配置基於ISE的WLC到Active Directory組對映的動態VLAN分配

目錄

簡介

本檔案介紹動態VLAN指派的概念。

必要條件

本文說明如何設定無線LAN控制器(WLC)和身分辨識服務引擎(ISE)伺服器，以便動態地將無線LAN(WLAN)使用者端指派到特定VLAN。

需求

思科建議您瞭解以下主題：

- 無線區域網路控制器(WLC)和輕量存取點(LAP)的基本知識
- 身份驗證、授權和記帳(AAA)伺服器（例如ISE）的功能知識
- 全面瞭解無線網路和無線安全問題
- 動態VLAN分配的功能和配置知識
- 基本瞭解Microsoft Windows AD服務，以及域控制器和DNS概念
- 具備存取點通訊協定(CAPWAP)控制與布建的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5520系列WLC（執行韌體版本8.8.111.0）
- Cisco 4800系列AP
- 本地Windows請求方和Anyconnect NAM
- 思科安全ISE版本2.3.0.298
- Microsoft Windows 2016 Server配置為域控制器
- 執行版本15.2(4)E1的Cisco 3560-CX系列交換器

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

使用RADIUS伺服器進行動態VLAN分配

在大多數WLAN系統中，每個WLAN都有一個靜態策略，該策略適用於與服務集識別符號(SSID)或控制器術語中的WLAN相關聯的所有客戶端。此方法雖然功能強大，但有一定的侷限性，因為它要求客戶端與不同的SSID關聯以繼承不同的QoS和安全策略。

Cisco WLAN解決方案透過支援身份網路解決了這一限制。 這允許網路通告單個SSID，但允許特定使用者根據使用者憑證繼承不同的QoS、VLAN屬性和/或安全策略。

動態VLAN分配是一種功能，可根據使用者提供的憑證將無線使用者置於特定VLAN中。將使用者分配到特定VLAN的任務由RADIUS身份驗證伺服器（如Cisco ISE）處理。例如，這可用於允許無線主機在園區網路中移動時保持在相同的VLAN上。

思科ISE伺服器根據多個可能的資料庫之一（包括其內部資料庫）對無線使用者進行身份驗證。舉例來說：

- 內部DB
- Active Directory
- 通用輕量型目錄存取通訊協定(LDAP)
- 開放資料庫連線(ODBC)相容關聯式資料庫
- Rivest、Shamir和Adelman (RSA) SecurID令牌伺服器
- 與RADIUS相容的權杖伺服器

Cisco ISE身份驗證協定和支援的外部身份源列出了ISE內部和外部資料庫支援的各種身份驗證協定。

本文檔重點介紹如何對使用Windows Active Directory外部資料庫的無線使用者進行身份驗證。

身份驗證成功後，ISE從Windows資料庫中檢索該使用者的組資訊，並將該使用者關聯到相應的授權配置檔案。

當客戶端嘗試與註冊到控制器的LAP關聯時，LAP會藉助相應的EAP方法將使用者的憑證傳遞到WLC。

WLC使用RADIUS協定（封裝EAP）將這些憑證傳送到ISE，ISE將使用者的憑證傳遞到AD以在KERBEROS協定的幫助下進行驗證。

AD驗證使用者憑證，並在身份驗證成功後通知ISE。

身份驗證成功後，ISE伺服器會將某些Internet工程任務組(IETF)屬性傳遞到WLC。這些RADIUS屬性決定了必須分配給無線客戶端的VLAN ID。使用者端的SSID （WLAN，從WLC的角度而言）並不重要，因為系統一律會將使用者指定給這個預先設定的VLAN ID。

用於VLAN ID分配的RADIUS使用者屬性包括：

- IETF 64（隧道型別）—將其設定為VLAN
- IETF 65（隧道介質型別）—將此值設定為802
- IETF 81（隧道專用組ID）—將其設定為VLAN ID

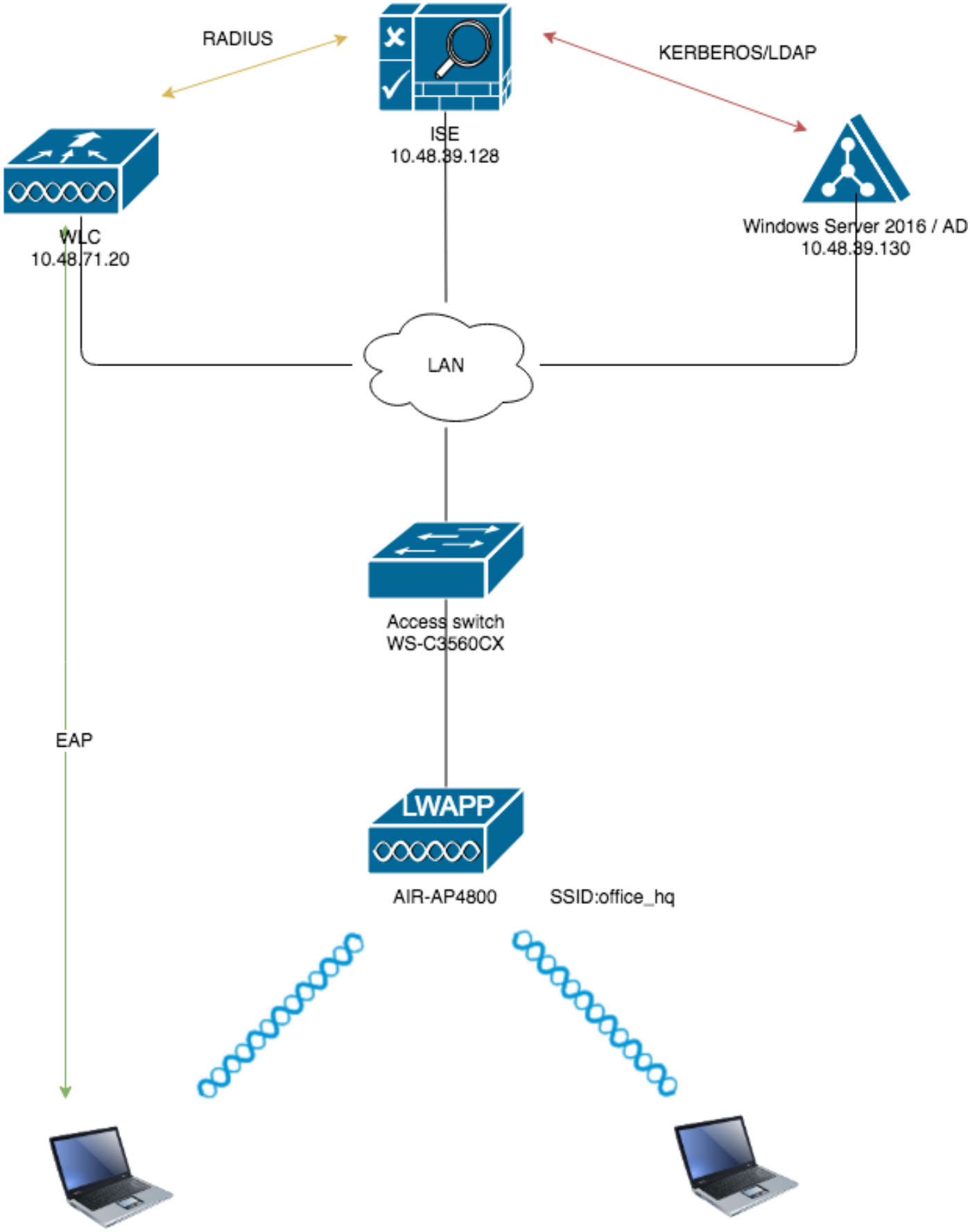
VLAN ID為12位，取值範圍為1至4094（含）。由於Tunnel-Private-Group-ID屬於字串型別（如RFC2868中所定義，用於IEEE 802.1X），因此VLAN ID整數值被編碼為字串。傳送這些隧道屬性時，需要填寫標籤欄位。

如RFC 2868第3.1部分中所述：標籤欄位的長度為一個八位組，用於提供在同一資料包中分組參考同一隧道的屬性的方法。此欄位的有效值為0x01到0x1F （含）。如果「標籤」欄位未使用，它必須是零(0x00)。有關所有RADIUS屬性的詳細資訊，請參閱RFC 2868 。

設定

本節提供設定檔案中所述功能所需的資訊。

網路圖表

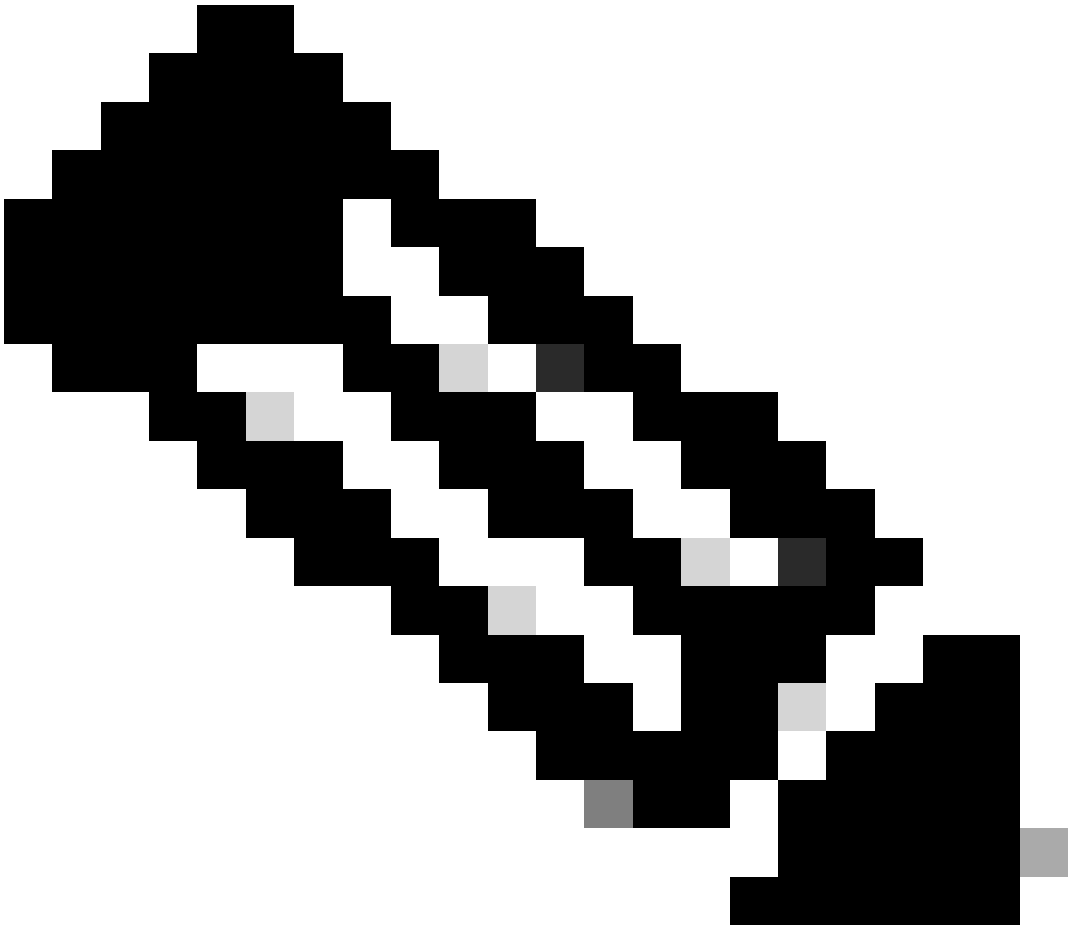


組態

以下是此圖中所用元件的配置詳細資訊：

- ISE (RADIUS)伺服器的IP地址是10.48.39.128。
- WLC的管理和AP管理器介面地址為10.48.71.20。
- DHCP伺服器駐留在LAN網路中，並且針對各個客戶端池進行了配置；圖中未顯示它。
- VLAN1477和VLAN1478用於此配置。市場行銷部門的使用者配置為置於VLAN1477中，而HR部門的使用者配置為由RADIUS伺服器置於VLAN1478中 當兩個使用者都連線到同一個SSID時— office_hq.

  VLAN1477:192.168.77.0/24。網關：192.168.77.1 VLAN1478:192.168.78.0/24。網關：192.168.78.1
- 本文檔使用帶PEAP-mschapv2的802.1x作為安全機制。



注意：Cisco建議您使用高級身份驗證方法，如EAP-FAST和EAP-TLS身份驗證，以便保護WLAN。

這些假設是在您執行此組態之前做出的：

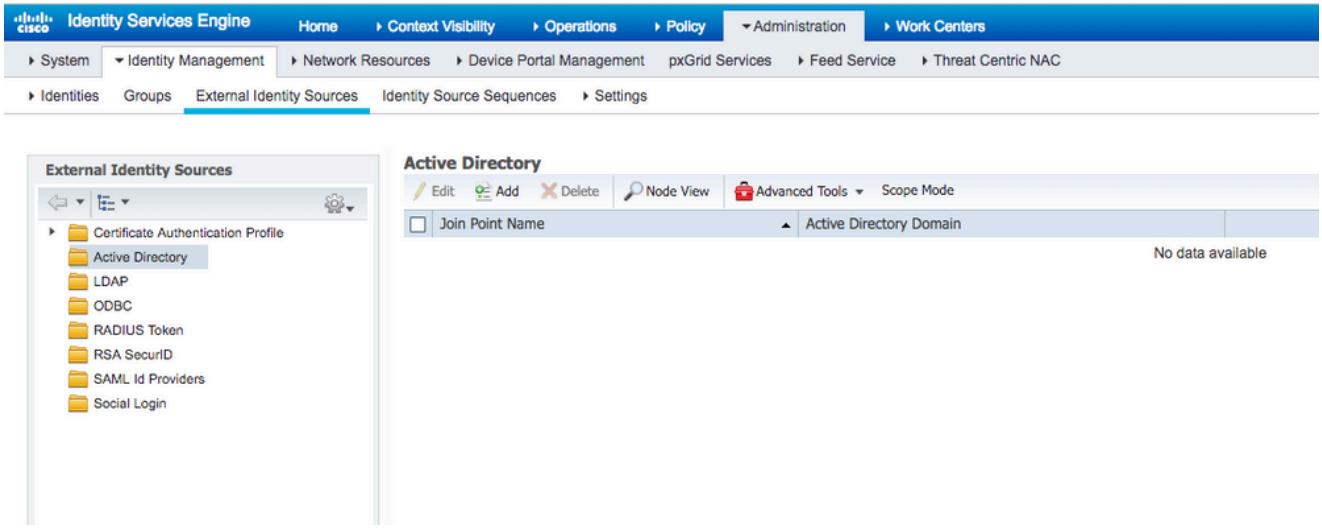
- LAP已註冊到WLC
- 為DHCP伺服器分配了DHCP作用域
- 網路中所有裝置之間存在第3層連線
- 本文檔討論無線端所需的配置，並假設有線網路已就緒
- 在AD上配置了各自的使用者和組

要根據ISE到AD組對映透過WLC完成動態VLAN分配，必須執行以下步驟：

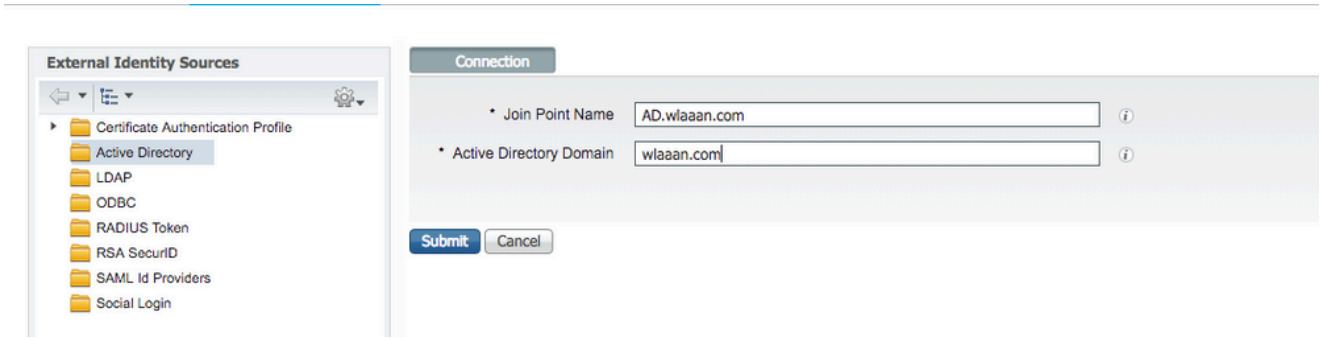
1. ISE到AD整合和配置ISE上使用者的身份驗證和授權策略。
2. 配置WLC，以支援SSID 'office_hq'的dot1x身份驗證和AAA覆蓋。
3. 最終客戶端請求方配置。

ISE到AD整合和配置ISE上使用者的身份驗證和授權策略

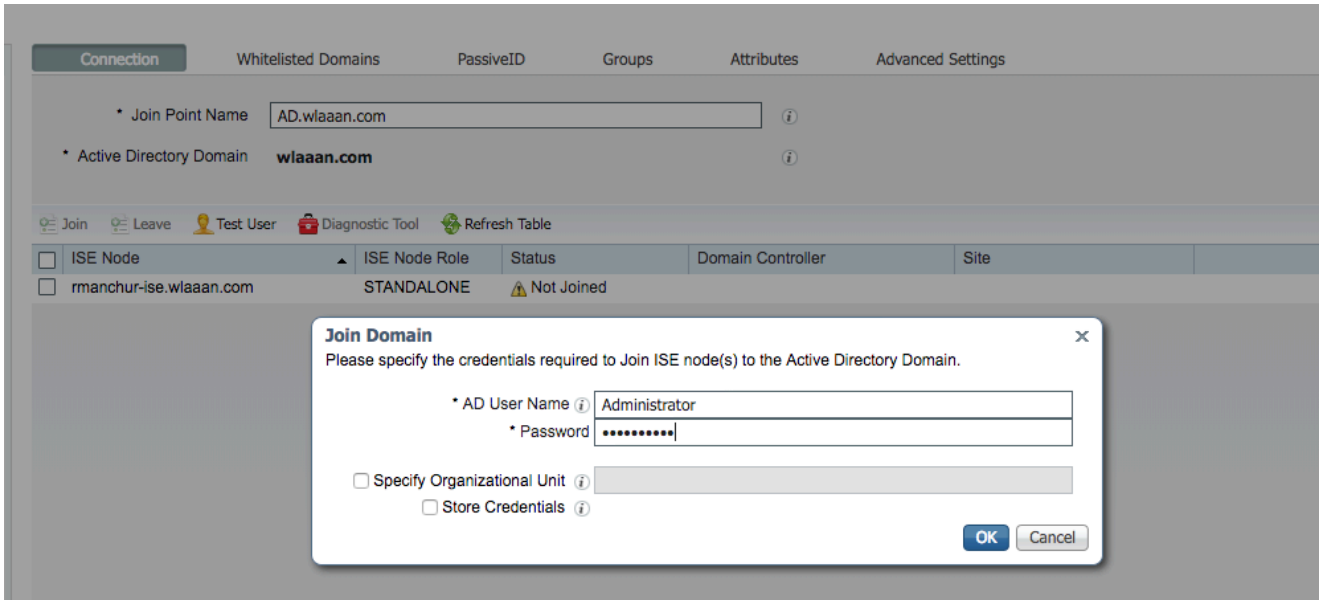
1. 使用admin帳戶登入ISE Web UI介面。
2. 導航到Administration > Identity management > External Identity Sources > Active directory。



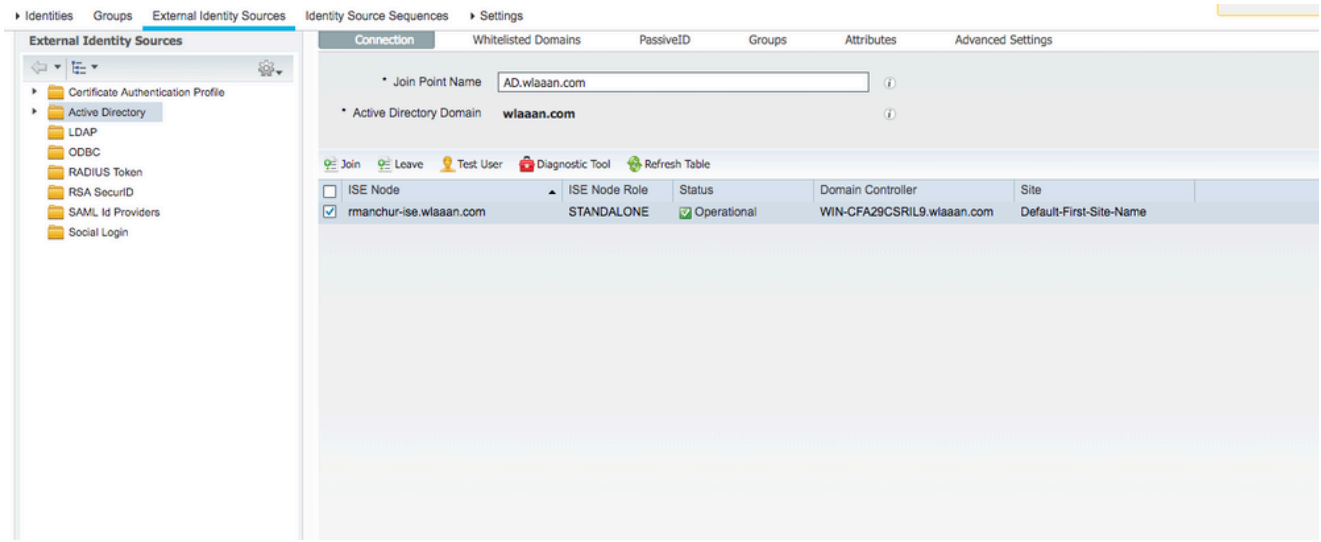
3. 按一下Add，然後從Active Directory加入點名稱設定輸入域名和身份庫名稱。在本例中，ISE註冊到域wlaaan.com，連線點指定為AD.wlaaan.com -對於ISE為本地重要名稱。



4. 按Submit下按鈕後，彈出窗口打開，詢問您是否要立即將ISE加入AD。按Yes，並提供具有管理員許可權的Active Directory使用者憑據以向域中增加新主機。



5. 在此之後，您必須將ISE成功註冊到AD。

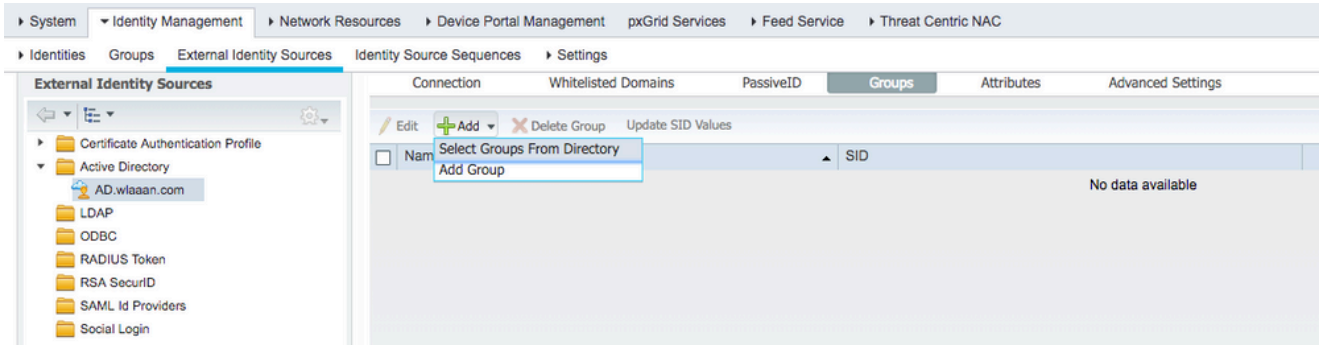


如果註冊過程有任何問題，您可以使用Diagnostic Tool 來運行AD連線所需的測試。

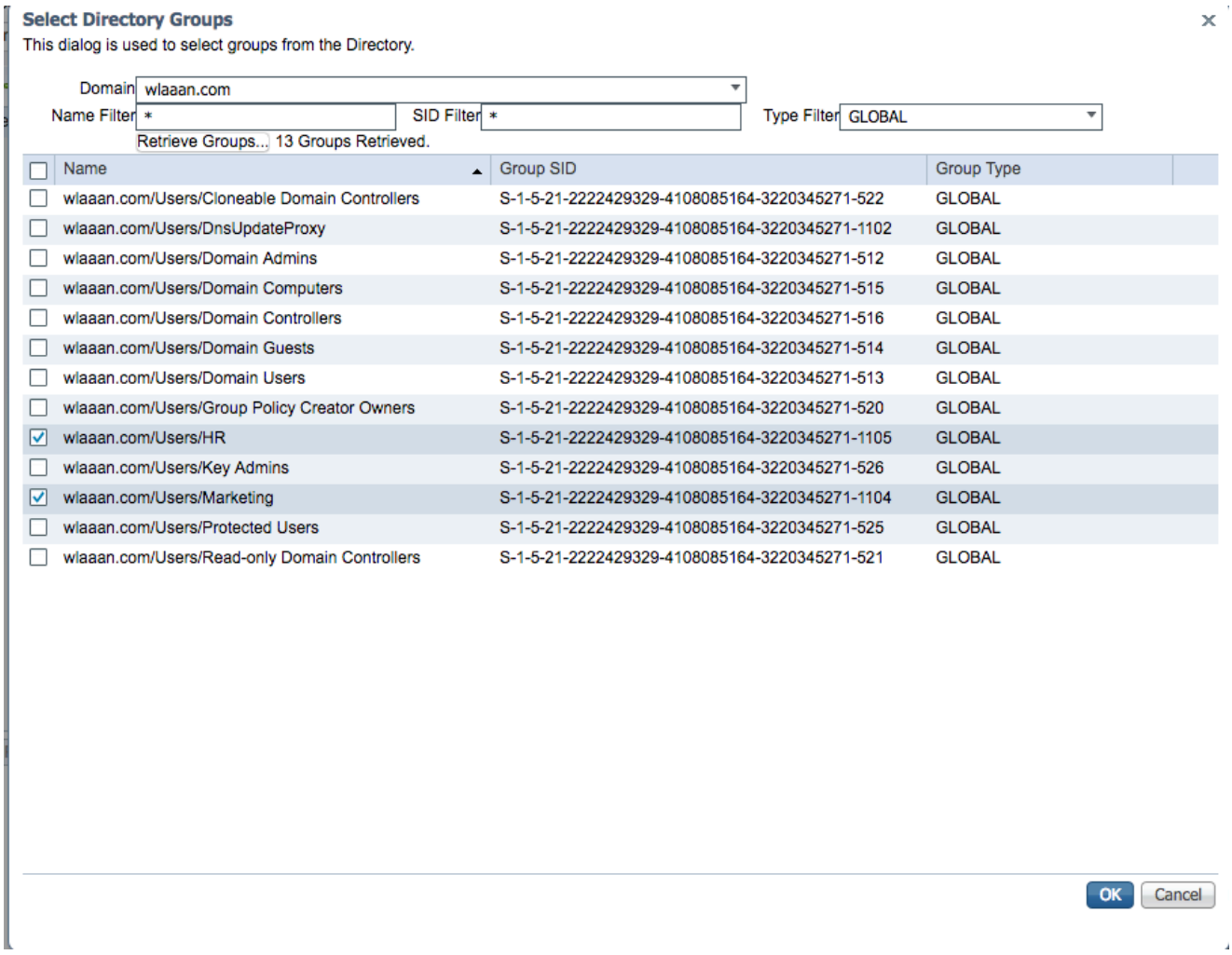
6. 您必須檢索用於分配相應授權配置檔案的活動目錄組。導航到Administration > Identity management > External Identity Sources > Active directory >

> Groups

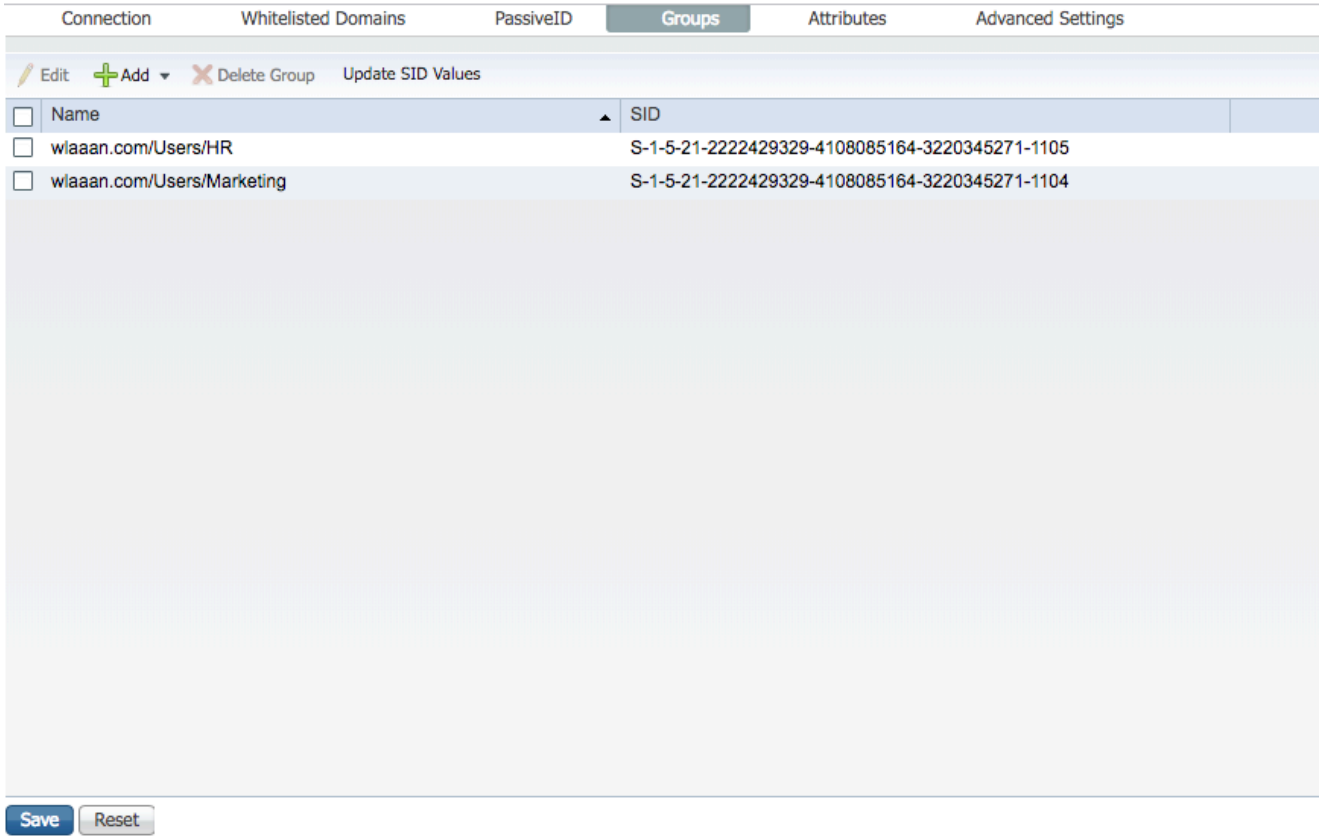
，然後點選Add並選擇Select Groups from Active Directory。



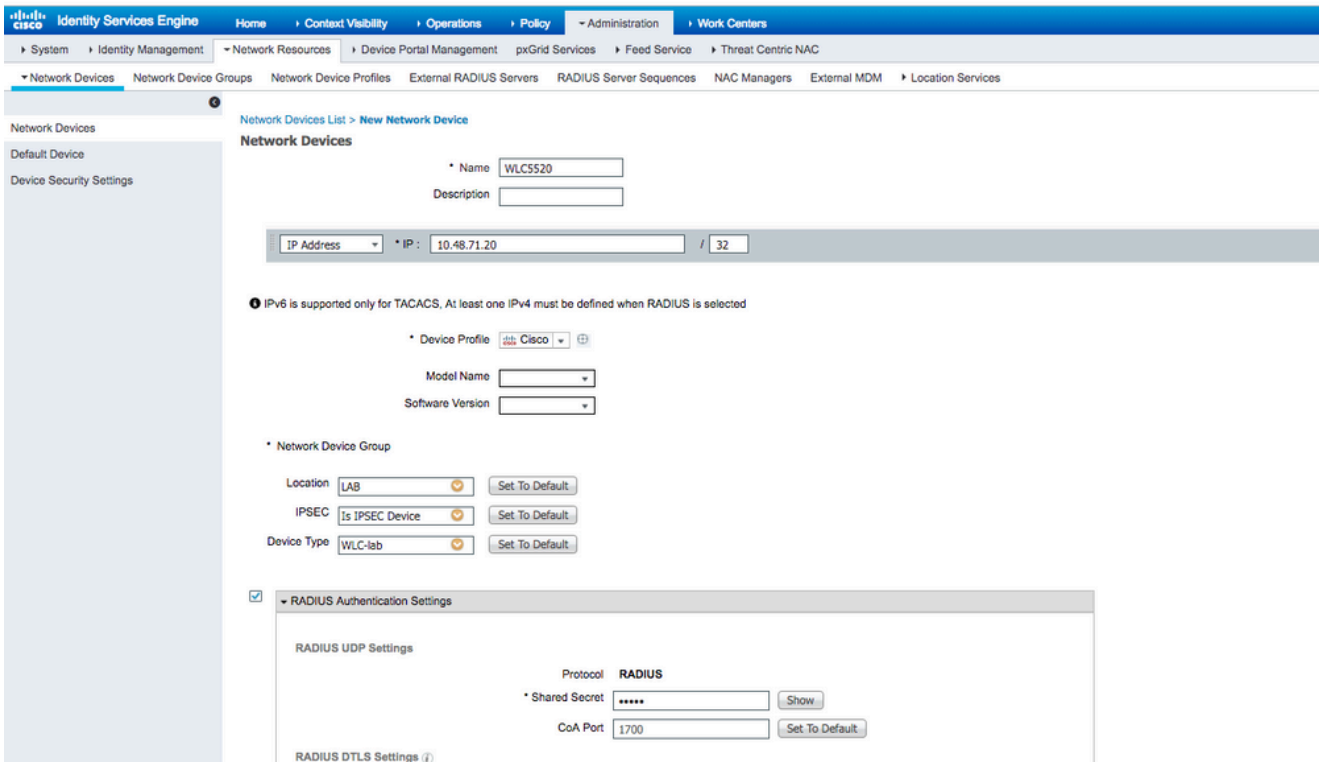
7. 新的彈出窗口隨即打開，您可以在其中指定過濾器以檢索特定組或從AD檢索所有組。從AD組清單中選擇相應的組，然後按OK。



8. 相應的組將增加到ISE並可儲存。按Save。

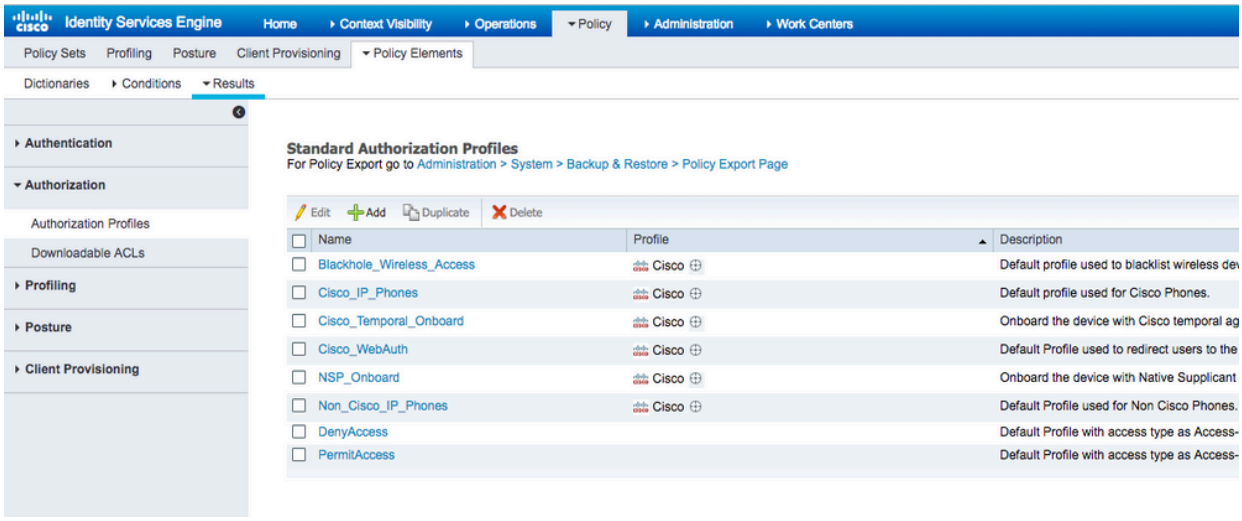


9. 將WLC增加到ISE網路裝置清單-導航到Administration > Network Resources > Network Devices ，然後按Add。在WLC和ISE之間提供WLC管理IP地址和RADIUS共用金鑰，從而完成配置。

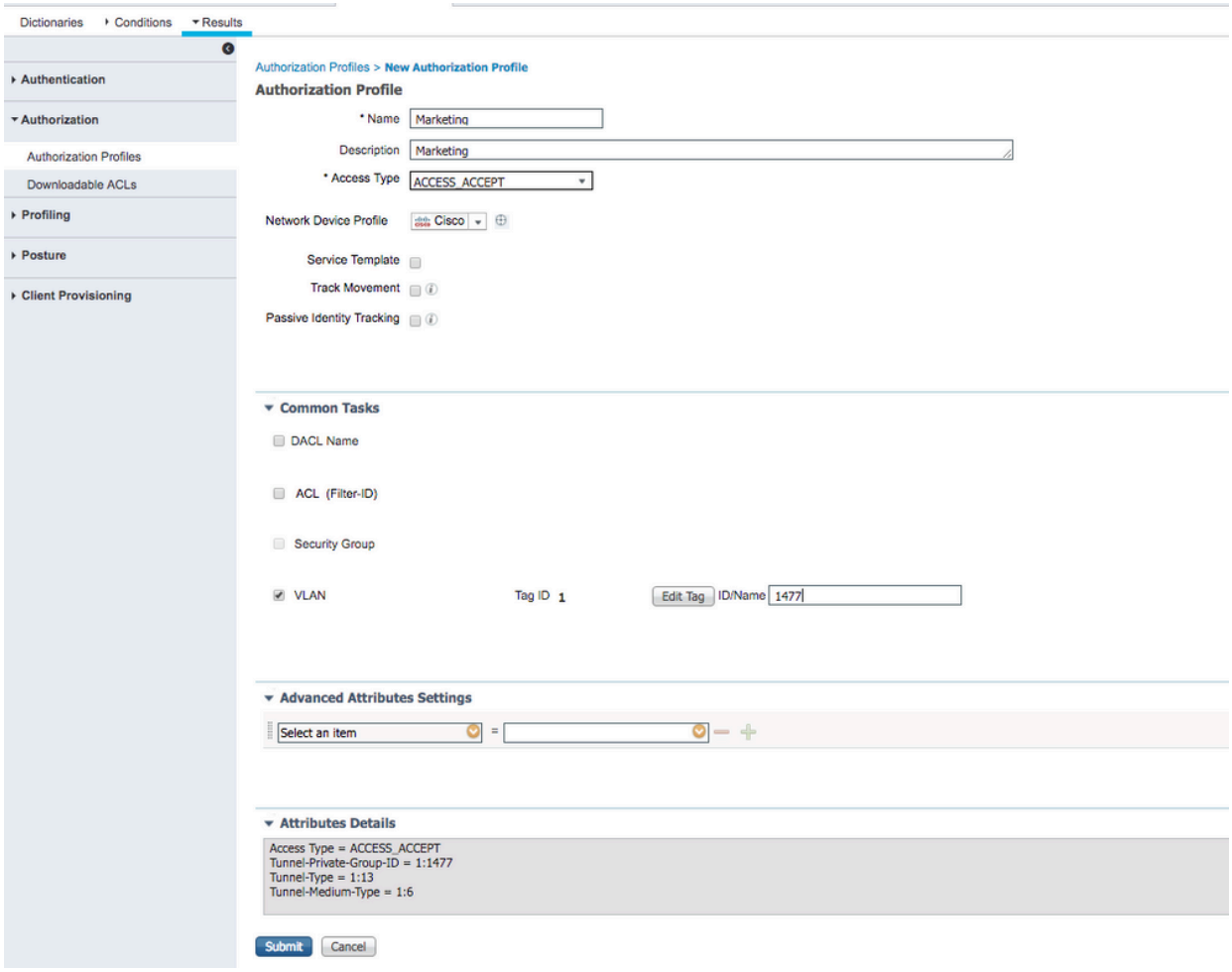


10. 現在，當您將ISE加入AD並將WLC增加到裝置清單後，您可以開始為使用者配置身份驗證和授權策略。

- 建立授權配置檔案，以將來自Marketing 的使用者分配到VLAN1477，將來自HR 組的使用者分配到VLAN1478。
  導航到Policy > Policy Elements > Results > Authorization > Authorization profiles ，然後按一下Add按鈕以建立新配置檔案。



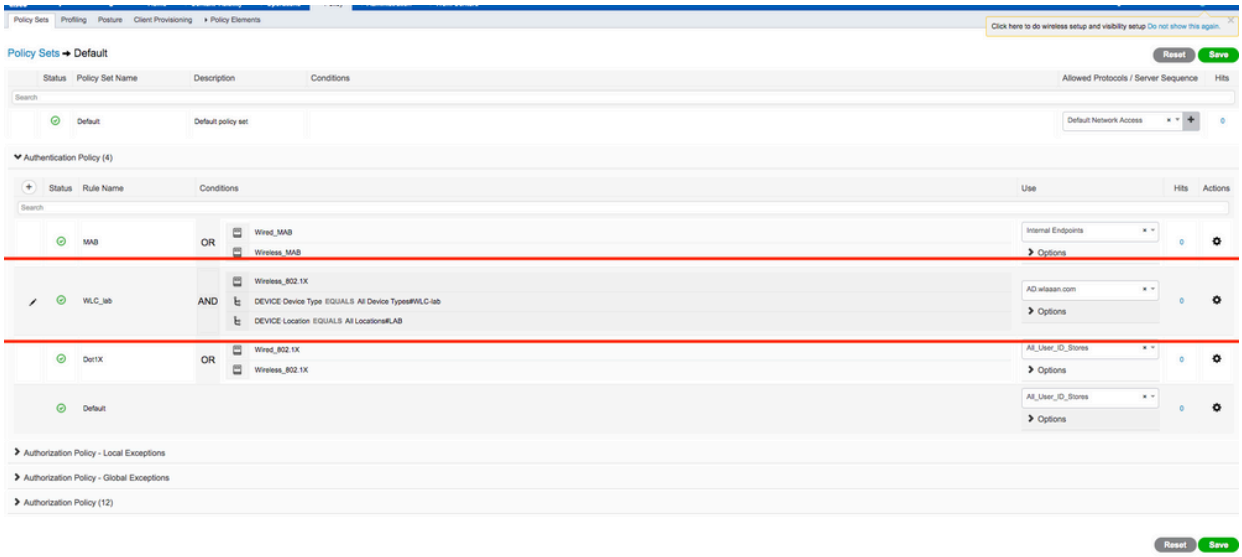
- 使用相應組的VLAN資訊完成授權配置檔案配置；該示例顯示Marketing組配置設定。



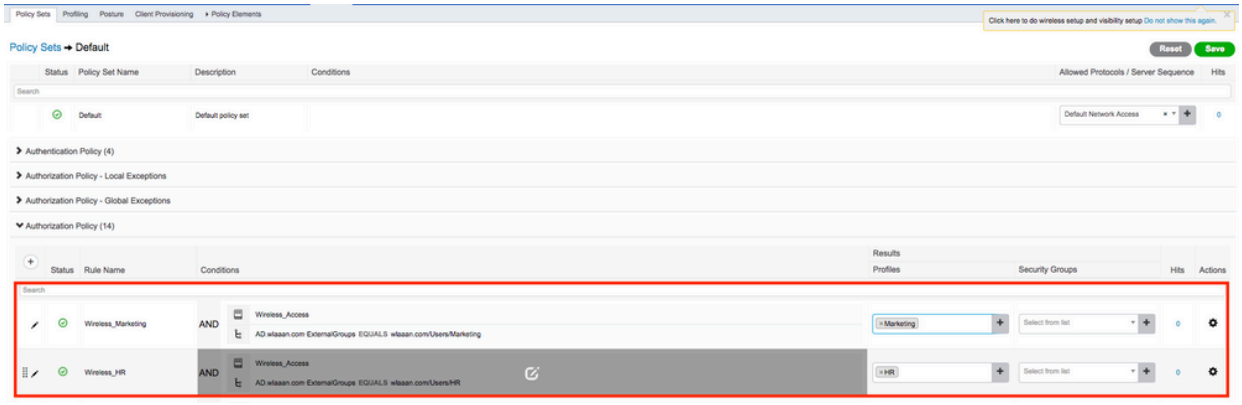
必須為其他組執行類似的配置，並且必須配置相應的VLAN標籤屬性。

- 配置授權配置檔案後，您可以為無線使用者定義身份驗證策略。這可以透過配置Custom或

修改Default Policy set來完成。在本示例中，預設策略集被修改。導航到Policy > Policy Sets > Default。預設情況下，對於dot1x身份驗證型別，ISE將使用All_User_ID_Stores，儘管它可以在當前預設設定下使用，因為AD是All_User_ID_Stores的身份源清單的一部分，此示例針對相應的LAB控制器使用更具體的規則WLC_lab，並使用AD作為唯一的身份驗證源。

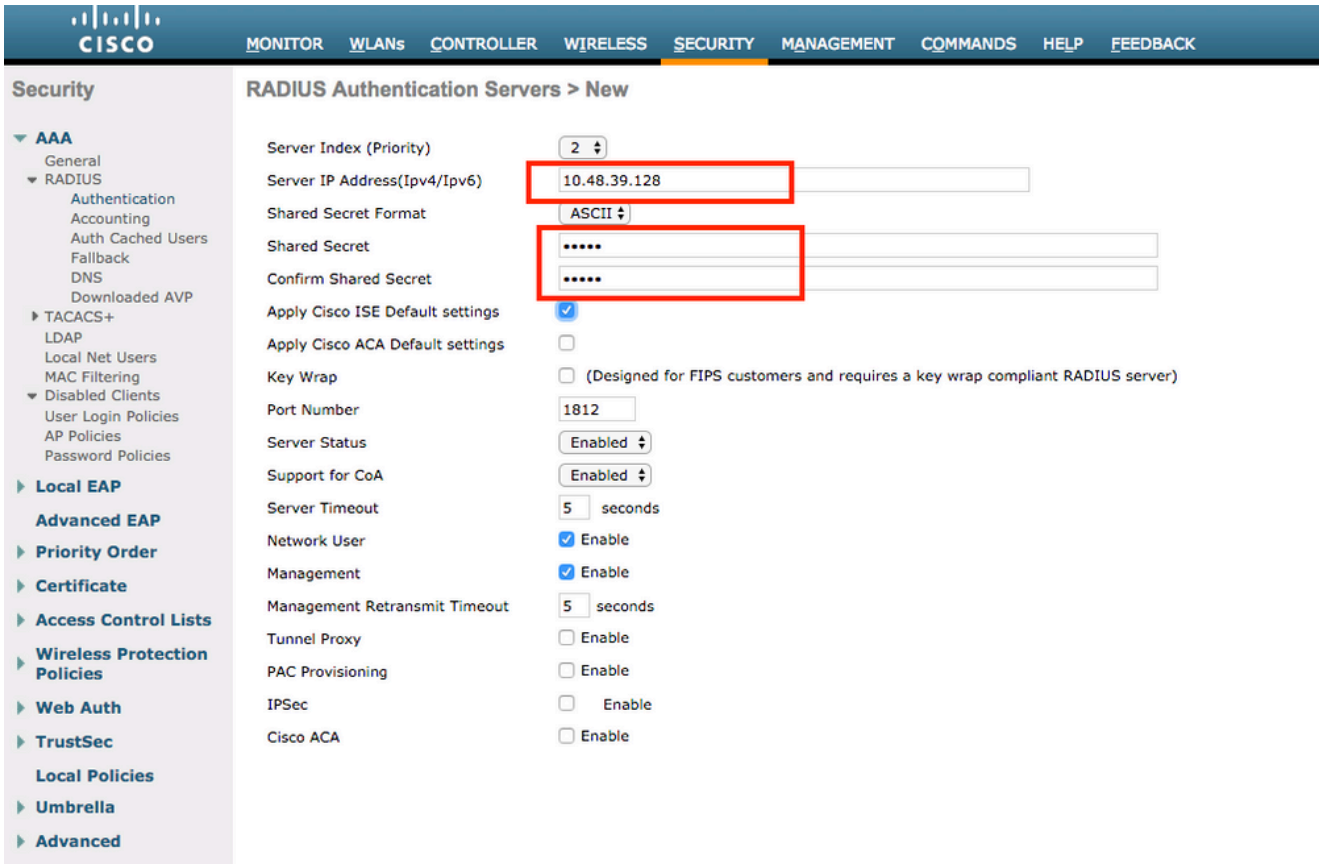


- 現在，您必須為根據組成員身份分配相應授權配置檔案的使用者建立授權策略。導航到Authorization policy部分並建立策略以滿足此要求。

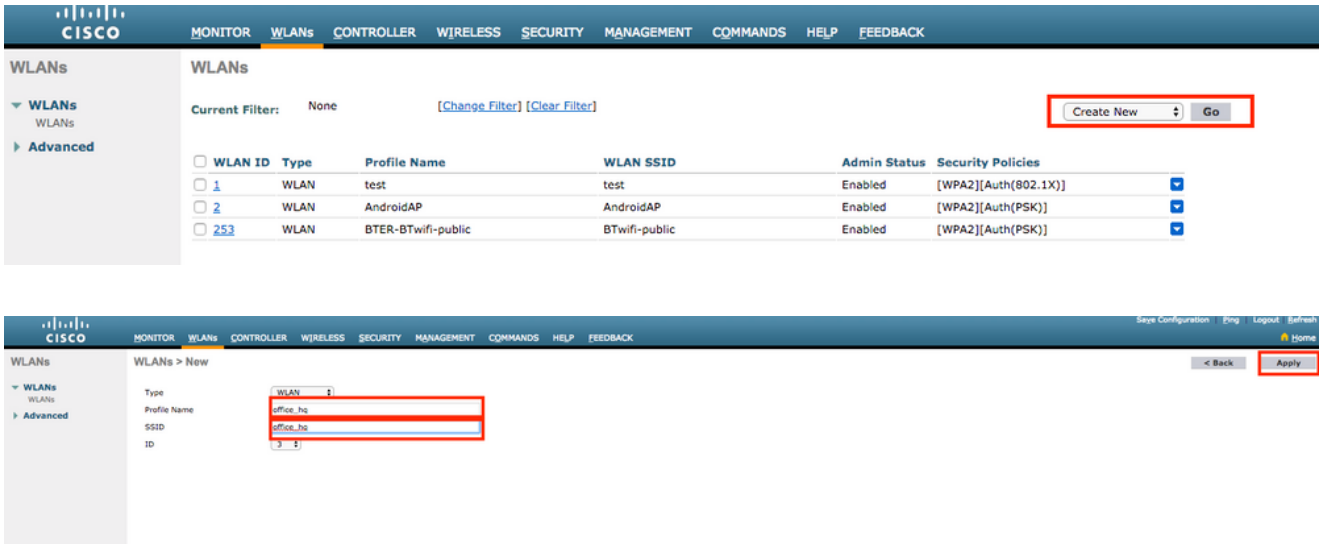


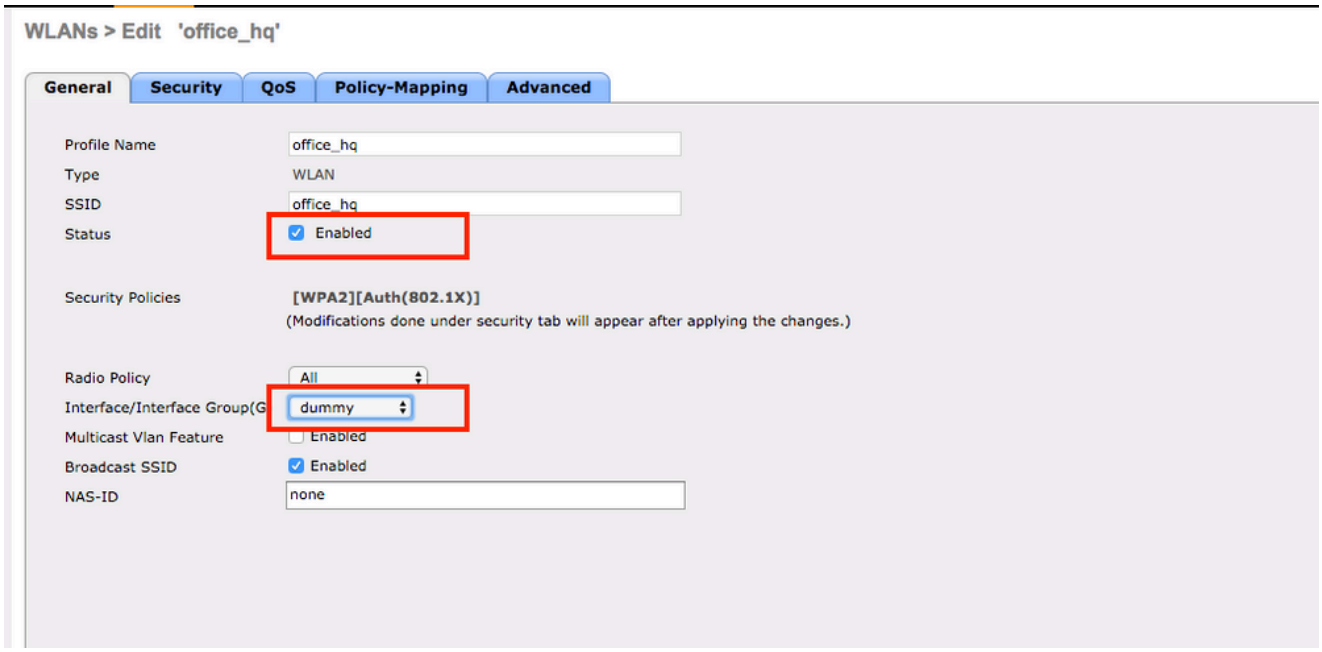
支援SSID 'office_hq'的dot1x身份驗證和AAA覆蓋的WLC配置

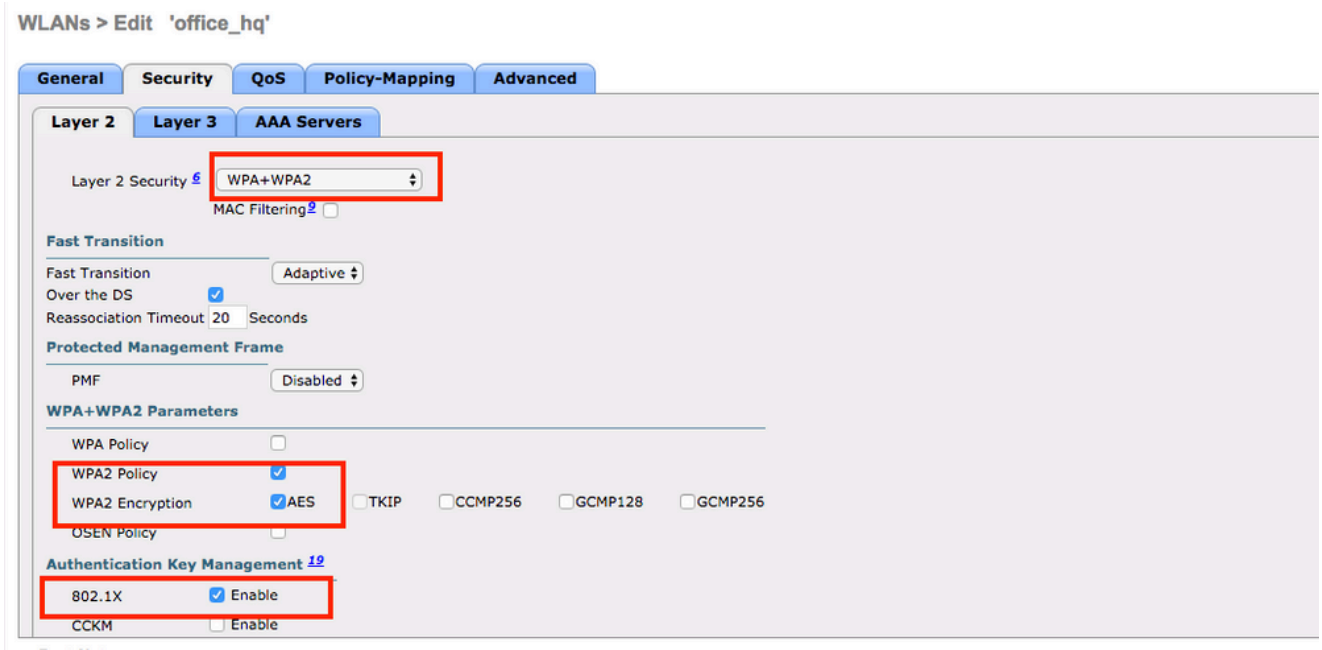
1. 將ISE配置為WLC上的RADIUS身份驗證伺服器。導航到Web UI介面中的Security > AAA > RADIUS > Authentication部分，提供ISE IP地址和共用金鑰資訊。

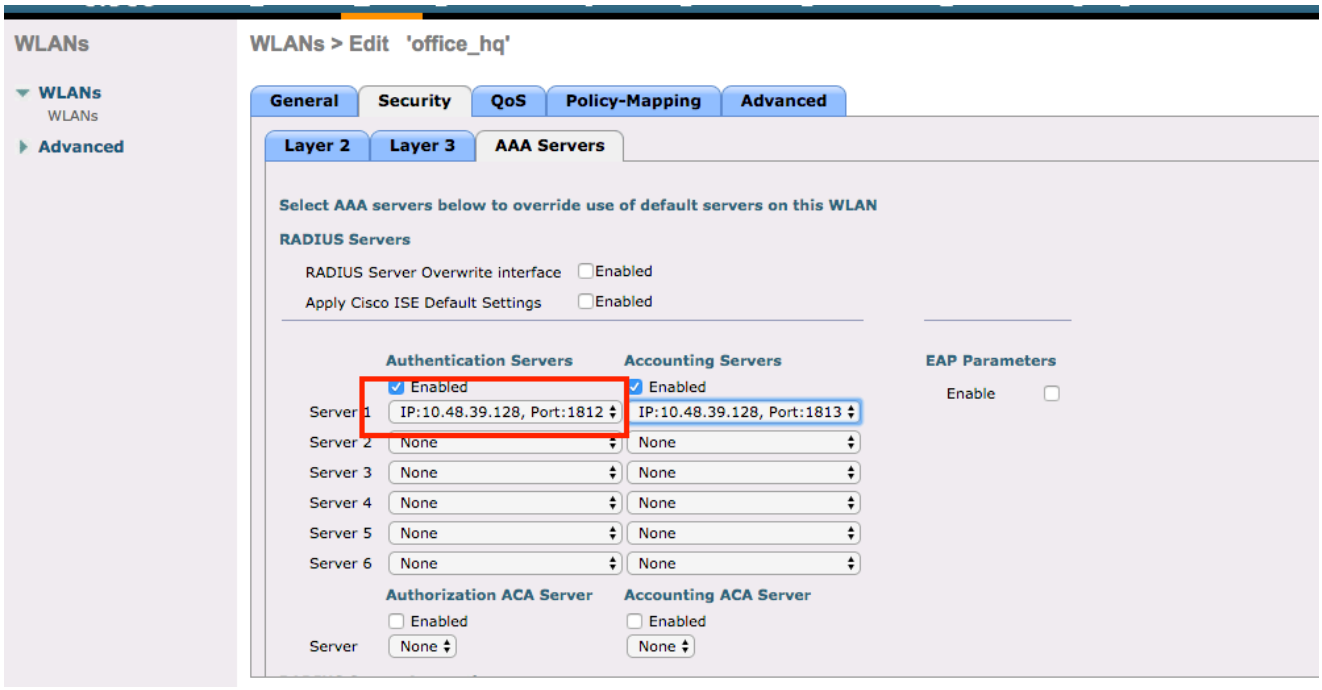


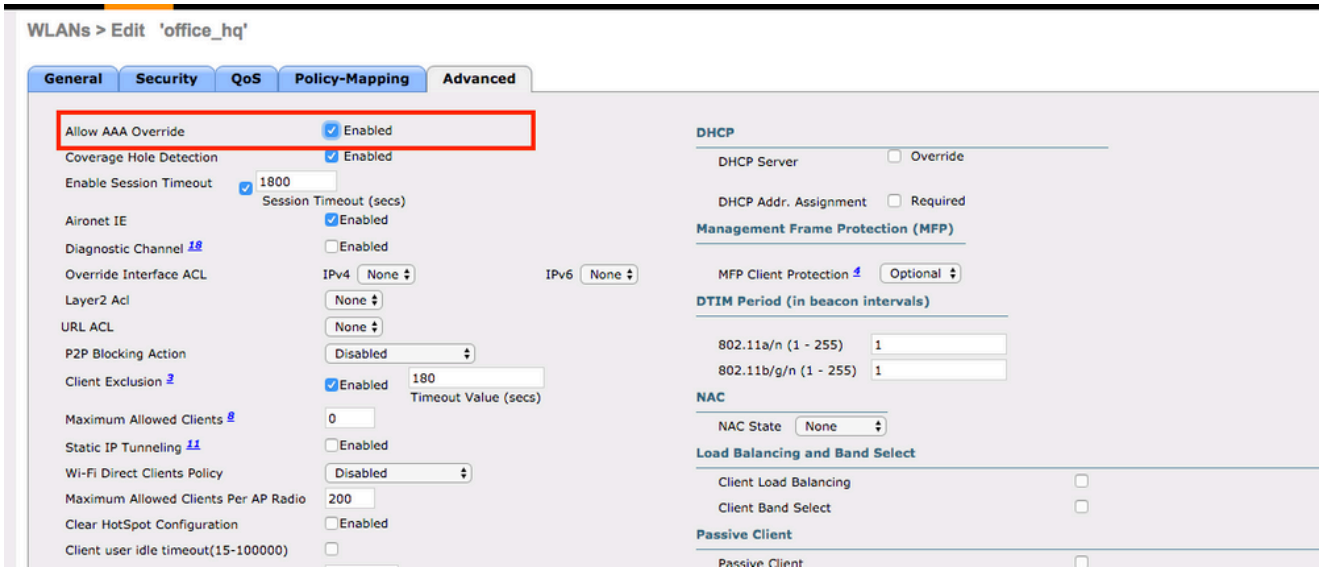
2. 在WLC上的WLANs部分下配置SSIDoffice_hq；本示例使用WPA2/AES+dot1x和AAA override配置SSID。已為WLAN選擇InterfaceDummy，因為還是透過RADIUS分配了正確的VLAN。必須在WLC上建立此虛擬介面並給予IP地址，但IP地址不必有效，並且不能在上行鏈路交換機中建立放置該虛擬介面的VLAN，因此，如果未分配VLAN，則客戶端無法前往任何地方。



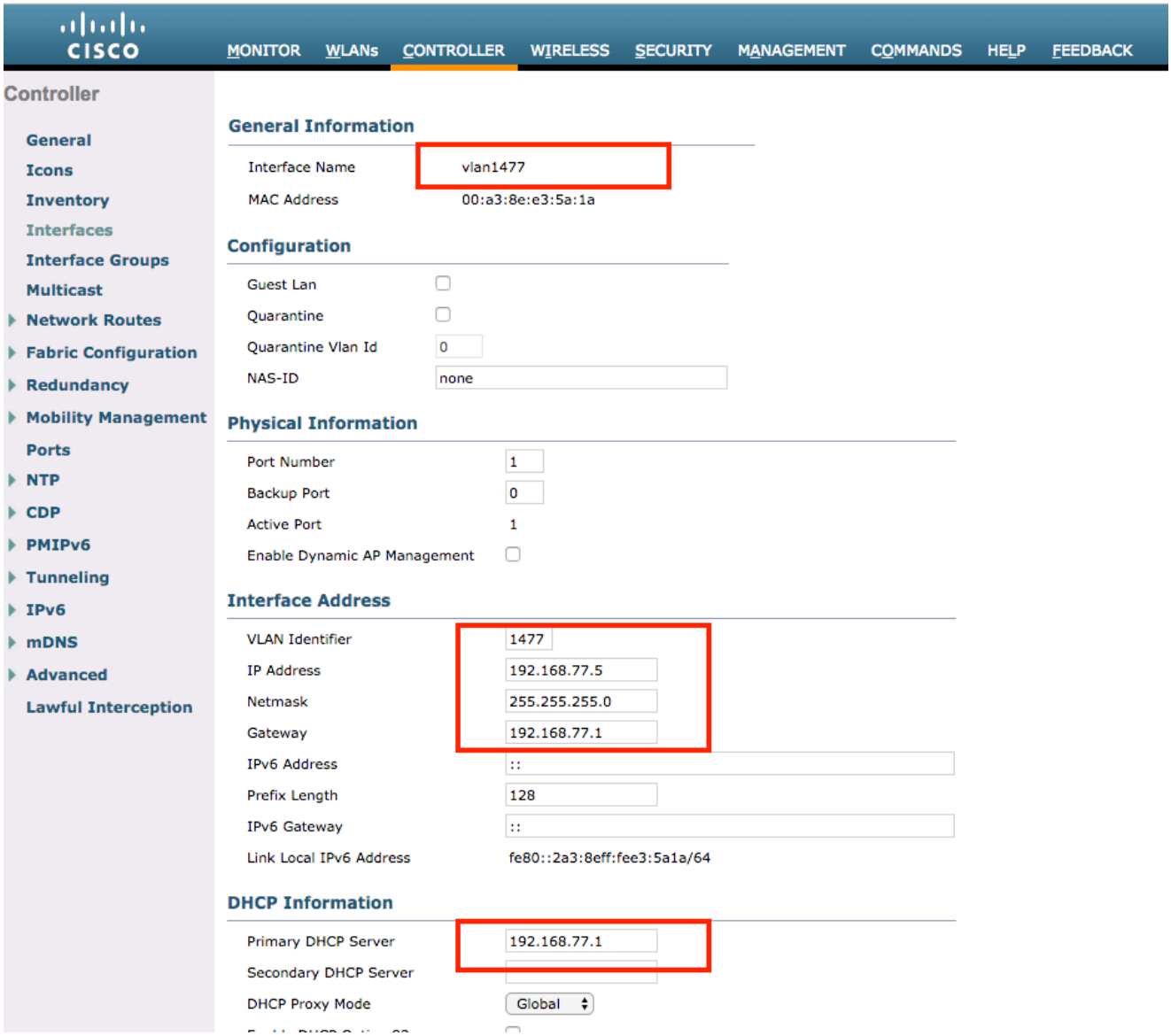

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. 您還必須在WLC上為使用者VLAN建立動態介面。導航到Controller > InterfacesUI選單。如果WLC在該VLAN中具有動態介面，則它只能支援透過AAA接收的VLAN分配。



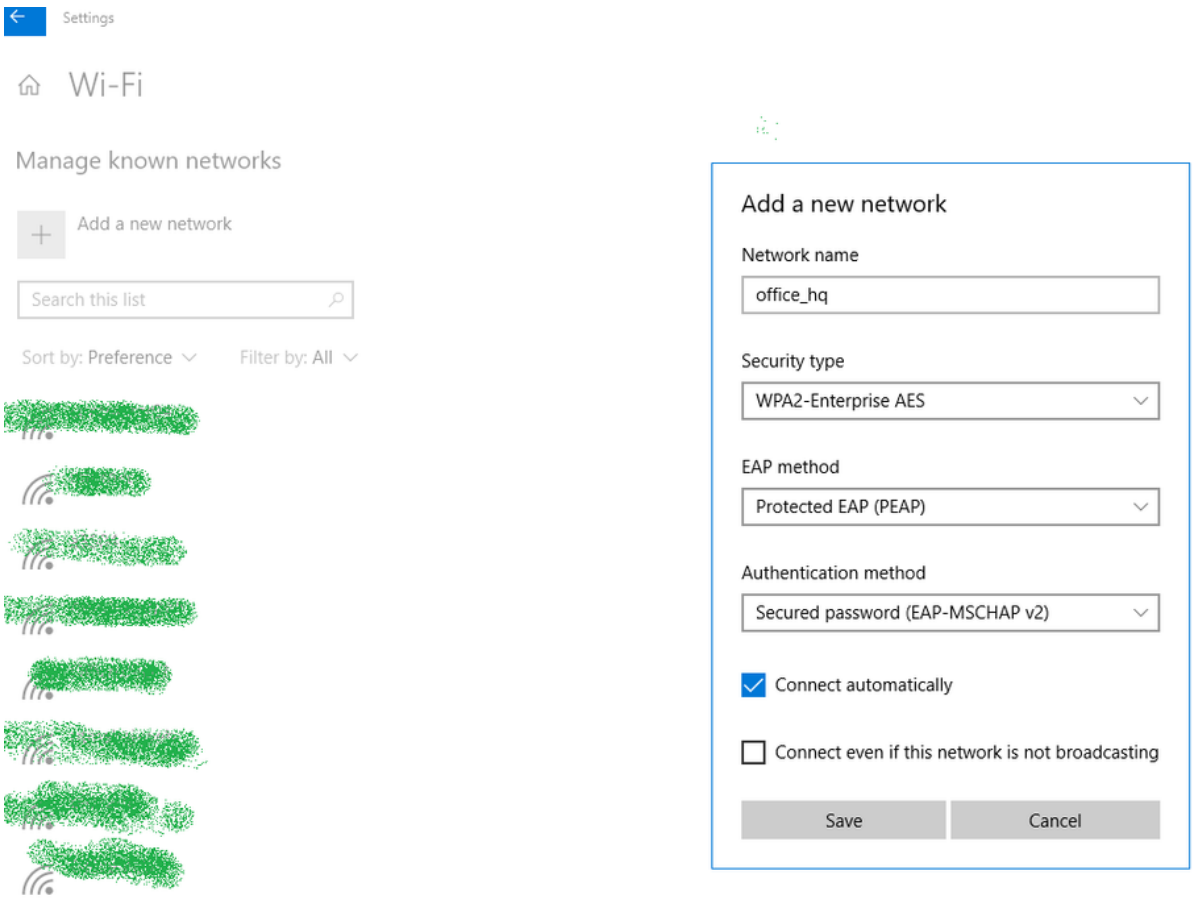
驗證

使用Windows 10本機請求方和Anyconnect NAM來測試連線。

由於您使用EAP-PEAP身份驗證且ISE使用自簽名證書(SSC)，您必須同意證書警告或停用證書驗證。在企業環境中，您必須在ISE上使用簽名和受信任的證書，並確保終端使用者裝置在受信任CA清單下安裝了適當的根證書。

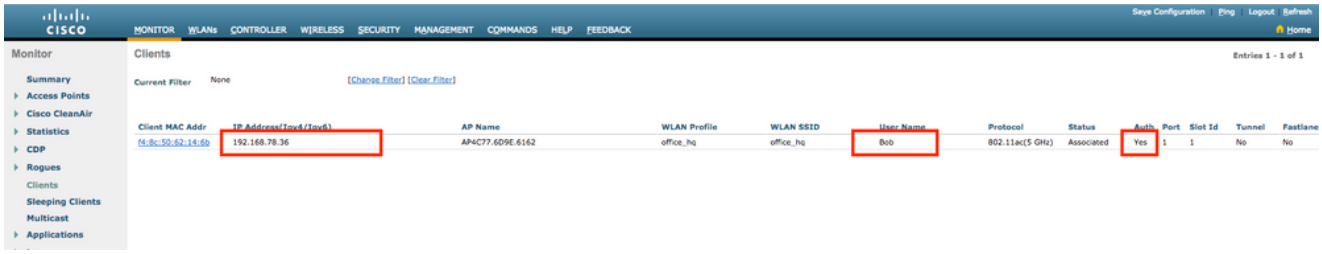
測試與Windows 10和本地請求方的連線：

1. 按Network & Internet settings > Wi-Fi > Manage known networksAdd new network按鈕打開並建立新網路配置檔案；填寫所需資訊。



2. 檢查ISE上的身份驗證日誌並確保為使用者選擇了正確的配置檔案。

3. 檢查WLC上的客戶端條目，確保已將其分配給正確的VLAN並處於RUN狀態。



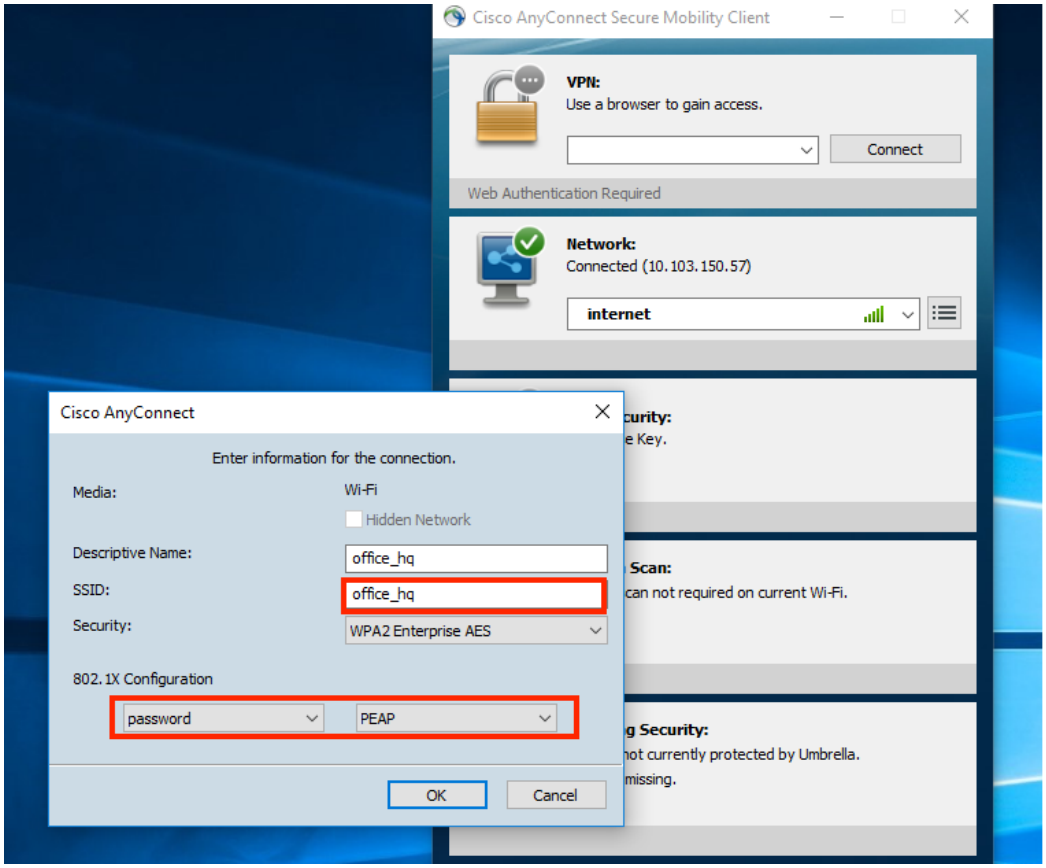
4. 從WLC CLI中，可以使用show client dertails
檢查客戶端狀態：

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
```

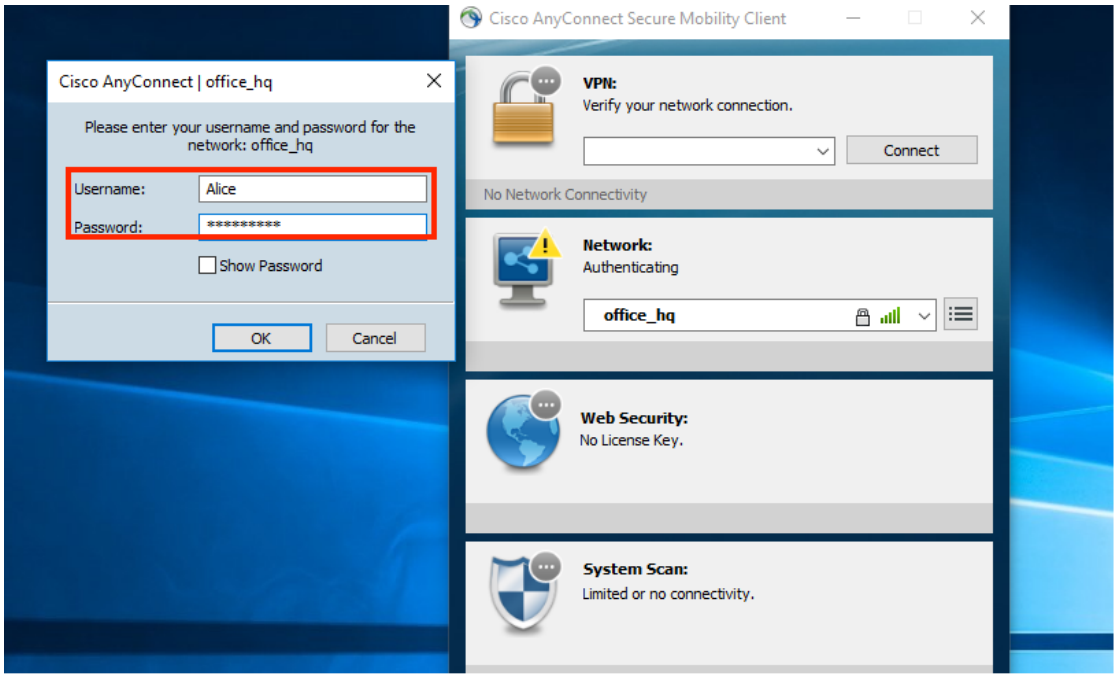
```
AP MAC Address..................................... 70:69:5a:51:4e:c0
AP Name............................................ AP4C77.6D9E.6162
AP radio slot Id................................... 1
Client State....................................... Associated
User Authenticated by ............................. RADIUS Server
Client User Group.................................. Bob
Client NAC OOB State............................... Access
Wireless LAN Id.................................... 3
Wireless LAN Network Name (SSID)................... office_hq
Wireless LAN Profile Name.......................... office_hq
Hotspot (802.11u).................................. Not Supported
Connected For ..................................... 242 secs
BSSID.............................................. 70:69:5a:51:4e:cd
Channel............................................ 36
IP Address......................................... 192.168.78.36
Gateway Address.................................... 192.168.78.1
Netmask............................................ 255.255.255.0
...
Policy Manager State............................... RUN
...
EAP Type........................................... PEAP
Interface.......................................... vlan1478
VLAN............................................... 1478
Quarantine VLAN.................................... 0
Access VLAN........................................ 1478
```

測試與Windows 10和Anyconnect NAM的連線：

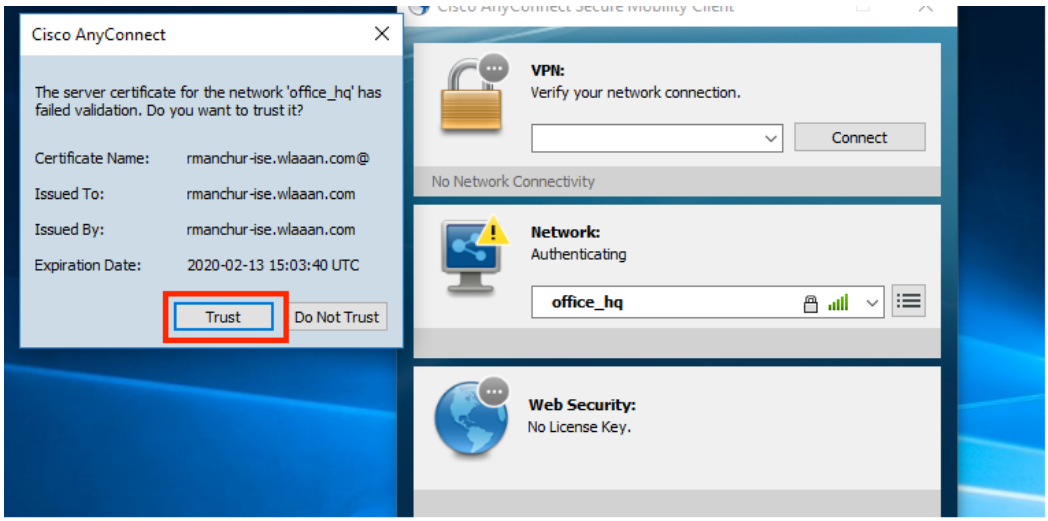
1. 從可用的SSID清單和相應的EAP驗證型別（在本例中為PEAP）以及內部驗證表單中選擇SSID。



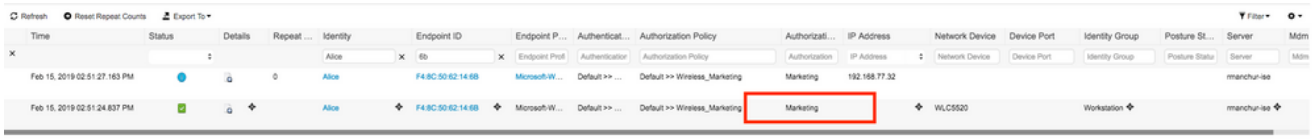
2. 提供使用者驗證的使用者名稱和密碼。



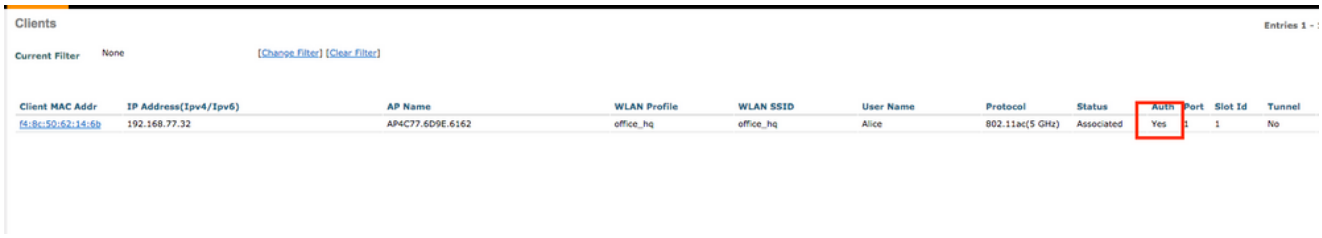
3. 由於ISE向客戶端傳送SSC，您必須手動選擇信任證書（在生產環境中，強烈建議在ISE上安裝受信任的證書）。



4. 檢查ISE上的身份驗證日誌並確保為使用者選擇了正確的授權配置檔案。



5. 檢查WLC上的客戶端條目，確保已將其分配給正確的VLAN並處於RUN狀態。



6. 從WLC CLI中，可以使用show client dertails
檢查客戶端狀態：

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
Client State.................................... Associated
User Authenticated by .......................... RADIUS Server
Client User Group............................... Alice
Client NAC OOB State............................ Access
Wireless LAN Id................................. 3
Wireless LAN Network Name (SSID)................ office_hq
Wireless LAN Profile Name....................... office_hq
Hotspot (802.11u)............................... Not Supported
Connected For .................................. 765 secs
BSSID........................................... 70:69:5a:51:4e:cd
Channel......................................... 36
IP Address...................................... 192.168.77.32
Gateway Address................................. 192.168.77.1
Netmask......................................... 255.255.255.0
...
Policy Manager State............................ RUN
...
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
Encryption Cipher............................... CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type........................................ PEAP
Interface....................................... vlan1477
VLAN............................................ 1477
```

疑難排解

1. 使用test aaa radius username

password

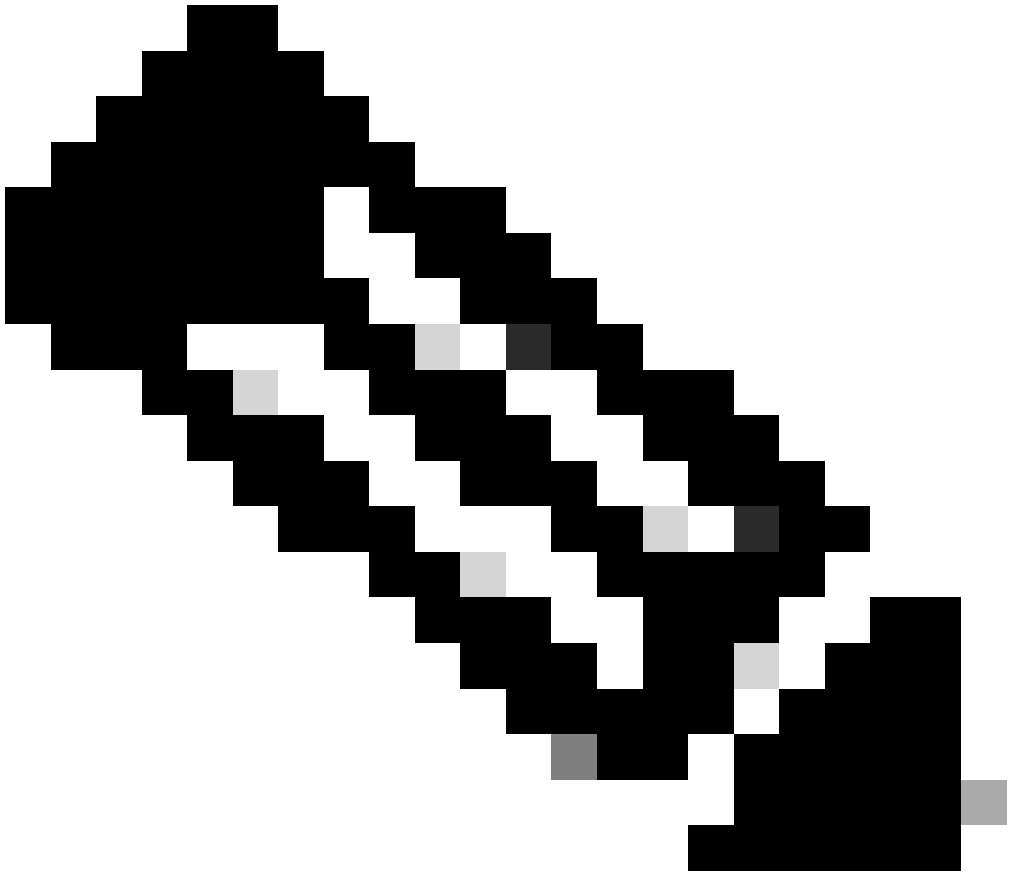
wlan-id

來測試WLC和ISE之間的RADIUS連線，使用test aaa show radius來顯示結果。

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  Called-Station-Id               00-00-00-00-00-00:AndroidAP
  Calling-Station-Id              00-11-22-33-44-55
  Nas-Port                        0x00000001 (1)
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
```

```
Tunnel-Type                    0x0000000d (13)
Tunnel-Medium-Type             0x00000006 (6)
Tunnel-Group-Id                0x000005c5 (1477)


(Cisco Controller) >
```

2. 使用debug client
   對無線客戶端連線問題進行故障排除。
3. 使用debug aaa all enable對WLC上的身份驗證和授權問題進行故障排除。



注意：請僅對debug mac addr使用此命令，以便根據進行調試的MAC地址限制輸出。

---

4. 請參閱ISE即時日誌和會話日誌，以確定問題身份驗證失敗和AD通訊問題。

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）。