使用ACS 5.1和Windows 2003 Server的UWN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) 5.1，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) 版本 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

我们假设安装者已掌握安装 Windows 2003 和 Cisco 无线局域网控制器的基本知识，因为本文档仅涵盖有助于开展测试的特定配置。

有关 Cisco 5508 系列控制器的初始安装和配置方面的信息，请参阅 Cisco 5500 系列无线控制器安装指南。有关Cisco 2100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 2100系列无线LAN控制器。

有关 Microsoft Windows 2003 安装和配置指南，请访问安装 Windows Server 2003 R2 。

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

此外还会用到 Windows Server 2003 Enterprise Edition SP1，以便配置自动注册用户功能以及进行 PEAP 身份验证所需的工作站证书。证书自动注册和自动续订功能可用于续订证书以及让证书自动过期，因此可以方便证书的部署并提高安全性。

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 7.0.98.0 的 Cisco 2106 或 5508 系列控制器
- Cisco 1142 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
- Cisco 1121 安全访问控制系统设备 (ACS) 5.1
- 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 3750 交换机

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

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

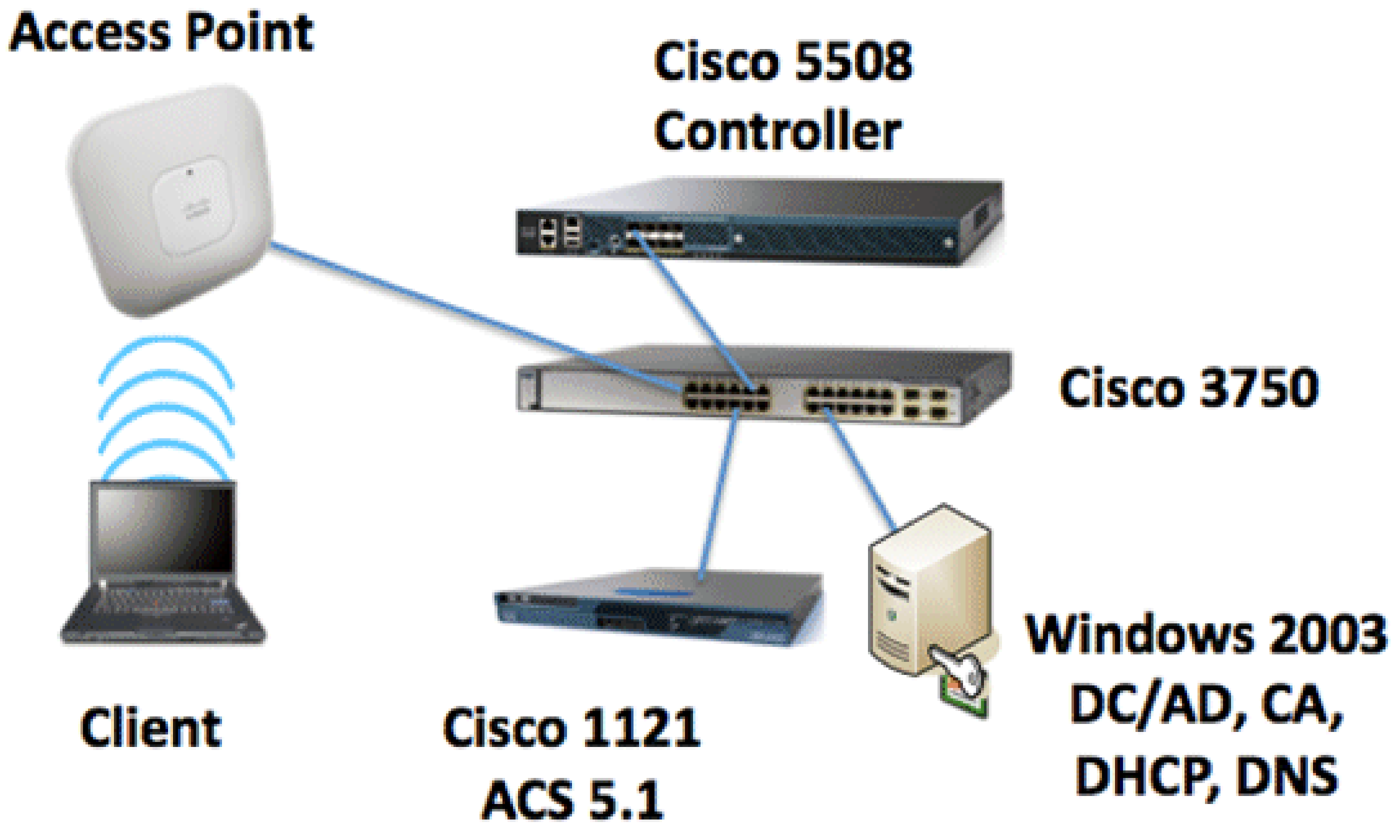
本部分提供有关如何配置本文档所述功能的信息。

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

网络图

本文档使用以下网络设置：

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 5.1 和 Windows 2003 Enterprise 服务器的统一无线网络下实施 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。

注意：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 Windows XP Professional with SP，请参阅适用于带Service Pack 2的Windows XP的WPA2/无线调配服务信息元素(WPS IE)更新。

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

CA (democa)

CA 是一台运行 Windows Server 2003 Enterprise Edition SP2 的计算机，该计算机担当以下角色：

- **demo.local 域的域控制器，运行 IIS**
- **demo.local DNS 域的 DNS 服务器**
- DHCP 服务器
- **demo.local 域的企业根 CA**

要为这些服务配置 CA，请执行以下步骤：

执行基本安装和配置

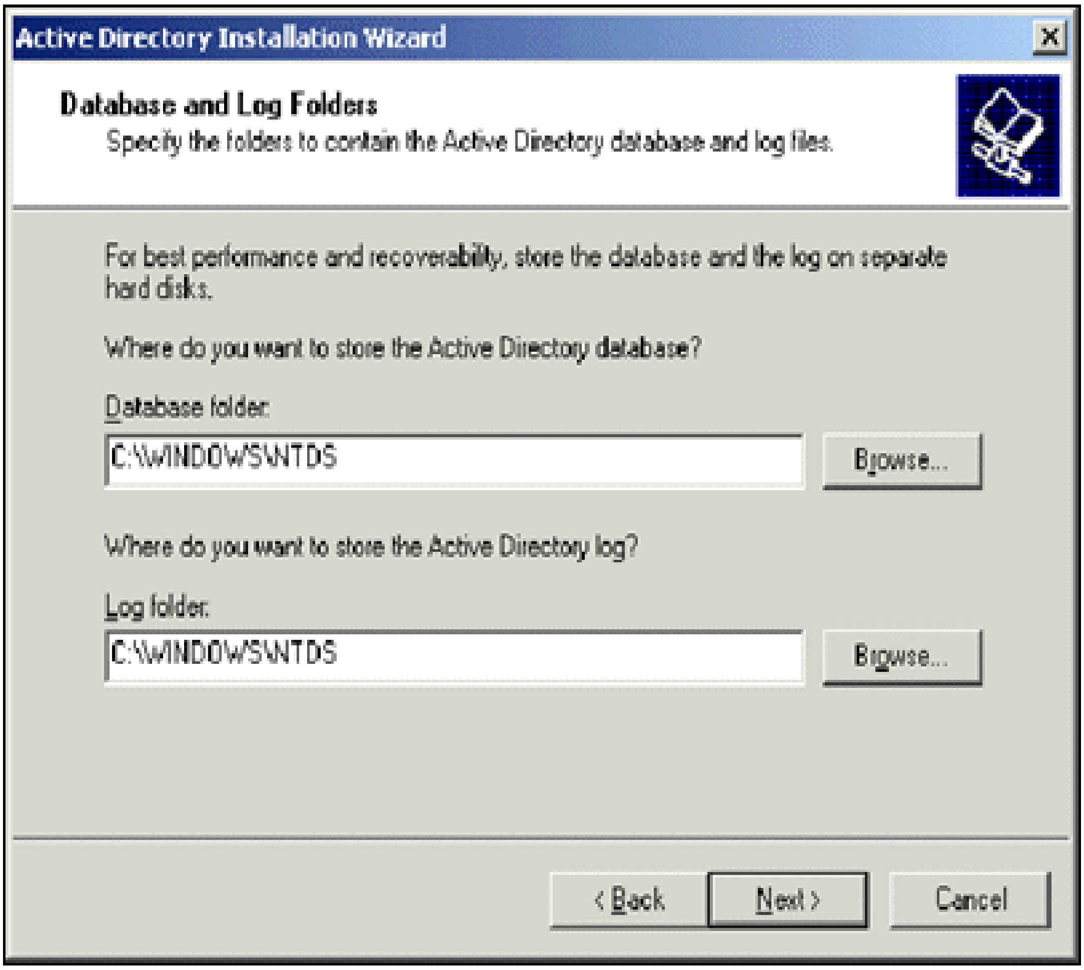
请执行以下步骤：

1. 将 Windows Server 2003 Enterprise Edition SP2 安装为独立服务器。
2. 用 IP 地址 *10.0.10.10 和子网掩码 255.255.255.0* 配置 TCP/IP 协议。

将计算机配置为域控制器

请执行以下步骤：

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 **demo.local，然后单击**下一步。
8. 在“NetBIOS 域名”页上，键入 NetBIOS 域名 **demo，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:

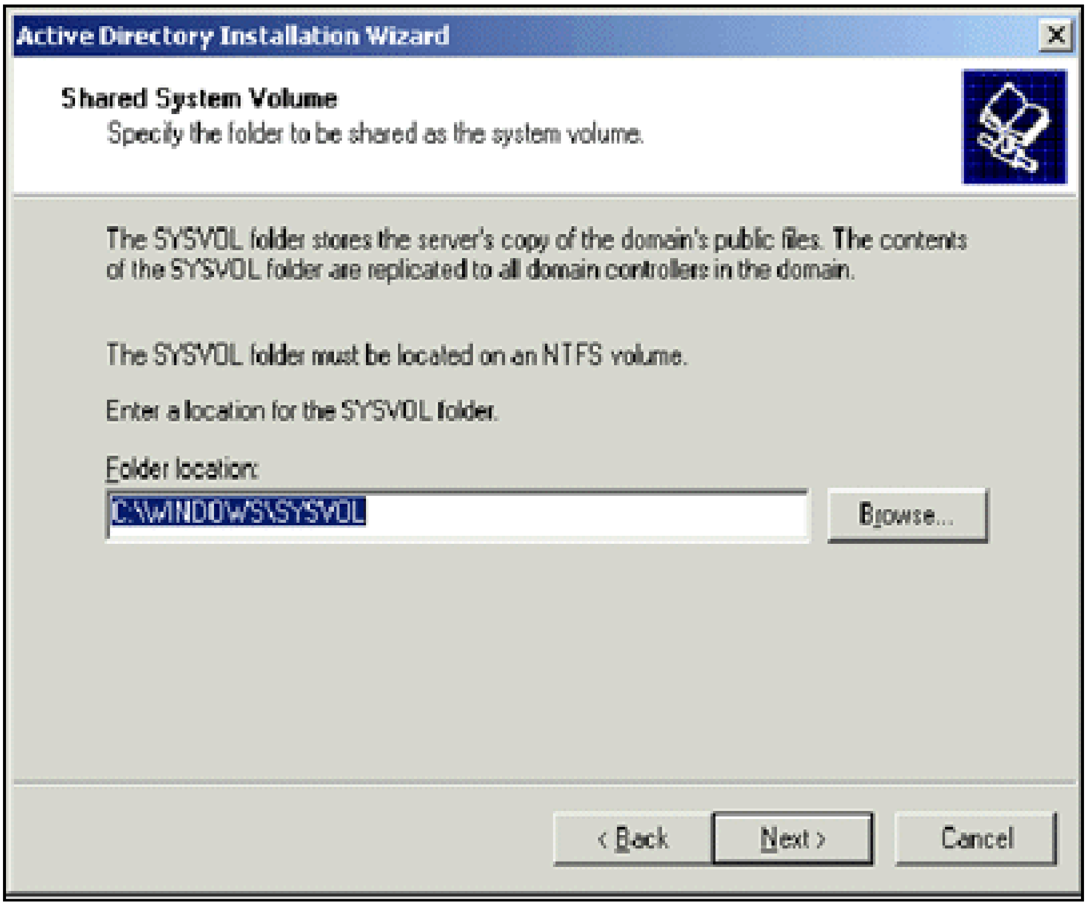
C:\WINDOWS\NTDS

Where do you want to store the Active Directory log?

Log folder:

C:\WINDOWS\NTDS

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



Active Directory Installation Wizard

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.

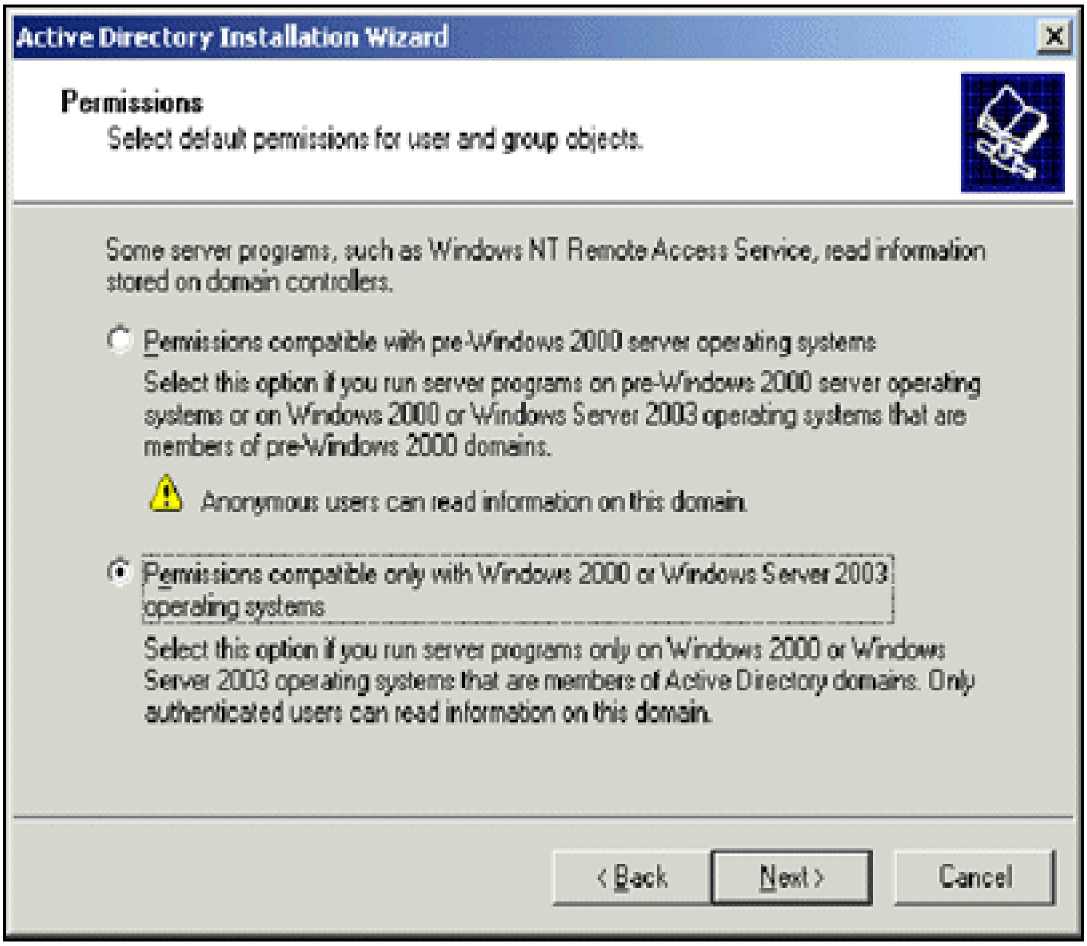
The SYSVOL folder must be located on an NTFS volume.

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”。**



Active Directory Installation Wizard

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

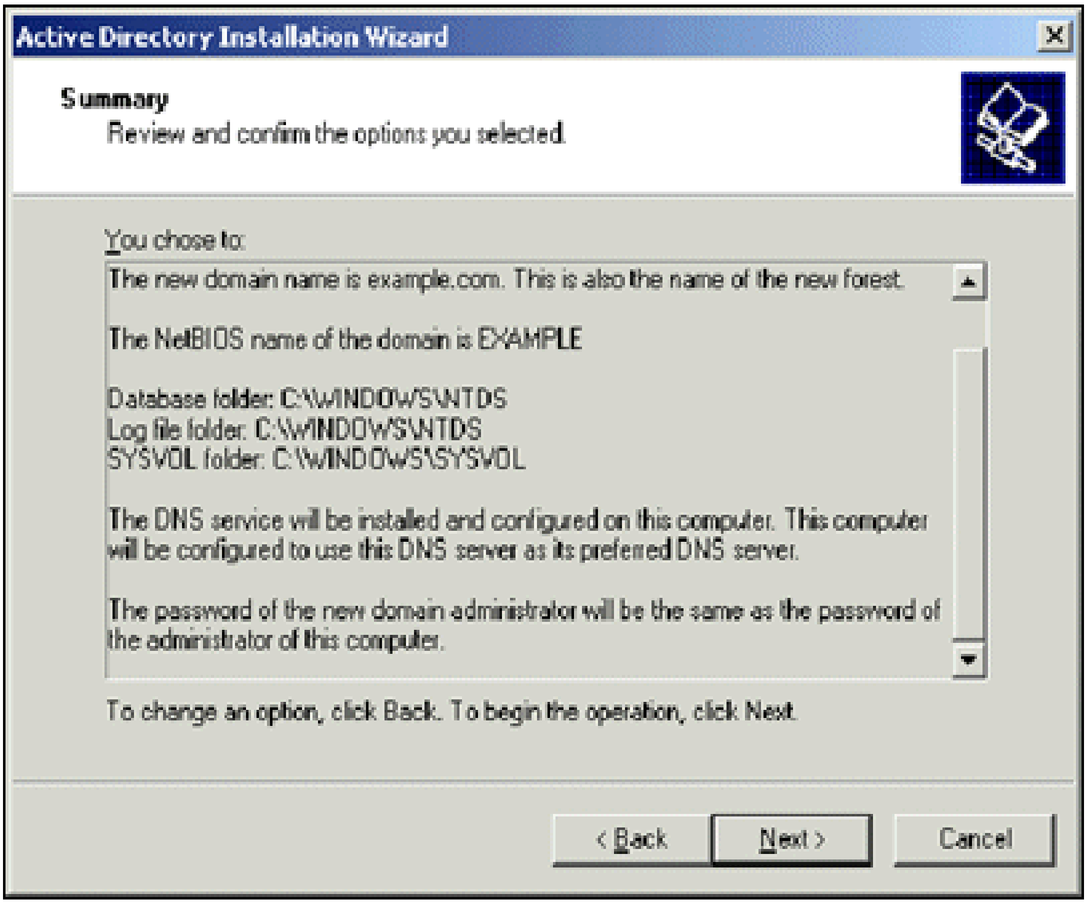
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.

⚠ 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.

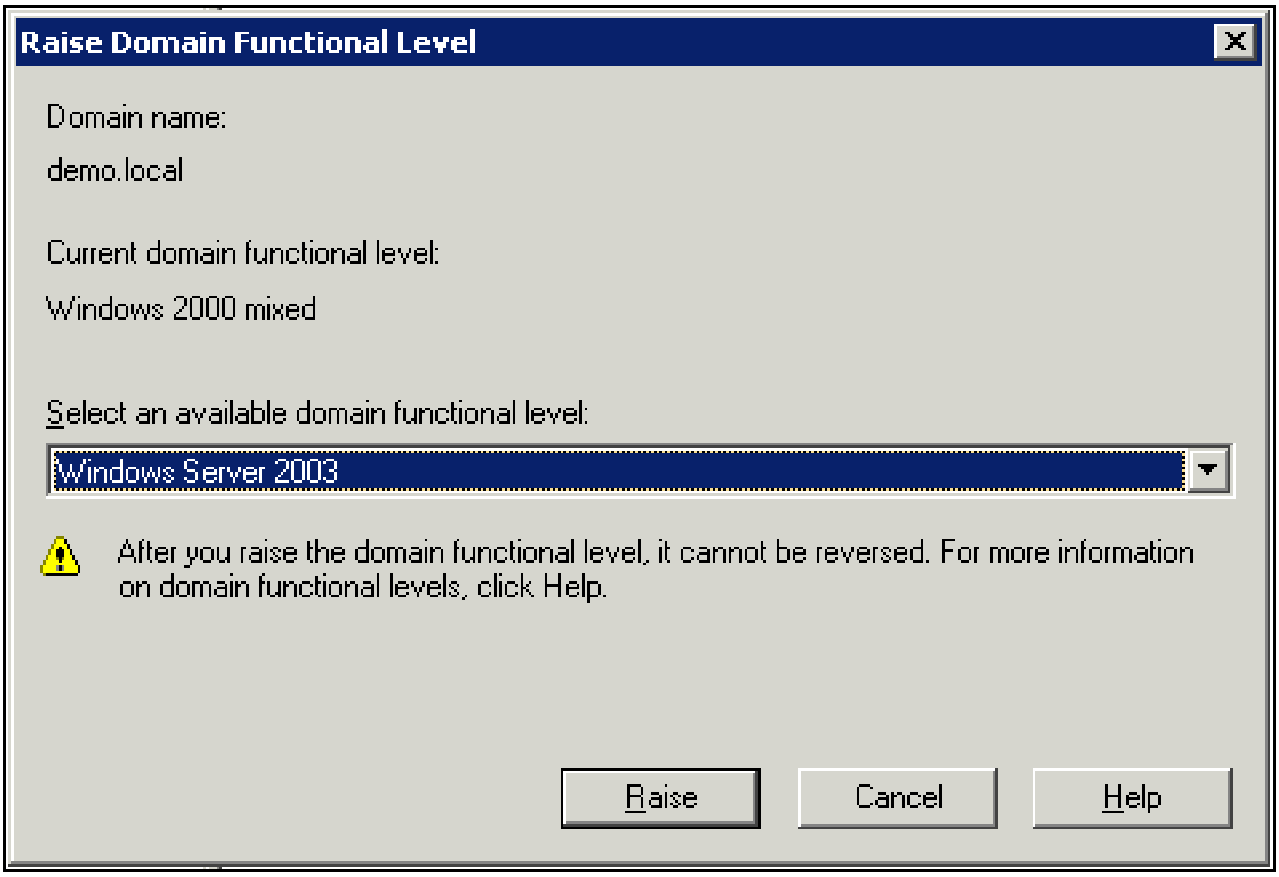
To change an option, click Back. To begin the operation, click Next.

14. 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**。

提升域功能级别

请执行以下步骤：

1. 从**管理工具文件夹打开 Active Directory 域和信任关系管理单元（“开始”>“程序”>“管理工具”>“Active Directory 域和信任关系”**），然后右键单击域计算机 **CA.demo.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:

demo.local

Current domain functional level:

Windows 2000 mixed

Select an available domain functional level:

Windows Server 2003

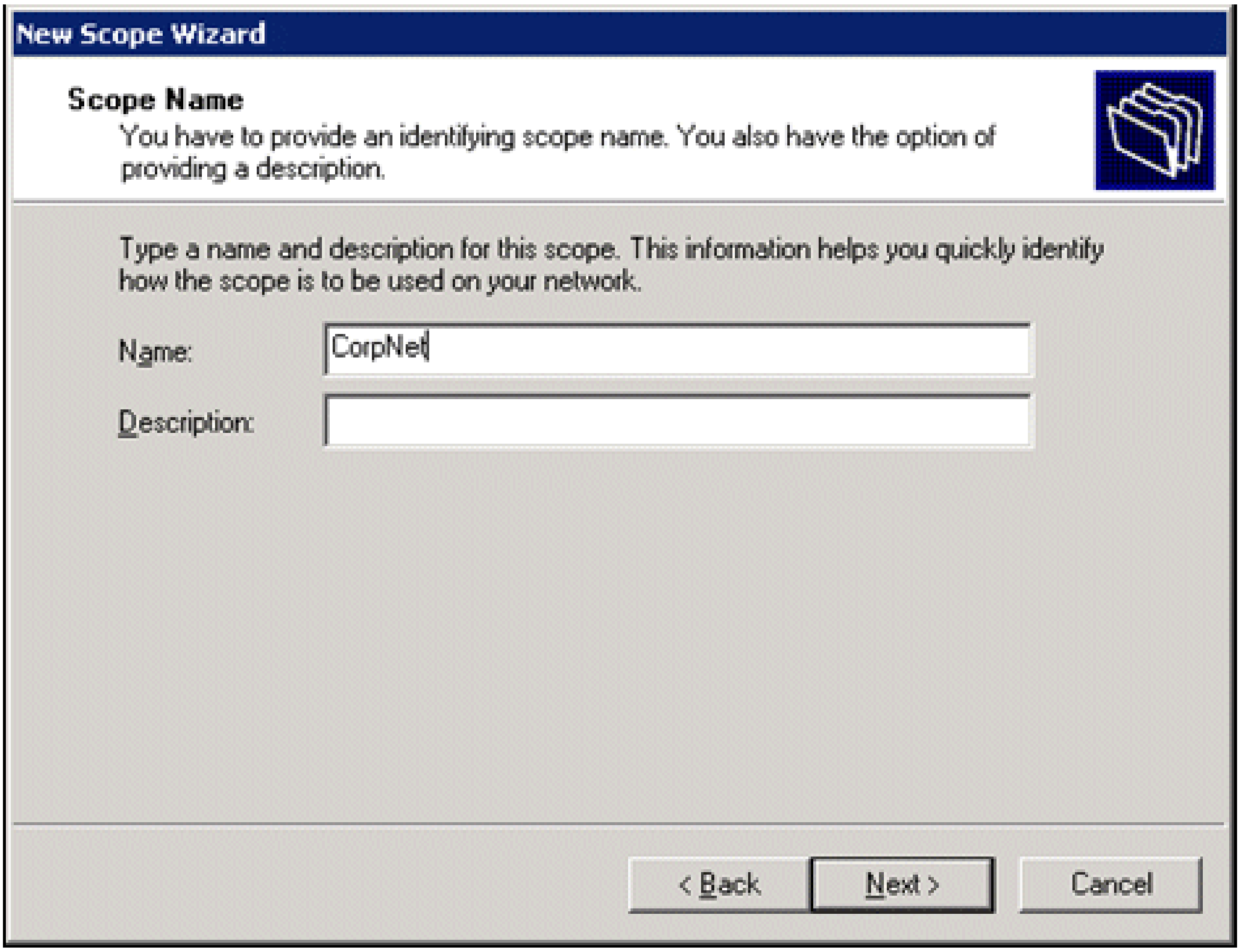
After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help.

3. 单击**提升**，单击“确定”，然后再次单击“确定”。

安装并配置 DHCP

请执行以下步骤：

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 **CA.demo.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 **CA.demo.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。**



New Scope Wizard

Scope Name

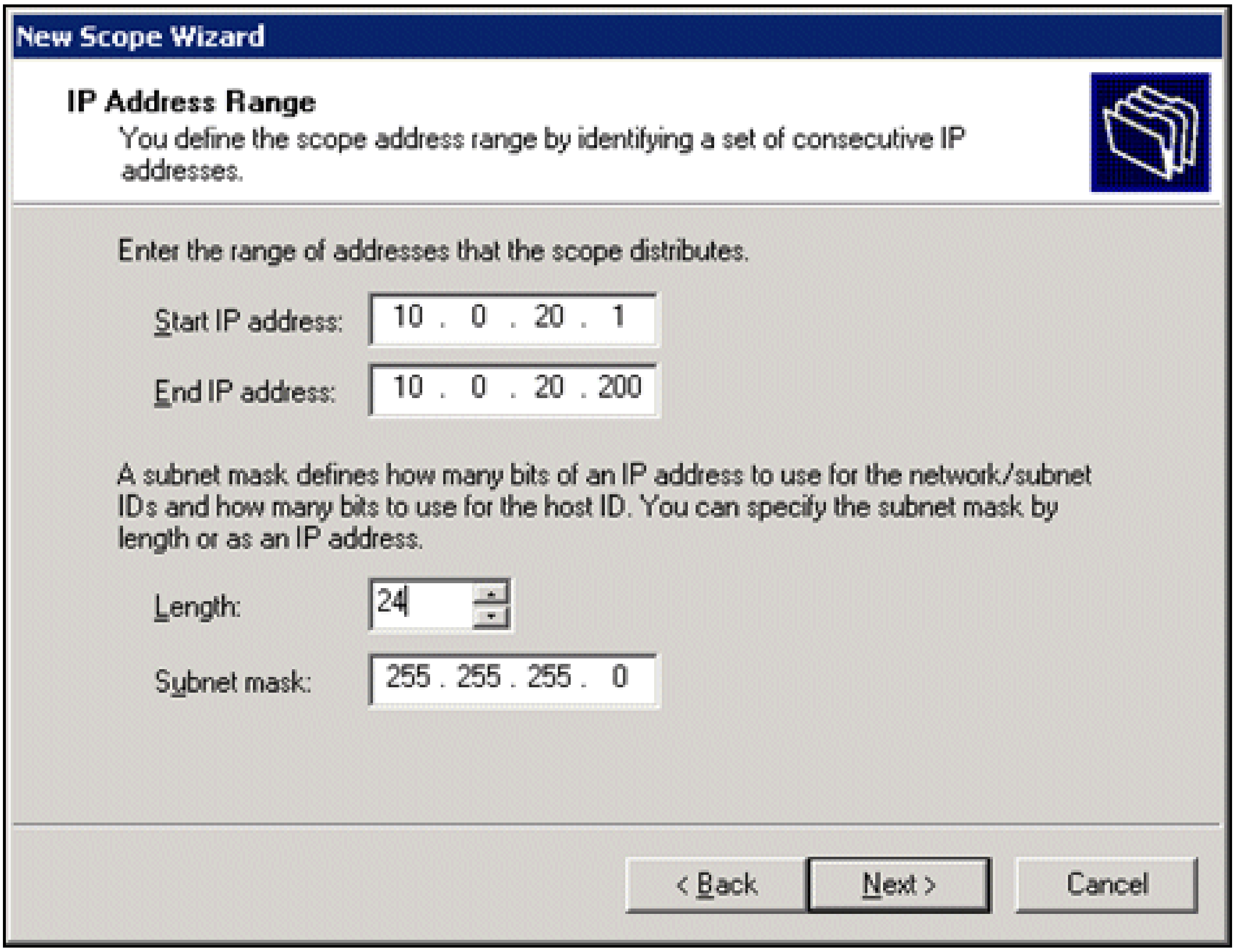
You have to provide an identifying scope name. You also have the option of providing a description.

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 - **10.0.20.1**结束 IP 地址 - **10.0.20.200**长度 - **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: 10 . 0 . 20 . 1

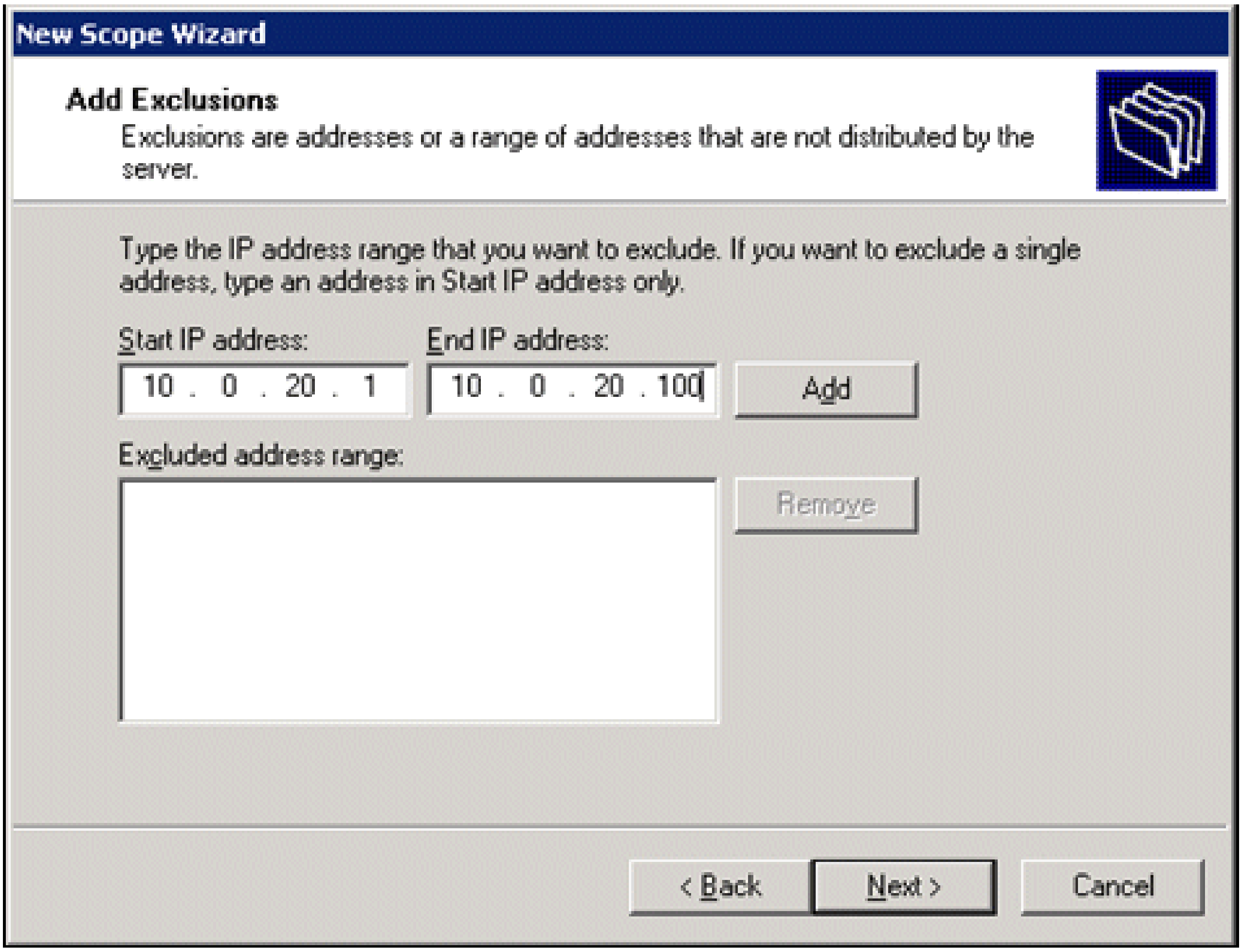
End IP address: 10 . 0 . 20 . 200

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，然后输入** *10.0.20.1 作为要排除的“起始 IP 地址”*，**输入** *10.0.20.100 作为要排除的“结束 IP 地址”*。然后，单击**下一步**。这将保留从 10.0.20.1 到 10.0.20.100 范围内的 IP 地址。这些保留的 IP 地址不会被 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.

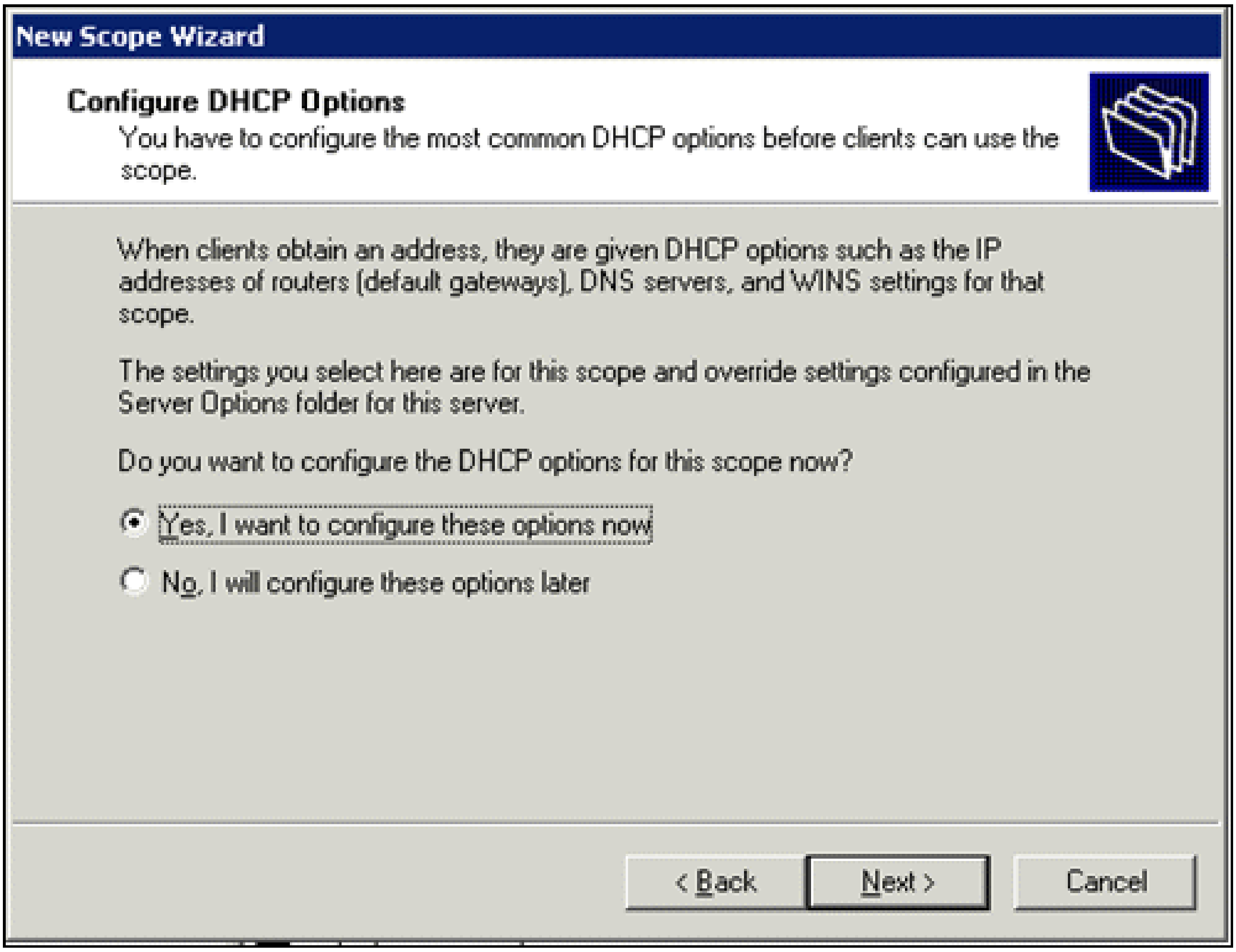
Start IP address: 10 . 0 . 20 . 1

End IP address: 10 . 0 . 20 . 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.

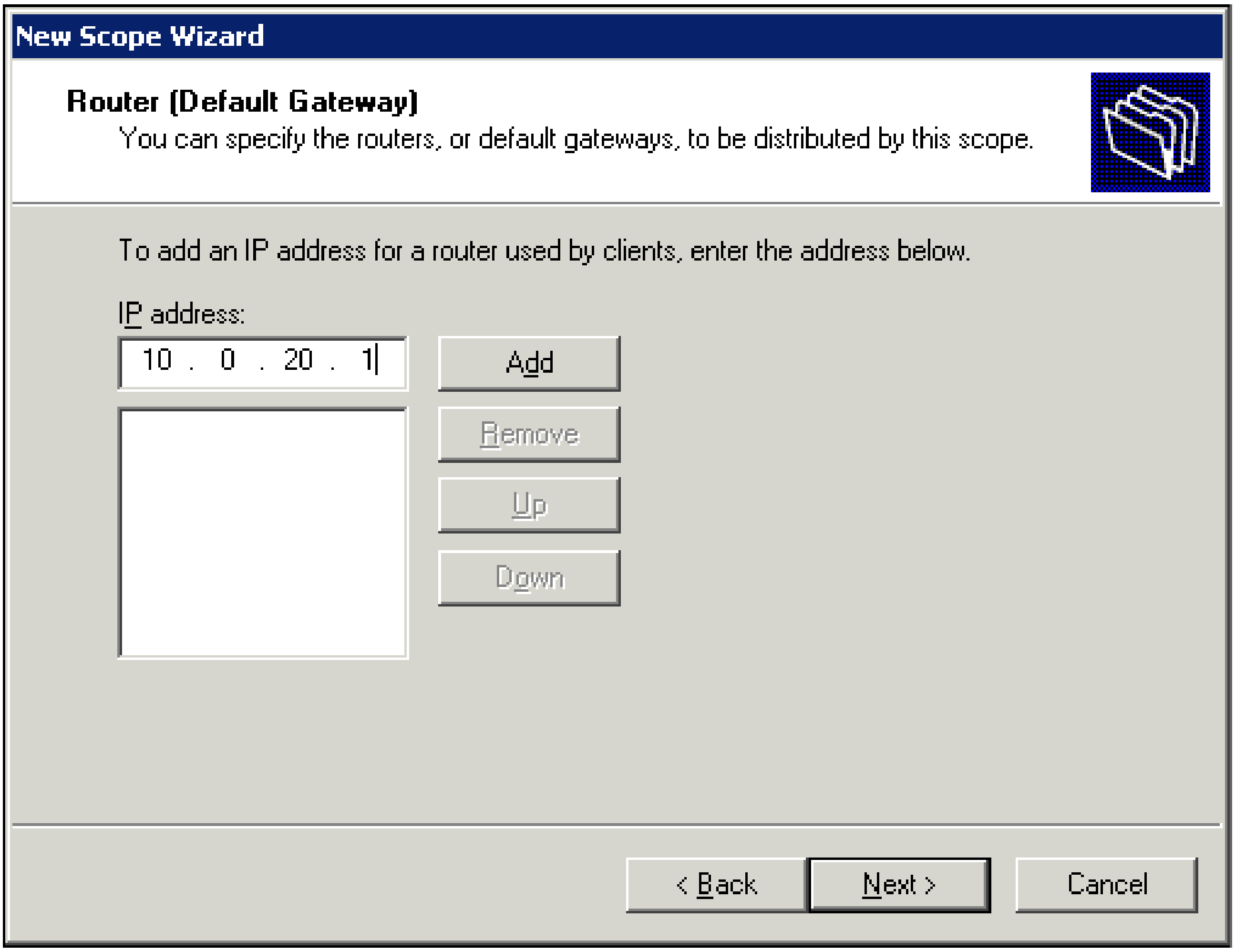
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

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 *10.0.20.1*，*然后单击***下一步**。



New Scope Wizard

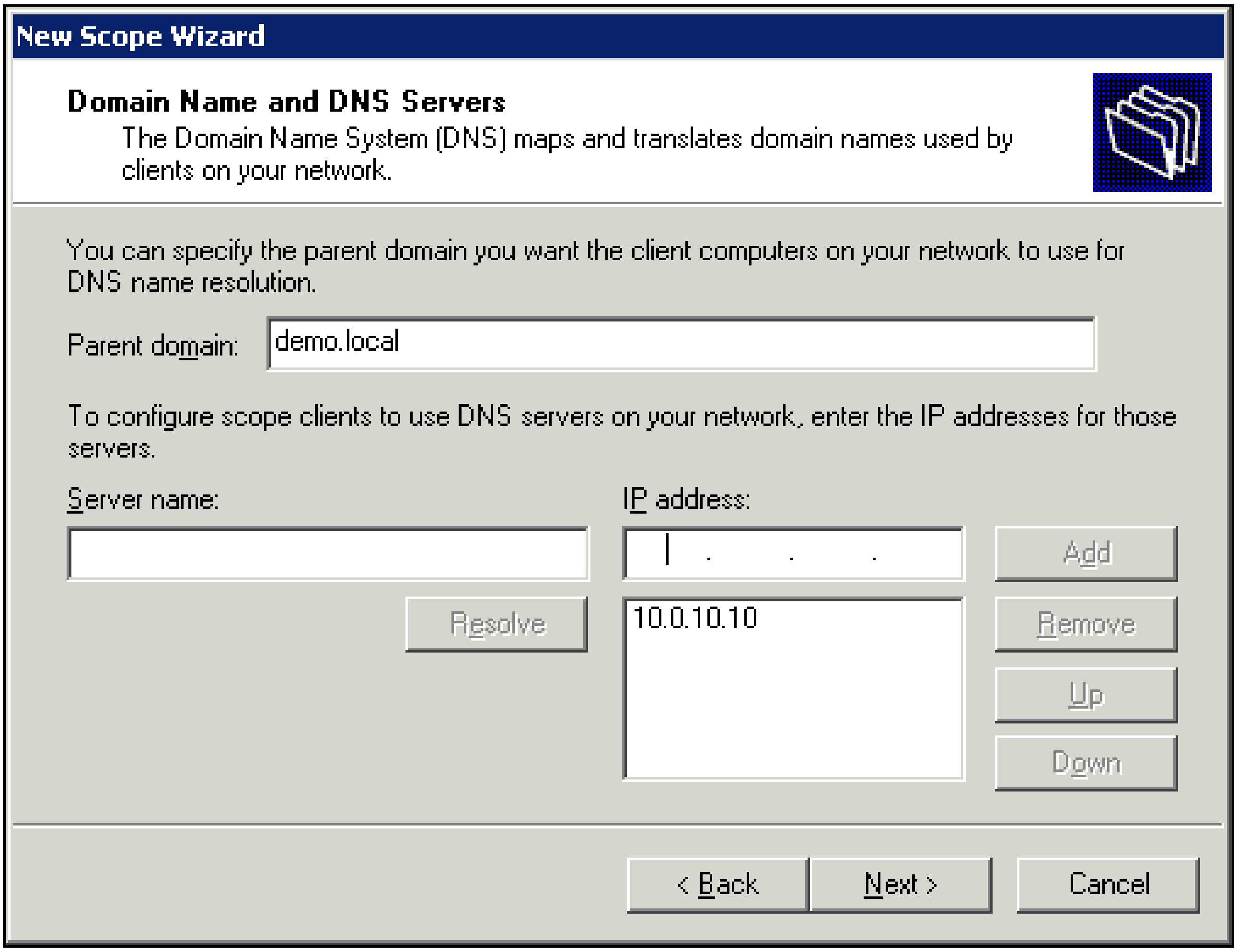
Router (Default Gateway)

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: 10 . 0 . 20 . 1

12. 在“域名称和 DNS 服务器”页上，在“父域”字段中键入 *demo.local，在“IP 地址”字段中键入 10.0.10.10，然后单击添加和下一步。



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.

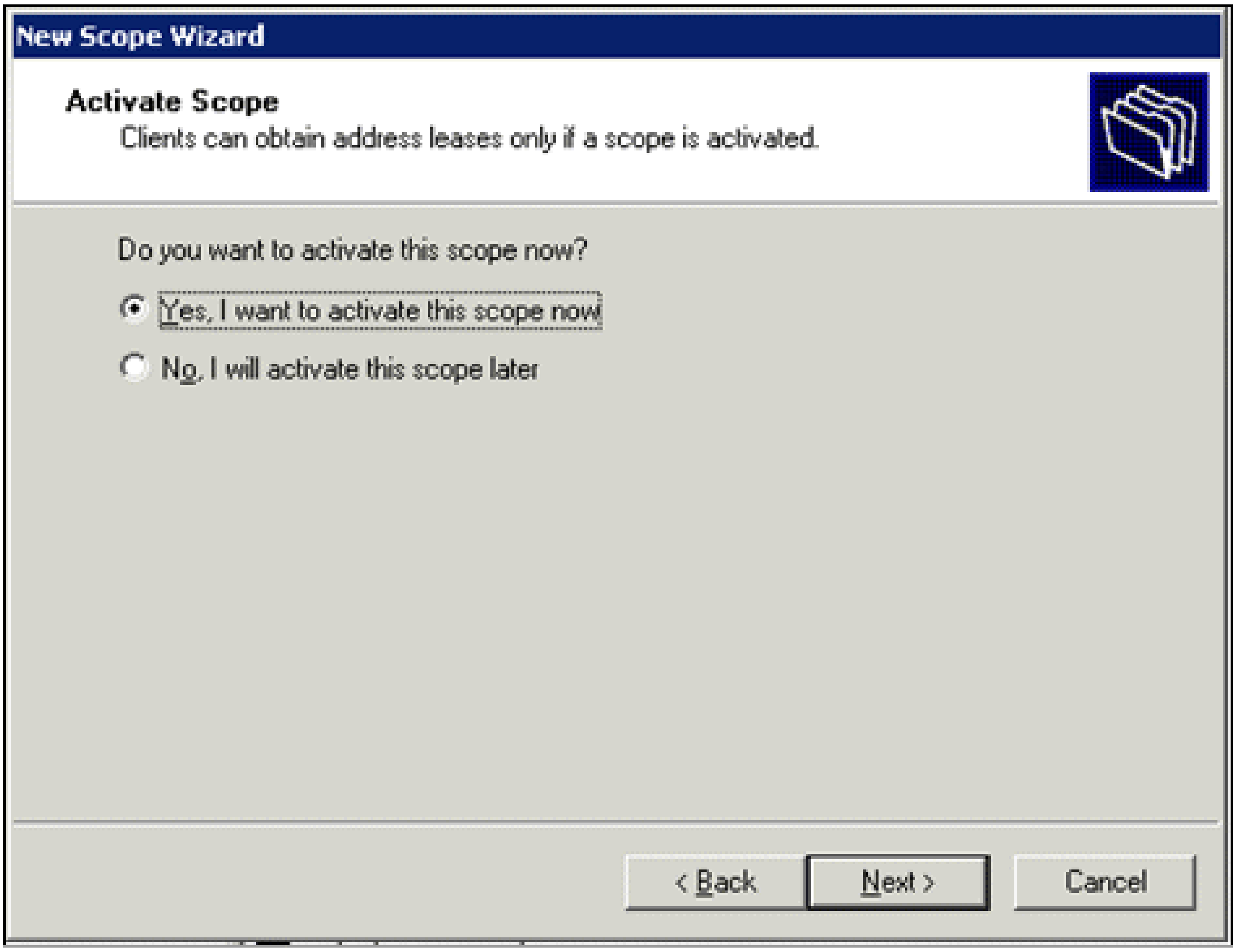
Parent domain: demo.local

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

Server name:

IP address: 10.0.10.10

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. 当您完成“新建作用域向导”页时，单击**完成**。

安装证书服务

请执行以下步骤：

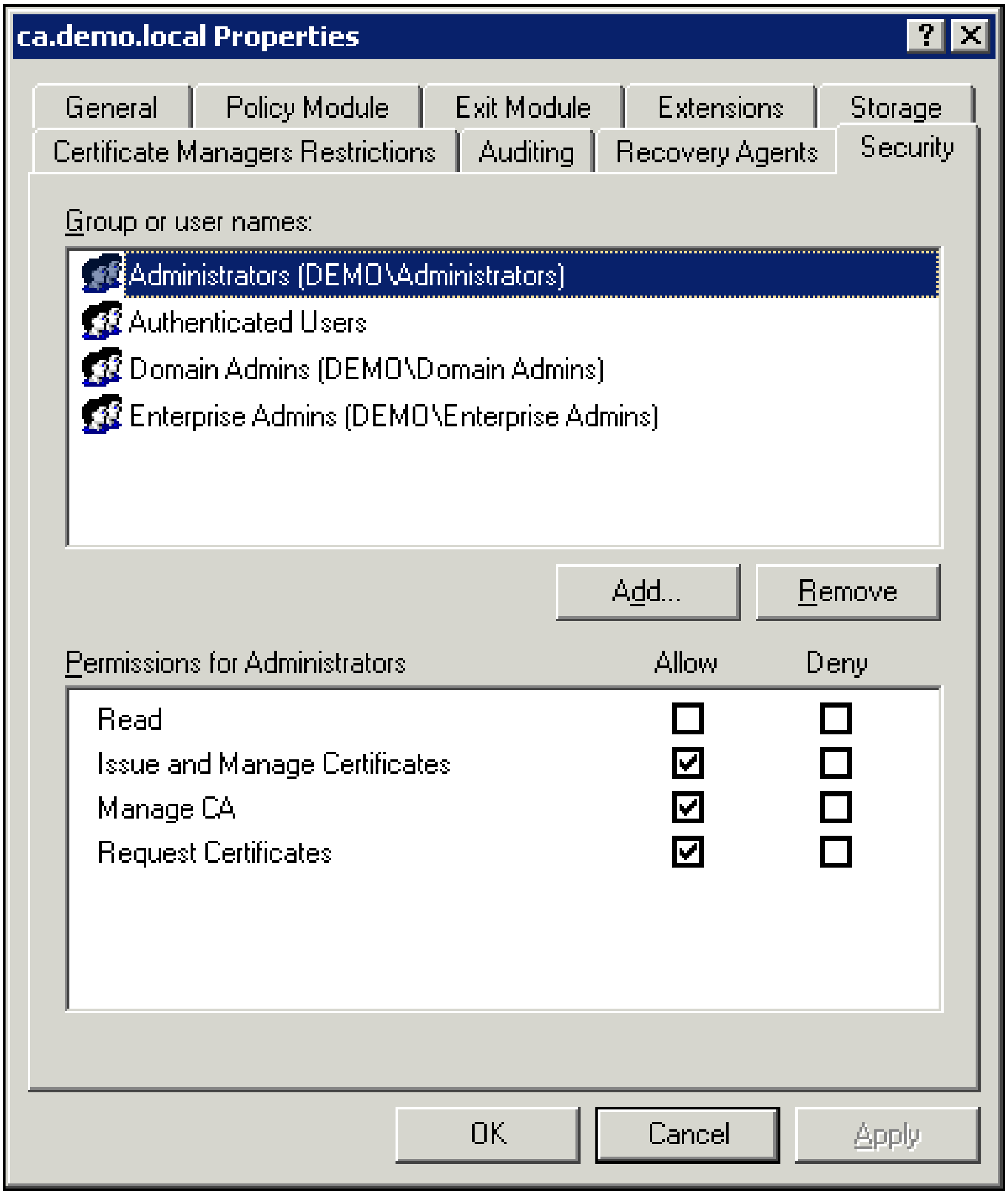
注意：在安装证书服务之前必须安装IIS，并且用户应该是“企业管理员OU”的一部分。

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”页的“此 CA 的公用名称”框中键入 *democa*。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。**

验证证书的管理员权限

请执行以下步骤：

1. 选择**开始 > 管理工具 > 证书颁发机构**。
2. 右键单击 **democa 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“管理员的权限”列表中，确保以下选项均设置为**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，请将其权限设置为**允许**。



ca.demo.local Properties

Group or user names:

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

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

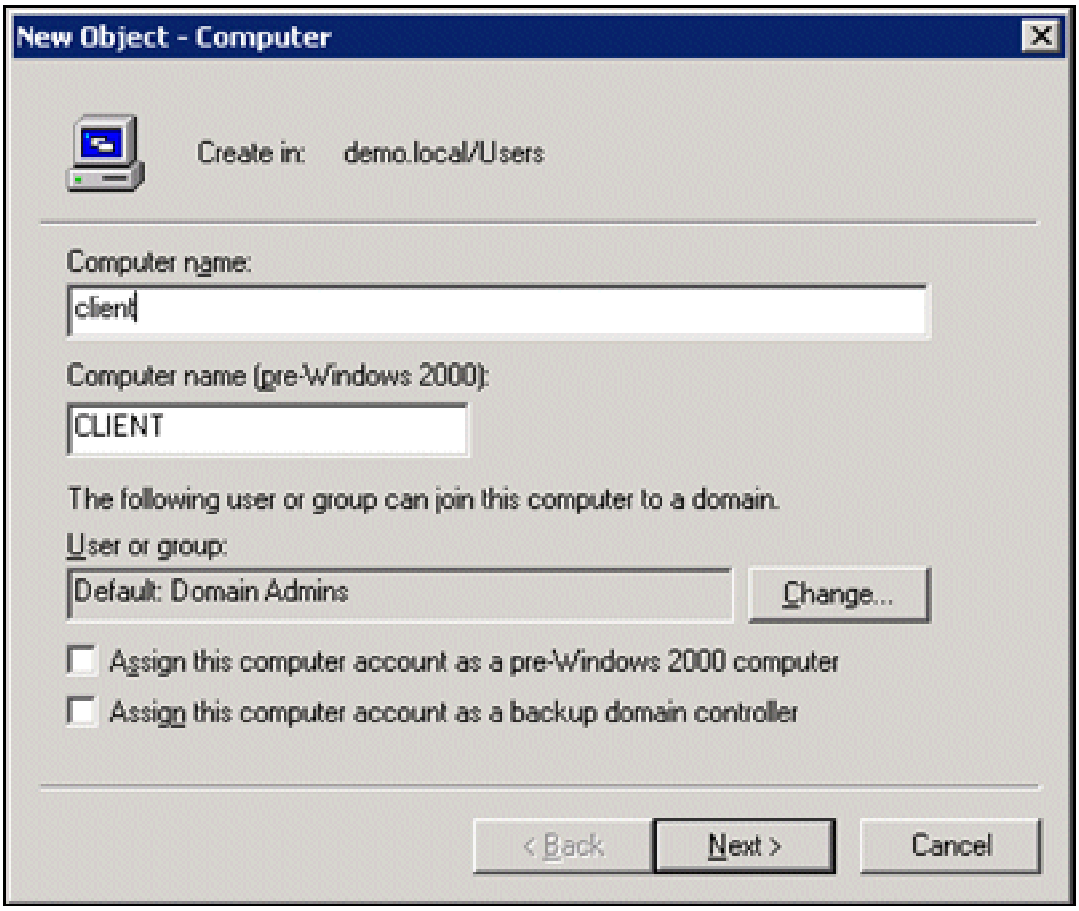
5. 单击**确定关闭“democa CA 属性”对话框，然后关闭“证书颁发机构”。**

向域中添加计算机

请执行以下步骤：

注：如果计算机已添加到域中，请继续执行向域中添加用户。

1. 打开 **Active Directory 用户和计算机管理单元。**
2. 在控制台树中，展开 **demo.local。**
3. 右键单击**计算机**，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: demo.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

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

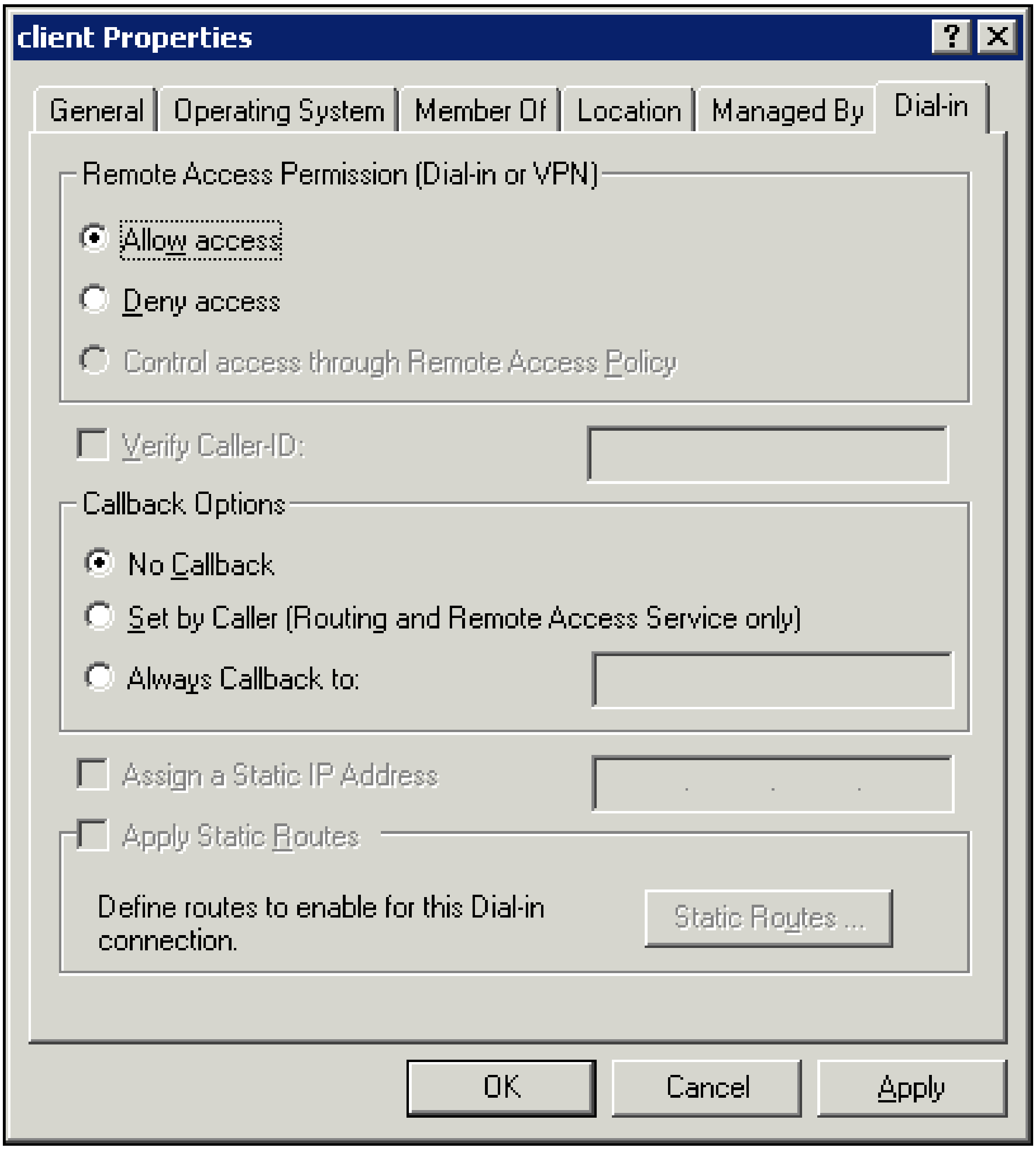
☐ Assign this computer account as a backup domain controller

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。

允许计算机进行无线访问

请执行以下步骤：

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。**本示例显示您在步骤7中添加的**Computer Client**的过程。单击**Properties**，然后转到**Dial-in**选项卡。
2. 在“远程访问权限”中选择**允许访问，然后单击确定。**



client Properties

General | Operating System | Member Of | Location | Managed By | Dial-in

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

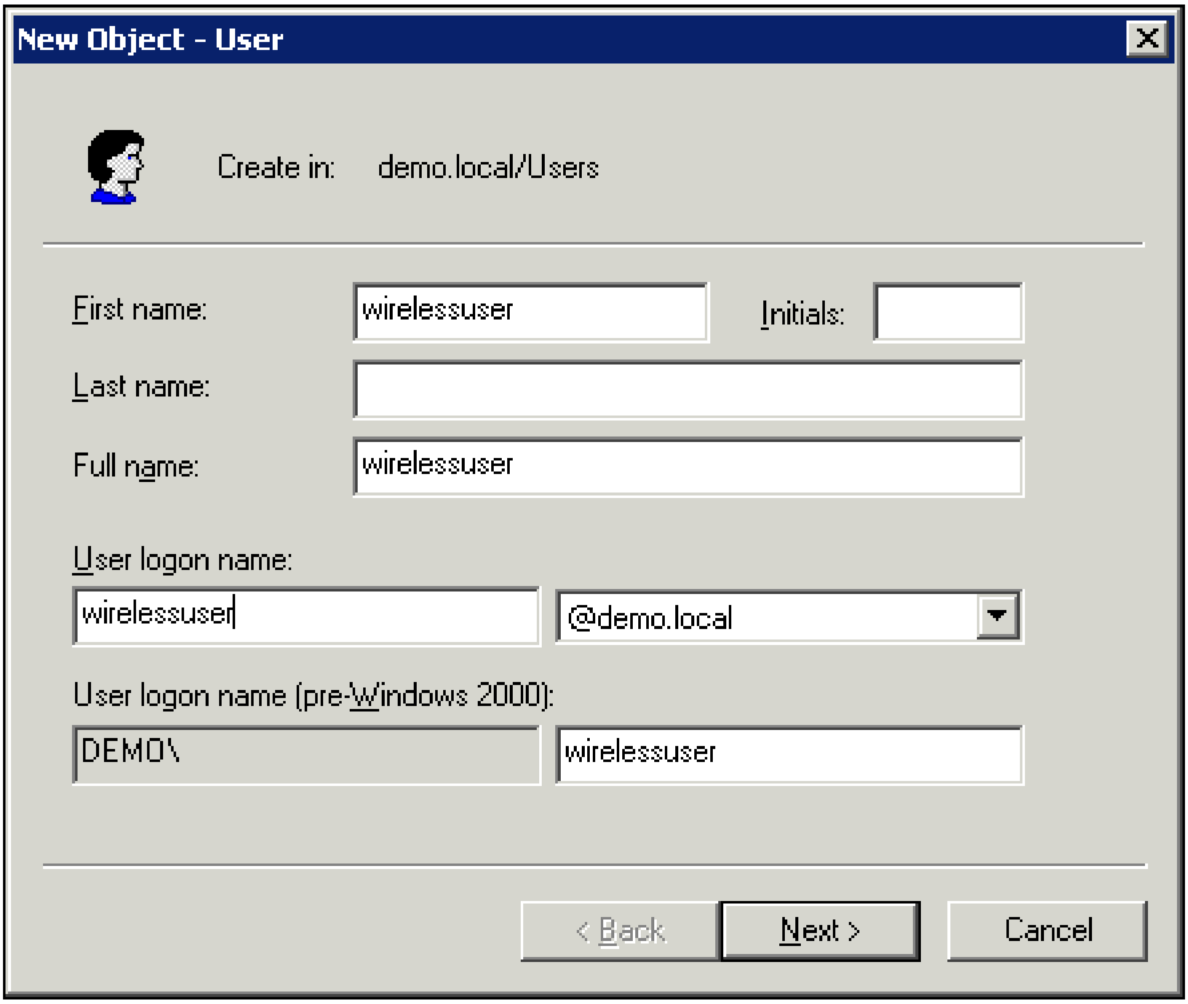
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

向域中添加用户

请执行以下步骤：

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**。



New Object - User

Create in: demo.local/Users

First name: wirelessuser

Initials:

Last name:

Full name: wirelessuser

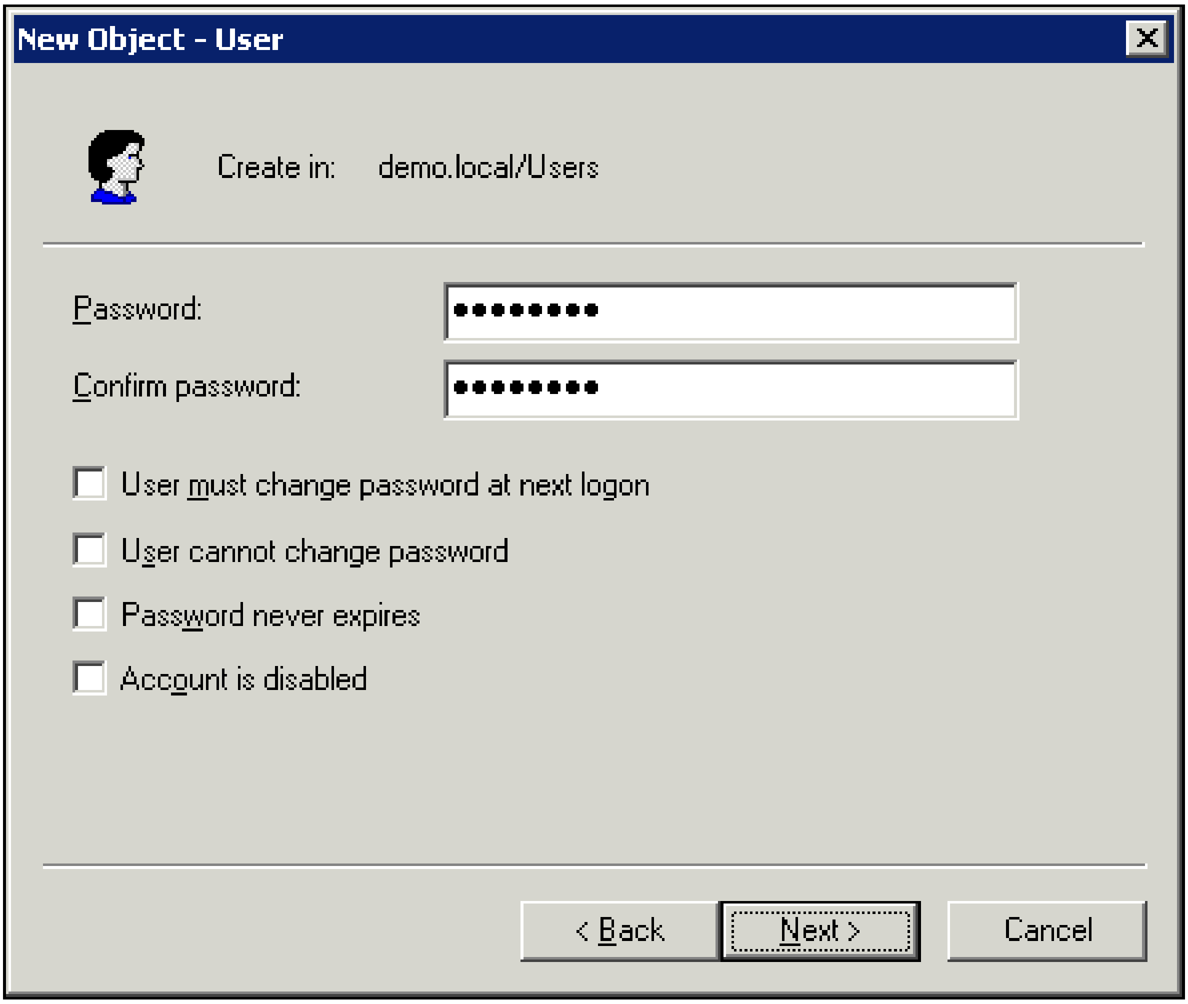
User logon name:

wirelessuser @demo.local

User logon name (pre-Windows 2000):

DEMO\ 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: demo.local/Users

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

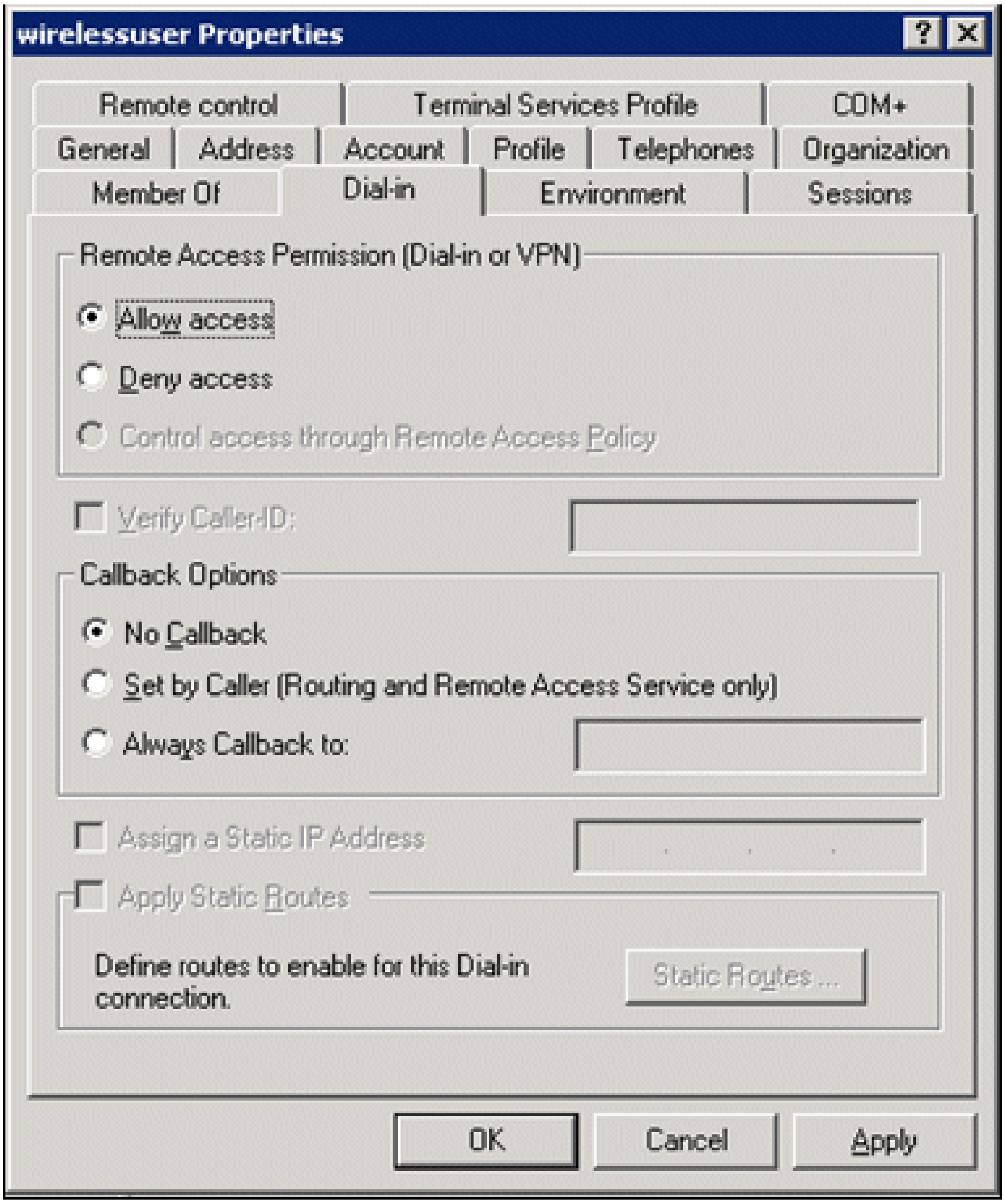
☐ Account is disabled

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。

允许用户进行无线访问

请执行以下步骤：

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. 在“远程访问权限”中选择**允许访问，然后单击确定**。



wirelessuser Properties

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

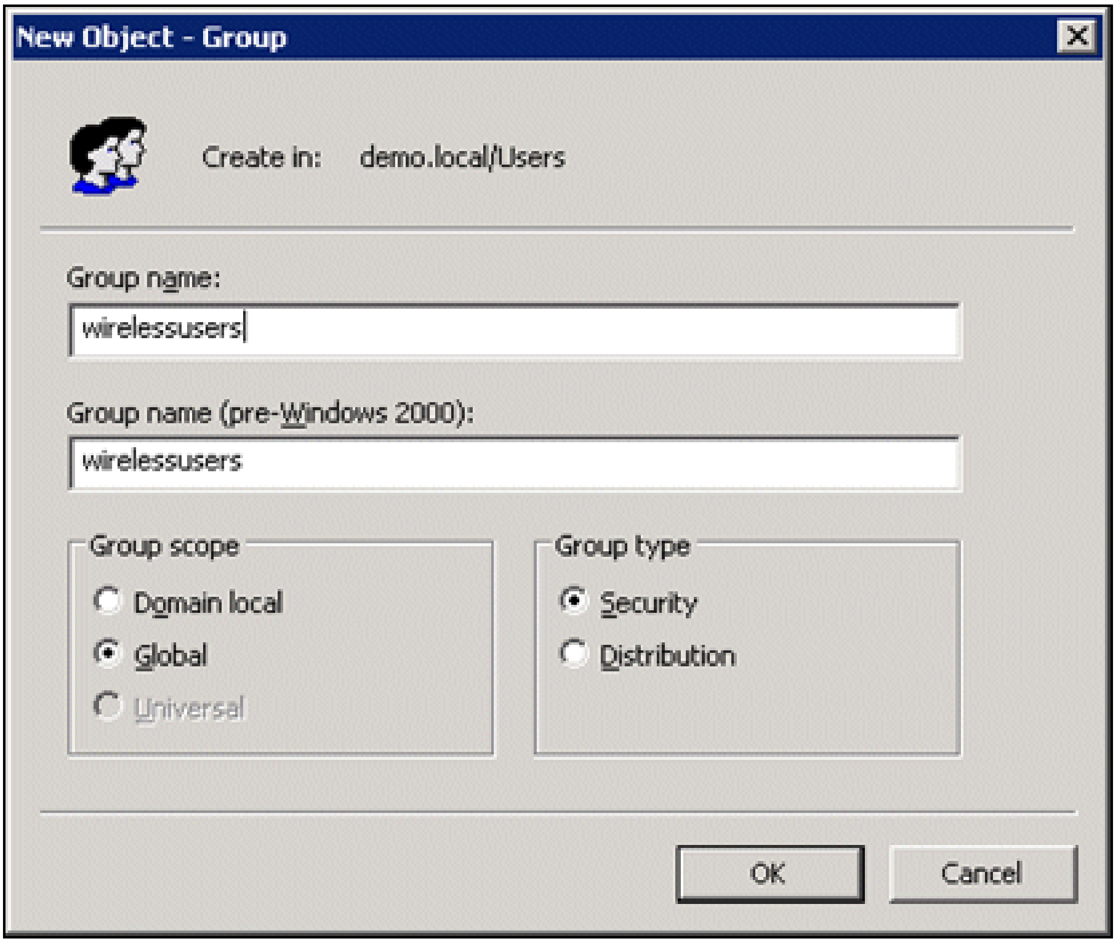
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

向域中添加组

请执行以下步骤：

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: demo.local/Users

Group name: wirelessusers

Group name (pre-Windows 2000): wirelessusers

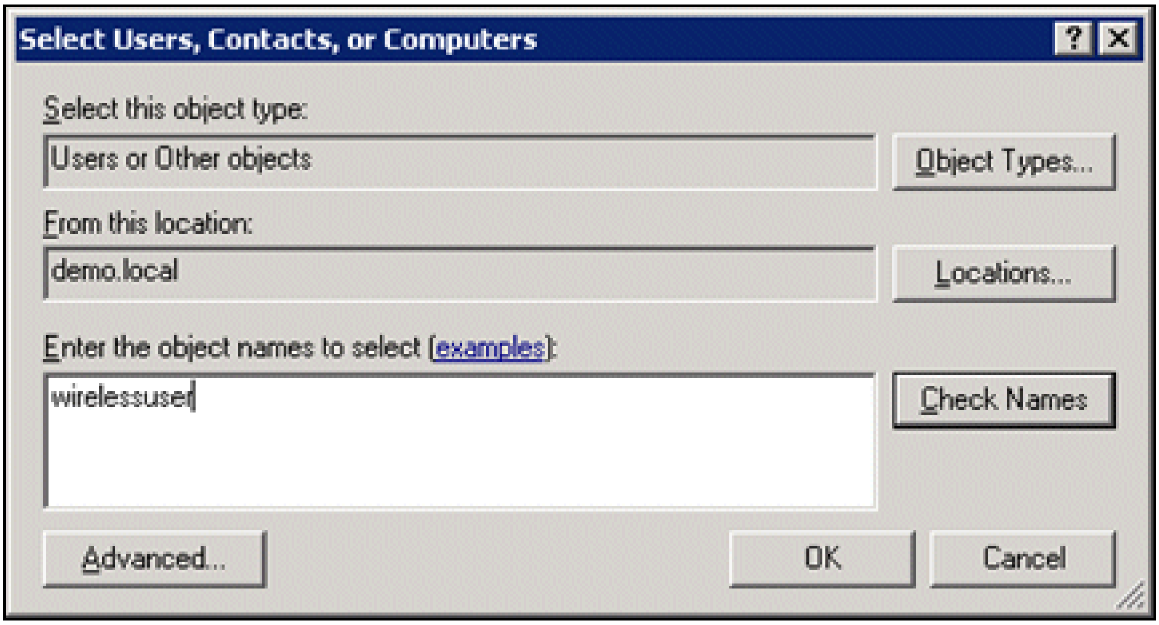
Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

向 wirelessusers 组中添加用户

请执行以下步骤：

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



Select Users, Contacts, or Computers

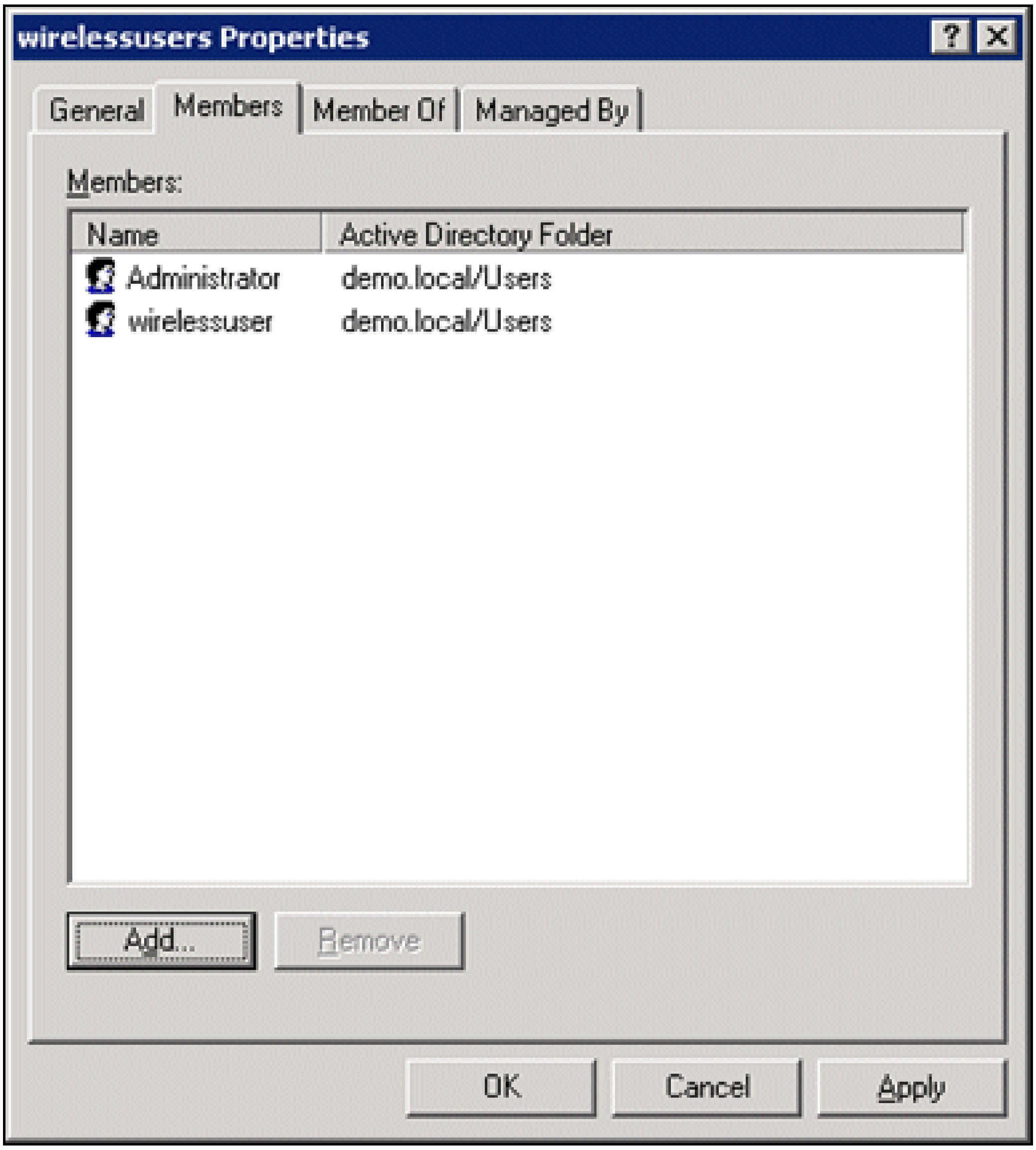
Select this object type: Users or Other objects

From this location: demo.local

Enter the object names to select (examples): wirelessuser

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



Name	Active Directory Folder
Administrator	demo.local/Users
wirelessuser	demo.local/Users

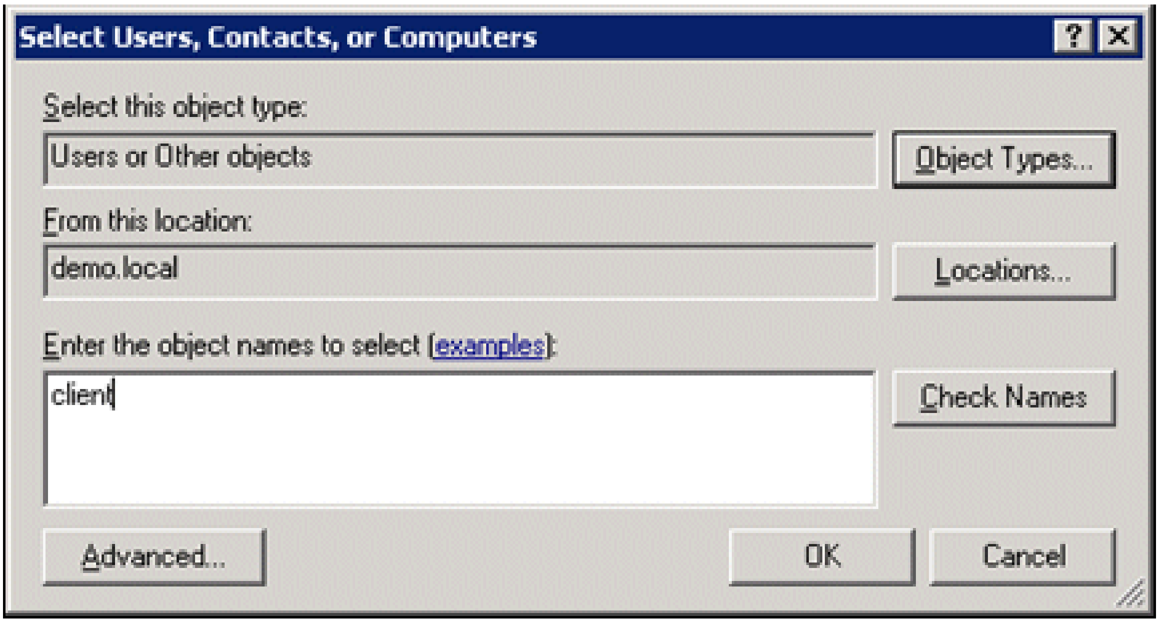
组中。

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。

向 wirelessusers 组中添加客户端计算机

请执行以下步骤：

1. 重复本文档向 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。*



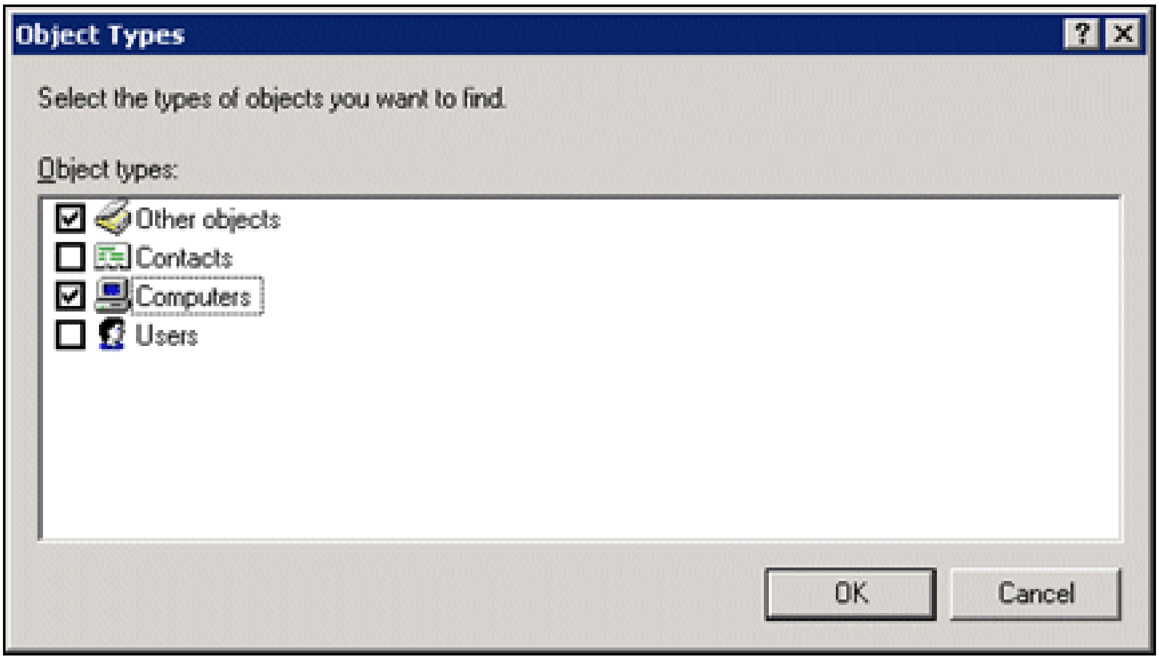
Select Users, Contacts, or Computers

Select this object type:
Users or Other objects

From this location:
demo.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”。



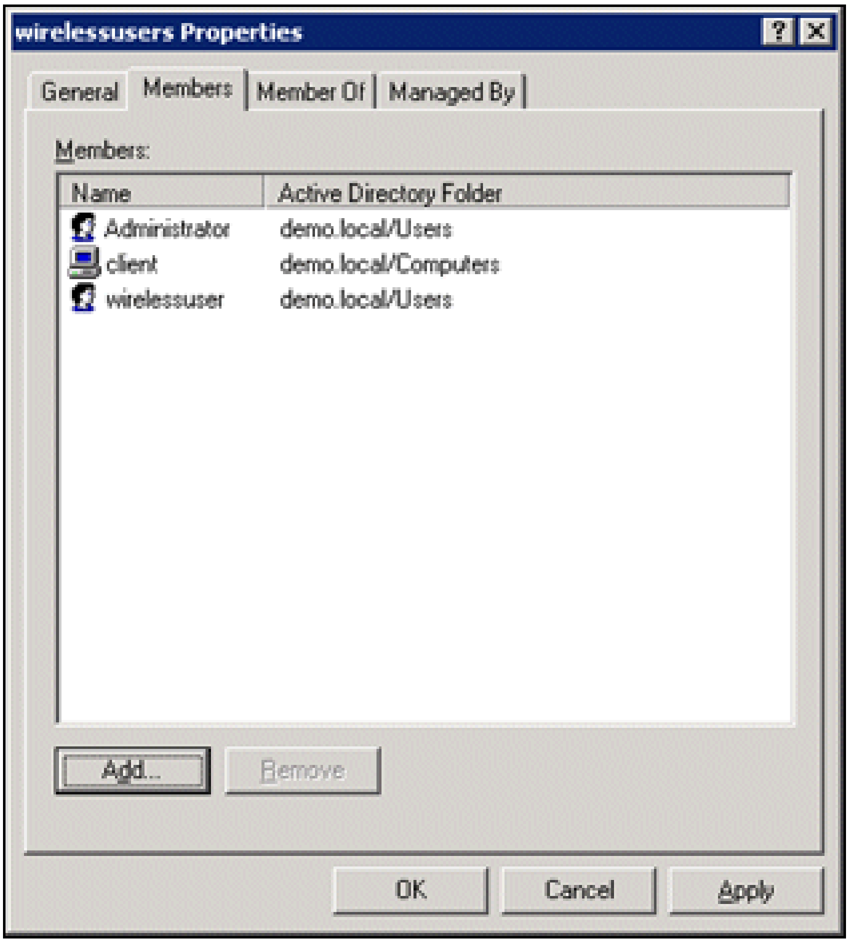
Object Types

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。



Name	Active Directory Folder
Administrator	demo.local/Users
client	demo.local/Computers
wirelessuser	demo.local/Users

5. 重复此过程，向该组中添加更多计算机。

Cisco 1121 安全 ACS 5.1

使用 CSACS-1121 系列设备进行安装

CSACS-1121 设备已预先安装了 ACS 5.1 软件。本部分概述安装过程及在安装 ACS 之前必须执行的任务。

1. 将 CSACS-1121 连接到网络和设备控制台。请参阅第 4 章“连接电缆”。
2. 启动 CSACS-1121 设备。请参阅第 4 章“启动 CSACS-1121 系列设备”。
3. 在 CLI 提示符下运行 **setup 命令，以配置 ACS 服务器的初始设置。**请参阅“运行安装程序”。

安装 ACS 服务器

本部分描述在 CSACS-1121 系列设备上安装 ACS 服务器的过程。

- 运行安装程序
- 验证安装过程
- 安装后任务

有关安装 Cisco Secure ACS 服务器的详细信息，请参阅 Cisco 安全访问控制系统 5.1 安装和升级指南。

Cisco WLC5508 控制器配置

为 WPAv2/WPA 创建必要的配置

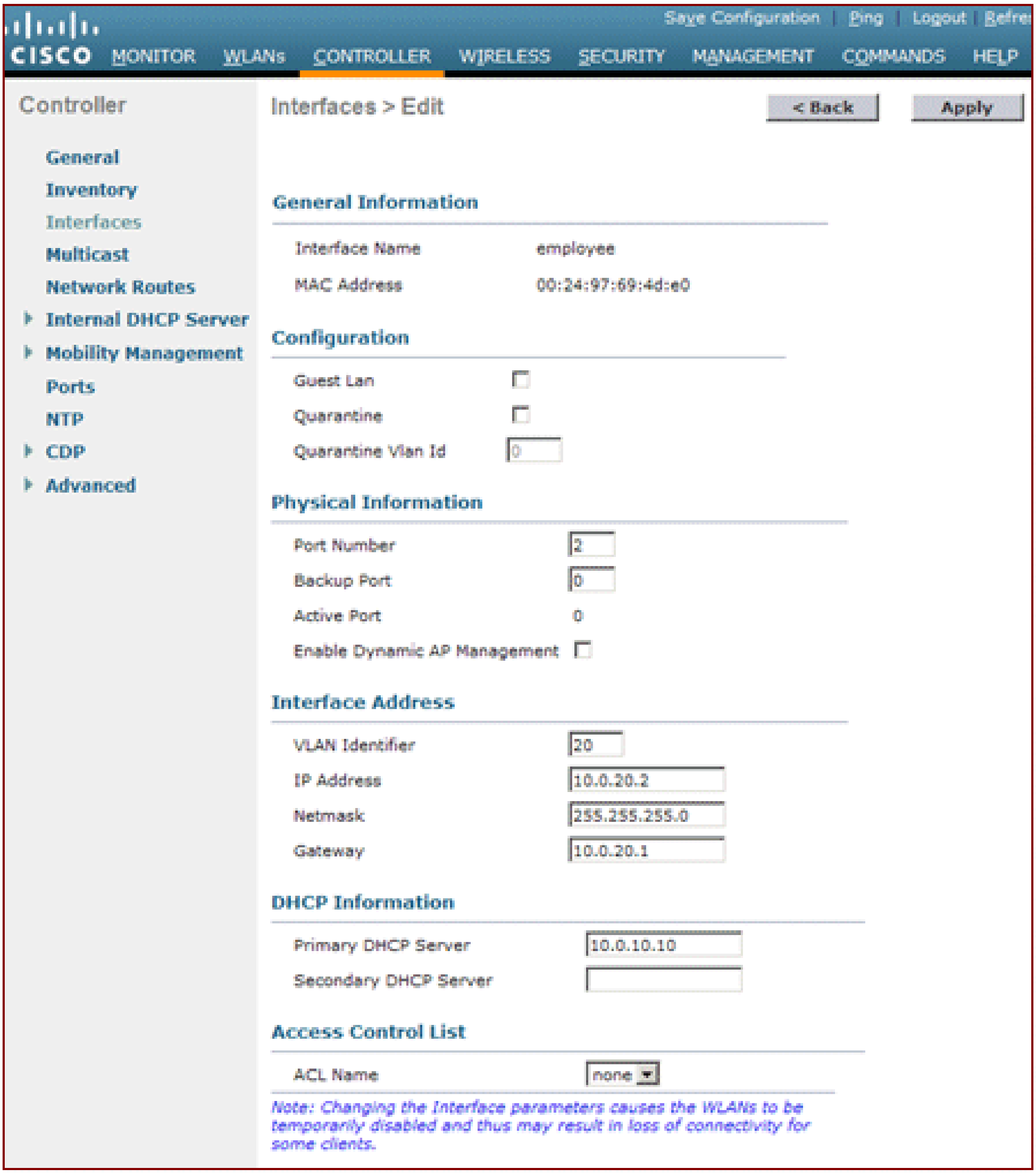
请执行以下步骤：

注意：假设控制器与网络具有基本连接，并且与管理接口的IP可达性成功。

1. 浏览到 **https://10.0.1.10，以便登录控制器。**

© 2005-2009 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

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 字段中输入 *Employee*。（此字段可以是您喜欢的任何值。）
8. 在VLAN ID字段中，输入*20*。（此字段可以是网络中携带的任何VLAN。）
9. 单击 **Apply**。
10. 在显示此 Interfaces > Edit 窗口时，配置相关信息：接口 IP 地址 - 10.0.20.2网络掩码 - **255.255.255.0**网关 - **10.0.10.1**主 DHCP - **10.0.10.10**



Interfaces > Edit

General Information

Interface Name employee

MAC Address 00:24:97:69:4d:e0

Configuration

Guest Lan □

Quarantine □

Quarantine Vlan Id 0

Physical Information

Port Number 2

Backup Port 0

Active Port 0

Enable Dynamic AP Management □

Interface Address

VLAN Identifier 20

IP Address 10.0.20.2

Netmask 255.255.255.0

Gateway 10.0.20.1

DHCP Information

Primary DHCP Server 10.0.10.10

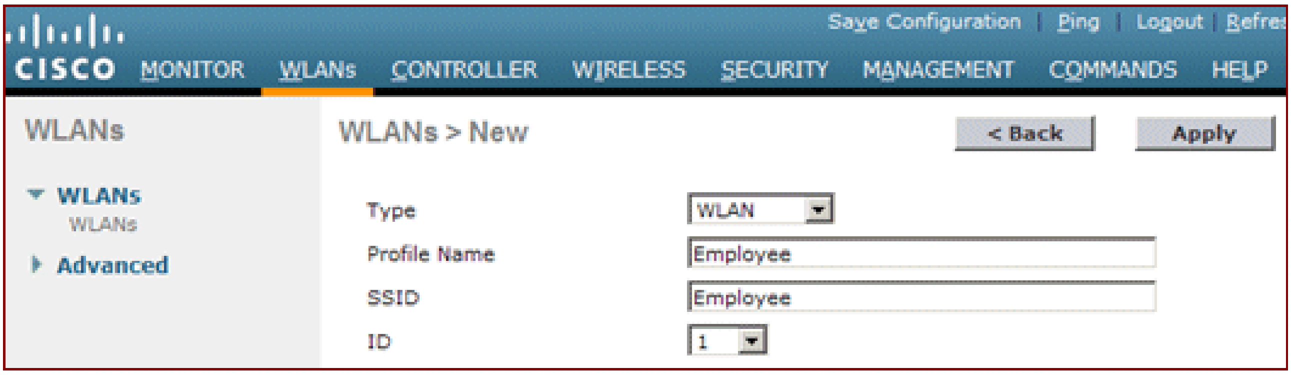
Secondary DHCP Server

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 **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 字段中输入 *Employee*。


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply

WLANs > New

Type WLAN

Profile Name Employee

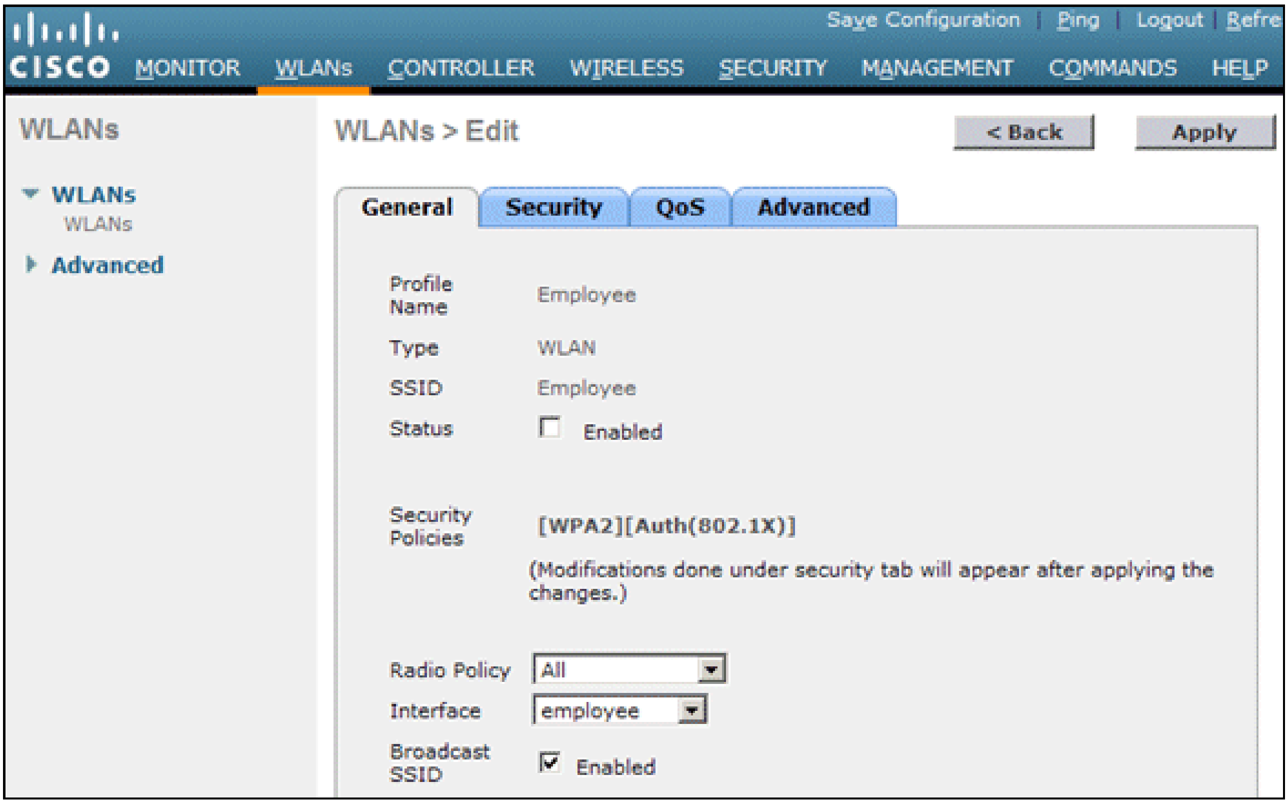
SSID Employee

ID 1

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 Interface (employee)。**并且，确保选中“Broadcast SSID”的**“Enabled”复选框。**



WLANs > Edit

Profile Name Employee

Type WLAN

SSID Employee

Status □ Enabled

Security Policies [WPA2][Auth(802.1X)]

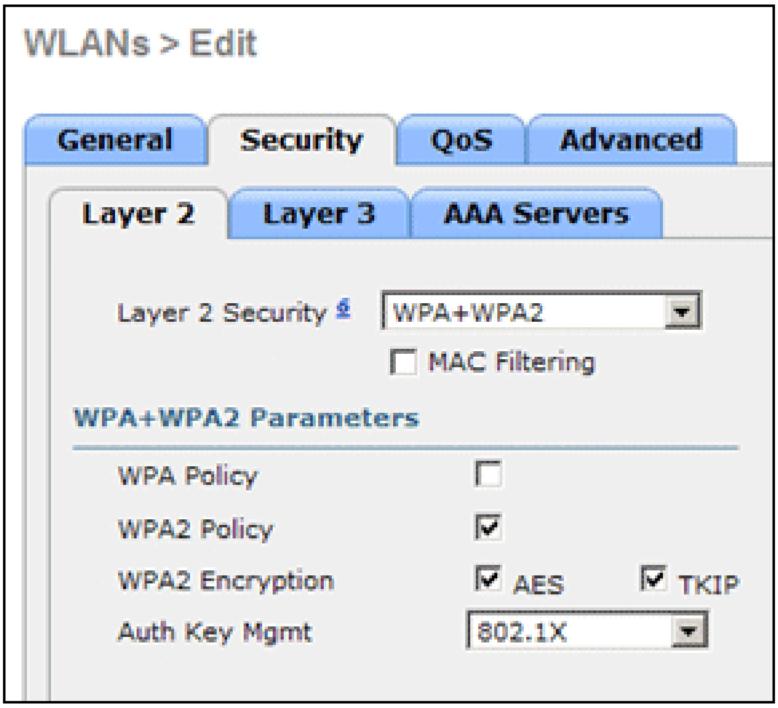
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface employee

Broadcast SSID ☑ Enabled

19. 单击“Security”选项卡。
20. 在“Layer 2”子菜单下，针对“Layer 2 Security”选中 **WPA + WPA2 。**对于“WPA2 encryption”，请选中 **AES + TKIP，以便启用 TKIP 客户端。**



WLANs > Edit

Layer 2 Security WPA+WPA2

□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy □

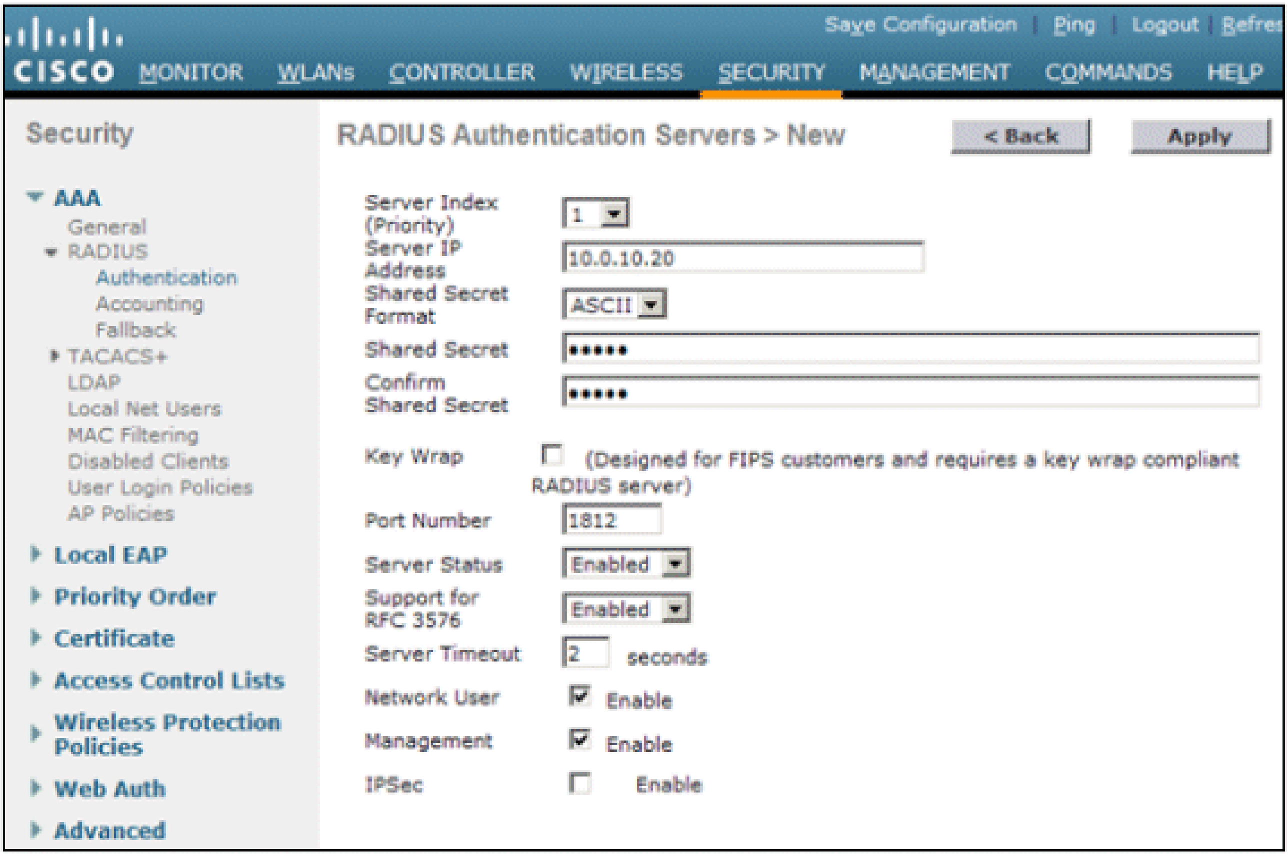
WPA2 Policy ☑

WPA2 Encryption ☑ AES ☑ TKIP

Auth Key Mgmt 802.1X

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 (10.0.10.20)，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 复选框，然后单击 Apply**。



RADIUS Authentication Servers > New

Server Index (Priority): 1
Server IP Address: 10.0.10.20
Shared Secret Format: ASCII
Shared Secret: •••••
Confirm Shared Secret: •••••
Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number: 1812
Server Status: Enabled
Support for RFC 3576: Enabled
Server Timeout: 2 seconds
Network User: ☑ Enable
Management: ☑ Enable
IPSec: □ Enable

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 CA 服务器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在Windows 2003 Enterprise CA发行版中更改了Web Server模板，因此密钥不再可导出，并且该选项呈灰色显示。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。

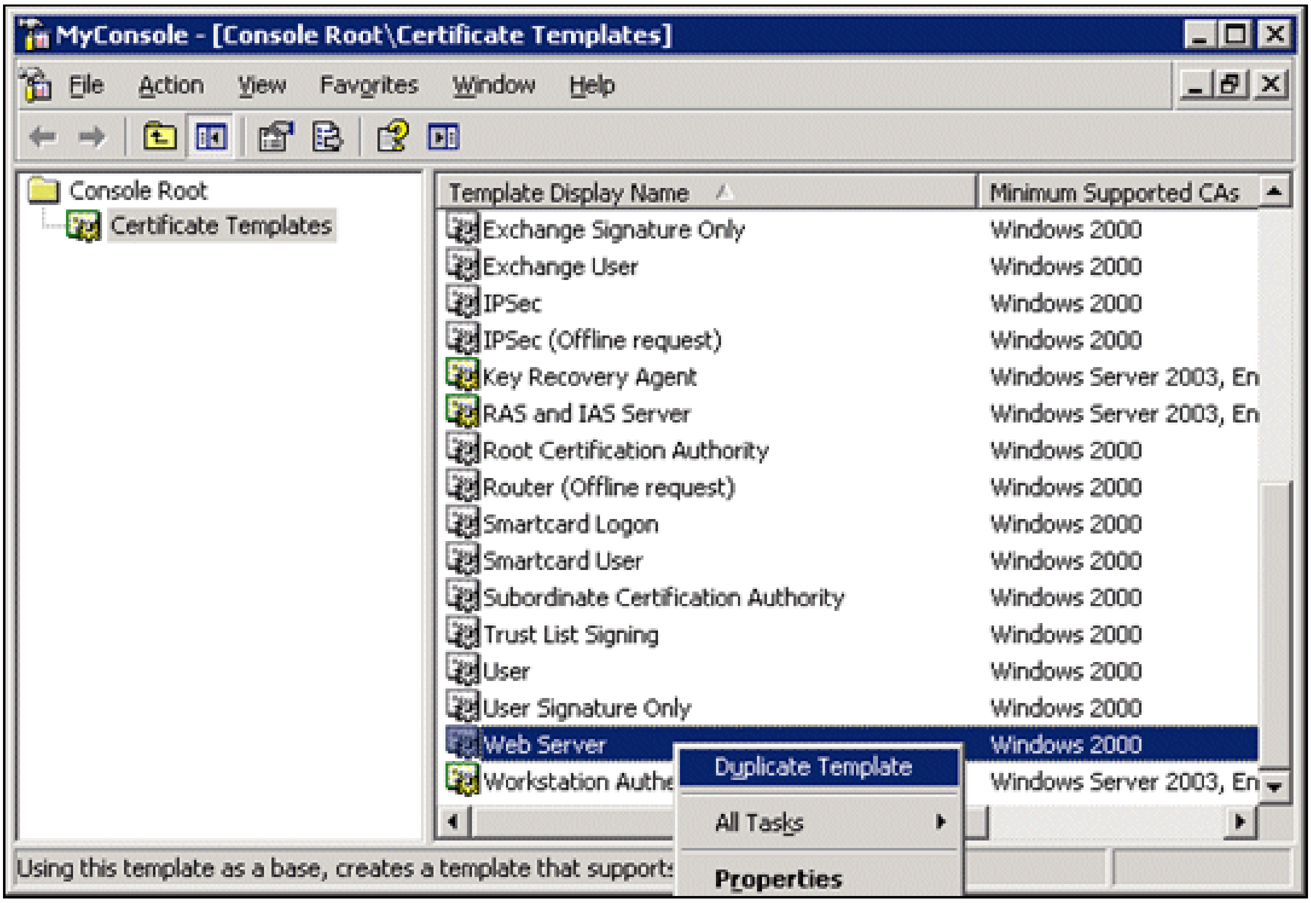
注意：Windows 2000允许导出密钥，如果您使用Windows 2000，则无需遵循这些步骤。

安装证书模板管理单元

请执行以下步骤：

1. 选择**“开始”>“运行”**，输入 *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，请输入 *certtmpl.msc*，*以打开“证书模板”管理单元。*



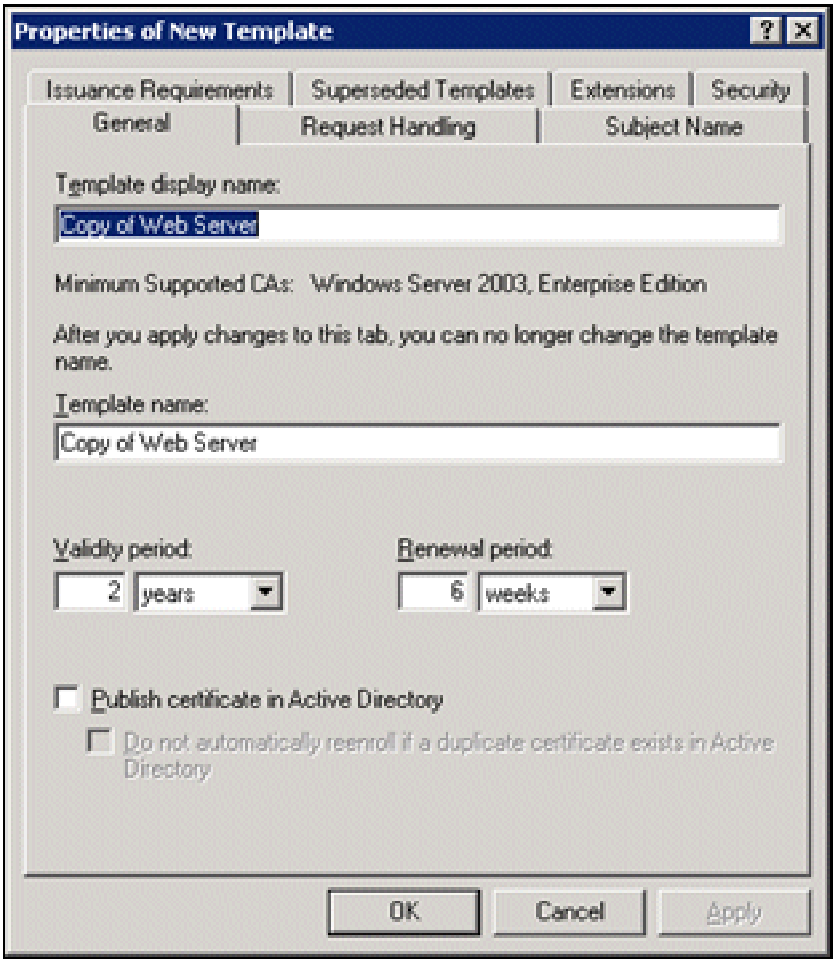
Template Display Name	Minimum Supported CAs
Exchange Signature Only	Windows 2000
Exchange User	Windows 2000
IPSec	Windows 2000
IPSec (Offline request)	Windows 2000
Key Recovery Agent	Windows Server 2003, En
RAS and IAS Server	Windows Server 2003, En
Root Certification Authority	Windows 2000
Router (Offline request)	Windows 2000
Smartcard Logon	Windows 2000
Smartcard User	Windows 2000
Subordinate Certification Authority	Windows 2000
Trust List Signing	Windows 2000
User	Windows 2000
User Signature Only	Windows 2000
Web Server	Windows 2000
Workstation Authe	Windows Server 2003, En

Using this template as a base, creates a template that supports

为 ACS Web Server 创建证书模板

请执行以下步骤：

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**。



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

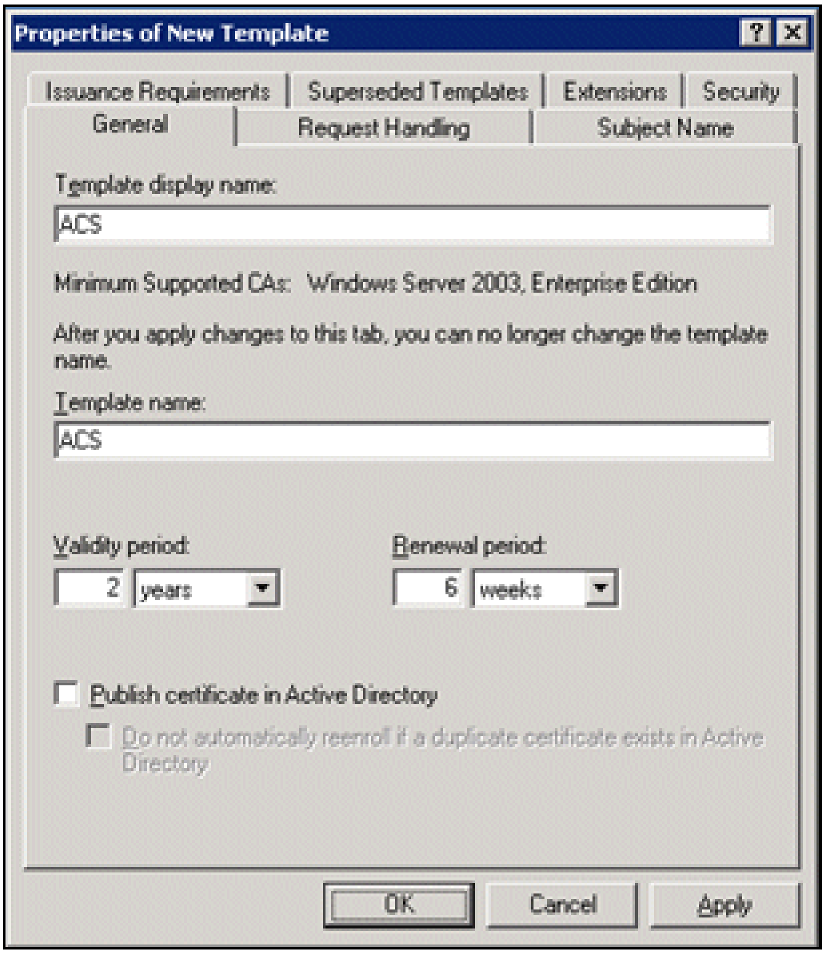
Validity period: 2 years

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”字段中输入 *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

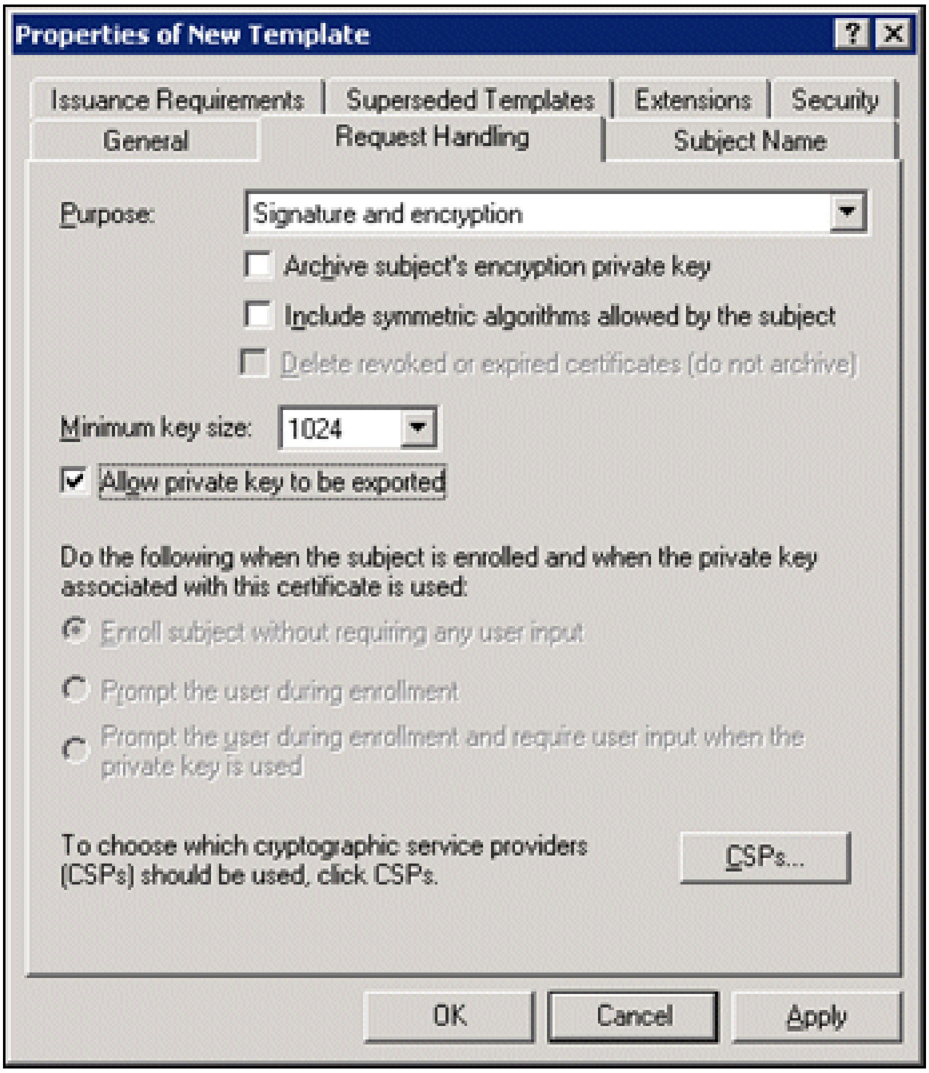
Validity period: 2 years

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**。并且，确保从“用途”下拉菜单中选择了**签名和**



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

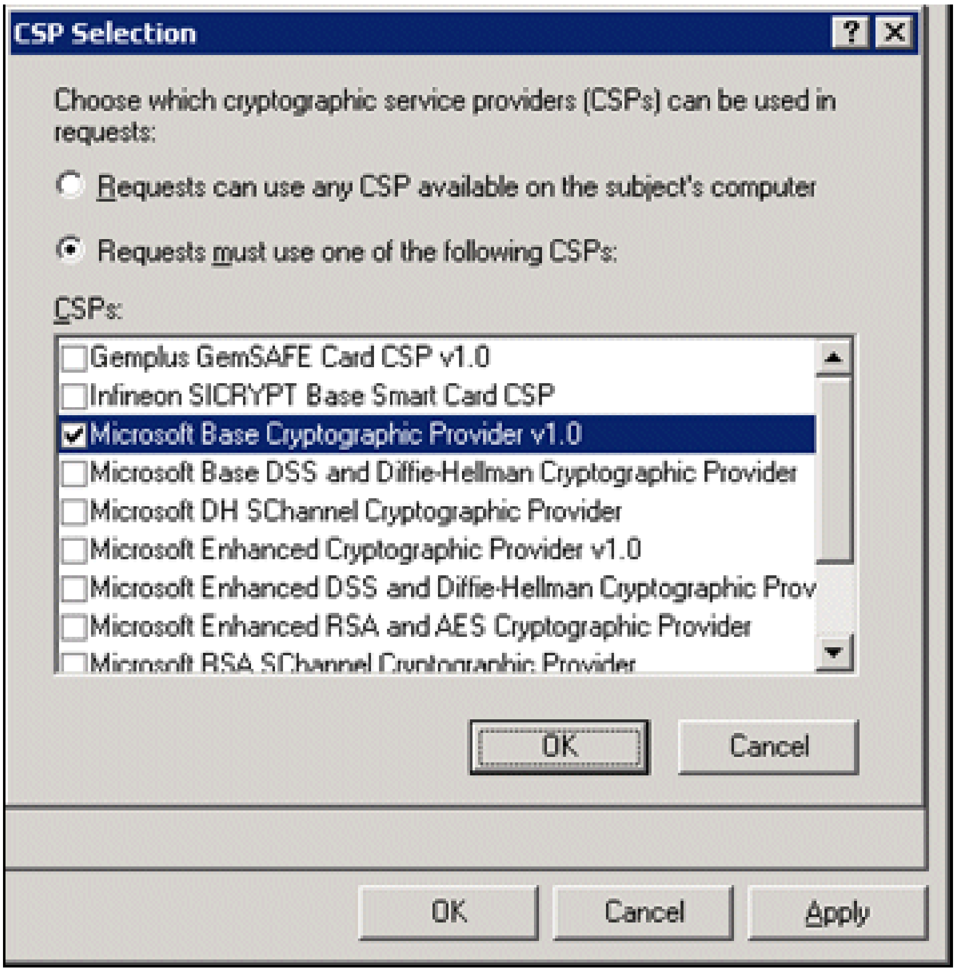
○ Prompt the user during enrollment

○ 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.

加密。

5. 选择**请求必须使用以下的一个 CSP 并选中“Microsoft Base Cryptographic Provider v1.0”。**取消选中其他已选中的 CSP，然后单击**确定**。



CSP Selection

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

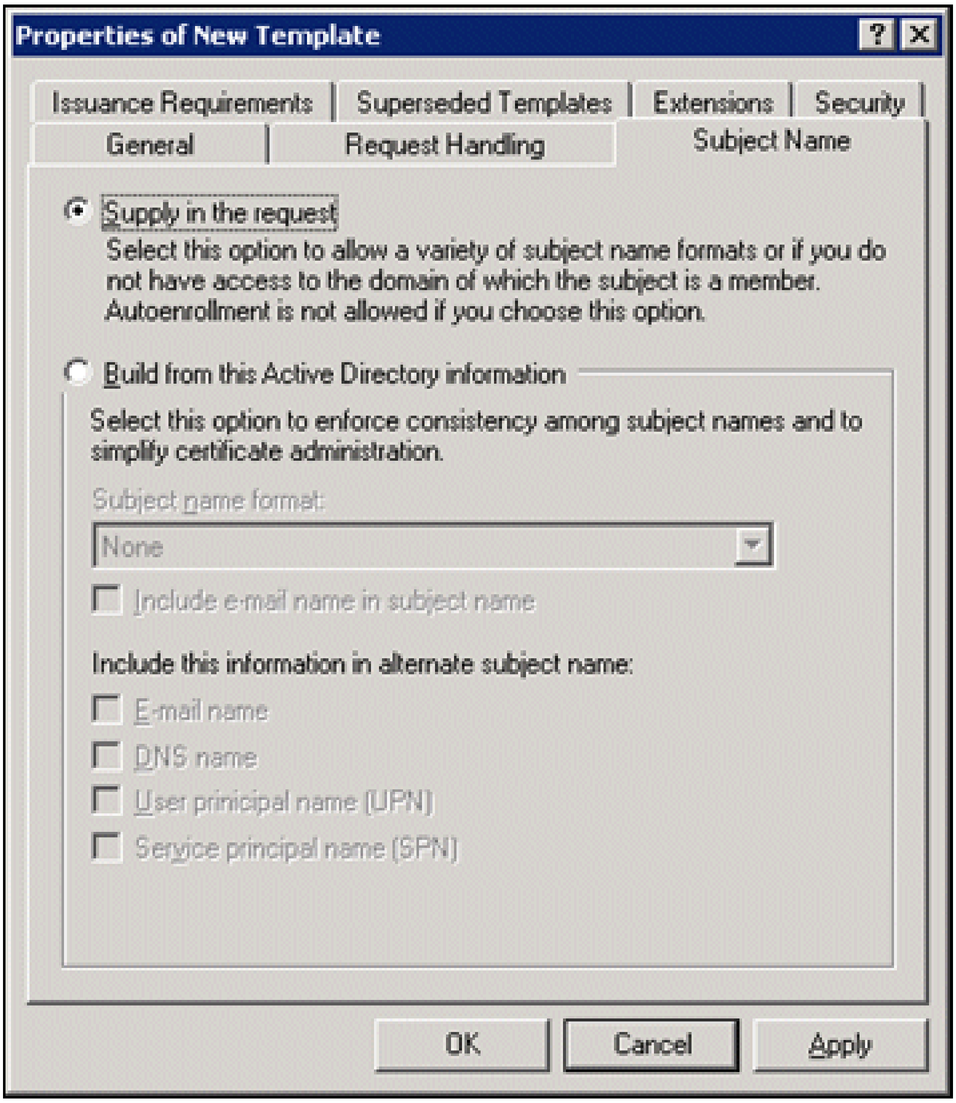
○ Requests can use any CSP available on the subject's computer

● 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

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:

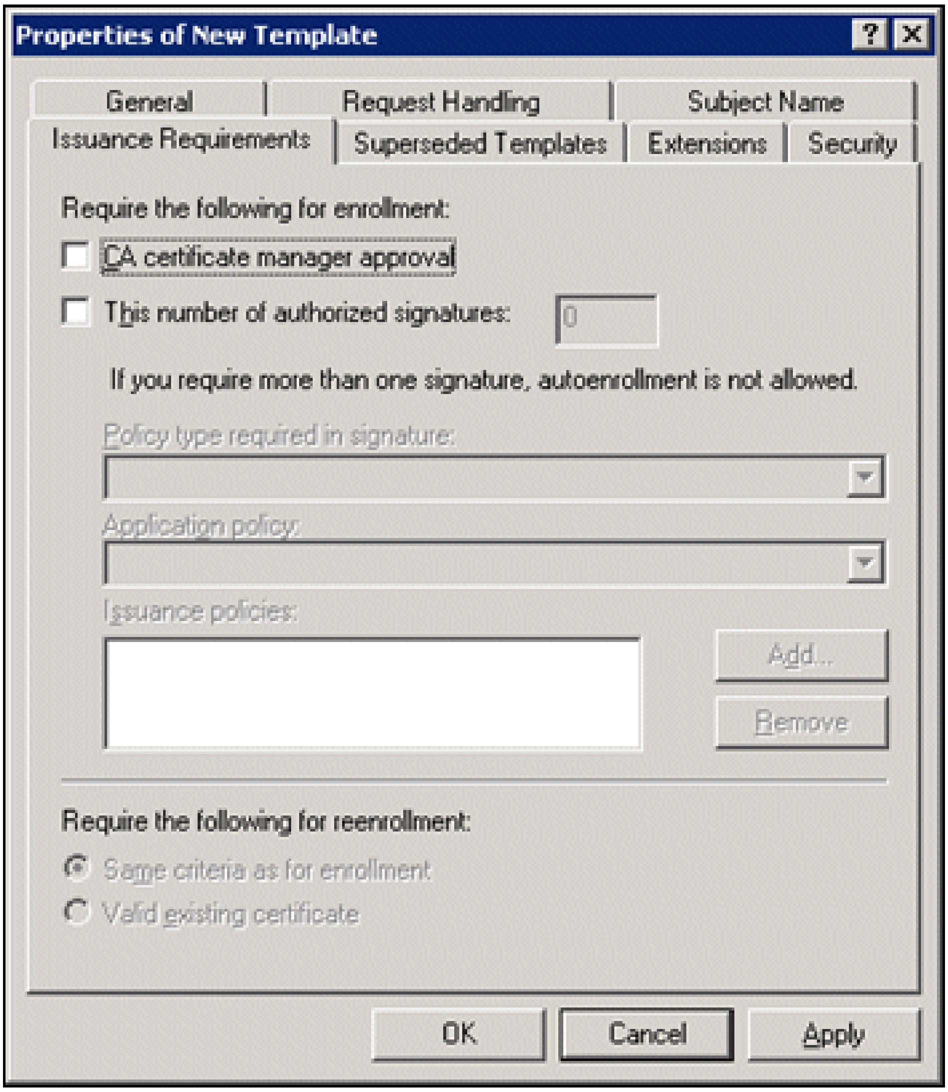
□ E-mail name

□ 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。注意：如果选择基于此**Active Directory信息构建，请仅选中**User principal name(UPN)，并取消选中Include email name** in subject name and E-mail name，因为未在Active Directory用户和计算机管理单元中为无线用户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。
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。



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

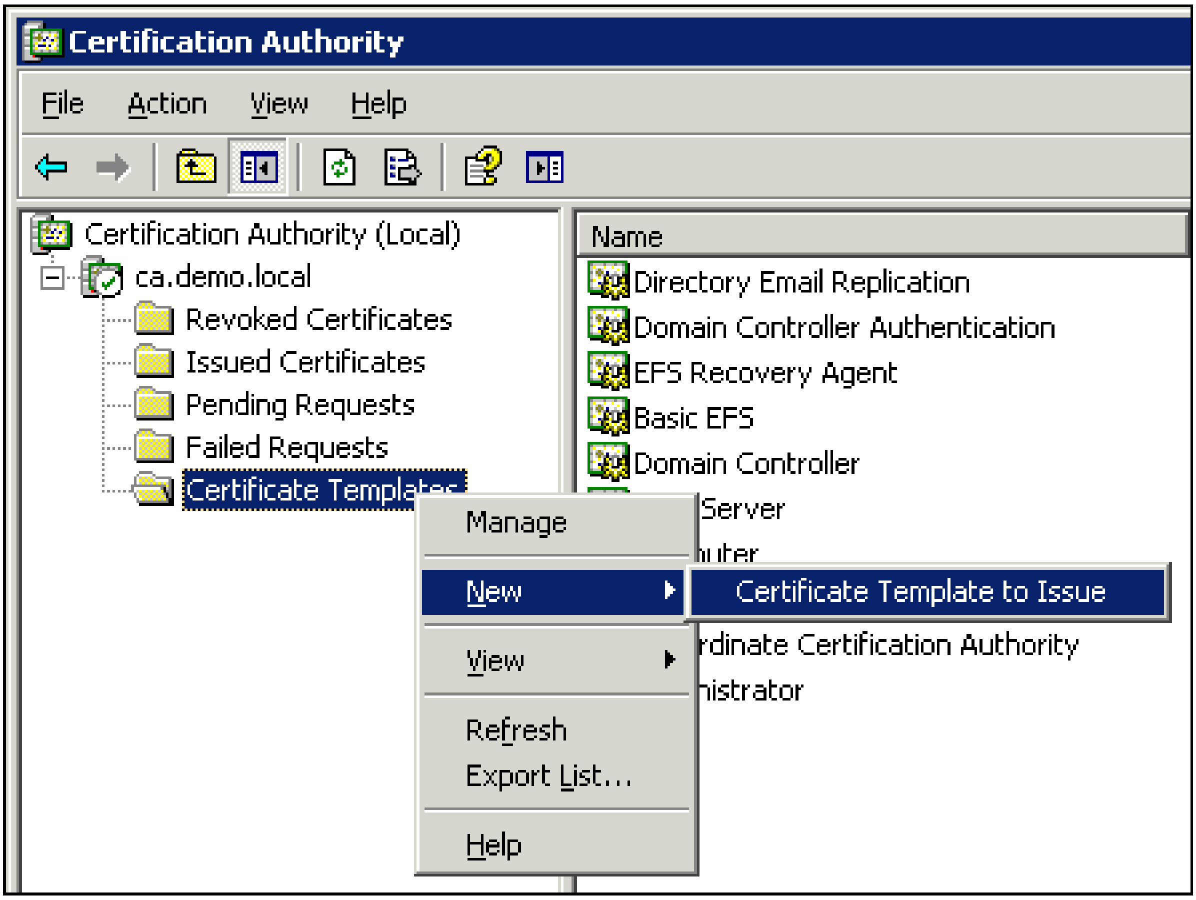
○ Valid existing certificate

9. 单击**确定以保存模板，然后从“证书颁发机构”管理单元发布此模板。**

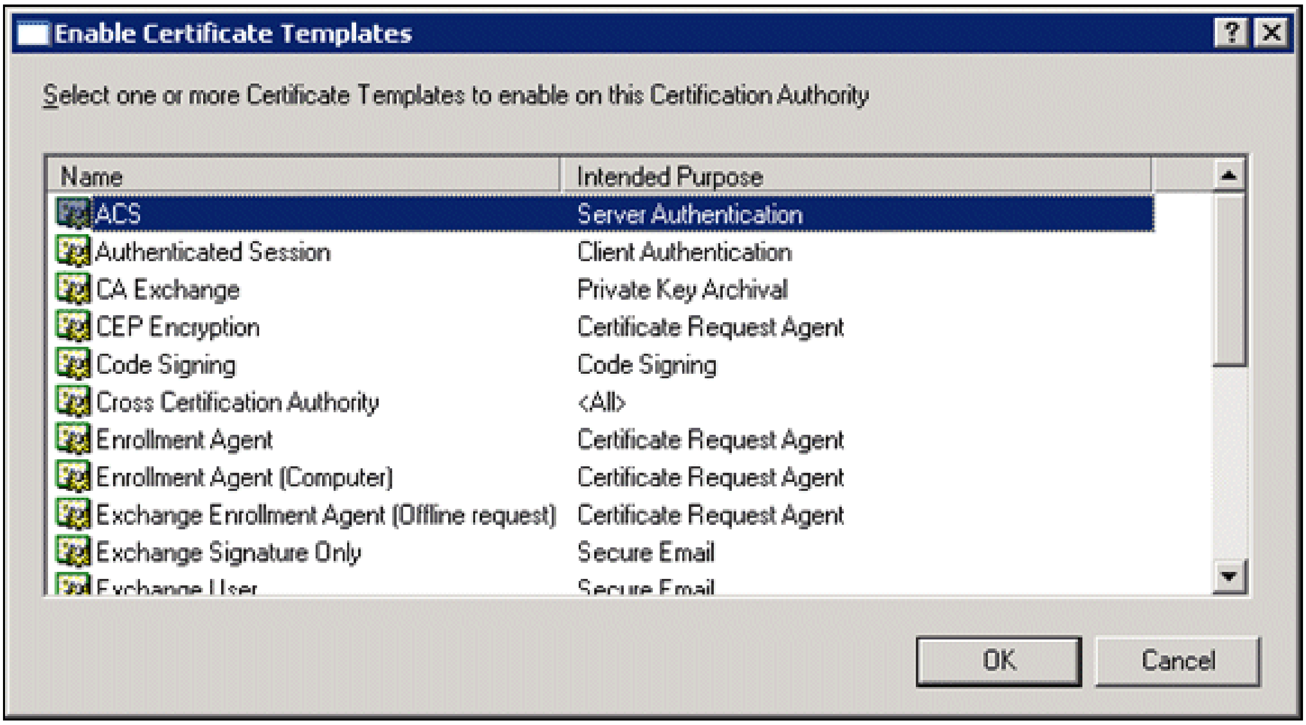
启用新的 ACS Web Server 证书模板

请执行以下步骤：

1. 打开“证书颁发机构”管理单元。执行为 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“证书颁发机构”控制台树中，展开 **ca.demo.local，然后右键单击**证书模板。
3. 转至**新建 > 要颁发的证书模板。**



4. 单击 **ACS 证书模板。**

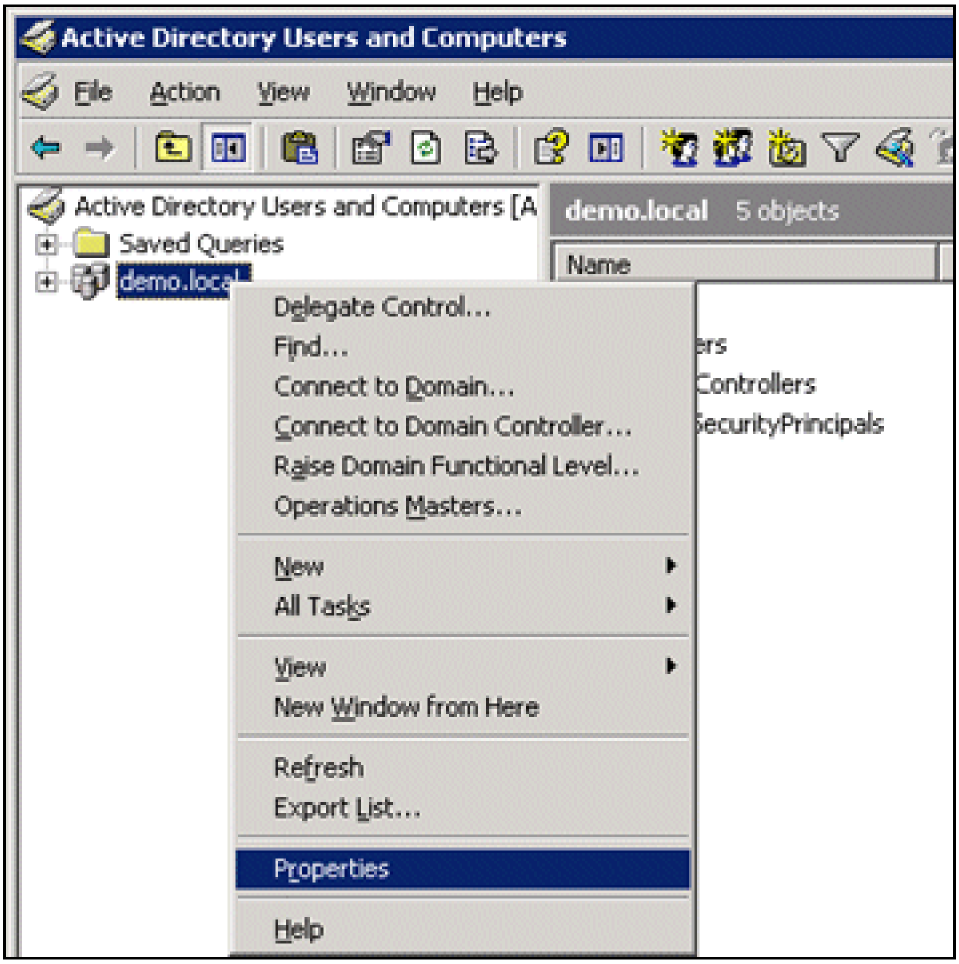


Select one or more Certificate Templates to enable on this Certification Authority

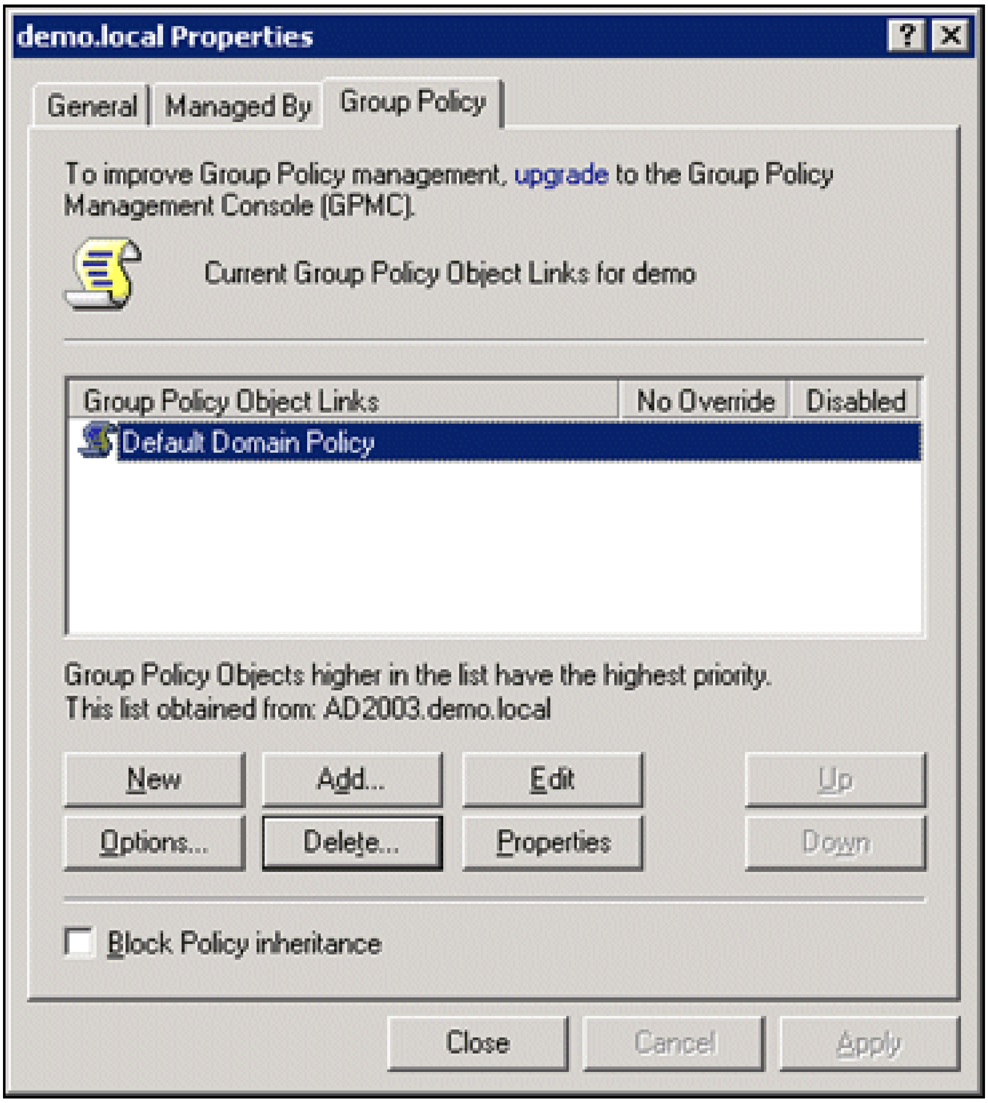
Name	Intended Purpose
ACS	Server Authentication
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate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


demo.local Properties

General | Managed By | Group Policy

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

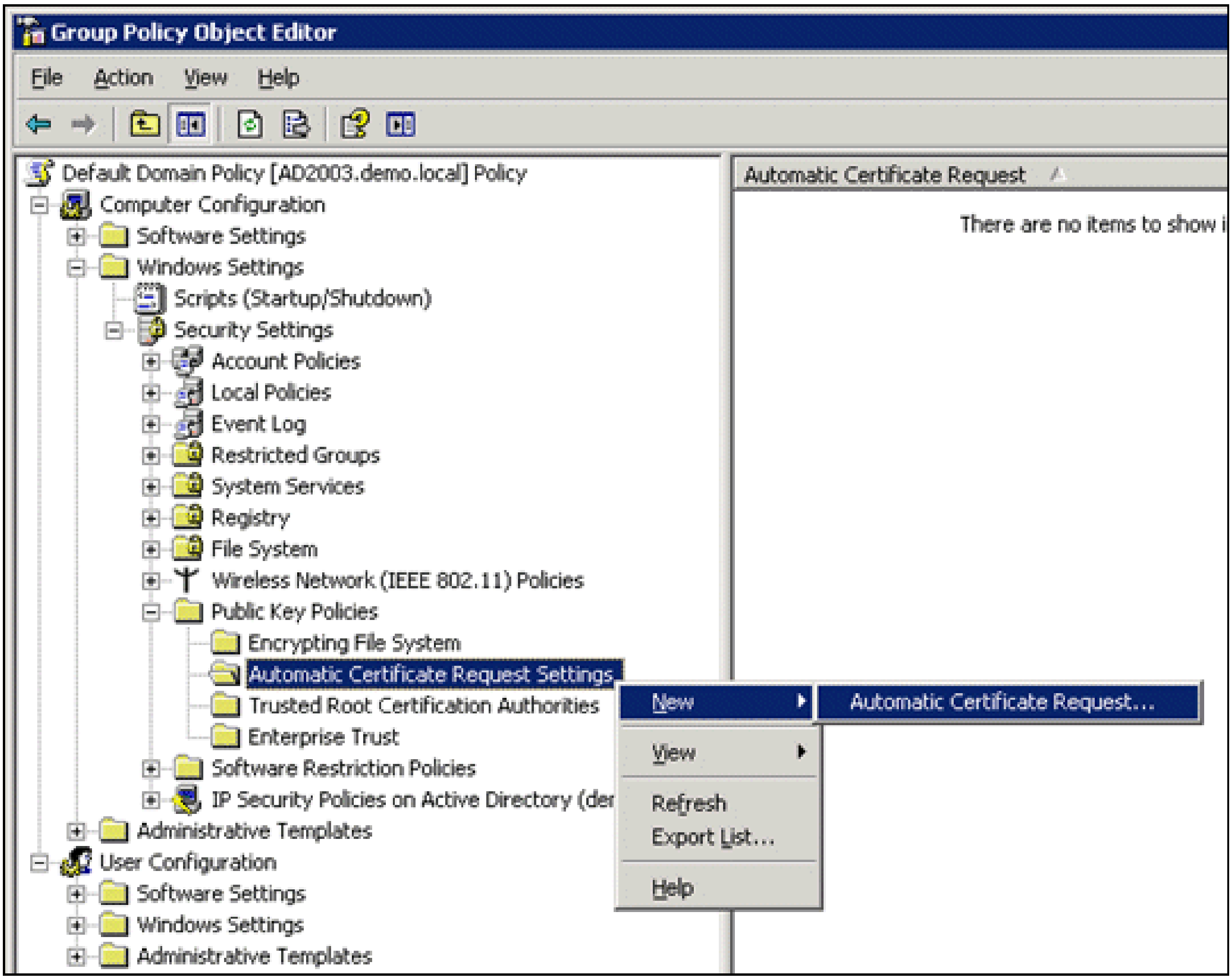
Current Group Policy Object Links for demo

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: AD2003.demo.local

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**。



Group Policy Object Editor

Default Domain Policy [AD2003.demo.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
      - Software Restriction Policies
      - IP Security Policies on Active Directory (der
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

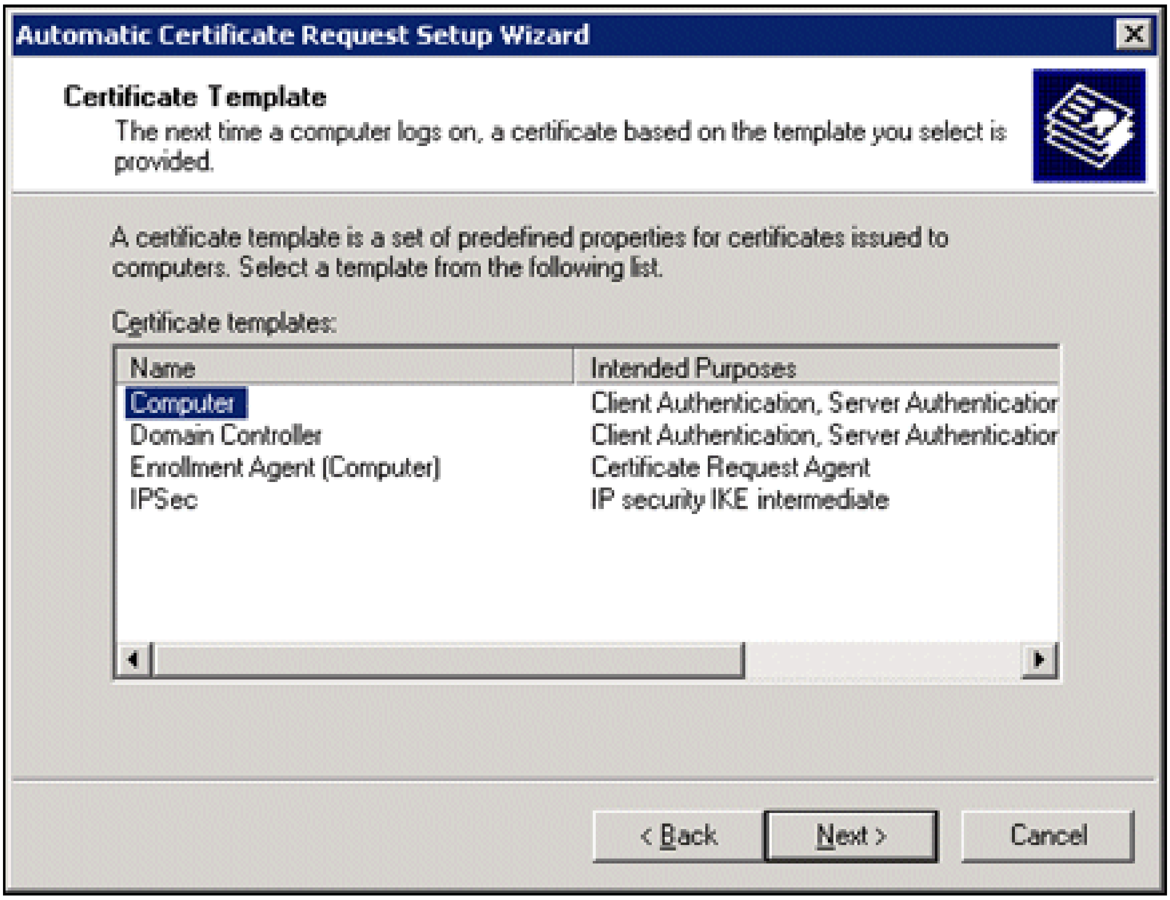
Automatic Certificate Request

There are no items to show i

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。**



Automatic Certificate Request Setup Wizard

Certificate Template

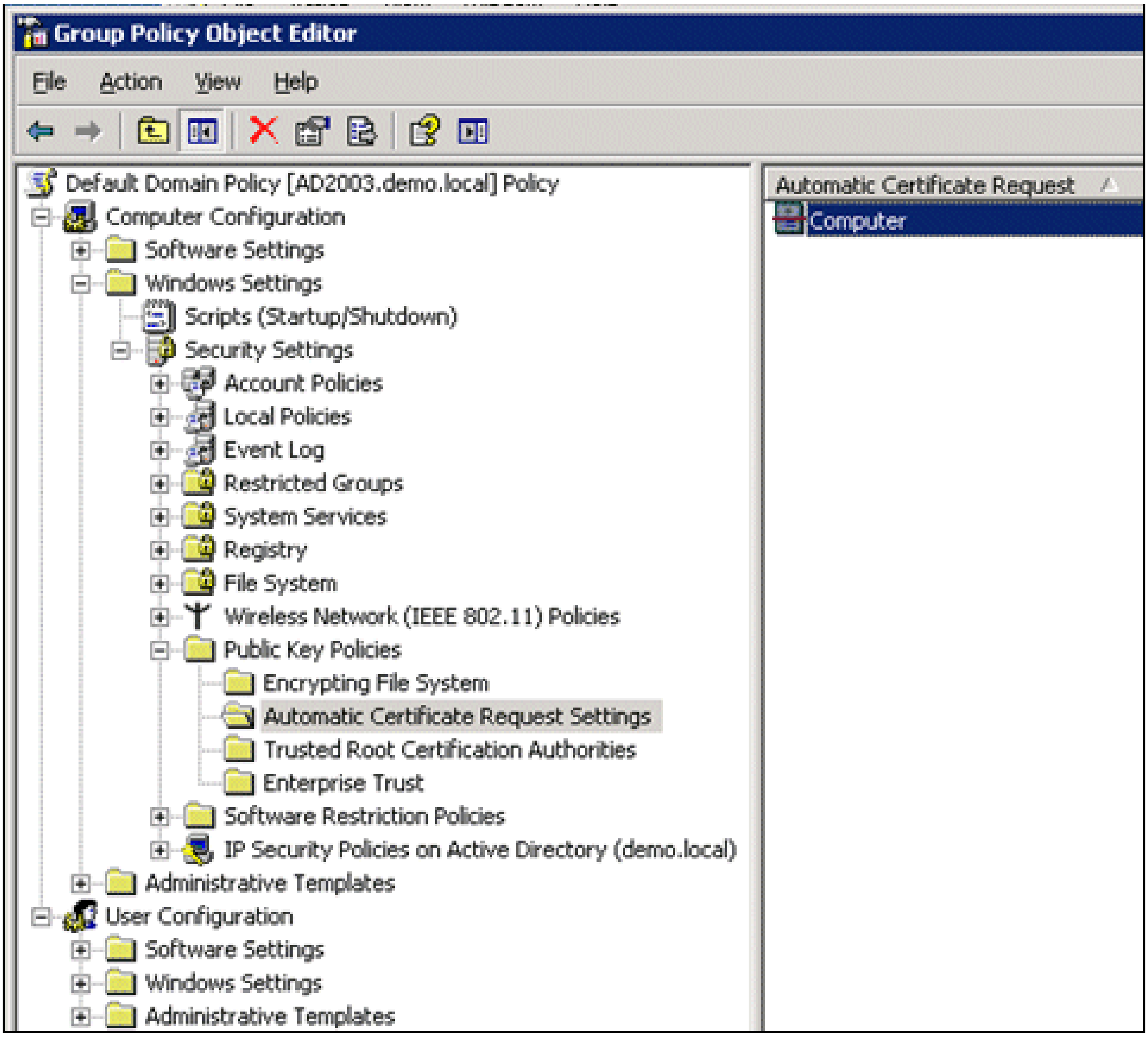
The next time a computer logs on, a certificate based on the template you select is provided.

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

Certificate templates:

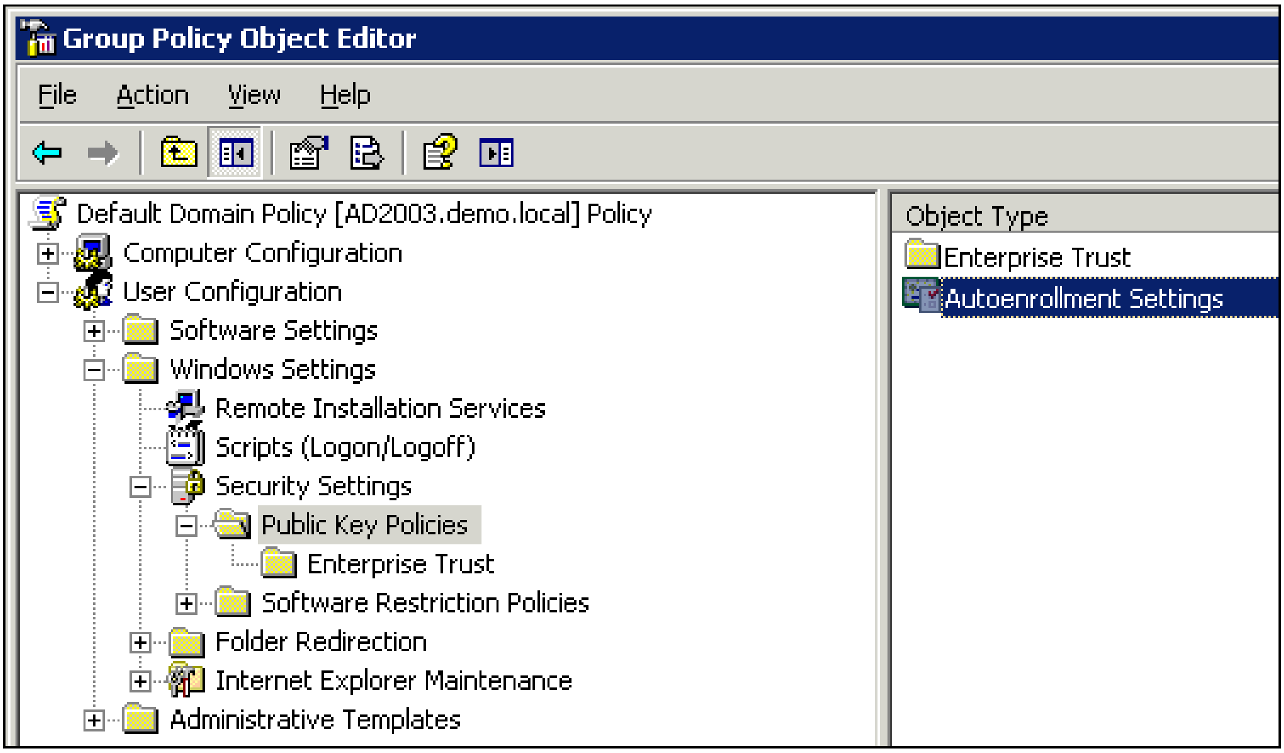
Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSec	IP security IKE intermediate

12. 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。

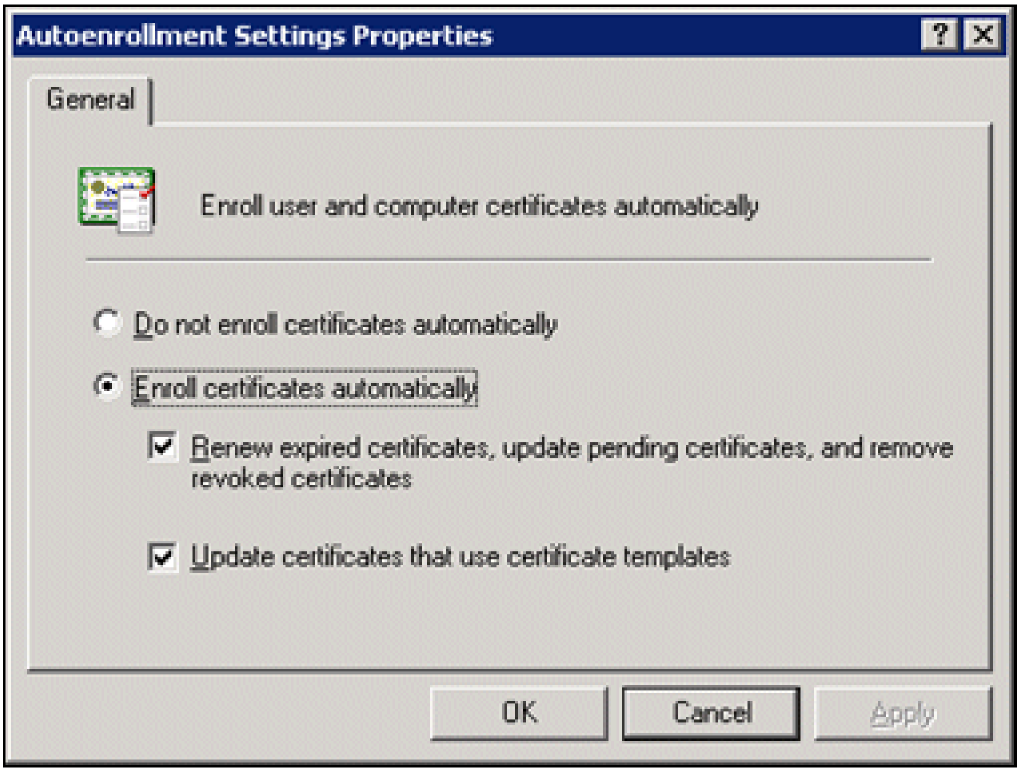


13. 在控制台树中，展开**用户配置 > Windows 设置 > 安全设置 > 公钥策略**。

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”。**



Autoenrollment Settings Properties

General

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**.

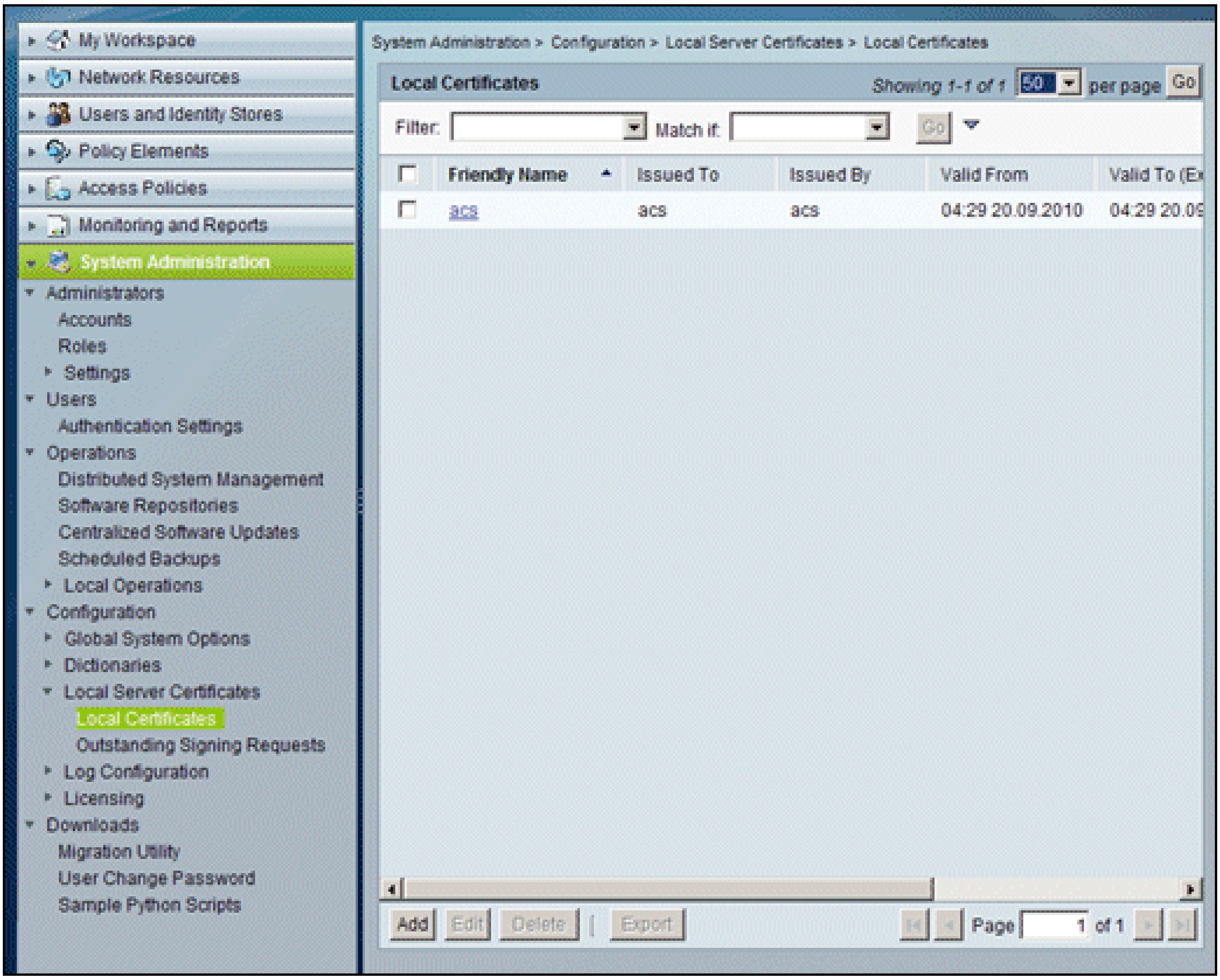
ACS 5.1 证书设置

为 ACS 配置可导出的证书

注意：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。

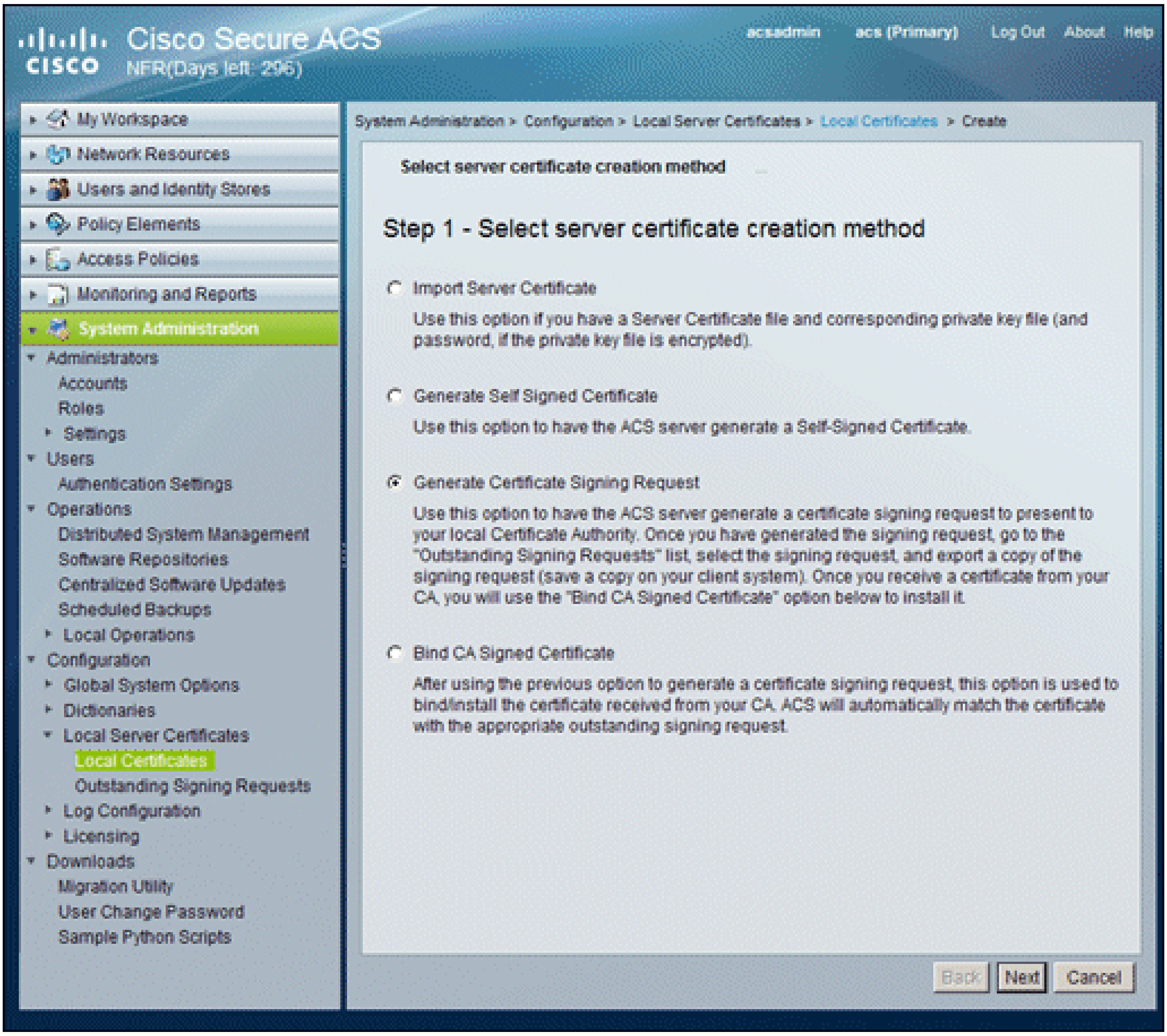
注意：请确保IIS管理器在证书设置过程中未打开，因为缓存的信息存在问题。

1. 使用管理员帐户权限登录到 ACS 服务器。
2. 转至 **System Administration > Configuration > Local Server Certificates**。单击 **Add**。



□	Friendly Name	Issued To	Issued By	Valid From	Valid To (E
□	acs	acs	acs	04:29 20.09.2010	04:29 20.09

3. 选择服务器证书创建方法时，请选择 Generate Certificate Signing Request。单击 Next。



Select server certificate creation method

Step 1 - Select server certificate creation method

○ Import Server Certificate

Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).

○ Generate Self Signed Certificate

Use this option to have the ACS server generate a Self-Signed Certificate.

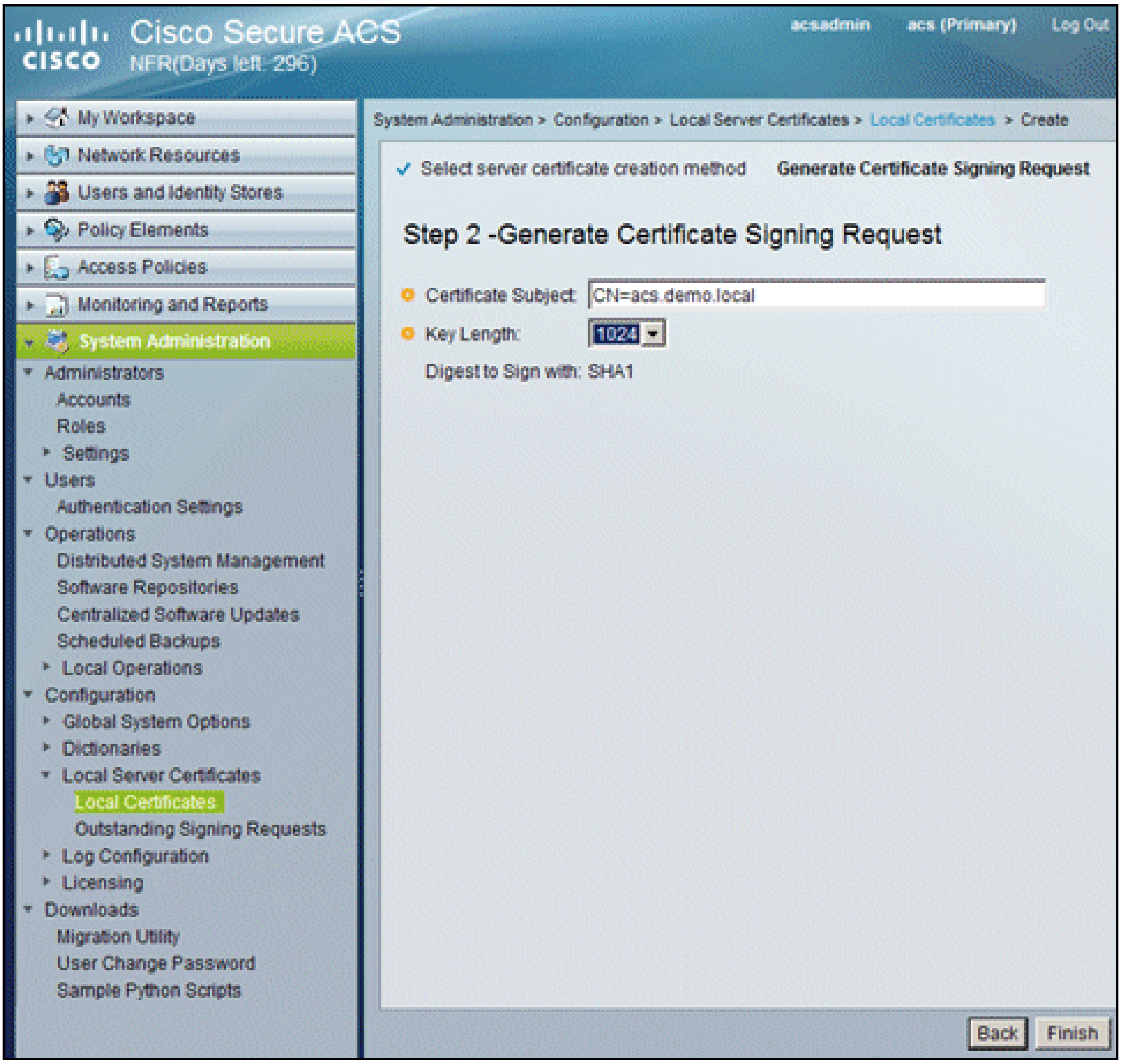
● Generate Certificate Signing Request

Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.

○ Bind CA Signed Certificate

After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

4. 输入证书使用者和密钥长度作为示例，然后单击 **Finish**：证书使用者 (Certificate Subject) - **CN=acs.demo.local**密钥长度 (Key Length) - **1024**



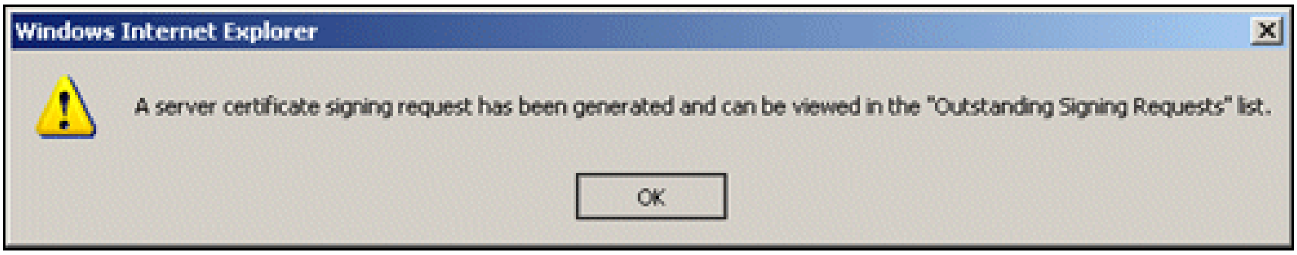
Step 2 -Generate Certificate Signing Request

Certificate Subject: CN=acs.demo.local

Key Length: 1024

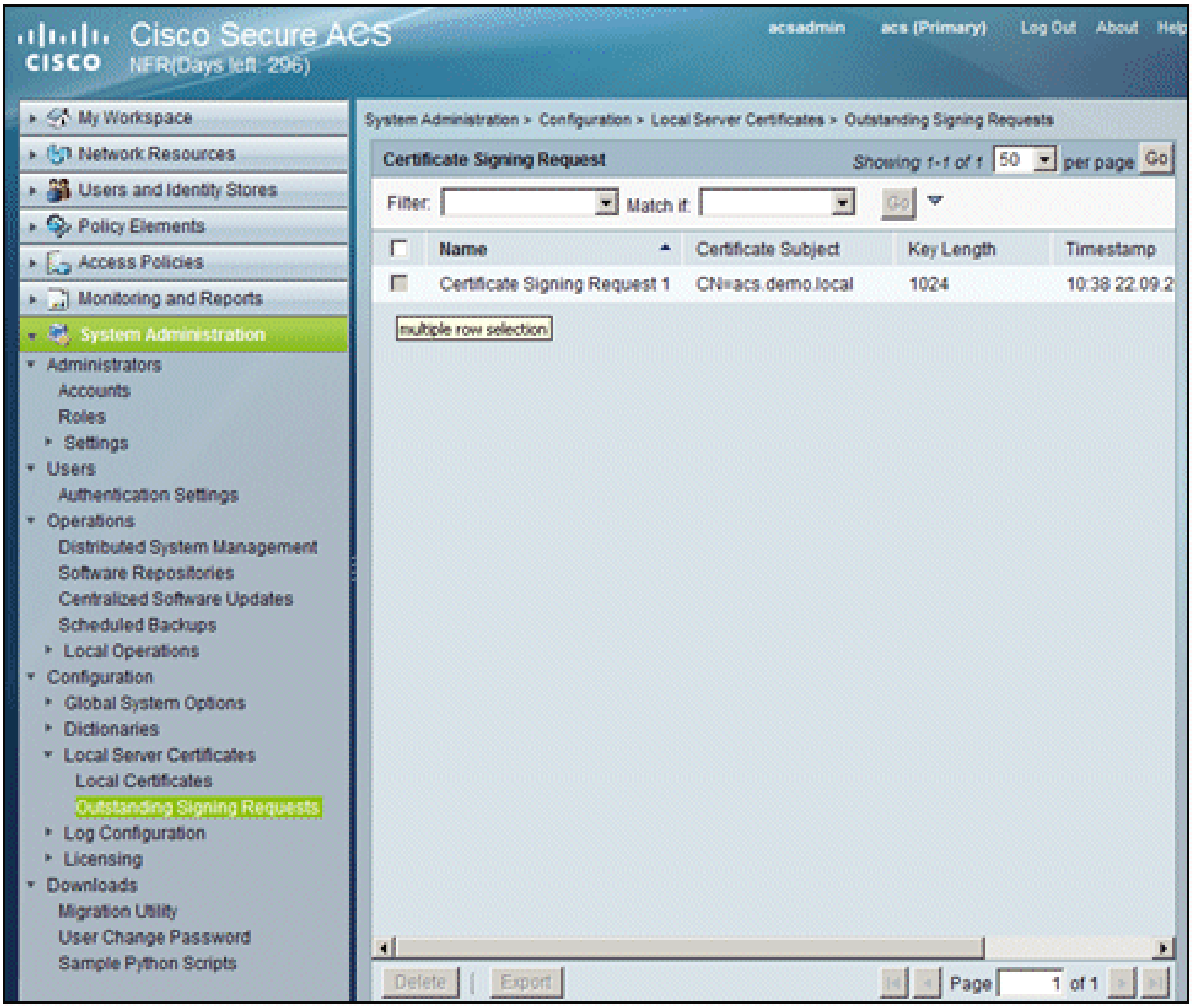
Digest to Sign with: SHA1

5. 生成证书签名申请后，ACS 将进行提示。Click **OK**.



A server certificate signing request has been generated and can be viewed in the "Outstanding Signing Requests" list.

6. 在 System Administration 下，转至 **Configuration > Local Server Certificates > Outstanding Signing Requests**。**注：此**步骤的原因是Windows 2003不允许可导出密钥，您需要根据之前创建的ACS证书生成证书请求。



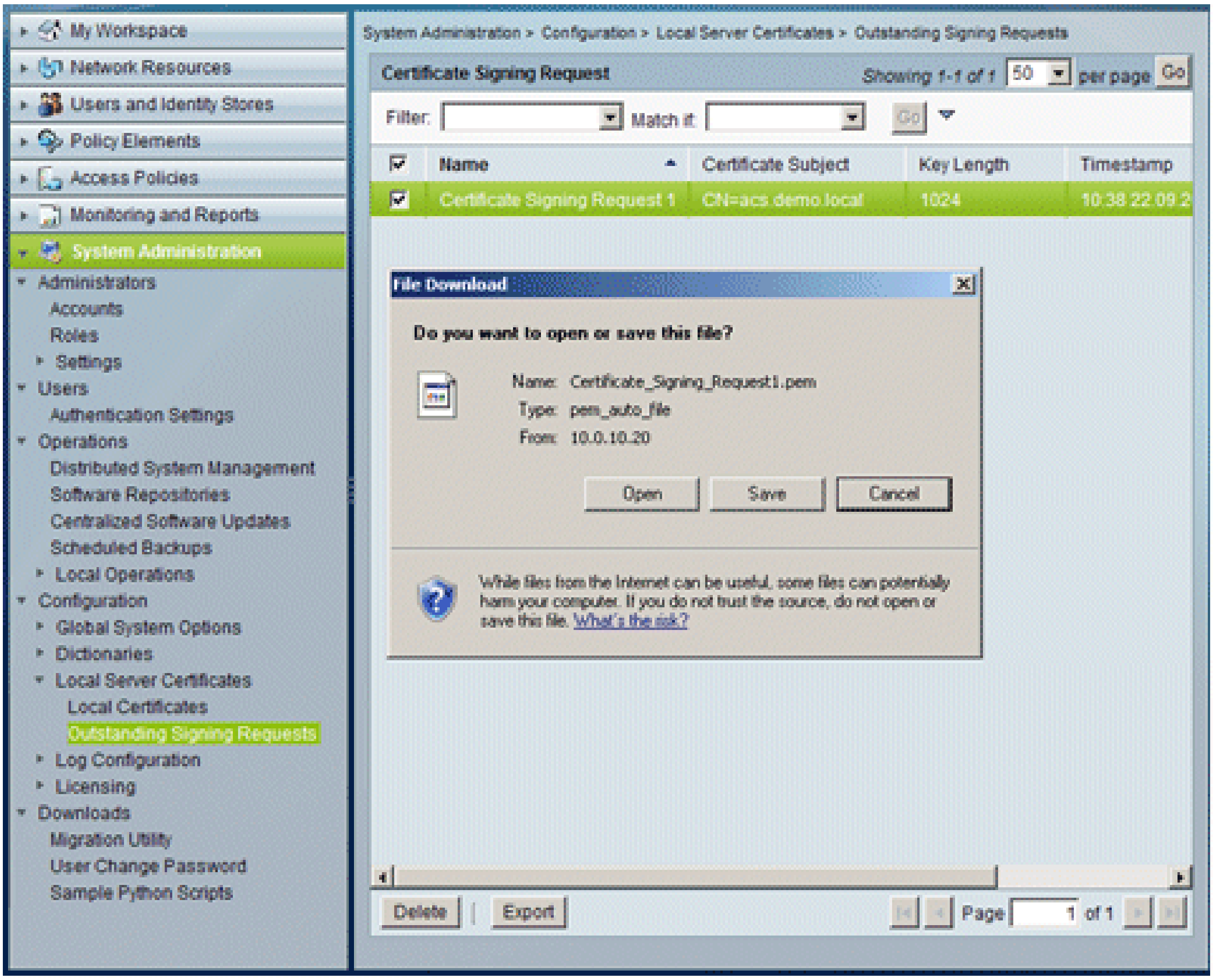
System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests

Certificate Signing Request — Showing 1-1 of 1 — 50 per page

Filter: Match if:

□	Name	Certificate Subject	Key Length	Timestamp
□	Certificate Signing Request 1	CN=acs.demo.local	1024	10:38 22.09.2

7. 选择 **Certificate Signing Request 条目，然后单击 Export**。



System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests

Certificate Signing Request — Showing 1-1 of 1 — 50 per page — Go

Filter: Match if: Go

☑	Name	Certificate Subject	Key Length	Timestamp
☑	Certificate Signing Request 1	CN=acs.demo.local	1024	10:38 22.09.2

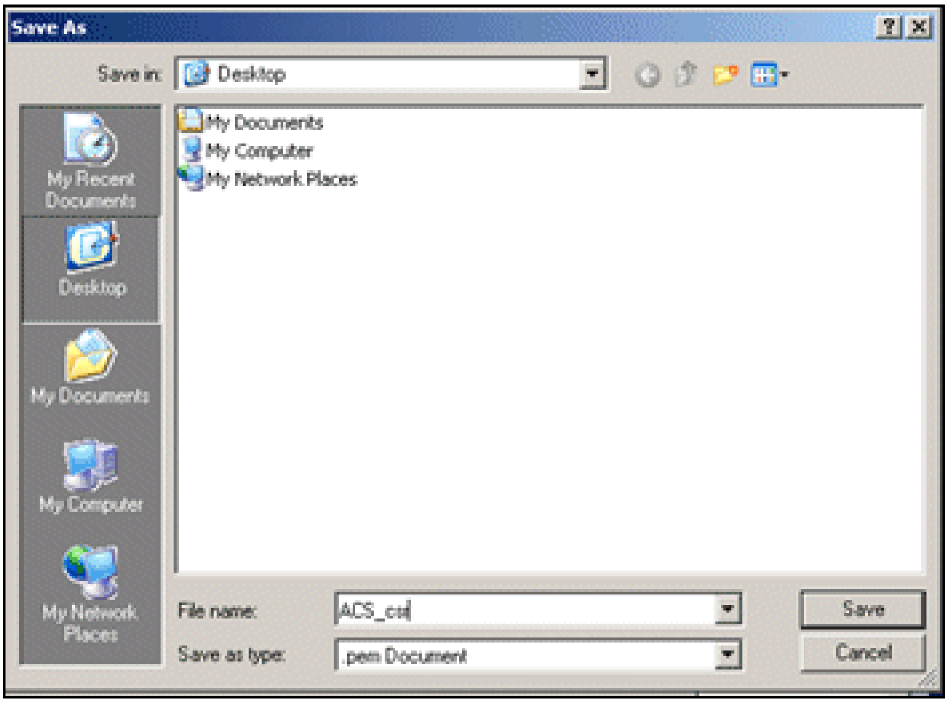
File Download

Do you want to open or save this file?

Name: Certificate_Signing_Request1.pem
Type: pem_auto_file
From: 10.0.10.20

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

8. 将 ACS 证书 **.pem 文件保存到桌面。**



Save As

Save in: Desktop

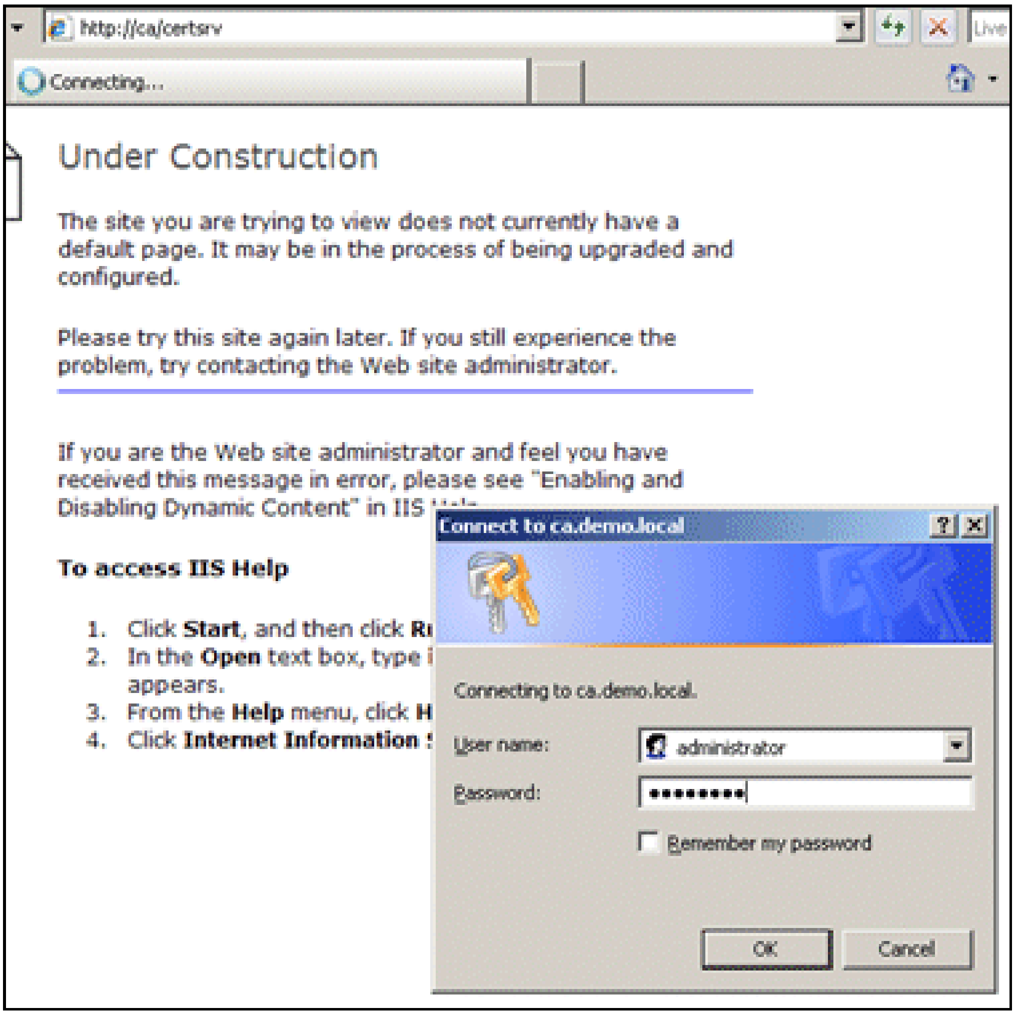
My Documents
My Computer
My Network Places

File name: ACS_csr
Save as type: .pem Document

在 ACS 5.1 软件中安装证书

请执行以下步骤：

1. 打开浏览器并连接到 CA 服务器 URL **http://10.0.10.10/certsrv**。


http://ca/certsrv

Connecting...

Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

If you are the Web site administrator and feel you have received this message in error, please see "Enabling and Disabling Dynamic Content" in IIS

To access IIS Help

1. Click **Start**, and then click **R**
2. In the **Open** text box, type i appears.
3. From the **Help** menu, click **H**
4. Click **Internet Information**

Connect to ca.demo.local

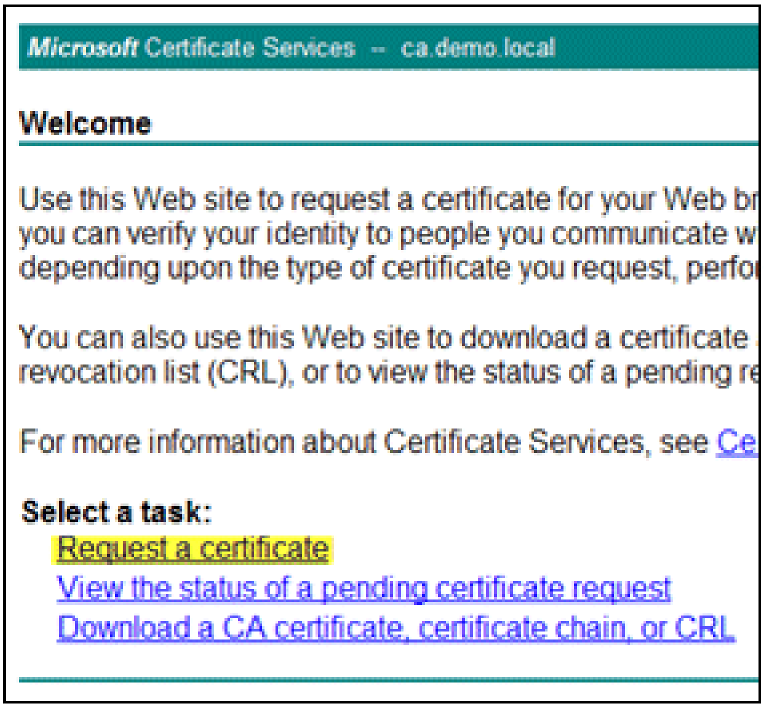
Connecting to ca.demo.local.

User name: administrator

Password: •••••••••

□ Remember my password

2. 此时将显示“Microsoft 证书服务”窗口。选择 **Request a certificate**。


Microsoft Certificate Services -- ca.demo.local

Welcome

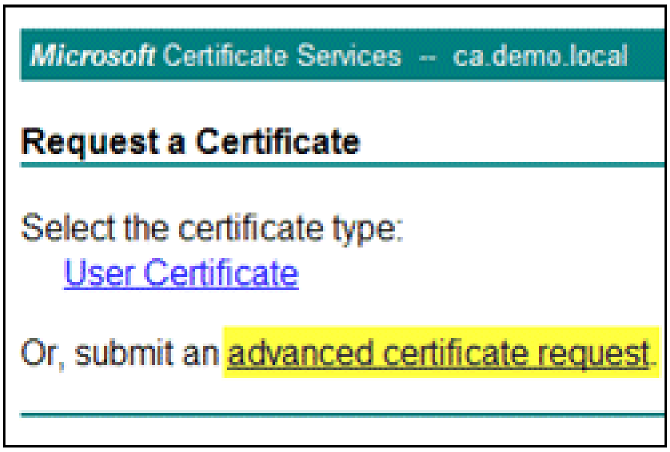
Use this Web site to request a certificate for your Web br you can verify your identity to people you communicate w depending upon the type of certificate you request, perfo

You can also use this Web site to download a certificate revocation list (CRL), or to view the status of a pending re

For more information about Certificate Services, see Ce

Select a task:

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



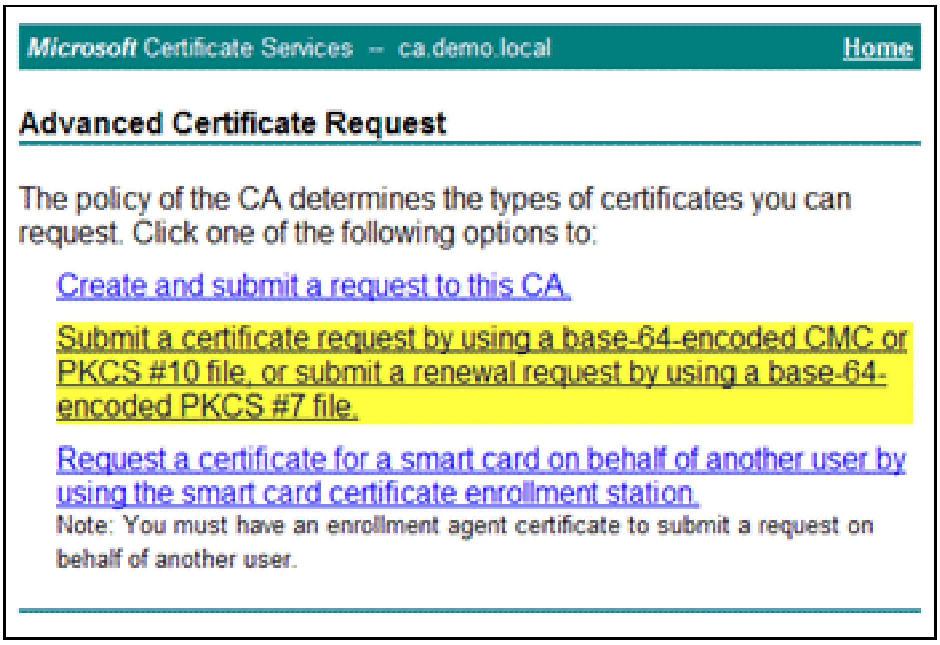
Microsoft Certificate Services -- ca.demo.local

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

3. 单击以提交**高级证书申请。**
4. 在“高级申请”中，单击**使用 Base 64 编码的...提交证书申请。**



Microsoft Certificate Services -- ca.demo.local Home

Advanced Certificate Request

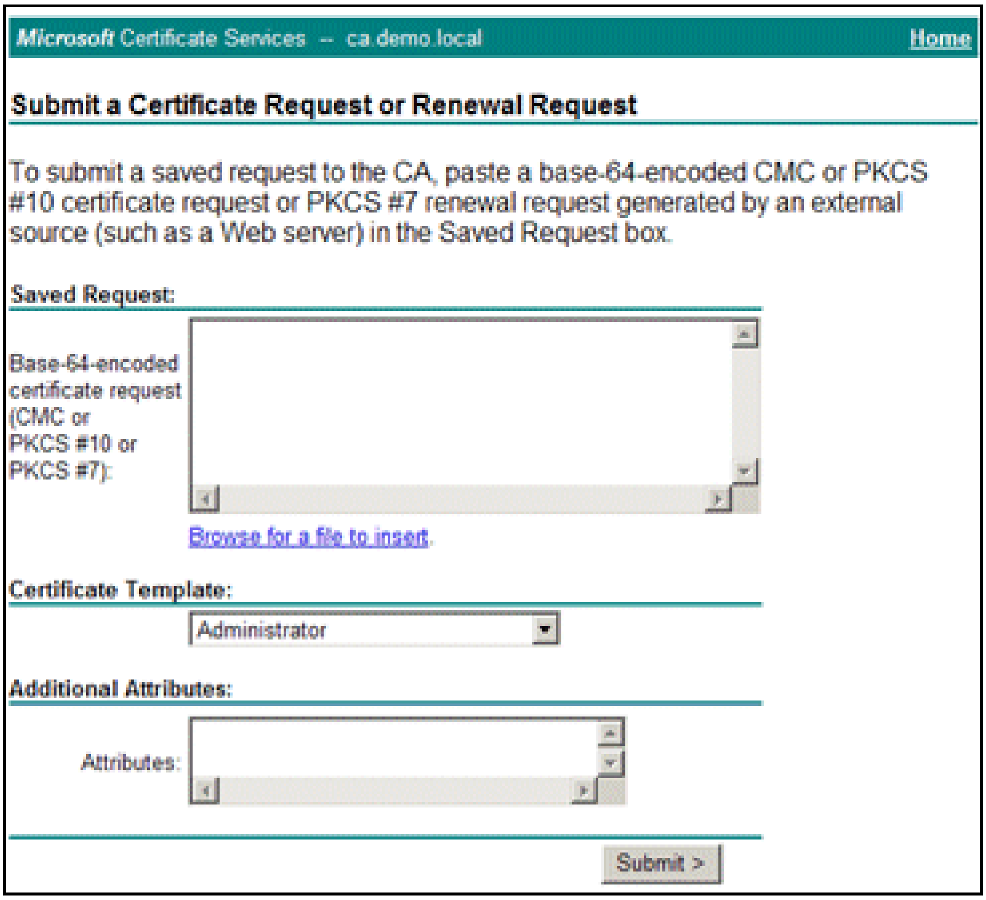
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

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.

5. 如果浏览器安全许可，请在“保存的申请”字段中浏览到上一个 ACS 证书申请文件并插入该文



Microsoft Certificate Services -- ca.demo.local

Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Browse for a file to insert.

Certificate Template:

Administrator

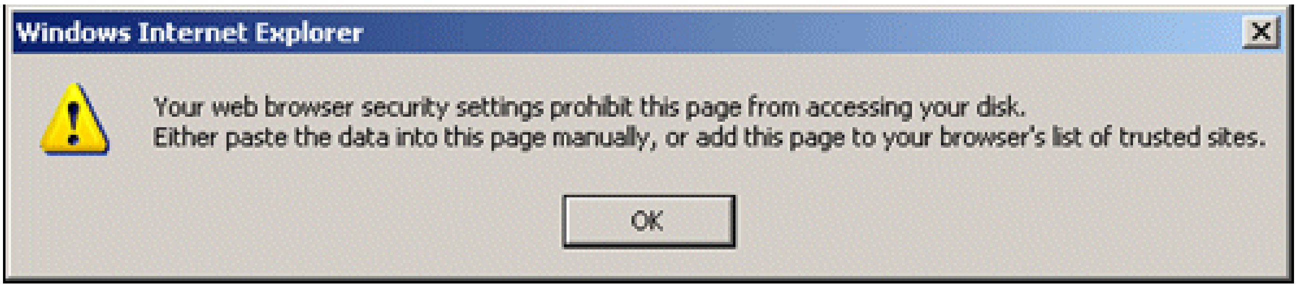
Additional Attributes:

Attributes:

Submit >

件。

6. 浏览器的安全设置可能不允许访问磁盘上的文件。如果出现这种情况，请单击**确定进行手动粘贴。**

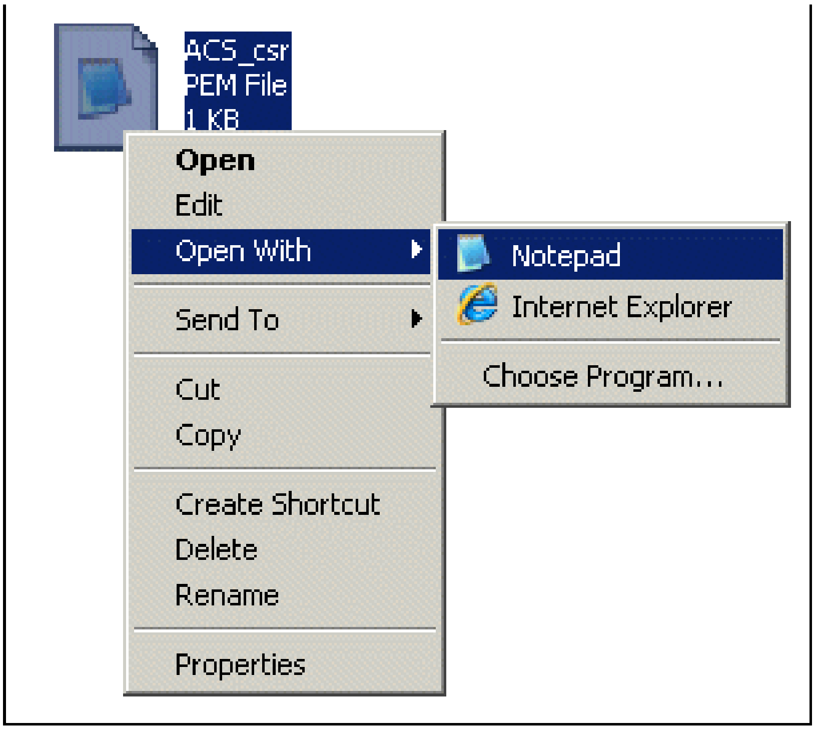


Windows Internet Explorer

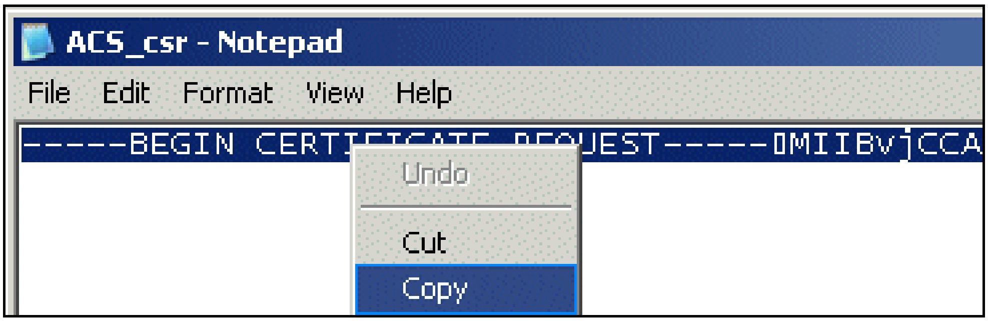
Your web browser security settings prohibit this page from accessing your disk.
Either paste the data into this page manually, or add this page to your browser's list of trusted sites.

OK

7. 找到之前从 ACS 导出的 ACS *.pem 文件。使用文本编辑器（如 Notepad）打开该文件。

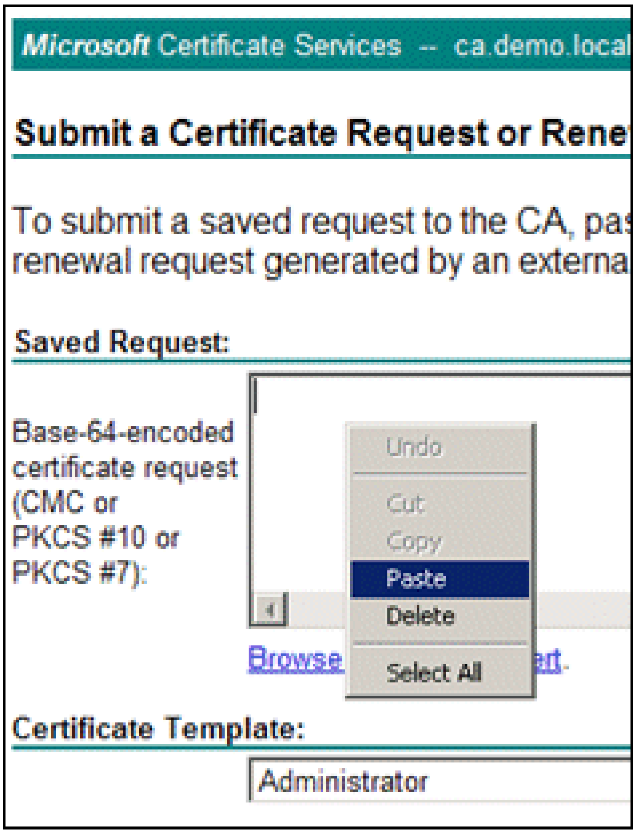


8. 突出显示文件的整个内容，然后单击**复制**。



```
-----BEGIN CERTIFICATE REQUEST-----MIIBvjCCA
```

9. 返回到 Microsoft 证书申请窗口。**将复制的内容粘贴到“保存的申请”字段。**



Submit a Certificate Request or Rene

To submit a saved request to the CA, pas renewal request generated by an externa

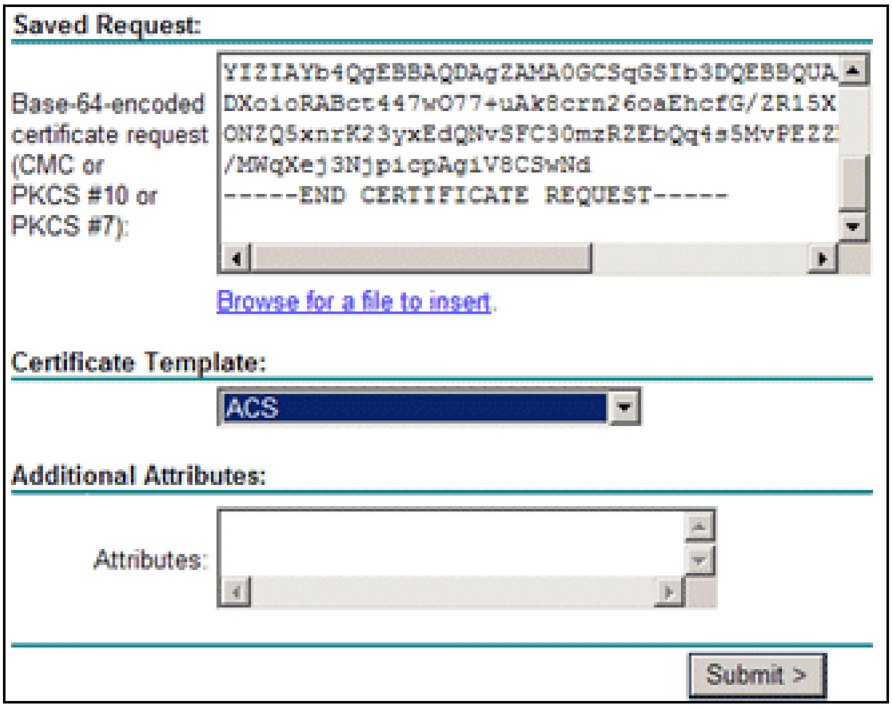
Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Administrator

10. 选择 **ACS 作为“证书模板”，然后单击提交。**



Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
YIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUA
DXoioRABct447wO77+uAk8crn26oaEhcfG/ZR15X
ONZQ5xnrK23yxEdQNvSFC30mzR2EbQq4s5MvPE2Z
/MWqXej3NjpicpAgiV8C3wNd
-----END CERTIFICATE REQUEST-----
```

Browse for a file to insert.

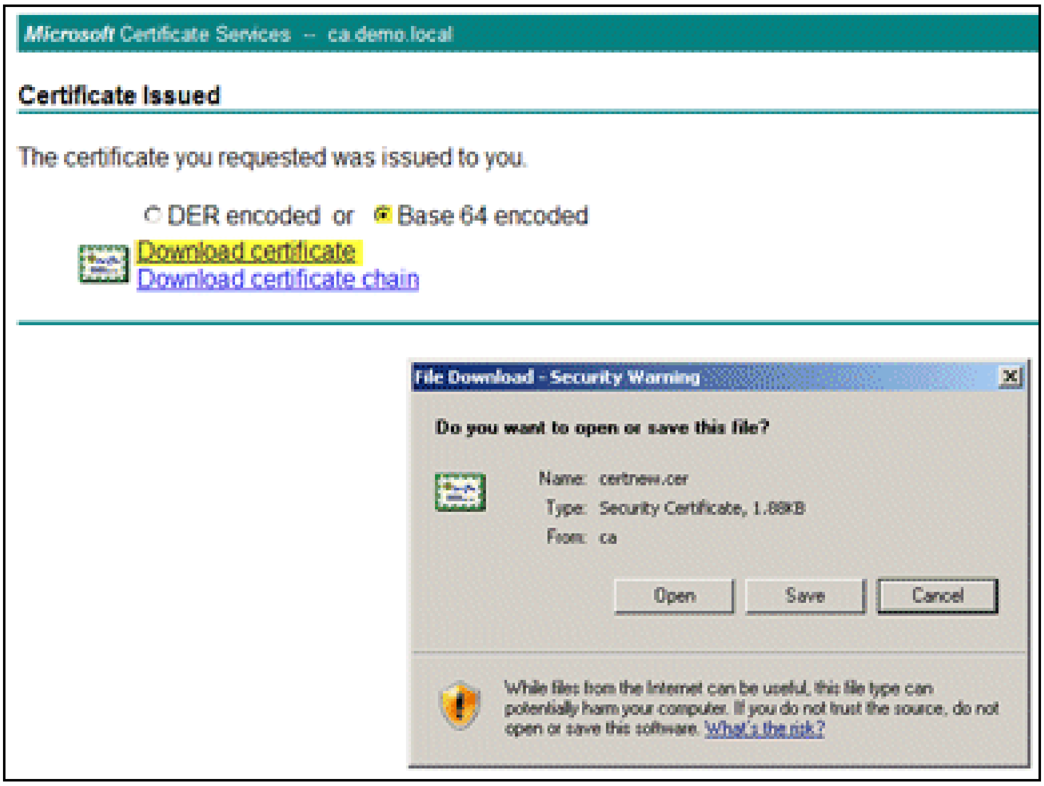
Certificate Template:

ACS

Additional Attributes:

Attributes:

11. 发布证书后，请选择 **Base 64 编码**，然后单击**下载证书。**



Microsoft Certificate Services -- ca.demo.local

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

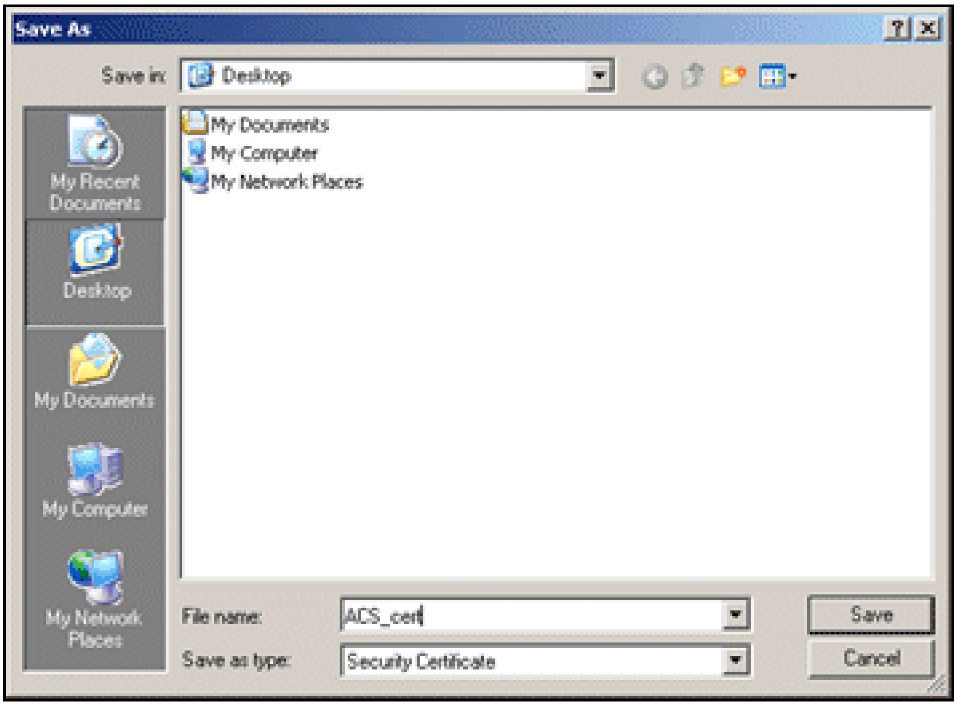
File Download - Security Warning

Do you want to open or save this file?

Name: certnew.cer
Type: Security Certificate, 1.88KB
From: ca

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?

12. 单击**保存，将证书保存到桌面。**



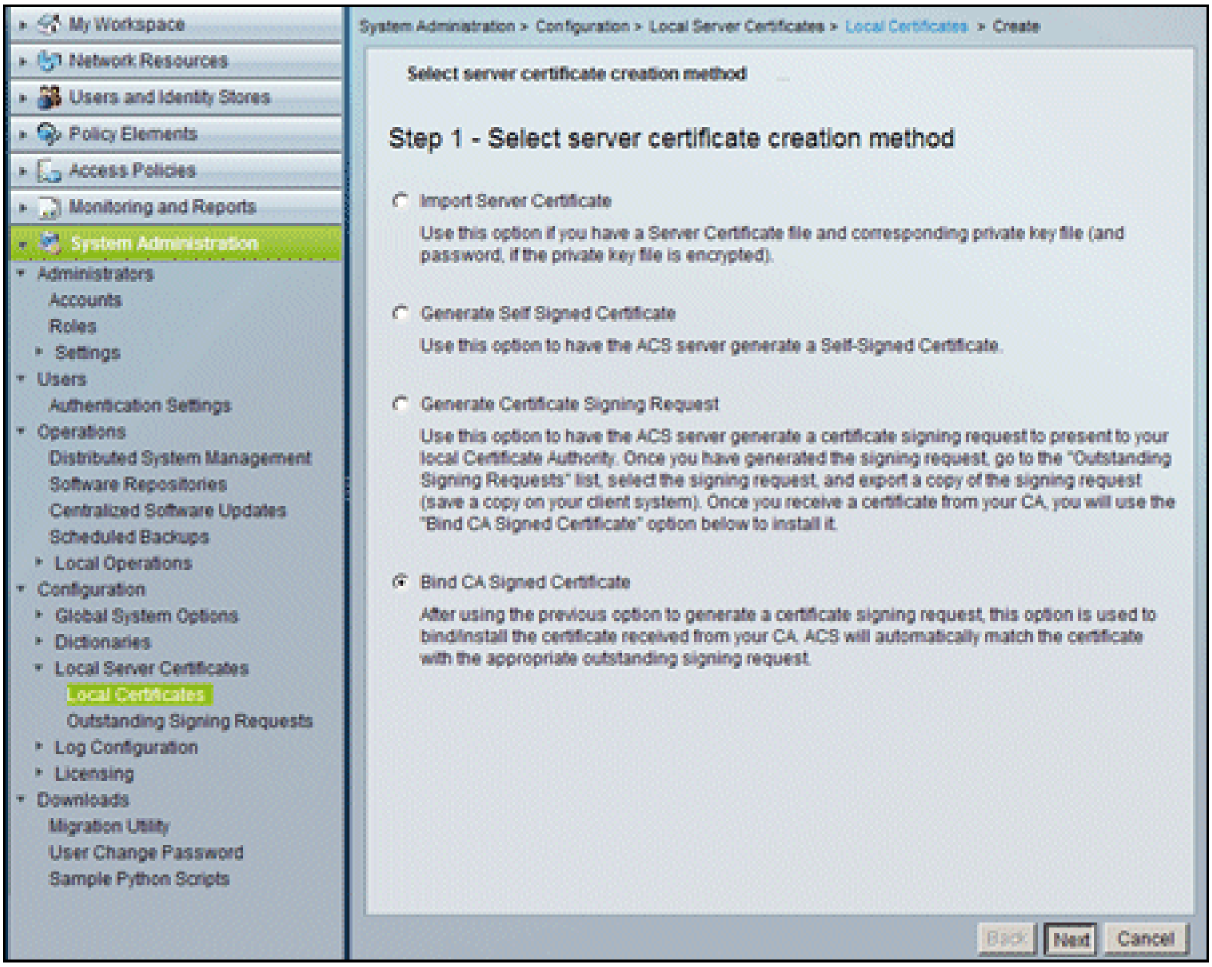
Save in: Desktop

My Documents
My Computer
My Network Places

File name: ACS_cert

Save as type: Security Certificate

13. 转至 **ACS > System Administration > Configuration > Local Server Certificates**。选择 **Bind CA Signed Certificate**，然后单击 **Next**。



System Administration > Configuration > Local Server Certificates > Local Certificates > Create

Select server certificate creation method

Step 1 - Select server certificate creation method

○ Import Server Certificate

Use this option if you have a Server Certificate file and corresponding private key file (and password, if the private key file is encrypted).

○ Generate Self Signed Certificate

Use this option to have the ACS server generate a Self-Signed Certificate.

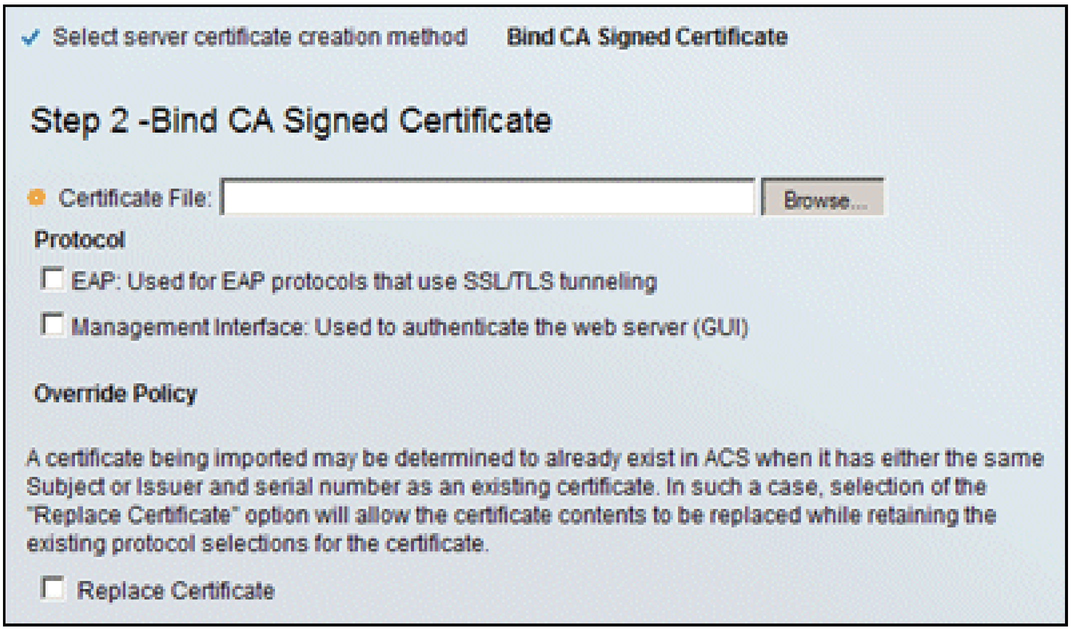
○ Generate Certificate Signing Request

Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.

● Bind CA Signed Certificate

After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

14. 单击 **Browse** 并找到保存的证书。



✓ Select server certificate creation method　**Bind CA Signed Certificate**

Step 2 -Bind CA Signed Certificate

Certificate File: 　Browse...

Protocol

□ EAP: Used for EAP protocols that use SSL/TLS tunneling

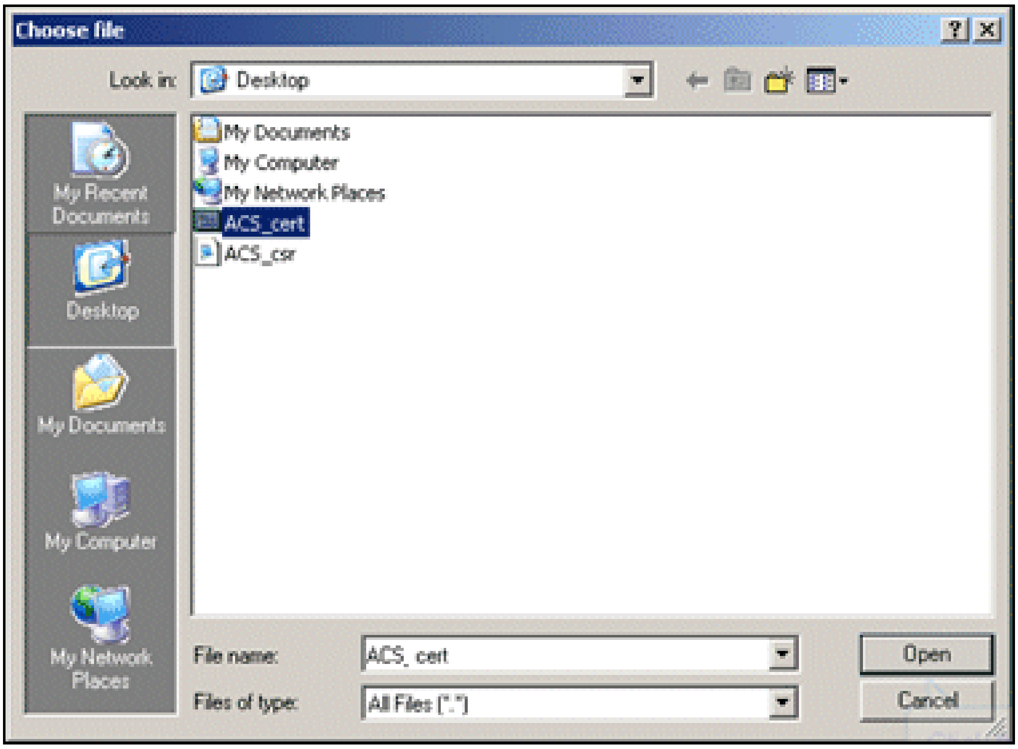
□ Management Interface: Used to authenticate the web server (GUI)

Override Policy

A certificate being imported may be determined to already exist in ACS when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

□ Replace Certificate

15. 选择由 CA 服务器发布的 ACS 证书，然后单击 **Open**。



Choose file

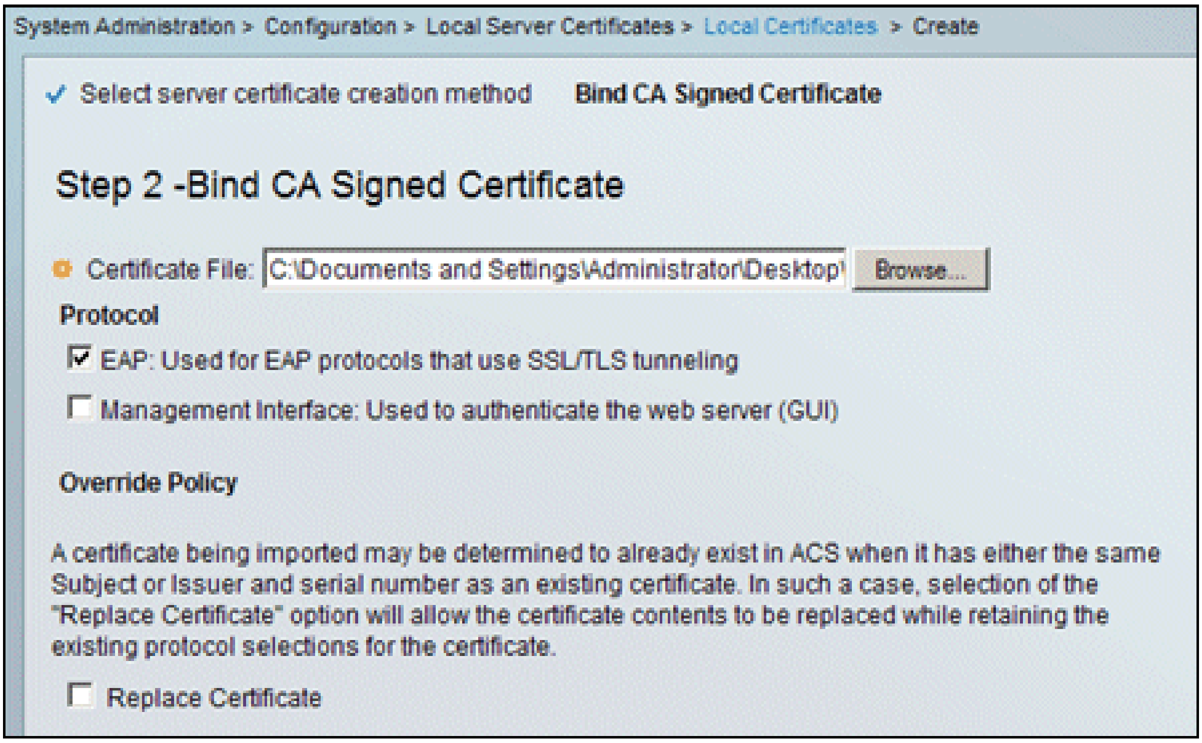
Look in: Desktop

My Documents
My Computer
My Network Places
ACS_cert
ACS_csr

File name: ACS_cert

Files of type: All Files (*.*)

16. 同时，选中 Protocol 下的 **EAP** 复选框，然后单击 **Finish**。


System Administration > Configuration > Local Server Certificates > Local Certificates > Create

✓ Select server certificate creation method   **Bind CA Signed Certificate**

Step 2 -Bind CA Signed Certificate

Certificate File: C:\Documents and Settings\Administrator\Desktop\ Browse...

Protocol

☑ EAP: Used for EAP protocols that use SSL/TLS tunneling

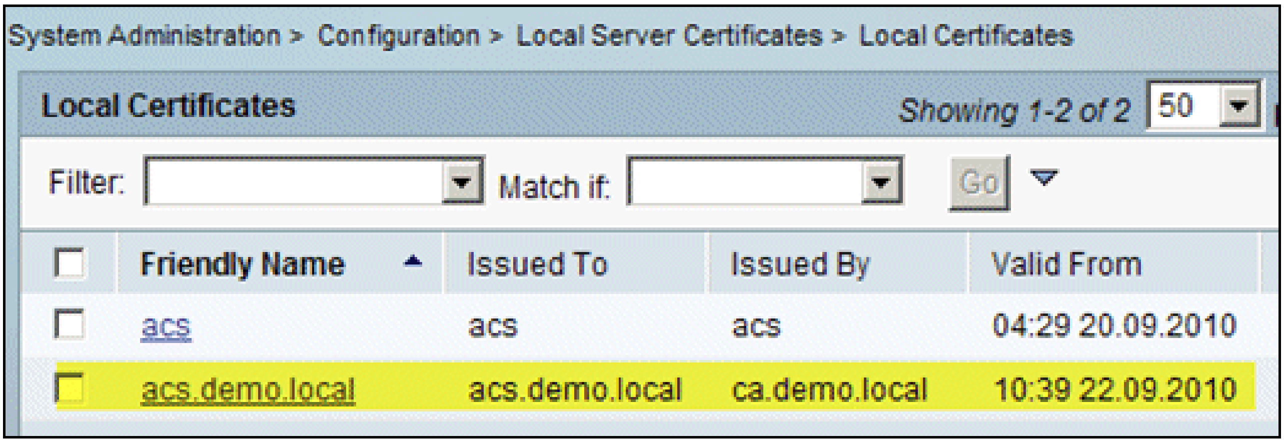
□ Management Interface: Used to authenticate the web server (GUI)

Override Policy

A certificate being imported may be determined to already exist in ACS when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

□ Replace Certificate

17. CA 发布的 ACS 证书将在 ACS 本地证书中出现。


System Administration > Configuration > Local Server Certificates > Local Certificates

Local Certificates   *Showing 1-2 of 2* 50

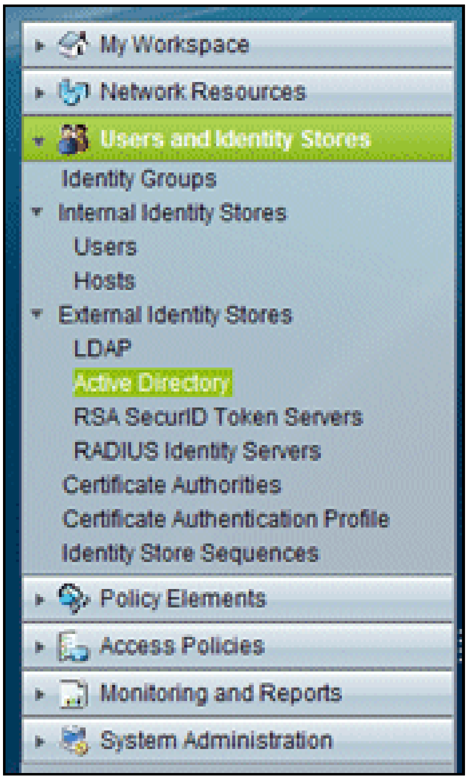
Filter: Match if: Go

□	Friendly Name ▲	Issued To	Issued By	Valid From
□	acs	acs	acs	04:29 20.09.2010
□	acs.demo.local	acs.demo.local	ca.demo.local	10:39 22.09.2010

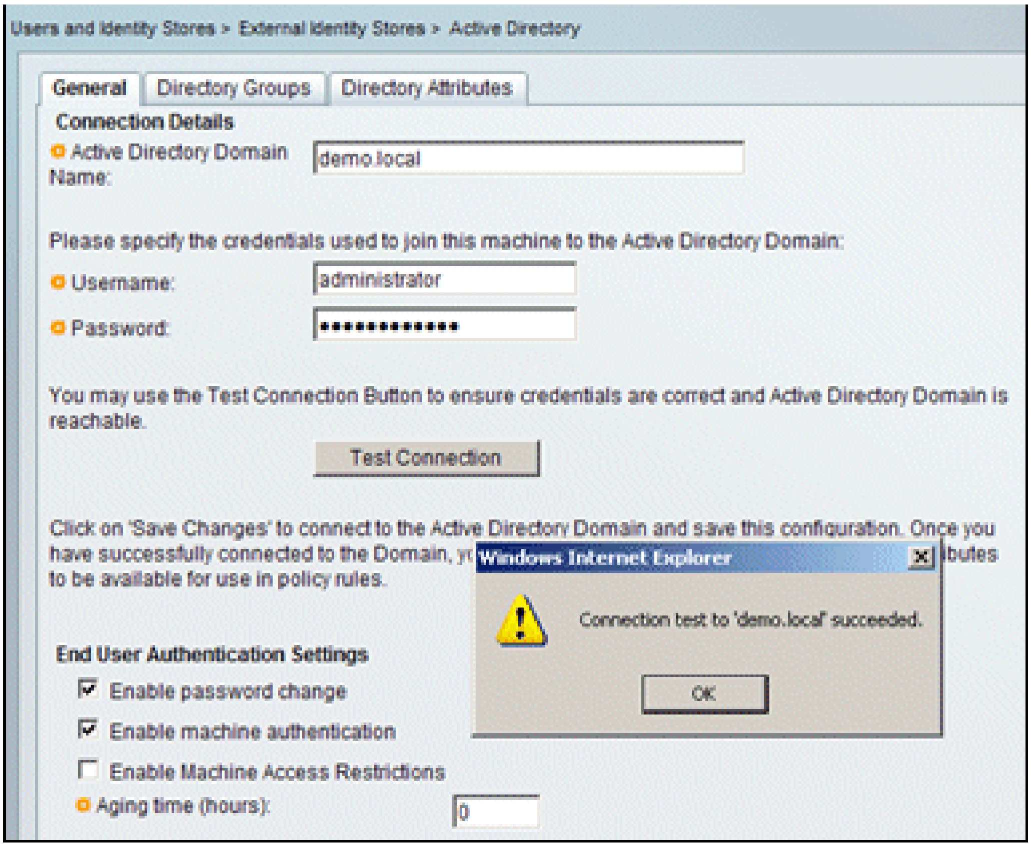
为 Active Directory 配置 ACS 标识存储

请执行以下步骤：

1. 使用管理员帐户连接到 ACS 并登录。
2. 转至 **Users and Identity Stores > External Identity Stores > Active Directory**。



3. 输入 Active Directory 域 *demo.local，输入服务器的口令，然后单击* Test Connection。单击 OK 以继续。


Users and Identity Stores > External Identity Stores > Active Directory
General
Directory Groups
Directory Attributes
Test Connection
OK

Connection Details

Active Directory Domain Name: demo.local

Please specify the credentials used to join this machine to the Active Directory Domain:

Username: administrator

Password: ●●●●●●●●●●●●●

You may use the Test Connection Button to ensure credentials are correct and Active Directory Domain is reachable.

Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have successfully connected to the Domain, y[illegible]ibutes to be available for use in policy rules.

Windows Internet Explorer

Connection test to 'demo.local' succeeded.

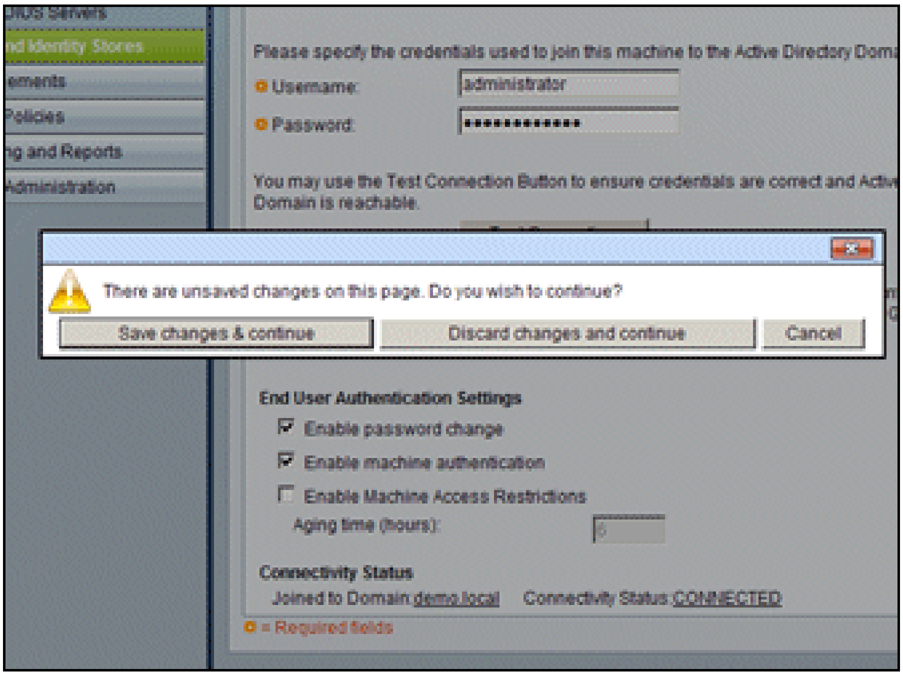
End User Authentication Settings

☑ Enable password change

☑ Enable machine authentication

☐ Enable Machine Access Restrictions

Aging time (hours): 0



Please specify the credentials used to join this machine to the Active Directory Doma

Username: administrator

Password: •••••••••••••

You may use the Test Connection Button to ensure credentials are correct and Activ Domain is reachable.

There are unsaved changes on this page. Do you wish to continue?

End User Authentication Settings

☑ Enable password change

☑ Enable machine authentication

☐ Enable Machine Access Restrictions

Aging time (hours): 6

Connectivity Status

Joined to Domain: demo.local   Connectivity Status: CONNECTED

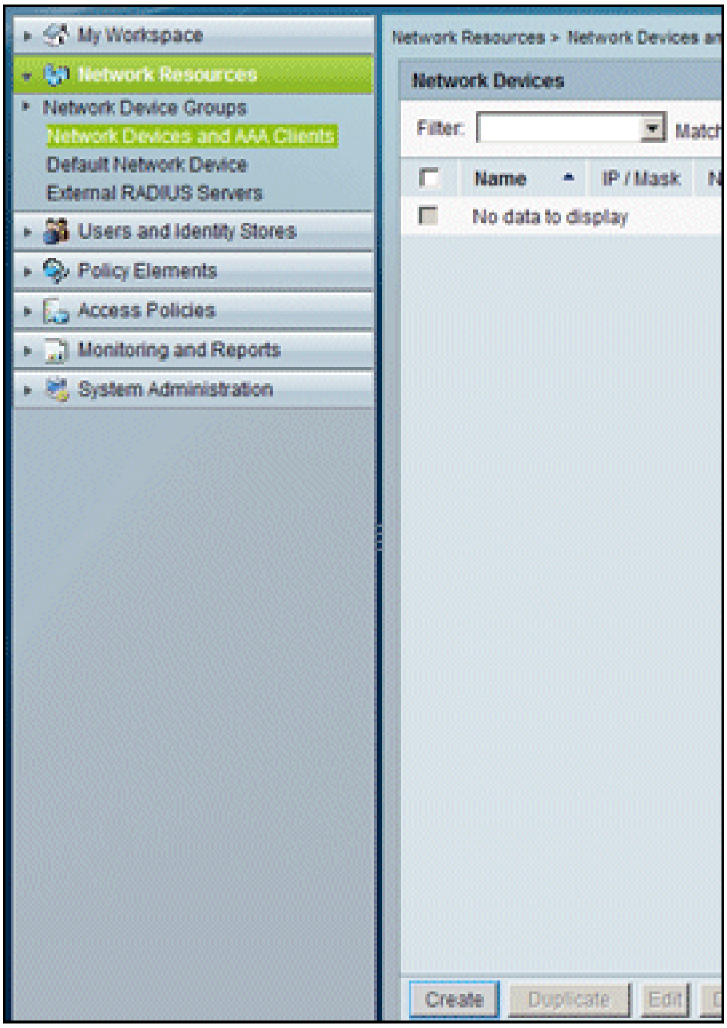
= Required fields

4. 点击**Save Changes**。 **注意**：有关ACS 5.x集成过程的详细信息，请参阅ACS 5.x及更高版本：与Microsoft Active Directory集成的配置示例。

将控制器作为 AAA 客户端添加到 ACS

请执行以下步骤：

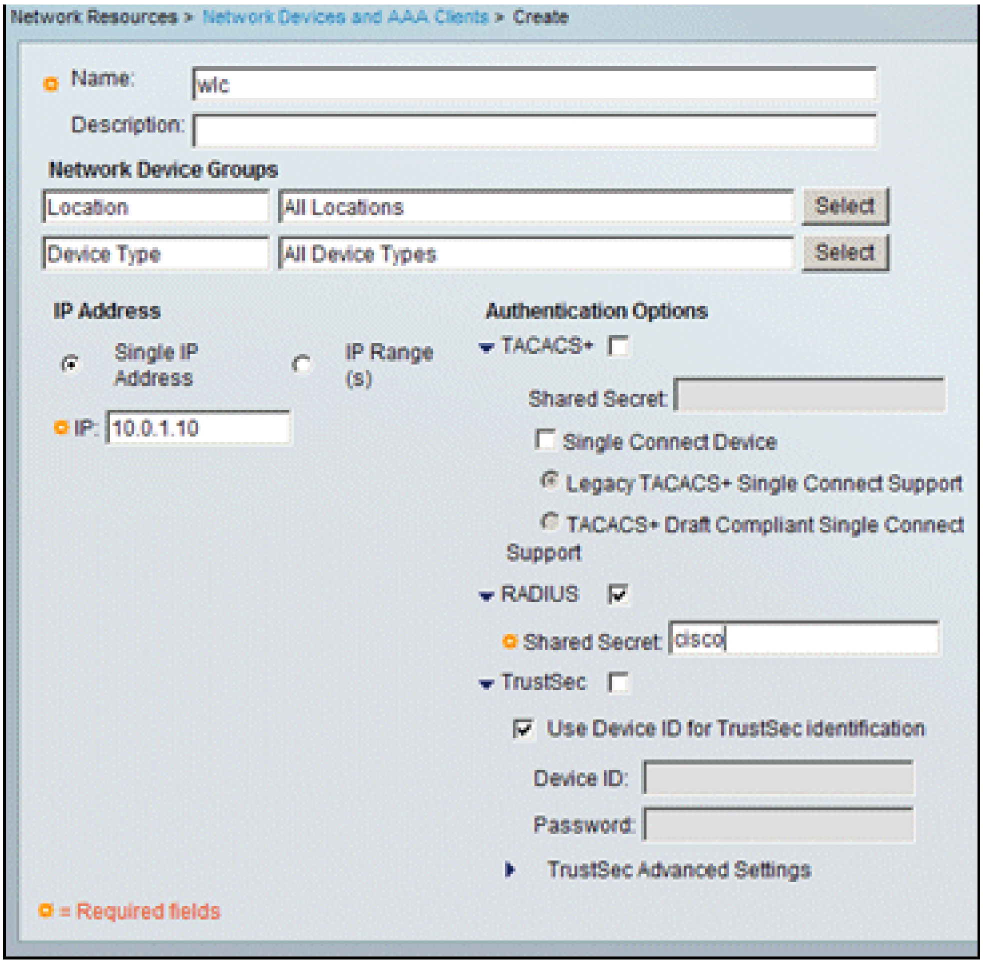
1. 连接到 ACS，然后转至 **Network Resources > Network Devices and AAA Clients**。Click



No data to display

Create.

2. 在以下字段中输入相关内容：名称 (Name) - **wlc**IP - **10.0.1.10**RADIUS 复选框 - **选中**共享密钥 (Shared Secret) -



Network Resources > Network Devices and AAA Clients > Create

Name: wlc

Description:

Network Device Groups

Location	All Locations	Select
Device Type	All Device Types	Select

IP Address

● Single IP Address ○ IP Range (s)

IP: 10.0.1.10

Authentication Options

TACACS+ □

Shared Secret:

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

RADIUS ☑

Shared Secret: cisco

TrustSec □

☑ Use Device ID for TrustSec identification

Device ID:

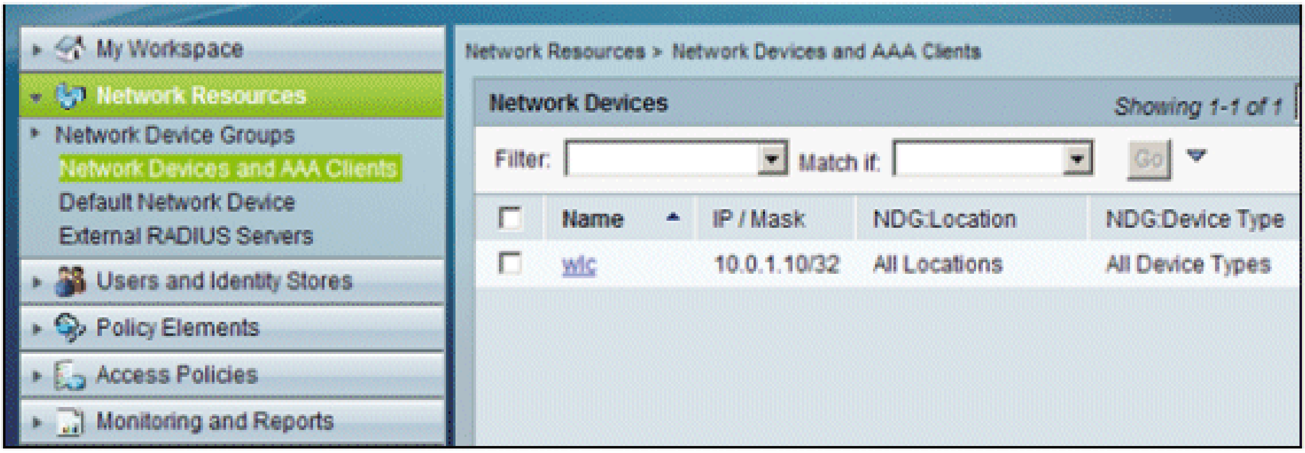
Password:

TrustSec Advanced Settings

= Required fields

cisco

3. 完成后，单击 **Submit**。此时控制器将显示为 ACS Network Devices 列表中的条目。



Network Resources > Network Devices and AAA Clients

Network Devices Showing 1-1 of 1

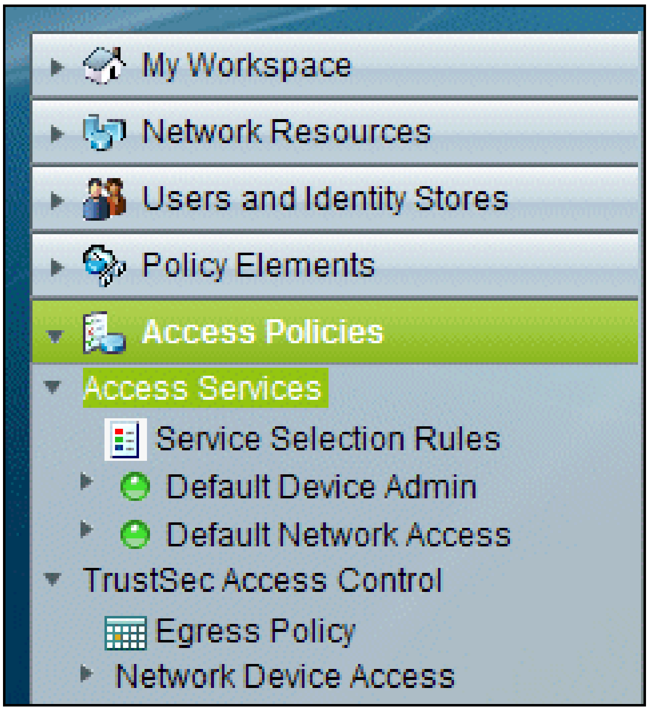
Filter: Match if: Go

□	Name	IP / Mask	NDG:Location	NDG:Device Type
□	wlc	10.0.1.10/32	All Locations	All Device Types

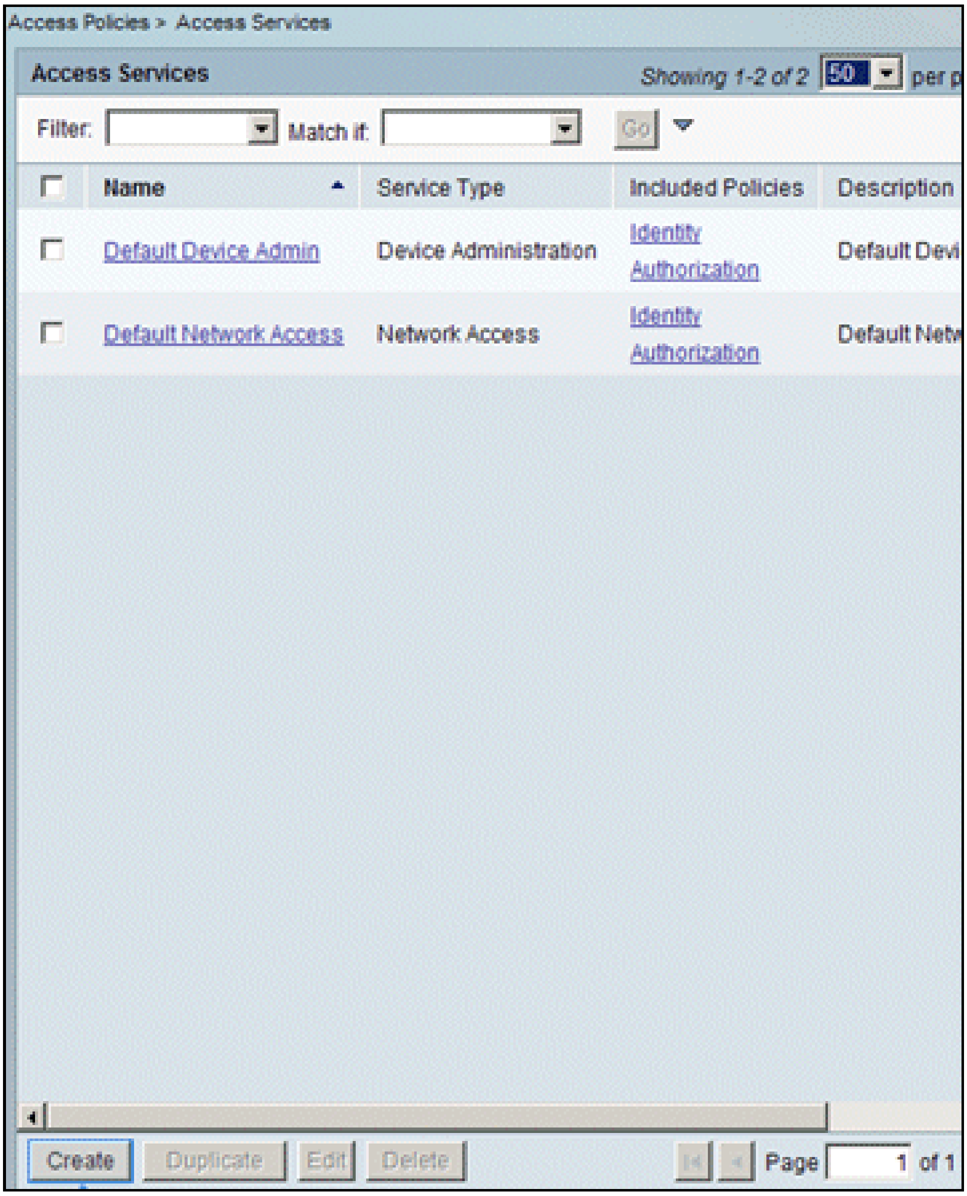
配置无线 ACS 访问策略

请执行以下步骤：

1. 在 ACS 中，转至 **Access Policies > Access Services**。

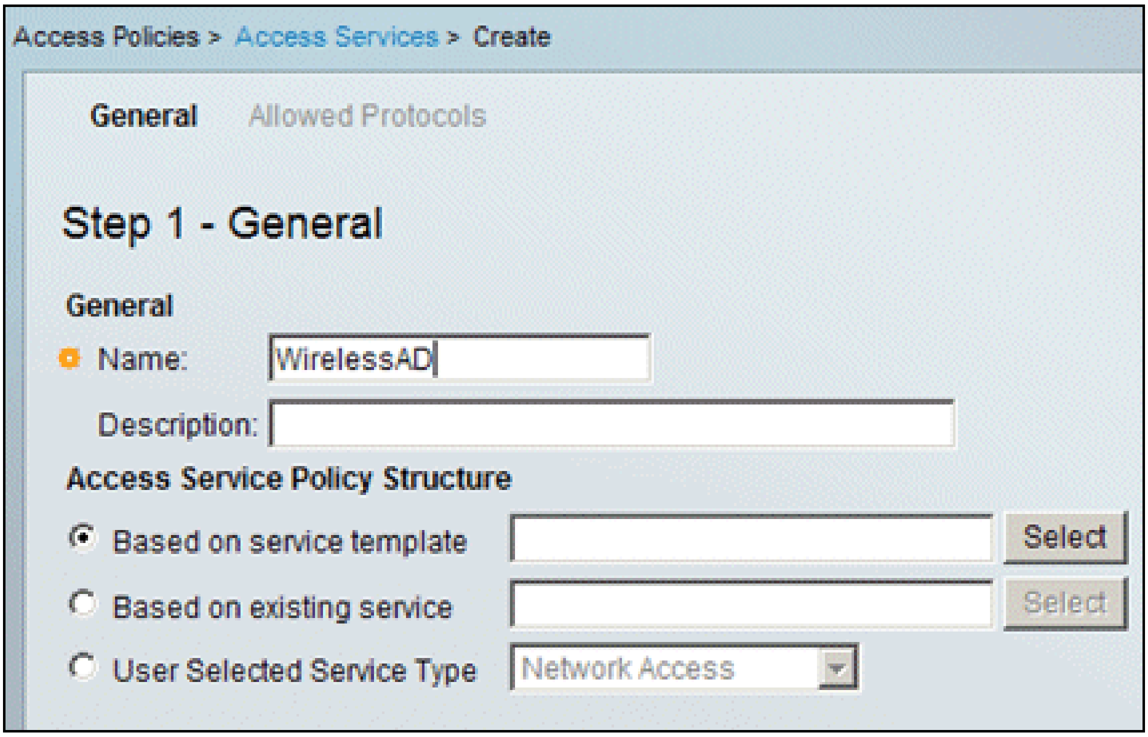


2. 在 Access Services 窗口中，单击 **Create**。



☐	Name	Service Type	Included Policies	Description
☐	Default Device Admin	Device Administration	Identity Authorization	Default Devi
☐	Default Network Access	Network Access	Identity Authorization	Default Netw

3. 创建访问服务并输入名称（如 WirelessAD）。选择 **Based on service template**，然后单击



Access Policies > Access Services > Create

General | Allowed Protocols

Step 1 - General

General

Name: WirelessAD

Description:

Access Service Policy Structure

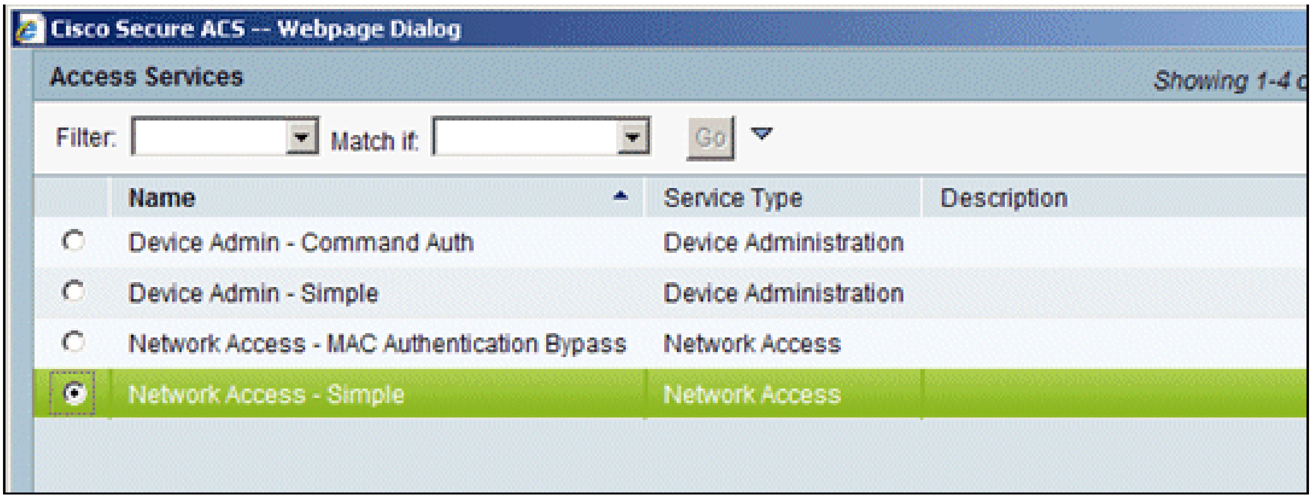
● Based on service template [ ] Select

○ Based on existing service [ ] Select

○ User Selected Service Type: Network Access

Select。

4. 在 Webpage 对话框中，选择 **Network Access – Simple**。Click **OK**.



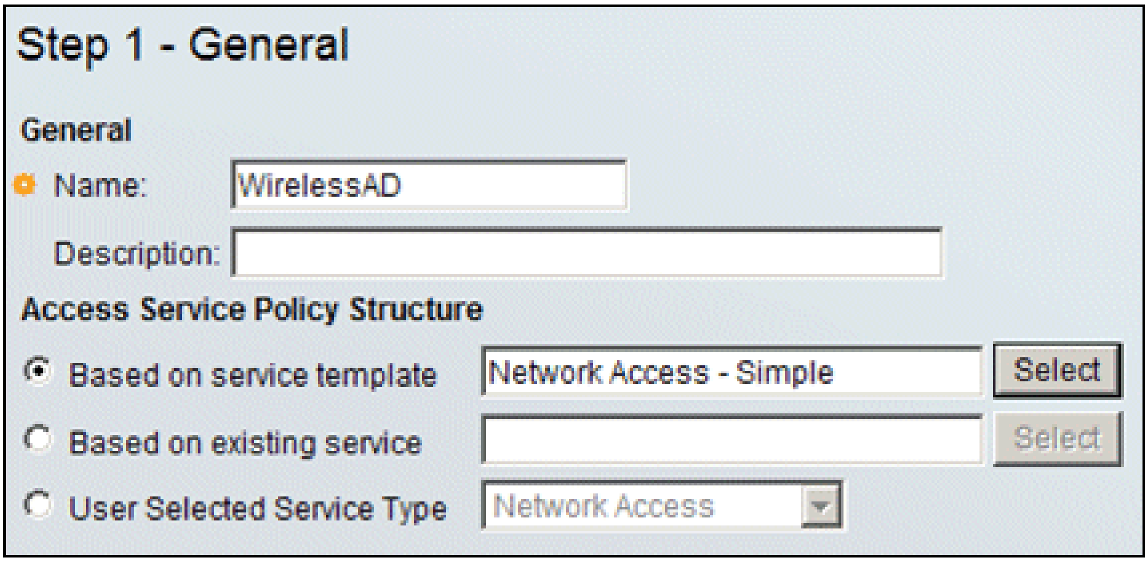
Cisco Secure ACS -- Webpage Dialog

Access Services — Showing 1-4 o

Filter: [ ] Match if: [ ] Go

	Name	Service Type	Description
○	Device Admin - Command Auth	Device Administration	
○	Device Admin - Simple	Device Administration	
○	Network Access - MAC Authentication Bypass	Network Access	
●	Network Access - Simple	Network Access	

5. 在 Webpage 对话框中，选择 **Network Access – Simple**。Click **OK.**选择模板后，单击 **Next**。



Step 1 - General

General

Name: WirelessAD

Description:

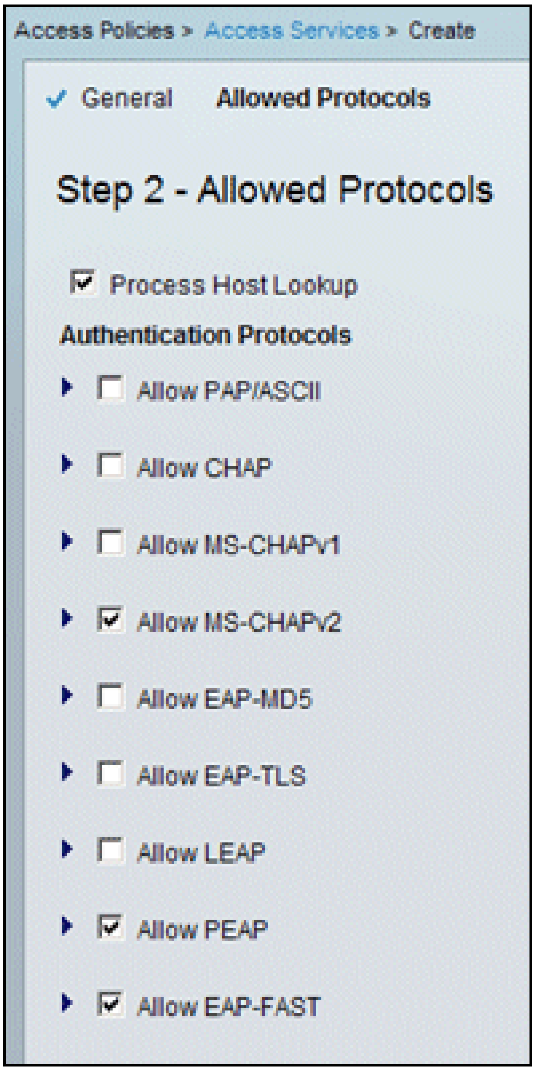
Access Service Policy Structure

● Based on service template: Network Access - Simple — Select

○ Based on existing service [ ] Select

○ User Selected Service Type: Network Access

6. 在 Allowed Protocols 下，选中 **Allow MS-CHAPv2 和 Allow PEAP** 复选框。单击 **完成**。



Access Policies > Access Services > Create

✓ General   Allowed Protocols

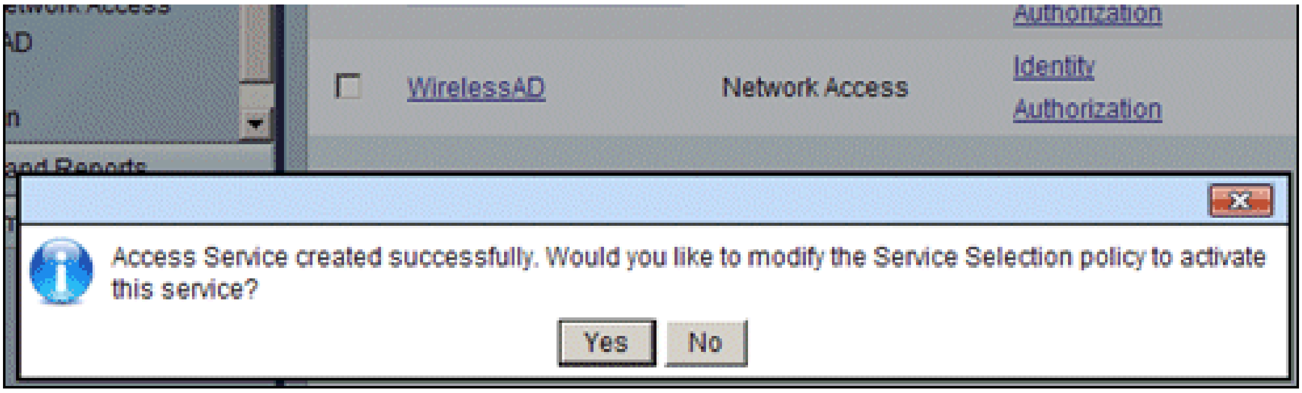
Step 2 - Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

- □ Allow PAP/ASCII
- □ Allow CHAP
- □ Allow MS-CHAPv1
- ☑ Allow MS-CHAPv2
- □ Allow EAP-MD5
- □ Allow EAP-TLS
- □ Allow LEAP
- ☑ Allow PEAP
- ☑ Allow EAP-FAST

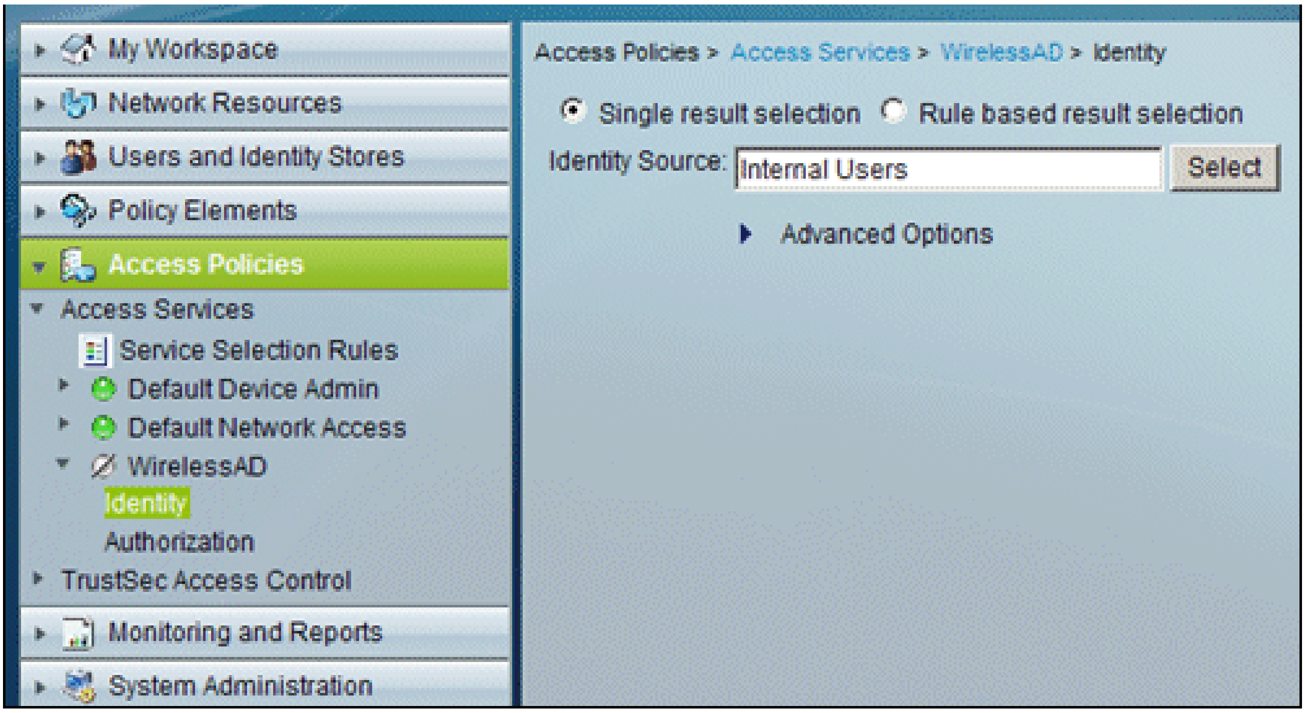
7. ACS 提示您激活新服务时，请单击 **Yes**。



□ WirelessAD   Network Access   Identity
Authorization

Access Service created successfully. Would you like to modify the Service Selection policy to activate this service?

8. 在刚刚创建/激活的新访问服务中，展开并选择 **Identity**。对于 Identity Source，请单击 **Select**。

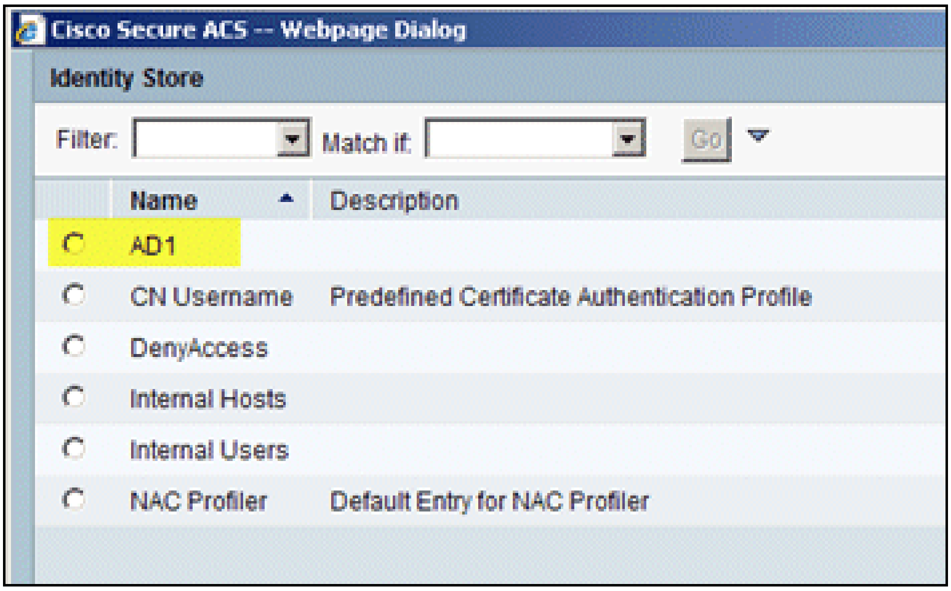


Access Policies > Access Services > WirelessAD > Identity

● Single result selection ○ Rule based result selection

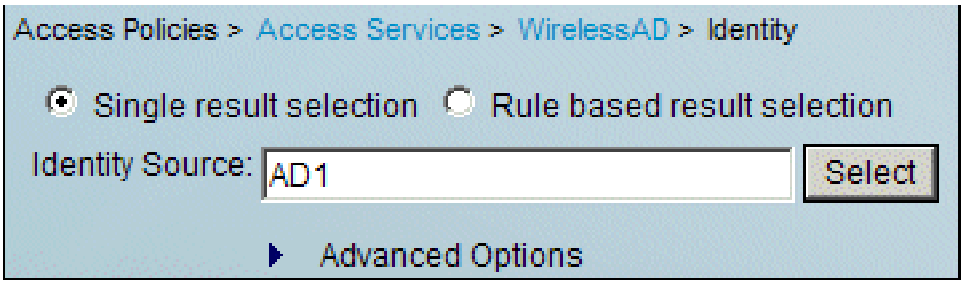
Identity Source: Internal Users

9. 为在 ACS 中配置的 Active Directory 选择 **AD1，然后单击 OK。**



	Name	Description
○	AD1	
○	CN Username	Predefined Certificate Authentication Profile
○	DenyAccess	
○	Internal Hosts	
○	Internal Users	
○	NAC Profiler	Default Entry for NAC Profiler

10. 确认 Identity Source 为 AD1，然后单击 **Save Changes**。



Access Policies > Access Services > WirelessAD > Identity

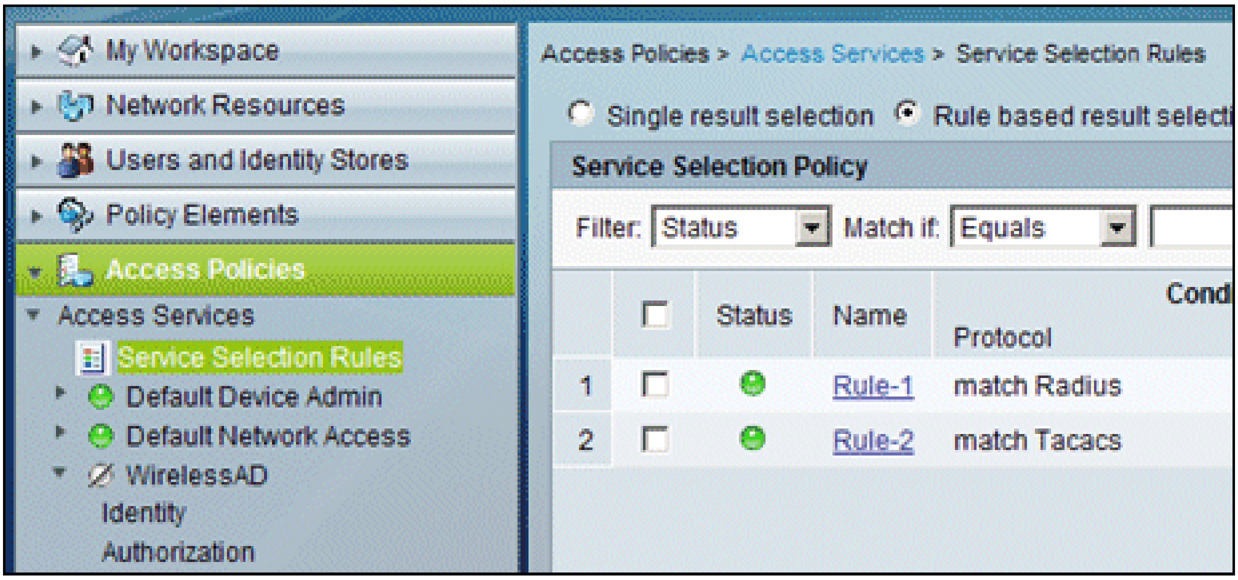
● Single result selection ○ Rule based result selection

Identity Source: AD1

创建 ACS 访问策略和服务规则

请执行以下步骤：

1. 转至 **Access Policies > Service Selection Rules**。



Access Policies > Access Services > Service Selection Rules

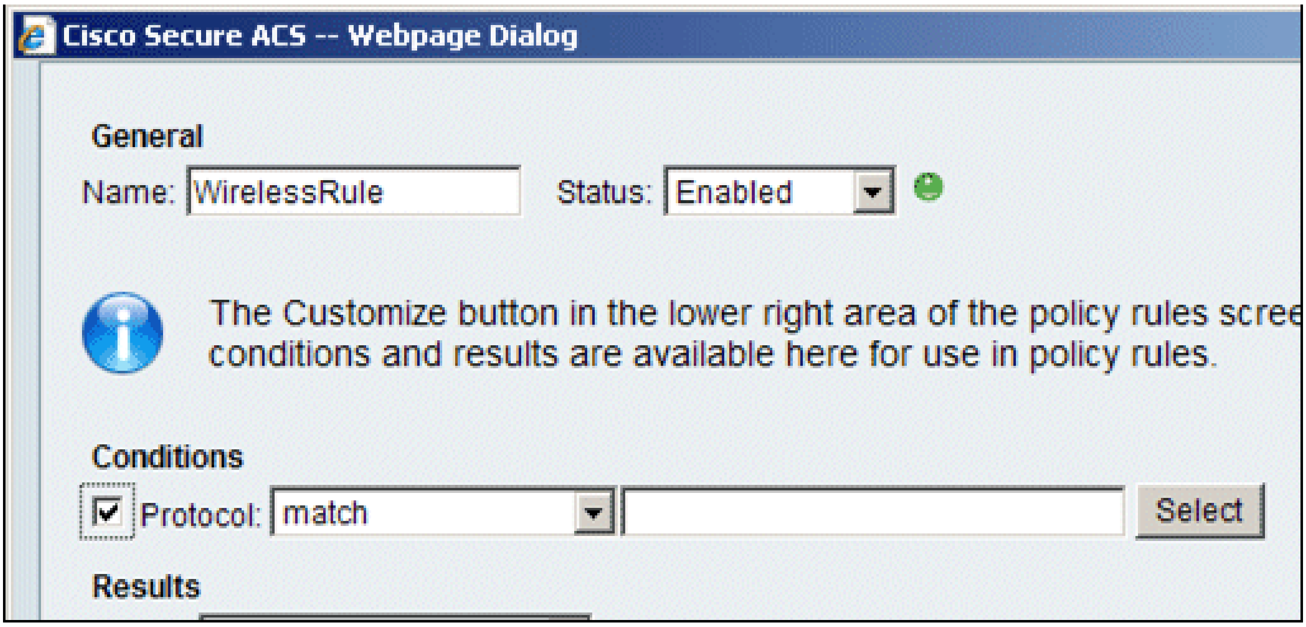
○ Single result selection ● Rule based result selecti

Service Selection Policy

Filter: Status Match if: Equals

	□	Status	Name	Cond Protocol
1	□	●	Rule-1	match Radius
2	□	●	Rule-2	match Tacacs

2. 在 Service Selection Policy 窗口中单击 **Create。**输入新规则名称（如 *WirelessRule*）。选中 **Protocol 复选框以匹配 Radius。**



General

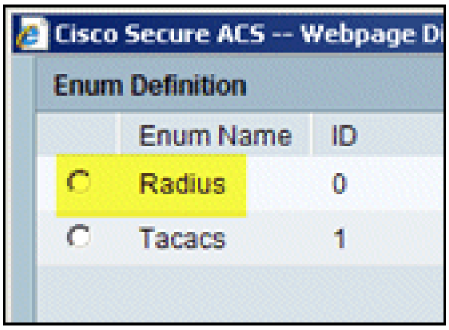
Name: WirelessRule Status: Enabled ●

The Customize button in the lower right area of the policy rules scree conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match

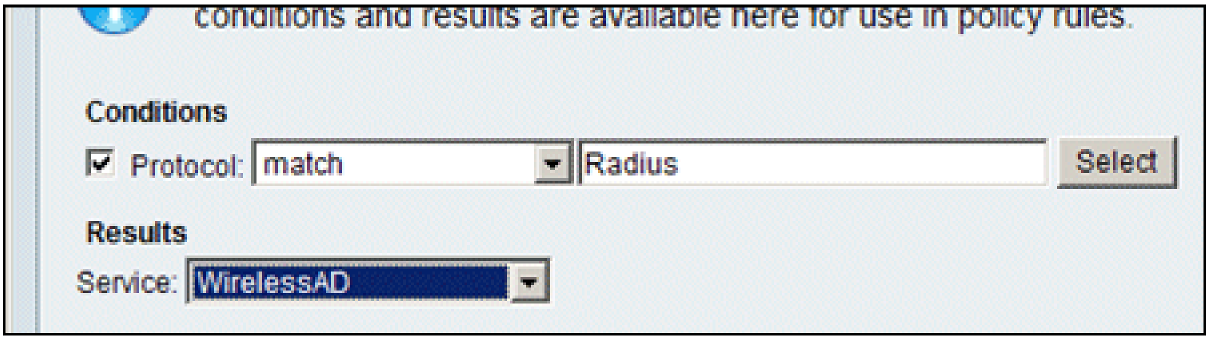
Results



Enum Definition

	Enum Name	ID
○	Radius	0
○	Tacacs	1

3. 选择 **Radius**，然后单击 **OK**。
4. 在 Results 下，针对 Service 选择 **WirelessAD（已在上一步创建）。**



conditions and results are available here for use in policy rules.

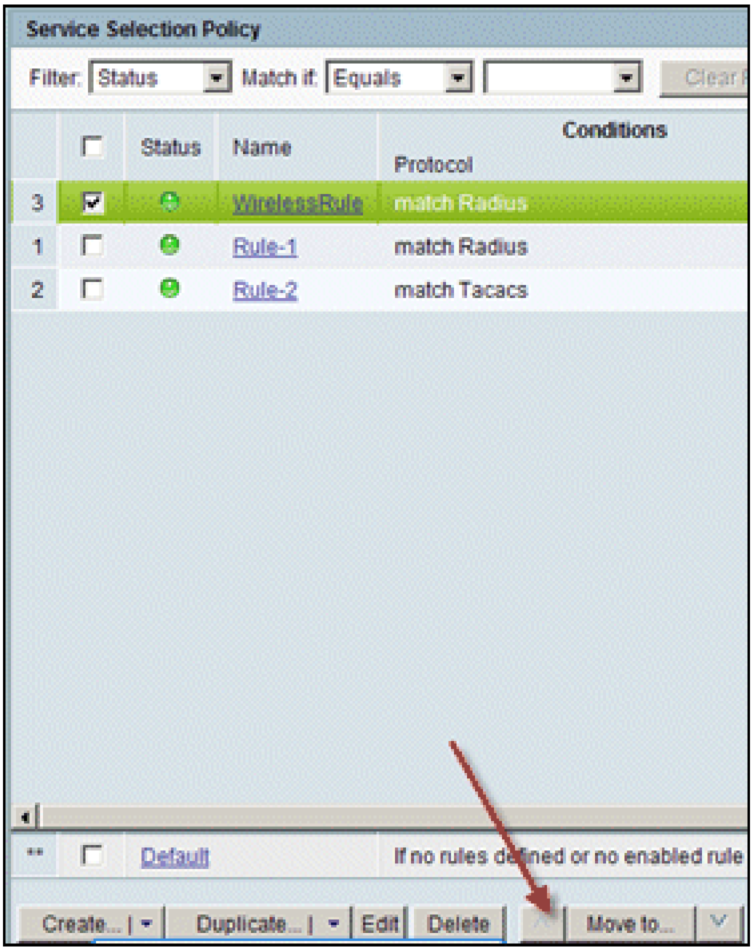
Conditions

☑ Protocol: match Radius Select

Results

Service: WirelessAD

5. 创建新的无线规则后，请选择此规则并将其**移动到顶部，该规则将成为第一个使用 Active Directory 来确定无线 RADIUS 身份验证的规则。**



Service Selection Policy

Filter: Status Match if: Equals Clear F

	□	Status	Name	Conditions Protocol
3	☑	●	WirelessRule	match Radius
1	□	●	Rule-1	match Radius
2	□	●	Rule-2	match Tacacs
**	□		Default	If no rules defined or no enabled rule

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

请执行以下步骤：

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 demo.local 域中名为 CLIENT 的成员计算机。
3. 安装 Windows XP Professional SP2。必须安装此操作系统才能获得 PEAP 支持。**注意**

：Windows XP Professional SP2中会自动打开Windows防火墙。请勿关闭防火墙。

安装无线网络适配器

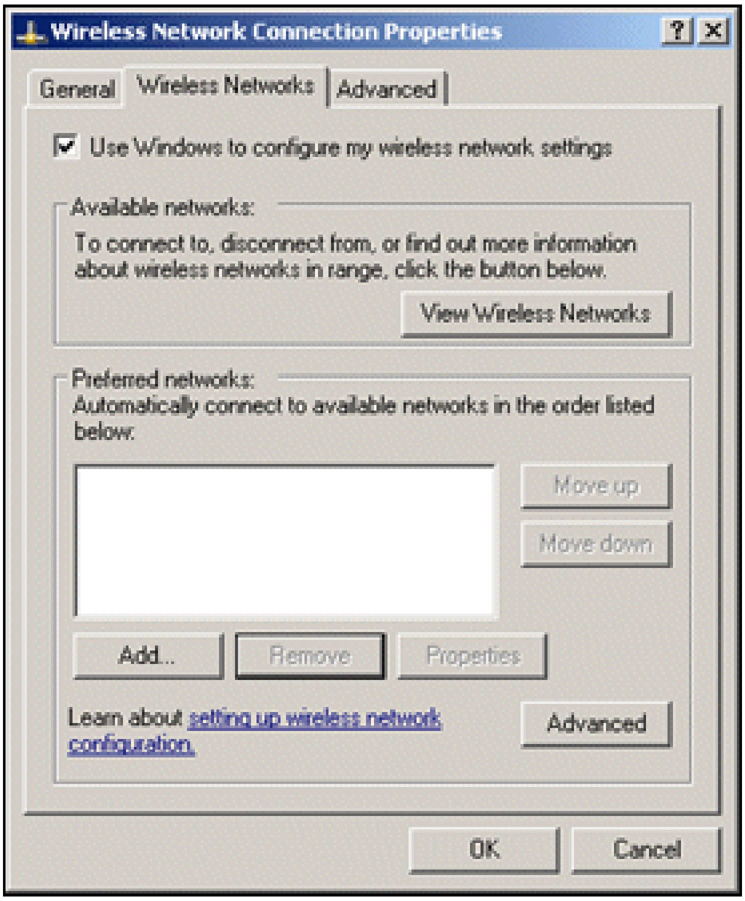
请执行以下步骤：

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。**注：**请勿安装无线适配器的制造商配置软件。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

请执行以下步骤：

1. 注销，然后使用 **demo.local domain 中的 WirelessUser 帐户登录。**
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。**



Wireless Network Connection Properties

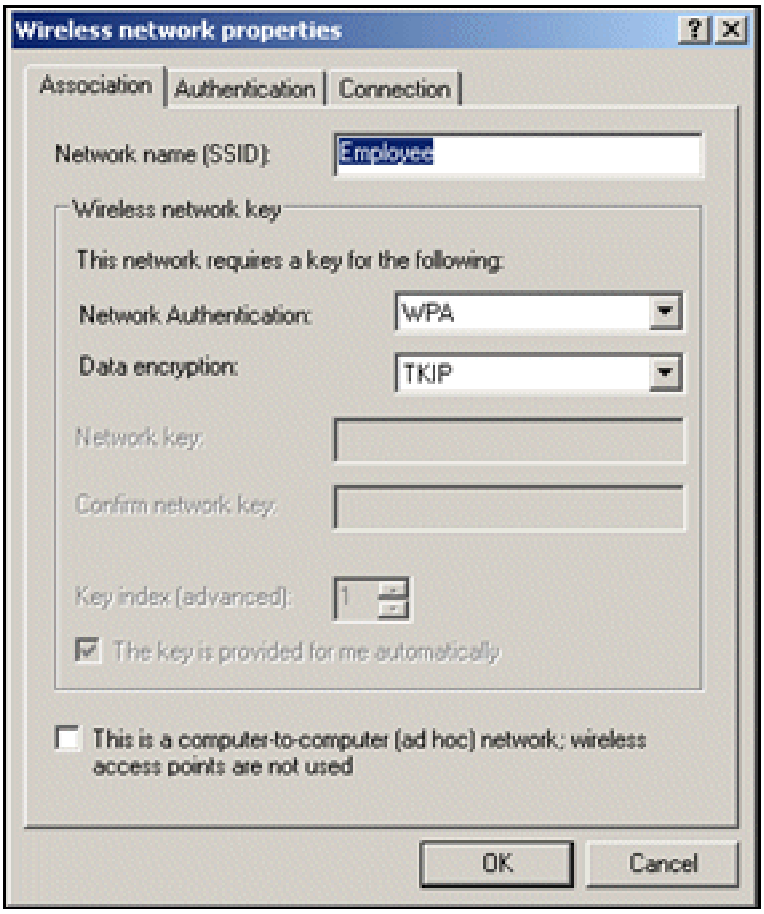
☑ Use Windows to configure my wireless network settings

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

Preferred networks:
Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

4. 单击 **Add。**
5. 在“关联”选项卡的“网络名称 (SSID)”字段中输入 *Employee。*
6. 针对“网络身份验证”选择 **WPA，并确保将“数据加密”设置为 TKIP。**



Network name (SSID): Employee

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

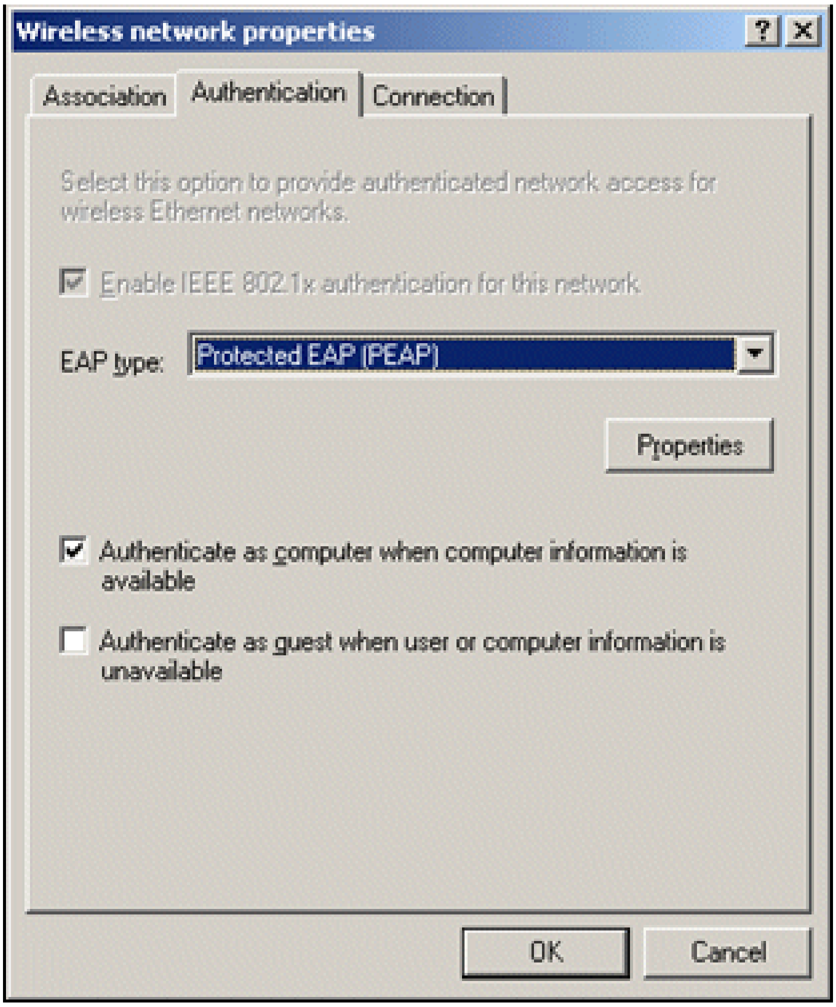
Confirm network key:

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. 单击 **Authentication 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。**



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

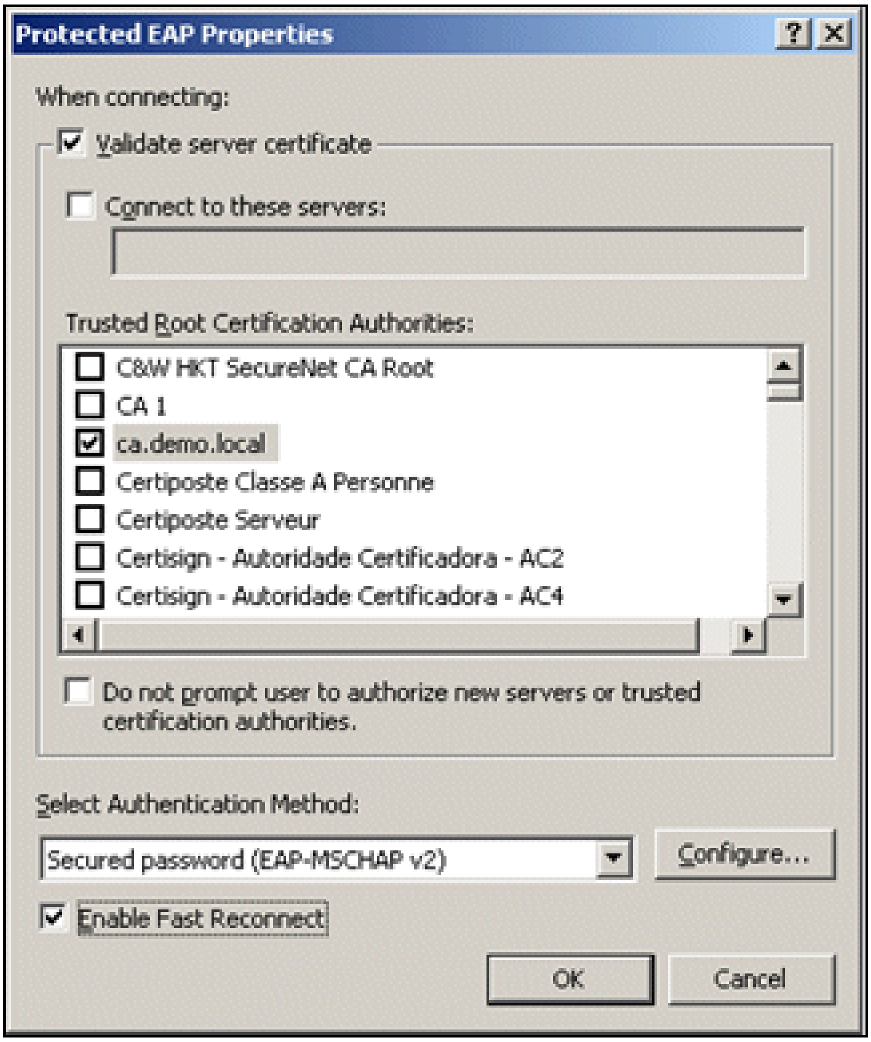
☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

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。**



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ C&W HKT SecureNet CA Root
□ CA 1
☑ ca.demo.local
□ Certiposte Classe A Personne
□ Certiposte Serveur
□ Certisign - Autoridade Certificadora - AC2
□ Certisign - Autoridade Certificadora - AC4

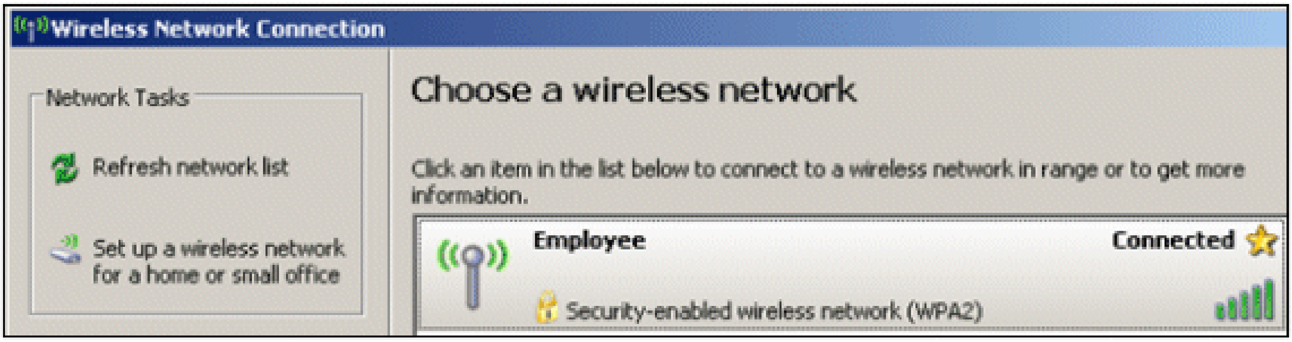
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

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，然后单击**连接**。如果连接成功，无线客户端将显示**已连接。**



Wireless Network Connection

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

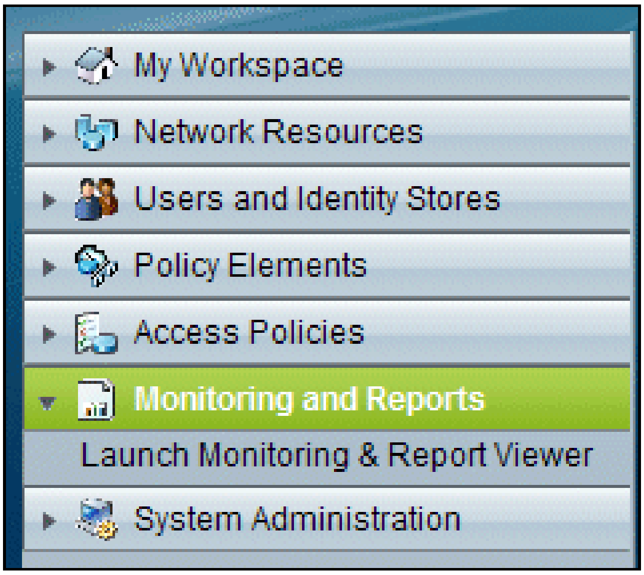
Security-enabled wireless network (WPA2)

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 10.0.20.100-10.0.20.200 应该来自 DHCP 范围或为 CorpNet 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://10.0.10.10（或 CA 服务器的 IP 地址）。**

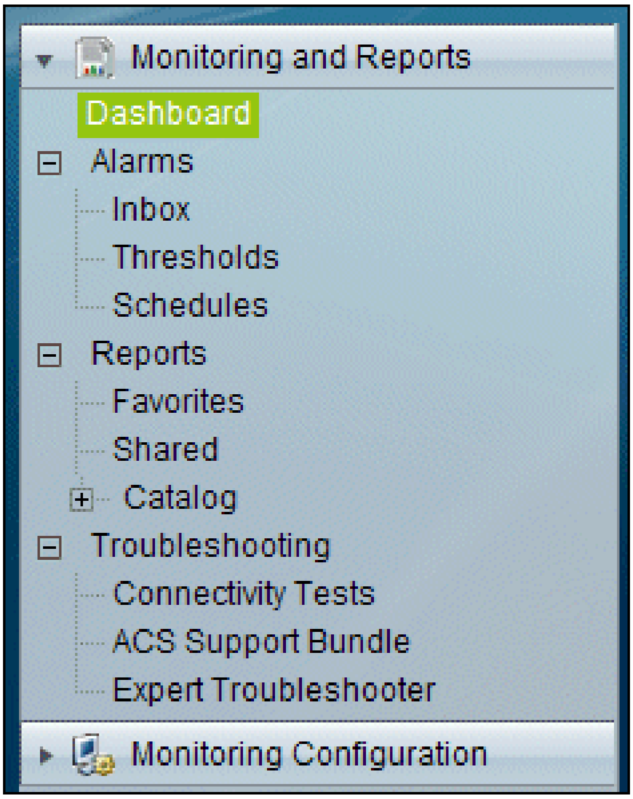
使用 ACS 排除无线身份验证故障

请执行以下步骤：

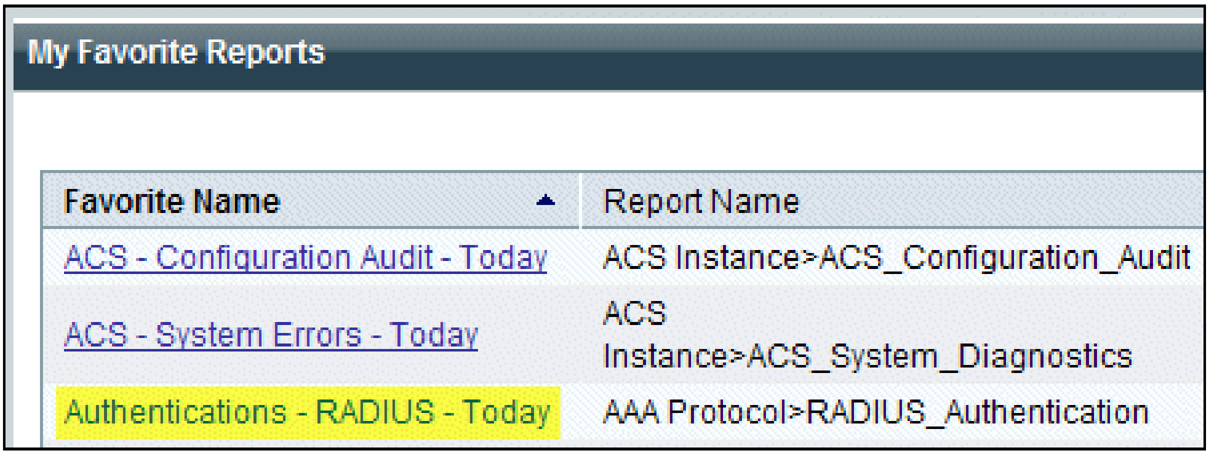
1. 转至 **ACS > Monitoring and Reports**，然后单击 **Launch Monitoring & Report Viewer**。



2. 此时将打开一个单独的 ACS 窗口。单击 **Dashboard**。



3. 在 My Favorite Reports 部分，单击 **Authentications – RADIUS – Today**。

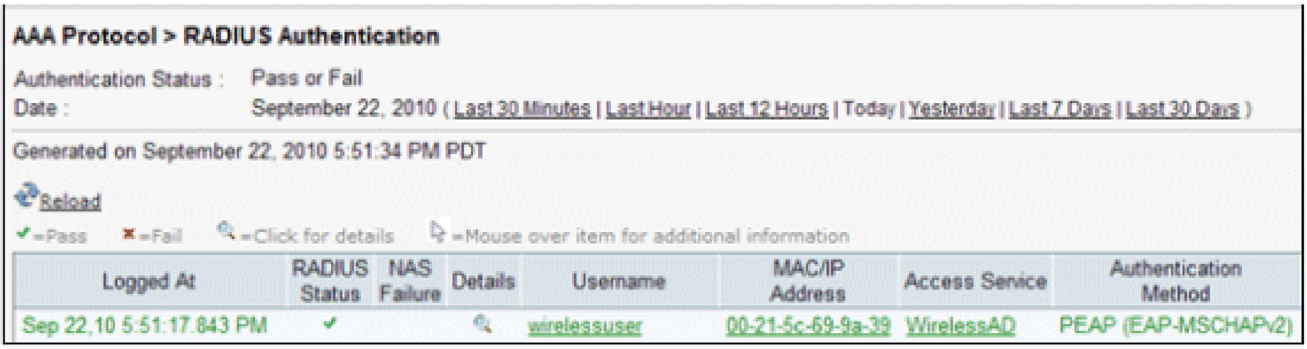


My Favorite Reports

Favorite Name	Report Name
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication

4. 此时将显示一个日志，其中包括所有通过 (Pass) 或失败 (Fail) 的 RADIUS 身份验证。在已记

录的条目中，单击 Details 列中的**放大镜图标。**



AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : September 22, 2010 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

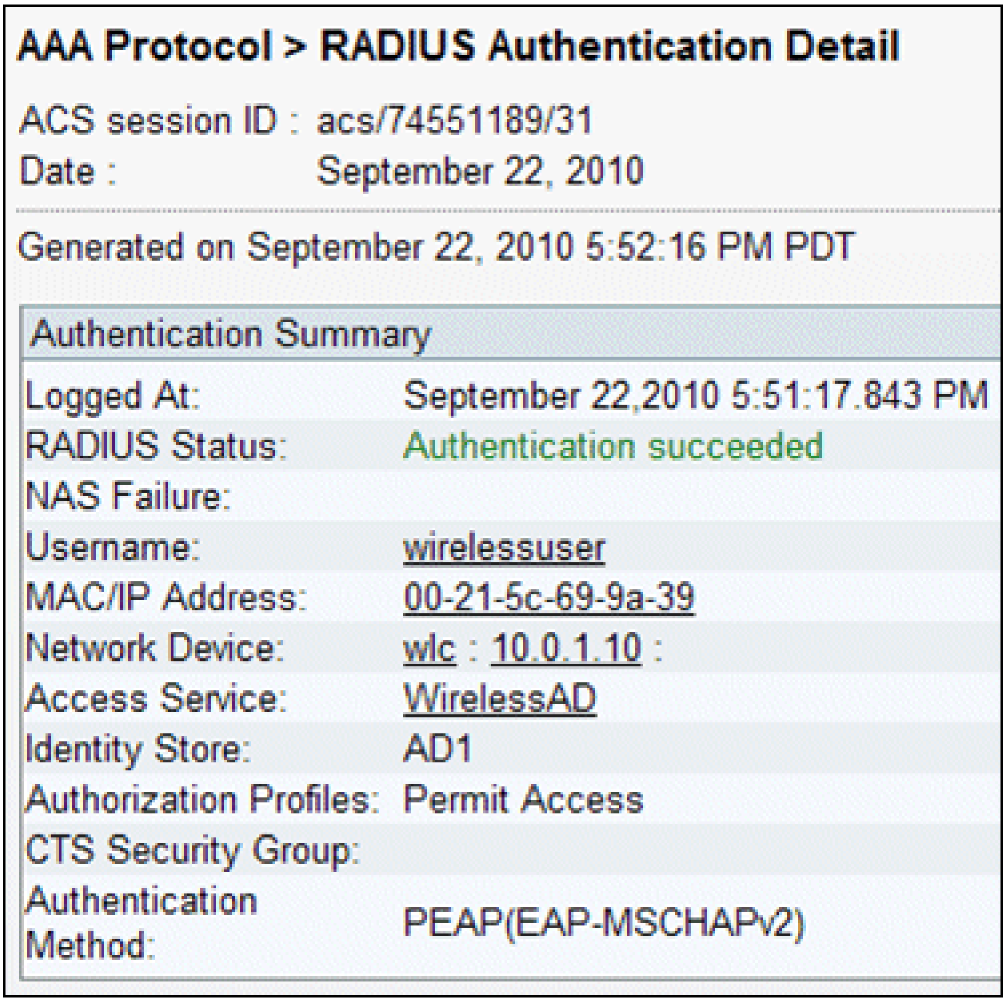
Generated on September 22, 2010 5:51:34 PM PDT

Reload

✓=Pass ✖=Fail 🔍=Click for details ↖=Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method
Sep 22,10 5:51:17.843 PM	✓		🔍	wirelessuser	00-21-5c-69-9a-39	WirelessAD	PEAP (EAP-MSCHAPv2)

5. RADIUS 身份验证详细信息将提供已记录尝试的更多信息。



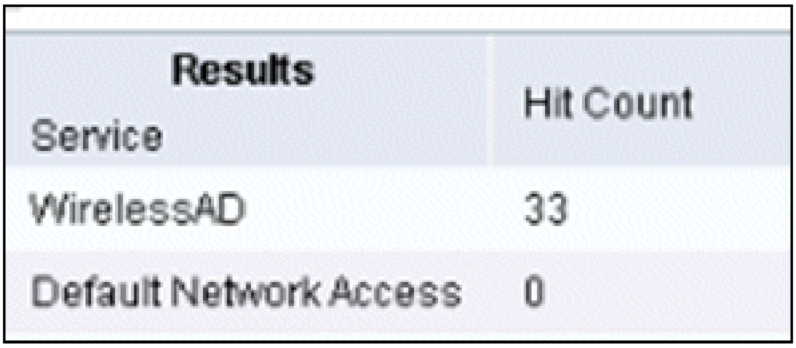
AAA Protocol > RADIUS Authentication Detail

ACS session ID : acs/74551189/31
Date : September 22, 2010

Generated on September 22, 2010 5:52:16 PM PDT

Authentication Summary	
Logged At:	September 22,2010 5:51:17.843 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	wirelessuser
MAC/IP Address:	00-21-5c-69-9a-39
Network Device:	wlc : 10.0.1.10 :
Access Service:	WirelessAD
Identity Store:	AD1
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

6. ACS Service Hit Count可提供与ACS中创建的规则匹配的尝试的概述。转至 **ACS > Access Policies > Access Services**，然后单击 **Service Selection Rules**。



Results Service	Hit Count
WirelessAD	33
Default Network Access	0

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` **Failed attempts option 中找到** `NAS duplicated authentication attempt`

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使用的方法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。

有关修补程序，请与 Microsoft 联系，并请参阅文章连接第三方 RADIUS 服务器时 PEAP 身份验证不成功 。问题的根源在客户端上：默认情况下，Windows 实用程序 中为 PEAP 禁用了快速重新连接选项。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，请取消选中 ACS 服务器上的 Fast Reconnect 选项（位于 Global System Options 下）。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”，请执行以下步骤：

1. 转至**“开始”>“设置”>“控制面板”**。
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 来配置我的无线网络设置选项，以便通过 Windows 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**。否则，请单击**新建以添加新的 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**为此网络启用 IEEE 802.1X 身份验证选项。**
10. 选择 **PEAP 作为“EAP 类型”，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

- ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAP
- 用于 Web 身份验证的 Cisco 无线 LAN 控制器 (WLC) 和 Cisco ACS 5.x (TACACS+) 配置示例
- Cisco 安全访问控制系统 5.1 安装和升级指南
- 技术支持和文档 - Cisco Systems

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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