

统一无线网络先的PEAP与Microsoft互联网认证服务(IAS)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[PEAP 概述](#)

[配置](#)

[网络图](#)

[配置](#)

[配置 Microsoft Windows 2003 Server](#)

[配置 Microsoft Windows 2003 Server](#)

[在 Microsoft Windows 2003 Server 上安装和配置 DHCP 服务](#)

[安装并配置Microsoft Windows 2003 Server作为证书颁发机构\(CA\)服务器](#)

[将客户端连接到域](#)

[在 Microsoft Windows 2003 Server 上安装 Internet 身份验证服务并请求证书](#)

[为 PEAP-MS-CHAP v2 身份验证配置 Internet 身份验证服务](#)

[将用户添加到 Active Directory](#)

[允许用户进行无线访问](#)

[配置无线局域网控制器和轻量 AP](#)

[通过 MS IAS RADIUS 服务器为 RADIUS 身份验证配置 WLC](#)

[为客户端配置 WLAN](#)

[配置无线客户端](#)

[为 PEAP-MS CHAPv2 身份验证配置无线客户端](#)

[验证与故障排除](#)

[相关信息](#)

简介

本文档提供了一个配置示例，在使用 Microsoft Internet 身份验证服务 (IAS) 作为 RADIUS 服务器的 Cisco 统一无线网络中设置受保护的可扩展的身份验证协议 (PEAP) 与 Microsoft 质询握手身份验证协议 (MS-CHAP) 版本 2 身份验证。

先决条件

要求

假设读者已经掌握基本的 Windows 2003 安装和 Cisco 控制器安装，因为本文档仅涵盖有助于开展测试的特定配置。

注意：本文档旨在为读者提供有关MS服务器上进行PEAP - MS CHAP身份验证所需的配置的示例。本部分所示的 Microsoft 服务器配置在实验室中进行了测试，确认能按照预期工作。如果在配置 Microsoft 服务器时遇到问题，请联系 Microsoft 以获取帮助。Cisco TAC 不支持 Microsoft Windows 服务器配置。

有关Cisco 4400系列控制器的初始安装和配置信息，请参阅[快速入门指南：Cisco 4400系列无线 LAN控制器](#)。

有关 Microsoft Windows 2003 安装和配置指南，请访问[安装 Windows Server 2003 R2](#)。

开始之前，请在测试实验室中的每台服务器上安装 Microsoft Windows Server 2003 SP1 操作系统并更新所有 Service Pack。安装控制器和轻量接入点 (LAP) 并确保配置了最新的软件更新。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 运行固件 4.0 版的 Cisco 4400 系列控制器
- Cisco 1131 轻量接入点协议 (LWAPP) AP
- 安装了Internet身份验证服务(IAS)、证书颁发机构(CA)、DHCP和域名系统(DNS)服务的 Windows 2003企业服务器(SP1)
- 带有SP 2的Windows XP Professional (以及更新的Service Pack) 和Cisco Aironet 802.11a/b/g无线网络接口卡(NIC)
- Aironet Desktop Utility 4.0 版
- Cisco 3560 交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

[PEAP 概述](#)

PEAP使用传输级安全(TLS)在身份验证PEAP客户端 (例如无线笔记本电脑) 和PEAP身份验证器 (例如Microsoft Internet身份验证服务(IAS)或任何RADIUS服务器之间创建加密通道。PEAP 不指定身份验证方法，但为可通过由 PEAP 提供的 TLS 加密通道进行操作的其他 EAP 身份验证协议 (例如 EAP-MSCHAPv2) 提供附加的安全性。PEAP 身份验证过程主要包括两个阶段：

PEAP阶段1:TLS加密通道

无线客户端将与 AP 相关联。在客户端与接入点 (LAP) 之间创建安全关联之前，基于 IEEE 802.11 的关联会提供开放式系统或共享密钥身份验证。在客户端与接入点之间成功建立基于 IEEE 802.11 的关联之后，TLS 会话就会与 AP 进行协商。在无线客户端与 IAS 服务器之间的身份验证成功完成之后，TLS 会话就会在它们之间进行协商。在此协商中派生的密钥将用来加密随后的所有通信。

PEAP阶段2:EAP身份验证通信

EAP 通信 (包括 EAP 协商) 发生在由 PEAP 在 PEAP 认证过程的第一阶段中创建的 TLS 通道内。IAS 服务器使用 EAP-MS-CHAP v2 对无线客户端进行身份验证。LAP 和控制器仅在无线客户端与 RADIUS 服务器之间转发消息。WLC 和 LAP 无法解密这些消息，因为它不是 TLS 终点。

在发生 PEAP 第一阶段并且在 IAS 服务器与 802.1X 无线客户端之间创建了 TLS 通道之后，为了在用户获得 PEAP-MS-CHAP v2 提供的基于密码的有效凭证时成功完成身份认证，RADIUS 消息顺序如下：

1. IAS服务器向客户端发送身份请求消息：EAP-Request/Identity。
2. 客户端使用身份响应消息进行响应：EAP-Response/Identity。
3. IAS服务器发送MS-CHAP v2询问消息：EAP-Request/EAP-Type=EAP MS-CHAP-V2 (询问)。
4. 客户端使用MS-CHAP v2质询和响应进行响应：EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (响应)。
5. 当服务器成功对客户端进行身份验证时，IAS服务器会发回MS-CHAP v2成功数据包：EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (成功)。
6. 当客户端成功对服务器进行身份验证时，客户端将使用MS-CHAP v2成功数据包进行响应：EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (成功)。
7. IAS 服务器发送一个指示身份验证成功的 EAP-TLV。
8. 客户端回复一个 EAP-TLV 状态成功消息。
9. 服务器完成身份验证并使用明文发送 EAP 成功消息。如果部署了 VLAN 用于客户端隔离，则此消息中还包含 VLAN 属性。

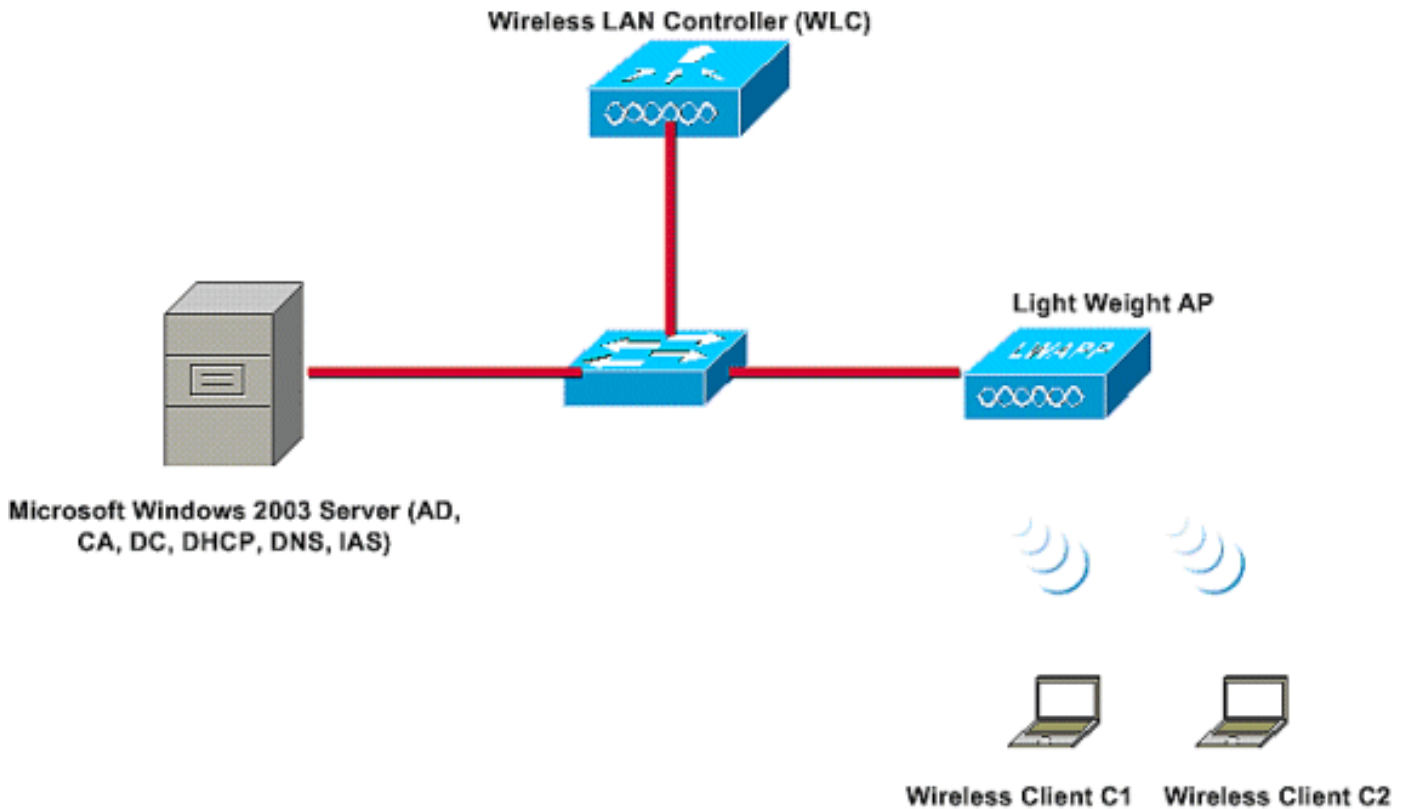
配置

本文档提供一个 PEAP MS-CHAP v2 配置示例。

注意：要获取此部分中所用命令的更多信息，可使用[命令查找工具](#) (仅限[已注册](#)客户)。

网络图

本文档使用以下网络设置：



在此设置中，Microsoft Windows 2003 Server 担当以下角色：

- **Wireless.com 域的域控制器**
- DHCP/DNS 服务器
- 证书颁发机构(CA)服务器
- Active Directory - 用于维护用户数据库
- 互联网身份验证服务(IAS) — 对无线用户进行身份验证

此服务器通过第 2 层交换机连接到有线网络（如图所示）。

无线LAN控制器(WLC)和注册的LAP也通过第2层交换机连接到网络。

无线客户端 C1 和 C2 将使用 Wi-Fi 保护访问 2 (WPA2) - PEAP MSCHAP v2 身份验证来连接到无线网络。

目标是配置 Microsoft 2003 Server、无线局域网控制器和轻量 AP，以便通过 PEAP MSCHAP v2 身份验证对无线客户端进行身份验证。

下一部分解释如何为此设置配置设备。

配置

本部分介绍在此 WLAN 中设置 PEAP MS-CHAP v2 身份验证时所需的配置：

- 配置 Microsoft Windows 2003 Server
- 配置无线局域网控制器(WLC)和轻量AP
- 配置无线客户端

首先配置 Microsoft Windows 2003 Server。

配置 Microsoft Windows 2003 Server

配置 Microsoft Windows 2003 Server

按照“网络设置”部分所述，请在网络中使用 Microsoft Windows 2003 Server 来执行以下功能。

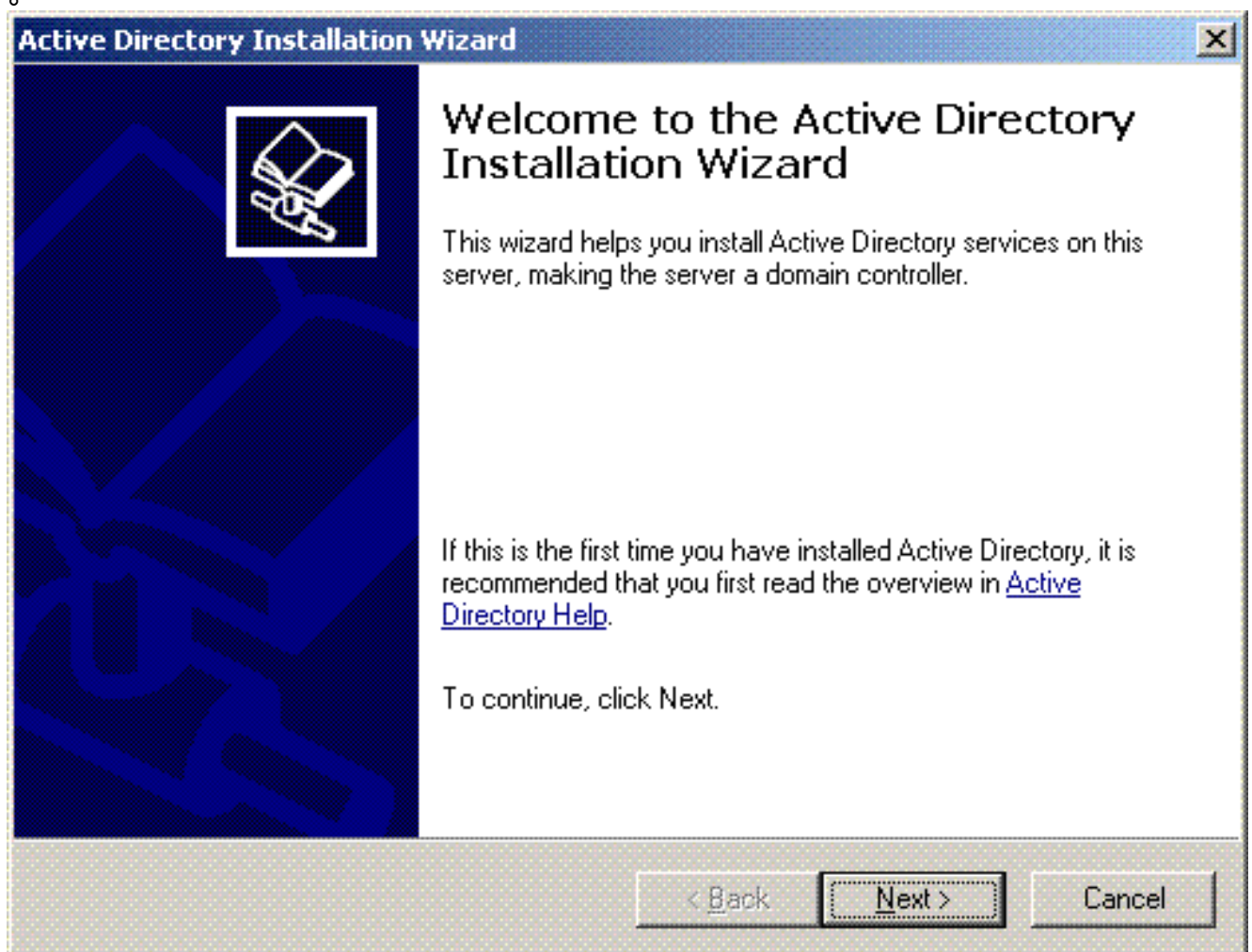
- 域控制器 – 用于 Wireless 域
- DHCP/DNS 服务器
- 证书颁发机构(CA)服务器
- Internet身份验证服务(IAS)-用于对无线用户进行身份验证
- Active Directory - 用于维护用户数据库

为这些服务配置 Microsoft Windows 2003 Server。首先将 Microsoft Windows 2003 Server 配置为域控制器。

将 Microsoft Windows 2003 Server 配置为域控制器

要将 Microsoft Windows 2003 Server 配置为域控制器，请完成以下步骤：

1. 单击开始，单击“运行”，键入 dcpromo.exe，然后单击“确定”以启动 Active Directory 安装向导。



2. 单击下一步运行 Active Directory 安装向导。

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

3. 要创建新域，请选择新域的**域控制器**选项。

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.

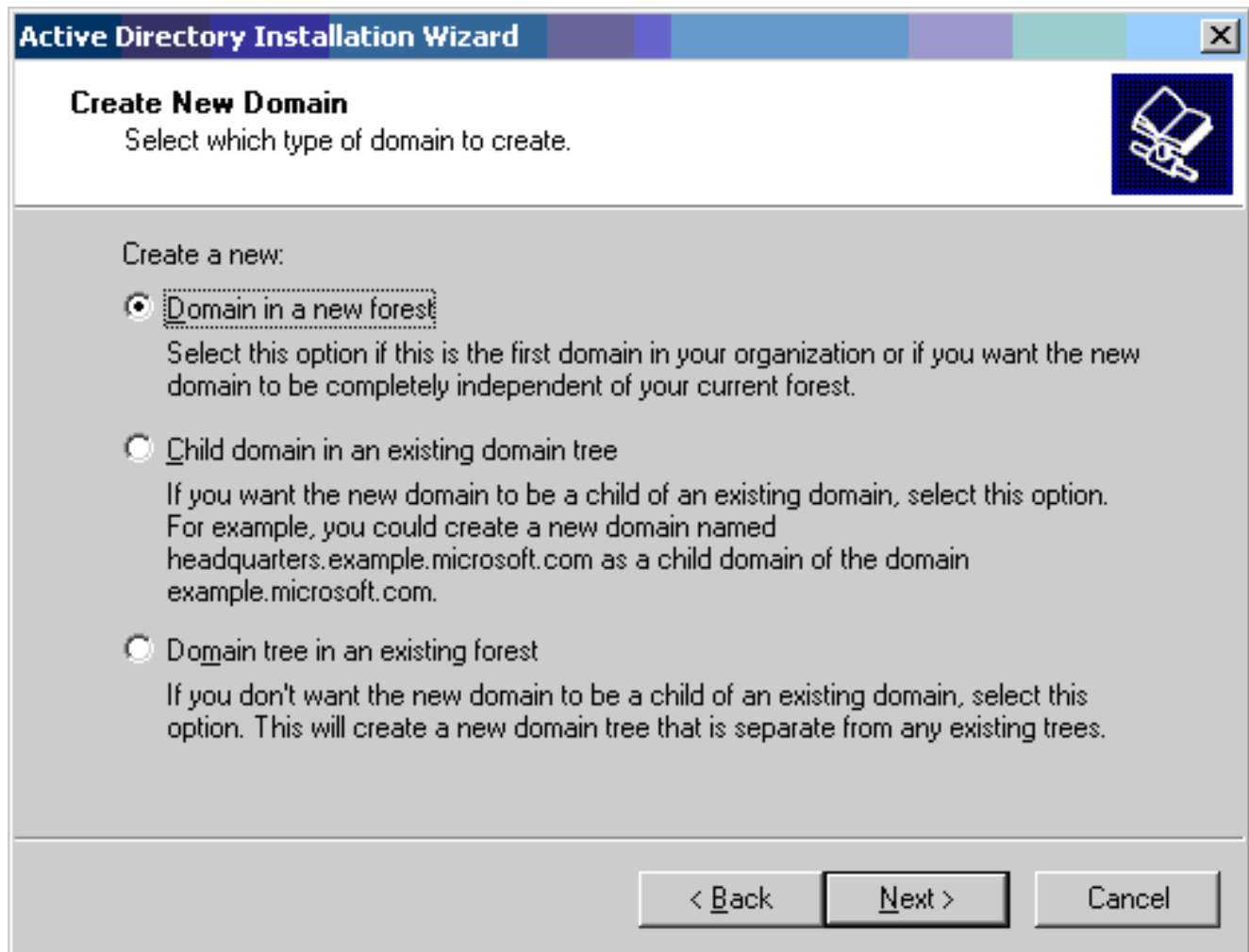
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

< Back

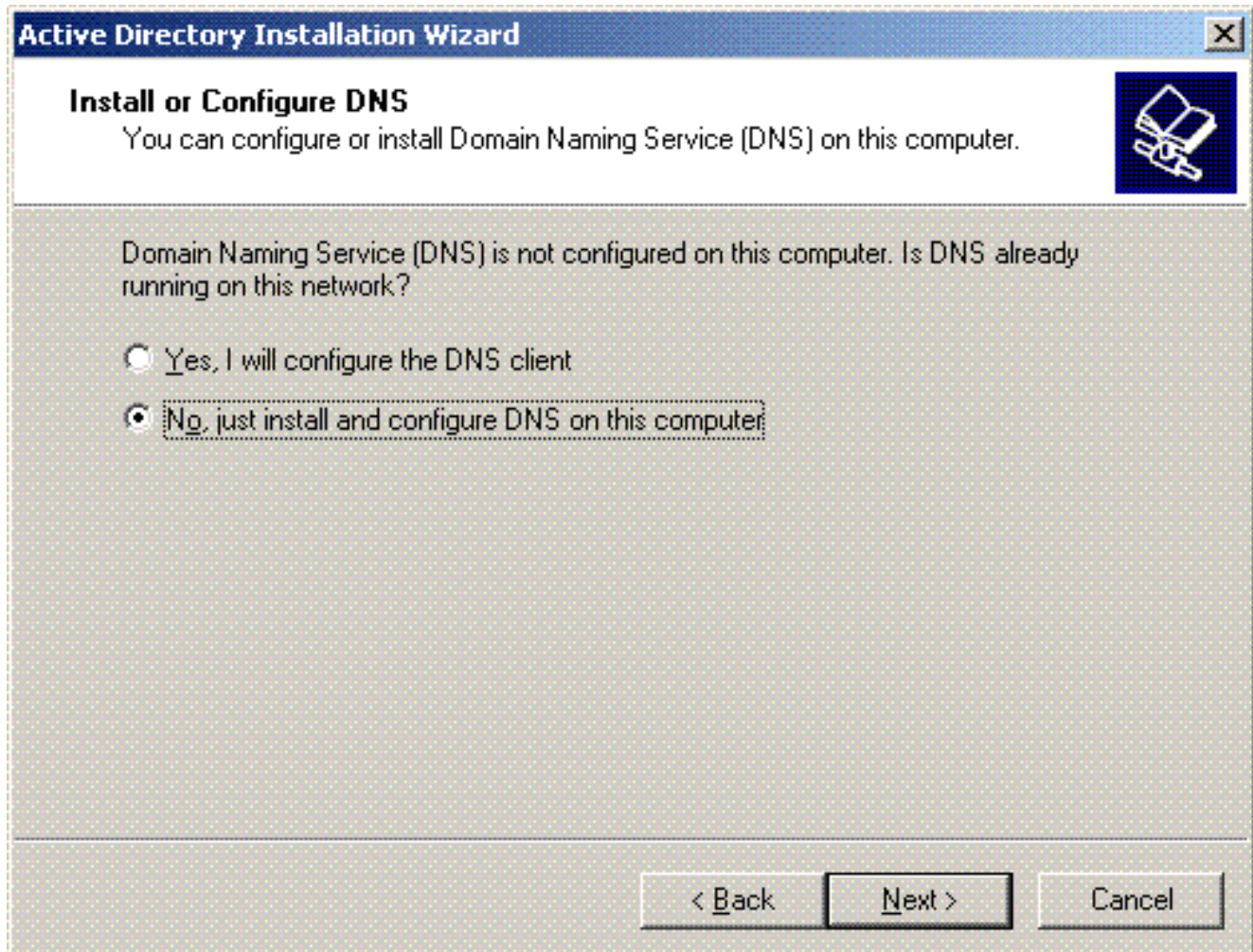
Next >

Cancel

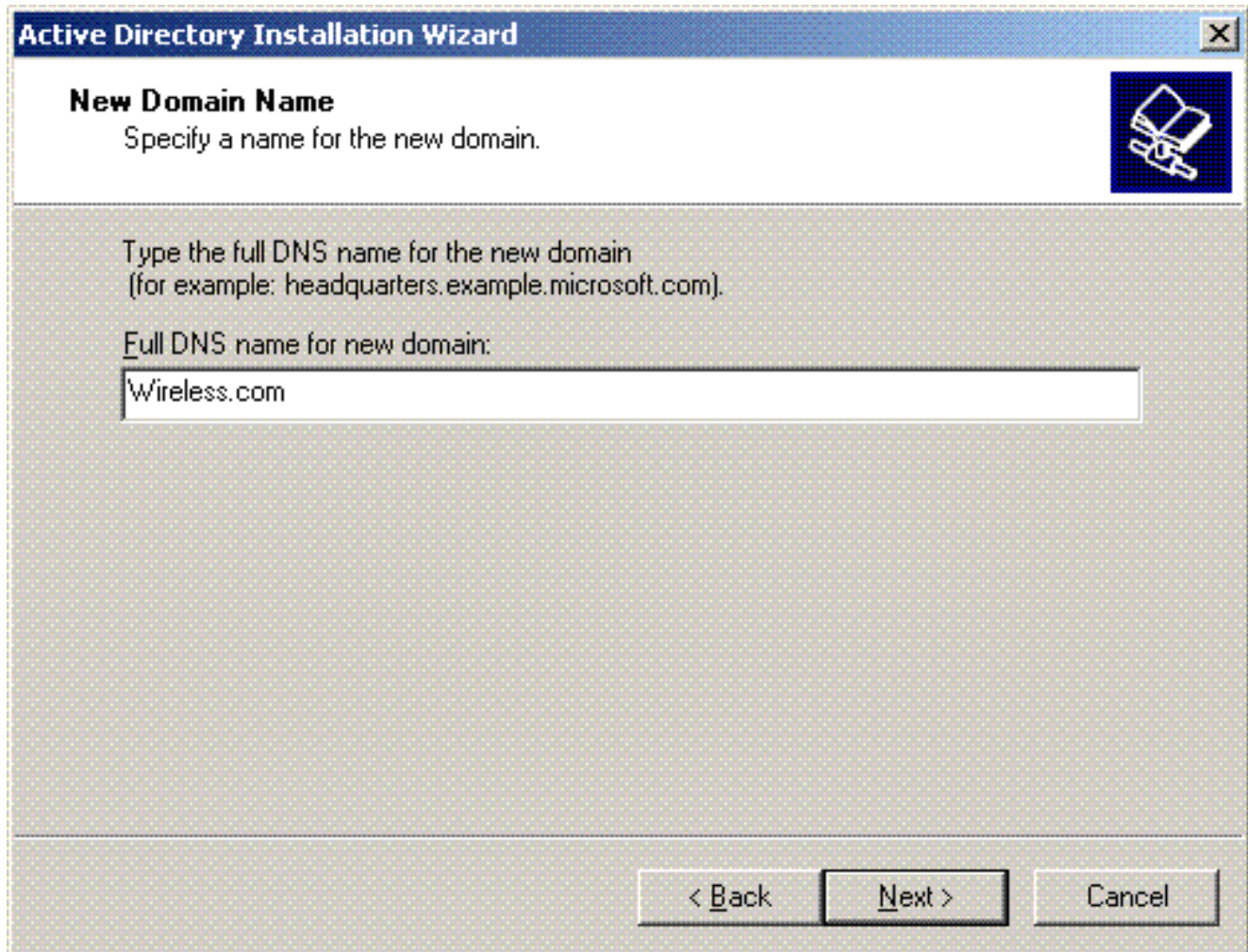
4. 单击下一步创建一个新的域树森林。



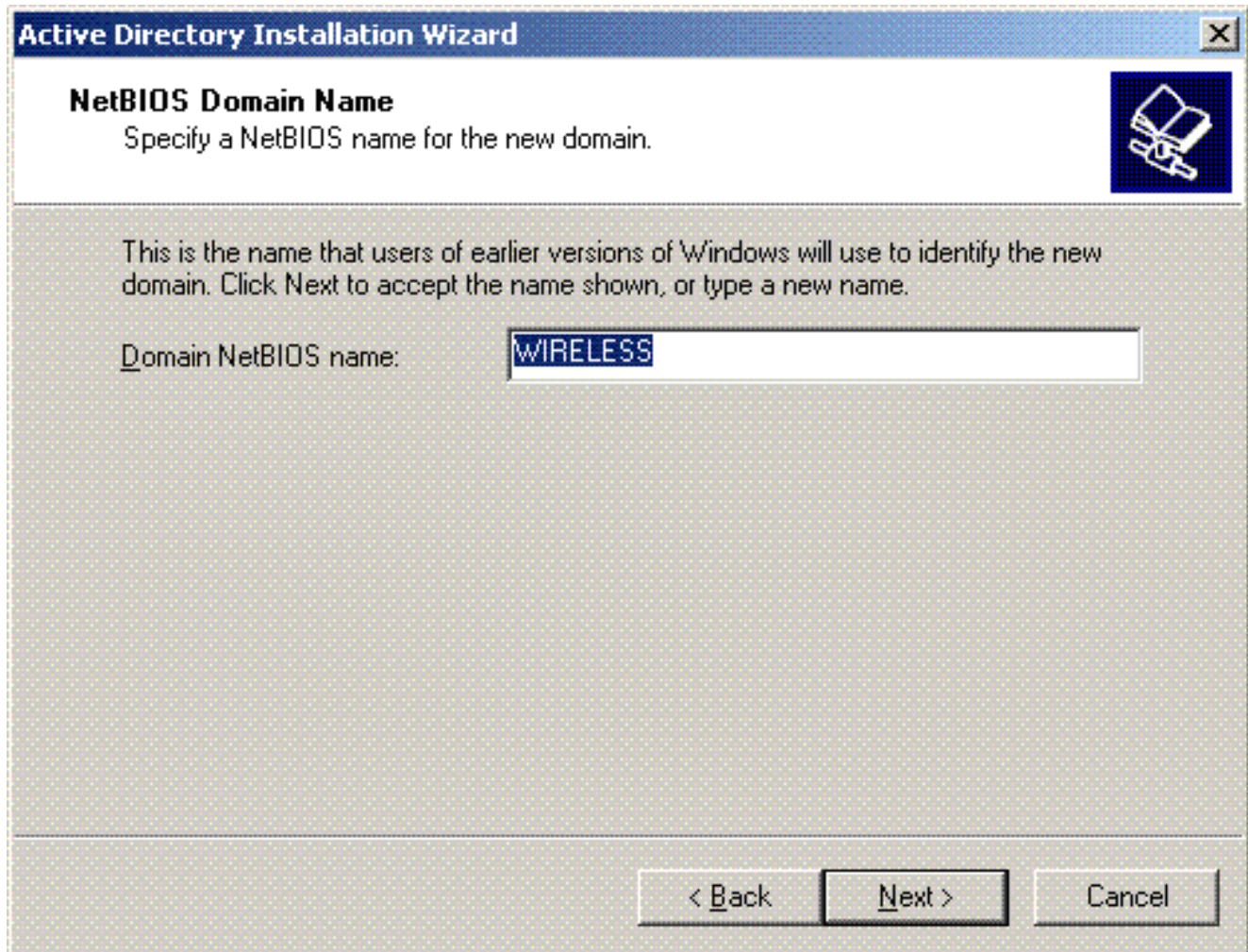
5. 如果系统上没有安装 DNS，此向导将为您提供选项用于配置 DNS。选择否，在本计算机上安装和配置 DNS。单击 Next。



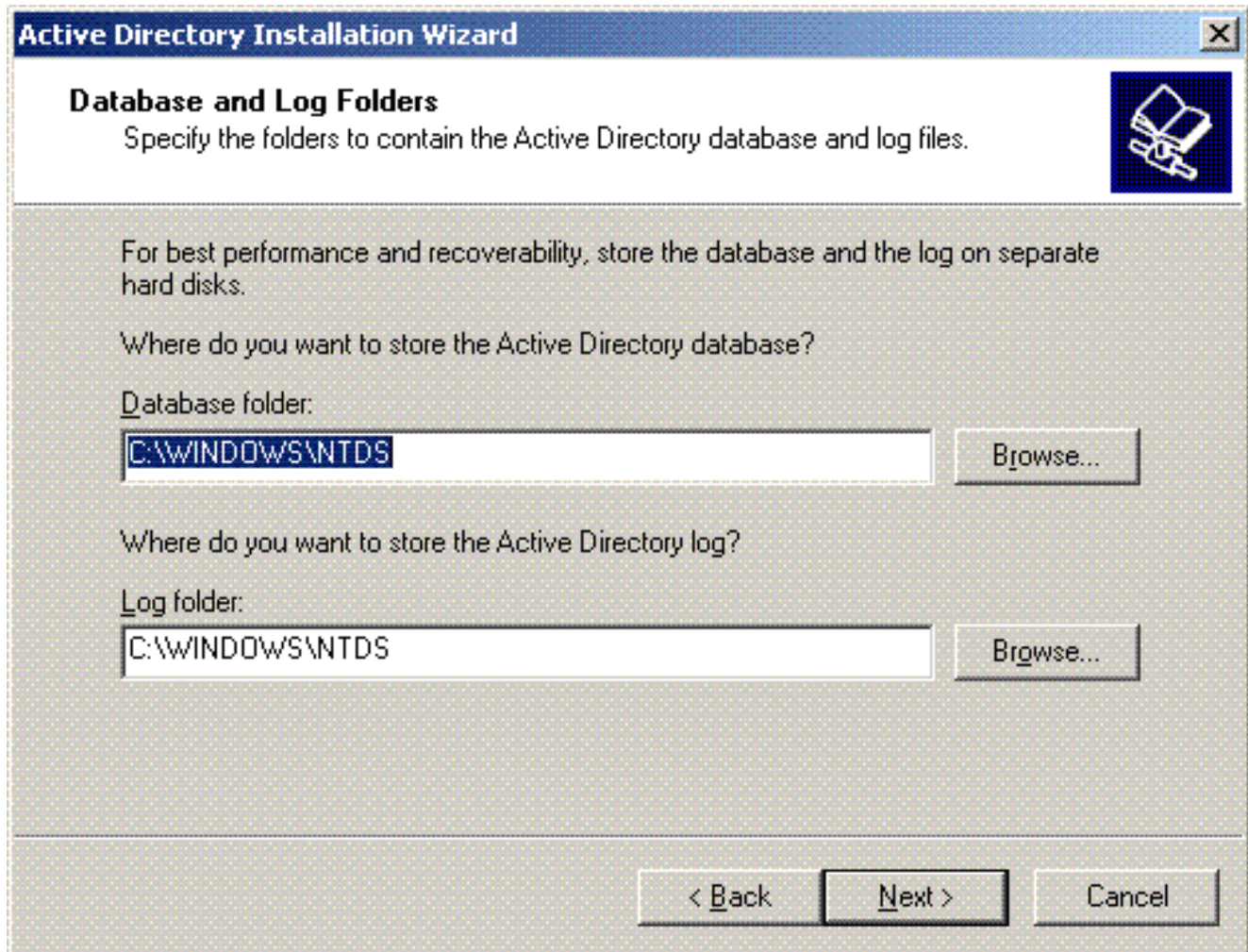
6. 为新域键入完整的 DNS 名称。本示例中使用 Wireless.com，然后单击“下一步”。



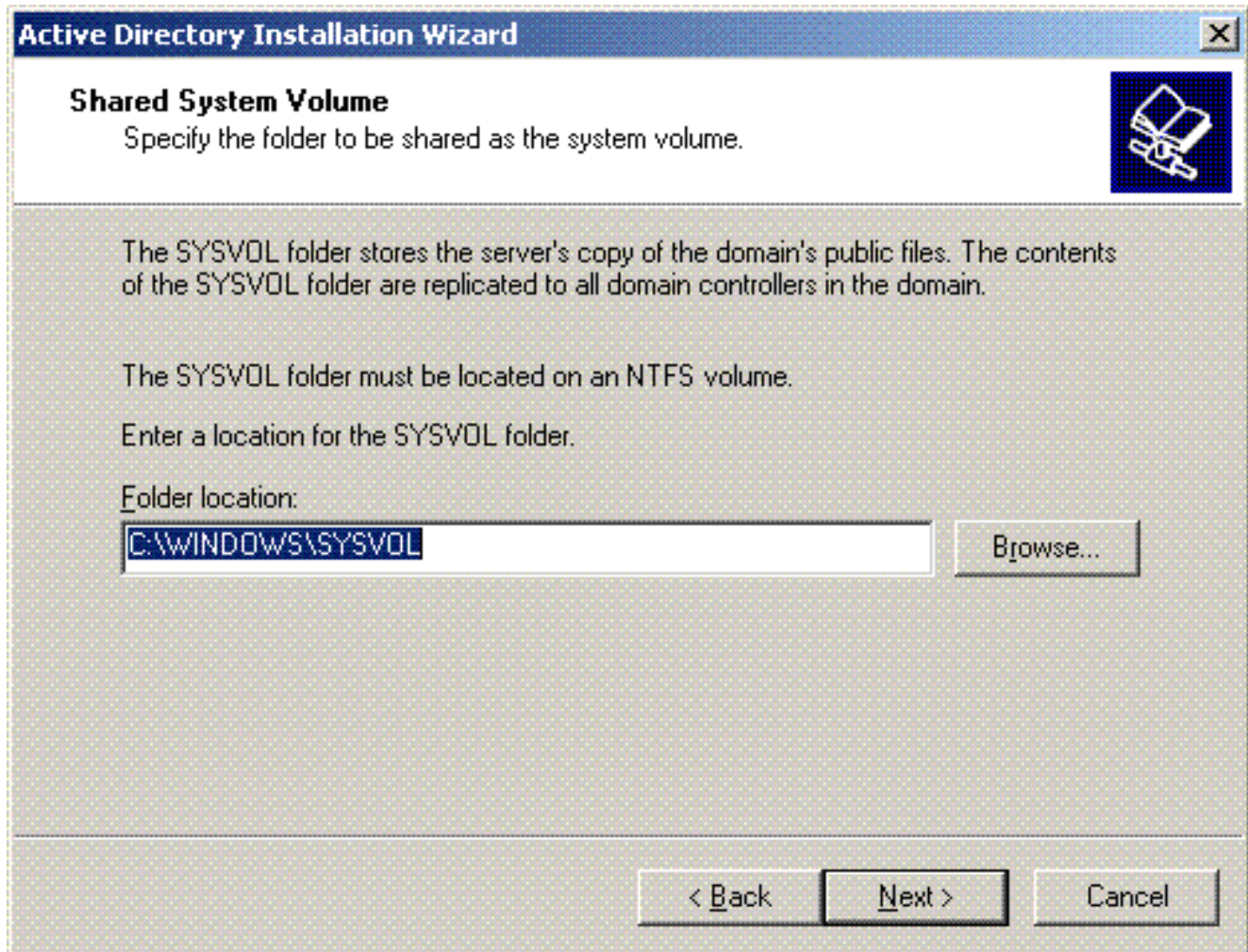
7. 为域输入 NETBIOS 名称，然后单击下一步。本示例使用 WIRELESS。



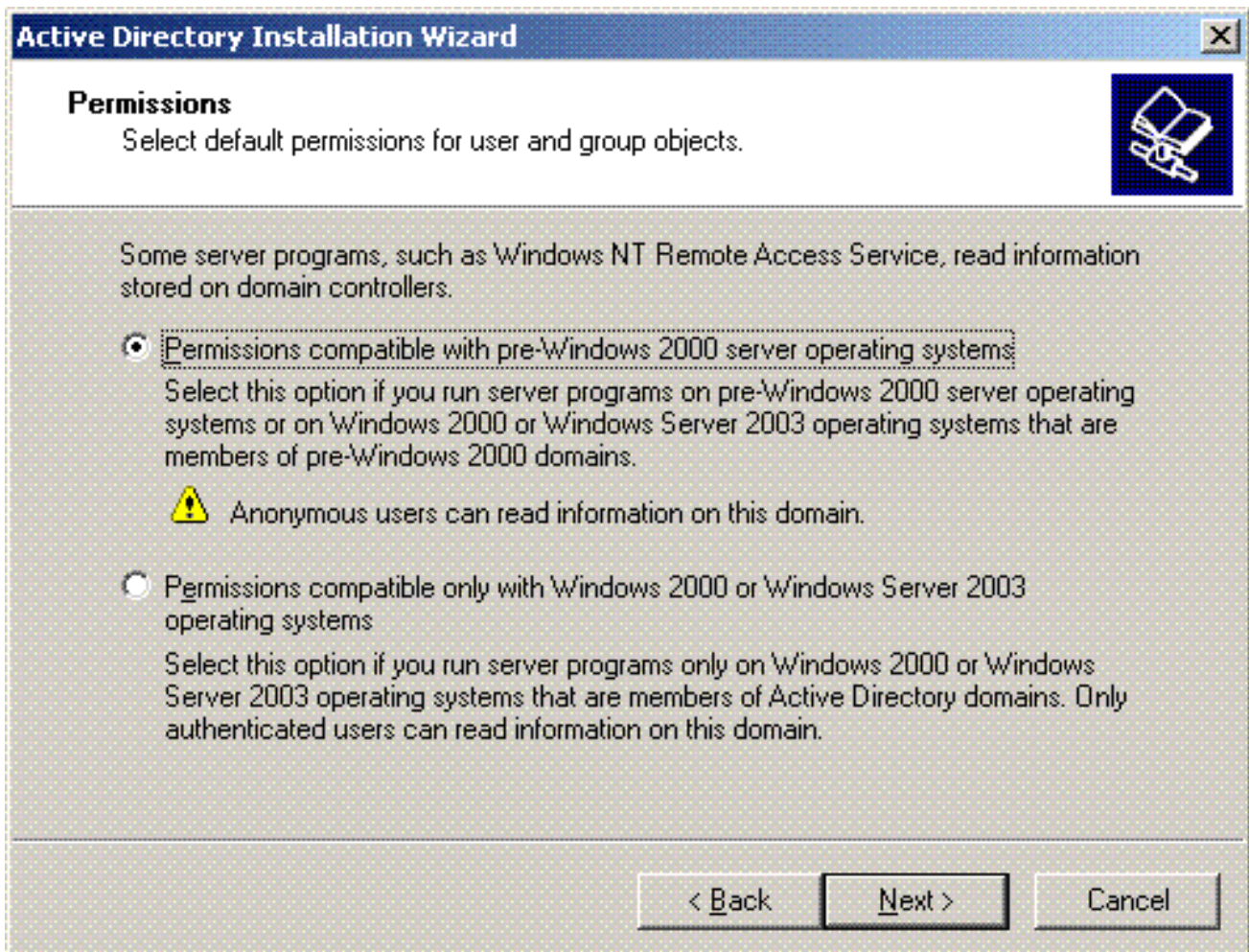
8. 为域选择数据库和日志位置。单击 **Next**。



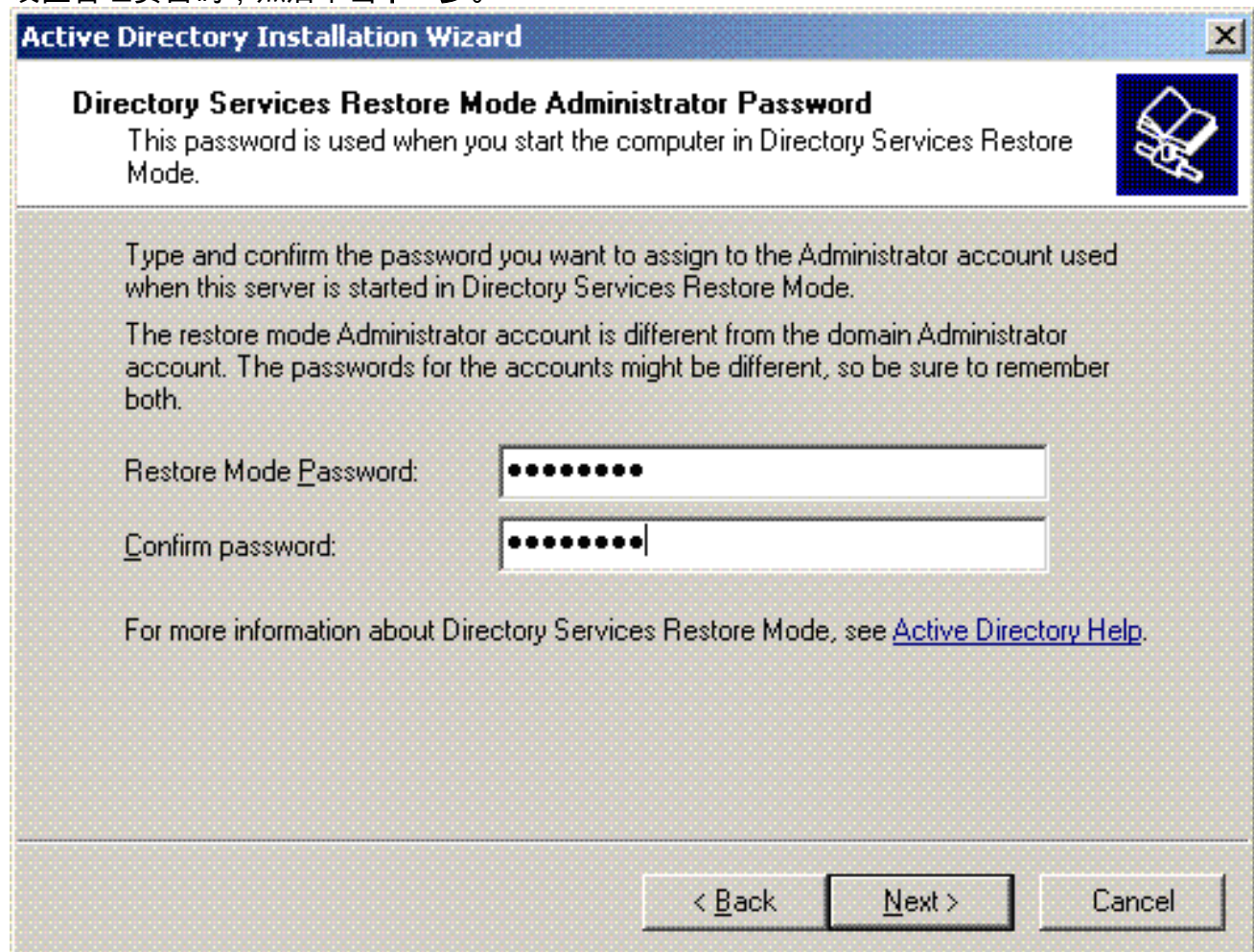
9. 选择 Sysvol 文件夹的位置。单击 **Next**。



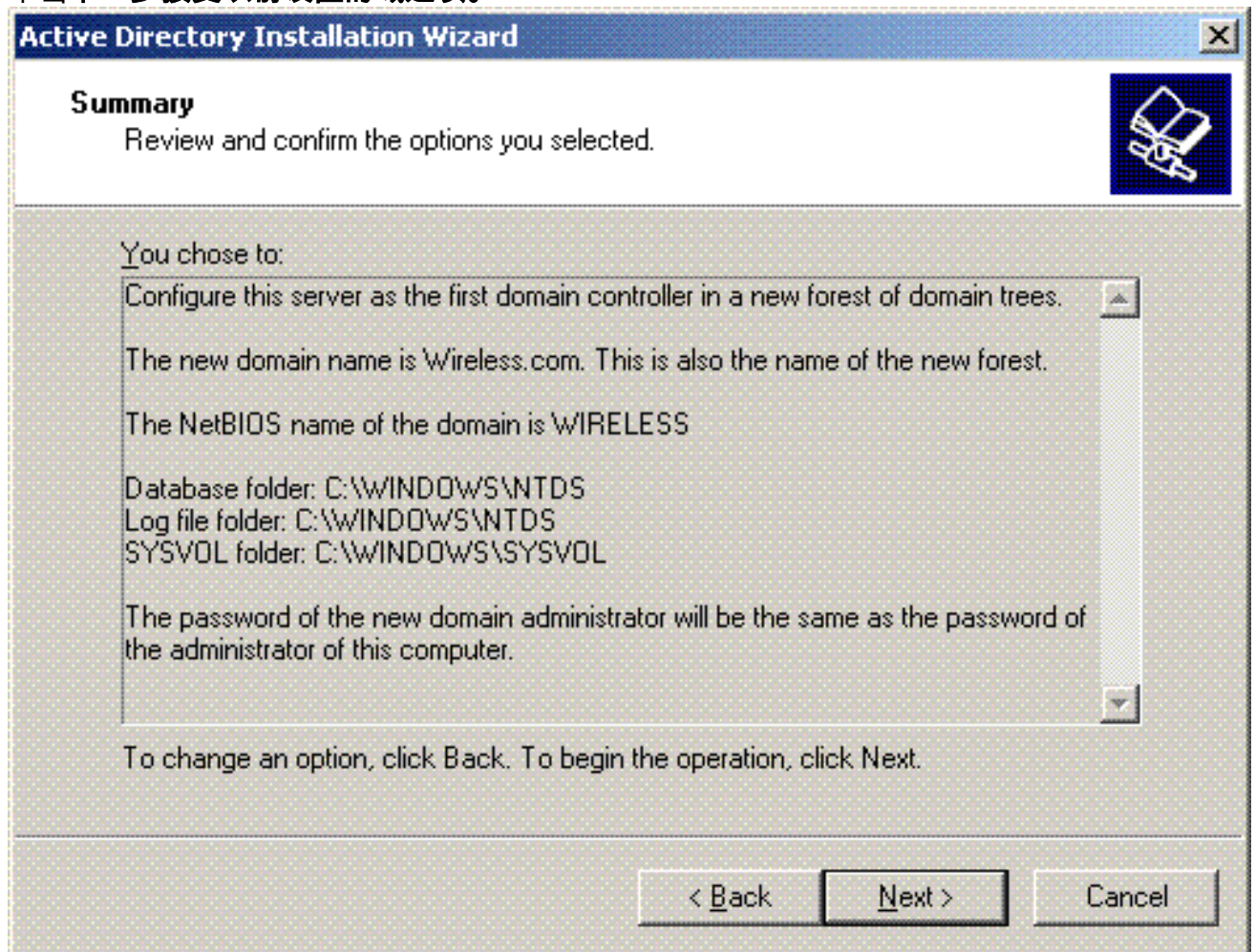
10. 选择用户和组的默认权限。单击 **Next**。



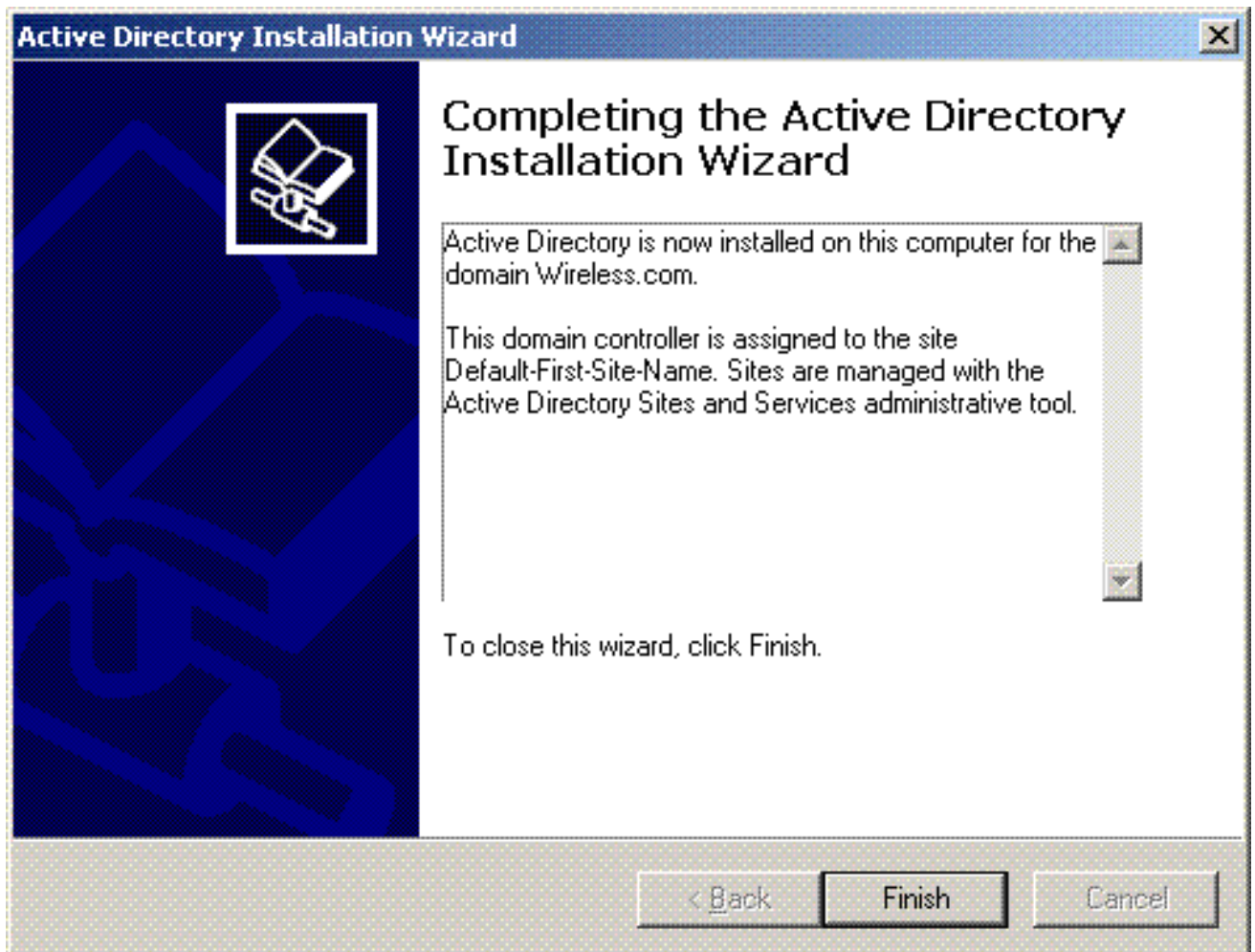
11. 设置管理员密码，然后单击下一步。



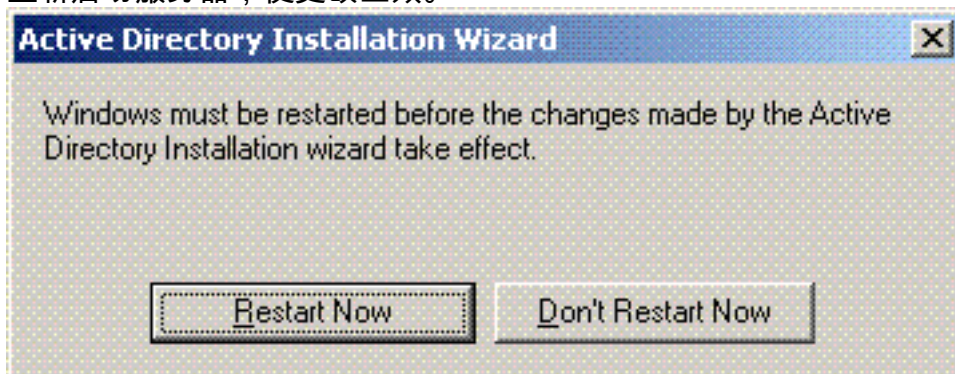
12. 单击下一步接受以前设置的域选项。



13. 单击完成关闭 Active Directory 安装向导。



14. 重新启动服务器，使更改生效。

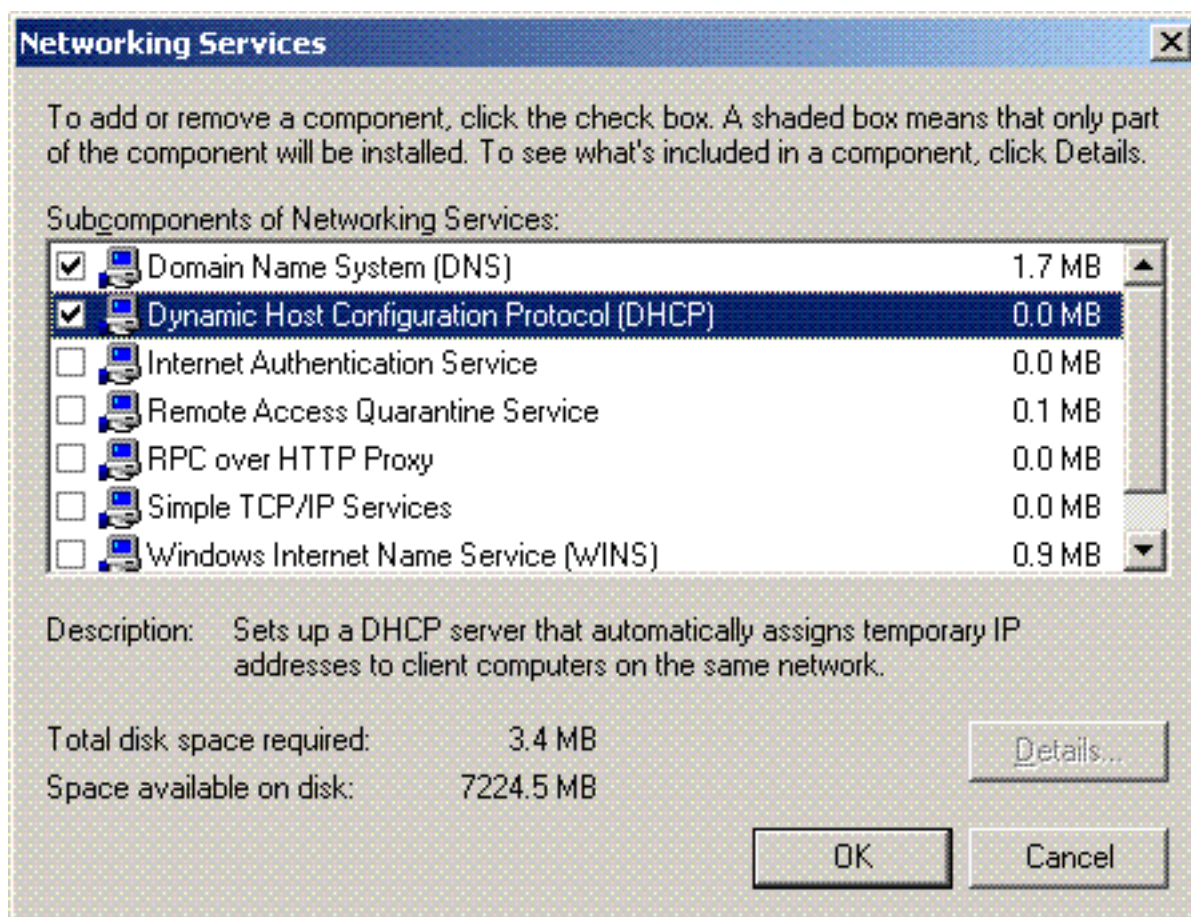


通过这些步骤，您已经将 Microsoft Windows 2003 Server 配置为域控制器，并且创建了新域 Wireless.com。下一步是在服务器上配置 DHCP 服务。

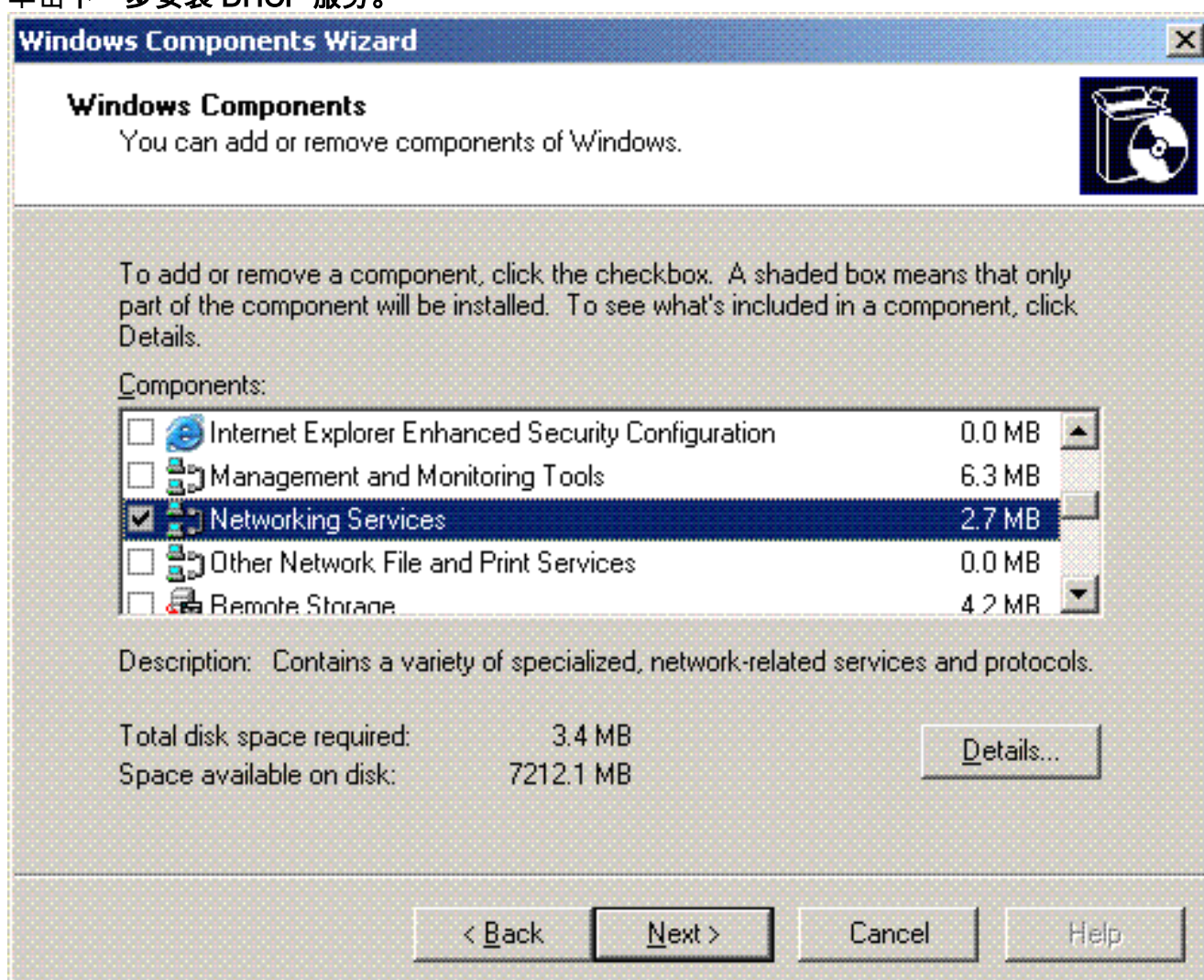
[在 Microsoft Windows 2003 Server 上安装和配置 DHCP 服务](#)

Microsoft 2003 Server 上的 DHCP 服务用于向无线客户端提供 IP 地址。要在此服务器上安装和配置 DHCP 服务，请完成以下步骤：

1. 在“控制面板”中单击添加或删除程序。
2. 单击添加/删除 Windows 组件。
3. 选择网络服务，然后单击“详细信息”。
4. 选择 Dynamic Host Configuration Protocol (DHCP)，然后单击 OK。



5. 单击下一步安装 DHCP 服务。



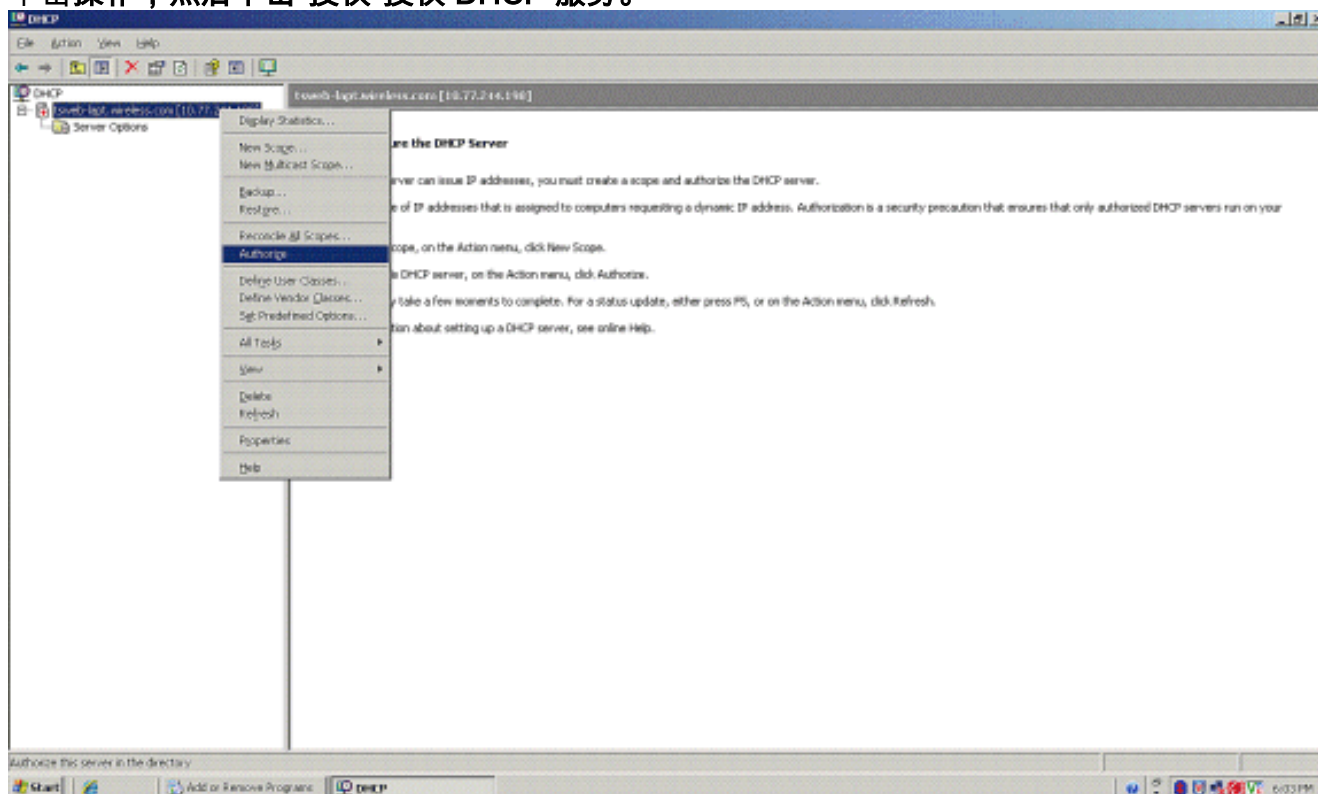
6. 单击完成完成安装。



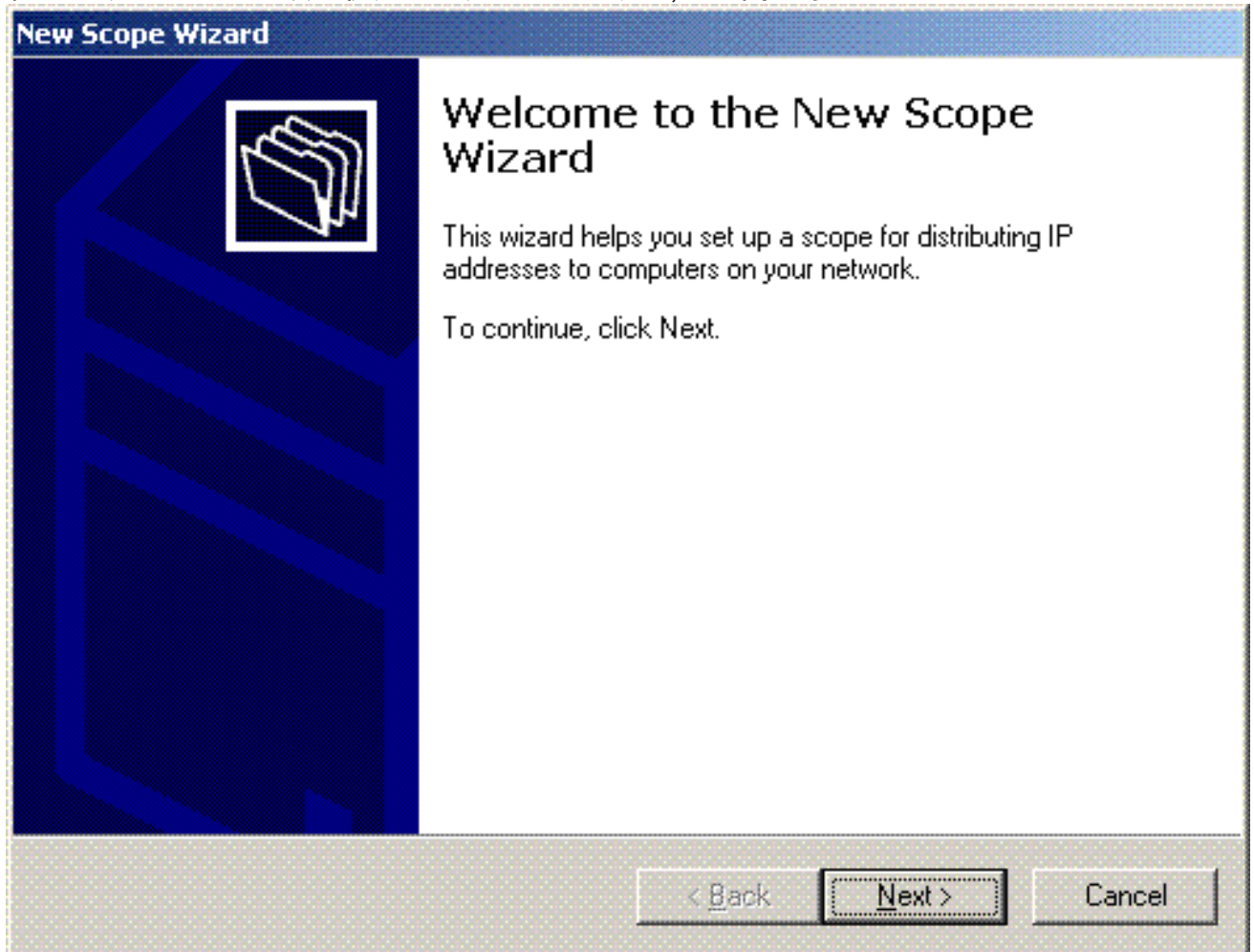
7. 要配置 DHCP 服务，请单击开始 > 程序 > 管理工具，然后单击 DHCP 管理单元。

8. 选择 DHCP 服务器 - tsweb-lapt.wireless.com (在本示例中)。

9. 单击操作，然后单击“授权”授权 DHCP 服务。



10. 在控制台树中，右键单击 `tsweb-lapt.wireless.com`，然后单击“新建范围”为无线客户端定义 IP 地址范围。
11. 在“新建范围”向导的“欢迎使用新建范围向导”页上，单击下一步。



12. 在“范围名称”页上，键入 DHCP 范围的名称。本示例中使用 `DHCP-Clients` 作为范围名称。单击 **Next**。

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 地址范围”页上，输入范围的开始和结束 IP 地址，然后单击下一步。

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:

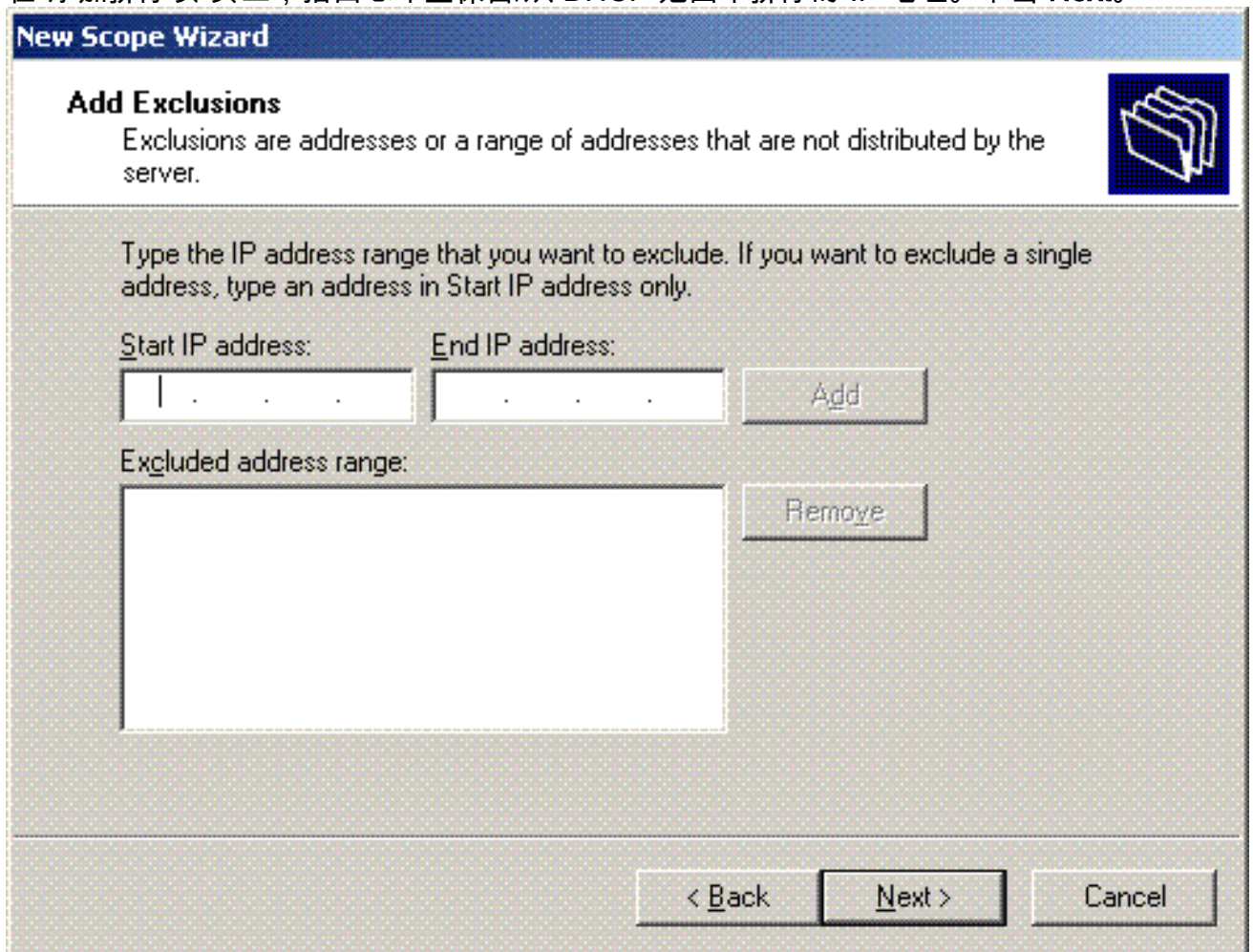
End IP address:

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“添加排除项”页上，指出您希望保留/从 DHCP 范围中排除的 IP 地址。单击 **Next**。



The screenshot shows a window titled "New Scope Wizard" with a sub-header "Add Exclusions". Below the sub-header is a descriptive text: "Exclusions are addresses or a range of addresses that are not distributed by the server." To the right of this text is a folder icon. The main area contains instructions: "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." Below this are two input fields: "Start IP address:" and "End IP address:". To the right of the "End IP address:" field is an "Add" button. Below these fields is a larger text area labeled "Excluded address range:" and a "Remove" button to its right. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

15. 在“租期”页上，指定租期，然后单击下一步。

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“配置 DHCP 选项”页上，选择是，我要立即配置 DHCP 选项，然后单击“下一步”。

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. 如果有默认的网关路由器，请在“路由器（默认网关）”页上指定网关路由器的 IP 地址，然后单击下一步。

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:

10.77.244.220

Add

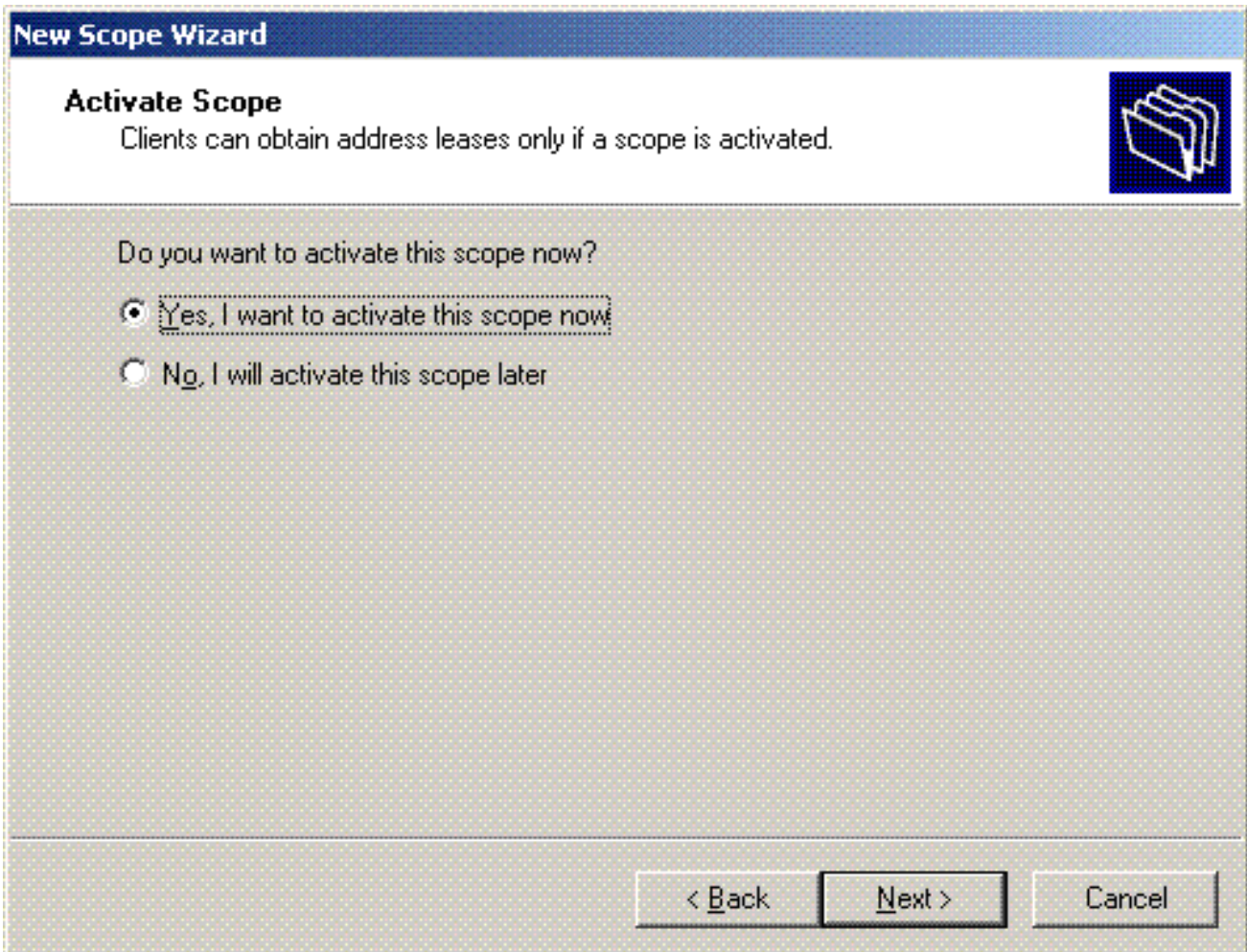
Remove

Up

Down

< Back Next > Cancel

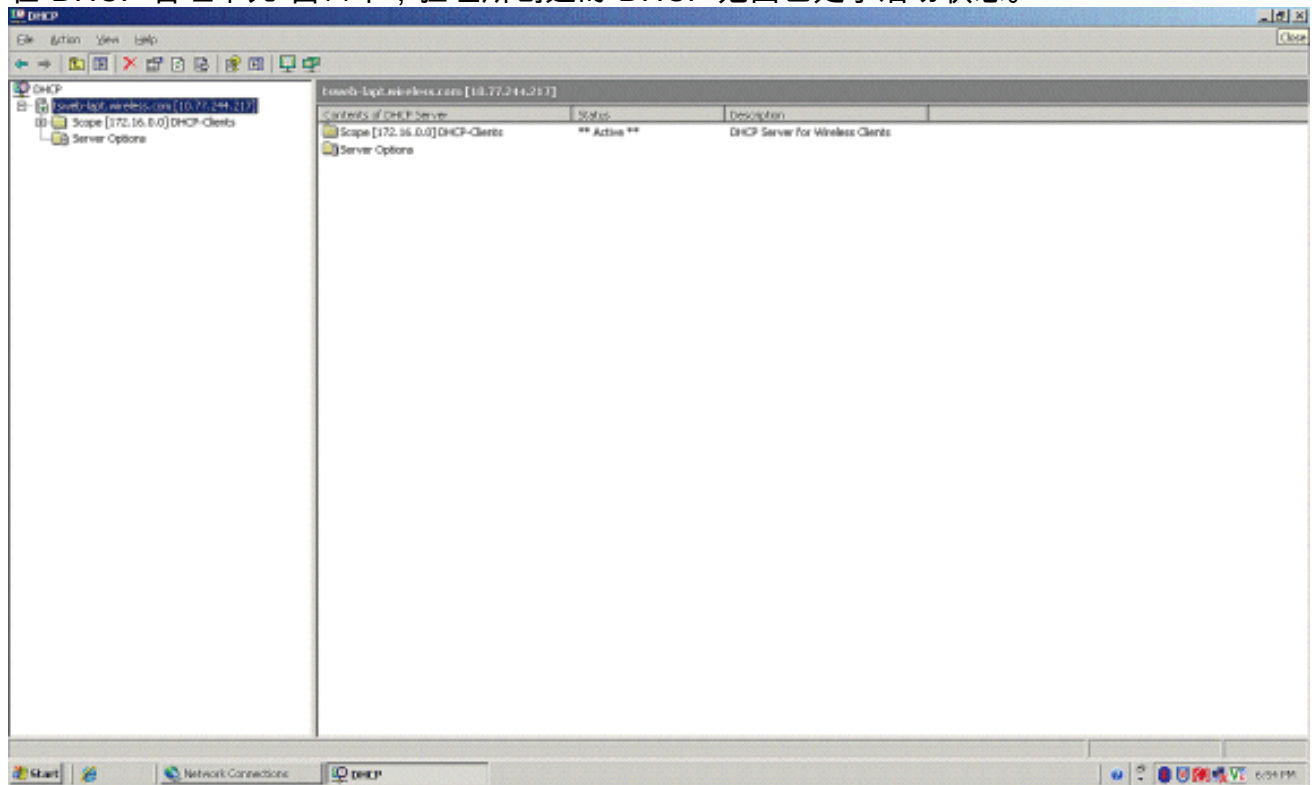
18. 在“域名和 DNS 服务器”页上，键入以前配置的域名。本示例中使用 **Wireless.com**。输入服务器的 IP 地址。单击 **Add**。



22. 在“完成新建范围”向导页上，单击完成。



23. 在“DHCP 管理单元”窗口中，验证所创建的 DHCP 范围已处于活动状态。



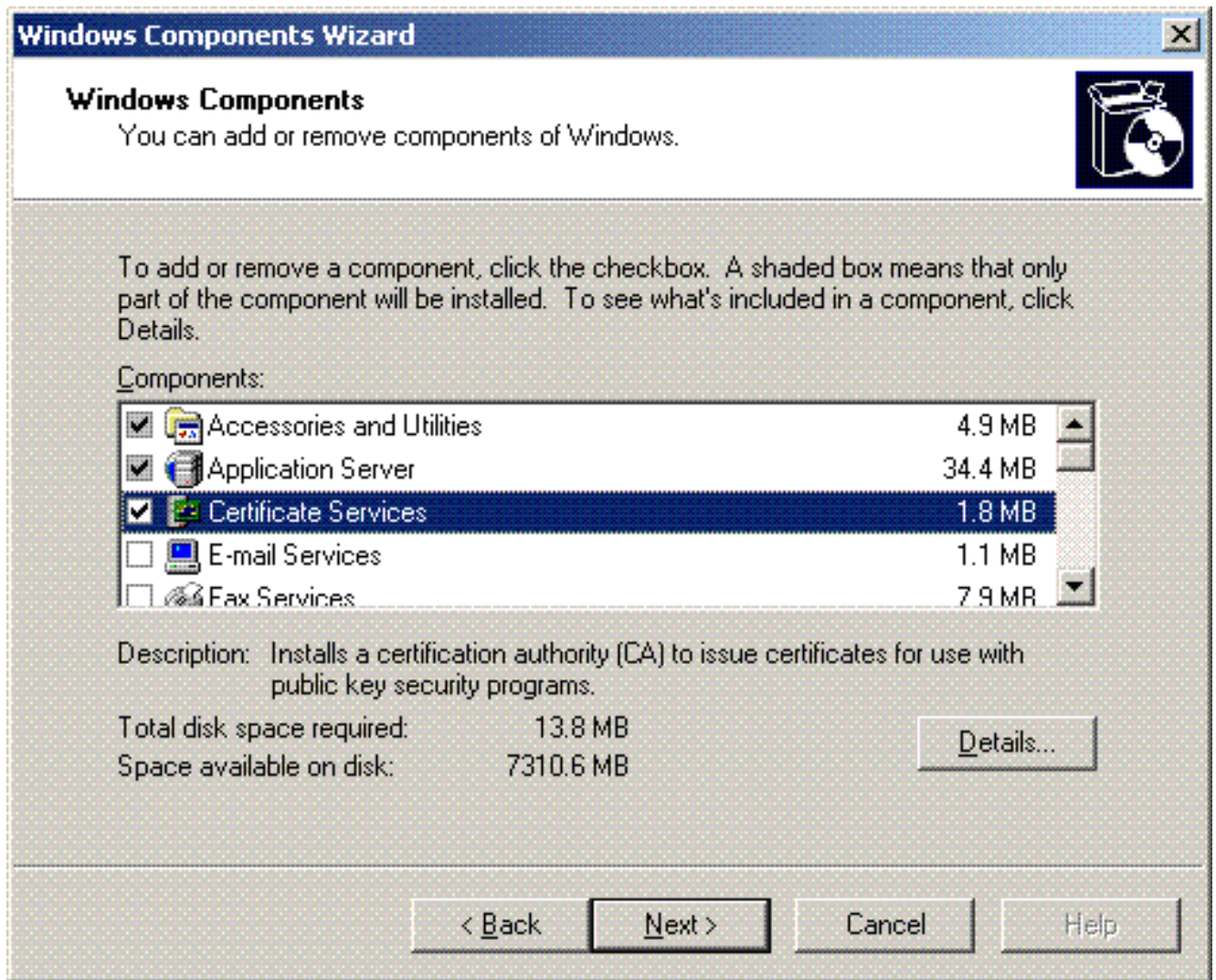
在服务器上启用DHCP/DNS后，请将该服务器配置为企业证书颁发机构(CA)服务器。

[安装并配置Microsoft Windows 2003 Server作为证书颁发机构\(CA\)服务器](#)

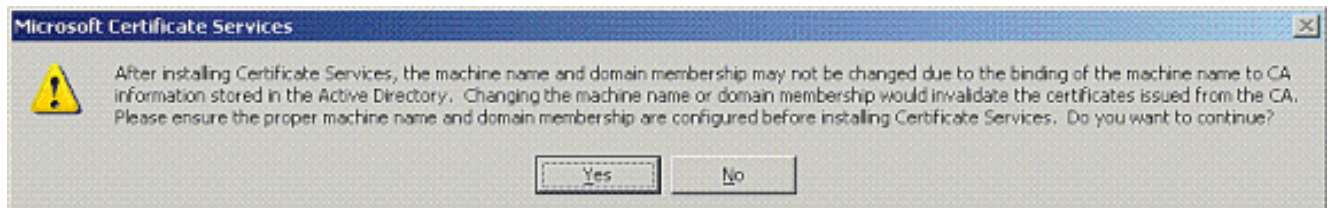
具有 EAP-MS-CHAPv2 的 PEAP 可根据服务器上现有的证书来验证 RADIUS 服务器。此外，服务器证书必须由受客户端计算机信任的公共证书颁发机构(CA)颁发（即，公共CA证书已经存在于客户端计算机证书存储库的受信任的根证书颁发机构文件夹中）。在本示例中，将Microsoft Windows 2003服务器配置为向Internet身份验证服务(IAS)颁发证书的证书颁发机构(CA)。

要在此服务器上安装和配置证书服务，请完成以下步骤：

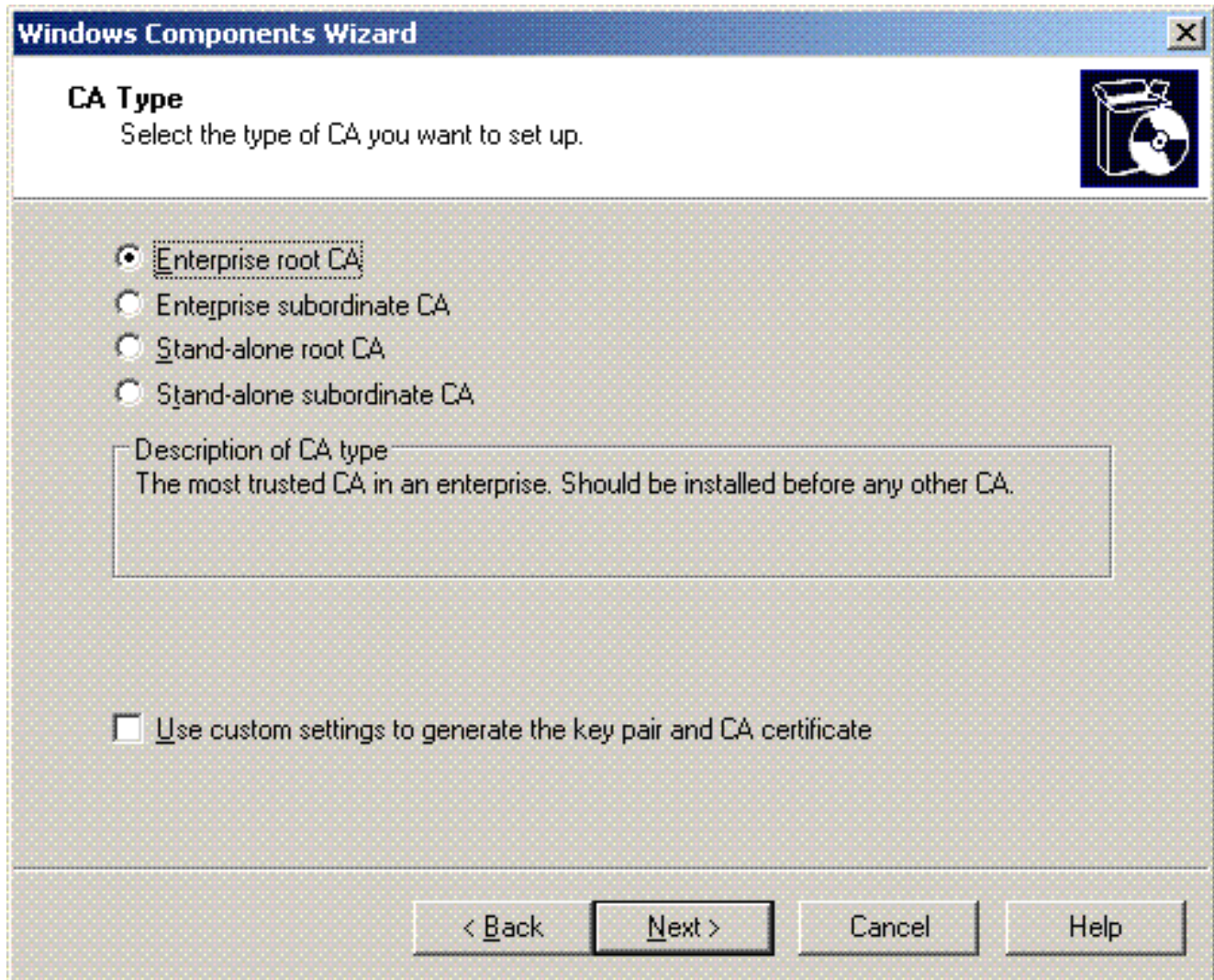
1. 在“控制面板”中单击**添加或删除程序**。
2. 单击添加/删除 Windows 组件。
3. 单击**证书服务**。



4. 在显示警告消息“安装证书服务后，就不能重命名此计算机，也不能将其加入域或从域中删除”时，单击是。是否要继续？




5. 在“证书颁发机构类型”下，选择企业根 CA，然后单击“下一步”。



6. 输入用于标识 CA 的名称。本示例使用 **Wireless-CA**。单击 **Next**。

Windows Components Wizard X

CA Identifying Information 
Enter information to identify this CA.

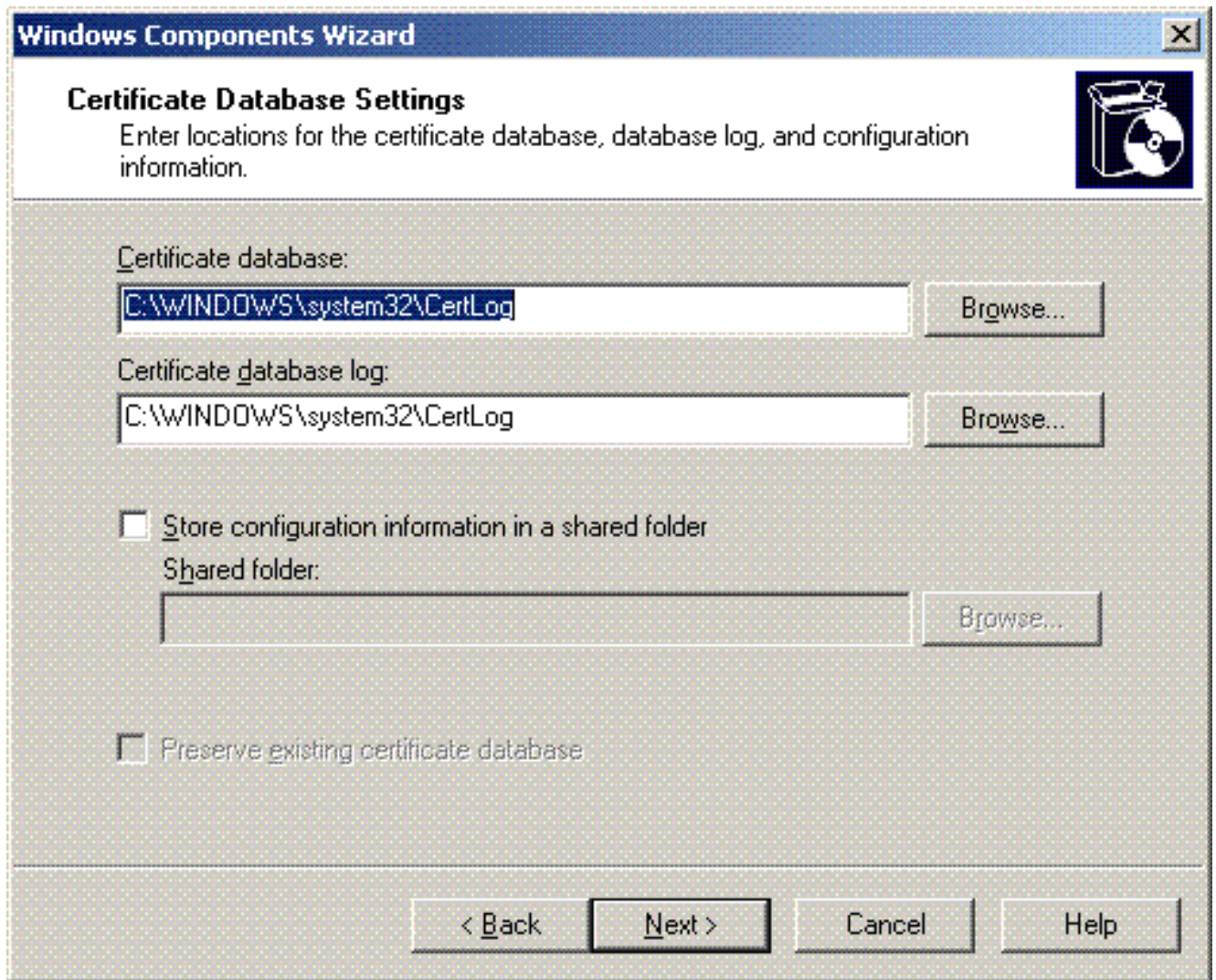
Common name for this CA:

Distinguished name suffix:

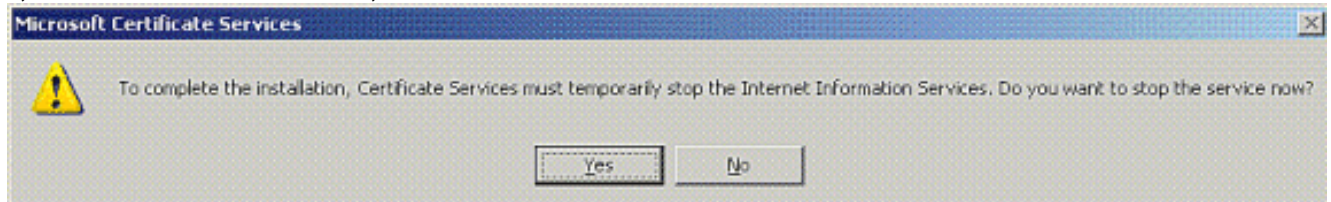
Preview of distinguished name:

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

7. 这就为证书数据库存储创建了一个“证书日志”目录。单击 **Next**。



8. 如果 IIS 是启用的，则必须先将其停止，才能继续操作。在显示必须停止 IIS 的警告消息时，单击**确定**。安装 CA 后，它会自动重新启动。



9. 单击**Finish**完成证书颁发机构(CA)服务的安装。

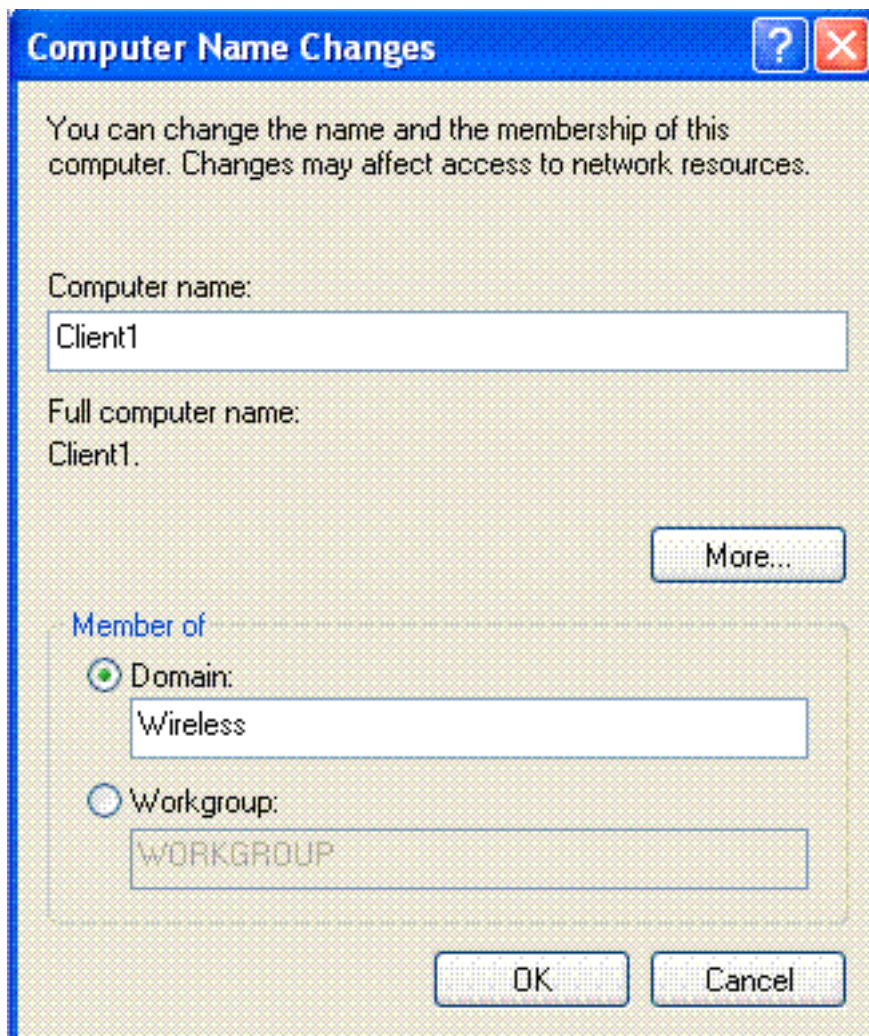


下一步是在 Microsoft Windows 2003 Server 上安装和配置 Internet 身份验证服务。

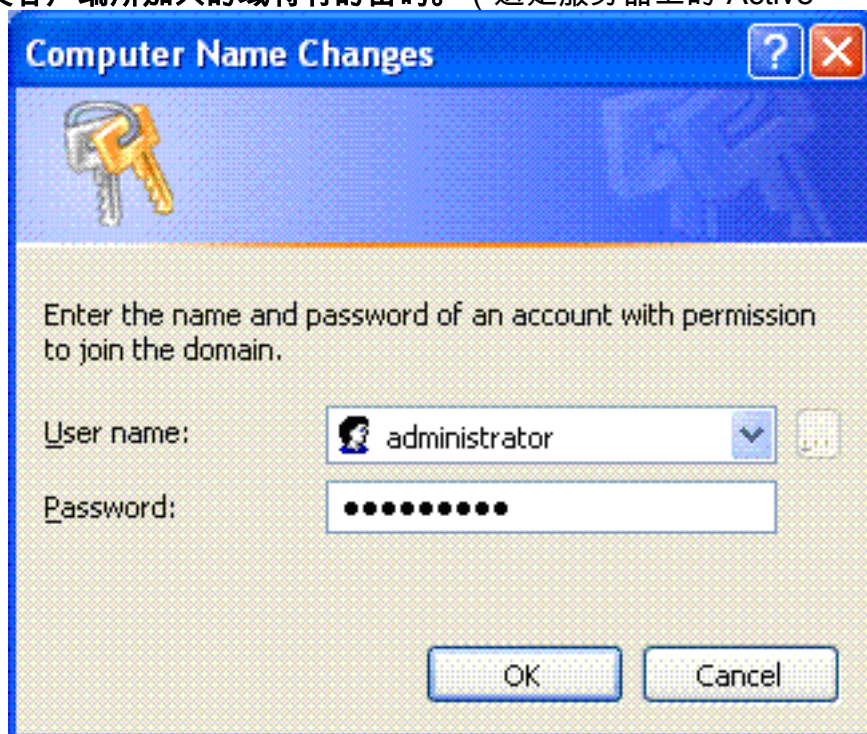
将客户端连接到域

下一步是将客户端连接到有线网络，并从新域下载域特有的信息。也就是说，将客户端连接到域。为此，请完成以下步骤：

1. 使用直通以太网电缆将客户端连接到有线网络。
2. 启动客户端，并用客户端的用户名/密码进行登录。
3. 单击**开始**；单击**运行**；键入**cmd**；然后单击**确定**。
4. 在命令提示符下，键入 **ipconfig**，然后按 Enter 键，以便验证 DHCP 能够正常使用，并且客户端从 DHCP 服务器收到了 IP 地址。
5. 要将客户端加入域中，请右键单击我的电脑，然后选择“属性”。
6. 单击 **Computer Name** 选项卡。
7. 单击 **Change**。
8. 单击 **Domain**；键入 **wireless.com**；然后单击 **OK**。



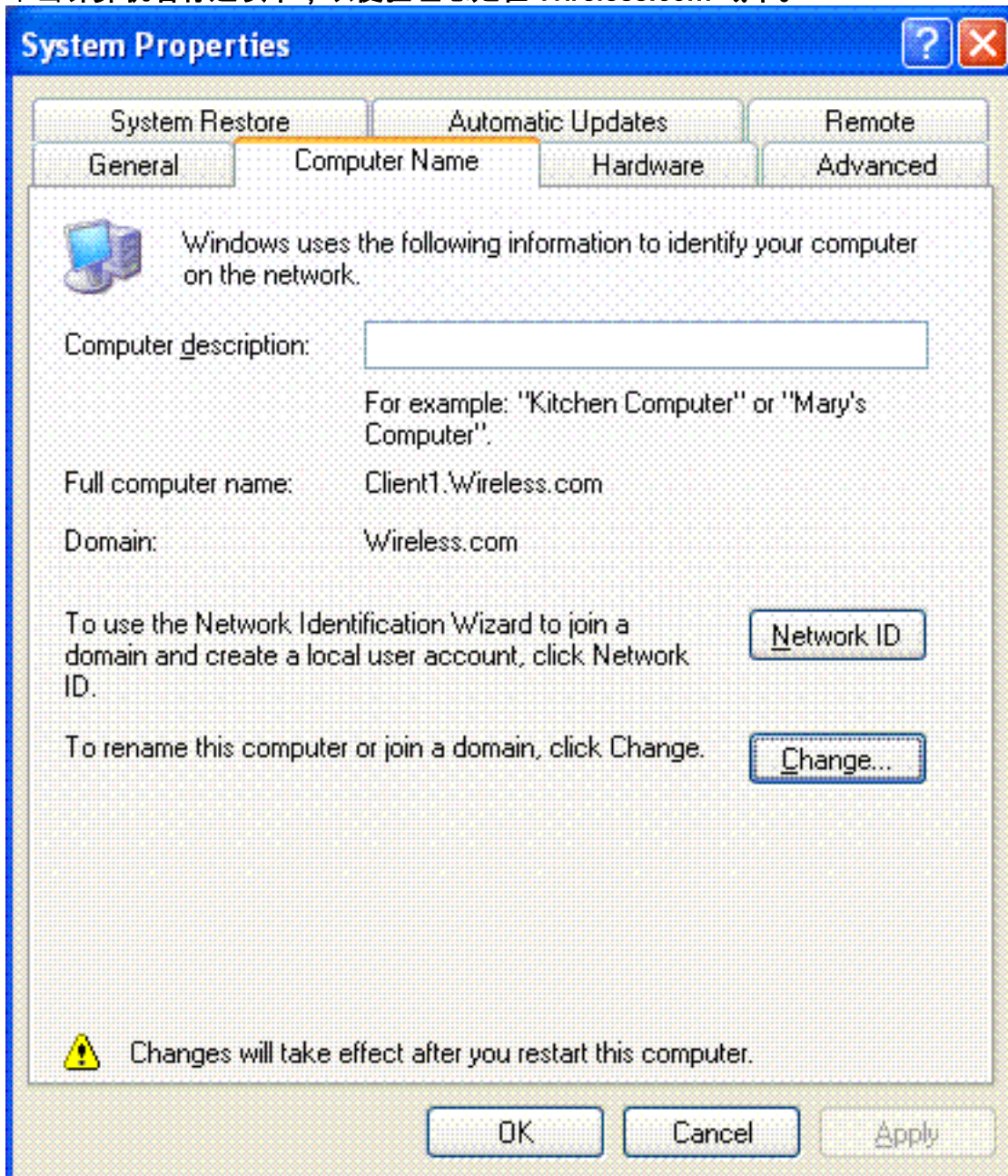
9. 键入用户名 Administrator 以及客户端所加入的域特有的密码。(这是服务器上的 Active



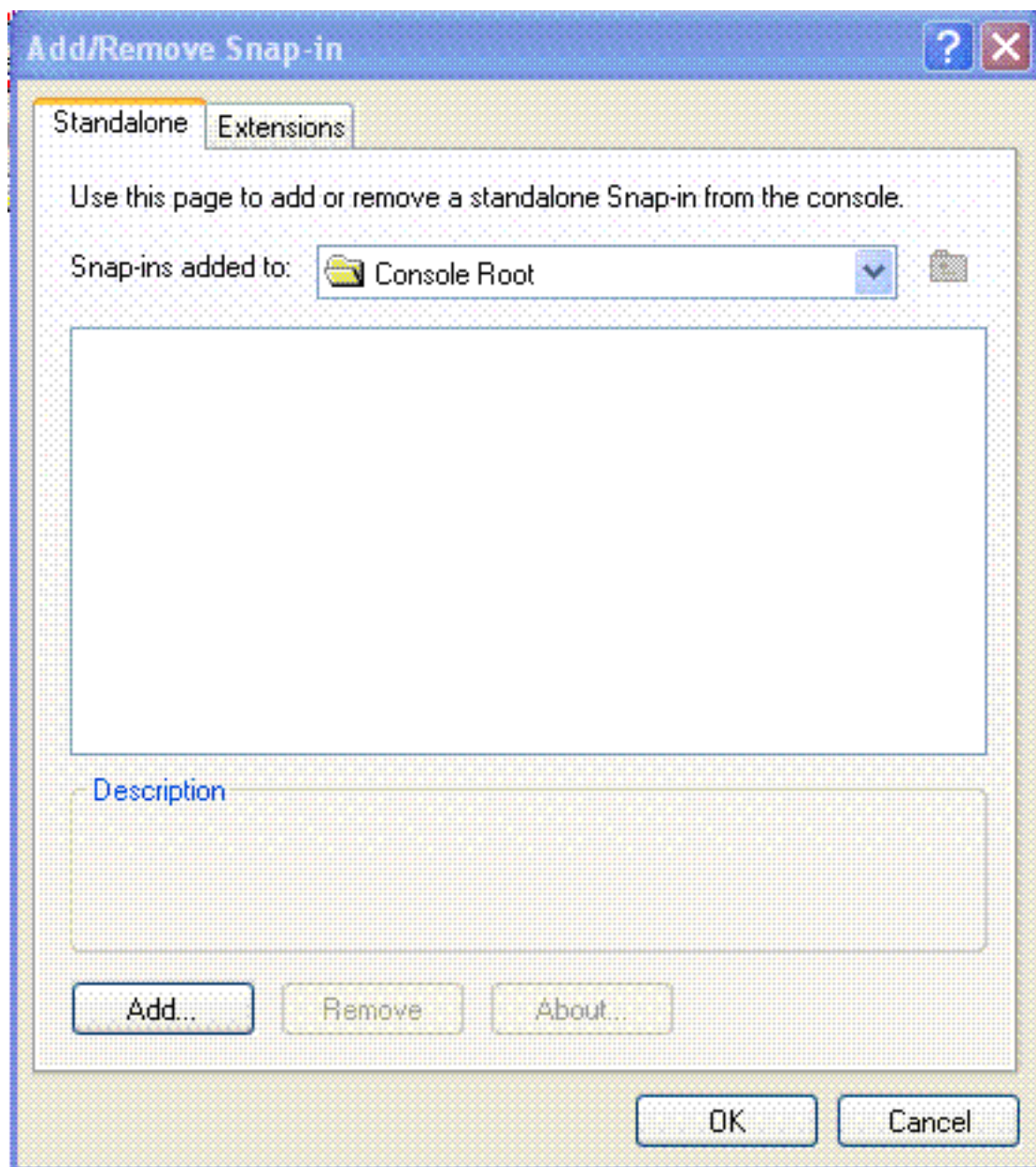
Directory 中的管理员帐户。)



10. Click OK.
11. 单击是重新启动计算机。
12. 计算机重新启动后，使用以下信息登录：用户名= Administrator；密码= <domain password>；域= Wireless。
13. 右键单击我的电脑，然后单击“属性”。
14. 单击计算机名称选项卡，以便验证您是在 Wireless.com 域中。

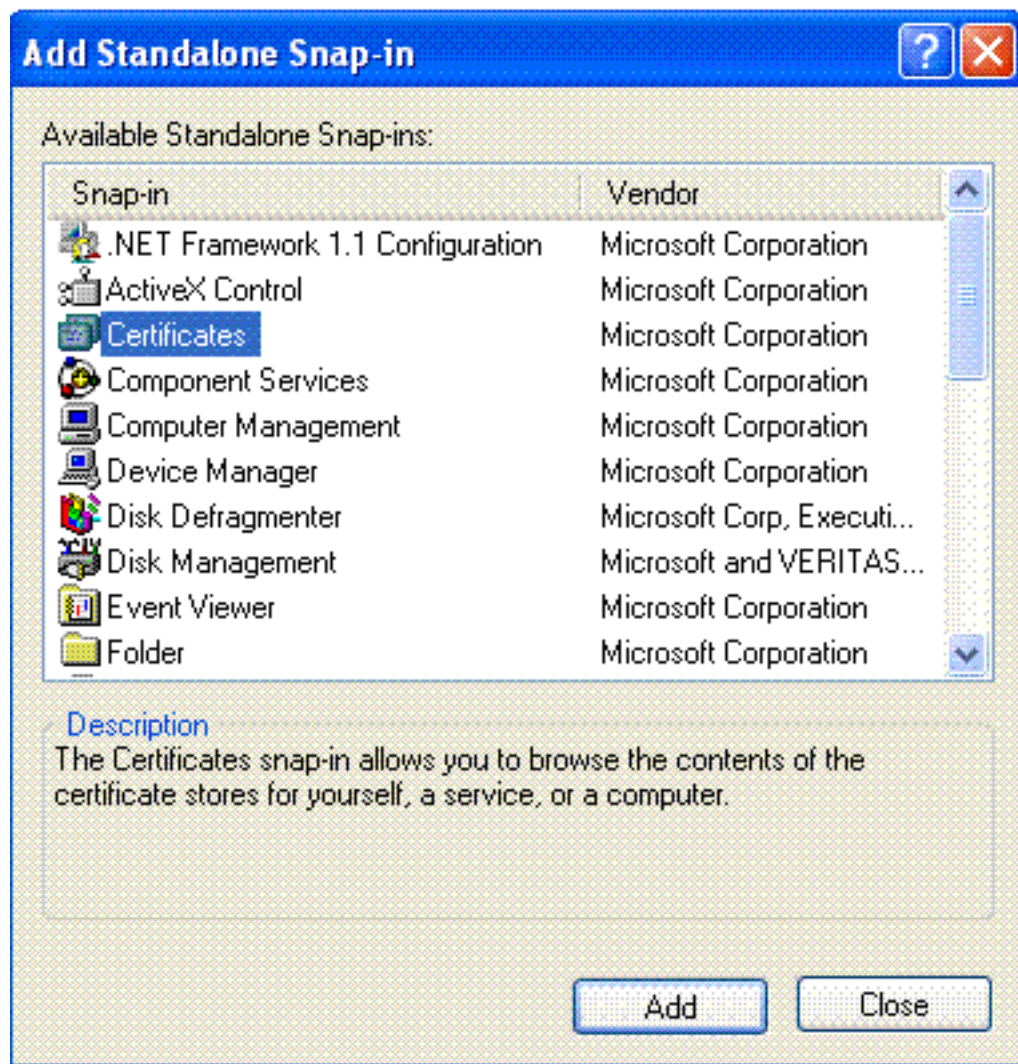


15. 下一步是验证客户端从服务器收到了 CA 证书（信任）。
16. 单击Start；单击Run；键入mmc，然后单击OK。
17. 单击文件，然后单击“添加/删除”管理单元。

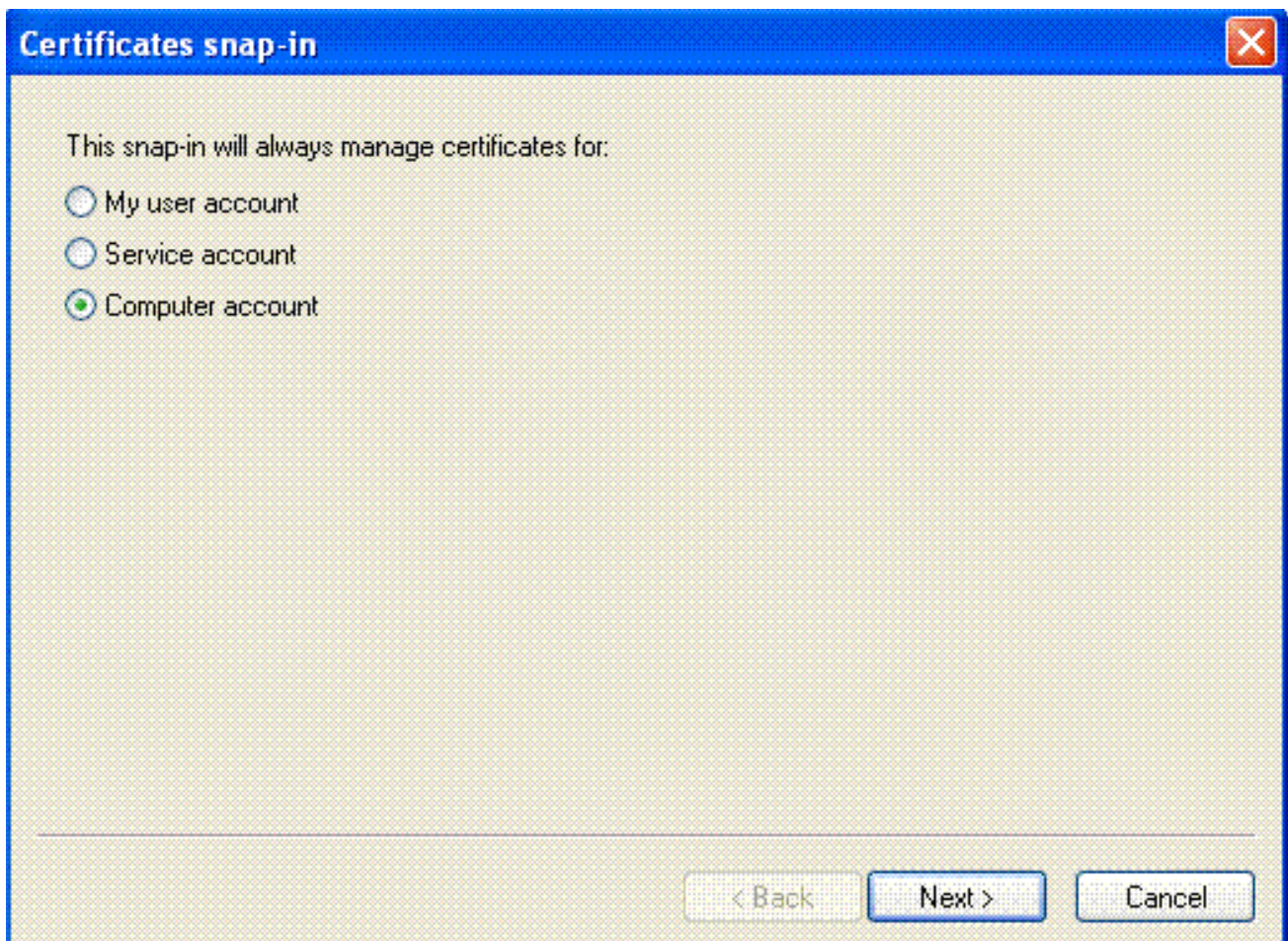


18. 单击 **Add**。

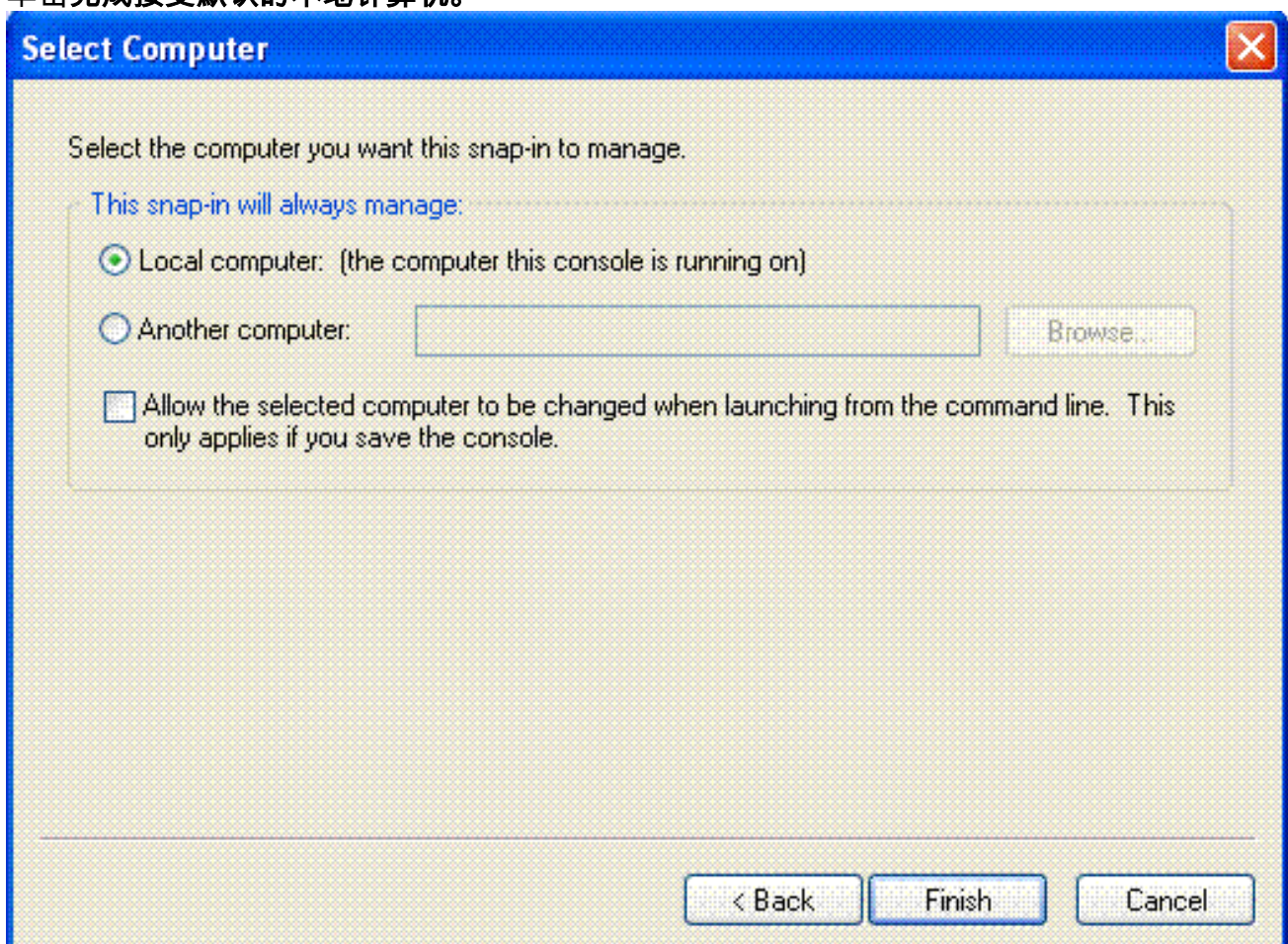
19. 选择**证书**，然后单击“添加”。



20. 选择计算机帐户，然后单击“下一步”。



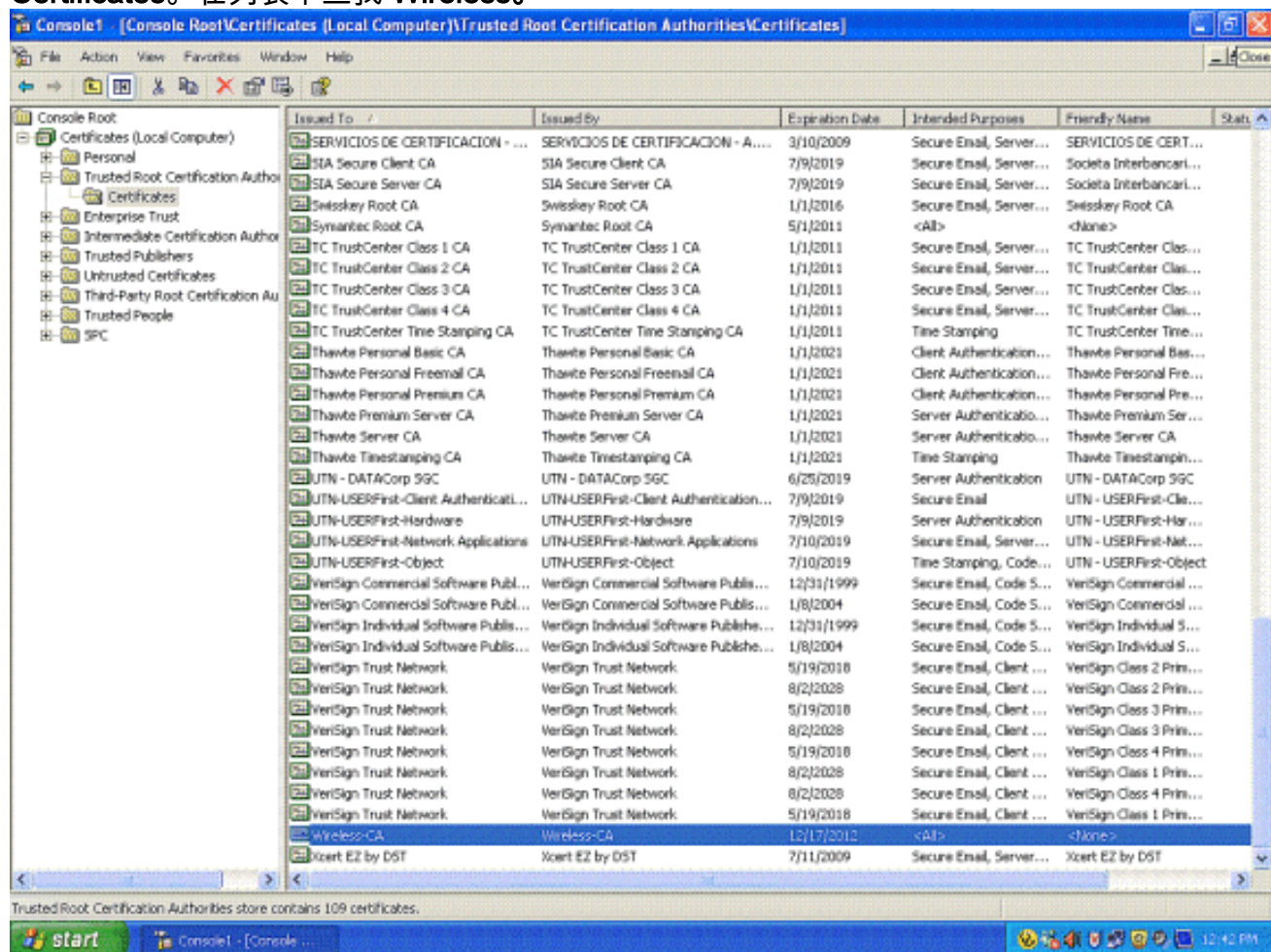
21. 单击完成接受默认的本地计算机。



22. 单击关闭，然后单击“确定”。

23. 展开Certificates(Local Computer)；展开Trusted Root Certification Authorities；然后单击

Certificates。在列表中查找 Wireless。



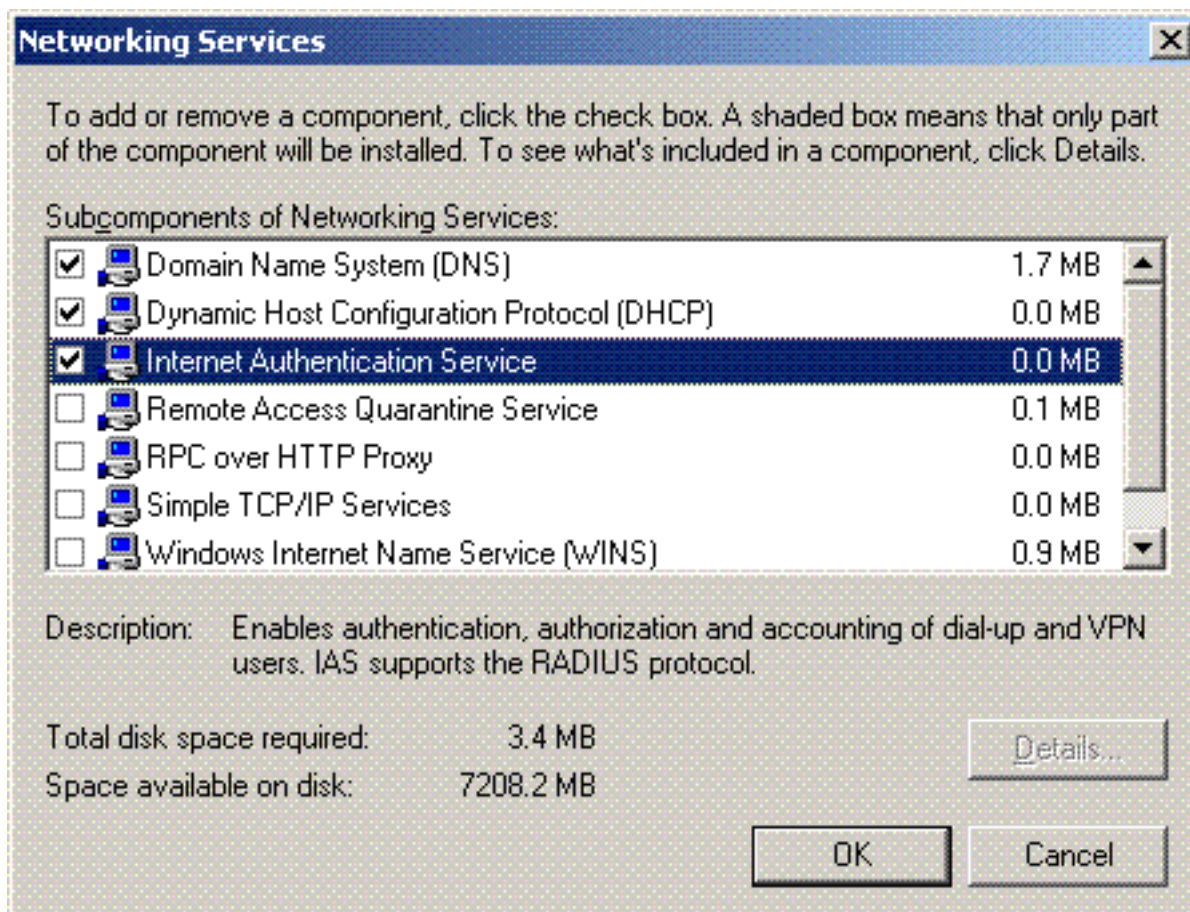
24. 重复此过程，以便将更多客户端添加到域中。

在 Microsoft Windows 2003 Server 上安装 Internet 身份验证服务并请求证书

在此设置中，Internet身份验证服务(IAS)用作RADIUS服务器，通过PEAP身份验证对无线客户端进行身份验证。

要在服务器上安装和配置 IAS，请完成以下步骤。

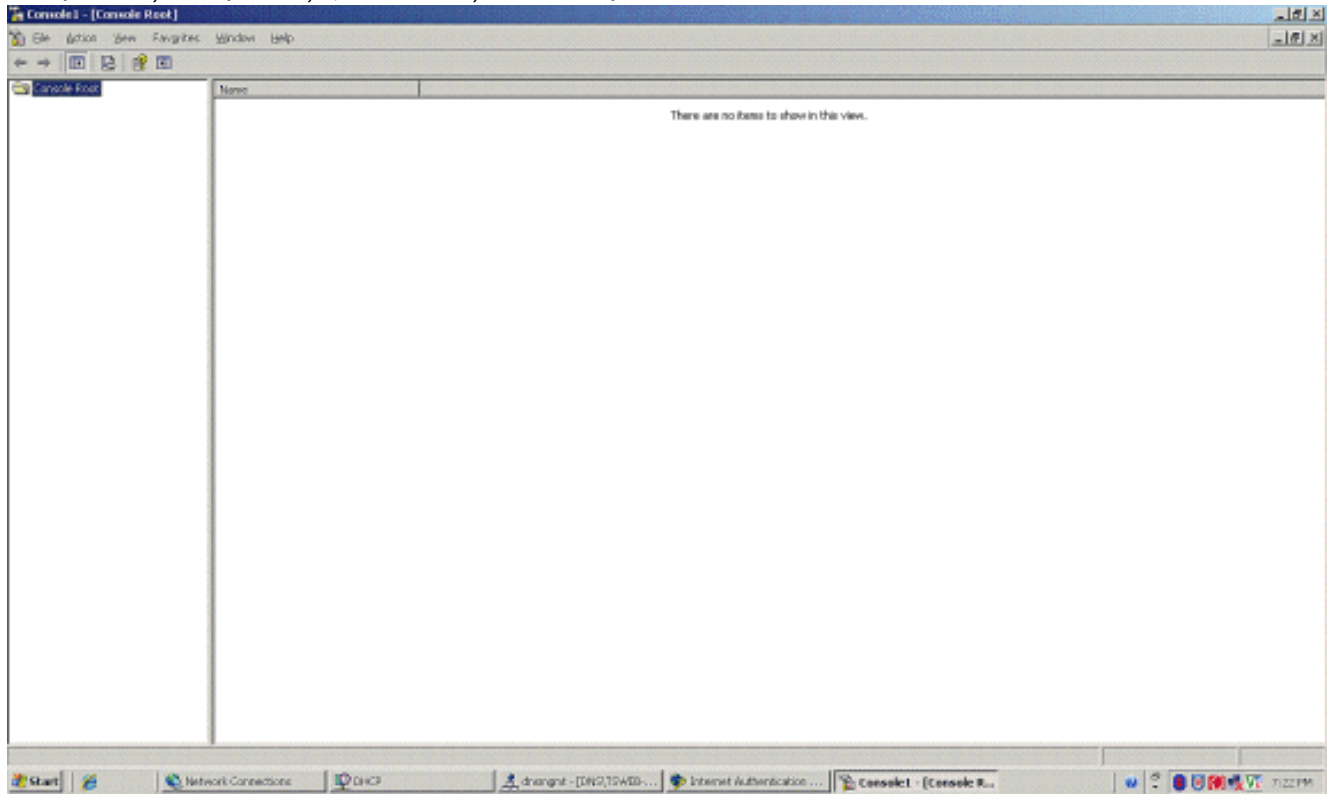
1. 在“控制面板”中单击**添加或删除程序**。
2. 单击**添加/删除 Windows 组件**。
3. 选择**网络服务**，然后单击“详细信息”。
4. 选择**Internet Authentication Service**；单击**OK**；然后单击**Next**。



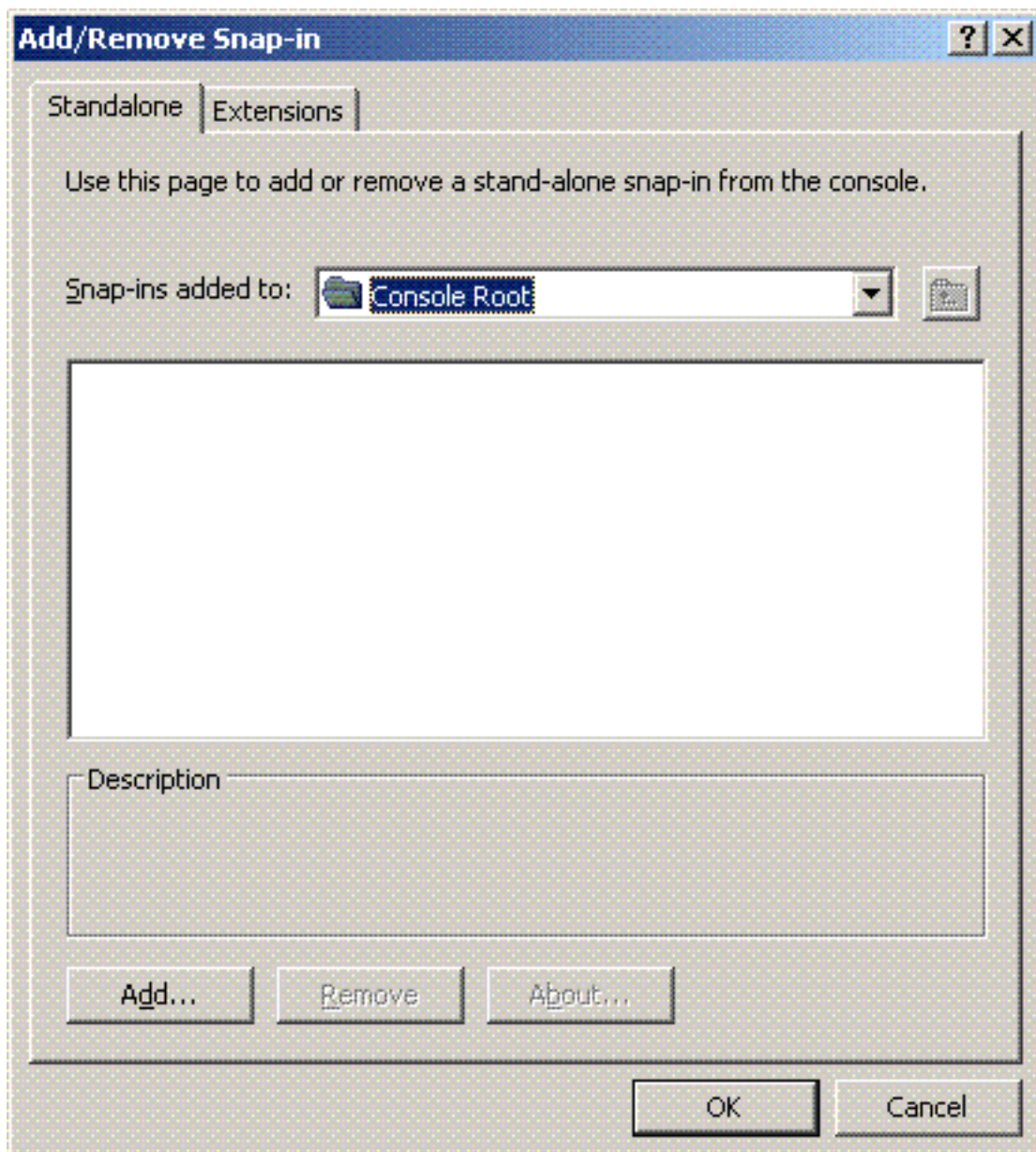
5. 单击完成完成 IAS 的安装。



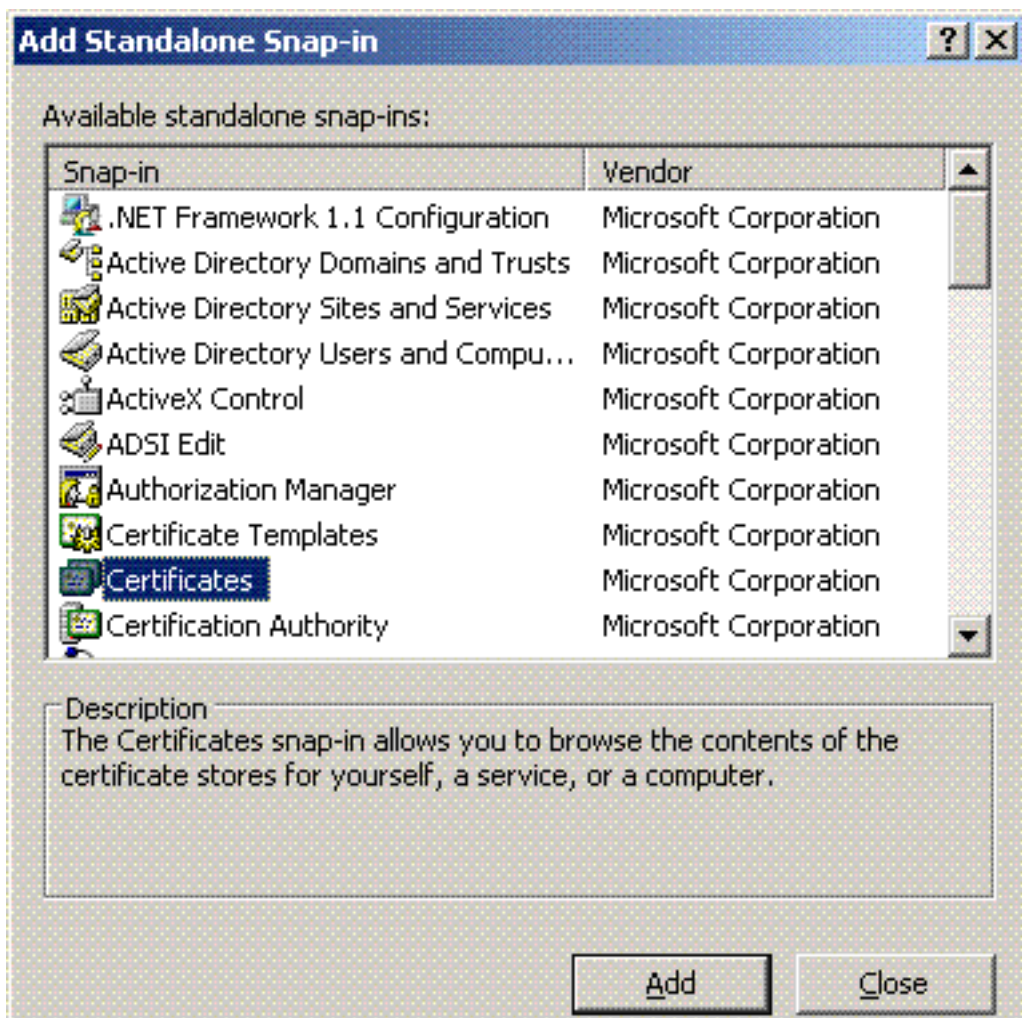
6. 下一步是安装Internet身份验证服务(IAS)的计算机证书。
7. 单击**Start**；单击**Run**；键入**mmc**；然后单击**OK**。



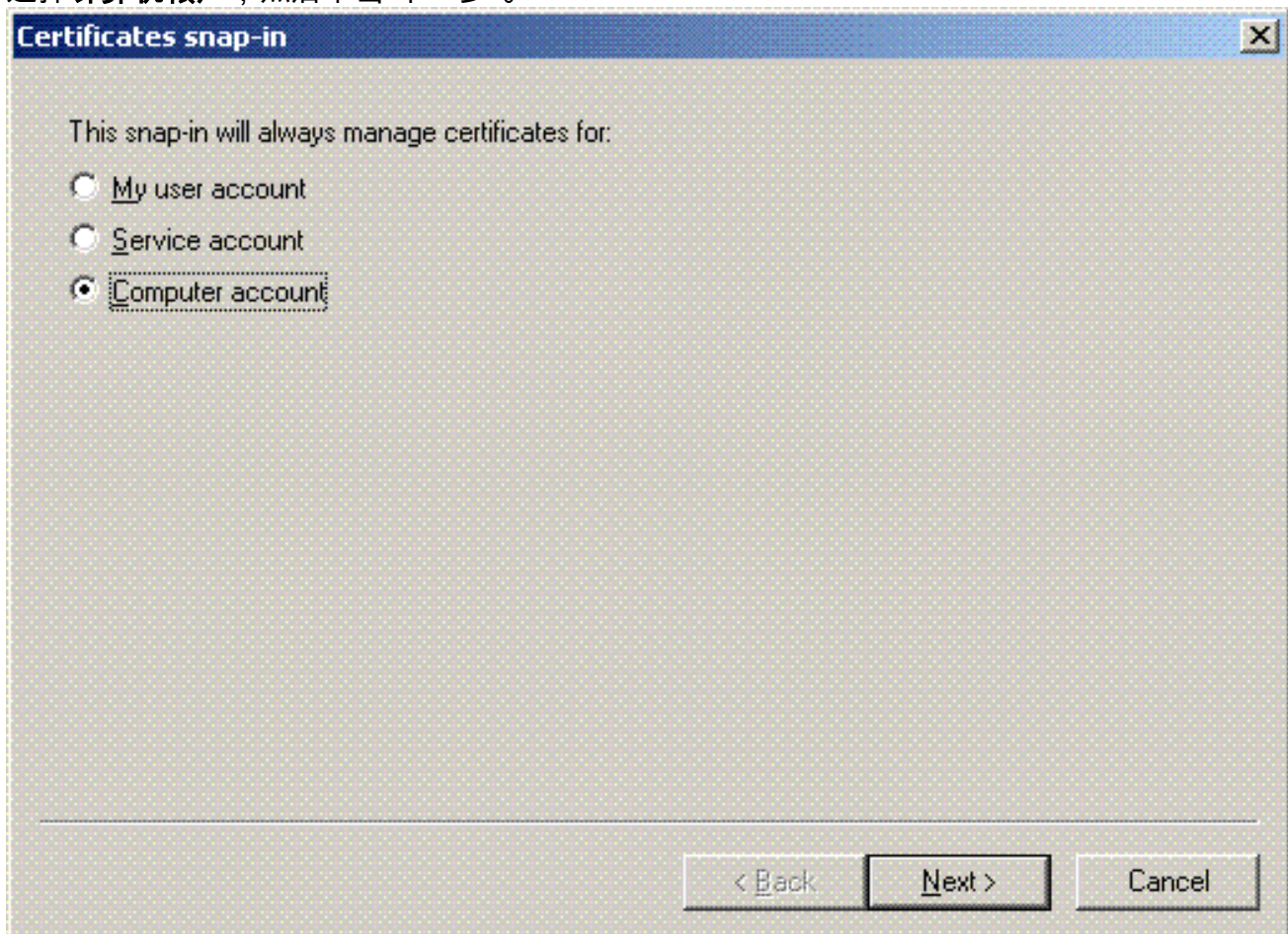
8. 在文件菜单中单击**控制台**，然后选择“**添加/删除**”管理单元。
9. 单击**添加**添加管理单元。



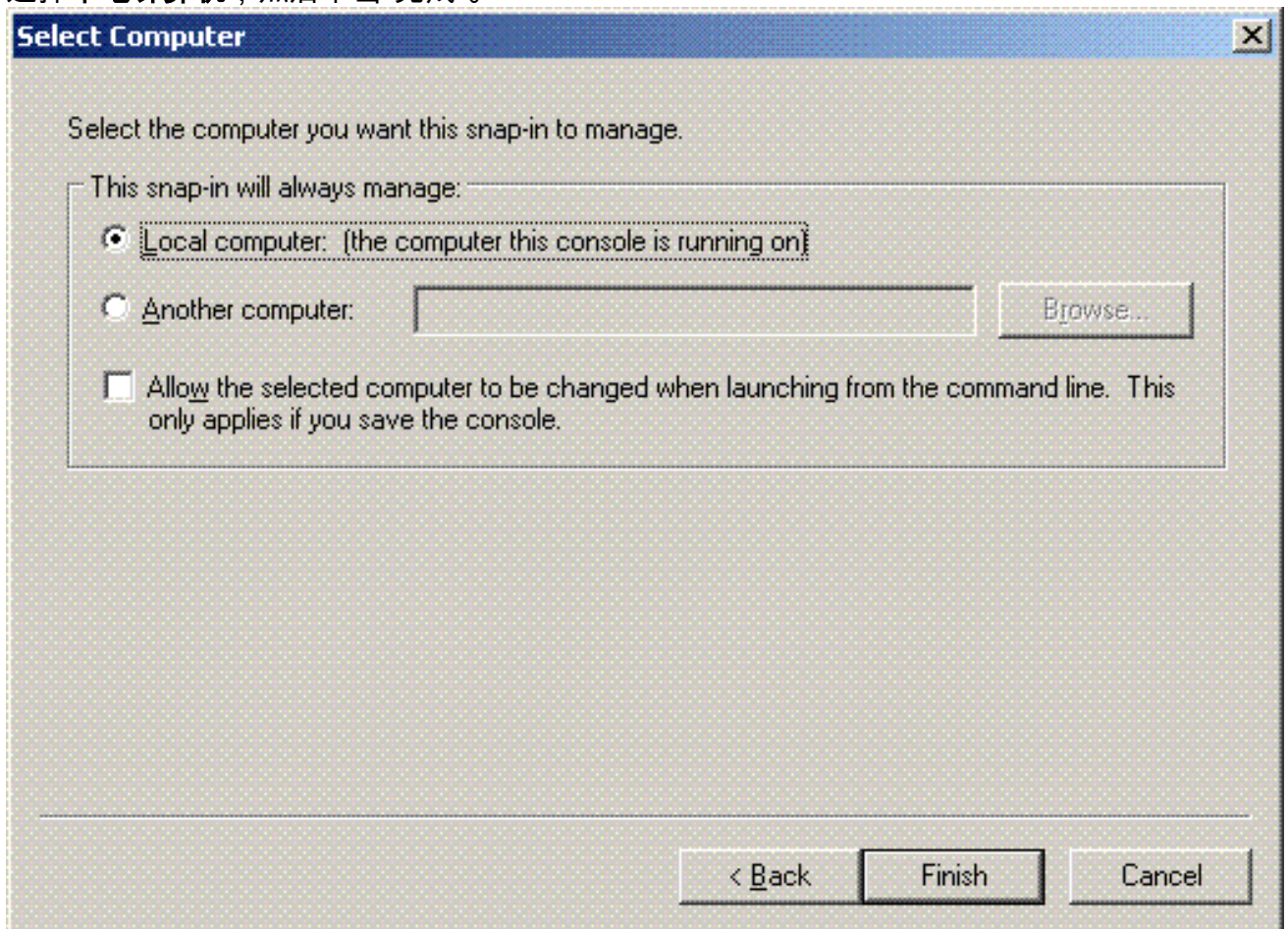
10. 从管理单元列表中选择证书，然后单击“添加”。



11. 选择计算机帐户，然后单击“下一步”。

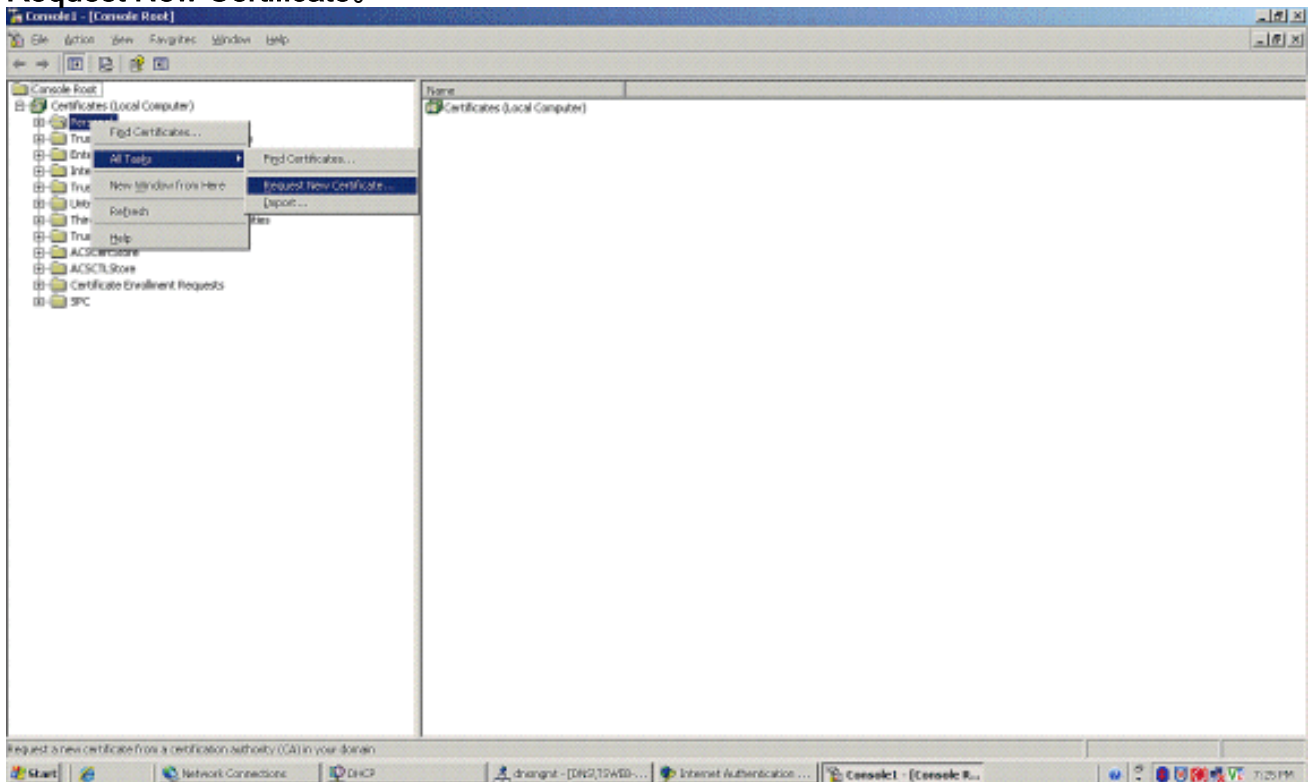


12. 选择本地计算机，然后单击“完成”。



13. 单击关闭，然后单击“确定”。

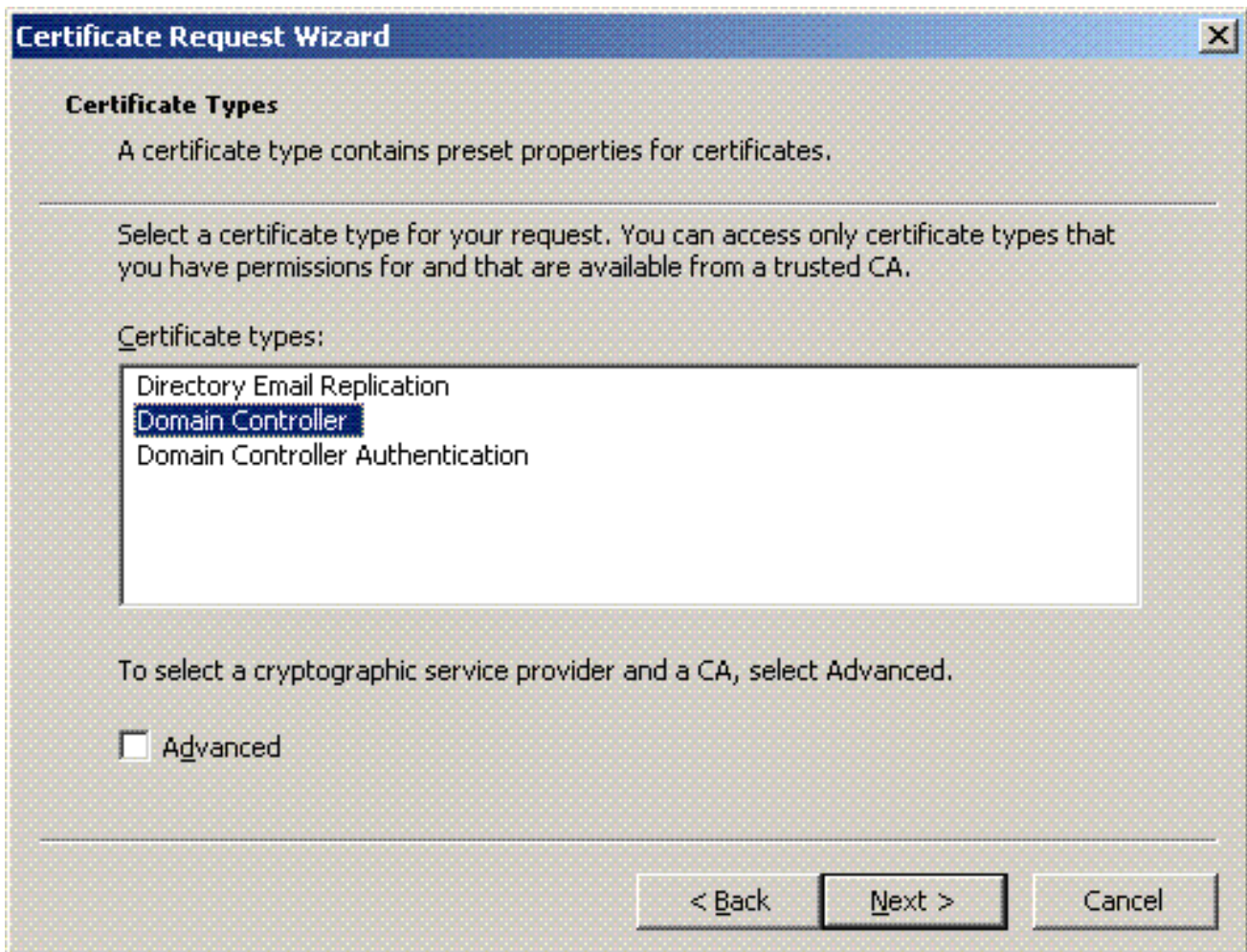
14. 展开Certificates(Local Computer)；右键单击Personal folder；选择All tasks，然后选择Request New Certificate。



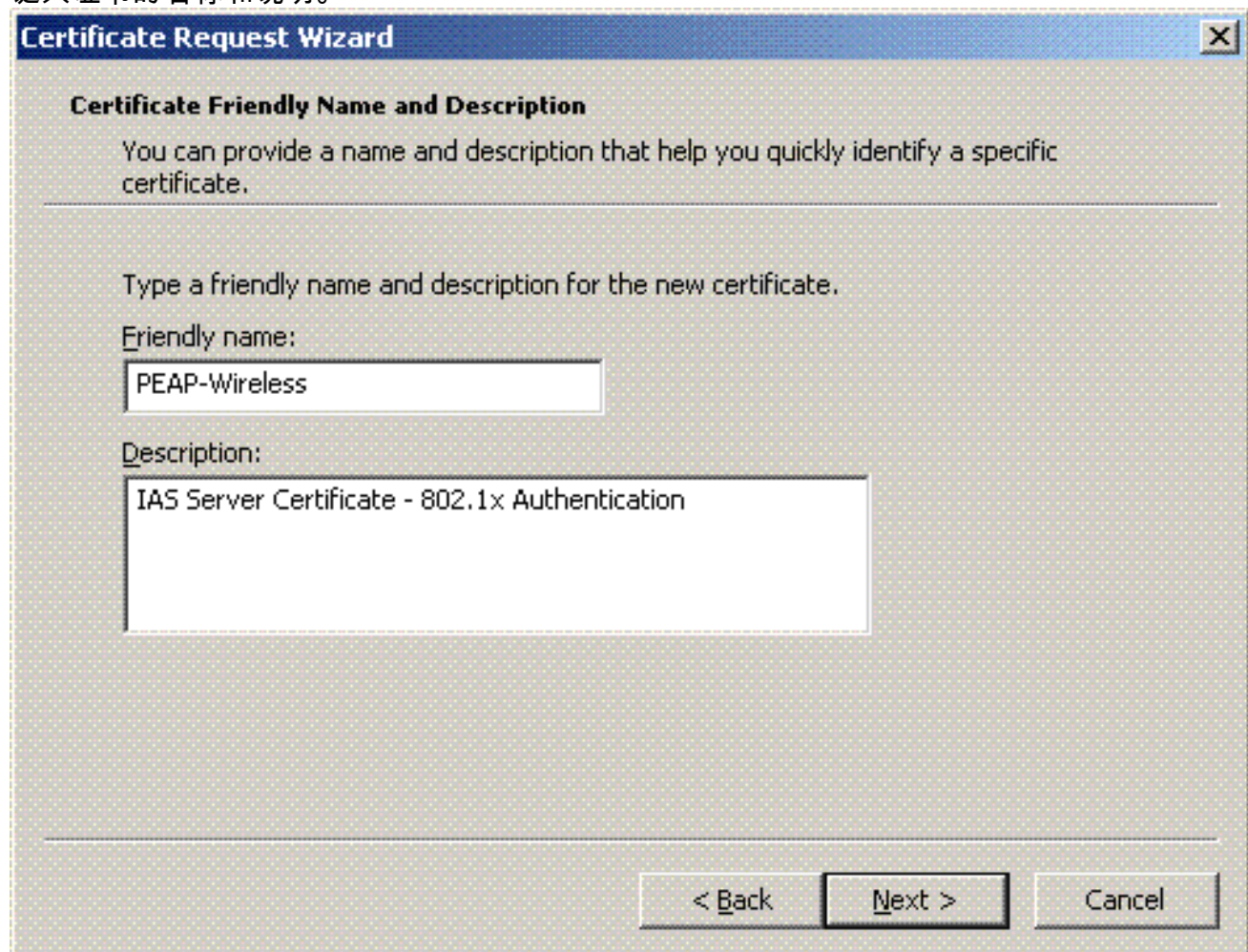
15. 在欢迎使用证书请求向导上，单击下一步。



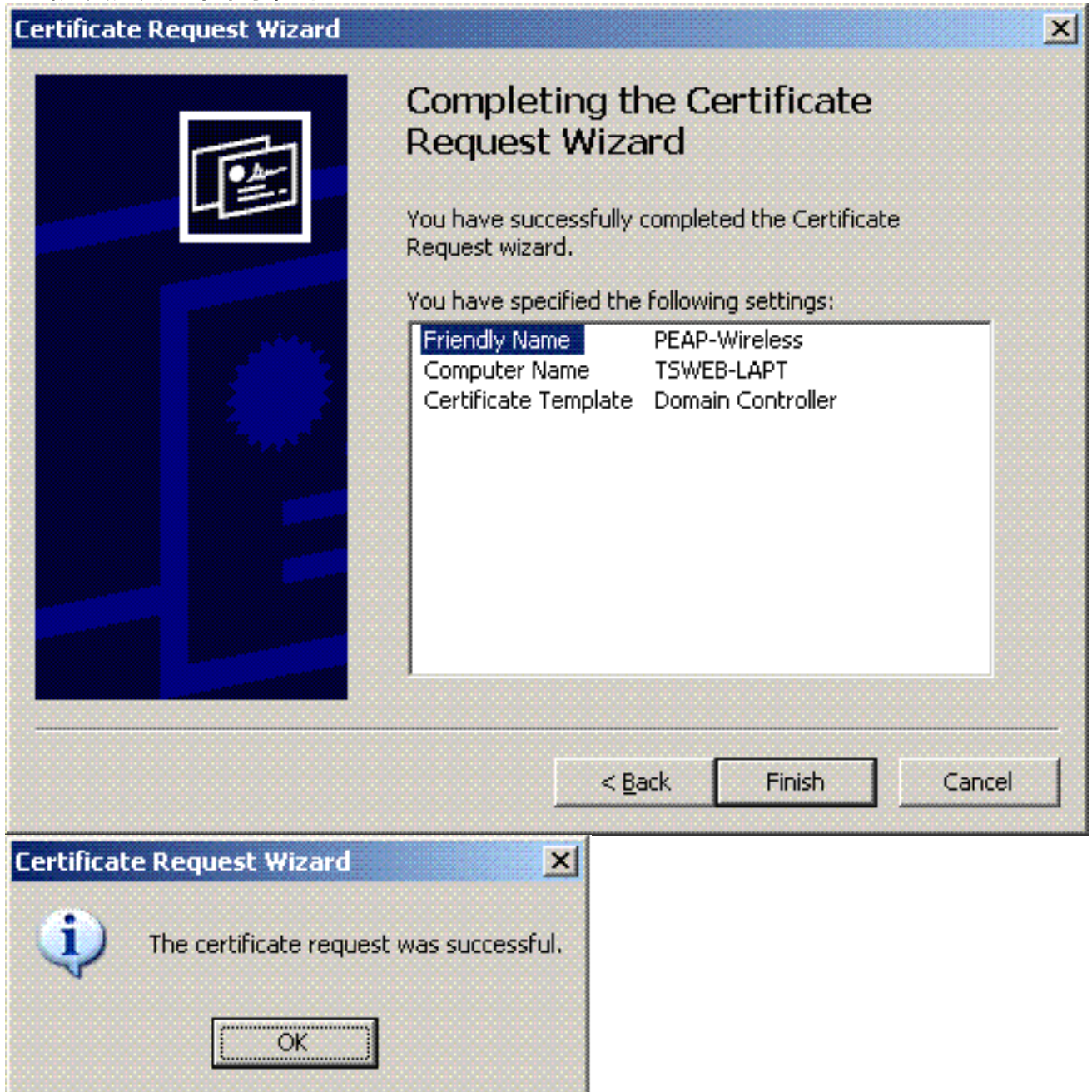
16. 选择域控制器证书模板（如果您从 DC 以外的服务器上请求计算机证书，请选择“计算机”证书模板），然后单击“下一步”。



17. 键入证书的名称和说明。



18. 单击完成完成证书请求向导。

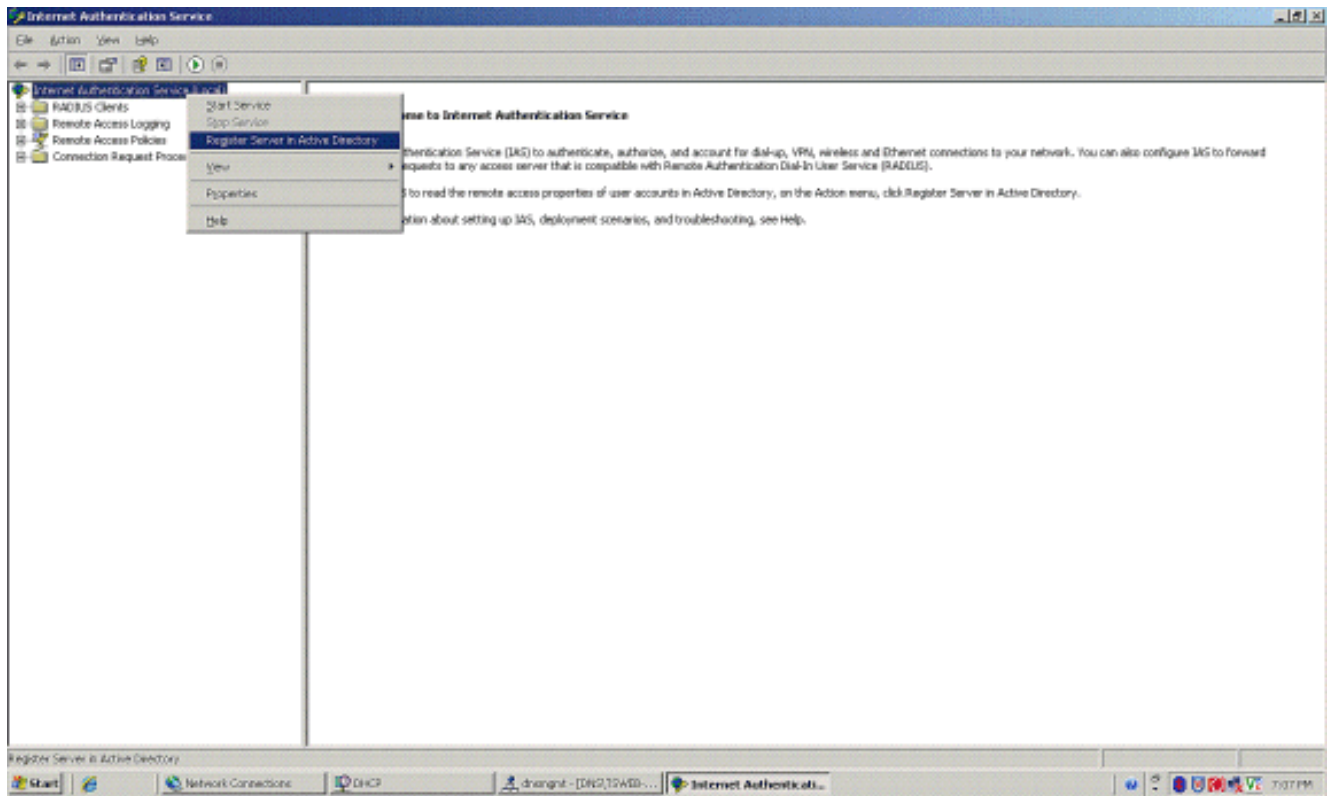


[为 PEAP-MS-CHAP v2 身份验证配置 Internet 身份验证服务](#)

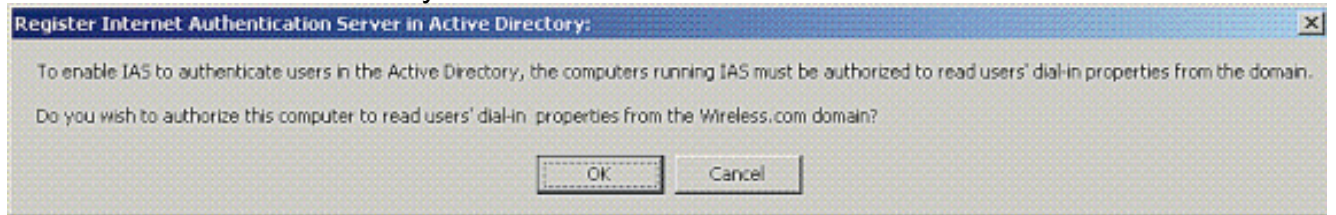
现在，您已经安装了 IAS 并为其请求了一个证书，可以开始为身份验证配置 IAS 了。

请完成以下步骤：

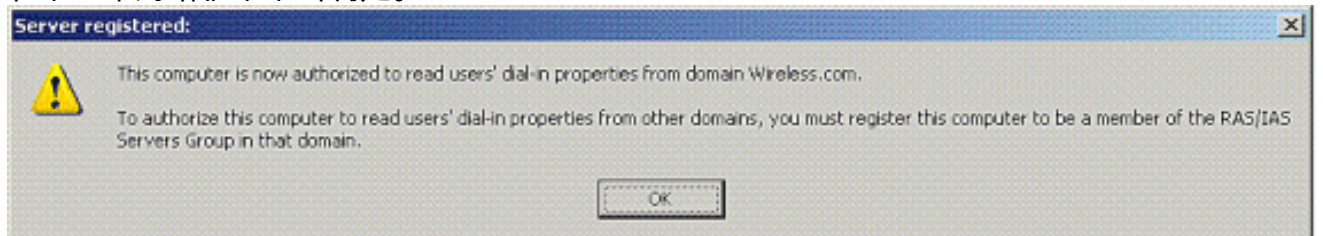
1. 单击开始 > 程序 > 管理工具，然后单击“Internet 身份验证服务”管理单元。
2. 右键单击Internet身份验证服务(IAS)，然后单击在Active Directory中注册服务。



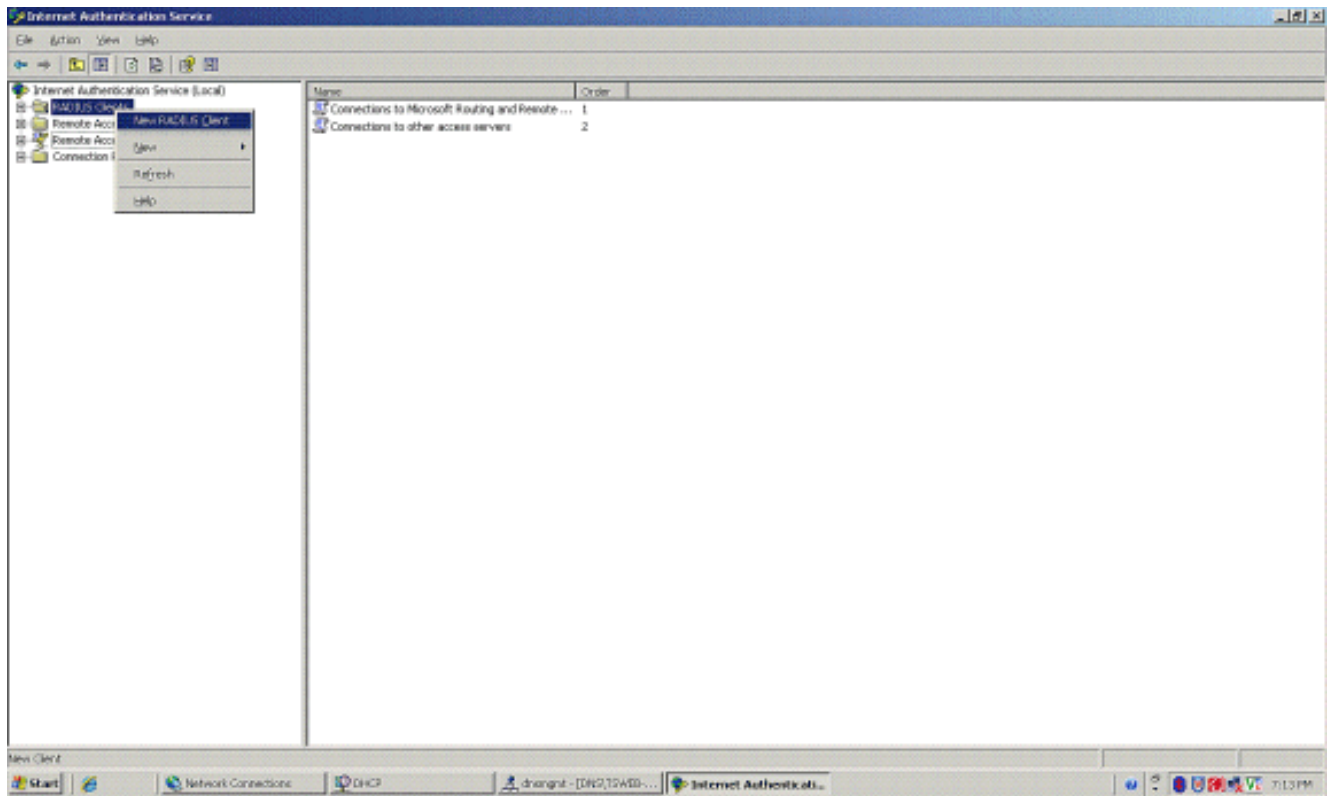
3. 系统将显示Register Internet Authentication Service in Active Directory对话框；单击**确定**。这使 IAS 能够对 Active Directory 中的用户进行身份验证。



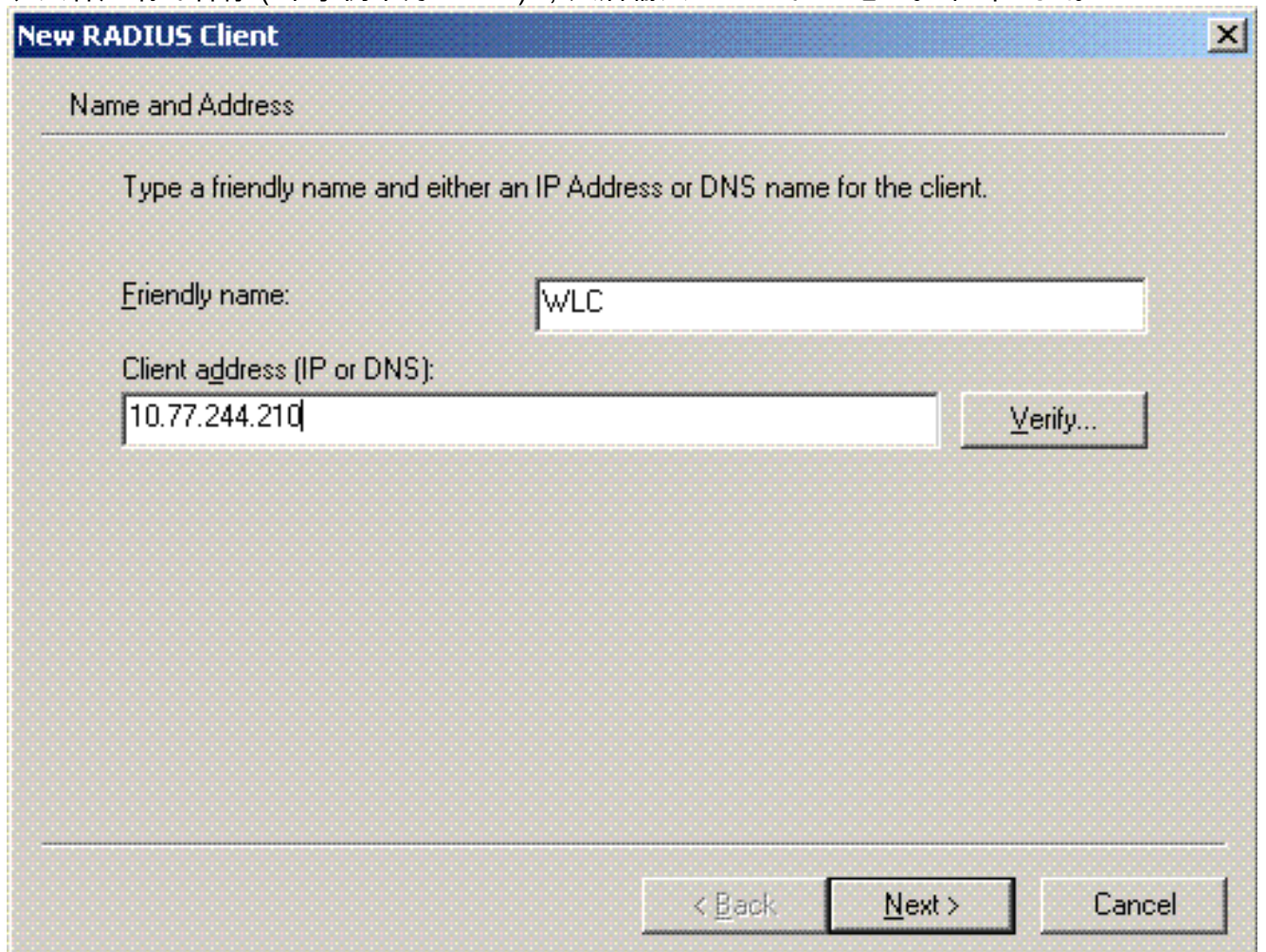
4. 在下一个对话框中单击**确定**。



5. 在 MS IAS 服务器上添加无线局域网控制器作为 AAA 客户端。
6. 右键单击 **RADIUS 客户端**，然后选择“新建 RADIUS 客户端”。

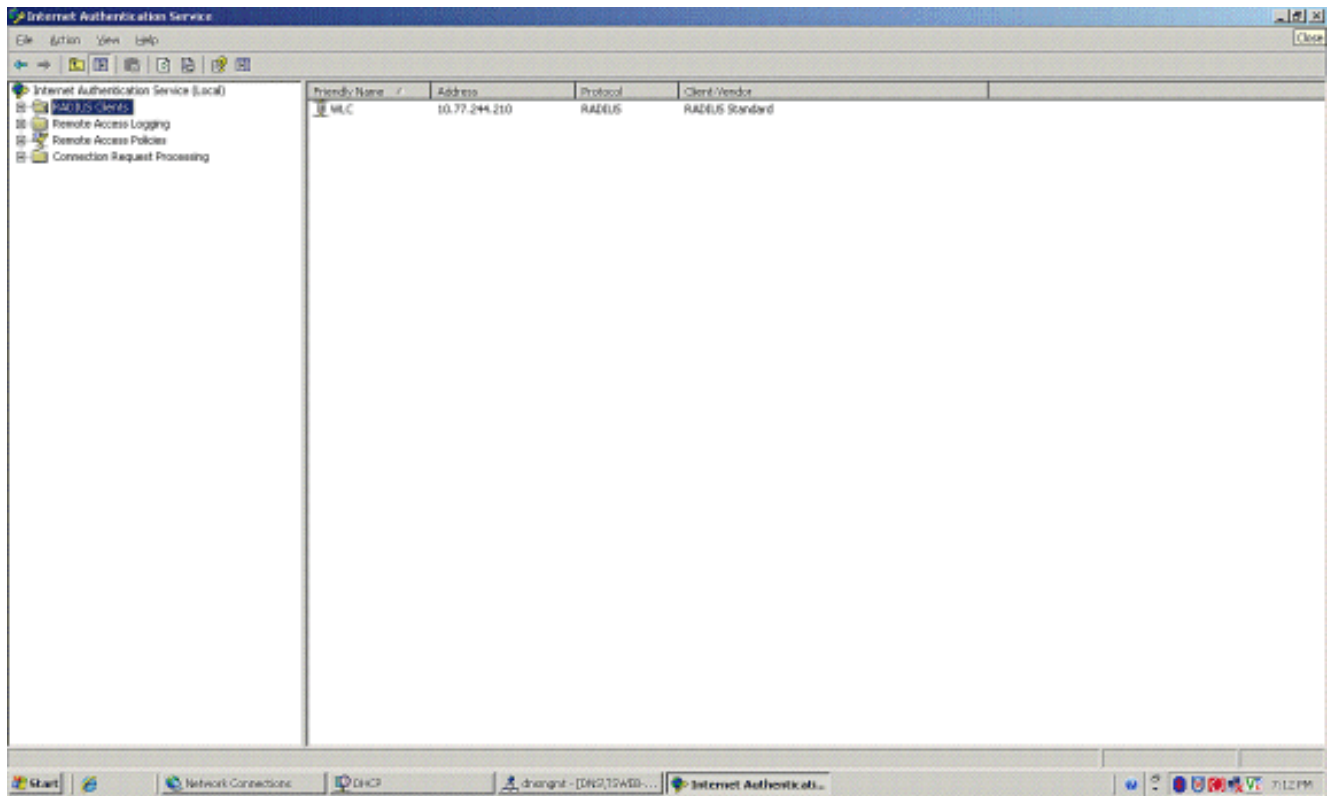


7. 键入客户端的名称（本示例中为 WLC），然后输入 WLC 的 IP 地址。单击 **Next**。



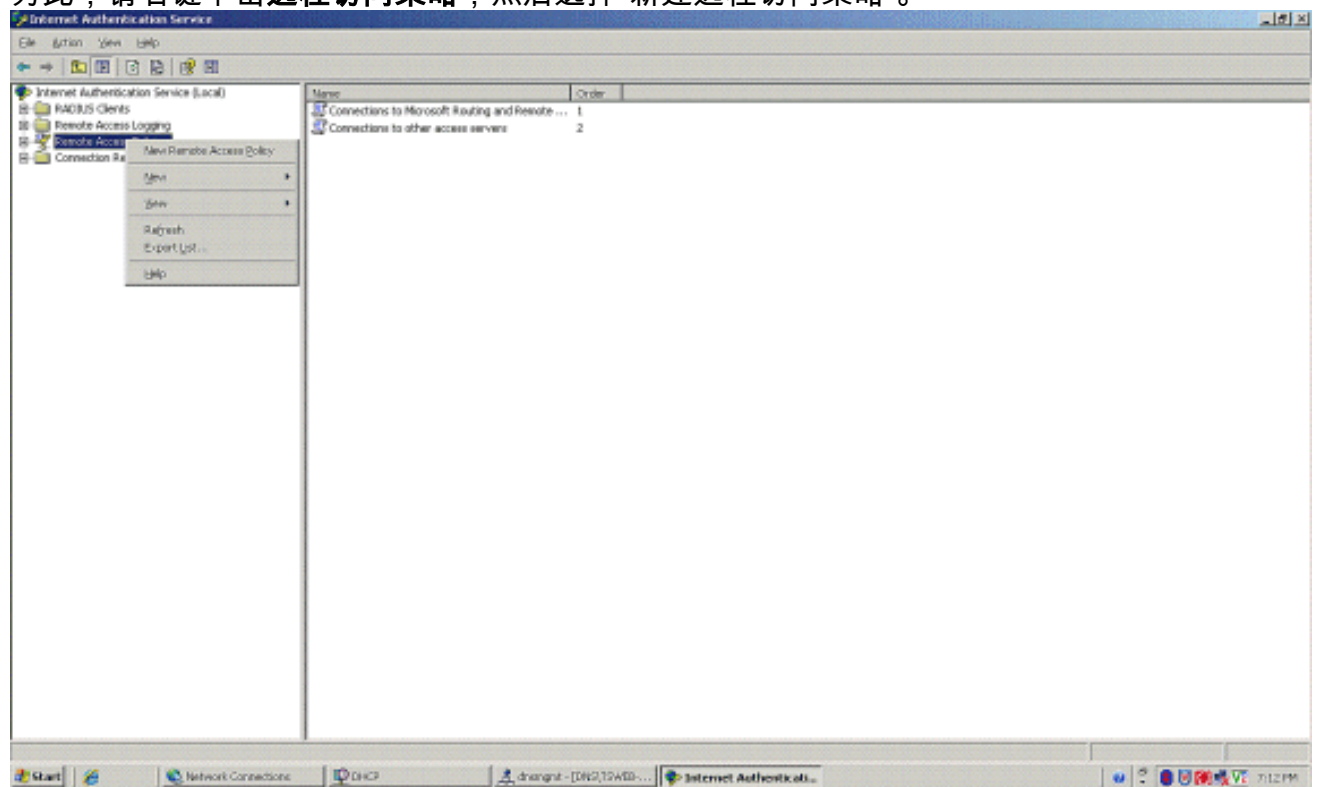
8. 在下一页的 Client-Vendor 下，选择 **RADIUS Standard**；输入共享密钥；然后单击 **Finish**。

9. 请注意，WLC 已作为 AAA 客户端添加到 IAS 上。




10. 为客户端创建远程访问策略。

11. 为此，请右键单击**远程访问策略**，然后选择“新建远程访问策略”。



12. 键入远程访问策略的名称。本示例中使用名称 **PEAP**。然后，单击下一步。

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

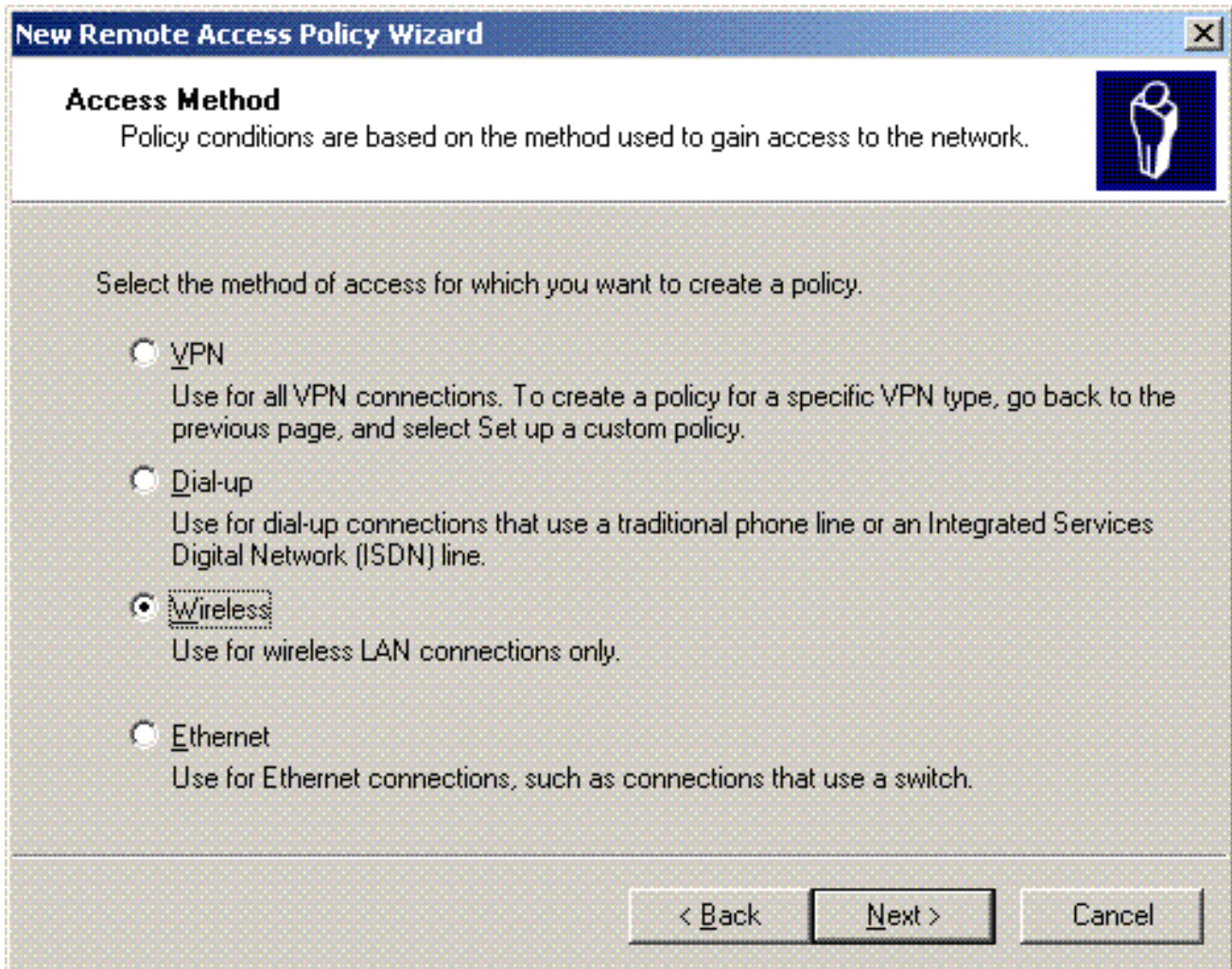
Set up a custom policy

Type a name that describes this policy.

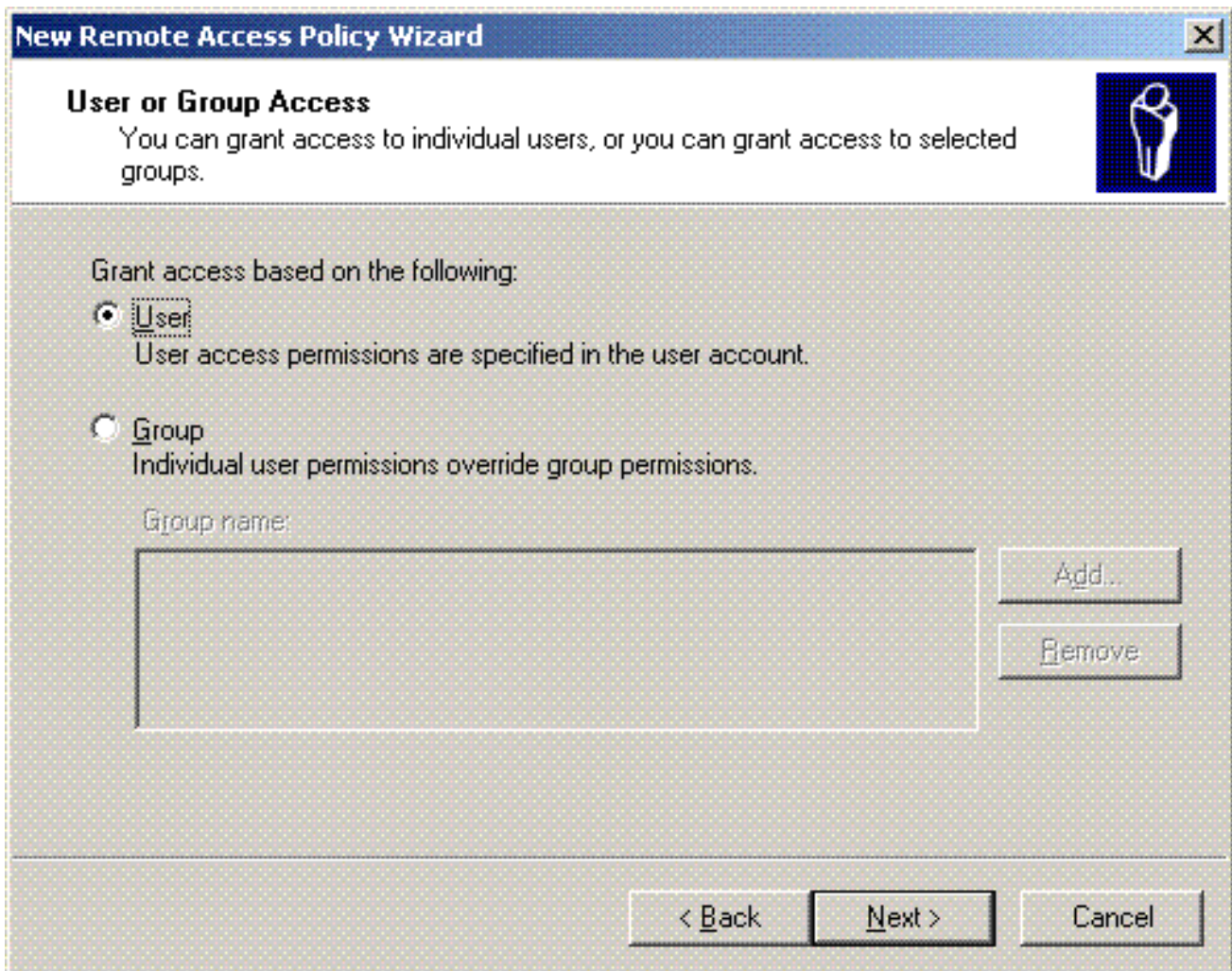
Policy name:

Example: Authenticate all VPN connections.

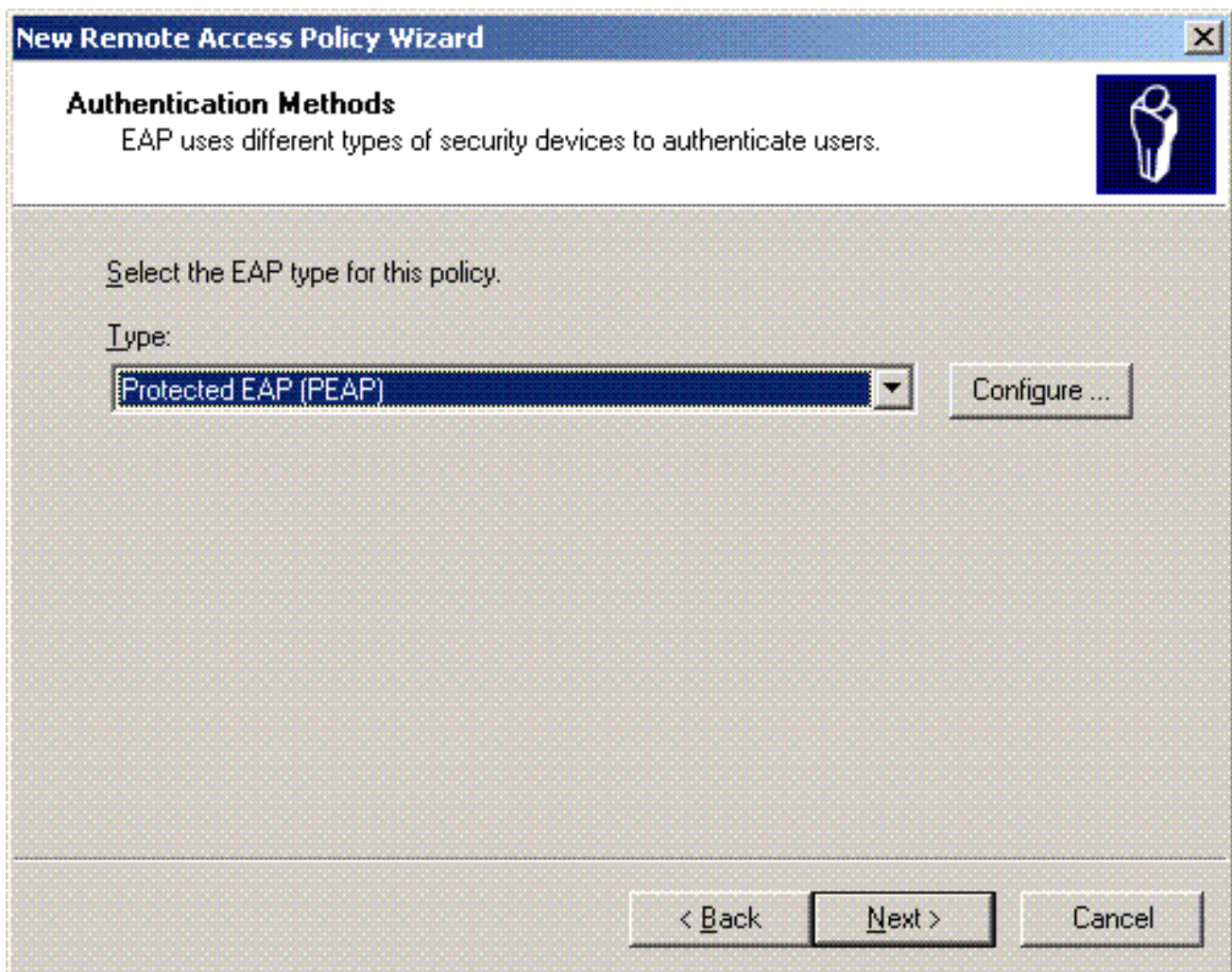
13. 根据您的需要选择策略属性。本示例中选择 **Wireless**。



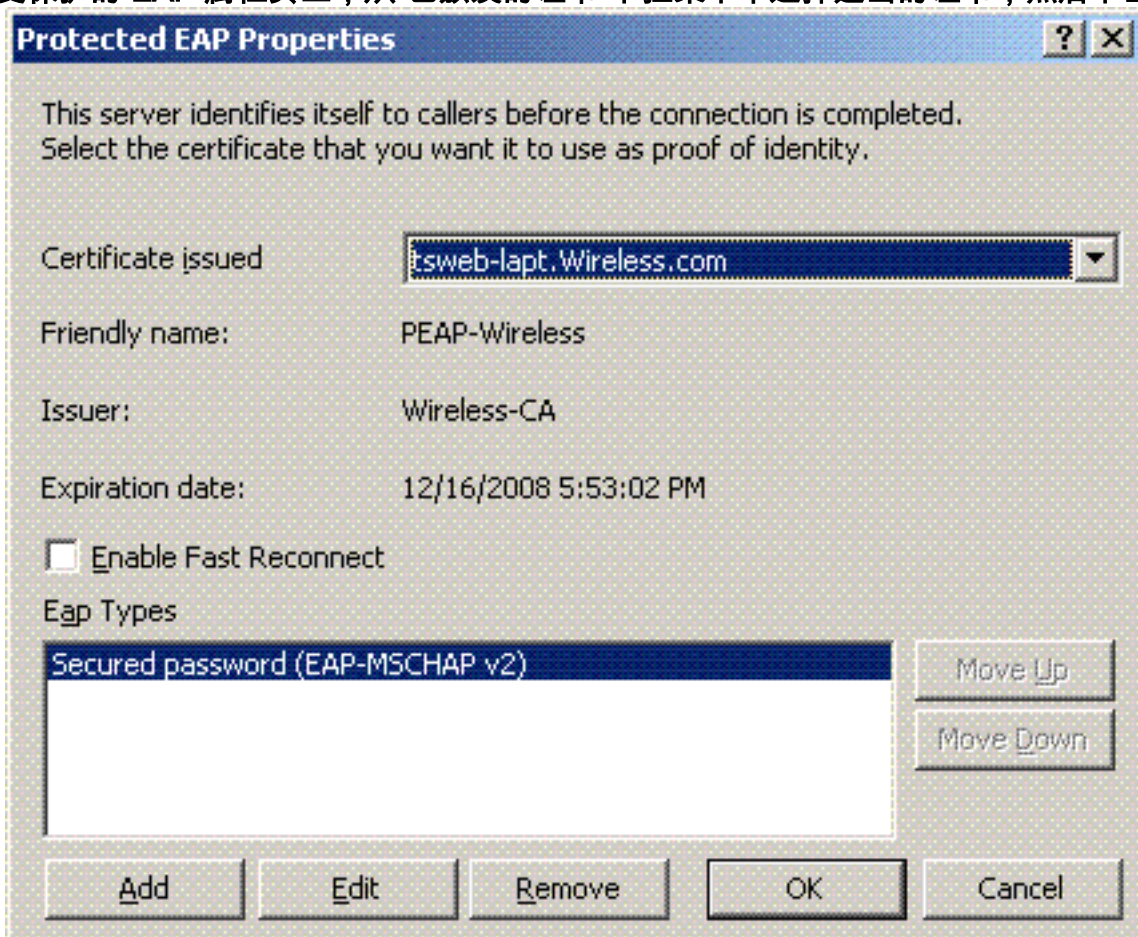
14. 在下一页上，选择用户，以便将此远程访问策略应用于用户列表。



15. 在“身份验证方法”下，选择受保护的 EAP (PEAP)，然后单击“配置”。



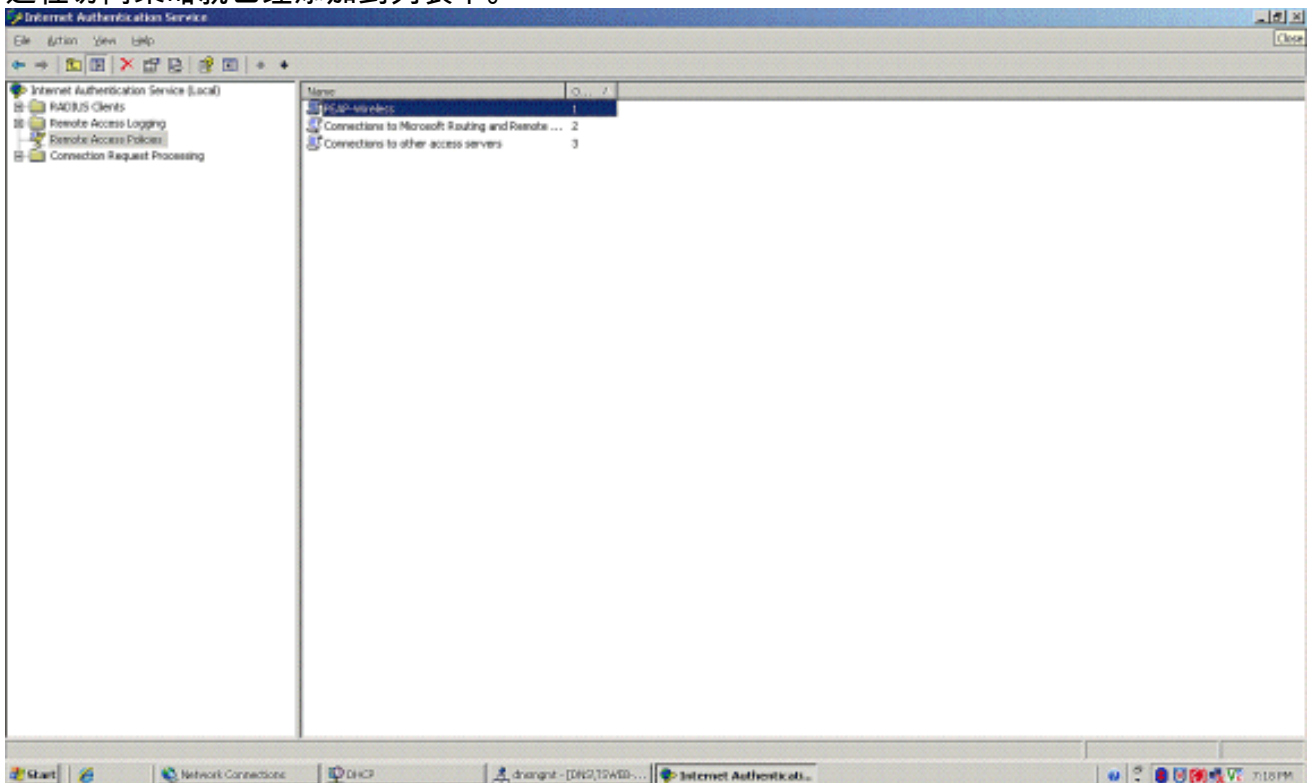
16. 在受保护的 EAP 属性页上，从“已颁发的证书”下拉菜单中选择适当的证书，然后单击“确定”。



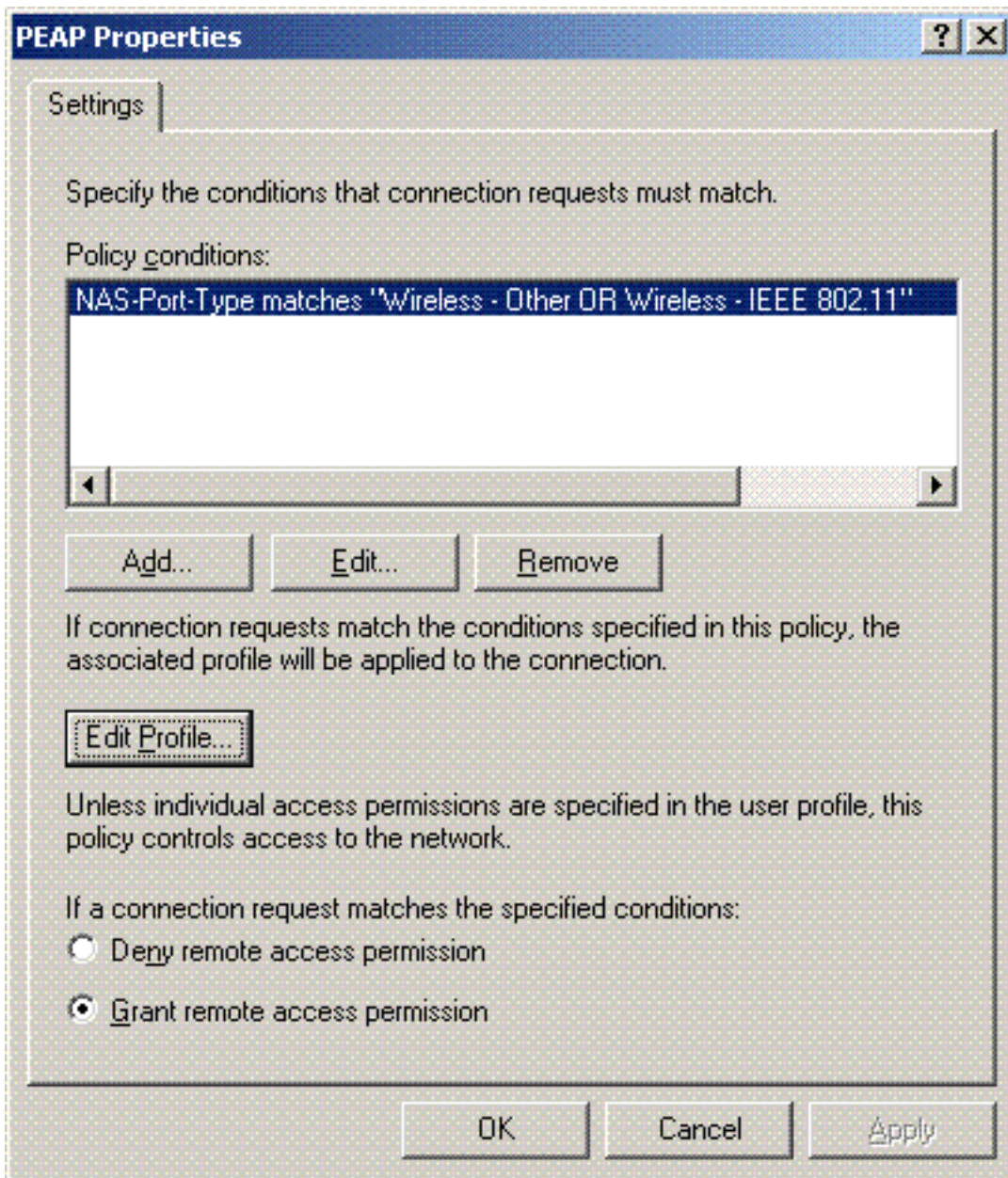
17. 验证远程访问策略的详细信息，然后单击完成。



18. 远程访问策略就已经添加到列表中。



19. 右键单击此策略，然后单击属性。在“如果连接请求满足指定的条件”下选择授予远程访问权限

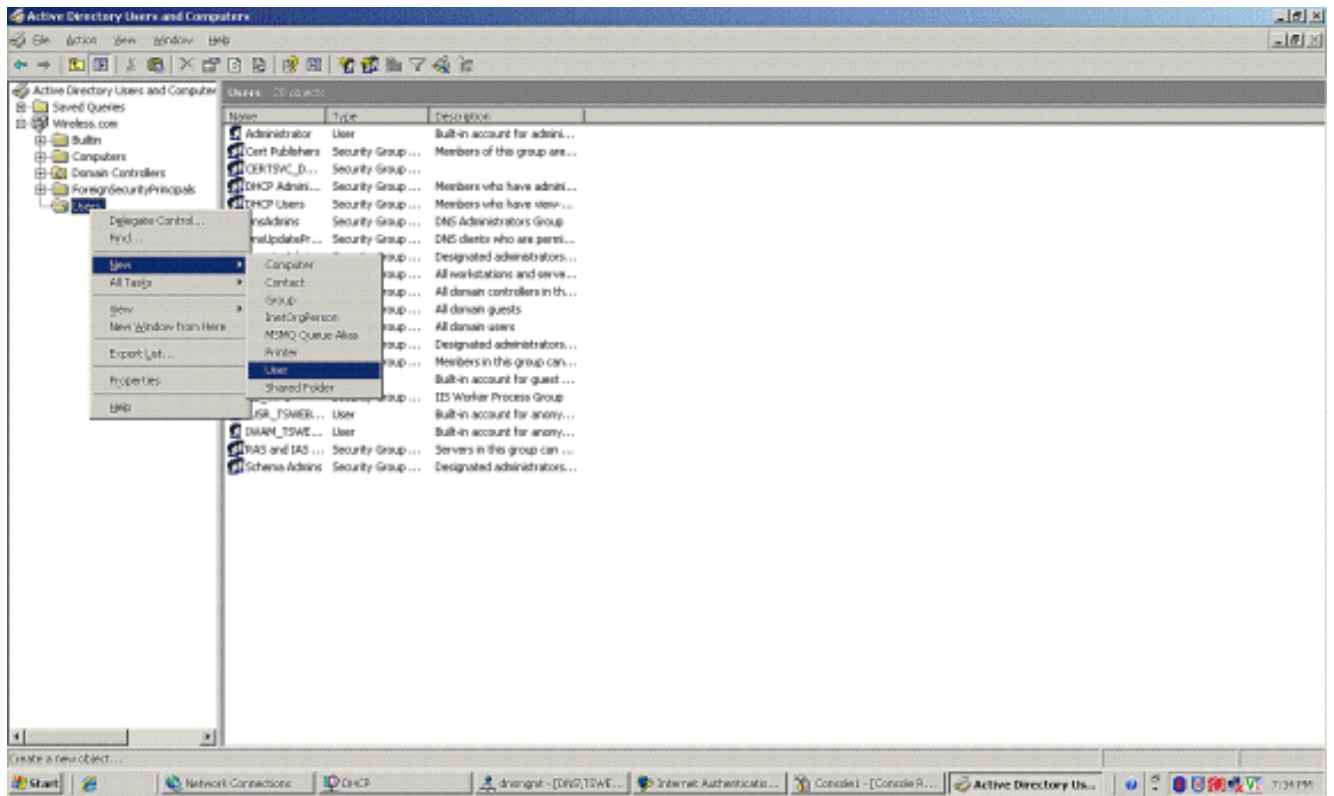


[将用户添加到 Active Directory](#)

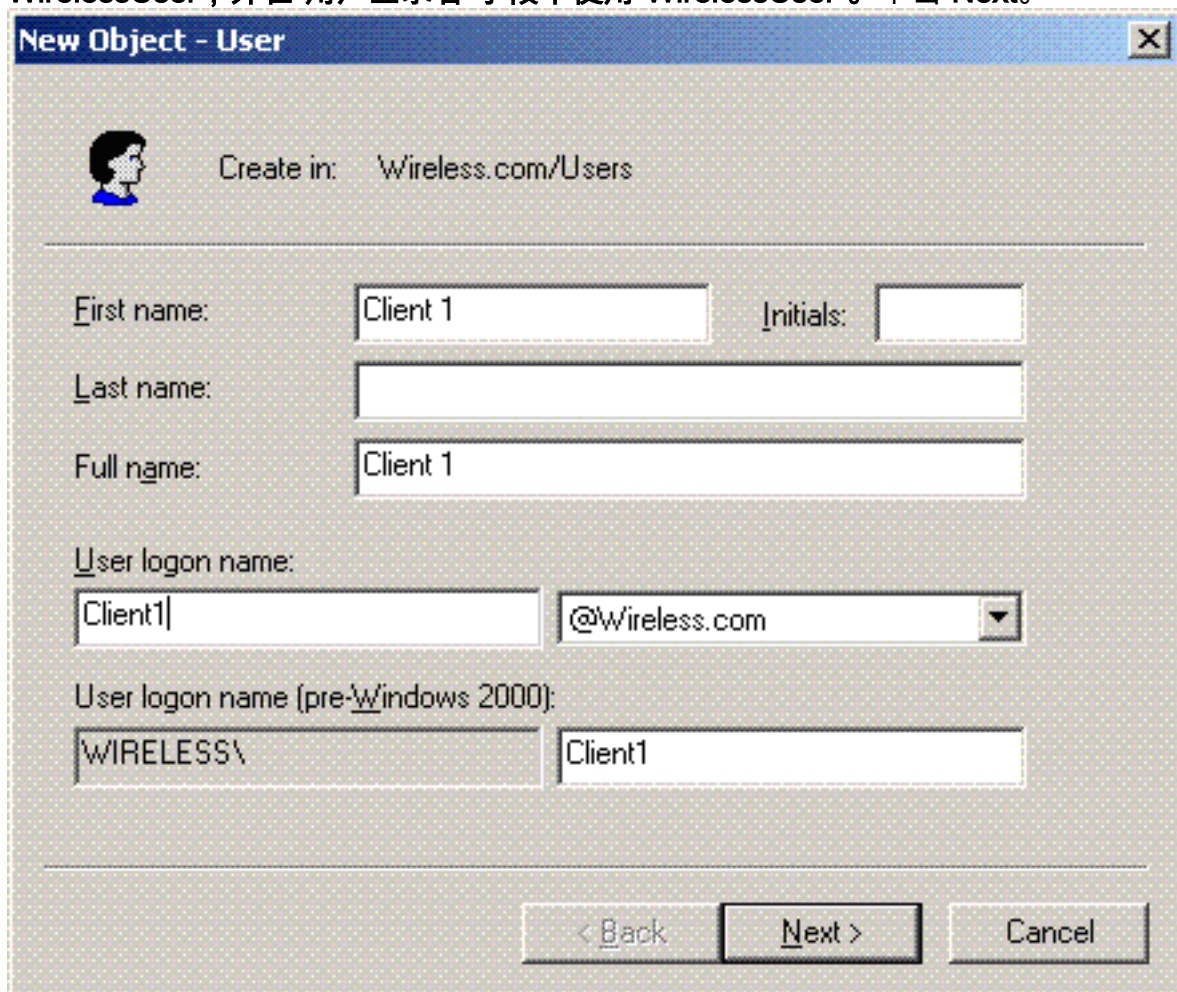
在此设置中，需要在 Active Directory 上维护用户数据库。

要将用户添加到 Active Directory 数据库中，请完成以下步骤：

1. 在“Active Directory用户和计算机”控制台树中，右键单击用户；单击新建；然后单击用户。




2. 在“新建对象 - 用户”对话框中，键入无线用户的名称。本示例在“名字”字段中使用名称 WirelessUser，并在“用户登录名”字段中使用“WirelessUser”。单击 Next。



3. 在“新建对象 - 用户”对话框中，在“密码”和“确认密码”字段中键入您选择的密码。清除用户必须在下次登录时更改密码复选框，然后单击“下一步”。

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“新建对象 – 用户”对话框中，单击完成。

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

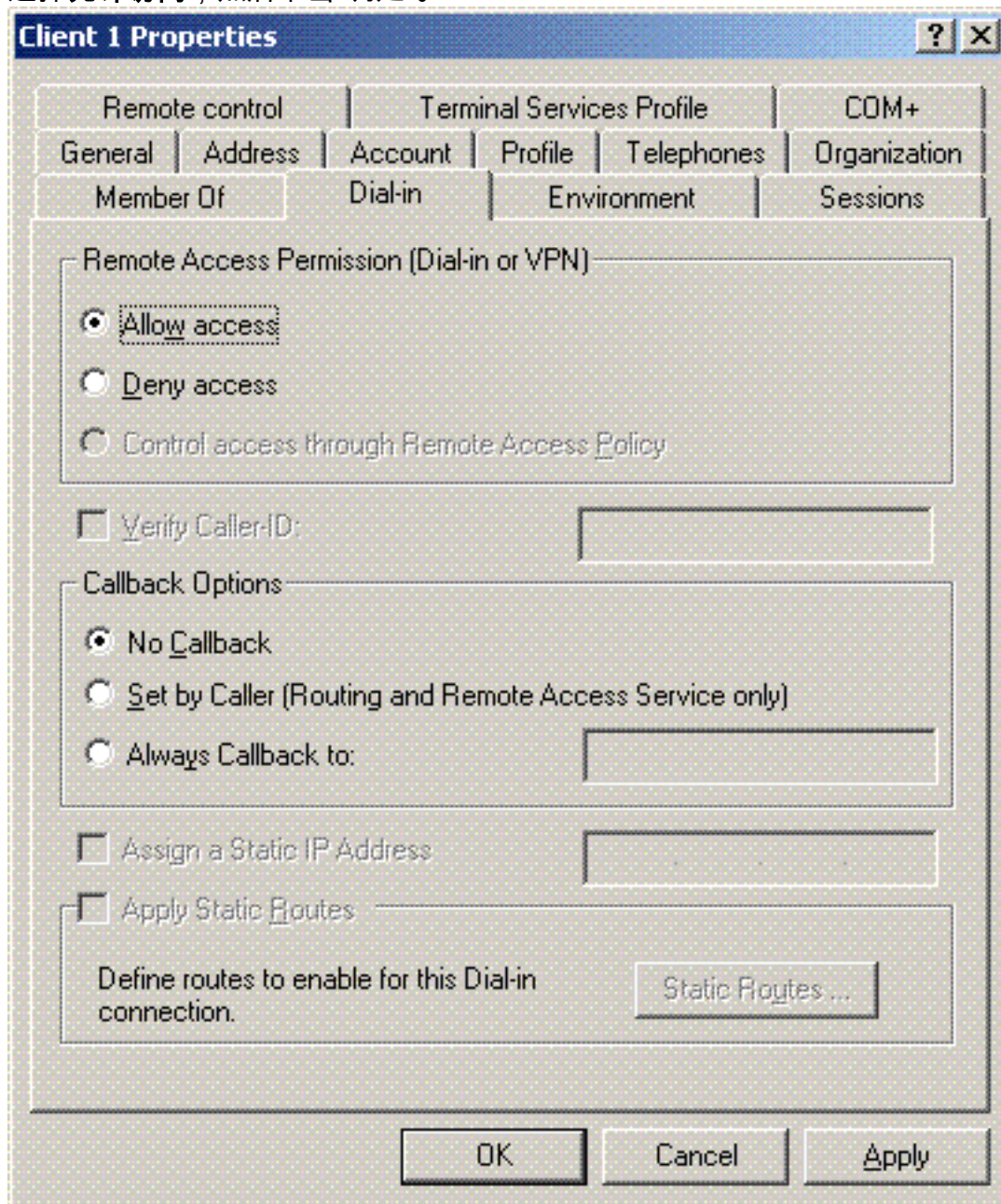
< Back Finish Cancel

5. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

允许用户进行无线访问

请完成以下步骤：

1. 在Active Directory用户和计算机控制台树中，单击Users文件夹；右键单击WirelessUser；单击Properties；然后转到Dial-in选项卡。
2. 选择允许访问，然后单击“确定”。



配置无线局域网控制器和轻量 AP

现在要为此设置配置无线设备。这包括配置无线局域网控制器、轻量 AP 和无线客户端。

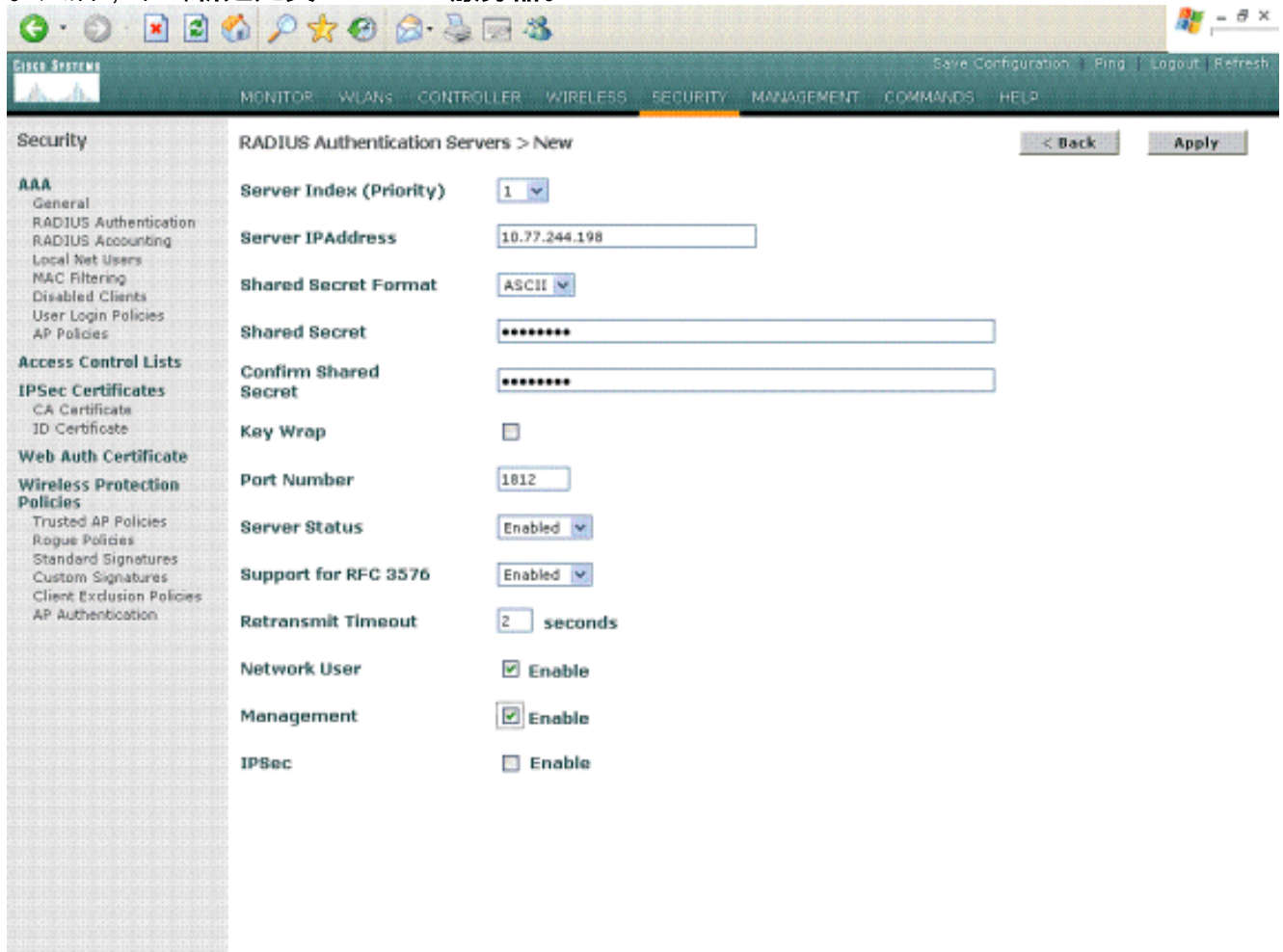
通过 MS IAS RADIUS 服务器为 RADIUS 身份验证配置 WLC

首先要配置 WLC，以便使用 MS IAS 作为身份验证服务器。需要配置 WLC 以便将用户凭证转发到

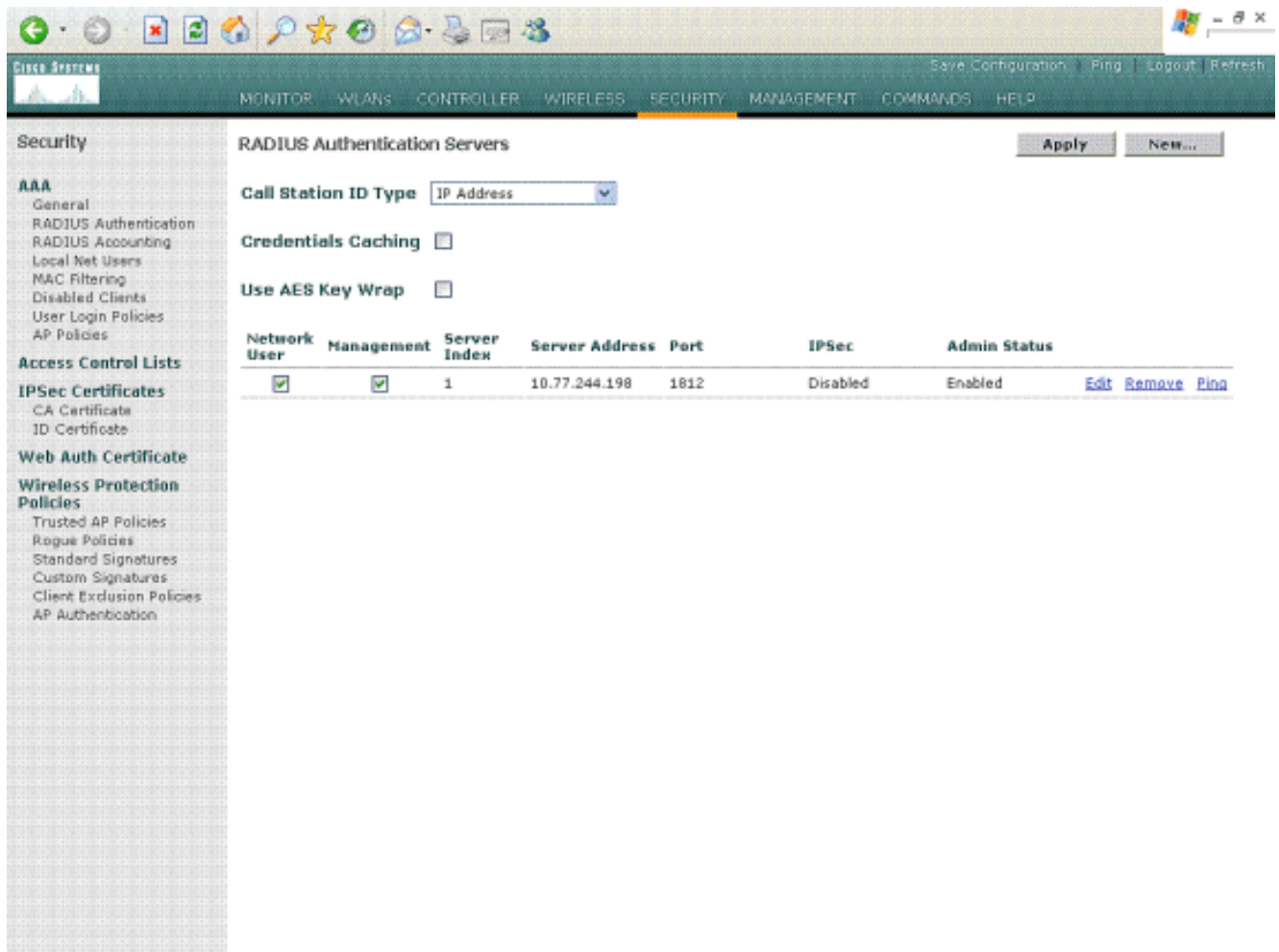
外部 RADIUS 服务器。然后，外部 RADIUS 服务器验证用户凭证，并向无线客户端提供访问权限。为此，请在**安全性 > RADIUS 验证**页中添加 MS IAS 服务器作为 RADIUS 服务器。

请完成以下步骤：

1. 从控制器的 GUI 中选择**安全性和“RADIUS 身份验证”**，以便显示“RADIUS 身份验证服务器”页。然后，单击**新建定义 RADIUS 服务器**。



2. 在 **RADIUS 身份验证服务器 > 新建**页中定义 RADIUS 服务器参数。这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。“网络用户”和“管理”复选框决定基于 RADIUS 的身份验证是否适用于管理和网络用户。本示例使用 IP 地址为 10.77.244.198 的 MS IAS 作为 RADIUS 服务器。



3. 单击 **Apply**。

4. MS IAS 服务器已作为 RADIUS 服务器添加到 WLC 中，并且可用于对无线客户端进行身份验证。

[为客户端配置 WLAN](#)

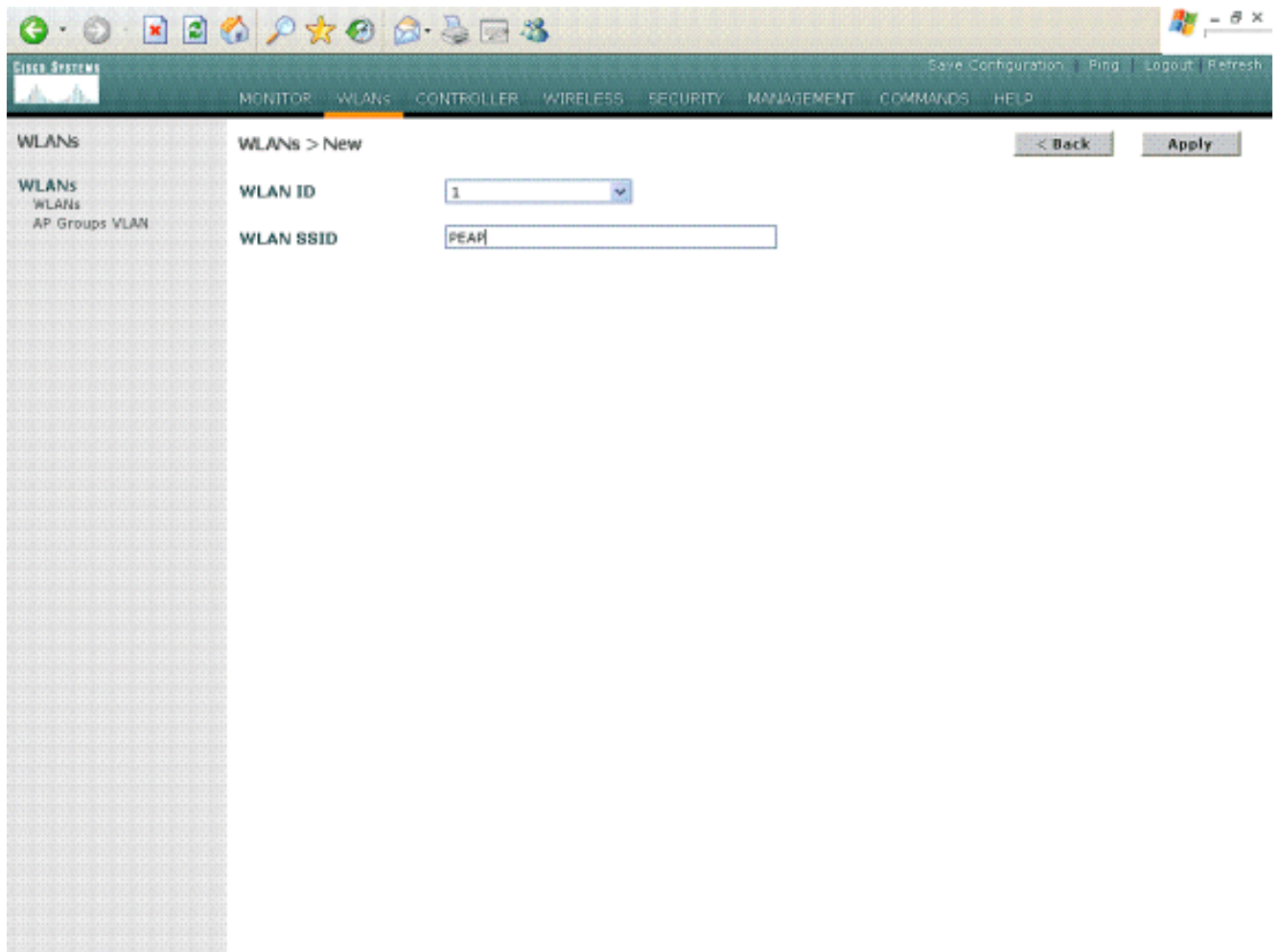
配置无线客户端要连接到的 SSID (WLAN)。本示例中将创建 SSID，并将其命名为 **PEAP**。

将第 2 层身份验证定义为 WPA2，使客户端能够执行基于 EAP 的身份验证（本示例中为 PEAP-MSCHAPv2）并使用 AES 作为加密机制。将其他所有值均保留默认值。

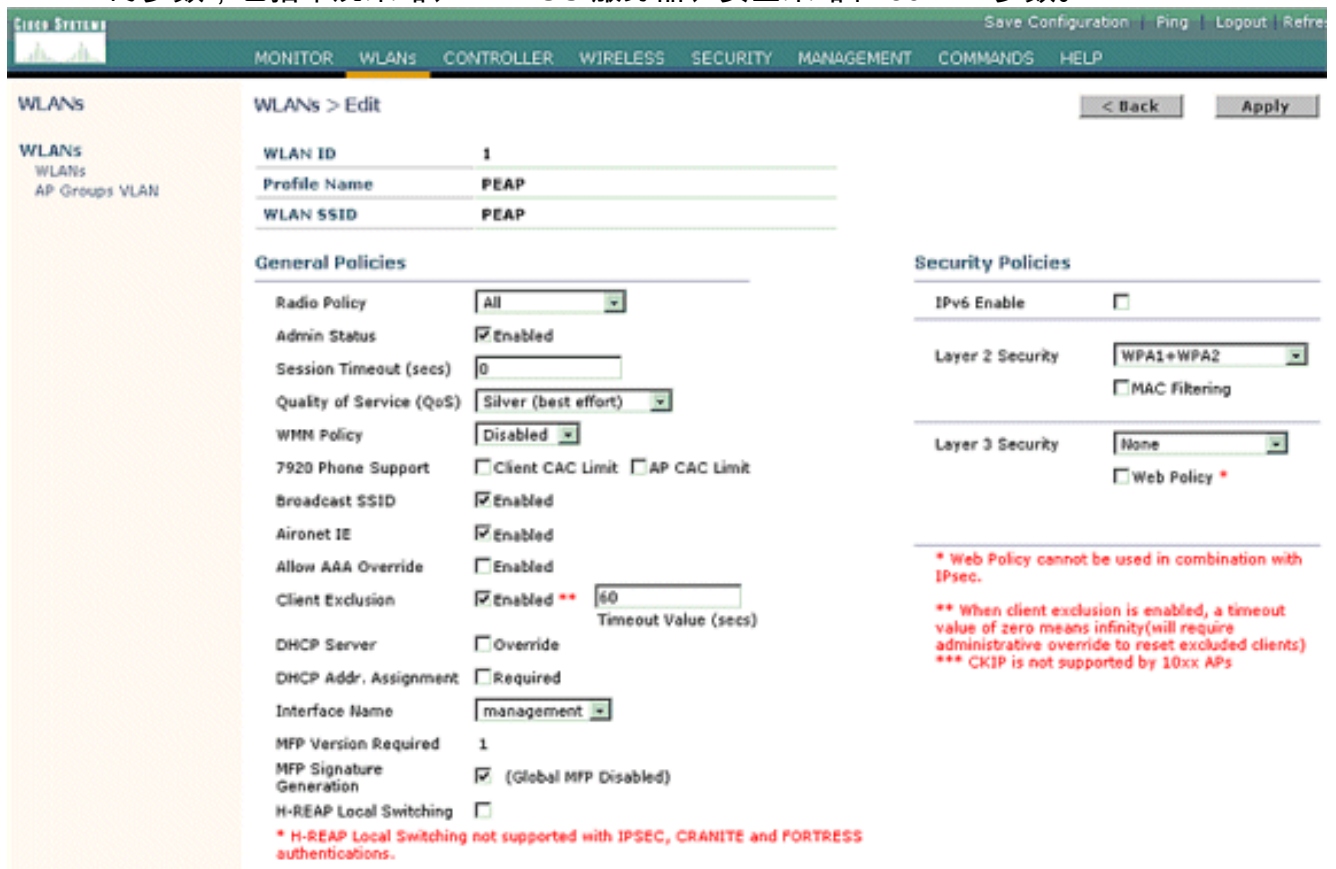
注意：本文档将 WLAN 与管理接口绑定。当您的网络中有多个 VLAN 时，可以创建一个单独的 VLAN 并将其绑定到 SSID。有关如何在 WLC 上配置 VLAN 的信息，请参阅[无线局域网控制器上的 VLAN 配置示例](#)。

要在 WLC 上配置 WLAN，请完成以下步骤：

1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出了控制器上现有的 WLAN。
2. 选择 **新建创建新的 WLAN**。输入 WLAN 的 WLAN ID 和 WLAN SSID，然后单击 **应用**。



3. 创建新 WLAN 后，就会显示新 WLAN 的 **WLAN > Edit** 页。在此页上，可以定义各种特定于此 WLAN 的参数，包括常规策略、RADIUS 服务器、安全策略和 802.1x 参数。



4. 选中“常规策略”下的**管理状态**，以便启用 WLAN。如果希望 AP 在其信标帧中广播 SSID，请选中**广播 SSID**。

5. 在“第 2 层安全性”下，选择 **WPA1+WPA2**。这将在 WLAN 上启用 WPA。向下滚动该页，然后选择 WPA 策略。本示例使用 WPA2 和 AES 加密。从“RADIUS 服务器”下的下拉菜单中选择相应的 RADIUS 服务器。本示例中使用 10.77.244.198 (MS IAS 服务器的 IP 地址)。可以根据 WLAN 网络的需要修改其他参数。



6. 单击 **Apply**。



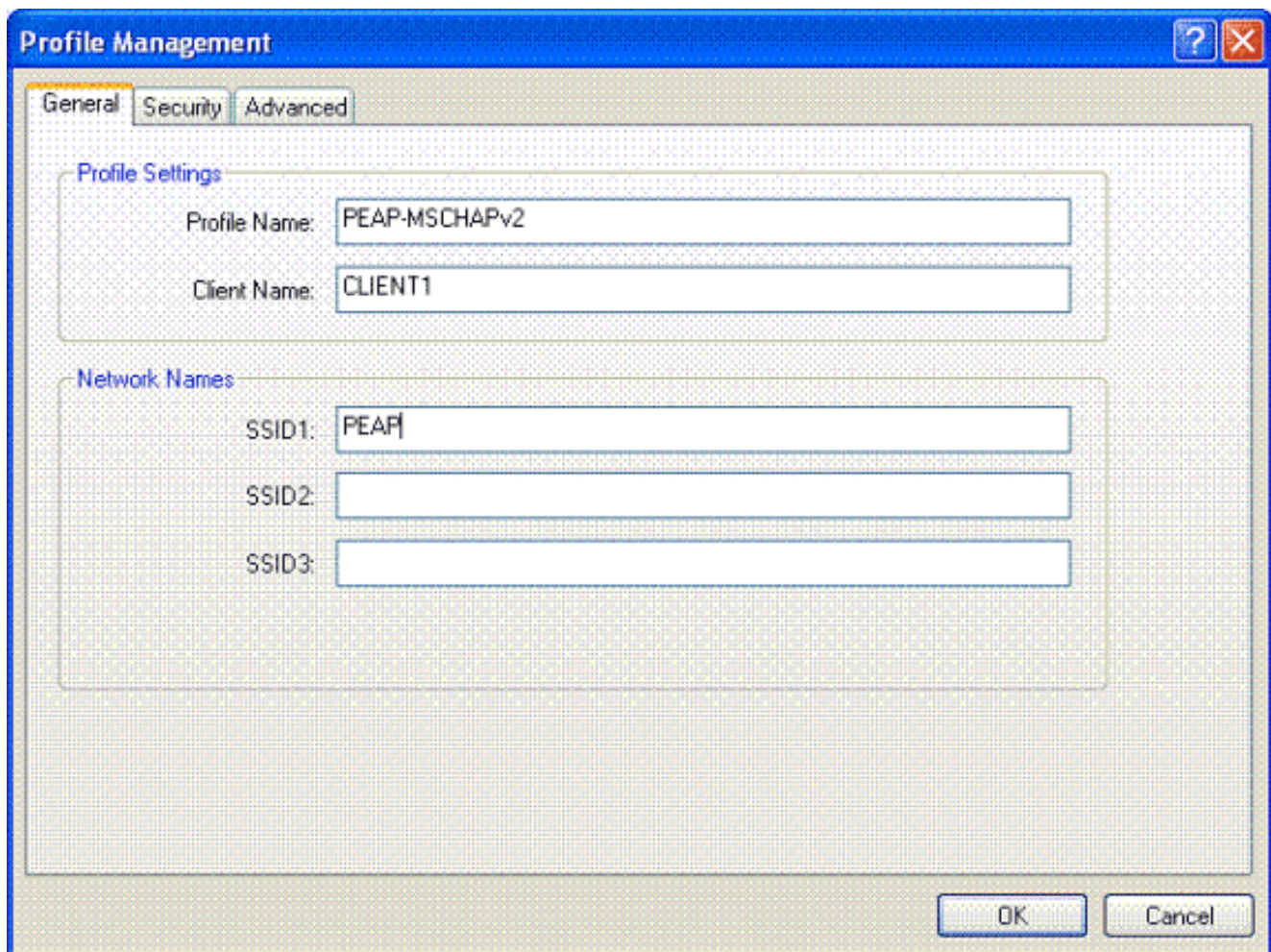
配置无线客户端

为 PEAP-MS CHAPv2 身份验证配置无线客户端

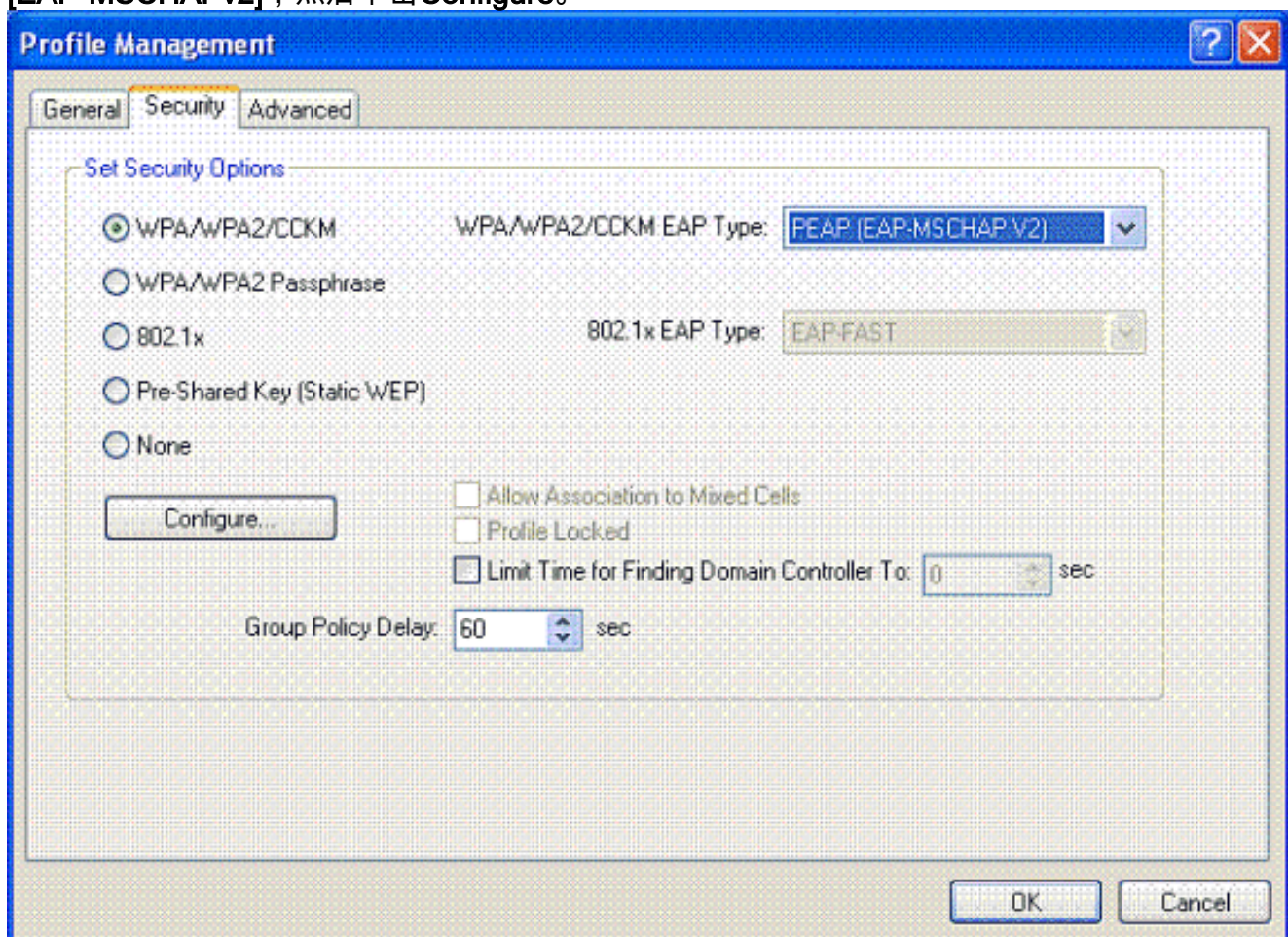
本示例提供有关如何使用 Cisco Aironet Desktop Utility 配置无线客户端的信息。在配置客户端适配器之前，请确保使用了最新版本的固件和实用程序。在 Cisco.com 上的无线下载页中查找最新版本的固件和实用程序。

要用 ADU 来配置 Cisco Aironet 802.11 a/b/g 无线客户端适配器，请完成以下步骤：

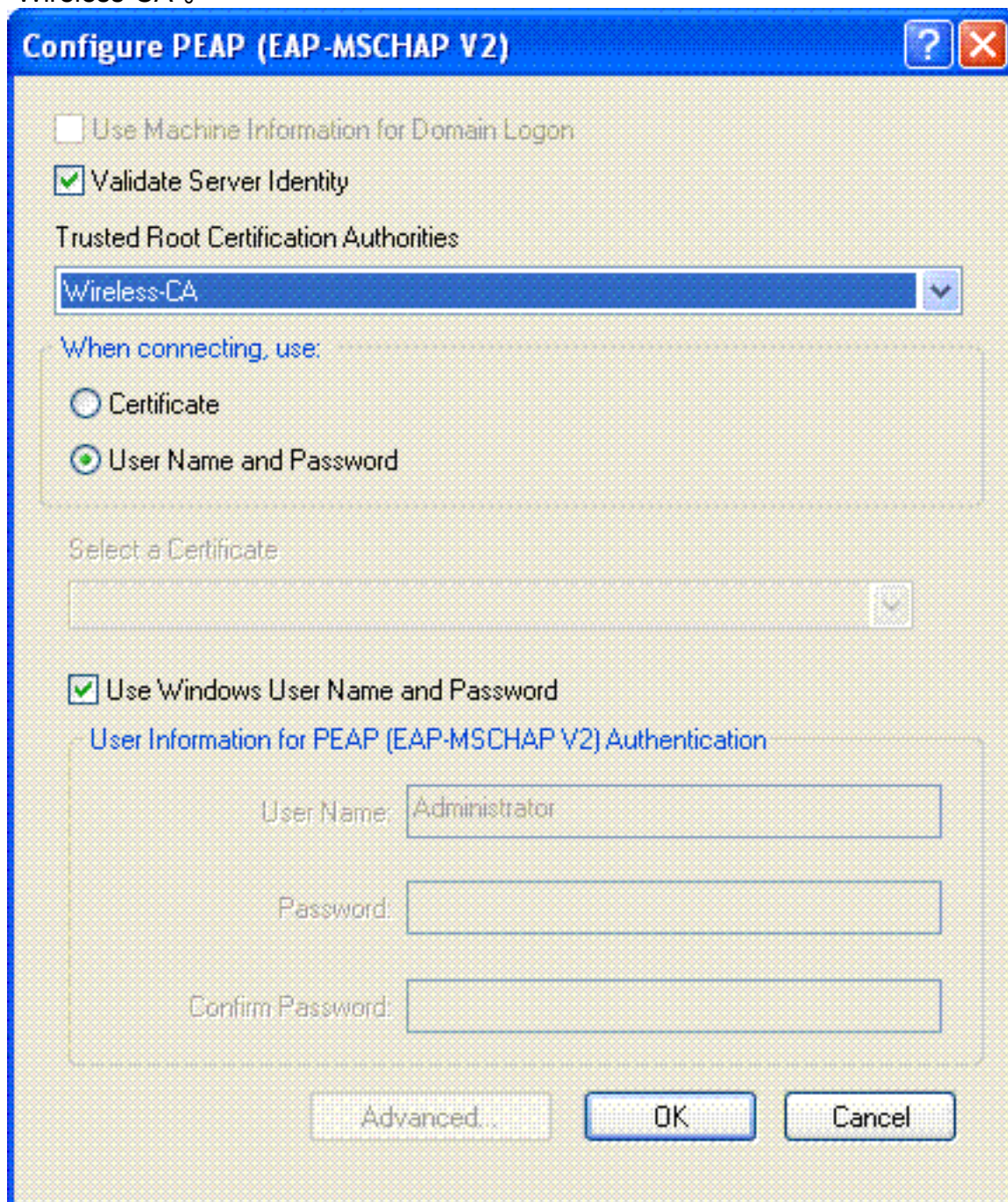
1. 打开 Aironet Desktop Utility。
2. 单击 **Profile Management**，然后单击“New”以定义配置文件。
3. 在“General”选项卡下，输入配置文件名称和 SSID。本示例中使用您在 WLC (PEAP) 上配置的 SSID。



4. 选择Security选项卡；选择WPA/WPA2/CCKM；在WPA/WPA2/CCKM EAP下，键入PEAP [EAP-MSCHAPv2]，然后单击Configure。



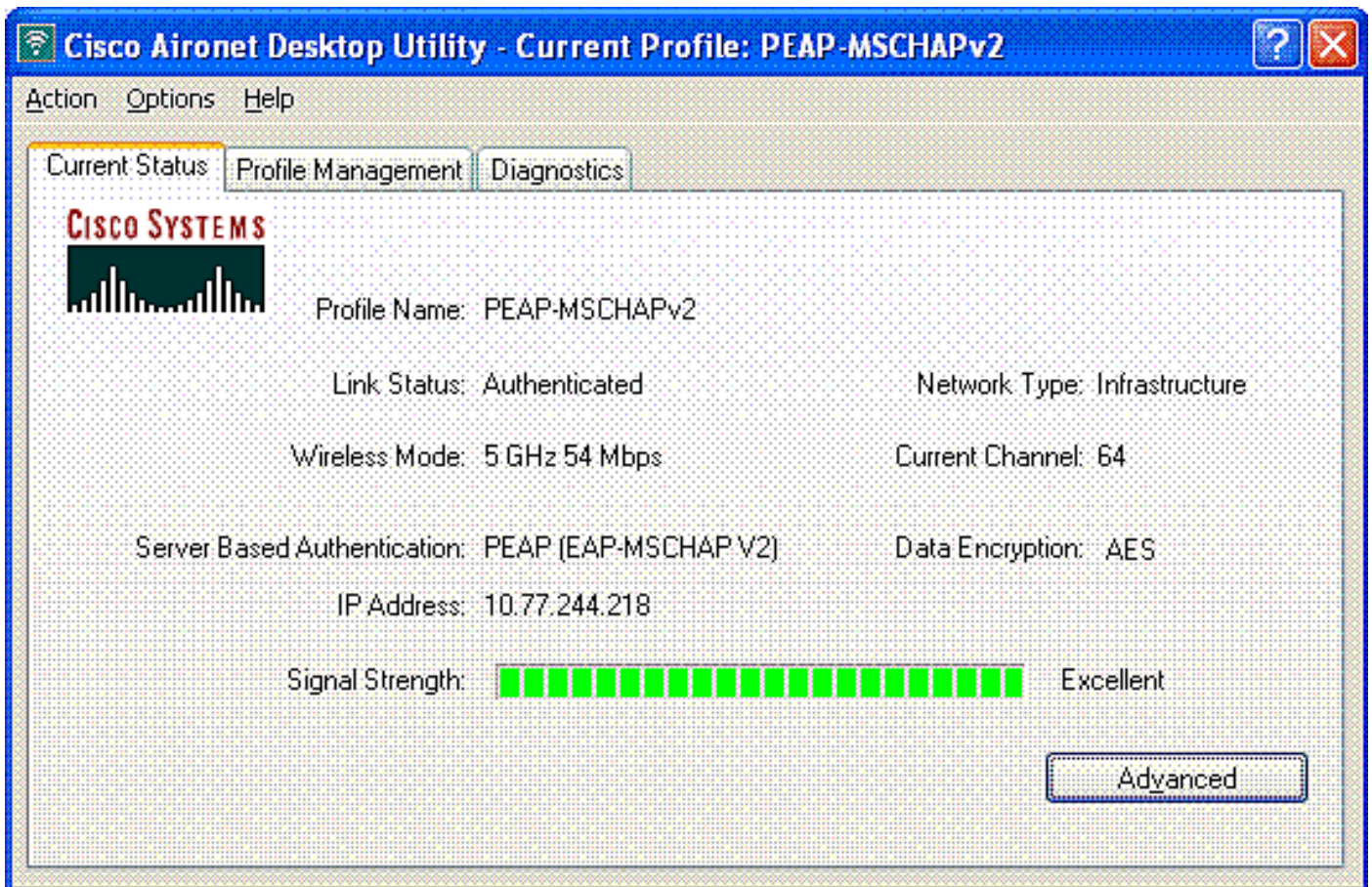
5. 选择 **Validate Server Certificate**，然后在“Trusted Root Certificate Authorities”下拉菜单下选择“Wireless-CA”。



6. 单击 **OK**，然后激活该配置文件。**注意**：将Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2(PEAP-MSCHAPv2)与Microsoft XP SP2配合使用时，无线卡由Microsoft Wireless Zero Configuration(WZC)管理，您必须应用Microsoft修补程序KB885453。这可以防止与PEAP快速恢复相关的几个身份验证问题。

验证与故障排除

要验证配置是否按预期工作，请在无线客户端 Client1 上激活配置文件 PEAP-MSCHAPv2。



当 ADU 上激活配置文件 PEAP-MSCHAPv2 后，客户端将执行 802.11 开放式身份验证，然后执行 PEAP-MSCHAPv2 身份验证。这是一个成功的 PEAP-MSCHAPv2 身份验证示例。

请使用调试命令来了解发生的事件顺序。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

以下调试命令在无线局域网控制器上非常有用。

- **debug dot1x events enable**—用于配置 802.1x 事件的调试
- **debug aaa events enable**—用于配置 AAA 事件的调试
- **debug mac addr <mac 地址>**—用于使用 debug mac 命令配置 MAC 调试
- **debug dhcp message enable**—用于配置 DHCP 错误消息的调试

下面是 debug dot1x events enable 命令和 debug client <mac 地址> 命令的输出示例。

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 地址> :

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客户端通过Cisco Secure ACS进行PEAP身份验证，则客户端可能无法成功进行身份验证。有时初始连接能够成功进行身份验证，但是随后的快速连接身份验证尝试不能成功连接。这是已知问题。有关此问题的详细信息及其修正方法，请参阅[此处](#)。

相关信息

- [ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAP](#)
- [WLAN 控制器 \(WLC\) 中 EAP 身份验证的配置示例](#)
- [无线局域网控制器\(WLC\)软件升级到版本3.2、4.0和4.1](#)
- [Cisco 4400 系列无线局域网控制器配置指南](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。