採用EAP-FAST驗證的Cisco安全服務使用者端

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[設計引數](#)
[資料庫](#)
[加密](#)
[單一登入和電腦憑據](#)
[網路圖表](#)
[設定存取控制伺服器(ACS)](#)
[在ACS中將接入點新增為AAA客戶端(NAS)](#)
[配置ACS以查詢外部資料庫](#)
[在ACS上啟用EAP-FAST支援](#)
[Cisco WLAN控制器](#)
[設定無線LAN控制器](#)
[LAP的基本操作和對控制器的註冊](#)
[通過Cisco Secure ACS的RADIUS身份驗證](#)
[WLAN引數的配置](#)
[驗證操作](#)
[附錄](#)
[適用於EAP-FAST Exchange的監聽器擷取](#)
[在WLAN控制器上偵錯](#)
[相關資訊](#)

簡介

本檔案介紹如何使用無線LAN控制器、Microsoft Windows 2000®軟體和Cisco安全存取控制伺服器(ACS)4.0通過EAP-FAST設定Cisco安全服務使用者端(CSSC)。本文檔介紹EAP-FAST架構，並提供部署和配置示例。CSSC是客戶端軟體元件，它向基礎設施提供使用者憑證通訊，以便驗證使用者對網路的身份並分配適當的訪問許可權。

本文檔中概述的CSSC解決方案具有以下優勢：

- 使用可擴充驗證通訊協定(EAP)取得存取許可權WLAN/LAN之前對每個使用者（或裝置）進行驗證
- 端到端WLAN安全解決方案，包括伺服器、驗證器和客戶端元件
- 用於有線和無線身份驗證的通用解決方案

- 在身份驗證過程中派生的動態每使用者加密金鑰
- 不需要公開金鑰基礎架構(PKI)或憑證（可選擇憑證驗證）
- 訪問策略分配和/或啟用NAC的EAP框架

註：有關安全無線部署的資訊，請參閱思科安全無線藍圖。

802.1x驗證框架已作為802.11i（無線LAN安全）標準的一部分納入其中，以在802.11無線LAN網路中啟用基於第2層的驗證、授權和計費功能。目前，有線和無線網路中都有多個EAP協定可供部署。常見部署的EAP協定包括LEAP、PEAP和EAP-TLS。除了這些協定外，思科還定義並實施了EAP通過安全隧道靈活身份驗證(EAP-FAST)協定，作為基於標準的EAP協定，可用於在有線和無線LAN網路中部署。EAP-FAST協定規範在IETF網站上公開 。

與一些其他EAP協定一樣，EAP-FAST是一種客戶端 — 伺服器安全架構，用於加密TLS隧道中的EAP事務。雖然這與PEAP或EAP-TTLS類似，但區別在於EAP-FAST隧道建立是基於每個使用者唯一的強共用金鑰與PEAP/EAP-TTLS（使用伺服器X.509證書來保護身份驗證會話）的區別。 這些共用金鑰稱為保護訪問憑證(PAC)，可以自動（自動或帶內調配）或手動（手動或帶外調配）分發到客戶端裝置。由於基於共用金鑰的握手比基於PKI基礎設施的握手更有效，因此EAP-FAST是提供受保護身份驗證交換的最快、處理器密集度較低的EAP型別。EAP-FAST還旨在簡化部署，因為它不需要在無線LAN客戶端或RADIUS基礎設施上提供證書，但加入了內建調配機制。

以下是EAP-FAST協定的一些主要功能：

- 使用Windows使用者名稱/密碼的單點登入(SSO)
- 支援執行登入指令碼
- Wi-Fi保護訪問(WPA)支援，無需第三方請求方（僅限Windows 2000和XP）
- 簡單部署，無需PKI基礎設施
- Windows密碼過期（即支援基於伺服器的密碼過期）
- 與思科信任代理整合，通過適當的客戶端軟體實現網路准入控制

必要條件

需求

假設安裝程式瞭解基本的Windows 2003安裝和Cisco WLC安裝，因為本文檔僅介紹便於測試的特定配置。

有關Cisco 4400系列控制器的初始安裝和配置資訊，請參閱快速入門手冊：Cisco 4400系列無線LAN控制器。有關Cisco 2000系列控制器的初始安裝和配置資訊，請參閱快速入門手冊：Cisco 2000系列無線LAN控制器。

開始之前，請安裝帶有最新Service Pack軟體的Microsoft Windows Server 2000。安裝控制器和輕量接入點(LAP)，並確保配置最新的軟體更新。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行4.0.155.5的Cisco 2006或4400系列控制器
- Cisco 1242 LWAPP AP
- 採用Active Directory的Windows 2000

- Cisco Catalyst 3750G交換器
- Windows XP，帶CB21AG介面卡卡和思科安全服務客戶端版本4.05

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設計引數

資料庫

部署WLAN網路並尋求驗證協定時，通常需要使用當前資料庫進行使用者/機器驗證。可以使用的典型資料庫是Windows Active Directory、LDAP或一次性密碼(OTP)資料庫（即RSA或SecureID）。所有這些資料庫都與EAP-FAST協定相容，但是在計畫部署時，必須考慮一些相容性要求。PAC檔案到客戶端的初始部署是通過匿名自動調配、身份驗證調配（通過當前客戶端X.509證書）或手動調配完成的。在本檔案中，考慮了匿名自動調配和手動調配。

自動PAC布建使用已驗證的Diffie-Hellman金鑰協定通訊協定(ADHP)建立安全通道。可以匿名地或通過伺服器驗證機制建立安全隧道。在建立的隧道連線中，MS-CHAPv2用於驗證客戶端，並在身份驗證成功後將PAC檔案分發到客戶端。成功調配PAC後，PAC檔案可用於啟動新的EAP-FAST身份驗證會話，以獲得安全網路訪問。

自動PAC設定與正在使用的資料庫相關，因為自動設定機制依賴MSCHAPv2，所以用於驗證使用者的資料庫必須與此密碼格式相容。如果將EAP-FAST用於不支援MSCHAPv2格式的資料庫（如OTP、Novell或LDAP），則需要使用其他機制（即手動調配或經過身份驗證的調配）來部署使用者PAC檔案。本文檔提供了使用Windows使用者資料庫進行自動預配的示例。

加密

EAP-FAST身份驗證不需要使用特定的WLAN加密型別。要使用的WLAN加密型別取決於客戶端NIC卡功能。建議使用WPA2(AES-CCM)或WPA(TKIP)加密，具體取決於特定部署中的NIC卡功能。請注意，Cisco WLAN解決方案允許WPA2和WPA客戶端裝置在通用SSID上共存。

如果客戶端裝置不支援WPA2或WPA，則可能使用動態WEP金鑰部署802.1X身份驗證，但由於已知存在針對WEP金鑰的漏洞，因此不建議使用此WLAN加密機制。如果需要支援僅WEP客戶端，建議使用會話超時時間間隔，這要求客戶端頻繁地派生新的WEP金鑰。對於典型的WLAN資料速率，建議會話時間間隔為30分鐘。

單一登入和電腦憑據

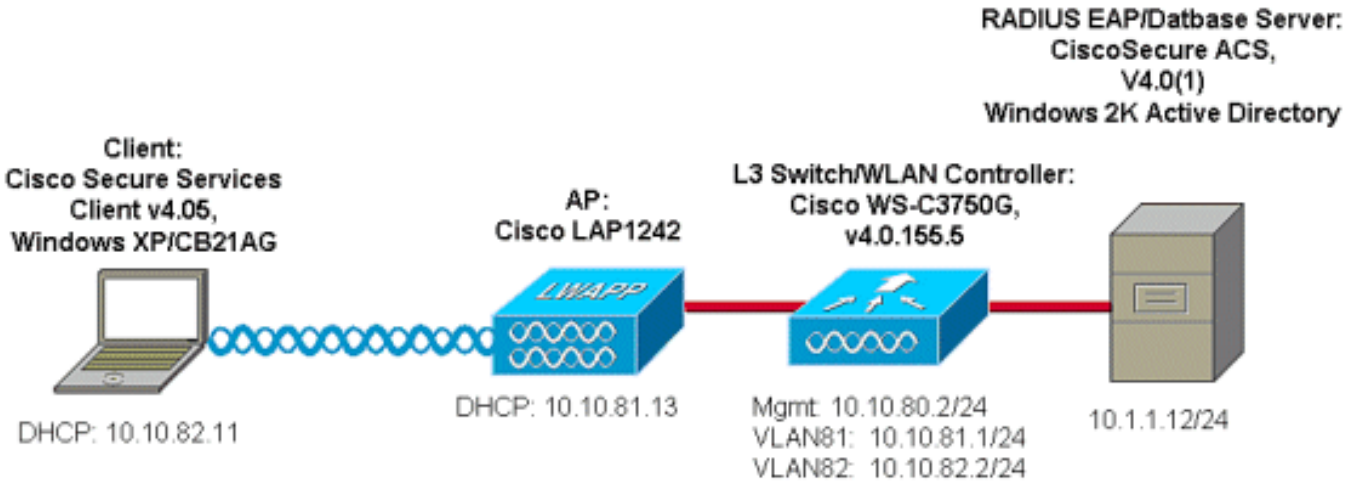
單一登入是指單一使用者登入或輸入用於訪問多個應用程式或多個裝置的身份驗證憑據的能力。對於本文檔而言，單點登入是指使用用於登入PC以驗證WLAN的憑證。

通過Cisco安全服務客戶端，可以使用使用者的登入憑證來向WLAN網路進行身份驗證。如果希望在使用者登入到PC之前對PC進行網路身份驗證，則需要使用儲存的使用者憑據或與電腦配置檔案關聯的憑據。當需要在PC啟動時（而不是使用者登入時）運行登入指令碼或對映驅動器時，這兩種方法都很有用。

網路圖表

這是本文檔中使用的網路圖。在此網路中，使用了四個子網。請注意，沒有必要將這些裝置劃分為不同的網路，但這為與實際網路整合提供了最大的靈活性。Catalyst 3750G整合式無線LAN控制器在通用機箱上提供乙太網路供電(POE)交換器連線埠、L3交換和WLAN控制器功能。

1. 網路10.1.1.0是ACS所在的伺服器網路。
2. 網路10.10.80.0是WLAN控制器使用的管理網路。
3. 網路10.10.81.0是AP所在的網路。
4. 網路10.10.82.0用於WLAN客戶端。



設定存取控制伺服器(ACS)

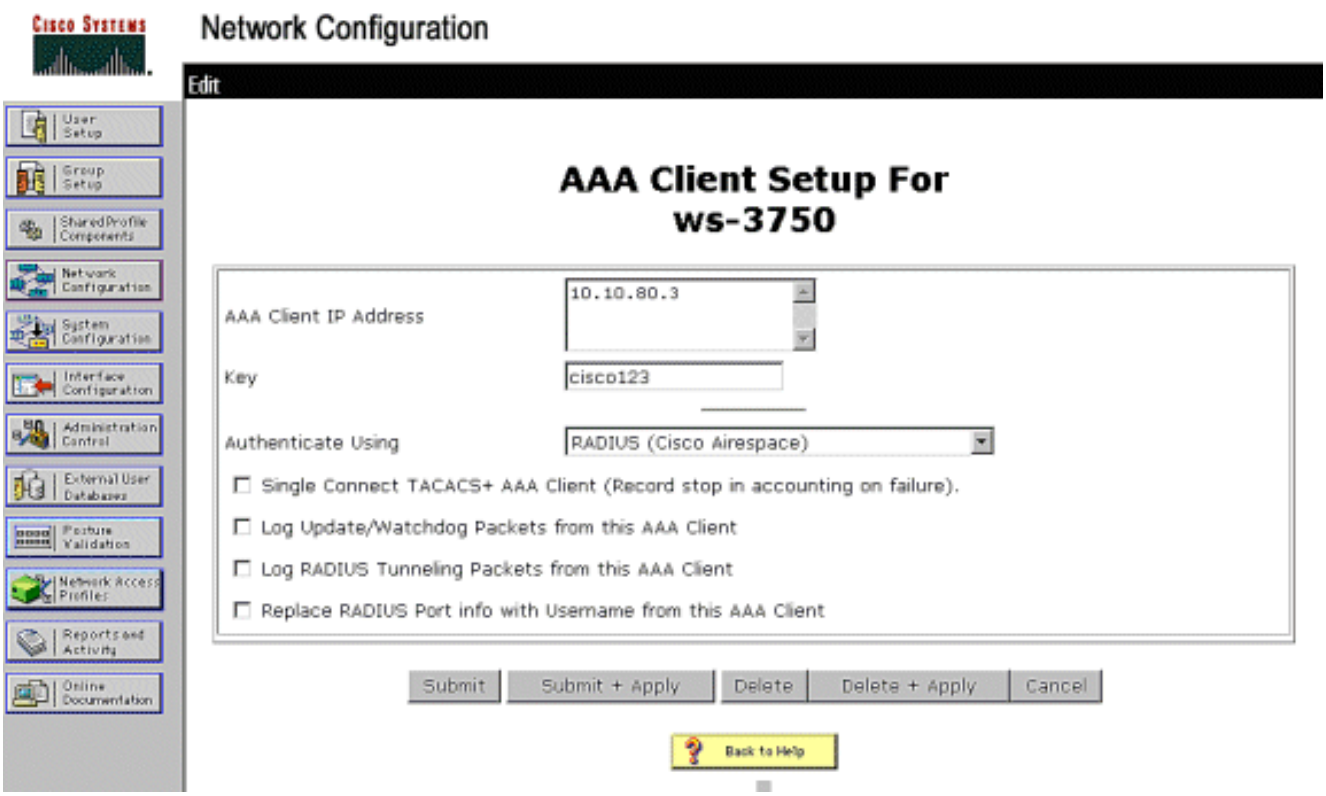
本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

在ACS中將接入點新增為AAA客戶端(NAS)

本節介紹如何配置用於EAP-FAST的ACS，其中帶內PAC調配使用Windows Active Directory作為外部資料庫。

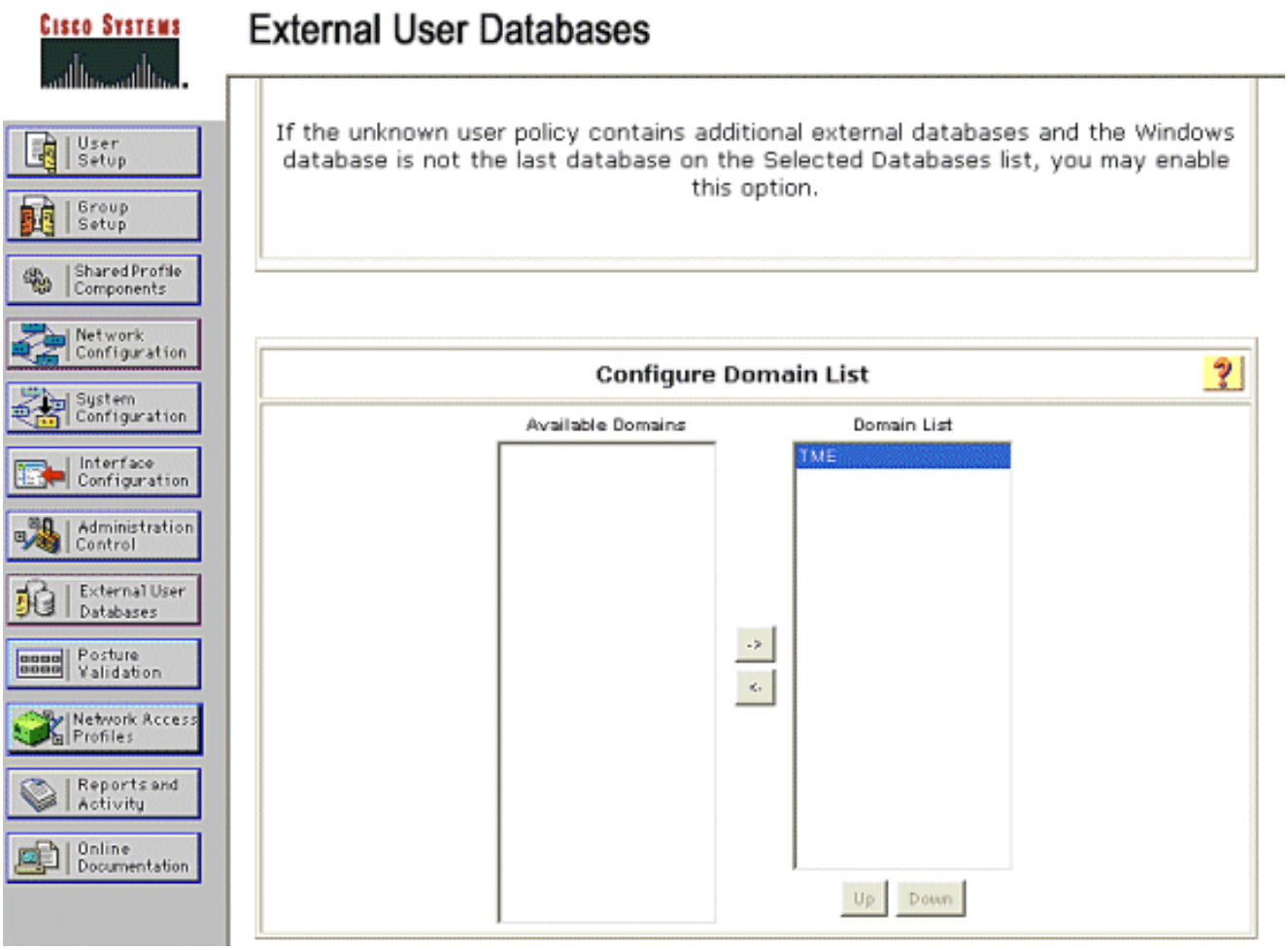
1. 登入到**ACS > Network Configuration**，然後按一下**Add Entry**。
2. 填寫WLAN Controller name、IP address、shared secret key，然後在Authenticate Using下選擇RADIUS(Cisco Airespace)，其中還包括RADIUS IETF屬性。**附註：** 如果啟用了網路裝置組(NDG)，請首先選擇適當的NDG並將WLAN控制器新增到其中。有關NDG的詳細資訊，請參閱ACS配置指南。
3. 按一下**Submit+ Restart**。



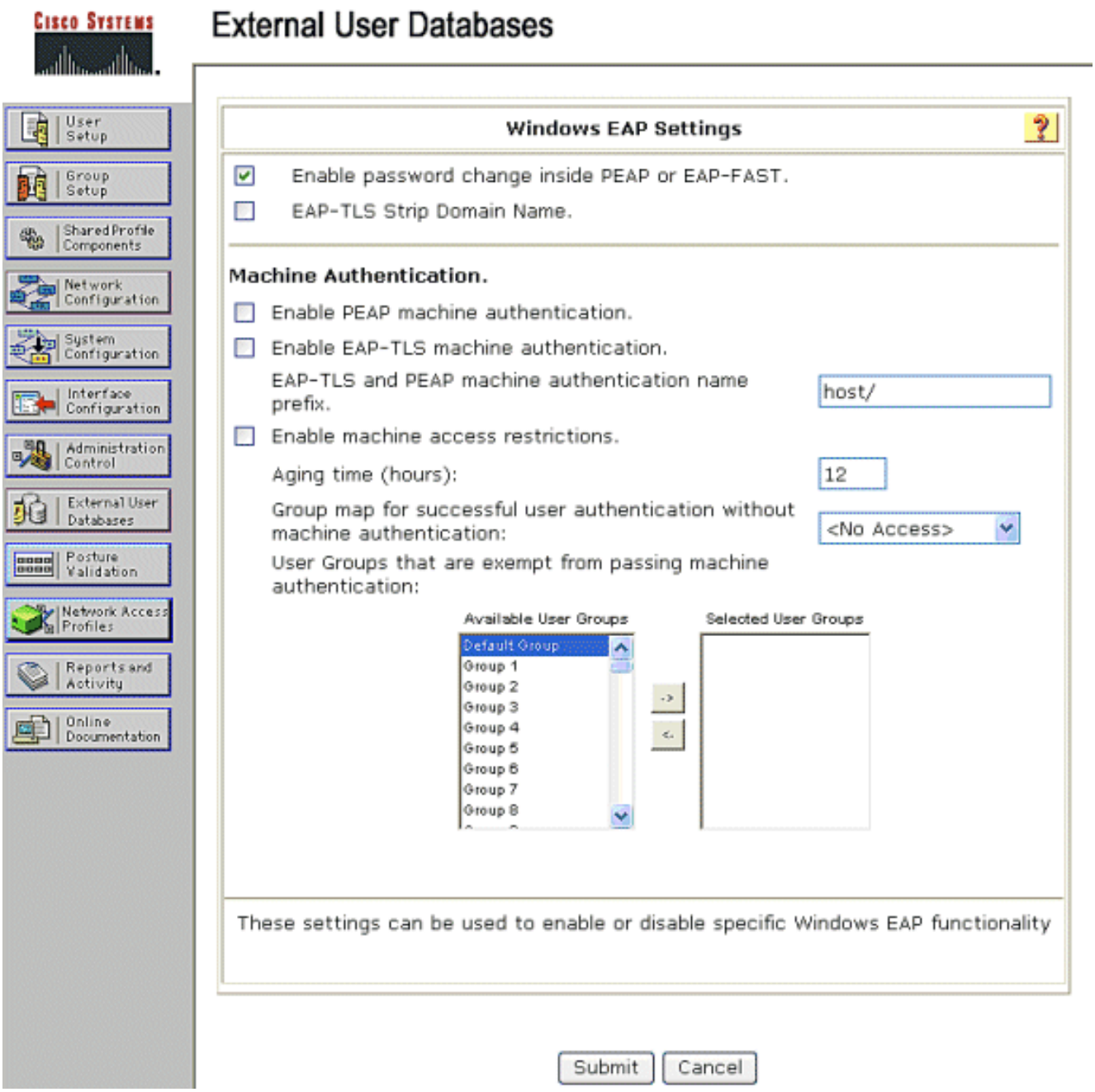
配置ACS以查詢外部資料庫

本節介紹如何配置ACS以查詢外部資料庫。

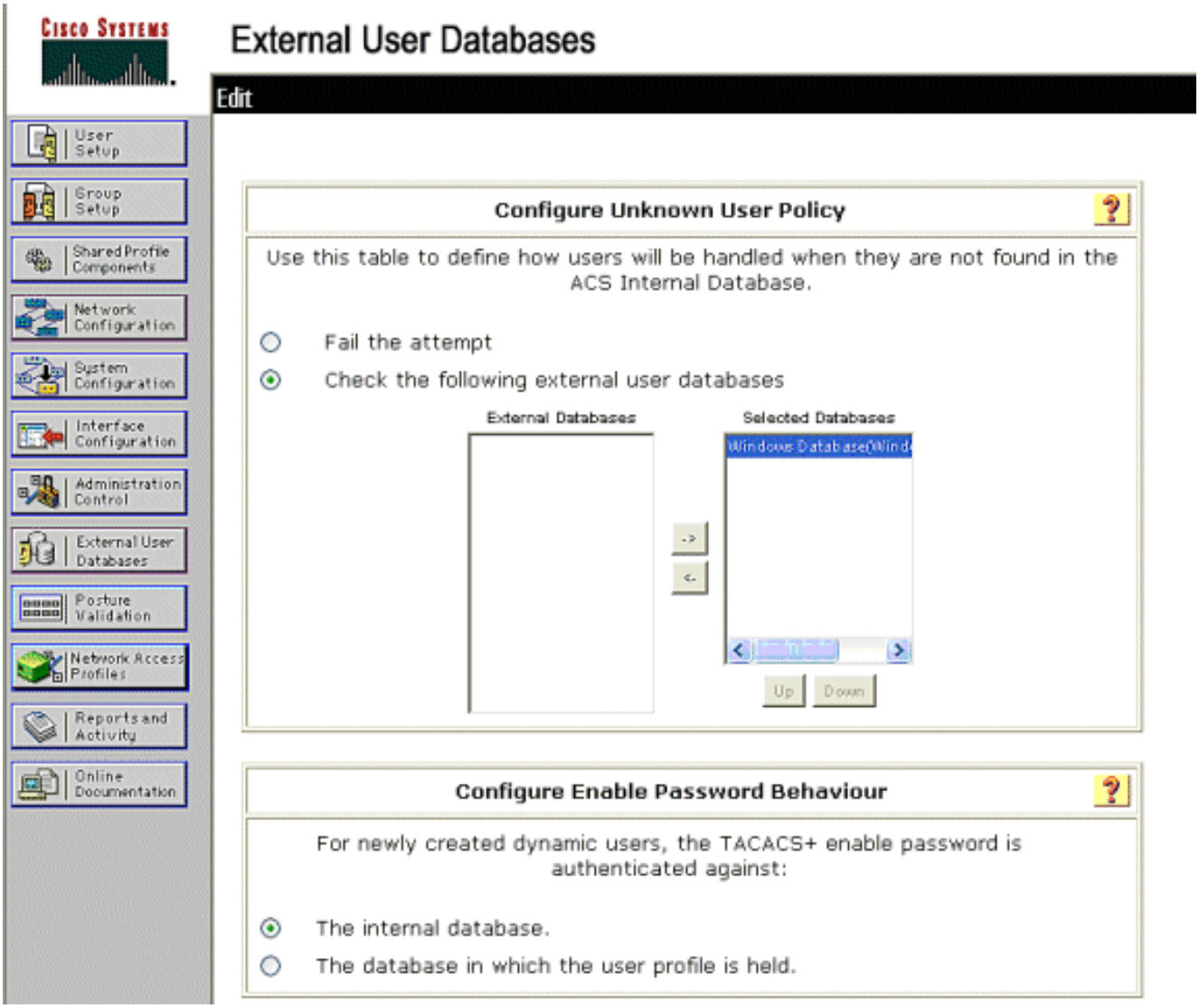
1. 按一下**External User Database > Database Configuration > Windows Database > Configure**。
2. 在Configure Domain List下，將**Domains**從Available Domains移動到Domain List。**注意：**運行ACS的伺服器必須瞭解這些域，以便ACS應用程式檢測這些域並將其用於身份驗證目的。



3. 在Windows EAP設定下，配置選項以允許在PEAP或EAP-FAST會話內更改密碼。請參閱 Cisco Secure ACS 4.1配置指南，以獲取有關EAP-FAST和Windows密碼老化的詳細資訊。
4. 按一下「**Submit**」。**注意**：您還可以在Windows使用者資料庫配置下為EAP-FAST啟用撥入許可權功能，以便允許Windows外部資料庫控制訪問許可權。在Windows資料庫配置頁面上更改密碼的MS-CHAP設定僅適用於非EAP MS-CHAP身份驗證。為了與EAP-FAST一起啟用密碼更改，必須在Windows EAP設定下啟用密碼更改。



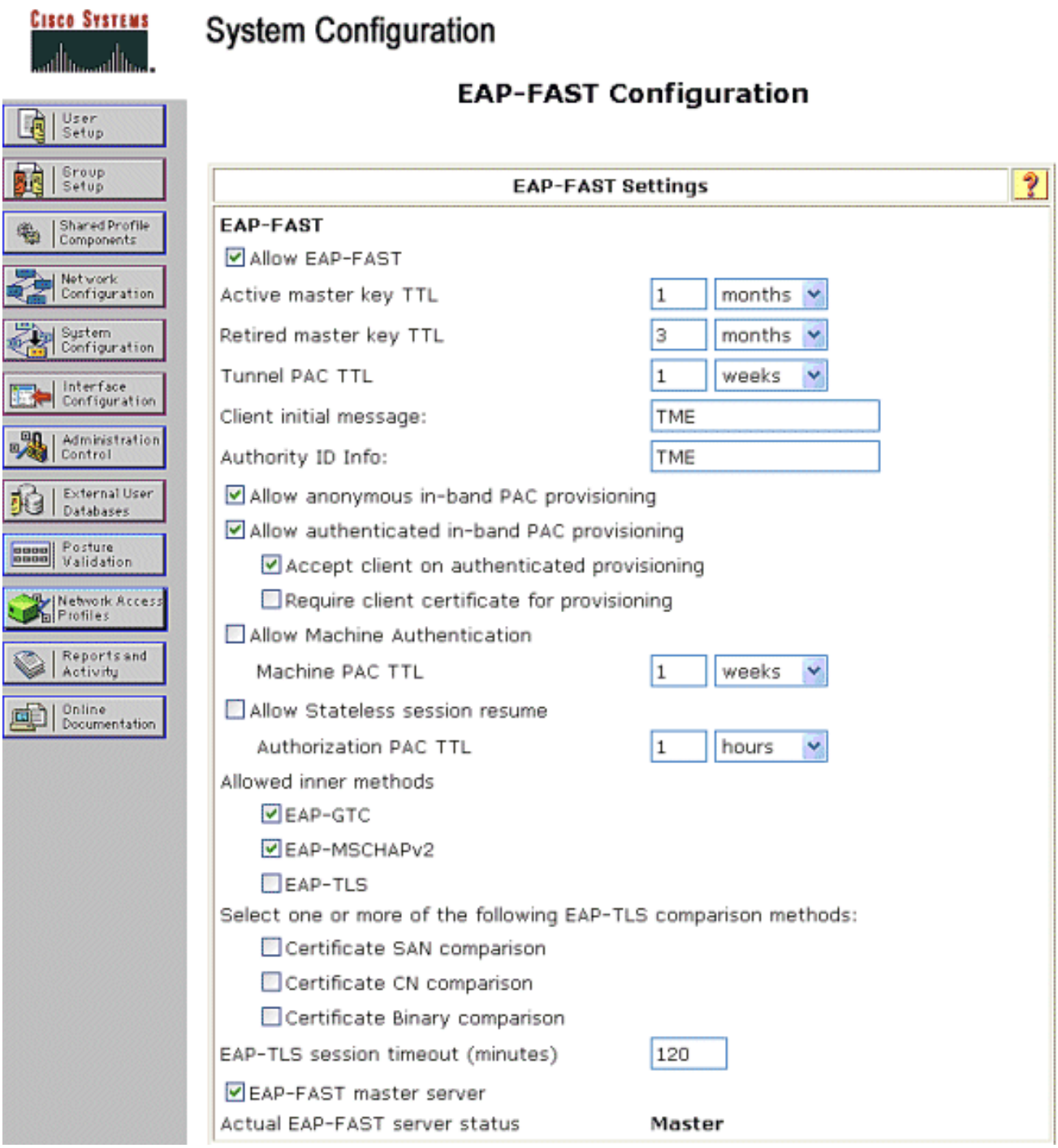
5. 按一下**External User Database > Unknown User Policy**，然後選擇**Check the following external user databases**單選按鈕。
6. 將Windows資料庫從外部數**據庫移**動到**所選資料庫**。
7. 按一下「**Submit**」。**注意**：從此時開始，ACS將檢查Windows資料庫。如果在ACS本地資料庫中找不到該使用者，則會將該使用者置於ACS預設組中。有關資料庫組對映的詳細資訊，請參閱ACS文檔。**注意**：當ACS查詢Microsoft Active Directory資料庫以驗證使用者憑據時，需要在Windows上配置其他訪問許可權設定。有關詳細資訊，請參閱Cisco Secure ACS for Windows Server安裝指南。



在ACS上啟用EAP-FAST支援

本節介紹如何在ACS上啟用EAP-FAST支援。

1. 轉至**System Configuration > Global Authentication Setup > EAP-FAST Configuration**。
2. 選擇**Allow EAP-FAST**。
3. 配置以下建議：主金鑰TTL/已停用主金鑰TTL/PAC TTL。預設情況下，這些設定在Cisco Secure ACS中配置：主金鑰TTL:1個月已停用的金鑰TTL:3個月PAC TTL:1週
4. 填寫授權**ID資訊**欄位。此文本顯示在某些EAP-FAST客戶端軟體上，其中控制器是PAC授權機構的選擇。**注意：**思科安全服務客戶端不會對PAC授權使用此描述性文本。
5. 選擇**Allow in-band PAC provisioning**欄位。此欄位為正確啟用的EAP-FAST客戶端啟用自動PAC調配。在此範例中，使用自動布建。
6. 選擇**Allowed inner methods**:EAP-GTC和EAP-MSCHAP2。這允許EAP-FAST v1和EAP-FAST v1a客戶端的操作。（思科安全服務客戶端支援EAP-FAST v1a。）如果不需要支援EAP-FAST v1客戶端，則只需啟用EAP-MSCHAPv2作為內部方法。
7. 選中**EAP-FAST Master Server**覈取方塊以啟用此EAP-FAST伺服器作為主機。這允許其他ACS伺服器使用此伺服器作為主PAC授權，以避免為網路中的每個ACS提供唯一金鑰。有關詳細資訊，請參閱ACS配置指南。
8. 按一下**Submit+Restart**。



Cisco WLAN控制器

在本部署指南中，Cisco WS3750G整合無線LAN控制器(WLC)與Cisco AP1240輕量AP(LAP)配合使用，為CSSC測試提供WLAN基礎設施。此組態適用於任何Cisco WLAN控制器。採用的軟體版本為4.0.155.5。

設定無線LAN控制器

LAP的基本操作和對控制器的註冊

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，進入啟動配置嚮導。使用配置嚮導配置基本設定。您可通過CLI或GUI訪問該嚮導

。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]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
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。在此範例組態中，WLC使用**10.10.80.3**作為管理介面IP位址，**10.10.80.4**作為AP管理員介面IP位址。

在WLC上配置任何其他功能之前，LAP必須向WLC註冊。本檔案假設LAP已註冊到WLC。有關如何輕量AP向WLC註冊的資訊，請參閱適用於輕量接入點的WLAN控制器故障轉移配置示例的將輕量AP註冊到WLC部分。要參考此配置示例，AP1240部署在WLAN控制器(10.10.80.0/24)之外的子網(10.10.81.0/24)上，並且DHCP選項43用於提供控制器發現。

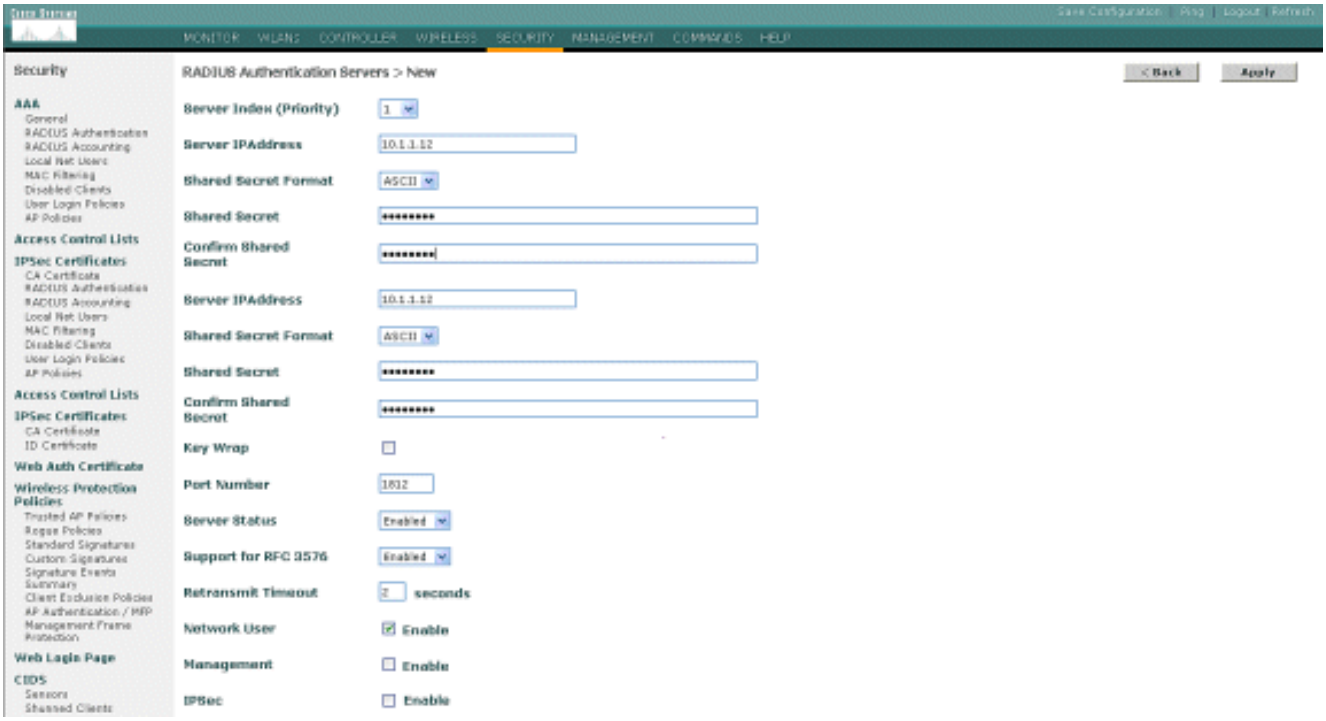
通過Cisco Secure ACS的RADIUS身份驗證

需要配置WLC以將使用者憑證轉發到Cisco Secure ACS伺服器。然後，ACS伺服器驗證使用者憑證（通過配置的Windows資料庫）並提供對無線客戶端的訪問。

完成以下步驟，配置WLC以與ACS伺服器通訊：

1. 從控制器GUI上按一下「**Security**」和「**RADIUS Authentication**」，以顯示「RADIUS Authentication Servers」頁面。然後按一下**New**定義ACS伺服器。

2. 在RADIUS Authentication Servers > New頁中定義ACS伺服器引數。這些引數包括ACS IP地址、共用金鑰、埠號和伺服器狀態。**注意**：埠號1645或1812與ACS相容，以進行RADIUS身份驗證。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於網路使用者（例如WLAN客戶端）和管理（即管理使用者）。 示例配置使用Cisco Secure ACS作為IP地址為10.1.1.12的RADIUS伺服器
：



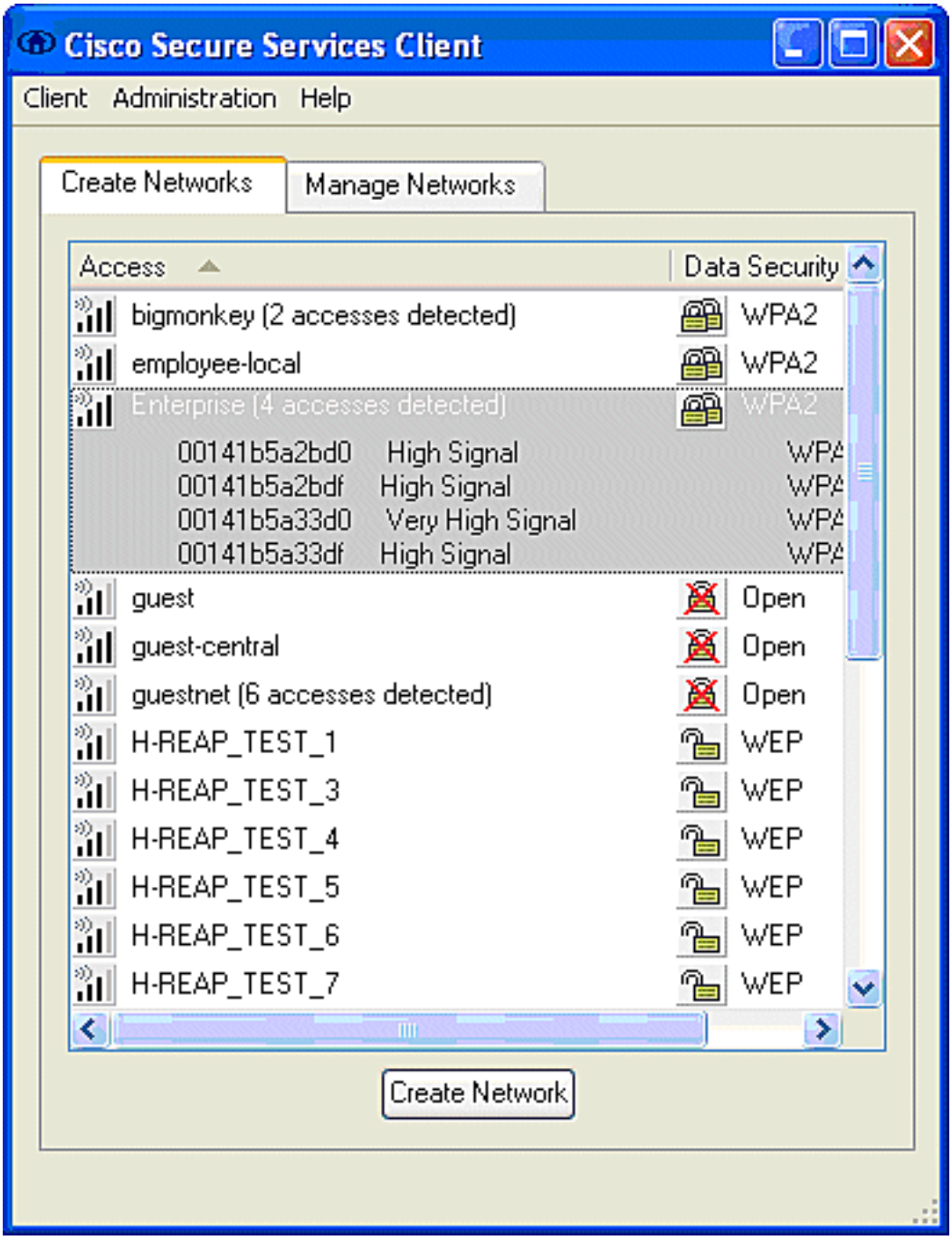
WLAN引數的配置

本節介紹思科安全服務客戶端的配置。在本示例中，CSSC v4.0.5.4783與Cisco CB21AG客戶端介面卡一起使用。在安裝CSSC軟體之前，請確認僅安裝了CB21AG的驅動程式，而不是Aironet案頭實用程式(ADU)。

安裝軟體並將其作為服務運行後，它會掃描可用網路並顯示可用的網路。

注意：CSSC禁用Windows零配置。

注意：只有那些為廣播啟用的SSID可見。



注意：預設情況下，WLAN控制器會廣播SSID，因此它在掃描SSID的「建立網路」清單中顯示。要建立網路配置檔案，只需按一下清單（企業）中的**SSID**和**建立網路**單選按鈕。

如果WLAN基礎設施配置為禁用廣播SSID，則必須手動新增SSID;按一下Access Devices下的**Add**單選按鈕，然後手動輸入適當的**SSID**（例如，Enterprise）。 為客戶端配置主動探測行為，即客戶端主動探測其配置的SSID;在Add Access Device視窗中輸入SSID後，請指定**Active search for this access device**。

註：如果沒有首先為配置檔案配置EAP身份驗證設定，則埠設定不允許企業模式(802.1X)。

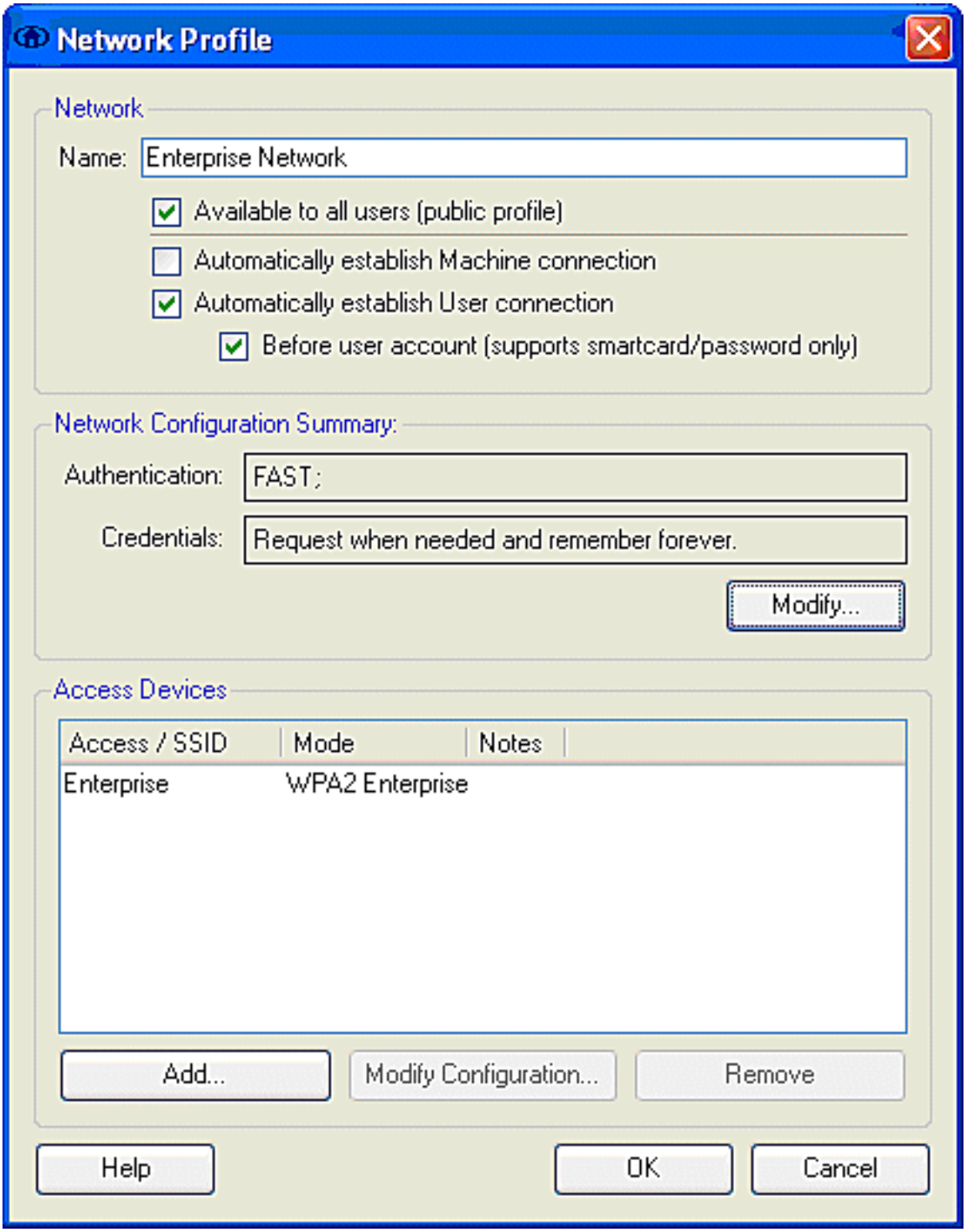
Create Network單選按鈕啟動Network Profile視窗，該視窗允許您將所選（或已配置的）SSID與身份驗證機制相關聯。為配置檔案分配描述性名稱。

注意：可在此身份驗證配置檔案下關聯多個WLAN安全型別和/或SSID。

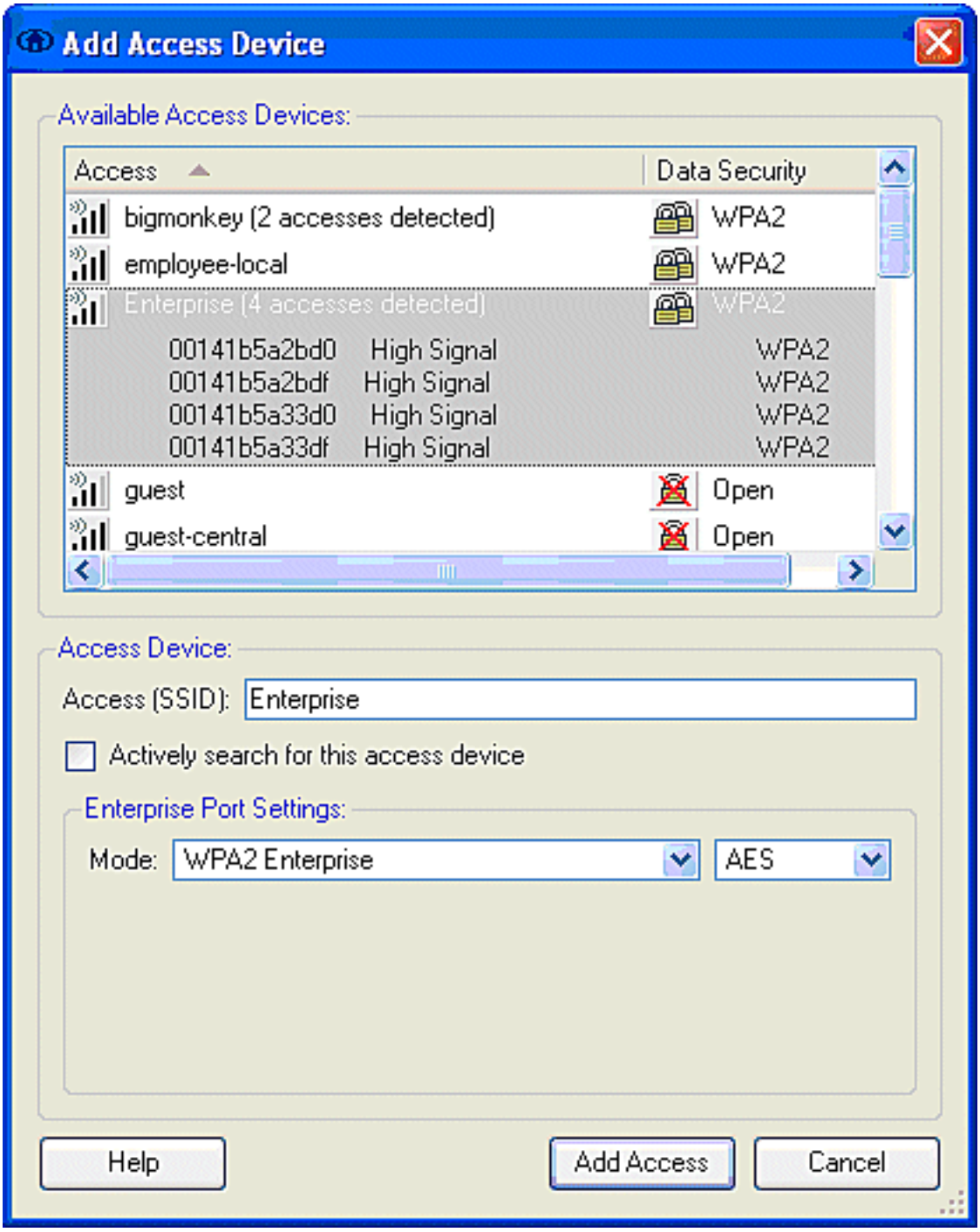
要使客戶端在RF覆蓋範圍內自動連線到網路，請選擇**自動建立使用者連線**。取消選中**Available to all users**（如果不想將此配置檔案用於電腦上的其他使用者帳戶，則對所有使用者可用）。如果未

選擇**Automatically established**，則使用者必須開啟CSSC視窗並使用**Connect**單選按鈕手動啟動WLAN連線。

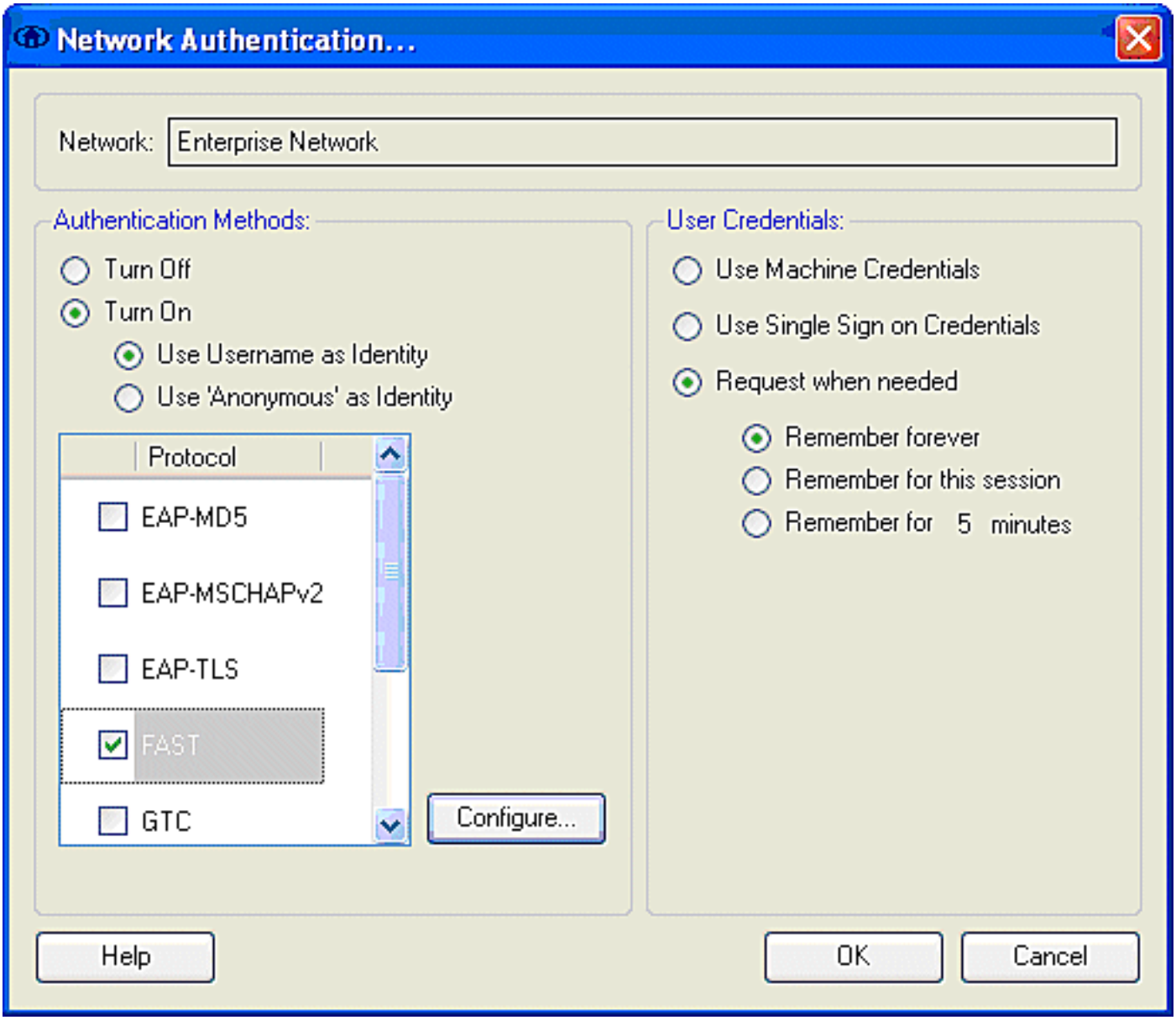
如果希望在使用者登入之前啟動WLAN連線，請選擇**Before user account**。這允許使用儲存的使用者憑證（在EAP-FAST中使用TLS時提供密碼或證書/智慧卡的單點登入操作）。



注意：對於使用Cisco Aironet 350系列客戶端介面卡的WPA/TKIP操作，必須禁用WPA握手驗證，因為CSSC客戶端與350驅動程式之間目前存在與WPA握手雜湊驗證相關的不相容性。在**客戶端>高級設定> WPA/WPA2握手驗證**下禁用此功能。禁用的握手驗證仍允許WPA中固有的安全功能（TKIP每資料包金鑰和消息完整性檢查），但禁用初始WPA金鑰身份驗證。



在Network Configuration Summary下，按一下**Modify**以配置EAP/憑據設定。指定**Turn On** Authentication，在Protocol下選擇**FAST**，然後選擇**'Anonymous'作為Identity**（以便在初始EAP請求中不使用使用者名稱）。 可以使用**使用使用者名稱作為標識**作為外部EAP標識，但許多客戶不希望在初始未加密EAP請求中顯示使用者ID。指定**使用單一登入憑據**以使用登入憑據進行網路身份驗證。按一下**Configure**以設定EAP-FAST引數。



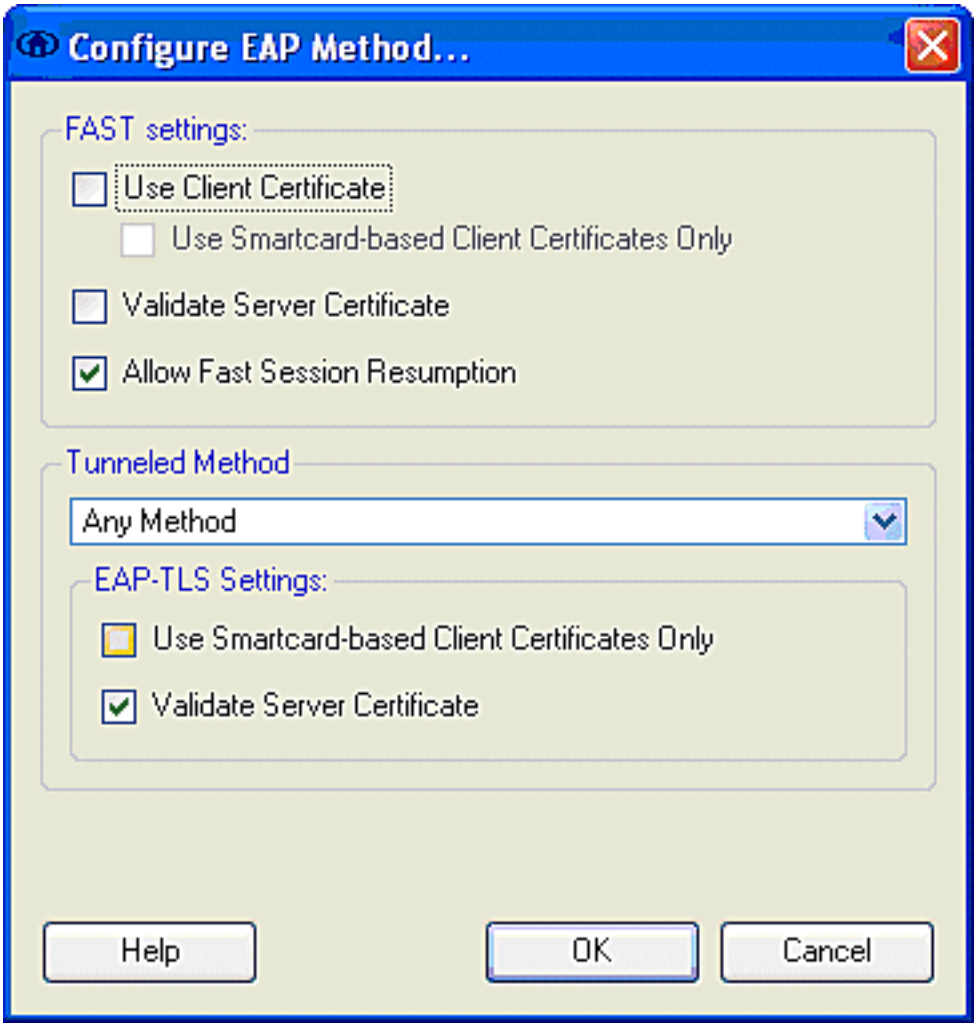
在FAST設定下，可以指定**Validate Server Certificate**，這將允許客戶端在建立EAP-FAST會話之前驗證EAP-FAST伺服器(ACS)證書。這可以保護客戶端裝置不連線到未知或欺詐EAP-FAST伺服器，並且不小心將其身份驗證憑證提交到不受信任的來源。這要求安裝ACS伺服器的證書，並且客戶端也安裝相應的根證書頒發機構證書。在本示例中，未啟用伺服器證書驗證。

在FAST設定下，可以指定**Allow Fast Session Resumption**，這允許基於隧道（TLS會話）資訊而恢復EAP-FAST會話，而不是要求完全的EAP-FAST重新驗證。如果EAP-FAST伺服器和客戶端具有在初始EAP-FAST身份驗證交換內協商的TLS會話資訊的公知，則可能發生會話恢復。

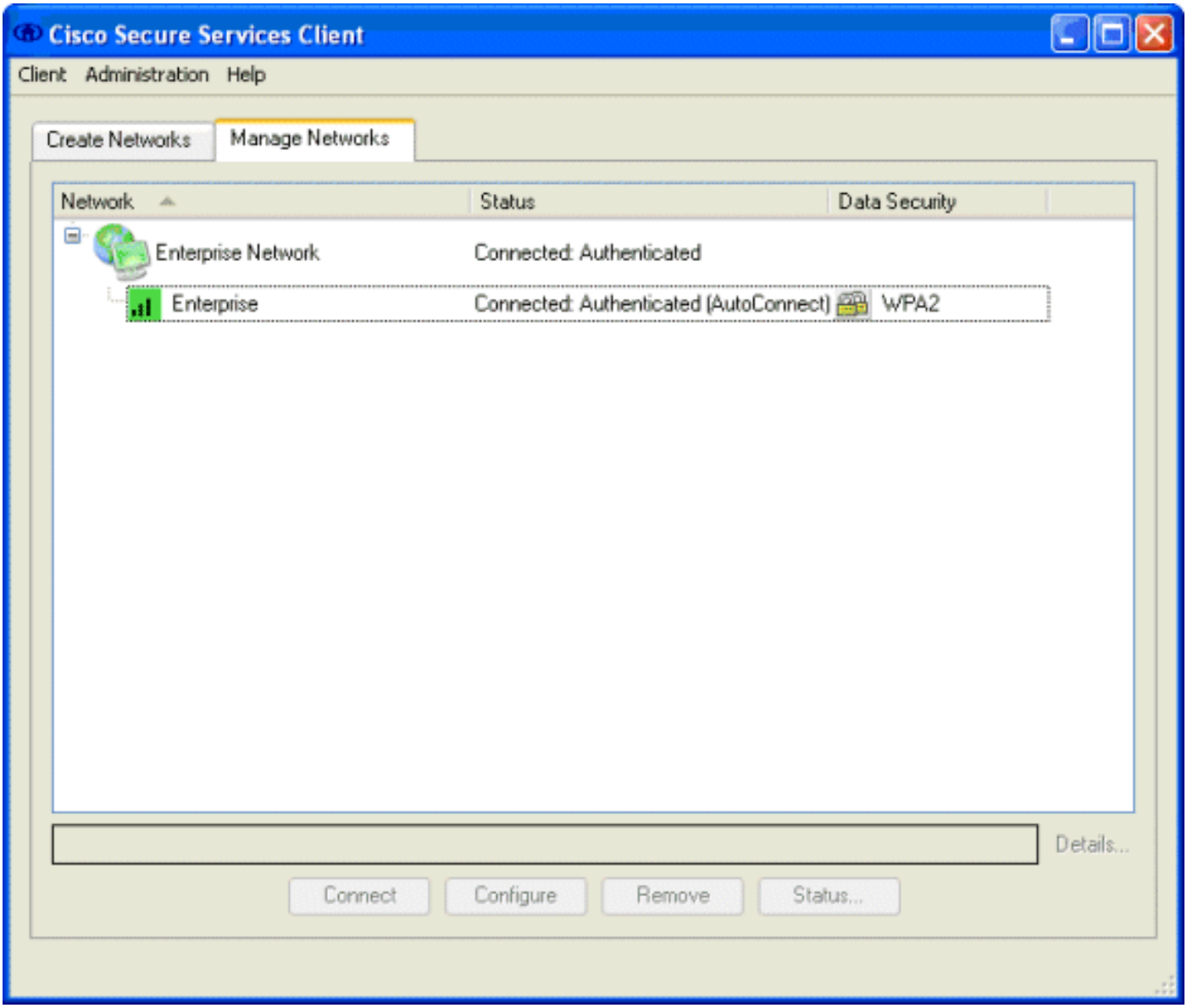
注意：必須為EAP-FAST會話恢復配置EAP-FAST伺服器和客戶端。

在Tunneled Method > EAP-TLS Settings下，指定**Any Method**以允許EAP-MSCHAPv2進行PAC自動調配，並允許EAP-GTC進行身份驗證。如果您使用Microsoft格式的資料庫（如Active Directory），並且如果網路上不支援任何EAP-FAST v1客戶端，則還可以指定僅使用**MSCHAPv2**作為隧道方法。

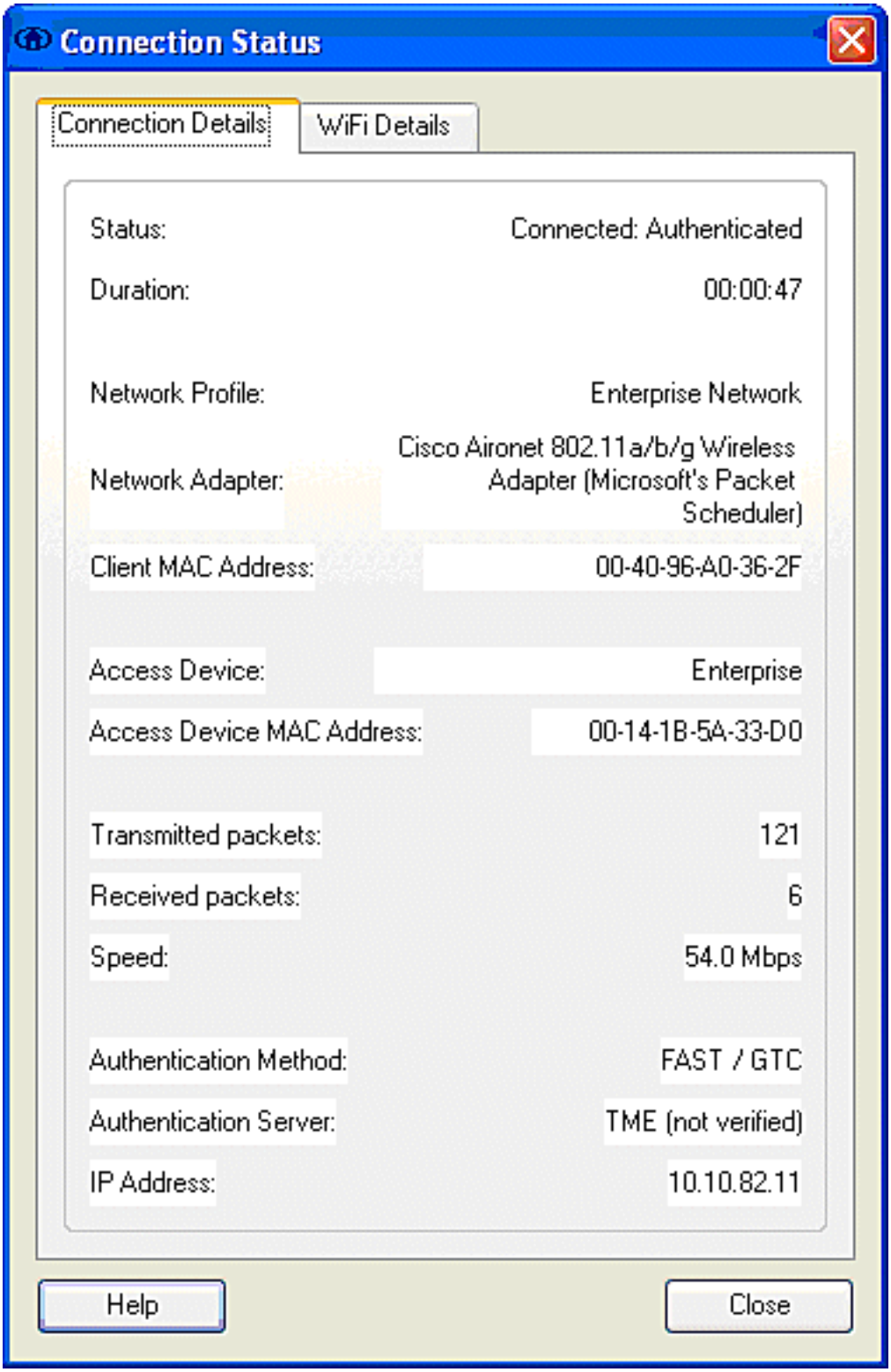
注意：在此視窗的EAP-TLS設定下預設啟用驗證伺服器證書。由於示例不使用EAP-TLS作為內部身份驗證方法，因此此欄位不適用。如果啟用此欄位，則除了在EAP-TLS內對客戶端證書進行伺服器驗證外，它還使客戶端能夠驗證伺服器證書。

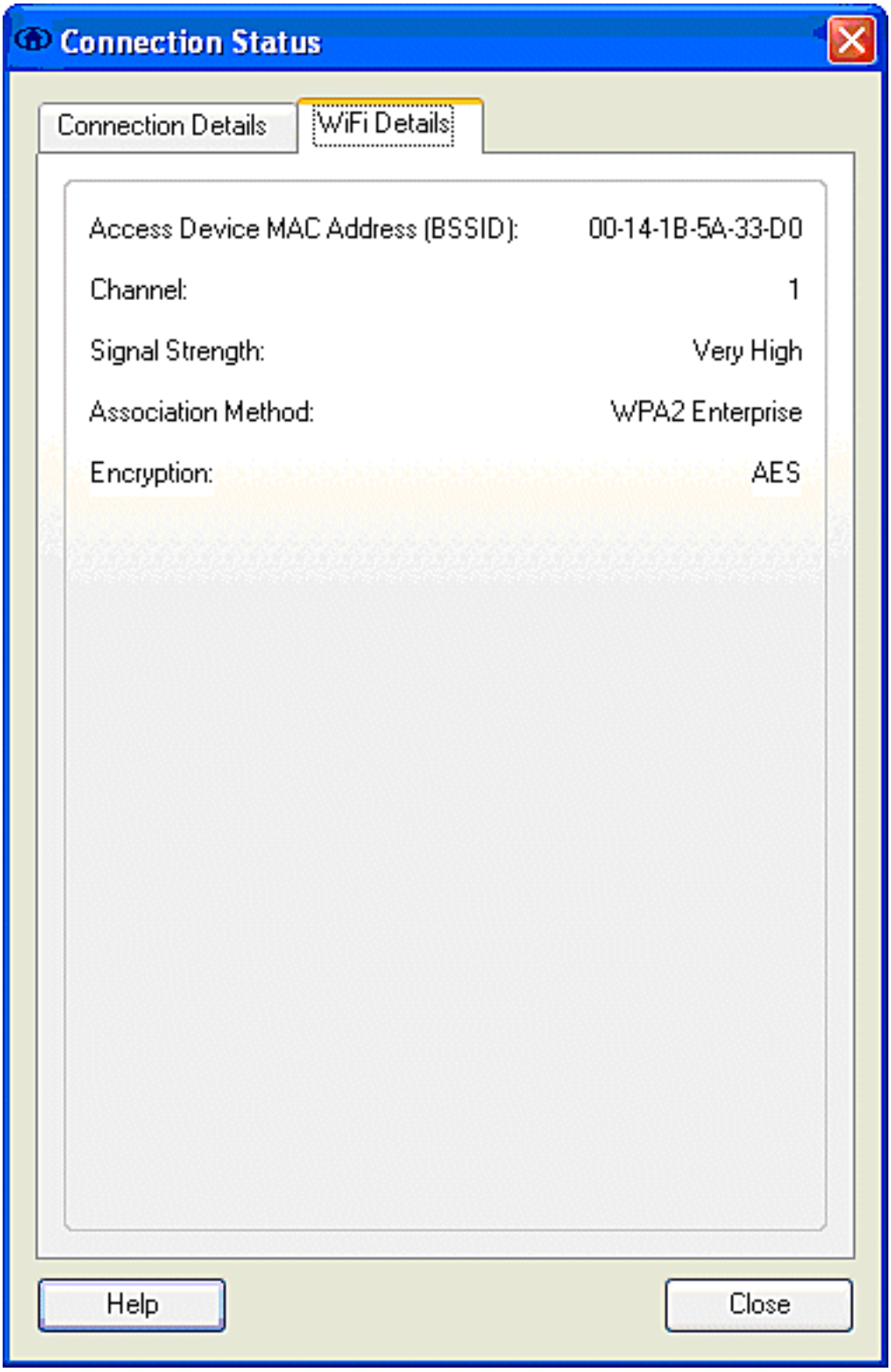


按一下**OK**儲存EAP-FAST設定。由於客戶端在profile下配置為「自動建立」，因此它會自動發起與網路的關聯/身份驗證。在管理網路頁籤中，網路、狀態和資料安全欄位指示客戶端的連線狀態。從示例中可以看到Profile Enterprise Network正在使用中，而Network Access Device是SSID Enterprise，它表示Connected:Authenticated並使用Autoconnect。Data Security欄位指示使用的802.11加密型別，例如WPA2。



客戶端進行身份驗證後，在Manage Networks頁籤的Profile下選擇**SSID**，然後按一下**Status**查詢連線詳細資訊。Connection Details視窗提供有關客戶端裝置、連線狀態和統計資訊以及身份驗證方法的資訊。WiFi Details（WiFi詳細資訊）頁籤提供有關802.11連線狀態的詳細資訊，包括RSSI、802.11通道和身份驗證/加密。


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



作為系統管理員，您有權使用診斷實用程式「Cisco Secure Services Client System Report」(Cisco Secure Services Client System Report)，該報告可用於標準CSSC分發。此實用程式可從「開始」選單或CSSC目錄中獲得。若要獲取資料，請按一下**收集資料>複製到剪貼簿>查詢報告檔案**。這會將Microsoft檔案資源管理器視窗引導至包含壓縮報告檔案的目錄。在壓縮的檔案中，最有用的資料位於log(log_current)下。

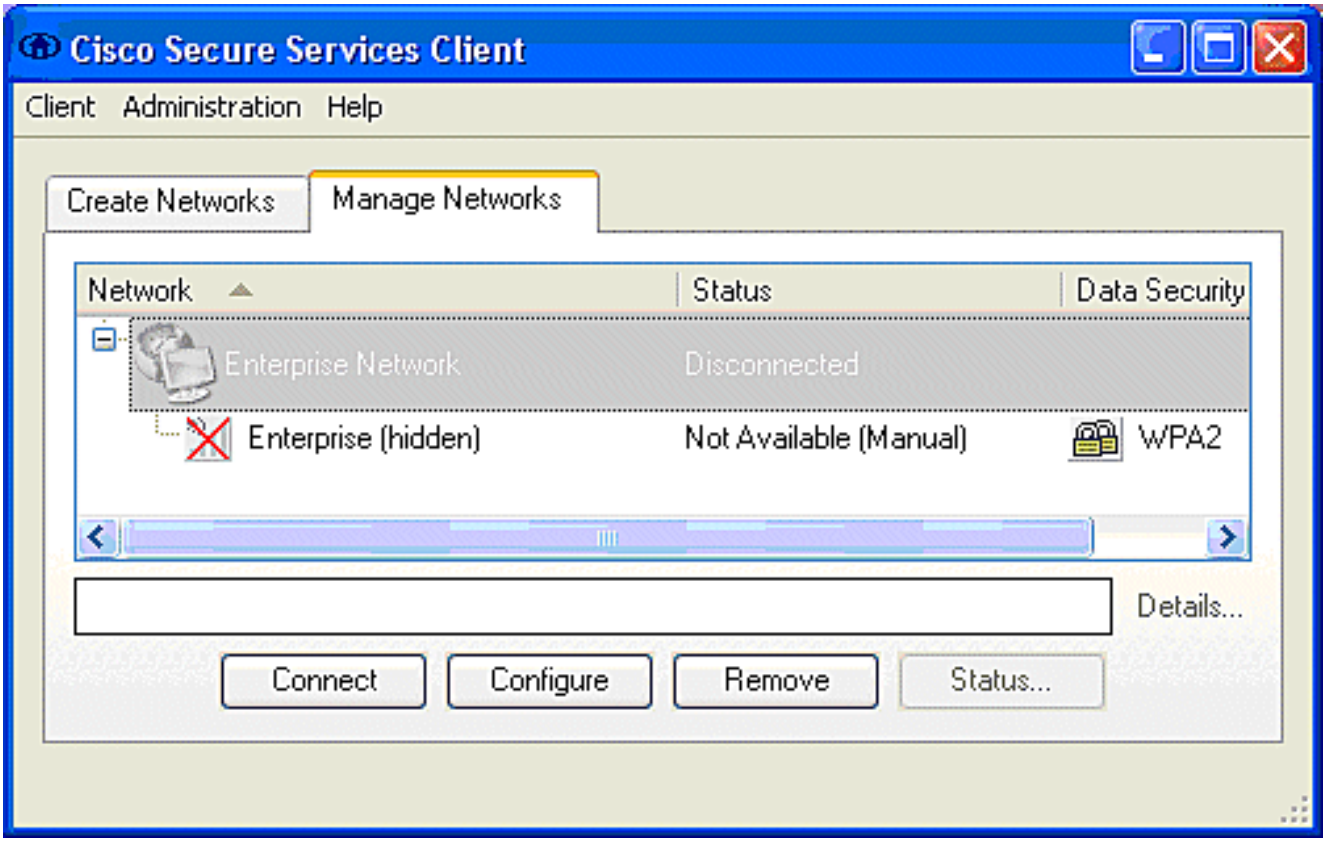
該實用程式提供CSSC的當前狀態、介面和驅動程式詳細資訊，以及WLAN資訊（檢測到的SSID、關聯狀態等）。 這非常有用，特別是用於診斷CSSC和WLAN介面卡之間的連線問題。

驗證操作

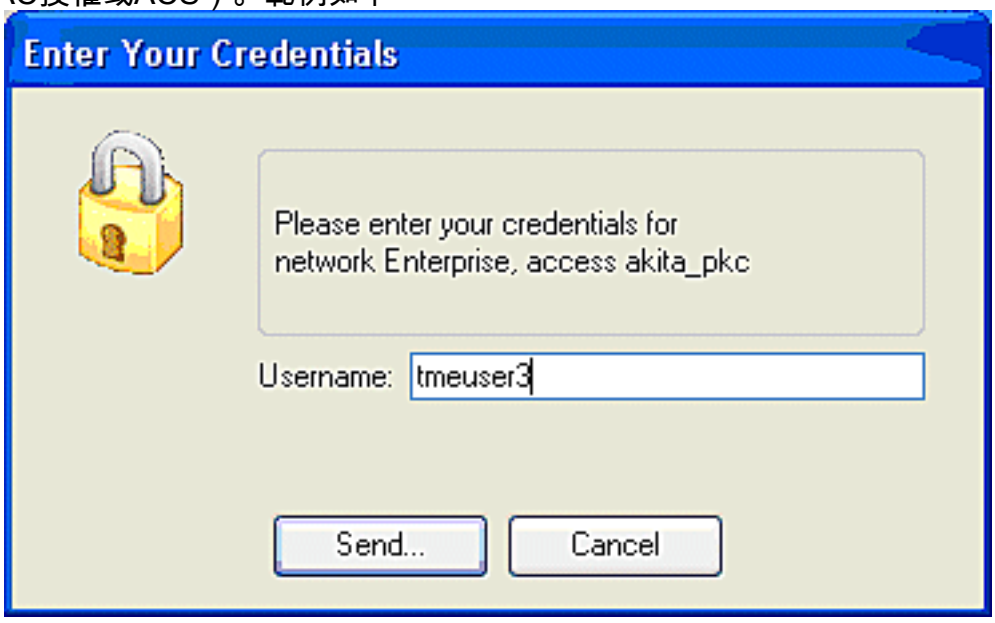
在配置Cisco Secure ACS伺服器、WLAN控制器、CSSC客戶端以及可能的正確配置和資料庫填充後，WLAN網路將配置為EAP-FAST身份驗證和安全客戶端通訊。可以監控許多點來檢查安全會話的進度/錯誤。

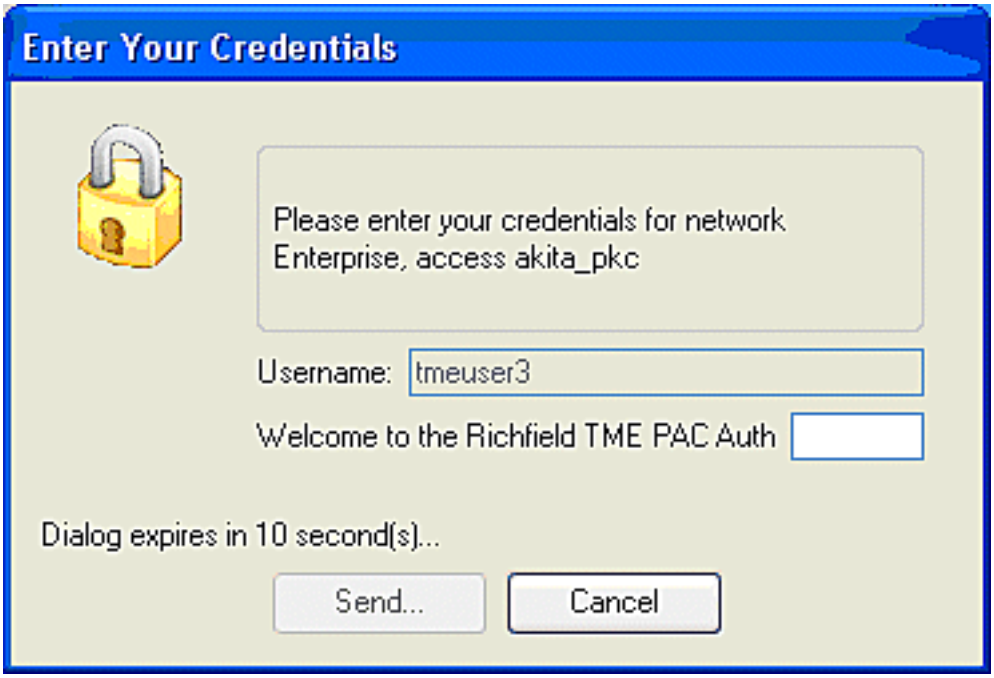
為了測試配置，請嘗試將無線客戶端與採用EAP-FAST身份驗證的WLAN控制器相關聯。

1. 如果CSSC配置為自動連線，客戶端將自動嘗試此連線。如果沒有將其配置為自動連線和單點登入操作，則使用者必須通過**Connect**單選按鈕啟動WLAN連線。這將啟動EAP身份驗證所經過的802.11關聯過程。範例如下
   ：

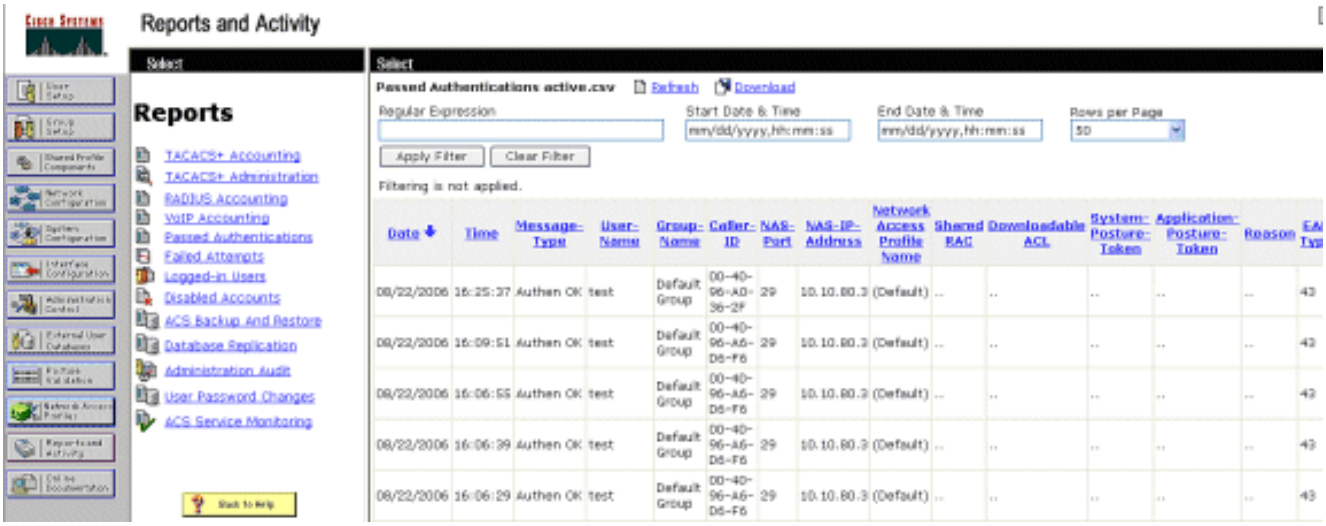


2. 隨後，系統將提示使用者提供用於EAP-FAST身份驗證的使用者名稱和密碼（來自EAP-FAST PAC授權或ACS）。範例如下
   ：

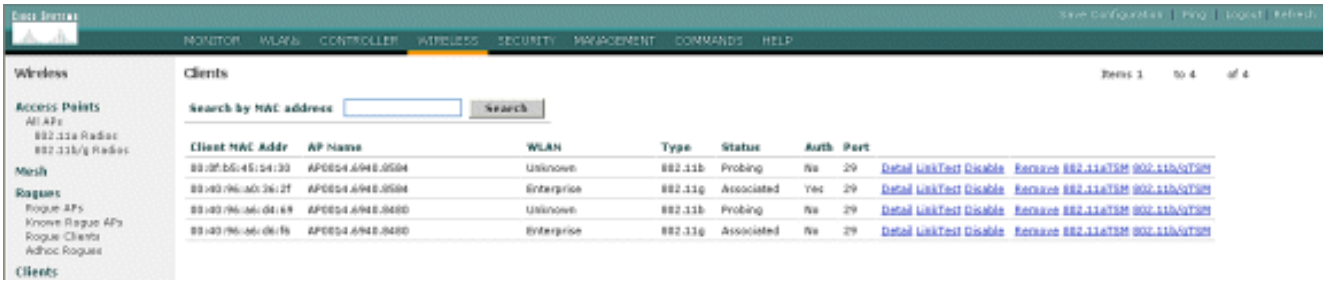




3. CSSC使用者端會通過WLC將使用者認證傳遞到RADIUS伺服器(Cisco Secure ACS)以驗證認證。ACS通過比較資料和配置的資料庫（在示例配置中，外部資料庫為Windows Active Directory）來驗證使用者憑據，並在使用者憑據有效時提供對無線客戶端的訪問。ACS伺服器上的Passed Authentications報告顯示客戶端已通過RADIUS/EAP身份驗證。範例如下：



4. RADIUS/EAP身份驗證成功後，無線客戶端（本例中為00:40:96:ab:36:2f）將使用AP/WLAN控制器進行身份驗證。



附錄

除Cisco Secure ACS和Cisco WLAN控制器上提供的診斷和狀態資訊外，還有其它點可用於診斷EAP-FAST身份驗證。雖然大多數身份驗證問題不需要使用WLAN嗅探器或在WLAN控制器上調試EAP交換即可診斷，但此參考資料也包含在內，有助於排除故障。

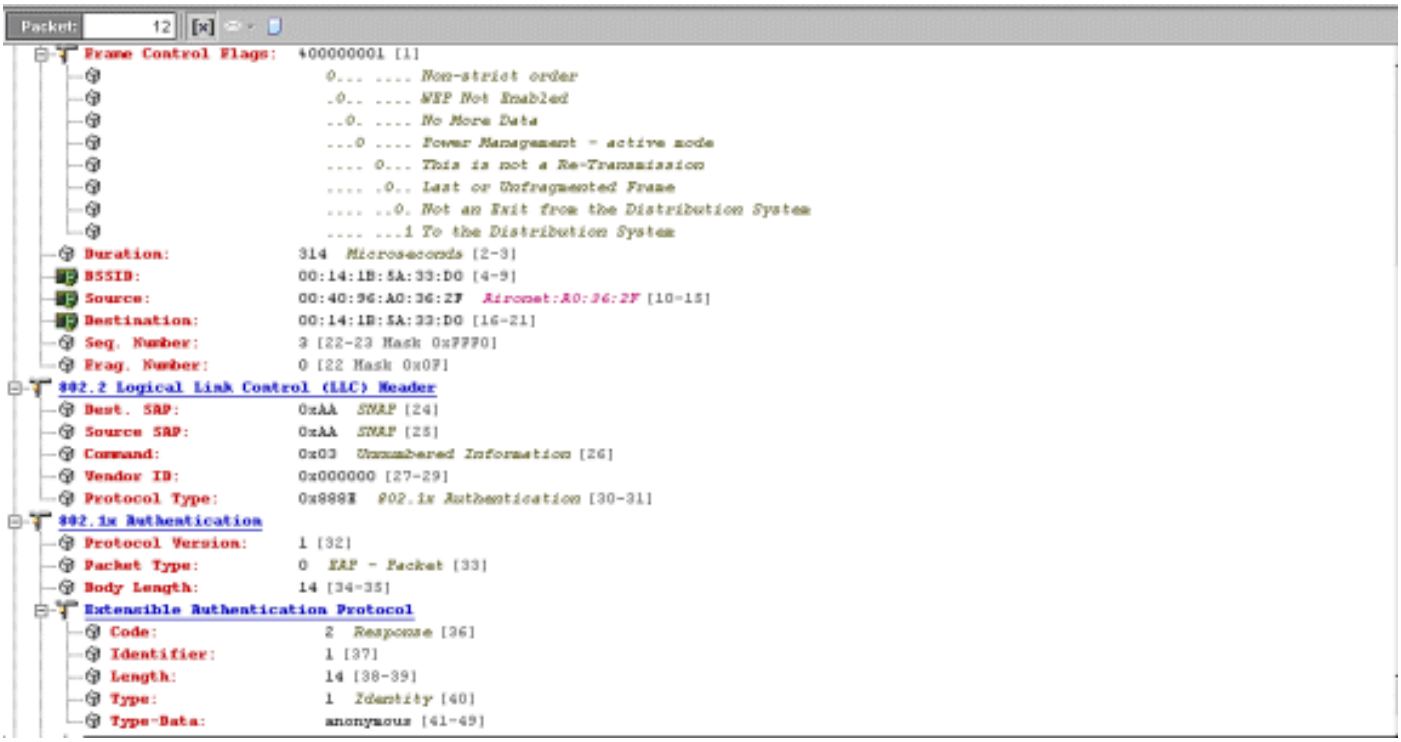
適用於EAP-FAST Exchange的監聽器擷取

此802.11監聽器擷取顯示驗證交換。

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

此資料包顯示初始EAP-FAST EAP響應。

註：如在CSSC客戶端上配置的那樣，匿名在初始EAP響應中用作外部EAP標識。



在WLAN控制器上偵錯

WLAN控制器上可以使用以下debug指令來監控驗證交換的進度：

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable

以下是在WLAN控制器上使用偵錯功能監控的CSSC使用者端和ACS之間開始驗證交易的範例：

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

這是從控制器調試成功完成EAP交換（使用WPA2身份驗證）：

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
```

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
```

```
Thu Aug 24 18:20:54 2006: AVP[10]
   Tunnel-Medium-Type.................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id....................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type...................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets..................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets.................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets.................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets................0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time..................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time....................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id.................10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id..................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

相關資訊

- 適用於Windows伺服器的Cisco Secure ACS安裝指南
- 思科安全ACS 4.1配置指南
- 使用WLC和Cisco Secure ACS配置示例根據SSID限制WLAN訪問
- 採用ACS 4.0和Windows 2003的統一無線網路下的EAP-TLS
- 使用RADIUS伺服器和無線LAN控制器進行動態VLAN分配配置示例
- 技術支援與文件 - Cisco Systems