為動態VLAN分配配置RADIUS伺服器和WLC

目錄

簡介

本文件介紹動態 VLAN 指派的概念。本文說明如何設定無線LAN控制器(WLC)和RADIUS伺服器，以動態地將無線LAN(WLAN)使用者端指派到特定VLAN中。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 具有WLC和輕量型存取點(LAP)的基本知識
- 瞭解AAA伺服器的功能
- 全面瞭解無線網路和無線安全問題
- 具備輕量AP協定(LWAPP)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 4400 WLC（執行韌體版本5.2）
- Cisco 1130系列LAP
- 執行韌體版本4.4的Cisco 802.11a/b/g無線使用者端配接器
- 運行4.4版的Cisco Aironet案頭實用程式(ADU)
- 執行4.1版的CiscoSecure存取控制伺服器(ACS)
- Cisco 2950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。如果您的網路正在作用，請確保您已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指派

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，但也有侷限性，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。

但是，Cisco WLAN解決方案支援身份網路。這允許網路通告單個SSID，但允許特定使用者基於使用者憑證繼承不同的QoS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（例如CiscoSecure ACS）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同一個VLAN上。

因此，當客戶端嘗試與註冊到控制器的LAP關聯時，LAP會將使用者的憑證傳遞到RADIUS伺服器以進行驗證。驗證成功後，RADIUS伺服器會將某些Internet工程工作小組(IETF)屬性傳遞給使用者。這些RADIUS屬性決定應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，因為系統總是將使用者指派給此預先確定的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）— 將其設定為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到4094（含1）。由於Tunnel-Private-Group-ID屬於字串型別(如RFC2868（與IEEE 802.1X一起使用），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Tag欄位。

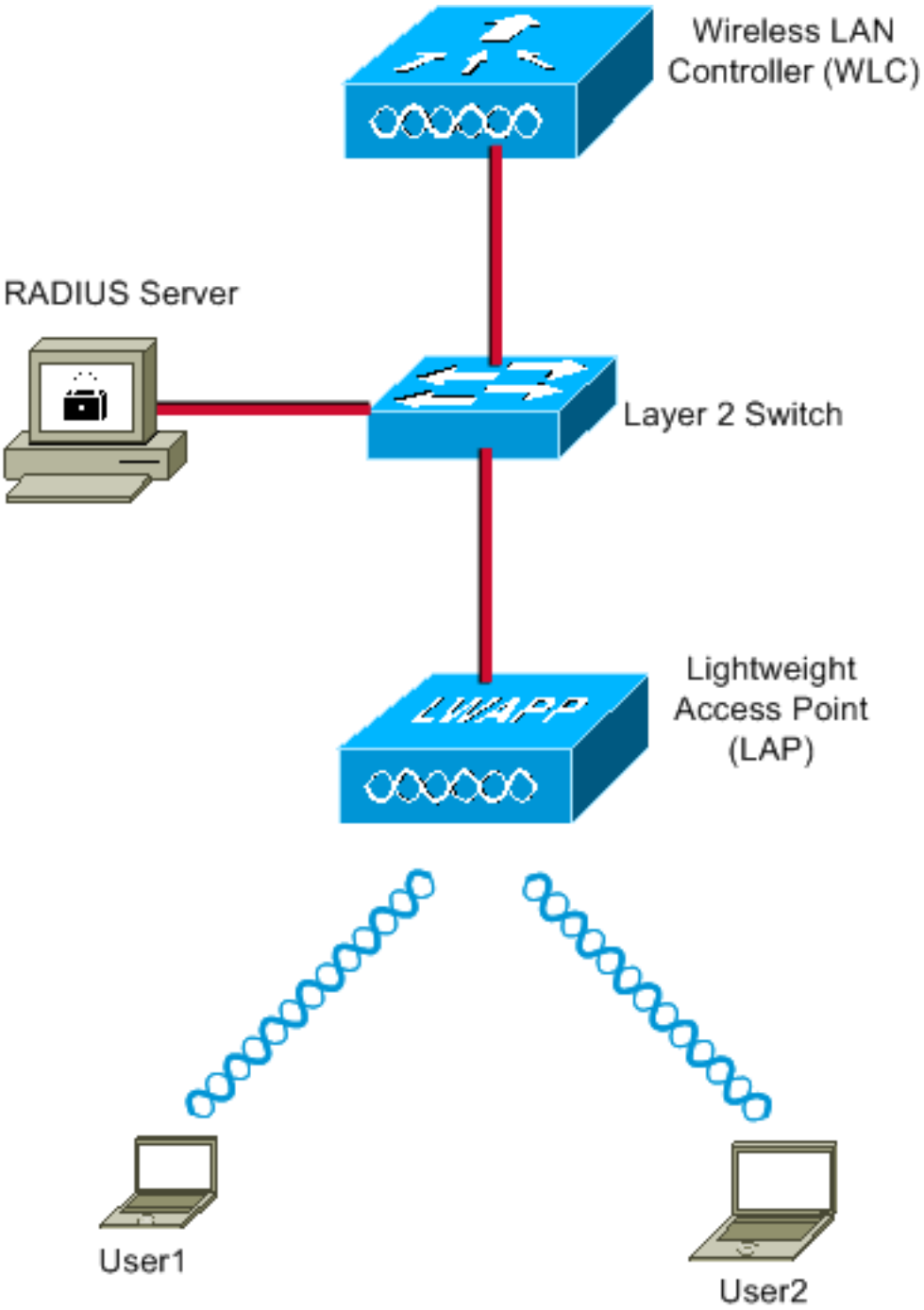
如RFC2868 第3.1節中所述：**Tag欄位的長度為一個八位組，旨在提供一種對同一資料包中引用同一隧道的屬性進行分組的方法。**此欄位的有效值為0x01到0x1F（包括0x1F）。如果「標籤」欄位未使用，則該欄位必須為零(0x00)。 如需所有RADIUS屬性的詳細資訊，請參閱RFC 2868 。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



以下是此圖中所用元件的配置詳細資訊：

- ACS(RADIUS)伺服器的IP地址是172.16.1.1。
- WLC的管理介面地址為172.16.1.30。
- WLC的AP-Manager介面地址是172.16.1.31。
- DHCP伺服器地址172.16.1.1用於為LWAPP分配IP地址。**控制器上的內部DHCP伺服器用於將IP地址分配給無線客戶端。**
- 整個配置中都使用VLAN10和VLAN11。使用者1配置為置於VLAN10中，使用者2配置為由RADIUS伺服器置於VLAN11中。**註：此**文檔僅顯示與user1相關的所有配置資訊。請完成本文檔中針對user2說明的相同步驟。
- 本文使用搭載LEAP的802.1x作為安全機制。**注意：**思科建議您使用高級身份驗證方法（例如EAP-FAST和EAP-TLS身份驗證）來保護WLAN。本文檔僅使用LEAP來簡化操作。

組態

設定之前，本檔案會假設LAP已向WLC註冊。如需詳細資訊，請參閱無線LAN控制器和輕量型存取點基本組態範例。請參閱輕量AP(LAP)註冊到無線LAN控制器(WLC)，以瞭解有關涉及的註冊程式的資訊。

配置步驟

此配置分為三類：

1. RADIUS伺服器組態
2. 為多個VLAN配置交換機
3. WLC組態
4. 無線客戶端實用程式配置

RADIUS伺服器組態

此配置需要執行以下步驟：

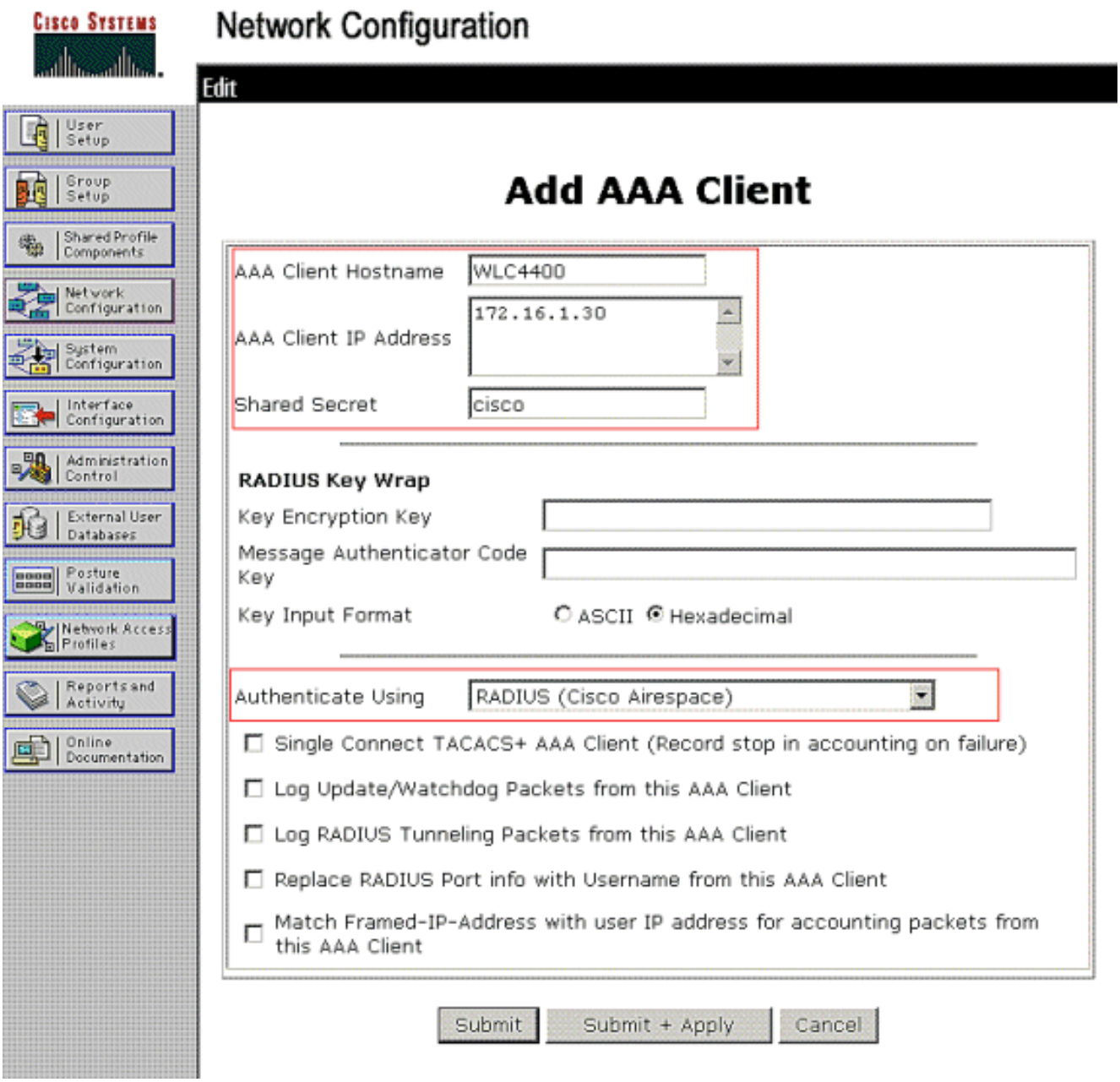
- 在RADIUS伺服器上將WLC設定為AAA使用者端
- 在RADIUS伺服器上設定用於動態VLAN分配的使用者和RADIUS(IETF)屬性

在RADIUS伺服器上設定WLC的AAA使用者端

以下程式說明如何將WLC新增為RADIUS伺服器上的AAA使用者端，以便WLC將使用者認證傳遞到RADIUS伺服器。

請完成以下步驟：

1. 在ACS GUI中，按一下**Network Configuration**。
2. 按一下AAA Clients欄位下的**Add Entry**部分。
3. 輸入AAA客戶端IP地址和金鑰。IP位址應該是WLC的管理介面IP位址。確認您輸入的金鑰與WLC上在「Security」視窗下設定的金鑰相同。這是用於AAA使用者端(WLC)和RADIUS伺服器之間通訊的金鑰。
4. 從Authenticate Using欄位為身份驗證型別選擇**RADIUS(Cisco Airespace)**。

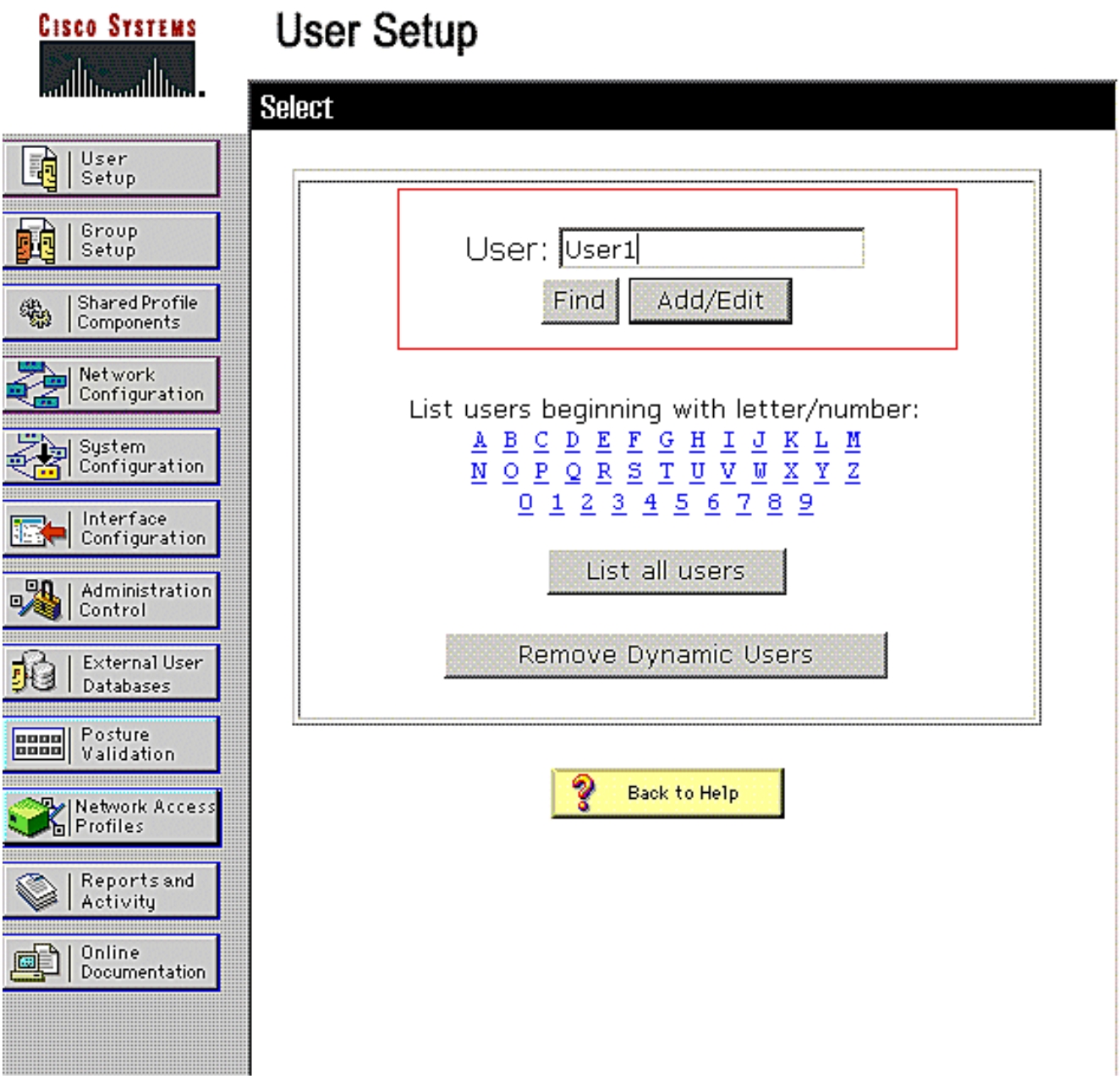


在RADIUS伺服器上設定用於動態VLAN分配的使用者和RADIUS(IETF)屬性

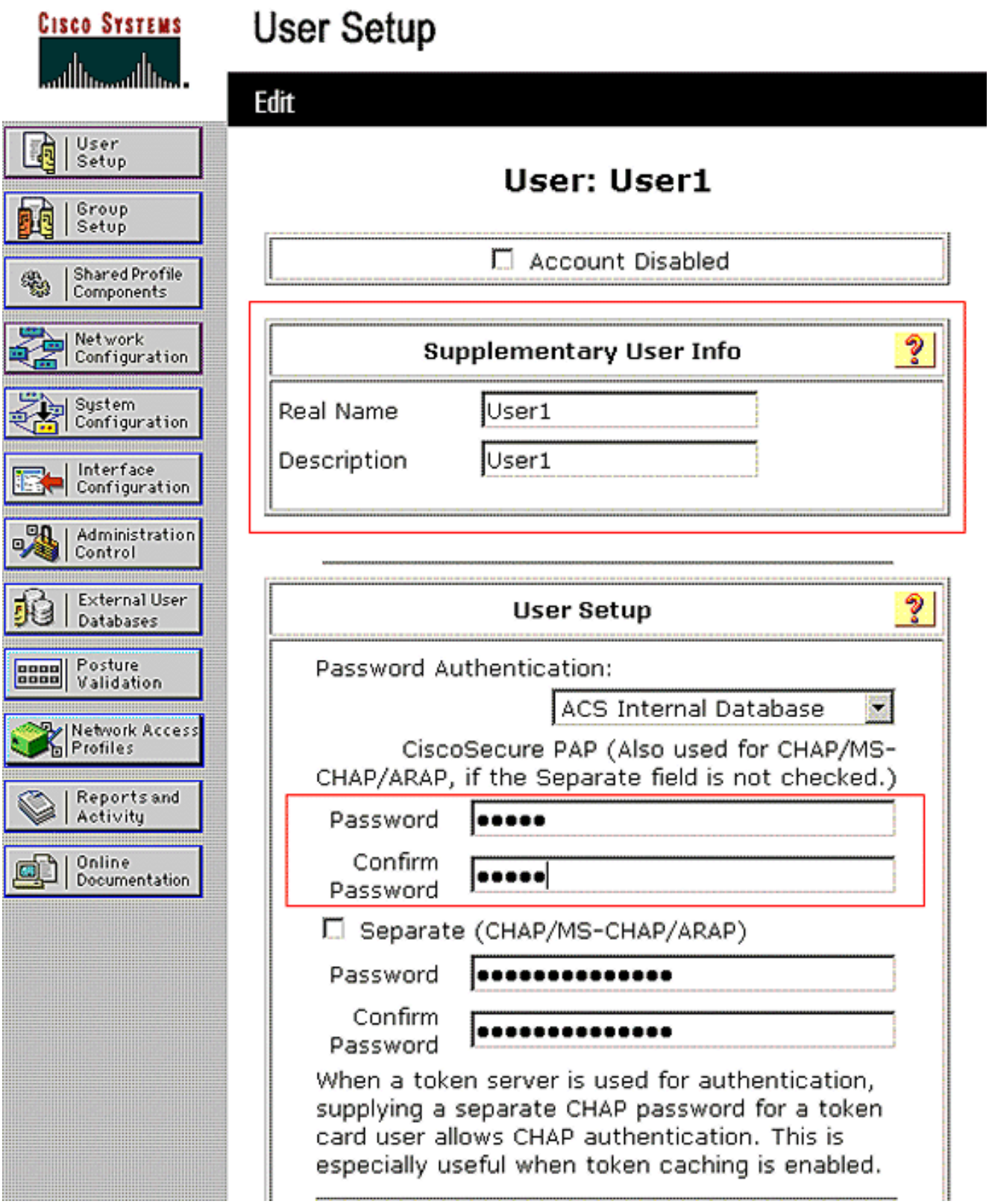
以下程式介紹如何設定RADIUS伺服器中的使用者以及用於將VLAN ID指派給這些使用者的RADIUS(IETF)屬性。

請完成以下步驟：

1. 在ACS GUI中，按一下**User Setup**。
2. 在「使用者設定」視窗的「使用者」欄位中輸入使用者名稱，然後按一下**新增/編輯**。

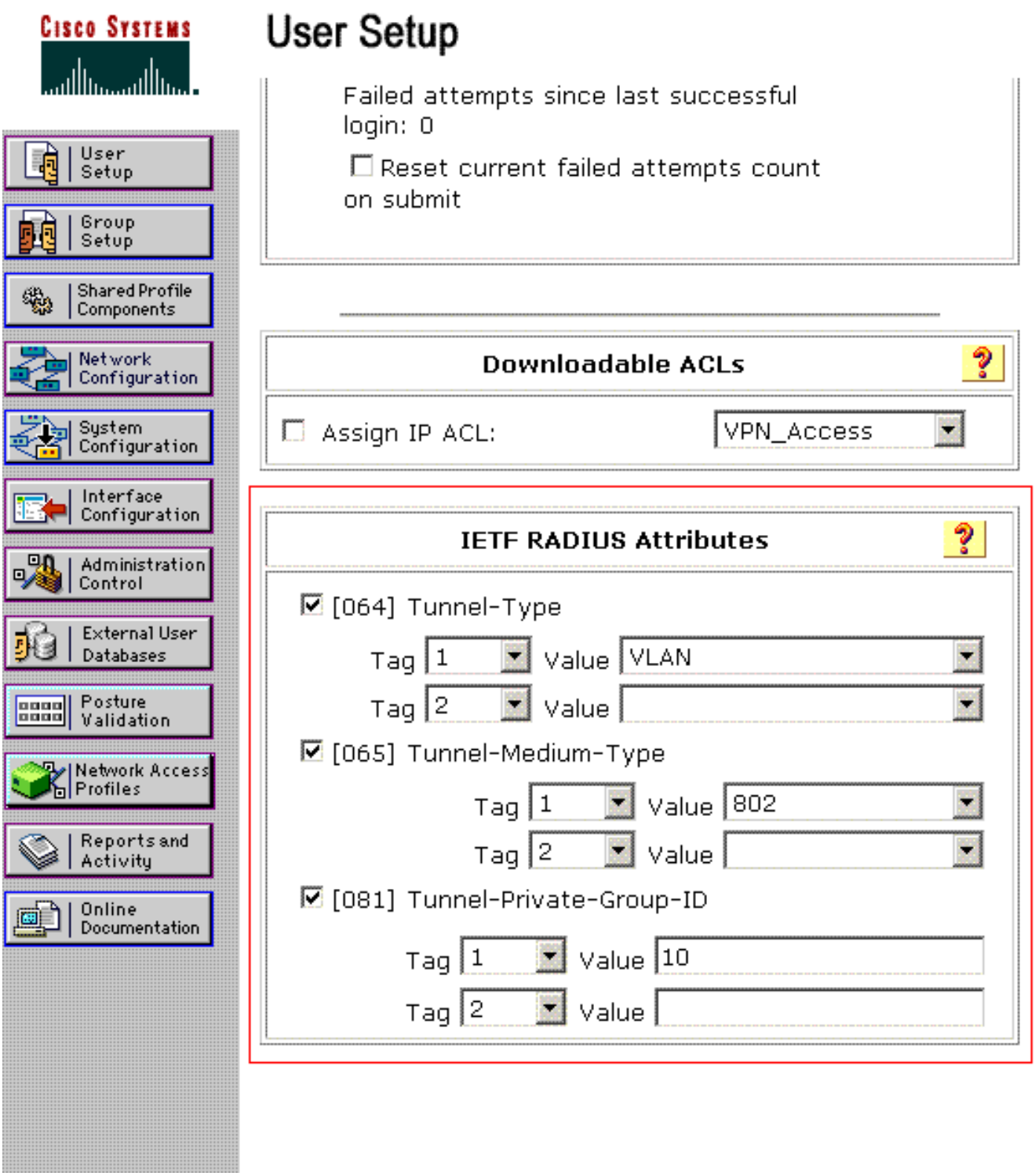


3. 在「編輯」頁上，輸入所需的使用者資訊，如下所示：

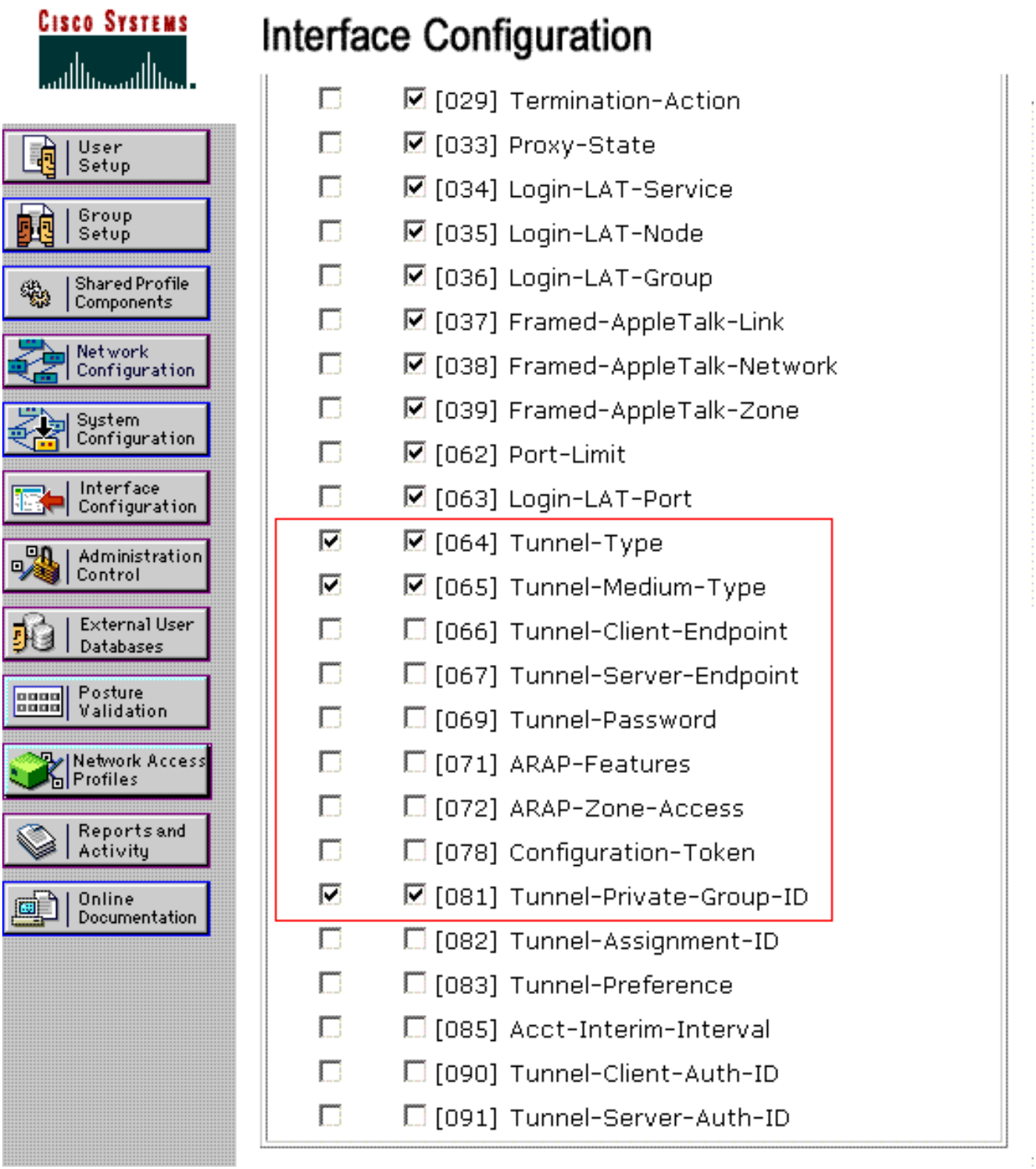


在此圖中，請注意，「使用者設定」部分下提供的密碼應與使用者身份驗證期間在客戶端提供的密碼相同。

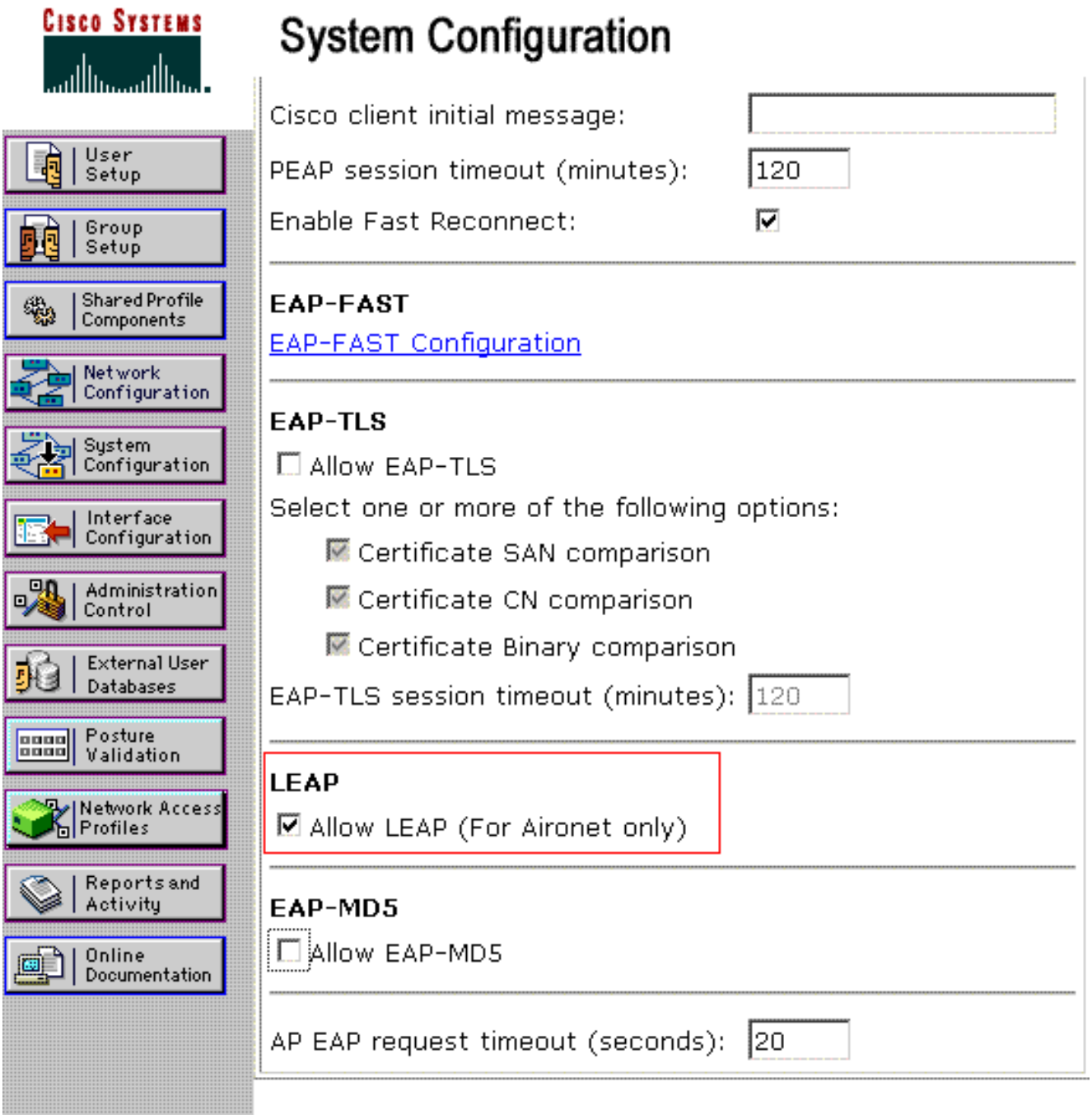
4. 向下滾動「編輯」頁並找到「**IETF RADIUS屬性**」欄位。
5. 在IETF RADIUS Attributes欄位中，選中三個隧道屬性旁邊的覈取方塊，然後配置屬性值，如下所示
：



注意：在ACS伺服器的初始配置中，可能未顯示IETF RADIUS屬性。依序選擇「**Interface Configuration > RADIUS(IETF)**」，以在使用者組態視窗中啟用IETF屬性。然後，在「使用者」和「組」**列中選中屬性64**、65和81的覈取方塊。



注意：若要使RADIUS伺服器將使用者端動態指派給特定VLAN，**WLC上必須存在RADIUS伺服器的IETF 81(Tunnel-Private-Group-ID)欄位下設定的VLAN-ID。**勾選「Interface Configuration > Advanced Options」底下的「**Per User TACACS+/RADIUS**」屬性覈取方塊，以便為每個使用者設定啟用RADIUS伺服器。此外，由於LEAP用作身份驗證協定，請確保在RADIUS伺服器的「系統配置」視窗中啟用LEAP，如下所示：



使用Cisco Airespace VSA屬性配置ACS以進行動態VLAN分配

在最新的ACS版本中，您還可以配置Cisco Airespace [VSA（供應商特定）]屬性，以根據ACS上的使用者配置為VLAN介面名稱（而不是VLAN ID）分配成功通過身份驗證的使用者。為此，請執行本節中的步驟。

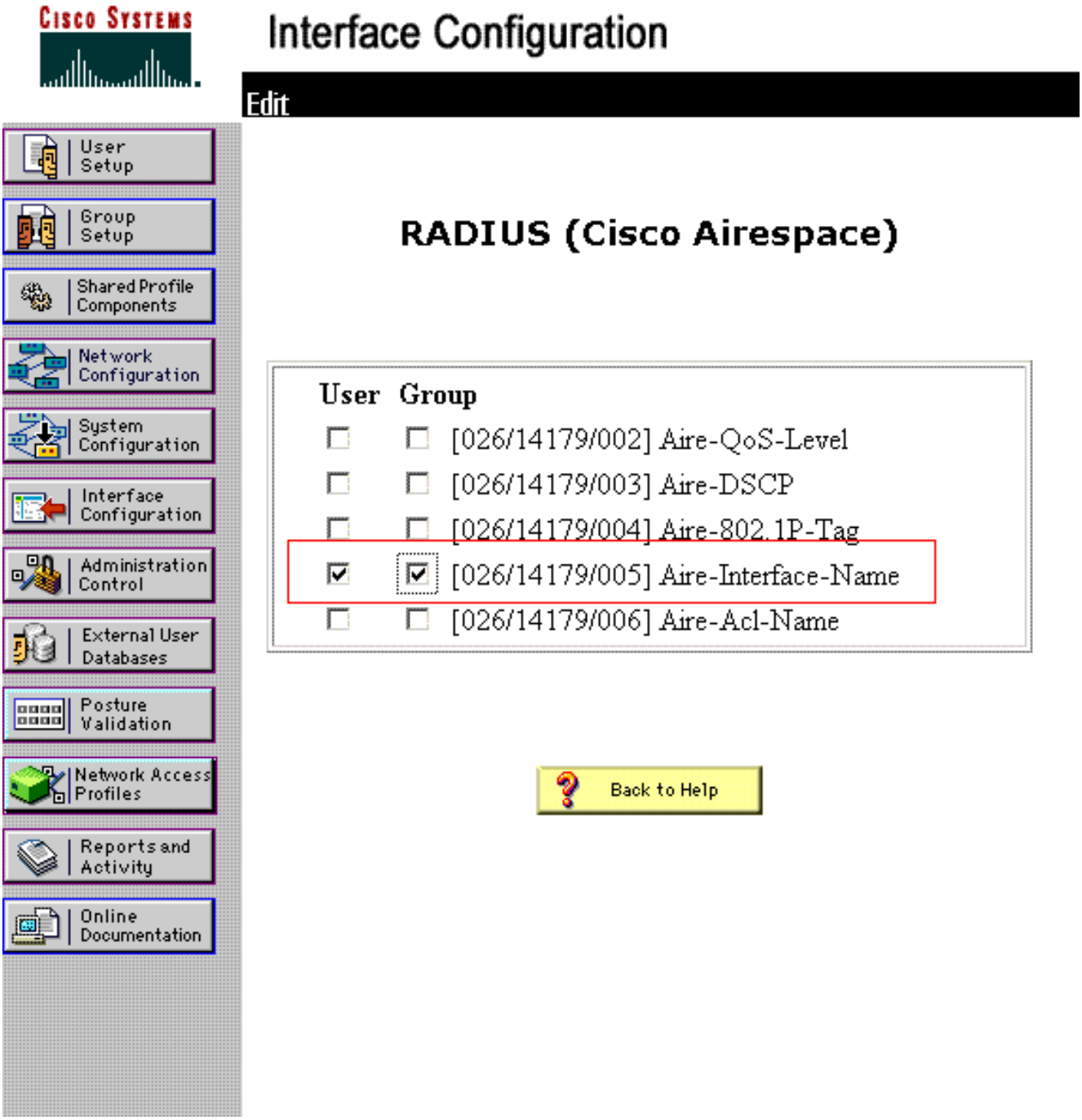
注意：本節使用ACS 4.1版本配置Cisco Airespace VSA屬性。

使用Cisco Airespace VSA屬性選項配置ACS組

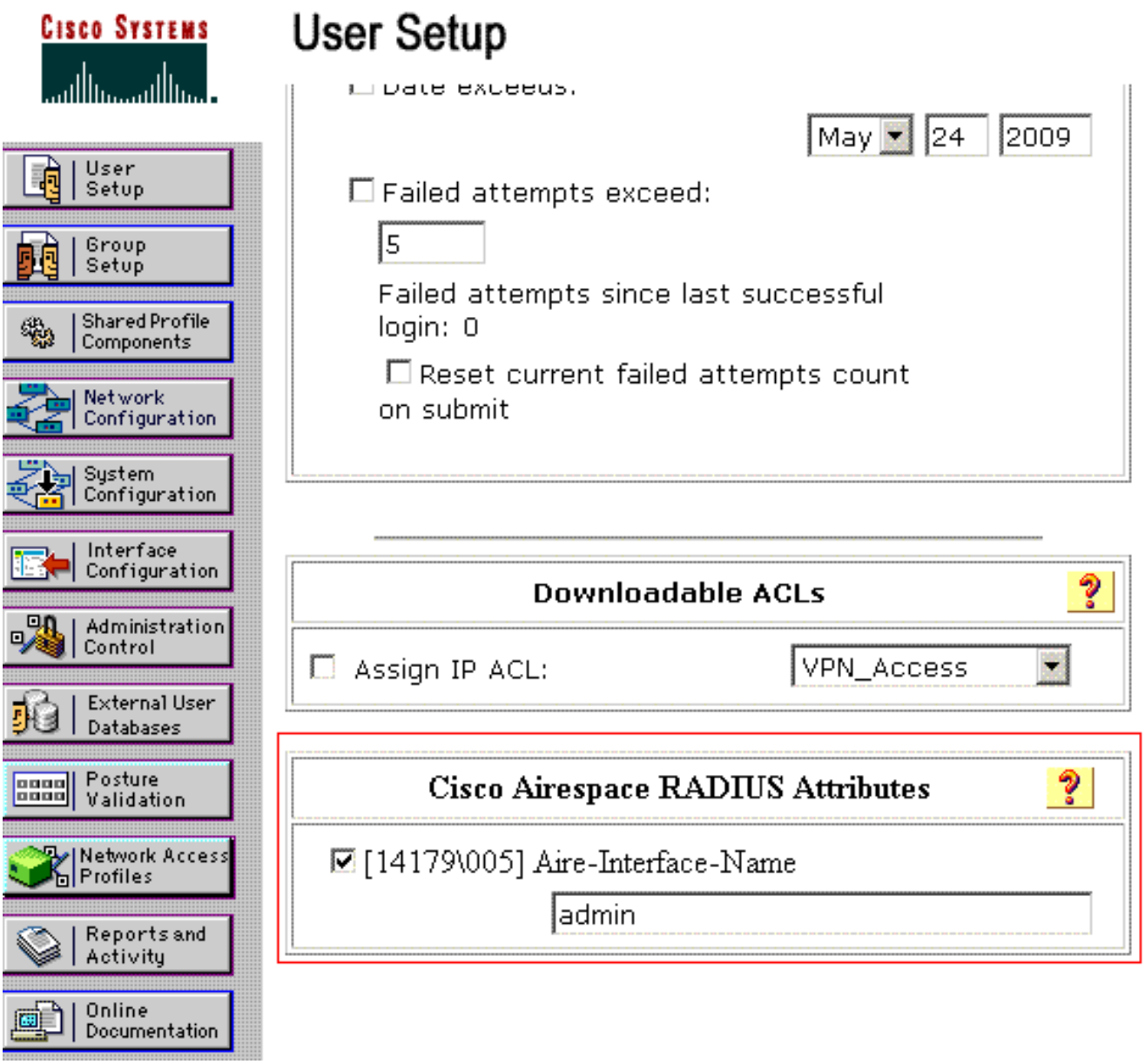
請完成以下步驟：

1. 在ACS 4.1 GUI中，按一下導航欄中的**Interface Configuration**。接下來，從Interface Configuration頁面選擇**RADIUS(Cisco Airespace)**，以設定Cisco Airespace屬性選項。
2. 在RADIUS(Cisco Airespace)視窗中，勾選**Aire-Interface-Name**旁邊的User覈取方塊（如有必

要，勾選組覈取方塊），以便在User Edit頁面上顯示它。然後，按一下**Submit**。



3. 轉到user1的Edit頁面。
4. 在User Edit頁面中，向下滾動到**Cisco Airespace RADIUS Attributes**部分。選中**Aire-Interface-Name**屬性旁邊的覈取方塊，並指定要在成功進行使用者身份驗證時分配的動態介面的名稱。此範例將使用者指派給**admin** VLAN。



5. 按一下「**Submit**」。

為多個VLAN配置交換機

若要允許多個VLAN通過交換器，需要發出以下命令，以設定連線到控制器的交換器連線埠：

1. Switch(config-if)#switchport **mode trunk**
2. Switch(config-if)#switchport **trunk encapsulation dot1q**

注意：預設情況下，大多數交換機都允許通過中繼埠在該交換機上建立所有VLAN。

這些命令對於Catalyst作業系統(CatOS)交換機有所不同。

如果有線網路連線到交換器，則此相同組態會套用到連線網路的交換器連線埠。這樣可啟用有線和無線網路中相同VLAN之間的通訊。

注意：本文檔不討論VLAN間通訊。這超出了本檔案的範圍。您必須瞭解，對於VLAN間路由，需要具有正確VLAN和中繼配置的第3層交換機或外部路由器。有幾份檔案解釋了VLAN間路由配置。

WLC組態

此配置需要執行以下步驟：

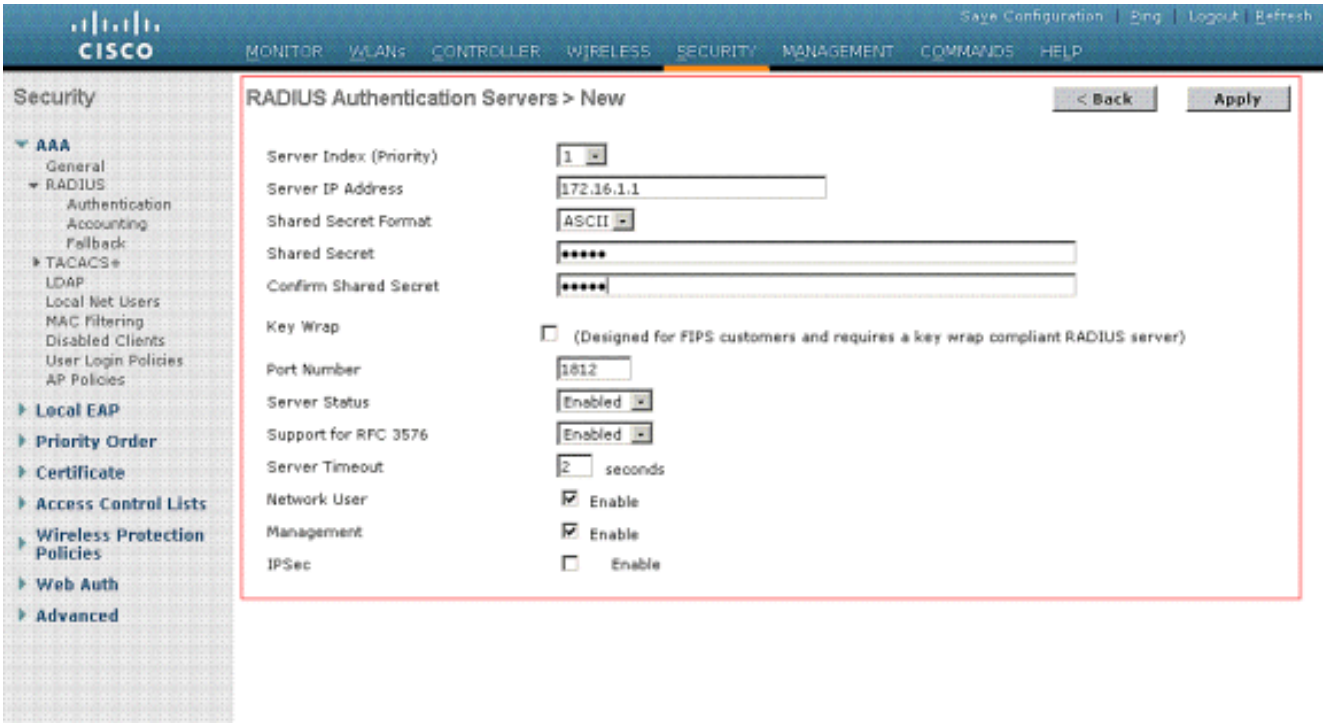
- 使用驗證伺服器的詳細資訊設定WLC
- 設定動態介面(VLAN)
- 配置WLAN(SSID)

使用驗證伺服器的詳細資訊設定WLC

必須設定WLC，才能與RADIUS伺服器通訊以驗證使用者端和任何其他交易。

請完成以下步驟：

1. 在控制器GUI上，按一下「**Security**」。
2. 輸入RADIUS伺服器的IP地址以及在RADIUS伺服器和WLC之間使用的共用金鑰。此共用金鑰應與RADIUS伺服器中Network Configuration > AAA Clients > Add Entry下配置的金鑰相同。以下是WLC的範例視窗
   ：

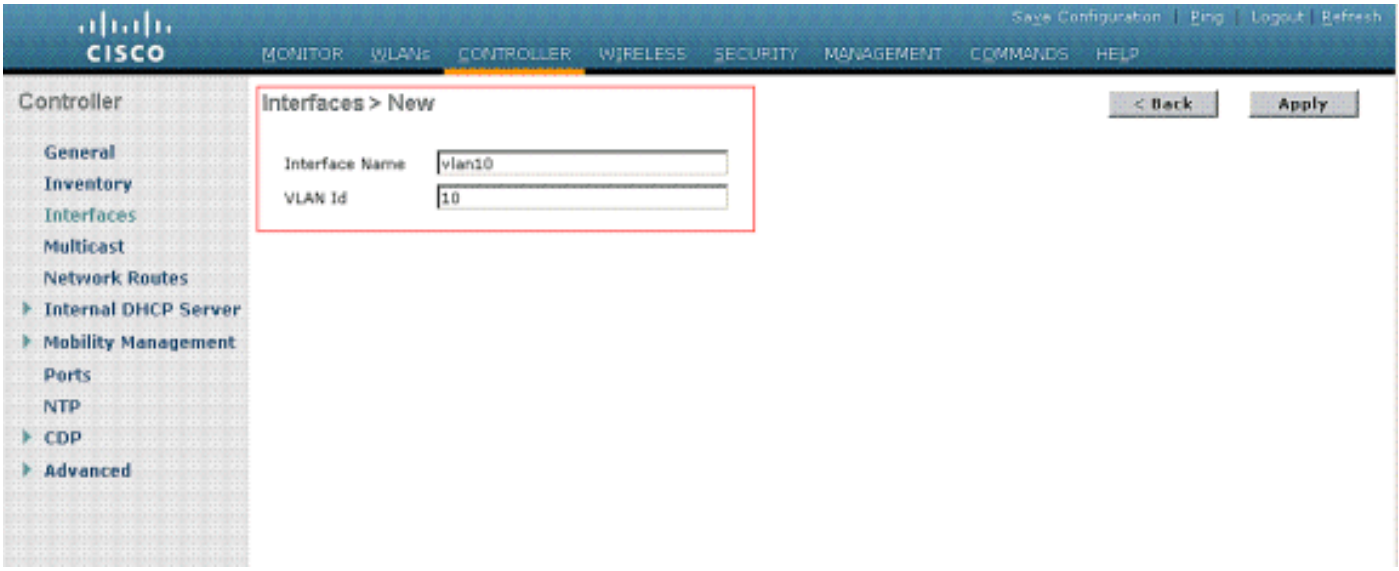


設定動態介面(VLAN)

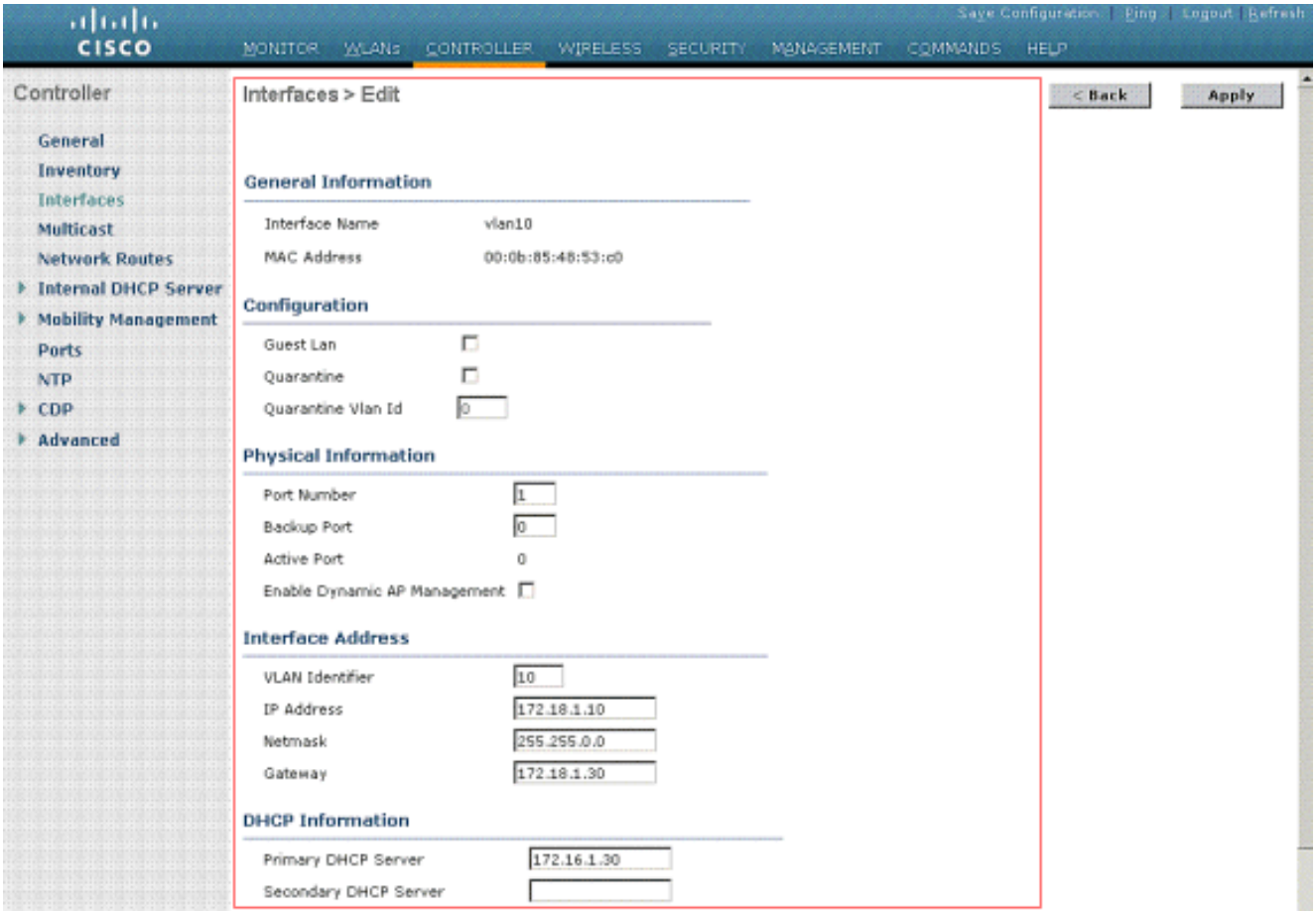
以下步驟說明如何在WLC上設定動態介面。如本檔案前面所述，WLC中還必須存在RADIUS伺服器的Tunnel-Private-Group ID屬性下指定的VLAN ID。

在本例中，在RADIUS伺服器上使用**Tunnel-Private-Group ID 10(VLAN =10)指**定使用者1。請參閱user1 User Setup視窗的IETF RADIUS Attributes部分。

在此範例中，您可以看到在WLC中設定了相同的動態介面(VLAN=10)。在控制器GUI的Controller > Interfaces視窗下，配置動態介面。



1. 在此視窗中按一下Apply。這將引導您進入此動態介面（此處為VLAN 10）的「編輯」視窗。
2. 輸入此動態介面的IP地址和預設網關。



註：由於本文檔使用控制器上的內部DHCP伺服器，因此此視窗的主要DHCP伺服器欄位指向WLC本身的管理介面。您也可以將外部DHCP伺服器、路由器或RADIUS伺服器本身用作無線客戶端的DHCP伺服器。在這種情況下，主DHCP伺服器欄位指向用作DHCP伺服器的裝置的IP地址。有關詳細資訊，請參閱DHCP伺服器文檔。

3. 按一下「Apply」。現在，您已在WLC中設定動態介面。同樣地，您可以在WLC中設定多個動態介面。但是，請記住，對於要分配給客戶端的特定VLAN，RADIUS伺服器中也必須存在相同的VLAN ID。

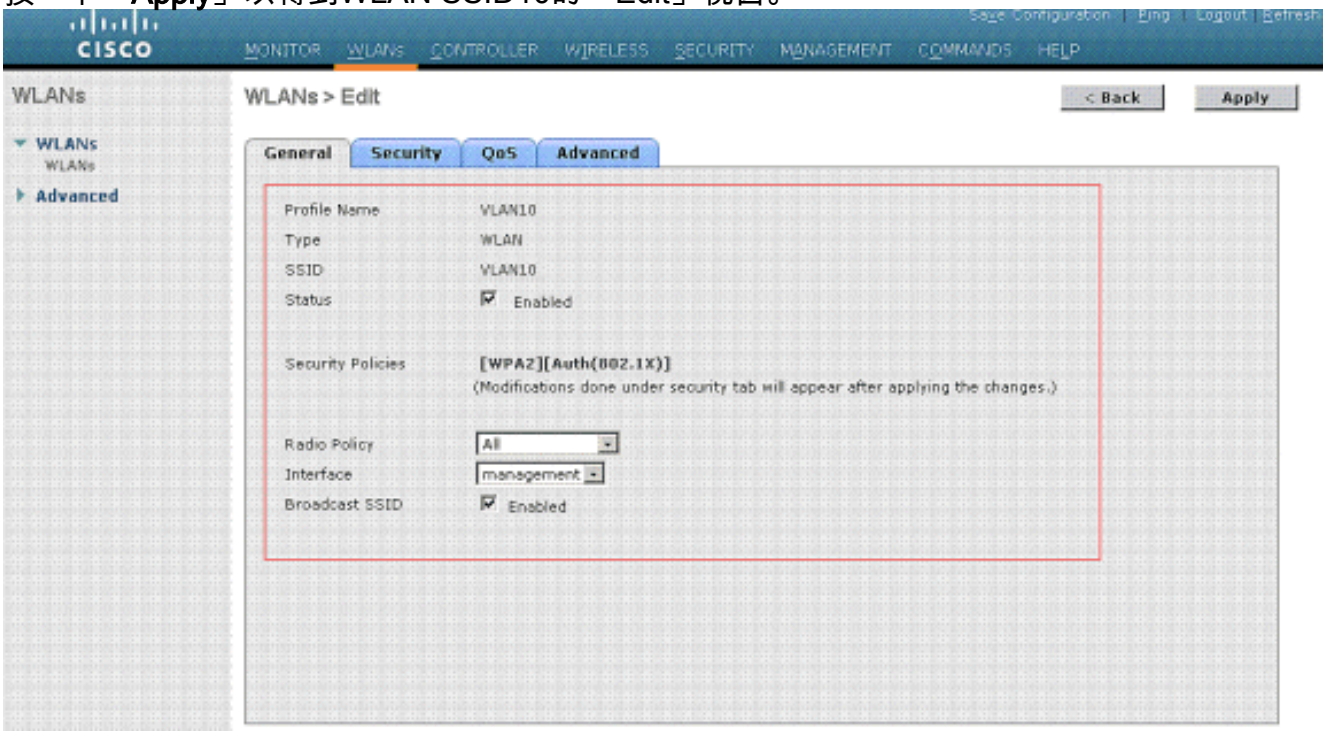
配置WLAN(SSID)

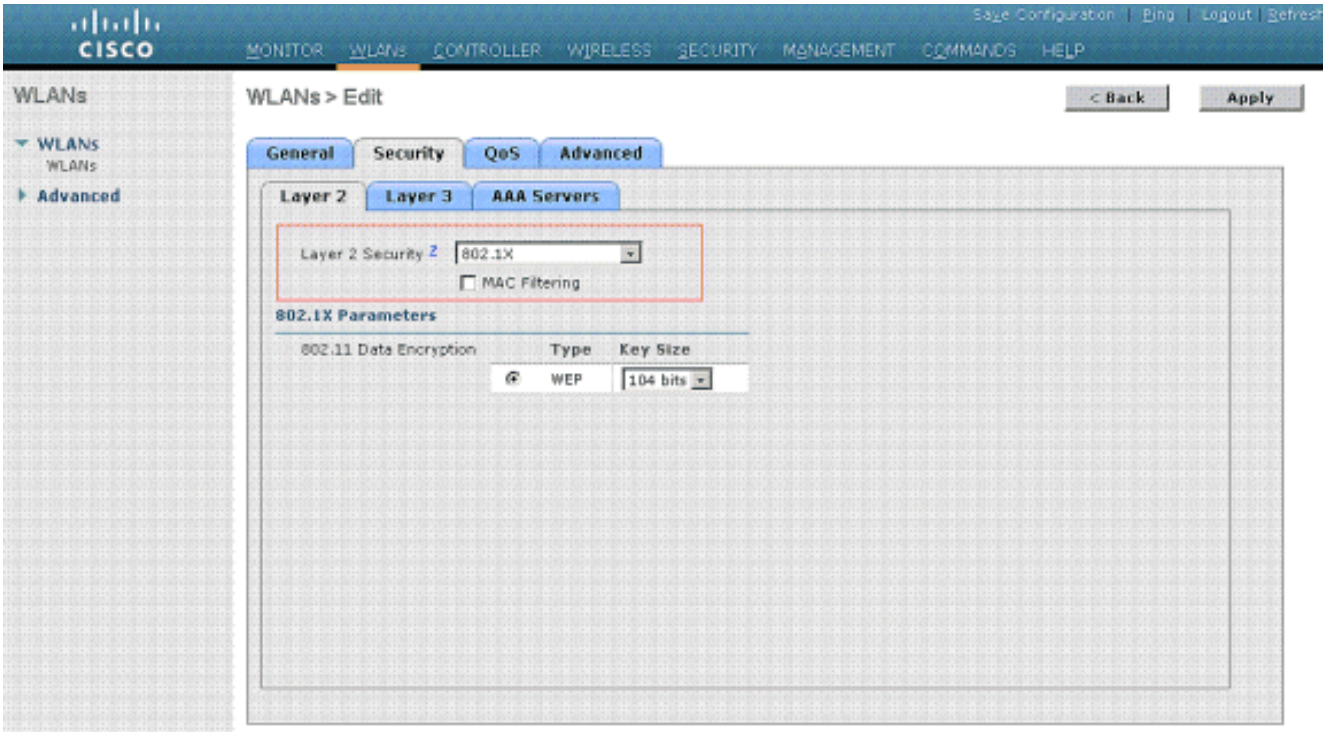
以下程式說明如何在WLC中設定WLAN。

請完成以下步驟：

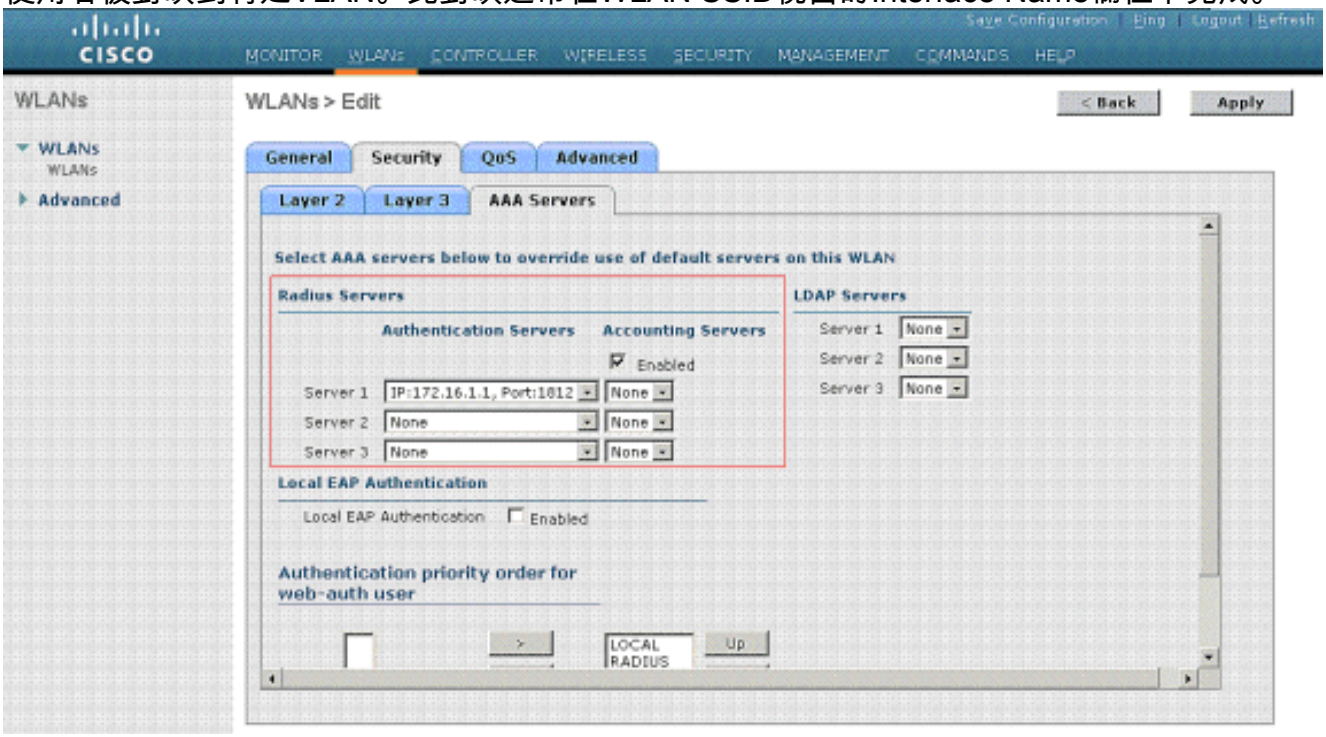
1. 在控制器GUI中，選擇**WLANs > New**以建立一個新的WLAN。將顯示「新建WLAN」視窗。
2. 輸入WLAN ID和WLAN SSID資訊。您可以輸入任何名稱作為WLAN SSID。本示例使用VLAN10作為WLAN SSID。

3. 按一下「**Apply**」以轉到WLAN SSID10的「Edit」視窗。



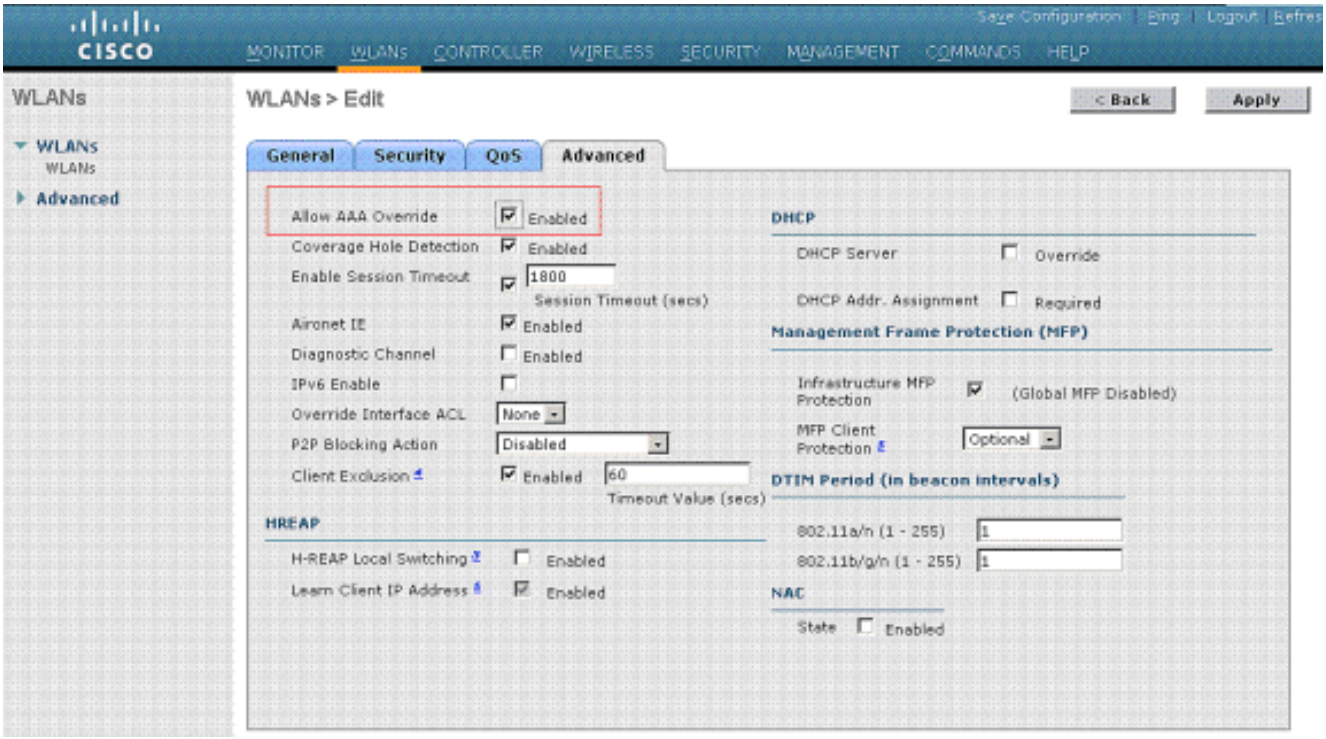


通常，在無線LAN控制器中，每個WLAN對映到特定VLAN(SSID)，以便屬於該WLAN的特定使用者被對映到特定VLAN。此對映通常在WLAN SSID視窗的Interface Name欄位下完成。



在所提供的範例中，RADIUS伺服器的作業是在成功驗證時將無線使用者端指派給特定的VLAN。WLAN不需要對映到WLC上的特定動態介面。或者，即使WLAN到動態介面對映是在WLC上完成的，RADIUS伺服器也會覆寫此對映，並將通過該WLAN的使用者指派給RADIUS伺服器中的user **Tunnel-Group-Private-ID**欄位下指定的VLAN。

4. 勾選**Allow AAA Override**核取方塊，以由RADIUS伺服器覆寫WLC組態。
5. 在控制器中針對配置的每個WLAN(SSID)啟用Allow AAA Override。



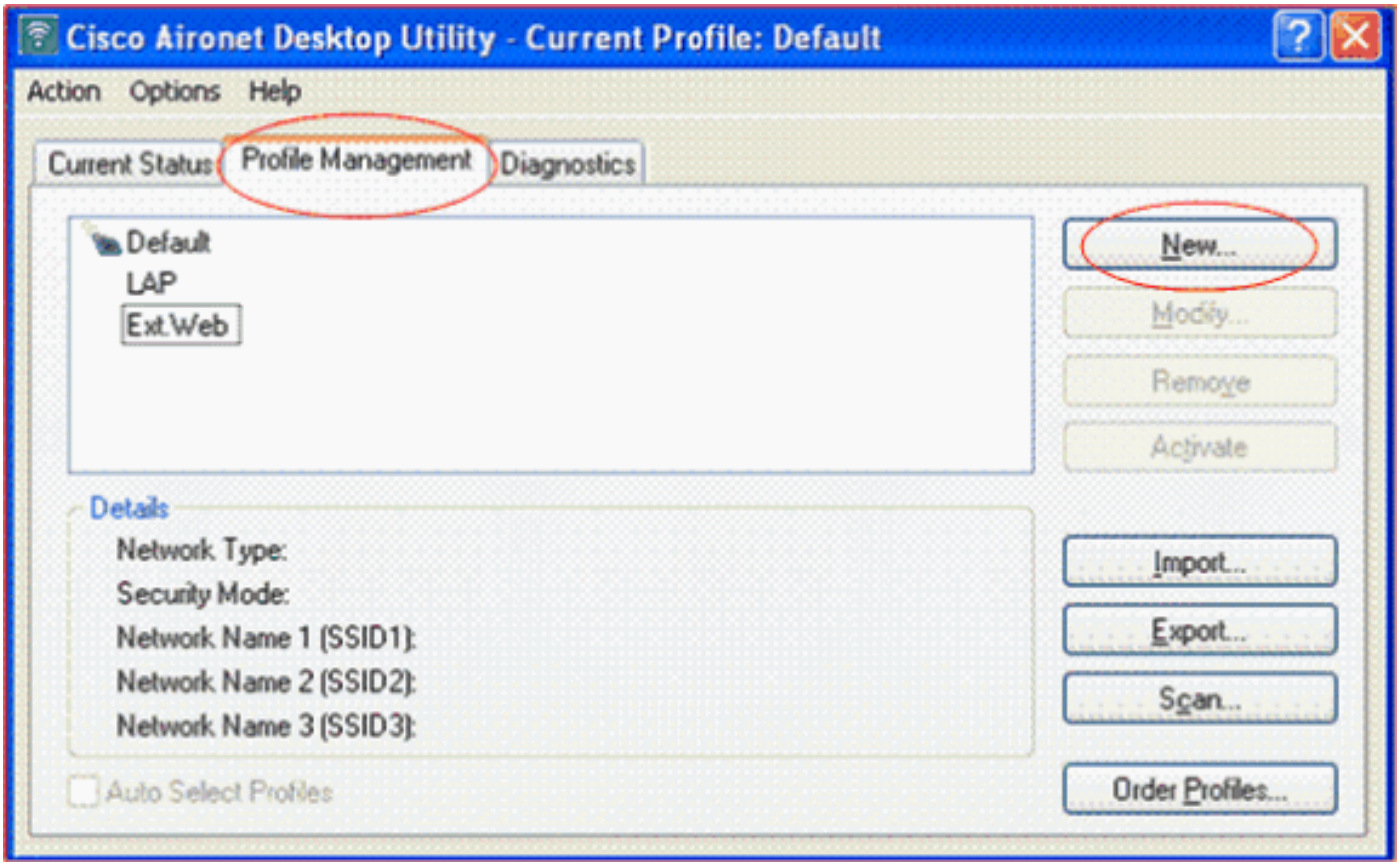
啟用AAA覆寫，且客戶端具有衝突的AAA和控制器WLAN驗證引數時，客戶端驗證由AAA(RADIUS)伺服器執行。作為身份驗證的一部分，作業系統將客戶端移動到AAA伺服器返回的VLAN。這是在控制器介面配置中預定義的。例如，如果企業WLAN主要使用分配給VLAN 2的管理介面，並且AAA Override返回重定向至VLAN 100，則作業系統會將所有客戶端傳輸重定向至VLAN 100，即使分配了VLAN 100的物理埠也是如此。禁用AAA覆蓋時，所有客戶端身份驗證都預設為控制器身份驗證引數設定，並且僅當控制器WLAN不包含任何客戶端特定的身份驗證引數時，AAA伺服器才執行身份驗證。

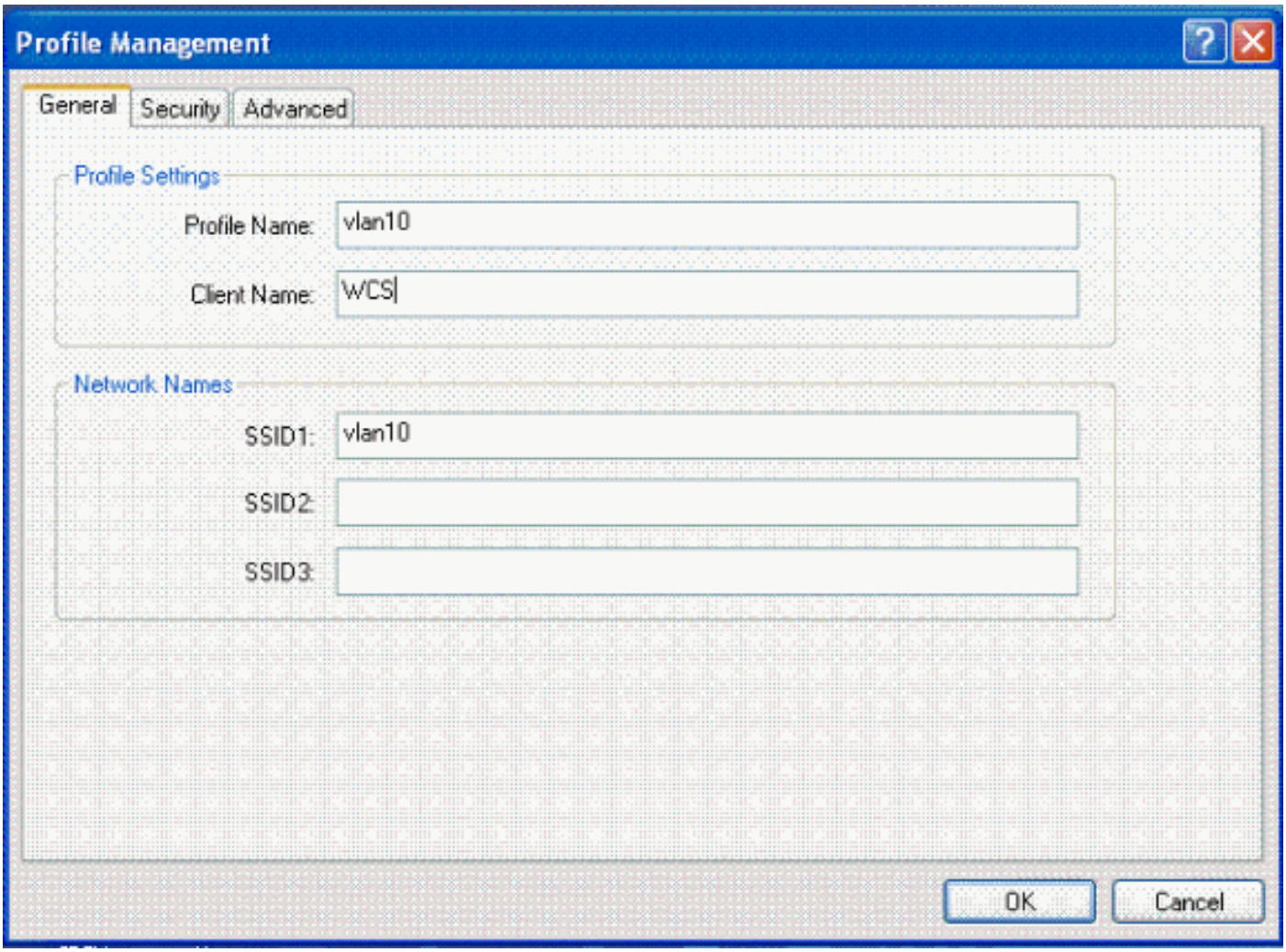
無線客戶端實用程式配置

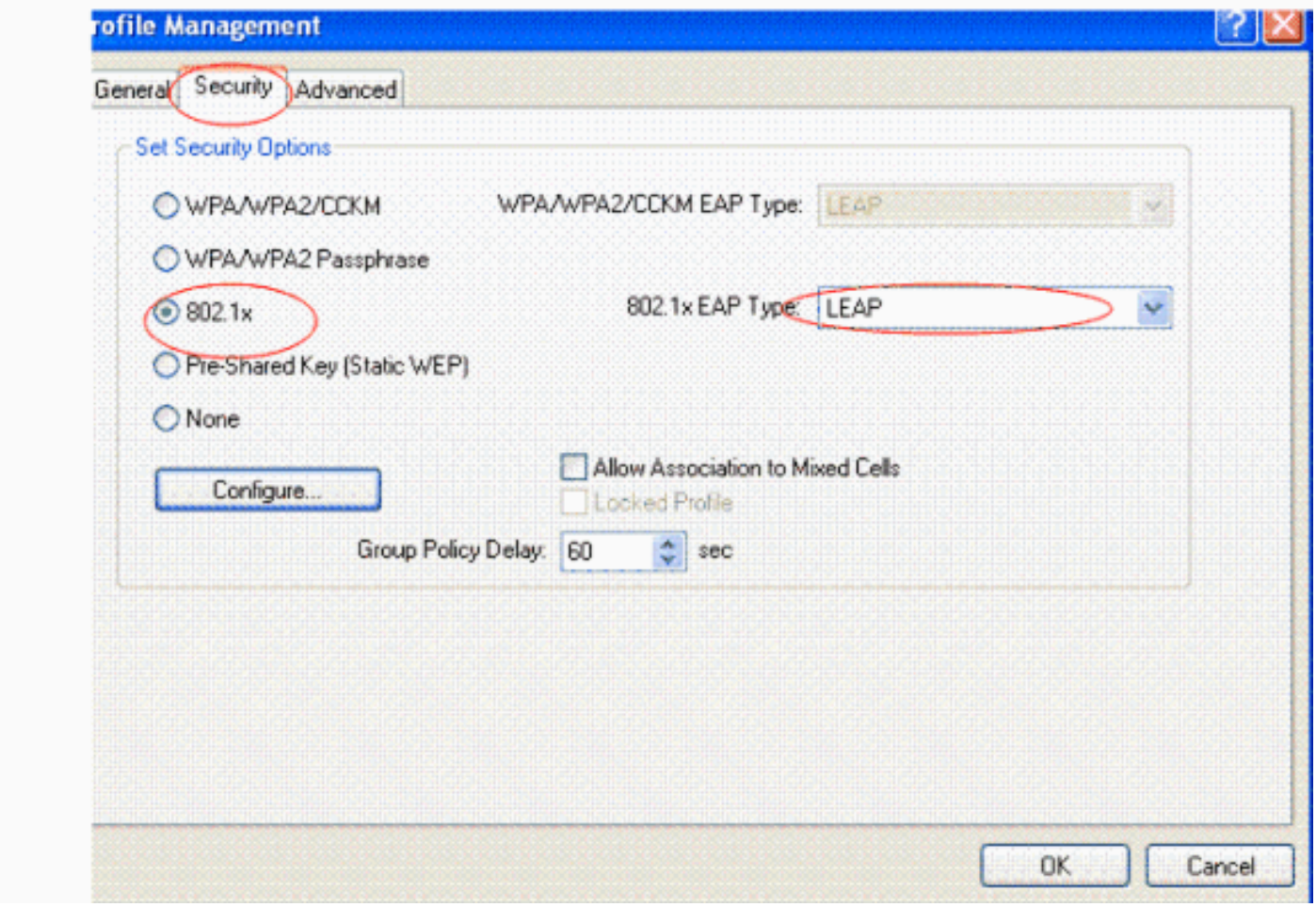
本文檔使用ADU作為客戶端實用程式來配置使用者配置檔案。此配置還使用LEAP作為身份驗證協定。如本節的示例所示，配置ADU。

在ADU選單欄中，選擇**Profile Management > New**以建立新配置檔案。

示例客戶端已配置為SSID VLAN10的一部分。以下圖顯示了如何在客戶端上配置使用者配置檔案：


Cisco Aironet Desktop Utility - Current Profile: Default
Action Options Help
Current Status
Profile Management
Diagnostics
Default
LAP
Ext.Web
New...
Modify...
Remove
Activate
Details
Network Type:
Security Mode:
Network Name 1 (SSID1):
Network Name 2 (SSID2):
Network Name 3 (SSID3):
Import...
Export...
Scan...
Auto Select Profiles
Order Profiles...


Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel



驗證

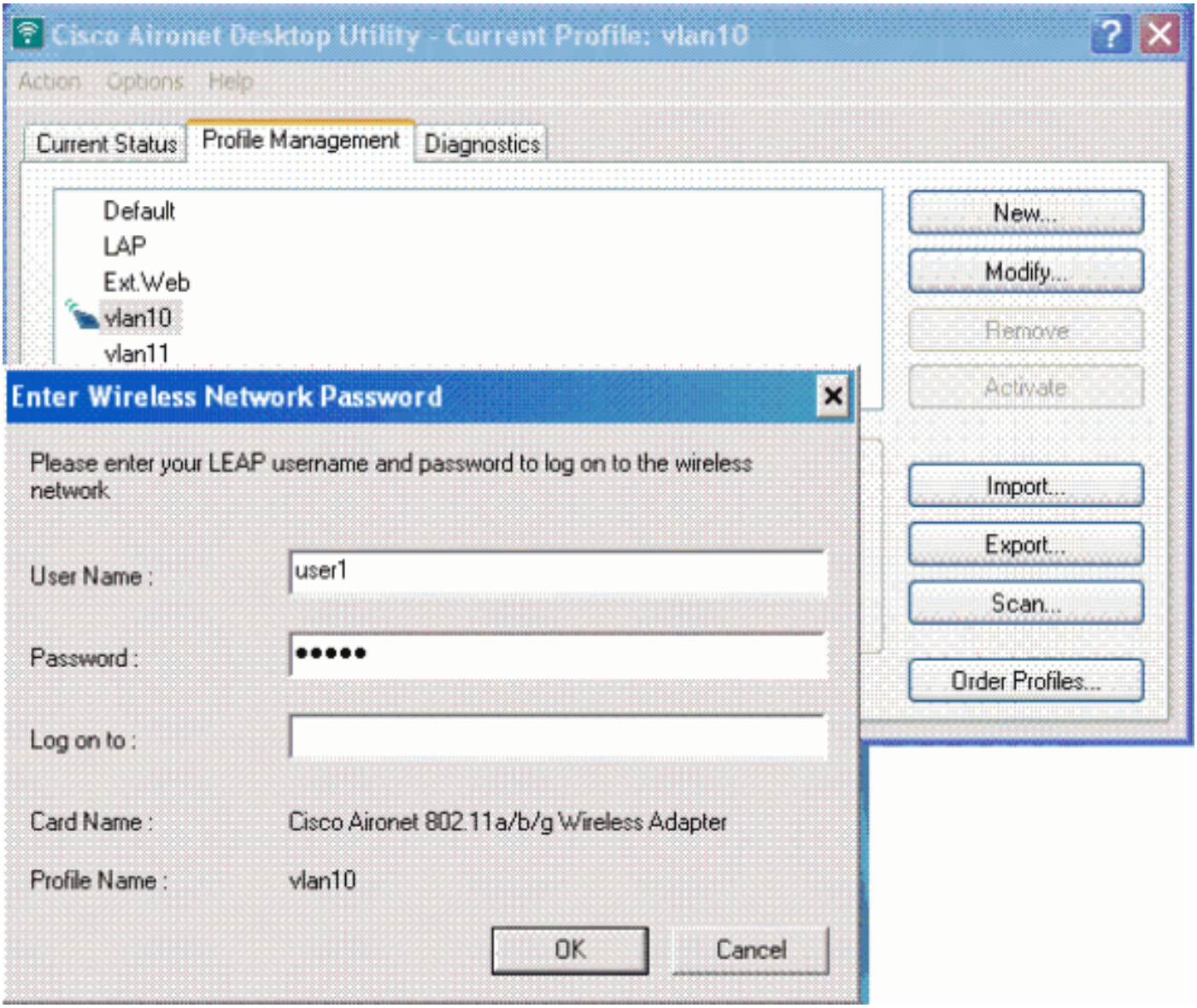
啟用您在ADU中配置的使用者配置檔案。根據組態，系統會提示您輸入使用者名稱和密碼。您也可以指示ADU使用Windows使用者名稱和密碼進行身份驗證。有許多選項可供客戶端接收身份驗證。您可以在已建立的使用者配置檔案的Security > Configure頁籤下配置這些選項。

在上一個範例中，請注意user1已指派給RADIUS伺服器中所指定的VLAN10。

此範例從使用者端使用此使用者名稱和密碼來接收驗證，並由RADIUS伺服器指派給VLAN:

- 使用者名稱= user1
- 密碼= user1

此示例說明如何提示SSID VLAN10輸入使用者名稱和密碼。在此範例中輸入使用者名稱和密碼：

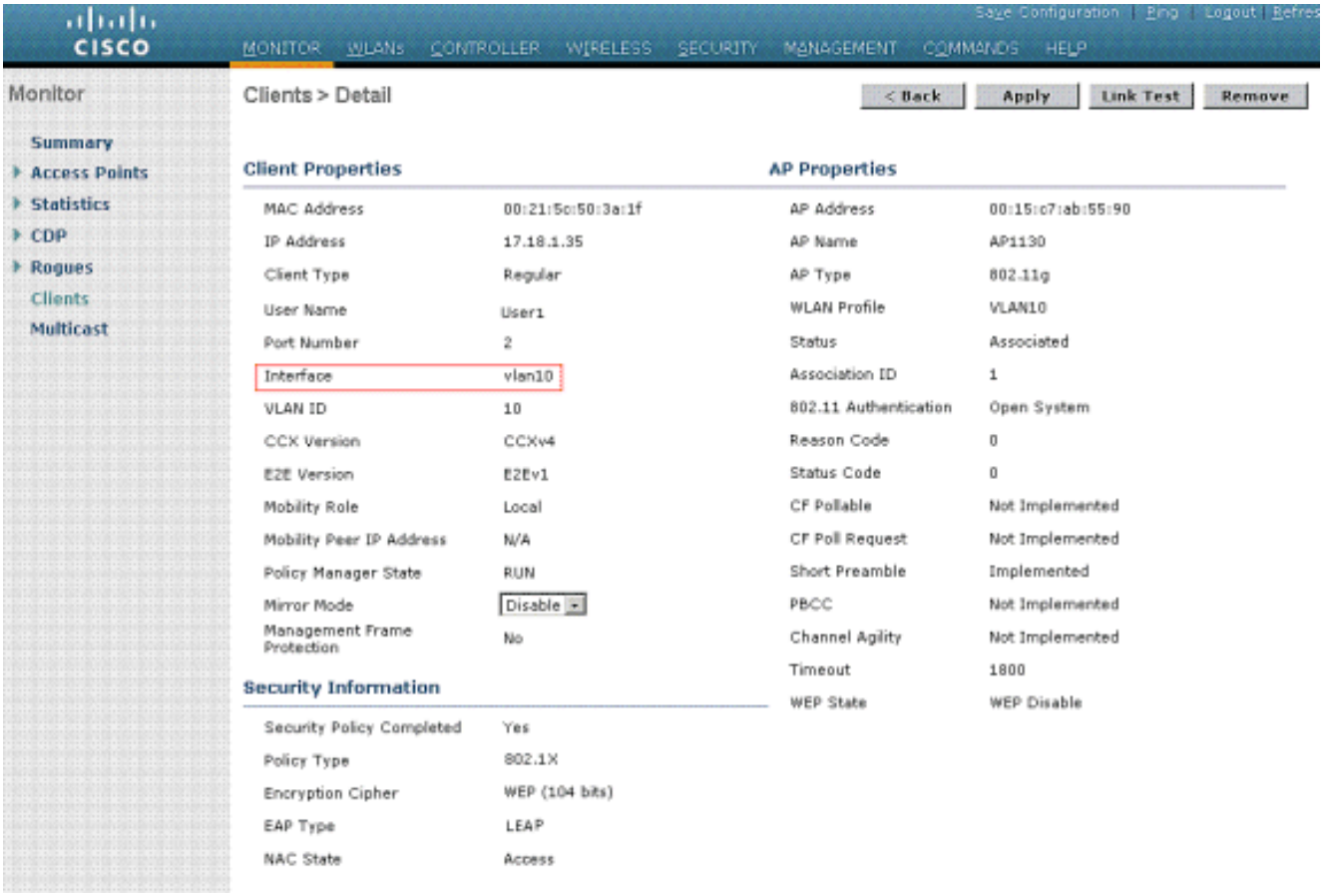


身份驗證和相應的驗證成功後，您將收到成功狀態消息。

接下來，您需要確認是否根據傳送的RADIUS屬性，將使用者端指派給適當的VLAN。完成以下步驟即可完成此操作：

1. 在控制器GUI中選擇**Wireless > AP**。
2. 按一下**Clients**（客戶端），該按鈕顯示在Access Points(AP)視窗的左角。將顯示客戶端統計資訊。

3. 按一下**Details**以識別使用者端的完整詳細資訊，例如IP位址、其指派的VLAN等。此示例顯示客戶端user1的這些詳細資訊
：



在此視窗中，您可以看到此使用者端是按照RADIUS伺服器上設定的RADIUS屬性指派給VLAN10。**註：如果動態VLAN分配基於Cisco Airespace VSA屬性設定，則Interface name（介面名稱）將顯示為admin(根據此示例在客戶端詳細資訊頁面上)。**

使用本節內容，確認您的組態是否正常運作。

- **debug aaa events enable** — 此命令可用於確保RADIUS屬性通過控制器成功傳輸到客戶端。偵錯輸出的以下部分可確保成功傳輸RADIUS屬性：

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- 以下命令也很有用：**debug dot1x aaa enabledebug aaa packets enable**

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

注意：動態VLAN分配不適用於WLC的Web驗證。

相關資訊

- 使用RADIUS伺服器的EAP身份驗證
- Cisco LEAP
- 思科無線LAN控制器組態設定指南4.0版
- 技術支援與文件 - Cisco Systems