RSA SecurID Ready with Wireless LAN Controllers and Cisco Secure ACS配置示例

目錄

簡介

本文說明如何設定和設定在RSA SecurID驗證的WLAN環境中使用的支援思科輕量型存取點通訊協定(LWAPP)的AP和無線LAN控制器(WLC)，以及思科安全存取控制伺服器(ACS)。特定於RSA SecurID的實施指南位於www.rsasecured.com。

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以及如何設定WLC基本引數。
- 瞭解如何使用Aironet案頭實用程式(ADU)配置思科無線客戶端配置檔案。
- 具備思科安全ACS的功能知識。
- 具有LWAPP基礎知識。
- 對Microsoft Windows Active Directory(AD)服務、域控制器和DNS概念有基礎認識。**注意：**在嘗試此配置之前，請確保ACS和RSA Authentication Manager伺服器位於同一域中，並且它們的系統時鐘完全同步。如果您使用的是Microsoft Windows AD服務，請參閱Microsoft文檔以配

置同一域中的ACS和RSA Manager伺服器。有關相關資訊，請參閱配置Active Directory和Windows使用者資料庫。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- RSA身份驗證管理器6.1
- 適用於Microsoft Windows的RSA驗證代理6.1
- Cisco安全ACS 4.0(1)內部版本27**註：**隨附的RADIUS伺服器可用於代替Cisco ACS。有關如何配置伺服器的資訊，請參閱RSA Authentication Manager附帶的RADIUS文檔。
- 適用於4.0版（4.0.155.0版）的Cisco WLC和輕量型存取點

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。

背景資訊

RSA SecurID系統是一個雙因素使用者身份驗證解決方案。RSA SecurID身份驗證器與RSA Authentication Manager和RSA Authentication Agent結合使用，要求使用者使用二元身份驗證機制來識別自己。

一個是RSA SecurID代碼，這是一個每60秒在RSA SecureID身份驗證器裝置上生成的隨機數。另一個是個人標識號(PIN)。

RSA SecurID身份驗證器與輸入密碼一樣簡單。為每個終端使用者分配一個RSA SecurID身份驗證器，該身份驗證器生成一次性代碼。登入時，使用者只需輸入此號碼和密碼PIN即可成功進行身份驗證。作為附加的優勢，RSA SecurID硬體令牌通常已預先程式設計為在收到時能夠完全正常工作。

此flash演示說明如何使用RSA secureID身份驗證器裝置：RSA演示。

通過RSA SecurID Ready程式，Cisco WLC和Cisco Secure ACS伺服器支援RSA SecurID身份驗證，開箱即用。RSA Authentication Agent軟體會攔截來自使用者（或使用者組）的本地或遠端訪問請求，並將它們定向到RSA Authentication Manager程式以進行身份驗證。

RSA Authentication Manager軟體是RSA SecurID解決方案的管理元件。它用於驗證身份驗證請求並集中管理企業網路的身份驗證策略。它與RSA SecurID身份驗證器和RSA Authentication Agent軟體配合使用。

在本文檔中，通過在思科ACS伺服器上安裝代理軟體，該伺服器用作RSA身份驗證代理。WLC是網路存取伺服器(NAS)（AAA使用者端），它反過來會將使用者端驗證轉送到ACS。本文檔演示了使用受保護的可擴展身份驗證協定(PEAP)客戶端身份驗證的概念和設定。

要瞭解PEAP身份驗證，請參閱思科受保護的可擴展身份驗證協定。

設定

本節提供用於設定本文件中所述功能的資訊。

本檔案會使用以下設定：

- 代理主機配置
- 驗證代理配置

代理主機配置

使用Cisco Secure ACS作為RADIUS伺服器

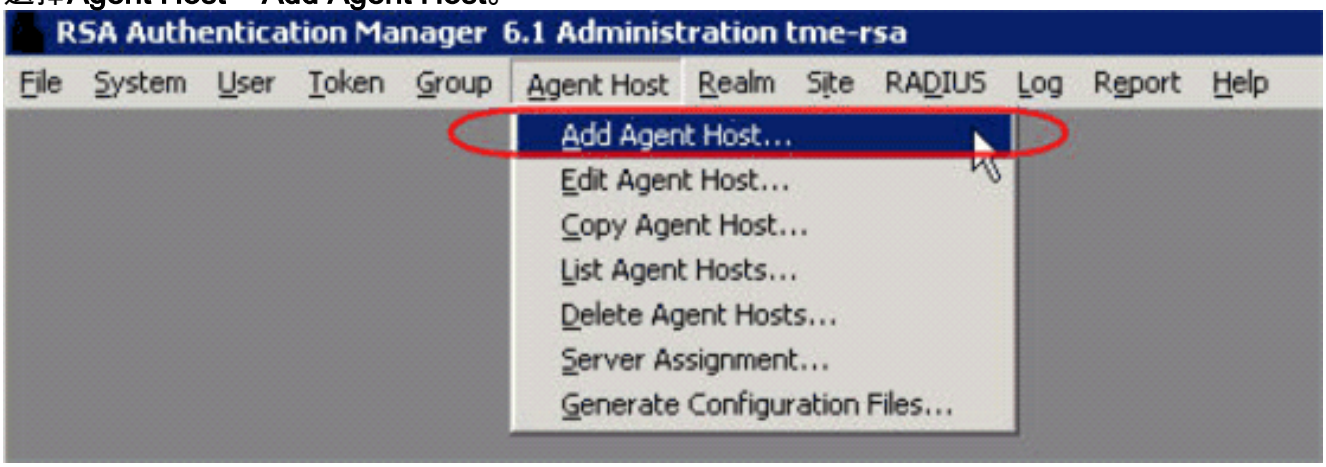
為了促進Cisco Secure ACS與RSA Authentication Manager/RSA SecurID裝置之間的通訊，必須將代理主機記錄新增到RSA Authentication Manager資料庫中。代理主機記錄標識其資料庫內的Cisco Secure ACS，並包含有關通訊和加密的資訊。

要建立代理主機記錄，需要以下資訊：

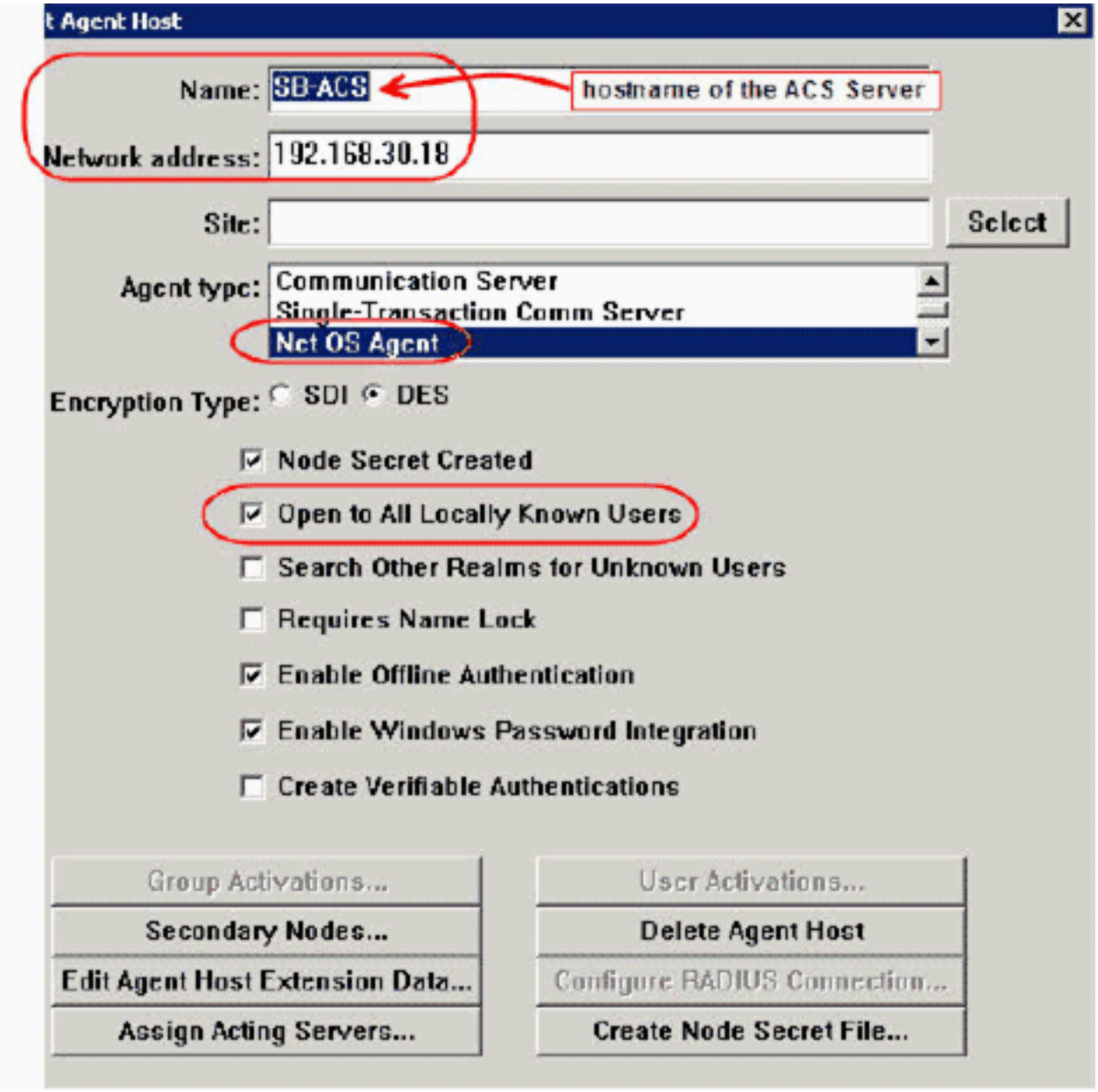
- Cisco ACS伺服器的主機名
- Cisco ACS伺服器所有網路介面的IP地址

請完成以下步驟：

1. 開啟RSA Authentication Manager主機模式應用程式。
2. 選擇**Agent Host > Add Agent Host**。



您會看到以下視窗



:

3. 為Cisco ACS伺服器名稱和網路地址輸入適當的資訊。選擇**NetOS**作為代理型別，並選中**Open to All Locally Known Users**覈取方塊。
4. 按一下「**OK**」（確定）。

使用RSA Authentication Manager 6.1 RADIUS伺服器

為了促進Cisco WLC和RSA Authentication Manager之間的通訊，必須將代理主機記錄新增到RSA Authentication Manager資料庫和RADIUS伺服器資料庫中。代理主機記錄用於識別其資料庫中的Cisco WLC，並包含有關通訊和加密的資訊。

要建立代理主機記錄，需要以下資訊：

- WLC的主機名
- WLC的管理IP地址
- RADIUS密碼，必須與Cisco WLC上的RADIUS密碼相符

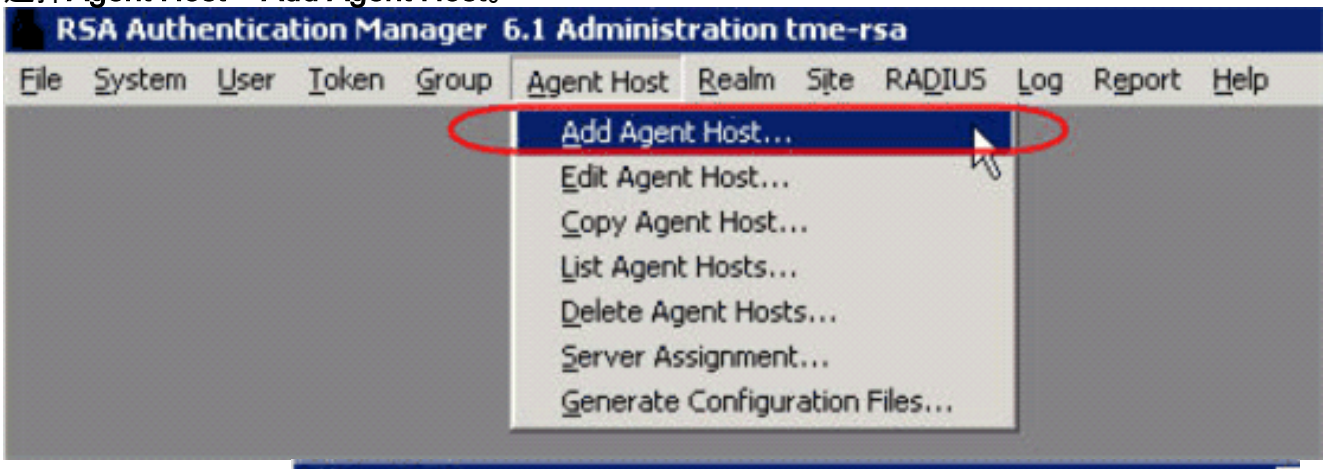
新增代理主機記錄時，WLC的角色配置為通訊伺服器。RSA Authentication Manager使用此設定來確定如何與WLC進行通訊。

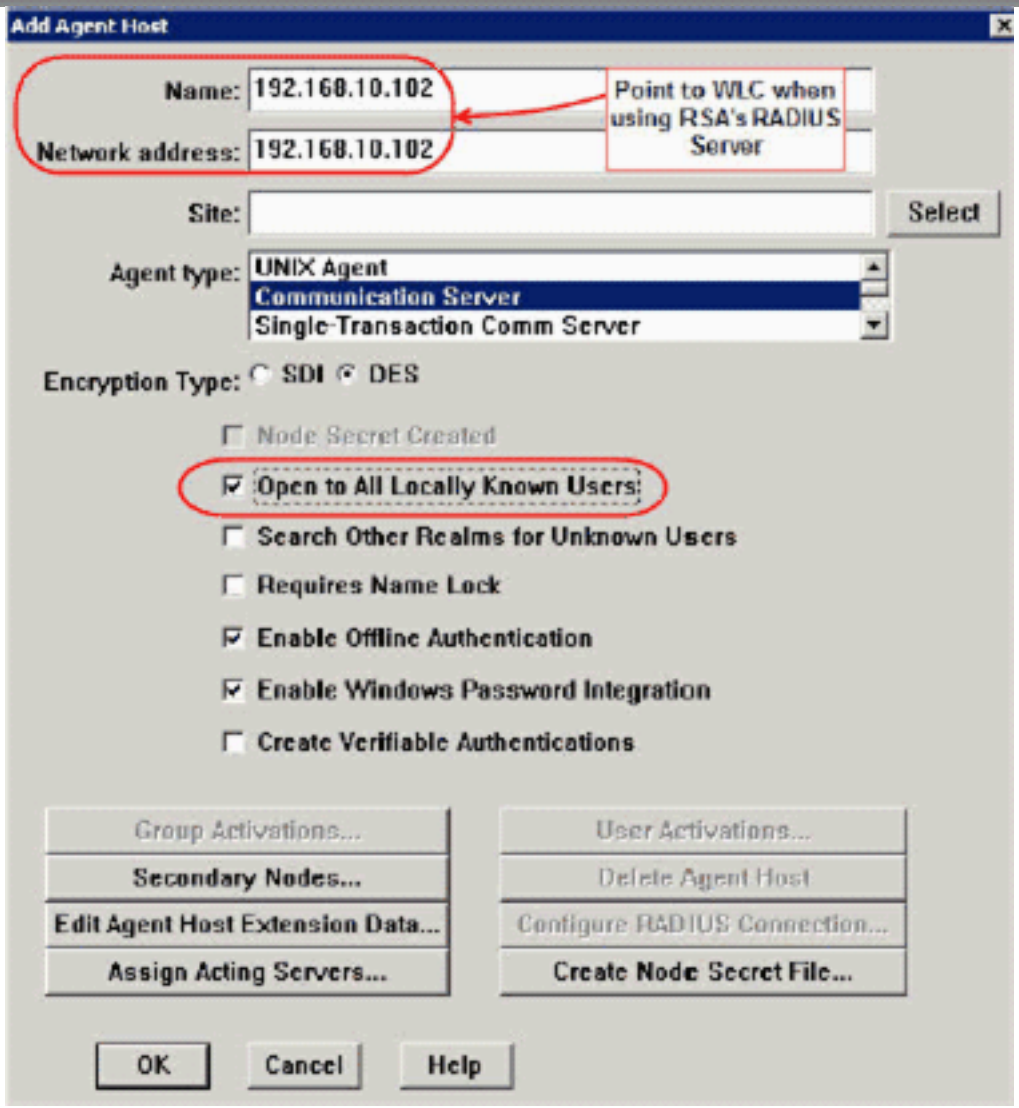
注意：RSA Authentication Manager/RSA SecurID裝置中的主機名必須解析為本地網路上的有效

IP地址。

請完成以下步驟：

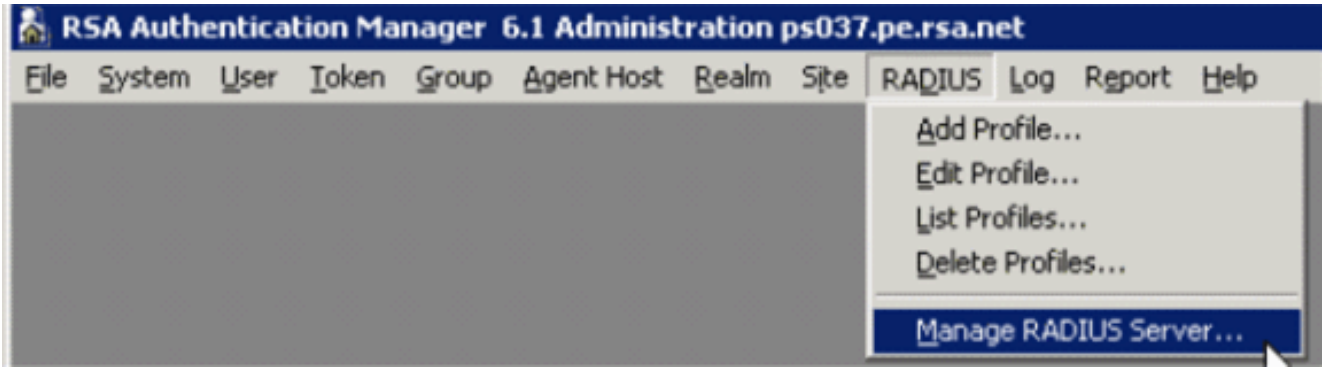
1. 開啟RSA Authentication Manager主機模式應用程式。
2. 選擇**Agent Host > Add Agent Host**。





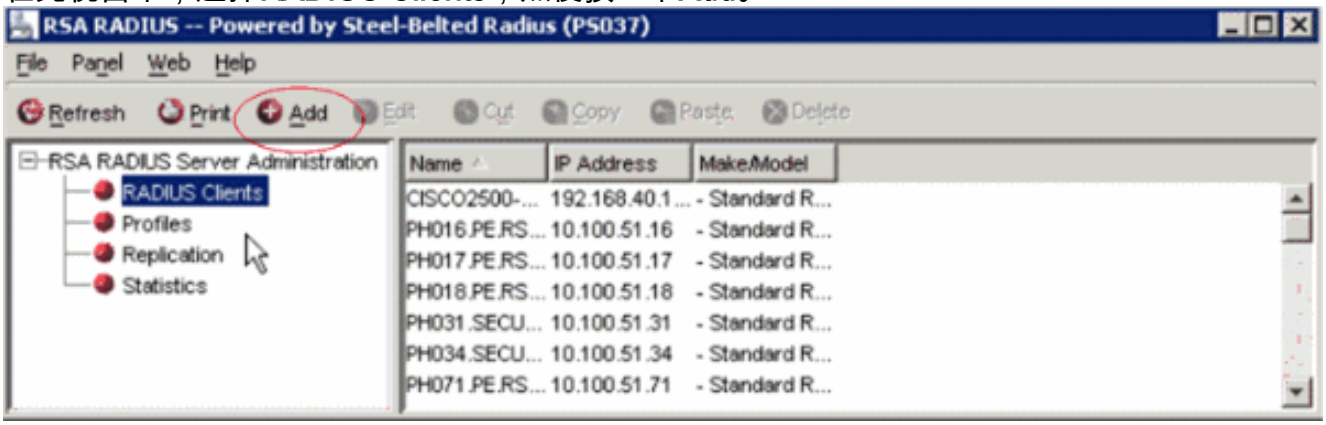
您會看到以下視窗：

3. 輸入WLC主機名（可解析的FQDN，如有必要）和網路地址的相應資訊。選擇**Communication Server**作為代理型別，並選中**Open to All Locally Known Users**覈取方塊。
4. 按一下「**OK**」（確定）。
5. 從選單中選擇**RADIUS > 管理RADIUS伺服器**。

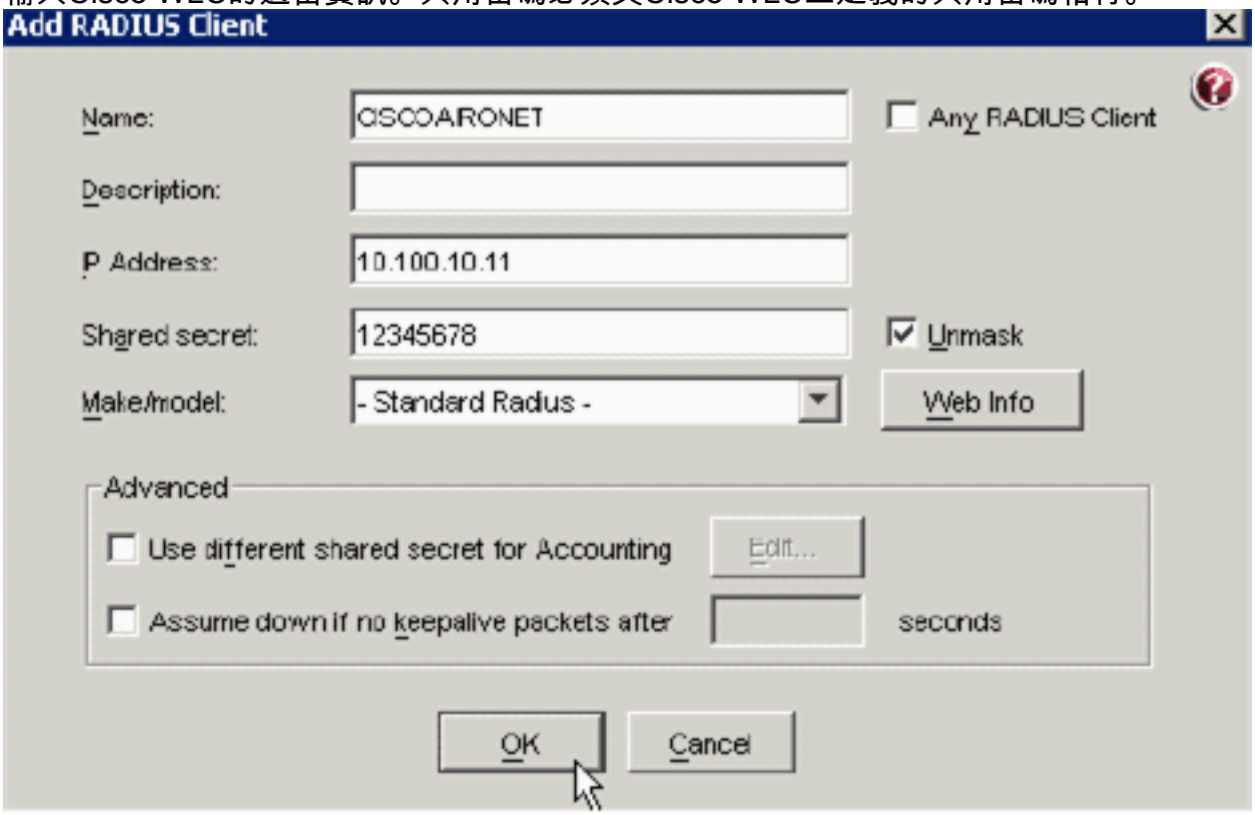


將開啟新的管理視窗。

6. 在此視窗中，選擇**RADIUS Clients**，然後按一下**Add**。



7. 輸入Cisco WLC的適當資訊。共用密碼必須與Cisco WLC上定義的共用密碼相符。



8. 按一下「**OK**」（確定）。

驗證代理配置

此表表示ACS的RSA身份驗證代理功能：

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

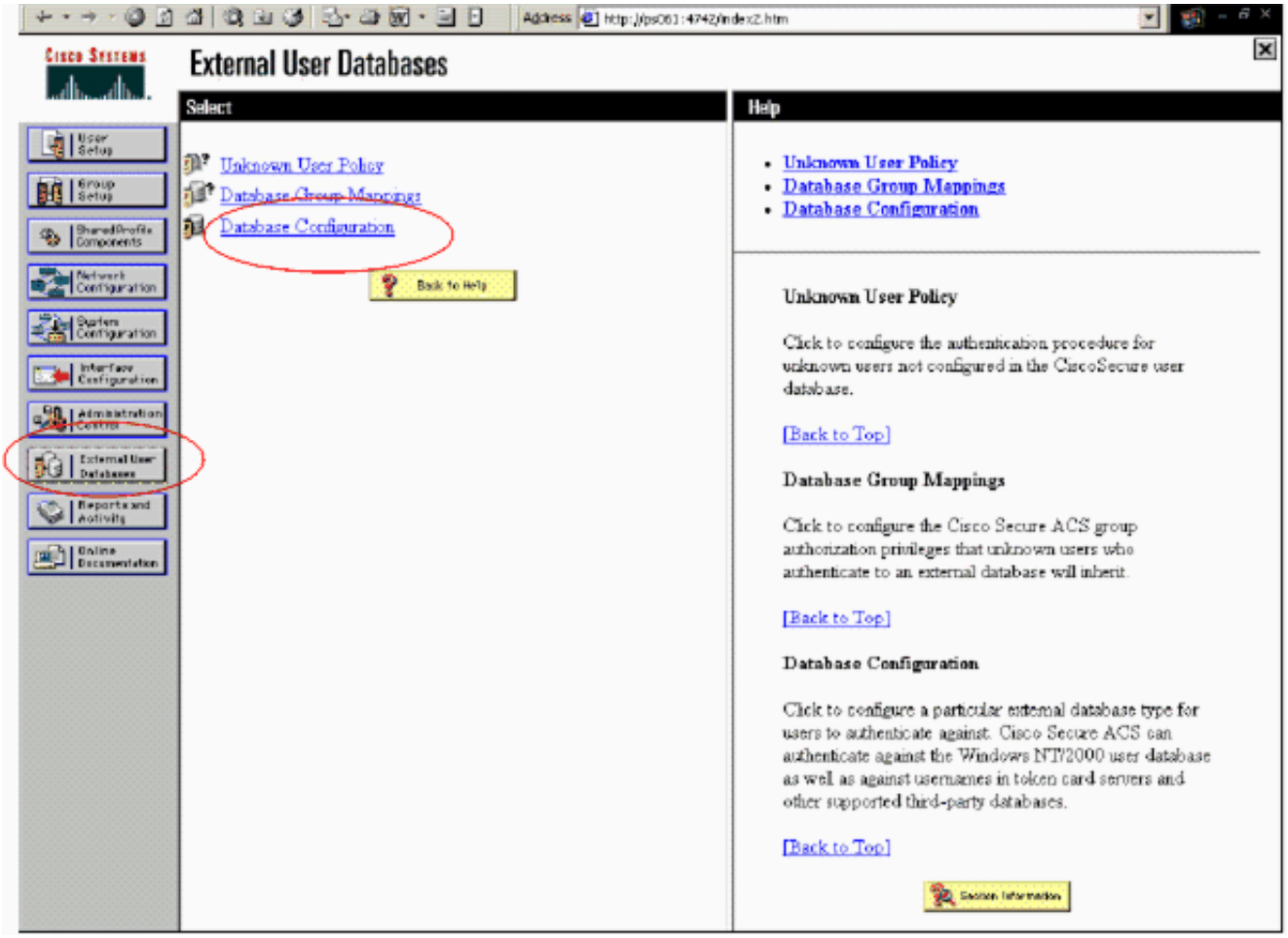
注意：請參閱RSA Authentication Manager附帶的RADIUS文檔，瞭解如何配置RADIUS伺服器（如果要使用的RADIUS伺服器）。

配置Cisco ACS

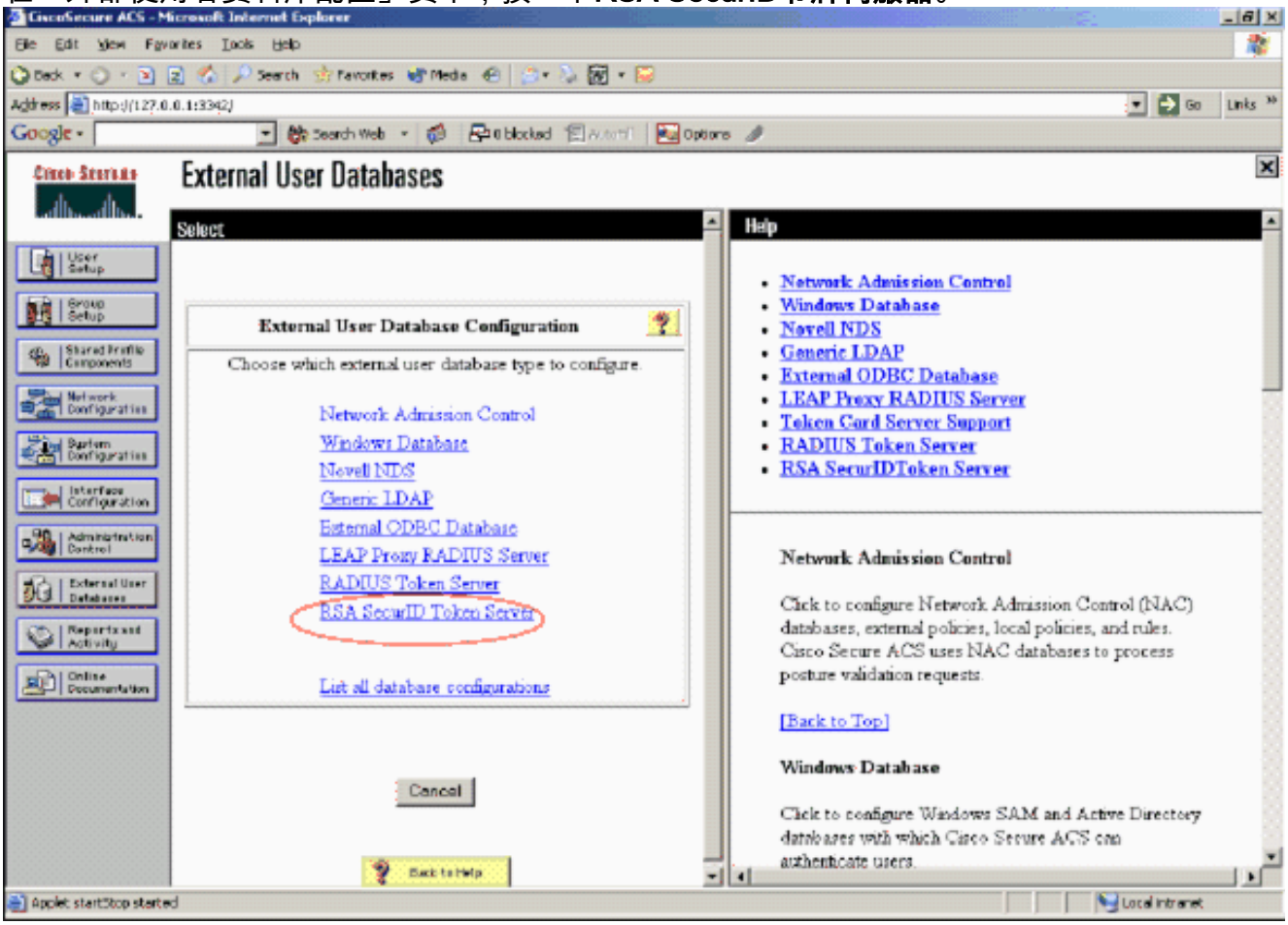
啟用RSA SecurID身份驗證

Cisco Secure ACS支援使用者的RSA SecurID身份驗證。完成以下步驟，以便配置Cisco Secure ACS以使用Authentication Manager 6.1對使用者進行身份驗證：

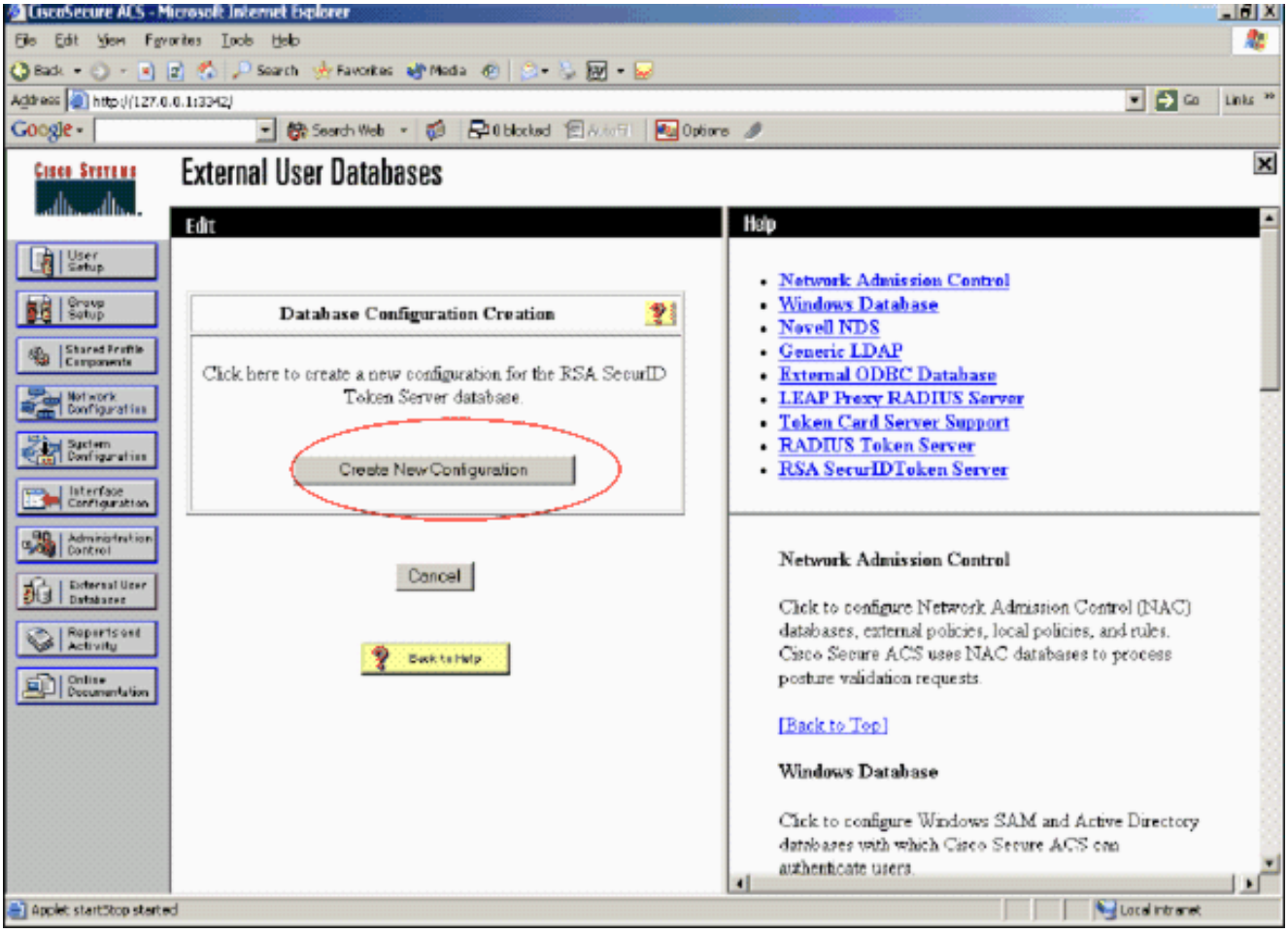
1. 在與Cisco Secure ACS伺服器相同的系統上安裝RSA Authentication Agent 5.6或更高版本。
2. 通過運行身份驗證代理的測試身份驗證功能驗證連線。
3. 將aceclnt.dll檔案從RSA伺服器**c:\Program Files\RSA Security\RSA Authentication Manager\prog**目錄複製到ACS伺服器的**c:\WINNT\system32**目錄。
4. 在導航欄中，按一下**外部使用者資料庫**。然後，在「外部資料庫」頁中按一下**資料庫配置**。



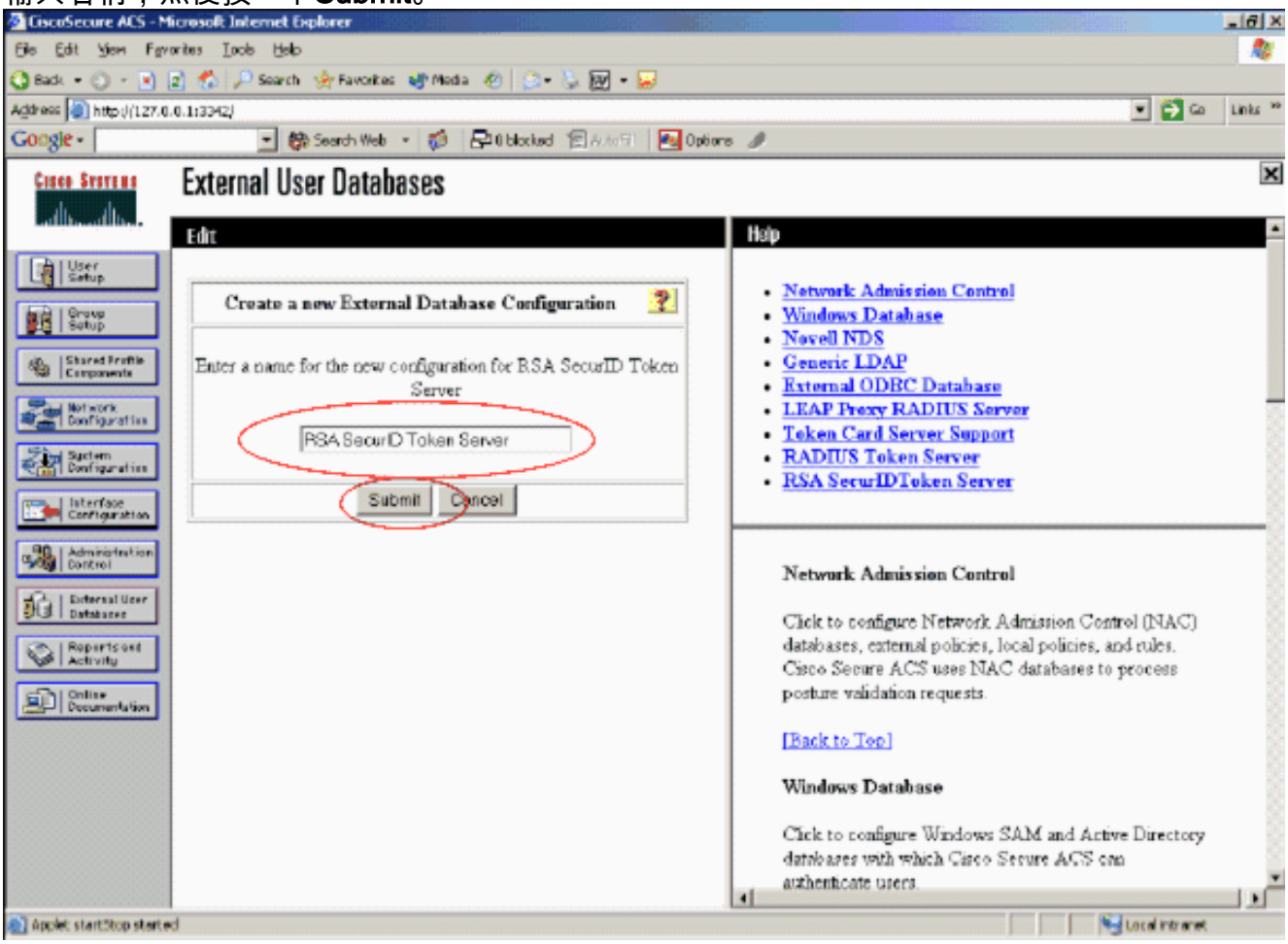
5. 在「外部使用者資料庫配置」頁中，按一下**RSA SecurID令牌伺服器**。



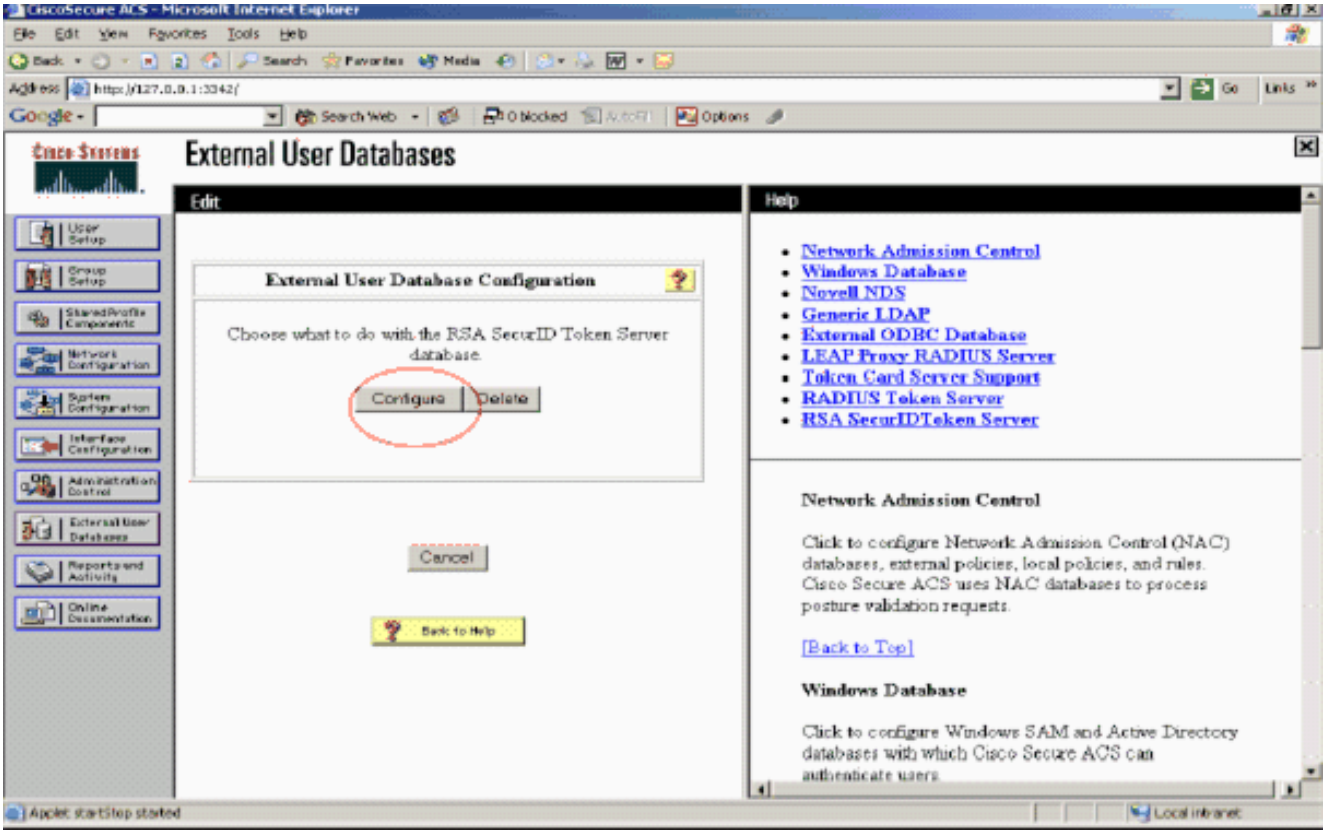
6. 按一下「**Create New Configuration**」。



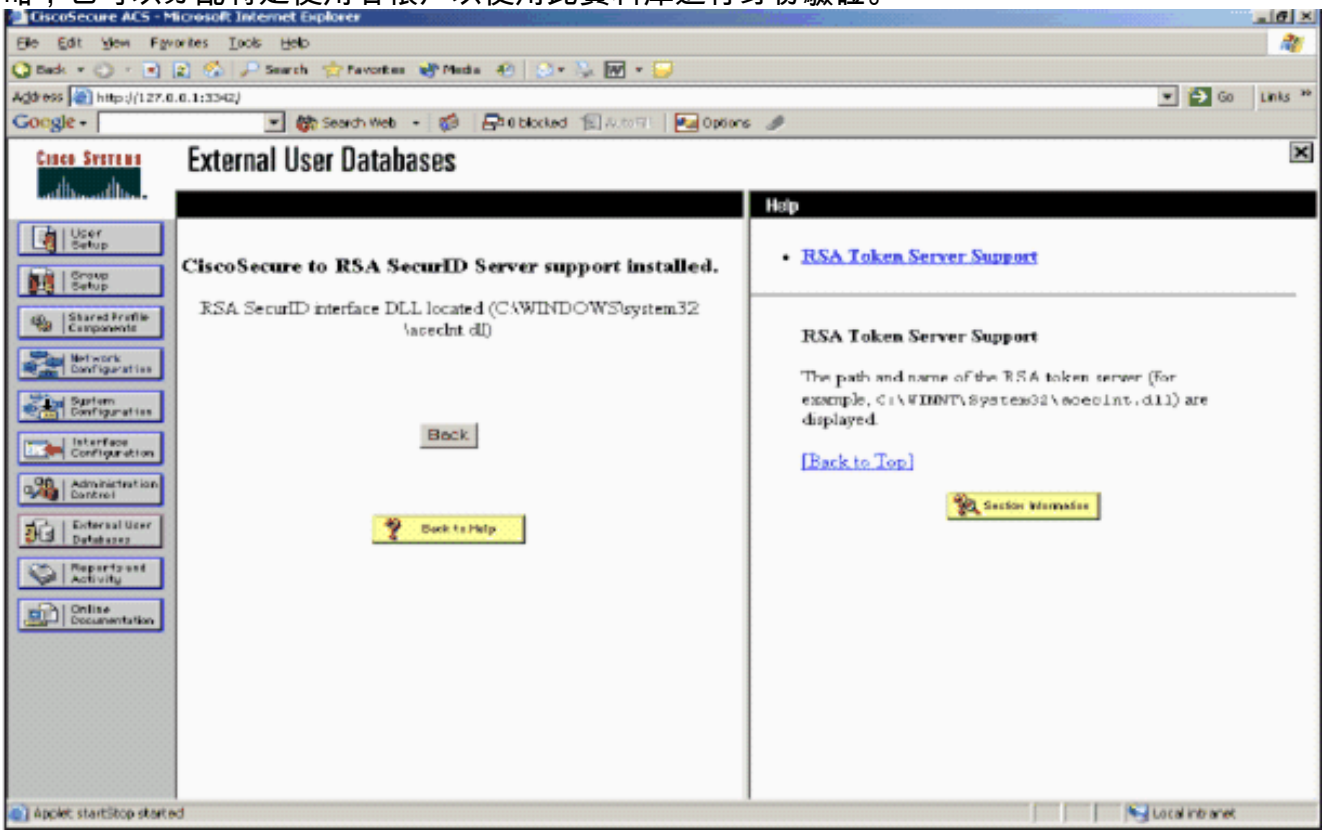
7. 輸入名稱，然後按一下**Submit**。



8. 按一下「**Configure**」。



Cisco Secure ACS顯示令牌伺服器的名稱和驗證器DLL的路徑。此資訊確認Cisco Secure ACS可以聯絡RSA身份驗證代理。可以將RSA SecurID外部使用者資料庫新增到未知使用者策略，也可以分配特定使用者帳戶以使用此資料庫進行身份驗證。

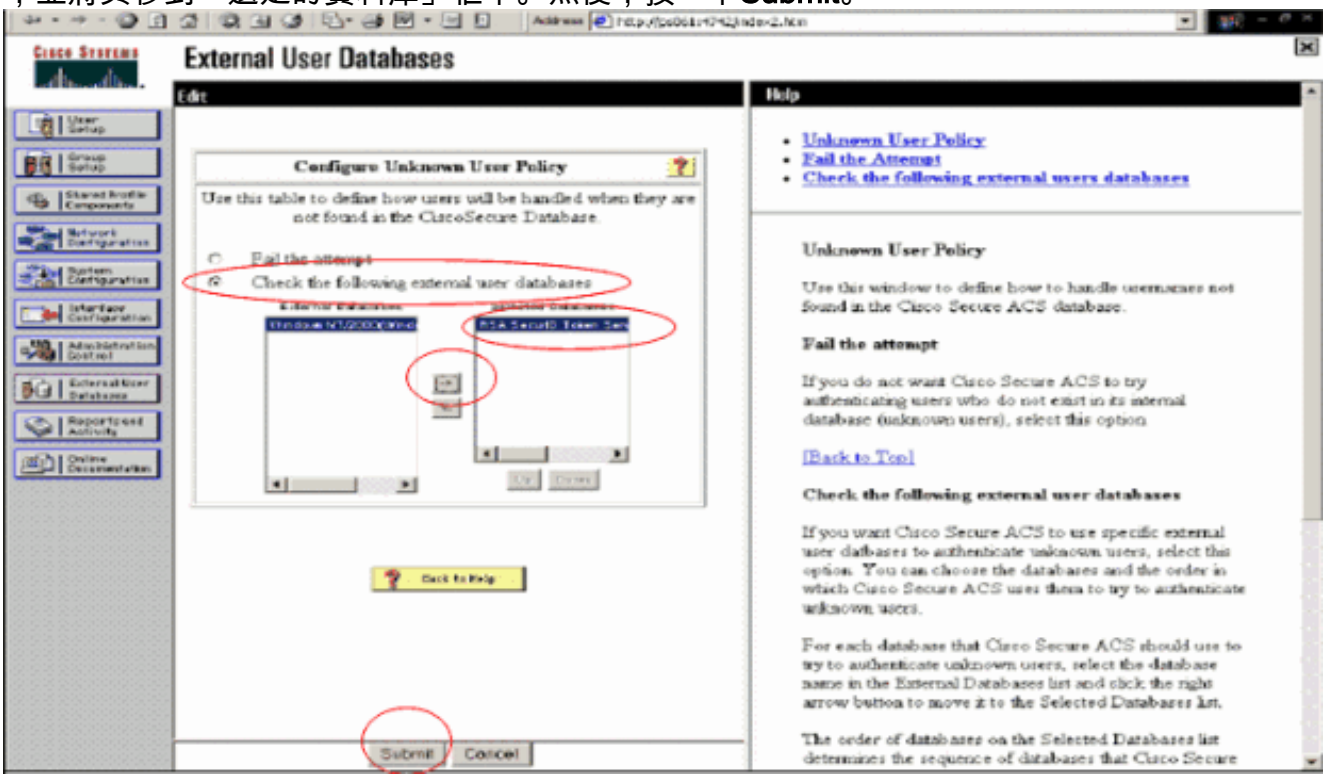


向未知使用者策略新增/配置RSA SecurID身份驗證

請完成以下步驟：

1. 在ACS導航欄中，按一下External User Database > Unknown User Policy。

2. 在**未知使用者策略**頁中，選擇**檢查以下外部使用者資料庫**，突出顯示**RSA SecurID令牌伺服器**，並將其移到「選定的資料庫」框中。然後，按一下**Submit**。

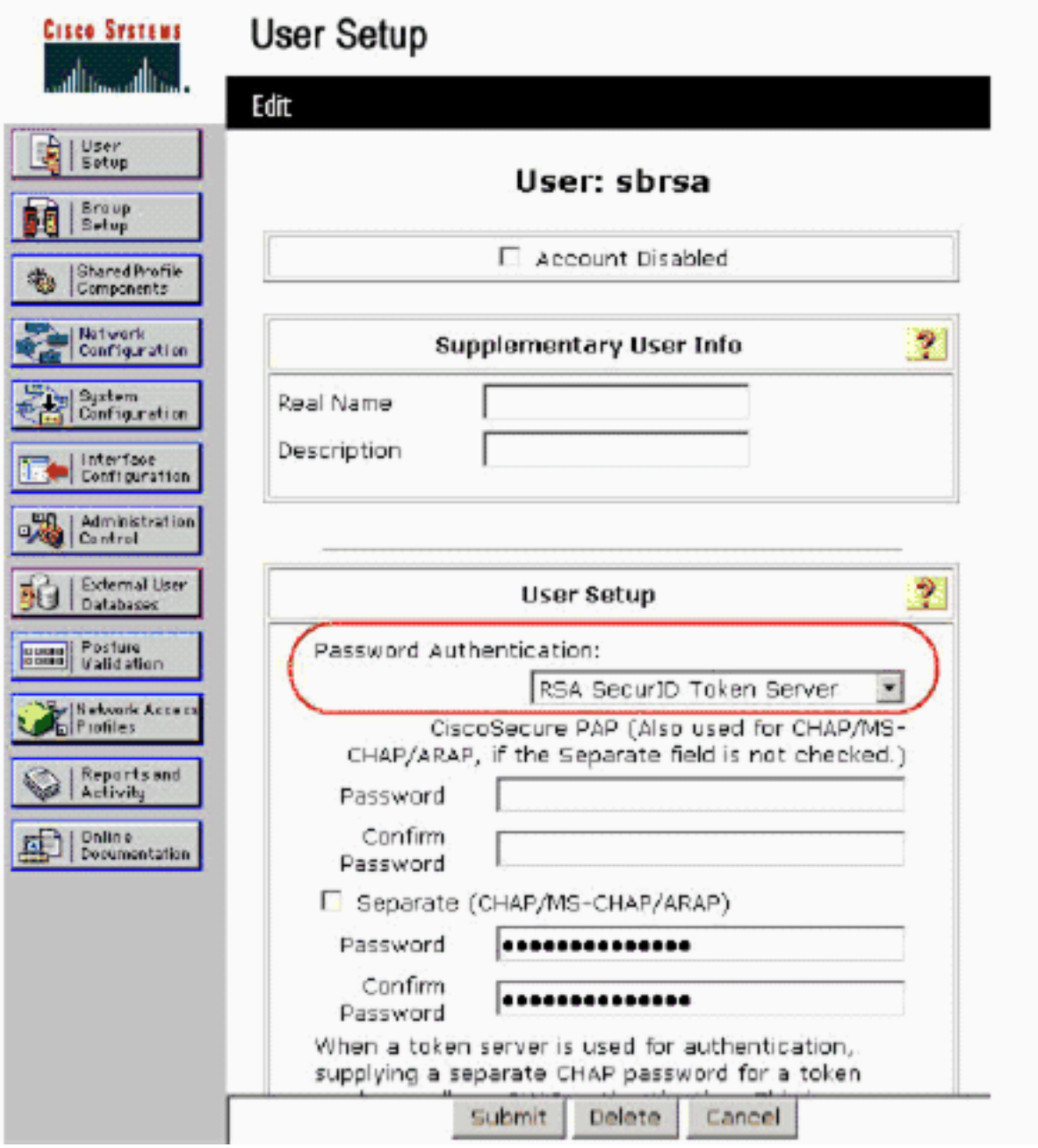


新增/配置特定使用者帳戶的RSA SecurID身份驗證

請完成以下步驟：

1. 從ACS主Admin GUI上按一下**User Setup**。輸入使用者名稱並按一下**Add**（或選擇要修改的現有使用者）。

2. 在User Setup > Password Authentication下，選擇**RSA SecurID Token Server**。然後，按一下**Submit**。

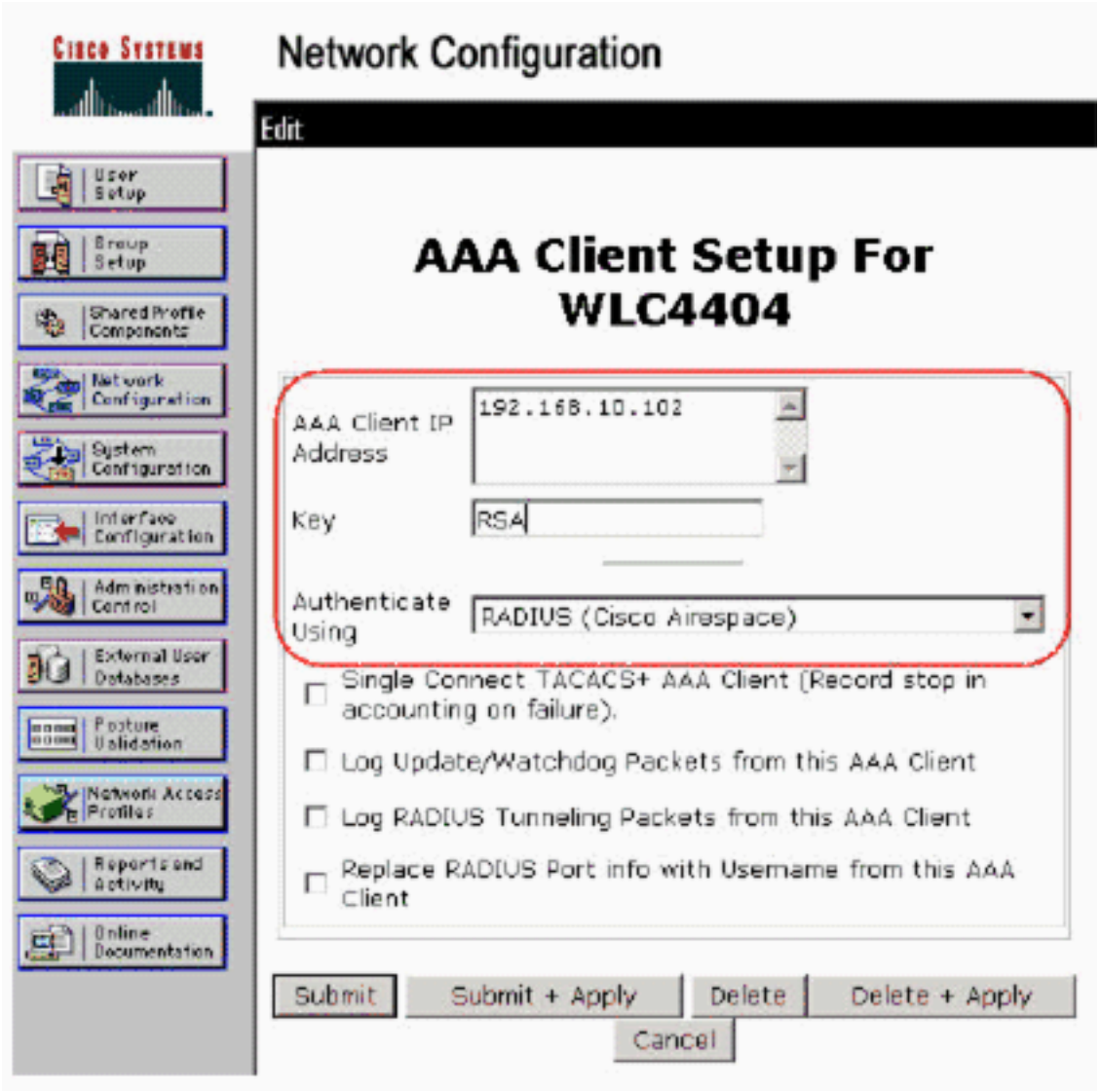


在Cisco ACS中新增RADIUS客戶端

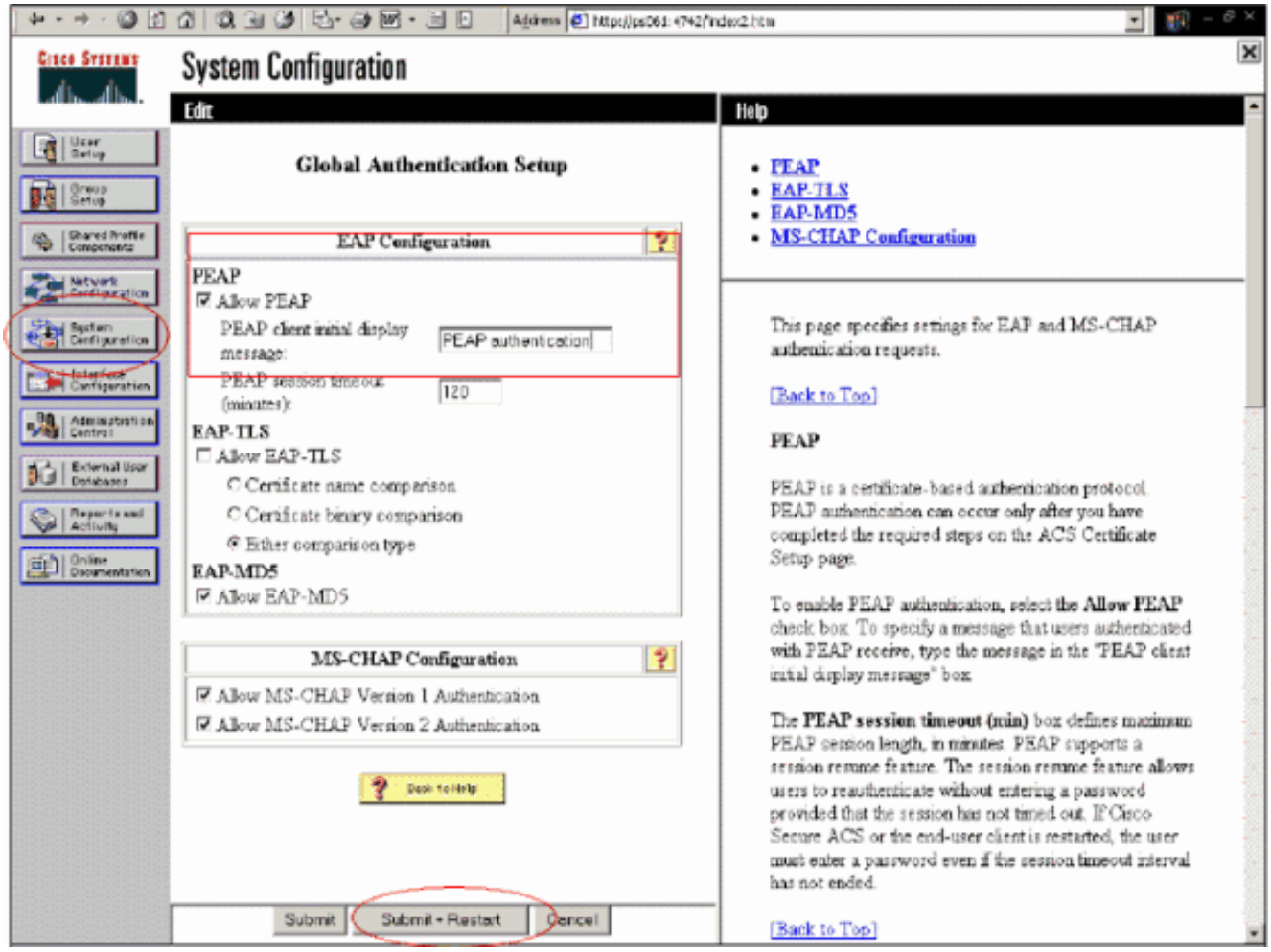
Cisco ACS伺服器安裝將需要WLC的IP地址來充當NAS，以便將客戶端PEAP身份驗證轉發到ACS。

請完成以下步驟：

1. 在**Network Configuration**下，為將要使用的WLC新增/編輯AAA使用者端。輸入在AAA客戶端和ACS之間使用的「共用金鑰」（WLC公用）。為此AAA客戶端選擇**Authenticate Using > RADIUS(Cisco Airespace)**。然後，按一下**Submit + Apply**。



2. 從已知的受信任證書頒發機構（如RSA Keon證書頒發機構）申請並安裝伺服器證書。有關此過程的詳細資訊，請參閱Cisco ACS附帶的文檔。如果您使用的是RSA Certificate Manager，則可以檢視《RSA Keon Aironet實施指南》以獲取其他幫助。您必須成功完成此任務才能繼續。**注意**：還可以使用自簽名證書。有關如何使用這些資訊，請參閱Cisco Secure ACS文檔。
3. 在**System Configuration > Global Authentication Setup**下，選中**Allow PEAP** authentication覈取方塊。



配置802.1x的Cisco無線LAN控制器配置

請完成以下步驟：

1. 連線到WLC的命令列介面以配置控制器，以便將其配置為連線到Cisco Secure ACS伺服器。
2. 從WLC輸入**config radius auth ip-address**命令以配置RADIUS伺服器進行身份驗證。**注意：**使用RSA Authentication Manager RADIUS伺服器進行測試時，輸入RSA Authentication Manager的RADIUS伺服器的IP地址。使用Cisco ACS伺服器進行測試時，請輸入Cisco Secure ACS伺服器的IP地址。
3. 從WLC輸入**config radius auth port**命令，以指定用於驗證的UDP連線埠。預設情況下，RSA Authentication Manager和Cisco ACS伺服器中的埠1645或1812均處於活動狀態。
4. 從WLC輸入**config radius auth secret**命令以設定WLC上的共用密碼。此金鑰必須與在RADIUS伺服器中為此RADIUS客戶端建立的共用金鑰匹配。
5. 從WLC輸入**config radius auth enable**命令以啟用驗證。如果需要，輸入**config radius auth disable**命令以停用驗證。請注意，預設情況下禁用身份驗證。
6. 在WLC為所需的WLAN選擇合適的第2層安全選項。
7. 使用**show radius auth statistics**和**show radius summary**命令驗證RADIUS設定是否正確配置。**注意：**EAP Request-timeout的預設計時器較低，可能需要修改。可以使用**config advanced eap request-timeout** <seconds>命令完成。它還有助於根據要求調整身份請求超時。可以使用**config advanced eap identity-request-timeout** <seconds>命令完成此操作。

802.11無線客戶端配置

有關如何配置無線硬體和客戶端請求方的詳細說明，請參閱各種思科文檔。

已知的問題

以下是RSA SecureID身份驗證的一些已知問題：

- RSA軟體令牌。在XP2上使用這種身份驗證形式時，不支援新的引腳模式和下一個令牌碼模式。(由ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip修復了)
- 如果您的ACS實施較舊或沒有上述修補程式，在使用者從「啟用；新PIN模式」轉換到「啟用」之前，客戶端將無法進行身份驗證。您可以通過讓使用者完成非無線身份驗證，或者使用「測試身份驗證」RSA應用程式來實現這一點。
- 拒絕4位數/字母數字PIN。如果處於「新PIN」模式的使用者違反PIN策略，則身份驗證過程會失敗，使用者不知道如何或原因。通常，如果使用者違反該策略，將向其傳送一條消息，指出該PIN被拒絕，並在再次向使用者顯示PIN策略時，再次提示該使用者（例如，如果PIN策略為5-7位，但使用者輸入4位）。

相關資訊

- 使用基於ACS的WLC進行動態VLAN分配到Active Directory組對映配置示例
- 使用WLC的無線LAN的客戶端VPN配置示例
- 無線LAN控制器上的驗證組態範例
- 使用無線LAN控制器和外部RADIUS伺服器的EAP-FAST身份驗證配置示例
- 通過SDM配置固定ISR上的無線身份驗證型別示例
- 固定ISR上的無線身份驗證型別配置示例
- 思科受保護的可擴充驗證通訊協定
- 使用RADIUS伺服器的EAP身份驗證
- 技術支援與文件 - Cisco Systems