思科統一無線網路中的Wi-Fi保護訪問(WPA)配置示例

目錄

簡介

本文檔介紹如何在思科統一無線網路中配置Wi-Fi保護訪問(WPA)。

必要條件

需求

嘗試此組態之前，請確認您已瞭解以下主題的基本知識：

- WPA
- 無線區域網路(WLAN)安全解決方案**註：有關**Cisco WLAN安全解決方案的資訊，請參閱Cisco無線LAN安全概述。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 1000系列輕量型存取點(LAP)
- 執行韌體4.2.61.0的Cisco 4404無線LAN控制器(WLC)

- 運行韌體4.1的Cisco 802.11a/b/g客戶端介面卡
- 運行韌體4.1的Aironet案頭實用程式(ADU)
- Cisco安全ACS伺服器版本4.1

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。

WPA和WPA2支援

思科統一無線網路包括對Wi-Fi聯盟認證WPA和WPA2的支援。WPA於2003年由Wi-Fi聯盟推出。WPA2於2004年由Wi-Fi聯盟推出。所有針對WPA2的Wi-Fi認證產品都必須與針對WPA的Wi-Fi認證產品互操作。

WPA和WPA2為終端使用者和網路管理員提供了高級別保證，確保他們的資料將保持私有狀態，而且對其網路的訪問將限制在授權使用者範圍內。兩者都有個人和企業運營模式，可滿足兩個市場細分的獨特需求。每個的企業模式使用IEEE 802.1X和EAP進行身份驗證。每個的個人模式使用預共用金鑰(PSK)進行身份驗證。思科不建議對商業或政府部署使用個人模式，因為它使用PSK進行使用者身份驗證。PSK對企業環境不安全。

WPA解決了原始IEEE 802.11安全實施中存在的所有已知WEP漏洞，為企業和小型辦公室/家庭辦公室(SOHO)環境中的WLAN提供了即時安全解決方案。WPA使用TKIP進行加密。

WPA2是下一代Wi-Fi安全性。它是Wi-Fi聯盟對已批准的IEEE 802.11i標準的互操作性實施。它採用帶密碼塊鏈結消息驗證碼協定(CCMP)的計數器模式，實現了美國國家標準技術研究所(NIST)推薦的AES加密演算法。WPA2促進政府FIPS 140-2合規性。

WPA和WPA2模式型別的比較

	WPA	WPA2
企業模式（企業、政府、教育）	• 身份驗證：IEEE 802.1X/EAP • 加密：TKIP/MIC	• 身份驗證：IEEE 802.1X/EAP • 加密：AES-CCMP
個人模式（SOHO、家庭/個人）	• 身份驗證：PSK • 加密：TKIP/MIC	• 身份驗證：PSK • 加密：AES-CCMP

在企業操作模式下，WPA和WPA2都使用802.1X/EAP進行身份驗證。802.1X為WLAN提供客戶端和身份驗證伺服器之間的強式相互身份驗證。此外，802.1X還提供每使用者、每會話的動態加密金鑰，從而消除了靜態加密金鑰的管理負擔和安全問題。

在802.1X中，用於身份驗證的憑證（如登入密碼）永遠不會通過無線介質以明文傳輸或未經加密。

儘管802.1X身份驗證型別為無線LAN提供強身份驗證，但除802.1X外，加密還需要TKIP或AES，因為標準802.11 WEP加密容易受到網路攻擊。

有幾種802.1X身份驗證型別，每種型別都提供不同的身份驗證方法，同時依賴相同的框架和EAP在客戶端和接入點之間進行通訊。Cisco Aironet產品支援的802.1X EAP身份驗證型別比任何其他WLAN產品都多。支援的型別包括：

- Cisco LEAP
- EAP — 通過安全隧道的靈活身份驗證(EAP-FAST)
- EAP — 傳輸層安全(EAP-TLS)
- 受保護的可擴充驗證通訊協定(PEAP)
- EAP — 隧道TLS(EAP-TTLS)
- EAP-Subscriber Identity Module(EAP-SIM)

802.1X身份驗證的另一個好處是集中管理WLAN使用者組，包括基於策略的金鑰輪替、動態金鑰分配、動態VLAN分配和SSID限制。這些功能可旋轉加密金鑰。

在個人操作模式下，預共用金鑰（密碼）用於身份驗證。個人模式只需要接入點和客戶端裝置，而企業模式通常需要網路上的RADIUS或其他身份驗證伺服器。

本文檔提供在思科統一無線網路中配置WPA2（企業模式）和WPA2-PSK（個人模式）的示例。

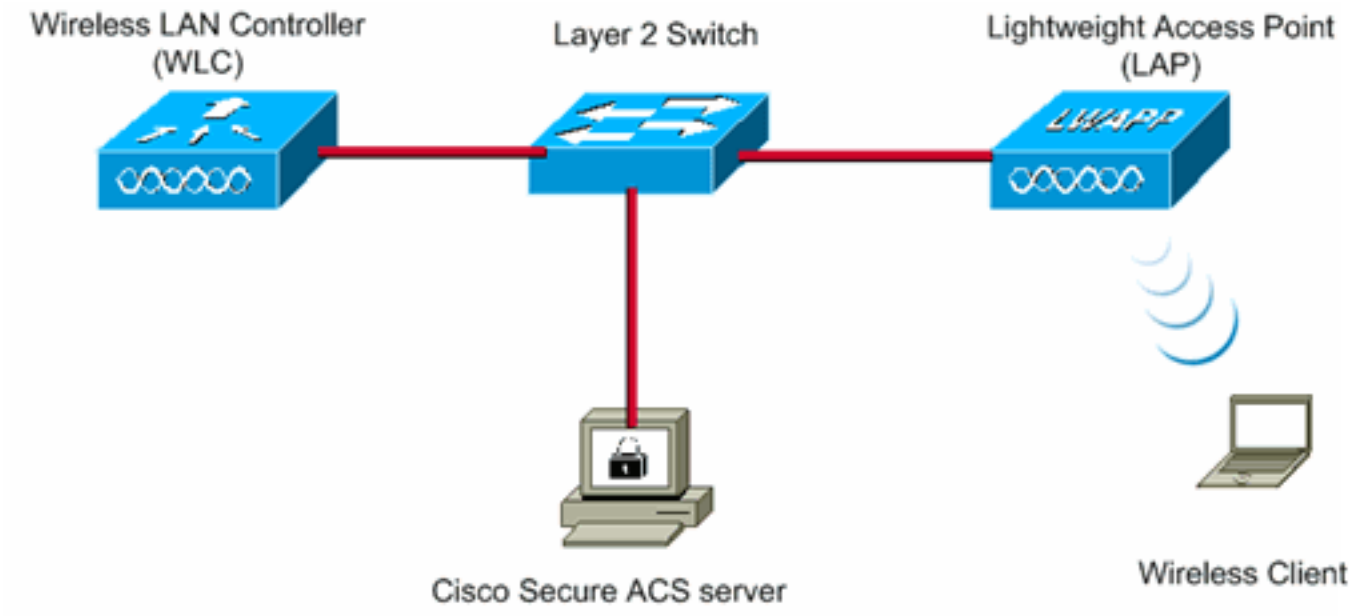
網路設定

在此設定中，Cisco 4404 WLC和Cisco 1000系列LAP通過第2層交換機連線。外部RADIUS伺服器(Cisco Secure ACS)也連線到同一交換器。所有裝置都位於同一個子網中。存取點(LAP)初始註冊到控制器。需要建立兩個無線LAN，一個用於WPA2企業模式，另一個用於WPA2個人模式。

WPA2-Enterprise模式WLAN(SSID: WPA2-Enterprise)將使用EAP-FAST對無線客戶端進行身份驗證，使用AES進行加密。Cisco Secure ACS伺服器將用作外部RADIUS伺服器，用於驗證無線客戶端。

WPA2 — 個人模式WLAN(SSID: WPA2-PSK)將使用WPA2-PSK使用預共用金鑰「abcdefghijk」進行身份驗證。

您需要為此設定配置裝置：



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

為WPA2企業模式配置裝置

本節提供用於設定本文件中所述功能的資訊。

執行以下步驟，將裝置配置為WPA2企業運行模式：

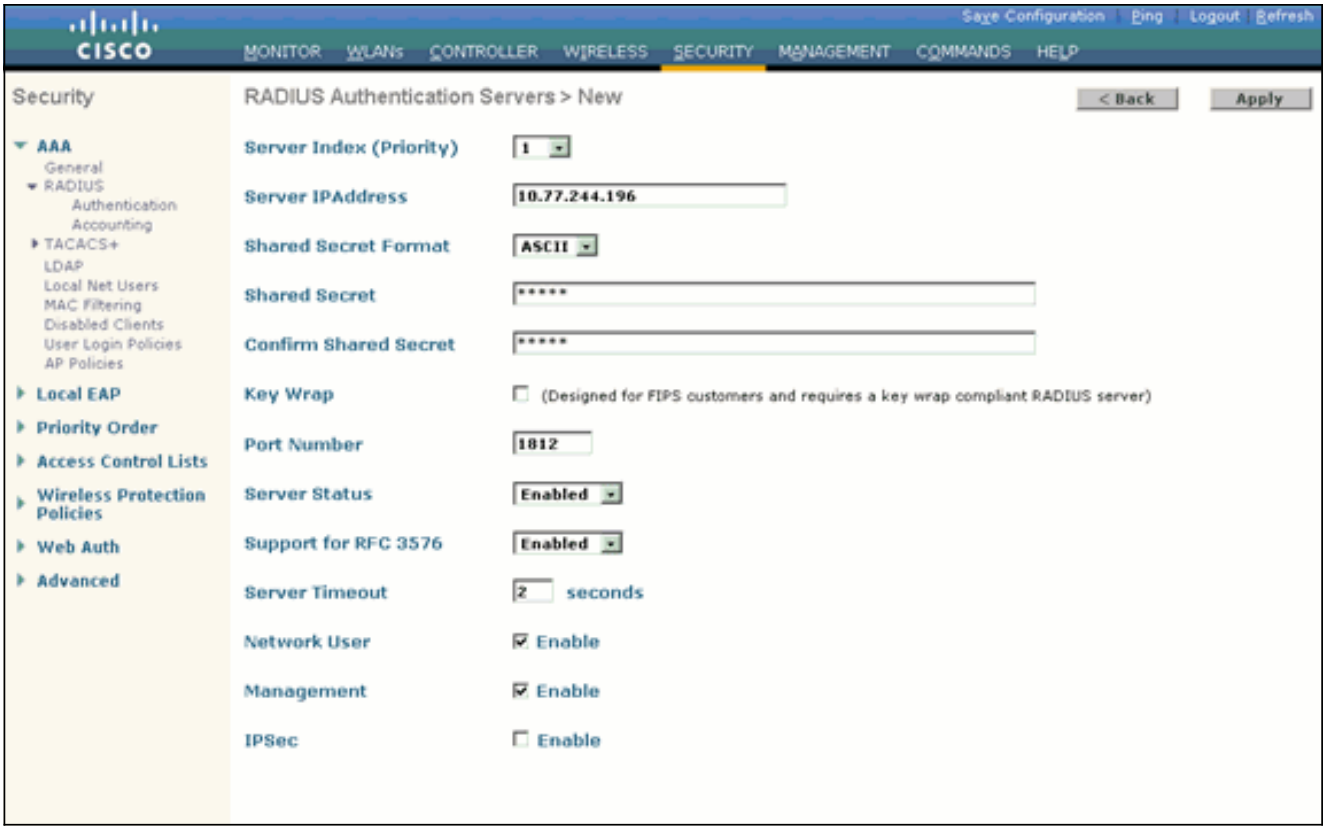
1. 設定WLC以透過外部RADIUS伺服器進行RADIUS驗證
2. 為WPA2企業模式身份驗證(EAP-FAST)配置WLAN
3. 為WPA2企業模式配置無線客戶端

設定WLC以透過外部RADIUS伺服器進行RADIUS驗證

需要設定WLC，才能將使用者認證轉送到外部RADIUS伺服器。外部RADIUS伺服器然後使用EAP-FAST驗證使用者認證並提供對無線使用者端的存取。

完成以下步驟，設定外部RADIUS伺服器的WLC:

1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**，以顯示「RADIUS Authentication Servers」頁面。接下來，按一下**New**以定義RADIUS伺服器。
2. 在**RADIUS Authentication Servers > New**頁面上**定義RADIUS伺服器**引數。這些引數包括：RADIUS伺服器IP位址共用金鑰連線埠號碼伺服器狀態本文檔使用IP地址為10.77.244.196的ACS伺服器。



3. 按一下「**Apply**」。

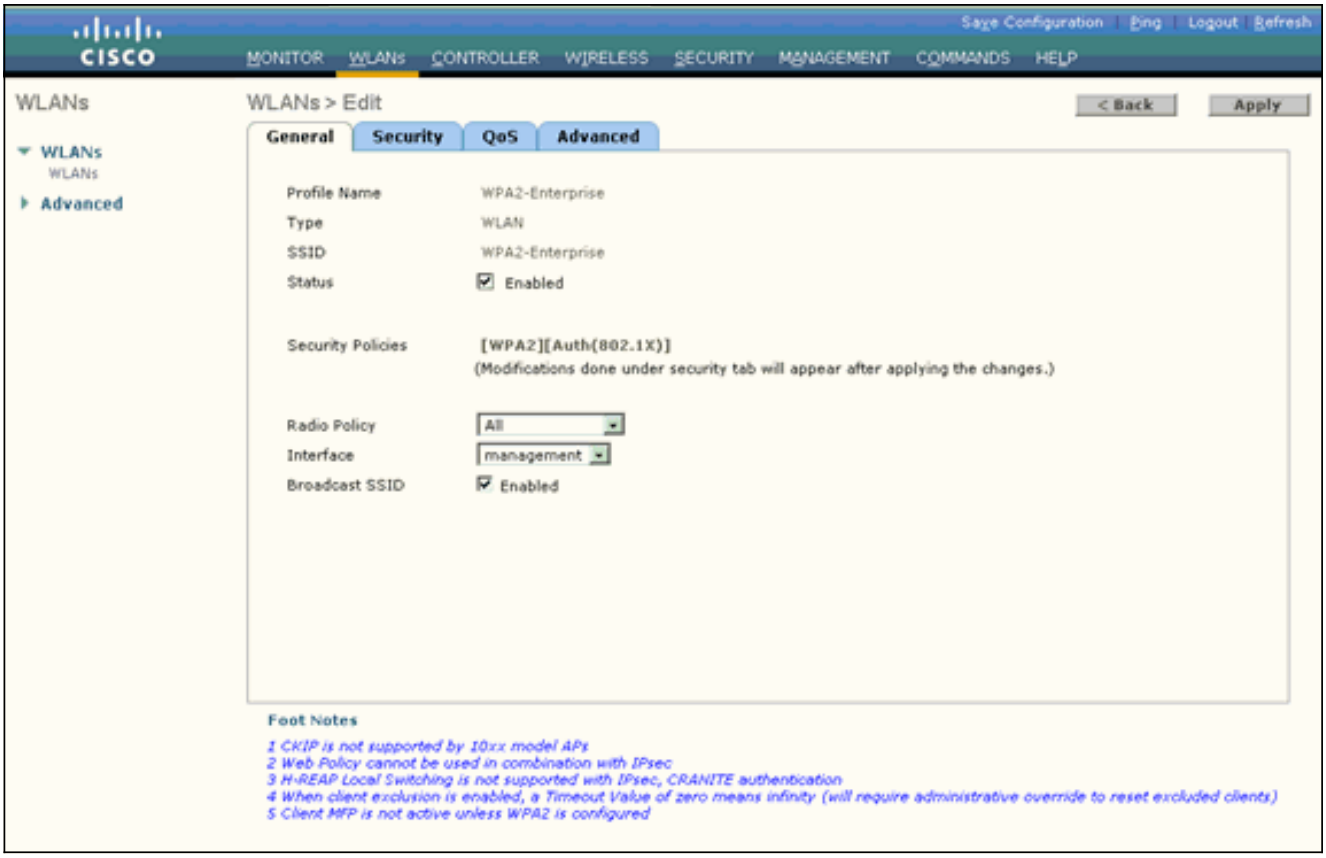
為WPA2企業操作模式配置WLAN

接下來，設定使用者端用來連線無線網路的WLAN。WPA2企業模式的WLAN SSID將為WPA2 — 企業。此範例將此WLAN指派給管理介面。

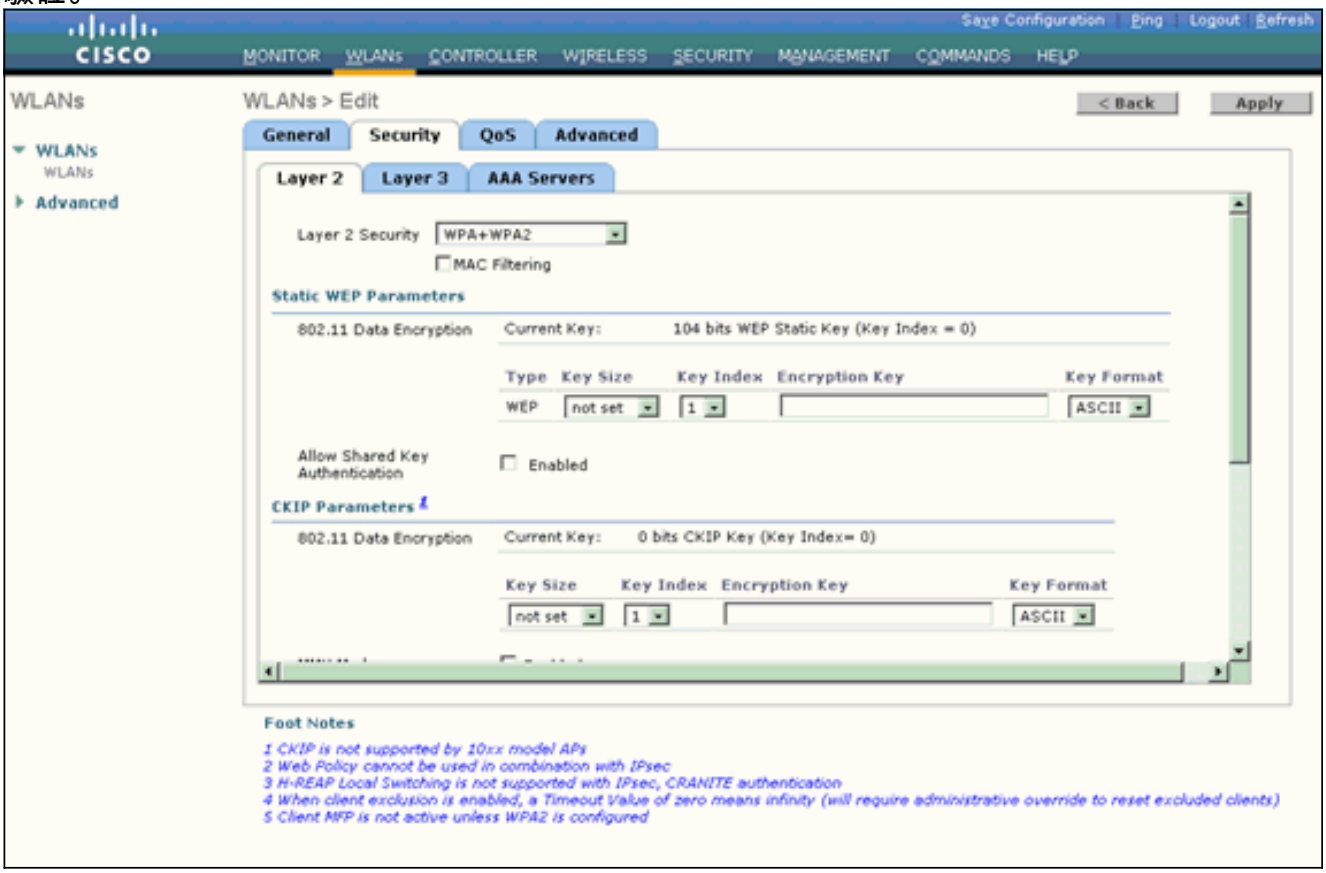
完成以下步驟即可設定WLAN及其相關引數：

1. 從控制器的GUI中按一下「**WLANs**」，以顯示「WLANs」頁面。此頁面列出控制器上存在的WLAN。
2. 按一下**New**以建立一個新的WLAN。
3. 在**WLANs > New**頁面上輸入WLAN SSID名稱和Profile名稱。然後，按一下「**Apply**」。本示例使用**WPA2-Enterprise**作為SSID。

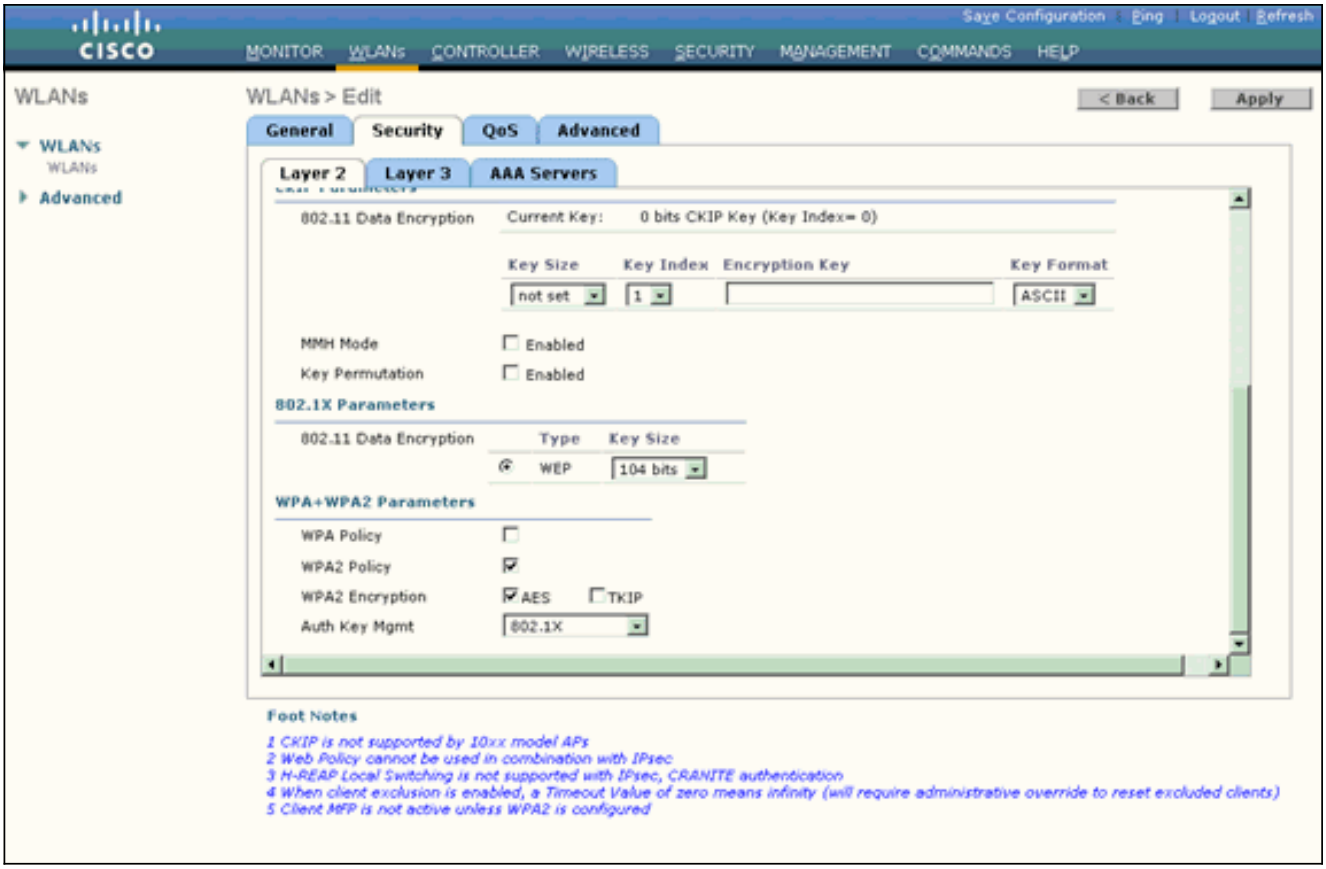
4. 建立新的WLAN後，系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上，您可以定義此WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和高級引數。
5. 在General Policies下，勾選**Status**覈取方塊以啟用WLAN。



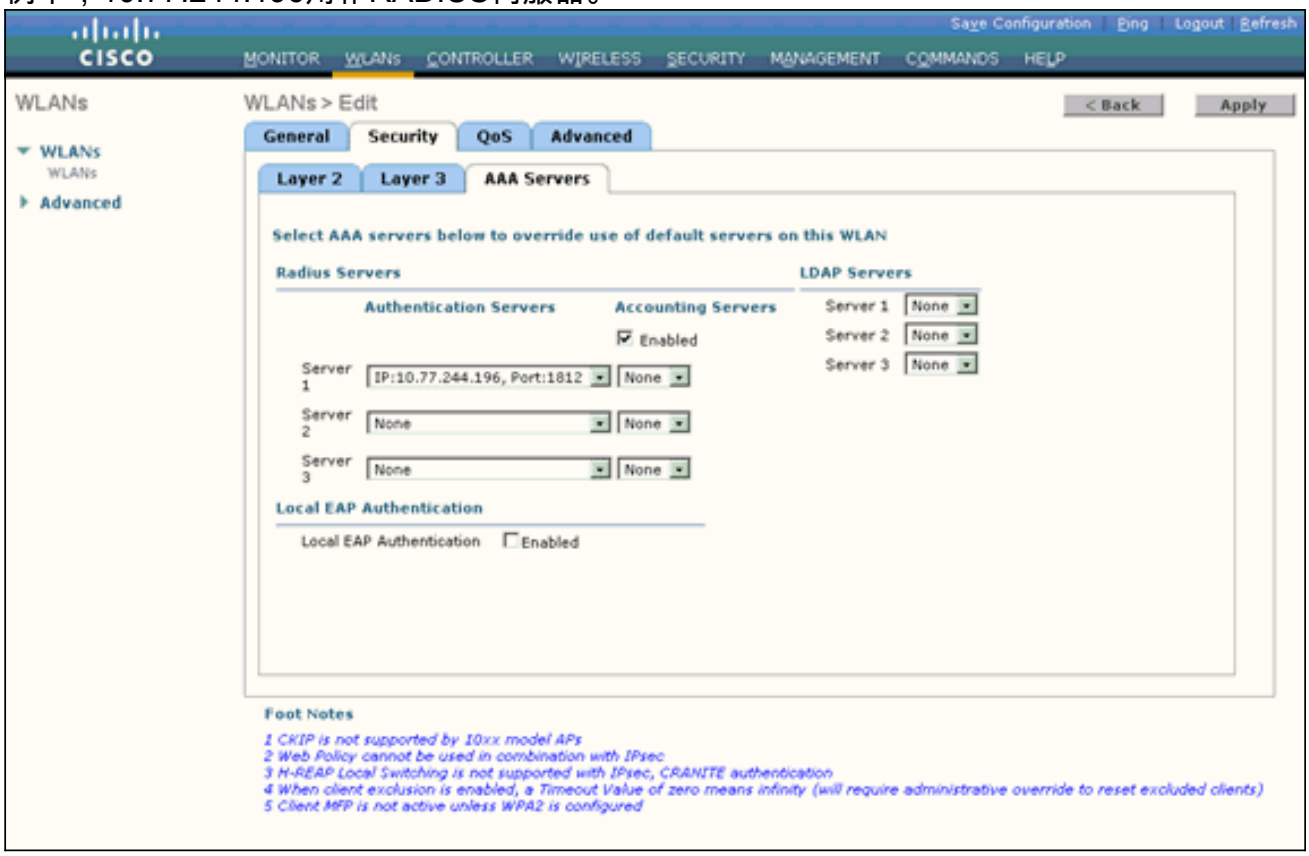
6. 如果您希望AP在其信標幀中廣播SSID，請選中**Broadcast SSID**覈取方塊。
7. 按一下**Security**頁籤。在Layer 2 Security下，選擇**WPA+WPA2**。這將為WLAN啟用WPA身份驗證。



8. 向下滾動頁面以修改**WPA+WPA2引數**。在此示例中，選擇了WPA2策略和AES加密。



9. 在Auth Key Mgmt下，選擇**802.1x**。這將為WLAN啟用使用802.1x/EAP身份驗證和AES加密的WPA2。
10. 按一下**AAA Servers**頁籤。在Authentication Servers下，選擇適當的伺服器IP地址。在本示例中，10.77.244.196用作RADIUS伺服器。



11. 按一下「**Apply**」。**注意**：這是需要在控制器上為EAP身份驗證配置的唯一EAP設定。EAP-FAST的所有其他特定配置需要在RADIUS伺服器和需要身份驗證的客戶端上完成。

為WPA2企業模式身份驗證(EAP-FAST)配置RADIUS伺服器

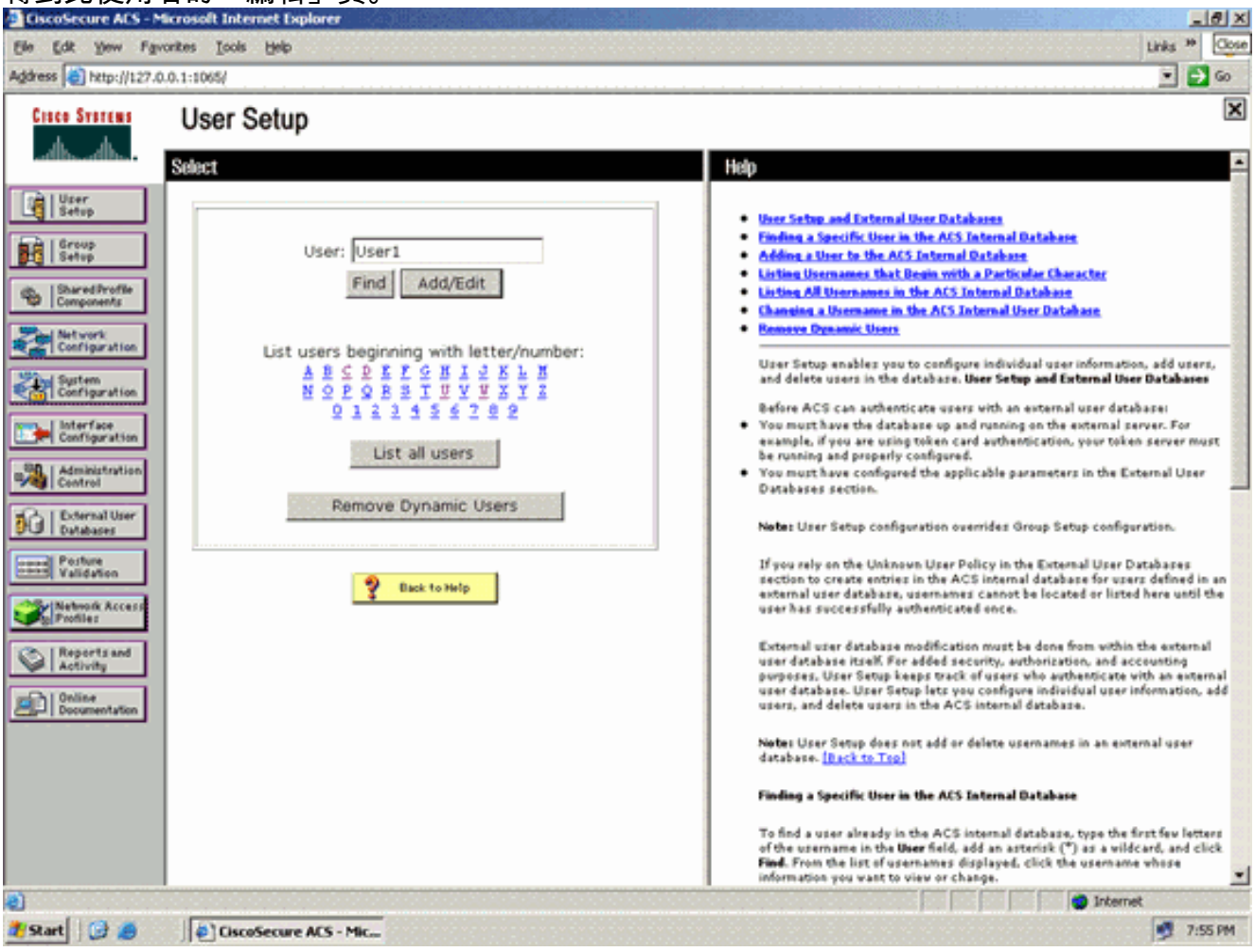
在本示例中，Cisco Secure ACS用作外部RADIUS伺服器。執行以下步驟以配置RADIUS伺服器進行EAP-FAST身份驗證：

1. 建立使用者資料庫以驗證客戶端
2. 將WLC作為AAA使用者端新增到RADIUS伺服器
3. 使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證**注意**：EAP-FAST可以使用匿名帶內PAC調配或經過身份驗證的帶內PAC調配進行配置。此示例使用匿名帶內PAC調配。有關使用匿名帶內PAC調配和經過身份驗證的帶內調配配置EAP FAST的詳細資訊和示例，請參閱使用無線LAN控制器和外部RADIUS伺服器配置EAP-FAST的示例。

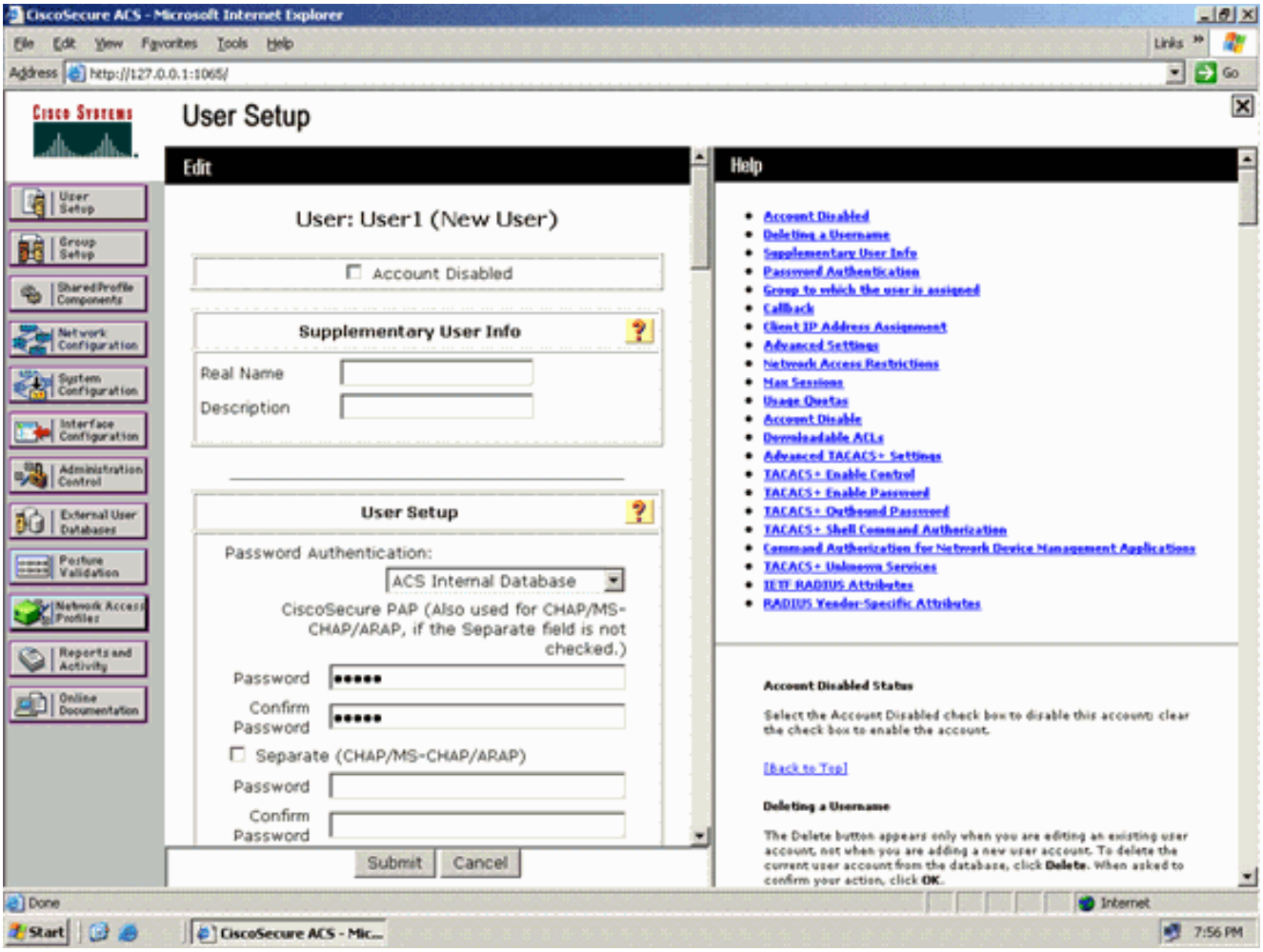
建立使用者資料庫以驗證EAP-FAST客戶端

完成以下步驟，以便為ACS上的EAP-FAST客戶端建立使用者資料庫。此示例將EAP-FAST客戶端的使用者名稱和密碼分別配置為User1和User1。

1. 從導航欄中的ACS GUI中選擇**User Setup**。建立一個新的無線使用者，然後按一下**Add/Edit**以轉到此使用者的「編輯」頁。



2. 在User Setup Edit頁中，配置真實名稱和說明以及口令設定，如本例所示。本文檔使用**ACS內部資料庫**進行口令驗證。

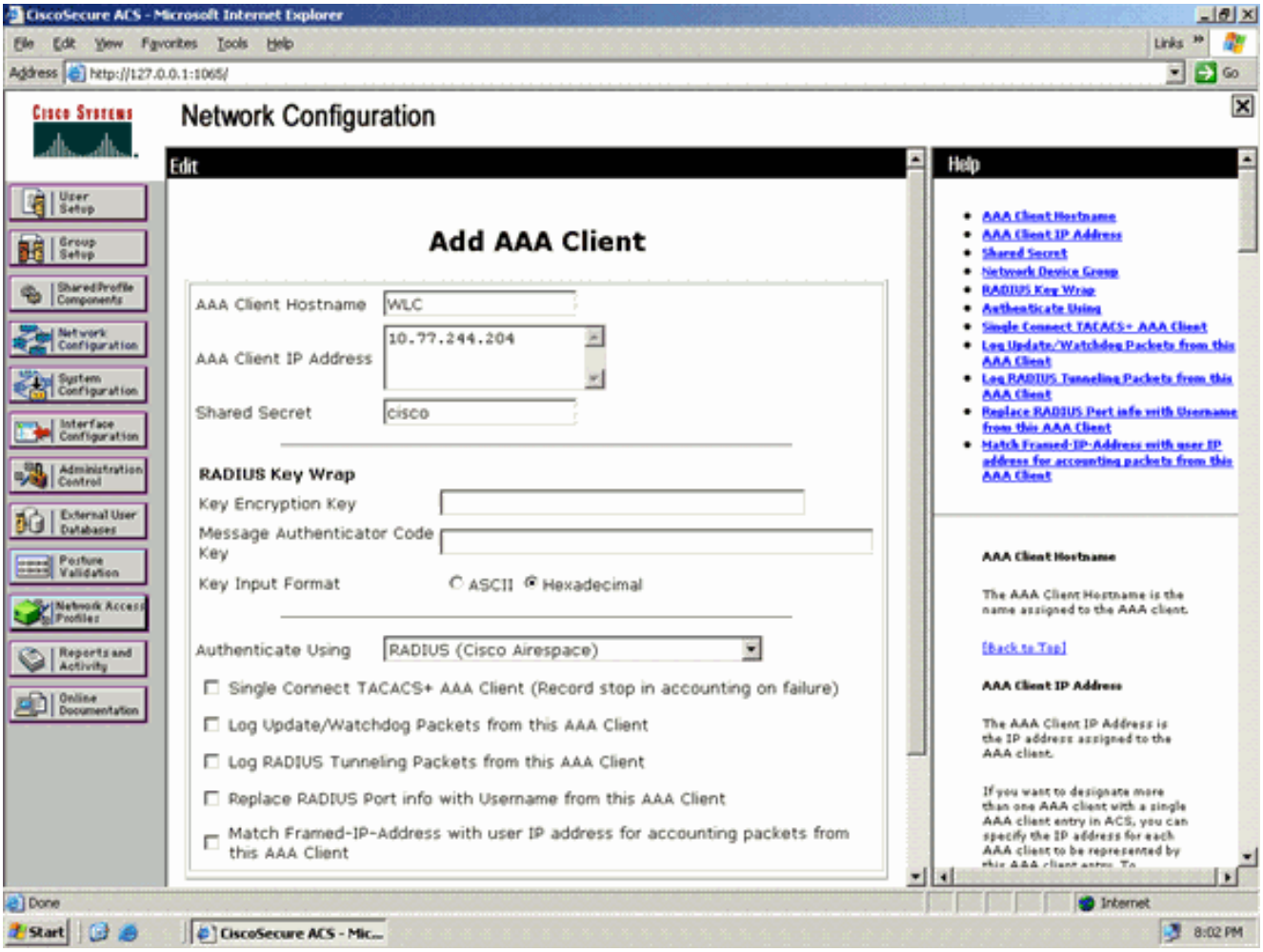


3. 從Password Authentication下拉框中選擇**ACS Internal Database**。
4. 配置所有其他所需的引數，然後按一下**Submit**。

將WLC作為AAA使用者端新增到RADIUS伺服器

完成以下步驟，即可將控制器定義為ACS伺服器上的AAA使用者端：

1. 在ACS GUI上按一下**Network Configuration**。在「Network Configuration」頁面的「Add AAA client」部分下，按一下**Add Entry**，將WLC作為AAA客戶端新增到RADIUS伺服器。
2. 在AAA使用者端頁面中，定義WLC的名稱、IP位址、共用密碼和驗證方法(RADIUS/Cisco Airespace)。請參閱製造商提供的文檔，瞭解其它非ACS身份驗證伺服器。



注意：您在WLC和ACS伺服器上配置的共用金鑰必須匹配。共用金鑰區分大小寫。

3. 按一下「**Submit+Apply**」。

使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證

匿名帶內調配

這是兩種帶內調配方法之一，其中ACS與終端使用者客戶端建立安全連線，以便為客戶端提供新的PAC。此選項允許在終端使用者客戶端和ACS之間匿名的TLS握手。

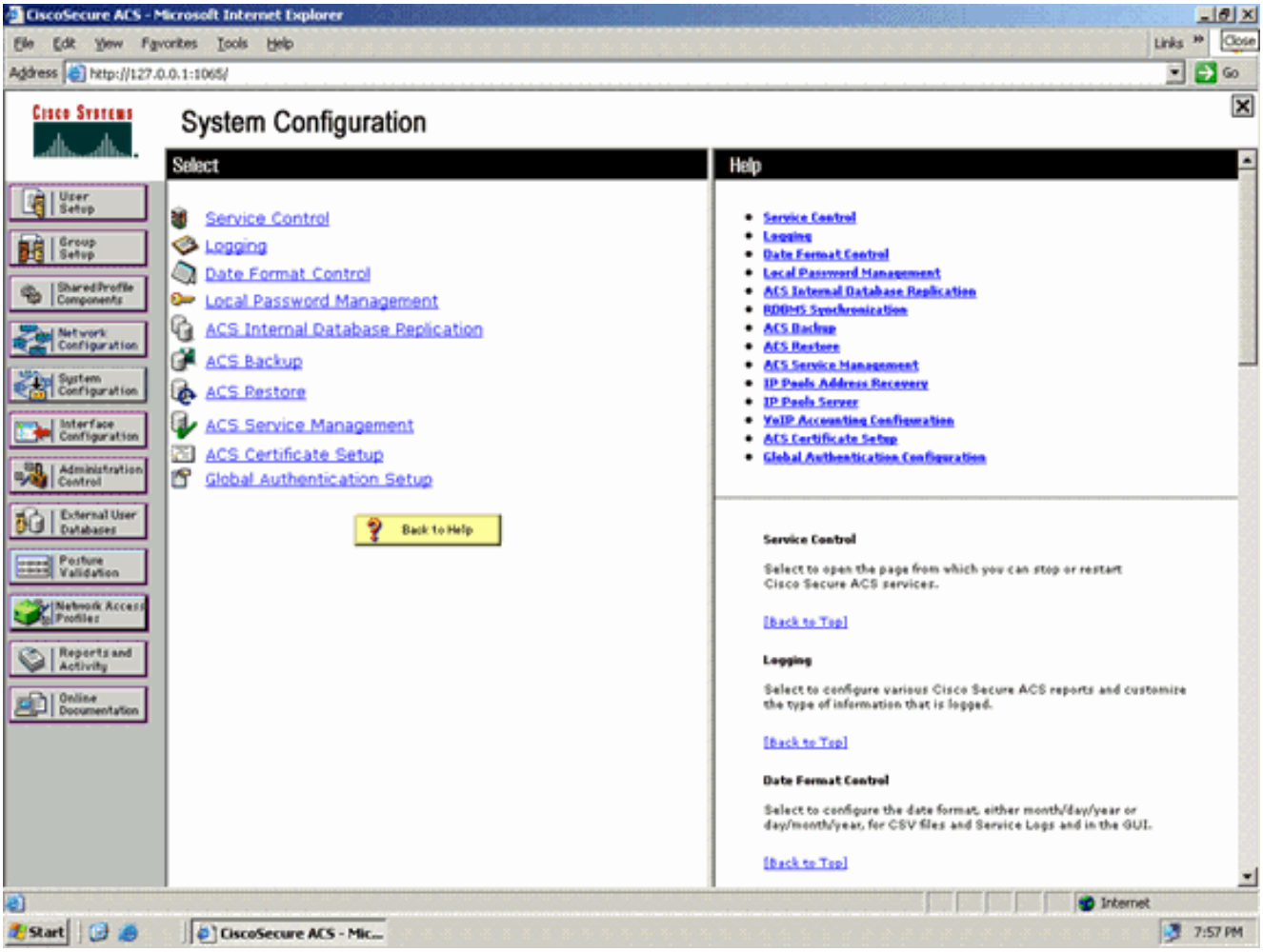
此方法在對等體驗證ACS伺服器之前，在經過身份驗證的Diffie-Hellman金鑰協定協定(ADHP)隧道內運行。

然後，ACS要求使用者的EAP-MS-CHAPv2身份驗證。成功進行使用者身份驗證後，ACS會與終端使用者客戶端建立Diffie-Hellman隧道。ACS為該使用者生成一個PAC，並將該PAC連同該ACS的資訊一起傳送到此隧道中的終端使用者客戶端。此調配方法使用EAP-MSCHAPv2作為零階段的身份驗證方法，使用EAP-GTC作為第二階段的身份驗證方法。

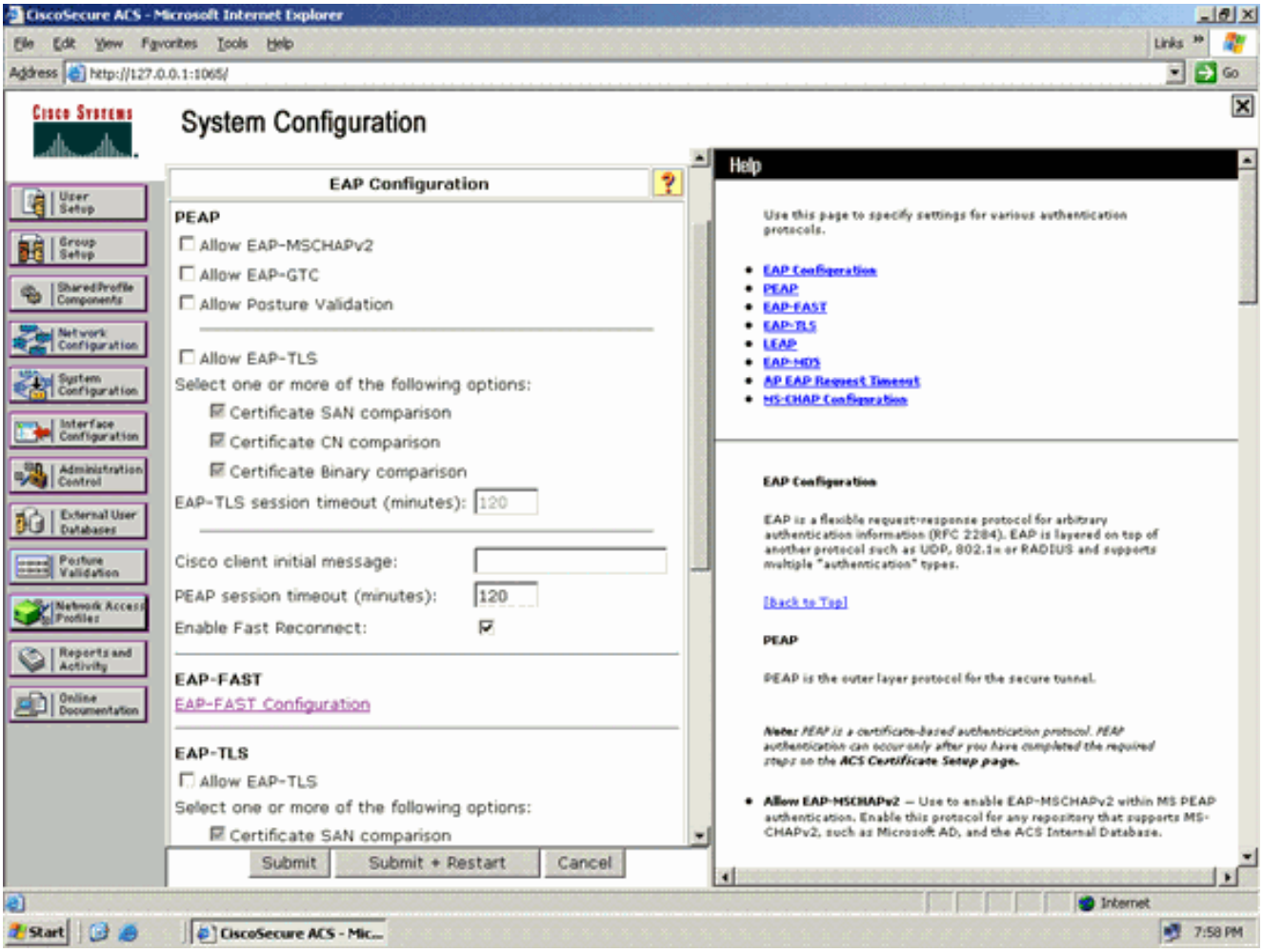
由於設定了未經身份驗證的伺服器，因此無法使用純文字檔案密碼。因此，隧道內只能使用MS-CHAP憑據。MS-CHAPv2用於證明對等體的身份，並為進一步的身份驗證會話接收PAC（EAP-MS-CHAP將僅用作內部方法）。

完成以下步驟，以便在RADIUS伺服器中配置用於匿名帶內調配的EAP-FAST身份驗證：

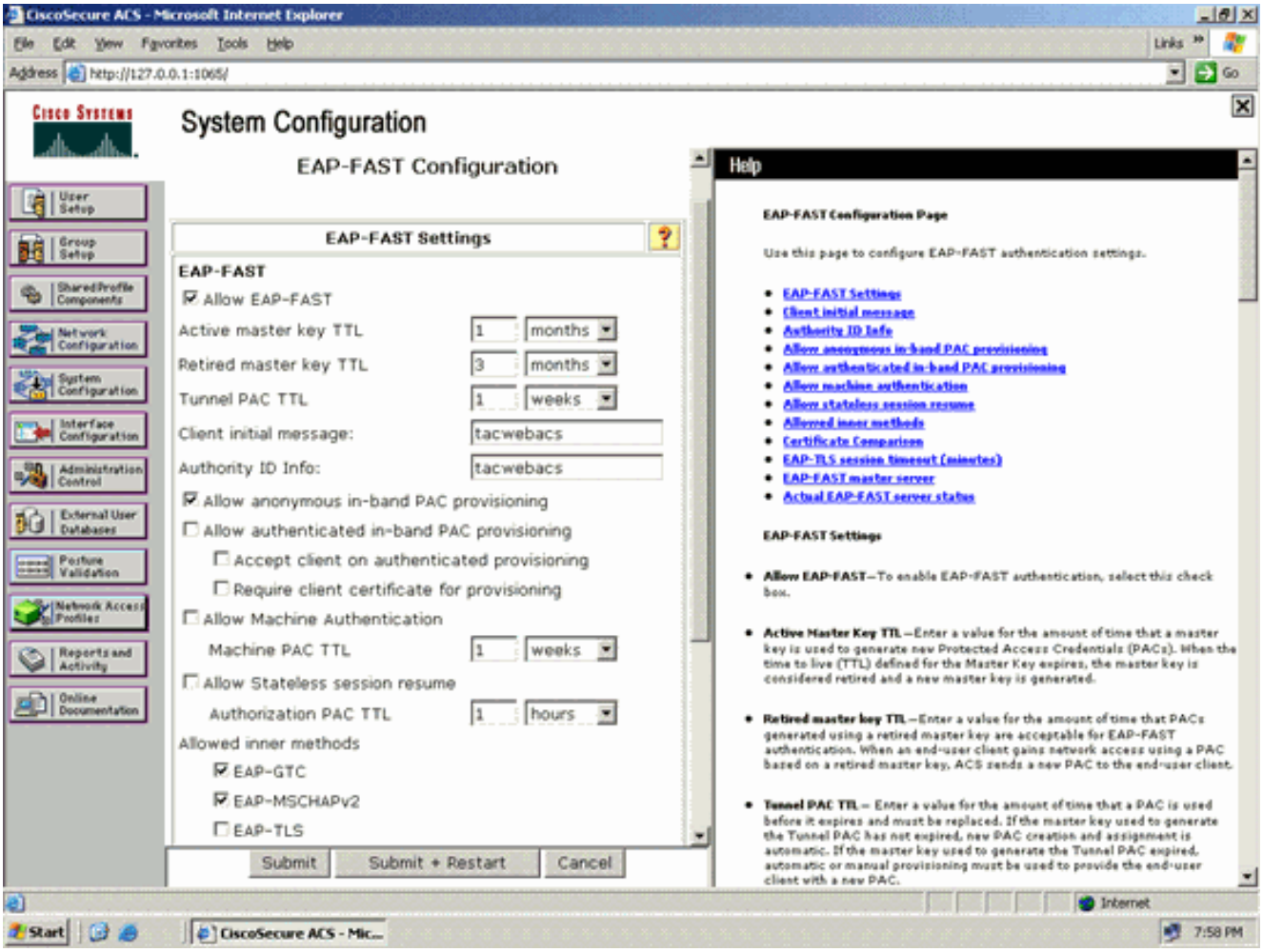
1. 在RADIUS伺服器GUI上按一下**System Configuration**。在System Configuration頁面中，選擇**Global Authentication Setup**。



2. 在Global Authentication setup頁中，按一下**EAP-FAST Configuration**以轉到EAP-FAST設定頁。



3. 在EAP-FAST設定頁面中，選中**Allow EAP-FAST**覈取方塊以在RADIUS伺服器中啟用EAP-FAST。



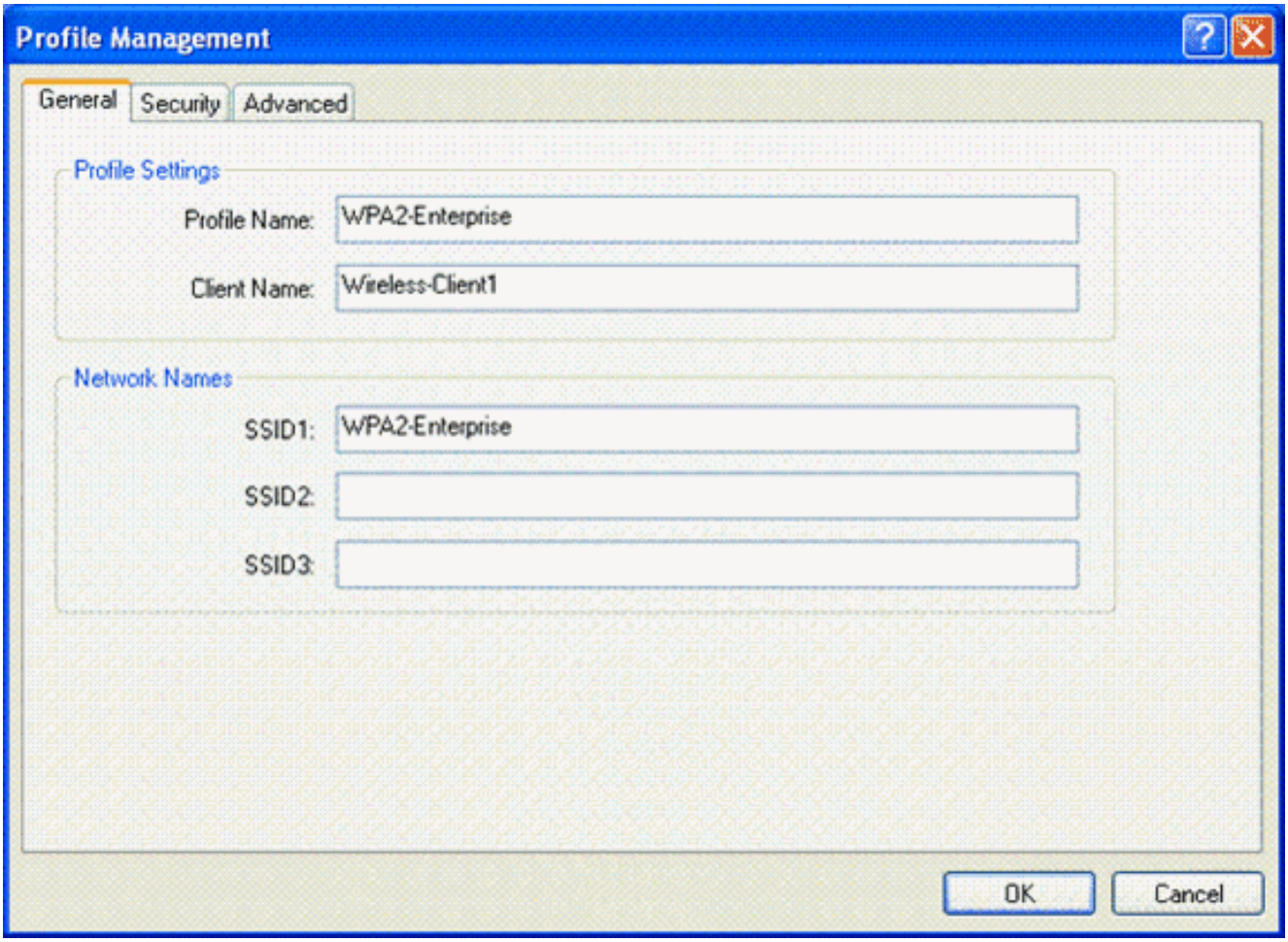
4. 根據需要配置活動/已停用主金鑰TTL（生存時間）值，或將其設定為預設值（如本例所示）。有關活動主金鑰和已停用主金鑰的資訊，請參閱主金鑰。此外，請參閱主金鑰和PAC TTL瞭解詳細資訊。Authority ID Info欄位表示此ACS伺服器的文本標識，終端使用者可以使用該標識來確定對其進行身份驗證的ACS伺服器。必須填寫此欄位。Client initial display message欄位指定要傳送給使用EAP-FAST客戶端進行身份驗證的使用者的消息。最大長度為40個字元。僅當終端使用者客戶端支援顯示時，使用者才會看到初始消息。
5. 如果您希望ACS執行匿名帶內PAC調配，請選中**允許匿名帶內PAC調配**覈取方塊。
6. **允許的內部方**法 — 此選項確定哪些內部EAP方法可以在EAP-FAST TLS隧道內運行。對於匿名帶內調配，必須啟用EAP-GTC和EAP-MS-CHAP以實現向後相容性。如果選擇Allow anonymous in-band PAC provisioning（允許匿名帶內PAC調配），則必須選擇EAP-MS-CHAP（零階段）和EAP-GTC（第二階段）。

為WPA2企業操作模式配置無線客戶端

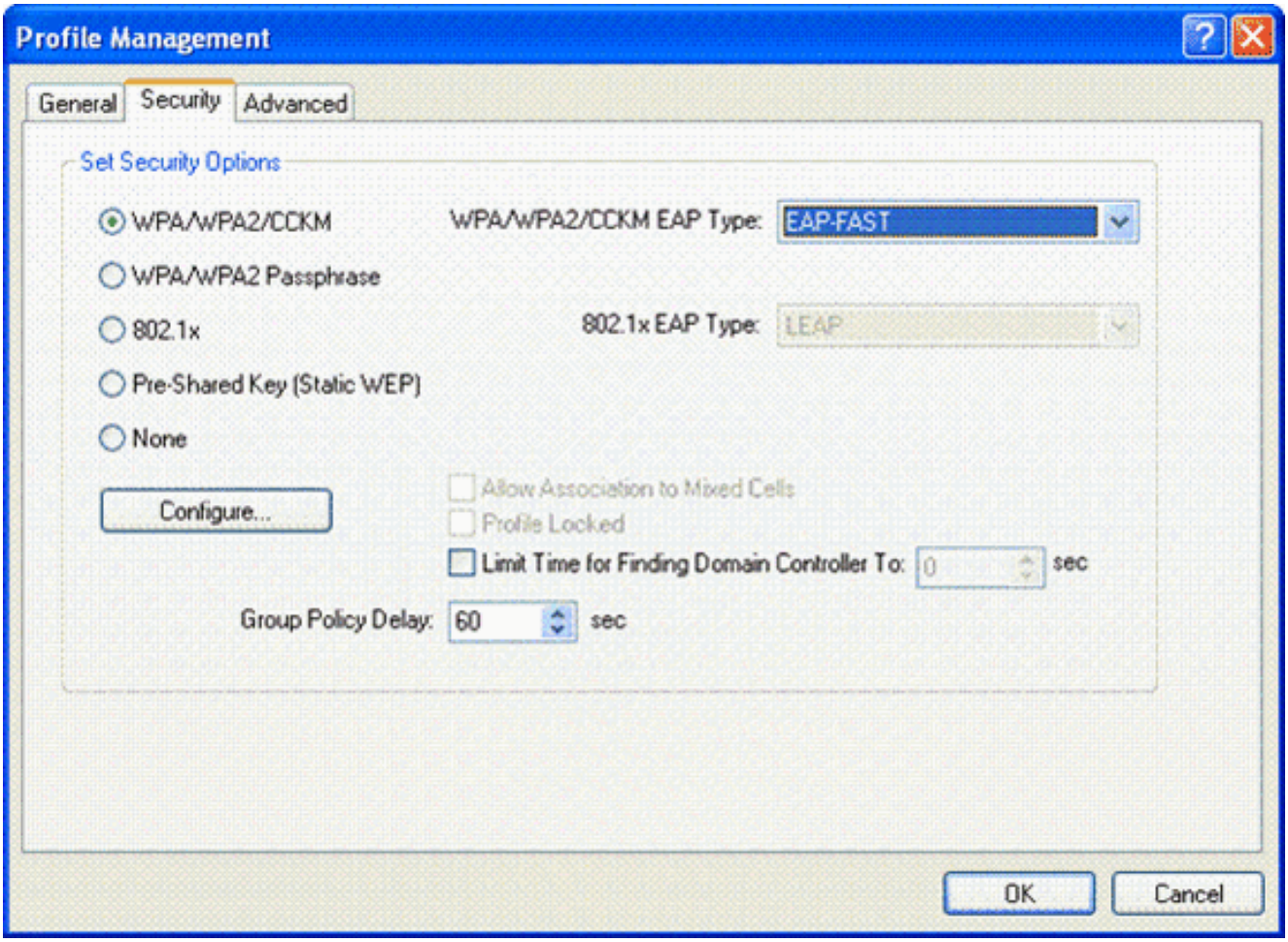
下一步是為WPA2企業模式配置無線客戶端。

完成這些步驟，為WPA2企業模式配置無線客戶端。

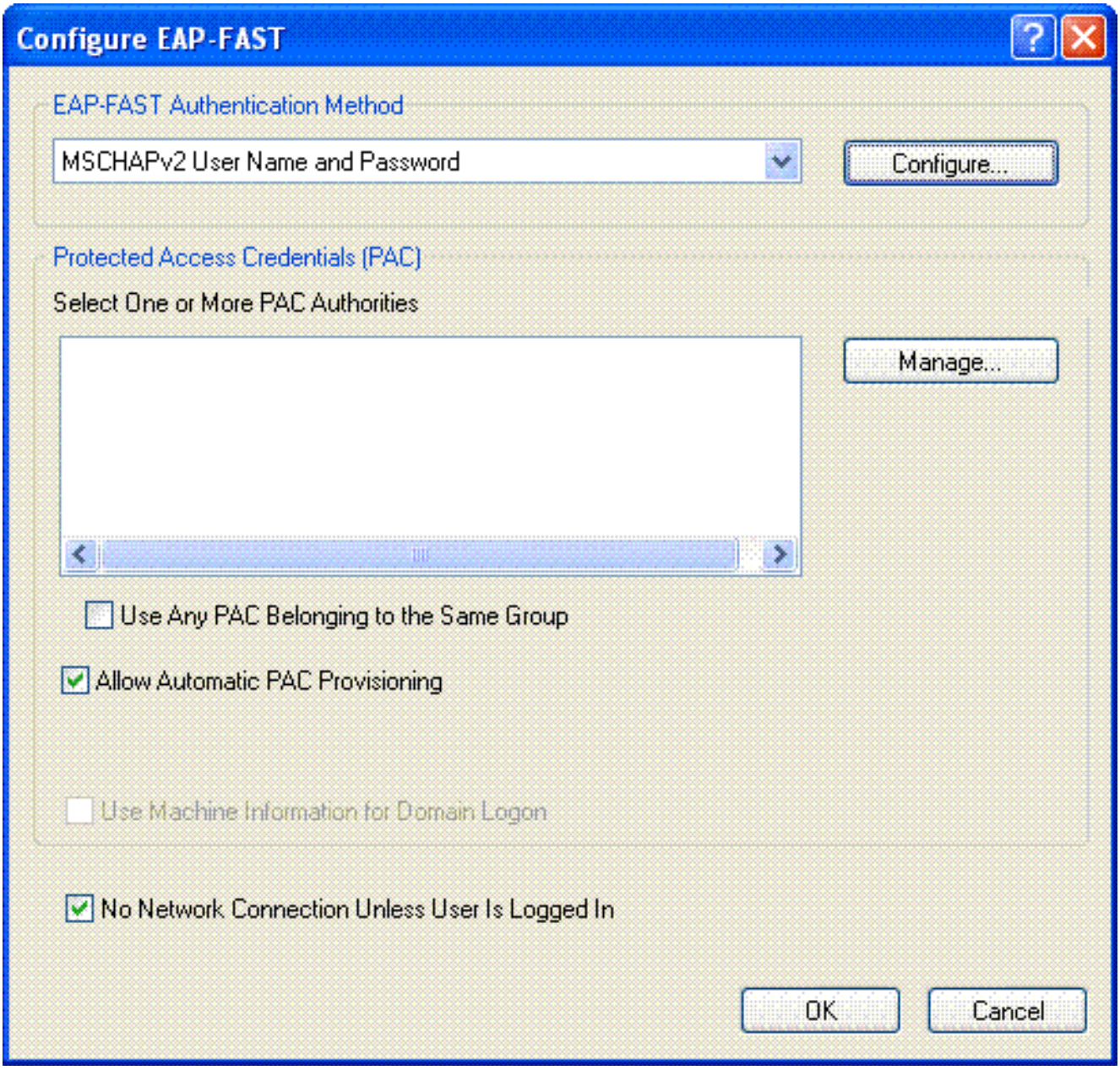
1. 在Aironet案頭實用程式視窗中，按一下**Profile Management > New**，以便為WPA2-Enterprise WLAN使用者建立配置檔案。如前所述，本文檔將WLAN/SSID名稱用作**WPA2-Enterprise**用於無線客戶端。
2. 在Profile Management視窗中，按一下**General**頁籤，然後配置Profile Name、Client Name和SSID名稱，如本例所示。然後，按一下
OK



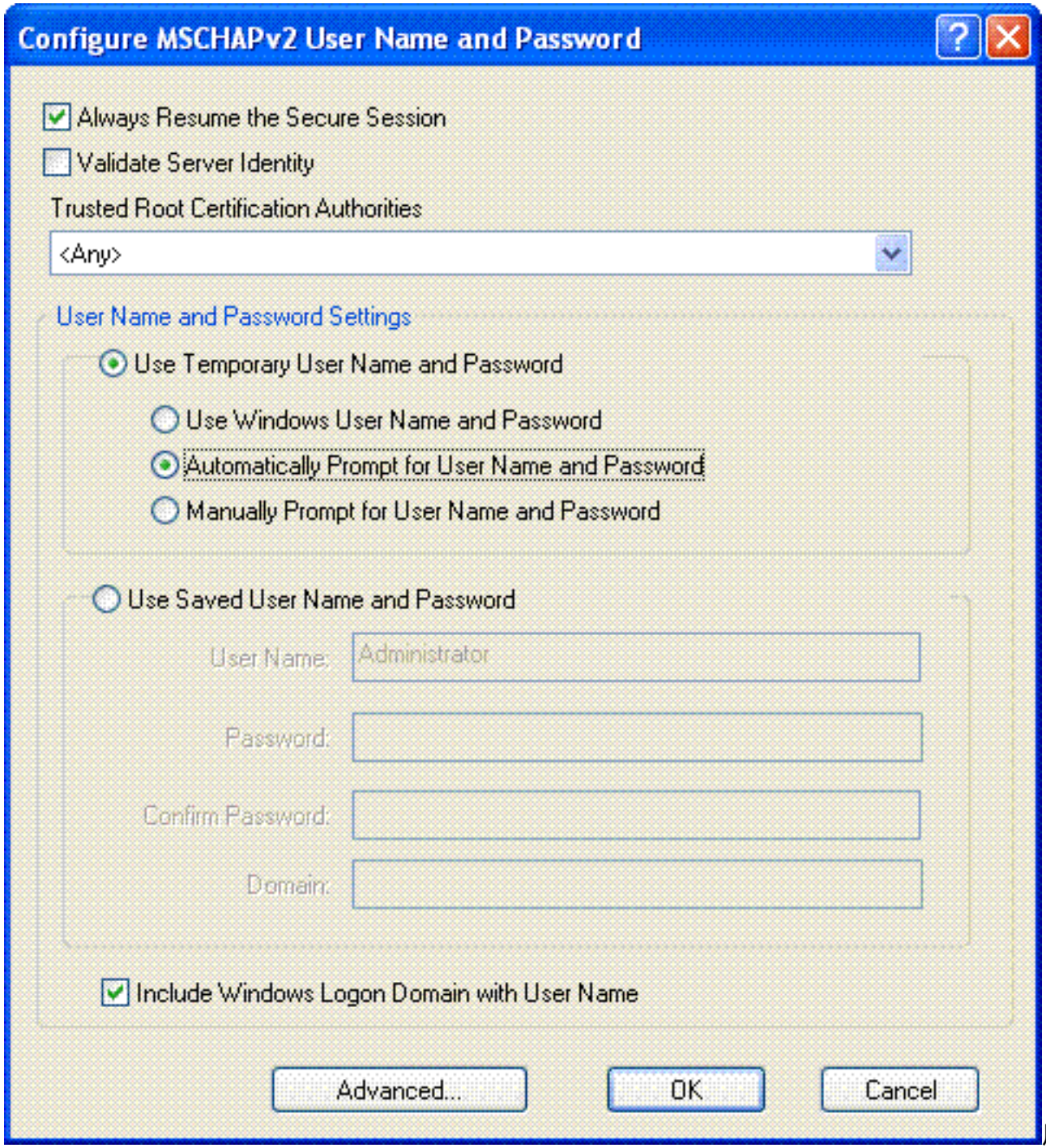
3. 按一下**Security**頁籤，然後選擇**WPA/WPA2/CCKM**以啟用WPA2操作模式。在WPA/WPA2/CCKM EAP Type下，選擇**EAP-FAST**。按一下**Configure**以配置EAP-FAST設定。



4. 在「配置EAP-FAST」視窗中，選中**允許自動PAC調配**覈取方塊。如果要配置匿名PAC調配，EAP-MS-CHAP將用作零階段中唯一的內部方法。



5. 從EAP-FAST Authentication Method下拉框中選擇MSCHAPv2 User Name and Password作為身份驗證方法。按一下「**Configure**」。
6. 從Configure MSCHAPv2 User Name and Password視窗，選擇相應的使用者名稱和密碼設定。本示例選擇**自動提示輸入使用者名稱和密碼**。



應在ACS中註冊相同的使用者名稱和密碼。如前所述，此示例分別使用User1和User1作為使用者名稱和密碼。另請注意，這是一個匿名的帶內調配。因此，使用者端無法驗證伺服器憑證。您需要確保未選中Validate Server Identity覈取方塊。

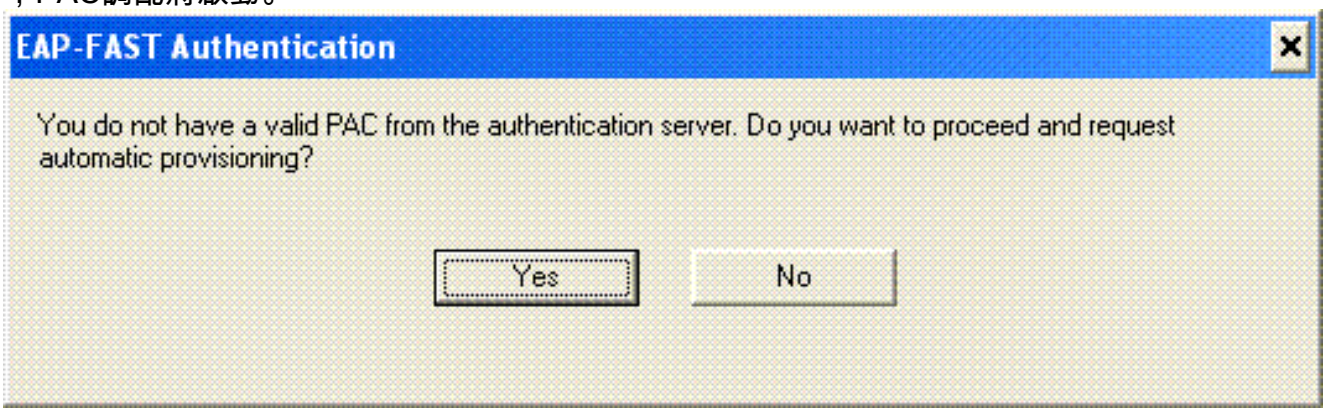
7. 按一下「**OK**」（確定）。

驗證WPA2企業運行模式

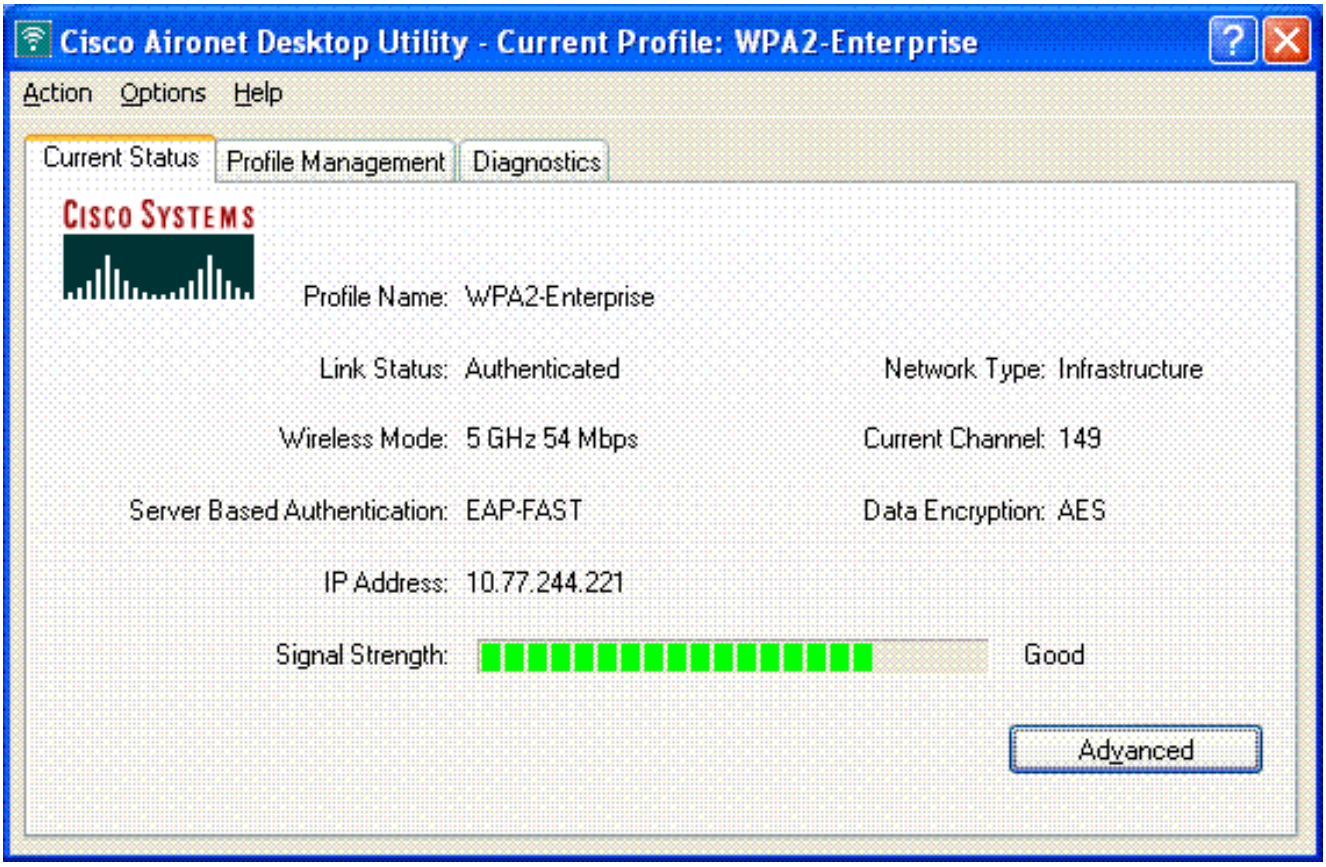
完成以下步驟以驗證WPA2企業模式配置是否正常工作：

1. 在Aironet案頭實用程式視窗中，選擇配置檔案**WPA2-Enterprise**，然後按一下**Activate**以啟用無線客戶端配置檔案。
2. 如果您已啟用MS-CHAP ver2作為身份驗證，則客戶端將提示輸入使用者名稱和密碼。

3. 在使用者的EAP-FAST處理期間，客戶端將提示您從RADIUS伺服器請求PAC。按一下**Yes**後，PAC調配將啟動。



4. 在零階段中成功調配PAC後，緊接著進行第一階段和第二階段，並成功執行身份驗證過程。身份驗證成功後，無線客戶端將與WLAN WPA2-Enterprise相關聯。螢幕截圖如下：



您還可以驗證RADIUS伺服器是否收到並驗證來自無線使用者端的驗證請求。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。

為WPA2個人模式配置裝置

執行以下步驟將裝置配置為WPA2-Personal操作模式：

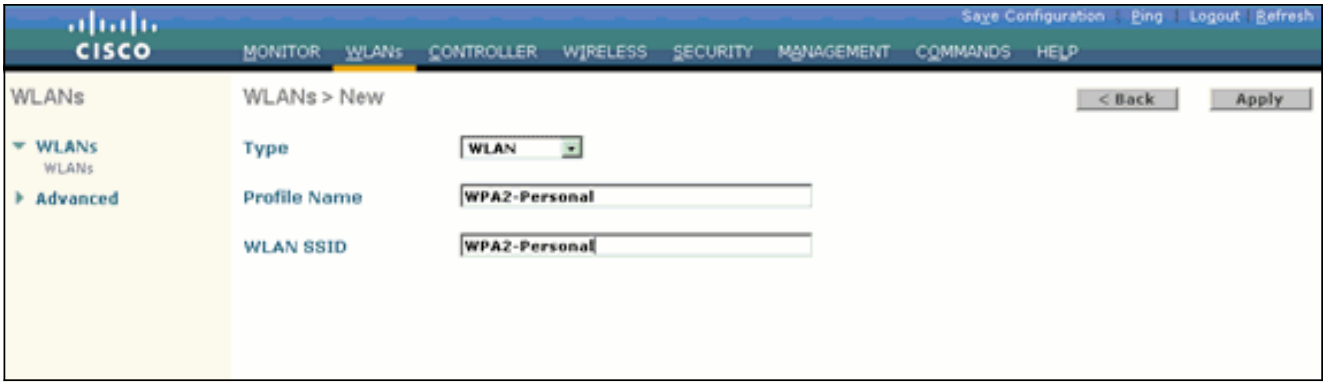
1. 為WPA2個人模式身份驗證配置WLAN
2. 為WPA2個人模式配置無線客戶端

為WPA2個人操作模式配置WLAN

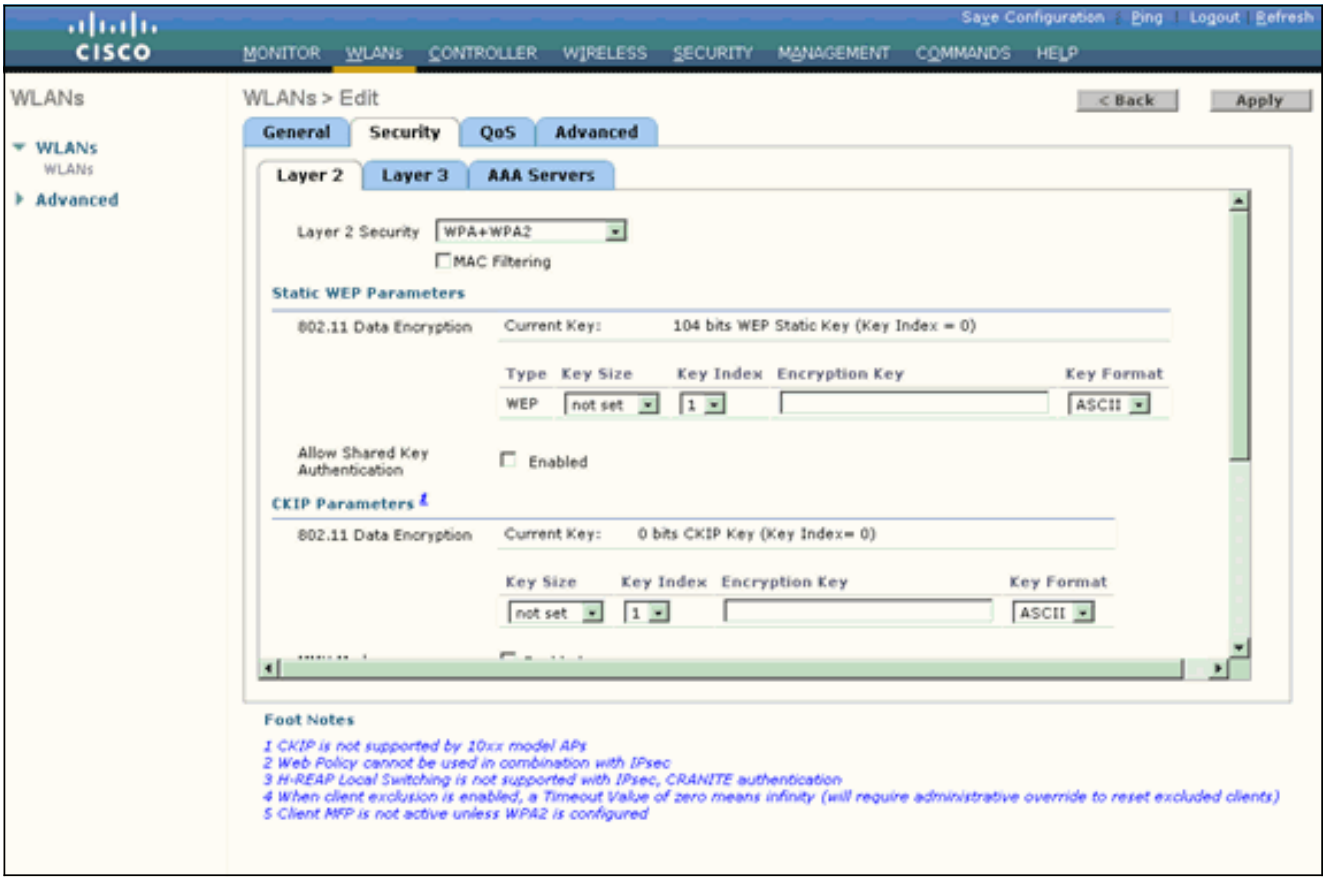
您需要設定使用者端用來連線到無線網路的WLAN。WPA2個人模式的WLAN SSID將為WPA2 — 個人。此範例將此WLAN指派給管理介面。

完成以下步驟即可設定WLAN及其相關引數：

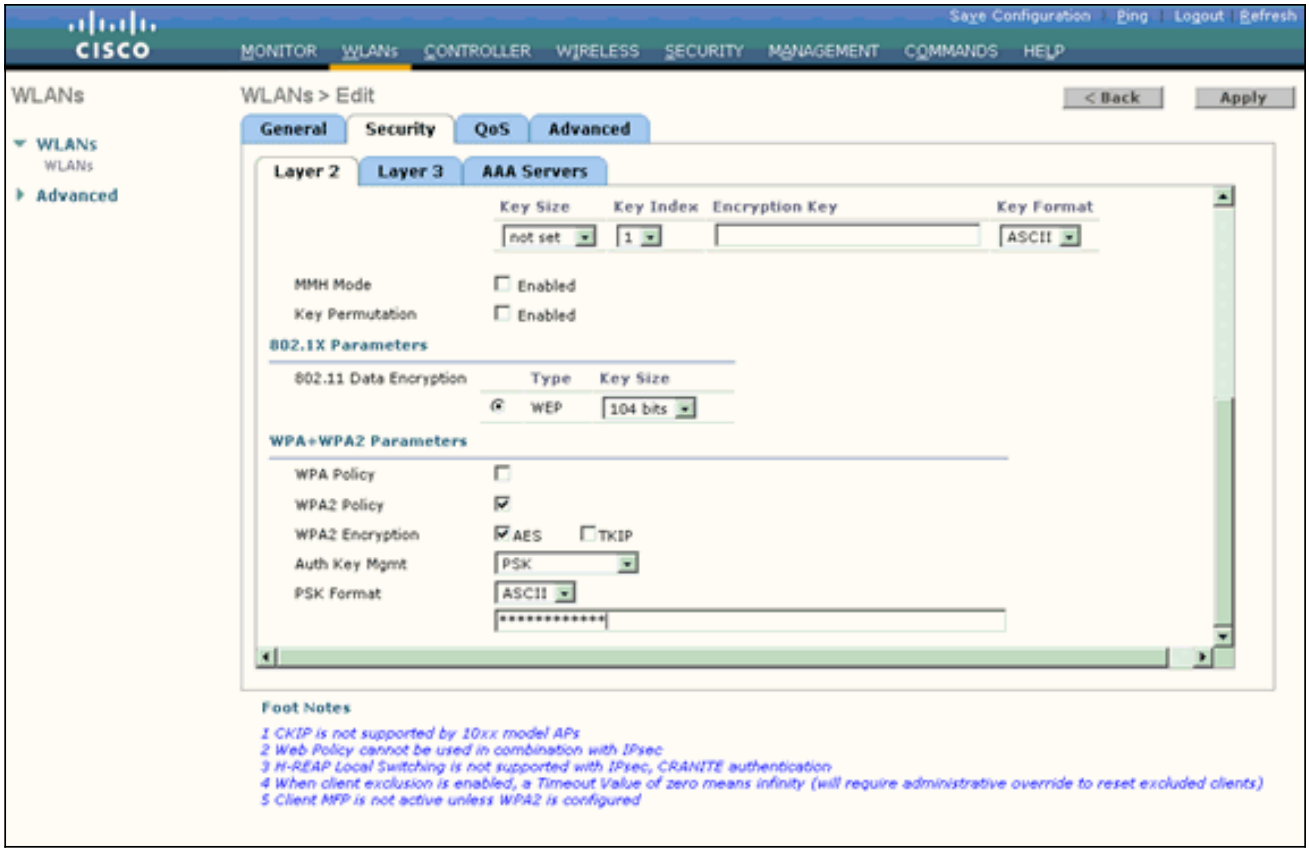
1. 從控制器的GUI中按一下「**WLANs**」，以顯示「WLANs」頁面。此頁面列出控制器上存在的WLAN。
2. 按一下**New**以建立一個新的WLAN。
3. 在WLANs > New頁面上輸入WLAN SSID名稱、配置檔名稱和WLAN ID。然後，按一下「**Apply**」。本示例使用**WPA2-Personal**作為SSID。



4. 建立新的WLAN後，系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上，您可以定義此WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和高級引數。
5. 在General Policies下，勾選**Status**覈取方塊以啟用WLAN。
6. 如果您希望AP在其信標幀中廣播SSID，請選中**Broadcast SSID**覈取方塊。
7. 按一下**Security**頁籤。在Layer Security下，選擇**WPA+WPA2**。這將為WLAN啟用WPA身份驗證。



8. 向下滾動頁面以修改**WPA+WPA2引數**。在此示例中，選擇了WPA2策略和AES加密。
9. 在Auth Key Mgmt下，選擇**PSK**以啟用WPA2-PSK。
10. 在相應的欄位中輸入預共用金鑰，如下所示。



注意：WLC上使用的預共用金鑰必須與無線客戶端上配置的金鑰匹配。

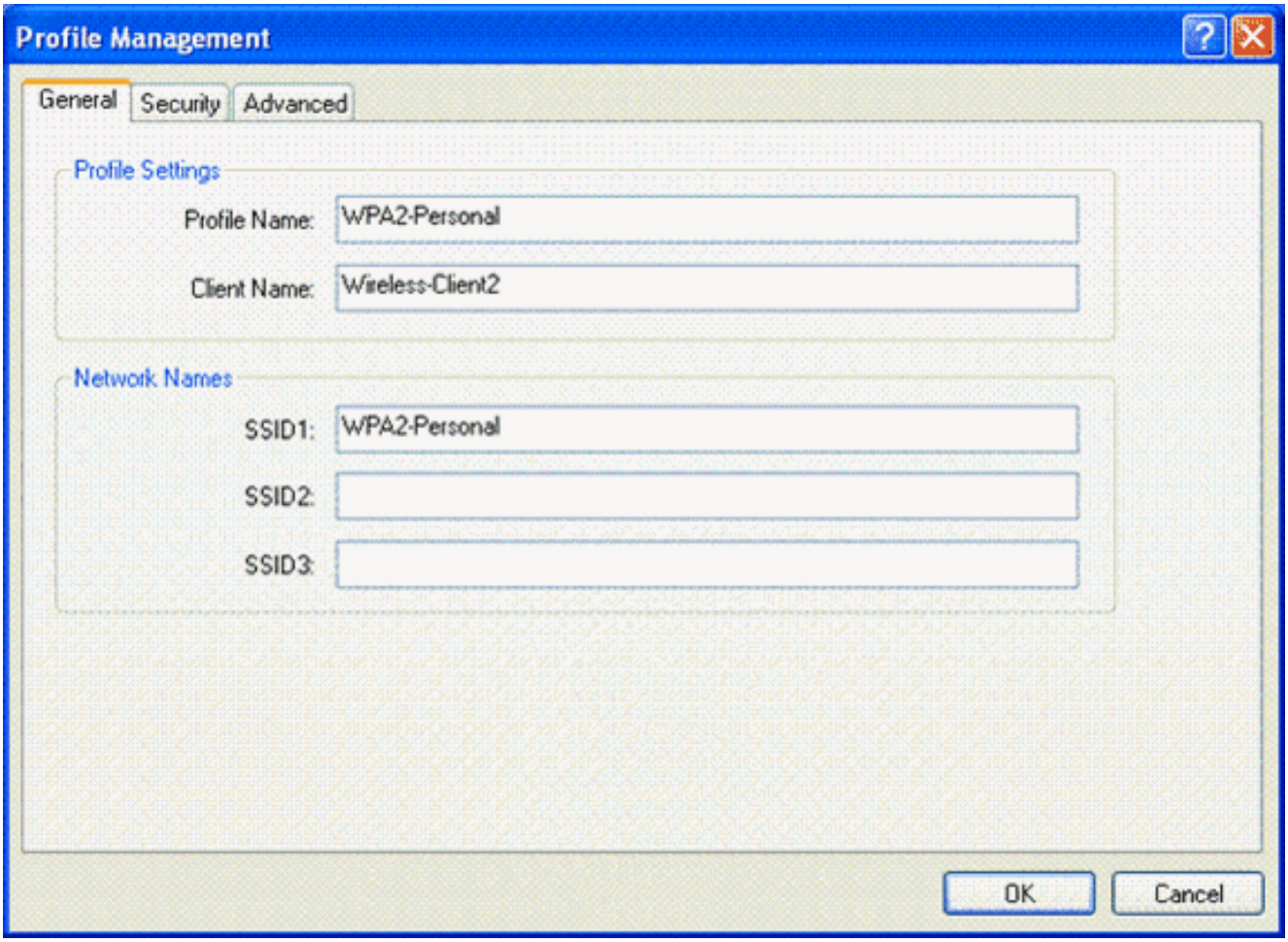
11. 按一下「**Apply**」。

為WPA2個人模式配置無線客戶端

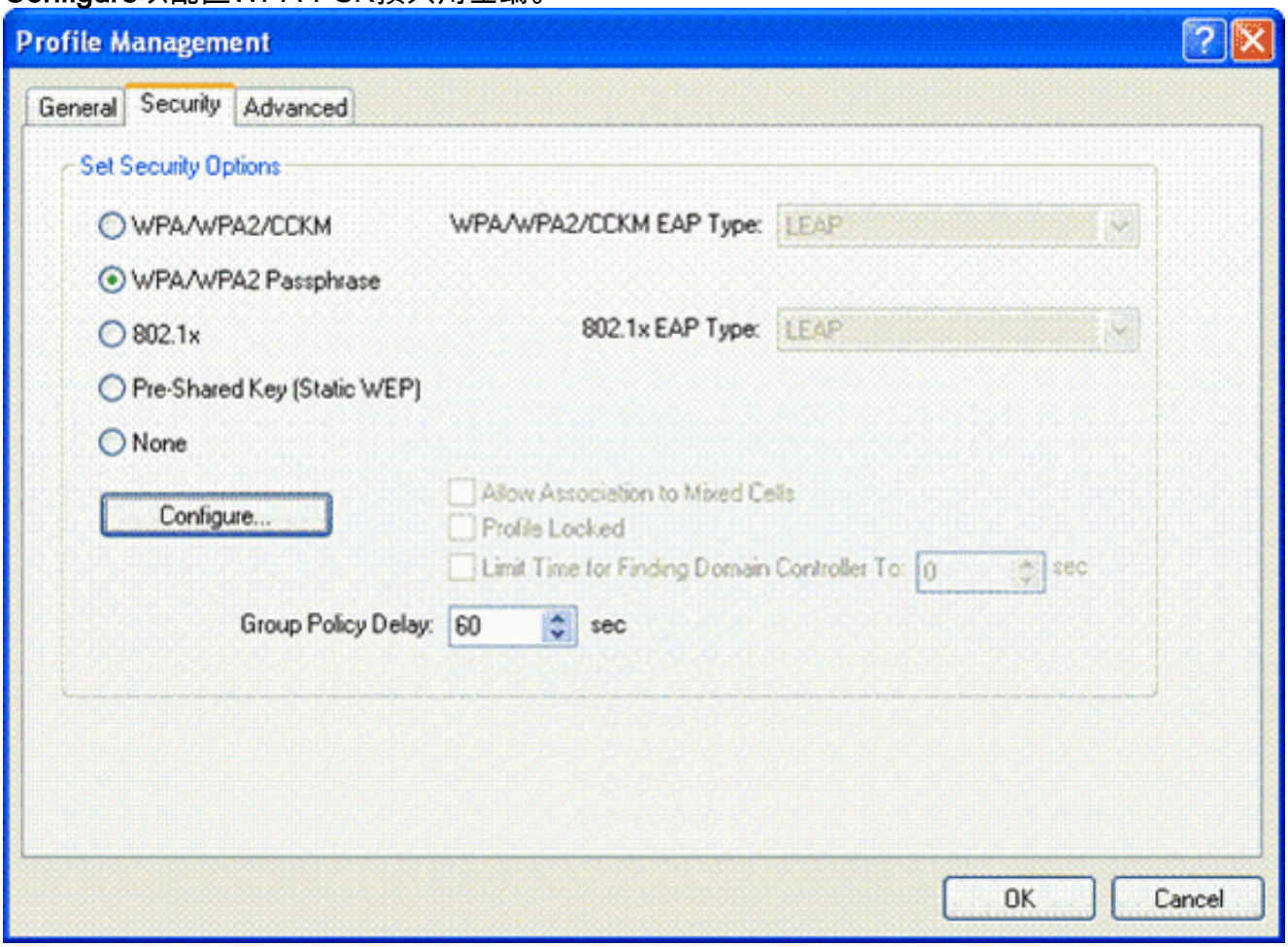
下一步是將無線客戶端配置為WPA2 — 個人操作模式。

完成以下步驟，將無線客戶端配置為WPA2 — 個人模式：

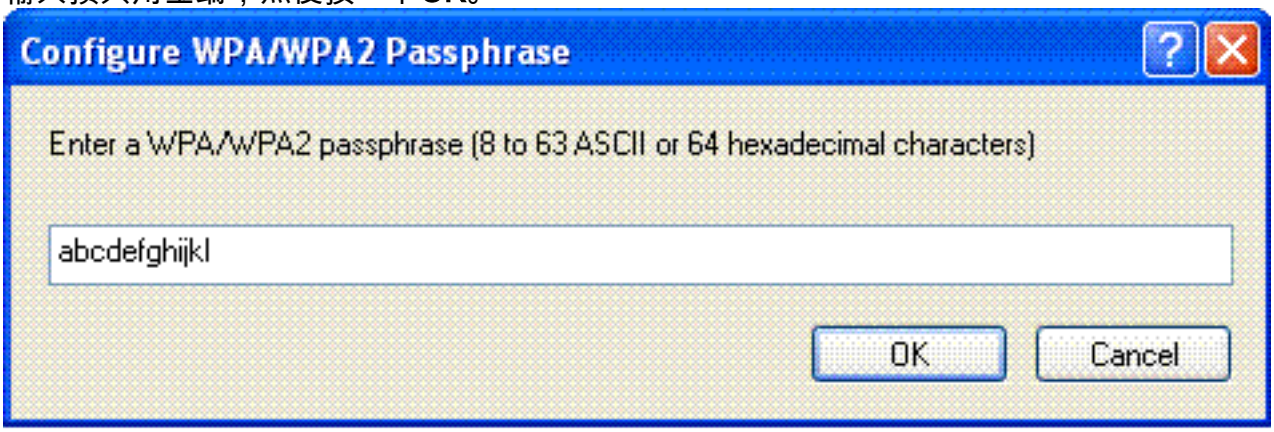
1. 在Aironet案頭實用程式視窗中，按一下**Profile Management > New**，以便為WPA2-PSK WLAN使用者建立配置檔案。
2. 在Profile Management視窗中，按一下**General**頁籤，然後配置Profile Name、Client Name和SSID名稱，如本例所示。然後，按一下**OK**。



3. 按一下**Security**頁籤，然後選擇**WPA/WPA2 Passphrase**以啟用WPA2-PSK操作模式。按一下**Configure**以配置WPA-PSK預共用金鑰。



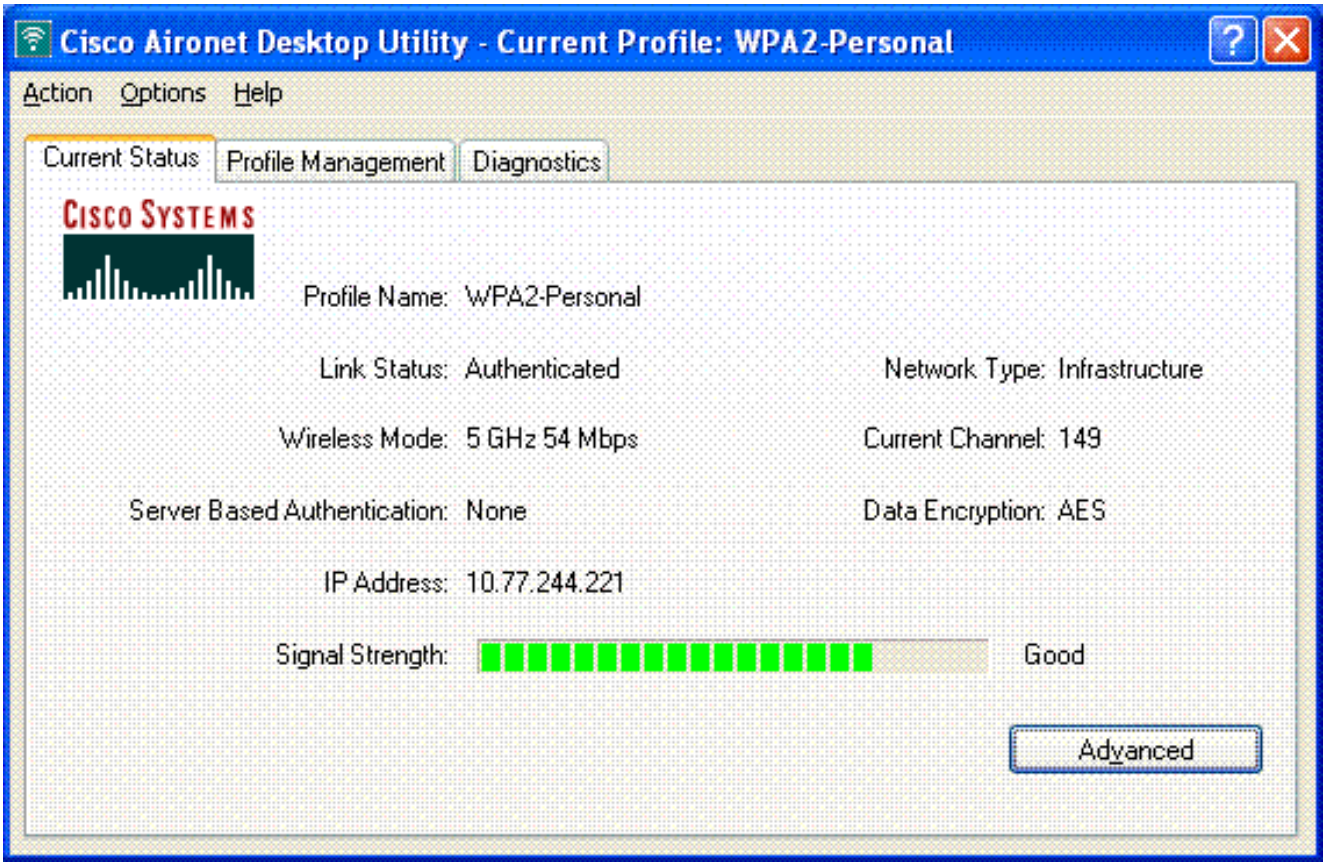
4. 輸入預共用金鑰，然後按一下**OK**。



驗證WPA2 — 個人操作模式

完成以下步驟，驗證WPA2-Enterprise模式配置是否正常工作：

1. 在Aironet案頭實用程式視窗中，選擇配置檔案**WPA2-Personal**，然後按一下**Activate**以啟用無線客戶端配置檔案。
2. 一旦配置檔案被啟用，無線客戶端就會在身份驗證成功後與WLAN關聯。螢幕截圖如下：



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下**debug**指令對組態疑難排解很有用：

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug dot1x events enable** — 啟用所有dot1x事件的調試。以下是基於成功身份驗證的調試輸出示例：**注意**：由於空間限制，此輸出的某些行已移至第二行。

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....................................................................
.....................................................................
.....................................................................
.....................................................................

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
```

```
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for
mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to
mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===>
20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
```

```
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===>
24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- debug dot1x packet enable — 啟用802.1x資料包消息的調試。
- debug aaa events enable — 啟用所有aaa事件的調試輸出。

相關資訊

- WPA2 - Wi-Fi保護訪問2
- 使用無線LAN控制器和外部RADIUS伺服器的EAP-FAST身份驗證配置示例
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- WPA配置概述
- 無線產品支援
- 技術支援與文件 - Cisco Systems

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）。