ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAP

目录

简介

本文档介绍如何使用无线局域网控制器、Microsoft Windows 2003 软件和 Cisco 安全访问控制服务器 (ACS) 4.0，通过受保护的扩展身份验证协议 (PEAP) 以及 Microsoft 质询握手身份验证协议 (MS-CHAP) 2，来配置安全的无线访问。

注意：有关安全无线部署的信息，请参阅Microsoft Wi-Fi网站和 Cisco SAFE无线蓝图。

先决条件

要求

假设安装者已经掌握基本的 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。

Cisco的初始安装和配置信息4400系列控制器，是指快速入门指南：Cisco 4400 系列无线局域网控制器。有关 Cisco 2000 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 2000 系列无线局域网控制器。

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。

重要信息：在撰写本文时，最新的 Microsoft Windows Server 2003 更新是 SP1，适用于 Microsoft Windows XP Professional 的最新软件是包含更新修补程序的 SP2。

Windows Server 2003 Enterprise Edition SP1 也已投入使用，因此可以配置为自动注册用户和工作站证书，以便进行 PEAP 身份验证。证书自动注册和自动续订还会自动过期和续订证书，因此很容易部署证书并提高安全性。

使用的组件

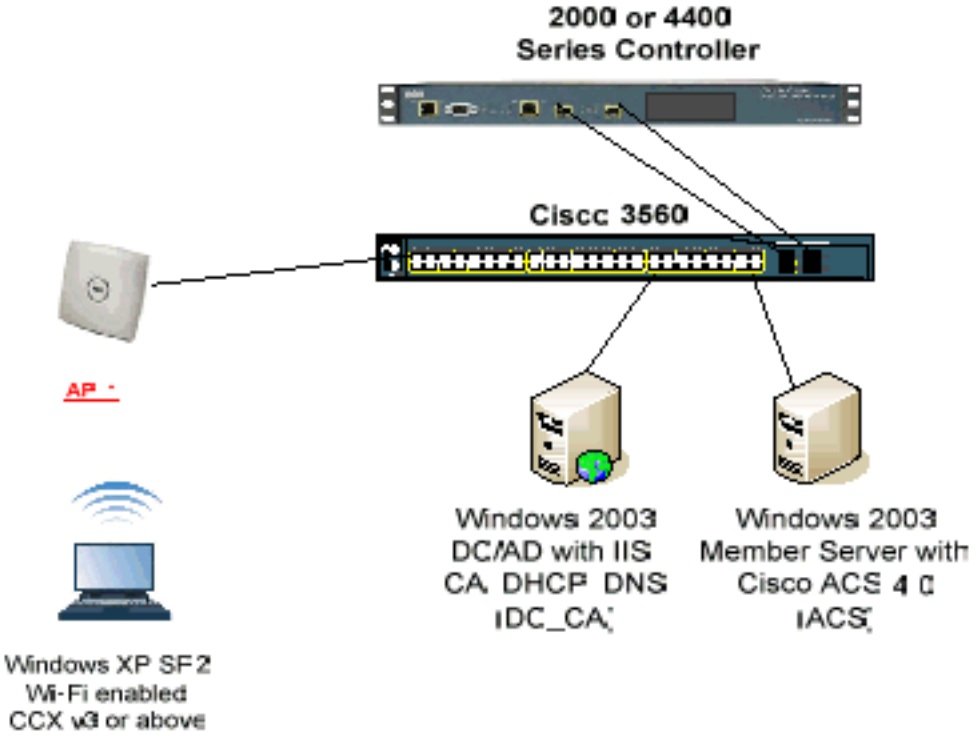
本文档中的信息基于以下软件和硬件版本：

- 运行 3.2.116.21 的 Cisco 2006 或 4400 系列控制器
- Cisco 1131 轻量接入点协议 (LWAPP) AP
- 装有 Internet Information Server (IIS)、证书颁发机构 (CA)、DHCP 和域名系统 (DNS) 的 Windows 2003 Enterprise
- 具有访问控制服务器 (ACS) 4.0 的 Windows 2003 Standard
- 具有 SP（和更新的 Service Pack）以及无线网络接口卡 (NIC)（支持 CCX v3）或第三方请求方的 Windows XP Professional。
- Cisco 3560 交换机

网络图

本文档使用以下网络设置：

Cisco 安全无线实验室拓扑



本文档的主要目的是提供分步过程，帮助您在装有 ACS 4.0 的统一无线网络和 Windows 2003 Enterprise 服务器下实施 PEAP。重点是自动注册客户端，使得客户端能够自动注册并从服务器获取证书。

注：要将带临时密钥完整性协议(TKIP)/高级加密标准(AES)的Wi-Fi保护访问(WPA)/WPA2添加到带SP的Windows XP Professional，请参阅WPA2/无线调配服务信息元素(WPS IE)更新用于Windows XP和Service Pack 2 。

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。

Windows Enterprise 2003 中关于 IIS、证书颁发机构、DNS、DHCP 的设置 (DC_CA)

DC_CA (wirelessdemoca)

DC_CA 是一台运行 Windows Server 2003 Enterprise Edition SP1 的计算机，该计算机担当以下角色：

- 运行 IIS 的 **wirelessdemo.local 域的域控制器**

- **wirelessdemo.local DNS 域的 DNS 服务器**
- DHCP 服务器
- **wirelessdemo.local 域的企业根 CA**

要为这些服务配置 DC_CA，请完成以下步骤：

1. 执行基本安装和配置。
2. 将计算机配置为域控制器。
3. 提升域功能级别。
4. 安装并配置 DHCP。
5. 安装证书服务。
6. 验证证书的管理员权限。
7. 向域中添加计算机。
8. 允许计算机进行无线访问。
9. 向域中添加用户。
10. 允许用户进行无线访问。
11. 向域中添加组。
12. 向 wirelessusers 组中添加用户。
13. 向 wirelessusers 组中添加客户端计算机。

步骤 1：执行基本安装和配置

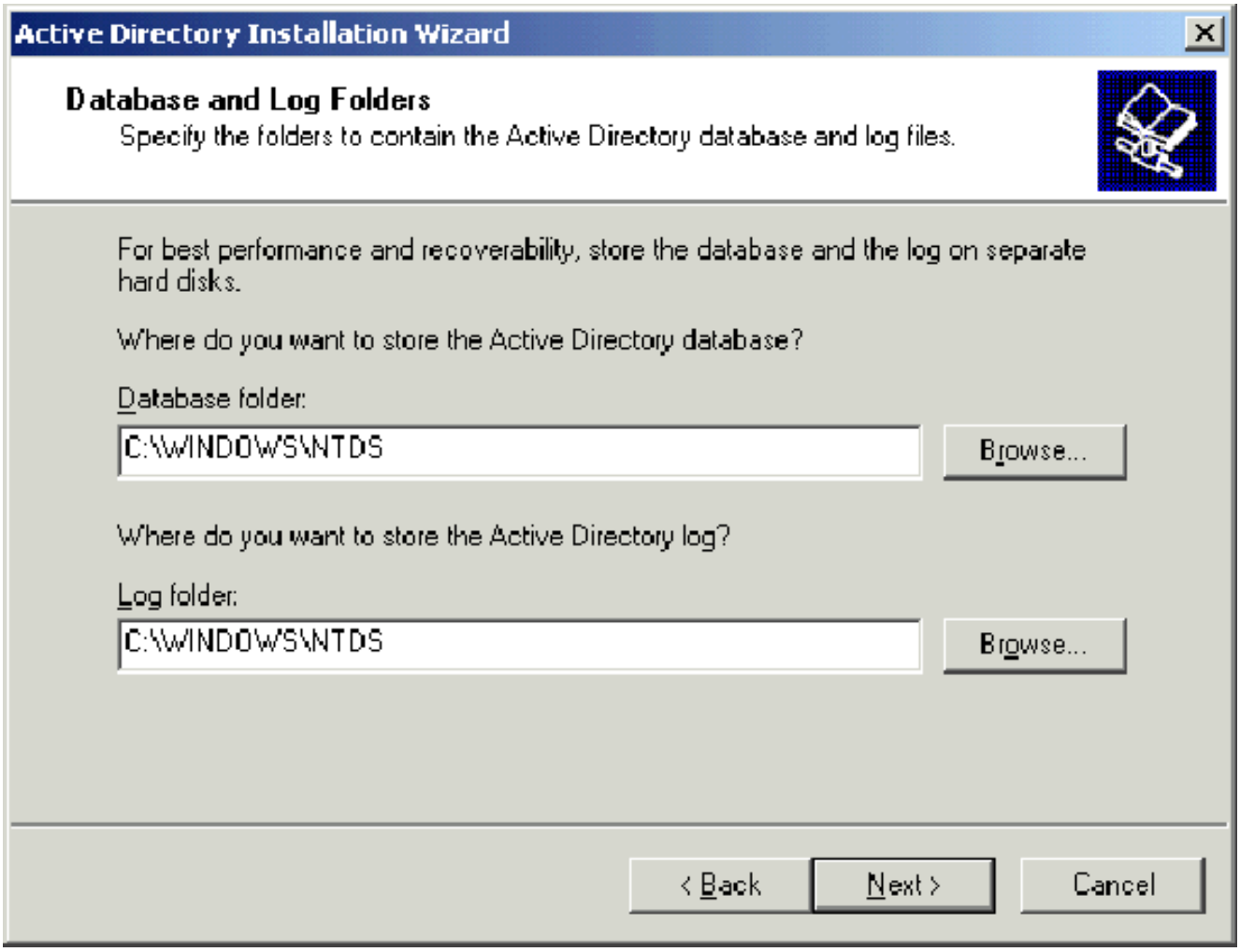
请完成以下步骤：

1. 将 Windows Server 2003 Enterprise Edition SP1 安装为独立服务器。
2. 用 IP 地址 **172.16.100.26 和子网掩码 255.255.255.0 配置 TCP/IP 协议。**

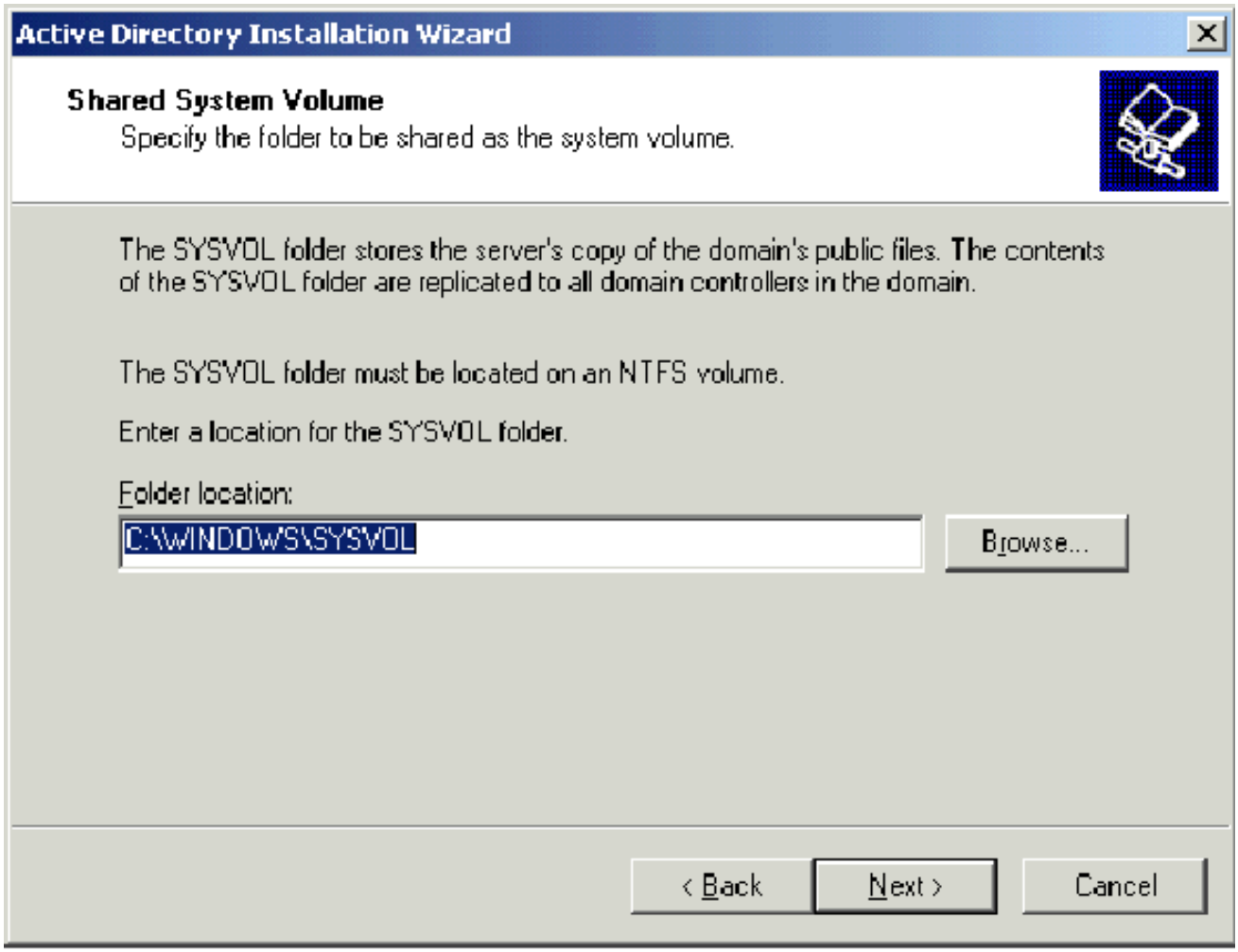
步骤 2：将计算机配置为域控制器

请完成以下步骤：

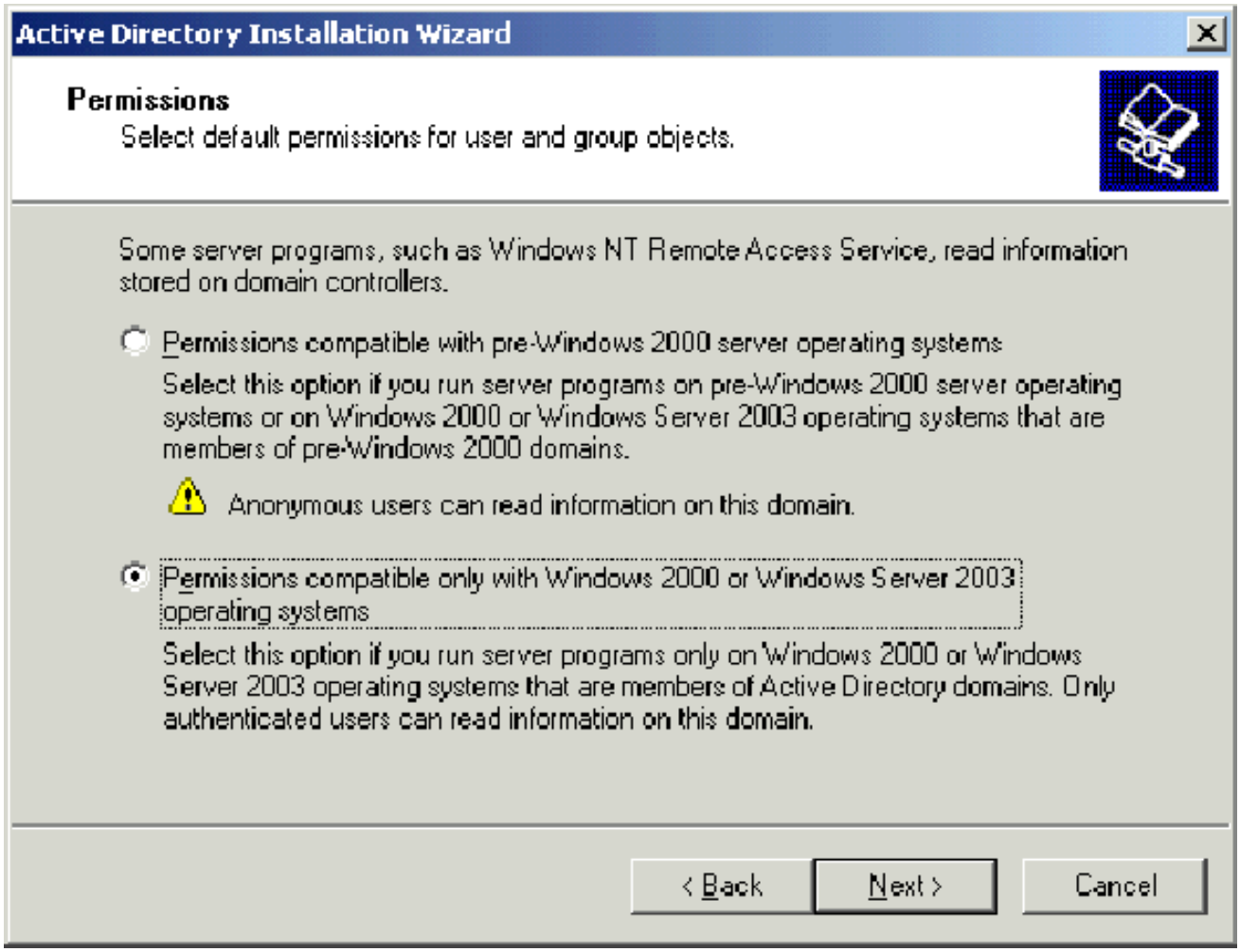
1. 要启动 Active Directory 安装向导，请选择**开始 > 运行**，键入 dcpromo.exe，然后单击“确定”。
2. 在“欢迎使用 Active Directory 安装向导”页上，单击**下一步**。
3. 在“操作系统兼容性”页上，单击**下一步**。
4. 在“域控制器类型”页上，选择**新域的域控制器，然后单击“下一步”。**
5. 在“创建一个新域”页上，选择**在新林中新建域，然后单击“下一步”。**
6. 在“安装或配置 DNS”页上，选择**否，只在这台计算机上安装并配置 DNS，然后单击“下一步”。**
7. 在“新的域名”页上，键入 **wirelessdemo.local，然后单击“下一步”。**
8. 在“NetBIOS 域名”页上，输入 NetBIOS 域名 **wirelessdemo，然后单击“下一步”。**
9. 在“数据库和日志文件夹位置”页上，接受默认的数据库和日志文件夹目录，然后单击**下一步**。



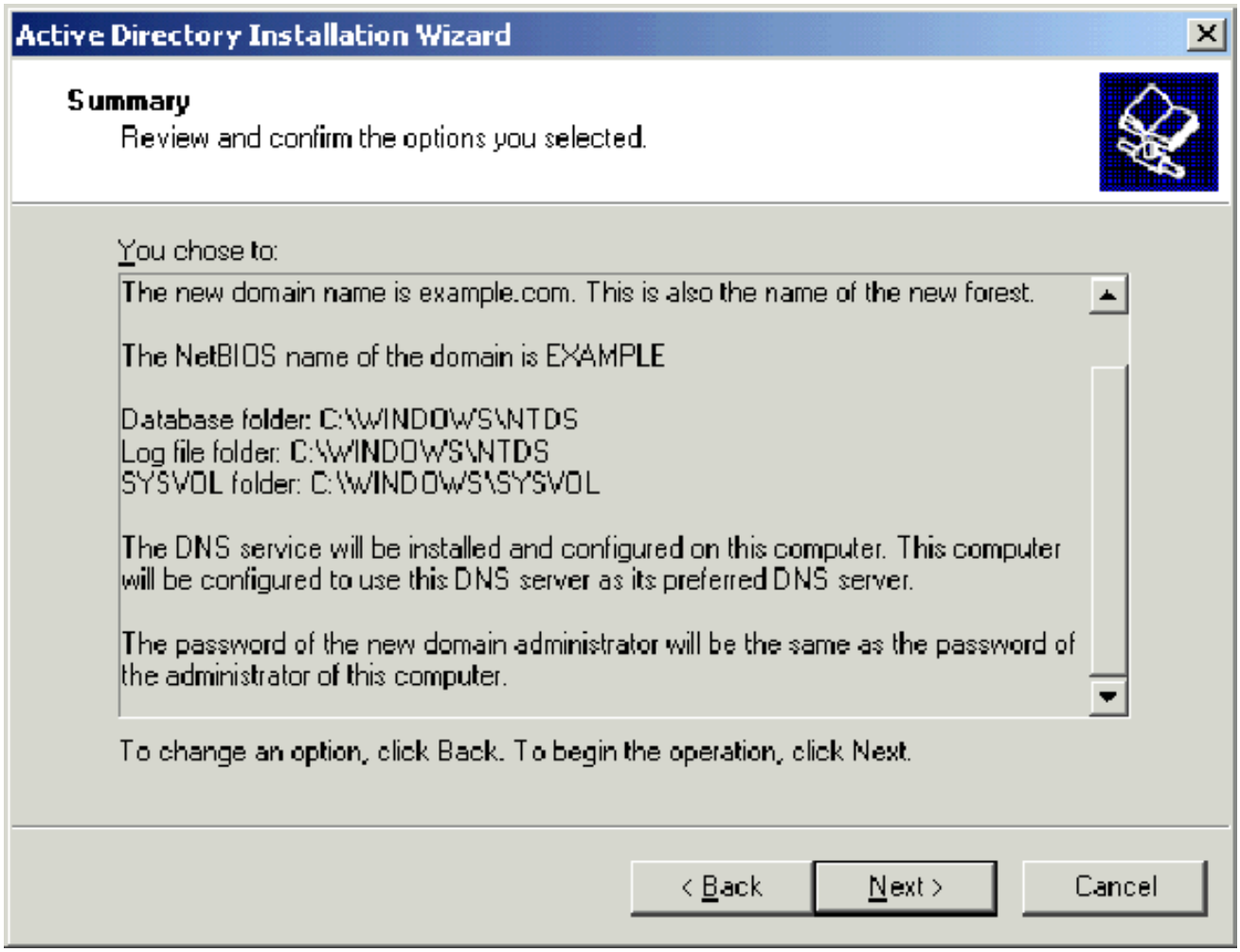
10. 在“共享的系统卷”页上，验证默认文件夹位置正确，然后单击**下一步**。



11. 在“权限”页上，验证选中了**只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限，然后单击“下一步”。**



12. 在“目录服务恢复模式管理密码”页上，将密码框保留为空，然后单击**下一步**。
13. 查看“摘要”页上的信息，然后单击**下一步**。

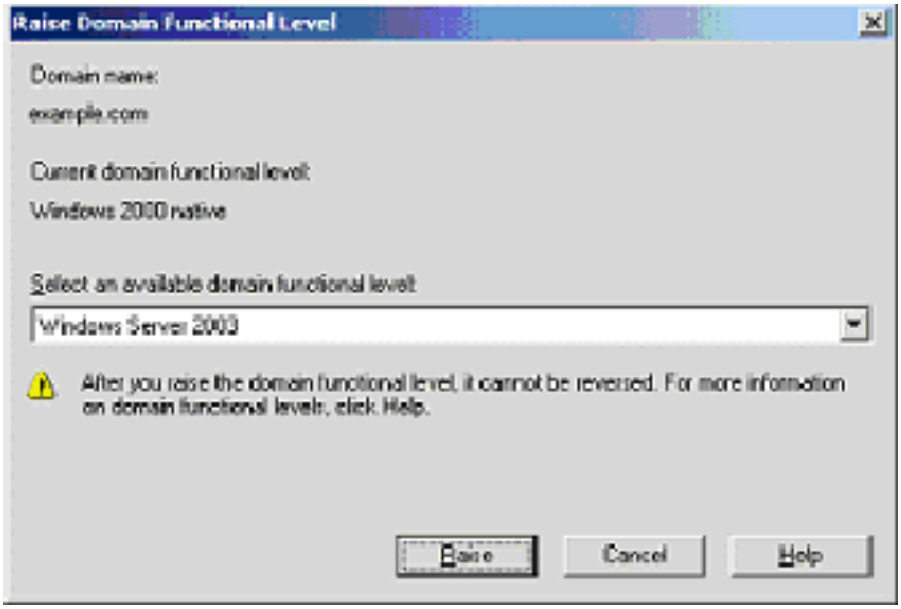


14. 当您完成 Active Directory 的安装后，单击**完成**。
15. 当提示重新启动计算机时，单击**立即重新启动**。

步骤 3：提升域功能级别

请完成以下步骤：

1. 从“管理工具”文件夹（“开始”>“程序”>“管理工具”>“Active Directory 域和信任关系”）打开 **Active Directory 域和信任关系管理单元，然后右键单击域计算机 DC_CA.wirelessdemo.local。**
2. 单击**提升域功能级别**，然后在“提升域功能级别”页上选择 Windows Server 2003。

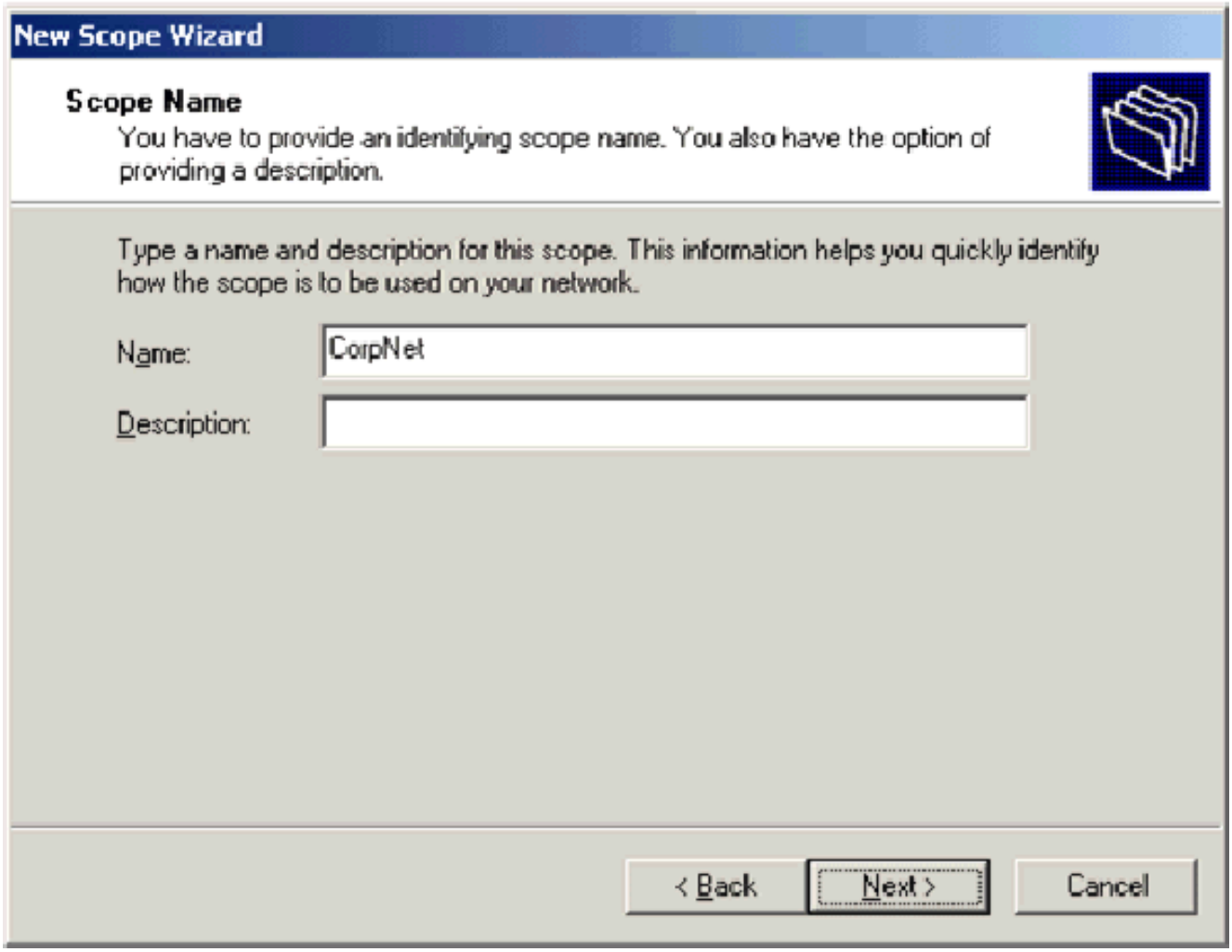


3. 单击**提升**，单击“确定”，然后再次单击“确定”。

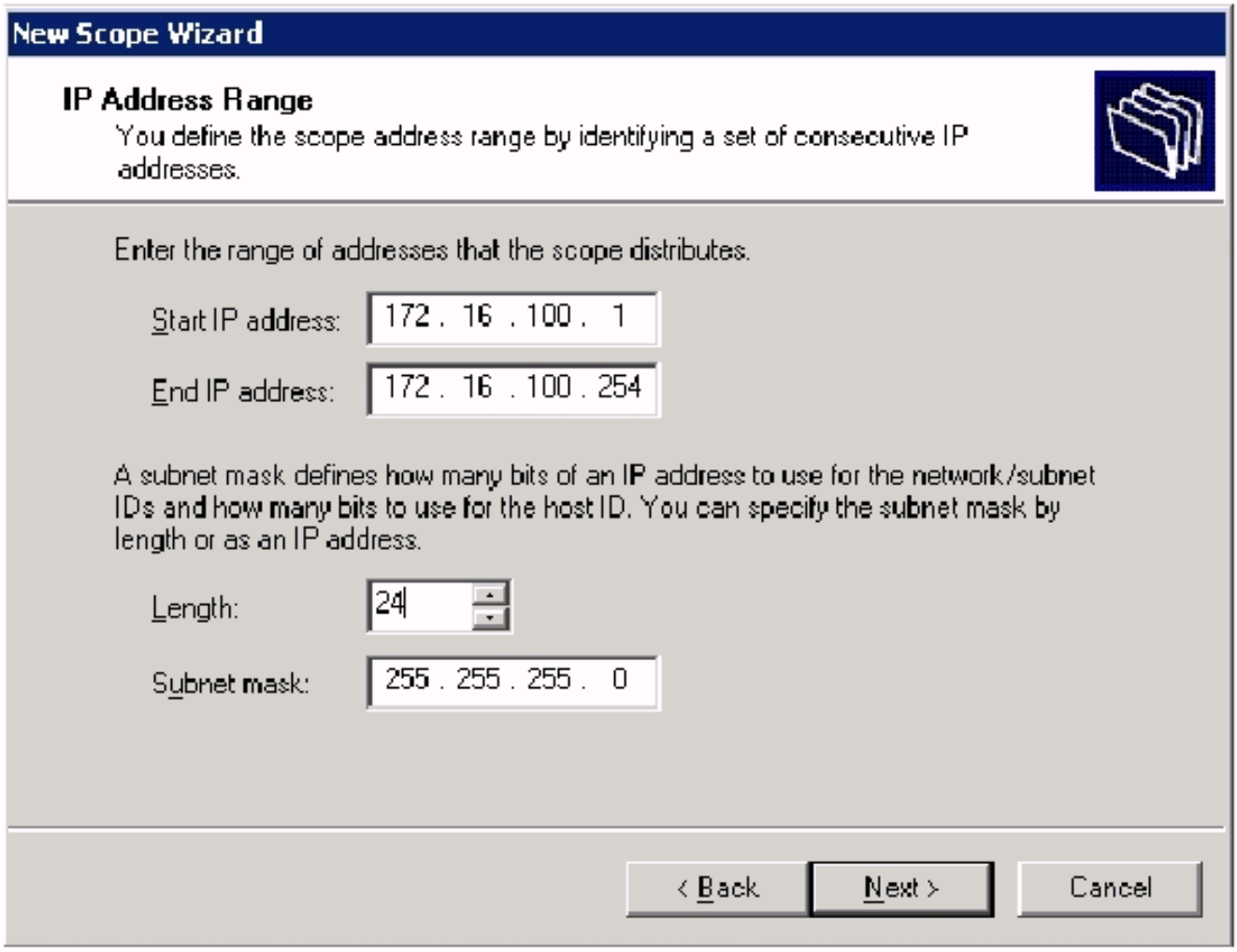
步骤 4：安装并配置 DHCP

请完成以下步骤：

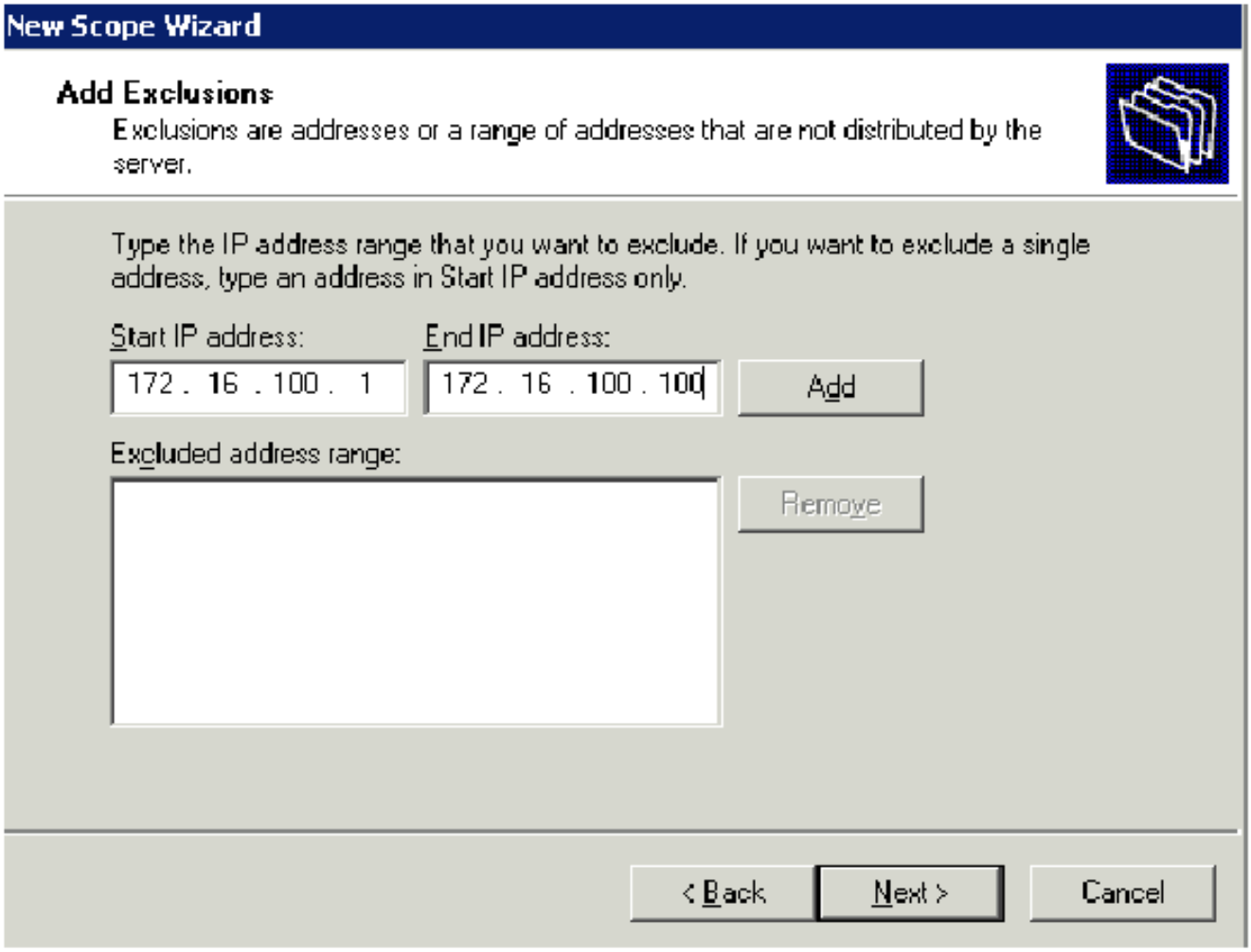
1. 使用“控制面板”中的“添加或删除程序”安装**动态主机配置协议 (DHCP) 作为网络服务组件。**
2. 从“管理工具”文件夹中打开 **DHCP 管理单元（“开始”>“程序”>“管理工具”>“DHCP”），然后突出显示 DHCP 服务器：DC_CA.wirelessdemo.local。**
3. 单击**操作**，然后单击“授权”以便授权 DHCP 服务。
4. 在控制台树中，右键单击 **DC_CA.wirelessdemo.local**，然后单击“新建作用域”。
5. 在“新建作用域向导”的“欢迎”页上，单击**下一步。**
6. 在“作用域名称”页上，在“名称”字段中键入 **CorpNet。**



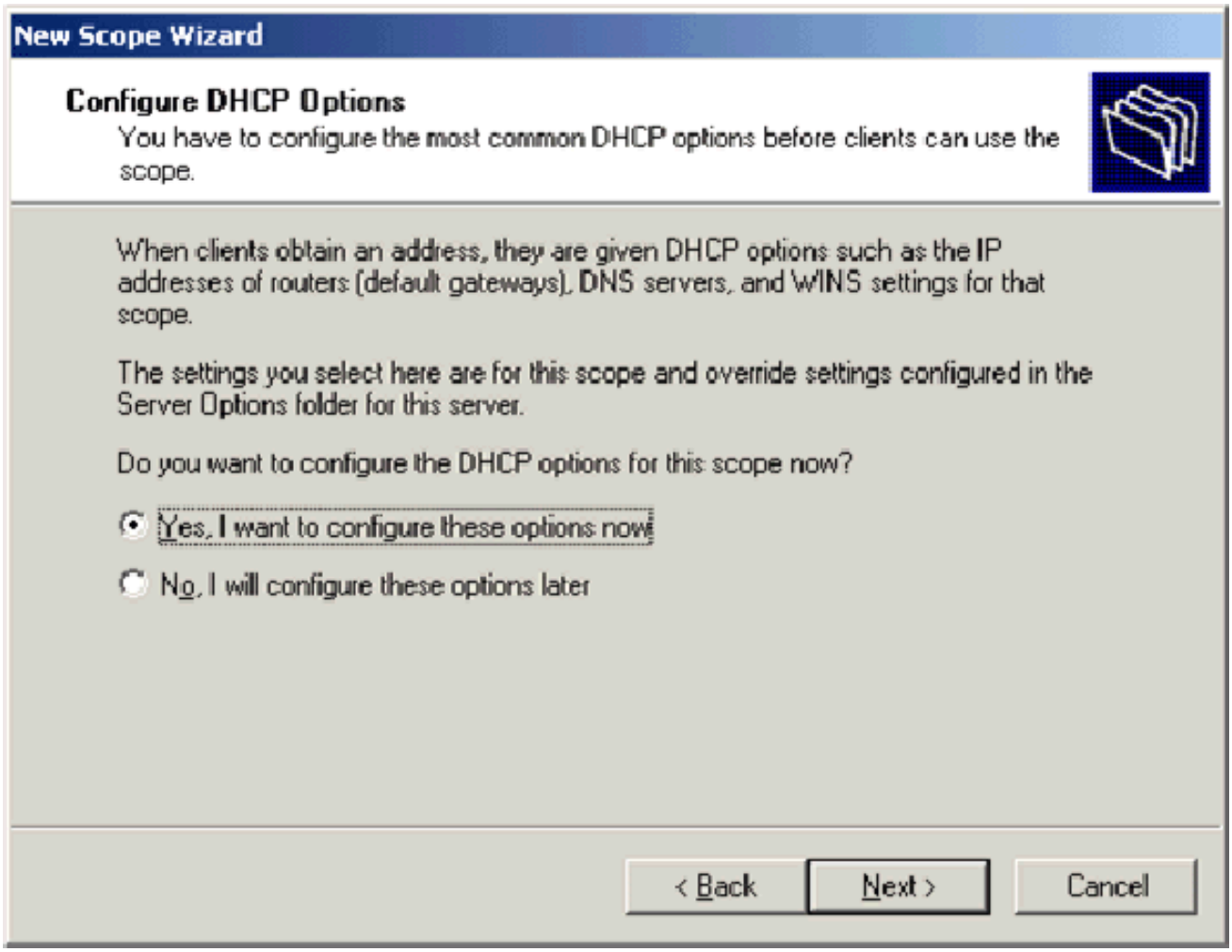
7. 单击**下一步 并填写以下参数：**起始 IP 地址 — **172.16.100.1**结束 IP 地址 — **172.16.100.254**长度(Length)- **24**子网掩码— **255.255.255.0**



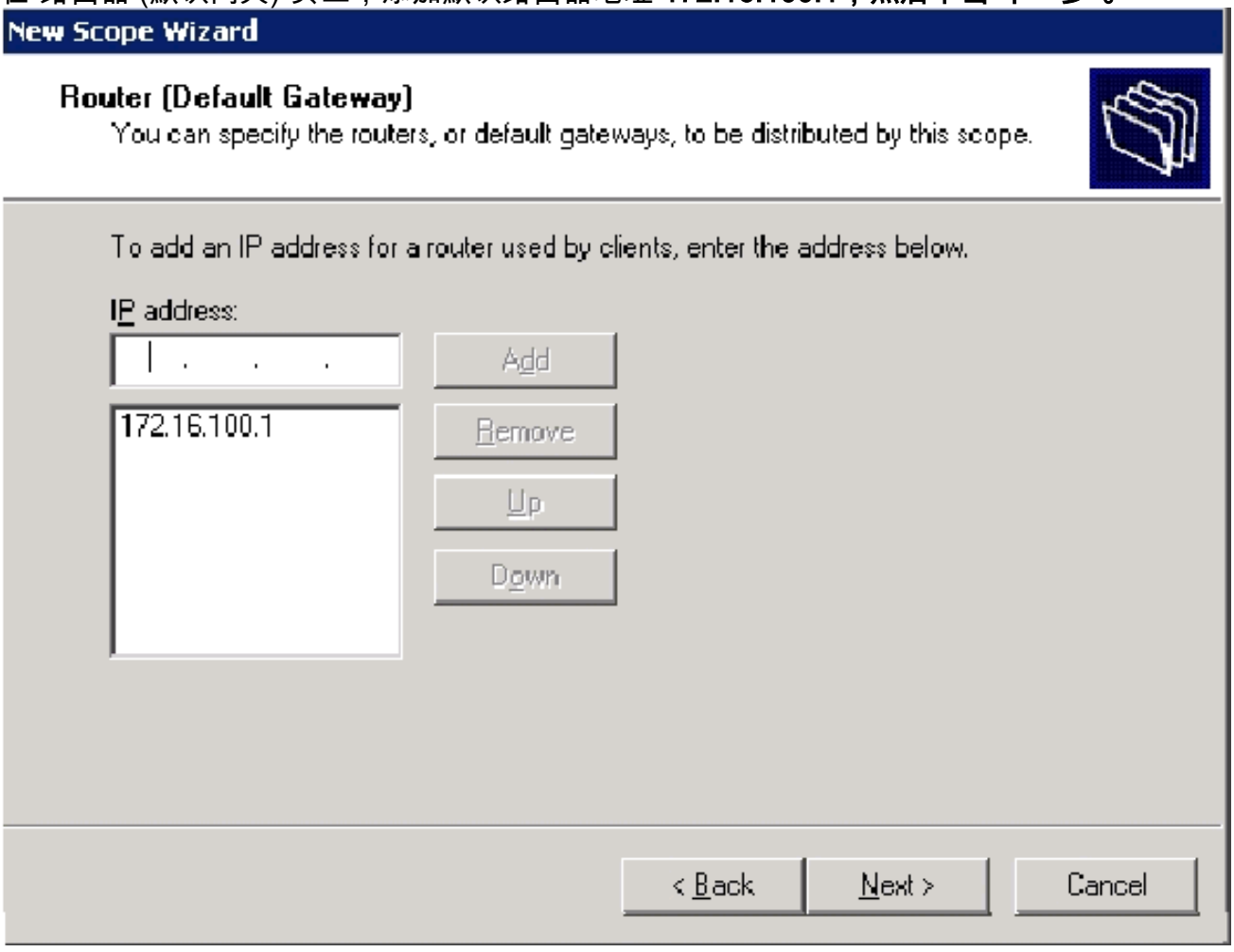
8. 单击**下一步，并输入 172.16.100.1 作为要排除的"起始 IP 地址"，输入 172.16.100.100 作为要排除的"结束 IP 地址"。**然后，单击**下一步**。这将保留172.16.100.1到172.16.100.100范围内的IP地址。这些保留的IP地址不由DHCP服务器分配。



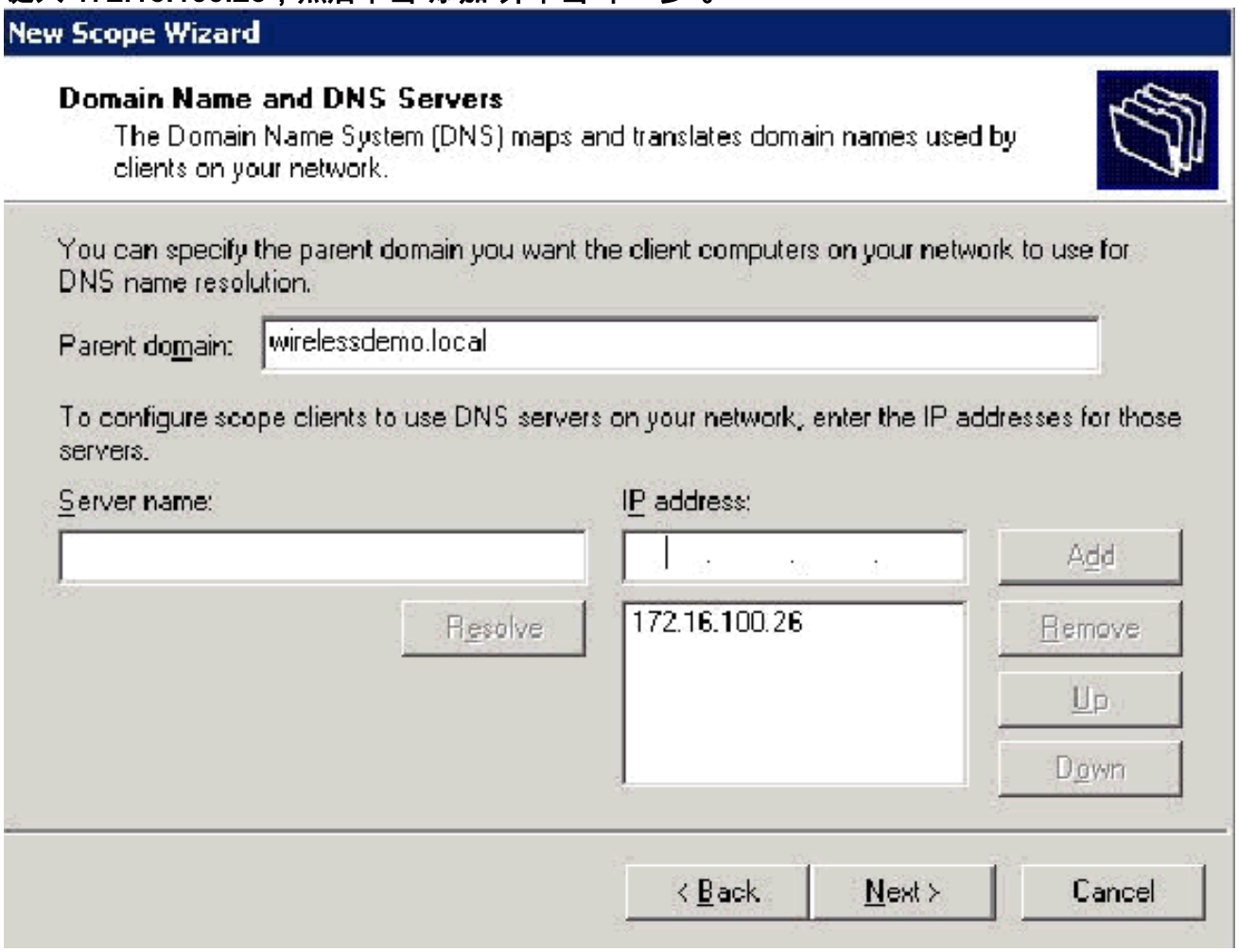
9. 在“租约期限”页上，单击**下一步**。
10. 在“配置 DHCP 选项”页上，选择**是，我想现在配置这些选项，然后单击“下一步”。**



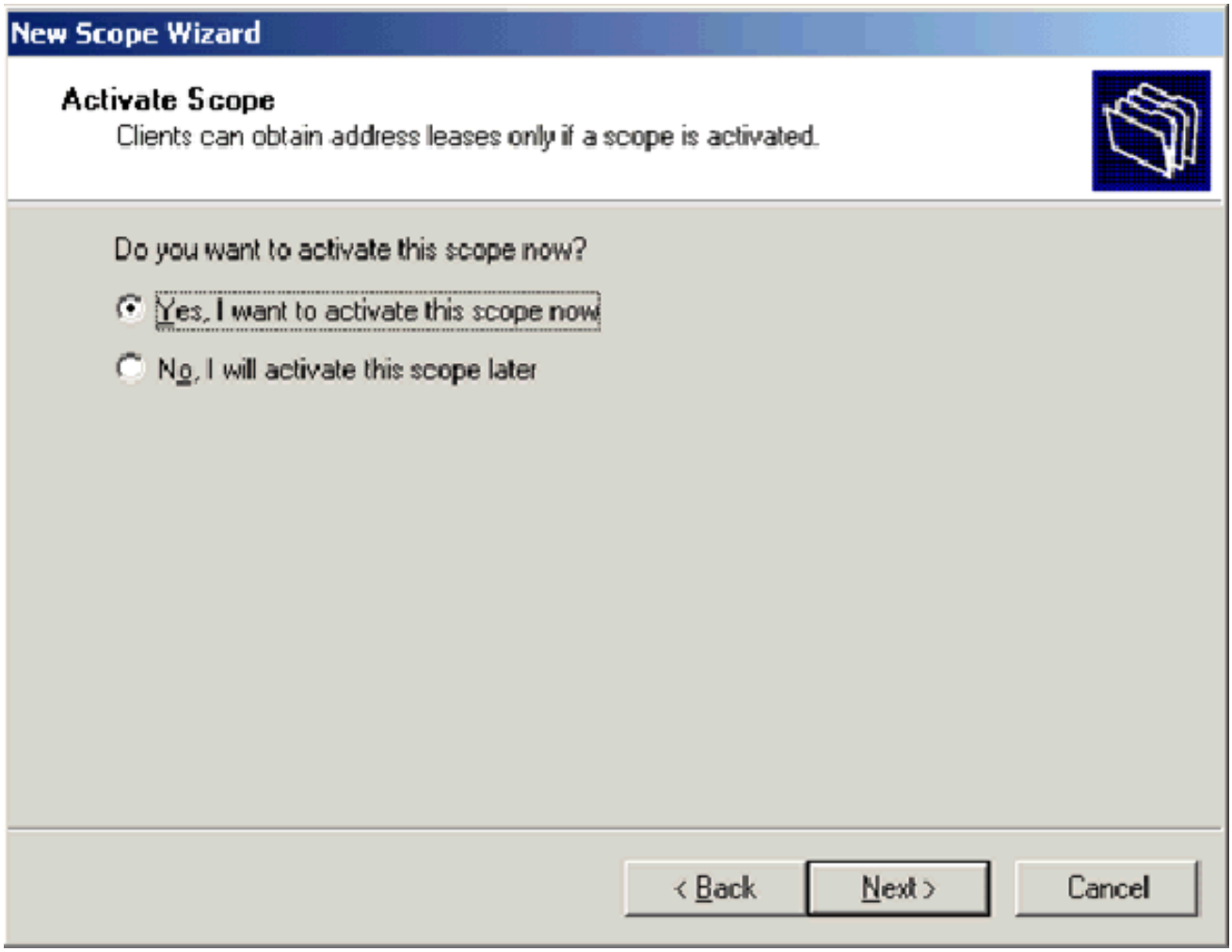
11. 在“路由器 (默认网关)”页上，添加默认路由器地址 172.16.100.1，然后单击“下一步”。



12. 在“域名称和 DNS 服务器”页上，在“父域”字段中键入 **wirelessdemo.local，在“IP 地址”字段中键入 172.16.100.26，然后单击“添加”并单击“下一步”。**



13. 在“WINS 服务器”页上，单击**下一步。**
14. 在“激活作用域”页上，选择**是，我想现在激活此作用域，然后单击“下一步”。**



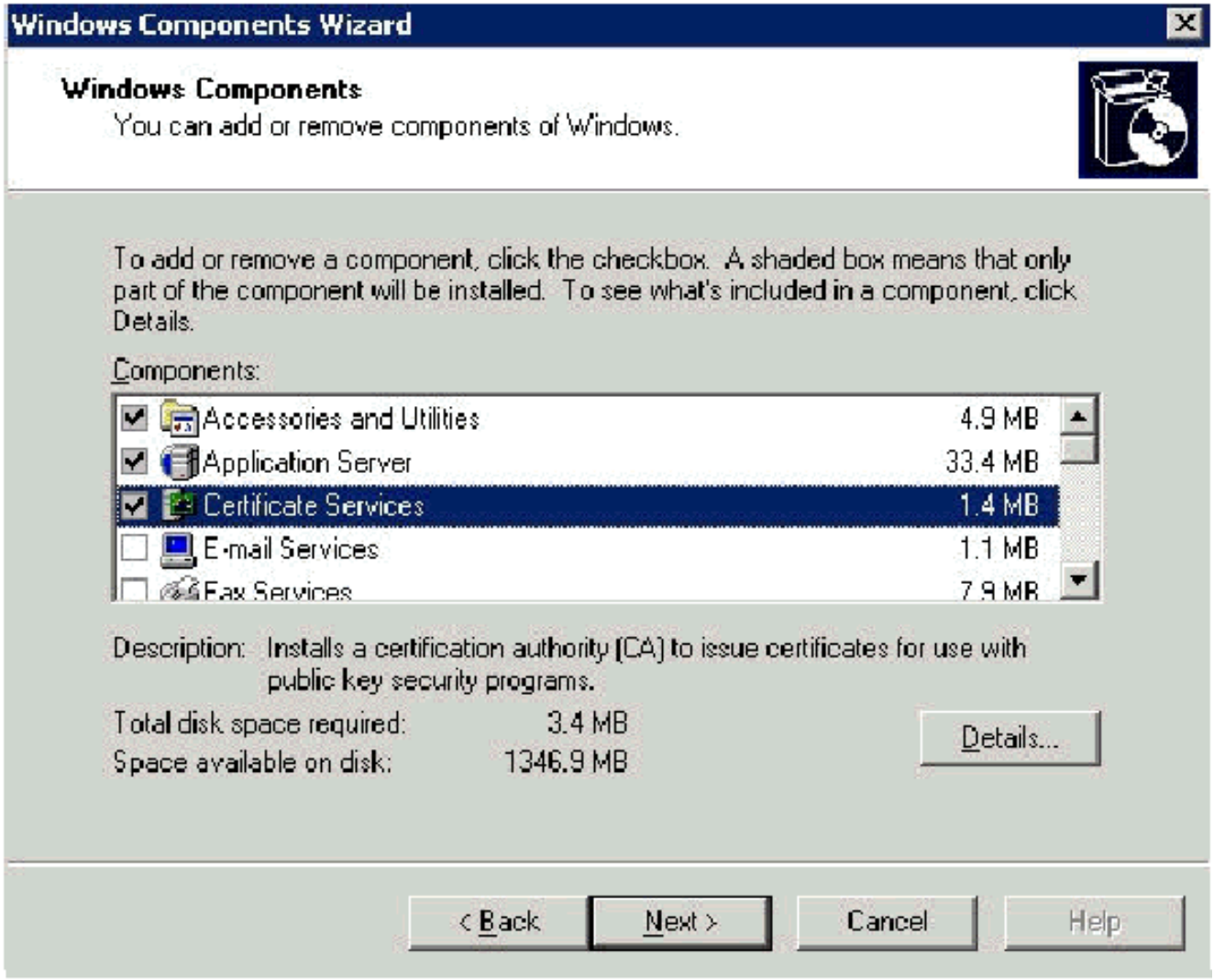
15. 当您完成“新建作用域向导”页时，单击**完成**。

步骤 5：安装证书服务

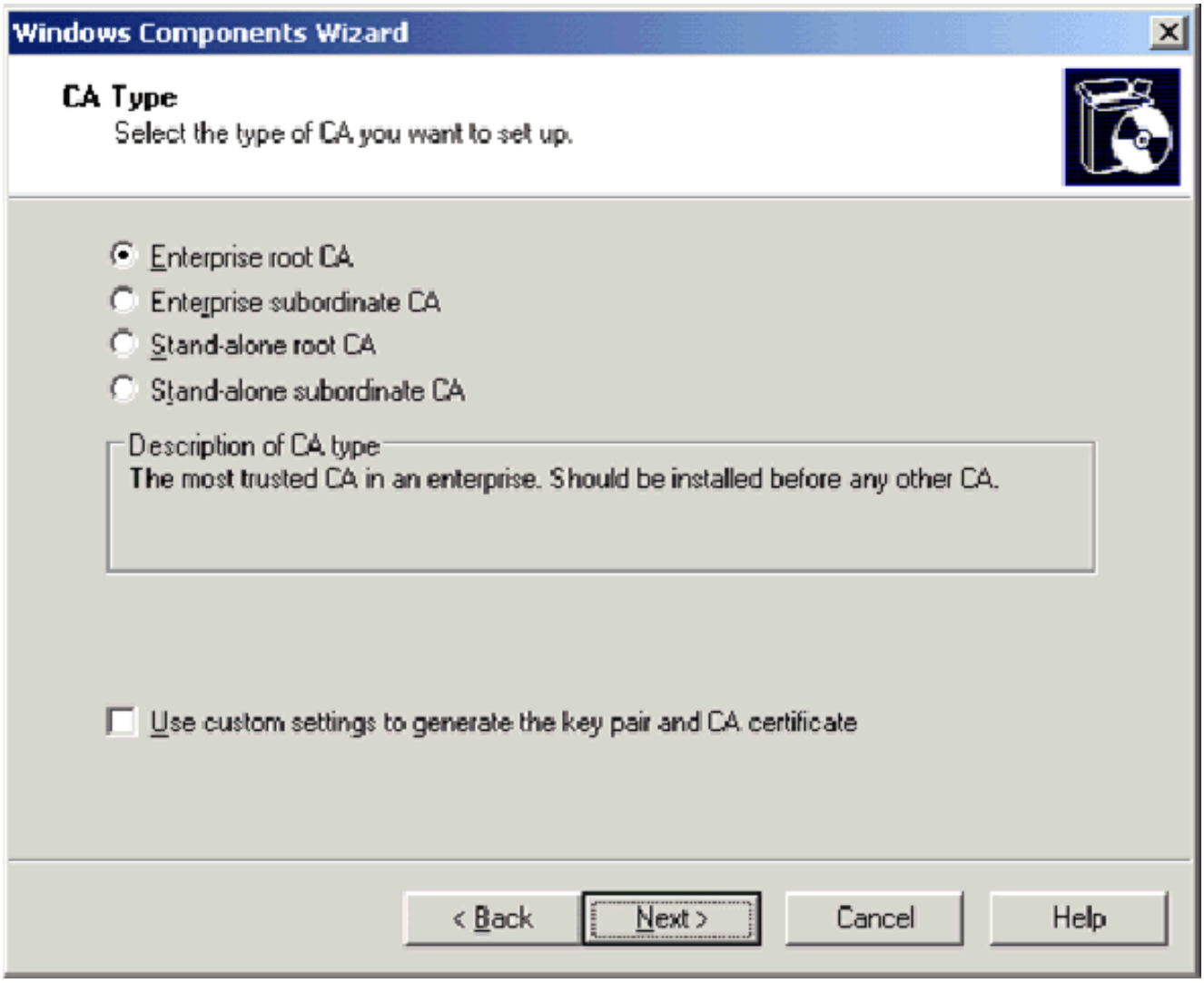
请完成以下步骤：

注意：在安装证书服务之前必须安装IIS，用户应是企业管理OU的一部分。

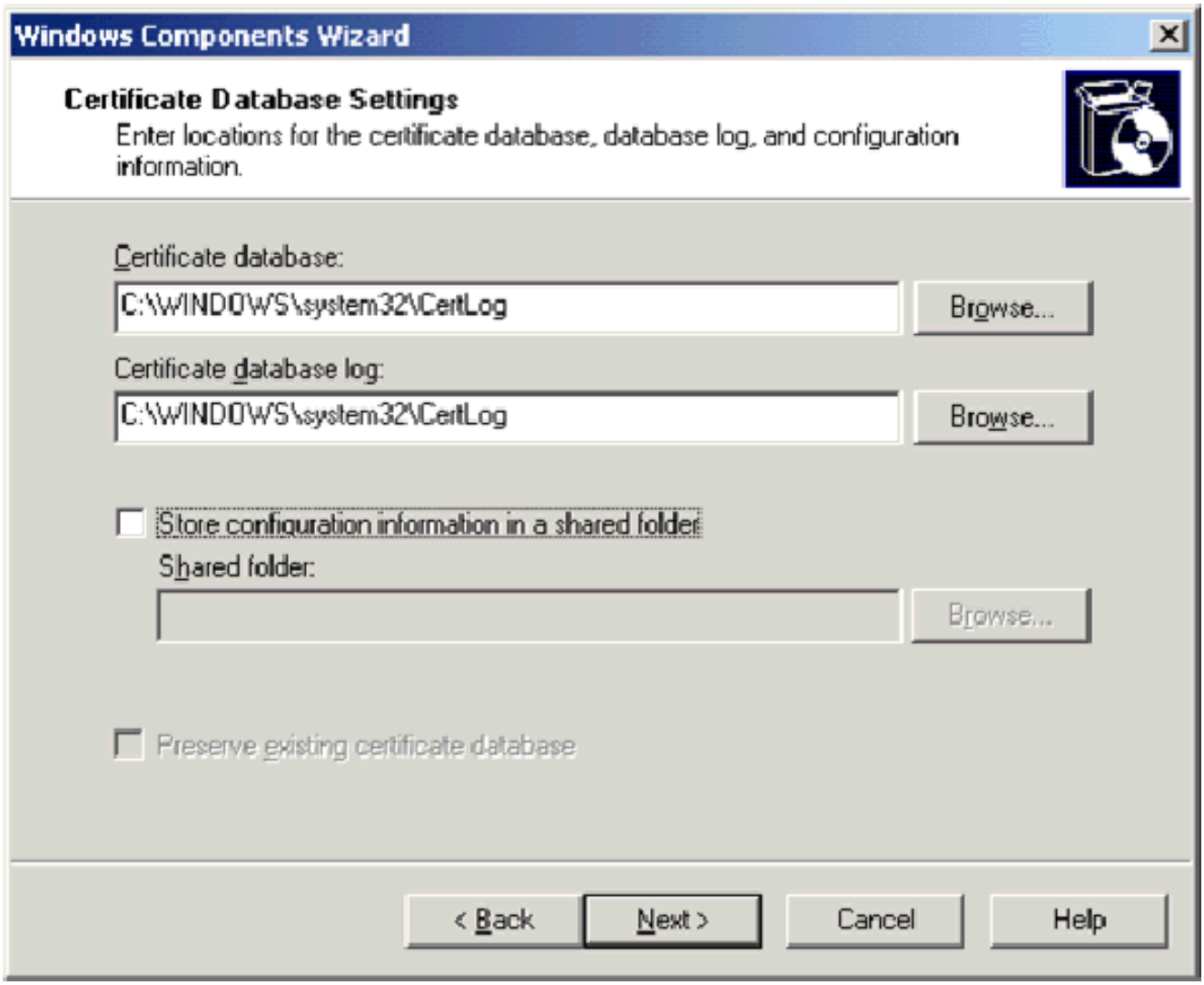
1. 在“控制面板”中，打开**添加或删除程序**，然后单击“添加/删除 Windows 组件”。
2. 在“Windows 组件向导”页上，选择**证书服务**，然后单击“下一步”。



3. 在“CA 类型”页上，选择**企业根 CA，然后单击“下一步”。**



4. 在“CA 识别信息”页上，在“此 CA 的公用名称”框中键入 **wirelessdemoca。**您也可以输入其他可选的详细信息。然后单击**下一步，并接受“证书数据库设置”页上的默认值。**

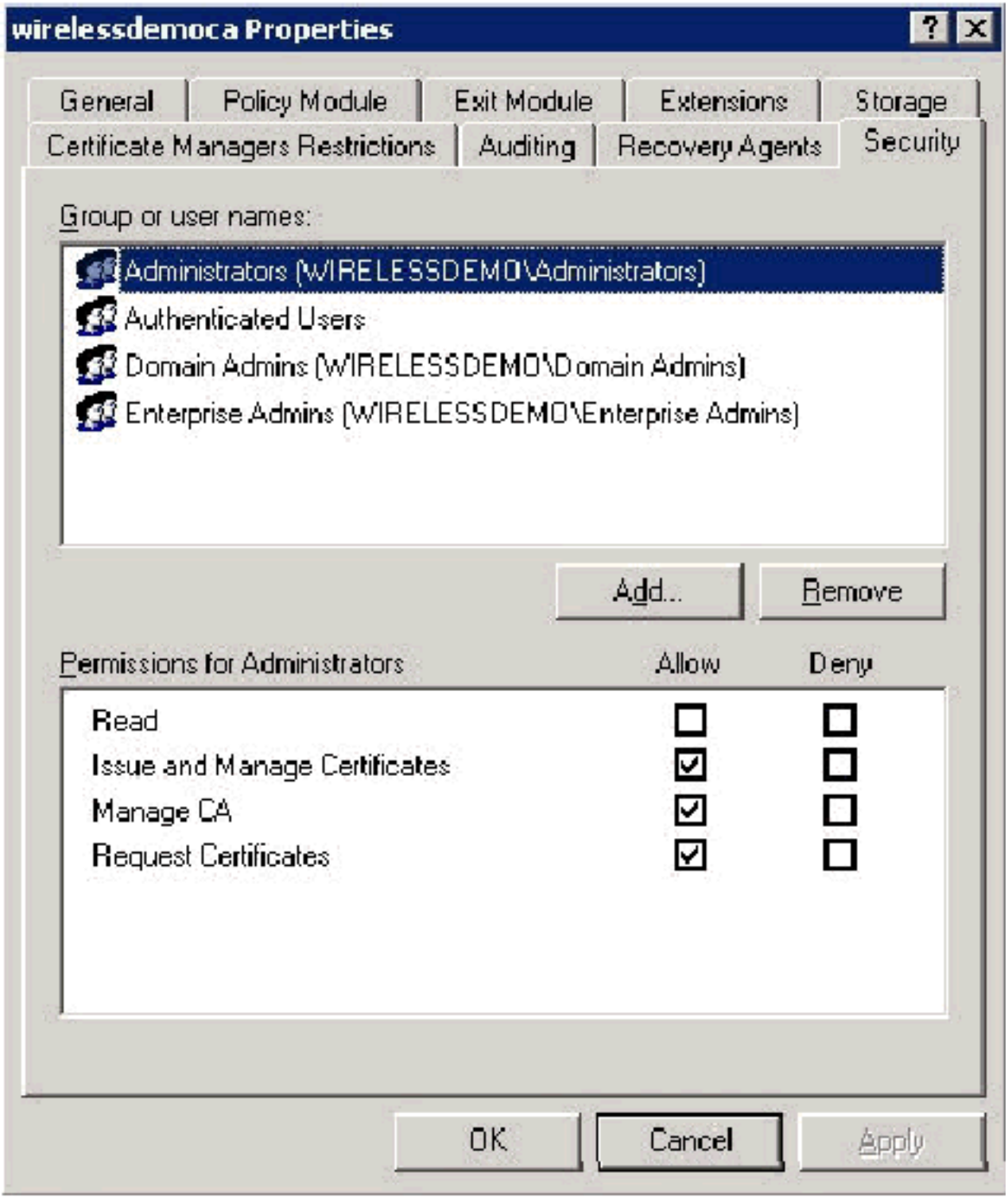


5. 单击 **Next**。在安装完成时，单击**完成**。
6. 在您读完有关安装 IIS 的警告消息后，单击**确定**。

步骤 6：验证证书的管理员权限

请完成以下步骤：

1. 选择**开始 > 管理工具 > 证书颁发机构**。
2. 右键单击 **wirelessdemoca CA，然后单击"属性"**。
3. 在"安全性"选项卡上，单击"组或用户名称"列表中的**管理员**。
4. 在"权限或管理员"列表中，验证以下选项均设置为**允许**：颁发和管理证书管理 CA请求证书如果其中任意一项设置为"拒绝"或未选中，请将该权限设置为**允许**。



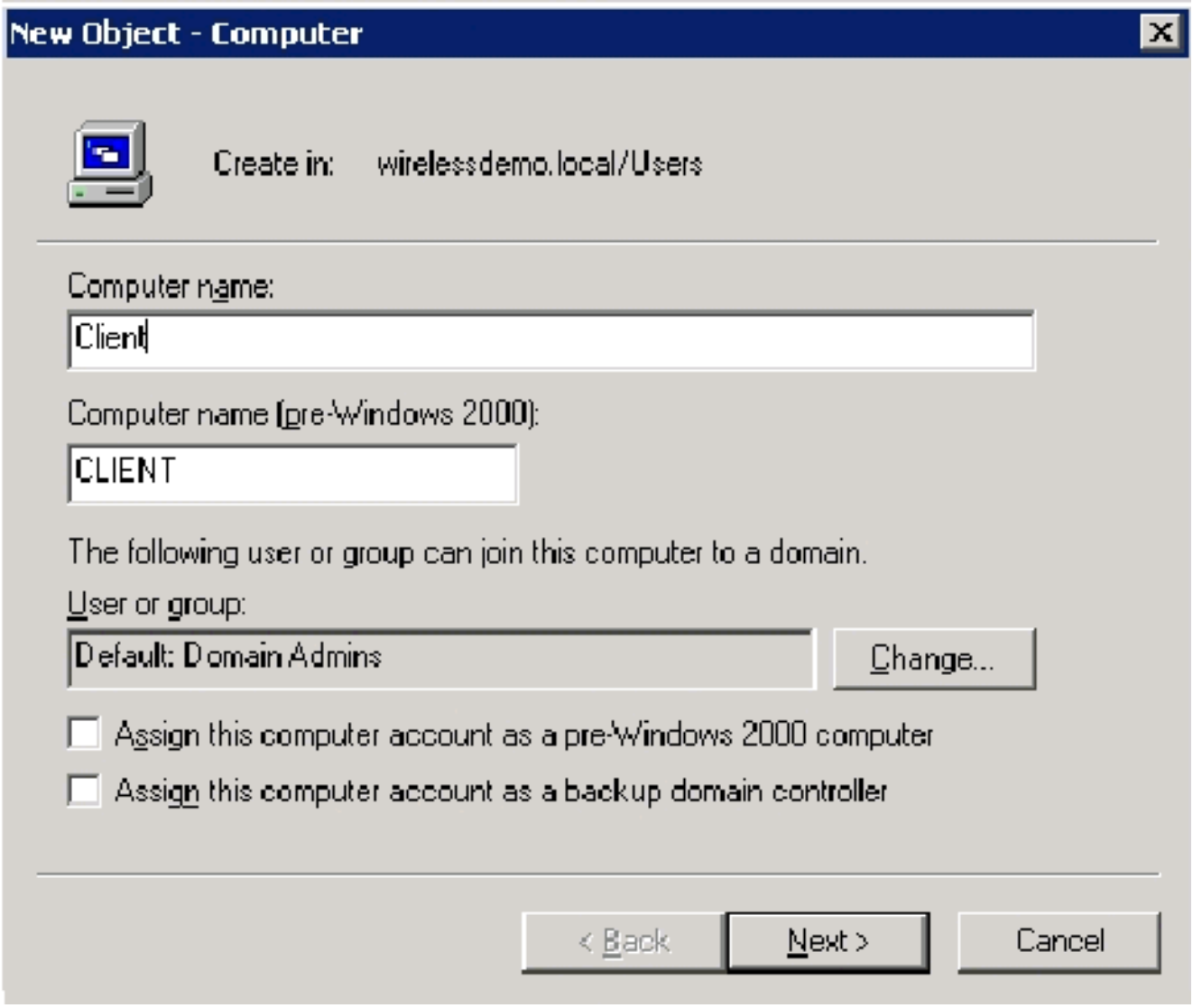
5. 单击**确定关闭“wirelessdemoca CA 属性”对话框，然后关闭“证书颁发机构”。**

步骤 7：向域中添加计算机

请完成以下步骤：

注意：如果计算机已添加到域，请继续执行向域添加用户。

1. 打开 **Active Directory 用户和计算机管理单元。**
2. 在控制台树中，展开 **wirelessdemo.local。**
3. 右键单击**用户**，单击“新建”，然后单击“计算机”。
4. 在“新建对象 – 计算机”对话框中，在“计算机名称”字段中键入计算机的名称，然后单击**下一步**。本示例使用计算机名称 **Client。**



5. 在“托管”对话框中，单击**下一步**。
6. 在“新建对象 – 计算机”对话框中，单击**完成**。
7. 重复步骤 3 到步骤 6，创建更多计算机帐户。

步骤 8::允许计算机进行无线访问

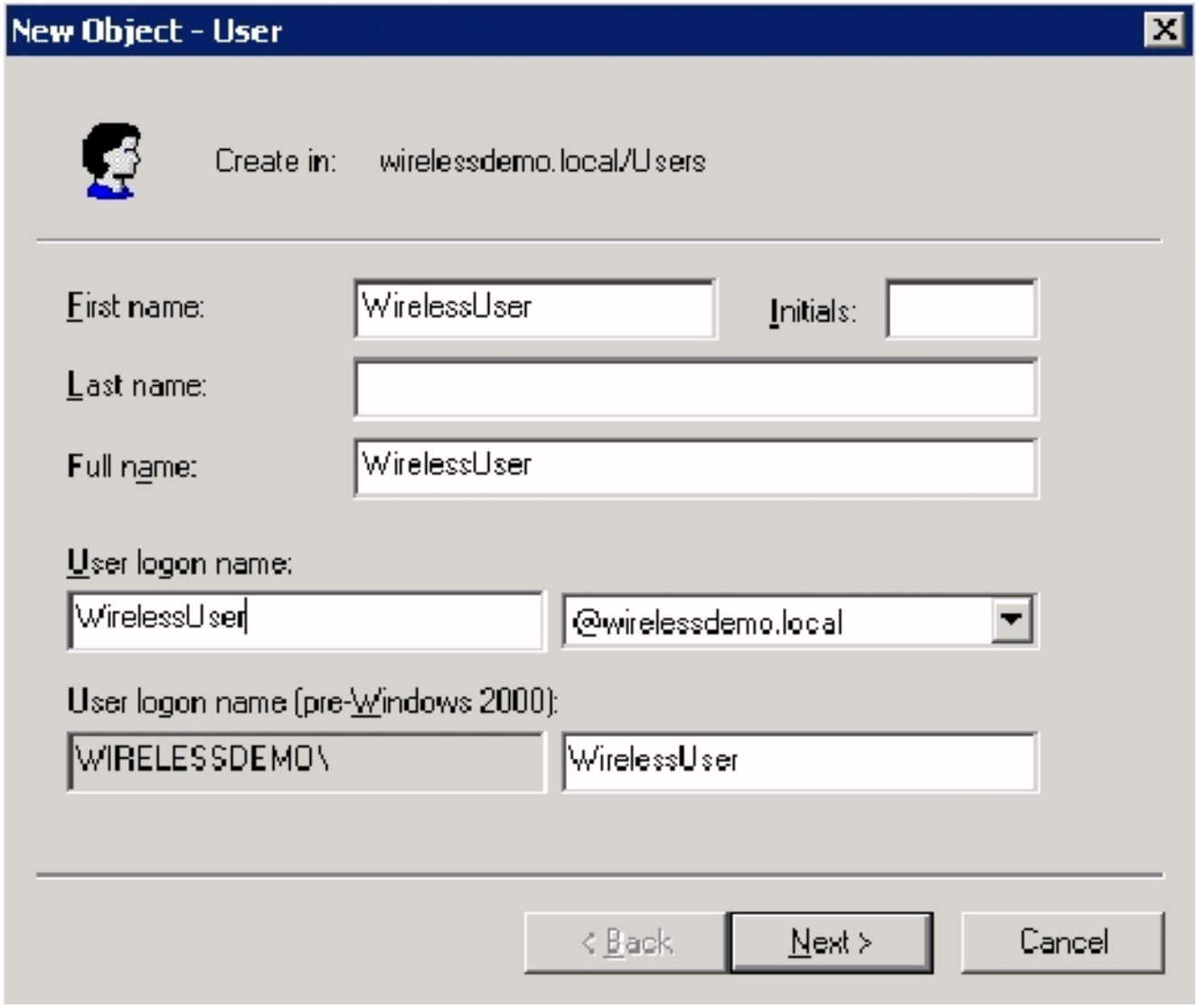
请完成以下步骤：

1. 在“Active Directory 用户和计算机”控制台树中，单击**计算机文件夹，然后右键单击要分配无线访问权限的计算机。**本示例显示的操作步骤针对您在步骤 7 中添加的计算机 **Client。单击“属性”，然后转至“拨号”选项卡。**
2. 选择**允许访问，然后单击“确定”。**

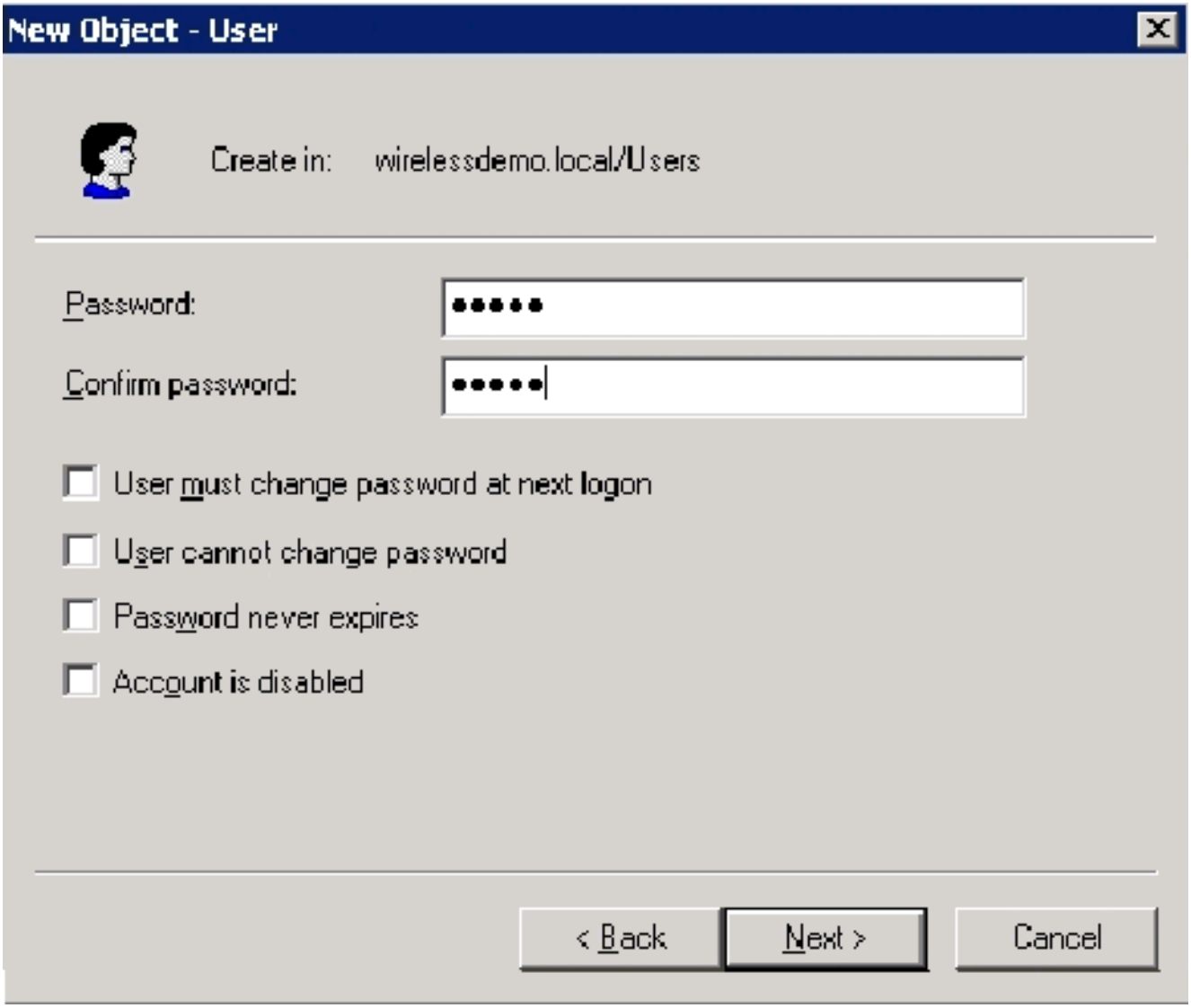
步骤 9：向域中添加用户

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，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”。**



4. 在“新建对象 – 用户”对话框中，单击**完成**。
5. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

步骤 10：允许用户进行无线访问

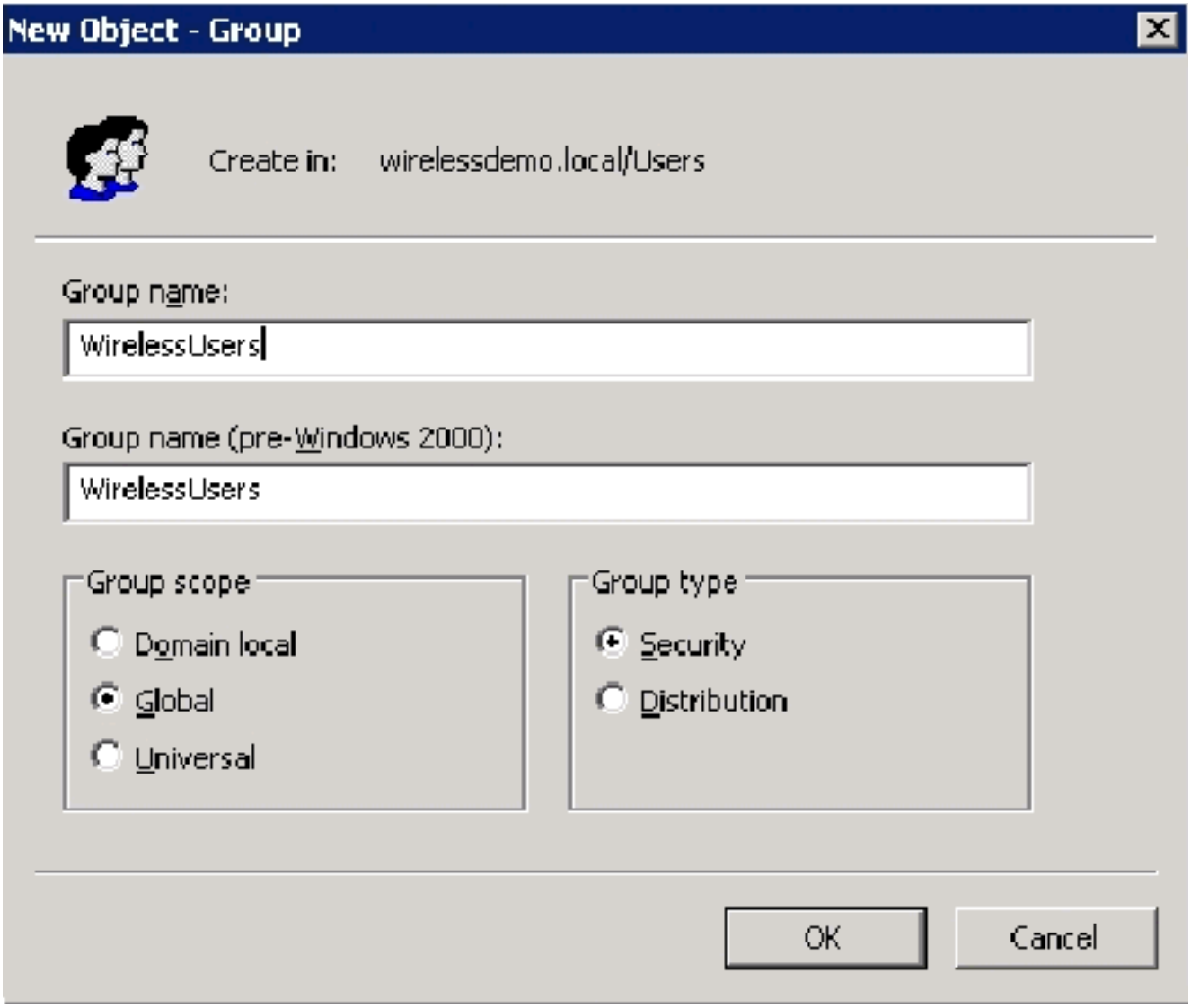
请完成以下步骤：

1. 在 **Active Directory 用户和计算机控制台树中，单击“用户”文件夹，右键单击“WirelessUser”，单击“属性”，然后转至“拨号”选项卡。**
2. 选择**允许访问，然后单击“确定”。**

步骤 11：向域中添加组

请完成以下步骤：

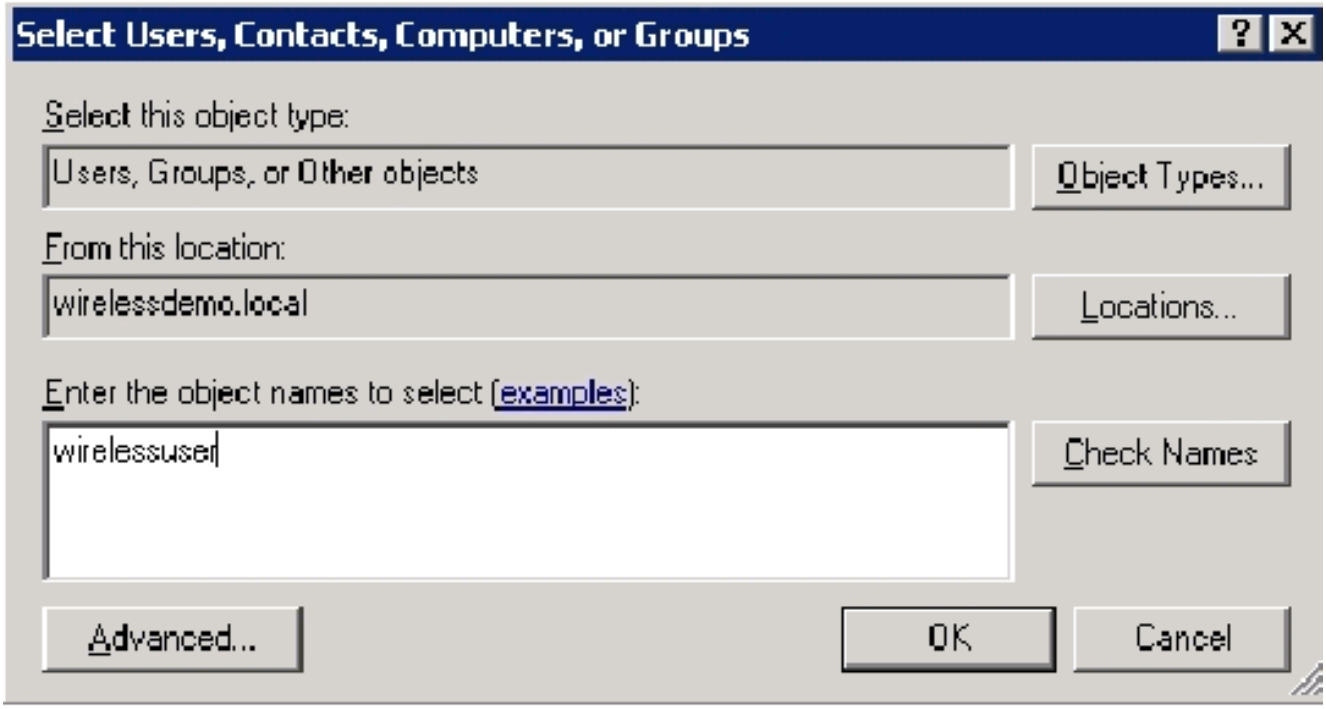
1. 在 **Active Directory 用户和计算机控制台树中，右键单击“用户”，单击“新建”，然后单击“组”。**
2. 在“新建对象 – 组”对话框中，在“组名”字段中键入组的名称，然后单击**确定**。本文档使用组名 **WirelessUsers**。



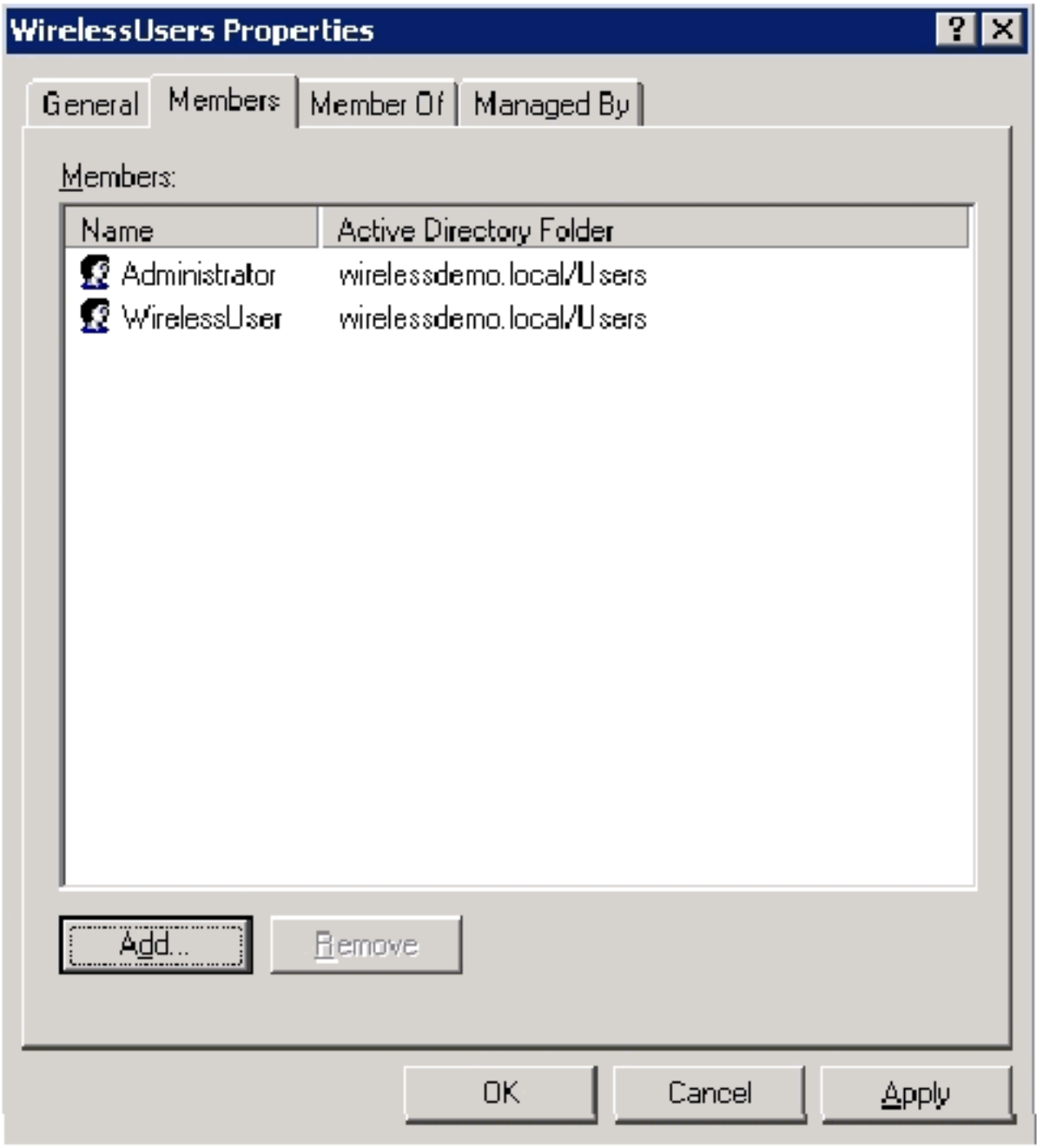
步骤 12：向 wirelessusers 组中添加用户

请完成以下步骤：

1. 在“Active Directory 用户和计算机”的详细信息窗格中，双击组 **WirelessUsers**。
2. 转至“成员”选项卡，然后单击**添加**。
3. 在“选择用户、联系人、计算机或组”对话框中，键入要添加到组中的用户的名称。本示例显示如何将用户 **wirelessuser 添加到组中。**Click
   OK.



4. 在“发现多个名称”对话框中，单击**确定**。此时会将 wirelessuser 用户帐户添加到 wirelessusers 组中。

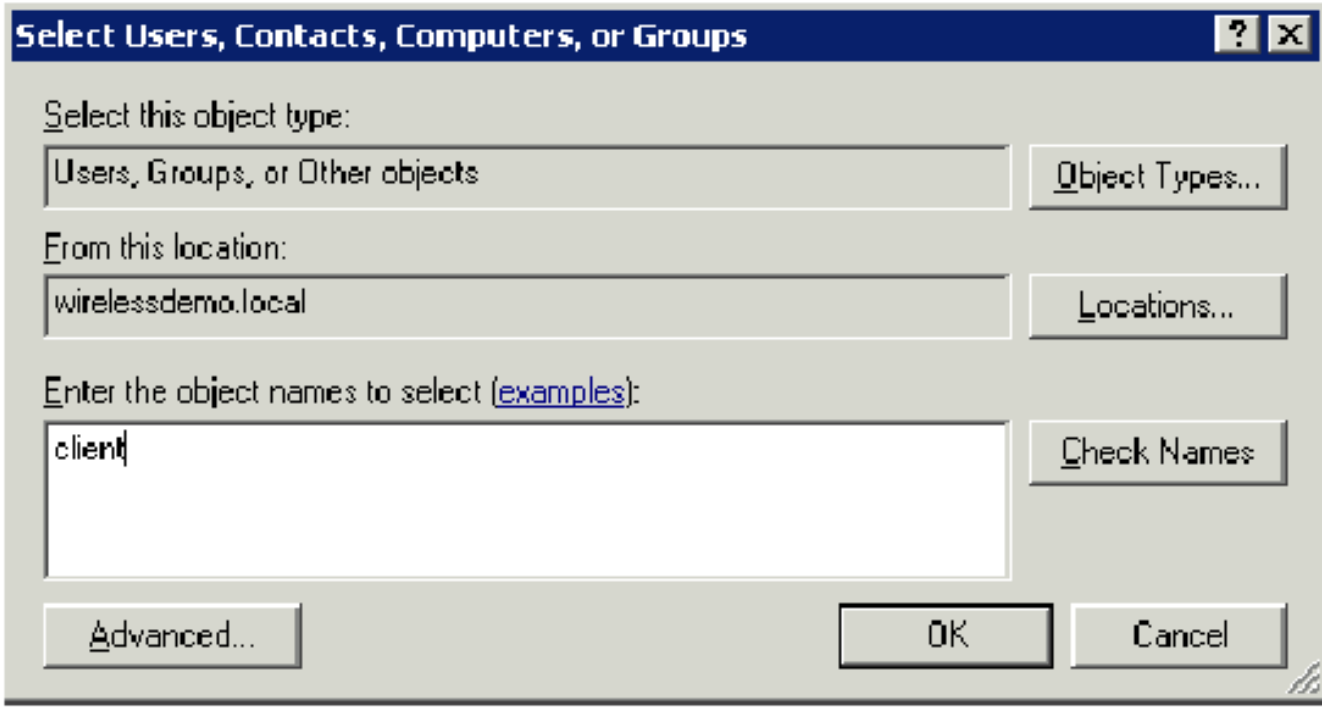


5. 单击**确定，以便保存对 WirelessUsers 组的更改。**
6. 重复此过程，向该组中添加更多用户。

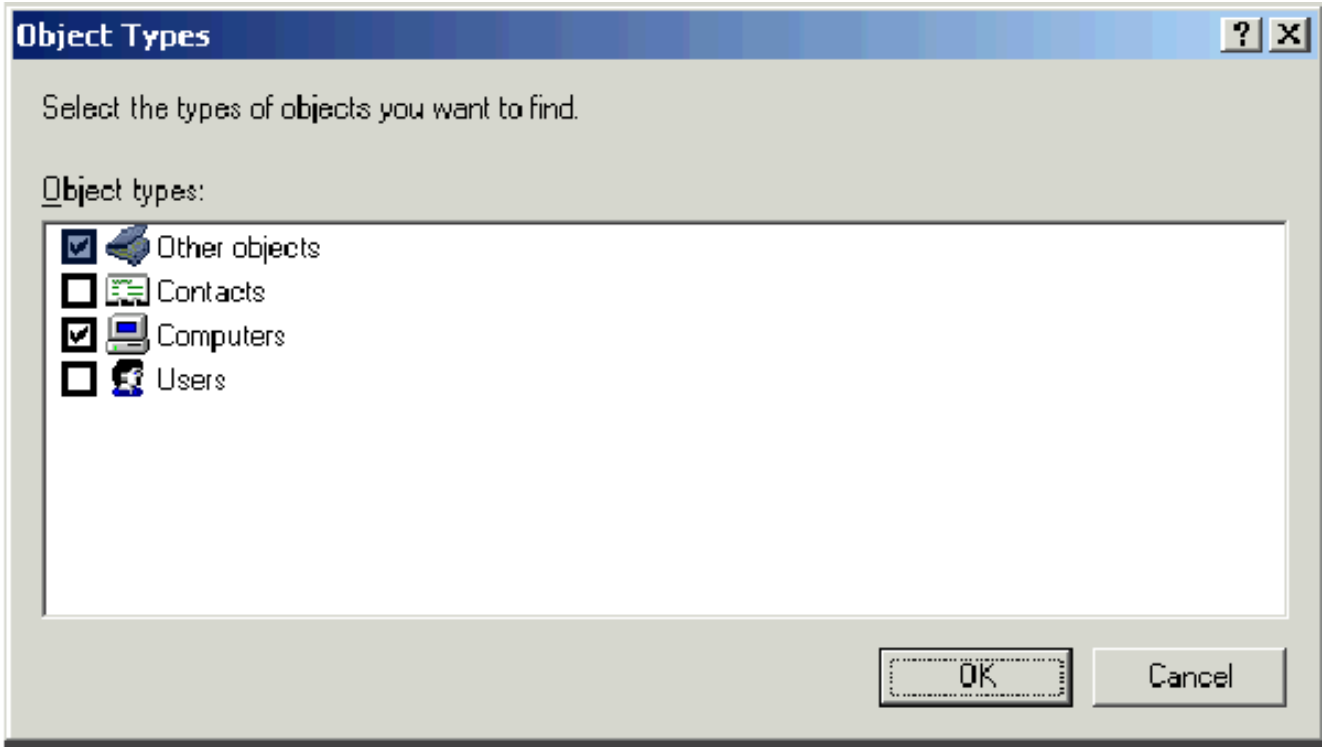
步骤 13：向 wirelessusers 组中添加客户端计算机

请完成以下步骤：

1. 重复本文档的向 WirelessUsers 组中添加用户部分中的步骤 1 和步骤 2。
2. 在“选择用户、联系人或计算机”对话框中，键入要添加到组中的计算机的名称。本示例显示如何将名为 **Client 的计算机添加到组中。**



3. 单击**对象类型**，清除“用户”复选框，然后选中“计算机”。



4. 单击**确定两次。**此时会将 CLIENT 计算机帐户添加到 wirelessusers 组中。
5. 重复此过程，向该组中添加更多计算机。

在 Windows Standard 2003 上设置 Cisco Secure ACS 4.0

Cisco Secure ACS 是一台运行 Windows Server 2003 Standard Edition SP1 的计算机，为控制器提供 RADIUS 身份验证和授权。要将 ACS 配置为 RADIUS 服务器，请完成本部分中的步骤：

基本安装和配置

请完成以下步骤：

1. 安装 Windows Server 2003 Standard Edition SP1，使其成为 wirelessdemo.local 域中名为 ACS 的成员服务器。**注意：**ACS服务器名称在其余配置中显示为cisco_w2003。请在余下的实验室设置中替换 ACS 或 cisco_w2003。
2. 对于本地连接，使用 IP 地址 **172.16.100.26**、子网掩码 255.255.255.0 和 DNS 服务器 IP 地址 127.0.0.1 来配置 TCP/IP 协议。

Cisco Secure ACS 4.0 安装

注意：有关如何配置Cisco Secure ACS 4.0 for Windows的详细信息，请参阅《Cisco Secure ACS 4.0 for Windows安装指南》。

请完成以下步骤：

1. 使用域管理员帐户来登录名为 ACS 的计算机，以便安装 Cisco Secure ACS。**注意：**仅支持在安装Cisco Secure ACS的计算机上执行的安装。使用 Windows 终端服务或虚拟网络计算 (VNC) 等产品进行远程安装的方式未经测试，也不受支持。
2. 在计算机的 CD-ROM 驱动器中插入 Cisco Secure ACS CD。
3. 如果 CD-ROM 驱动器支持 Windows 自动运行功能，就会显示“Cisco Secure ACS for Windows Server”对话框。**注：如**果计算机未安装所需的Service Pack，则会显示对话框。Windows Service Pack 可在安装 Cisco Secure ACS 之前或之后应用。您可以继续安装，但是必须在完成安装后应用所需的 Service Pack。否则，Cisco Secure ACS 可能不可靠。
4. 执行这些任务之一：如果显示了“Cisco Secure ACS for Windows Server”对话框，请单击 **Install**。如果未显示“Cisco Secure ACS for Windows Server”对话框，请运行 Cisco Secure ACS CD 根目录中的 **setup.exe**。
5. “Cisco Secure ACS Setup”对话框将显示软件许可协议。
6. 阅读软件许可协议。如果您接受软件许可协议，请单击 **Accept**。“Welcome”对话框显示有关安装程序的基本信息。
7. 当您读完“Welcome”对话框中的信息后，单击 **Next**。
8. “Before You Begin”对话框列出了您必须在继续安装之前要完成的任务。如果您已经完成了“Before You Begin”对话框中的所有任务，请选择每一项任务的相应对话框，然后单击 **Next**。**注意：如**果尚未完成“开始前”对话框中列出的所有项目，请单击“取消”**，然**后单击“退**出设置”**。**当您完成“Before You Begin”对话框中列出的所有任务之后，再重新启动安装。
9. 此时将显示“Choose Destination Location”对话框。“Destination Folder”下将显示安装位置。这是安装程序用来安装 Cisco Secure ACS 的驱动器和路径。
10. 如果您希望更改安装位置，请完成以下步骤：单击**浏览**。此时将显示“Choose Folder”对话框。“Path”框包含安装位置。更改安装位置。您可以在“Path”框中键入新位置，也可以使用“Drives”和“Directories”列表来选择新的驱动器和目录。安装位置必须在计算机的本地驱动器上。**注意：**不要指定包含百分比字符“%”的路径。 如果这么做，安装看起来能够正确进行，但是会在完成前失败。Click **OK**.**注：如**果指定的文件夹不存在，安装程序将显示一个对话框，以确认文件夹的创建。要继续安装，请单击 **Yes**。
11. 在“Choose Destination Location”对话框中，新的安装位置显示在“Destination Folder”下。
12. 单击 **Next**。
13. “Authentication Database Configuration”对话框列出了有关对用户进行身份验证的选项。您可以仅使用 Cisco Secure 用户数据库进行身份验证，也可以使用 Cisco Secure 用户数据库和 Windows 用户数据库进行身份验证。**注意：安**装Cisco Secure ACS后，除了Windows用户数据库外，您还可以为所有外部用户数据库类型配置身份验证支持。
14. 如果您希望仅使用 Cisco Secure 用户数据库对用户进行身份验证，请选中 **Check the Cisco Secure ACS database only 选项。**

15. 如果除了 Cisco Secure 用户数据库以外，您还希望使用 Windows 安全访问管理器 (SAM) 用户数据库或 Active Directory 用户数据库对用户进行身份验证，请完成以下步骤：选中 **Also check the Windows User Database 选项。Yes, refer to "Grant dialin permission to user" setting 复选框就变为可用。注意：**“是，请参阅“向用户授予拨入权限”设置复选框适用于 Cisco Secure ACS控制的所有访问形式，而不仅仅是拨入访问。例如，通过 VPN 隧道访问网络的用户无需拨号进入网络访问服务器。但是，如果选中了 **Yes, refer to "Grant dialin permission to user" setting 复选框，Cisco Secure ACS 也会应用 Windows 用户拨号权限，以便决定是否向该用户授予网络访问权限。**如果您希望仅当用户的 Windows 帐户具有拨号权限时，才允许通过 Windows 域用户数据库身份验证的用户获得访问权限，请选中 **Yes, refer to "Grant dialin permission to user" setting 复选框。**
16. 单击 **Next**。
17. 安装程序将安装 Cisco Secure ACS 并更新 Windows 注册表。
18. “Advance Options”对话框将列出在默认情况下处于禁用状态的 Cisco Secure ACS 功能。有关这些功能的更多信息，请参阅 Cisco Secure ACS for Windows Server 4.0 用户指南。**注意：仅**当您启用所列功能时，这些功能才会显示在Cisco Secure ACS HTML界面中。安装之后，您可以在“Advanced Options”页的“Interface Configuration”部分中启用或禁用它们。
19. 对于您要启用的每项功能，请选中相应的复选框。
20. 单击 **Next**。
21. 此时将显示“Active Service Monitoring”对话框。**注意：安**装后，可以在“系统配置”部分的“活动服务管理”页上配置活动服务监控功能。
22. 如果您希望 Cisco Secure ACS 监视用户身份验证服务，请选中 **Enable Login Monitoring 复选框。**从“Script to Execute”列表中，选择在出现身份验证服务故障时要应用的选项：**No Remedial Action—Cisco Secure ACS 不运行脚本。注意：如**果启用事件邮件通知，此选项非常有用。**Reboot—Cisco Secure ACS 运行一个脚本，以便重新引导运行了 Cisco Secure ACS 的计算机。Restart All—Cisco Secure ACS 重新启动所有 Cisco Secure ACS 服务。Restart RADIUS/TACACS+—Cisco Secure ACS 仅重新启动 RADIUS 和 TACACS+ 服务。**
23. 如果您希望 Cisco Secure ACS 在服务监视功能检测到事件时发送电子邮件消息，请选中 **Mail Notification 复选框。**
24. 单击 **Next**。
25. 此时将显示“Database Encryption Password”对话框。**注意：数**据库加密密码已加密并存储在ACS注册表中。在出现重大问题并且需要手动访问数据库时，您可能需要再次使用此密码。请保留此密码，以使技术支持能够访问数据库。密码在每个有效期内都可以更改。
26. 输入用于加密数据库的密码。密码至少要有 8 个字符长，并且需要同时包含字符和数字。不存在无效字符。
27. 单击 **Next**。
28. 安装程序就会完成安装，并显示“Cisco Secure ACS Service Initiation”对话框。
29. 对于您需要的每个“Cisco Secure ACS Services Initiation”选项，请选中相应的复选框。与选项相关的操作将在安装程序完成后执行。**Yes, I want to start the Cisco Secure ACS Service now—启动组成 Cisco Secure ACS 的 Windows 服务。**如果您不选中此选项，则除非您重新引导计算机或启动 CSAdmin 服务，否则就不能使用 Cisco Secure ACS HTML 界面。**Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation—在默认 Web 浏览器中为当前 Windows 用户帐户打开 Cisco Secure ACS HTML 界面。Yes, I want to view the Readme File—在 Windows 记事本中打开 README.TXT 文件。**
30. 单击 **Next**。
31. 如果您选择了某个选项，将启动 Cisco Secure ACS 服务。“Setup Complete”对话框显示有关 Cisco Secure ACS HTML 界面的信息。
32. 单击 **完成。注意：**其余配置记录在配置的EAP类型的一节下。

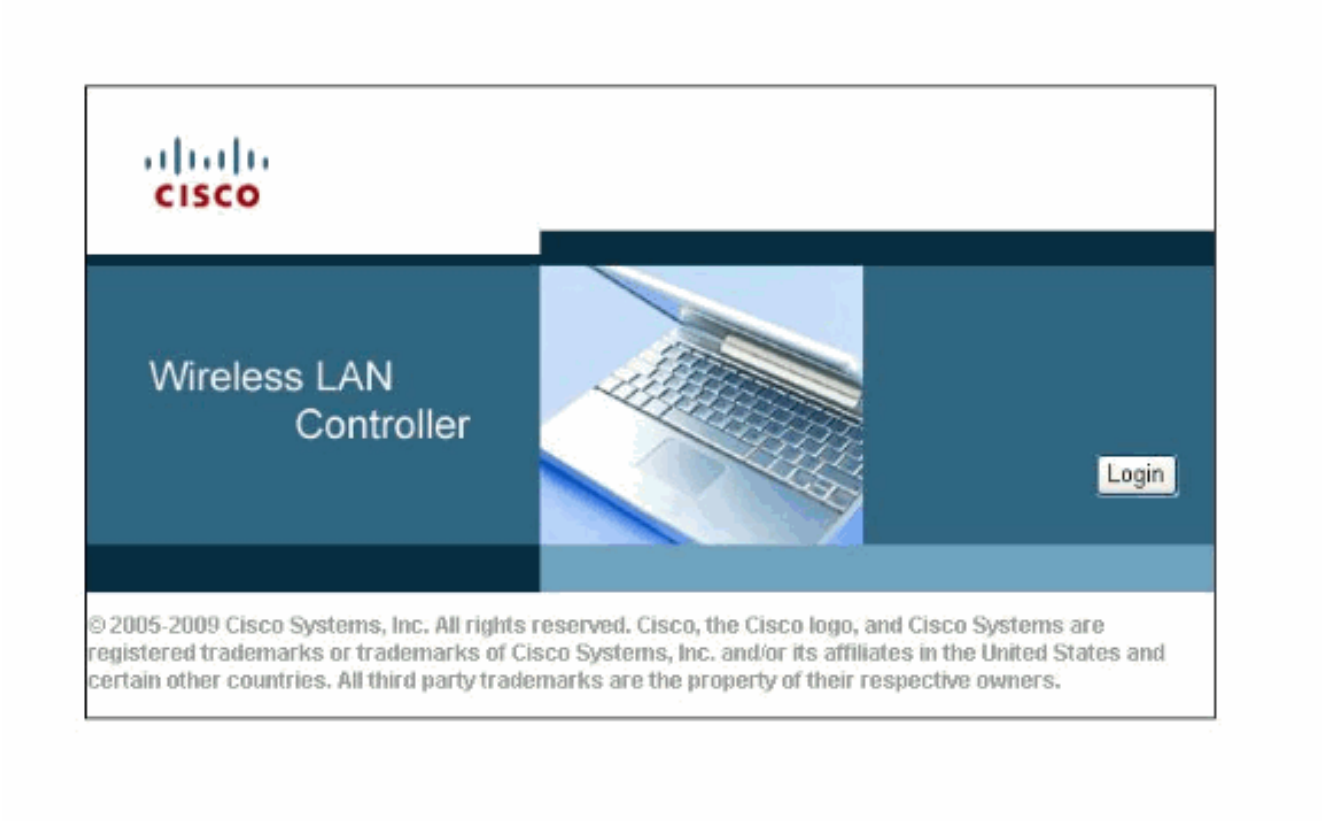
Cisco LWAPP 控制器配置

为 WPAv2/WPA 创建必要的配置

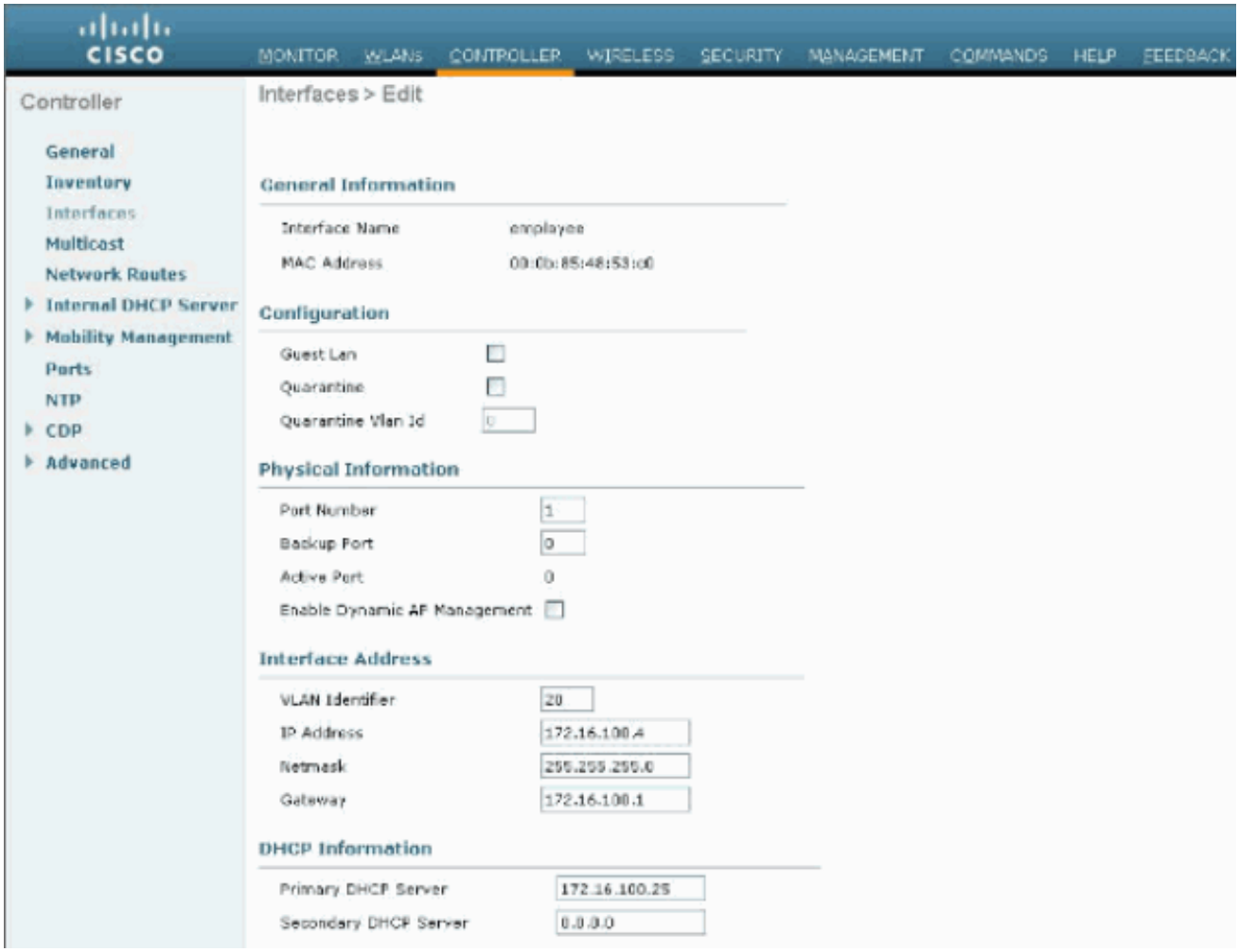
请完成以下步骤：

注意：假设控制器具有基本的网络连接，并且管理接口的IP可达性成功。

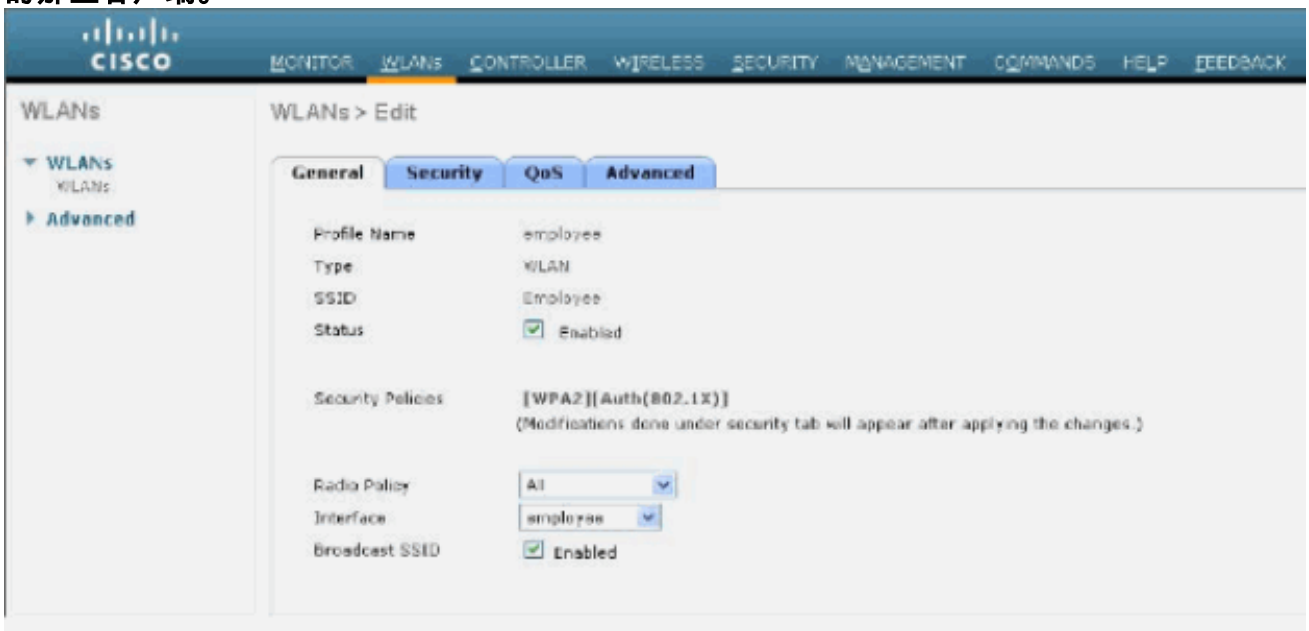
1. 浏览到 **https://172.16.101.252，以便登录控制器。**



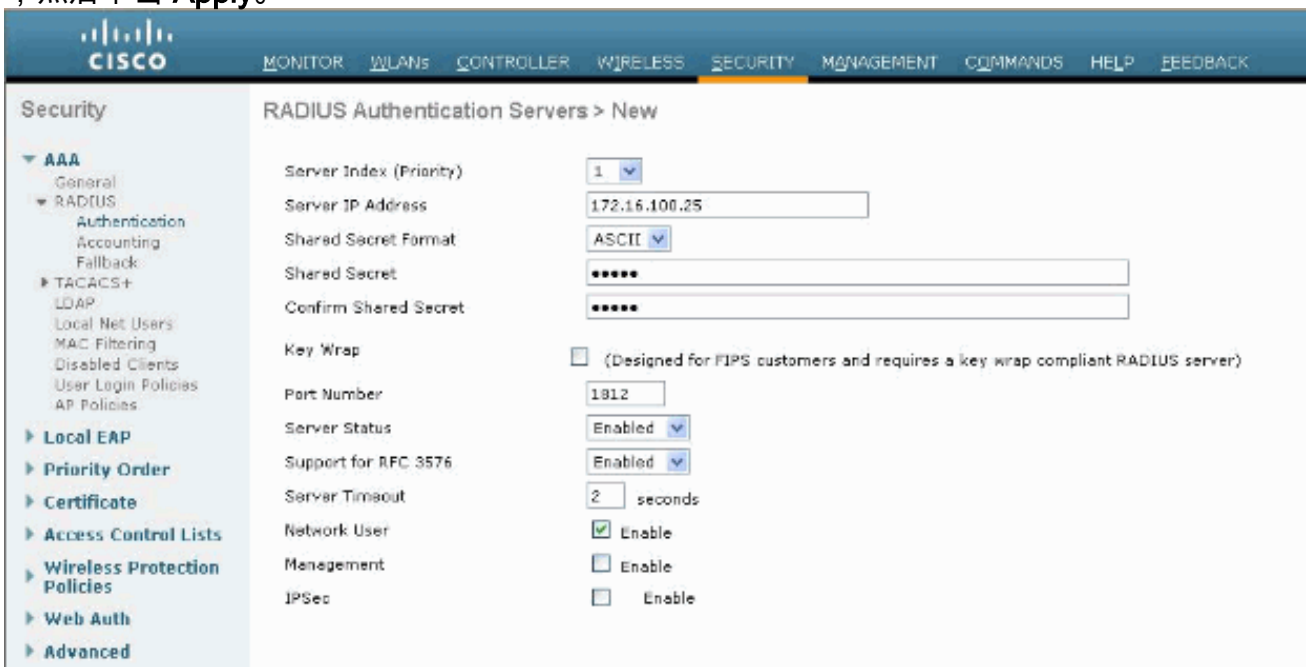
2. 单击 **Login**
3. 用默认用户 **admin 和默认密码 admin 进行登录。**
4. 在 **Controller 菜单下为 VLAN 映射创建新接口。**
5. 单击 **Interfaces**。
6. 单击 **New**。
7. 在“Interface name”字段中，键入 **Employee**。（此字段可以是您喜欢的任何值。）
8. 在VLAN ID字段中键入**20**。（此字段可以是网络中传输的任何VLAN。）
9. 单击 **Apply**。
10. 在显示“Interfaces > Edit”窗口时，配置相关信息。



11. 单击 **Apply**。
12. 单击 **WLANs 选项卡。**
13. 选择 **Create New，然后单击“Go”。**
14. 输入配置文件名称，然后在“WLAN SSID”字段中，键入 **Employee**。
15. 为 WLAN 选择 ID，然后单击 **Apply**。
16. 在显示“WLANs > Edit”窗口时，为此 WLAN 配置信息。**注意**：WPAv2是本实验选择的第2层加密方法。要允许具有 TKIP-MIC 的 WPA 客户端关联到此 SSID，您还可以选中 **WPA compatibility mode 和“Allow WPA2 TKIP Clients”复选框，或者不支持 802.11i AES 加密方法的那些客户端。**



17. 在“WLANs > Edit”屏幕上，单击 **General 选项卡。**
18. 确保选中 **Enabled 状态框，并且选择了适当的接口 (employee)。**并且，确保选中“Broadcast SSID”的“Enabled”复选框。
19. 单击“Security”选项卡。
20. 在 **Layer 2 子菜单下，选择 WPA + WPA2 作为第 2 层安全性。**对于 WPA2 加密方法，选中 **AES + TKIP，以便允许 TKIP 客户端。**
21. 选择 **802.1x 作为身份验证方法。**
22. 跳过“Layer 3”子菜单，因为不需要。配置 RADIUS 服务器之后，可以从“Authentication”菜单中选择适当的服务器。
23. 除非需要任何特殊的配置，否则可以使 **QoS 和“Advanced”选项卡保留默认设置。**
24. 单击 **Security 菜单，以便添加 RADIUS 服务器。**
25. 在 **RADIUS 子菜单下，单击“Authentication”。**然后单击 **New**。
26. 添加 RADIUS 服务器 IP 地址 (172.16.100.25)，该服务器是前面配置的 ACS 服务器。
27. 确保共享密钥与 ACS 服务器中配置的 AAA 客户端相匹配。确保选中“Network User”复选项，然后单击 **Apply**。



28. 基本配置到此已经全部完成，您可以开始测试 PEAP。

PEAP 身份验证

具有 MS-CHAP 2 的 PEAP 要求在 ACS 服务器上有证书，而不要求无线客户端上有证书。可以为 ACS 服务器自动注册计算机证书，从而简化部署过程。

要配置 DC_CA 以便自动注册计算机和用户证书，请完成本部分中的步骤。

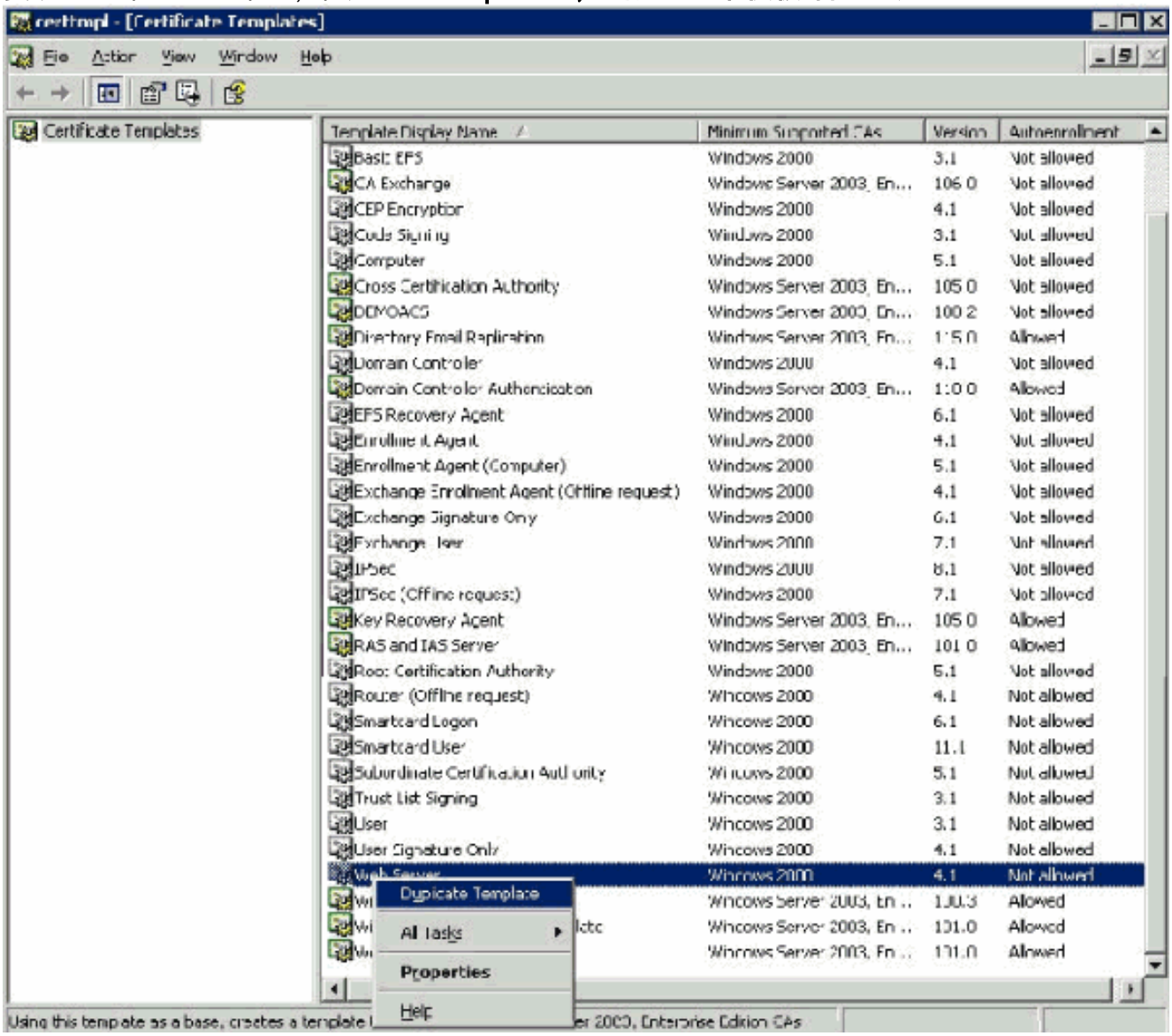
注意：Microsoft已通过Windows 2003企业CA版本更改了Web Server模板，因此密钥不再可导出，并且选项灰显。证书服务没有为服务器身份验证提供其他证书模板，但是可以在下拉菜单中将密钥标记为可导出，从而使您能够为服务器身份验证创建新模板。

注意：Windows 2000允许导出密钥，如果使用Windows 2000，则无需遵循这些步骤。

安装证书模板管理单元

请完成以下步骤：

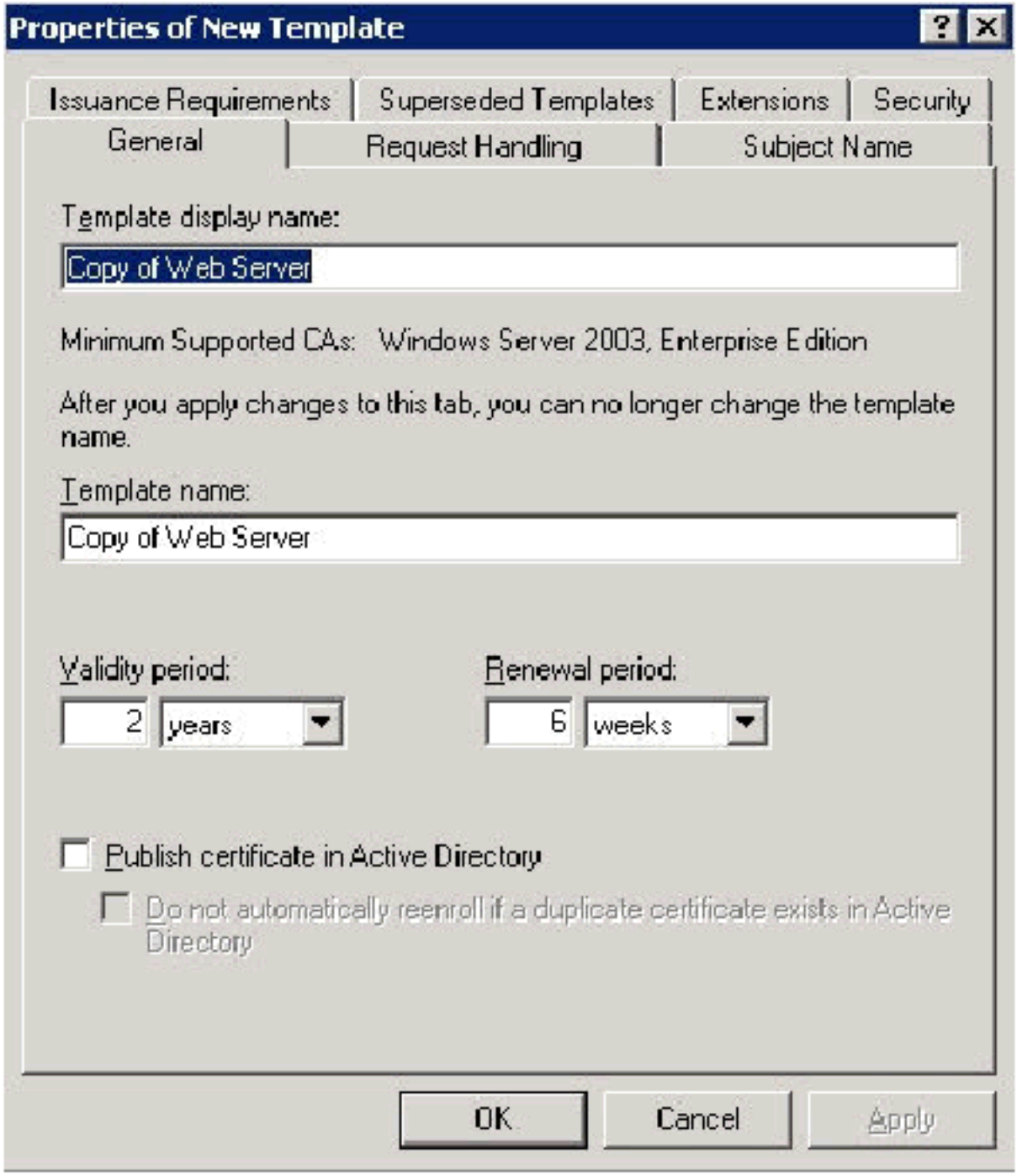
1. 选择**“开始”>“运行”**，键入 mmc，然后单击“确定”。
2. 在“文件”菜单上，单击**添加/删除管理单元，然后单击“添加”。**
3. 在“管理单元”下，双击**证书模板**，单击“关闭”，然后单击“确定”。
4. 在控制台树中，单击**证书模板**。所有证书模板都将显示在“详细信息”窗格中。
5. 要跳过步骤 2 到步骤 4，请键入 **certtmpl.msc，以打开“证书模板”管理单元。**



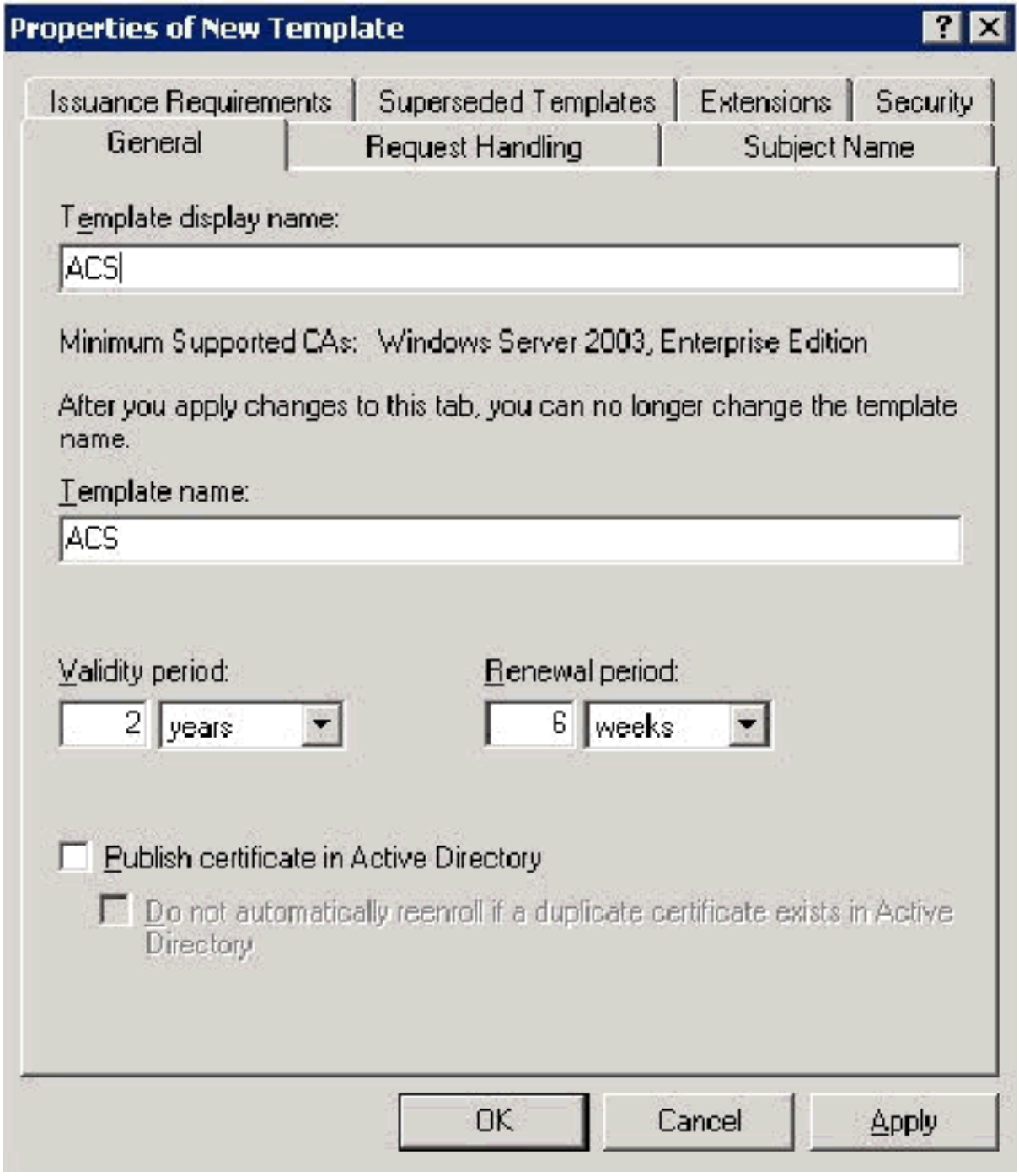
为 ACS Web Server 创建证书模板

请完成以下步骤：

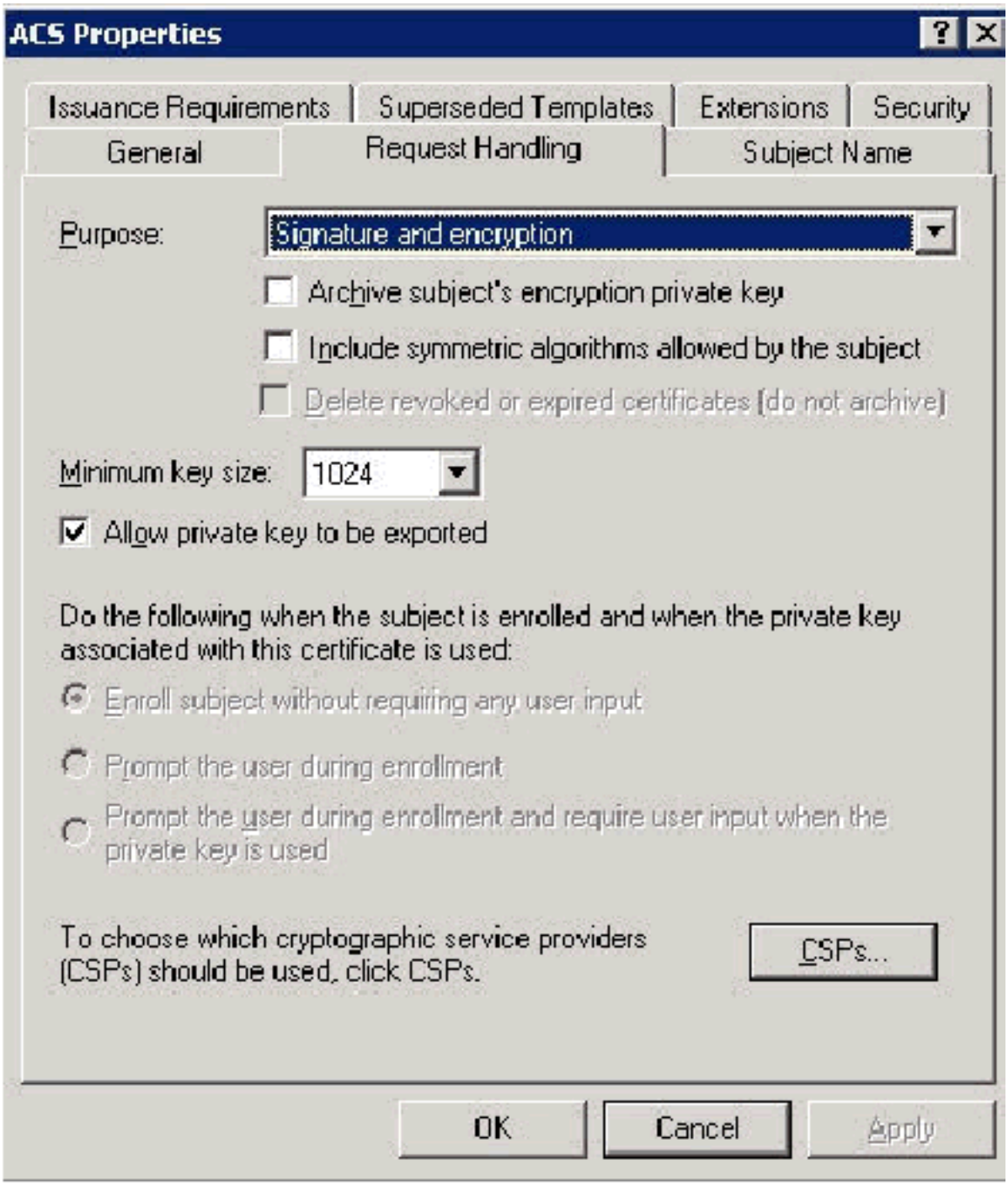
1. 在“证书模板”管理单元的“详细信息”窗格中，单击 **Web Server 模板。**
2. 在“操作”菜单上，单击**复制模板。**



3. 在“模板显示名称”字段中，键入 **ACS**。

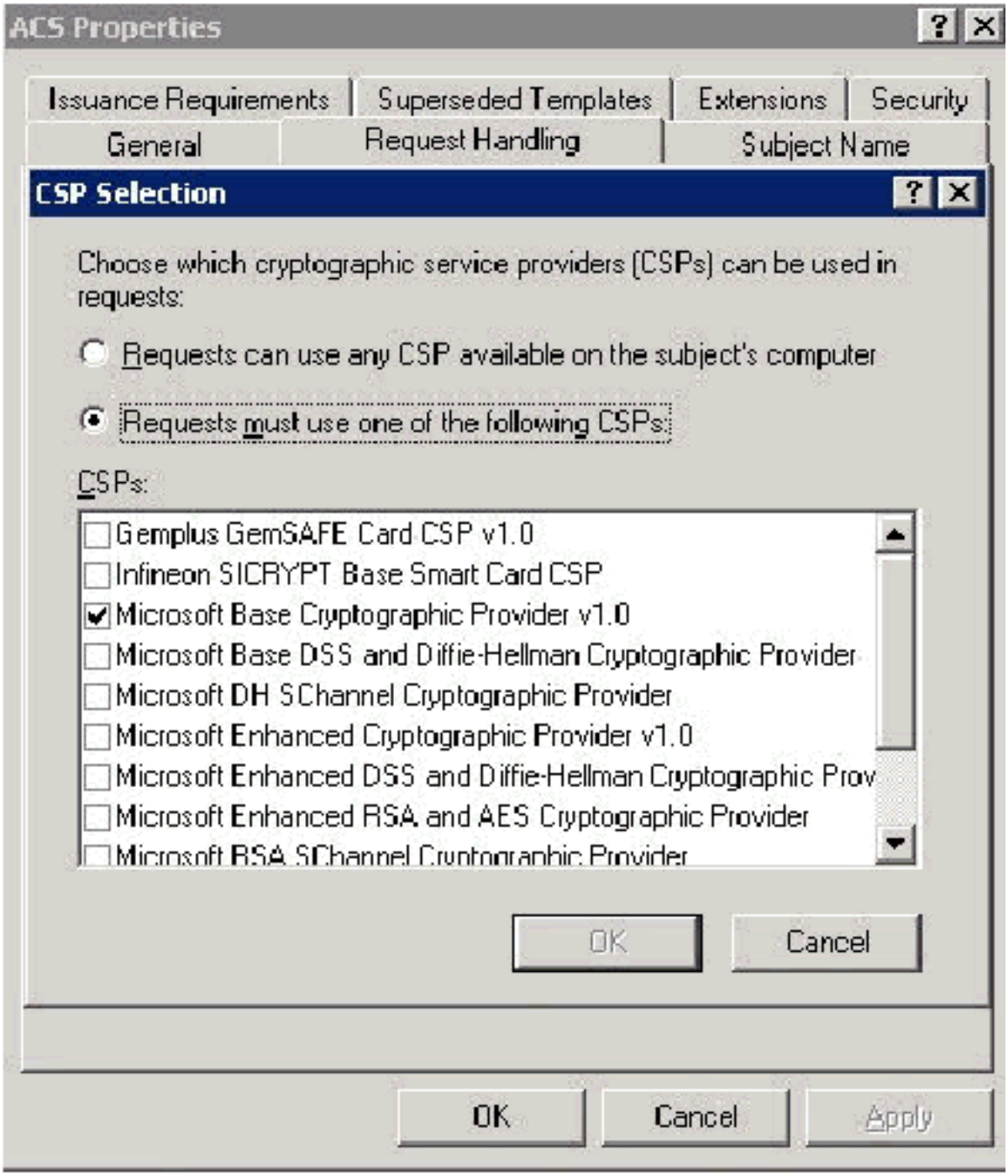


4. 转到“请求处理”选项卡，并选中**允许导出私钥**。并且，确保从“用途”下拉菜单中选择了**签名和**



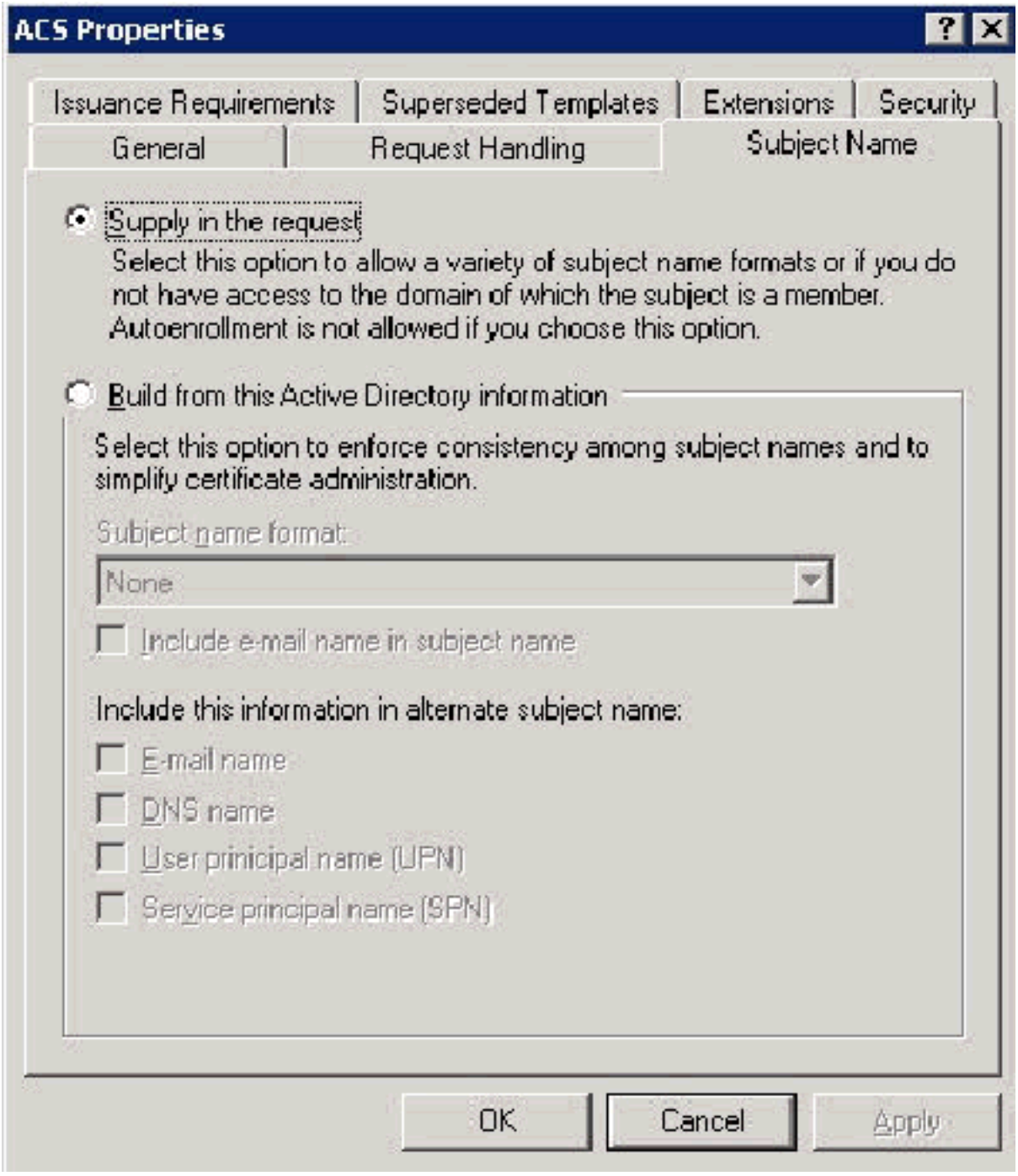
加密。

5. 选择**Requests must use of the following CSPs（请求必须使用以下CSP之一）**并选中**Microsoft Base Cryptographic Provider v1.0**。取消选中已选中的任何其他CSP，然后单击

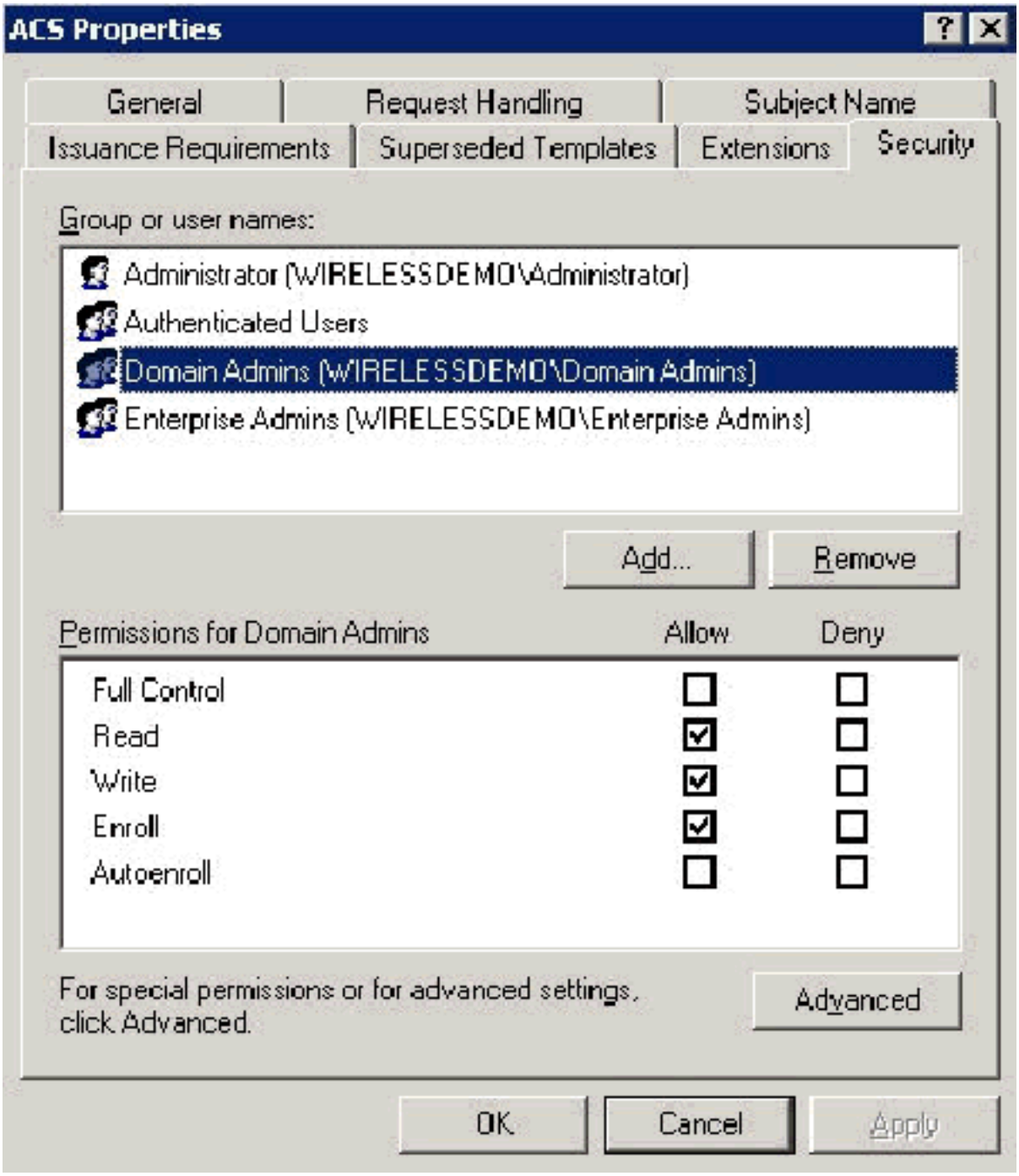


OK。

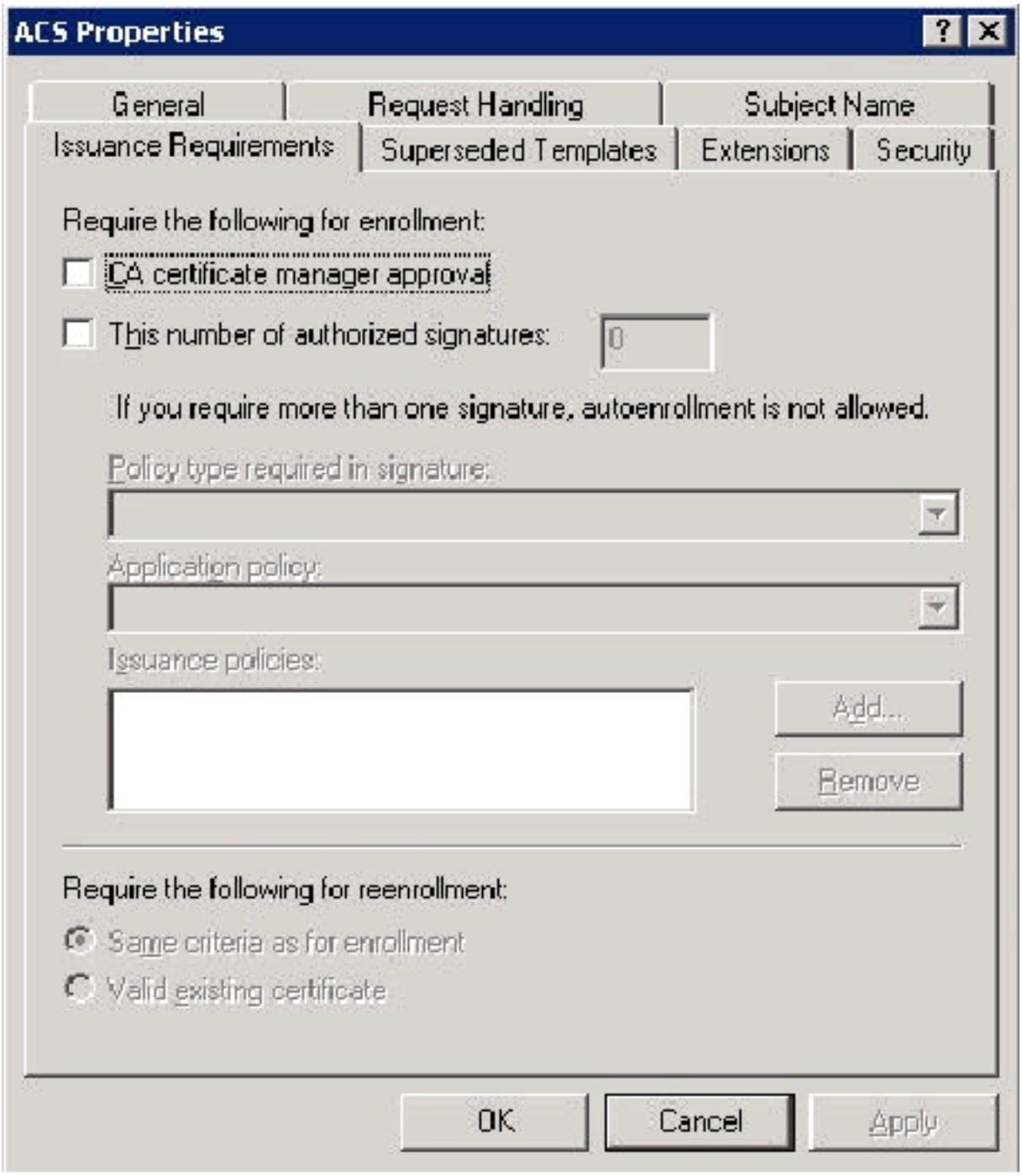
6. 转至“使用者名称”选项卡，选择**在请求中提供，然后单击“确定”。**



7. 转至“安全性”选项卡，突出显示**域管理员组，并确保在“允许”下选中“注册”选项。重要信息：**如果您选择从此 Active Directory 信息开始构建，只需选中**用户主体名称 (UPN) ，并且取消选中“在主题名称中包含电子邮件名称”和“电子邮件名称”，因为在“Active Directory 用户和计算机”管理单元中没有为无线用户输入电子邮件名称。**如果您不禁用这两个选项，自动注册功能将尝试使用电子邮件，从而导致自动注册错误。



8. 如果需要，还有一些附加的安全措施，可防止证书被自动推出。这些措施可以在“颁发要求”选项卡下找到。此内容在本文档中不做进一步讨论。

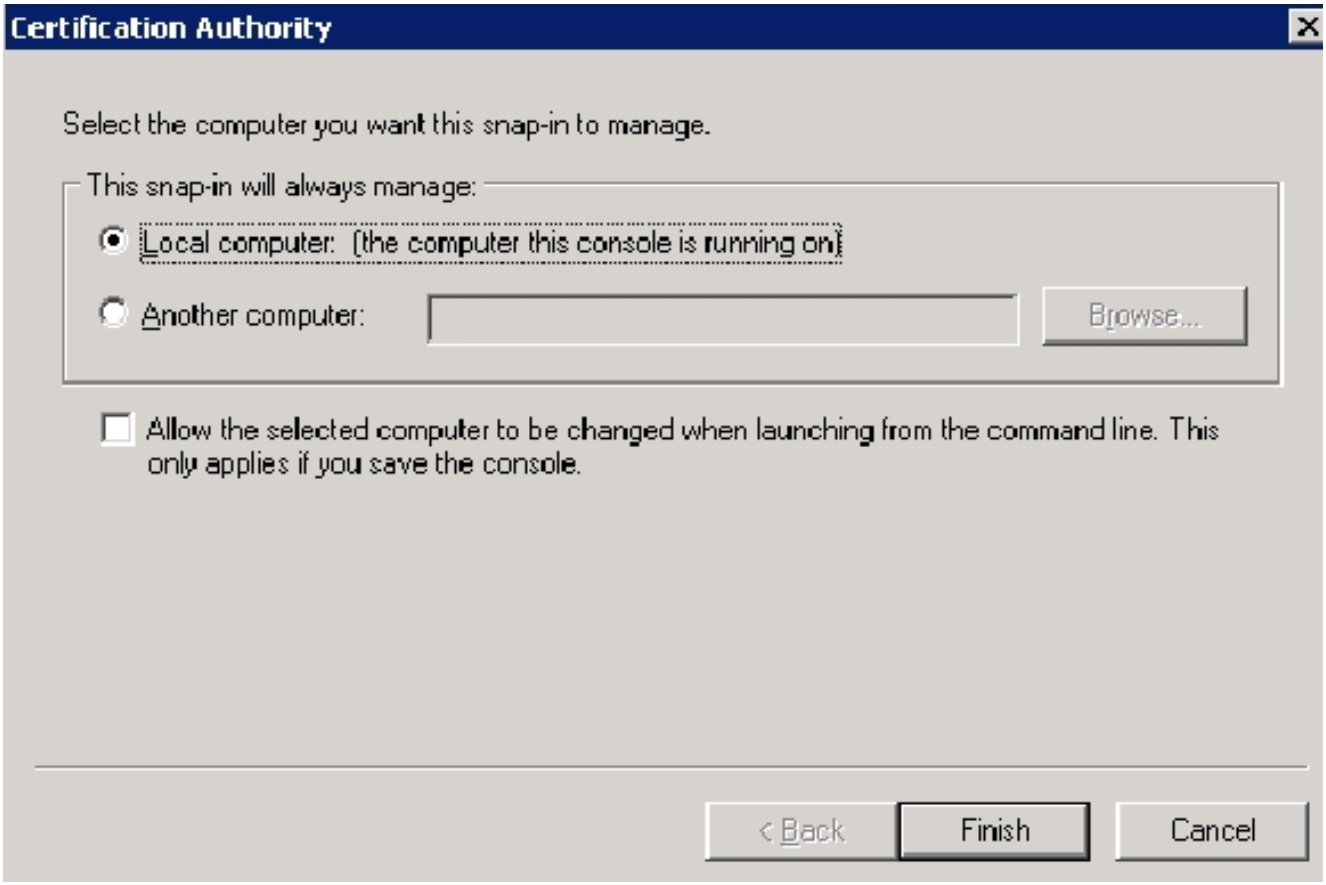


9. 单击**确定，以便保存模板，并从“证书颁发机构”管理单元发布此模板。**

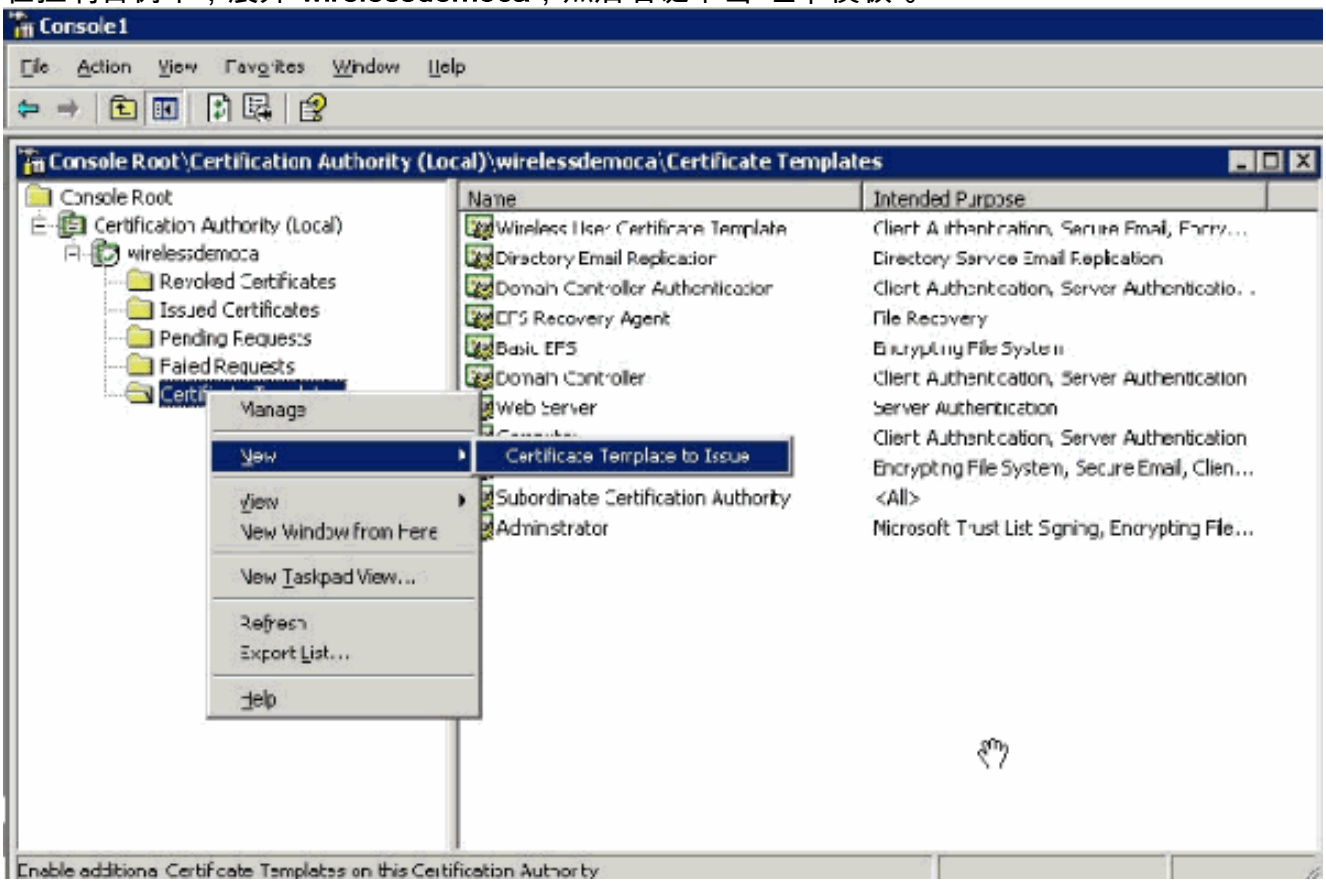
启用新的 ACS Web Server 证书模板

请完成以下步骤：

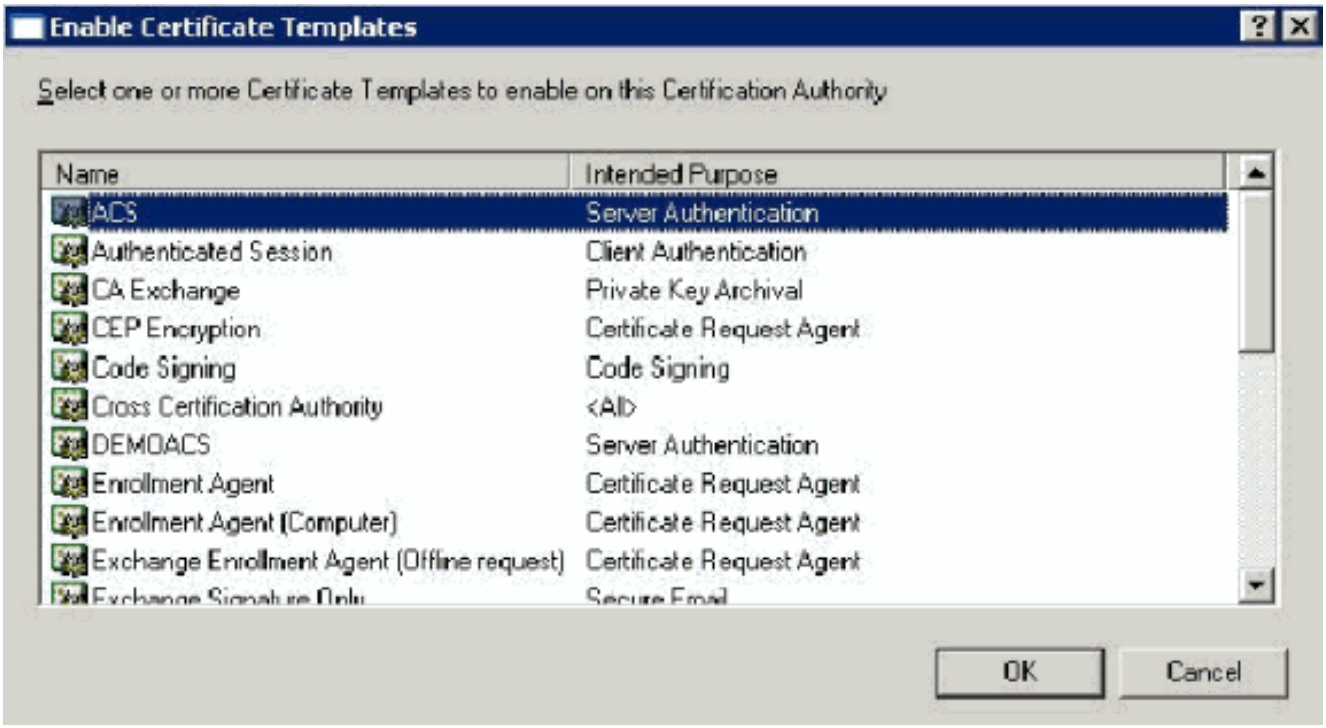
1. 打开“证书颁发机构”管理单元。按照为 ACS Web Server 创建证书模板部分中的步骤 1 到步骤 3，选择**证书颁发机构选项，选择“本地计算机”，然后单击“完成”。**



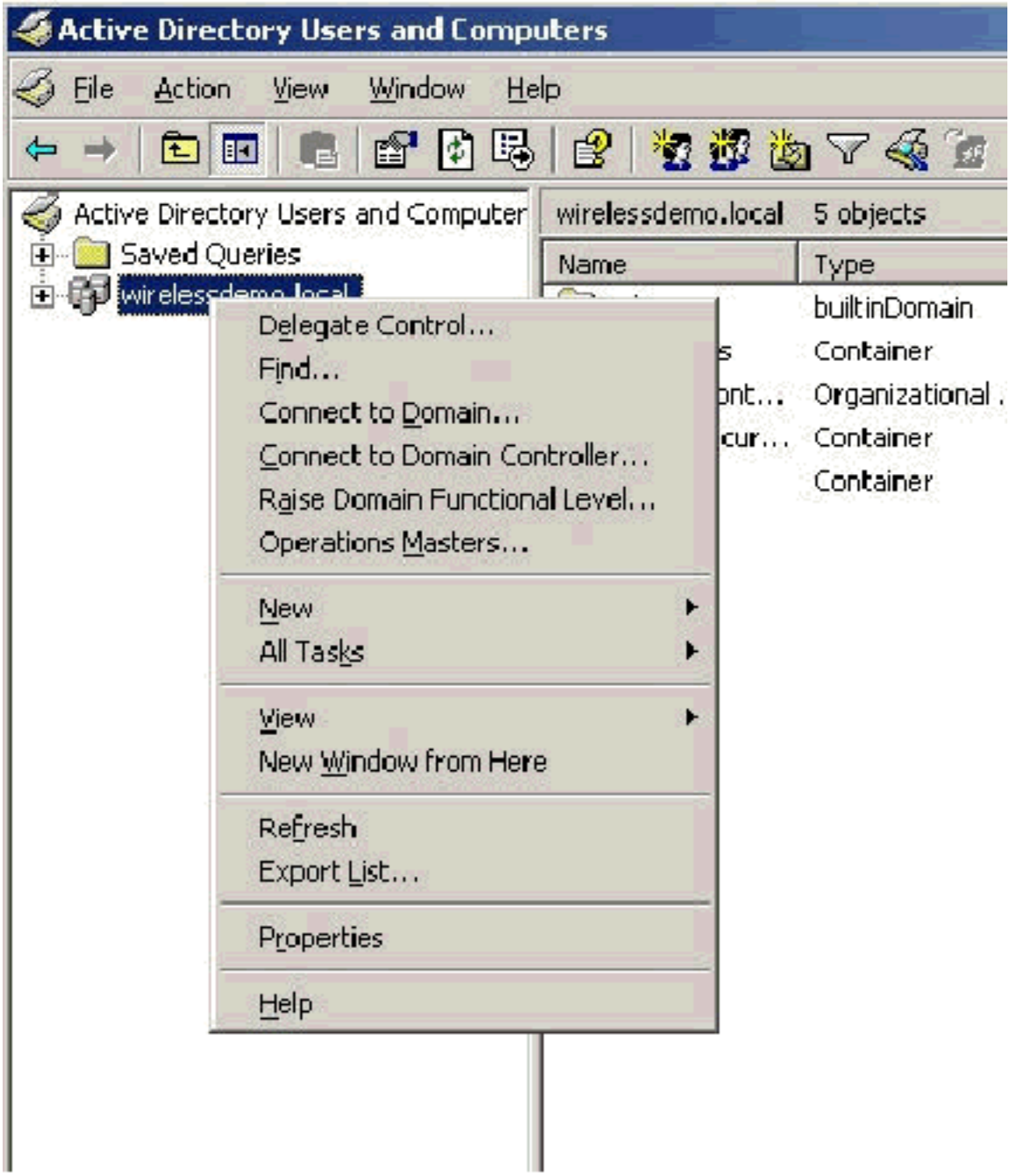
2. 在控制台树中，展开 **wirelessdemoca**，然后右键单击“证书模板”。



3. 选择**新>发行的认证模板**。
4. 单击 **ACS 证书模板**。

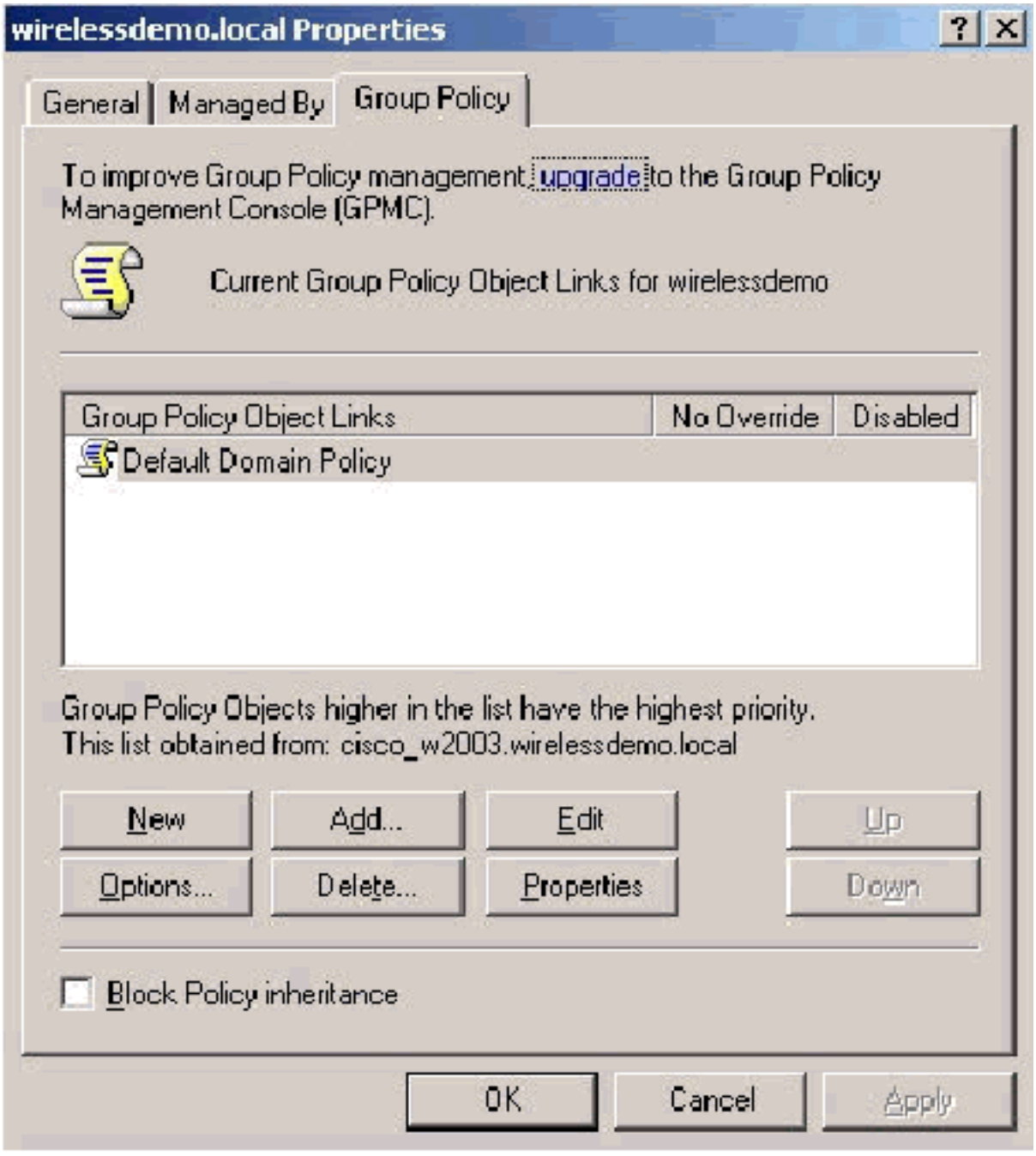


5. 单击**确定，然后打开“Active Directory 用户和计算机”管理单元。**
6. 在控制台树中，双击 **Active Directory 用户和计算机**，右键单击“wirelessdemo.local”，然后单



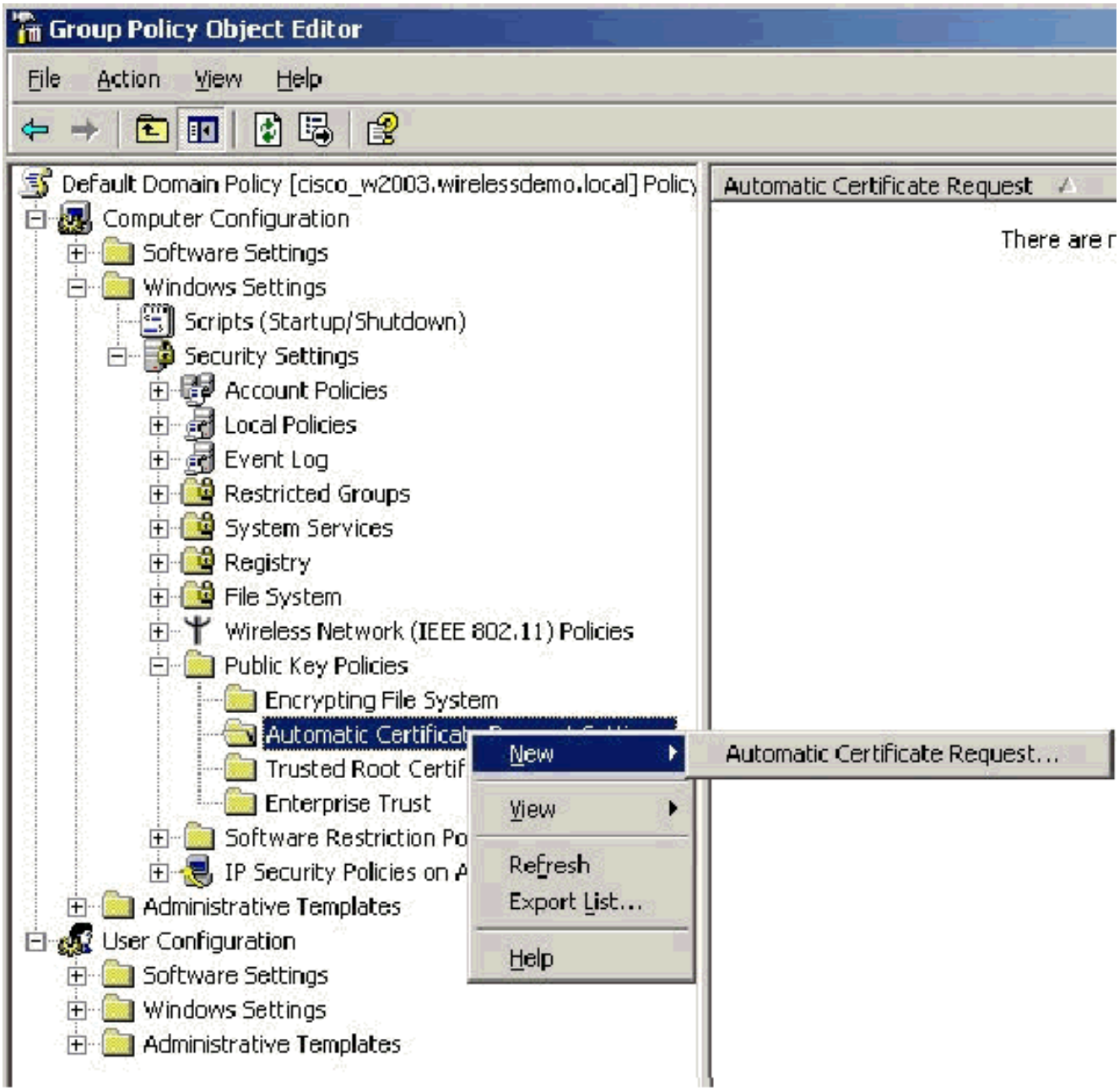
击“属性”。

7. 在“组策略”选项卡上，单击**默认域策略**，然后单击“编辑”。这将打开“组策略对象编辑器”管理单

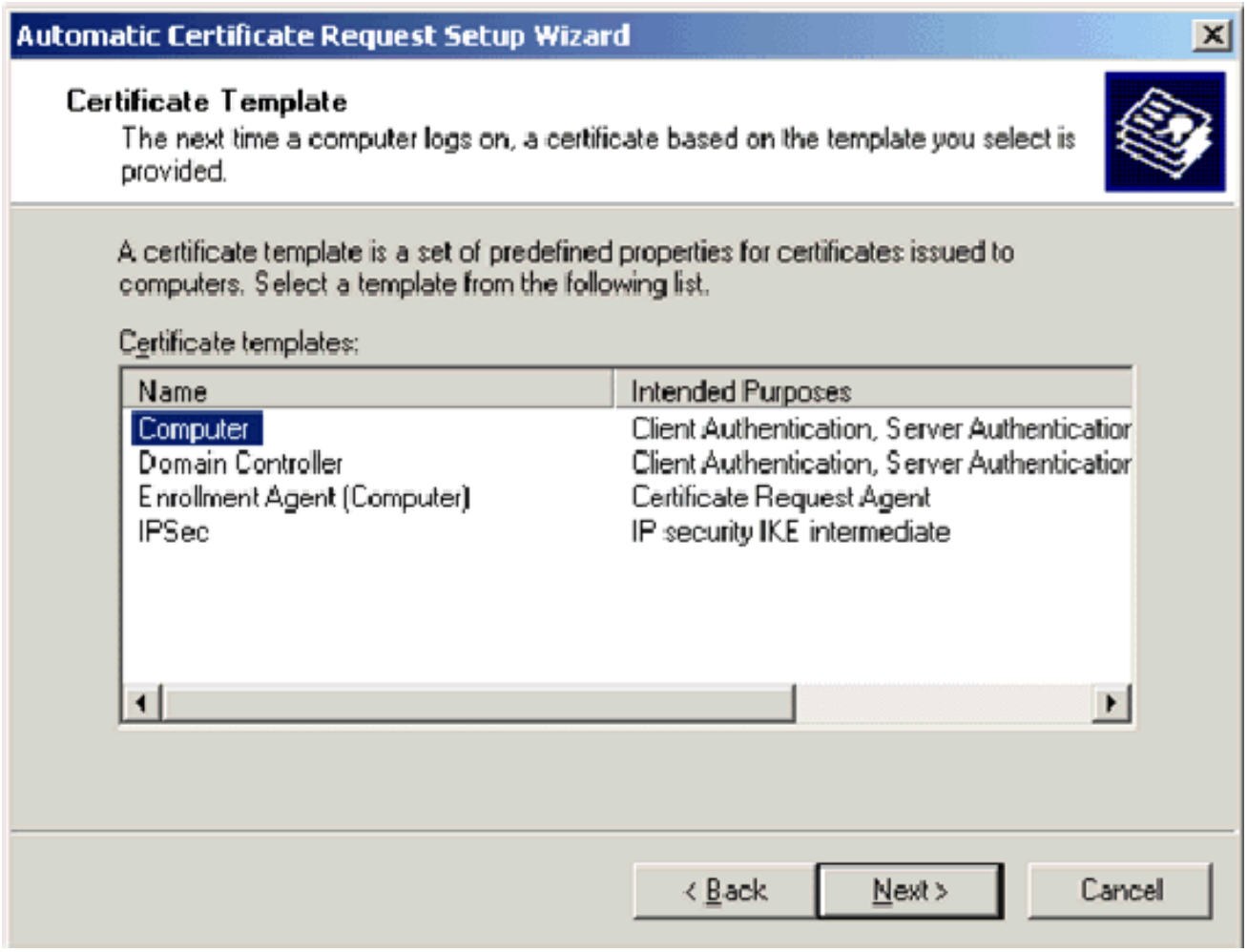


元。

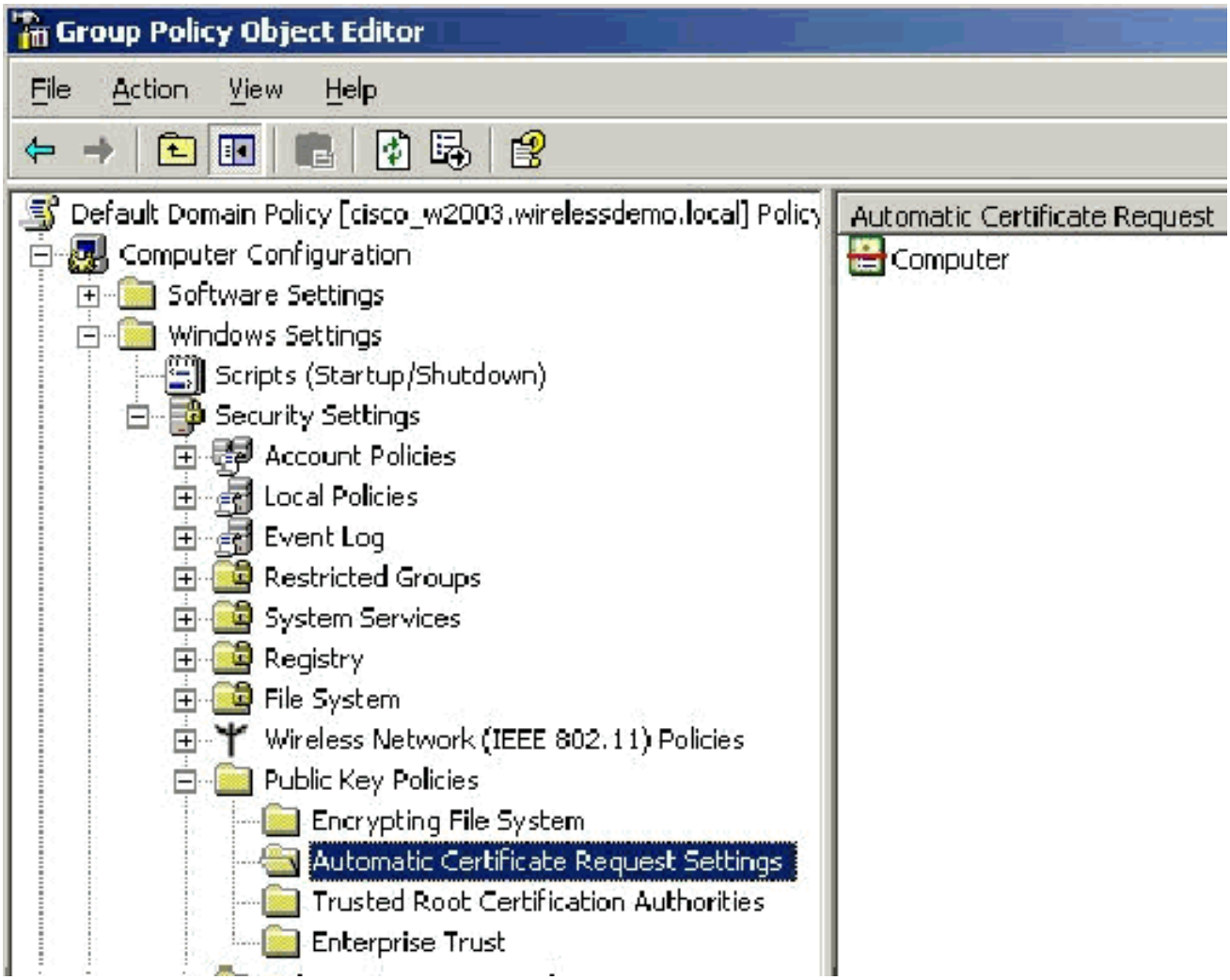
8. 在控制台树中，展开**计算机配置 > Windows 设置 > 安全设置 > 公钥策略**，然后选择“自动证书申请设置”。



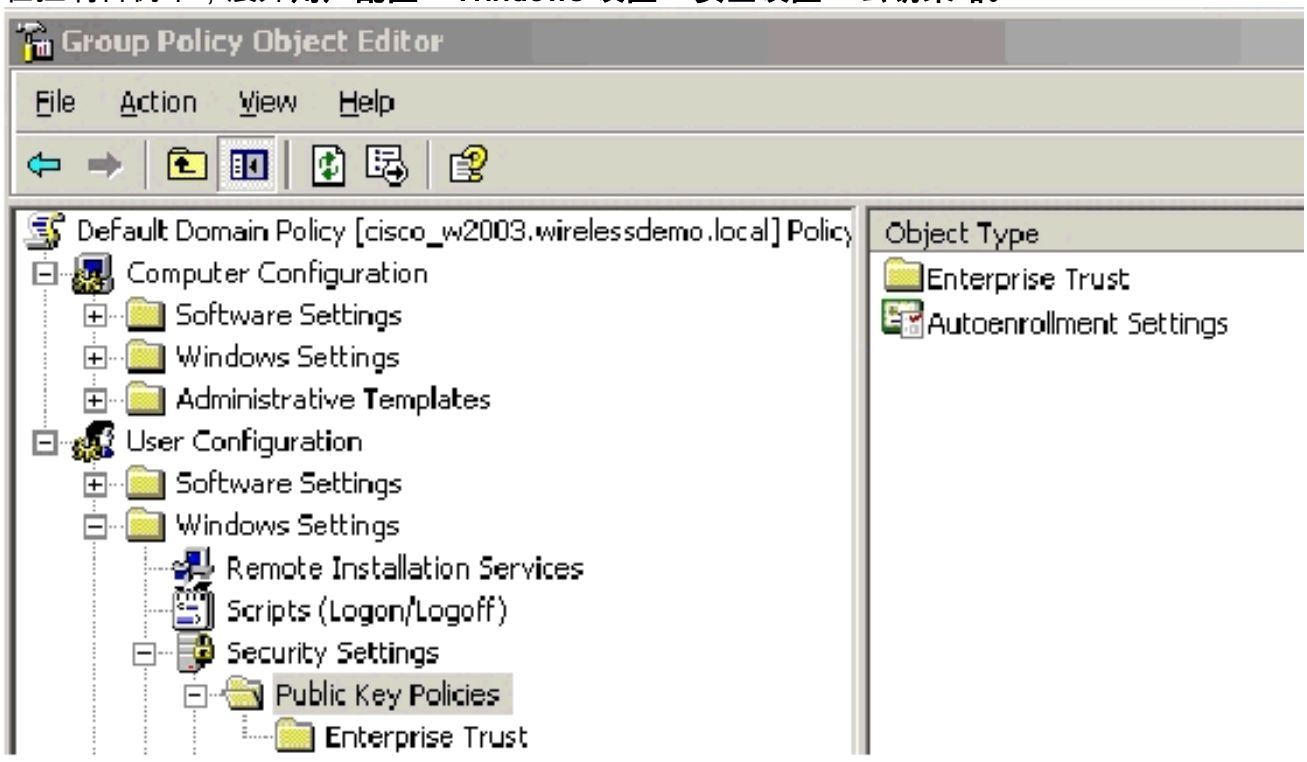
9. 右键单击**自动证书申请设置，然后选择"新建">"自动证书申请"。**
10. 在"欢迎使用自动证书申请设置向导"页上，单击**下一步。**
11. 在"证书模板"页上，单击**计算机，然后单击"下一步"。**



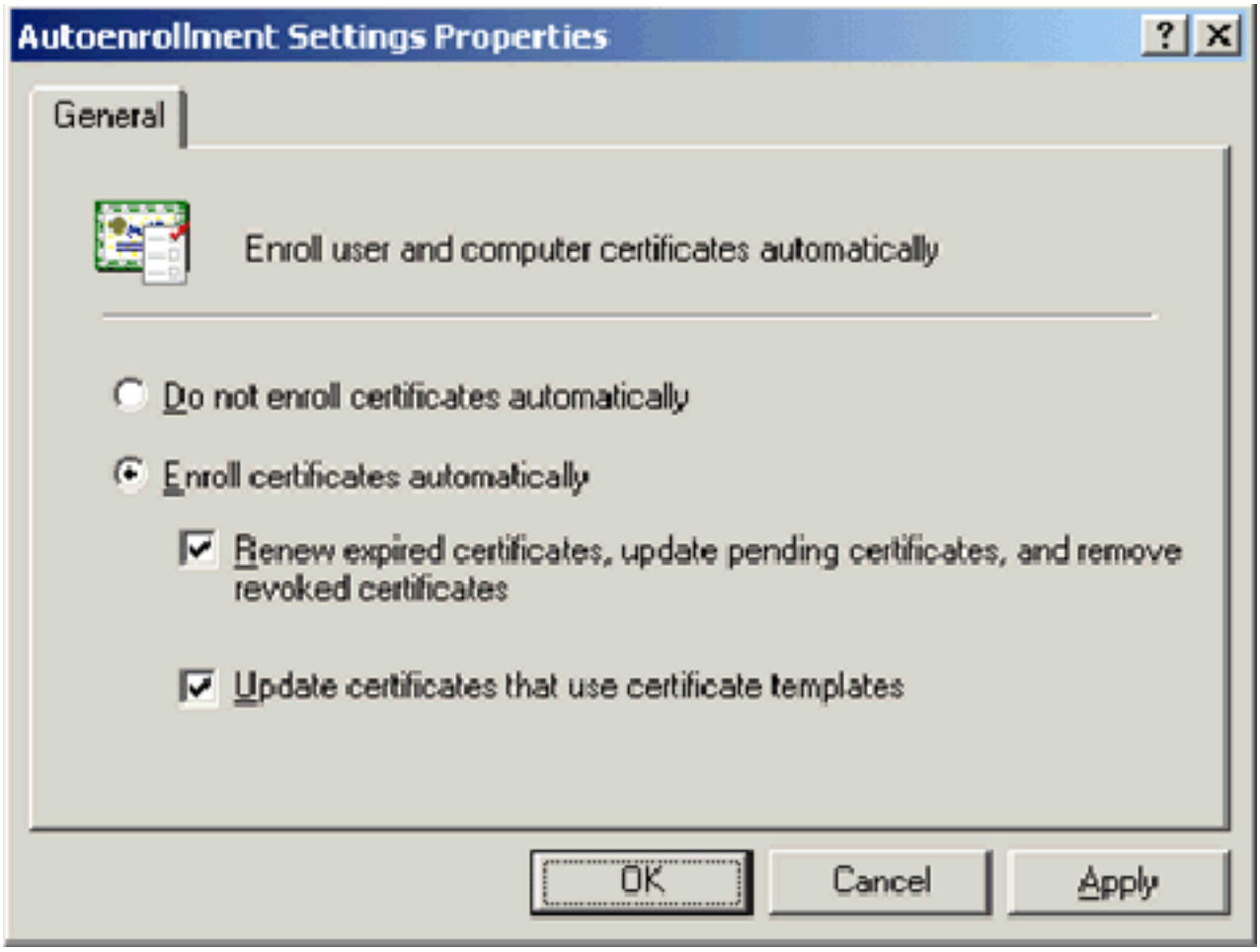
12. 当您完成“自动证书申请设置向导”页时，单击**完成**。“计算机”证书类型现在就会显示在“组策略对象编辑器”管理单元的详细信息窗格中。



13. 在控制台树中，展开**用户配置 > Windows 设置 > 安全设置 > 公钥策略。**



14. 在详细信息窗格中，双击**自动注册设置。**
15. 选择**自动注册证书，然后选中“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”。**



16. Click **OK**.

ACS 4.0 证书设置

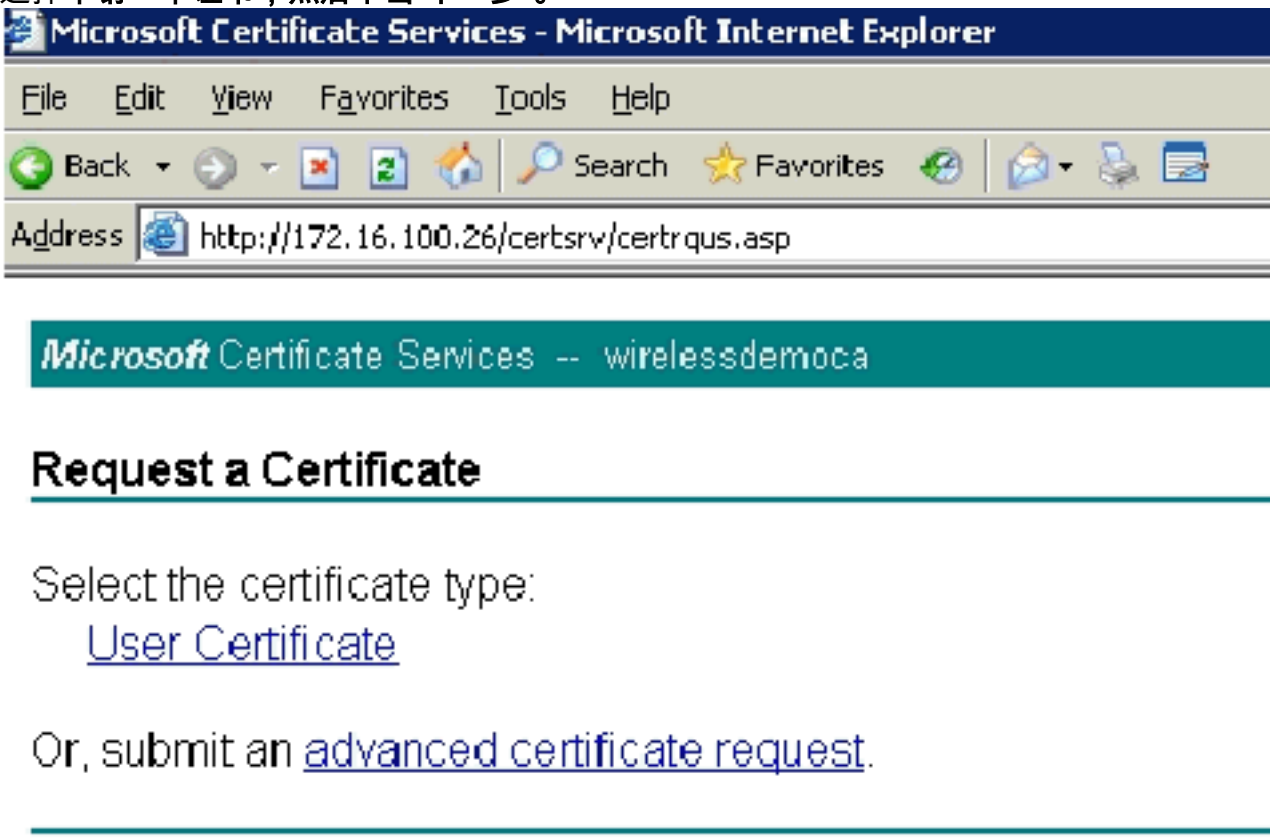
为 ACS 配置可导出的证书

重要信息：ACS 服务器必须从企业根 CA 服务器获取服务器证书，才能对 WLAN PEAP 客户端进行身份验证。

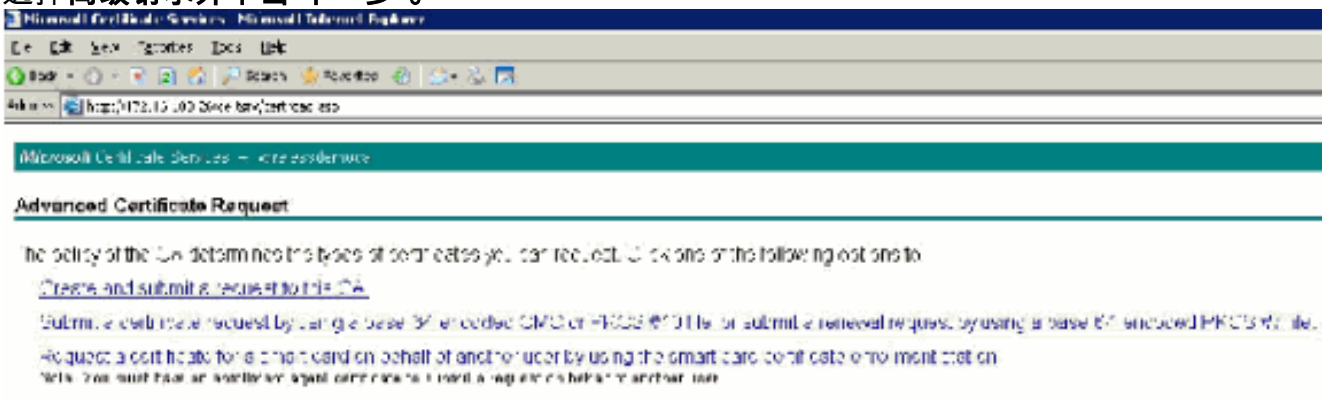
重要信息：请勿在证书设置过程中打开 IIS 管理器，因为缓存的信息会导致问题。

1. 用具有“Enterprise Admin”权限的帐户登录 ACS 服务器。
2. 在本地 ACS 计算机上，使 Microsoft 证书颁发机构服务器上的浏览器指向 **http://IP-address-of-Root-CA/certsrv**。在本示例中，IP 地址是 **172.16.100.26**。
3. 以 **Administrator** 的身份登录。

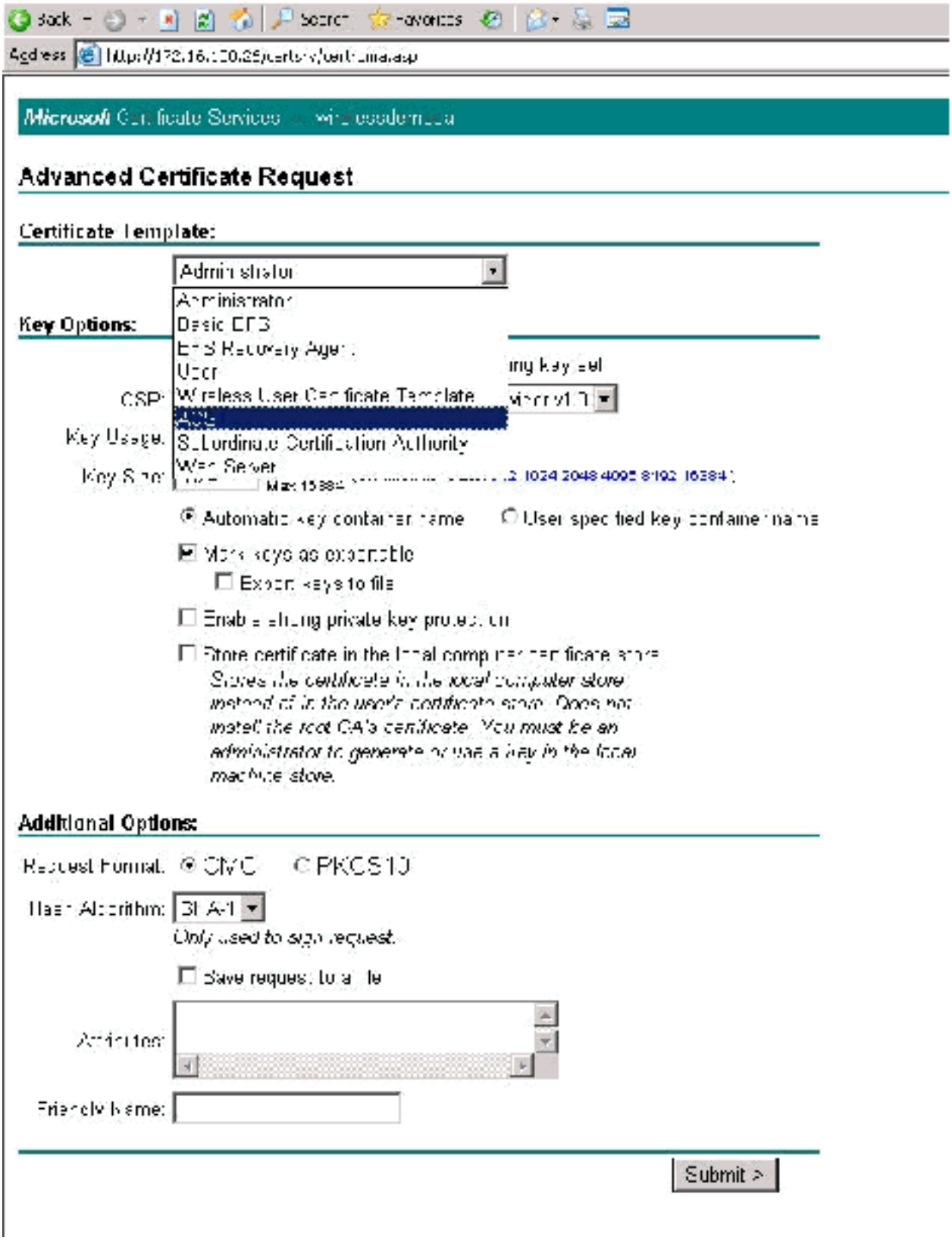
4. 选择**申请一个证书，然后单击"下一步"。**



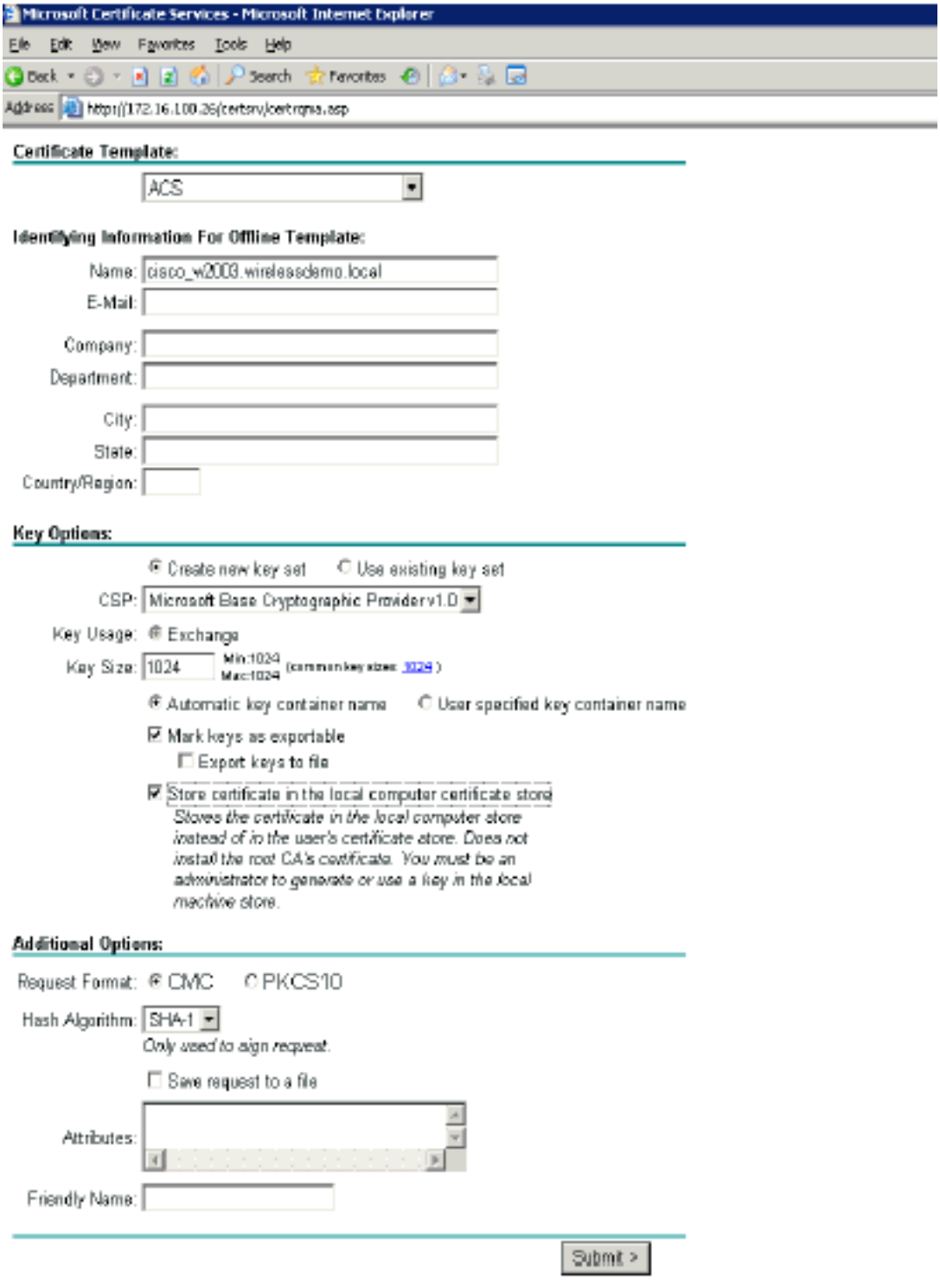
5. 选择**高级请求并单击"下一步"。**



6. 选择**创建并向此 CA 提交一个申请，然后单击"下一步"。重要信息：**此步骤的原因是 Windows 2003 不允许使用可导出的密钥，您必须基于前面创建的 ACS 证书来生成证书请求。

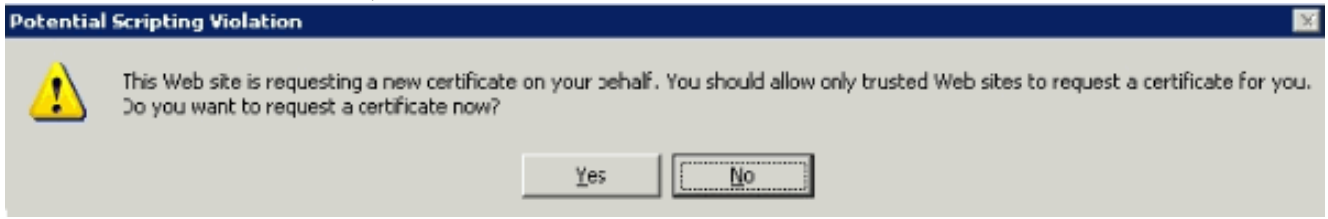


7. 从“证书模板”中，选择以前创建的名为 **ACS** 的证书模板。选择模板之后，所显示的选项会随之变化。
8. 将**名称配置为 ACS 服务器的完全限定的域名。**在本示例中，ACS 服务器的名称为 cisco_w2003.wirelessdemo.local。确保选中**将证书保存在本地计算机存储中，然后单击“提交**

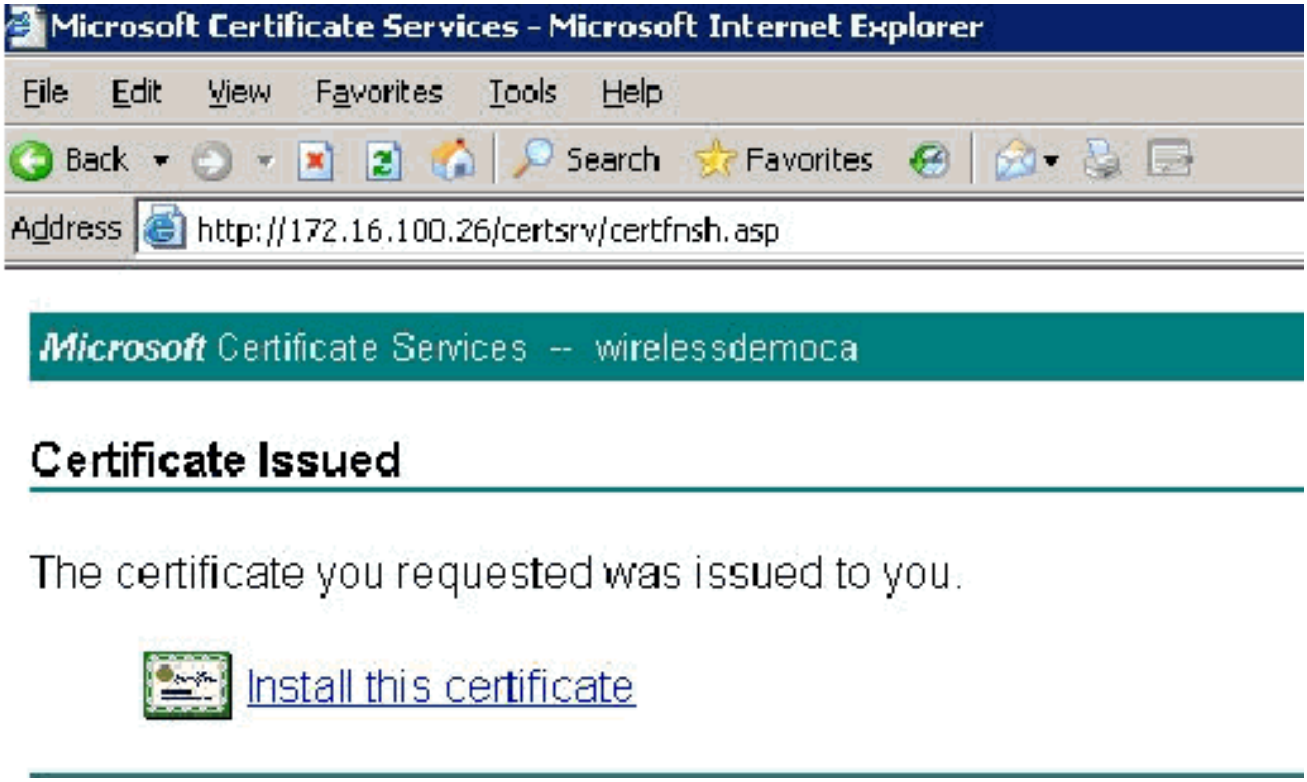


”。

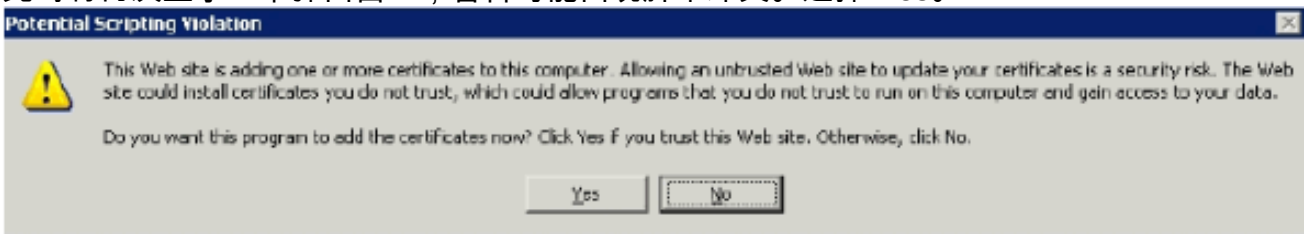
9. 此时将显示一个弹出窗口，警告可能出现脚本冲突。选择 **Yes**。



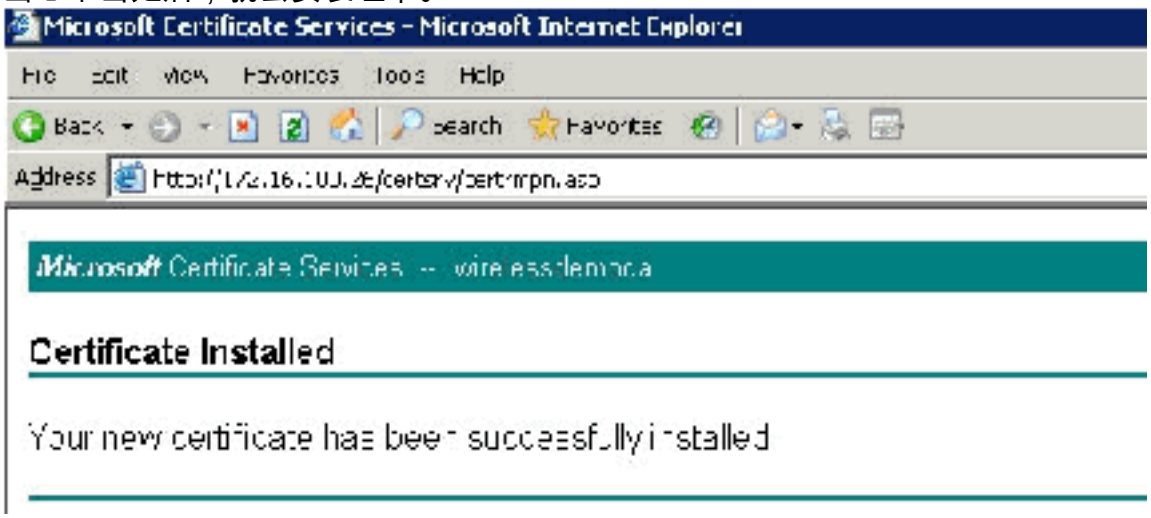
10. 单击 **Install this certificate**。



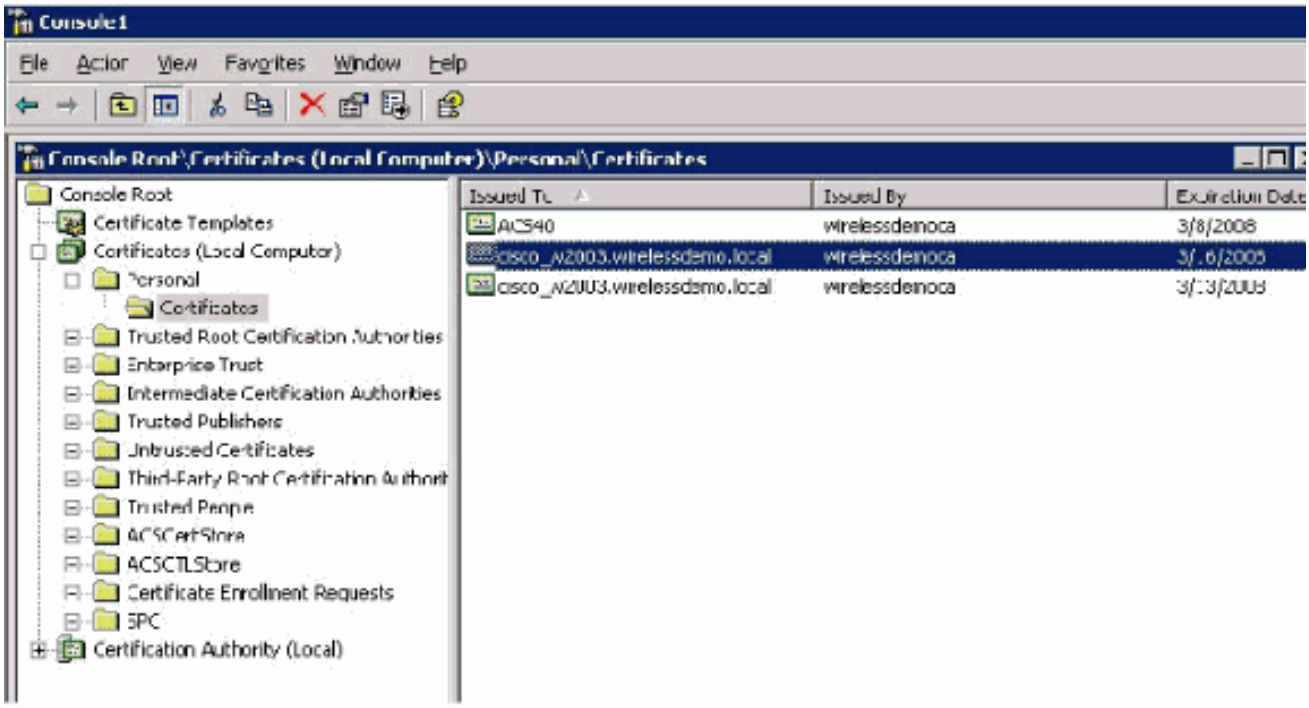
11. 此时将再次显示一个弹出窗口，警告可能出现脚本冲突。选择 Yes。



12. 当您单击**是**后，就会安装证书。



13. 此时，证书安装在证书 MMC 的**个人 > 证书**下。

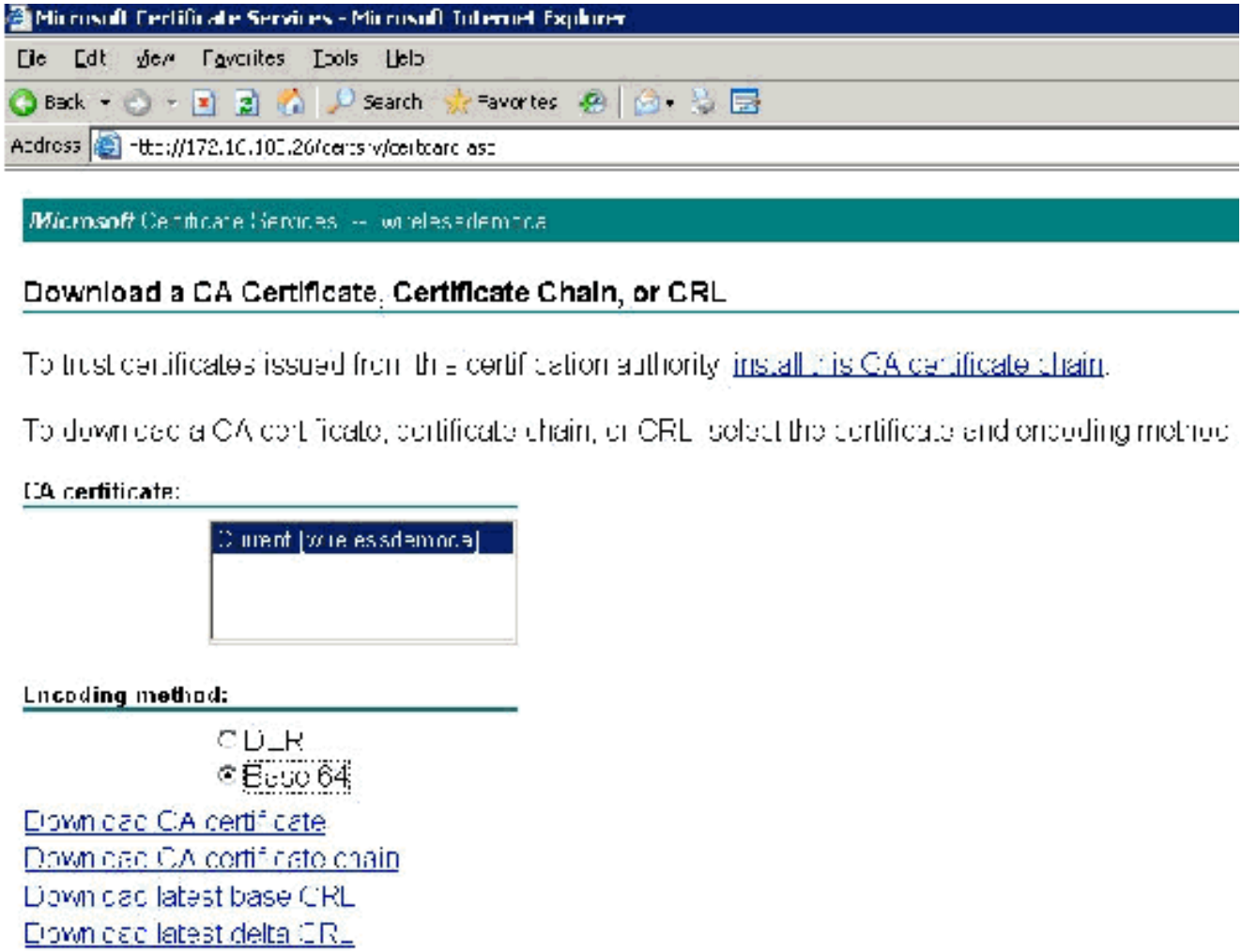


14. 请注意，证书安装在本地计算机（本示例中为 ACS 或 cisco_w2003）上，您需要为 ACS 4.0 证书文件配置生成证书文件 (.cer)。
15. 在 ACS 服务器（本示例中为 cisco_w2003）上，使 Microsoft 证书颁发机构服务器上的浏览器指向 **http://172.16.100.26/certsrv**。

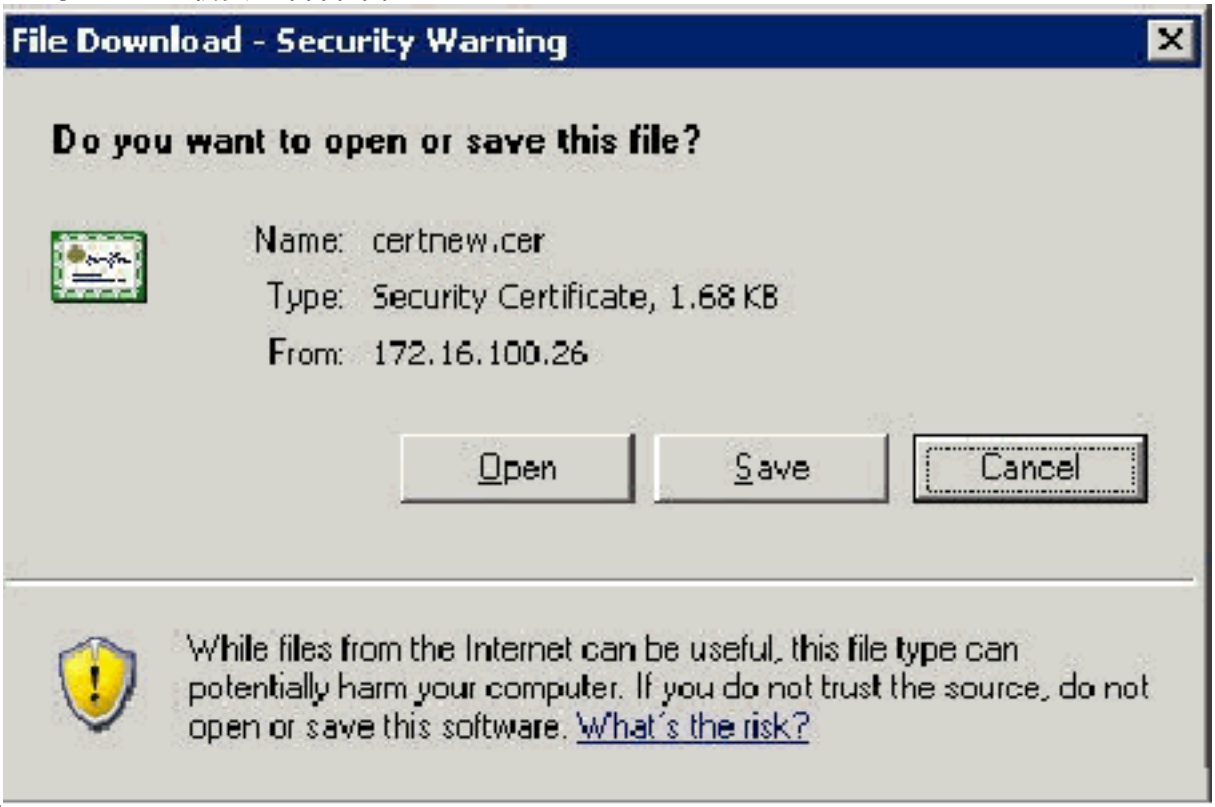
在 ACS 4.0 软件中安装证书

请完成以下步骤：

1. 在 ACS 服务器（本示例中为 cisco_w2003）上，使 Microsoft CA 服务器上的浏览器指向 **http://172.16.100.26/certsrv**。
2. 从“选择一个任务”选项中选择**下载 CA 证书、证书链或 CRL**。
3. 选择 **Base 64 无线电编码方法，然后单击“下载 CA 证书”。**

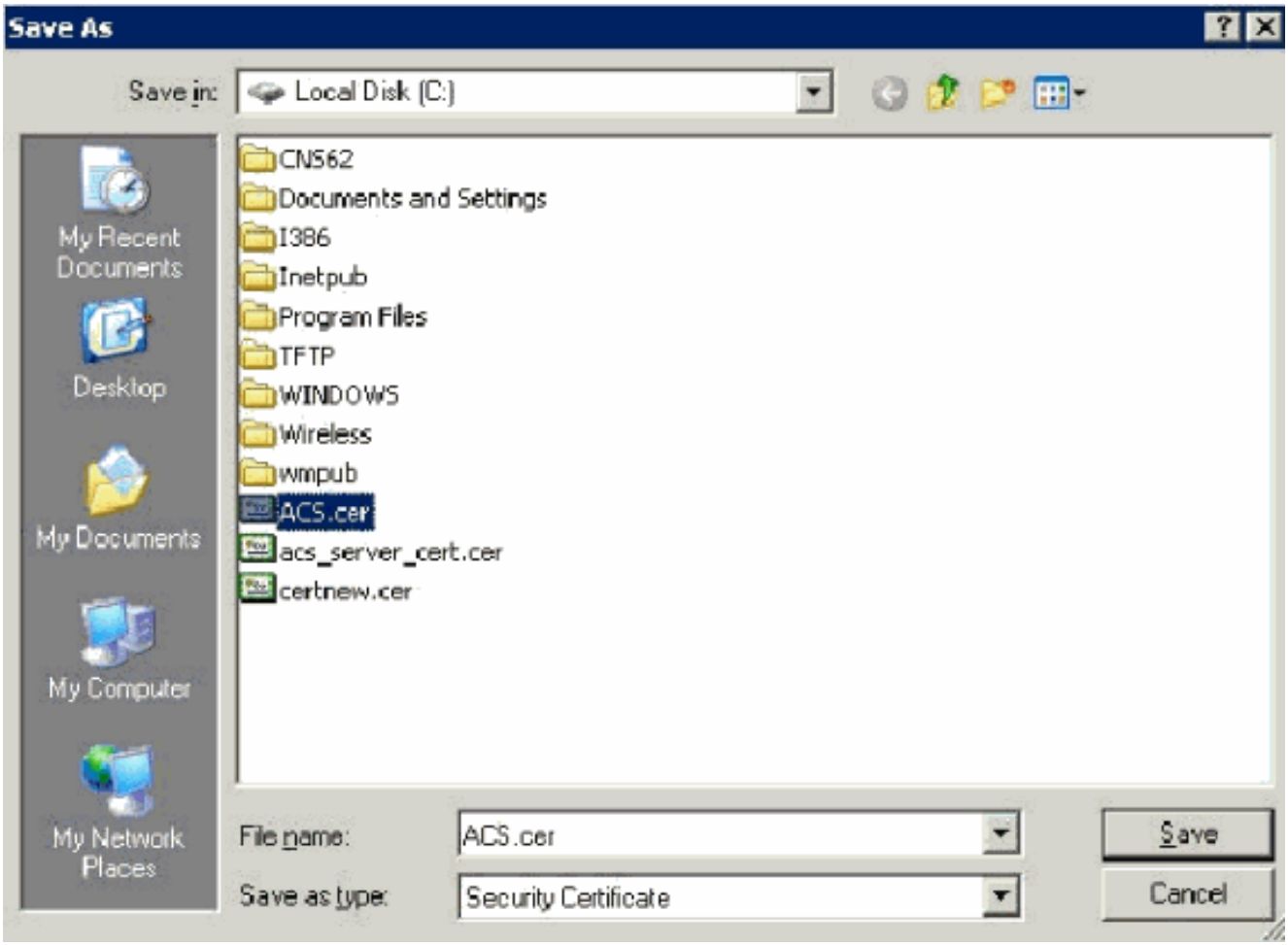


4. 此时将显示“文件下载安全警告”窗口。Click

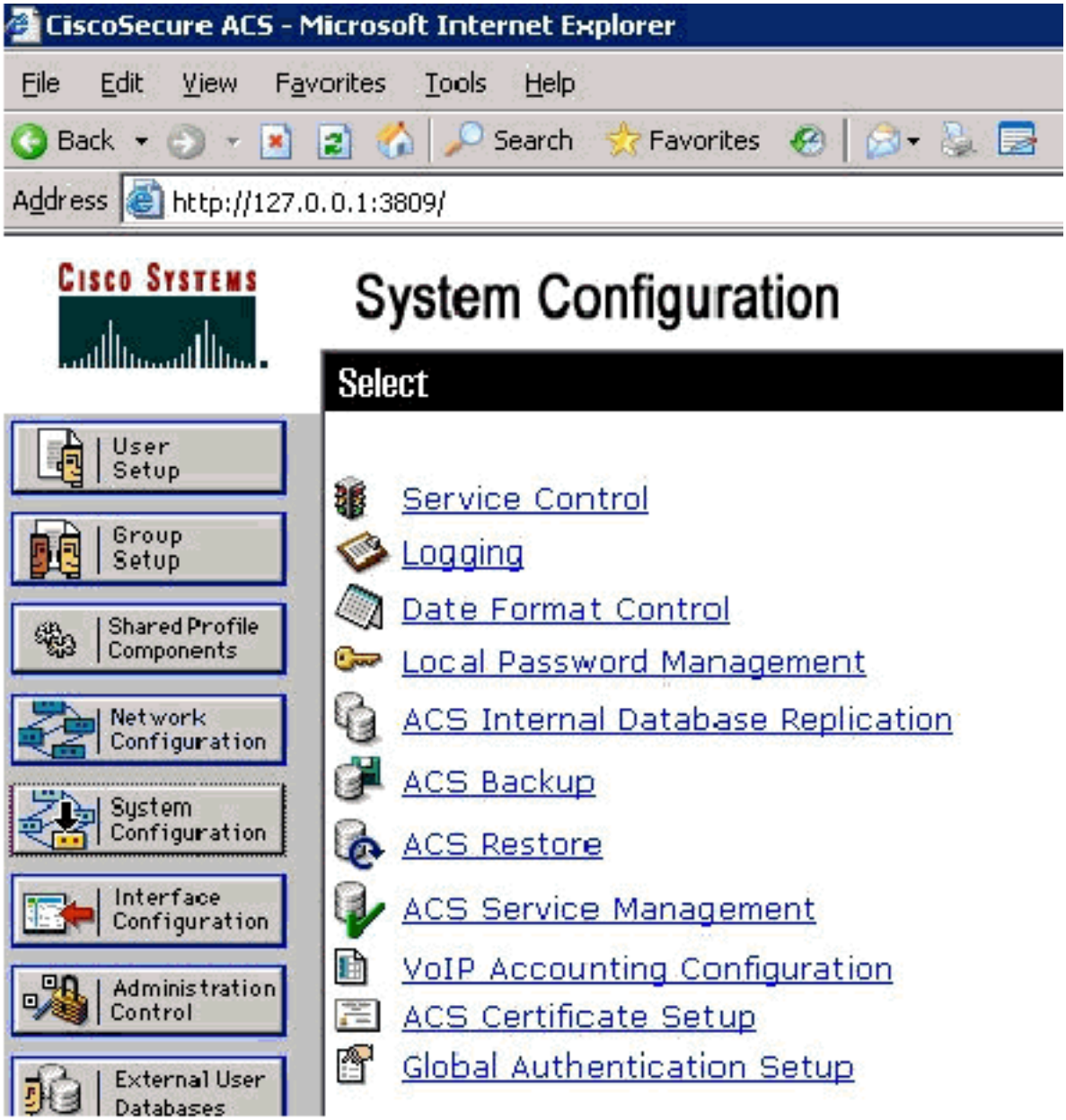


Save.

5. 用 ACS.cer 或您需要的任意名称保存文件。请记住此名称，因为您在 ACS 4.0 中设置 ACS 证书颁发机构的过程中要用到它。

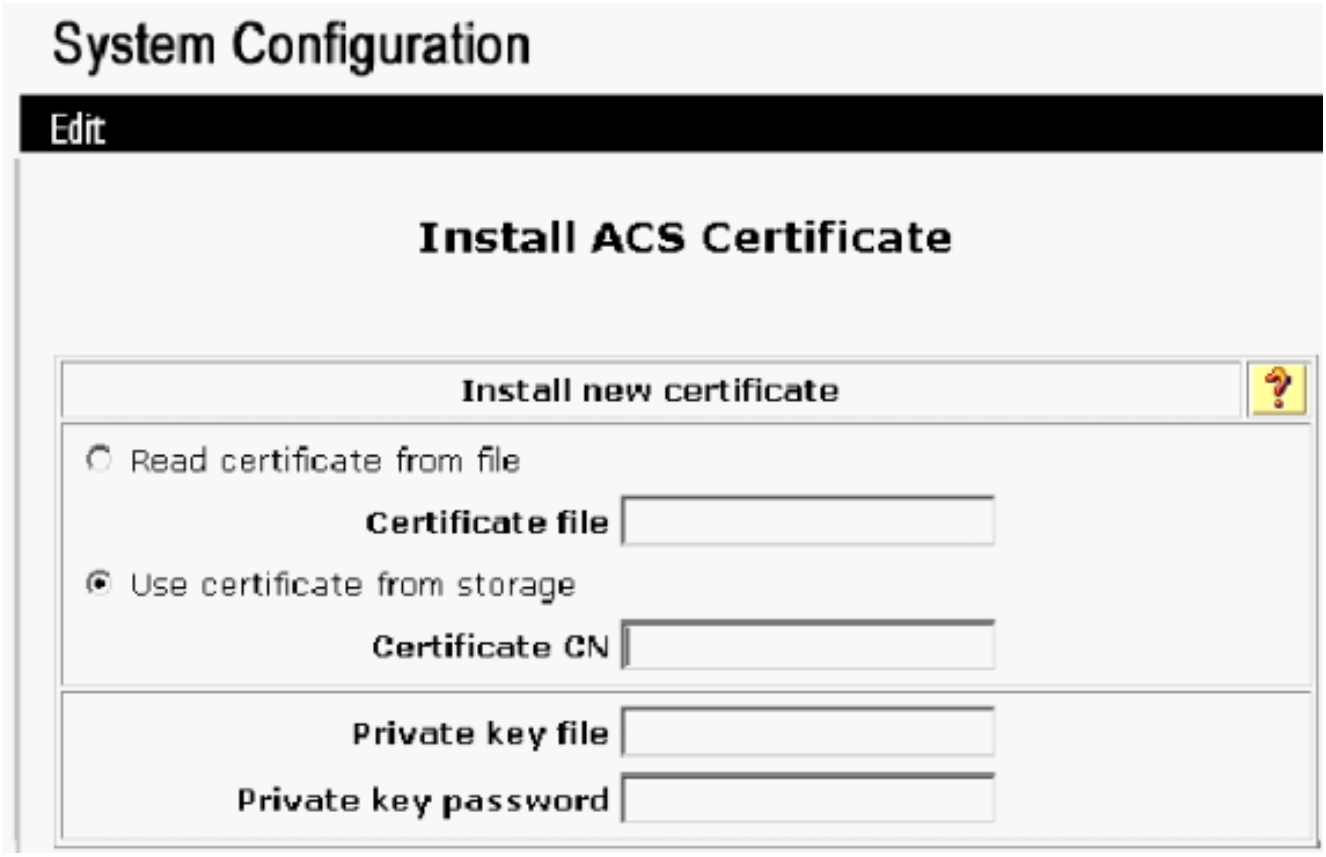


6. 从安装过程中创建的桌面快捷方式打开 **ACS Admin**。
7. 单击 **System Configuration**。



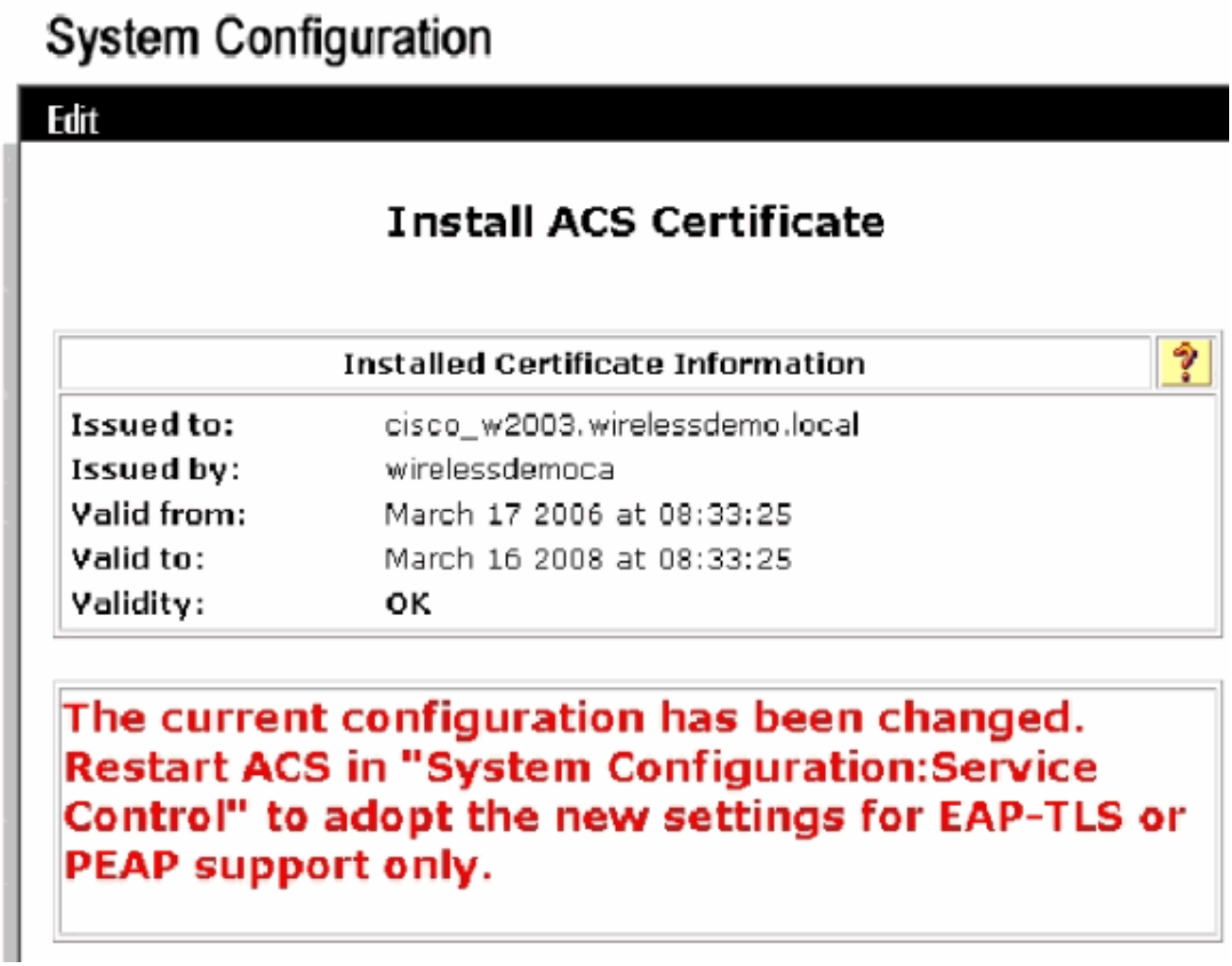
8. 单击 **ACS Certificate Setup**。

9. 单击 Install ACS Certificate。

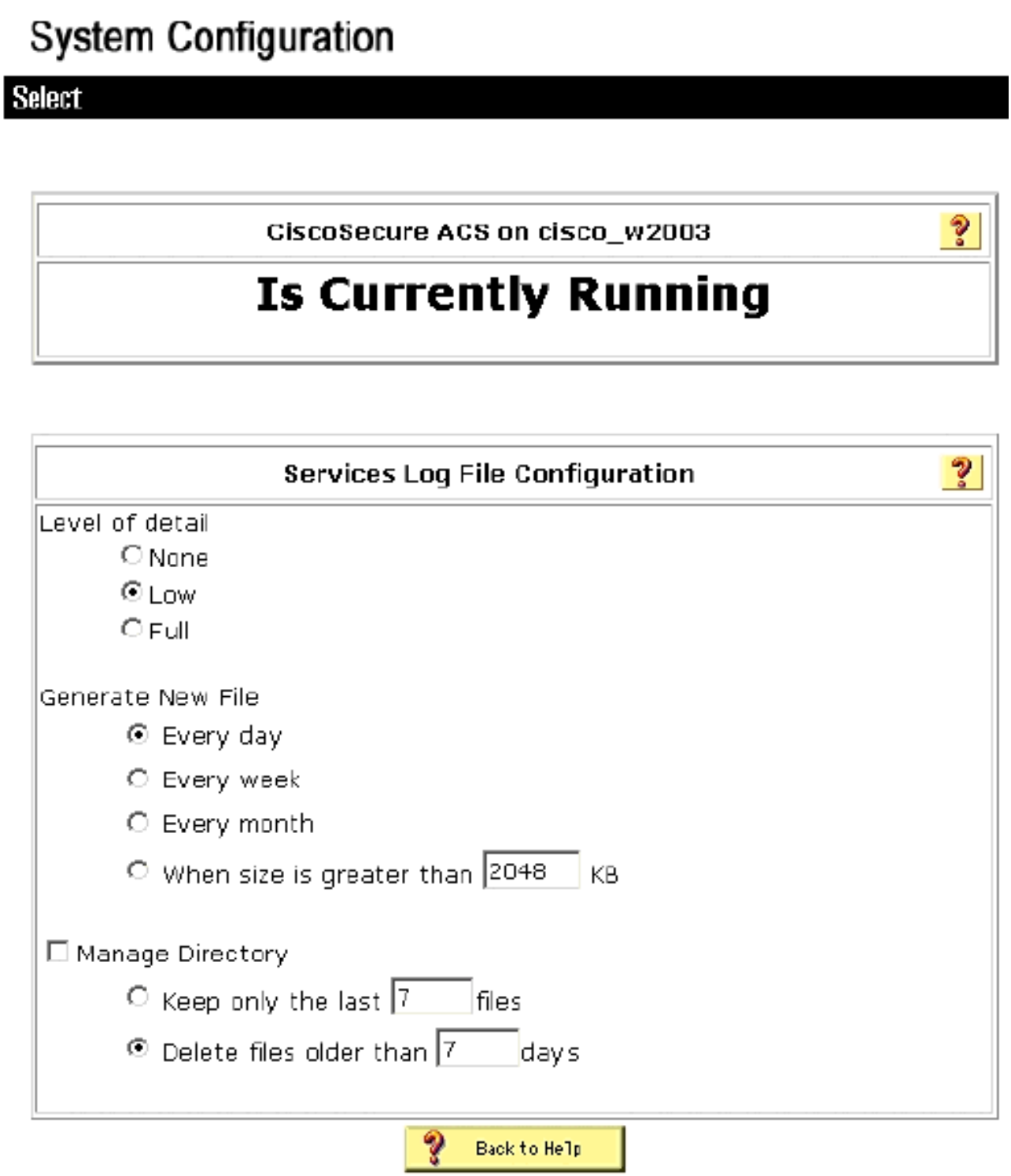


10. 选择 Use certificate from storage 并键入完全限定的域名 cisco_w2003.wirelessdemo.local（如果您使用 ACS 作为名称，则为 ACS.wirelessdemo.local）。

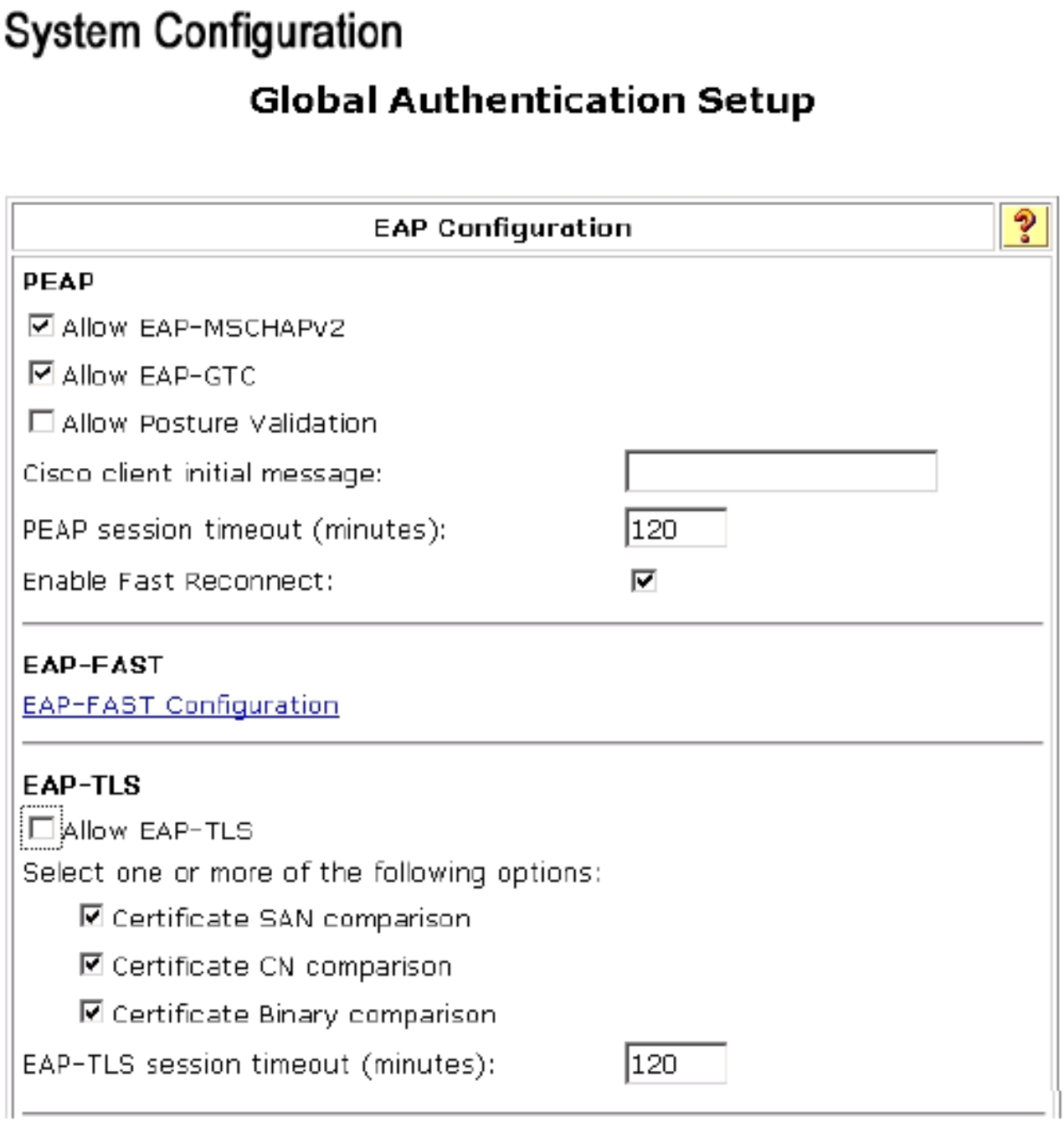
11. 单击“Submit”。



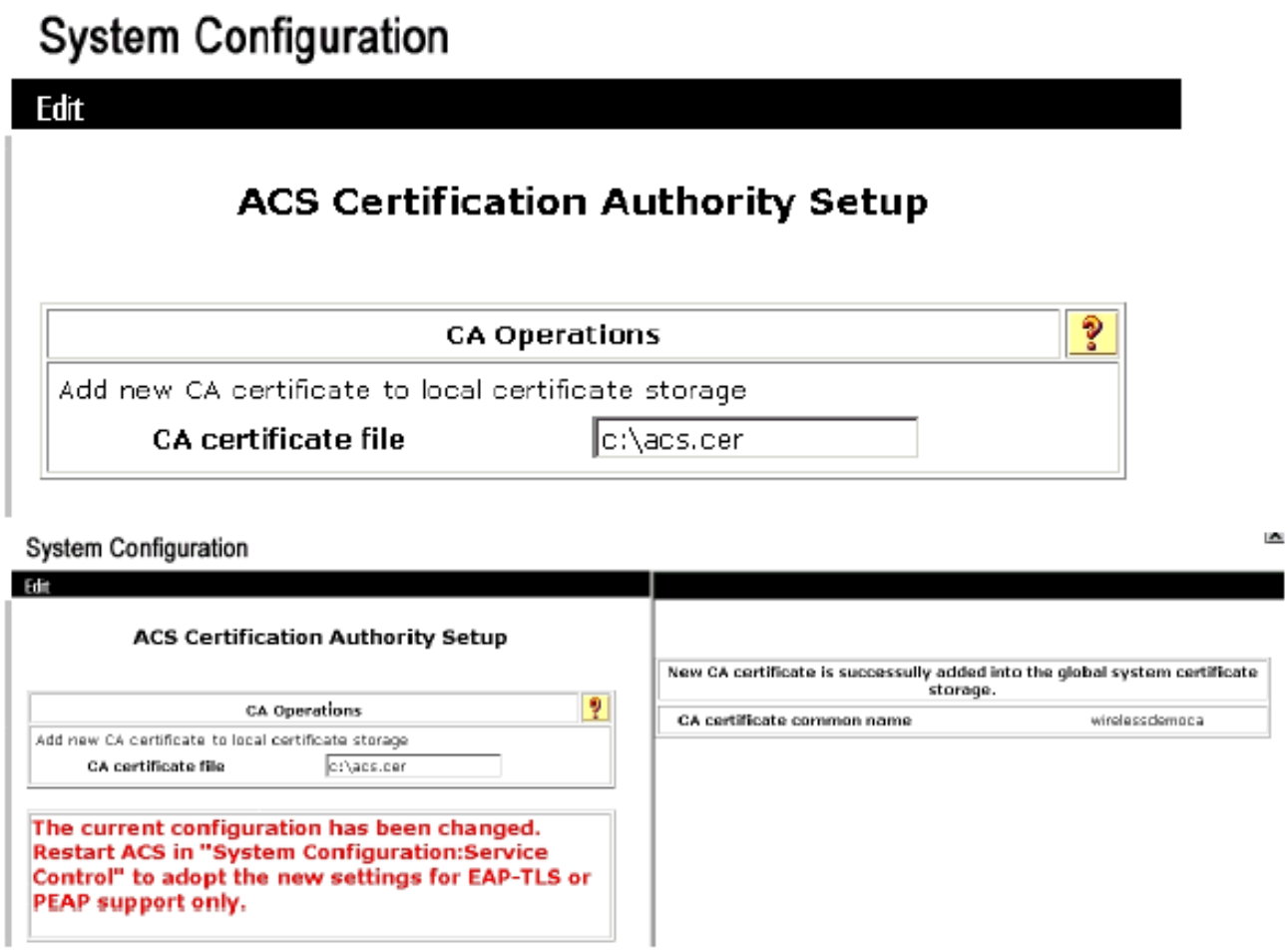
12. 单击 **System Configuration**。
13. 单击 **Service Control**，然后单击“Restart”。



14. 单击 System Configuration。
15. 单击 Global Authentication Setup。
16. 选中 Allow EAP-MSCHAPV2 和“Allow EAP-GTC”。



17. 单击 **Submit+ Restart。**
18. 单击 **System Configuration**。
19. 单击 **ACS Certification Authority Setup**。
20. 在“ACS Certification Authority Setup”窗口下，键入前面创建的 *.cer 文件的名称和位置。在本示例中，所创建的 *.cer 文件是 c:\ 根目录中的 **ACS.cer。**
21. 在“CA certificate file”字段中键入 **c:\acs.cer，然后单击“Submit”。**



22. 重新启动 ACS 服务。

使用 Windows Zero Touch 的 PEAP 的客户端配置

在我们的示例中，CLIENT 是一台运行 Windows XP Professional SP 的计算机，该计算机担当无线客户端，并通过无线 AP 获取对 Intranet 资源的访问权限。要将 CLIENT 配置为无线客户端，请完成本部分中的步骤。

执行基本安装和配置

请完成以下步骤：

1. 使用与集线器相连的以太网电缆，将 CLIENT 连接到 Intranet 网络段。
2. 在 CLIENT 上，安装 Windows XP Professional SP2，使其成为 wirelessdemo.local 域中名为 CLIENT 的成员计算机。
3. 安装Windows XP Professional with SP2。必须安装此程序才能获得PEAP支持。**注意：**在 Windows XP Professional with SP2中，Windows防火墙自动打开。请勿关闭防火墙。

安装无线网络适配器

请完成以下步骤：

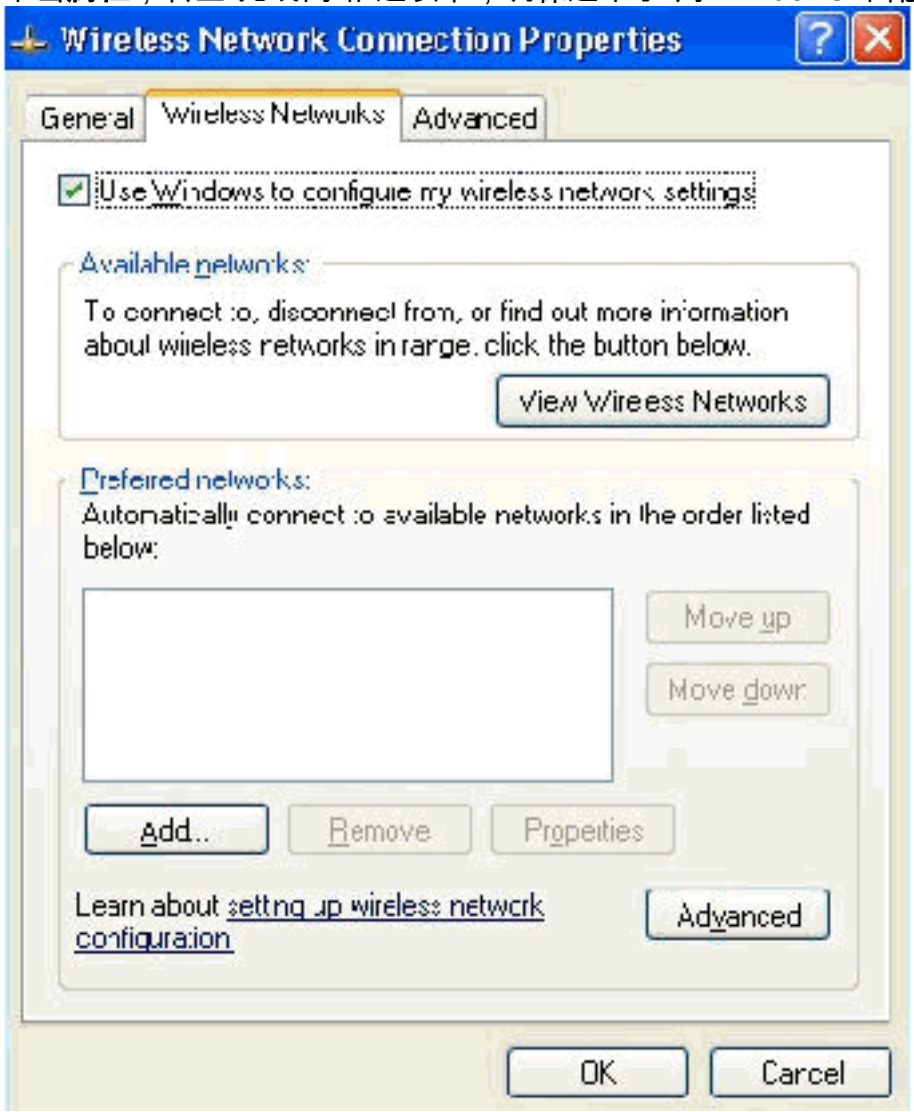
1. 关闭 CLIENT 计算机。
2. 从 Intranet 网络段断开 CLIENT 计算机的连接。
3. 重新启动 CLIENT 计算机，然后使用本地管理员帐户进行登录。

4. 安装无线网络适配器。**重要信息：**请勿安装制造商为无线适配器提供的配置软件。使用“添加硬件向导”安装无线网络适配器的驱动程序。并且在出现提示时，提供由制造商提供的 CD 或包含用于 Windows XP Professional SP2 的更新驱动程序的磁盘。

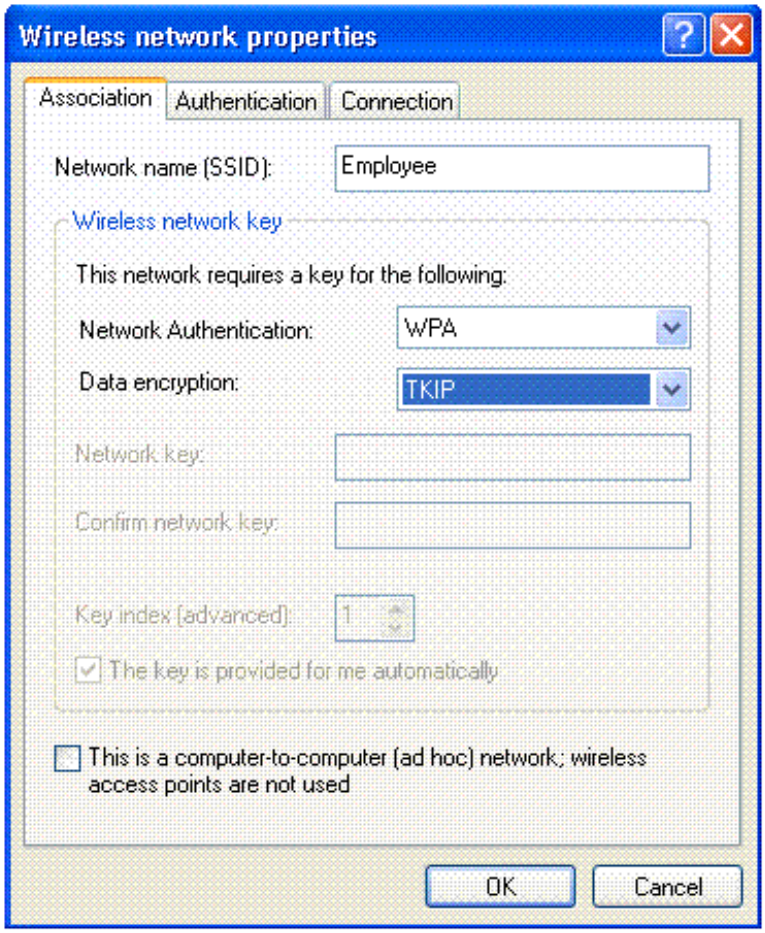
配置无线网络连接

请完成以下步骤：

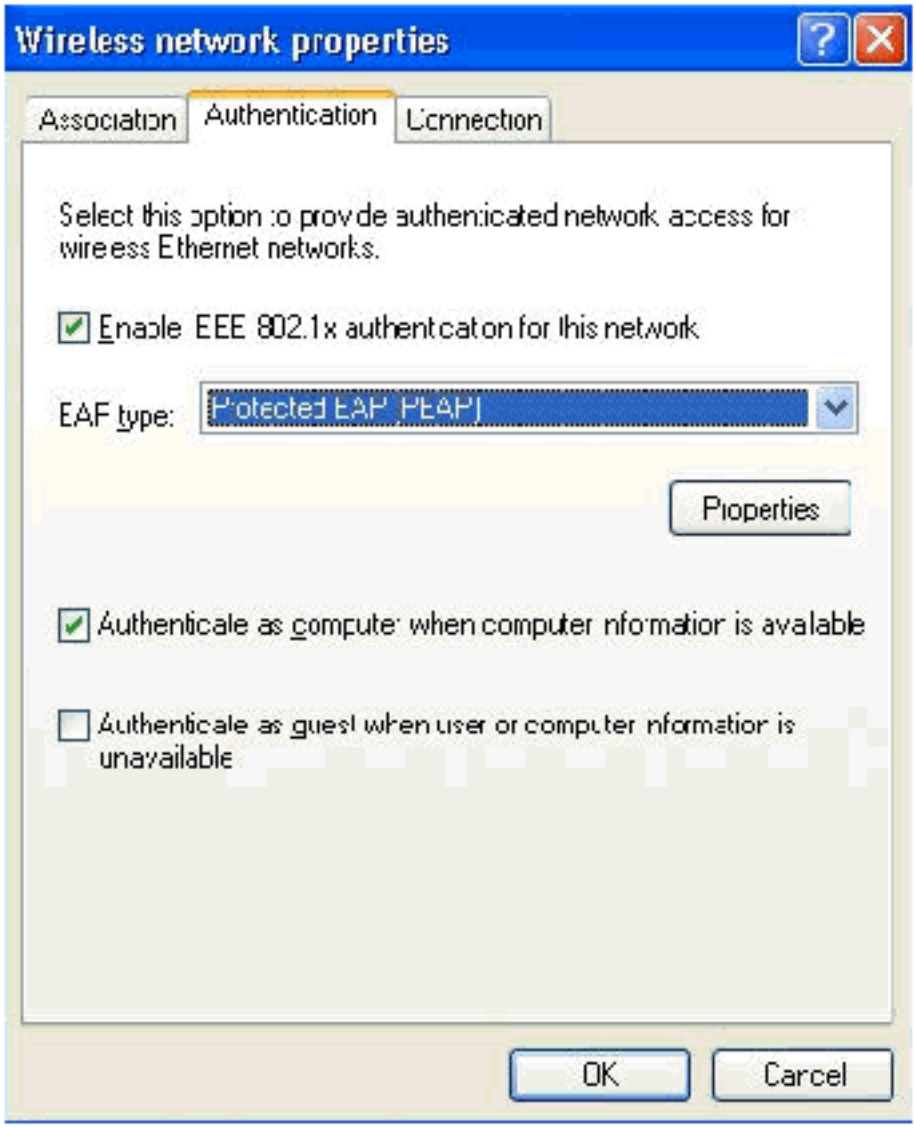
1. 注销，然后使用 wirelessdemo.local 域中的 WirelessUser 帐户重新登录。
2. 选择**开始 > 控制面板**，双击“网络连接”，然后右键单击“无线网络连接”。
3. 单击**属性**，转至“无线网络”选项卡，确保选中了“用 Windows 来配置我的无线网络设置”。



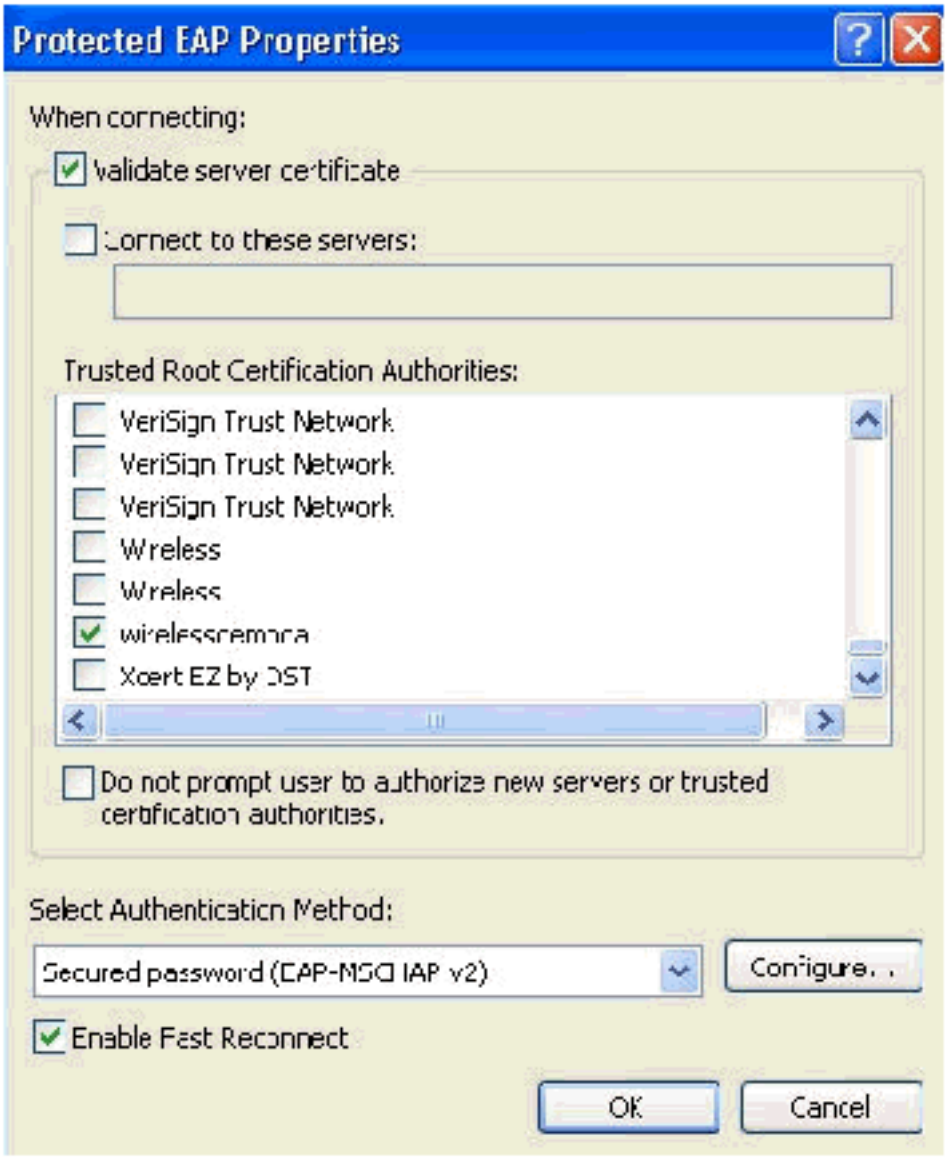
4. 单击 **Add**。
5. 在“关联”选项卡下，在“网络名称 (SSID)”字段中键入 **Employee**。
6. 为“网络身份验证”选中 **WPA，并确保“数据加密”设置为 TKIP**。



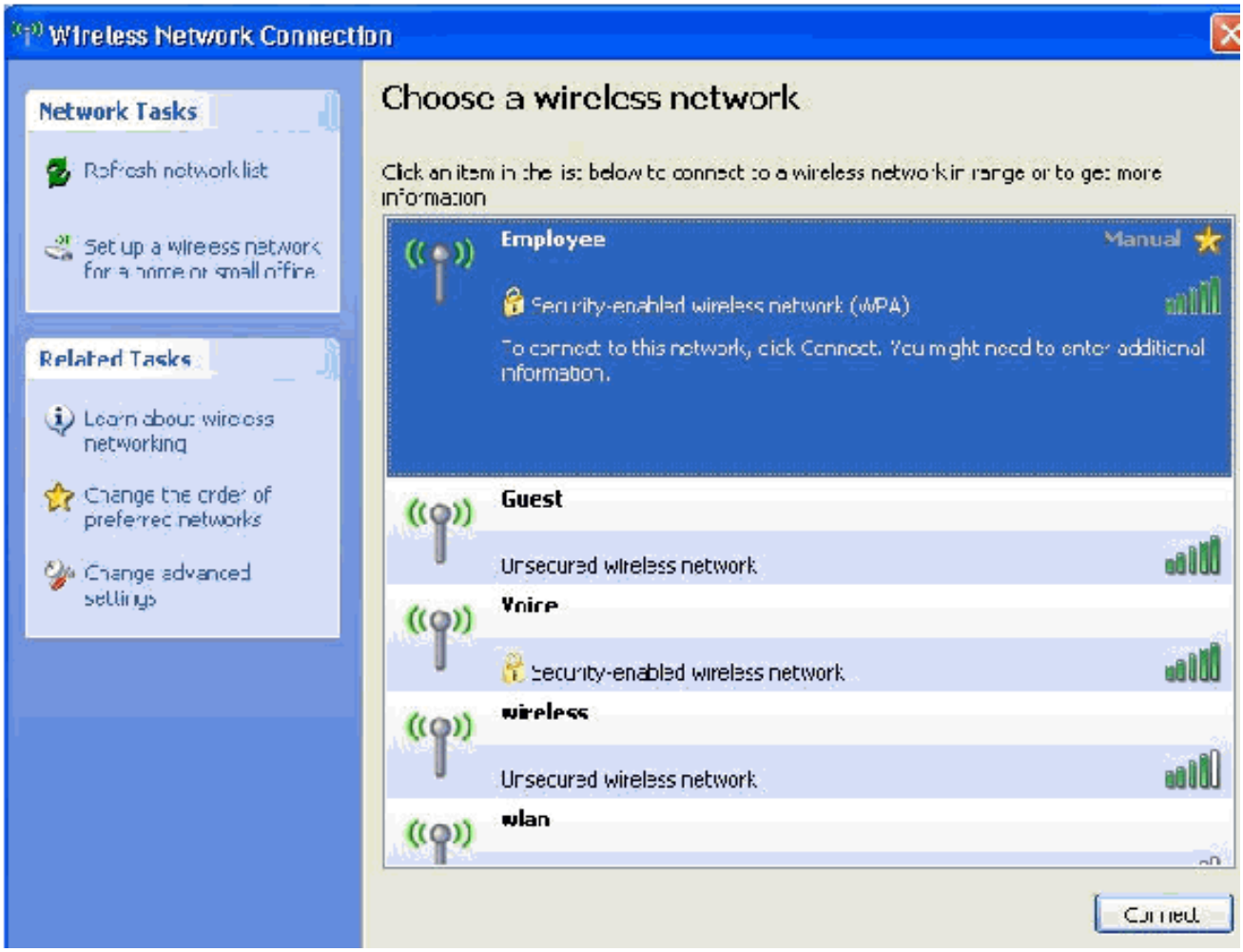
7. 转至“身份验证”选项卡。
8. 验证“EAP 类型”配置为使用**受保护的 EAP (PEAP)**。 如果不是，请从下拉菜单中选择此选项。
9. 如果您希望计算机在登录之前进行身份验证（从而应用登录脚本或组策略推送），请选中**当计算机信息可用时身份验证为计算机**。



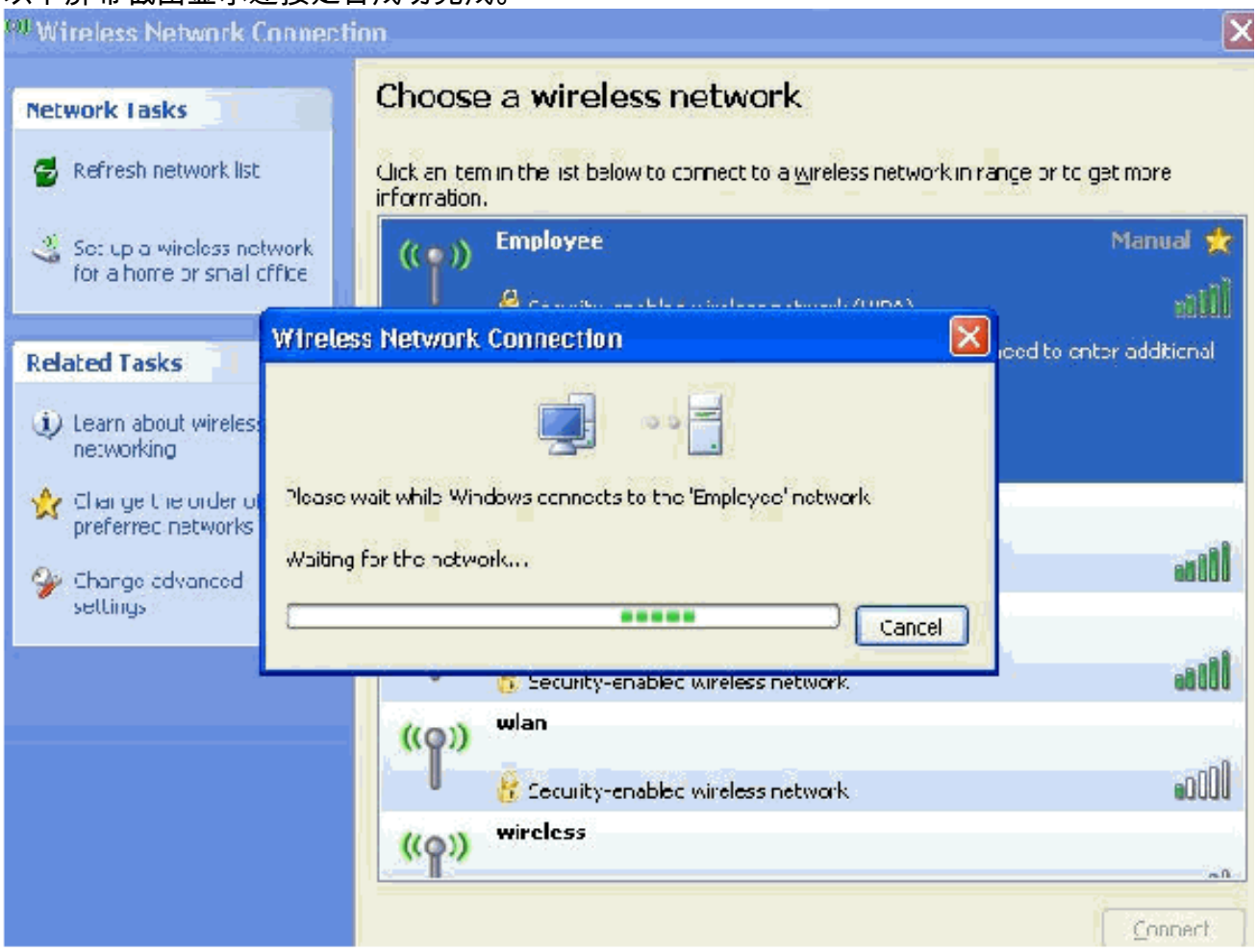
10. 单击 **Properties**。
11. 由于 PEAP 涉及由客户端对服务器进行身份验证，请确保选中“验证服务器证书”。并且，确保在*受信任的根证书颁发机构菜单下选中“颁发 ACS 证书的 CA”*。
12. 在“身份验证方法”下选择**安全密码 (EAP-MSCHAP v2)，因为它用于内部身份验证。**

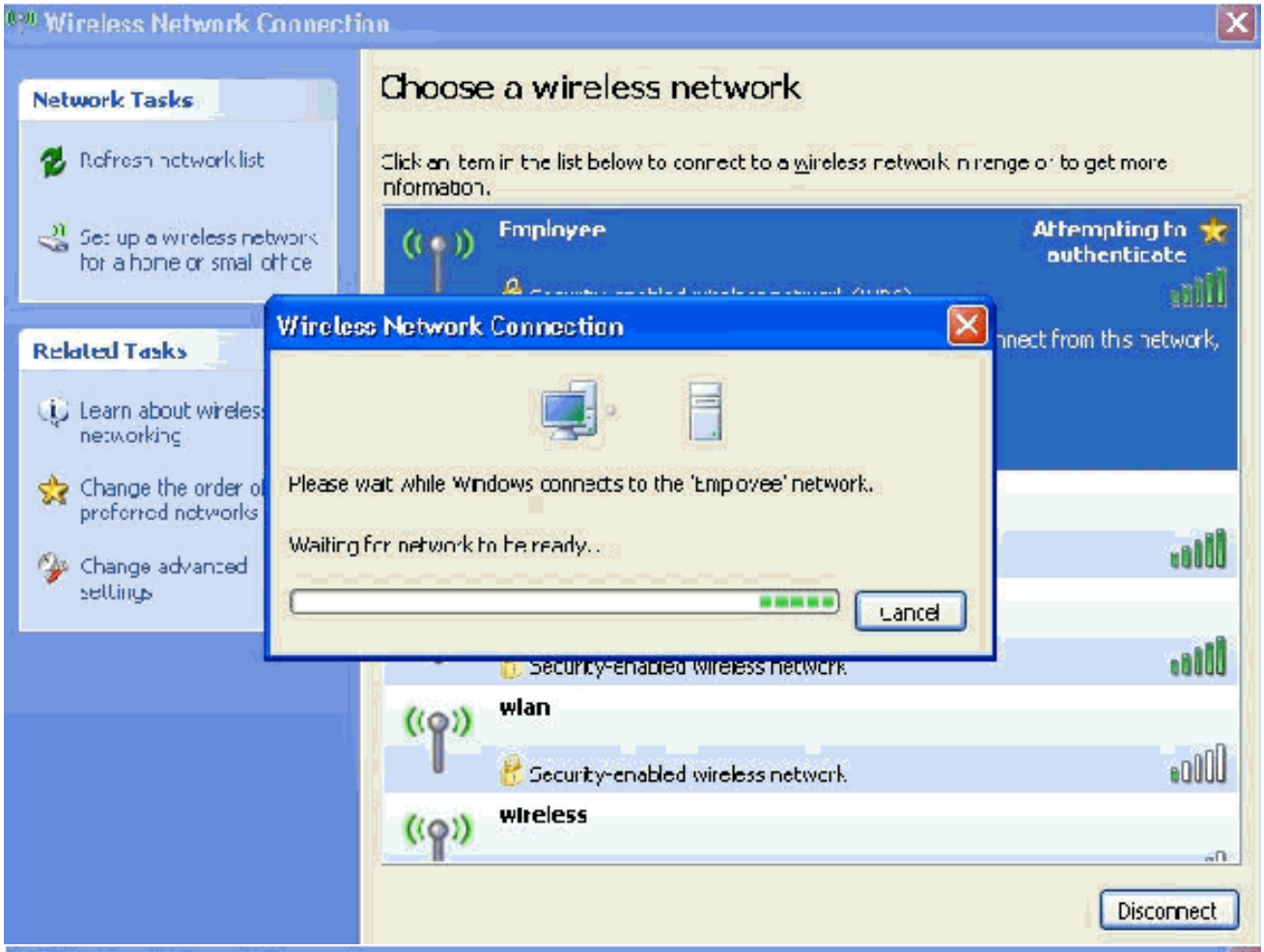


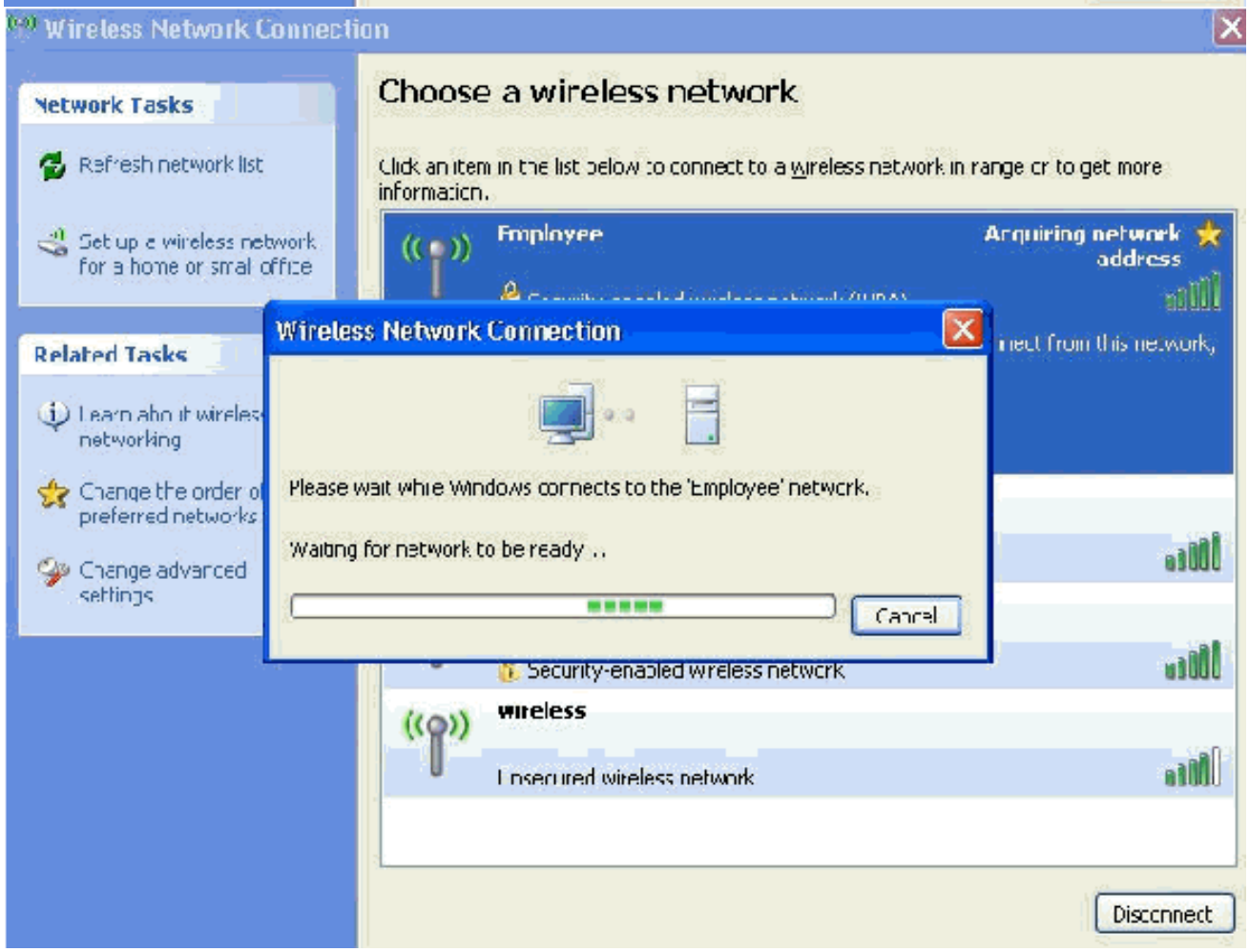
13. 确保选中“启用快速重新连接”复选框。然后，单击三次**确定。**
14. 右键单击系统任务栏中的无线网络连接图标，然后单击**查看可用的无线网络。**
15. 单击 **Employee 无线网络并单击“连接”。**

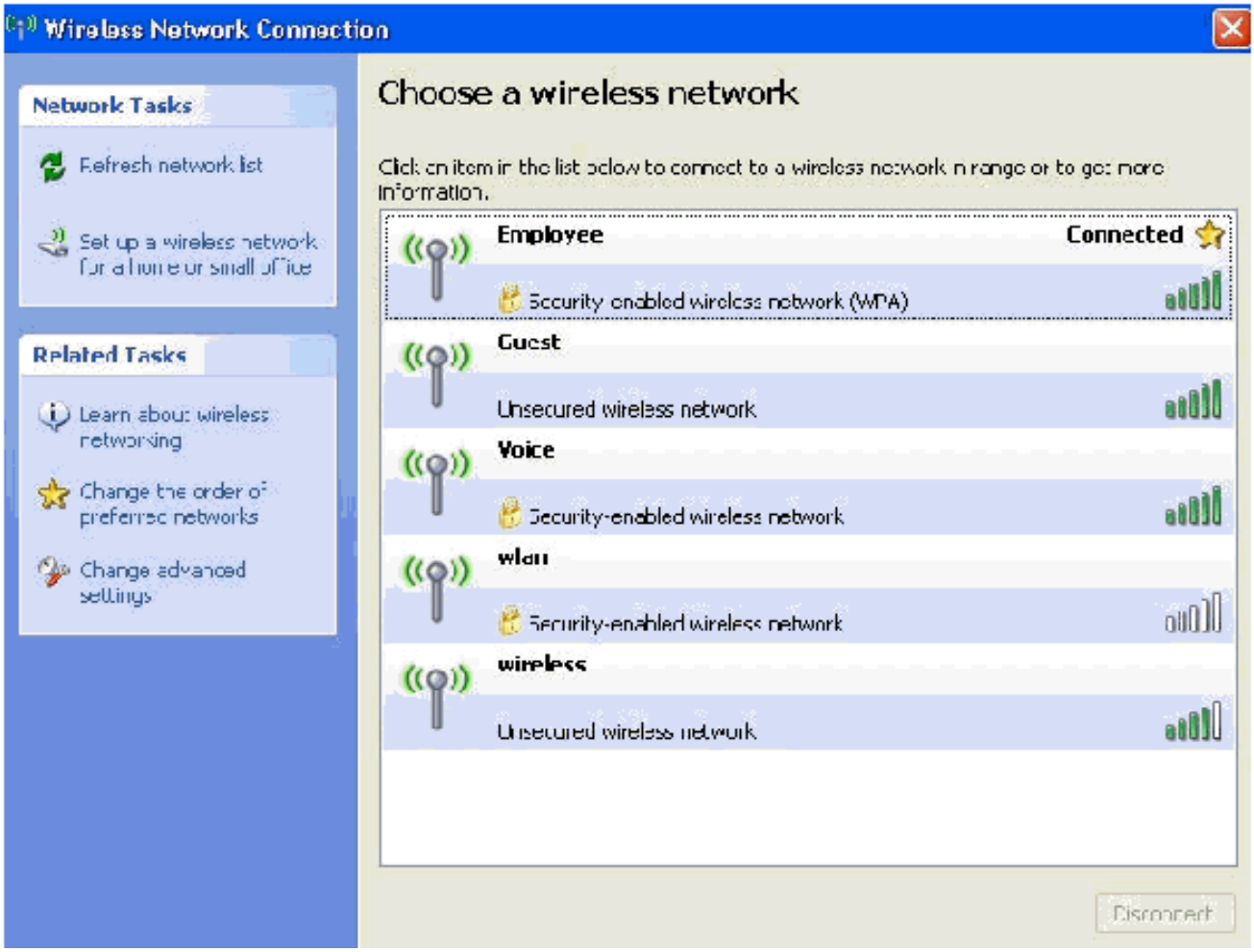


以下屏幕截图显示连接是否成功完成。




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



16. 身份验证成功后，使用“网络连接”来检查无线适配器的 TCP/IP 配置。它的地址范围 172.16.100.100-172.16.100.254 应该来自 DHCP 范围或为无线客户端创建的范围。
17. 要测试功能，请打开浏览器，并浏览到 **http://wirelessdemoca（或企业 CA 服务器的 IP 地址）。**

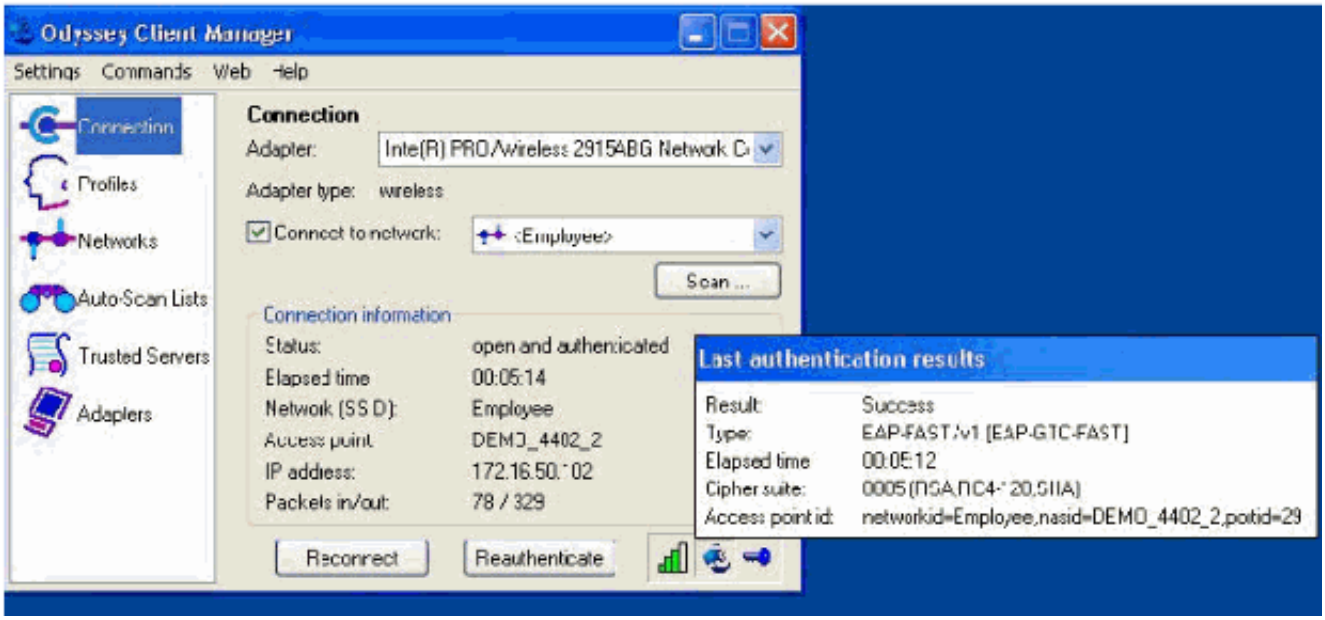
问题：Odyssey 客户端为令牌身份验证平台提示三次

此问题出现在所有 Windows 版本和 2.x 解决方案中。

通常，此问题是由 XP 中的无线服务设置引起的。

要更正此问题，请执行以下步骤：

1. 选择**开始 > 设置 > 控制面板 > 管理工具 > 服务**。
2. 转至列表底部，找到**无线零配置**。
3. 双击此设置。
4. 选择选项以停止此服务。
5. 在启动类型的设置下，选择**禁用**。**注意：**如果您所做的只是停止服务，则服务会在重新启动时重新启动，因此您必须禁用它，以便不再出现此问题。
6. 保存设置并关闭。



使用 ACS Server 进行 PEAP 身份验证失败

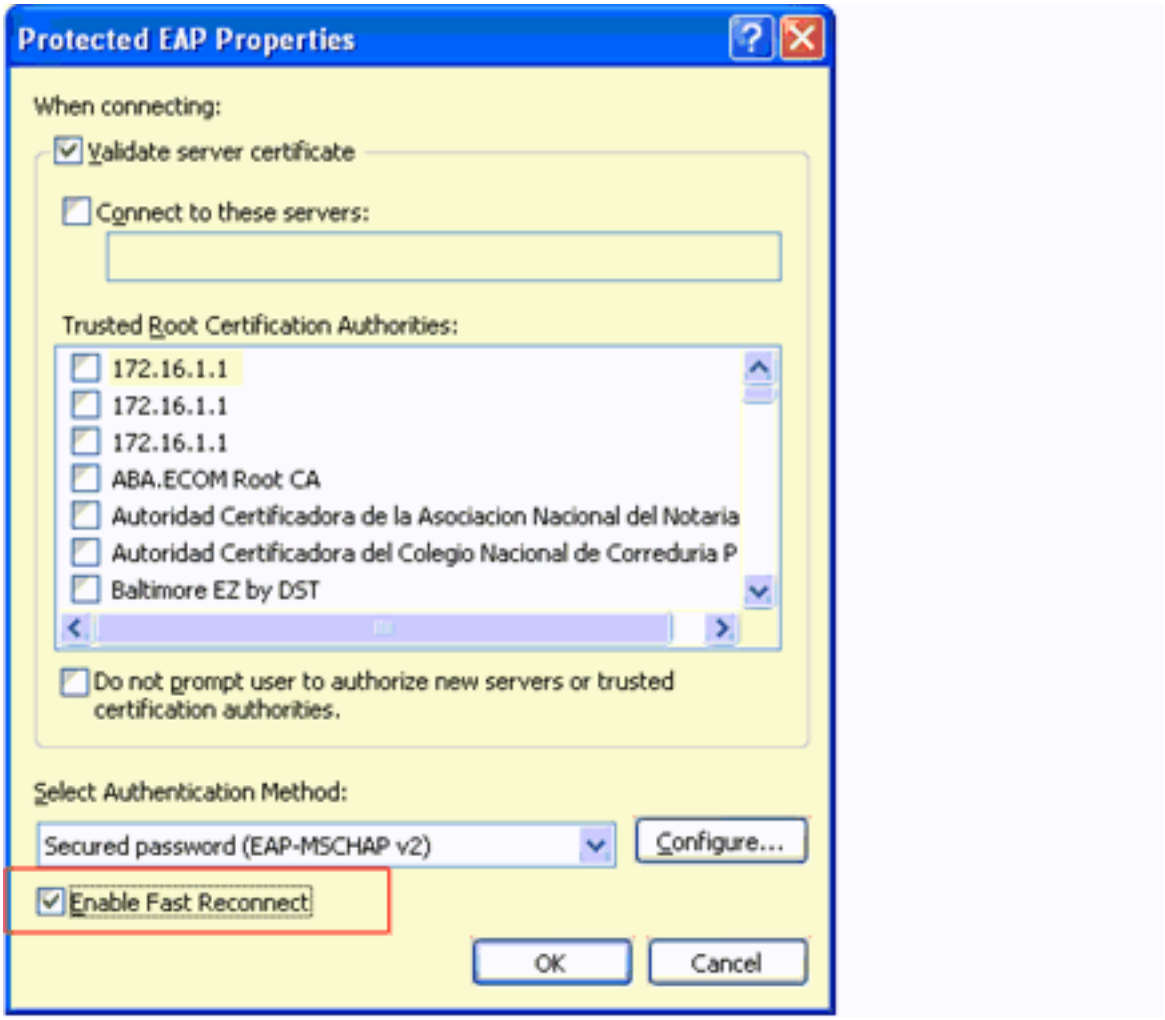
当您的客户端未能通过 ACS 服务器的 PEAP 身份验证时，请检查您是否能在 ACS 的“Report and Activity”菜单下的 **Failed attempts option 中找到** *NAS duplicated authentication attempt 错误消息。*

如果在客户端计算机上安装了 Microsoft Windows XP SP2，并且 Windows XP SP2 针对第三方服务器而不是 Microsoft IAS 进行身份验证，就会收到此错误消息。特别是，Cisco RADIUS服务器(ACS)使用与Windows XP不同的方法来计算可扩展身份验证协议类型：长度：值格式(EAP-TLV)ID。Microsoft 认为此问题是 XP SP2 请求方中的缺陷。

对于修补程序，请与Microsoft联系并参阅文章KB885453。根本问题是，在客户端，使用*windows实用程序*时，默认情况下，*快速重新连接*选项对PEAP处于禁用状态。而在服务器端 (ACS)，此选项在默认情况下是启用的。 要解决此问题，请在 ACS 服务器上取消选中 **Fast Reconnect 选项，并按“submit+restart”。**此外，您也可以在客户端上启用“快速重新连接”选项，以便解决此问题。

要在运行 Windows XP 的客户端上，使用 Windows 实用程序启用“快速重新连接”，请完成以下步骤：

1. 单击Start > Settings > Control Panel。
2. 双击**网络连接图标。**
3. 右键单击**无线网络连接图标，然后单击“属性”。**
4. 单击 **Wireless Networks 选项卡。**
5. 选中*用 Windows 配置我的无线网络设置选项，允许 Windows 来配置客户端适配器。*
6. 如果您已经配置了 SSID，请选择该 SSID 并单击**属性。**如果没有配置，请单击*新建，以便添加新的 WLAN。*
7. 在**关联选项卡下输入 SSID。**确保*网络身份验证设置为***开，并且“数据加密”设置为“WEP”。**
8. 单击**身份验证。**
9. 选中*启用此网络的 IEEE 802.1x 身份验证选项。*
10. 为 *EAP 类型选择* **PEAP，然后单击“属性”。**
11. 选中页面底部的**启用快速重新连接选项。**



相关信息

- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- 无线局域网控制器配置指南
- 无线 LAN 控制器和轻量接入点基本配置示例
- 无线局域网控制器上的 VLAN 配置示例
- 具有无线局域网控制器的 AP 组 VLAN 配置示例
- 技术支持和文档 - Cisco Systems