使用無線LAN控制器和Cisco Secure ACS的每個使用者ACL配置示例

目錄

簡介

本檔案將通過範例說明如何在WLC上建立存取控制清單(ACL)，並將其套用到依賴RADIUS授權的使用者。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 有關如何配置Cisco Secure ACS伺服器以驗證無線客戶端的基本知識
- 瞭解Cisco Aironet輕量型存取點(LAP)和Cisco無線LAN控制器(WLC)的組態
- 思科統一無線安全解決方案知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行5.0.148.0版的Cisco 4400系列無線LAN控制器
- 思科Aironet 1231系列輕量型接入點(LAP)
- 運行3.6版的Cisco Aironet 802.11 a/b/g Cisco無線LAN客戶端介面卡
- Cisco Aironet案頭實用程式版本3.6
- Cisco安全ACS伺服器版本4.1
- 執行IOS®版本12.4(11)T的Cisco 2800系列整合式服務路由器
- 執行12.0(5)WC3b版的Cisco Catalyst 2900XL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

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

每使用者訪問控制清單(ACL)是思科身份網路的一部分。Cisco無線LAN解決方案支援身份網路，雖然它允許網路通告單個SSID，但也允許特定使用者根據其使用者配置檔案繼承不同的策略。

每使用者ACL功能提供將無線LAN控制器上配置的ACL基於RADIUS授權應用到使用者的功能。這是使用Airespace-ACL-Name供應商特定屬性(VSA)完成的。

此屬性指明應用於客戶端的ACL名稱。當RADIUS存取接受中存在ACL屬性時，系統會在使用者站進行驗證之後將ACL名稱套用到使用者站。這會覆蓋分配給介面的所有ACL。它會忽略分配的介面ACL並應用新的介面ACL。

ACL-Name屬性格式的摘要如下所示。欄位從左向右傳輸

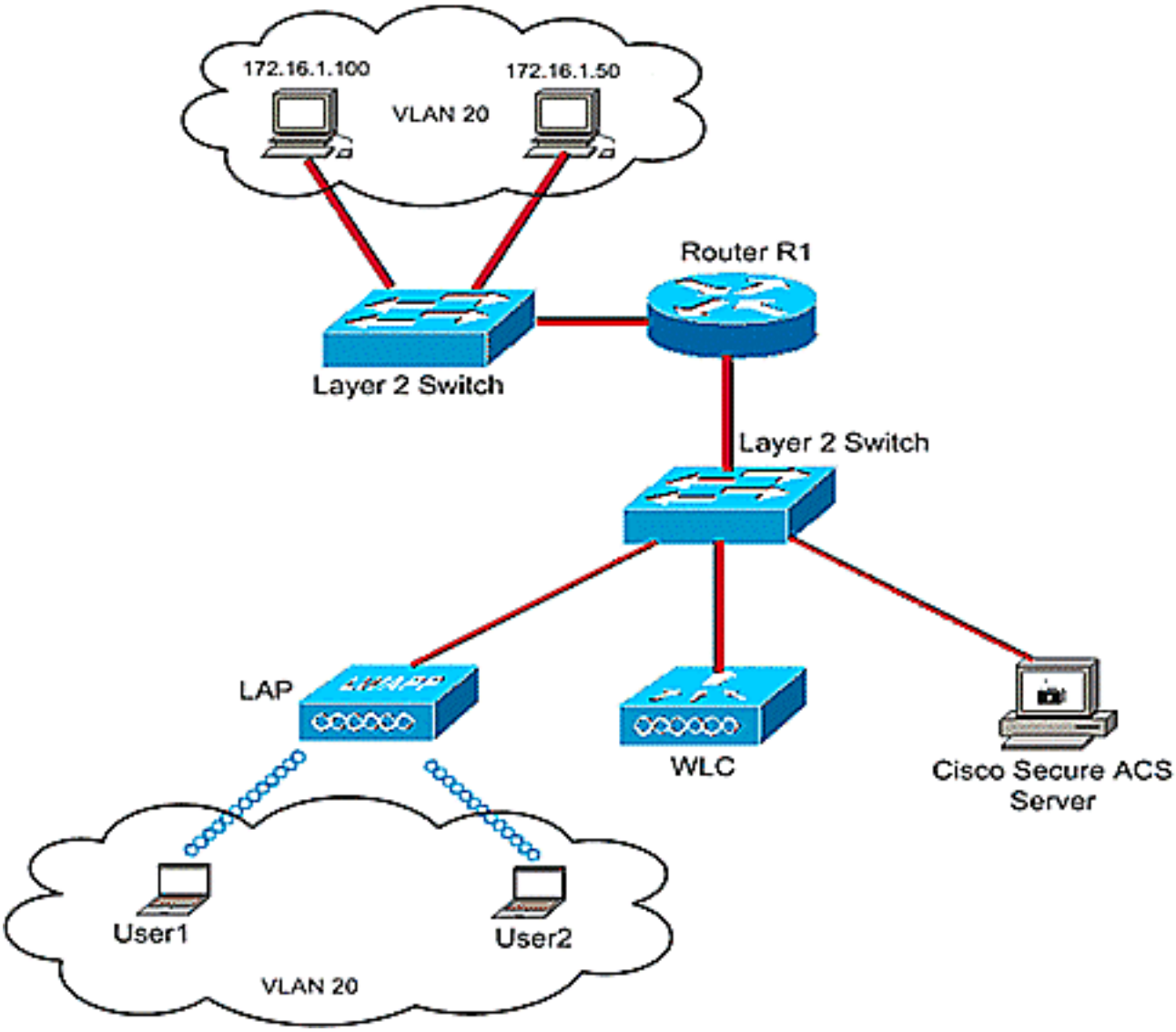
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to use for the client.
   The string is case sensitive.
```

有關Cisco統一無線網路身份網路的詳細資訊，請參閱配置安全解決方案文檔的配置身份網路部分。

網路圖表

本檔案會使用以下網路設定：

在此設定中，無線LAN控制器WLC和LAP用於為部門A和部門B中的使用者提供無線服務。所有無線使用者都使用通用的WLAN(SSID)Office來訪問網路，並且處於VLAN Office-VLAN中。



Cisco Secure ACS伺服器用於驗證無線使用者。EAP身份驗證用於驗證使用者。WLC、LAP和Cisco Secure ACS伺服器連線到第2層交換機，如圖所示。

路由器R1通過第2層交換機連線有線端上的伺服器，如圖所示。路由器R1還充當DHCP伺服器，為子網172.16.0.0/16中的無線客戶端提供IP地址。

您需要配置裝置以便發生以下情況：

部門A的User1隻能訪問伺服器172.16.1.100

部門B的使用者2僅訪問伺服器172.16.1.50

為此，您需要在WLC上建立2個ACL:一個用於User1，另一個用於User2。建立ACL後，您需要配置Cisco Secure ACS伺服器，以便在無線使用者成功身份驗證時將ACL名稱屬性返回到WLC。接著，WLC會將ACL套用至使用者，因此網路會根據使用者設定檔而受限制。

注意：本文檔使用LEAP身份驗證對使用者進行身份驗證。Cisco LEAP易受字典攻擊。在即時網路中，應使用更安全的身份驗證方法，如EAP FAST。由於本檔案的重點是解釋如何配置每使用者ACL功能，因此使用LEAP是為了簡化。

下一節將提供為此設定配置裝置的逐步說明。

設定

設定每個使用者ACL功能之前，您必須設定WLC以達成基本操作，並向WLC註冊LAP。本檔案假設WLC已設定為基本操作，且LAP已註冊到WLC。如果您是嘗試設定WLC以使用LAP執行基本操作的新使用者，請參閱向無線LAN控制器(WLC)註冊輕量AP(LAP)。

註冊LAP後，請完成以下步驟，為此設定配置裝置：

1. 設定無線LAN控制器。
2. 配置Cisco Secure ACS伺服器。
3. 驗證設定.

註：本文檔討論無線端所需的配置。本檔案假設有線組態已就緒。

設定無線LAN控制器

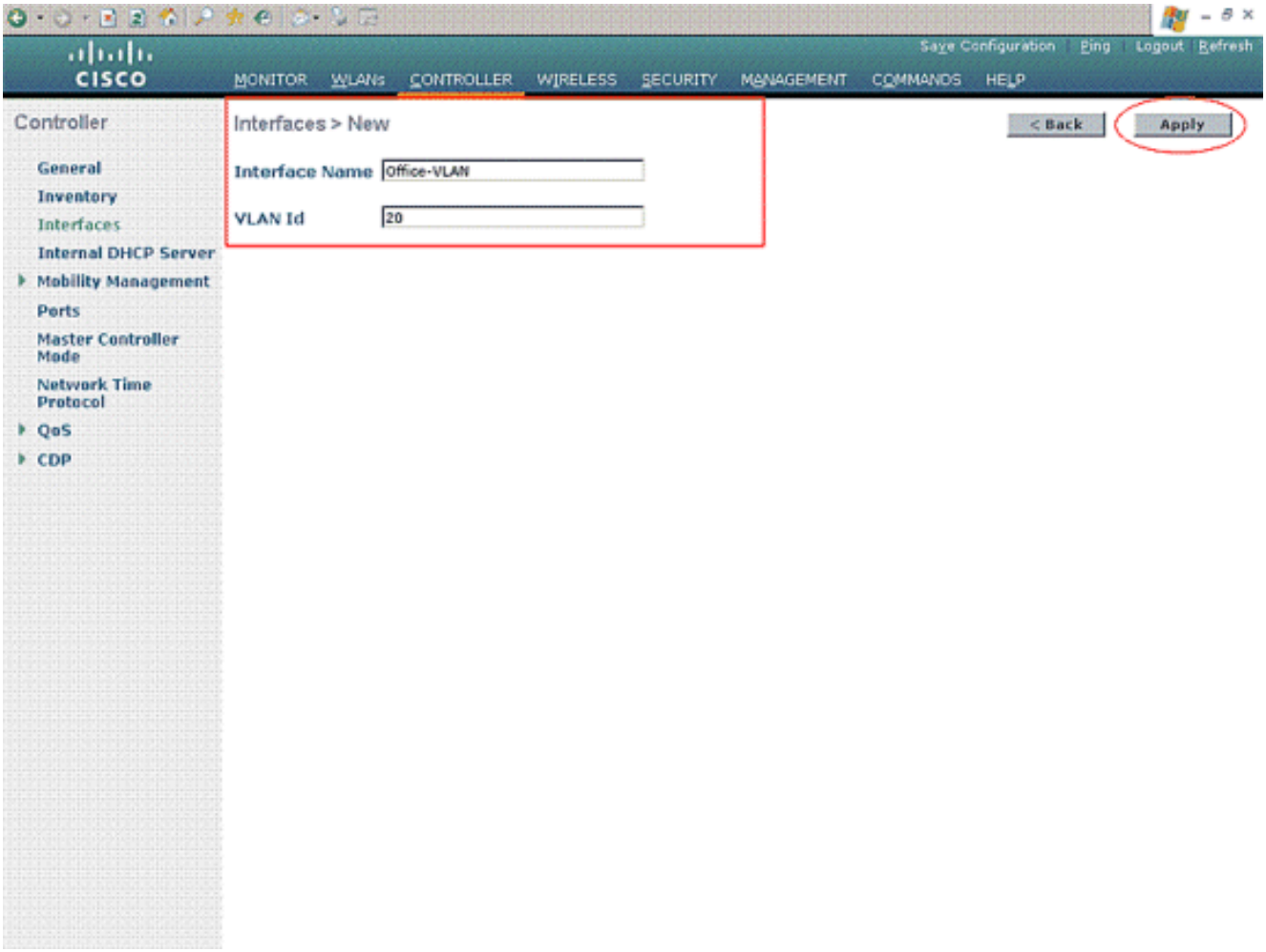
在無線LAN控制器上，您需要執行以下操作：

- 為無線使用者建立VLAN。
- 配置WLC以使用Cisco Secure ACS驗證無線使用者。
- 為無線使用者建立新的WLAN。
- 為無線使用者定義ACL。

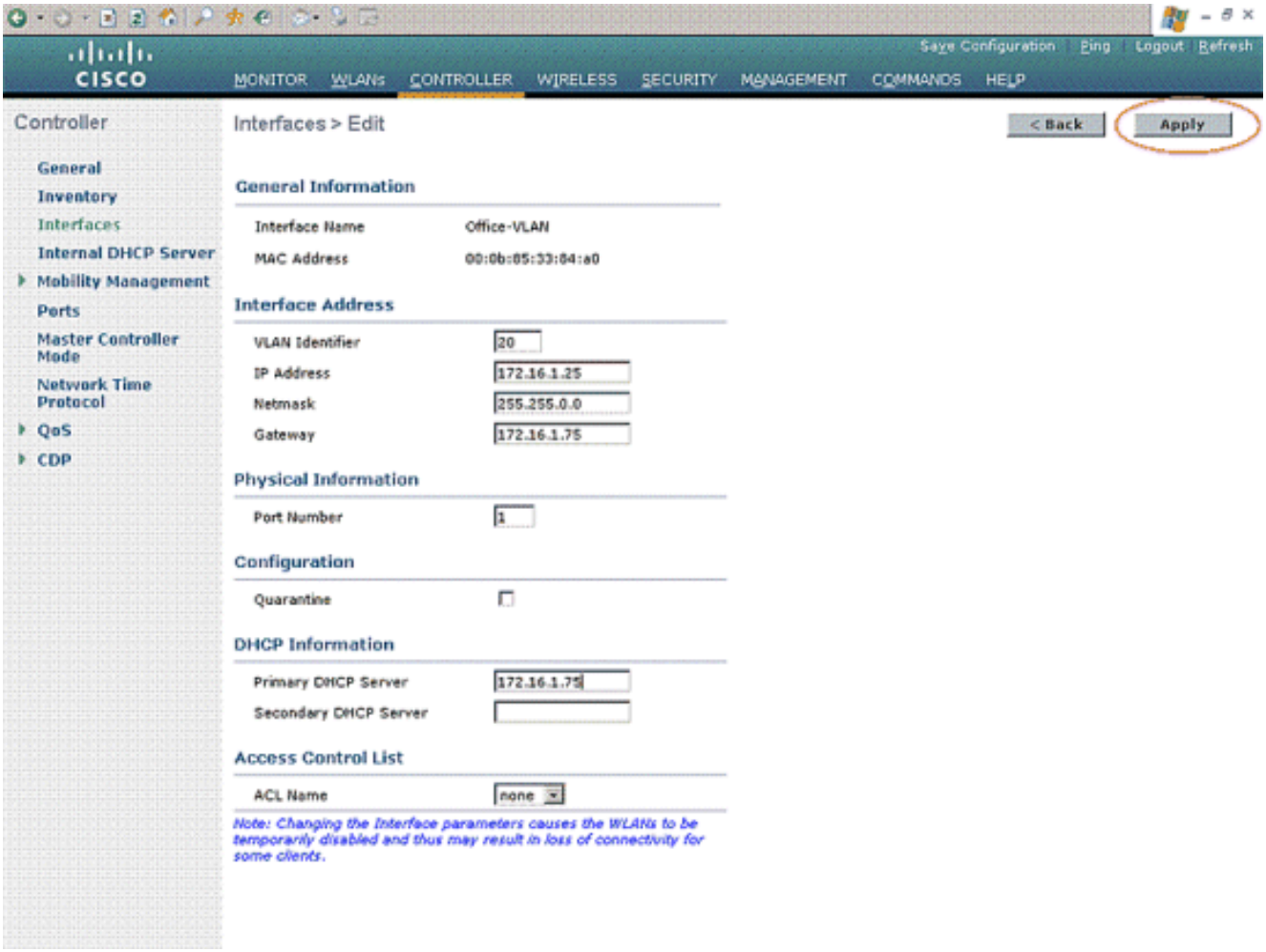
為無線使用者建立VLAN

要為無線使用者建立VLAN，請完成以下步驟。

1. 前往WLC GUI並選擇**Controller > Interfaces**。出現「Interfaces（介面）」視窗。此視窗列出控制器上配置的介面。
2. 按一下「**New**」以建立一個新的動態介面。
3. 在**Interfaces > New**視窗中，輸入介面名稱和VLAN ID。然後點選應用。在本示例中，動態介面命名為Office-VLAN，VLAN ID分配為20。



4. 在**Interfaces > Edit**視窗中，輸入動態介面的IP地址、子網掩碼和預設網關。將其分配給WLC上的物理埠，並輸入DHCP伺服器的IP地址。然後按一下「**Apply**」。



在本例中，以下引數用於Office-VLAN介面：

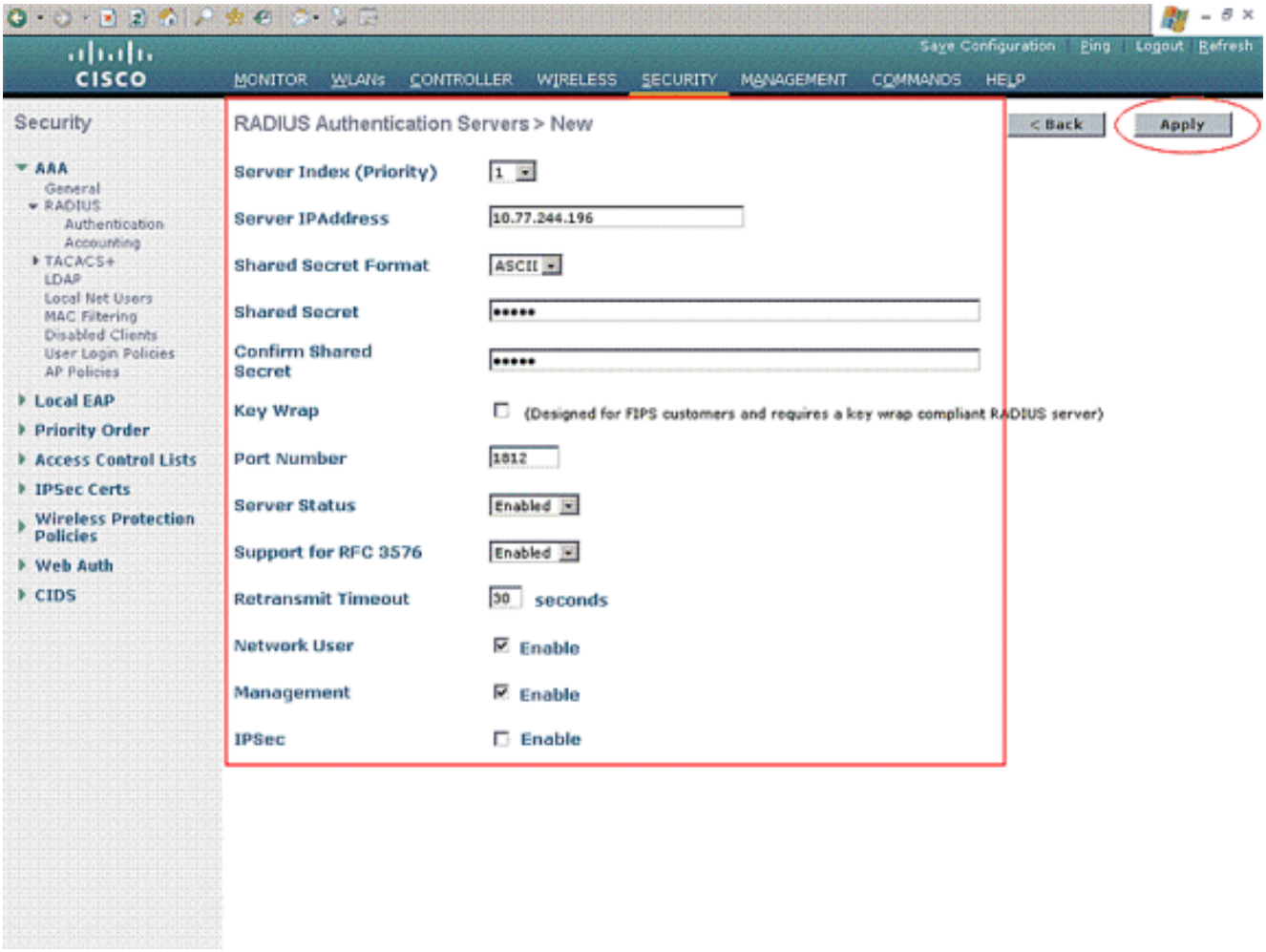
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

配置WLC以使用Cisco Secure ACS進行身份驗證

需要設定WLC，才能將使用者憑證轉送到外部RADIUS伺服器（在本案例中為Cisco Secure ACS）。 接著，RADIUS伺服器會驗證使用者認證，並在無線使用者成功驗證後，將ACL name屬性返回到WLC。

完成以下步驟，以便為RADIUS伺服器設定WLC:

1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**，以顯示**RADIUS Authentication Servers**頁面。然後按一下**New**以定義RADIUS伺服器。
2. 在**RADIUS Authentication Servers > New**頁中定義RADIUS伺服器引數。這些引數包括RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。

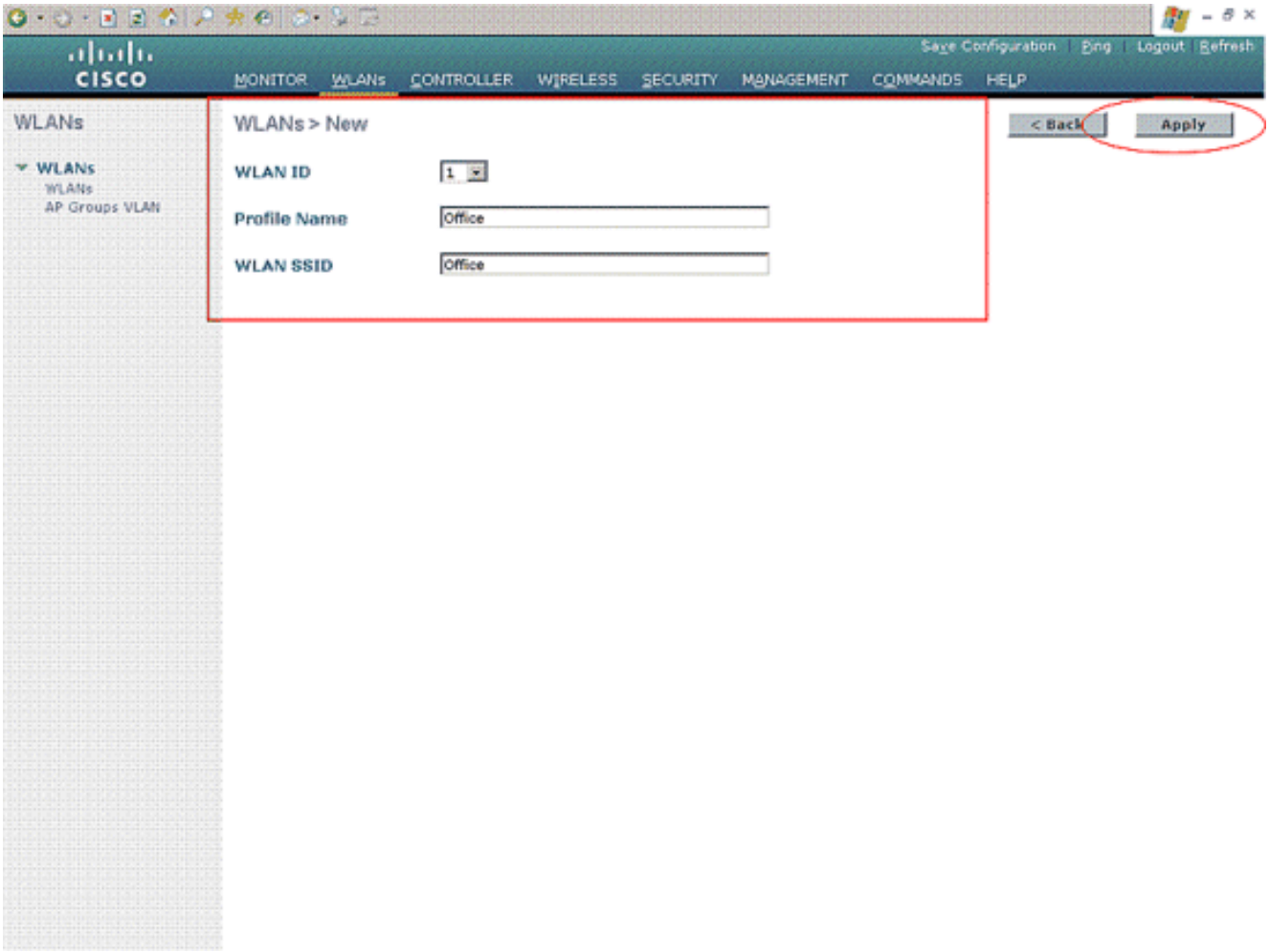


3. **Network User**和**Management**覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用Cisco Secure ACS作為IP地址為10.77.244.196的RADIUS伺服器。按一下**Apply**。

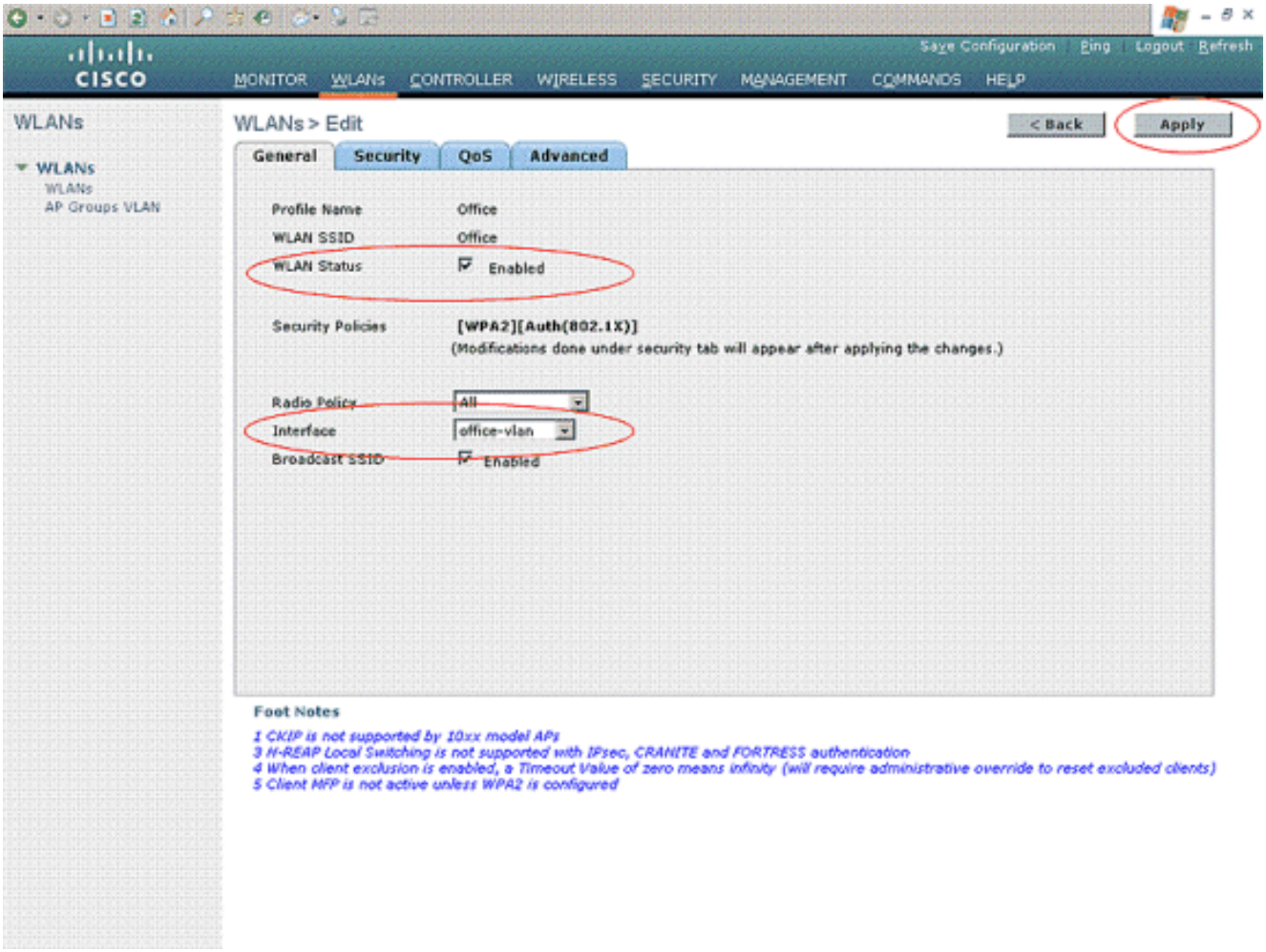
為無線使用者建立新的WLAN

接下來，您需要建立無線使用者可連線的WLAN。若要建立新的WLAN，請完成以下步驟：

1. 在無線LAN控制器GUI中，按一下「**WLANs**」。此頁面列出控制器上存在的WLAN。
2. 選擇**New**以建立一個新的WLAN。輸入WLAN的WLAN ID、Profile Name和WLAN SSID，然後點選**Apply**。對於此設定，請建立WLAN **Office**。

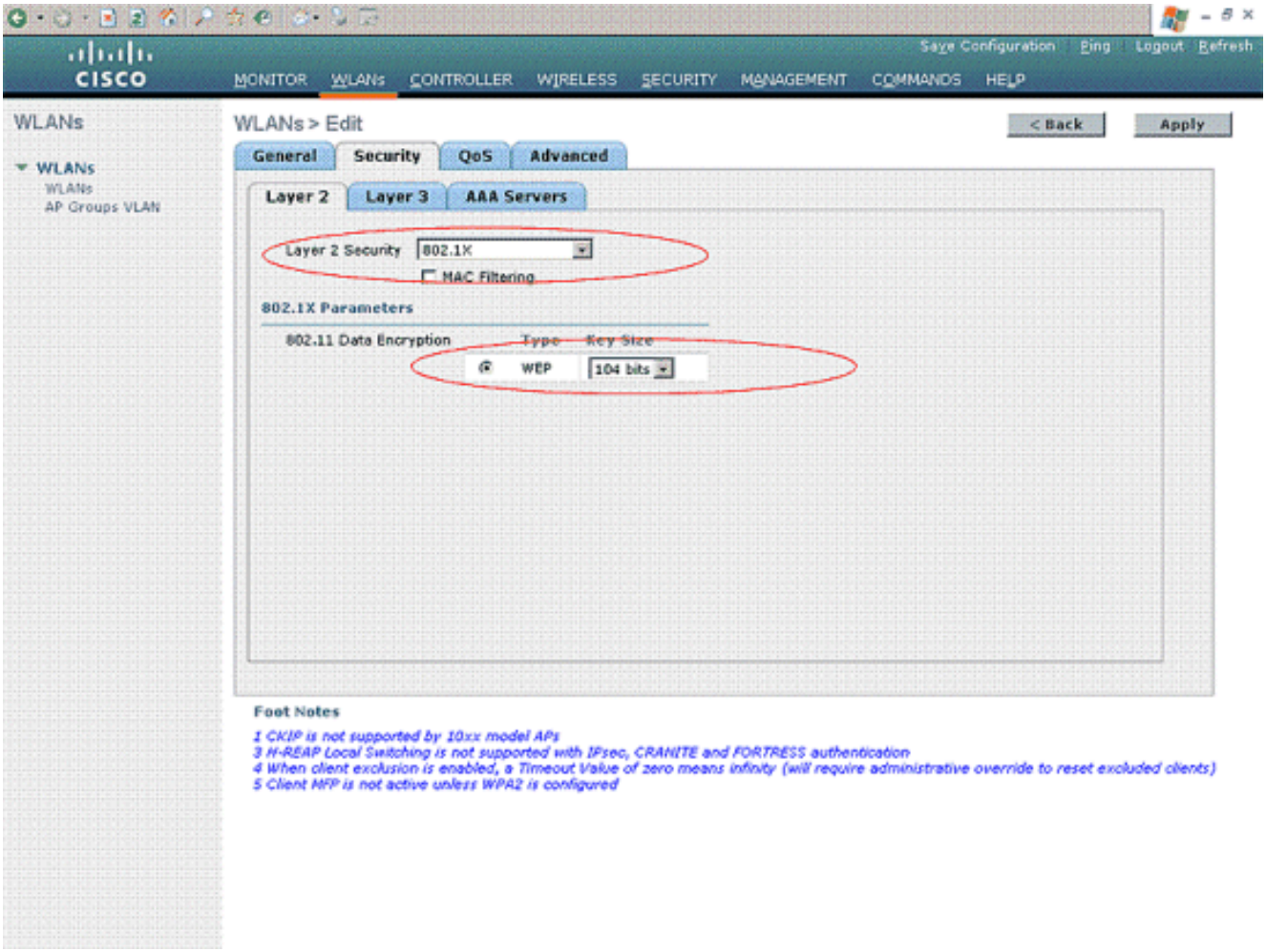


3. 建立新的WLAN後，系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面中，您可以定義特定於此WLAN的各種引數，其中包括常規策略、安全、QoS和高級引數。

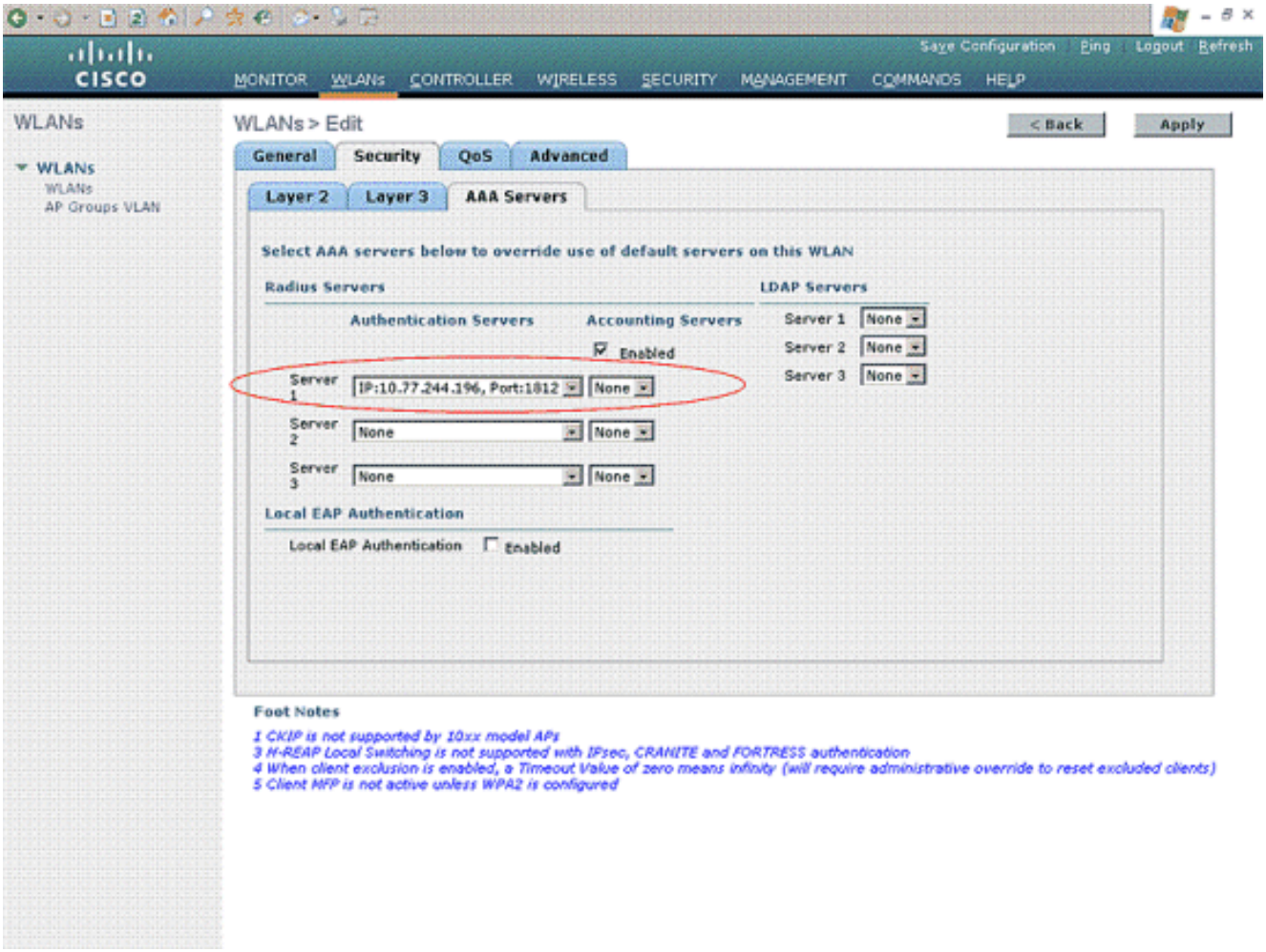


檢查General策略下的**WLAN Status**，以啟用WLAN。從下拉選單中選擇適當的介面。在本例中，使用介面**Office-vlan**。本頁上的其他引數可以根據WLAN網路的要求進行修改。

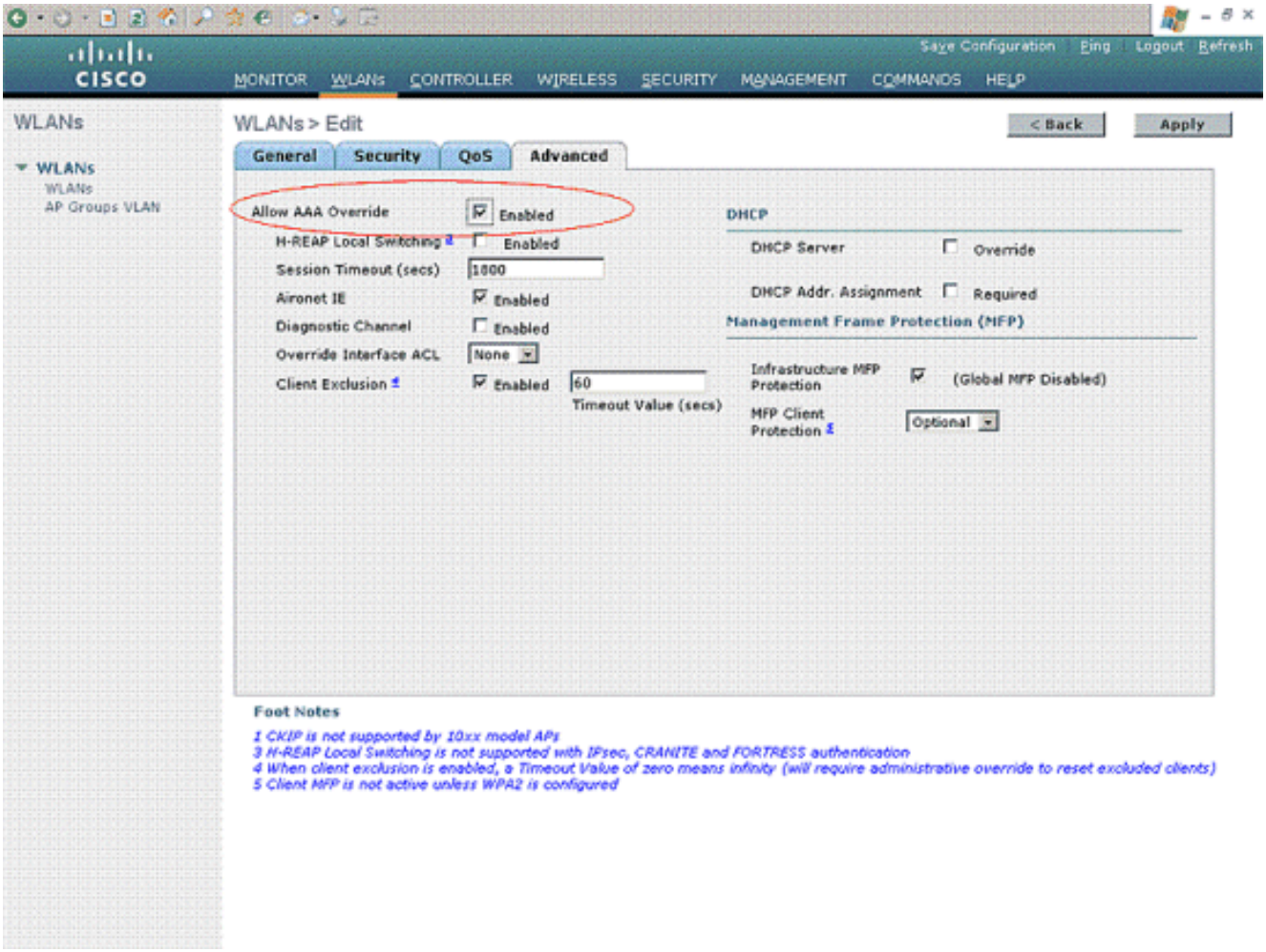
4. 選擇**Security**頁籤。從Layer 2 security下拉選單中選擇**802.1x**（因為這是LEAP身份驗證）。在802.1x引數下選擇適當的WEP金鑰大小。



5. 在Security頁籤下，選擇**AAA server**子頁籤。選擇用於對無線客戶端進行身份驗證的AAA伺服器。在本示例中，使用ACS伺服器10.77.244.196對無線客戶端進行身份驗證。



6. 選擇Advanced 索引標籤。選中Allow AAA Override以配置通過無線LAN上的AAA的使用者策略覆蓋。



如果啟用AAA覆蓋，且客戶端的AAA和Cisco無線LAN控制器無線LAN身份驗證引數發生衝突，則客戶端身份驗證由AAA伺服器執行。作為此驗證的一部分，作業系統會將客戶端從預設思科無線LAN解決方案無線LAN VLAN移動到AAA伺服器返回並在Cisco無線LAN控制器介面配置中預定義的VLAN中，這僅在針對MAC過濾、802.1X和/或WPA操作進行配置時發生。在所有情況下，作業系統還使用AAA伺服器提供的QoS、DSCP、802.1p優先順序標籤值和ACL，只要這些值是在Cisco無線LAN控制器介面配置中預定義的。

7. 根據網路要求選擇其他引數。按一下「**Apply**」。

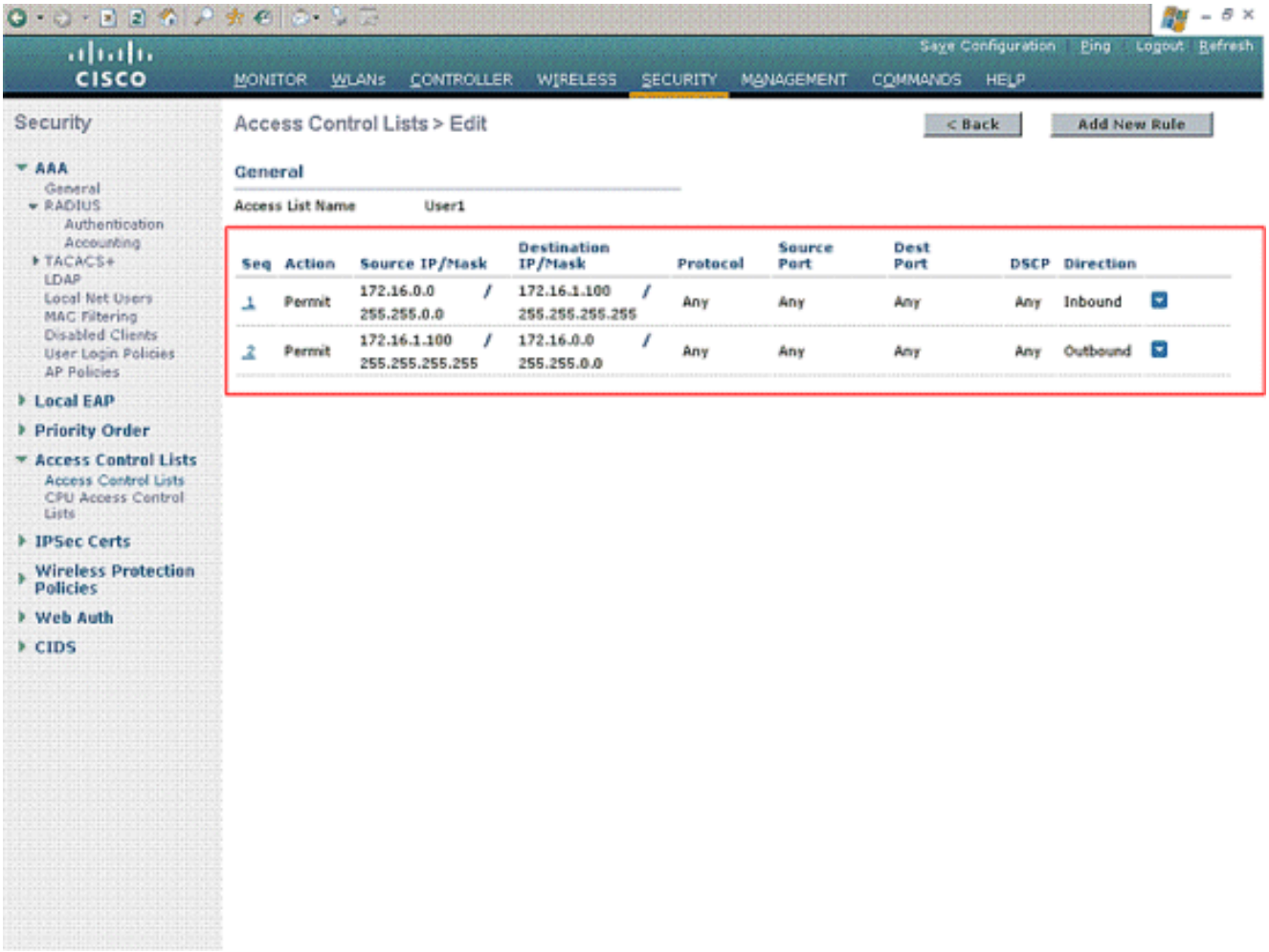
定義使用者的ACL

您需要為此設定建立兩個ACL:

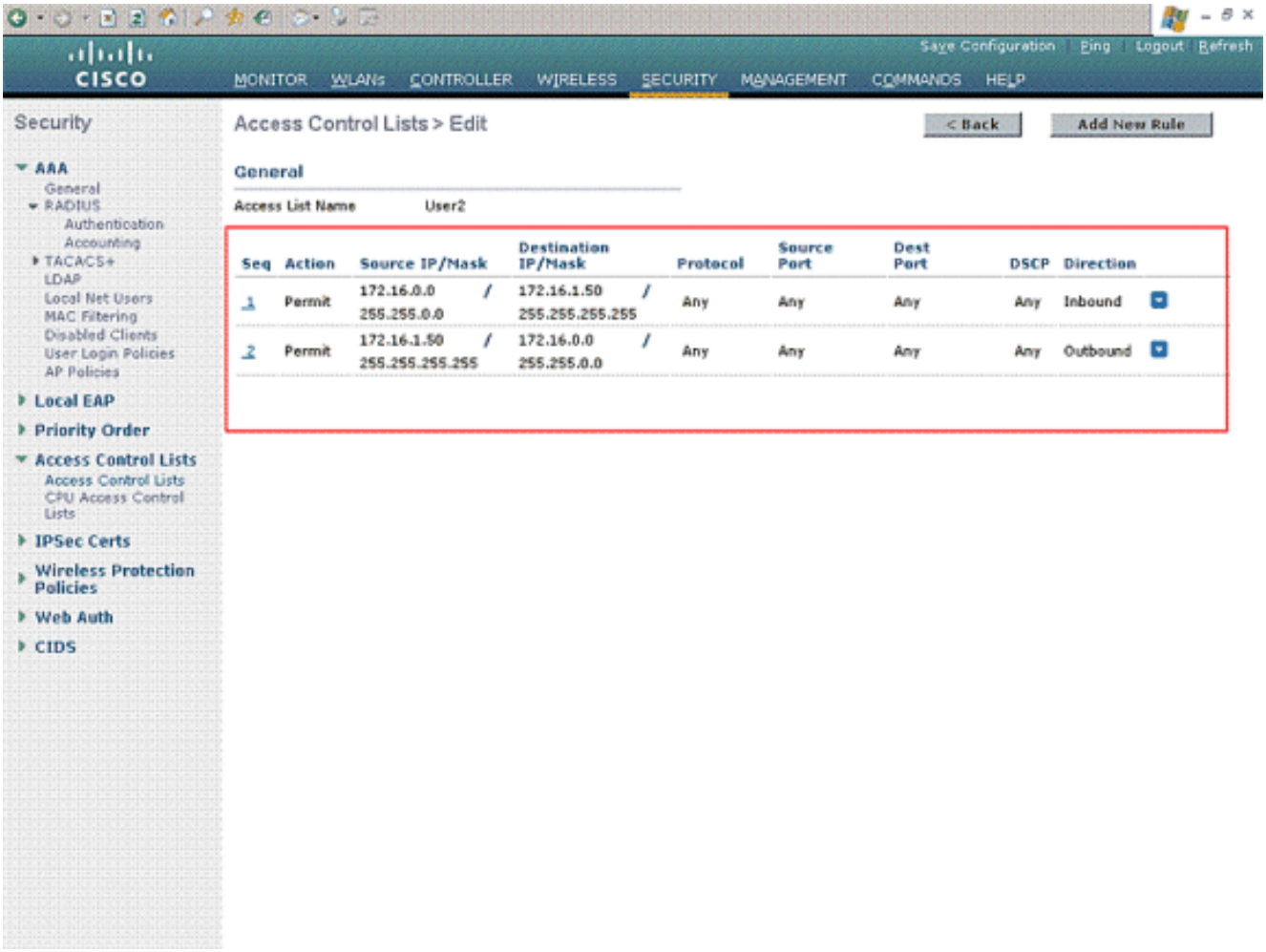
- ACL1:為了僅提供對User1對伺服器172.16.1.100的訪問
- ACL2:為了僅提供對User2對伺服器172.16.1.50的訪問

完成以下步驟即可在WLC上設定ACL:

1. 在WLC GUI中選擇**Security > Access Control Lists**。系統將顯示Access Control Lists頁面。此頁列出在WLC上配置的ACL。此功能也允許您編輯或刪除任何ACL。若要建立新的ACL，請按一下**New**。
2. 此頁允許您建立新的ACL。輸入ACL的名稱，然後按一下**Apply**。建立ACL後，按一下**Edit**為ACL建立規則。
3. User1只需要能夠訪問伺服器172.16.1.100，並且必須拒絕訪問所有其他裝置。為此，您需要定義這些規則。有關如何配置無線LAN控制器上ACL的詳細資訊，請參閱無線LAN控制器上的ACL配置示例。



4. 同樣，您需要為User2建立ACL，僅允許User2訪問伺服器172.16.1.50。這是User2所需的ACL。



現在您已為此設定配置無線LAN控制器。下一步是將Cisco安全存取控制伺服器設定為驗證無線使用者端，並在成功驗證後將ACL Name屬性傳回WLC。

配置Cisco Secure ACS伺服器

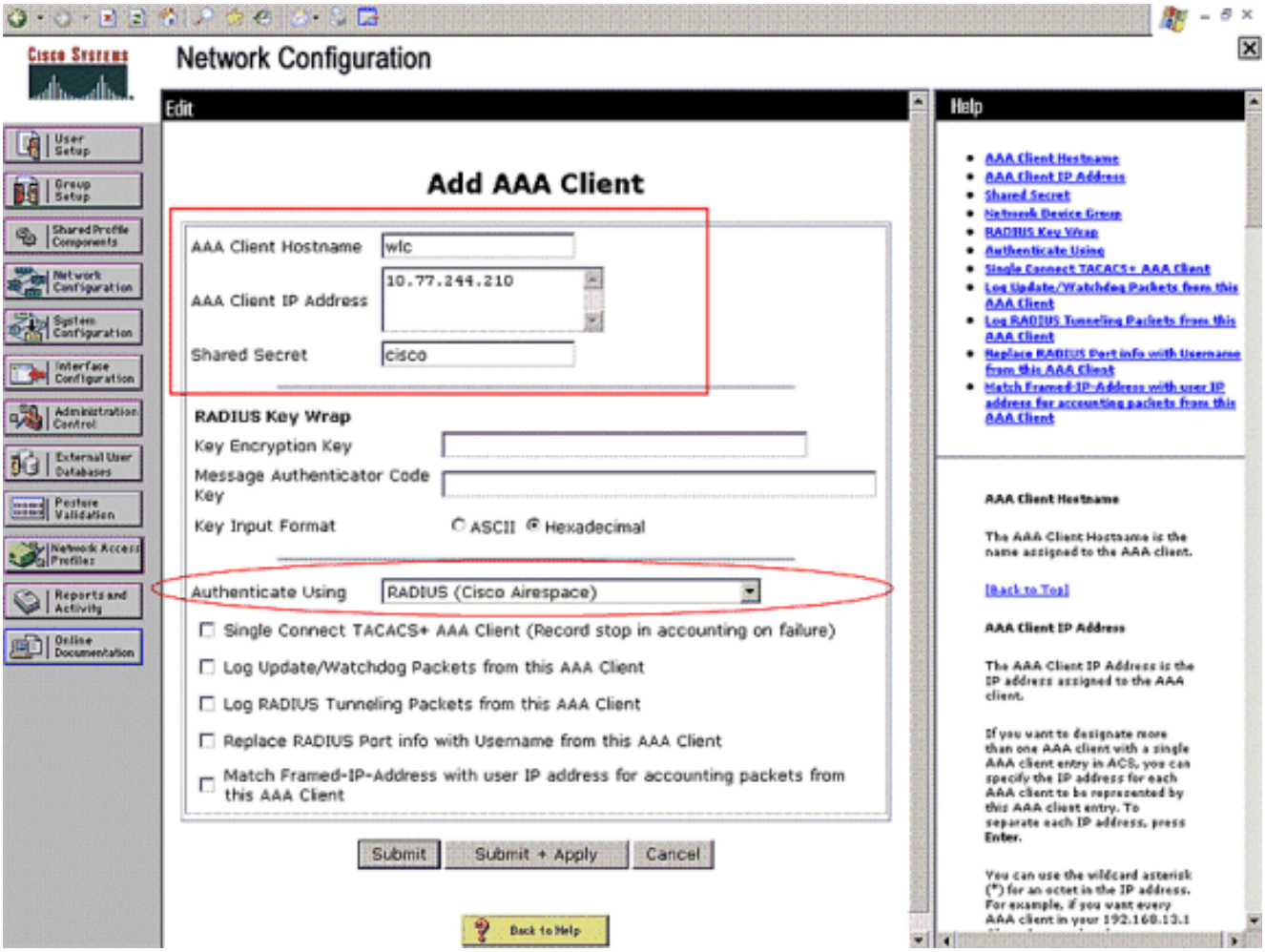
要使Cisco Secure ACS能夠對無線客戶端進行身份驗證，您需要完成以下步驟：

- 將無線區域網控制器配置為Cisco Secure ACS上的AAA客戶端。
- 在Cisco Secure ACS上配置使用者和使用者配置檔案。

將無線區域網控制器配置為Cisco Secure ACS上的AAA客戶端

若要將無線LAN控制器設定為Cisco Secure ACS上的AAA使用者端，請完成以下步驟：

1. 按一下**Network Configuration > Add AAA client**。系統將顯示**Add AAA client**頁面。在此頁面中，定義WLC系統名稱、管理介面IP位址、共用金鑰和使用**Radius** Airespace進**行驗證**。以下是範例
   ：



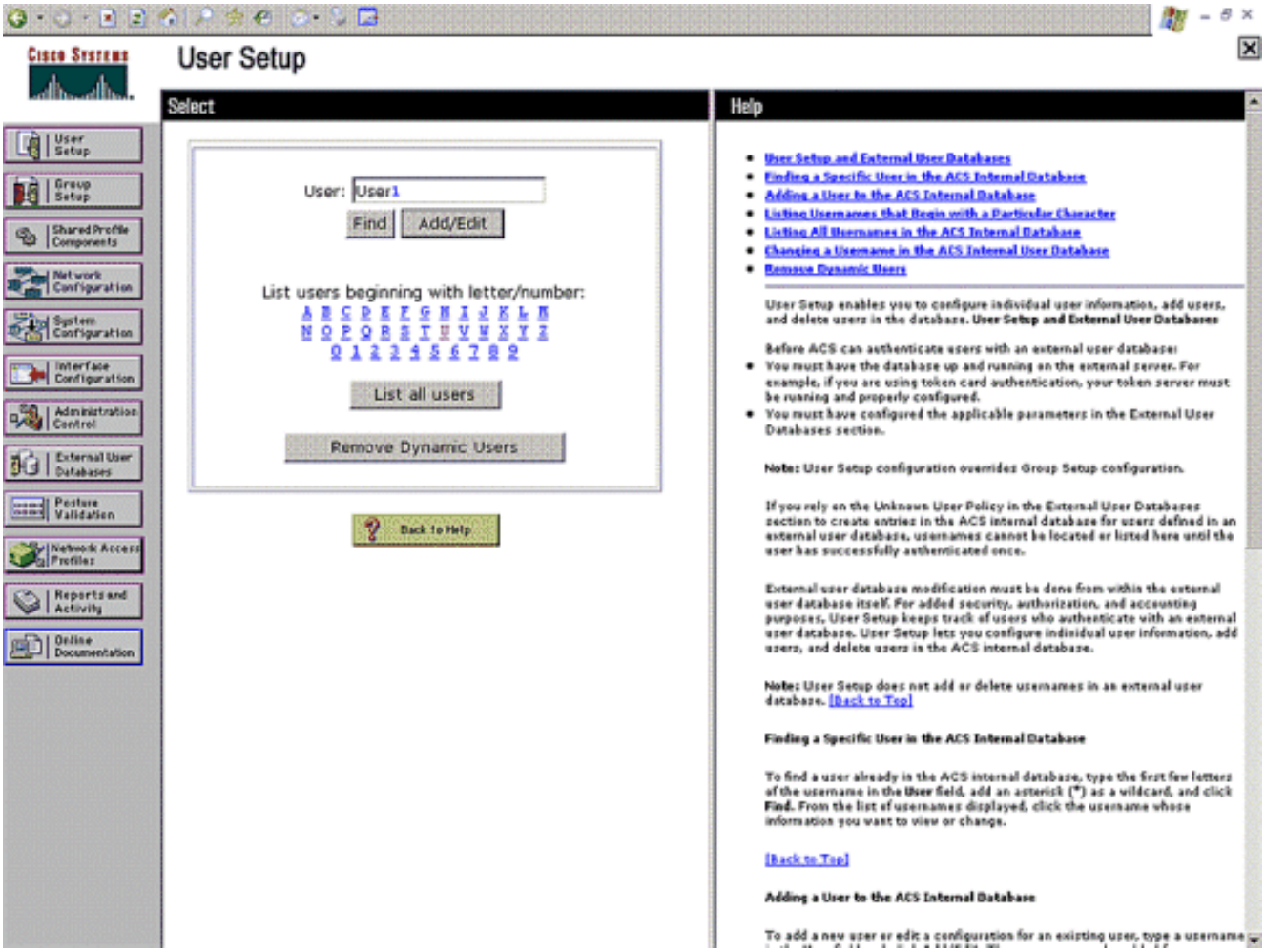
注意：在Cisco Secure ACS上配置的共用金鑰必須與WLC上在**RADIUS Authentication Servers > New下配置的共用金鑰匹配。**

2. 按一下「**Submit+Apply**」。

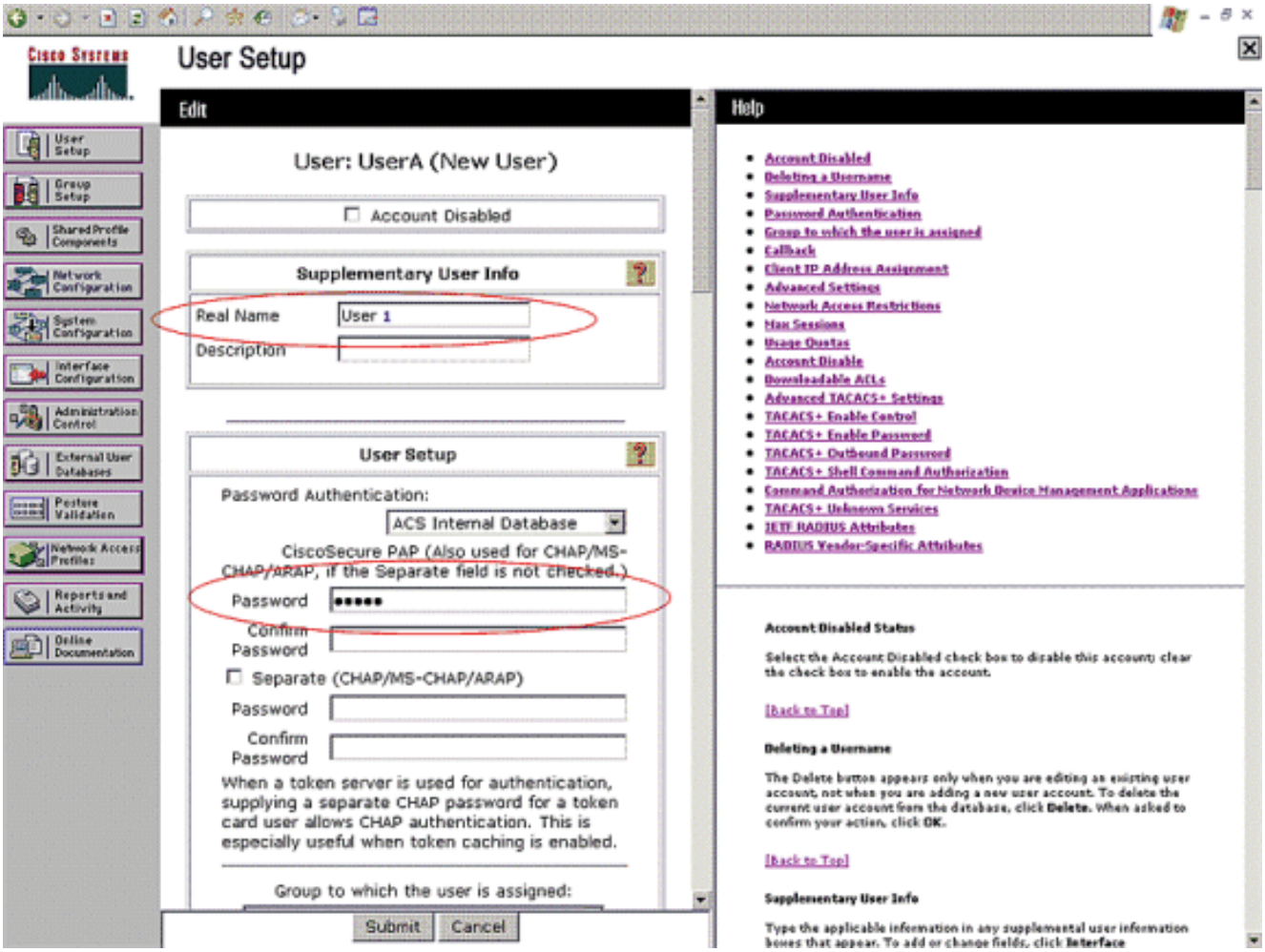
在Cisco Secure ACS上配置使用者和使用者配置檔案

要在Cisco Secure ACS上配置使用者，請完成以下步驟：

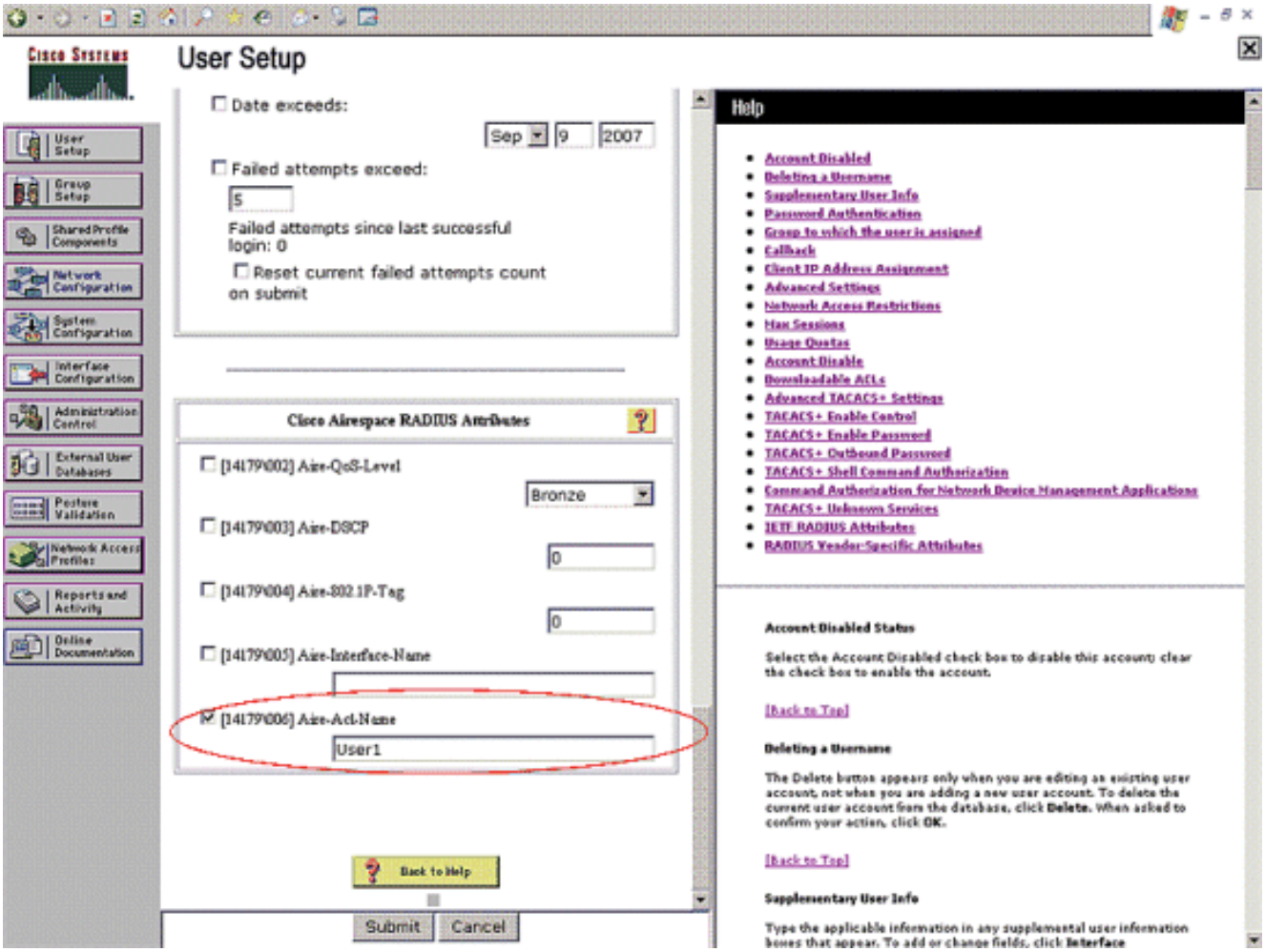
1. 從ACS GUI中選擇**User Setup**，輸入使用者名稱，然後按一下**Add/Edit**。在本示例中，使用者為**User1**。



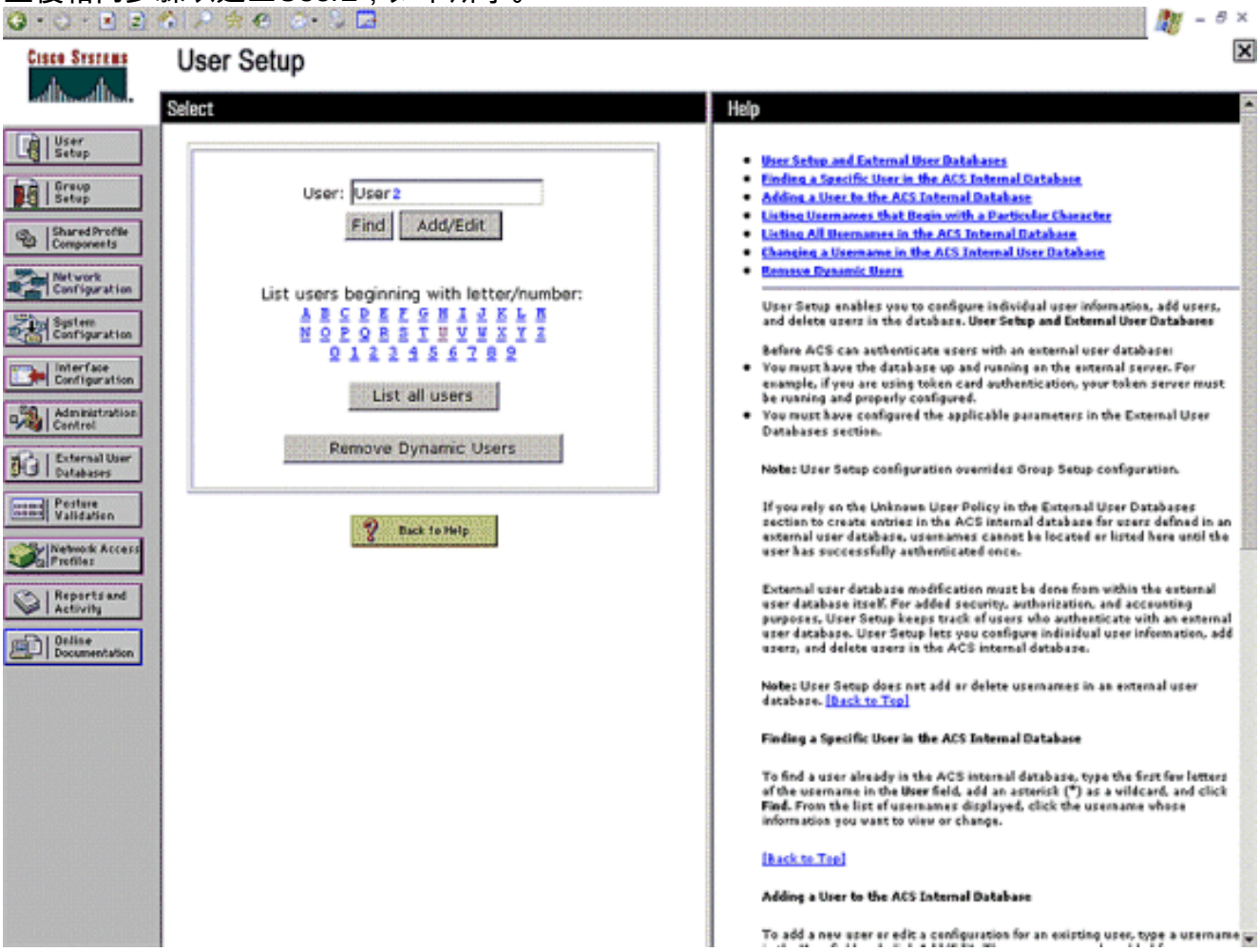
2. 顯示「**使用者設定**」頁時，定義特定於使用者的所有引數。在本示例中，由於僅需要這些引數進行EAP身份驗證，因此配置了username、password、Supplementary User Information和RADIUS屬性。

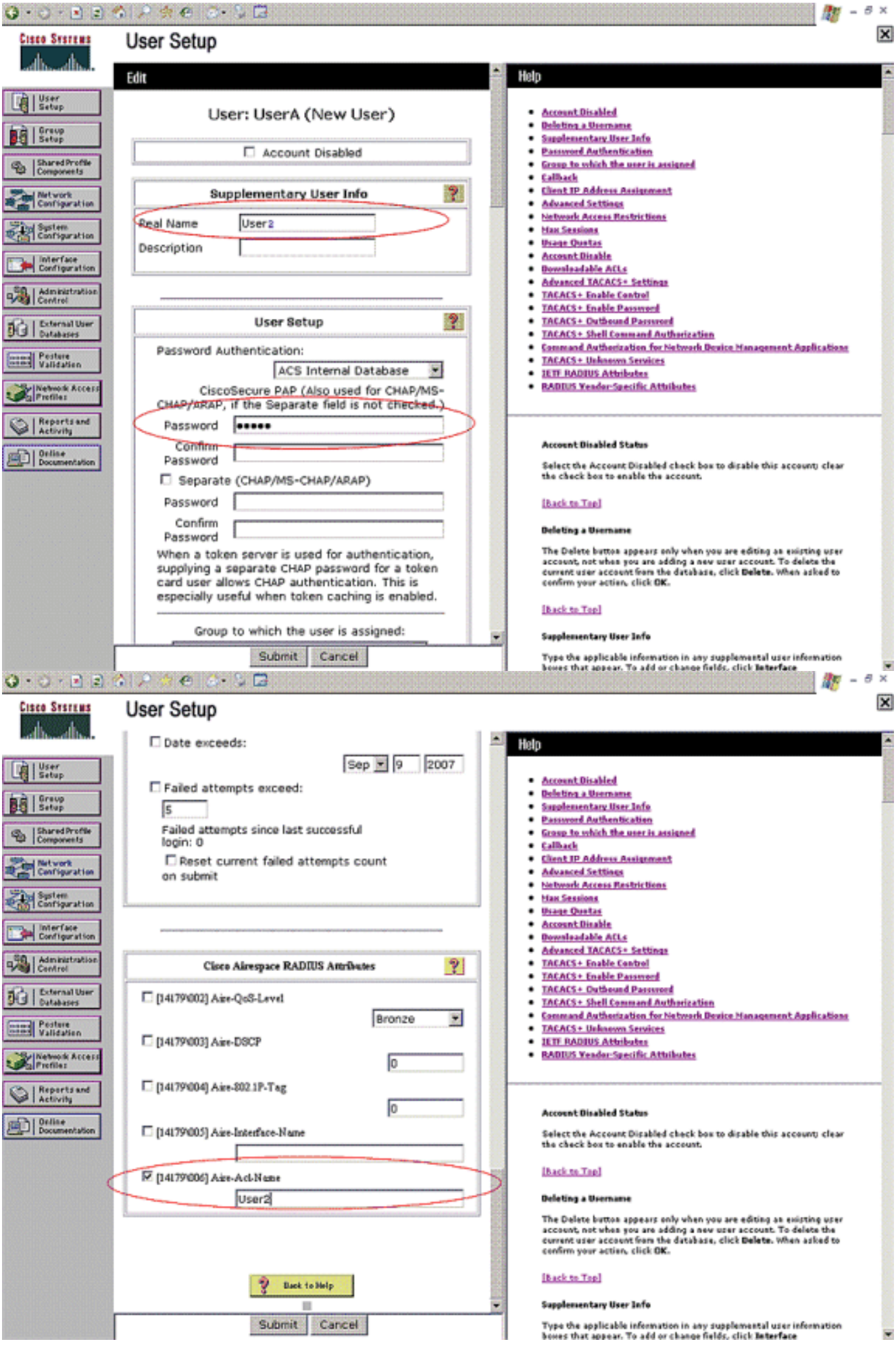


向下滾動，直到看到特定於使用者的Cisco Airespace RADIUS屬性。檢查**Aire-ACL-Name**，以使ACS能夠將ACL名稱與成功的身份驗證響應一起返回到WLC。對於User1，在WLC上建立ACL User1。輸入ACL名稱作為User1。



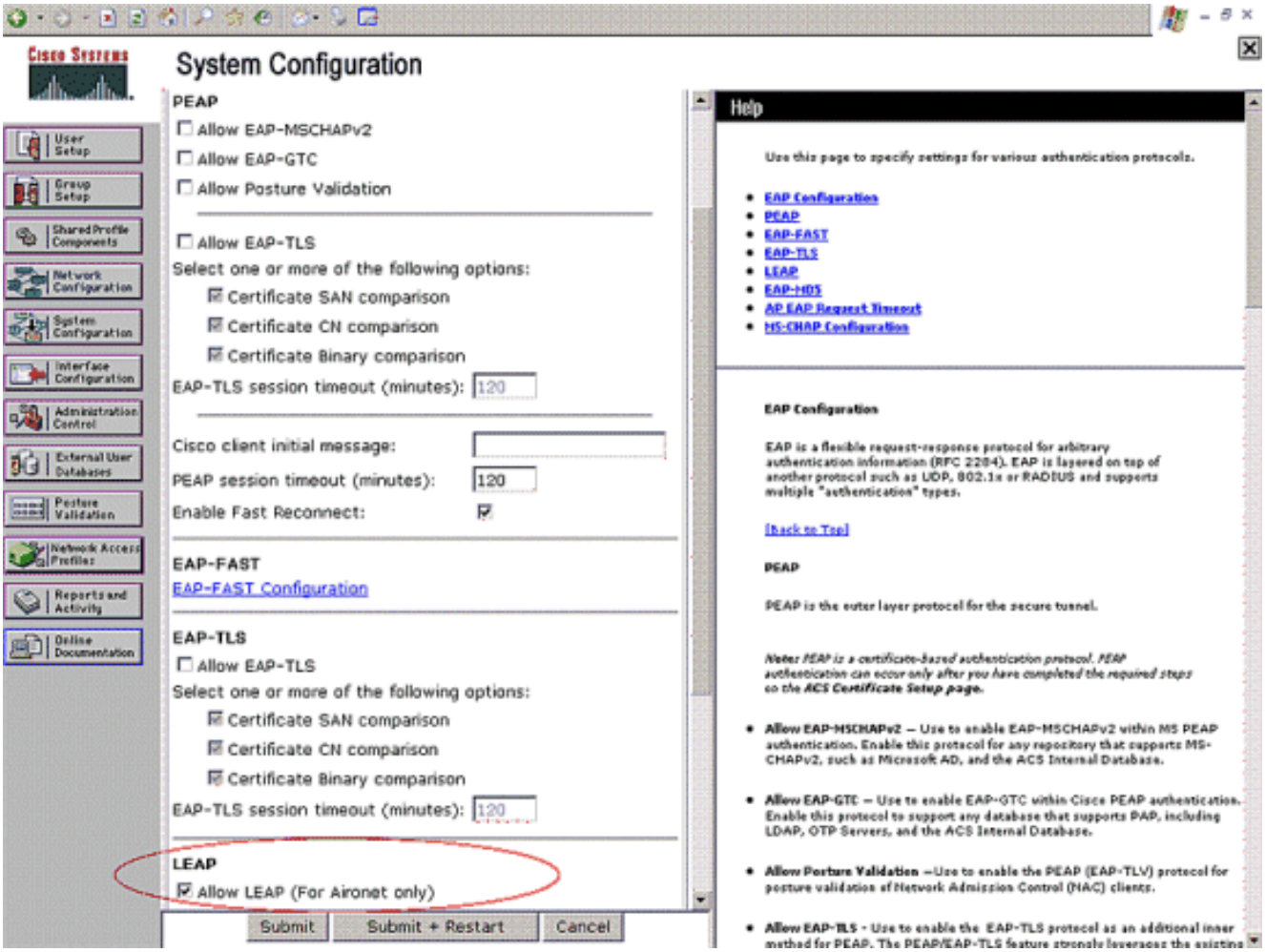
3. 重複相同步驟以建立User2，如下所示。





4. 按一下System Configuration和Global Authentication Setup以確保身份驗證伺服器配置為執行

所需的EAP身份驗證方法。在EAP配置設定下，選擇適當的EAP方法。此示例使用LEAP身份驗證。完成後按一下**Submit**。



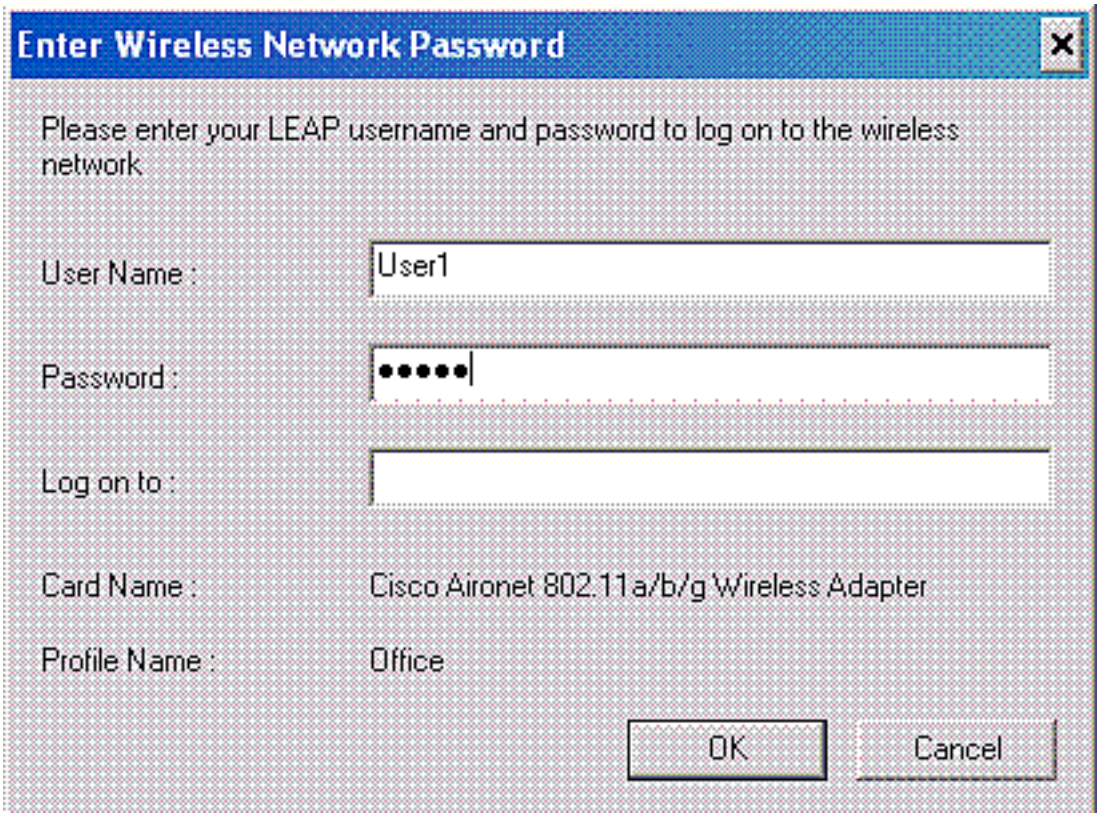
驗證

使用本節內容，確認您的組態是否正常運作。

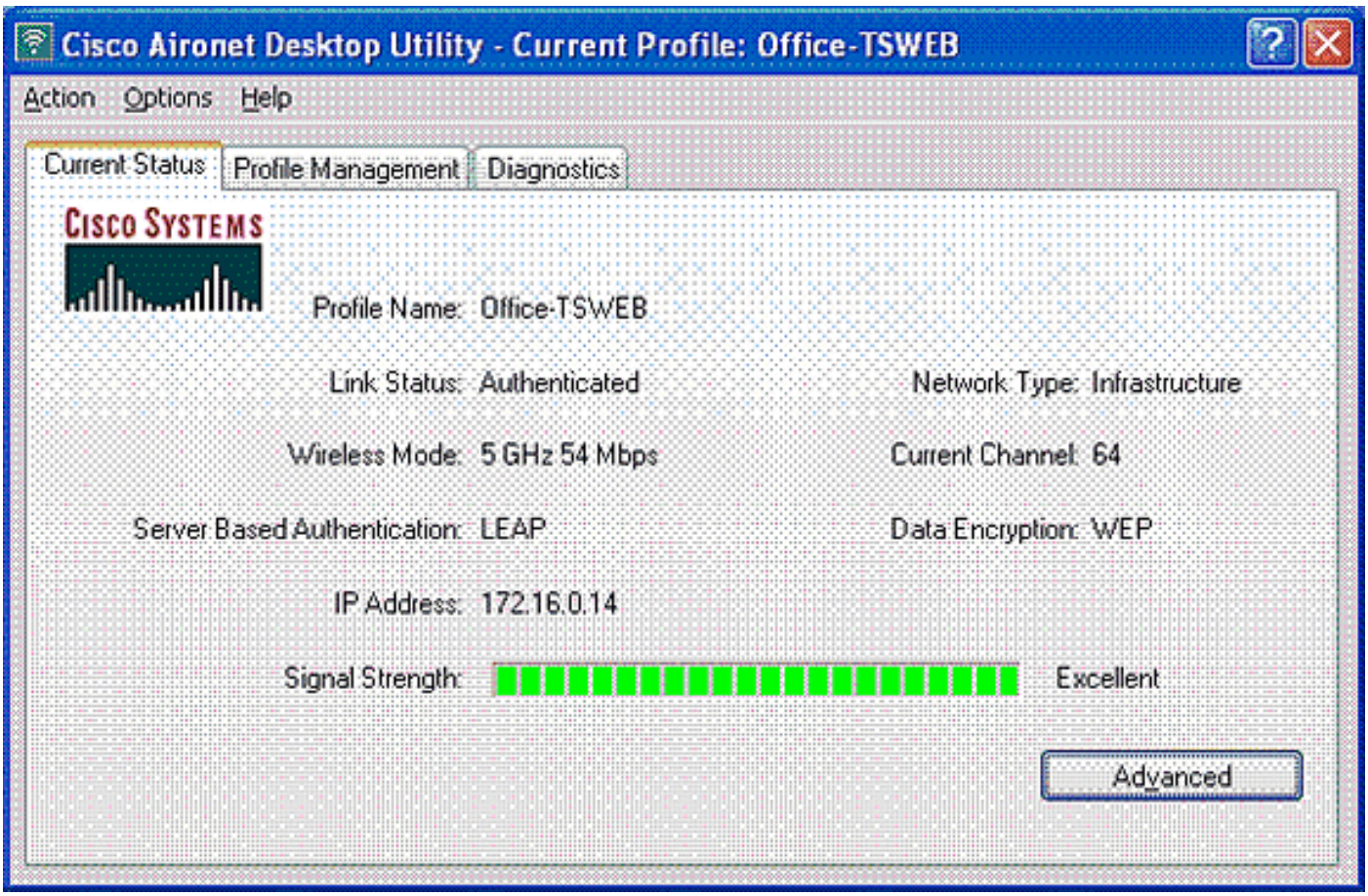
嘗試將無線客戶端與採用LEAP身份驗證的輕量AP相關聯，以驗證配置是否按預期工作。

注意：本文檔假定客戶端配置檔案已配置為LEAP身份驗證。有關如何為LEAP身份驗證配置802.11 a/b/g無線客戶端介面卡的詳細資訊，請參閱使用EAP身份驗證。

啟用無線客戶端的配置檔案後，將要求使用者提供用於LEAP身份驗證的使用者名稱/密碼。這是使用者1嘗試向LAP進行身份驗證時會發生的情況。



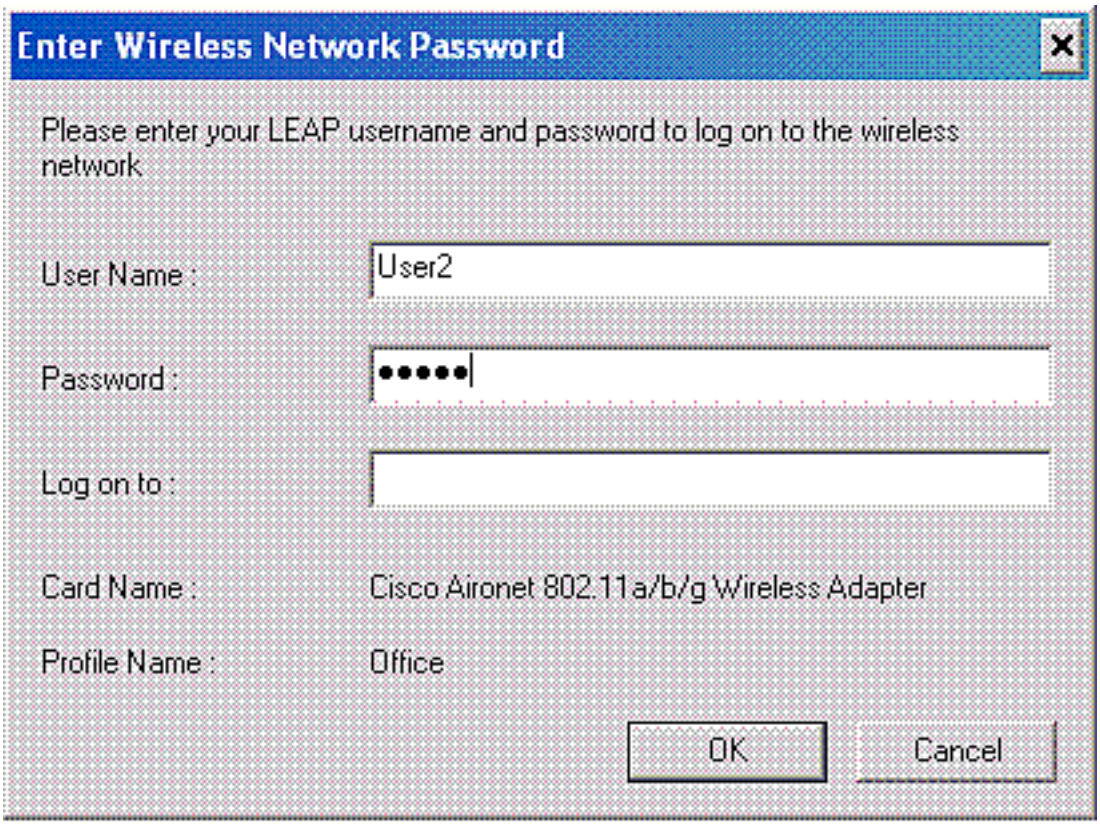
輕量AP和WLC將使用者認證傳遞到外部RADIUS伺服器(Cisco Secure ACS)以驗證認證。RADIUS伺服器會將資料與使用者資料庫進行比較，並在成功驗證後，將針對使用者設定的ACL名稱傳回WLC。在這種情況下，ACL User1會傳回WLC。

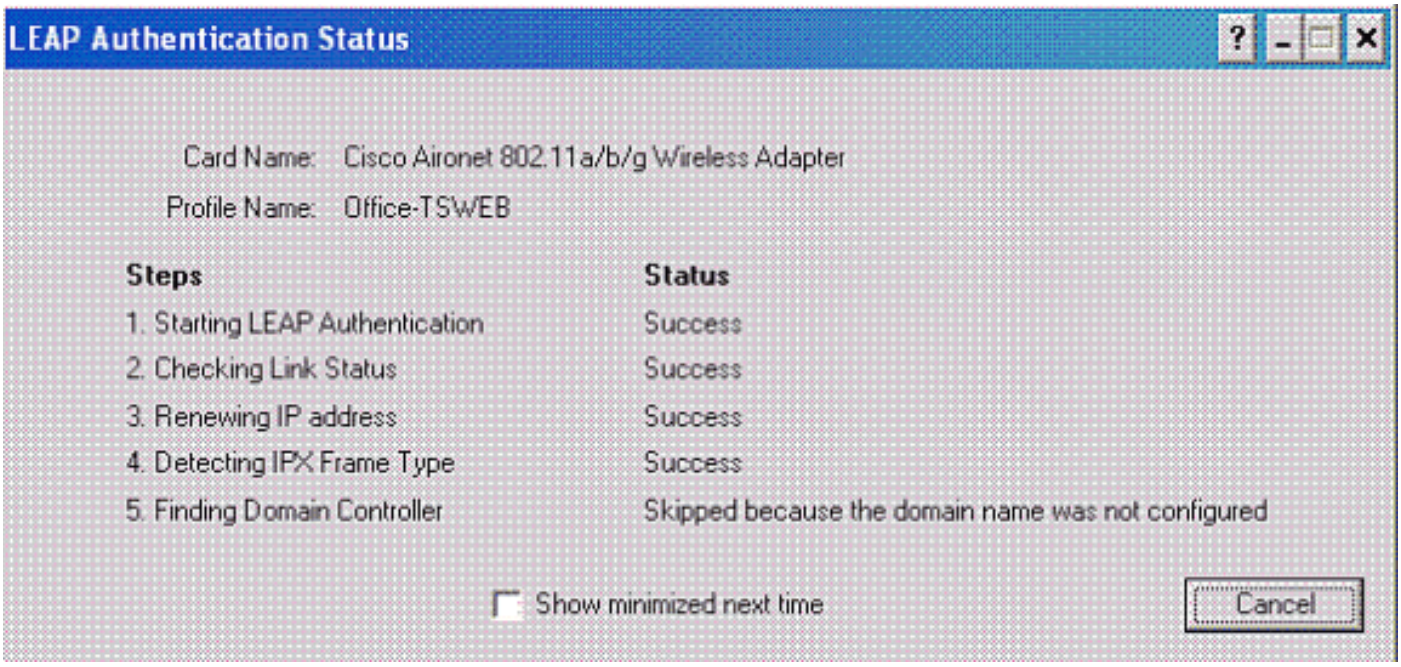


無線LAN控制器將此ACL套用到User1。此ping輸出顯示User1隻能存取伺服器172.16.1.100，不能存取任何其他裝置。

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

同樣地，當User2嘗試存取WLAN時，RADIUS伺服器會在成功驗證後將ACL User2傳回WLC。





無線LAN控制器將此ACL套用到User2。此ping輸出顯示User2僅能存取伺服器172.16.1.50，不能存取任何其他裝置。

```
D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

在無線LAN控制器上，您還可以使用這些debug命令來排除AAA身份驗證的故障

- **debug aaa all enable** — 配置所有AAA消息的調試

- **debug dot1x packet enable** — 啟用所有dot1x資料包的調試
- **debug client <MAC Address>** — 啟用無線客戶端調試

以下是**debug aaa all enable**指令的範例

註：由於空間限制，輸出中的某些行已移至第二行。

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.............0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.....0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.....00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%...........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............104
Thu Aug 16 14:42:54 2007:       resultCode..............255
Thu Aug 16 14:42:54 2007:       protocolUsed............0x00000001
Thu Aug 16 14:42:54 2007:       proxyState..............
   00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.............0x85ed228
```

```
Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.......................
   00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
```
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
```
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
   ....8....[..d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
   ...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
   ...A.....Q.20O..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
   ..........e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
   ..k........9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
   .....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
   3m.!......O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
   ......1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
   B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
   1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
   ssion-key=)..,..
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
   ..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
   ,;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
   ....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
   pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
   c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
   /9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
   ..}t......q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
```
Access-Accept received from RADIUS server
10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
```
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............236
```

```
Thu Aug 16 14:42:54 2007:       resultCode.............0
Thu Aug 16 14:42:54 2007:       protocolUsed.............0x0
0000001
Thu Aug 16 14:42:54 2007:       proxyState..............00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address.........0xffffffff (-1)
   (4 bytes)
Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message...............DATA (37 bytes)
Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.......User1 (5 bytes)
Thu Aug 16 14:42:54 2007:  AVP[05] Class.....................CACS:0/9/a4df4d2/1
   (18 bytes)
Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator......DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
   for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
   for station 00:40:96:af:3e:93
               source: 4, valid bits: 0x400
         qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                    vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
   Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

您可以使用**show wlan summary**指令的組合來識別哪個WLAN使用RADIUS伺服器驗證。然後您可以檢視**show client summary**命令，以瞭解哪些MAC位址（使用者端）在RADIUS WLAN上成功通過驗證。您還可以將此項與Cisco Secure ACS已通過的嘗試或失敗的嘗試日誌關聯。

思科建議您使用無線客戶端測試ACL配置，以確保已正確配置ACL。如果無法正常工作，請驗證ACL網頁上的ACL，並驗證您的ACL更改是否已應用到控制器的介面。

您還可以使用以下show命令來驗證您的設定：

- **show acl summary** — 若要顯示控制器上配置的ACL，請使用**show acl summary命**令。

以下是範例：

```
(Cisco Controller) >show acl summary

ACL Name                          Applied
------------------------------- -------
User1                                Yes
User2                                Yes
```

- **show acl detailed** <ACL_Name> — 顯示有關已配置ACL的詳細資訊。以下是範例：**註：**由於空間限制，輸出中的某些行已移至第二行。

```
Cisco Controller) >show acl detailed User1

                    Source                        Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP   Action
-- --- ------------------------------ ------------------------------
   ---- ---------- ---------- ----    ------
```

```
 1  In      172.16.0.0/255.255.0.0        172.16.1.100/255.255.255.255
   Any  0-65535       0-65535   Any    Permit
 2 Out    172.16.1.100/255.255.255.255      172.16.0.0/255.255.0.0
   Any  0-65535       0-65535   Any    Permit


(Cisco Controller) >show acl detailed User2

                   Source                      Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot    Range       Range    DSCP Action
-- --- ------------------------------ ------------------------------
   ---- ----------- ----------- ---- ------
1  In      172.16.0.0/255.255.0.0         172.16.1.50/255.255.255.255
   Any   0-65535       0-65535    Any  Permit
2 Out     172.16.1.50/255.255.255.255      172.16.0.0/255.255.0.0
   Any   0-65535       0-65535    Any  Permit
```

- **show client detail** <MAC Address of the client> — 顯示有關無線客戶端的詳細資訊。

疑難排解提示

使用以下提示進行疑難排解：

- 在控制器上驗證RADIUS伺服器是否處於活動狀態，而不是待機或禁用。
- 在控制器上，檢查是否從WLAN(SSID)下拉選單選擇RADIUS伺服器。
- 檢查RADIUS伺服器是否收到並驗證來自無線使用者端的驗證要求。
- 檢查ACS伺服器上的Passed Authentications and Failed Attempts報告以完成此操作。這些報告可在ACS伺服器的「報告和活動」下找到。

相關資訊

- 無線LAN控制器上的ACL:規則、限制和示例
- 無線LAN控制器上的ACL組態範例
- 使用無線LAN控制器(WLC)的MAC過濾器組態範例
- 思科無線LAN控制器組態設定指南5.2版
- 技術支援與文件 - Cisco Systems