

# EAP-TLS en Unified Wireless Network con ACS 4.0 y Windows 2003

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Configuración de Windows Enterprise 2003 con IIS, autoridad certificadora, DNS, DHCP \(DC CA\) DC CA \(alámbrico democa\)](#)

[Configuración de Windows Standard 2003 con Cisco Secure ACS 4.0](#)

[Instalación y configuración básicas](#)

[Instalación de Cisco Secure ACS 4.0](#)

[Configuración del controlador LWAPP de Cisco](#)

[Crear la configuración necesaria para WPA2/WPA](#)

[Autenticación EAP-TLS](#)

[Instalación del complemento Plantillas de certificado](#)

[Creación de la Plantilla de Certificado para el Servidor Web ACS](#)

[Habilitación de la Nueva Plantilla de Certificado de Servidor Web ACS](#)

[Configuración de certificados ACS 4.0](#)

[Configuración del Certificado Exportable para ACS](#)

[Instalación del certificado en el software ACS 4.0](#)

[Configuración del CLIENTE para EAP-TLS con Windows Zero Touch](#)

[Realizar una Instalación y Configuración Básicas](#)

[Configuración de la conexión de red inalámbrica](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar el acceso inalámbrico seguro mediante controladores de LAN inalámbrica (WLC), software Microsoft Windows 2003 y Cisco Secure Access Control Server (ACS) 4.0 a través del protocolo de autenticación extensible - seguridad de capa de transporte (EAP-TLS).

**Nota:** Para obtener más información sobre la implementación de tecnología inalámbrica segura, refiérase al [sitio Web Wi-Fi de Microsoft y Cisco SAFE Wireless Blueprint](#).

## Prerequisites

## Requirements

Se supone que el instalador tiene conocimiento de la instalación básica de Windows 2003 y de la instalación del controlador de Cisco, ya que este documento sólo cubre las configuraciones específicas para facilitar las pruebas.

Para obtener información de configuración e instalación inicial para los Cisco 4400 Series Controllers, refiérase a la [Guía de Inicio Rápido: Controladores LAN inalámbricos Cisco de la serie 4400](#). Para obtener información de configuración e instalación inicial para los Cisco 2000 Series Controllers, refiérase a la [Guía de Inicio Rápido: Controladores LAN inalámbricos Cisco de la serie 2000](#).

Antes de comenzar, instale Windows Server 2003 con el sistema operativo Service Pack (SP)1 en cada uno de los servidores del laboratorio de pruebas y actualice todos los Service Packs. Instale los controladores y los AP y asegúrese de que se configuran las últimas actualizaciones de software.

**Importante:** En el momento de escribir este documento, SP1 es la última actualización de Windows Server 2003, y SP2 con parches de actualización es el software más reciente para Windows XP Professional.

Windows Server 2003 con SP1, Enterprise Edition se utiliza para que se pueda configurar la inscripción automática de certificados de usuario y estación de trabajo para la autenticación EAP-TLS. Esto se describe en la sección [Autenticación EAP-TLS](#) de este documento. La inscripción automática de certificados y la renovación automática facilitan la implementación de certificados y mejoran la seguridad al vencer y renovar certificados automáticamente.

## Componentes Utilizados

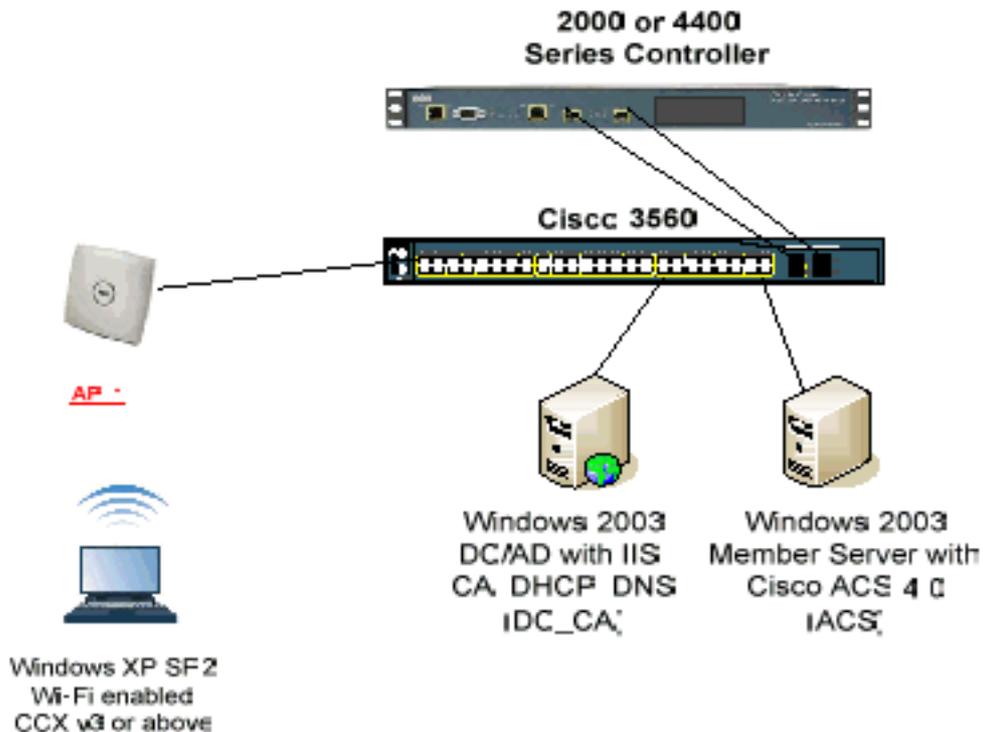
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2006 o 4400 Series Controller que ejecuta 3.2.116.21
- Punto de acceso ligero (LWAPP) Cisco 1131
- Windows 2003 Enterprise con Internet Information Server (IIS), Certificate Authority (CA), DHCP y sistema de nombres de dominio (DNS) instalado
- Windows 2003 Standard con Access Control Server (ACS) 4.0
- Windows XP Professional con SP (y Service Packs actualizados) y tarjeta de interfaz de red inalámbrica (NIC) (compatible con CCX v3) o suplicante de terceros.
- Switch Cisco 3560

## Diagrama de la red

En este documento, se utiliza esta configuración de red:

**Topología del laboratorio Cisco Secure Wireless**



El propósito principal de este documento es proporcionarle el procedimiento paso a paso para implementar EAP-TLS en Redes Inalámbricas Unificadas con ACS 4.0 y el servidor Windows 2003 Enterprise. El énfasis principal se centra en la inscripción automática del cliente de modo que el cliente se inscriba automáticamente y tome el certificado del servidor.

**Nota:** Para agregar acceso Wi-Fi protegido (WPA)/WPA2 con protocolo de integridad de clave temporal (TKIP)/estándar de cifrado avanzado (AES) a Windows XP Professional con SP, consulte la [actualización de WPA2/Elemento de información de servicios de aprovisionamiento inalámbrico \(WPS IE\) para Windows XP con 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.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## Configuración de Windows Enterprise 2003 con IIS, autoridad certificadora, DNS, DHCP (DC\_CA)

### DC\_CA (alámbrico democa)

DC\_CA es un equipo que ejecuta Windows Server 2003 con SP1, Enterprise Edition y realiza estas funciones:

- Controlador de dominio para el dominio wireless demo.local que ejecuta IIS
- Un servidor DNS para el dominio DNS local de demostración inalámbrica
- Un servidor DHCP
- CA raíz empresarial para el dominio local de demostración inalámbrica

Complete estos pasos para configurar DC\_CA para estos servicios:

1. [Realice una instalación y configuración básica.](#)
2. [Configure el equipo como controlador de dominio.](#)
3. [Aumente el nivel funcional del dominio.](#)
4. [Instale y configure DHCP.](#)
5. [Instale los servicios de certificados.](#)
6. [Verifique los permisos de administrador para los certificados.](#)
7. [Agregue ordenadores al dominio.](#)
8. [Permitir el acceso inalámbrico a los ordenadores.](#)
9. [Agregue usuarios al dominio.](#)
10. [Permitir el acceso inalámbrico a los usuarios.](#)
11. [Agregue grupos al dominio.](#)
12. [Agregue usuarios al grupo WirelessUsers.](#)
13. [Agregue los equipos cliente al grupo WirelessUsers.](#)

## Paso 1: Instalación y configuración básicas

Complete estos pasos:

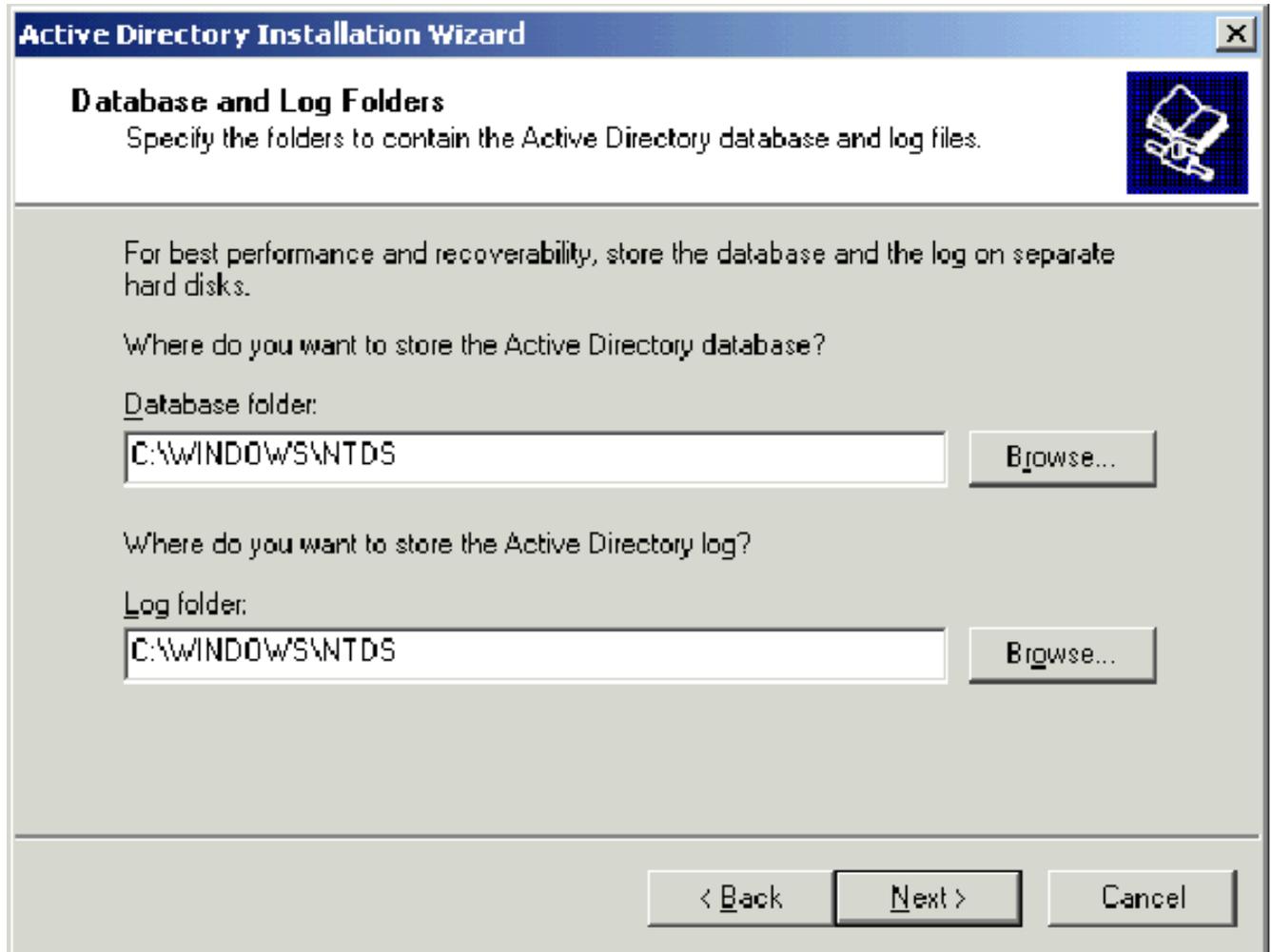
1. Instale Windows Server 2003 con SP1, Enterprise Edition como servidor independiente.
2. Configure el protocolo TCP/IP con la dirección IP 172.16.100.26 y la máscara de subred 255.255.255.0.

## Paso 2: Configuración del equipo como controlador de dominio

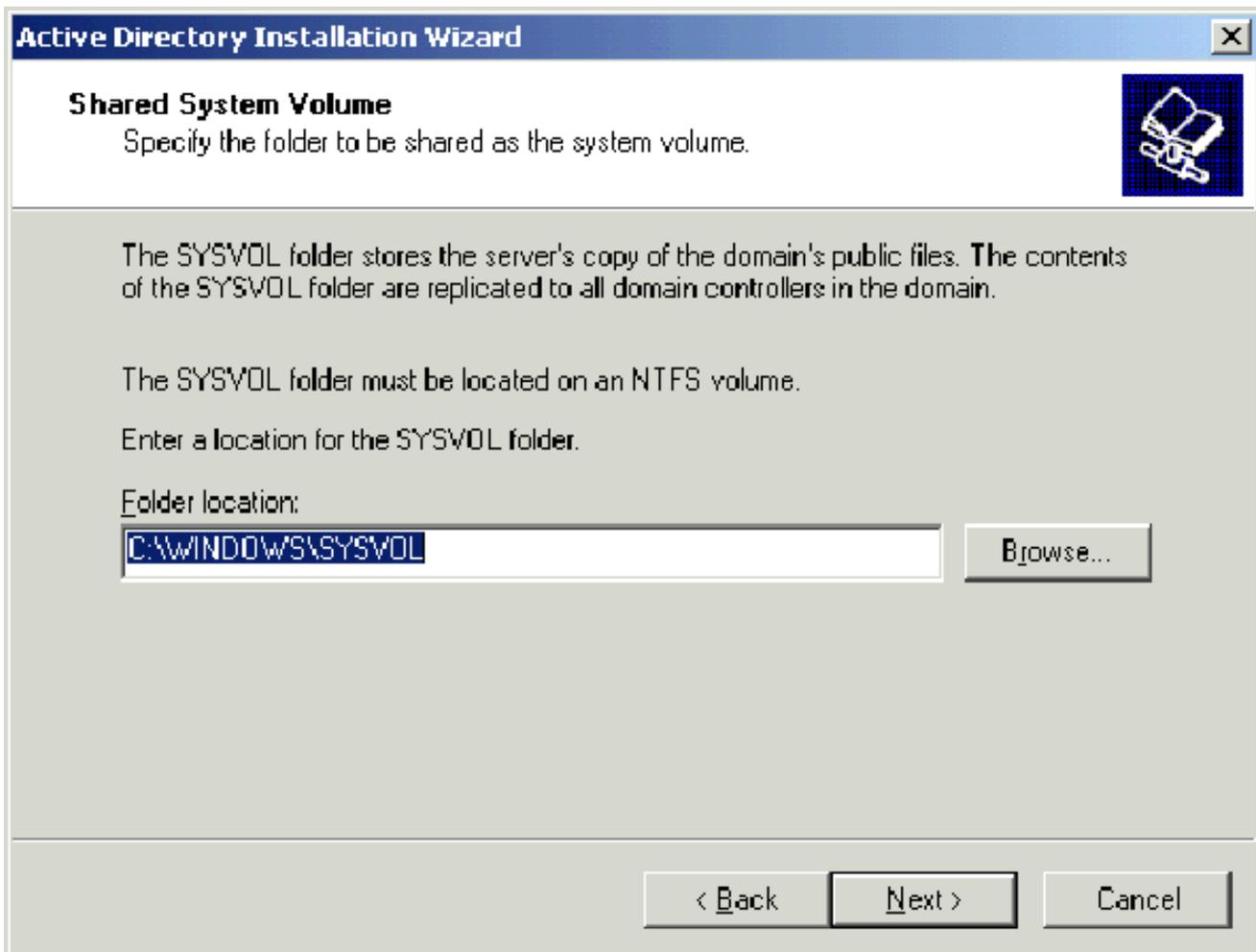
Complete estos pasos:

1. Para iniciar el asistente de instalación de Active Directory, elija **Inicio > Ejecutar**, escriba **dcpromo.exe** y haga clic en **Aceptar**.
2. En la página Welcome to the Active Directory Installation Wizard (Bienvenido al Asistente de instalación de Active Directory), haga clic en **Next**.
3. En la página Compatibilidad del sistema operativo, haga clic en **Siguiente**.
4. En la página Domain Controller Type (Tipo de controlador de dominio), seleccione **Domain controller for a new domain** y haga clic en **Next**.
5. En la página Crear nuevo dominio, seleccione **Dominio en un nuevo bosque** y haga clic en **Siguiente**.
6. En la página Install or Configure DNS (Instalar o configurar DNS), seleccione **No, simplemente instale y configure DNS en este equipo** y haga clic en **Next** (Siguiente).
7. En la página New Domain Name (Nuevo nombre de dominio), escriba **wirelessdemo.local** y haga clic en **Next**.

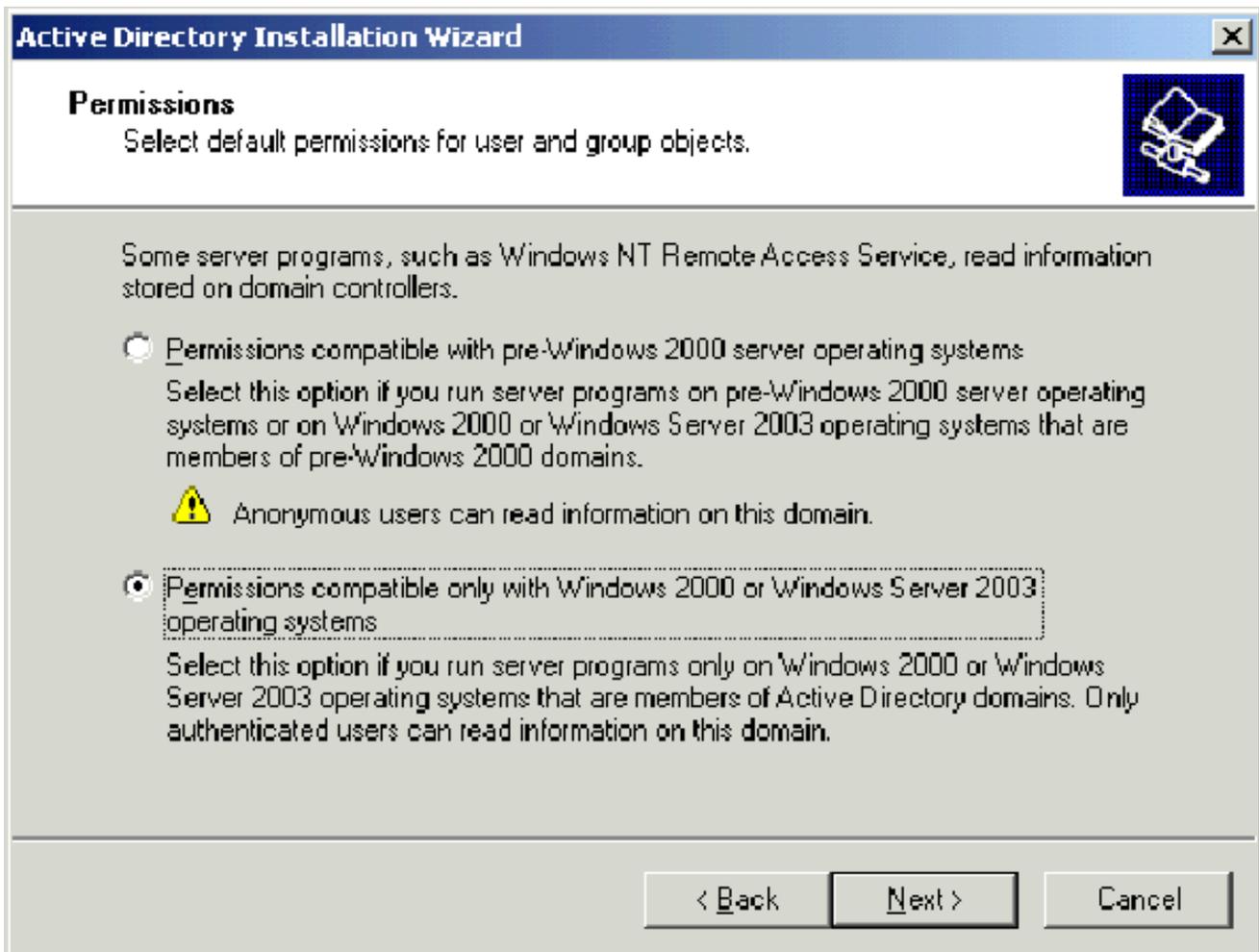
8. En la página NetBIOS Domain Name (Nombre de dominio de NetBIOS), ingrese el nombre de NetBIOS de dominio como **demostración inalámbrica** y haga clic en **Next**.
9. En la página Ubicación de la Base de Datos y las Carpetas de Registro, acepte los directorios predeterminados Database y Log Folders y haga clic en **Next**.



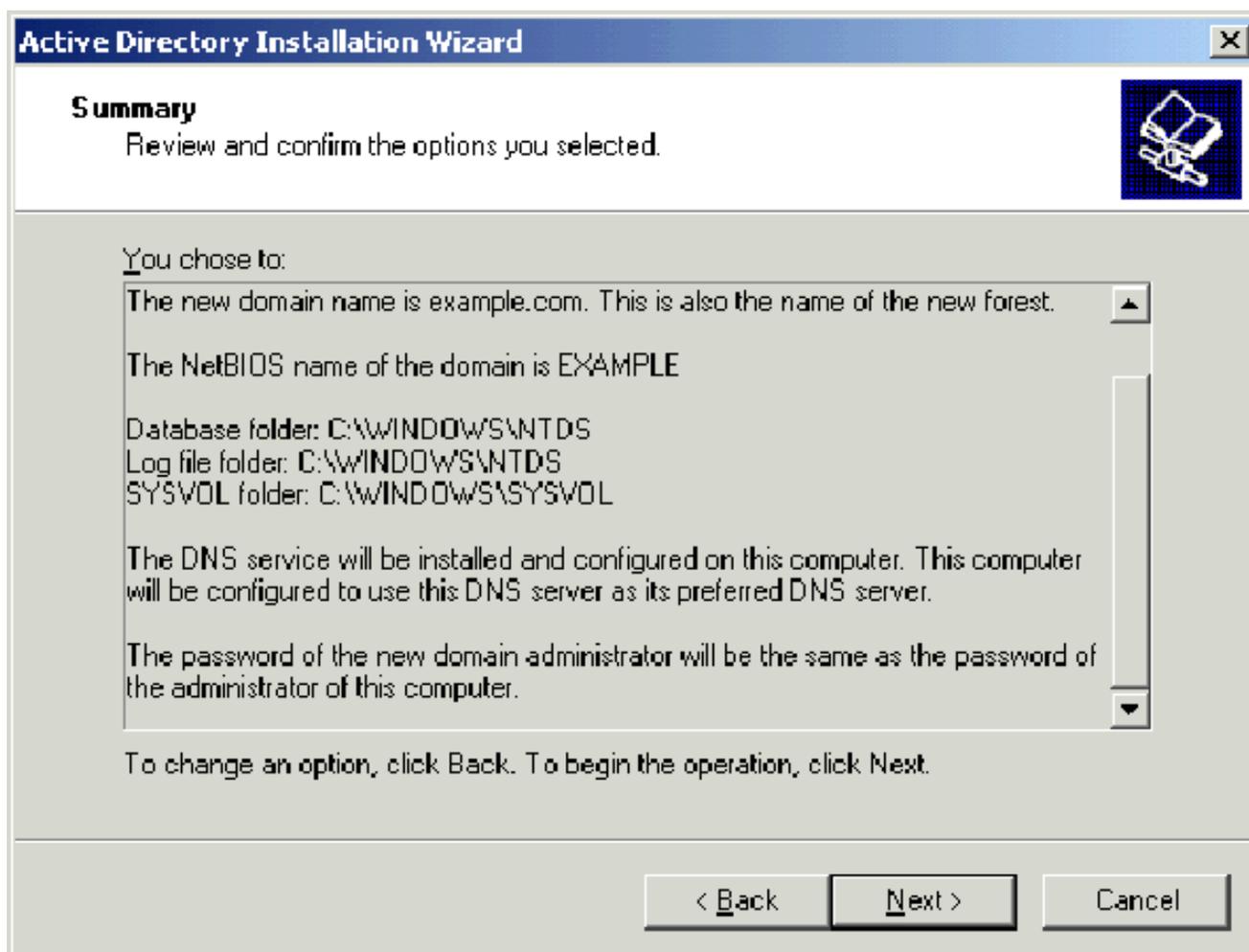
10. En el cuadro de diálogo Volumen del sistema compartido, verifique que la ubicación predeterminada de la carpeta sea correcta y haga clic en **Siguiente**.



11. En la página Permisos, verifique que **Permisos compatibles sólo con sistemas operativos Windows 2000 o Windows Server 2003** esté seleccionado y haga clic en **Siguiente**.



12. En la página Directory Services Restore Mode Administration Password, deje los cuadros de contraseña en blanco y haga clic en **Next**.
13. Revise la información de la página Resumen y haga clic en **Siguiente**.

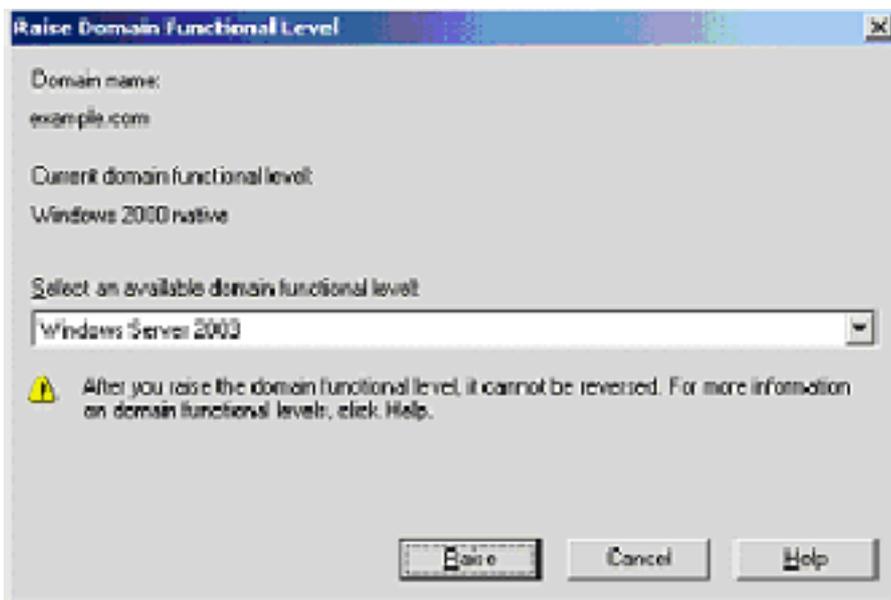


14. En la página Finalización del Asistente para instalación de Active Directory, haga clic en **Finalizar**.
15. Cuando se le solicite reiniciar el equipo, haga clic en **Reiniciar ahora**.

### [Paso 3: Elevar el nivel funcional del dominio](#)

Complete estos pasos:

1. Abra el complemento Dominios y confianza de Active Directory desde la carpeta **Herramientas administrativas (Inicio > Herramientas administrativas > Dominios y confianzas de Active Directory)** y, a continuación, haga clic con el botón derecho en el equipo de dominio **DC\_CA.wirelessdemo.local**.
2. Haga clic en **Elevar el nivel funcional del dominio** y, a continuación, seleccione **Windows Server 2003** en la página Aumentar el nivel funcional del



dominio.

3. Haga clic en **Levantar**, haga clic en **Aceptar** y, a continuación, haga clic en **Aceptar** de nuevo.

#### [Paso 4: Instalación y configuración de DHCP](#)

Complete estos pasos:

1. Instale el protocolo de configuración dinámica de host (DHCP) como componente de servicio de red mediante **Agregar o quitar programas** en el Panel de control.
2. Abra el complemento DHCP desde la carpeta Herramientas administrativas (**Inicio > Programas > Herramientas administrativas > DHCP** y, a continuación, resalte el servidor DHCP, **DC\_CA.wirelessdemo.local**).
3. Haga clic en **Acción** y luego haga clic en **Autorizar** para autorizar el servicio DHCP.
4. En el árbol de la consola, haga clic con el botón derecho del mouse en **DC\_CA.wirelessdemo.local** y, a continuación, haga clic en **Nuevo alcance**.
5. En la página de bienvenida del asistente Nuevo alcance, haga clic en **Siguiente**.
6. En la página Nombre del ámbito, escriba **CorpNet** en el campo Nombre.

## New Scope Wizard

### Scope Name

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



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

7. Haga clic en **Next** y rellene estos parámetros: Dirección IP inicial: **172.16.100.1** Dirección IP final: **172.16.100.254** Longitud: **24** Máscara de subred: **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

- Haga clic en **Next** e ingrese **172.16.100.1** para la dirección IP inicial y **172.16.100.100** para excluir la dirección IP final. Luego haga clic en Next (Siguiente). Esto reserva las direcciones IP en el rango de 172.16.100.1 a 172.16.100.100. El servidor DHCP no asigna estas direcciones IP reservadas.

## 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:

Excluded address range:

9. En la página Duración del arrendamiento, haga clic en **Siguiente**.

10. En la página Configure DHCP Options (Configurar opciones DHCP), elija **Yes (Sí), I want to configure this options now** y haga clic en **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. En la página Router (Default Gateway), agregue la dirección predeterminada del router **172.16.100.1** y haga clic en **Next**.

### 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

172.16.100.1
--------------

Remove

Up

Down

< Back

Next >

Cancel

12. En la página Nombre de dominio y Servidores DNS, escriba **wirelessdemo.local** en el campo Dominio principal, escriba **172.16.100.26** en el campo Dirección IP y, a continuación, haga clic en **Agregar** y haga clic en **Siguiente**.

## 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:

Add

Resolve

172.16.100.26

Remove

Up

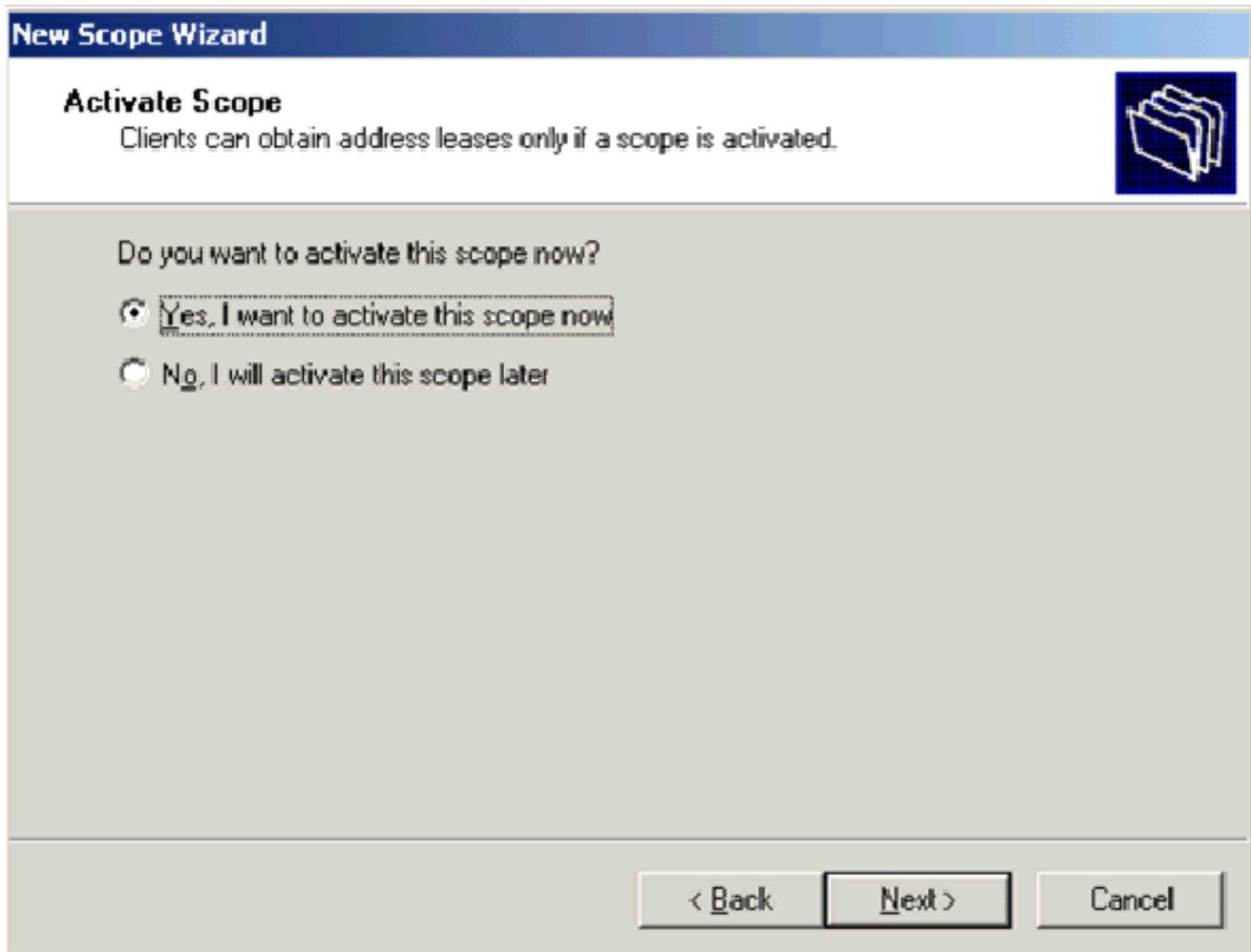
Down

< Back

Next >

Cancel

13. En la página Servidores WINS, haga clic en **Siguiente**.
14. En la página Activate Scope (Activar alcance), elija **Yes (Sí)**. Deseo activar este ámbito ahora y haga clic en **Next (Siguiente)**.



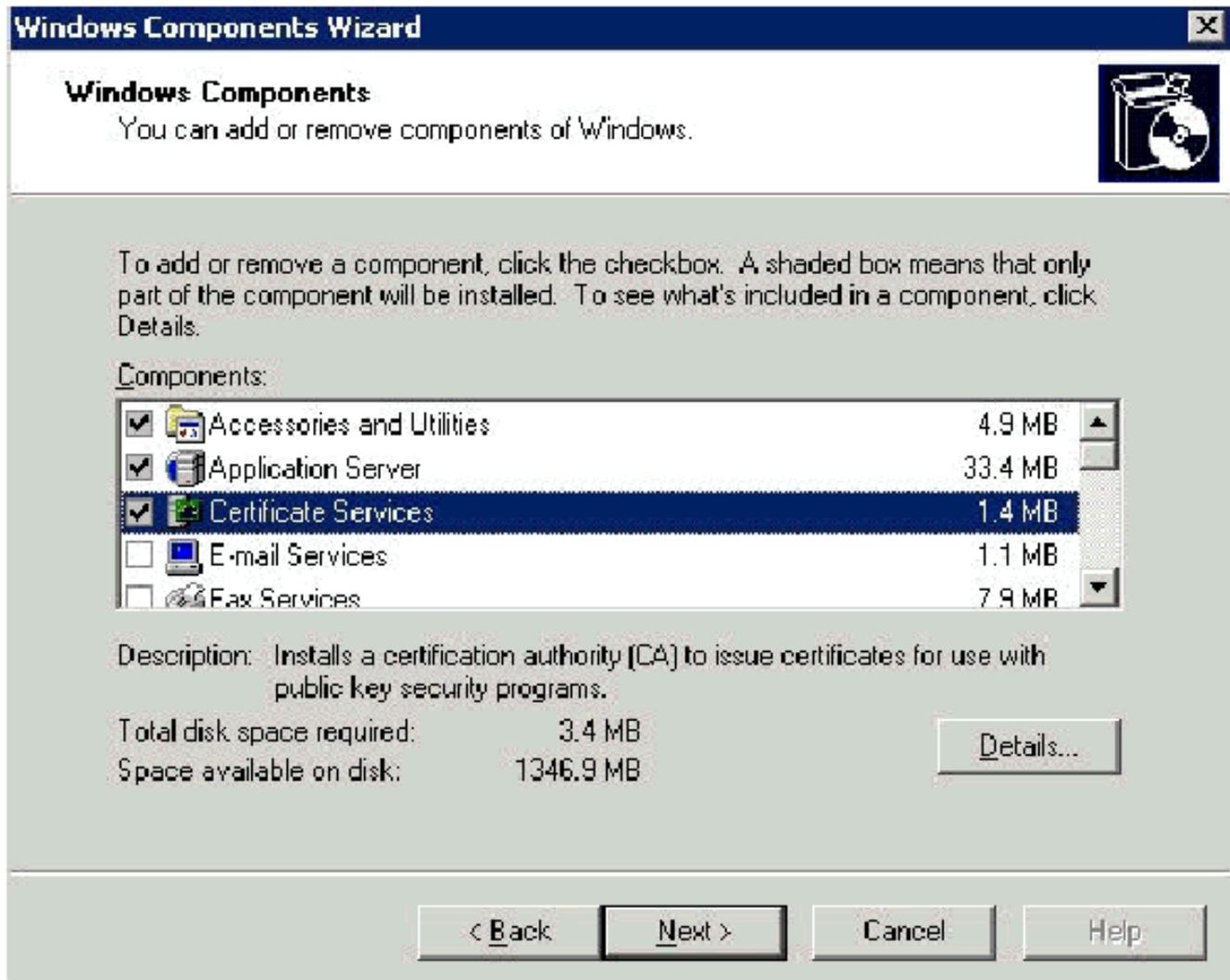
15. En la página Completar el Asistente para nuevo alcance, haga clic en **Finalizar**.

#### [Paso 5: Instalar servicios de certificados](#)

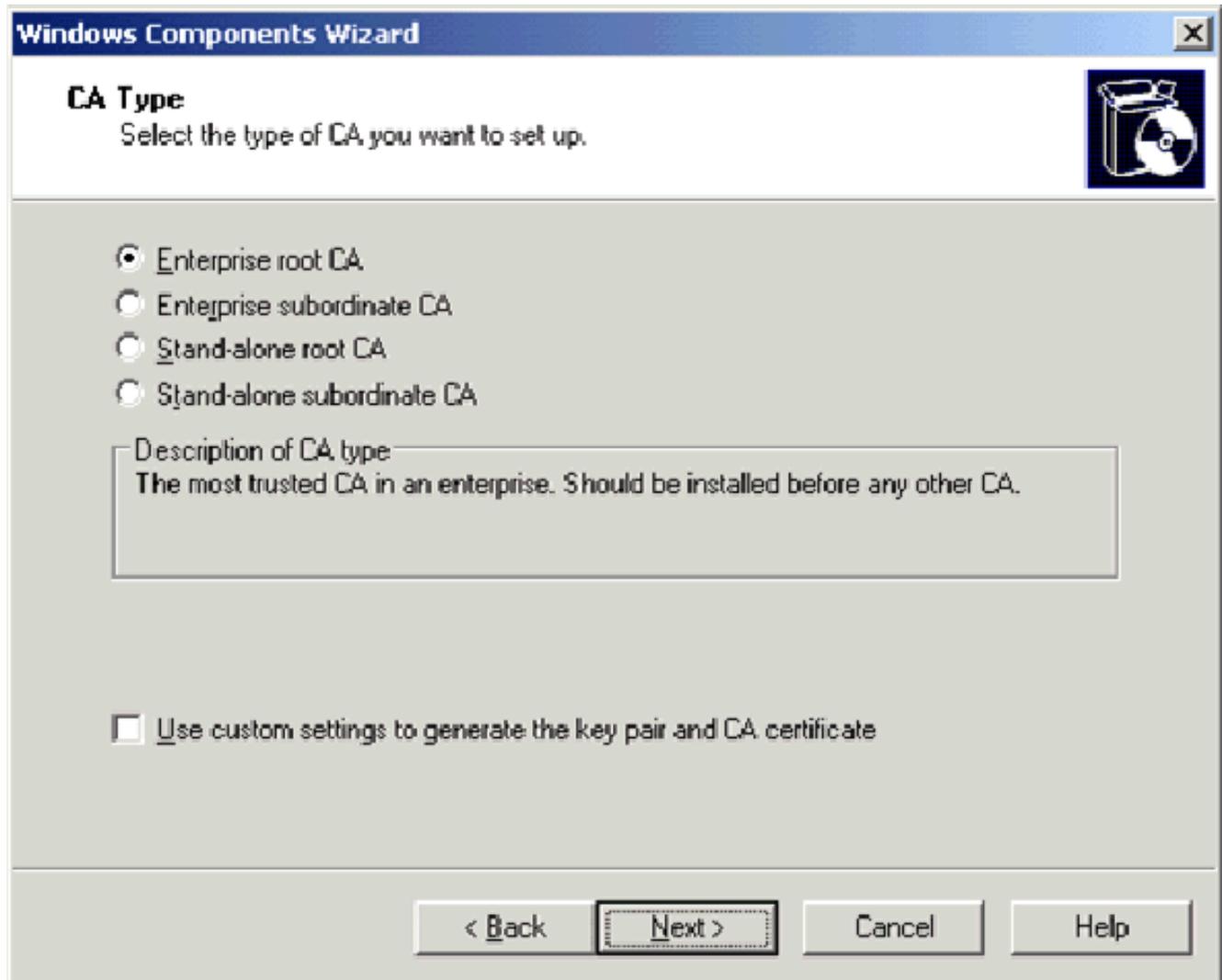
Complete estos pasos:

**Nota:** IIS debe estar instalado antes de instalar Servicios de Certificate Server y el usuario debe formar parte de la OU de Enterprise Admin.

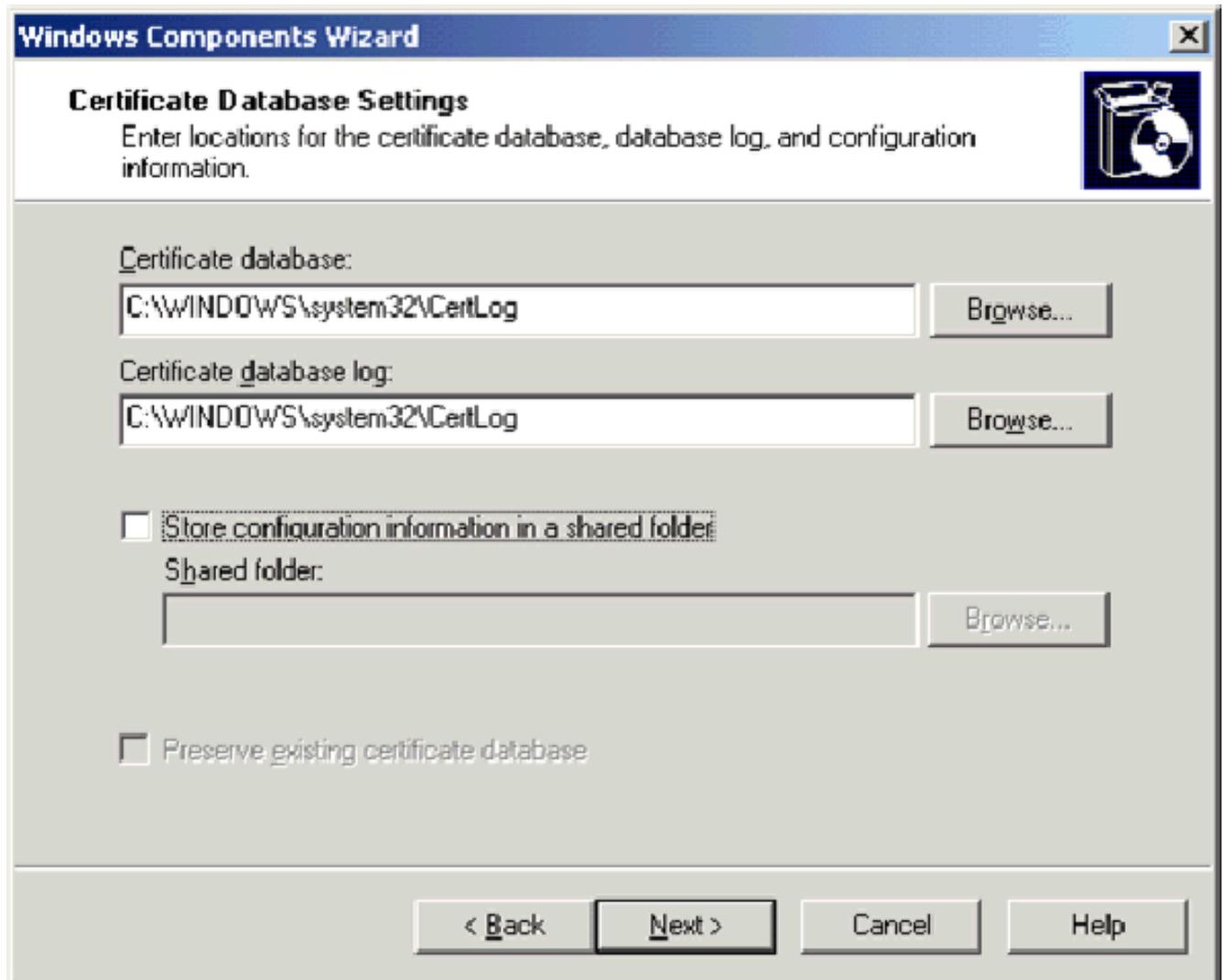
1. En el Panel de control, abra **Agregar o quitar programas** y, a continuación, haga clic en **Agregar o quitar componentes de Windows**.
2. En la página Asistente para componentes de Windows, elija **Servicios de certificados** y, a continuación, haga clic en **Siguiente**.



3. En la página CA Type , elija **Enterprise root CA** y haga clic en **Next**.



4. En la página de información de identificación de CA, escriba **wirelessdemoca** en el nombre común de este cuadro de CA. Puede introducir los demás detalles opcionales y, a continuación, hacer clic en **Siguiente**. Acepte los valores predeterminados en la página Configuración de la base de datos de certificados.

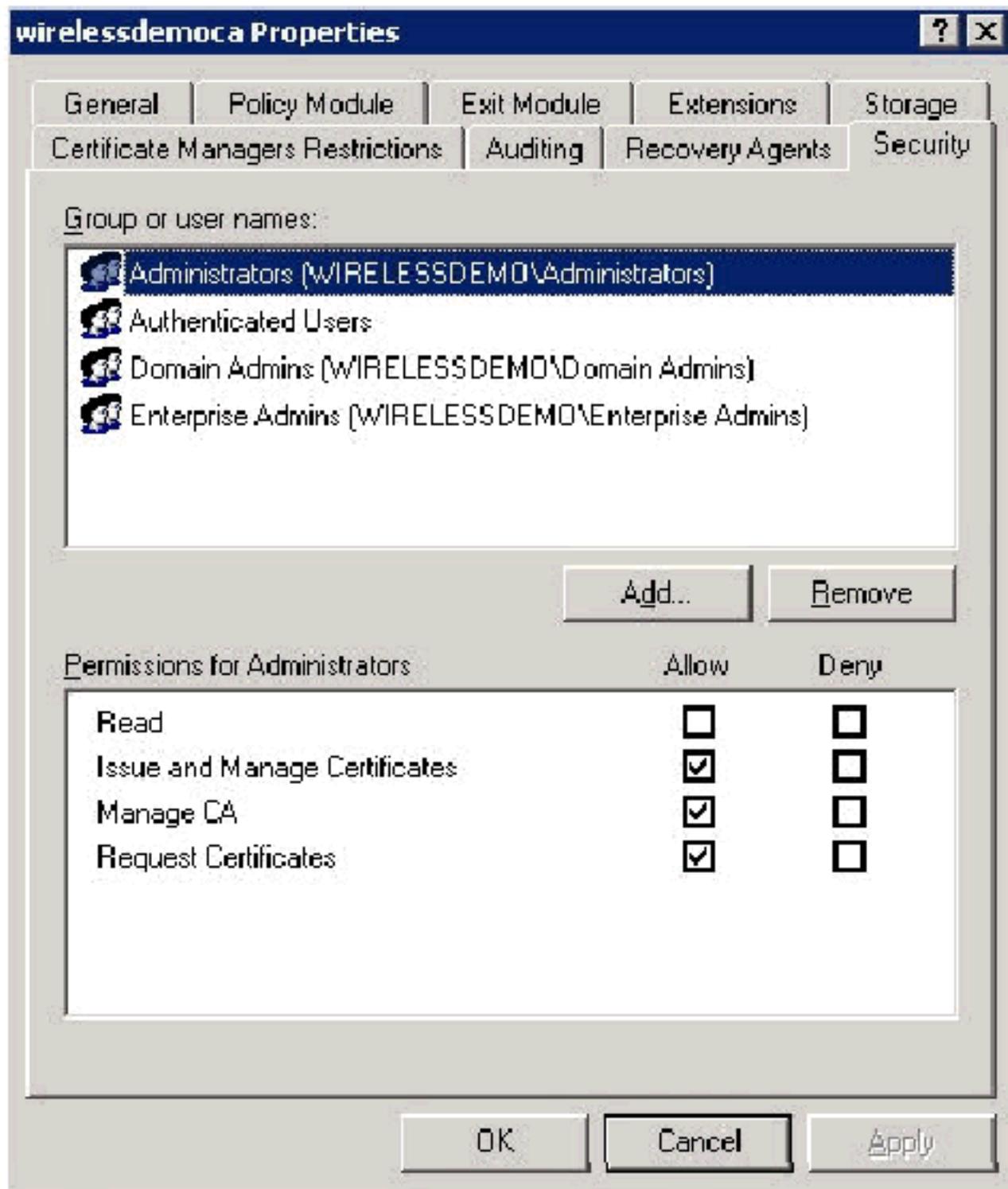


5. Haga clic en Next (Siguiente). Una vez finalizada la instalación, haga clic en **Finalizar**.
6. Haga clic en **Aceptar** después de leer la advertencia sobre la instalación de IIS.

### [Paso 6: Verificar permisos de administrador para certificados](#)

Complete estos pasos:

1. Elija **Inicio > Herramientas administrativas > Autoridad de certificación**.
2. Haga clic con el botón derecho del mouse en **Wireless-democa CA** y, a continuación, haga clic en **Propiedades**.
3. En la ficha Seguridad, haga clic en **Administradores** en la lista Grupos o Nombres de usuario.
4. En la lista Permisos o Administradores, verifique que estas opciones estén configuradas en **Permitir**: Ejecutar y administrar certificados, Administrar CA, Solicitar certificados. Si alguno de ellos está establecido en Denegar o no está seleccionado, establezca el permiso en **Permitir**.



5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Propiedades de la CA inalámbrica de democa y, a continuación, cierre la Autoridad de certificación.

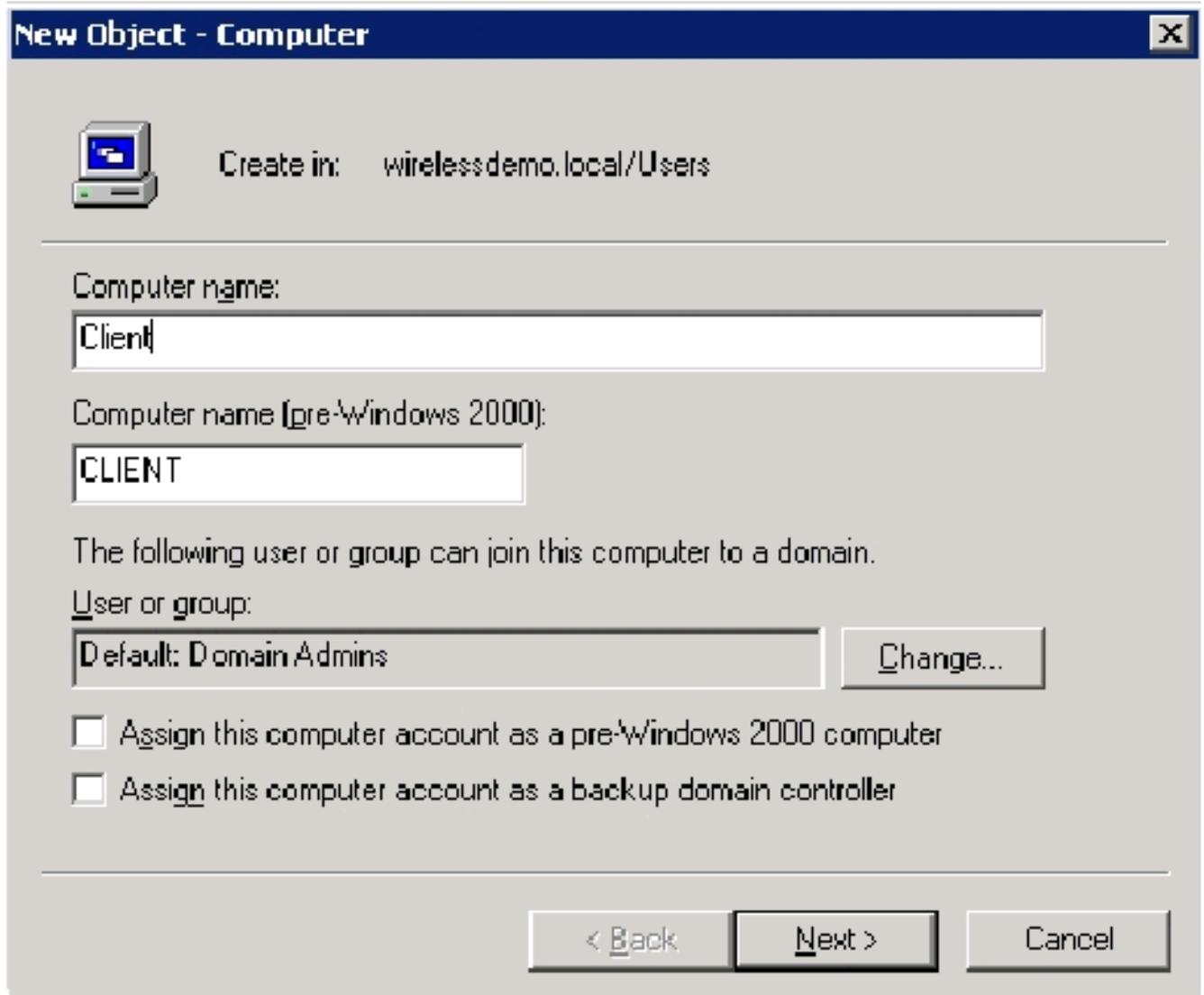
### [Paso 7: Agregar ordenadores al dominio](#)

Complete estos pasos:

**Nota:** Si el equipo ya se ha agregado al dominio, vaya a [Agregar usuarios al dominio](#).

1. Abra el complemento Usuarios y equipos de Active Directory.
2. En el árbol de la consola, expanda **wireless demo.local**.
3. Haga clic con el botón derecho del mouse en **Usuarios**, haga clic en **Nuevo** y, a continuación, haga clic en **Equipo**.

4. En el cuadro de diálogo Nuevo objeto - Equipo, escriba el nombre del equipo en el campo Nombre del equipo y haga clic en **Siguiente**. Este ejemplo utiliza el nombre de equipo **Client**.



**New Object - Computer**

Create in: wirelessdemo.local/Users

Computer name:  
Client

Computer name (pre-Windows 2000):  
CLIENT

The following user or group can join this computer to a domain.  
User or group:  
Default: Domain Admins Change...

Assign this computer account as a pre-Windows 2000 computer  
 Assign this computer account as a backup domain controller

< Back Next > Cancel

5. En el cuadro de diálogo Administrado, haga clic en **Siguiente**.  
6. En el cuadro de diálogo Nuevo equipo de objetos, haga clic en **Finalizar**.  
7. Repita los pasos 3 a 6 para crear cuentas de equipo adicionales.

### [Paso 8: Permitir el acceso inalámbrico a los ordenadores](#)

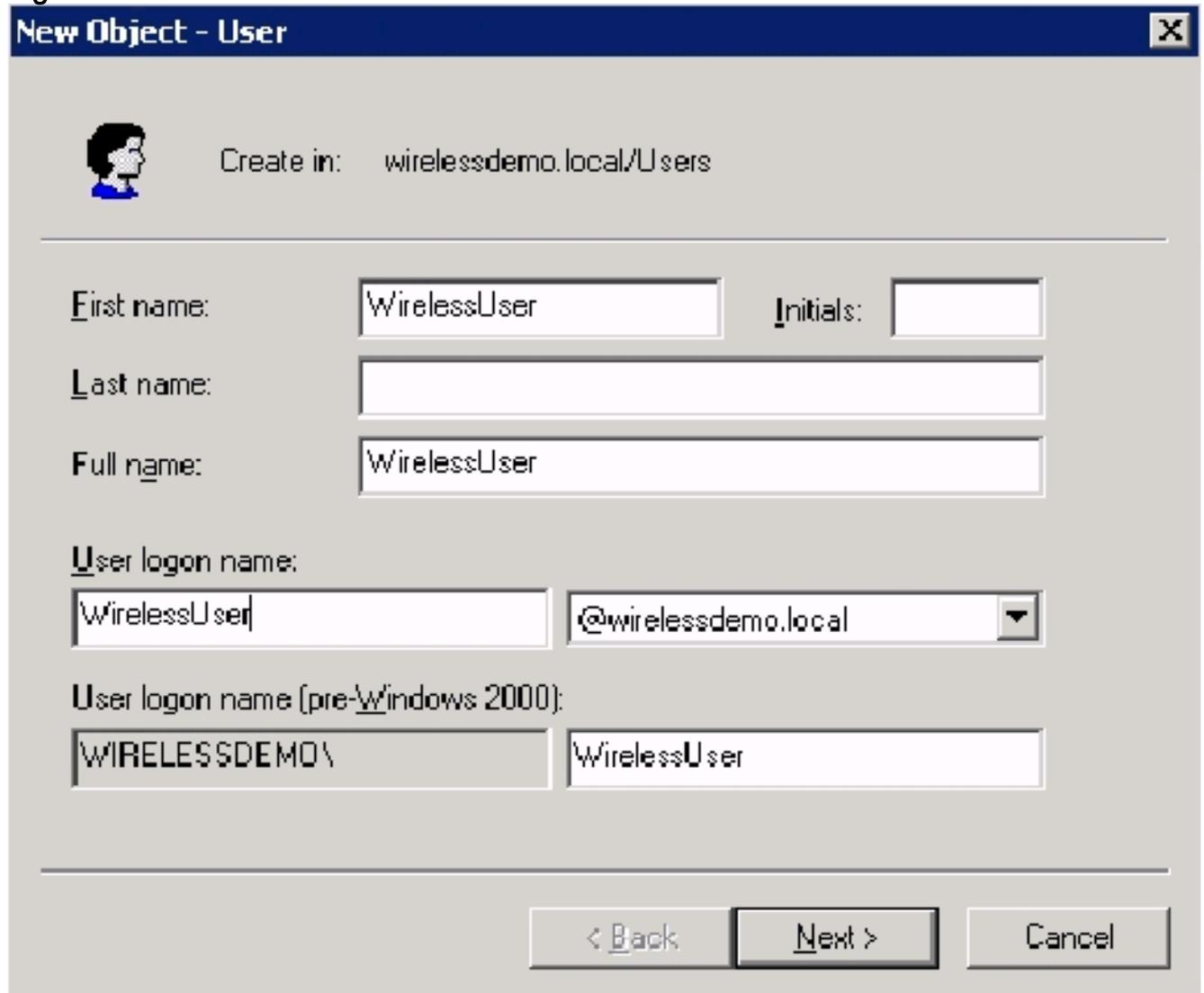
Complete estos pasos:

1. En el árbol de la consola Usuarios y equipos de Active Directory, haga clic en la carpeta **Equipos** y haga clic con el botón derecho del ratón en el equipo para el que desea asignar acceso inalámbrico. Este ejemplo muestra el procedimiento con el **CLIENTE** del equipo que agregó en el paso 7.
2. Haga clic en **Propiedades** y, a continuación, vaya a la ficha Marcar.
3. Elija **Allow access** y haga clic en **OK**.

### [Paso 9: Agregar usuarios al dominio](#)

Complete estos pasos:

1. En el árbol de la consola Usuarios y equipos de Active Directory, haga clic con el botón derecho en **Usuarios**, haga clic en **Nuevo** y, a continuación, haga clic en **Usuario**.
2. En el cuadro de diálogo Nuevo objeto - usuario, escriba **Usuario inalámbrico** en el campo Nombre, y escriba **Usuario inalámbrico** en el campo Nombre de inicio de sesión de usuario y haga clic en **Siguiente**.



**New Object - User**

Create in: wirelessdemo.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back    Next >    Cancel

3. En el cuadro de diálogo Nuevo objeto - Usuario, escriba la contraseña que desee en los campos Contraseña y Confirmar contraseña. Desactive la casilla de verificación **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** y haga clic en **Siguiente**.

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. En el cuadro de diálogo Nuevo objeto - usuario, haga clic en **Finalizar**.
5. Repita los pasos 2 a 4 para crear cuentas de usuario adicionales.

### [Paso 10: Permitir el acceso inalámbrico a los usuarios](#)

Complete estos pasos:

1. En el árbol de la consola Usuarios y equipos de Active Directory, haga clic en la carpeta **Usuarios**, haga clic con el botón derecho en **Usuario inalámbrico**, haga clic en **Propiedades** y, a continuación, vaya a la ficha **Marcar**.
2. Elija **Allow access** y haga clic en **OK**.

### [Paso 11: Agregar grupos al dominio](#)

Complete estos pasos:

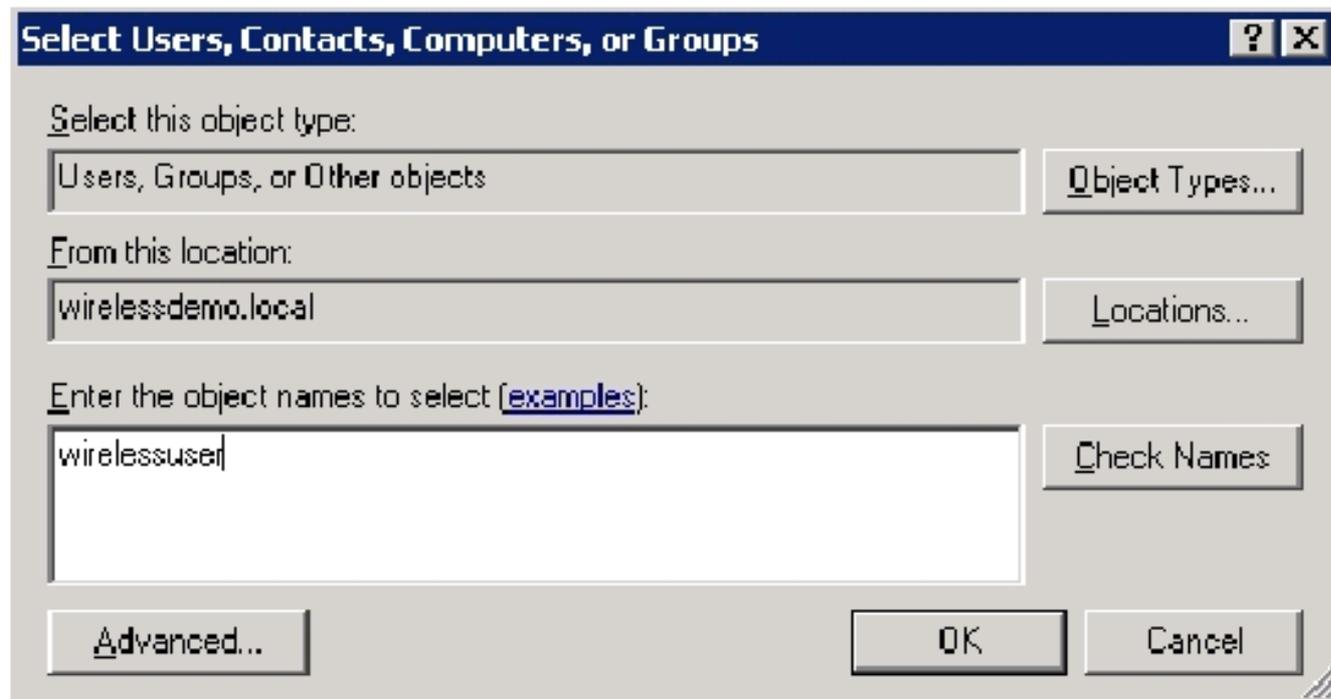
1. En el árbol de la consola Usuarios y equipos de Active Directory, haga clic con el botón derecho del mouse en **Usuarios**, haga clic en **Nuevo** y, a continuación, haga clic en **Grupo**.
2. En el cuadro de diálogo Nuevo objeto - grupo, escriba el nombre del grupo en el campo Nombre del grupo y haga clic en **Aceptar**. Este documento utiliza el nombre de grupo **WirelessUsers**.

The image shows a Windows dialog box titled "New Object - Group". At the top, it says "Create in: wirelessdemo.local/Users". Below this, there are two text input fields, both containing "WirelessUsers". The first is labeled "Group name:" and the second is labeled "Group name (pre-Windows 2000):". There are two sections with radio button options. The "Group scope" section has three options: "Domain local", "Global" (which is selected), and "Universal". The "Group type" section has two options: "Security" (which is selected) and "Distribution". At the bottom right, there are "OK" and "Cancel" buttons.

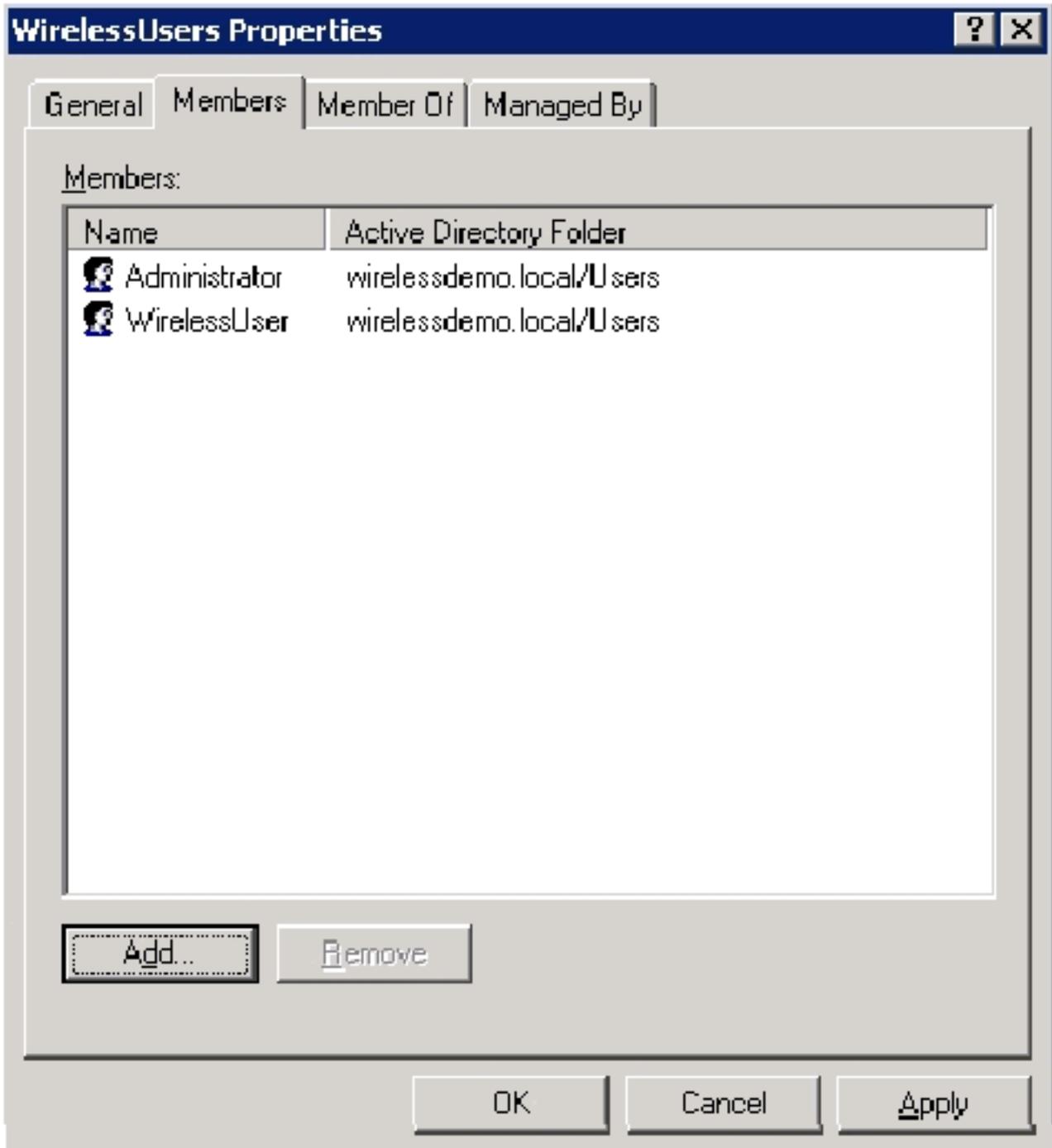
## [Paso 12: Agregar usuarios al grupo de usuarios inalámbricos](#)

Complete estos pasos:

1. En el panel de detalles de Active Directory Users and Computers, haga doble clic en Group **WirelessUsers**.
2. Vaya a la ficha Miembros y haga clic en **Agregar**.
3. En el cuadro de diálogo Seleccionar usuarios, contactos, equipos o grupos, escriba el nombre de los usuarios que desea agregar al grupo. Este ejemplo muestra cómo agregar el usuario **wireless** al grupo. Click OK.



4. En el cuadro de diálogo Varios nombres encontrados, haga clic en **Aceptar**. La cuenta de usuario WirelessUser se agrega al grupo WirelessUsers.

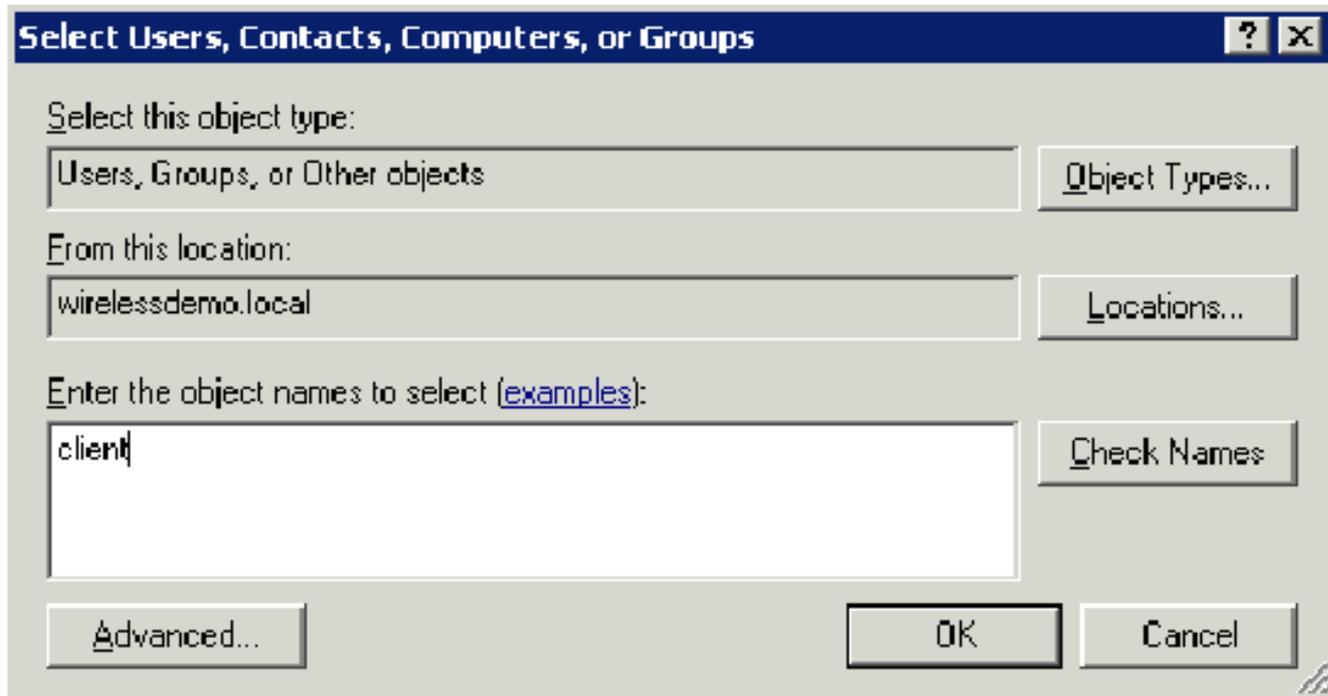


5. Haga clic en **Aceptar** para guardar los cambios en el grupo WirelessUsers.
6. Repita este procedimiento para agregar más usuarios al grupo.

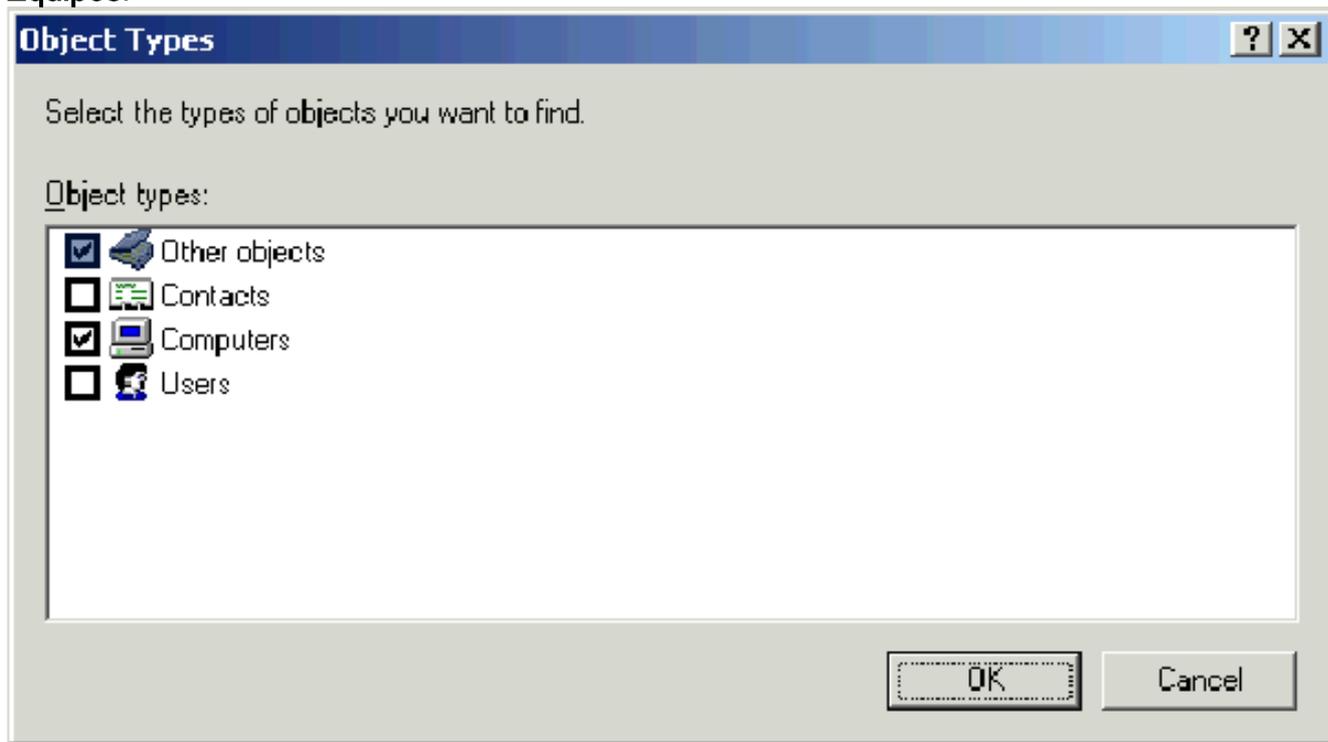
### [Paso 13: Agregar equipos cliente al grupo de usuarios inalámbricos](#)

Complete estos pasos:

1. Repita los pasos 1 y 2 en la sección [Agregar usuarios al grupo de usuarios inalámbricos](#) de este documento
2. En el cuadro de diálogo Seleccionar usuarios, contactos o equipos, escriba el nombre del equipo que desea agregar al grupo. Este ejemplo muestra cómo agregar el equipo denominado **client** al grupo.



3. Haga clic en **Tipos de objetos**, desactive la **casilla de verificación Usuarios** y, a continuación, active **Equipos**.



4. Haga clic en OK dos veces. La cuenta de equipo CLIENT se agrega al grupo WirelessUsers.
5. Repita el procedimiento para agregar más ordenadores al grupo.

## [Configuración de Windows Standard 2003 con Cisco Secure ACS 4.0](#)

Cisco Secure ACS es un equipo que ejecuta Windows Server 2003 con SP1, Standard Edition, que proporciona autenticación RADIUS y autorización para el controlador. Complete los procedimientos de esta sección para configurar el ACS como servidor RADIUS:

## Instalación y configuración básicas

Complete estos pasos:

1. Instale Windows Server 2003 con SP1, Standard Edition, como un **servidor miembro** denominado **ACS** en el dominio **wirelessdemo.local**. **Nota:** El nombre del servidor ACS aparece como cisco\_w2003 en las configuraciones restantes. Sustituya ACS o cisco\_w2003 en la configuración de laboratorio restante.
2. Para la conexión de área local, configure el protocolo TCP/IP con la dirección IP de **172.16.100.26**, la máscara de subred de **255.255.255.0** y la dirección IP del servidor DNS de **127.0.0.1**.

## Instalación de Cisco Secure ACS 4.0

**Nota:** Refiérase a la [Guía de Instalación de Cisco Secure ACS 4.0 para Windows](#) para obtener más información sobre cómo configurar Cisco Secure ACS 4.0 para Windows.

Complete estos pasos:

1. Mediante una cuenta de administrador de dominio, inicie sesión en el equipo llamado ACS a Cisco Secure ACS. **Nota:** Sólo se soportan las instalaciones realizadas en el equipo donde se instala Cisco Secure ACS. Las instalaciones remotas que se realizan con servicios de terminal de Windows o productos como Virtual Network Computing (VNC) no se han probado y no son compatibles.
2. Inserte el CD de Cisco Secure ACS en una unidad de CD-ROM del ordenador.
3. Si la unidad de CD-ROM admite la función de ejecución automática de Windows, aparece el cuadro de diálogo Cisco Secure ACS para Windows Server. **Nota:** Si el equipo no tiene instalado un Service Pack necesario, aparecerá un cuadro de diálogo. Los Service Pack de Windows se pueden aplicar antes o después de instalar Cisco Secure ACS. Puede continuar con la instalación, pero se debe aplicar el paquete de servicio necesario una vez finalizada la instalación. De lo contrario, es posible que Cisco Secure ACS no funcione de forma fiable.
4. Realice una de estas tareas: Si aparece el cuadro de diálogo Cisco Secure ACS para Windows Server, haga clic en **Install**. Si no aparece el cuadro de diálogo Cisco Secure ACS para Windows Server, ejecute **setup.exe**, ubicado en el directorio raíz del CD de Cisco Secure ACS.
5. El cuadro de diálogo Cisco Secure ACS Setup muestra el acuerdo de licencia de software.
6. Lea el acuerdo de licencia de software. Si acepta el contrato de licencia de software, haga clic en **Aceptar**. El cuadro de diálogo Bienvenido muestra información básica sobre el programa de instalación.
7. Después de leer la información en el cuadro de diálogo Bienvenido, haga clic en **Siguiente**.
8. El cuadro de diálogo Antes de empezar muestra los elementos que debe completar antes de continuar con la instalación. Si ha completado todos los elementos enumerados en el cuadro de diálogo Antes de empezar, active la casilla correspondiente para cada elemento y haga clic en **Siguiente**. **Nota:** Si no ha completado todos los elementos enumerados en el cuadro Antes de empezar, haga clic en **Cancelar** y, a continuación, haga clic en **Salir de la configuración**. Después de completar todos los elementos enumerados en el cuadro de diálogo Antes de empezar, reinicie la instalación.
9. Aparecerá el cuadro de diálogo Elegir ubicación de destino. En Carpeta de destino, aparece

la ubicación de instalación. Esta es la unidad y la ruta donde el programa de instalación instala Cisco Secure ACS.

10. Si desea cambiar la ubicación de instalación, siga estos pasos:Haga clic en **Examinar**. Aparecerá el cuadro de diálogo Elegir carpeta. El cuadro Ruta contiene la ubicación de instalación.Cambie la ubicación de instalación. Puede escribir la nueva ubicación en el cuadro Ruta o utilizar las listas Unidades y directorios para seleccionar una nueva unidad y directorio. La ubicación de instalación debe estar en una unidad local del ordenador.**Nota:** No especifique una ruta de acceso que contenga un carácter porcentual, "%". Si lo hace, puede parecer que la instalación continúa correctamente pero falla antes de que se complete.Click OK.**Nota:** Si ha especificado una carpeta que no existe, el programa de instalación muestra un cuadro de diálogo para confirmar la creación de la carpeta. Para continuar, haga clic en **Sí**.
11. En el cuadro de diálogo Elegir ubicación de destino, aparece la nueva ubicación de instalación en Carpeta de destino.
12. Haga clic en Next (Siguiete).
13. El cuadro de diálogo Configuración de la base de datos de autenticación muestra las opciones para autenticar a los usuarios. Sólo puede autenticarse con la base de datos de usuarios de Cisco Secure o también con una base de datos de usuarios de Windows.**Nota:** Después de instalar Cisco Secure ACS, puede configurar el soporte de autenticación para todos los tipos de base de datos de usuarios externos además de las bases de datos de usuarios de Windows.
14. Si sólo desea autenticar usuarios con la base de datos de usuario de Cisco Secure, elija la opción **Verificar la base de datos de Cisco Secure ACS solamente**.
15. Si desea autenticar usuarios con una base de datos de usuarios de Windows Security Access Manager (SAM) o con una base de datos de usuarios de Active Directory además de la base de datos de usuarios de Cisco Secure, realice estos pasos:Elija la opción **También verifique la base de datos de usuario de Windows**.La **casilla de verificación Sí, consulte "Conceder permiso de marcado al usuario"** vuelve a estar disponible.**Nota:** La **casilla de verificación Sí, consulte "Conceder permiso de marcado al usuario"** se aplica a todas las formas de acceso controladas por Cisco Secure ACS, no sólo al acceso de marcado. Por ejemplo, un usuario que accede a la red a través de un túnel VPN no marca en un servidor de acceso a la red. Sin embargo, si la casilla de configuración Sí, consulte "Conceder permiso de marcado al usuario" está marcada, Cisco Secure ACS aplica los permisos de marcado del usuario de Windows para determinar si se concede el acceso del usuario a la red.Si desea permitir el acceso a los usuarios autenticados por una base de datos de usuarios de dominio de Windows sólo cuando tienen permiso de marcación en su cuenta de Windows, marque el **cuadro de configuración Sí, consulte "Conceder permiso de marcado al usuario"**.
16. Haga clic en Next (Siguiete).
17. El programa de instalación instala Cisco Secure ACS y actualiza el registro de Windows.
18. El cuadro de diálogo Opciones avanzadas muestra varias funciones de Cisco Secure ACS que no están habilitadas de forma predeterminada. Para obtener más información sobre estas funciones, refiérase a la [Guía del Usuario de Cisco Secure ACS para Windows Server, Versión 4.0](#).**Nota:** Las funciones enumeradas aparecen en la interfaz HTML de Cisco Secure ACS sólo si las habilita. Después de la instalación, puede habilitarlos o desactivarlos en la página Opciones avanzadas de la sección Configuración de la interfaz.
19. Para cada función que desee habilitar, active la casilla correspondiente.
20. Haga clic en Next (Siguiete).

21. Aparecerá el cuadro de diálogo Supervisión de servicio activa. **Nota:** Después de la instalación, puede configurar las funciones de supervisión de servicio activas en la página Administración de servicio activa de la sección Configuración del sistema.
22. Si desea que Cisco Secure ACS monitoree los servicios de autenticación de usuario, marque la casilla **Enable Login Monitoring** . En la lista Script to Execute, elija la opción que desea aplicar en caso de que se produzca un error en el servicio de autenticación: **Sin acción correctiva:** Cisco Secure ACS no ejecuta una secuencia de comandos. **Nota:** Esta opción es útil si habilita las notificaciones de correo de eventos. **Reinicio:** Cisco Secure ACS ejecuta una secuencia de comandos que reinicia el equipo que ejecuta Cisco Secure ACS. **Reiniciar todo:** Cisco Secure ACS reinicia todos los servicios Cisco Secure ACS. **Reiniciar RADIUS/TACACS+:** Cisco Secure ACS reinicia solamente los servicios RADIUS y TACACS+.
23. Si desea que Cisco Secure ACS envíe un mensaje de correo electrónico cuando el monitoreo de servicio detecte un evento, marque la casilla **Notificación de correo**.
24. Haga clic en Next (Siguiete).
25. Aparecerá el cuadro de diálogo Contraseña de cifrado de la base de datos. **Nota:** La contraseña de cifrado de la base de datos se cifra y se almacena en el registro ACS. Es posible que tenga que volver a utilizar esta contraseña cuando surjan problemas críticos y se deba acceder a la base de datos manualmente. Mantenga esta contraseña a mano para que el soporte técnico pueda acceder a la base de datos. La contraseña se puede cambiar cada período de vencimiento.
26. Introduzca una contraseña para el cifrado de la base de datos. La contraseña debe tener al menos ocho caracteres y debe contener tanto caracteres como dígitos. No hay caracteres no válidos. Haga clic en Next (Siguiete).
27. El programa de configuración finaliza y aparece el cuadro de diálogo Cisco Secure ACS Service Initiation.
28. Para cada opción Cisco Secure ACS Services Initiation que desee, marque la casilla correspondiente. Las acciones asociadas a las opciones se producen después de que finalice el programa de instalación. **Sí, deseo iniciar el servicio Cisco Secure ACS ahora:** inicia los servicios de Windows que componen Cisco Secure ACS. Si no selecciona esta opción, la interfaz HTML de Cisco Secure ACS no está disponible a menos que reinicie el equipo o inicie el servicio CSAdmin. **Sí, deseo que el programa de instalación inicie Cisco Secure ACS Administrator desde mi navegador tras la instalación:** abre la interfaz HTML de Cisco Secure ACS en el navegador web predeterminado para la cuenta de usuario de Windows actual. **Sí, deseo ver el archivo Léame:** abre el archivo README.TXT en el Bloc de notas de Windows.
29. Haga clic en Next (Siguiete).
30. Si ha seleccionado una opción, se inician los servicios Cisco Secure ACS. El cuadro de diálogo Setup Complete (Configuración completa) muestra información sobre la interfaz HTML de Cisco Secure ACS.
31. Haga clic en Finish (Finalizar). **Nota:** El resto de la configuración se documenta en la sección para el tipo EAP configurado.

## [Configuración del controlador LWAPP de Cisco](#)

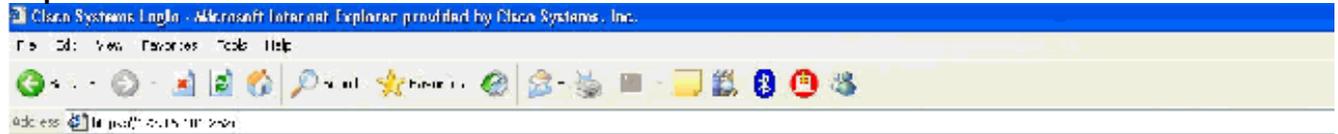
### [Crear la configuración necesaria para WPA2/WPA](#)

Complete estos pasos:

**Nota:** Se supone que el controlador tiene conectividad básica a la red y que el alcance de IP a la interfaz de administración es exitoso.

1. Inicie sesión en el controlador navegando a

**https://172.16.101.252.**



2. Haga clic en Login (Conexión).

3. Inicie sesión con el usuario predeterminado **admin** y la contraseña predeterminada **admin**.

4. Cree el mapping de VLAN de interfaz bajo el menú Controller.

5. Haga clic en **Interfaces**.

6. Haga clic en **New**.

7. En el campo Nombre de la interfaz, escriba **Empleado**. (Este campo puede ser cualquier valor que desee.)

8. En el campo VLAN ID, escriba **20**. (Este campo puede ser cualquier VLAN que se transporta en la red.)

9. Haga clic en Apply (Aplicar).

10. Configure la información como muestra esta ventana Interfaces > Edit

Address: https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management

Mobility Groups

Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

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

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

11. Haga clic en Apply (Aplicar).
12. Haga clic en **WLAN**.
13. Haga clic en **New**.
14. En el campo WLAN SSID, escriba **Employee**.
15. Haga clic en Apply (Aplicar).
16. Configure la información como muestra esta ventana WLANs > Edit .**Nota:** WPA2 es el método de encriptación de capa 2 elegido para este laboratorio. Para permitir que WPA con clientes TKIP-MIC se asocien a este SSID, también puede marcar las casillas **Modo de compatibilidad WPA** y **Permitir clientes TKIP WPA2** o aquellos clientes que no soportan el método de encriptación 802.11i AES.

## WLAN6 > 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 Services (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Pkts Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow PPP 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

### 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 IPsec and L2TP.

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

### 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)

17. Haga clic en Apply (Aplicar).
18. Haga clic en el menú **Seguridad** y agregue el servidor RADIUS.
19. Haga clic en **New**.
20. Agregue la dirección IP del servidor RADIUS (172.16.100.25) que es el servidor ACS configurado anteriormente.
21. Asegúrese de que la clave compartida coincida con el cliente AAA configurado en el servidor ACS.
22. Haga clic en Apply (Aplicar).



## 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

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

The screenshot shows the CiscoSecure ACS Network Configuration interface. The browser title is "CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The address bar shows "http://172.16.100.25:3052/index2.htm". The main content area is titled "AAA Client Setup For DEMO\_2006\_1". The configuration fields are as follows:

AAA Client IP Address	173.16.101.253
Key	shared secret
Authentication Using	RADIUS (Cisco Aires-GT)
<input type="checkbox"/>	single Connect TACACS+ AAA Client (Record step in accounting on failure).
<input type="checkbox"/>	Log Update/Watchdog Packets from this AAA Client
<input type="checkbox"/>	Log RADIUS Tunneling Packets from this AAA Client
<input type="checkbox"/>	Replace RADIUS Port info with Username from this AAA Client

23. La configuración básica se ha completado y puede comenzar a probar EAP-TLS.

## Autenticación EAP-TLS

La autenticación EAP-TLS requiere certificados de equipo y usuario en el cliente inalámbrico, la adición de EAP-TLS como tipo EAP a la política de acceso remoto para el acceso inalámbrico y una reconfiguración de la conexión de red inalámbrica.

Para configurar DC\_CA para proporcionar la inscripción automática para certificados de equipo y usuario, complete los procedimientos de esta sección.

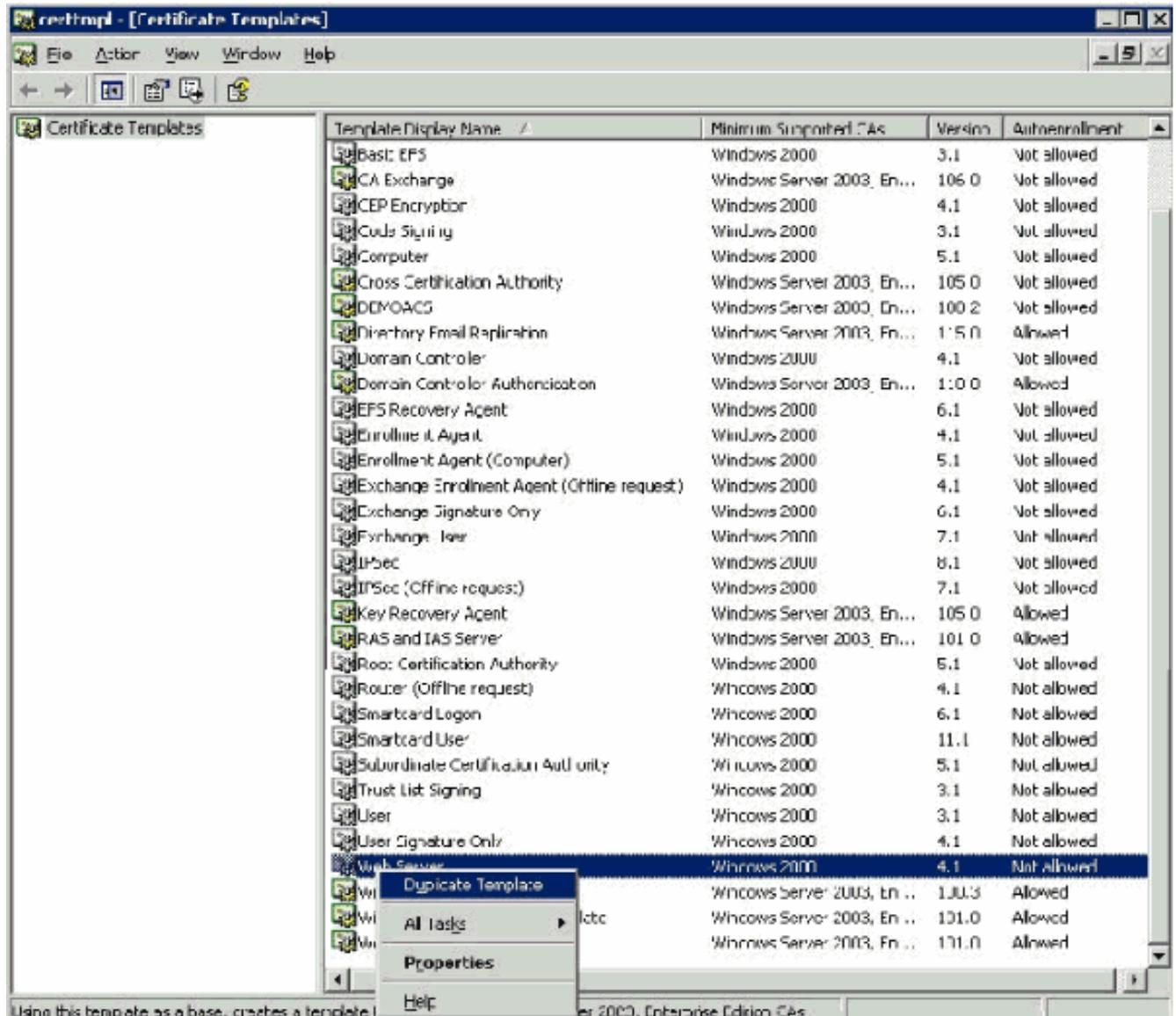
**Nota:** Microsoft ha cambiado la plantilla de servidor Web con la versión de la CA empresarial de Windows 2003, de modo que las claves ya no se pueden exportar y la opción está atenuada. No hay otras plantillas de certificados suministradas con servicios de certificados para la autenticación del servidor y ofrecen la capacidad de marcar claves como exportables disponibles en la lista desplegable, por lo que debe crear una nueva plantilla que lo haga.

**Nota:** Windows 2000 permite exportar claves y no es necesario seguir estos procedimientos si utiliza Windows 2000.

## Instalación del complemento Plantillas de certificado

Complete estos pasos:

1. Elija **Inicio > Ejecutar**, escriba **mmc** y haga clic en **Aceptar**.
2. En el menú **Archivo**, haga clic en **Agregar o quitar complemento** y, a continuación, haga clic en **Agregar**.
3. En **Complemento**, haga doble clic en **Plantillas de certificado**, haga clic en **Cerrar** y, a continuación, haga clic en **Aceptar**.
4. En el árbol de la consola, haga clic en **Plantillas de certificado**. Todas las plantillas de certificados aparecen en el panel **Detalles**.
5. Para omitir los pasos 2 a 4, escriba **certtmpl.msc** que abre el complemento **Plantillas de certificado**.



## [Creación de la Plantilla de Certificado para el Servidor Web ACS](#)

Complete estos pasos:

1. En el panel **Detalles** del complemento **Plantillas de certificado**, haga clic en la plantilla **Servidor Web**.
2. En el menú **Acción**, haga clic en **Duplicar plantilla**.

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:

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:

Validity period:  years  weeks

Renewal period:  weeks

Publish certificate in Active Directory

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

OK Cancel Apply

3. En el campo Template display name, escriba

**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 [▼]

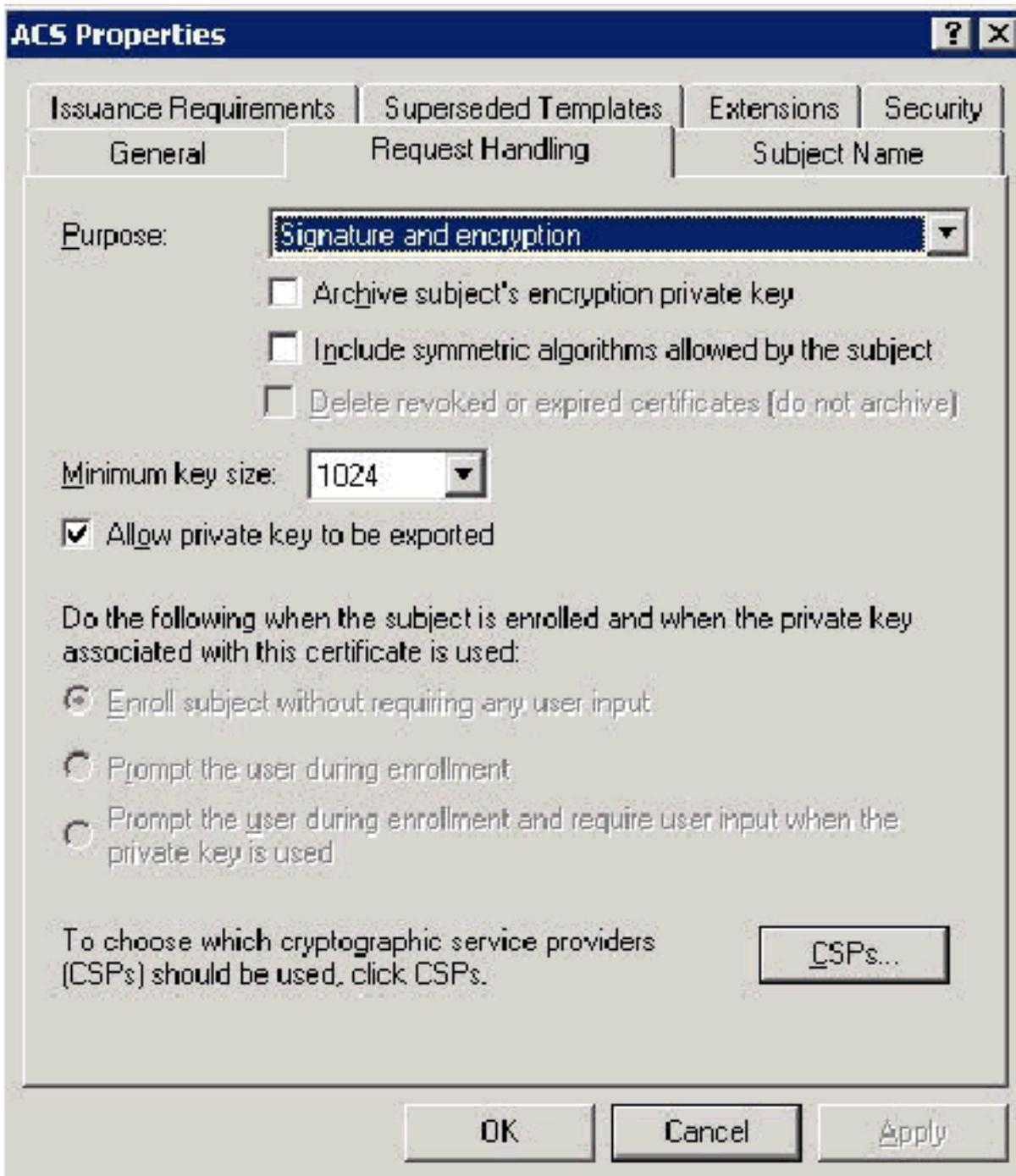
Publish certificate in Active Directory

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

[ OK ] [ Cancel ] [ Apply ]

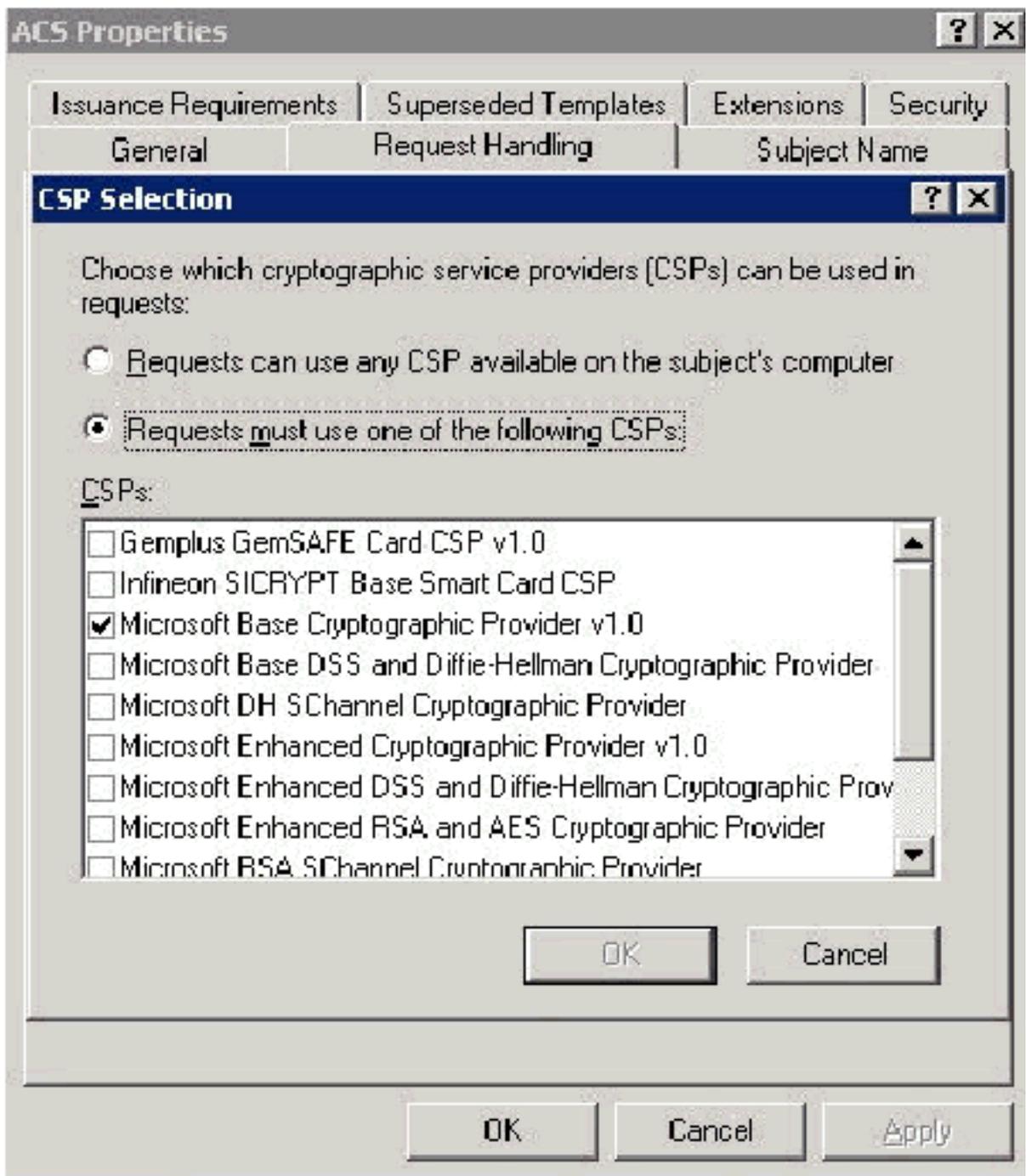
ACS.

4. Vaya a la ficha Request Handling (Gestión de solicitudes) y marque **Allow private key to be export (Permitir exportación de clave**



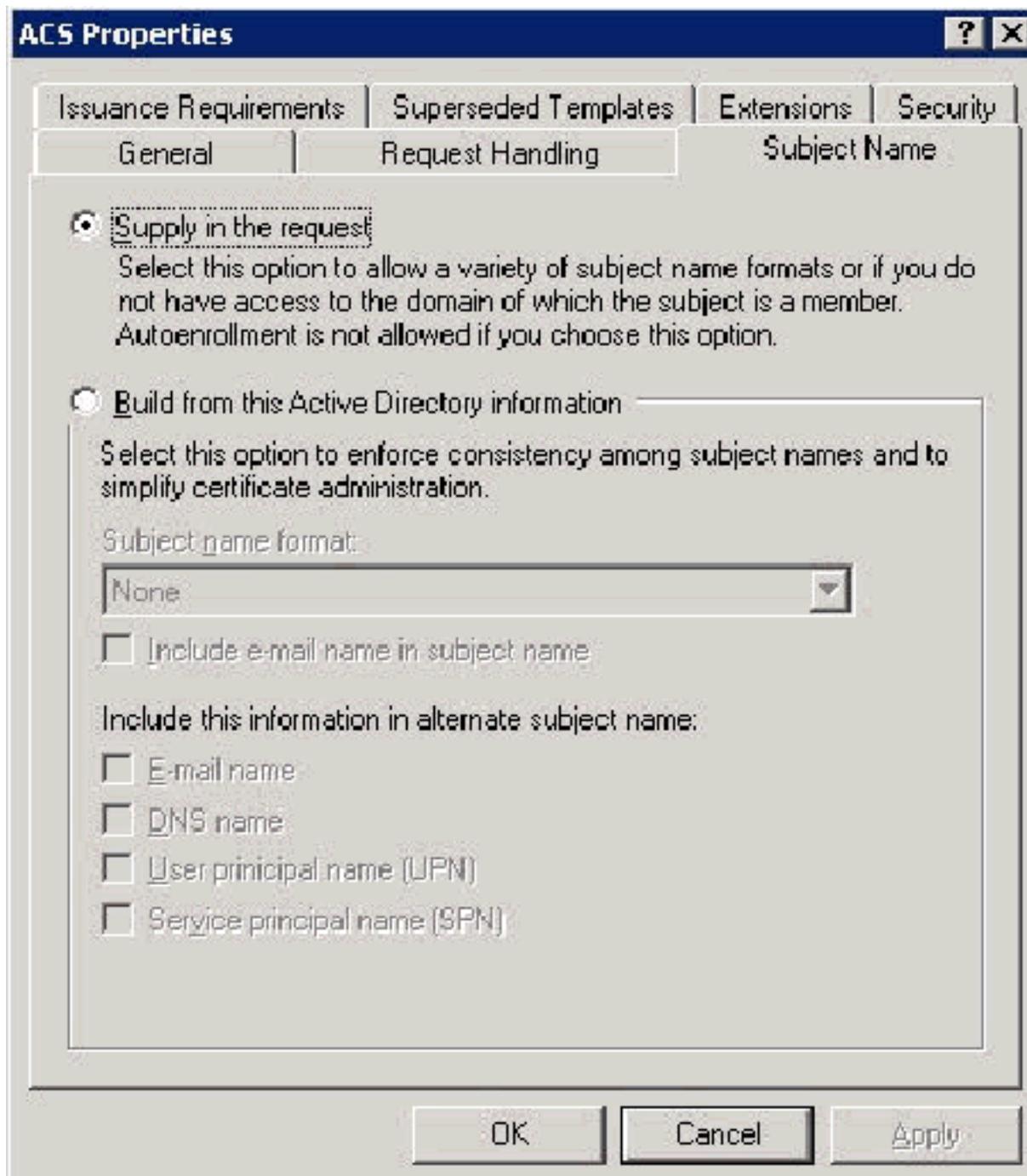
privada).

5. Elija Solicitudes debe utilizar uno de los siguientes CSP y verificar Proveedor criptográfico de Microsoft Base v1.0. Desactive cualquier otro CSP que esté marcado y luego haga clic en

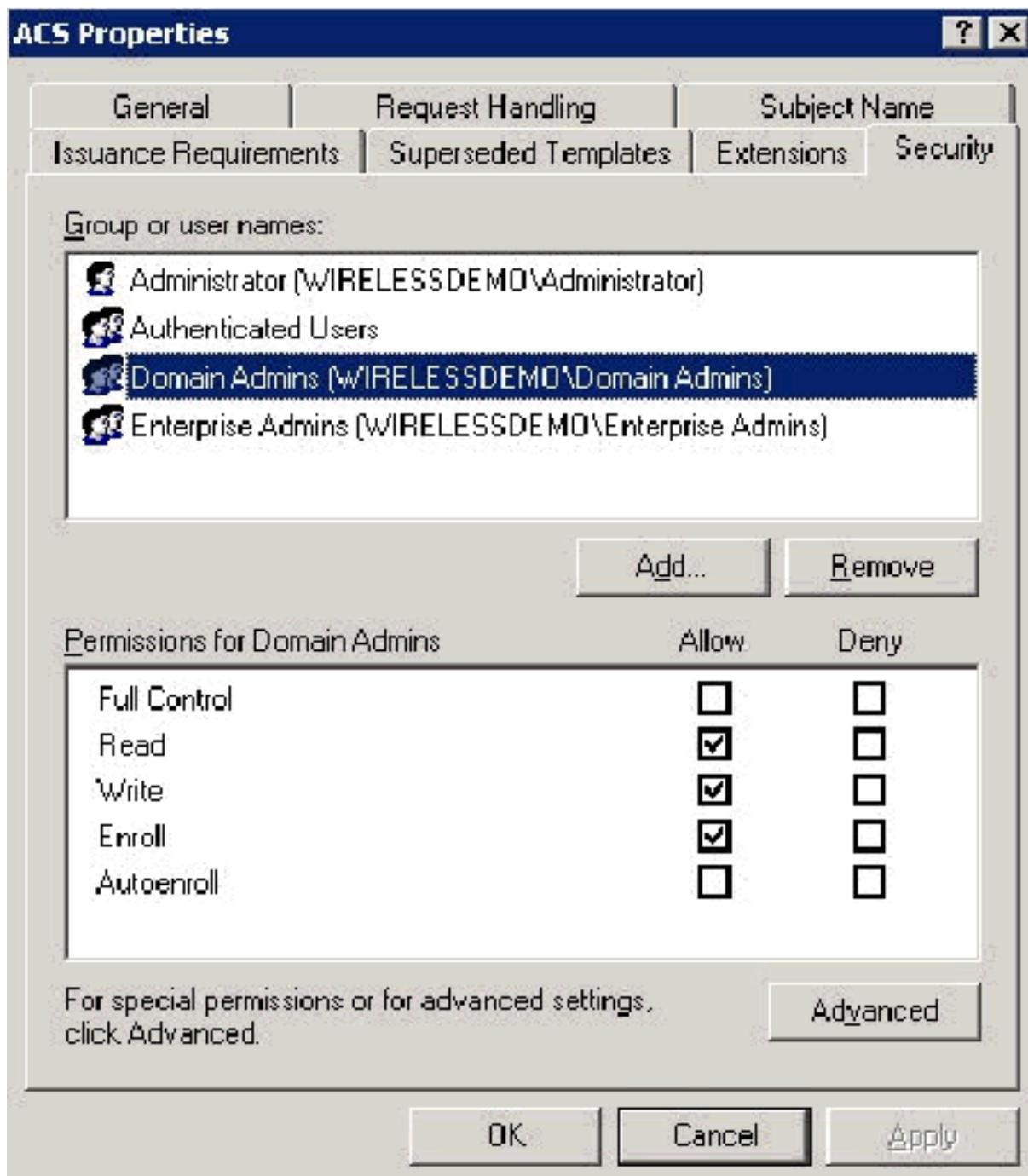


Aceptar.

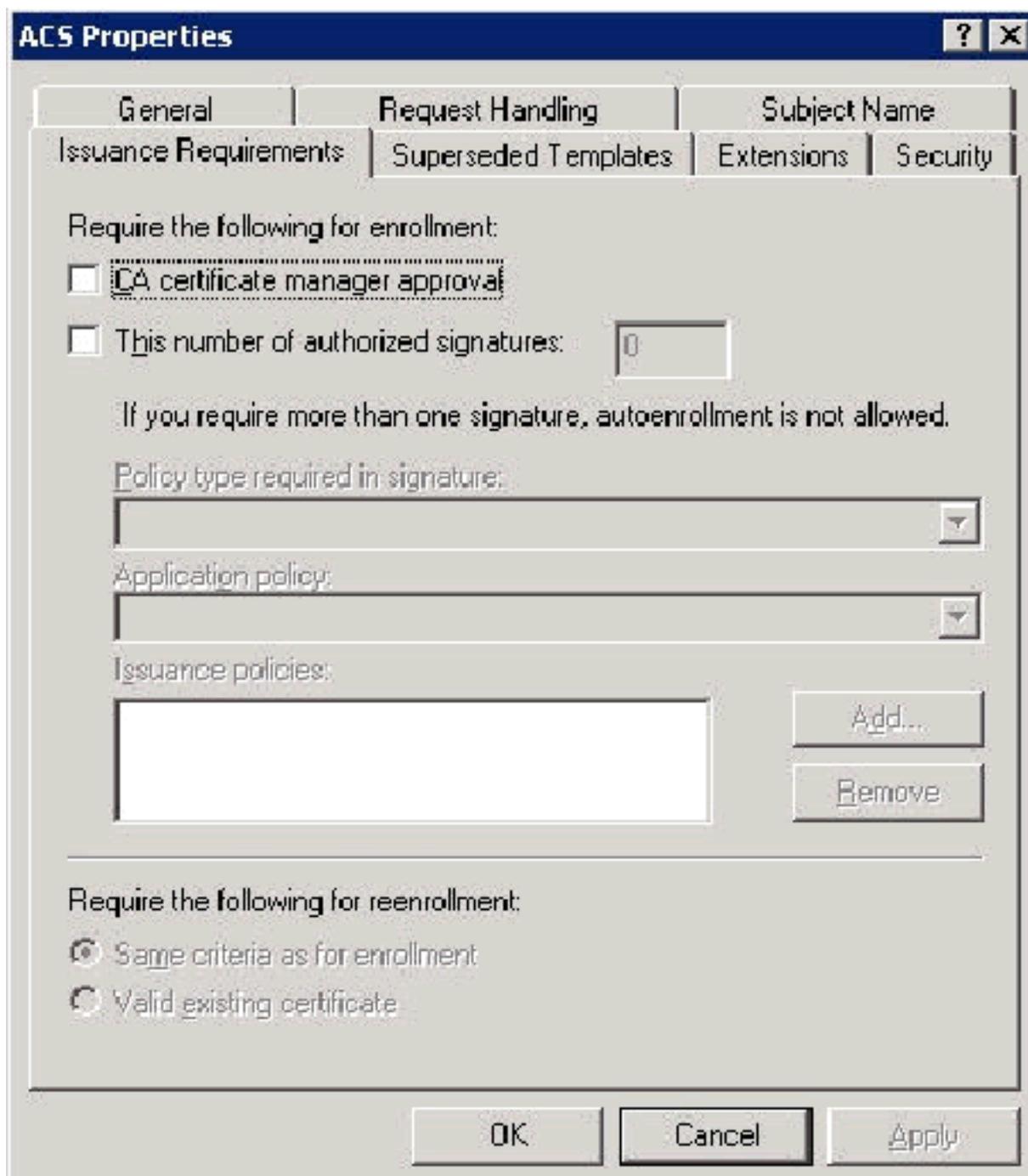
6. Vaya a la pestaña Nombre del asunto, elija **Suministrar en la solicitud** y haga clic en **Aceptar**.



7. Vaya a la ficha Seguridad, resalte el **grupo de administradores de dominio** y asegúrese de que la opción **Inscripción** esté marcada en Permitida. **Importante:** Si elige generar sólo de esta información de Active Directory, marque **Nombre principal de usuario (UPN)** y desmarque **Incluir nombre de correo electrónico** en Nombre de asunto y Nombre de correo electrónico porque no se ha introducido un nombre de correo electrónico para la cuenta de usuario inalámbrico en el complemento Usuarios y equipos de Active Directory. Si no desactiva estas dos opciones, la inscripción automática intenta utilizar el correo electrónico, lo que da lugar a un error de inscripción automática.



8. Existen medidas de seguridad adicionales si es necesario para evitar que los certificados se eliminen automáticamente. Estos se pueden encontrar en la pestaña Requisitos de emisión. Esto no se analiza más a fondo en este documento.

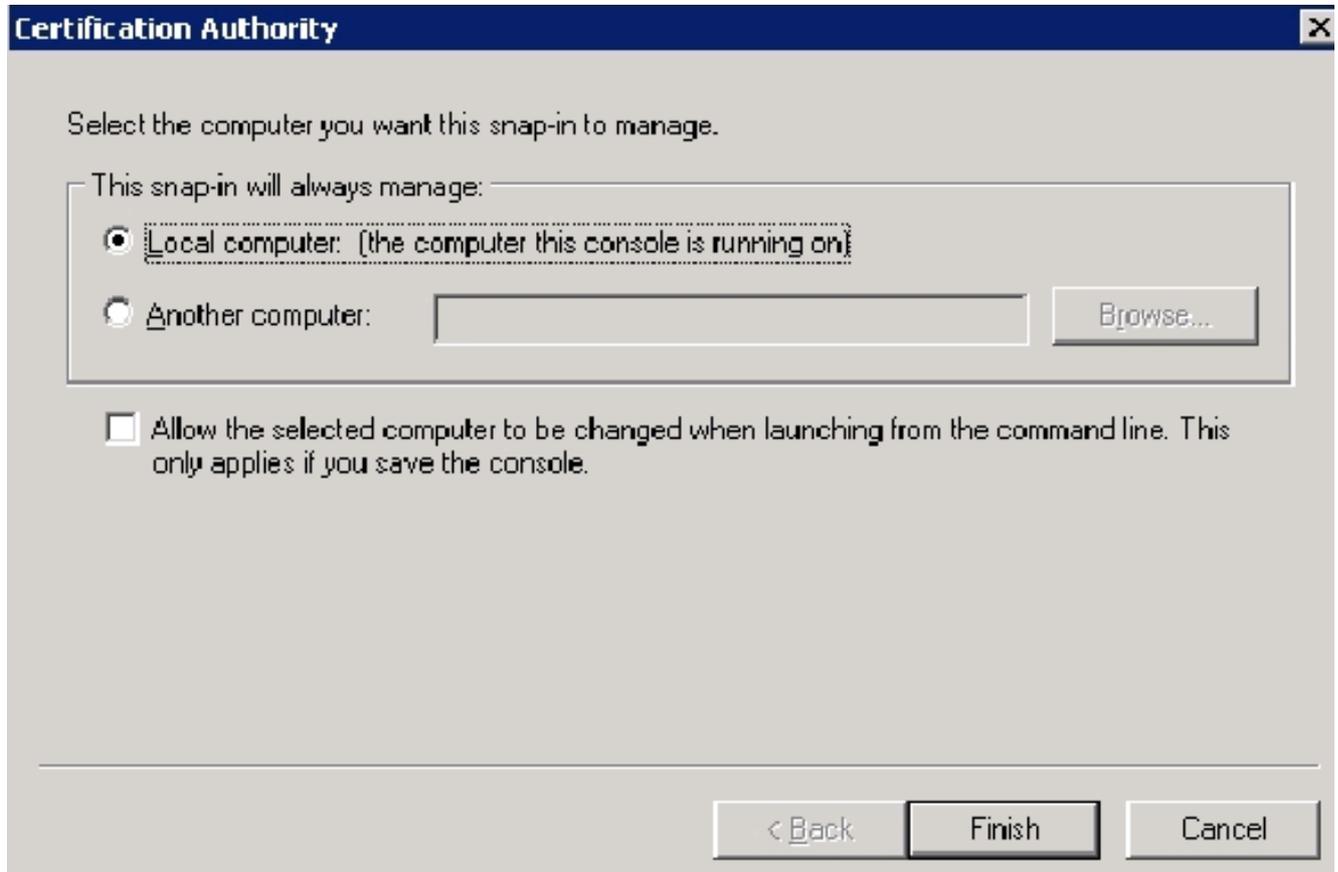


9. Haga clic en **Aceptar** para guardar la plantilla y pasar a emitir esta plantilla desde el complemento Autoridad de certificados.

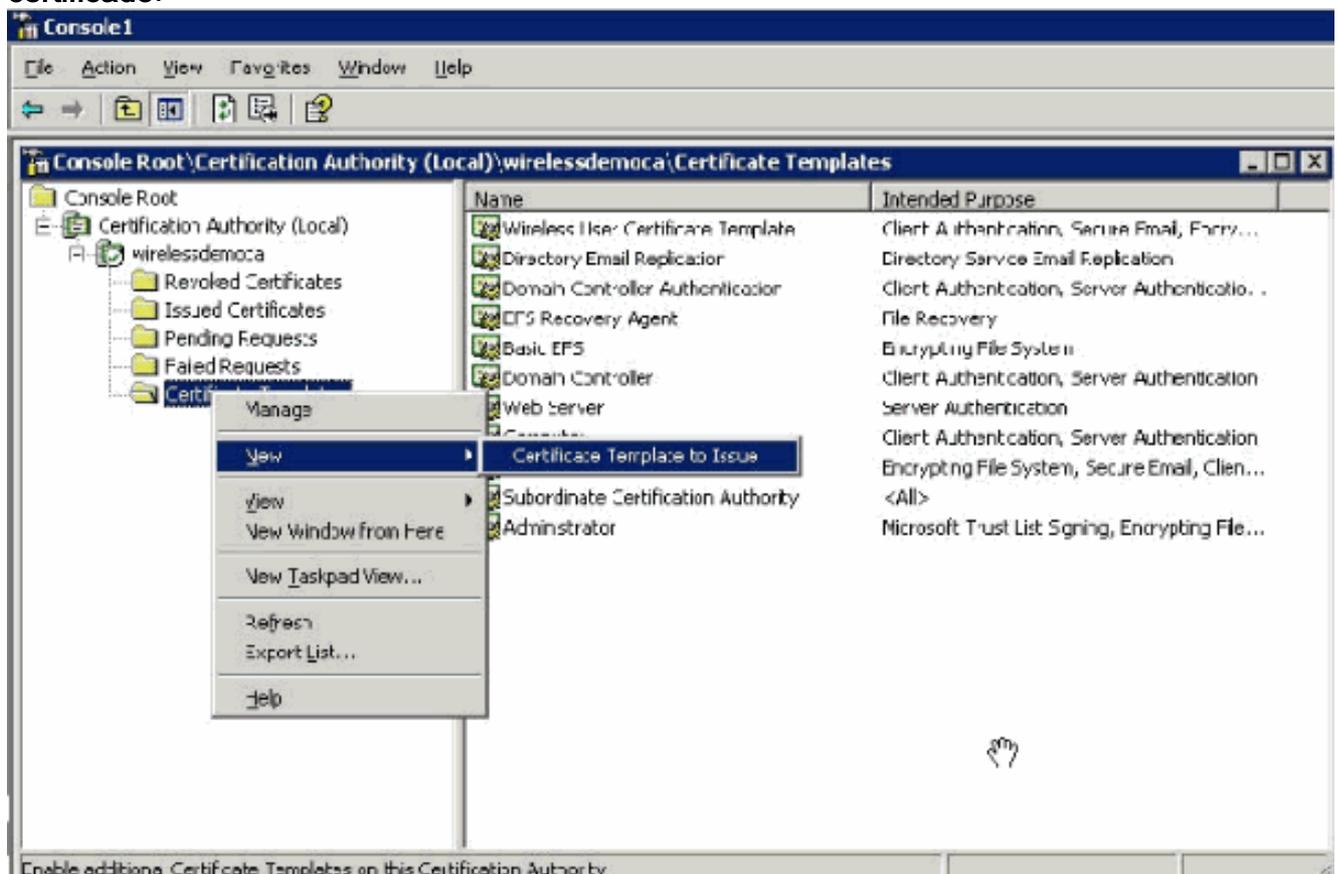
## [Habilitación de la Nueva Plantilla de Certificado de Servidor Web ACS](#)

Complete estos pasos:

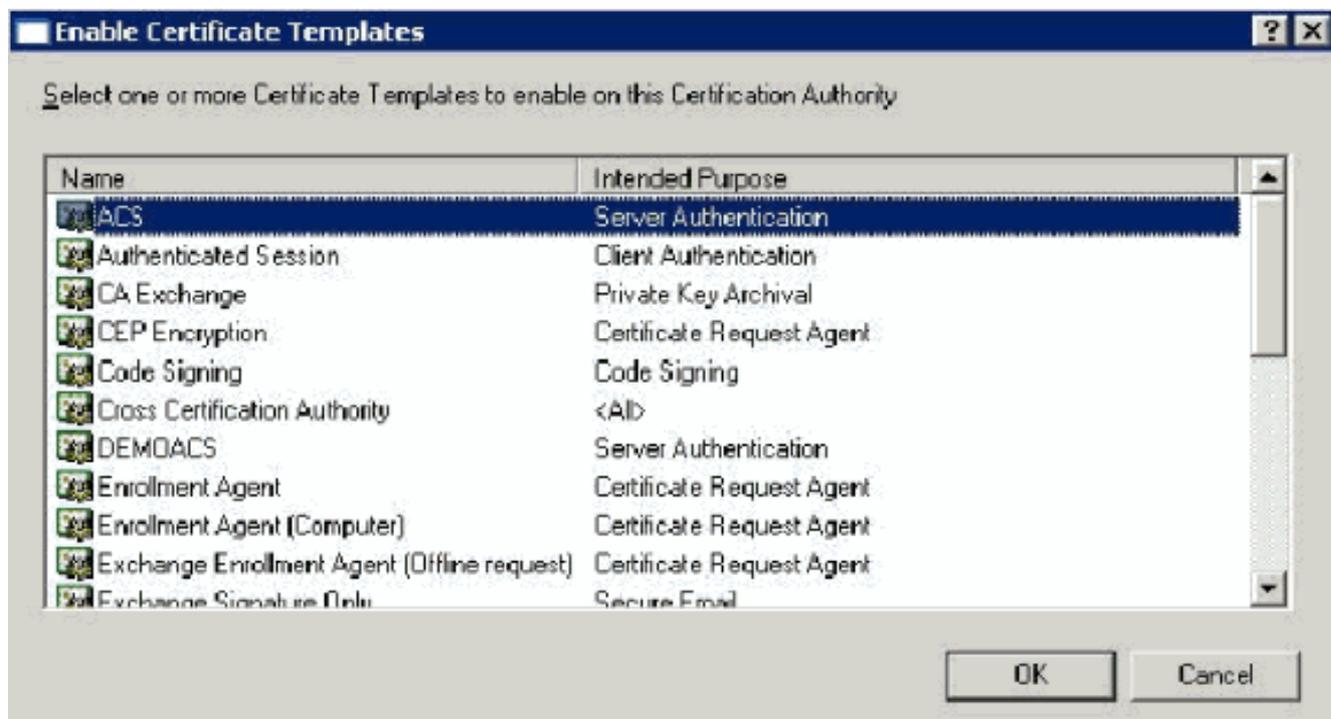
1. Abra el complemento **Autoridad de certificación**. Siga los pasos 1-3 en la sección [Creación de la Plantilla de Certificado para el Servidor Web ACS](#), elija la opción **Autoridad de Certificación**, elija **Equipo Local** y haga clic en **Finalizar**.



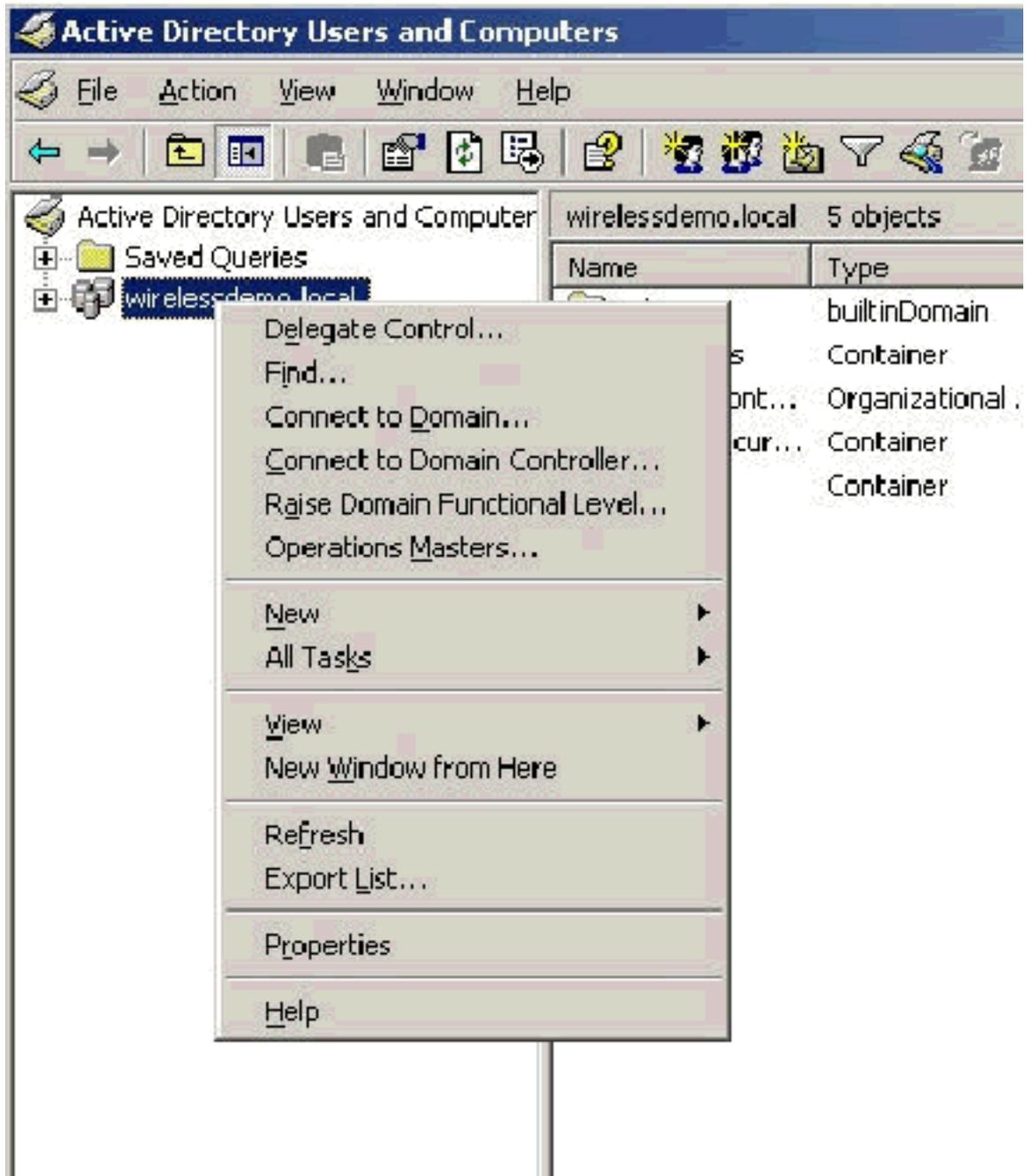
2. En el árbol de la consola, expanda **wirelessdemoca** y, a continuación, haga clic con el botón derecho en **Plantillas de certificado**.



3. Elija **New > Certificate Template** para emitir.
4. Haga clic en la plantilla **ACS Certificate**.

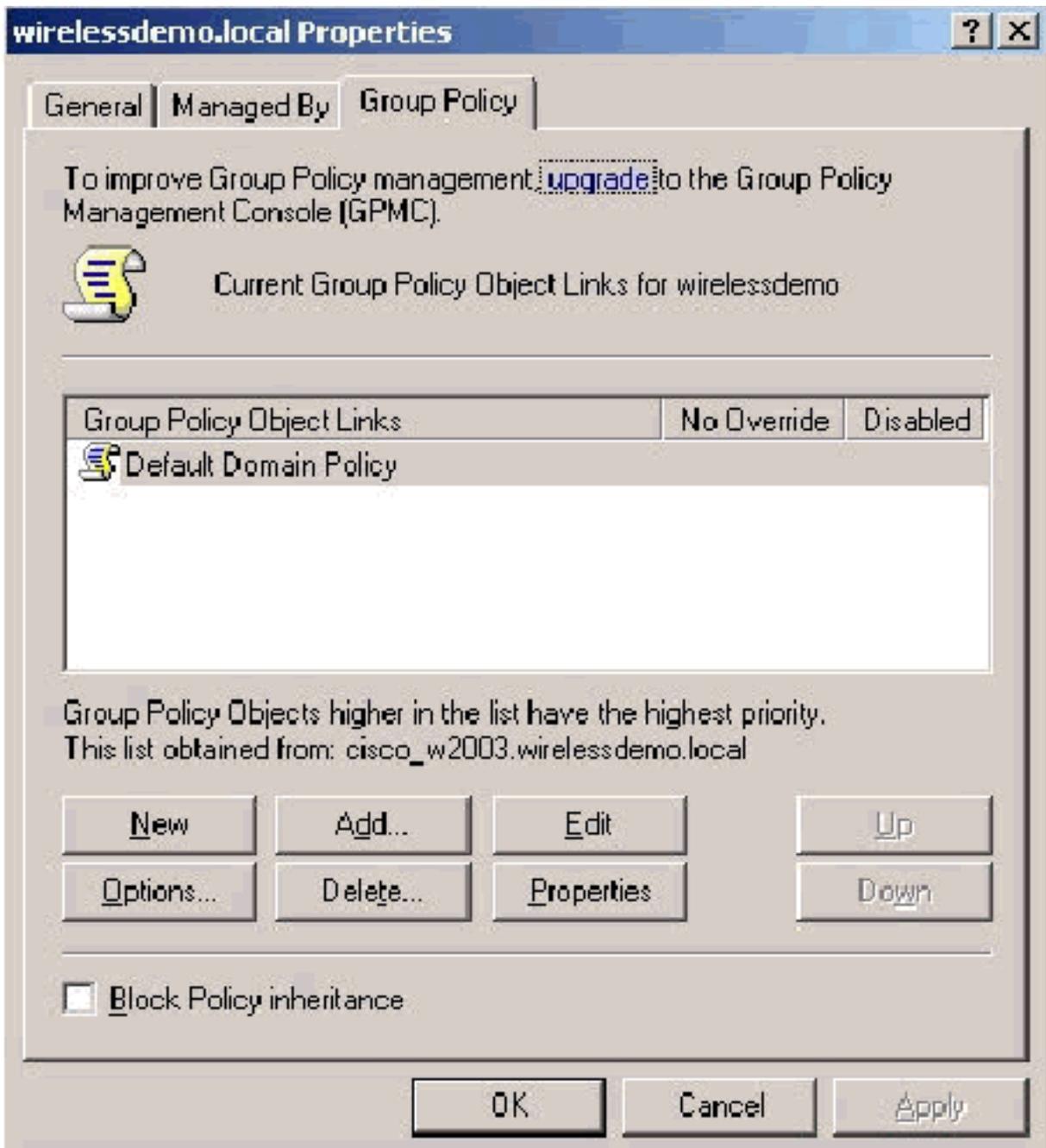


5. Haga clic en **Aceptar** y abra el **complemento Usuarios y equipos de Active Directory**.
6. En el árbol de la consola, haga doble clic en **Active Directory Users and Computers**, haga clic con el botón derecho del mouse en el **dominio alámbressedemo.local** y, a continuación, haga clic en



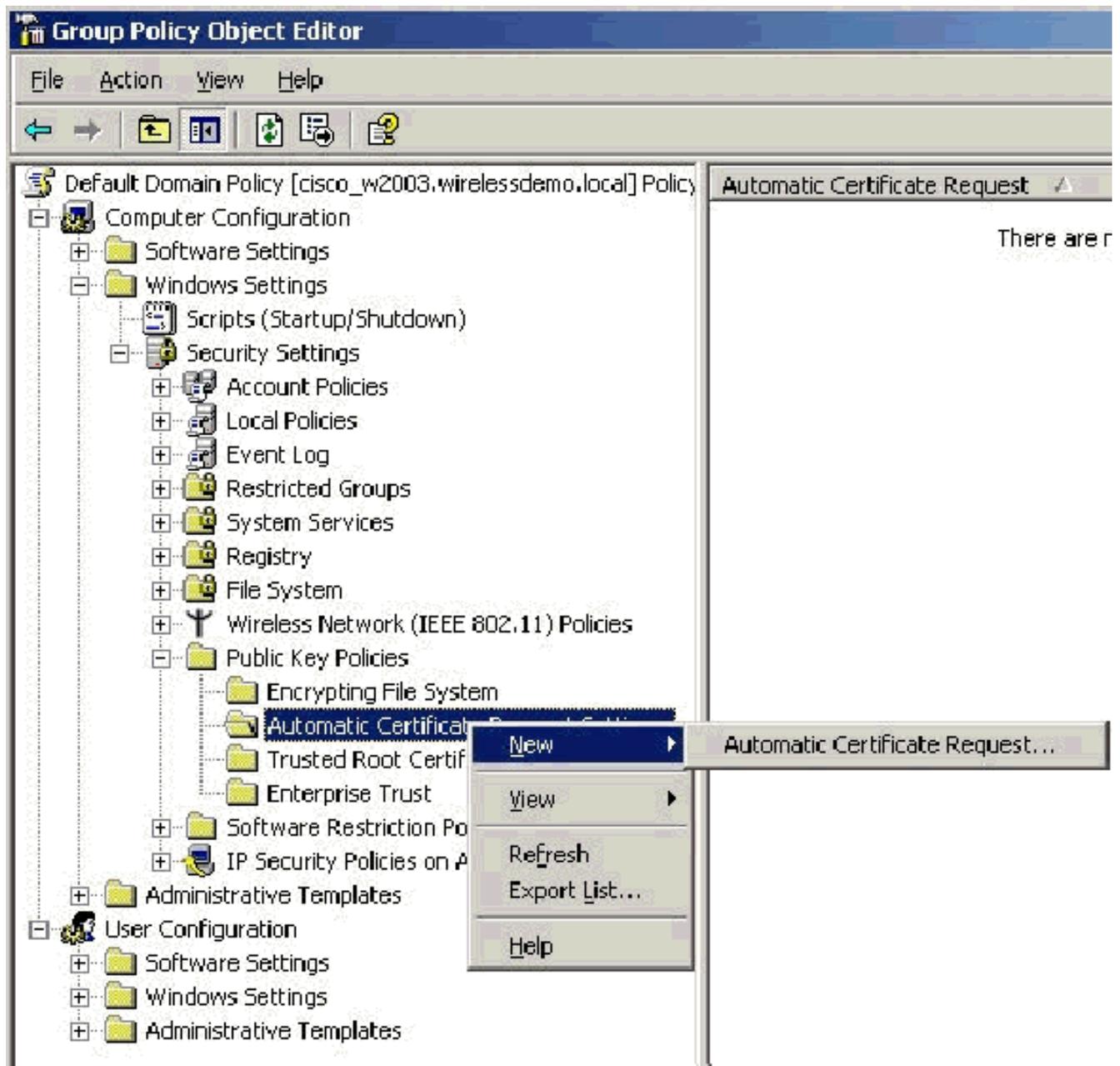
### Properties.

7. En la ficha Directiva de grupo, haga clic en **Política de dominio predeterminada** y, a continuación, haga clic en **Editar**. Se abre el complemento Editor de objetos de directiva de



grupo.

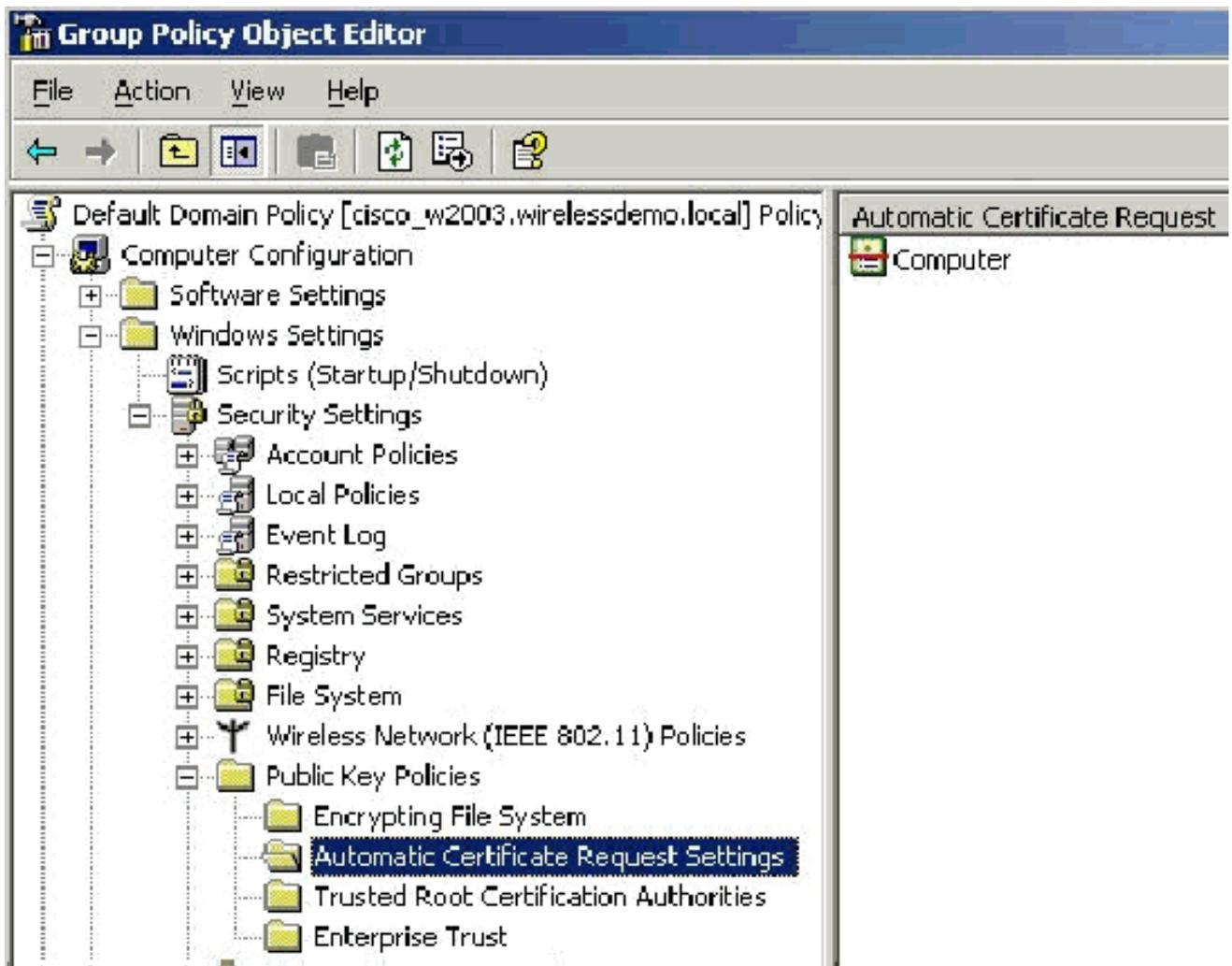
8. En el árbol de la consola, expanda **Computer Configuration > Windows Settings > Security Settings > Public Key Policies** y, a continuación, seleccione **Automatic Certificate Request Settings**.



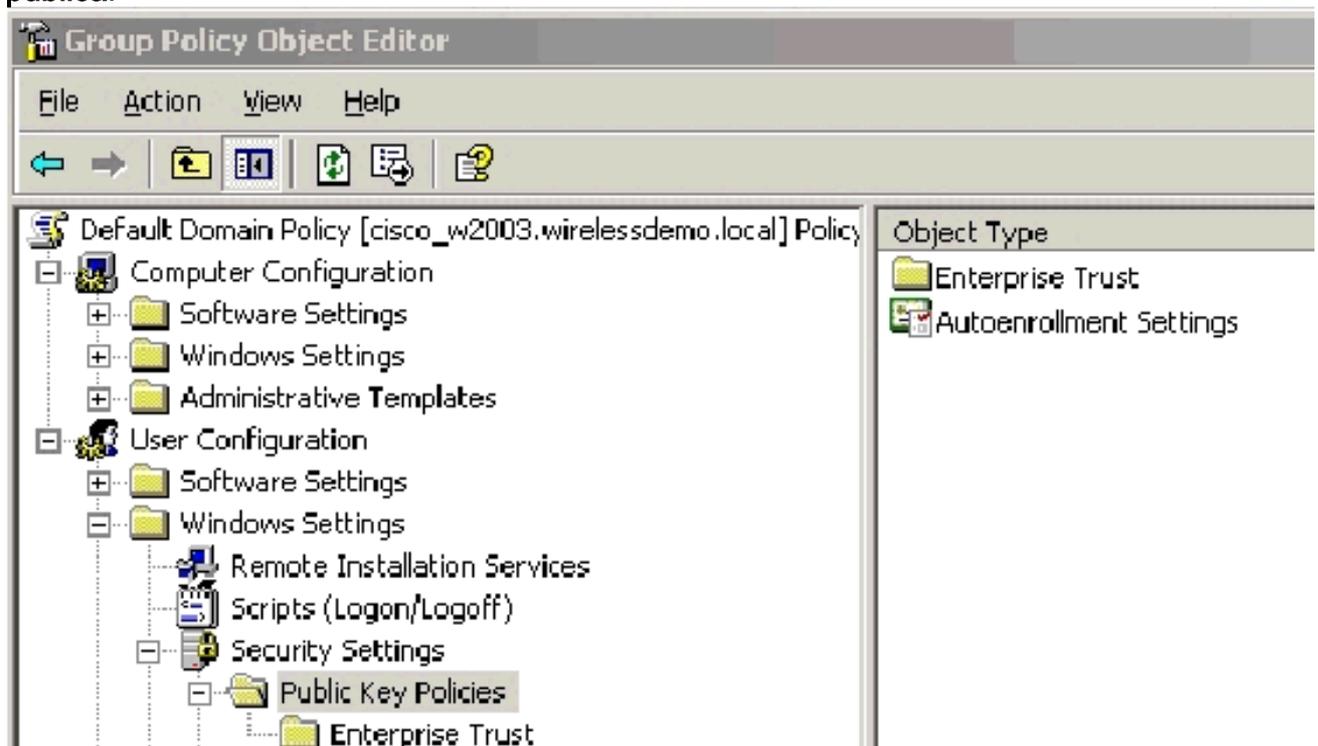
9. Haga clic con el botón derecho en **Configuración automática de solicitud de certificado** y elija **Nuevo > Solicitud automática de certificado**.
10. En la página Welcome to the Automatic Certificate Request Setup Wizard (Bienvenido al Asistente de configuración automática de solicitudes de certificado), haga clic en **Next**.
11. En la página Plantilla de certificado, haga clic en **Equipo** y haga clic en **Siguiente**.



12. En la página Finalización del Asistente de Configuración de Solicitud de Certificado Automática, haga clic en **Finalizar**. El tipo de certificado de equipo ahora aparece en el panel de detalles del complemento Editor de objetos de directiva de grupo.

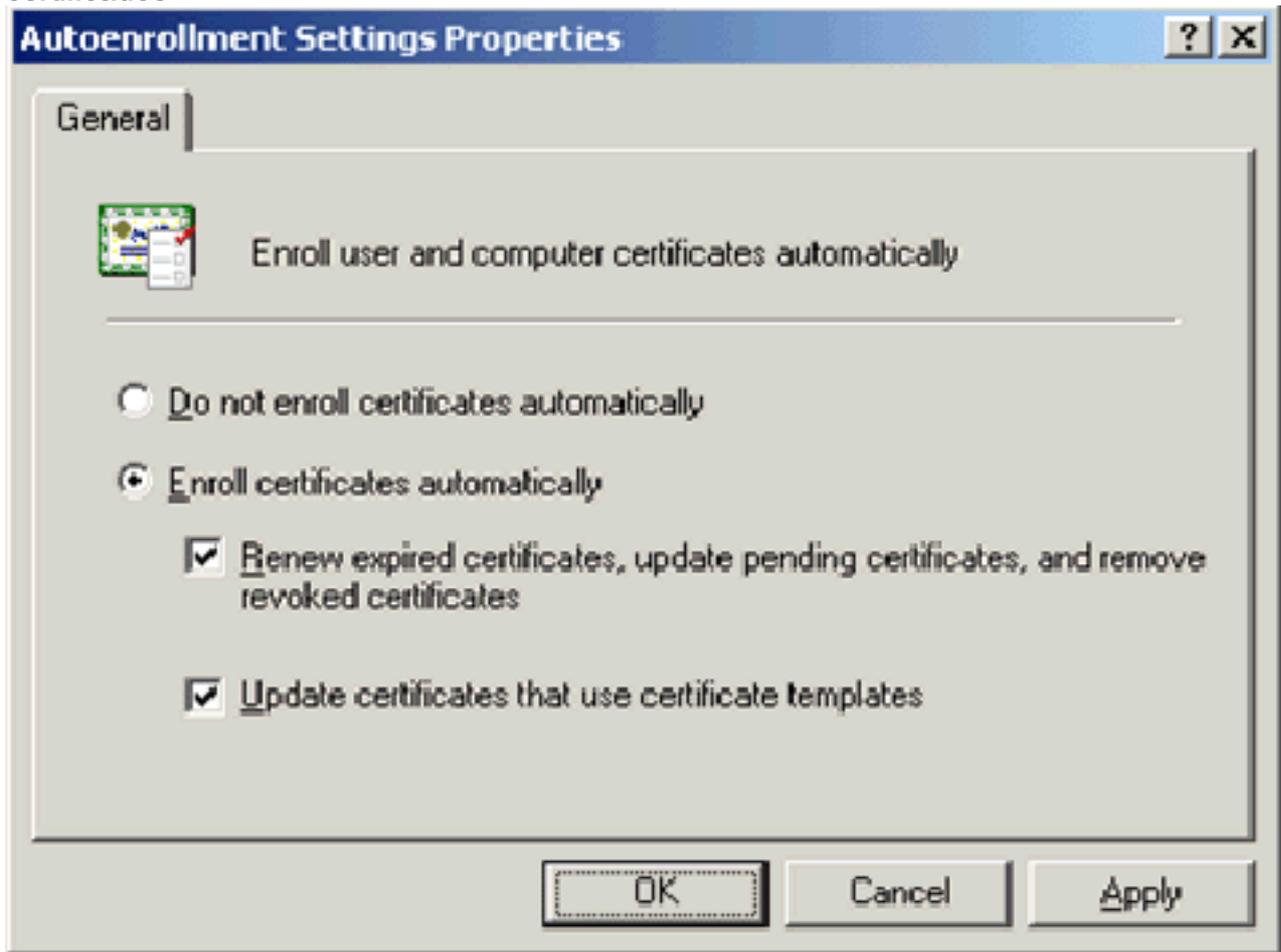


13. En el árbol de la consola, expanda **Configuración de usuario** > **Configuración de Windows** > **Configuración de seguridad** > **Políticas de clave pública**.



14. En el panel de detalles, haga doble clic en **Configuración de inscripción automática**.  
 15. Elija **Inscribir certificados automáticamente** y marque **Renovar certificados caducados**,

actualizar certificados pendientes y eliminar certificados revocados y Actualizar certificados que utilicen plantillas de certificados.



16. Click OK.

## [Configuración de certificados ACS 4.0](#)

### [Configuración del Certificado Exportable para ACS](#)

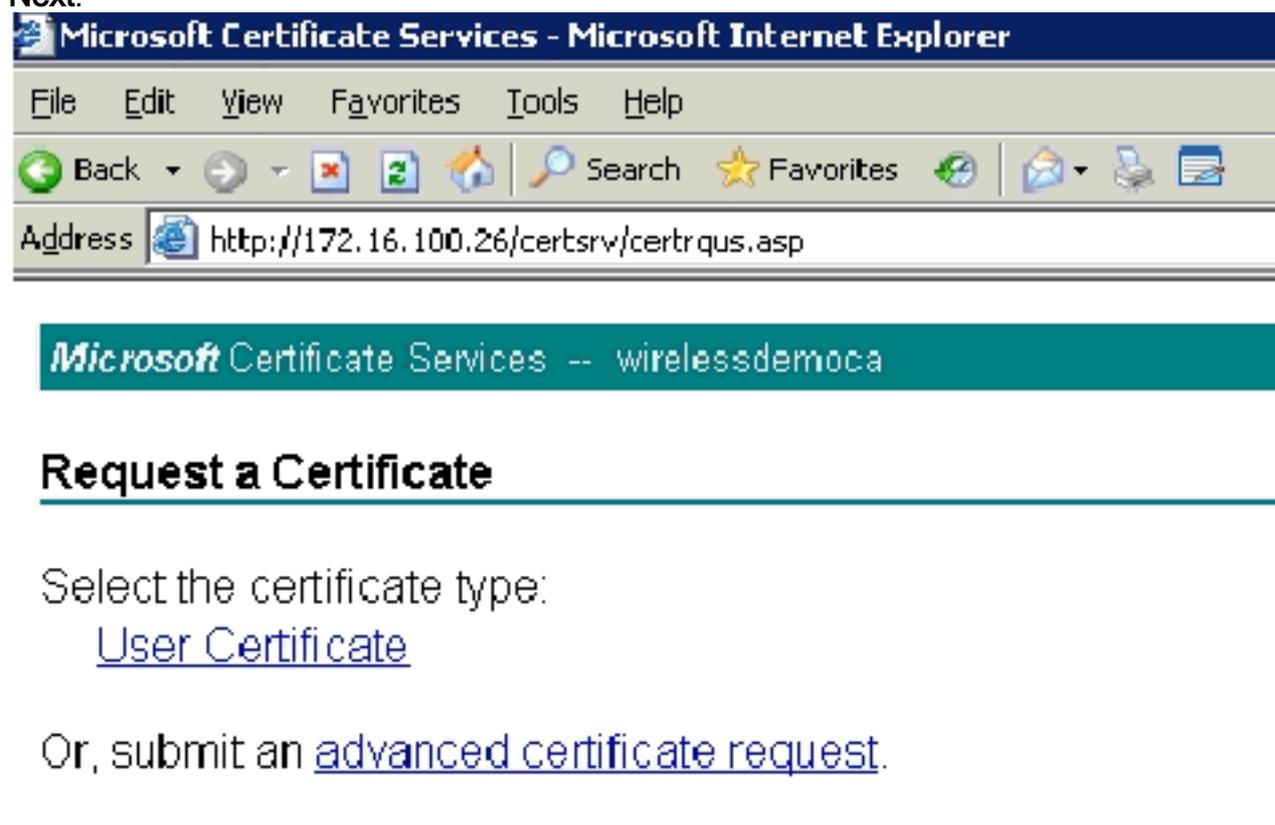
**Importante:** El servidor ACS debe obtener un certificado de servidor del servidor CA raíz de la empresa para autenticar un cliente WLAN EAP-TLS.

**Importante:** Asegúrese de que el Administrador IIS no esté abierto durante el proceso de configuración del certificado, ya que causa problemas con la información almacenada en caché.

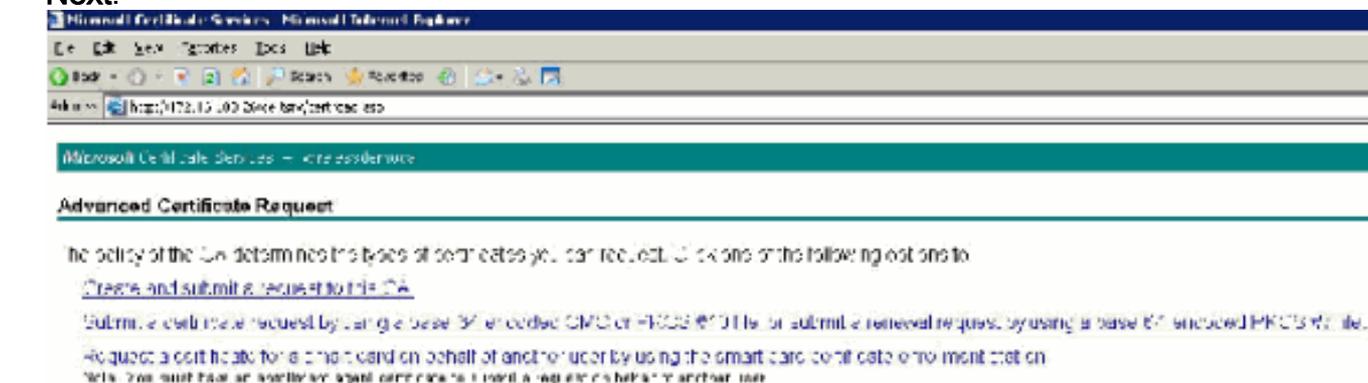
1. Inicie sesión en el servidor ACS con una cuenta que tenga derechos de administrador de empresa.
2. En la máquina ACS local, señale el explorador en el servidor de Microsoft Certification Authority en <http://IP-address-of-Root-CA/certsrv>. En este caso, la dirección IP es **172.16.100.26**.
3. Inicie sesión como administrador.



4. Elija **Request a Certificate** y haga clic en **Next**.



5. Elija **Advanced Request** y haga clic en **Next**.



6. Elija **Crear y enviar una solicitud a esta CA** y haga clic en **Siguiente**. **Importante:** El motivo de este paso es que Windows 2003 no permite las claves exportables y necesita generar una solicitud de certificado basada en el certificado ACS que creó anteriormente que sí lo permite.

sock - [Icons] Secret - Favorites [Icons] [Icons]

Address: http://172.16.1.10:2544/ctrl/ctrlmain.asp

**Microsoft Certificate Services** - wirelessdemo.local

---

### Advanced Certificate Request

---

**Certificate Template:**

Administrator

---

**Key Options:**

Administrator  
Basic EFS  
EFS Recovery Agent  
User  
CSP: Wireless User Certificate Template  
Key Usage: S\_Lordine Certification Authority  
Key Store: Web Server  
Max: 15384

Key Length: 1024 2048 4096 8192 16384

Automatic key container name     User specified key container name

Mark keys as exportable  
 Export keys to file

Enable storing private key protection

Store certificate in the local computer certificate store  
*Saves 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

Attributes: [List Box]

Friendly Name: [Text Box]

7. En Plantillas de certificado, seleccione la plantilla de certificado creada anteriormente con el nombre **ACS**. Las opciones cambian después de seleccionar la plantilla.
8. Configure el Nombre para que sea el nombre de dominio completo del servidor ACS. En este caso, el nombre del servidor ACS es cisco\_w2003.wirelessdemo.local. Asegúrese de que el **certificado de almacenamiento en el almacén de certificados del equipo local** esté activado y haga clic en

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://172.16.100.26/certsrv/certreqna.asp

---

**Certificate Template:**

ACS

---

**Identifying Information For Offline Template:**

Name: cisco\_w2003\_wirelessdemo.local

E-Mail:

Company:

Department:

City:

State:

Country/Region:

---

**Key Options:**

Create new key set  Use existing key set

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage:  Exchange

Key Size: 1024 Min:1024 Max:1024 (common key sizes: 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  PKCS10

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

Save request to a file

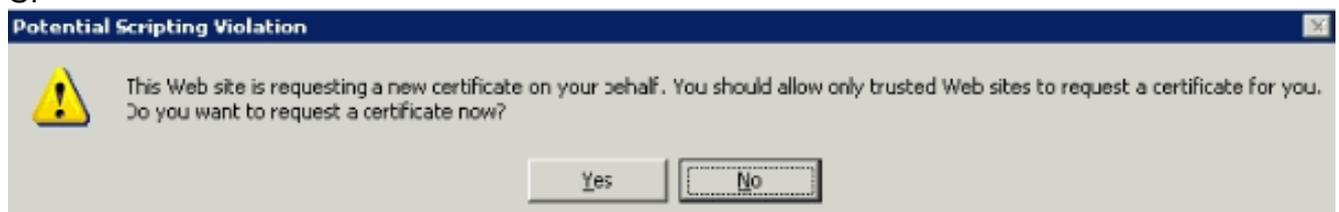
Attributes:

Friendly Name:

Submit >

Enviar.

9. Aparece una ventana emergente que advierte sobre una posible violación de secuencias de comandos. Haga clic en Sí



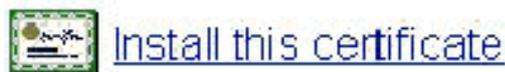
10. Haga clic en Install this certificate (Instalar este certificado).



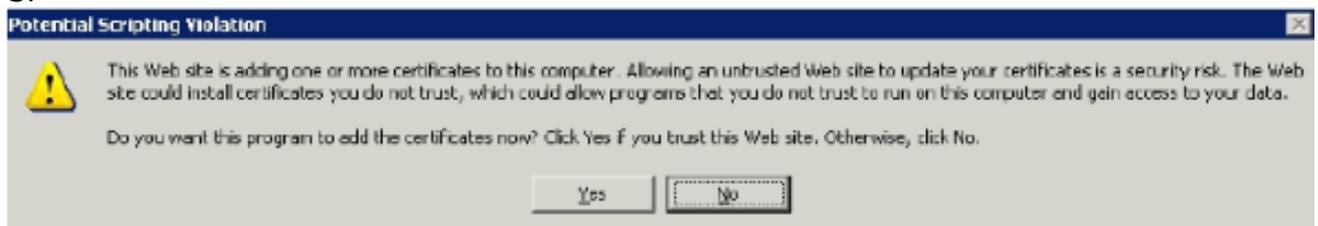
Microsoft Certificate Services -- wirelessdemoca

## Certificate Issued

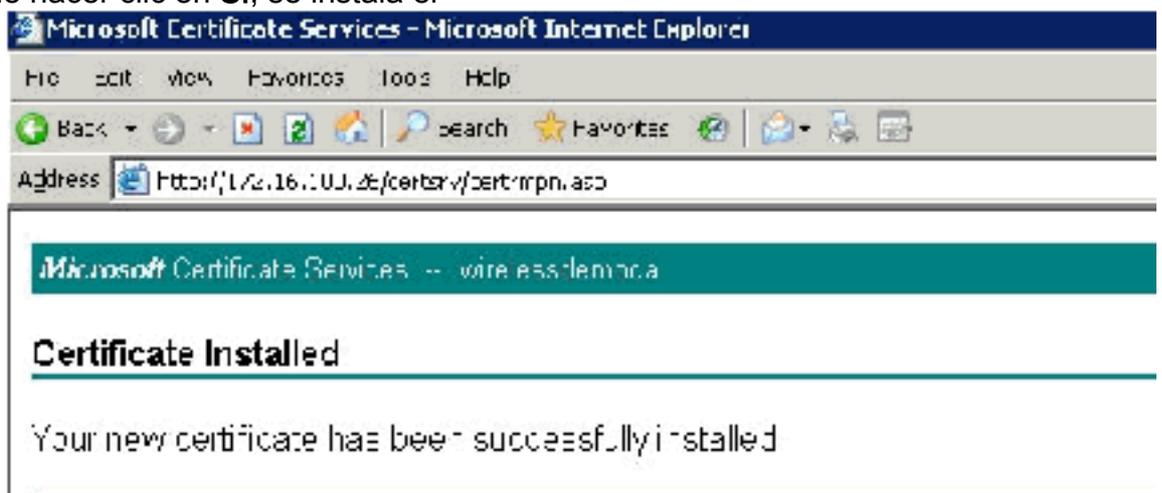
The certificate you requested was issued to you.



11. Una ventana emergente aparece de nuevo y advierte sobre una posible violación de secuencias de comandos. Haga clic en **Sí**

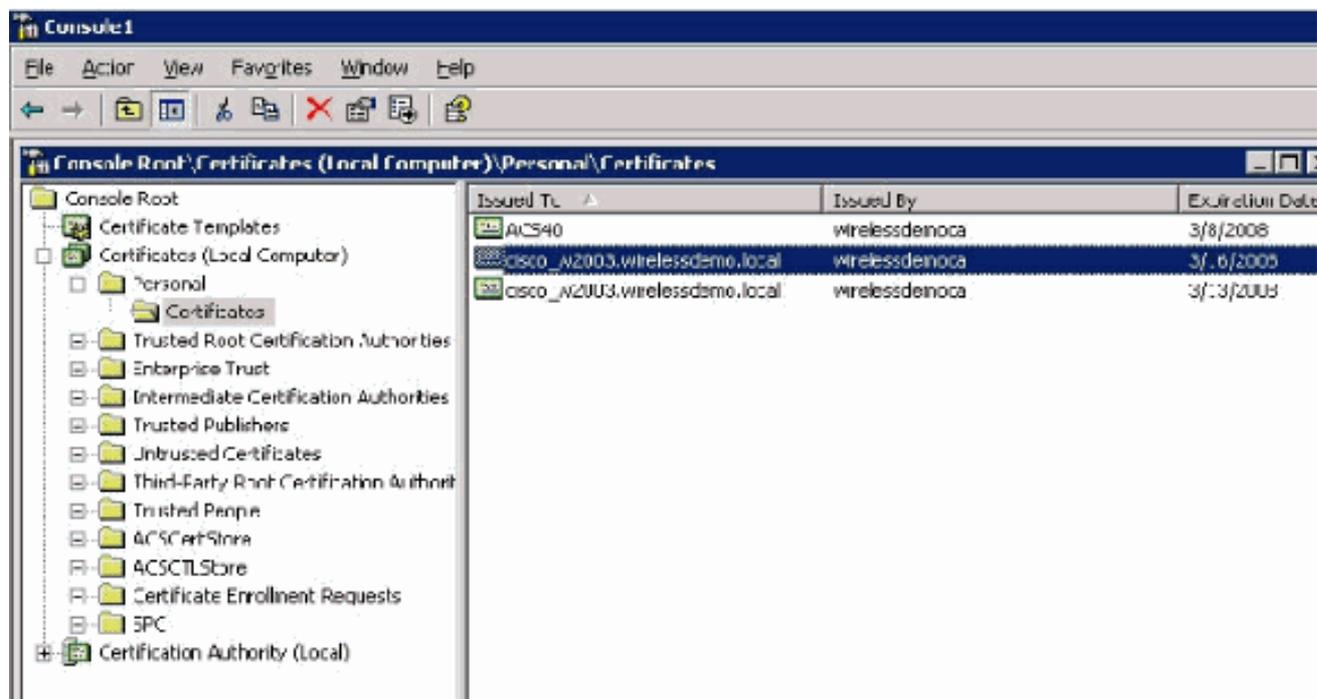


12. Después de hacer clic en **Sí**, se instala el



certificado.

13. En este momento, el certificado se instala en la carpeta Certificates (Certificados). Para acceder a esta carpeta, elija **Start > Run**, escriba **mmc**, presione **Enter** y elija **Personal > Certificates**.



14. Ahora que el certificado está instalado en el equipo local (ACS o cisco\_w2003 en este ejemplo), debe generar un archivo de certificado (.cer) para la configuración del archivo de certificado ACS 4.0.
15. En el servidor ACS (cisco\_w2003 en este ejemplo), señale el explorador en el servidor de Microsoft Certification Authority a [http://172.16.100.26 /certsrv](http://172.16.100.26/certsrv).

## [Instalación del certificado en el software ACS 4.0](#)

Complete estos pasos:

1. En el servidor ACS (cisco\_w2003 en este ejemplo), señale el explorador en el servidor de Microsoft CA a [http://172.16.100.26 /certsrv](http://172.16.100.26/certsrv).
2. En la opción Seleccionar una tarea elija **Descargar un certificado de CA, cadena de certificado o CRL**.
3. Elija el método de codificación de radio **Base 64** y haga clic en **Descargar certificado CA**.

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://172.16.100.26/certs/certnew.asp

---

Microsoft Certificate Services -- wirelessdemora

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority [install this CA certificate chain](#).

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

**CA certificate:**

Current (wirelessdemora)

**Encoding method:**

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

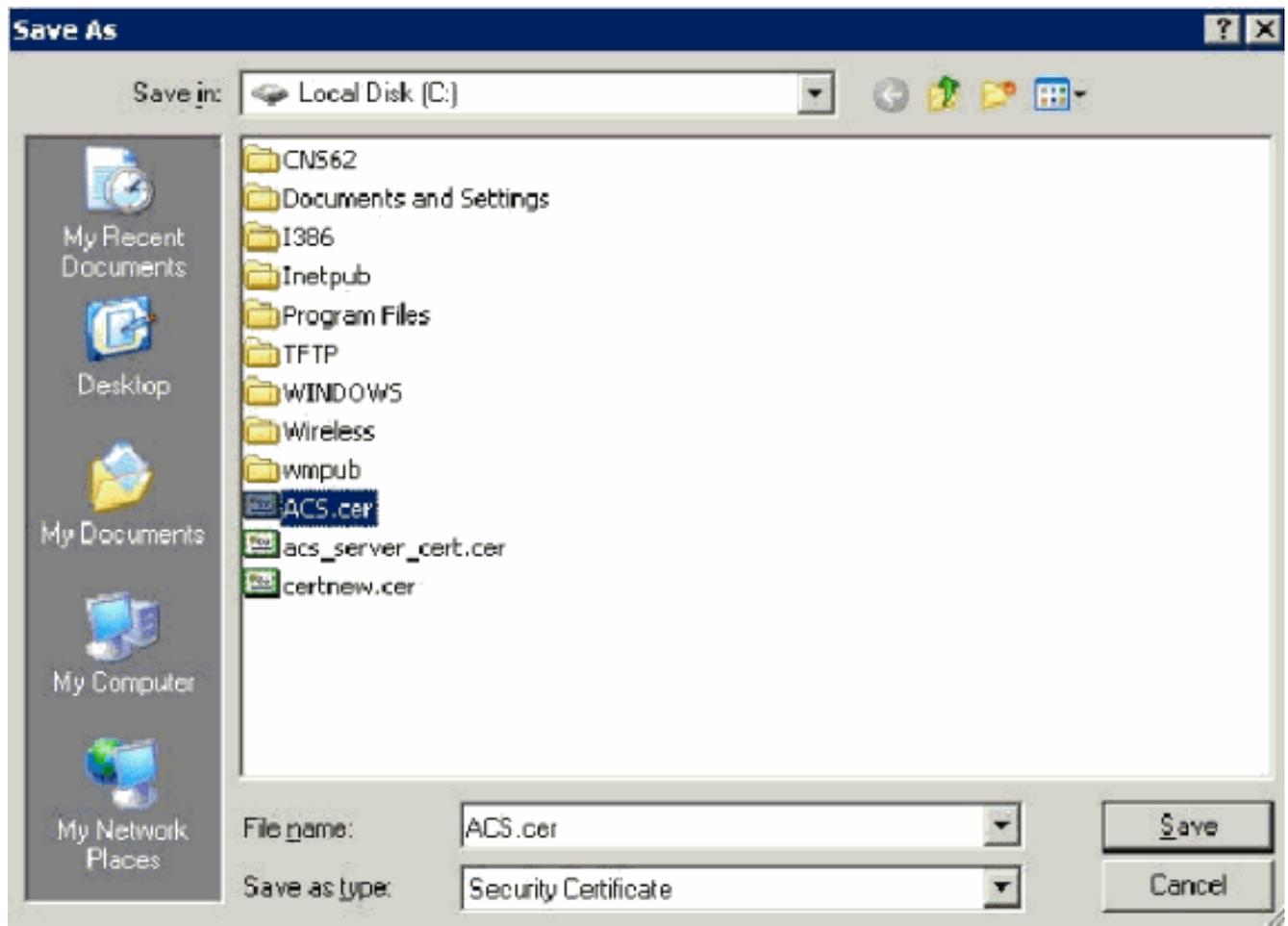
[Download latest delta CRL](#)

4. Aparecerá una ventana de advertencia de seguridad de descarga de archivos. Click



Save.

5. Guarde el archivo con un nombre como ACS.cer o cualquier nombre que desee. Recuerde este nombre ya que lo utiliza durante la configuración de ACS Certificate Authority en ACS 4.0.

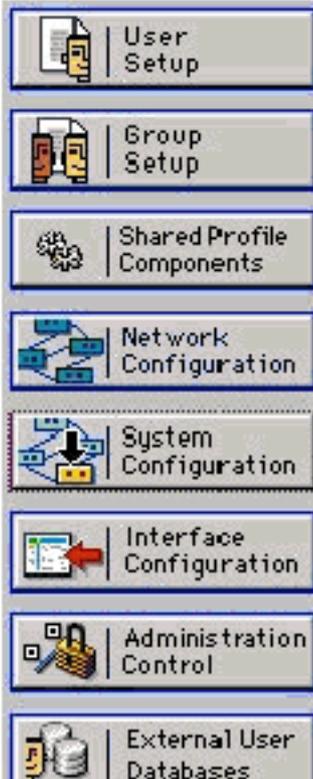


6. Abra **ACS Admin** desde el acceso directo de escritorio creado durante la instalación.
7. Haga clic en **Configuración del**



## System Configuration

### Select



- [Service Control](#)
- [Logging](#)
- [Date Format Control](#)
- [Local Password Management](#)
- [ACS Internal Database Replication](#)
- [ACS Backup](#)
- [ACS Restore](#)
- [ACS Service Management](#)
- [VoIP Accounting Configuration](#)
- [ACS Certificate Setup](#)
- [Global Authentication Setup](#)

sistema.

- Haga clic en **ACS Certificate Setup**.

# System Configuration

Select

## ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. Haga clic en Install ACS Certificate (Instalar certificado ACS).

# System Configuration

Edit

## Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
<b>Certificate file</b>	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
<b>Certificate CN</b>	<input type="text"/>
<b>Private key file</b>	<input type="text"/>
<b>Private key password</b>	<input type="text"/>

10. Elija **Use certificate from storage** y escriba el nombre de dominio completo de `cisco_w2003.wirelessdemo.local` (o `ACS.wirelessdemo.local` si utilizó ACS como nombre).

## System Configuration

Edit

### Install ACS Certificate

Install new certificate 	
<input type="radio"/> Read certificate from file	
<b>Certificate file</b>	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
<b>Certificate CN</b>	<input type="text" value="cisco_w2003.wirelessdemo.local"/>
<b>Private key file</b>	<input type="text"/>
<b>Private key password</b>	<input type="text"/>

11. Haga clic en Submit (Enviar).

## System Configuration

Edit

### Install ACS Certificate

Installed Certificate Information 	
<b>Issued to:</b>	cisco_w2003.wirelessdemo.local
<b>Issued by:</b>	wirelessdemoca
<b>Valid from:</b>	March 17 2006 at 08:33:25
<b>Valid to:</b>	March 16 2008 at 08:33:25
<b>Validity:</b>	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. Haga clic en Configuración del sistema.
13. Haga clic en Service Control y luego haga clic en

Restart.

## System Configuration

Select

CiscoSecure ACS on cisco\_w2003 

### Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week

Every month

When size is greater than  KB

Manage Directory

Keep only the last  files

Delete files older than  days

 [Back to Help](#)

14. Haga clic en **Configuración del sistema**.
15. Haga clic en **Configuración de autenticación global**.
16. Marque **Allow EAP-TLS** y todas las casillas debajo.

# 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. Haga clic en **Enviar + Reiniciar**.
18. Haga clic en **Configuración del sistema**.
19. Haga clic en **ACS Certification Authority Setup**.
20. En la ventana ACS Certification Authority Setup , escriba el nombre y la ubicación del archivo \*.cer creado anteriormente. En este ejemplo, el archivo \*.cer creado es **ACS.cer** en el directorio raíz c:\.
21. Escriba **c:\acs.cer** en el campo del archivo de certificado de CA y haga clic en **Enviar**.

# System Configuration

**ACS Certification Authority Setup**

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

System Configuration

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

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

CA certificate common name	wirelessdemo.ca
----------------------------	-----------------

**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.**

22. Reinicie el servicio ACS.

## [Configuración del CLIENTE para EAP-TLS con Windows Zero Touch](#)

CLIENT es un equipo que ejecuta Windows XP Professional con SP2 que actúa como cliente inalámbrico y obtiene acceso a los recursos de Intranet a través del AP inalámbrico. Complete los procedimientos de esta sección para configurar CLIENT como cliente inalámbrico.

### [Realizar una Instalación y Configuración Básicas](#)

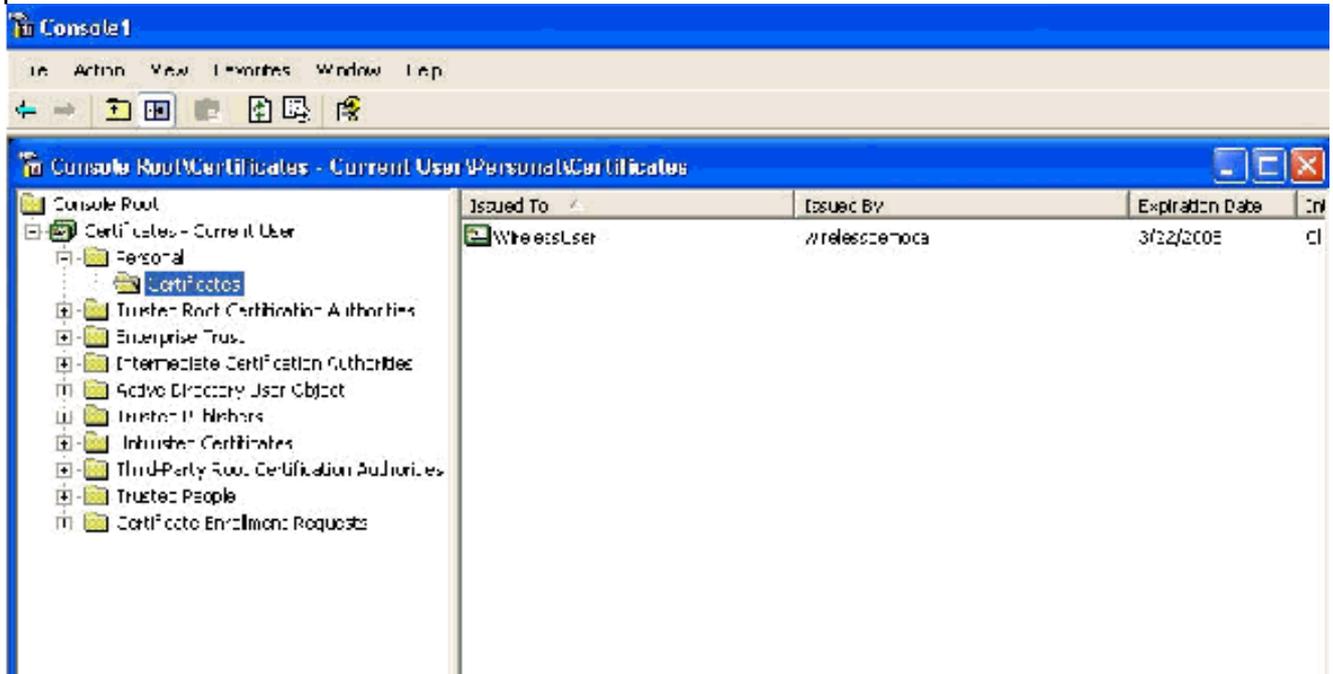
Complete estos pasos:

1. Conecte el CLIENTE al segmento de red de la Intranet mediante un cable Ethernet conectado al switch.
2. En CLIENT, instale Windows XP Professional con SP2 como equipo miembro denominado **CLIENT** en el dominio wirelessdemo.local.
3. Instale Windows XP Professional con SP2. Esto se debe instalar para tener soporte EAP-TLS y PEAP. **Nota:** Firewall de Windows se activa automáticamente en Windows XP Professional con SP2. No apague el firewall.

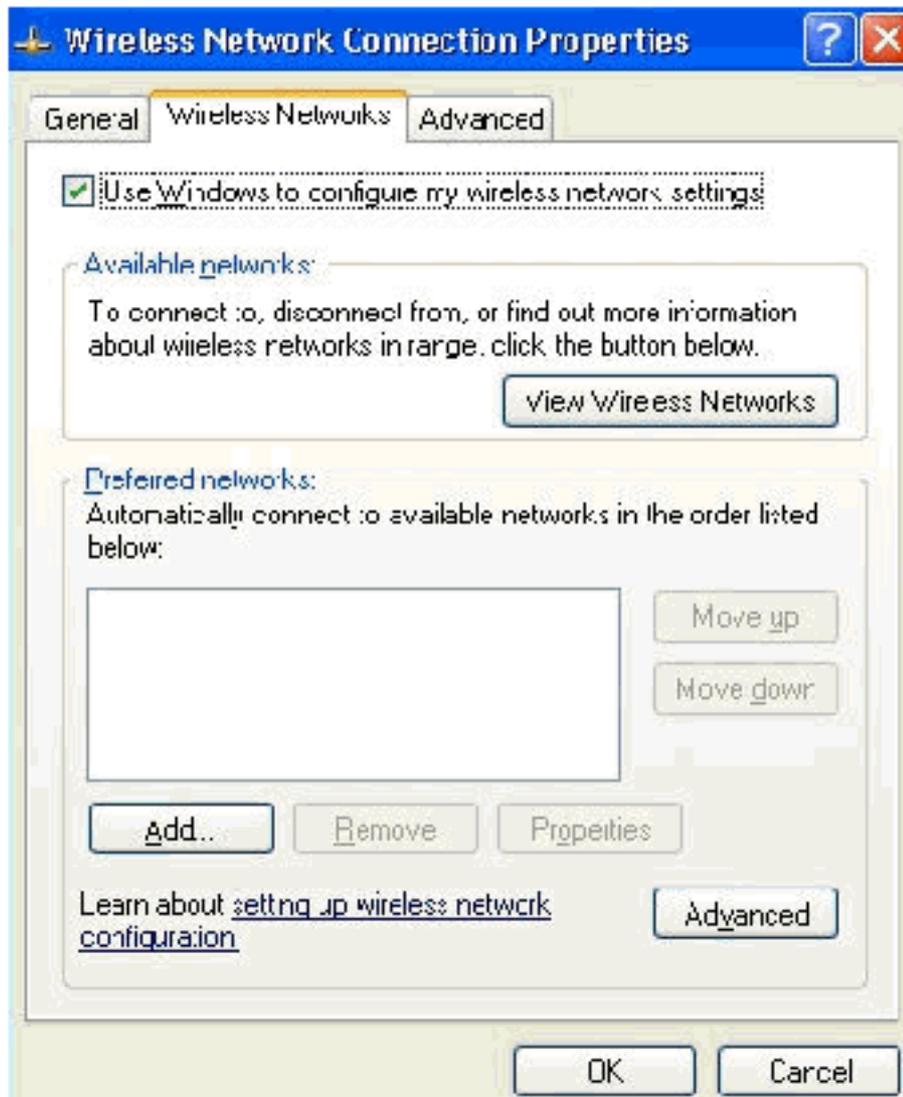
### [Configuración de la conexión de red inalámbrica](#)

Complete estos pasos:

1. Cierre la sesión y, a continuación, conéctese utilizando la cuenta WirelessUser en el dominio wirelessdemo.local. **Nota:** Actualice la configuración de la política del equipo y del grupo de configuración del usuario y obtenga inmediatamente un certificado de equipo y usuario para el equipo cliente inalámbrico, escribiendo **gpupdate** en un símbolo del sistema. De lo contrario, cuando se desconecta y después se conecta, realiza la misma función que **gpupdate**. Debe haber iniciado sesión en el dominio conectándose a través del cable. **Nota:** Para validar que el certificado se instala automáticamente en el cliente, abra el certificado MMC y valide que el certificado WirelessUser esté disponible en la carpeta Certificados personales.

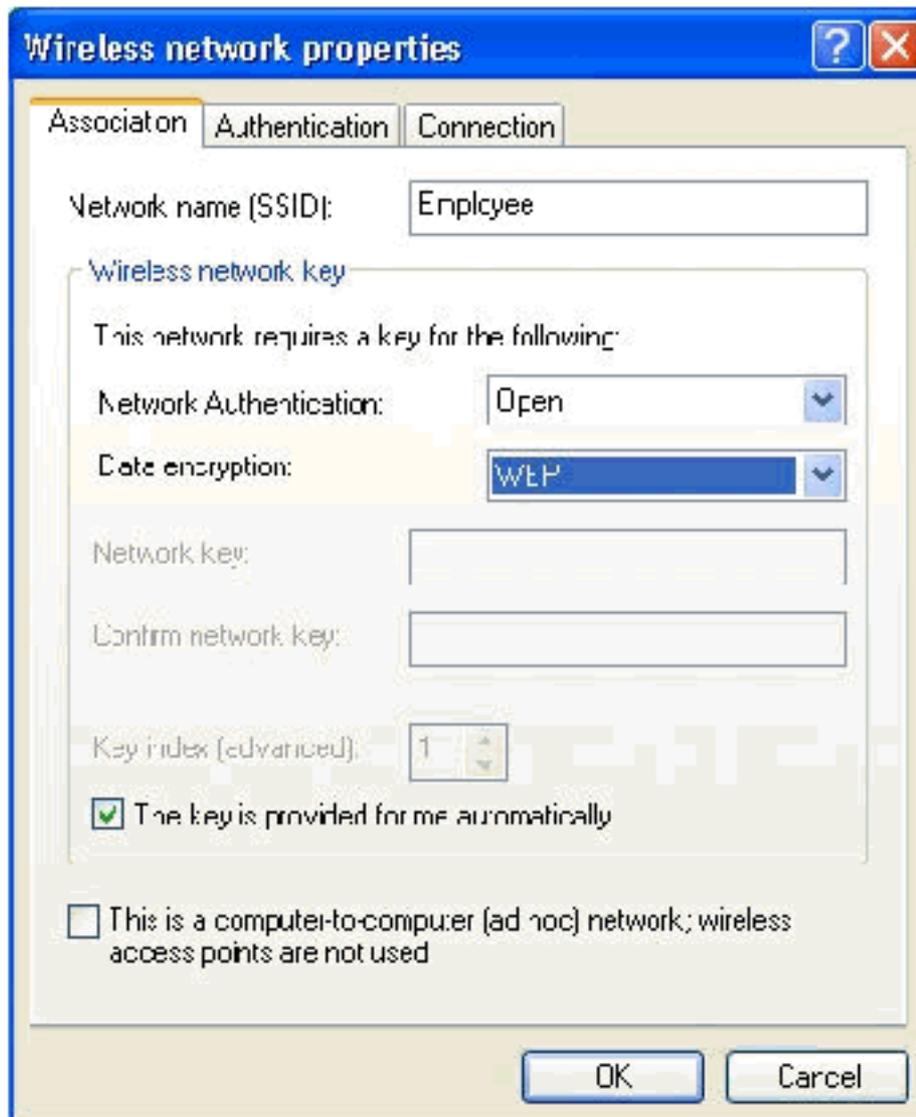


2. Elija **Inicio > Panel de control**, haga doble clic en **Conexiones de red** y, a continuación, haga clic con el botón derecho en **Conexión de red inalámbrica**.
3. Haga clic en **Properties**, vaya a la ficha **Wireless Networks** y asegúrese de que **User Windows para configurar mi red inalámbrica** esté



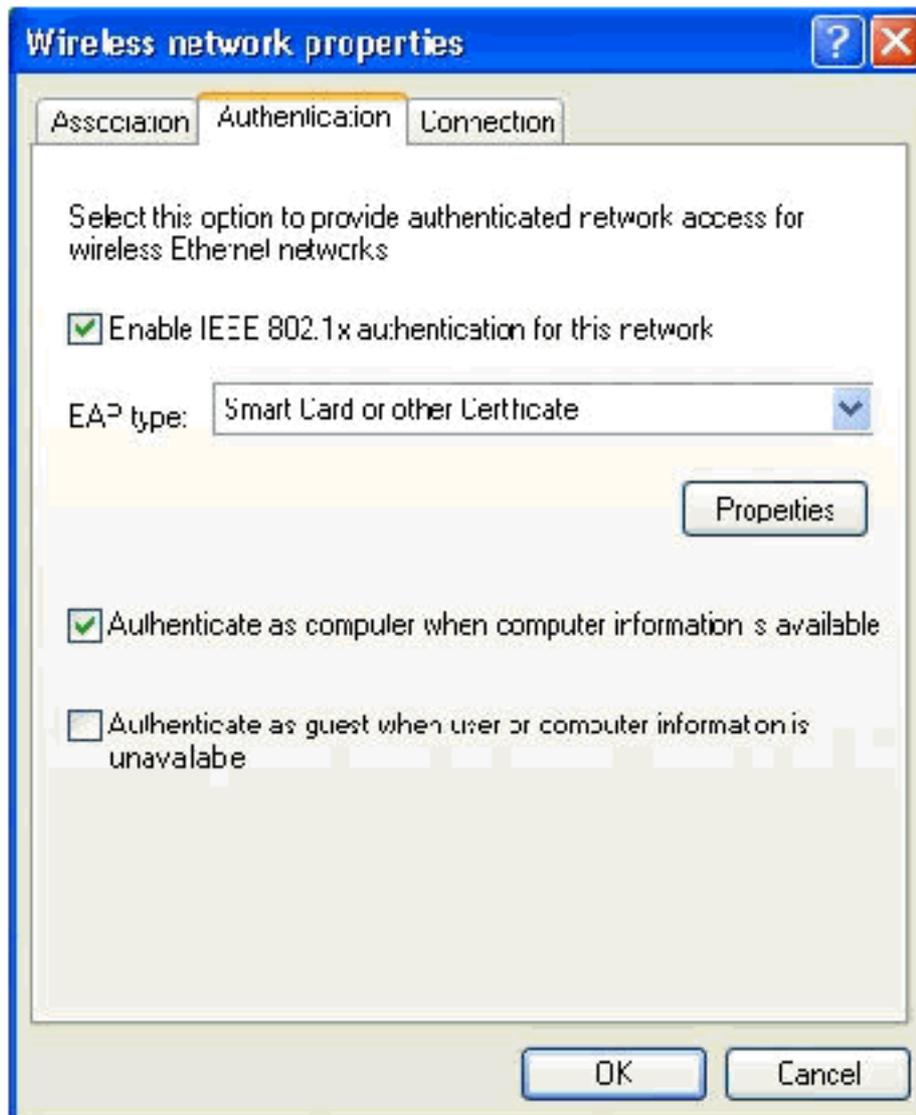
marcado.

4. Haga clic en Add (Agregar).
5. Vaya a la ficha Asociación y escriba **Empleado** en el campo Nombre de red (SSID).
6. Asegúrese de que Data Encryption esté configurado en **WEP** y la clave se proporciona automáticamente está



marcada.

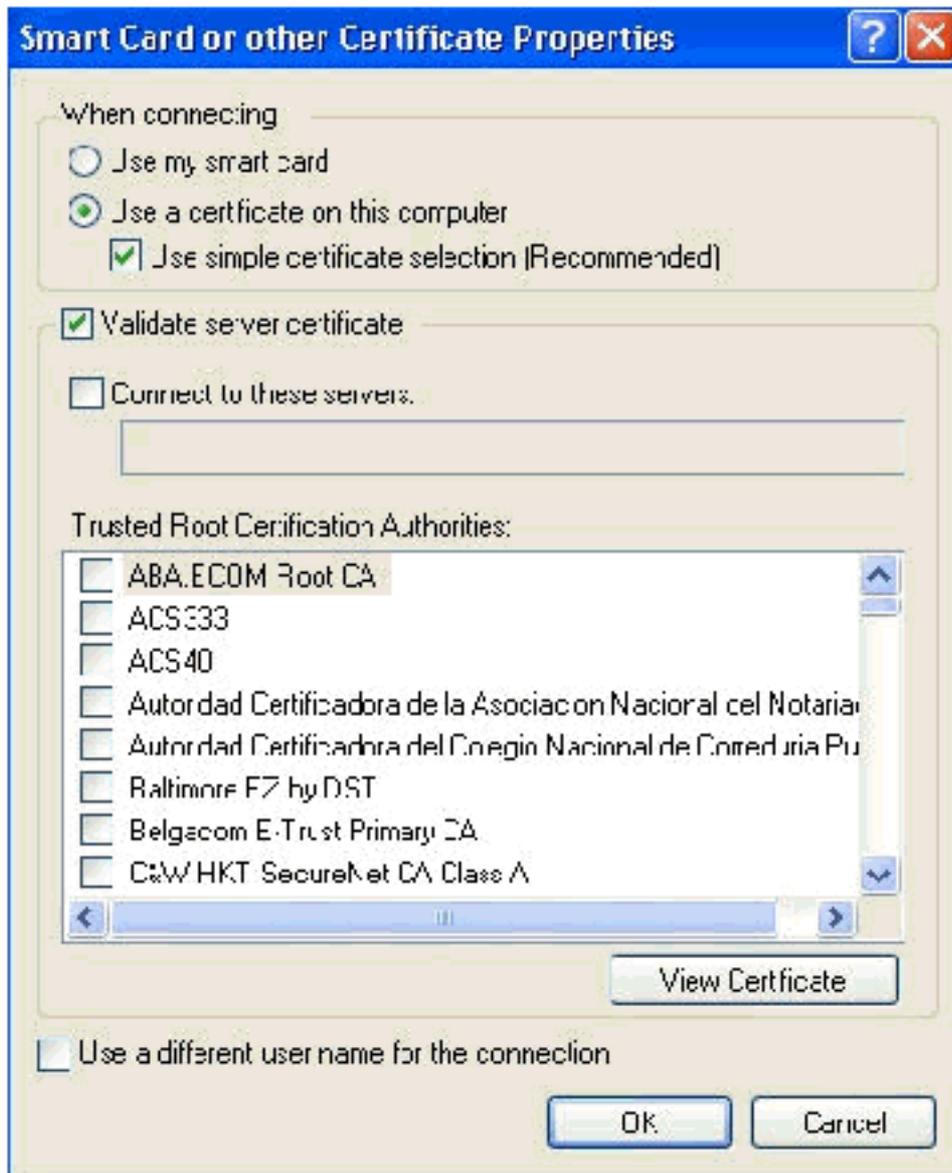
7. Vaya a la ficha Authentication (Autenticación).
8. Valide que el tipo EAP esté configurado para utilizar **Smart Card u otro certificado**. Si no es así, selecciónelo en el menú desplegable.
9. Si desea que la máquina se autentique antes del inicio de sesión (lo que permite aplicar secuencias de comandos de inicio de sesión o directivas de grupo), elija la opción **Autenticar como equipo cuando la información del equipo esté**



disponible.

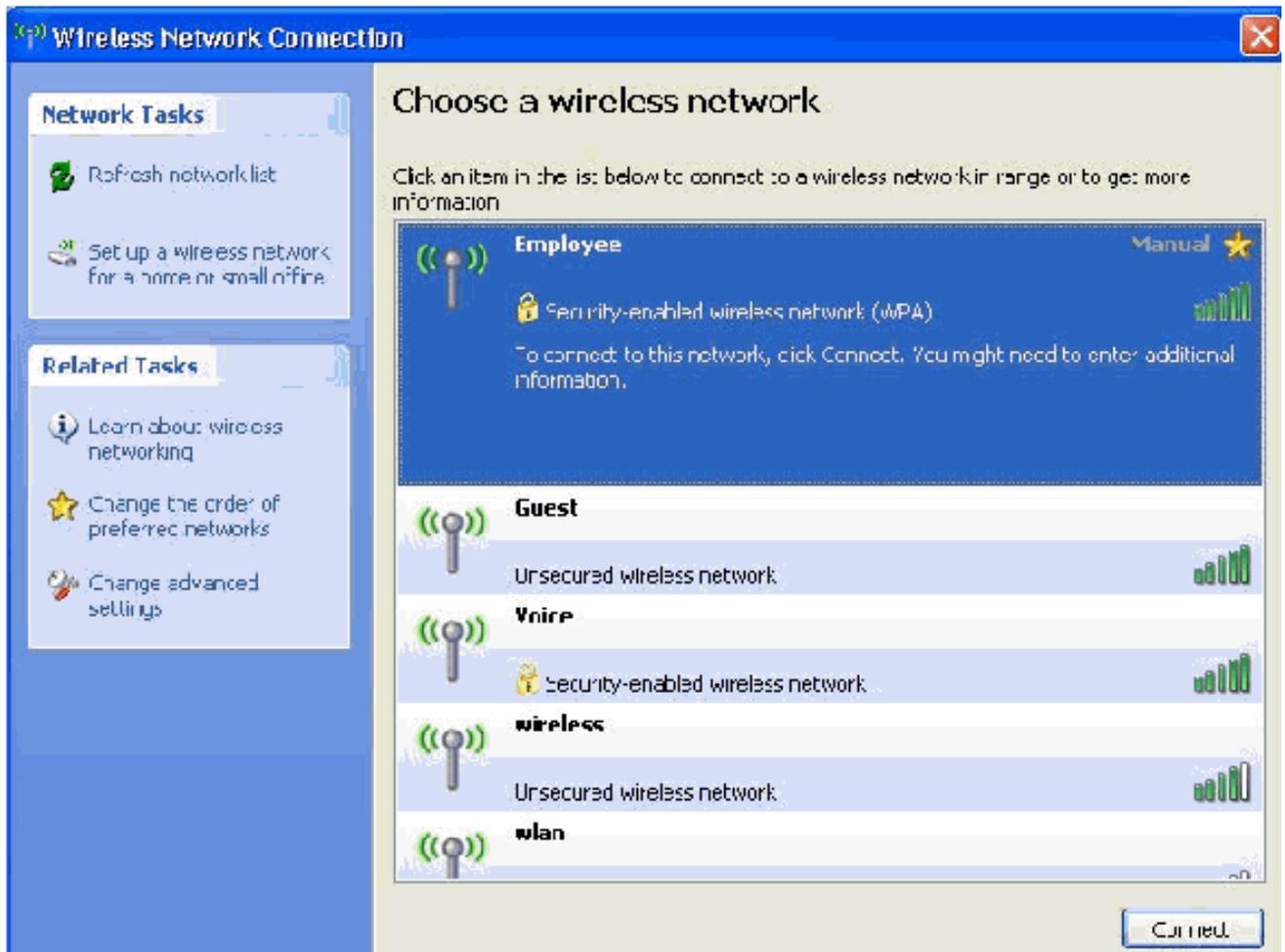
10. Haga clic en Properties (Propiedades).

11. Asegúrese de que las casillas de esta ventana estén

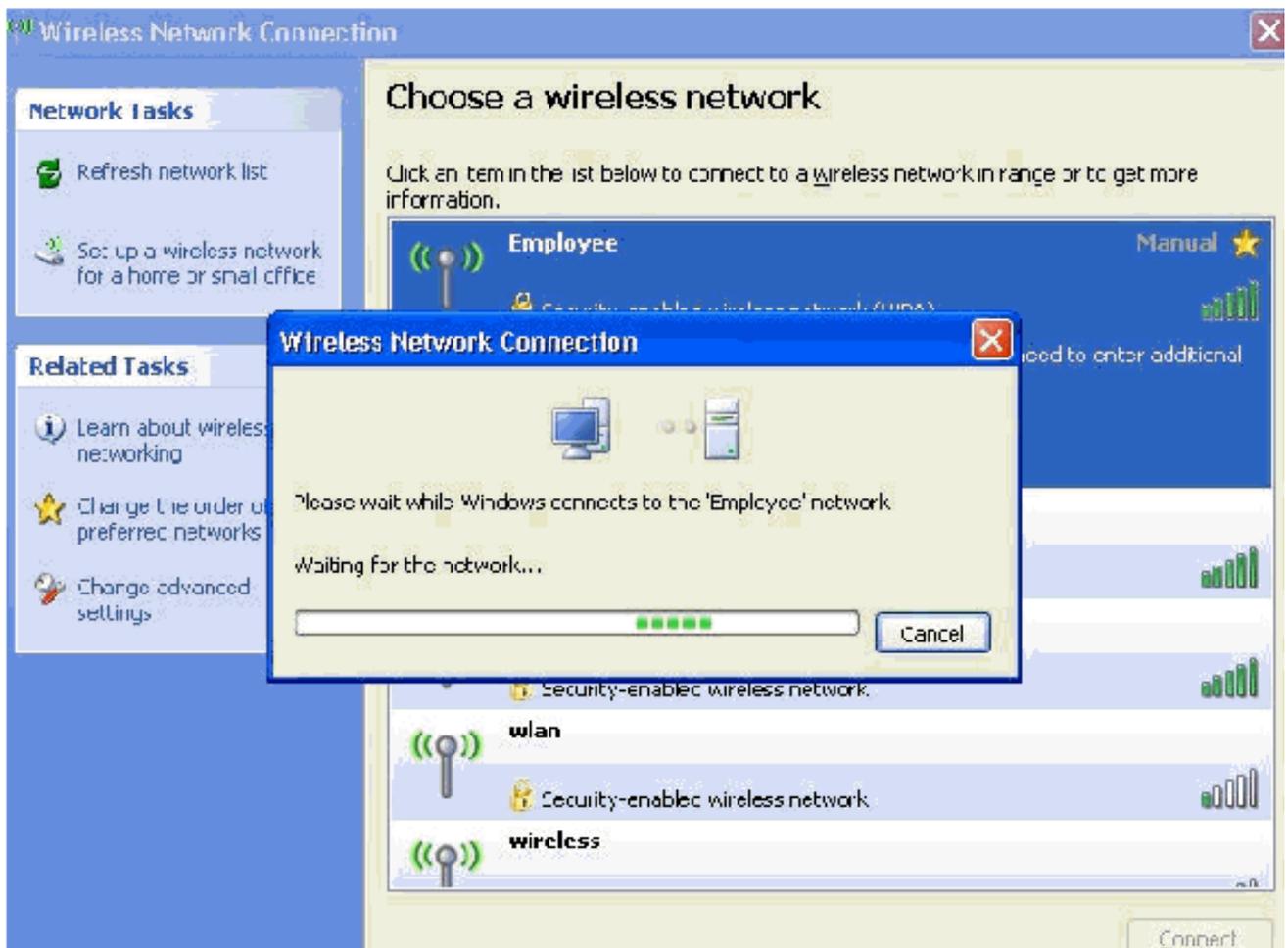


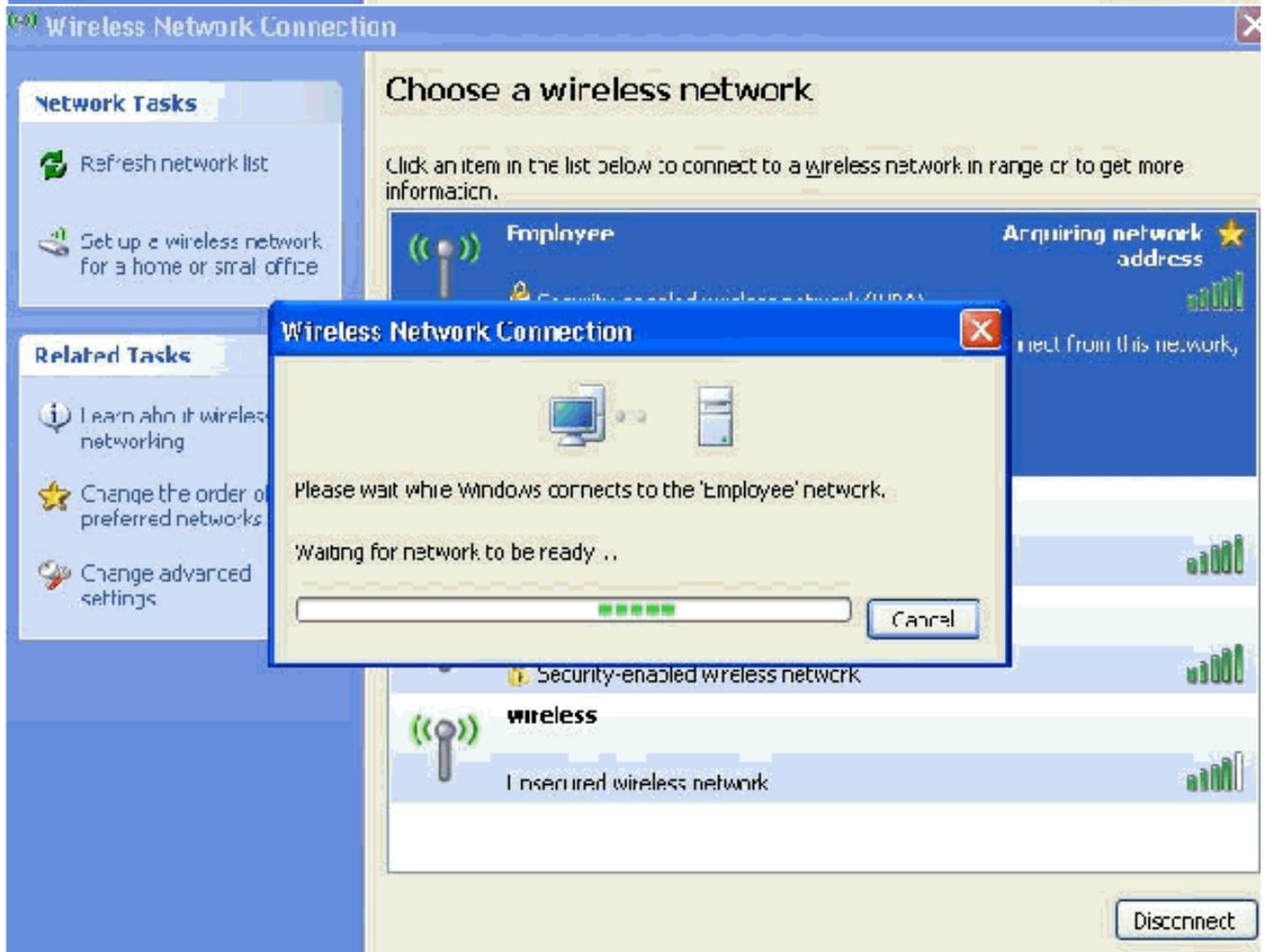
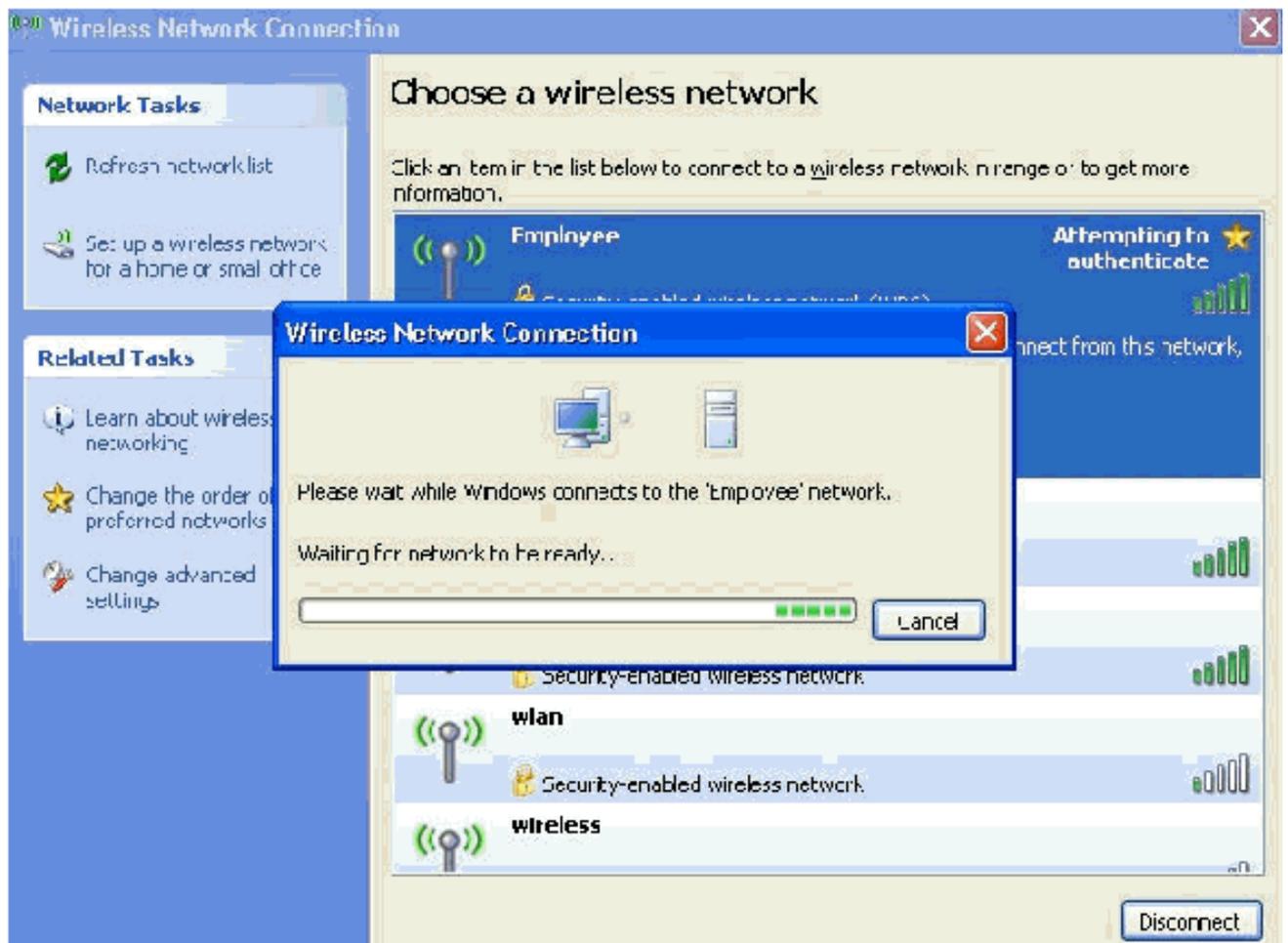
marcadas.

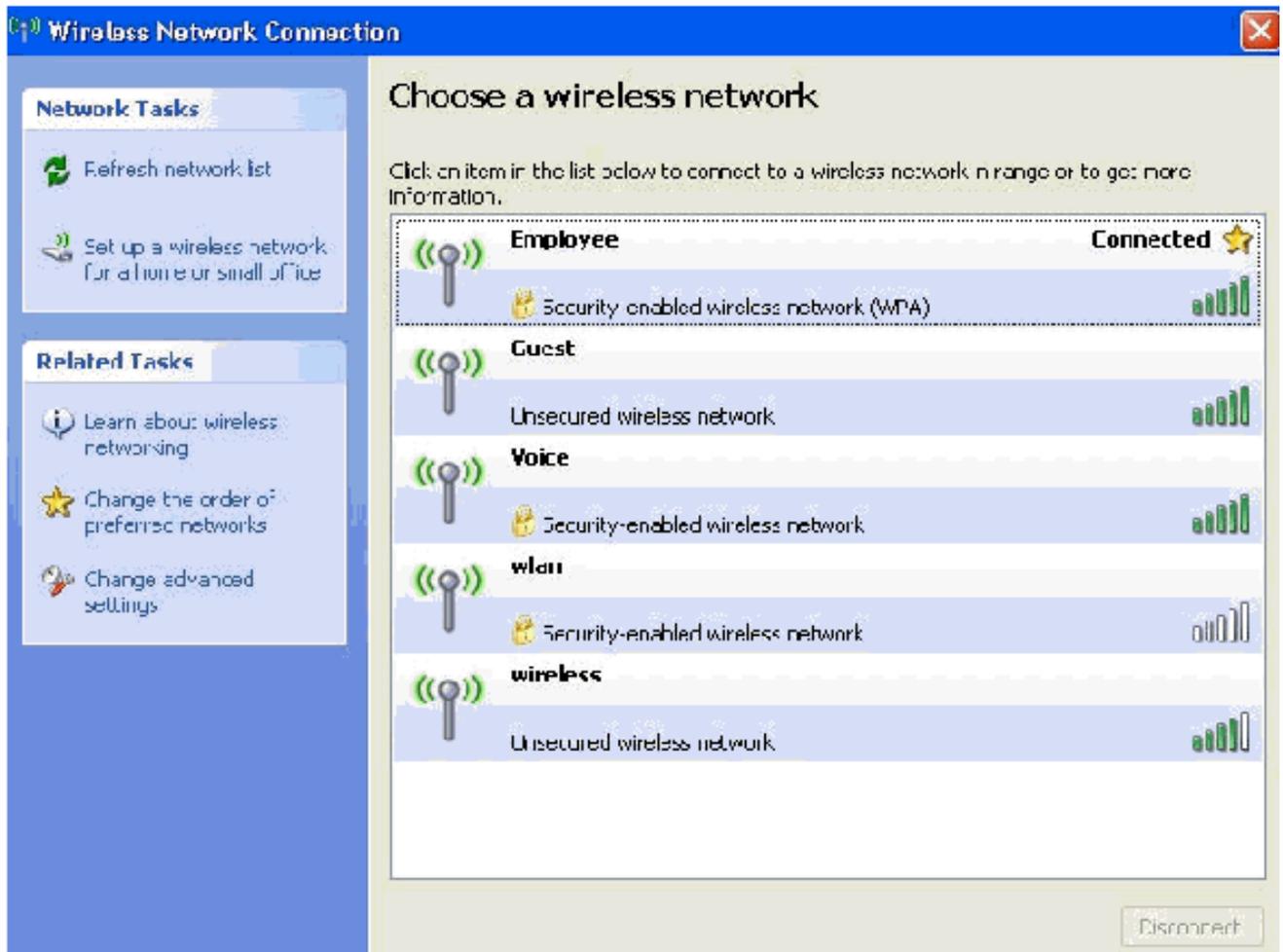
12. Haga clic en **Aceptar** tres veces.
13. Haga clic con el botón derecho del ratón en el icono de conexión de red inalámbrica del sistema y, a continuación, haga clic en **Ver redes inalámbricas disponibles**.
14. Haga clic en la red inalámbrica **Empleado** y haga clic en **Conectar**.



Estas capturas de pantalla indican si la conexión se completa correctamente.







15. Después de que la autenticación se realice correctamente, verifique la configuración TCP/IP del adaptador inalámbrico mediante Conexiones de red. Debe tener un rango de direcciones de 172.16.100.100-172.16.100.254 desde el alcance DHCP o el alcance creado para los clientes inalámbricos.
16. Para probar la funcionalidad, abra un explorador y navegue hasta <http://wirelessdemoca> (o la dirección IP del servidor de CA de la empresa).

## Información Relacionada

- [Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN \(WLC\)](#)
- [Guía de Configuración del Controlador de LAN Inalámbrica](#)
- [Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN](#)
- [Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica](#)
- [Ejemplo de Configuración de VLANs de Grupo de AP con Controladores de LAN Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)