

採用Microsoft Internet身份驗證服務(IAS)的統一無線網路下的PEAP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[PEAP概述](#)

[設定](#)

[網路圖表](#)

[組態](#)

[配置Microsoft Windows 2003 Server](#)

[配置Microsoft Windows 2003 Server](#)

[在Microsoft Windows 2003 Server上安裝並配置DHCP服務](#)

[安裝Microsoft Windows 2003 Server並將其配置為證書頒發機構\(CA\)伺服器](#)

[將客戶端連線到域](#)

[在Microsoft Windows 2003 Server上安裝Internet身份驗證服務並請求證書](#)

[為PEAP-MS-CHAP v2身份驗證配置Internet身份驗證服務](#)

[將使用者新增到Active Directory](#)

[允許對使用者進行無線訪問](#)

[配置無線區域網控制器和輕量AP](#)

[通過MS IAS RADIUS伺服器配置WLC進行RADIUS身份驗證](#)

[為客戶端配置WLAN](#)

[配置無線客戶端](#)

[為PEAP-MS CHAPv2身份驗證配置無線客戶端](#)

[驗證和疑難排解](#)

[相關資訊](#)

簡介

本文提供一個組態範例，用於在以Microsoft Internet Authentication Service(IAS)作為RADIUS伺服器的思科整合無線網路中設定使用Microsoft Challenge Handshake驗證通訊協定(MS-CHAP)第2版驗證之受保護可擴充驗證通訊協定(PEAP)。

必要條件

需求

假設讀者瞭解基本的Windows 2003安裝和思科控制器安裝知識，因為本文檔僅介紹便於測試的特定配置。

注意：本文檔旨在為讀者提供一個示例，說明MS伺服器上進行PEAP - MS CHAP身份驗證所需的配置。本部分介紹的Microsoft伺服器配置已在實驗室經過測試，並且發現可以按預期工作。如果配置Microsoft伺服器時遇到問題，請與Microsoft聯絡以獲取幫助。Cisco TAC不支援Microsoft Windows伺服器配置。

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](#)。

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。

[採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體版本4.0的Cisco 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身份驗證服務(IAS)、證書頒發機構(CA)、DHCP和域名系統(DNS)服務的Windows 2003 Enterprise Server(SP1)
- Windows XP Professional SP 2 (和更新的Service Pack) 和Cisco Aironet 802.11a/b/g無線網路介面卡(NIC)
- Aironet案頭實用程式版本4.0
- Cisco 3560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](#)。

[PEAP概述](#)

PEAP使用傳輸級別安全(TLS)在身份驗證PEAP客戶端 (如無線筆記型電腦) 和PEAP身份驗證器(如Microsoft Internet身份驗證服務(IAS)或任何RADIUS伺服器之間建立加密通道。PEAP不指定身份驗證方法，但為其他EAP身份驗證協定提供額外的安全性，例如EAP-MSCHAPv2，這些協定可以通過PEAP提供的TLS加密通道運行。PEAP身份驗證過程包括兩個主要階段：

PEAP階段1:TLS加密通道

無線客戶端與AP關聯。基於IEEE 802.11的關聯在客戶端和接入點(LAP)之間建立安全關聯之前提供開放系統或共用金鑰身份驗證。在客戶端和接入點之間成功建立基於IEEE 802.11的關聯之後，與AP協商TLS會話。在無線客戶端和IAS伺服器之間成功完成身份驗證後，將在它們之間協商TLS會話。在此協商中匯出的金鑰用於加密所有後續通訊。

PEAP階段2:EAP身份驗證通訊

EAP通訊 (包括EAP協商) 在PEAP身份驗證過程的第一階段由PEAP建立的TLS通道內發生。IAS伺服器使用EAP-MS-CHAP v2對無線客戶端進行身份驗證。LAP和控制器僅在無線客戶端和RADIUS伺服器之間轉發消息。WLC和LAP無法解密這些消息，因為它不是TLS終點。

發生PEAP第1階段後，在IAS伺服器和802.1X無線客戶端之間建立TLS通道，對於成功的身份驗證嘗試，使用者已使用PEAP-MS-CHAP v2提供有效的基於密碼的憑據，RADIUS消息序列如下：

1. IAS伺服器向客戶端傳送身份請求消息：EAP-Request/Identity。
2. 客戶端以身份響應消息進行響應：EAP-Response/Identity。
3. IAS伺服器傳送MS-CHAP v2質詢消息：EAP-Request/EAP-Type=EAP MS-CHAP-V2 (質詢)。
4. 客戶端使用MS-CHAP v2質詢和響應進行響應：EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (響應)。
5. 當伺服器成功驗證客戶端時，IAS伺服器會發回MS-CHAP v2成功資料包：EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (成功)。
6. 當客戶端成功驗證伺服器時，客戶端使用MS-CHAP v2成功資料包進行響應：EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (成功)。
7. IAS伺服器傳送一個EAP-TLV，指示身份驗證成功。
8. 客戶端以EAP-TLV狀態成功消息進行響應。
9. 伺服器完成身份驗證並使用明文傳送EAP-Success消息。如果為客戶端隔離部署了VLAN，則此消息中會包含VLAN屬性。

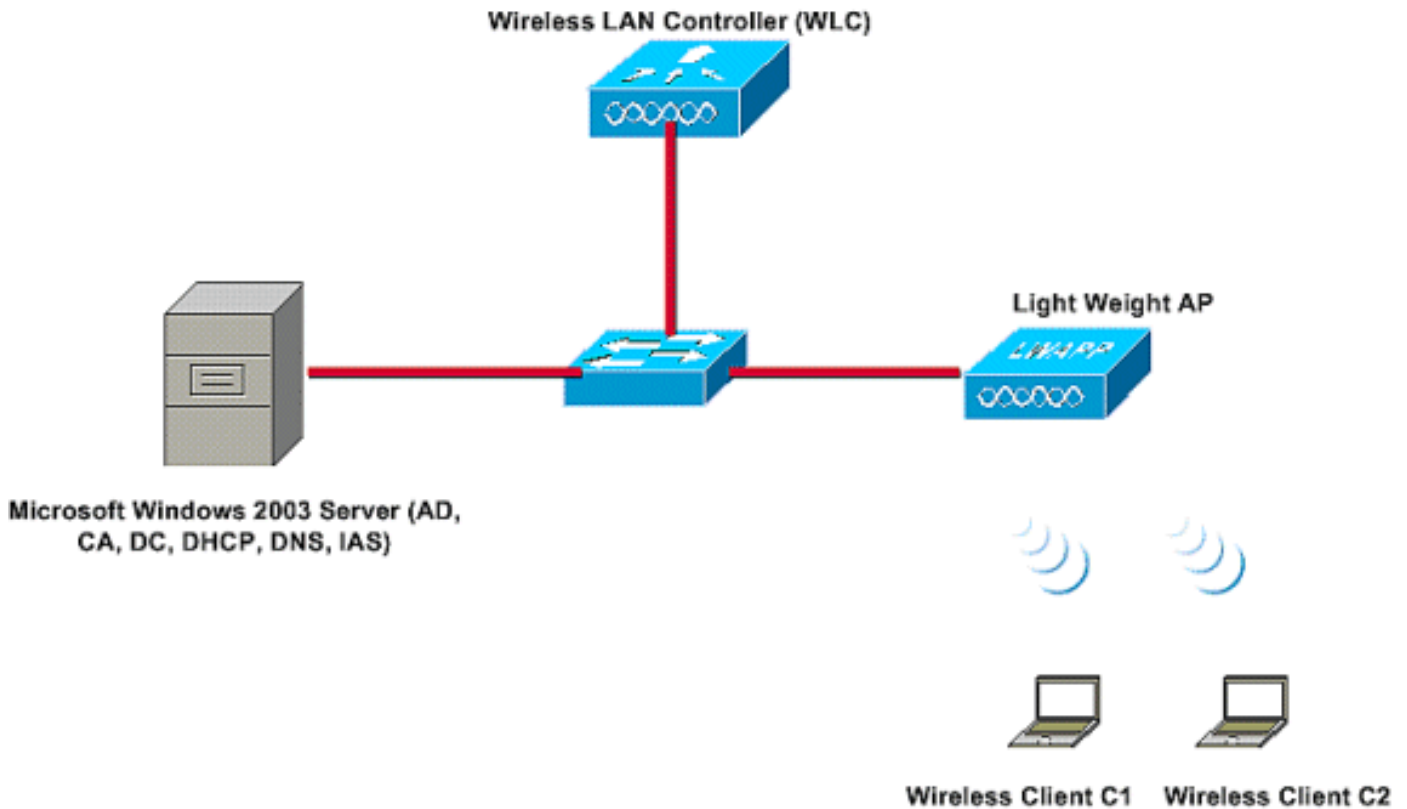
設定

本文檔提供配置PEAP MS-CHAP v2的示例。

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：



在此設定中，Microsoft Windows 2003伺服器執行以下角色：

- 域的域控制器Wireless.com
- DHCP/DNS伺服器
- 證書頒發機構(CA)伺服器
- Active Directory — 維護使用者資料庫
- 網際網路身份驗證服務(IAS) — 對無線使用者進行身份驗證

如圖所示，此伺服器通過第2層交換機連線到有線網路。

無線LAN控制器(WLC)和註冊的LAP也透過第2層交換器連線至網路。

無線客戶端C1和C2將使用Wi-Fi保護訪問2(WPA2)- PEAP MSCHAP v2身份驗證連線到無線網路。

目標是配置Microsoft 2003伺服器、無線LAN控制器和輕量AP，以使用PEAP MSCHAP v2身份驗證對無線客戶端進行身份驗證。

下一節說明如何為此設定配置裝置。

組態

本節介紹在該WLAN中設定PEAP MS-CHAP v2身份驗證所需的配置：

- 配置Microsoft Windows 2003 Server
- 設定無線LAN控制器(WLC)和輕量AP
- 配置無線客戶端

首先配置Microsoft Windows 2003伺服器。

配置Microsoft Windows 2003 Server

配置Microsoft Windows 2003 Server

如網路設定部分中所述，使用網路中的Microsoft Windows 2003伺服器執行這些功能。

- 域控制器 — 用於域無線
- DHCP/DNS伺服器
- 證書頒發機構(CA)伺服器
- 網際網路驗證服務(IAS) — 對無線使用者進行驗證
- Active Directory — 用於維護使用者資料庫

為這些服務配置Microsoft Windows 2003伺服器。首先將Microsoft Windows 2003伺服器配置為域控制器。

將Microsoft Windows 2003伺服器配置為域控制器

若要將Microsoft Windows 2003伺服器配置為域控制器，請完成以下步驟：

1. 按一下**Start**，按一下**Run**，鍵入**dcpromo.exe**，然後按一下**OK**以啟動Active Directory安裝嚮導。



2. 按一下**Next >**以運行Active Directory安裝嚮導。

Active Directory Installation Wizard



Operating System Compatibility

Improved security settings in Windows Server 2003 affect older versions of Windows.



Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.

Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.

For more information, see [Compatibility Help](#).

< Back

Next >

Cancel

- 若要建立新域，請為新域選擇Domain Controller選項。

Active Directory Installation Wizard

Domain Controller Type

Specify the role you want this server to have.



Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

Additional domain controller for an existing domain



Proceeding with this option will delete all local accounts on this server.

All cryptographic keys will be deleted and should be exported before continuing.

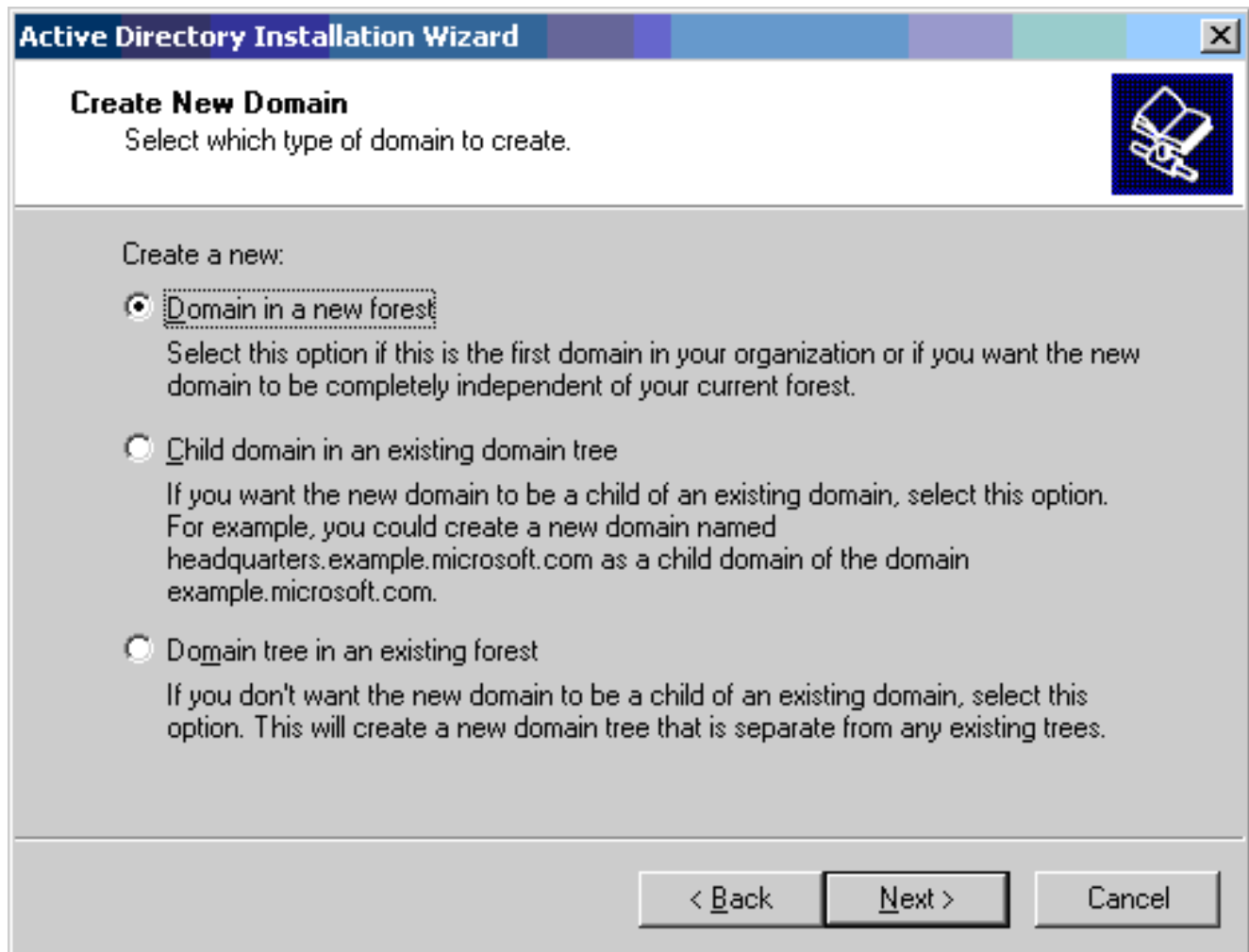
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

< Back

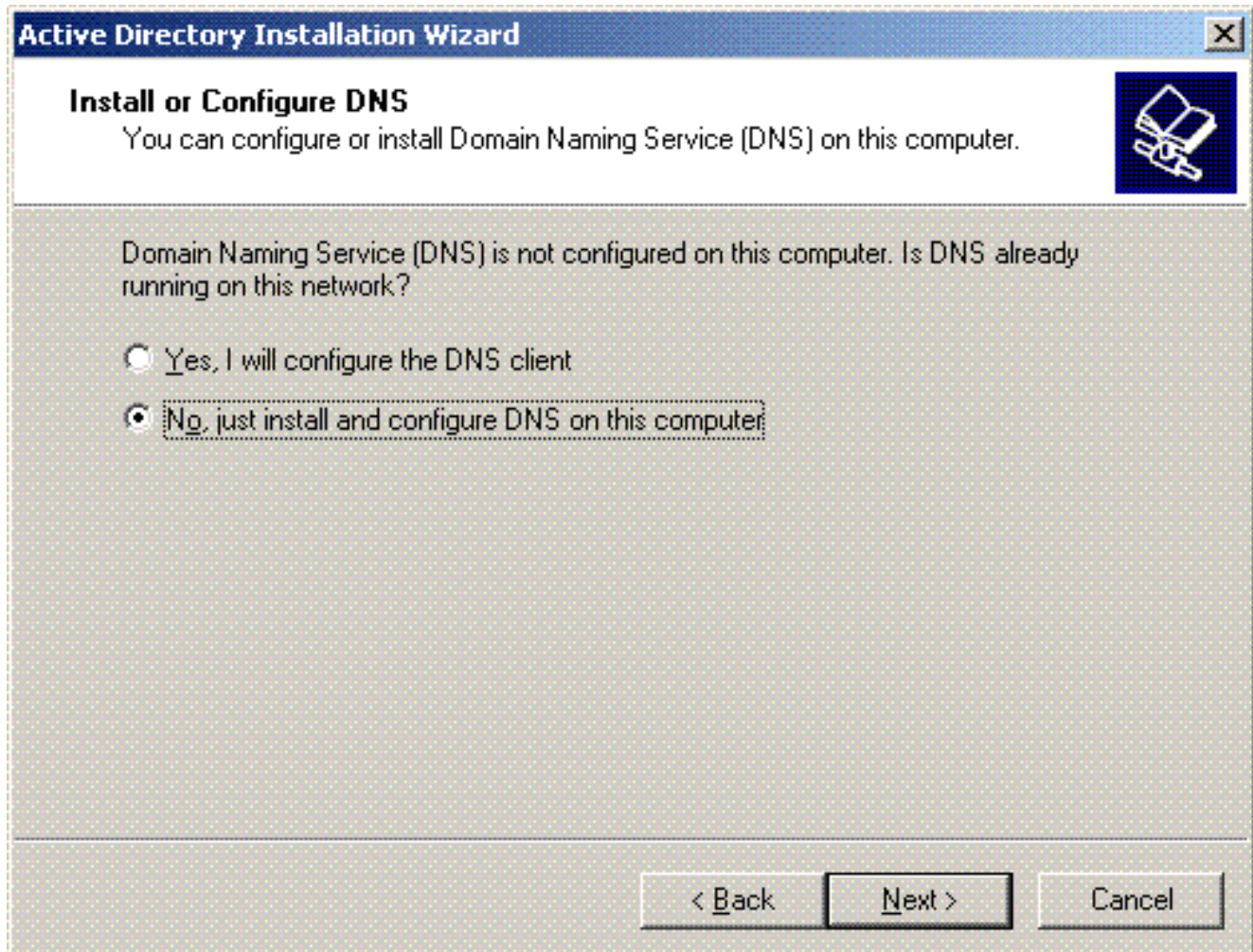
Next >

Cancel

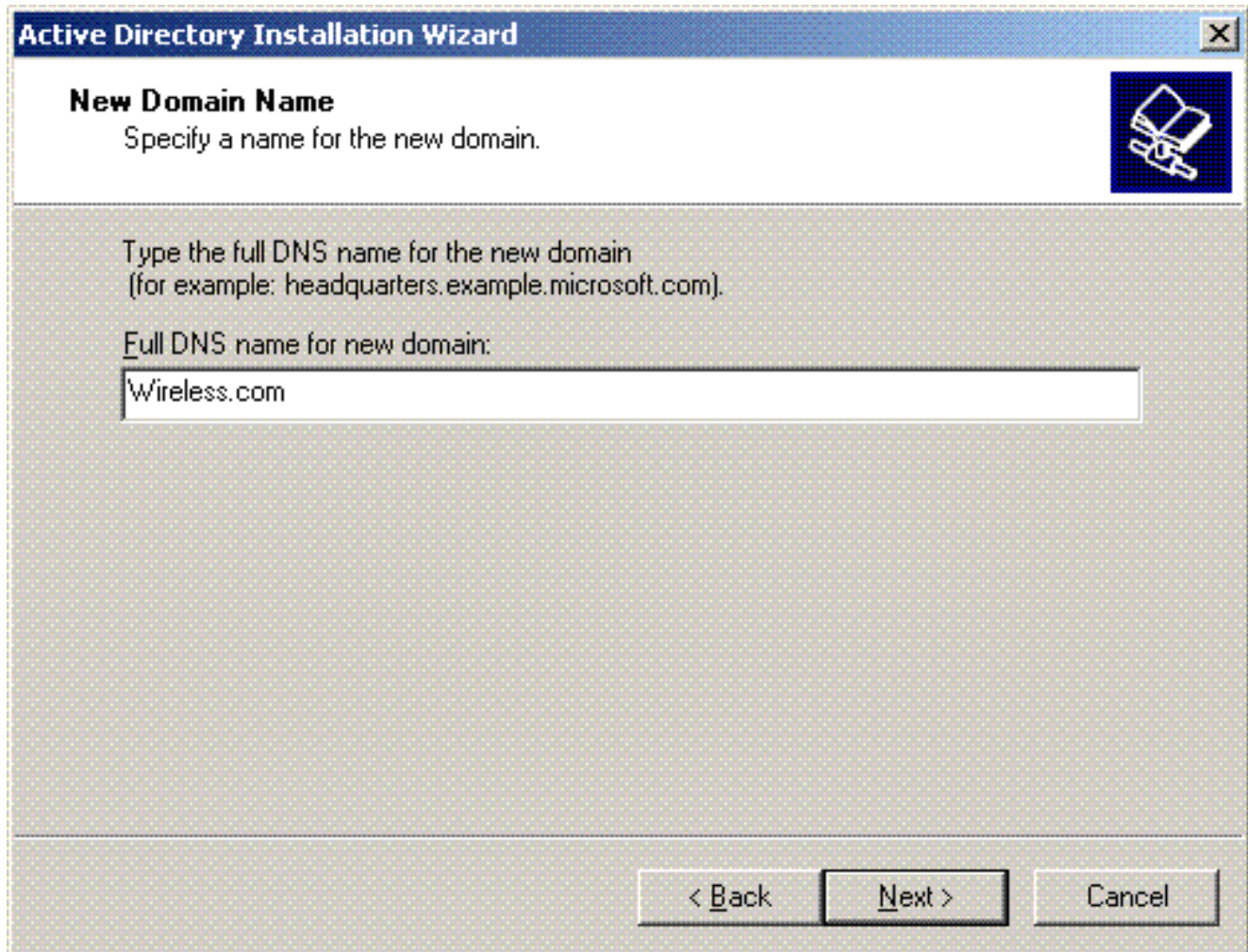
4. 按一下下一步以建立新的域樹林。



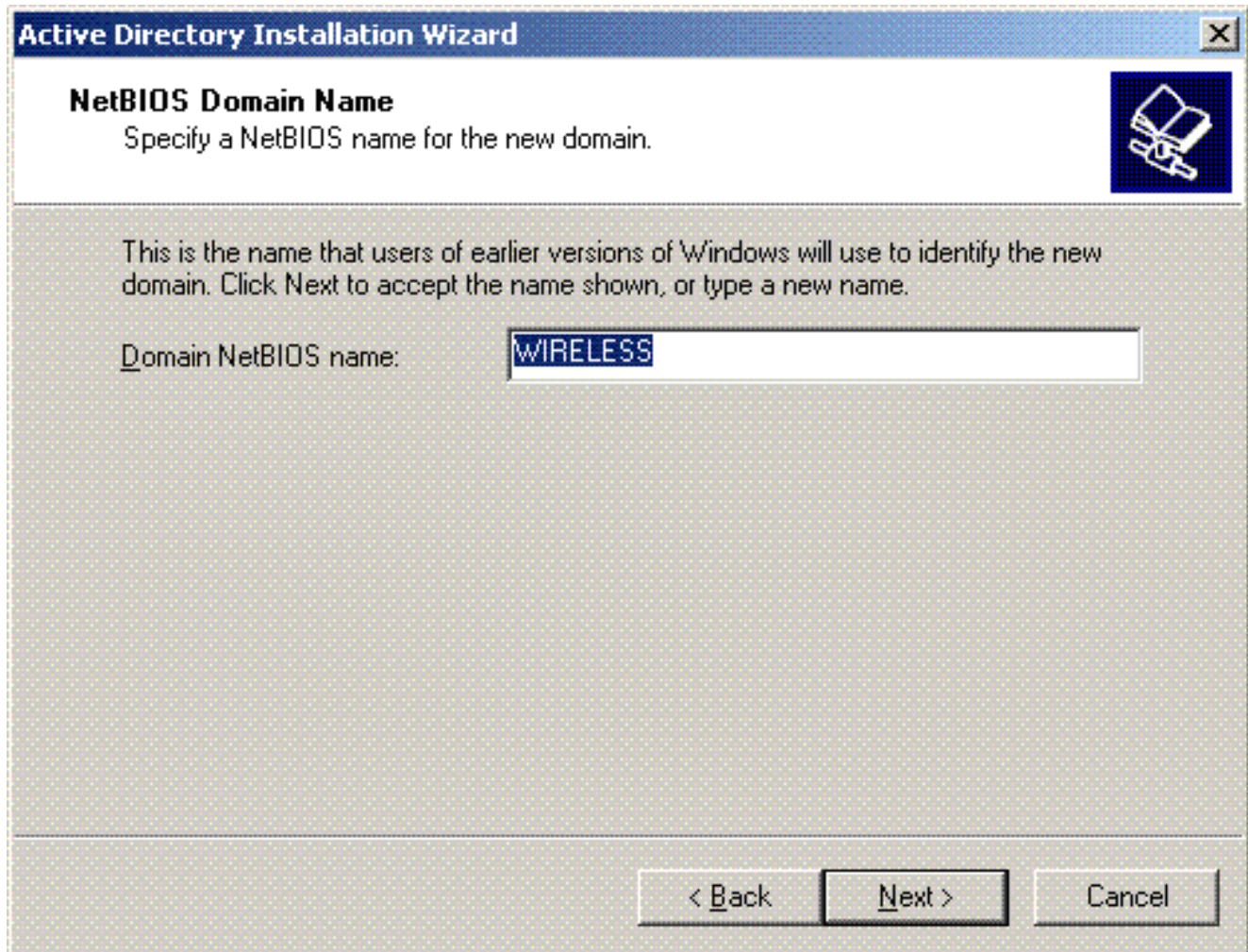
5. 如果系統中未安裝DNS，嚮導將為您提供配置DNS的選項。選擇**No**，**Just Install and Configure DNS on this computer**。按「**Next**」（下一步）。



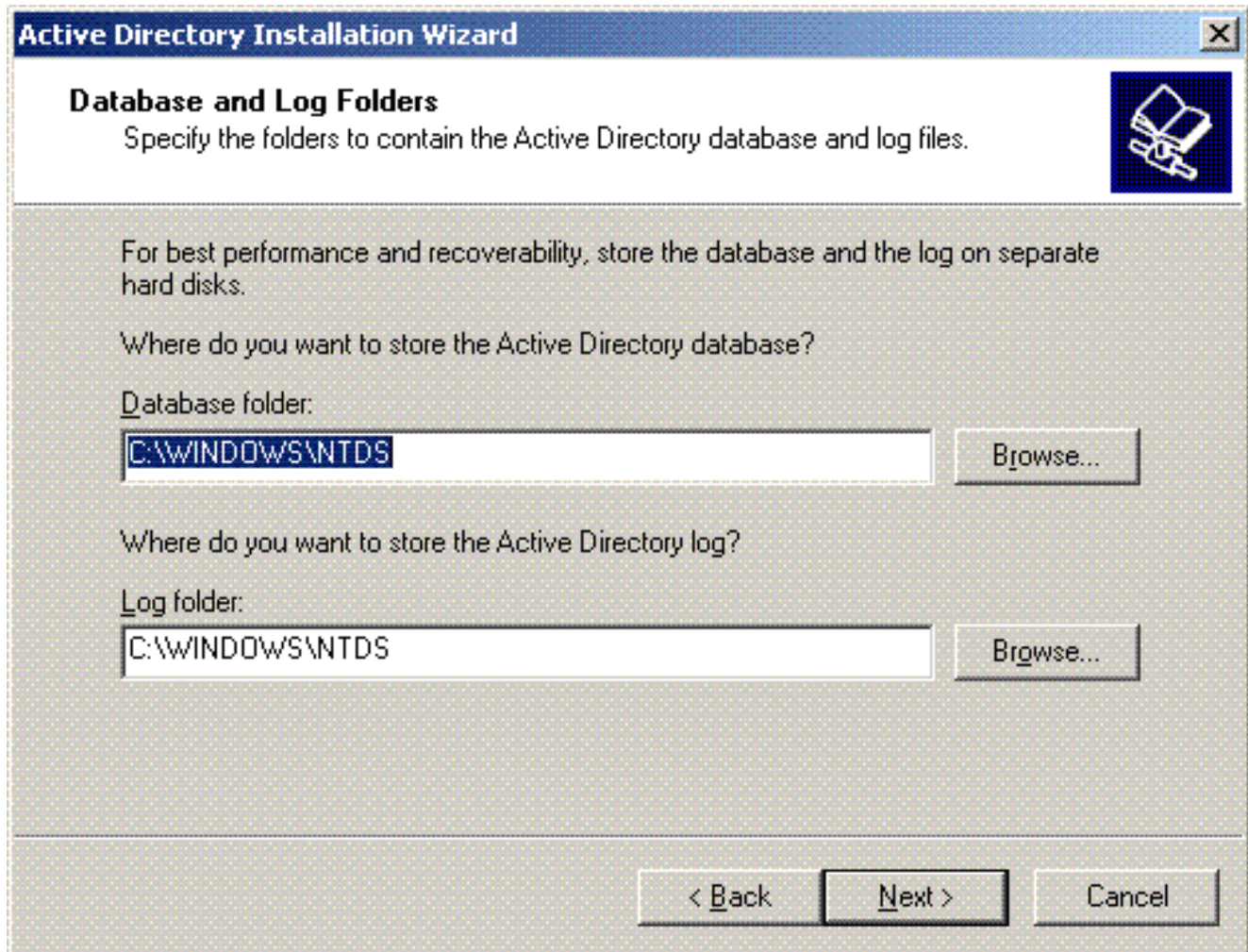
6. 鍵入新域的完整DNS名稱。在此範例中使用Wireless.com，然後按一下「Next」。



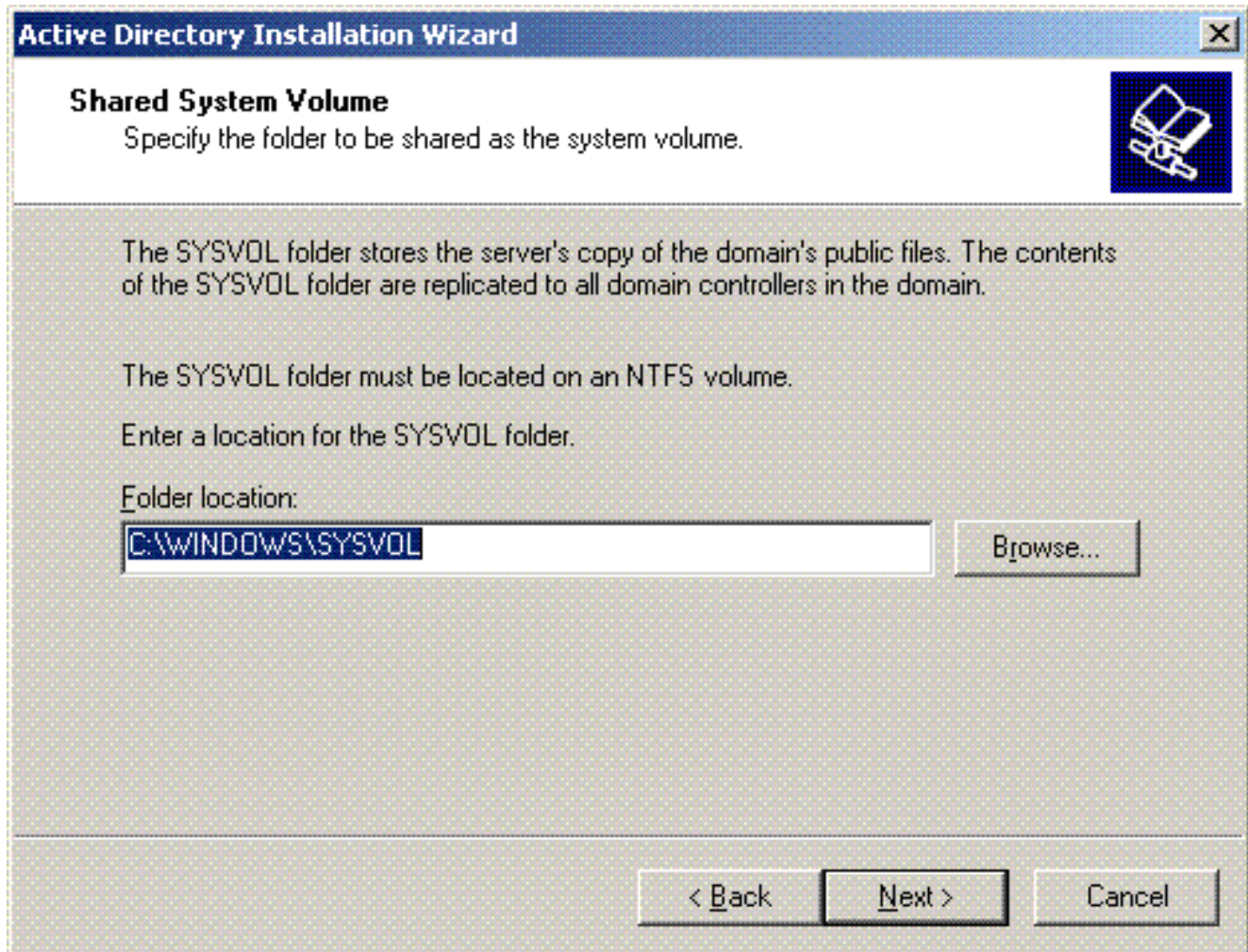
7. 輸入域的NETBIOS名稱，然後按一下**Next**。此範例使用**WIRELESS**。



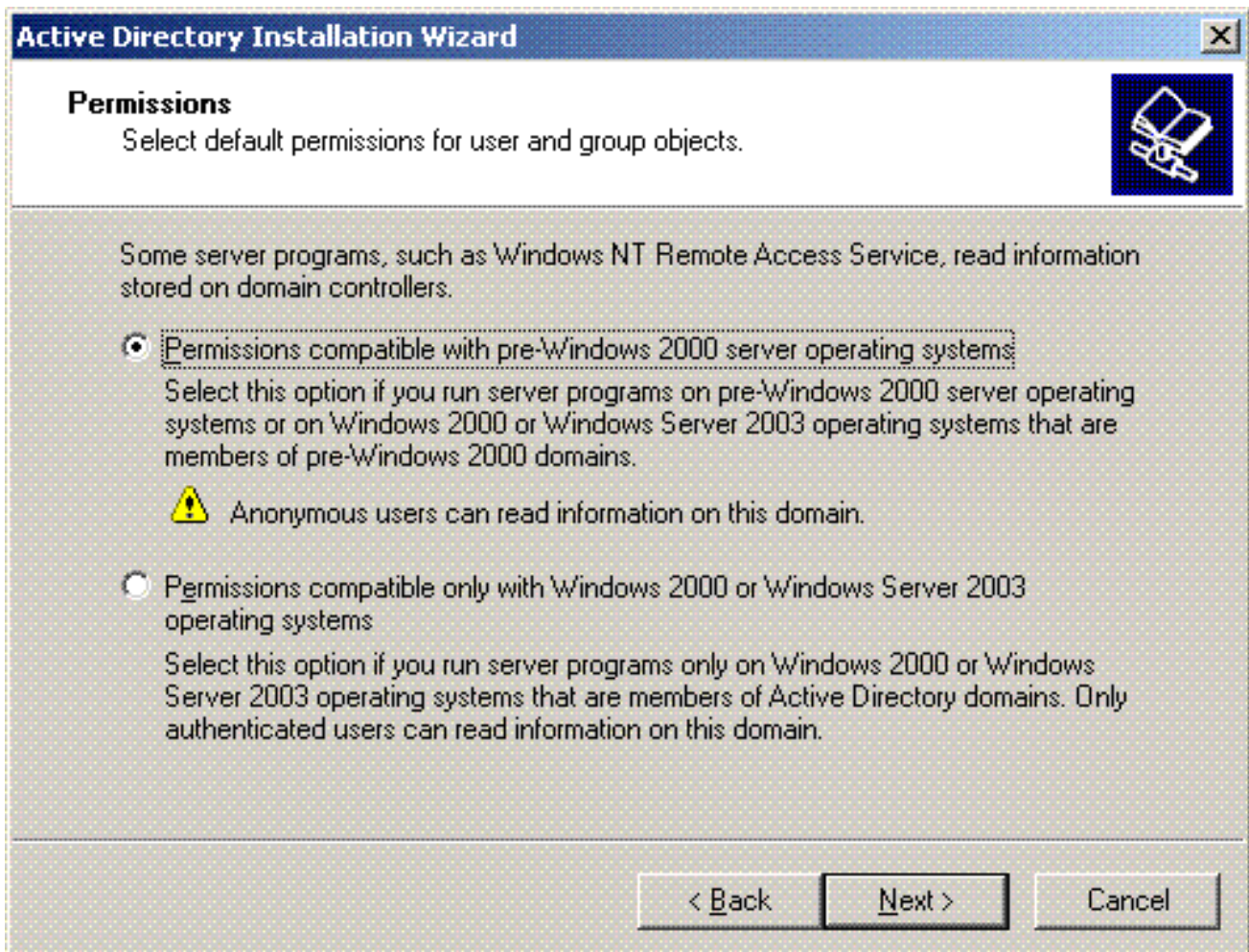
8. 選擇域的資料庫和日誌位置。按「Next」（下一步）。



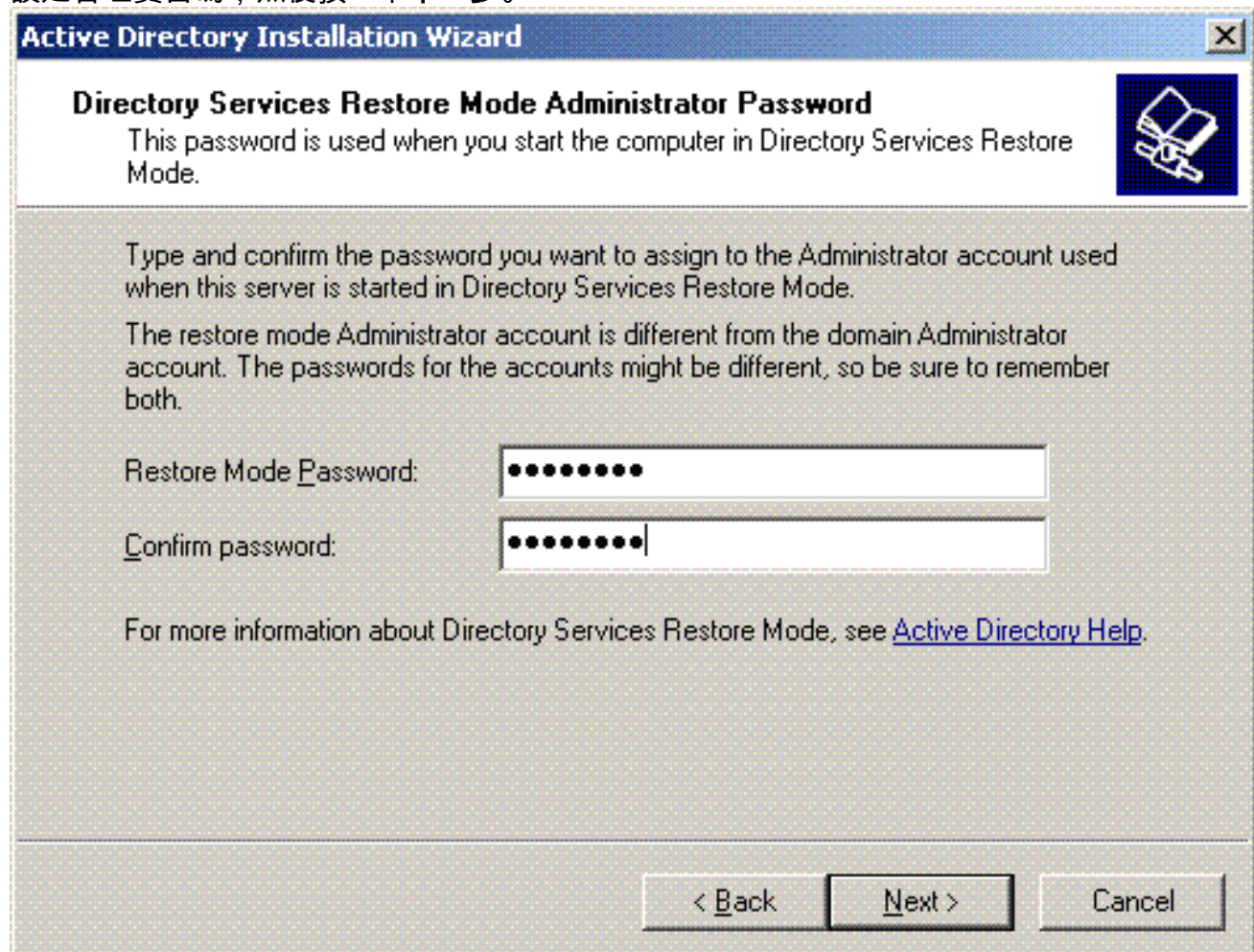
9. 選擇Sysvol資料夾的位置。按「Next」（下一步）。



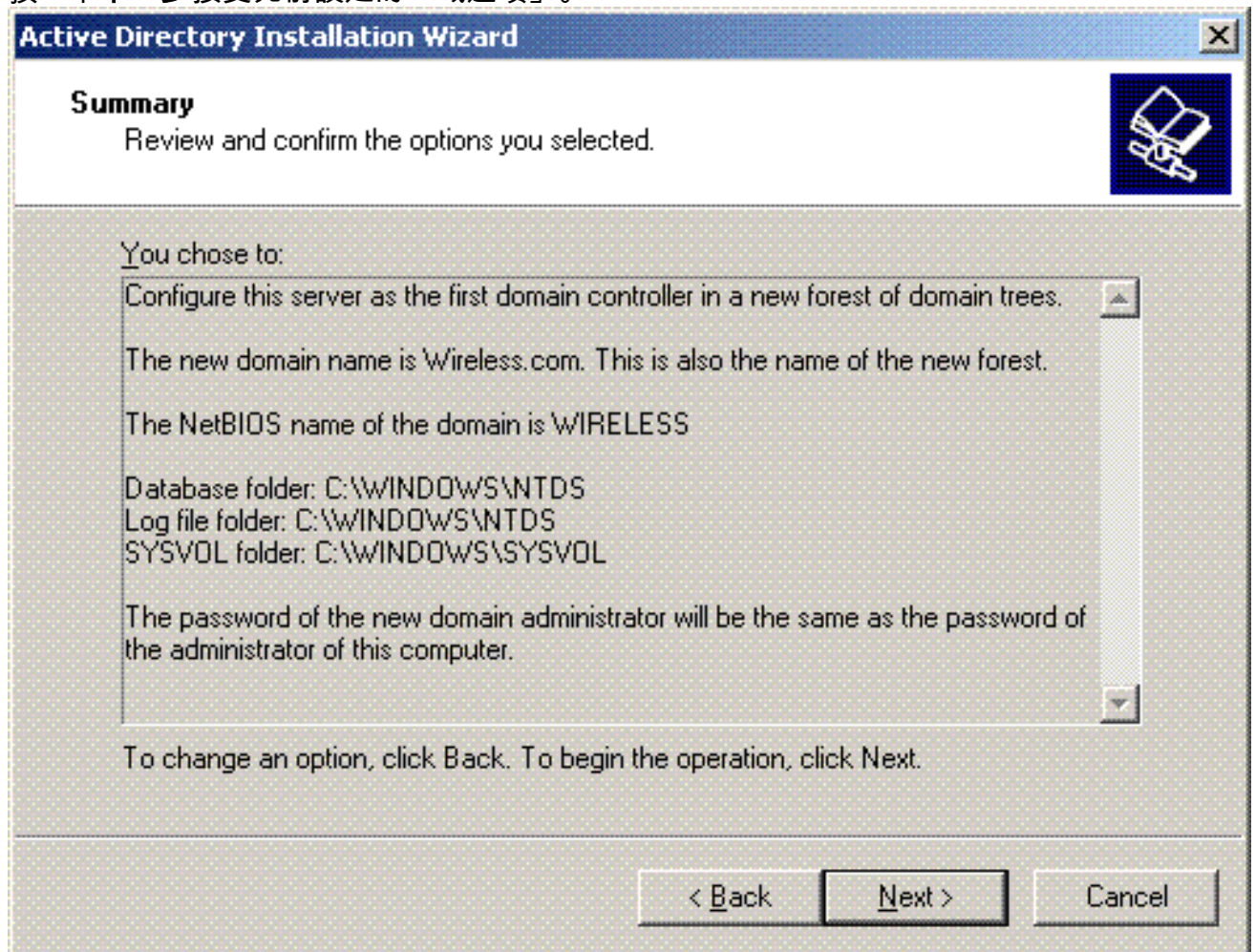
10. 選擇使用者和組的預設許可權。按「Next」（下一步）。



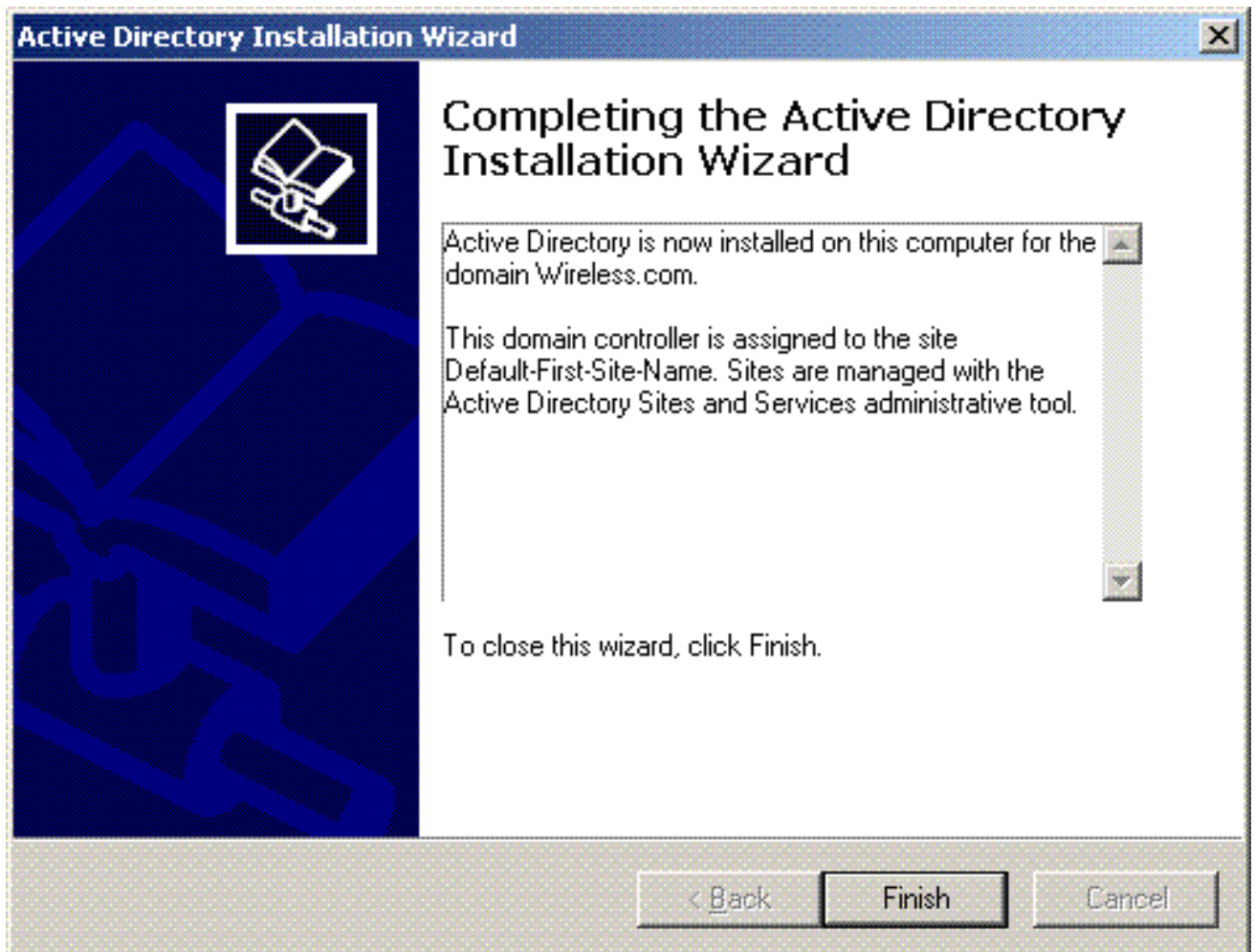
11. 設定管理員密碼，然後按一下下一步。



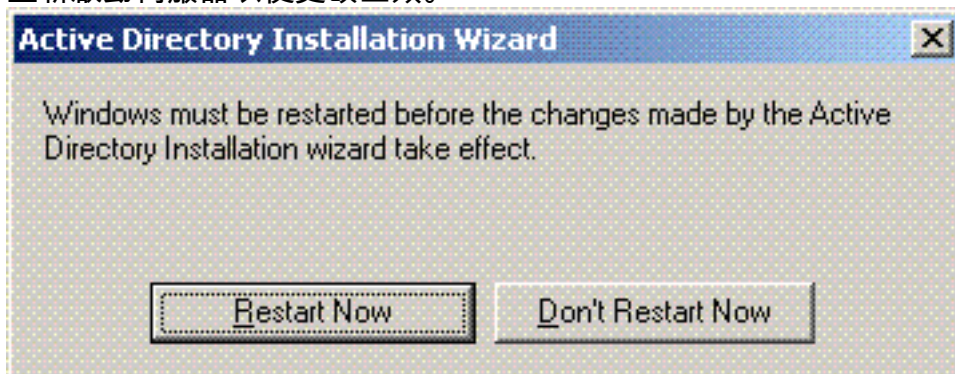
12. 按一下**下一步**接受先前設定的「域選項」。



13. 按一下**完成**關閉Active Directory安裝嚮導。



14. 重新啟動伺服器以使更改生效。

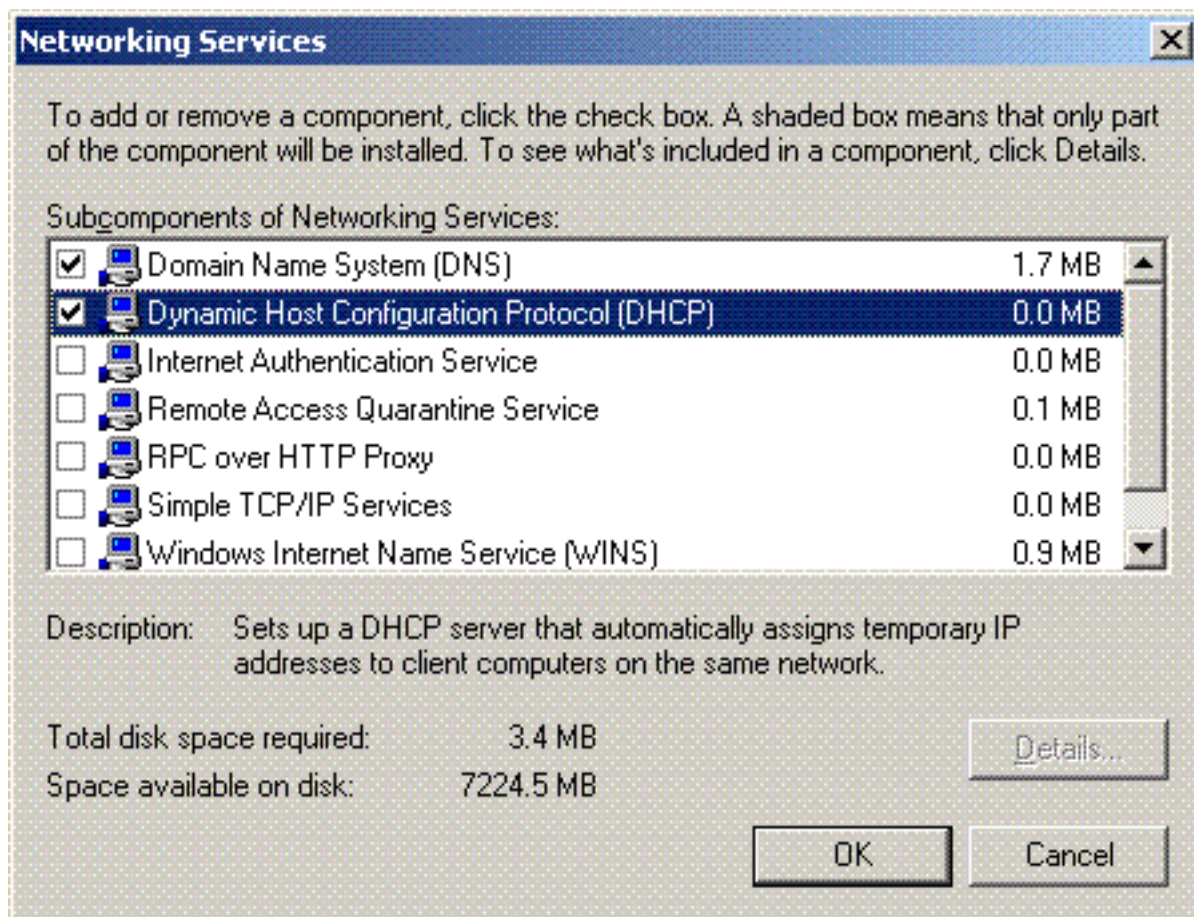


通過此步驟，您已將Microsoft Windows 2003伺服器配置為域控制器，並建立了新域 Wireless.com。接下來，在伺服器上配置DHCP服務。

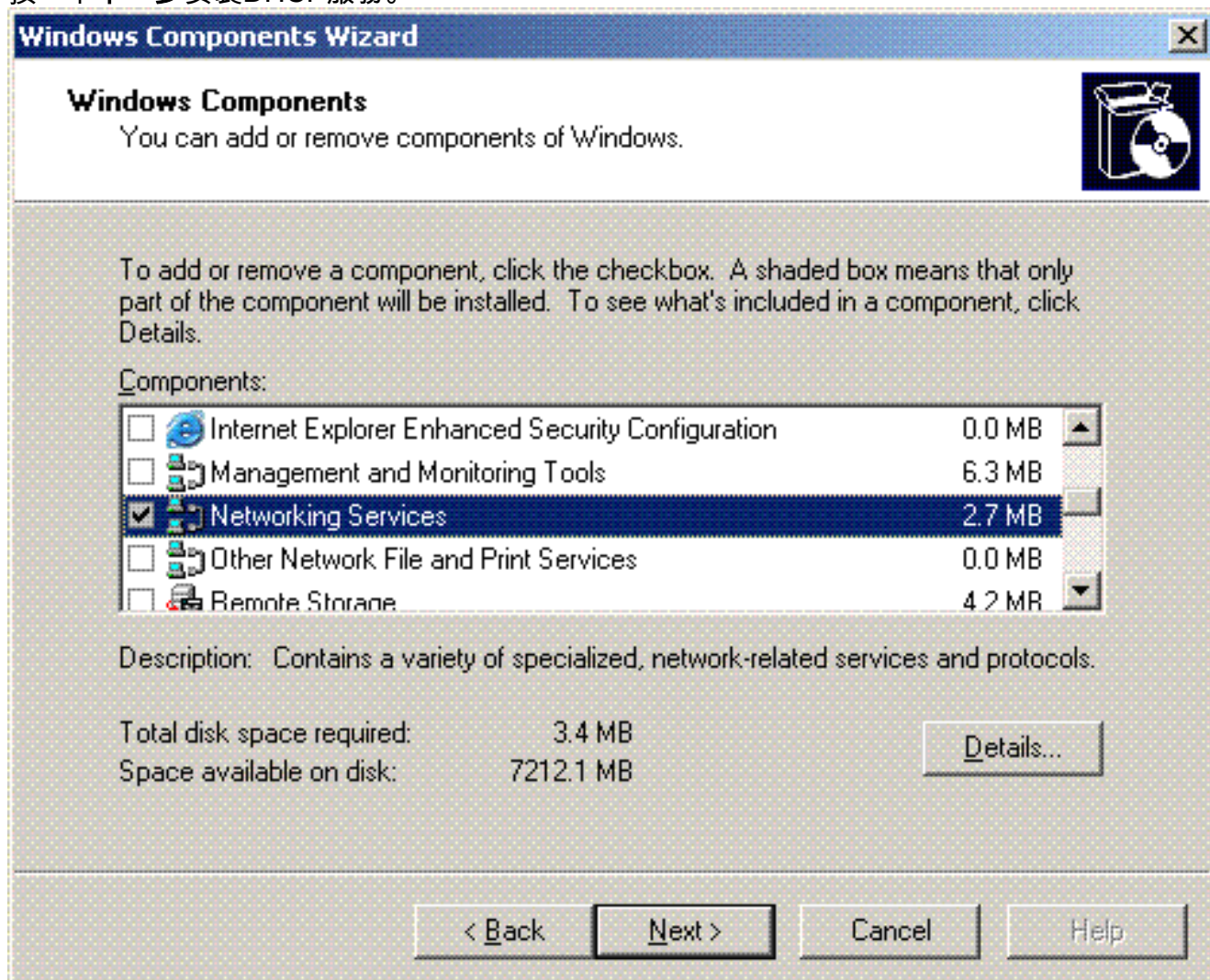
[在Microsoft Windows 2003 Server上安裝並配置DHCP服務](#)

Microsoft 2003伺服器上的DHCP服務用於為無線客戶端提供IP地址。若要在此伺服器上安裝和配置DHCP服務，請完成以下步驟：

1. 在「Control Panel (控制面板)」中按一下**Add or Remove Programs**。
2. 按一下**Add/Remove Windows Components**。
3. 選擇**Networking Services**，然後按一下**Details**。
4. 選擇**Dynamic Host Configuration Protocol(DHCP)**，然後按一下**OK**。



5. 按一下下一步安裝DHCP服務。



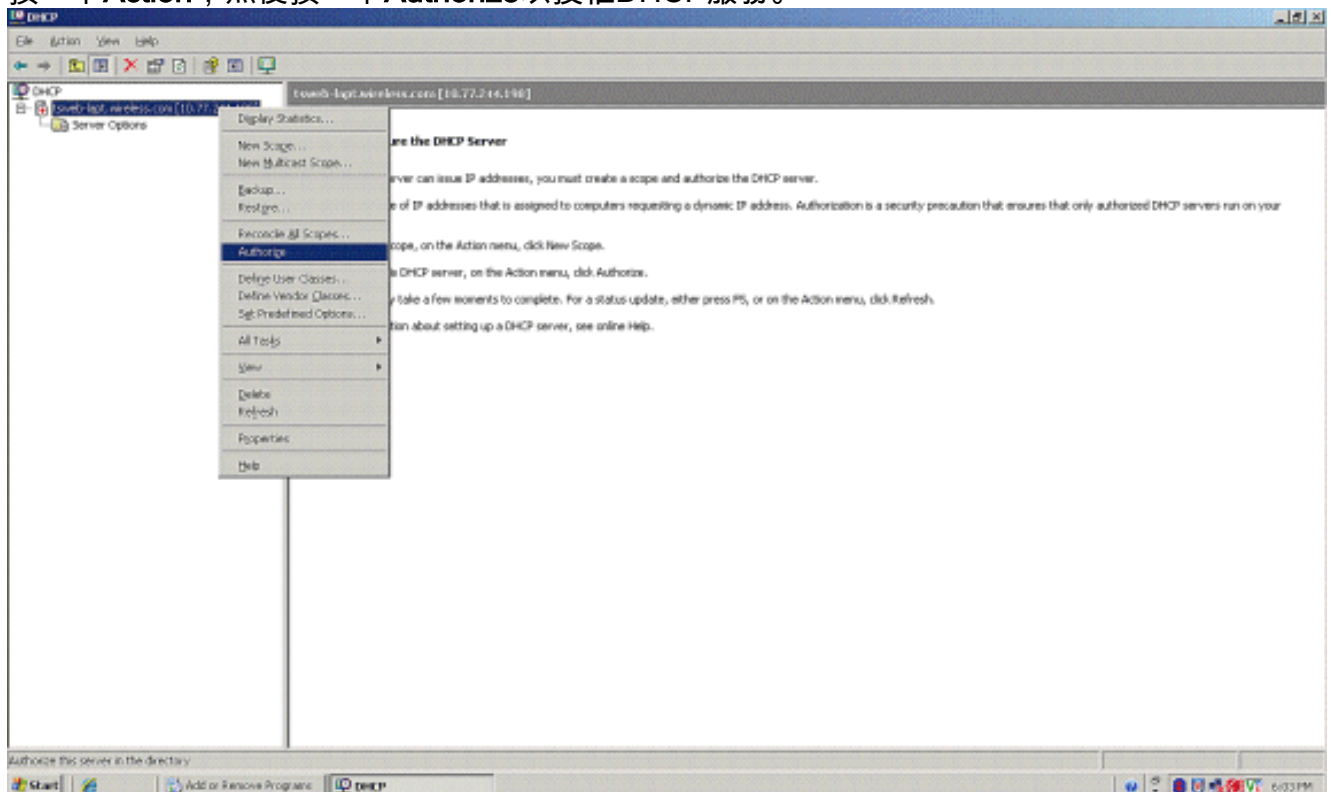
6. 按一下**Finish**完成安裝。



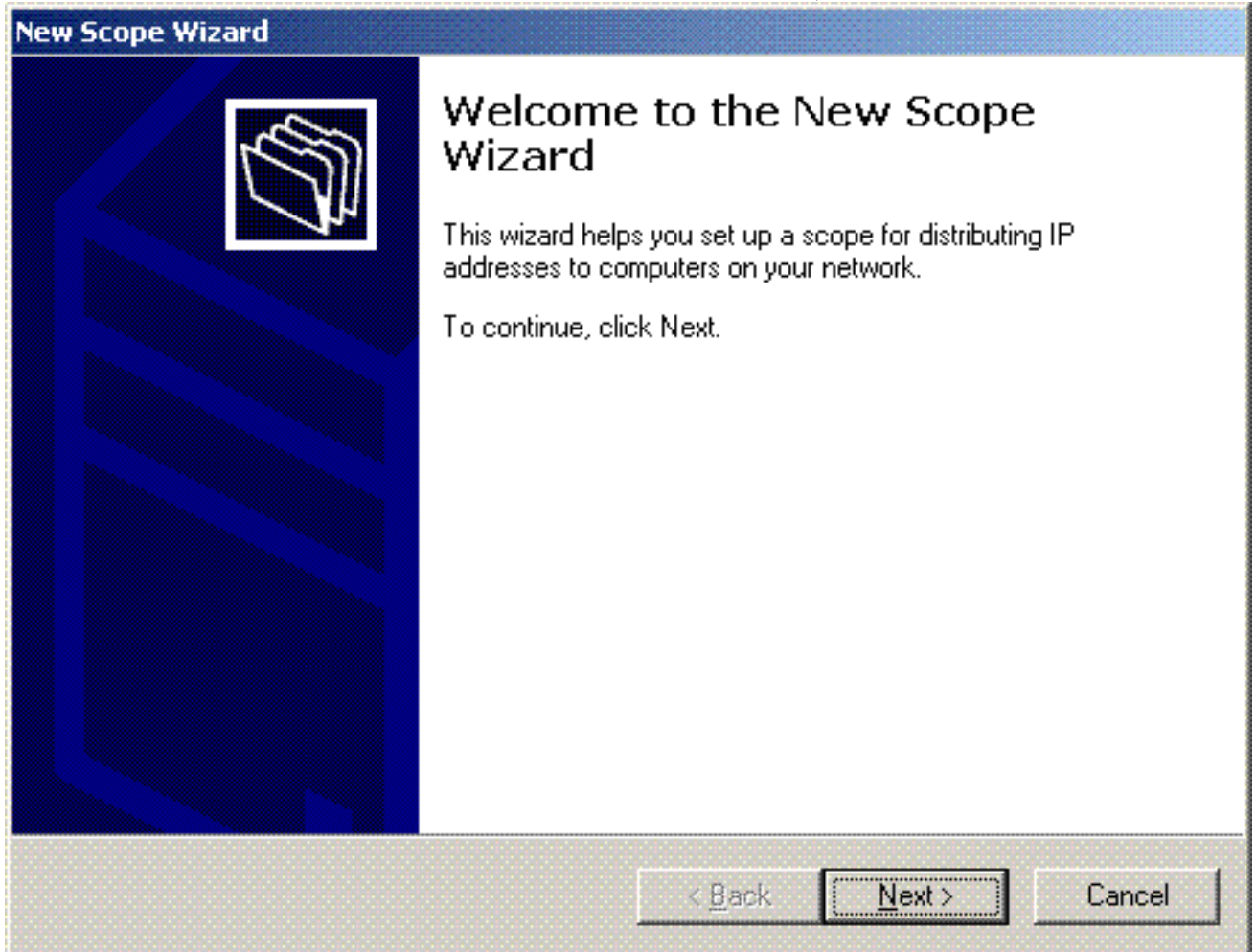
7. 要配置DHCP服務，請按一下**開始>程式>管理工具**，然後按一下**DHCP管理單元**。

8. 選擇DHCP伺服器 — **tsweb-lapt.wireless.com** (在本例中) 。

9. 按一下**Action**，然後按一下**Authorize**以授權DHCP服務。



10. 在控制檯樹中，按一下右鍵`tsweb-lapt.wireless.com`，然後按一下**New Scope**以定義無線客戶端的IP地址範圍。
11. 在「新建作用域嚮導」的「歡迎使用新建作用域嚮導」頁上，按一下下一步。



12. 在Scope Name頁面上，鍵入DHCP作用域的名稱。在本示例中，使用**DHCP-Clients**作為作用域名稱。按「**Next**」（下一步）。

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

13. 在「IP地址範圍」頁上，輸入範圍的起始IP地址和結束IP地址，然後按一下下一步。

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address:

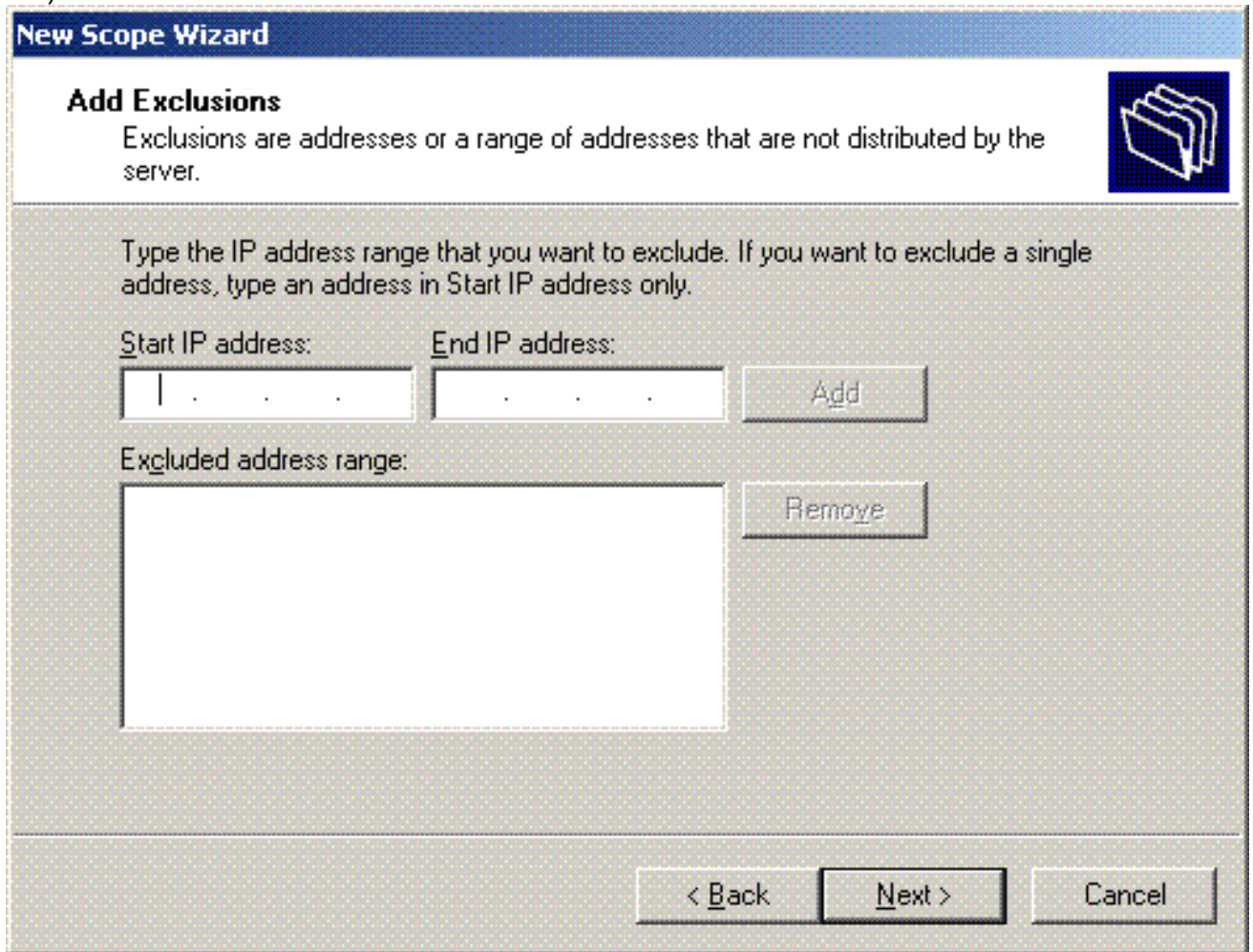
End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

14. 在Add Exclusions頁面上，提及要從DHCP作用域中保留/排除的IP地址。按「Next」（下一步）。



The screenshot shows a Windows dialog box titled "New Scope Wizard" with a sub-header "Add Exclusions". The main text reads: "Exclusions are addresses or a range of addresses that are not distributed by the server." Below this, instructions state: "Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only." There are two input fields: "Start IP address:" and "End IP address:", each followed by a text box and an "Add" button. Below these is an "Excluded address range:" label and a large empty text box, with a "Remove" button to its right. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

15. 在Lease Duration頁面中提及租用持續時間，然後按一下Next。

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

16. 在Configure DHCP options頁上，選擇Yes，I want to configure DHCP Option now，然後按一下Next。

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

17. 如果有預設網關路由器，請在Router(Default Gateway)頁面中提及網關路由器的IP地址，然後按一下Next。

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

Remove

Up

Down

< Back

Next >

Cancel

18. 在「域名和DNS伺服器」頁面上，鍵入之前配置的域的名稱。在本例中，使用 **Wireless.com**。輸入伺服器的IP地址。按一下「Add」。

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

Add

Resolve

10.77.244.217

Remove

Up

Down

< Back

Next >

Cancel

19. 按「**Next**」(下一步)。
20. 在「WINS伺服器」頁上，按一下下一步。
21. 在「啟用作用域」頁上，選擇「**是，我想立即啟用作用域**」，然後按一下「下一步」。

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

Next >

Cancel

22. 完成「新建作用域嚮導」後，按一下**完成**。

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

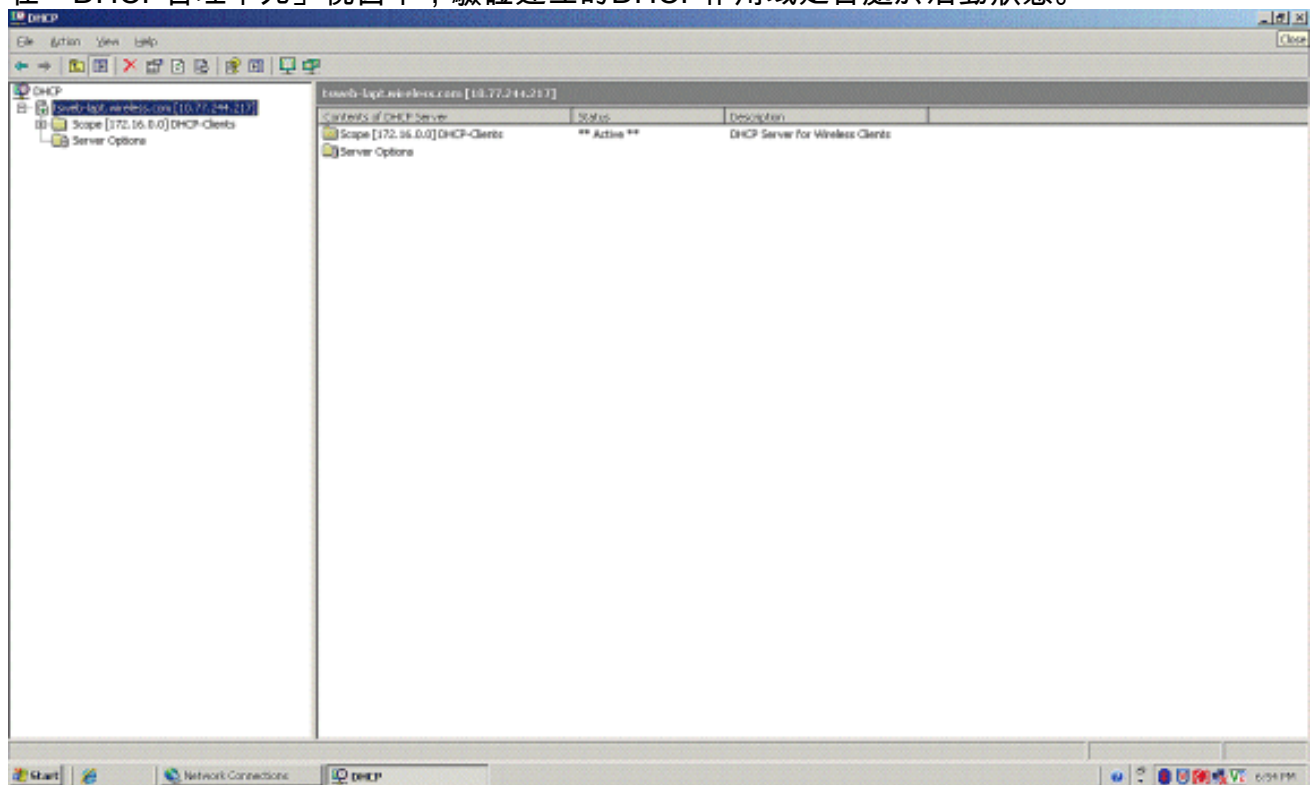
To close this wizard, click Finish.

< Back

Finish

Cancel

23. 在「DHCP管理單元」視窗中，驗證建立的DHCP作用域是否處於活動狀態。



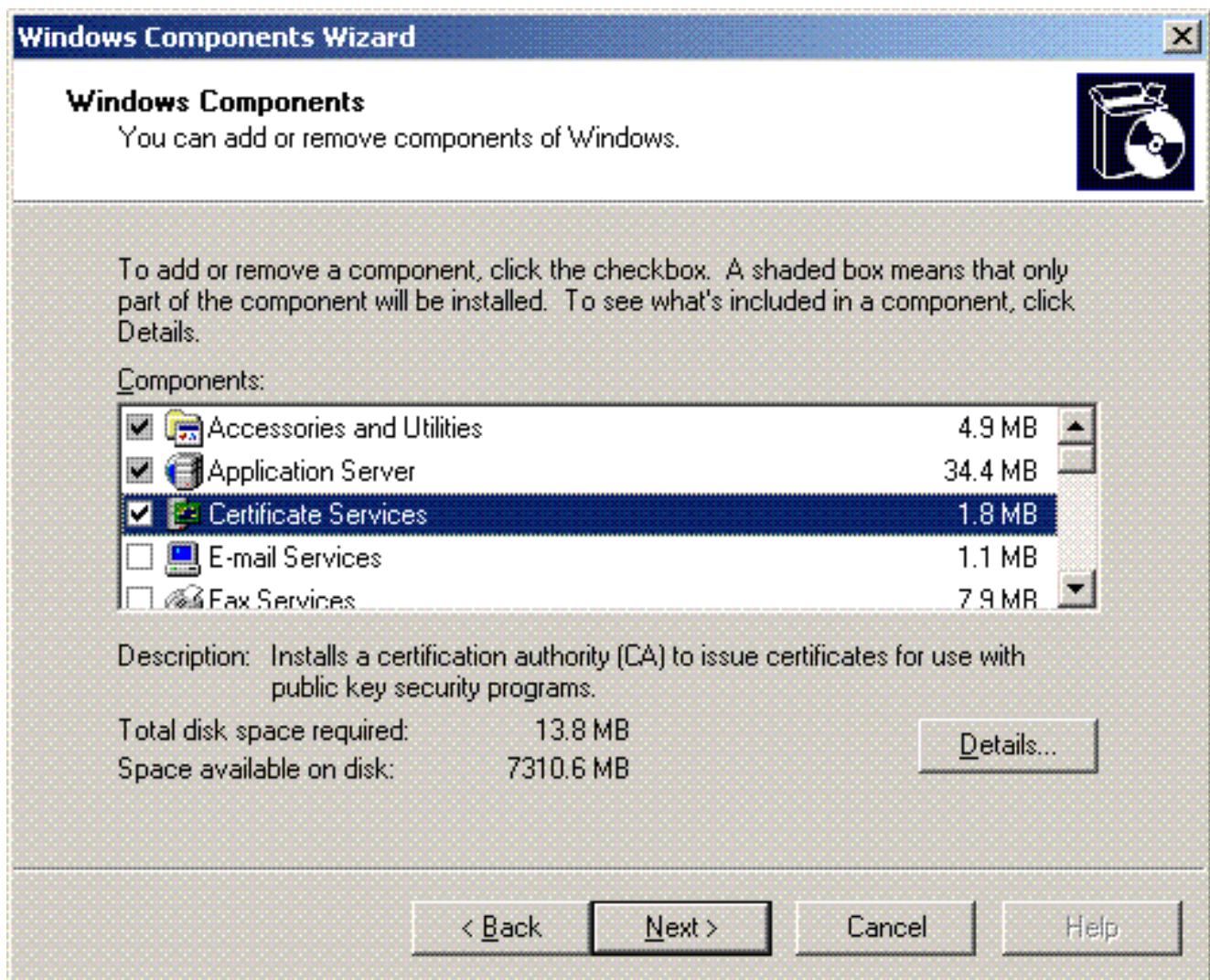
既然在伺服器上啟用了DHCP/DNS，請將伺服器配置為企業證書頒發機構(CA)伺服器。

[安裝Microsoft Windows 2003 Server並將其配置為證書頒發機構\(CA\)伺服器](#)

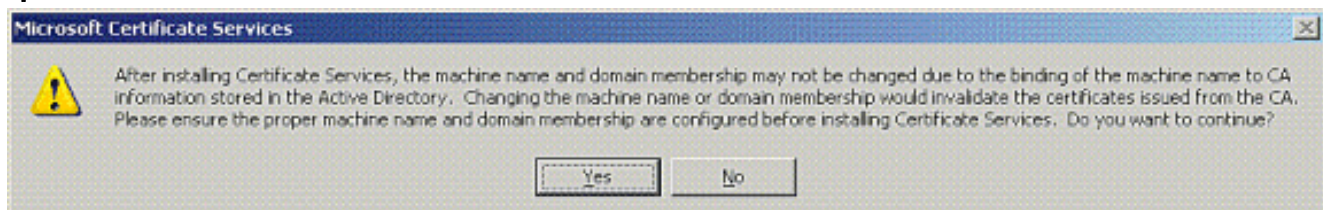
使用EAP-MS-CHAPv2的PEAP根據伺服器上存在的證書驗證RADIUS伺服器。此外，伺服器證書必須由受客戶端電腦信任的公共證書頒發機構(CA)頒發（即，公共CA證書已存在於客戶端電腦證書儲存上的受信任的根證書頒發機構資料夾中）。在本示例中，將Microsoft Windows 2003伺服器配置為向Internet身份驗證服務(IAS)頒發證書的證書頒發機構(CA)。

若要在伺服器上安裝和設定憑證服務，請完成以下步驟：

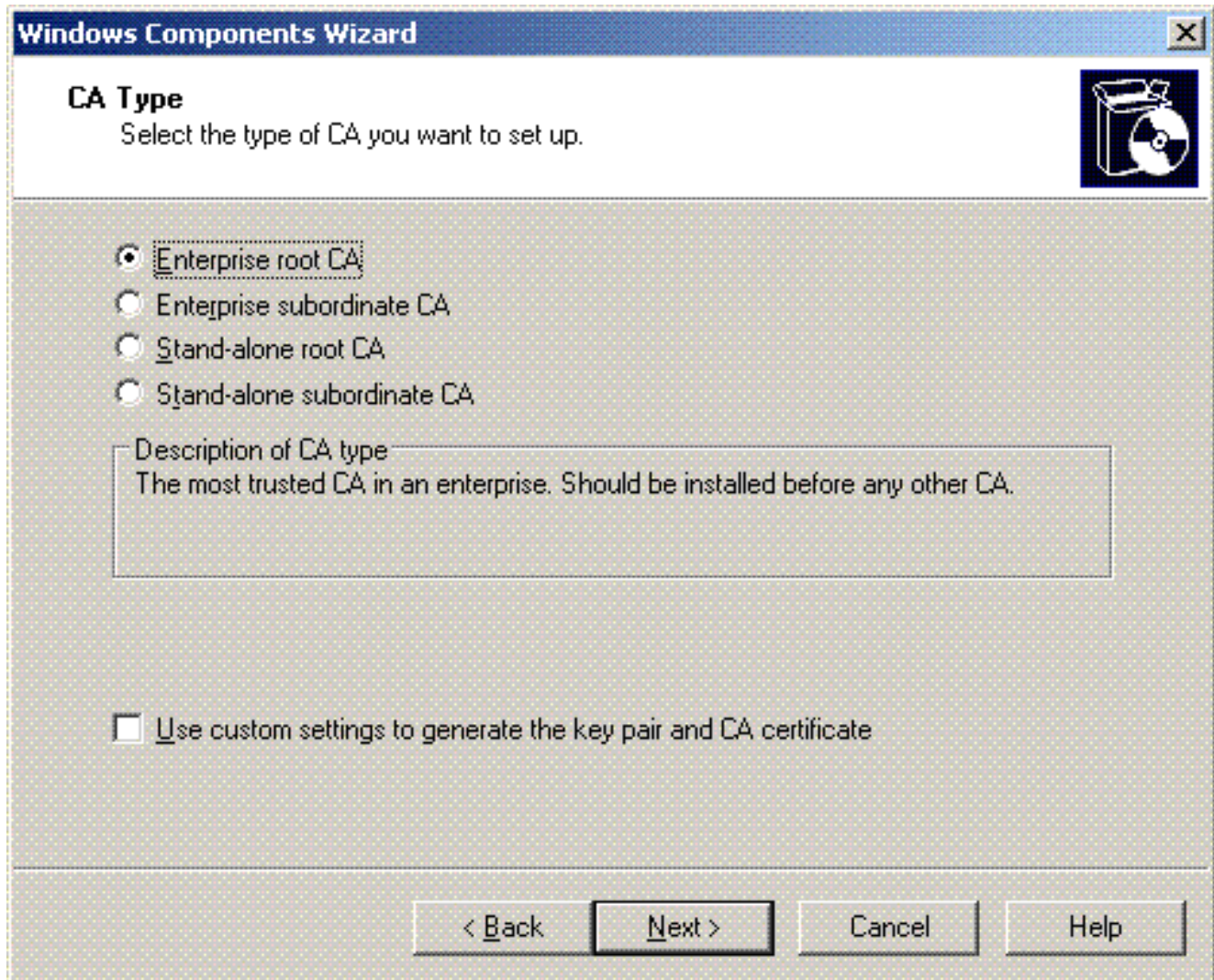
1. 在「Control Panel (控制面板)」中按一下「Add or Remove programs (新增/刪除程式)」。
2. 按一下**新增/刪除Windows元件**。
3. 按一下「Certificate Services」。



4. 按一下Yes轉到警告消息After Installing Certificate Services，該電腦不能重新命名，並且不能加入域或從域中刪除。是否要繼續？




5. 在Certificate Authority Type下，選擇Enterprise root CA，然後按一下Next。



6. 輸入用於標識CA的名稱。此範例使用Wireless-CA。按「Next」（下一步）。

Windows Components Wizard X

CA Identifying Information 
Enter information to identify this CA.

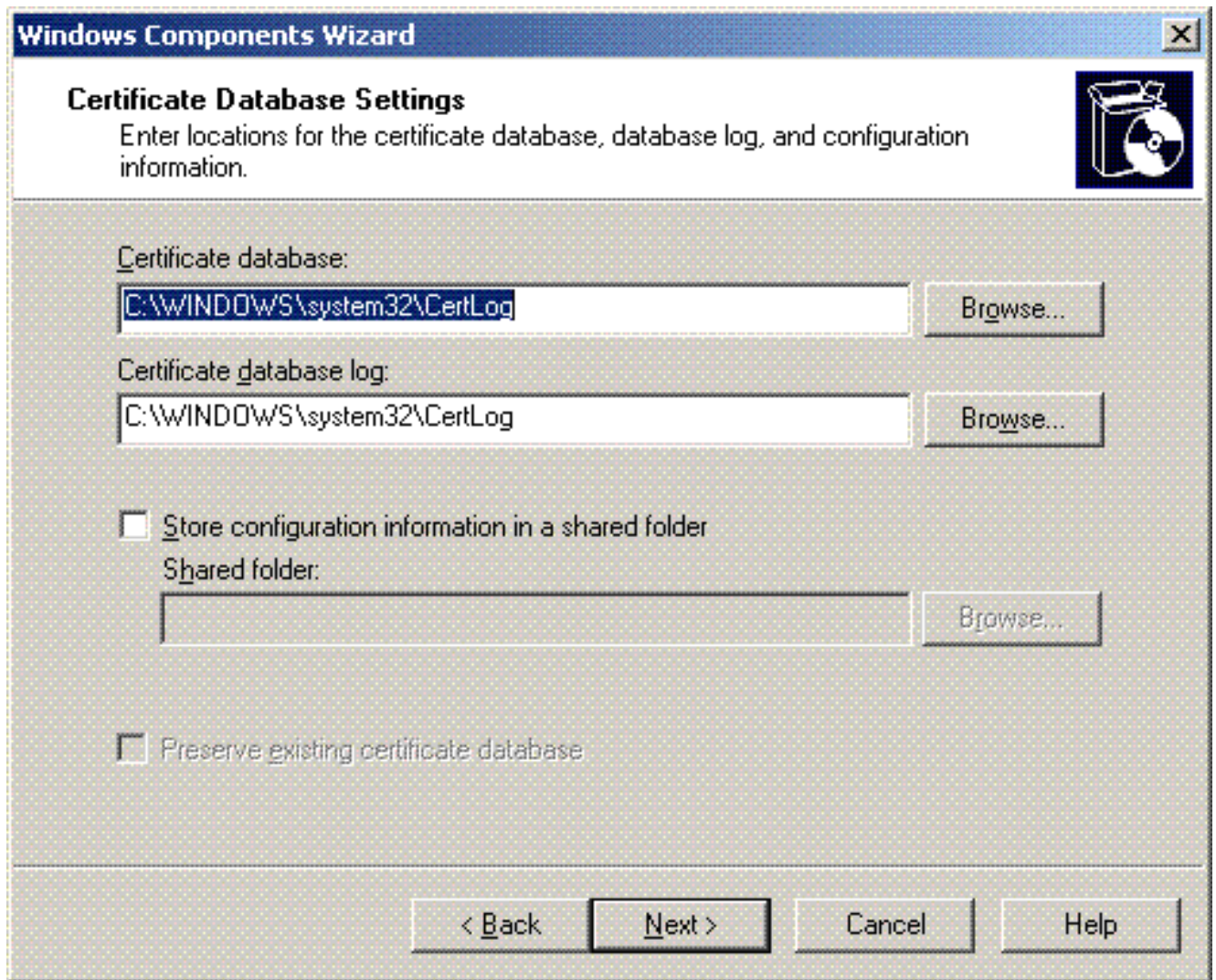
Common name for this CA:

Distinguished name suffix:

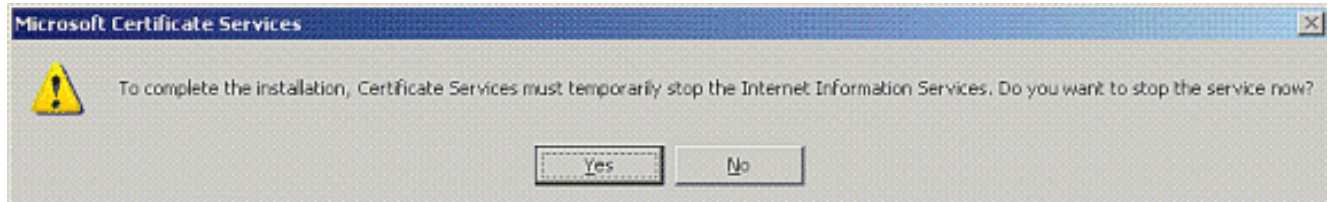
Preview of distinguished name:

Validity period:
Expiration date: 12/12/2012 7:01 PM

7. 為證書資料庫儲存建立「證書日誌」目錄。按「Next」（下一步）。



8. 如果已啟用IIS，則必須先將其停止，然後才能繼續。按一下OK可顯示必須停止IIS的警告消息。安裝CA後它會自動重新啟動。



9. 按一下Finish完成證書頒發機構(CA)服務的安裝。

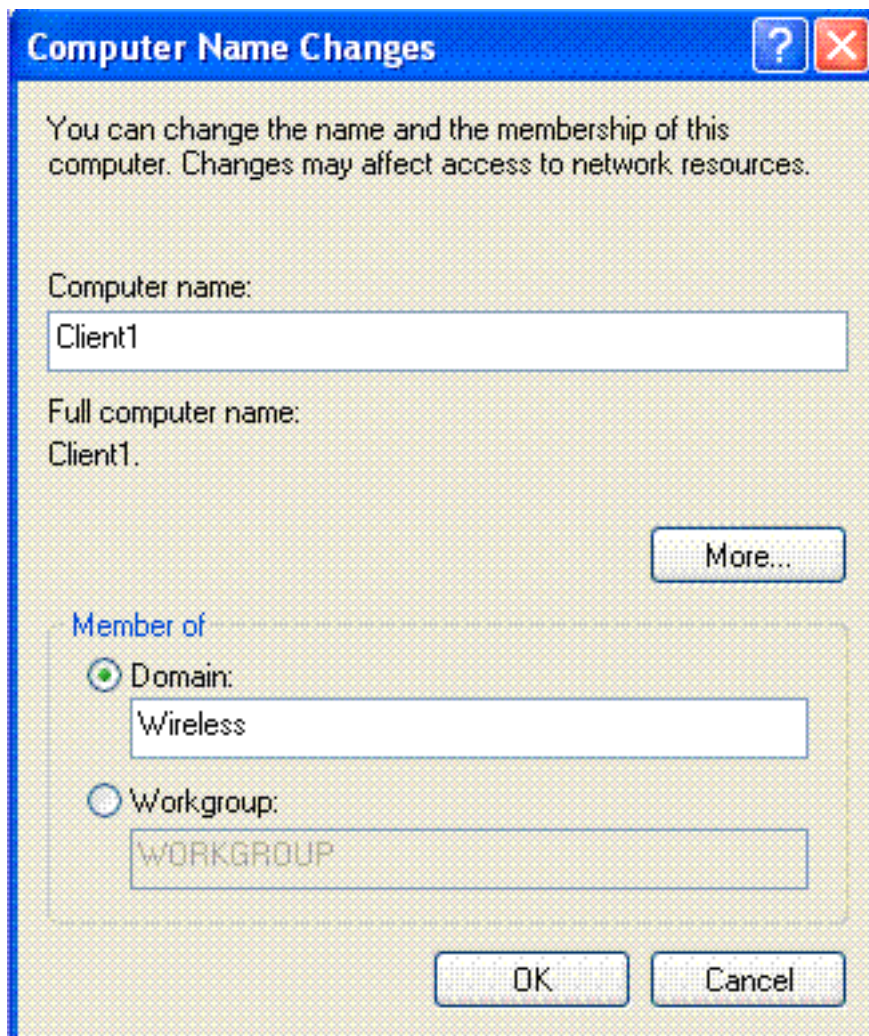


下一步是在Microsoft Windows 2003伺服器上安裝和配置Internet身份驗證服務。

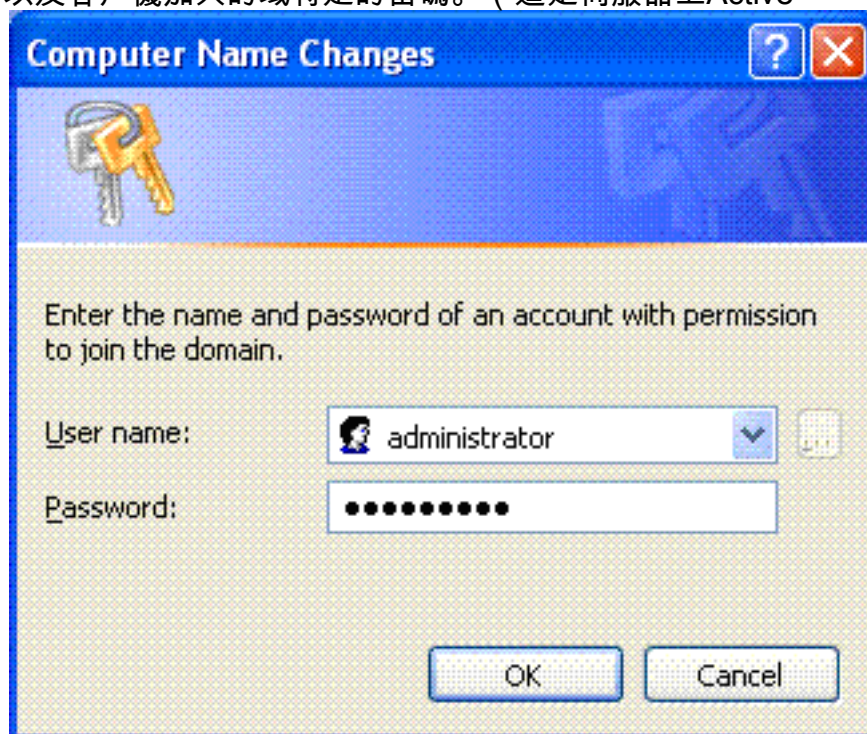
將客戶端連線到域

下一步是將客戶端連線到有線網路，並從新域下載域特定資訊。換句話說，將客戶端連線到域。為此，請完成以下步驟：

1. 使用直通乙太網電纜將客戶端連線到有線網路。
2. 啟動客戶端並使用客戶端的使用者名稱/密碼登入。
3. 按一下**開始**；按一下**運行**；鍵入**cmd**；然後按一下**確定**。
4. 在命令提示符下，鍵入**ipconfig**，然後按一下**Enter**以驗證DHCP是否正常工作，並且客戶端從DHCP伺服器收到IP地址。
5. 若要將客戶端加入域，請按一下右鍵**My Computer**，然後選擇**Properties**。
6. 按一下**Computer Name**頁籤。
7. 按一下「**Change**」。
8. 按一下**Domain**；鍵入**wireless.com**；然後按一下**OK**。



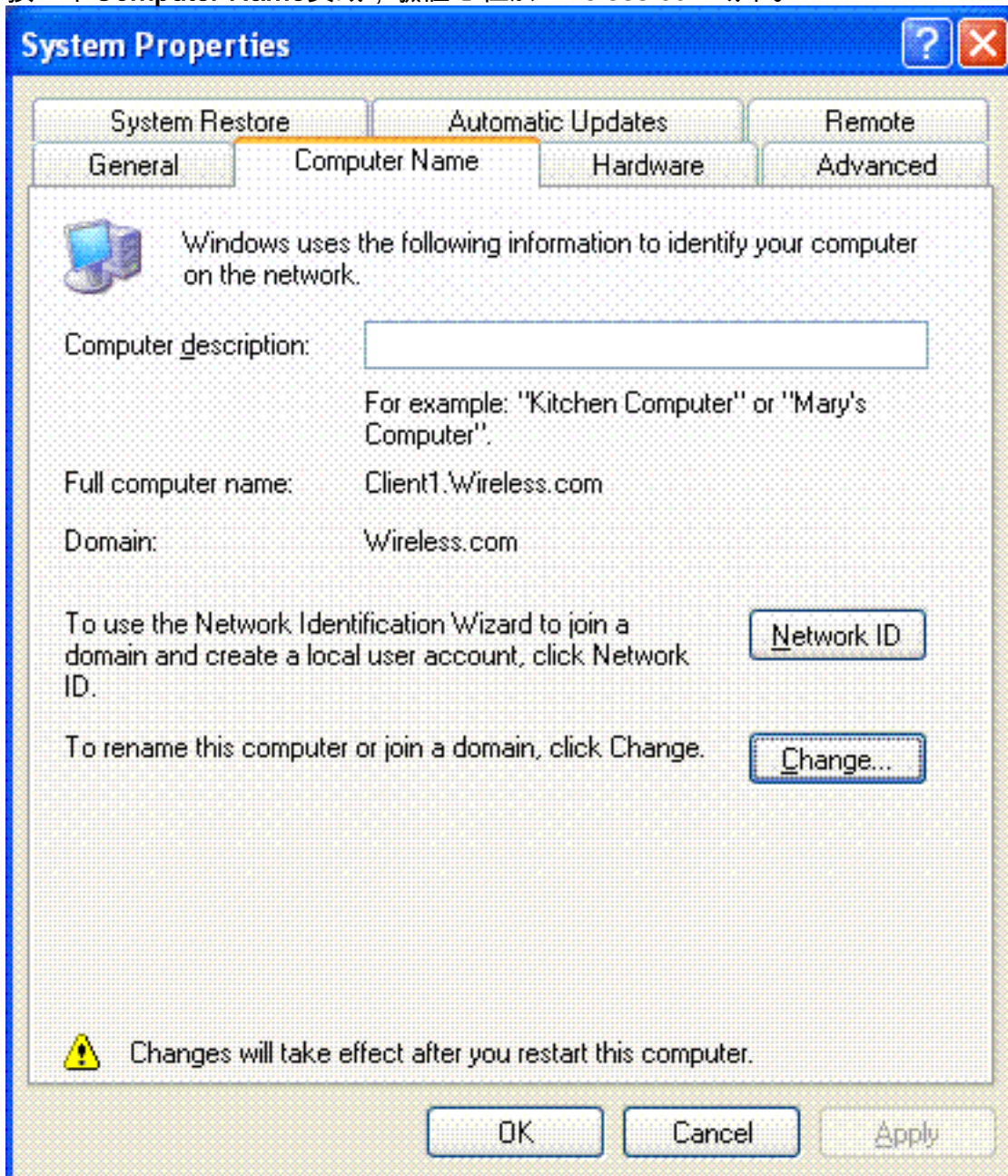
9. 鍵入Username Administrator以及客戶機加入的域特定的密碼。(這是伺服器上Active



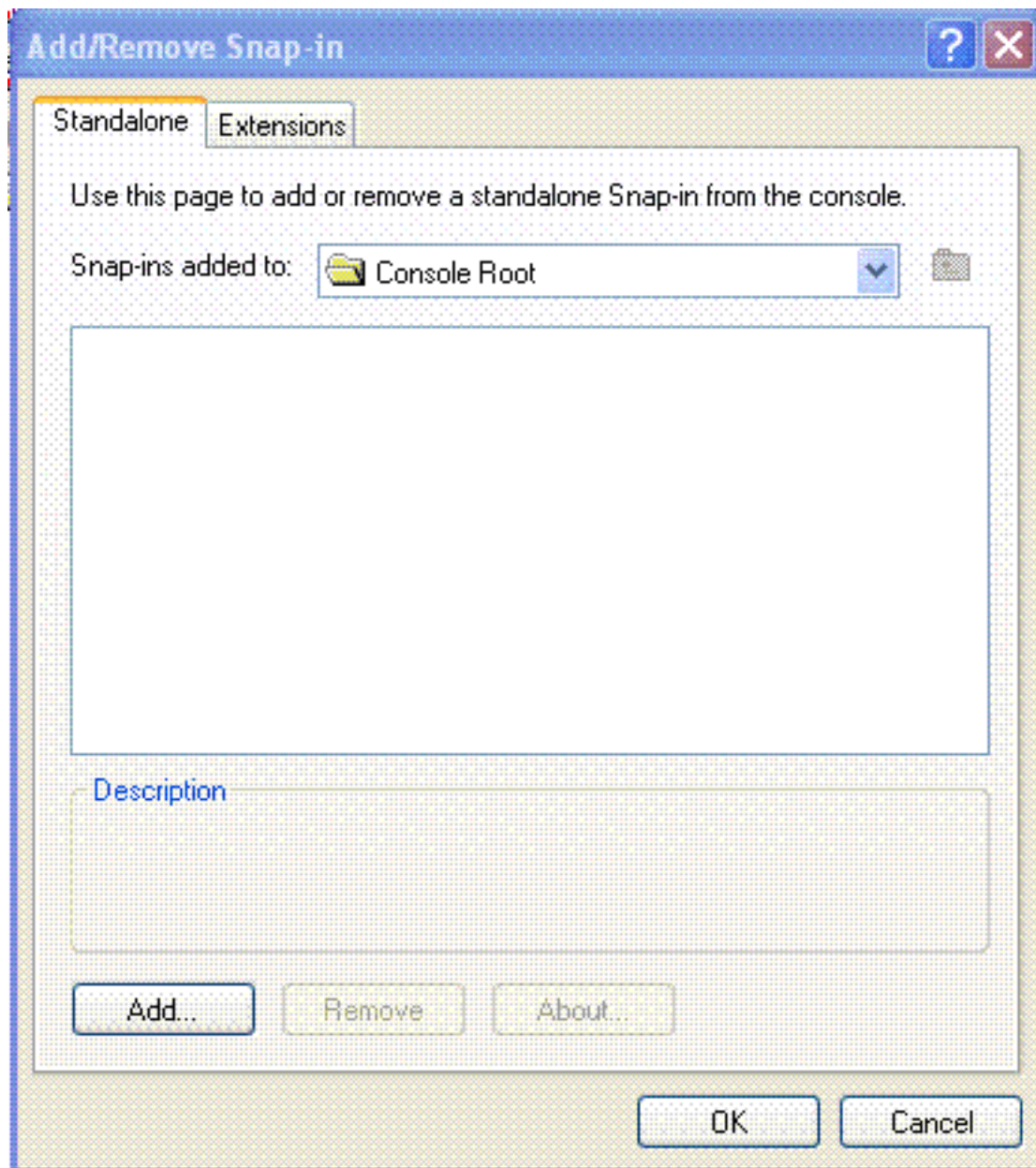
Directory中的管理員帳戶。)



10. 按一下「OK」(確定)。
11. 按一下**Yes**重新啟動電腦。
12. 電腦重新啟動後，使用以下資訊登入：使用者名稱= **Administrator**；密碼= <domain password>；域= **Wireless**。
13. 按一下右鍵**My Computer**，然後按一下**Properties**。
14. 按一下**Computer Name**頁籤，驗證您位於Wireless.com域中。

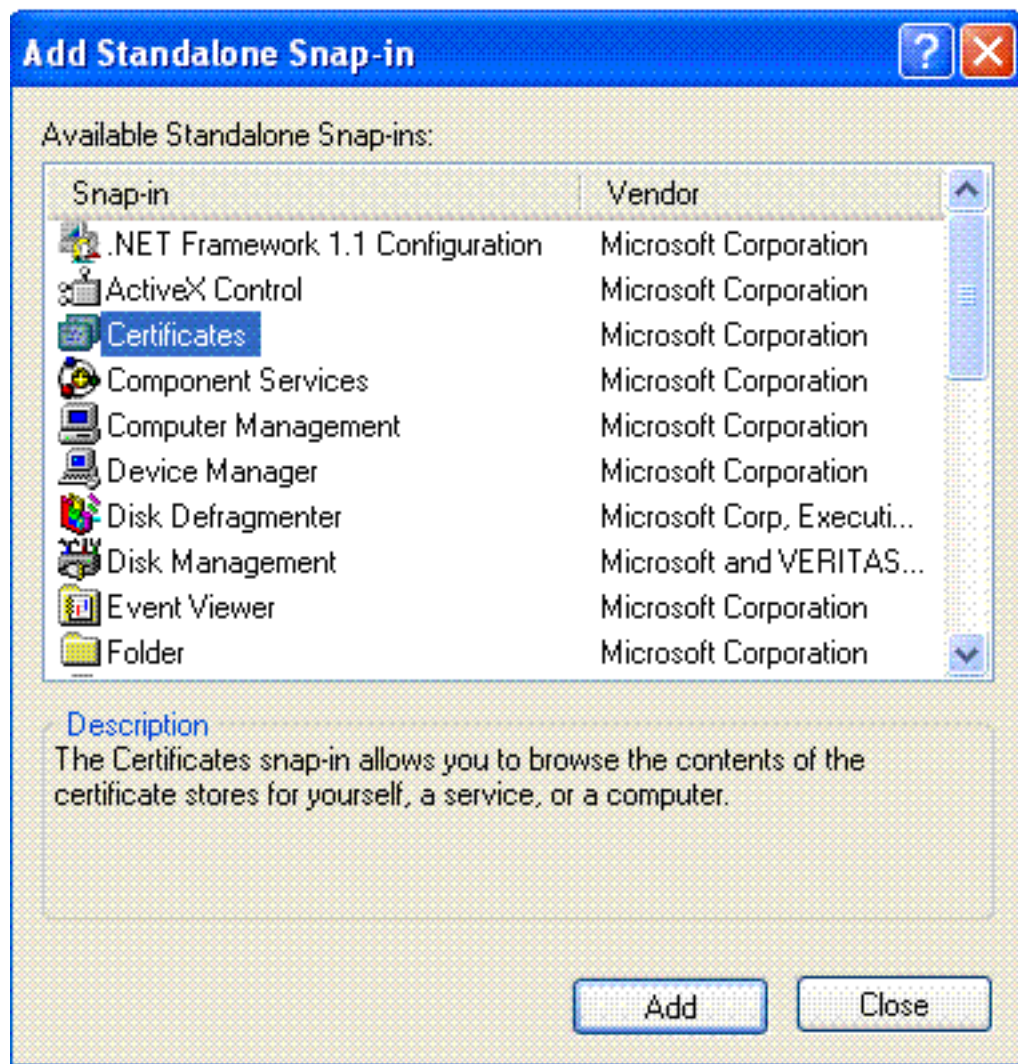


15. 下一步是驗證使用者端是否從伺服器收到CA憑證(信任)。
16. 按一下**Start**；按一下**Run**；鍵入**mmc**，然後按一下**OK**。
17. 按一下**檔案**，然後按一下**新增/刪除管理單元**。

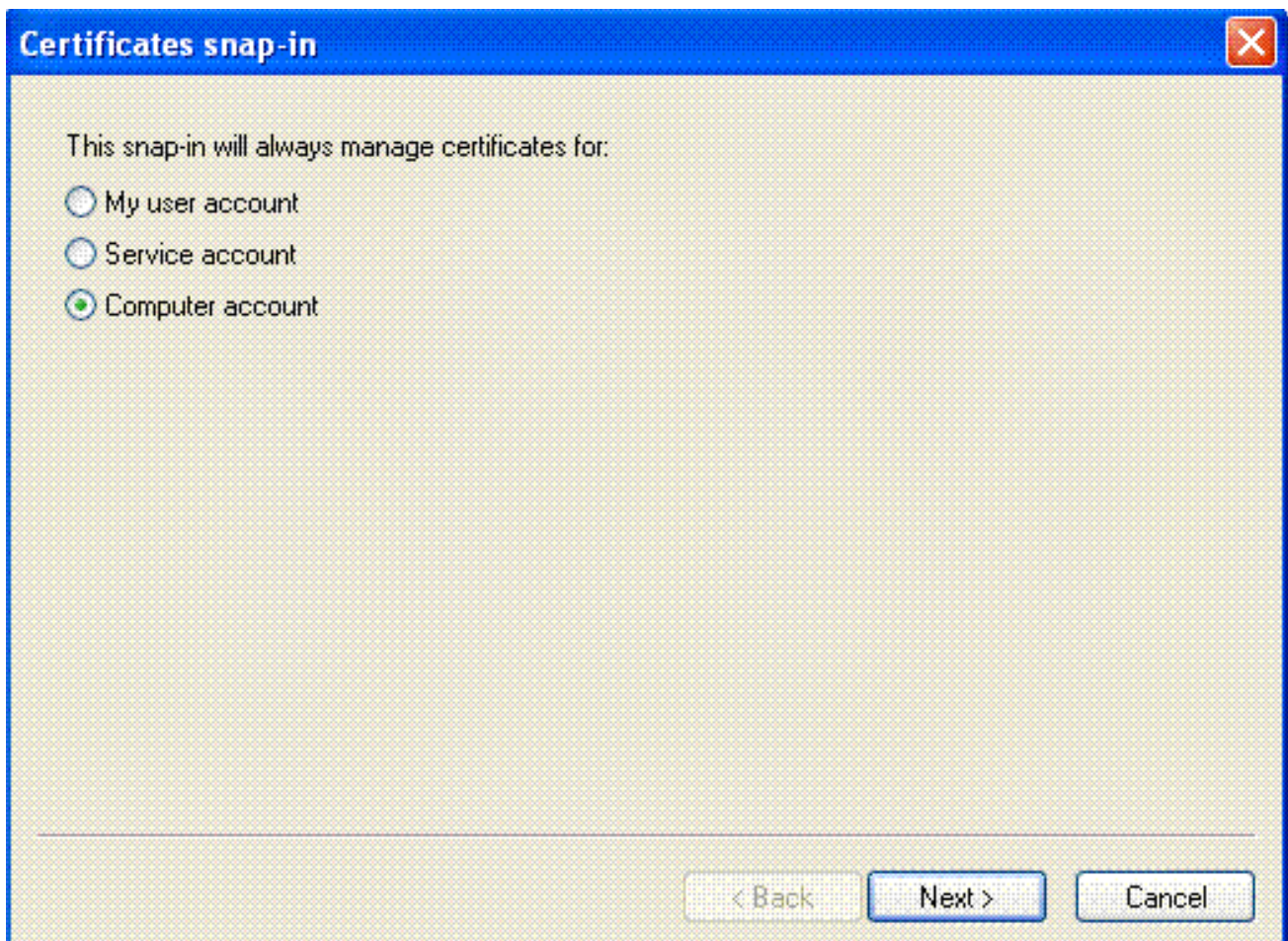


18. 按一下「Add」。

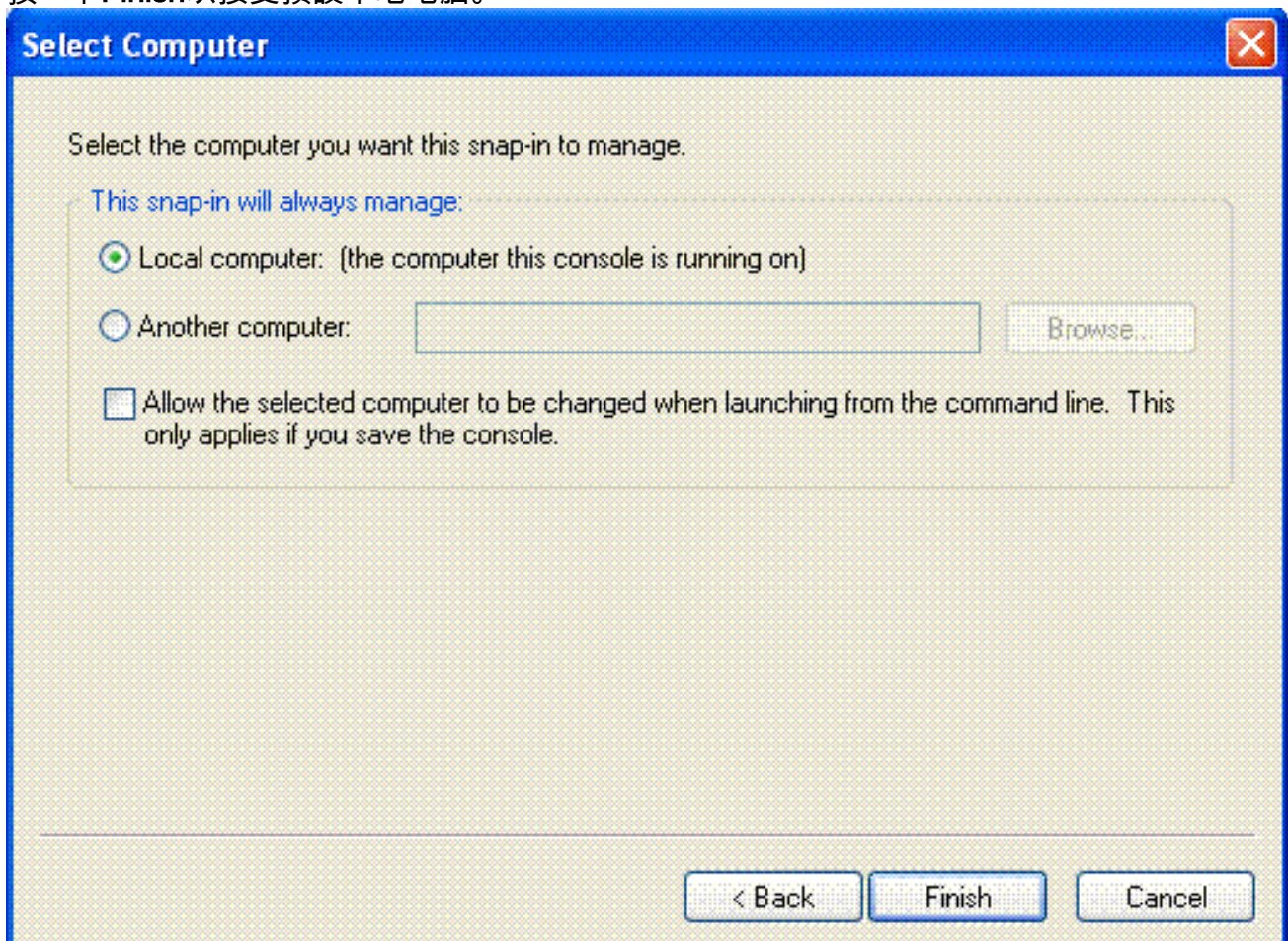
19. 選擇「Certificate」，然後按一下「Add」。



20. 選擇「Computer Account」，然後按一下「Next」。



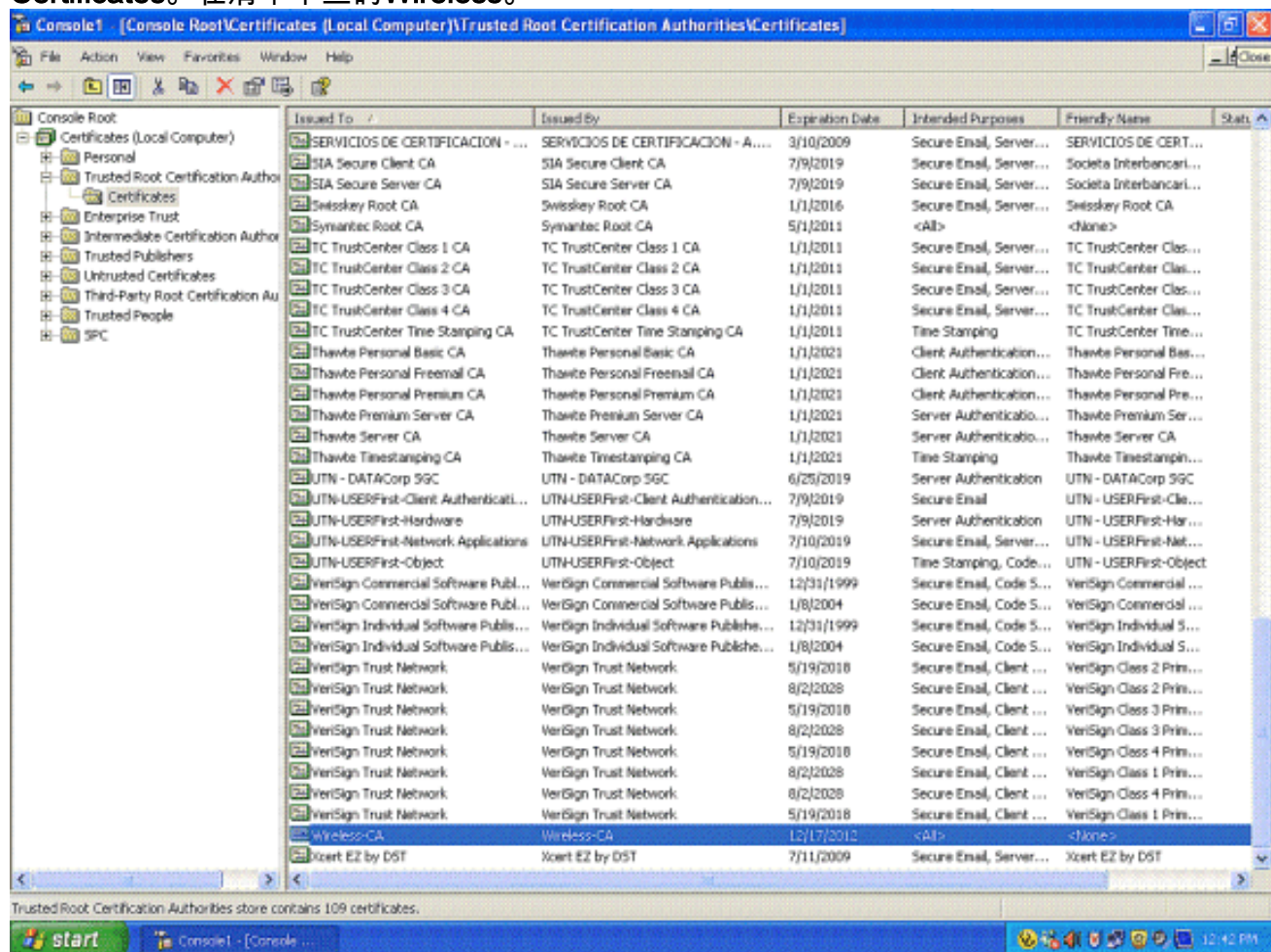
21. 按一下**Finish**以接受預設本地電腦。



22. 按一下「Close」，然後按一下「OK」。

23. 展開**Certificates(Local Computer)**；展開**Trusted Root Certification Authorities**；然後按一下

Certificates。在清單中查詢Wireless。



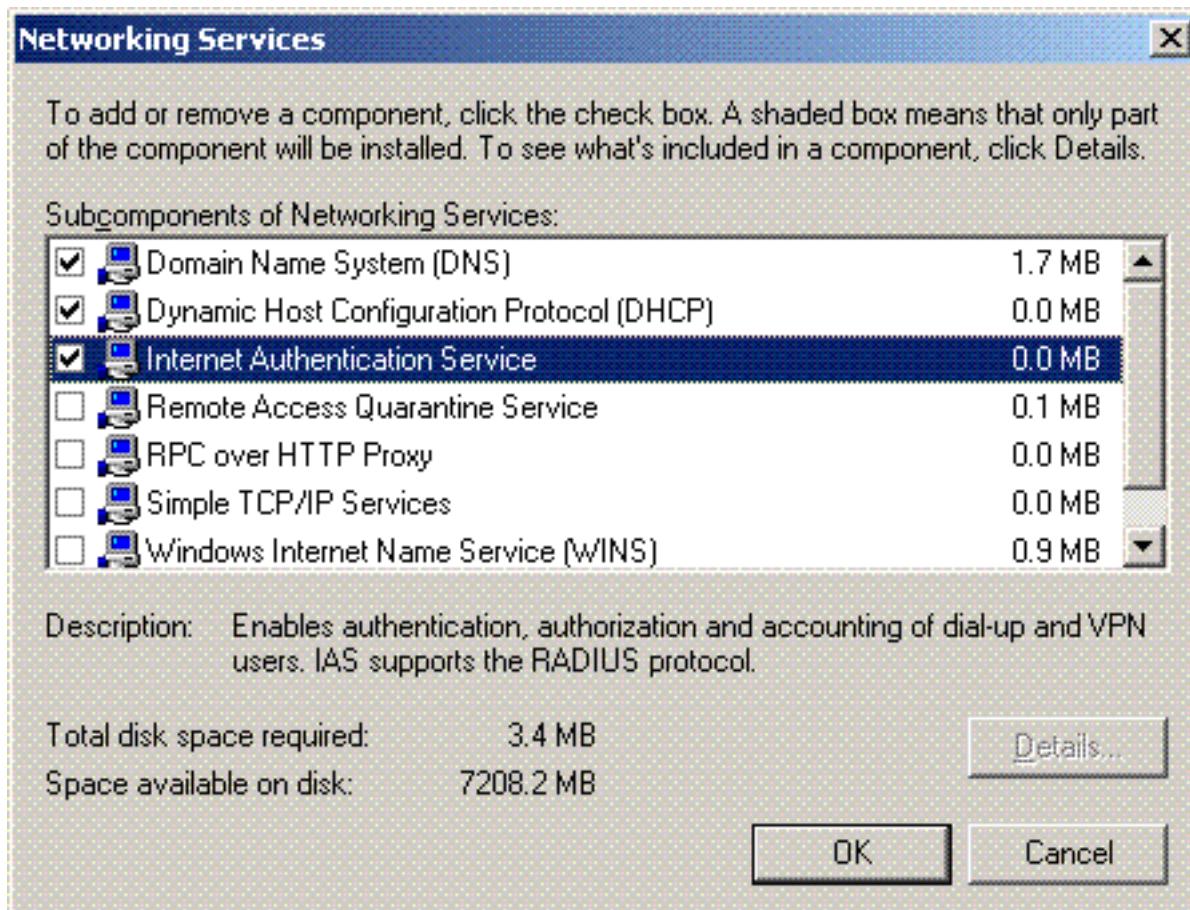
24. 重複此過程，向域中新增更多客戶端。

[在Microsoft Windows 2003 Server上安裝Internet身份驗證服務並請求證書](#)

在此設定中，Internet身份驗證服務(IAS)用作RADIUS伺服器，通過PEAP身份驗證對無線客戶端進行身份驗證。

完成以下步驟，在伺服器上安裝和配置IAS。

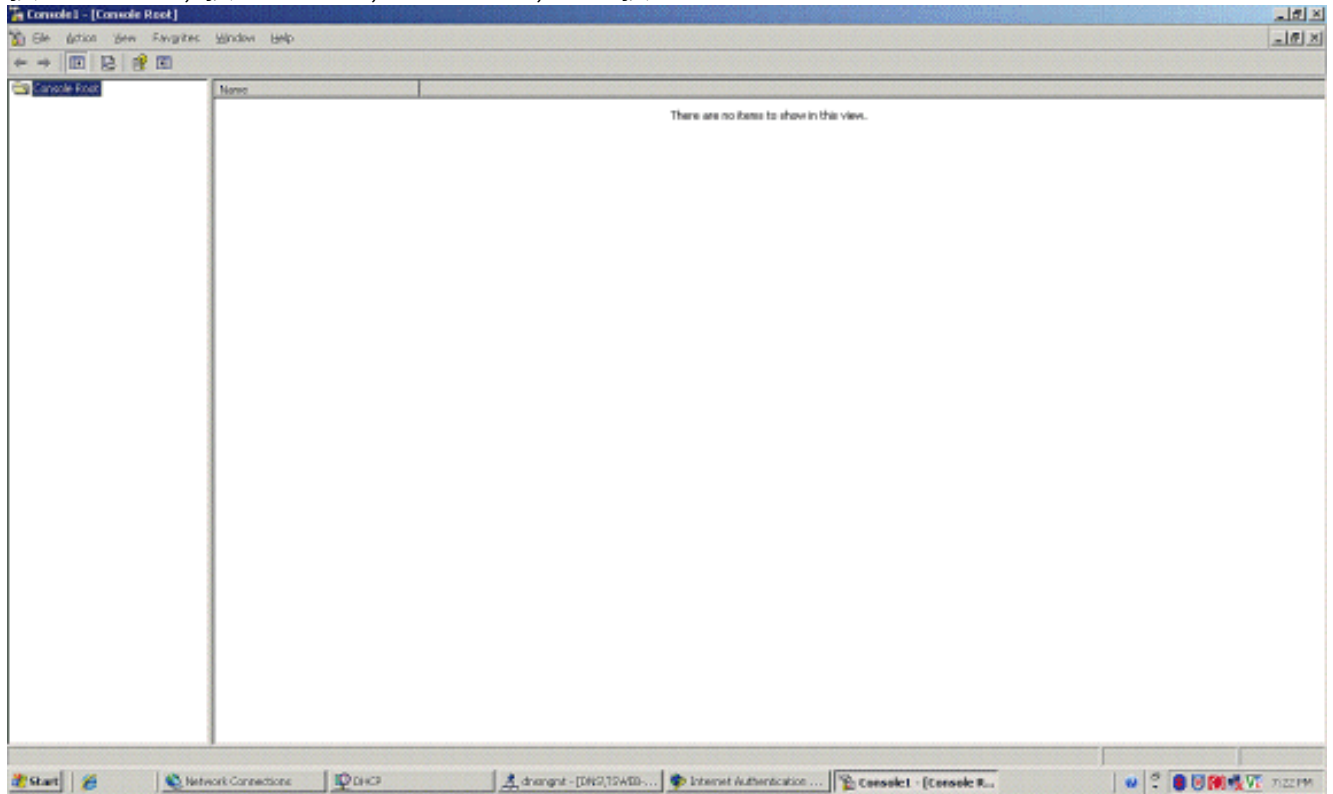
1. 在「Control Panel (控制面板)」中按一下Add or Remove Programs。
2. 按一下Add/Remove Windows Components。
3. 選擇Networking Services，然後按一下Details。
4. 選擇Internet Authentication Service；按一下OK；然後按一下Next。



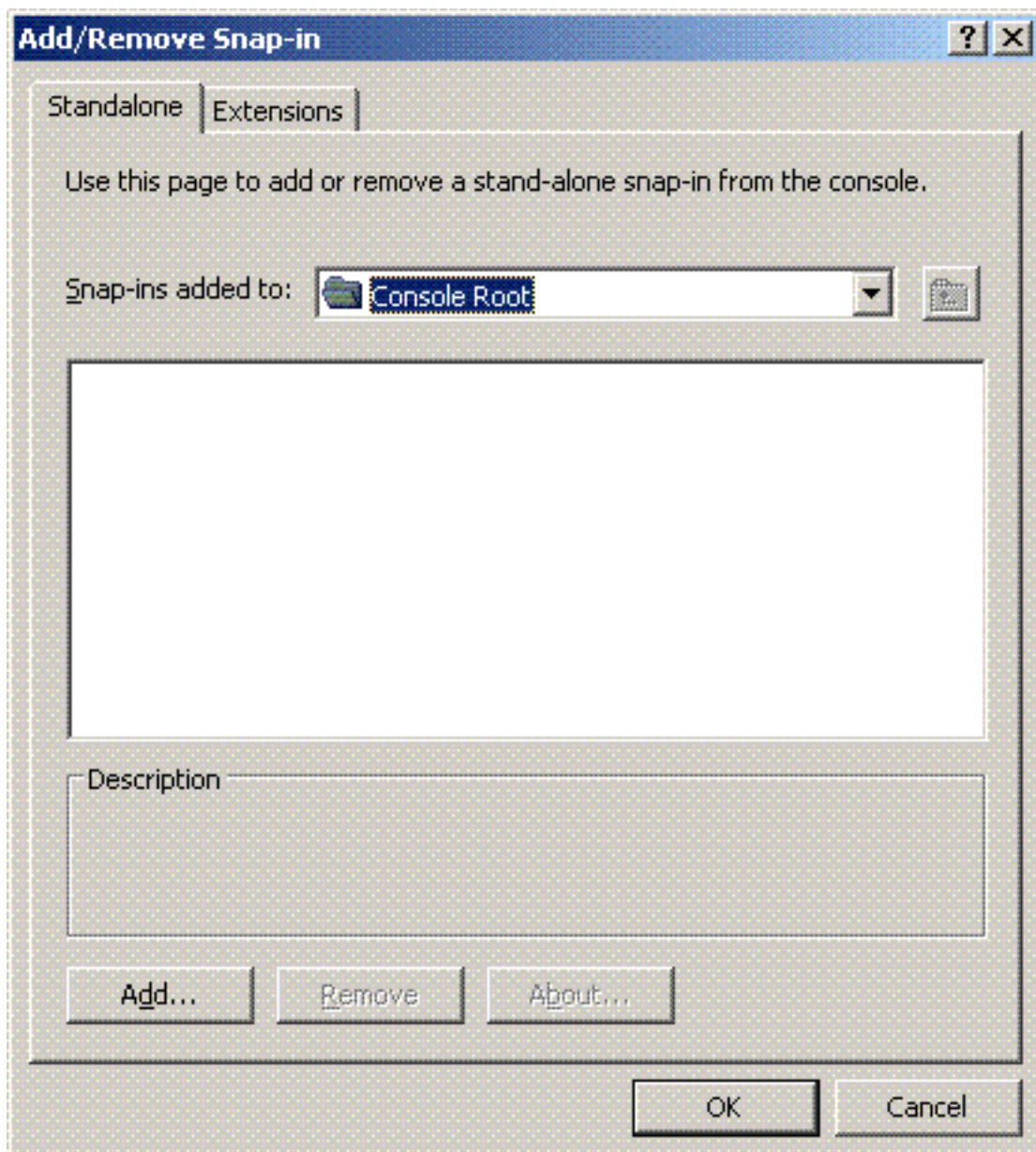
5. 按一下**Finish**完成IAS安裝。



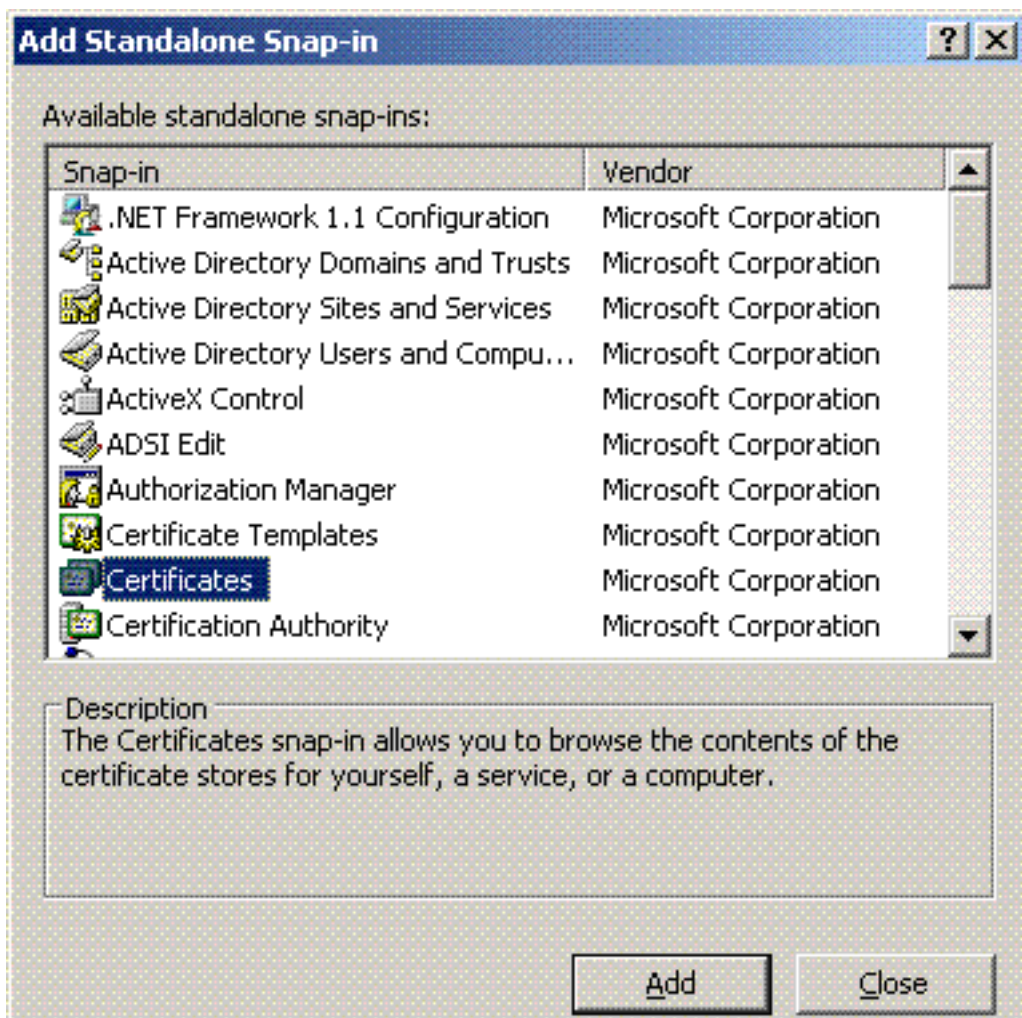
6. 下一步是安裝Internet身份驗證服務(IAS)的電腦證書。
7. 按一下**Start**；按一下**Run**；鍵入**mmc**；然後按一下**OK**。



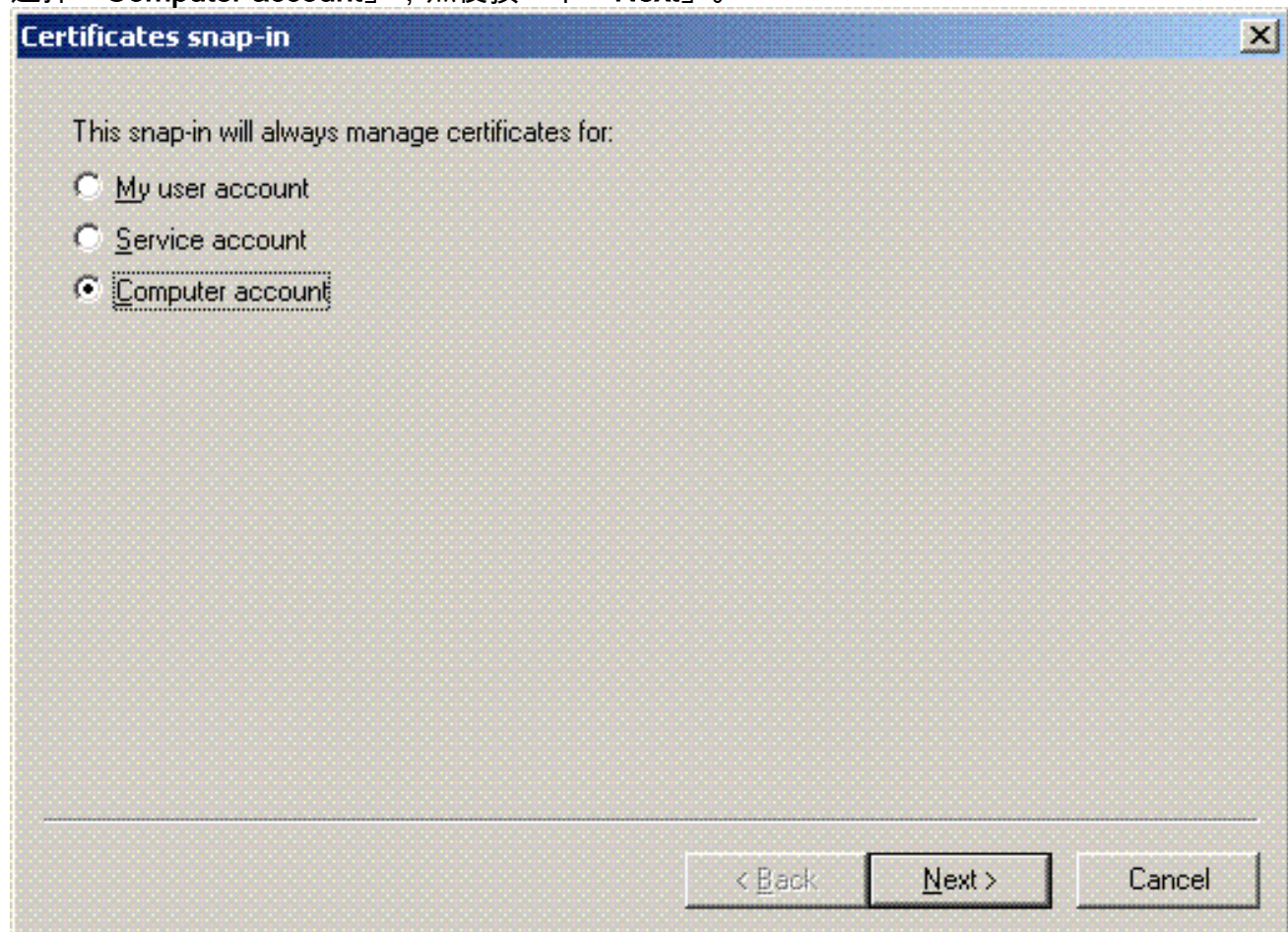
8. 在「檔案」選單中按一下**Console**，然後選擇**Add/Remove**管理單元。
9. 按一下**Add**以新增管理單元。



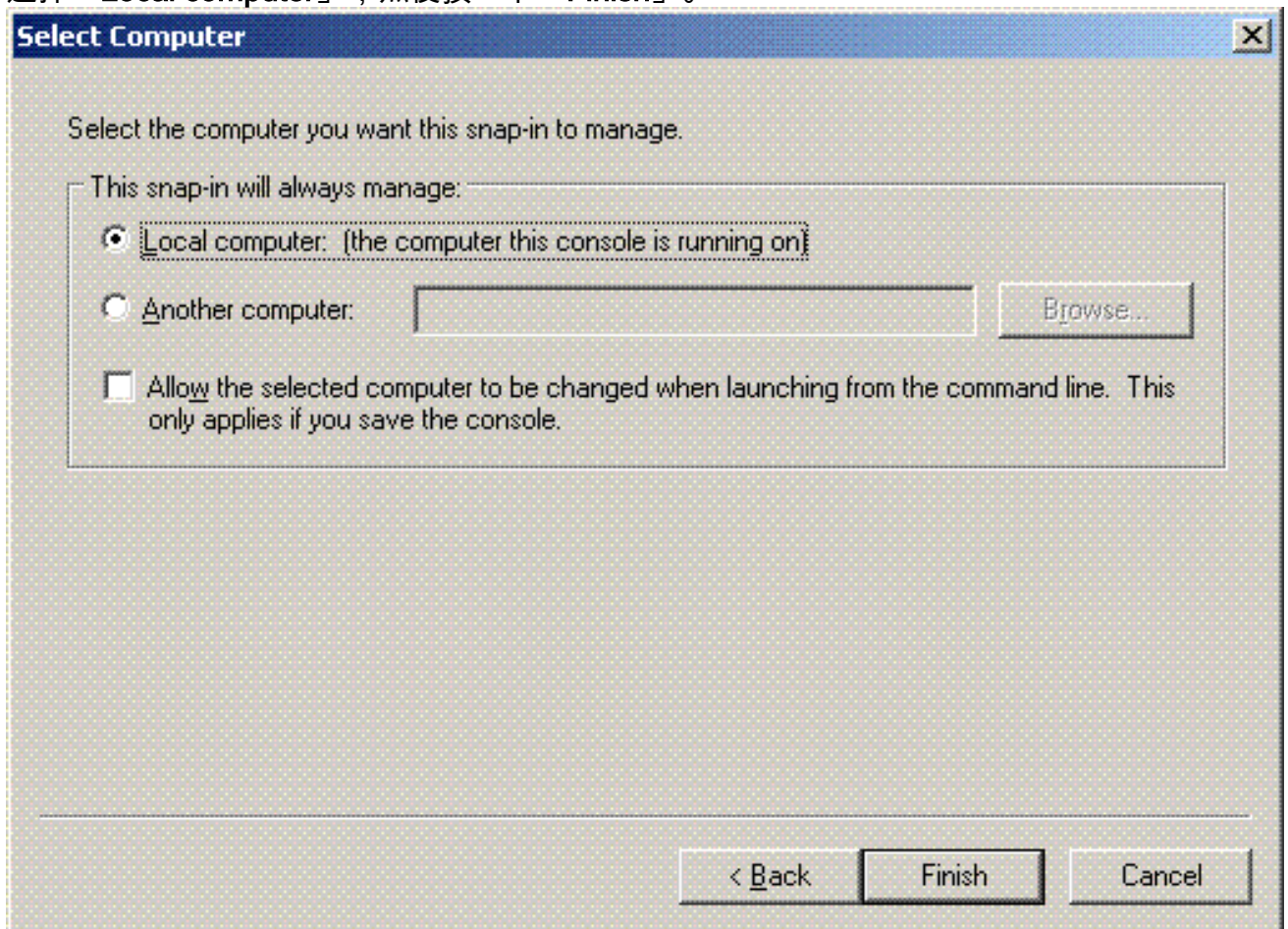
10. 從管理單元清單中選擇**Certificates**，然後按一下**Add**。



11. 選擇「Computer account」，然後按一下「Next」。

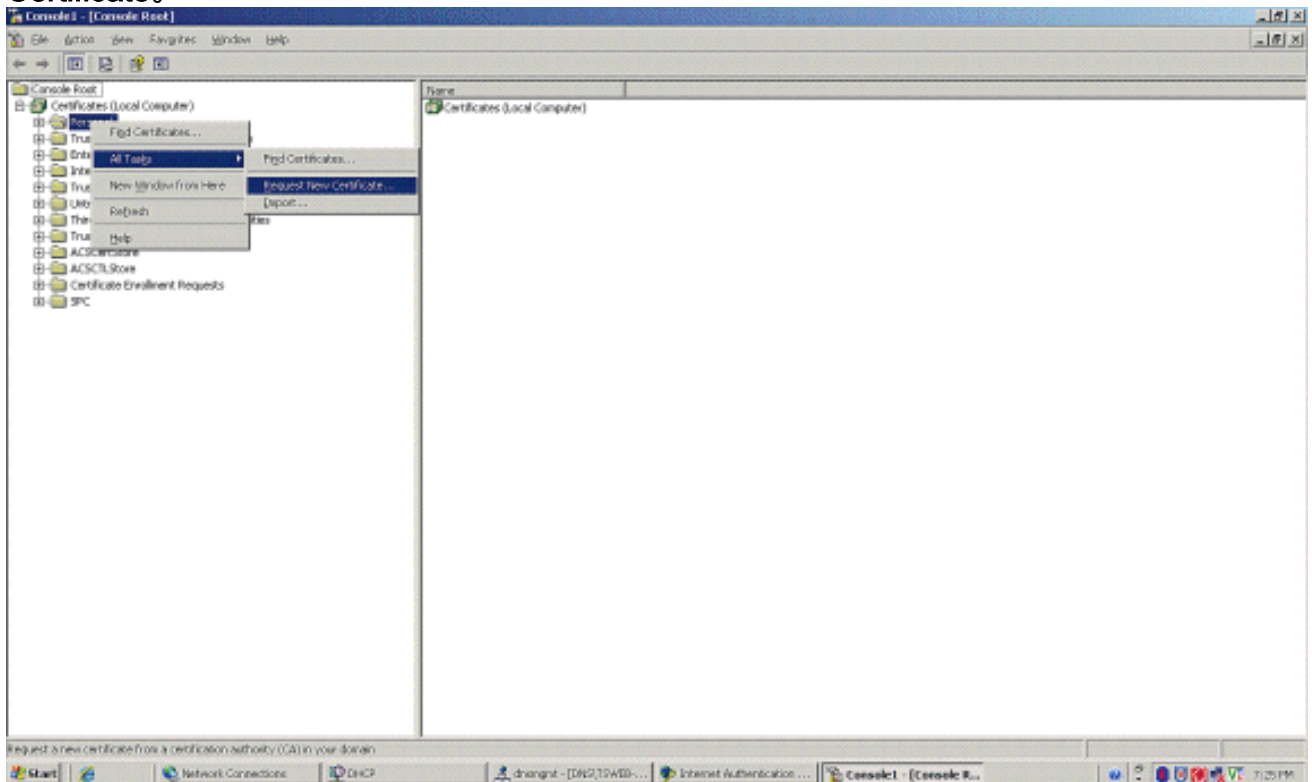


12. 選擇「Local computer」，然後按一下「Finish」。



13. 按一下「Close」，然後按一下「OK」。

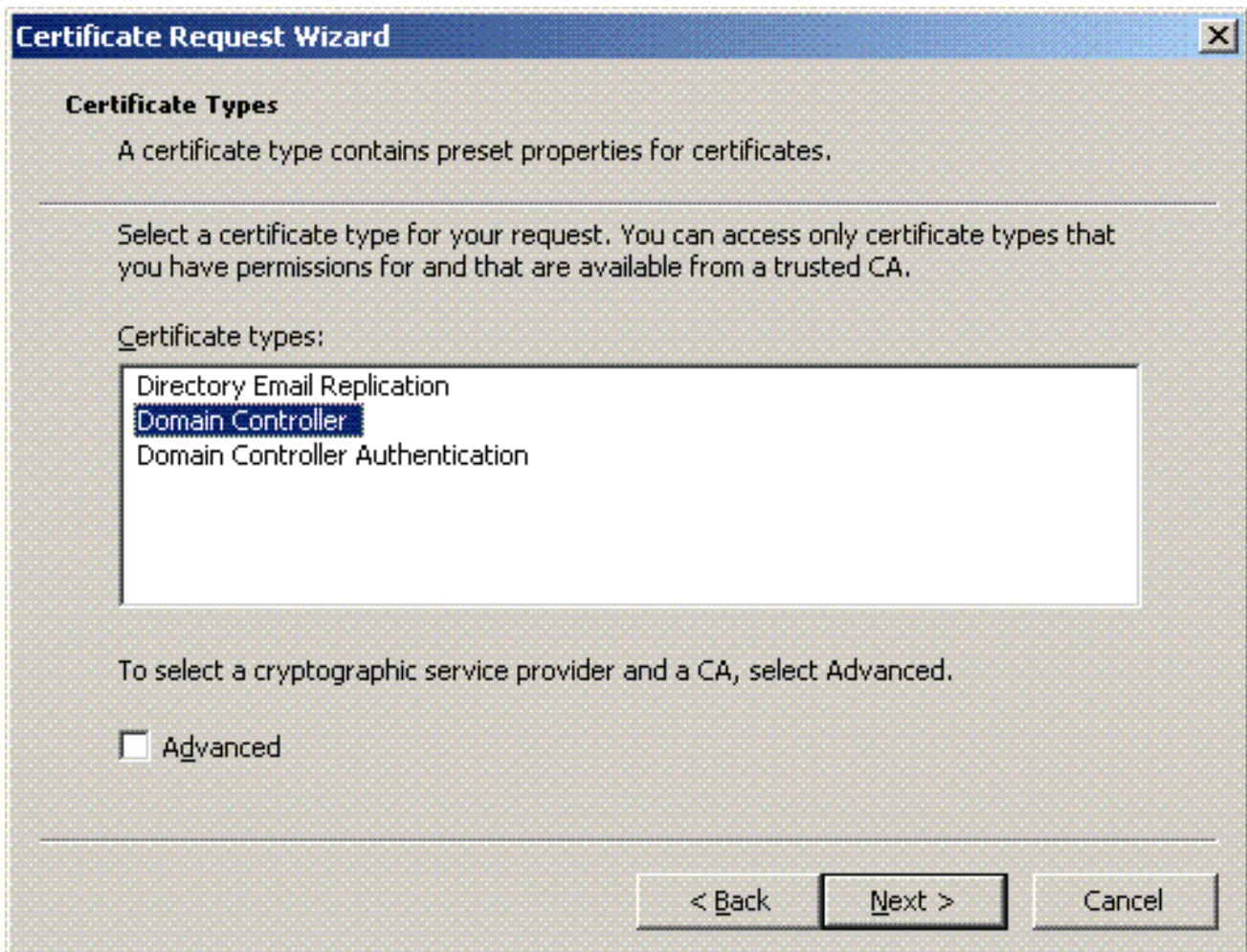
14. 展開證書 (本地電腦)；按一下右鍵Personal資料夾；選擇All tasks，然後選擇Request New Certificate。



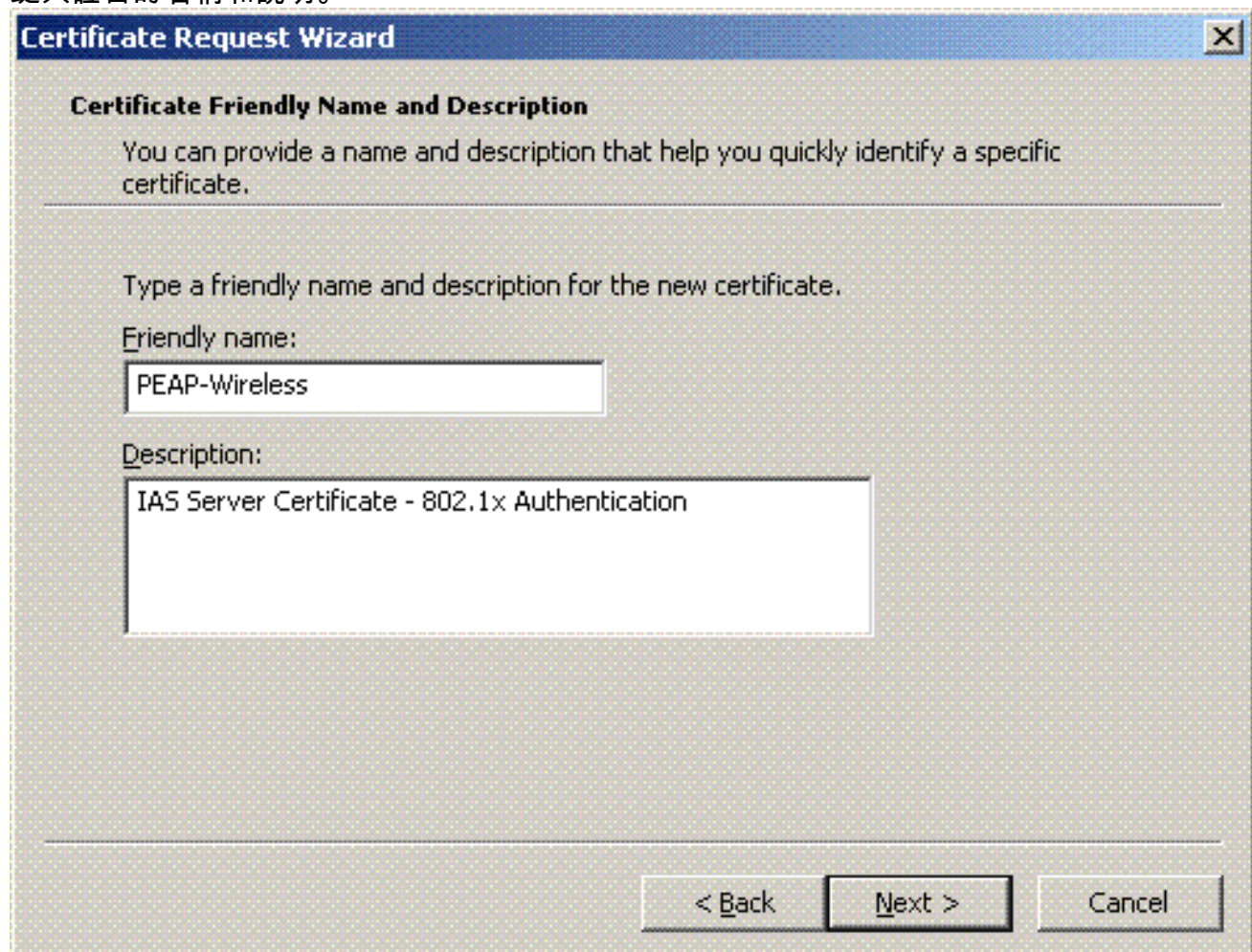
15. 在「Welcome to the Certificate Request Wizard」上按一下Next。



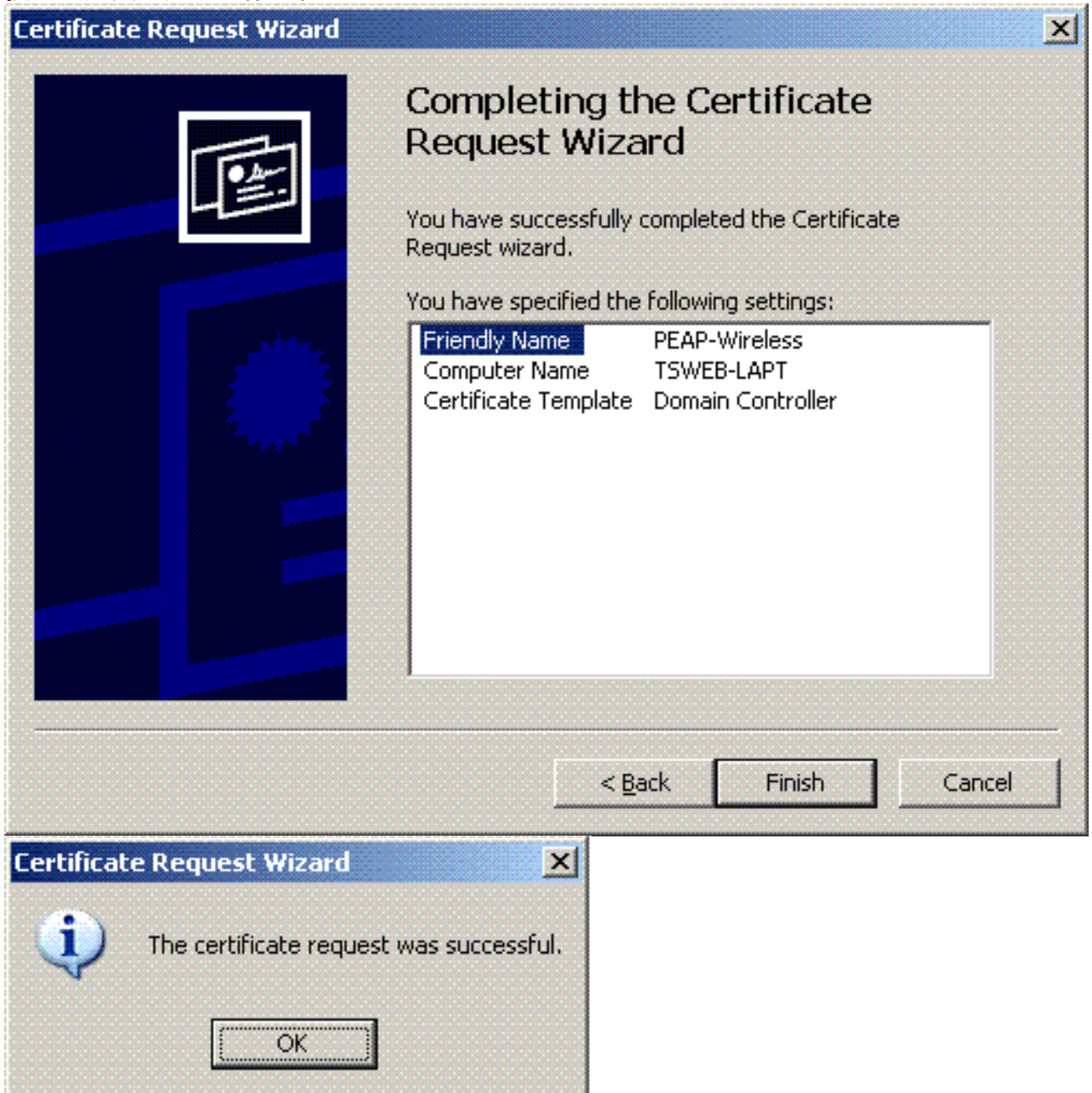
16. 選擇Domain Controller certificate模板(如果您請求非DC伺服器上的電腦證書，請選擇Computer證書模板)，然後按一下Next。



17. 鍵入證書的名稱和說明。



18. 按一下**完成**完成認證請求嚮導。

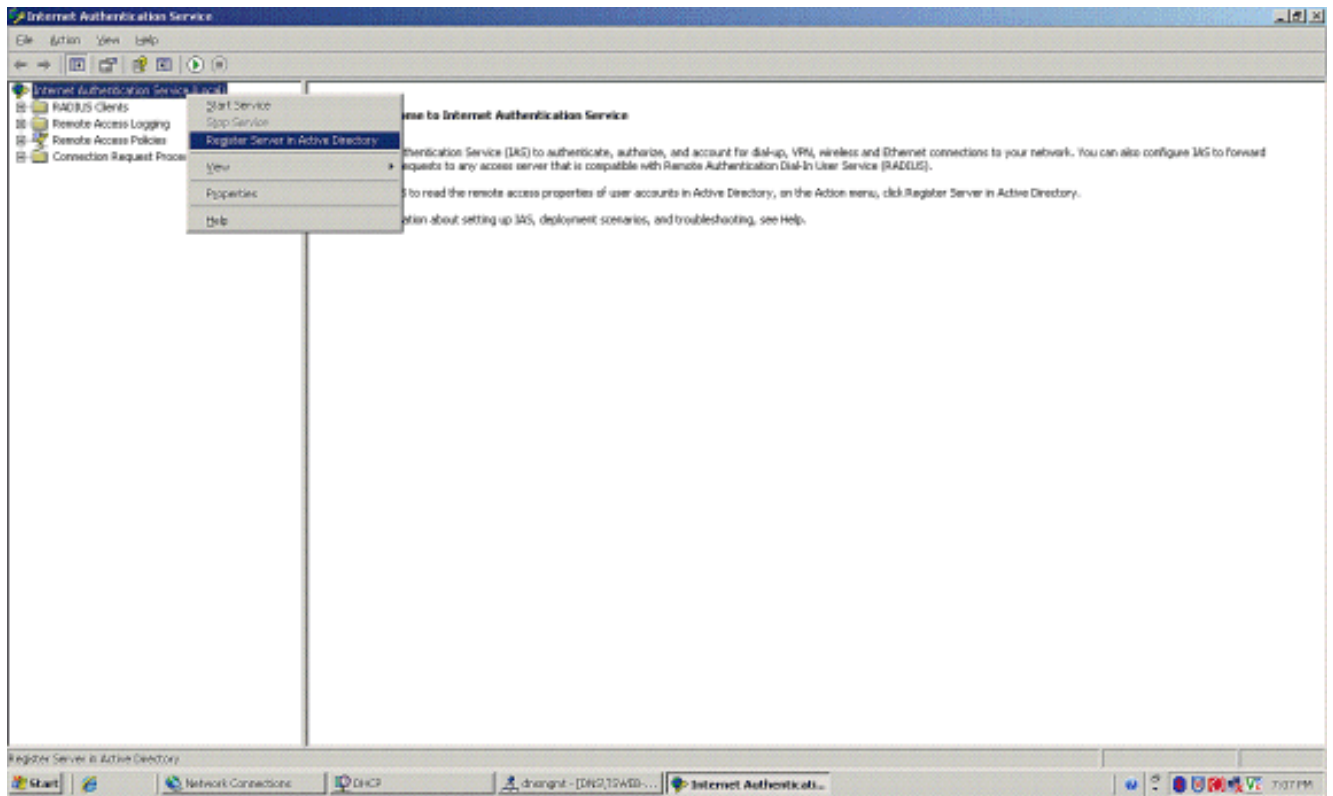


[為PEAP-MS-CHAP v2身份驗證配置Internet身份驗證服務](#)

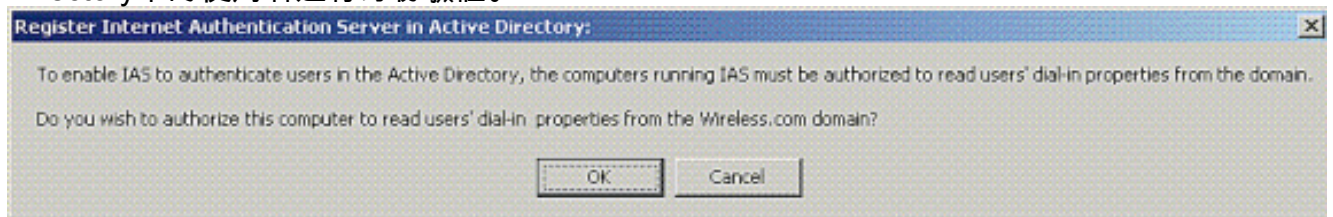
現在您已安裝並請求了IAS的證書，請配置IAS進行身份驗證。

請完成以下步驟：

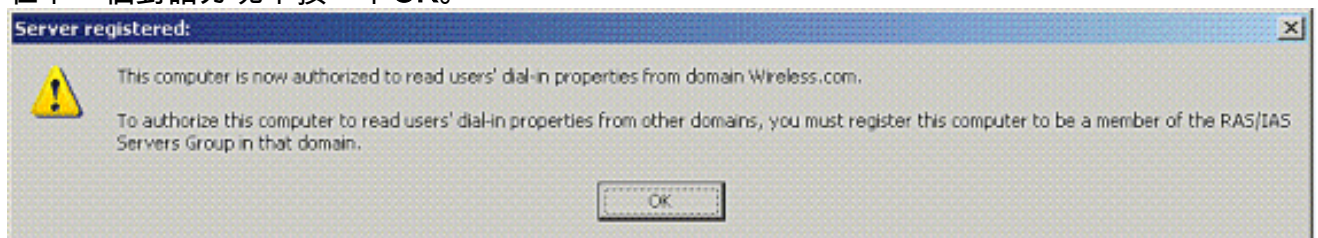
1. 按一下**Start > Programs > Administrative Tools**，然後按一下**Internet Authentication Service**管理單元。
2. 按一下右鍵**Internet身份驗證服務(IAS)**，然後按一下**Register Service in Active Directory**。



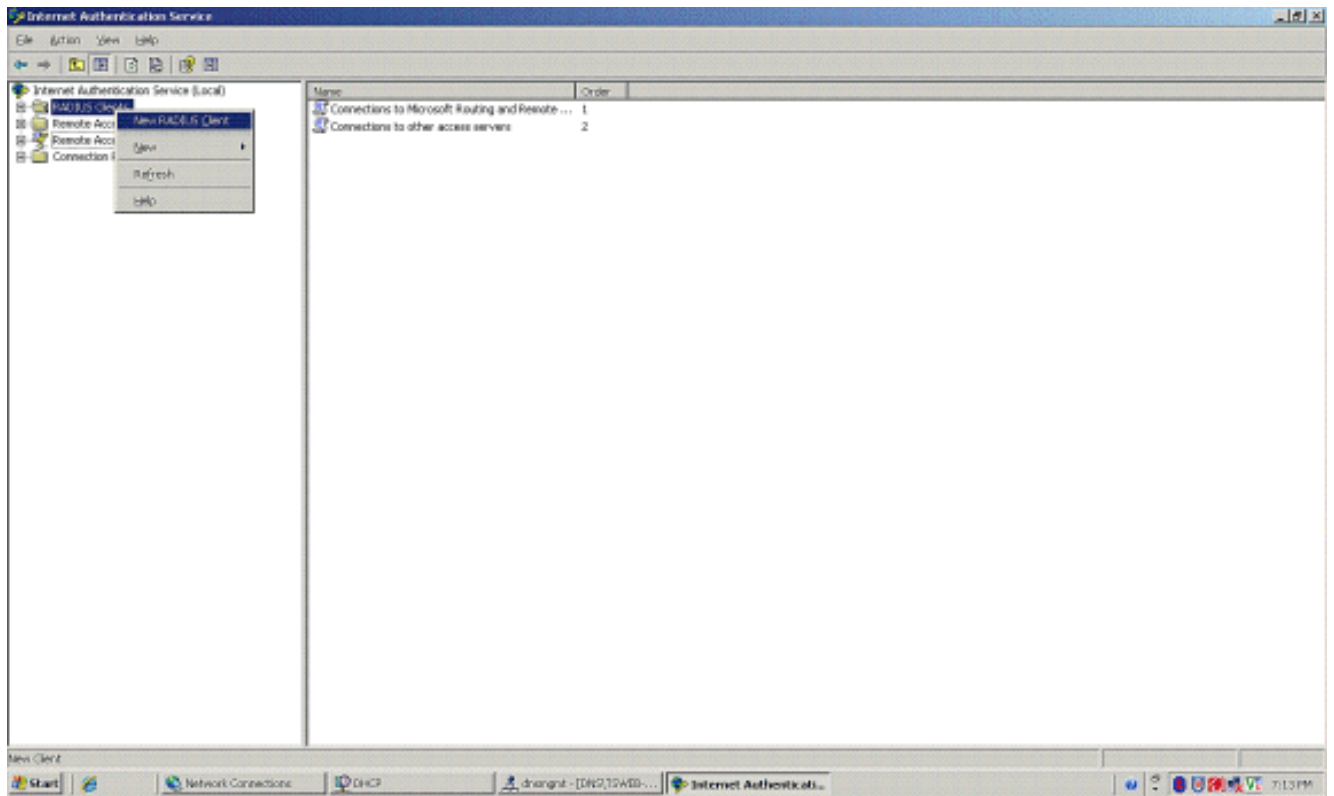
3. 出現「Register Internet Authentication Service in Active Directory(在Active Directory中註冊Internet身份驗證服務)」對話方塊；按一下「OK (確定)」。這使得IAS能夠對Active Directory中的使用者進行身份驗證。



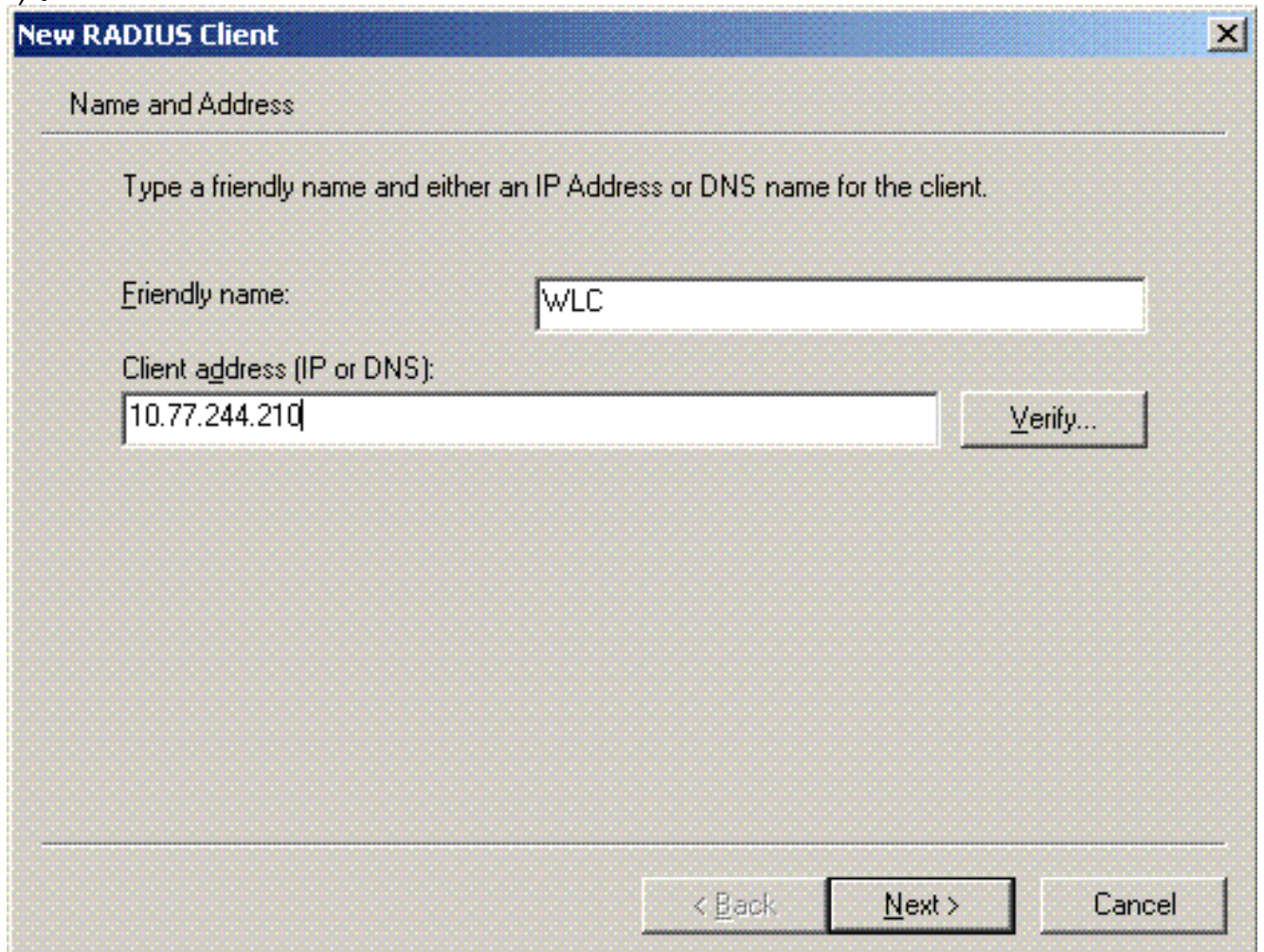
4. 在下一個對話方塊中按一下OK。



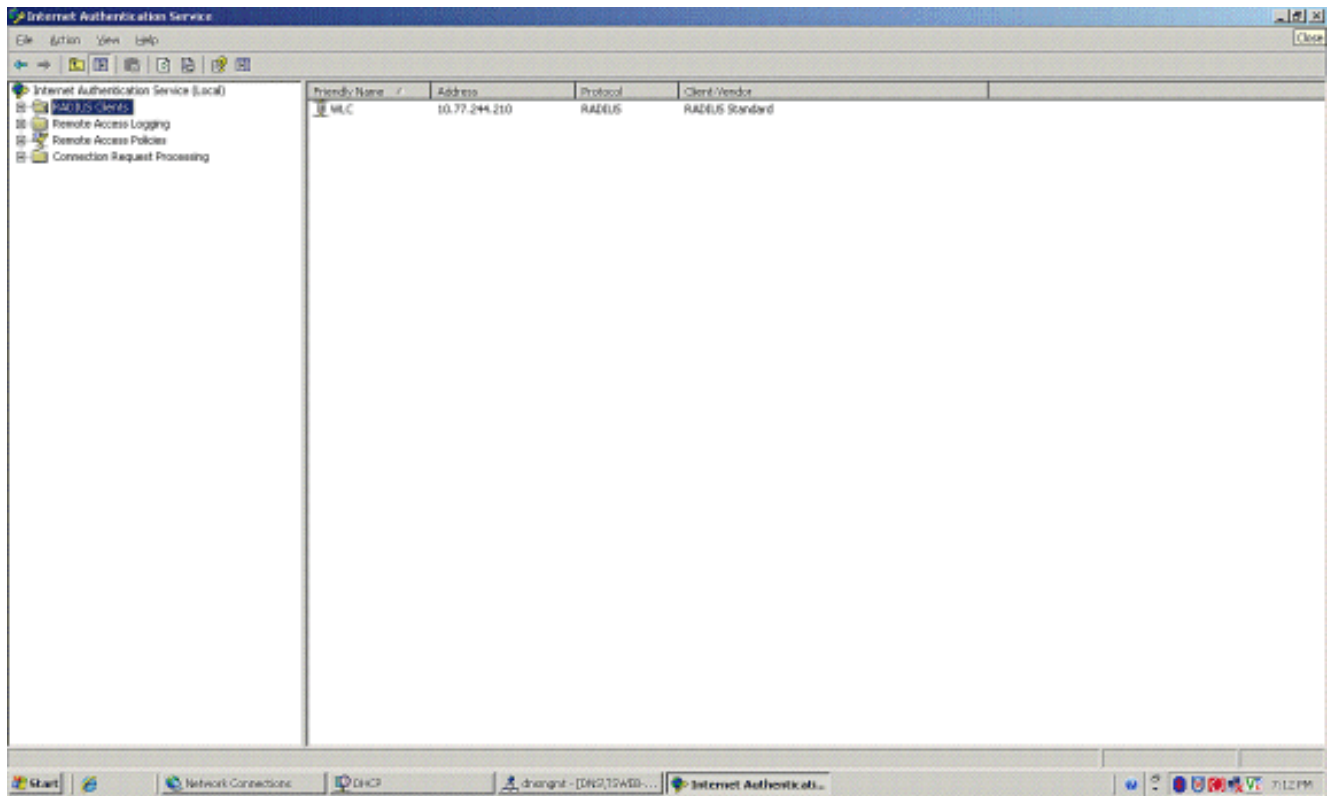
5. 將無線區域網控制器新增為MS IAS伺服器上的AAA客戶端。
6. 按一下右鍵RADIUS Clients，然後選擇New RADIUS Client。



7. 輸入使用者端的名稱（在此案例中為WLC），並輸入WLC的IP位址。按「Next」（下一步）。

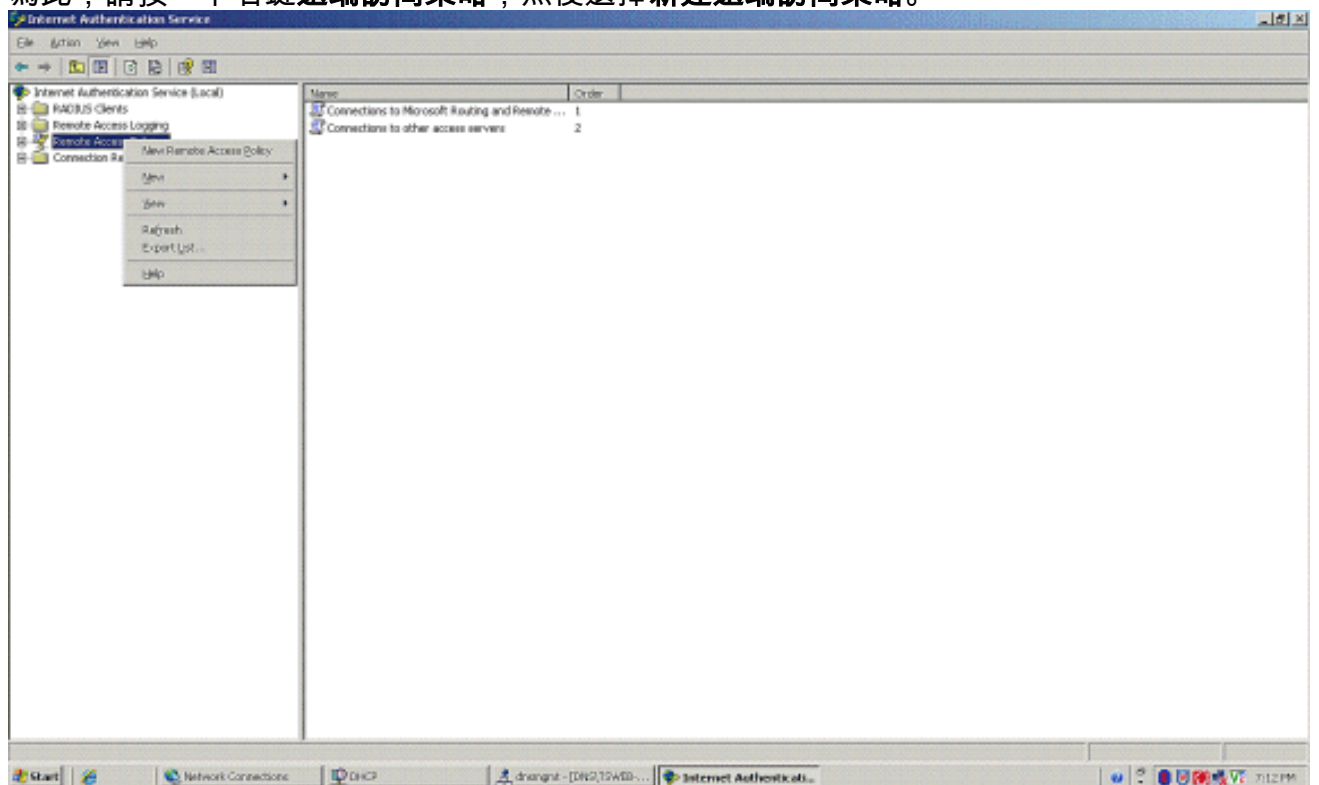


8. 在下一頁的Client-Vendor下，選擇**RADIUS Standard**；輸入共用金鑰；然後點選**Finish**。
9. 請注意，WLC作為AAA客戶端新增到IAS中。



10. 為客戶端建立遠端訪問策略。

11. 為此，請按一下右鍵遠端訪問策略，然後選擇新建遠端訪問策略。




12. 鍵入遠端訪問策略的名稱。在本示例中，使用名稱PEAP。然後點選下一步。

New Remote Access Policy Wizard [X]

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

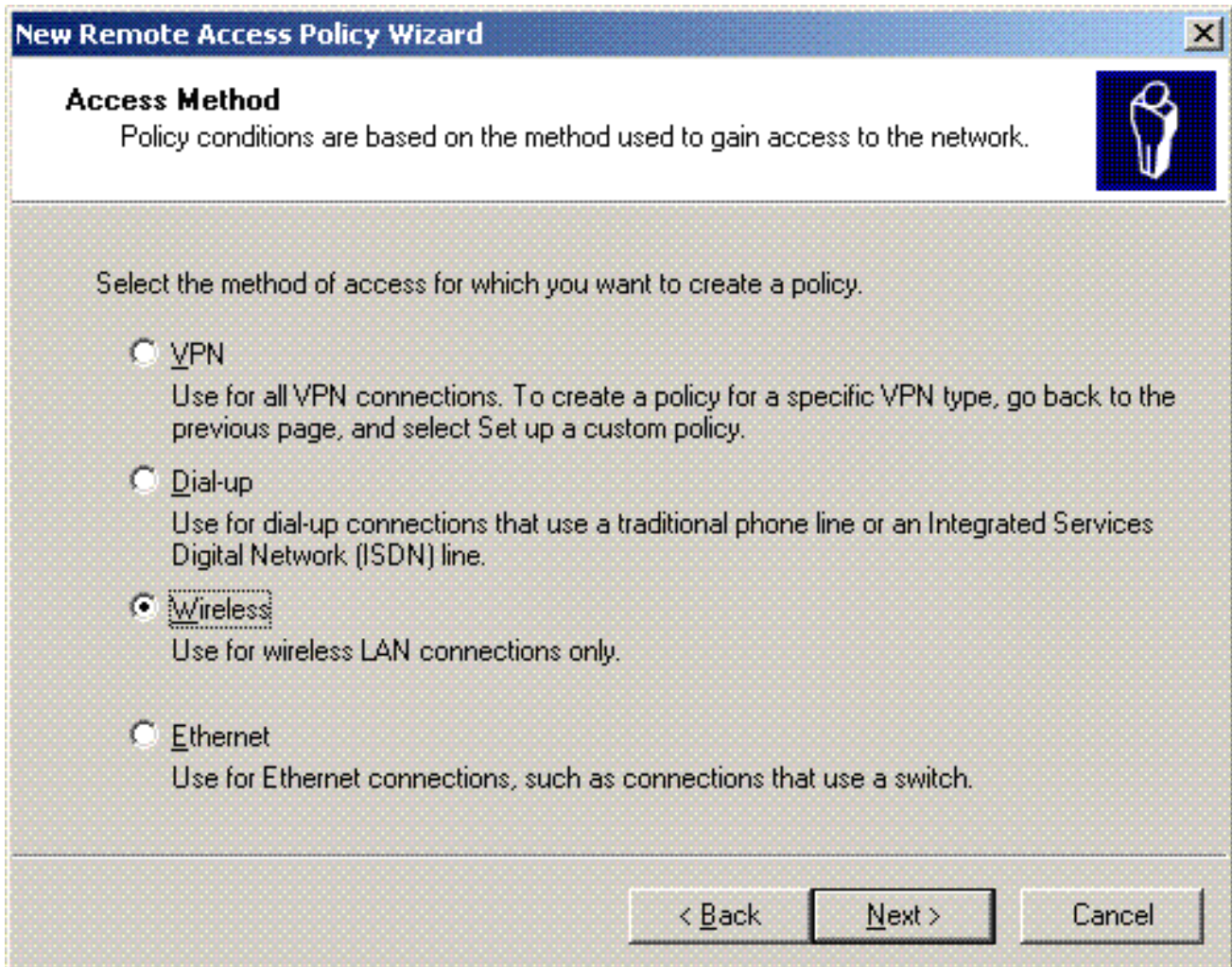
Type a name that describes this policy.

Policy name:

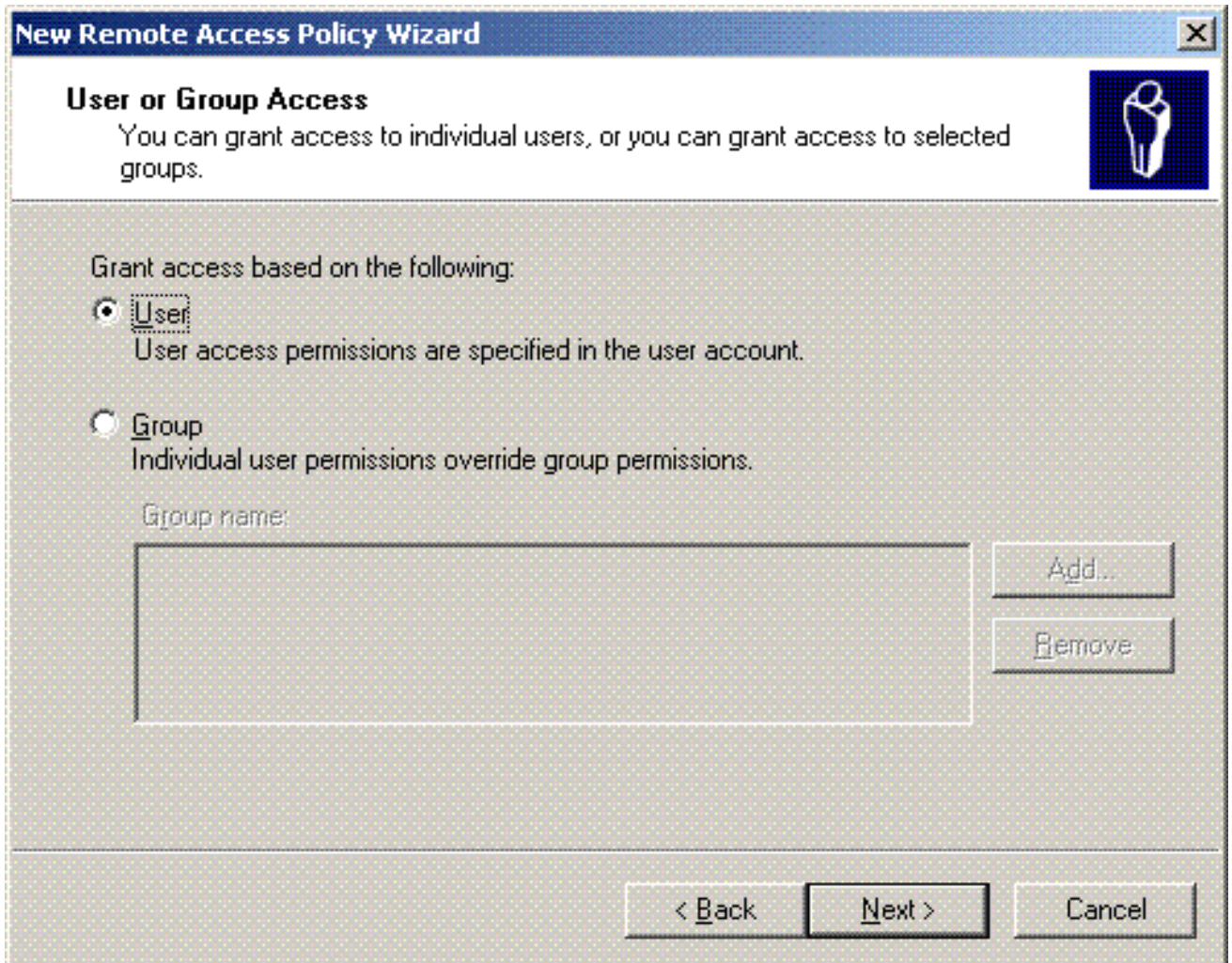
Example: Authenticate all VPN connections.

< Back Next > Cancel

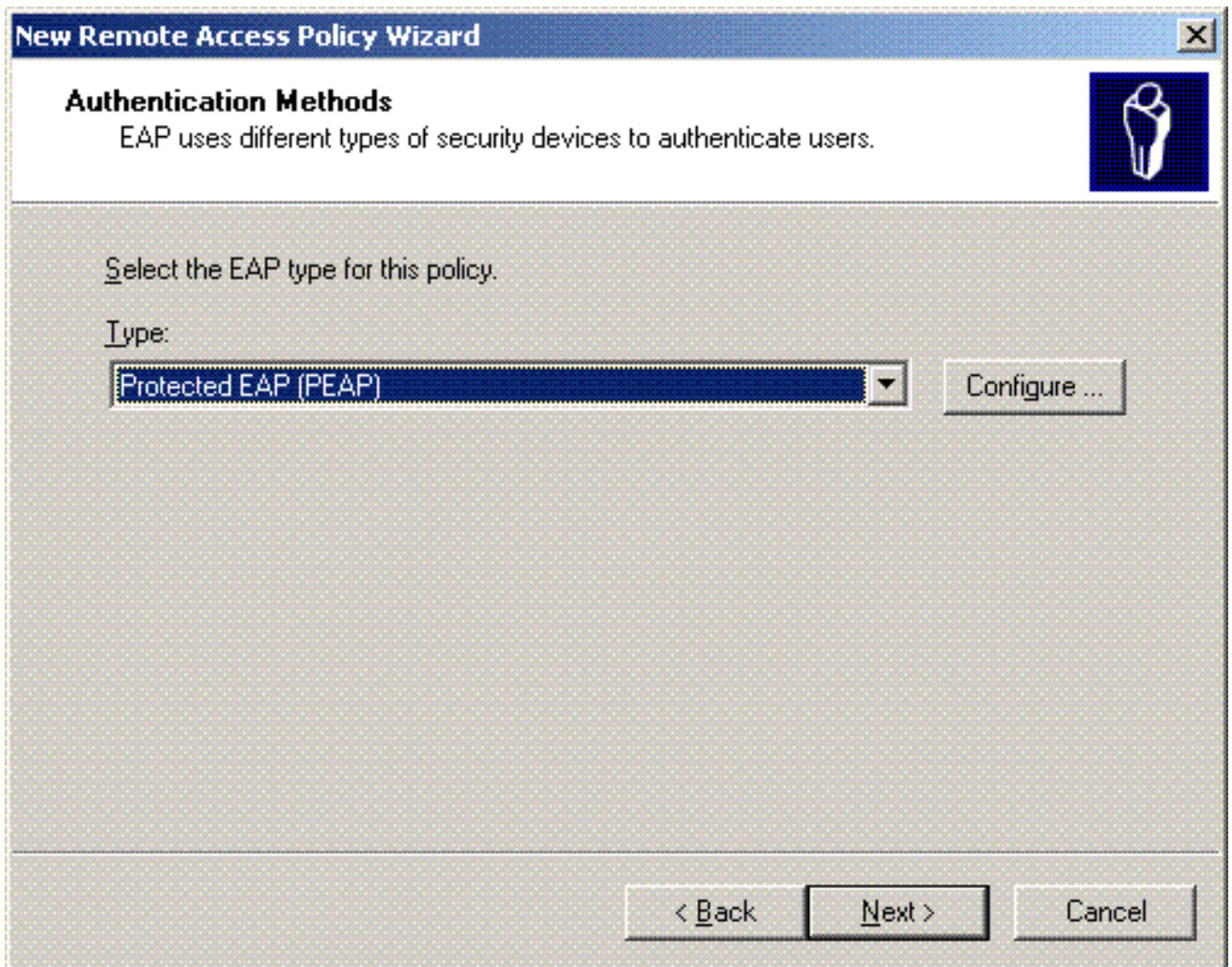
13. 根據您的需求選擇策略屬性。在本例中，選擇**Wireless**。



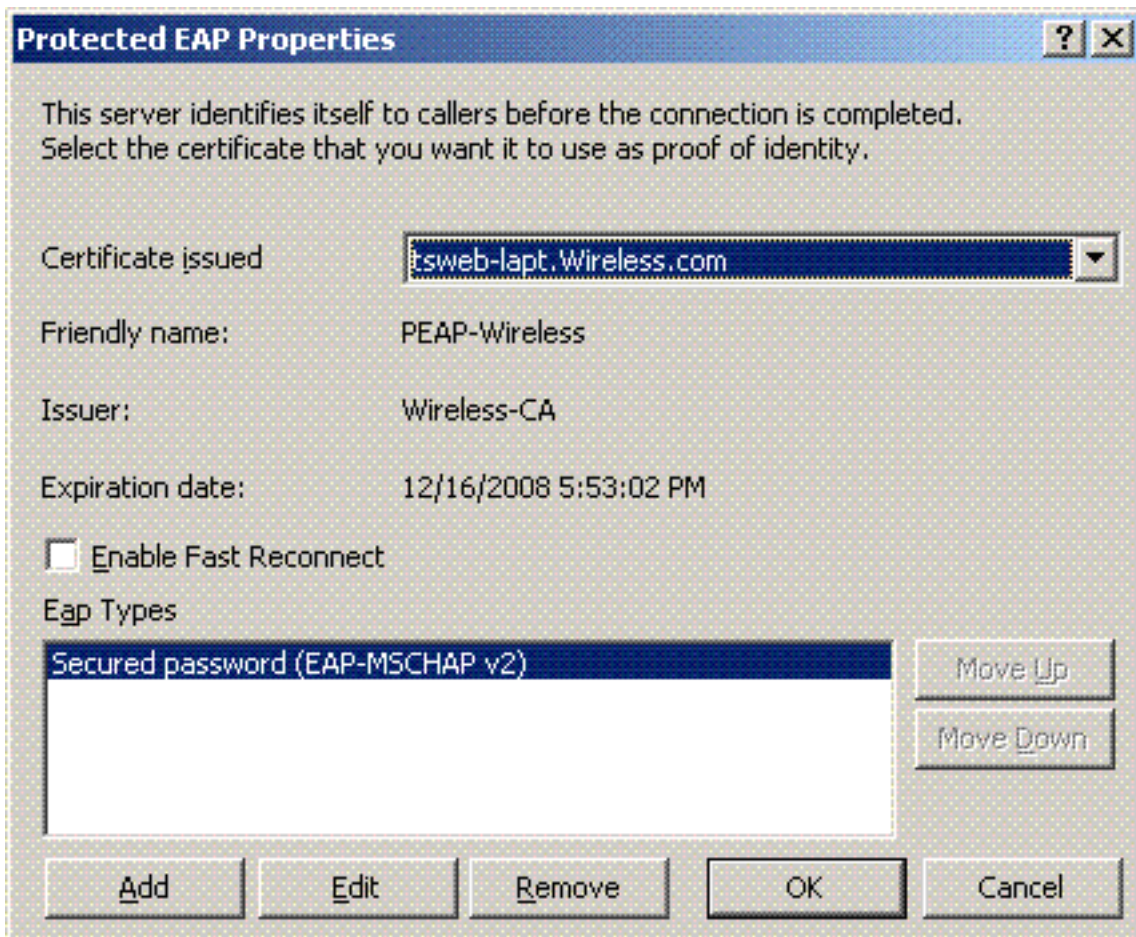
14. 在下一頁上，選擇**User**，將此遠端訪問策略應用到使用者清單。



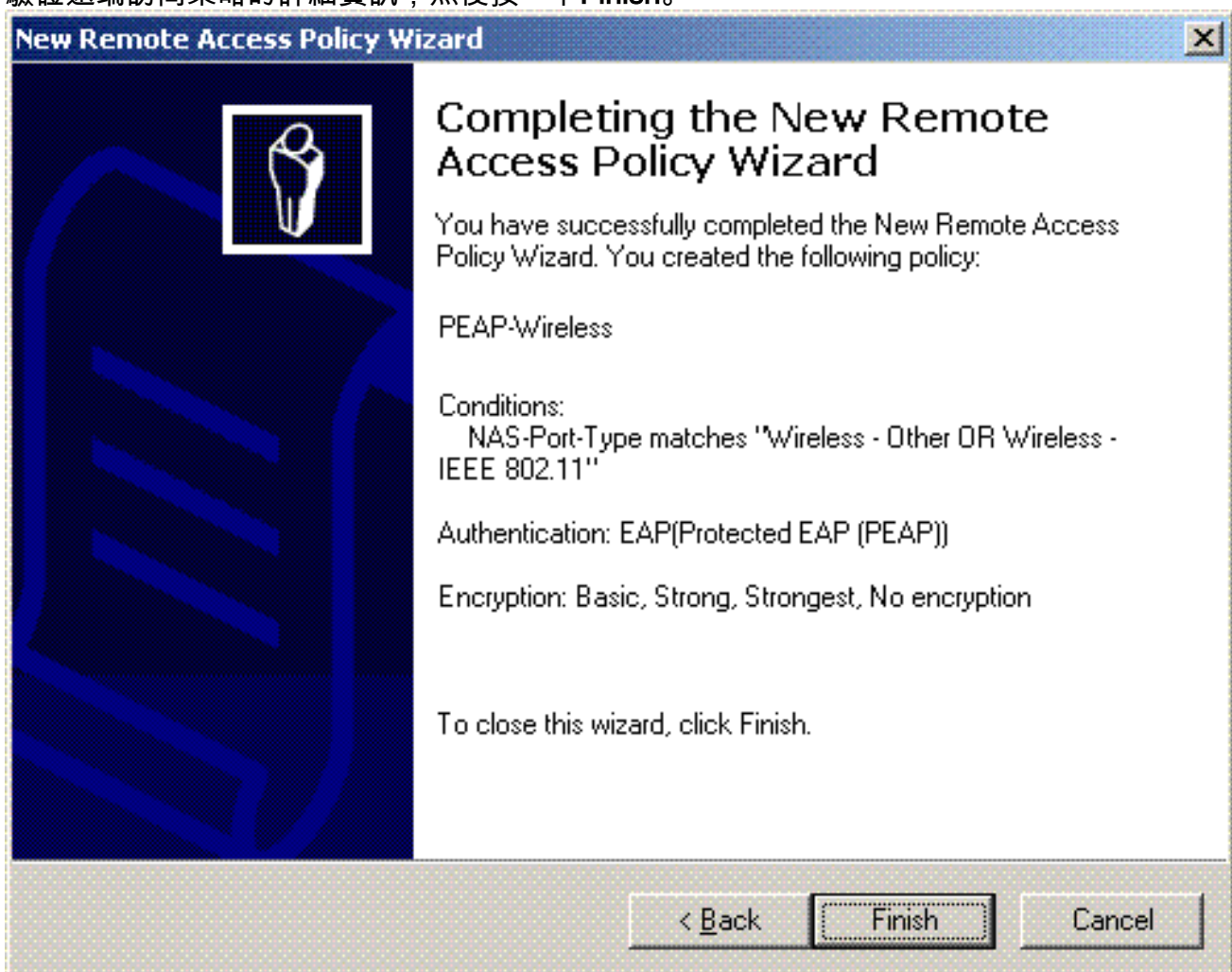
15. 在Authentication Methods下，選擇Protected EAP(PEAP)，然後按一下Configure。



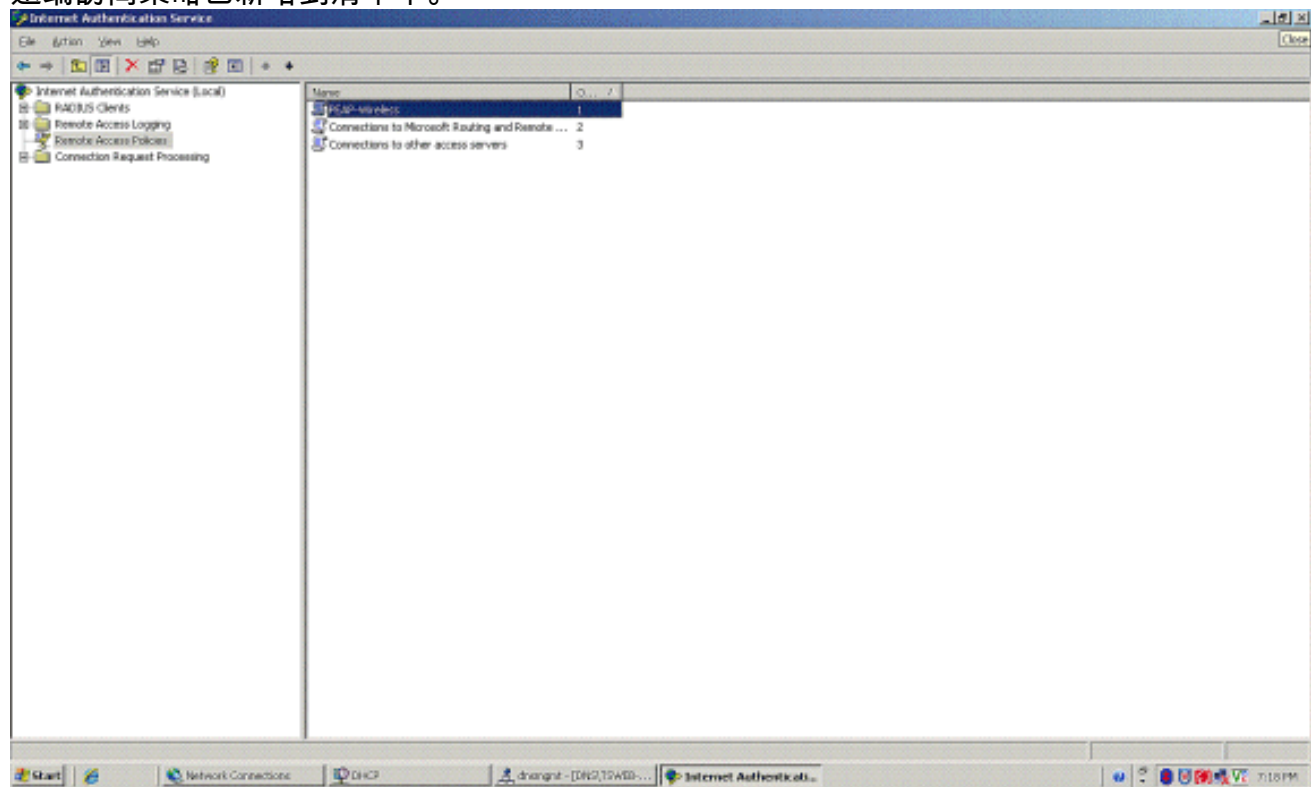
16. 在Protected EAP Properties頁面上，從Certificate Issued下拉選單中選擇適當的證書，然後按一下OK。



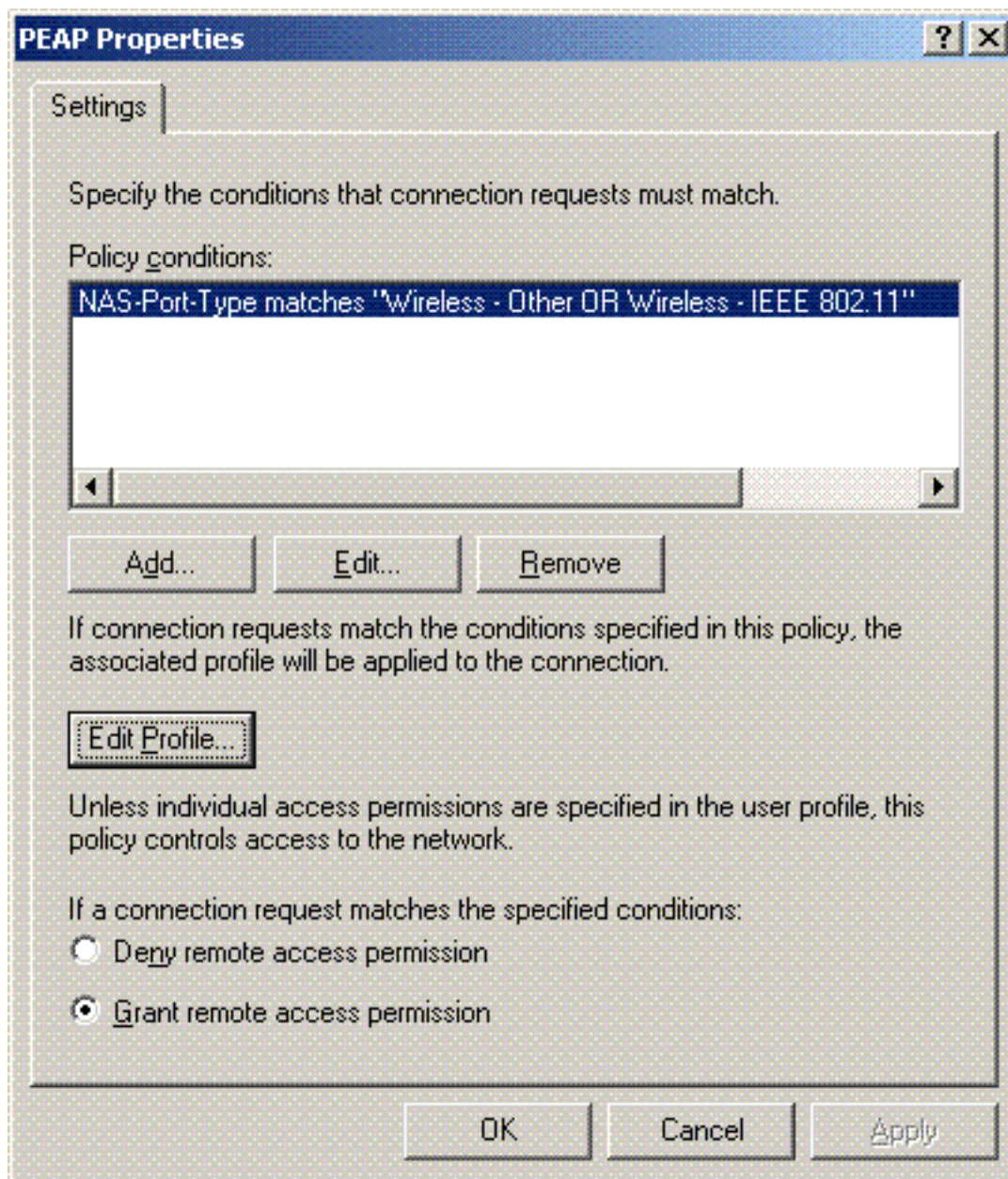
17. 驗證遠端訪問策略的詳細資訊，然後按一下**Finish**。



18. 遠端訪問策略已新增到清單中。



19. 按一下右鍵該策略，然後按一下**Properties**。在「如果連接請求與指定條件匹配」下選擇「授予遠端訪問許可權」。

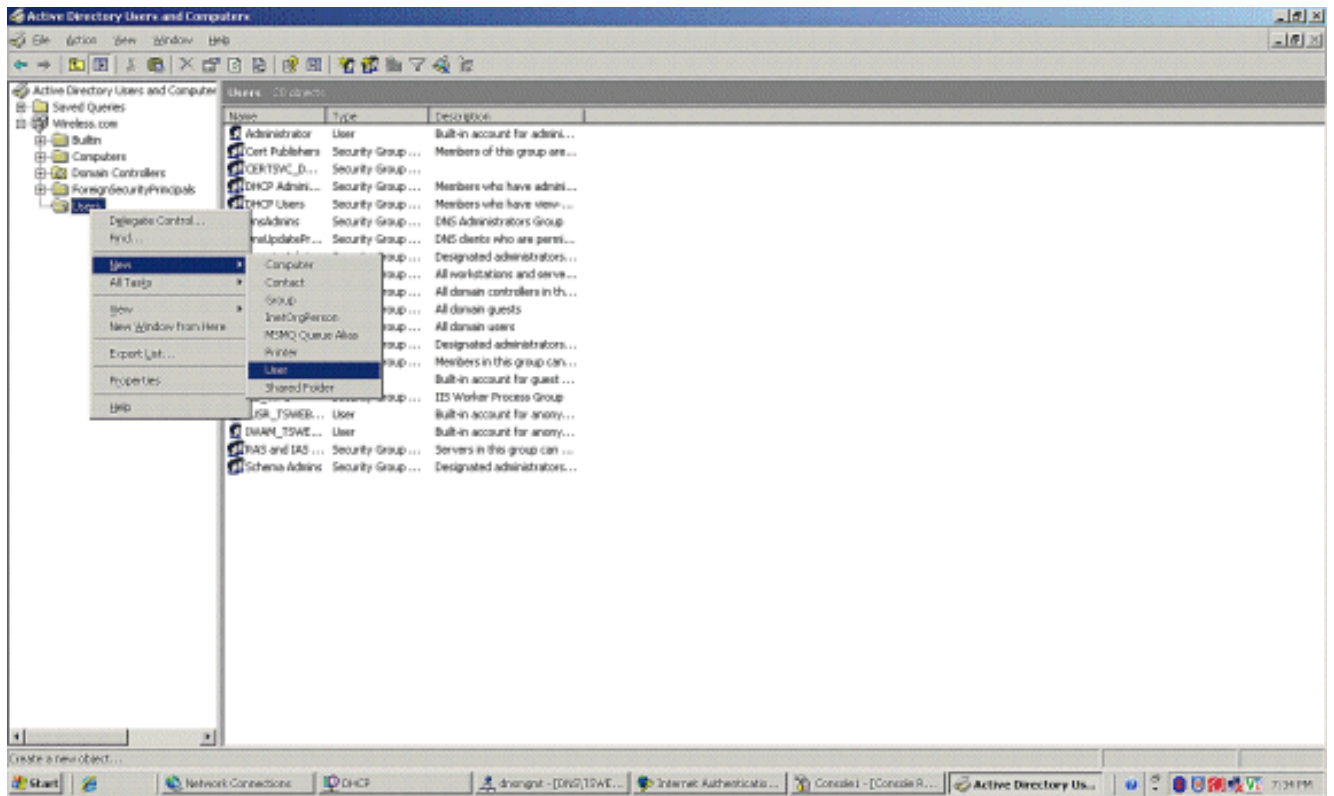


將使用者新增到Active Directory

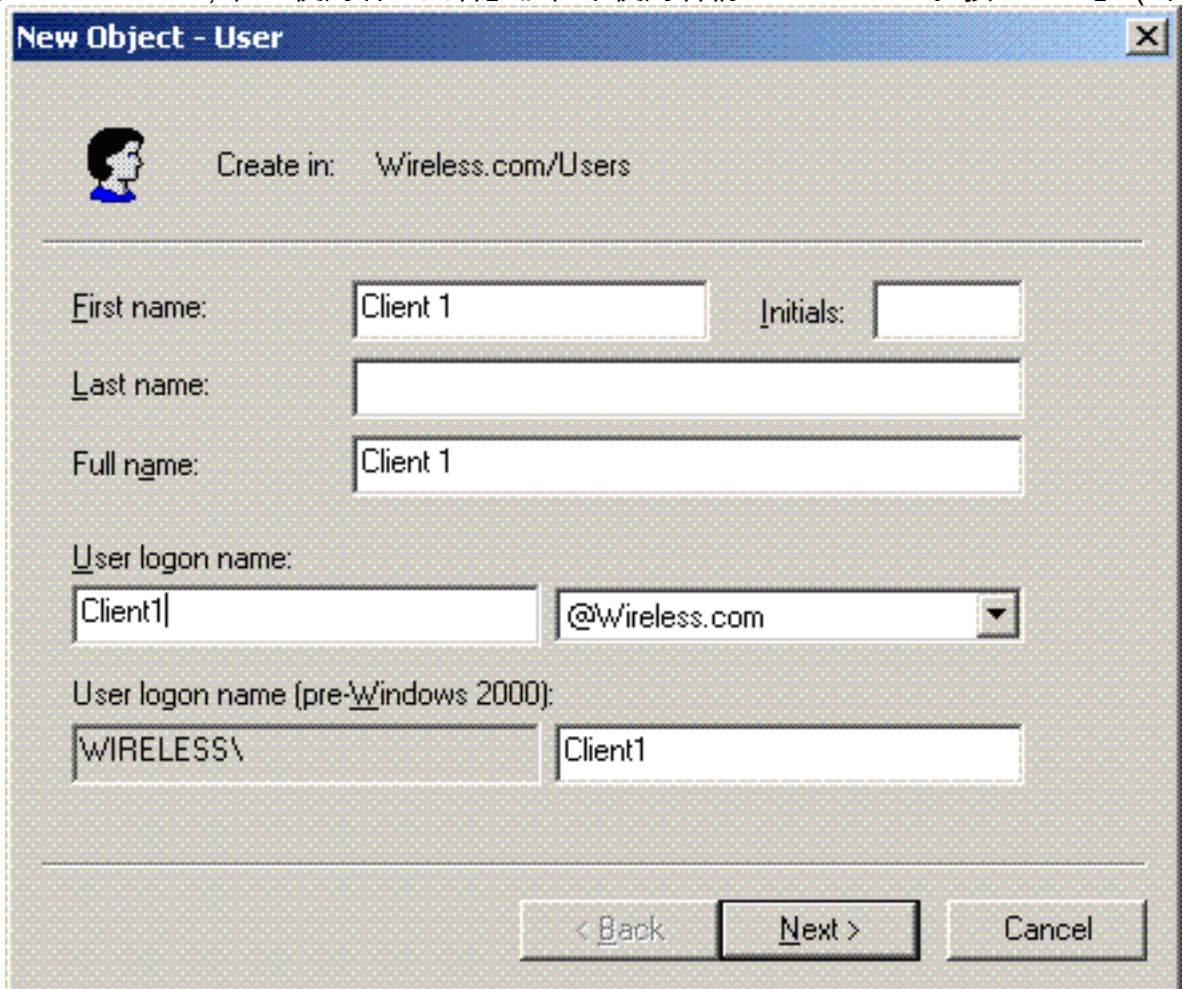
在此設定中，使用者資料庫在Active Directory上維護。

若要將使用者新增到Active Directory資料庫，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「名字」欄位中使用名稱WirelessUser，在「使用者登入名」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覈取方塊，然後按一下Next。

New Object - User [X]

 Create in: Wireless.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password


Password never expires

Account is disabled

< Back Next > Cancel

4. 在「新建對象 — 使用者」對話方塊中，按一下完成。

New Object - User [X]

 Create in: Wireless.com/Users

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

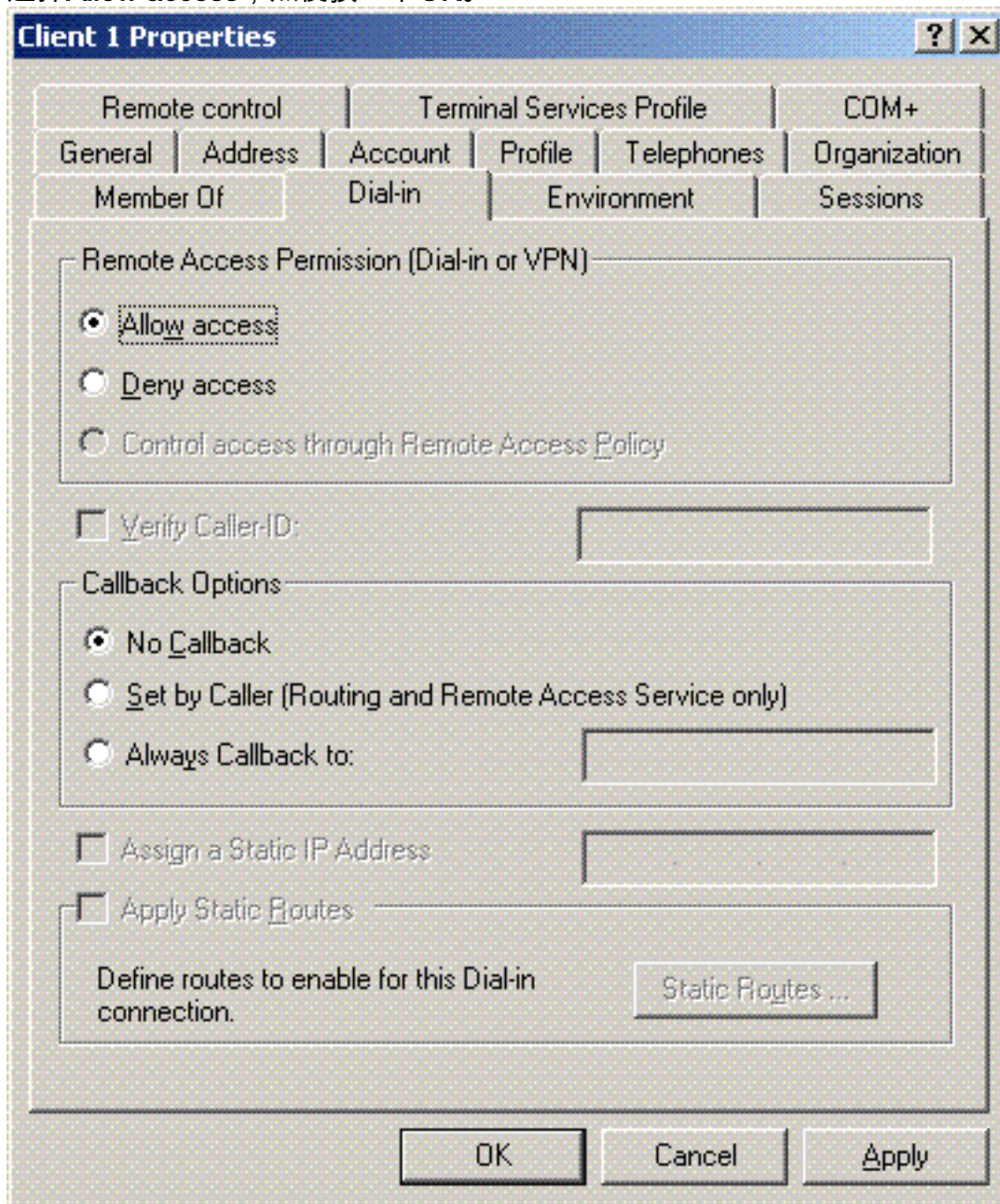
< Back Finish Cancel

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

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；單擊Properties；然後轉到Dial-in頁籤。
2. 選擇Allow access，然後按一下OK。



配置無線區域網控制器和輕量AP

現在為此設定配置無線裝置。其中包括無線LAN控制器、輕量AP和無線客戶端的配置。

通過MS IAS RADIUS伺服器配置WLC進行RADIUS身份驗證

首先配置WLC以使用MS IAS作為身份驗證伺服器。需要設定WLC，才能將使用者認證轉送到外部

RADIUS伺服器。外部RADIUS伺服器接著驗證使用者認證並提供對無線使用者端的存取許可權。為此，請在**Security > RADIUS Authentication**頁中將MS IAS伺服器新增為RADIUS伺服器。

請完成以下步驟：

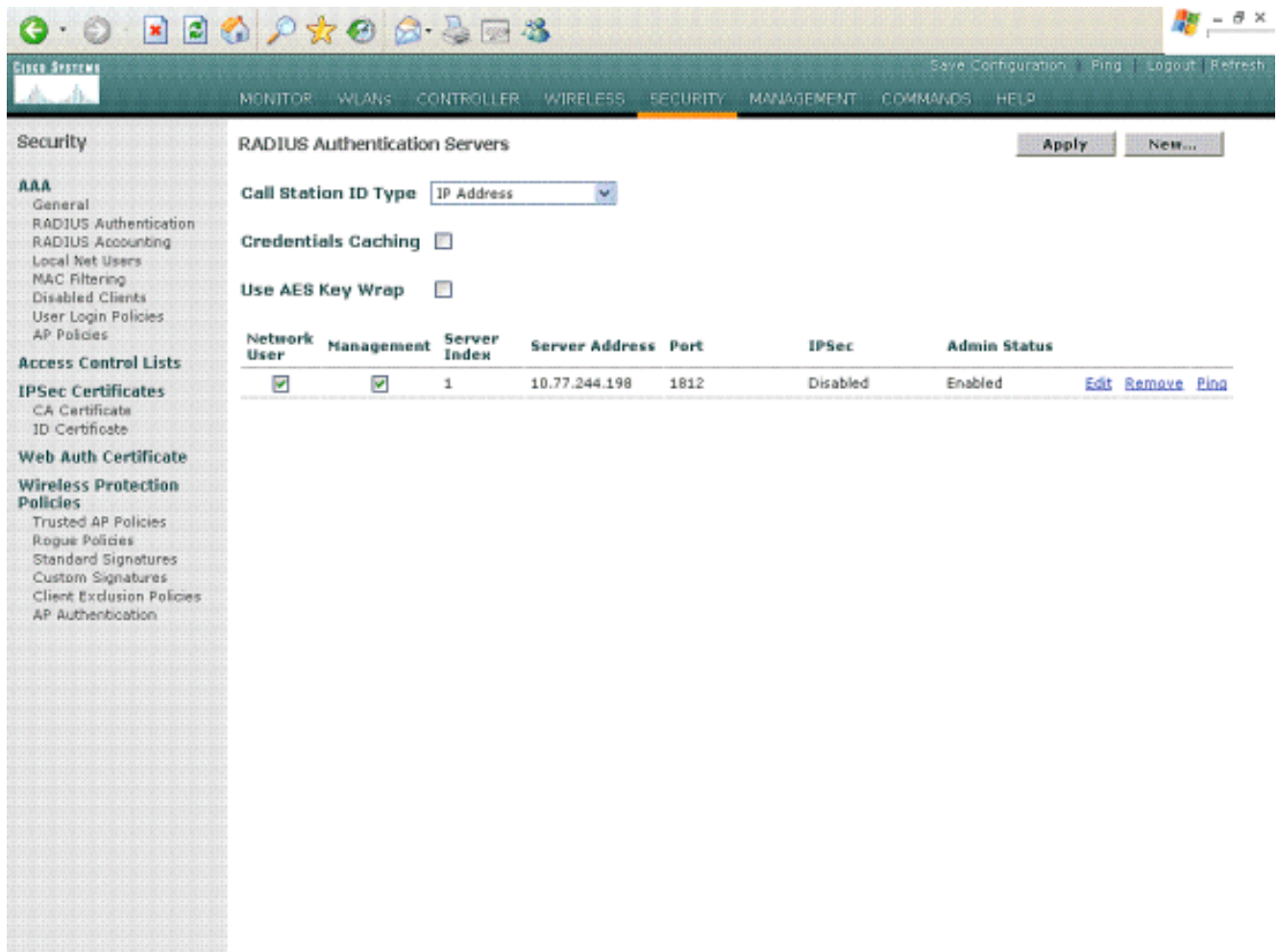
1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**，以顯示「RADIUS Authentication Servers」頁面。然後按一下**New**以定義RADIUS伺服器。

The screenshot displays the Cisco Systems GUI for configuring a new RADIUS Authentication Server. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (selected), MANAGEMENT, COMMANDS, and HELP. A left sidebar lists various configuration categories under 'Security', with 'RADIUS Authentication' selected. The main configuration area, titled 'RADIUS Authentication Servers > New', contains the following fields and options:

- Server Index (Priority):** 1
- Server IP Address:** 10.77.244.198
- Shared Secret Format:** ASCII
- Shared Secret:** [Masked]
- Confirm Shared Secret:** [Masked]
- Key Wrap:**
- Port Number:** 1812
- Server Status:** Enabled
- Support for RFC 3576:** Enabled
- Retransmit Timeout:** 2 seconds
- Network User:** Enable
- Management:** Enable
- IPsec:** Enable

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

2. 在**RADIUS Authentication Servers > New**頁中定義RADIUS伺服器引數。這些引數包括RADIUS伺服器IP地址、共用金鑰、埠號和伺服器狀態。Network User和Management覈取方塊確定基於RADIUS的身份驗證是否適用於管理和網路使用者。此示例使用MS IAS作為IP地址為10.77.244.198的RADIUS伺服器。



3. 按一下「Apply」。
4. MS IAS伺服器已作為Radius伺服器新增到WLC，可用於驗證無線客戶端。

為客戶端配置WLAN

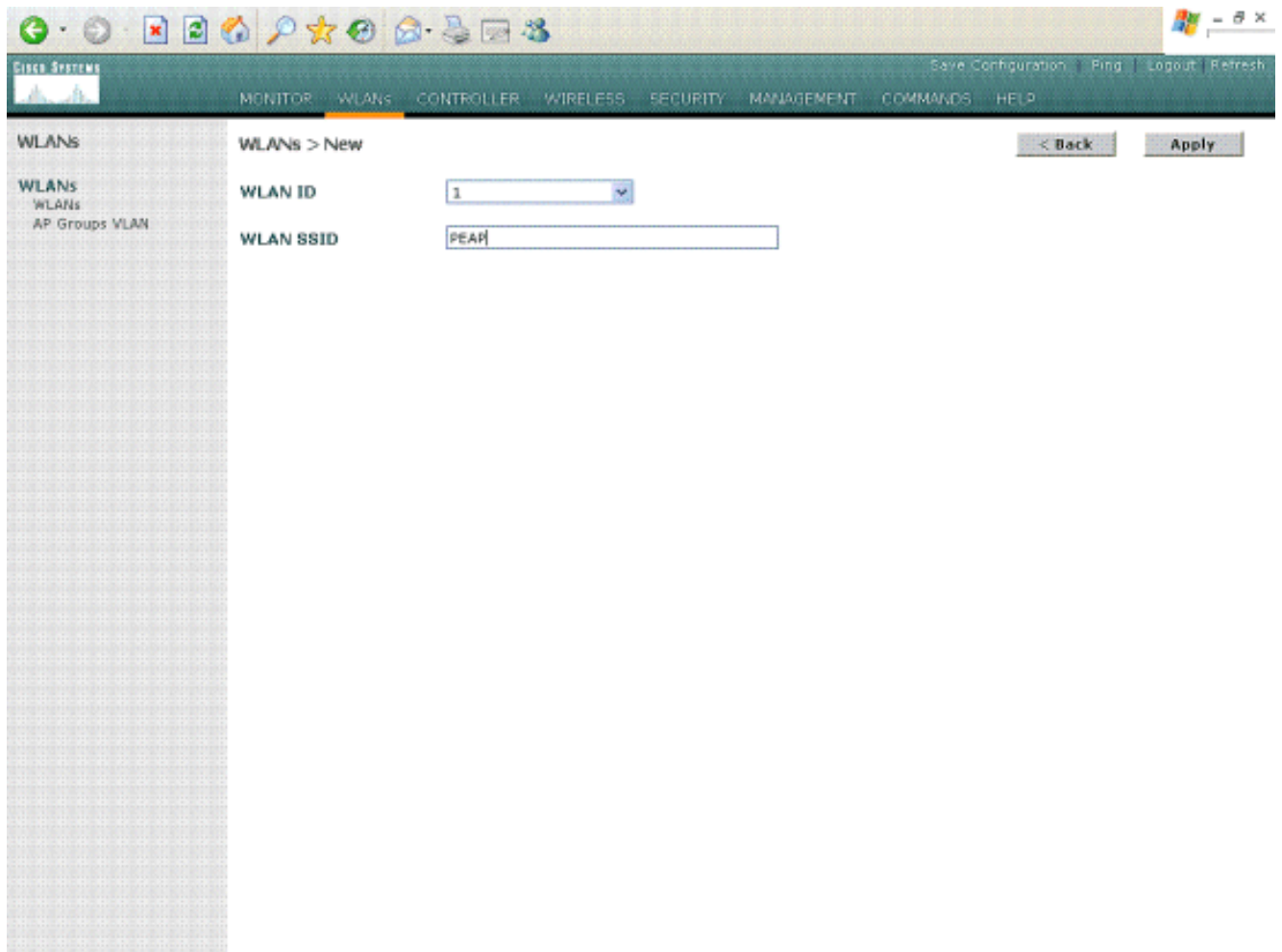
配置無線客戶端連線的SSID(WLAN)。在本示例中，建立SSID並將其命名為PEAP。

將第2層身份驗證定義為WPA2，以便客戶端執行基於EAP的身份驗證（本例中為PEAP-MSCHAPv2）並使用AES作為加密機制。將所有其他值保留為預設值。

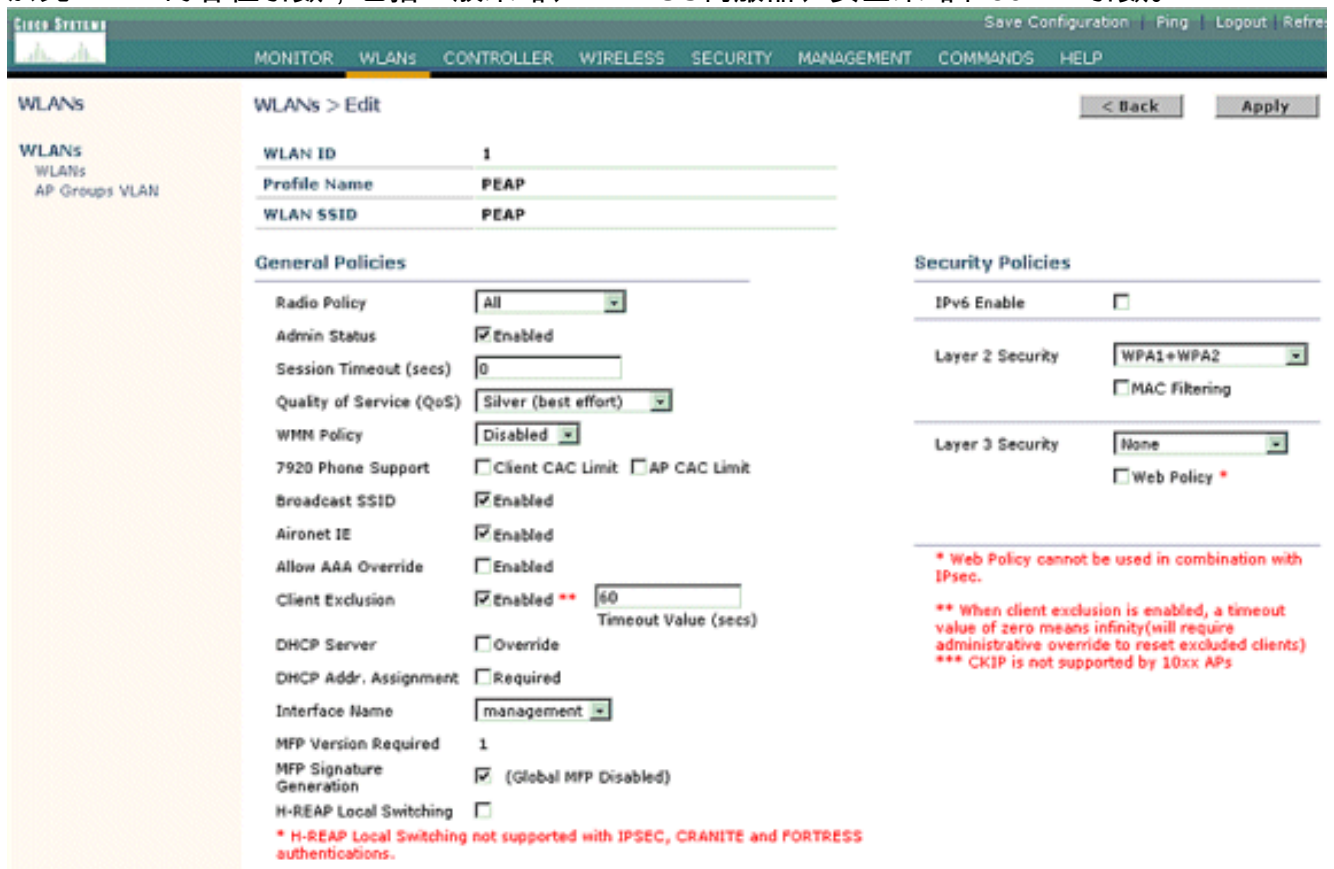
注意：本檔案將WLAN與管理介面繫結。當網路中有多個VLAN時，您可以建立一個單獨的VLAN並將其繫結到SSID。有關如何在WLC上設定VLAN的資訊，請參閱[無線LAN控制器上的VLAN組態範例](#)。

若要在WLC上設定WLAN，請完成以下步驟：

1. 從控制器的GUI中按一下「WLANs」，以顯示「WLANs」頁面。此頁面列出控制器上存在的WLAN。
2. 選擇**New**以建立一個新的WLAN。輸入WLAN的WLAN ID和WLAN SSID，然後按一下**Apply**。



3. 建立新的WLAN後，系統會顯示新WLAN的WLAN > Edit頁面。在此頁面上，您可以定義特定於此WLAN的各種引數，包括一般策略、RADIUS伺服器、安全策略和802.1x引數。

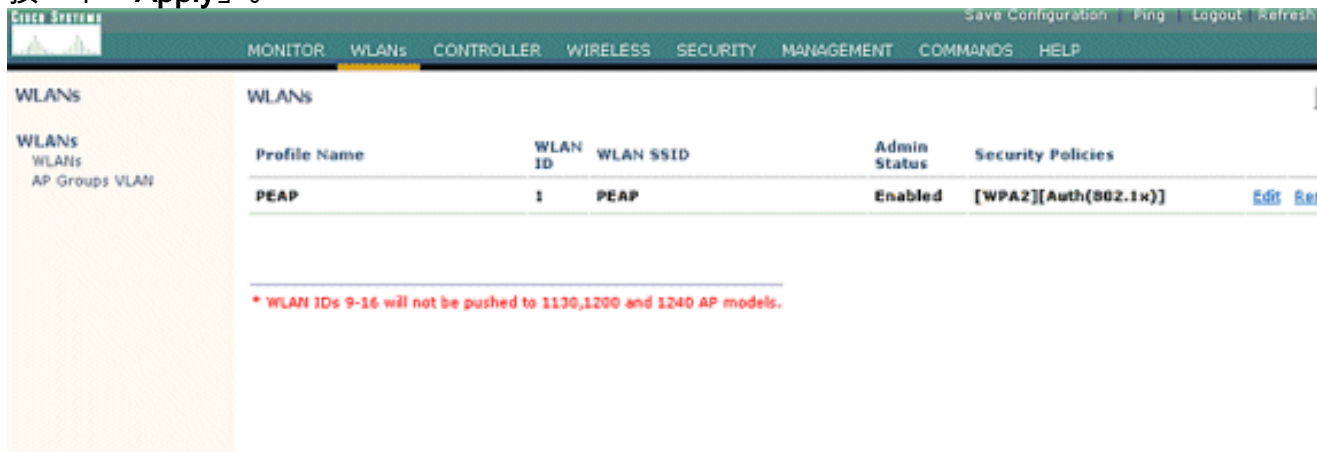


4. 檢查General Policies底下的Admin Status，以啟用WLAN。如果您希望AP在其信標幀中廣播SSID，請選中Broadcast SSID。

5. 在Layer 2 Security下，選擇WPA1+WPA2。這會在WLAN上啟用WPA。向下滾動頁面並選擇WPA策略。此示例使用WPA2和AES加密。從RADIUS Servers下的下拉選單中選擇適當的RADIUS伺服器。在本示例中，使用10.77.244.198 (MS IAS伺服器的IP地址)。其它引數可以根據WLAN網路的要求進行修改。



6. 按一下「Apply」。



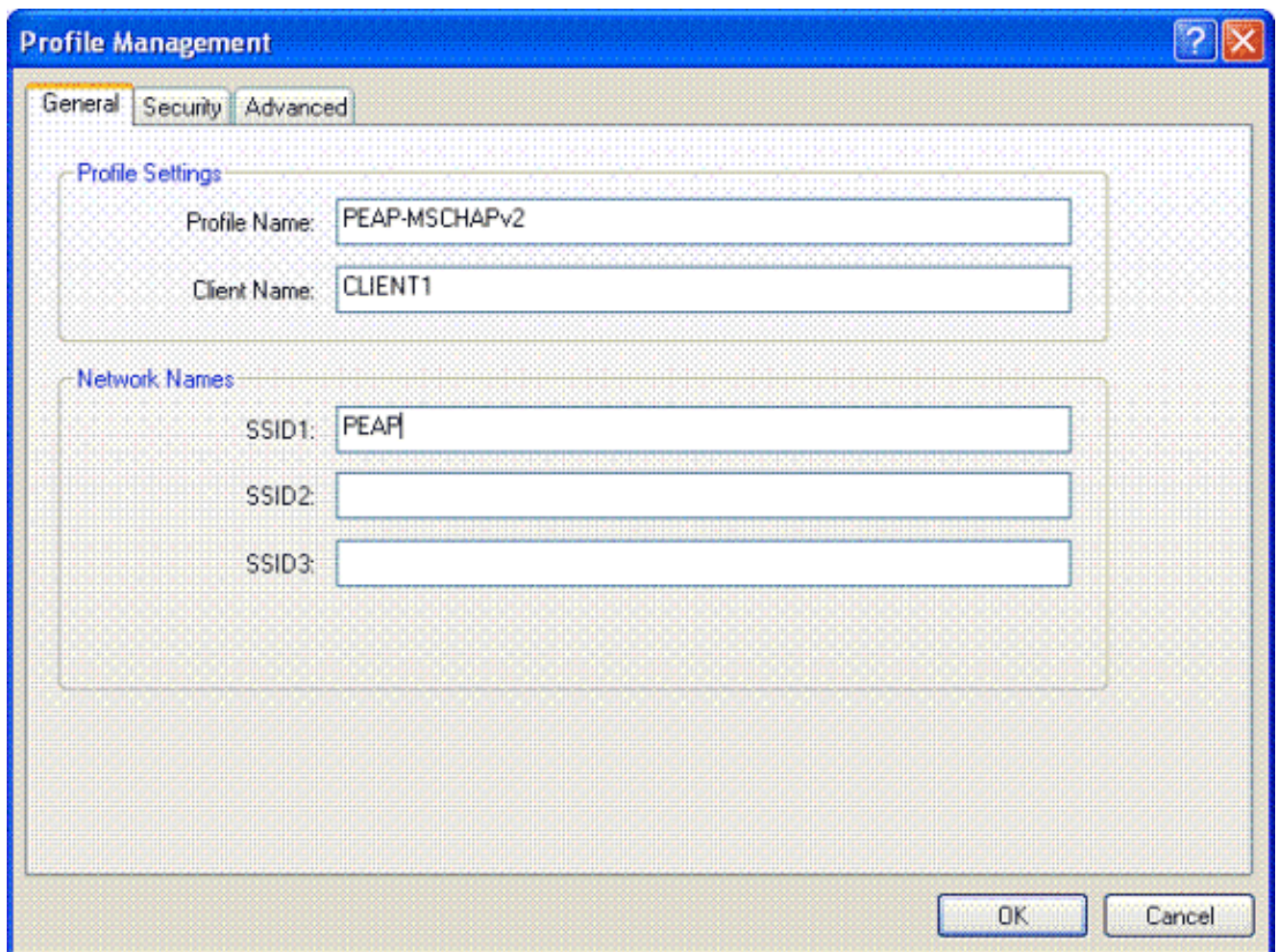
配置無線客戶端

為PEAP-MS CHAPv2身份驗證配置無線客戶端

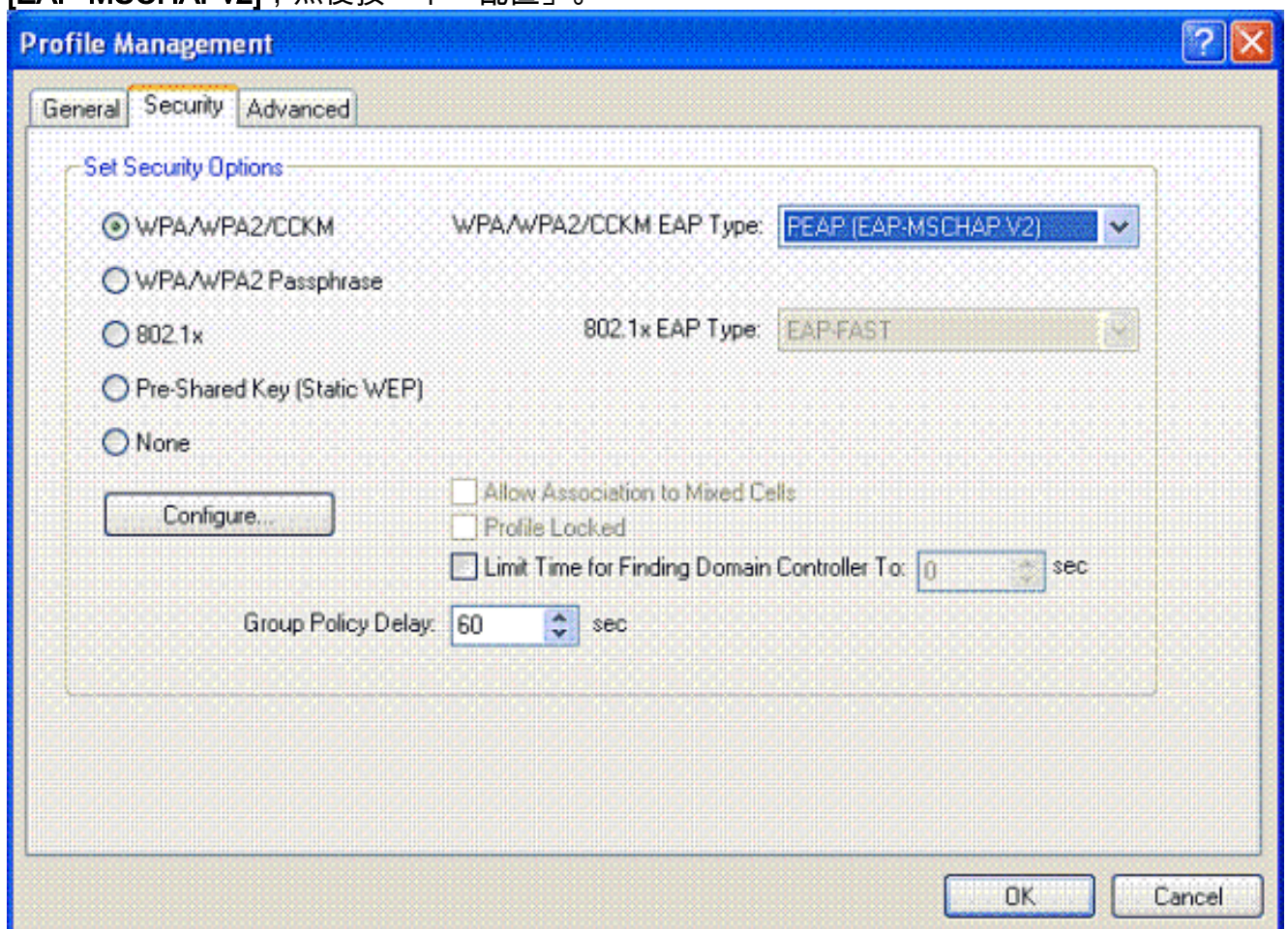
本示例提供有關如何使用Cisco Aironet Desktop Utility配置無線客戶端的資訊。配置客戶端介面卡之前，請確保使用韌體和實用程式的最新版本。在Cisco.com上的Wireless downloads (無線下載) 頁面中查詢韌體和實用程式的最新版本。

要使用ADU配置Cisco Aironet 802.11 a/b/g無線客戶端介面卡，請完成以下步驟：

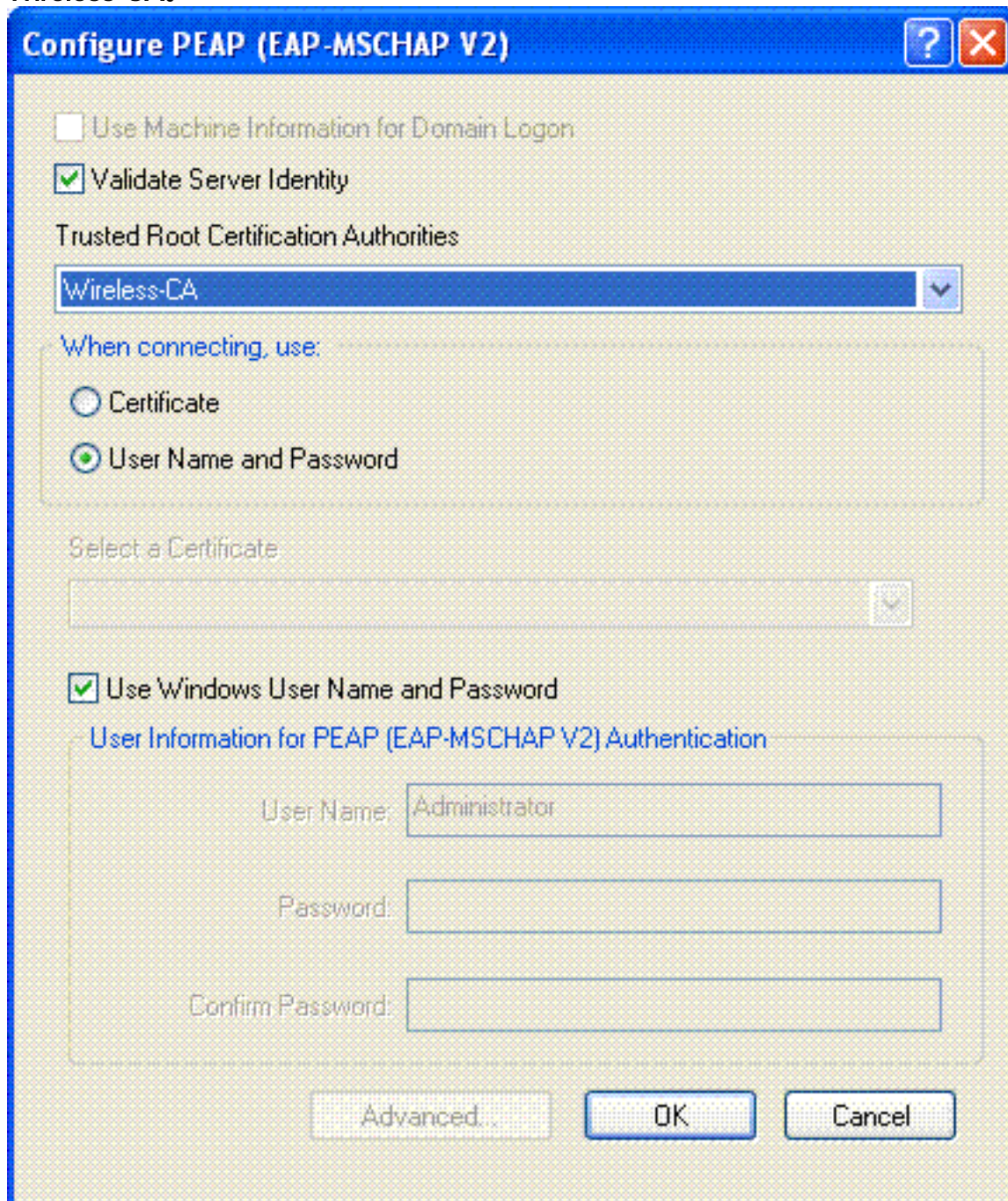
1. 開啟Aironet案頭實用程式。
2. 按一下**Profile Management**，然後按一下**New**以定義配置檔案。
3. 在「General (常規)」頁籤下，輸入配置檔名稱和SSID。在本範例中，使用您在WLC(PEAP)上設定的SSID。



4. 選擇「安全」頁籤；選擇WPA/WPA2/CCKM；在「WPA/WPA2/CCKM EAP」下，鍵入PEAP [EAP-MSCHAPv2]，然後按一下「配置」。



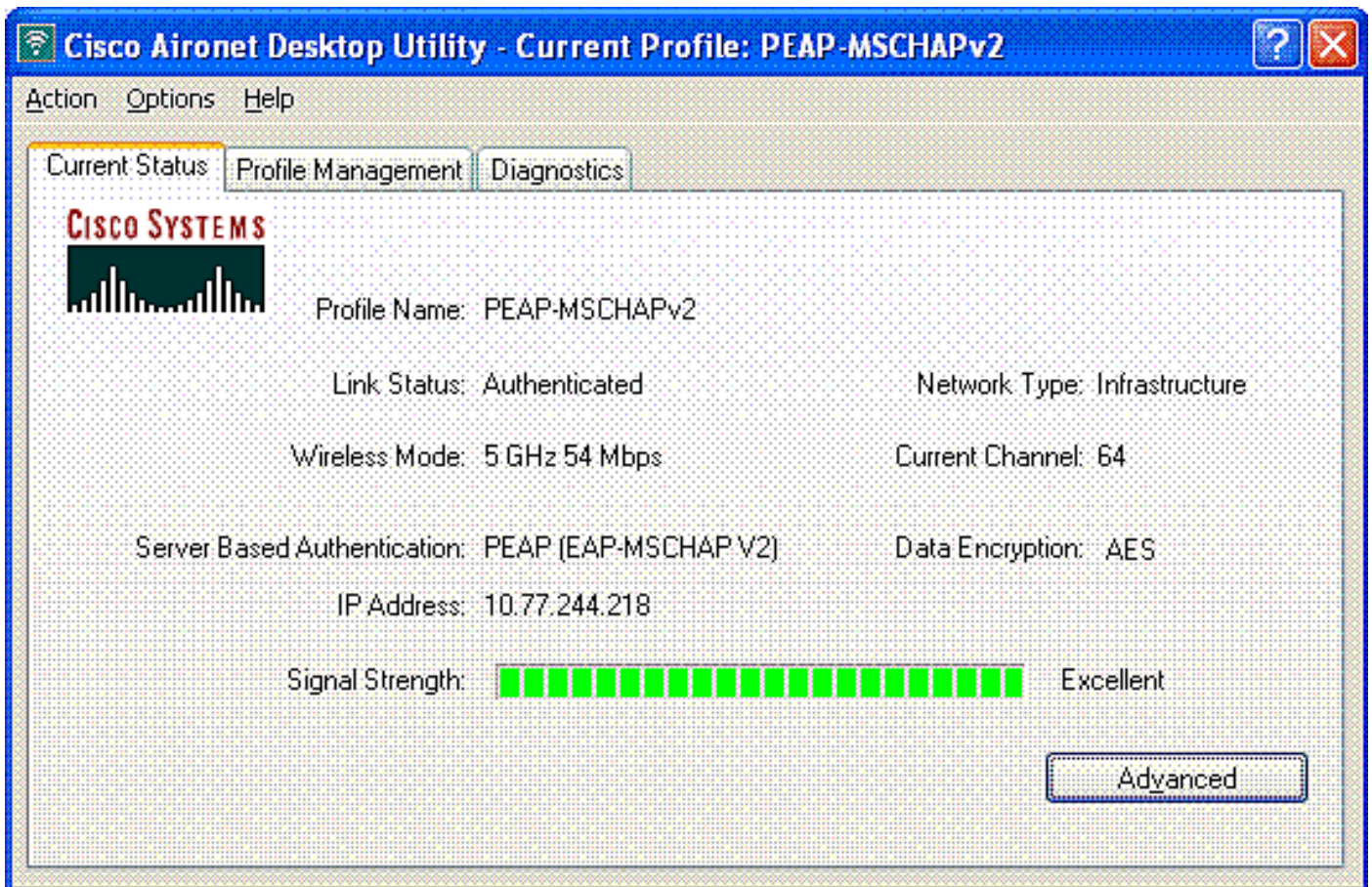
5. 選擇**Validate Server Certificate**，然後在Trusted Root Certificate Authorities下拉選單中選擇**Wireless-CA**。



6. 按一下**OK**，然後啟用配置檔案。**注意**：在Microsoft XP SP2中使用受保護的EAP-Microsoft質詢握手身份驗證協定版本2(PEAP-MSCHAPv2)時，無線卡由Microsoft無線零配置(WZC)管理，必須應用Microsoft修補程式KB885453。這可防止與PEAP快速恢復相關的身份驗證出現多個問題。

驗證和疑難排解

為了驗證配置是否按預期工作，請在無線客戶端Client1上啟用配置檔案PEAP-MSCHAPv2。



一旦在ADU上啟用配置檔案PEAP-MSCHAPv2，客戶端將執行802.11開放式身份驗證，然後執行PEAP-MSCHAPv2身份驗證。以下是成功的PEAP-MSCHAPv2身份驗證的示例。

使用debug命令瞭解發生的事件的順序。

[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

無線LAN控制器上的以下debug命令很有用。

- **debug dot1x events enable** — 用於配置802.1x事件的調試
- **debug aaa events enable** — 要配置AAA事件的調試
- **debug mac addr <mac address>** — 要配置MAC調試，請使用debug mac命令
- **debug dhcp message enable** — 要配置DHCP錯誤消息的調試

以下是debug dot1x events enable命令和debug client <mac address> 命令的示例輸出。

debug dot1x events enable:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
mobile 00:40:96:ac:e6:57 (EAP Id 3)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
```

mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9)

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13)**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**

mobile 00:40:96:ac:e6:57

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

debug mac addr <MAC Address>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)**

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy**

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)**

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3)**

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)**
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**

Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)**

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)**
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached PLUMBFASPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Replacing Fast Path rule
type = Airespace AP Client
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,

```
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

注意：如果使用Microsoft Supplicant客戶端通過Cisco Secure ACS進行PEAP身份驗證，則客戶端可能無法成功進行身份驗證。有時，初始連線可以成功進行身份驗證，但隨後的快速連線身份驗證嘗試無法成功連線。這是一個已知問題。此問題的詳細資訊和解決方法可從此處[獲取](#)。

相關資訊

- [採用ACS 4.0和Windows 2003的統一無線網路下的PEAP](#)
- [使用WLAN控制器\(WLC\)的EAP驗證組態範例](#)
- [無線區域網路控制器\(WLC\)軟體升級到3.2、4.0和4.1版](#)
- [Cisco 4400系列無線LAN控制器組態設定指南](#)
- [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）。