺服器回應，WLC將不會觸發本機驗證。

CLI:

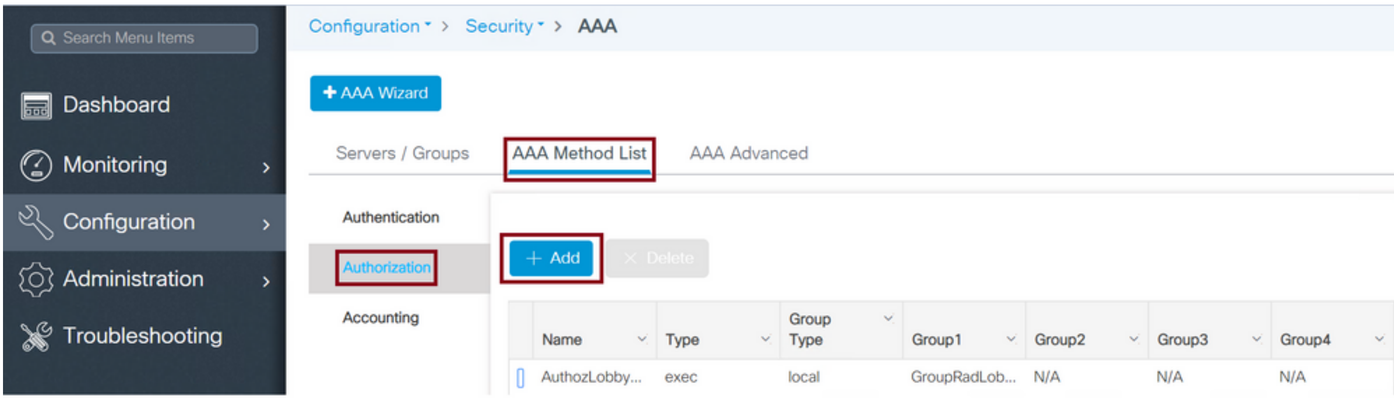
```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local
```

```
Tim-eWLC1(config)#end
```

步驟4.建立授權方法清單。Authorization Method List定義您需要Lobby Ambassador的授權型別，在本例中為「exec」。 它也會附加到定義的同一伺服器組。它也會允許選擇驗證是在WLC本機上完成還是在RADIUS伺服器外部完成。

GUI:

導覽至 「組態」>「安全性」>「AAA」>「AAA 方法清單」>「授權」>「+ 新增」（如圖所示）。



當開啟配置視窗以提供名稱時，選擇type選項作為「exec」，並分配先前建立的伺服器組。

請注意，組型別的應用方式與「身份驗證方法清單」部分中介紹的方法相同。

CLI:

組型別為本地。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

組型別作為組。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Group Type as group並選中fallback to local選項。

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

步驟5.分配方法。設定好方法後，必須將其指派給選項以登入WLC，以便建立訪客使用者(例如線路VTY(SSH/Telnet)或HTTP(GUI))。

這些步驟無法從GUI完成，因此需要從CLI完成。

HTTP/GUI身份驗證：

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod
Tim-eWLC1(config)#end
```

當您對HTTP配置執行更改時，最好重新啟動HTTP和HTTPS服務：

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

線路VTY。

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end
```

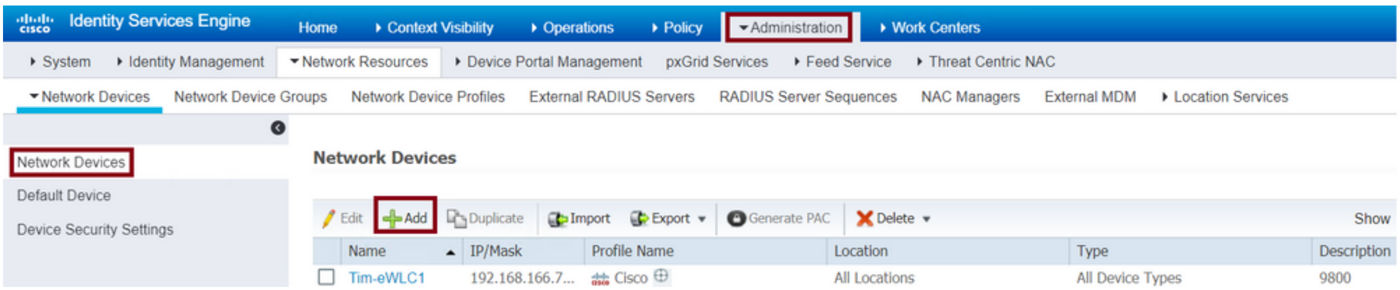
步驟6.只有在17.5.1或17.3.3之前的軟體版本中才需要此步驟，而在[CSCvu](#)之前的版本中則不需要此步驟29748 已實施。定義遠端使用者。在ISE上為游說大使建立的使用者名稱必須定義為WLC上的遠端使用者名稱。如果沒有在WLC中定義遠端使用者名稱，驗證將會正確執行，但使用者會獲得對WLC的完整存取許可權，而不是只獲得對大堂大使特權的存取許可權。此配置只能通過CLI完成。

CLI:

```
Tim-eWLC1(config)#aaa remote username lobby
```

配置ISE - RADIUS

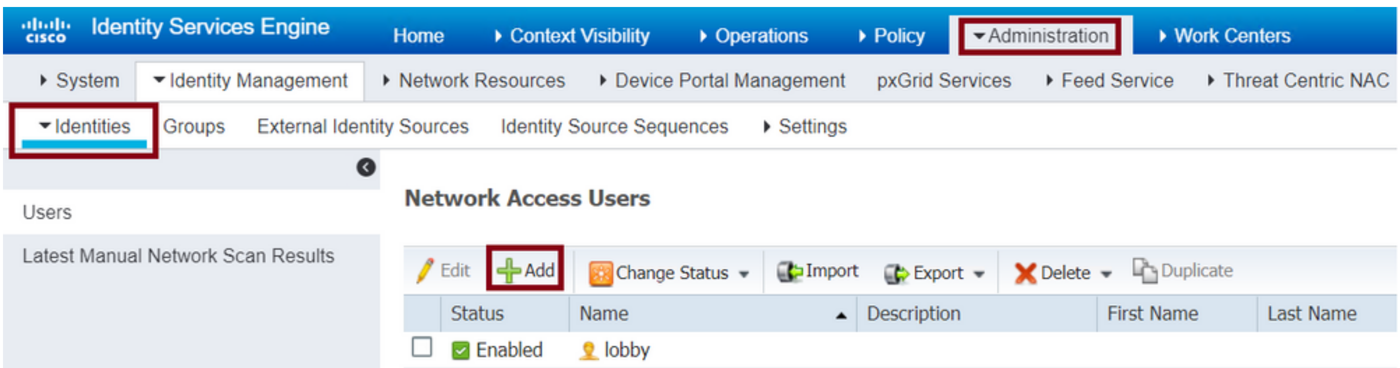
步驟1.將WLC新增到ISE。導覽至**Administration > Network Resources > Network Devices > Add**。需要將WLC新增到ISE。將WLC新增到ISE時，啟用RADIUS身份驗證設定並配置所需的引數，如圖所示。



當配置視窗開啟時，提供名稱IP ADD，啟用RADIUS身份驗證設定，並在Protocol Radius下輸入所需的共用金鑰。

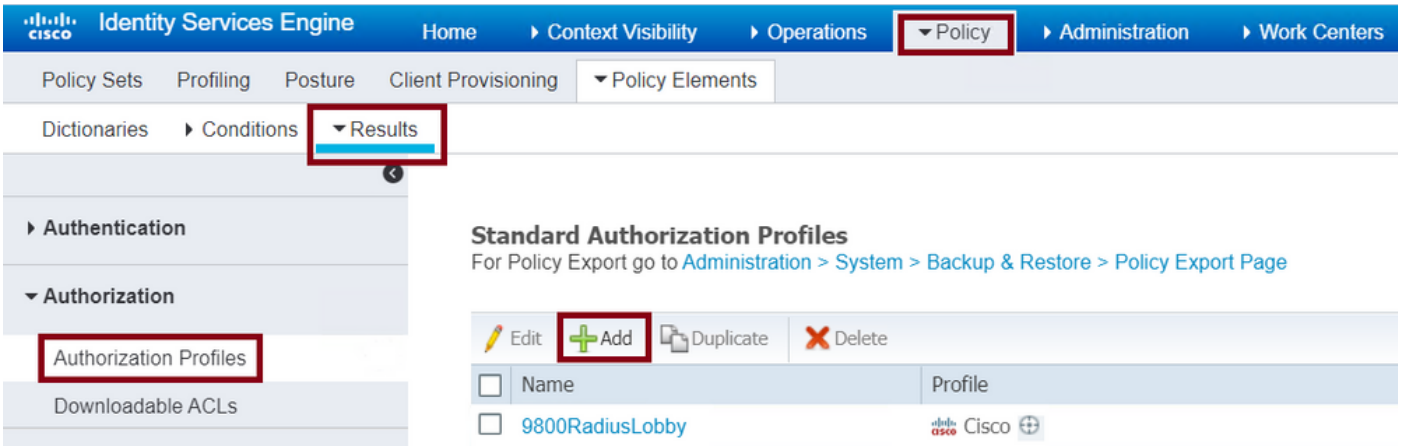
步驟2.在ISE上建立大廳大使使用者。導航到**管理>身份管理>身份>使用者>新增**。

將分配給建立訪客使用者的大廳大使的使用者名稱和密碼新增到ISE。這是管理員將分配給Lobby Ambassador的使用者名稱。

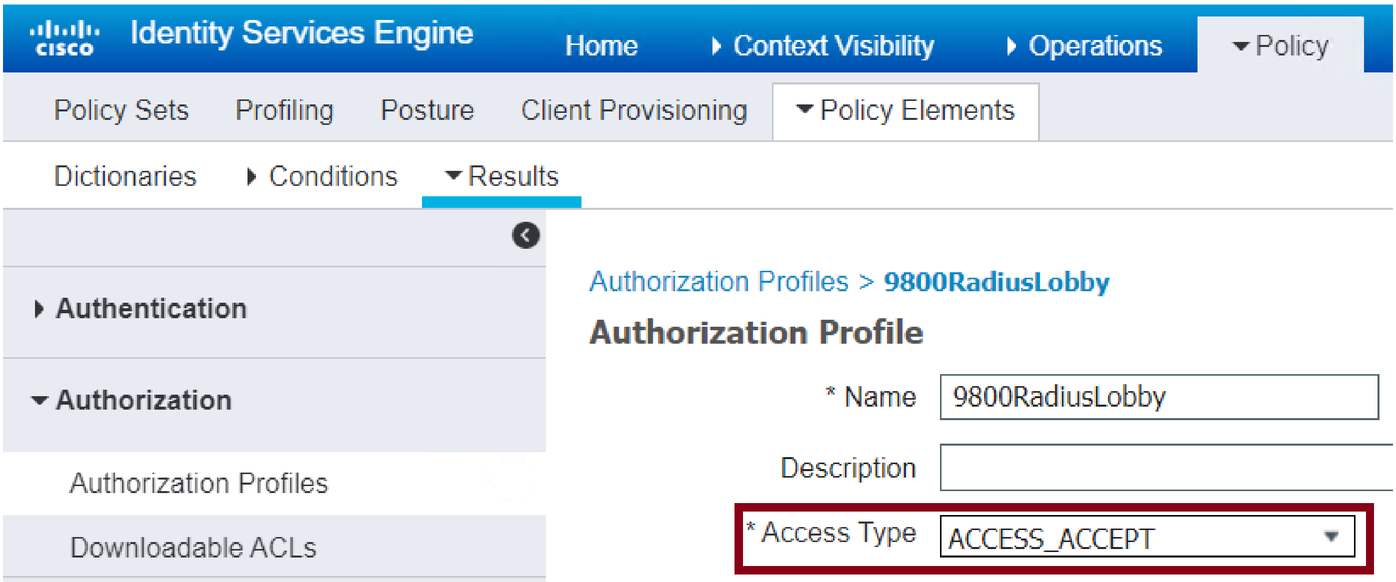


當配置視窗開啟時，請提供Lobby Ambassador使用者的名稱和密碼。此外，請確保狀態為已啟用。

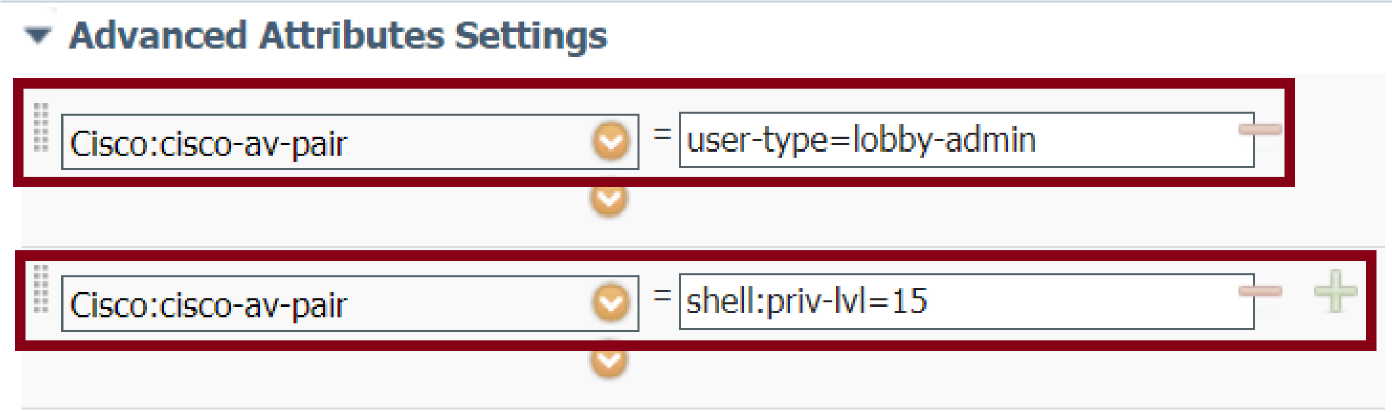
步驟3.建立結果授權配置檔案。導航至**Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add**。建立結果授權設定檔，以便使用所需的屬性回覆Access-Accept至WLC，如下圖所示。

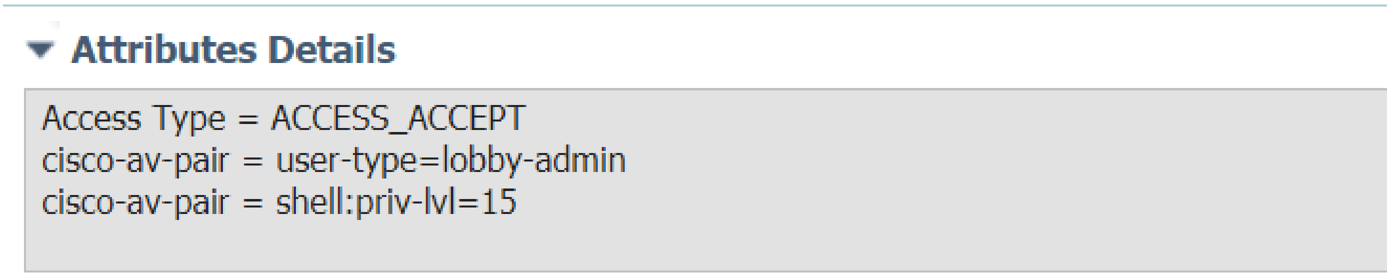


確保將配置檔案配置為傳送Access-Accept，如下圖所示。



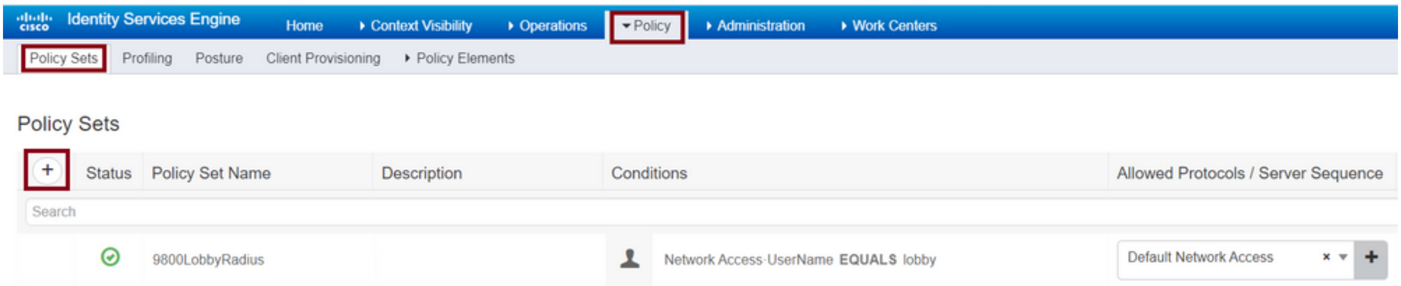
您需要在「高級屬性設定」下手動新增屬性。需要這些屬性以將使用者定義為大堂大使並提供許可權，以允許大堂大使進行所需的更改。



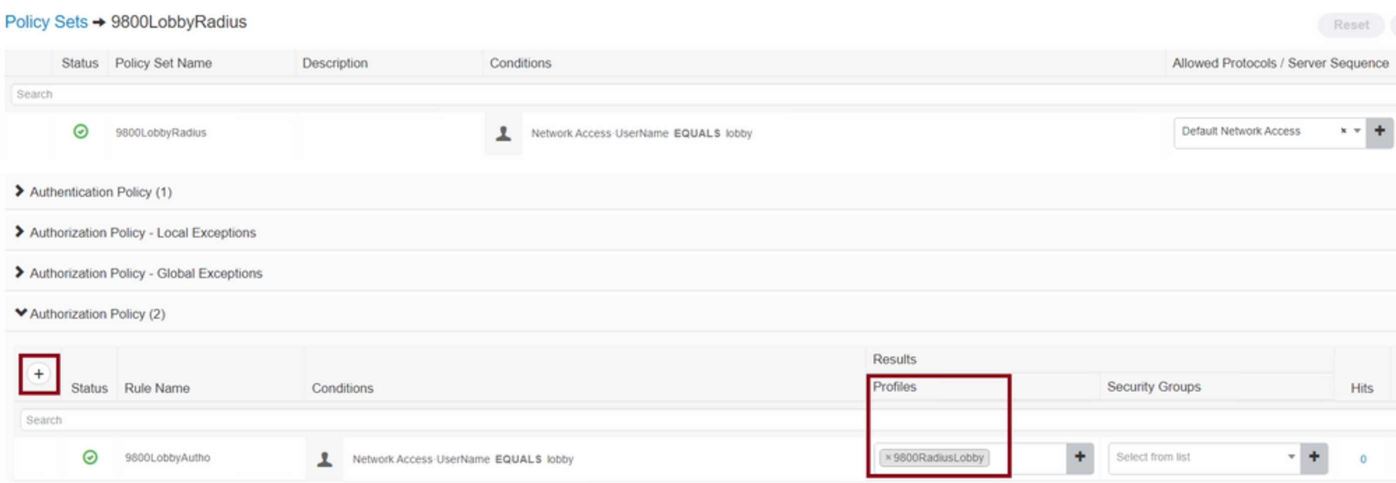


步驟4.建立策略以處理身份驗證。導航到**Policy > Policy Sets > Add**。配置策略的條件取決於管理員的決定。此處使用Network Access-Username條件和預設網路訪問協定。

必須確保在授權策略下選擇結果授權下配置的配置檔案，這樣您就可以將所需的屬性返回到WLC，如圖所示。



當配置視窗開啟時，配置授權策略。身份驗證策略可以保留為預設值。



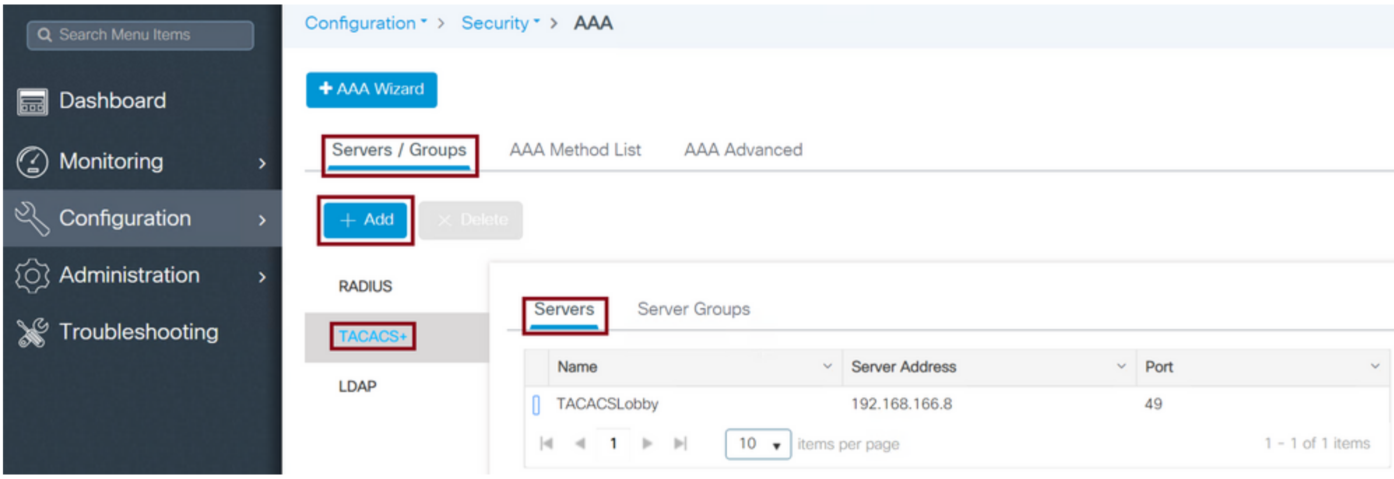
驗證TACACS+

設定WLC上的TACACS+

步驟1.宣告TACACS+伺服器。在WLC中建立ISE TACACS伺服器。

GUI:

導覽至**Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add**，如下圖所示。



當配置視窗開啟時，強制配置引數是TACACS+伺服器名稱（它不必與ISE/AAA系統名稱匹配）、TACACS伺服器IP地址和共用金鑰。任何其他引數都可以保留為預設值，也可以根據需要進行配置。

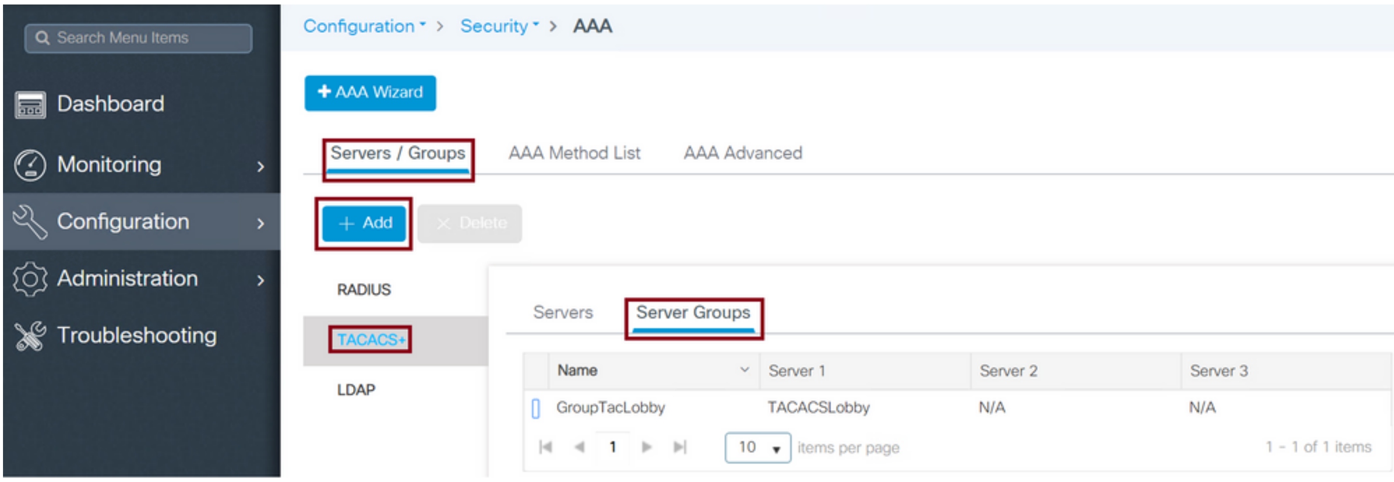
CLI:

```
Tim-eWLC1(config)#tacacs server TACACSLobby
Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8
Tim-eWLC1(config-server-tacacs)#key 0 Cisco123
Tim-eWLC1(config-server-tacacs)#end
```

步驟2.將TACACS+伺服器新增到伺服器組。定義伺服器組並新增已配置的所需TACACS+伺服器。這是用於身份驗證的TACACS+伺服器。

GUI:

導覽至**Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add**，如下圖所示。



開啟配置視窗時，為組指定一個名稱，並將所需的TACACS+伺服器從「可用伺服器」清單移動到「分配的伺服器」清單。

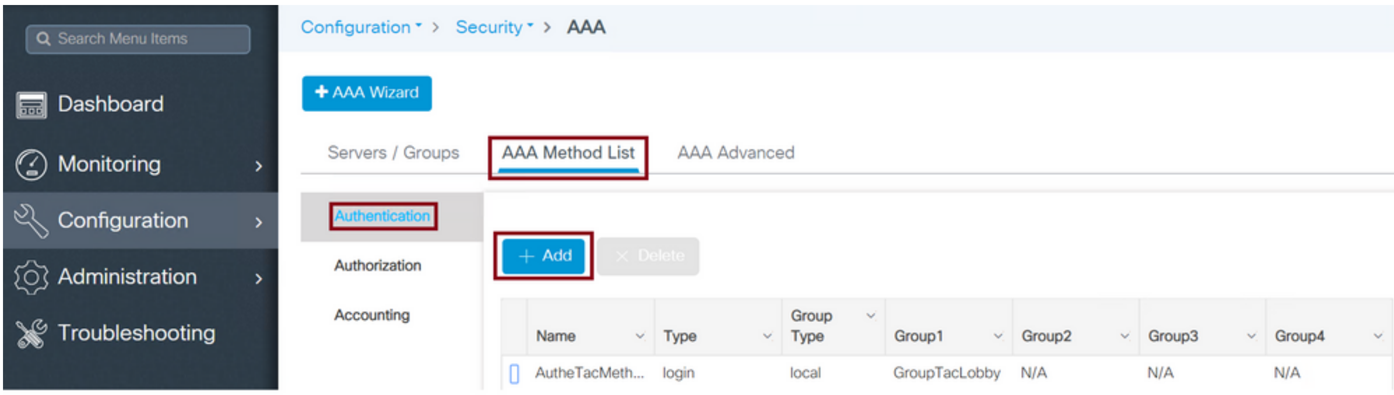
CLI:

```
Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby
Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby
Tim-eWLC1(config-sg-tacacs+)#end
```

步驟3.建立身份驗證方法清單。身份驗證方法清單定義所需的身份驗證型別，並將將其附加到已配置的伺服器組。此功能也允許選擇驗證是在WLC本機上進行，還是在TACACS+伺服器外部進行。

GUI:

導覽至**Configuration > Security > AAA > AAA Method List > Authentication > + Add**，如下圖所示。



開啟配置視窗時，提供名稱，選擇型別選項作為**登入**，並分配先前建立的伺服器組。

組型別為本地。

GUI:

如果選擇「組型別」為「本地」，WLC將首先檢查本地資料庫中是否存在該使用者，然後僅在本地資料庫中找不到Lobby Ambassador使用者時回退到伺服器組。

> **附註**：請注意此錯誤CSCvs87163在17.3中修復。

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

組型別作為組。

GUI:

如果選擇「組型別」作為組並且選中了「不回退到本地」選項，則WLC將僅針對伺服器組檢查使用者，並且不會簽入其本地資料庫。

CLI:

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Group Type as group並選中fallback to local選項。

GUI:

如果選擇「Group Type」作為「group」，並選中「Fallback to local」選項，則WLC將針對伺服器組檢查使用者，並且僅當TACACS伺服器在響應中超時時才查詢本地資料庫。如果伺服器傳送拒絕消息，則使用者不會被驗證，即使該使用者存在於本地資料庫中。

CLI:

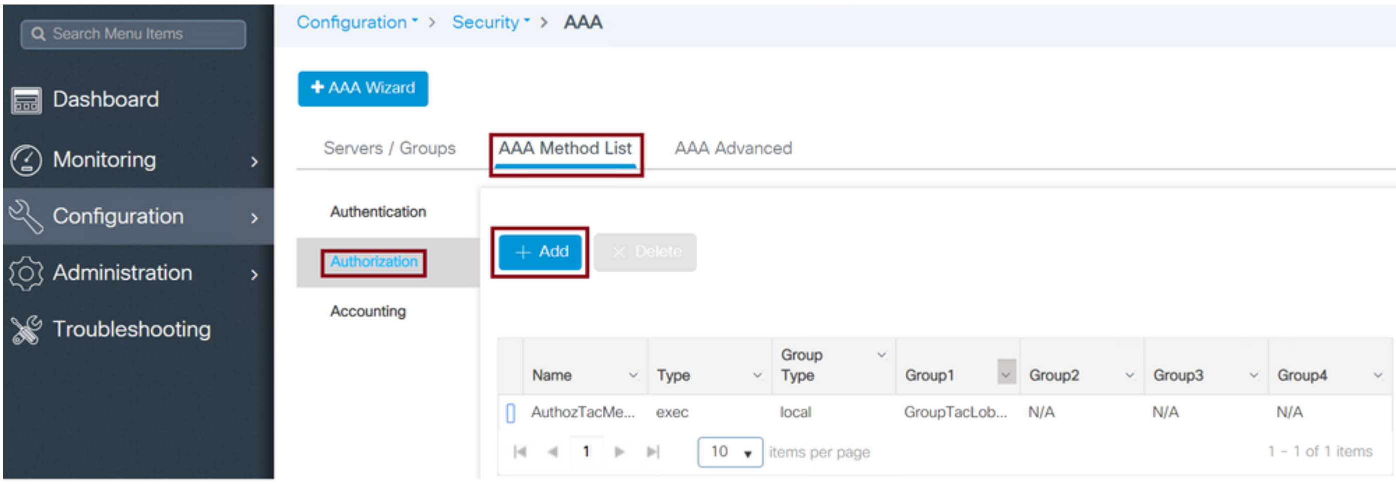
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

步驟4.建立授權方法清單。

Authorization Method List（授權方法清單）將定義大堂大使所需的授權型別，在這種情況下將執行。它還連線到配置的同一伺服器組。也允許選擇驗證是在WLC本機上完成還是在TACACS+伺服器外部完成。

GUI:

導覽至 「組態」>「安全性」>「AAA」>「AAA 方法清單」>「授權」>「+ 新增」（如圖所示）。



開啟配置視窗時，提供名稱，選擇type選項作為exec，並分配先前建立的Server Group。

請注意，「組型別」應用的方式與「身份驗證方法清單」部分中的說明相同。

CLI:

組型別為本地。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

組型別作為組。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Group Type as group並選中Fallback to local選項。

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

步驟5.分配方法。設定好方法後，必須將其指派給選項，才能登入WLC建立訪客使用者(例如線路VTY或HTTP(GUI))。 這些步驟無法從GUI完成，因此需要從CLI完成。

HTTP/GUI身份驗證：

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod
Tim-eWLC1(config)#end
```

當您更改HTTP配置時，最好重新啟動HTTP和HTTPS服務：

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

線路VTY:

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end
```

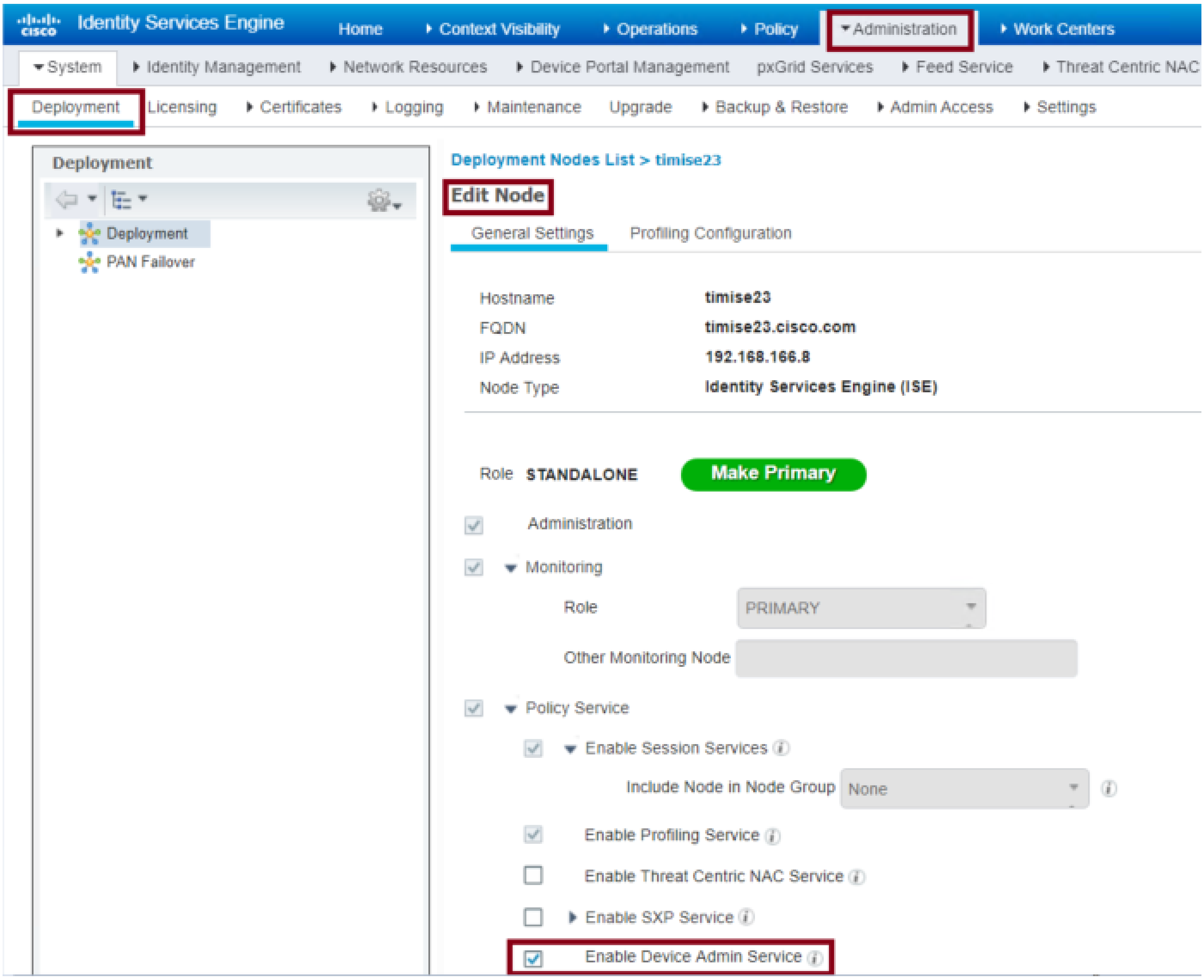
步驟6.定義遠端使用者。在ISE上為游說大使建立的使用者名稱必須定義為WLC上的遠端使用者名稱。如果沒有在WLC中定義遠端使用者名稱，驗證將會正確執行，但使用者會獲得對WLC的完整存取許可權，而不是只獲得對大堂大使特權的存取許可權。此配置只能通過CLI完成。

CLI:

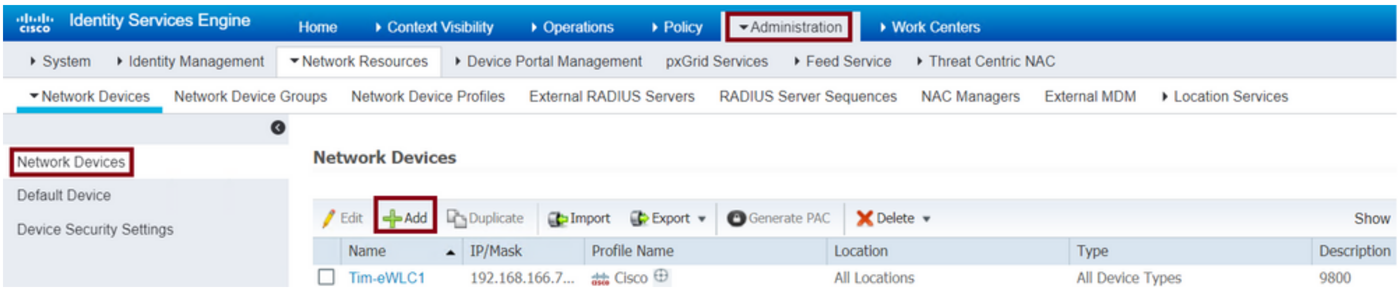
```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

配置ISE - TACACS+

步驟1.啟用Device Admin。導航到**管理>系統>部署**。繼續任何操作之前，請選擇**Enable Device Admin Service**並確保已啟用ISE，如下圖所示。

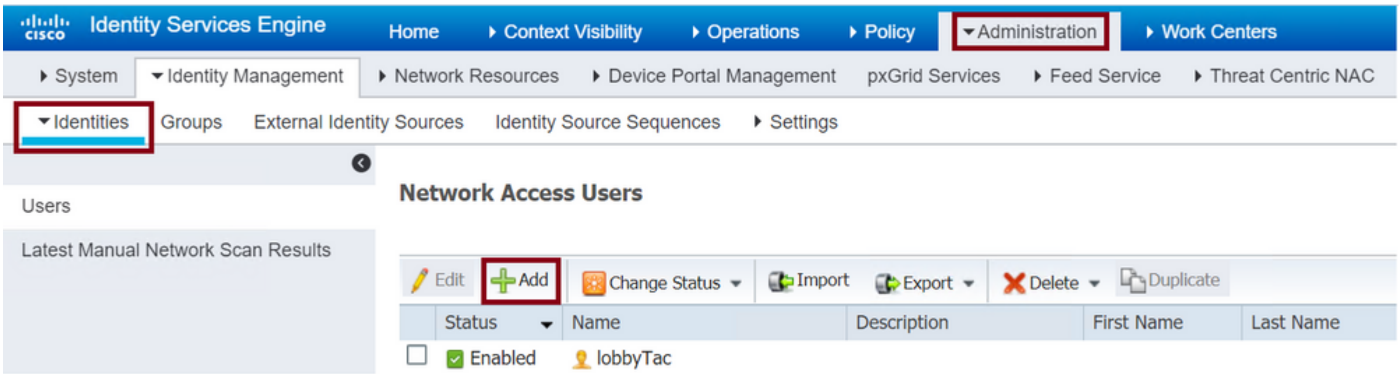


步驟2.將WLC新增到ISE。導覽至**Administration > Network Resources > Network Devices > Add**。需要將WLC新增到ISE。將WLC新增到ISE時，啟用TACACS+身份驗證設定並配置所需的引數，如圖所示。



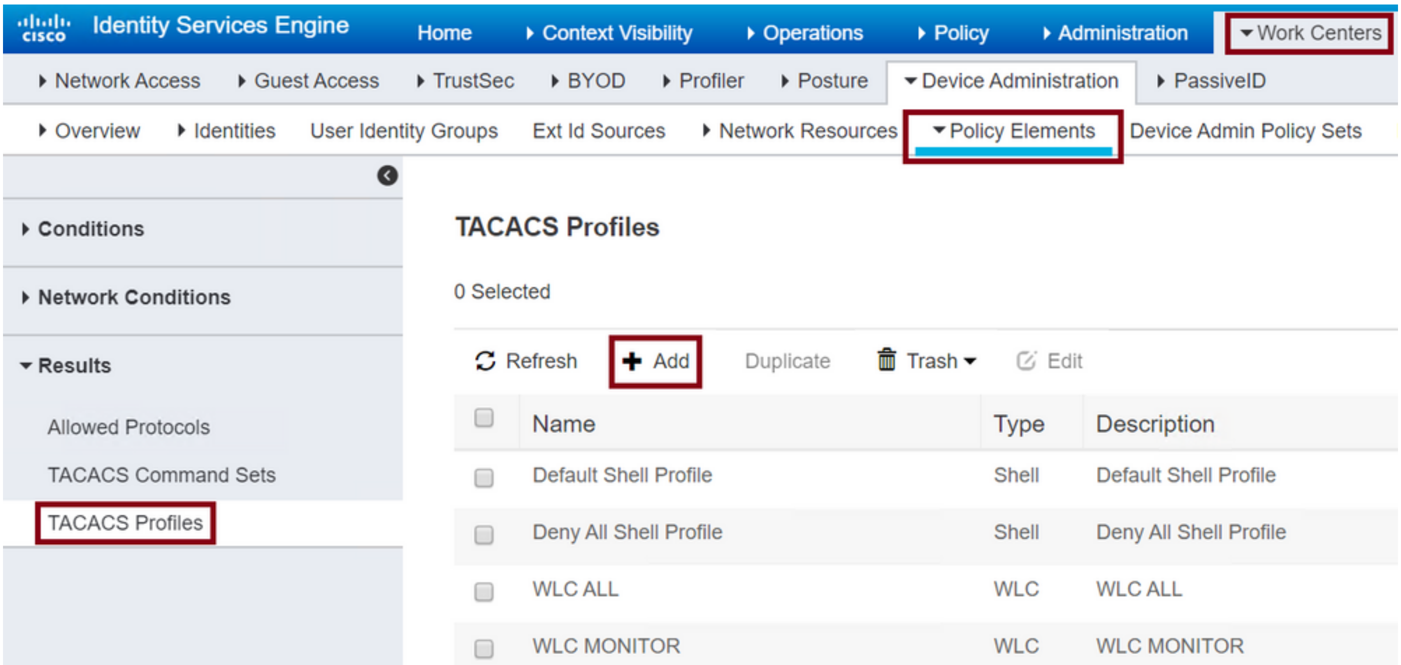
當開啟配置視窗以提供名稱IP ADD時，啟用TACACS+身份驗證設定並輸入所需的共用金鑰。

步驟3.在ISE上建立大廳大使使用者。導航到**管理>身份管理>身份>使用者>新增**。新增到ISE中，為將建立訪客使用者的大廳大使分配的使用者名稱和密碼。這是管理員分配給大堂大使的使用者名稱，如下圖所示。

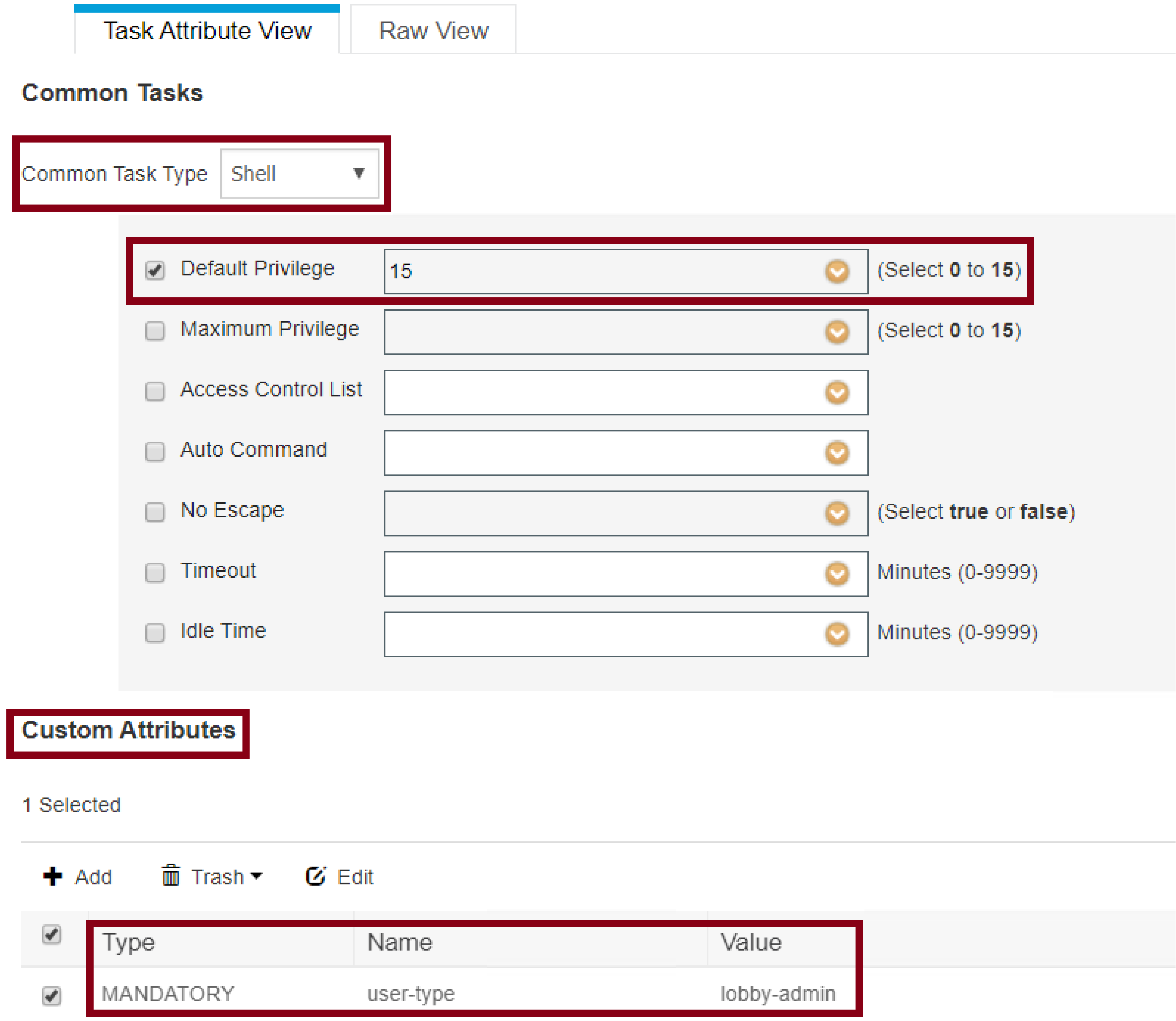


當配置視窗開啟時，請提供Lobby Ambassador使用者的名稱和密碼。此外，請確保狀態為已啟用
。

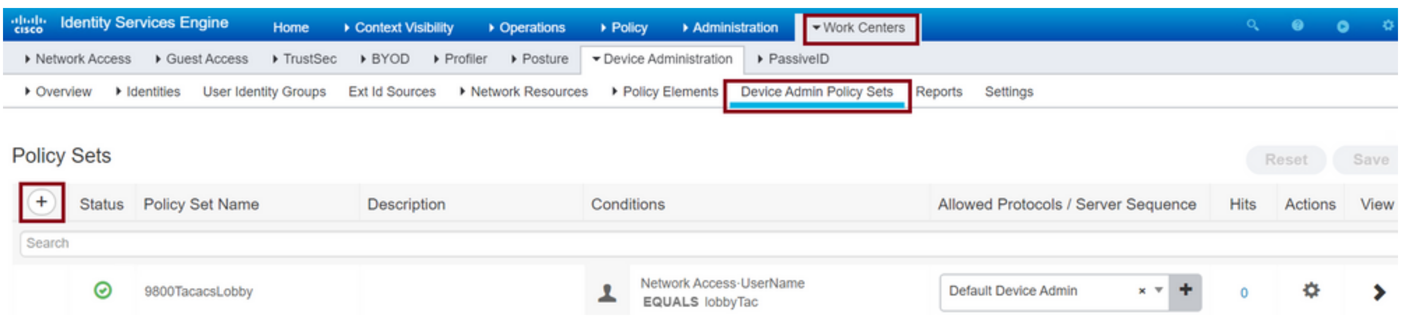
步驟4.建立結果TACACS+配置檔案。導覽至**Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**，如下圖所示。透過此設定檔，將所需的屬性傳回WLC，以便讓使用者擔任大堂大使。



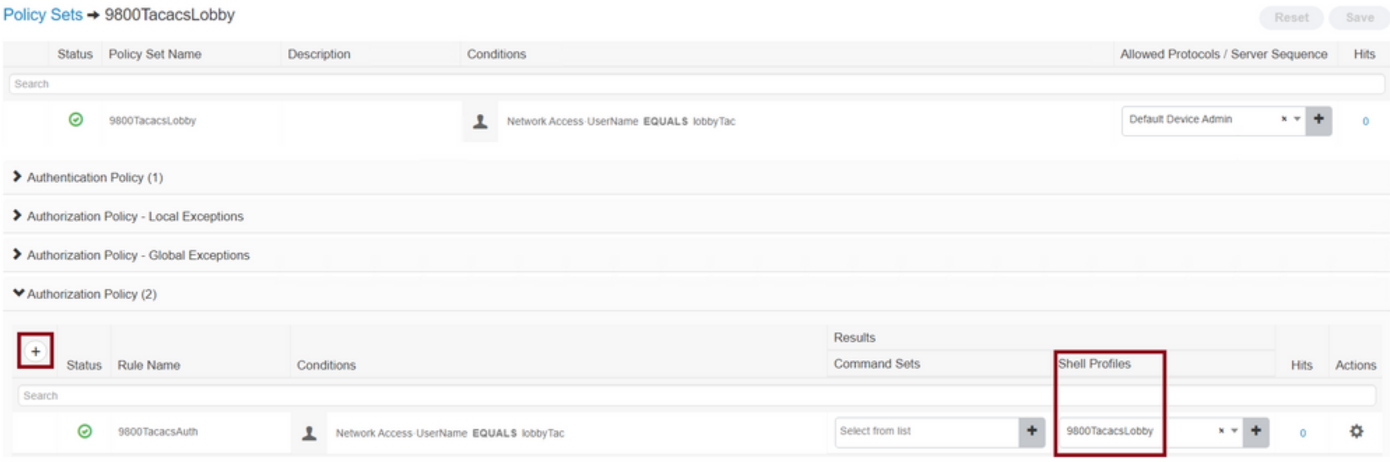
開啟配置視窗時，為配置檔案提供名稱，還將預設特權15和自定義屬性配置為強制型別，名稱為使用者型別和值looby-admin。此外，還可將「**Common Task Type**」選擇為「Shell」，如下圖所示
。



步驟5.建立策略集。導覽至**Work Centers > Device Administration > Device Admin Policy Sets**，如下圖所示。配置策略的條件取決於管理員的決定。本文檔使用網路訪問使用者名稱條件和預設裝置管理協定。在授權策略下，必須確保選擇結果授權下配置的配置檔案，這樣您就可以將所需的屬性返回到WLC。



當配置視窗開啟時，配置授權策略。驗證策略可以保留為預設值，如下圖所示。

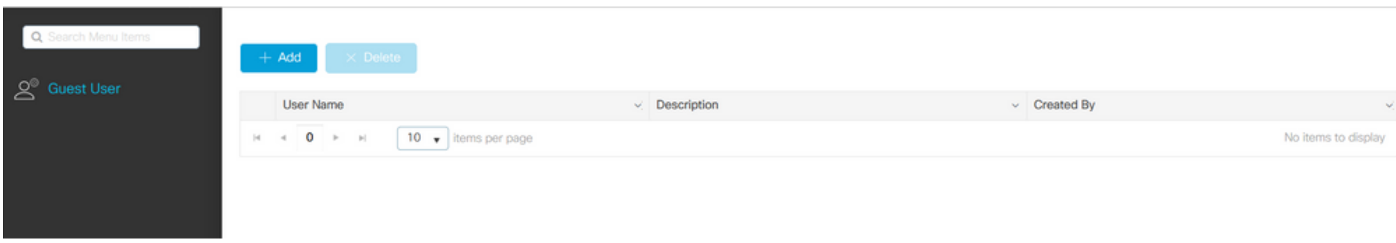


驗證

使用本節內容，確認您的組態是否正常運作。

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

成功驗證後，大廳大使GUI的外觀是這樣的。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

驗證RADIUS

針對RADIUS驗證，可以使用以下偵錯：

```
Tim-eWLC1#debug aaa authentication
Tim-eWLC1#debug aaa authorization
Tim-eWLC1#debug aaa attr
Tim-eWLC1#terminal monitor
```

確保從調試中選擇了正確的方法清單。此外，ISE伺服器會返回所需屬性，這些屬性具有正確的使用者名稱、使用者型別和許可權。

```
Feb 5 02:35:27.659: AAA/AUTHEN/LOGIN (00000000): Pick method list 'AuthenLobbyMethod'
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(0):
```

```
7FBA5500C870 0 00000081 username(450) 5 lobby
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1):
7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2):
7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F)
Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host
192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
```

驗證TACACS+

針對TACACS+驗證，可以使用以下偵錯：

```
Tim-eWLC1#debug tacacs
Tim-eWLC1#terminal monitor
```

確保使用正確的使用者名稱和ISE IP ADD處理身份驗證。此外，應看到狀態「PASS」。在同一調試中，身份驗證階段過後，將立即顯示授權過程。在此授權中，階段確保使用正確的使用者名稱以及正確的ISE IP ADD。在此階段中，您應該能夠看到在ISE上配置的屬性，這些屬性將WLC宣告為具有許可權的大廳大使使用者。

驗證階段示例：

```
Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing
Feb 5 02:06:48.245: TPLUS: Authentication start packet created for 0(lobbyTac)
Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8)
Feb 5 02:06:48.266: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)
```

授權階段示例：

```
Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing
Feb 5 02:06:48.267: TPLUS: Authorization request created for 0(lobbyTac)
Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.279: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15
Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin
Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS
```

前面提到的RADIUS和TACACS+的偵錯範例包含成功登入的關鍵步驟。調試更加詳細，輸出更大。若要停用偵錯，可以使用以下命令：

```
Tim-eWLC1#undebug all
```