配置帶RADIUS和TACACS+身份驗證的9800 WLC接待大使

目錄

簡介

本文檔介紹如何為接待大使使用者的RADIUS和TACACS+外部身份驗證配置Catalyst 9800無線控制器。

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

接待大使使用者由網路管理員建立。接待大使使用者能夠建立訪客使用者使用者名稱、密碼、說明和生存期。它還可以刪除訪客使用者。訪客使用者可透過GUI或CLI建立。

設定

網路圖表

在此範例中，已設定大廳大使「lobby」和「lobbyTac」。接待大使「lobby」用於針對RADIUS伺服器進行身份驗證，而接待大使「lobbyTac」用於針對TACACS+進行身份驗證。

先為RADIUS接待大使完成配置，最後為TACACS+接待大使完成配置。RADIUS和TACACS+ ISE配置也共用。

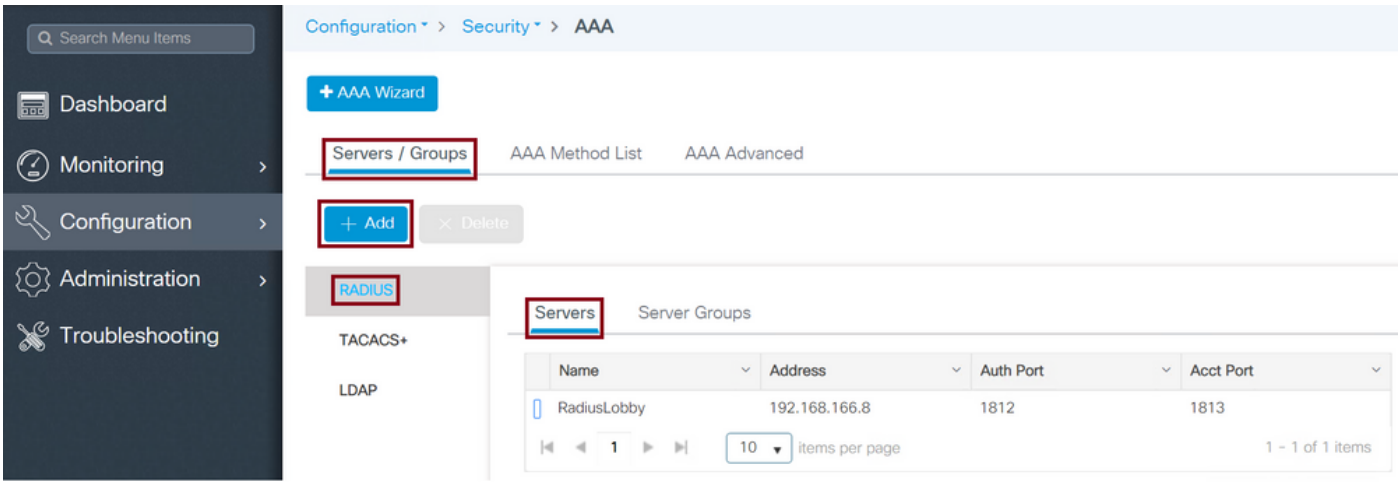
驗證RADIUS

在無線區域網路控制器(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。



當配置窗口打開時，強制配置引數為RADIUS伺服器名稱（它不必匹配ISE/AAA系統名稱）、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，也可以視需要設定。

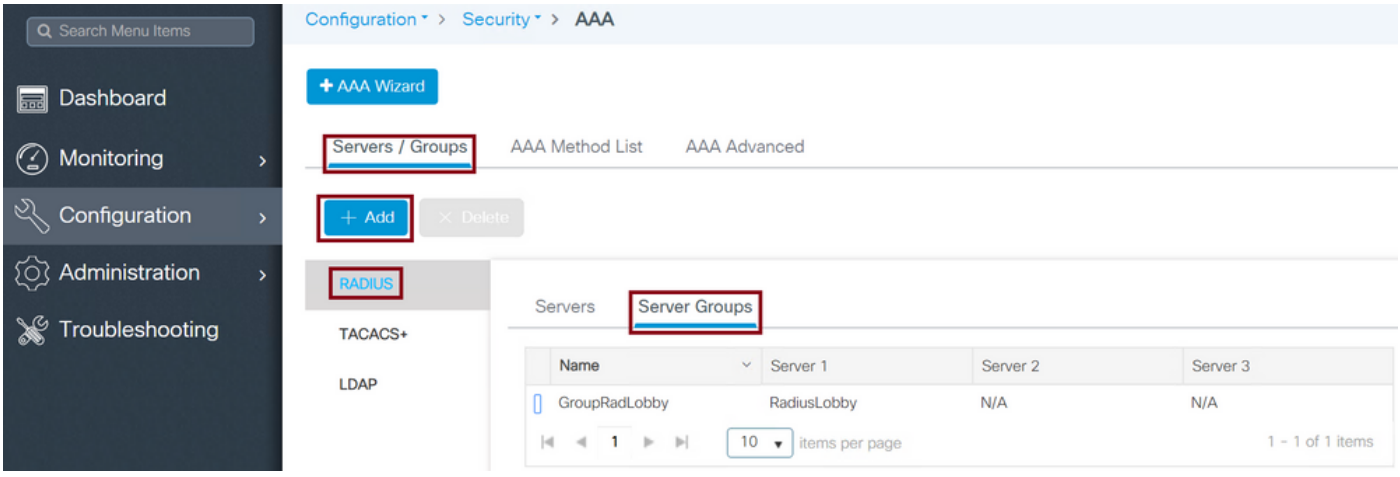
CLI：

```
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伺服器增加到伺服器組。定義伺服器組並增加配置的RADIUS伺服器。這是用於驗證接待大使使用者的RADIUS伺服器。如果WLC中配置了多個可用於身份驗證的RADIUS伺服器，則建議向同一伺服器組中增加所有RADIUS伺服器。如果這樣做，WLC會載入伺服器群組中RADIUS伺服器之間的驗證平衡。

GUI：

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



當配置窗口打開以為組提供名稱時，將配置的RADIUS伺服器從Available Servers清單移到

Assigned Servers清單。

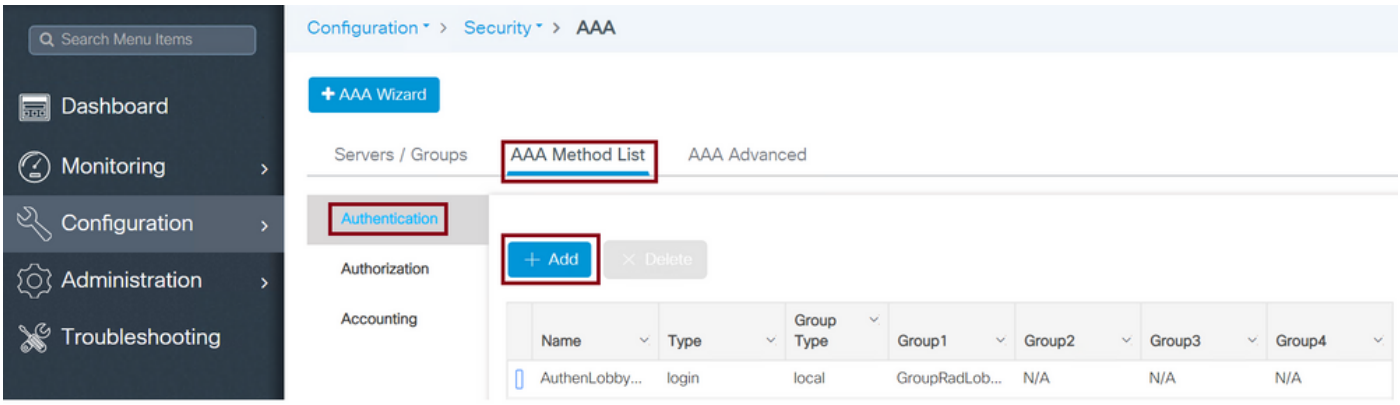
CLI：

```
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.建立驗證方法清單。「驗證方法清單」會定義您尋找的驗證型別，也會將其附加到您定義的伺服器群組。您知道驗證是在WLC本機上完成還是在RADIUS伺服器外部完成。

GUI：

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



當配置窗口打開時，請提供名稱，選擇Login作為type選項，並分配之前建立的伺服器組。

群組型別為本機。

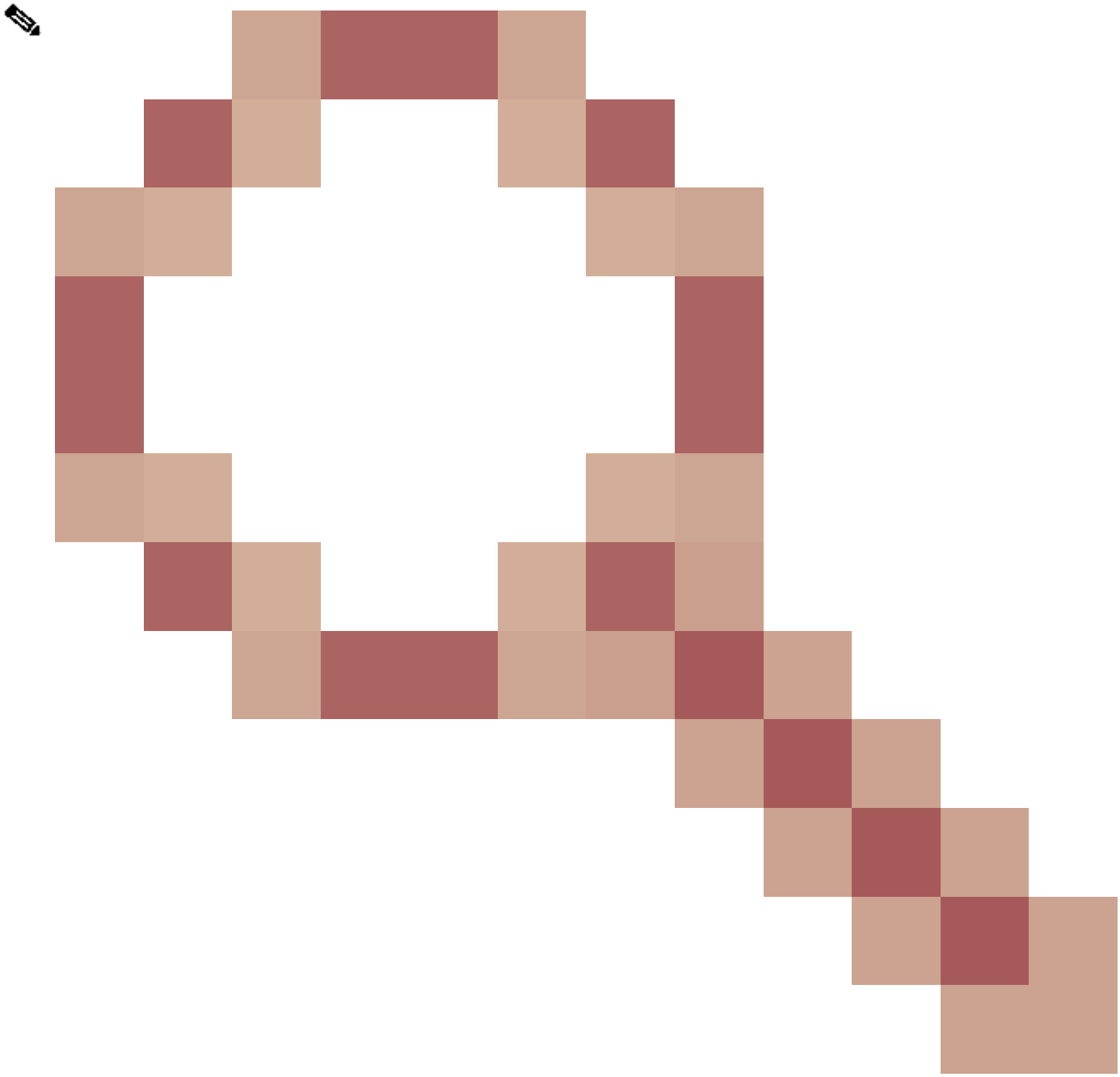
GUI：

如果選擇「組型別」作為「本地」，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未找到接待大使使用者時返回伺服器組。

CLI：

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

注意：



先使用本地時，請注意Bug CSCvs87163。17.3中已修復。

群組型別為群組。

GUI：

如果您選擇「Group Type」作為「group」，並且未選中「fallback to local」選項，則WLC將僅檢查伺服器組的使用者，並且不會簽入其本地資料庫。

CLI：

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

組型別作為組，並且選中回退到本地選項。

GUI：

如果選擇「Group Type」作為「group」，並且選中了fallback to local選項，則WLC將根據伺服器組檢查使用者，並且僅當響應中的RADIUS伺服器超時時，WLC才會查詢本地資料庫。如果伺服器回應，WLC將不會觸發本機驗證。

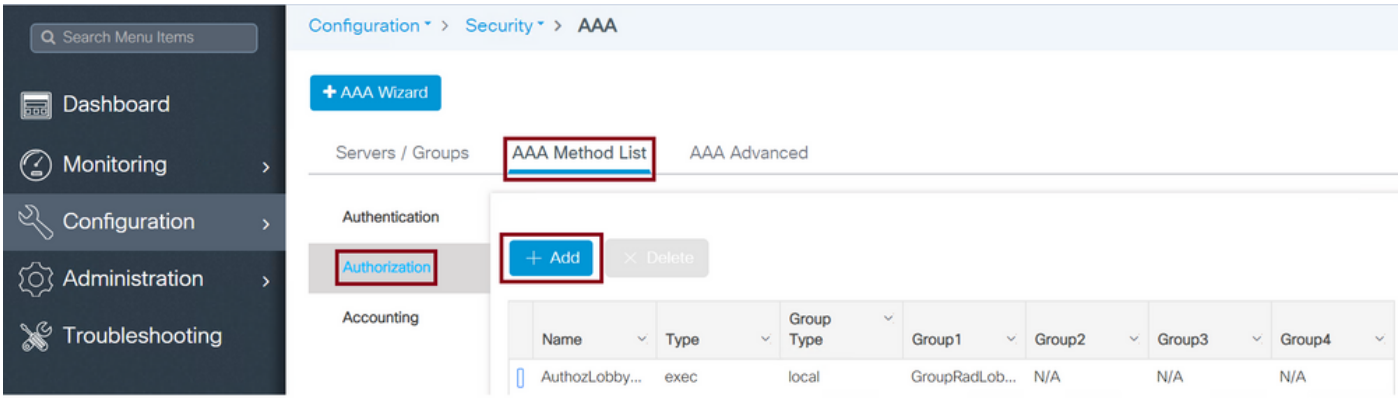
CLI：

```
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定義了接待大使所需的授權型別，在本例中為「exec」。它也會附加至定義的同一個伺服器群組。它也會允許選取驗證是在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）。



當組態視窗開啟以提供名稱時，請選取「exec」作為「type」選項，並指定先前建立的「Server Group」。

請注意，「群組型別」的套用方式與「驗證方法清單」一節中說明的套用方式相同。

CLI：

群組型別為本機。

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

群組型別為群組。

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

群組型別為群組且已核取「回退至本機」選項。

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

步驟 5.指派方法。設定方法後，必須將其指派給用於登入WLC的選項，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中完成，因此需要從CLI中完成。

HTTP/GUI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
```

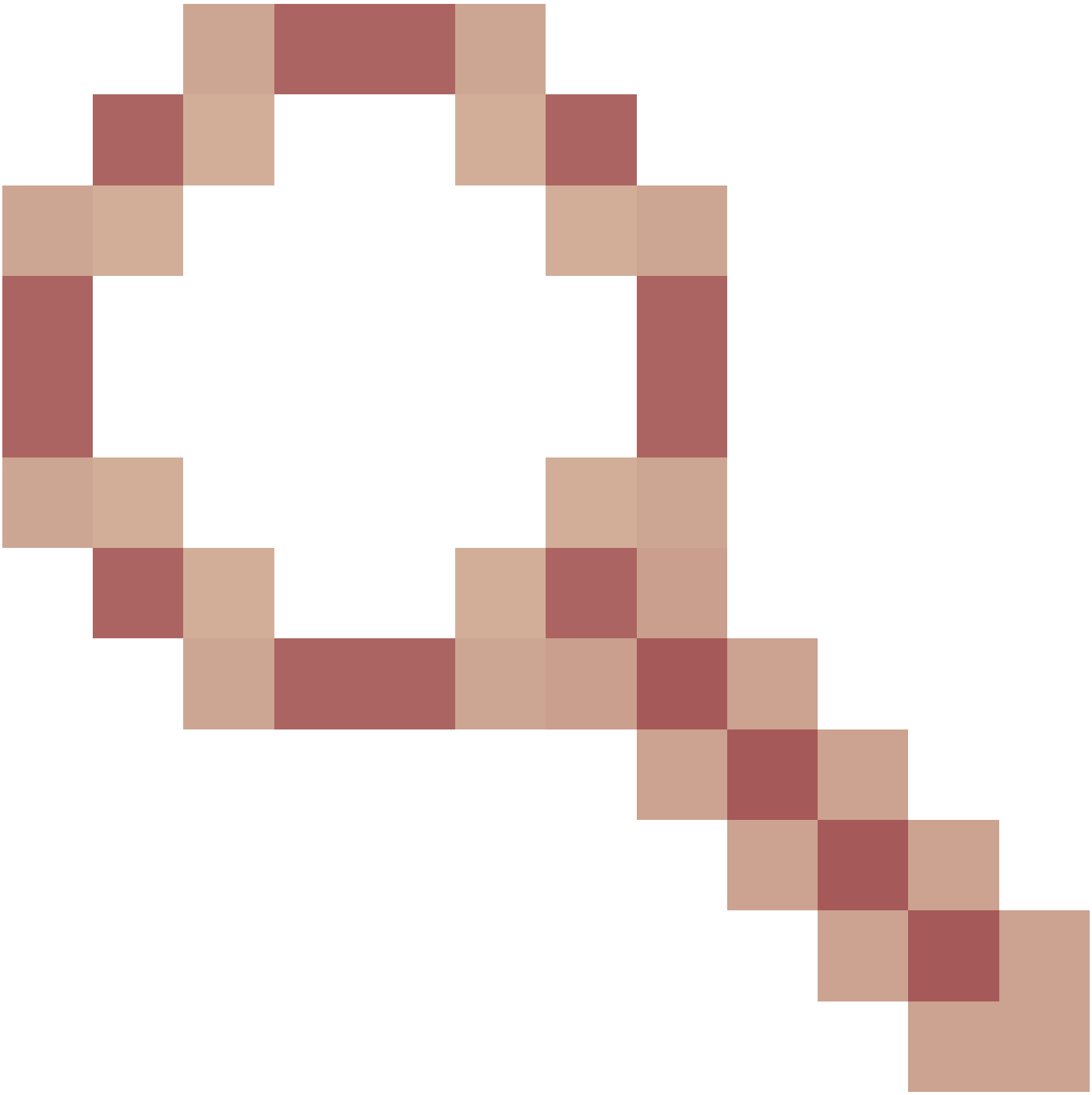
當您對HTTP配置執行更改時，最好重新啟動HTTP和HTTPS服務：

```
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.此步驟僅在17.5.1或17.3.3之前的軟體版本中是必需的，並且在實施CSCvu29748的版本之後



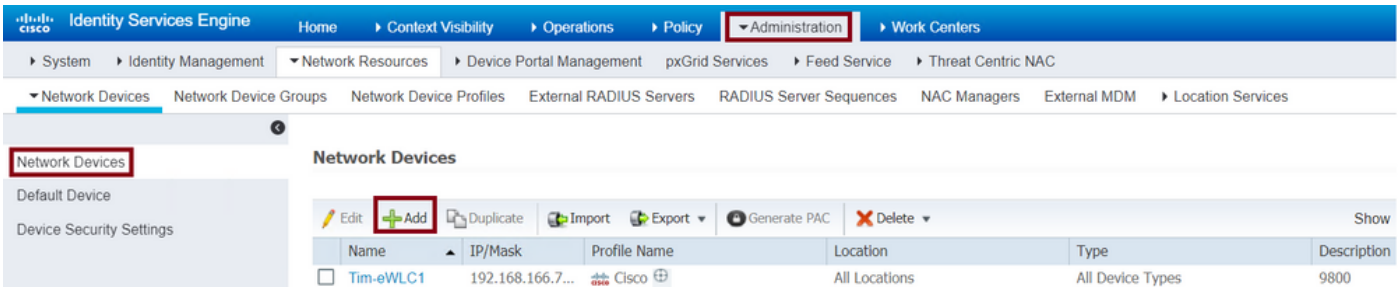
不再需要。定義遠端使用者。在ISE上為接待大使建立的使用者名稱必須定義為WLC上的遠端使用者名稱。如果沒有在WLC中定義遠端使用者名稱，身份驗證將正確進行，但是，將授予使用者對WLC的完全訪問許可權，而不是僅授予使用者對Lobby Ambassador許可權的許可權。此配置只能透過CLI完成。

CLI：

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

配置ISE - RADIUS

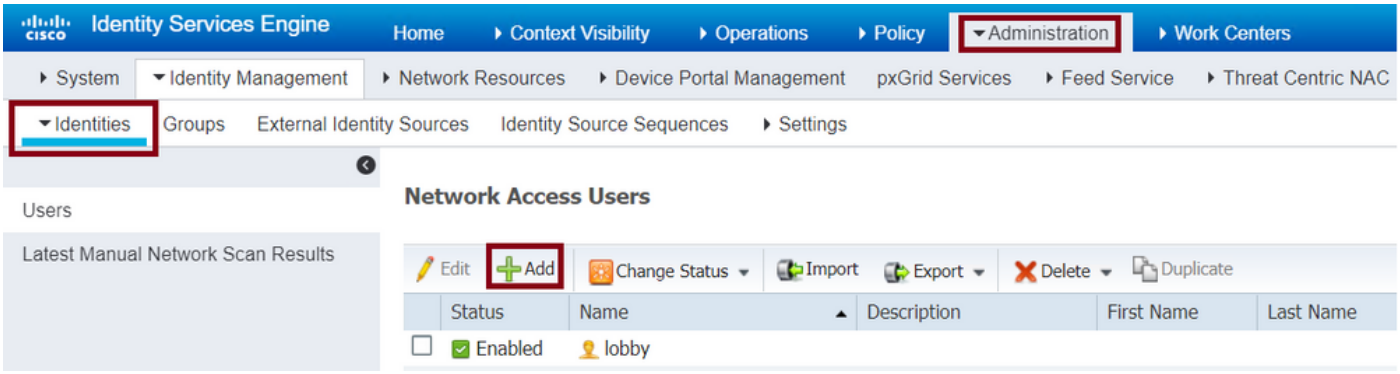
步驟 1.將WLC增加到ISE。導航到管理>網路資源>網路裝置>增加。需要將WLC增加到ISE。將WLC增加到ISE時，啟用RADIUS身份驗證設定並配置所需的引數，如圖所示。



當配置窗口打開時，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。

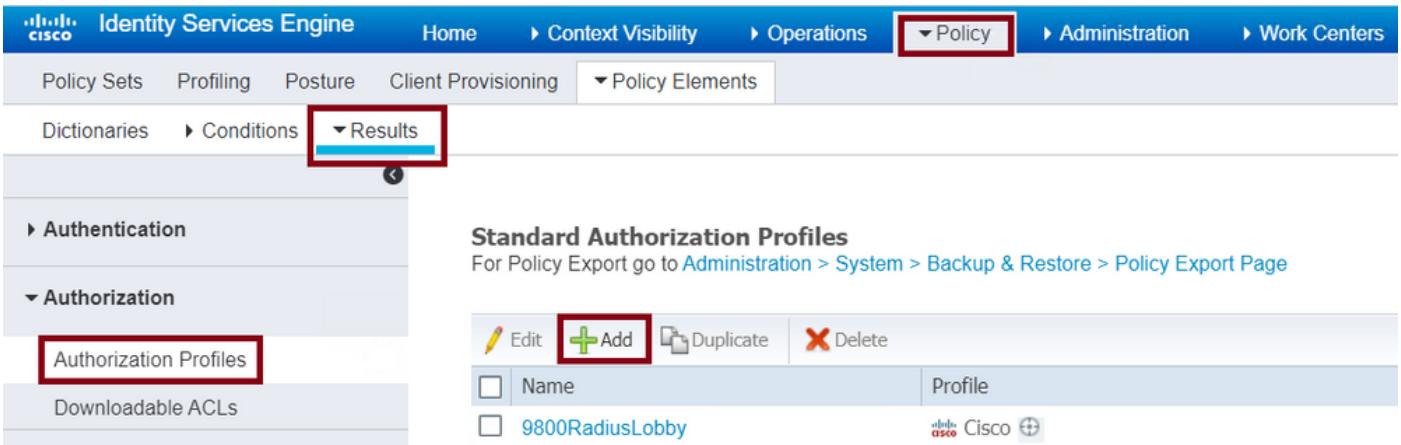
步驟 2.在ISE上建立接待大使使用者。導航到管理>身份管理>身份>使用者>增加。

將分配給建立訪客使用者的接待大使的使用者名稱和密碼增加到ISE。這是管理員將分配給接待大使的使用者名稱。

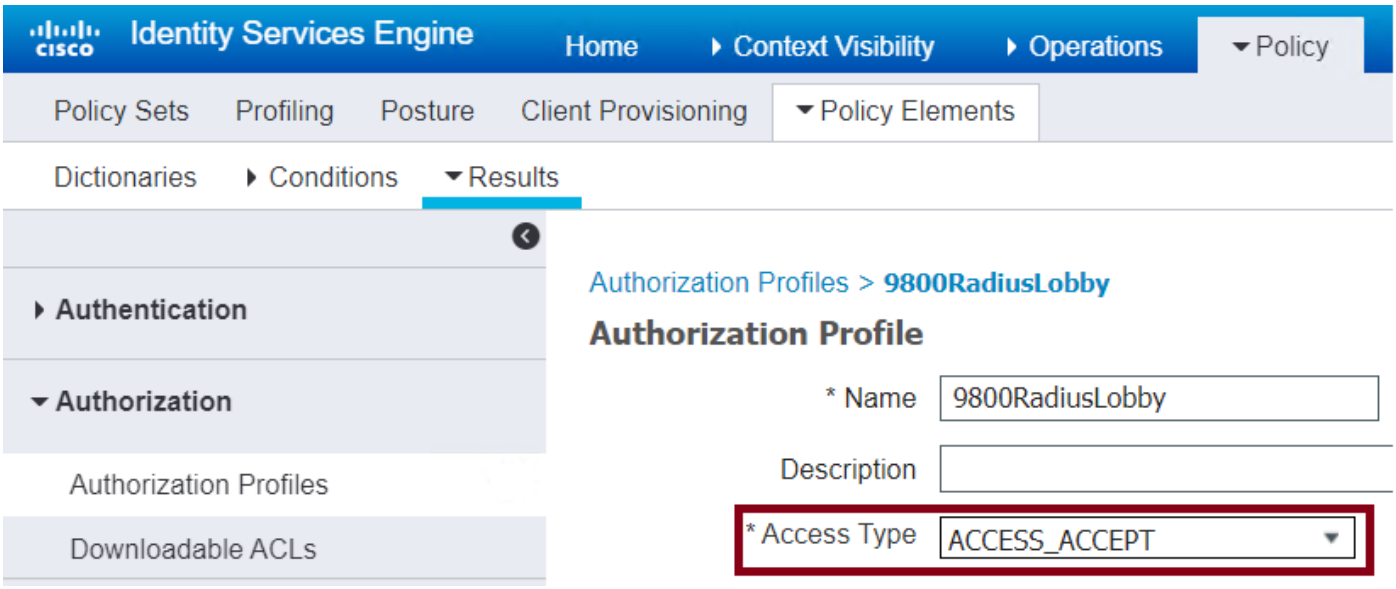


當配置窗口打開時，請提供接待大使使用者的名稱和密碼。此外，請確認「狀態」為「已啟用」。

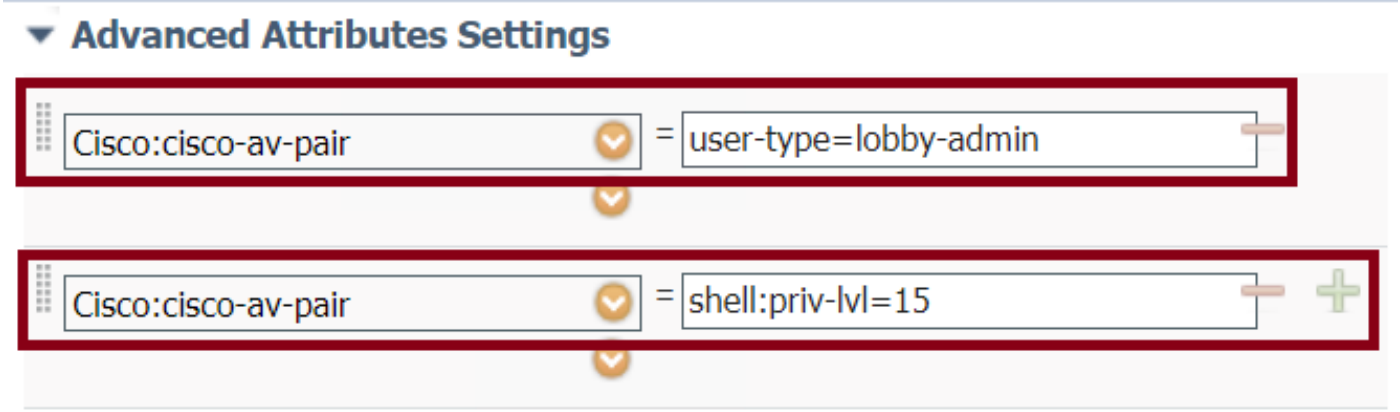
步驟 3.建立結果授權配置檔案。導航到策略>策略元素>結果>授權>授權配置檔案>增加。建立結果授權設定檔，以便將Access-Accept傳回WLC，並具備所需的屬性，如下圖所示。

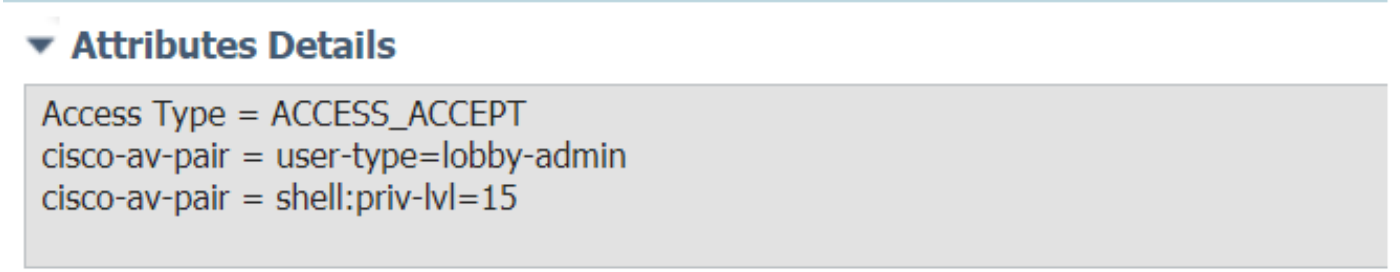


確認設定檔已設定為傳送「Access-Accept」，如下圖所示。



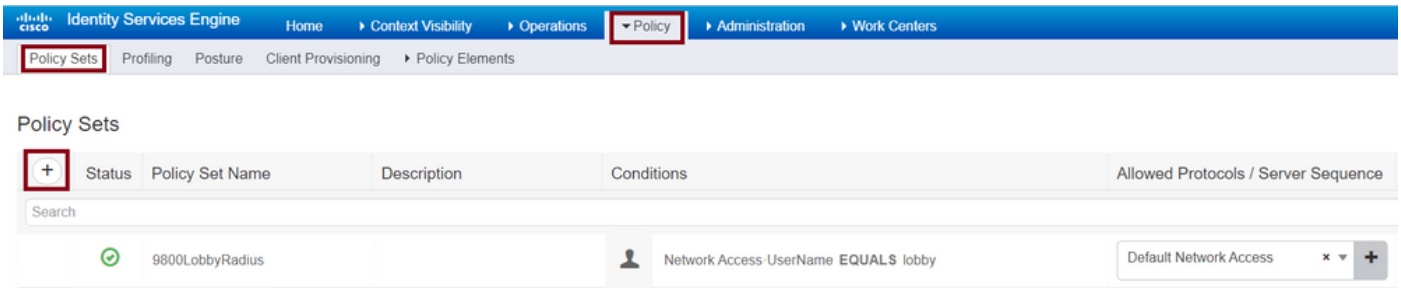
您需要在「進階屬性設定」下手動新增屬性。需要這些屬性以將使用者定義為接待大使並提供許可權，以便允許接待大使進行所需的更改。



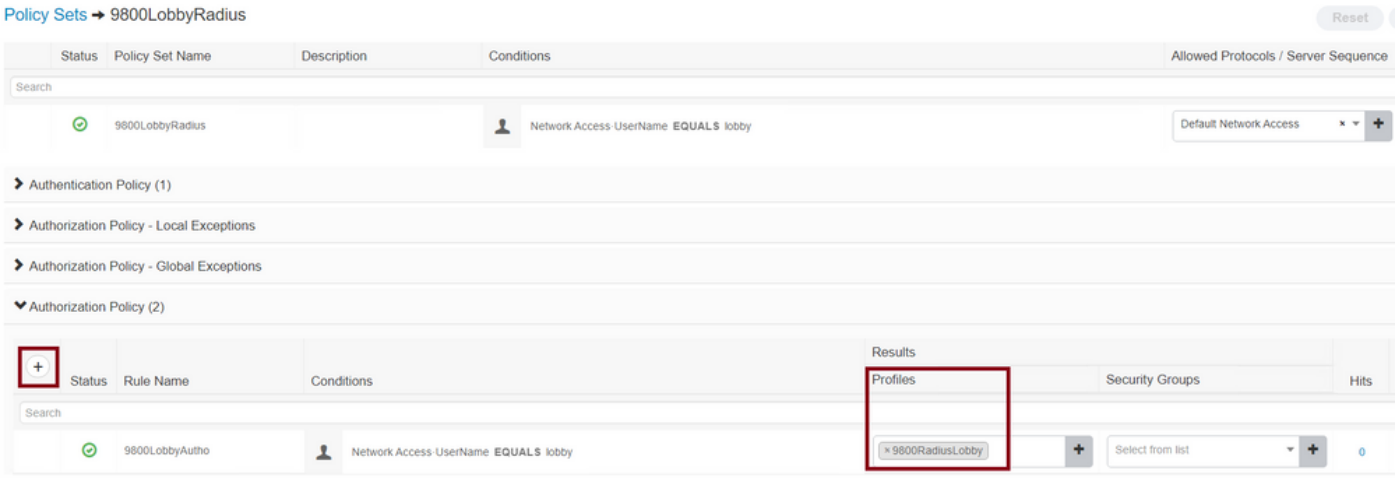


步驟 4.建立策略以處理身份驗證。導航到策略>策略集>增加。配置策略的條件取決於管理員的決定。此處使用「網路訪問使用者名稱」條件和預設網路訪問協定。

務必確保在「Authorization Policy」下選擇了「Results Authorization」下配置的配置檔案，這樣您才能將所需的屬性返回到WLC，如下圖所示。



當配置窗口打開時，配置授權策略。身份驗證策略可以保留為預設值。



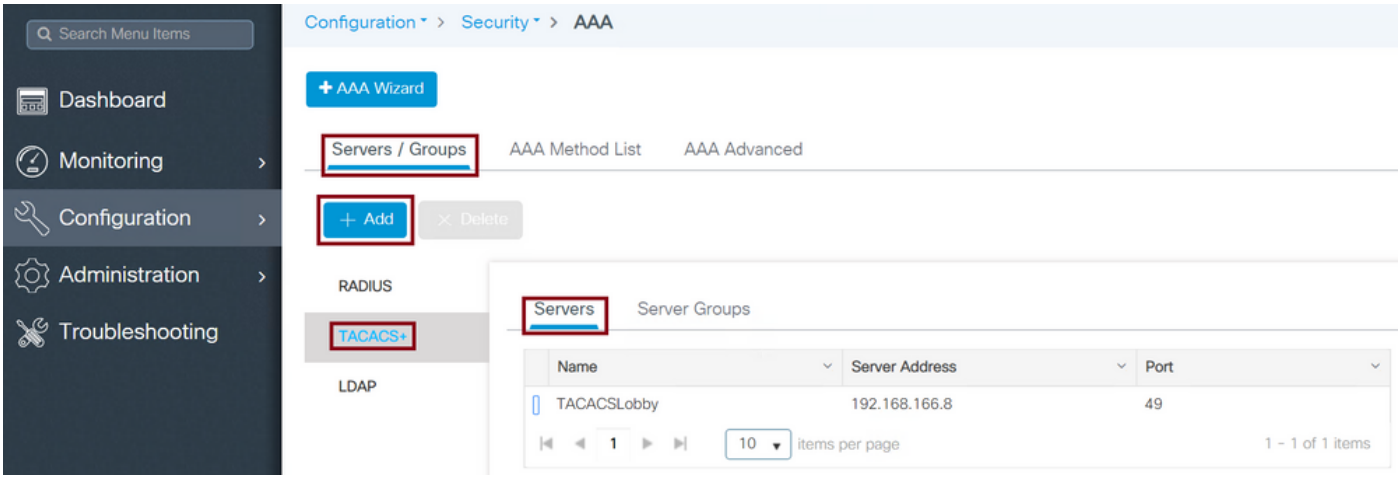
驗證TACACS+

在WLC上配置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。



當配置窗口打開時，必需的配置引數為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。其他任何引數都可以保留為預設值，也可以視需要配置。

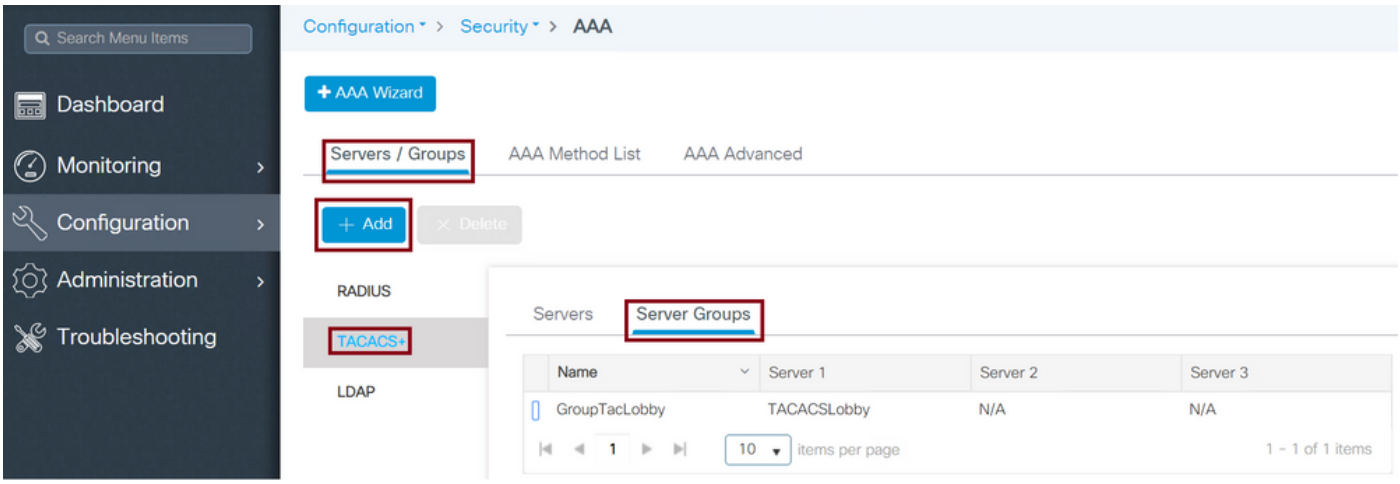
CLI：

```
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+伺服器增加到伺服器組。定義伺服器組並增加所配置的TACACS+伺服器。這將會是用來進行驗證的TACACS+伺服器。

GUI：

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



當配置窗口打開時，為該組指定名稱，並將所需的TACACS+伺服器從Available Servers清單移到Assigned Servers清單。

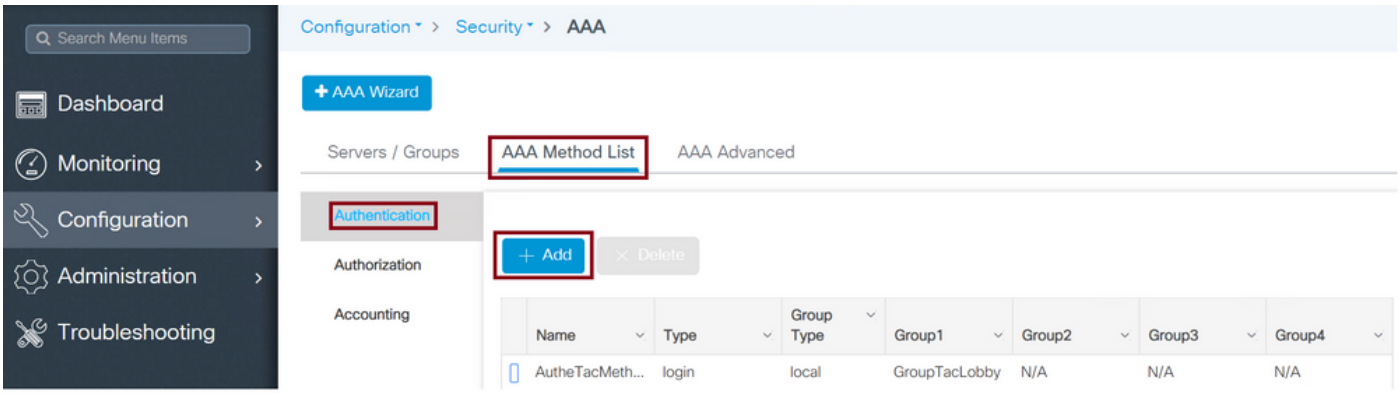
CLI：

```
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，並且還會將其附加到已配置的伺服器組。它還可選擇身份驗證是在WLC上本地進行，還是在TACACS+伺服器的外部進行。

GUI：

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

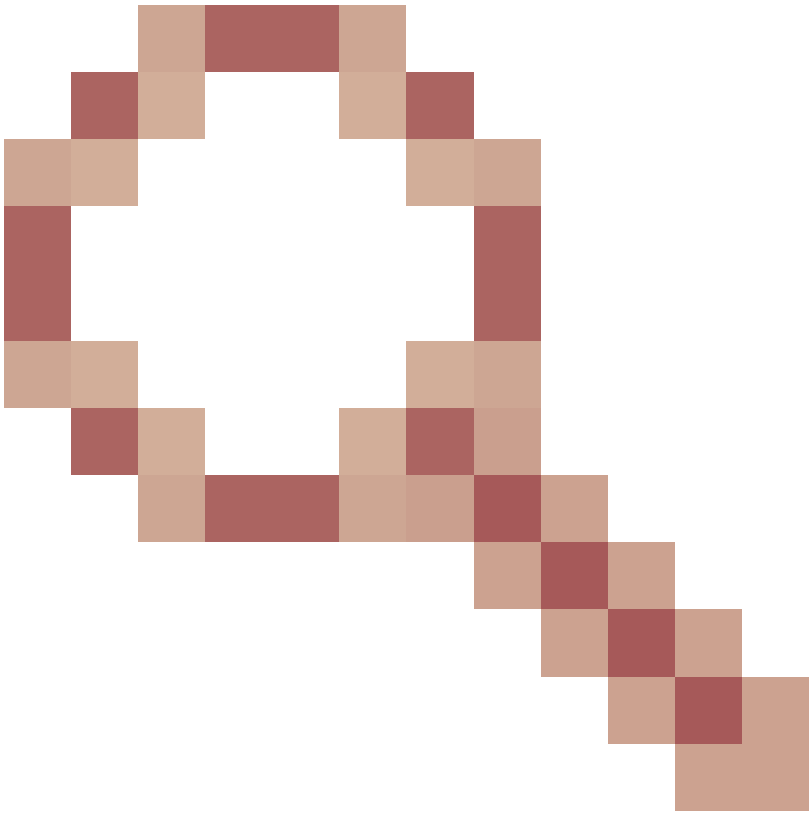


當配置窗口打開時，請提供名稱，選擇Login作為type選項，並分配之前建立的伺服器組。

群組型別為本機。

GUI：

如果您選取[群組型別]為[本機]，WLC會先檢查本機資料庫中是否存在該使用者，然後只有在本機資料庫中找不到Lobby Ambassador使用者時，才會回退至[伺服器群組]。



注意：請注意此Bug CSCvs87163，
已在17.3中進行了修復。

CLI：

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

群組型別為群組。

GUI：

如果選擇Group Type as group並且未選中Fallback to local選項，則WLC將僅檢查伺服器組的使用者，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
```

群組型別為群組且已核取「回退至本機」選項。

GUI：

如果您選擇Group Type作為「group」，並且選中了Fallback to local選項，則WLC將根據伺服器組檢查使用者，並且僅在TACACS伺服器在響應中超時時查詢本地資料庫。如果伺服器傳送拒絕訊息，則使用者不會透過驗證，即使本機資料庫中有該使用者也不例外。

CLI：

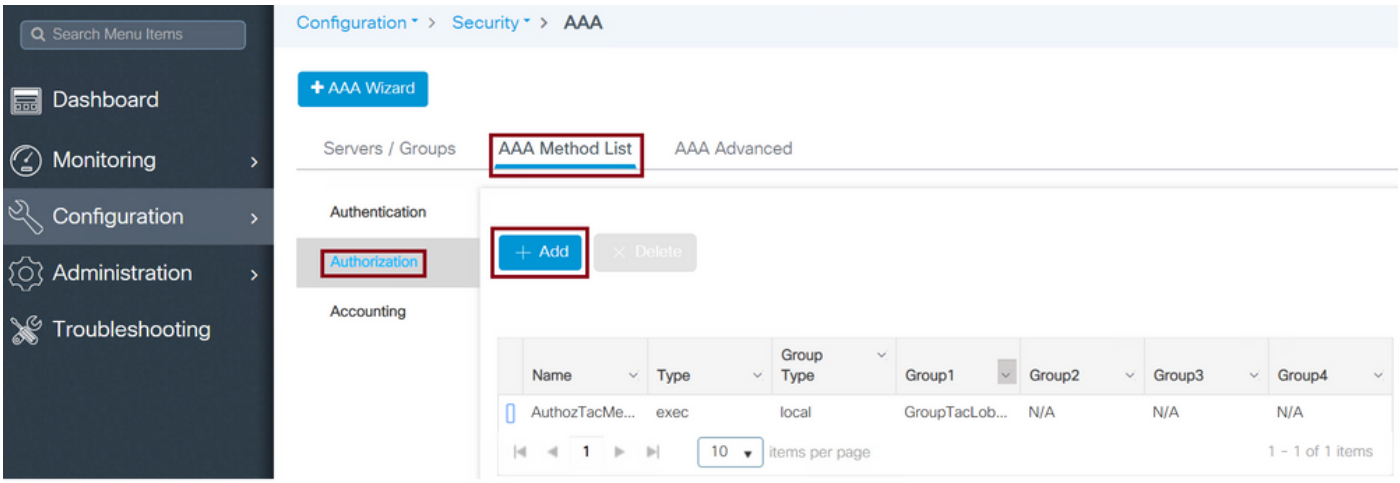
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

步驟 4.建立授權方法清單。

Authorization Method List將定義接待大使所需的授權型別，在本例中是執行型。它還連線到配置的同一伺服器組。也可選擇驗證是在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）。



當組態視窗開啟時，請提供名稱，選取exec作為type選項，並指定先前建立的Server Group。

請注意，「群組型別」的套用方式與「驗證方法清單」部分中說明的套用方式相同。

CLI：

群組型別為本機。

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

群組型別為群組。

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

群組型別為群組且已核取[Fallback to local]選項。

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

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

HTTP/GUI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
```

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
```

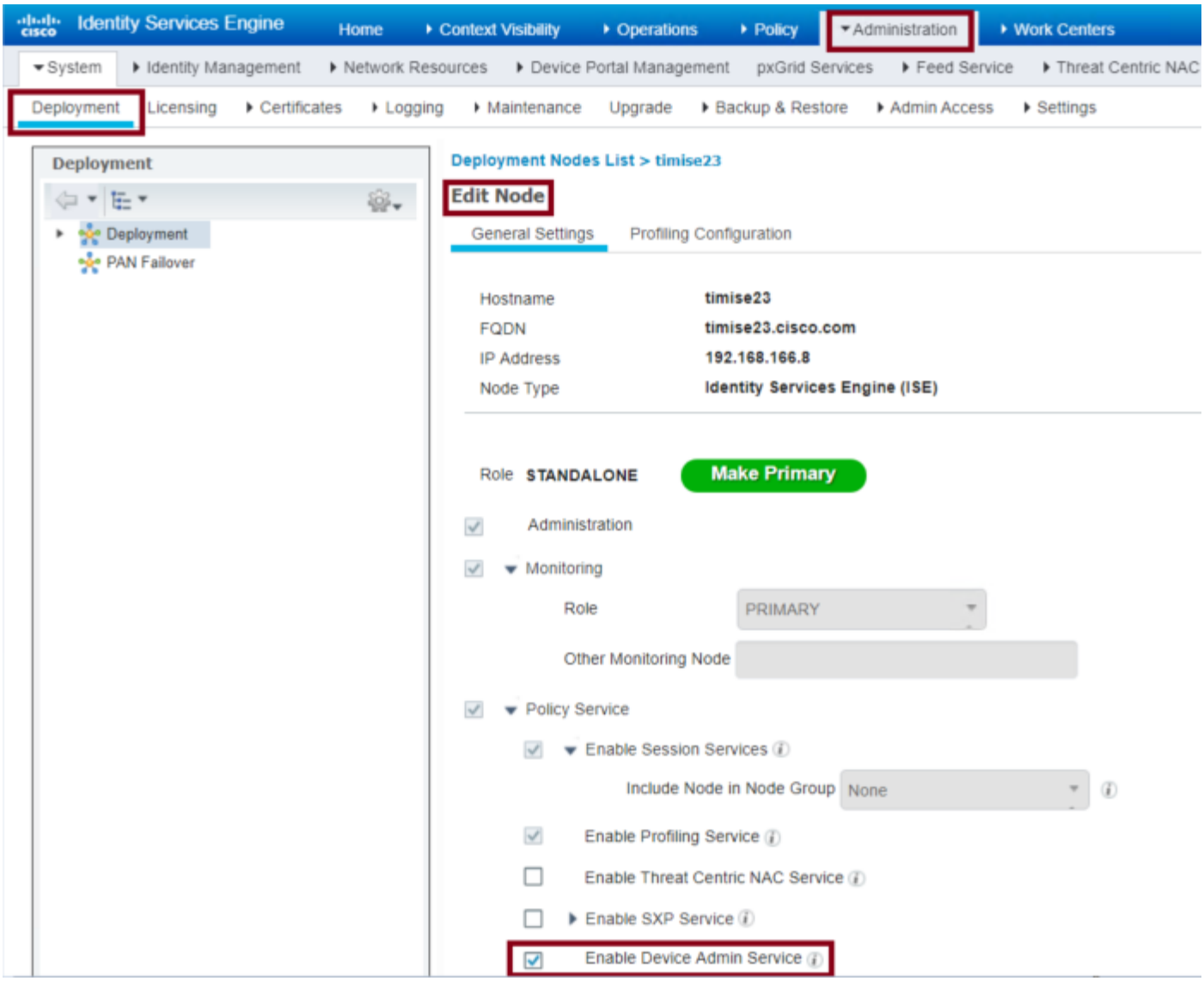
步驟 6. 定義遠端使用者。在ISE上為接待大使建立的使用者名稱必須定義為WLC上的遠端使用者名稱。如果沒有在WLC中定義遠端使用者名稱，身份驗證將正確進行，但是，將授予使用者對WLC的完全訪問許可權，而不是僅授予使用者對Lobby Ambassador許可權的許可權。此配置只能透過CLI完成。

CLI：

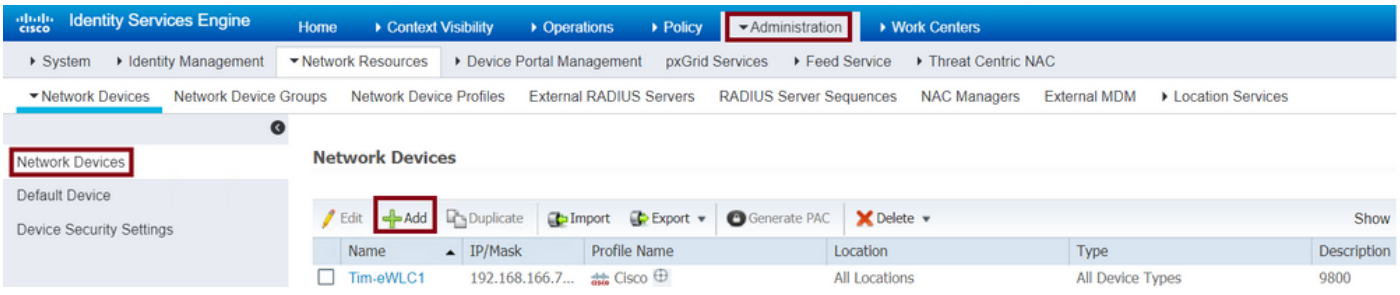
```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

配置ISE - TACACS+

步驟 1. 啟用Device Admin。導航到管理>系統>部署。在您繼續下一步之前，請選擇Enable Device Admin Service，並確保ISE已啟用，如圖所示。

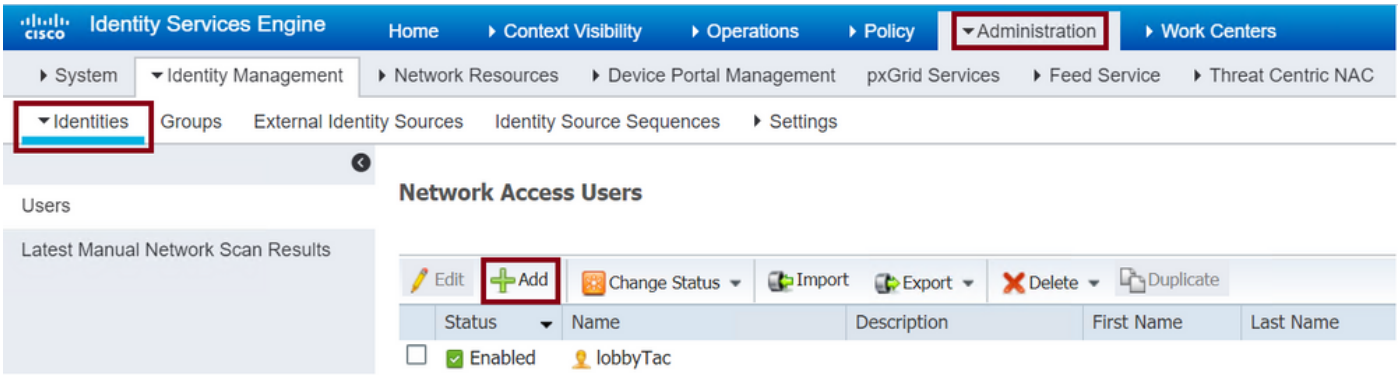


步驟 2.將WLC增加到ISE。導航到管理>網路資源>網路裝置>增加。需要將WLC增加到ISE。將WLC增加到ISE時，啟用TACACS+身份驗證設定並配置所需的引數，如圖所示。



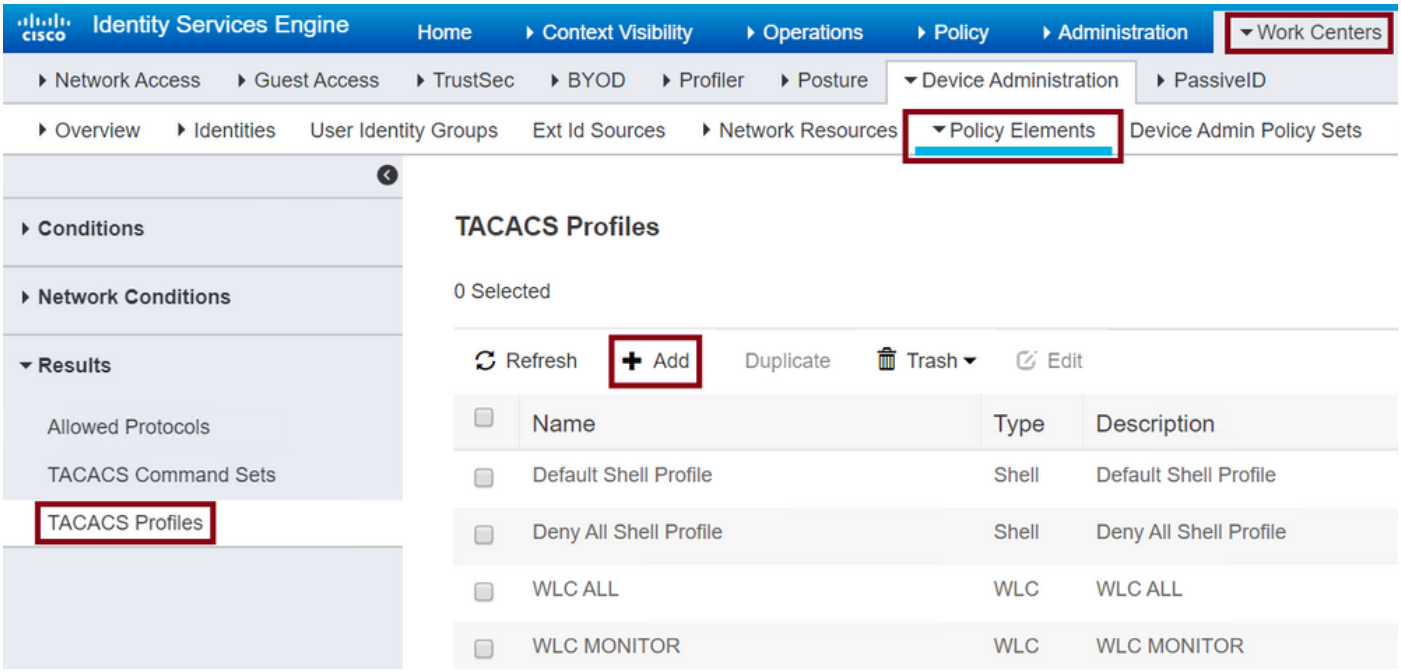
當配置窗口打開以提供名稱IP ADD時，啟用TACACS+身份驗證設定並輸入所需的共用金鑰。

步驟 3.在ISE上建立接待大使使用者。導航到管理>身份管理>身份>使用者>增加。增加至ISE，為將建立訪客使用者的接待大使分配的使用者名稱和密碼。這是管理員指定給接待大使的使用者名稱，如下圖所示。

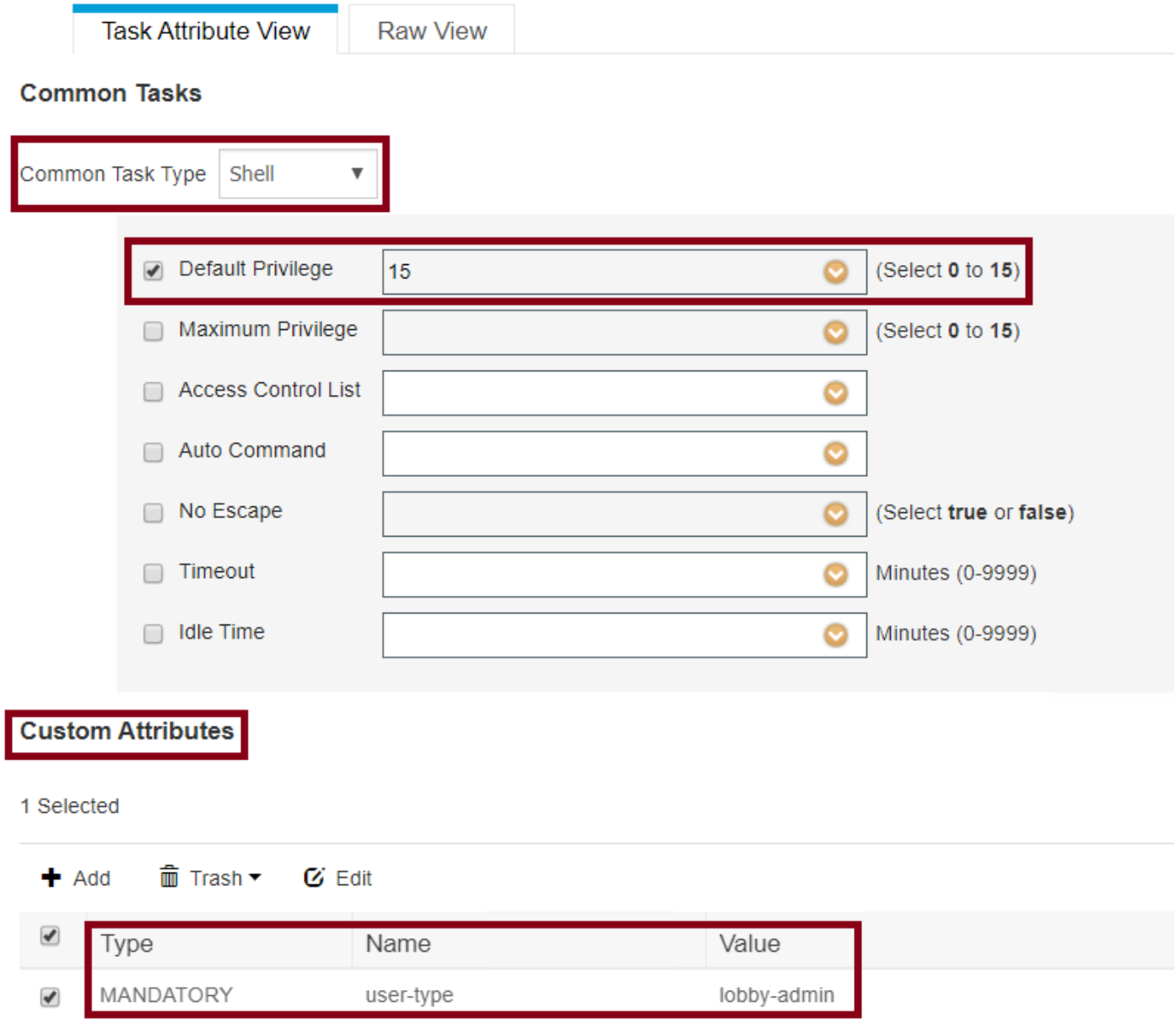


當配置窗口打開時，請提供接待大使使用者的名稱和密碼。此外，請確認「狀態」為「已啟用」。

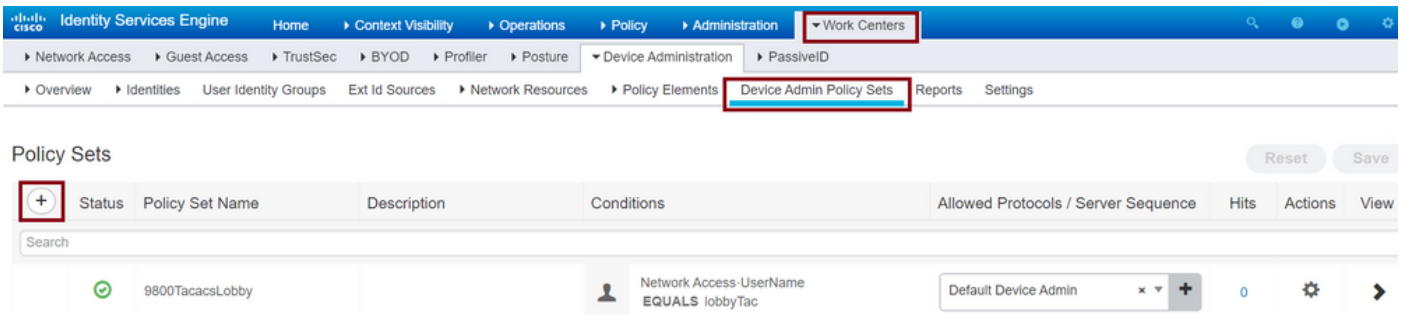
步驟 4.建立結果TACACS+配置檔案。導覽至Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles，如下圖所示。透過此設定檔，將所需的屬性傳回WLC，以便將使用者定位為接待大使。



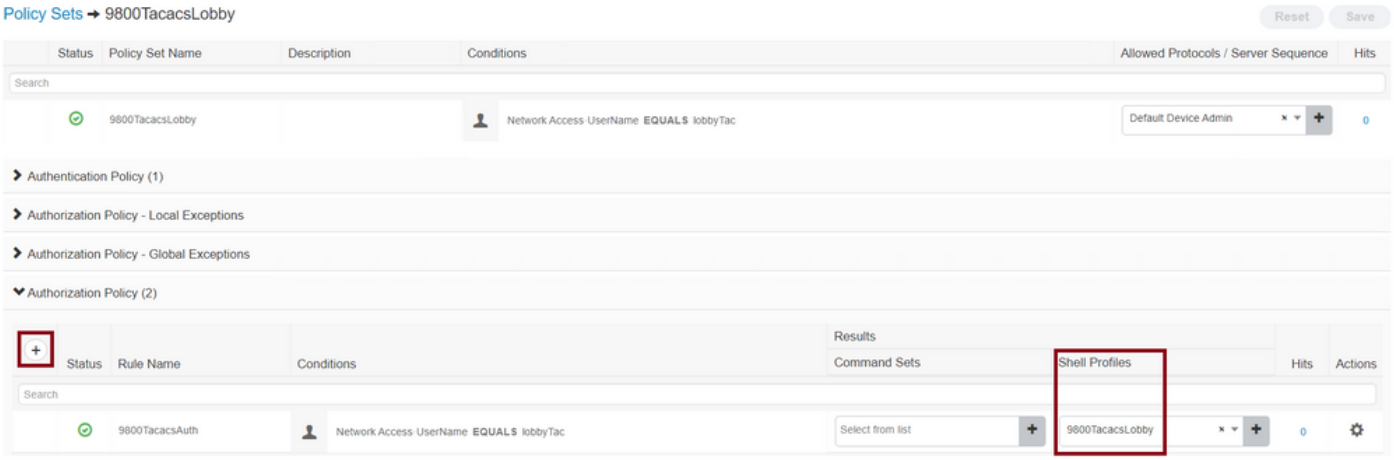
當配置窗口打開時，為配置檔案提供一個名稱，同時將Default Privileged 15和Custom Attribute配置為Type Mandatory，將name配置為user-type和value lobby-admin。此外，還可將常見任務型別選擇為Shell，如下圖所示。



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Network Access-Username條件和預設裝置管理協定。在授權策略下，必須確保在結果授權下配置的配置檔案處於選中狀態，這樣您才能將所需的屬性返回到WLC。



當配置窗口打開時，配置授權策略。「Authentication Policy（身份驗證策略）」可以保留為預設值，如圖所示。

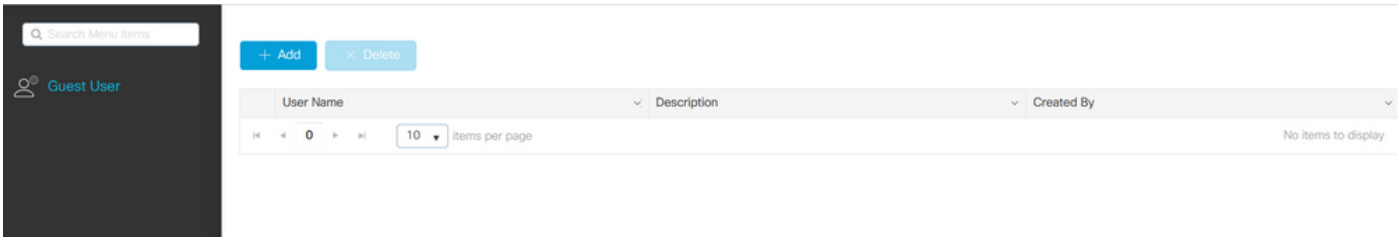


驗證

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的外觀如下所示。



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

對於RADIUS身份驗證，可以使用以下調試：

```
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伺服器會使用正確的使用者名稱、使用者型別和許可權返回所需的屬性。

```
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+

對於TACACS+身份驗證，可以使用以下調試：

```
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。另外，必須看到「PASS」狀態。在同一調試中，身份驗證階段結束後，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和正確的ISE IP ADD。在此階段，您可以檢視ISE上配置的屬性，這些屬性表明WLC是擁有適當許可權的大廳大使使用者。

驗證階段範例：

```
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)
```

授權階段範例：

```
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+調試示例包含成功登入的關鍵步驟。調試更加詳細，輸出將更大。要停用調試，可以使用以下命令：

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

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）。