ACS 4.0 和 Windows 2003 中统一无线网络下的 EAP-TLS

目录

简介

本文档介绍如何使用无线局域网控制器(WLC)、Microsoft Windows 2003软件和思科安全访问控制服务器(ACS)4.0通过可扩展身份验证协议传输层安全(EAP-TLS)配置安全无线访问。

注：有关安全无线部署的详细信息，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。

开始之前，请在测试实验室的每台服务器上安装带有Service Pack(SP)1的Windows Server 2003操作系统，并更新所有Service Pack。安装控制器和AP并确保配置了最新的软件更新。

重要信息：在编写本文档时，SP1是最新的Windows Server 2003更新，带有更新补丁的SP2是Windows XP Professional的最新软件。

使用带SP1的Windows Server 2003企业版，以便可以配置用户证书和工作站证书的自动注册以进行EAP-TLS身份验证。本文档的“EAP-TLS身份验证”部分对此进行了说明。证书自动注册和自动续约通过自动过期和续约证书，使部署证书和提高安全性变得更加容易。

使用的组件

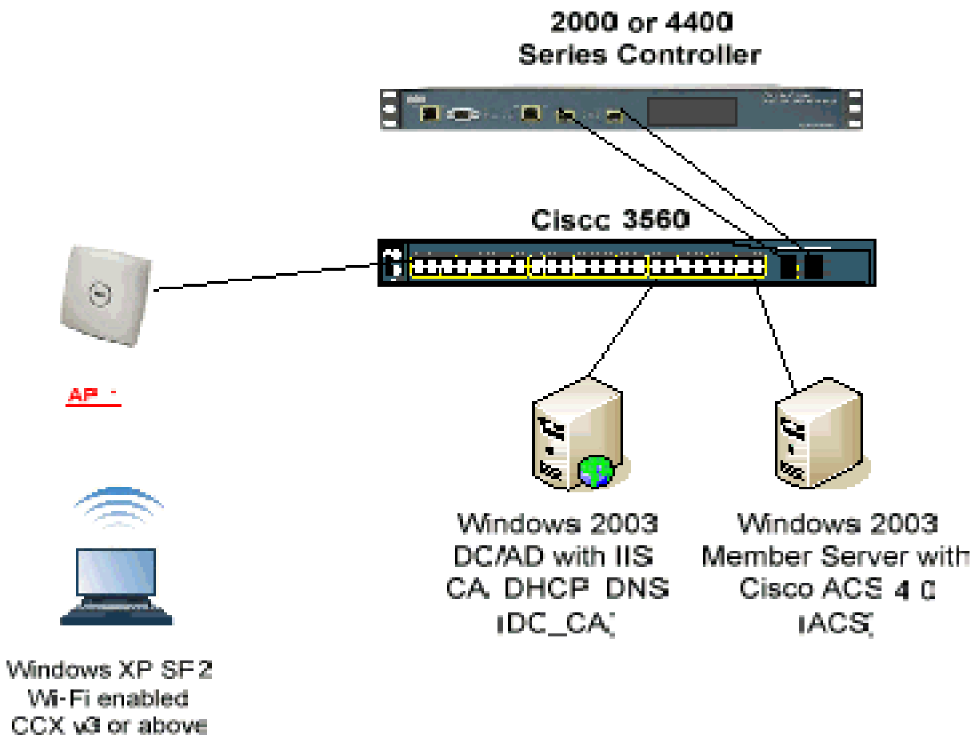
本文档中的信息基于以下软件和硬件版本：

- 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在使用ACS 4.0和Windows 2003 Enterprise服务器的统一无线网络下实施EAP-TLS的分步过程。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 SP2 。

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

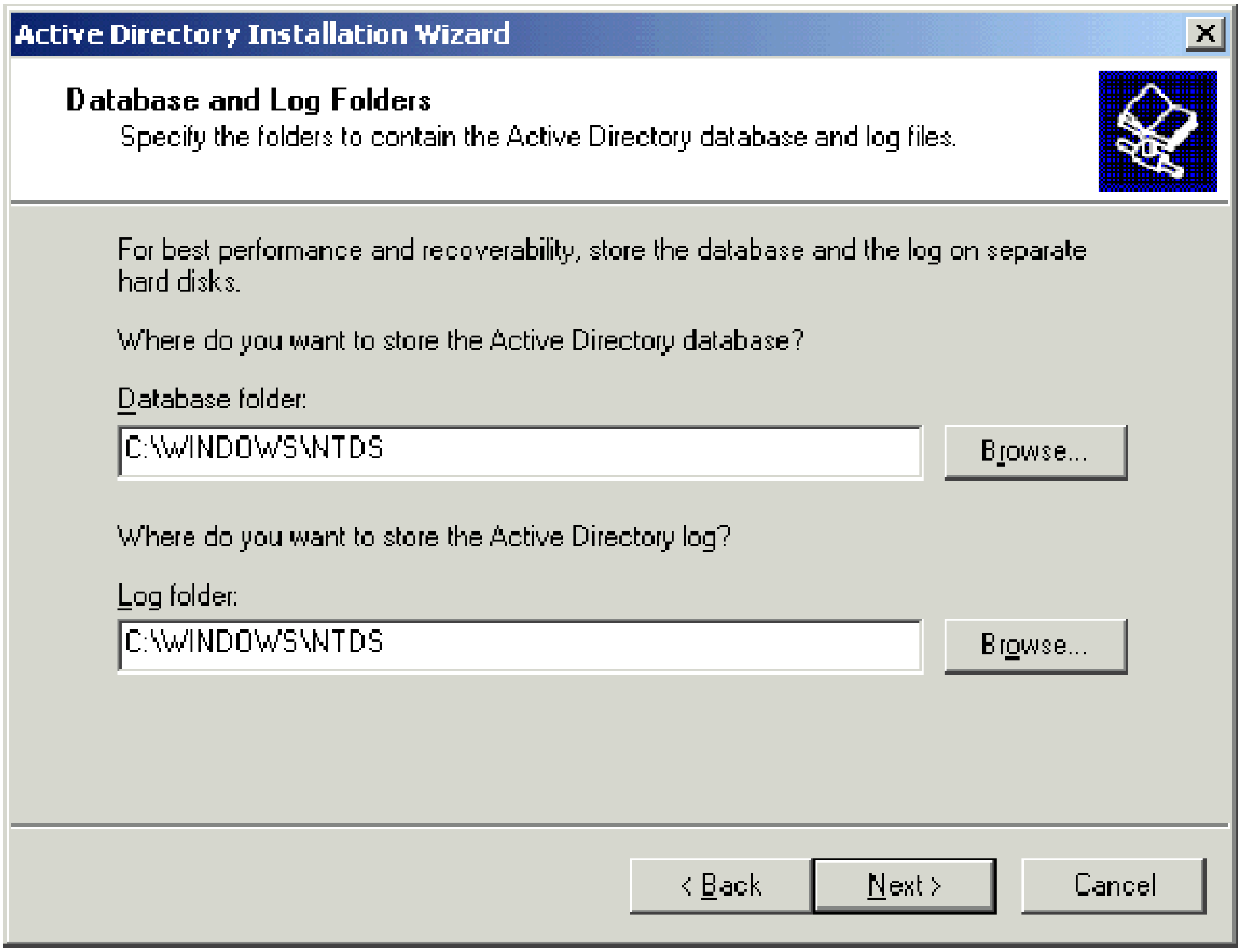
请完成以下步骤：

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”页面上，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**。



Active Directory Installation Wizard

Database and Log Folders

Specify the folders to contain the Active Directory database and log files.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

Database folder:

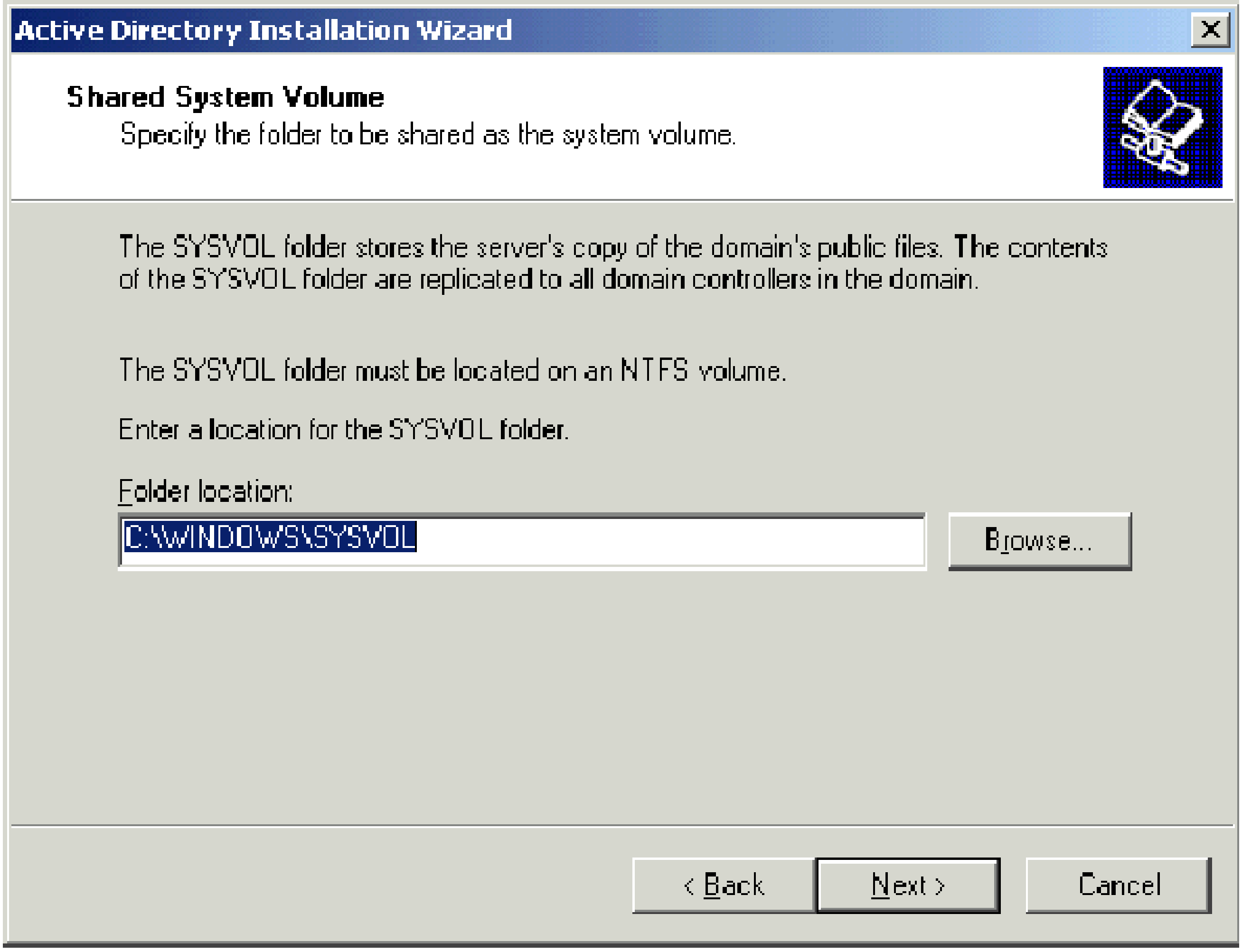
C:\WINDOWS\NTDS

Where do you want to store the Active Directory log?

Log folder:

C:\WINDOWS\NTDS

10. 在“共享系统卷”对话框中，验证默认文件夹位置是否正确，然后单击“下**一步”**。



Shared System Volume

Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

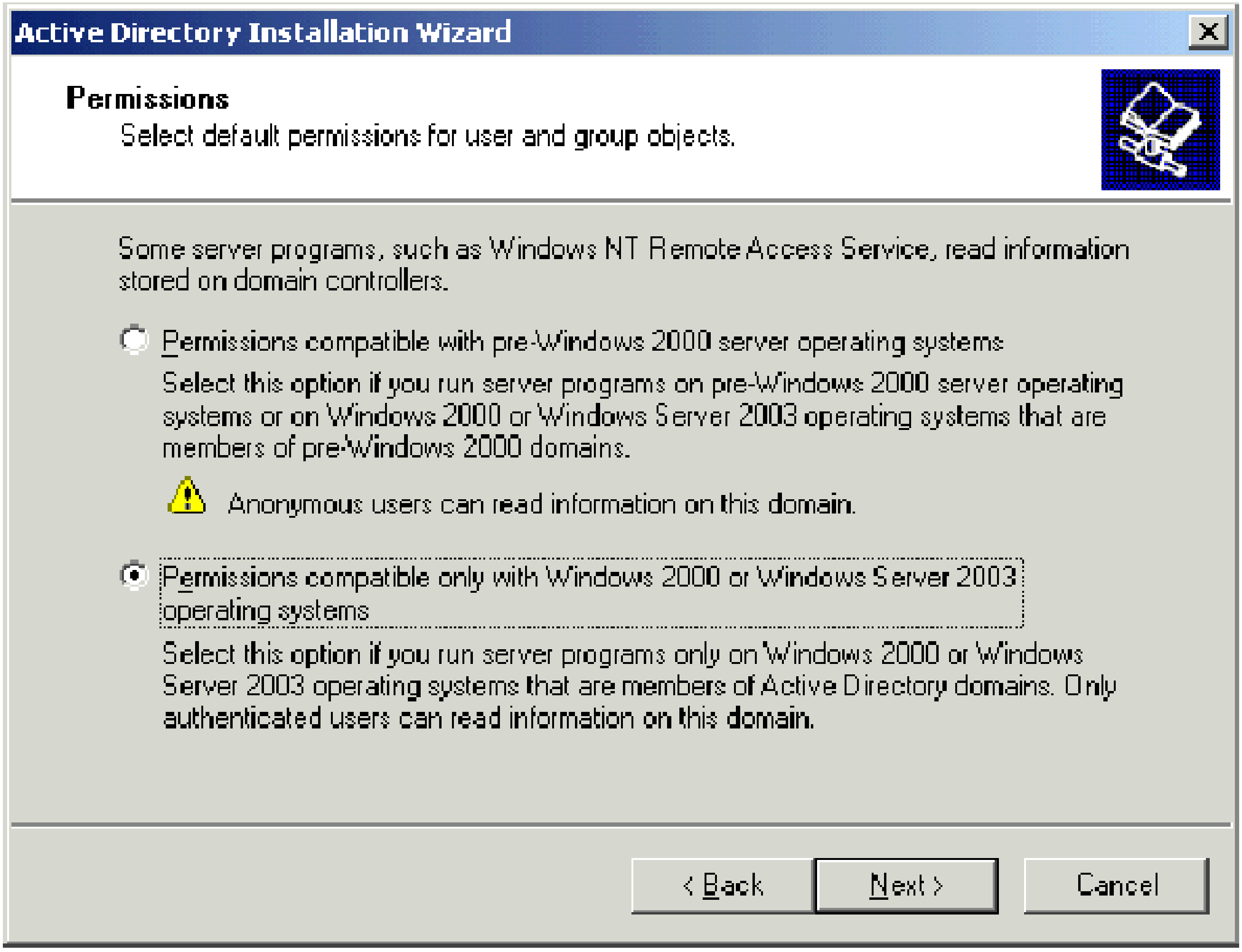
The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

Folder location:

C:\WINDOWS\SYSVOL

11. 在“权限”页上，验证是否**已选择“仅与Windows 2000或Windows Server 2003操作系统兼容的权限**”并单**击“下一步**”。



Permissions

Select default permissions for user and group objects.

Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.

○ Permissions compatible with pre-Windows 2000 server operating systems

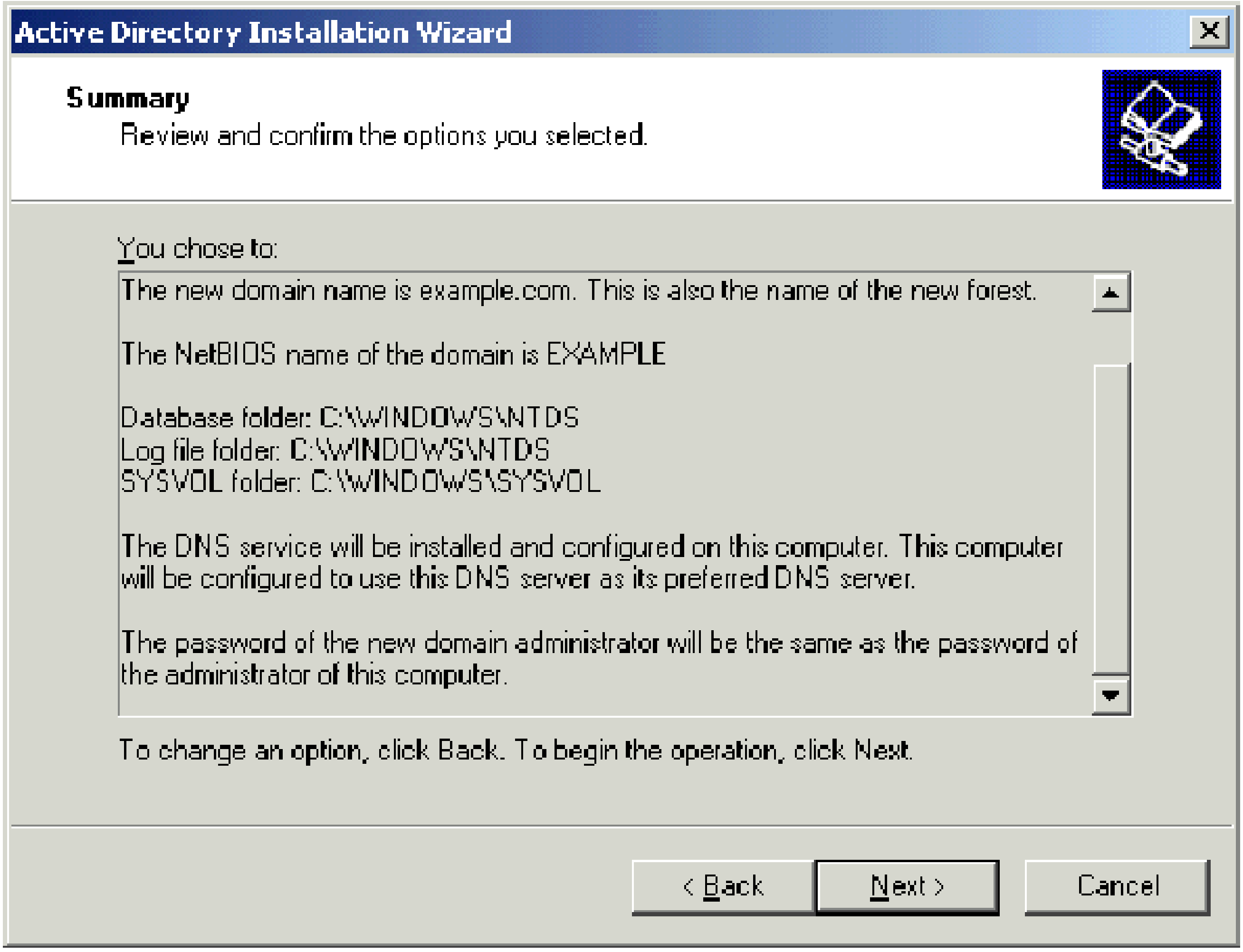
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.

⚠ Anonymous users can read information on this domain.

● Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems

Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.

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**。



Active Directory Installation Wizard

Summary

Review and confirm the options you selected.

You chose to:

The new domain name is example.com. This is also the name of the new forest.

The NetBIOS name of the domain is EXAMPLE

Database folder: C:\WINDOWS\NTDS
Log file folder: C:\WINDOWS\NTDS
SYSVOL folder: C:\WINDOWS\SYSVOL

The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.

The password of the new domain administrator will be the same as the password of the administrator of this computer.

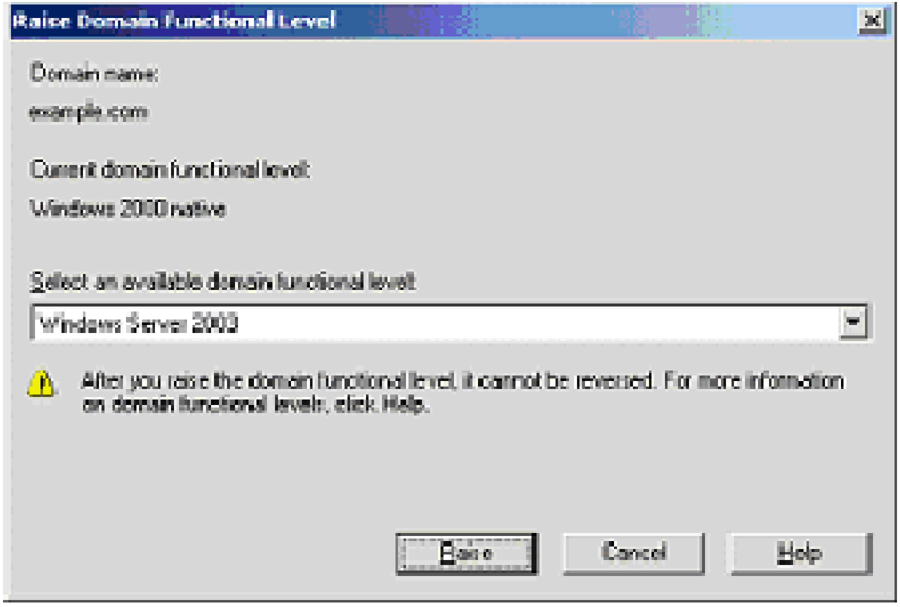
To change an option, click Back. To begin the operation, click Next.

14. 在“完成Active Directory安装向导”页上，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”>“管理工具”>“Active Directory域和信任”**）打开“Active Directory域和信任”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。



Raise Domain Functional Level

Domain name:
example.com

Current domain functional level:
Windows 2000 native

Select an available domain functional level:
Windows Server 2003

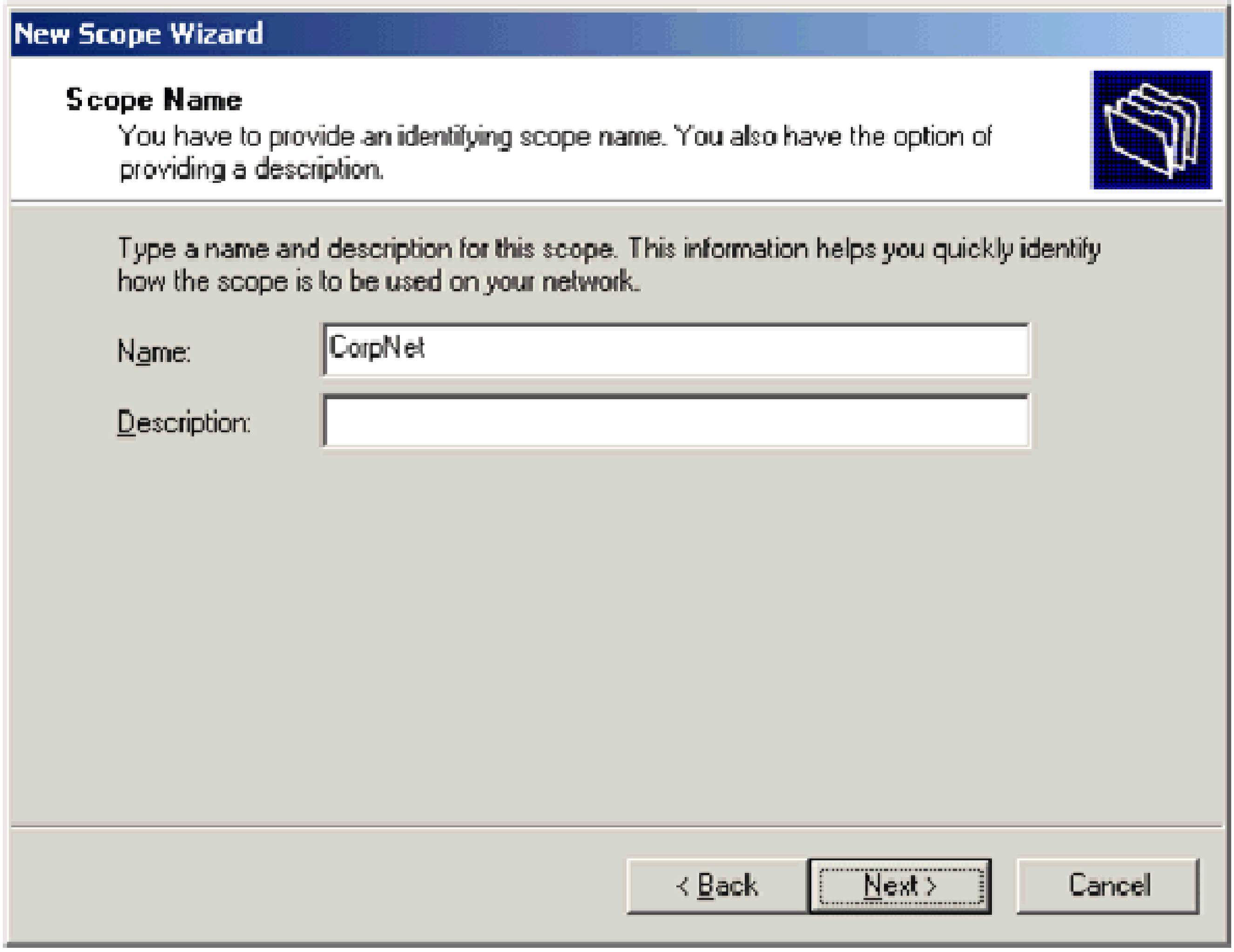
After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help.

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（**“开始”>“程序”>“管理工具”>“DHCP”）打开DHCP管理单元**，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. 在控制台树上，右键单击**DC_CA.wirelessdemo.local，然**后单击“新建**范围”**。
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。**



New Scope Wizard

Scope Name

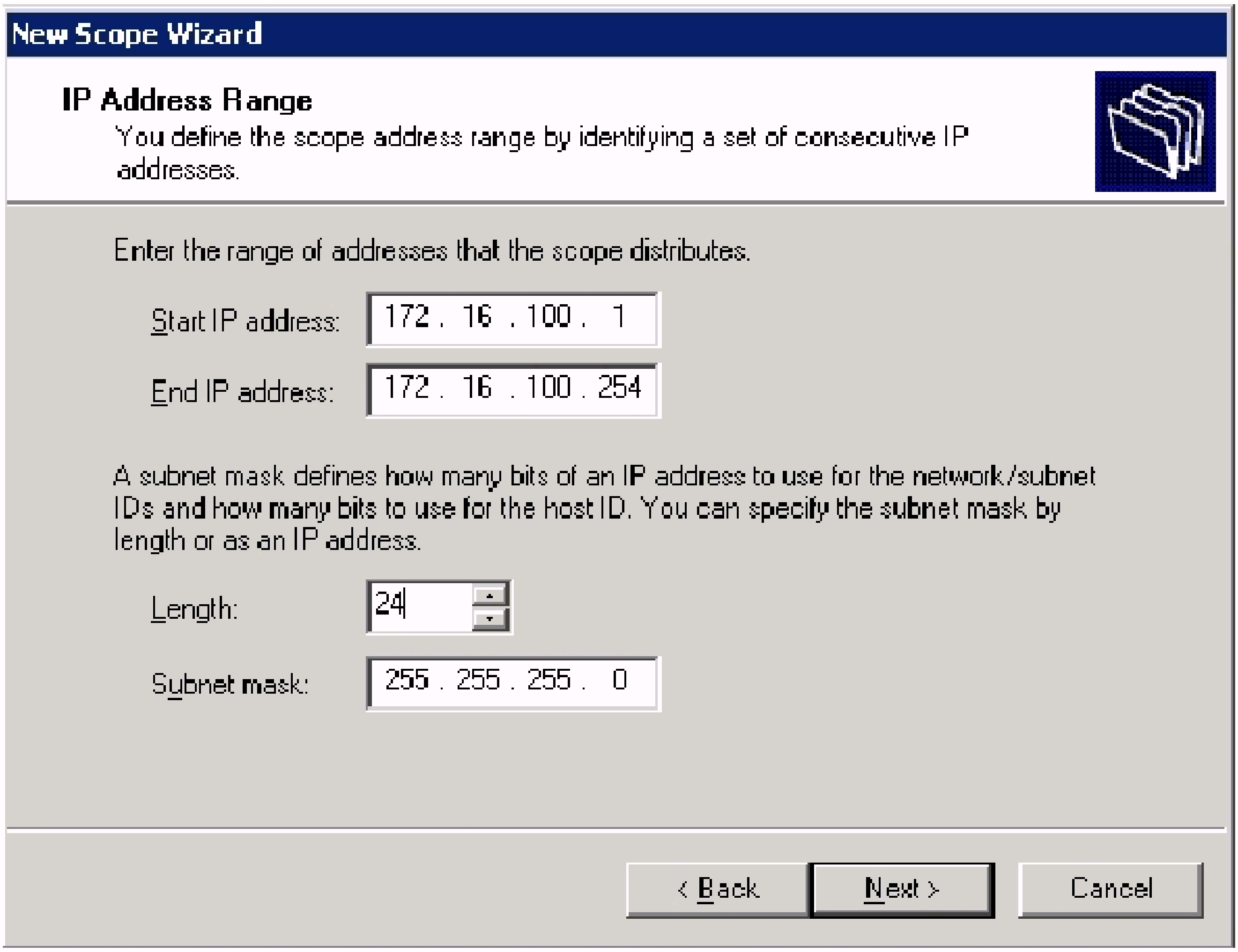
You have to provide an identifying scope name. You also have the option of providing a description.

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: CorpNet

Description:

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


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: 172 . 16 . 100 . 1

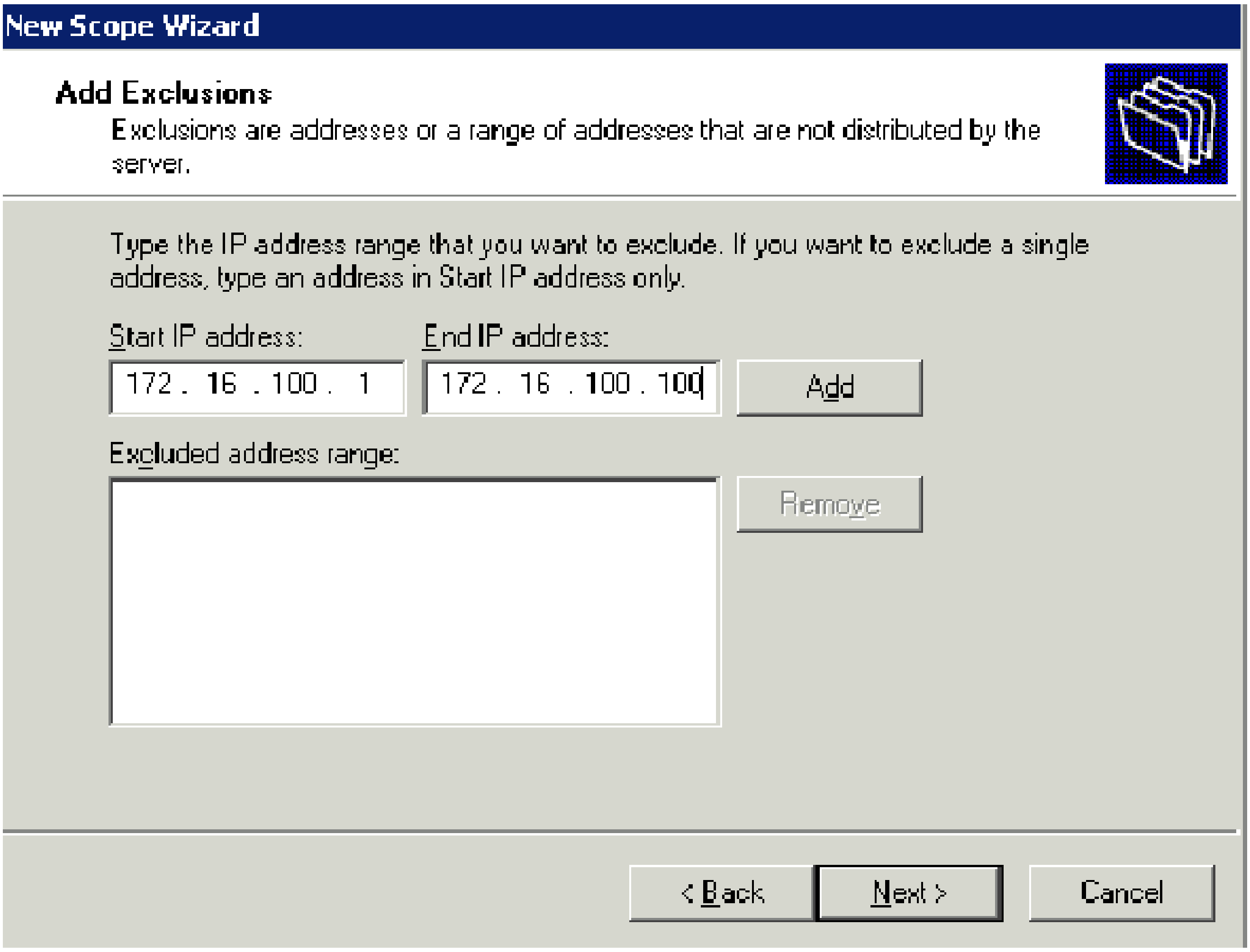
End IP address: 172 . 16 . 100 . 254

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: 24

Subnet mask: 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。



New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.

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.

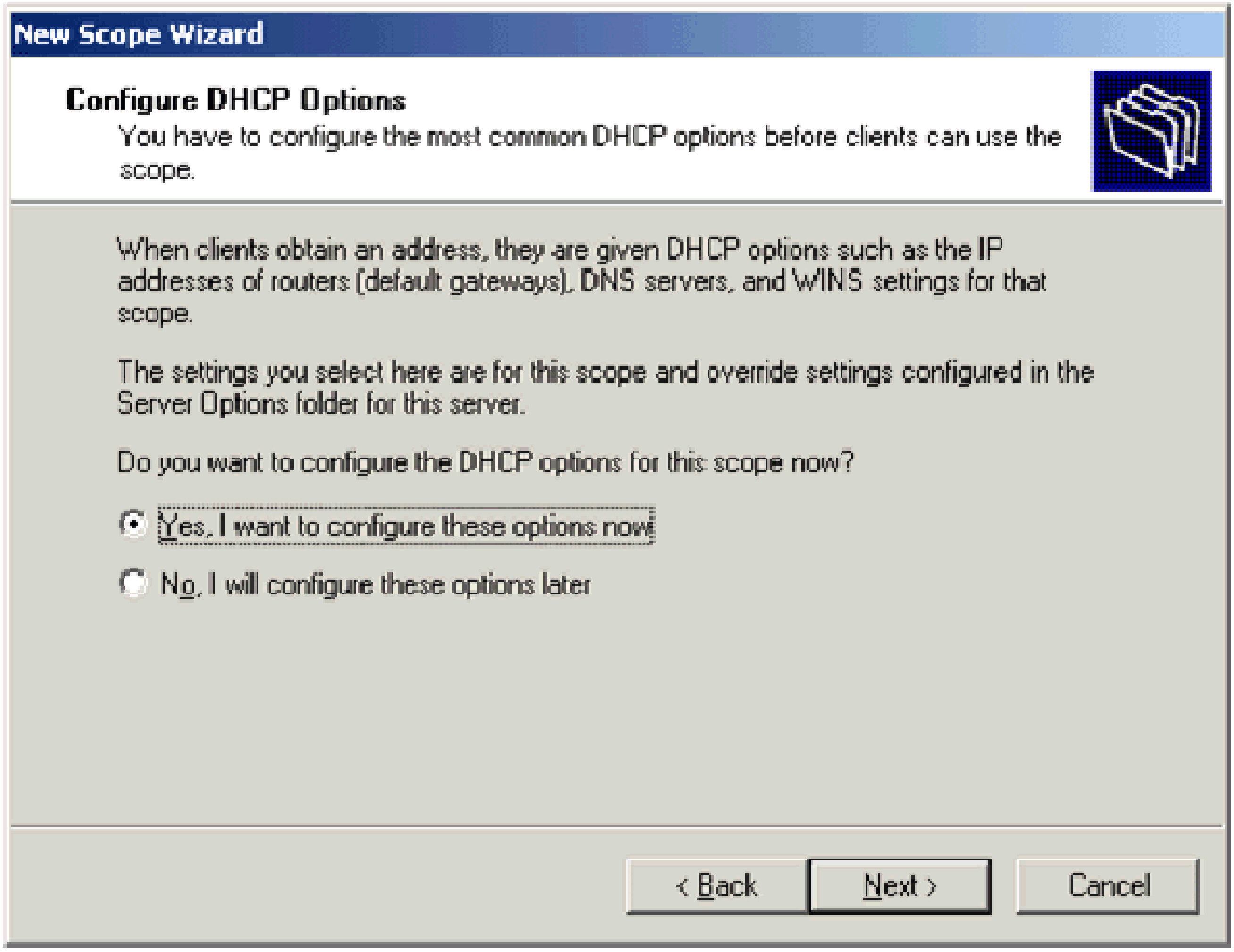
Start IP address: 172 . 16 . 100 . 1

End IP address: 172 . 16 . 100 . 100

Excluded address range:

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”。**



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.

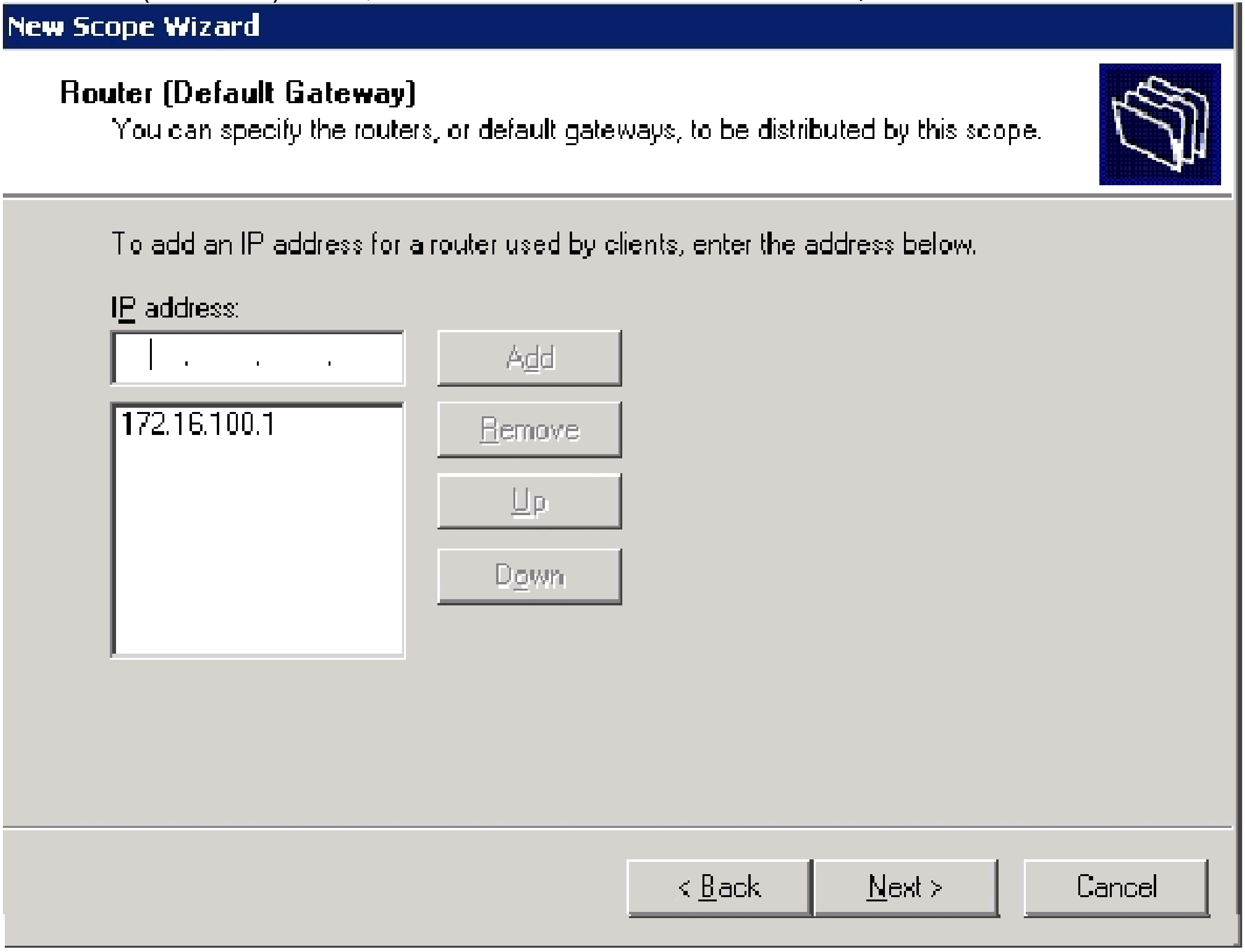
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

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

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”。**



New Scope Wizard

Router (Default Gateway)

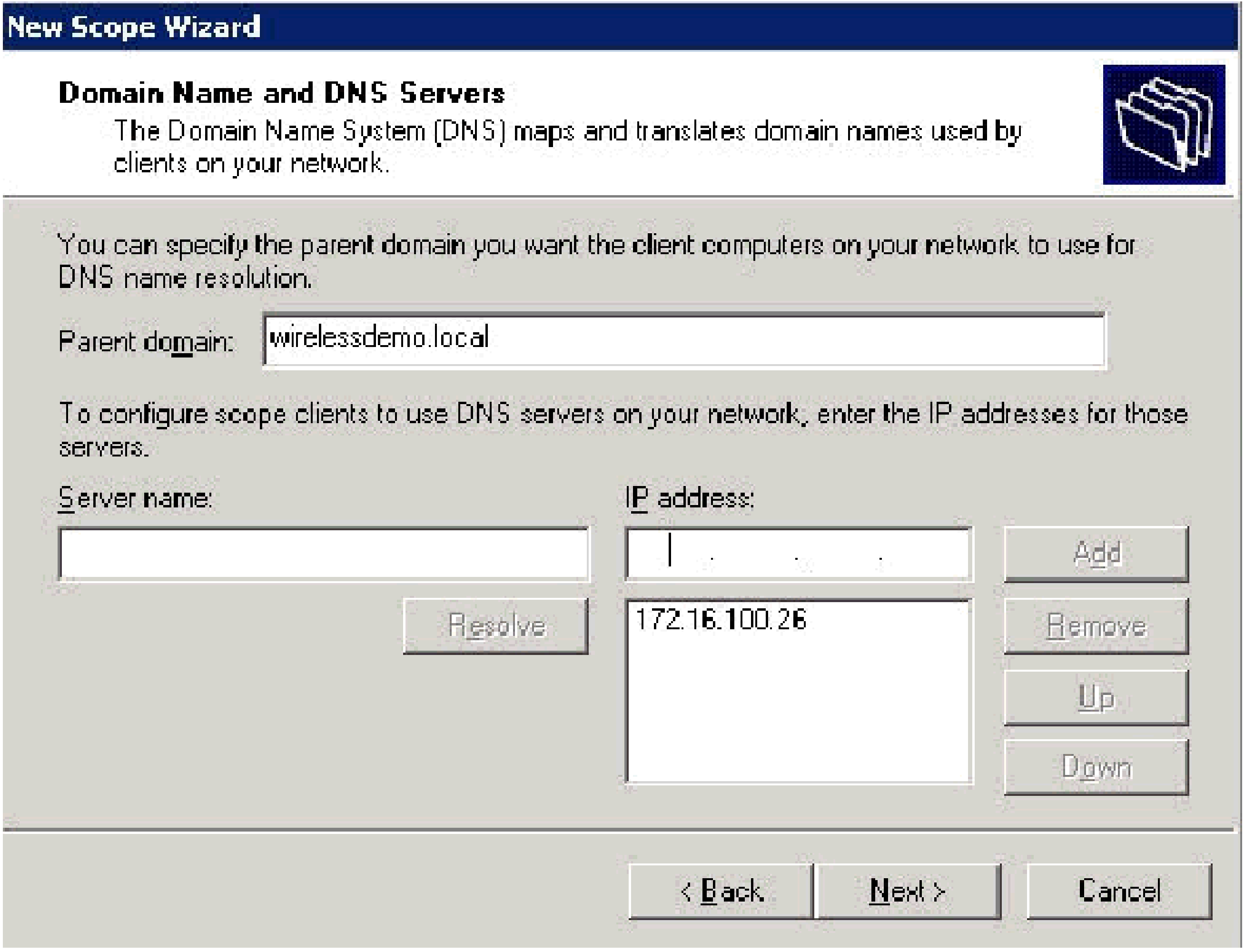
You can specify the routers, or default gateways, to be distributed by this scope.

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

IP address:

172.16.100.1

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”。**



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: wirelessdemo.local

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

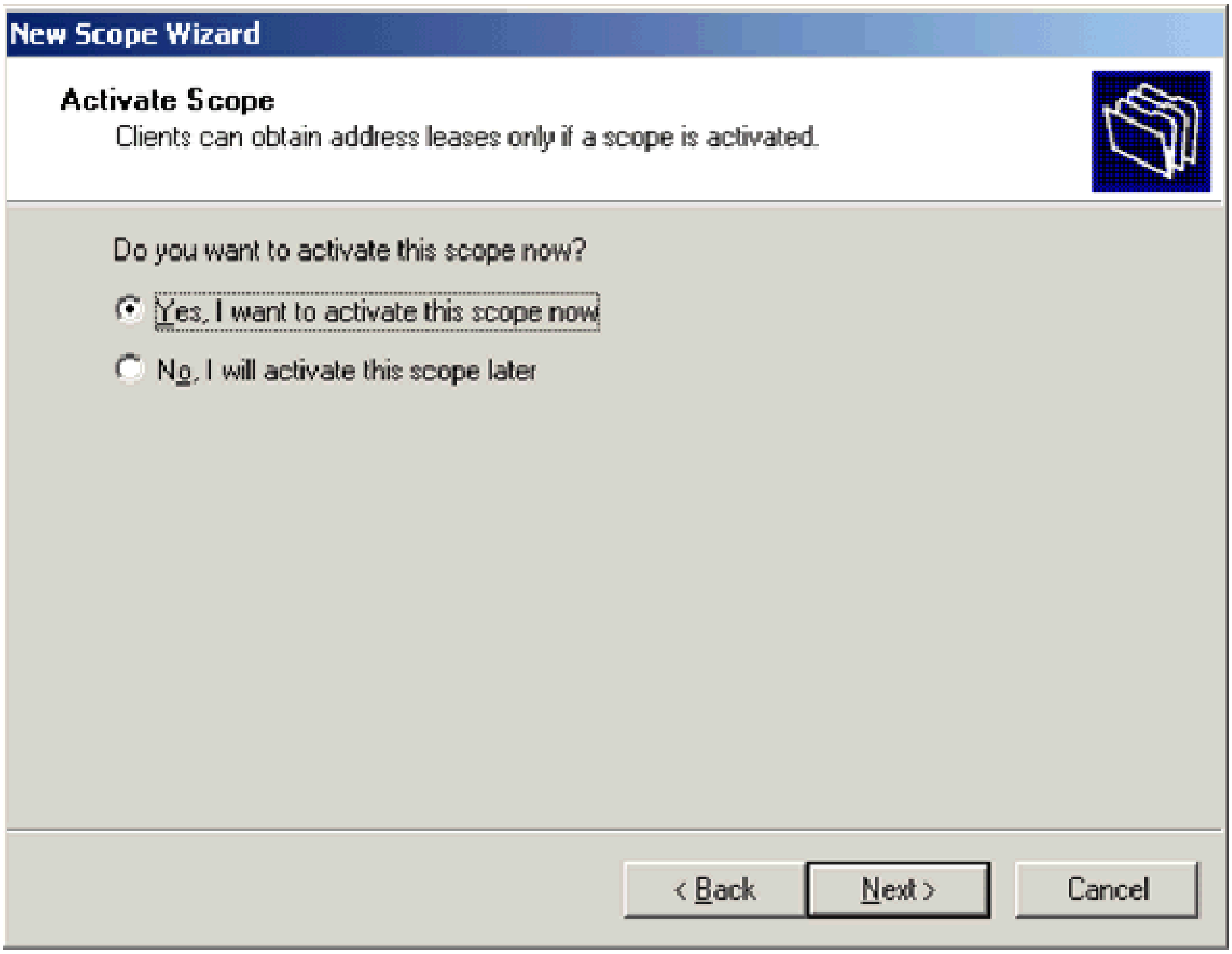
Server name:

IP address:

172.16.100.26

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”。**



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

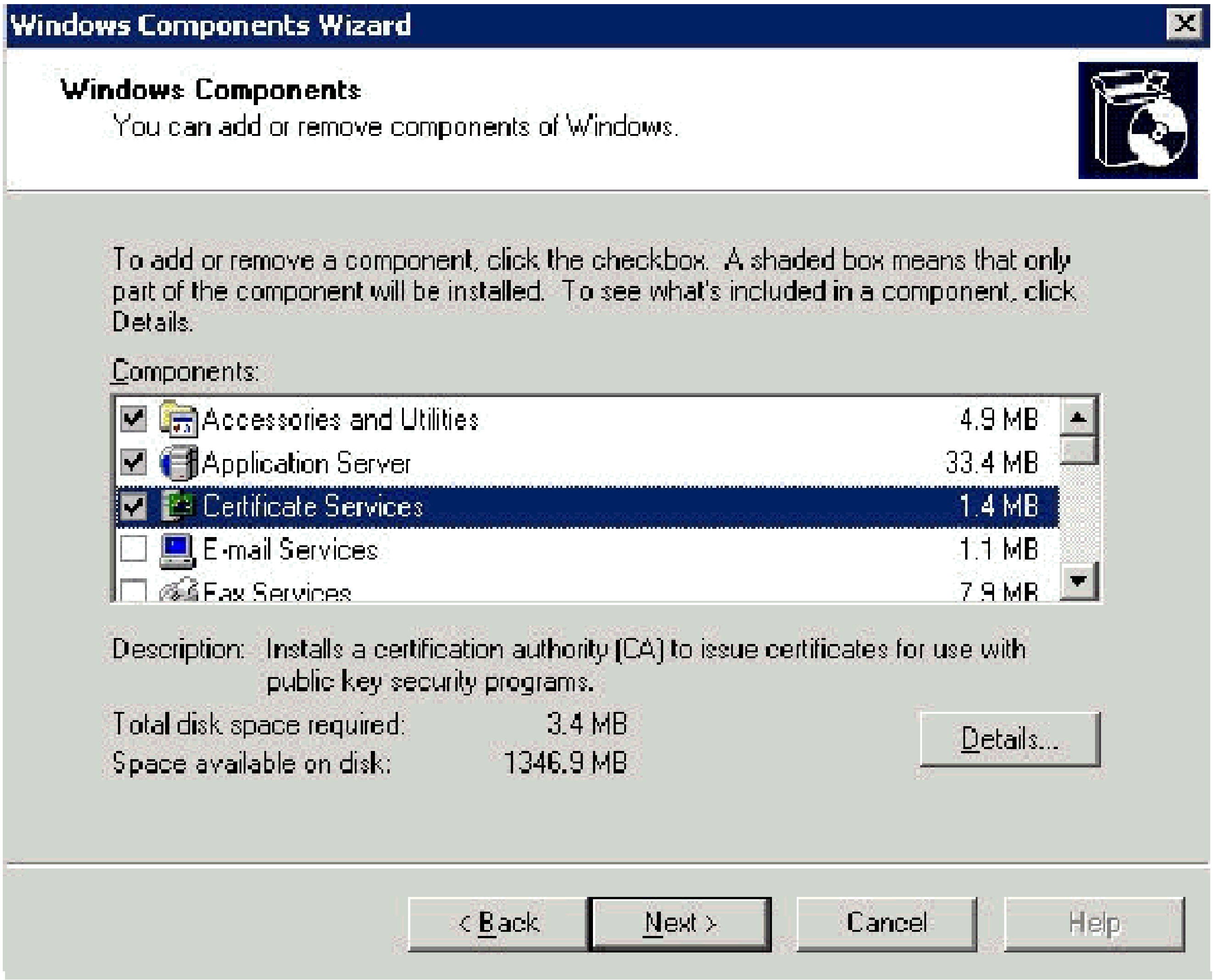
15. 在“完成新范围向导”页上，单击**完成。**

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”**。



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

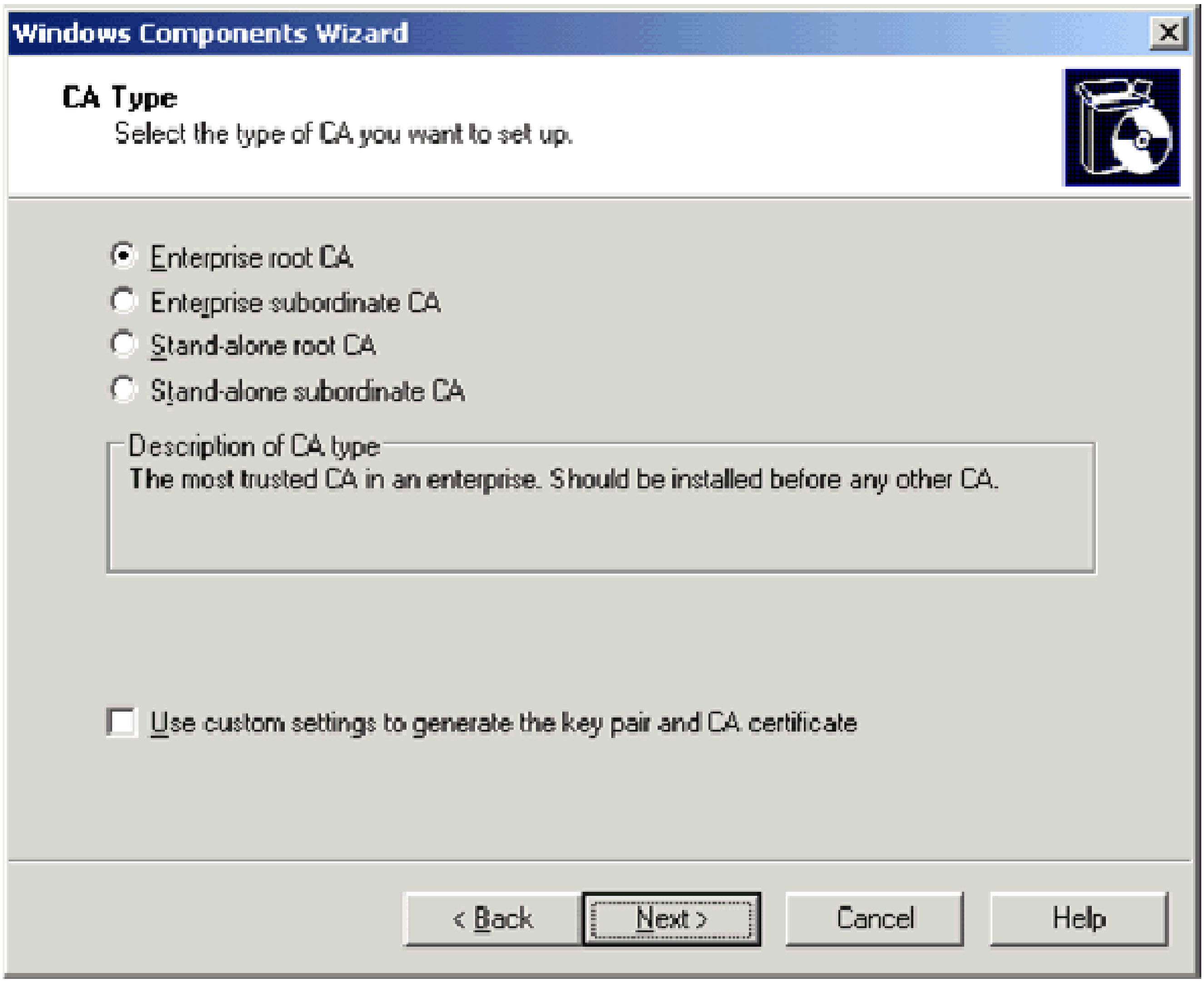
☑	Accessories and Utilities	4.9 MB
☑	Application Server	33.4 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	7.9 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 3.4 MB

Space available on disk: 1346.9 MB

3. 在“CA 类型”页上，选择**企业根 CA，然后单击“下一步”。**



Windows Components Wizard

CA Type

Select the type of CA you want to set up.

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

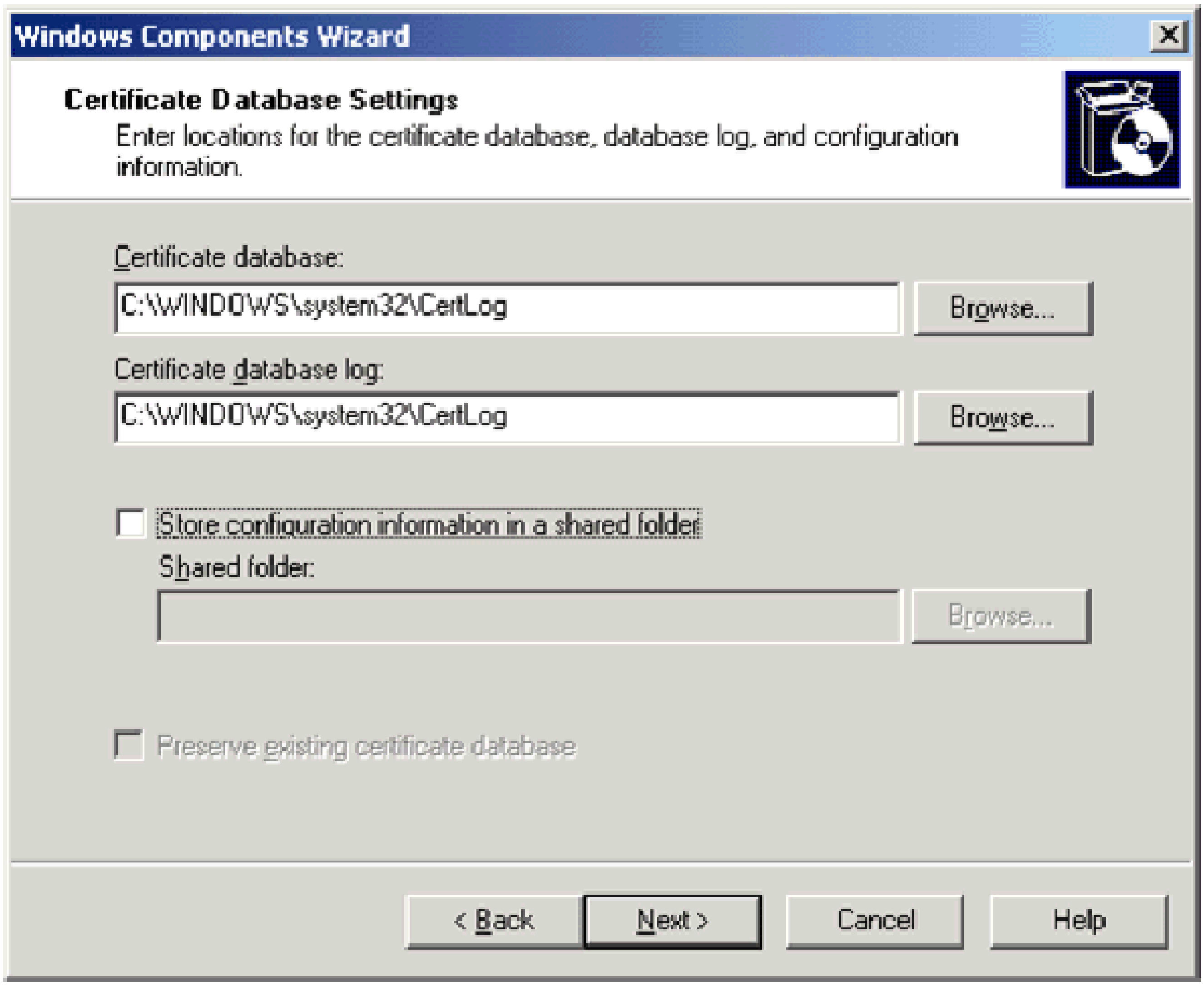
○ Stand-alone subordinate CA

Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

4. 在“CA识别信息”页面的“此CA的公用名”框中**键入wirelessdemoca。**您可以输入其他可选详细信息，然后单击“下**一步”**。接受Certificate Database Settings页面上的默认值。



Windows Components Wizard

Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database:
C:\WINDOWS\system32\CertLog

Certificate database log:
C:\WINDOWS\system32\CertLog

□ Store configuration information in a shared folder

Shared folder:

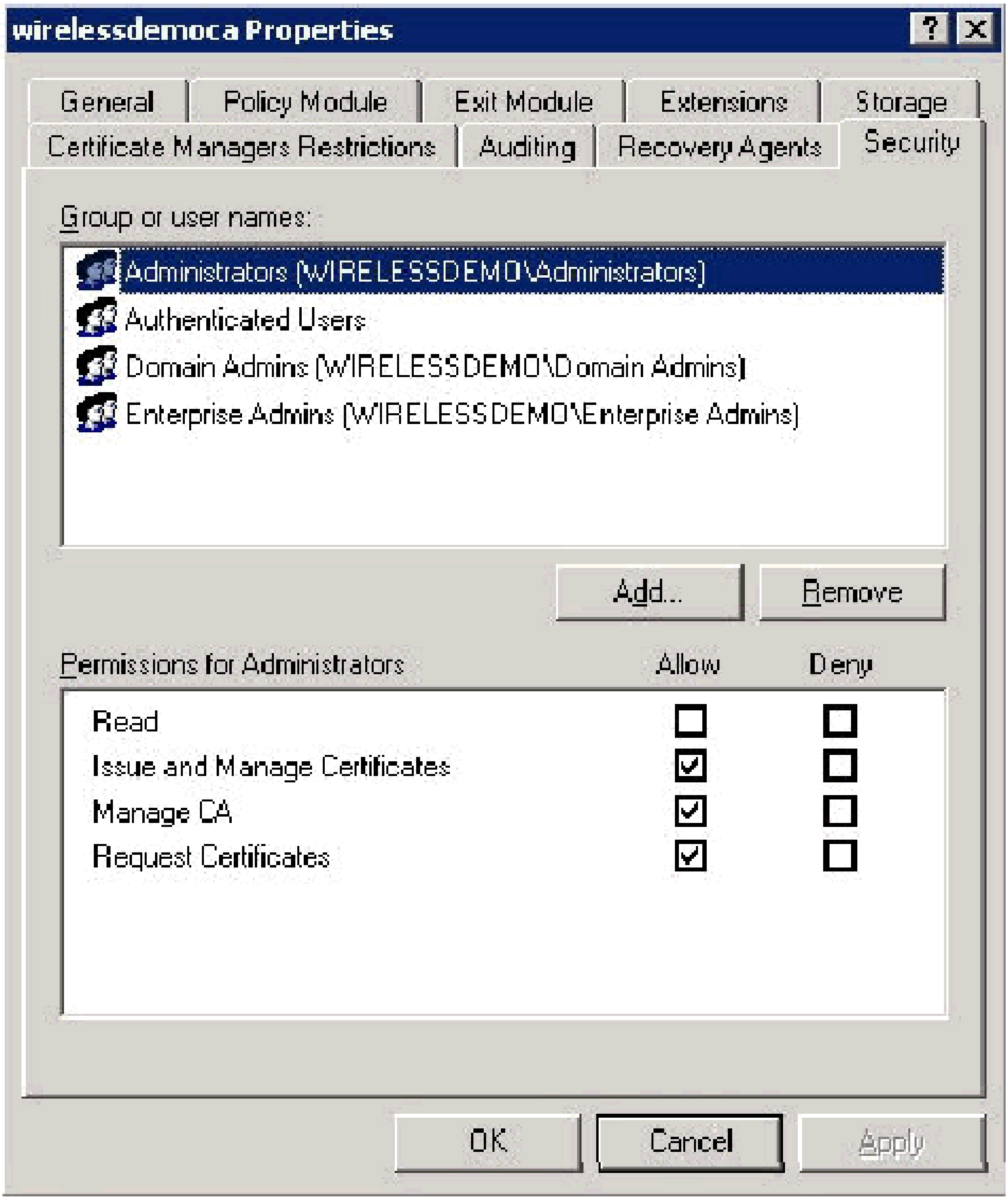
□ Preserve existing certificate database

5. 单击 **Next**。在安装完成时，单击**完成**。
6. 阅读有关安装IIS的警告后，单击**OK**。

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**。



Group or user names:

- Administrators (WIRELESSDEMO\Administrators)
- Authenticated Users
- Domain Admins (WIRELESSDEMO\Domain Admins)
- Enterprise Admins (WIRELESSDEMO\Enterprise Admins)

Permissions for Administrators	Allow	Deny
Read	□	□
Issue and Manage Certificates	☑	□
Manage CA	☑	□
Request Certificates	☑	□

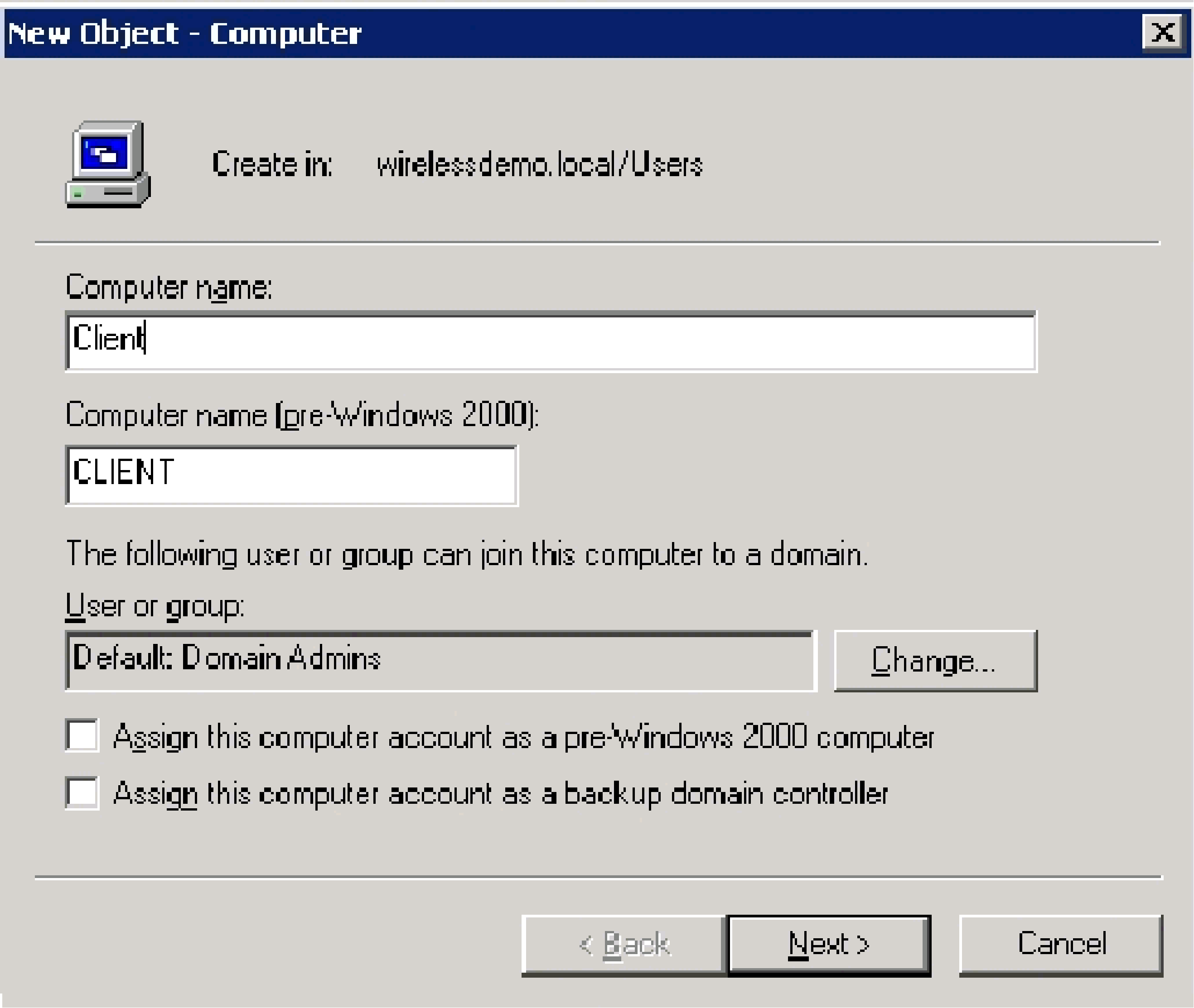
5. 单击**确定关闭“wirelessdemoca CA 属性”对话框，然后关闭“证书颁发机构”。**

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**。



Create in: wirelessdemo.local/Users

Computer name: Client

Computer name (pre-Windows 2000): CLIENT

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins [Change...]

□ Assign this computer account as a pre-Windows 2000 computer

□ Assign this computer account as a backup domain controller

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

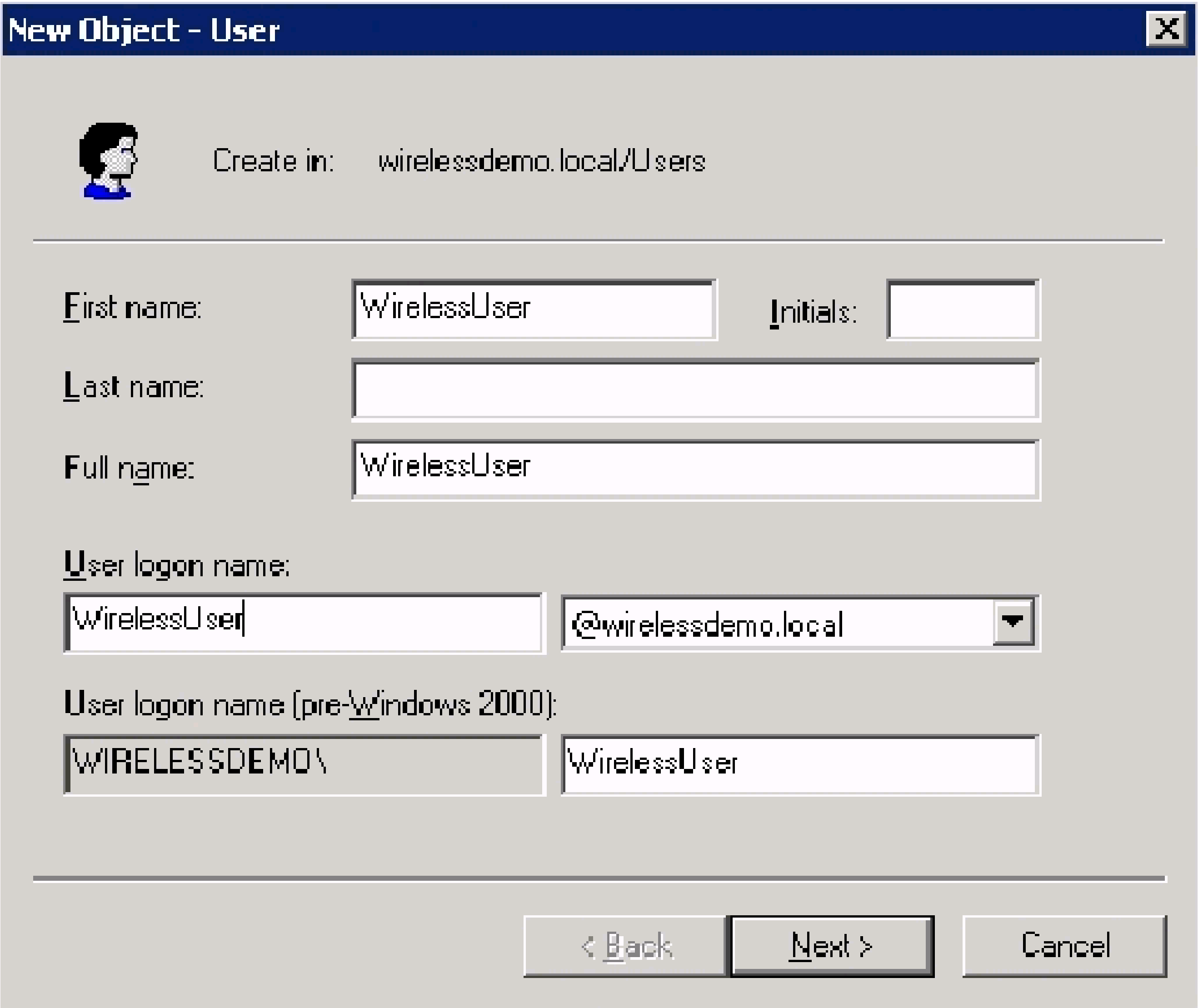
请完成以下步骤：

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。**此示例显示了在步骤7中添**加的**计算机CLIENT的过程。
2. 单击**属性**，然后转到“拨入”选项卡。
3. 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”对话框的“名字”字段中键入**WirelessUser**，然后在“用户登录名”字段中键入**WirelessUser**，然后单击**下一步**。



Create in: wirelessdemo.local/Users

First name: WirelessUser

Initials:

Last name:

Full name: WirelessUser

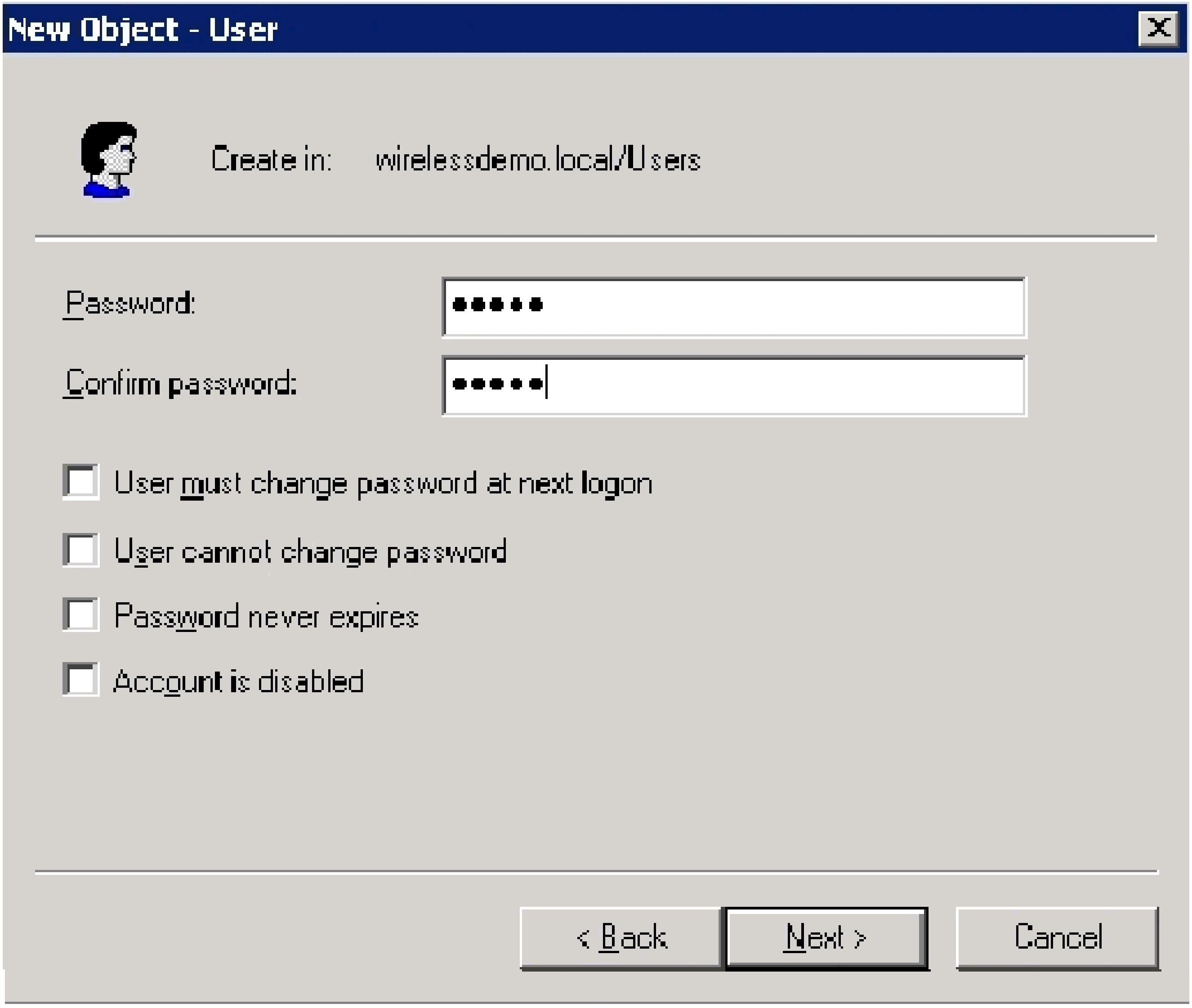
User logon name:

WirelessUser @wirelessdemo.local

User logon name (pre-Windows 2000):

WIRELESSDEMO\ WirelessUser

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

Create in: wirelessdemo.local/Users

Password: ●●●●●

Confirm password: ●●●●●

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

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

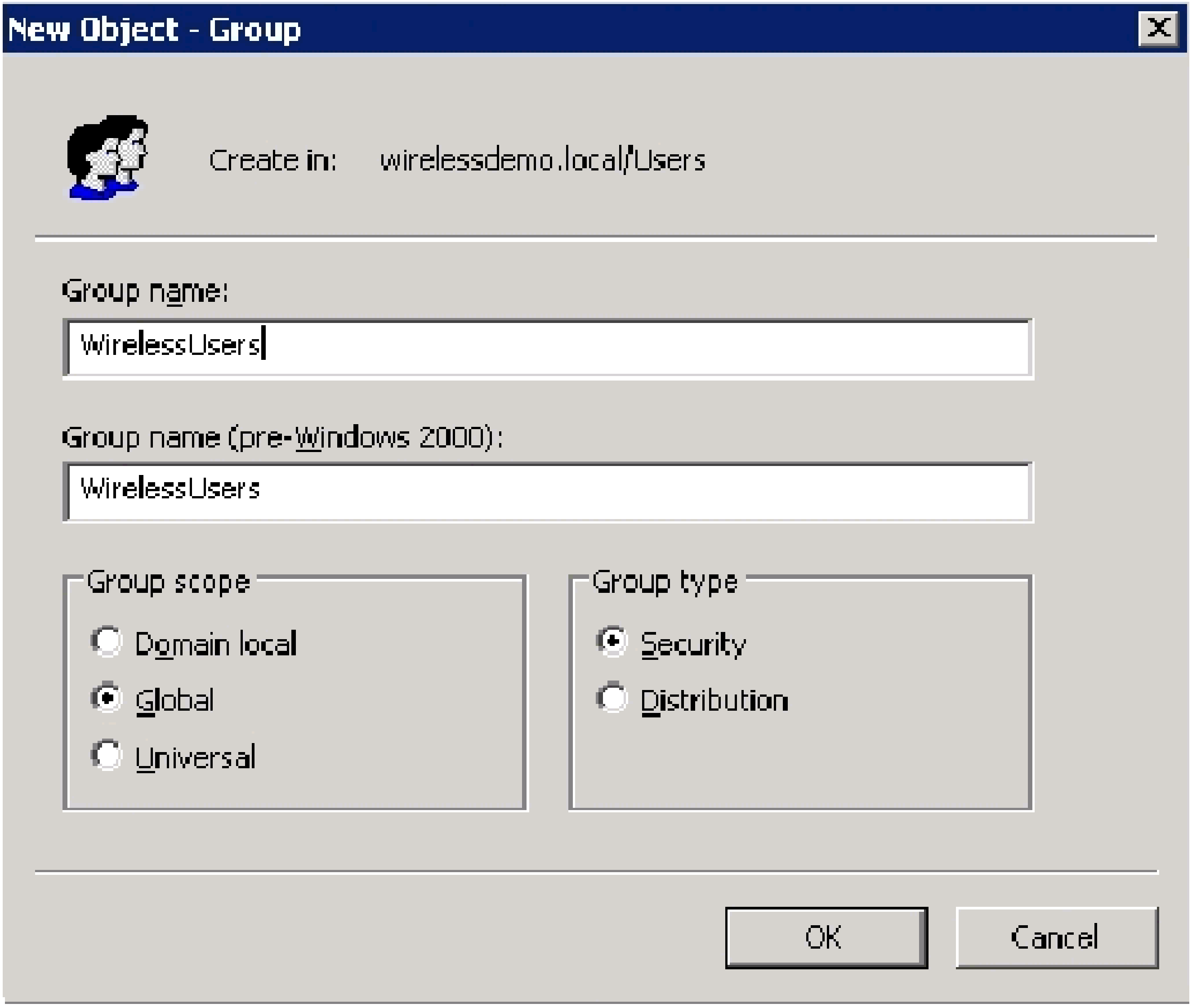
请完成以下步骤：

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**。



New Object - Group

Create in: wirelessdemo.local/Users

Group name:
WirelessUsers

Group name (pre-Windows 2000):
WirelessUsers

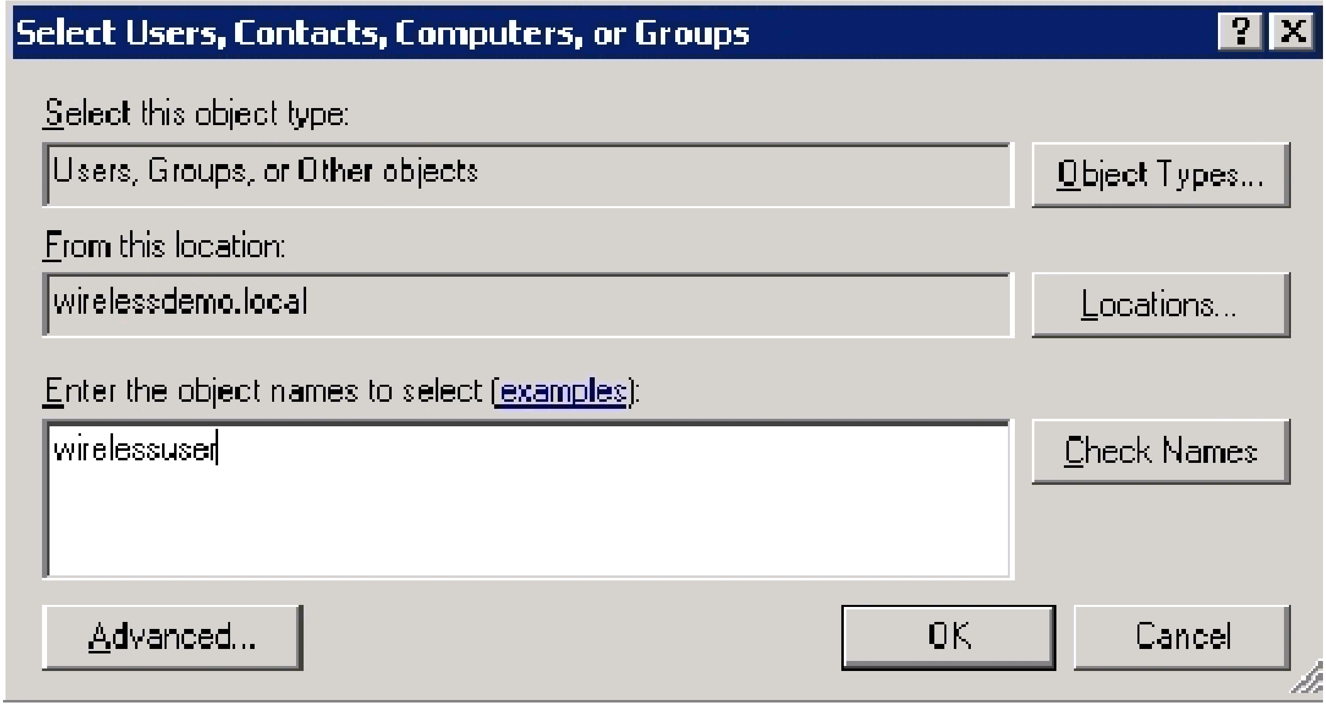
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

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.



Select this object type:

Users, Groups, or Other objects

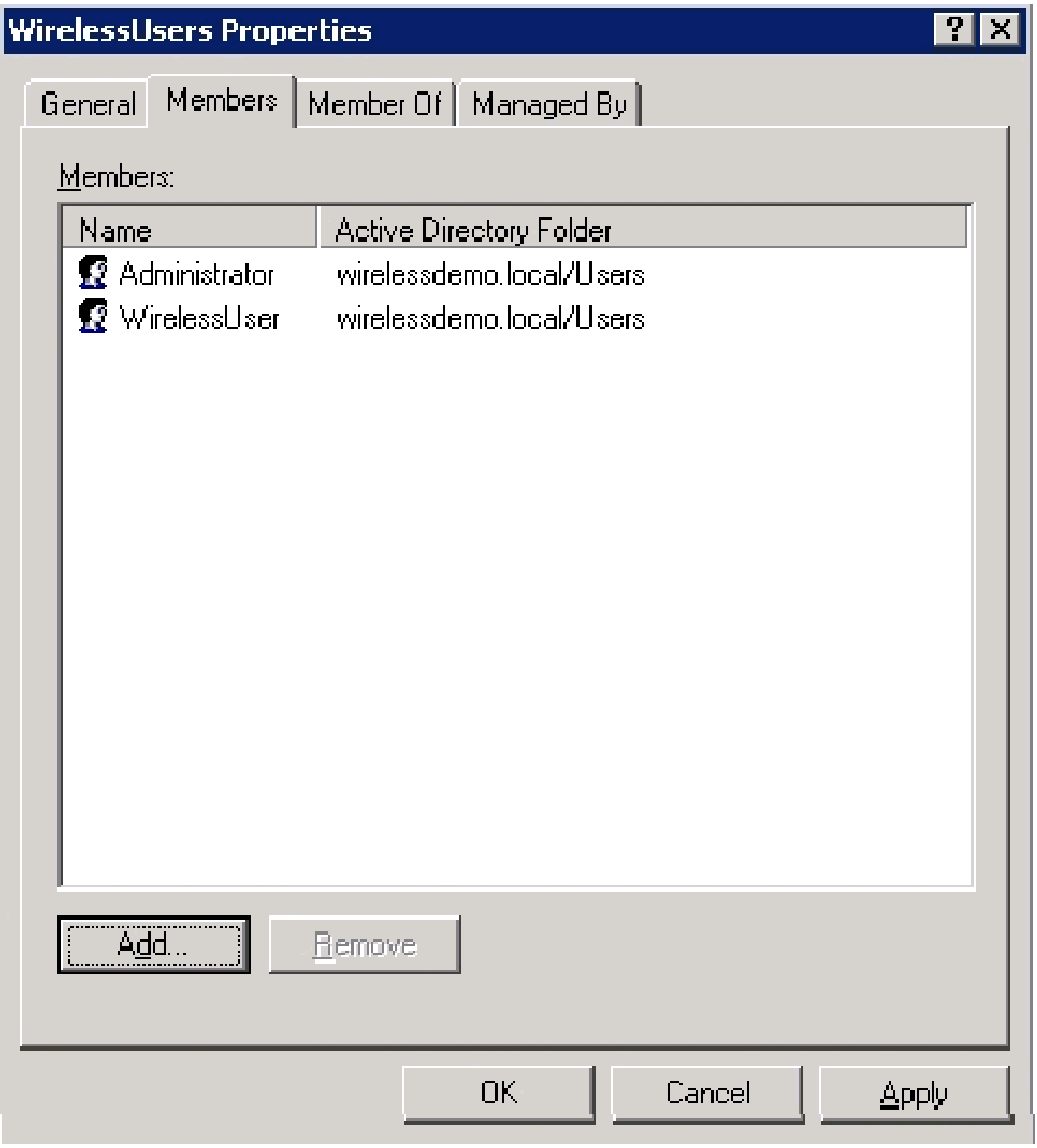
From this location:

wirelessdemo.local

Enter the object names to select (examples):

wirelessuser

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。

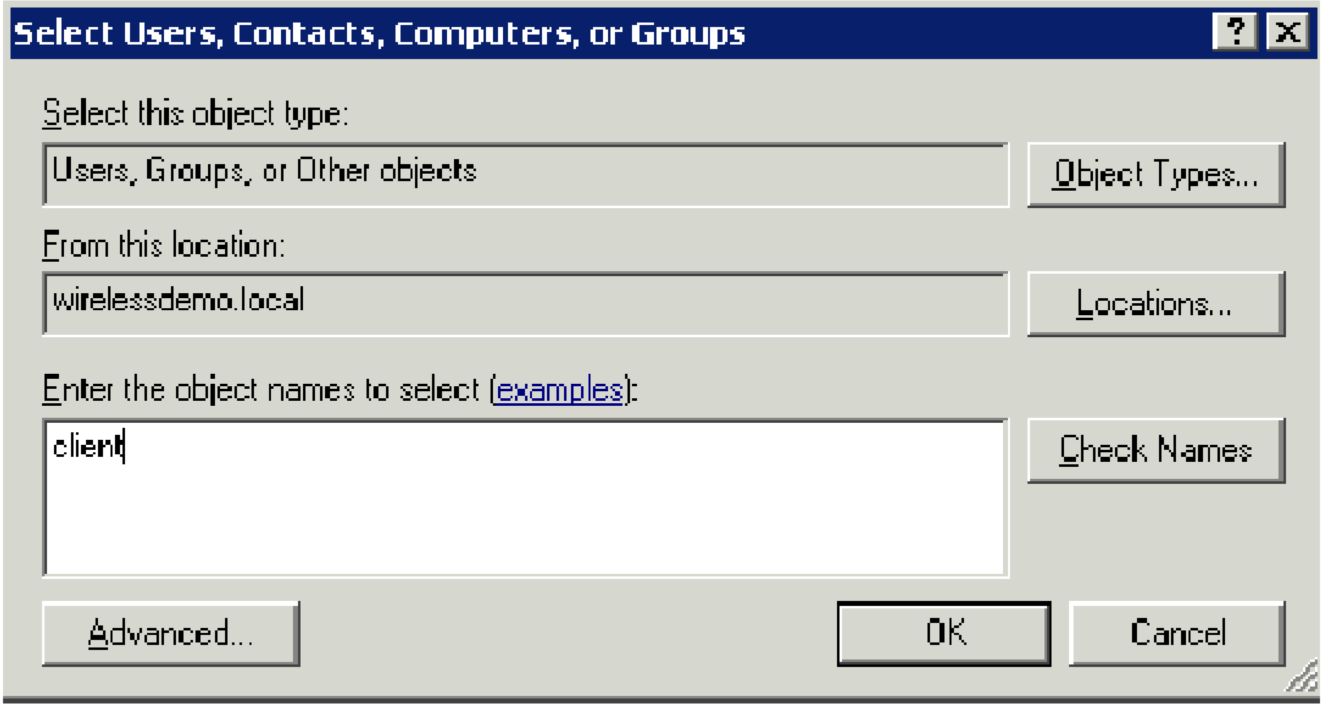


5. 单击**确定，以便保存对 WirelessUsers 组的更改。**
6. 重复此过程，向该组中添加更多用户。

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。**

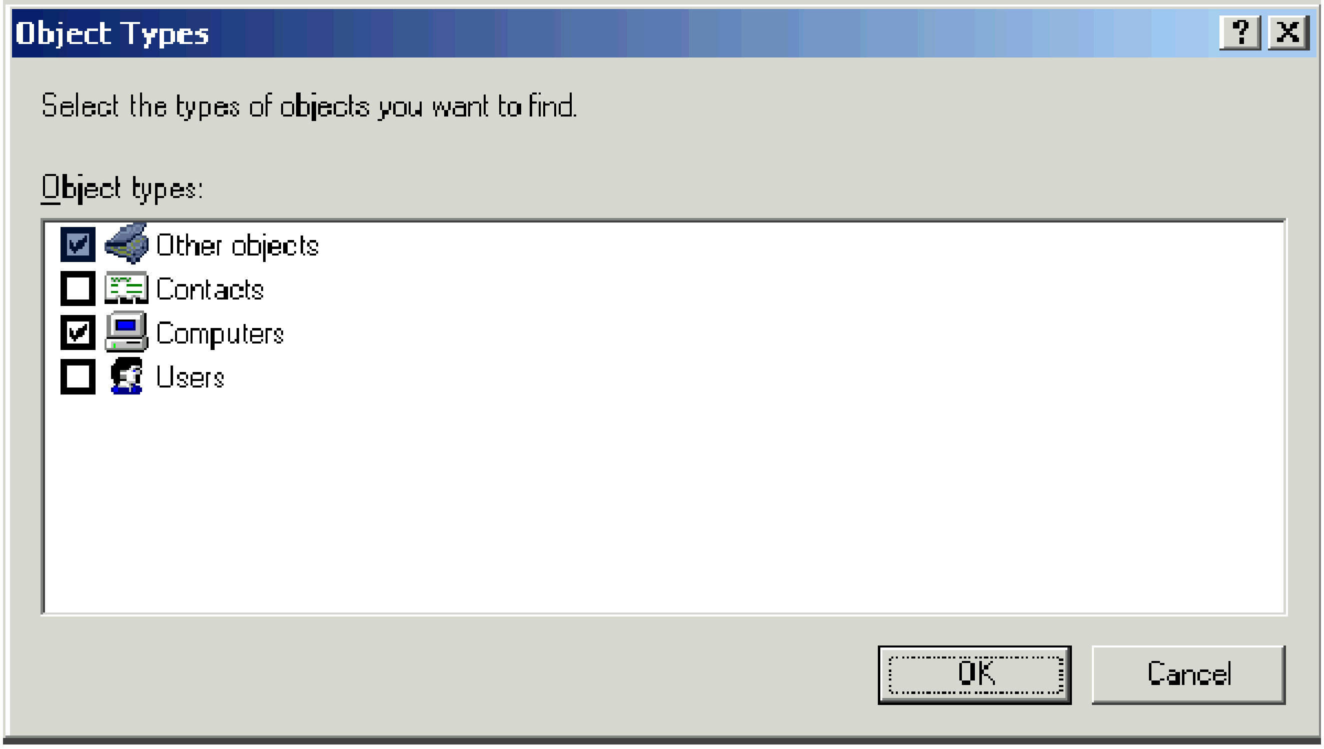


Select this object type: Users, Groups, or Other objects

From this location: wirelessdemo.local

Enter the object names to select (examples): client

3. 单击**对象类型**，清除“用户”复选框，然后选中“计算机”。



Select the types of objects you want to find.

Object types:

- ☑ Other objects
- □ Contacts
- ☑ Computers
- □ Users

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，登录名为ACS的计算机到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)等产品执行的远程安装不会经过测试，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”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**，此复选框适用于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不会拨入网络访问服务器。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。**从要执行的脚本列表中，选择在身份验证服务失败时要应用的选项：**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。单击 **Next**。
27. 安装程序就会完成安装，并显示“Cisco Secure ACS Service Initiation”对话框。
28. 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。**
29. 单击 **Next**。
30. 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。
31. 单击 **完成**。**注意：**其余配置记录在配置的EAP类型的一节下。

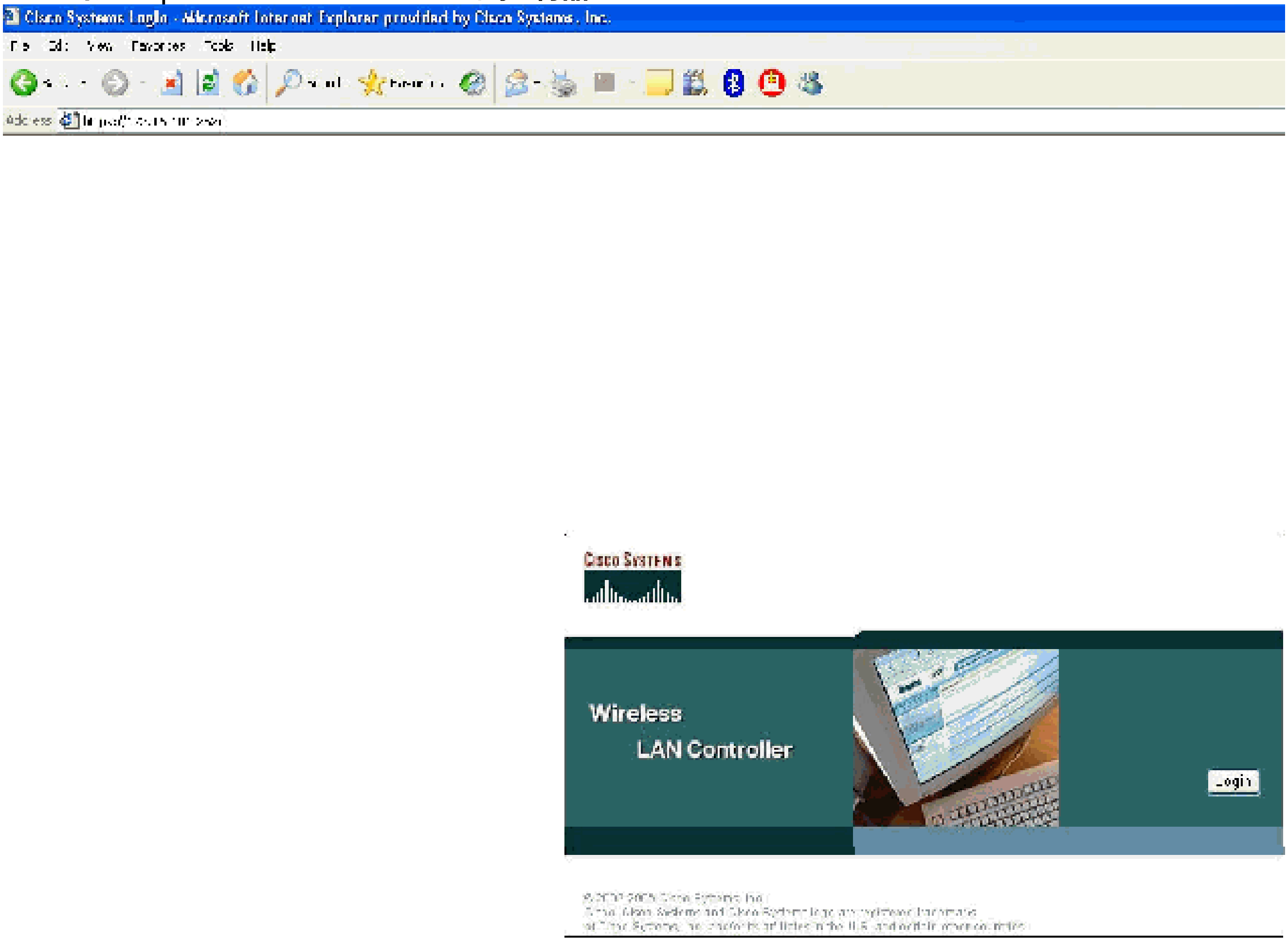
Cisco LWAPP 控制器配置

为WPA2/WPA创建必要配置

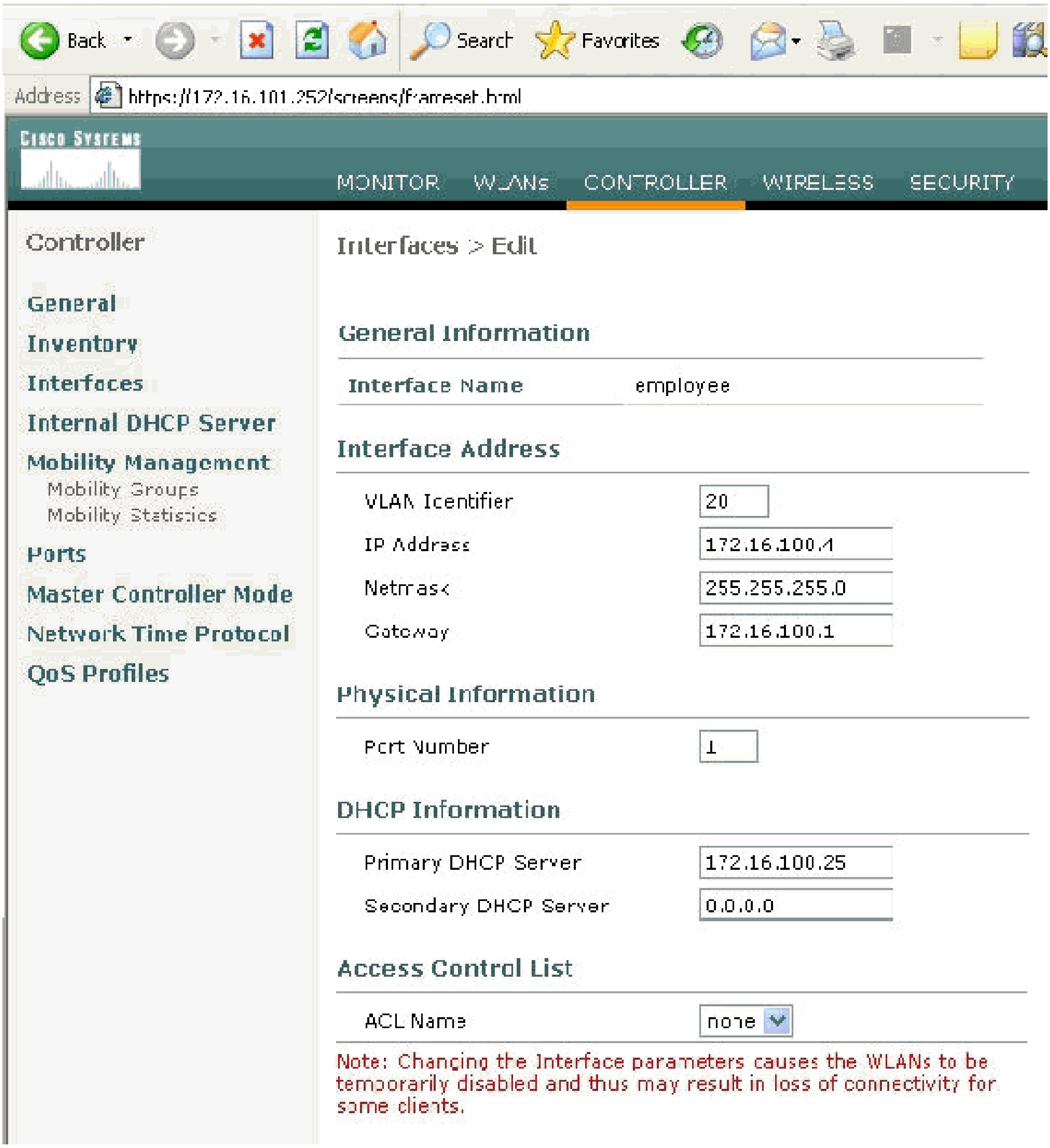
请完成以下步骤：

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. 通过浏览https://172.16.101.252登录**控制器**。


Cisco Systems Login - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address https://172.16.101.252
Cisco Systems
Wireless
LAN Controller
Login

2. 单击 **Login**。
3. 用默认用户 **admin 和默认密码 admin 进行登录。**
4. 在Controller菜单下创建接口VLAN映射。
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。



Interfaces > Edit

General Information

Interface Name	employee

Interface Address

VLAN Identifier	20
IP Address	172.16.100.4
Netmask	255.255.255.0
Gateway	172.16.100.1

Physical Information

Port Number	1

DHCP Information

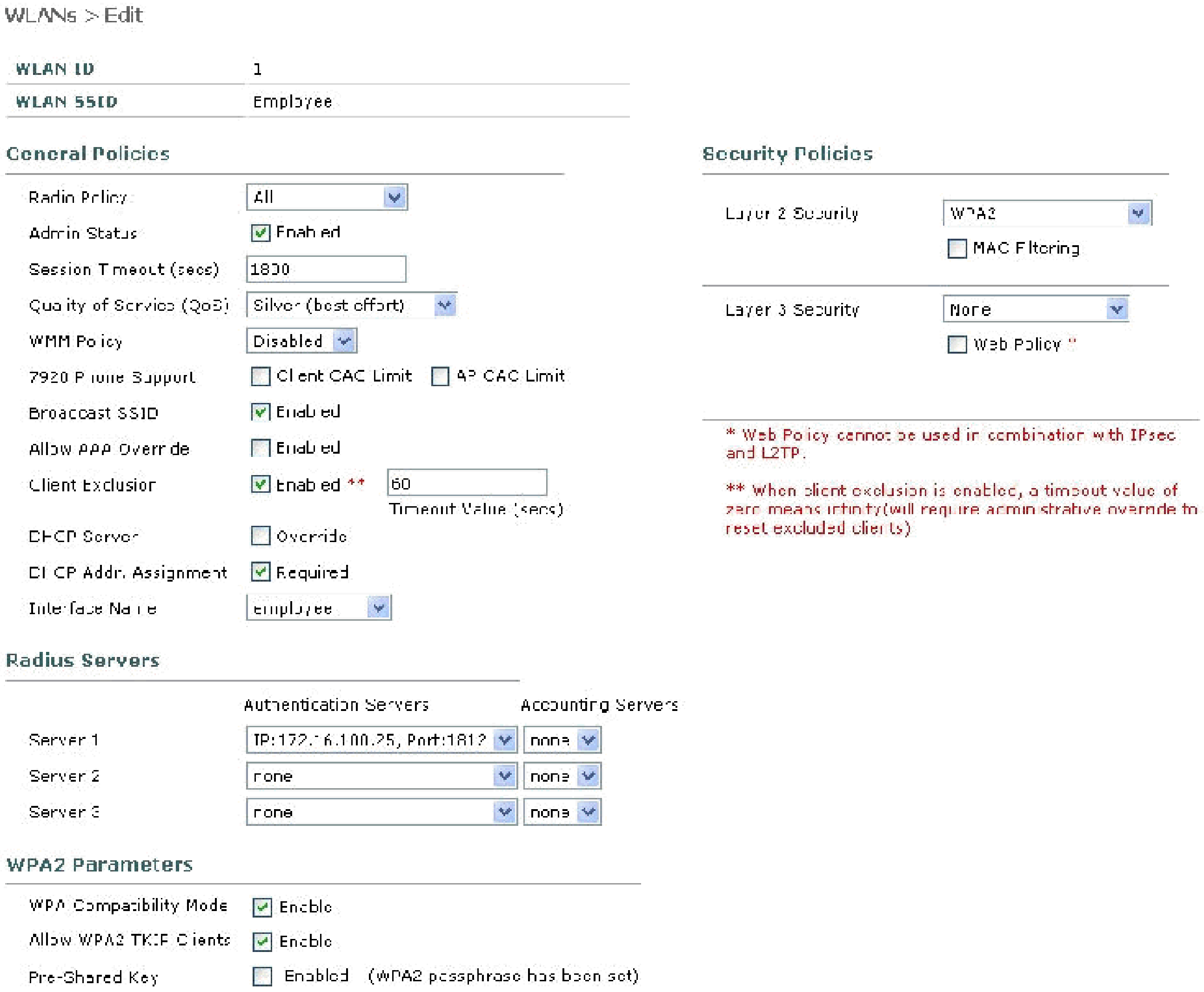
Primary DHCP Server	172.16.100.25
Secondary DHCP Server	0.0.0.0

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. 单击 **Apply**。
12. 单击**WLAN**。
13. 单击 **New**。
14. 在WLAN SSID字段中，键入**Employee**。
15. 单击 **Apply**。
16. 如此WLANs > Edit窗口所示配置信息。**注意：**WPA2是本实验选择的第2层加密方法。为了允许具有TKIP-MIC客户端的WPA与此SSID关联，您还可以选中**WPA兼容模式**和**允许WPA2 TKIP客户端**或不支持802.11i AES加密方法的客户端。



WLANs > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Allow AAA Override	□ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	☑ Required
Interface Name	employee

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

WPA2 Parameters

WPA Compatibility Mode	☑ Enable
Allow WPA2 TKIP Clients	☑ Enable
Pre-Shared Key	□ Enabled (WPA2 passphrase has been set)

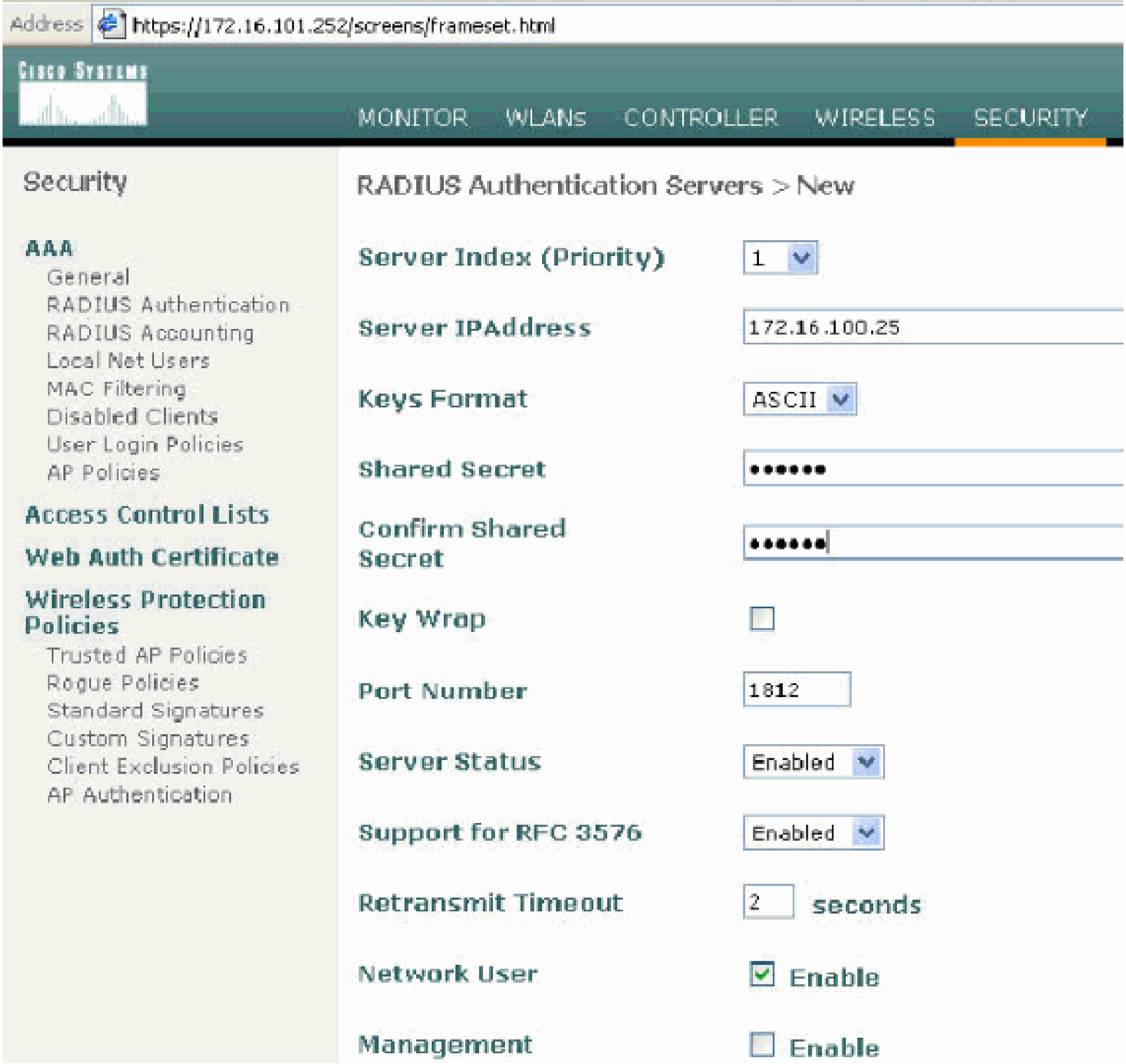
Security Policies

Layer 2 Security	WPA2 □ MAC Filtering
Layer 3 Security	None □ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

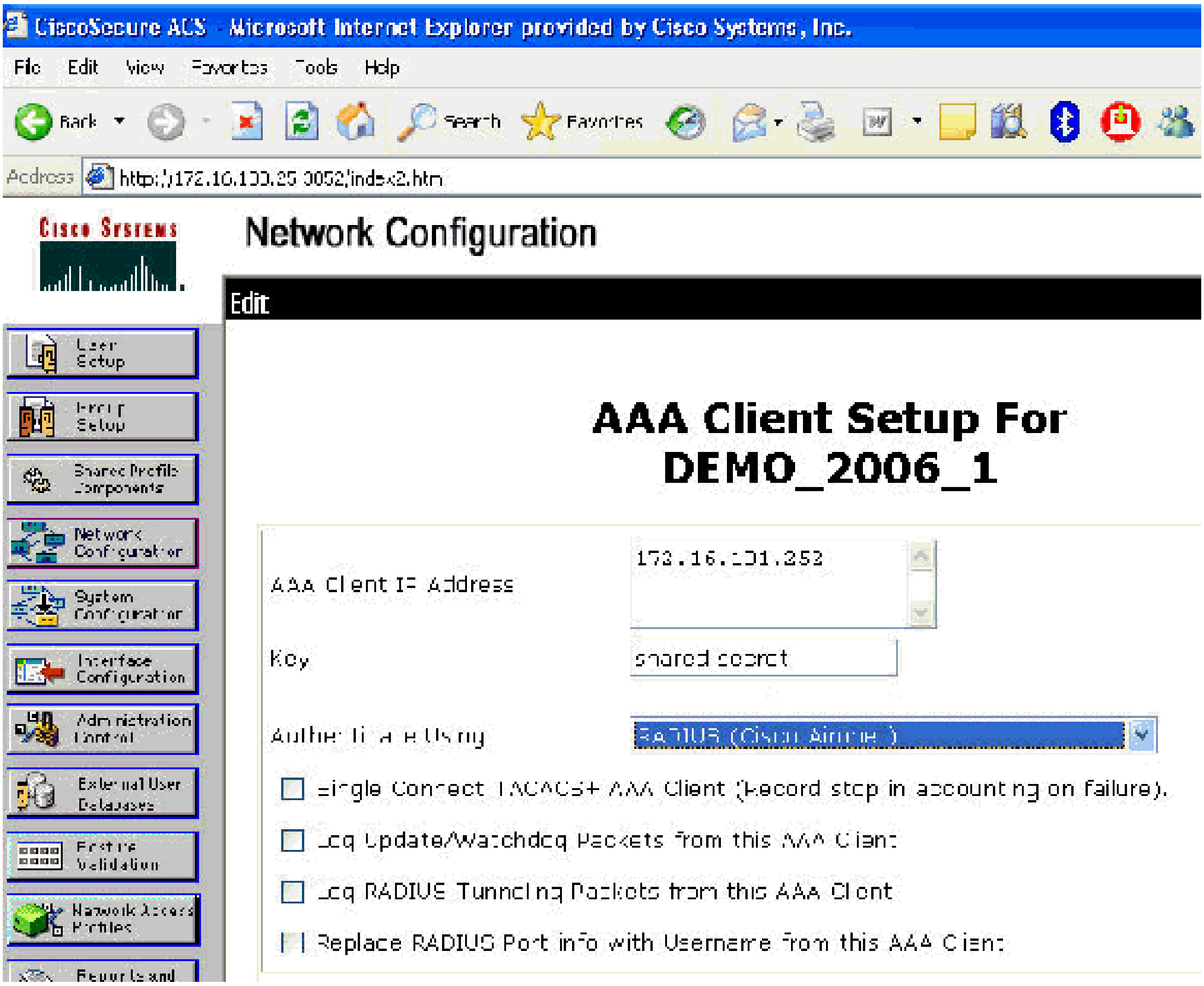
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

17. 单击 **Apply**。
18. 单击**Security**菜单并添加RADIUS服务器。
19. 单击 **New**。
20. 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。
21. 确保共享密钥与 ACS 服务器中配置的 AAA 客户端相匹配。
22. 单击 **Apply**。



RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IPAddress	172.16.100.25
Keys Format	ASCII
Shared Secret	••••••
Confirm Shared Secret	••••••
Key Wrap	□
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	☑ Enable
Management	□ Enable



Network Configuration

Edit

AAA Client Setup For DEMO_2006_1

AAA Client IP Address: 172.16.101.252

Key: shared secret

Authenticate Using: RADIUS (Cisco Aironet)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

23. 基本配置现在已完成，您可以开始测试EAP-TLS。

EAP-TLS身份验证

EAP-TLS身份验证要求无线客户端上的计算机和用户证书，将EAP-TLS作为EAP类型添加到远程访问策略以进行无线访问，以及重新配置无线网络连接。

要配置DC_CA以为计算机和用户证书提供自动注册，请完成本节中的步骤。

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。

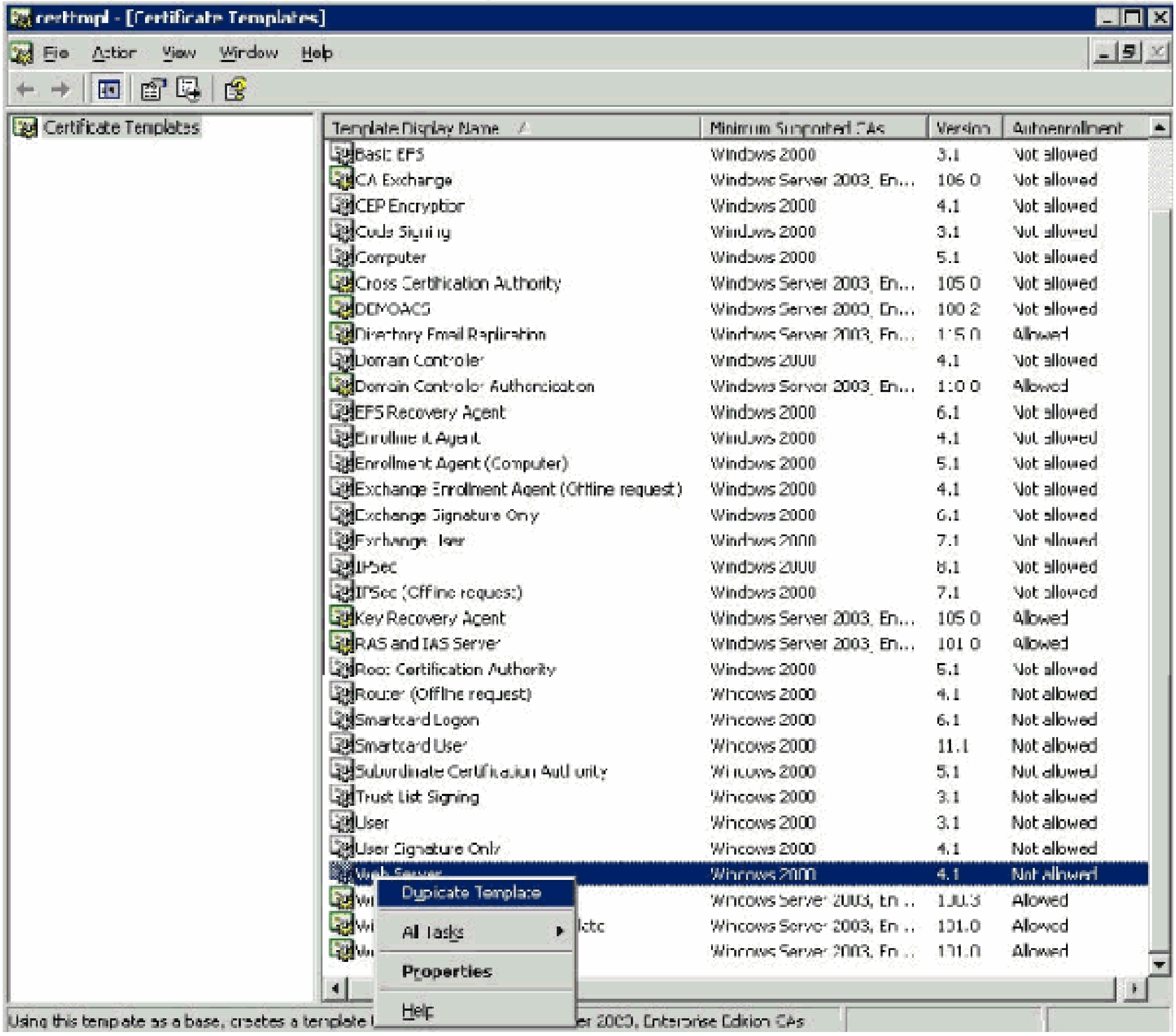
注意：Windows 2000允许导出密钥，如果使用Windows 2000，则无需遵循这些步骤。

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。**



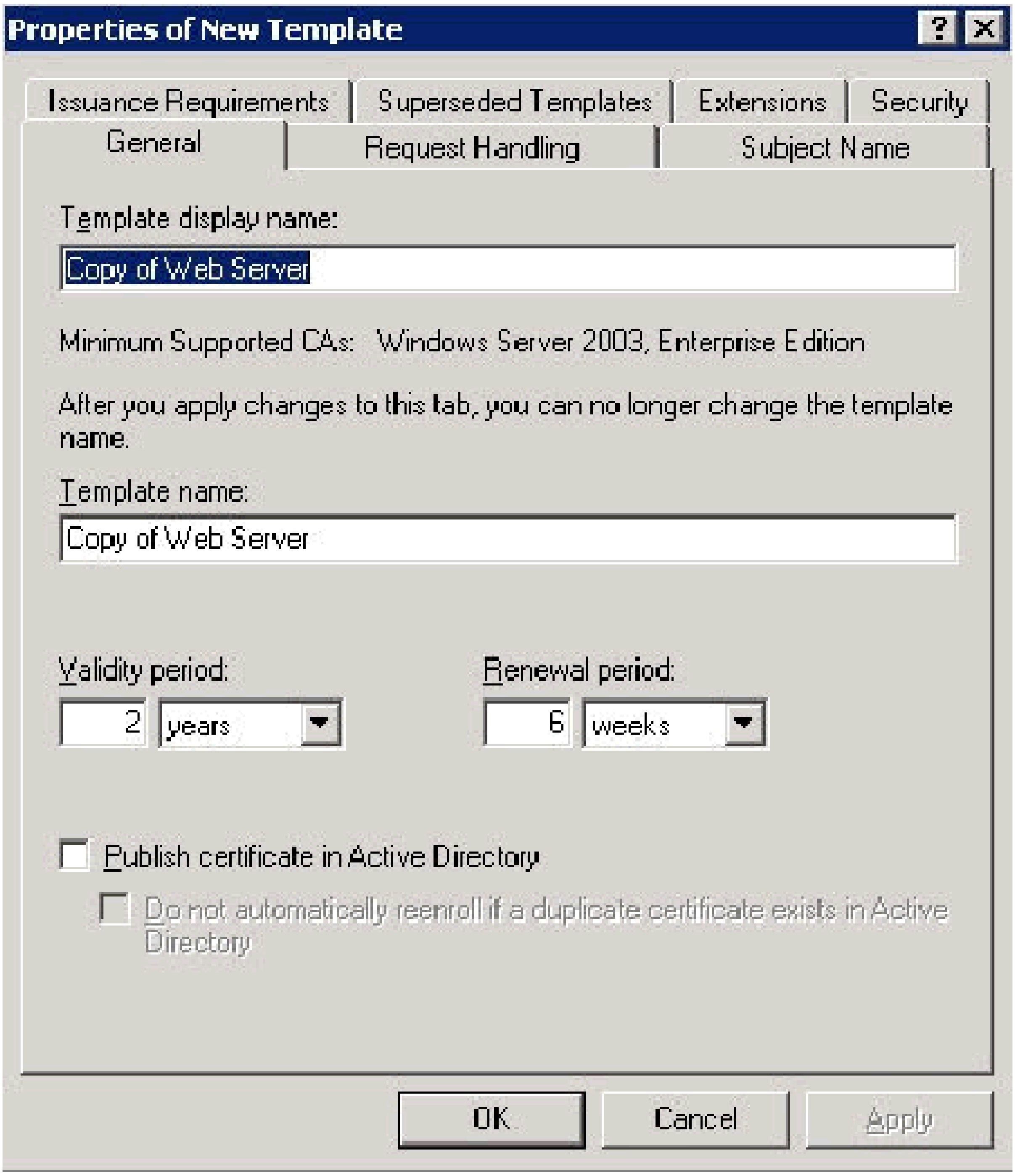
Template Display Name	Minimum Supported CAs	Version	Autoenrollment
Basic EFS	Windows 2000	3.1	Not allowed
CA Exchange	Windows Server 2003, En...	106.0	Not allowed
CEP Encryption	Windows 2000	4.1	Not allowed
Code Signing	Windows 2000	3.1	Not allowed
Computer	Windows 2000	5.1	Not allowed
Cross Certification Authority	Windows Server 2003, En...	105.0	Not allowed
DEMOACS	Windows Server 2003, En...	100.2	Not allowed
Directory Email Replication	Windows Server 2003, En...	115.0	Allowed
Domain Controller	Windows 2000	4.1	Not allowed
Domain Controller Authentication	Windows Server 2003, En...	110.0	Allowed
EFS Recovery Agent	Windows 2000	6.1	Not allowed
Enrollment Agent	Windows 2000	4.1	Not allowed
Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed
Exchange Signature Only	Windows 2000	6.1	Not allowed
Exchange User	Windows 2000	7.1	Not allowed
IPSec	Windows 2000	8.1	Not allowed
IPSec (Offline request)	Windows 2000	7.1	Not allowed
Key Recovery Agent	Windows Server 2003, En...	105.0	Allowed
RAS and IAS Server	Windows Server 2003, En...	101.0	Allowed
Root Certification Authority	Windows 2000	5.1	Not allowed
Router (Offline request)	Windows 2000	4.1	Not allowed
Smartcard Logon	Windows 2000	6.1	Not allowed
Smartcard User	Windows 2000	11.1	Not allowed
Subordinate Certification Authority	Windows 2000	5.1	Not allowed
Trust List Signing	Windows 2000	3.1	Not allowed
User	Windows 2000	3.1	Not allowed
User Signature Only	Windows 2000	4.1	Not allowed
Web Server	Windows 2000	4.1	Not allowed
Wi	Windows Server 2003, En...	100.3	Allowed
Wi ... tatio	Windows Server 2003, En...	101.0	Allowed
Wi	Windows Server 2003, En...	101.0	Allowed

Using this template as a base, creates a template t... er 2003, Enterprise Edition CAs

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**。



Properties of New Template

Template display name:

Copy of Web Server

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:

Copy of Web Server

Validity period:

2 years

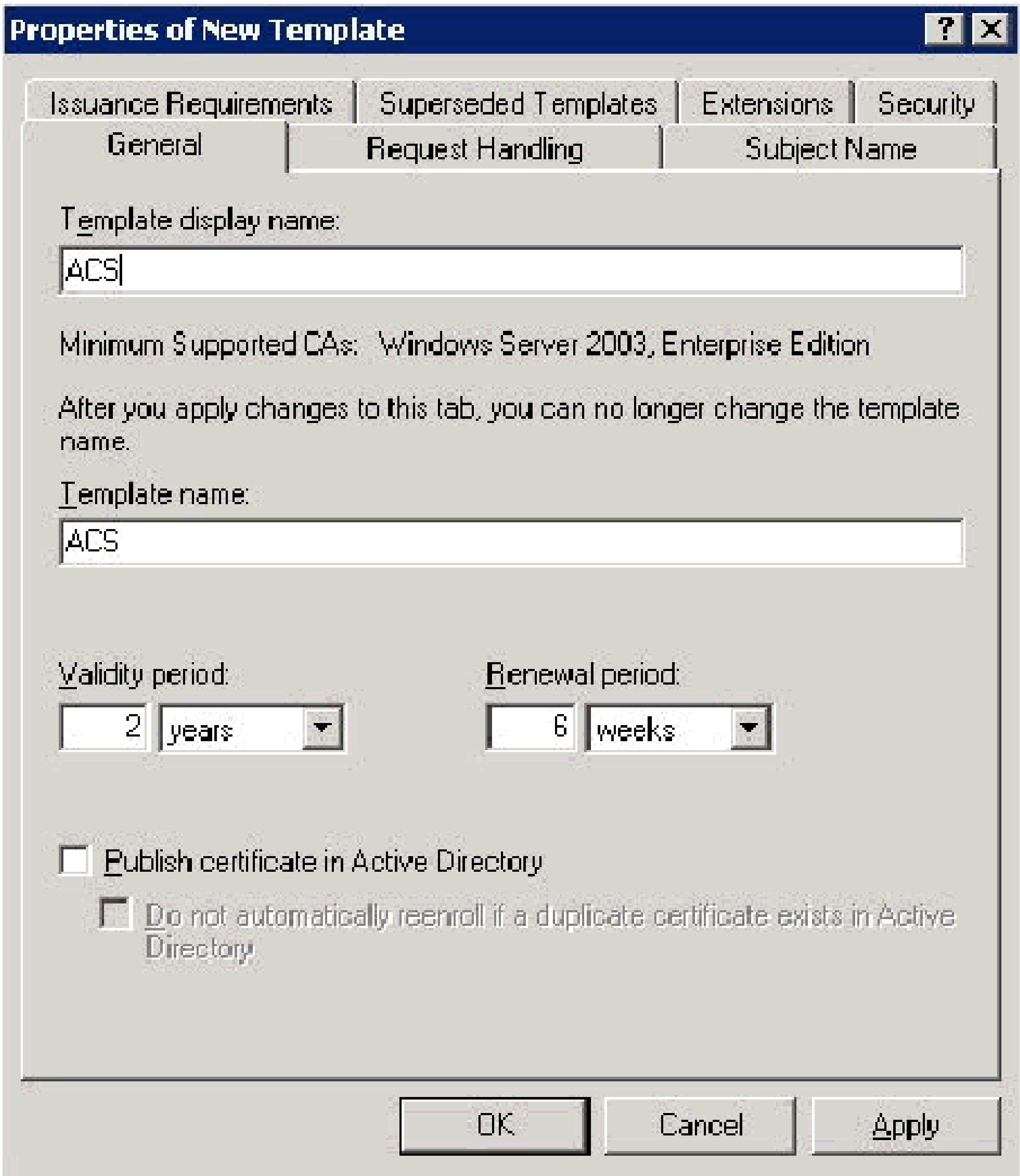
Renewal period:

6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

3. 在“模板显示名称”字段中，键入 **ACS**。



Template display name: ACS

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: ACS

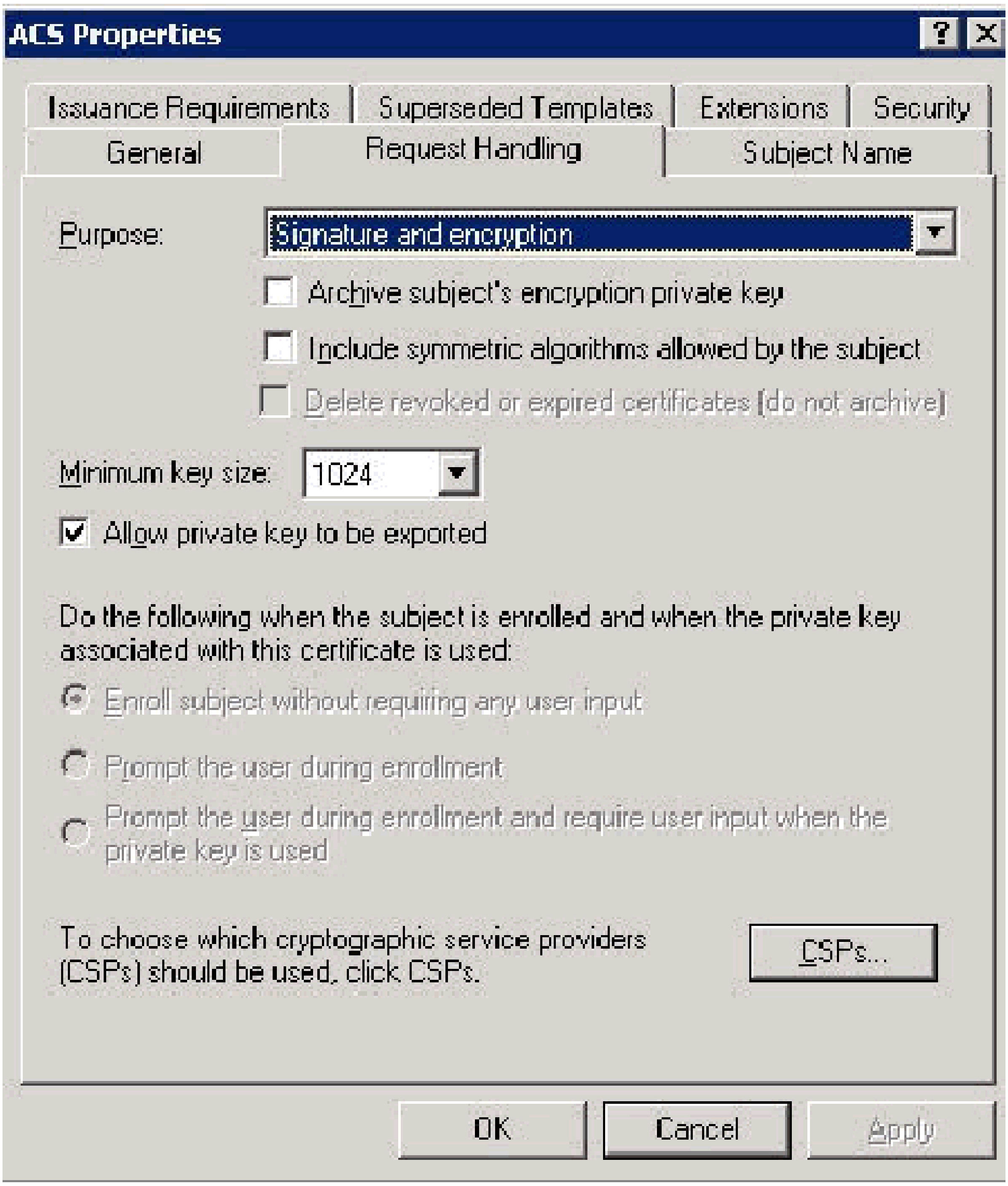
Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

4. 转到“请求处理”选项卡，并选中**允许导出私钥**。



Purpose: Signature and encryption

□ Archive subject's encryption private key

□ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

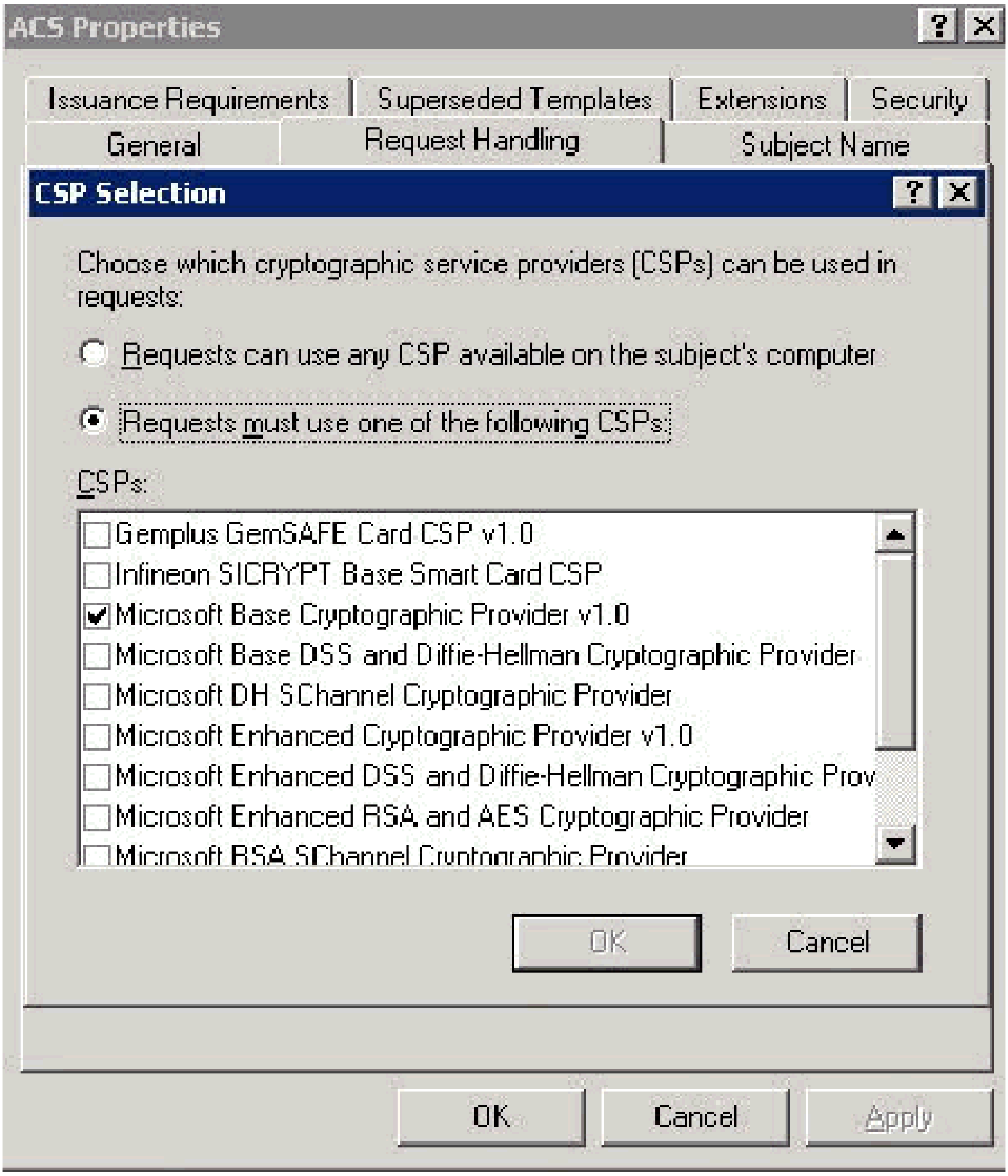
● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

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



Choose which cryptographic service providers (CSPs) can be used in requests:

○ Requests can use any CSP available on the subject's computer

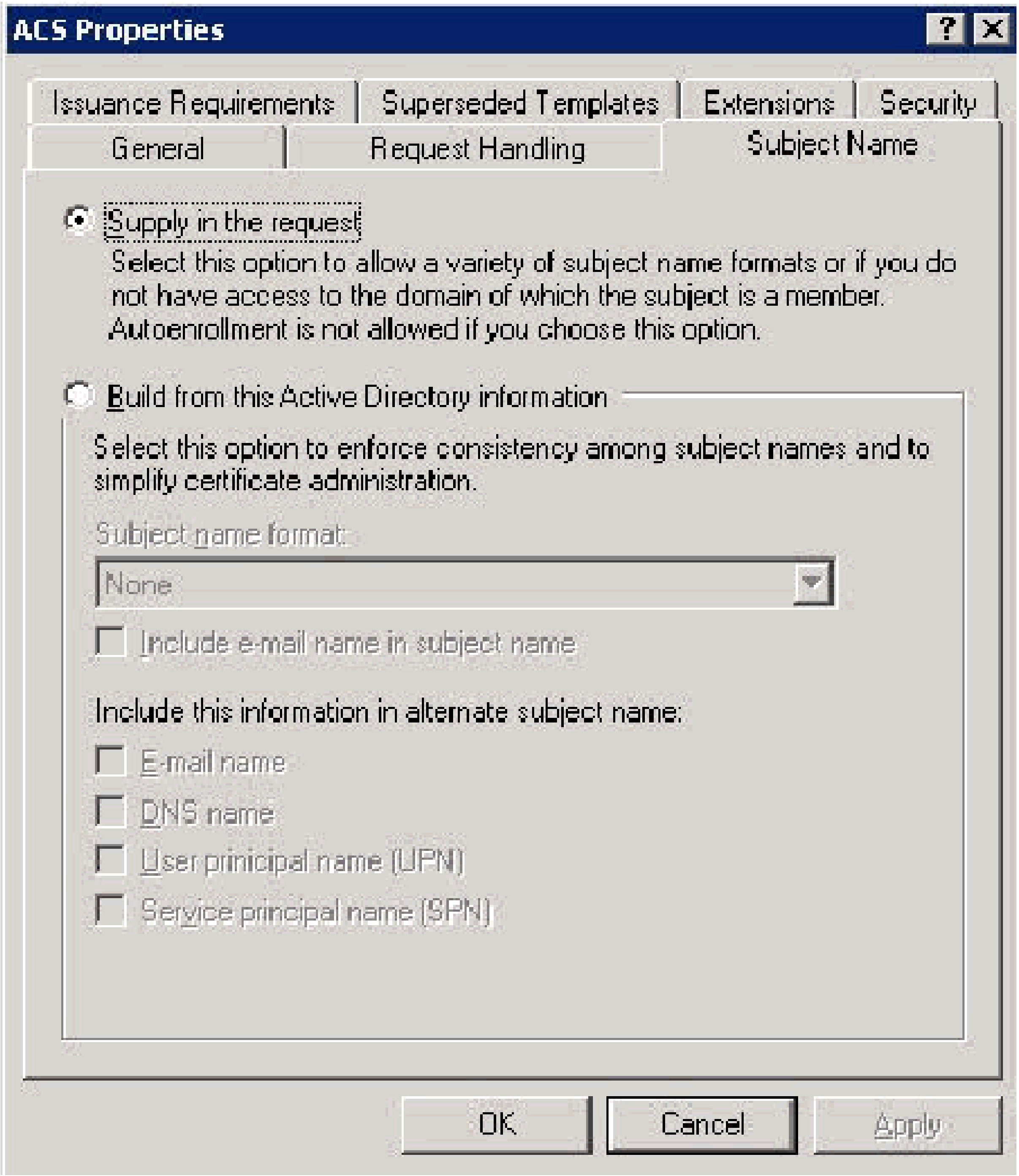
● Requests must use one of the following CSPs:

CSPs:

- □ Gemplus GemSAFE Card CSP v1.0
- □ Infineon SICRYPT Base Smart Card CSP
- ☑ Microsoft Base Cryptographic Provider v1.0
- □ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
- □ Microsoft DH SChannel Cryptographic Provider
- □ Microsoft Enhanced Cryptographic Provider v1.0
- □ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov
- □ Microsoft Enhanced RSA and AES Cryptographic Provider
- □ Microsoft RSA SChannel Cryptographic Provider

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”。**



● Supply in the request

Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

□ Include e-mail name in subject name

Include this information in alternate subject name:

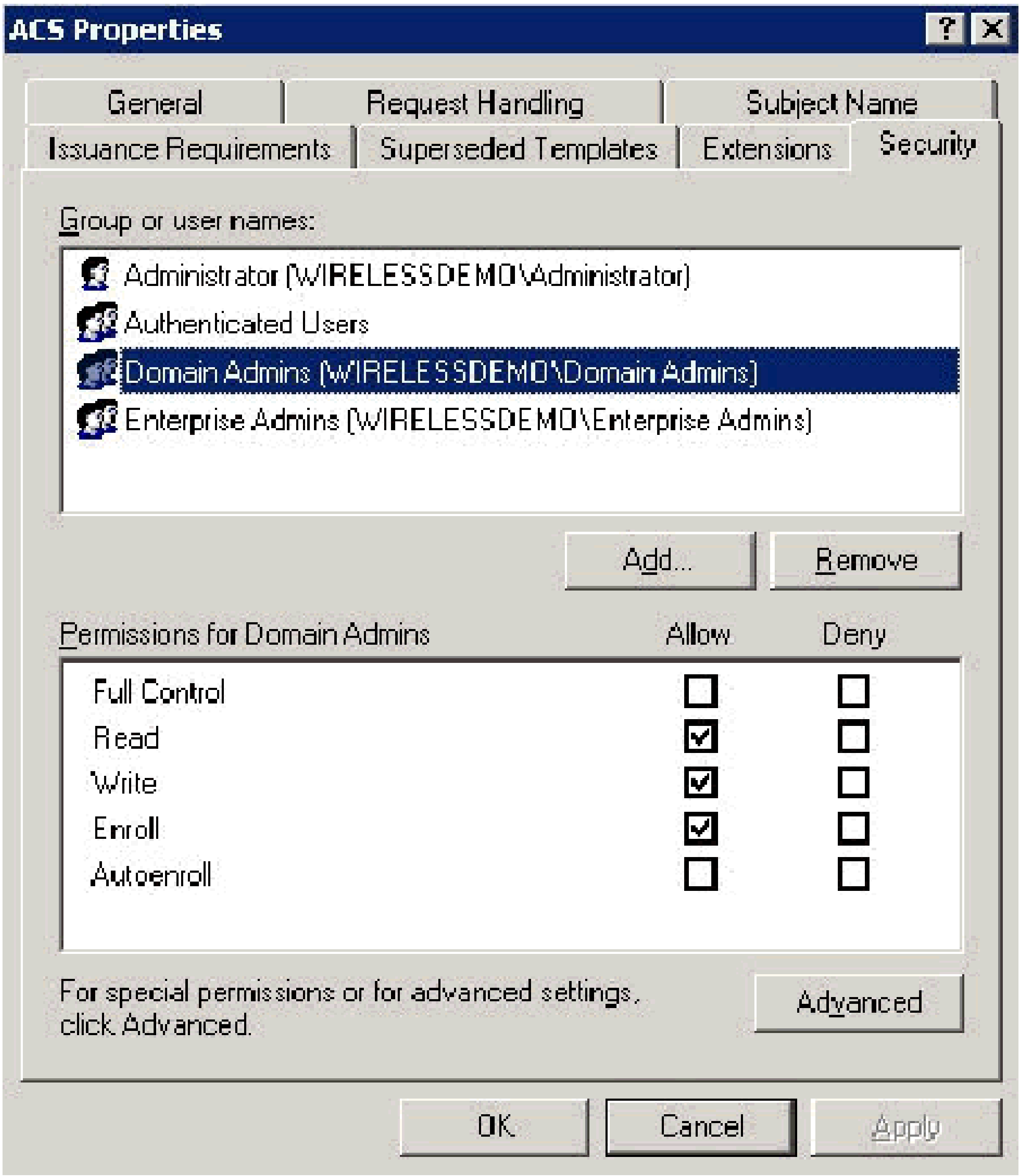
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

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**：如果选择仅根据此Active Directory信息生成，请选中**用户主体名称(UPN)**，并取消选中**将电子邮件名称包含在主题名称和电子邮件名称中**，因为未在Active Directory用户和计算机管理单元中为WirelessUser帐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，这会导致自动注册错误。



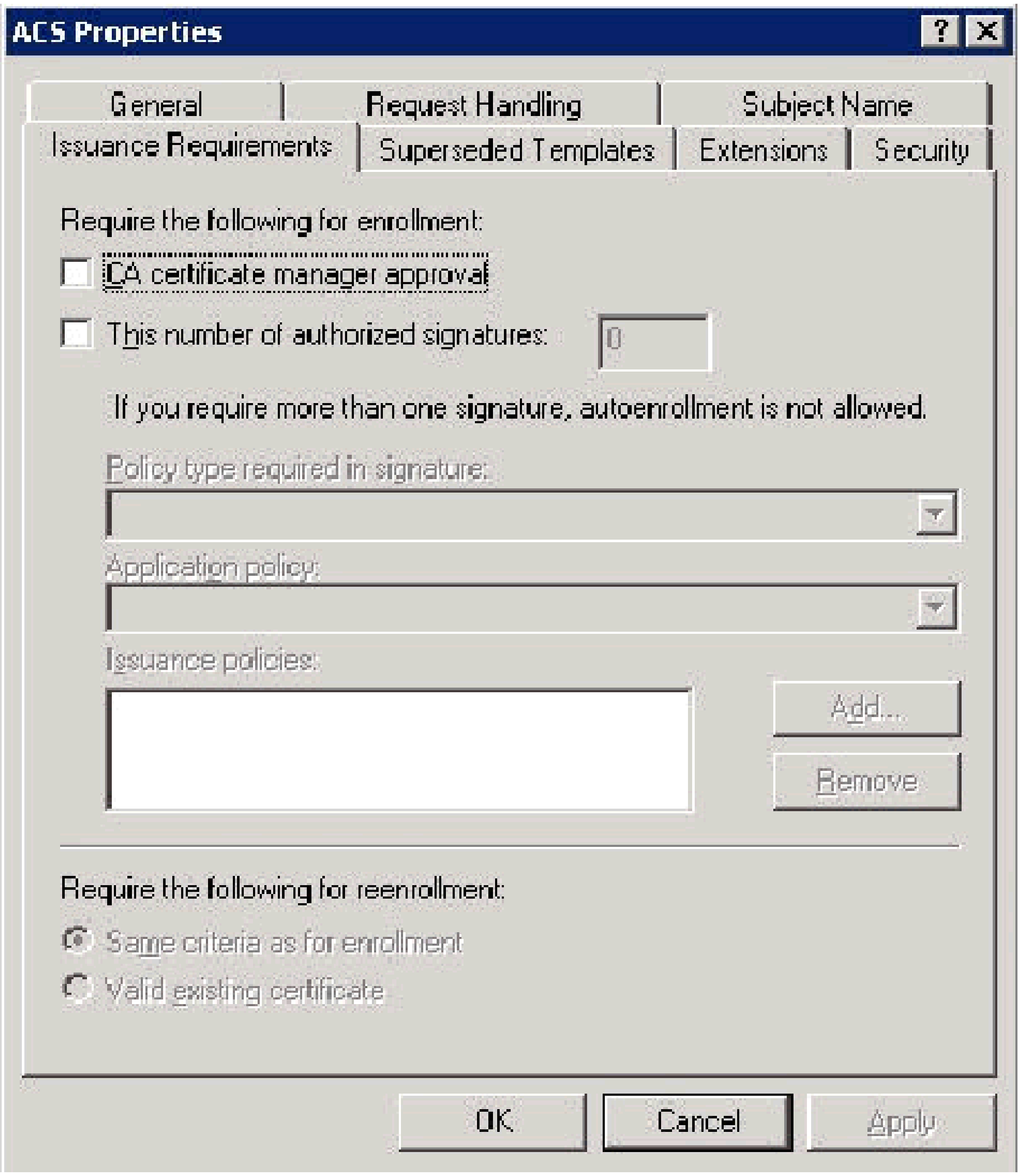
Group or user names:

- Administrator (WIRELESSDEMO\Administrator)
- Authenticated Users
- Domain Admins (WIRELESSDEMO\Domain Admins)
- Enterprise Admins (WIRELESSDEMO\Enterprise Admins)

Permissions for Domain Admins	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or for advanced settings, click Advanced.

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。



ACS Properties

General | Request Handling | Subject Name

Issuance Requirements | Superseded Templates | Extensions | Security

Require the following for enrollment:

□ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

● Same criteria as for enrollment

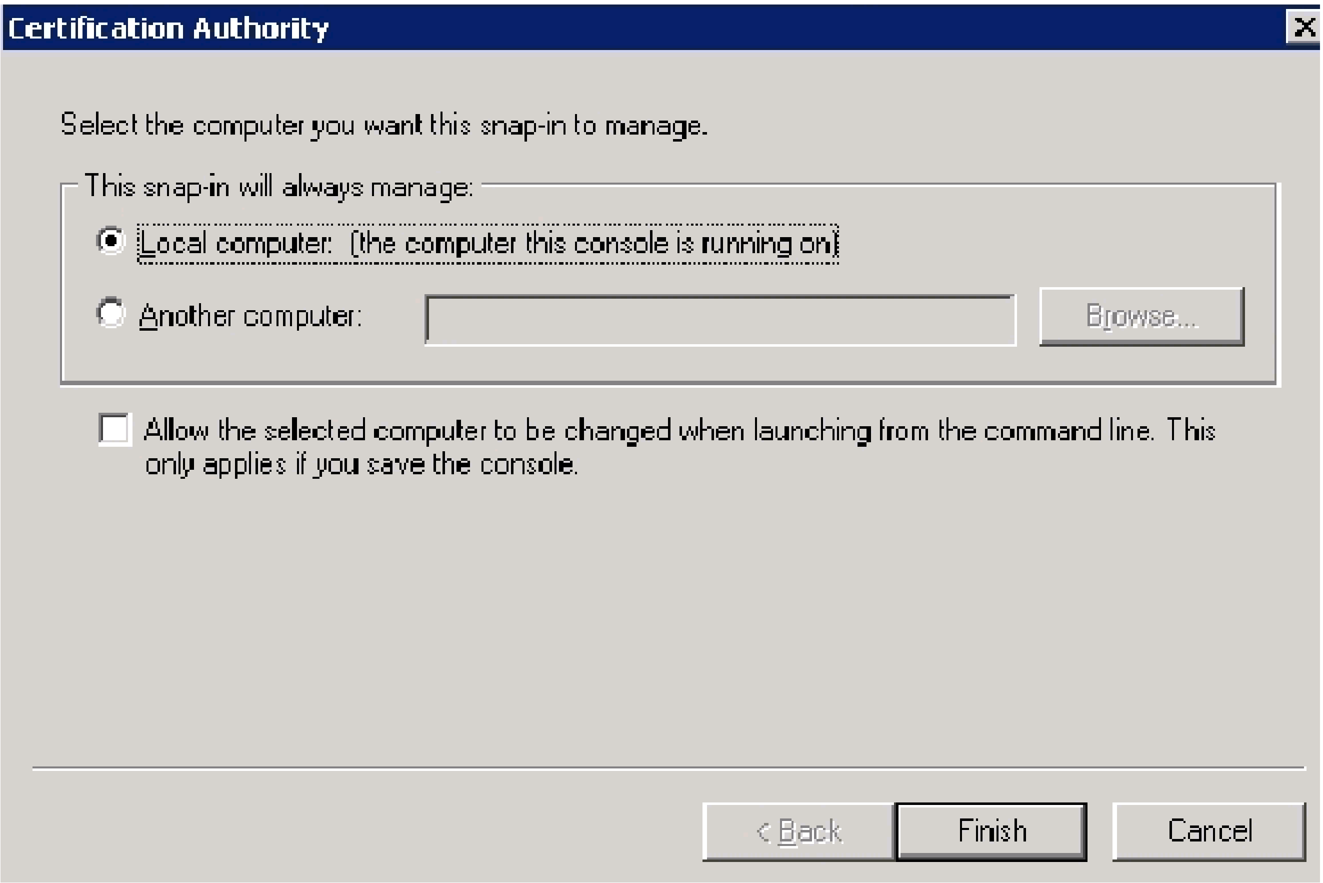
○ Valid existing certificate

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”。**



Certification Authority

Select the computer you want this snap-in to manage.

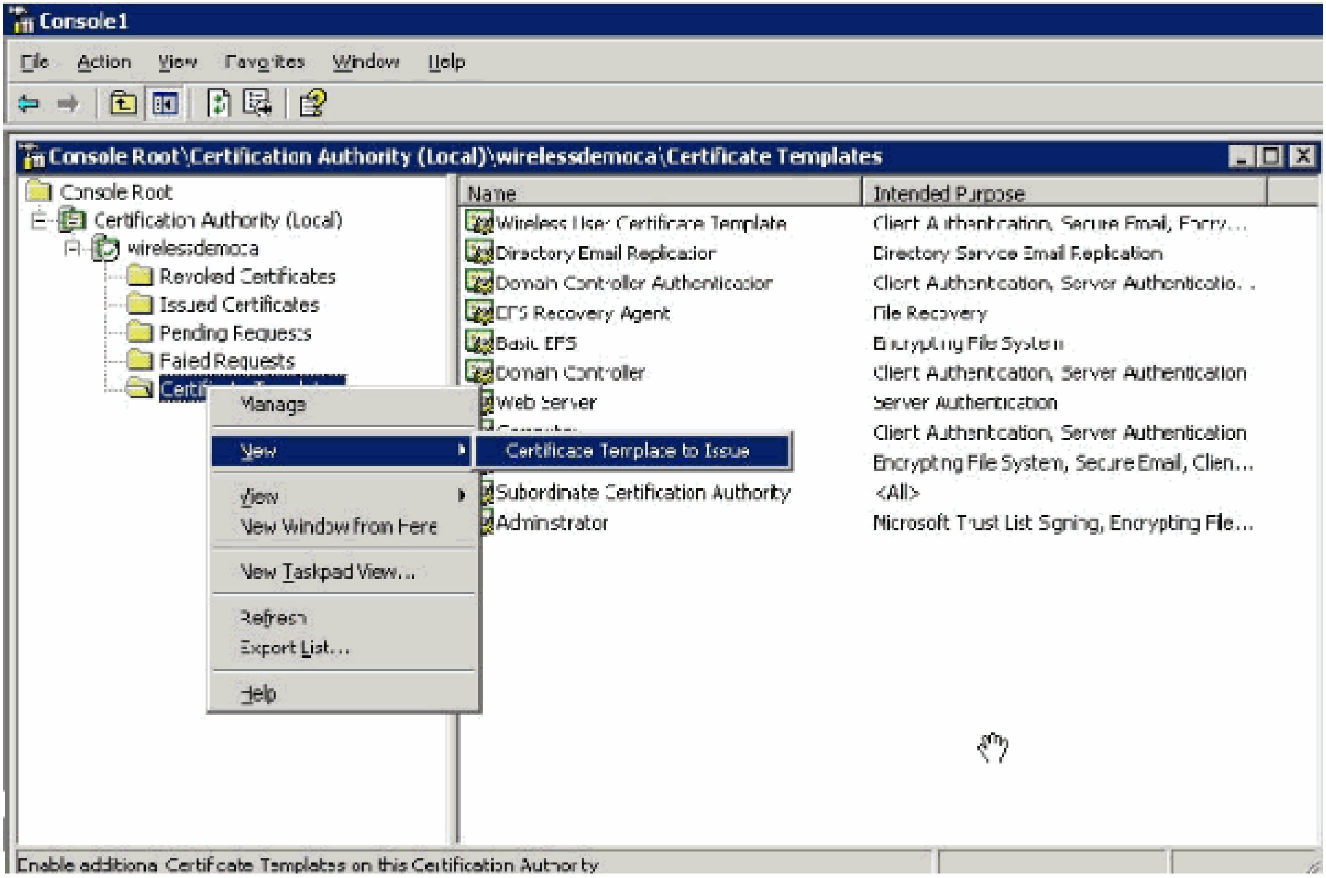
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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



Console1

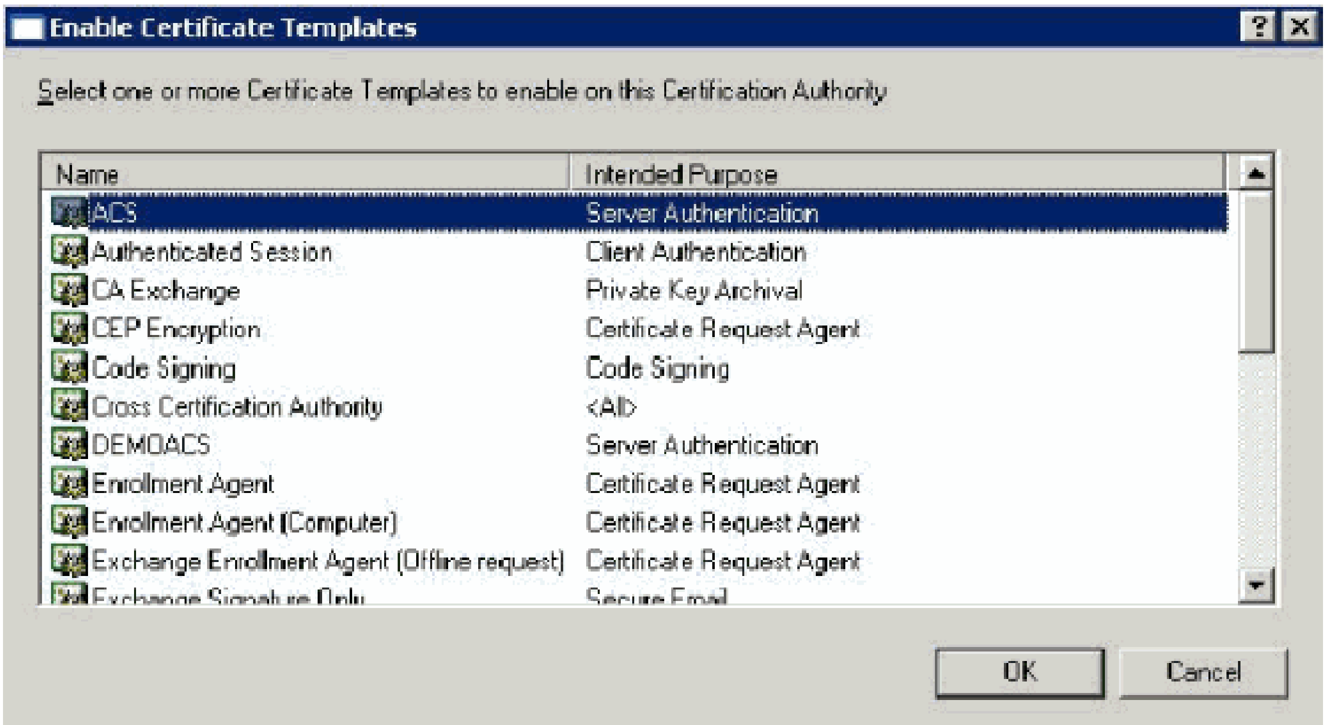
Console Root\Certification Authority (Local)\wirelessdemoca\Certificate Templates

Name	Intended Purpose
Wireless User Certificate Template	Client Authentication, Secure Email, Encry...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

Enable additional Certificate Templates on this Certification Authority

3. 选择**新>发行的认证模板。**

4. 单击 **ACS 证书模板。**

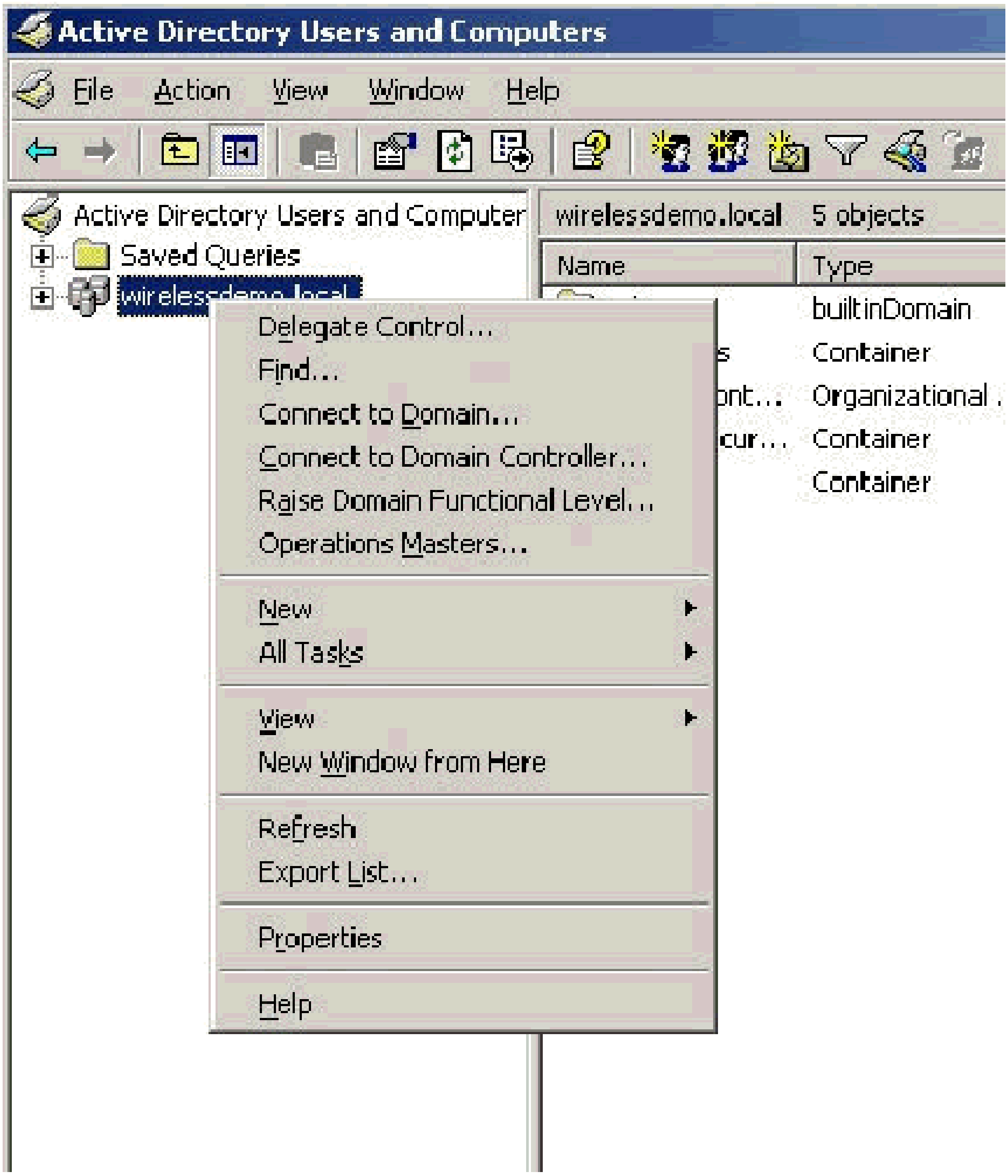


Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
ACS	Server Authentication
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
Code Signing	Code Signing
Cross Certification Authority	<All>
DEMOACS	Server Authentication
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email

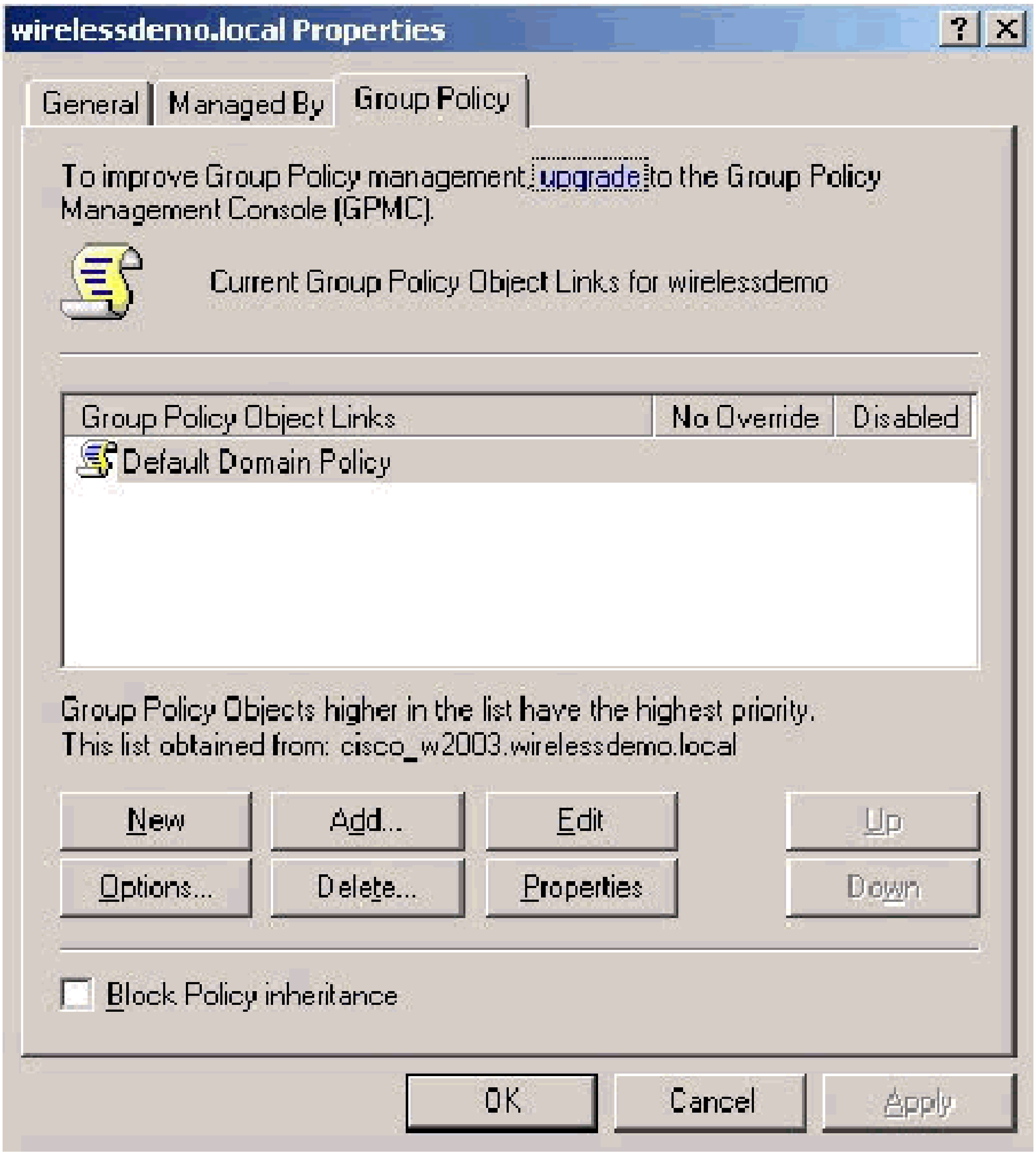
5. 单击**确定，然后打开“Active Directory 用户和计算机”管理单元。**

6. 在控制台树中，双击**Active Directory用户和计算机**，右键单击**wirelessdemo.local域**，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



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for wirelessdemo

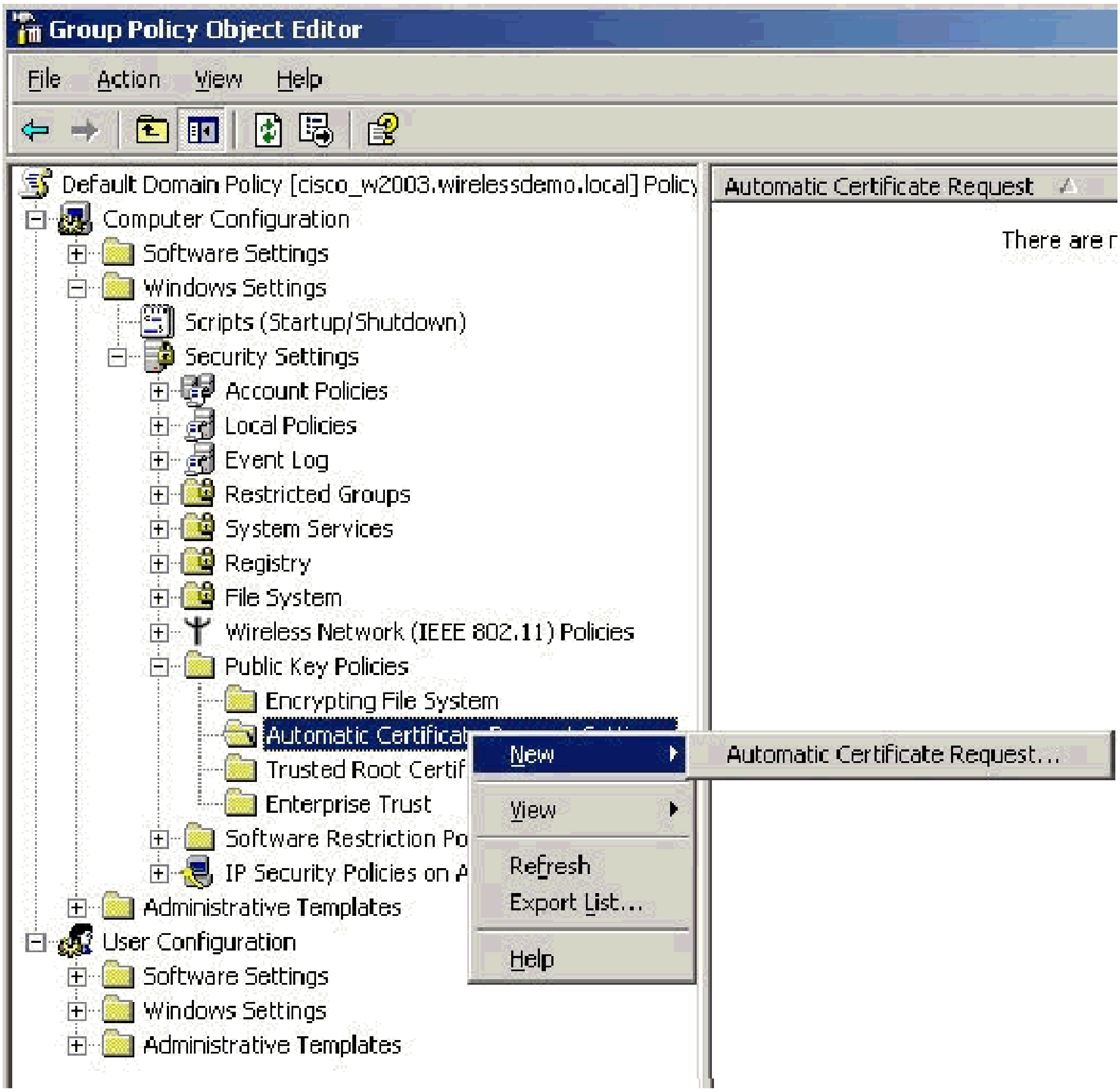
Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: cisco_w2003.wirelessdemo.local

□ Block Policy inheritance

元。

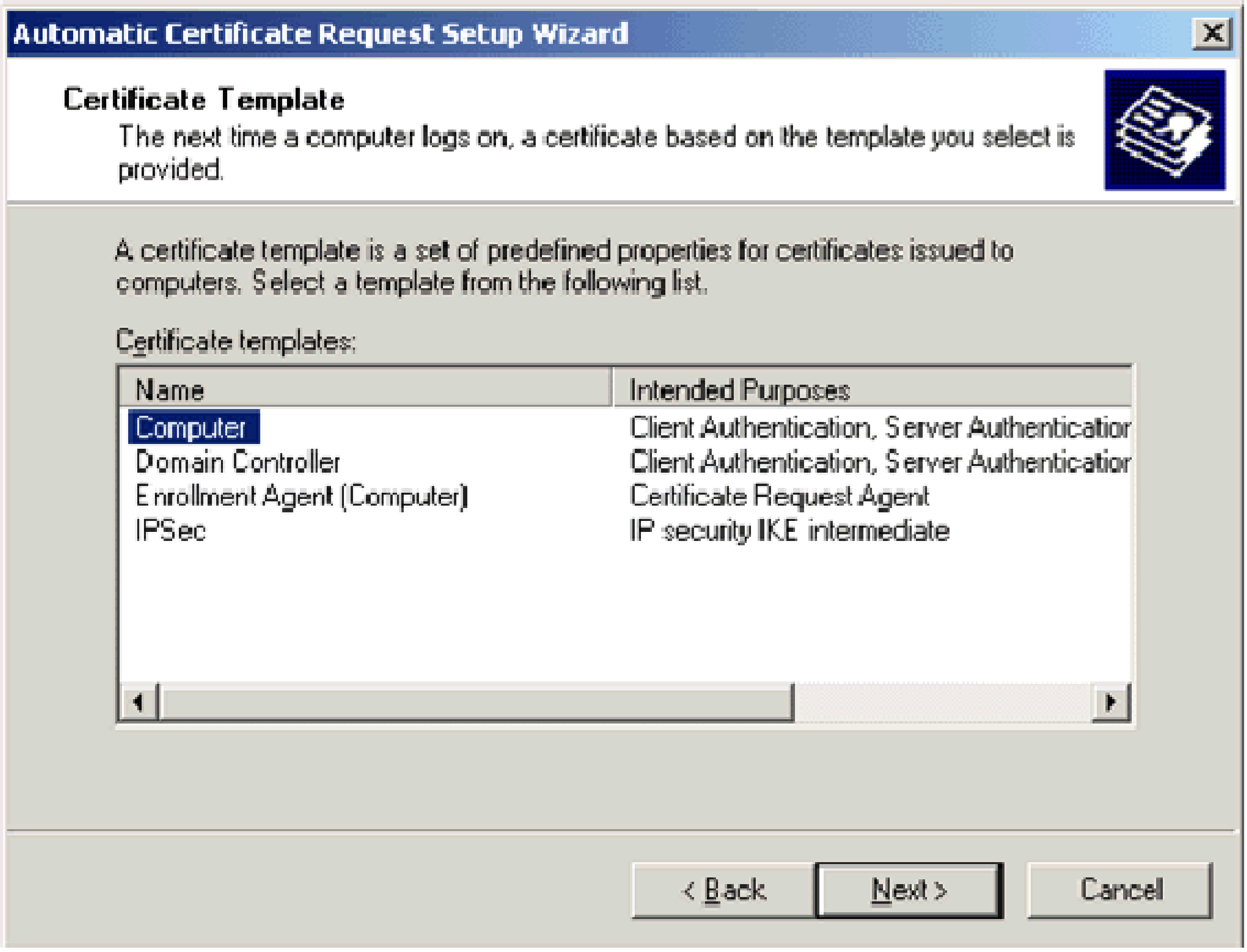
8. 在控制台树中，展开**计算机配置 > Windows 设置 > 安全设置 > 公钥策略**，然后选择“自动证书申请设置”。



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”。**



Certificate Template

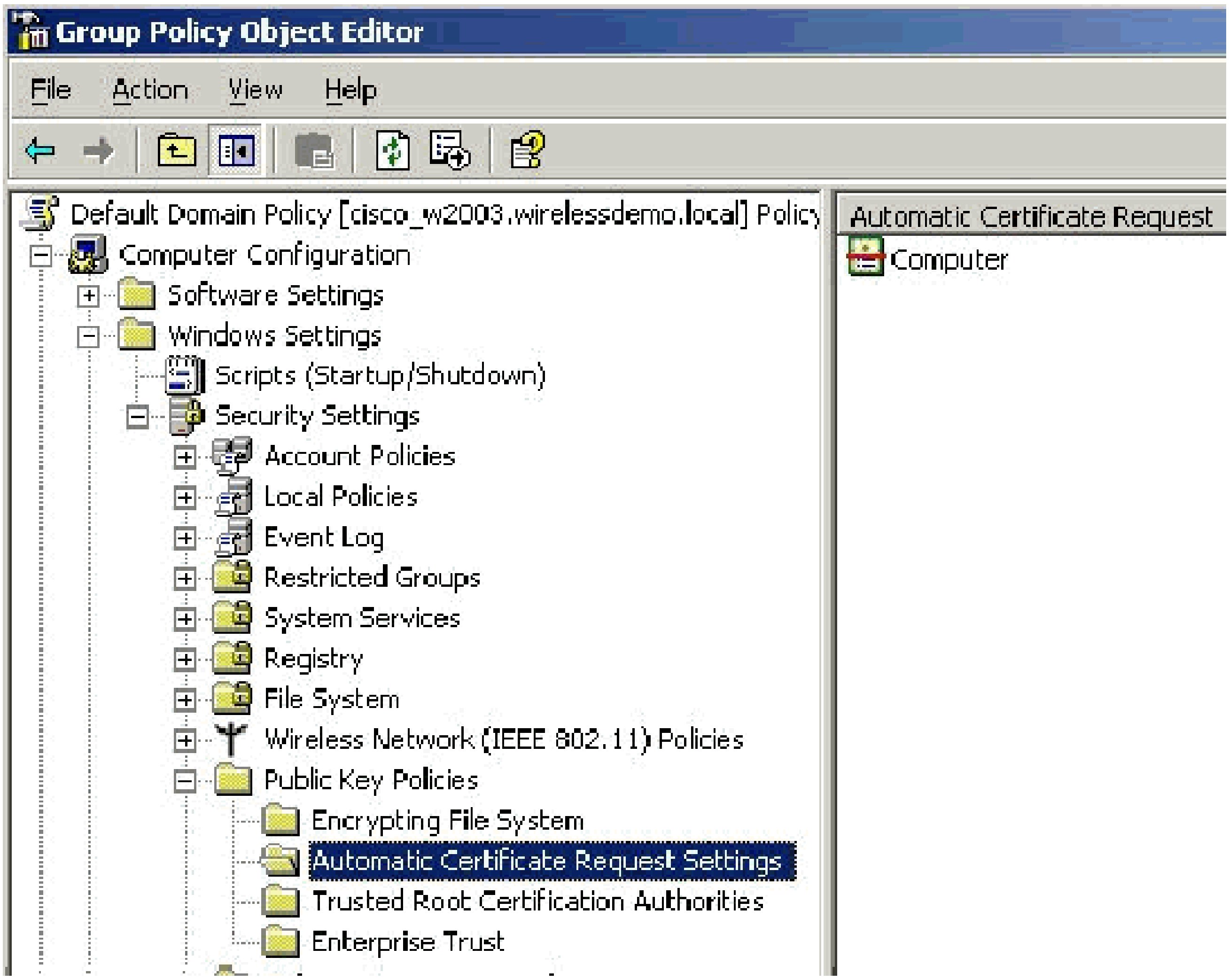
The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

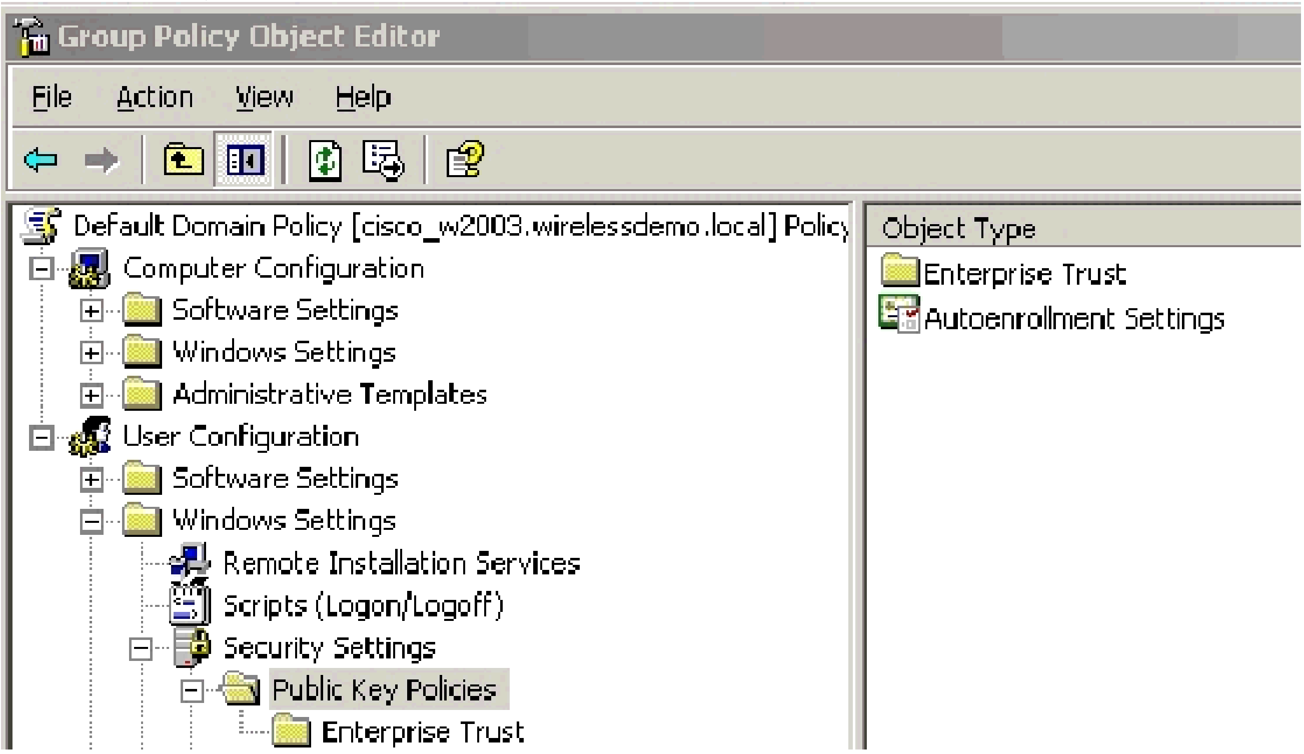
Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSec	IP security IKE intermediate

12. 在“完成自动证书请求设置向导”页上，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。

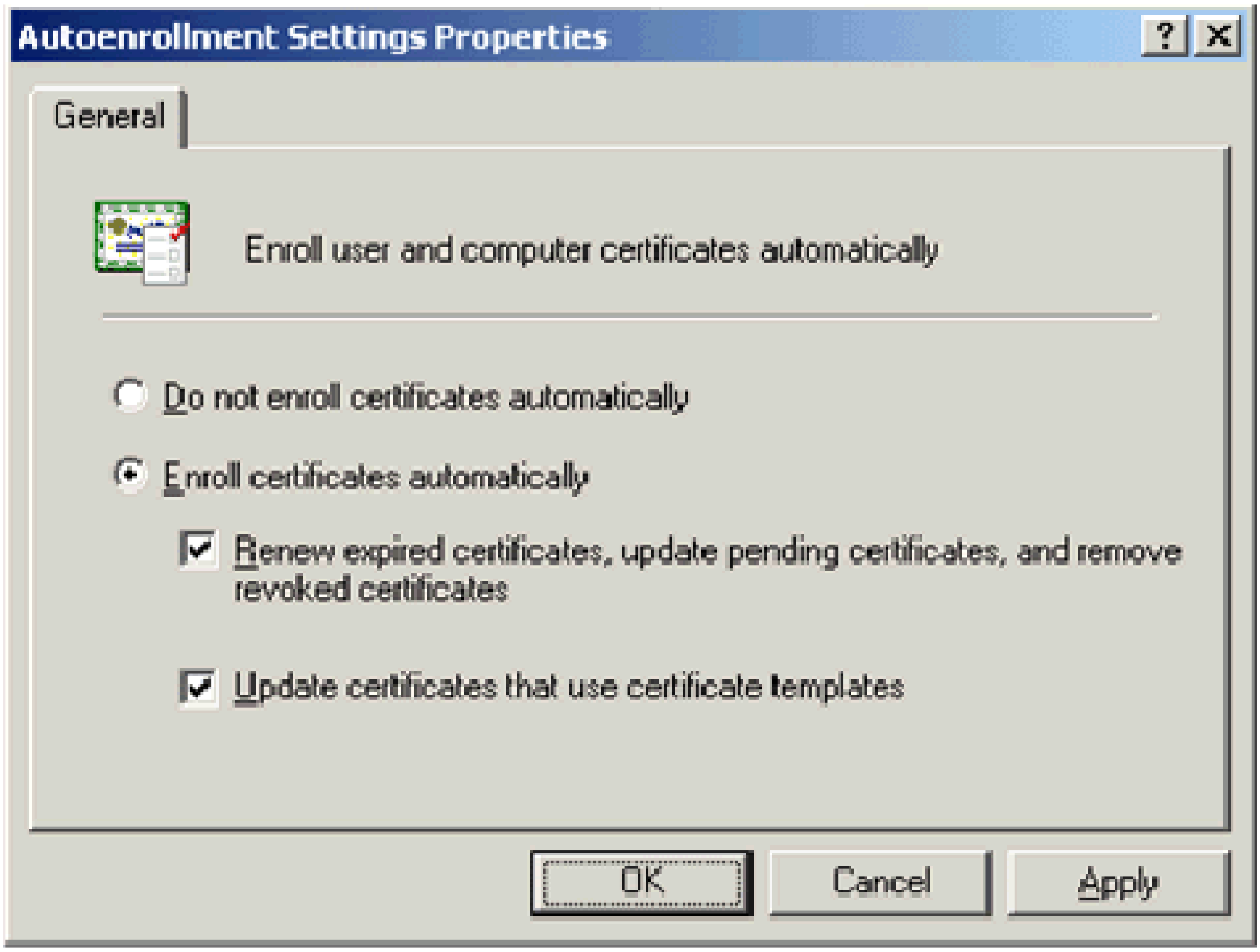

Group Policy Object Editor
File Action View Help
Default Domain Policy [cisco_w2003.wirelessdemo.local] Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Automatic Certificate Request
Computer

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”。**



Enroll user and computer certificates automatically

○ Do not enroll certificates automatically

● Enroll certificates automatically

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

16. Click **OK**.

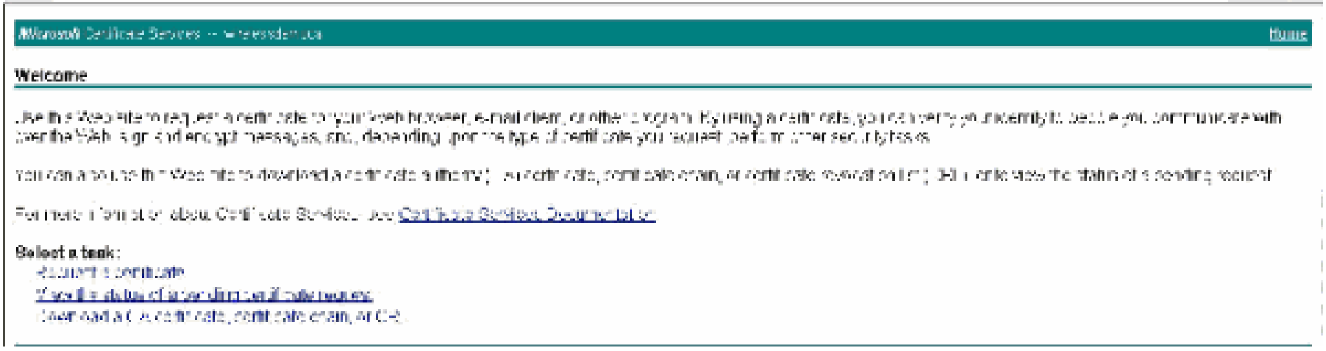
ACS 4.0 证书设置

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 EAP-TLS客户端进行身份验证。

重要信息：确保在证书设置过程中IIS管理器未打开，因为它会导致缓存信息出现问题。

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。


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://172.16.100.26/certsrv/
Go
Links
Home

Microsoft Certificate Services -- [illegible]

Welcome

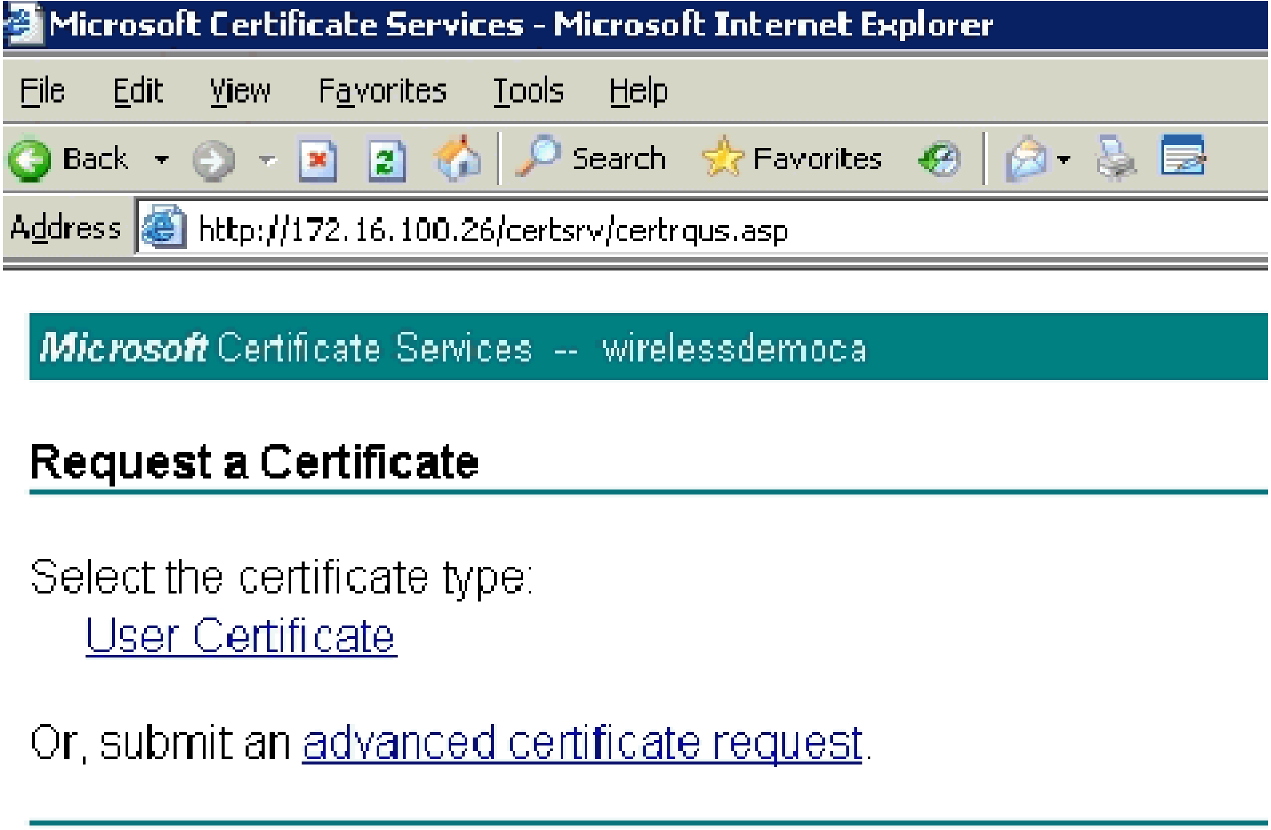
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

4. 选择**申请一个证书，然后单击“下一步”。**


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address

http://172.16.100.26/certsrv/certrqus.asp

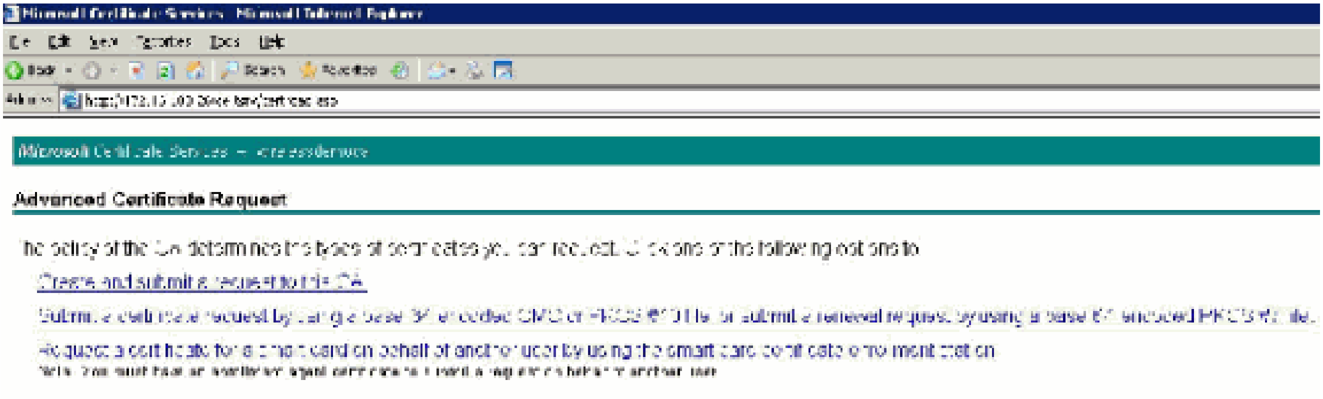
Microsoft Certificate Services -- wirelessdemoca

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

5. 选择**高级请求并单击“下一步”。**


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address

http://172.16.100.26/certsrv/certrqad.asp

Microsoft Certificate Services -- wirelessdemoca

Advanced Certificate Request

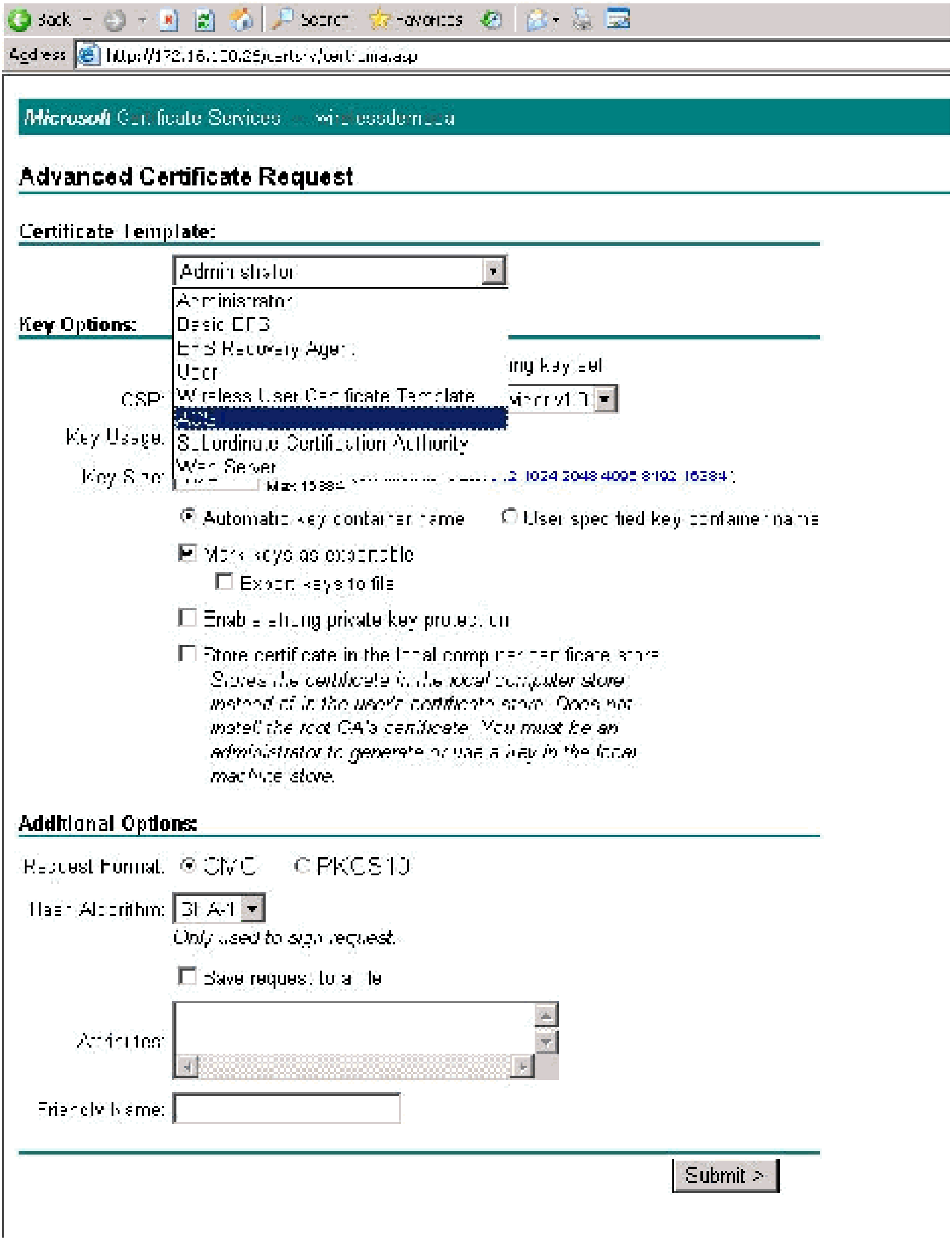
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

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。



Back
Search
Favorites
Address http://172.16.100.25/certsrv/certrqma.asp
Microsoft Certificate Services -- wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administrator

Administrator
Basic EFS
EFS Recovery Agent
User
Wireless User Certificate Template
ACS
Subordinate Certification Authority
Web Server

Key Options:

...ing key set

CSP: ...nced v1.0

Key Usage:

Key Size: Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Export keys to file

□ Enable strong private key protection

□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

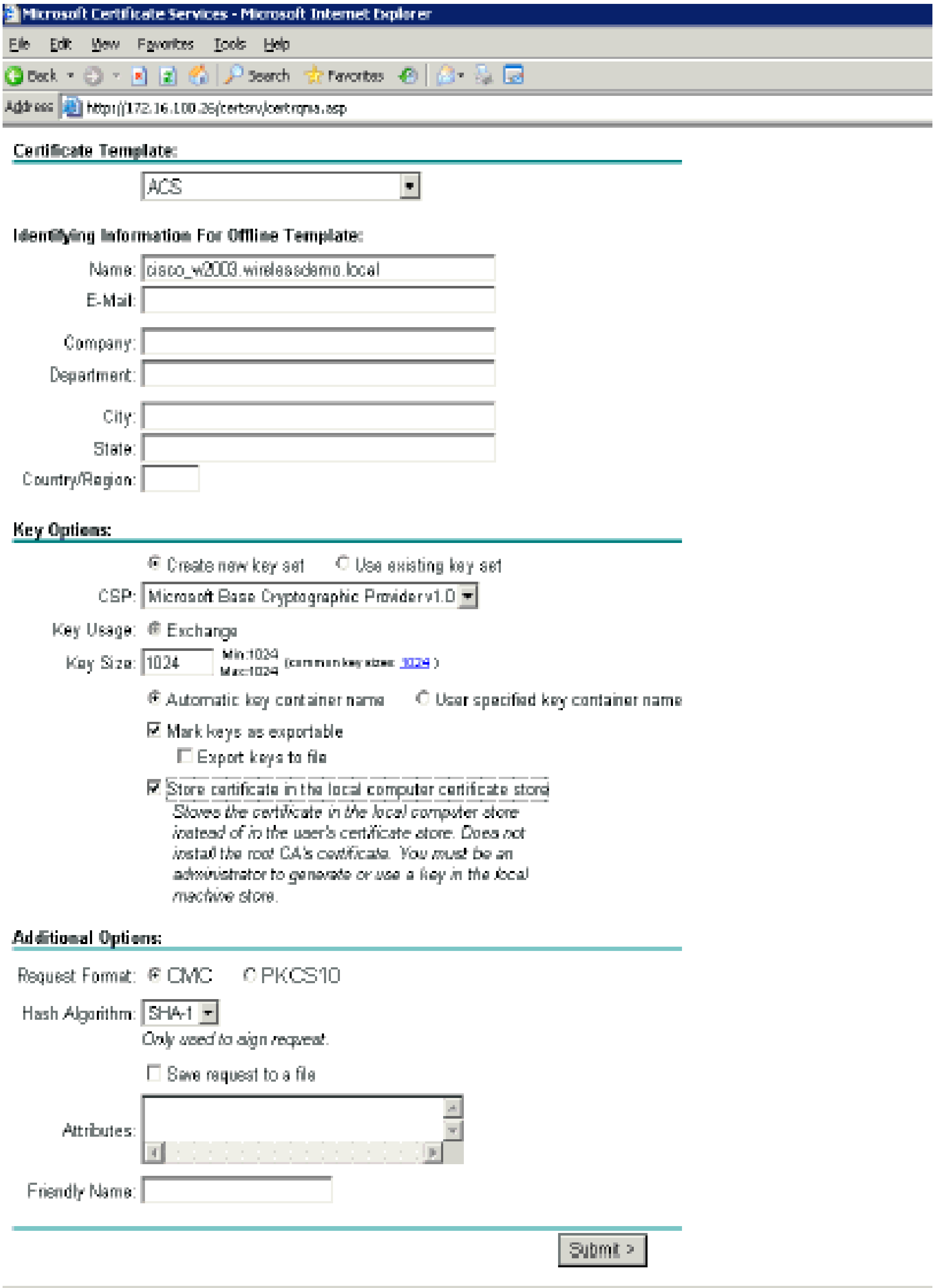
Only used to sign request.

□ Save request to a file

Attributes:

Friendly Name:

7. 从Certificate Templates（证书模板）中，选择之前创建的名为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**



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.100.26/certsrv/certrqma.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name: cisco_w2003.wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: ● Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 1024)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Export keys to file

☑ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

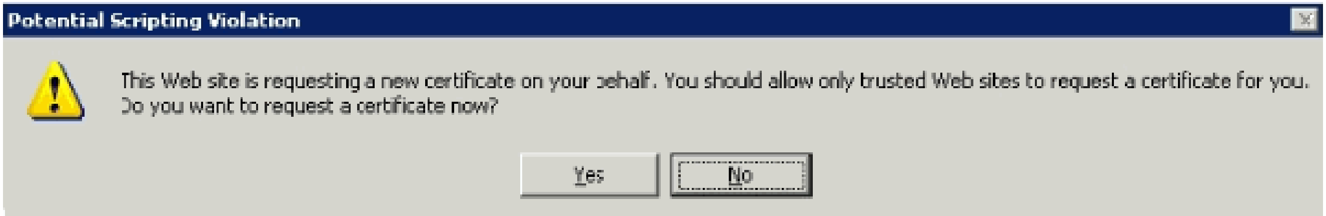
□ Save request to a file

Attributes:

Friendly Name:

”。

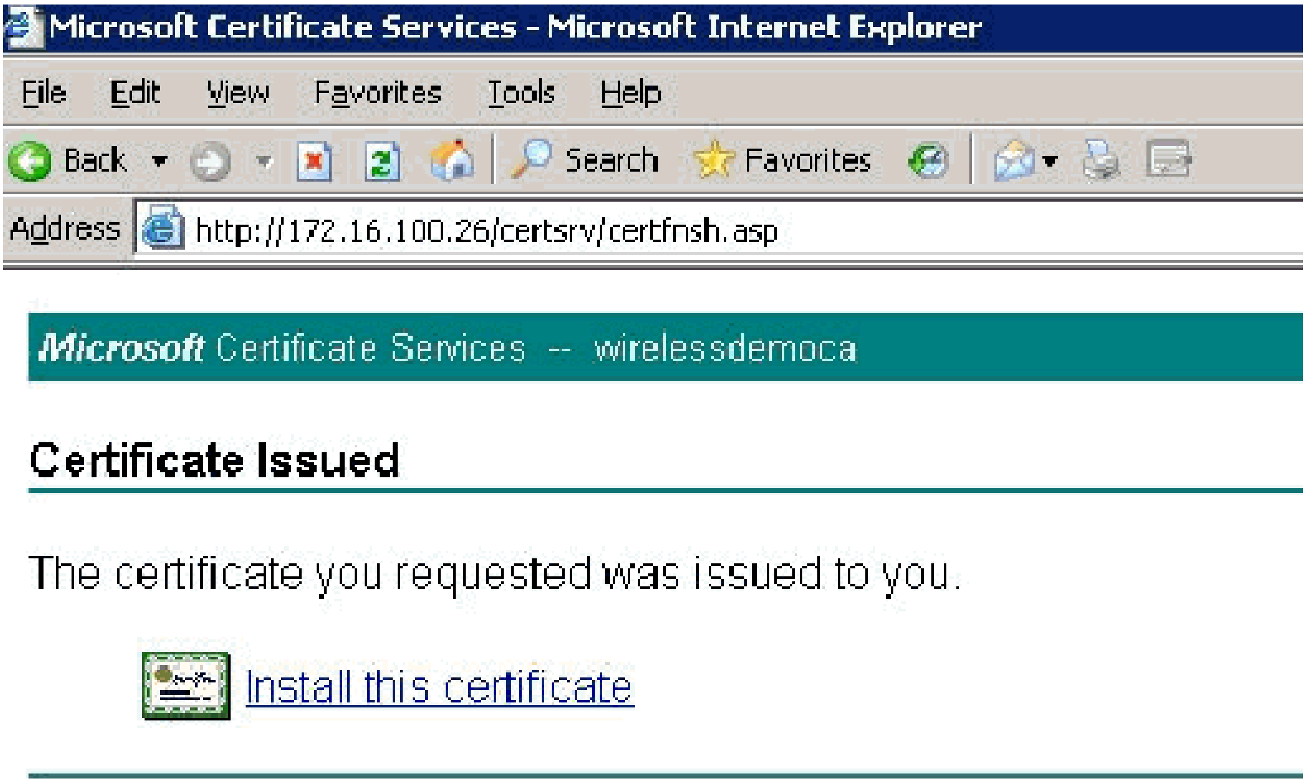
9. 系统将显示一个弹出窗口，警告可能存在脚本违规。单击 Yes。



Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

10. 单击 Install this certificate。


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address

http://172.16.100.26/certsrv/certfnsh.asp

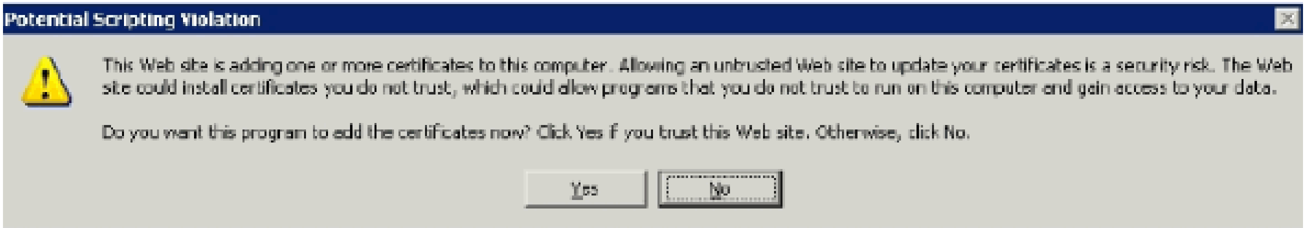
Microsoft Certificate Services -- wirelessdemoca

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

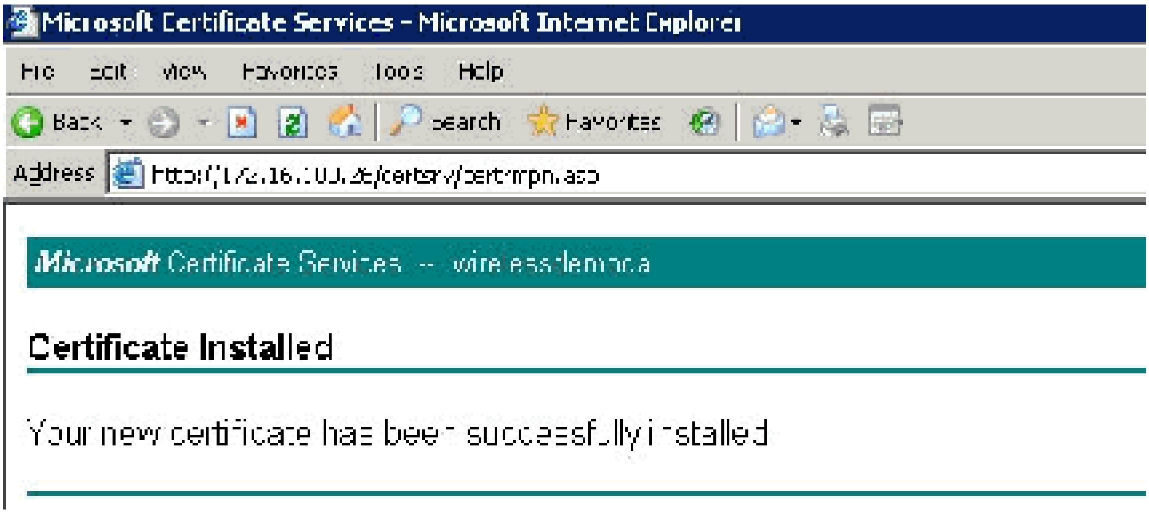
11. 此时将再次显示一个弹出窗口，警告可能出现脚本冲突。单击 **Yes**。



This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

12. 当您单击**是**后，就会安装证书。


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address

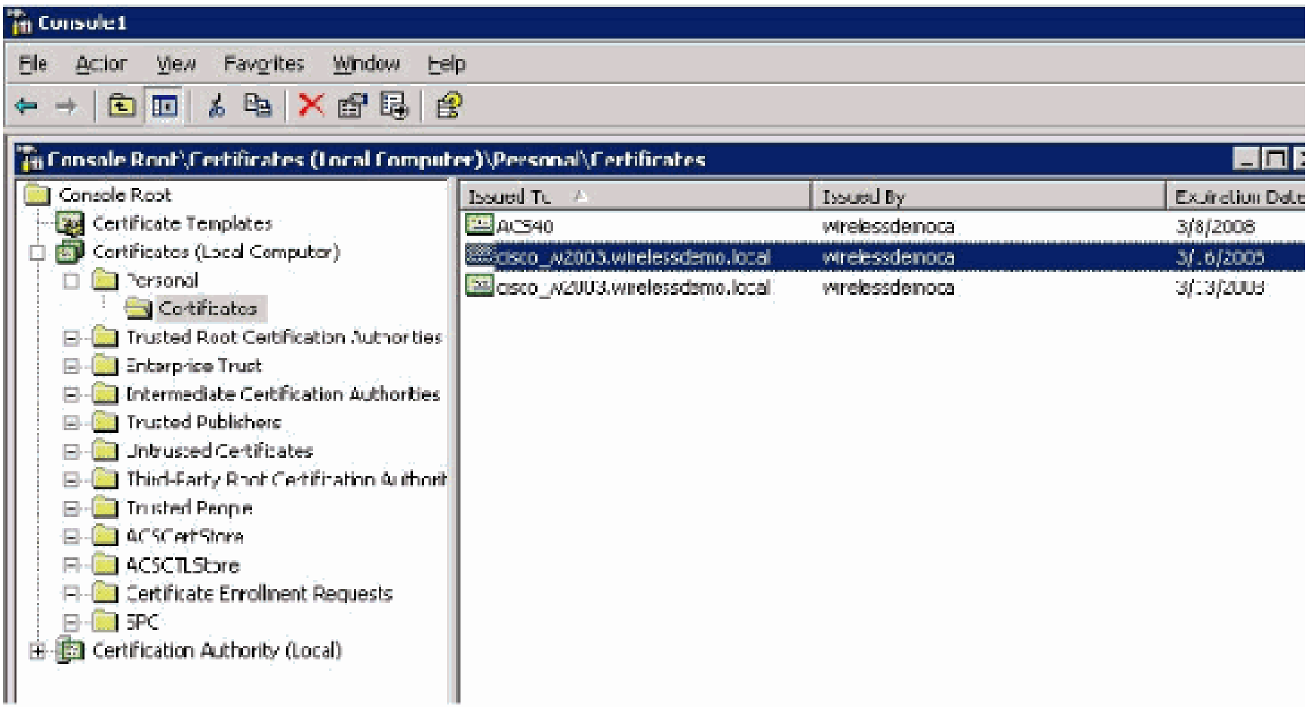
http://172.16.100.26/certsrv/certrmpn.asp

Microsoft Certificate Services -- wirelessdemoca

Certificate Installed

Your new certificate has been successfully installed

13. 此时，证书将安装在Certificates文件夹中。要访问此文件夹，请选择**开始>运行**，键入**mmc**，按**Enter**，然后选择**个人>证书**。


Console1
File
Action
View
Favorites
Window
Help
Console Root\Certificates (Local Computer)\Personal\Certificates
Console Root
Certificate Templates
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorit
Trusted People
ACSCertStore
ACSCTLStore
Certificate Enrollment Requests
SPC
Certification Authority (Local)

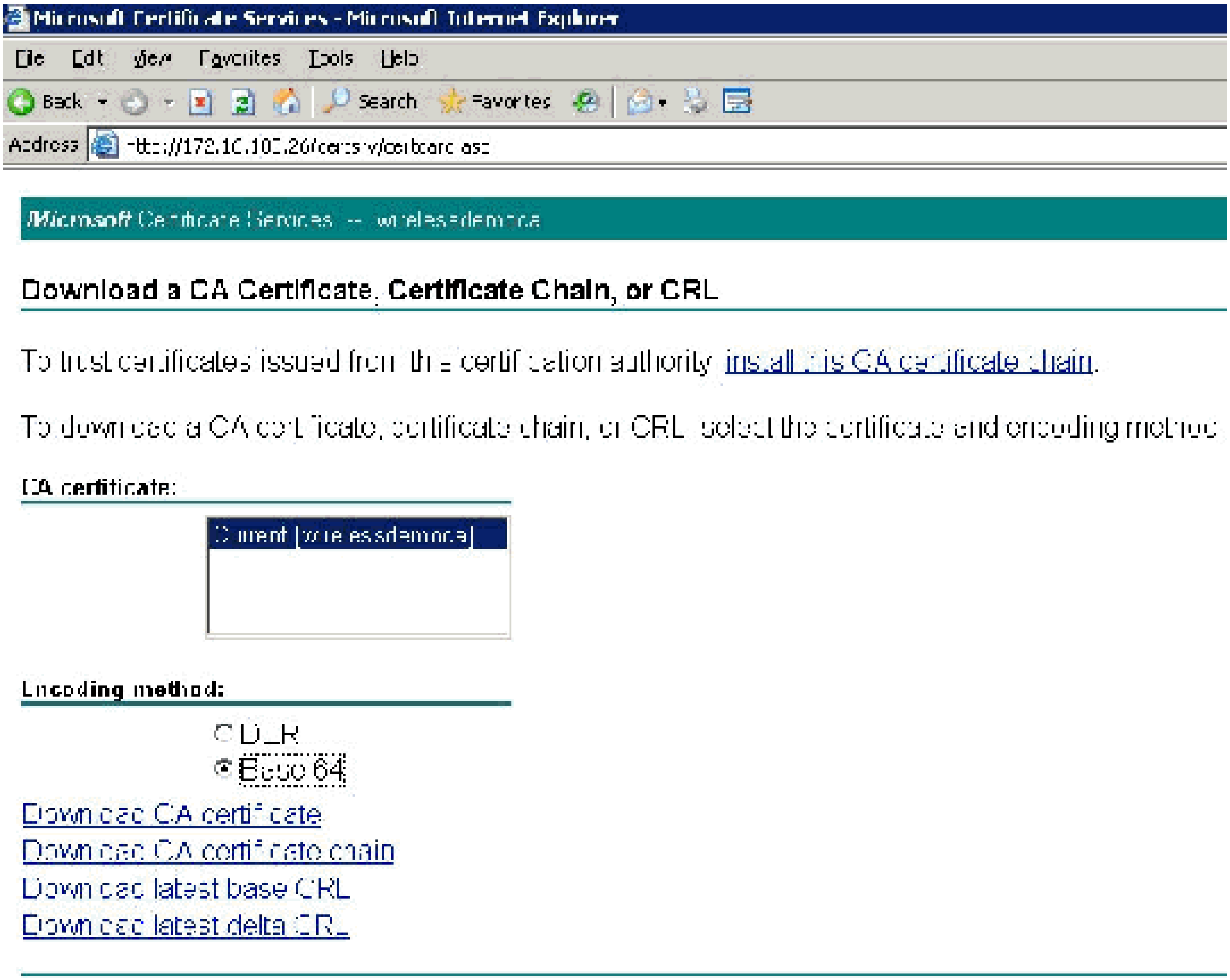
Issued To	Issued By	Expiration Date
ACS40	wirelessdemoca	3/8/2008
cisco_w2003.wirelessdemo.local	wirelessdemoca	3/16/2008
cisco_w2003.wirelessdemo.local	wirelessdemoca	3/13/2008

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”。**


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.100.26/certsrv/certcarc.asp
Microsoft Certificate Services -- wirelessdemoca

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method

CA certificate:

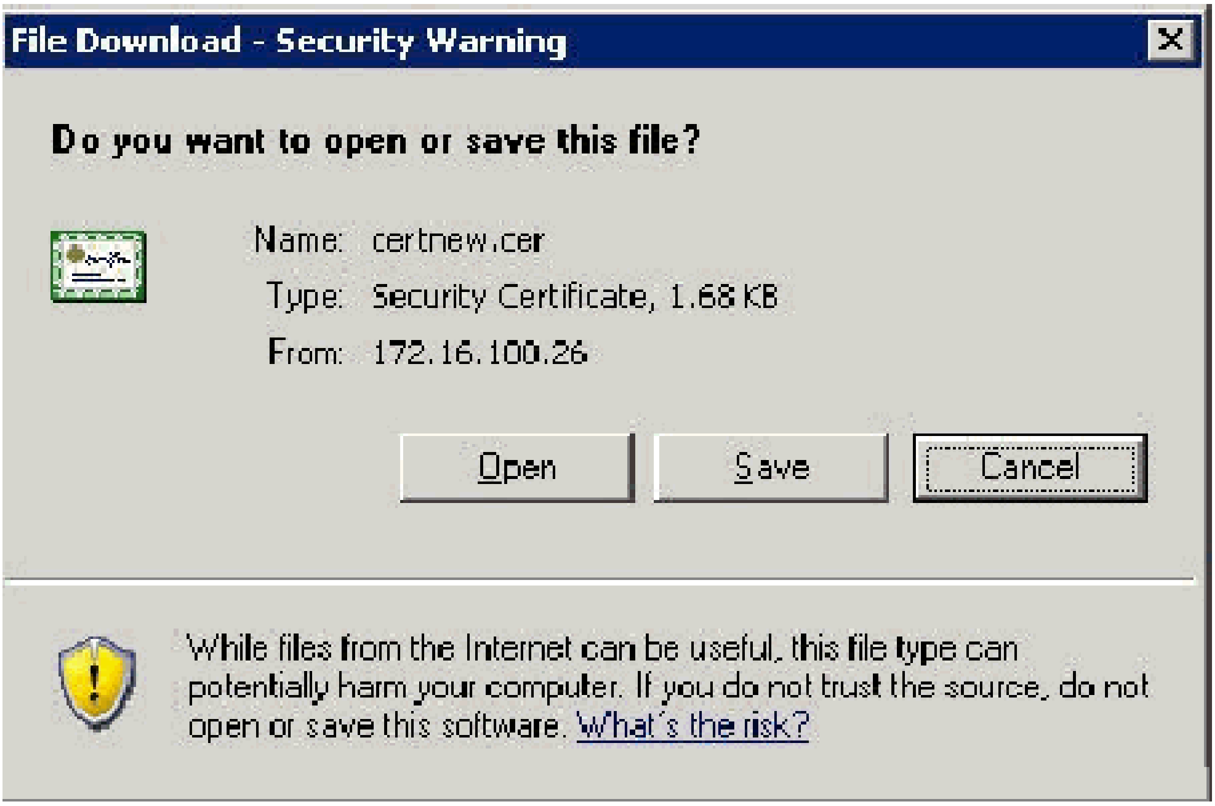
Current [wirelessdemoca]

Encoding method:

○ DER
● Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

4. 此时将显示“文件下载安全警告”窗口。Click



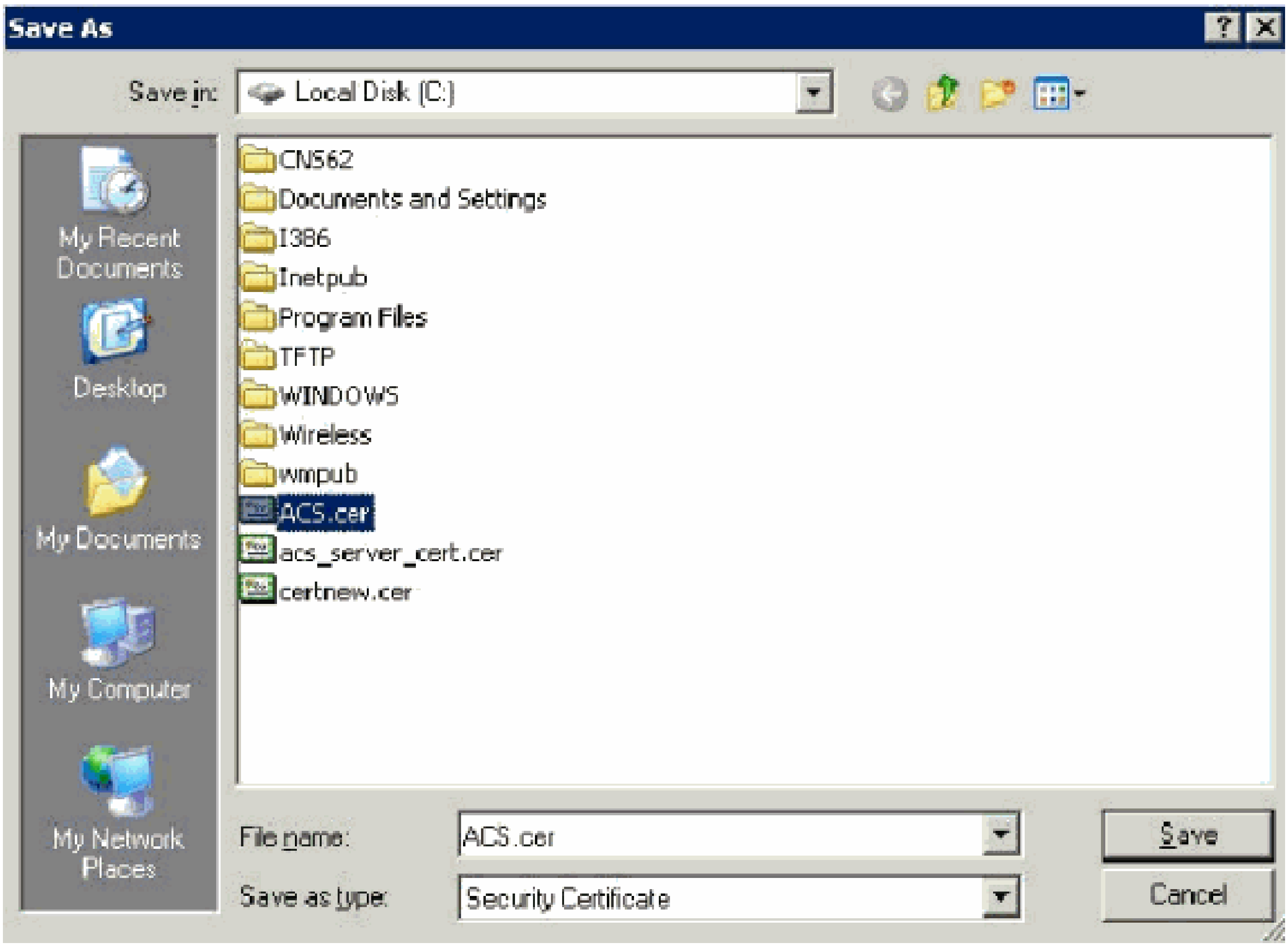
Do you want to open or save this file?

Name: certnew.cer
Type: Security Certificate, 1.68 KB
From: 172.16.100.26

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Save.

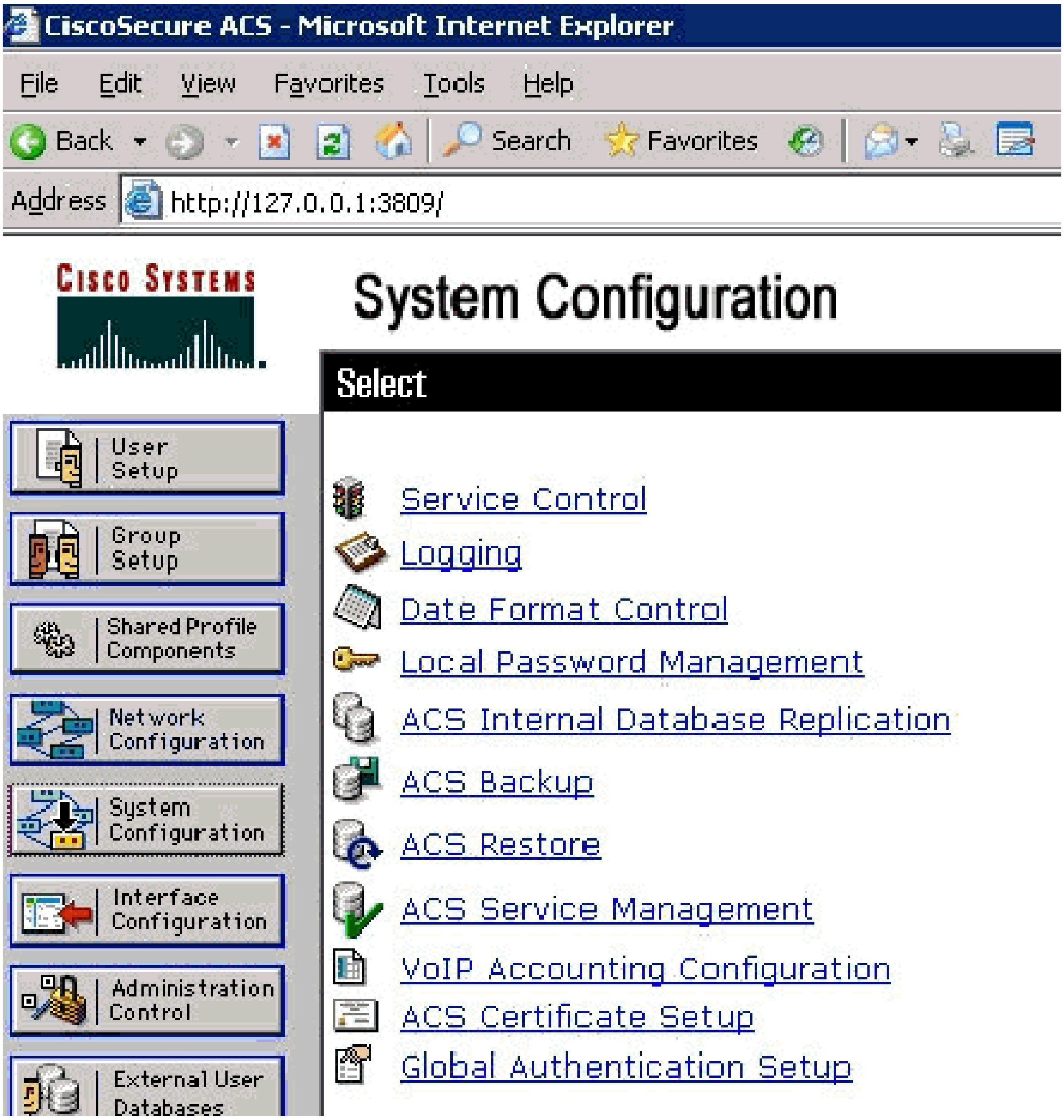
5. 用 ACS.cer 或您需要的任意名称保存文件。请记住此名称，因为您在 ACS 4.0 中设置 ACS 证书颁发机构的过程中要用到它。



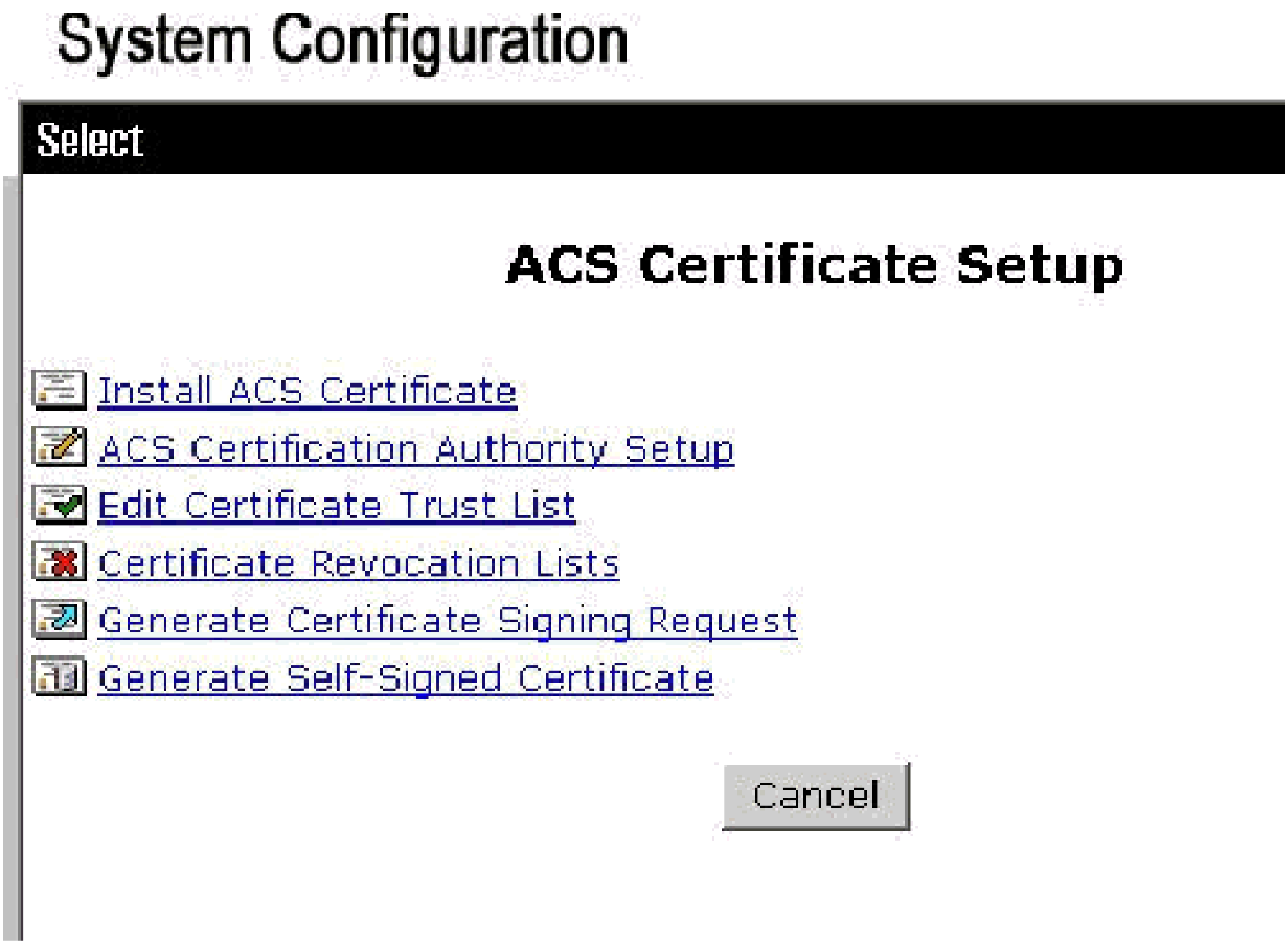
File name: ACS.cer

Save as type: Security Certificate

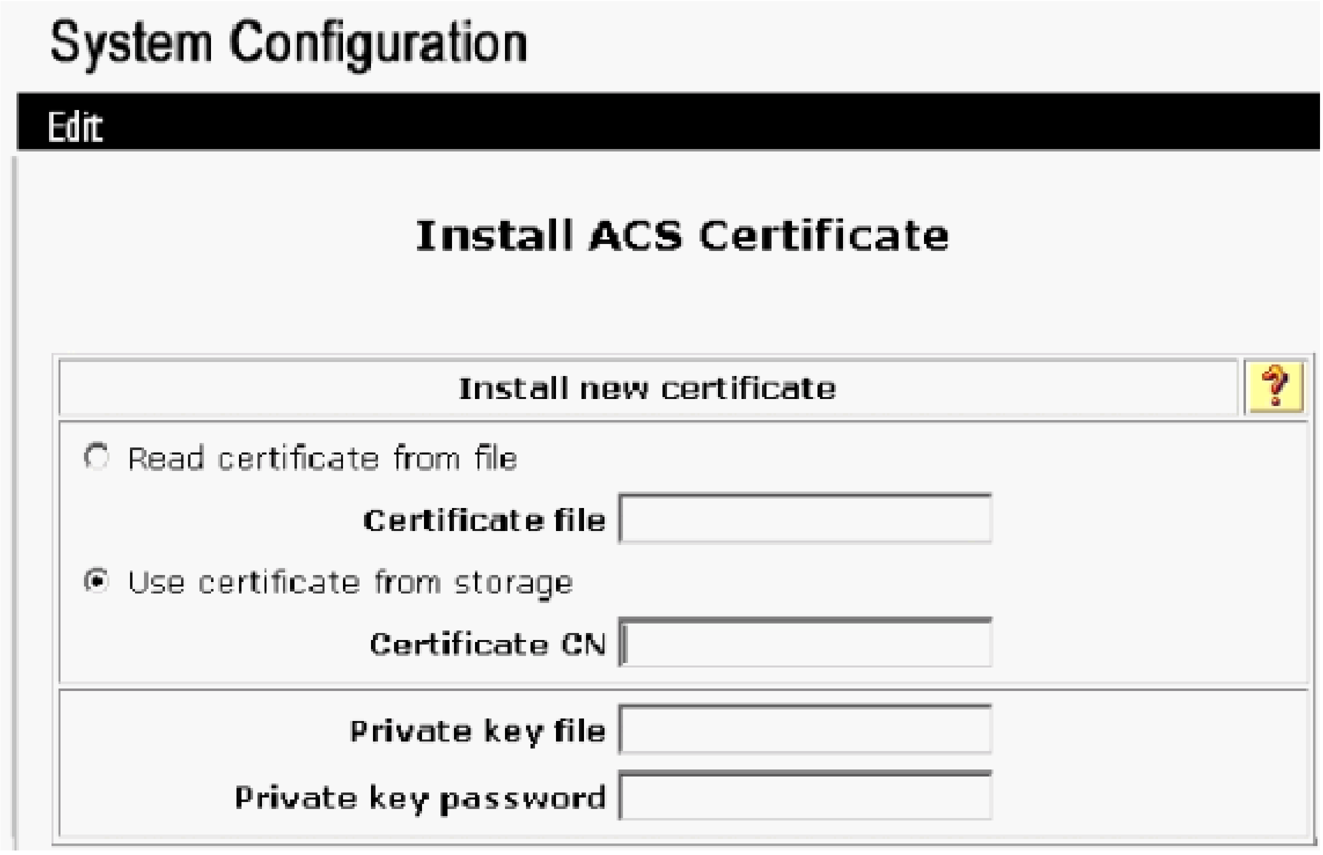
6. 从安装过程中创建的桌面快捷方式打开 **ACS Admin**。
7. 单击 **System Configuration**。



8. 单击 **ACS Certificate Setup**。


System Configuration
Select
ACS Certificate Setup
Install ACS Certificate
ACS Certification Authority Setup
Edit Certificate Trust List
Certificate Revocation Lists
Generate Certificate Signing Request
Generate Self-Signed Certificate
Cancel

9. 单击 Install ACS Certificate。

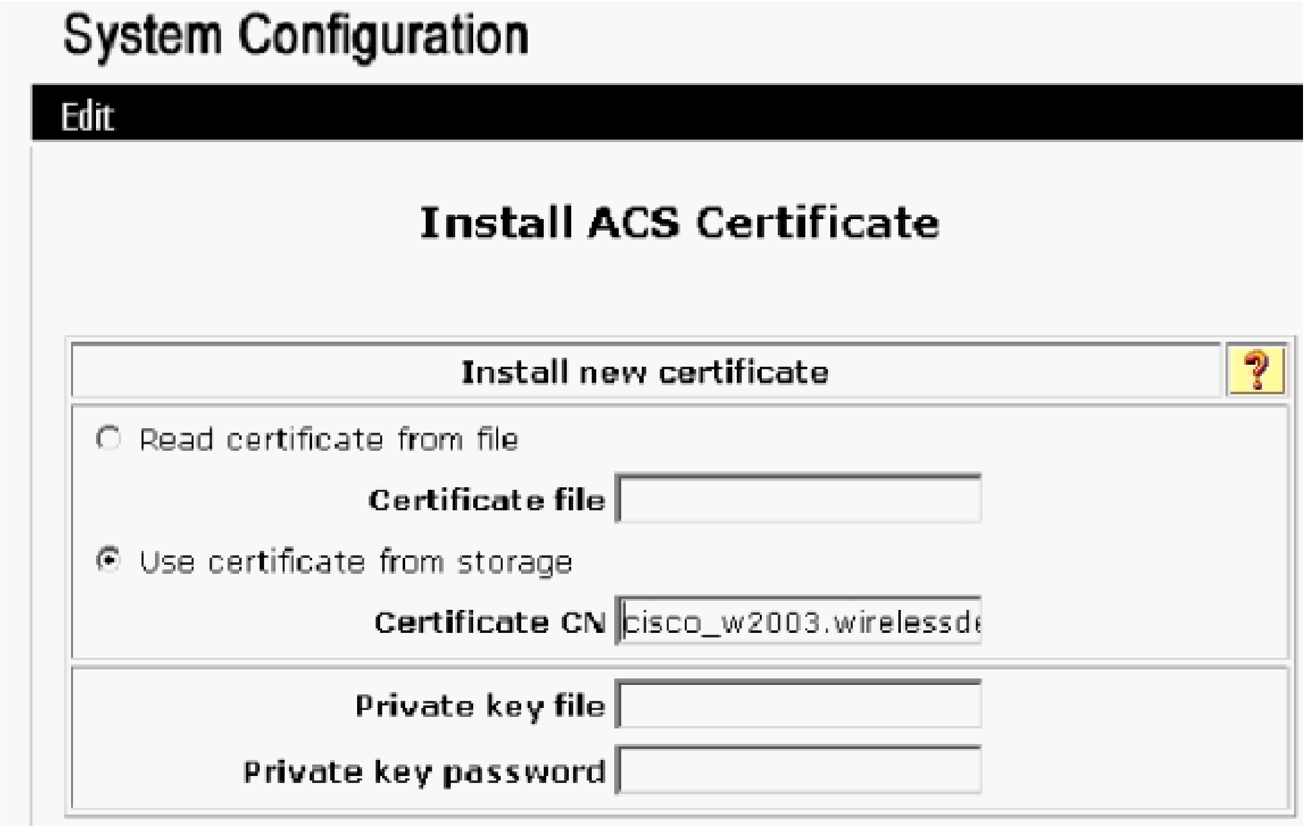

System Configuration

Edit

Install ACS Certificate

Install new certificate	
○ Read certificate from file	
Certificate file	
● Use certificate from storage	
Certificate CN	
Private key file	
Private key password	

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）。



System Configuration

Edit

Install ACS Certificate

Install new certificate

○ Read certificate from file

Certificate file

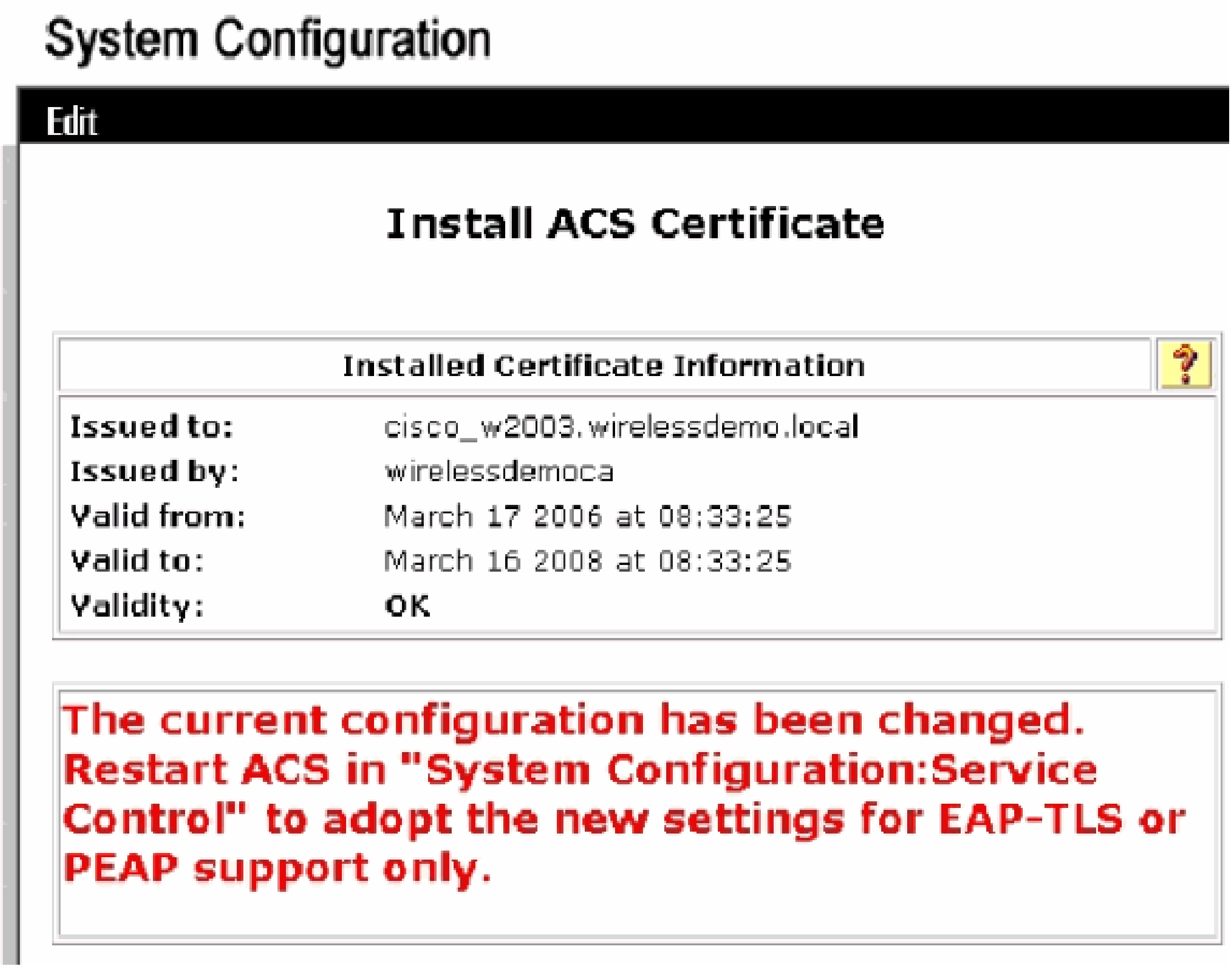
● Use certificate from storage

Certificate CN: cisco_w2003.wirelessde

Private key file

Private key password

11. 单击“Submit”。



System Configuration

Edit

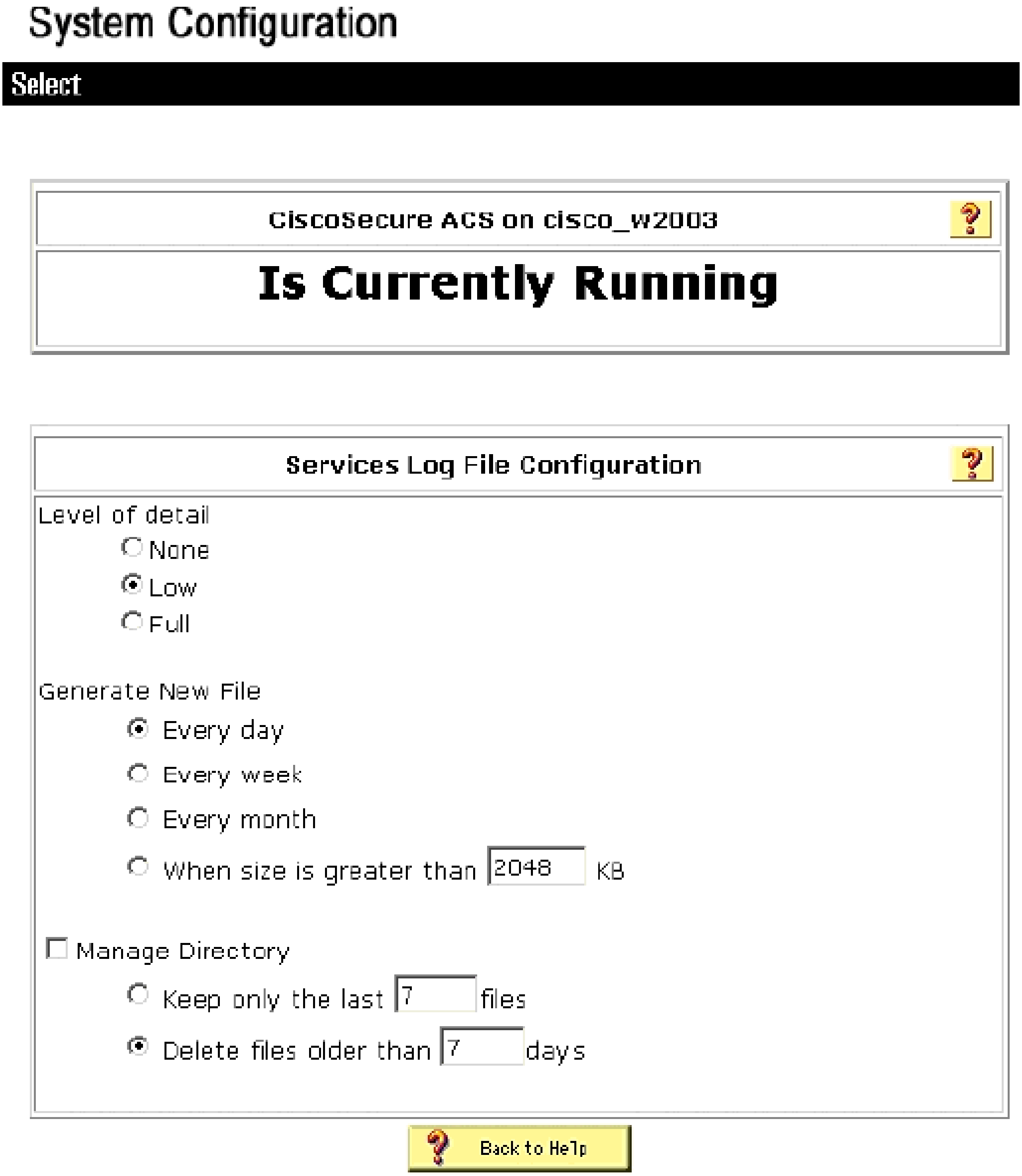
Install ACS Certificate

Installed Certificate Information

Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

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



System Configuration

Select

CiscoSecure ACS on cisco_w2003

Is Currently Running

Services Log File Configuration

Level of detail

○ None
● Low
○ Full

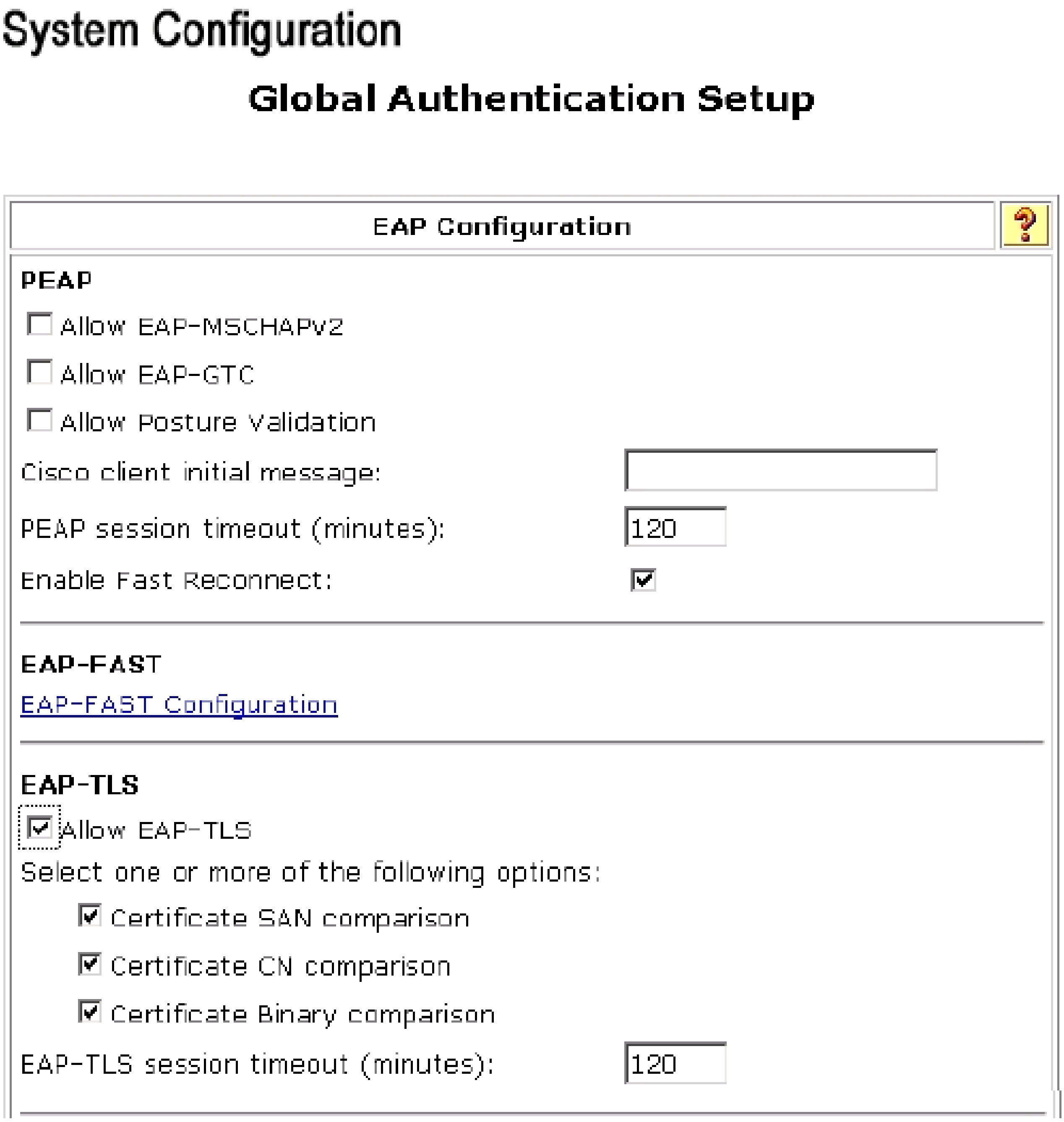
Generate New File

● Every day
○ Every week
○ Every month
○ When size is greater than 2048 KB

□ Manage Directory

○ Keep only the last 7 files
● Delete files older than 7 days

14. 单击 System Configuration。
15. 单击 Global Authentication Setup。
16. 选中Allow EAP-TLS和其下的所有框。



System Configuration

Global Authentication Setup

EAP Configuration

PEAP

□ Allow EAP-MSCHAPv2

□ Allow EAP-GTC

□ Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

EAP-FAST

EAP-FAST Configuration

EAP-TLS

☑ Allow EAP-TLS

Select one or more of the following options:

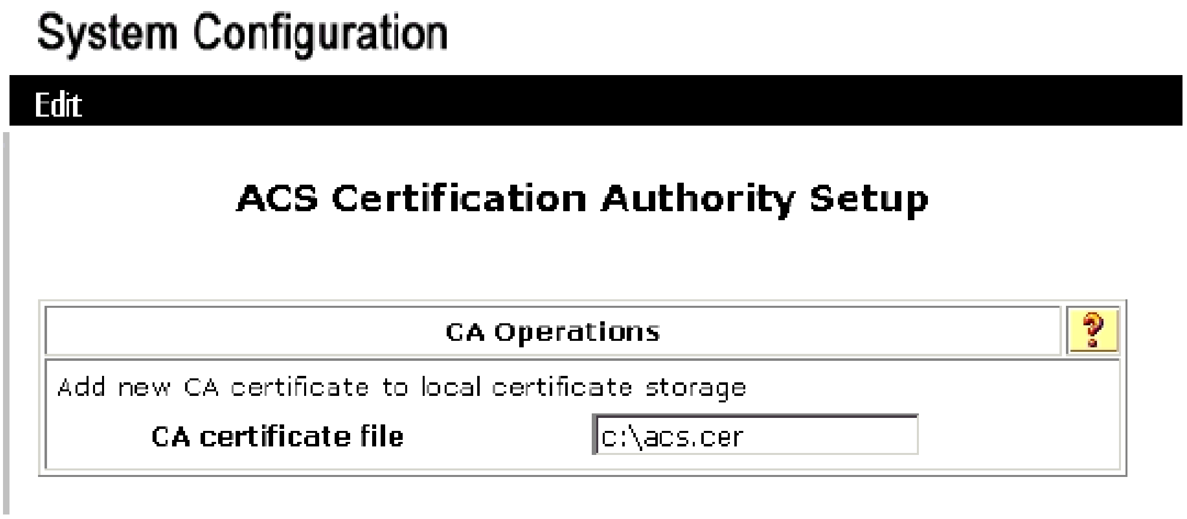
☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

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”。**

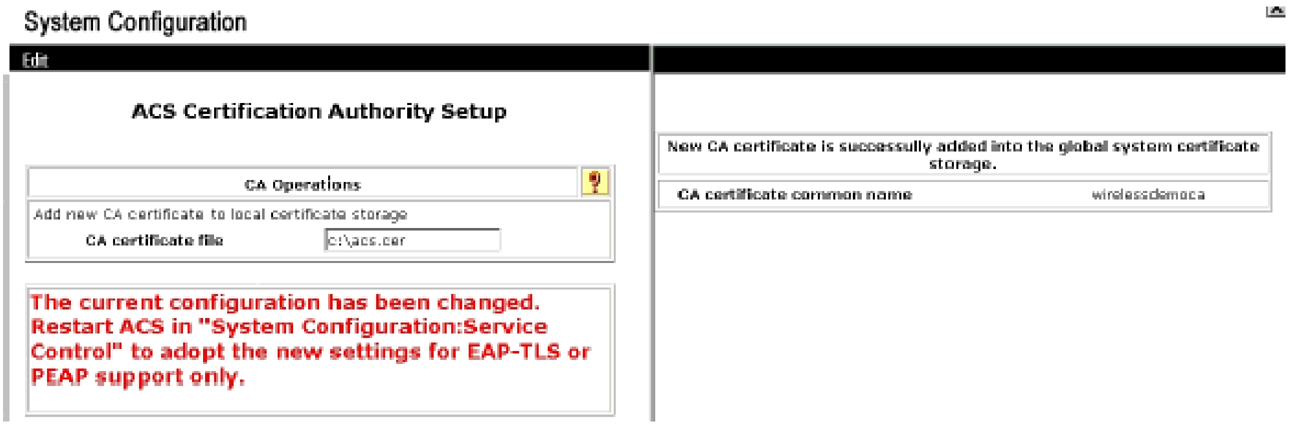


ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file: c:\acs.cer



ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file: c:\acs.cer

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

New CA certificate is successully added into the global system certificate storage.

CA certificate common name: wirelessdemoca

22. 重新启动 ACS 服务。

使用Windows零接触的EAP-TLS的客户端配置

CLIENT是运行Windows XP Professional和SP2的计算机，它充当无线客户端并通过无线AP访问内部网资源。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：

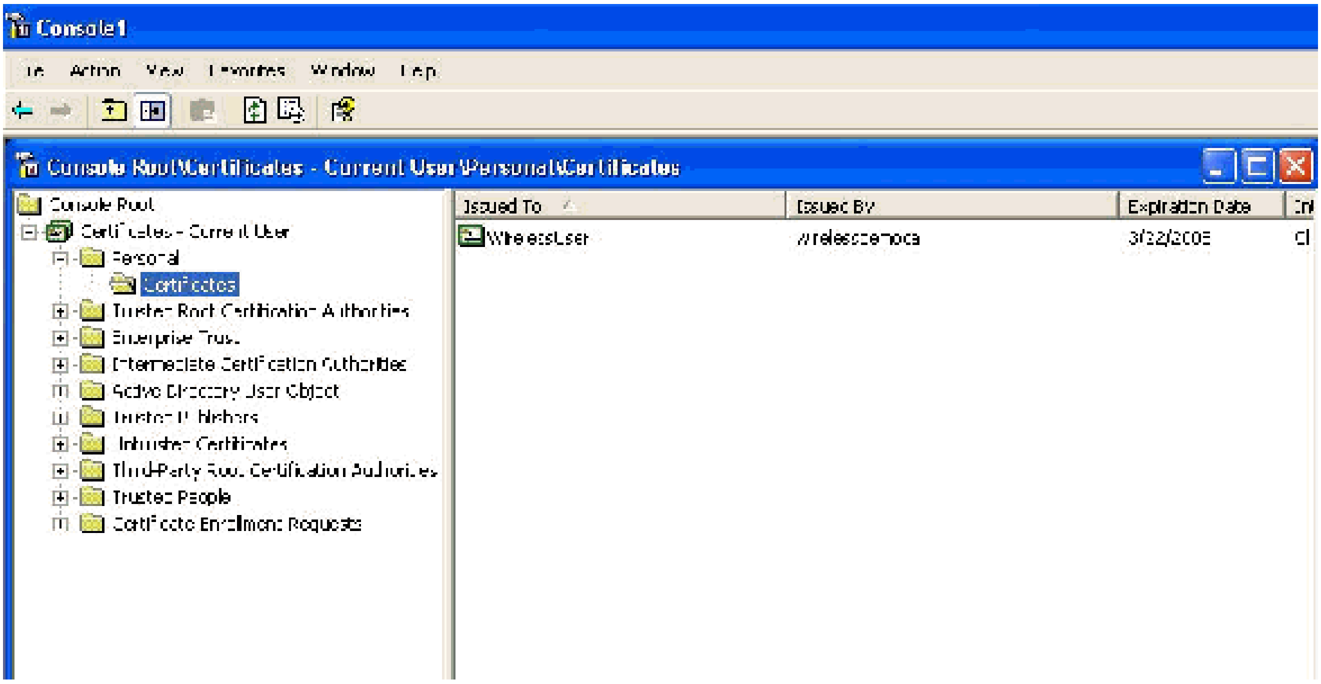
1. 使用连接到交换机的以太网电缆将客户端连接到内联网网段。
2. 在CLIENT上，将Windows XP Professional with SP2安装为wirelessdemo.local域上名为**CLIENT**的成员计算机。
3. 安装Windows XP Professional with SP2。必须安装此软件才能获得EAP-TLS和PEAP支持。**注意：**在Windows XP Professional with SP2中，Windows防火墙自动打开。请勿关闭防火墙。

配置无线网络连接

请完成以下步骤：

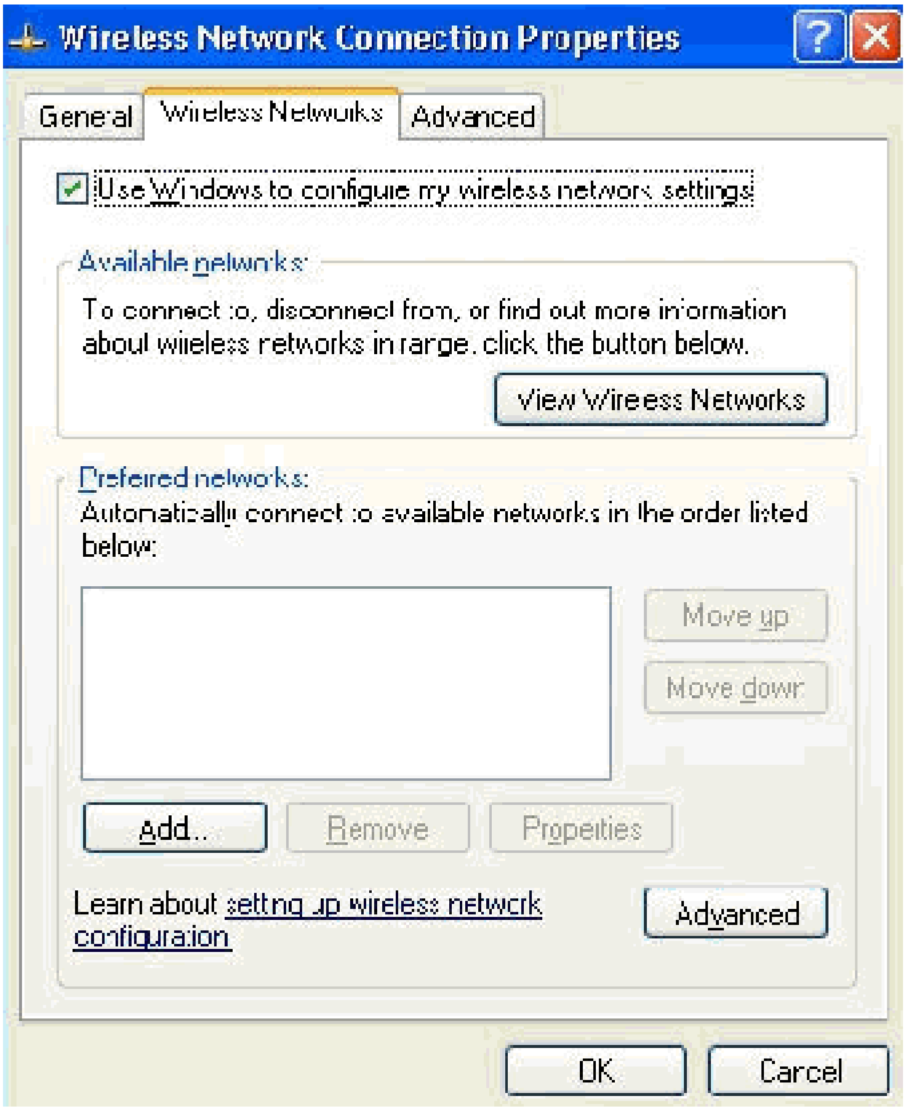
1. 注销，然后使用 wirelessdemo.local 域中的 WirelessUser 帐户重新登录。**注意：在**命令提示符下键入gpupdate，立即更新计算机和用户配置组策略设置并获取无线客户端计算机的计算机和**用户**证书。否则，当您注销然后登录时，它将执行与gpupdate相同的**功能**。您必须通过电线

连接登录域。**注意：**要验证证书是否自动安装在客户端上，请打开证书MMC并验证WirelessUser证书是否在“个人证书”文件夹中可用。


Console1
File Action View Favorites Window Help
Console Root\Certificates - Current User\Personal\Certificates
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date	Int
WirelessUser	wirelessdemoca	3/22/2008	Cl

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**Properties**，转到Wireless Networks选项卡，并确保选**中User Windows以配置我的无线网络**设置。



☑ Use Windows to configure my wireless network settings

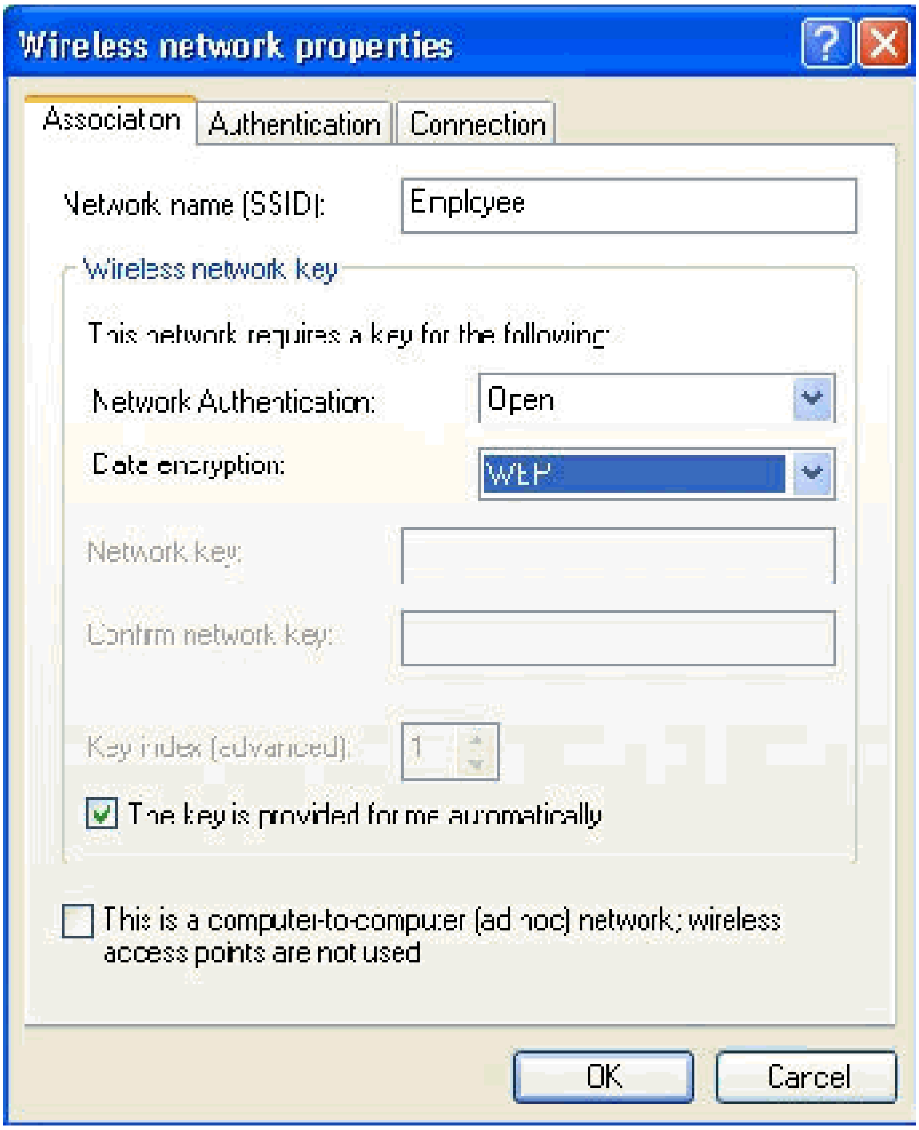
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration

4. 单击 **Add**。

5. 转到Association选项卡，在Network name(SSID)(网络名称(SSID))字段中键入**Employee。**
6. 确保Data Encryption（数据加密）设**置为WEP,并选中The key is provided for me automatically(自动为我提供密**钥)。



Network name (SSID): Employee

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

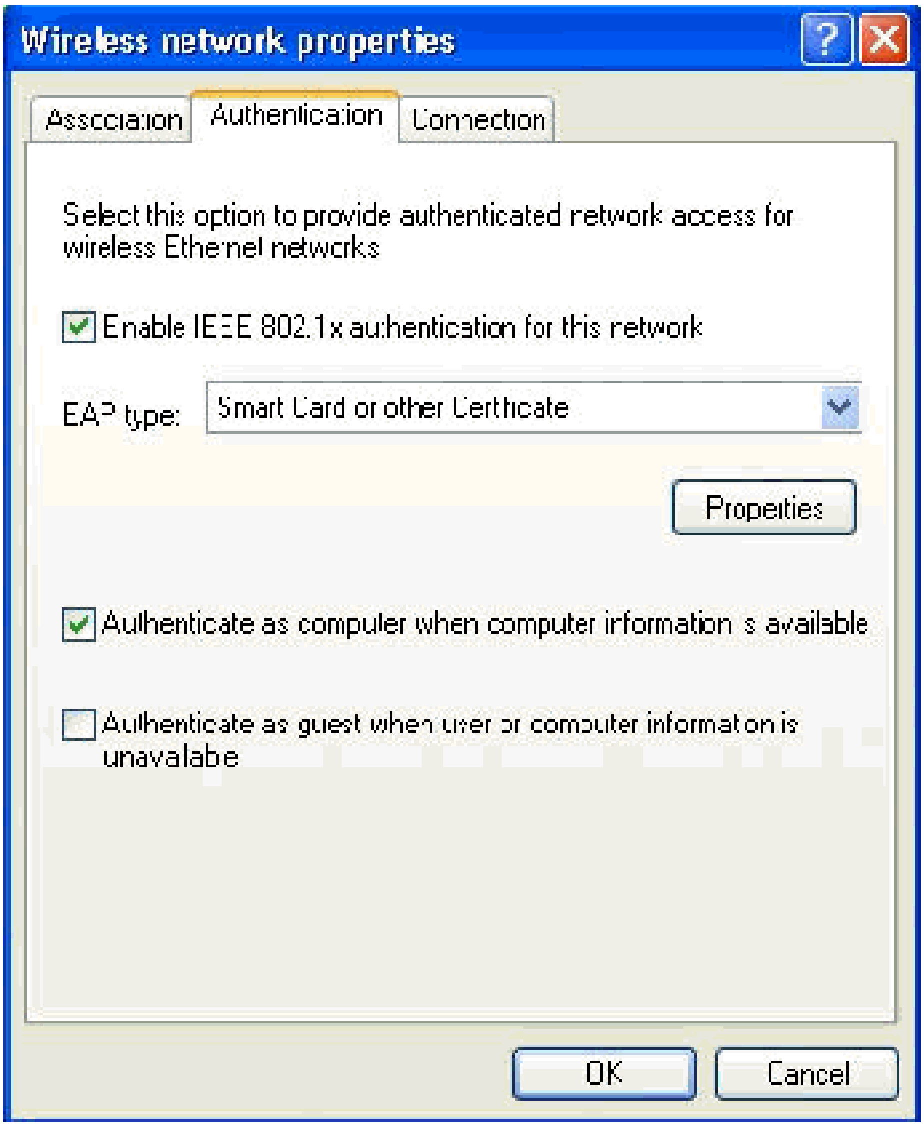
Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

7. 转至“身份验证”选项卡。
8. 验证EAP类型是否配置为使用智**能卡或其他证书**。如果不是，请从下拉菜单中选择此选项。
9. 如果希望在登录之前对计算机进行身份验证（允许应用登录脚本或组策略推送），请选择选项 **Authenticate as computer when computer information available**。



Select this option to provide authenticated network access for wireless Ethernet networks

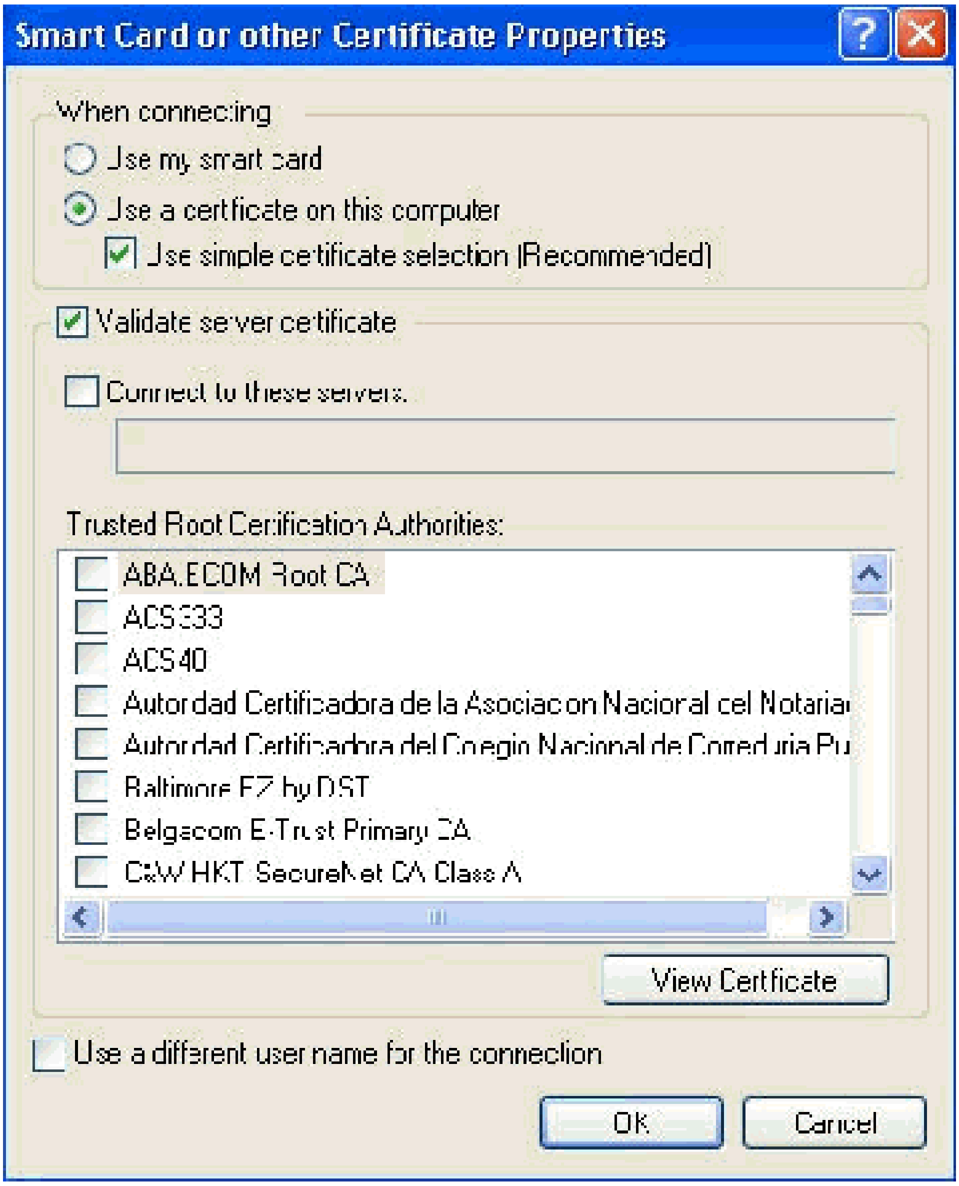
☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

10. 单击 **Properties**。
11. 确保选中此窗口中的框。



Smart Card or other Certificate Properties

When connecting

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

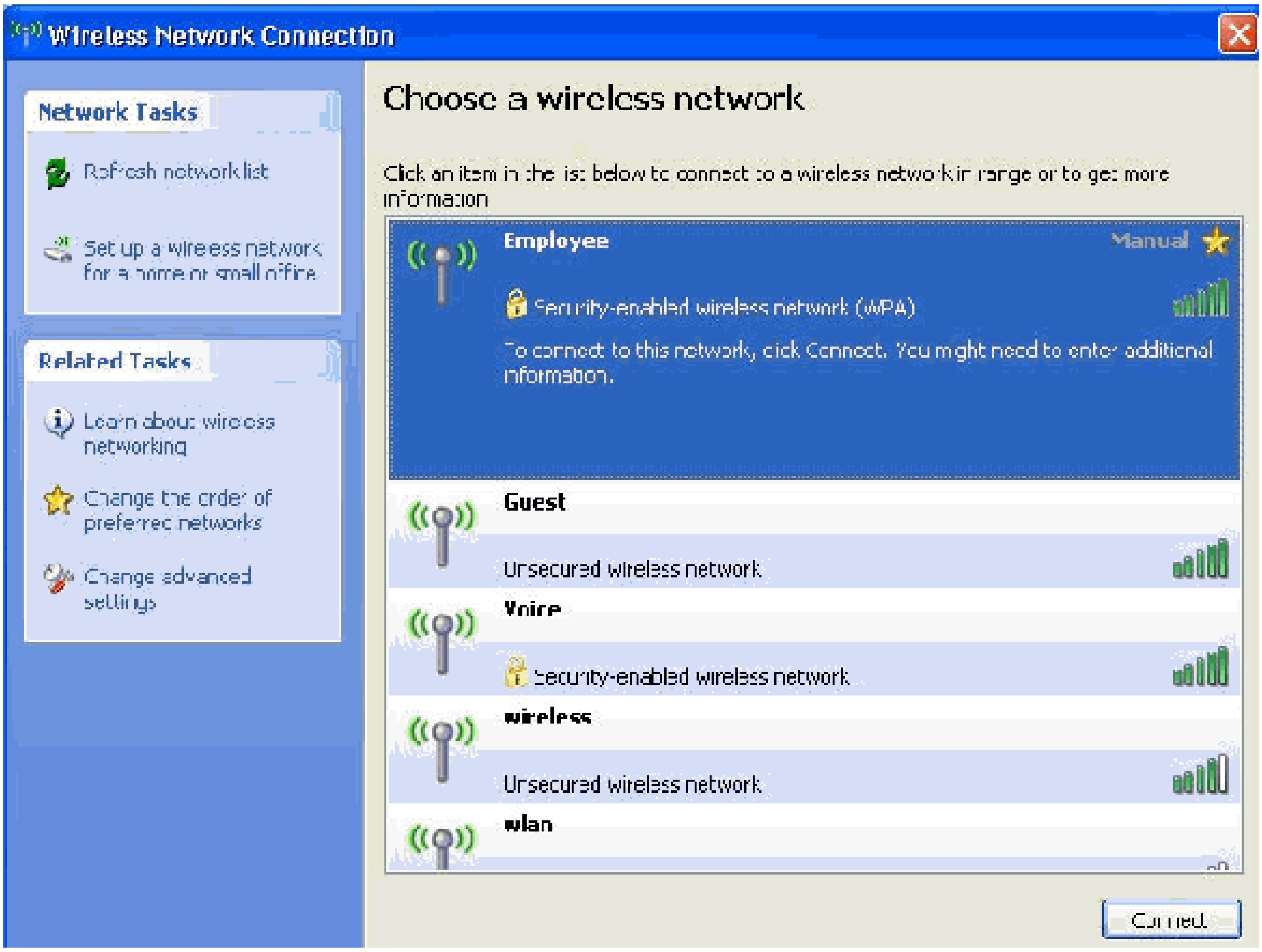
□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ ACS333
□ ACS40
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A

□ Use a different user name for the connection

12. 单击 **OK 三次。**
13. 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。**
14. 单击 **Employee 无线网络并单击“连接”。**



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 — Manual ★
Security-enabled wireless network (WPA)
To connect to this network, click Connect. You might need to enter additional information.

Guest
Unsecured wireless network

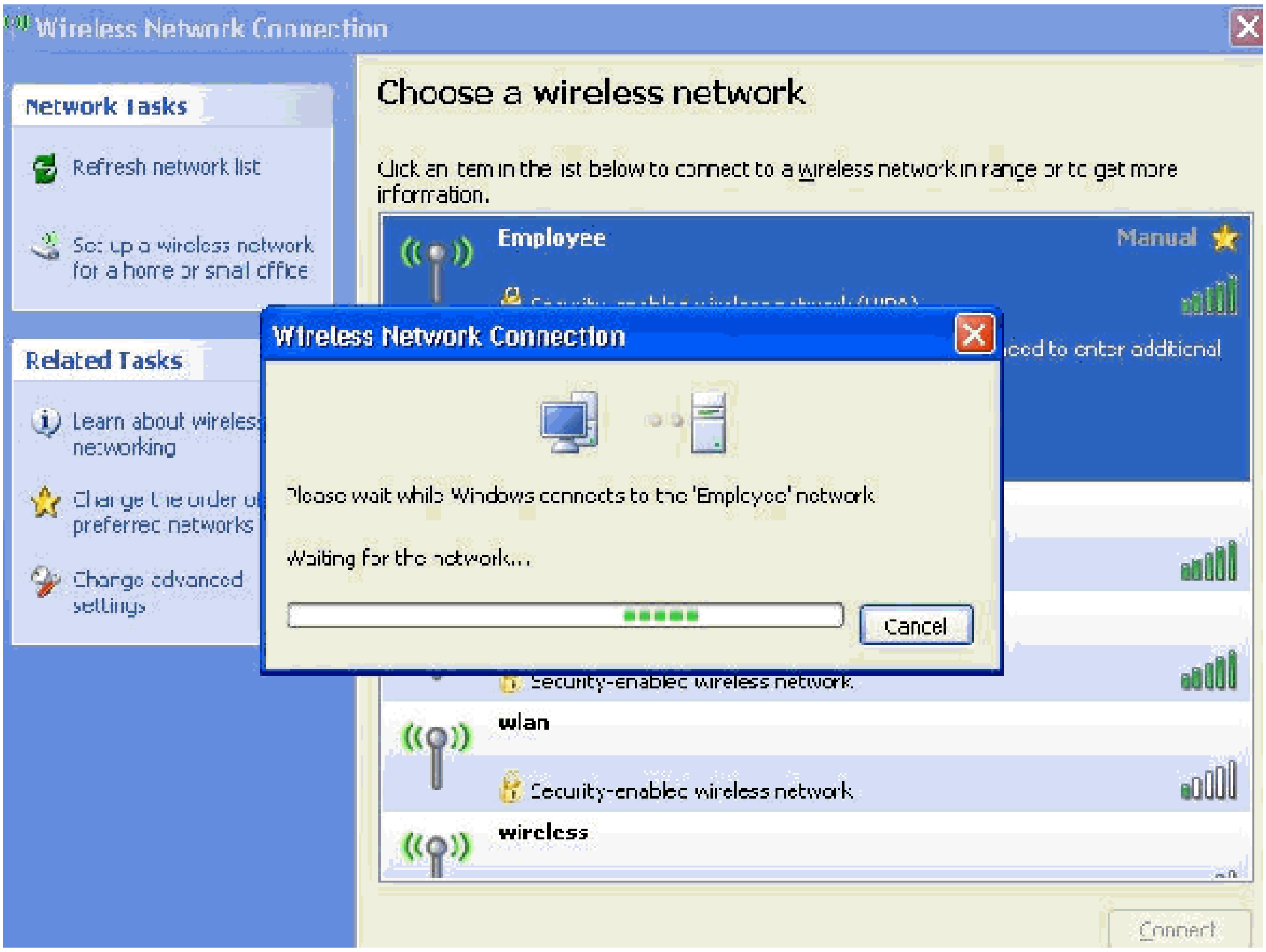
Voice
Security-enabled wireless network

wireless
Unsecured wireless network

wlan

Connect

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 — Manual ★
Security-enabled wireless network (WPA)
…need to enter additional…

Wireless Network Connection

Please wait while Windows connects to the 'Employee' network.

Waiting for the network...

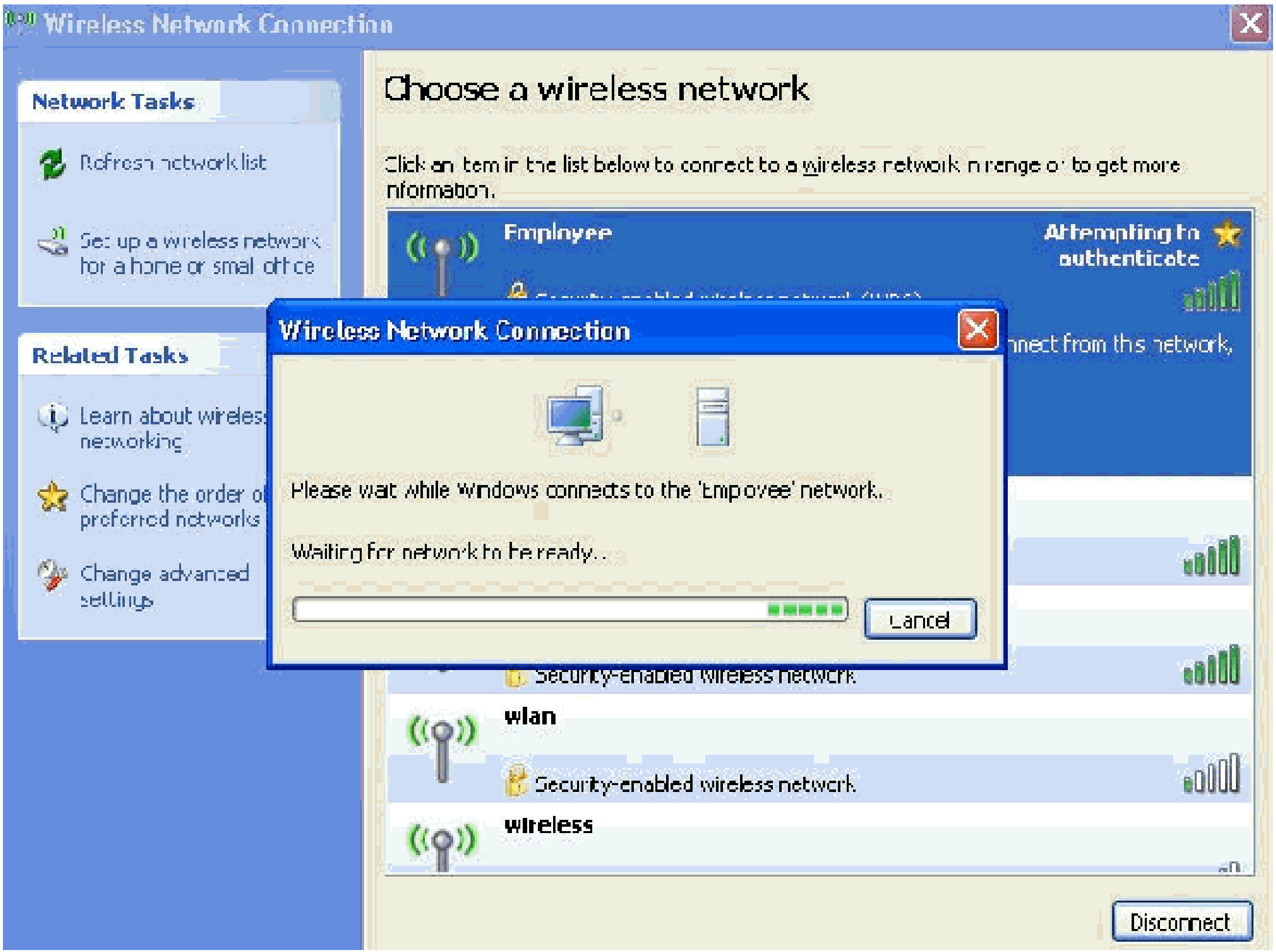
Cancel

Security-enabled wireless network

wlan
Security-enabled wireless network

wireless

Connect



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
Employee
Attempting to authenticate
wlan
wireless
Cancel
Disconnect

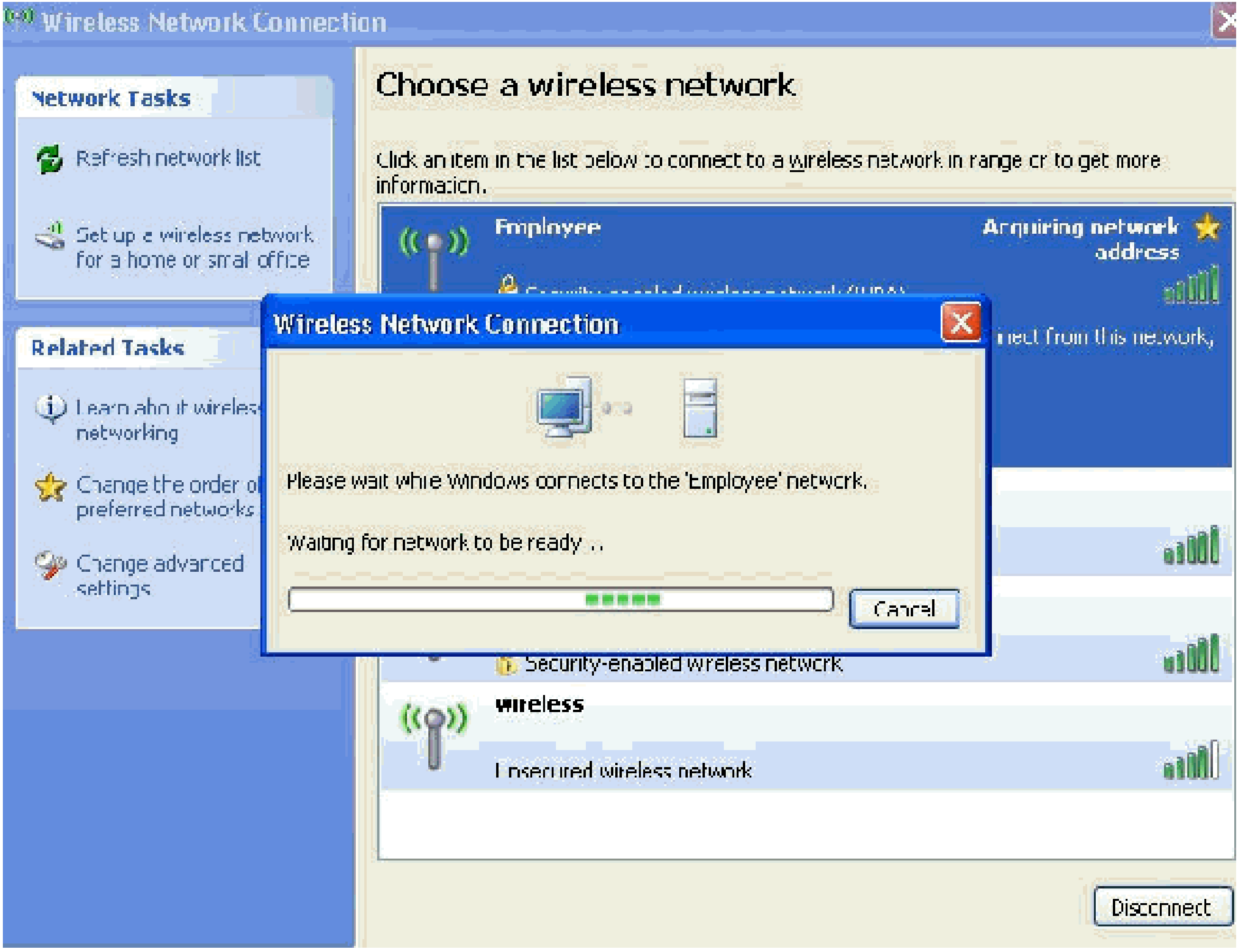
Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Security-enabled wireless network

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...



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
Employee
Acquiring network address
wireless
Cancel
Disconnect

Choose a wireless network

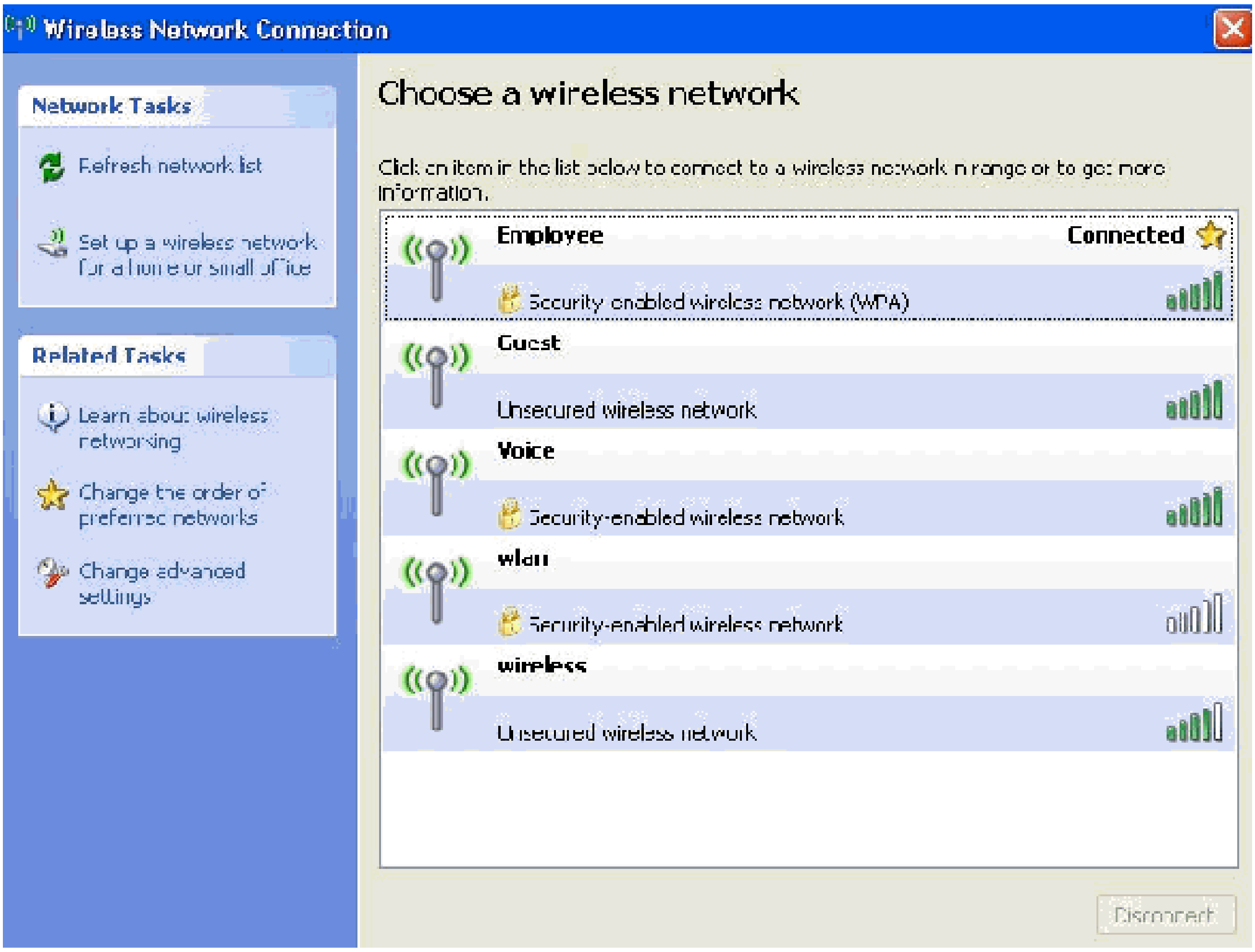
Click an item in the list below to connect to a wireless network in range or to get more information.

Security-enabled wireless network

Unsecured wireless network

Please wait while Windows connects to the 'Employee' network.

Waiting for network to be ready...


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
Disconnect

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 — Connected
Security-enabled wireless network (WPA)

Guest
Unsecured wireless network

Voice
Security-enabled wireless network

wlan
Security-enabled wireless network

wireless
Unsecured wireless network

15. 身份验证成功后，使用网络连接检查无线适配器的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。
16. 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）**。

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