

# 使用WLAN控制器(WLC)設定EAP驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[設定WLC的基本運作並向控制器註冊輕量AP](#)

[設定WLC以透過外部RADIUS伺服器進行RADIUS驗證](#)

[配置WLAN引數](#)

[將Cisco Secure ACS配置為外部RADIUS伺服器並為身份驗證客戶端建立使用者資料庫](#)

[配置客戶端](#)

[驗證](#)

[疑難排解](#)

[疑難排解提示](#)

[操作EAP計時器](#)

[正在從ACS RADIUS伺服器提取程式包檔案以排除故障](#)

[相關資訊](#)

## 簡介

本檔案將說明如何使用外部RADIUS伺服器設定無線LAN控制器(WLC)以進行可擴充驗證通訊協定(EAP)驗證。此組態範例使用思科安全存取控制伺服器(ACS)作為外部RADIUS伺服器，以驗證使用者認證。

## 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(AP)和思科WLC組態的基本知識。
- 輕量AP協定(LWAPP)基礎知識。
- 瞭解如何配置外部RADIUS伺服器 ( 如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：

- Cisco Aironet 1232AG系列輕量AP
- 執行韌體5.1的Cisco 4400系列WLC
- 執行4.1版的Cisco Secure ACS
- Cisco Aironet 802.11 a/b/g使用者端配接器
- 運行韌體4.2的Cisco Aironet案頭實用程式(ADU)

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](#)。

## 設定

本節提供用於設定本文件中所述功能的資訊。

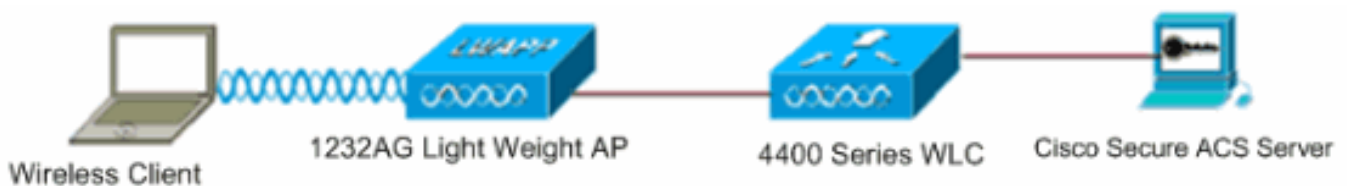
**註：**使用[Command Lookup Tool](#)(僅限[註冊](#)客戶)可以查詢有關本文檔中使用的命令的詳細資訊。

完成以下步驟，配置裝置以進行EAP身份驗證：

1. [設定WLC以達成基本操作，並向控制器註冊輕量AP。](#)
2. [設定WLC以透過外部RADIUS伺服器進行RADIUS驗證。](#)
3. [配置WLAN引數。](#)
4. [將Cisco Secure ACS配置為外部RADIUS伺服器，並建立用於驗證客戶端的使用者資料庫。](#)

## 網路圖表

在此設定中，Cisco 4400 WLC和輕量AP通過集線器連線。外部RADIUS伺服器(Cisco Secure ACS)也連線到同一個集線器。所有裝置都在同一個子網中。AP最初註冊到控制器。您必須將WLC和AP配置為使用輕型可擴展身份驗證協定(LEAP)身份驗證。連線到AP的客戶端使用LEAP身份驗證與AP關聯。Cisco Secure ACS用於執行RADIUS身份驗證。



## 設定WLC的基本運作並向控制器註冊輕量AP

使用命令列介面(CLI)上的啟動配置嚮導，配置WLC的基本操作。或者，您也可使用GUI設定WLC。本檔案將透過CLI上的啟動組態嚮導說明WLC上的組態。

WLC首次啟動後，直接進入啟動配置嚮導。使用配置嚮導配置基本設定。您可以在CLI或GUI上運行該嚮導。此輸出顯示了CLI上啟動配置嚮導的示例：

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
```

```
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
```

Configuration saved!

Resetting system with new configuration..

這些引數設定WLC的基本操作。在此組態範例中，WLC使用**10.77.244.204**作為管理介面IP位址，**10.77.244.205**作為AP管理員介面IP位址。

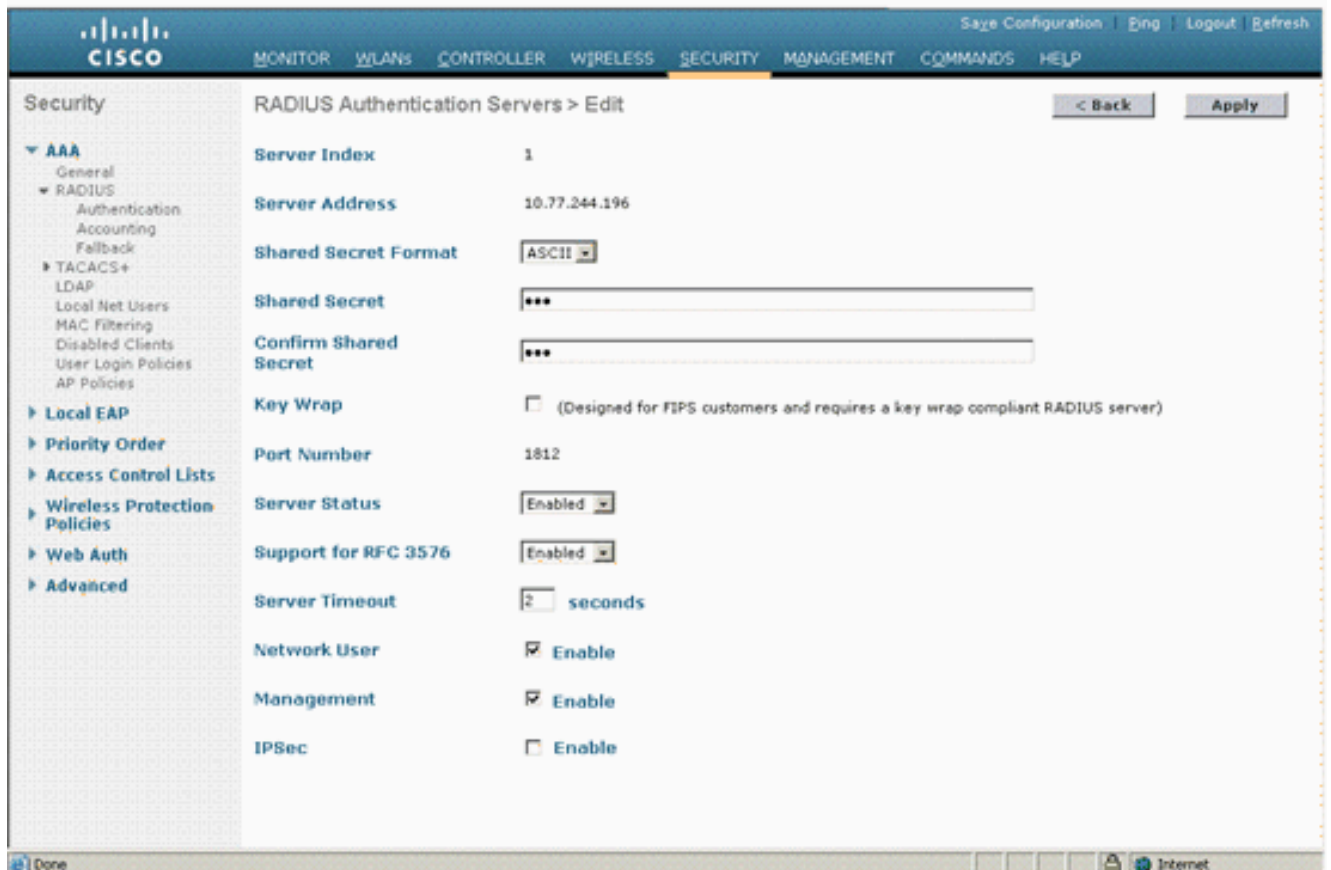
在WLC上設定任何其他功能之前，輕量AP必須向WLC註冊。本檔案假設輕量AP已註冊到WLC。請參閱[輕量AP\(LAP\)註冊到無線LAN控制器\(WLC\)](#)，以瞭解更多有關輕量AP如何註冊到WLC的資訊。

## [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伺服器接著驗證使用者認證並提供對無線使用者端的存取許可權。

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。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。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於WLC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。
3. WLC現在可以使用RADIUS伺服器進行驗證。如果您選擇「Security > Radius > Authentication」，可以找到列出的Radius伺服器。



Cisco CNS Access Registrar(CAR)RADIUS伺服器支援RFC 3576，但Cisco Secure ACS Server 4.0版及更低版本不支援。您還可以使用本地RADIUS伺服器功能來驗證使用者身分。本地RADIUS伺服器引入了4.1.171.0版代碼。執行舊版的WLC沒有本地RADIUS功能。本地EAP是一種允許使用者和無線客戶端在本地進行身份驗證的身份驗證方法。它適用於想要在後端系統中斷或外部身份驗證伺服器關閉時保持與無線客戶端連線的遠端辦公室。本地EAP從本地使用者資料庫或LDAP後端資料庫中檢索使用者憑證以驗證使用者。本地EAP支援使用PAC的LEAP、使用PAC的EAP-FAST、使用證書的EAP-FAST，以及在控制器和無線客戶端之間的EAP-TLS身份驗證。本地EAP設計為備用身份驗證系統。如果在控制器上設定了任何

RADIUS伺服器，控制器會先嘗試使用RADIUS伺服器驗證無線使用者端。僅當未找到RADIUS伺服器時嘗試本地EAP，原因可能是RADIUS伺服器超時或未配置RADIUS伺服器。有關如何配置無線LAN控制器上的本地EAP的詳細資訊，請參閱[使用EAP-FAST和LDAP伺服器的無線LAN控制器上的本地EAP身份驗證配置示例](#)。

## 配置WLAN引數

接下來，設定使用者端用來連線無線網路的WLAN。當您為WLC配置基本引數時，也為WLAN配置了SSID。您可以將此SSID用於WLAN或建立新的SSID。在本示例中，您將建立一個新的SSID。

**注意：**您最多可以在控制器上配置十六個WLAN。Cisco WLAN解決方案最多可以控制十六個輕量AP的WLAN。可以為每個WLAN分配唯一的安全策略。輕量AP廣播所有活動的Cisco WLAN解決方案WLAN SSID，並強制實施您為每個WLAN定義的策略。

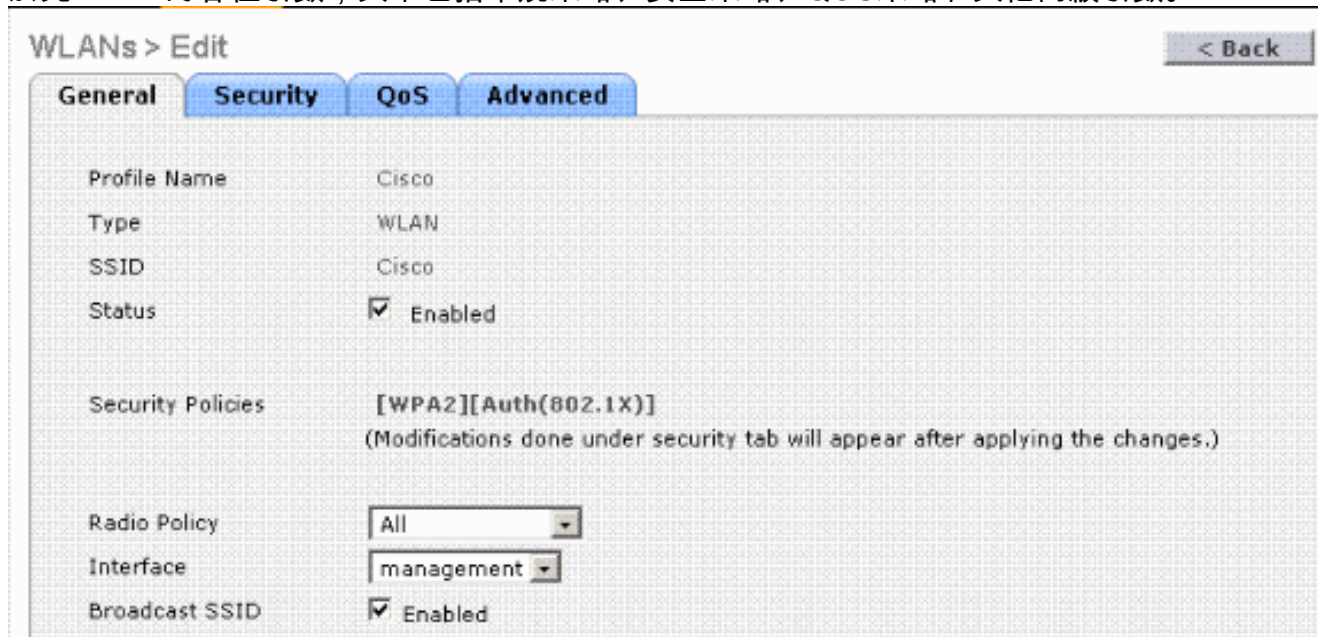
完成以下步驟以設定新的WLAN及其相關引數：

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. 選擇**New**以建立一個新的WLAN。輸入WLAN的Profile name和WLAN SSID，然後點選**Apply**。本示例使用Cisco作為SSID。



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'WLANs' section is active, showing a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > New' and contains three input fields: 'Type' (set to 'WLAN'), 'Profile Name' (set to 'Cisco'), and 'WLAN SSID' (set to 'Cisco').

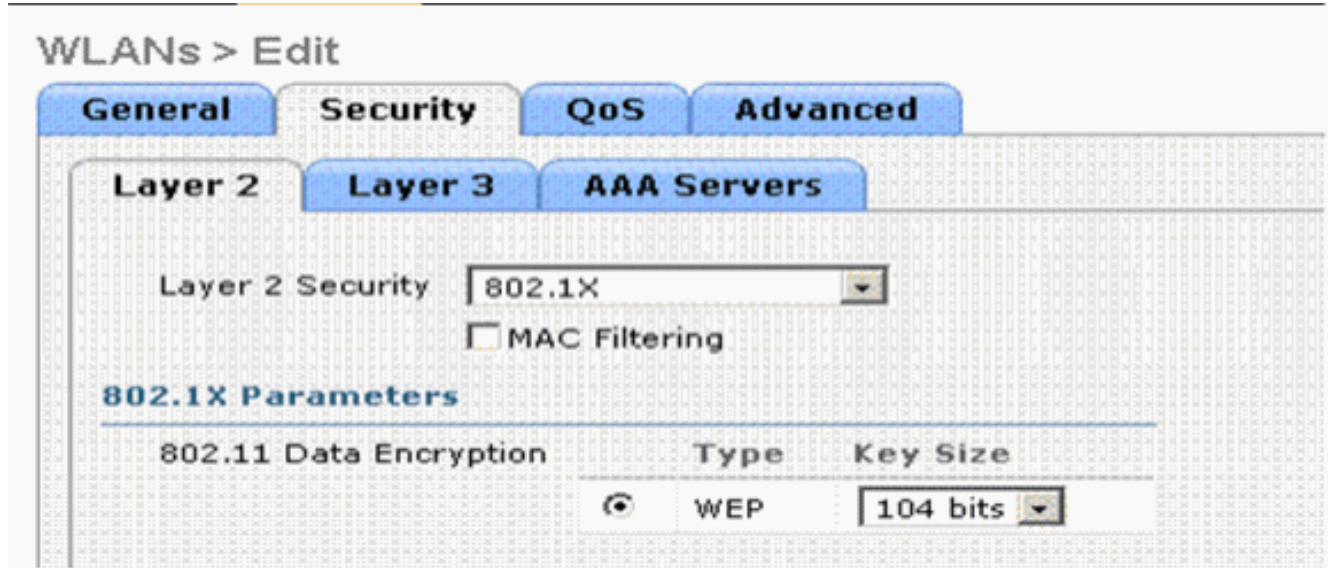
3. 建立新的WLAN後，系統會顯示新WLAN的WLAN > Edit頁面。在此頁面中，您可以定義特定於此WLAN的各種引數，其中包括常規策略、安全策略、QoS策略和其他高級引數。



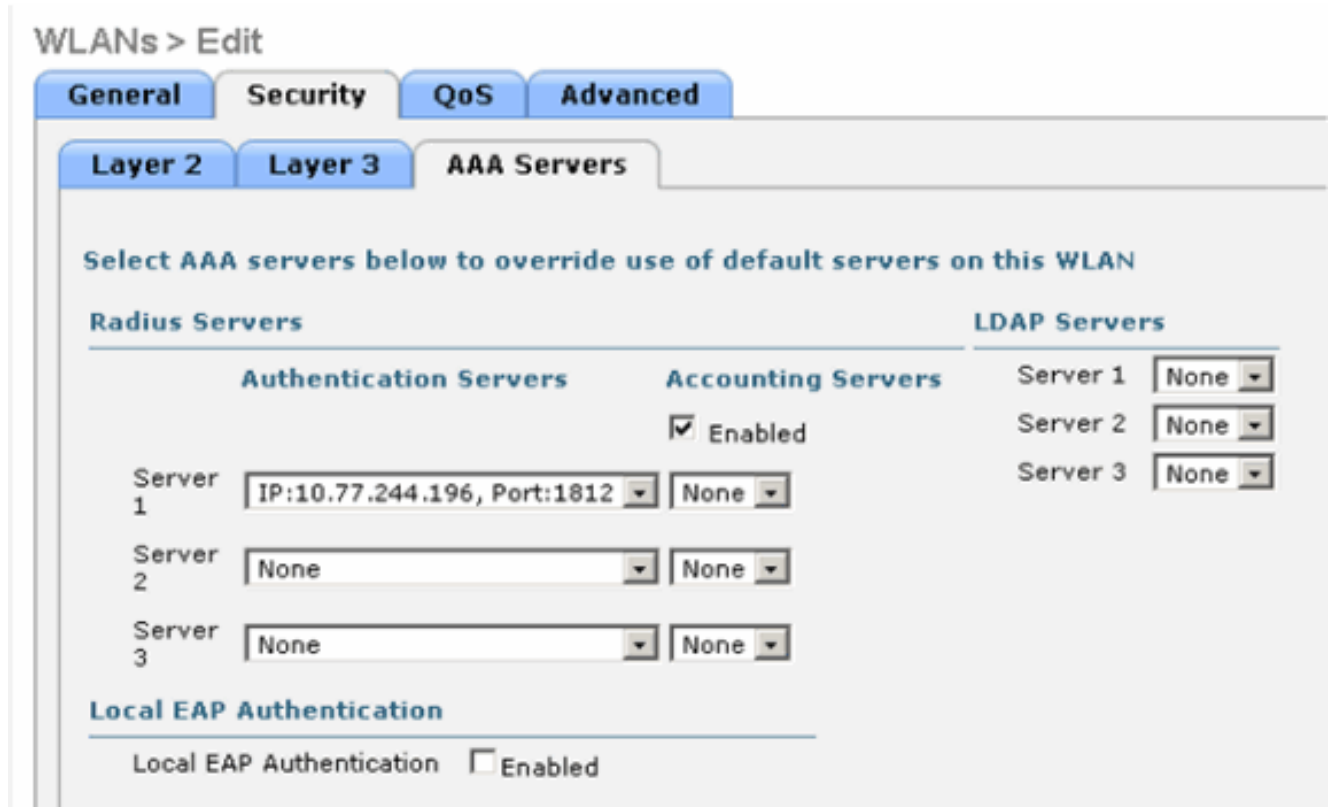
The screenshot shows the Cisco WLAN configuration interface for editing a WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'WLANs' section is active, showing a sidebar with 'WLANs' and 'Advanced' options. The main content area is titled 'WLANs > Edit' and contains a 'Back' button. The 'Security' tab is selected, showing the following configuration: 'Profile Name' (Cisco), 'Type' (WLAN), 'SSID' (Cisco), 'Status' (Enabled), 'Security Policies' ([WPA2][Auth(802.1X)]), 'Radio Policy' (All), 'Interface' (management), and 'Broadcast SSID' (Enabled). A note below the Security Policies field states: '(Modifications done under security tab will appear after applying the changes.)'

從下拉選單中選擇適當的介面。其它引數可以根據WLAN網路的要求進行修改。勾選General Policies底下的**Status**方塊以啟用WLAN。

- 按一下**Security**頁籤，然後選擇**Layer 2 Security**。從Layer 2 Security下拉選單中選擇**802.1x**。在802.1x引數中，選擇WEP金鑰大小。本示例使用128位WEP金鑰，即104位WEP金鑰加上24位初始化向量。



- 選擇**AAA Servers**頁籤。從Authentication Servers(RADIUS)下拉選單中，選擇適當的RADIUS伺服器。此伺服器用於對無線客戶端進行身份驗證。



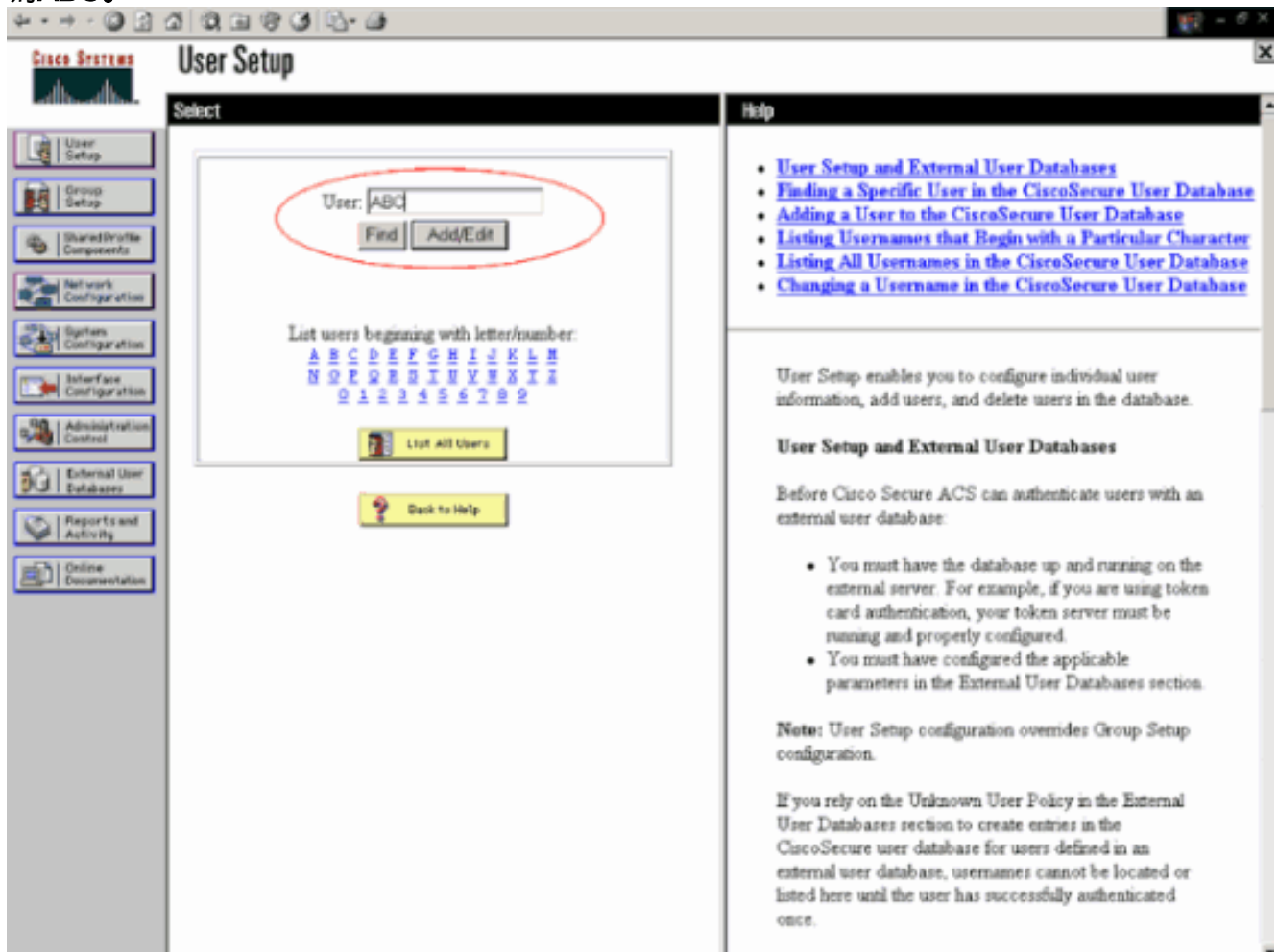
- 按一下**Apply**以儲存組態。

## [將Cisco Secure ACS配置為外部RADIUS伺服器並為身份驗證客戶端建立使用者資料庫](#)

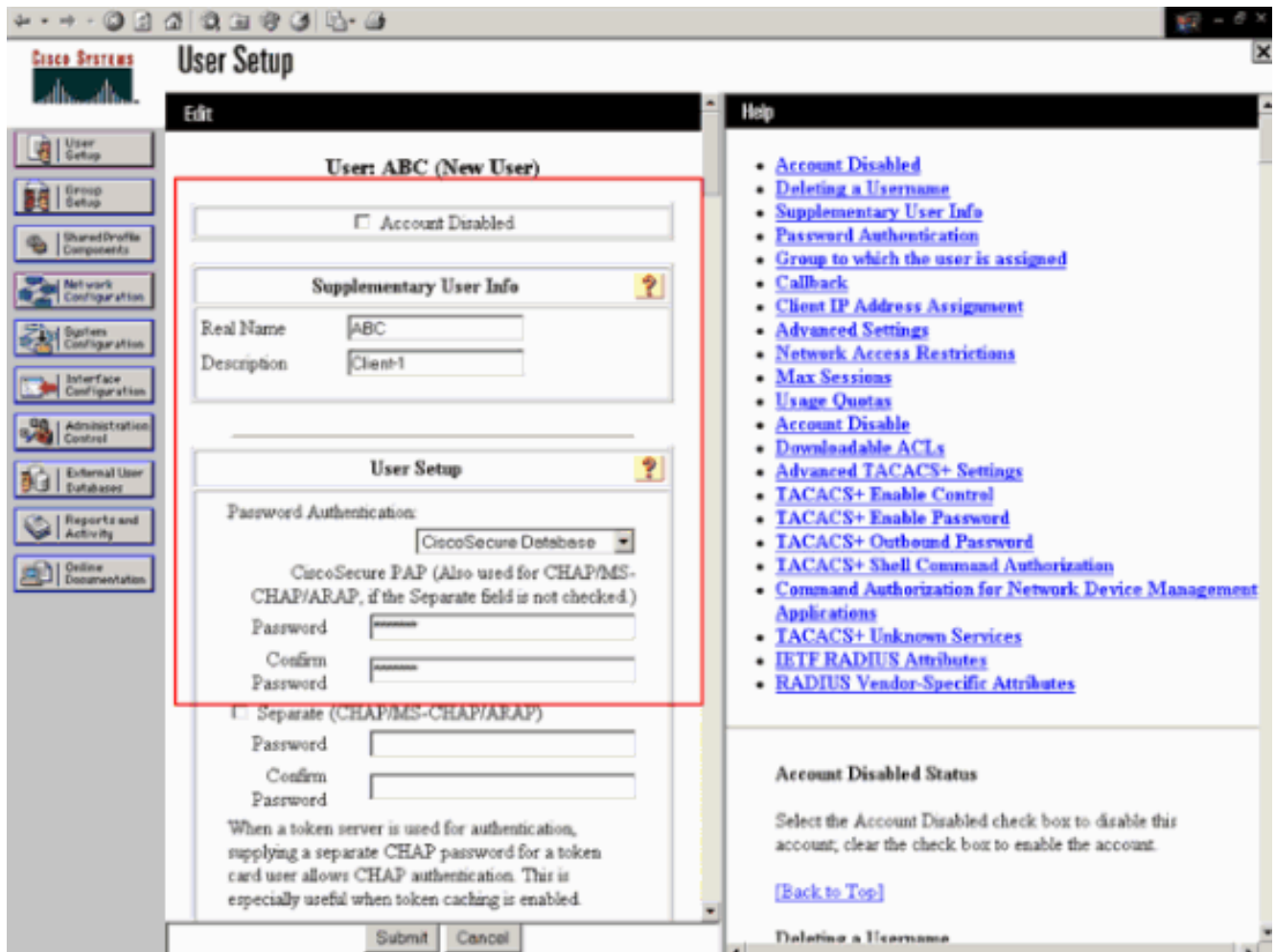
完成以下步驟，在Cisco Secure ACS上建立使用者資料庫並啟用EAP身份驗證：

- 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ABC。



2. 出現「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，由於您僅需要此引數進行EAP身份驗證，因此配置了使用者名稱、密碼和補充使用者資訊。按一下Submit並重複相同的過程，以便向資料庫新增更多使用者。預設情況下，所有使用者都分組在預設組下，並被分配與為該組定義的相同策略。如果要將特定使用者分配給不同的組，請參閱[適用於Windows Server 3.2的Cisco Secure ACS使用手冊](#)的[使用者組管理](#)部分，以獲取詳細資訊。



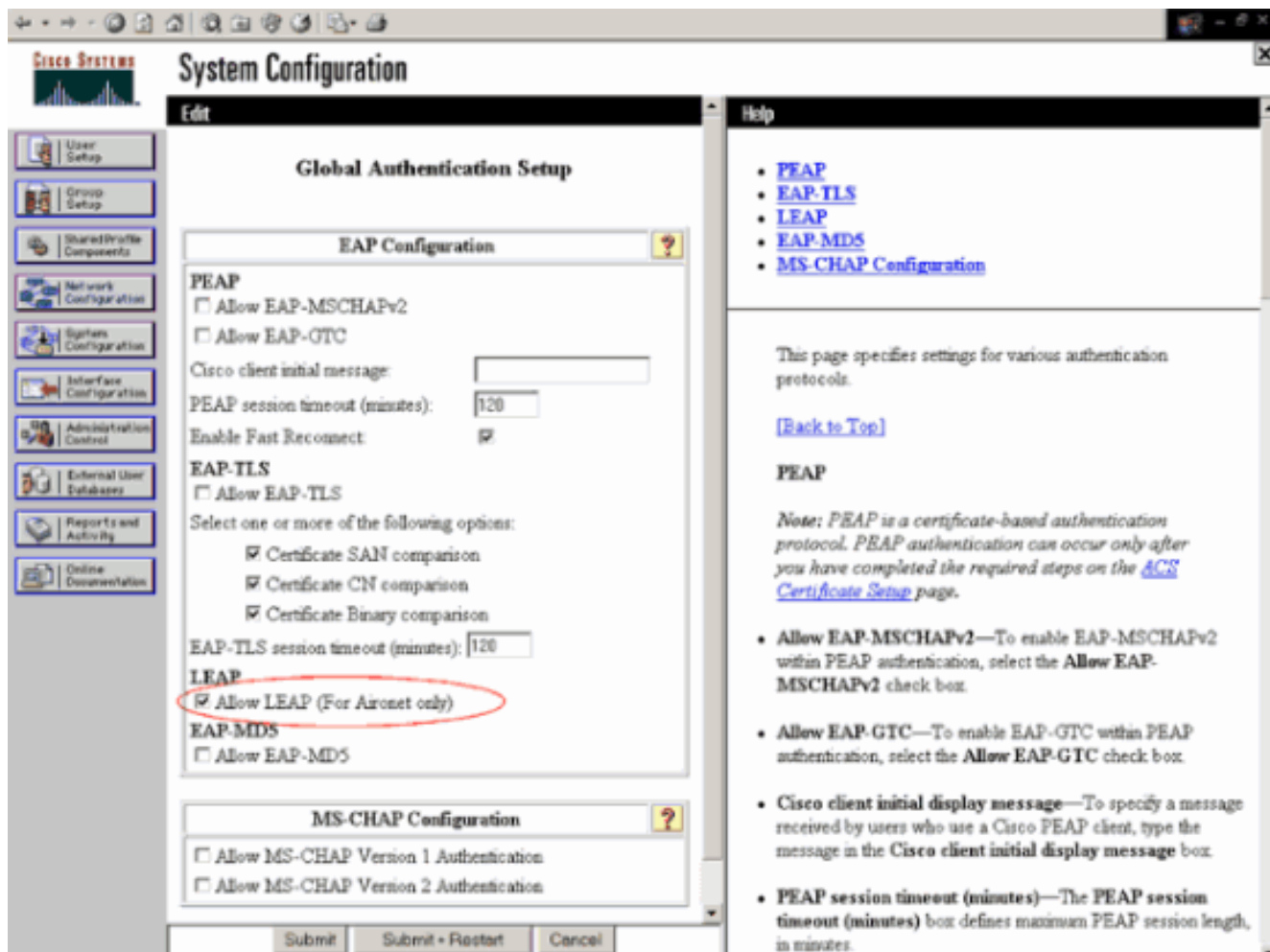
3. 將控制器定義為ACS伺服器上的AAA客戶端。在ACS GUI上按一下**Network Configuration**。顯示「網路組態」頁面時，定義WLC的名稱、IP位址、共用密碼和驗證方法(RADIUS Cisco Airespace)。請參閱製造商提供的文檔，瞭解其它非ACS身份驗證伺服器。注意：您在WLC和ACS伺服器上配置的共用金鑰必須匹配。共用金鑰區分大小寫。



## Add AAA Client

AAA Client Hostname	<input type="text" value="WLC-1"/>
AAA Client IP Address	<input type="text" value="10.77.244.204"/>
Shared Secret	<input type="text" value="cisco"/>
<hr/>	
<b>RADIUS Key Wrap</b>	
Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal
<hr/>	
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	

- 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**。

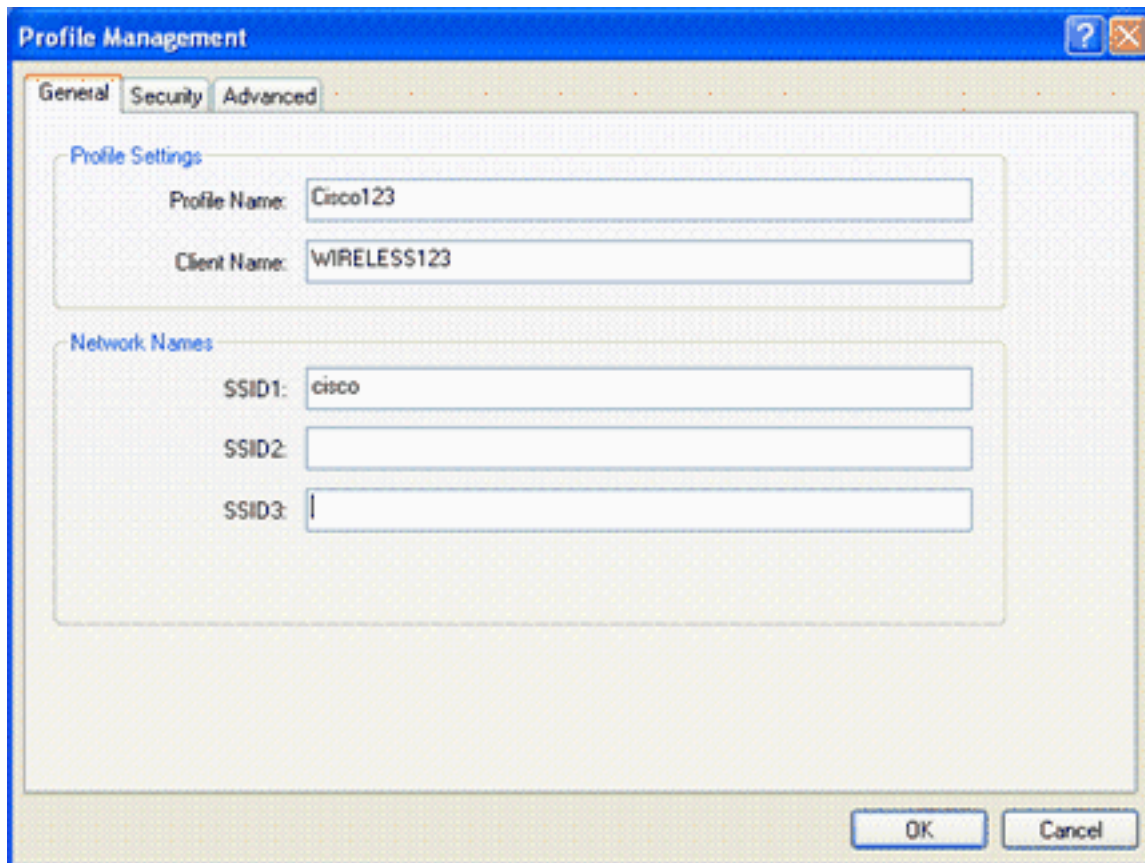


## 配置客戶端

還應為客戶端配置適當的EAP型別。客戶端在EAP協商過程中向伺服器提出EAP型別。如果伺服器支援該EAP型別，則它確認該EAP型別。如果EAP型別不受支援，它將傳送否定確認，並且客戶端再次與不同的EAP方法協商。此過程會一直持續，直到協商支援的EAP型別為止。此示例使用LEAP作為EAP型別。

完成以下步驟，以便使用Aironet案頭實用程式在客戶端上配置LEAP。

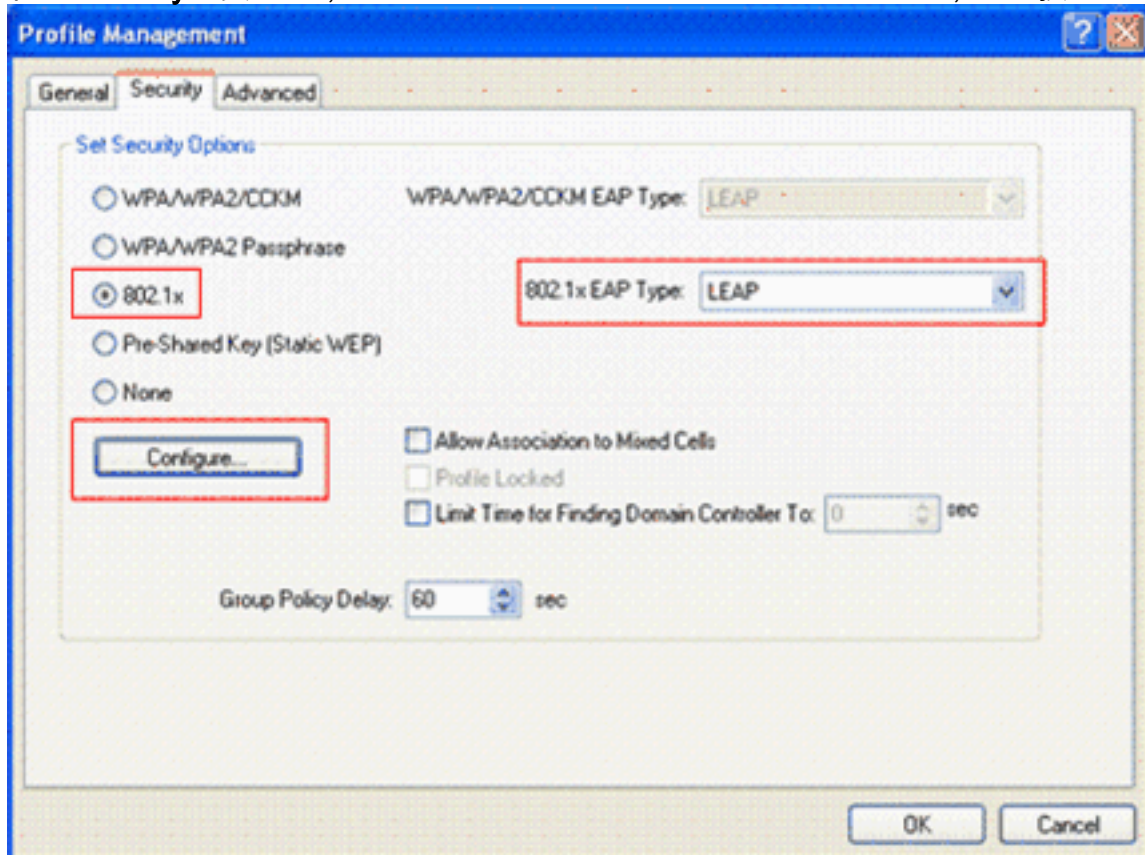
1. 按兩下Aironet Utility圖示將其開啟。
2. 按一下Profile Management頁籤。
3. 按一下配置檔案並選擇Modify。
4. 在「General」頁籤下，選擇Profile Name。輸入WLAN的SSID。



注意

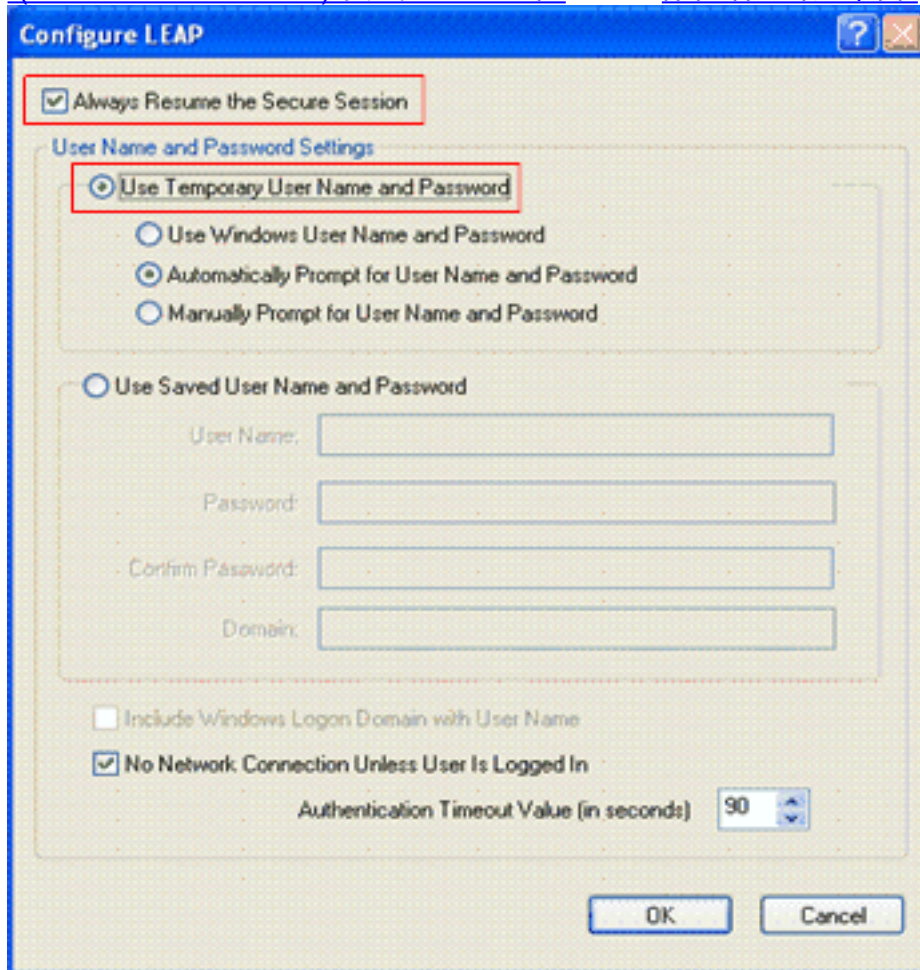
: SSID區分大小寫，並且需要與WLC上配置的SSID完全匹配。

5. 在「Security」頁籤下，選擇「802.1x」。選擇EAP型別作為LEAP，然後按一下Configure。



6. 選擇Use Temporary Username and Password，該選項會在每次電腦重新啟動時提示您輸入使用者證書。檢查此處提供的三個選項之一。此示例使用自動提示輸入使用者名稱和密碼，這要求您在登入到Windows之前輸入LEAP使用者憑據以及Windows使用者名稱和密碼。如果您希望LEAP請求方始終嘗試恢復上一個會話，而不需要在客戶端介面卡漫遊並重新關聯到網路時提示您重新輸入憑證，請選中視窗頂部的Always Resume the Secure Session覈取方塊。註

：有關其它選項的詳細資訊，請參閱[Cisco Aironet 802.11a/b/g無線LAN客戶端介面卡 \(CB21AG和PI21AG\) 安裝及設定指南](#)文檔的[配置客戶端介面卡](#)部分。



7. 在**Advanced**頁籤下，可以配置前導碼、Aironet擴展和其他802.11選項（如電源、頻率等）。
8. 按一下「OK」（確定）。客戶端現在嘗試與配置的引數關聯。

## 驗證

使用本節內容，確認您的組態是否正常運作。

嘗試使用LEAP身份驗證將無線客戶端與輕量AP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。以下是範例：

**Enter Wireless Network Password** [X]

Please enter your LEAP username and password to log on to the wireless network

User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

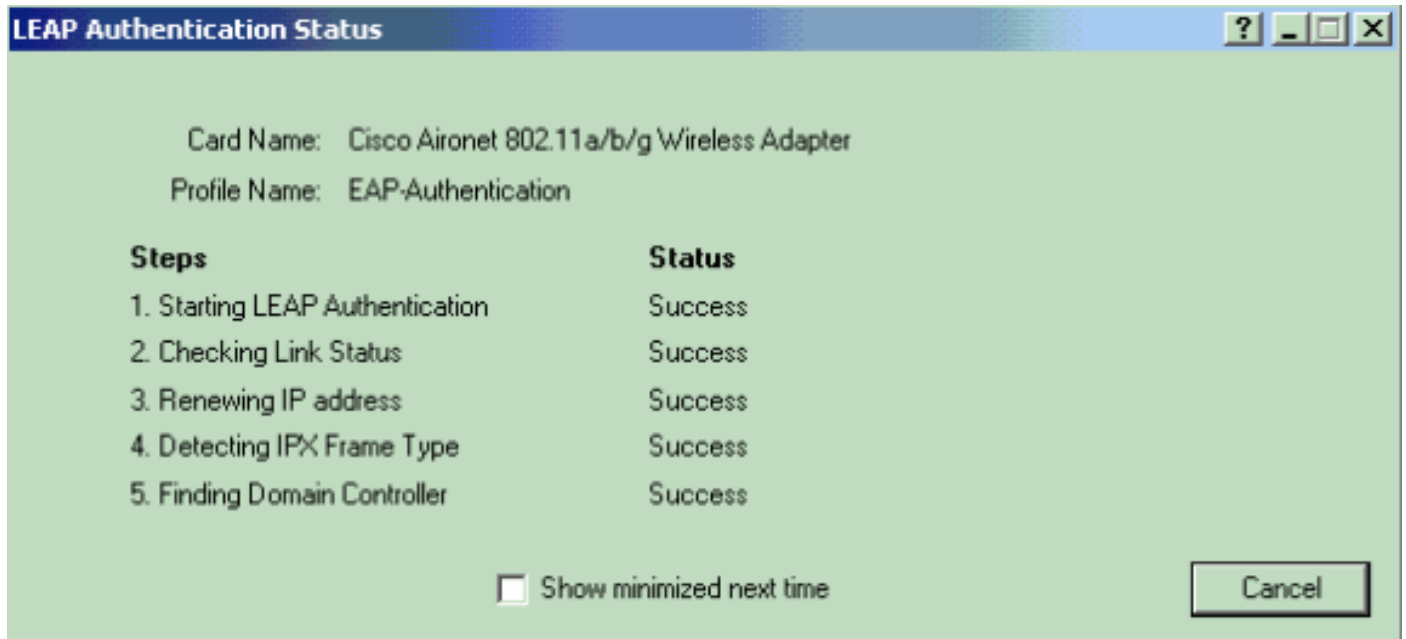
Profile Name : EAP-Authentication

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伺服器會比較資料與使用者資料庫，並在使用者認證有效時提供存取無線使用者端的許可權，以便驗證使用者認證。ACS伺服器上的Passed Authentication報告顯示客戶端已通過RADIUS身份驗證。以下是範例：

The screenshot shows the Cisco Systems Reports and Activity interface. On the left is a navigation menu with categories like User Setup, Group Setup, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Reports and Activity' and contains a list of reports such as TACACS+ Accounting, RADIUS Accounting, and Passed Authentications. The 'Passed Authentications' report is selected, displaying a table of active authentications.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
04/04/2006	15:01:33	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30
04/04/2006	15:00:37	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30

RADIUS驗證成功後，無線客戶端會與輕量AP關聯。



也可在WLC GUI的Monitor索引標籤下檢查此專案。選擇Monitor > Clients，然後檢查客戶端的MAC地址。



## 疑難排解

完成以下步驟以排除配置故障：

1. 使用 `debug lwapp events enable` 命令以檢查AP是否註冊到WLC。
2. 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NAS-IP位址、日期和時間，確認WLC是否能夠連線到Radius伺服器。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。以下是RADIUS伺服器驗證失敗時的範例：  
：

The screenshot shows the Cisco Systems 'Reports and Activity' interface. On the left is a navigation sidebar with icons and labels for various system functions. The main area is divided into a 'Reports' list and a data table. The table, titled 'Failed Attempts active.csv', has columns for Date, Time, Message Type, User Name, Group Name, Caller ID, Authen Failure Code, Authn Failure Code, Authn Data, NAS Port, and NAS IP Address. One row of data is visible, showing a failed authentication attempt on 04/04/2006 at 15:42:51 for user 'cde' from caller ID '00-40-96-AC-E6-57' with an authentication failure code of 'CS user unknown' and a NAS IP address of '172.16.1.30'.

註：有關如何對Cisco Secure ACS進行故障排除和獲取調試資訊的資訊，請參閱[獲取適用於Windows的Cisco Secure ACS的版本和AAA調試資訊](#)。

3. 您還可以使用以下debug命令來排除AAA身份驗證故障：**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。以下是**debug 802.1x aaa enable**命令的輸出示例：

```
(Cisco Controller) >debug dot1x aaa enable
```

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
.....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
```

Response'

\*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-req] Returning AAA response

\*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f  
.....B:...

\*Sep 23 15:15:43.799: 00000010: 41 42 43  
ABC

\*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_USER\_NAME(1) index=0

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_CALLING\_STATION\_ID(31) index=1

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_CALLED\_STATION\_ID(30) index=2

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_PORT(5) index=3

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_IP\_ADDRESS(4) index=4

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_IDENTIFIER(32) index=5

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_VAP\_ID(1) index=6

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_SERVICE\_TYPE(6) index=7

\*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA\_ATT\_FRAMED\_MTU(12) index=8

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_PORT\_TYPE(61) index=9

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA\_ATT\_EAP\_MESSAGE(79) index=10

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA\_ATT\_RAD\_STATE(24) index=11

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA\_ATT\_MESS\_AUTH(80) index=12

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!!

\*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed  
...#. ....[2.e..

\*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13  
..O...5..k..WP..

\*Sep 23 15:15:43.904: 00000020: 41 42 43  
ABC

\*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001)

\*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-req] AAA response 'Interim Response'

\*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-req] Returning AAA response

\*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 **AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05**

\*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.907: 00000000: 03 03 00 04  
....

\*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_USER\_NAME(1) index=0

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_CALLING\_STATION\_ID(31) index=1

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_CALLED\_STATION\_ID(30) index=2

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_PORT(5) index=3

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_IP\_ADDRESS(4) index=4

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_IDENTIFIER(32) index=5

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_VAP\_ID(1) index=6

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_SERVICE\_TYPE(6) index=7

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_FRAMED\_MTU(12) index=8

\*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA\_ATT\_NAS\_PORT\_TYPE(61) index=9



```

*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae
    .....)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
    vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
    vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
    vendorId 0, valueLen 16

```

**注意：**由於空間限制，調試輸出中的某些行已被換行。

4. 監控WLC上的日誌，以檢查RADIUS伺服器是否收到使用者認證。按一下「Monitor」以檢查WLC GUI中的日誌。在左側選單中，按一下**Statistics**，然後按一下選項清單中的**Radius server**。這非常重要，因為在某些情況下，如果WLC上的RADIUS伺服器設定不正確，RADIUS伺服器永遠不會收到使用者認證。如果RADIUS引數設定不正確，以下情況就會在WLC上顯示日誌



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。

## 疑難排解提示

- 在控制器上驗證RADIUS伺服器是否處於active狀態，而不是standby或disabled。
- 使用ping命令以檢查是否可從WLC連線至Radius伺服器。
- 檢查是否已從WLAN(SSID)的下拉選單中選擇RADIUS伺服器。
- 如果使用WPA，則必須安裝用於Windows XP SP2的最新Microsoft WPA修補程式。此外，應將客戶端請求方的驅動程式升級到最新版本。
- 如果執行PEAP，例如使用XP、SP2的證書，其中卡由Microsoft無線-0實用程式管理，則需要從Microsoft獲得KB885453修補程式。如果使用Windows零配置/客戶端請求方，請禁用啟用快速重新連線。如果您選擇Wireless Network Connection Properties > Wireless Networks > Preferred networks，則可以執行此操作。然後選擇SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect。您可以在視窗結尾找到要啟用或禁用的選項。
- 如果您使用的是英特爾2200或2915卡，請參閱英特爾網站上有關其卡的已知問題的宣告：[英特爾® PRO/無線2200BG網絡卡](#)英特爾® PRO/無線2915ABG網絡卡下載最新的英特爾驅動程式以避免任何問題。您可以從<http://downloadcenter.intel.com/>下載英特爾驅動程式
- 如果在WLC中啟用了主動故障切換功能，則WLC過於主動，無法將AAA伺服器標籤為。但是，這不應該完成，因為AAA伺服器可能並不只響應該特定客戶端（如果您執行靜默丟棄）。它可能是對具有有效證書的其他有效客戶端的響應。但是，WLC仍然可以將AAA伺服器標籤為不無法。為了克服此問題，請禁用主動故障切換功能。從控制器GUI發出config radius aggressive-failover disable命令以執行此操作。如果此選項處於禁用狀態，則只有在連續三個客戶端無法從RADIUS伺服器接收響應時，控制器才會故障切換到下一個AAA伺服器。

## 操作EAP計時器

在802.1x驗證期間，使用者可能會看到DOT1X-1-MAX\_EAPOL\_KEY\_RETRANS\_FOR\_MOBILE:xx:xx:xx:xx:xx:xx M1傳錯誤消息。

此錯誤訊息表示在WPA(802.1x)金鑰交涉期間，使用者端沒有及時回應控制器。控制器為金鑰協商期間的響應設定計時器。通常，當您看到此消息時，是由於請求方出現問題。確保運行最新版本的客戶端驅動程式和韌體。在WLC上，您可以操縱幾個EAP計時器以幫助進行客戶端身份驗證。這些EAP計時器包括：

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

在操縱這些值之前，您需要瞭解它們的用途，以及更改它們會對網路產生什麼影響：

- **EAP-Identity-Request超時**：此計時器會影響在EAP身份請求之間等待的時間。預設情況下，此值為一秒（4.1及以下）和30秒（4.2及以上）。出現這種變化的原因是，有些客戶端，例如手持裝置、手機、掃描器等，很難快速響應。筆記型電腦等裝置通常不需要對這些值進行操控。可用值為1到120。那麼，將此屬性設定為值30時會發生什麼情況？當客戶端首次連線時，它向網路傳送EAPOL Start，WLC傳送EAP資料包，請求使用者或電腦的身份。如果WLC沒有收到

身分識別回應，它會在第一個要求的30秒後傳送另一個身分識別要求。在初始連線以及客戶端漫遊時會發生這種情況。增加計時器後會發生什麼？如果一切正常，則沒有影響。但是，如果網路出現問題（包括客戶端問題、AP問題或RF問題），則可能導致網路連線延遲。例如，如果將計時器設定為最大值120秒，則WLC會在兩次身份請求之間等待2分鐘。如果使用者端正在漫遊，而WLC沒有收到回應，則我們至少為此使用者端建立了兩分鐘的中斷時間。此計時器的建議值為5。此時，沒有理由將此計時器設定為最大值。

- **EAP-Identity-Request最大重試次數**：Max Retries值是WLC在從MSCB中移除其專案之前，將身分要求傳送到使用者端的次數。達到最大重試次數後，WLC會向客戶端傳送一個取消身份驗證幀，強制它們重新啟動EAP進程。可用值為1到20。接下來，我們將更詳細地瞭解這一點。Max Retries與Identity Timeout一起使用。如果您的Identity Timeout設定為120，而Max Retries設定為20，則需要2400（或 $120 * 20$ ）多長時間。這意味著需要40分鐘才能刪除客戶端，並重新開始EAP進程。如果將身份超時設定為5，最大重試次數值為12，則需要60次（或 $5 * 12$ ）。與先前的示例不同，客戶端被刪除之前只有一分鐘，並且必須重新開始EAP。最大重試次數建議為12。
- **EAPOL-Key超時**：對於EAPOL-Key Timeout值，預設值為1秒或1000毫秒。這意味著，當AP和客戶端之間交換EAPOL金鑰時，AP將傳送金鑰，並預設等待1秒以等待客戶端響應。等待定義的時間值後，AP將再次重新傳輸金鑰。您可以使用`config advanced eap eapol-key-timeout <time>`命令修改此設定。6.0中的可用值介於200和5000毫秒之間，而6.0之前的代碼允許值介於1和5秒之間。請記住，如果您有一個不響應關鍵嘗試的客戶端，將計時器擴展出去可以給他們多一點時間響應。但是，這也會延長WLC/AP取消驗證使用者端以使整個802.1x程式重新開始所需的時間。
- **EAPOL-Key最大重試次數**：對於EAPOL-Key Max Retries值，預設值為2。這意味著我們將重試對客戶端的原始金鑰嘗試兩次。可以使用`config advanced eap eapol-key-retries <retries>`指令變更此設定。可用值介於0和4次重試之間。使用EAPOL-Key Timeout的預設值（即1秒）和EAPOL-Key Retry的預設值(2)時，如果客戶端不響應初始金鑰嘗試，則過程將如下所示：AP向客戶端傳送金鑰嘗試。它會等待一秒鐘的回覆。如果沒有回覆，則傳送第一個EAPOL-Key Retry。它會等待一秒鐘的回覆。如果沒有回覆，則傳送第二個EAPOL-Key Retry。如果仍然沒有來自客戶端的響應且滿足重試值，則客戶端將取消身份驗證。同樣，與EAPOL-Key Timeout一樣，在某些情況下延長EAPOL-Key重試值也是有益的。但是，將其設定為最大值可能再次有害，因為取消身份驗證消息會延長。

## [正在從ACS RADIUS伺服器提取程式包檔案以排除故障](#)

如果使用ACS作為外部RADIUS伺服器，本節可用於排除配置故障。package.cab是一個Zip檔案，其中包含對ACS進行高效故障排除所需的所有檔案。您可以使用CSSupport.exe實用程式建立package.cab，也可以手動收集檔案。

有關如何從WCS建立和提取包檔案的詳細資訊，請參閱[獲取適用於Windows的Cisco Secure ACS的版本和AAA調試資訊](#)的[建立package.cab檔案](#)部分。

## [相關資訊](#)

- [輕量接入點的WLAN控制器故障切換配置示例](#)
- [無線區域網路控制器 \(WLC\) 軟體升級](#)
- [Cisco無線LAN控制器命令參考](#)
- [技術支援與文件 - Cisco Systems](#)