無線LAN控制器啟動顯示頁面重新導向組態範例

目錄

簡介

本檔案介紹如何在無線LAN控制器上設定啟動顯示頁面重新導向功能。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解LWAPP安全解決方案
- 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：

- 執行韌體版本5.0的Cisco 4400系列無線LAN控制器(WLC)
- 思科1232系列輕型接入點(LAP)
- 執行韌體版本4.1的Cisco Aironet 802.a/b/g無線使用者端配接器
- 運行版本4.1的Cisco Secure ACS伺服器
- 任何第三方外部Web伺服器

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。

背景資訊

啟動顯示頁面Web重新導向是無線LAN控制器版本5.0中引入的功能。使用此功能，使用者在802.1x驗證完成後將被重定向到特定網頁。使用者開啟瀏覽器（設定為預設首頁）或嘗試存取URL時，會發生重新導向。重新導向網頁完成後，使用者會獲得網路的完整存取許可權。

您可以在遠端驗證撥入使用者服務(RADIUS)伺服器上指定重新導向頁面。應將RADIUS伺服器設定為在802.1x驗證成功時將思科av配對url-redirect RADIUS屬性傳回到無線LAN控制器。

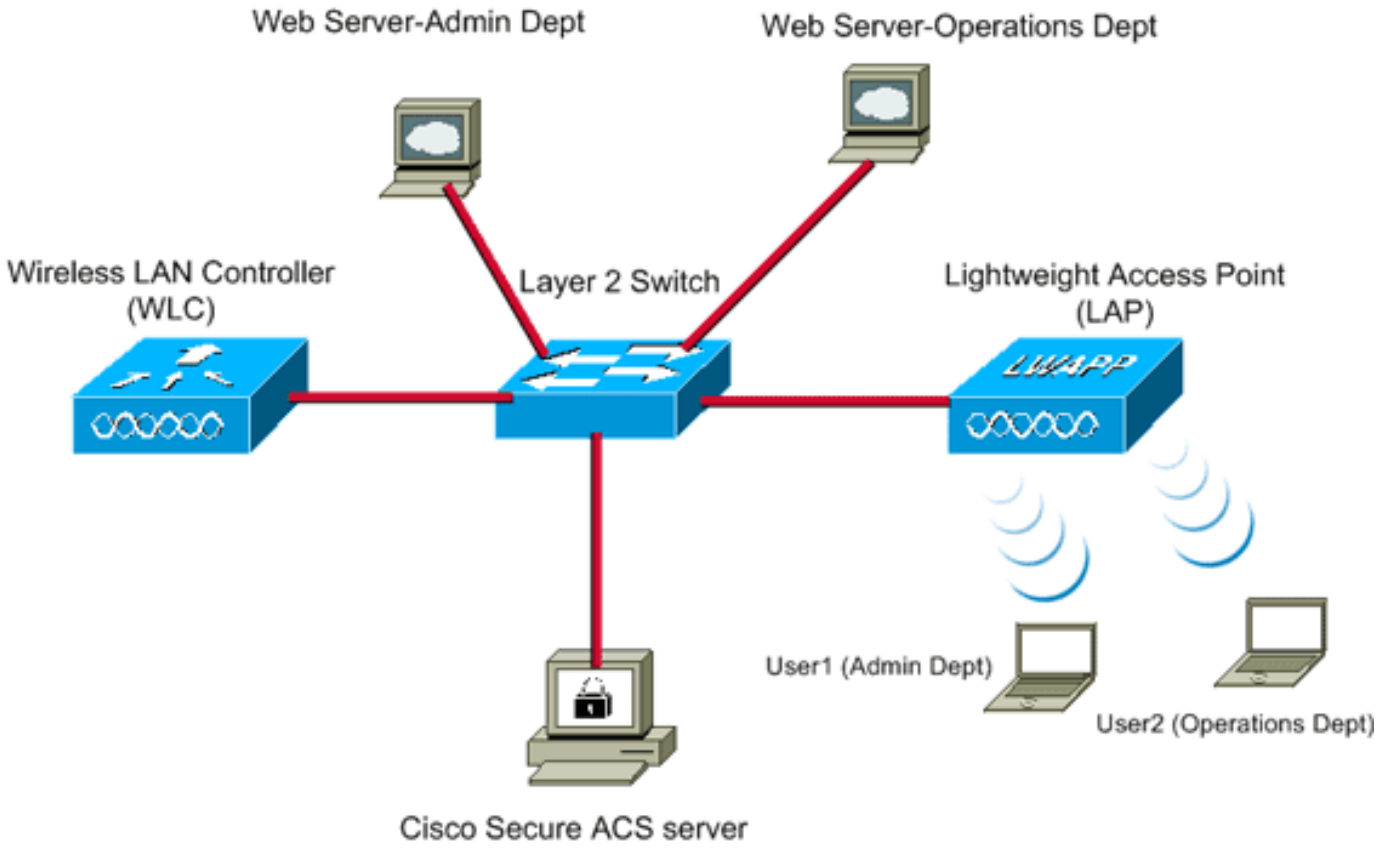
啟動顯示頁面Web重新導向功能僅適用於針對802.1x或WPA/WPA2第2層安全性設定的WLAN。

網路設定

在以下範例中，Cisco 4404 WLC和Cisco 1232系列LAP透過第2層交換器連線。Cisco Secure ACS伺服器（充當外部RADIUS伺服器）也連線到同一台交換機。所有裝置都位於同一個子網中。

LAP最初註冊到控制器。您必須建立兩個WLAN：一個用於**管理部**使用者，另一個用於**運營部**使用者。兩個無線LAN都使用WPA2/AES（EAP-FAST用於身份驗證）。兩種WLAN均使用啟動顯示頁面重新導向功能將使用者重新導向到適當的首頁URL（在外部Web伺服器上）。

本檔案會使用以下網路設定：



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

下一節說明如何為此設定配置裝置。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

完成以下步驟，將裝置設定為使用啟動顯示頁面重新導向功能：

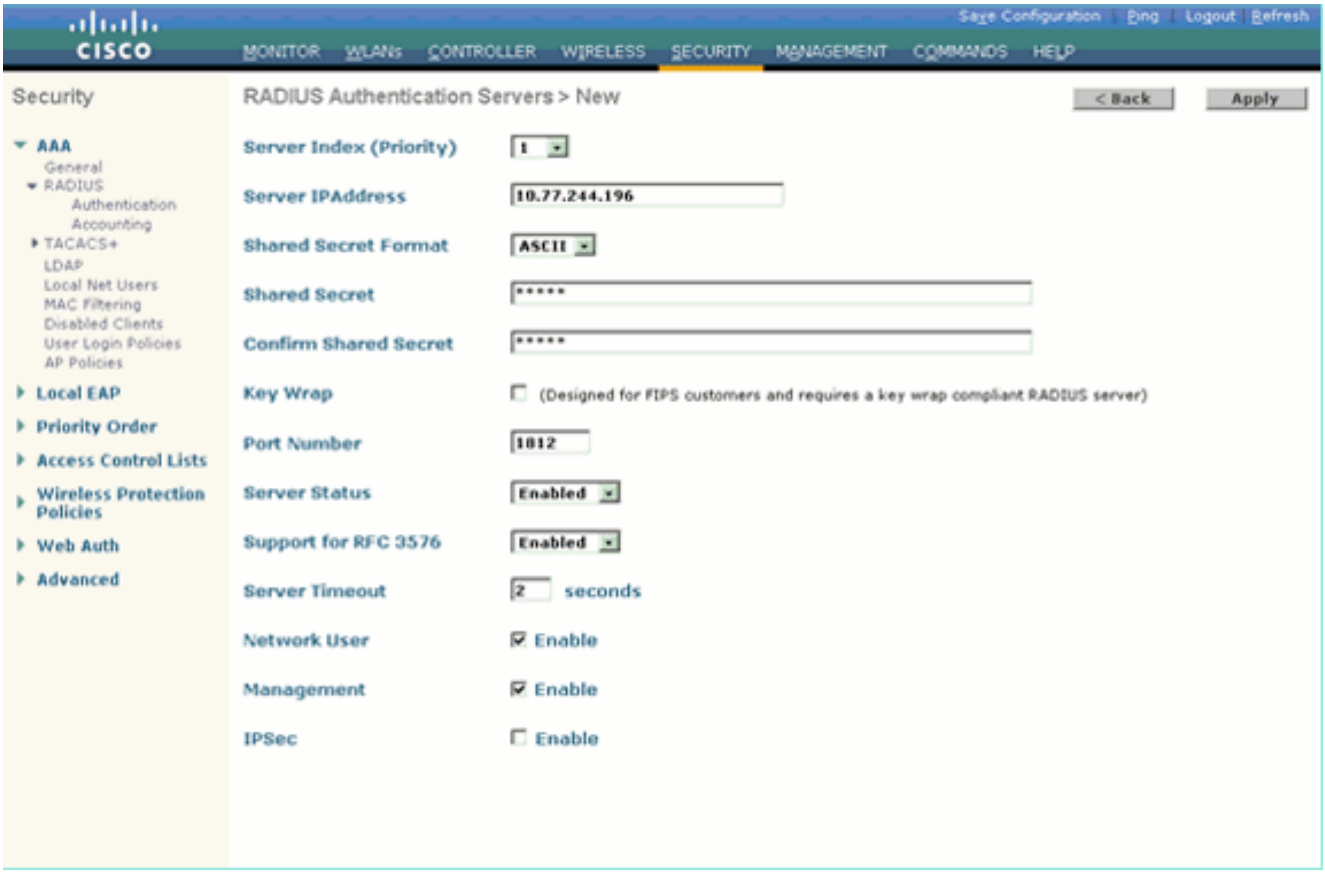
1. 配置WLC以通過Cisco Secure ACS伺服器進行RADIUS身份驗證。
2. 為管理部門和運營部門配置WLAN。
3. 配置Cisco Secure ACS以支援啟動顯示頁面重定向功能。

步驟1.配置WLC以通過Cisco Secure ACS伺服器進行RADIUS身份驗證。

需要設定WLC，才能將使用者認證轉送到外部RADIUS伺服器。

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。
2. 按一下**New**以定義RADIUS伺服器。
3. 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。

4. 按一下「**Apply**」。

步驟2.為管理和操作部門配置WLAN。

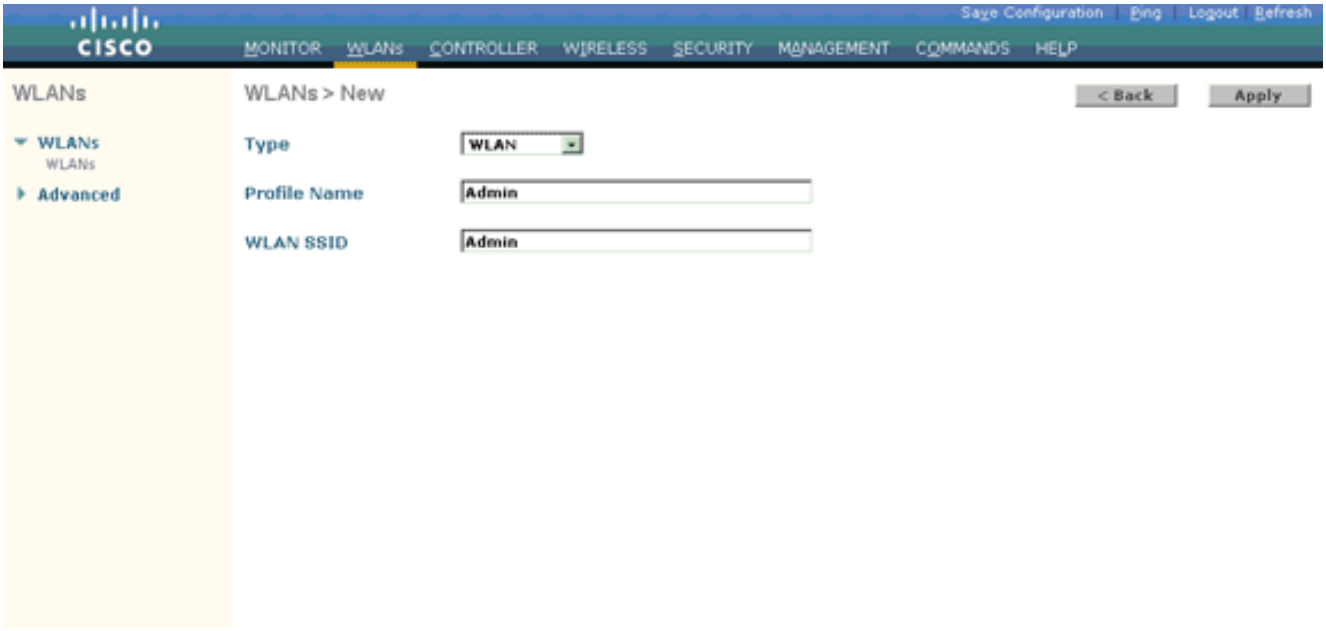
在此步驟中，您配置客戶端用於連線無線網路的兩個WLAN（一個用於管理部門，另一個用於運營部門）。

管理部門的WLAN SSID將為*Admin*。操作部門的WLAN SSID為操作。

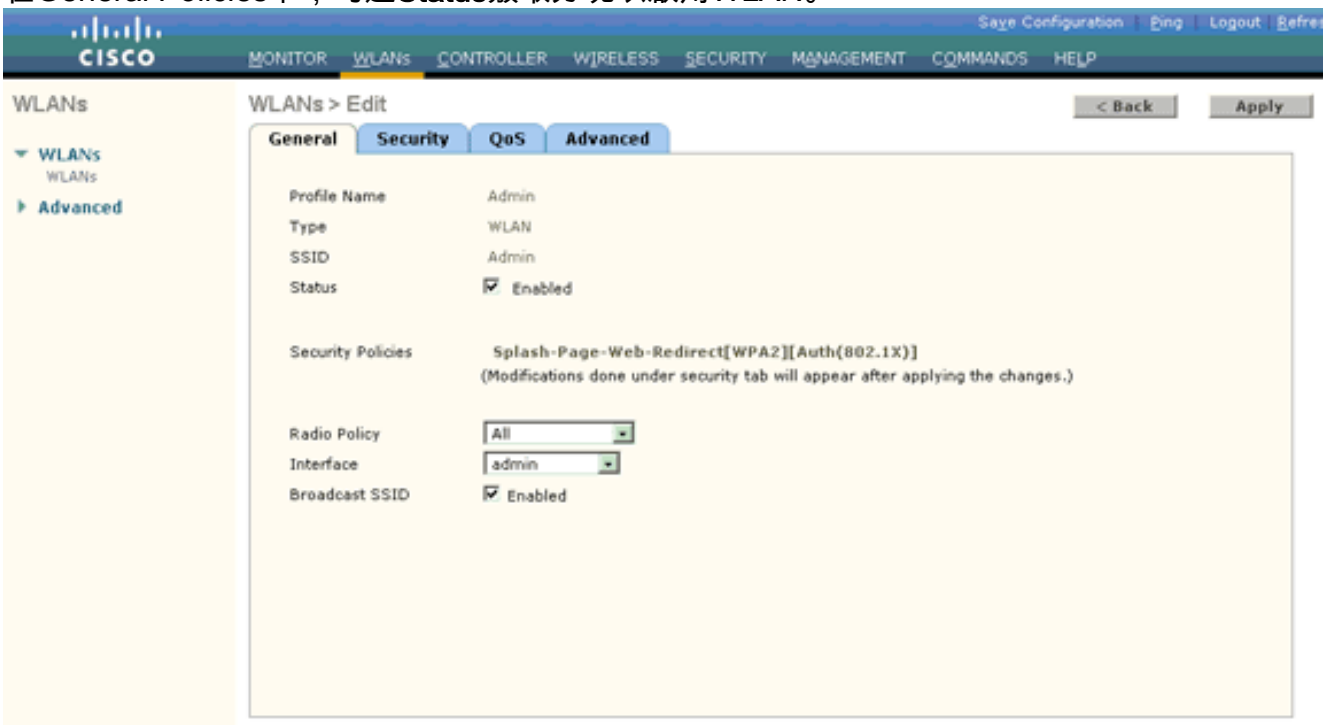
使用EAP-FAST驗證以啟用WPA2作為WLAN上的第2層安全機制，並使用Web策略 — 啟動顯示頁面Web重新導向功能作為第3層安全方法。

完成以下步驟即可設定WLAN及其相關引數：

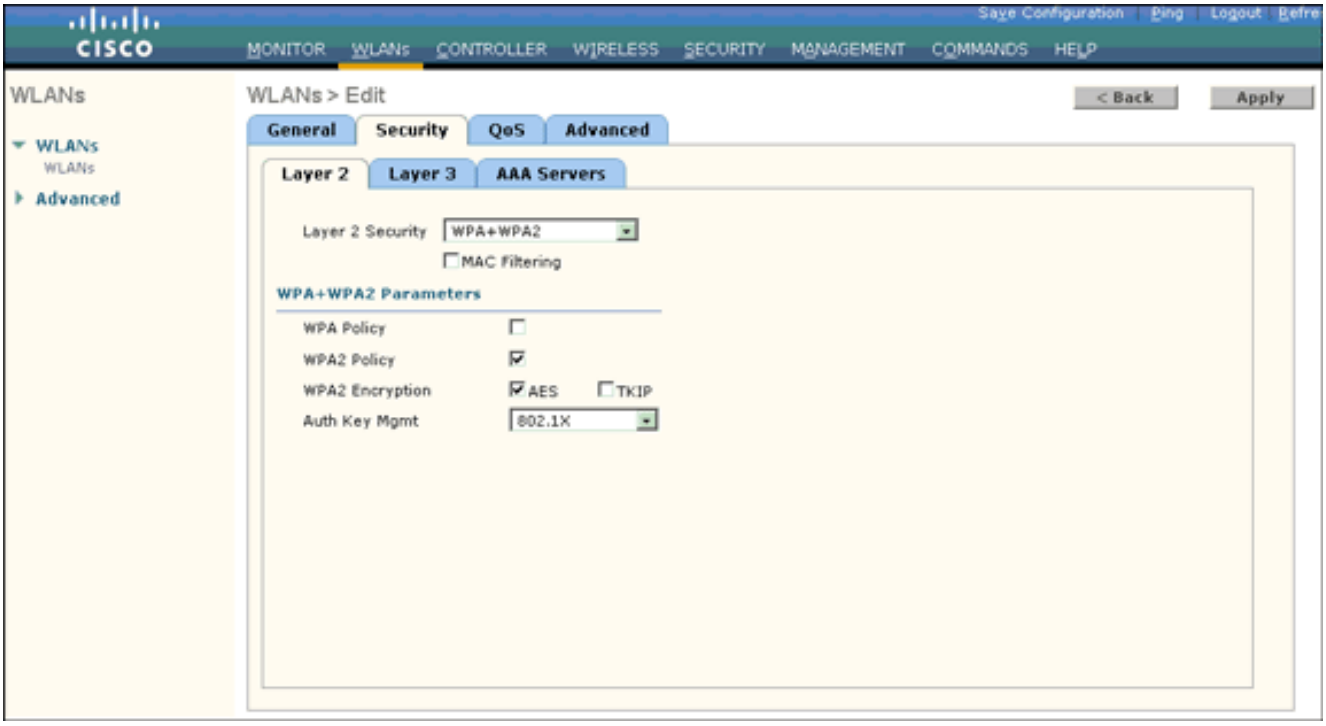
1. 從控制器的GUI中按一下「**WLANs**」，以顯示「WLANs」頁面。此頁面列出控制器上存在的WLAN。
2. 按一下**New**以建立一個新的WLAN。



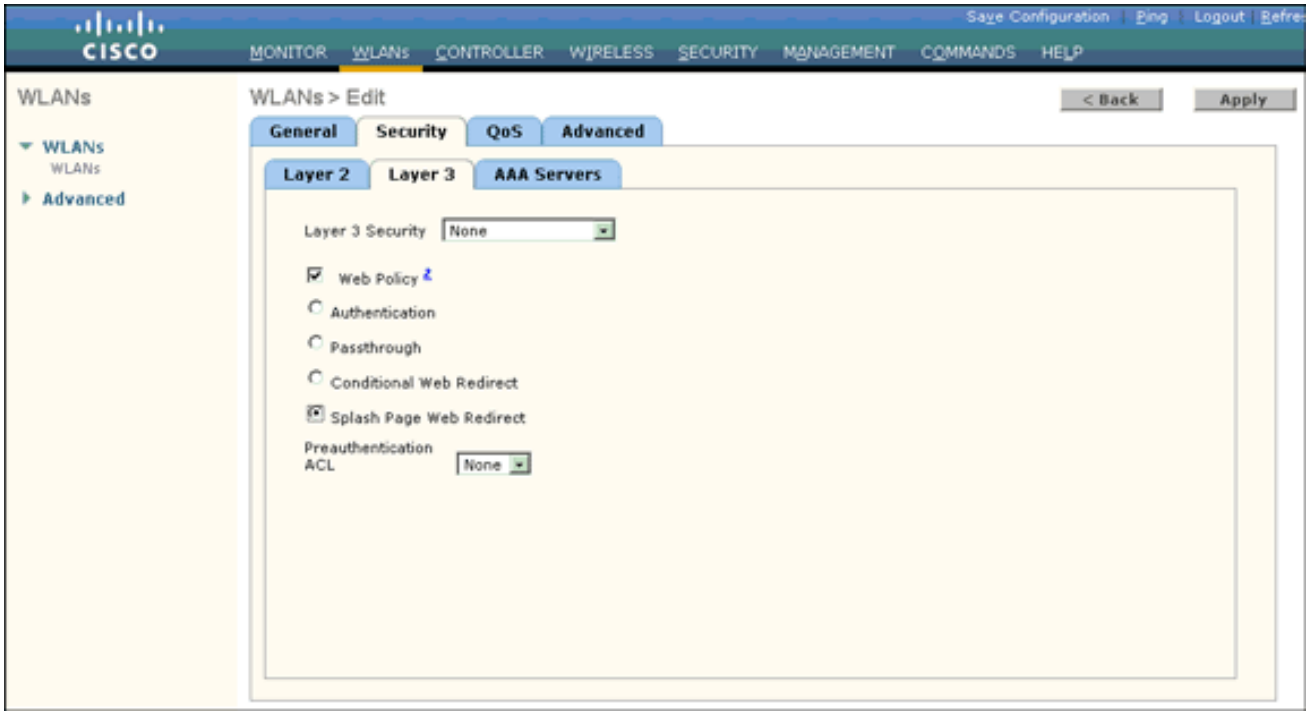
3. 在WLANs > New頁面上輸入WLAN SSID名稱和配置檔名稱。
4. 按一下「**Apply**」。
5. 首先為管理部門建立WLAN。建立新的WLAN後，系統會顯示新WLAN的WLAN > Edit頁面。在此頁面上，您可以定義此WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和高級引數。
6. 在General Policies下，勾選**Status**覈取方塊以啟用WLAN。



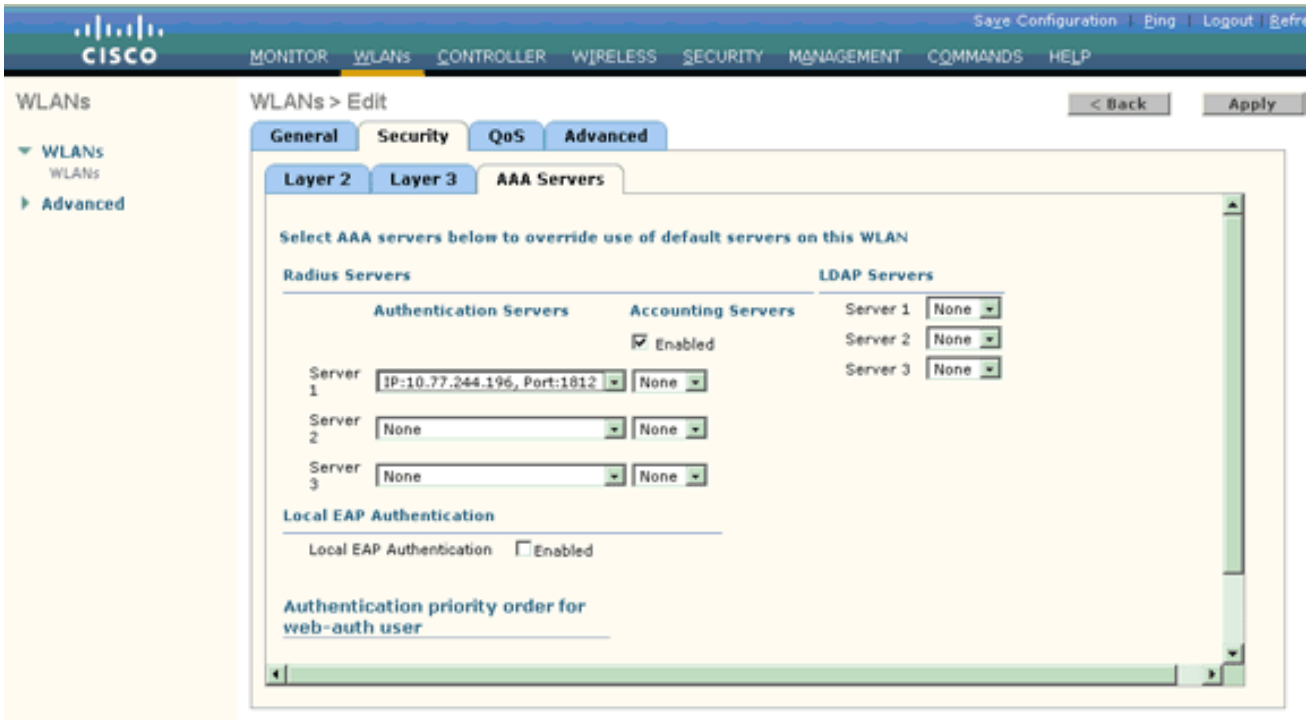
7. 按一下**Security**頁籤，然後按一下**Layer 2**頁籤。
8. 從Layer 2 Security下拉選單中選擇**WPA+WPA2**。此步驟為WLAN啟用WPA身份驗證。
9. 在WPA+WPA2引數下，選中**WPA2 Policy**和**AES Encryption**覈取方塊。



10. 從Auth Key Mgmt下拉選單中選擇**802.1x**。此選項為WLAN啟用具有802.1x/EAP身份驗證和AES加密的WPA2。
11. 按一下**Layer 3 Security**頁籤。
12. 選中**Web Policy**框，然後按一下**Splash Page Web Redirect**單選按鈕。此選項可啟用啟動顯示頁面Web重新導向功能。



13. 按一下**AAA Servers**頁籤。
14. 在Authentication Servers下，從Server 1下拉選單中選擇適當的伺服器IP地址。



在本示例中，10.77.244.196用作RADIUS伺服器。

15. 按一下「**Apply**」。
16. 重複步驟2至15，為運營部門建立WLAN。WLANs頁面列出您建立的兩個WLAN。

請注意，安全策略包括啟動顯示頁面重新導向。

步驟3.配置Cisco Secure ACS以支援啟動顯示頁面重定向功能。

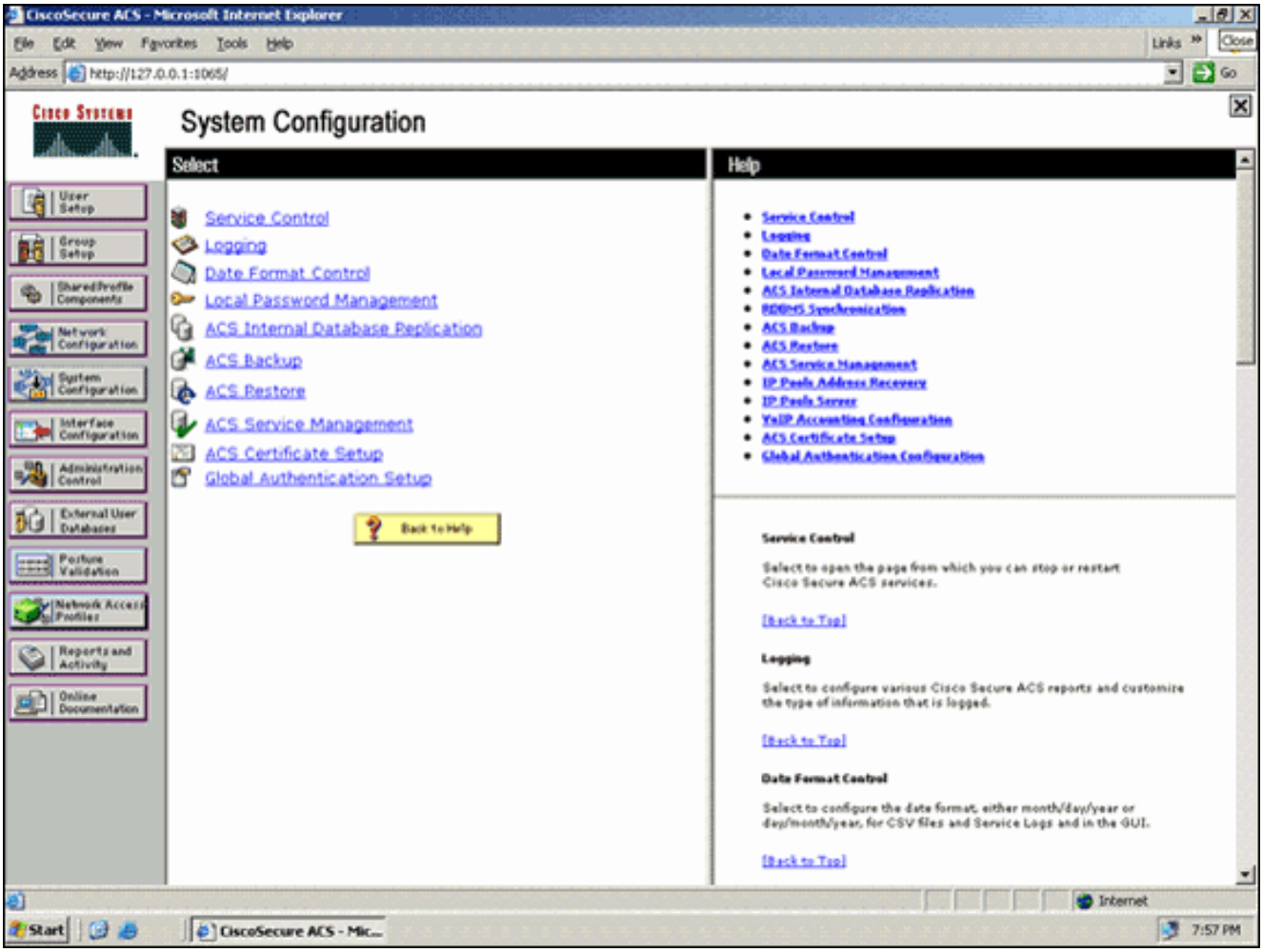
下一步是為此功能設定RADIUS伺服器。RADIUS伺服器需要執行EAP-FAST驗證以驗證使用者端憑證，並在成功驗證後，將使用者重新導向至Cisco av配對*url-redirect* RADIUS屬性中指定的網址（在外部Web伺服器上）。

配置Cisco Secure ACS進行EAP-FAST身份驗證

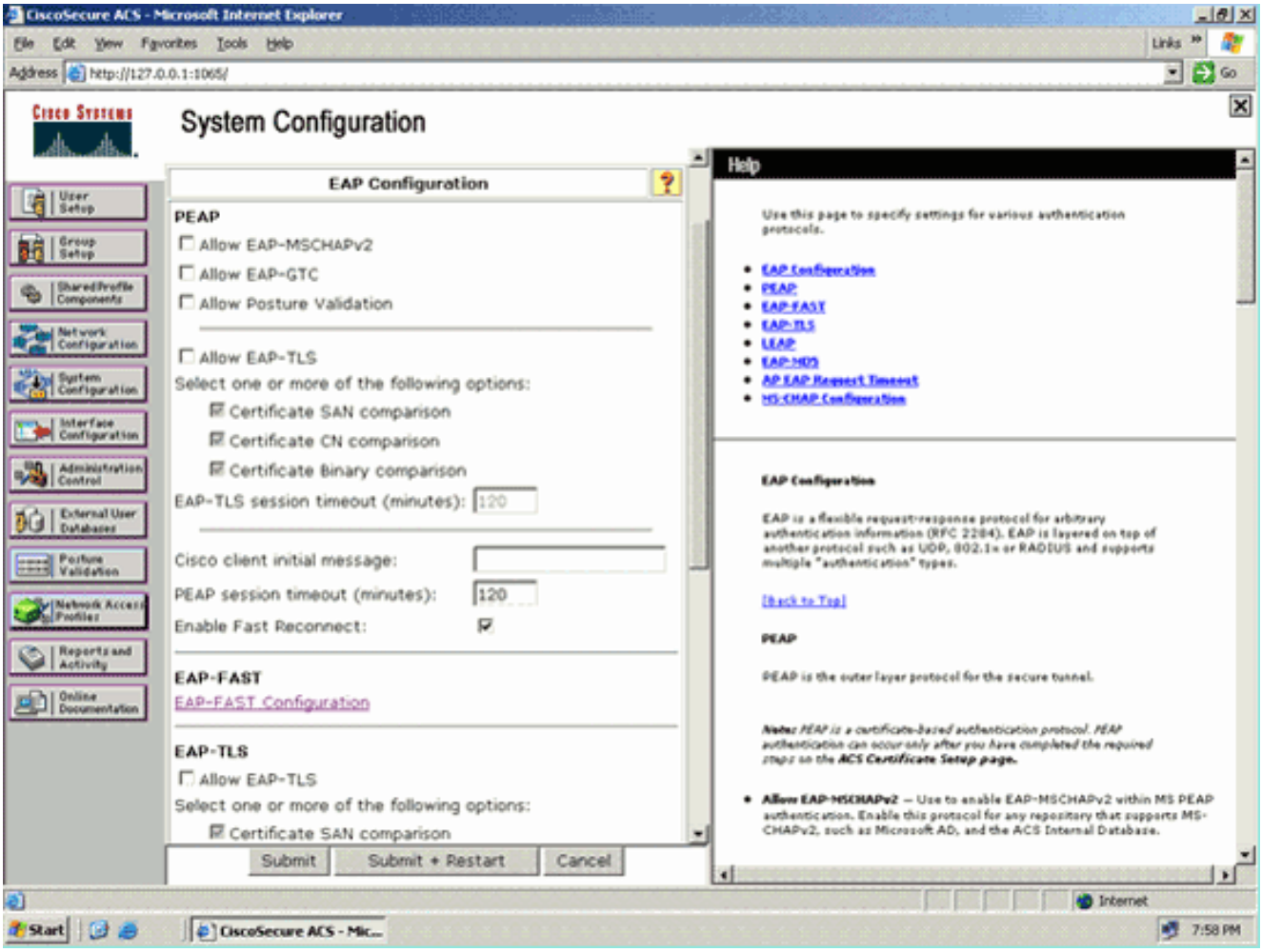
注意：本檔案假設無線LAN控制器作為AAA使用者端新增到Cisco Secure ACS。

完成以下步驟，以便在RADIUS伺服器中設定EAP-FAST驗證：

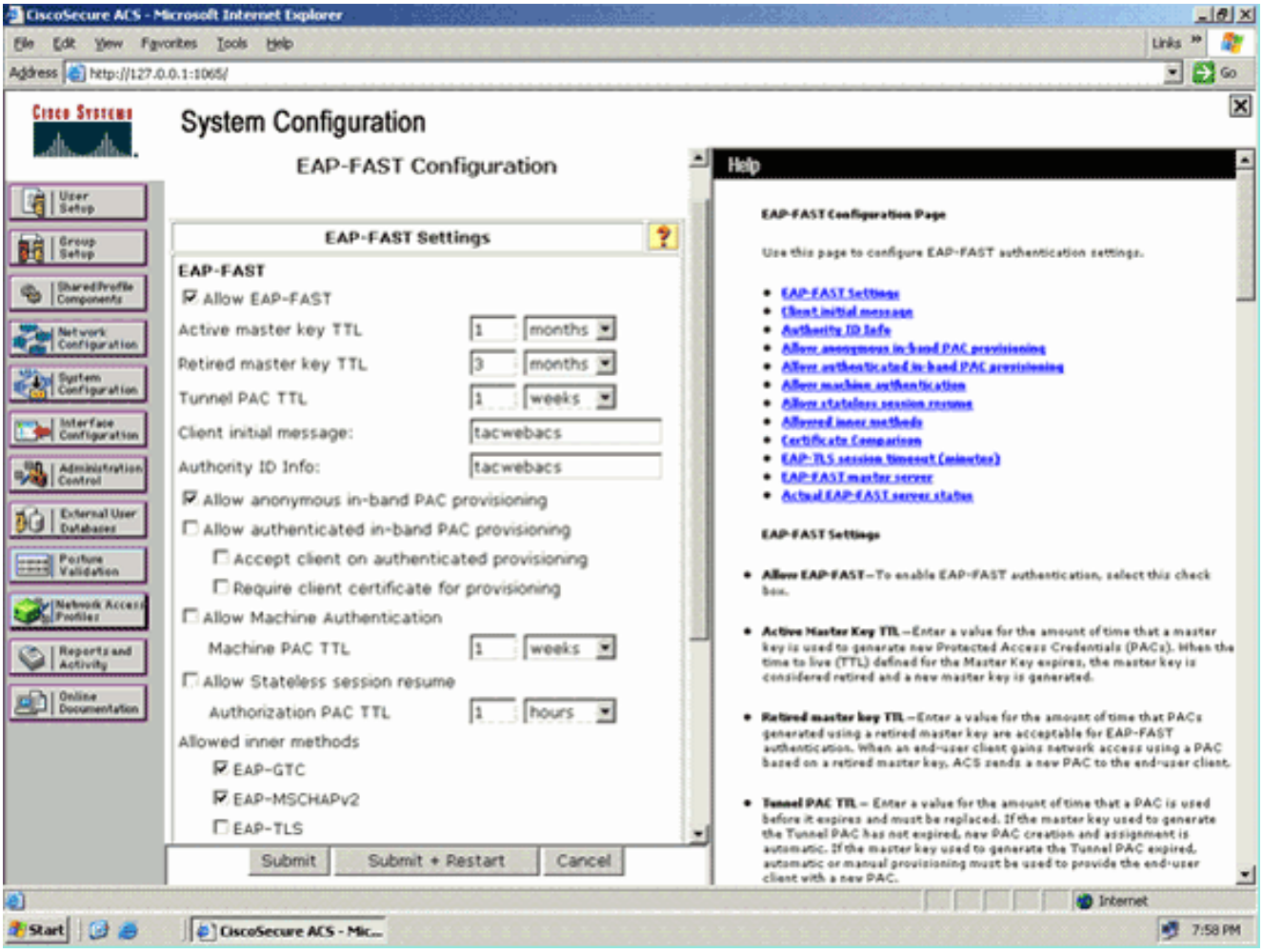
1. 在RADIUS伺服器GUI中按一下**System Configuration**，然後在System Configuration頁面中選擇**Global Authentication Setup**。



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**覈取方塊以便在RADIUS伺服器中啟用EAP-FAST。



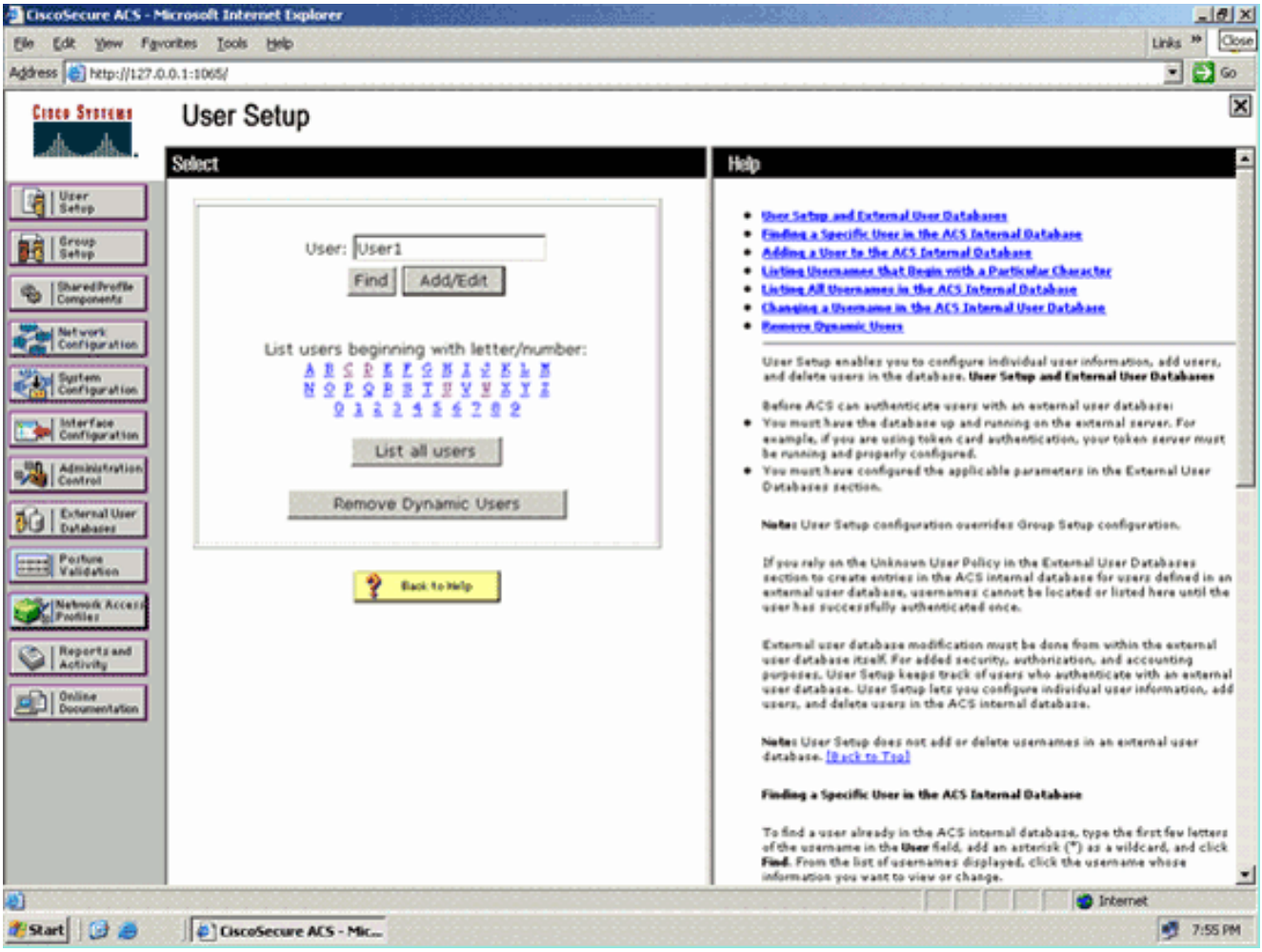
4. 根據需要配置活動/已停用主金鑰TTL（生存時間）值，或將其設定為預設值（如本例所示）。Authority ID Info欄位表示此ACS伺服器的文本標識，終端使用者可以使用該標識來確定對其進行身份驗證的ACS伺服器。必須填寫此欄位。Client initial display message欄位指定要傳送給使用EAP-FAST客戶端進行身份驗證的使用者的消息。最大長度為40個字元。僅當終端使用者客戶端支援顯示時，使用者才會看到初始消息。
5. 如果您希望ACS執行匿名帶內PAC調配，請選中**允許匿名帶內PAC調配**覈取方塊。
6. *Allowed inner methods*選項確定哪些內部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）。
7. 按一下「**Submit**」。**注意：有關如何使用匿名帶內PAC調配和身份驗證帶內調配配置**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伺服器配置的EAP-FAST身份驗證示例。

配置使用者資料庫並定義*url-redirect* RADIUS屬性

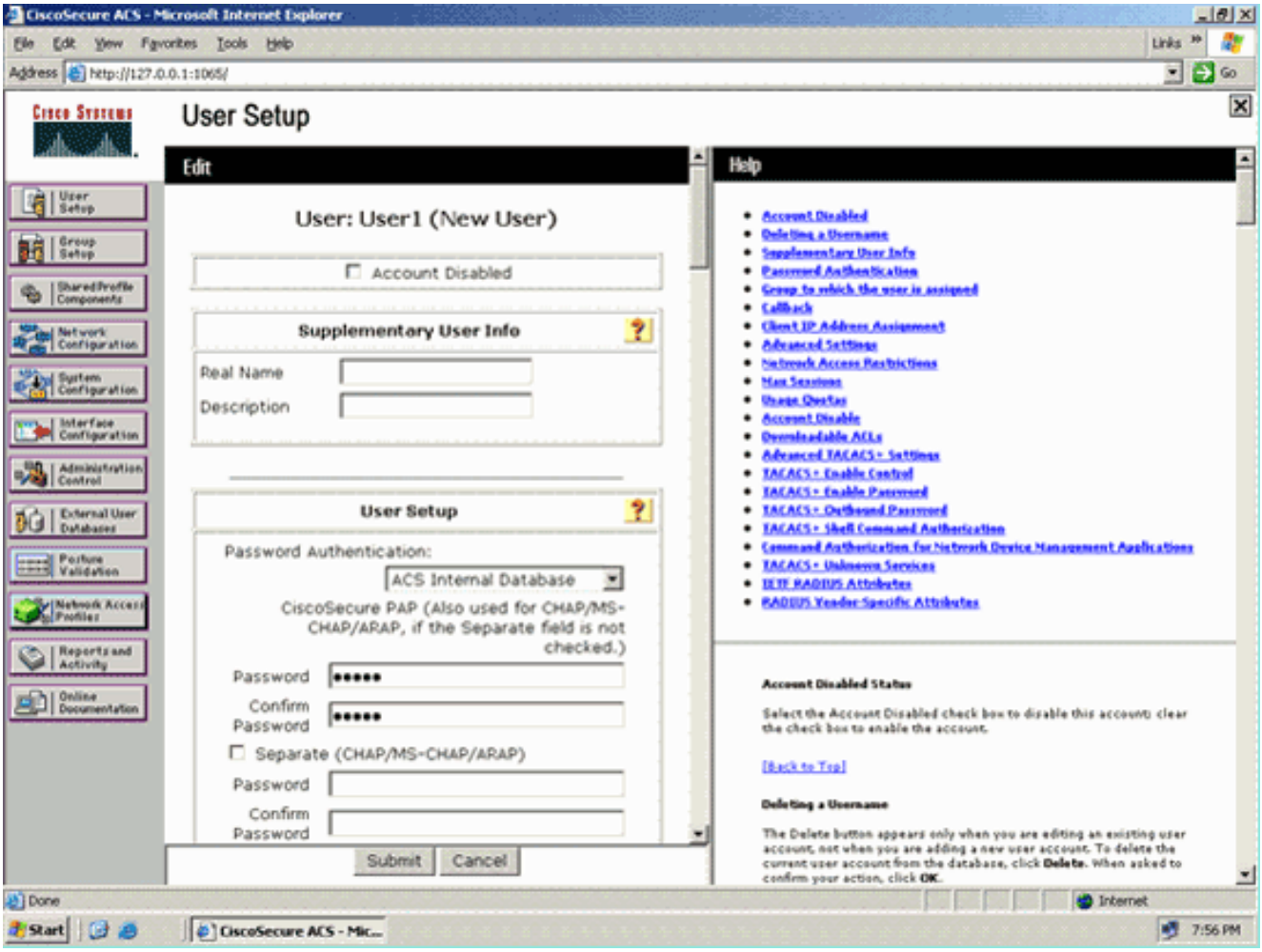
此示例將無線客戶端的使用者名稱和密碼分別配置為User1和User1。

完成以下步驟即可建立使用者資料庫：

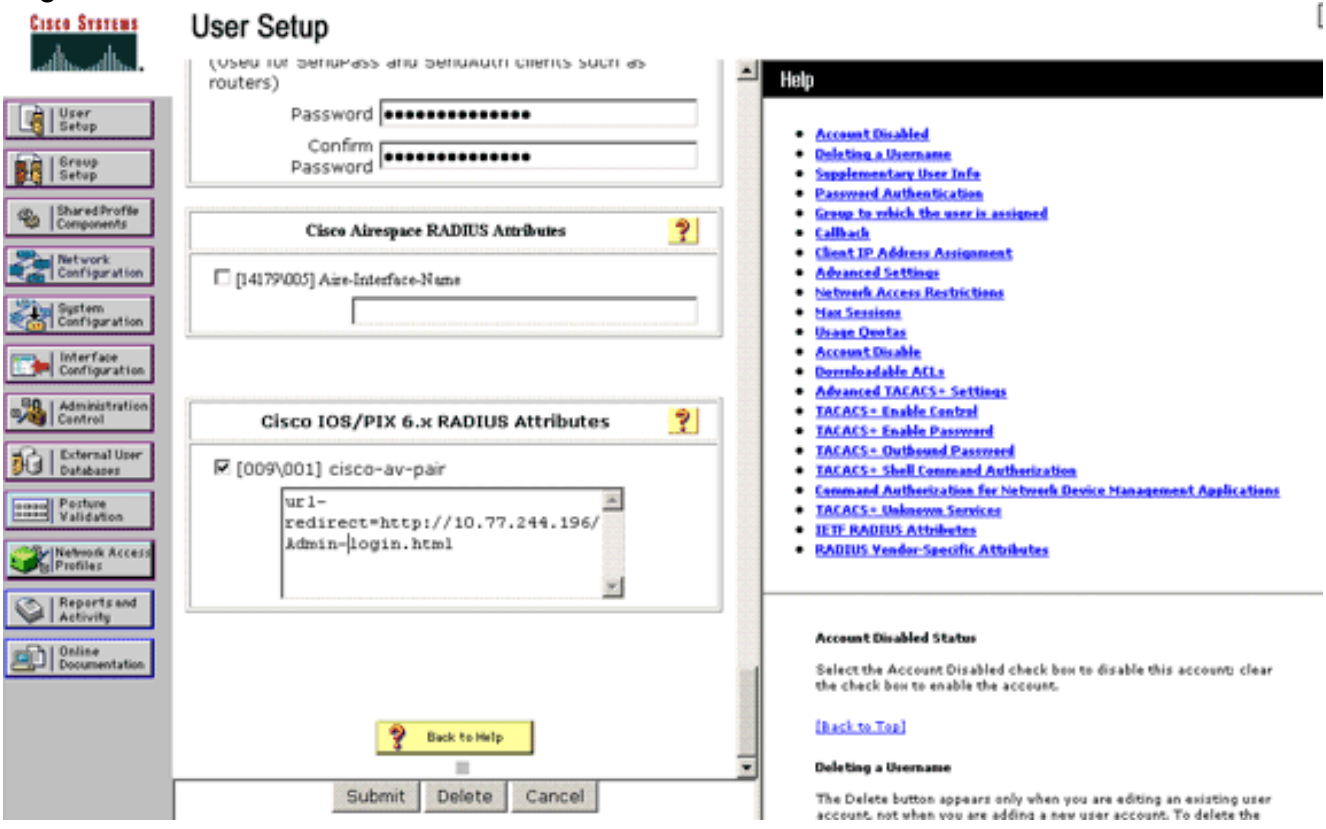
1. 從導航欄中的ACS GUI中選擇**User Setup**。
2. 建立一個新的無線使用者，然後按一下**Add/Edit**以轉到此使用者的「編輯」頁。



3. 在User Setup Edit頁中，配置Real Name和Description以及Password設定，如本例所示。本文檔使用ACS內部資料庫進行口令驗證。



4. 向下滾動頁面以修改RADIUS屬性。
5. 選中**[009\001] cisco-av-pair**覈取方塊。
6. 在[009\001] cisco-av-pair編輯框中輸入此Cisco av-pair，以指定將使用者重定向到的URL:url-redirect=http://10.77.244.196/Admin-Login.html



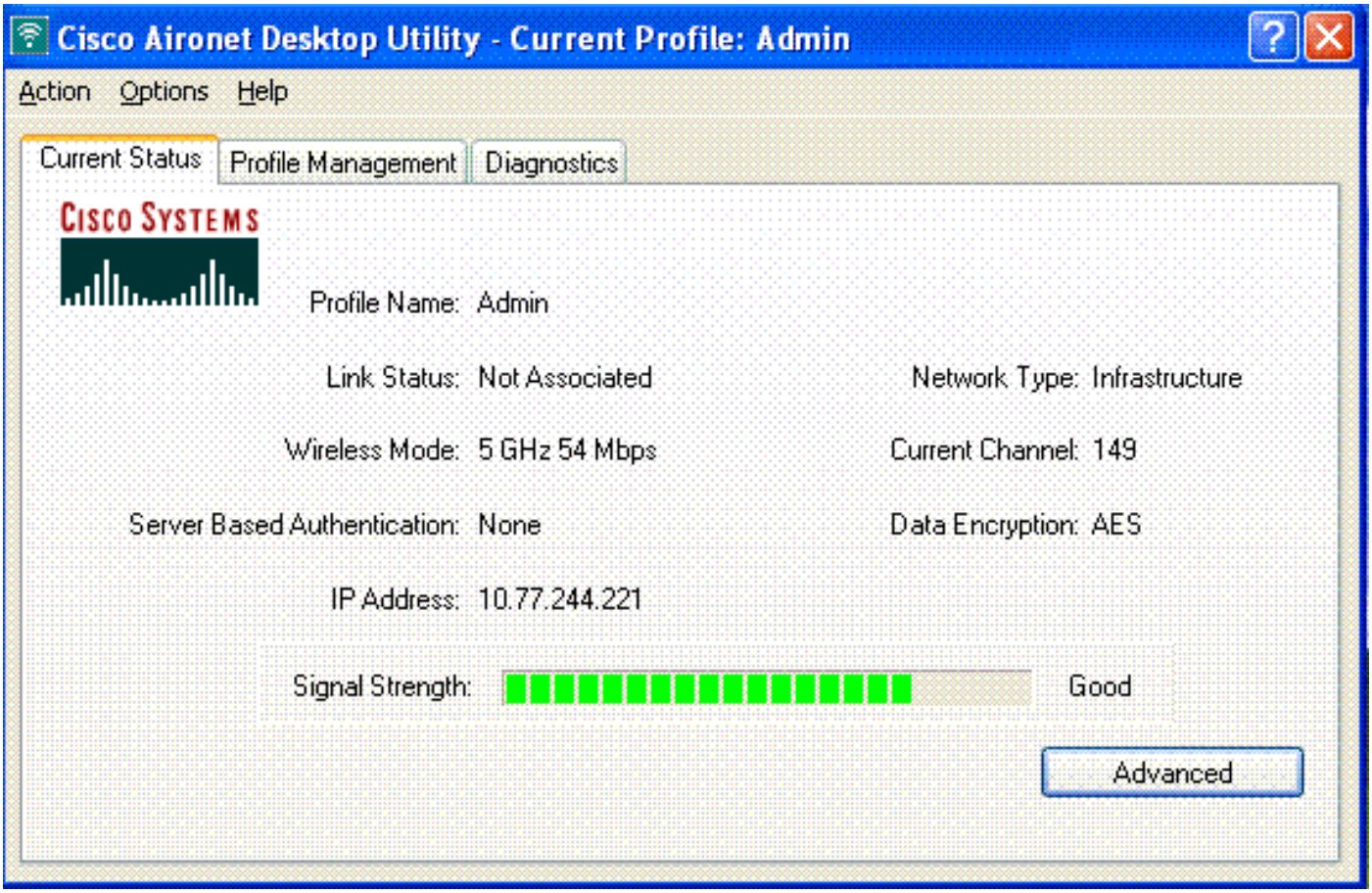
這是管理部門使用者的首頁。

7. 按一下「**Submit**」。
8. 重複此過程以新增User2（操作部門使用者）。
9. 重複步驟1到6，以便向資料庫中新增更多的管理部門使用者和操作部門使用者。**注意**：RADIUS屬性可在Cisco Secure ACS上的使用者級別或組級別進行配置。

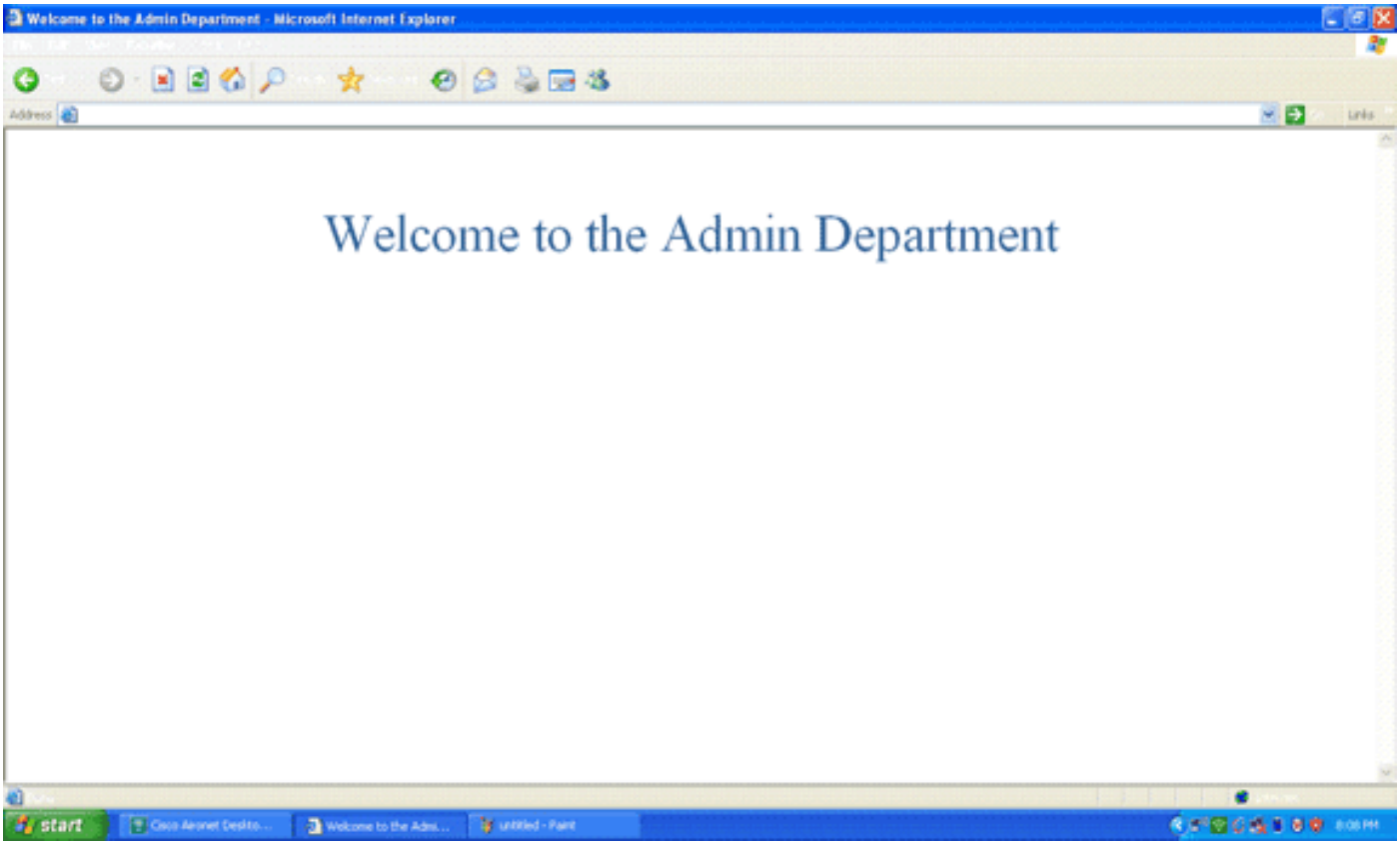
驗證

為了驗證配置，請將管理部門和運營部門的WLAN客戶端與其相應的WLAN相關聯。

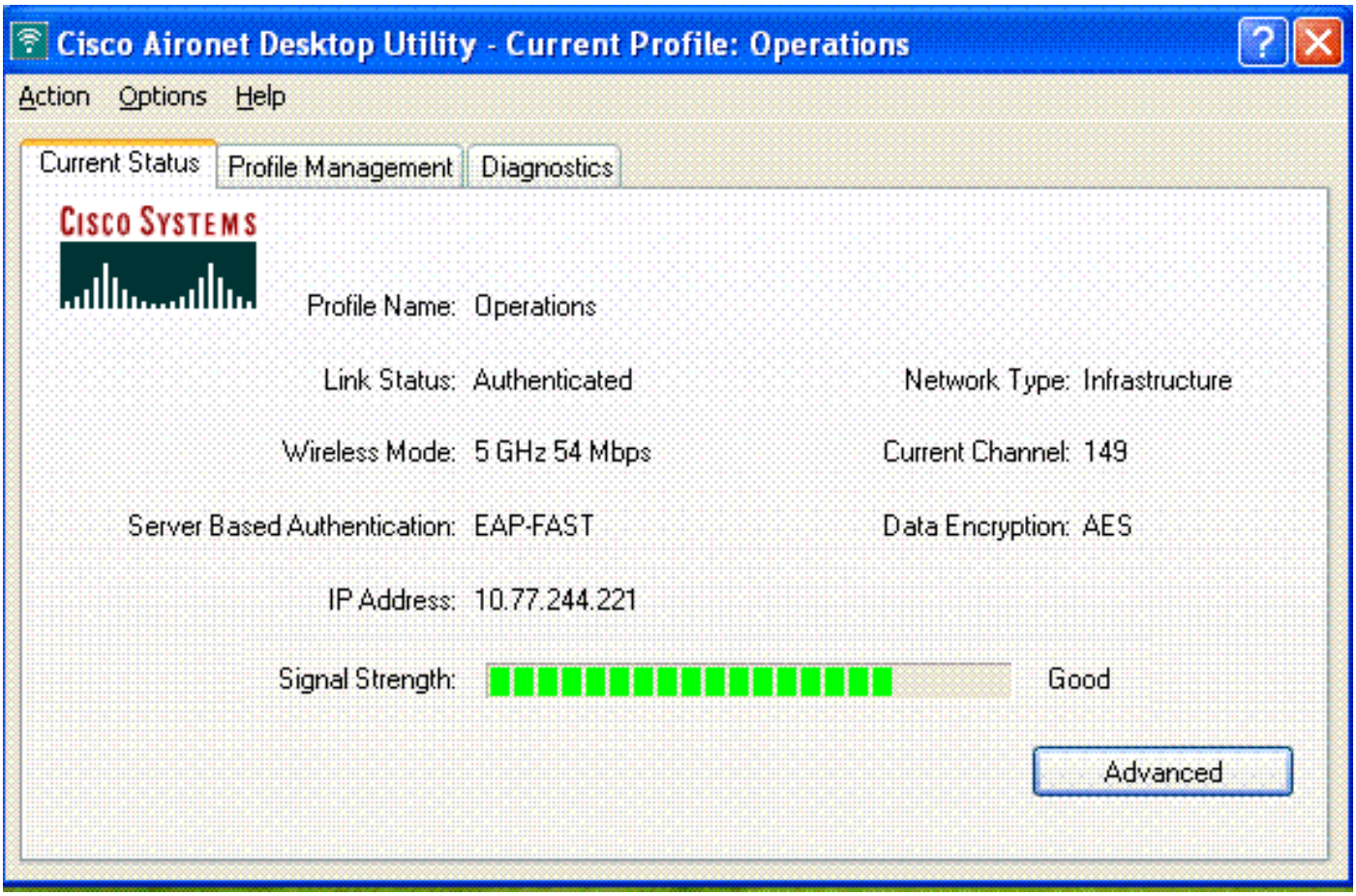
當管理員部門的使用者連線到Wireless LAN Admin時，系統將提示該使用者輸入802.1x憑證（在本例中為EAP-FAST憑證）。使用者提供憑證後，WLC會將這些憑證傳遞到Cisco Secure ACS伺服器。Cisco Secure ACS伺服器根據資料庫驗證使用者憑證，並在身份驗證成功後將url-redirect屬性返回到無線LAN控制器。身份驗證在此階段完成。

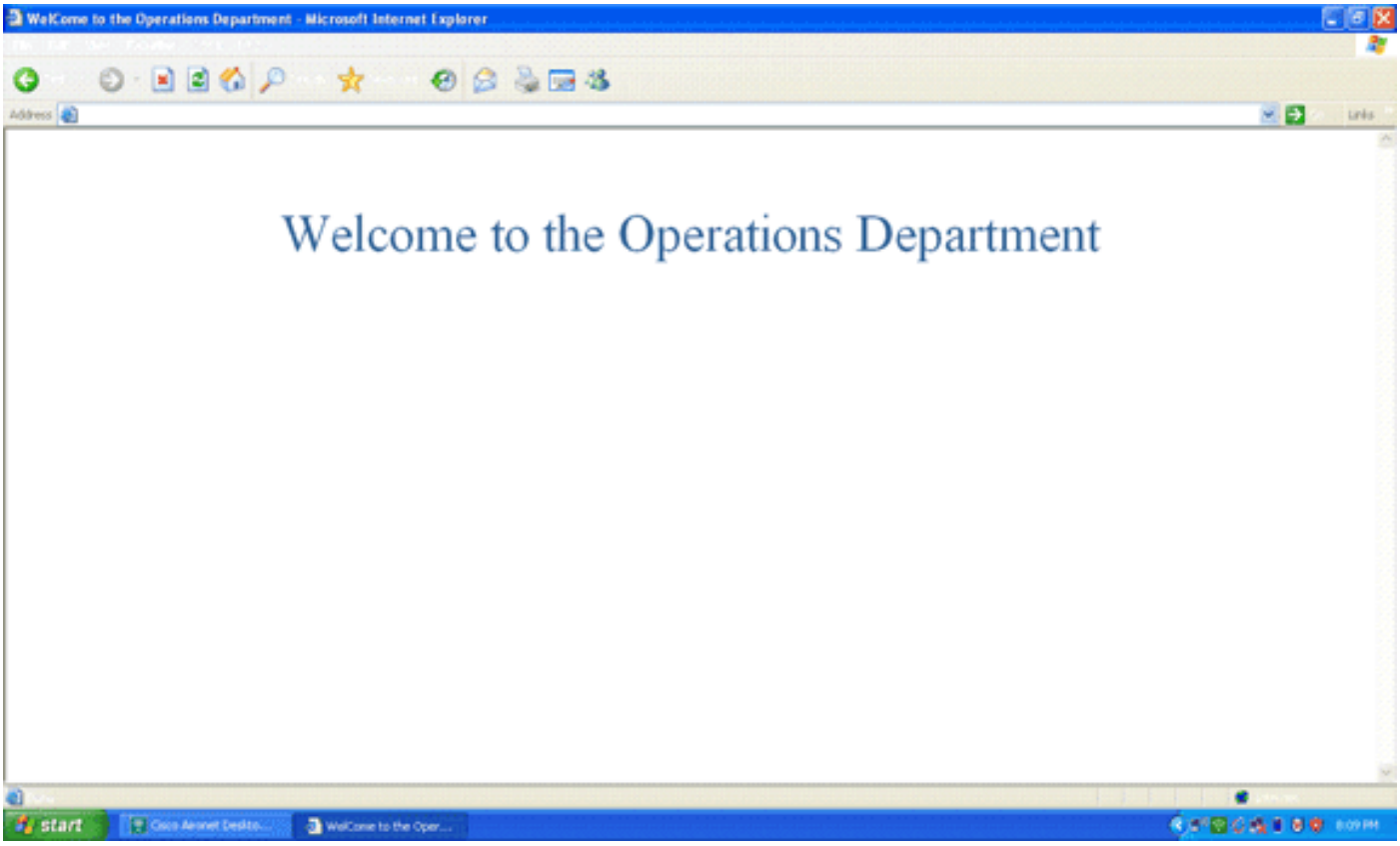


當使用者開啟Web瀏覽器時，系統會將使用者重定向到管理部門的首頁URL。（此URL會透過cisco-av-pair屬性傳回WLC）。重新導向後，使用者會獲得網路的完整存取權限。以下截圖：



當操作部門的使用者連線到WLAN Operations時，會發生相同的事件序列。





疑難排解

本節提供的資訊可用於對組態進行疑難排解。

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

您可以使用以下命令對配置進行故障排除。

- **show wlan wlan_id** — 顯示特定WLAN的Web重新導向功能的狀態。以下是範例：

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debug dot1x events enable** — 啟用802.1x資料包消息的調試。以下是範例：

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
    mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
    mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
    seconds, got from WLAN config.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
    setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
    for station 00:40:96:ac:dd:05 (RSN 2)
```

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
    to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
    lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
    00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
    mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
    in Authenticating state for mobile 00:40:96:ac:dd:05
```

- debug aaa events enable — 啟用所有aaa事件的調試輸出。以下是範例：

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
       source: 4, valid bits: 0x0
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

相關資訊

- 思科無線LAN控制器組態設定指南5.0版
- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 無線支援頁面
- 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）。