使用RADIUS伺服器的外部Web驗證

目錄

簡介

本檔案將說明如何使用外部RADIUS伺服器執行外部Web驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 輕量型存取點(LAP)和Cisco WLC組態的基本知識
- 瞭解如何設定和配置外部Web伺服器
- 瞭解如何配置Cisco Secure ACS

採用元件

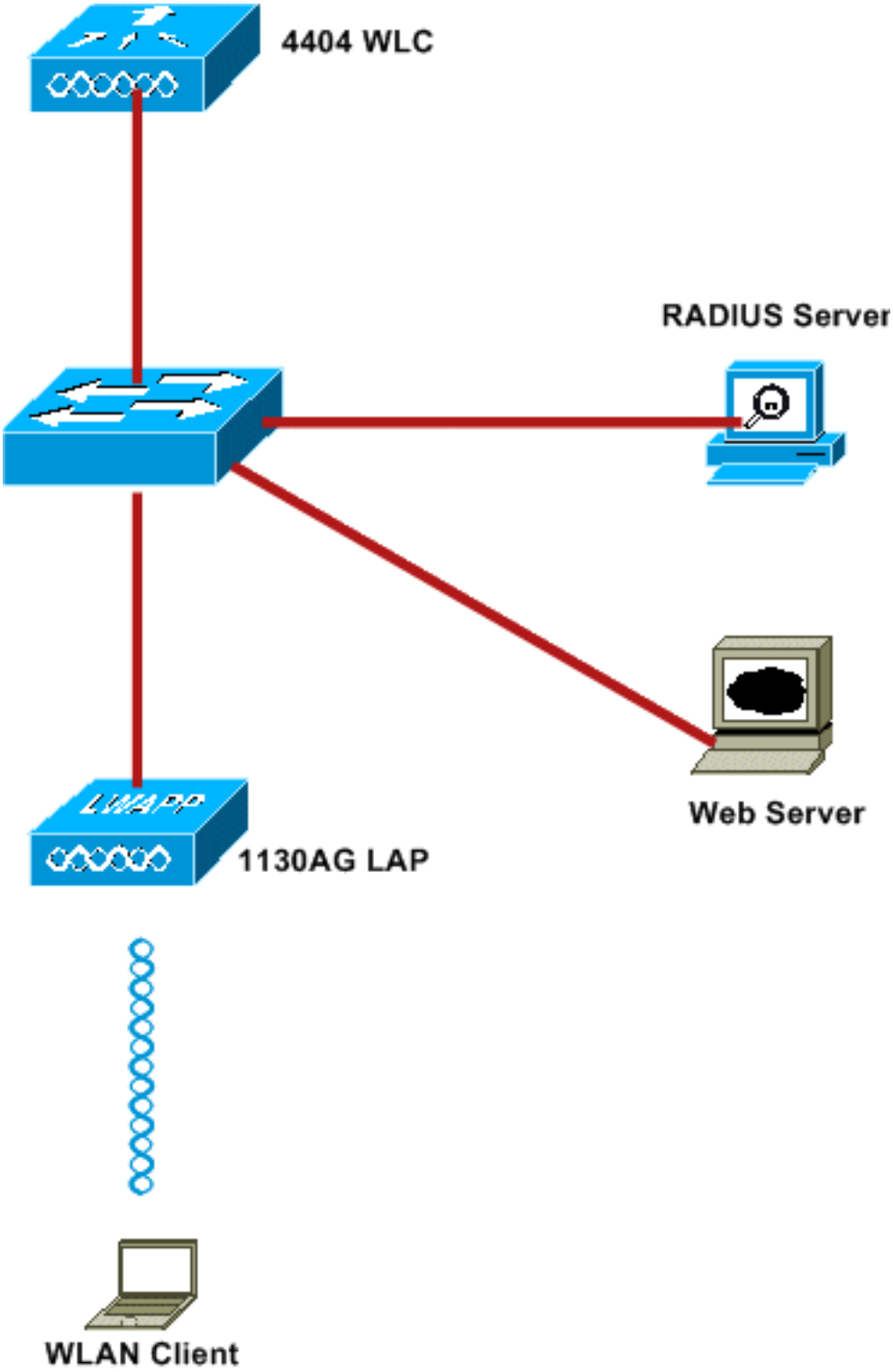
本文中的資訊係根據以下軟體和硬體版本：

- 運行韌體版本5.0.148.0的無線LAN控制器
- 思科1232系列LAP
- 思科802.11a/b/g無線客戶端介面卡3.6.0.61
- 承載Web驗證登入頁面的外部Web伺服器
- 運行韌體版本4.1.1.24的Cisco Secure ACS版本

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。

網路圖表

本檔案會使用以下網路設定：



以下是本文中使用的IP位址：

- WLC使用IP地址10.77.244.206
- LAP已註冊到IP地址為10.77.244.199的WLC
- Web伺服器使用IP地址10.77.244.210
- Cisco ACS伺服器使用IP地址10.77.244.196
- 客戶端從對映到WLAN的管理介面接收IP地址 — 10.77.244.208

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。

外部Web驗證

Web驗證是第3層驗證機制，用於對訪客使用者進行網際網路存取的驗證。使用此程式進行身份驗證的使用者在成功完成身份驗證過程之前將無法訪問Internet。有關外部Web驗證程式的完整資訊，請參閱檔案使用無線LAN控制器的外部Web驗證組態範例的外部Web驗證程式一節。

在本檔案中，我們看到一個組態範例，其中使用外部RADIUS伺服器執行外部Web驗證。

設定WLC

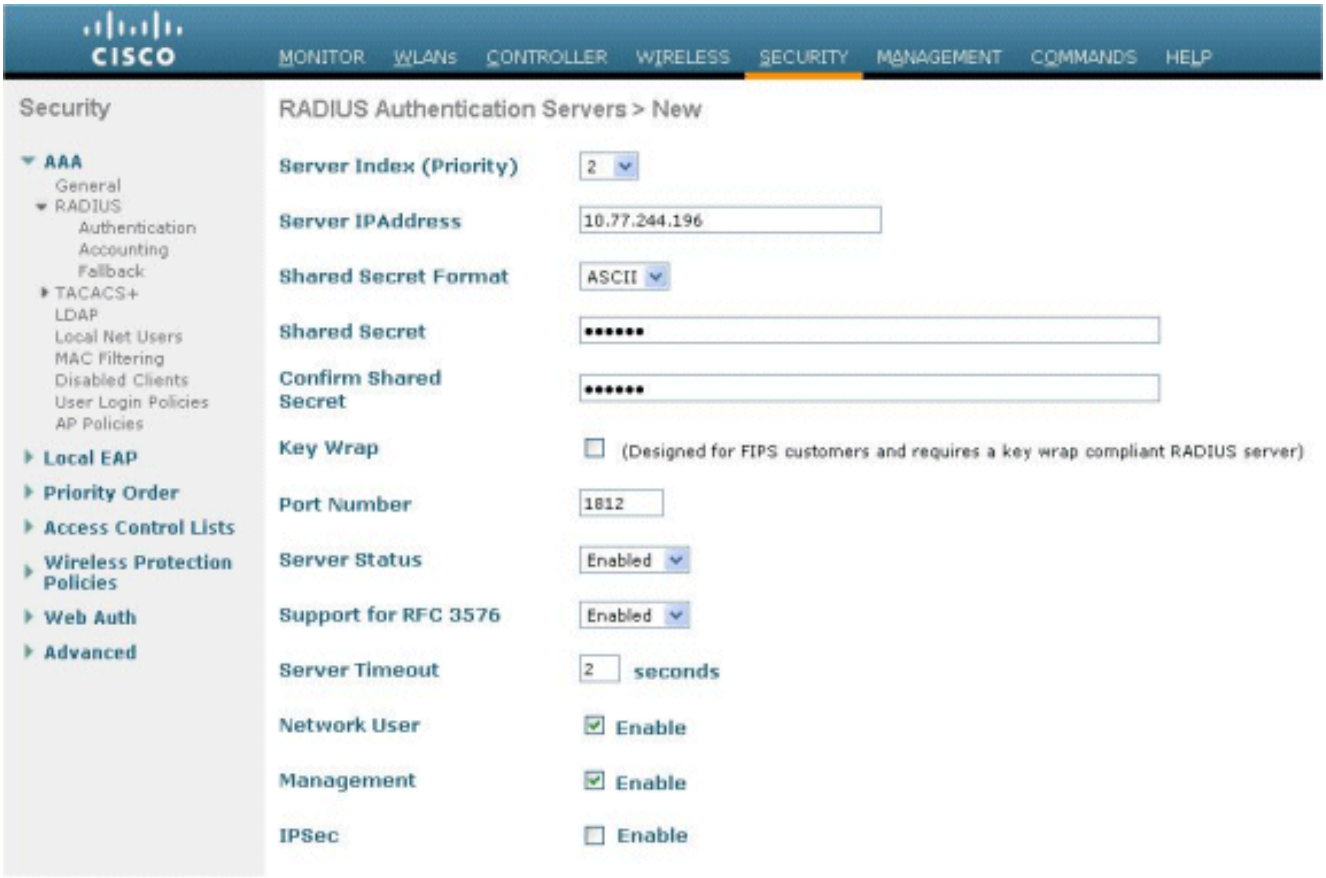
在本檔案中，我們假設已設定WLC，且其LAP已註冊到WLC。本檔案進一步假設WLC已設定為基本操作，且LAP已註冊到WLC。如果您是嘗試將 WLC 設定為搭配 LAP 進行基本操作的新使用者，請參閱向無線 LAN 控制器 (WLC) 註冊輕量型 AP (LAP)。若要檢視註冊到WLC的LAP，請導覽至**Wireless > All APs**。

在WLC設定為基本操作並具有一個或多個LAP註冊到它後，您可以使用外部Web伺服器設定WLC進行外部Web驗證。在我們的示例中，我們使用Cisco Secure ACS版本4.1.1.24作為RADIUS伺服器。首先，我們將為此RADIUS伺服器配置WLC，然後，我們將在Cisco Secure ACS上查詢此設定所需的配置。

為Cisco Secure ACS配置WLC

執行以下步驟以在WLC上新增RADIUS伺服器：

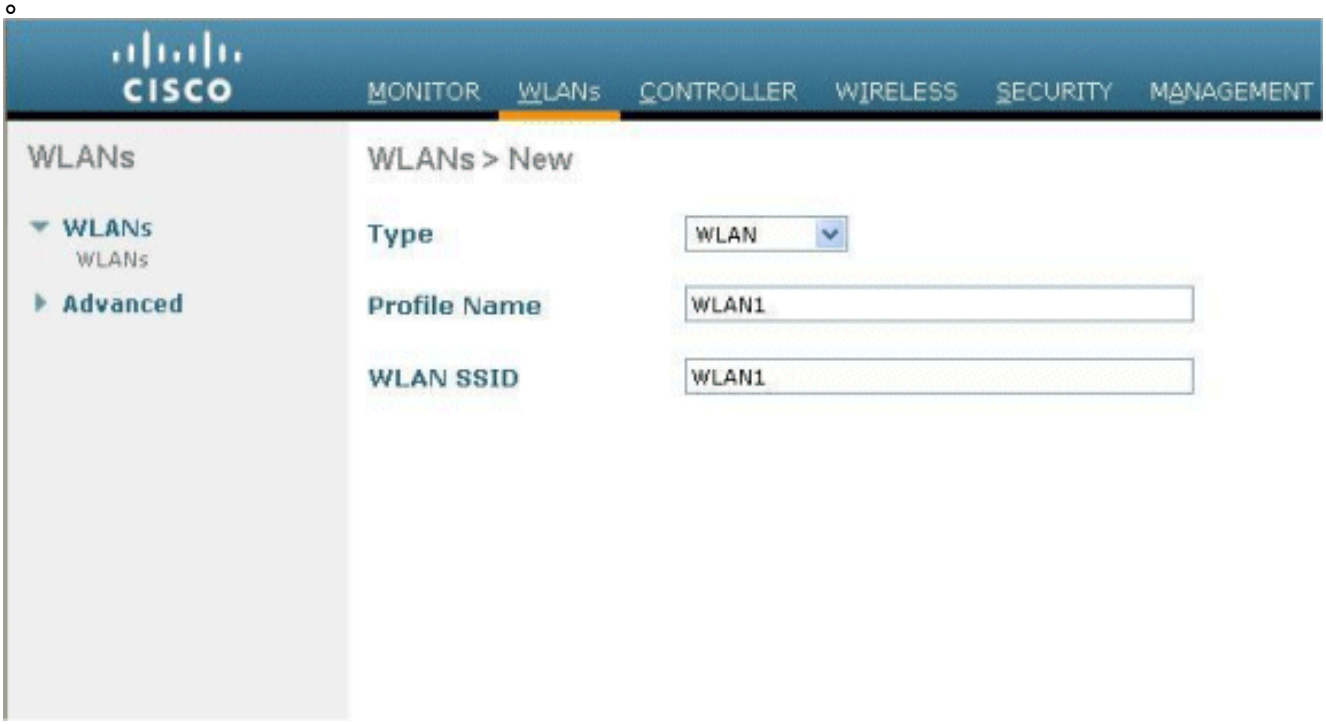
1. 在WLC GUI中，按一下「**SECURITY**」功能表。
2. 在**AAA**功能表下，導覽至**Radius > Authentication**子功能表。
3. 按一下**New**，然後輸入RADIUS伺服器的IP地址。在本例中，伺服器的IP地址為*10.77.244.196*。
4. 在WLC中輸入Shared Secret。應在WLC上以相同方式配置共用金鑰。
5. 為共用金鑰格式選擇**ASCII**或**十六進位制**。在WLC上需要選擇相同的格式。
6. **1812**是用於RADIUS身份驗證的埠號。
7. 確保Server Status選項設定為**Enabled**。
8. 選中Network User **Enable**框以對網路使用者進行身份驗證。
9. 按一下「**Apply**」。



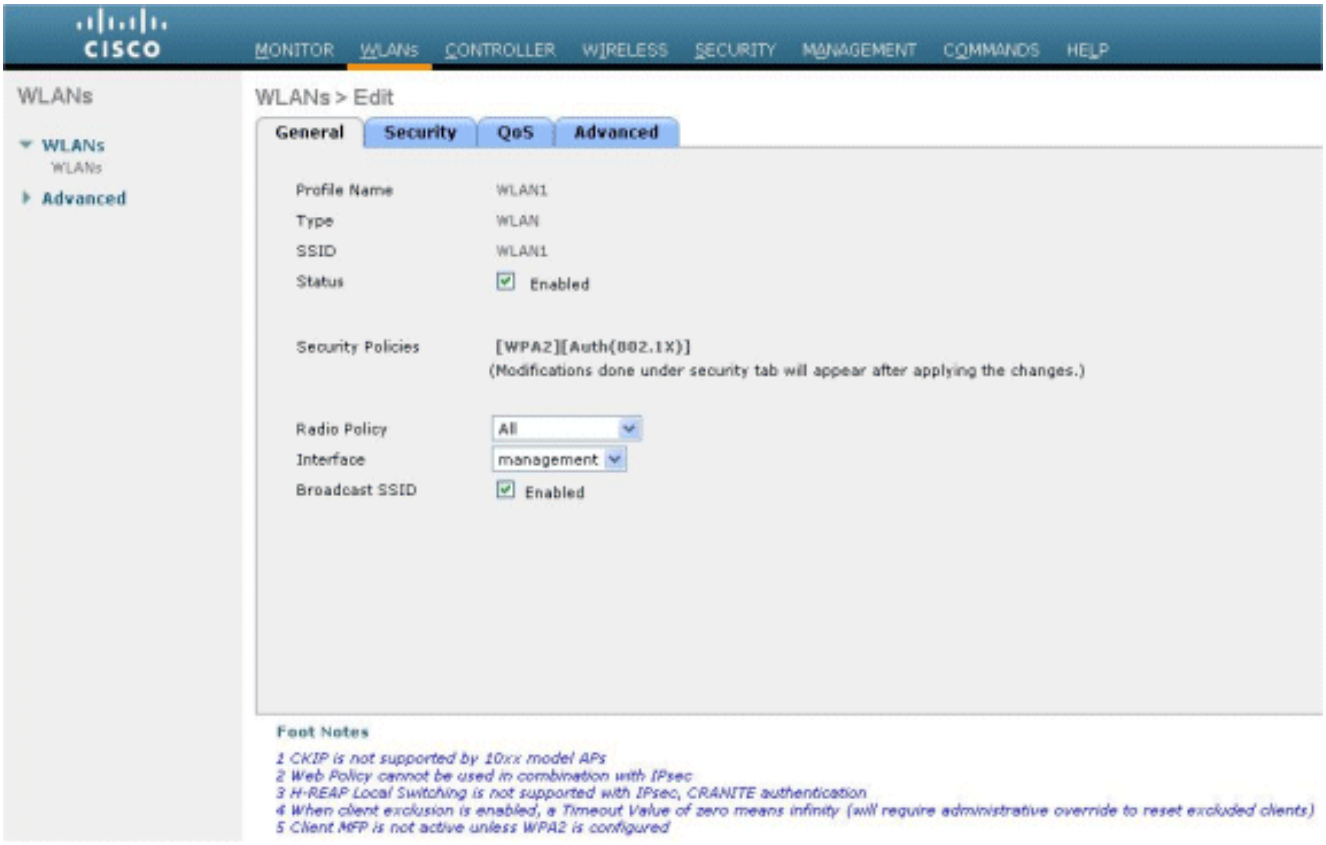
在WLC上設定WLAN以進行Web驗證

下一步是在WLC上設定WLAN以進行Web驗證。若要在WLC上設定WLAN，請執行以下步驟：

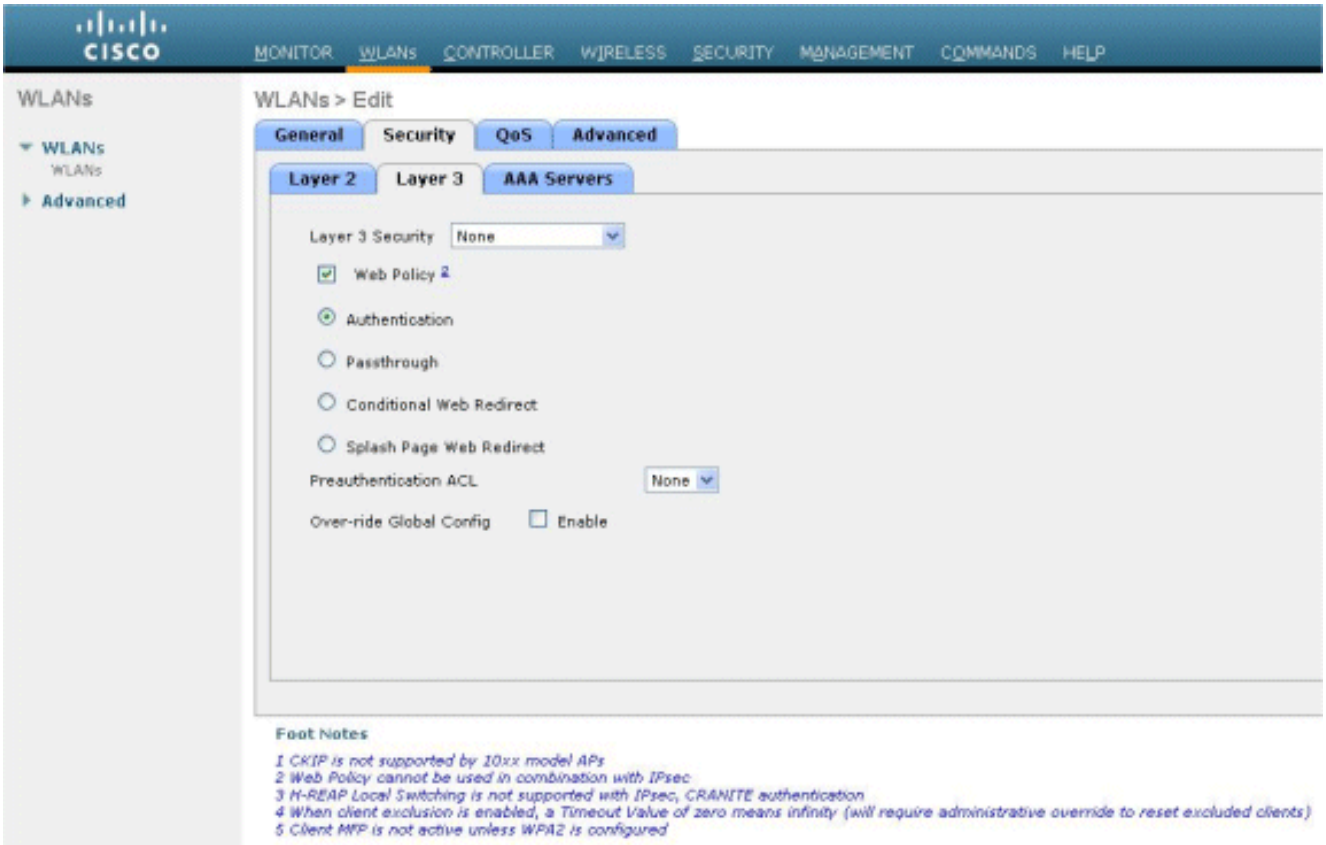
1. 從控制器GUI上按一下「**WLANs**」功能表，然後選擇**New**。
2. 選擇**WLAN**作為Type。
3. 輸入您選擇的Profile Name和WLAN SSID，然後點選**Apply**。**注意**：WLAN SSID區分大小寫。



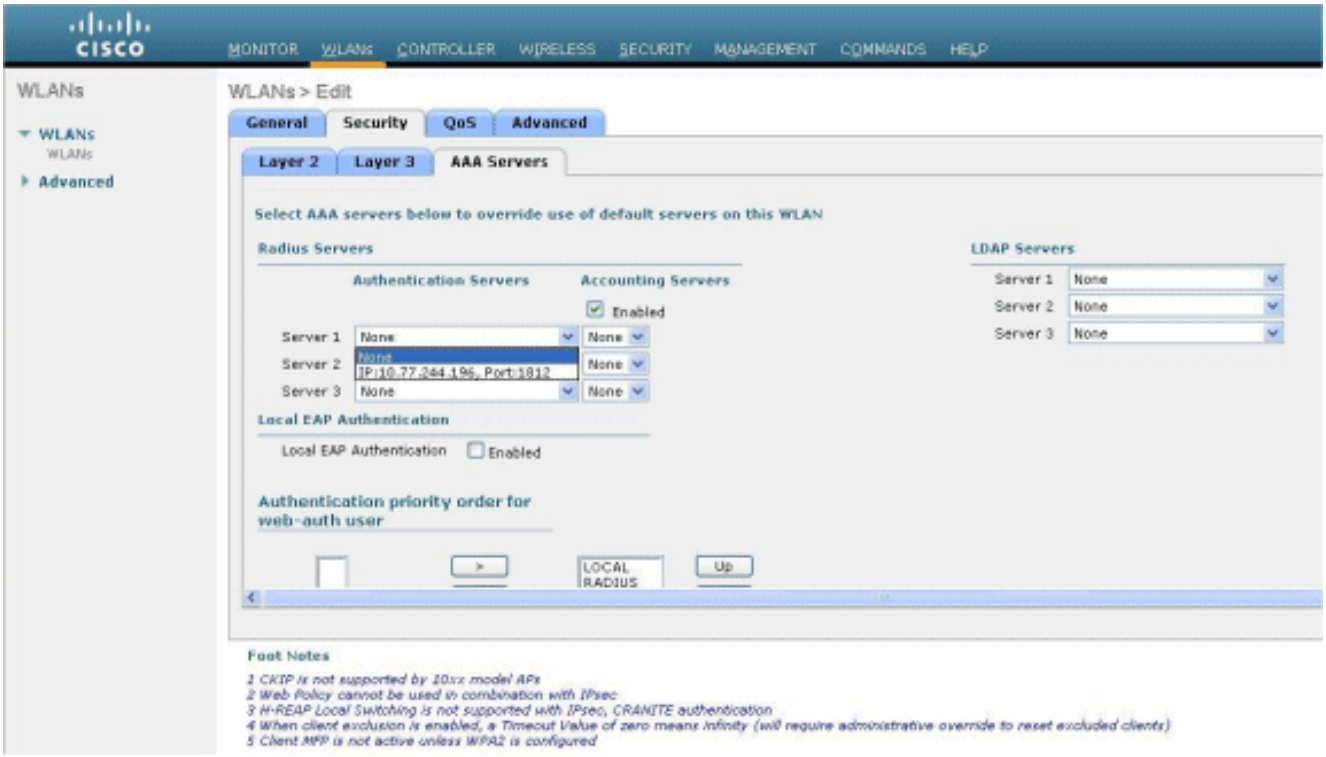
4. 在**General**索引標籤下，確保為Status和Broadcast SSID選中了**Enabled**選項。**WLAN配置**



5. 為WLAN選擇介面。通常，在唯一VLAN中配置的介面會對映到WLAN，以便客戶端接收該VLAN中的IP地址。在本例中，我們將*management*用於介面。
6. 選擇**Security**頁籤。
7. 在**Layer 2**選單下，為Layer 2 Security選擇**None**。
8. 在**Layer 3**選單下，為Layer 3 Security選擇**None**。勾選「**Web Policy**」覈取方塊，然後選擇「**Authentication**」。



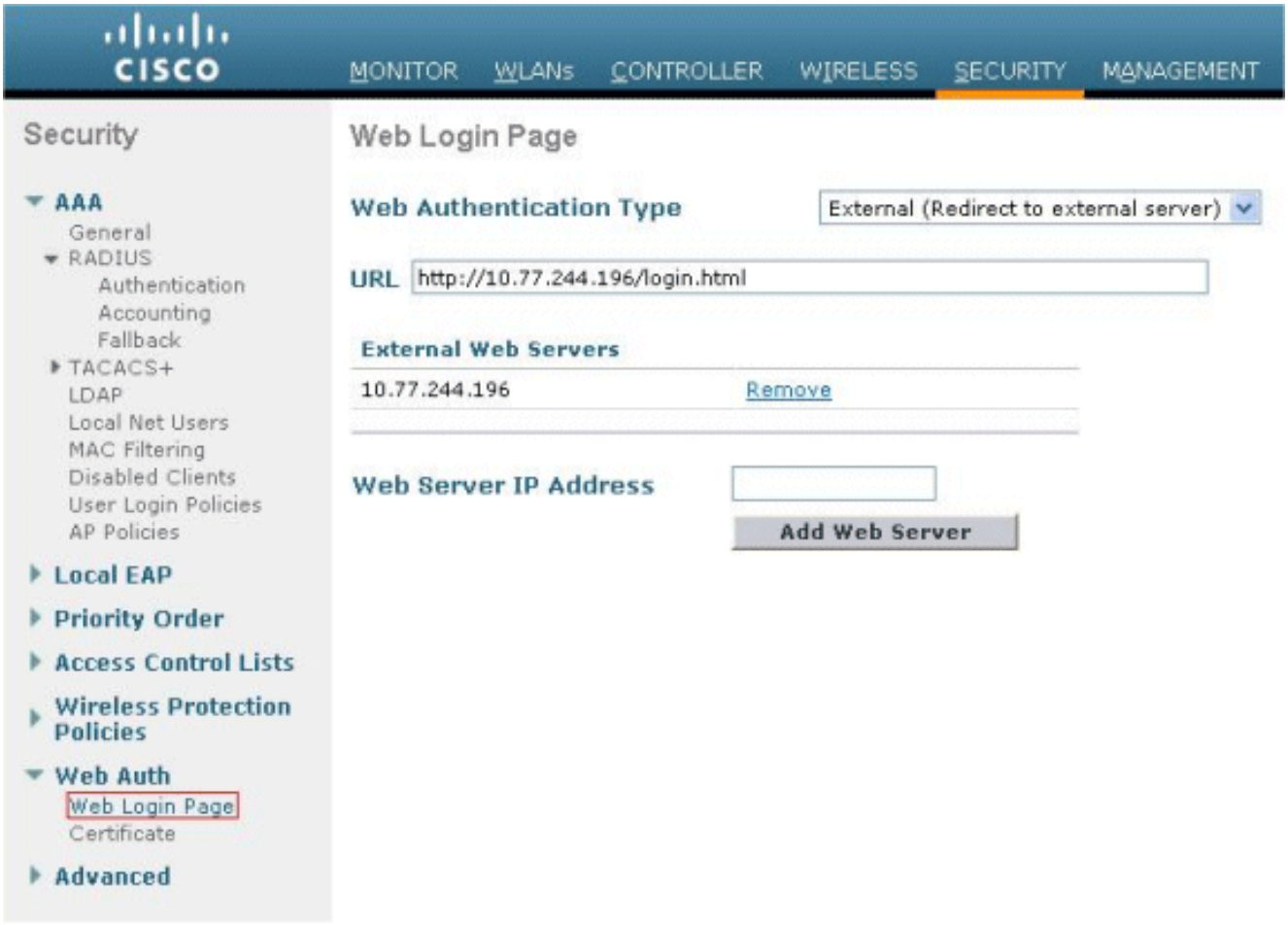
9. 在「**AAA servers**」功能表下，對於「驗證伺服器」，選擇在此WLC上設定的RADIUS伺服器。其他選單應保留預設值。



在WLC上配置Web伺服器資訊

應在WLC上配置承載Web身份驗證頁面的Web伺服器。執行以下步驟配置Web伺服器：

1. 按一下**Security**頁籤。前往**Web Auth > Web Login Page**。
2. 將Web驗證型別設定為**External**。
3. 在「Web伺服器IP地址」欄位中，輸入託管「Web身份驗證」頁的伺服器的IP地址，然後按一下**新增Web伺服器**。在本例中，IP地址為*10.77.244.196*，該地址顯示在External Web Servers下。
4. 在URL欄位中輸入Web Authentication頁面的URL(在本例中為*http://10.77.244.196/login.html*)。



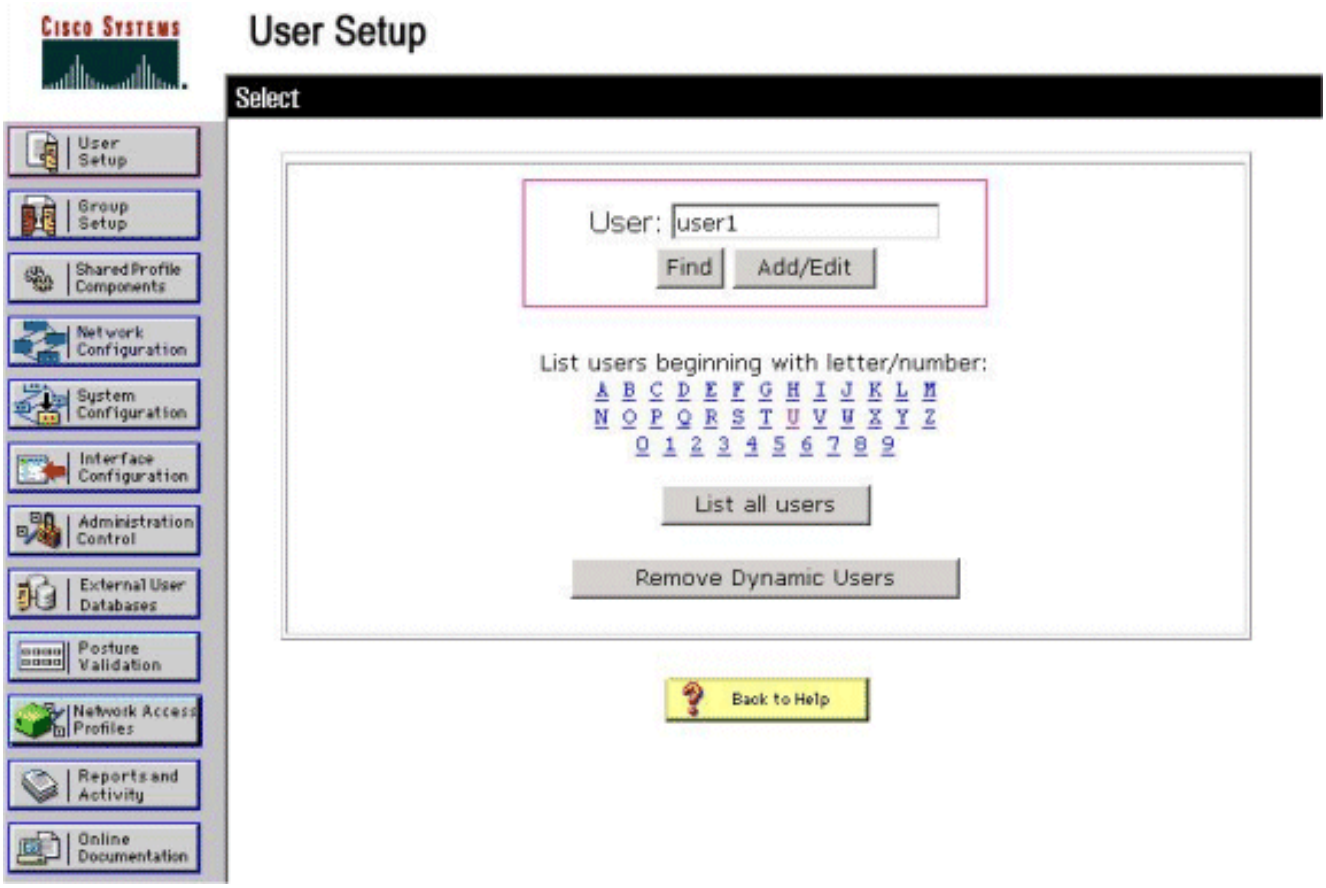
配置Cisco Secure ACS

在本文檔中，我們假設Cisco Secure ACS伺服器已經安裝並在電腦上運行。有關如何設定Cisco Secure ACS的詳細資訊，請參閱Cisco Secure ACS 4.2配置指南。

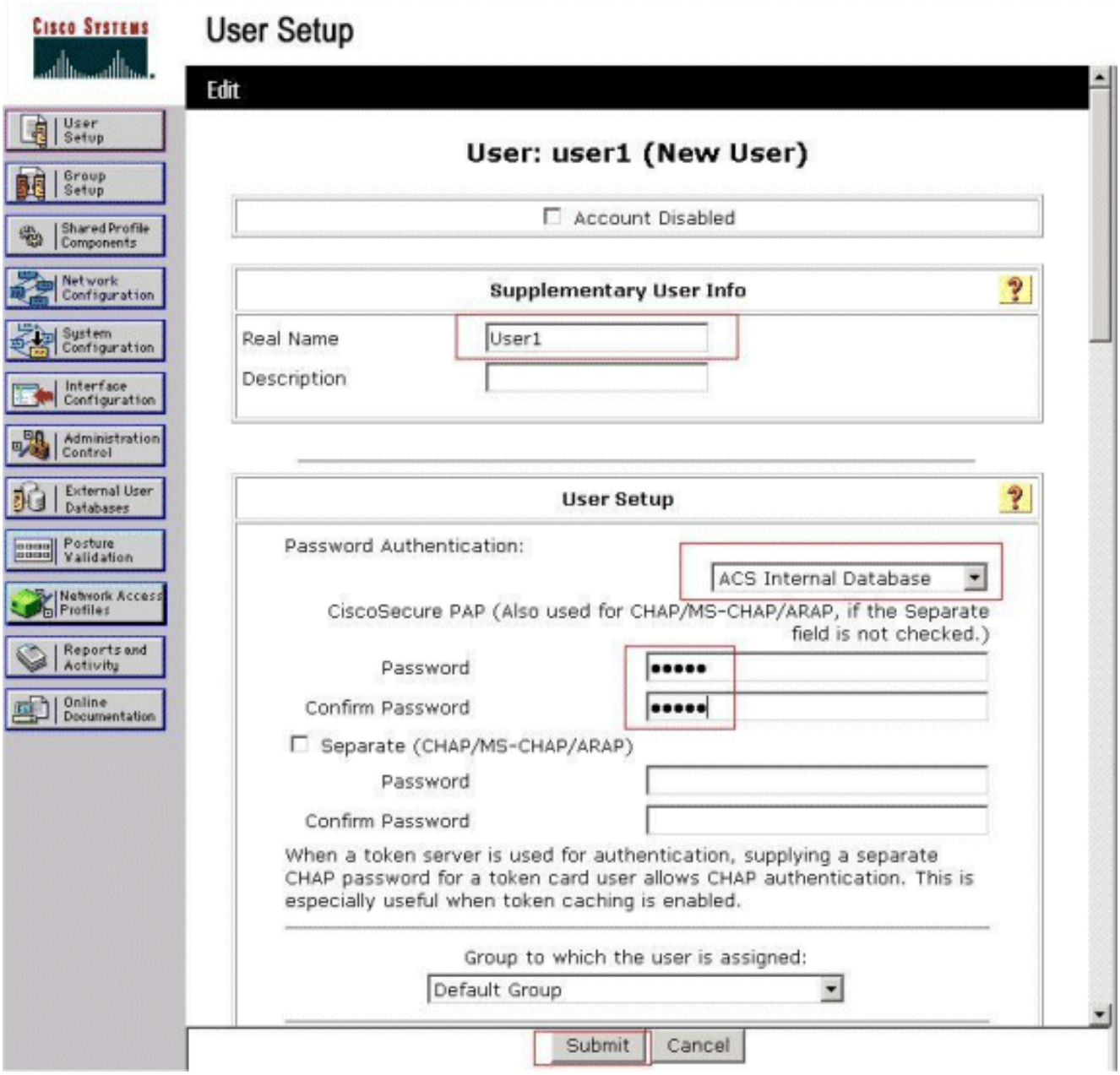
在Cisco Secure ACS上配置使用者資訊

要在Cisco Secure ACS上配置使用者，請執行以下步驟：

1. 從Cisco Secure 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. 預設情況下，PAP用於驗證客戶端。使用者的密碼在**User Setup > Password Authentication > Cisco Secure PAP**下輸入。確保選擇**ACS Internal Database**進行密碼身份驗證。

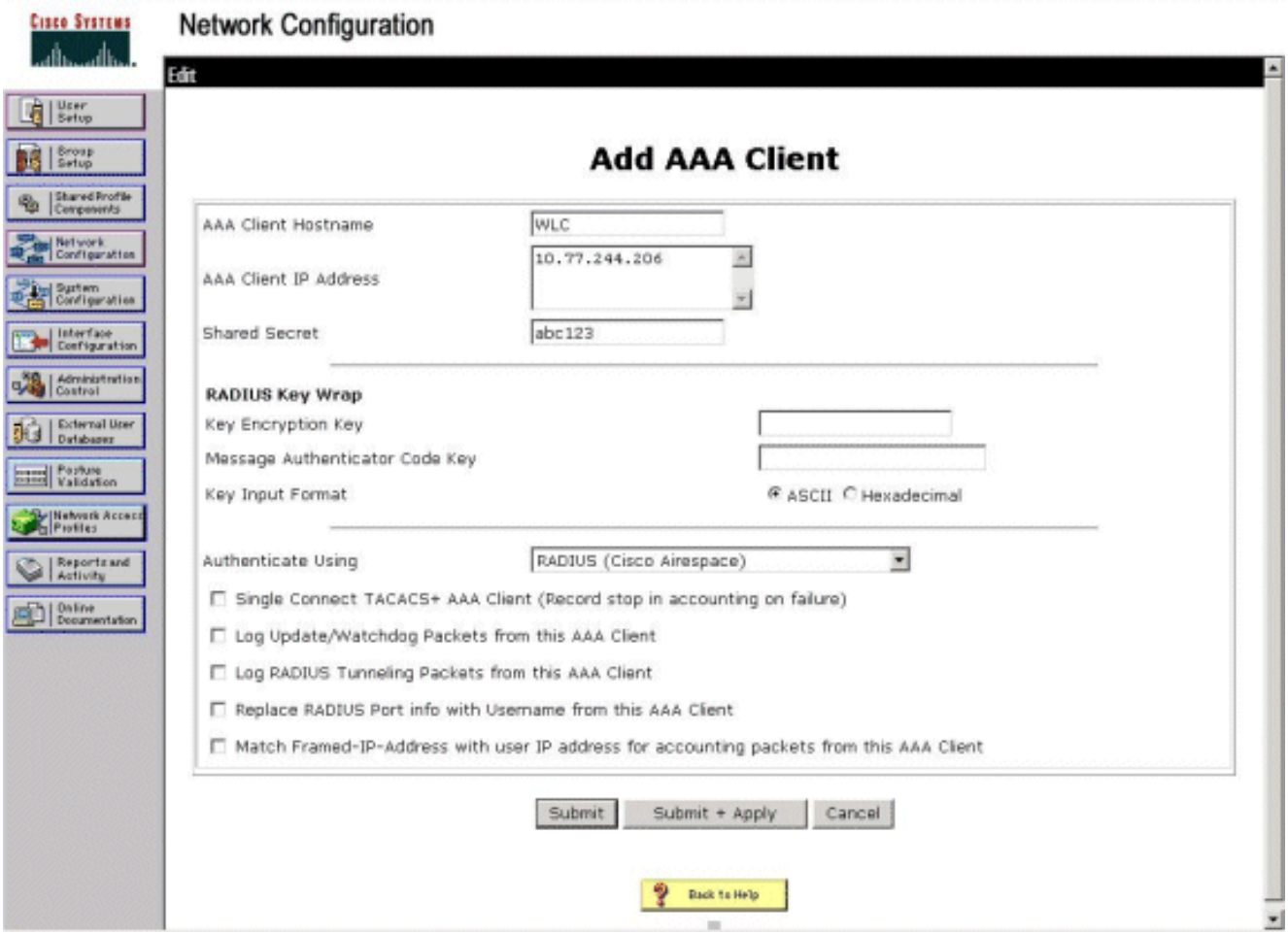


3. 需要為使用者分配使用者所屬的組。選擇**Default Group**。
4. 按一下「**Submit**」。

在Cisco Secure ACS上配置WLC資訊

要在Cisco Secure ACS上配置WLC資訊，請執行以下步驟：

1. 在ACS GUI中，按一下**Network Configuration**頁籤，然後按一下**Add Entry**。
2. 系統將顯示Add AAA client螢幕。
3. 輸入客戶端的名稱。在本範例中，我們使用*WLC*。
4. 輸入客戶端的IP地址。WLC的IP地址是*10.77.244.206*。
5. 輸入共用金鑰和金鑰格式。此專案應與WLC的「**Security**」功能表中建立的專案相符。
6. 選擇**ASCII**作為按鍵輸入格式，在WLC上應該相同。
7. 選擇**RADIUS(Cisco Airespace)**以使用Authenticate，以設定WLC和RADIUS伺服器之間使用的通訊協定。
8. 按一下「**Submit + Apply**」。

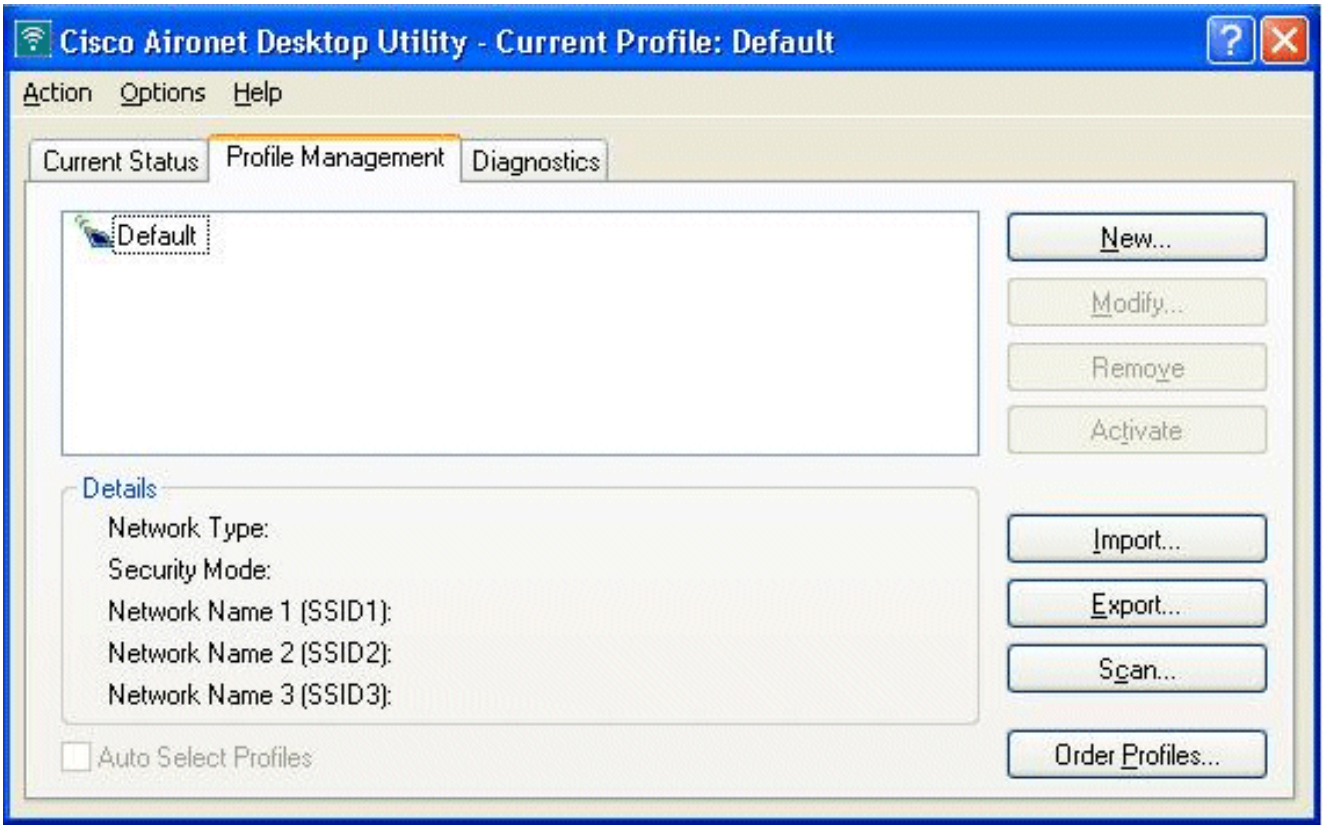


客戶端身份驗證過程

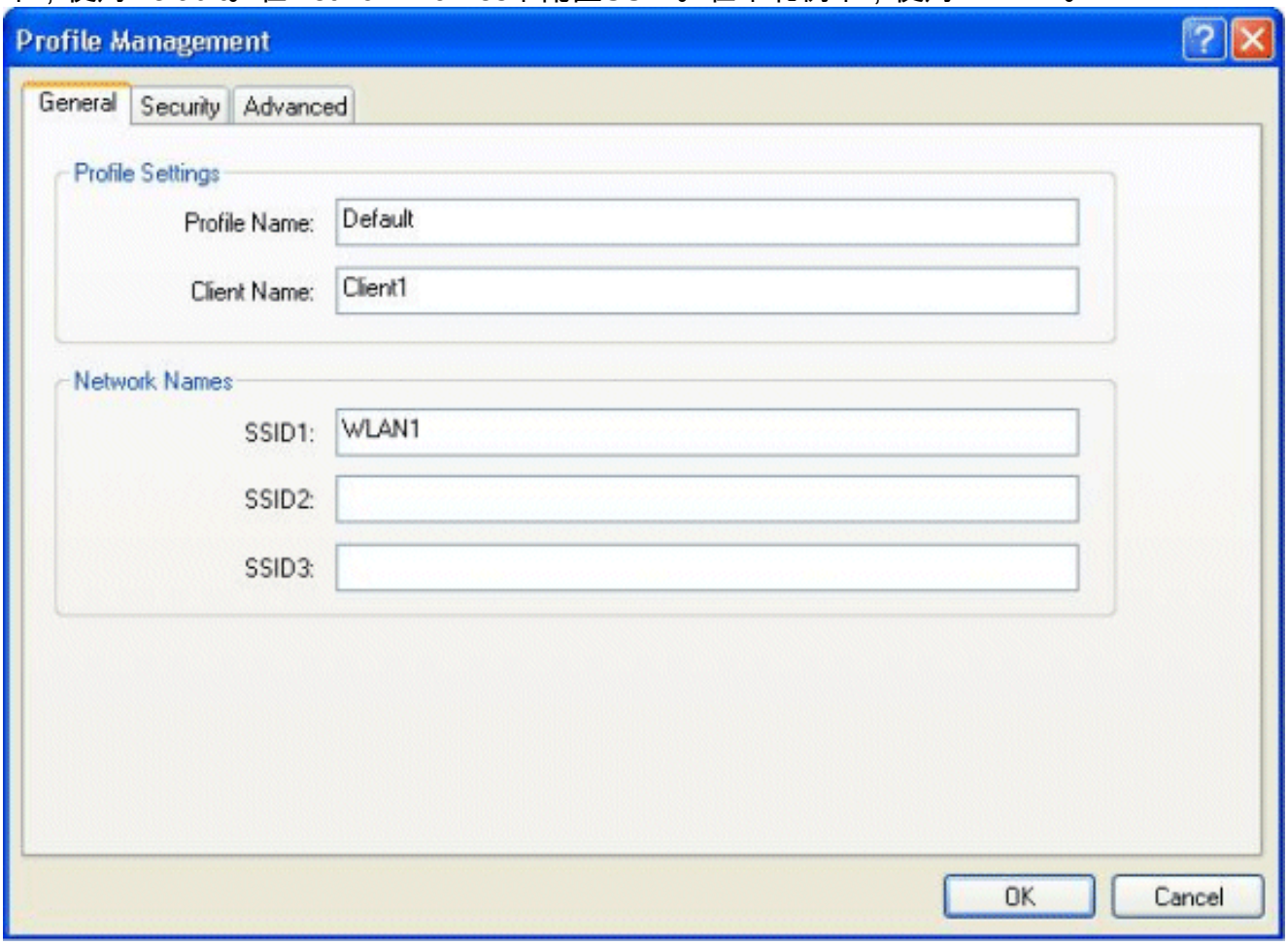
客戶端配置

在本示例中，我們使用Cisco Aironet案頭實用程式執行Web身份驗證。執行以下步驟以配置Aironet案頭實用程式。

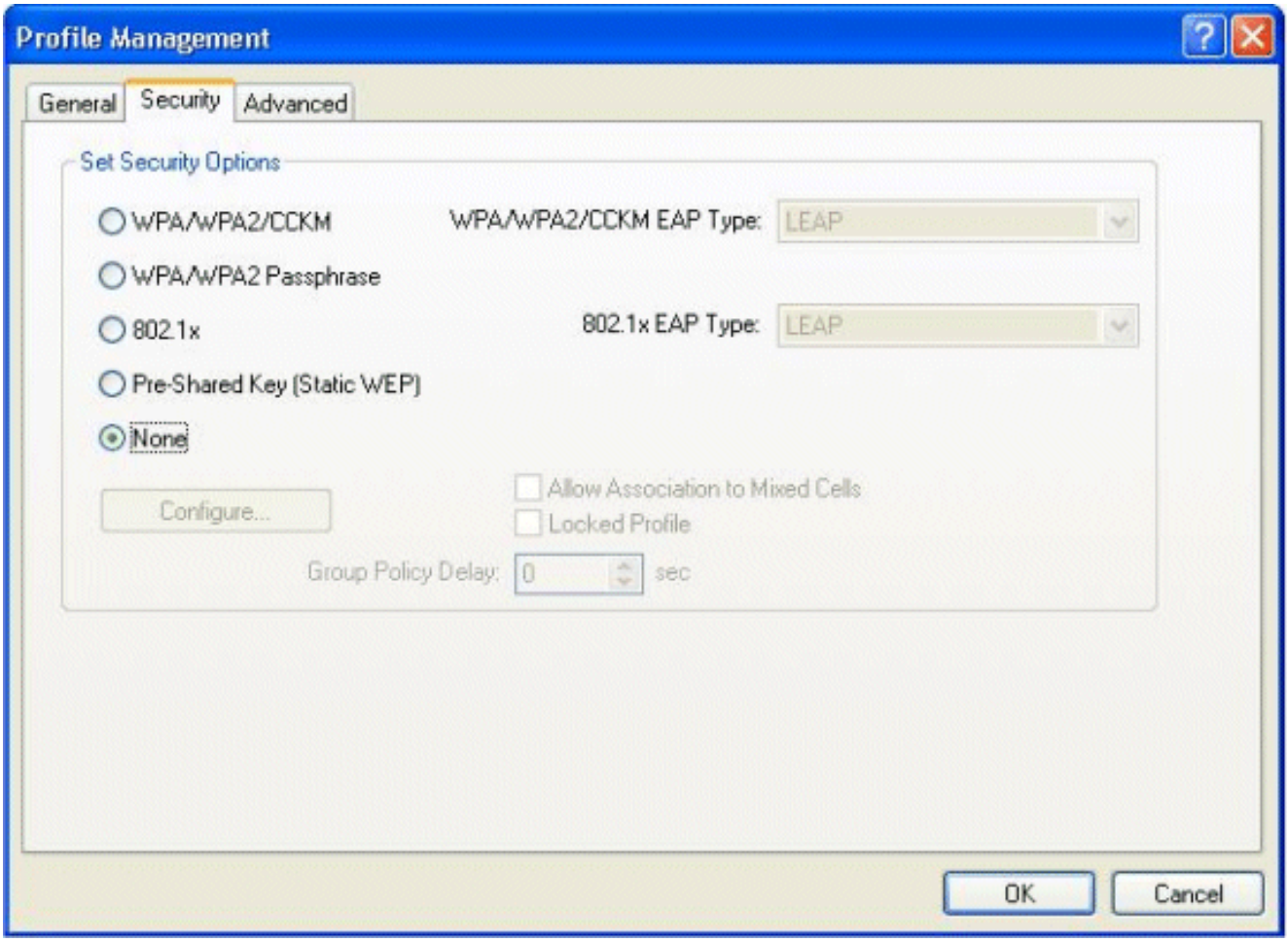
1. 從**開始>Cisco Aironet > Aironet Desktop Utility**開啟Aironet案頭實用程式。
2. 點選**Profile Management選項**卡。



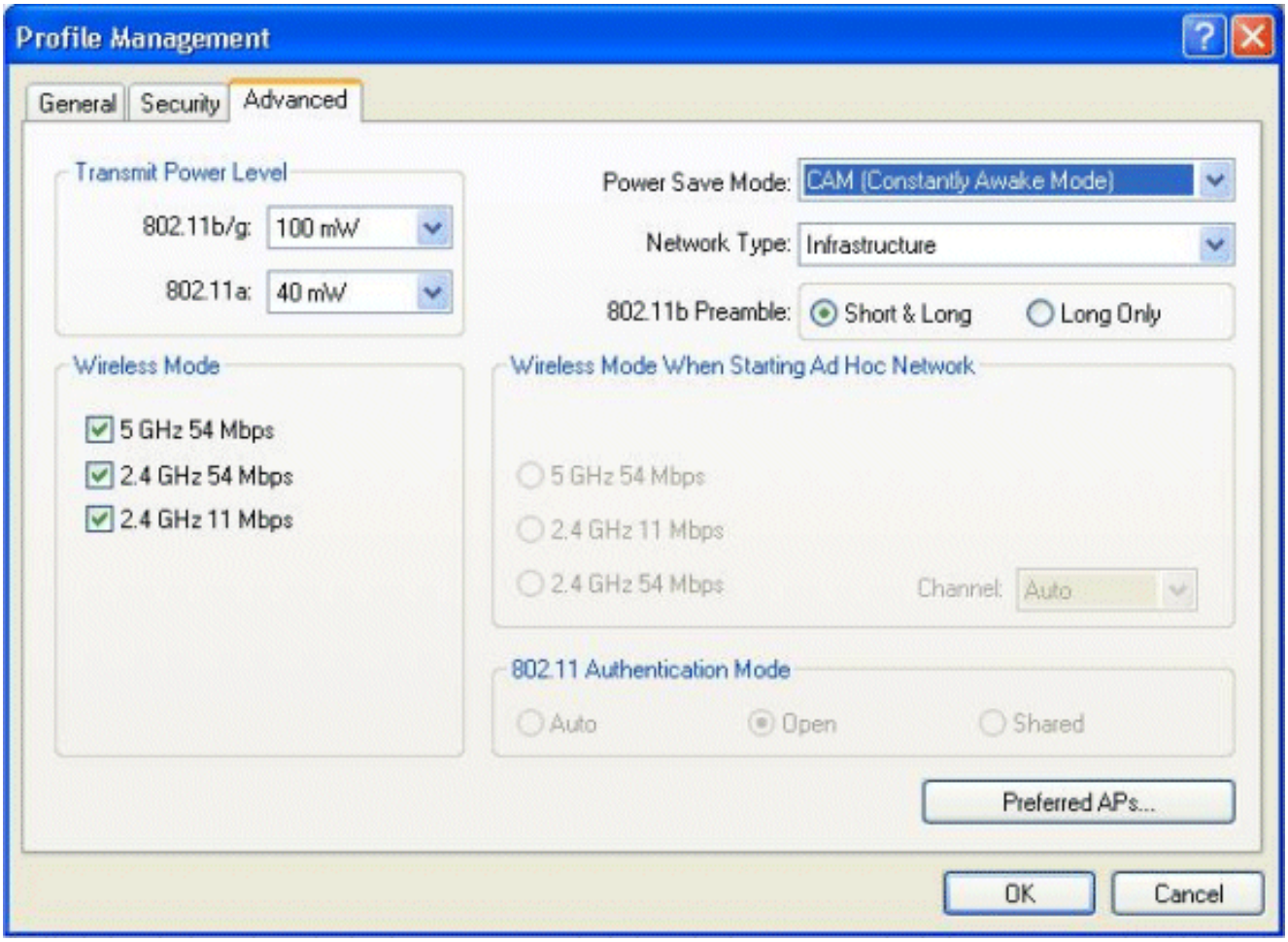
3. 選擇**Default**配置檔案，然後按一下**Modify**。按一下**General**頁籤。配置配置檔名稱。在此範例中，使用*Default*。在Network Names下配置SSID。在本範例中，使用*WLAN*1。



注意：SSID區分大小寫，並且應該與WLC上配置的WLAN匹配。按一下**Security**頁籤。為Web驗證選擇**None**作為Security。



按一下**Advanced**頁籤。在「**Wireless Mode**」選單下，選擇無線客戶端與LAP通訊的頻率。在**Transmit Power Level**下，選擇WLC上設定的電源。保留「Power Save Mode（節能模式）」的預設值。選擇**Infrastructure**作為Network Type。將802.11b前導碼設定為**Short & Long**以獲得更好的相容性。按一下「**OK**」（確定）。

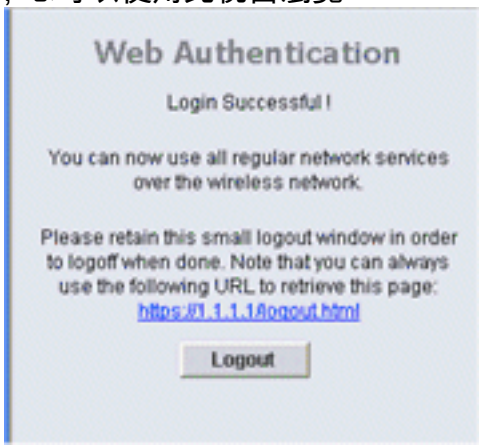


4. 在客戶端軟體上配置配置檔案後，客戶端將成功關聯並從為管理介面配置的VLAN池接收IP地址。

使用者端登入程式

本節說明如何進行使用者端登入。

1. 開啟瀏覽器視窗並輸入任何URL或IP地址。這會將Web驗證頁面導向使用者端。如果控制器執行的是低於3.0的任何版本，使用者必須輸入*https://1.1.1.1/login.html*以開啟Web驗證頁面。此時將顯示一個安全警報視窗。
2. 按一下「**Yes**」以繼續。
3. 出現「Login（登入）」視窗時，輸入在RADIUS伺服器上配置的使用者名稱和密碼。如果登入成功，您將看到兩個瀏覽器視窗。較大的視窗表示登入成功，您可以使用此視窗瀏覽Internet。使用較小的視窗，以便在使用完訪客網路後註銷。

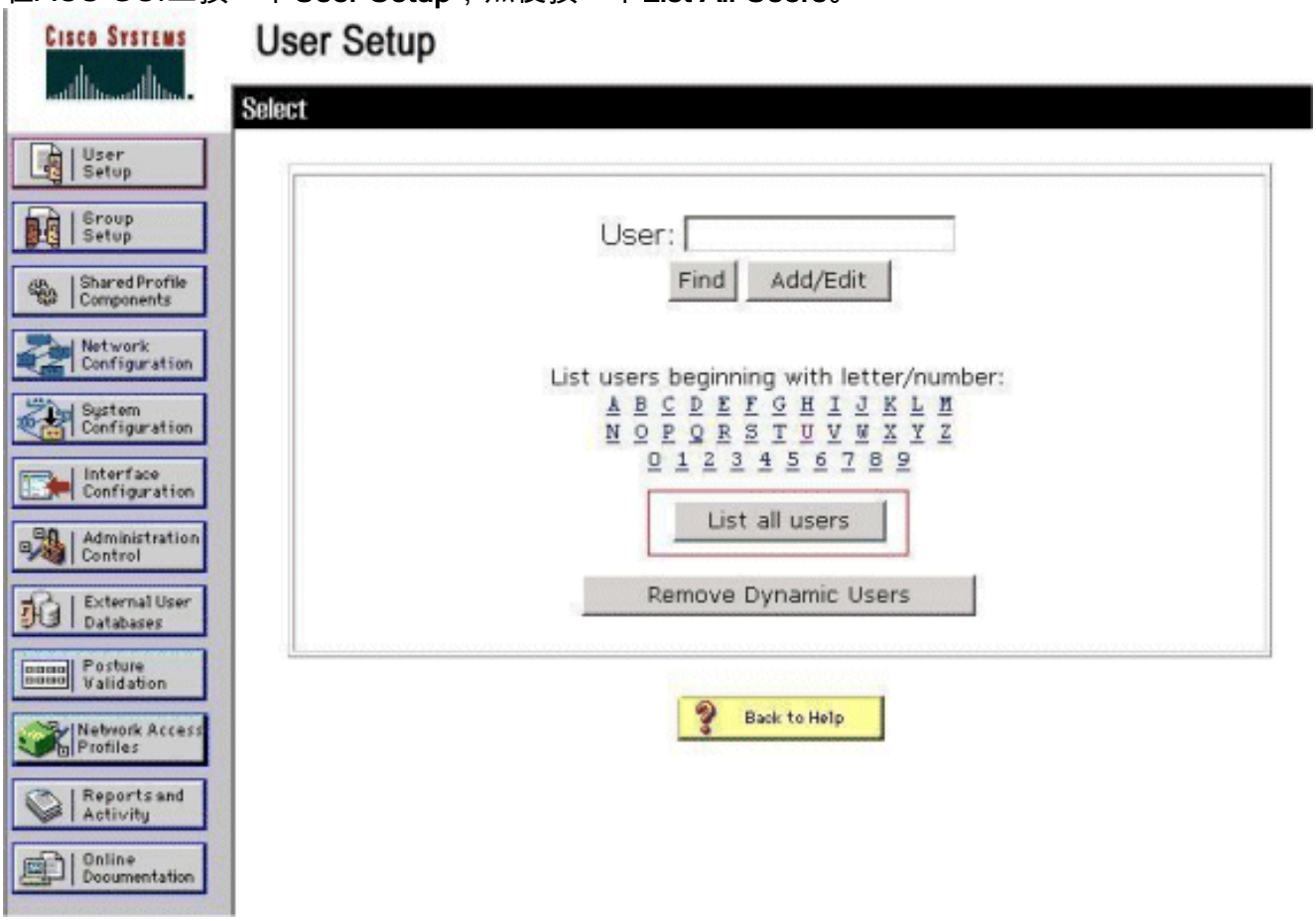


驗證

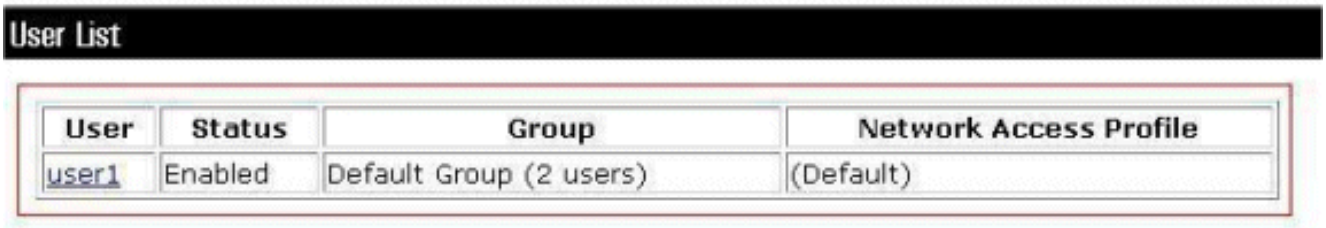
要成功進行Web身份驗證，您需要檢查裝置是否以適當的方式配置。本節介紹如何驗證過程中使用的裝置。

檢驗ACS

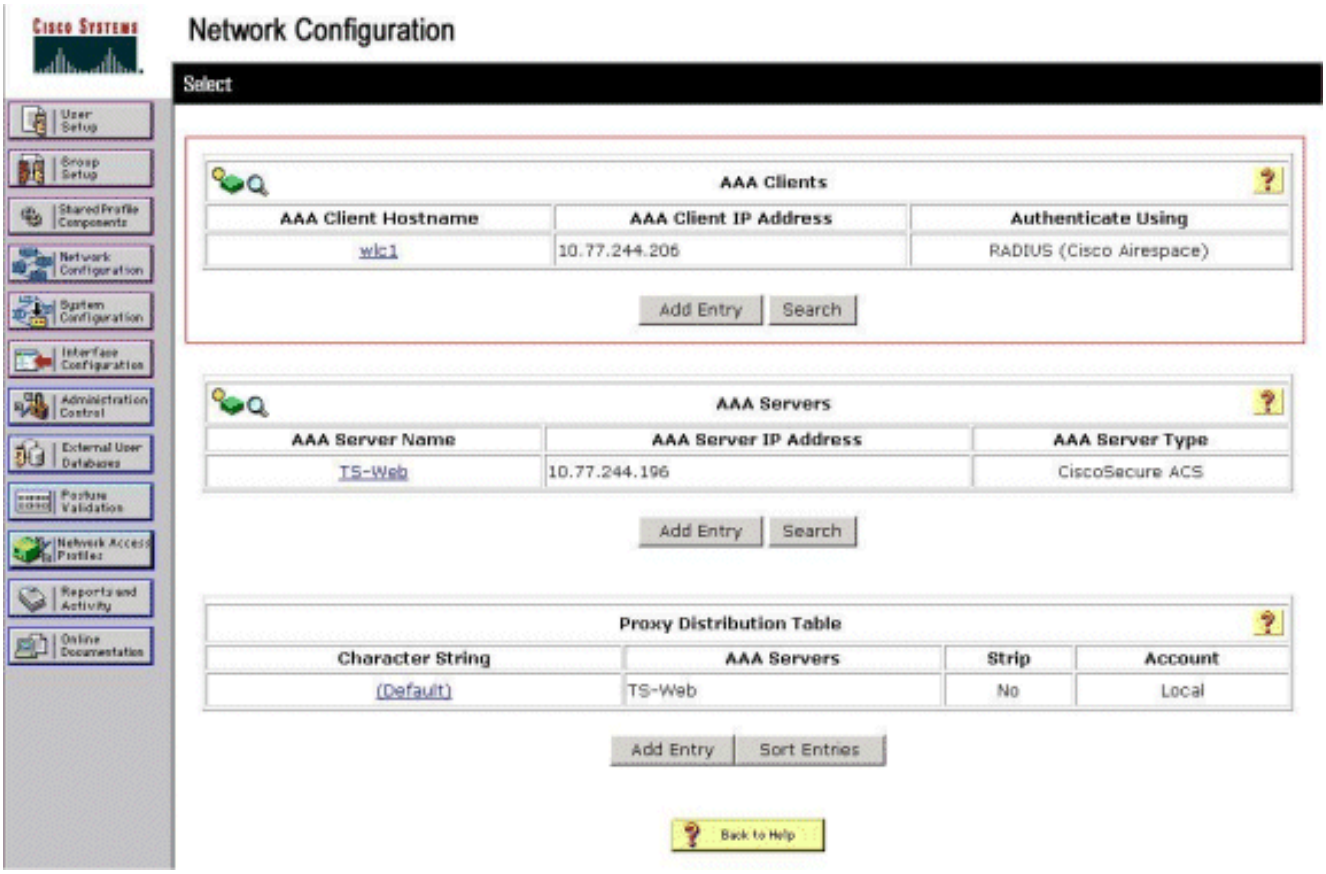
1. 在ACS GUI上按一下**User Setup**，然後按一下**List All Users**。



確保Status of the User為*Enabled*，並且Default組對映到使用者。

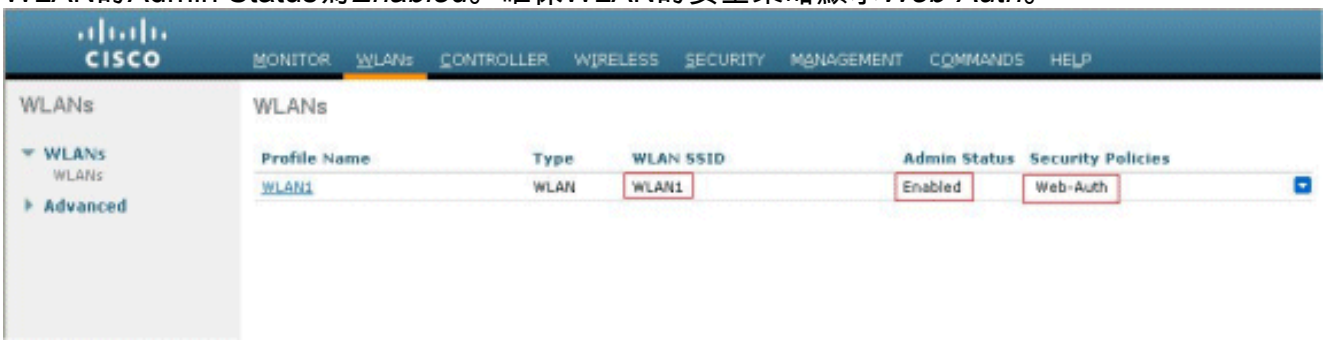


2. 按一下**Network Configuration**索引標籤，然後檢視**AAA Clients**表，以驗證WLC是否已設定為AAA使用者端。

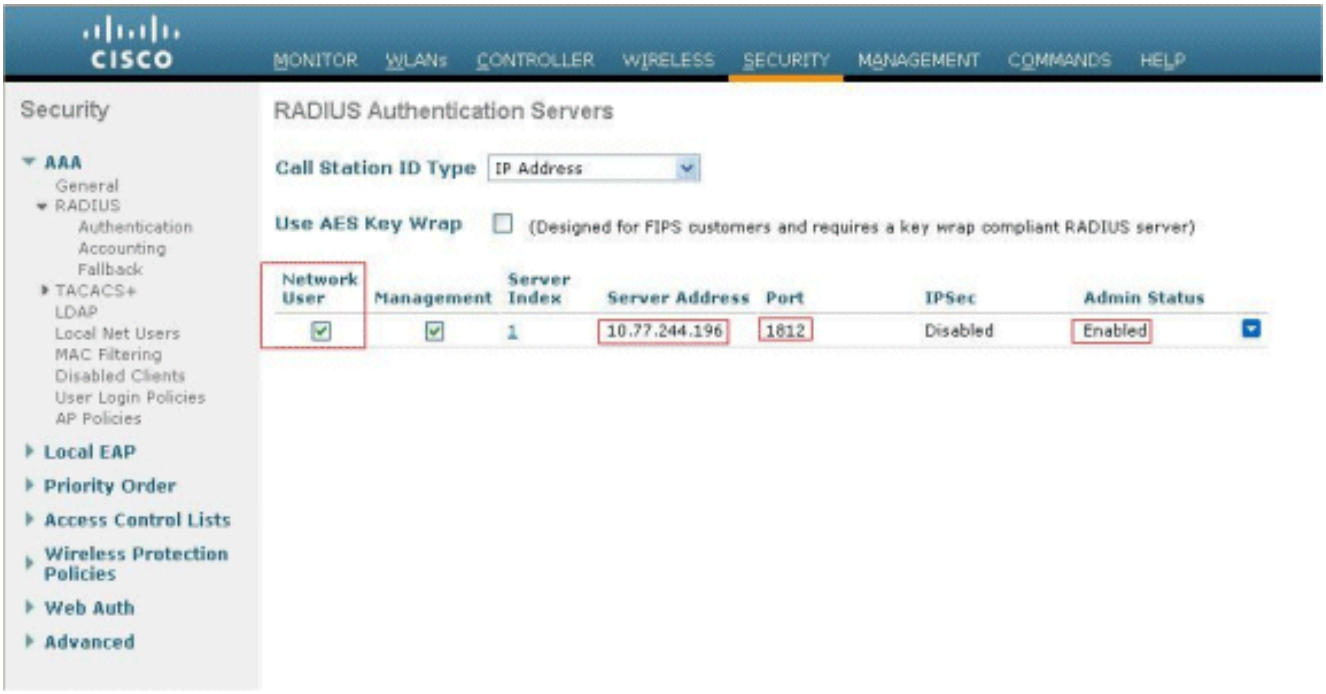


驗證WLC

1. 在WLC GUI上按一下**WLANs**選單。確保頁面中列出了用於Web身份驗證的WLAN。確保WLAN的Admin Status為*Enabled*。確保WLAN的安全策略顯示*Web-Auth*。



2. 在WLC GUI上按一下「**SECURITY**」選單。確保頁面上列出了Cisco Secure ACS(10.77.244.196)。確保選中「Network User（網路使用者）」框。確認連線埠為*1812*，且管理狀態為*Enabled*。



疑難排解

Web驗證不成功的原因有很多，對無線LAN控制器(WLC)上的Web驗證進行排解疑難檔案清楚說明這些原因。

疑難排解指令

注意：使用這些debug命令之前，請先參閱有關Debug命令的重要資訊。

Telnet至WLC並發出以下命令對驗證進行疑難排解：

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
Fri Sep 24 13:59:52 2010:       resultCode................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
0000001
Fri Sep 24 13:59:52 2010:       proxyState................................00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address.................
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class.............................
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
```

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                              vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] User-Name.............................
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Nas-Port..............................
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[03] Nas-Ip-Address........................
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[04] Framed-IP-Address.....................
.....0x0a4df4c7 (172881095) (4 bytes)
```

- debug aaa detail enable

失敗的身份驗證嘗試列在Reports and Activity > Failed Attempts處的選單中。

相關資訊

- 無線 LAN 控制器 Web 驗證組態範例
- 對無線 LAN 控制器 (WLC) 上的 Web 驗證進行排解疑難
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 在無線LAN控制器(WLC)上使用LDAP的Web驗證組態範例
- 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）。