使用ACS 5.2和WLC配置PEAP和EAP-FAST

目錄

簡介

本檔案將說明如何使用外部RADIUS伺服器(例如存取控制伺服器(ACS)5.2)將無線LAN控制器(WLC)設定為可擴充驗證通訊協定(EAP)驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解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

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5508 WLC（執行韌體版本7.0.220.0）
- Cisco 3502系列LAP
- 採用英特爾6300-N驅動程式14.3版的Microsoft Windows 7原生請求方
- 執行5.2版的Cisco Secure ACS
- Cisco 3560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。

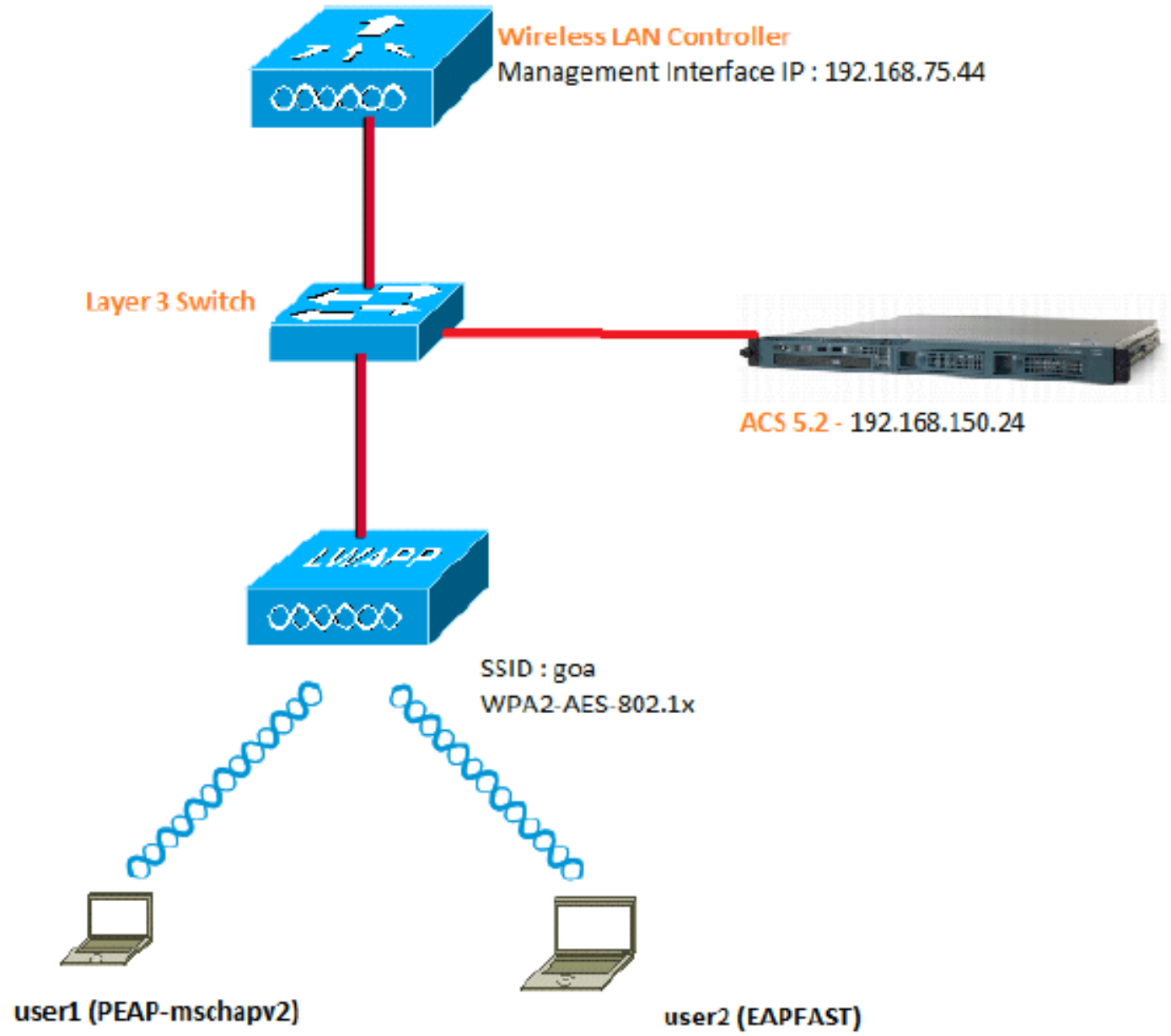
設定

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。

網路圖表

此文件使用以下網路設定：



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192.168.150.24。
- WLC的管理和AP管理器介面地址為192.168.75.44。
- DHCP伺服器地址為192.168.150.25。
- 整個配置中都使用VLAN 253。兩個使用者都連線到同一個SSID「goa」。但是，使用者1配置為使用PEAP-MSCHAPv2進行身份驗證，使用者2使用EAP-FAST進行身份驗證。
- 使用者將分配到VLAN 253中：
  - VLAN 253:192.168.153.x/24。網關：192.168.153.1
  - VLAN 75:192.168.75.x/24。網關：192.168.75.1

假設

- 所有第3層VLAN都配置了交換機。
- 為DHCP伺服器分配一個DHCP作用域。
- 網路中所有裝置之間都存在第3層連線。
- LAP已連線到WLC。
- 每個VLAN都有/24掩碼。
- ACS 5.2安裝了自簽名證書。

配置步驟

此配置分為三個高級步驟：

1. 設定RADIUS伺服器。
2. 設定WLC。
3. 配置無線客戶端實用程式。

設定RADIUS伺服器

RADIUS伺服器設定分為四個步驟：

1. 配置網路資源。
2. 配置使用者。
3. 定義策略元素。
4. 應用訪問策略。

ACS 5.x是基於策略的訪問控制系統。也就是說，ACS 5.x使用基於規則的策略模型，而不是4.x版本中使用的基於組的模型。

ACS 5.x基於規則的策略模型提供比舊的基於組的方法更強大、更靈活的訪問控制。

在較舊的基於組的模型中，組定義策略是因為它包含三種型別的資訊並將它們連線在一起：

- 標識資訊 — 此資訊可以基於AD或LDAP組中的成員身份或內部ACS使用者的靜態分配。
- 其他限制或條件 — 時間限制、裝置限制等。
- 許可權 — VLAN或Cisco IOS®許可權級別。

ACS 5.x策略模型基於以下形式的規則：

- 如果condition為result

例如，我們使用為基於組的模型描述的資訊：

- 如果為identity-condition、restriction-condition、則為authorization-profile。

因此，這使我們能夠靈活地限制在什麼條件下允許使用者訪問網路，以及在滿足特定條件時允許什麼授權級別。

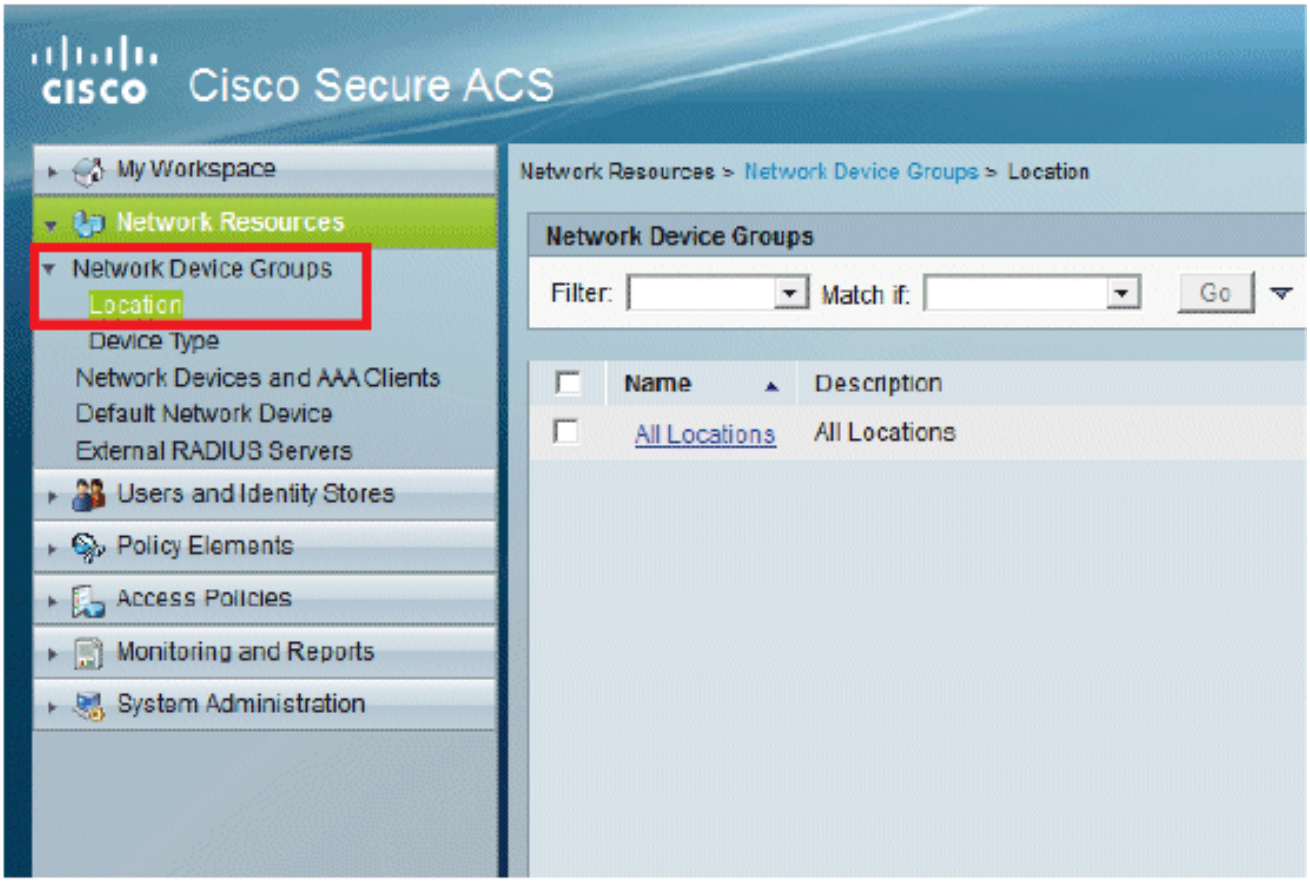
配置網路資源

在本節中，我們為RADIUS伺服器上的WLC設定AAA使用者端。

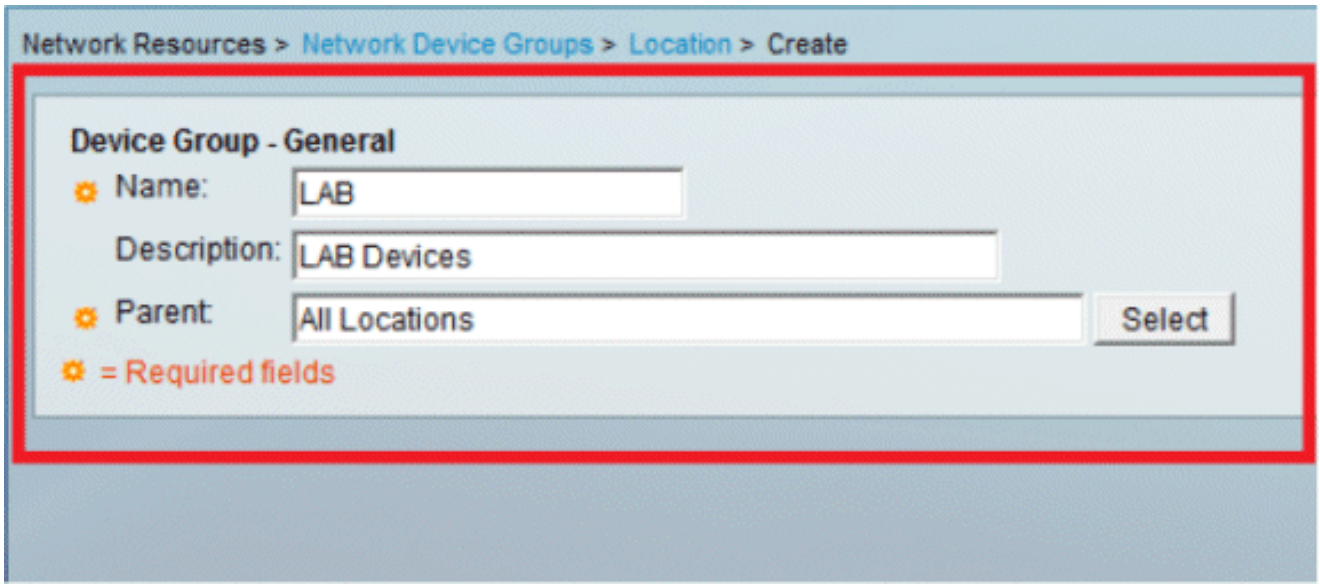
以下程式說明如何將WLC新增為RADIUS伺服器上的AAA使用者端，以便WLC將使用者認證傳遞到RADIUS伺服器。

請完成以下步驟：

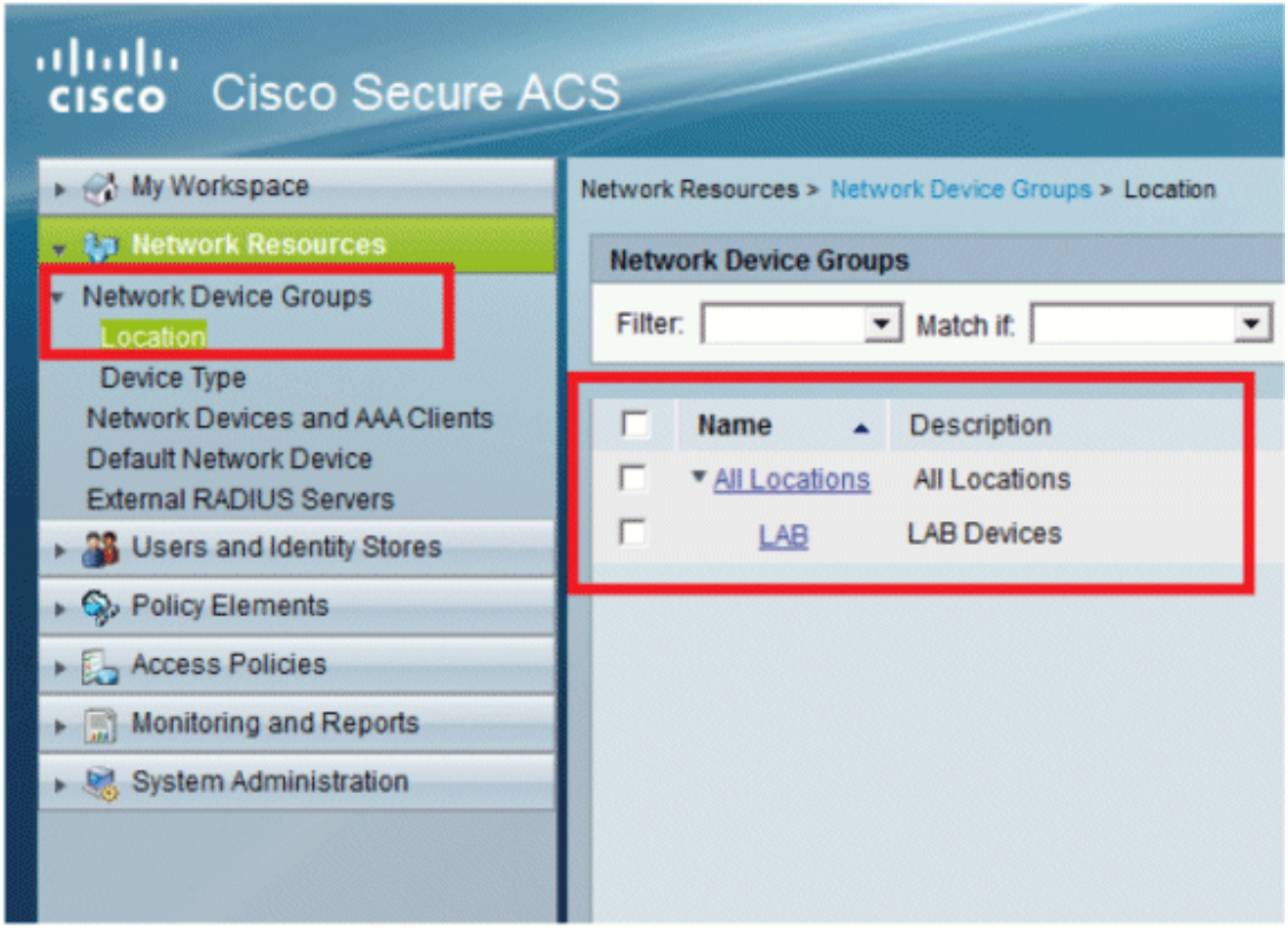
1. 在ACS GUI中，前往Network Resources > Network Device Groups > Location，然後按一下Create（位於底部）。



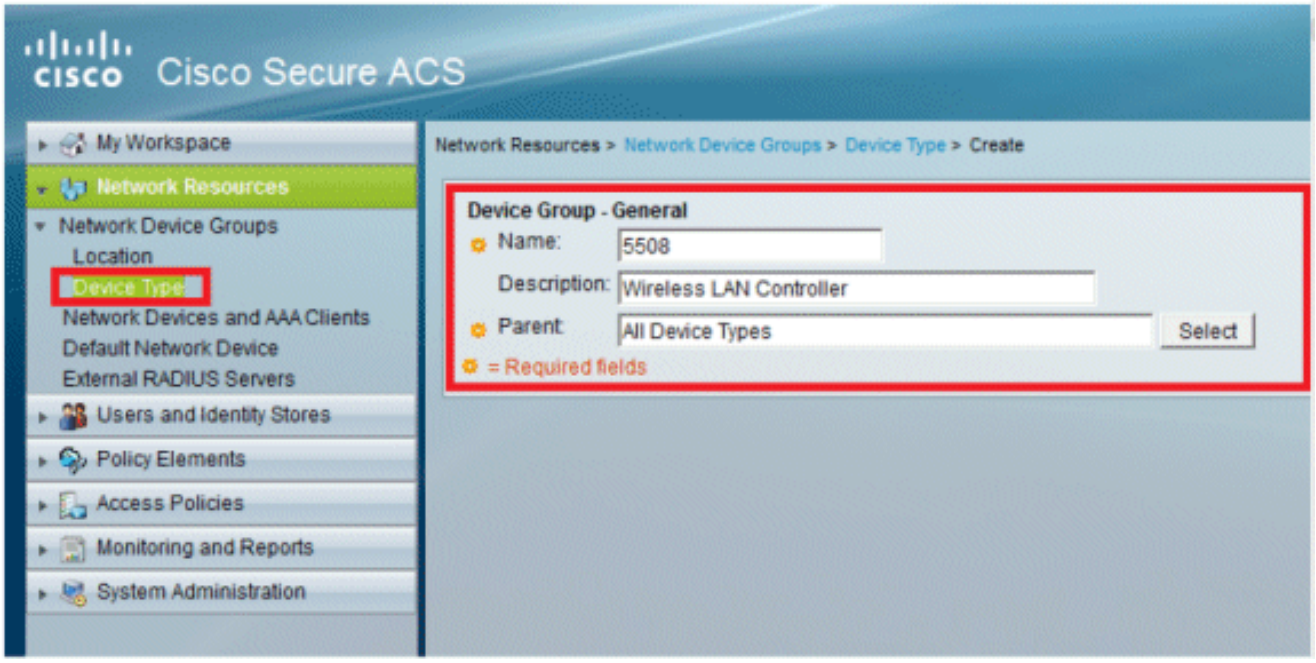
2. 新增必填欄位，然後按一下Submit。



現在您會看到以下螢幕：



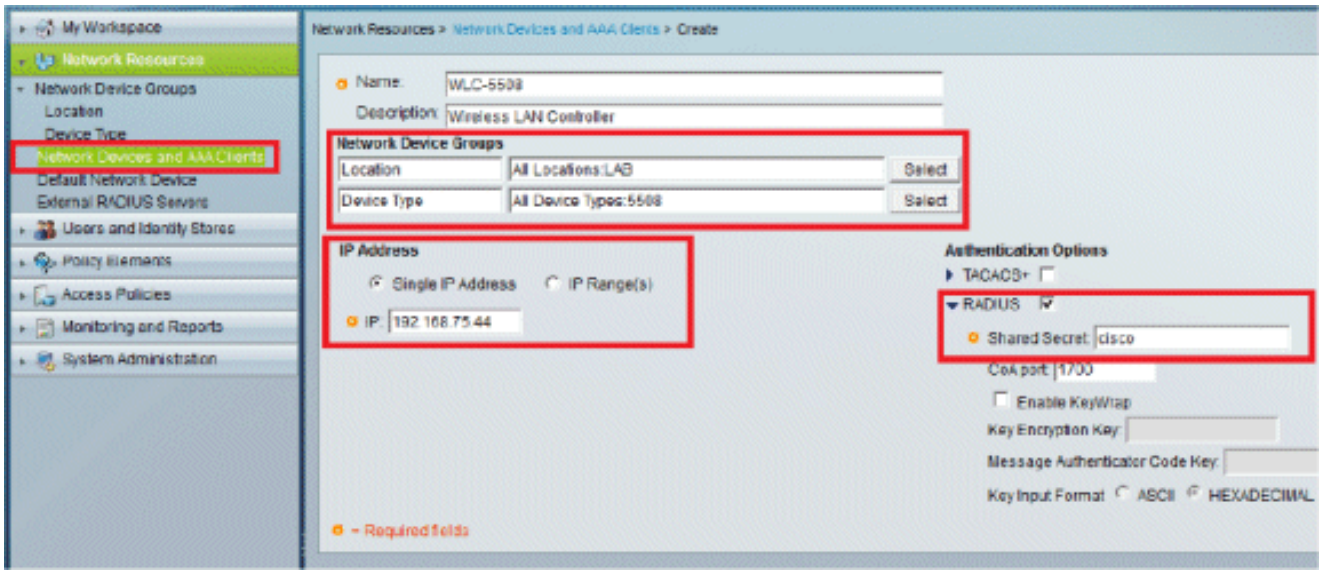
3. 按一下Device Type > Create。



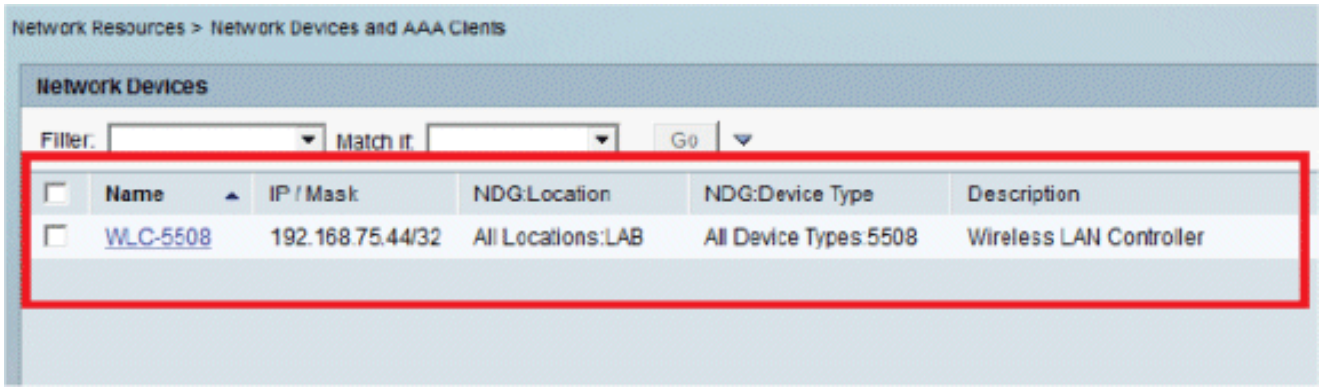
4. 按一下「Submit」。現在您會看到以下螢幕：

5. 前往Network Resources > Network Devices and AAA Clients。

6. 按一下「Create」，然後填寫詳細資訊，如下所示：



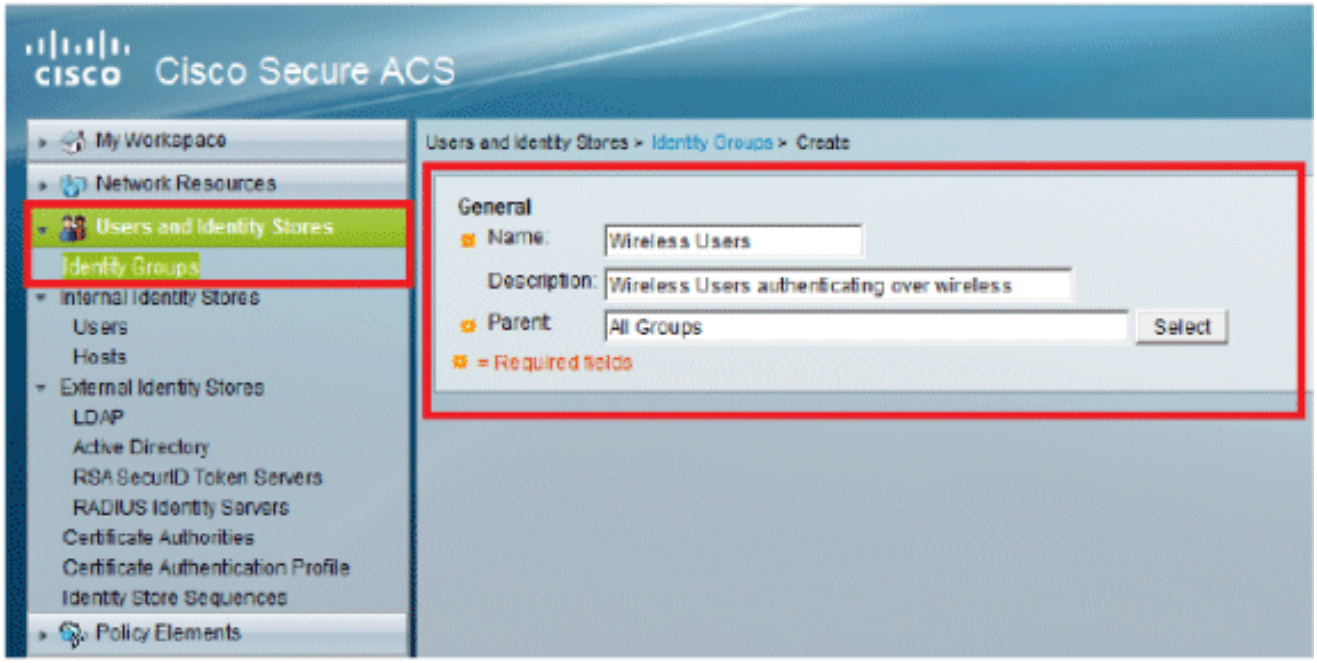
7. 按一下「Submit」。現在您會看到以下螢幕：



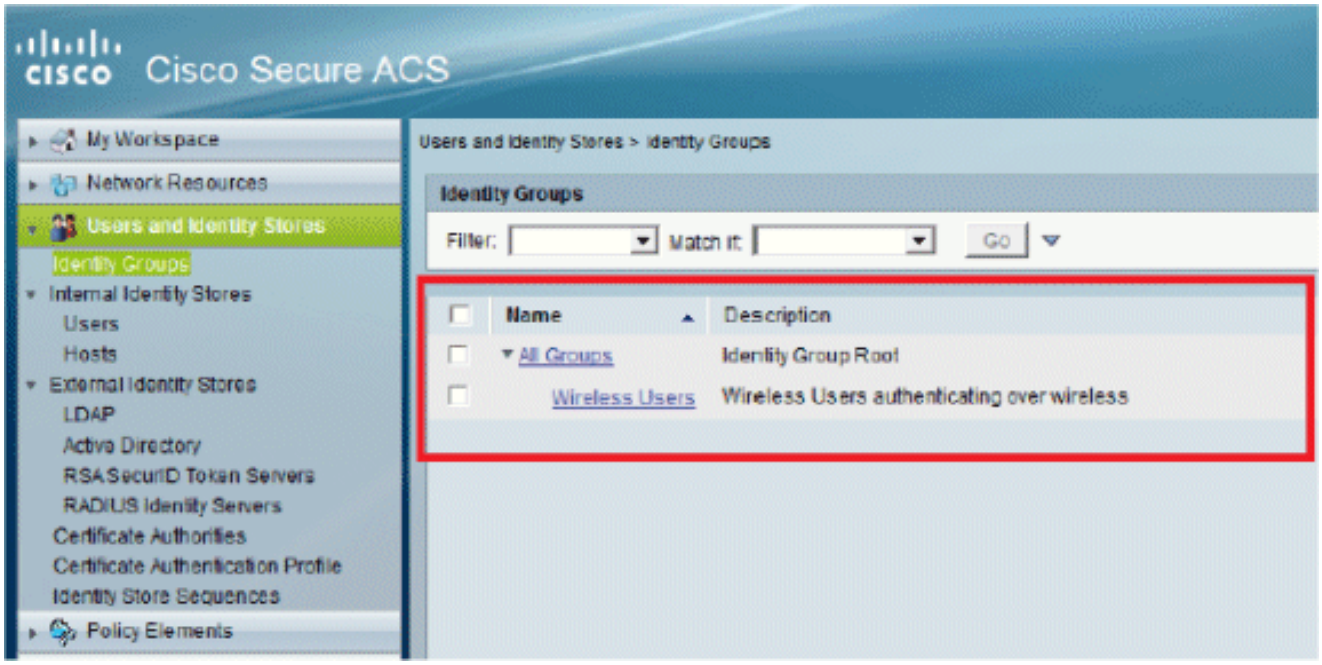
配置使用者

在本節中，我們將在ACS上建立本地使用者。兩個使用者（user1和user2）都分配到名為「無線使用者」的組中。

1. 轉至使用者和身份庫 > 身份組 > 建立。

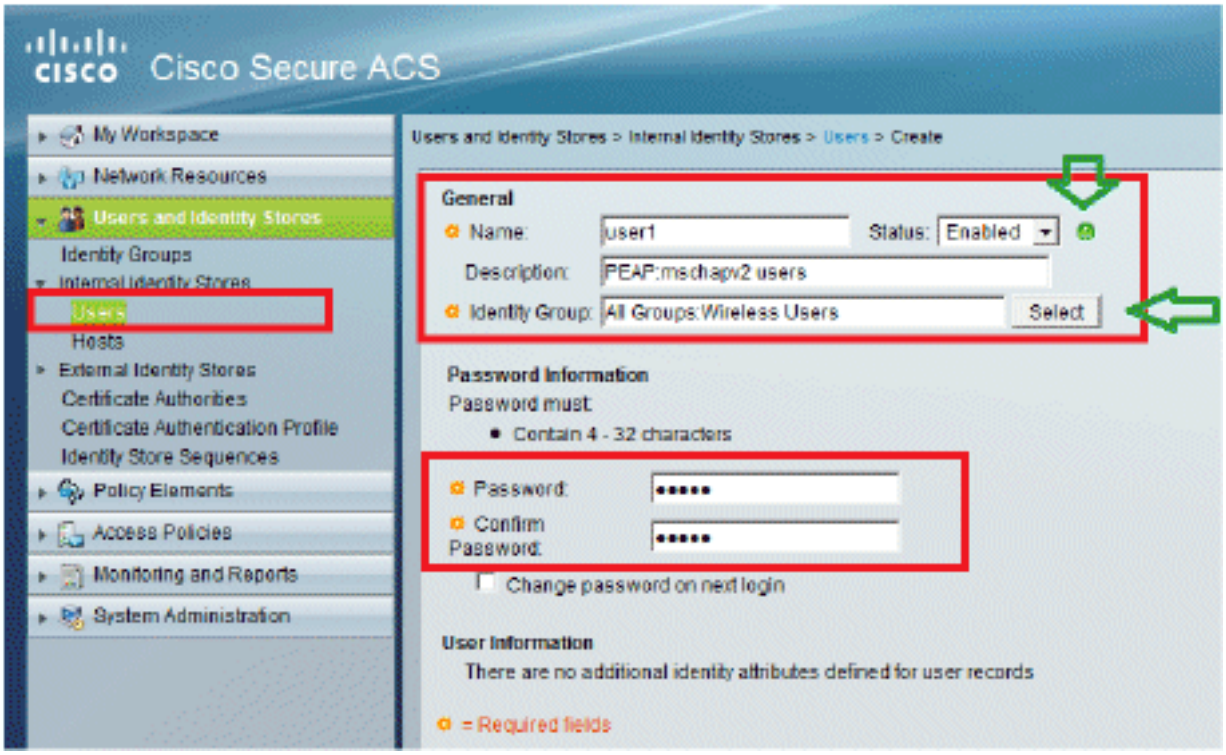


2. 按一下Submit後，頁面將如下所示：

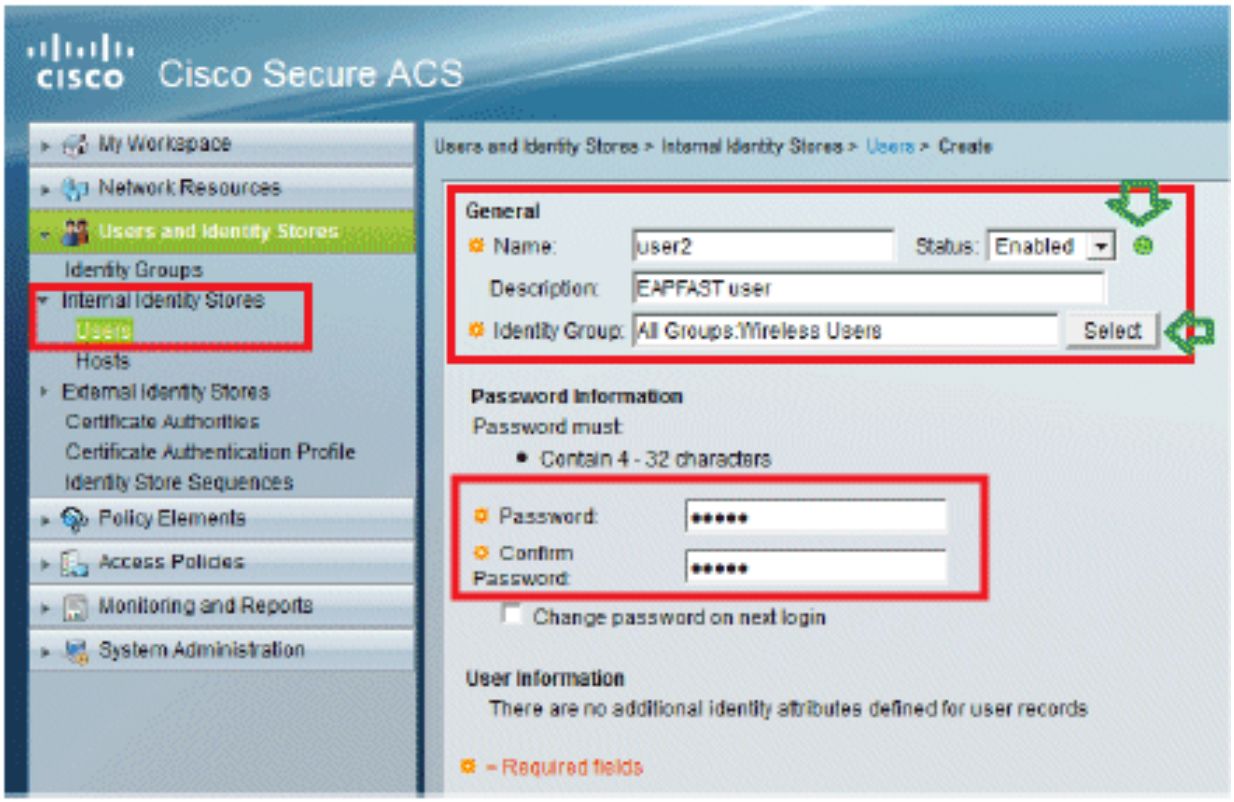


3. 建立users user1和user2，並將它們分配到「Wireless Users」組。

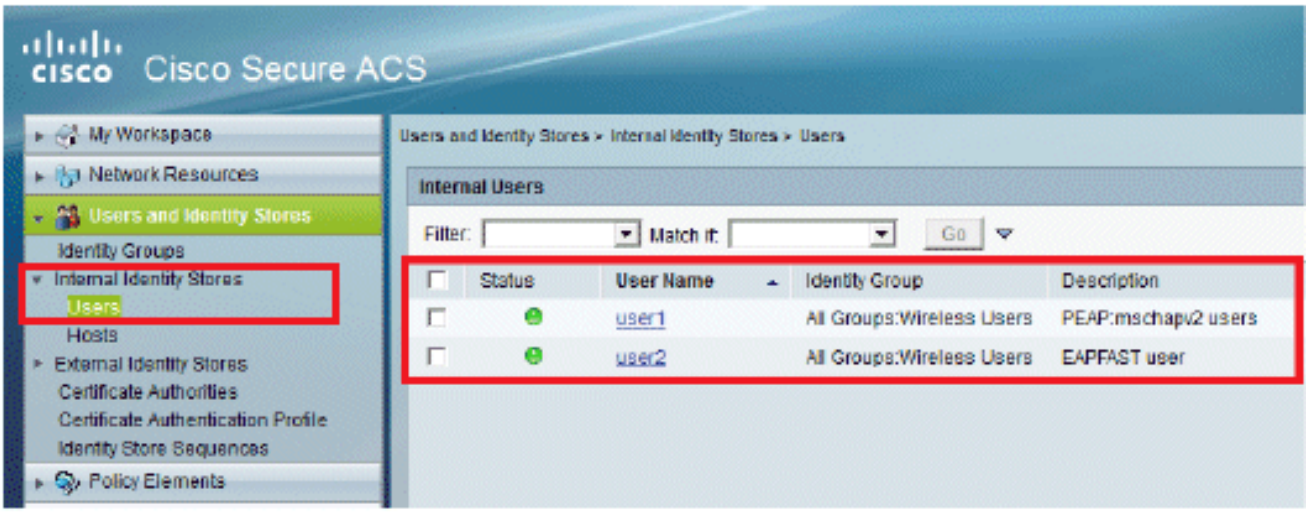
a. 按一下Users and Identity Stores > Identity Groups > Users > Create。



b. 類似地，建立user2。

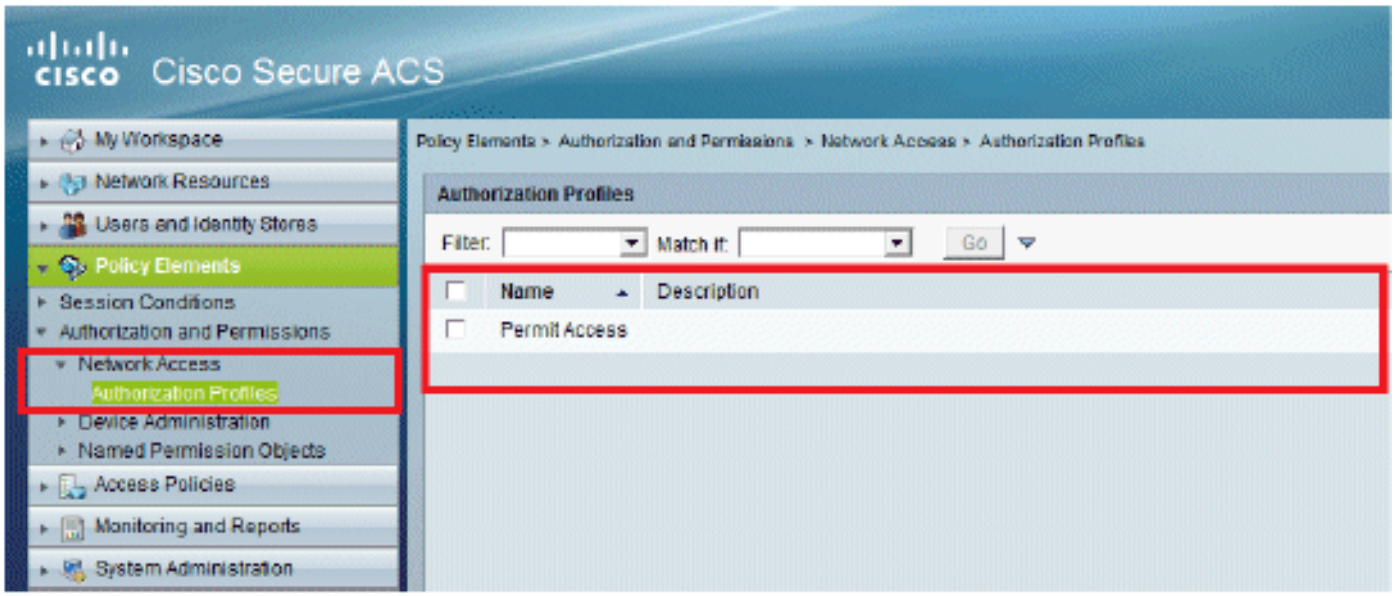


螢幕將如下所示：



定義策略元素

驗證Permit Access是否已設定。

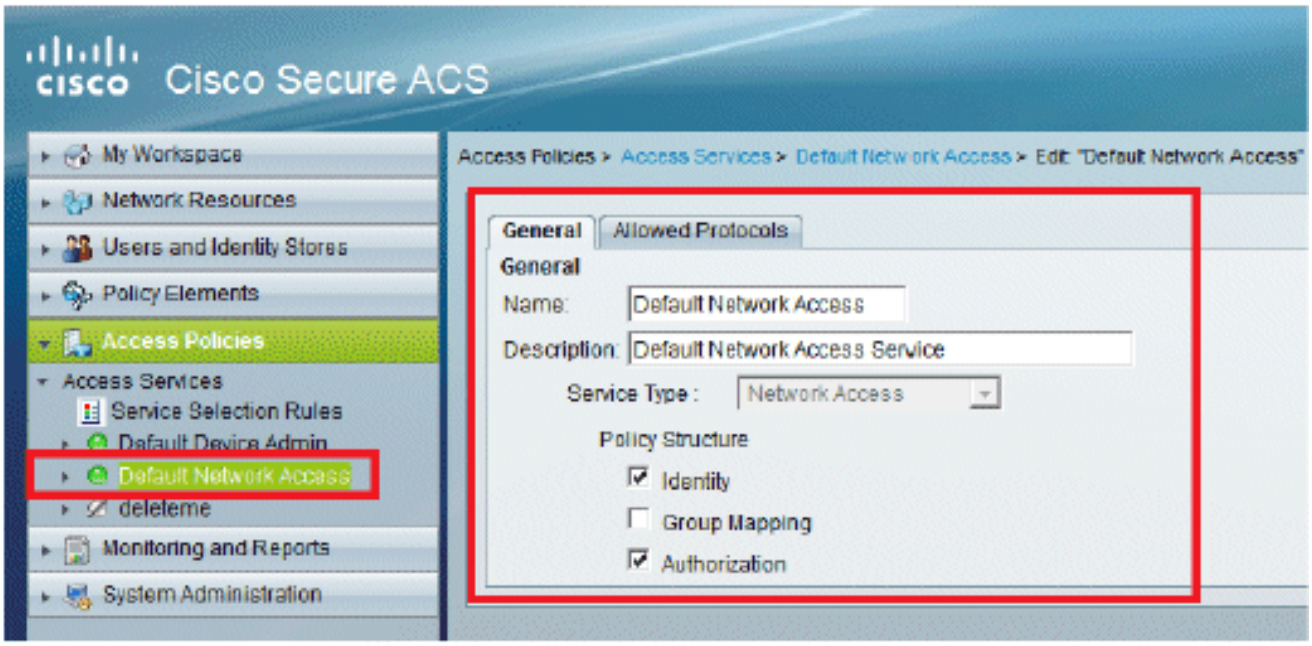


應用訪問策略

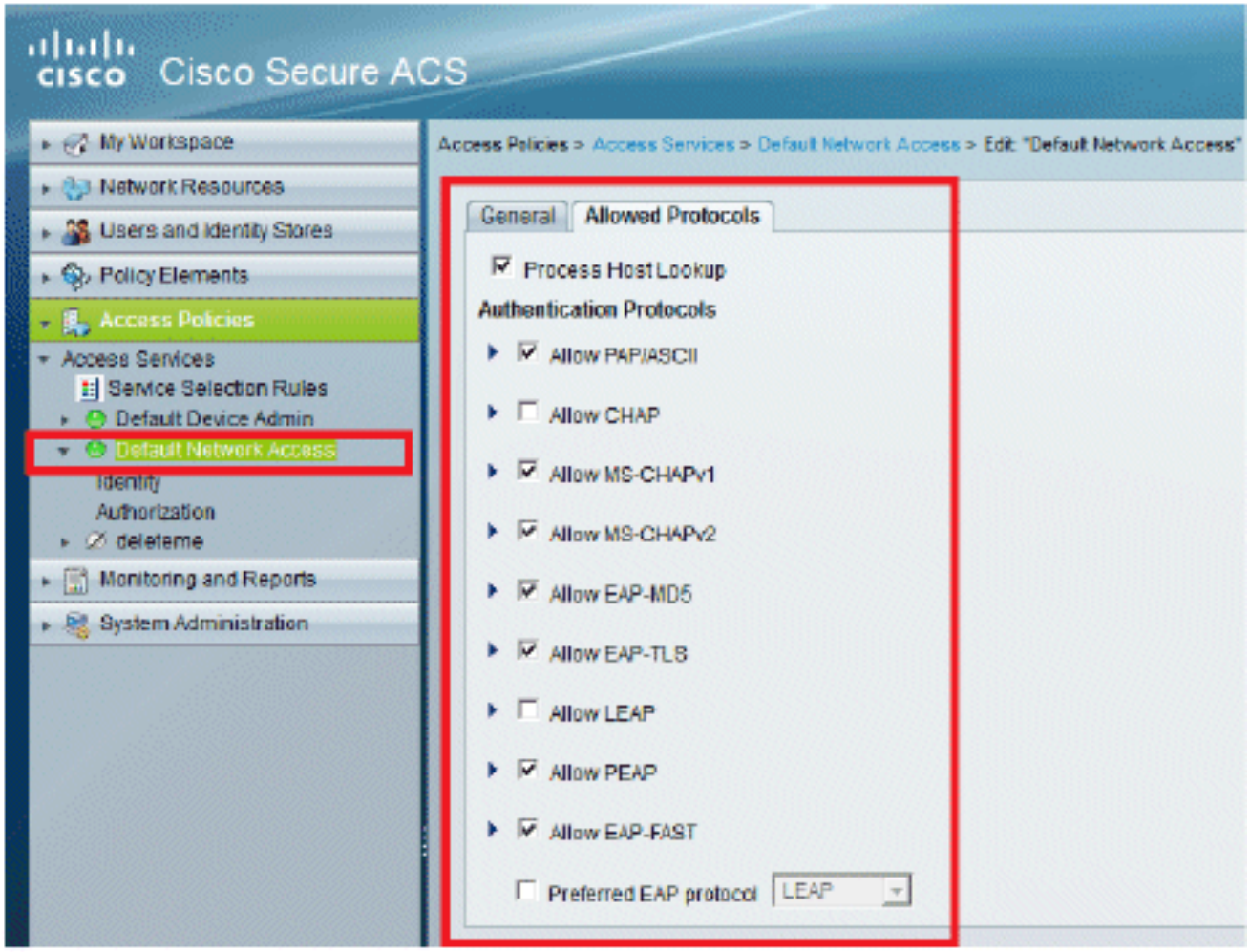
在本節中，我們將選擇要使用的身份驗證方法，以及如何配置規則。我們將根據前面的步驟建立規則。

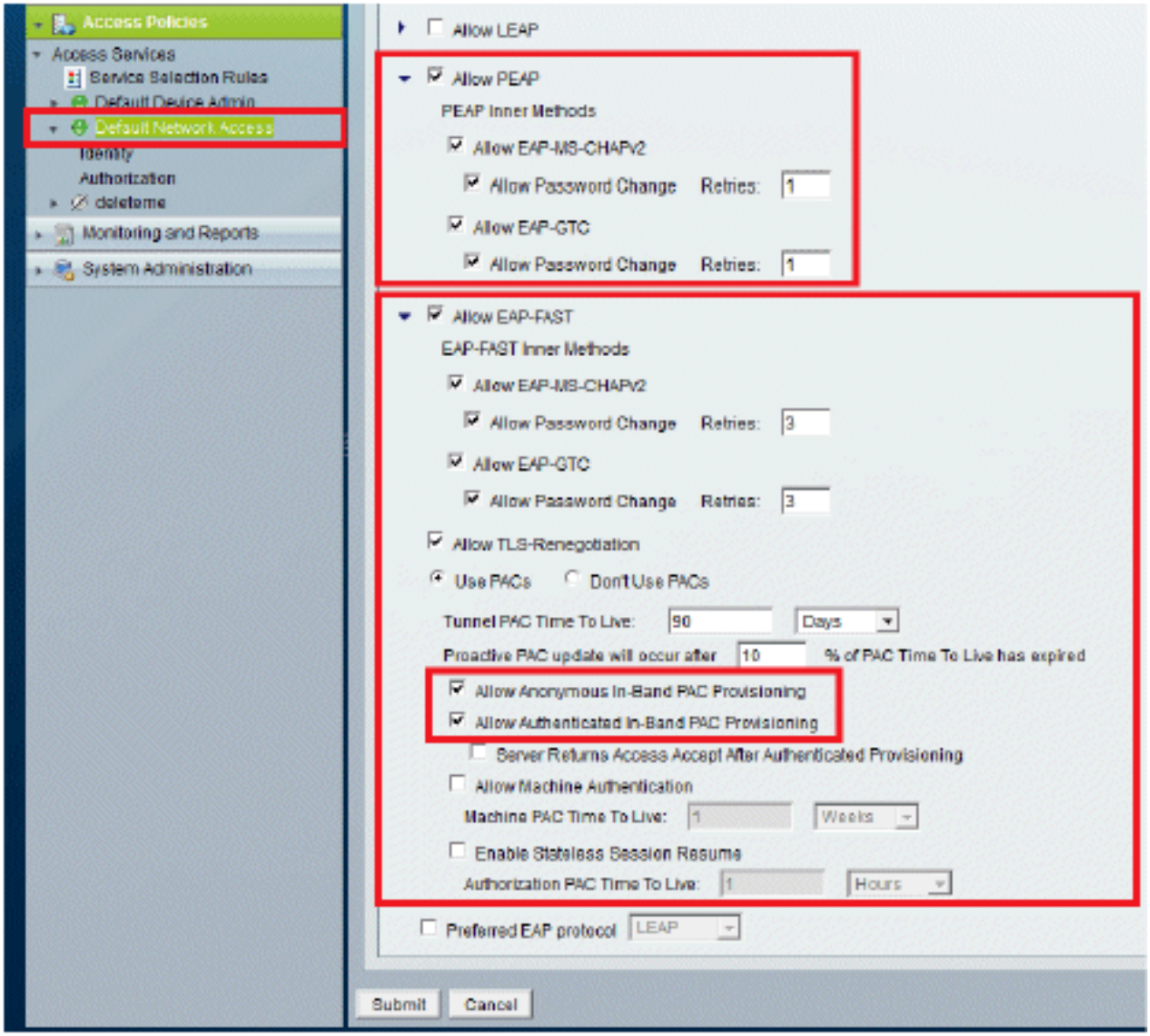
請完成以下步驟：

1. 前往Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。



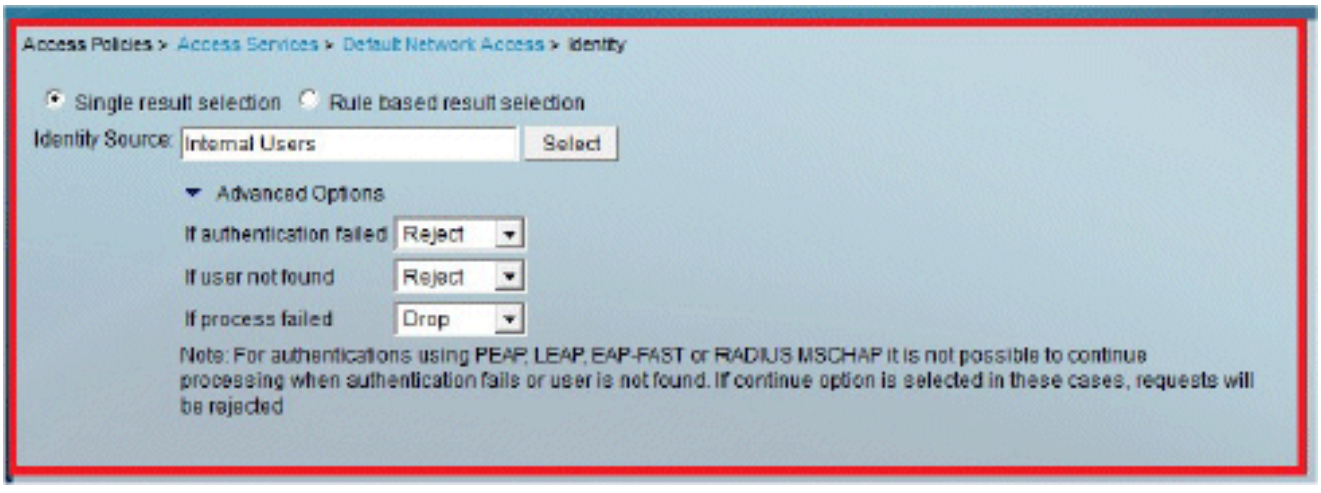
2. 選擇您希望無線客戶端進行身份驗證的EAP方法。在本示例中，我們使用PEAP-MSCHAPv2和EAP-FAST。





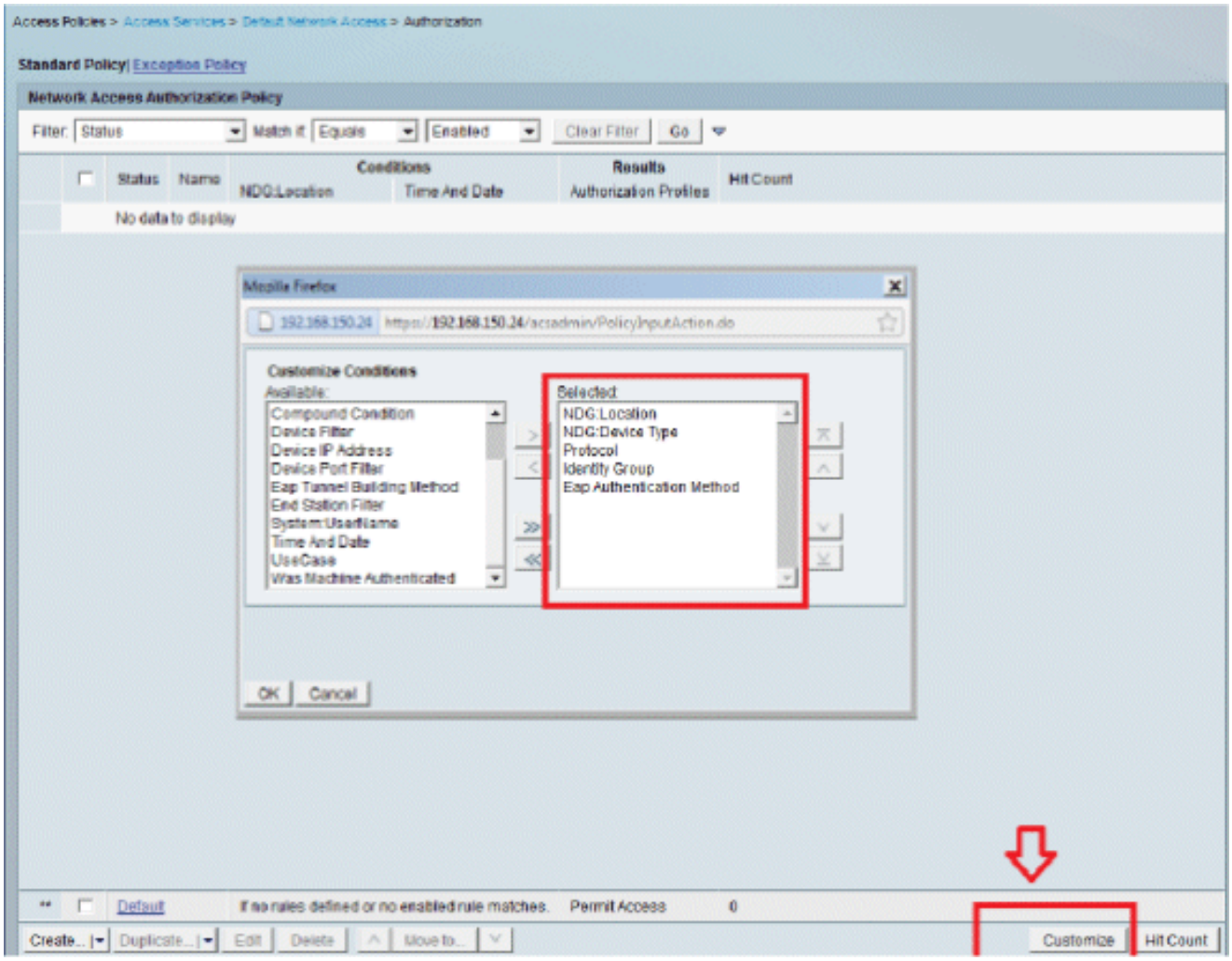
3. 按一下「Submit」。

4. 驗證您選擇的身份組。在本例中，我們使用Internal Users（在ACS上建立）。保存更改。



5. 若要驗證授權設定檔，請前往Access Policies > Access Services > Default Network Access > Authorization。

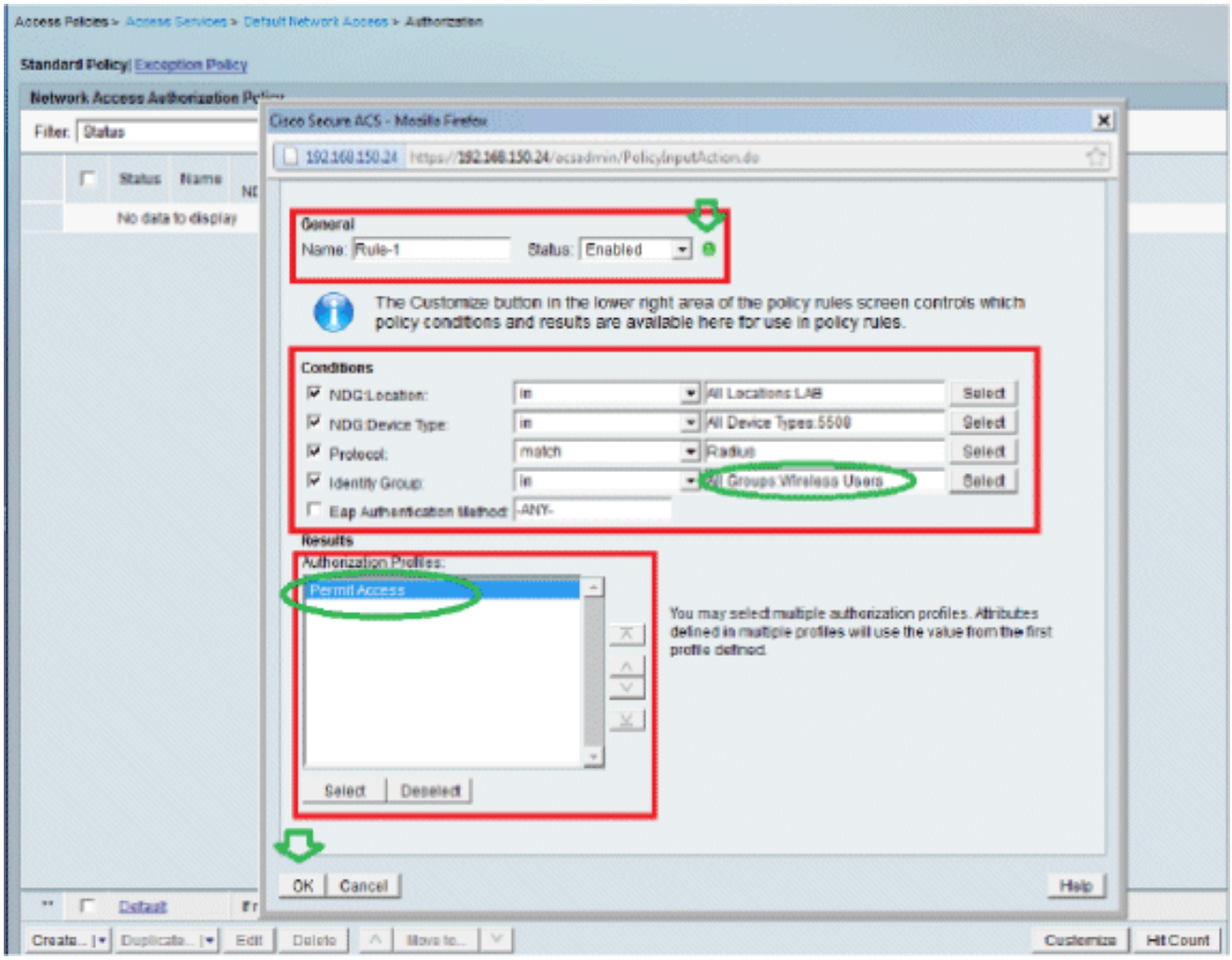
您可以自定義在哪些條件下允許使用者訪問網路，以及經過身份驗證後將通過的授權配置檔案（屬性）。此粒度僅在ACS 5.x中可用。在本示例中，我們選擇了Location、Device Type、Protocol、Identity Group和EAP Authentication Method。



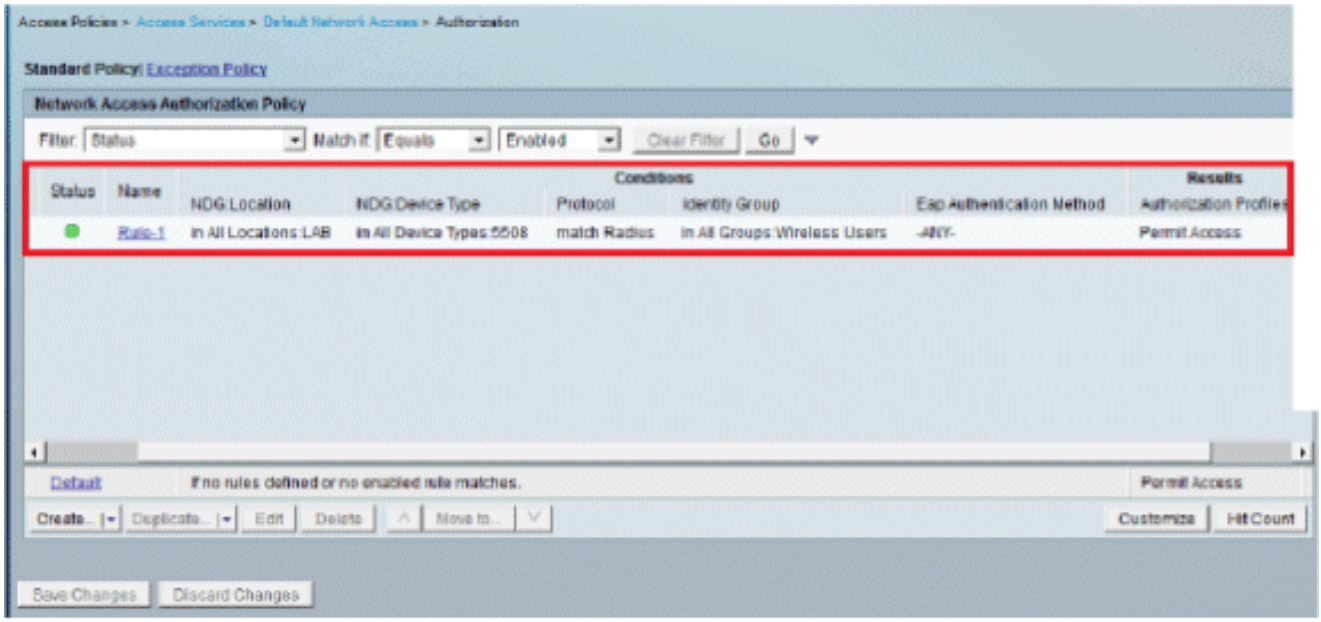
6. 按一下「OK」，然後「Save Changes」。

7. 下一步是建立規則。如果未定義規則，則允許客戶端在不帶任何條件的情況下訪問。

   按一下Create > Rule-1。此規則適用於「無線使用者」組中的使用者。

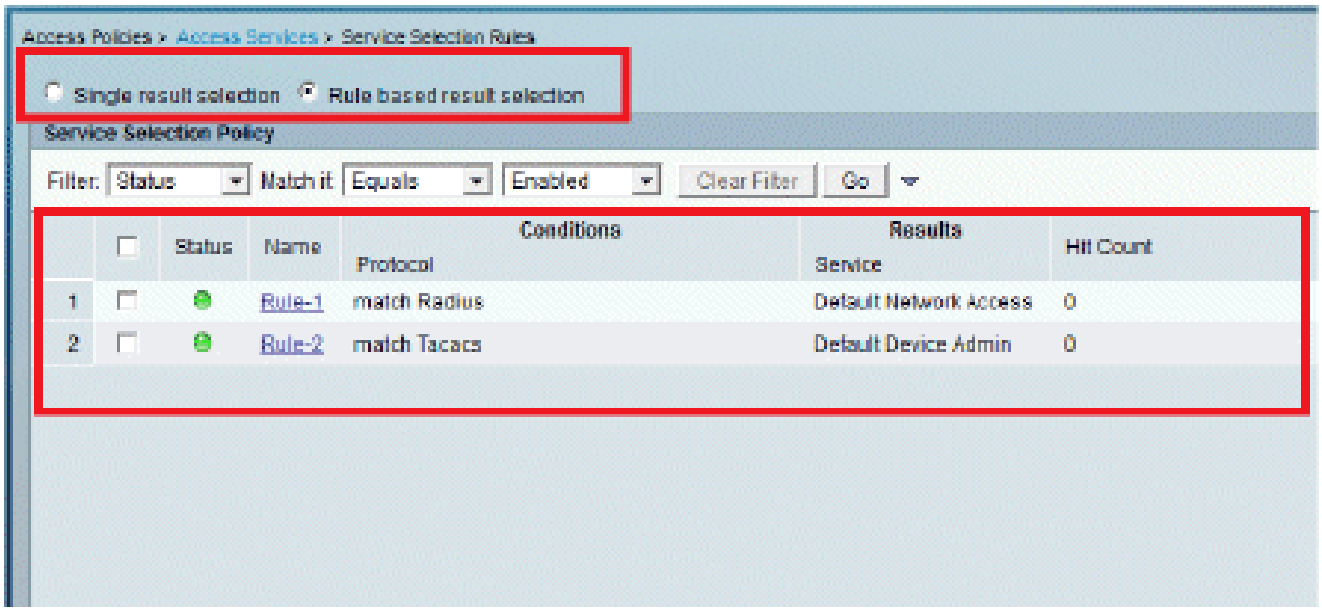


8. 儲存更改。螢幕將如下所示：



如果您希望拒絕不符合條件的使用者，請編輯預設規則以顯示「拒絕訪問」。

9. 現在我們將定義服務選擇規則。使用此頁可以配置簡單策略或基於規則的策略，以確定將哪種服務應用於傳入請求。在此示例中，使用基於規則的策略。



設定WLC

此配置需要執行以下步驟：

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

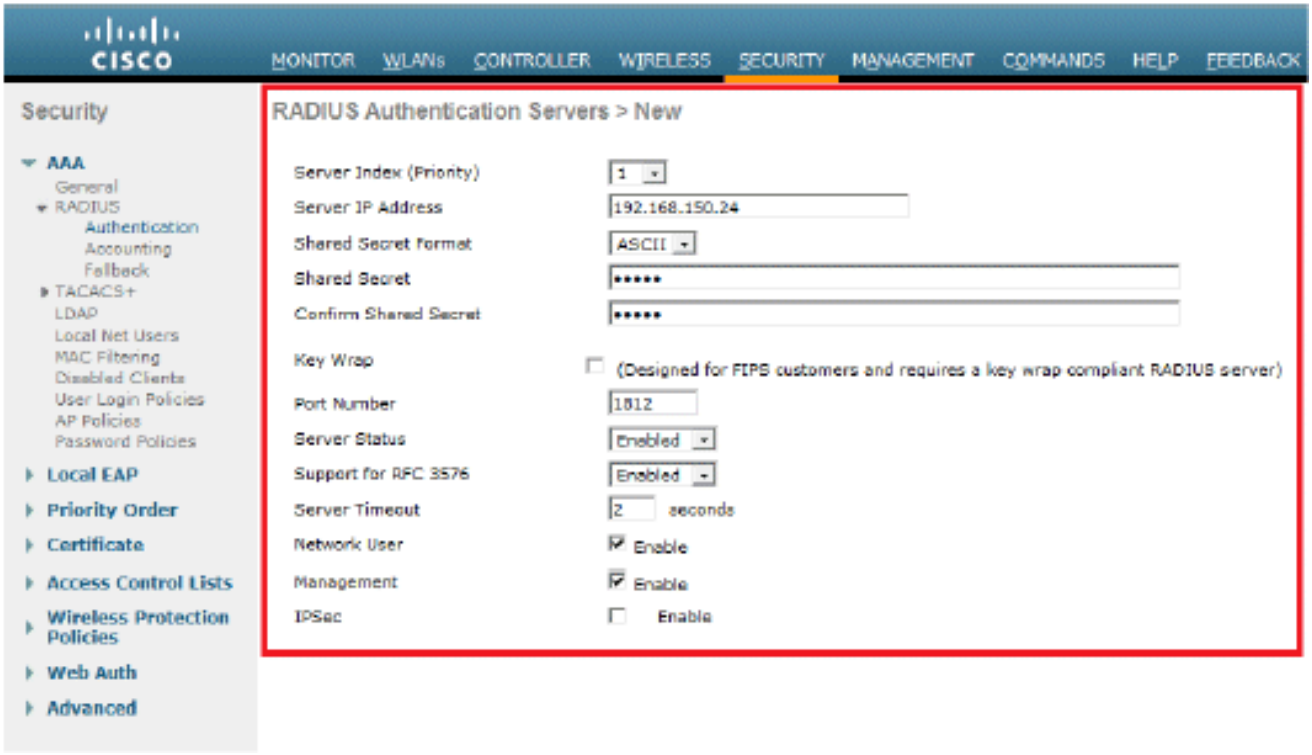
使用驗證伺服器的詳細資訊設定WLC

必須設定WLC，才能與RADIUS伺服器通訊以驗證使用者端，以及驗證任何其他交易。

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伺服器中配置的金鑰相同。

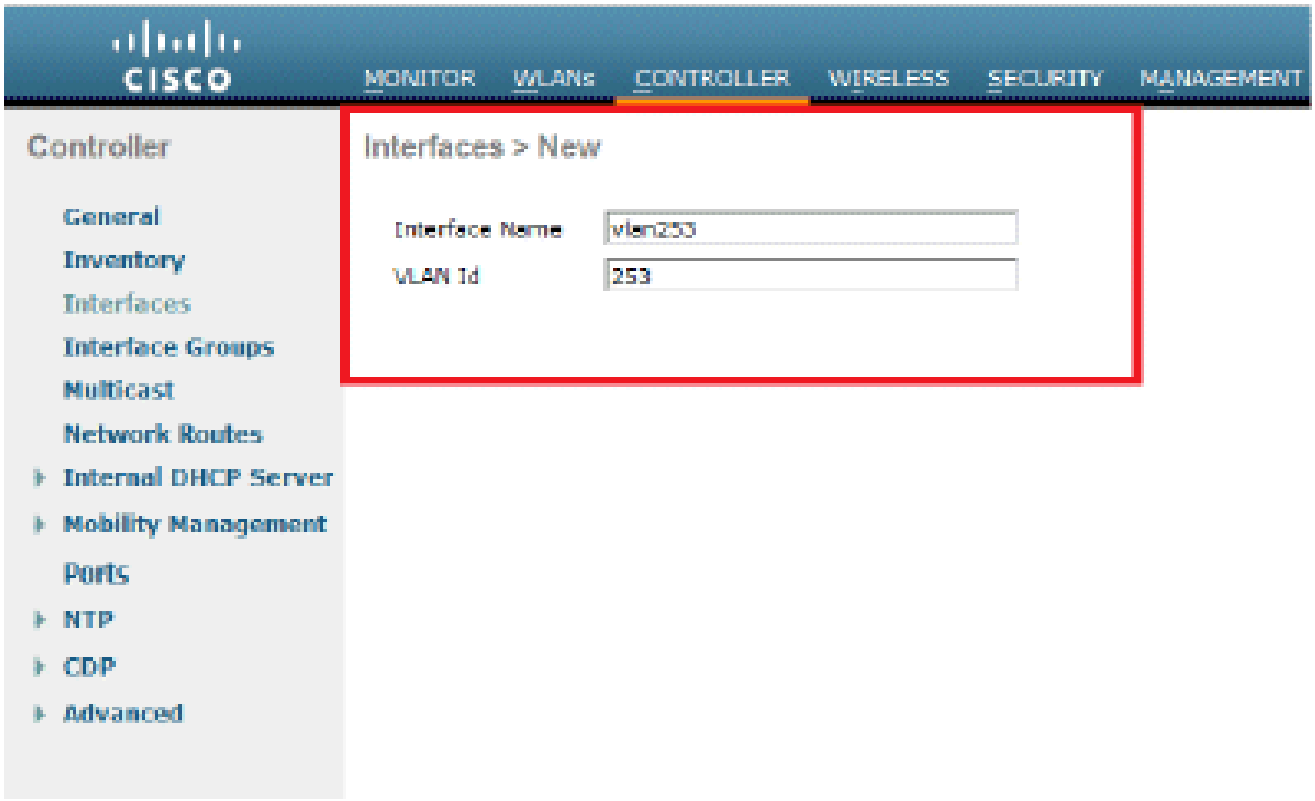


設定動態介面(VLAN)

以下過程介紹了如何在WLC上配置動態介面。

請完成以下步驟：

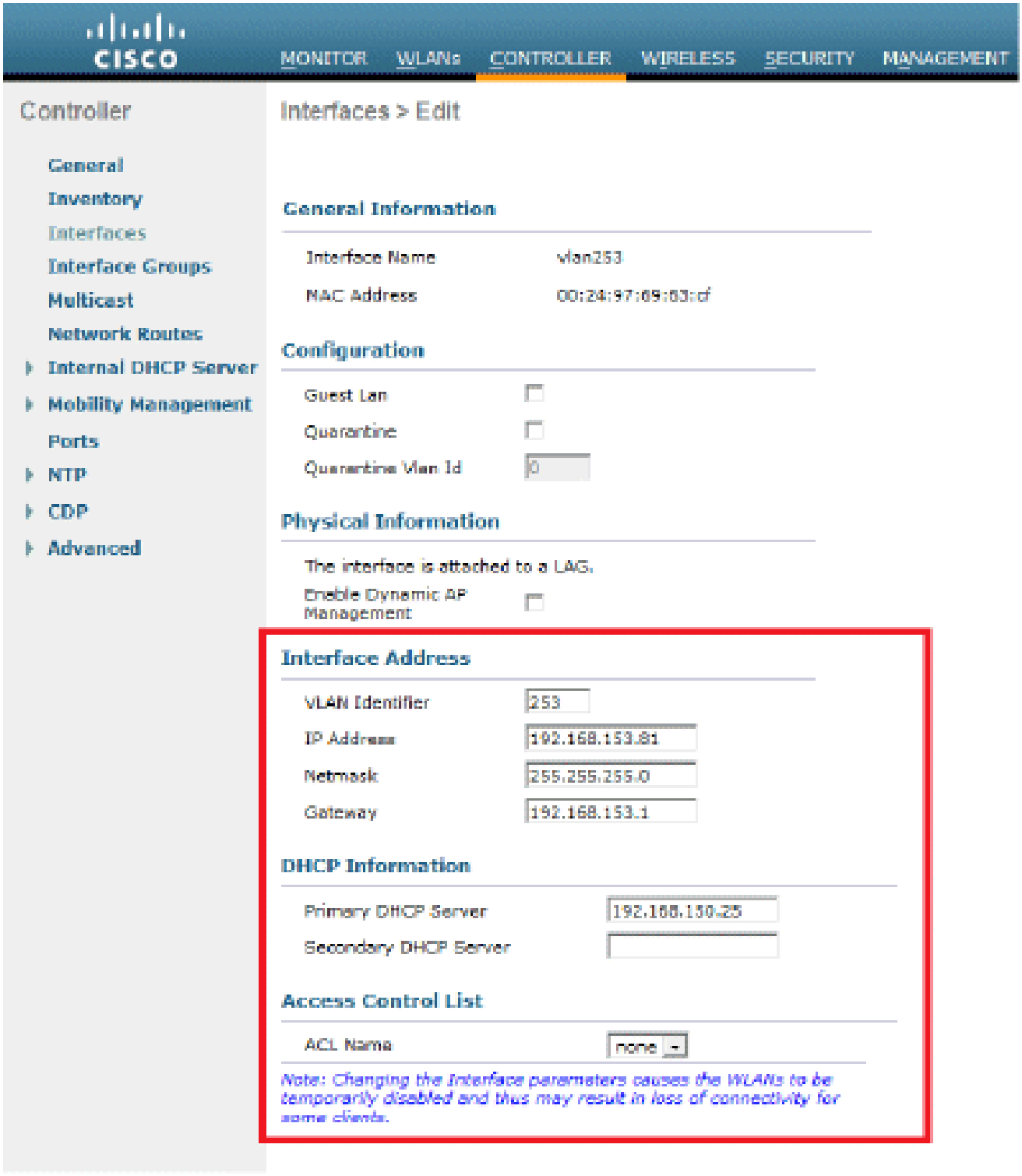
1. 動態介面是在Controller > Interfaces視窗中的控制器GUI上設定的。



2. 按一下「Apply」。

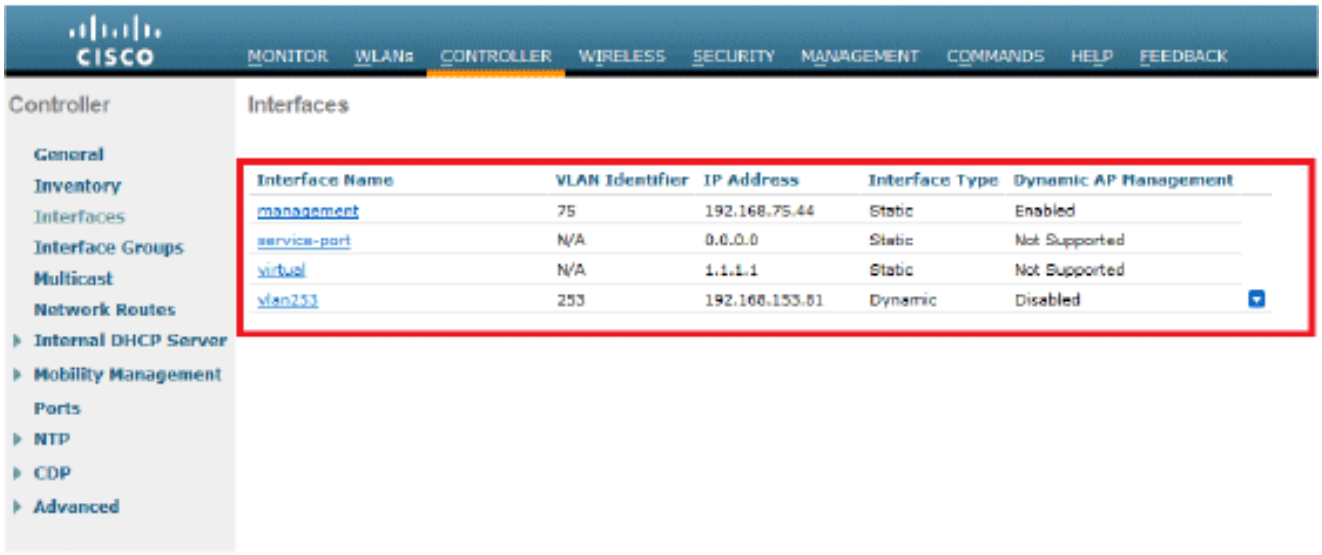
這將引導您進入此動態介面（此處為VLAN 253）的Edit（編輯）視窗。

3. 輸入此動態介面的IP地址和預設網關。



4. 按一下「Apply」。

5. 配置的介面將如下所示：



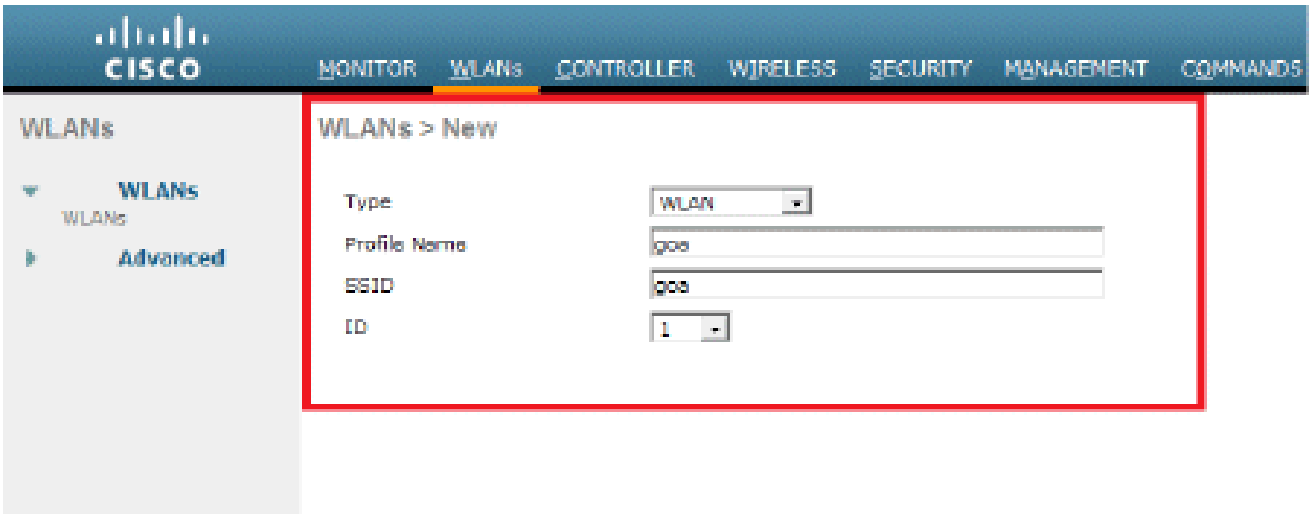
配置WLAN(SSID)

以下程式說明如何在WLC中設定WLAN。

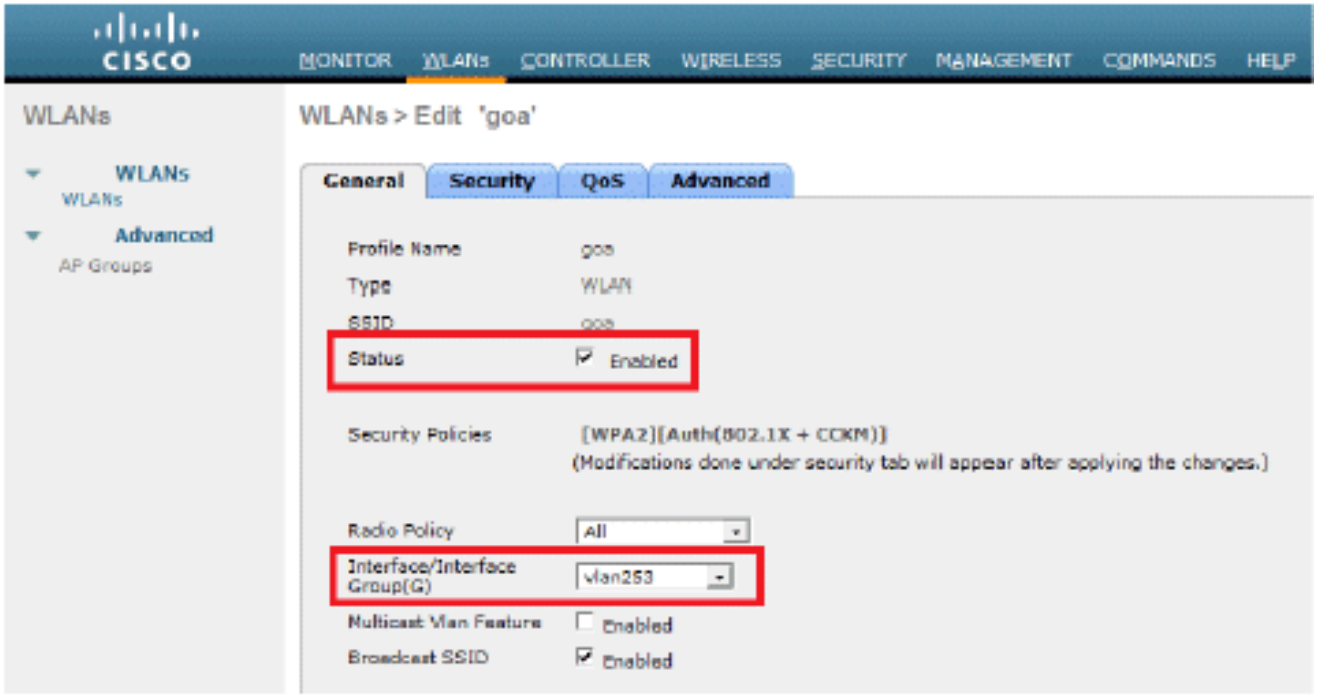
請完成以下步驟：

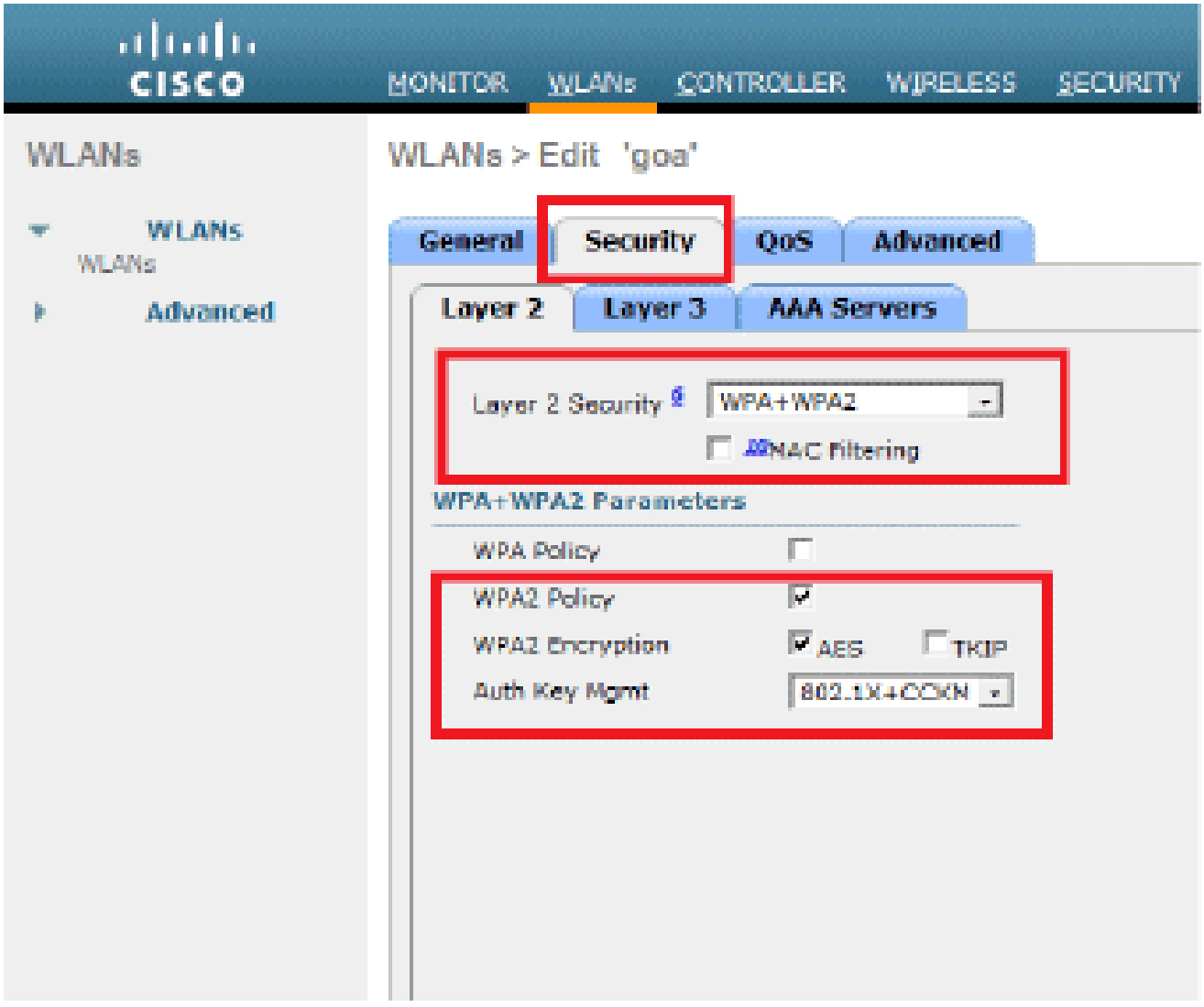
1. 在控制器GUI上，前往WLANs > Create New以建立一個新的WLAN。此時會顯示「新建WLAN」視窗。
2. 輸入WLAN ID和WLAN SSID資訊。

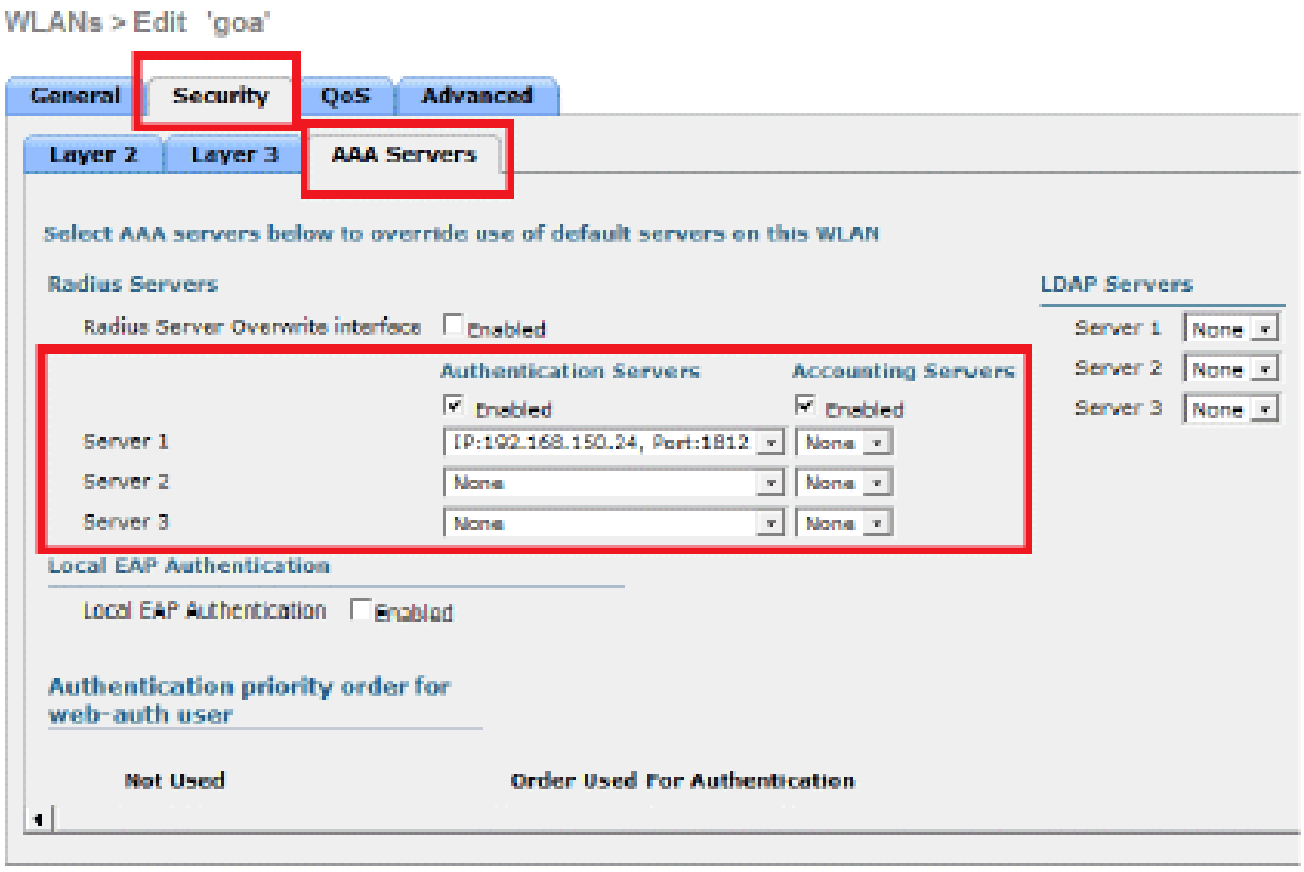
   您可以輸入任何名稱作為WLAN SSID。此範例使用goa作為WLAN SSID。

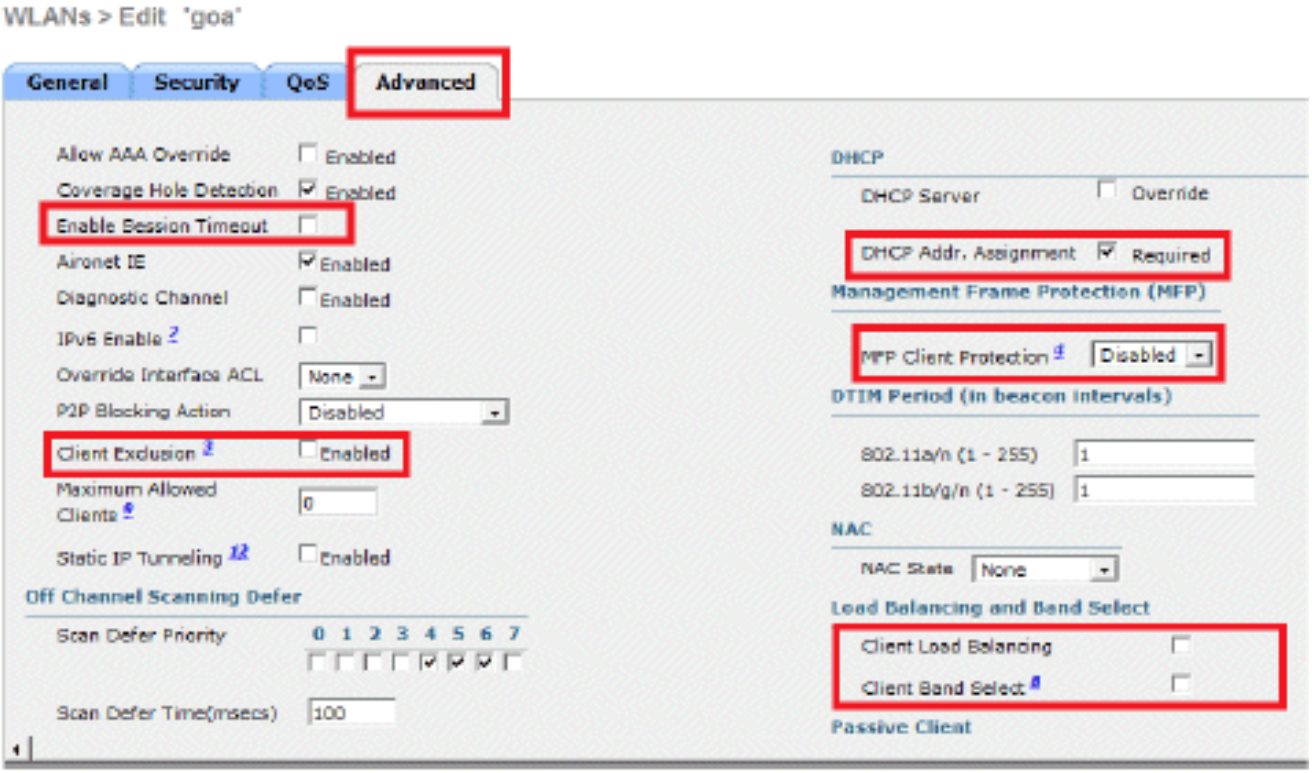


3. 按一下「Apply」以前往WLAN Goa的「Edit」視窗。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'goa'
General Security QoS Advanced
Profile Name goa
Type WLAN
SSID goa
Status Enabled
Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface/Interface Group(G) vlan253
Multicast Vlan Feature Enabled
Broadcast SSID Enabled


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'goa'
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption AES TKIP
Auth Key Mgmt 802.1X+CCKM





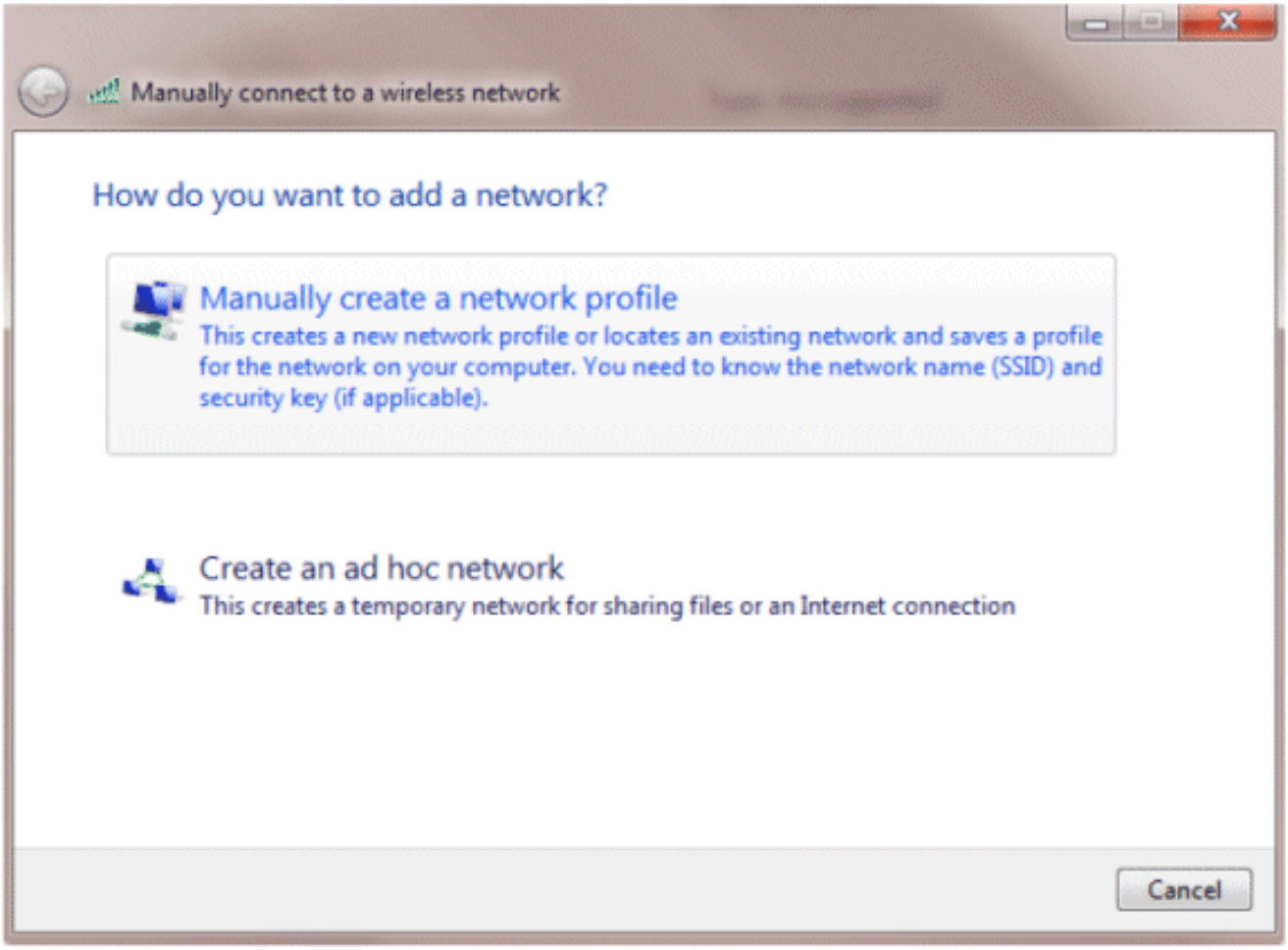
配置無線客戶端實用程式

PEAP-MSCHAPv2（使用者1）

在我們的測試客戶端中，我們使用Windows 7本機請求方和運行14.3驅動程式版本的英特爾6300-N卡。建議使用供應商提供的最新驅動程式進行測試。

完成以下步驟，以便在Windows零配置(WZC)中建立配置檔案：

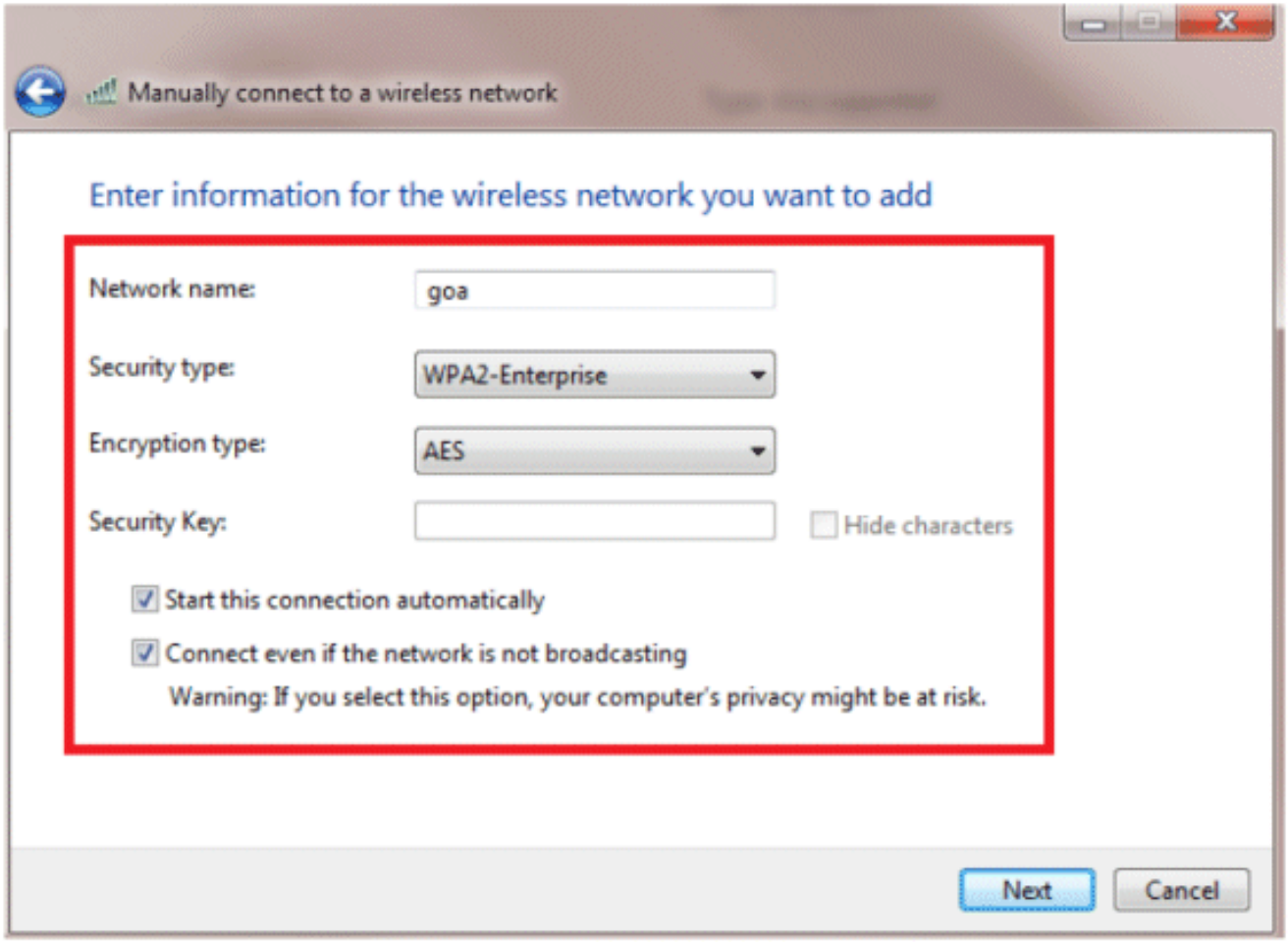
1. 前往控制面板 > 網路和Internet > 管理無線網路。
2. 按一下Add頁籤。
3. 按一下「Manually create a network profile」。



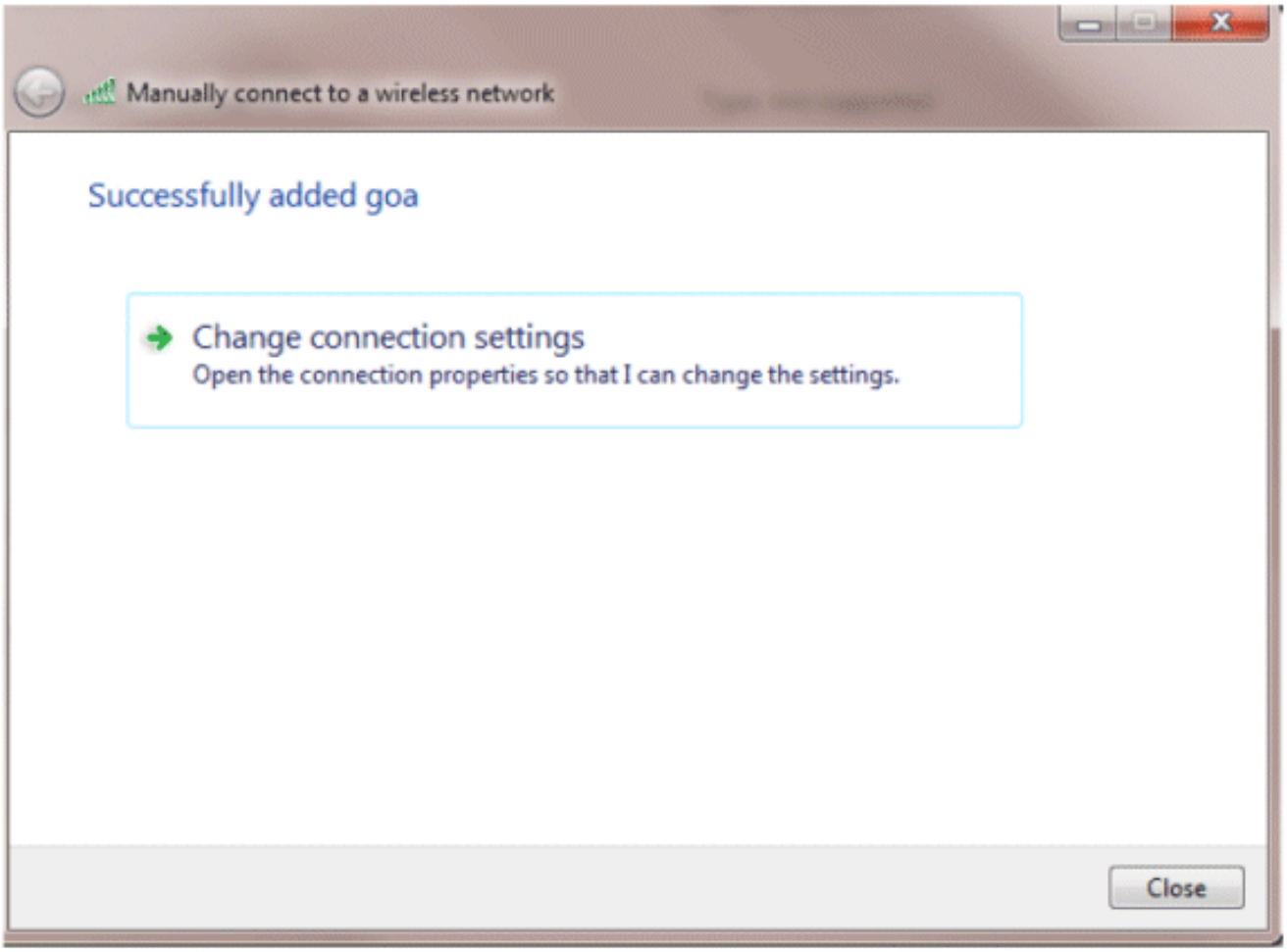
4. 新增在WLC上設定的詳細資訊。

   注意：SSID區分大小寫。

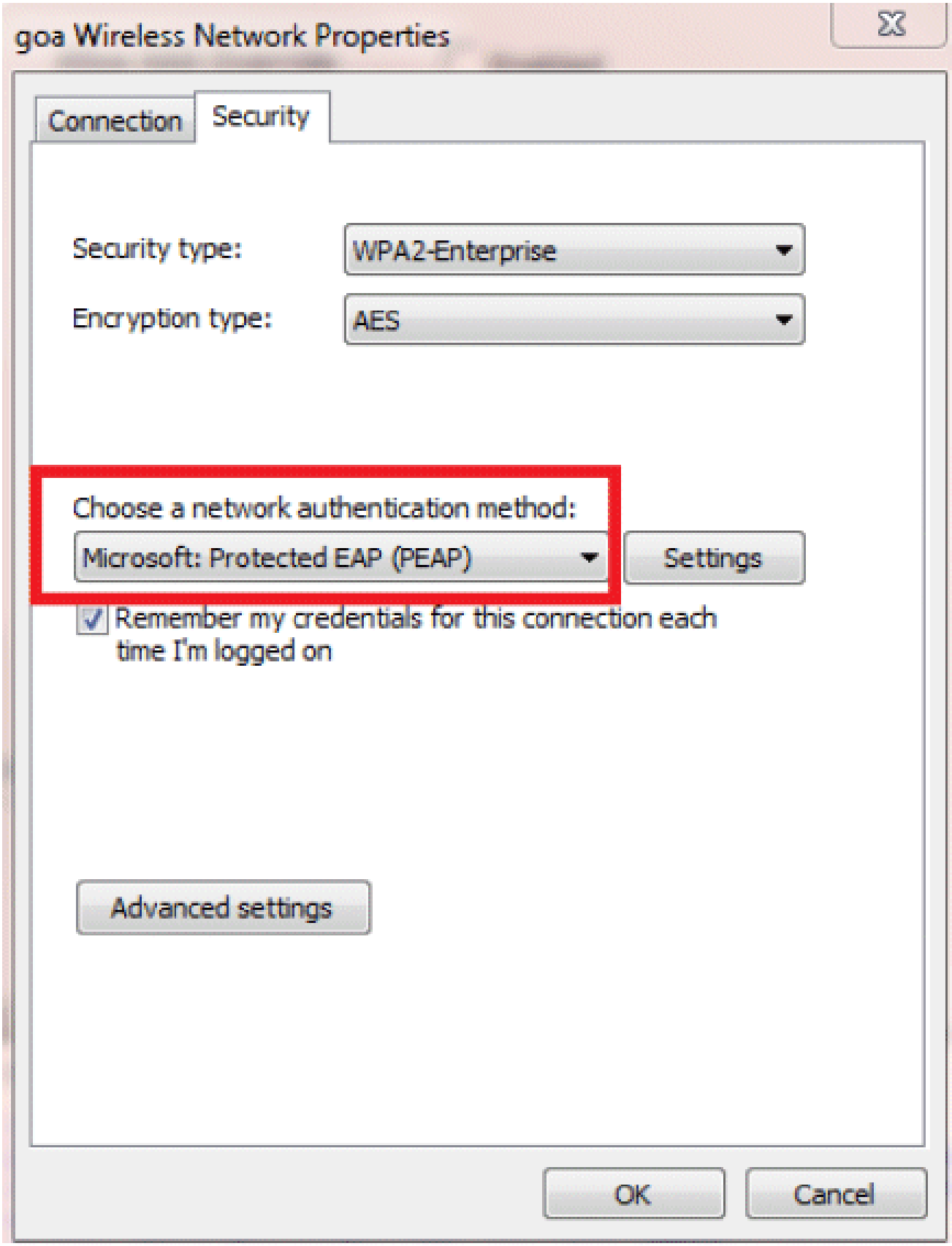
5. 按「Next」（下一步）。

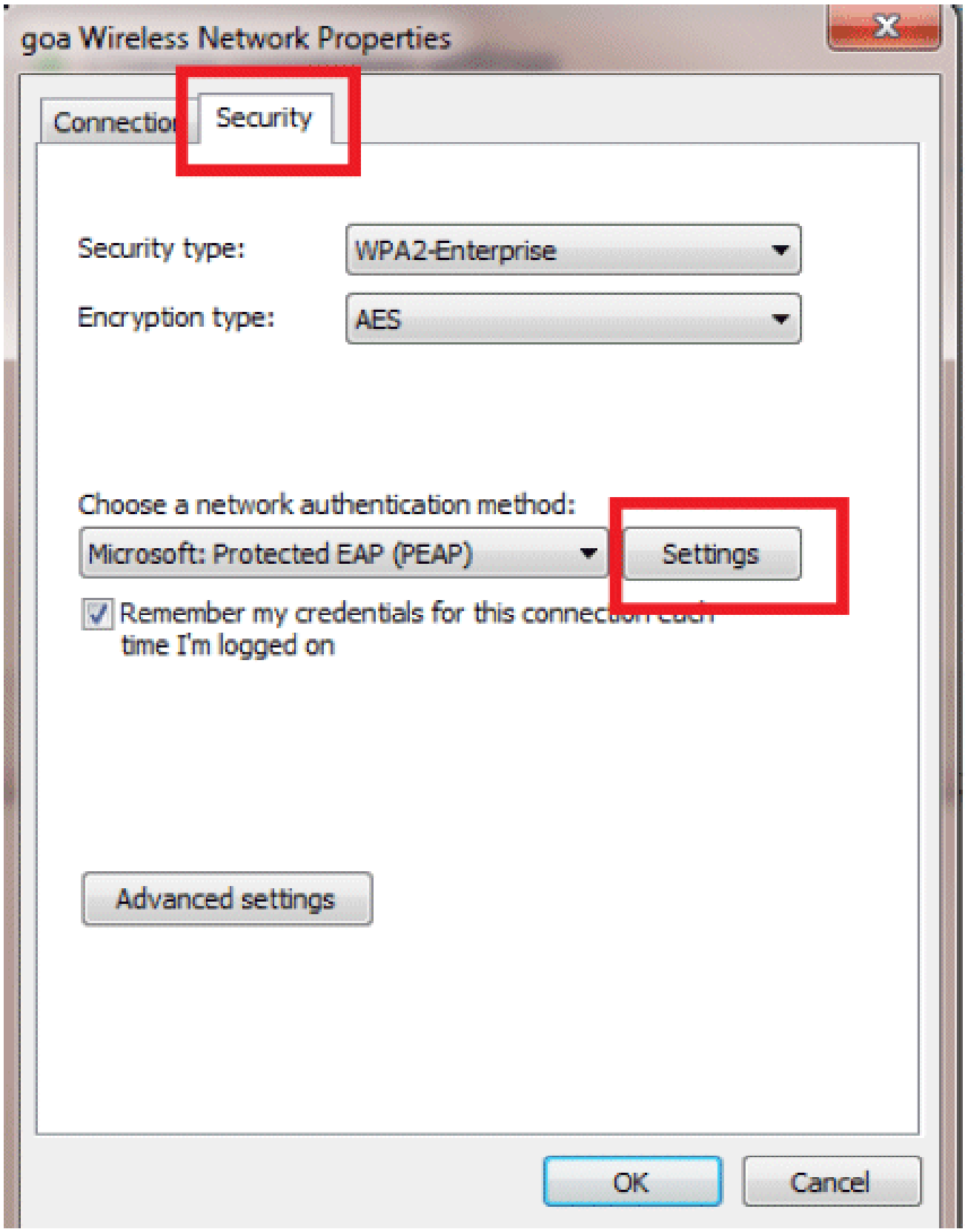


6. 按一下「Change connection settings」以再次檢查設定。

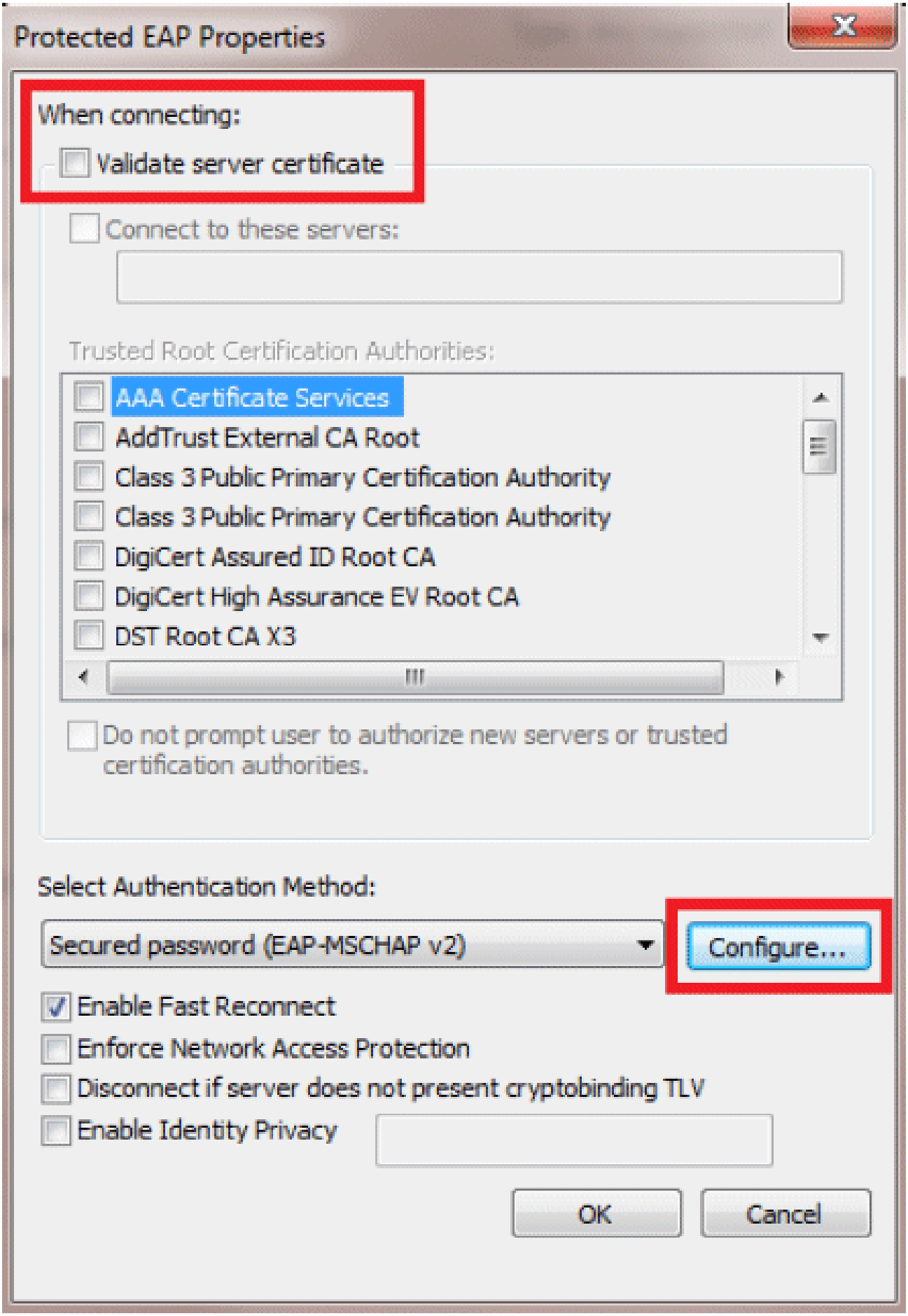


7. 請確保您已啟用PEAP。


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel

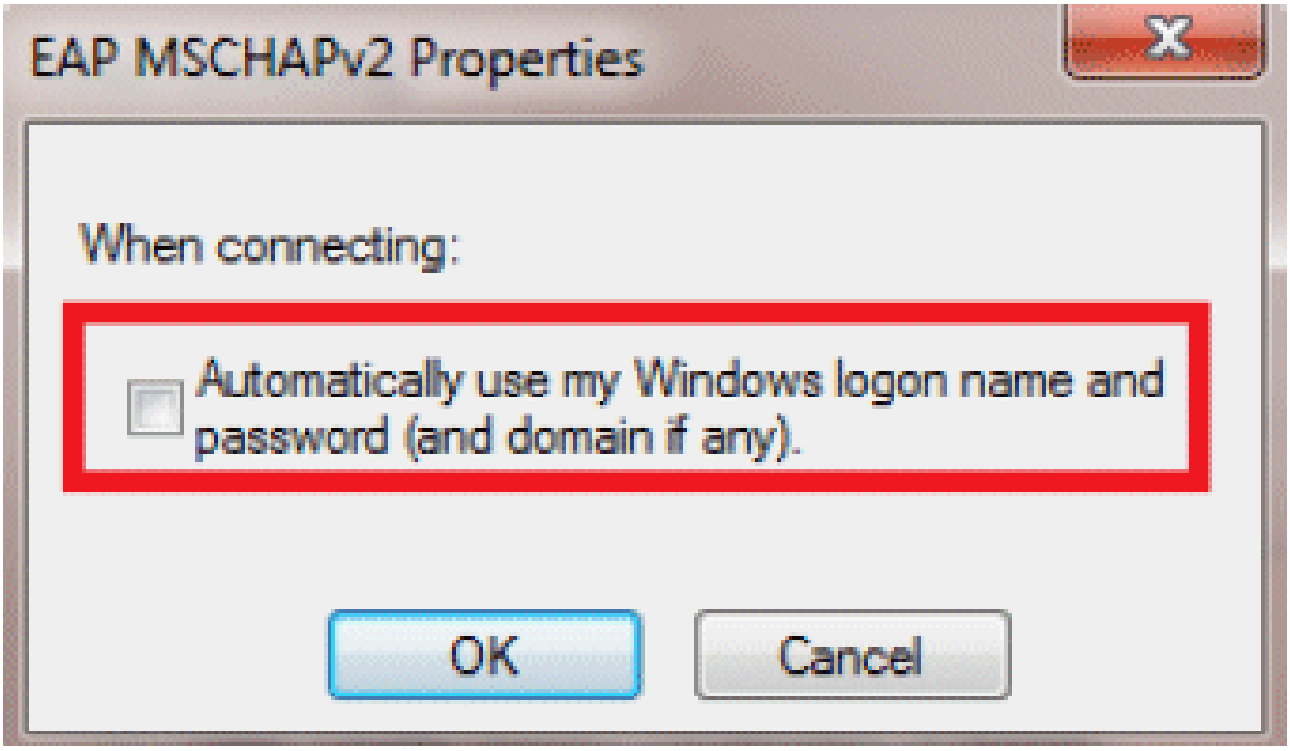


8. 在本例中，我們沒有驗證伺服器證書。如果選中此框且無法連線，請嘗試禁用該功能並再次測試。

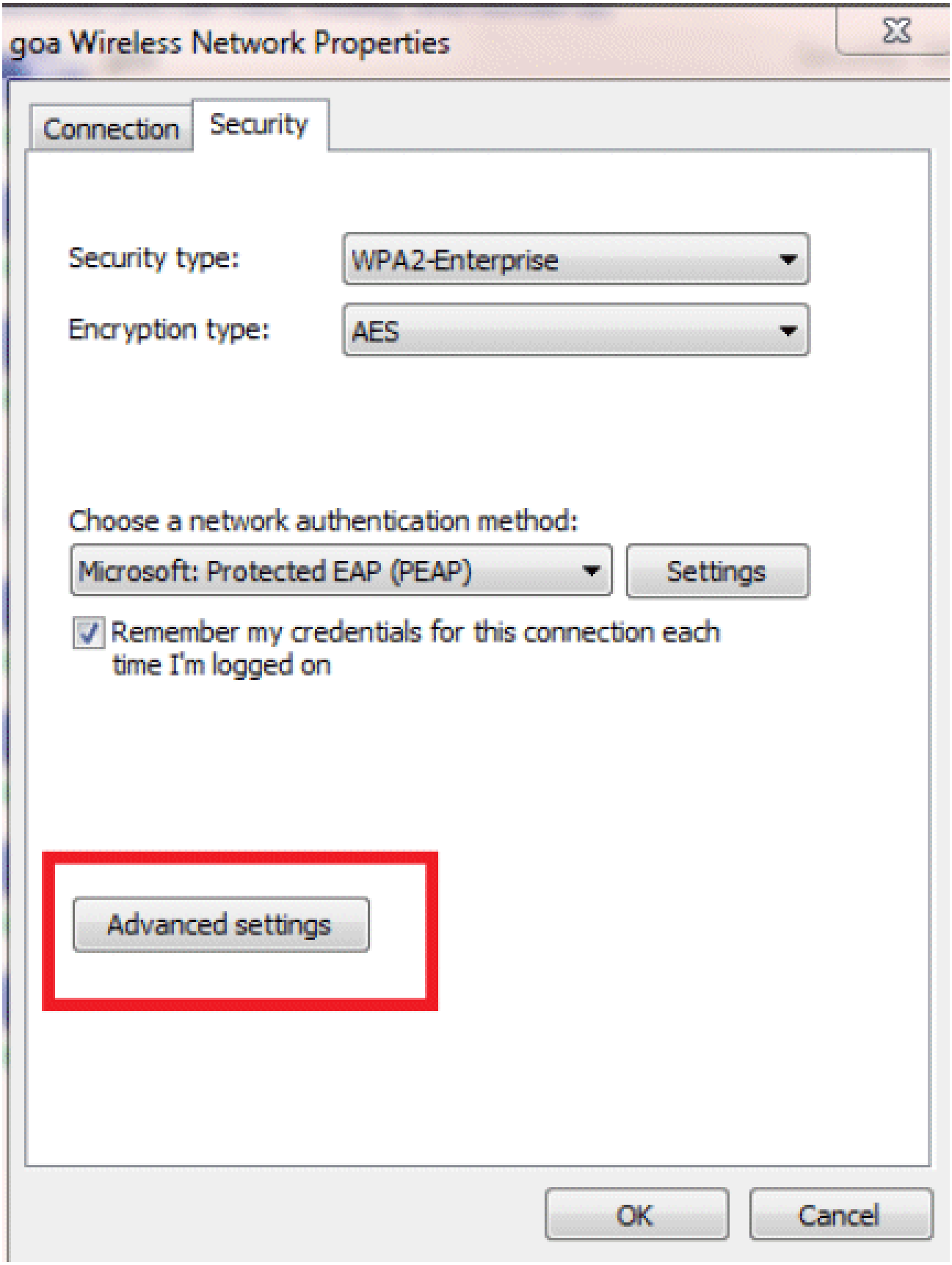


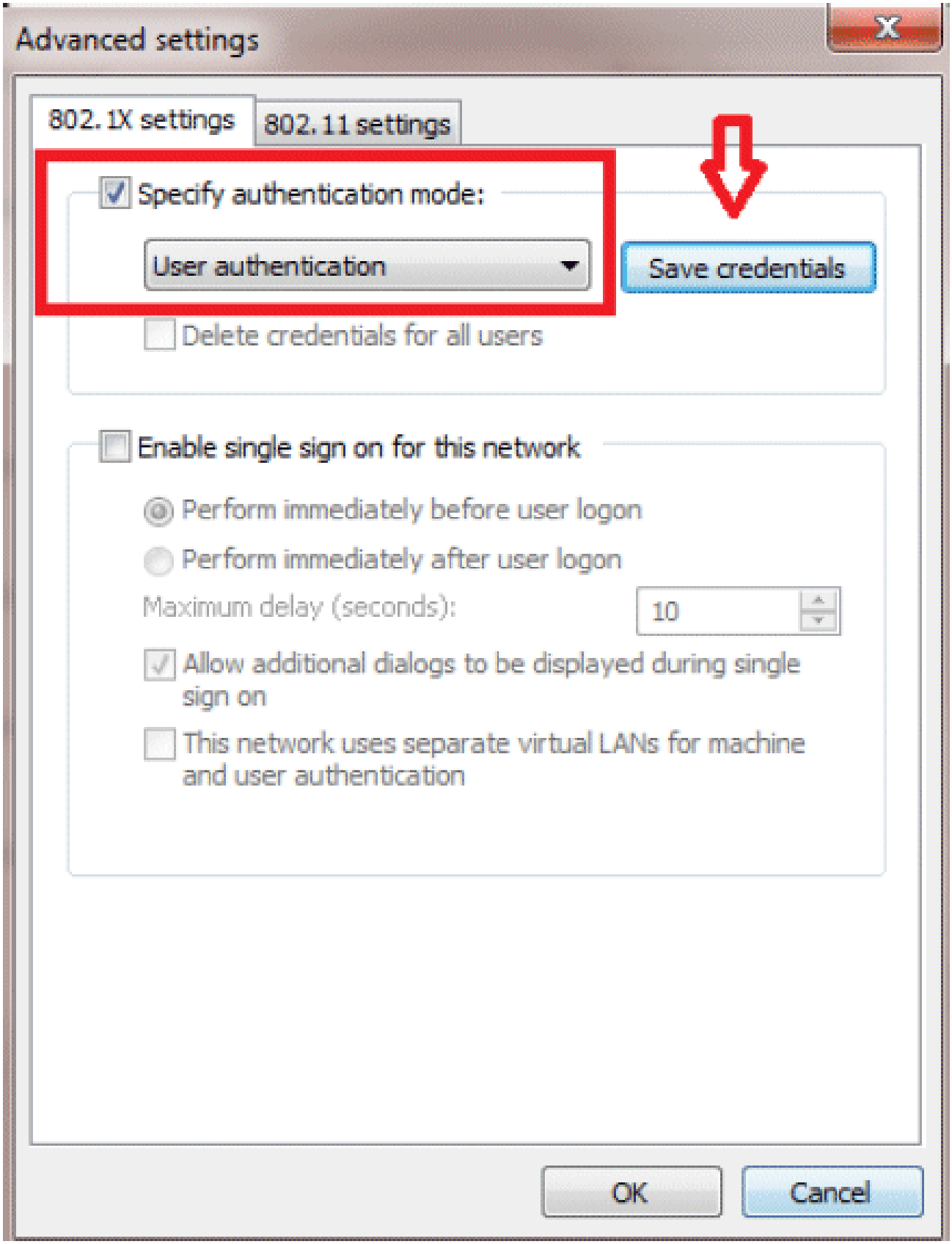
9. 或者，您可以使用您的Windows憑據登入。但是，在本例中，我們不打算使用它。按一下「

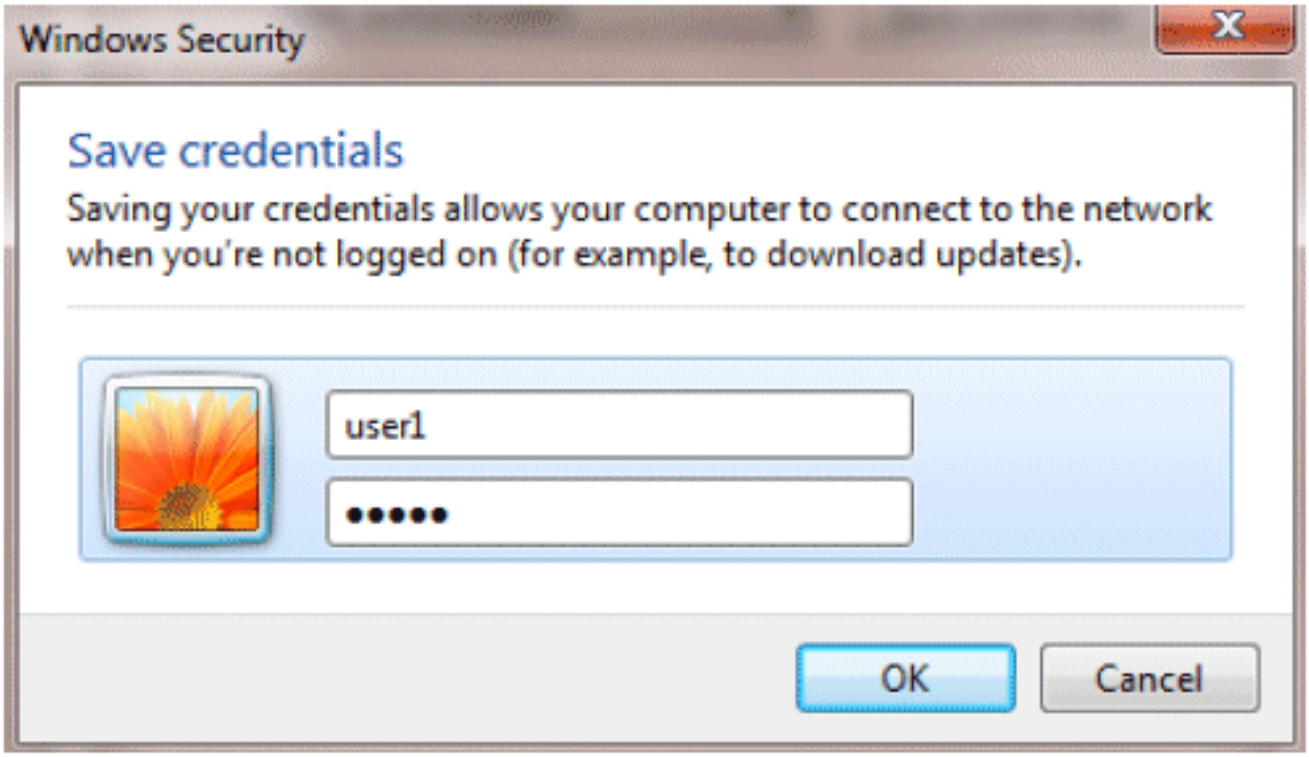
OK」（確定）。



10. 按一下「Advanced settings」以設定使用者名稱和密碼。


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



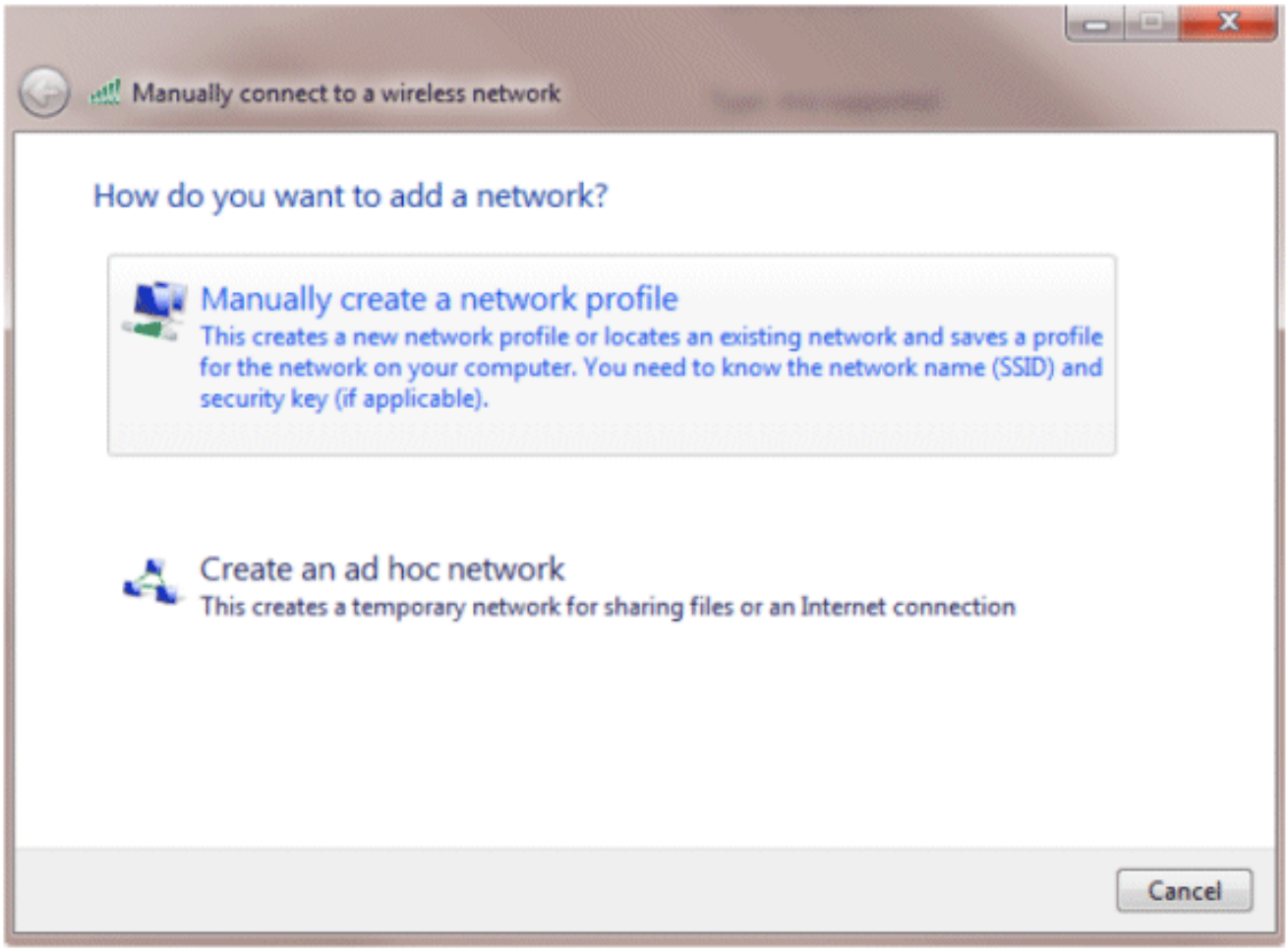
您的客戶端實用程式現在已準備好連線。

EAP-FAST（使用者2）

在我們的測試客戶端中，我們使用Windows 7本機請求方和運行14.3驅動程式版本的英特爾6300-N卡。建議使用供應商提供的最新驅動程式進行測試。

完成以下步驟，以便在WZC中建立配置檔案：

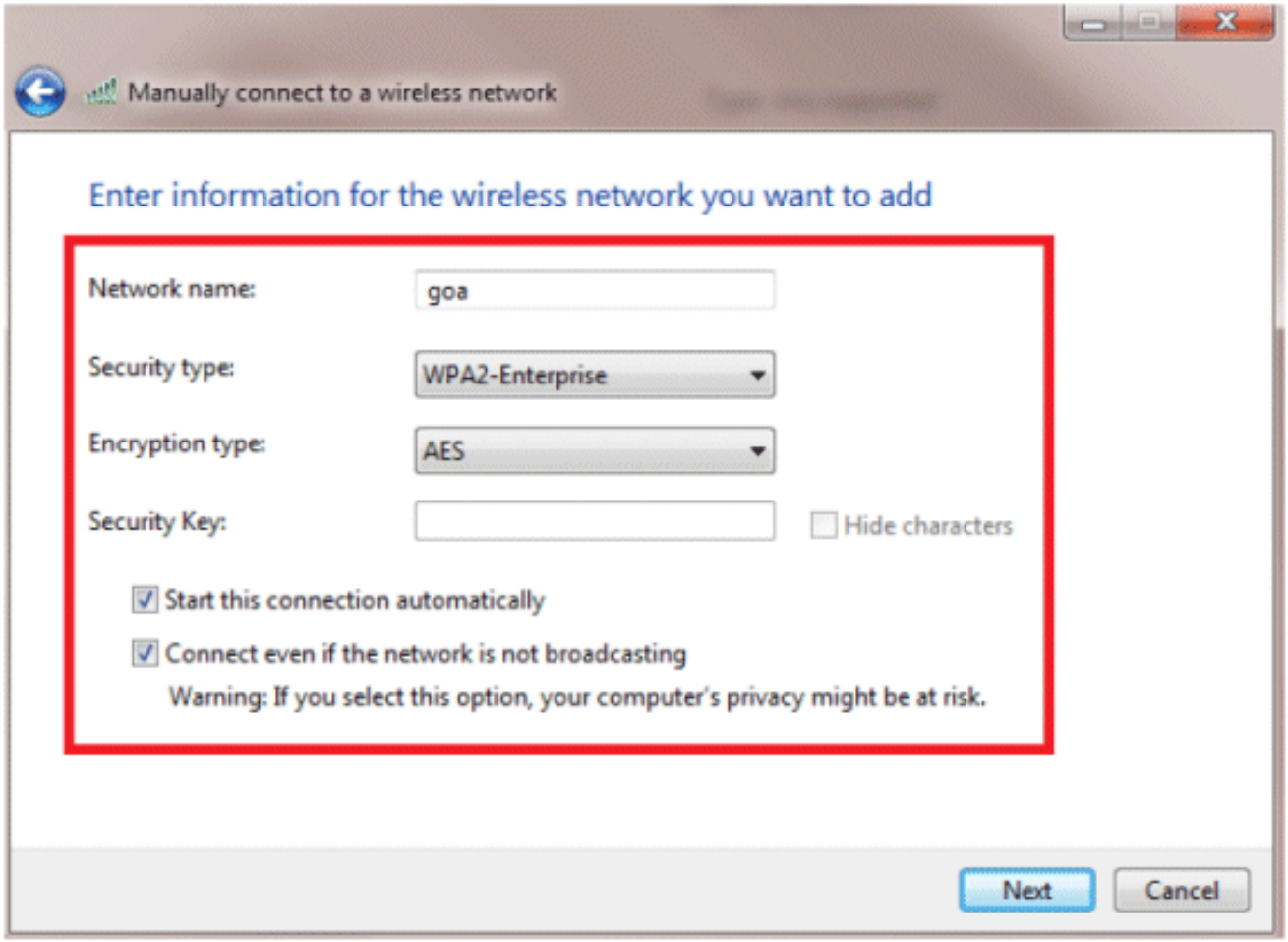
1. 前往控制面板 > 網路和Internet > 管理無線網路。
2. 按一下Add頁籤。
3. 按一下「Manually create a network profile」。



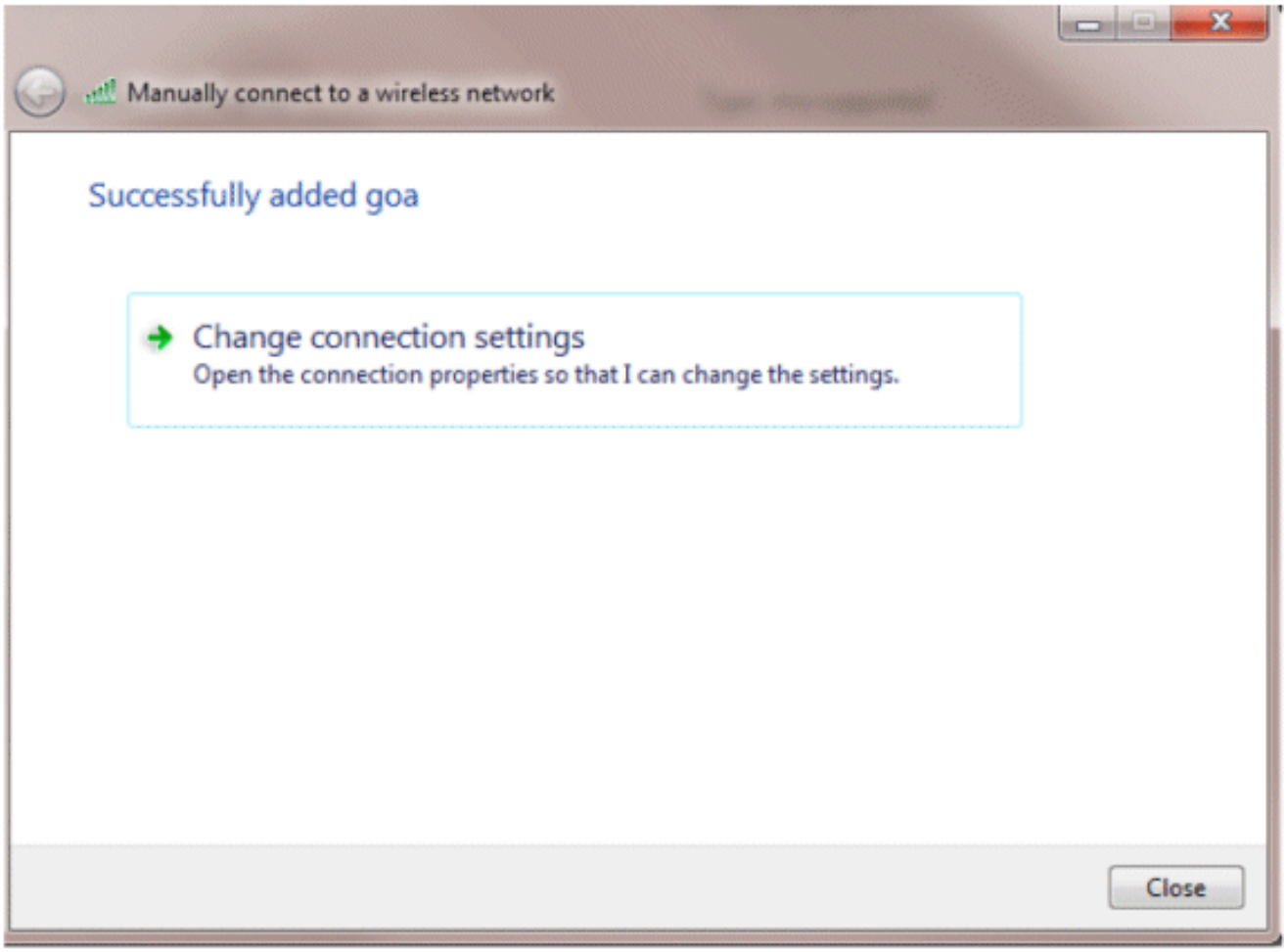
4. 新增在WLC上設定的詳細資訊。

   注意：SSID區分大小寫。

5. 按「Next」（下一步）。

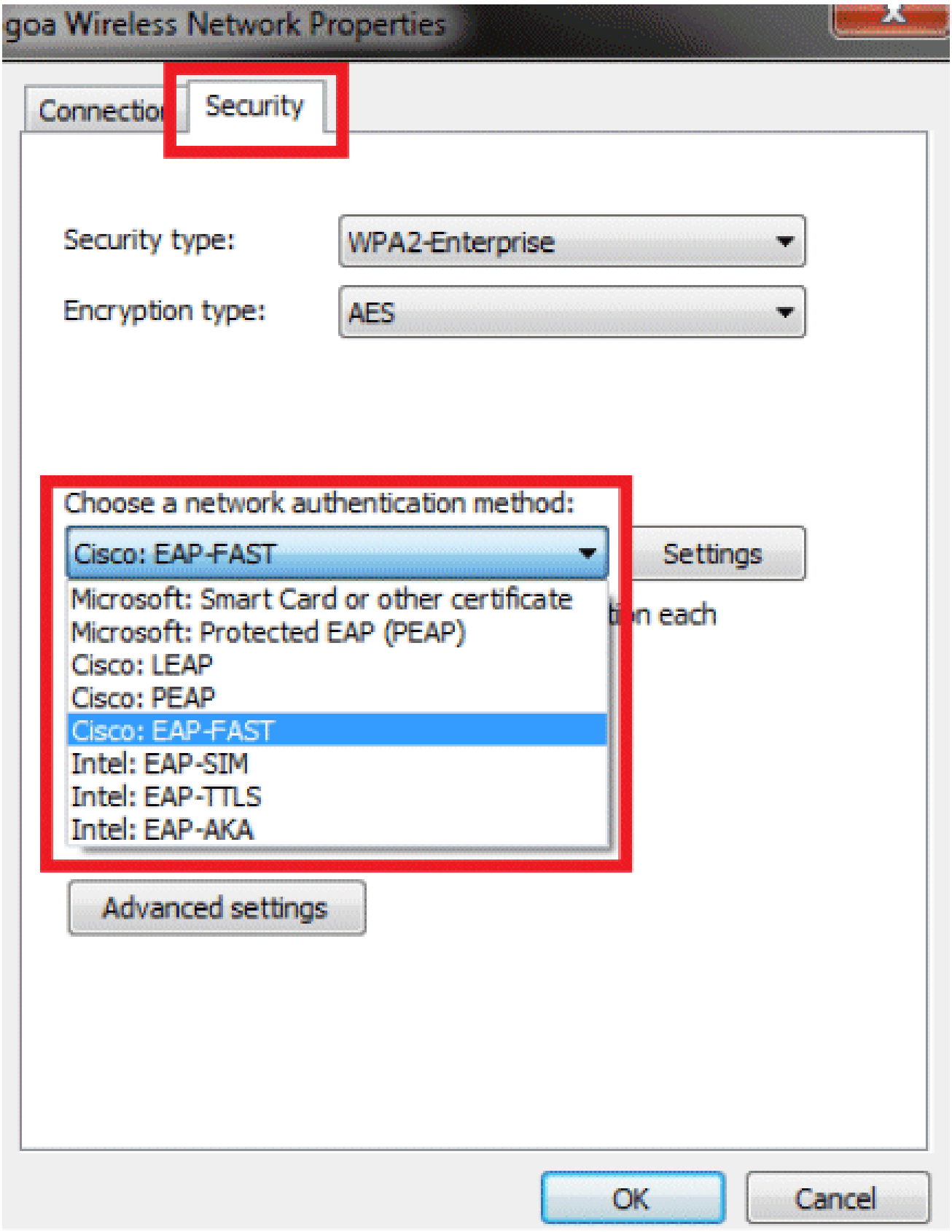


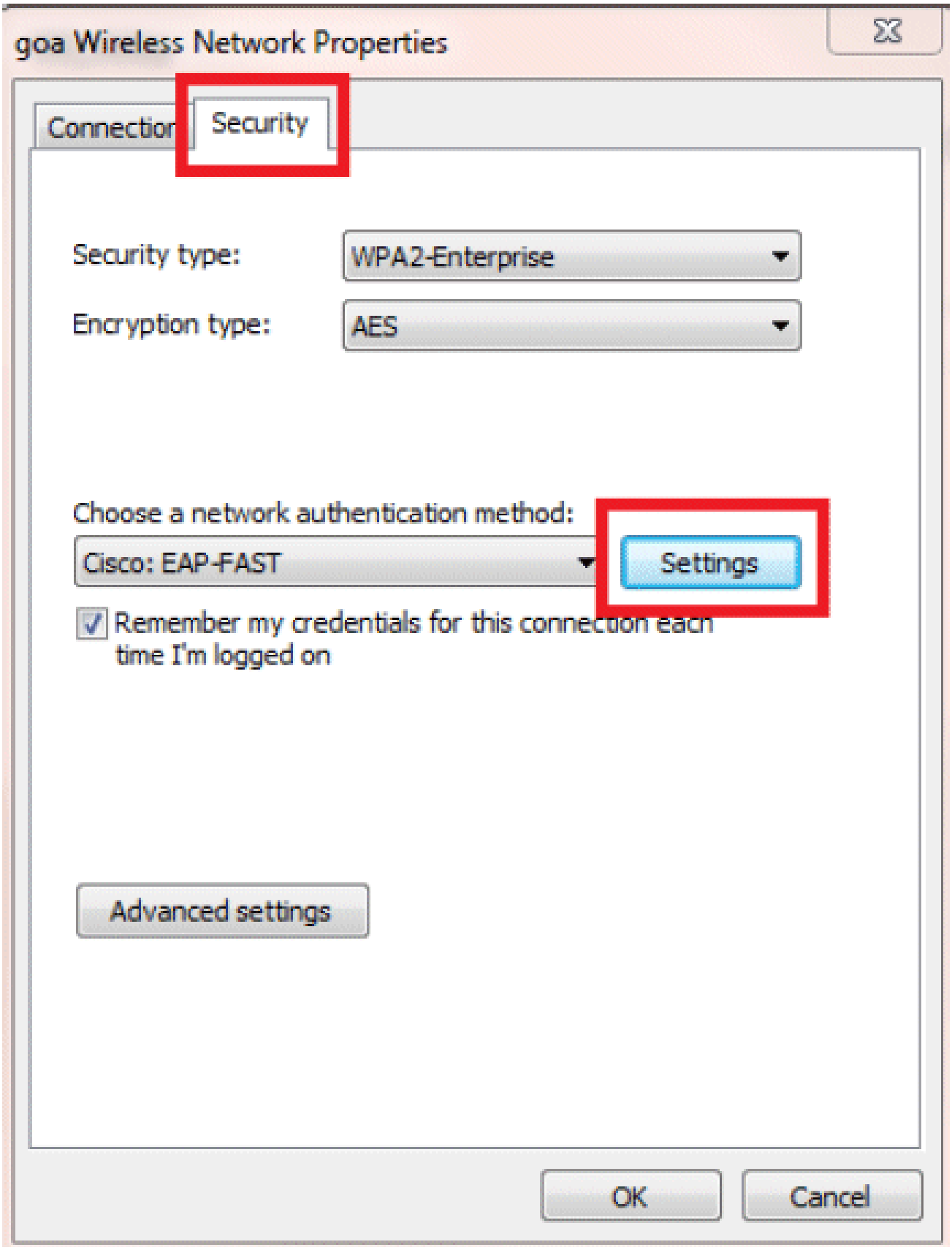
6. 按一下「Change connection settings」以再次檢查設定。



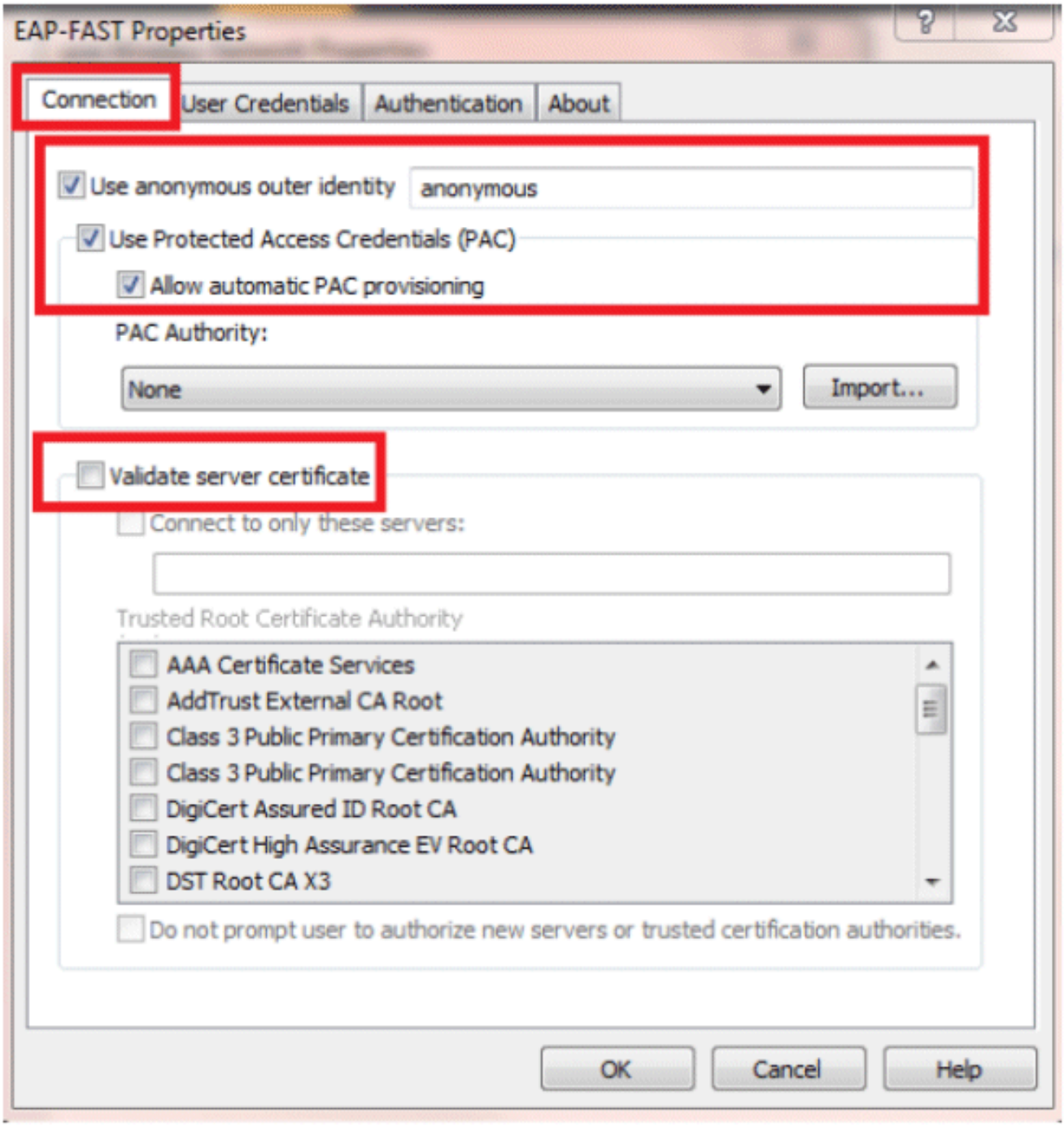
7. 確保已啟用EAP-FAST。

注意：預設情況下，WZC沒有EAP-FAST作為身份驗證方法。您必須從第三方供應商下載該實用程式。在本示例中，由於它是英特爾卡，因此系統中安裝了英特爾PROSet。

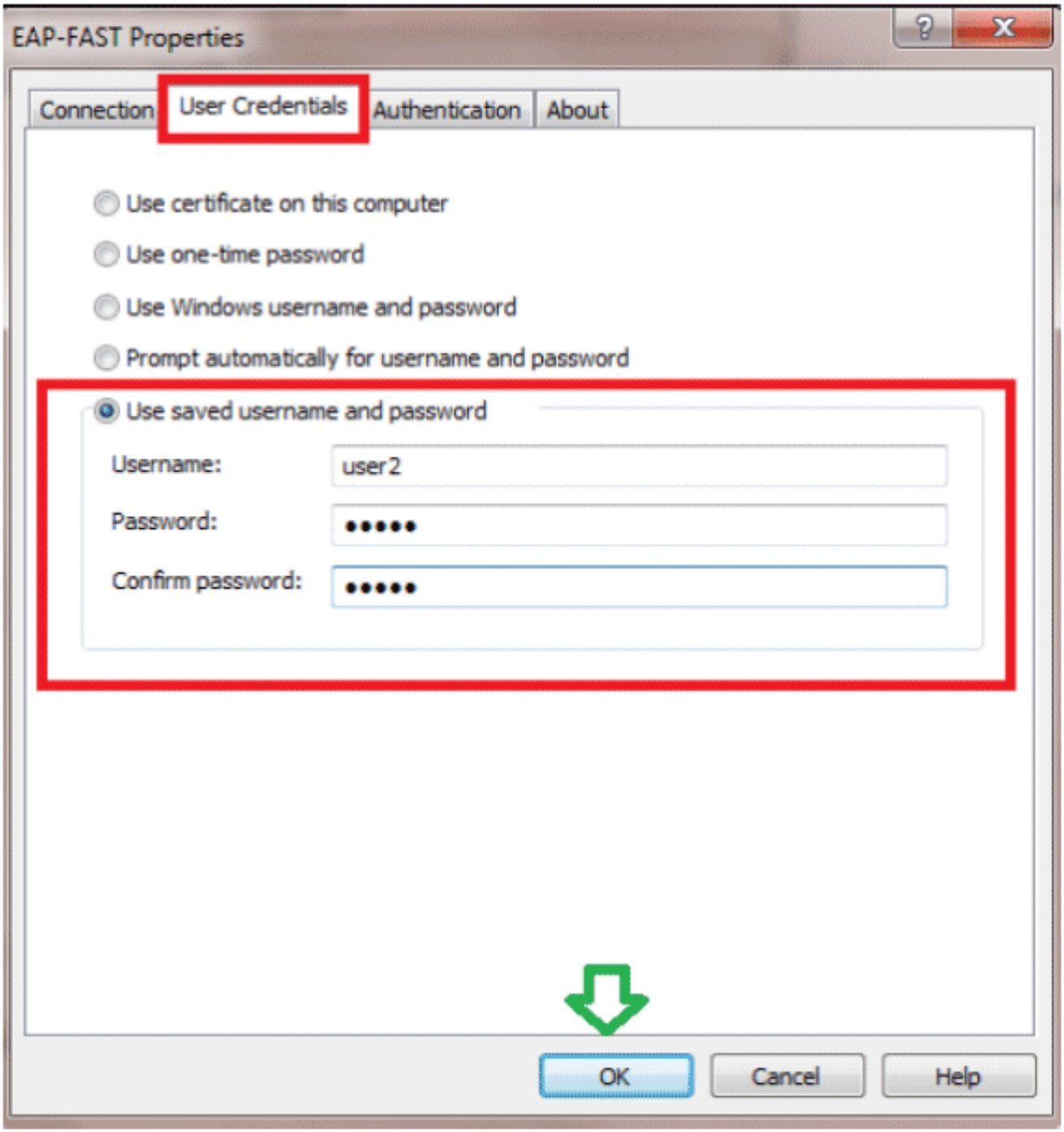

goa Wireless Network Properties
Connectio
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Cisco: EAP-FAST
Settings
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Cisco: LEAP
Cisco: PEAP
Cisco: EAP-FAST
Intel: EAP-SIM
Intel: EAP-TTLS
Intel: EAP-AKA
Advanced settings
OK
Cancel



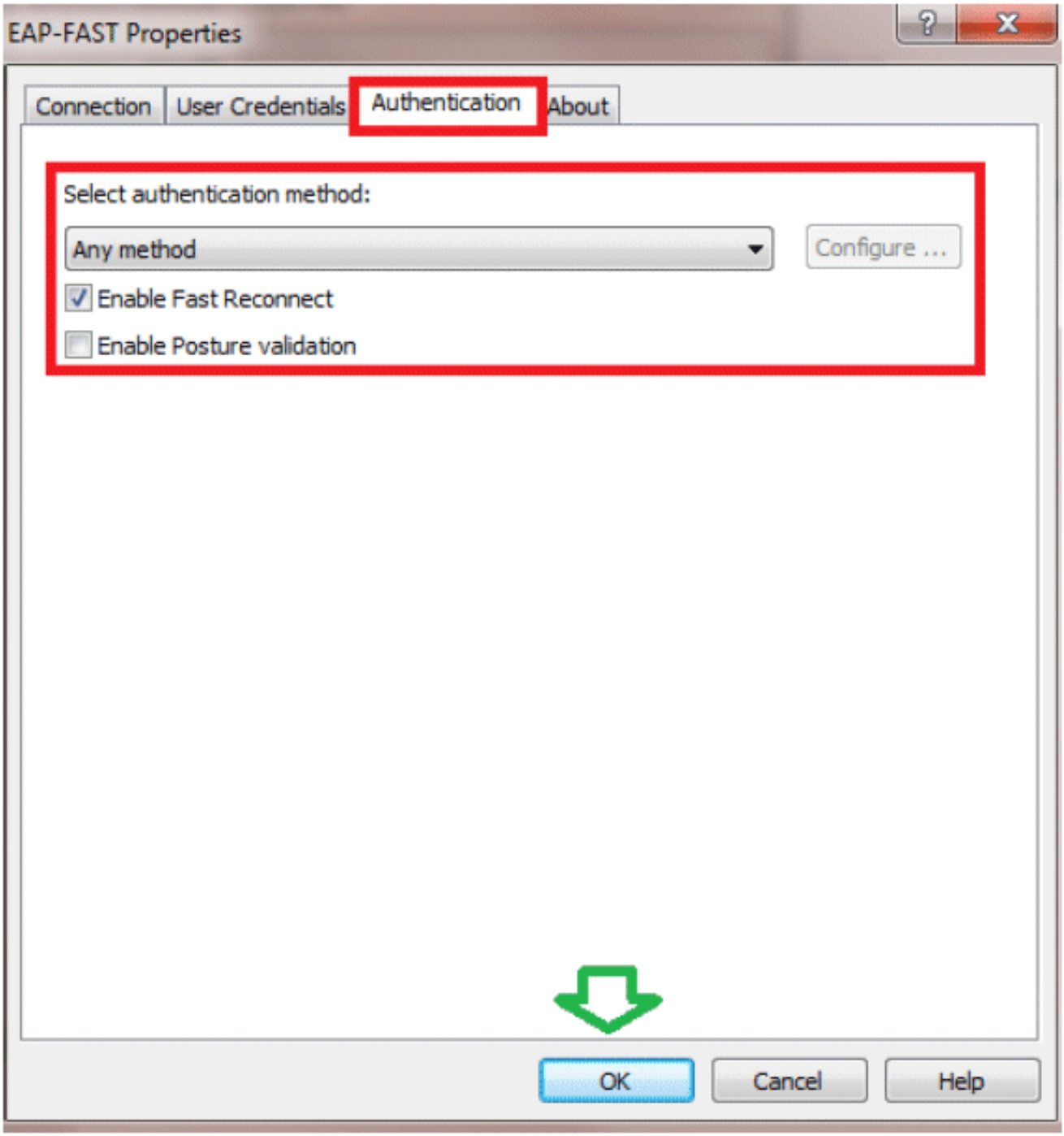
8. 啟用Allow automatic PAC provisioning並確保未選中Validate server certificate。



9. 按一下User Credentials頁籤，然後輸入user2的憑據。或者，您可以使用您的Windows憑據登入。但是，在本例中，我們不打算使用它。

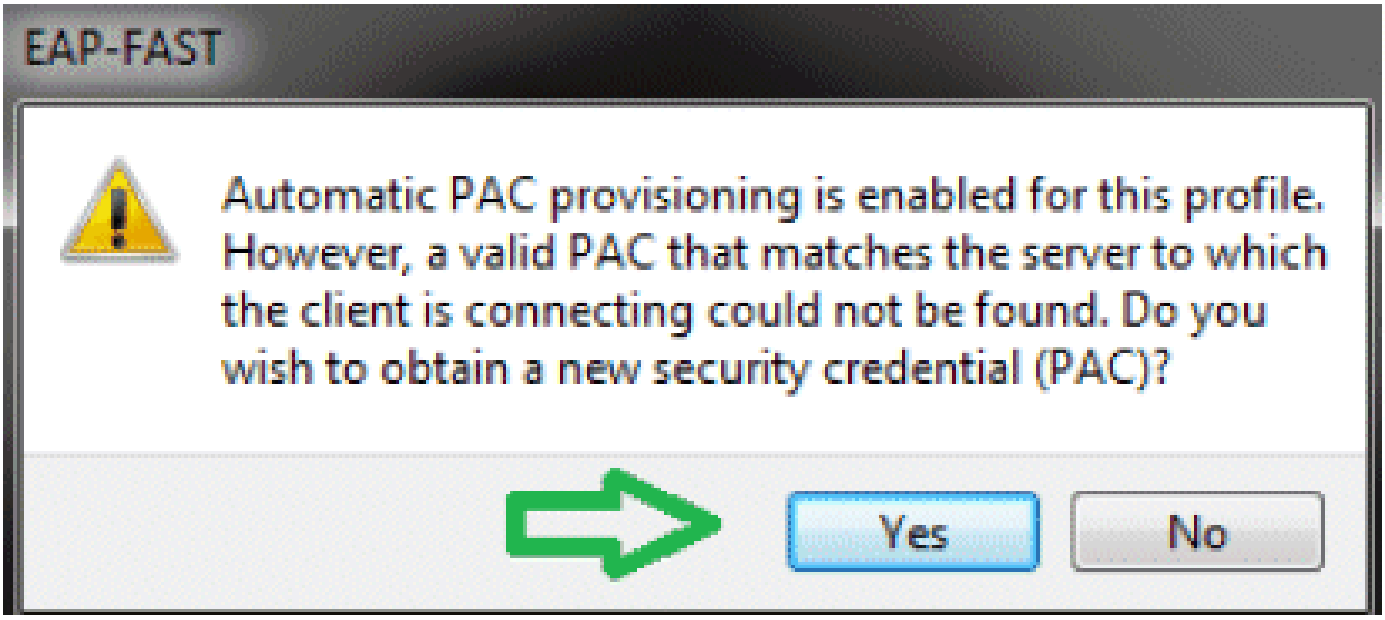

EAP-FAST Properties
Connection
User Credentials
Authentication
About
Use certificate on this computer
Use one-time password
Use Windows username and password
Prompt automatically for username and password
Use saved username and password
Username:
user2
Password:
Confirm password:
OK
Cancel
Help

10. 按一下「OK」（確定）。



現在，您的客戶端實用程式已準備就緒，可以連線user2。

注意：user2嘗試進行身份驗證時，RADIUS伺服器將傳送PAC。接受PAC以完成身份驗證。



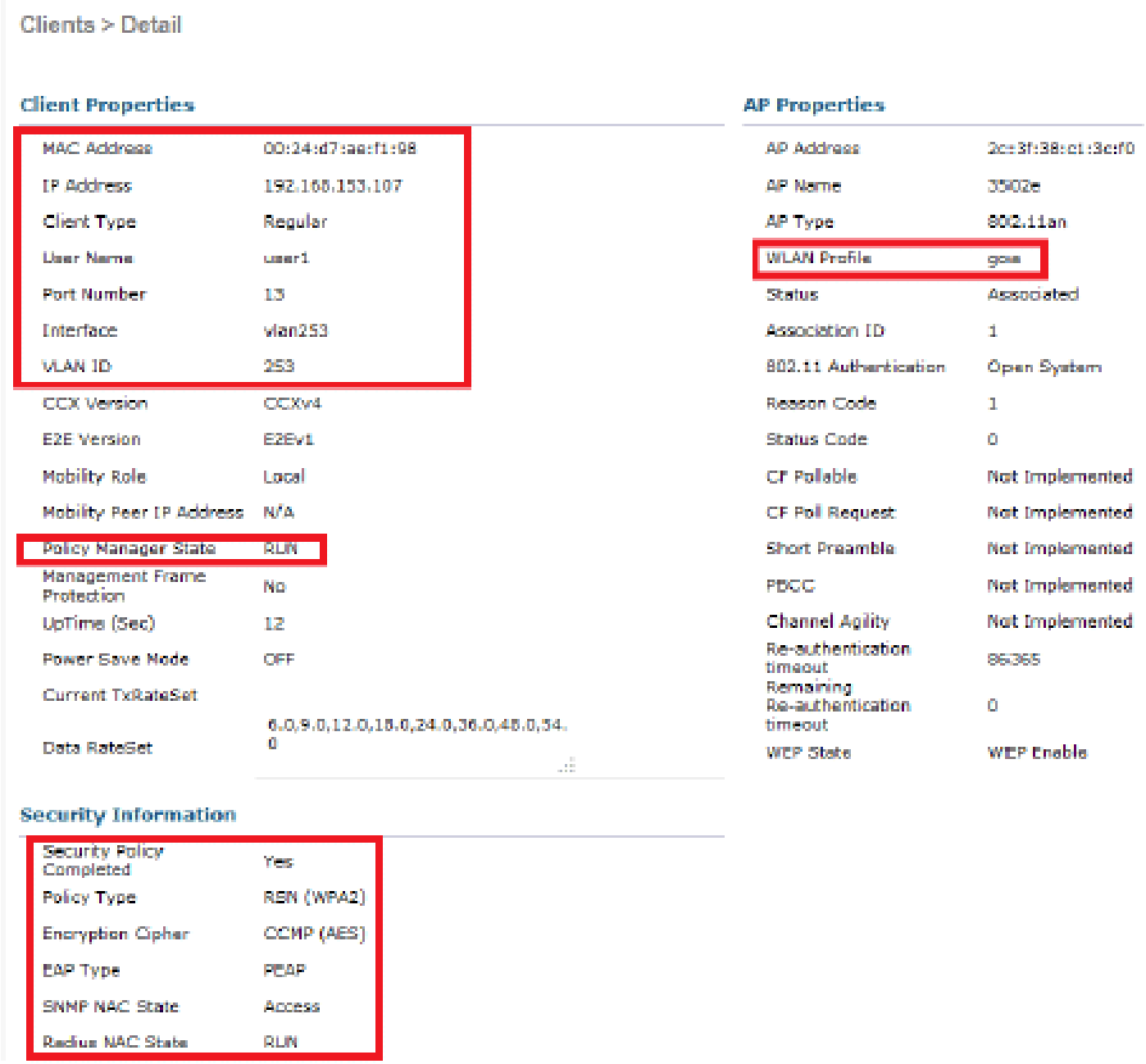
驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

驗證user1(PEAP-MSCHAPv2)

在WLC GUI中，前往Monitor > Clients，然後選擇MAC位址。



WLC RADIUS統計資訊：

<#root>

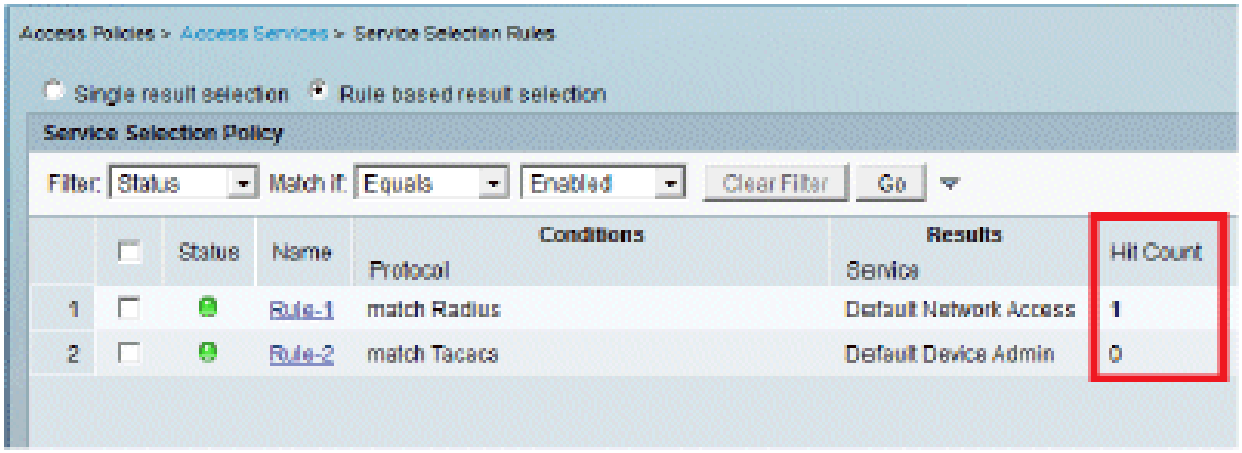
```
(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
```

```
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

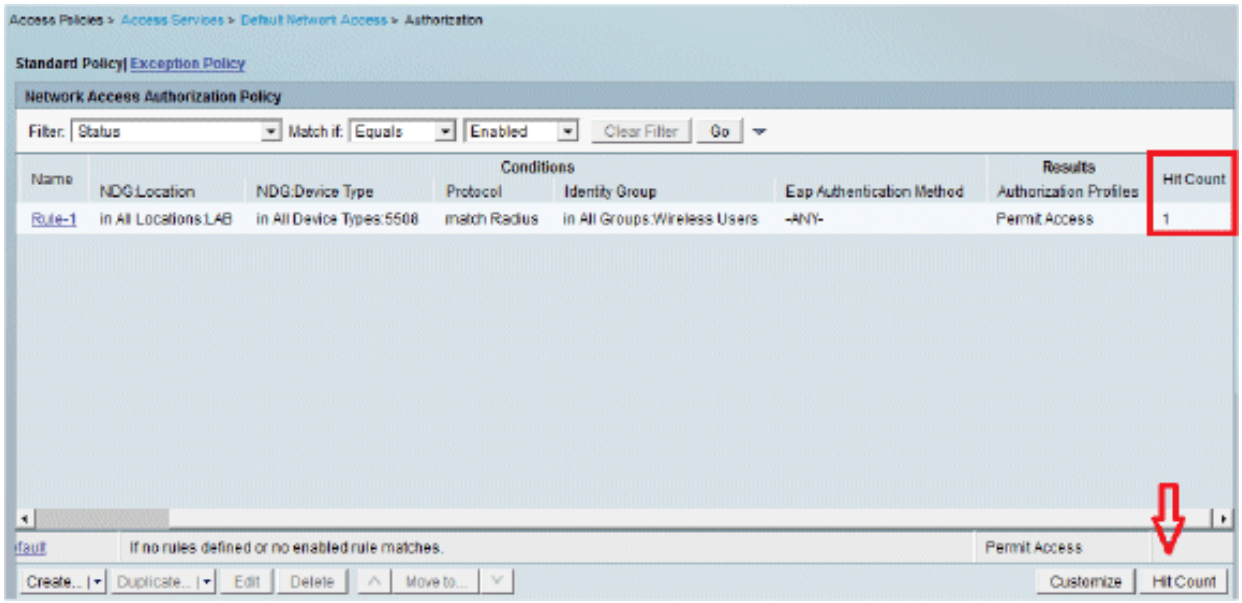
ACS日誌：

1. 完成以下步驟即可檢視命中次數：

   a. 如果您在身份驗證的15分鐘內檢查日誌，請確保刷新命中數。



   b. 同一頁底部有一個Hit Count頁籤。



2. 按一下Monitoring and Reports，此時會顯示New彈出視窗。轉到Authentications -Radius - Today。您還可以按一下Details以驗證應用了哪個服務選擇規則。

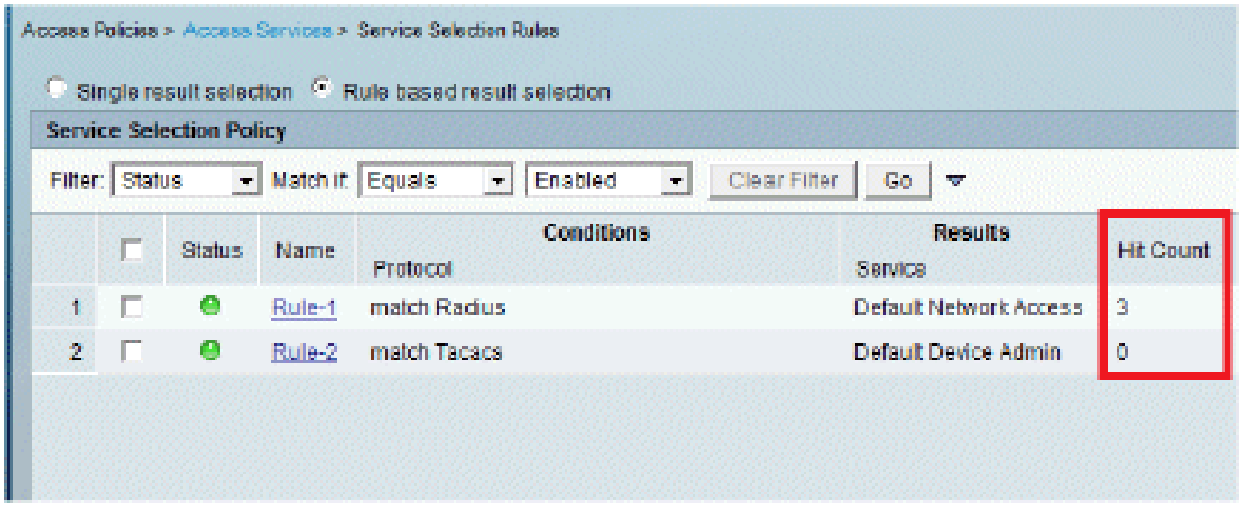
驗證user2(EAP-FAST)

在WLC GUI中，前往Monitor > Clients，然後選擇MAC位址。

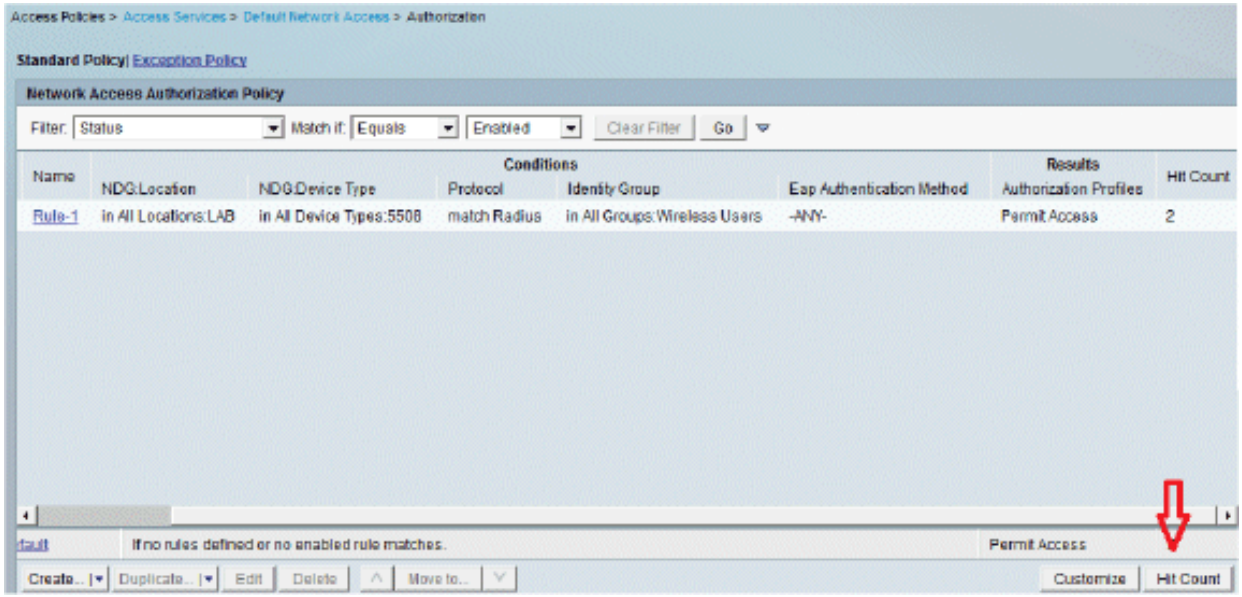
ACS日誌：

1. 完成以下步驟即可檢視命中次數：

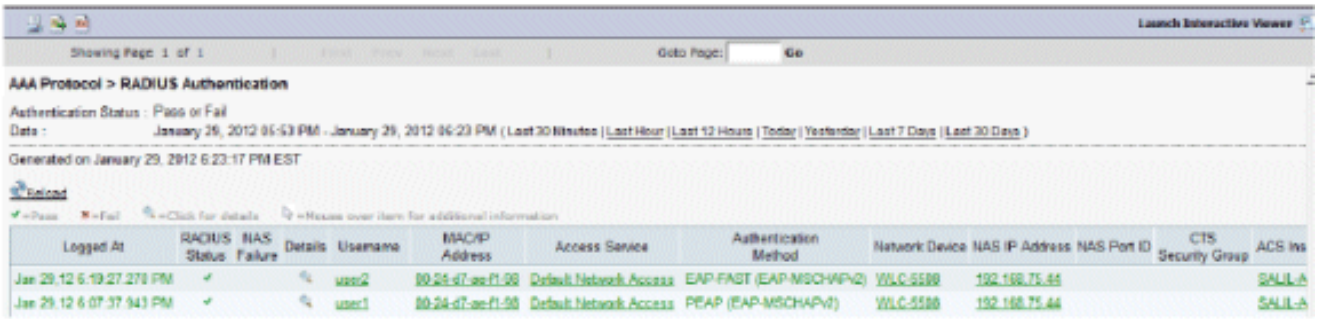
a. 如果您在身份驗證的15分鐘內檢查日誌，請確保刷新HIT計數。



b. 同一頁底部有一個Hit Count頁籤。



2. 按一下Monitoring and Reports，此時會顯示New彈出視窗。轉到Authentications -Radius - Today。您還可以按一下Details以驗證應用了哪個服務選擇規則。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

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

1. 如果您遇到任何問題，請在WLC上發出以下命令：
    - debug client <mac add of the client>
    - debug aaa all enable
    - show client detail <mac addr> — 驗證策略管理器狀態。
    - show radius auth statistics — 驗證失敗原因。
    - debug disable-all — 關閉調試。
    - clear stats radius auth all - Clear radius statistics on the WLC。
2. 驗證ACS中的日誌並記錄故障原因。

相關資訊

- 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）。