

EAP–TLS under Unified Wireless Network with ACS 4.0 and Windows 2003

Document ID: 71929

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP (DC_CA)

DC_CA (wirelessdemoca)

Windows Standard 2003 Setup with Cisco Secure ACS 4.0

- Basic Installation and Configuration
- Cisco Secure ACS 4.0 Installation

Cisco LWAPP Controller Configuration

- Create the Necessary Configuration for WPA2/WPA

EAP–TLS Authentication

- Install the Certificate Templates Snap–in
- Create the Certificate Template for the ACS Web Server
- Enable the New ACS Web Server Certificate Template

ACS 4.0 Certificate Setup

- Configure Exportable Certificate for ACS
- Install the Certificate in ACS 4.0 Software

CLIENT Configuration for EAP–TLS using Windows Zero Touch

- Perform a Basic Installation and Configuration
- Configure the Wireless Network Connection

Related Information

Introduction

This document describes how to configure secure wireless access using Wireless LAN Controllers (WLCs), Microsoft Windows 2003 software and Cisco Secure Access Control Server (ACS) 4.0 via Extensible Authentication Protocol–Transport Layer Security (EAP–TLS).

Note: For more information about the deployment of secure wireless, refer to the Microsoft Wi–Fi web site and Cisco SAFE Wireless Blueprint.

Prerequisites

Requirements

There is an assumption that the installer has knowledge of basic Windows 2003 installation and Cisco controller installation as this document only covers the specific configurations to facilitate the tests.

For initial installation and configuration information for the Cisco 4400 Series Controllers, refer to the Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers. For initial installation and configuration information for the Cisco 2000 Series Controllers, refer to the Quick Start Guide: Cisco 2000 Series Wireless LAN Controllers.

Before you begin, install the Windows Server 2003 with Service Pack (SP)1 operating system on each of the servers in the test lab and update all Service Packs. Install the controllers and APs and ensure that the latest software updates are configured.

Important: At the time this document was written, SP1 is the latest Windows Server 2003 update, and SP2 with update patches is the latest software for Windows XP Professional.

Windows Server 2003 with SP1, Enterprise Edition, is used so that auto-enrollment of user and workstation certificates for EAP-TLS authentication can be configured. This is described in the EAP-TLS Authentication section of this document. Certificate auto-enrollment and auto-renewal make it easier to deploy certificates and improve security by automatically expiring and renewing certificates.

Components Used

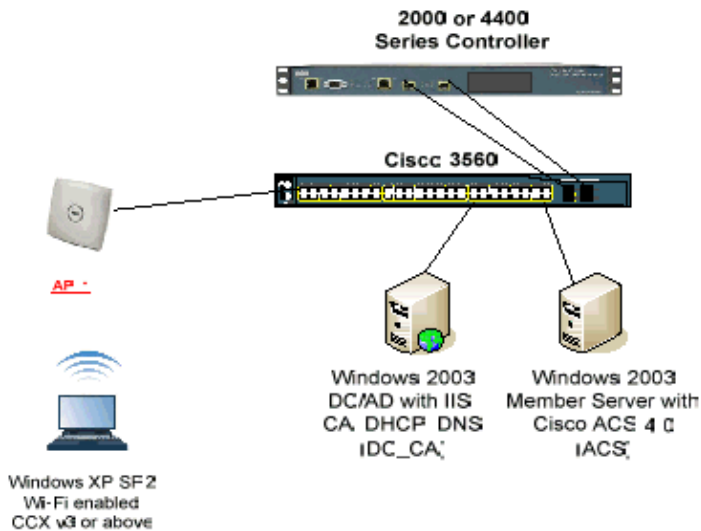
The information in this document is based on these software and hardware versions:

- Cisco 2006 or 4400 Series Controller that runs 3.2.116.21
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise with Internet Information Server (IIS), Certificate Authority (CA), DHCP, and Domain Name System (DNS) installed
- Windows 2003 Standard with Access Control Server (ACS) 4.0
- Windows XP Professional with SP (and updated Service Packs) and wireless network interface card (NIC) (with CCX v3 support) or third party supplicant.
- Cisco 3560 Switch

Network Diagram

This document uses this network setup:

Cisco Secure Wireless Lab Topology



The primary purpose of this document is to provide you the step-by-step procedure to implement the EAP-TLS under Unified Wireless Networks with ACS 4.0 and the Windows 2003 Enterprise server. The main emphasis is on auto-enrollment of the client so that the client auto-enrolls and takes the certificate from the server.

Note: In order to add Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) to Windows XP Professional with SP, refer to WPA2/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with SP2 .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP (DC_CA)

DC_CA (wirelessdemoca)

DC_CA is a computer that runs Windows Server 2003 with SP1, Enterprise Edition, and performs these roles:

- A domain controller for the wirelessdemo.local domain that runs IIS
- A DNS server for the wirelessdemo.local DNS domain
- A DHCP server
- Enterprise root CA for the wirelessdemo.local domain

Complete these steps in order to configure DC_CA for these services:

1. Perform a basic installation and configuration.

2. Configure the computer as a domain controller.
3. Raise the domain functional level.
4. Install and configure DHCP.
5. Install certificate services.
6. Verify Administrator permissions for certificates.
7. Add computers to the domain.
8. Allow wireless access to computers.
9. Add users to the domain.
10. Allow wireless access to users.
11. Add groups to the domain.
12. Add users to the WirelessUsers group.
13. Add client computers to the WirelessUsers group.

Step 1: Perform Basic Installation and Configuration

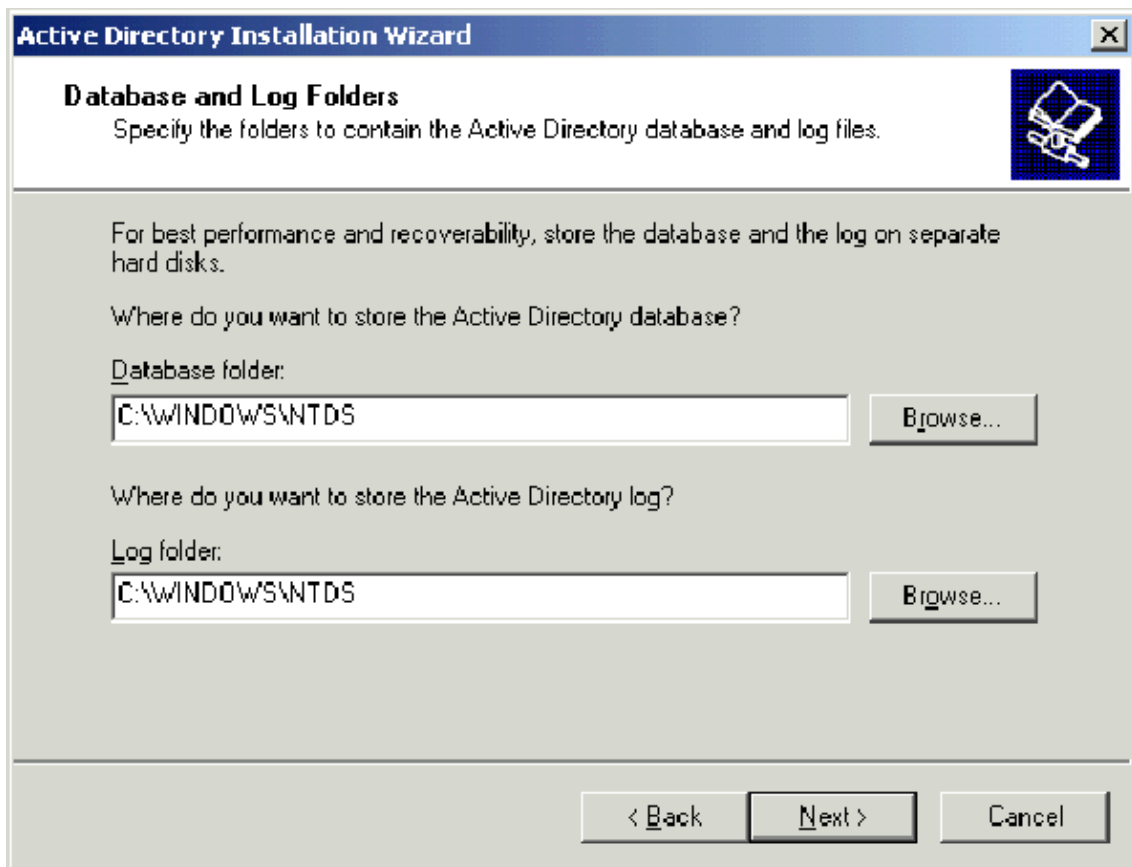
Complete these steps:

1. Install Windows Server 2003 with SP1, Enterprise Edition, as a stand-alone server.
2. Configure the TCP/IP protocol with the IP address of 172.16.100.26 and the subnet mask of 255.255.255.0.

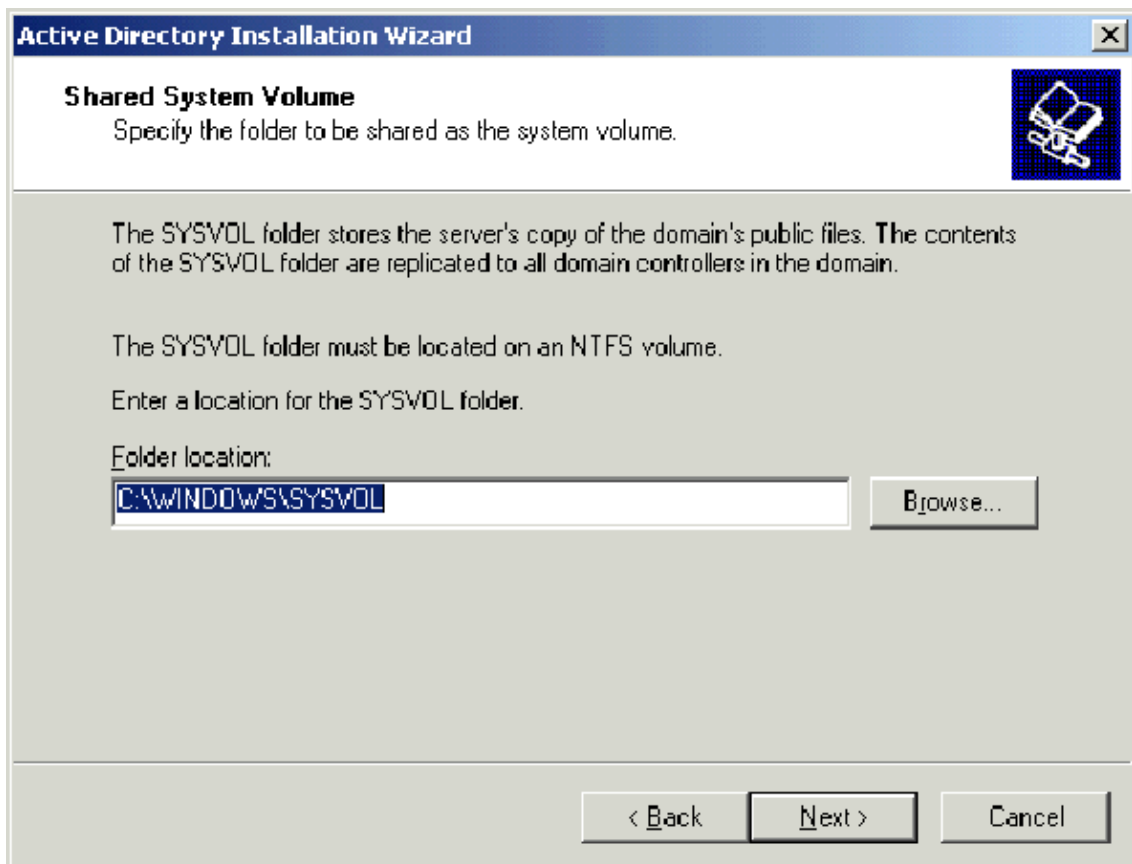
Step 2: Configure the Computer as a Domain Controller

Complete these steps:

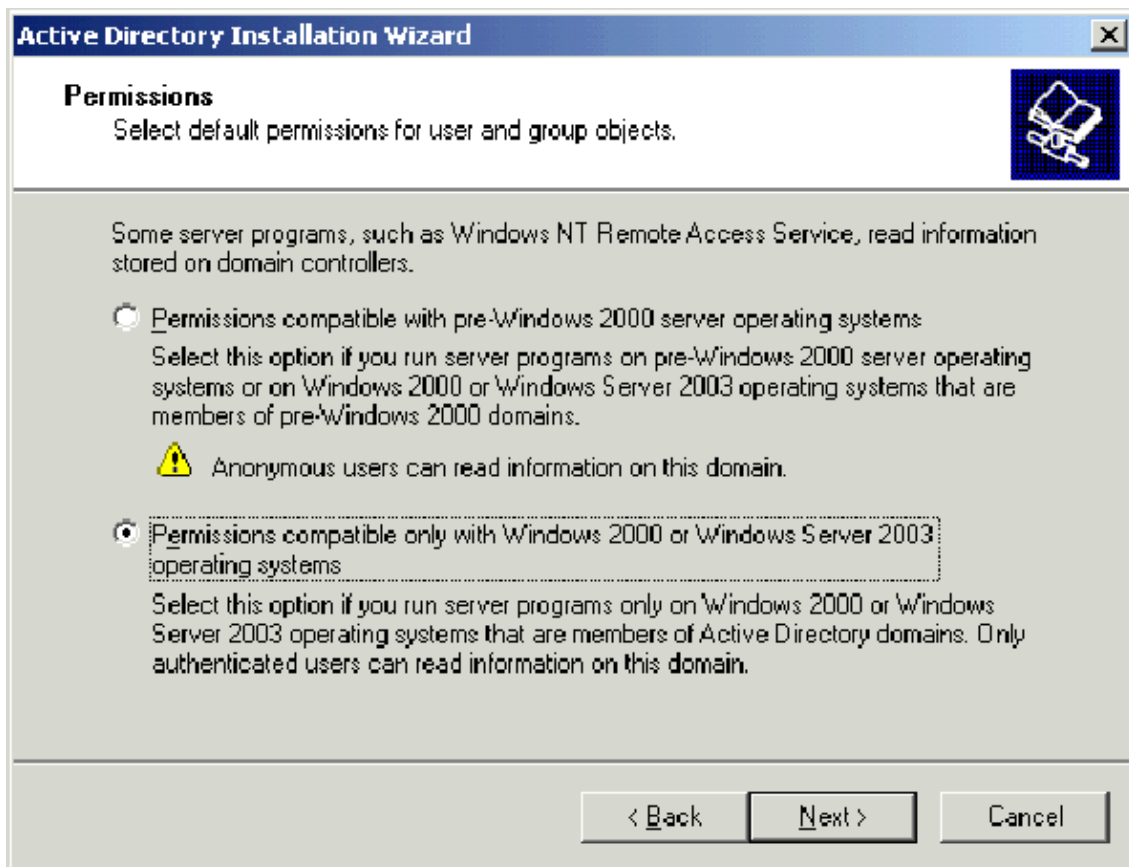
1. In order to start the Active Directory Installation wizard, choose **Start > Run**, type **dcpromo.exe**, and click **OK**.
2. On the Welcome to the Active Directory Installation Wizard page, click **Next**.
3. On the Operating System Compatibility page, click **Next**.
4. On the Domain Controller Type page, select **Domain controller for a new domain** and click **Next**.
5. On the Create New Domain page, select **Domain in a new forest** and click **Next**.
6. On the Install or Configure DNS page, select **No, just install and configure DNS on this computer** and click **Next**.
7. On the New Domain Name page, type **wirelessdemo.local** and click **Next**.
8. On the NetBIOS Domain Name page, enter the Domain NetBIOS name as **wirelessdemo** and click **Next**.
9. On the Database and Log Folders Location page, accept the default Database and Log Folders directories and click **Next**.



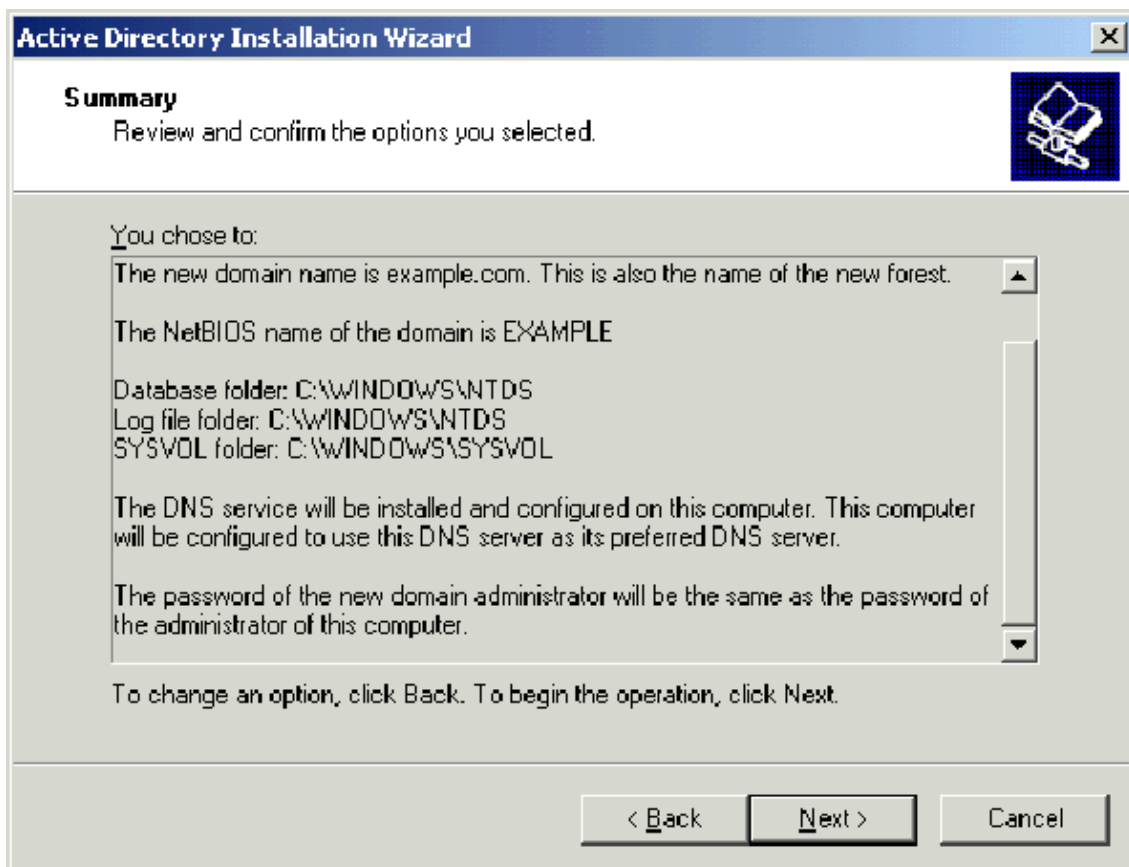
10. On the Shared System Volume dialog box, verify that the default folder location is correct and click **Next**.



11. On the Permissions page, verify that **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** is selected and click **Next**.



12. On the Directory Services Restore Mode Administration Password page, leave the password boxes blank and click **Next**.
13. Review the information on the Summary page and click **Next**.



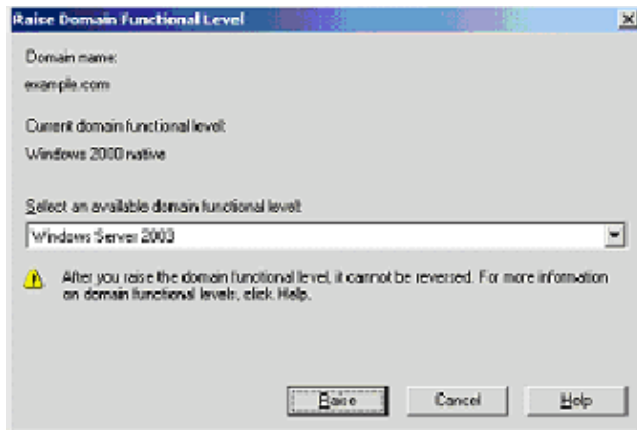
14. On the Completing the Active Directory Installation Wizard page, click **Finish**.

15. When prompted to restart the computer, click **Restart Now**.

Step 3: Raise the Domain Functional Level

Complete these steps:

1. Open the Active Directory Domains and Trusts snap-in from the **Administrative Tools** folder (**Start > Administrative Tools > Active Directory Domains and Trusts**), and then right-click the domain computer **DC_CA.wirelessdemo.local**.
2. Click **Raise Domain Functional Level**, and then select **Windows Server 2003** on the Raise Domain Functional Level page.



3. Click **Raise**, click **OK**, and then click **OK** again.

Step 4: Install and Configure DHCP

Complete these steps:

1. Install Dynamic Host Configuration Protocol (DHCP) as a Networking Service component by using **Add or Remove Programs** in the Control Panel.
2. Open the DHCP snap-in from the Administrative Tools folder (**Start > Programs > Administrative Tools > DHCP**), and then highlight the DHCP server, **DC_CA.wirelessdemo.local**.
3. Click **Action**, and then click **Authorize** in order to authorize the DHCP service.
4. On the console tree, right-click **DC_CA.wirelessdemo.local**, and then click **New Scope**.
5. On the Welcome page of the New Scope wizard, click **Next**.
6. On the Scope Name page, type **CorpNet** in the Name field.
7. Click **Next** and fill in these parameters:

- ◆ Start IP address **172.16.100.1**
- ◆ End IP address **172.16.100.254**
- ◆ Length **24**
- ◆ Subnet mask **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:

End IP address:

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

Length:

Subnet mask:

< Back Next > Cancel

8. Click **Next** and enter **172.16.100.1** for the Start IP address and **172.16.100.100** for the End IP address to be excluded. Then click **Next**. This reserves the IP addresses in the range from 172.16.100.1 to 172.16.100.100. These reserved IP addresses are not allotted by the DHCP server.

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: End IP address: Add

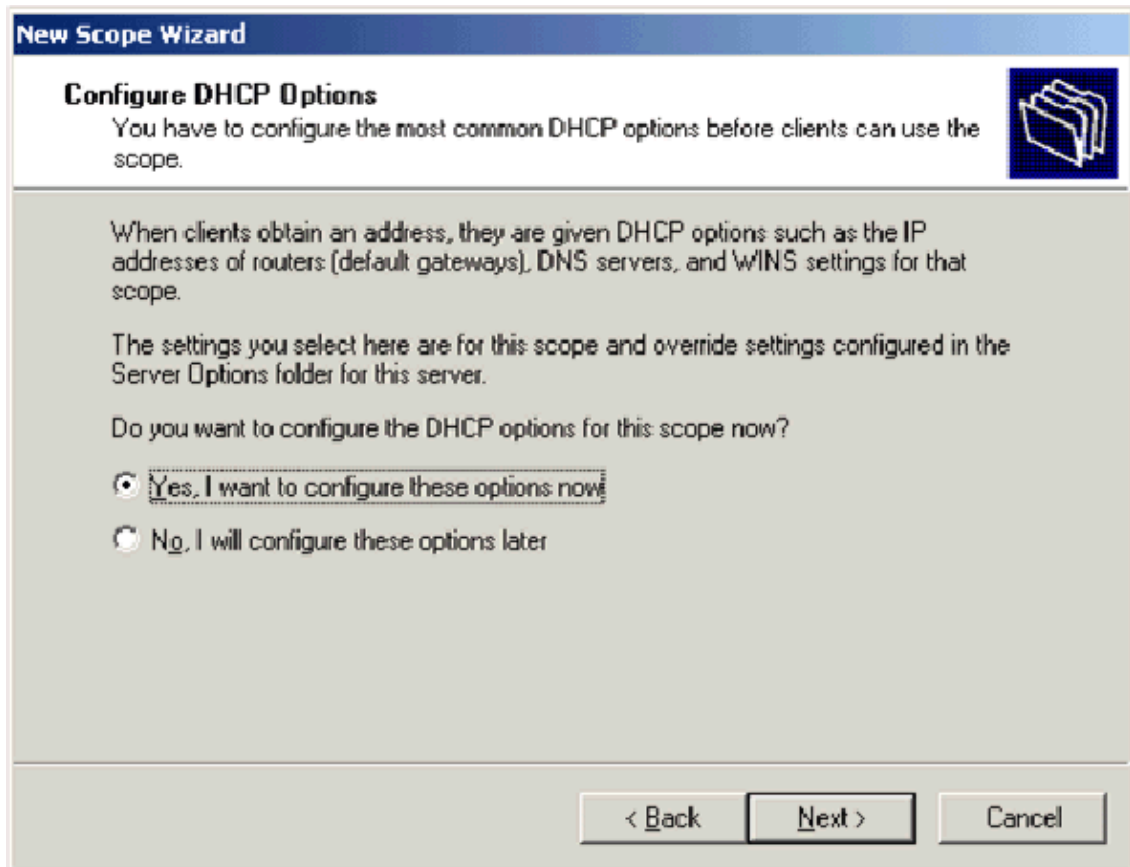
Excluded address range:

Remove

< Back Next > Cancel

9. On the Lease Duration page, click **Next**.

10. On the Configure DHCP Options page, choose **Yes, I want to configure these options now** and click **Next**.



New Scope Wizard

Configure DHCP Options

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

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

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

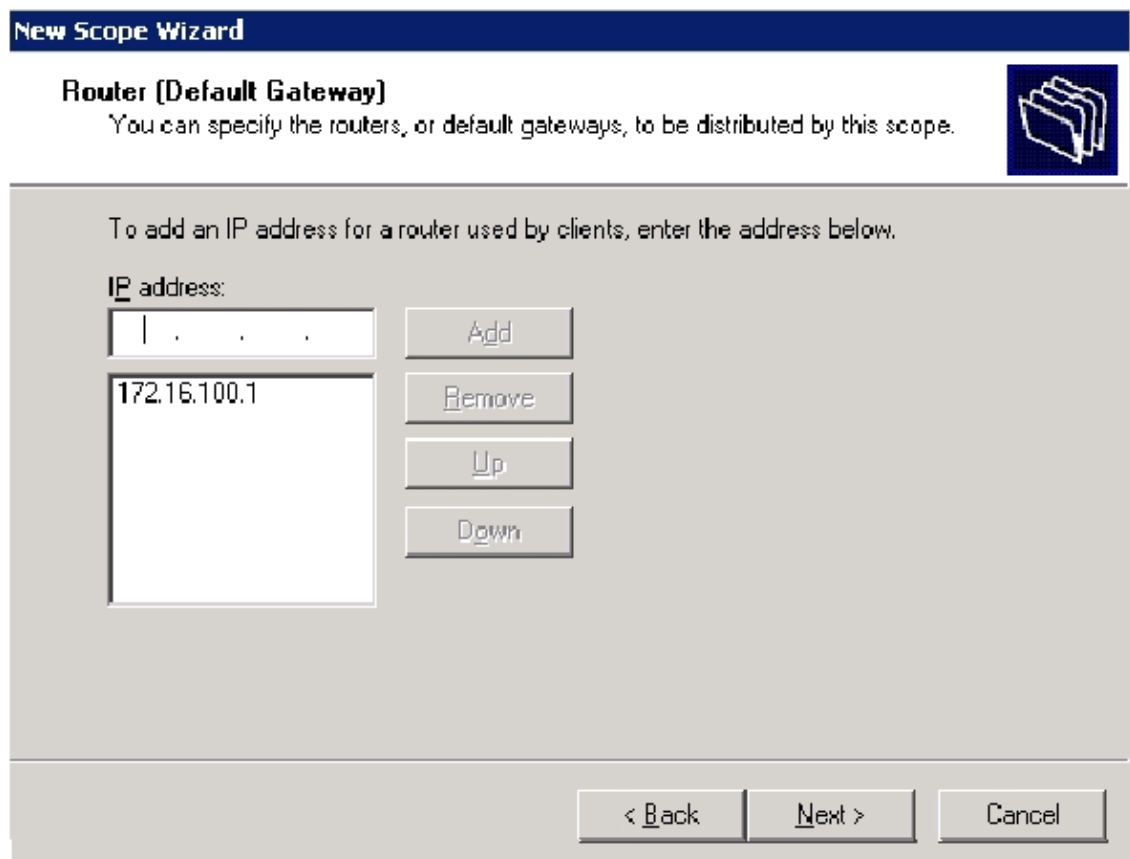
Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now

No, I will configure these options later

< Back Next > Cancel

11. On the Router (Default Gateway) page add the default router address of **172.16.100.1** and click **Next**.



New Scope Wizard

Router (Default Gateway)

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

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

IP address:

Add Remove Up Down

< Back Next > Cancel

12. On the Domain Name and DNS Servers page, type **wirelessdemo.local** in the Parent domain field, type **172.16.100.26** in the IP address field, and then click **Add** and click **Next**.

New Scope Wizard

Domain Name and DNS Servers

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

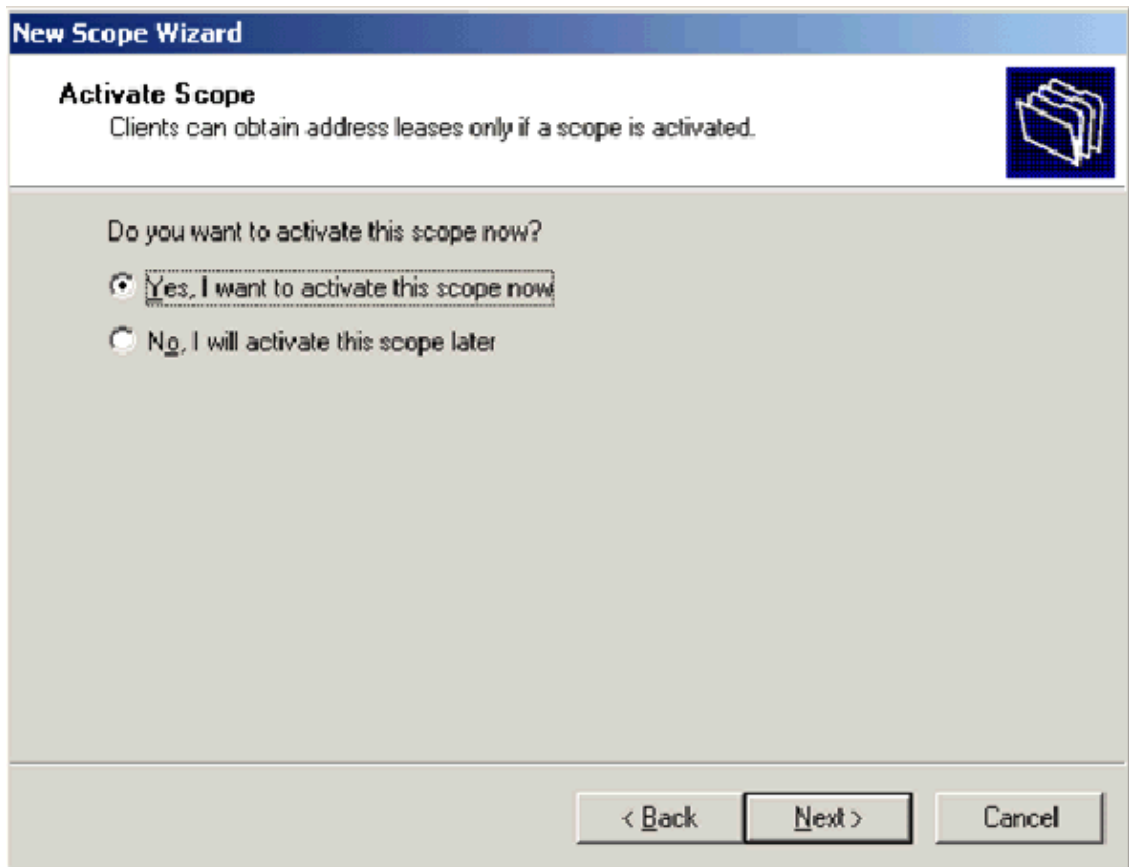
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

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

Server name:	IP address:	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="172.16.100.26"/>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

13. On the WINS Servers page, click **Next**.
14. On the Activate Scope page, choose **Yes, I want to activate this scope now** and click **Next**.



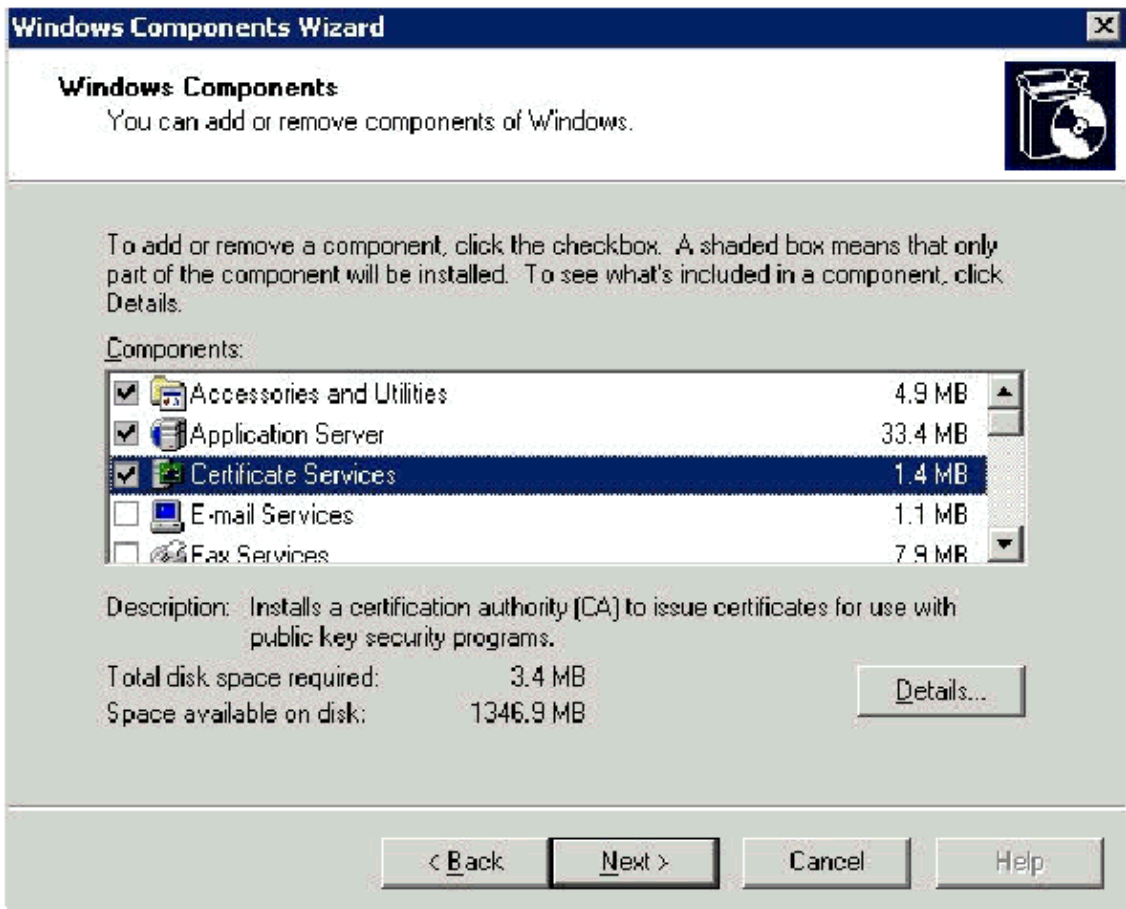
15. On the Completing the New Scope Wizard page, click **Finish**.

Step 5: Install Certificate Services

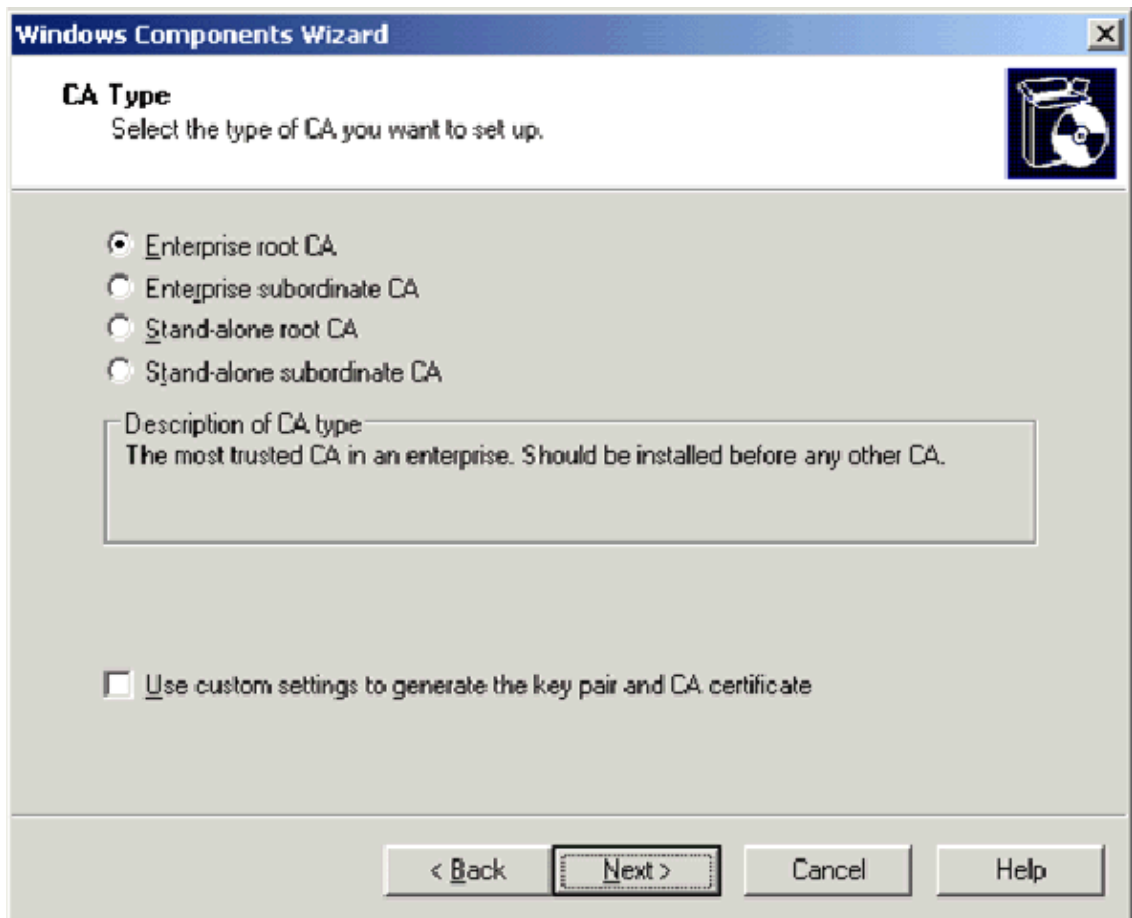
Complete these steps:

Note: IIS must be installed before you install Certificate Services and the user should be part of the Enterprise Admin OU.

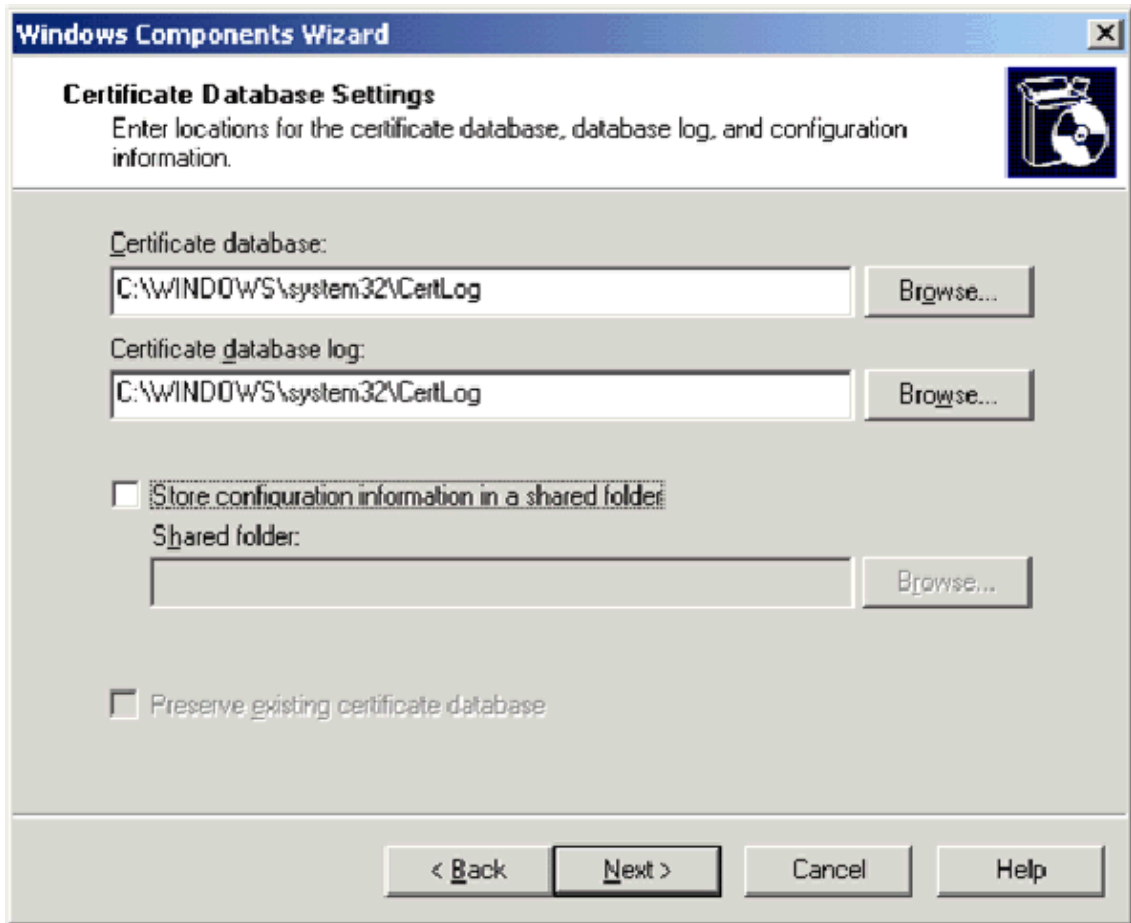
1. In the Control Panel, open **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. On the Windows Components Wizard page, choose **Certificate Services**, and then click **Next**.



3. On the CA Type page, choose **Enterprise root CA** and click **Next**.



4. On the CA Identifying information page, type **wirelessdemoca** in the Common name for this CA box. You can enter the other optional details and then click **Next**. Accept the defaults on the Certificate Database Settings page.



5. Click **Next**. Upon completion of the installation, click **Finish**.
6. Click **OK** after you read the warning about installing IIS.

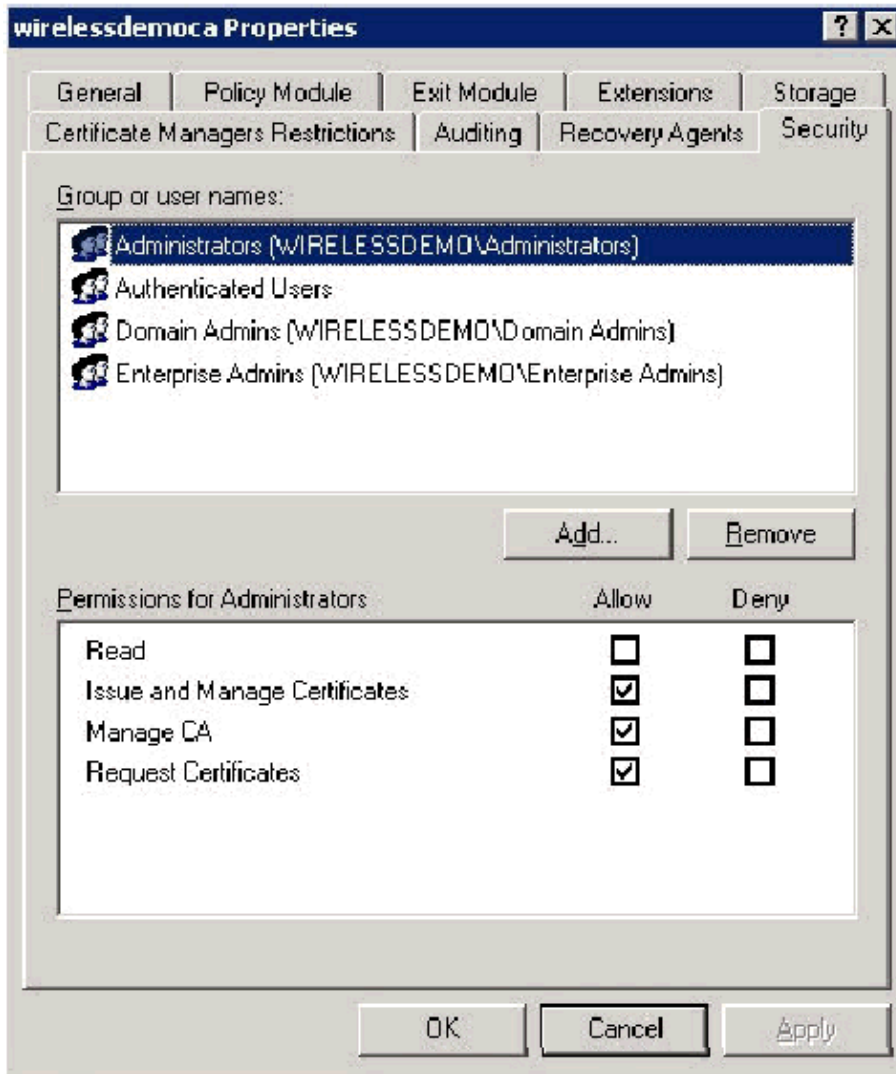
Step 6: Verify Administrator Permissions for Certificates

Complete these steps:

1. Choose **Start > Administrative Tools > Certification Authority**.
2. Right-click **wirelessdemoca CA** and then click **Properties**.
3. On the Security tab, click **Administrators** in the Group or User names list.
4. In the Permissions or Administrators list, verify that these options are set to **Allow**:

- ◆ Issue and Manage Certificates
- ◆ Manage CA
- ◆ Request Certificates

If any of these are set to Deny or are not selected, set the permission to **Allow**.



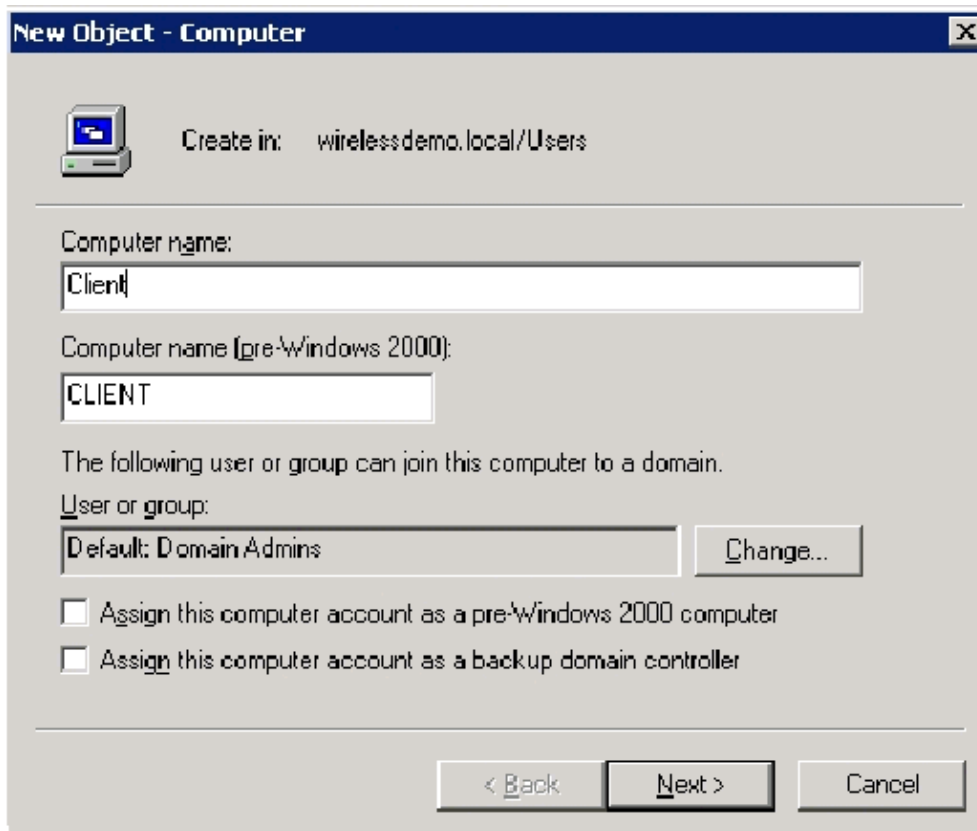
5. Click **OK** to close the wirelessdemoca CA Properties dialog box, and then close Certification Authority.

Step 7: Add Computers to the Domain

Complete these steps:

Note: If the computer is already added to the domain, proceed to Add Users to the Domain.

1. Open the Active Directory Users and Computers snap-in.
2. In the console tree, expand **wirelessdemo.local**.
3. Right-click **Users**, click **New**, and then click **Computer**.
4. In the New Object - Computer dialog box, type the name of the computer in the Computer Name field and click **Next**. This example uses the computer name **Client**.



5. In the Managed dialog box, click **Next**.
6. In the New Object–computer dialog box, click **Finish**.
7. Repeat steps 3 through 6 in order to create additional computer accounts.

Step 8: Allow Wireless Access to Computers

Complete these steps:

1. In the Active Directory Users and Computers console tree, click the **Computers** folder and right-click on the computer for which you want to assign wireless access. This example shows the procedure with computer **CLIENT** which you added in step 7.
2. Click **Properties**, and then go to the Dial-in tab.
3. Choose **Allow access** and click **OK**.

Step 9: Add Users to the Domain

Complete these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**, click **New**, and then click **User**.
2. In the New Object – User dialog box, type **WirelessUser** in the First name field, and type **WirelessUser** in the User logon name field and click **Next**.

New Object - User

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

< Back Next > Cancel

3. In the New Object - User dialog box, type a password of your choice in the Password and Confirm password fields. Clear the **User must change password at next logon** check box, and click **Next**.

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

< Back Next > Cancel

4. In the New Object - User dialog box, click **Finish**.
5. Repeat steps 2 through 4 in order to create additional user accounts.

Step 10: Allow Wireless Access to Users

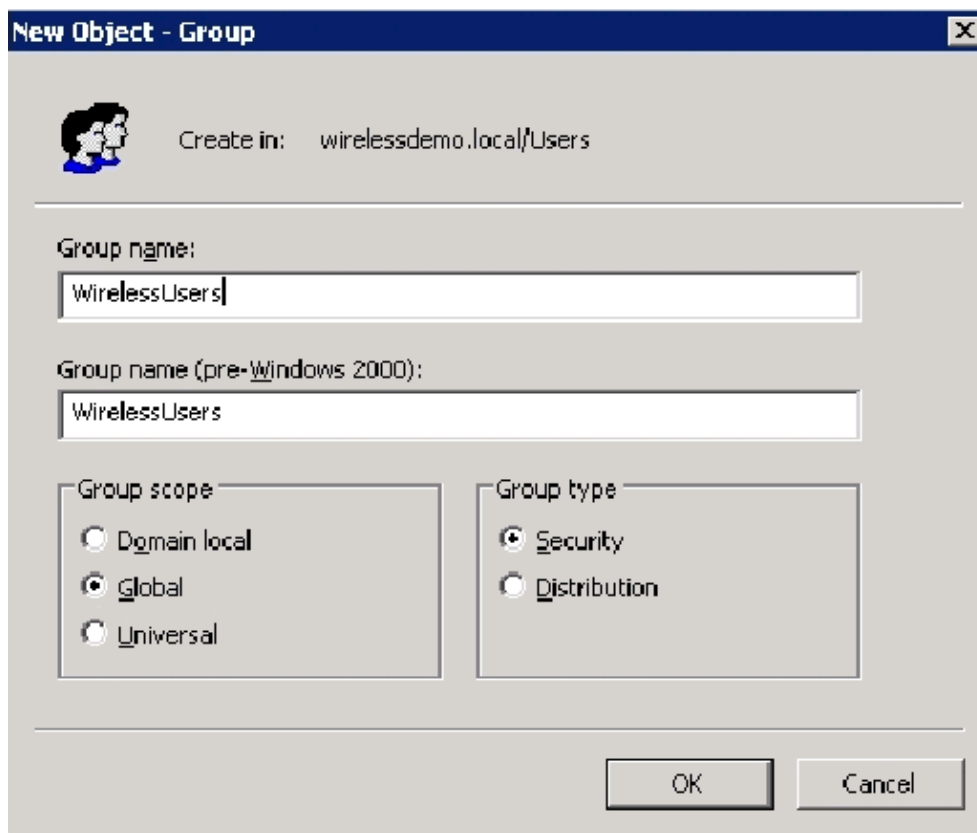
Complete these steps:

1. In the Active Directory Users and Computers console tree, click the **Users** folder, right-click **WirelessUser**, click **Properties**, and then go to the Dial-in tab.
2. Choose **Allow access** and click **OK**.

Step 11: Add Groups to the Domain

Complete these steps:

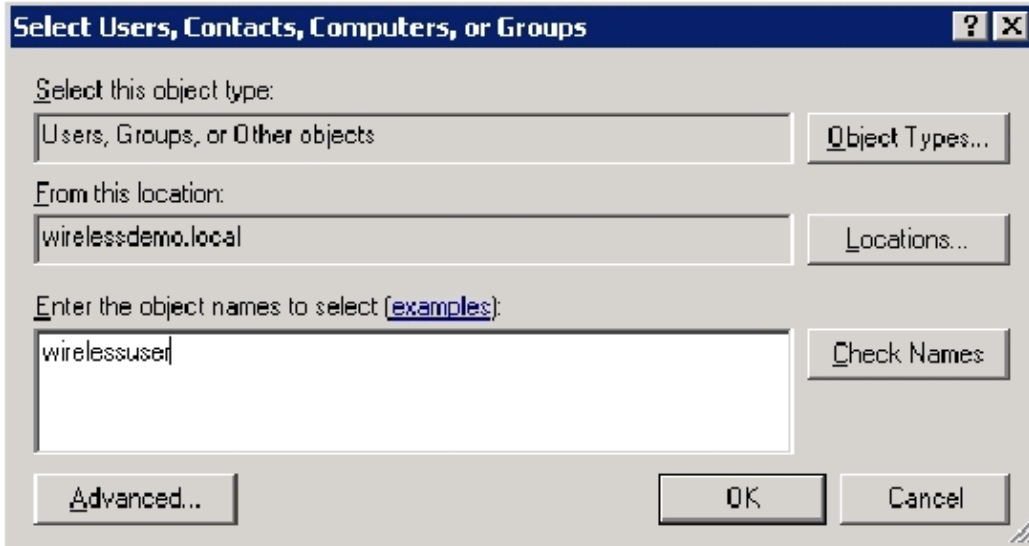
1. In the Active Directory Users and Computers console tree, right-click **Users**, click **New**, and then click **Group**.
2. In the New Object Group dialog box, type the name of the group in the Group name field and click **OK**. This document uses the group name **WirelessUsers**.



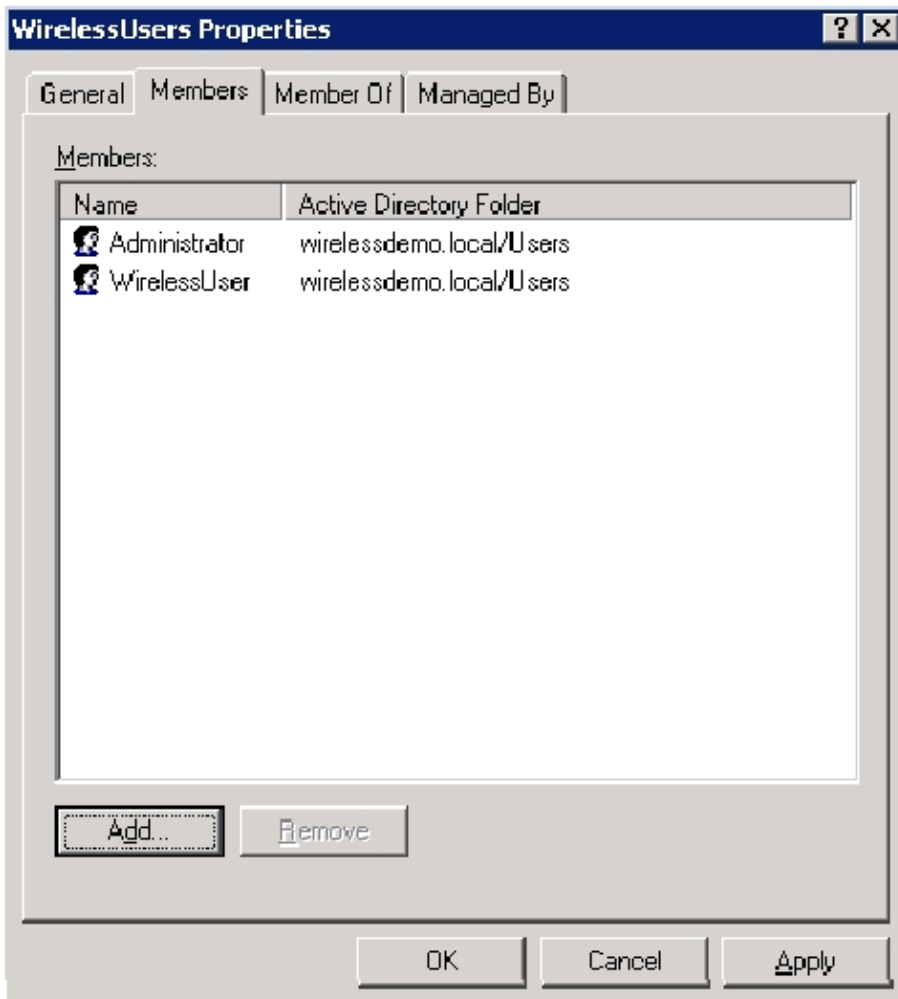
Step 12: Add Users to the WirelessUsers Group

Complete these steps:

1. In the details pane of Active Directory Users and Computers, double-click on the Group **WirelessUsers**.
2. Go to the Members tab and click **Add**.
3. In the Select Users, Contacts, Computers, or Groups dialog box, type the name of the users that you want to add to the group. This example shows how to add the user **wirelessuser** to the group. Click **OK**.



4. In the Multiple Names Found dialog box, click **OK**. The WirelessUser user account is added to the WirelessUsers group.

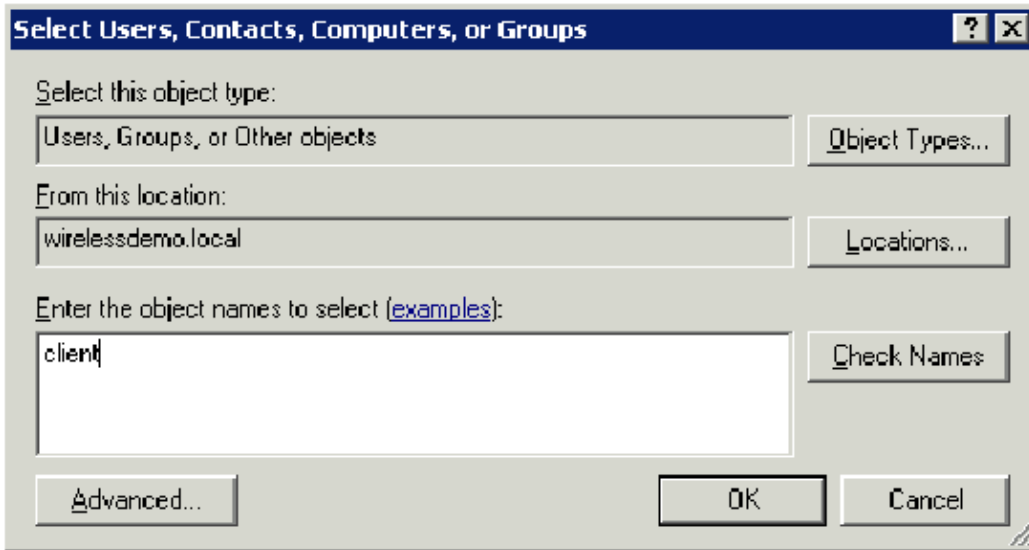


5. Click **OK** in order to save changes to the WirelessUsers group.
6. Repeat this procedure to add more users to the group.

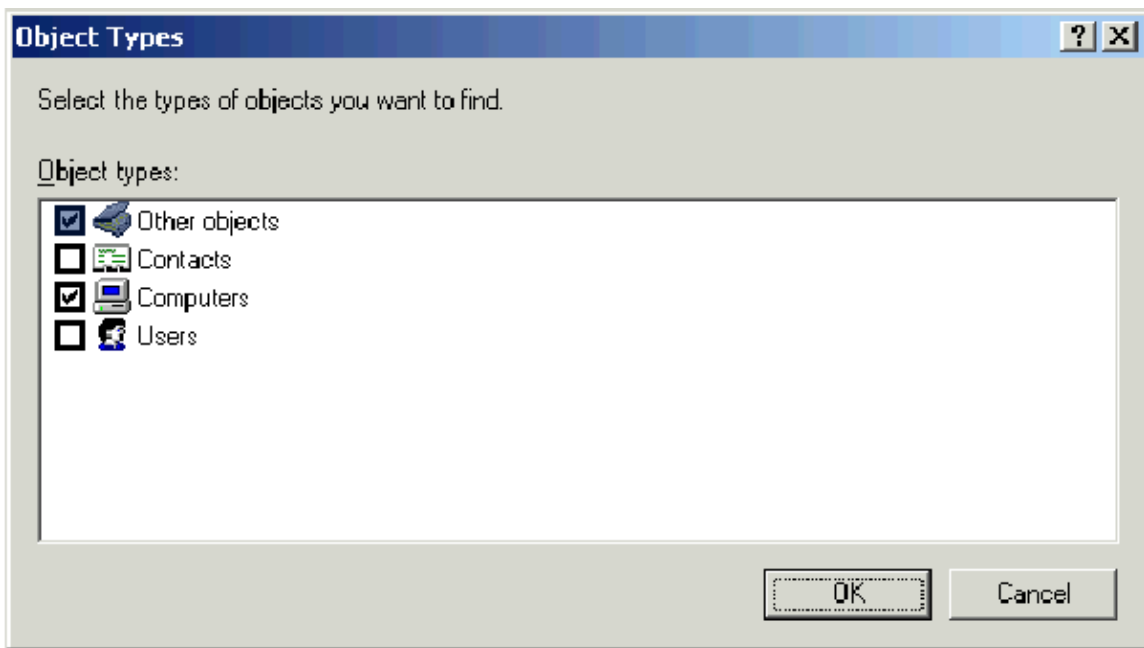
Step 13: Add Client Computers to the WirelessUsers Group

Complete these steps:

1. Repeat steps 1 and 2 in the Add Users to the WirelessUsers Group section of this document
2. In the Select Users, Contacts, or Computers dialog box, type the name of the computer that you want to add to the group. This example shows how to add the computer named **client** to the group.



3. Click **Object Types**, clear the **Users** check box, and then check **Computers**.



4. Click **OK** twice. The CLIENT computer account is added to the WirelessUsers group.
5. Repeat the procedure to add more computers to the group.

Windows Standard 2003 Setup with Cisco Secure ACS 4.0

Cisco Secure ACS is a computer that runs Windows Server 2003 with SP1, Standard Edition, that provides RADIUS authentication and authorization for the controller. Complete the procedures in this section in order to configure ACS as a RADIUS server:

Basic Installation and Configuration

Complete these steps:

1. Install Windows Server 2003 with SP1, Standard Edition, as a **member server** named **ACS** in the **wirelessdemo.local** domain.

Note: The ACS server name appears as cisco_w2003 in the remaining configurations. Substitute ACS or cisco_w2003 on the remaining lab setup.

2. For the local area connection, configure the TCP/IP protocol with the IP address of **172.16.100.26**, the subnet mask of **255.255.255.0**, and the DNS server IP address of **127.0.0.1**.

Cisco Secure ACS 4.0 Installation

Note: Refer to the Installation Guide for Cisco Secure ACS 4.0 for Windows for more information on how to configure Cisco Secure ACS 4.0 for Windows.

Complete these steps:

1. Using a Domain Administrator account, login to the computer named ACS to Cisco Secure ACS.

Note: Only installations performed at the computer where you install Cisco Secure ACS are supported. Remote installations performed using Windows Terminal Services or products such as Virtual Network Computing (VNC), are not tested, and are not supported.

2. Insert the Cisco Secure ACS CD into a CD-ROM drive on the computer.
3. If the CD-ROM drive supports the Windows autorun feature, the Cisco Secure ACS for Windows Server dialog box appears.

Note: If the computer does not have a required service pack installed, a dialog box appears. Windows service packs can be applied either before or after you install Cisco Secure ACS. You can continue with the installation, but the required service pack must be applied after the installation is complete. Otherwise, Cisco Secure ACS might not function reliably.

4. Perform one of these tasks:

- ◆ If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- ◆ If the Cisco Secure ACS for Windows Server dialog box does not appear, run **setup.exe**, located in the root directory of the Cisco Secure ACS CD.

5. The Cisco Secure ACS Setup dialog box displays the software license agreement.
6. Read the software license agreement. If you accept the software license agreement, click **Accept**.

The Welcome dialog box displays basic information about the setup program.

7. After you have read the information in the Welcome dialog box, click **Next**.
8. The Before You Begin dialog box lists items that you must complete before you continue with the installation. If you have completed all items listed in the Before You Begin dialog box, check the corresponding box for each item and click **Next**.

Note: If you have not completed all items listed in the Before You Begin box, click **Cancel** and then click **Exit Setup**. After you complete all items listed in the Before You Begin dialog box, restart the installation.

9. The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. This is the drive and path where the setup program installs Cisco Secure ACS.
10. If you want to change the installation location, complete these steps:
 - a. Click **Browse**. The Choose Folder dialog box appears. The Path box contains the installation location.
 - b. Change the installation location. You can either type the new location in the Path box or use the Drives and Directories lists to select a new drive and directory. The installation location must be on a drive local to the computer.

Note: Do not specify a path that contains a percent character, "%". If you do so, the installation might appear to continue properly but fails before it completes.

c. Click **OK**.

Note: If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. In order to continue, click **Yes**.

11. In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.
12. Click **Next**.
13. The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the Cisco Secure user database only, or also with a Windows user database.

Note: After you install Cisco Secure ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

14. If you want to authenticate users with the Cisco Secure user database only, choose the **Check the Cisco Secure ACS database only** option.
15. If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the Cisco Secure user database, complete these steps:
 - a. Choose the **Also check the Windows User Database** option.
 - b. The **Yes, refer to "Grant dialin permission to user" setting** check-box becomes available.

Note: The **Yes, refer to "Grant dialin permission to user"** setting check-box applies to all forms of access controlled by Cisco Secure ACS, not just dial-in access. For example, a user accessing the network through a VPN tunnel is not dialing into a network access server. However, if the **Yes, refer to "Grant dialin permission to user"** setting box is checked, Cisco Secure ACS applies the Windows user dial-in permissions in order to determine whether to grant the user access to the network.

- c. If you want to allow access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check the **Yes, refer to "Grant dialin permission to user" setting** box.
16. Click **Next**.
17. The setup program installs Cisco Secure ACS and updates the Windows registry.
18. The Advance Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, refer to the User Guide for Cisco Secure ACS for Windows Server, Version 4.0.

Note: The listed features appear in the Cisco Secure ACS HTML interface only if you enable them. After installation, you can enable or disable them on the Advanced Options page in the Interface Configuration section.

19. For each feature you want to enable, check the corresponding box.
20. Click **Next**.
21. The Active Service Monitoring dialog box appears.

Note: After installation, you can configure active service monitoring features on the Active Service Management page in the System Configuration section.

22. If you want Cisco Secure ACS to monitor user authentication services, check the **Enable Login Monitoring** box. From the Script to Execute list, choose the option you want applied in the event of an authentication service failure:

◆ **No Remedial Action** Cisco Secure ACS does not run a script.

Note: This option is useful if you enable event mail notifications.

- ◆ **Reboot** Cisco Secure ACS runs a script that reboots the computer that runs Cisco Secure ACS.
 - ◆ **Restart All** Cisco Secure ACS restarts all Cisco Secure ACS services.
 - ◆ **Restart RADIUS/TACACS+** Cisco Secure ACS restarts only the RADIUS and TACACS+ services.
23. If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, check the **Mail Notification** box.
 24. Click **Next**.
 25. The Database Encryption Password dialog box appears.

Note: The Database Encryption Password is encrypted and stored in the ACS registry. You might need to reuse this password when critical problems arise and the database needs to be accessed manually. Keep this password at hand so that Technical Support can gain access to the database. The password can be changed each expiration period.

26. Enter a password for database encryption. The password needs to be at least eight characters long and needs to contain both characters and digits. There are no invalid characters. Click **Next**.
27. The setup program finishes and the Cisco Secure ACS Service Initiation dialog box appears.
28. For each Cisco Secure ACS Services Initiation option you want, check the corresponding box. The actions associated with the options occur after the setup program finishes.

- ◆ **Yes, I want to start the Cisco Secure ACS Service now** Starts the Windows services that compose Cisco Secure ACS. If you do not select this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.
 - ◆ **Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation** Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.
 - ◆ **Yes, I want to view the Readme File** Opens the README.TXT file in Windows Notepad.
29. Click **Next**.
 30. If you selected an option, the Cisco Secure ACS services start. The Setup Complete dialog box displays information about the Cisco Secure ACS HTML interface.
 31. Click **Finish**.

Note: The rest of the configuration is documented under the section for the EAP type that is configured.

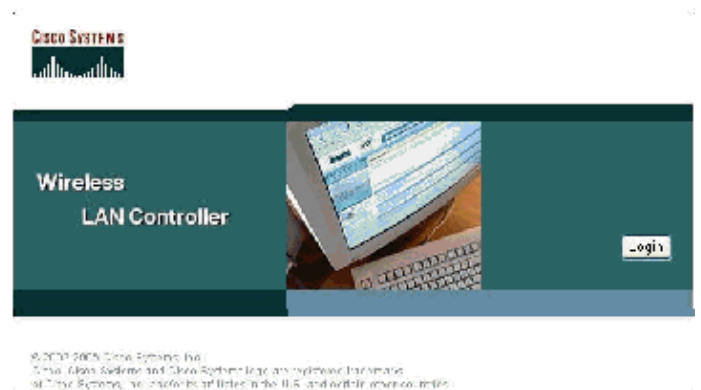
Cisco LWAPP Controller Configuration

Create the Necessary Configuration for WPA2/WPA

Complete these steps:

Note: The assumption is that the controller has basic connectivity to the network and IP reachability to the management interface is successful.

1. Login into the controller by browsing to **https://172.16.101.252**.



2. Click **Login**.
3. Login with the default user **admin** and default password **admin**.
4. Create the Interface VLAN mapping under the Controller menu.
5. Click **Interfaces**.
6. Click **New**.
7. In the Interface name field type **Employee**. (This field can be any value you like.)
8. In the VLAN ID field type **20**. (This field can be any VLAN that is carried in the network.)
9. Click **Apply**.
10. Configure the information as this Interfaces > Edit window shows.

The screenshot shows the Cisco Systems web interface for configuring a wireless LAN. The left sidebar contains navigation options: Controller, General, Inventory, Interfaces, Internal DHCP Server, Mobility Management (with sub-options: Mobility Groups, Mobility Statistics), Ports, Master Controller Mode, Network Time Protocol, and QoS Profiles. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name: employee
- Interface Address:**
 - VLAN Identifier: 20
 - IP Address: 172.16.100.1
 - 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

A red note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

11. Click **Apply**.
12. Click **WLAN**.
13. Click **New**.
14. In the WLAN SSID field type **Employee**.
15. Click **Apply**.
16. Configure the information as this WLANs > Edit window shows.

Note: WPA2 is the chosen Layer 2 encryption method for this lab. In order to allow WPA with TKIP-MIC clients to associate to this SSID, you can also check the boxes **WPA compatibility mode** and **Allow WPA2 TKIP Clients** or those clients that do not support the the 802.11i AES encryption method.

WLANs > Edit

WLAN ID	1
WLAN SSID	Employee

General Policies

Radio Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Power Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow AAA Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

Security Policies

Layer 2 Security	WPA2 <input type="checkbox"/> MAC Filtering
Layer 3 Security	None <input type="checkbox"/> Web Policy **

* Web Policy cannot be used in combination with L2TP.

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

17. Click **Apply**.
18. Click the **Security** menu and add the RADIUS server.
19. Click **New**.
20. Add the RADIUS server IP address (172.16.100.25) which is the ACS server configured earlier.
21. Ensure that the shared key matches the AAA client configured in the ACS server.
22. Click **Apply**.



Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

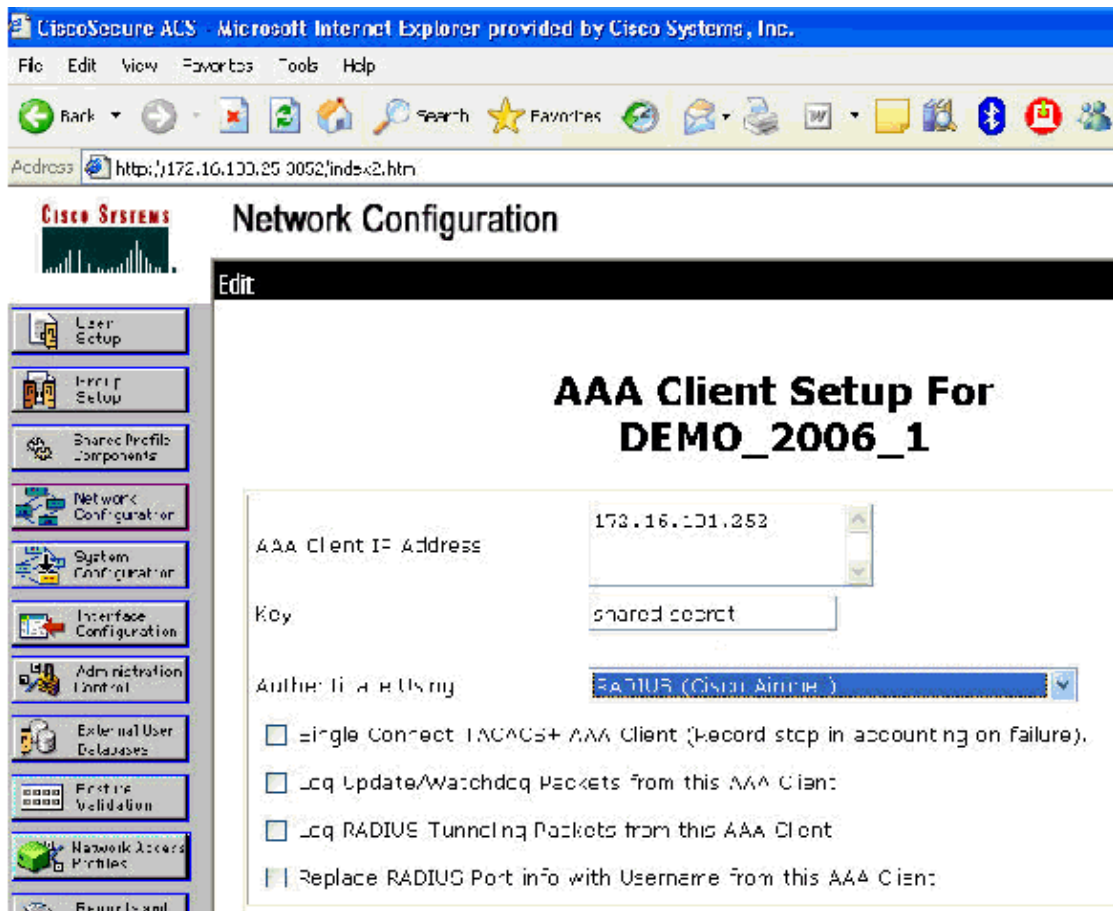
Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

RADIUS Authentication Servers > New

Server Index (Priority)	<input type="text" value="1"/>
Server IP Address	<input type="text" value="172.16.100.25"/>
Keys Format	<input type="text" value="ASCII"/>
Shared Secret	<input type="password" value="....."/>
Confirm Shared Secret	<input type="password" value="....."/>
Key Wrap	<input type="checkbox"/>
Port Number	<input type="text" value="1812"/>
Server Status	<input type="text" value="Enabled"/>
Support for RFC 3576	<input type="text" value="Enabled"/>
Retransmit Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable



23. The basic configuration is now complete and you can begin to test the EAP-TLS.

EAP-TLS Authentication

EAP-TLS authentication requires computer and user certificates on the wireless client, the addition of EAP-TLS as an EAP type to the remote access policy for wireless access, and a reconfiguration of the wireless network connection.

In order to configure DC_CA to provide auto-enrollment for computer and user certificates, complete the procedures in this section.

Note: Microsoft has changed the Web Server template with the release of the Windows 2003 Enterprise CA so that keys are no longer exportable and the option is greyed out. There are no other certificate templates supplied with certificate services that are for server authentication and give the ability to mark keys as exportable that are available in the drop-down so you have to create a new template that does so.

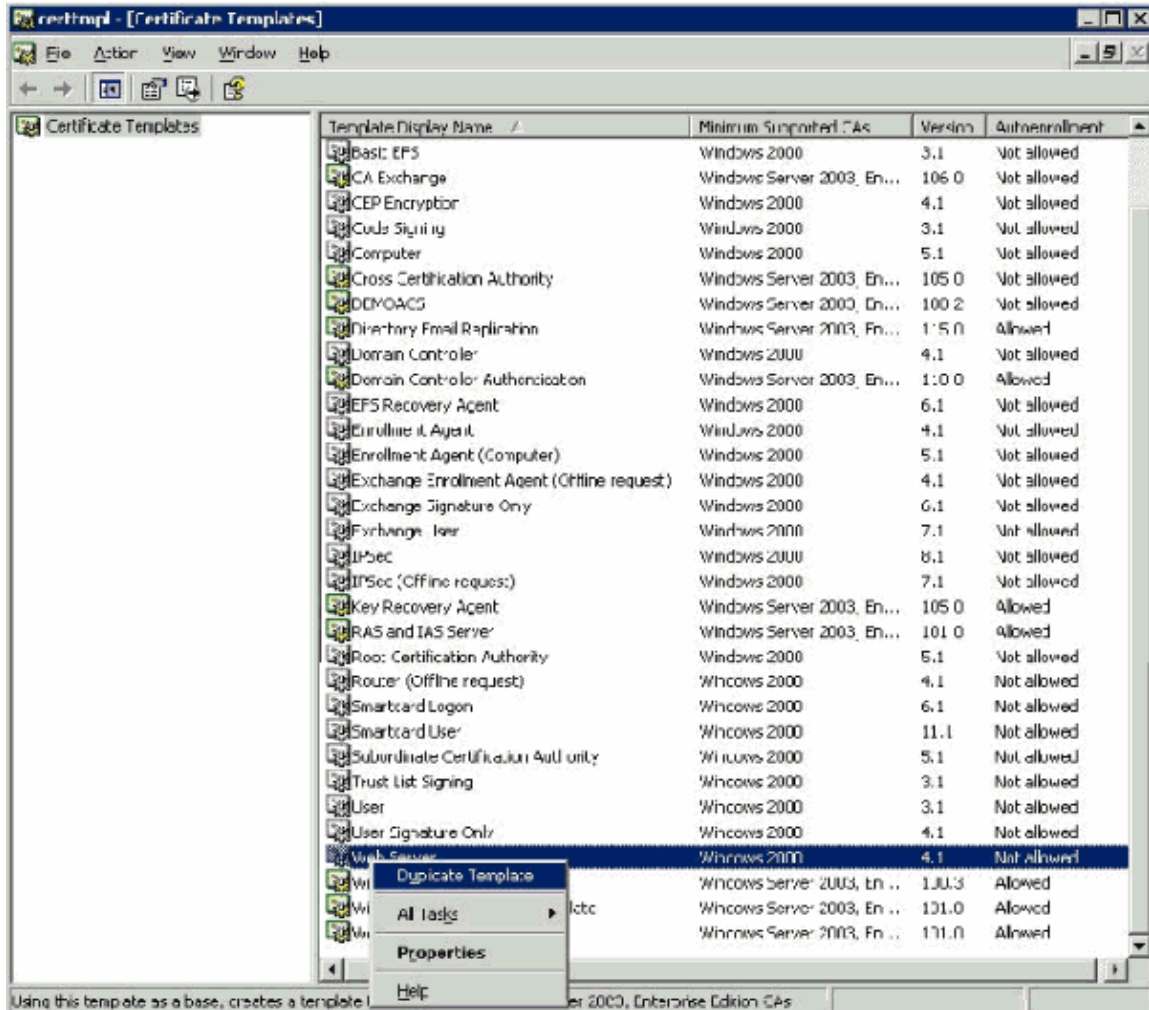
Note: Windows 2000 allows for exportable keys and these procedures do not need to be followed if you use Windows 2000.

Install the Certificate Templates Snap-in

Complete these steps:

1. Choose **Start > Run**, type **mmc**, and click **OK**.
2. On the File menu, click **Add/Remove Snap-in** and then click **Add**.
3. Under Snap-in, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. In the console tree, click **Certificate Templates**. All of the certificate templates appear in the Details pane.

5. In order to bypass steps 2 through 4, type **certtmpl.msc** which opens the Certificate Templates snap-in.



Create the Certificate Template for the ACS Web Server

Complete these steps:

1. In the Details pane of the Certificate Templates snap-in, click the **Web Server** template.
2. On the Action menu, click **Duplicate Template**.

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

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

OK Cancel Apply

3. In the Template display name field, type ACS.

Properties of New Template [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

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.

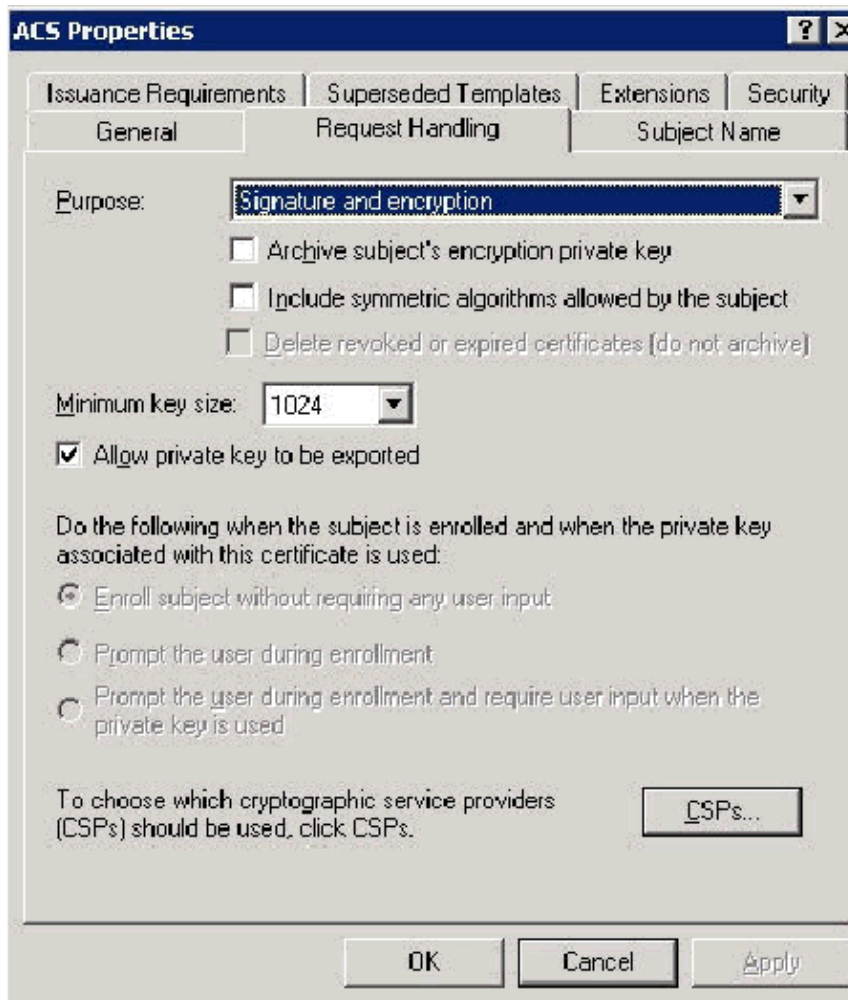
Template name:
ACS

Validity period: 2 years
Renewal period: 6 weeks

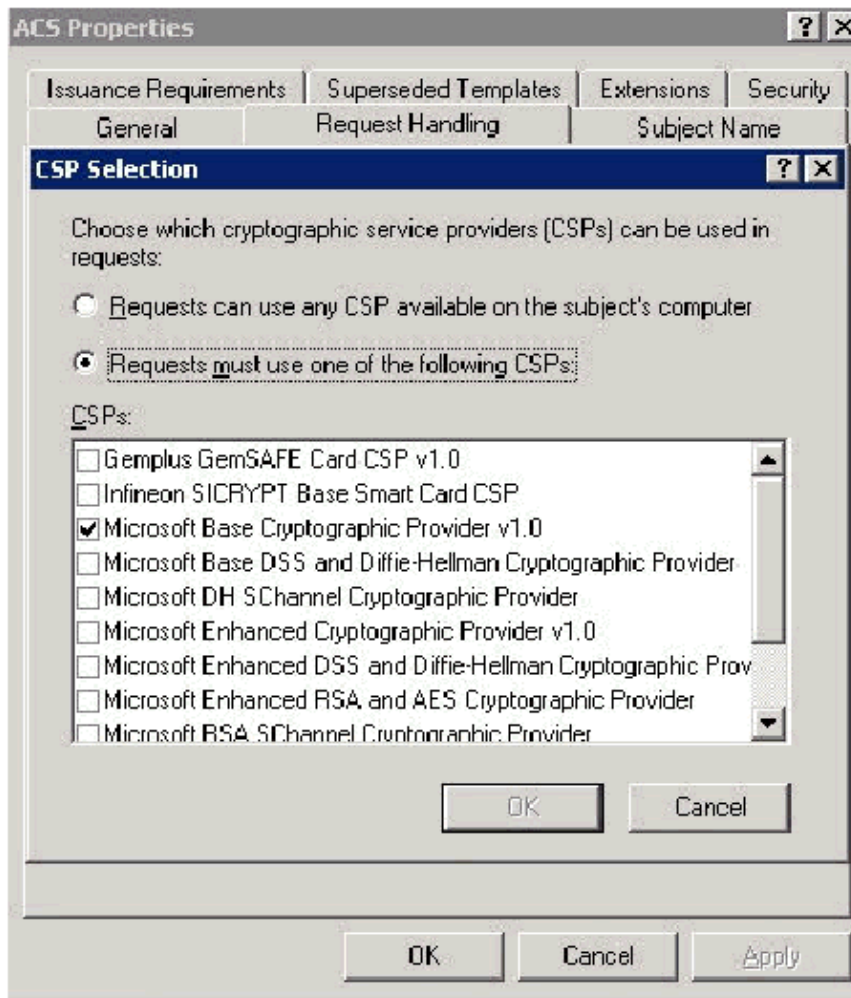
Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

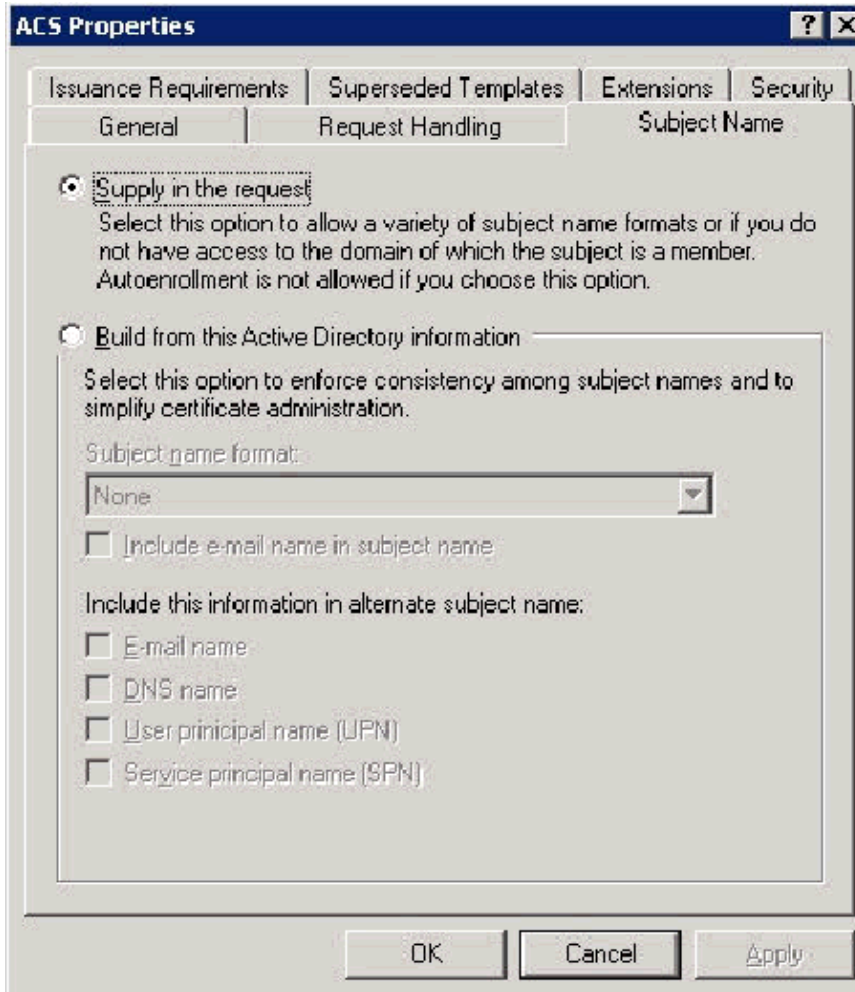
4. Go to the Request Handling tab and check **Allow private key to be exported**.



5. Choose **Requests must use one of the following CSPs** and check **Microsoft Base Cryptographic Provider v1.0**. Uncheck any other CSPs that are checked and then click **OK**.

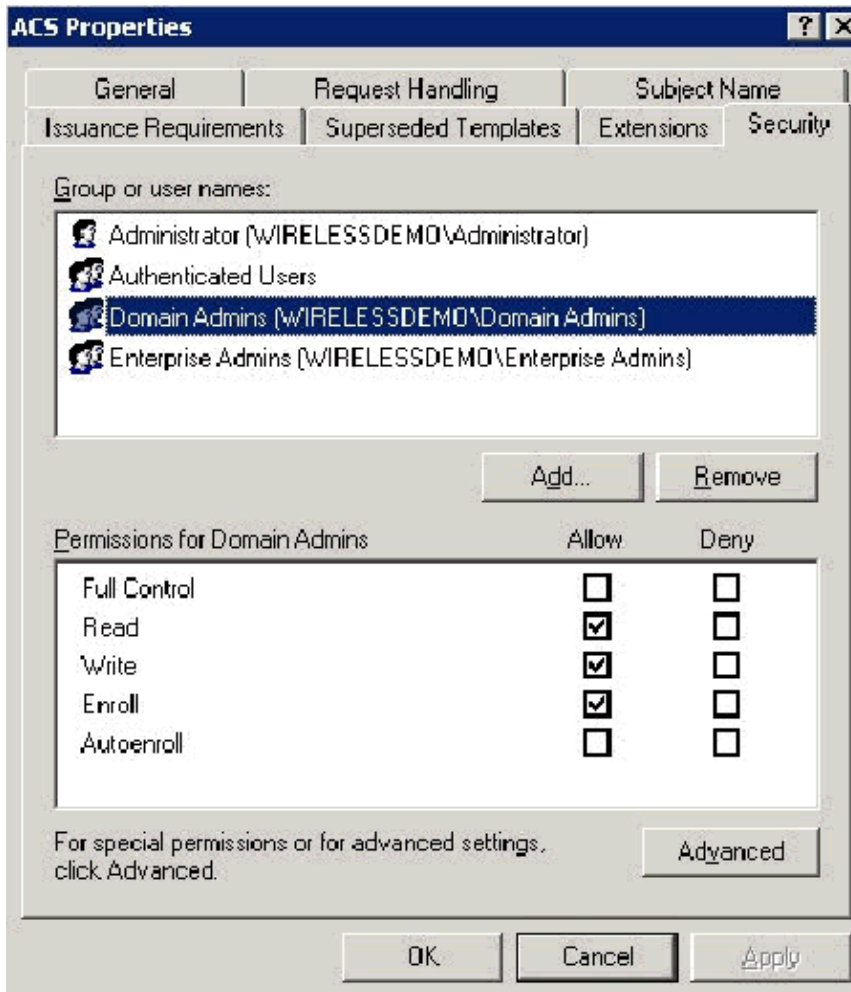


6. Go to the Subject Name tab, choose **Supply in the request** and click **OK**.

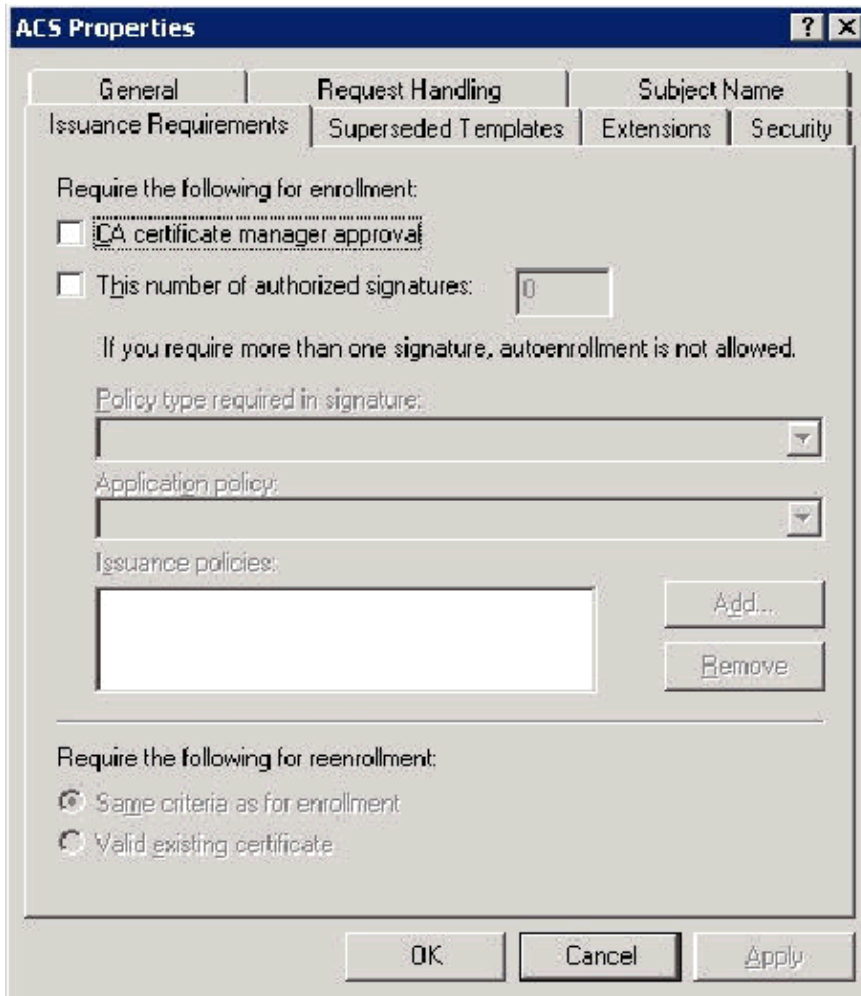


7. Go to the Security tab, highlight the **Domain Admins Group** and ensure that the **Enroll** option is checked under Allowed.

Important: If you choose to build from this Active Directory information only, check **User principal name (UPN)** and uncheck **Include email name** in Subject name and E-mail name because an e-mail name was not entered for the WirelessUser account in the Active Directory Users and Computers snap-in. If you do not disable these two options, auto-enrollment attempts to use e-mail, which results in an auto-enrollment error.



8. There are additional security measures if needed to prevent certificates from being automatically pushed out. These can be found under the Issuance Requirements tab. This is not discussed further in this document.

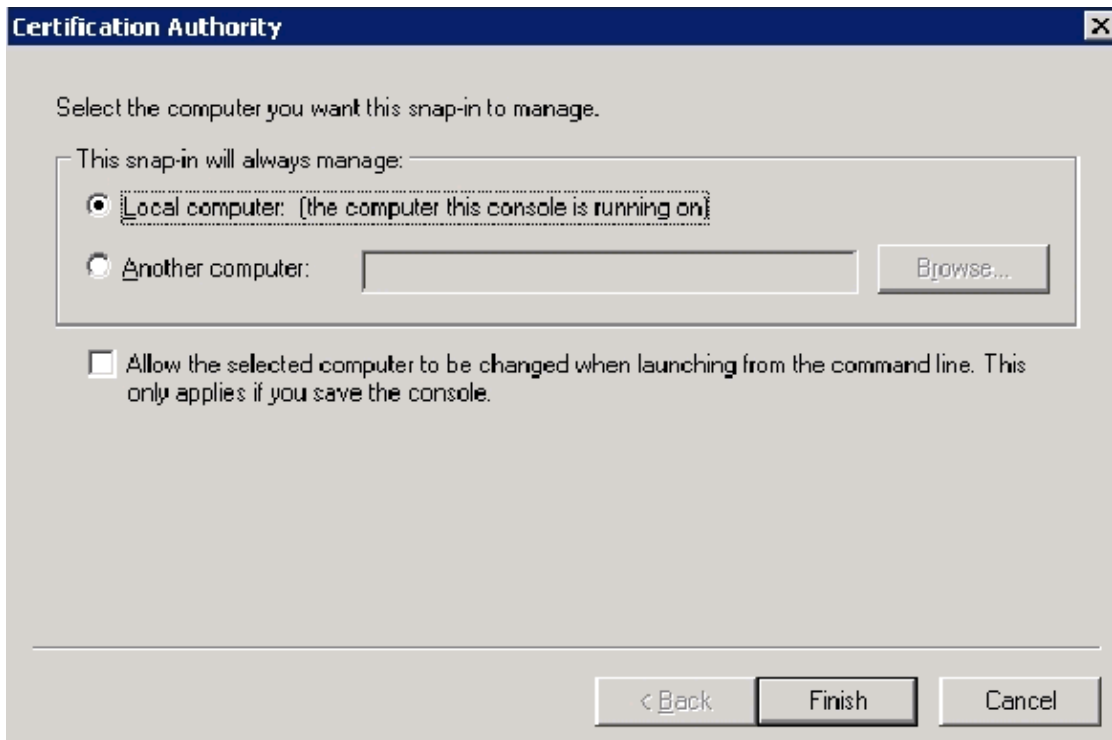


9. Click **OK** to save the template and move onto issuing this template from the Certificate Authority snap-in.

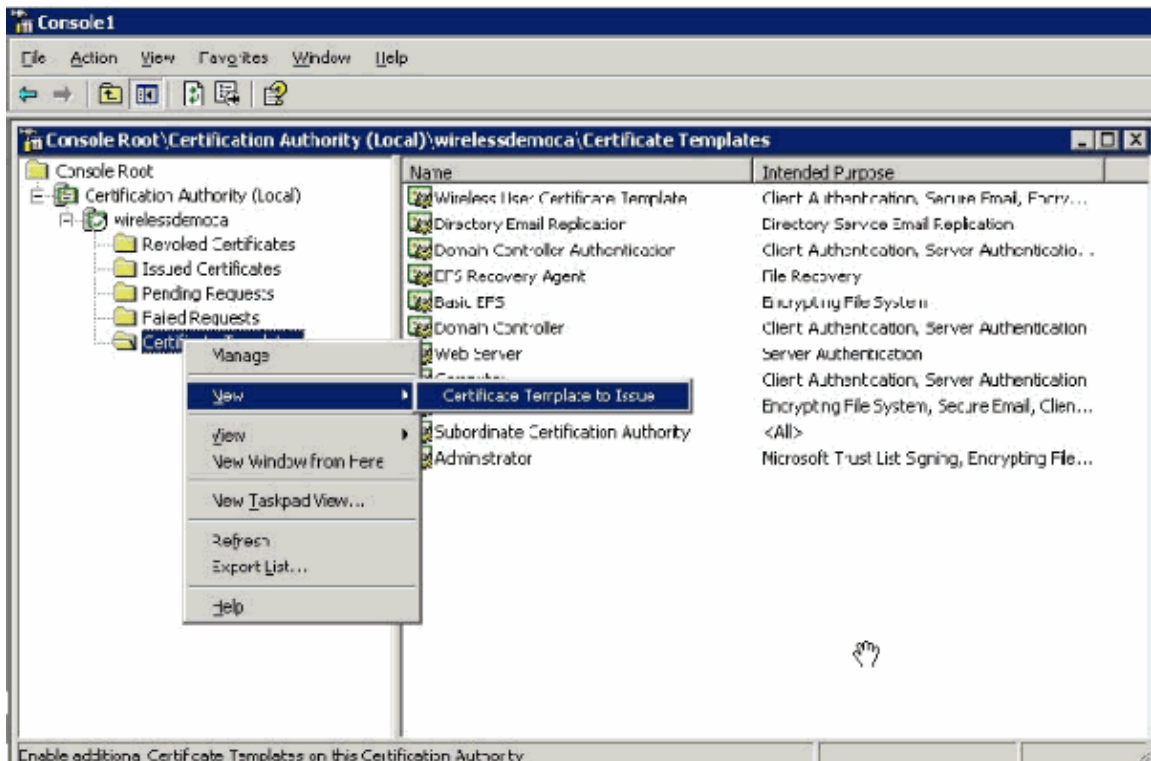
Enable the New ACS Web Server Certificate Template

Complete these steps:

1. Open the **Certification Authority** snap-in. Follow steps 1–3 in the Create the Certificate Template for the ACS Web Server section, choose the **Certificate Authority** option, choose **Local Computer** and click **Finish**.

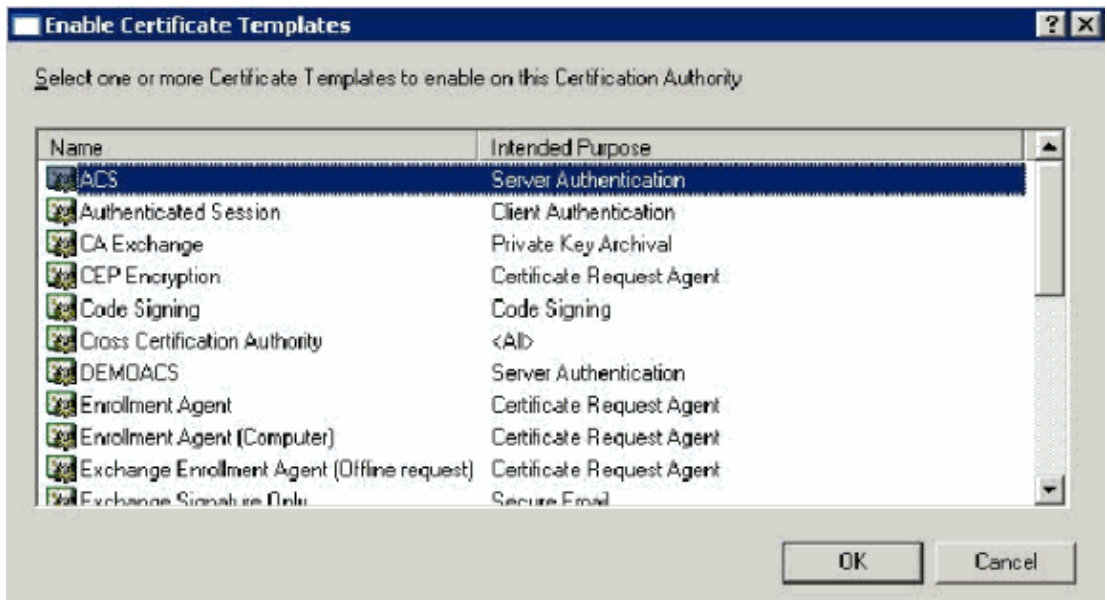


2. In the console tree, expand **wirelessdemoca**, and then right-click **Certificate Templates**.

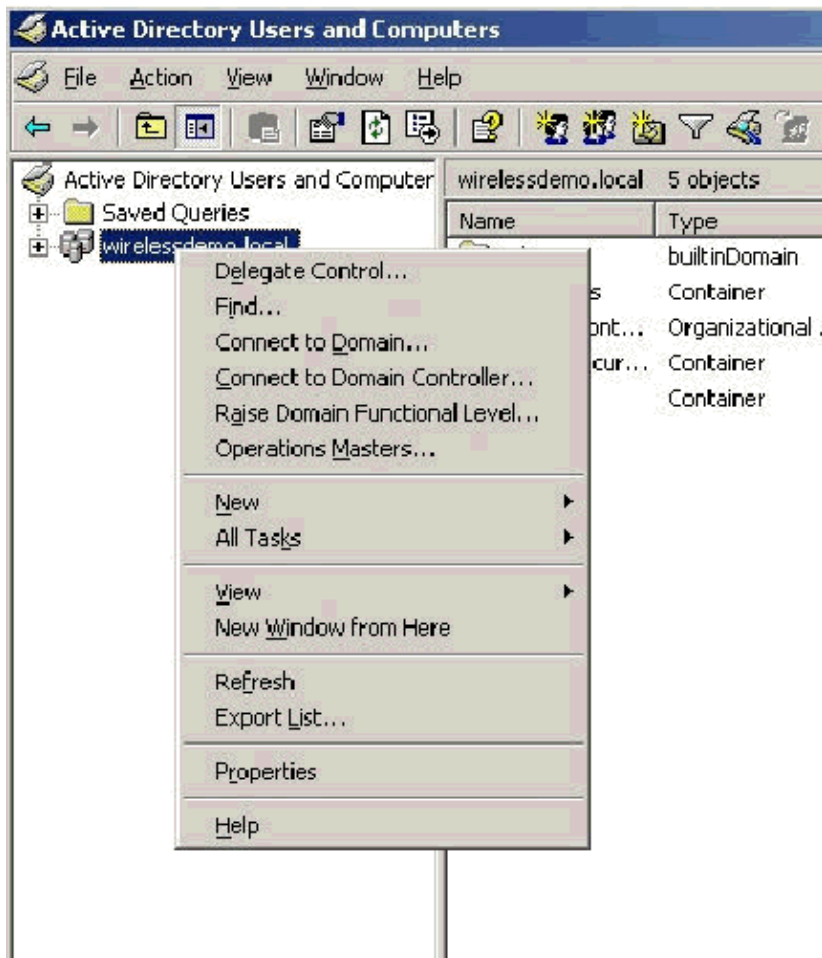


3. Choose **New > Certificate Template to Issue**.

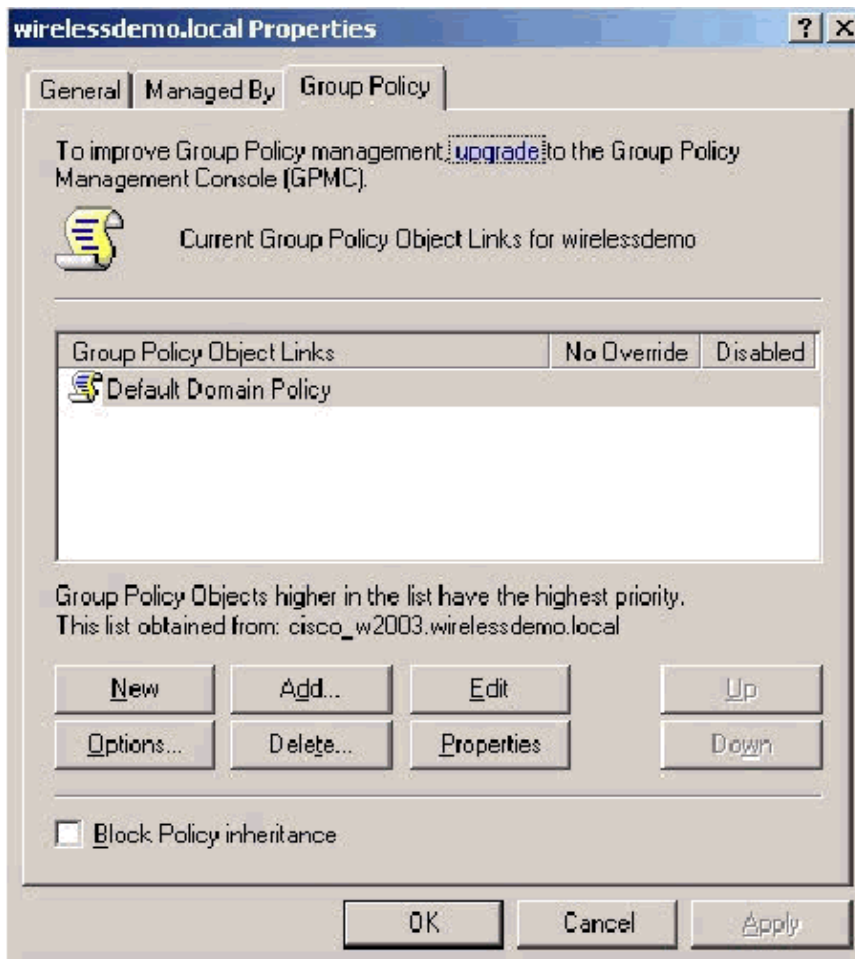
4. Click the ACS Certificate Template.



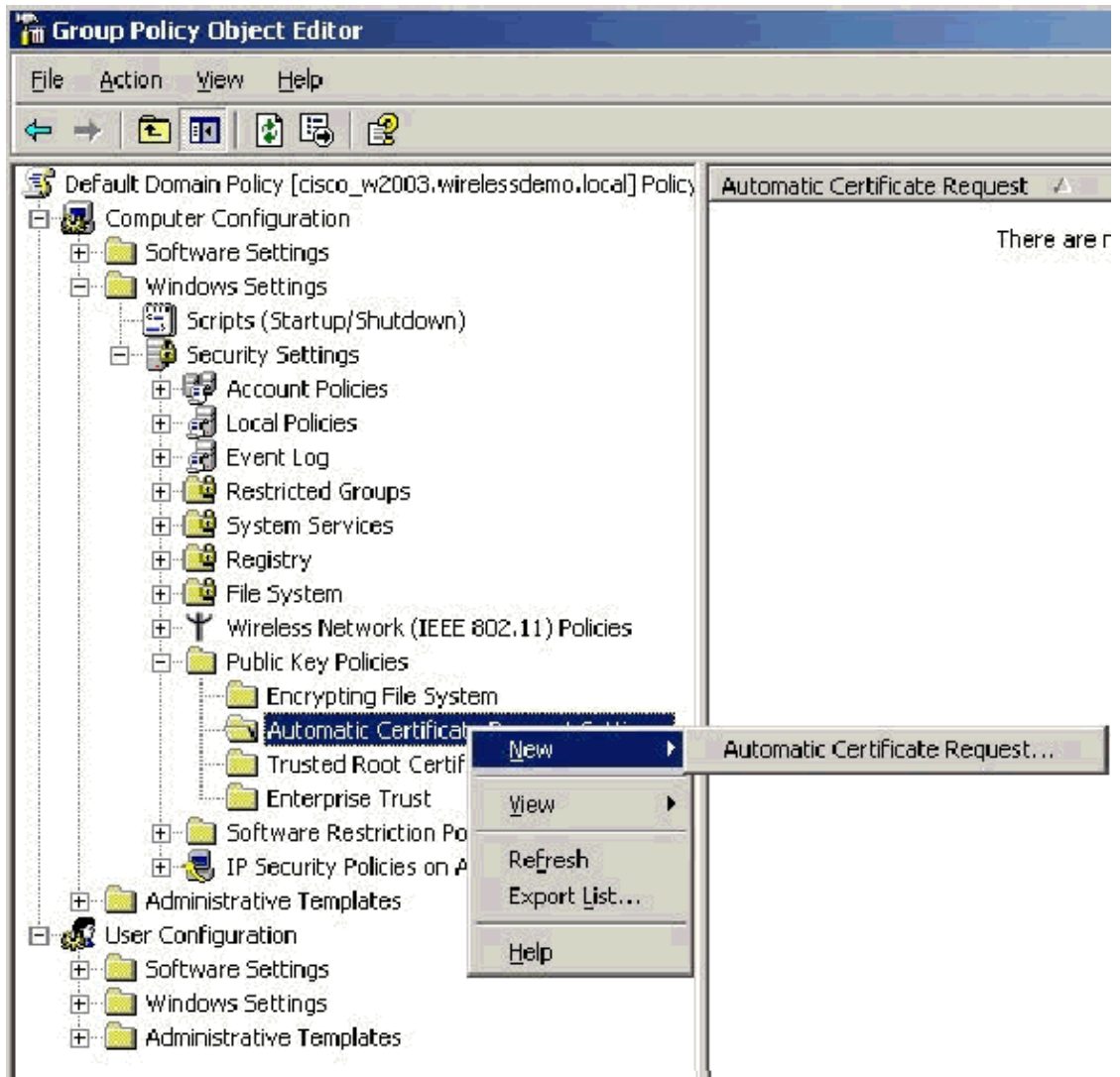
5. Click **OK** and open the **Active Directory Users and Computers** snap-in.
6. In the console tree, double-click **Active Directory Users and Computers**, right-click the **wirelessdemo.local** domain, and then click **Properties**.



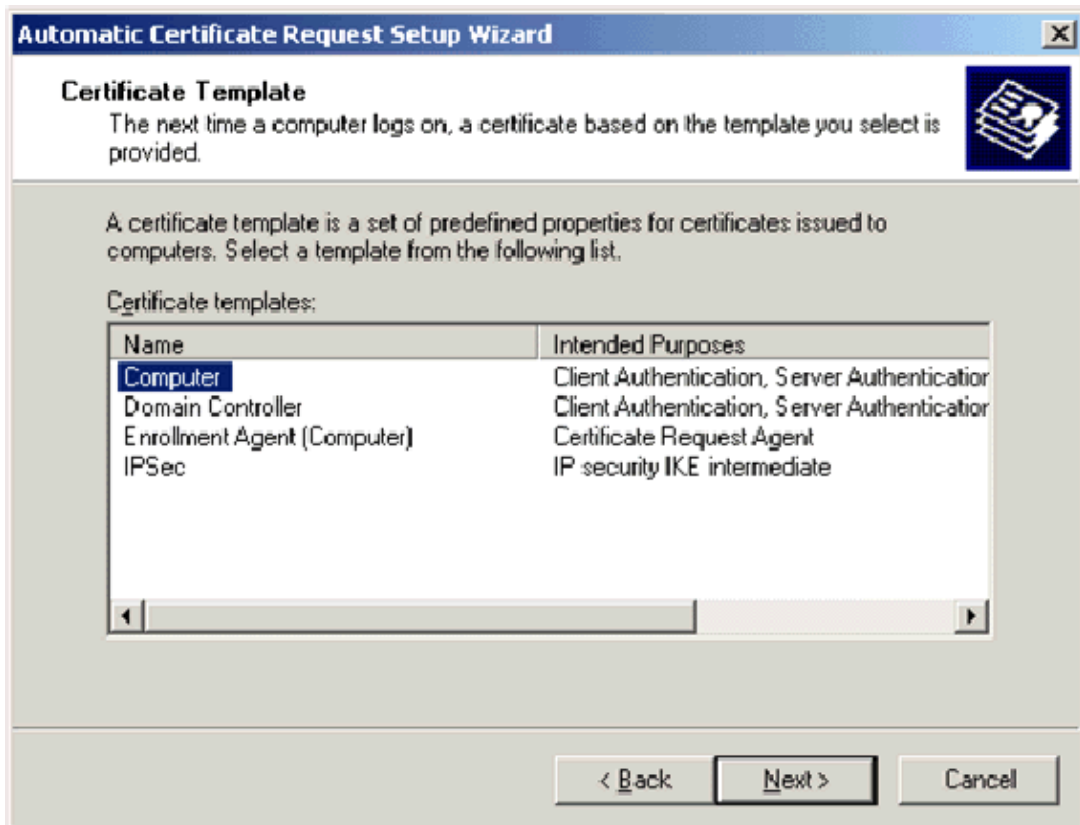
7. On the Group Policy tab, click **Default Domain Policy**, and then click **Edit**. This opens the Group Policy Object Editor snap-in.



8. In the console tree, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**, and then select **Automatic Certificate Request Settings**.

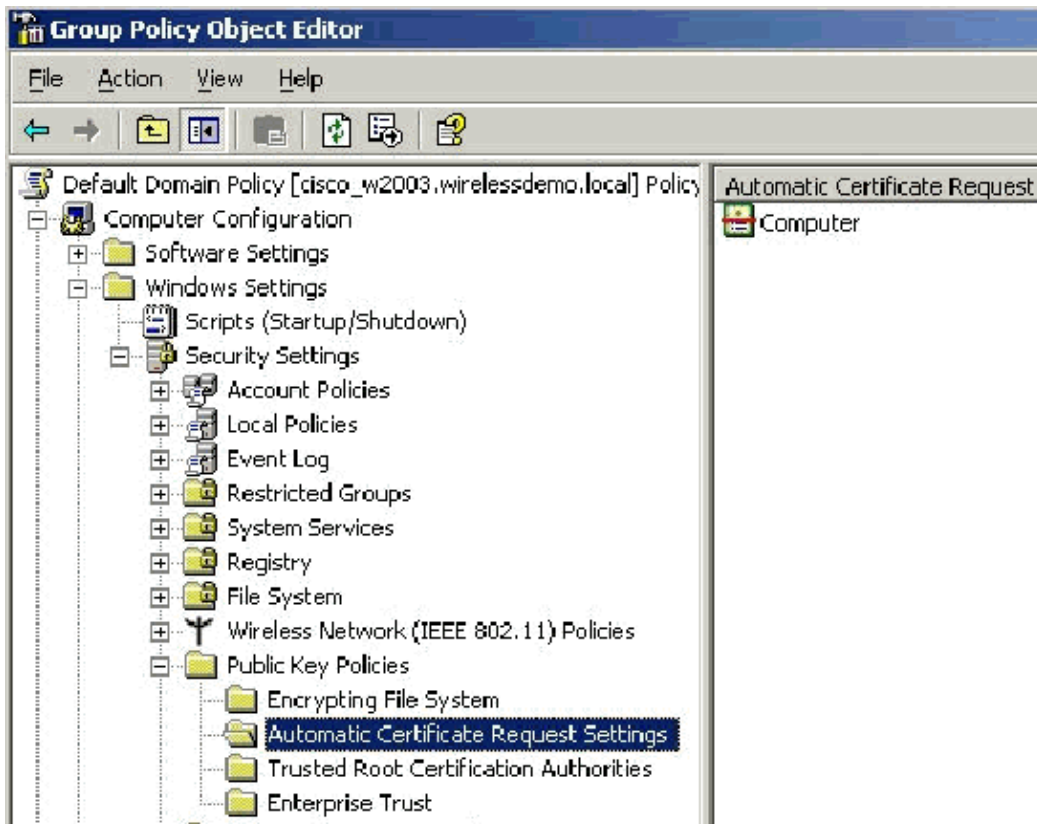


9. Right-click **Automatic Certificate Request Settings** and choose **New > Automatic Certificate Request**.
10. On the Welcome to the Automatic Certificate Request Setup Wizard page, click **Next**.
11. On the Certificate Template page, click **Computer** and click **Next**.

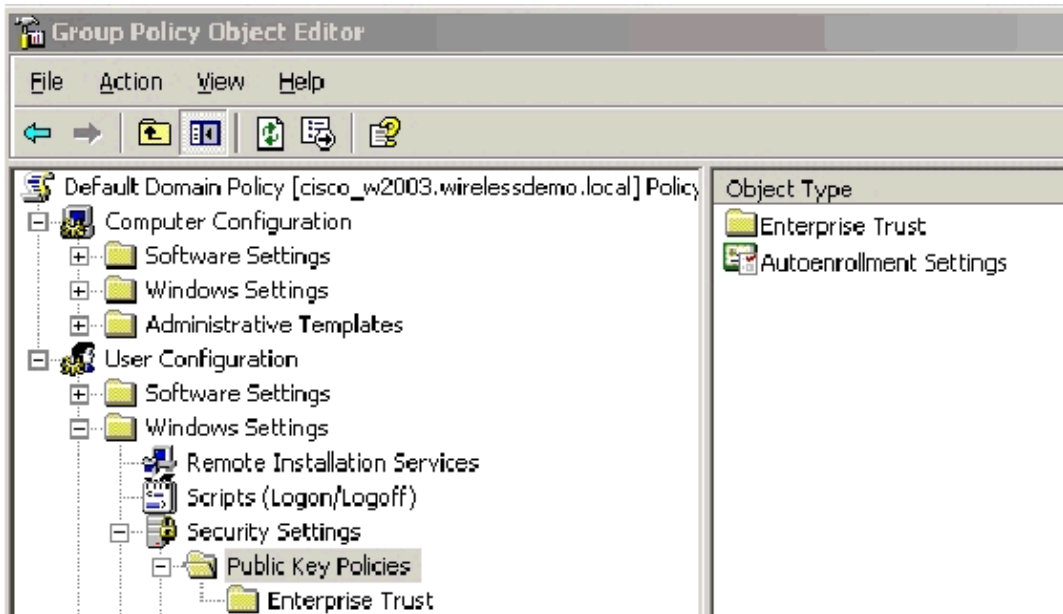


- On the Completing the Automatic Certificate Request Setup Wizard page, click **Finish**.

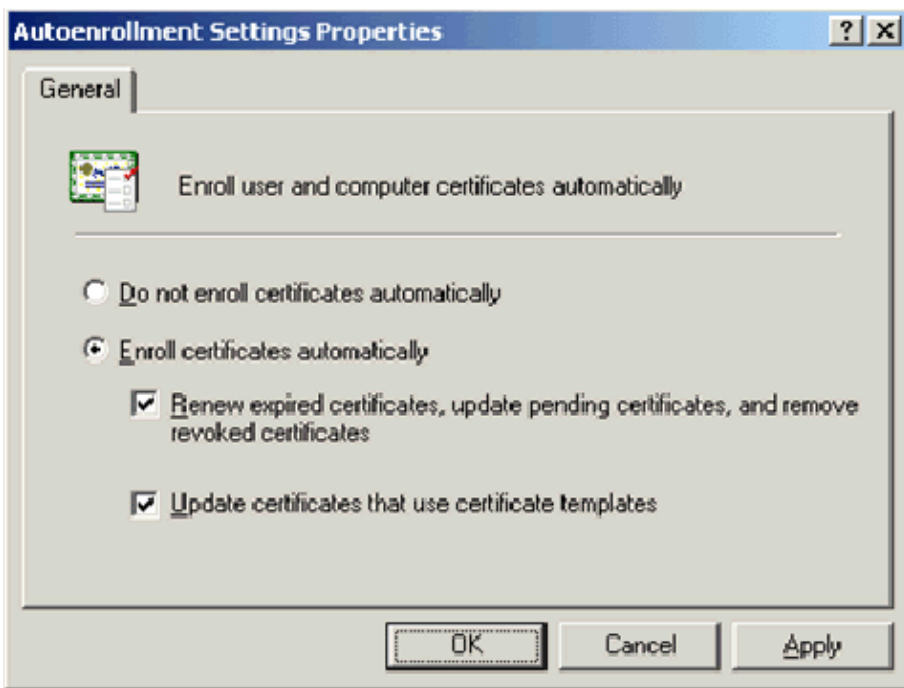
The Computer certificate type now appears in the details pane of the Group Policy Object Editor snap-in.



- In the console tree, expand **User Configuration > Windows Settings > Security Settings > Public Key Policies**.



14. In the details pane, double-click **Auto-enrollment Settings**.
15. Choose **Enroll certificates automatically** and check **Renew expired certificates, update pending certificates and remove revoked certificates** and **Update certificates that use certificate templates**.



16. Click **OK**.

ACS 4.0 Certificate Setup

Configure Exportable Certificate for ACS

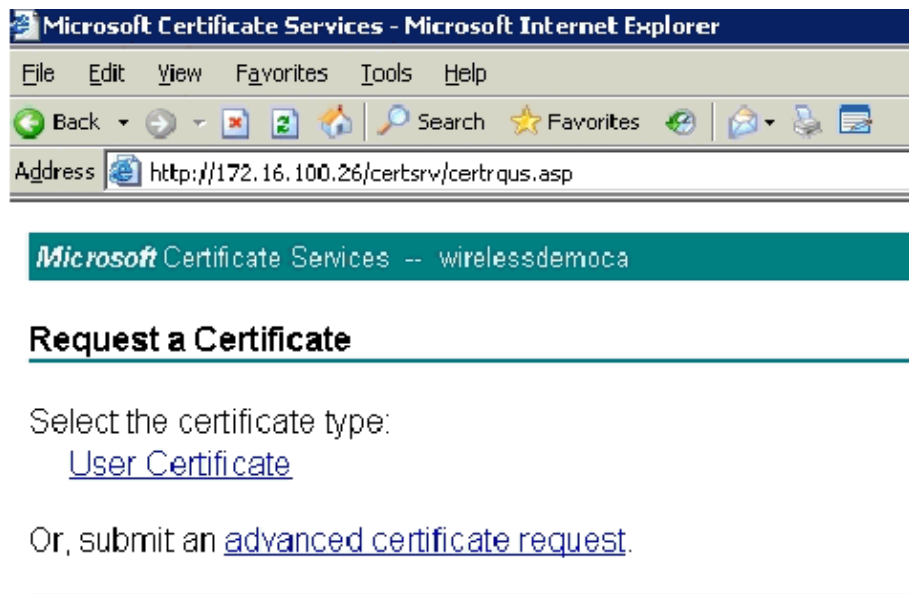
Important: The ACS server must obtain a server certificate from the Enterprise root CA server in order to authenticate a WLAN EAP-TLS client.

Important: Ensure that the IIS Manager is not open during the certificate setup process as it causes problems with cached information.

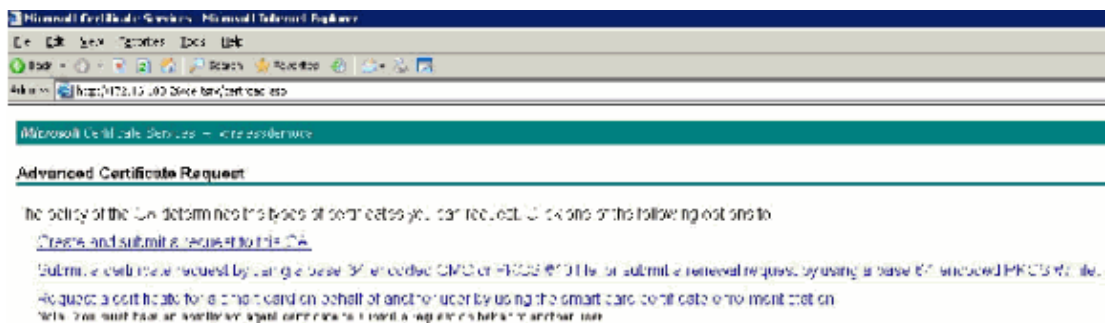
1. Log into the ACS server with an account that has Enterprise Admin rights.
2. On the local ACS machine, point the browser at the Microsoft certification authority server at **http://IP-address-of-Root-CA/certsrv**. In this case, the IP address is **172.16.100.26**.
3. Log in as the Administrator.



4. Choose **Request a Certificate** and click **Next**.



5. Choose **Advanced Request** and click **Next**.



6. Choose **Create and submit a request to this CA** and click **Next**.

Important: The reason for this step is due to the fact that Windows 2003 does not allow for exportable keys and you need to generate a certificate request based on the ACS Certificate that you created earlier that does.

Microsoft Certificate Services - wirelessdemo.local

Advanced Certificate Request

Certificate Template:

Administrator

Key Options:

Basic EFS
 EFS Recovery Agent
 User
 Wireless User Certificate Template

CSP: Microsoft Base Cryptographic Provider for Windows
 Microsoft Base Cryptographic Provider for Windows

Key Usage:

- Signing
- Non-repudiation
- Key Encipherment
- Key Agreement
- Data Encipherment
- Data Authentication

Key Size: 1024 bits (Max: 15360 bits)

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 file

Authority: [Empty field]

Friendly Name: [Empty field]

Submit >

- From the Certificate Templates, select the certificate template created earlier named **ACS**. The options change after you select the template.
- Configure the Name to be the fully qualified domain name of the ACS server. In this case the ACS server name is **cisco_w2003.wirelessdemo.local**. Ensure that **Store certificate in the local computer certificate store** is checked and click **Submit**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Deck Search Favorites

Address http://172.16.100.25/certsrv/cestrgna.asp

Certificate Template:

ACS

Identifying Information For Offline Template:

Name: gisco_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: 3072)

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 PKCS#10

Hash Algorithm: SHA-1
Only used to sign request.

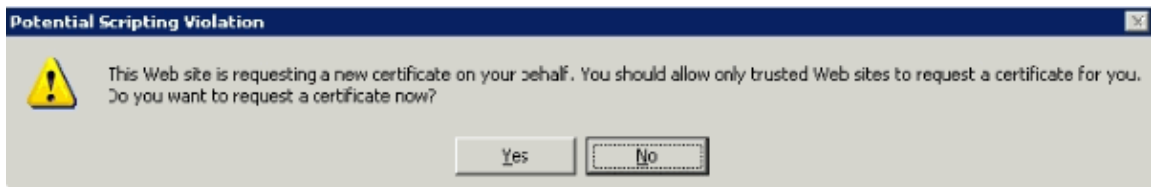
Save request to a file

Attributes:

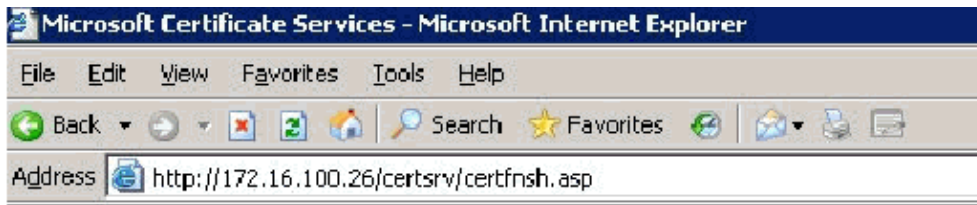
Friendly Name:

Submit >

9. A pop up window appears that warns about a potential scripting violation. Click **Yes**.



10. Click **Install this certificate**.



Microsoft Certificate Services -- wirelessdemoca

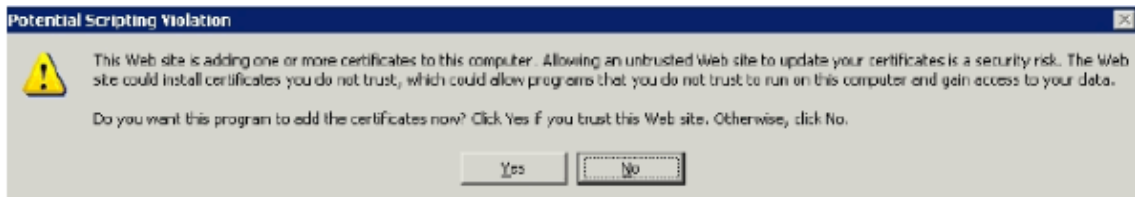
Certificate Issued

The certificate you requested was issued to you.

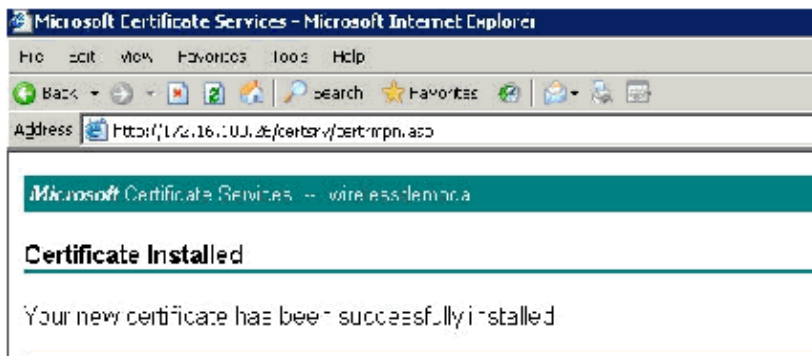


[Install this certificate](#)

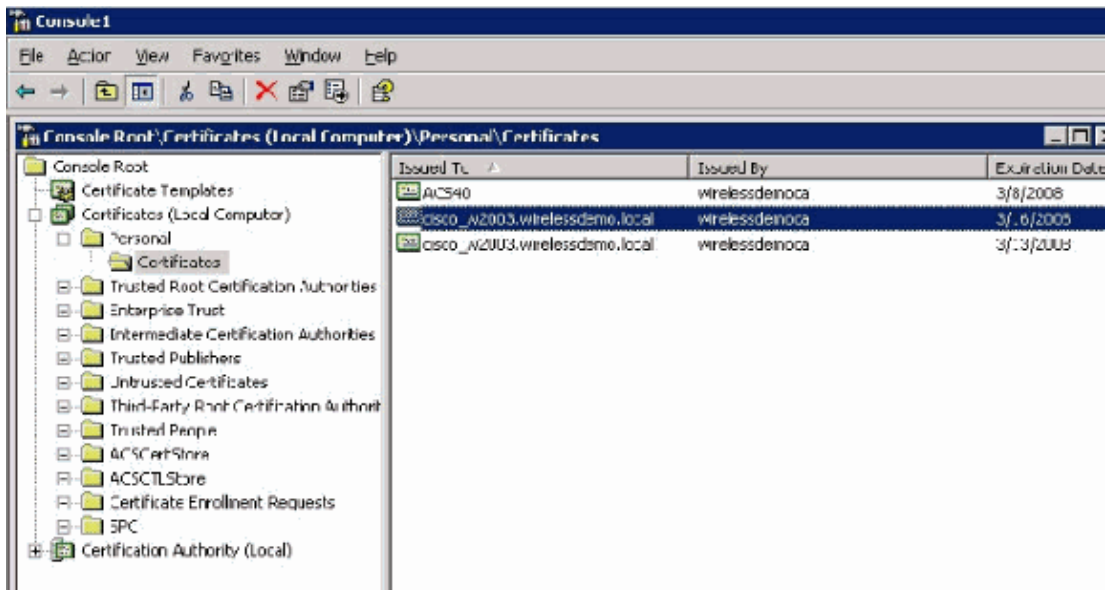
11. A pop up window appears again and warns about a potential scripting violation. Click **Yes**.



12. After you click **Yes**, the certificate is installed.



13. At this point, the certificate is installed in the Certificates folder. In order to access this folder, choose **Start > Run**, type **mmc**, press **Enter**, and choose **Personal > Certificates**.

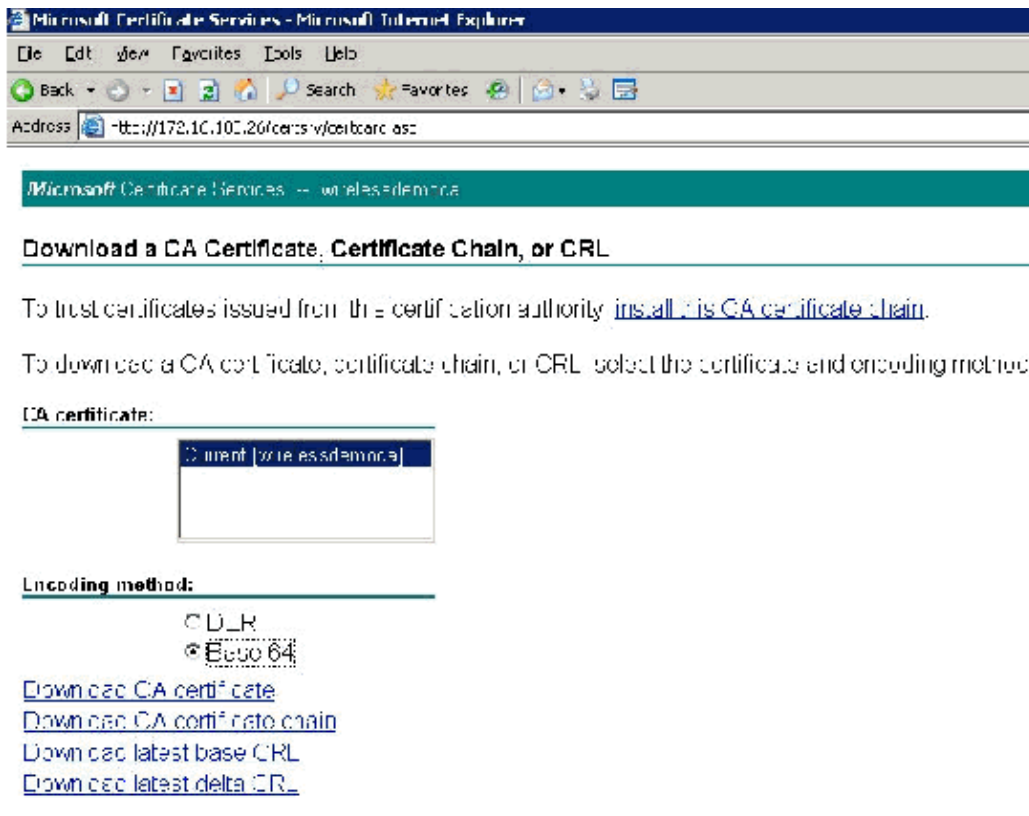


- Now that the certificate is installed to the local computer (ACS or cisco_w2003 in this example), you need to generate a certificate file (.cer) for the ACS 4.0 certificate file configuration.
- On the ACS server (cisco_w2003 in this example), point the browser at the Microsoft Certification Authority server to **http://172.16.100.26 /certsrv**.

Install the Certificate in ACS 4.0 Software

Complete these steps:

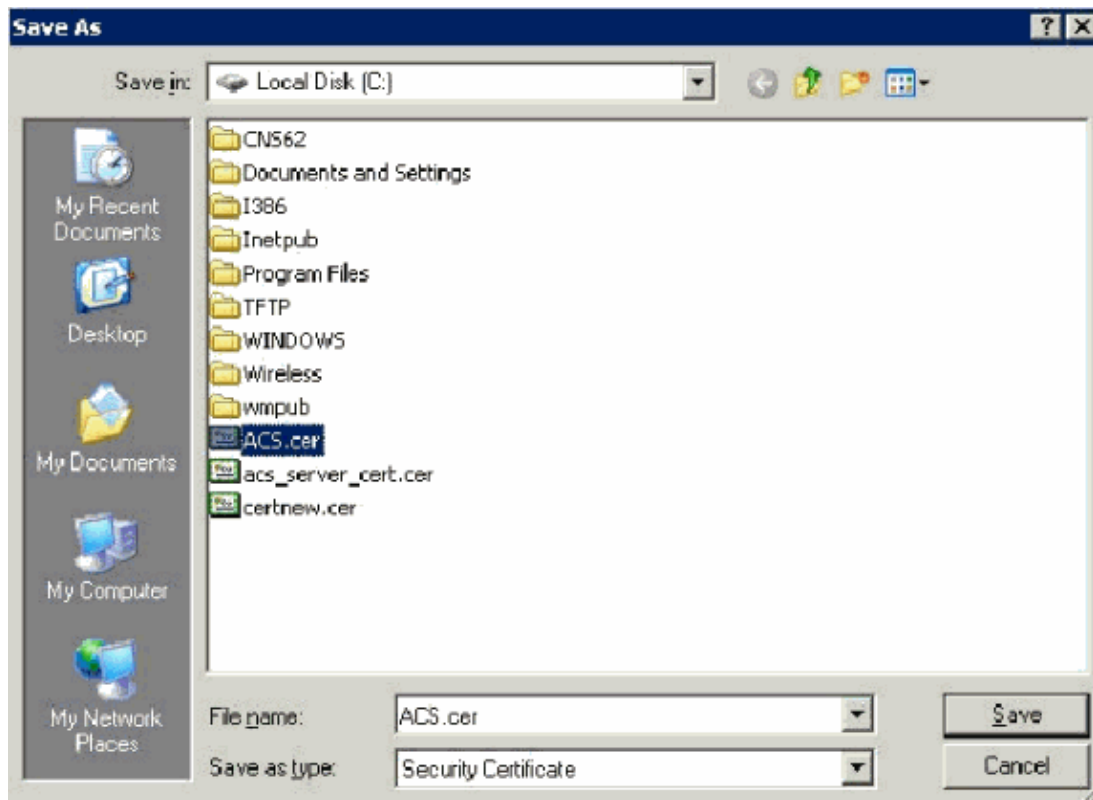
- On the ACS server (cisco_w2003 in this example), point the browser at the Microsoft CA server to **http://172.16.100.26 /certsrv**.
- From the Select a Task option choose **Download a CA certificate, certificate chain or CRL**.
- Choose the **Base 64** radio encoding method and click **Download CA Certificate**.



4. A File Download Security Warning window appears. Click **Save**.

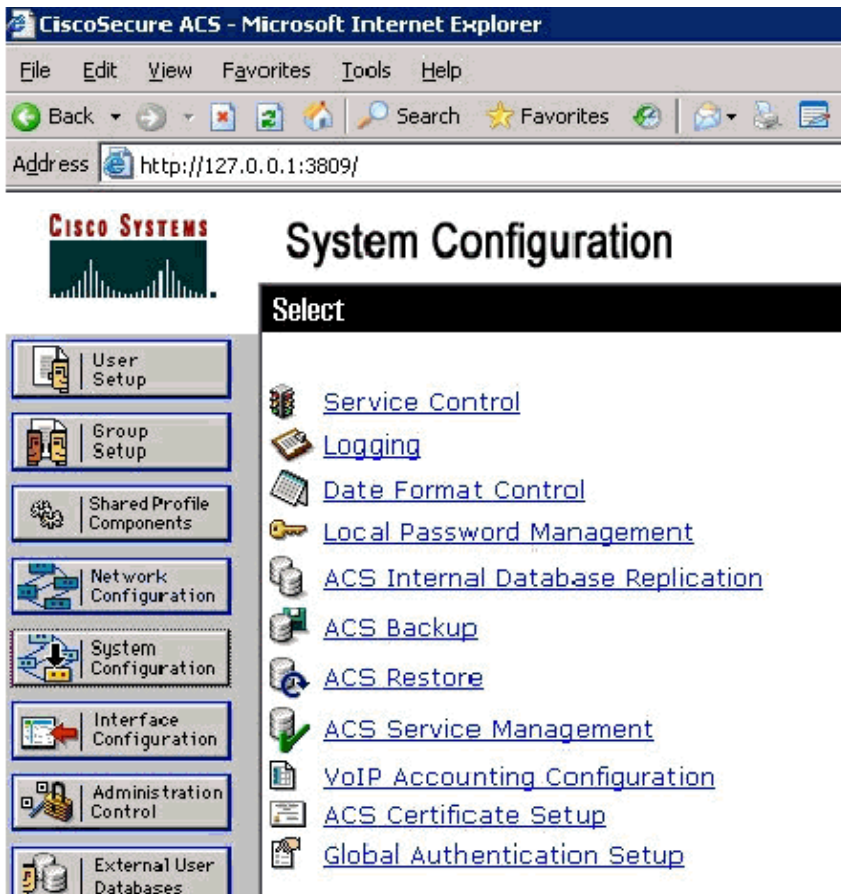


5. Save the file with a name such as ACS.cer or any name that you wish. Remember this name since you use it during the ACS Certificate Authority setup in ACS 4.0.



6. Open **ACS Admin** from the desktop shortcut created during the installation.

7. Click **System Configuration**.



8. Click **ACS Certificate Setup**.




9. Click **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. Choose **Use certificate from storage** and type in the fully qualified domain name of **cisco_w2003.wirelessdemo.local** (or **ACS.wirelessdemo.local** if you used ACS as the name).

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

11. Click **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. Click **System Configuration**.
13. Click **Service Control** and then click **Restart**.

System Configuration

Select

CiscoSecure ACS on cisco_w2003 
Is Currently Running


Services Log File Configuration 
Level of detail <input type="radio"/> None <input checked="" type="radio"/> Low <input type="radio"/> Full
Generate New File <input checked="" type="radio"/> Every day <input type="radio"/> Every week <input type="radio"/> Every month <input type="radio"/> When size is greater than <input type="text" value="2048"/> KB
<input type="checkbox"/> Manage Directory <input type="radio"/> Keep only the last <input type="text" value="7"/> files <input checked="" type="radio"/> Delete files older than <input type="text" value="7"/> days

 [Back to Help](#)

14. Click **System Configuration**.
15. Click **Global Authentication Setup**.
16. Check **Allow EAP-TLS** and all the boxes underneath it.

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):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

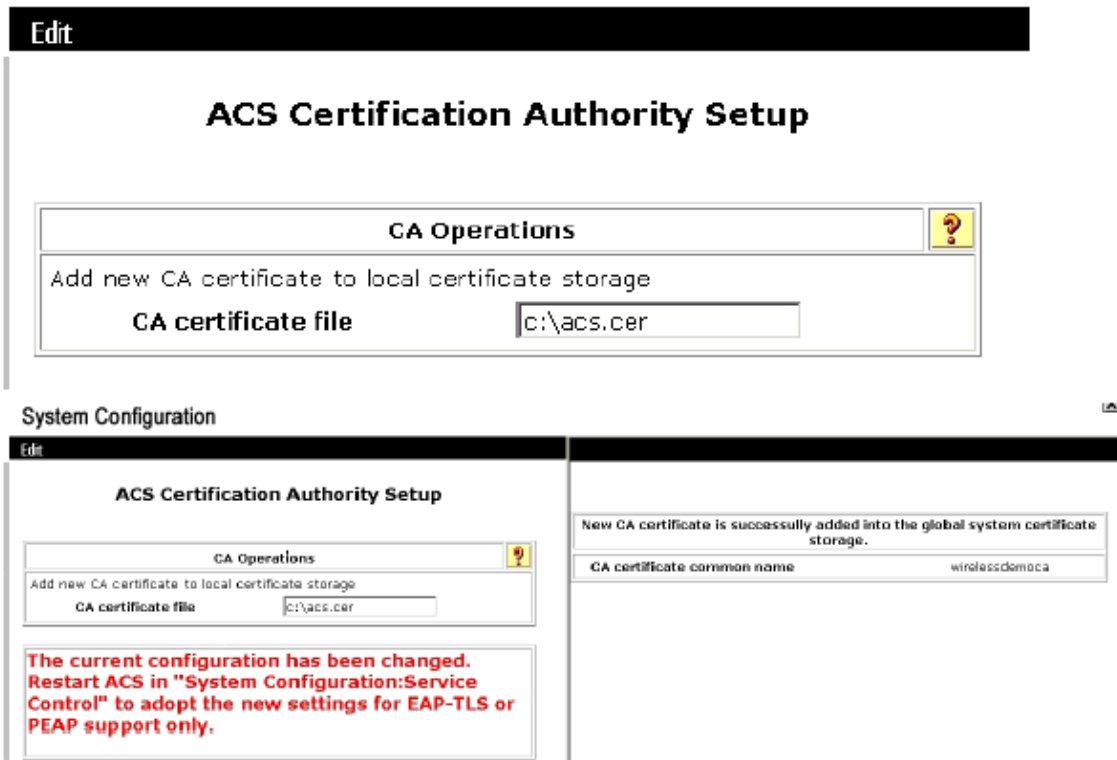
Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

17. Click **Submit + Restart**.
18. Click **System Configuration**.
19. Click **ACS Certification Authority Setup**.
20. Under the ACS Certification Authority Setup window, type the name and location of the *.cer file created earlier. In this example, the *.cer file created is **ACS.cer** in the root directory c:\.
21. Type **c:\acs.cer** in the CA certificate file field and click **Submit**.

System Configuration



The screenshot shows the 'ACS Certification Authority Setup' window. At the top, there is a black bar with the word 'Edit' in white. Below this, the title 'ACS Certification Authority Setup' is centered. A section titled 'CA Operations' contains a text box with the label 'CA certificate file' and the value 'c:\acs.cer'. A yellow help icon is visible in the top right corner of this section. Below the main window, a smaller version of the same window is shown, but with a red message box overlaid: '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.' To the right of this smaller window, a status message reads: 'New CA certificate is successfully added into the global system certificate storage.' Below this message is a table with two columns: 'CA certificate common name' and 'wirelessdemo.ca'.

22. Restart the ACS service.

CLIENT Configuration for EAP-TLS using Windows Zero Touch

CLIENT is a computer that runs Windows XP Professional with SP2 that acts as a wireless client and obtains access to Intranet resources through the wireless AP. Complete the procedures in this section in order to configure CLIENT as a wireless client.

Perform a Basic Installation and Configuration

Complete these steps:

1. Connect CLIENT to the Intranet network segment using an Ethernet cable connected to the switch.
2. On CLIENT, install Windows XP Professional with SP2 as a member computer named **CLIENT** on the wirelessdemo.local domain.
3. Install Windows XP Professional with SP2. This must be installed in order to have EAP-TLS and PEAP support.

Note: Windows Firewall is automatically turned on in Windows XP Professional with SP2. Do not turn the firewall off.

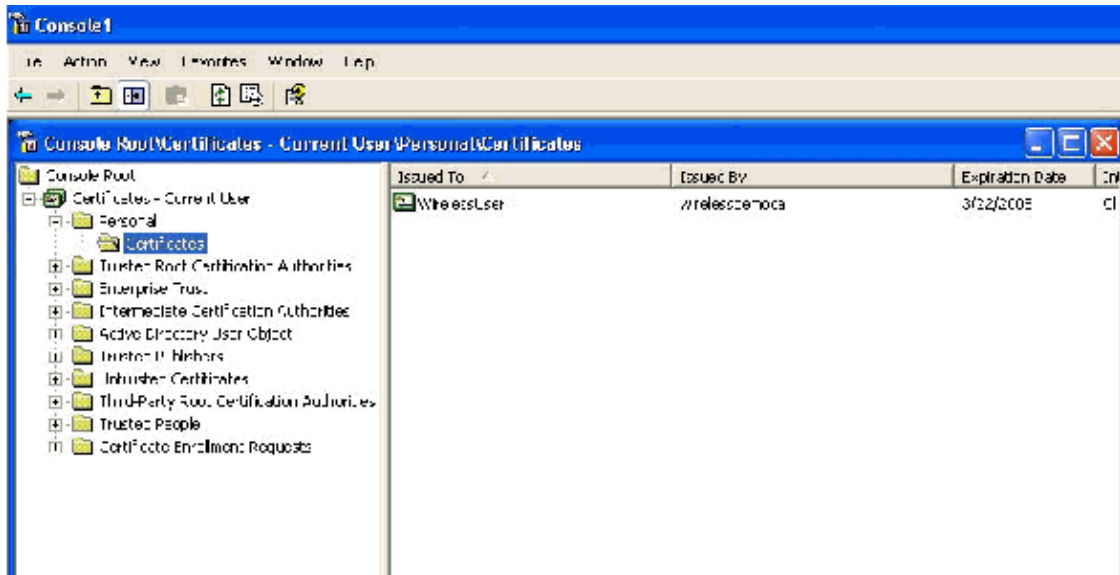
Configure the Wireless Network Connection

Complete these steps:

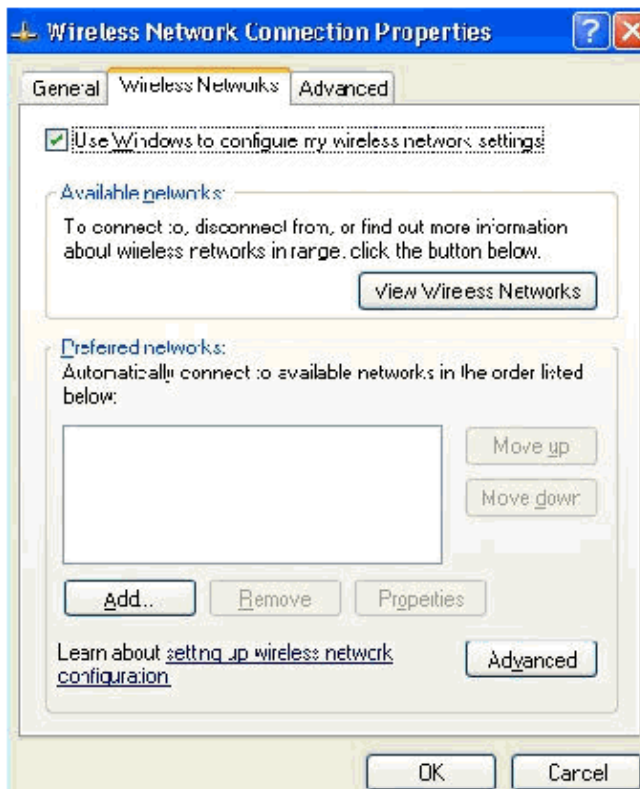
1. Log off and then log on by using the WirelessUser account in the wirelessdemo.local domain.

Note: Update computer and user configuration group policy settings and obtain a computer and user certificate for the wireless client computer immediately, by typing **gpupdate** at a command prompt. Otherwise, when you log off and then log on, it performs the same function as **gpupdate**. You must be logged on to the domain by connecting over the wire.

Note: In order to validate that the certificate is automatically installed on the client, open the certificate MMC and validate that the WirelessUser certificate is available in the Personal Certificates folder.

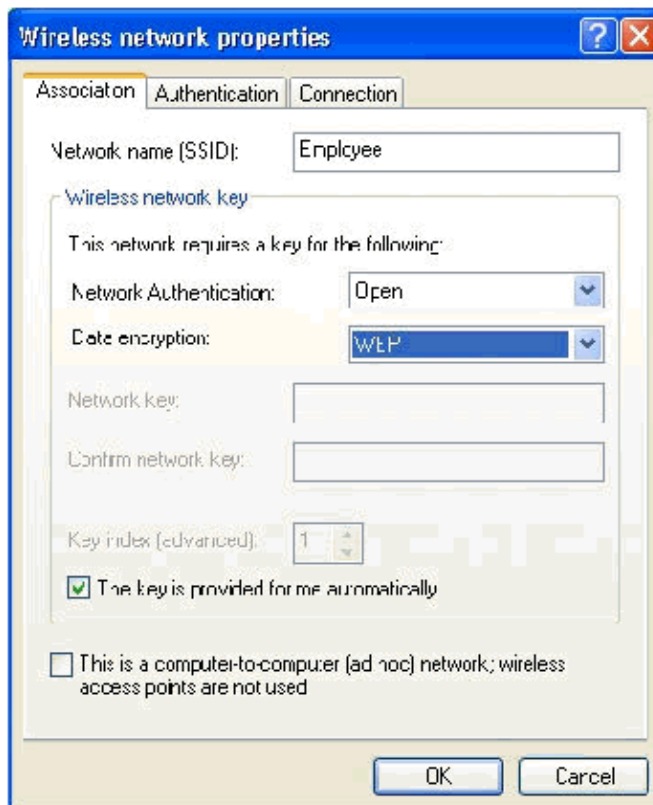


2. Choose **Start > Control Panel**, double-click **Network Connections**, and then right-click **Wireless Network Connection**.
3. Click **Properties**, go to the **Wireless Networks** tab, and ensure that **User Windows to configure my wireless network settings** is checked.

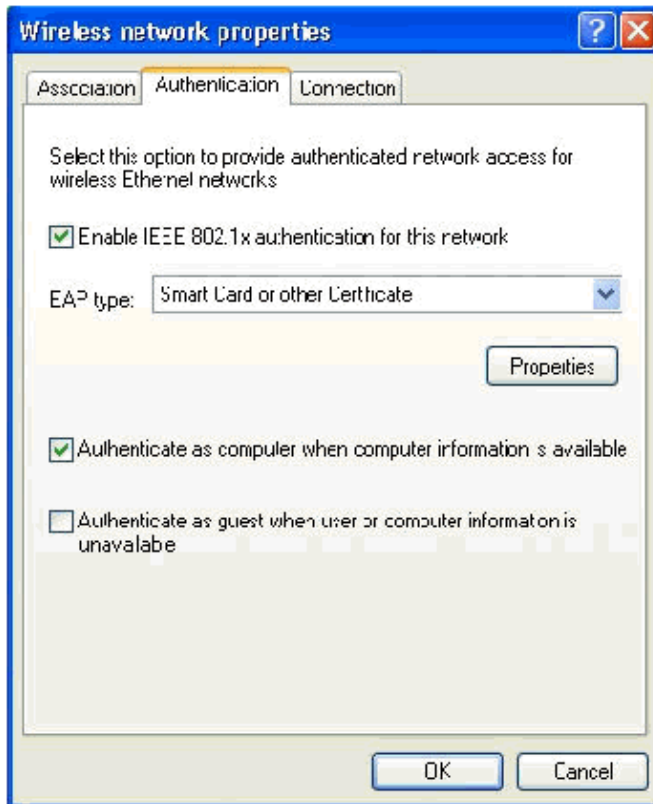


4. Click **Add**.

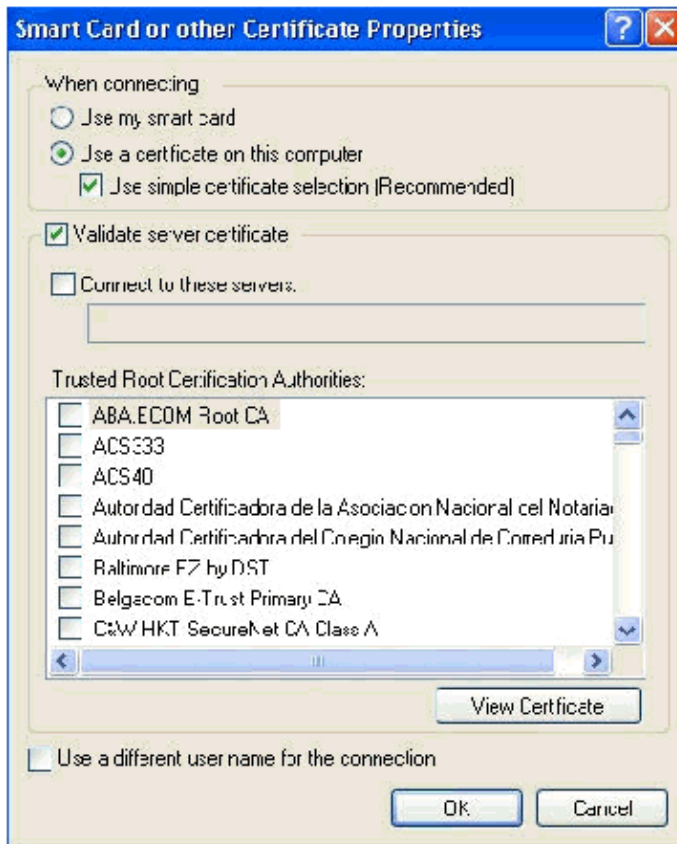
5. Go to the Association tab, and type **Employee** in the Network name (SSID) field.
6. Ensure that Data Encryption is set to **WEP** and **The key is provided for me automatically** is checked.



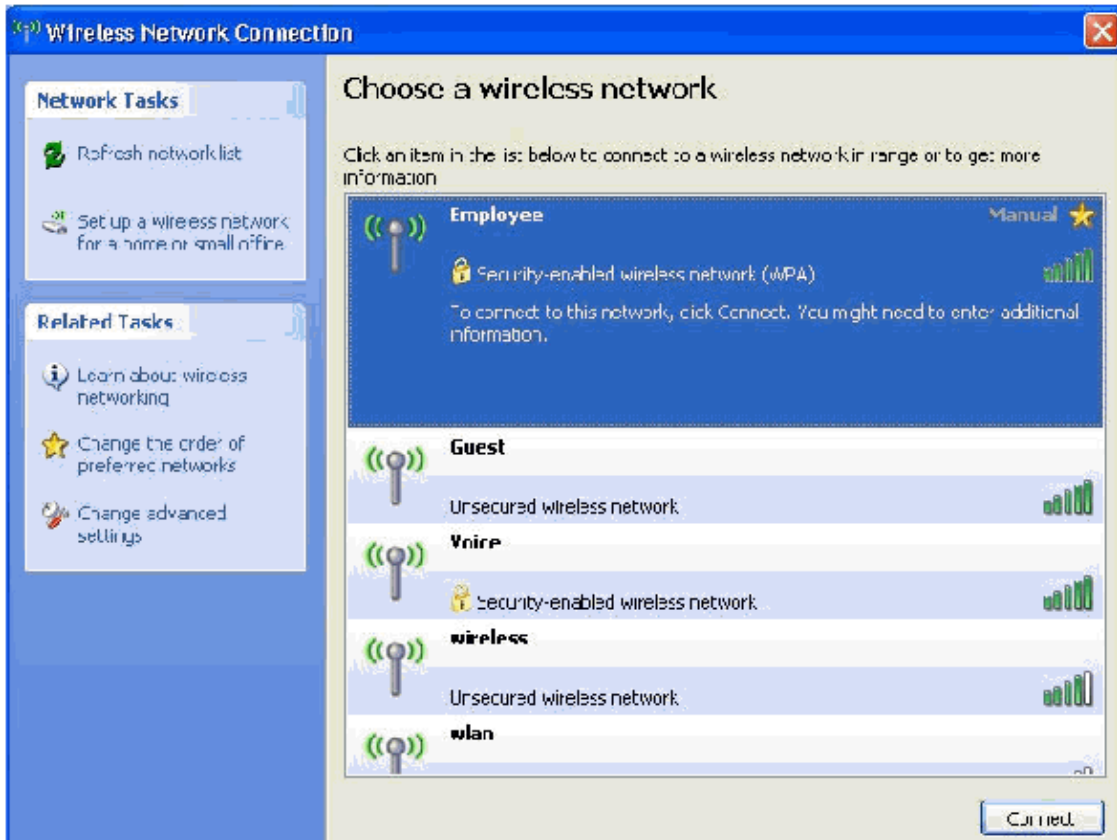
7. Go to the Authentication tab.
8. Validate that EAP type is configured to use **Smart Card or other Certificate**. If it is not, select it from the drop-down menu.
9. If you want the machine to be authenticated prior to login (which allows login scripts or group policy pushes to be applied) choose the option **Authenticate as computer when computer information is available**.



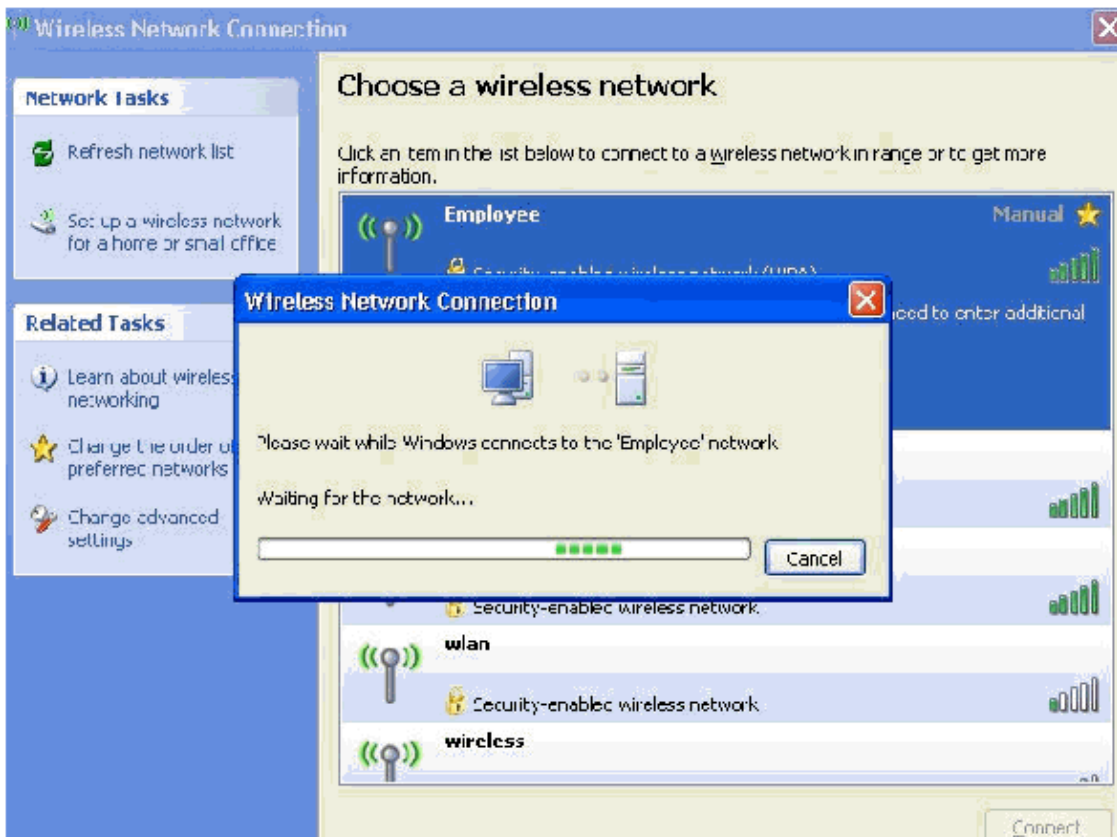
10. Click **Properties**.
11. Ensure that the boxes in this window are checked.

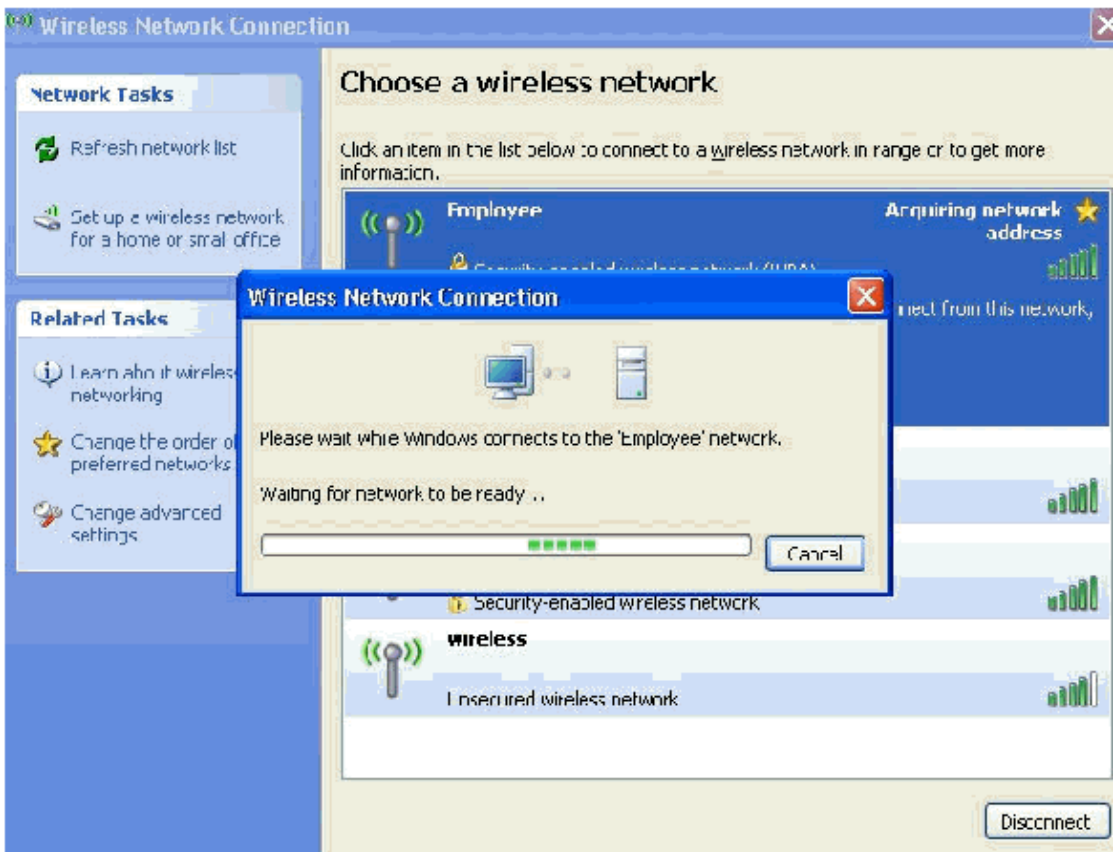
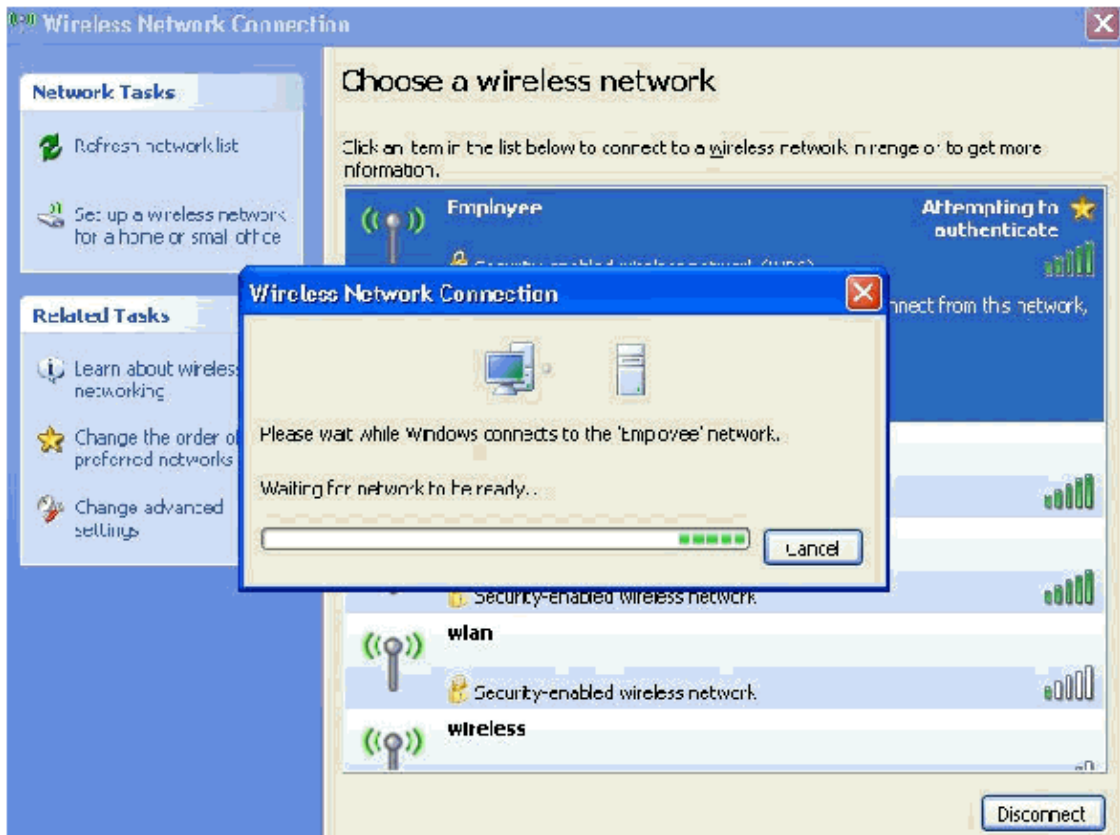


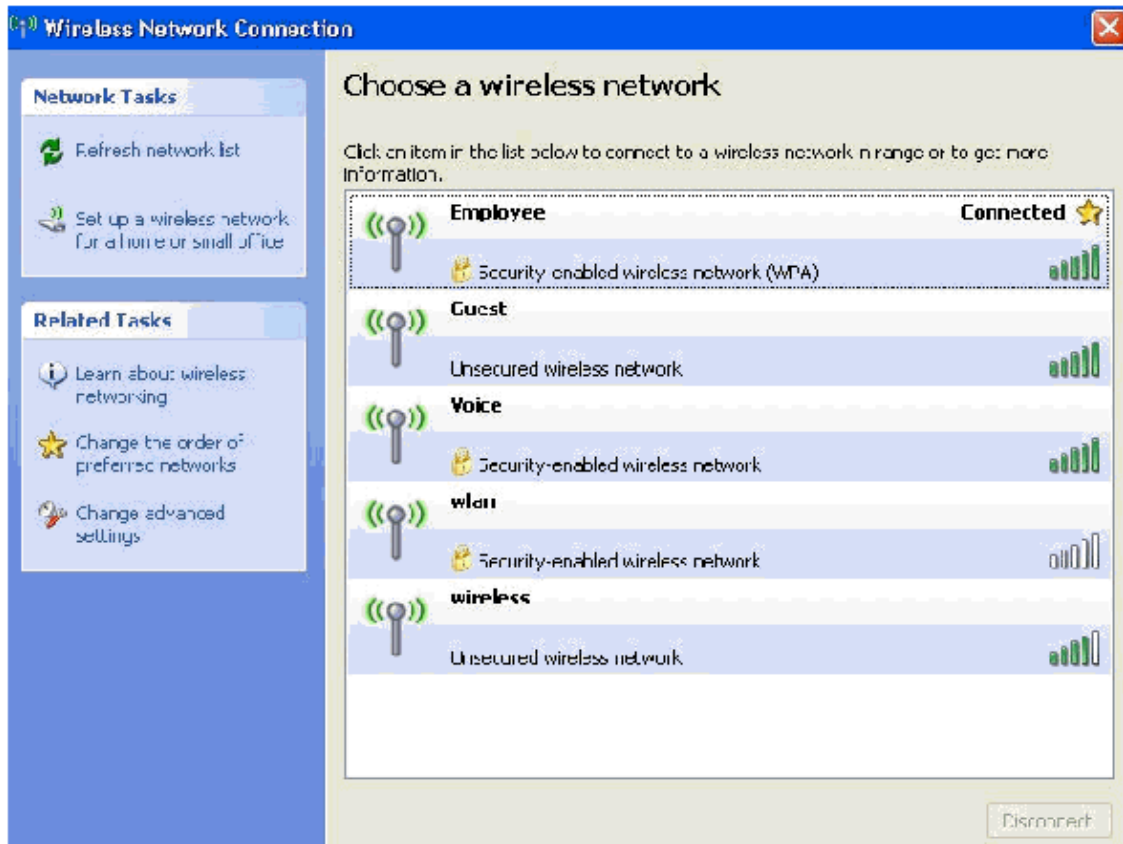
12. Click **OK** three times.
13. Right-click the wireless network connection icon in systray and then click **View Available Wireless Networks**.
14. Click the **Employee** wireless network and click **Connect**.



These screen shots indicate if the connection completes successfully.







15. After the authentication is successful, check the TCP/IP configuration for the wireless adapter by using Network Connections. It should have an address range of 172.16.100.100–172.16.100.254 from the DHCP scope or the scope created for the wireless clients.
16. In order to test functionality, open up a browser and browse to <http://wirelessdemoca> (or the IP address of the Enterprise CA server).

Related Information

- [EAP Authentication with WLAN Controllers \(WLC\) Configuration Example](#)
- [Wireless LAN Controller Configuration Guide](#)
- [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
- [VLANs on Wireless LAN Controllers Configuration Example](#)
- [AP Group VLANs with wireless LAN Controllers Configuration Example](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 04, 2008

Document ID: 71929
