使用ACS 5.1和Windows 2003 Server的UWN下的PEAP

目錄

簡介

本檔案介紹如何使用Wireless LAN controllers、Microsoft Windows 2003軟體和Cisco Secure

Access Control Server(ACS)5.1，透過使用Microsoft Challenge Handshake Authentication Protocol(MS-CHAP)版本2的受保護可擴充驗證通訊協定(PEAP)來設定安全無線存取。

注意：有關安全無線部署的資訊，請參閱Microsoft Wi-Fi網站和Cisco SAFE無線藍圖。

必要條件

需求

假設安裝程式瞭解基本的Windows 2003安裝和思科無線LAN控制器安裝，因為本文檔僅介紹便於測試的特定配置。

有關Cisco 5508系列控制器的初始安裝和配置資訊，請參閱Cisco 5500系列無線控制器安裝指南。有關Cisco 2100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 2100系列無線LAN控制器。

Microsoft Windows 2003安裝及設定指南可在安裝Windows Server 2003 R2 中找到。

開始之前，請在測試實驗室中的每台伺服器上安裝Microsoft Windows Server 2003 SP1作業系統並更新所有Service Pack。安裝控制器和輕量接入點(LAP)，並確保配置最新的軟體更新。

使用Windows Server 2003 SP1 Enterprise Edition，可以配置用於PEAP身份驗證的使用者和工作站證書的自動註冊。證書自動註冊和自動續訂使證書自動到期和續訂證書更易於部署證書並提高安全性。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行7.0.98.0的思科2106或5508系列控制器
- Cisco 1142輕量型存取點通訊協定(LWAPP)AP
- 安裝了Internet Information Server(IIS)、證書頒發機構(CA)、DHCP和域名系統(DNS)的Windows 2003 Enterprise
- 思科1121安全存取控制系統裝置(ACS)5.1
- Windows XP Professional，帶SP（和更新的服務包）和無線網路介面卡(NIC)（支援CCX v3）或第三方請求方。
- Cisco 3750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

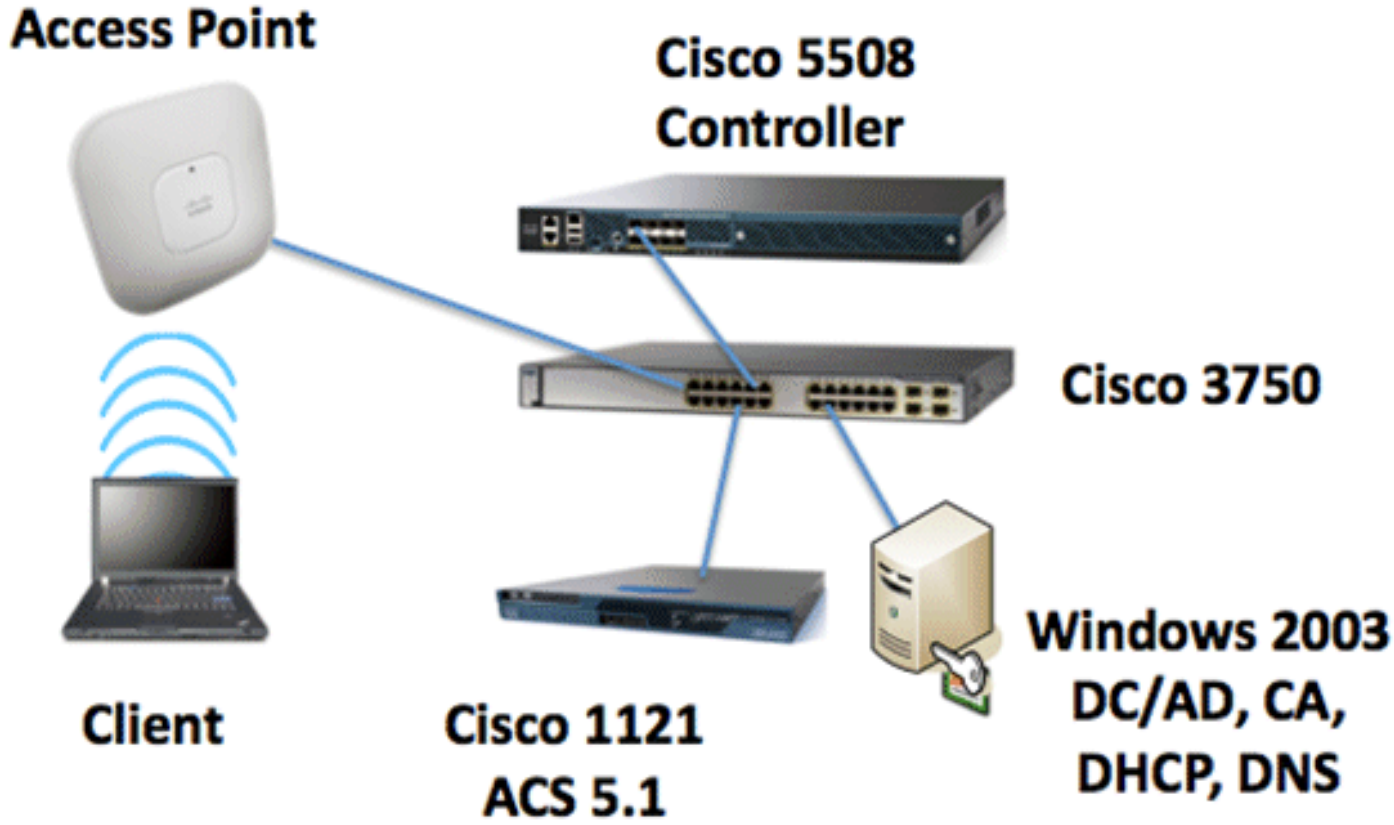
本節提供用於設定本文件中所述功能的資訊。

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

本檔案會使用以下網路設定：

思科安全無線實驗室拓撲



本文檔的主要目的是提供在Unified Wireless Networks with ACS 5.1和Windows 2003 Enterprise Server下實施PEAP的逐步過程。主要強調的是客戶端的自動註冊，以便客戶端自動註冊並從伺服器獲取證書。

註：要將帶有臨時金鑰完整性協定(TKIP)/高級加密標準(AES)的 Wi-Fi保護訪問(WPA)/WPA2新增到Windows XP Professional with SP中，請參閱Windows XP Service Pack 2 的WPA2/無線調配服務資訊元素(WPS IE)更新。

Windows Enterprise 2003安裝程式，帶IIS、證書頒發機構、DNS、DHCP(CA)

CA(democa)

CA是運行Windows Server 2003 SP2企業版並執行以下角色的電腦：

- 運行IIS的**demo.local**域的域控制器
- 用於**demo**.**local** DNS**域的DNS**伺服器
- DHCP伺服器
- **demo**.local域的**企業根**CA

執行以下步驟，為這些服務配置CA:

1. 執行基本安裝和配置。
2. 將電腦配置為域控制器。
3. 提升域功能級別。
4. 安裝和配置DHCP。
5. 安裝證書服務。
6. 驗證證書的管理員許可權。
7. 向域中新增電腦。
8. 允許對電腦進行無線訪問。
9. 向域中新增使用者。
10. 允許對使用者進行無線訪問。
11. 向域中新增組。
12. 將使用者新增到wirelessusers組。
13. 將客戶端電腦新增到無線使用者組。

執行基本安裝和配置

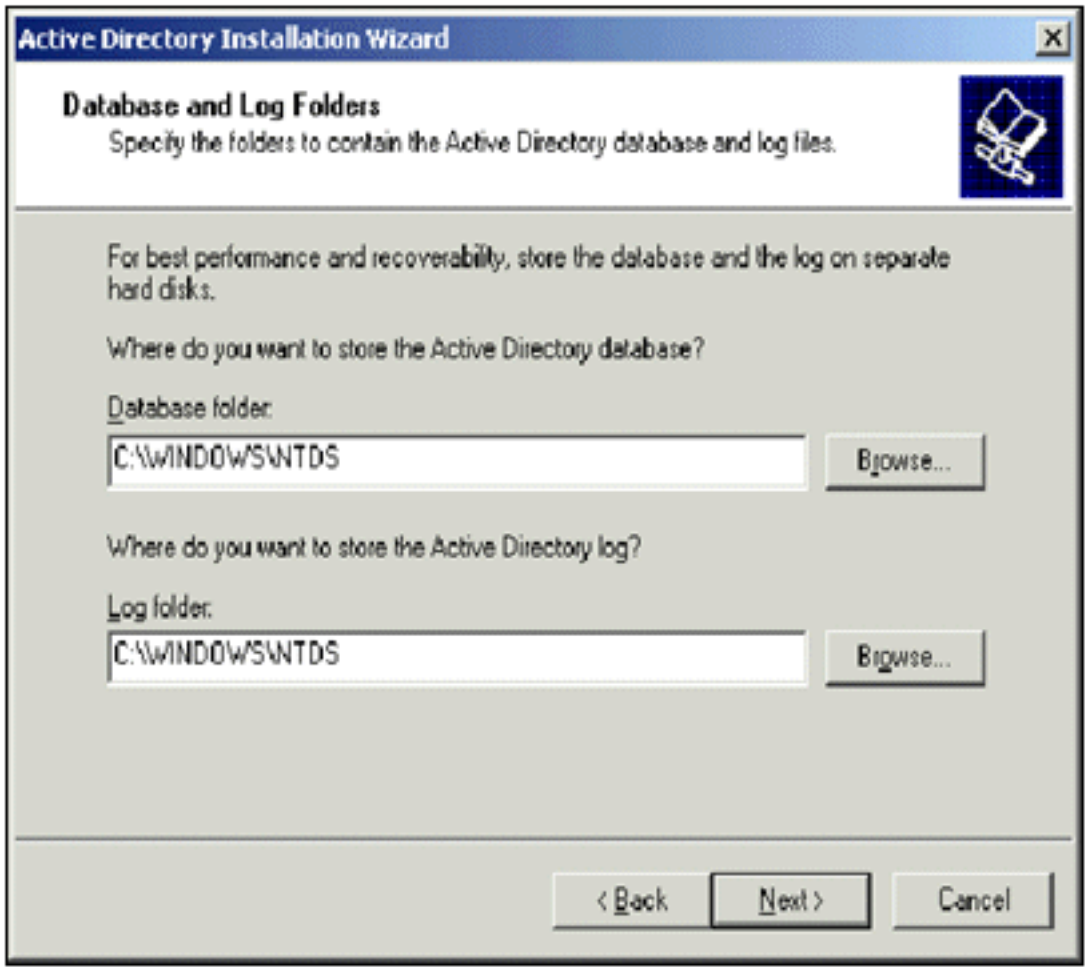
執行以下步驟：

1. 安裝Windows Server 2003 SP2 Enterprise Edition作為獨立的伺服器。
2. 使用IP地址*10.0.10.10*和子網掩碼*255.255.255.0*配置TCP/*IP協定*。

將電腦配置為域控制器

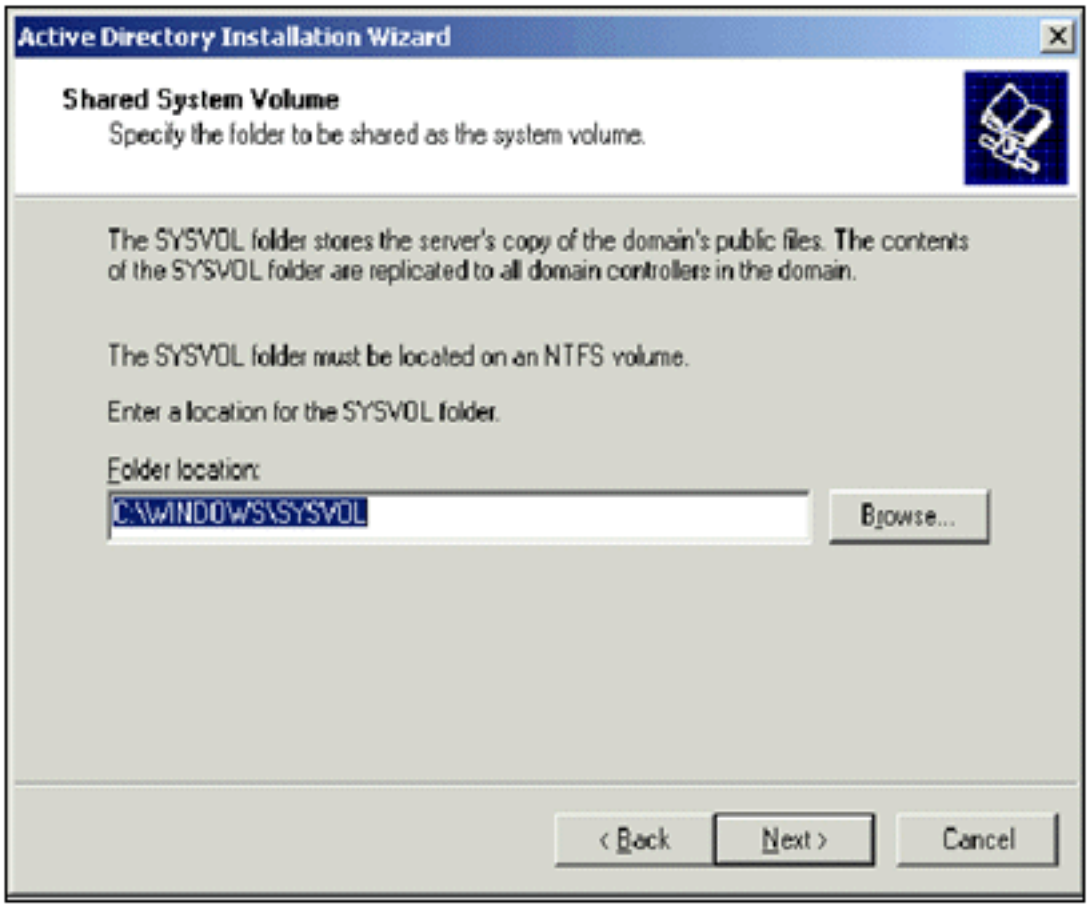
執行以下步驟：

1. 要啟動Active Directory安裝嚮導，請選擇**開始 > 運行**，然後鍵入dcpromo.exe，然後按一下**確定**。
2. 在「歡迎使用Active Directory安裝嚮導」頁面上，按一下**下一步**。
3. 在「Operating System Compatibility（作業系統相容性）」頁面上，按一下**Next**。
4. 在「域控制器型別」頁上，為新**的域選擇域控制器，然**後按一下**下一步**。
5. 在「建立新域」頁上，選擇新**林中的域，然後單**擊「下一**步**」。
6. 在「安裝或配置DNS」頁面上，選擇「**否**」，**僅在此電腦上安裝並配置DNS，然後**按一下「**下一步**」。
7. 在「新建域名」頁上，鍵入**demo.local**，然後按一下**下一步**。
8. 在「NetBIOS域名」頁上，輸入域NetBIOS名稱作為**demo**，然後按一下**下一步**。
9. 在「資料庫和日誌資料夾位置」頁中，接受預設的「資料庫和日誌資料夾」目錄，然後按一下

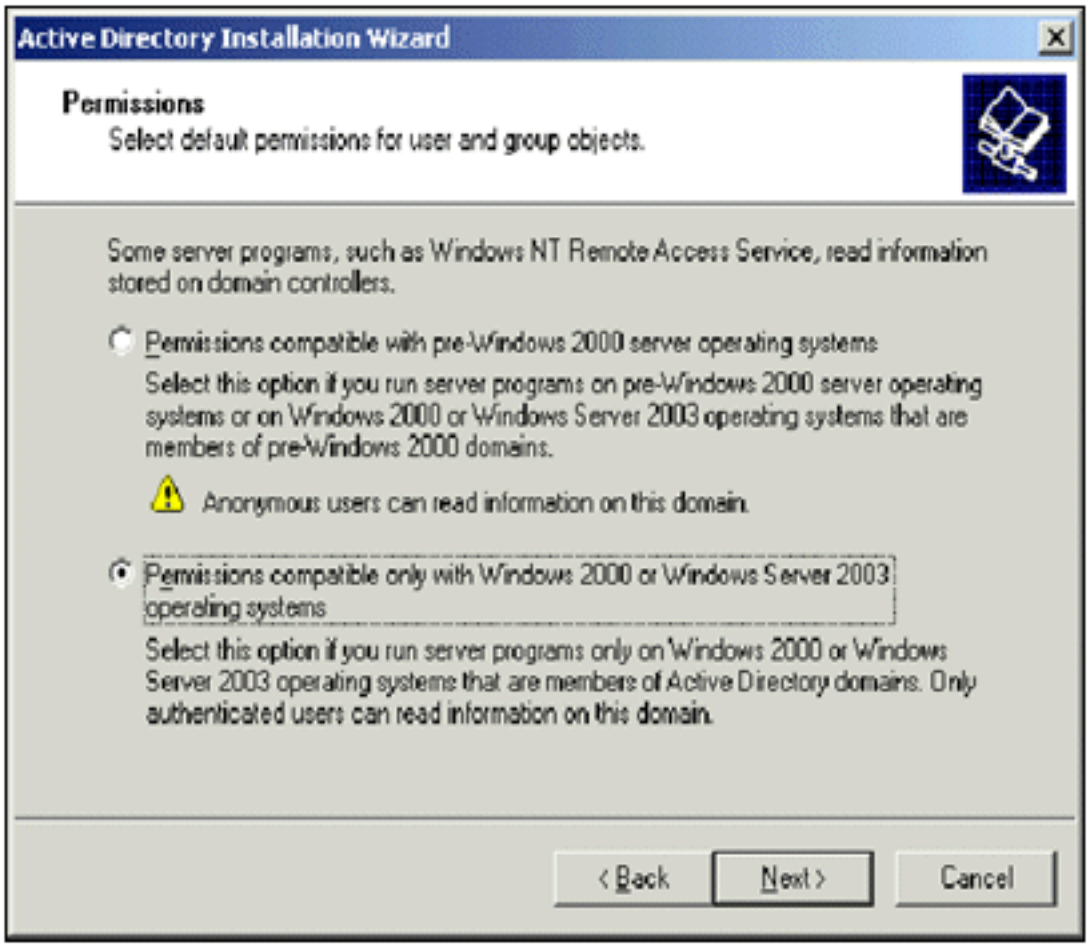


下一步。

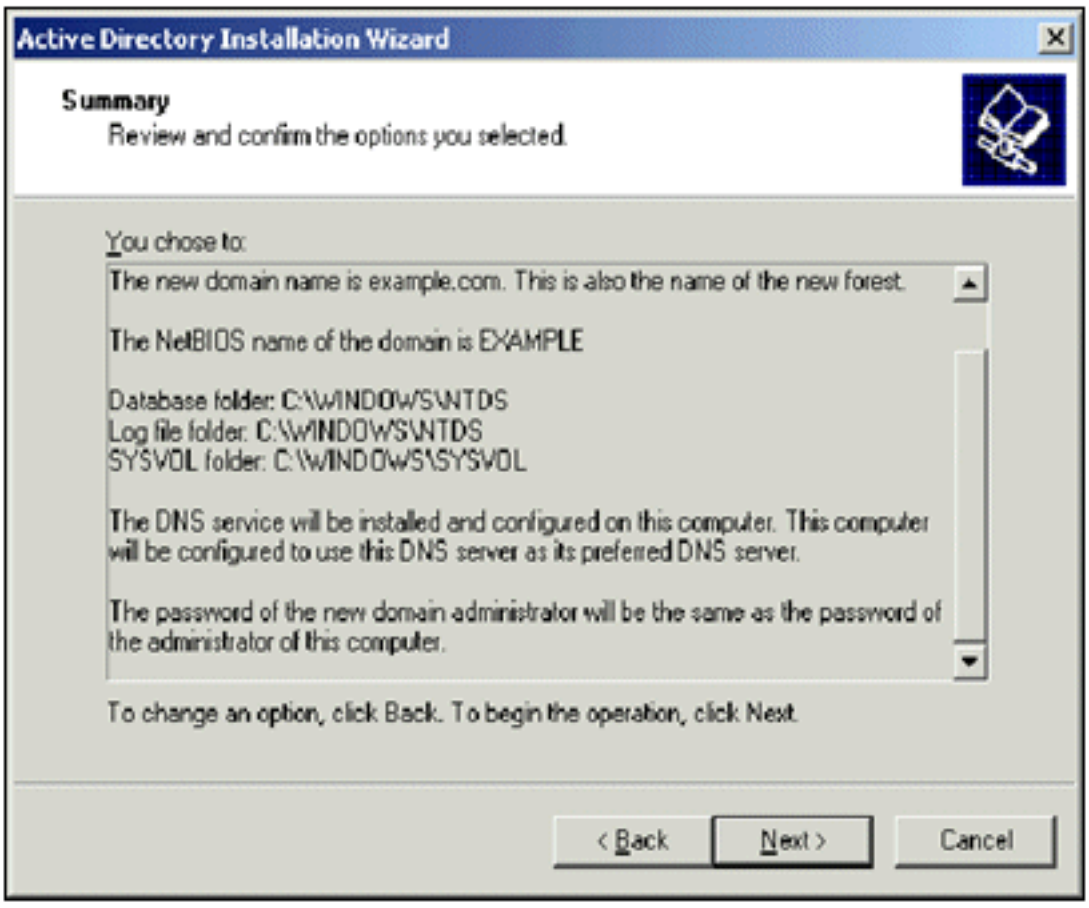
10. 在「共用系統卷」頁中，驗證預設資料夾位置是否正確，然後按一下**下一步**。



11. 在「許可權」頁面上，驗證是**否已選擇僅與Windows 2000或Windows Server 2003作業系統相容的許可權**，然後按一下「下一步」。



12. 在「目錄服務：恢復模式管理密碼」頁面上，將密碼框留空，然後按一下**下一步**。
13. 檢視「摘要」頁上的資訊，然後按一下**下一步**。

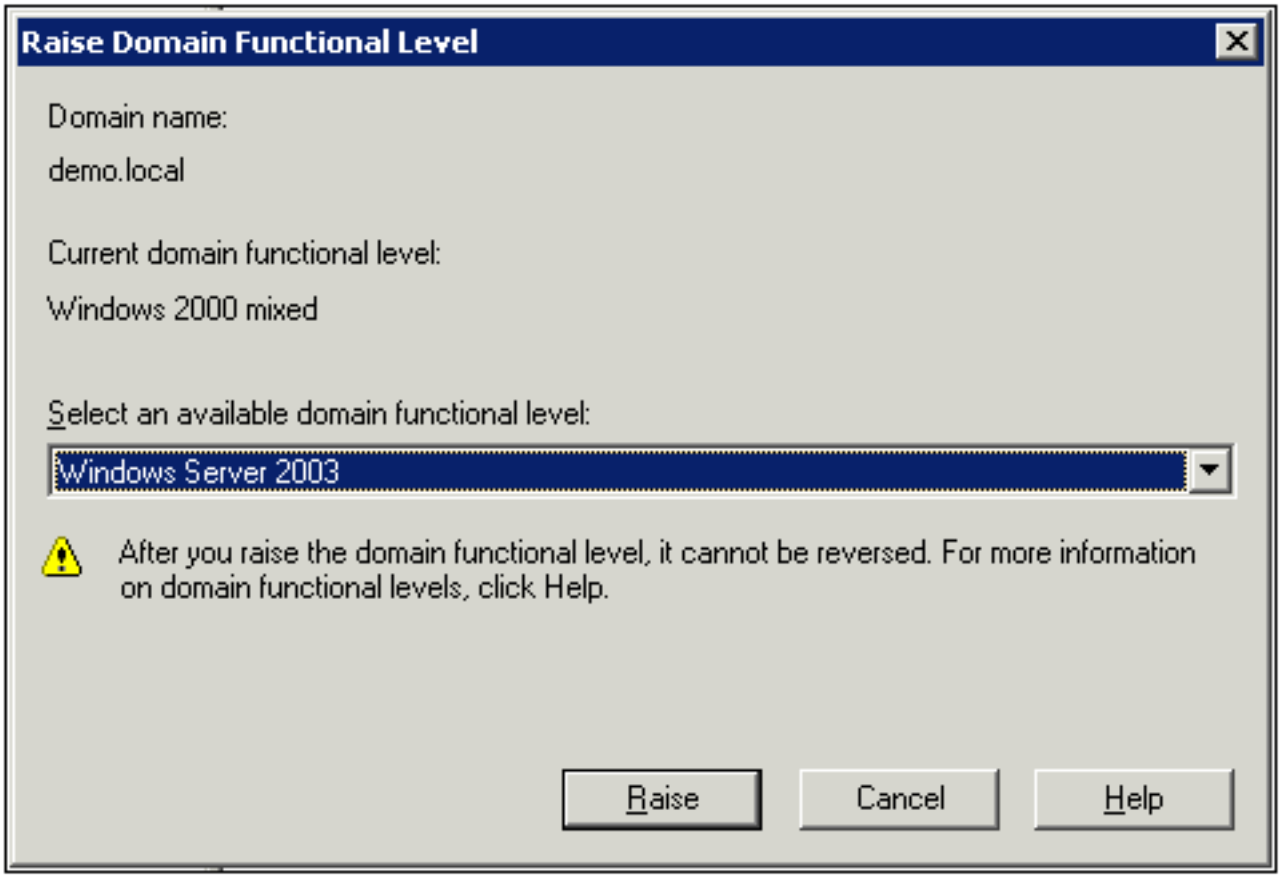


14. 完成Active Directory安裝後，按一下**Finish**。
15. 當系統提示重新啟動電腦時，按一下**Restart Now**。

提升域功能級別

執行以下步驟：

1. 從Administrative Tools（管理工具）資料夾(「開始」(Start)>「程式」(Programs)>「管理工具」(Administrative Tools)>「**Active Directory域和信任」(Active Directory Domains and Trusts**)，開啟Active Directory域和信任管理單元，然後按一下右鍵域電腦**CA.demo.local**。
2. 按一下**Raise Domain Functional Level**，然後在**Raise Domain Functional Level**頁上選擇**Windows Server 2003。**

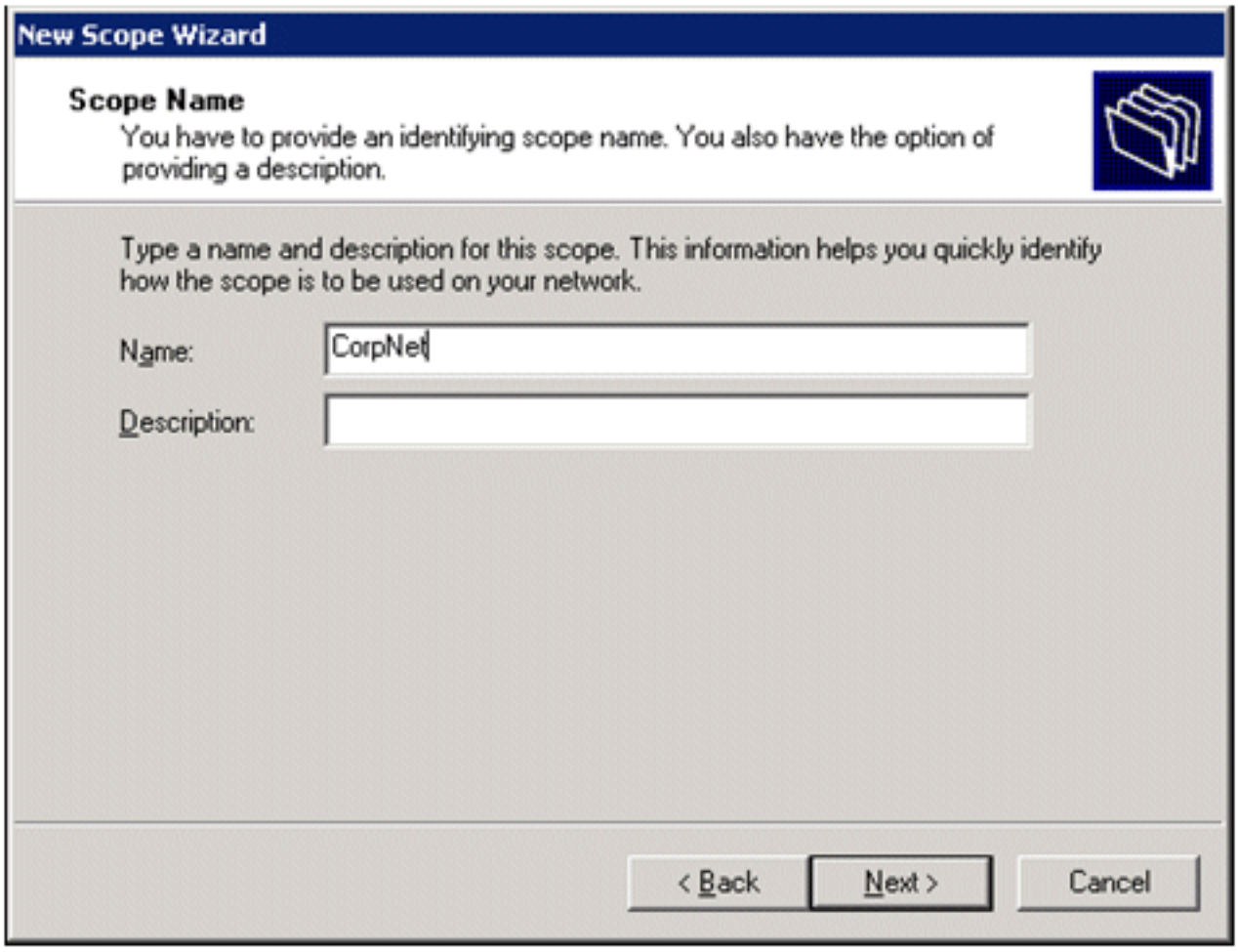


3. 按一下「**Raise**」，按一下「**OK**」，然後再次按一下「**OK**」。

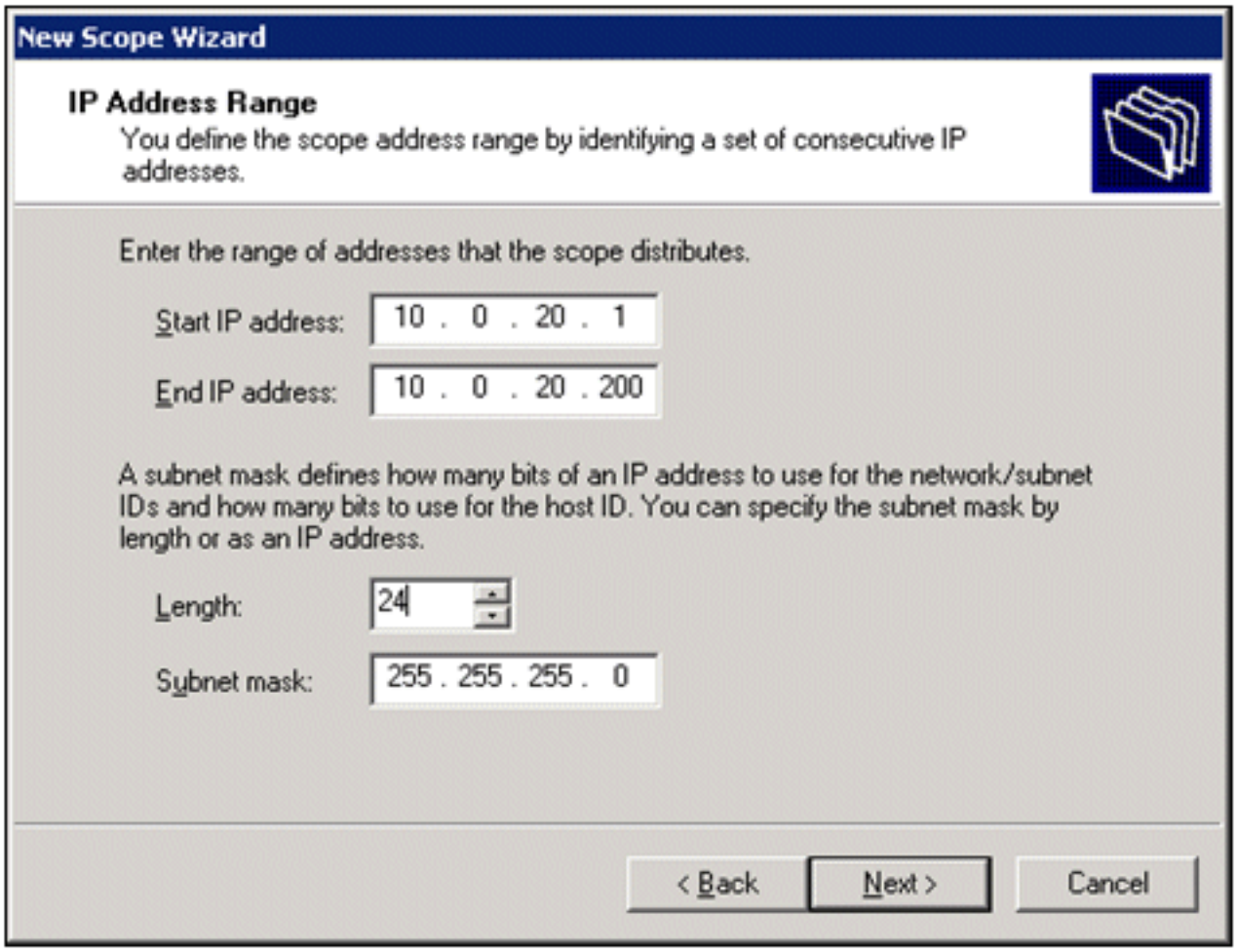
安裝和配置DHCP

執行以下步驟：

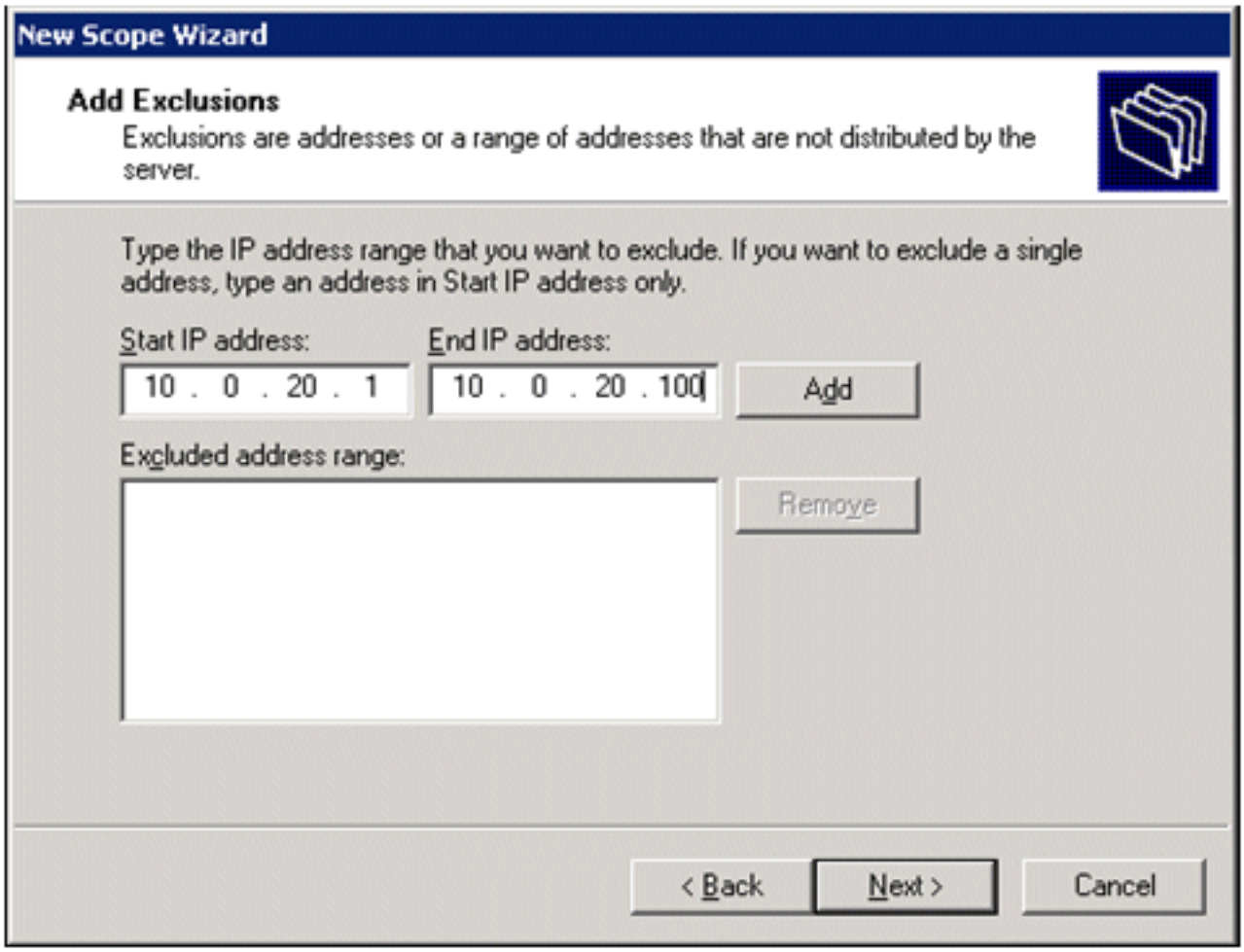
1. 使用「控制面板」中的**新增或刪除程式**，安裝**動態主機配置協定(DHCP)**作為**網路服務元件。**
2. 從Administrative Tools文件夾(「開始」>「程式」>「管理工具」>「**DHCP**」)開啟DHCP管理單元，然後選中DHCP伺服器CA.demo.local。
3. 按一下**Action**，然後按一下**Authorize**以授權DHCP服務。
4. 在控制檯樹中，按一下右鍵**CA.demo.local**，然後按一下**New Scope**。
5. 在「新建作用域」嚮導的「歡迎」頁上，按一下**下一步**。
6. 在「範圍名稱」頁面的「名稱」欄位中鍵入**CorpNet**。



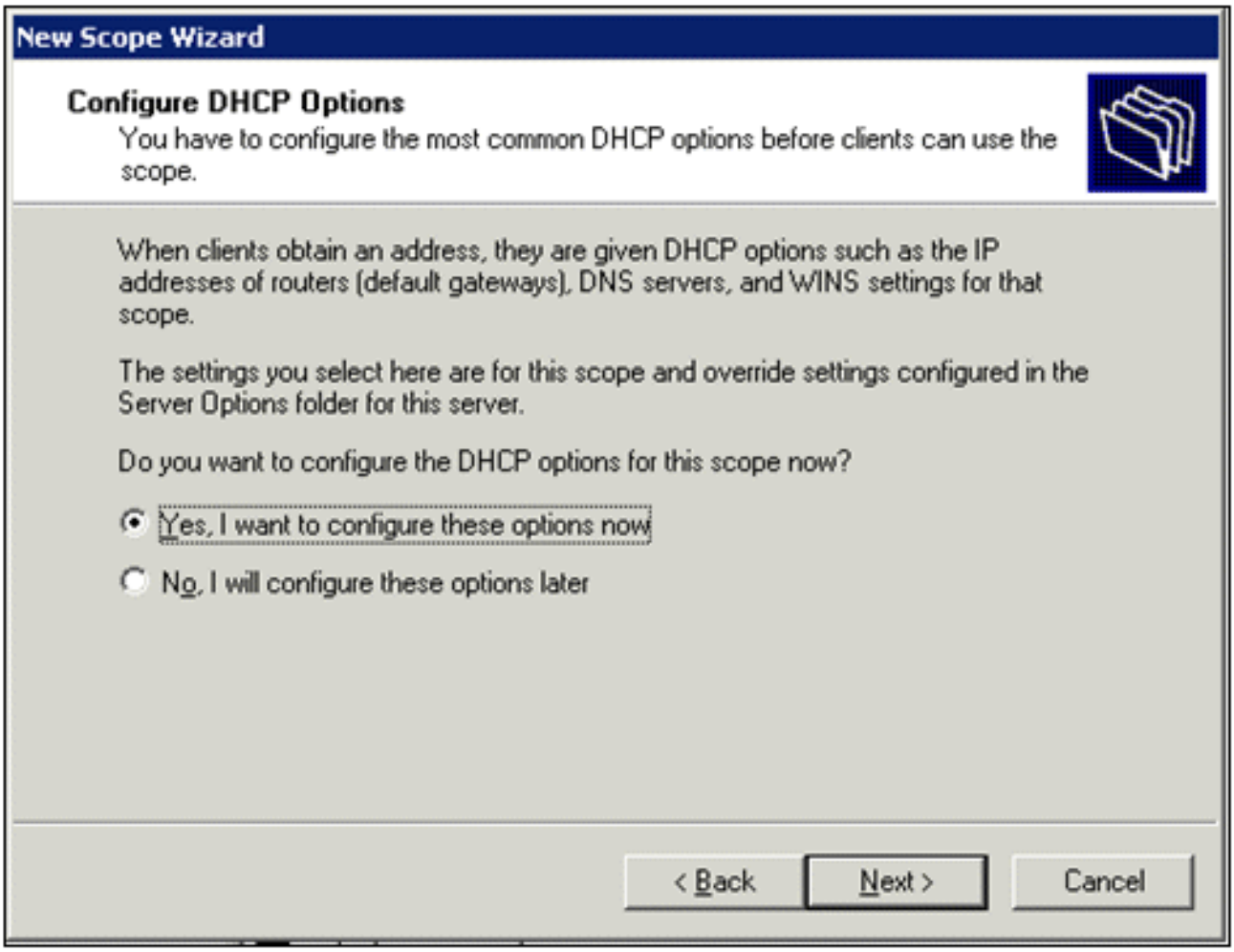
7. 按一下**Next**並填寫以下引數：起始IP地址- 10.0.20.1結束IP地址- 10.0.20.200長度 — 24子網掩碼-
   255.255.255.0



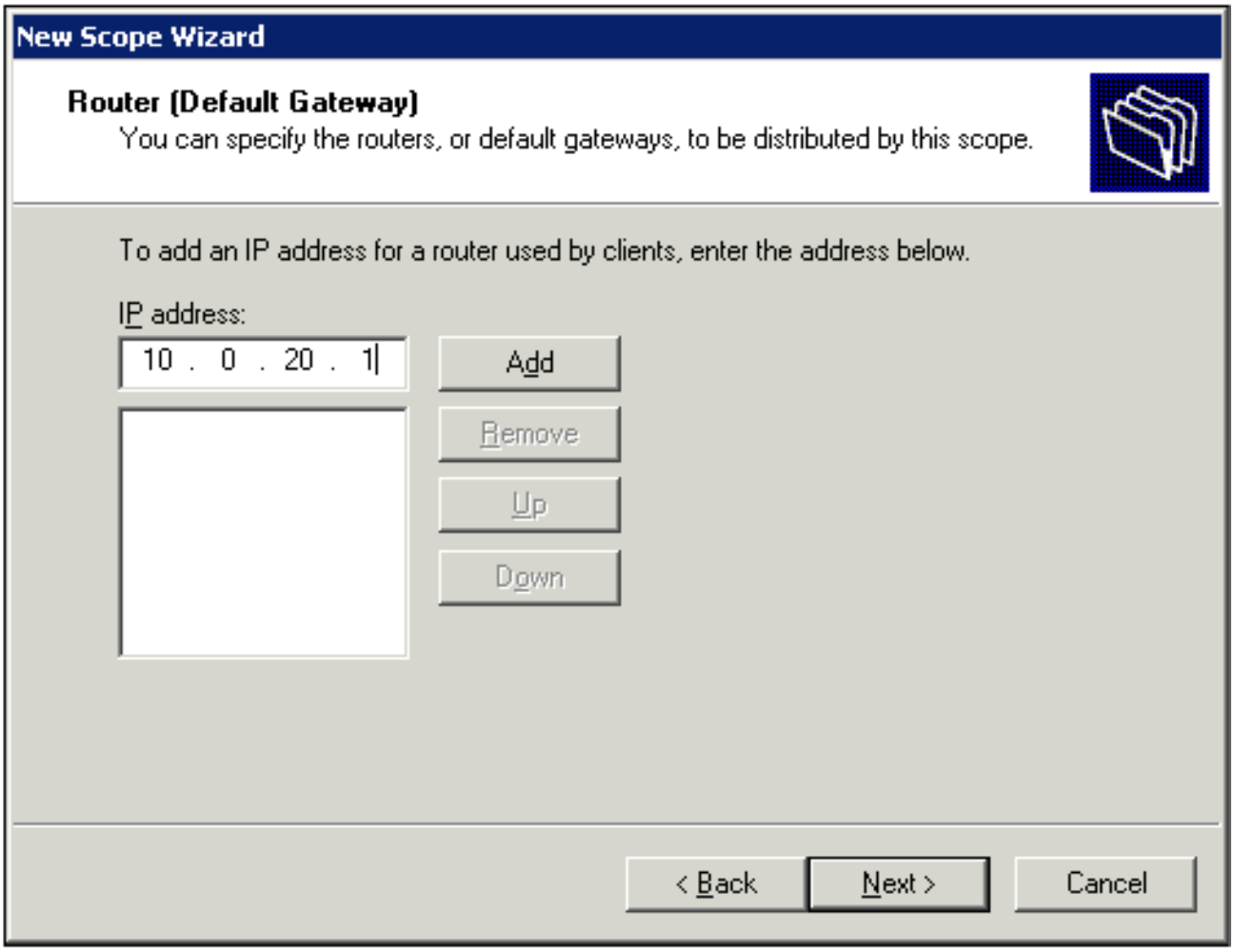
8. 按一下**Next**，輸入*10.0.20.1*作為起始IP地址，輸入*10.0.20.100*作為要排除的結束IP地址。然後點選**下一步**。這樣會保留從10.0.20.1到10.0.20.100範圍內的IP地址。DHCP伺服器不分配這些保留IP地址。



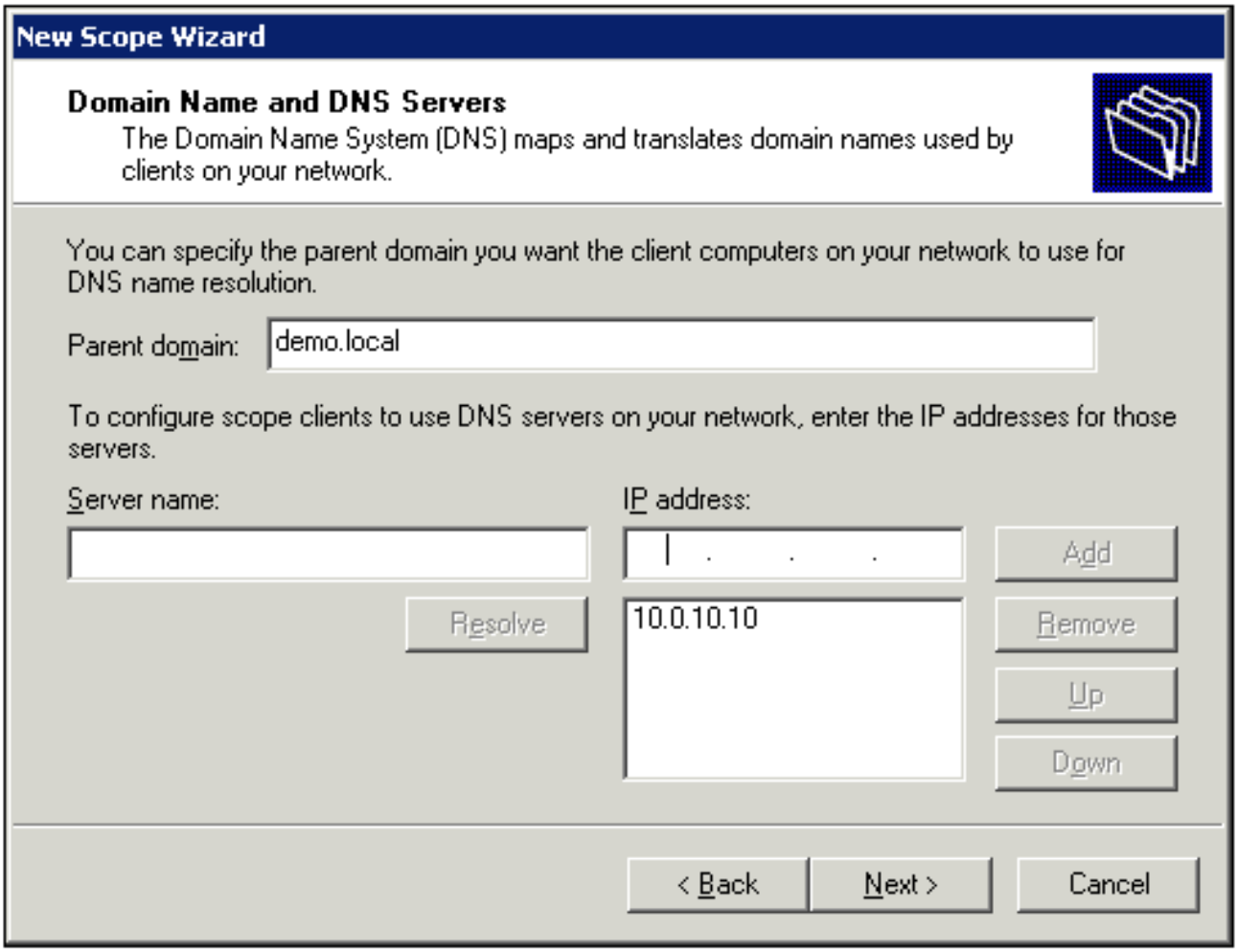
9. 在Lease Duration頁面上，按一下**Next**。
10. 在Configure DHCP Options頁上，選擇**Yes， I want to configure these options now，然後單擊Next**。



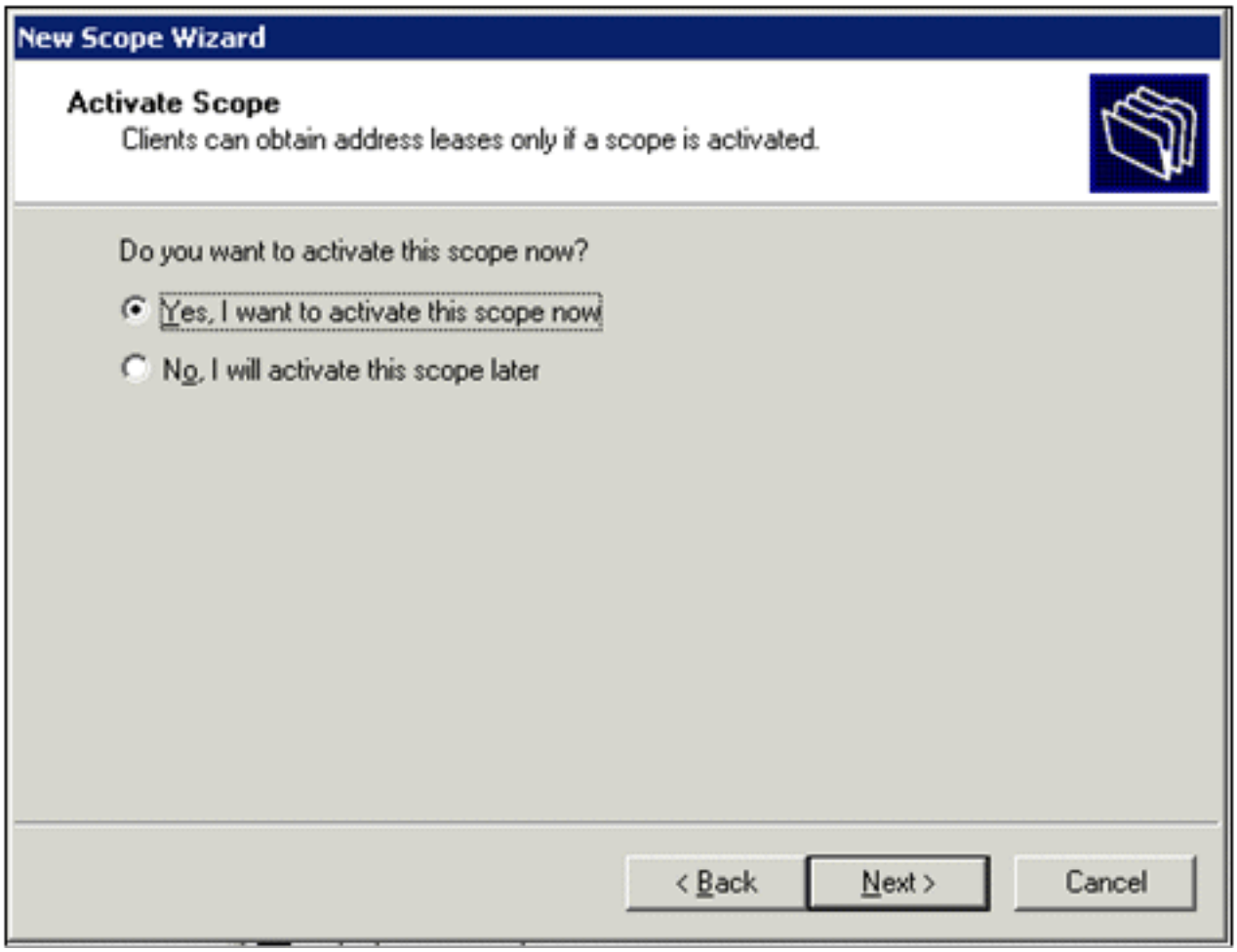
11. 在Router(Default Gateway)頁面上，新增預設路由器地址*10.0.20.1*，然後按一下**Next**。



12. 在「域名和DNS伺服器」頁面的「父域」欄位中鍵入*demo.local*，在「IP地址」欄位中鍵入*10.0.10.10*，然後按一下**Add**並按一下*Next*。



13. 在「WINS伺服器」頁上，按一下**下一步**。
14. 在「啟用作用域」頁上，選擇**「是，我想立即啟用此作用域」，然**後按一下「**下一步**」。



15. 完成「新建作用域嚮導」頁後，按一下**完成**。

安裝證書服務

執行以下步驟：

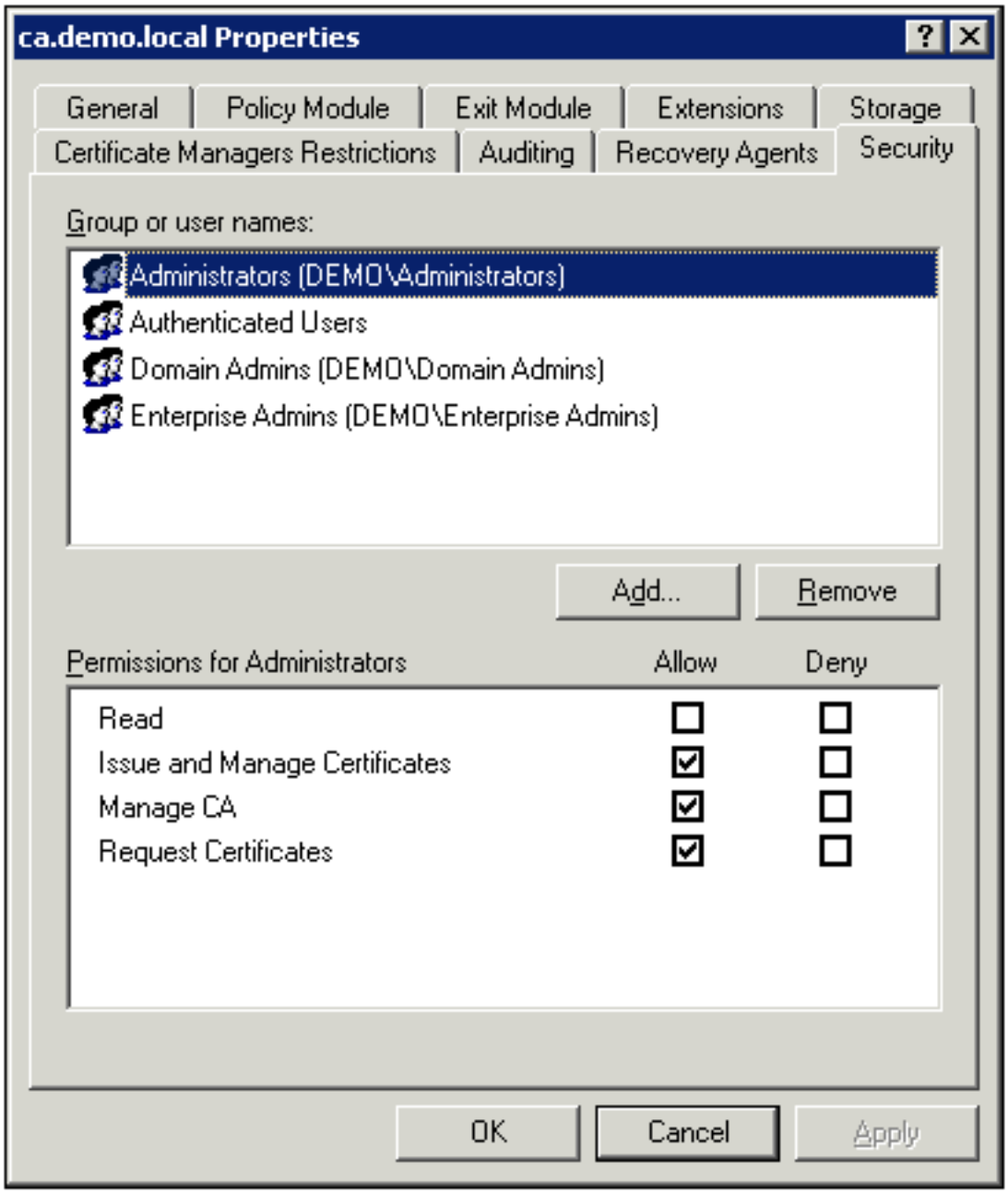
注意：在安裝證書服務之前必須安裝IIS，並且使用者應該是Enterprise Admin OU的一部分。

1. 在「控制面板」中，開啟**新增或刪除程式**，然後按一下**新增/刪除Windows元件**。
2. 在「Windows元件嚮導」頁中，選擇「證書服務」，然後按一下「下一步」。
3. 在「CA型別」頁上，選擇企業根CA並按一下下一步。
4. 在「CA標識資訊」頁的「此CA的公用名」框中鍵入*democa*。您還可以輸入其他可選詳細資訊。然後按一下**Next**，接受「Certificate Database Settings」頁面上的預設值。
5. 按「**Next**」（下一步）。安裝完成後，按一下**Finish**。
6. 閱讀有關安裝IIS的警告消息後，按一下**OK**。

驗證證書的管理員許可權

執行以下步驟：

1. 選擇**開始 > 管理工具 > 證書頒發機構**。
2. 按一下右鍵**democa CA**，然後按一下**Properties**。
3. 在「安全」頁籤上，按一下「組」或「使用者名稱」清單中的**Administrators**。
4. 在「管理員的許可權」清單中，驗證這些選項是否設定為**Allow**:頒發和管理證書管理CA請求證書如果其中任何一項設定為「拒絕」或未選中，則將許可權設定為**Allow**。



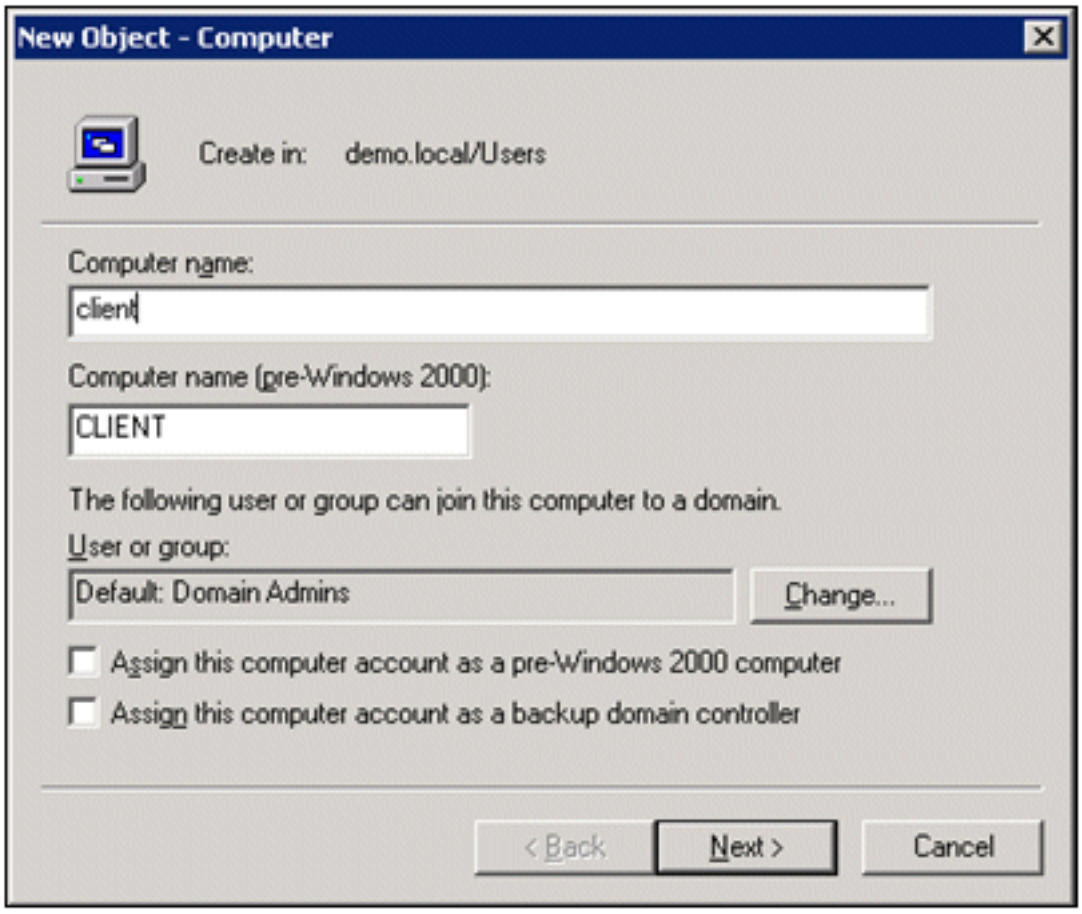
5. 按一下**OK**關閉democa CA Properties對話方塊，然後關閉Certification Authority。

將電腦新增到域

執行以下步驟：

注意：如果電腦已新增到域中，請繼續執行向域中新增使用者操作。

1. 開啟**Active Directory使用者和計**算機管理單元。
2. 在控制檯樹中，展開**demo.local**。
3. 按一下右鍵「**Computers**」，按一下「**New**」，然後按一下「**Computer**」。
4. 在「新建對象 — 電腦」對話方塊中，在「電腦名稱」欄位中鍵入電腦名稱，然後按一下**下一步**。此示例使用電腦名*Client*。

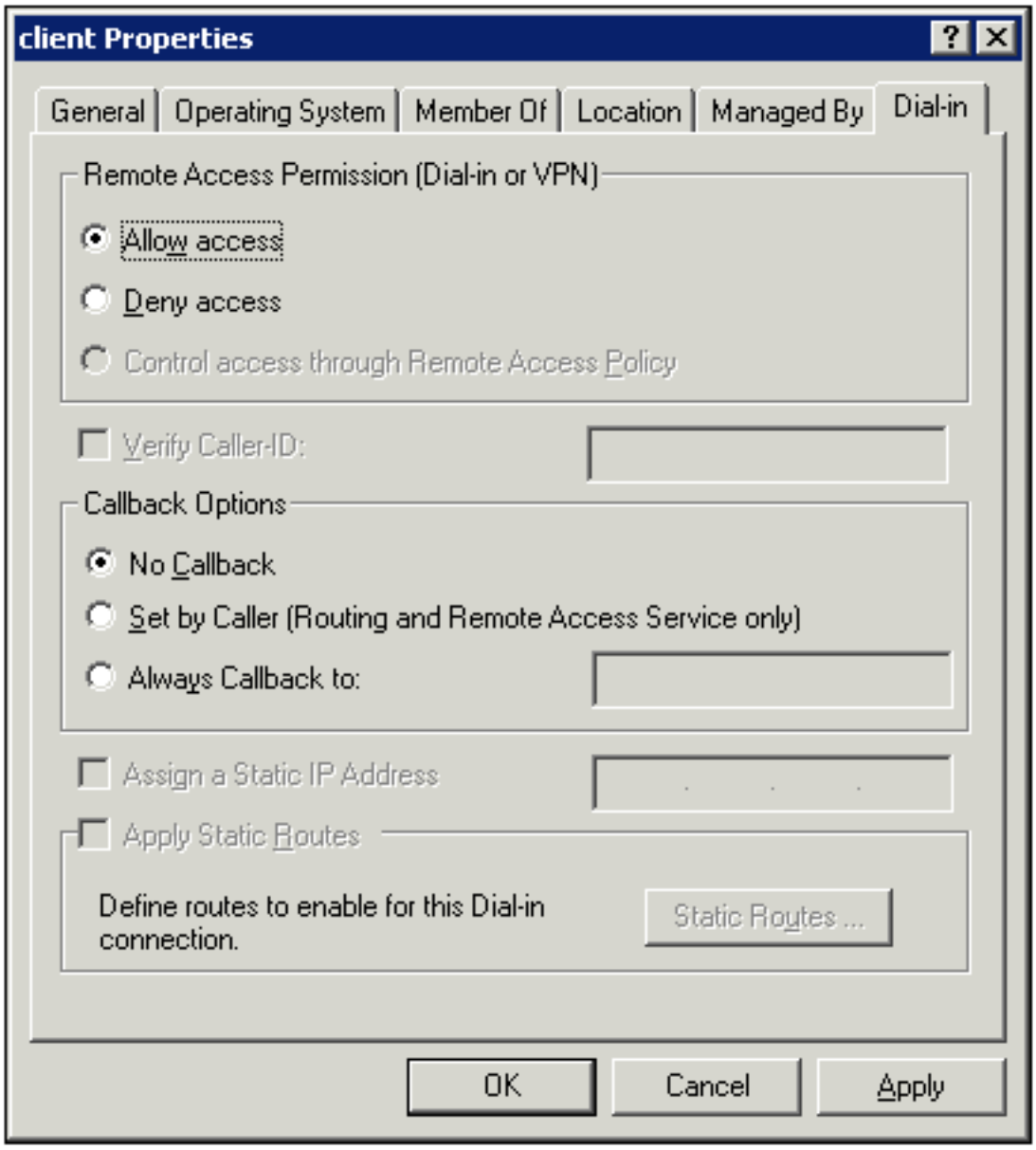


5. 在「託管」對話方塊中，按一下**下一步**。
6. 在「新建對象 — 電腦」對話方塊中，按一下**完成**。
7. 重複步驟3至6以建立其他電腦帳戶。

允許對電腦進行無線訪問

執行以下步驟：

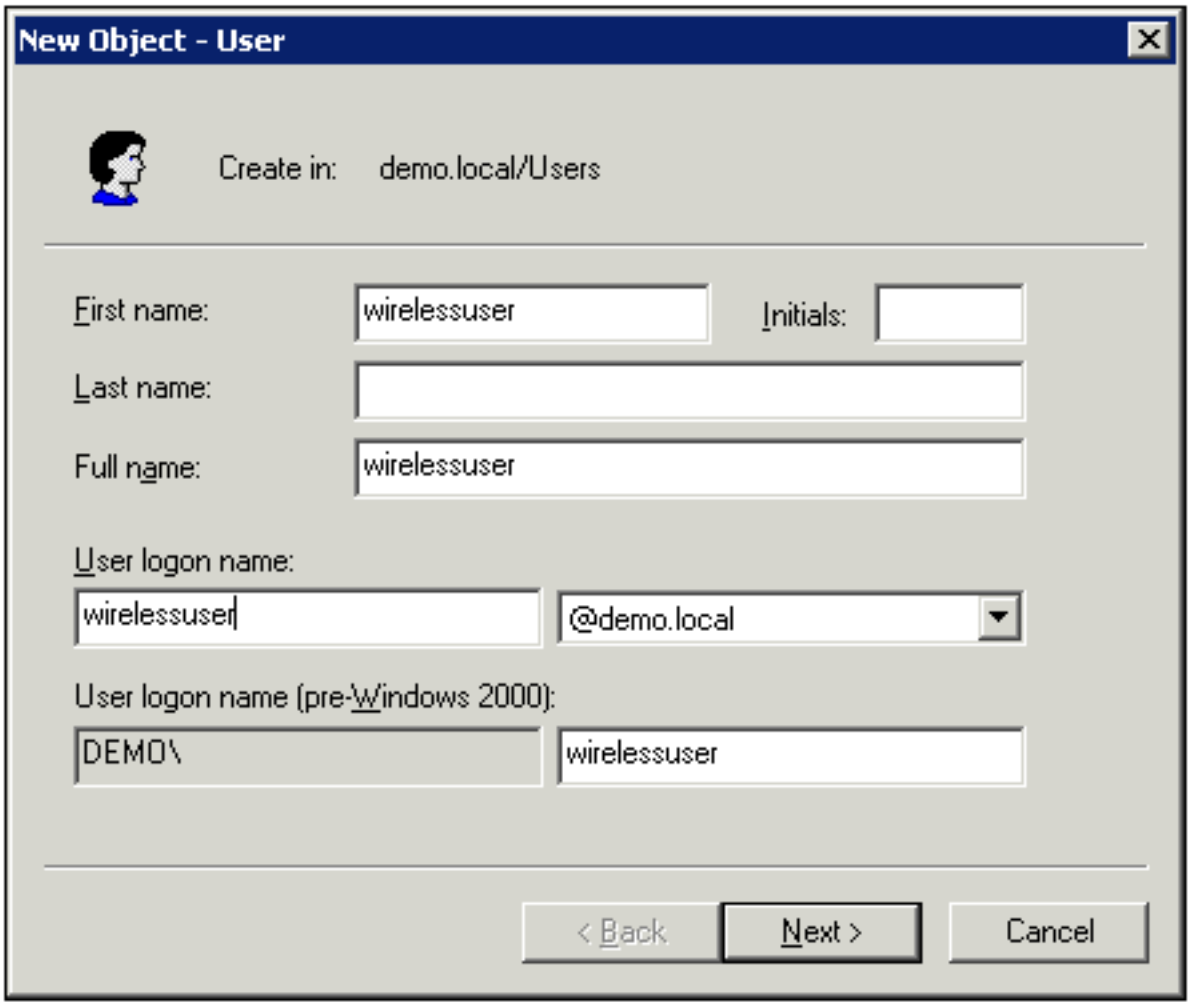
1. 在Active Directory使用者和電腦控制檯樹中，按一下**Computers**資料夾，然後按一下右鍵要為其分配無線訪問許可權的電腦。此範例顯示您在步驟7中新增的**computer Client**程式。按一下**Properties**，然後轉到**Dial-in**頁籤。
2. 在「Remote Access Permission」中，選擇**Allow access**，然後按一下**OK**。



向域中新增使用者

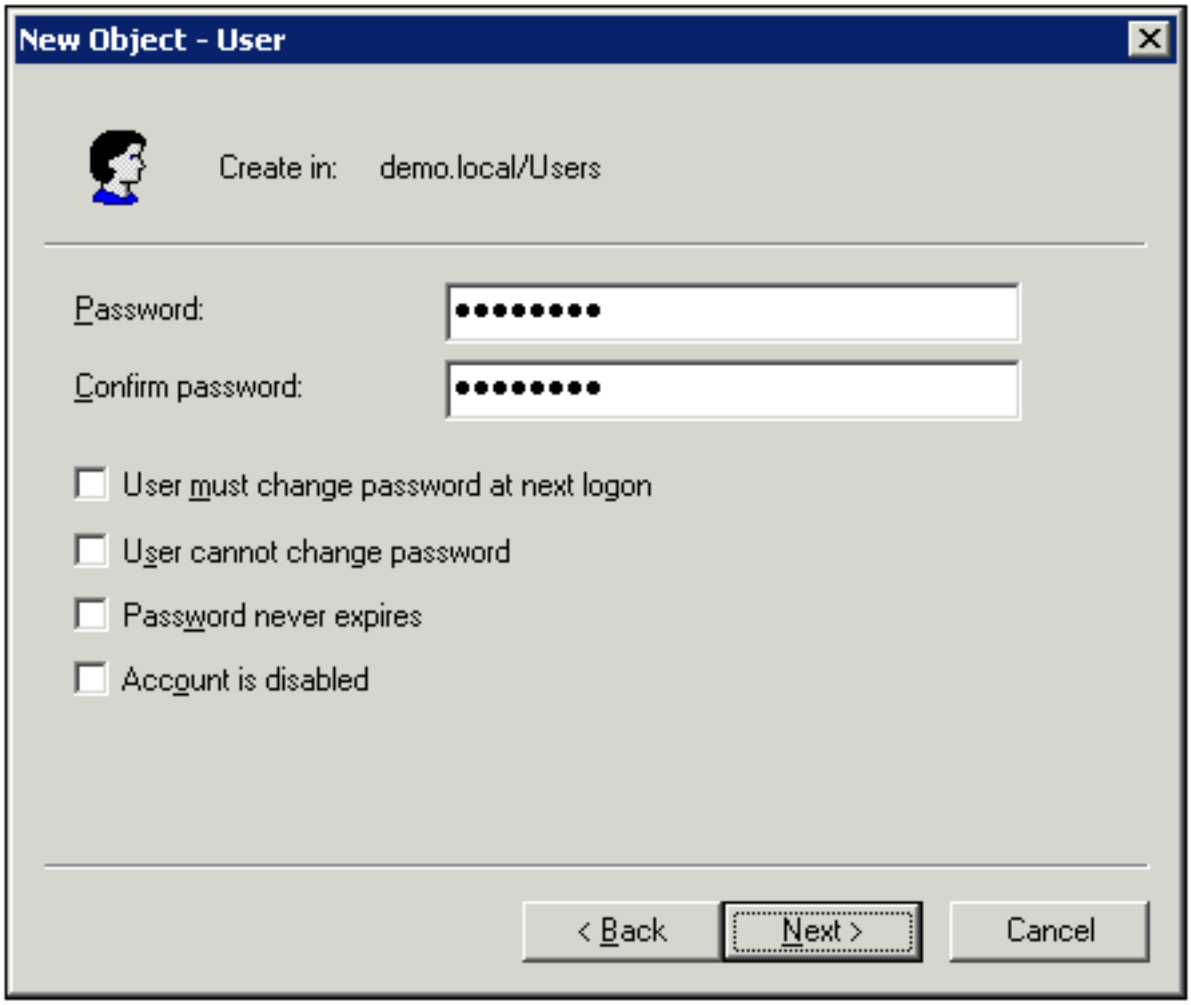
執行以下步驟：

1. 在「Active Directory使用者和電腦」控制檯樹中，按一下右鍵**使用者**，按一下**新建**，然後按一下**使用者**。
2. 在「新建對象 — 使用者」對話方塊中，鍵入無線使用者的名稱。此示例在First name欄位中使用名稱*wirelessuser*，在User logon name欄位中使用名稱*wirelessuser*。按「**Next**」（下一



步）。

3. 在「新建對象 — 使用者」對話方塊中，在「密碼」和「確認密碼」欄位中鍵入您選擇的密碼。清除「**User must change password at next logon(使用者下次登入時必須更改密碼)」覈取方塊，然後按一下「Next**（下一步）」。

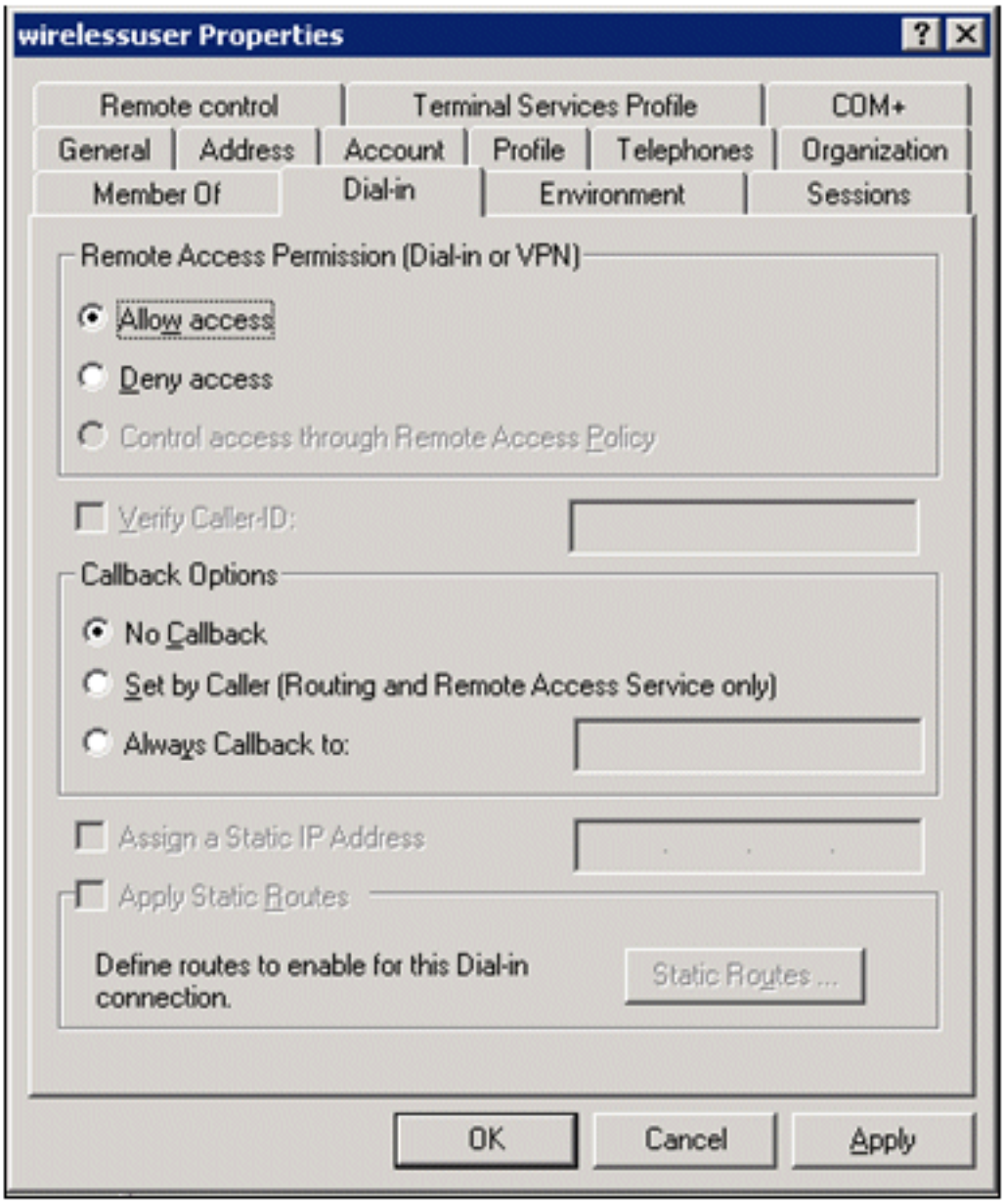


4. 在「新建對象 — 使用者」對話方塊中，按一下**完成**。
5. 重複步驟2至4以建立其他使用者帳戶。

允許對使用者進行無線訪問

執行以下步驟：

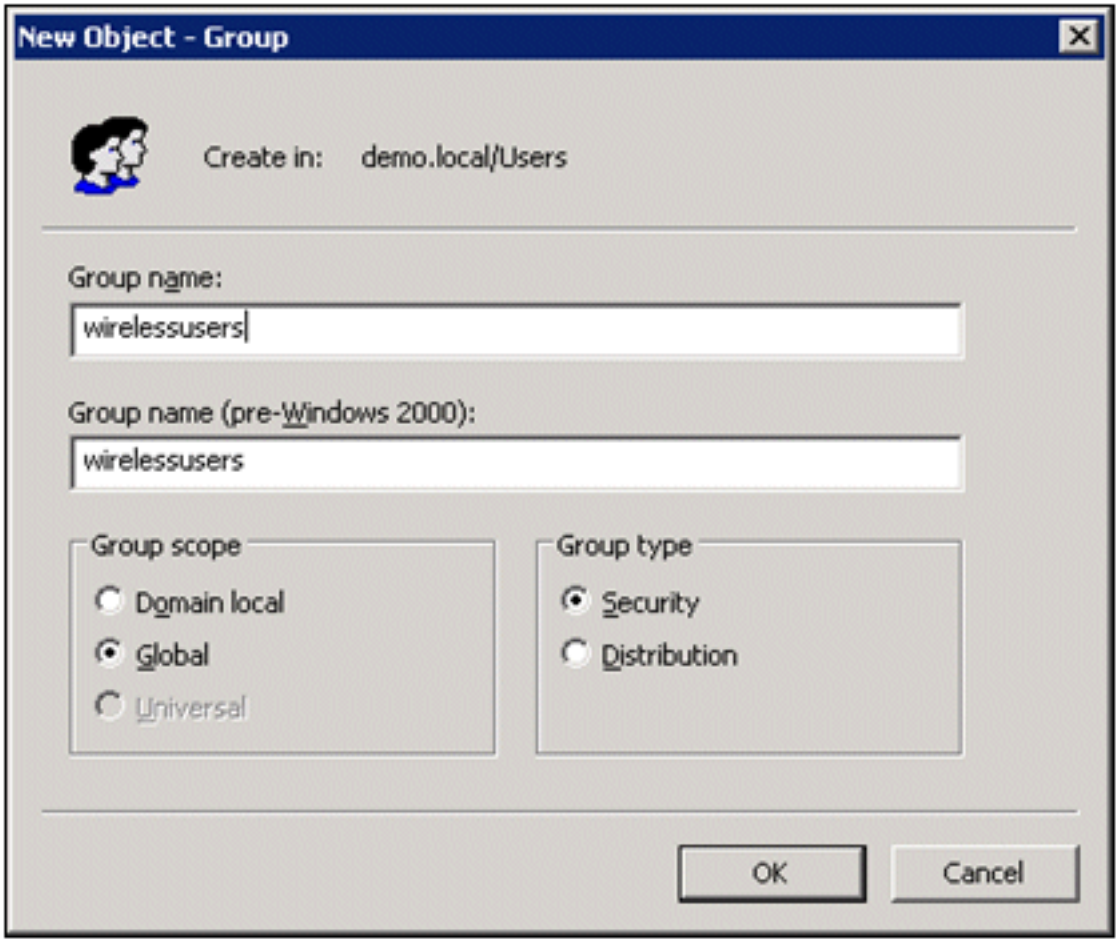
1. 在Active Directory使用者和電腦控制檯樹中，按一下**Users**資料夾，按一下右鍵**wirelessuser**，按一下**Properties**，然後轉到**Dial-in**頁籤。
2. 在「Remote Access Permission」中，選擇**Allow access**，然後按一下**OK**。



向域中新增組

執行以下步驟：

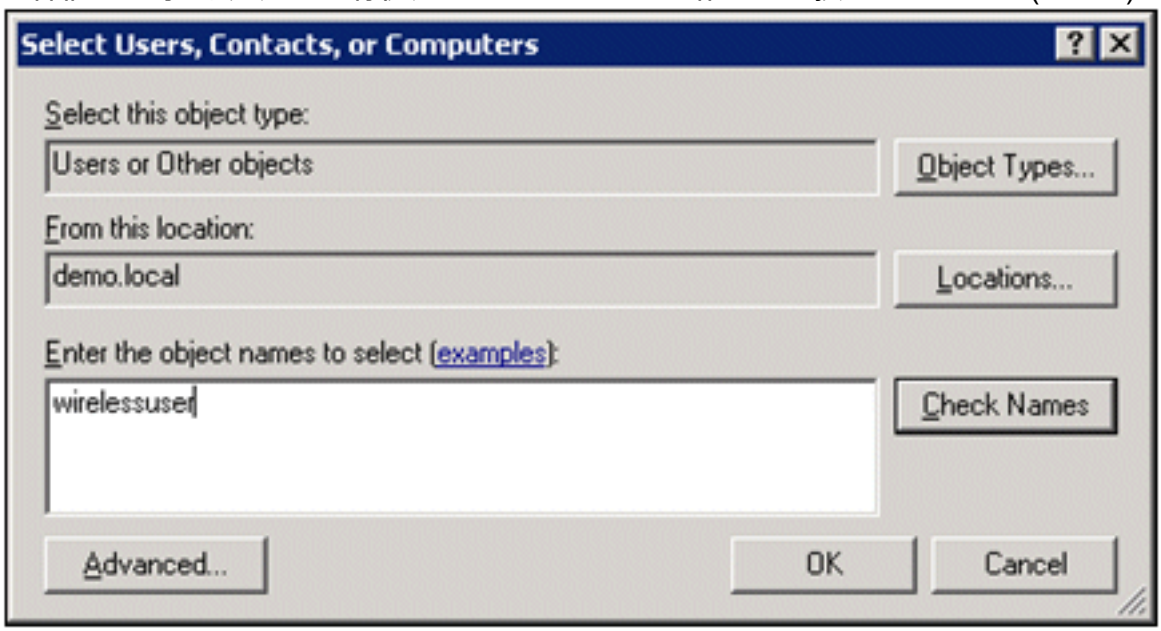
1. 在Active Directory使用者和電腦控制檯樹中，按一下右鍵**Users**，按一下**New**，然後按一下**Group**。
2. 在「新建對象 — 組」(New Object - Group)對話方塊中，在「組名稱」(Group name)欄位中鍵入組的名稱，然後按一下**確定**。本文檔使用組名*wirelessusers*。



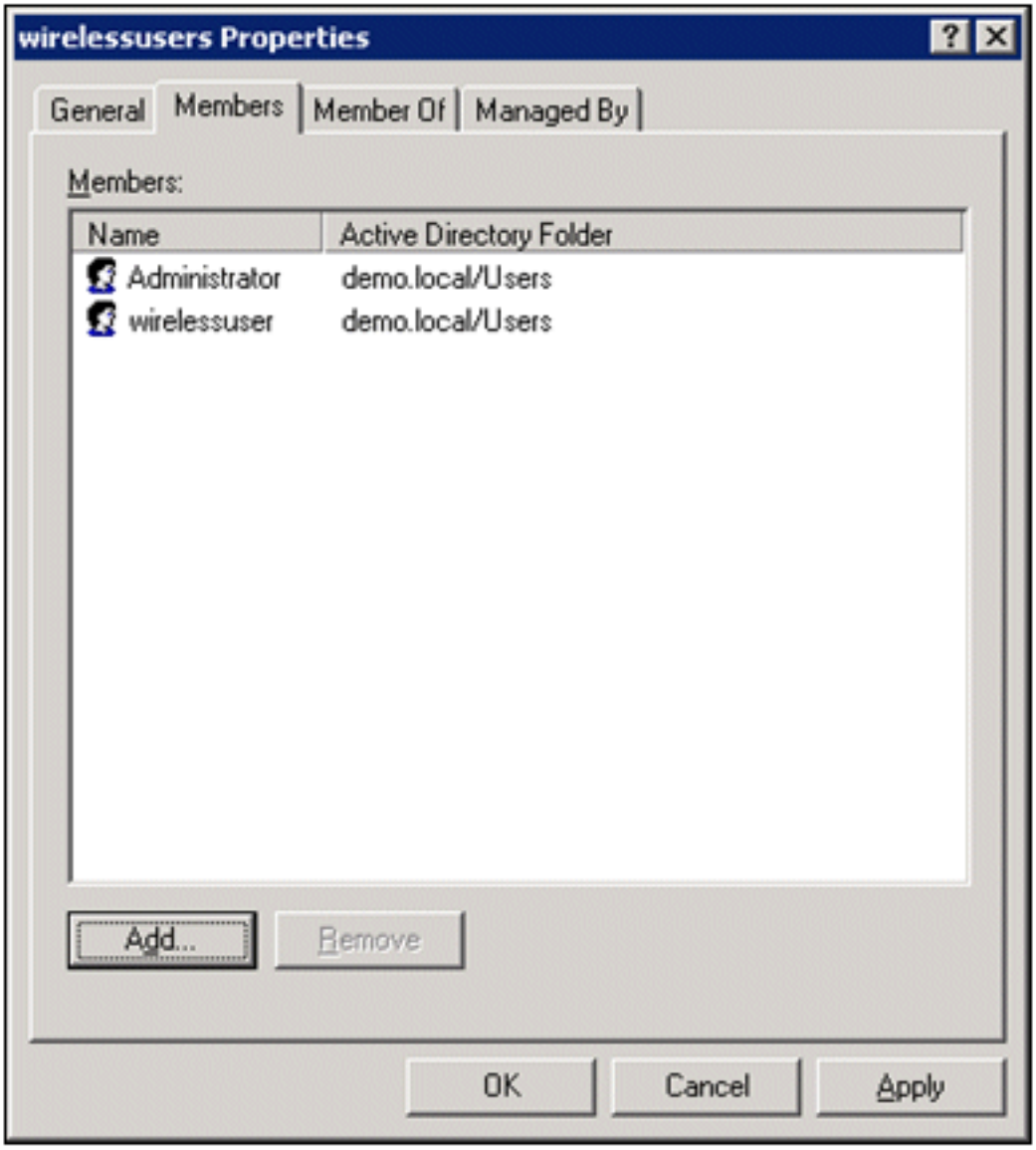
將使用者新增到無線使用者組

執行以下步驟：

1. 在Active Directory使用者和電腦的詳細資訊窗格中，按兩下組*WirelessUsers*。
2. 轉到「成員」頁籤，然後按一下**新增**。
3. 在「選擇使用者」、「聯絡人」、「電腦」或「組」對話方塊中，鍵入要新增到組中的使用者的名稱。此示例說明如何將使用者*wirelessuser*新增到組。按一下「**OK**」（確定）。



4. 在「找到多個名稱」對話方塊中，按一下**確定**。wirelessusers使用者帳戶將新增到wirelessusers組中。

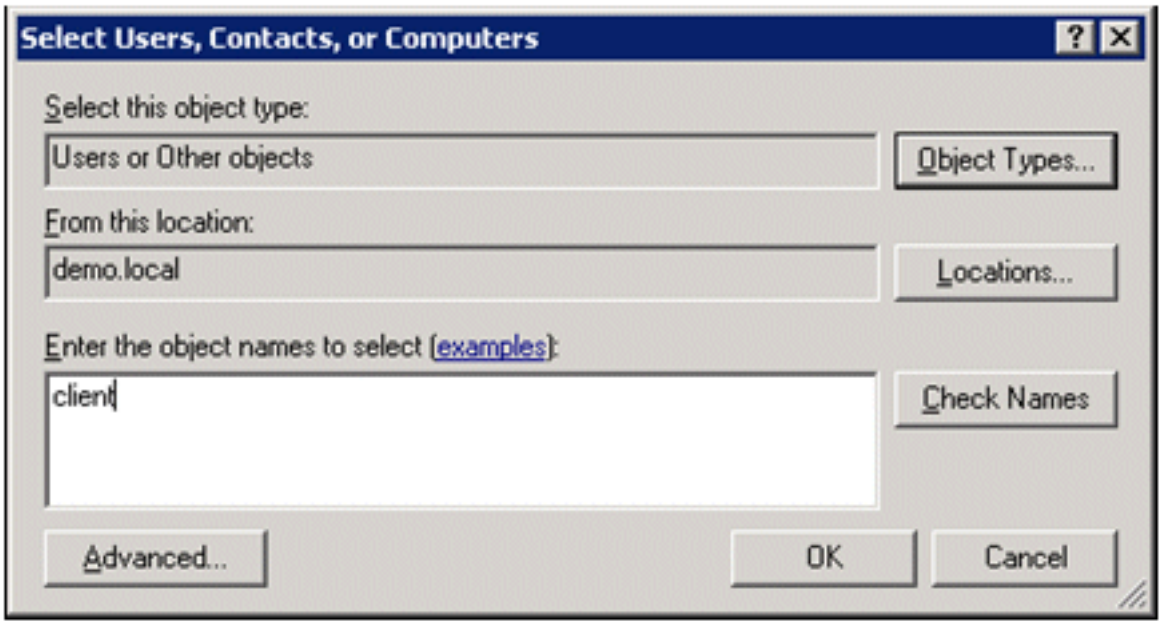


5. 按一下**OK**以儲存對wirelessusers組的更改。
6. 重複此過程，向該組中新增更多使用者。

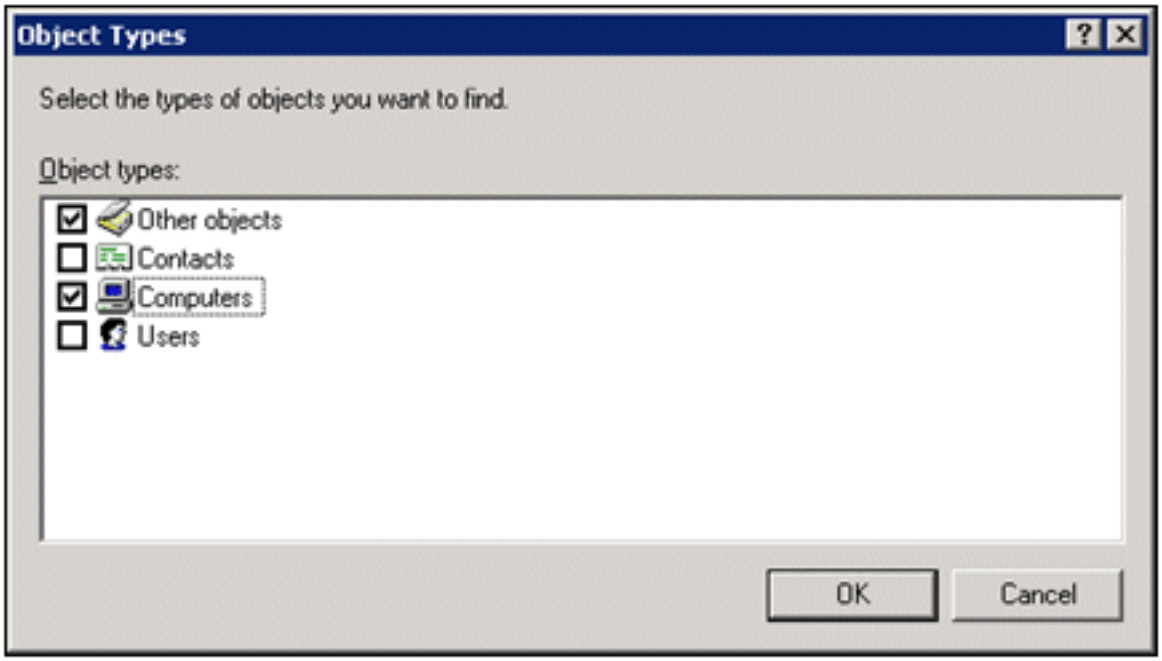
將客戶端電腦新增到無線使用者組

執行以下步驟：

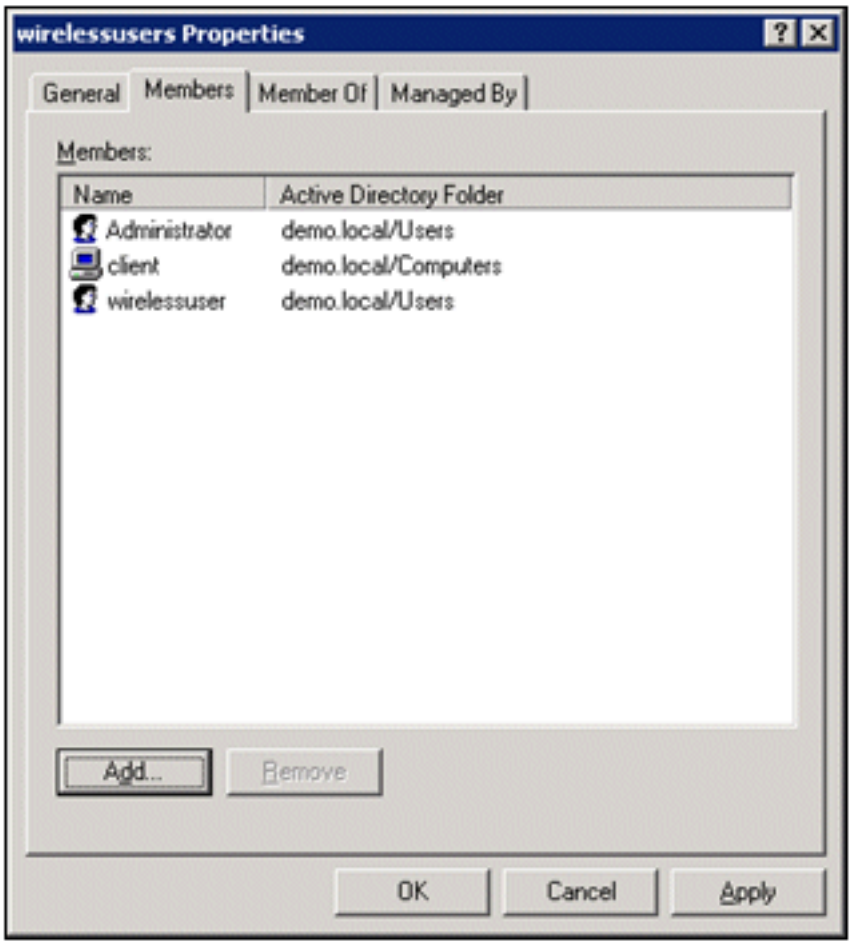
1. 重複本文檔的將使用者新增到無線使用者組部分中的步驟1和2。
2. 在「選擇使用者」、「聯絡人」或「電腦」對話方塊中，鍵入要新增到組中的電腦的名稱。此示例說明如何將名為*client*的電腦新增到組中。



3. 按一下**Object Types**，清除**Users**覈取方塊，然後選中**Computers**。



4. 按一下**OK**兩次。CLIENT電腦帳戶將新增到wirelessusers組中。



5. 重複該過程，向該組中新增更多電腦。

Cisco 1121安全ACS 5.1

使用CSACS-1121系列裝置進行安裝

CSACS-1121裝置預裝了ACS 5.1軟體。本節概述了安裝過程以及安裝ACS之前必須執行的任務。

1. 將CSACS-1121連線到網路和裝置控制檯。請參閱第4章「連線電纜」。
2. 開啟CSACS-1121裝置的電源。請參閱第4章「為CSACS-1121系列裝置加電」。
3. 在CLI提示符下運行**setup**命令以配置ACS伺服器的初始設定。請參閱運行安裝程式。

安裝ACS伺服器

本節介紹CSACS-1121系列裝置上ACS伺服器的安裝過程。

- 運行安裝程式
- 驗證安裝過程
- 安裝後任務

有關安裝Cisco Secure ACS伺服器的詳細資訊，請參閱Cisco Secure Access Control System 5.1的安裝和升級指南。

Cisco WLC5508控制器配置

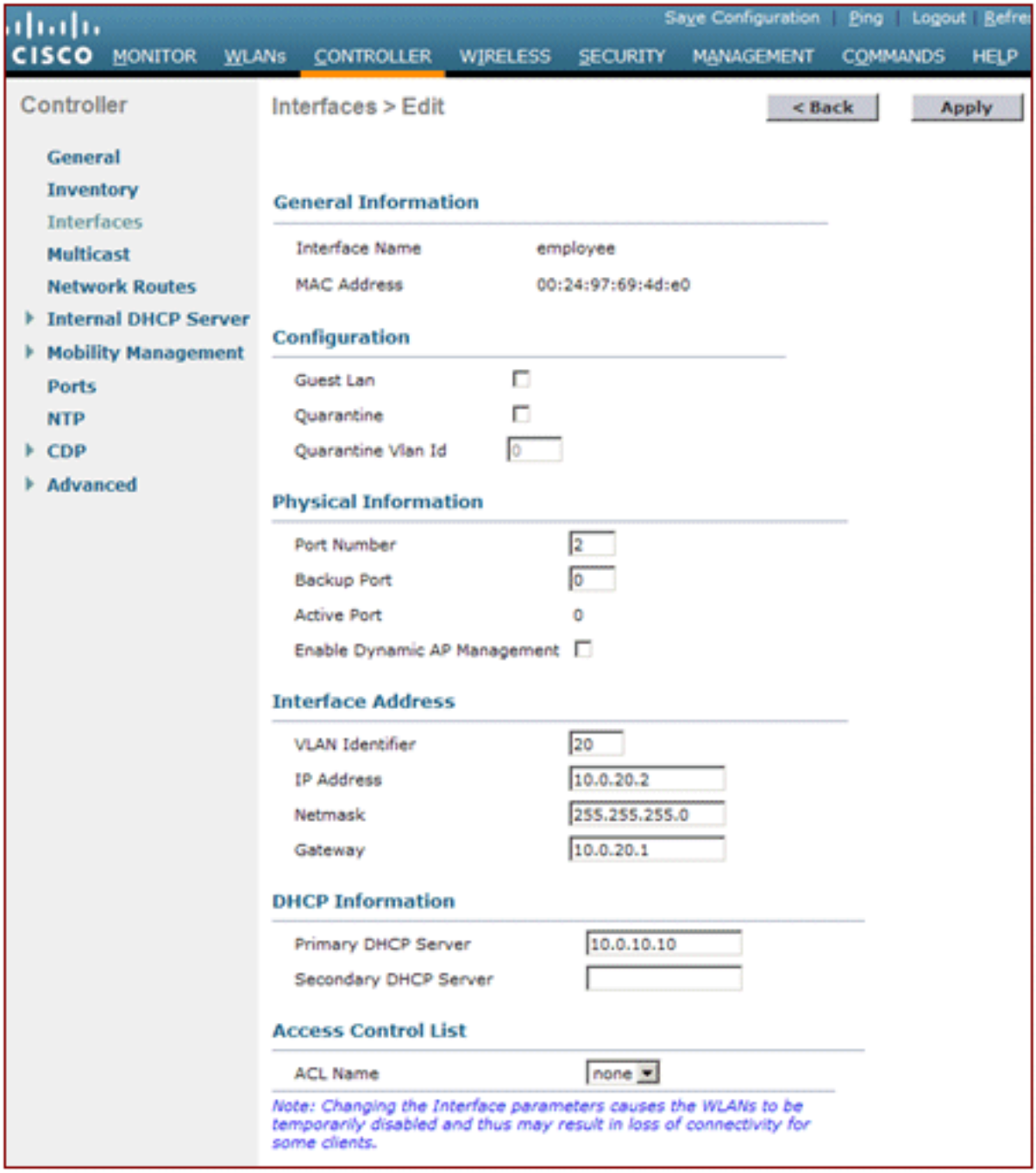
為WPAv2/WPA建立必要的配置

執行以下步驟：

註：假設控制器與網路具有基本連線，並且與管理介面的IP可達性成功。

1. 瀏覽至**https://10.0.1.10**以登入控制器。

2. 按一下「**Login**」。
3. 使用預設使用者*admin*和預設密碼*admin*登入。
4. 在**Controller**選單下為VLAN對映建立新的介面。
5. 按一下「**Interfaces**」。
6. 按一下「**New**」。
7. 在介面名稱欄位中，輸入*Employee*。（此欄位可以是您喜歡的任何值。）
8. 在VLAN ID欄位中，輸入*20*。（此欄位可以是網路中攜帶的任何VLAN。）
9. 按一下「**Apply**」。
10. 配置資訊，如此Interfaces > Edit視窗所示：介面IP地址**- 10.0.20.2**網路掩碼**- 255.255.255.0**網關 — **10.0.10.1**主DHCP - **10.0.10.10**



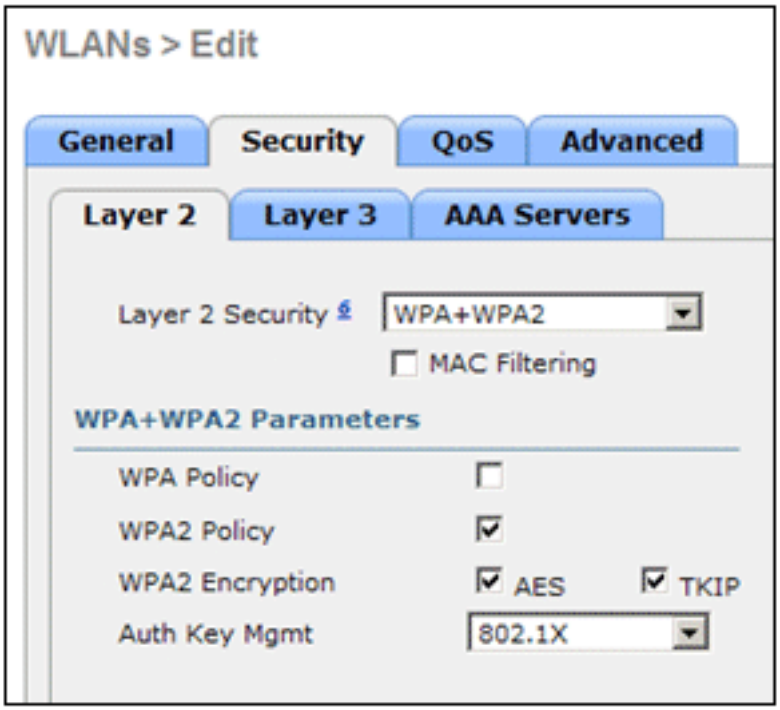
11. 按一下「**Apply**」。
12. 按一下**WLANs**頁籤。
13. 選擇**Create New**，然後按一下**Go**。
14. 輸入Profile Name，然後在WLAN SSID欄位中輸入*Employee*。

15. 選擇WLAN的ID，然後按一下**Apply**。
16. 在出現WLANs > Edit視窗時，配置此WLAN的資訊。**注意**：WPAv2是本實驗選擇的第2層加

密方法。若要允許具有TKIP-MIC客戶端的WPA與此SSID關聯，您還可以選中**WPA相容模式**和**允許WPA2 TKIP客戶端**框，或那些不支援802.11i AES加密方法的客戶端。

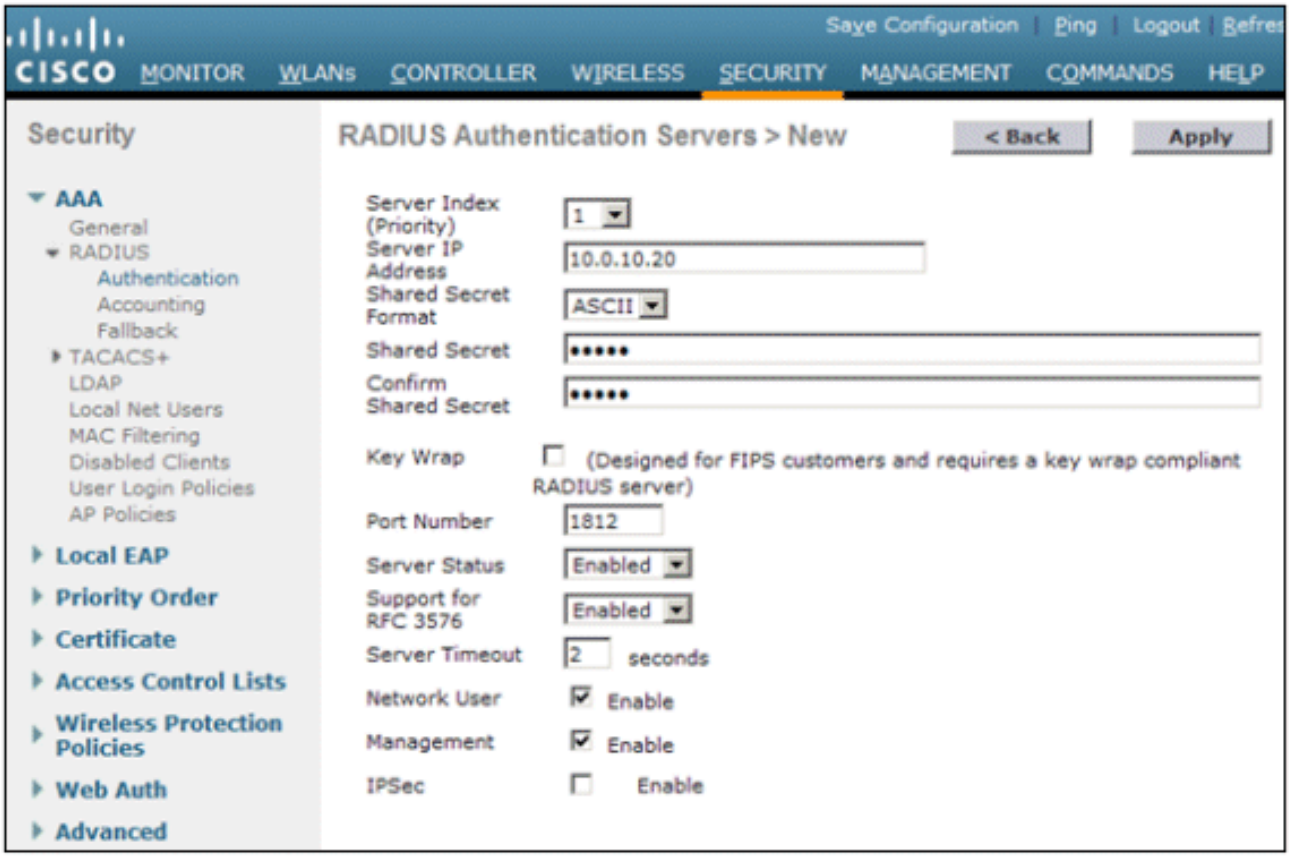
17. 在WLANs > Edit螢幕上，按一下**General**頁籤。
18. 確保選中**Enabled**的Status框並選擇適當的**Interface**（員工）。此外，確保選中**Broadcast SSID**的**Enabled**覈取方塊。

19. 按一下**Security**頁籤。
20. 在Layer 2（第2層）子選單下，選中**WPA + WPA2**以獲得Layer 2 Security（第2層安全）。若是WPA2加密，請勾選**AES + TKIP**以允許TKIP使用者端。



21. 選擇**802.1x**作為身份驗證方法。
22. 跳過「第3層」子選單，因為這不是必需的。設定RADIUS伺服器後，您就可以從「Authentication」功能表中選擇適當的伺服器。
23. **QoS**和**Advanced**頁籤可以保留為預設值，除非需要任何特殊配置。
24. 按一下**Security**選單以新增RADIUS伺服器。

25. 在「RADIUS」子選單下，按一下**Authentication**。然後，按一下**New**。
26. 新增RADIUS伺服器IP地址(10.0.10.20)，該地址是之前配置的ACS伺服器。
27. 確保共用金鑰與ACS伺服器中配置的AAA客戶端匹配。確保選中**Network User**框，然後按一下**Apply**。



28. 基本配置現已完成，您可以開始測試PEAP。

PEAP身份驗證

MS-CHAP版本2的PEAP需要ACS伺服器上的證書，但無線客戶端上不需要。ACS伺服器的電腦證書自動註冊可用於簡化部署。

若要配置CA伺服器以為電腦和使用者證書提供自動註冊，請完成本節中的過程。

注意：Microsoft在Windows 2003 Enterprise CA發佈後更改了Web Server模板，使金鑰不再可匯出，並且該選項呈灰色顯示。沒有其他證書模板隨用於伺服器身份驗證的證書服務一起提供，並且允許將下拉選單中的金鑰標籤為可匯出，因此您必須建立一個執行此操作的新模板。

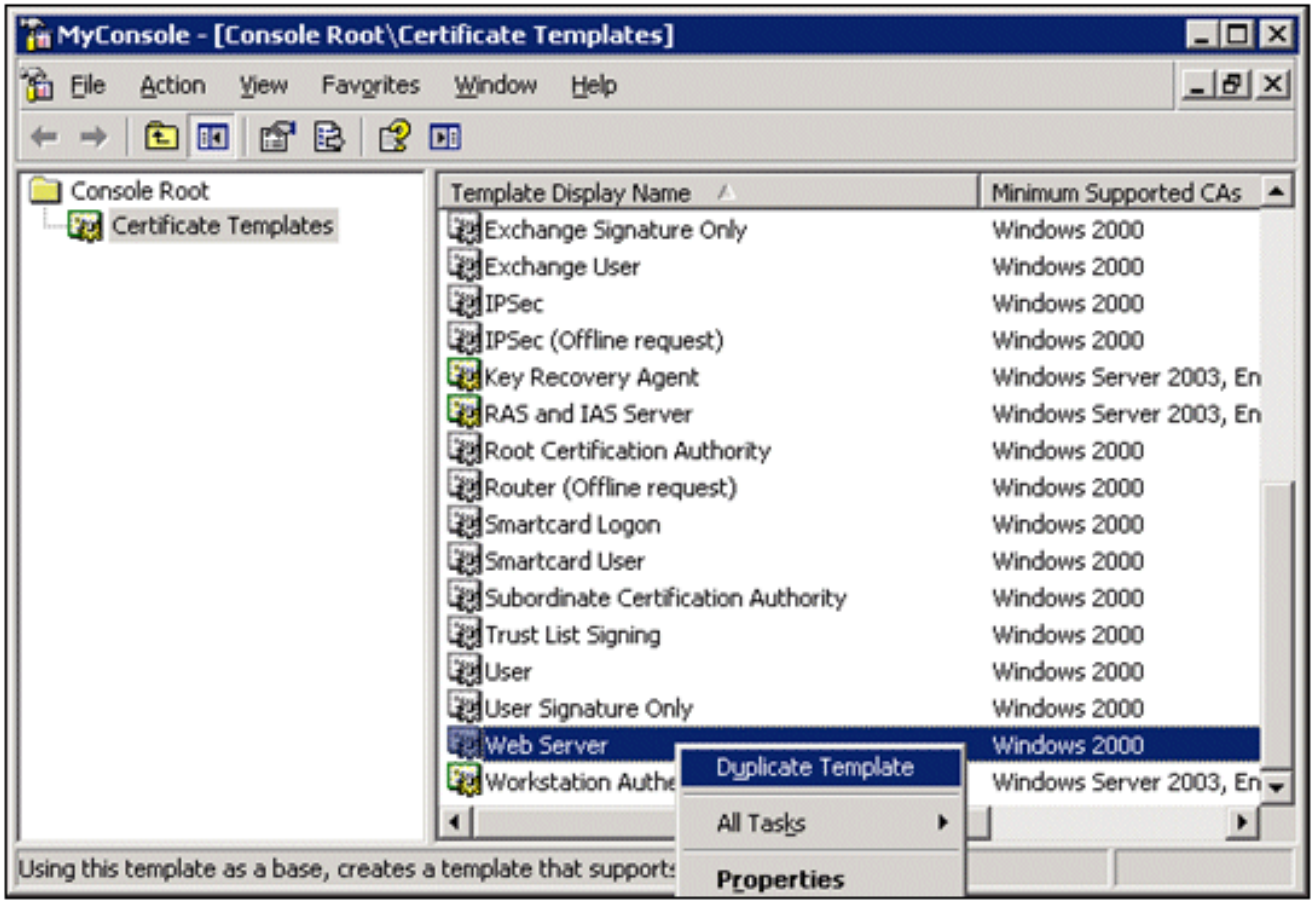
注意：Windows 2000允許匯出金鑰，如果您使用Windows 2000，則無需遵循這些步驟。

安裝證書模板管理單元

執行以下步驟：

1. 選擇**開始 > 運行**，輸入**mmc**，然後按一下**確定**。
2. 在「檔案」選單上，按一下**「新增/刪除管理單元」**，然後按一下**新增**。
3. 在「管理單元」下，按兩下**Certificate Templates**，按一下**Close**，然後按一下**OK**。
4. 在控制檯樹中，按一下**Certificate Templates**。所有證書模板都會顯示在「詳細資訊」窗格中。

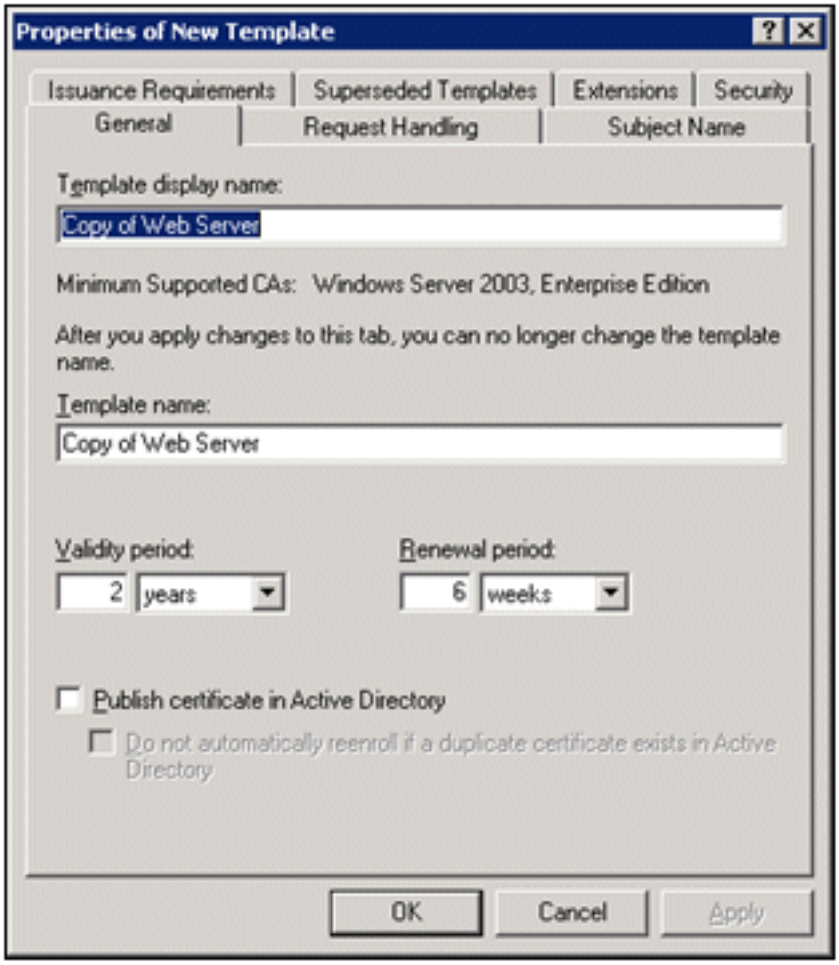
5. 若要繞過步驟2至4，請輸入*certtmpl.msc*，以開啟「證書模板」管理單元。



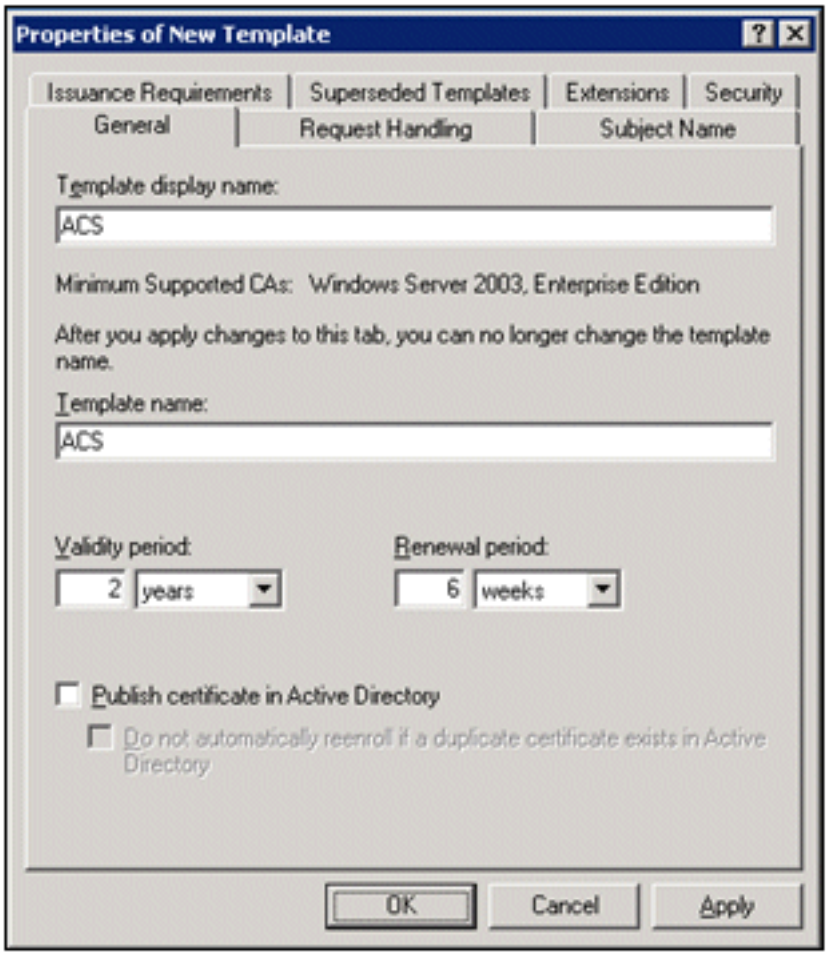
為ACS Web伺服器建立證書模板

執行以下步驟：

1. 在「證書模板」管理單元的「詳細資訊」窗格中，按一下**Web Server**模板。
2. 在「操作」選單上，按一下**複製模板**。

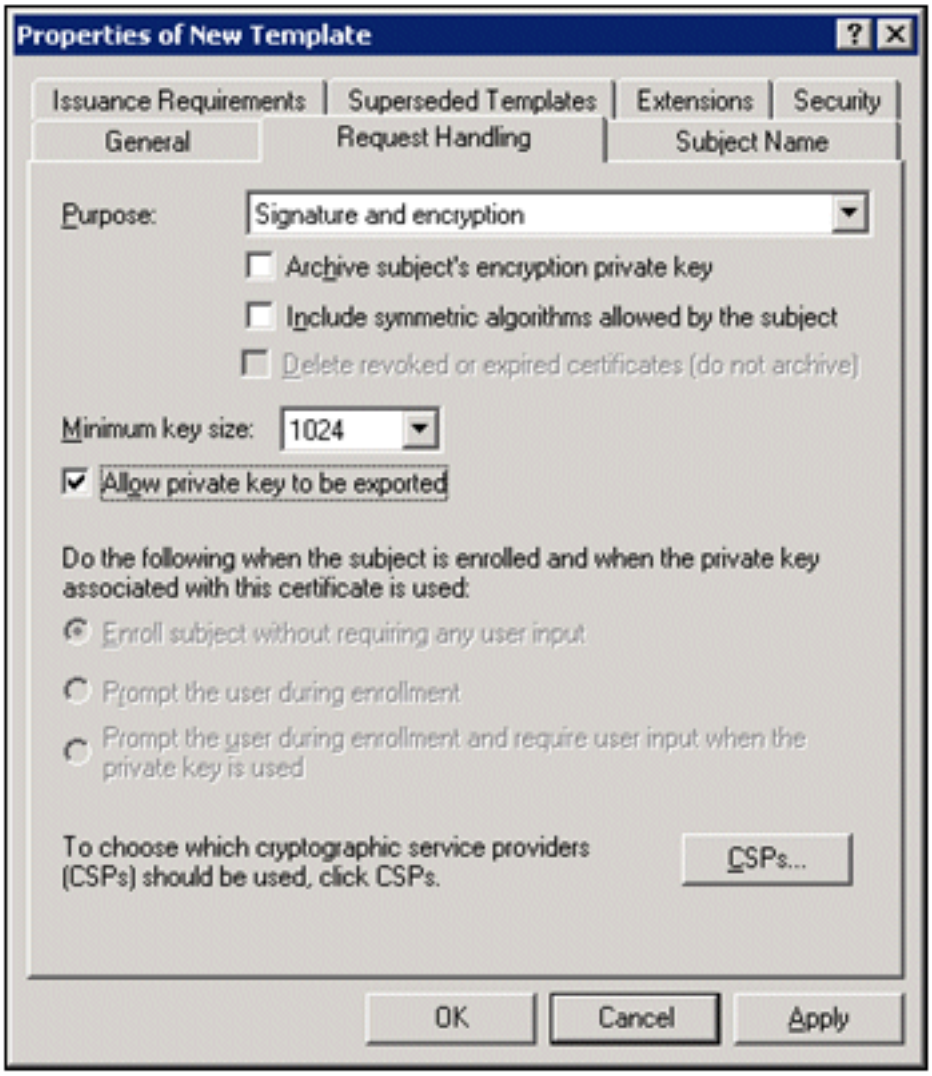


3. 在「模板顯示名稱」欄位中，輸入*ACS*。

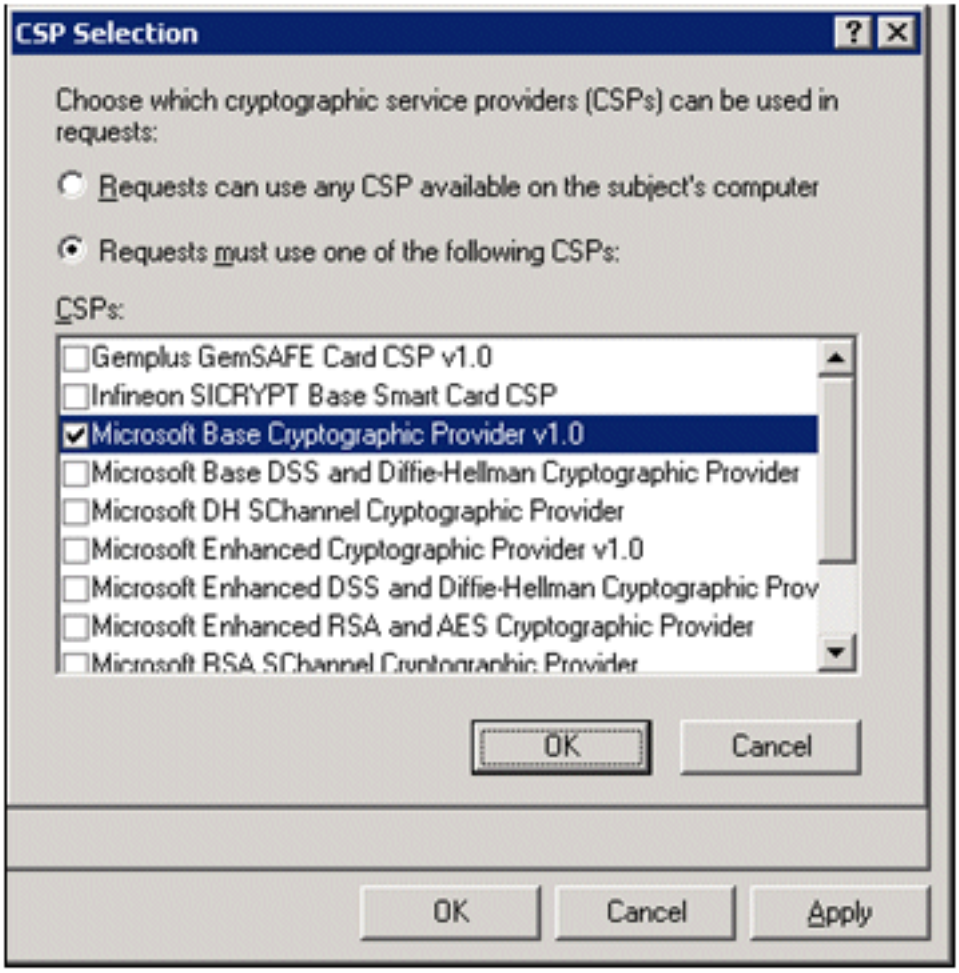


4. 轉至**請求處理**頁籤，並選中**Allow private key to be exported**。此外，請確保從「用途」下拉選

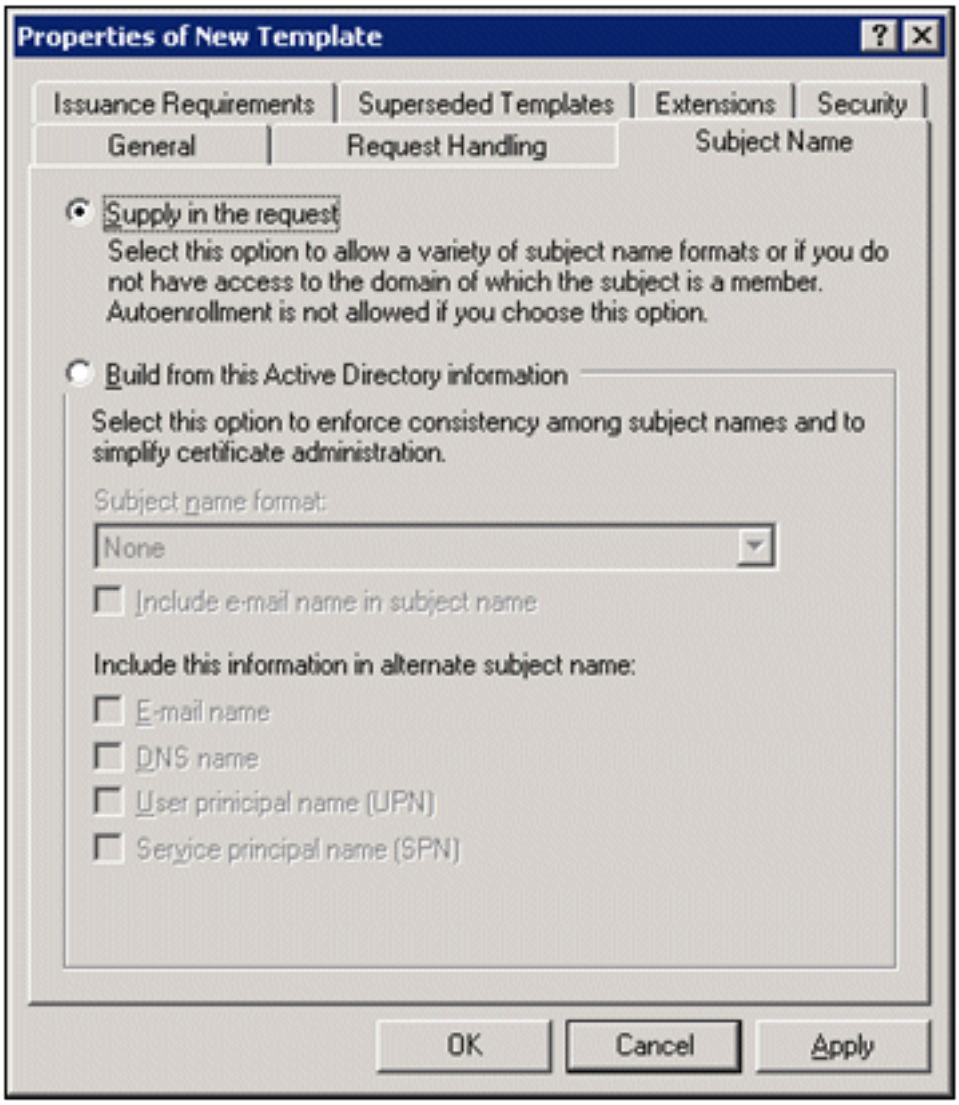
單中選擇**「簽名和加密」**。



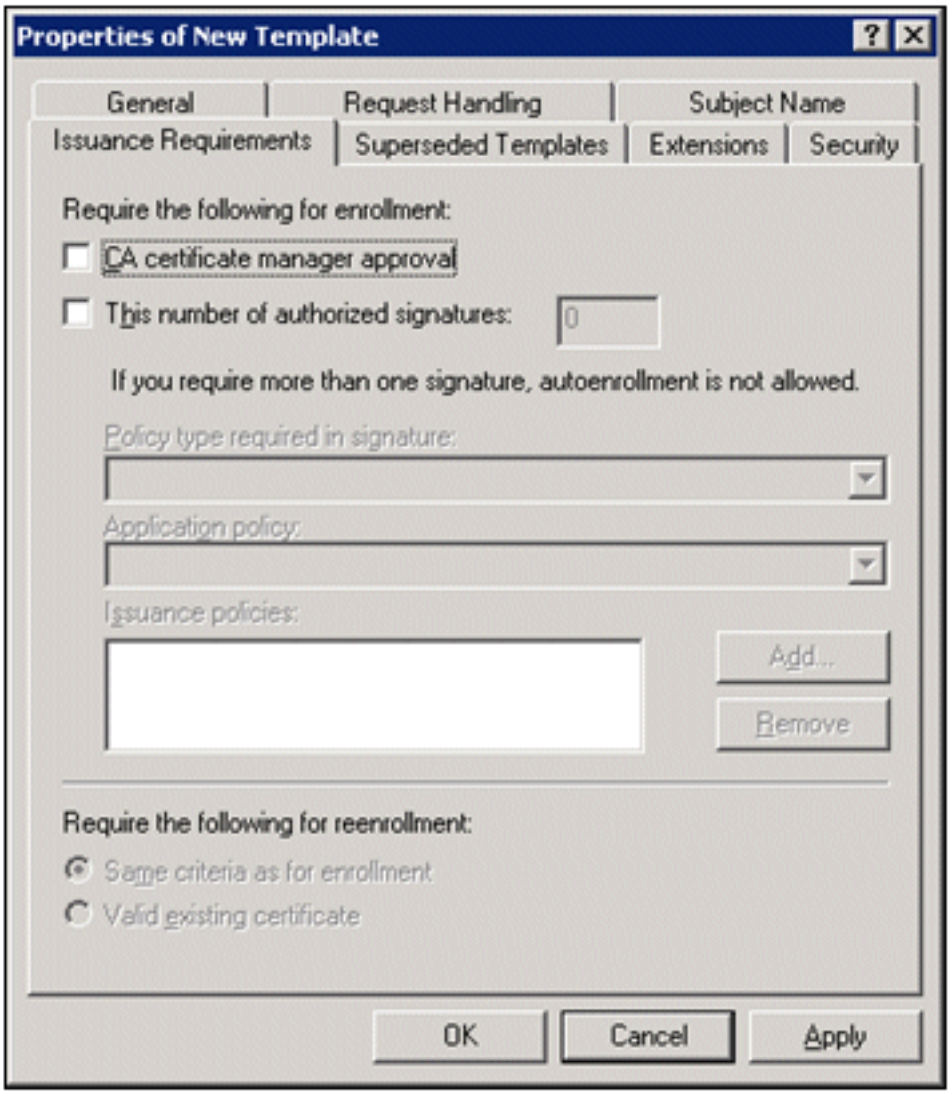
5. 選擇**請求必須使用以下CSP之一**並選中**Microsoft Base Cryptographic Provider v1.0**。取消選中任何已選中的CSP，然後按一下**OK**。



6. 轉到**Subject Name**頁籤，在請求中選擇**Supply**，然後按一下**OK**。



7. 轉到**Security**頁籤，選中**Domain Admins Group**，並確保選中了Allowed下的**Enroll**選項。**注意：如果您選擇根據此**Active Directory資訊構建，請僅檢查**使用者主體名稱(UPN)**，並取消選中**Include email name** in subject name and E-mail name，因為未在Active Directory使用者和電腦管理單元中為無線使用者帳戶輸入電子郵件名稱。如果不禁用這兩個選項，自動註冊將嘗試使用電子郵件，這將導致自動註冊錯誤。
8. 如果需要，還可以採取其他安全措施來防止證書自動推出。可在Issuance Requirements頁籤下找到它們。本檔案不會進一步討論此問題。

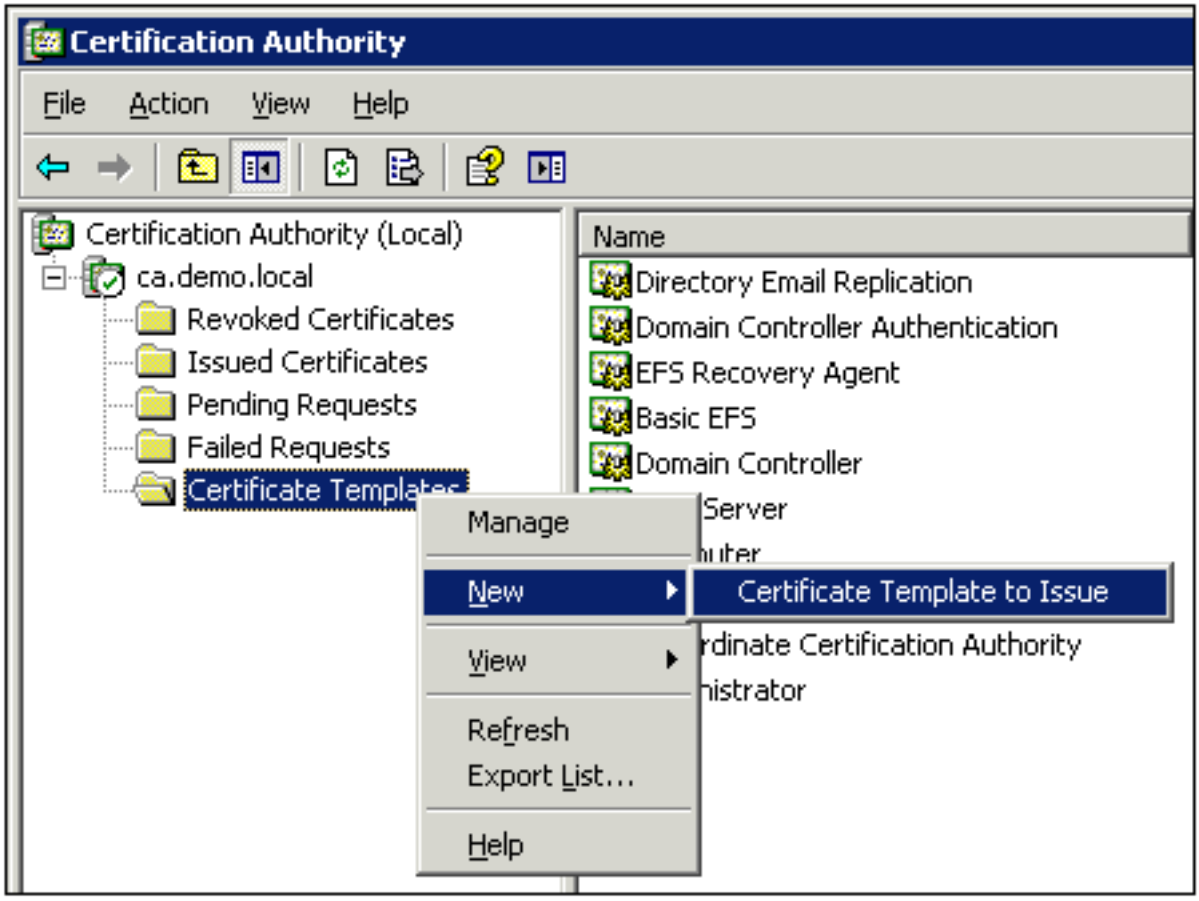


9. 按一下**OK**以儲存模板，然後從「證書頒發機構」管理單元發佈此模板。

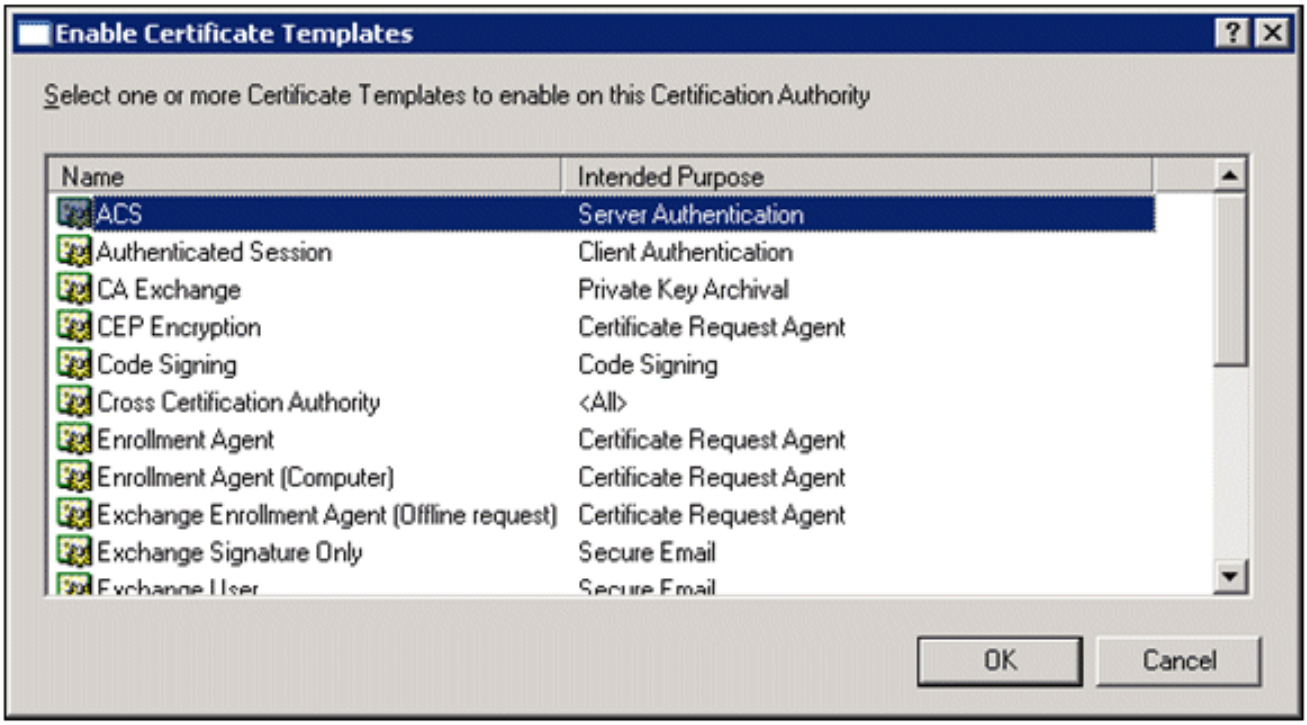
啟用新的ACS Web伺服器證書模板

執行以下步驟：

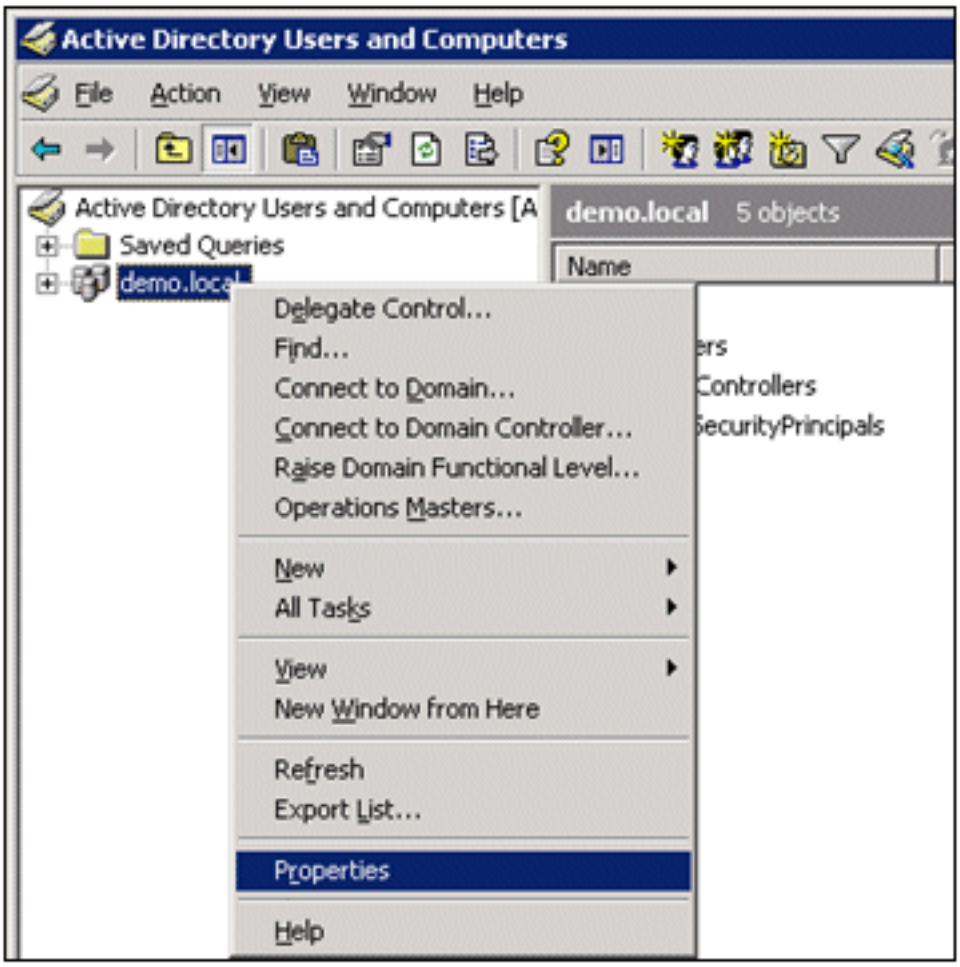
1. 開啟證書頒發機構管理單元。執行為ACS Web伺服器建立證書模板部分中的步驟1至3，選擇**Certificate Authority**選項，選擇**Local Computer**，然後按一下**Finish**。
2. 在「證書頒發機構」控制檯樹中，展開**ca.demo.local**，然後按一下右鍵**Certificate Templates**。
3. 前往**New > Certificate Template to Issue**。



4. 按一下**ACS Certificate Template**。

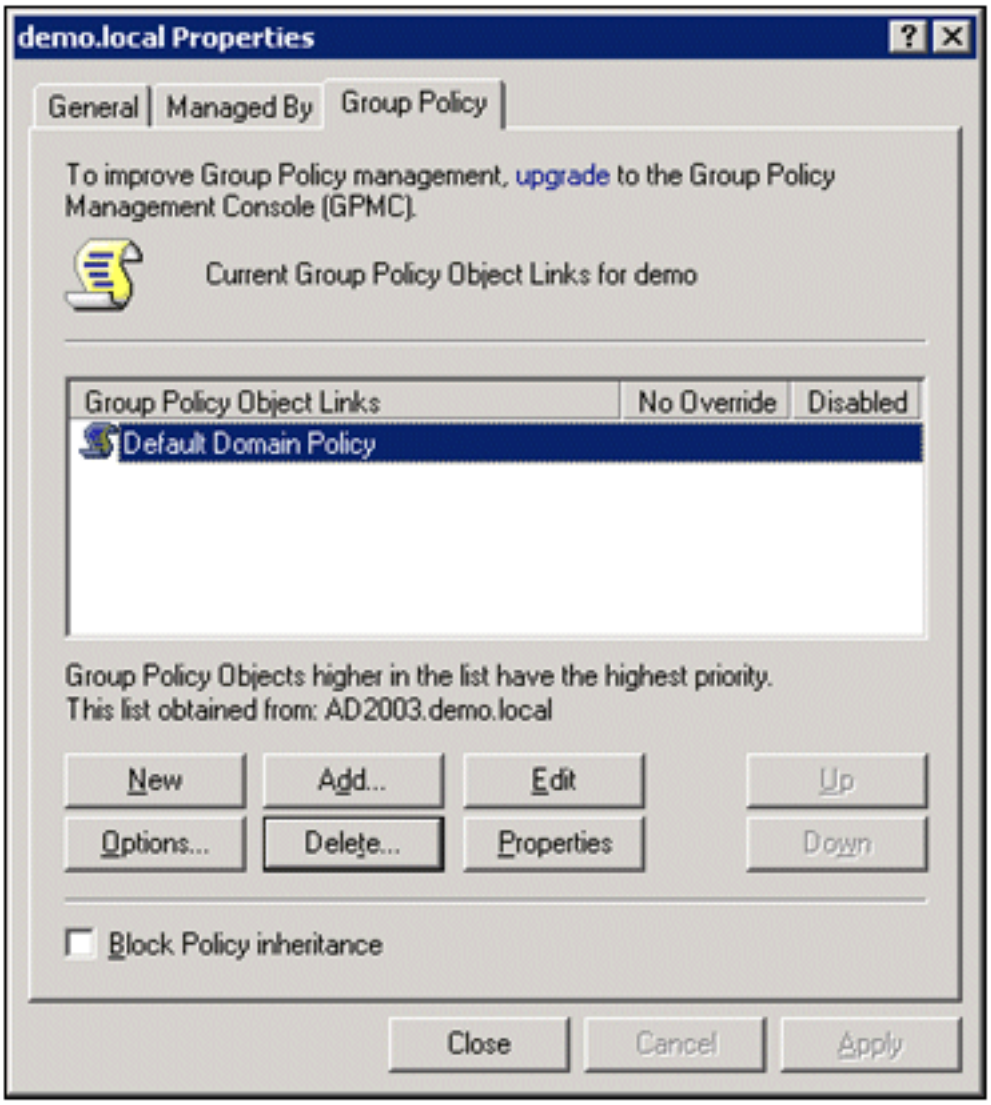


5. 按一下**OK**，然後開啟**Active Directory使用者和電腦**管理單元。
6. 在控制檯樹中，按兩下**Active Directory Users and Computers**，按一下右鍵**demo.local**，然後



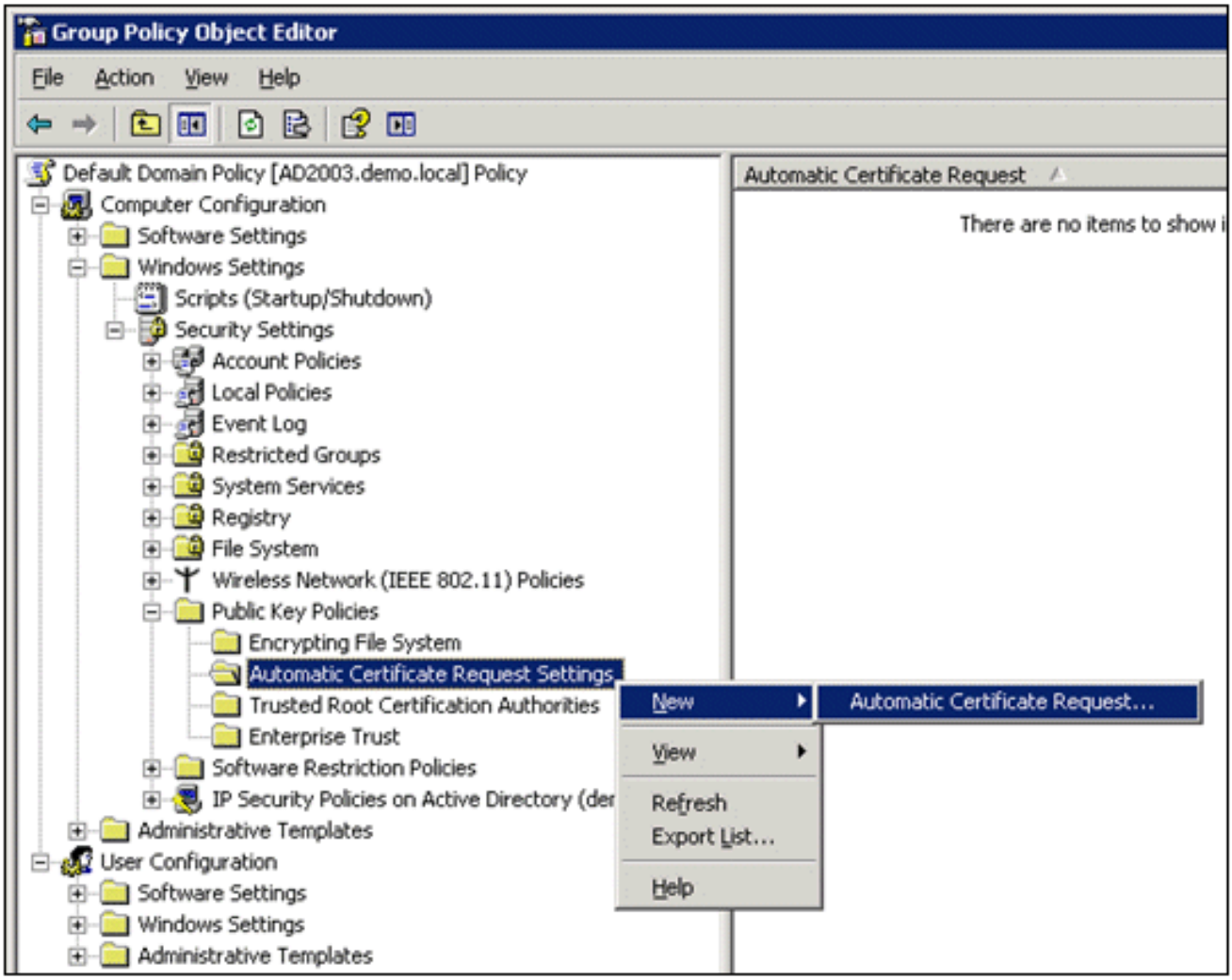
按一下**Properties**。

7. 在Group Policy頁籤上，按一下**Default Domain Policy**，然後按一下**Edit**。這將開啟組策略對



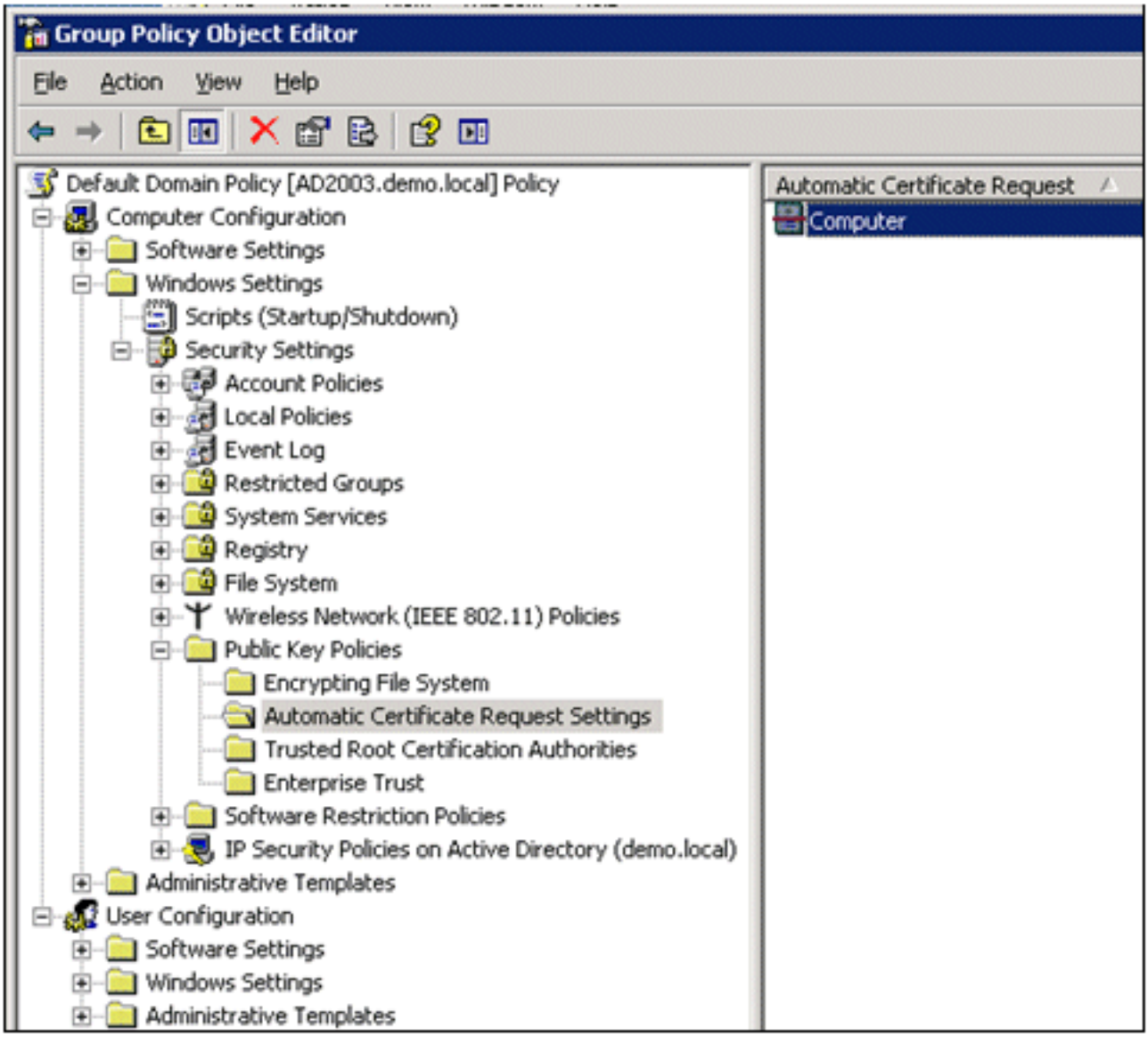
象編輯器管理單元。

8. 在控制檯樹中，展開Computer Configuration > **Windows Settings** > **Security Settings** > **Public Key Policies**，然後選擇Automatic Certificate Request Settings。

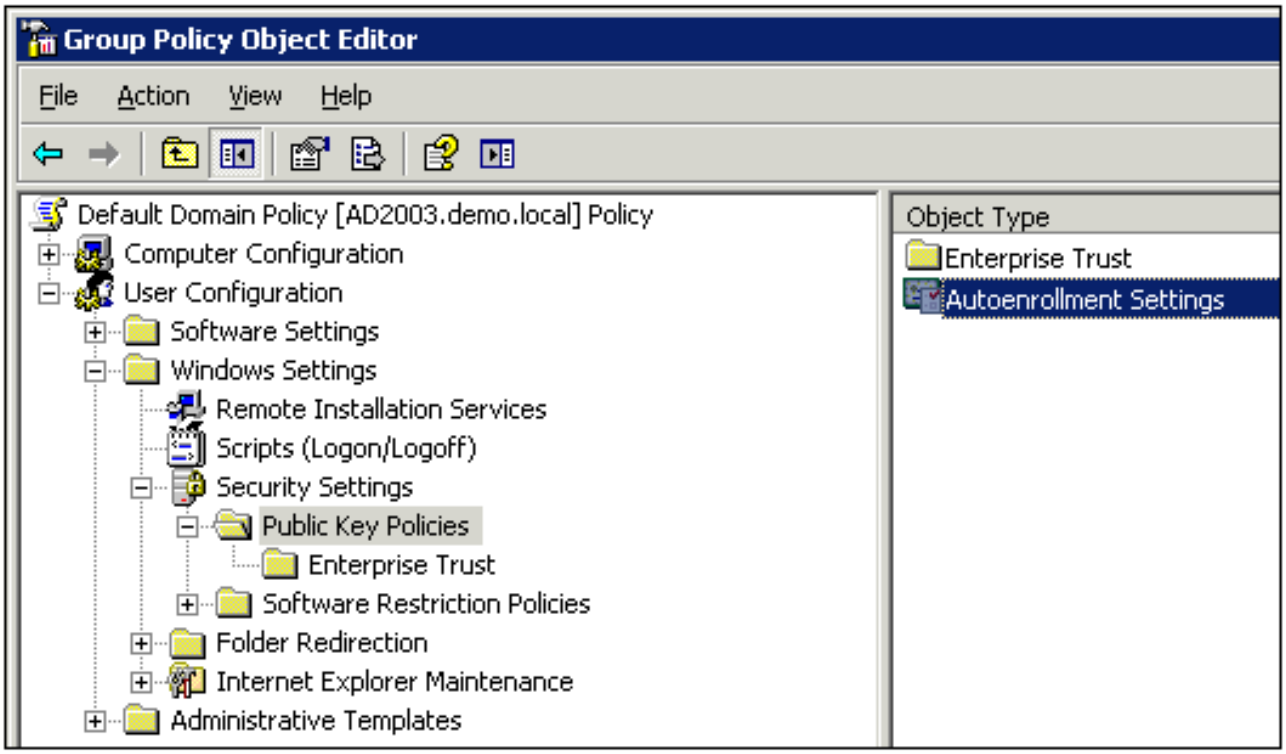


9. 按一下右鍵**Automatic Certificate Request Settings**，然後選擇**New > Automatic Certificate Request**。
10. 在「歡迎使用自動證書請求設定嚮導」頁面上，按一下**下一步**。
11. 在「Certificate Template」頁面上，按一下**Computer**，然後按一下**Next**。

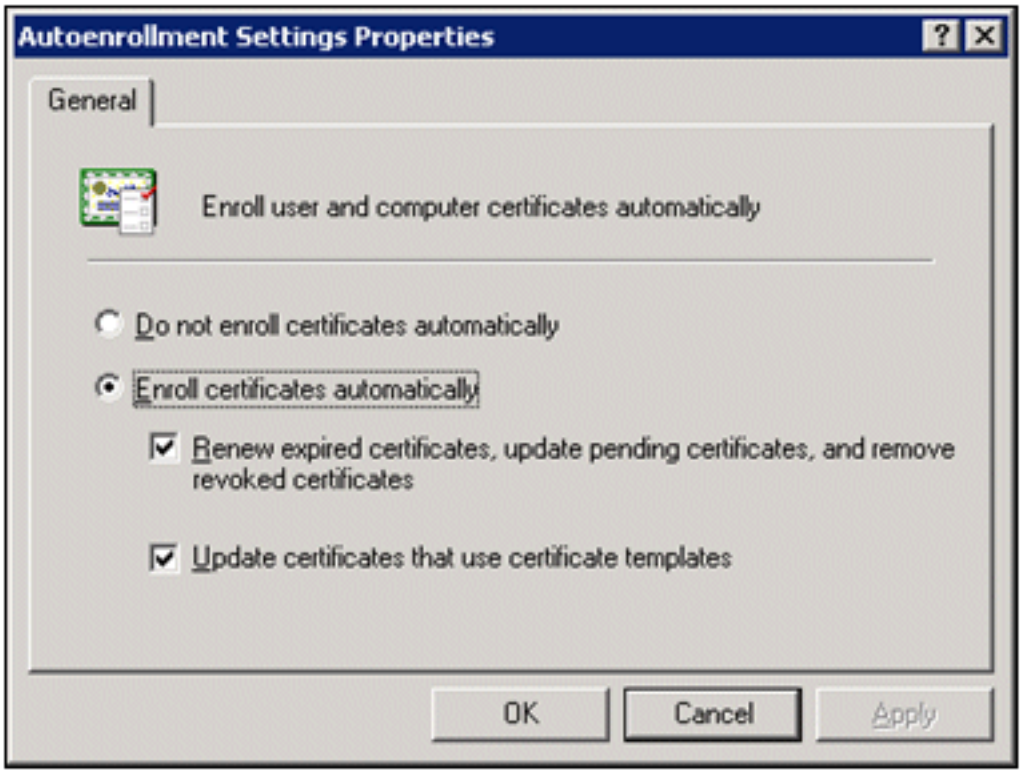
12. 完成「自動證書請求設定嚮導」頁後，按一下**完成**。電腦證書型別現在顯示在組策略對象編輯器管理單元的詳細資訊窗格中。



13. 在控制檯樹中，展開**User Configuration > Windows Settings > Security Settings > Public Key Policies**。
14. 在詳細資訊窗格中，按兩下**Auto-enrollment Settings**。



15. 選擇Enroll certificates automatically，然後選中Renew expired certificates， update pending certificates and remove revoked certificates和Update certificate that using certificate templates。



16. 按一下「OK」（確定）。

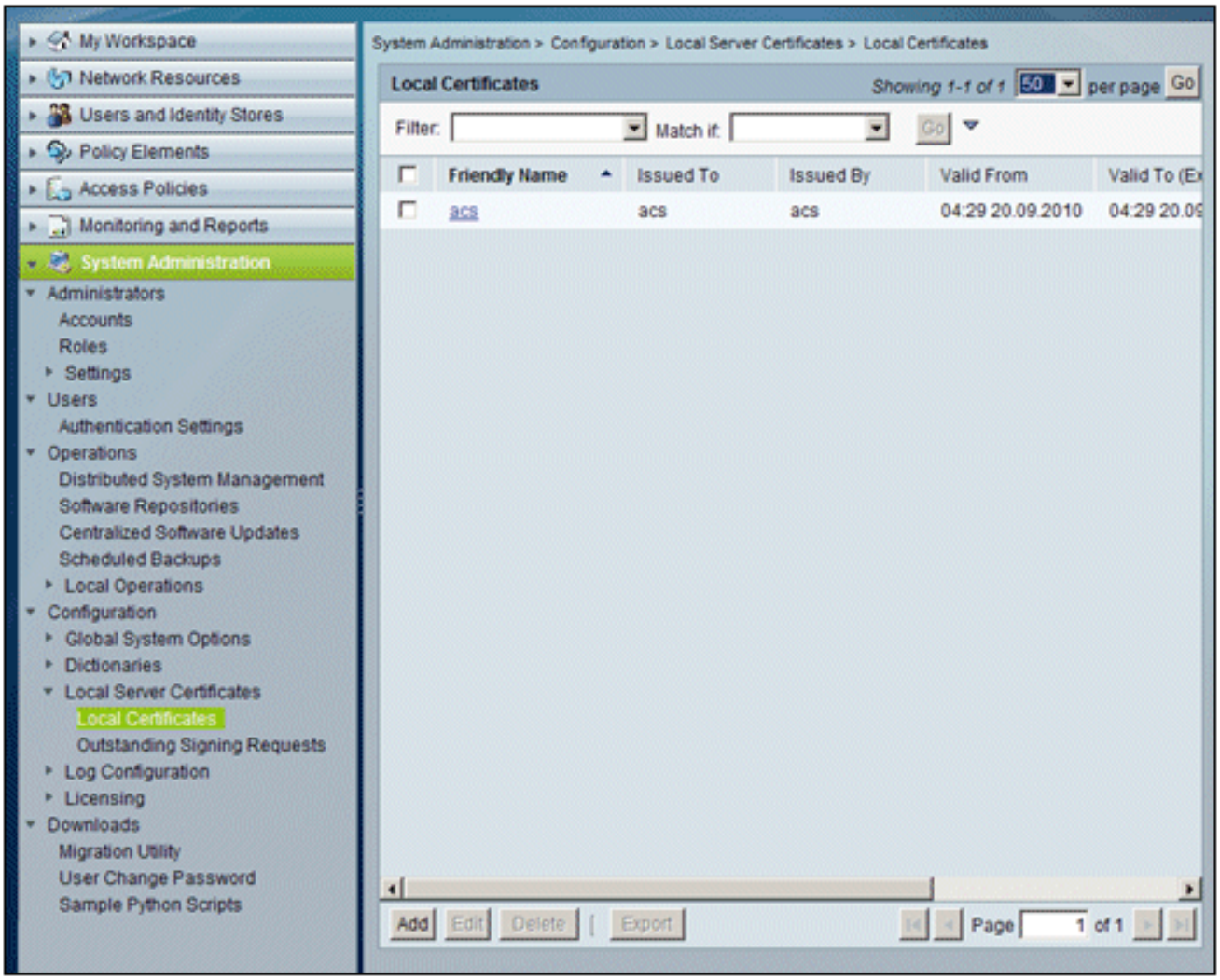
ACS 5.1證書設定

為ACS配置可匯出證書

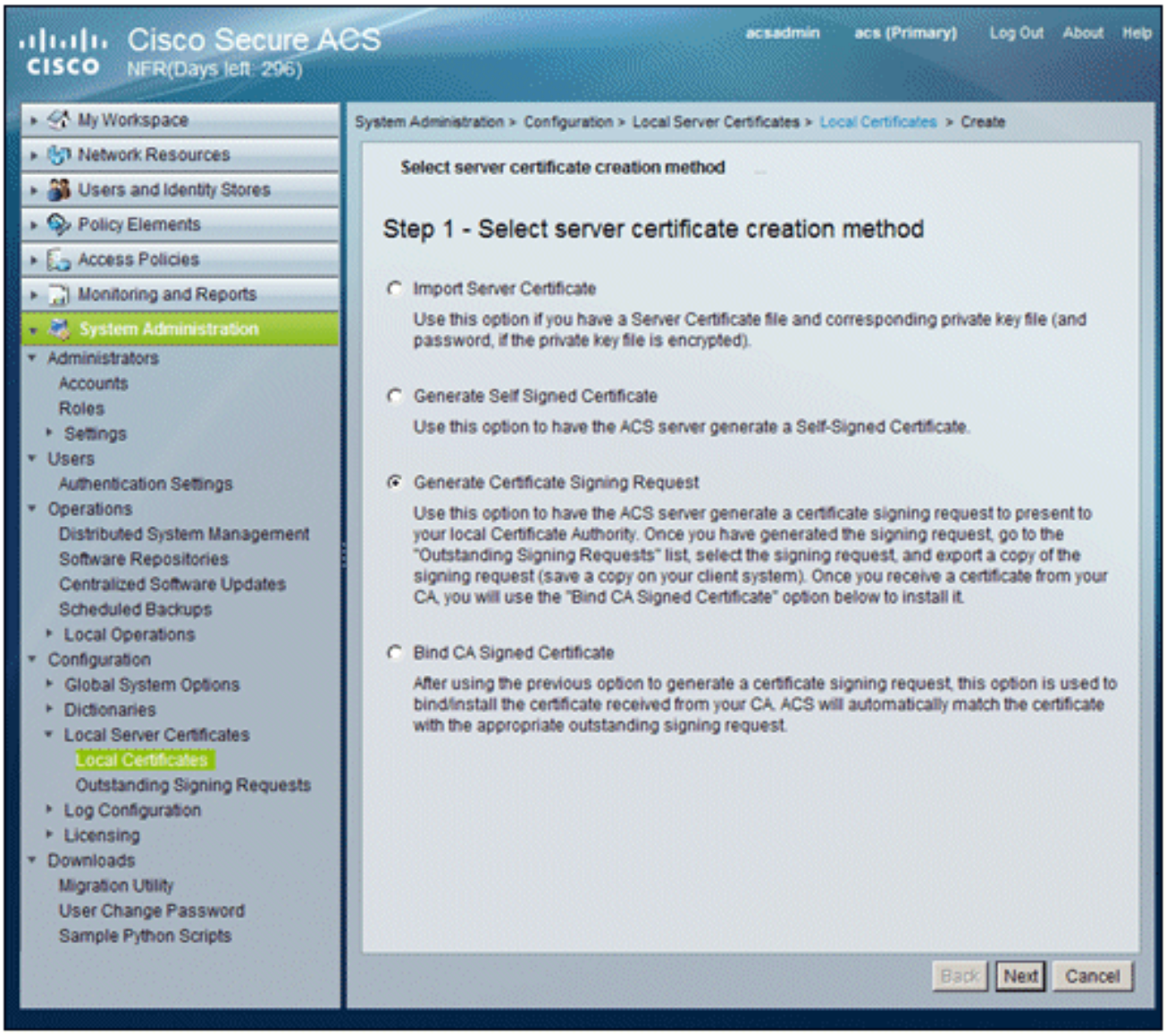
注意：ACS伺服器必須從企業根CA伺服器獲取伺服器證書，才能對WLAN PEAP客戶端進行身份驗證。

注意：確保IIS管理器在證書設定過程中未開啟，因為這會導致快取資訊出現問題。

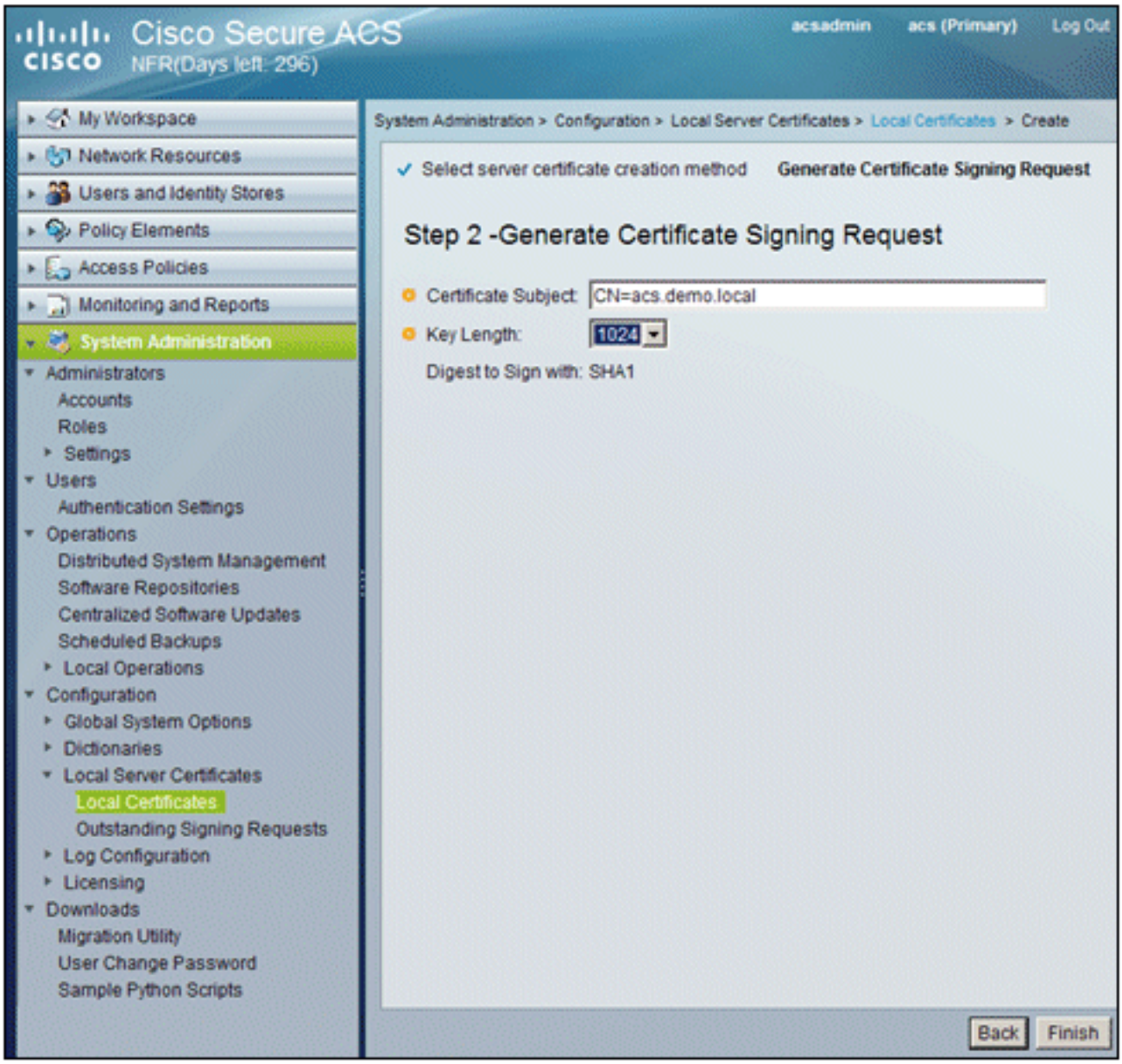
1. 使用帳戶管理員許可權登入到ACS伺服器。
2. 前往**System Administration > Configuration > Local Server Certificates**。按一下「**Add**」。



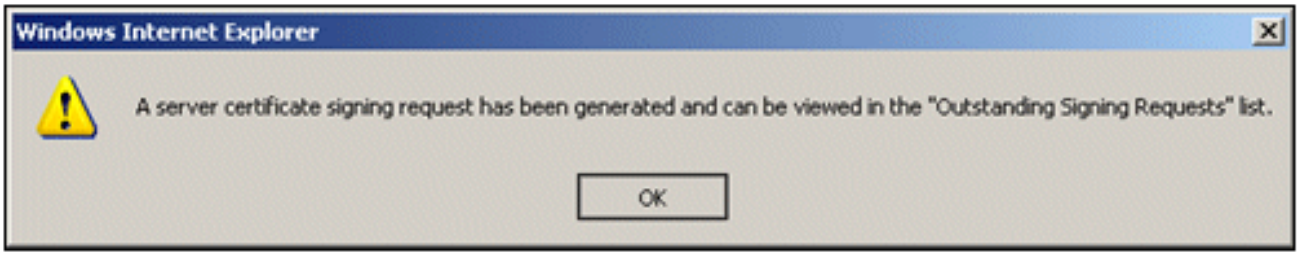
3. 選擇伺服器證書建立方法時，請選擇**Generate Certificate Signing Request**。按「**Next**」（下一步）。



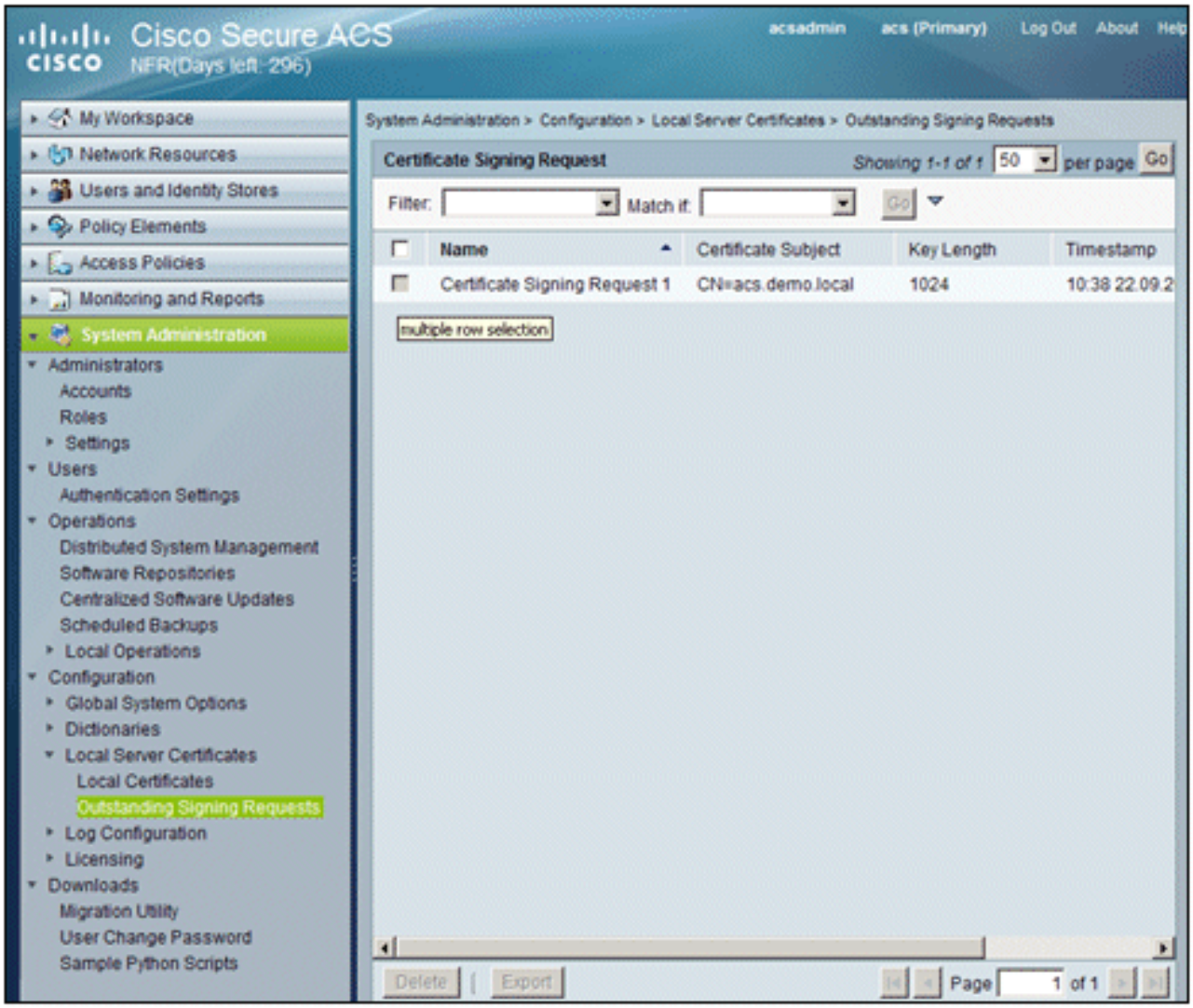
4. 輸入證書主題和金鑰長度作為示例，然後按一下Finish:證書主題- CN=acs.demo.local金鑰長度 —
1024



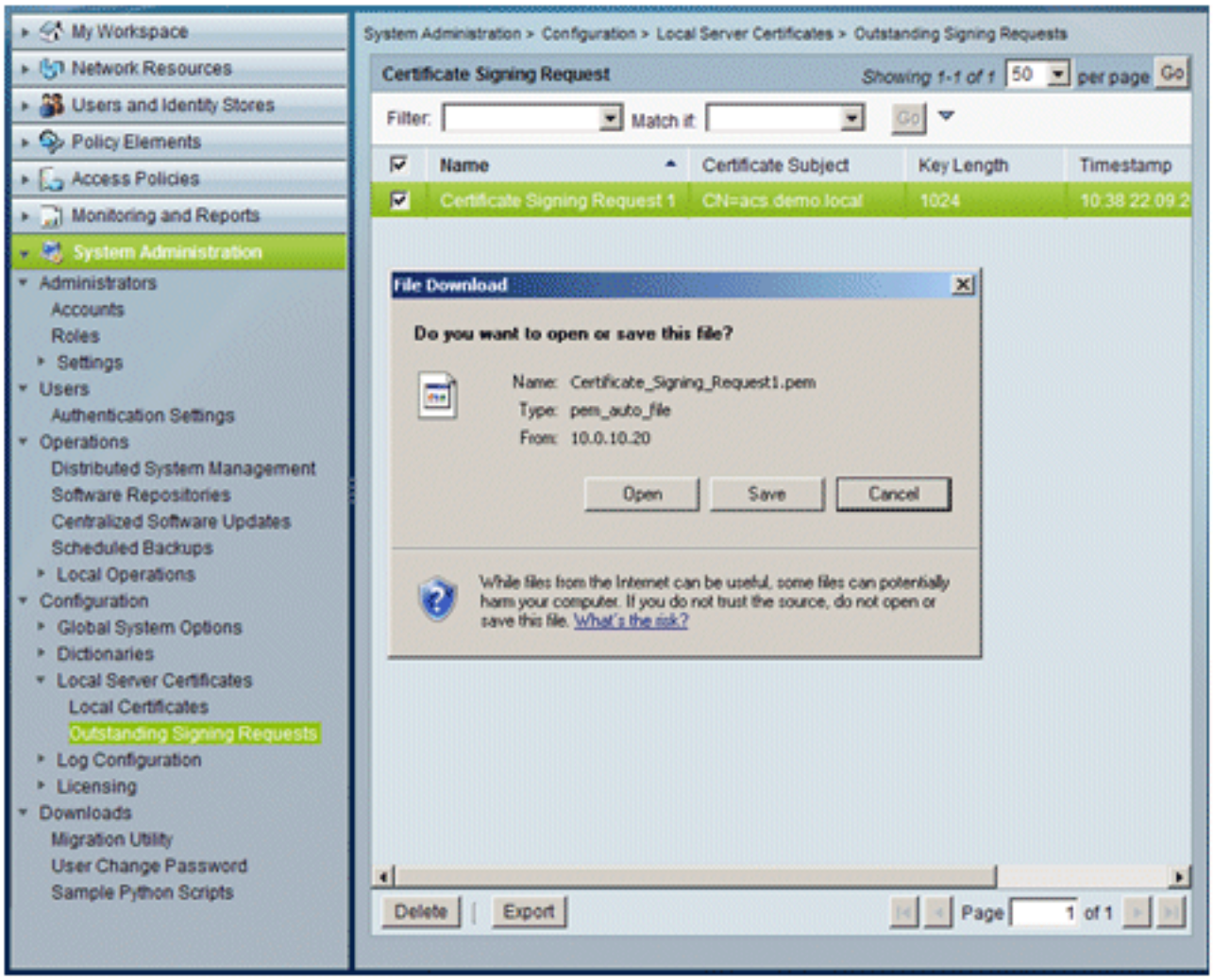
5. ACS將提示已生成證書簽名請求。按一下「**OK**」（確定）。



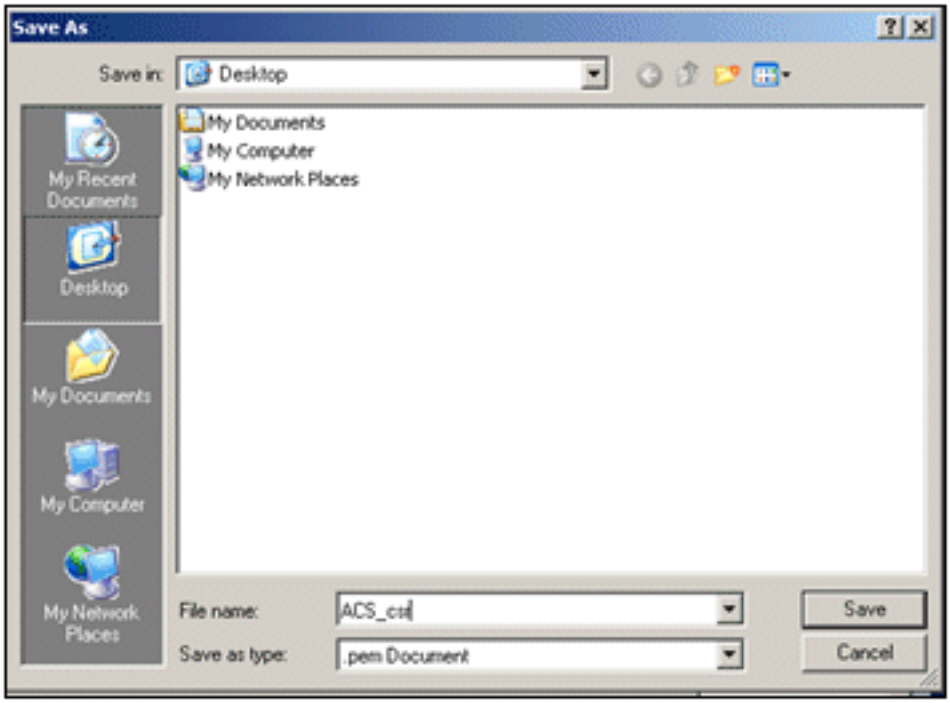
6. 在「系統管理」下，轉至**配置 > 本地伺服器證書 > 未完成的簽名請求。注意：**此步驟的原因是Windows 2003不允許可匯出的金鑰，並且您需要根據之前建立的ACS證書生成證書請求。



7. 選擇Certificate Signing Request條目，然後按一下Export。



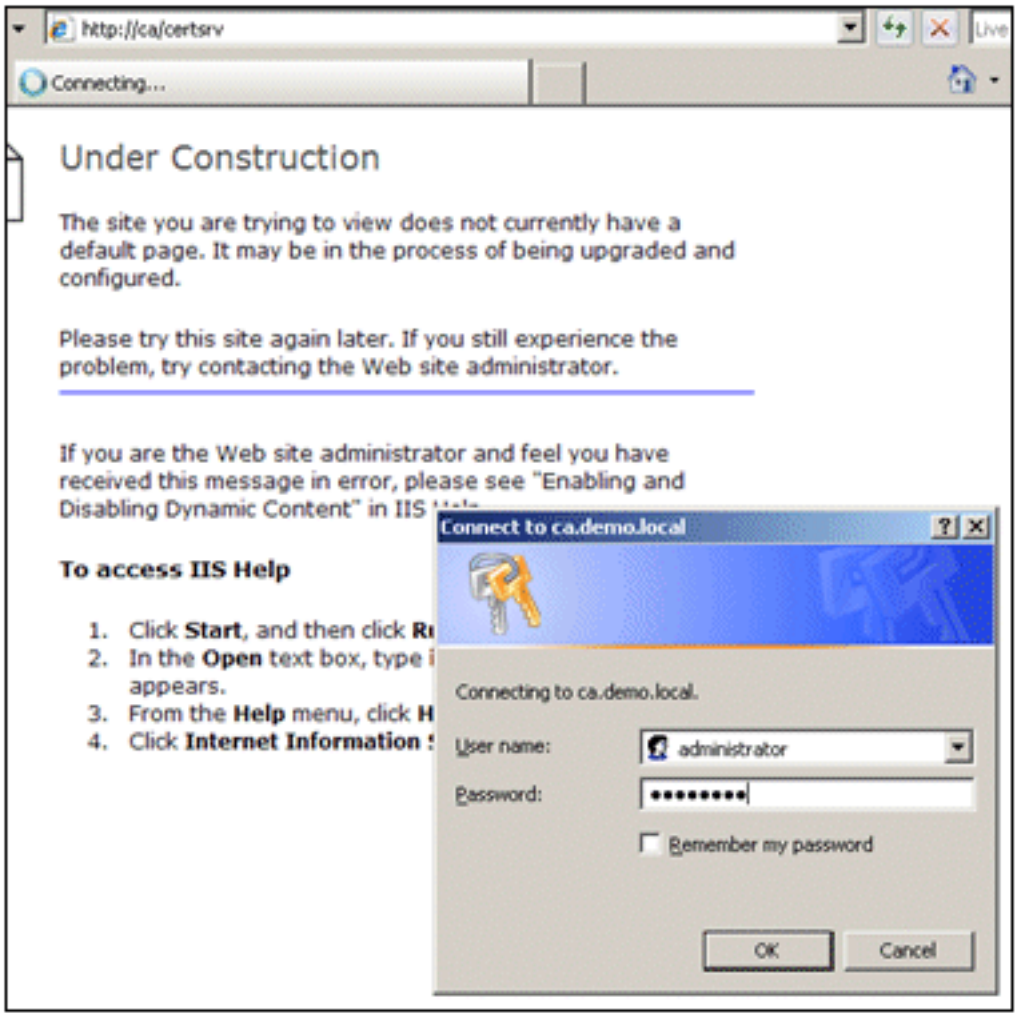
8. 將ACS證書.pem檔案儲存到案頭。



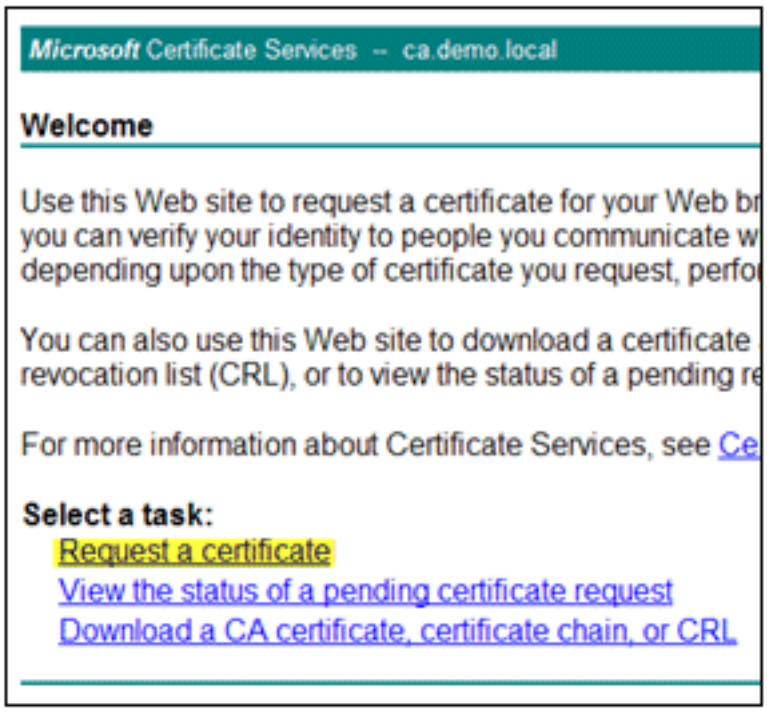
在ACS 5.1軟體中安裝證書

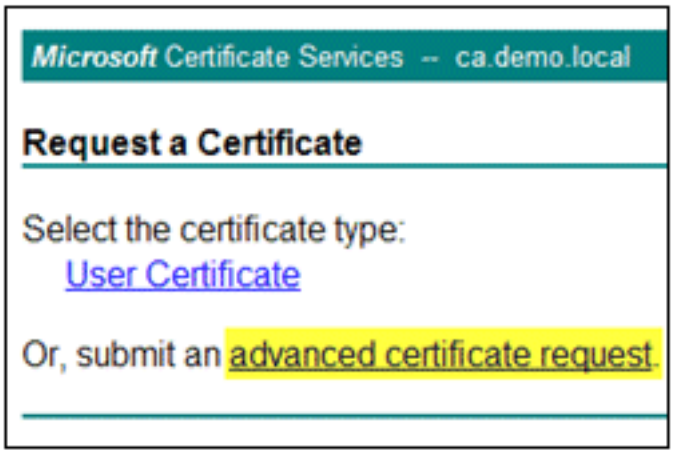
執行以下步驟：

1. 開啟瀏覽器並連線到CA伺服器URL **http://10.0.10.10/certsrv**。

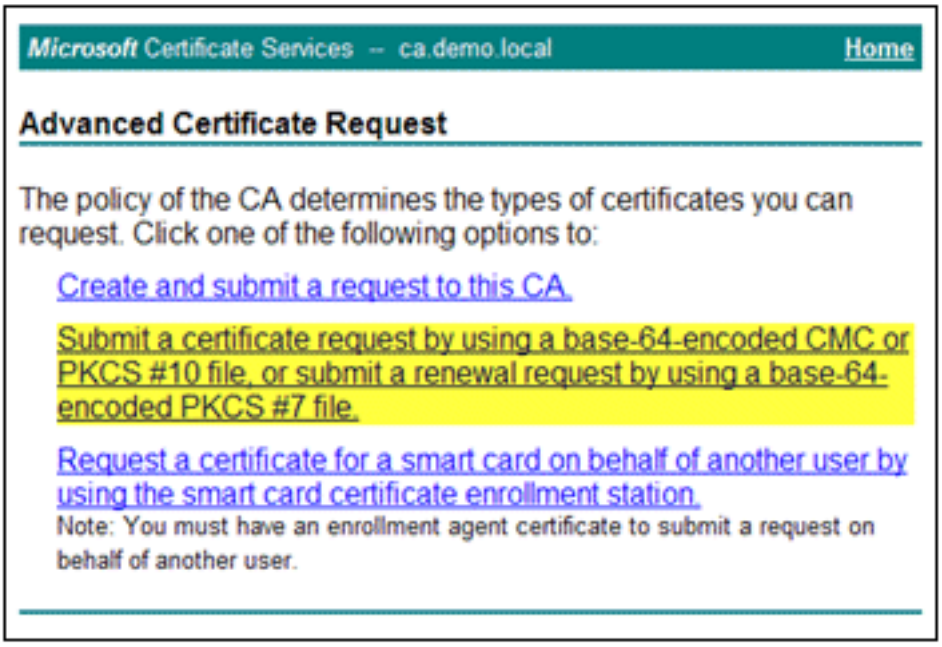


2. 出現「Microsoft Certificate Services（Microsoft證書服務）」視窗。選擇**請求證書**。



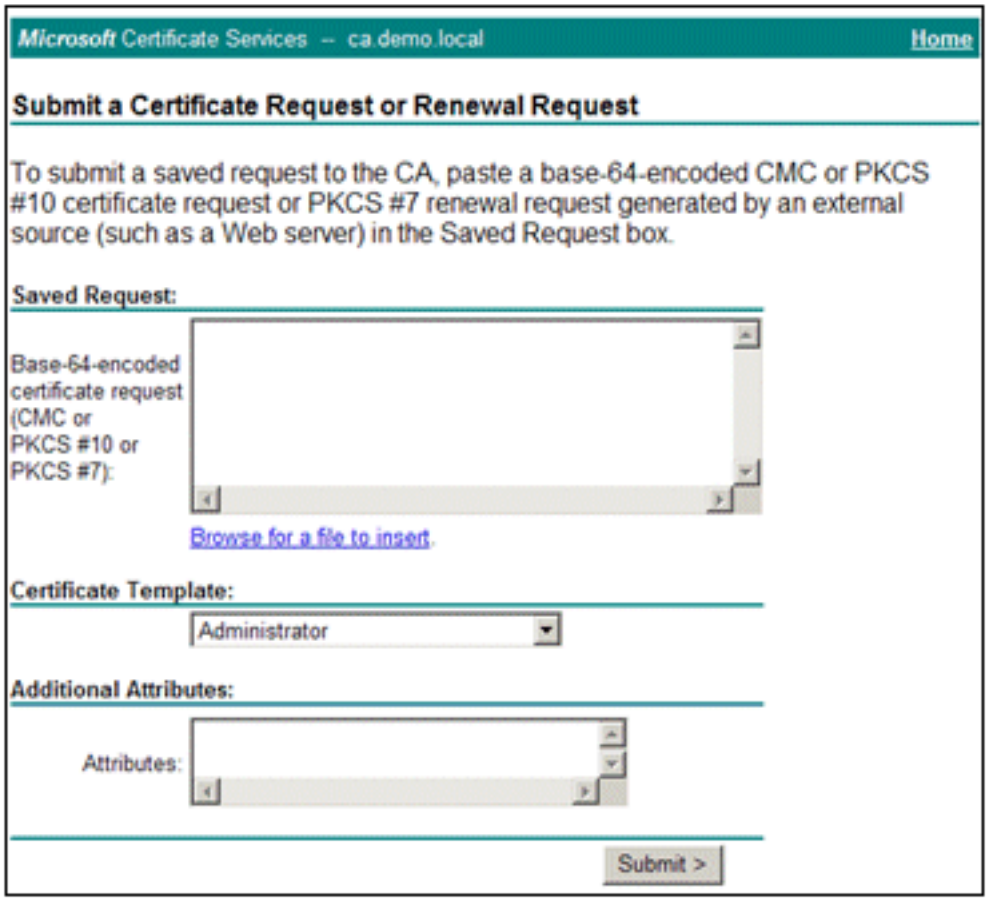


3. 按一下以提交高**級證書請求**。
4. 在高級請求中，按一下**Submit a certificate request using a base-64-**

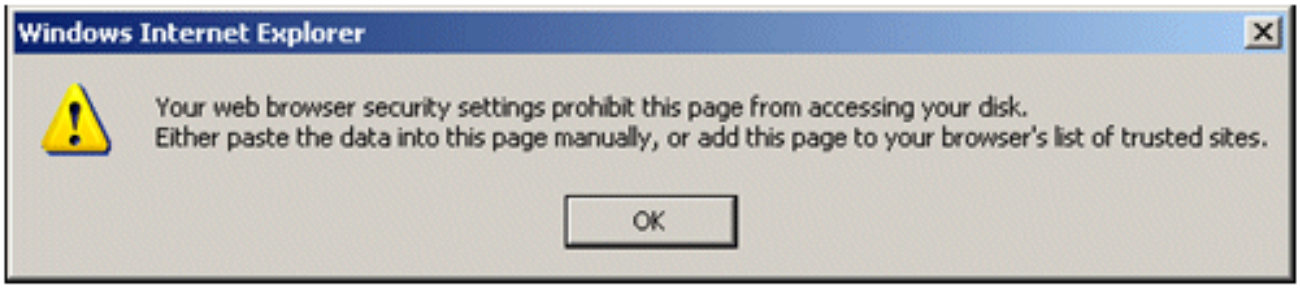


encoded...

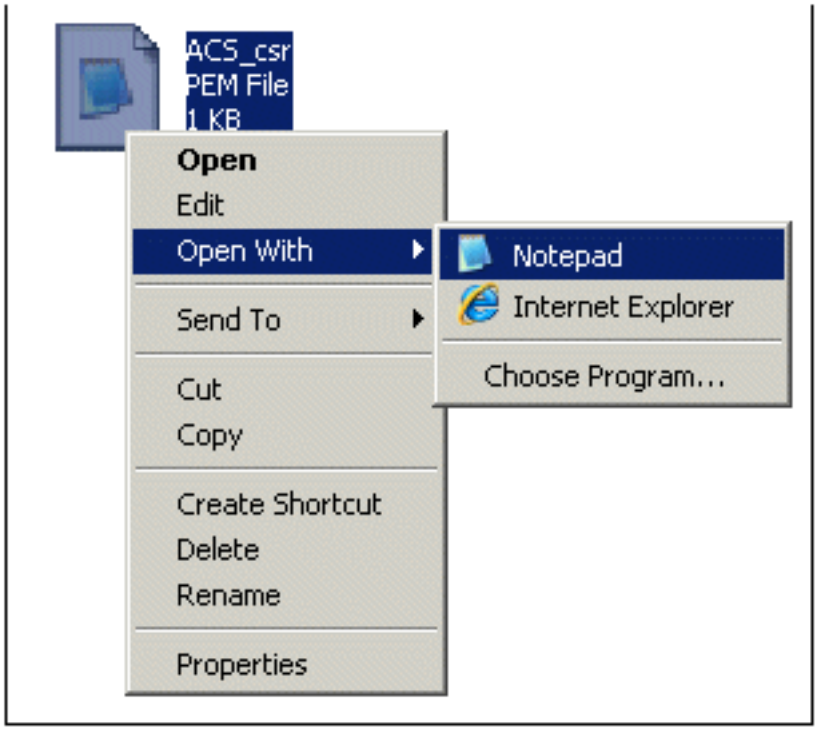
5. 在Saved Request欄位中，如果瀏覽器安全允許，瀏覽到以前的ACS證書請求檔案並插入。



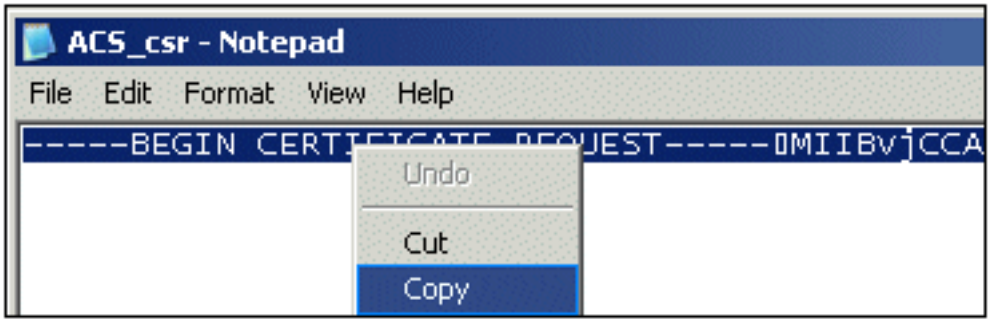
6. 瀏覽器的安全設定可能不允許訪問磁碟上的檔案。如果是，請按一下**OK**執行手動貼上。



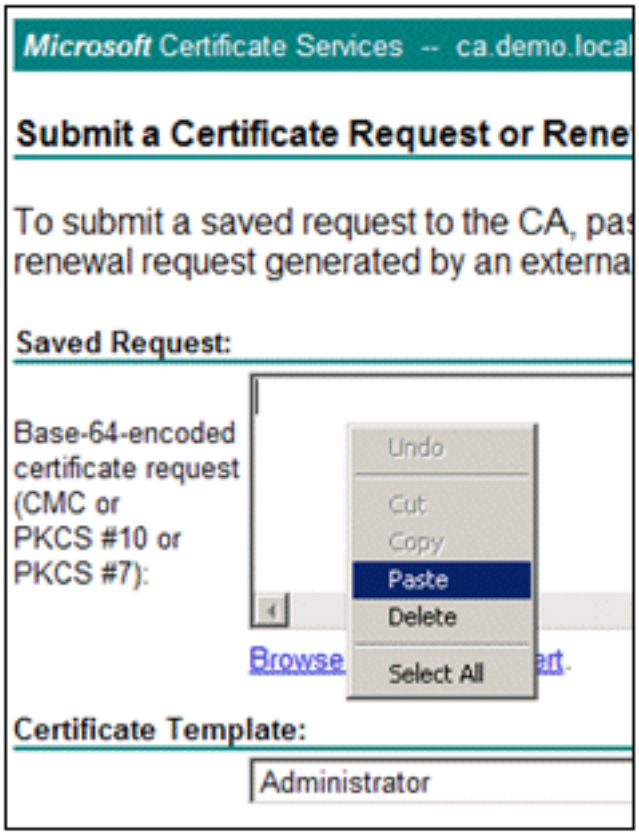
7. 從以前的ACS匯出中找到ACS *.pem檔案。使用文字編輯器開啟檔案（例如記事本）。



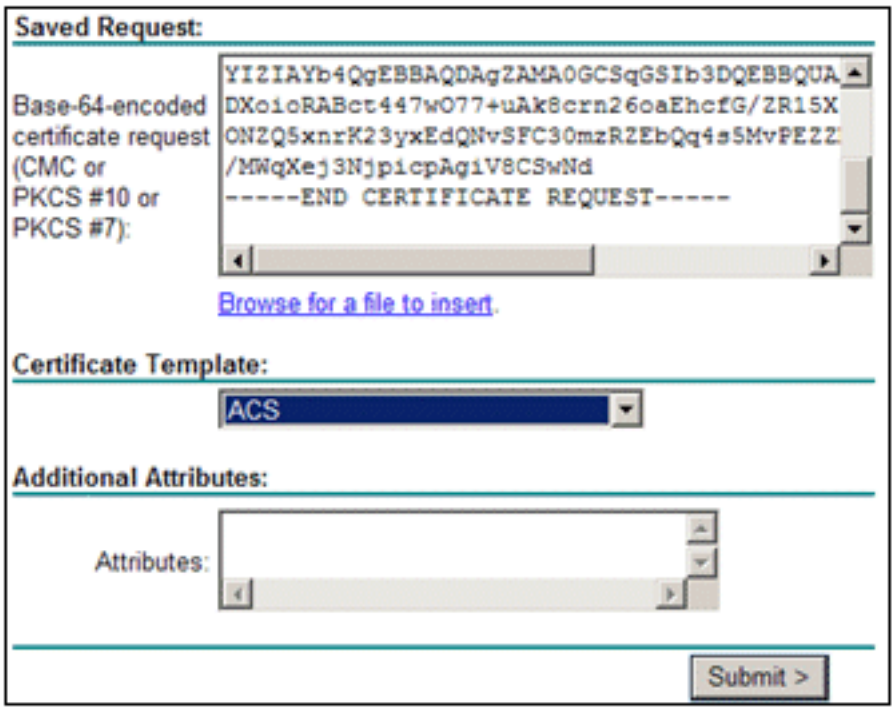
8. 突出顯示檔案的整個內容，然後按一下**Copy**。



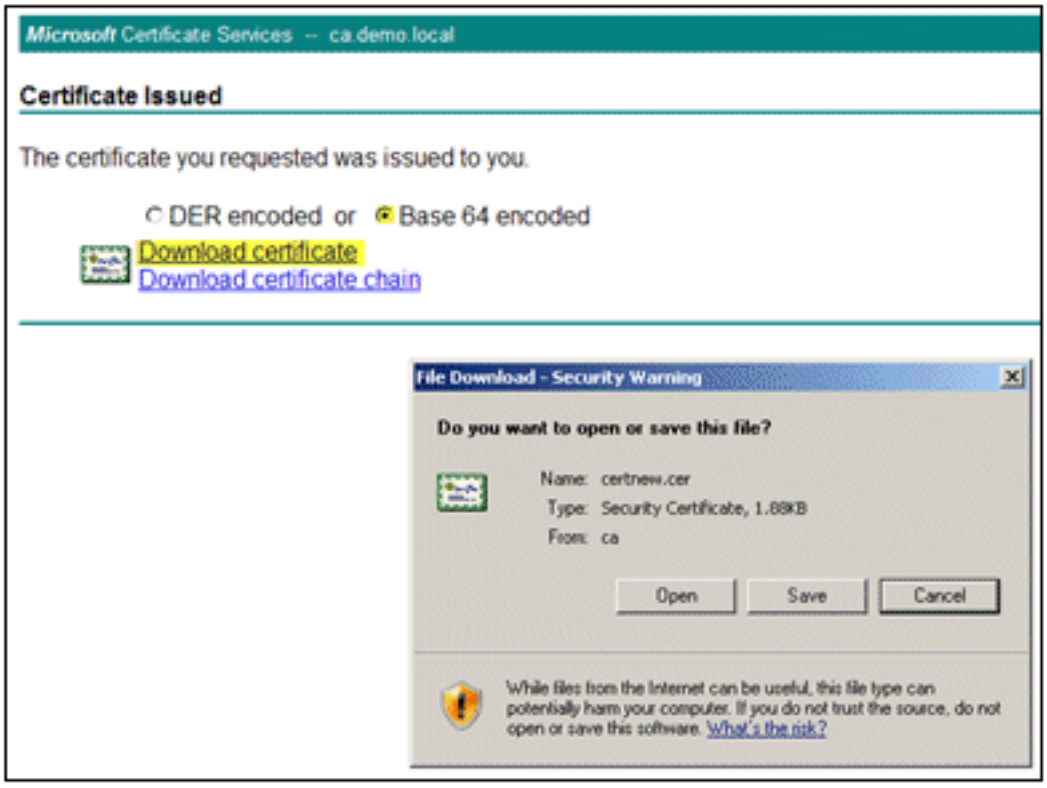
9. 返回到Microsoft證書請求視窗。**將複製**的內容貼上到「已儲存請求」欄位中。



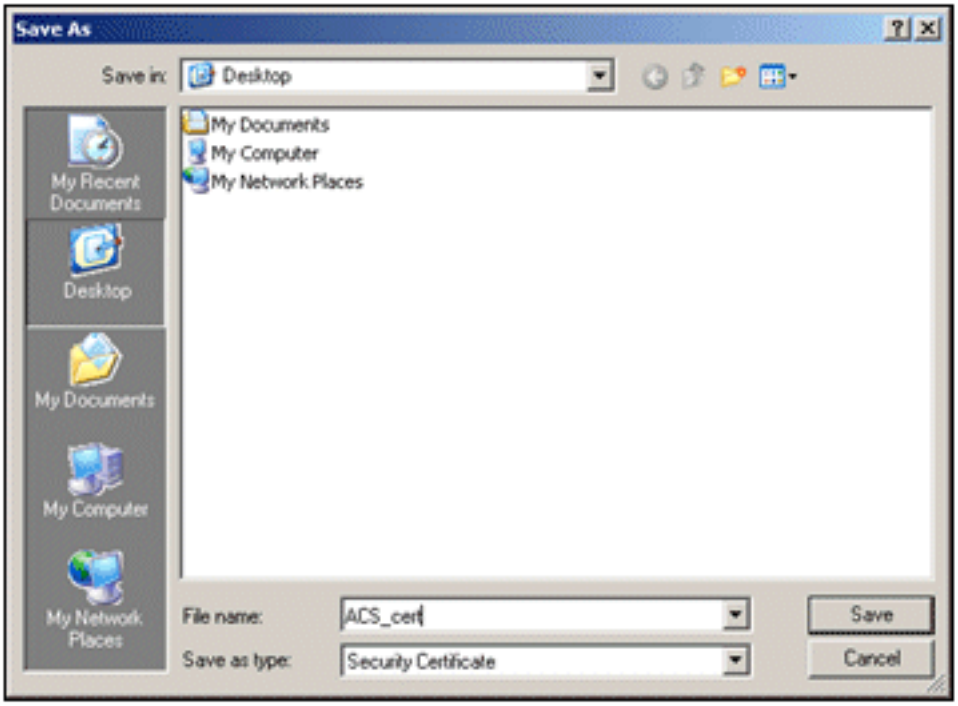
10. 選擇ACS作為證書模板，然後按一下Submit。



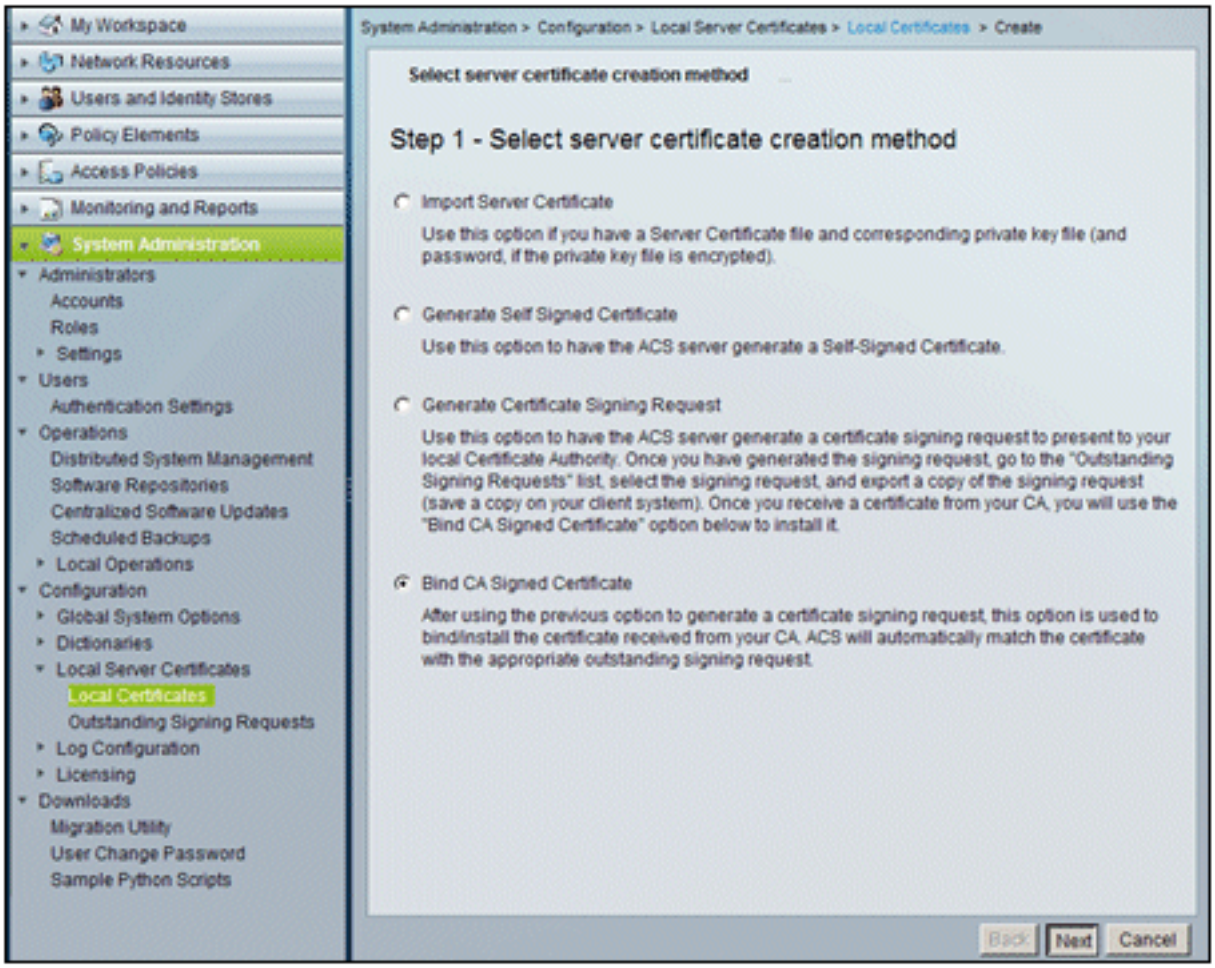
11. 憑證核發後，選擇Base 64 encoded，然後按一下Download certificate。



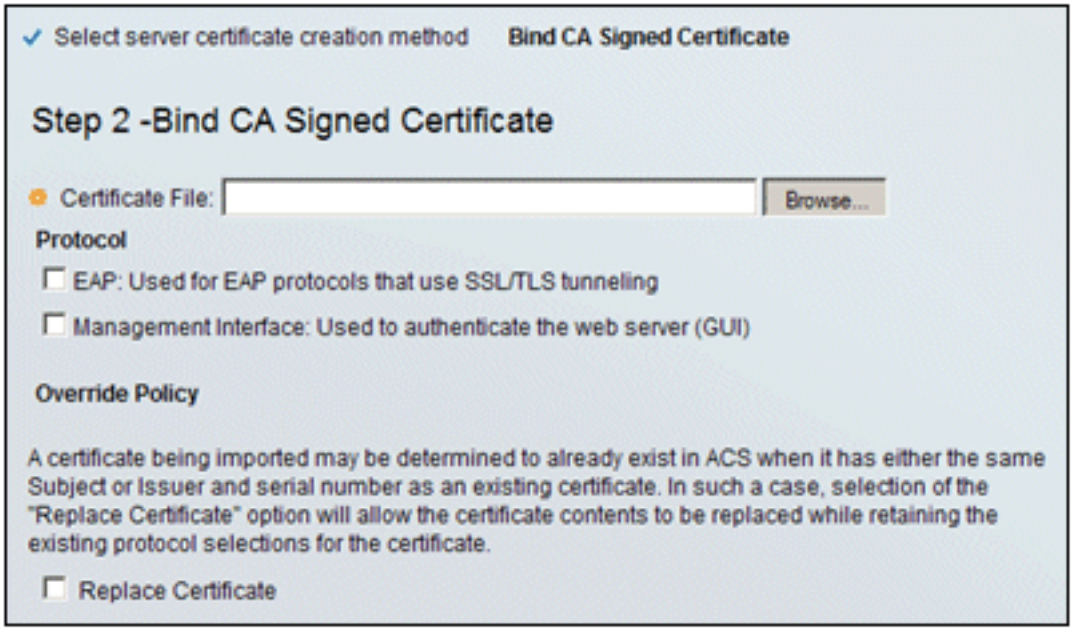
12. 按一下「Save」將憑證儲存到案頭上。



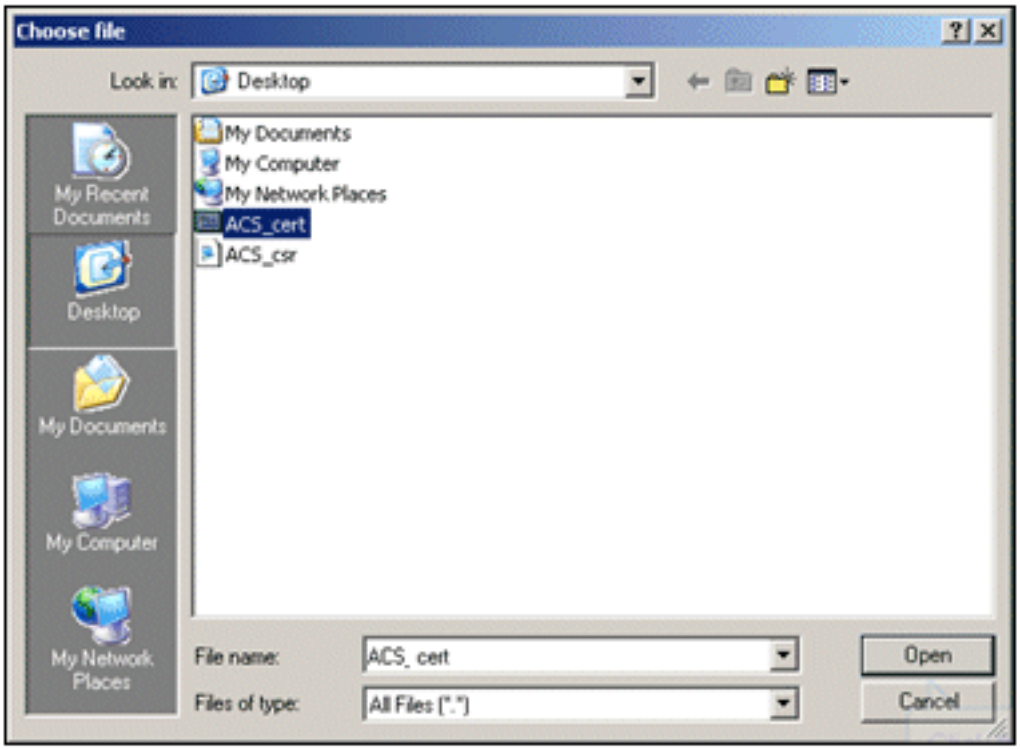
13. 前往**ACS > System Administration > Configuration > Local Server Certificates**。選擇**Bind CA Signed Certificate**，然後按一下**Next**。



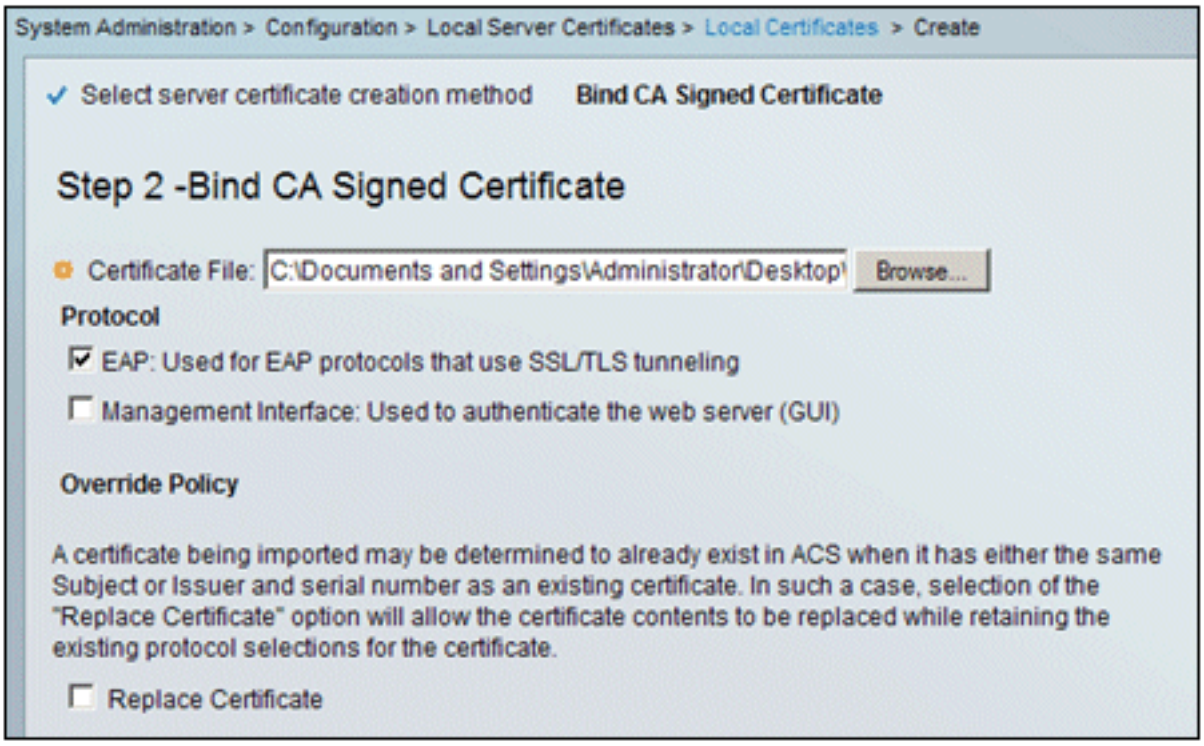
14. 按一下「**Browse**」，然後找到儲存的憑證。



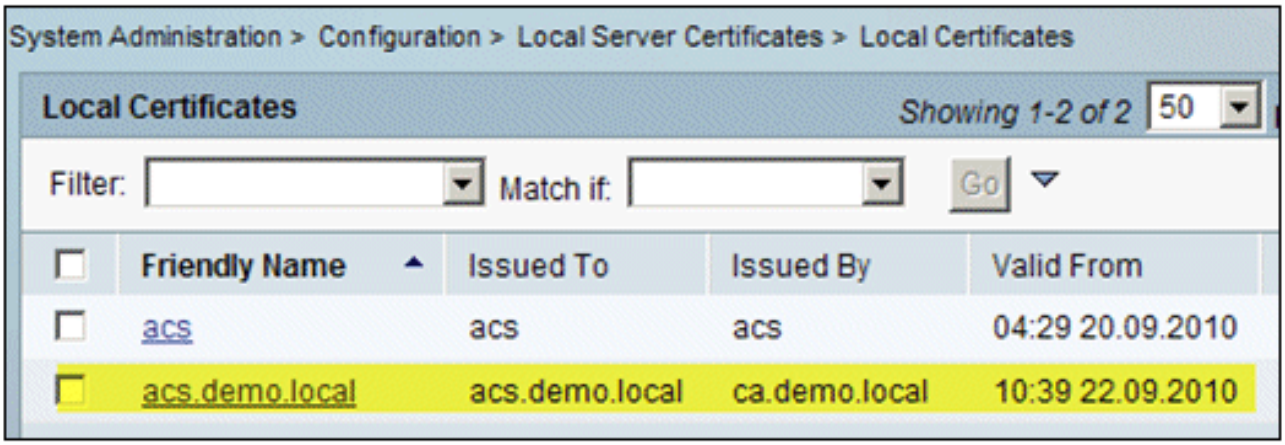
15. 選擇CA伺服器頒發的ACS證書，然後按一下**Open**。



16. 此外，選中**EAP**的Protocol框，然後按一下**Finish**。



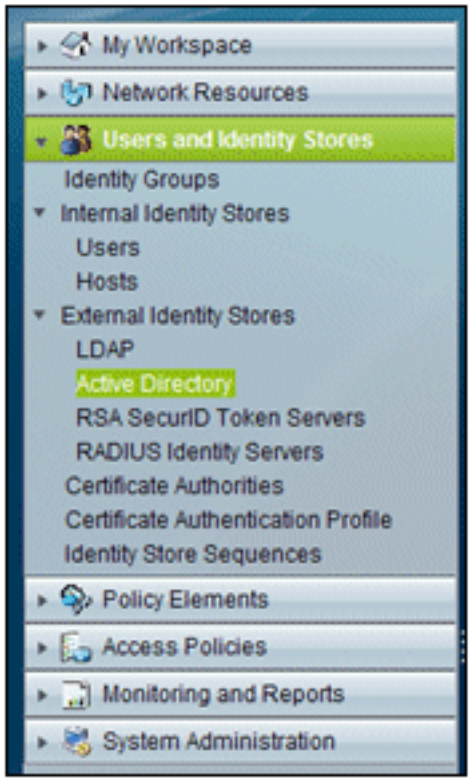
17. CA頒發的ACS證書將顯示在ACS本地證書中。



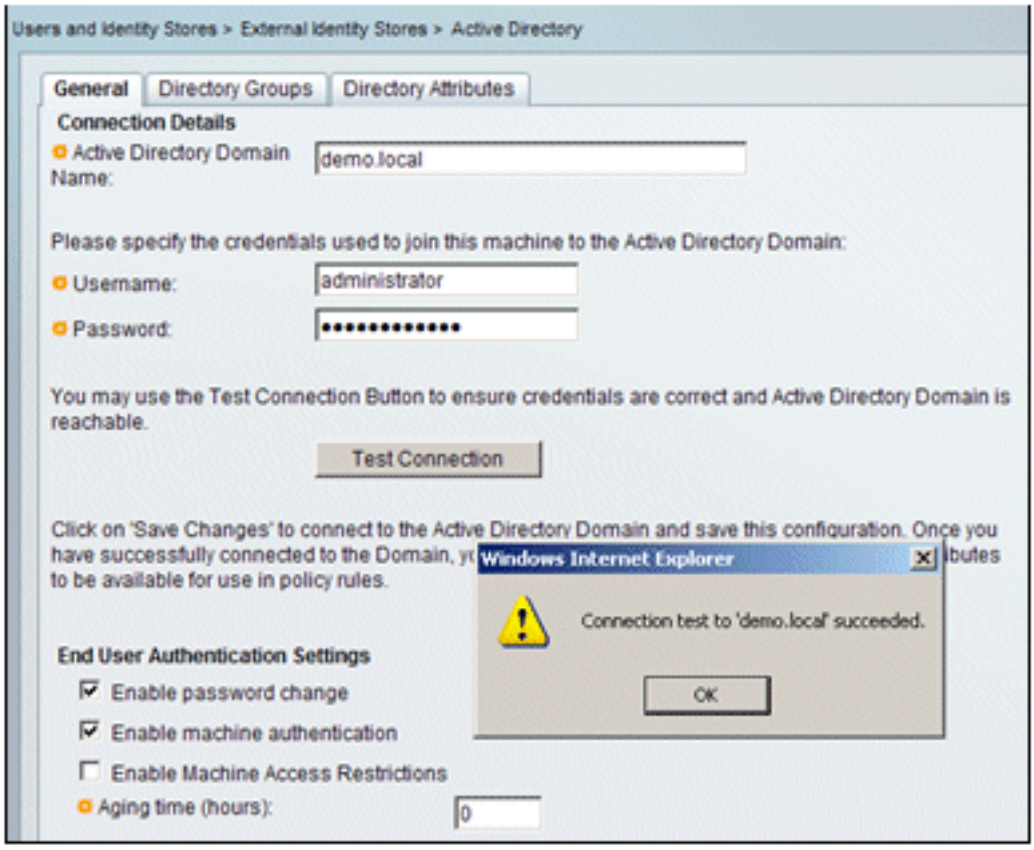
為Active Directory配置ACS身份儲存

執行以下步驟：

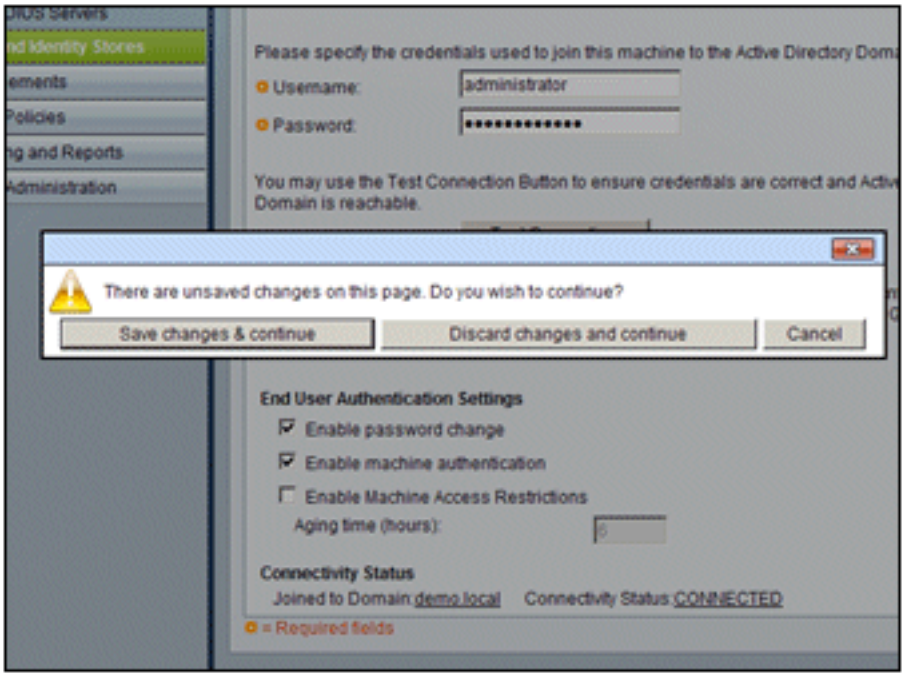
1. 連線到ACS並使用管理員帳戶登入。



2. 轉至**使用者和身份庫 > 外部身份庫 > Active Directory**。
3. 輸入Active Directory域*demo.local*，輸入伺服器的密碼，然後按一下**測試連線**。按一下「OK」以繼續。



4. 按一下「**Save Changes**」。

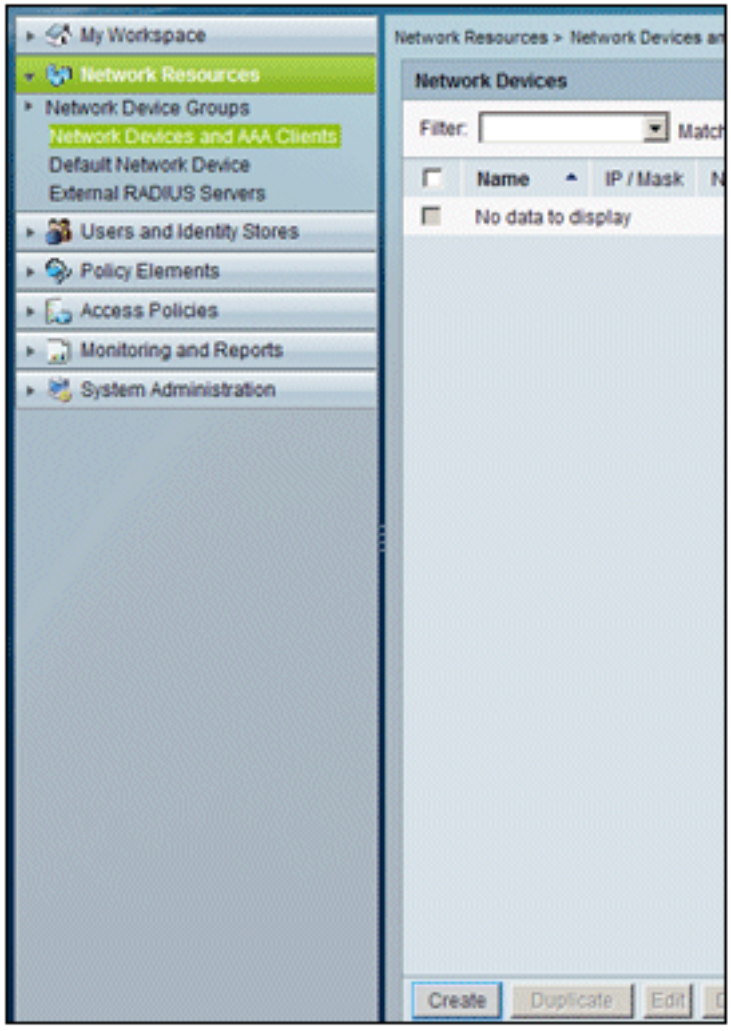


注意：有關ACS 5.x整合過程的詳細資訊，請參閱[ACS 5.x及更高版本：與Microsoft Active Directory整合配置示例](#)。

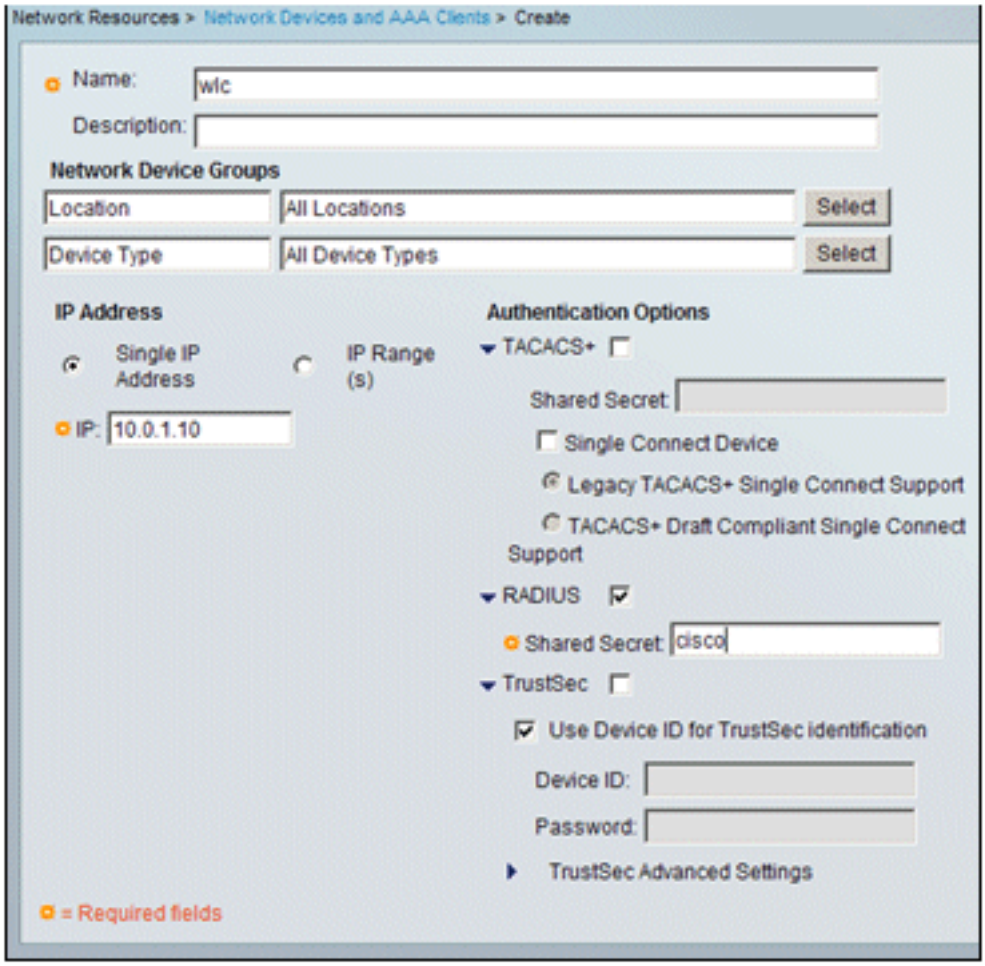
將控制器作為AAA客戶端新增到ACS

執行以下步驟：

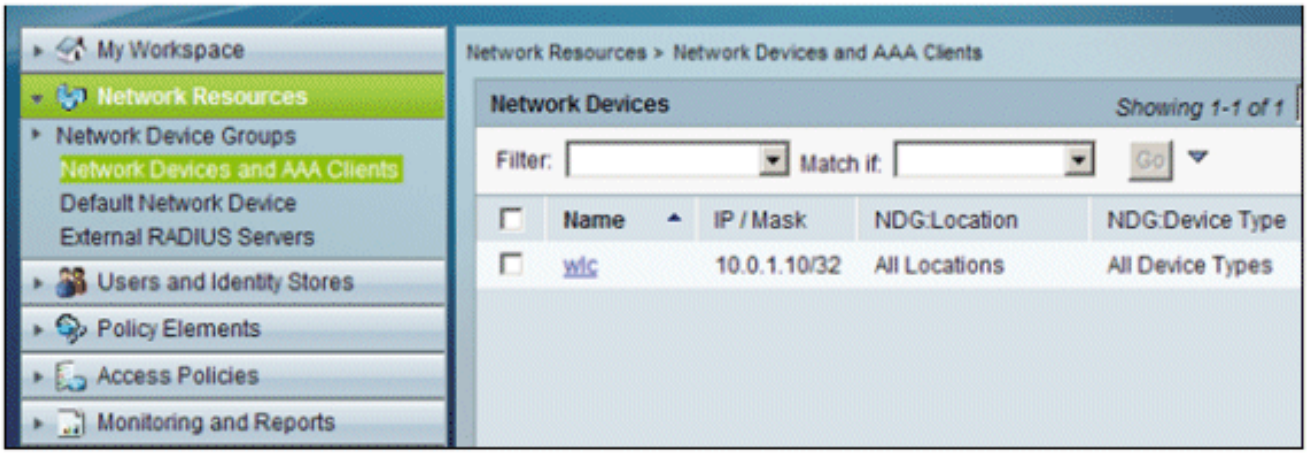
1. 連線到ACS，然後轉到**Network Resources > Network Devices and AAA Clients**。按一下「**Create**」。



2. 輸入以下欄位：名稱 — **wlc**IP - **10.0.1.10**RADIUS霰取方塊 — 已**選中**共用密碼 — **cisco**



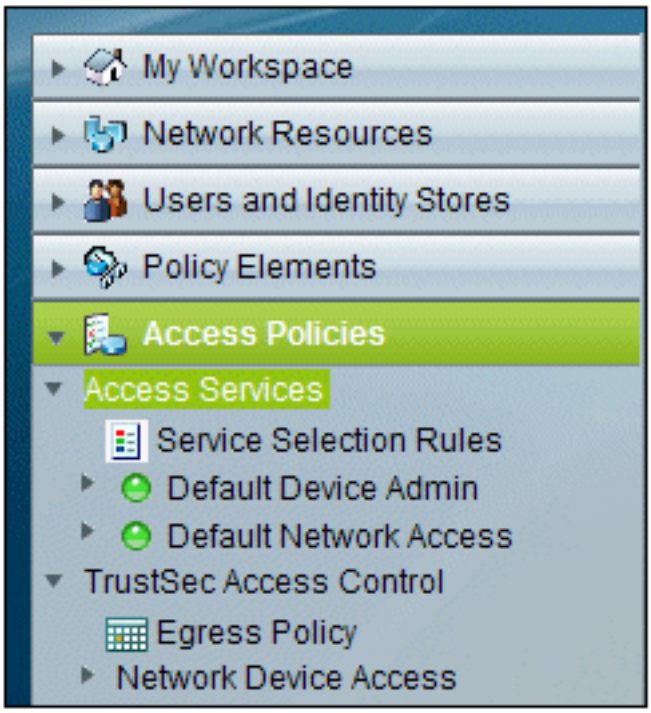
3. 完成後按一下**Submit**。控制器將顯示為ACS網路裝置清單中的條目。



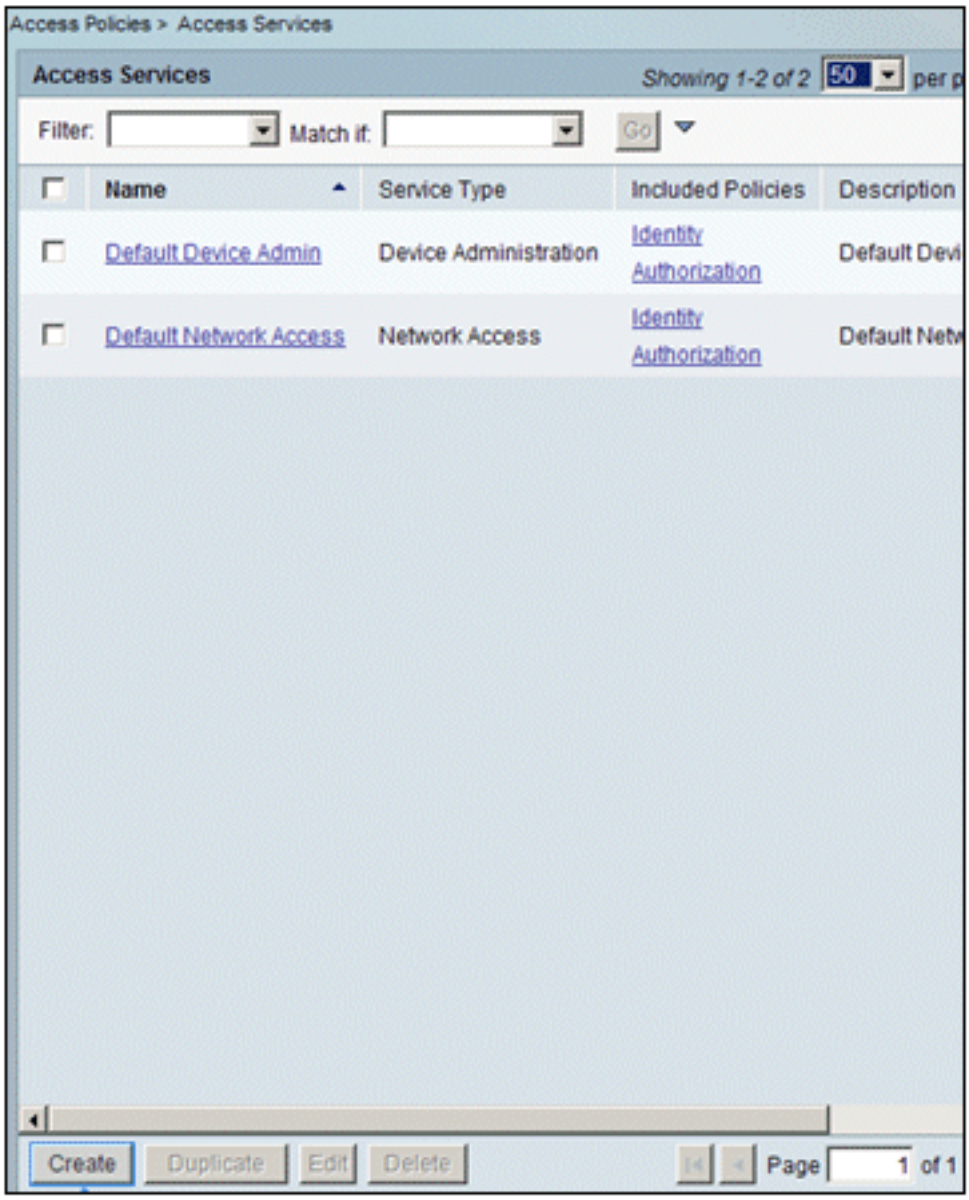
配置無線的ACS訪問策略

執行以下步驟：

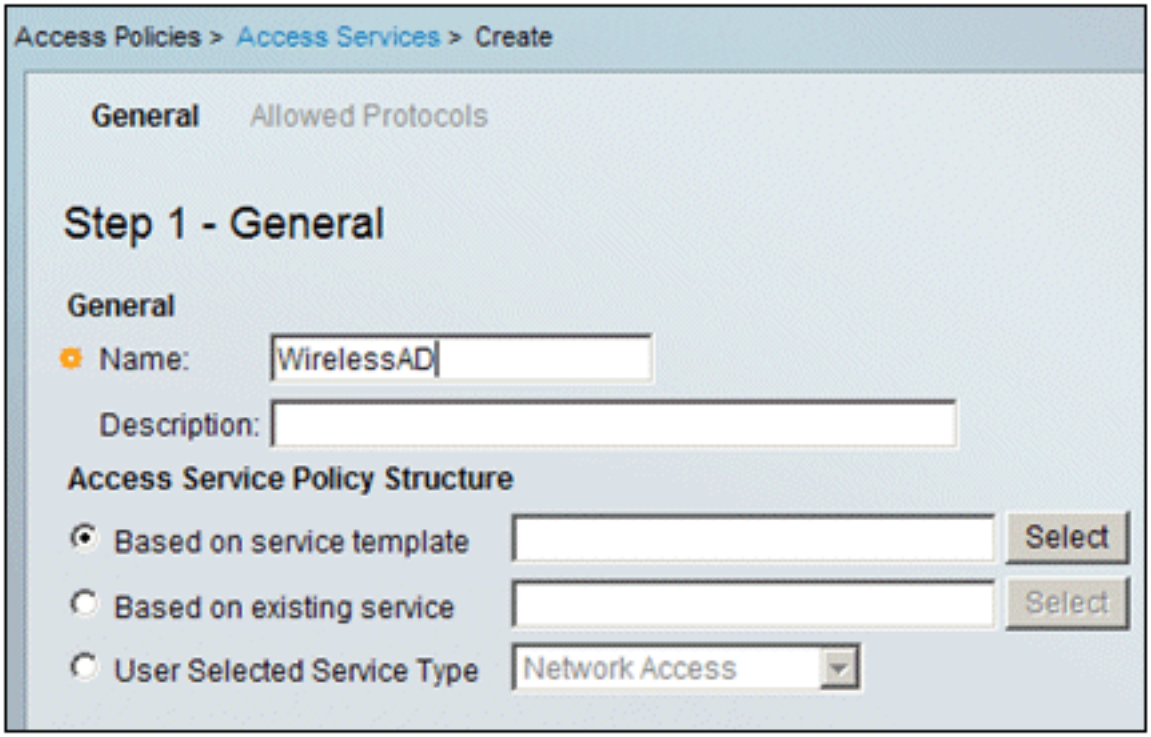
1. 在ACS中，轉至**Access Policies > Access Services**。



2. 在Access Services視窗中，按一下**Create**。

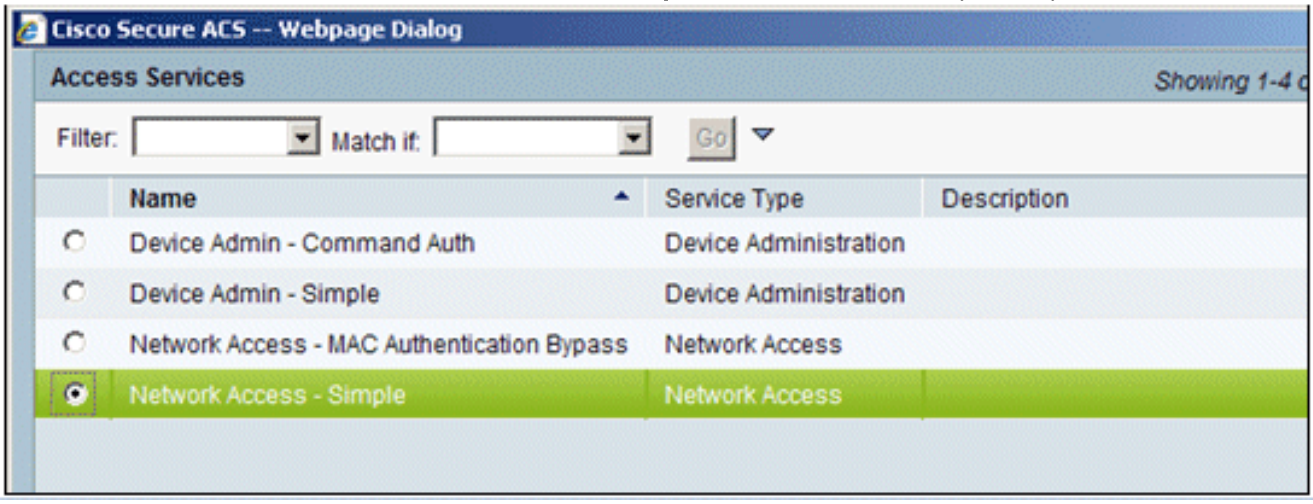


3. 建立訪問服務，並輸入名稱（例如WirelessAD）。選擇**Based on service template**，然後按一

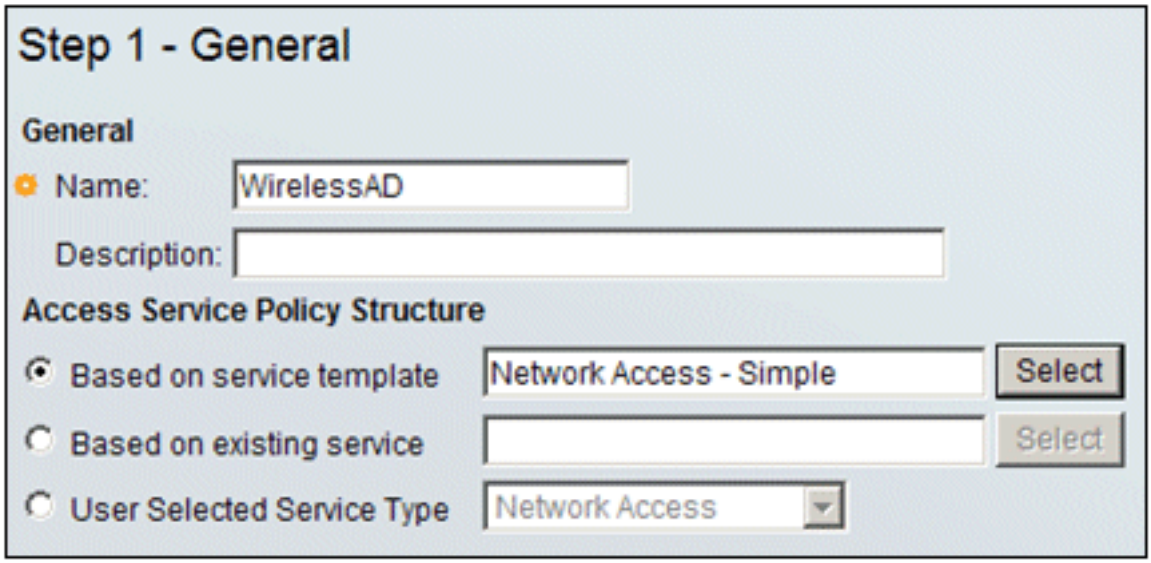


下**Select**。

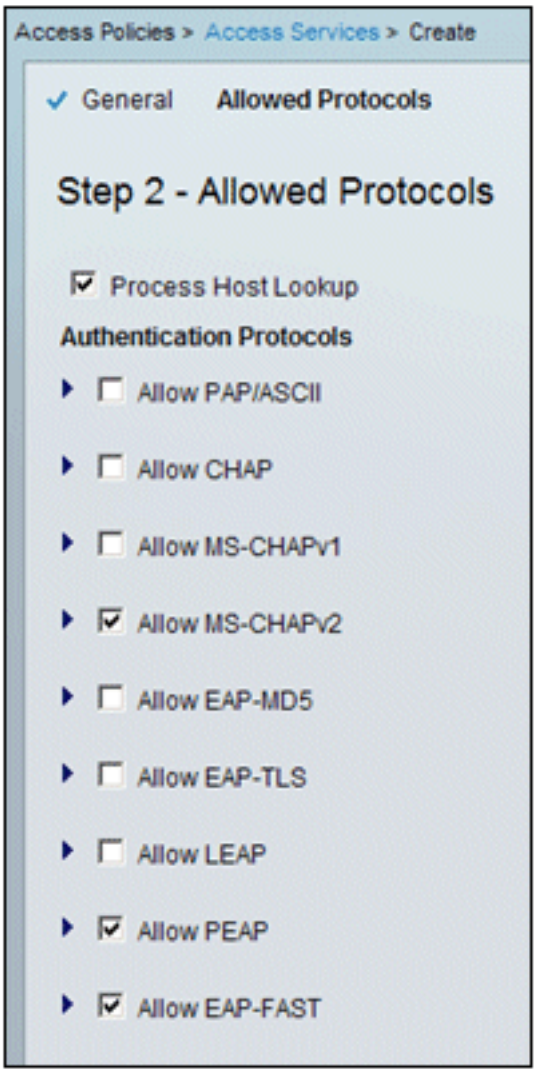
4. 在網頁對話方塊中，選擇**Network Access - Simple**。按一下「**OK**」（確定）。



5. 在網頁對話方塊中，選擇**Network Access - Simple**。按一下「**OK**」（確定）。選擇模板後，按一下**下一步**。

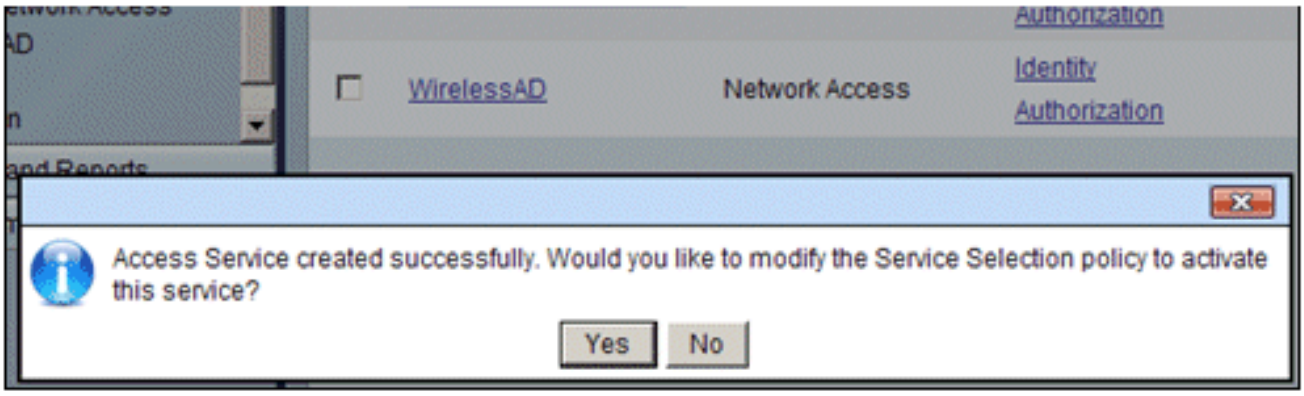


6. 在Allowed Protocols下，選中**Allow MS-CHAPv2**和**Allow PEAP**覈取方塊。按一下「**Finish**」

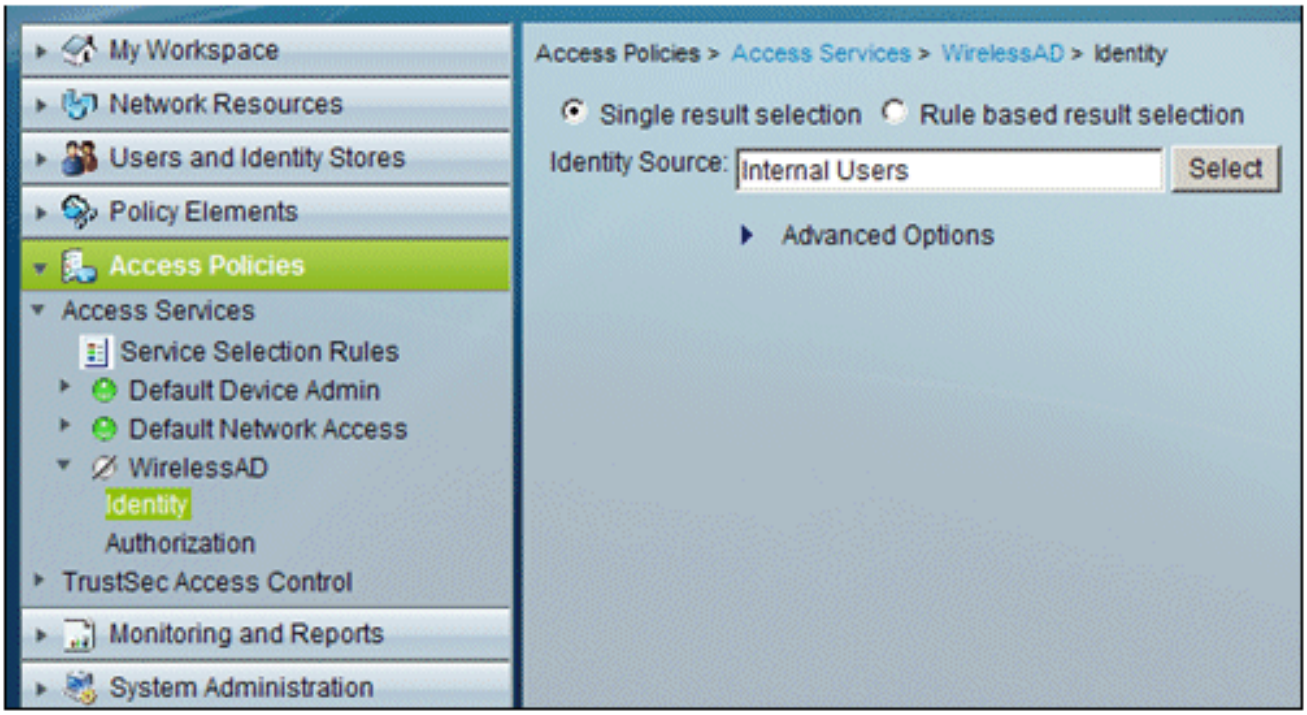


（結束）。

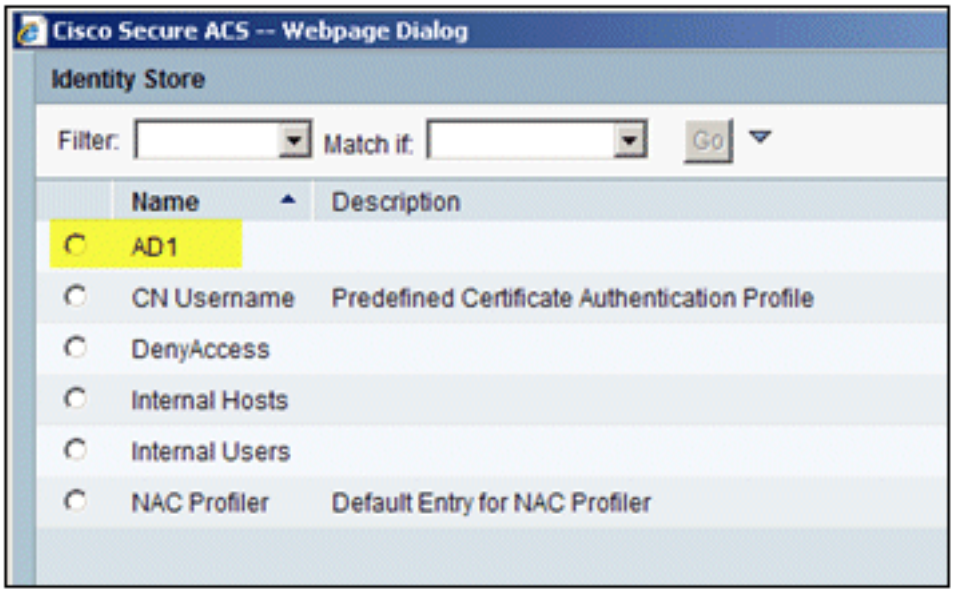
7. 當ACS提示您啟用新服務時，按一下**Yes**。



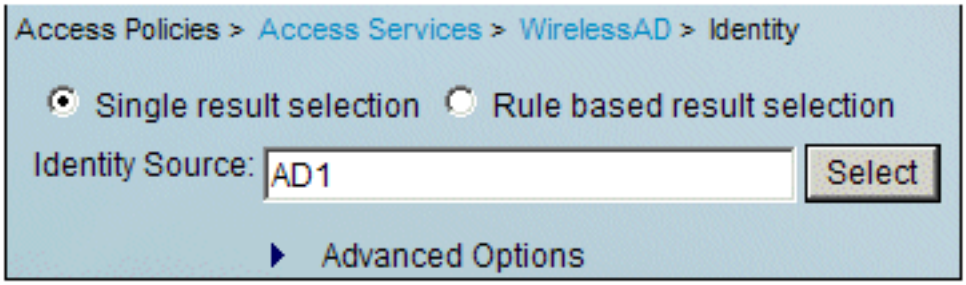
8. 在剛剛建立/啟用的新訪問服務中，展開並選擇**身份**。對於身份源，按一下**選擇**。



9. 為ACS中配置的Active Directory選擇**AD1**，然後按一下**OK**。



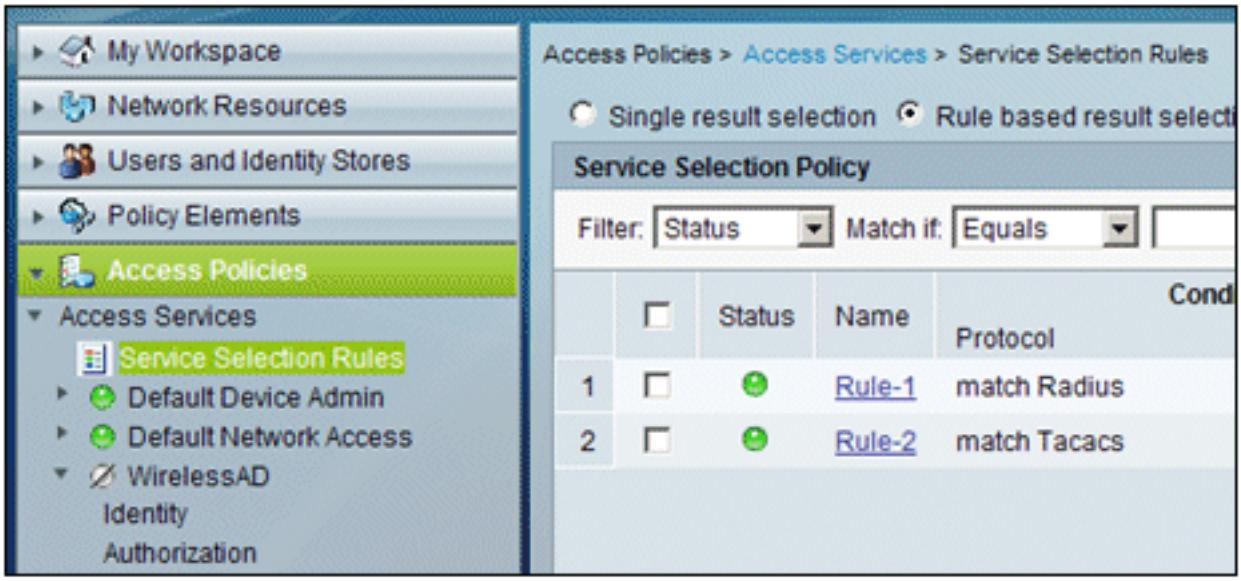
10. 確認身份源為AD1，然後按一下**Save Changes**。



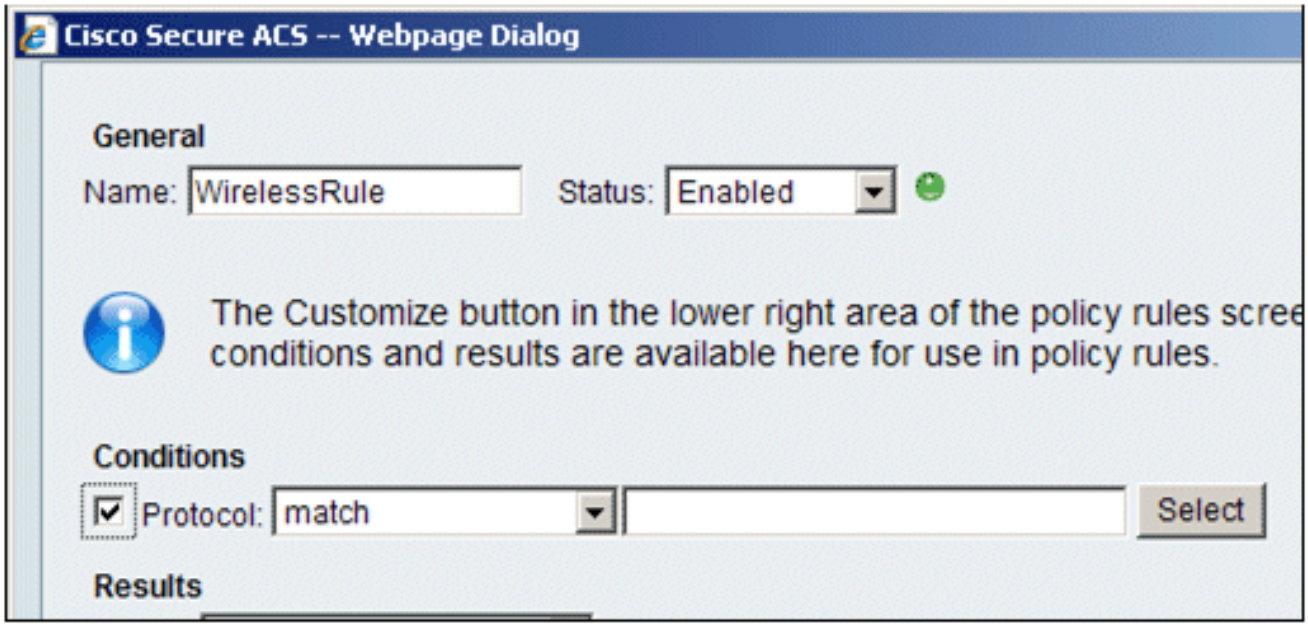
建立ACS訪問策略和服務規則

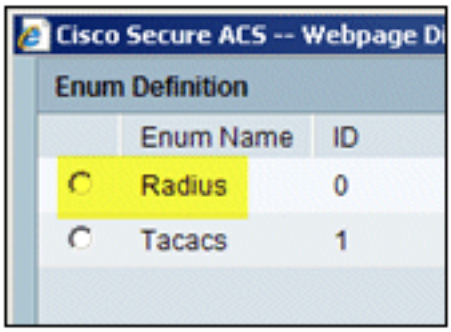
執行以下步驟：

1. 轉至**Access Policies > Service Selection Rules**。

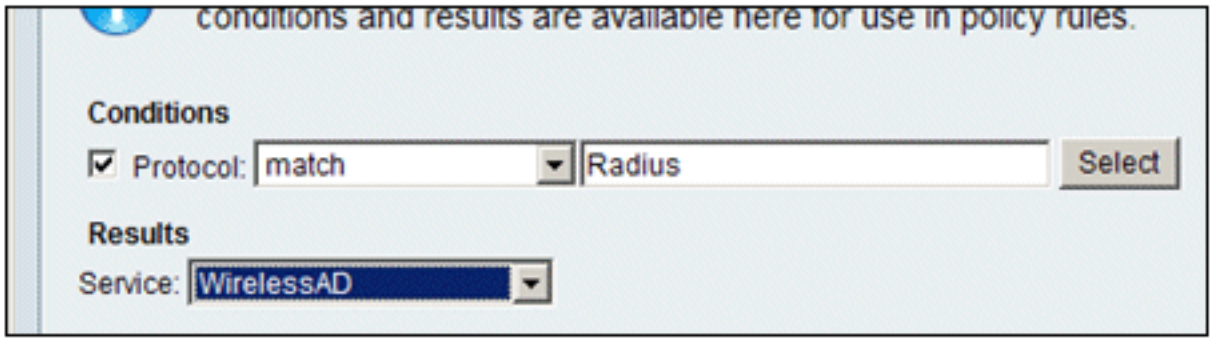


2. 在Service Selection Policy視窗中按一下**Create**。為新規則指定一個名稱(例如*WirelessRule*)。選中**Protocol**以匹配**Radius**的覈取方塊。

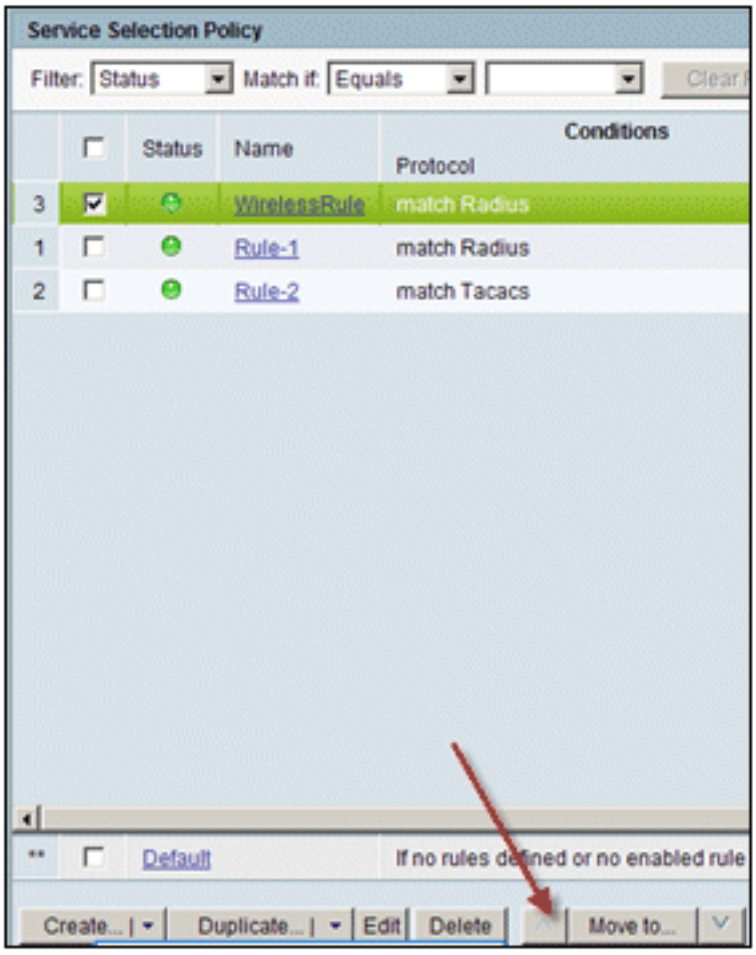




3. 選擇「**Radius**」，然後按一下「**OK**」。
4. 在「結果」下，選擇**WirelessAD** for Service（在上一步中建立）。



5. 建立新的無線規則後，選擇並上移**此規則**，這將是使用Active Directory識別無線radius身份驗證的第一個規則。



使用Windows零接觸的PEAP客戶端配置

在我們的示例中，CLIENT是運行Windows XP Professional with SP的電腦，充當無線客戶端，通過無線AP獲得對Intranet資源的訪問。完成本節中的步驟，將CLIENT配置為無線客戶端。

執行基本安裝和配置

執行以下步驟：

1. 使用連線到集線器的乙太網電纜將CLIENT連線到Intranet網段。
2. 在CLIENT上，將Windows XP Professional with SP2安裝為demo.local域名為CLIENT的成員電腦。
3. 安裝Windows XP Professional with SP2。必須安裝該元件才能獲得PEAP支援。**注意**：Windows XP Professional SP2中會自動開啟Windows防火牆。請勿關閉防火牆。

安裝無線網路介面卡

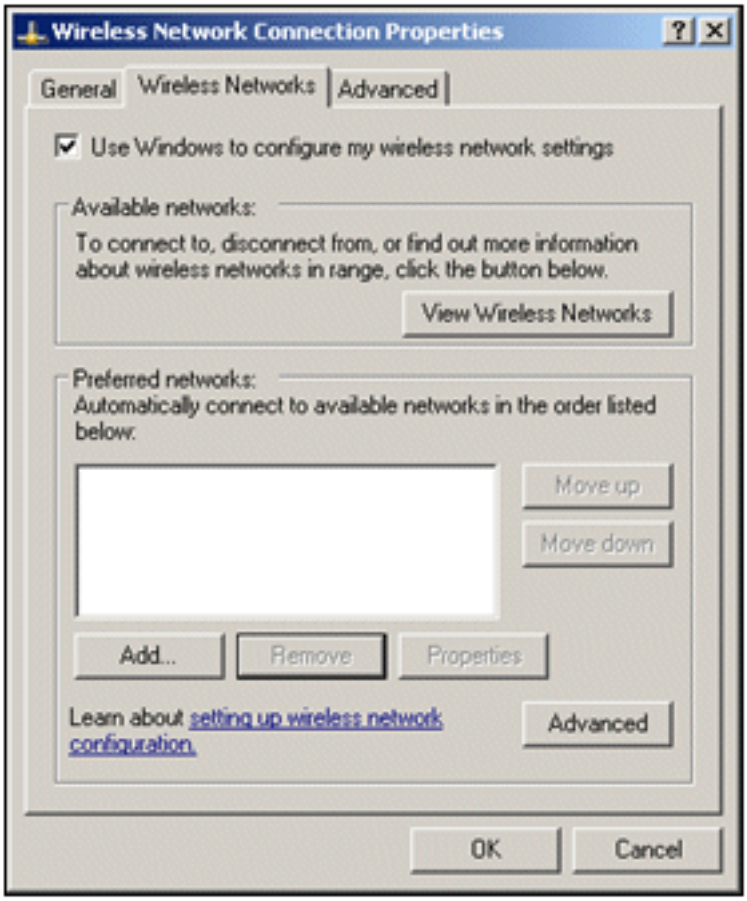
執行以下步驟：

1. 關閉客戶端電腦。
2. 從Intranet網段斷開客戶端電腦。
3. 重新啟動CLIENT電腦，然後使用本地管理員帳戶登入。
4. 安裝無線網路介面卡。**註：**請勿為無線介面卡安裝製造商的配置軟體。使用「Add Hardware Wizard（新增硬體嚮導）」安裝無線網路介面卡驅動程式。此外，在出現提示時，請提供製造商提供的CD或包含更新驅動程式的磁碟，以用於Windows XP Professional with SP2。

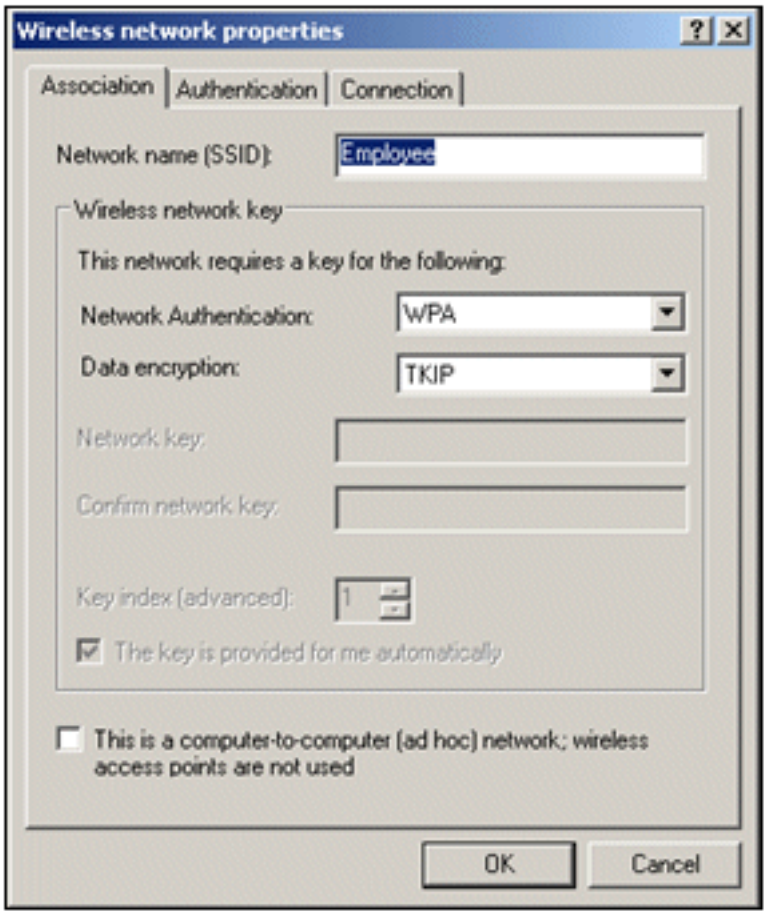
配置無線網路連線

執行以下步驟：

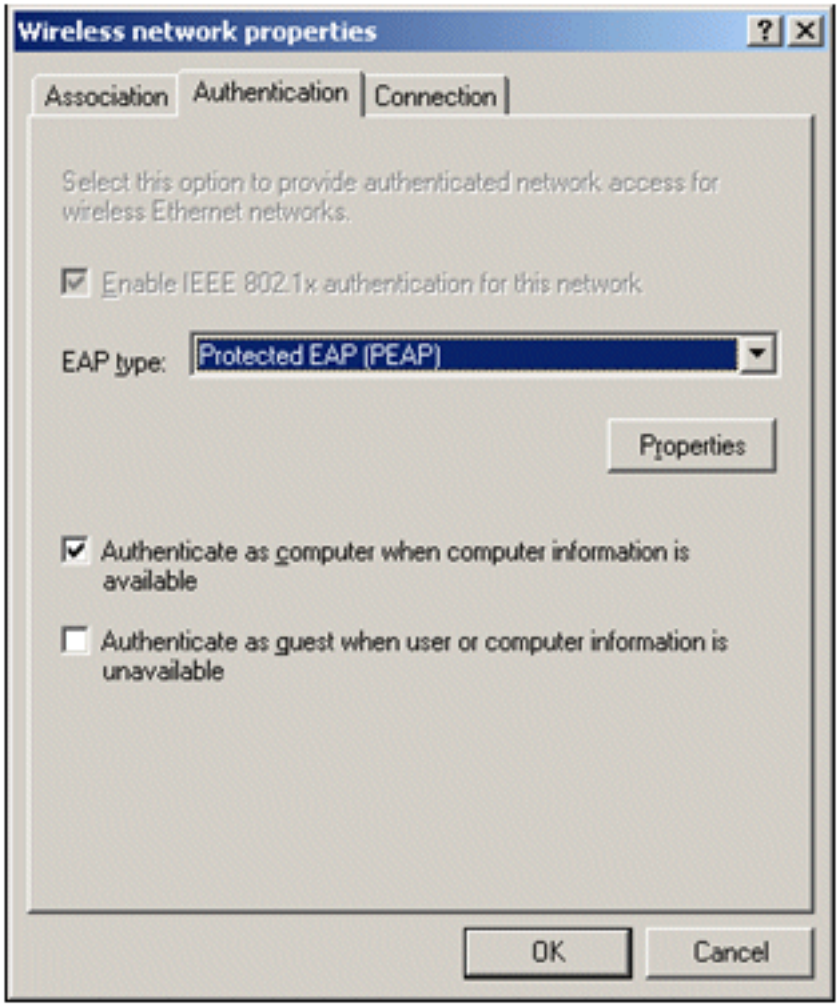
1. 註銷，然後使用**demo.local域**中的WirelessUser**帳戶登**入。
2. 選擇**Start > Control Panel**，按兩下**Network Connections**，然後按一下右鍵**Wireless Network Connection**。
3. 按一下**Properties**，轉到**Wireless Networks**頁籤，並確保已選中**Use Windows to configure my wireless network settings**。



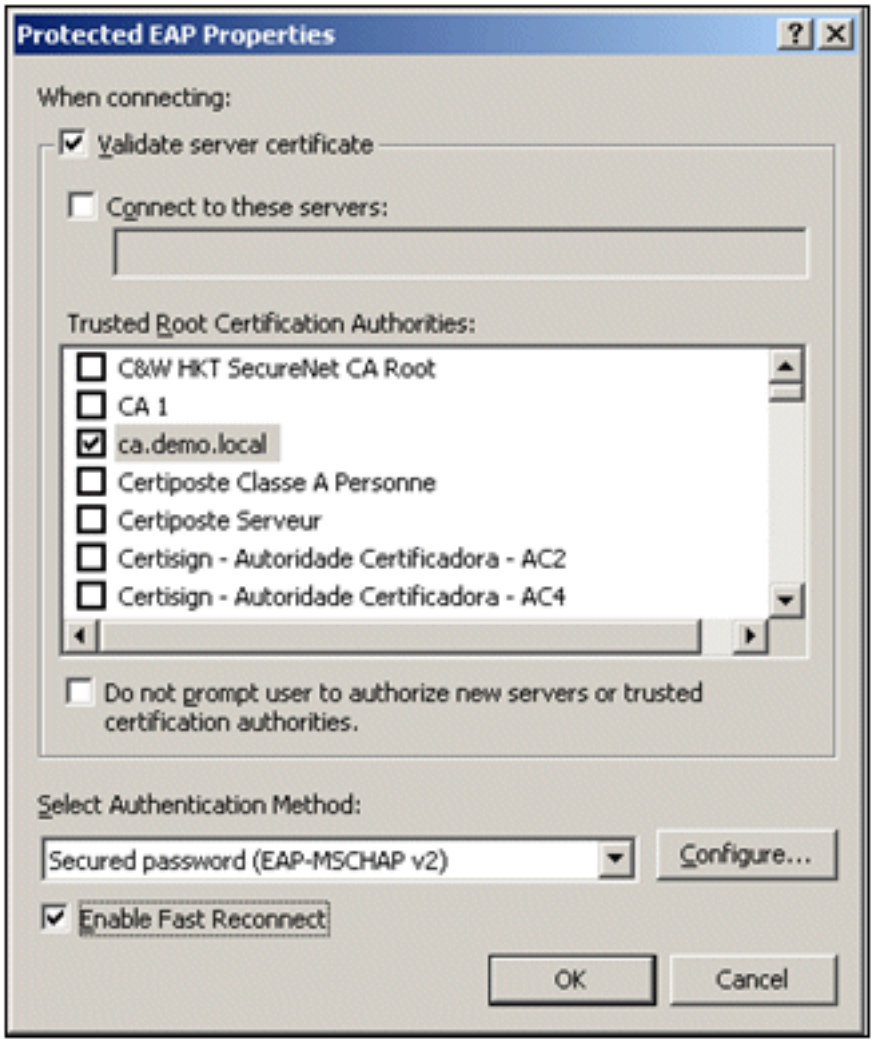
4. 按一下「**Add**」。
5. 在Association頁籤的Network name(SSID)欄位中輸入*Employee*。
6. 為網路身份驗證選擇**WPA**，並確保資料加密設定為**TKIP**。



7. 按一下**Authentication**頁籤。
8. 驗證EAP型別是否配置為使用**受保護的EAP(PEAP)**。如果沒有，則從下拉選單中選擇該選項。
9. 如果您希望在登入之前驗證電腦（這允許應用登入指令碼或組策略推送），請選中**Authenticate as computer when computer information available**。



10. 按一下「**Properties**」。
11. 由於PEAP涉及客戶端對伺服器的身份驗證，請確保選中**Validate server certificate**。此外，請確保在Trusted Root Certification Authorities（受信任的根證書頒發機構）選單下檢查頒發了ACS證書的CA。
12. 在Authentication Method下選擇**Secure password(EAP-MSCHAP v2)**，因為它用於內部身份



驗證。

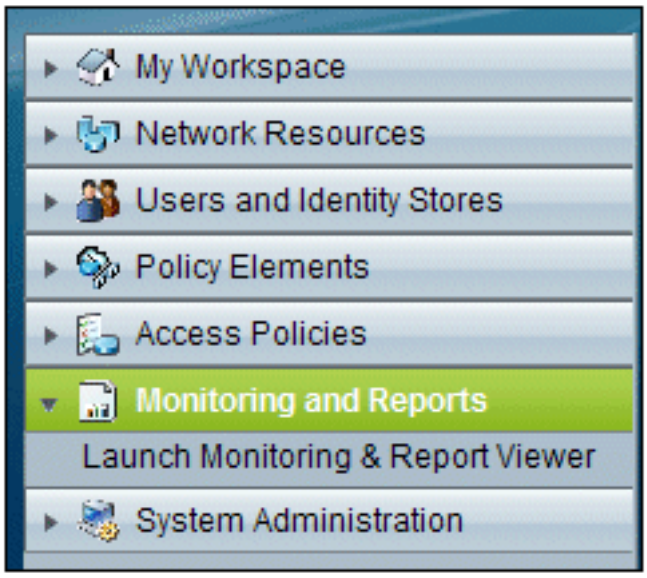
13. 確保選中**Enable Fast Reconnect**覈取方塊。然後，按一下**OK**三次。
14. 按一下右鍵systray中的無線網路連線圖示，然後按一下**View Available Wireless Networks**。
15. 按一下員工無線網路，然後按一下**Connect**。如果連線成功，無線客戶端將顯示**Connected**。

16. 身份驗證成功後，使用網路連線檢查無線介面卡的TCP/IP配置。從DHCP範圍或為CorpNet無線客戶端建立的範圍中，它的地址範圍應為10.0.20.100-10.0.20.200。
17. 若要測試功能，請開啟瀏覽器並瀏覽**http://10.0.10.10**（或CA伺服器的IP位址）。

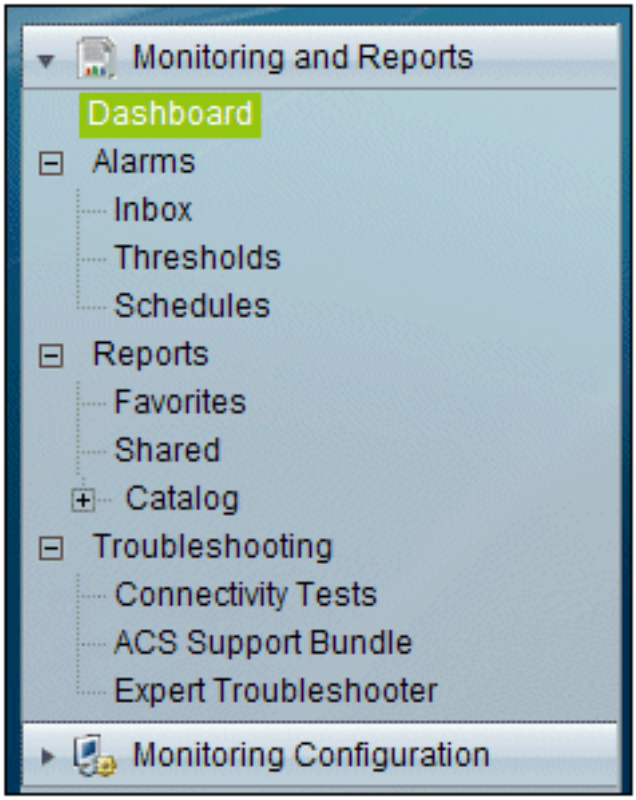
使用ACS排除無線身份驗證故障

執行以下步驟：

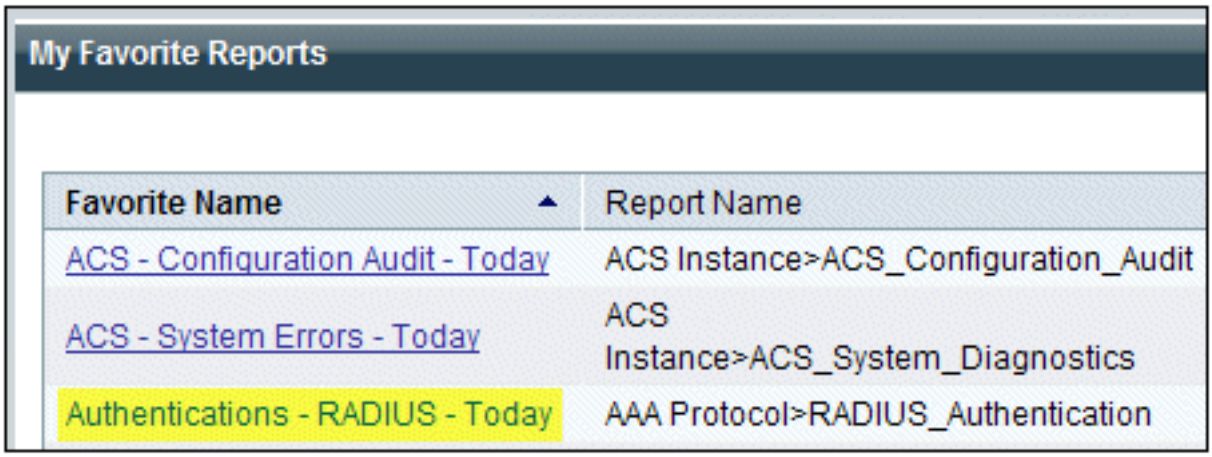
1. 轉至**ACS > Monitoring and Reports**，然後按一下**Launch Monitoring & Report Viewer**。



2. 將會開啟單獨的ACS視窗。按一下**Dashboard**。

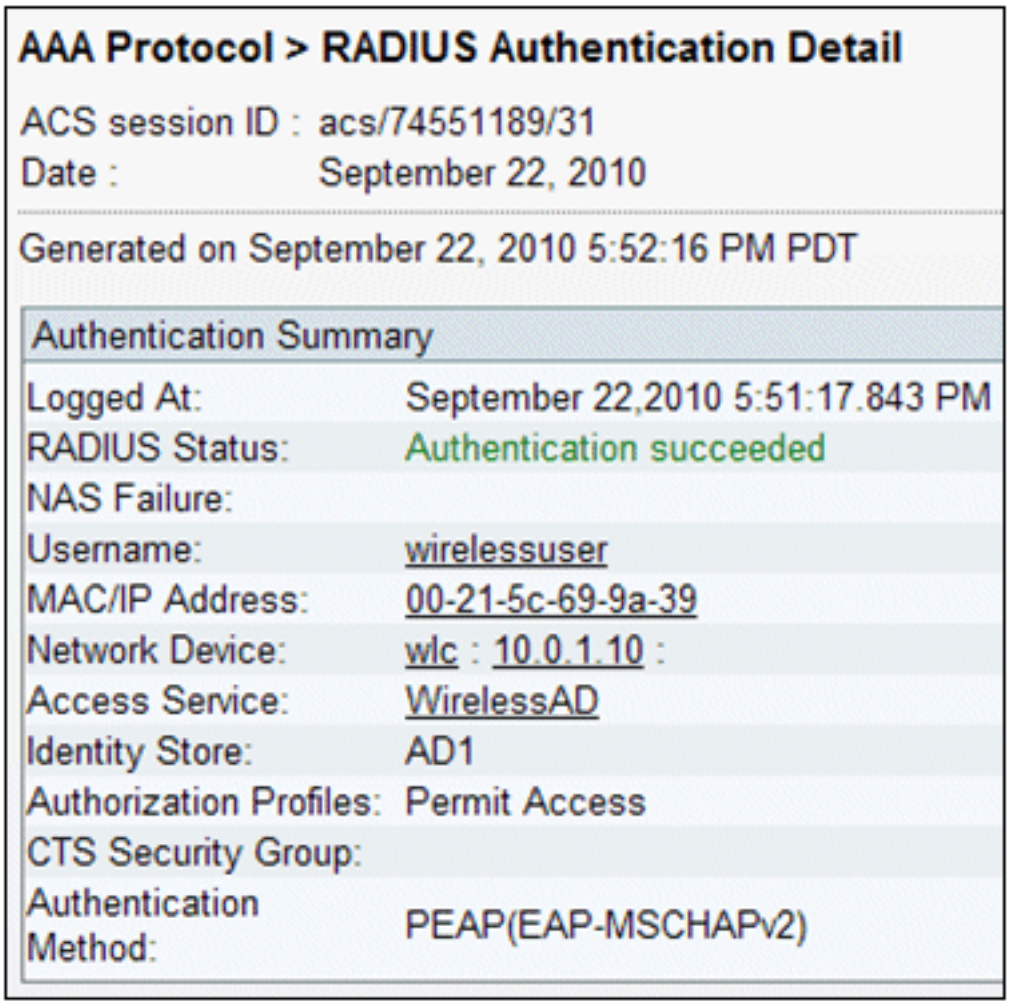


3. 在「My Favorite Reports（我的收藏夾報告）」部分，按一下**Authentications - RADIUS - Today**。

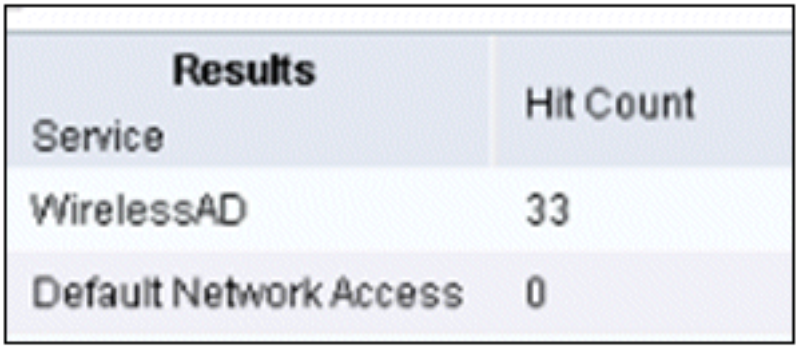


4. 日誌將顯示所有RADIUS身份驗證為通過或失敗。在記錄的條目中，按一下「詳細資訊」(Details)列中的放大鏡圖示。

5. RADIUS Authentication Detail將提供許多有關記錄嘗試的資訊。



6. ACS服務命中計數可以提供與ACS中建立的規則相匹配的嘗試的概述。轉至**ACS > Access Policies > Access Services**，然後按一下**Service Selection Rules**。



ACS伺服器的PEAP身份驗證失敗

當您的客戶端未能通過ACS伺服器的PEAP身份驗證時，請檢查ACS的**報告和活動**選單下的**嘗試失敗**選項中是否找到NAS錯誤消息。

如果在客戶端電腦上安裝了Microsoft Windows XP SP2，並且Windows XP SP2對Microsoft IAS伺服器以外的第三方伺服器進行身份驗證，您可能會收到此錯誤消息。特別是，Cisco RADIUS伺服器(ACS)與Windows XP使用的方法不同，使用不同的方法來計算可擴充驗證通訊協定型別：長度：值格式(EAP-TLV)ID。Microsoft已將此診斷為XP SP2請求方的一個缺陷。

有關修補程式，請與Microsoft聯絡，並參閱連線到第三方RADIUS伺服器時PEAP身份驗證不成功文章 。根本問題在於，在客戶端，使用Windows實用程式時，PEAP預設禁用「快速重新連線」選項。但是，預設情況下在伺服器端(ACS)啟用此選項。要解決此問題，請取消選中ACS伺服器上的Fast Reconnect選項（在Global System Options下）。或者，您也可以在客戶端上啟用「快速重新連線」選項以解決問題。

執行以下步驟，以在使用Windows實用程式運行Windows XP的客戶端上啟用快速重新連線：

1. 轉至**開始 > 設定 > 控制面板**。
2. 按兩下**Network Connections**圖標。
3. 按一下右鍵**Wireless Network Connection**圖示，然後按一下**Properties**。
4. 按一下**Wireless Networks**頁籤。
5. 選擇**Use Windows to configure my wireless network settings**選項，以便啟用Windows以配置客戶端介面卡。
6. 如果您已配置SSID，請選擇SSID並按一下**Properties**。如果沒有，則按一下**New**以新增一個WLAN。
7. 在Association（關聯）頁籤下輸入SSID。確保網路身份驗證為**Open**，資料加密設定為**WEP**。
8. 按一下「**Authentication**」。
9. 選擇**Enable IEEE 802.1x authentication for this network**選項。
10. 選擇**PEAP**作為EAP型別，然後按一下**Properties**。
11. 選擇頁面底部的**Enable Fast Reconnect**選項。

相關資訊

- 採用ACS 4.0和Windows 2003的統一無線網路下的PEAP
- 適用於Web驗證的Cisco無線LAN控制器(WLC)和Cisco ACS 5.x(TACACS+)組態範例
- 思科安全存取控制系統5.1安裝和升級指南
- 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）。