採用ACS 4.0和Windows 2003的統一無線網路下的EAP-TLS

目錄

簡介

本檔案介紹如何透過可擴充驗證通訊協定 — 傳輸層安全(EAP-TLS)，使用無線LAN控制器(WLC)、Microsoft Windows 2003軟體和Cisco安全存取控制伺服器(ACS)4.0設定安全無線存取。

注意：有關安全無線部署的更多資訊，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 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，請在測試實驗室中的每台伺服器上安裝Windows Server 2003 Service Pack(SP)1作業系統並更新所有Service Pack。安裝控制器和AP，並確保配置最新的軟體更新。

重要事項：編寫本文檔時，SP1是最新的Windows Server 2003更新，SP2帶有更新補丁是Windows XP Professional的最新軟體。

使用Windows Server 2003 SP1企業版，可以配置用於EAP-TLS身份驗證的使用者和工作站證書的自動註冊。本文檔的EAP-TLS身份驗證部分對此進行了說明。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

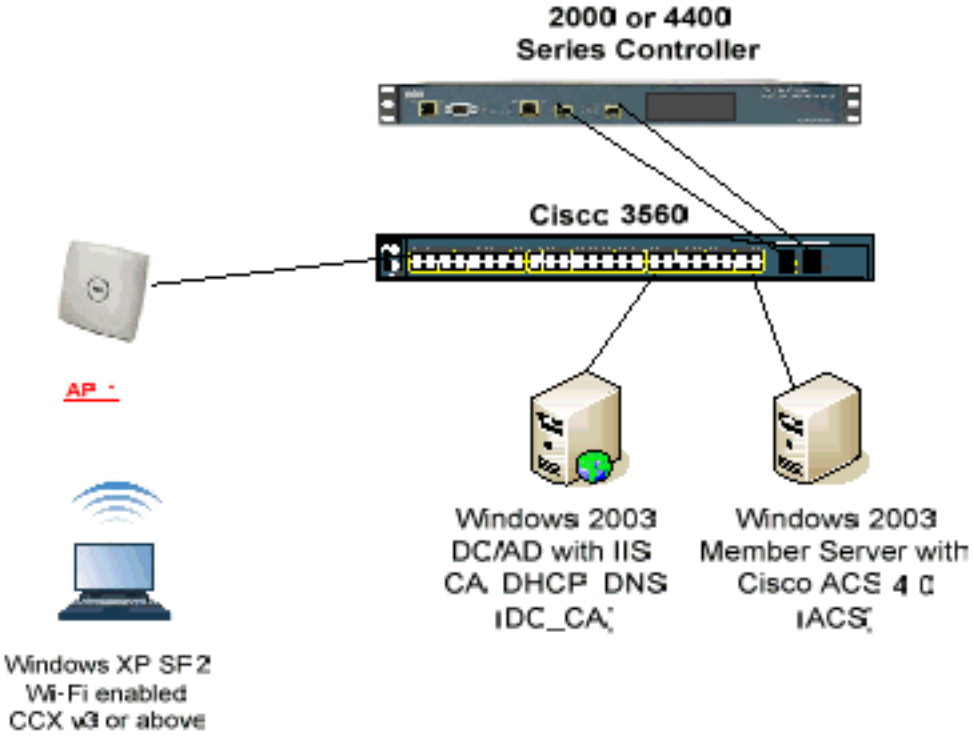
本文中的資訊係根據以下軟體和硬體版本：

- 運行3.2.116.21的Cisco 2006或4400系列控制器
- 思科1131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
- 採用存取控制伺服器(ACS)4.0的Windows 2003標準版
- 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 3560交換器

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 4.0和Windows 2003 Enterprise Server下實施EAP-TLS的逐步過程。重點是自動註冊客戶端，以便客戶端自動註冊並從伺服器獲取證書。

註意：要將具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，請參閱適用於Windows XP with SP2 的WPA2/無線調配服務資訊元素(WPS IE)更新。

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。

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

DC_CA（無線）

DC_CA是運行Windows Server 2003 SP1企業版並執行以下角色的電腦：

- 運行IIS的wirelessdemo.local域的域控制器
- 用於wirelessdemo.local DNS域的DNS伺服器

- DHCP伺服器
- wirelessdemo.local域的企業根CA

完成以下步驟，以便為這些服務配置DC_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WirelessUsers組。

第1步：執行基本安裝和配置

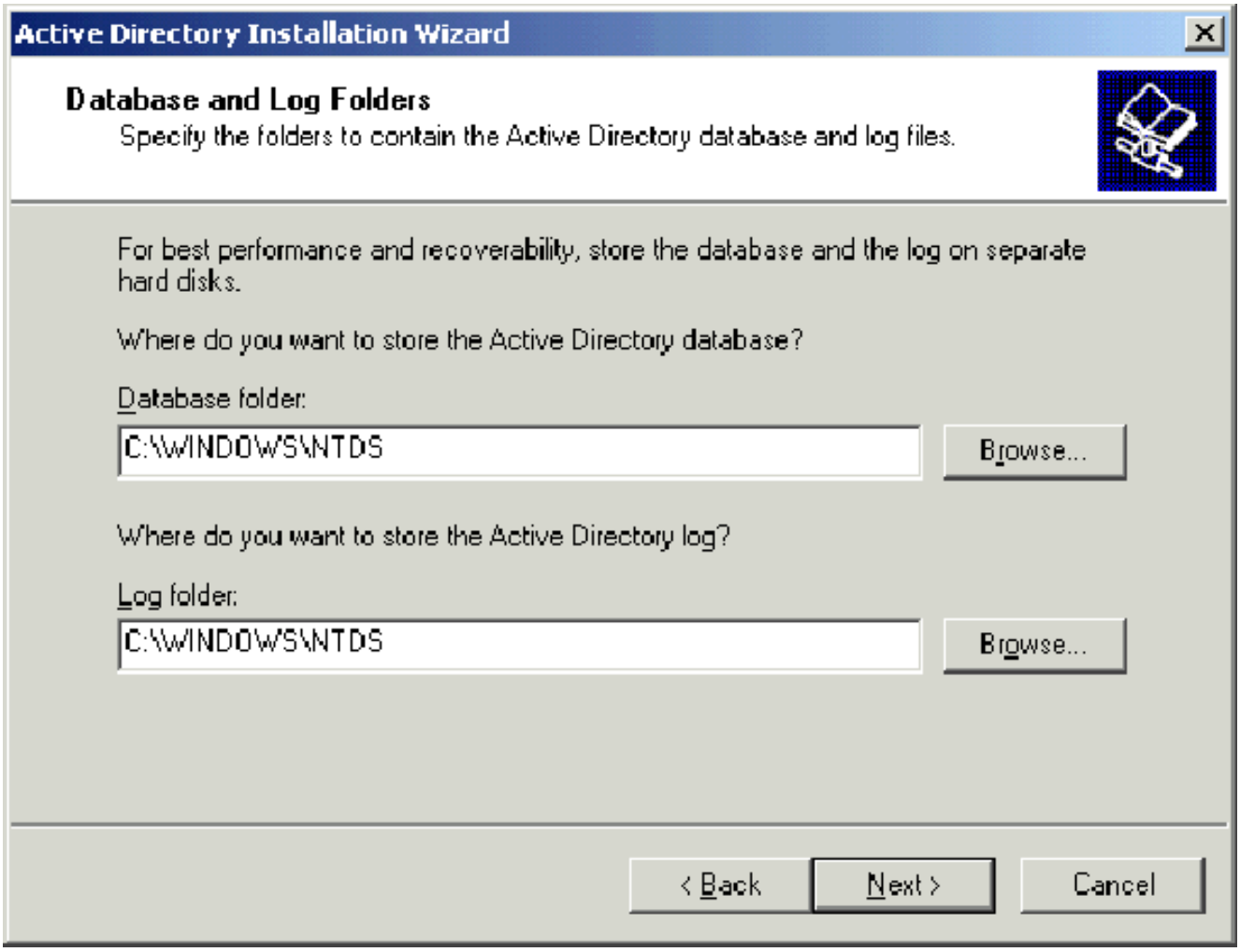
請完成以下步驟：

1. 安裝Windows Server 2003 SP1 Enterprise Edition作為獨立的伺服器。
2. 使用IP地址172.16.100.26和子網掩碼255.255.255.0配置TCP/IP協定。

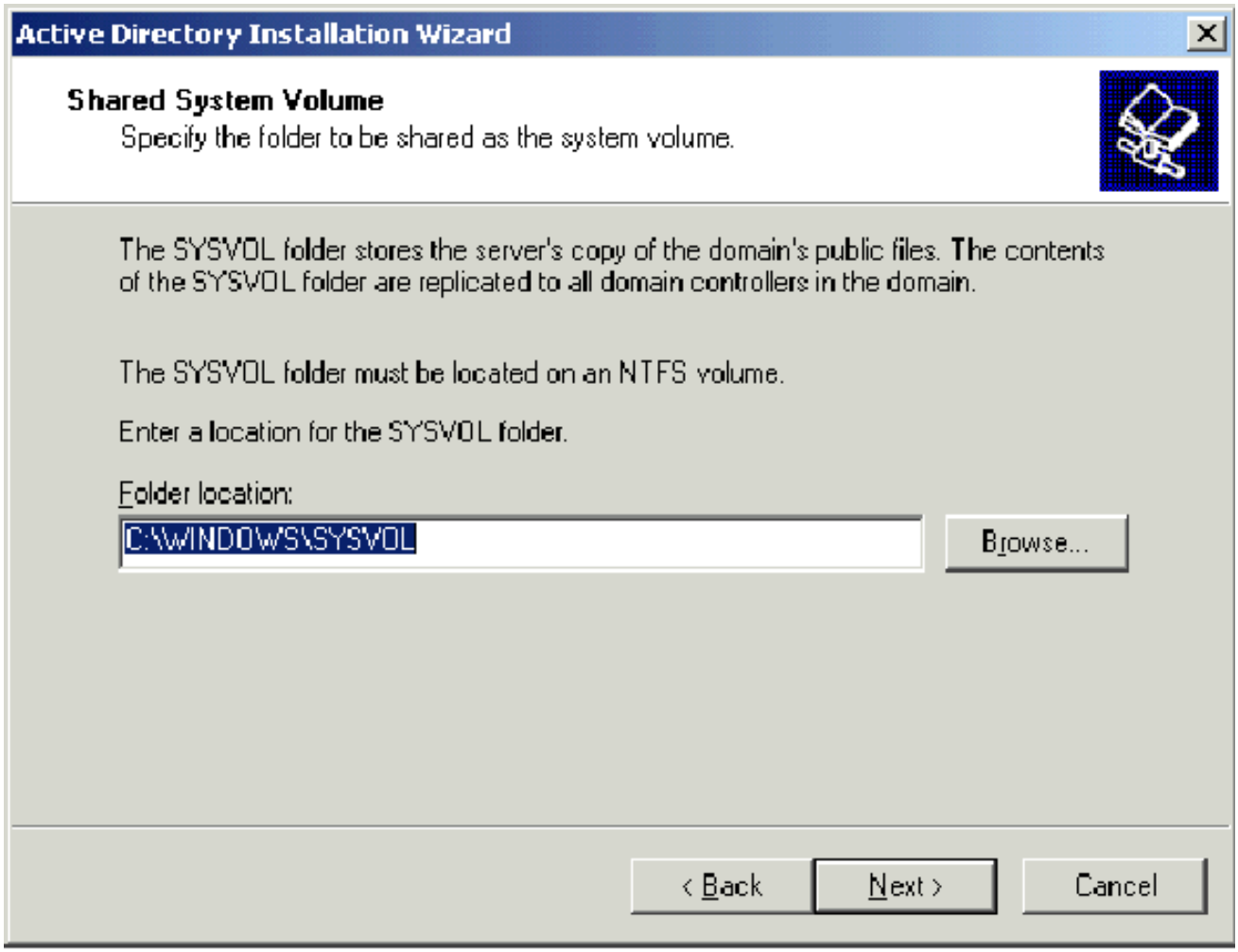
第2步：將電腦配置為域控制器

請完成以下步驟：

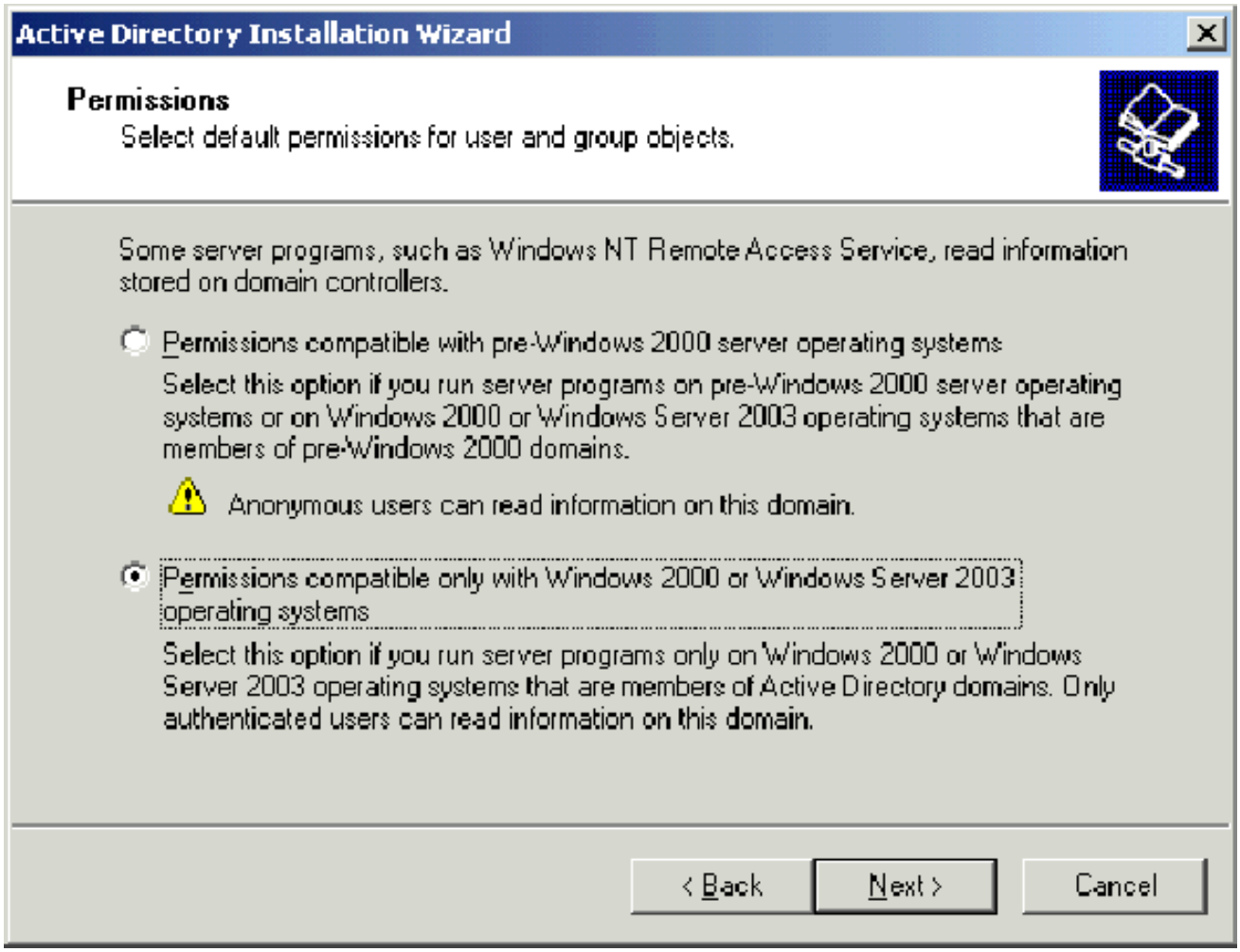
1. 若要啟動Active Directory安裝嚮導，請選擇**「開始」>「運行」**，鍵入**dcpromo.exe**，然後按一下**確定**。
2. 在「歡迎使用Active Directory安裝嚮導」頁面上，按一下**下一步**。
3. 在「作業系統相容性」頁上，按一下**下一步**。
4. 在「域控制器型別」頁上，為新**的域選擇域控制器，然**後按一下**下一步**。
5. 在「建立新域」頁上，選擇新**林中的域，然後單**擊「下一**步」**。
6. 在「安裝或配置DNS」頁面上，選擇**「否」，僅在此電腦上安裝並配置DNS，**然後按一下**「下一步」**。
7. 在「新建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



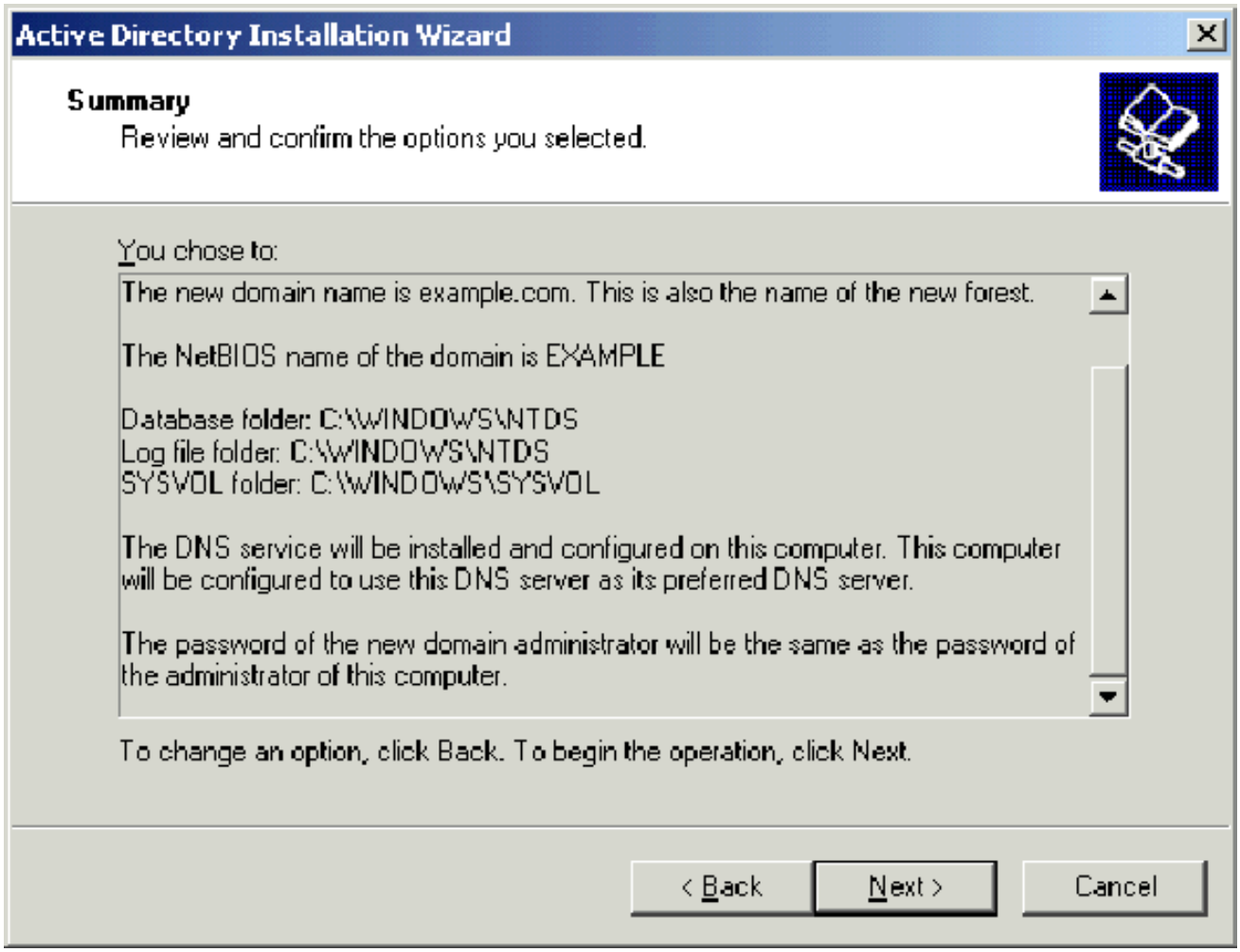
10. 在「共用系統卷」對話方塊中，驗證預設資料夾位置是否正確，然後按一下**下一步**。



11. 在「許可權」頁上，驗證是否選**擇了僅與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**。

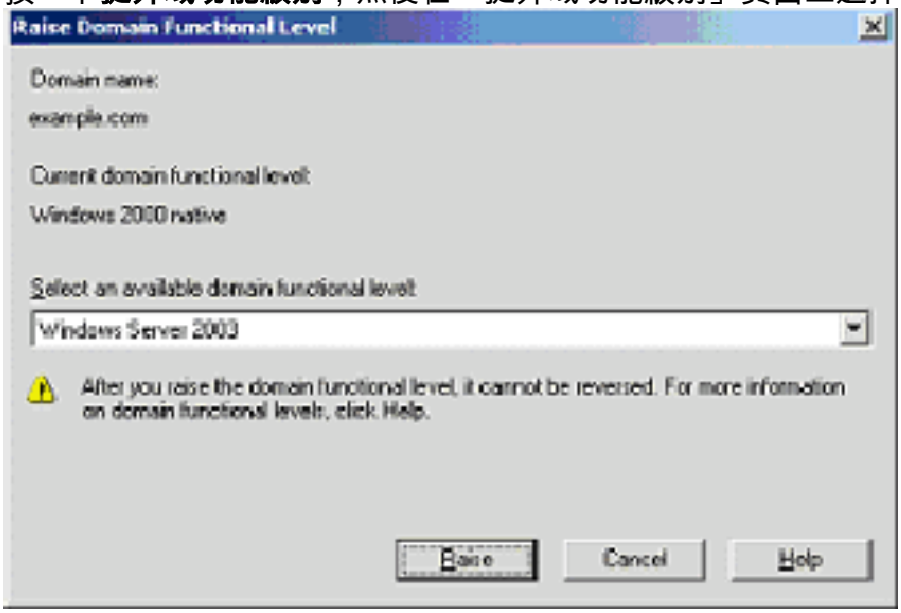


14. 在「完成Active Directory安裝嚮導」頁上，按一下**完成**。
15. 當系統提示重新啟動電腦時，按一下**Restart Now**。

步驟3:提升域功能級別

請完成以下步驟：

1. 從**管理工具**資料夾（開始>管理工具> Active Directory域和信任）中開啟Active Directory域和信任管理單元，然後按一下右鍵域電腦**DC_CA.wirelessdemo.local**。
2. 按一下**提升域功能級別**，然後在「提升域功能級別」頁面上選擇**Windows Server 2003**。

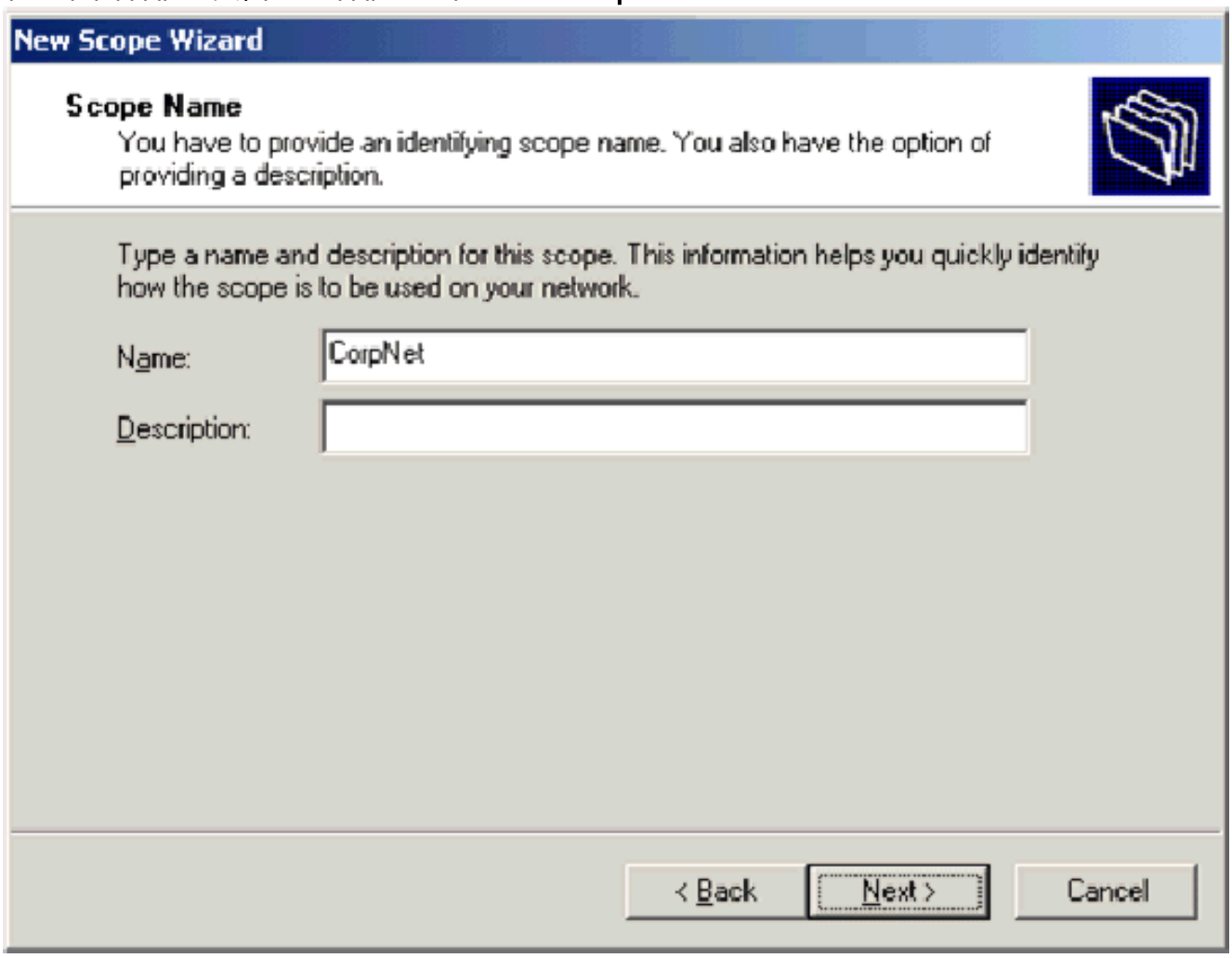


3. 按一下「**Raise**」，按一下「**OK**」，然後再次按一下「**OK**」。

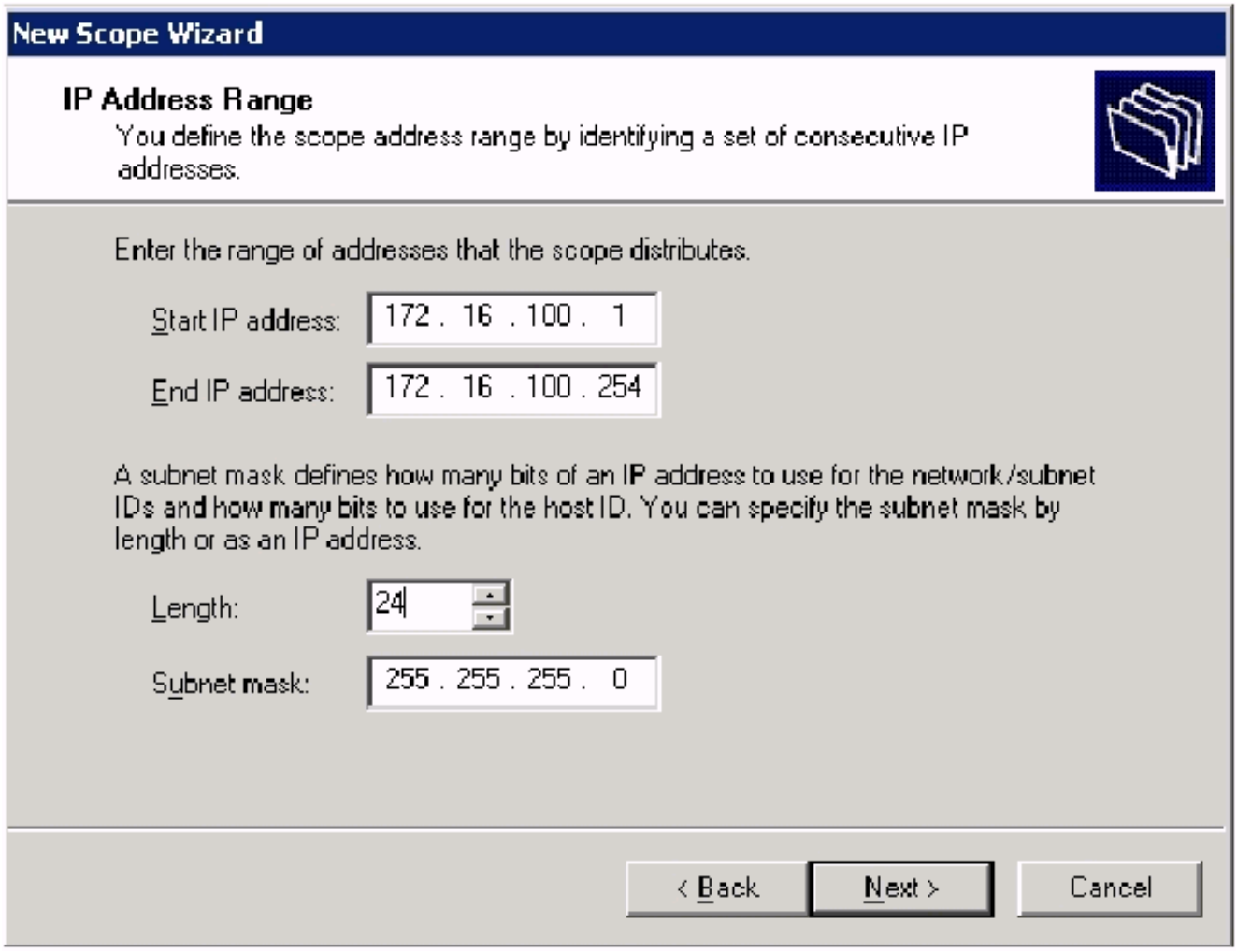
第4步：安裝和配置DHCP

請完成以下步驟：

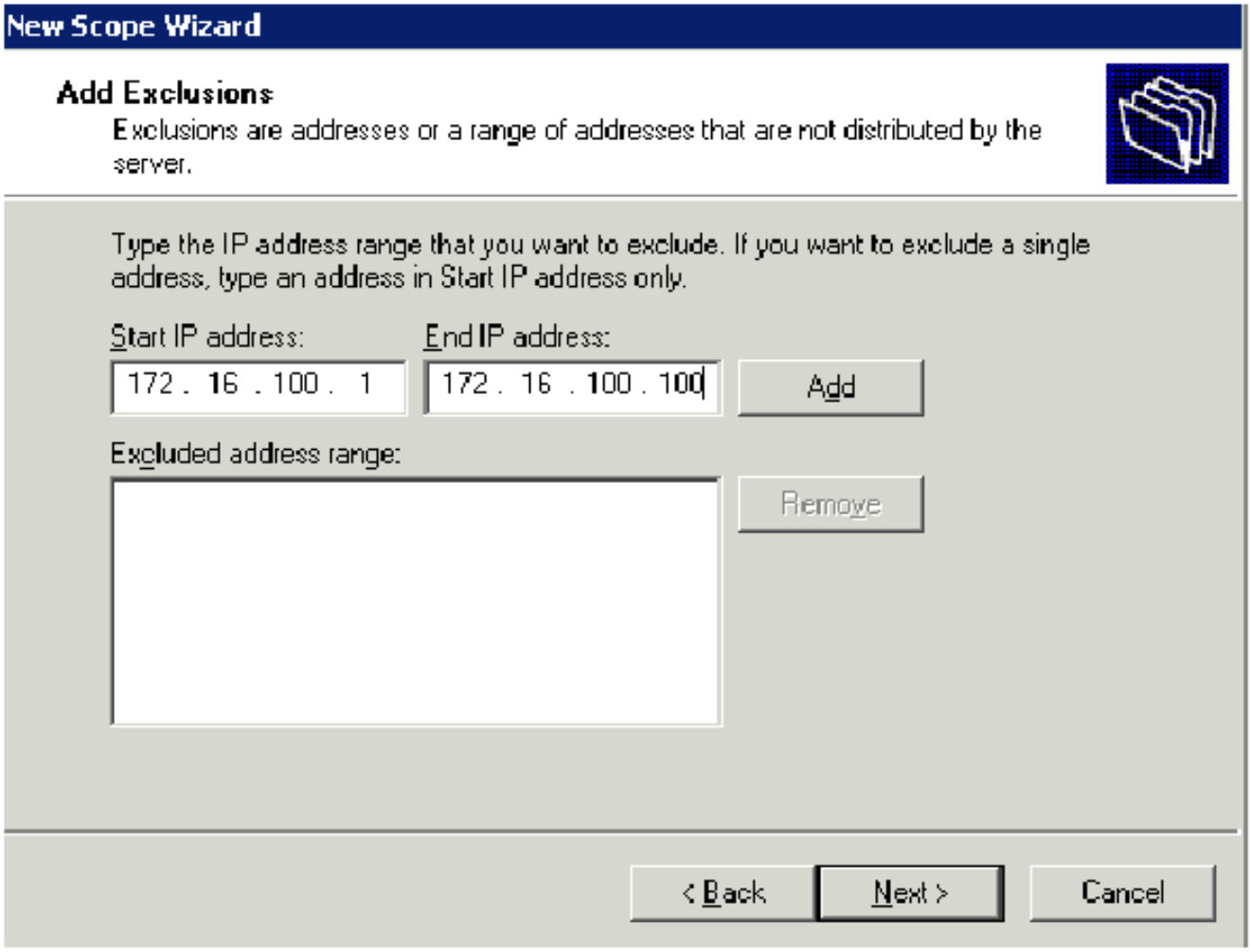
1. 使用「控制面板」中的「新增或刪除程式」，將動態主機配置協定(DHCP)安裝為網路服務元件。
2. 從Administrative Tools資料夾(**Start > Programs > Administrative Tools > DHCP**)中開啟DHCP管理單元，然後選中DHCP伺服器**DC_CA.wirelessdemo.local**。
3. 按一下**Action**，然後按一下**Authorize**以授權DHCP服務。
4. 在控制檯樹上，按一下右鍵**DC_CA.wirelessdemo.local**，然後按一下**New Scope**。
5. 在「新建作用域」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**。



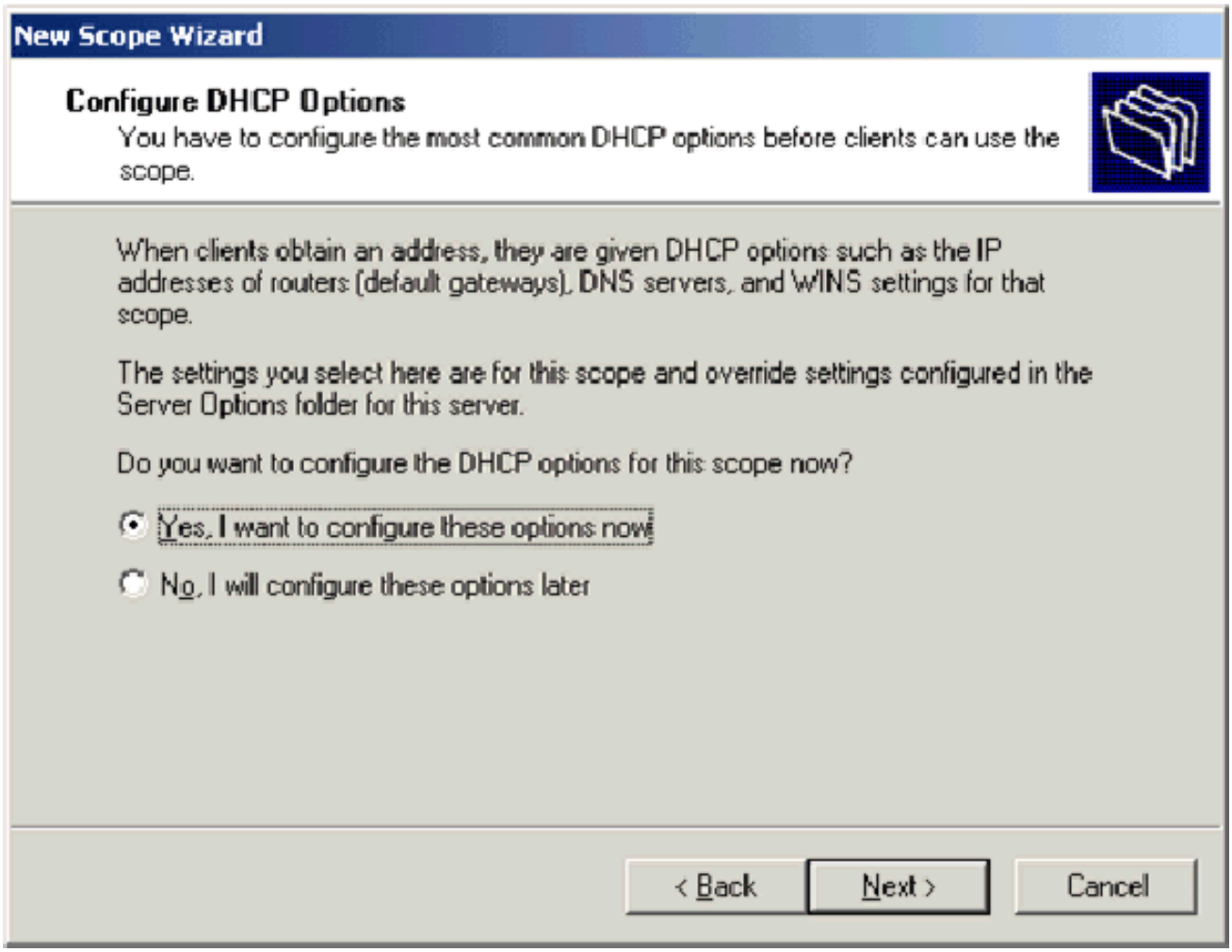
7. 按一下**Next**並填寫以下引數：起始IP地址— **172.16.100.1**結束IP地址— **172.16.100.254**長度(Length)- **24**子網掩碼— **255.255.255.0**



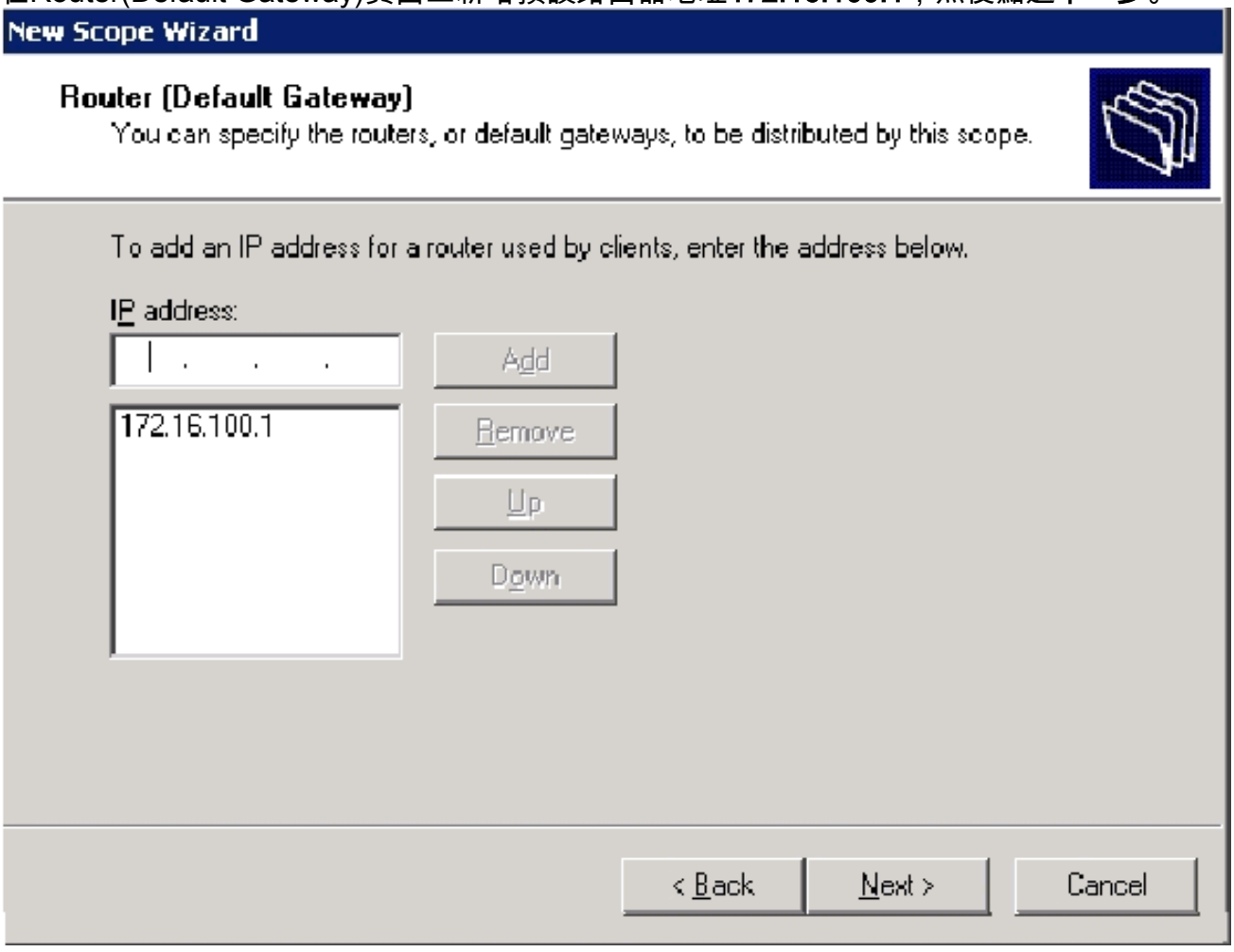
8. 按一下**Next**，輸入**172.16.100.1**作為起始IP地址，輸入**172.16.100.100**作為要排除的結束IP地址。然後按一下**Next**。這將保留172.16.100.1到172.16.100.100範圍內的IP地址。這些保留的IP地址不由DHCP伺服器分配。



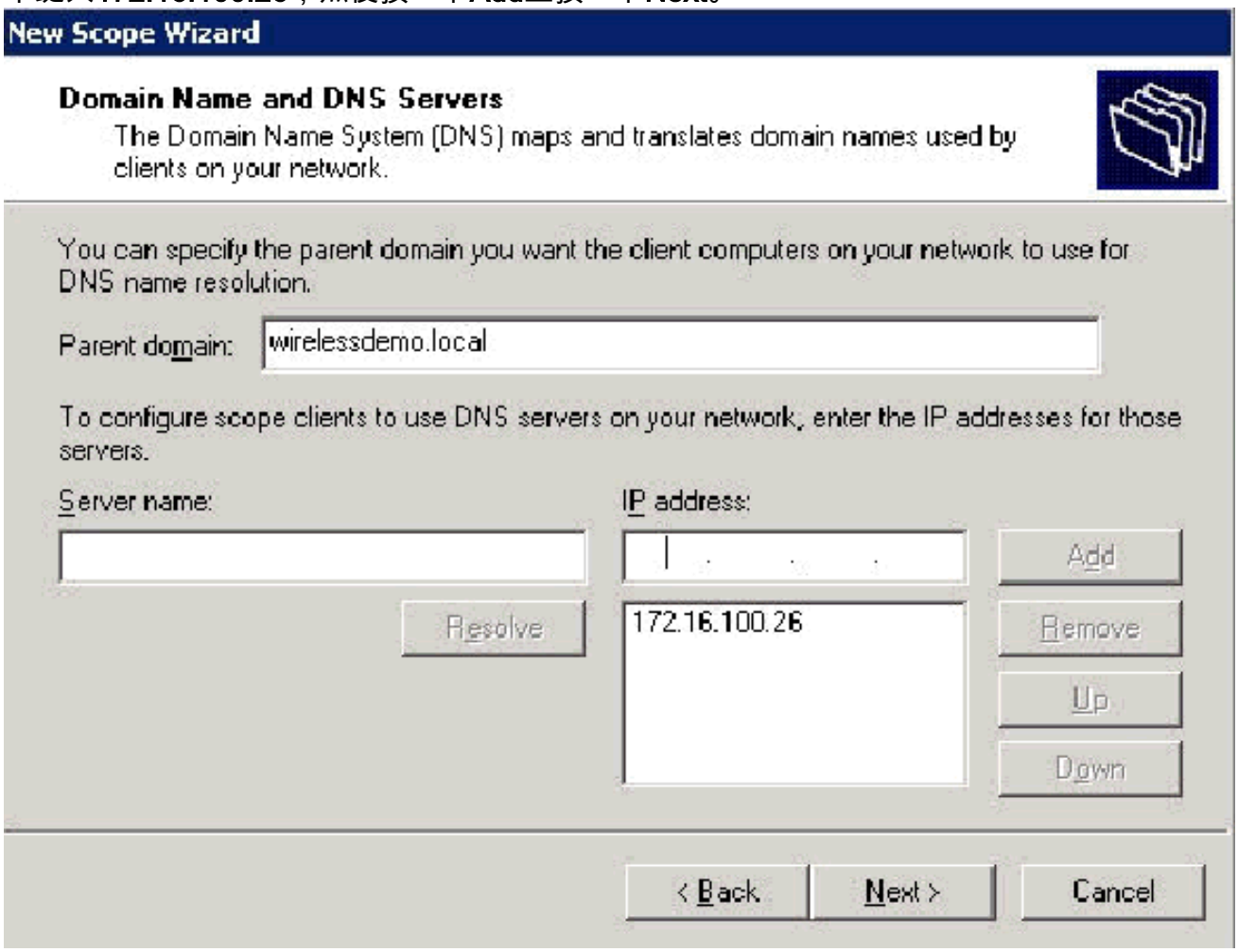
9. 在Lease Duration頁面上，按一下**Next**。
10. 在Configure DHCP Options頁上，選擇**Yes， I want to configure these options now**，然後按一下**Next**。



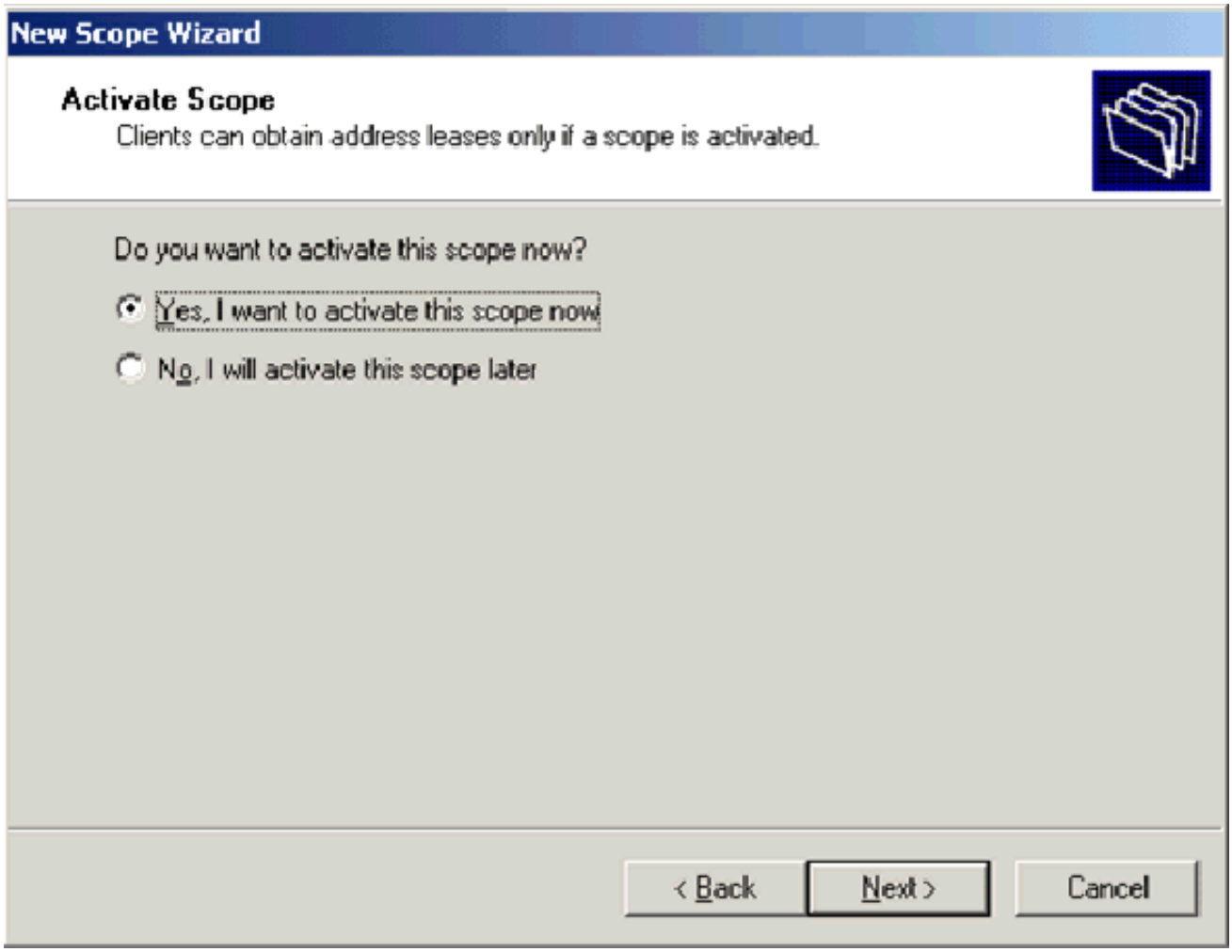
11. 在Router(Default Gateway)頁面上新增預設路由器地址**172.16.100.1**，然後點選**下一步**。



12. 在「域名和DNS伺服器」頁面的「父域」欄位中鍵入**wirelessdemo.local**，在「IP地址」欄位中鍵入**172.16.100.26**，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**」。



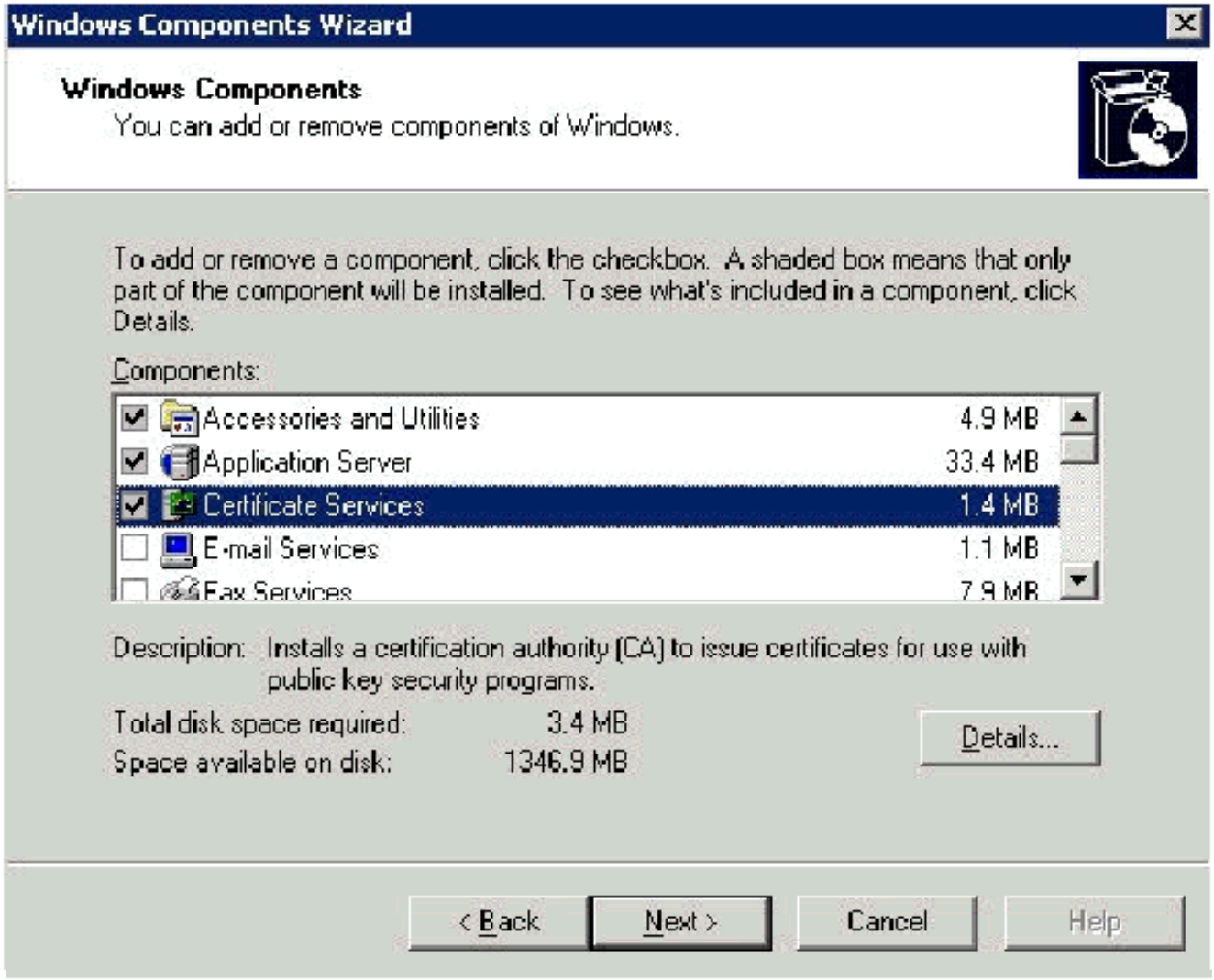
15. 在「完成新建作用域嚮導」頁上，按一下**完成**。

第5步：安裝證書服務

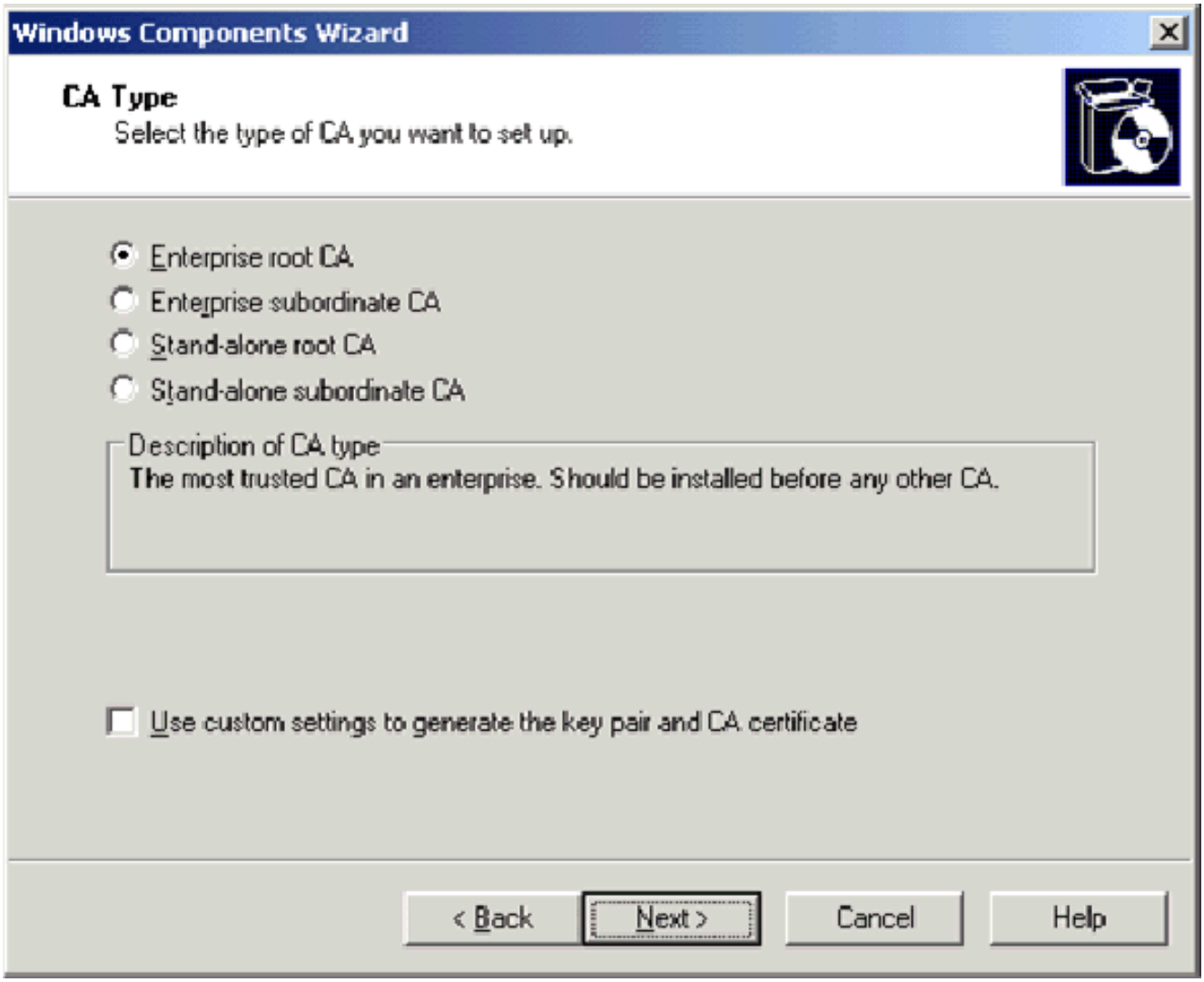
請完成以下步驟：

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。

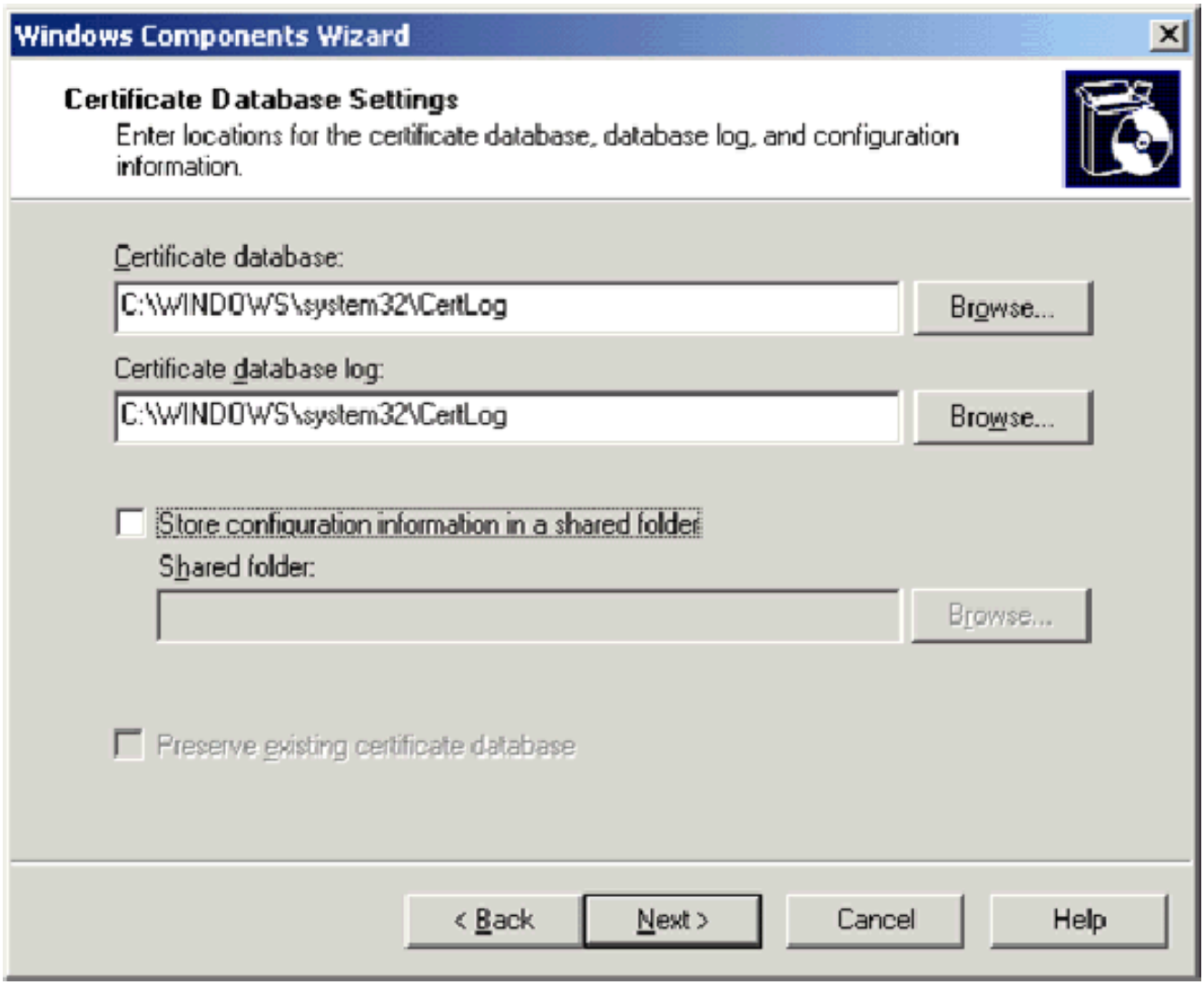
1. 在「控制面板」中，開啟**新增或刪除程式**，然後按一下**新增/刪除Windows元件**。
2. 在「Windows元件嚮導」頁面上，選擇**證書服務**，然後按一下**下一步**。



3. 在「CA型別」頁上，選擇**企業根CA**，然後按一下**下一步**。



4. 在「CA標識」資訊頁面上，在此CA的公用名框中鍵入**wirelessdemoca**。您可以輸入其他可選詳細資訊，然後按一下**下一步**。接受「證書資料庫設定」頁上的預設值。

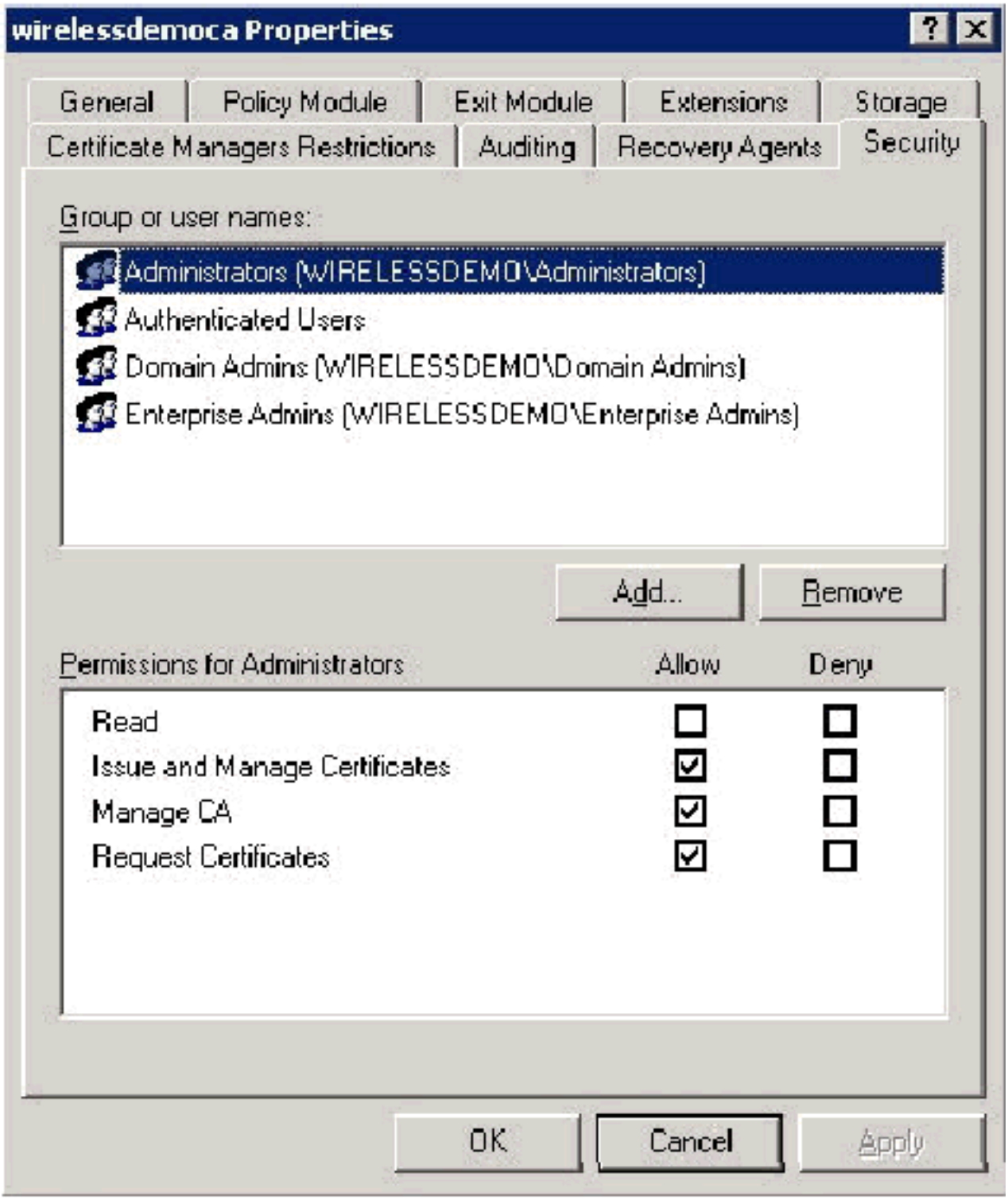


5. 按「**Next**」（下一步）。安裝完成後，按一下**Finish**。
6. 閱讀安裝IIS的警告後，按一下**OK**。

第6步：驗證證書的管理員許可權

請完成以下步驟：

1. 選擇**開始>管理工具>證書頒發機構**。
2. 按一下右鍵**wirelessdemoca 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**管理員**。
4. 在「許可權」或「管理員」清單中，驗證這些選項是否設定為**允許**: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**。



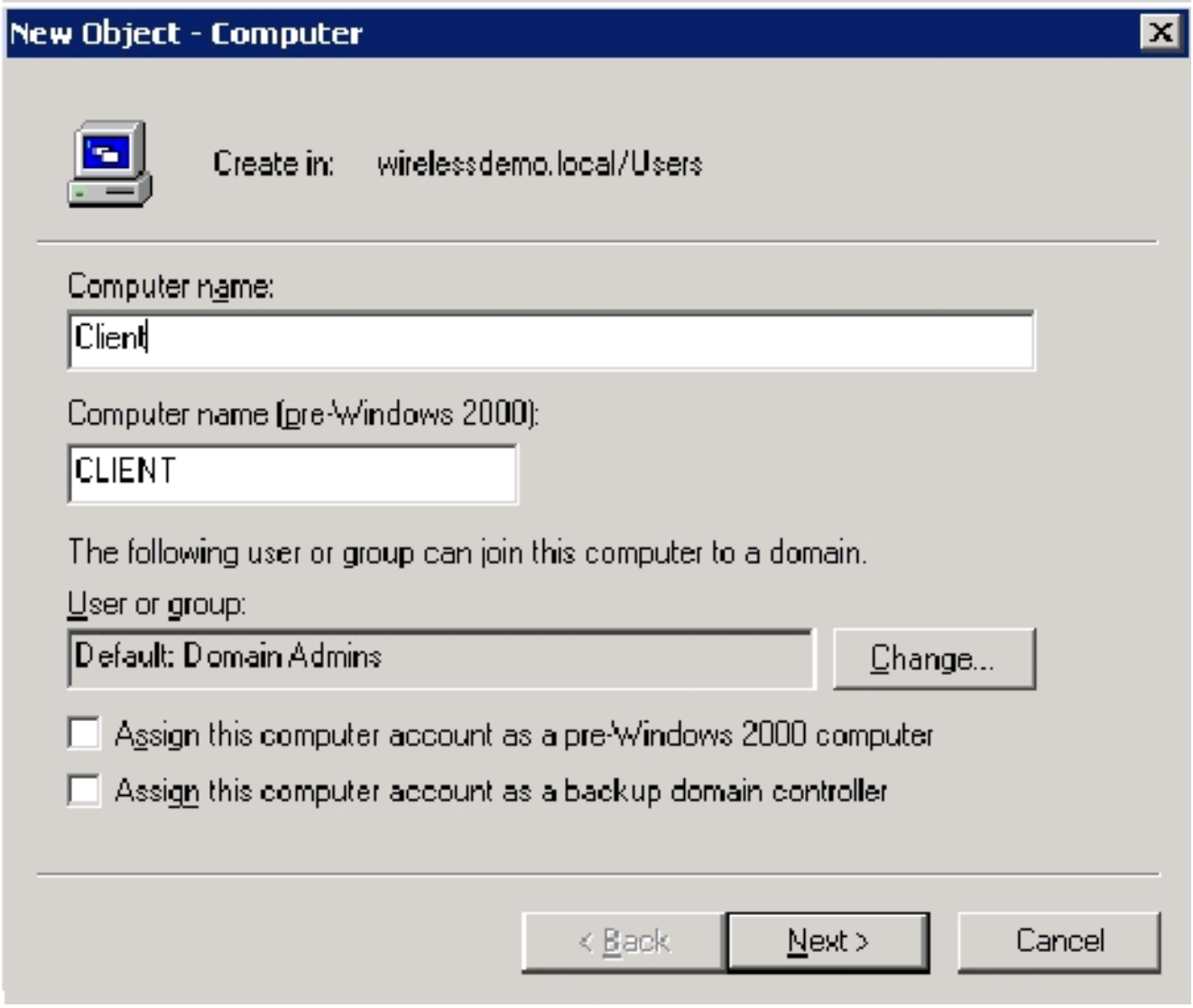
5. 按一下**OK**關閉wireless.democa CA Properties對話方塊，然後關閉Certification Authority。

第7步：將電腦新增到域

請完成以下步驟：

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使用者和電腦管理單元。
2. 在控制檯樹中，展開**wirelessdemo.local**。
3. 按一下右鍵**Users**，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」欄位中鍵入電腦的名稱，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。

第8步：允許對電腦進行無線訪問

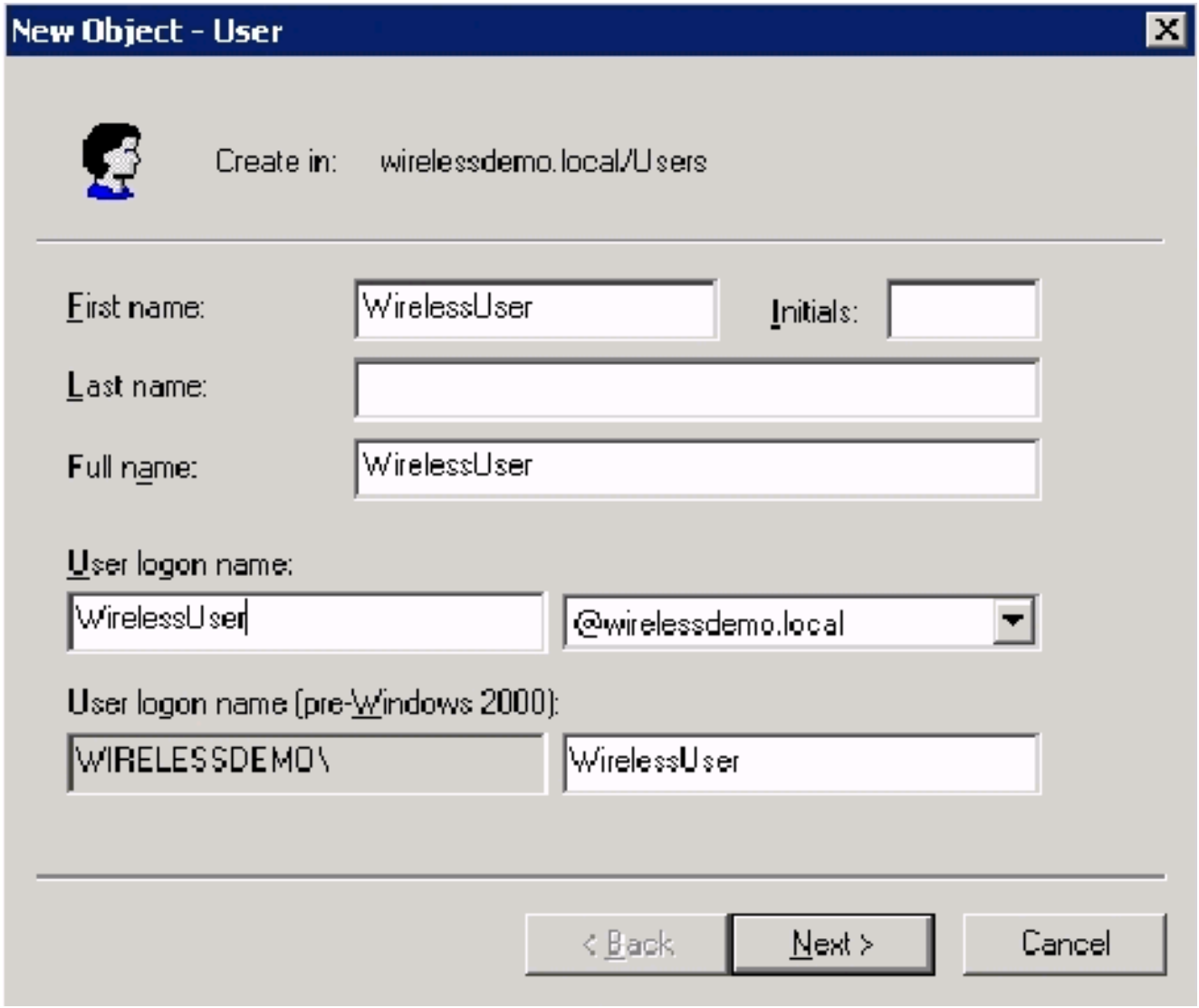
請完成以下步驟：

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。
2. 按一下**Properties**，然後轉到「Dial-in（撥入）」頁籤。
3. 選擇**Allow access**，然後按一下**OK**。

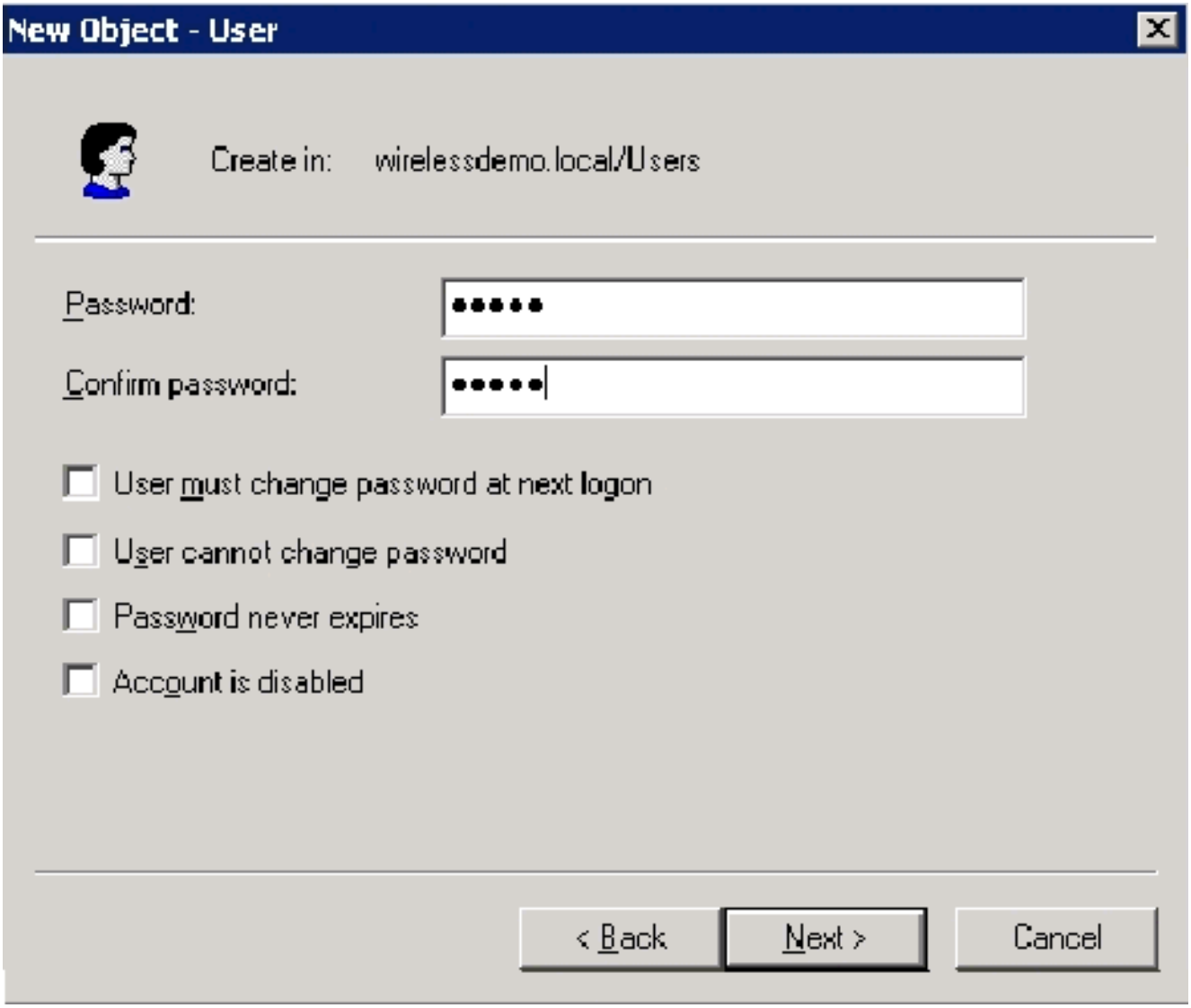
第9步：向域中新增使用者

請完成以下步驟：

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「新對象 — 使用者」對話方塊中，在「名字」欄位中鍵入**WirelessUser**，然後在「使用者登入名」欄位中鍵入**WirelessUser**，然後按一下**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。

步驟10:允許對使用者進行無線訪問

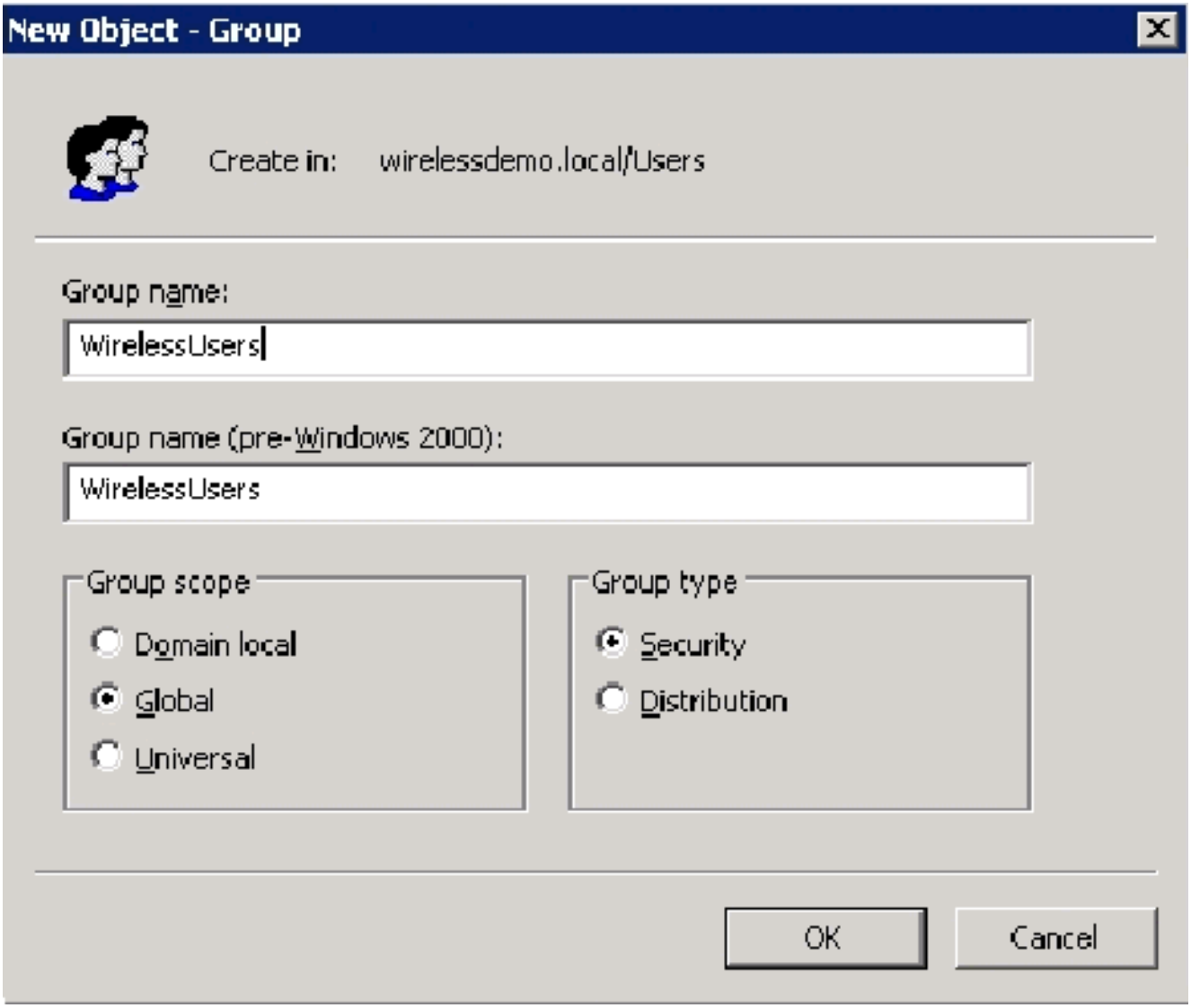
請完成以下步驟：

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「撥入」頁籤。
2. 選擇**Allow access**，然後按一下**OK**。

步驟11:向域中新增組

請完成以下步驟：

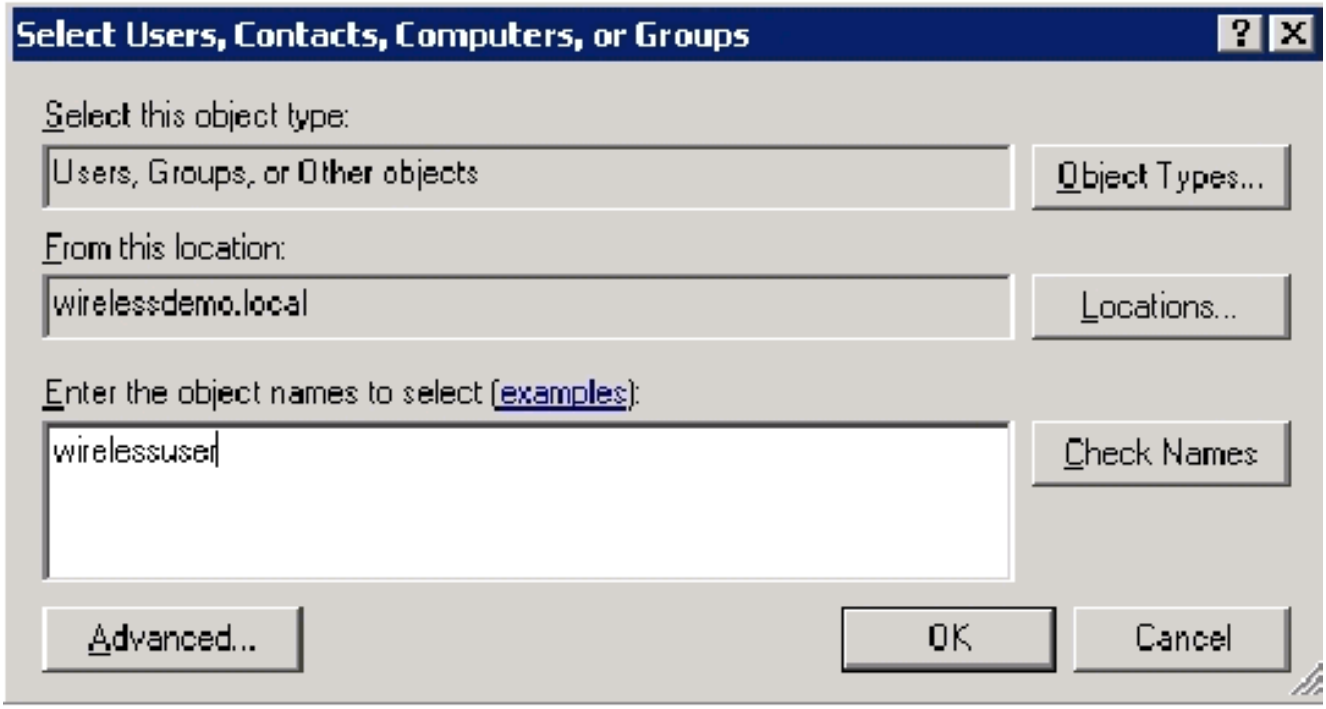
1. 在「Active Directory使用者和電腦」控制檯樹中，按一下右鍵**使用者**，按一下**新建**，然後按一下**組**。
2. 在「新建對象 — 組」對話方塊中，在「組名稱」欄位中鍵入組的名稱，然後按一下**確定**。本文檔使用組名稱**WirelessUsers**。



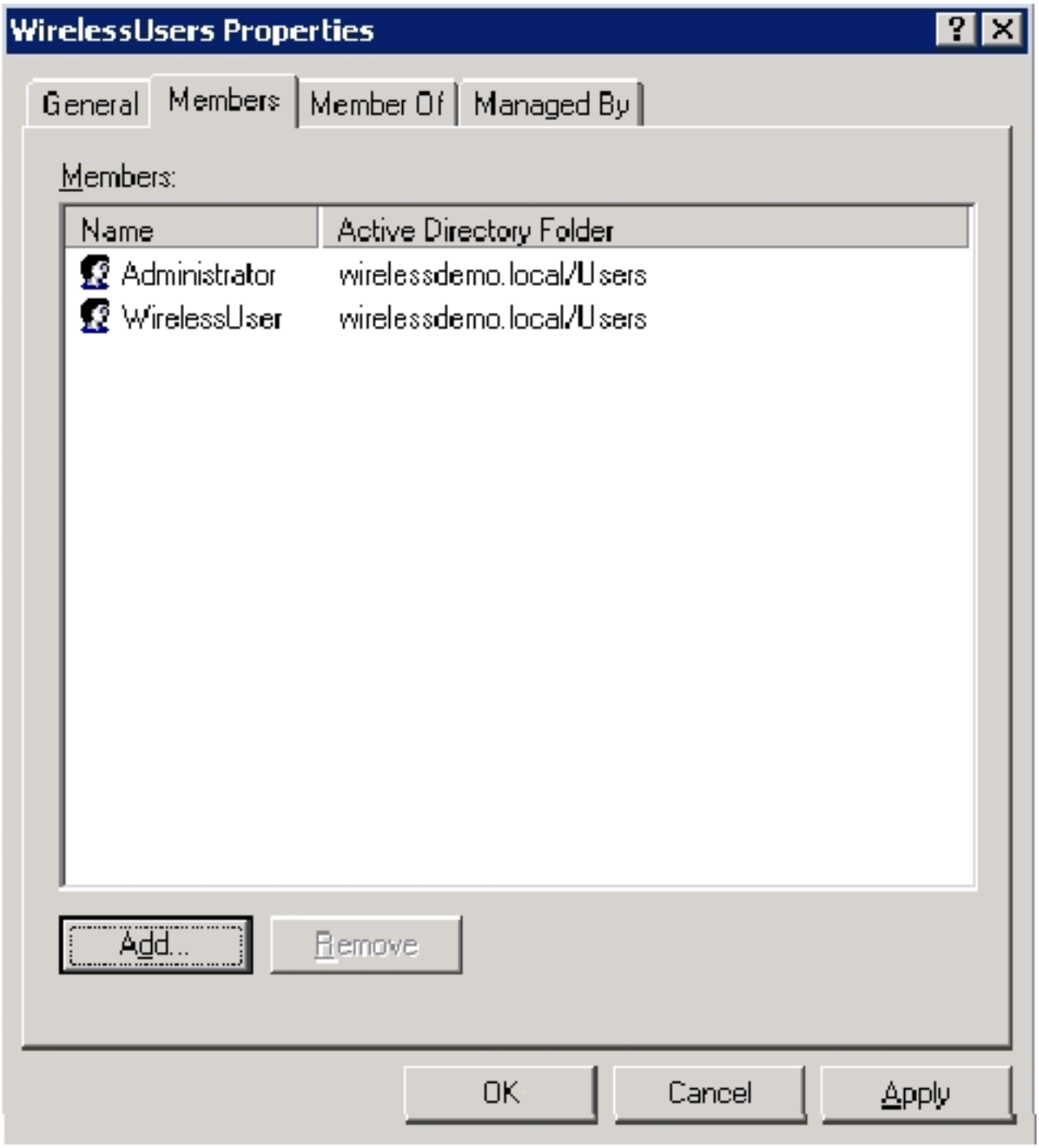
步驟12:將使用者新增到WirelessUsers組

請完成以下步驟：

1. 在Active Directory使用者和電腦的詳細資訊窗格中，按兩下Group **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**。WirelessUser使用者帳戶將新增到WirelessUsers組。

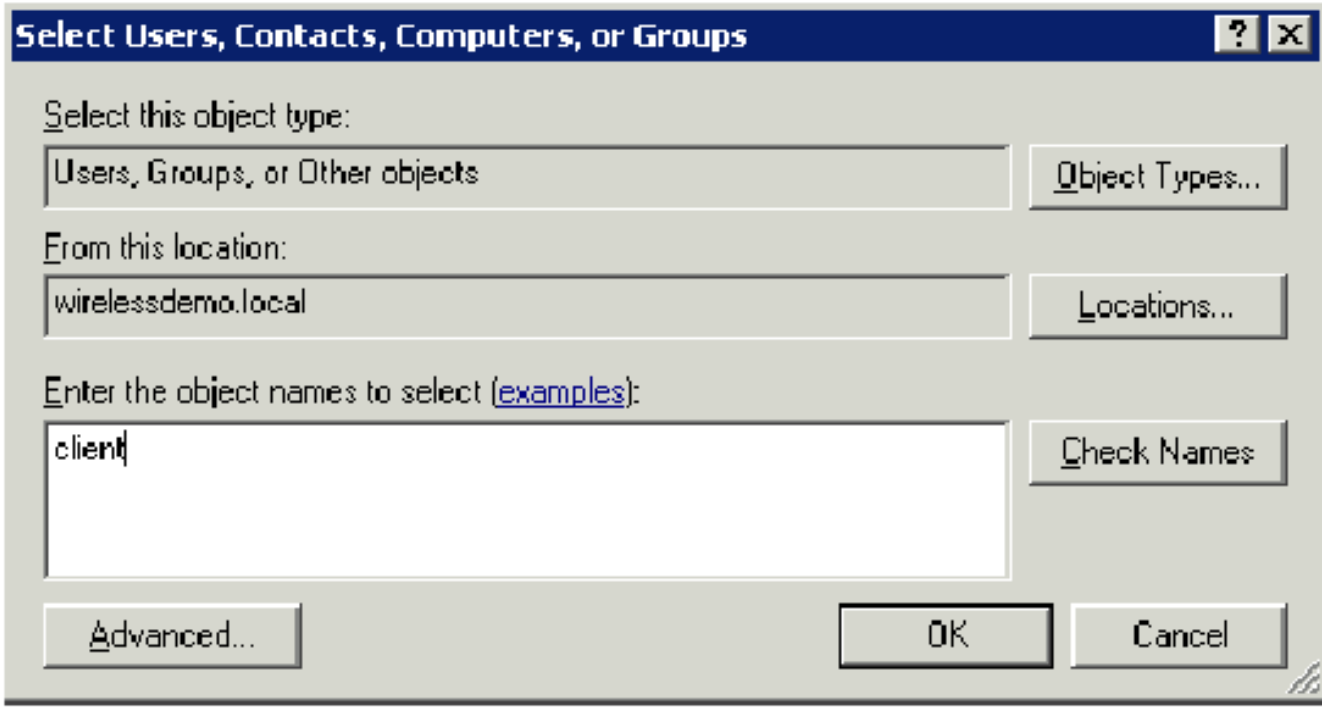


5. 按一下**OK**以儲存對WirelessUsers組的更改。
6. 重複此過程，向該組中新增更多使用者。

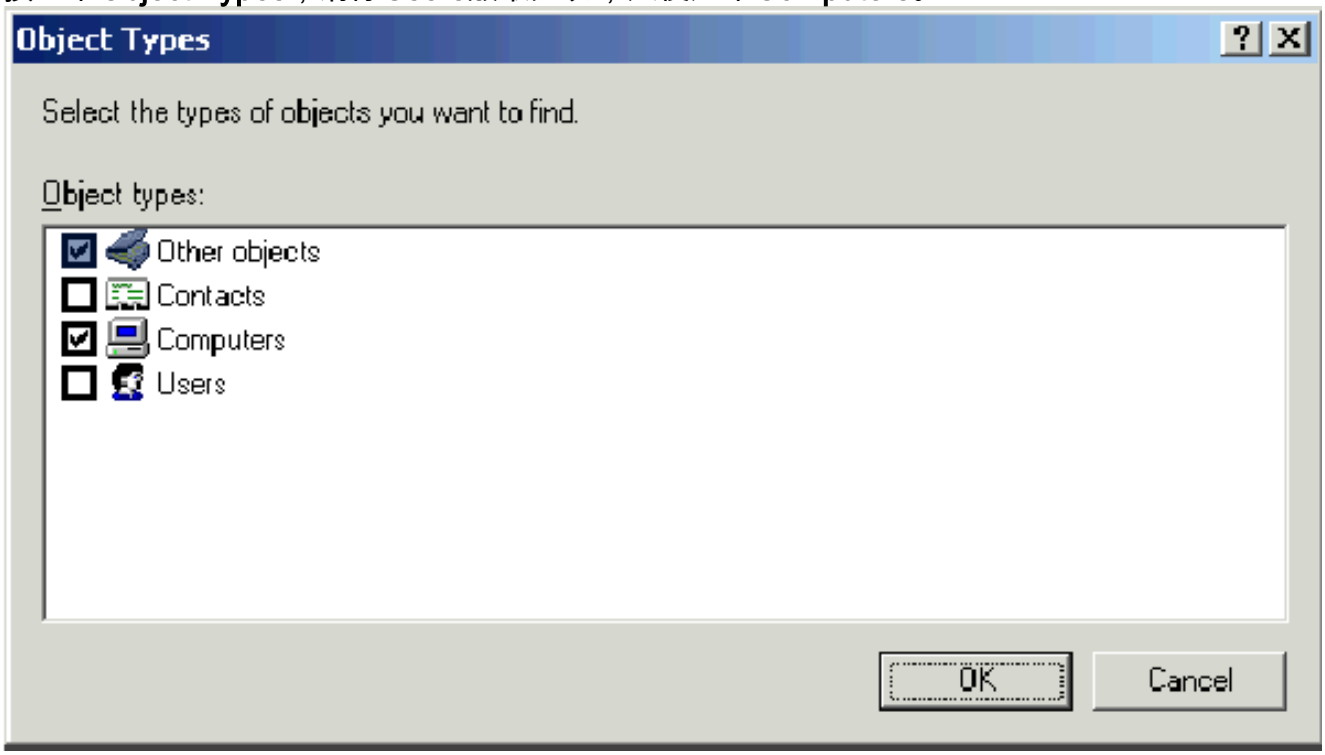
步驟13:將客戶端電腦新增到WirelessUsers組

請完成以下步驟：

1. 重複本文檔的將使用者新增到WirelessUsers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。客戶端電腦帳戶將新增到WirelessUsers組中。
5. 重複該過程，向該組中新增更多電腦。

採用Cisco Secure ACS 4.0的Windows Standard 2003安裝程式

Cisco Secure ACS是運行Windows Server 2003 SP1標準版的電腦，為控制器提供RADIUS身份驗證和授權。完成本節中的步驟，將ACS配置為RADIUS伺服器：

基本安裝和配置

請完成以下步驟：

1. 將Windows Server 2003 SP1 Standard Edition安裝為**ACS**成員伺服器，位於**wireless.demo.local**域中。**注意：**ACS伺服器名稱在其餘配置中顯示為cisco_w2003。在其餘實驗設定中替換ACS或cisco_w2003。
2. 對於本地連線，使用IP地址**172.16.100.26**、子網掩碼**255.255.255.0**和DNS伺服器IP地址**127.0.0.1**配置TCP/IP協定。

Cisco Secure ACS 4.0安裝

注意：有關如何配置Cisco Secure ACS 4.0 for Windows的詳細資訊，請參閱Cisco Secure ACS 4.0 for Windows安裝指南。

請完成以下步驟：

1. 使用域管理員帳戶，登入到名為ACS的電腦以訪問Cisco Secure ACS。**注意：**僅支援在安裝Cisco Secure ACS的電腦上執行的安裝。使用Windows終端服務或產品（如虛擬網路計算[VNC]）執行的遠端安裝未經過測試，並且不受支援。
2. 將Cisco Secure ACS CD插入電腦的CD-ROM驅動器。
3. 如果CD-ROM驅動器支援Windows自動運行功能，則會出現Cisco Secure ACS for Windows Server對話方塊。**注意：**如果電腦沒有安裝所需的Service Pack，則會出現一個對話方塊。可以在安裝Cisco Secure ACS之前或之後應用Windows服務包。您可以繼續安裝，但必須在安裝完成後應用所需的Service Pack。否則，Cisco Secure ACS可能無法可靠地運行。
4. 執行以下任務之一：如果出現「Cisco Secure ACS for Windows Server」對話方塊，請按一下**Install**。如果未出現「Cisco Secure ACS for Windows Server」對話方塊，請運行**setup.exe**（位於Cisco Secure ACS CD的根目錄中）。
5. Cisco Secure ACS Setup對話方塊顯示軟體許可協定。
6. 閱讀軟體許可協定。如果您接受軟體許可協定，請按一下**Accept**。歡迎對話方塊顯示有關安裝程式的基本資訊。
7. 閱讀歡迎對話方塊中的資訊後，按一下**下一步**。
8. 「開始之前」對話方塊列出了繼續安裝之前必須完成的專案。如果您已完成「開始之前」對話方塊中列出的所有專案，請選中每個專案的對應框，然後按一下**下一步**。**注意：如**果尚未完成「開始之前」框中列出的所有專案，請按一下**「取消」**，然後按一下「退出**設定」**。完成「開始之前」對話方塊中列出的所有專案後，請重新啟動安裝。
9. 系統將顯示Choose Destination Location對話方塊。在目標資料夾下，將顯示安裝位置。這是安裝程式安裝Cisco Secure ACS的驅動器和路徑。
10. 如果要更改安裝位置，請完成以下步驟：按一下「**Browse**」。出現「Choose Folder（選擇資料夾）」對話方塊。路徑框包含安裝位置。更改安裝位置。您可以在「路徑」框中鍵入新位置，也可以使用「驅動器和目錄」清單選擇新的驅動器和目錄。安裝位置必須位於電腦的本地驅動器上。**注意：**不要指定包含百分比字元「%」的路徑。 如果這樣做，安裝似乎可以正確繼續，但在完成之前失敗。按一下「**OK**」（確定）。**註：如**果您指定了不存在的資料夾，安裝程式將顯示一個對話方塊來確認資料夾的建立。若要繼續，請按一下**Yes**。
11. 在「選擇目標位置」對話方塊中，新的安裝位置將出現在「目標資料夾」下。
12. 按「**Next**」（下一步）。
13. 身份驗證資料庫配置對話方塊列出了用於驗證使用者的選項。您只能通過Cisco Secure使用者資料庫或Windows使用者資料庫進行身份驗證。**註：安**裝Cisco Secure ACS後，除Windows使用者資料庫外，您還可以為所有外部使用者資料庫型別配置身份驗證支援。
14. 如果只想使用Cisco Secure使用者資料庫對使用者進行身份驗證，請選擇**Check the Cisco Secure ACS database only**選項。
15. 除了Cisco Secure使用者資料庫之外，如果要使用Windows安全訪問管理器(SAM)使用者資

料庫或Active Directory使用者資料庫對使用者進行身份驗證，請完成以下步驟：選擇**Also check the Windows User Database**選項。**Yes， refer to "Grant dialin permission to user" setting**覈取方塊變為可用。**注意：**是，請參閱**「向使用者授予撥入許可權」設定複選**框，適用於由Cisco Secure ACS控制的所有形式的訪問，而不僅僅是撥入訪問。例如，通過VPN隧道訪問網路的使用者沒有撥入網路訪問伺服器。但是，如果選中**是，請參閱「向使用者授予撥入許可權」設定**框，則Cisco Secure ACS應用Windows使用者撥入許可權，以確定是否授予使用者網路訪問許可權。如果您希望僅當使用者在其Windows帳戶中具有撥入許可權時才允許訪問通過Windows域使用者資料庫進行身份驗證的使用者，請選中**Yes，請參閱「向使用者授予撥入許可權」設定**框。
16. 按「**Next**」（下一步）。
17. 安裝程式將安裝Cisco Secure ACS並更新Windows登錄檔。
18. 「高級選項」對話方塊列出了預設情況下未啟用的Cisco Secure ACS的多個功能。有關這些功能的詳細資訊，請參閱適用於Windows Server 4.0版的Cisco Secure ACS使用手冊。**注意**：僅當您啟用列出的功能時，這些功能才會顯示在Cisco Secure ACS HTML介面中。安裝後，您可以在Interface Configuration部分的Advanced Options頁面上啟用或禁用它們。
19. 對於要啟用的每個功能，請選中相應的覈取方塊。
20. 按「**Next**」（下一步）。
21. 出現Active Service Monitoring對話方塊。**注意：安**裝之後，您可以在「系統配置」部分的「活動服務管理」頁上配置活動服務監視功能。
22. 如果您希望Cisco Secure ACS監控使用者身份驗證服務，請選中**Enable Login Monitoring**框。從「要執行的指令碼」清單中，選擇要在身份驗證服務失敗時應用的選項：**無補救操**作 — Cisco Secure ACS不運行指令碼。**註：如果**啟用事件郵件通知，此選項非常有用。**Reboot** - Cisco Secure ACS運行一個指令碼，該指令碼將重新啟動運行Cisco Secure ACS的電腦。**Restart All** - Cisco Secure ACS重新啟動所有Cisco Secure ACS服務。**重新啟動RADIUS/TACACS+** - Cisco Secure ACS僅重新啟動RADIUS和TACACS+服務。
23. 如果您希望Cisco Secure ACS在服務監控檢測到事件時傳送電子郵件，請選中**Mail Notification**框。
24. 按「**Next**」（下一步）。
25. 此時將顯示資料庫加密口令對話方塊。**註：數**據庫加密密碼已加密並儲存在ACS登錄檔中。當出現嚴重問題並且需要手動訪問資料庫時，您可能需要重複使用此密碼。保留此密碼，以便技術支援可以訪問資料庫。可在每個過期期間更改密碼。
26. 輸入用於資料庫加密的口令。密碼長度至少需要八個字元，並且必須同時包含字元和數字。沒有無效字元。按「**Next**」（下一步）。
27. 安裝程式完成，出現Cisco Secure ACS服務啟動對話方塊。
28. 對於所需的每個Cisco Secure ACS Services Initiation選項，選中相應的覈取方塊。與選項相關聯的操作在安裝程式完成後發生。**是，我要立即啟動Cisco Secure ACS服務** — 啟動組成Cisco Secure ACS的Windows服務。如果不選擇此選項，除非重新啟動電腦或啟動CSAdmin服務，否則Cisco Secure ACS HTML介面不可用。**是，安裝後，我希望安裝程式從我的瀏覽器啟動Cisco Secure ACS管理員** — 在當前Windows使用者帳戶的預設Web瀏覽器中開啟Cisco Secure ACS HTML介面。**是，我想檢視自述檔案 —** 在Windows記事本中開啟README.TXT檔案。
29. 按「**Next**」（下一步）。
30. 如果選擇了某個選項，Cisco Secure ACS服務將啟動。設定完成對話方塊顯示有關Cisco Secure ACS HTML介面的資訊。
31. 按一下「**Finish**」（結束）。**註：**配置的其餘部分在已配置的EAP型別的部分下記錄。

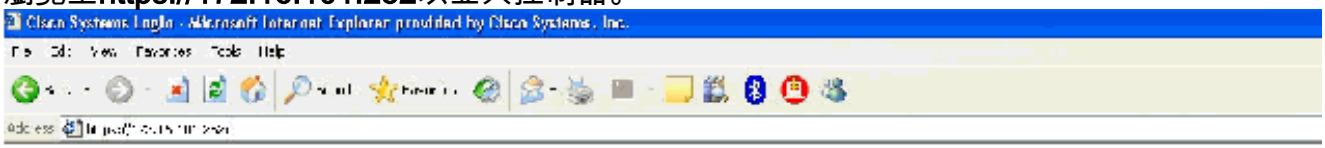
Cisco LWAPP控制器配置

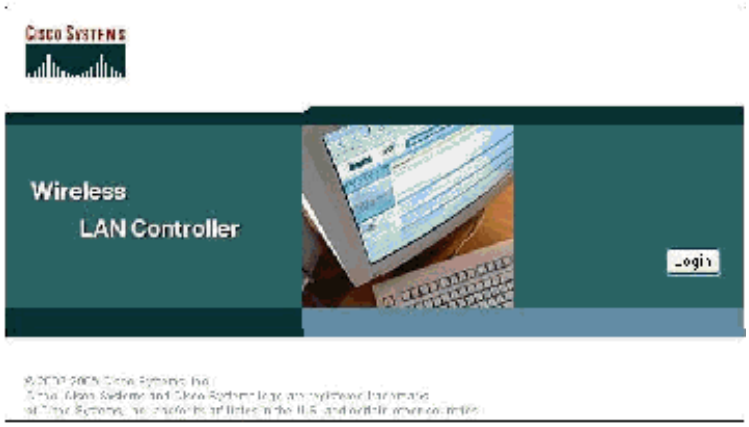
為WPA2/WPA建立必要的配置

請完成以下步驟：

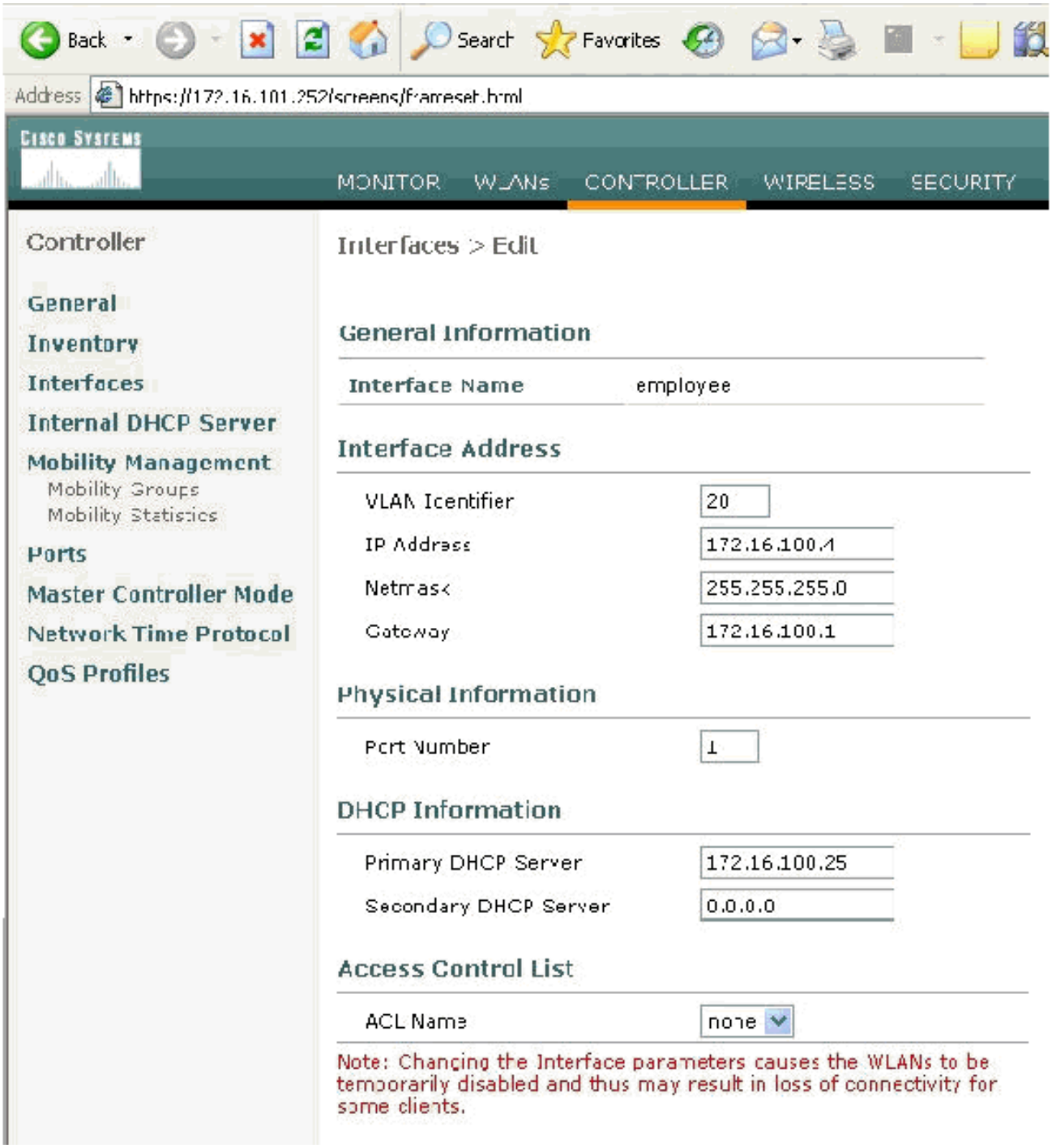
註：假設控制器與網路具有基本連線，並且與管理介面的IP可達性成功。

1. 瀏覽至**https://172.16.101.252**以登入控制器。

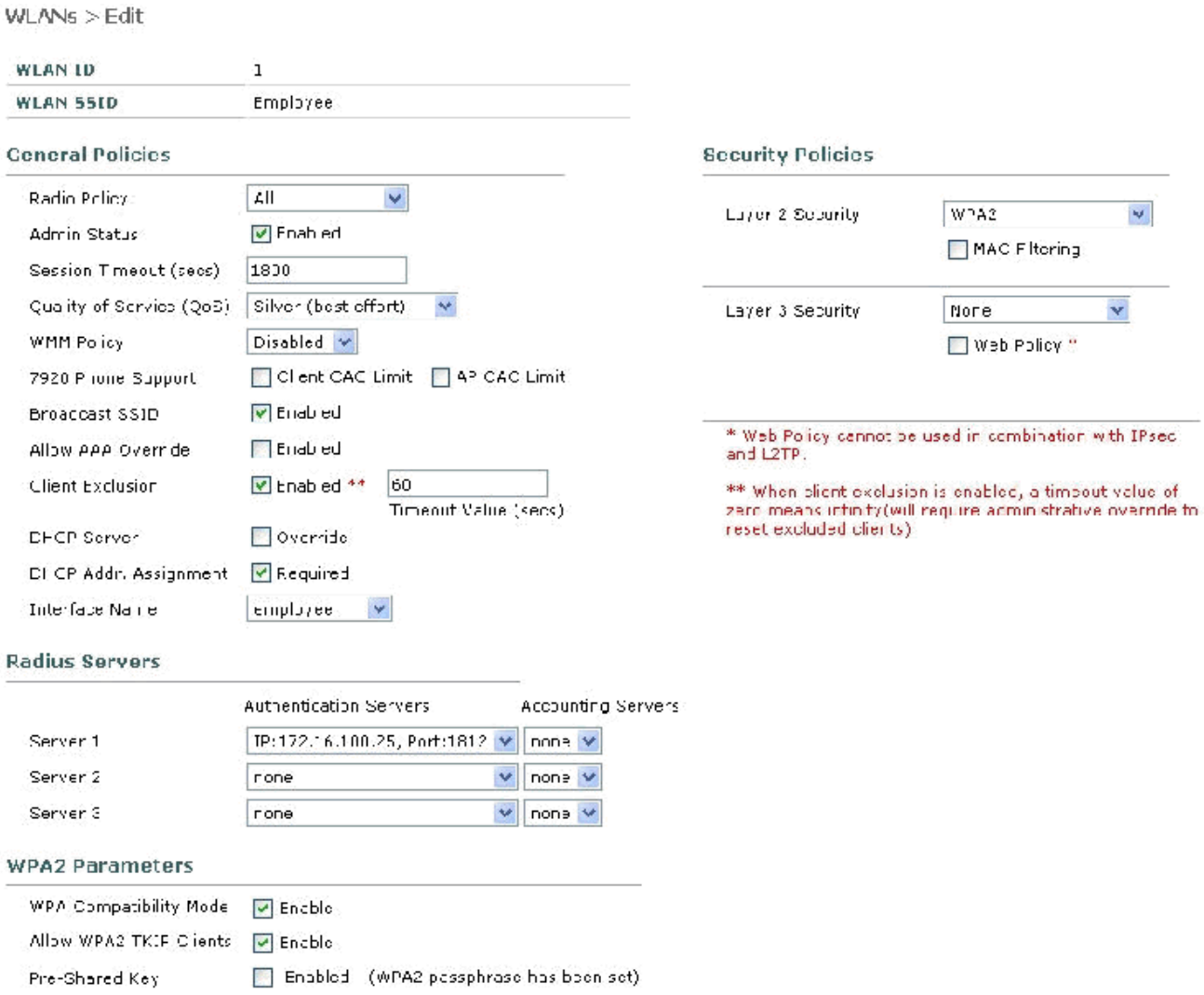




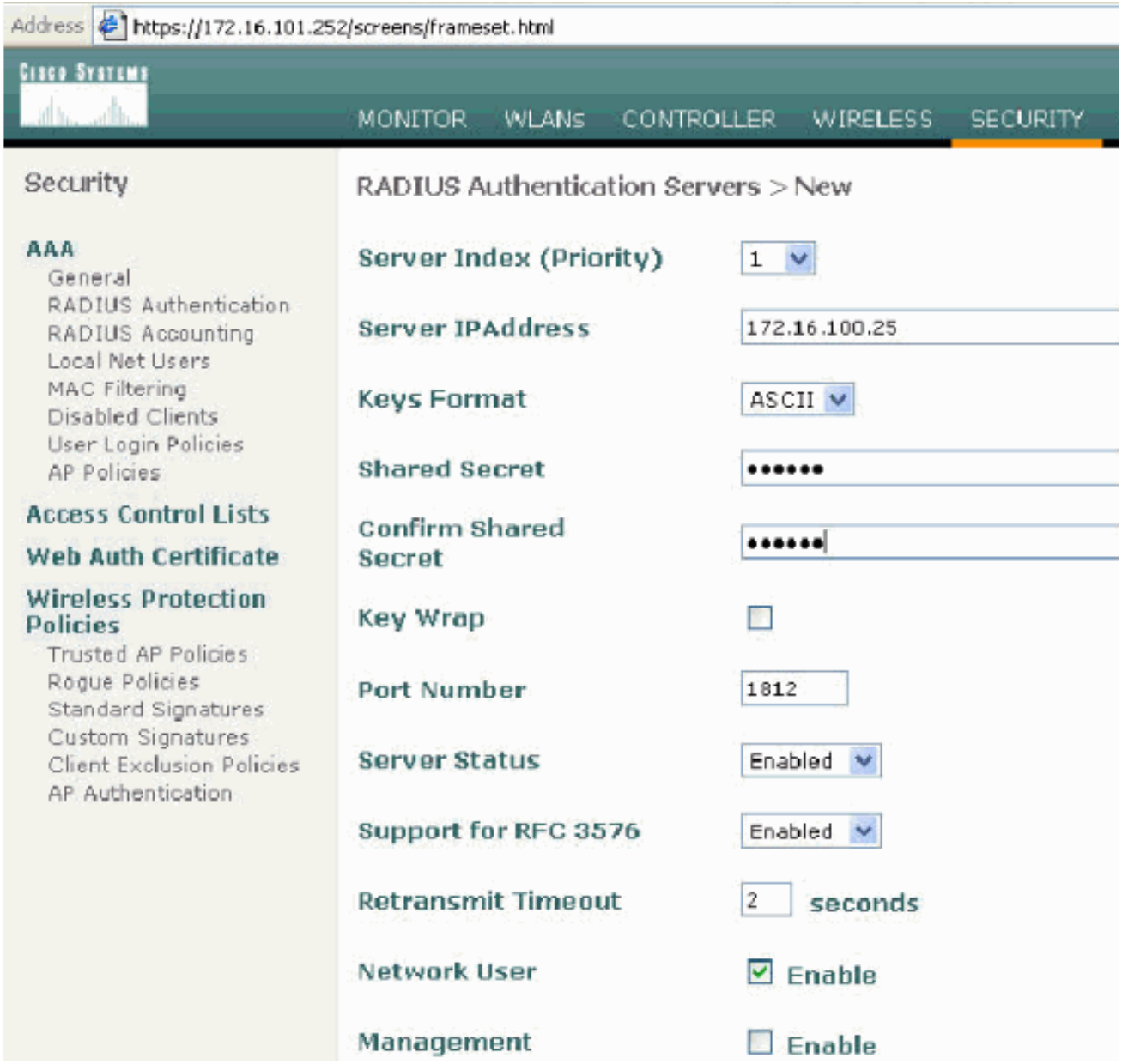
2. 按一下「**Login**」。
3. 使用預設使用者**admin**和預設密碼**admin**登入。
4. 在控制器選單下建立介面VLAN對映。
5. 按一下「**Interfaces**」。
6. 按一下「**New**」。
7. 在Interface name欄位中鍵入**Employee**。（此欄位可以是您喜歡的任何值。）
8. 在VLAN ID欄位中輸入**20**。（此欄位可以是網路中傳輸的任何VLAN。）
9. 按一下「**Apply**」。
10. 按照此Interfaces > Edit視窗的顯示配置資訊。

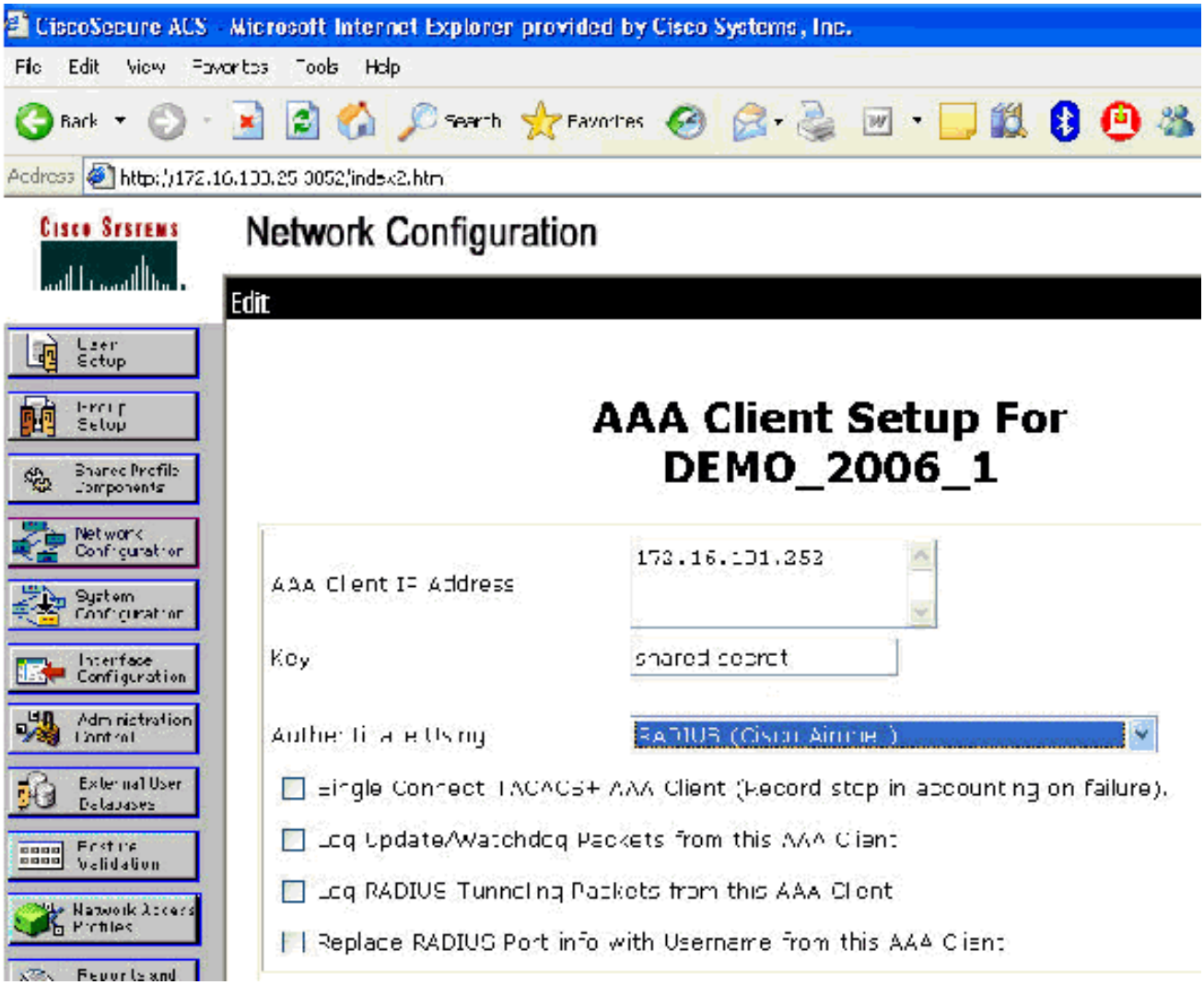


11. 按一下「**Apply**」。
12. 按一下「**WLAN**」。
13. 按一下「**New**」。
14. 在WLAN SSID欄位中鍵入**Employee**。
15. 按一下「**Apply**」。
16. 將資訊設定為此WLANs > Edit視窗所示。**注意：**WPA2是本實驗選擇的第2層加密方法。若要允許具有TKIP-MIC客戶端的WPA與此SSID關聯，您還可以選中**WPA相容模式**和**允許WPA2 TKIP客戶端**覈取方塊，或者選中不支援802.11i AES加密方法的客戶端。



17. 按一下「Apply」。
18. 按一下Security選單並新增RADIUS伺服器。
19. 按一下「New」。
20. 新增先前配置的ACS伺服器的RADIUS伺服器IP地址(172.16.100.25)。
21. 確保共用金鑰與ACS伺服器中配置的AAA客戶端匹配。
22. 按一下「Apply」。


Address
https://172.16.101.252/screens/frameset.html
Cisco Systems
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Client Exclusion Policies
AP Authentication
RADIUS Authentication Servers > New
Server Index (Priority)
1
Server IPAddress
172.16.100.25
Keys Format
ASCII
Shared Secret
Confirm Shared Secret
Key Wrap
Port Number
1812
Server Status
Enabled
Support for RFC 3576
Enabled
Retransmit Timeout
2
seconds
Network User
Enable
Management
Enable



23. 基本配置現已完成，您可以開始測試EAP-TLS。

EAP-TLS身份驗證

EAP-TLS身份驗證要求在無線客戶端上提供電腦和使用者證書，將EAP-TLS作為EAP型別新增到遠端訪問策略以進行無線訪問，並重新配置無線網路連線。

要配置DC_CA以為電腦和使用者證書提供自動註冊，請完成本節中的步驟。

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。

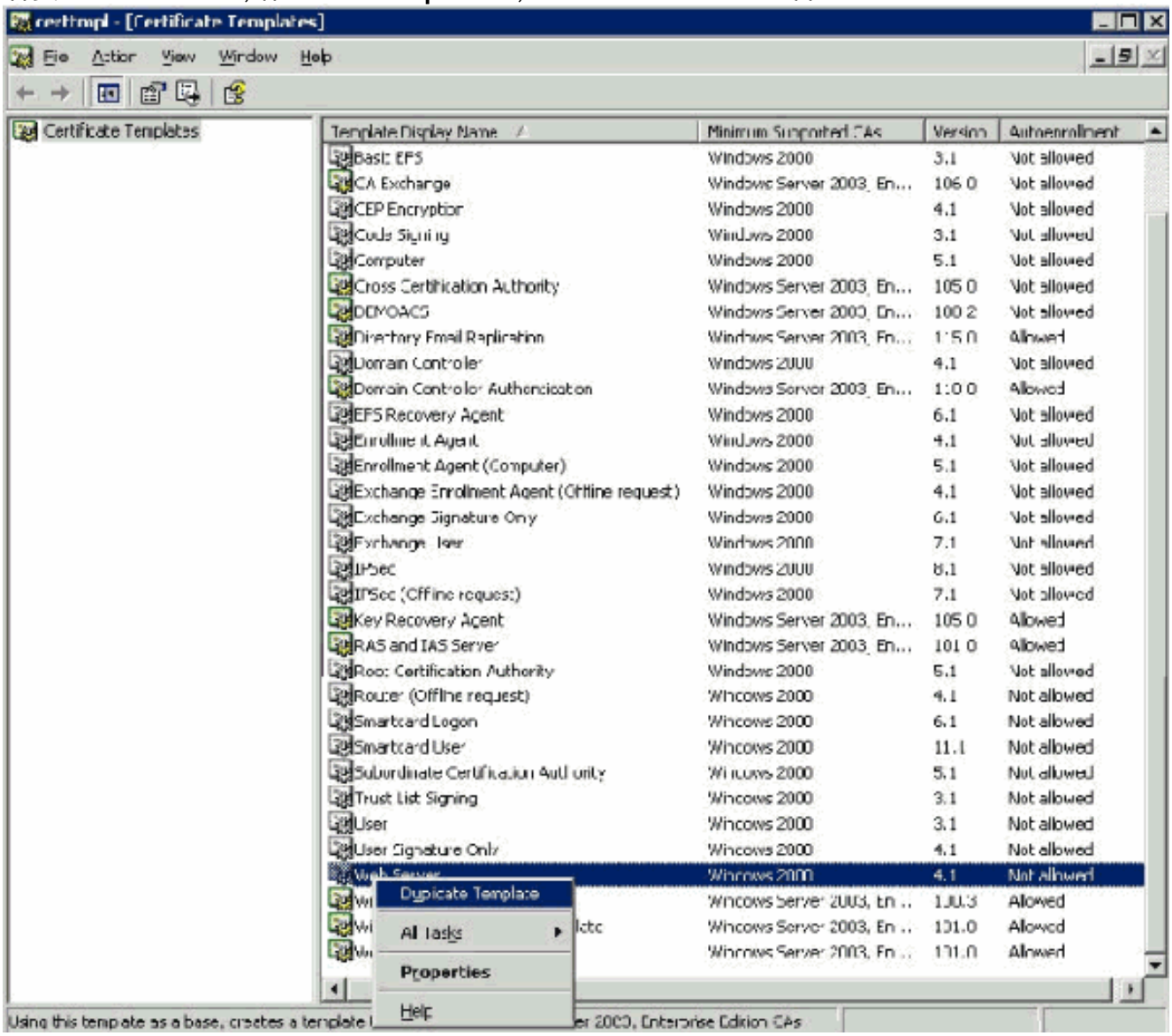
注意：Windows 2000允許匯出金鑰，如果您使用Windows 2000，則無需遵循這些步驟。

安裝證書模板管理單元

請完成以下步驟：

1. 選擇**開始>運行**，鍵入**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**證書模板**，按一下**關閉**，然後按一下**確定**。
4. 在控制檯樹中，按一下**Certificate Templates**。所有證書模板都將顯示在詳細資訊窗格中。

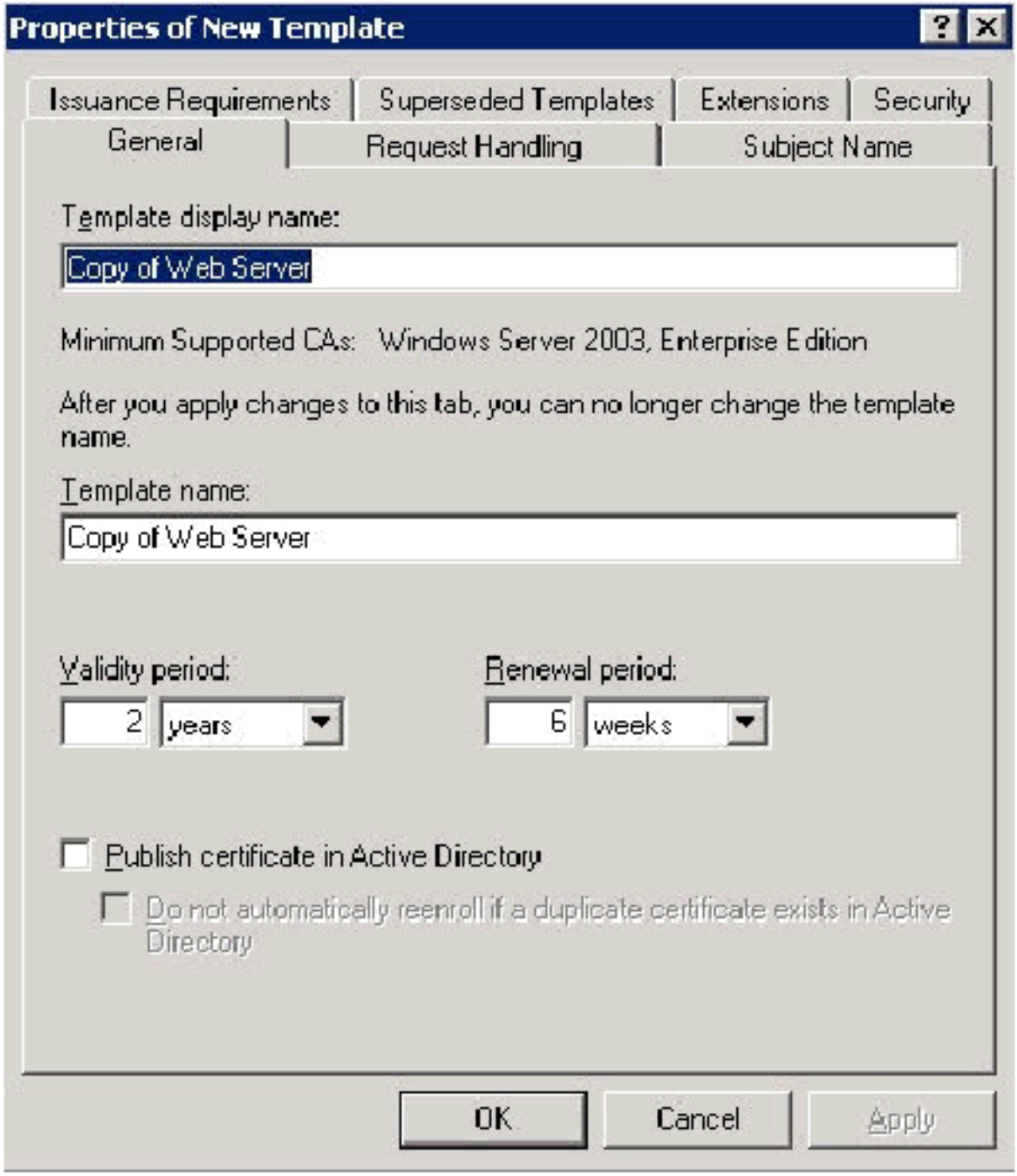
5. 若要繞過步驟2至4，請鍵入**certtmpl.msc**，以開啟「證書模板」管理單元。



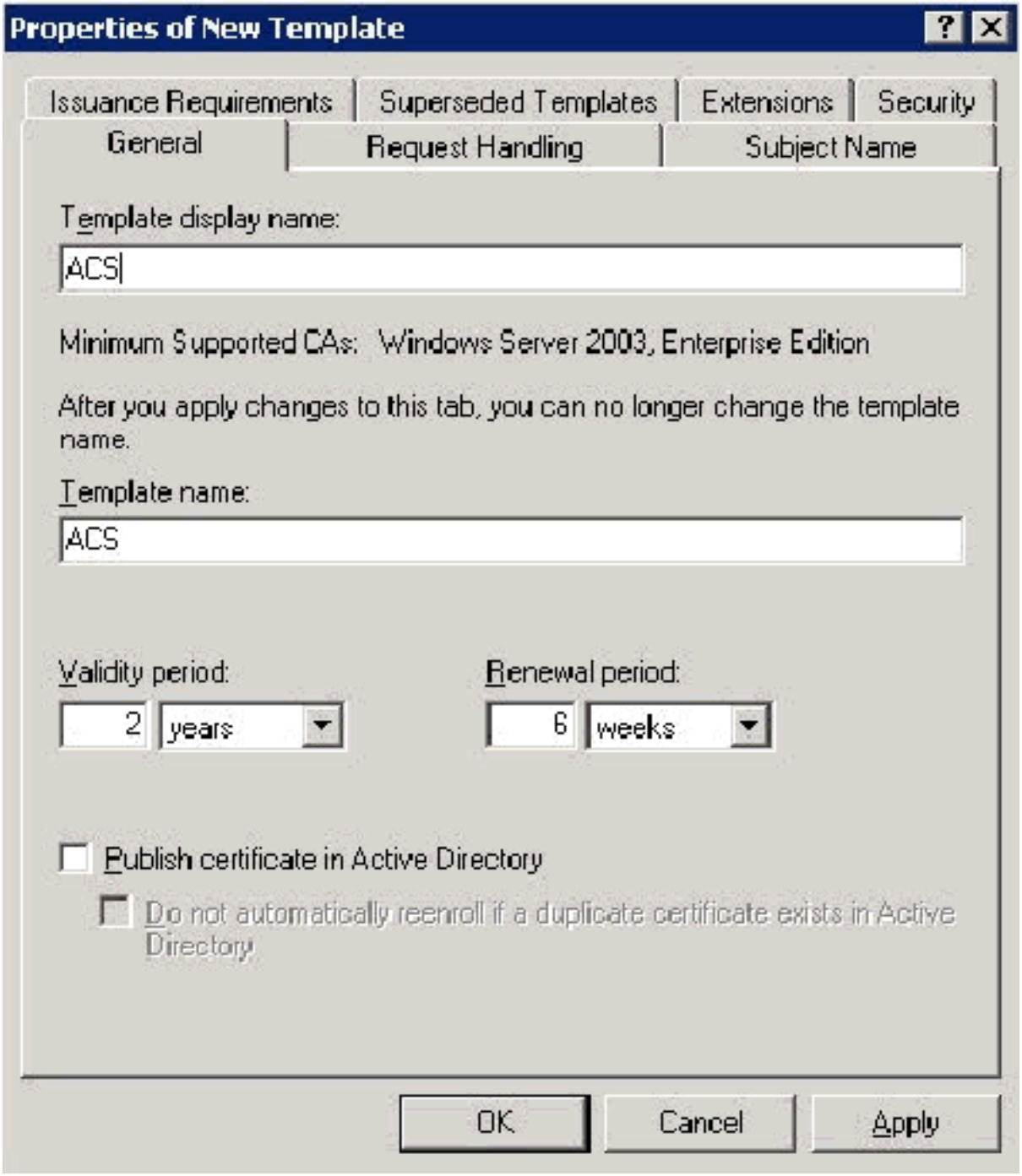
為ACS Web伺服器建立證書模板

請完成以下步驟：

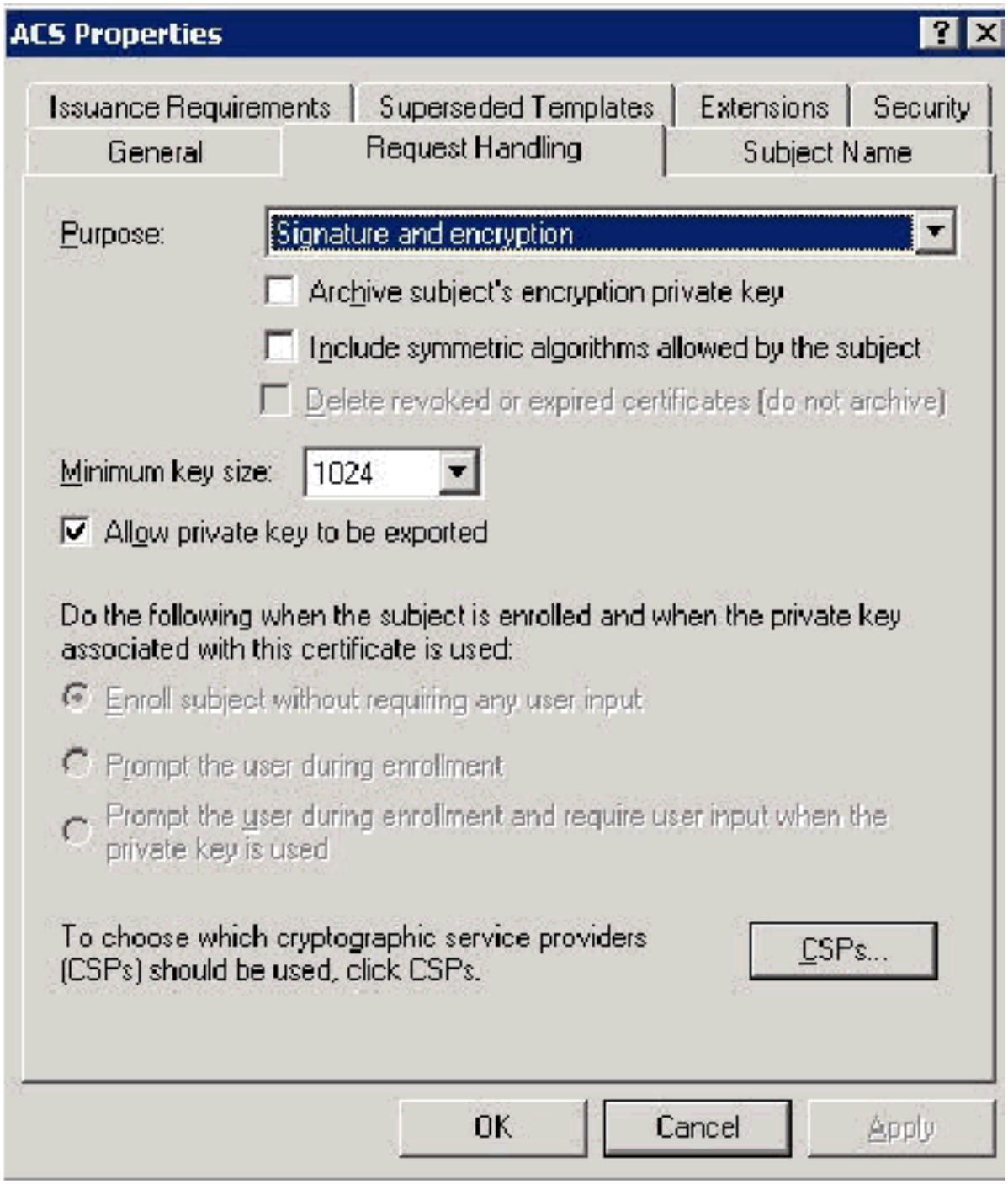
1. 在「證書模板」管理單元的「詳細資訊」窗格中，按一下**Web Server**模板。
2. 在「操作」選單上，按一下**複製模板**。



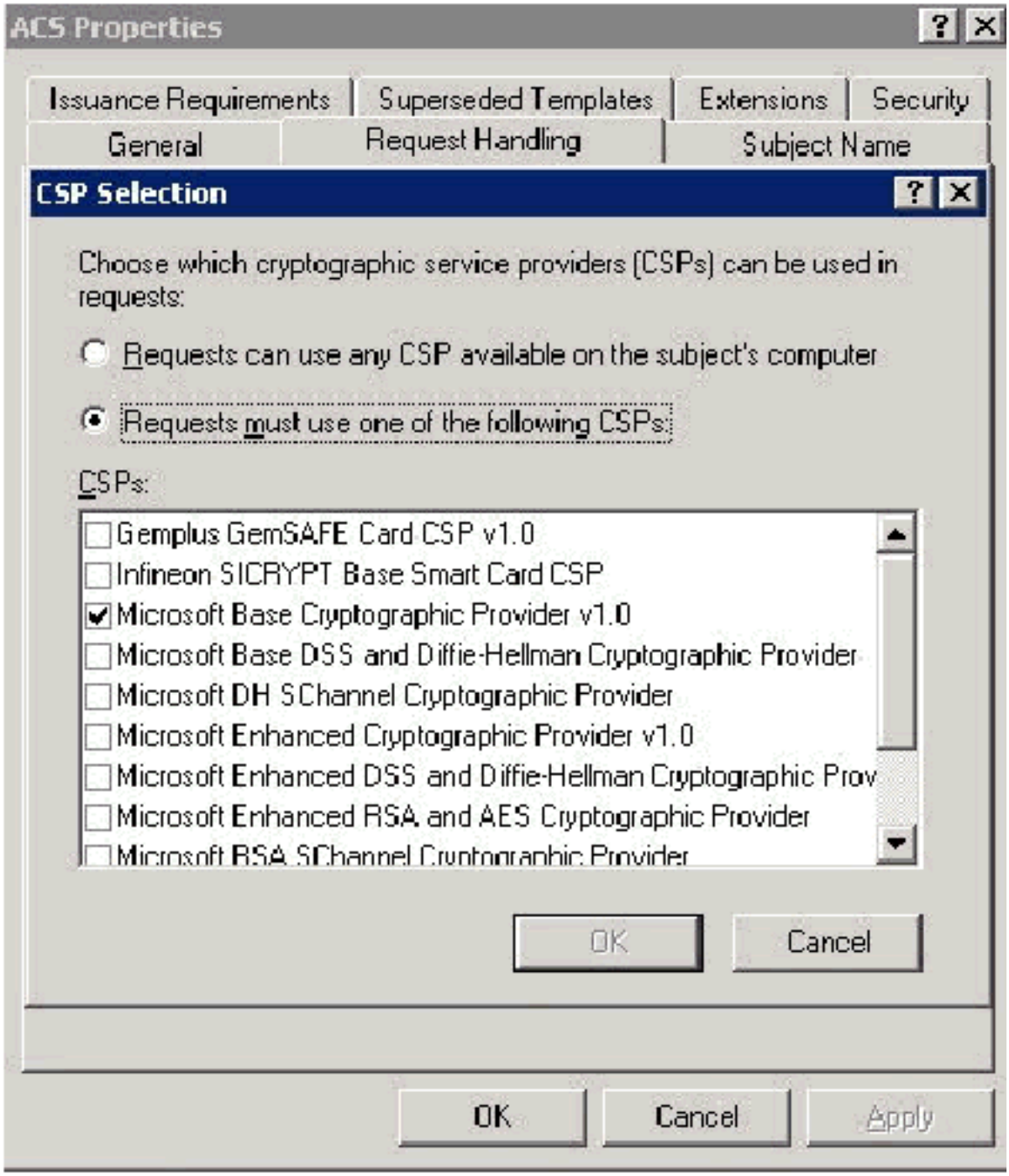
3. 在「模板顯示名稱」欄位中，鍵入**ACS**。



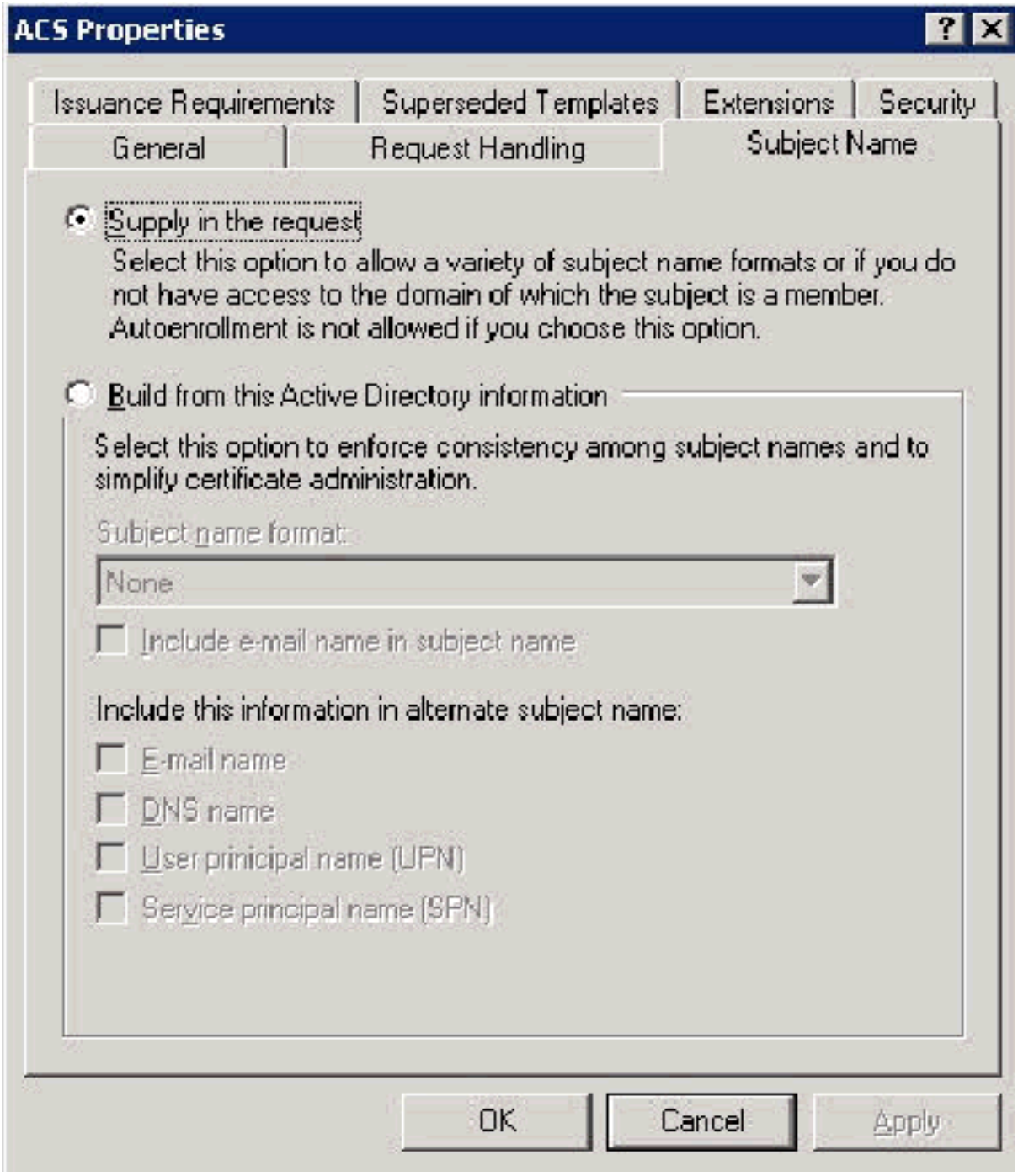
4. 轉到「請求處理」頁籤，然後選中**允許匯出私鑰**。



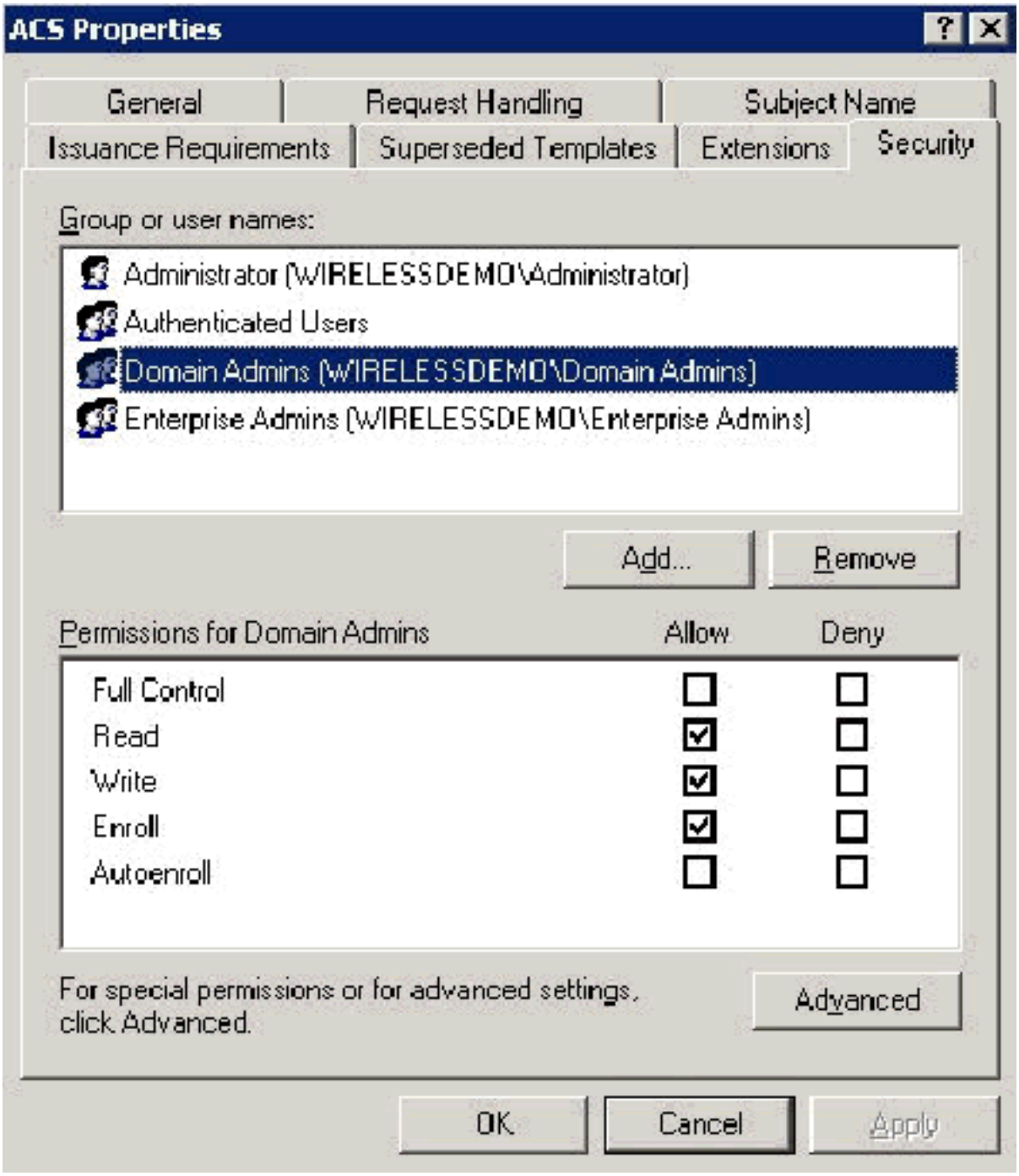
5. 選擇**請求必須使用以下CSP之一**，並選中**Microsoft Base Cryptographic Provider v1.0**。取消選中任何其他CSP，然後按一下**確定**。



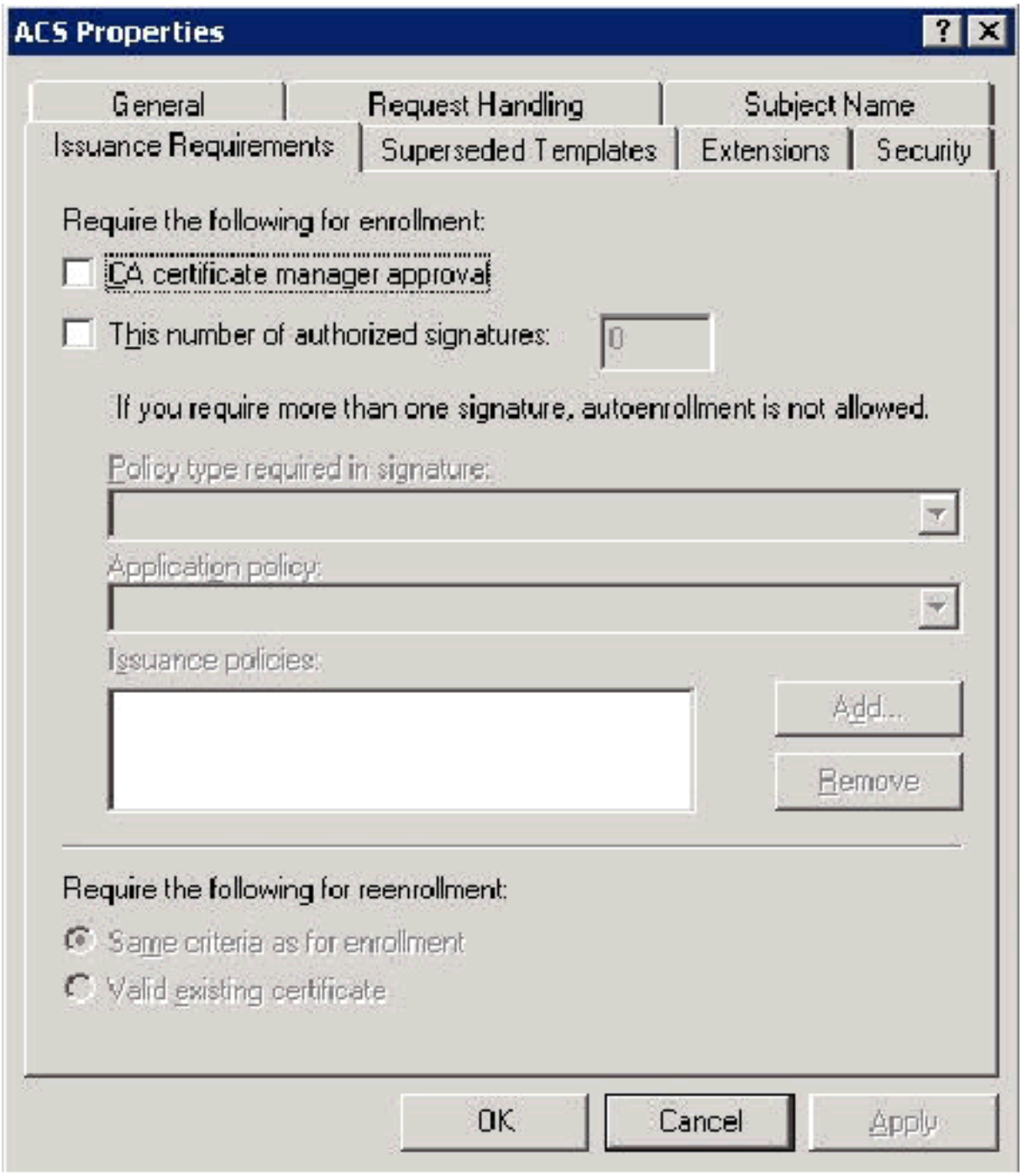
6. 轉至「主題名稱」頁籤，在請求**中選擇「供應」，**然後單**擊「確定」**。



7. 轉到「安全」頁籤，選中**Domain Admins Group**，並確保選中「允許」下的**Enroll**選項。**重要事項：**如果您選擇僅基於此Active Directory資訊構建，請選中**User principal name(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WirelessUser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。

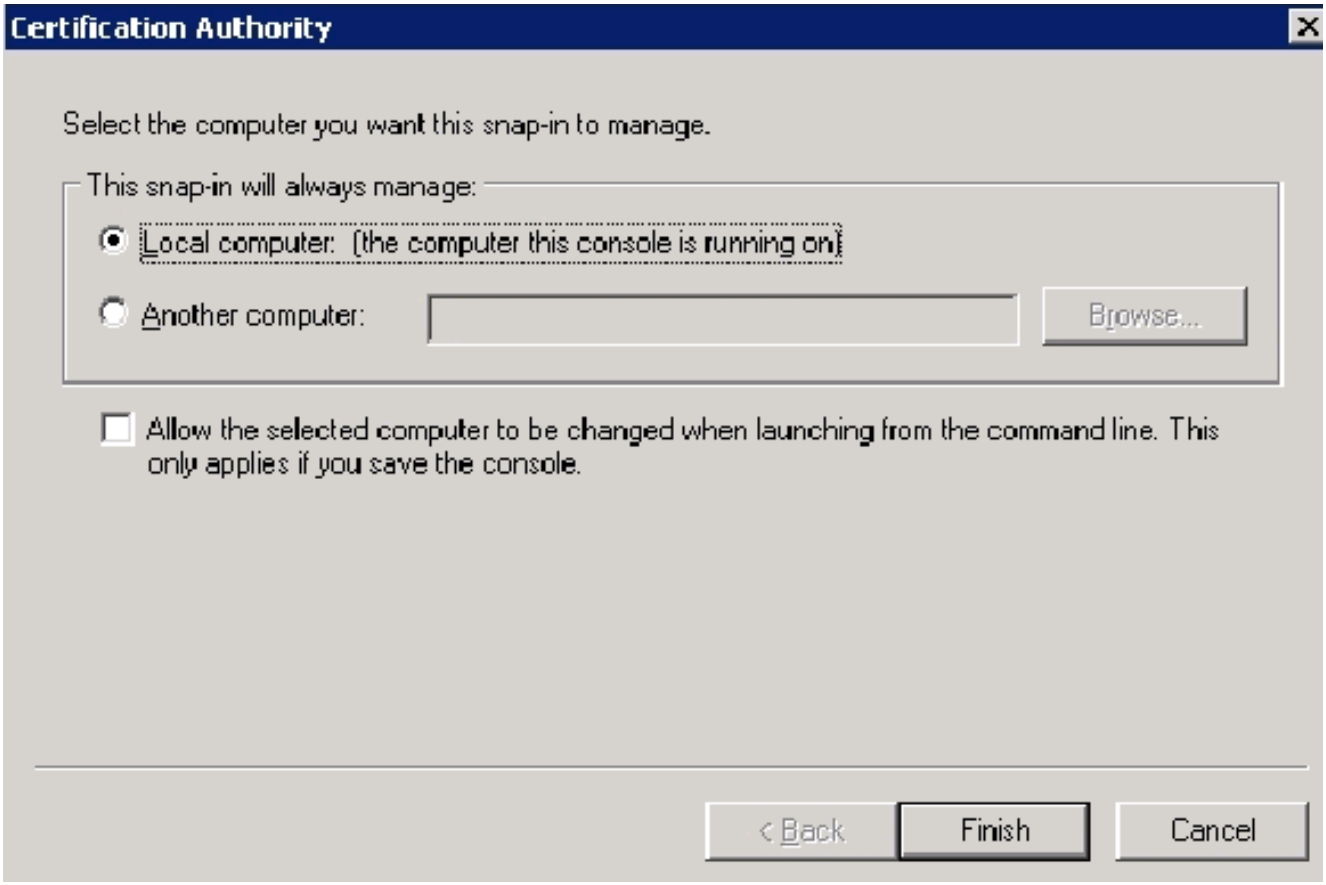


9. 按一下**OK**儲存模板，然後從「證書頒發機構」管理單元發佈此模板。

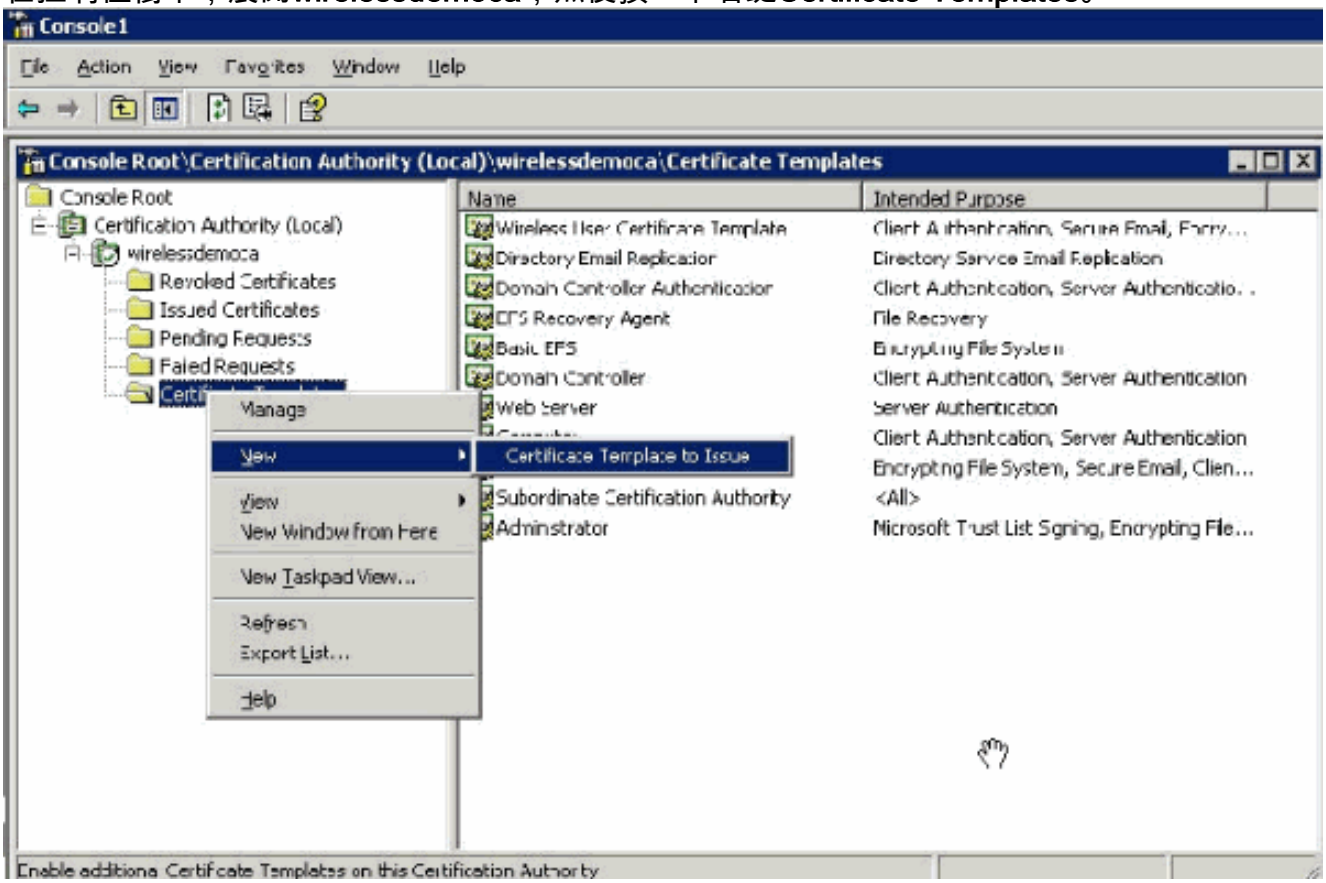
啟用新的ACS Web伺服器證書模板

請完成以下步驟：

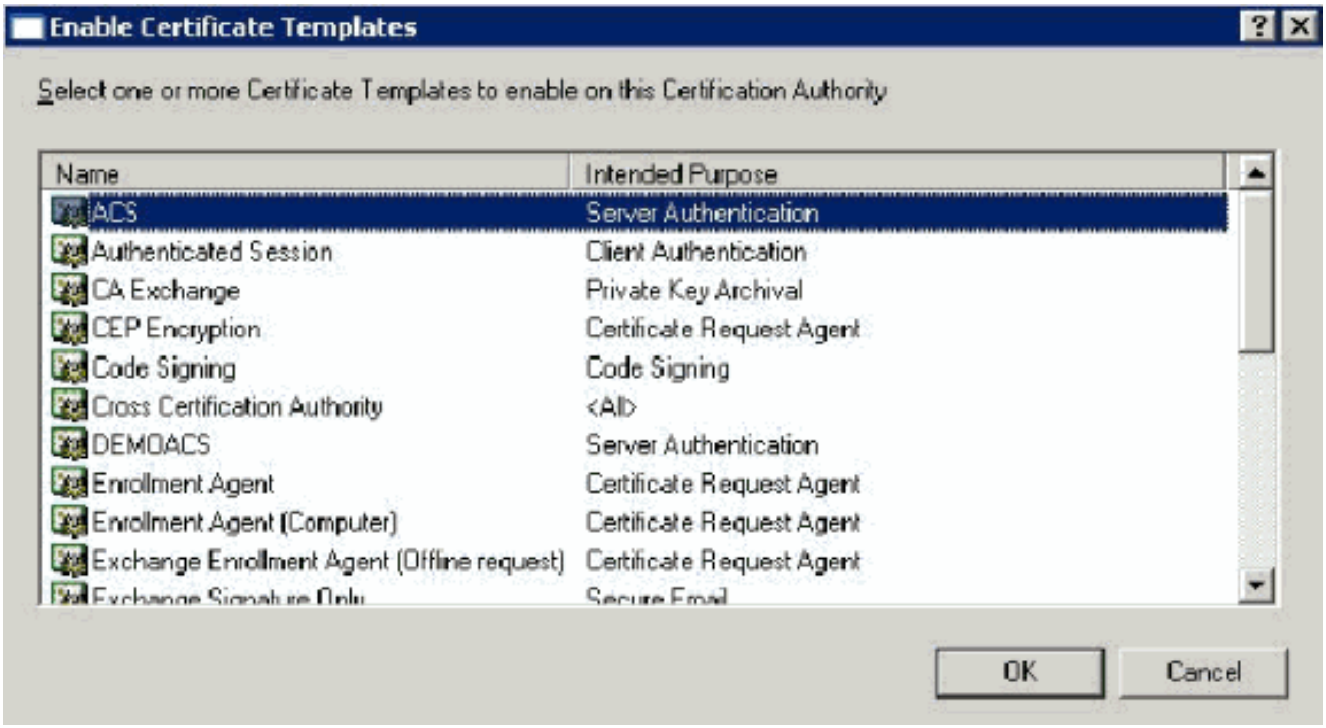
1. 開啟**證書頒發機**構管理單元。按照為ACS Web伺服器建立證書模板部分中的步驟1-3操作，選擇**Certificate Authority**選項，選擇**Local Computer**，然後按一下**Finish**。



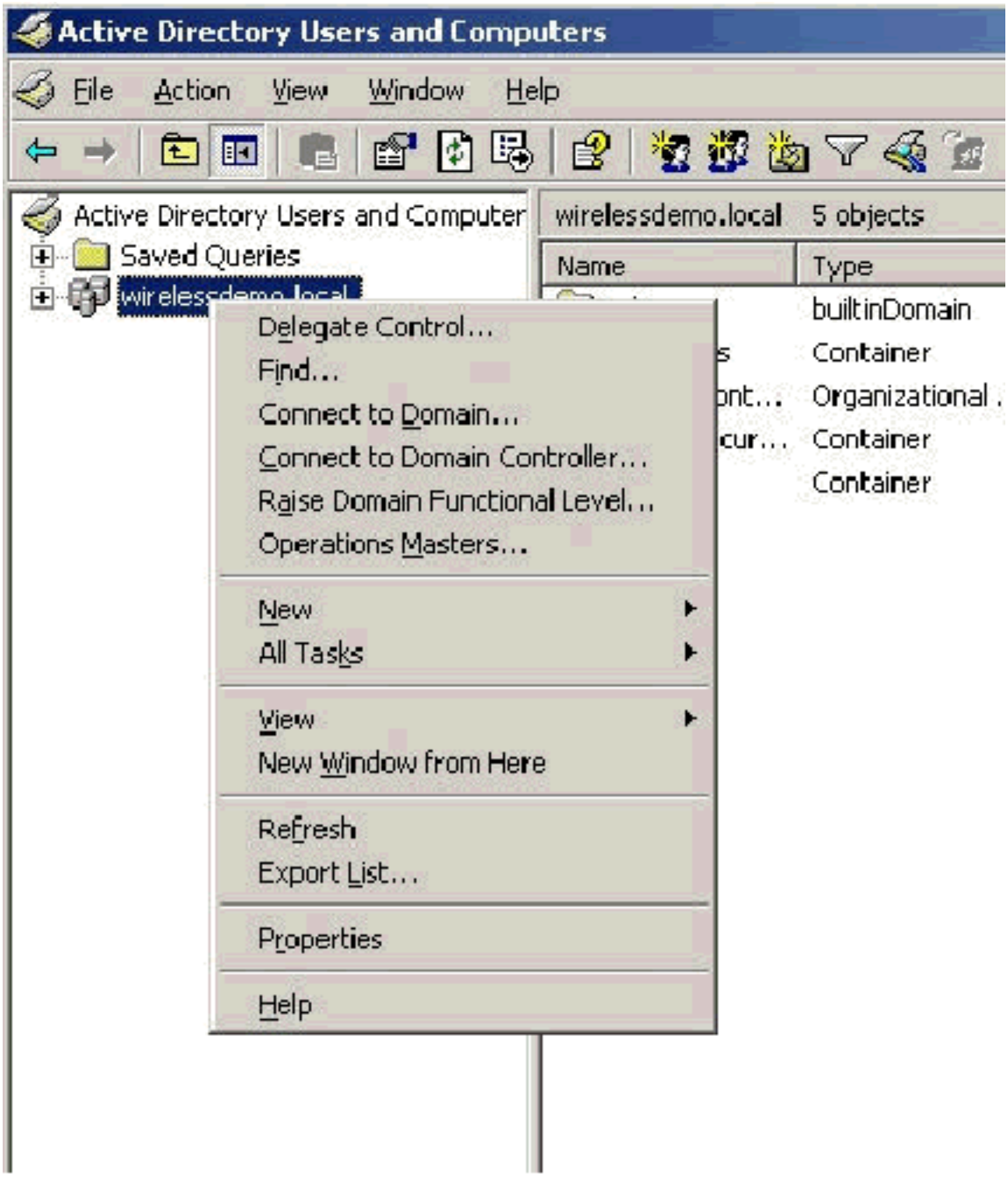
2. 在控制檯樹中，展開**wirelessdemoca**，然後按一下右鍵**Certificate Templates**。



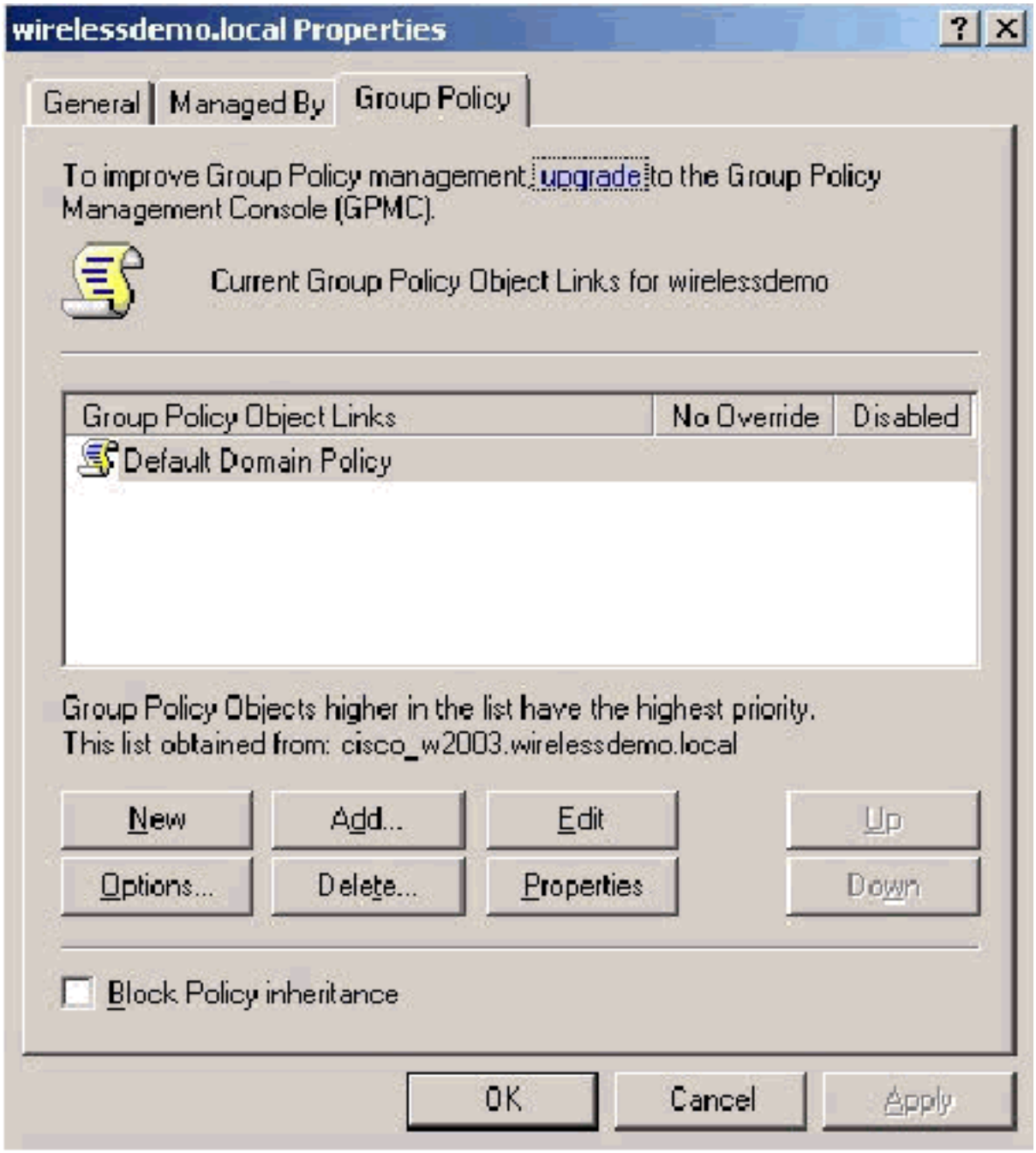
3. 選擇**New > Certificate Template to Issue**。
4. 按一下**ACS** Certificate Template。



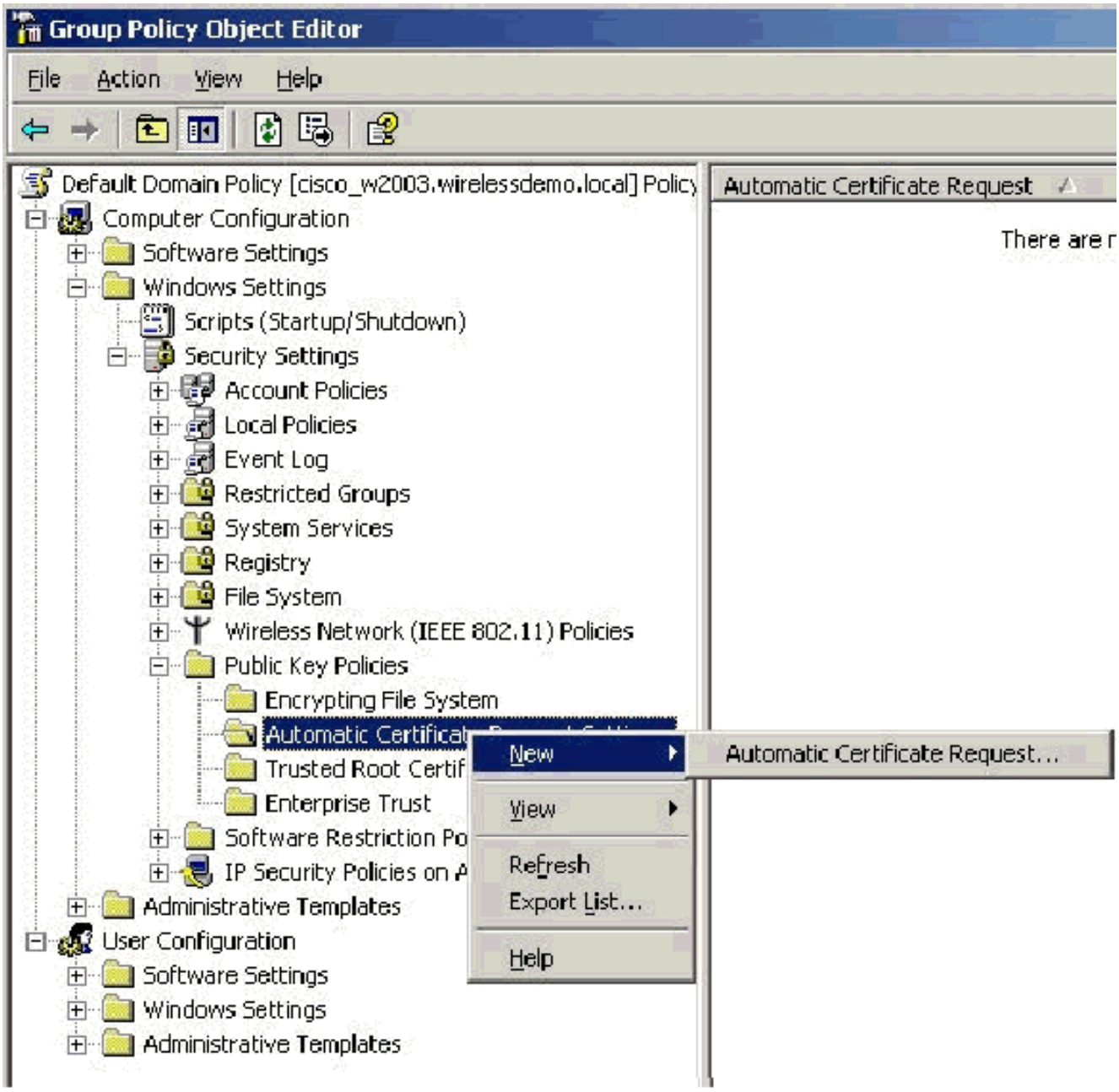
5. 按一下**OK**，然後開啟**Active Directory使用者和電腦**管理單元。
6. 在控制檯樹中，按兩下**Active Directory Users and Computers**，按一下右鍵 **wirelessdemo.local domain**，然後按一下**Properties**。



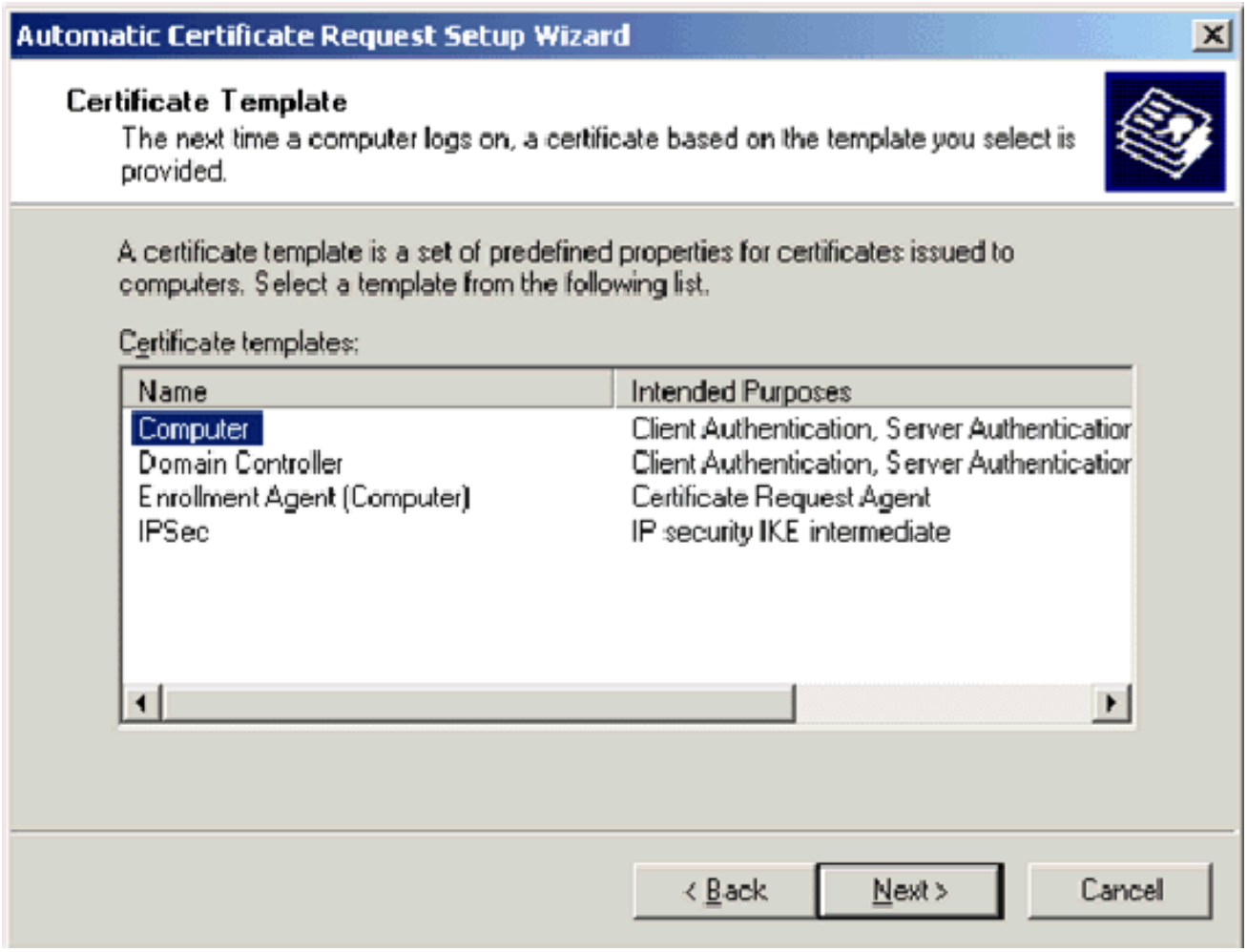
7. 在Group Policy頁籤上，按一下**Default Domain Policy**，然後按一下**Edit**。這將開啟組策略對象編輯器管理單元。



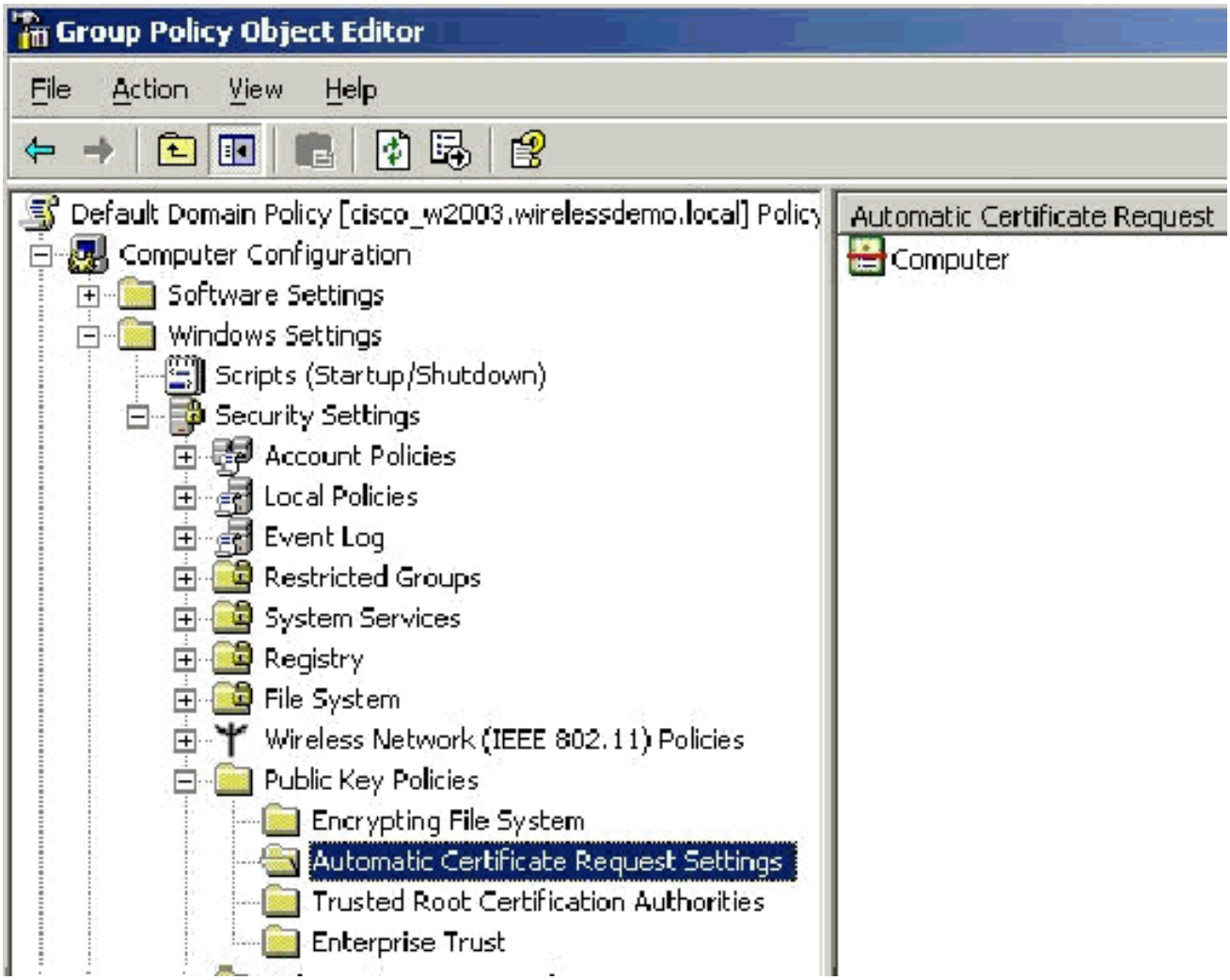
8. 在控制檯樹中，展開**Computer Configuration > Windows Settings > Security Settings > Public Key Policies**，然後選擇**Automatic Certificate Request Settings**。



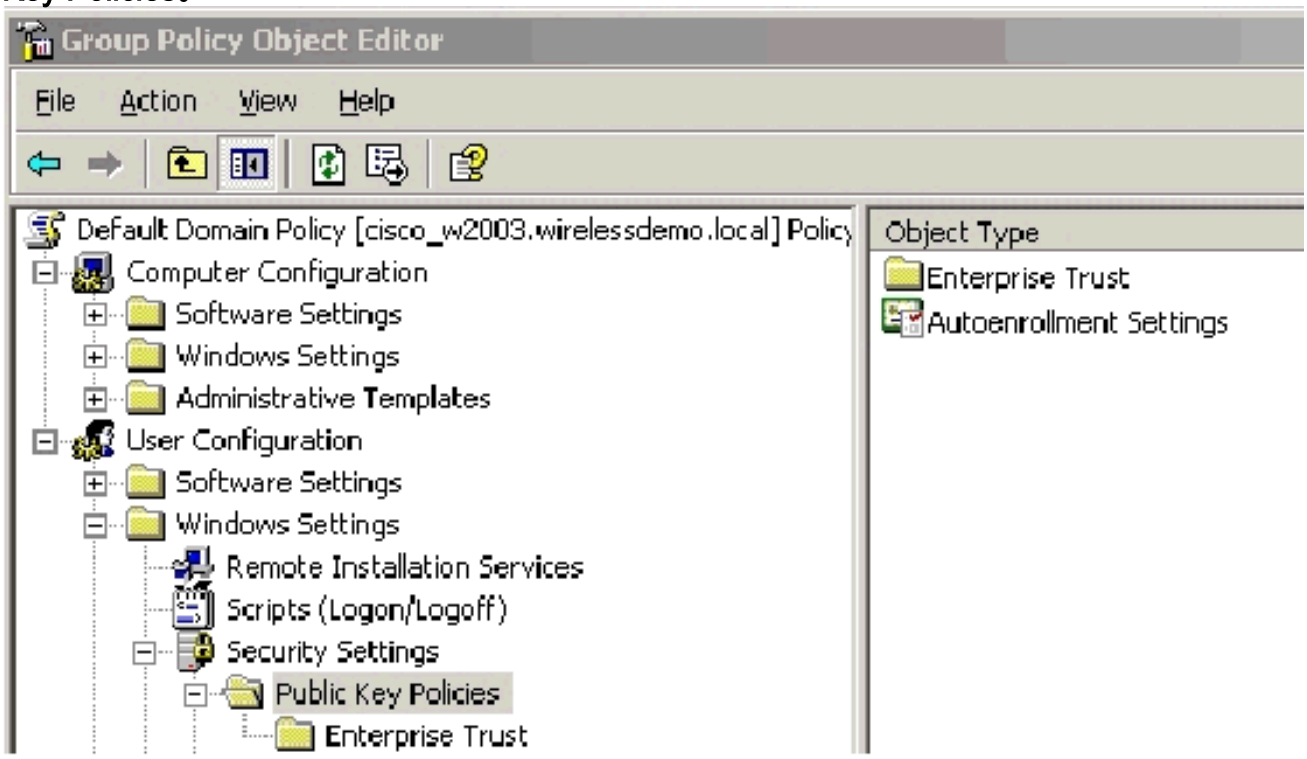
9. 按一下右鍵**Automatic Certificate Request Settings**，然後選擇**New > Automatic Certificate Request**。
10. 在「歡迎使用自動證書請求設定嚮導」頁面上，按一下**下一步**。
11. 在「Certificate Template」頁面上，按一下**Computer**，然後按一下**Next**。



12. 在「完成自動證書請求設定嚮導」頁上，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。

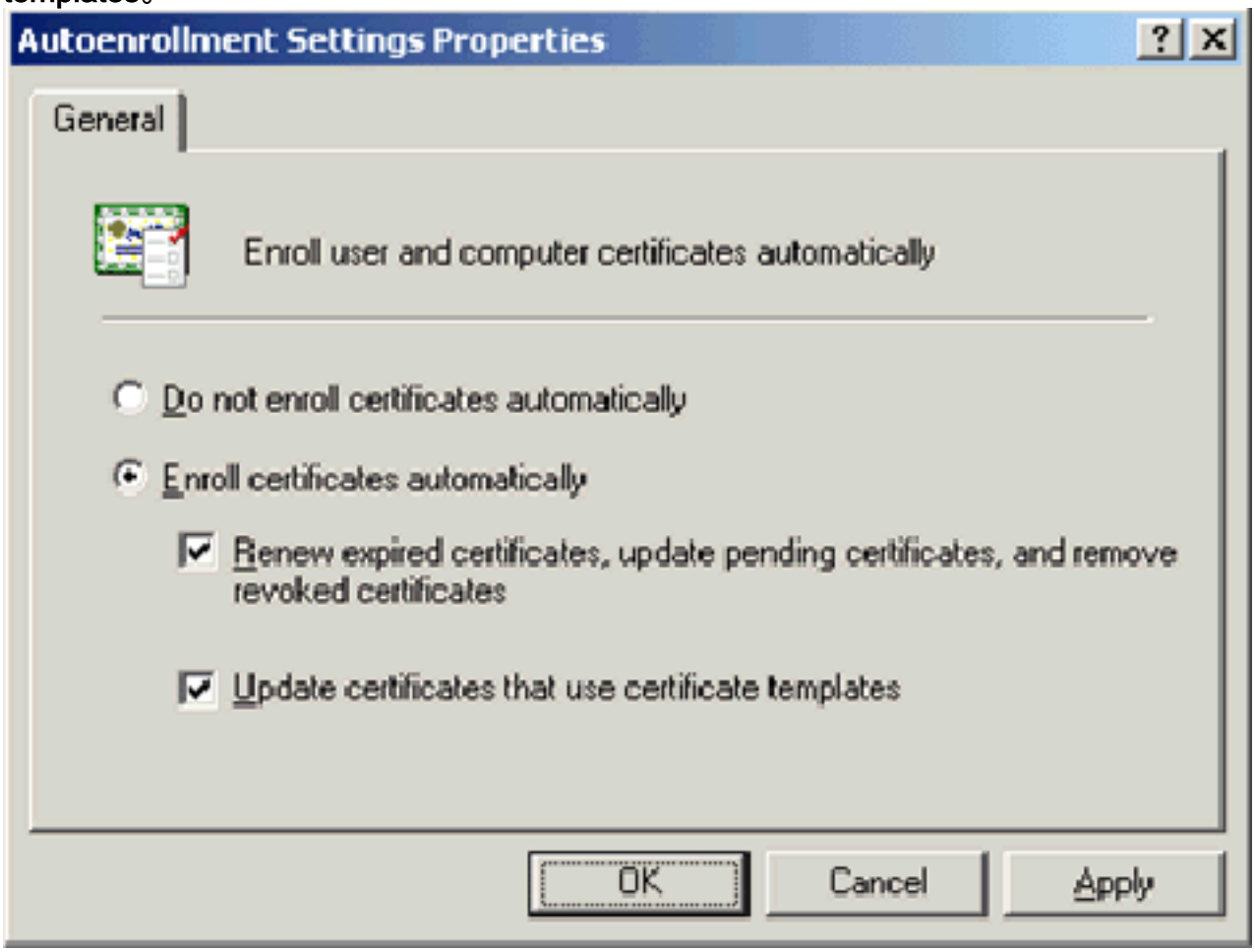


13. 在控制檯樹中，展開User Configuration > Windows Settings > Security Settings > Public Key Policies。



14. 在詳細資訊窗格中，按兩下**自動註冊設定**。
15. 選擇Enroll certificates automatically，然後選中Renew expired certificates， update pending certificates and remove revoked certificates和Update certificate that use certificate

templates。



16. 按一下「OK」（確定）。

ACS 4.0證書設定

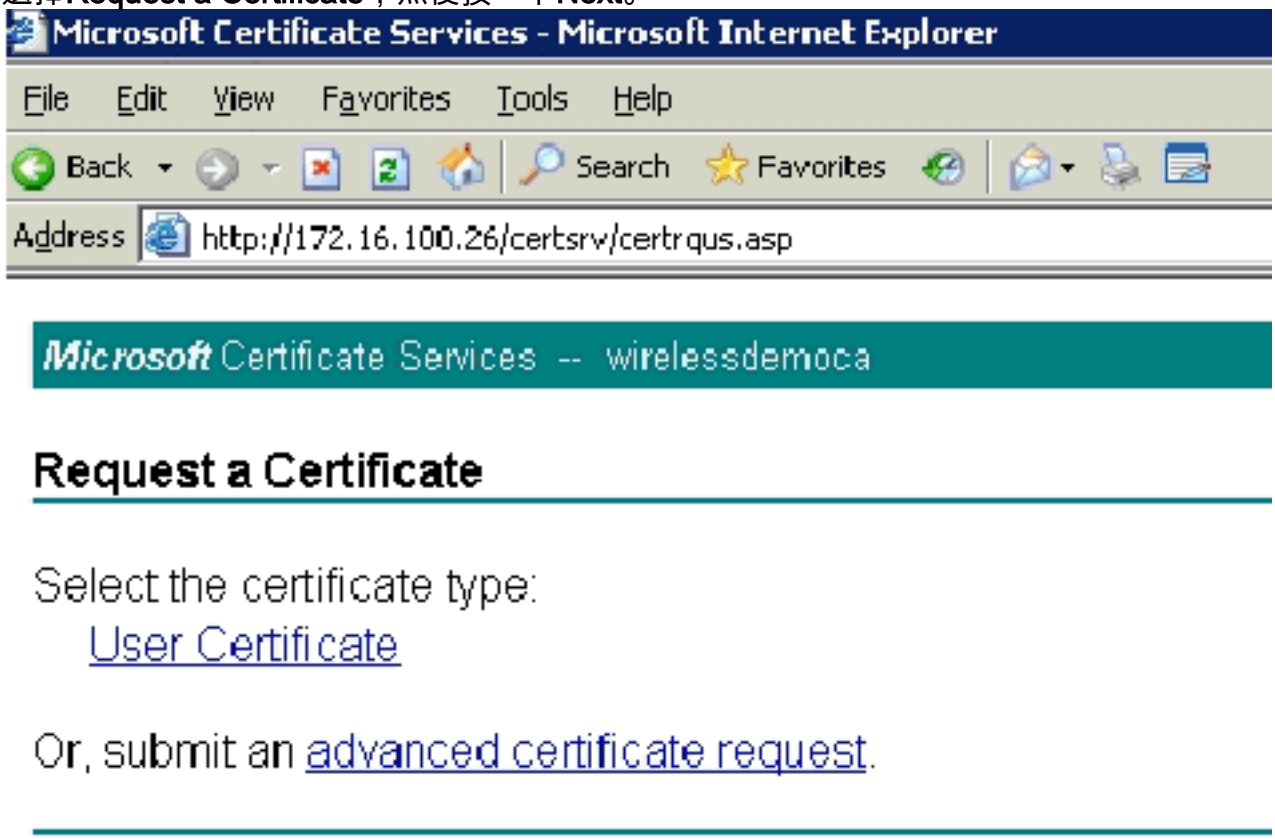
配置ACS的可匯出證書

重要事項：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 EAP-TLS客戶端進行身份驗證。

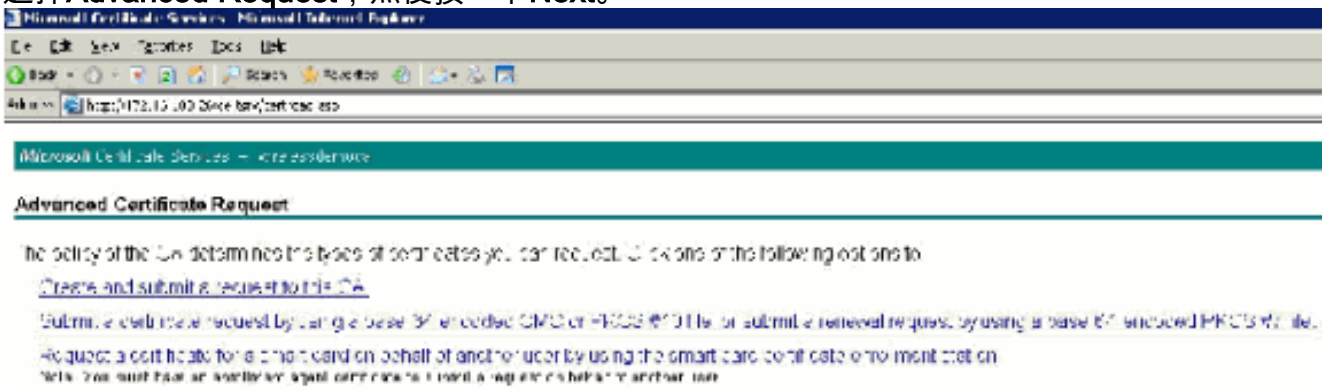
重要事項：確保IIS管理器在證書設定過程中未開啟，因為它會導致快取資訊出現問題。

1. 使用具有企業管理員許可權的帳戶登入到ACS伺服器。
2. 在本地ACS電腦上，將瀏覽器指向Microsoft證書頒發機構伺服器**http://IP-address-of-Root-CA/certsrv**。在本例中，IP地址為**172.16.100.26**。
3. 以管理員身份登入。

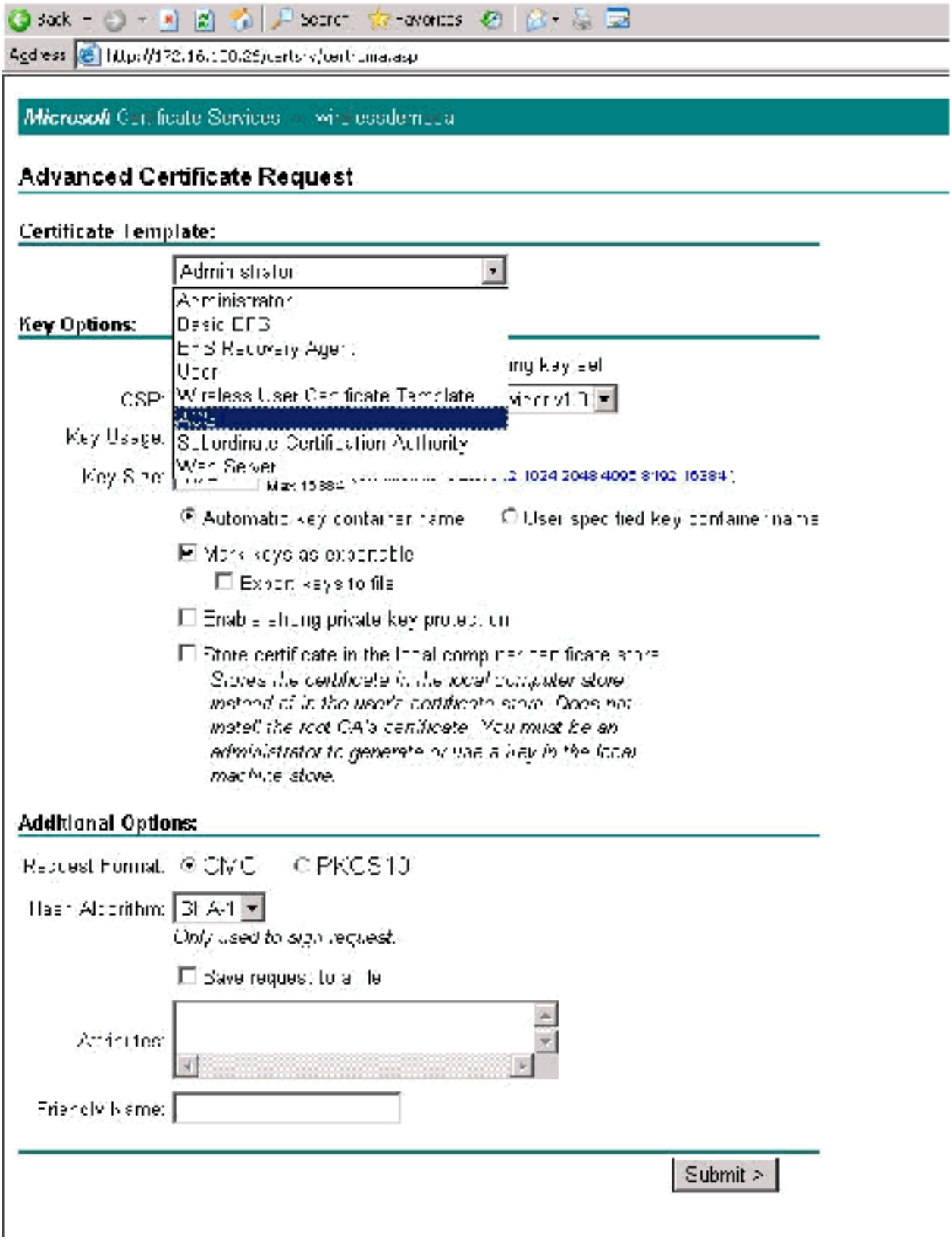
4. 選擇**Request a Certificate**，然後按一下**Next**。



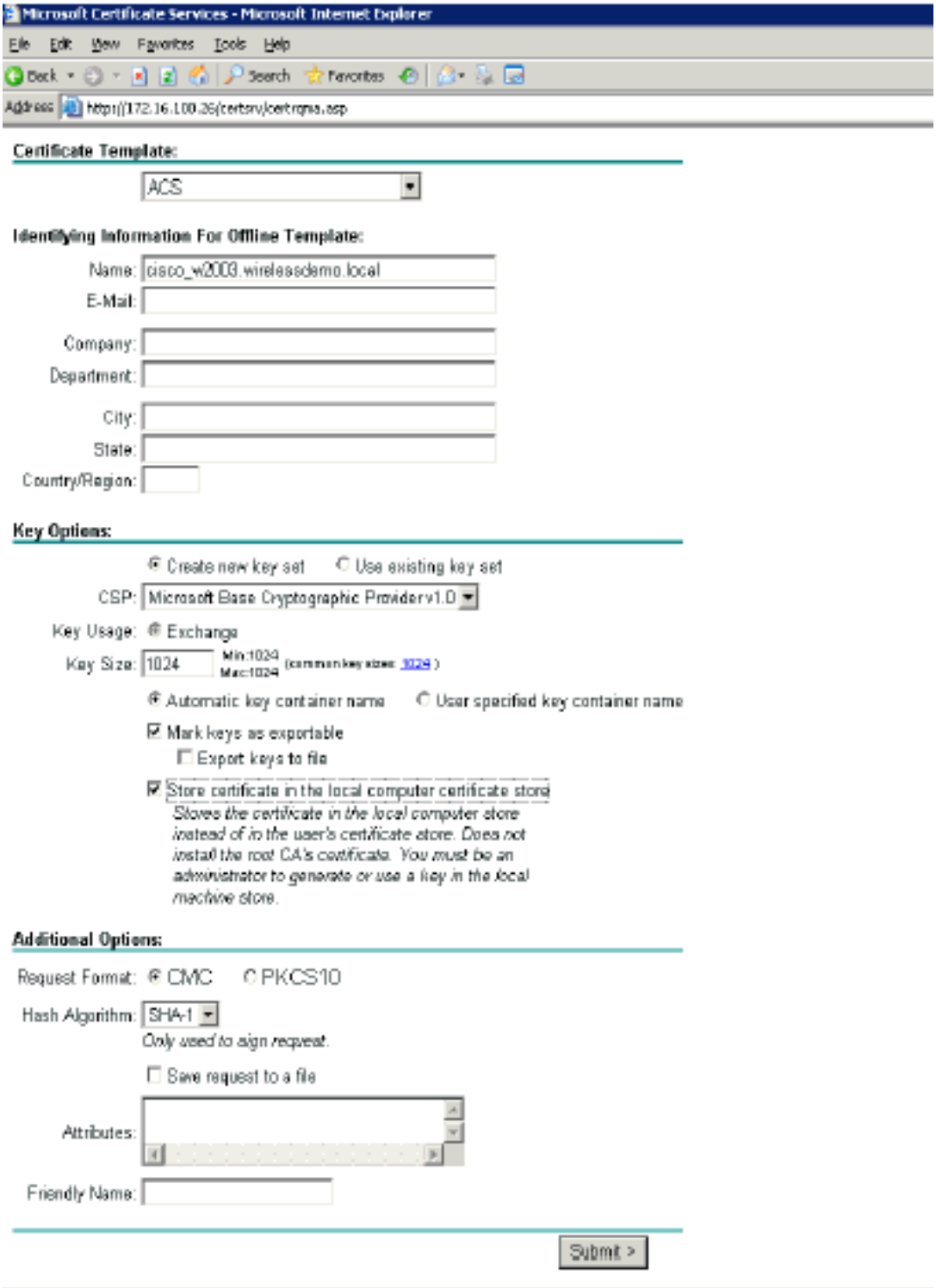
5. 選擇**Advanced Request**，然後按一下**Next**。



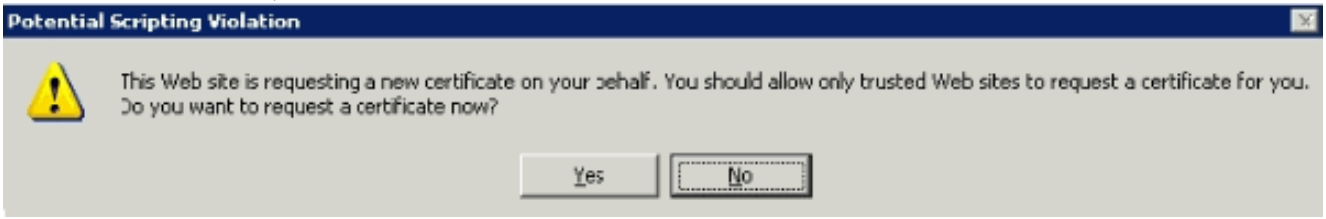
6. 選擇**Create and submit a request to this CA**，然後按一下**Next**。**重要事項**：執行此步驟的原因是Windows 2003不允許可匯出金鑰，並且您需要根據之前建立的ACS證書生成證書請求。



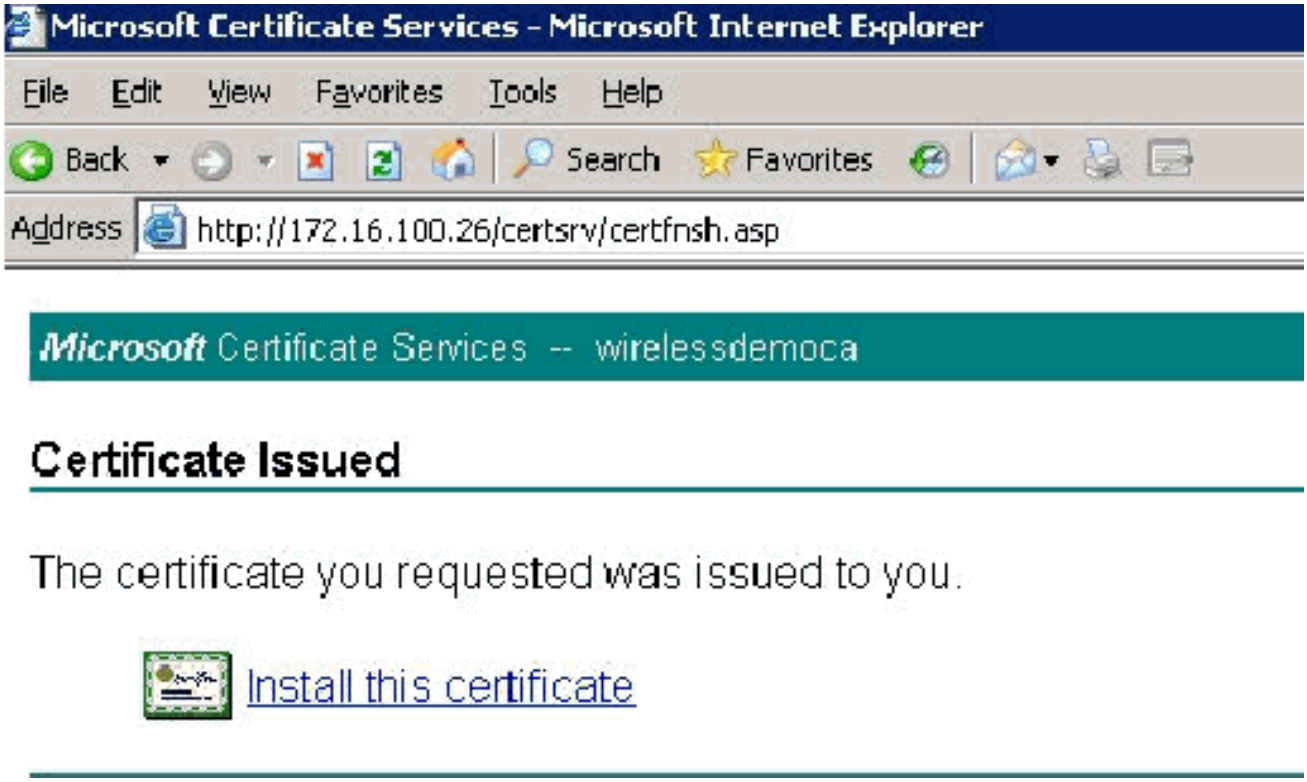
7. 在「Certificate Templates」中，選擇先前建立的名為**ACS**的證書模板。選擇模板後，選項會更改。
8. 將名稱配置為ACS伺服器的完全限定域名。在這種情況下，ACS伺服器名稱為cisco_w2003.wirelessdemo.local。確保選中**Store certificate in the local computer certificate store**，然後按一下**Submit**。



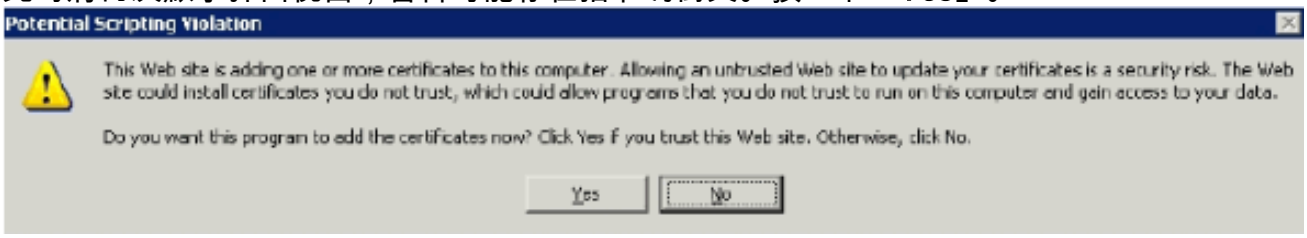
9. 出現一個彈出視窗，警告可能存在指令碼衝突。按一下「**Yes**」。



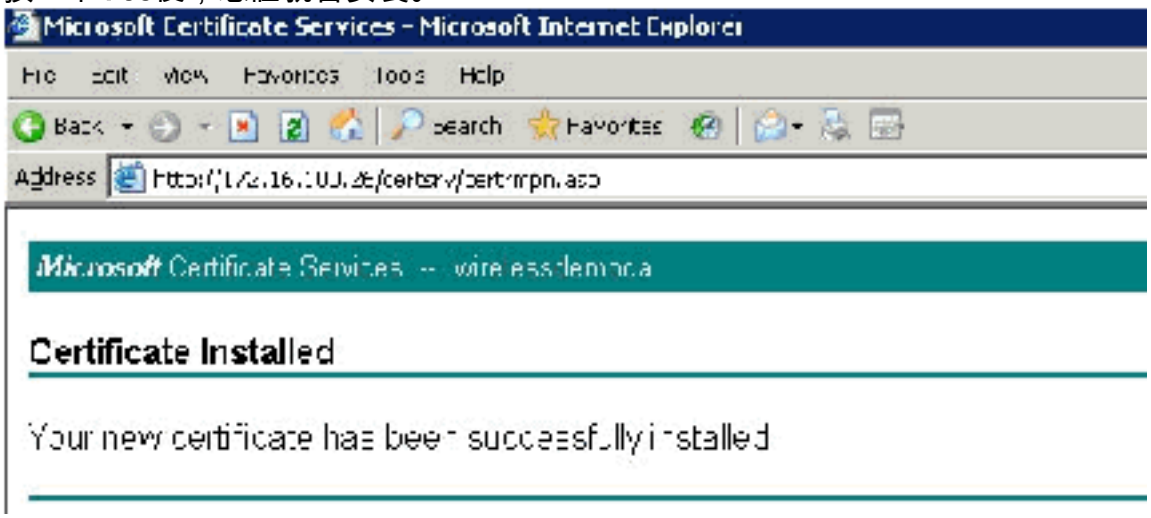
10. 按一下「**Install this certificate**」。



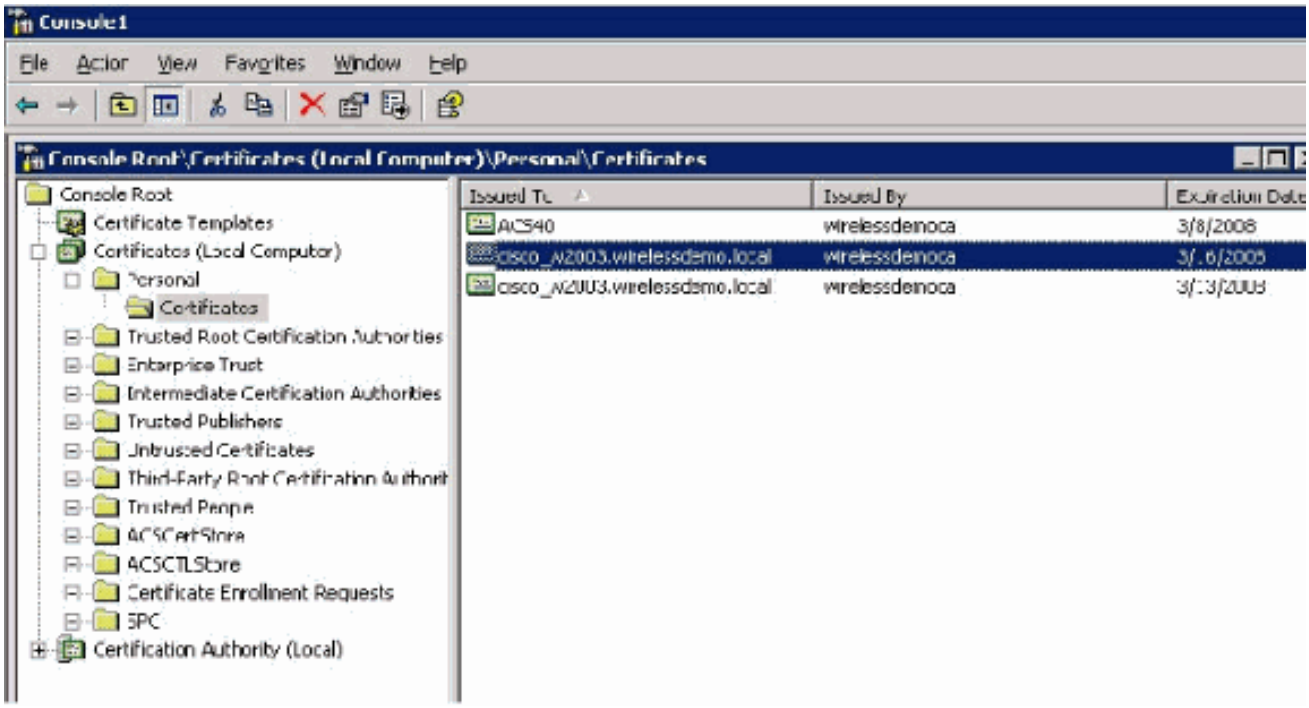
11. 此時將再次顯示彈出視窗，警告可能存在指令碼衝突。按一下「**Yes**」。



12. 按一下**Yes**後，憑證就會安裝。



13. 此時，證書安裝在Certificates資料夾中。若要訪問此資料夾，請選擇**「開始」>「運行」**，鍵入**mmc**，按**Enter**，然後選擇**「個人」>「證書」**。

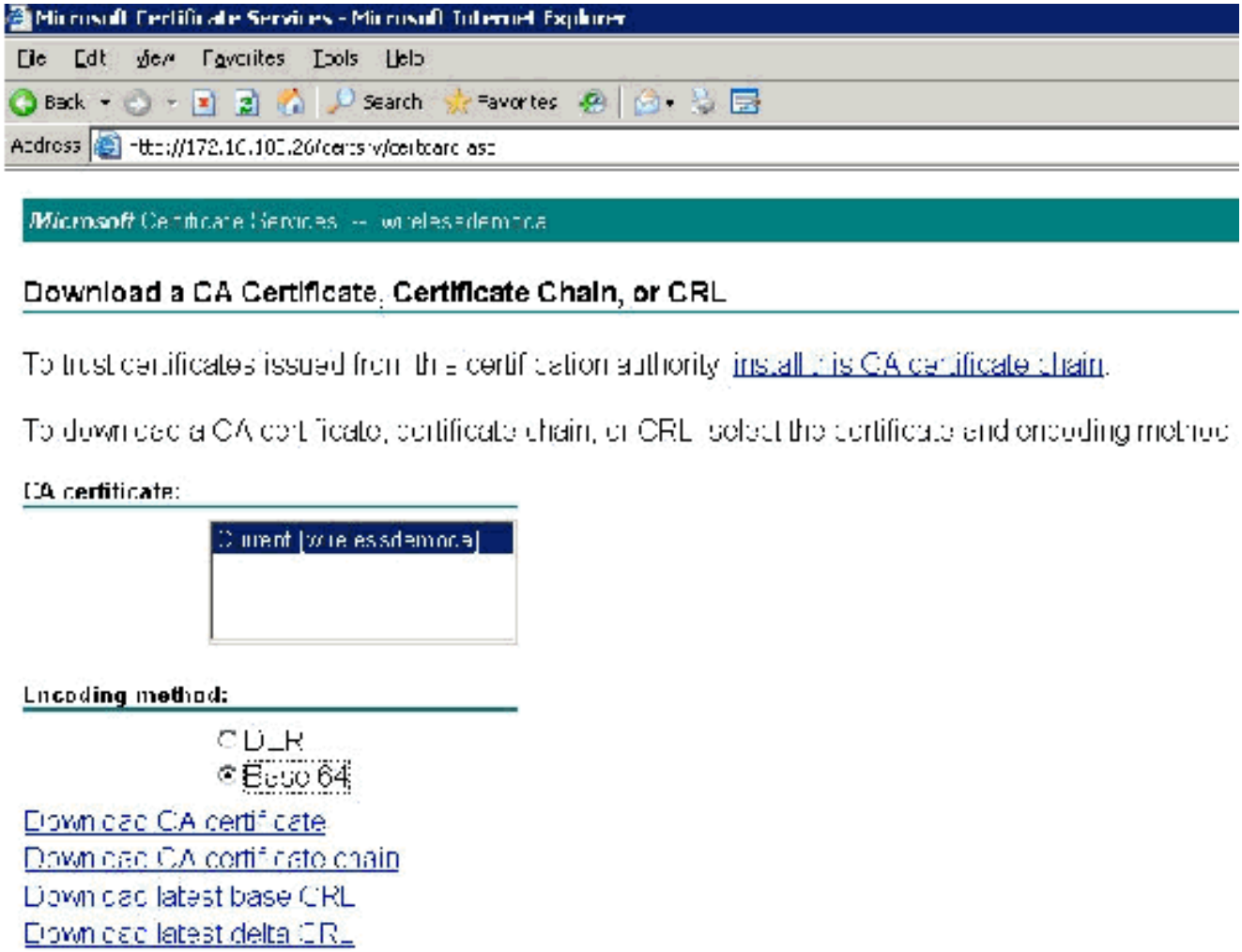


14. 由於證書已安裝到本地電腦（在本例中為ACS或cisco_w2003），因此您需要為ACS 4.0證書檔案配置生成證書檔案(.cer)。
15. 在ACS伺服器（本例中為cisco_w2003）上，將Microsoft證書頒發機構伺服器上的瀏覽器指向**http://172.16.100.26 /certsrv**。

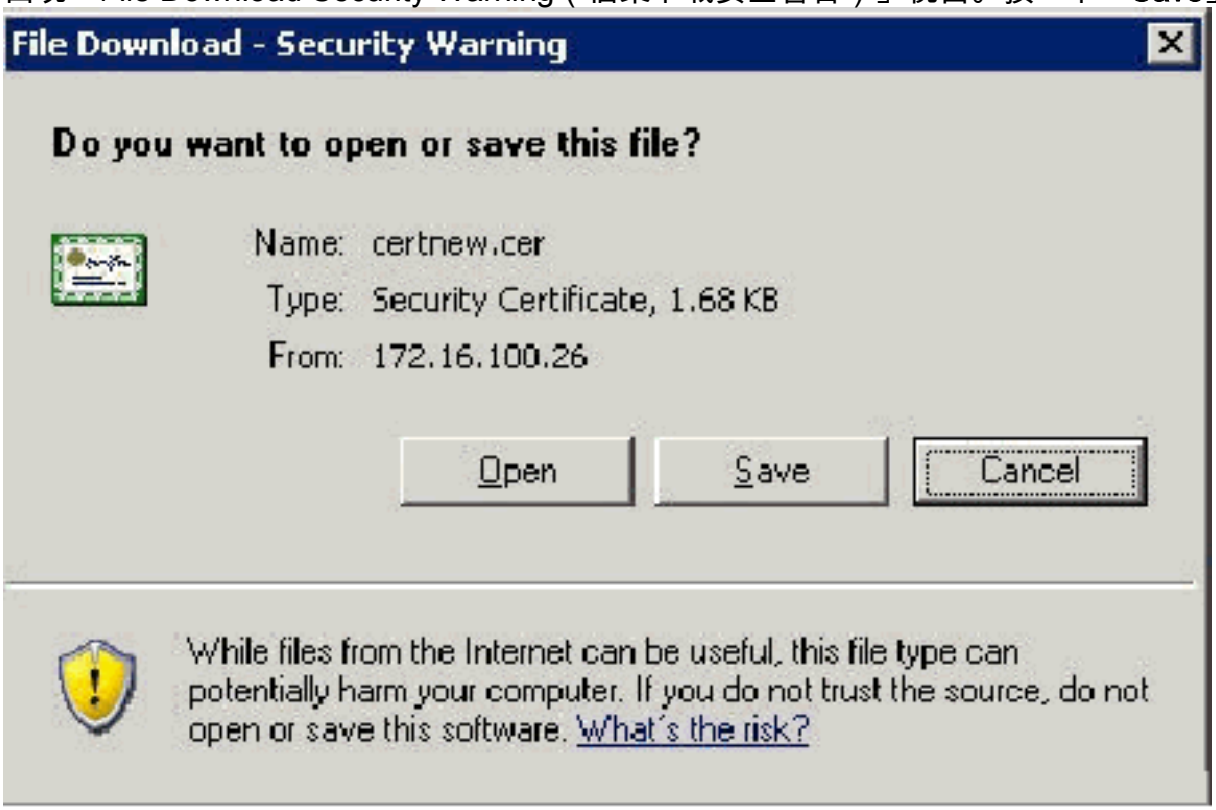
在ACS 4.0軟體中安裝證書

請完成以下步驟：

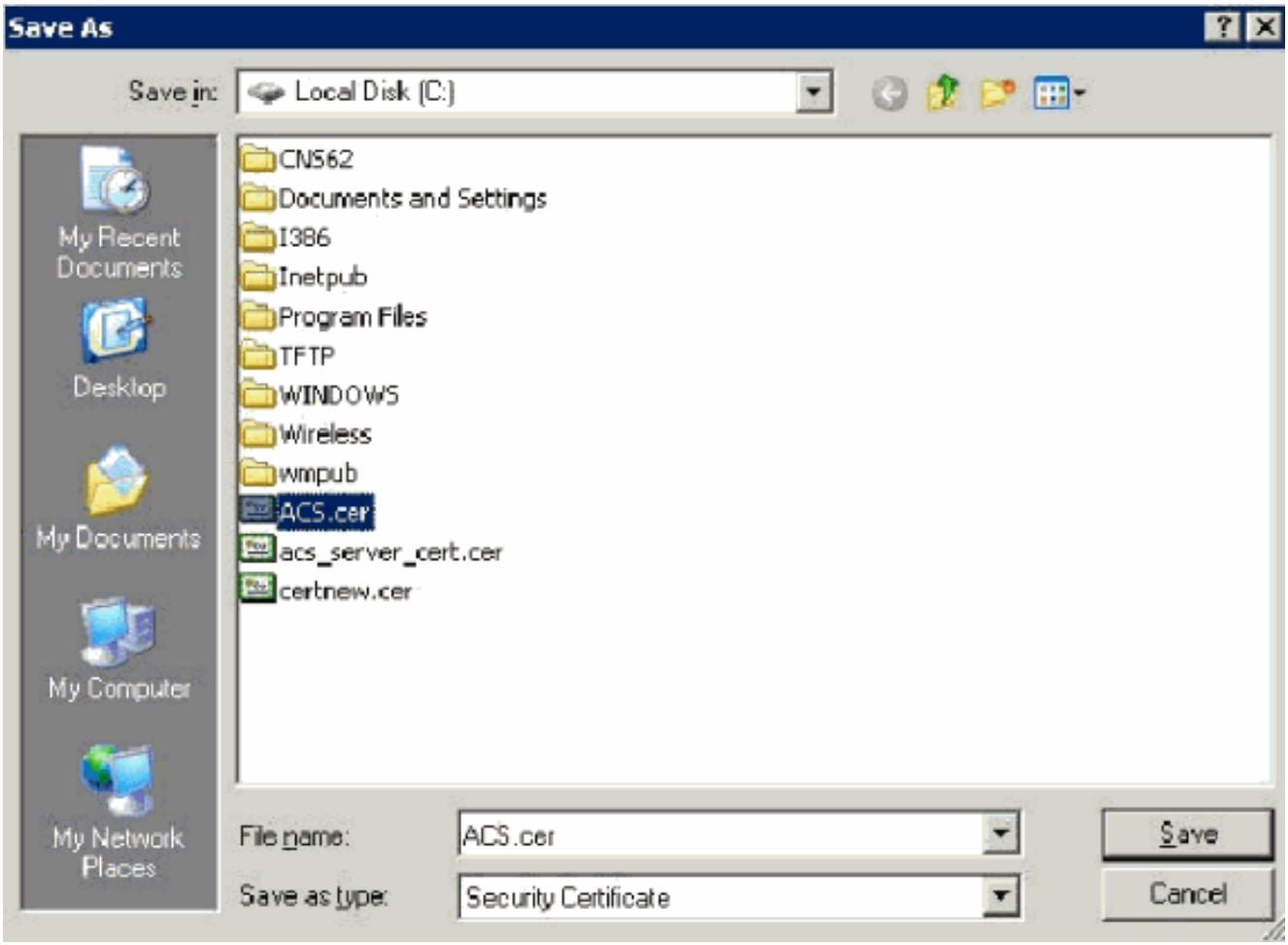
1. 在ACS伺服器（本例中為cisco_w2003）上，將Microsoft CA伺服器上的瀏覽器指向**http://172.16.100.26 /certsrv**。
2. 在「選擇任務」選項中選擇**「下載CA證書、證書鏈或CRL」**。
3. 選擇**Base 64**無線電編碼方法，然後按一下**Download CA Certificate**。



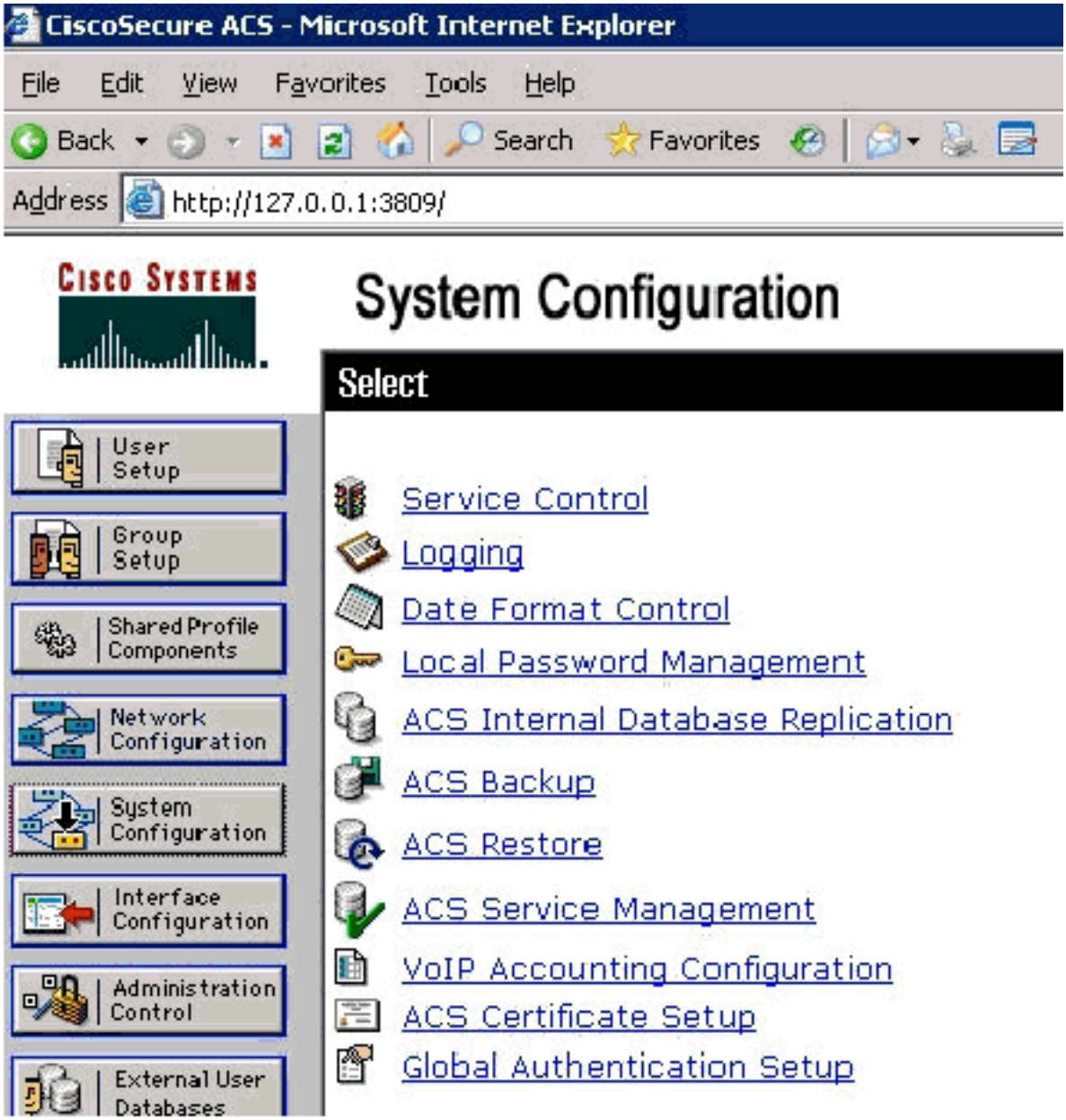
4. 出現「File Download Security Warning（檔案下載安全警告）」視窗。按一下「**Save**」。



5. 使用ACS.cer等名稱或您所需的任何名稱儲存檔案。請記住此名稱，因為您在ACS 4.0中的ACS證書頒發機構設定期間會使用它。

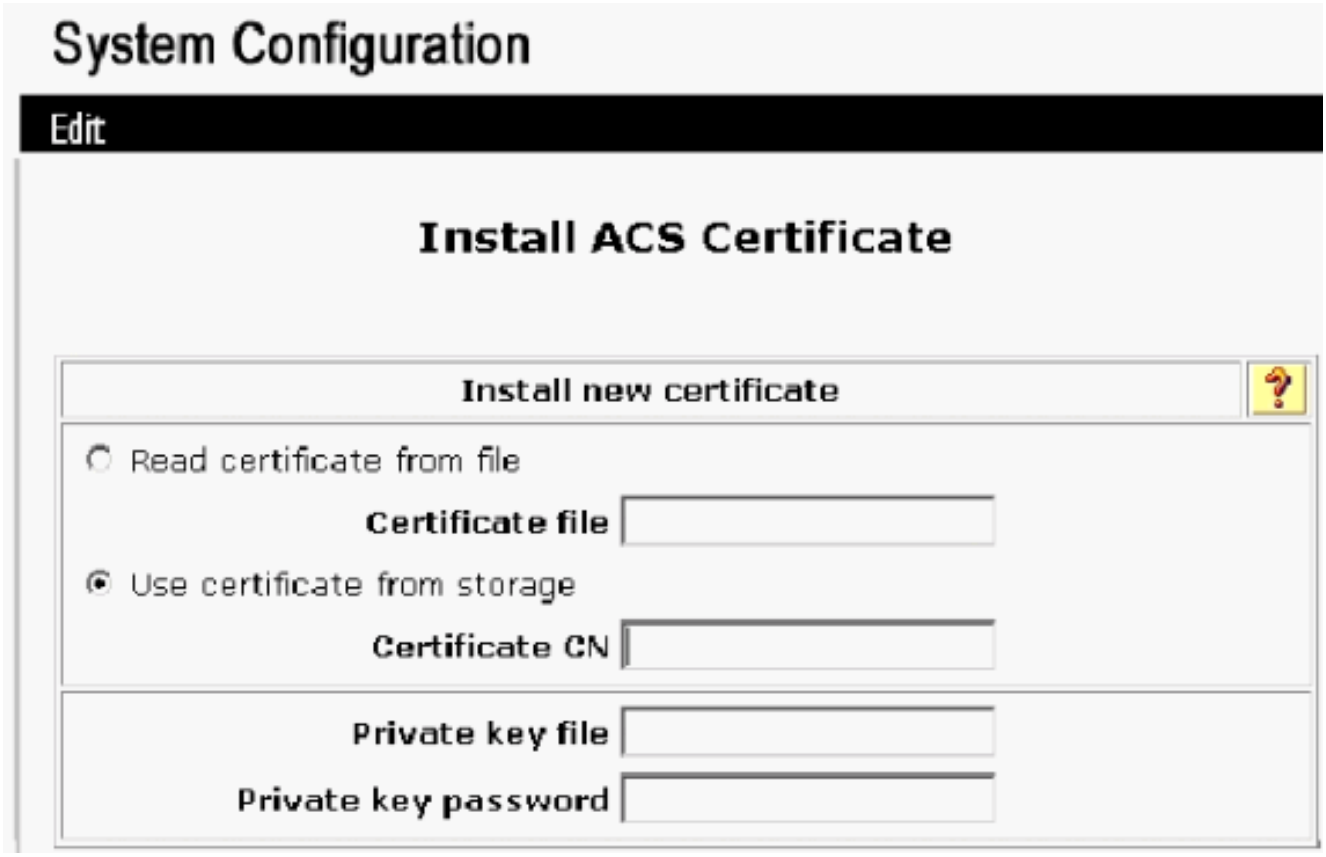


6. 從安裝過程中建立的案頭快捷方式開啟**ACS管理員**。
7. 按一下「**System Configuration**」。



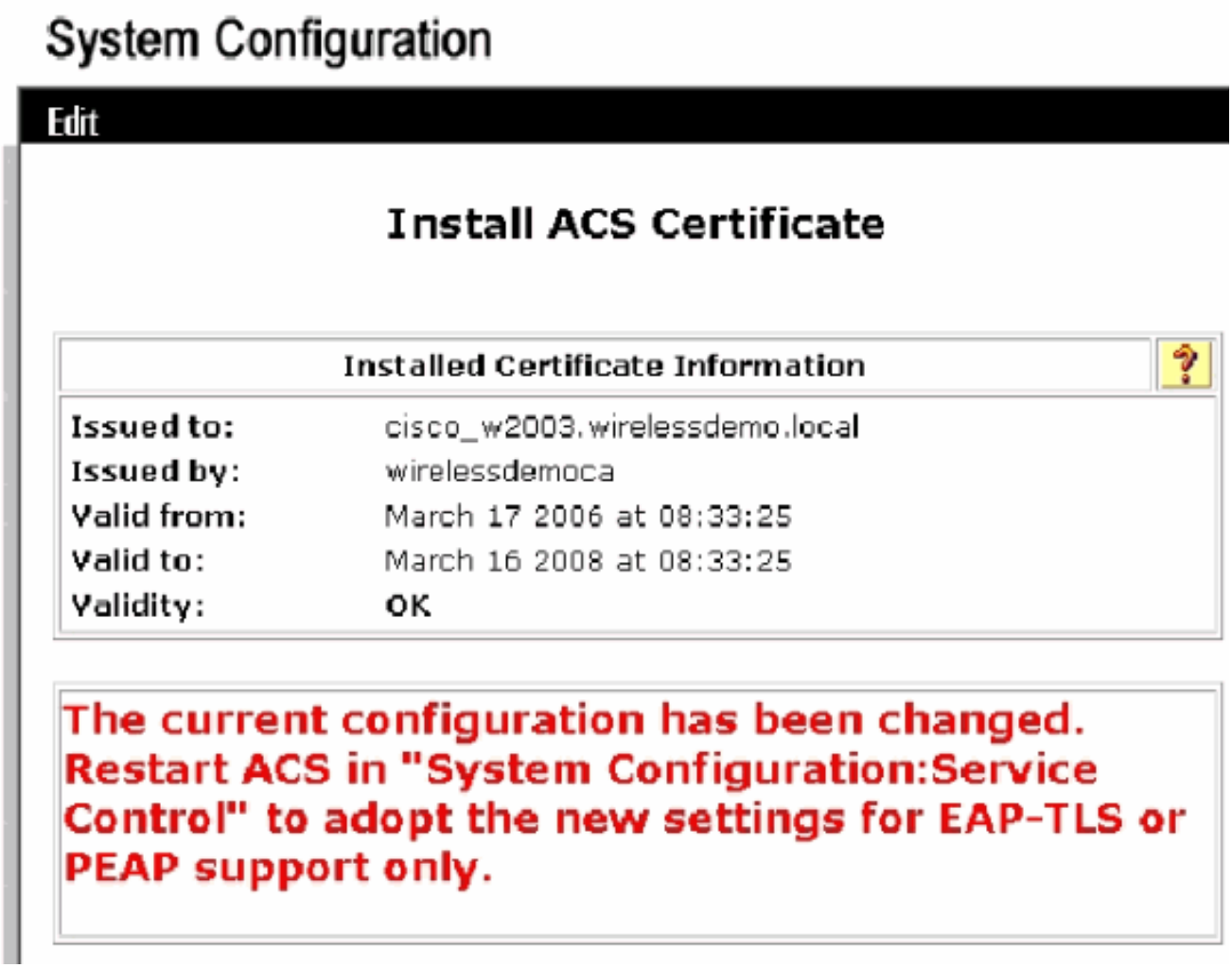
8. 按一下**ACS Certificate Setup**。

9. 按一下**安裝ACS證書**。

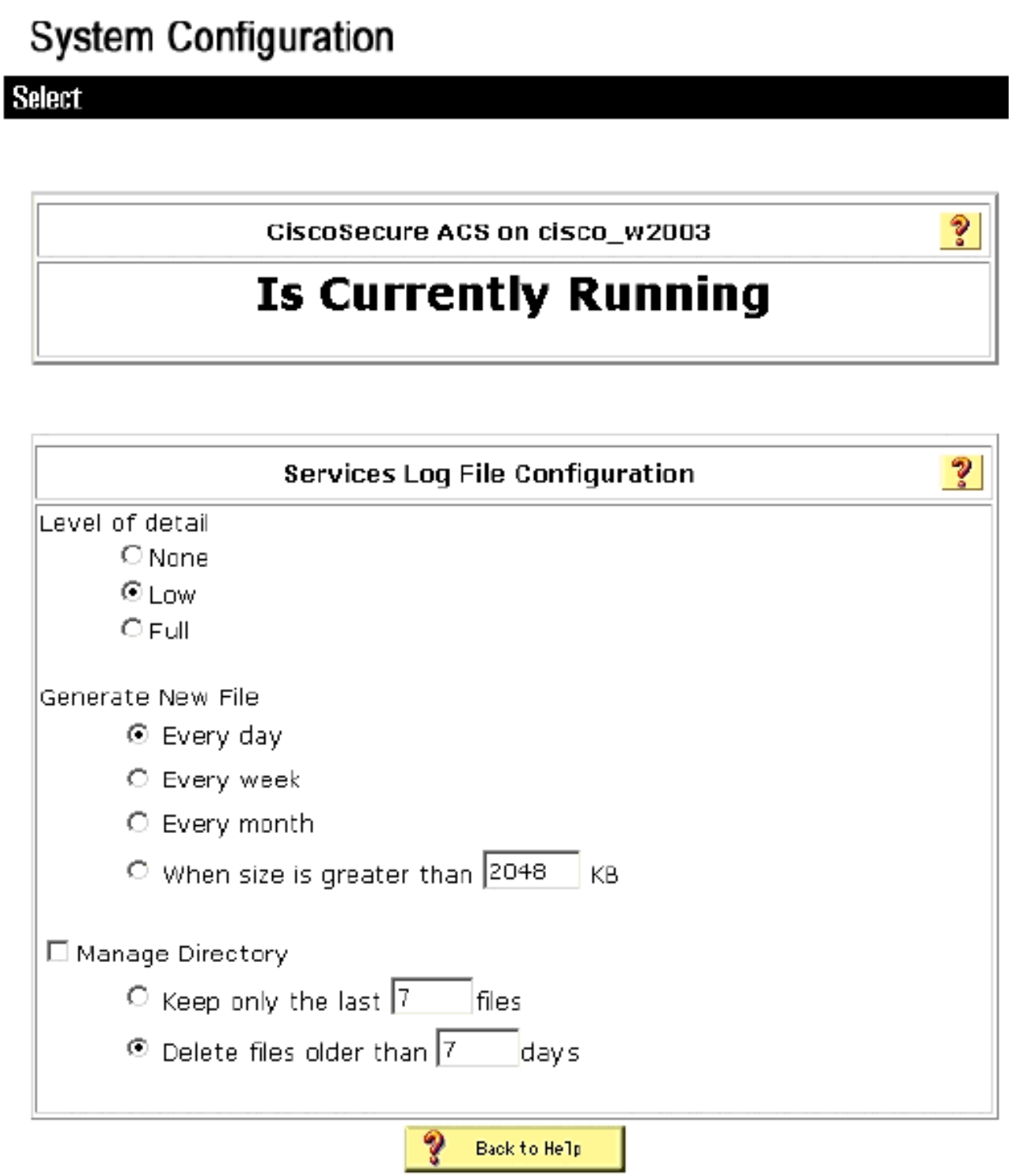


10. 選擇**Use certificate from storage**，然後輸入**cisco_w2003.wirelessdemo.local**(如果使用ACS作為名稱，請輸入**ACS.wirelessdemo.local**)的完全限定域名。

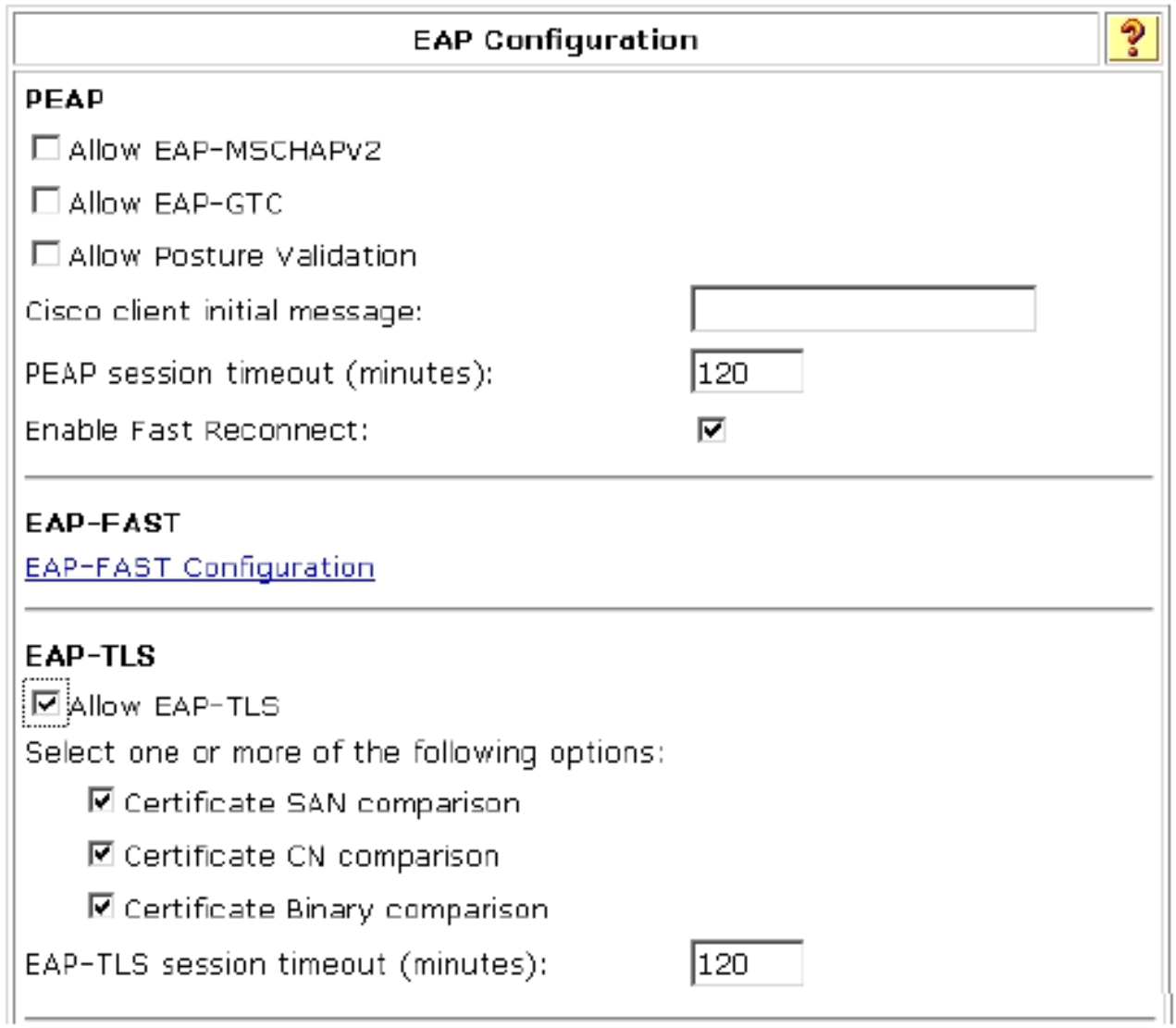
11. 按一下「Submit」。



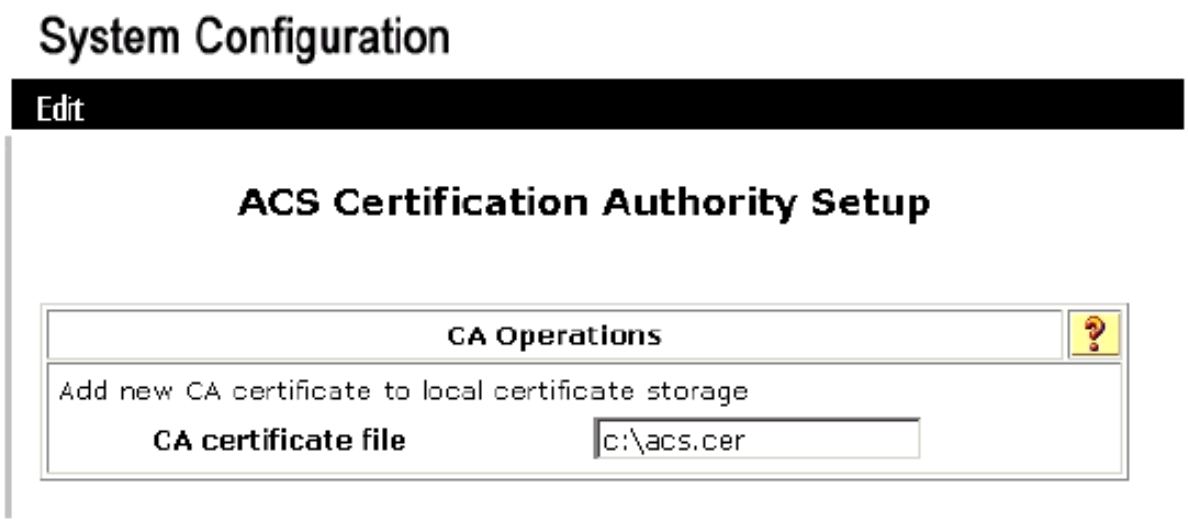
12. 按一下「System Configuration」。
13. 按一下Service Control，然後按一下Restart。

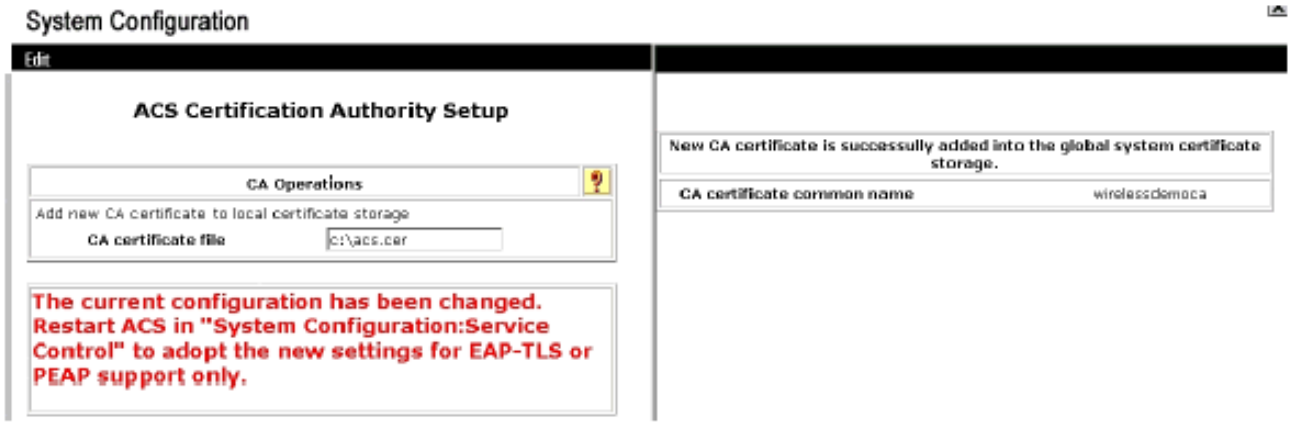


14. 按一下「System Configuration」。
15. 按一下Global Authentication Setup。
16. 選中Allow EAP-TLS及其下面的所有框。



17. 按一下「**Submit + Restart**」。
18. 按一下「**System Configuration**」。
19. 按一下**ACS Certification Authority Setup**。
20. 在「ACS證書頒發機構設定」(ACS Certification Authority Setup)視窗中，鍵入之前建立的*.cer檔案的名稱和位置。在本示例中，建立的*.cer檔案是**ACS.cer**，位於根目錄c:\中。
21. 在CA certificate file欄位中鍵入**c:\acs.cer**，然後按一下**Submit**。





22. 重新啟動ACS服務。

使用Windows零接觸的EAP-TLS的客戶端配置

CLIENT是運行Windows XP Professional SP2的電腦，充當無線客戶端，通過無線AP訪問Intranet資源。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

請完成以下步驟：

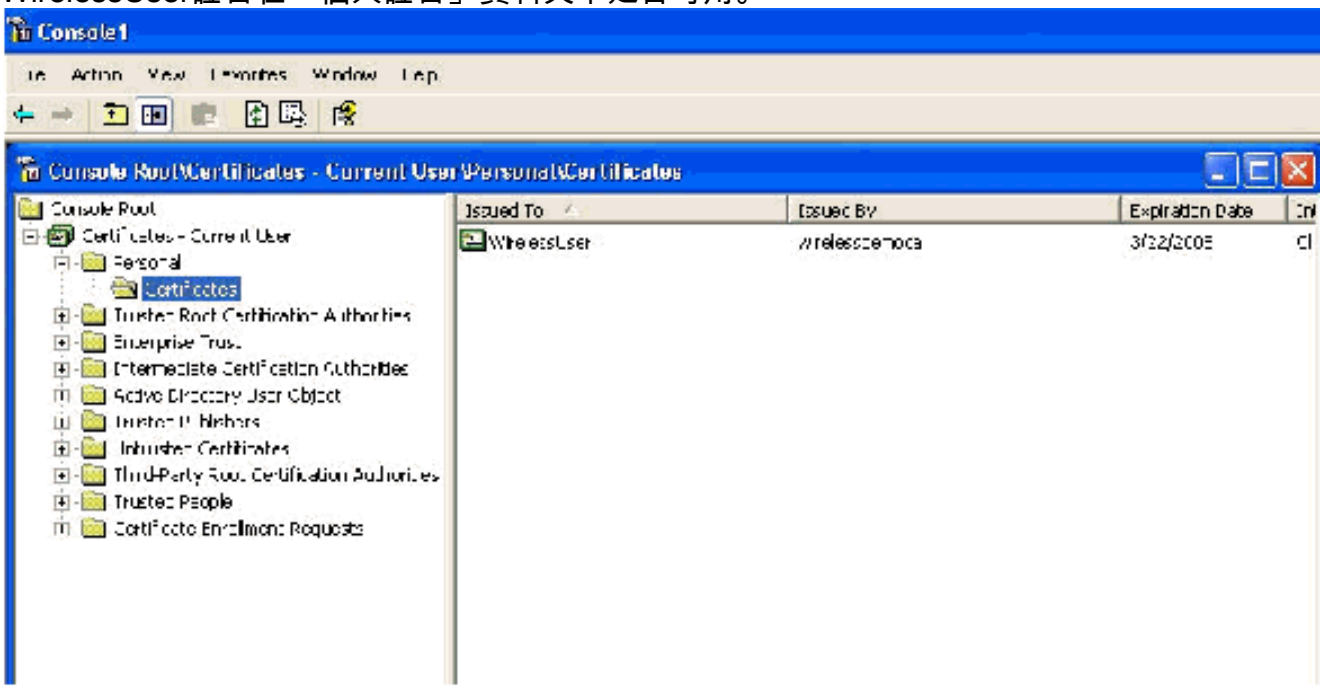
1. 使用連線到交換機的乙太網電纜將CLIENT連線到Intranet網段。
2. 在CLIENT上，將Windows XP Professional with SP2安裝為成員電腦，該電腦名為**CLIENT**，位於wirelessdemo.local域中。
3. 安裝Windows XP Professional with SP2。必須安裝此程式才能獲得EAP-TLS和PEAP支援。**注意：**在Windows XP Professional SP2中自動開啟Windows防火牆。請勿關閉防火牆。

配置無線網路連線

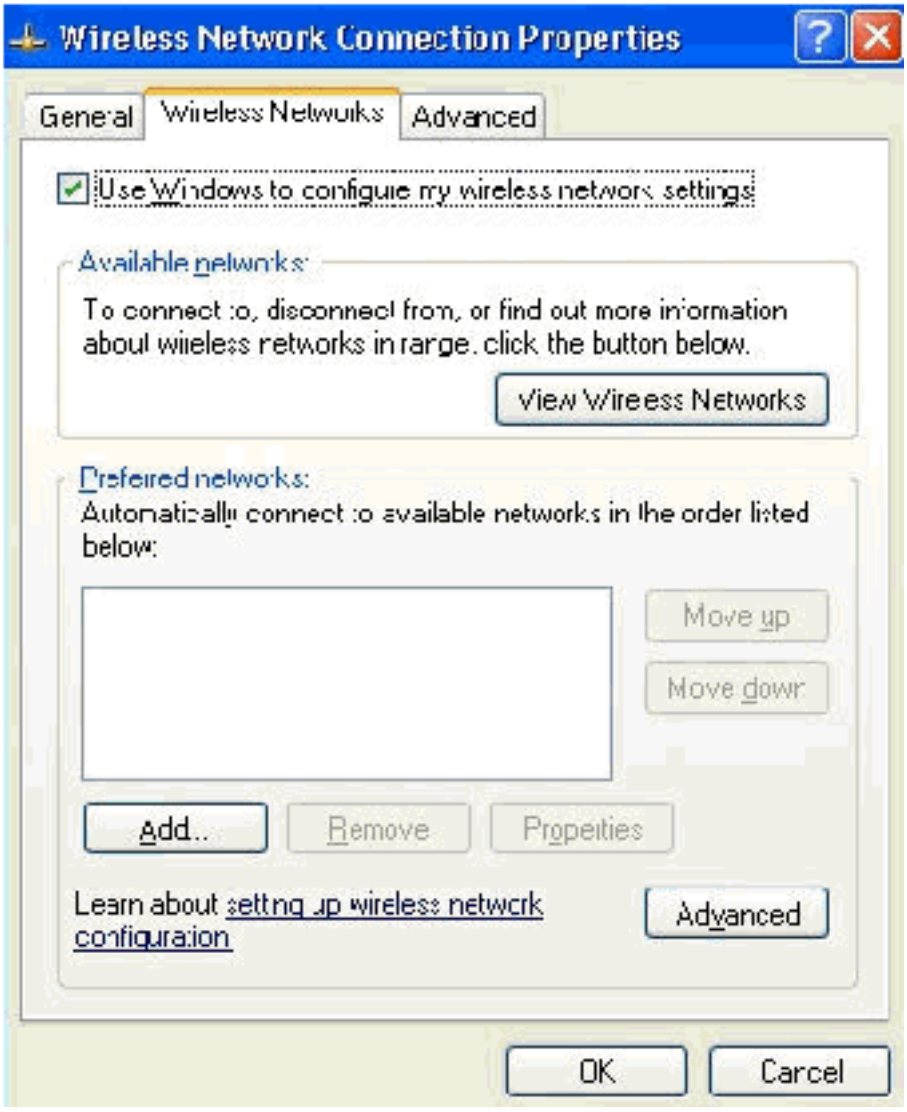
請完成以下步驟：

1. 註銷，然後使用wirelessdemo.local域中的WirelessUser帳戶登入。**注意：通**過在命令提示符下鍵入**gpupdate，立即更新電腦和使用者配置組策略設定並獲取無線客戶端電腦的**電腦和使用者證書。否則，當您註銷然後登入時，它將執行與**gpupdate**相同的功能。您必須通過線路連線登入到域。**注意：**若要驗證證書是否自動安裝在客戶端上，請開啟證書MMC並驗證

WirelessUser證書在「個人證書」資料夾中是否可用。

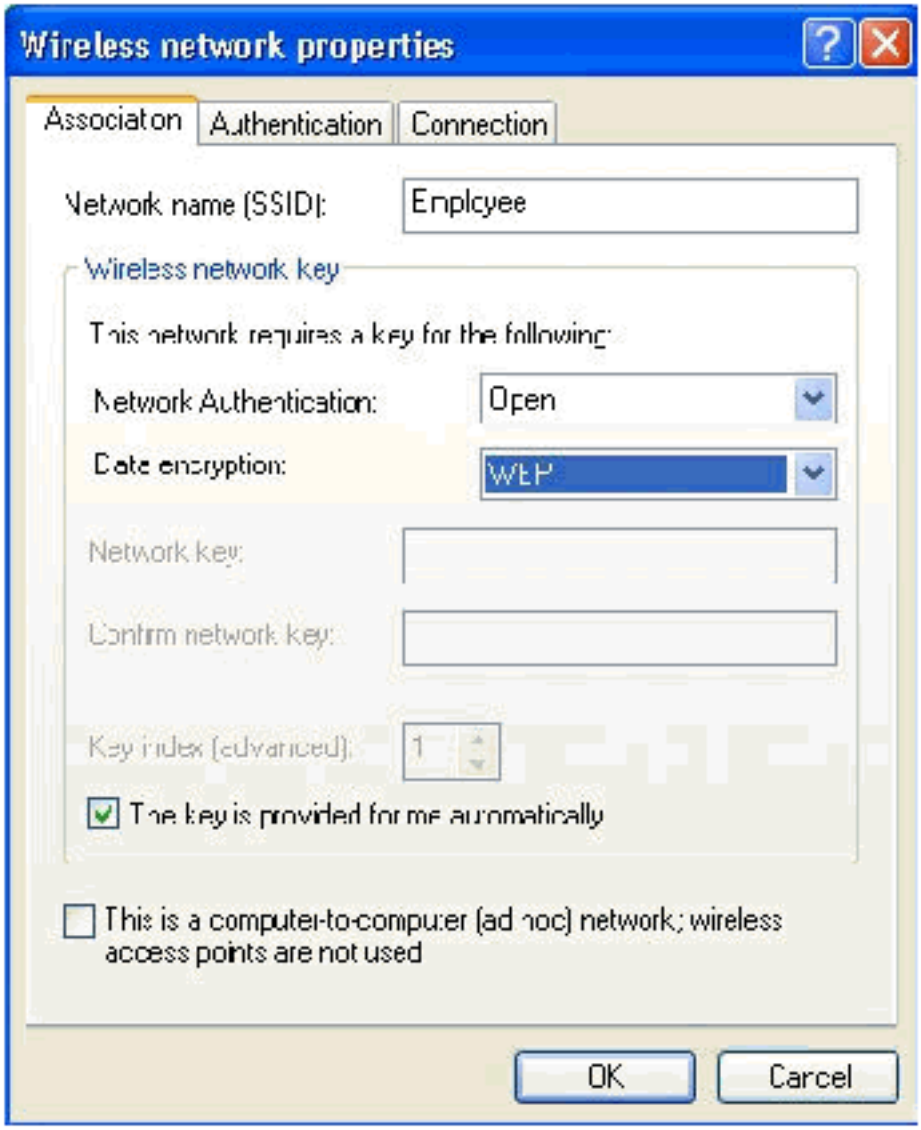


2. 選擇**開始>控制面板**，按兩下**網路連線**，然後按一下右鍵**無線網路連線**。
3. 按一下**Properties**，轉到「Wireless Networks（無線網路）」頁籤，並確保選中「**User Windows to configure my wireless network settings**(使用者視窗配置我的無線網路設定)」。

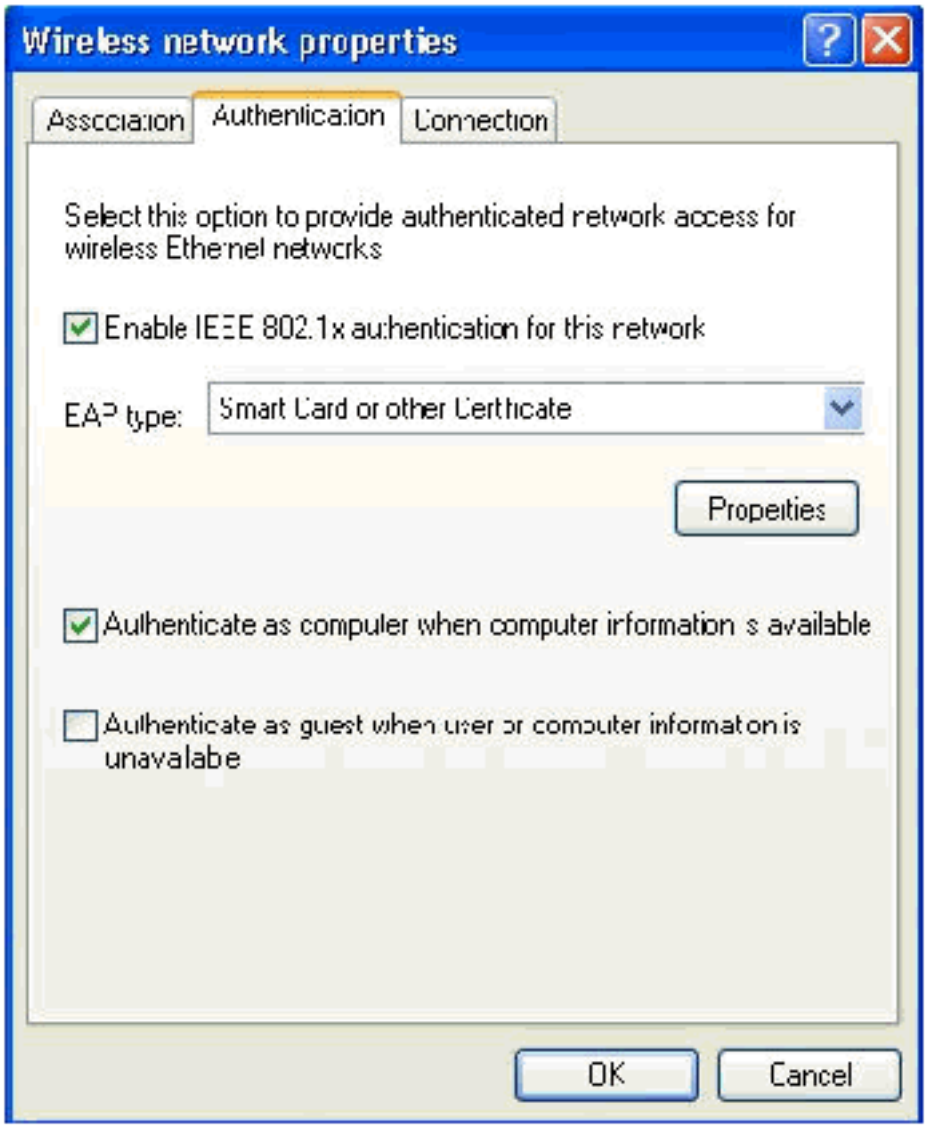


4. 按一下「**Add**」。

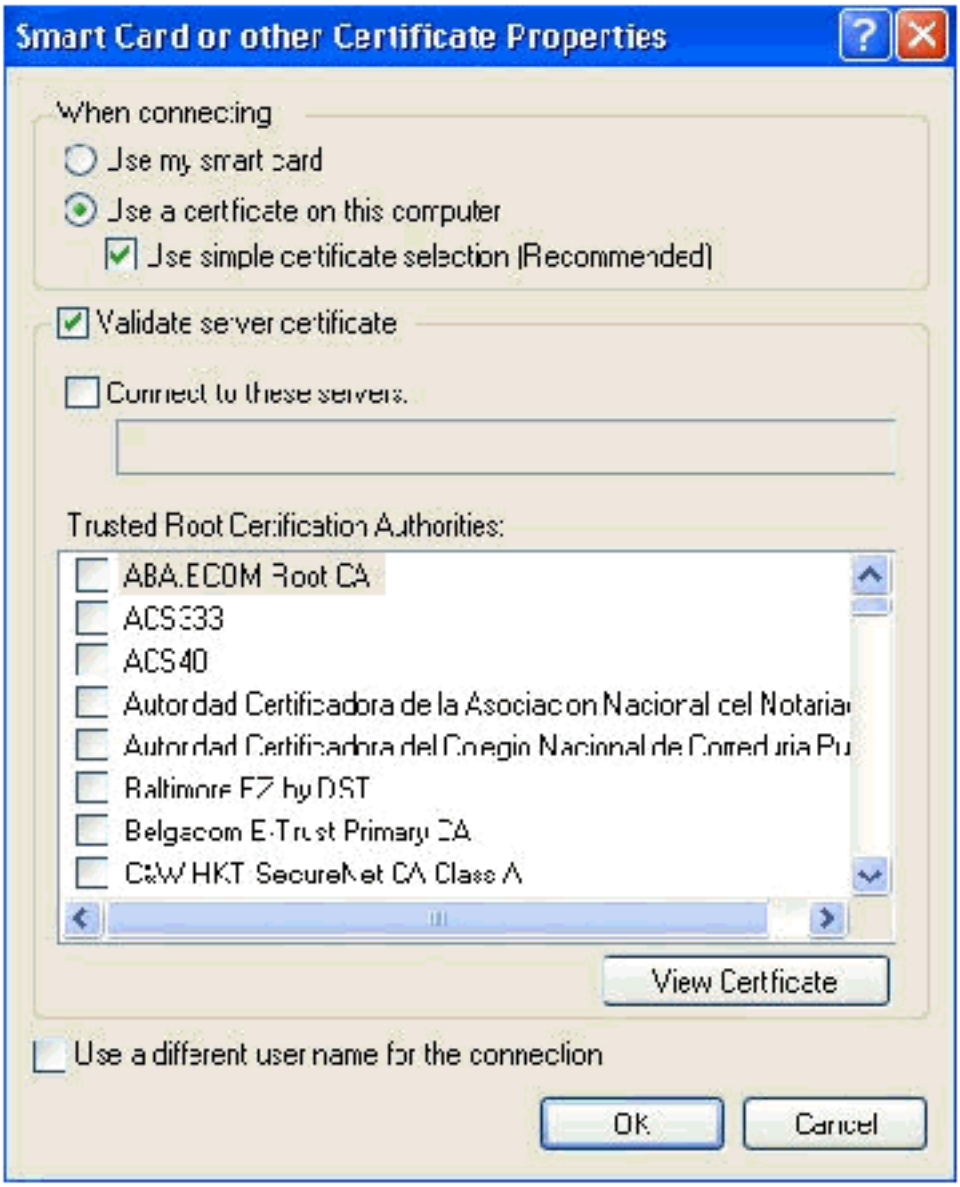
5. 轉到Association頁籤，然後在Network name(SSID)欄位中鍵入**Employee**。
6. 確保將「Data Encryption（資料加密）」設定為**WEP**，並**選中自動為我提供**的金鑰。



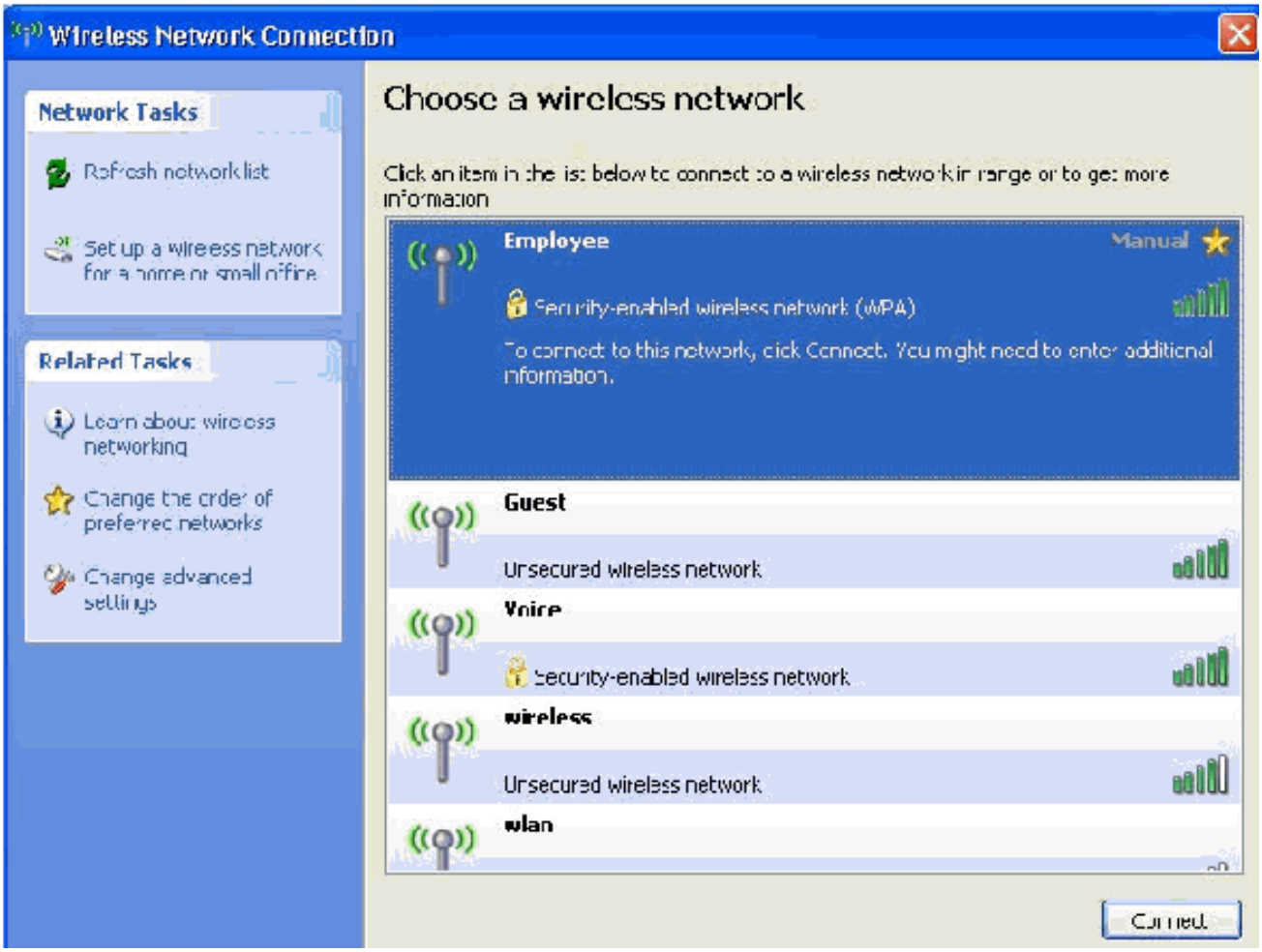
7. 轉到Authentication頁籤。
8. 驗證EAP型別是否配置為使用智**能卡或其他證書**。如果不是，請從下拉選單中選擇它。
9. 如果您希望在登入前對電腦進行身份驗證（這允許應用登入指令碼或組策略推送），請選擇選項**Authenticate as computer when computer information available**。



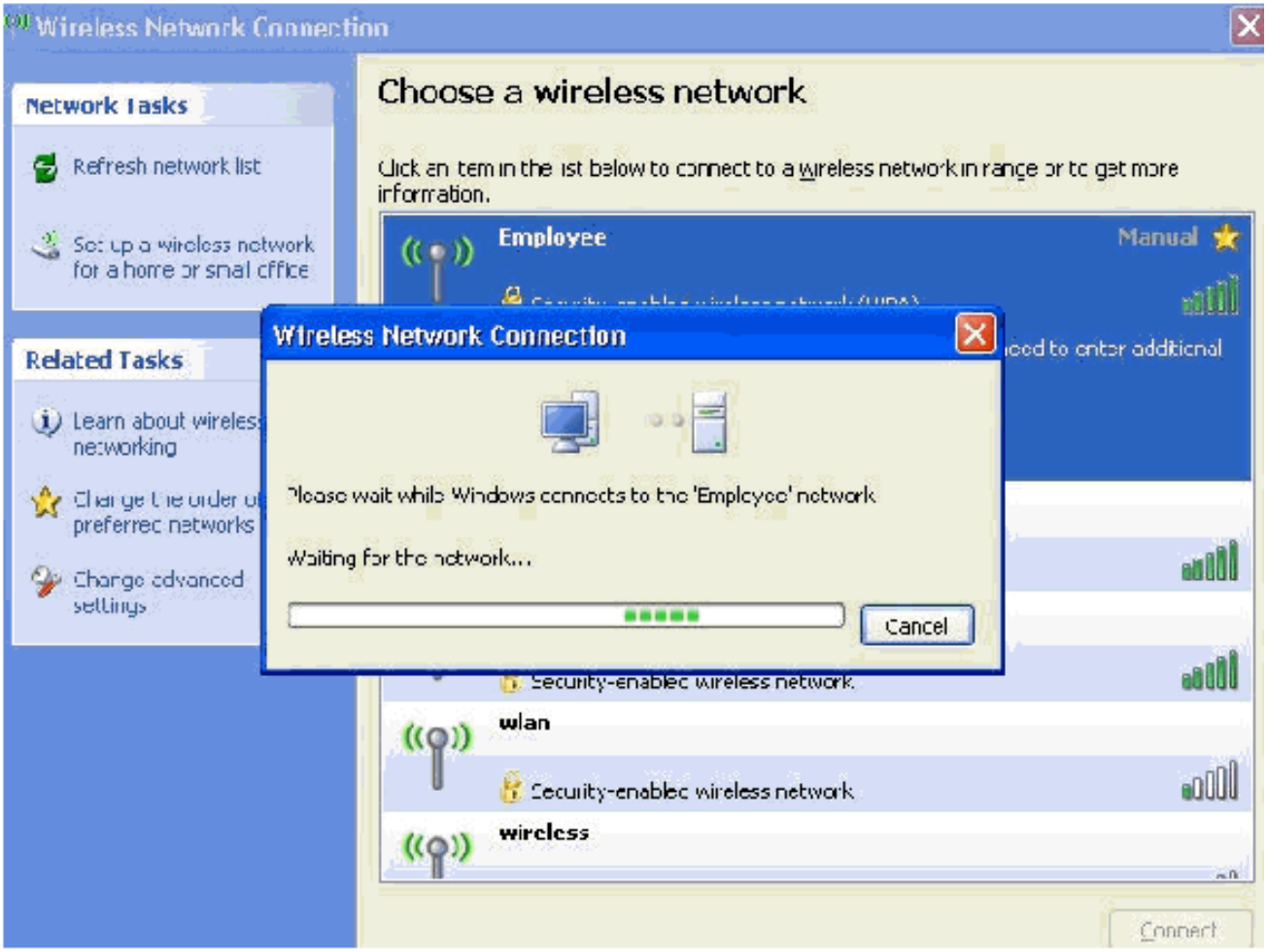
10. 按一下「**Properties**」。
11. 確保已選中此視窗中的框。

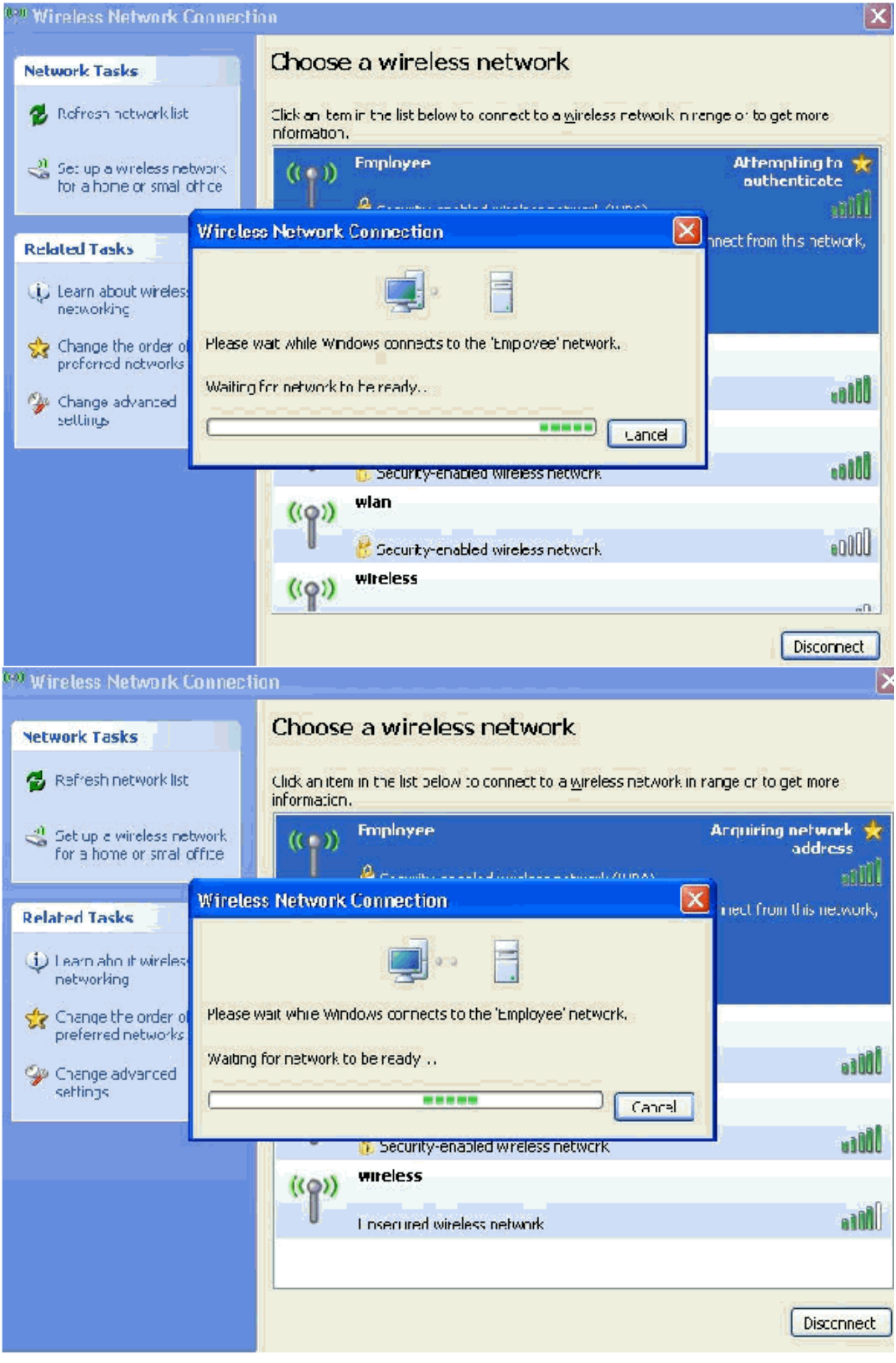


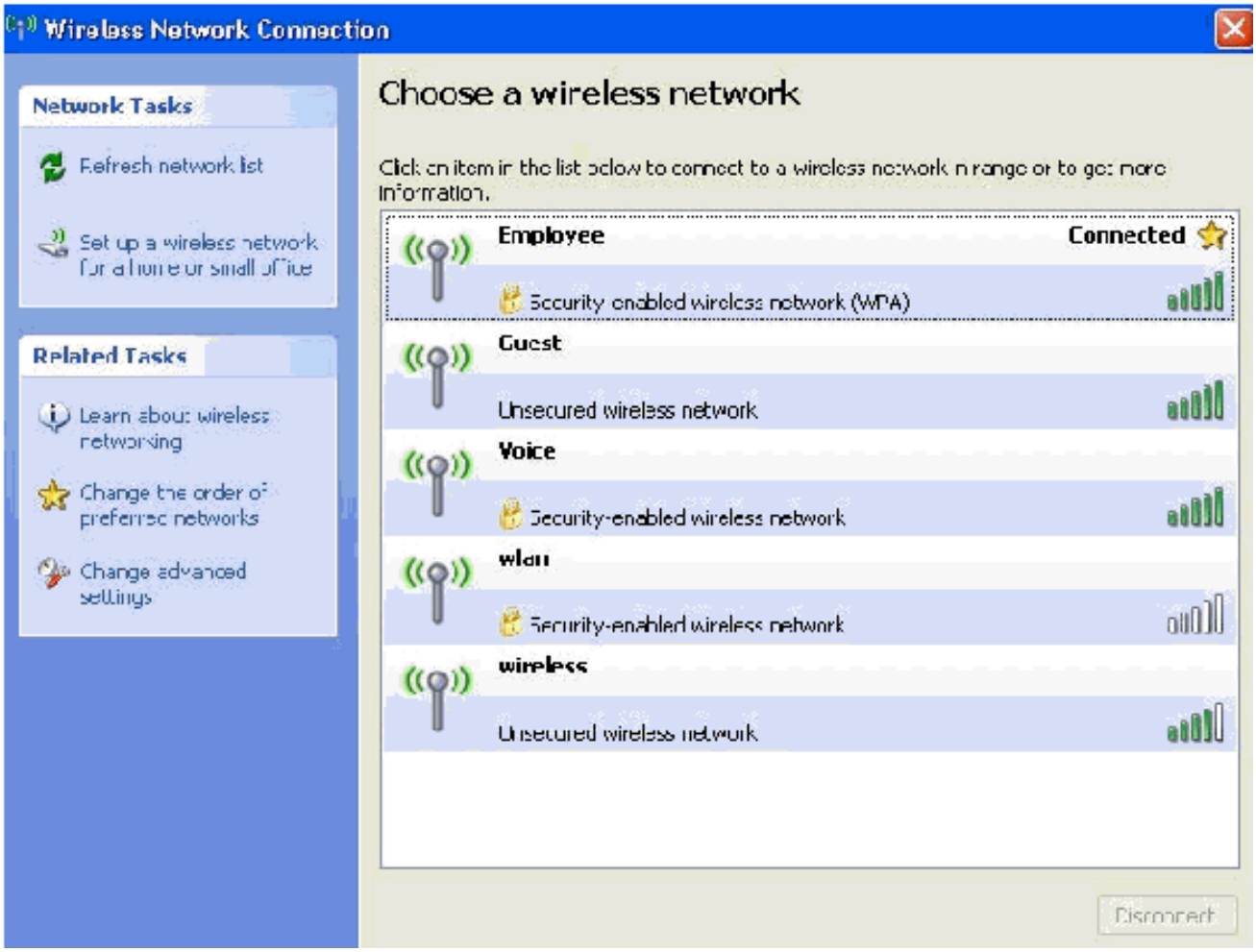
12. 按一下**OK**三次。
13. 按一下右鍵systray中的無線網路連線圖示，然後按一下**View Available Wireless Networks**。
14. 按一下**Employee**無線網路，然後按一下**Connect**。



這些螢幕截圖指示連線是否成功完成。




Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Employee
Attempting to authenticate
Wireless Network Connection
Please wait while Windows connects to the 'Employee' network.
Waiting for network to be ready...
Cancel
Security-enabled wireless network
wlan
Security-enabled wireless network
wireless
Disconnect
Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Employee
Acquiring network address
Wireless Network Connection
Please wait while Windows connects to the 'Employee' network.
Waiting for network to be ready...
Cancel
Security-enabled wireless network
wireless
Unsecured wireless network
Disconnect



15. 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作用域或為無線客戶端建立的作用域中，它的地址範圍應為172.16.100.100-172.16.100.254。
16. 若要測試功能，請開啟瀏覽器並瀏覽**http://wirelessdemoca**（或企業CA伺服器的IP位址）。

相關資訊

- 使用WLAN控制器(WLC)的EAP驗證組態範例
- 無線LAN控制器組態設定指南
- 無線LAN控制器和輕量型存取點基本組態範例
- 無線 LAN 控制器上的 VLAN 組態範例
- 使用無線LAN控制器的AP組VLAN配置示例
- 技術支援與文件 - Cisco Systems