

# PEAP en redes inalámbricas unificadas 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](#)

[Cree la configuración necesaria para WPAv2/WPA](#)

[Autenticación PEAP](#)

[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 PEAP con Windows Zero Touch](#)

[Realizar una instalación y configuración básicas](#)

[Instalación del adaptador de red inalámbrico](#)

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

[Problema: El cliente Odyssey solicita tres veces la plataforma de autenticación Token](#)

[La autenticación PEAP falla con el servidor ACS](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo configurar el acceso inalámbrico seguro mediante controladores LAN inalámbricos, el software Microsoft Windows 2003 y Cisco Secure Access Control Server (ACS) 4.0 a través de Protected Extensible Authentication Protocol (PEAP) con Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versión 2.

**Nota:** Para obtener información sobre la implementación de tecnología inalámbrica segura,

refiérase al [sitio Web de Microsoft Wi-Fi 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](#).

Las guías de instalación y configuración de Microsoft Windows 2003 se pueden encontrar en [Instalación de Windows Server 2003 R2](#).

Antes de comenzar, instale Microsoft Windows Server 2003 con el sistema operativo SP1 en cada uno de los servidores del laboratorio de pruebas y actualice todos los Service Packs. Instale los controladores y los puntos de acceso ligeros (LAP) y asegúrese de que se configuran las últimas actualizaciones de software.

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

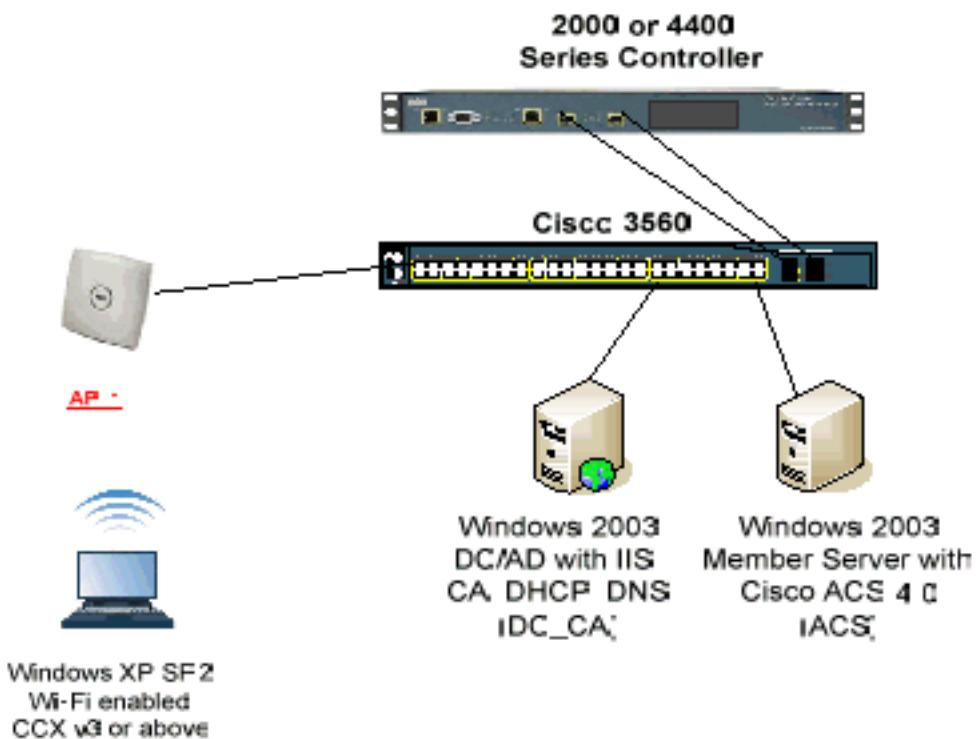
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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 PEAP 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 Service Pack 2](#).

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 **wirelessdemo.local** que ejecuta IIS
- Un servidor DNS para el dominio DNS **alámbressdemo.local**
- Un servidor DHCP
- CA raíz empresarial para el dominio **inalámbrico demo.local**

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:

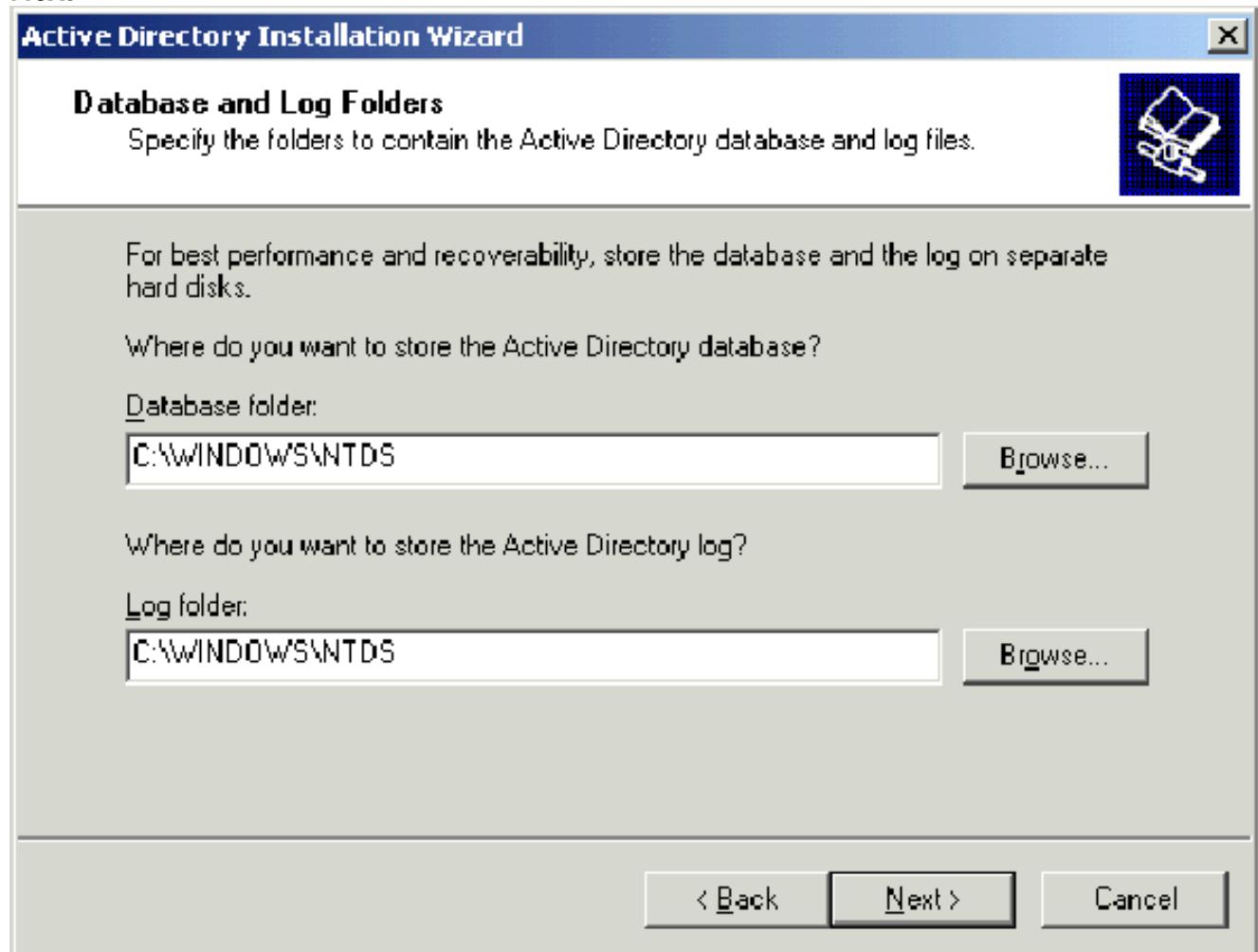
1. Instale Windows Server 2003 con SP1, Enterprise Edition como servidor independiente.
2. Configure el protocolo TCP/IP con la dirección IP de **172.16.100.26** y la máscara de subred de **255.255.255.0**.

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

Complete estos pasos:

1. Para iniciar el asistente de instalación de Active Directory, elija **Iniciar > Ejecutar**, escriba **dcromo.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 Ubicaciones de la Base de Datos y las Carpetas de Registro, acepte los directorios predeterminados Database y Log Folders y haga clic en **Next**.



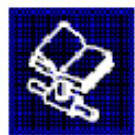
10. En la página Volumen del sistema compartido, verifique que la ubicación predeterminada de la carpeta sea correcta y haga clic en **Siguiente**.

## Active Directory Installation Wizard



### Shared System Volume

Specify the folder to be shared as the system volume.



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

The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

Folder location:

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**.

## Active Directory Installation Wizard



### Permissions

Select default permissions for user and group objects.



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

**Permissions compatible with pre-Windows 2000 server operating systems**

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

Anonymous users can read information on this domain.

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

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

< Back

Next >

Cancel

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**.

## Active Directory Installation Wizard

### Summary

Review and confirm the options you selected.



You chose to:

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

The NetBIOS name of the domain is EXAMPLE

Database folder: C:\WINDOWS\NTDS

Log file folder: C:\WINDOWS\NTDS

SYSVOL folder: C:\WINDOWS\SYSVOL

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

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

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

< Back

Next >

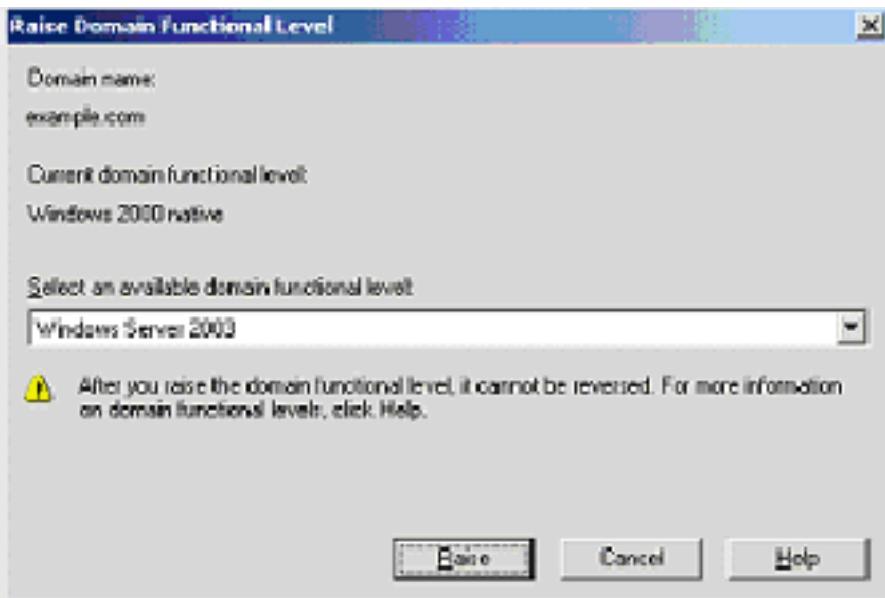
Cancel

14. Cuando haya terminado la 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 > Programas > Herramientas administrativas > **Dominios y confianza 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 un **componente de servicio de red** mediante **Agregar o quitar programas** en el Panel de control.
2. Abra el complemento **DHCP** de la carpeta **Administrative Tools** (Inicio > Programas > Herramientas administrativas > DHCP) y, a continuación, resalte el servidor DHCP, **DC\_CА.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\_CА.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:

CorpNet

Description:

< Back

Next >

Cancel

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

8. 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 de reserva.

## 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**.

## 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

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:

[Resolve](#)

[Add](#)

[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)**.

## New Scope Wizard

### Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

Next >

Cancel

15. Cuando termine con la página 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 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**.

## Windows Components Wizard



### Windows Components

You can add or remove components of Windows.



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

#### Components:

<input checked="" type="checkbox"/>		Accessories and Utilities	4.9 MB		
<input checked="" type="checkbox"/>		Application Server	33.4 MB		
<input checked="" type="checkbox"/>		Certificate Services	1.4 MB		
<input type="checkbox"/>		E-mail Services	1.1 MB		
<input type="checkbox"/>		Fax Services	7.9 MB		

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

Total disk space required: 3.4 MB

[Details...](#)

Space available on disk: 1346.9 MB

[Back](#) [Next >](#) [Cancel](#) [Help](#)

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

## Windows Components Wizard



### CA Type

Select the type of CA you want to set up.



- Enterprise root CA
- Enterprise subordinate CA
- Stand-alone root CA
- Stand-alone subordinate CA

#### Description of CA type

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

Use custom settings to generate the key pair and CA certificate

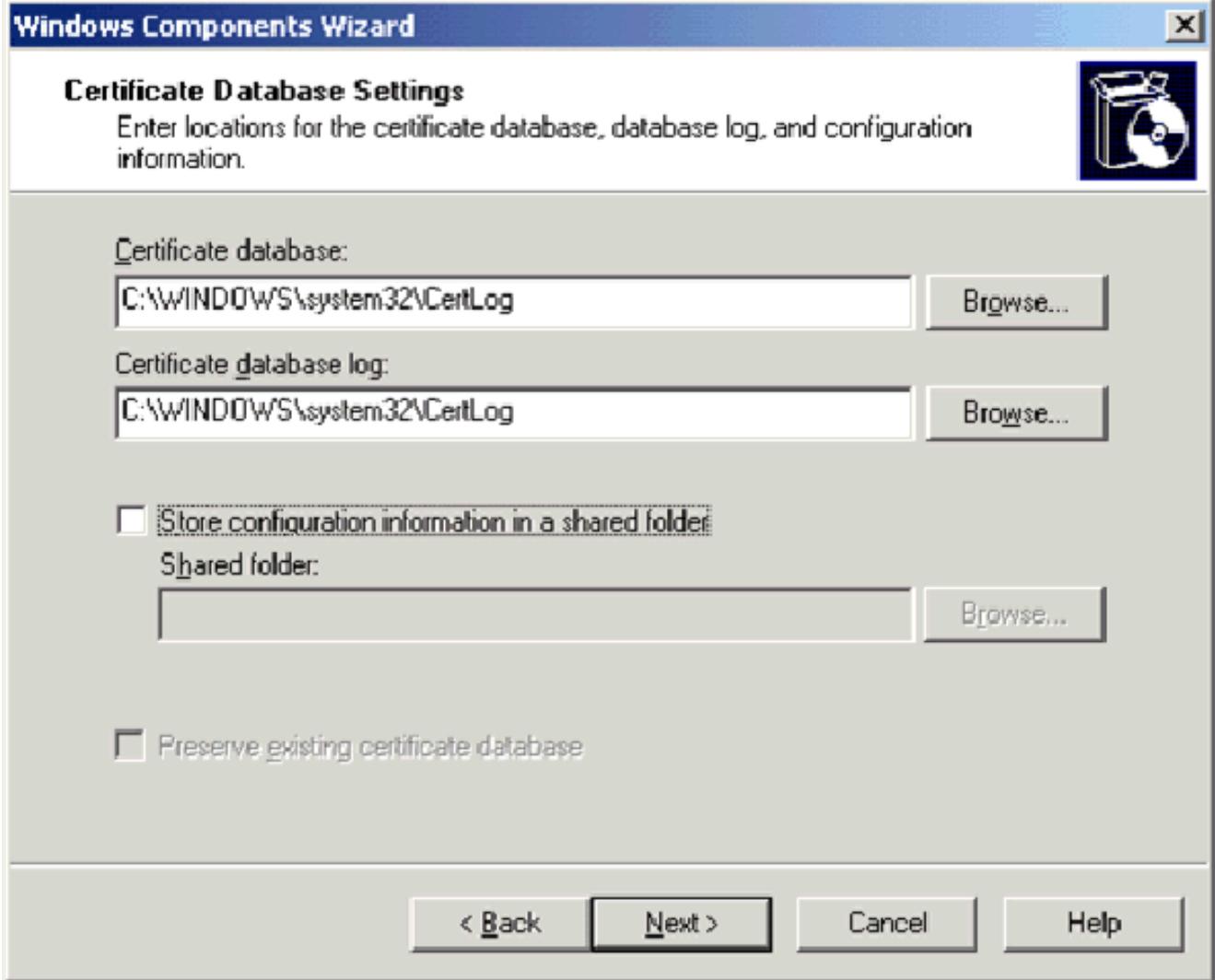
< Back

Next >

Cancel

Help

4. En la página CA Identificación de información, escriba **wirelessdemoca** en el nombre común de este cuadro CA. También puede introducir los demás detalles opcionales. A continuación, haga clic en **Next** y acepte los valores predeterminados en la página Certificate Database Settings (Parámetros de la base de datos de certificados).

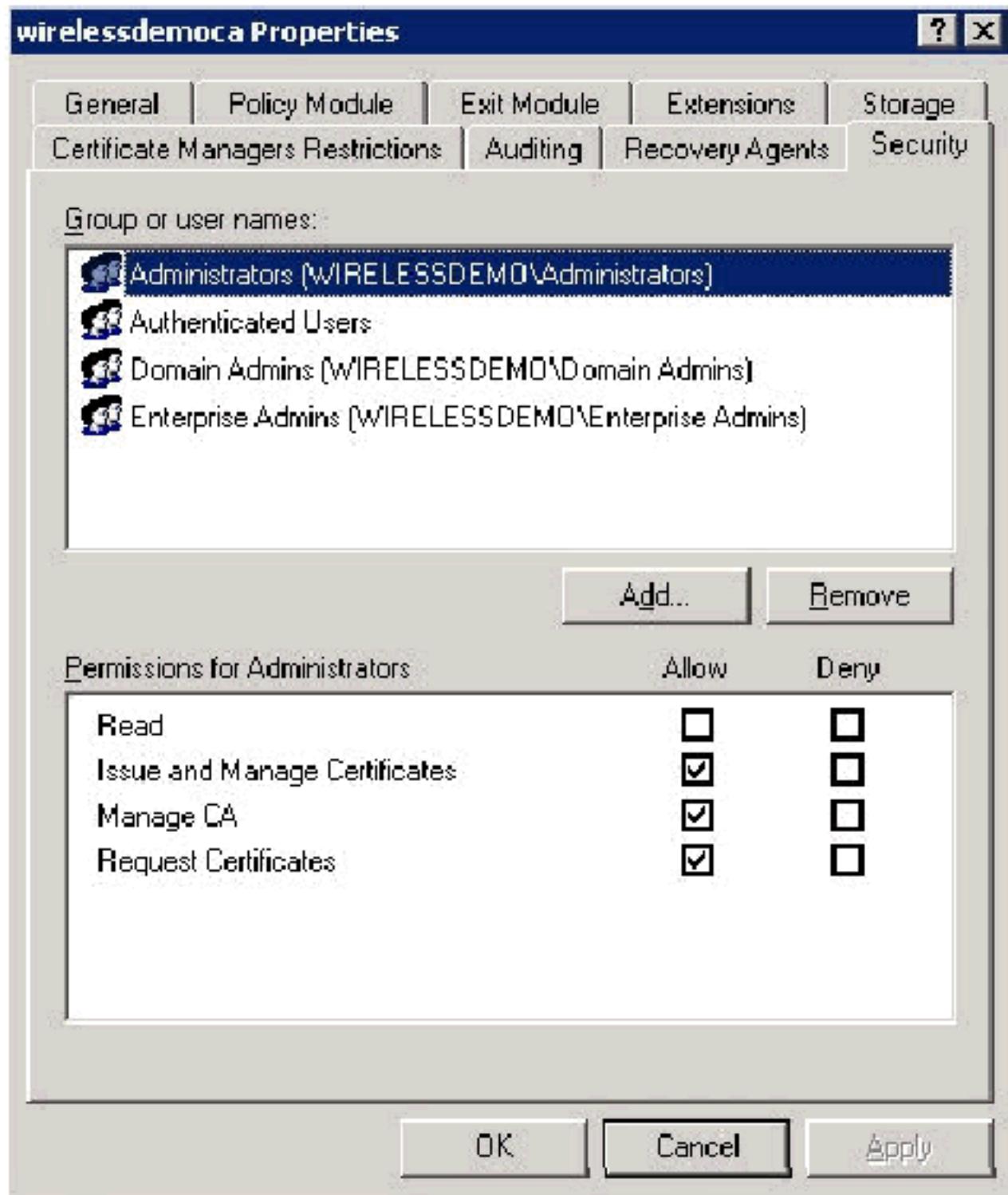


5. Haga clic en **Next (Siguiente)**. Una vez finalizada la instalación, haga clic en **Finalizar**.
6. Haga clic en **Aceptar** después de leer el mensaje de advertencia sobre la instalación de IIS.

#### 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.

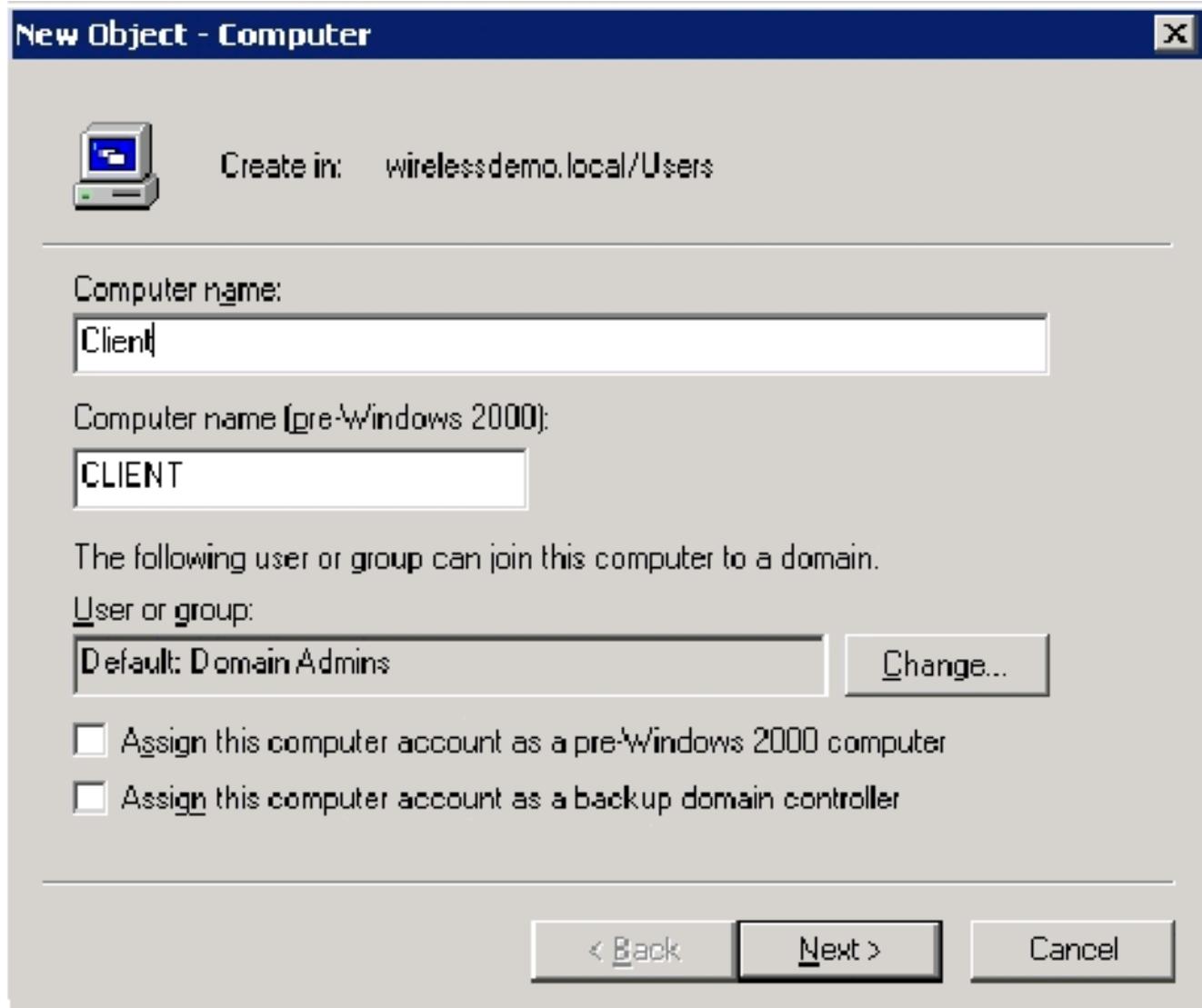
#### [Paso 7: Agregar ordenadores al dominio](#)

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.



5. En el cuadro de diálogo Administrado, haga clic en **Siguiente**.  
6. En el cuadro de diálogo Nuevo objeto - Equipo, 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

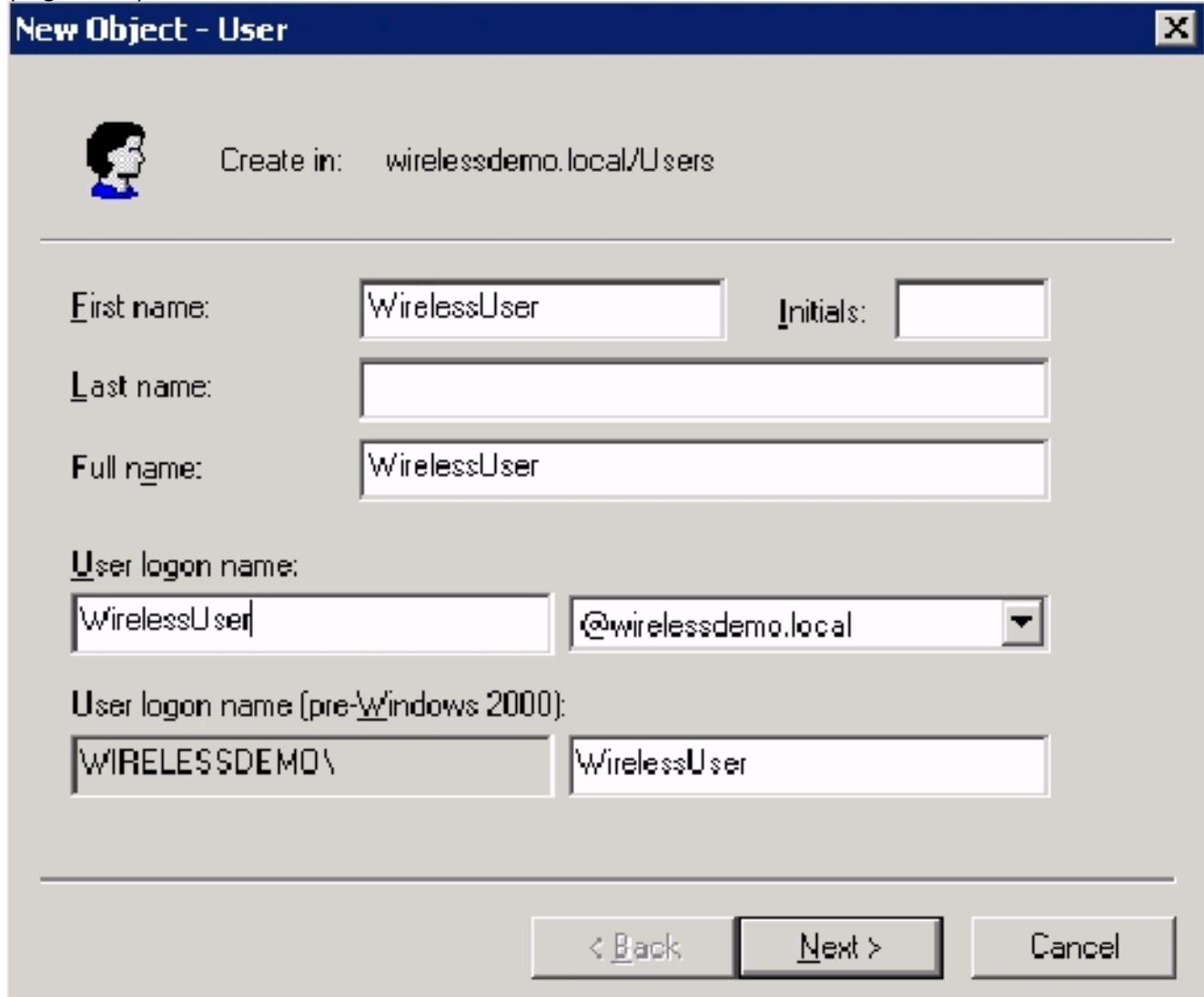
Complete estos pasos:

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** de equipo que agregó en el Paso 7. Haga clic en **Propiedades** y, a continuación, vaya a la ficha **Marcar**.
2. Elija **Allow access** y haga clic en **OK**.

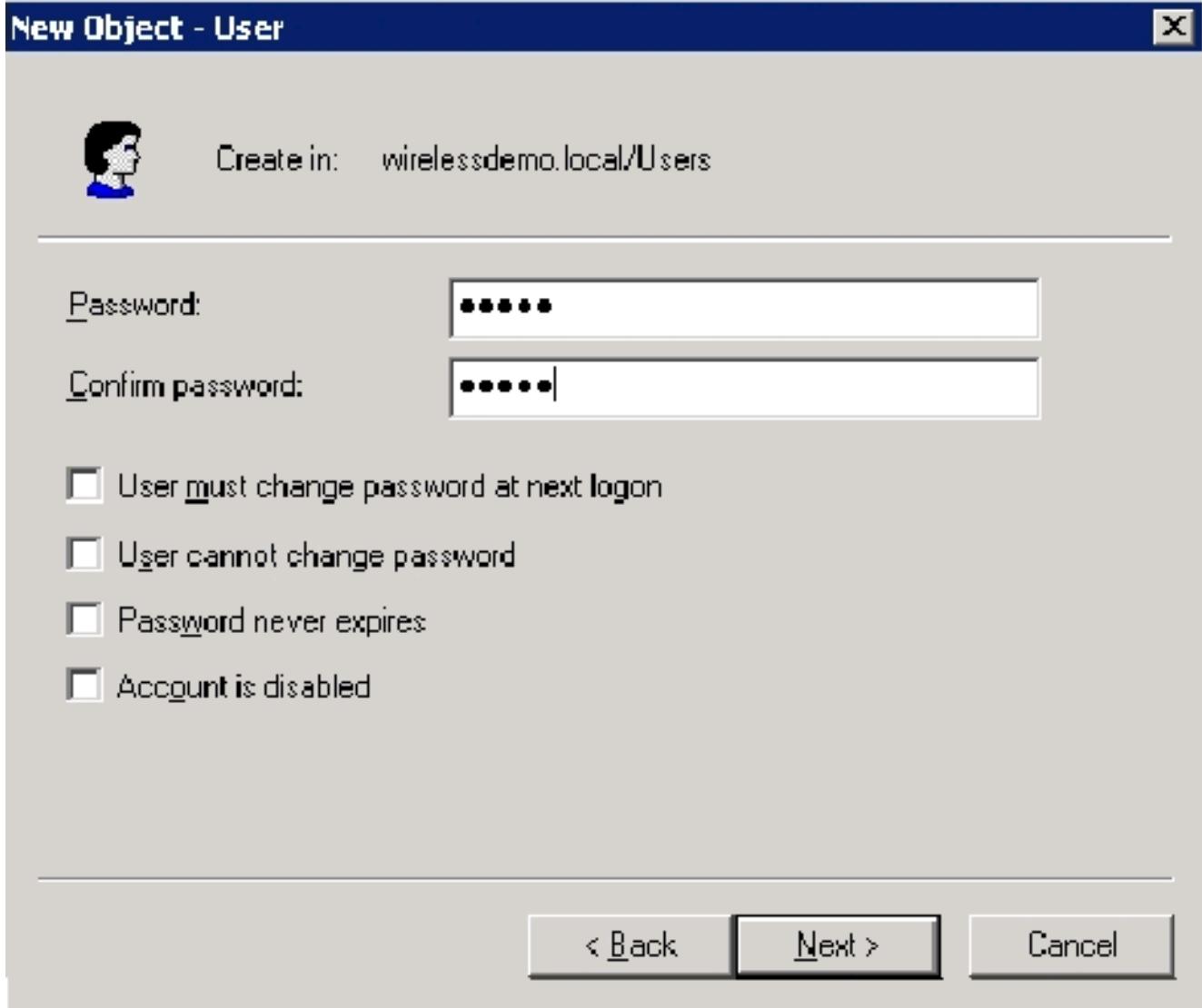
#### Paso 9: Agregar usuarios al dominio

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 el nombre del usuario inalámbrico. En este ejemplo se utiliza el nombre **WirelessUser** en el campo First name y **WirelessUser** en el campo User Logon name. Haga clic en **Next** (Siguiente).



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**.



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 **Active Directory Users and Computers**, haga clic en la carpeta **Users**, haga clic con el botón derecho del mouse en **WirelessUser**, haga clic en **Properties** y, a continuación, vaya a la ficha **Dial-in**.
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 **Active Directory Users and Computers**, haga clic con el botón derecho en **Users**, haga clic en **New** y, a continuación, haga clic en **Group**.
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**.

## New Object - Group



Create in: wirelessdemo.local/Users

Group name:

WirelessUsers

Group name (pre-Windows 2000):

WirelessUsers

Group scope:

- Domain local
- Global
- Universal

Group type:

- Security
- Distribution

OK

Cancel

### 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 el grupo **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.

## Select Users, Contacts, Computers, or Groups



Select this object type:

Users, Groups, or Other objects

Object Types...

From this location:

wirelessdemo.local

Locations...

Enter the object names to select (examples):

wirelessuser

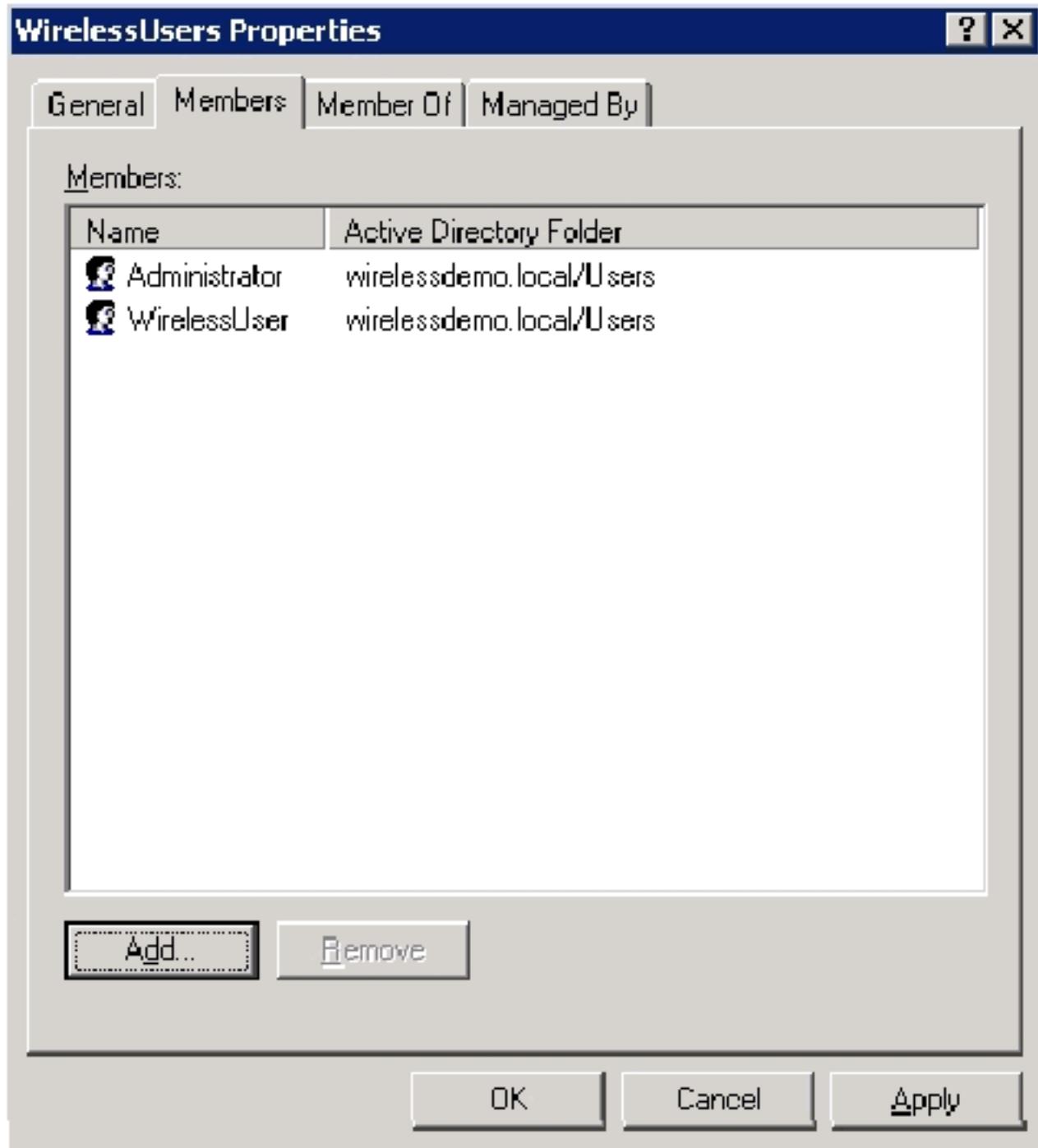
Check Names

Advanced...

OK

Cancel

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

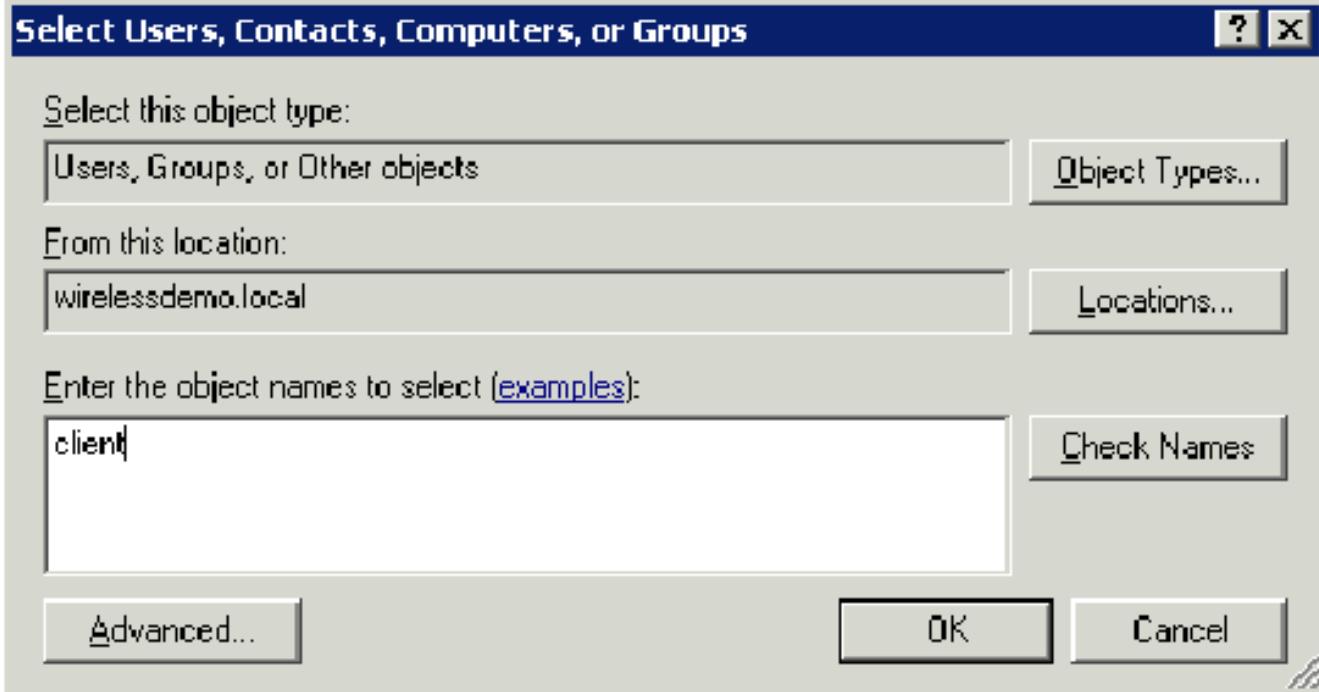


5. Haga clic en **Aceptar** para guardar los cambios en el grupo WirelessUsers.
6. Repita este procedimiento para agregar más usuarios al grupo.

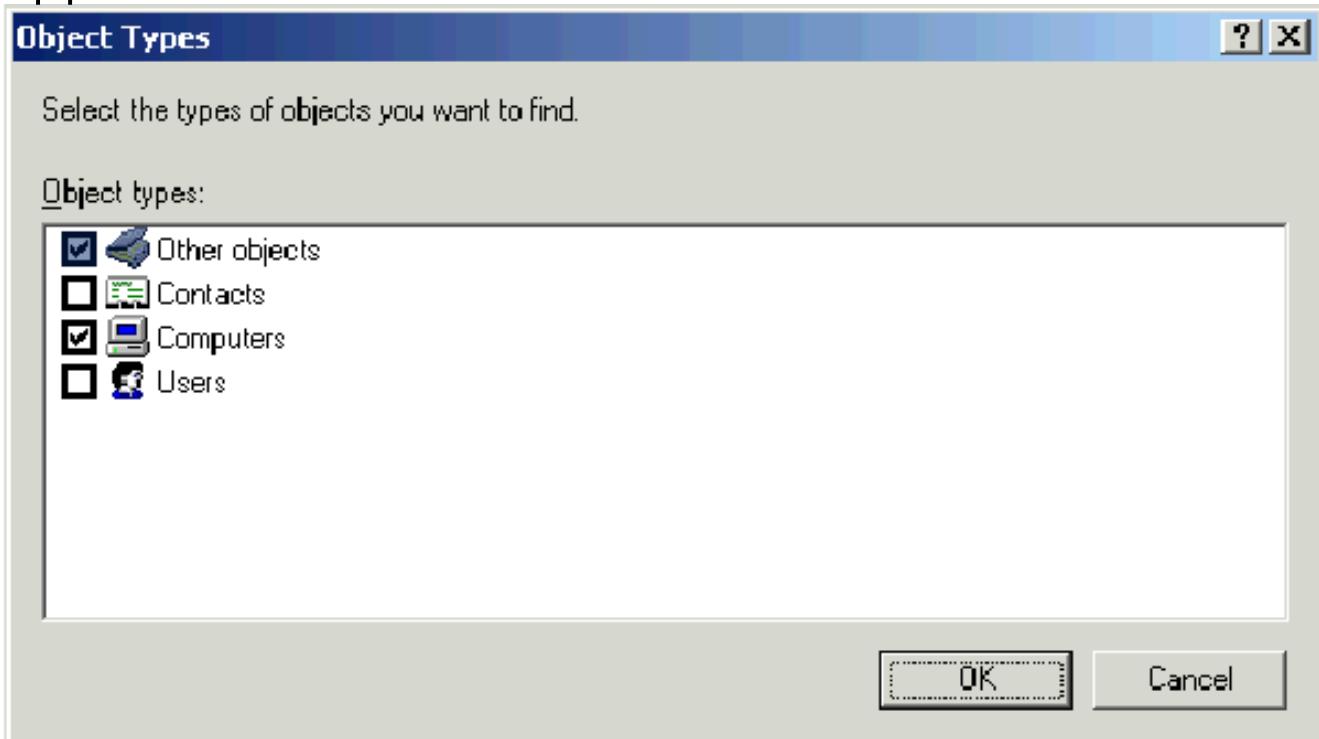
#### [Paso 13: Agregar equipos cliente al grupo de usuarios inalámbricos](#)

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. Utilice una cuenta de administrador de dominio para iniciar sesión en el equipo llamado ACS para instalar 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 de diálogo 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 (Siguiente)**.
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 a 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 (Siguiente)**.
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 deseé habilitar, active la casilla correspondiente.
20. Haga clic en **Next (Siguiente)**.

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 falla del 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 (Siguiente).
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.
27. Haga clic en Next (Siguiente).
28. El programa de configuración finaliza y aparece el cuadro de diálogo Cisco Secure ACS Service Initiation.
29. 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.
30. Haga clic en Next (Siguiente).
31. 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.
32. Haga clic en Finish (Finalizar).**Nota:** El resto de la configuración se documenta en la sección para el tipo EAP configurado.

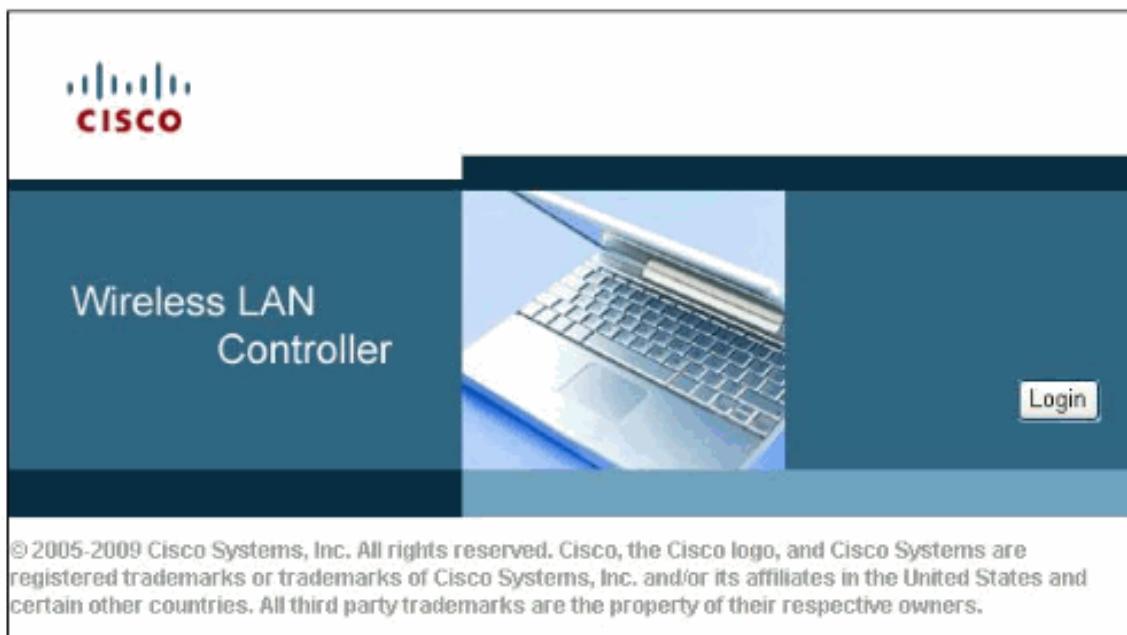
## Configuración del controlador LWAPP de Cisco

[Cree la configuración necesaria para WPAv2/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. Vaya a <https://172.16.101.252> para iniciar sesión en el controlador.



2. Haga clic en Login (Conexión)
3. Inicie sesión con el usuario predeterminado **admin** y la contraseña predeterminada **admin**.
4. Cree una nueva interfaz para la asignación de VLAN bajo el menú **Controlador**.
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

The screenshot shows the Cisco Controller interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The CONTROLLER tab is selected. On the left, a sidebar menu lists various controller functions: General, Inventory, Interfaces (which is selected), Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced.

The main content area is titled "Interfaces > Edit". It displays the configuration for an interface named "employee".

**General Information:**

- Interface Name: employee
- MAC Address: 00:0b:85:48:53:d6

**Configuration:**

- Guest Lan:
- Quarantine:
- Quarantine VLAN Id:

**Physical Information:**

- Port Number:
- Backup Port:
- Active Port: 0
- Enable Dynamic AF Management:

**Interface Address:**

- VLAN Identifier:
- IP Address:
- Netmask:
- Gateway:

**DHCP Information:**

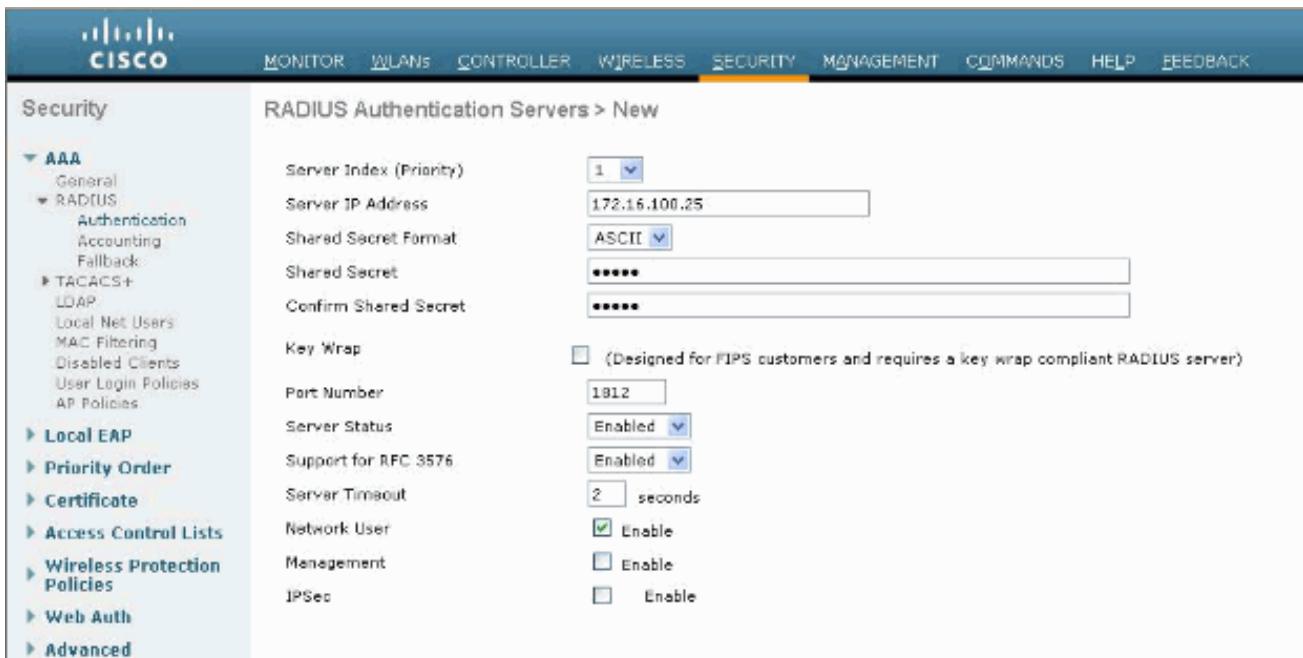
- Primary DHCP Server:
- Secondary DHCP Server:

11. Haga clic en Apply (Aplicar).
  12. Haga clic en la pestaña WLANs.
  13. Elija Create New y haga clic en Go.
  14. Ingrese un Nombre de Perfil y en el campo WLAN SSID escriba Empleado.
  15. Elija un ID para la WLAN y haga clic en Aplicar.
  16. Configure la información para esta WLAN cuando aparezca la ventana WLANs > Edit
- .Nota: WPAv2 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 802.11i.

The screenshot shows the Cisco WLC Management interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar has a tree view with WLANS expanded, showing WLANs and Advanced. The main area is titled 'WLANs > Edit'. The 'General' tab is selected. The configuration details are as follows:

Profile Name	employee
Type	WLAN
SSID	Employee
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	employee
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

17. En la pantalla WLANs > Edit , haga clic en la pestaña **General**.
18. Asegúrese de que la casilla Status esté marcada para **Enabled** y de que se haya elegido la **interfaz** (empleado) adecuada. Además, asegúrese de activar la casilla de verificación Habilitado para el SSID de difusión.
19. Haga clic en la ficha **Security** (Seguridad).
20. En el submenú **Capa 2**, verifique **WPA + WPA2** para Seguridad de Capa 2. Para la encriptación WPA2, verifique **AES + TKIP** para permitir clientes TKIP.
21. Elija **802.1x** como método de autenticación.
22. Omita el submenú Capa 3 porque no es necesario. Una vez que se configura el servidor RADIUS, se puede elegir el servidor adecuado en el menú **Authentication** (Autenticación).
23. Las fichas **QoS** y **Advanced** se pueden dejar de forma predeterminada a menos que se requiera alguna configuración especial.
24. Haga clic en el menú **Seguridad** para agregar el servidor RADIUS.
25. En el submenú **RADIUS**, haga clic en **Authentication**. A continuación, haga clic en **Nuevo**.
26. Agregue la dirección IP del servidor RADIUS (172.16.100.25) que es el servidor ACS configurado anteriormente.
27. Asegúrese de que la clave compartida coincida con el cliente AAA configurado en el servidor ACS. Asegúrese de que la casilla **Network User** esté marcada y haga clic en **Apply**.



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the 'SECURITY' tab. On the left, a navigation tree is open under 'AAA' with 'RADIUS' selected. The main panel is titled 'RADIUS Authentication Servers > New'. It contains fields for 'Server Index (Priority)' (set to 1), 'Server IP Address' (172.16.100.25), 'Shared Secret Format' (ASCII), 'Shared Secret' (\*\*\*\*\*), 'Confirm Shared Secret' (\*\*\*\*\*), and 'Key Wrap' (unchecked). Below these are fields for 'Port Number' (1812), 'Server Status' (Enabled), 'Support for RFC 3576' (Enabled), 'Server Timeout' (2 seconds), and 'Network User' (Enable checked). Under 'Management' and 'IPSec', both 'Enable' checkboxes are unchecked.

28. La configuración básica se ha completado y puede comenzar a probar PEAP.

## Autenticación PEAP

PEAP con MS-CHAP versión 2 requiere certificados en los servidores ACS pero no en los clientes inalámbricos. La inscripción automática de certificados informáticos para los servidores ACS se puede utilizar para simplificar una implementación.

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

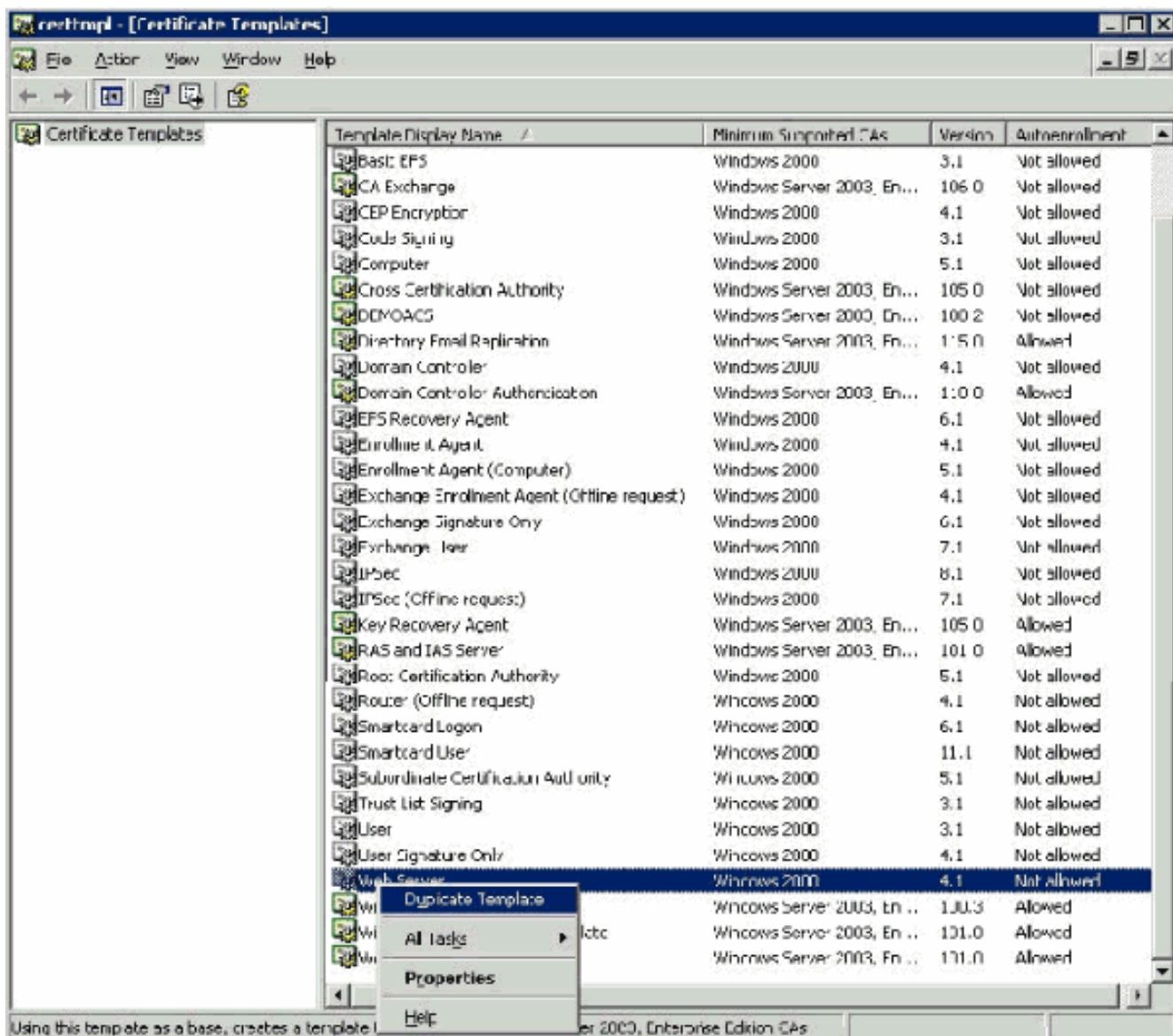
**Nota:** Microsoft ha cambiado la plantilla de servidor Web con la versión de la CA empresarial de Windows 2003, de modo que las claves ya no se pueden exportar y la opción está atenuada. No hay otras plantillas de certificados suministradas con servicios de certificados para la autenticación del servidor 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:

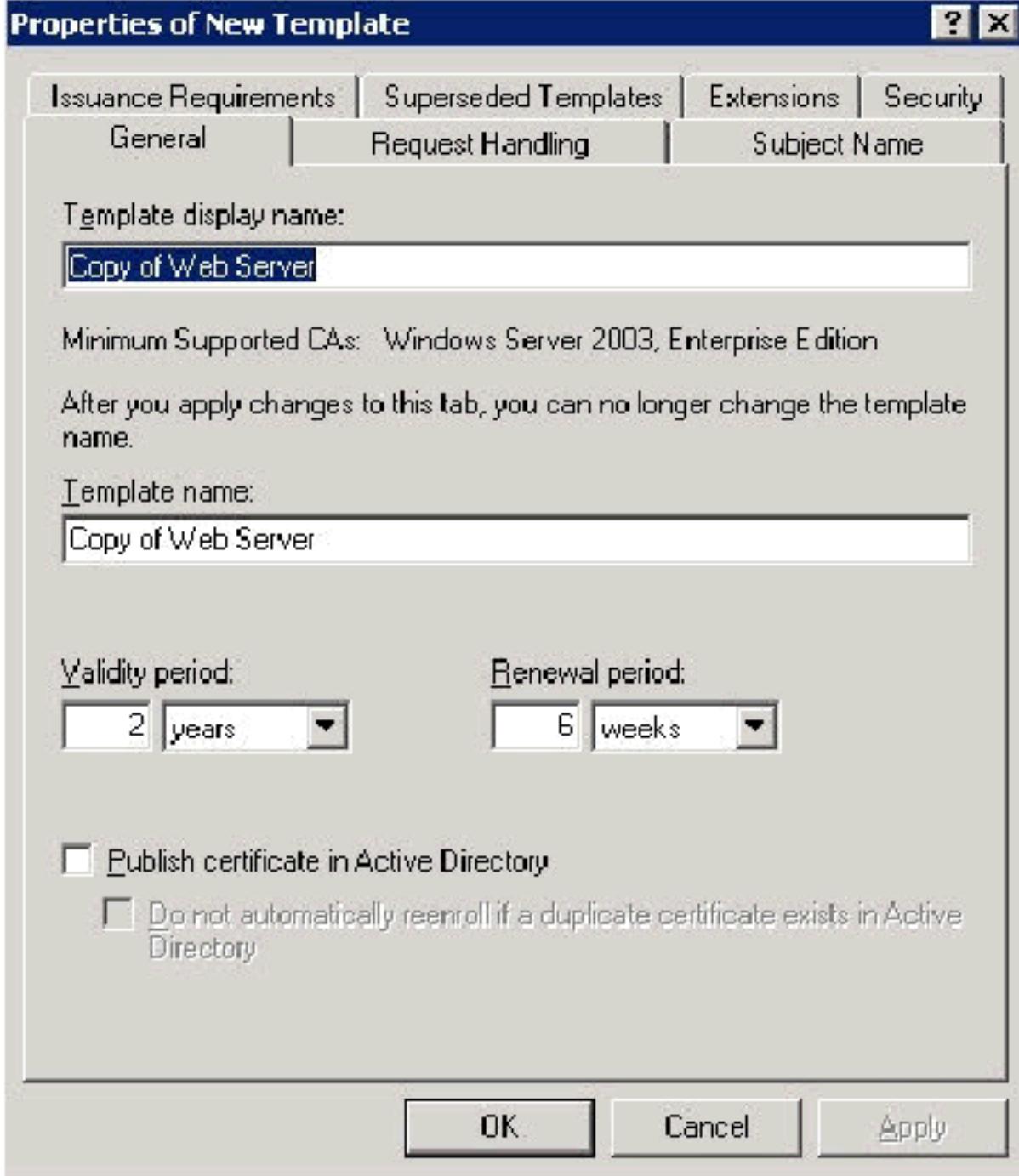
1. Elija **Inicio > Ejecutar**, escriba **mmc** y haga clic en **Aceptar**.
2. En el menú Archivo, haga clic en **Agregar o quitar complemento** y, a continuación, haga clic en **Agregar**.
3. En Complemento, haga doble clic en **Plantillas de certificado**, haga clic en **Cerrar** y, a continuación, 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**.



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**). Asegúrese también de que **Signature and Encryption** esté seleccionado en el menú desplegable Purpose (Propósito).

## ACS Properties



Issuance Requirements | Superseded Templates | Extensions | Security

General

Request Handling

Subject Name

Purpose:

Signature and encryption



- Archive subject's encryption private key
- Include symmetric algorithms allowed by the subject
- Delete revoked or expired certificates (do not archive)

Minimum key size:

1024



Allow private key to be exported

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

- Enroll subject without requiring any user input
- Prompt the user during enrollment
- Prompt the user during enrollment and require user input when the private key is used

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

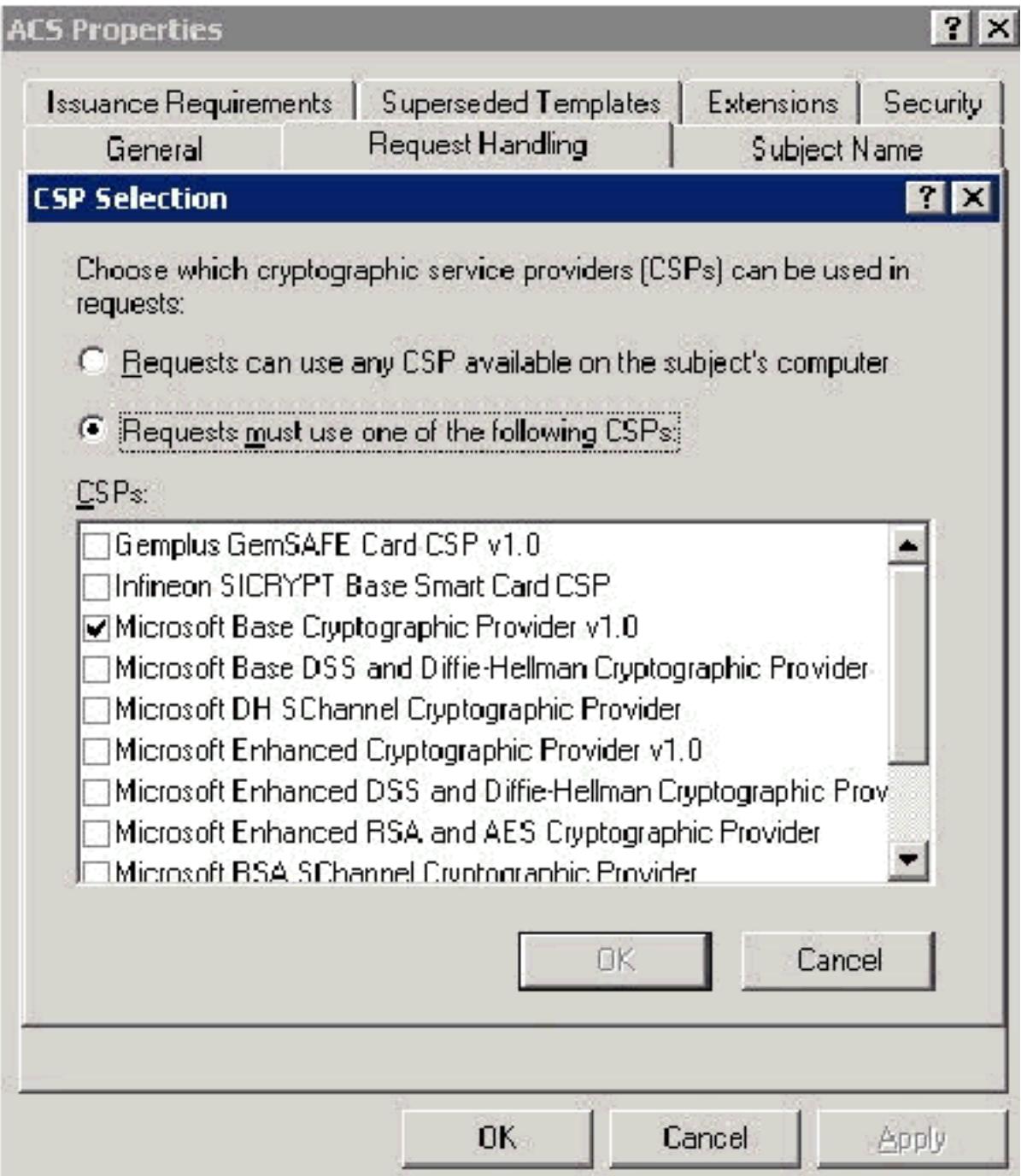
CSPs...

OK

Cancel

Apply

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.

## ACS Properties



Issuance Requirements | Superseded Templates | Extensions | Security

General

Request Handling

Subject Name

Supply in the request

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

Build from this Active Directory information

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

Subject name format:

None

Include e-mail name in subject name

Include this information in alternate subject name:

E-mail name

DNS name

User principal name (UPN)

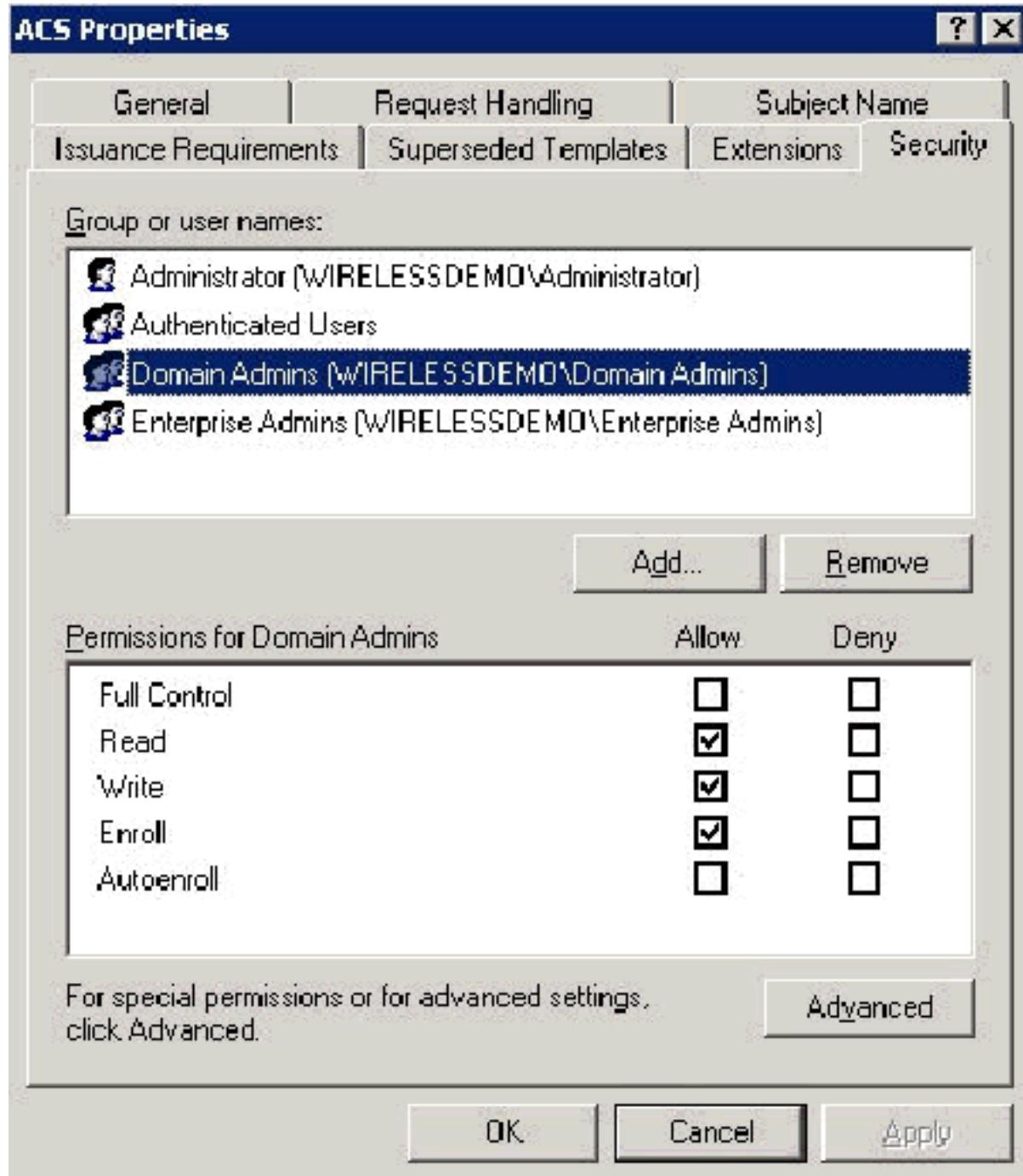
Service principal name (SPN)

OK

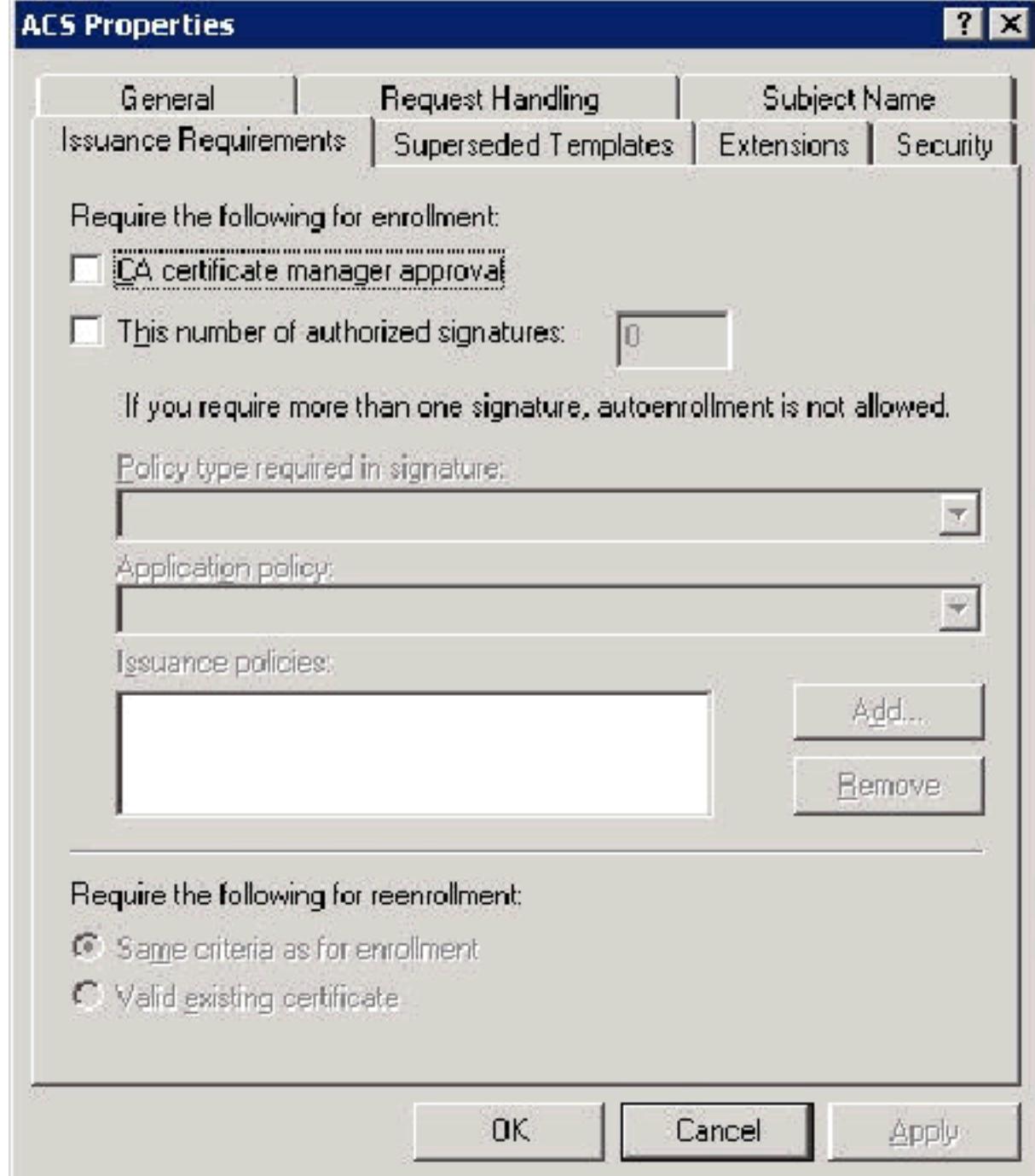
Cancel

Apply

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 de esta información de Active Directory, sólo verifique el **nombre principal de usuario (UPN)** y desmarque **Incluir nombre de correo electrónico** en el nombre del asunto y el nombre del correo electrónico porque no se introdujo 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 eliminan automáticamente. Estos se pueden encontrar en la pestaña Requisitos de emisión. Esto no se analiza más a fondo en este documento.

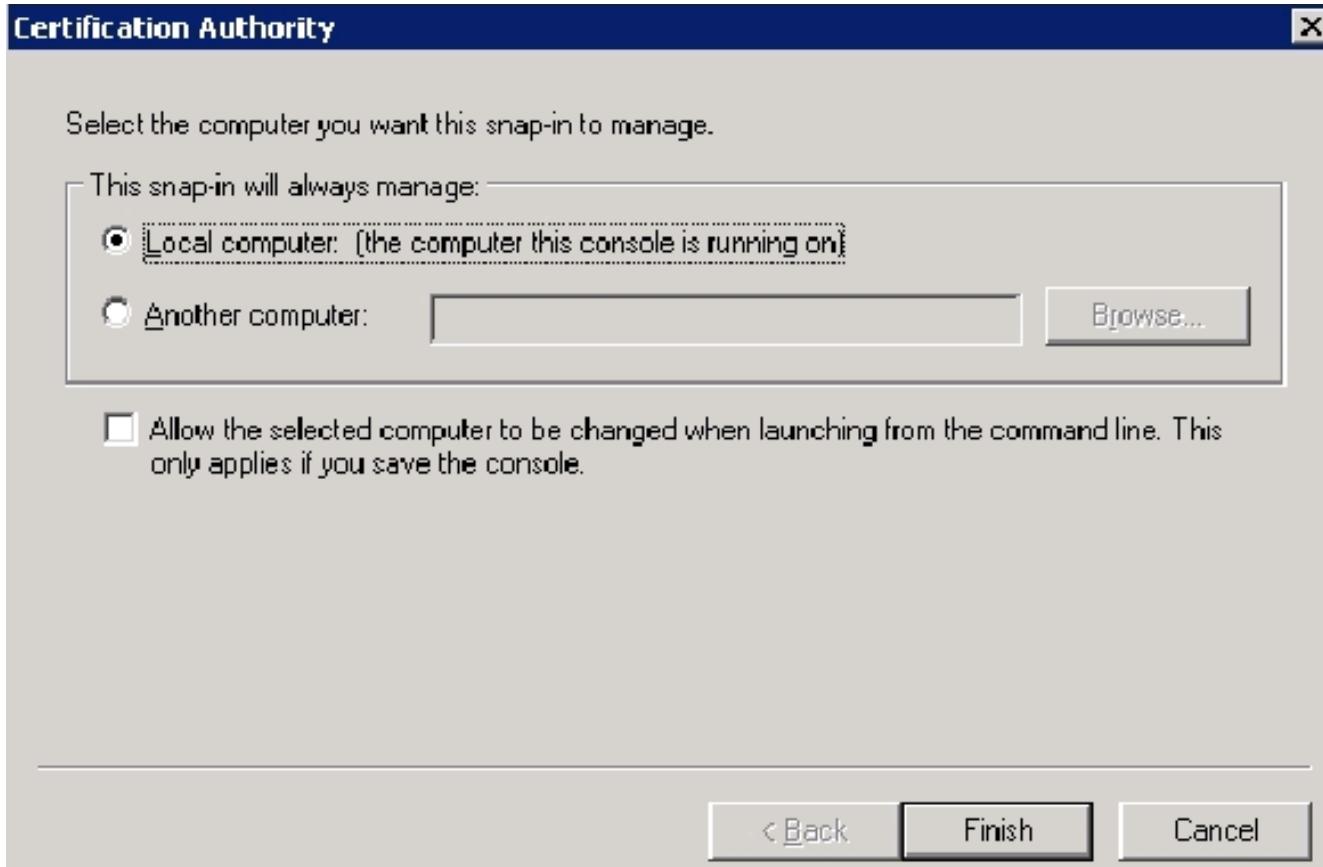


9. Haga clic en **Aceptar** para guardar la plantilla y pasar a emitir esta plantilla desde el complemento Autoridad de certificados.

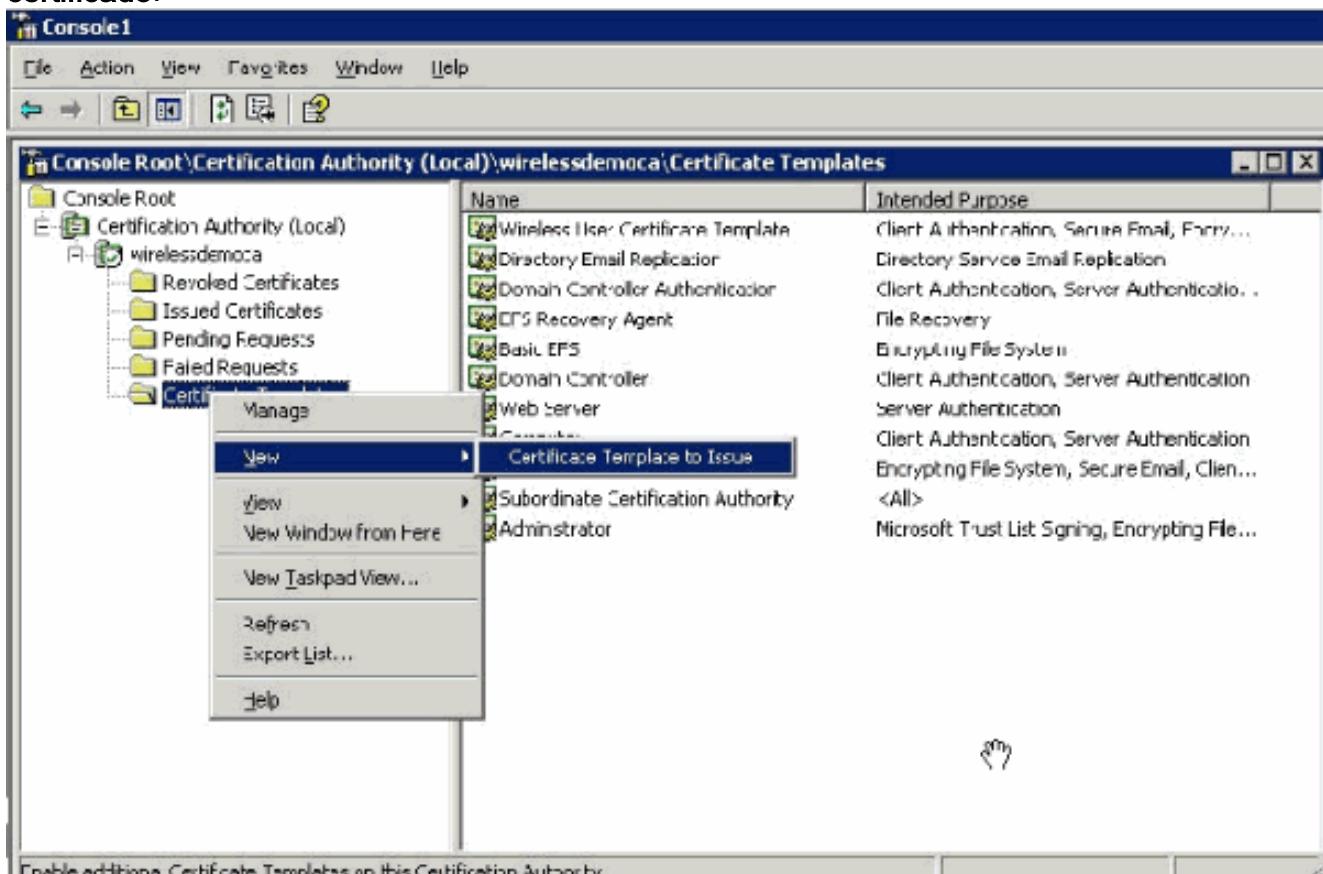
## [Habilitación de la Nueva Plantilla de Certificado de Servidor Web ACS](#)

Complete estos pasos:

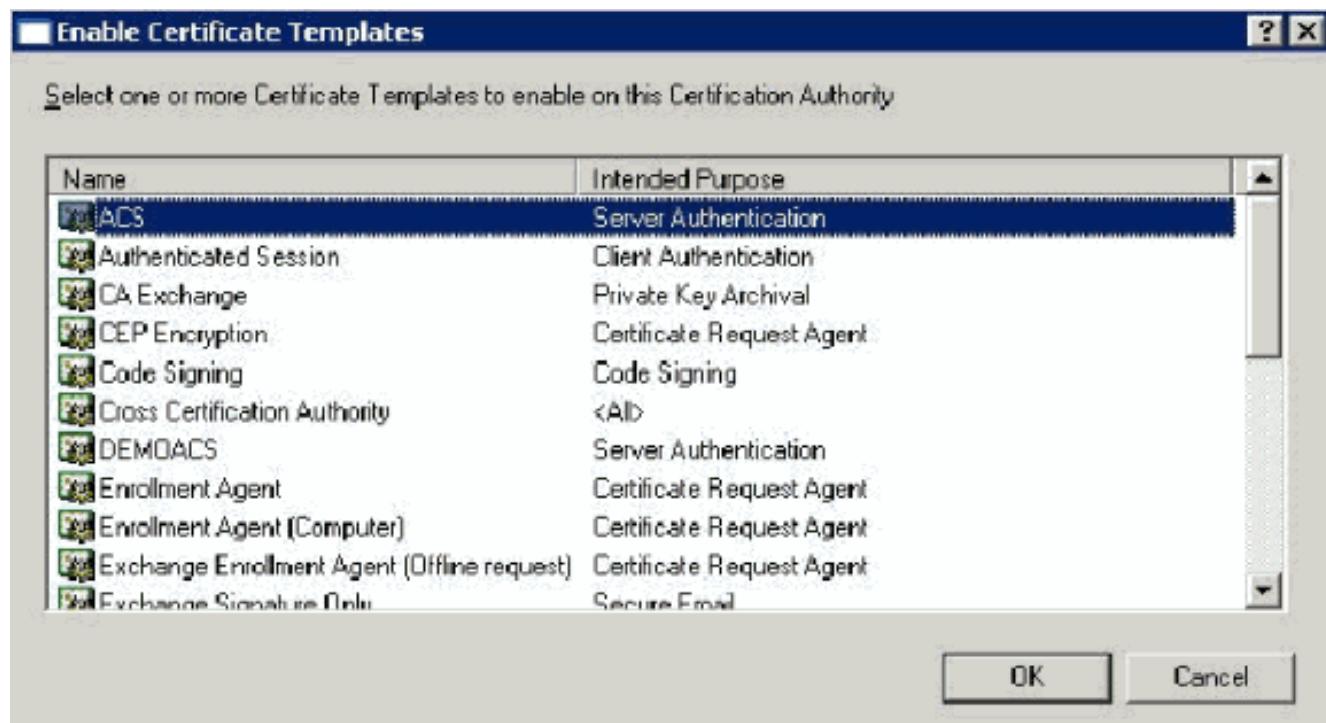
1. Abra el complemento Entidad de certificación. Siga los pasos 1-3 en la sección [Creación de la Plantilla de Certificado para el Servidor Web ACS](#), elija la opción **Autoridad de Certificación**, elija **Equipo Local** y haga clic en **Finalizar**.



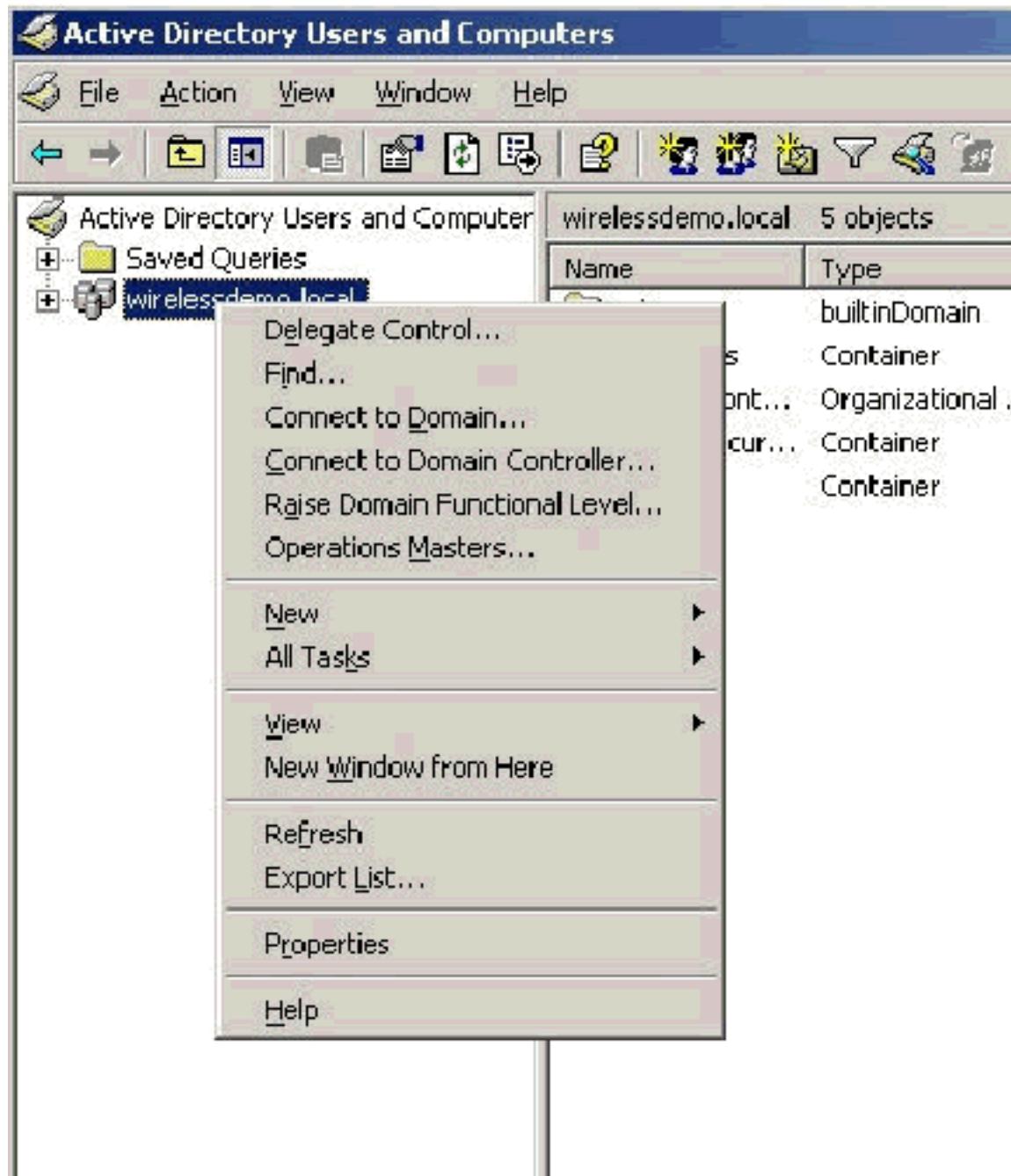
2. En el árbol de la consola, expanda **wirelessdemoca** y, a continuación, haga clic con el botón derecho en **Plantillas de certificado**.



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

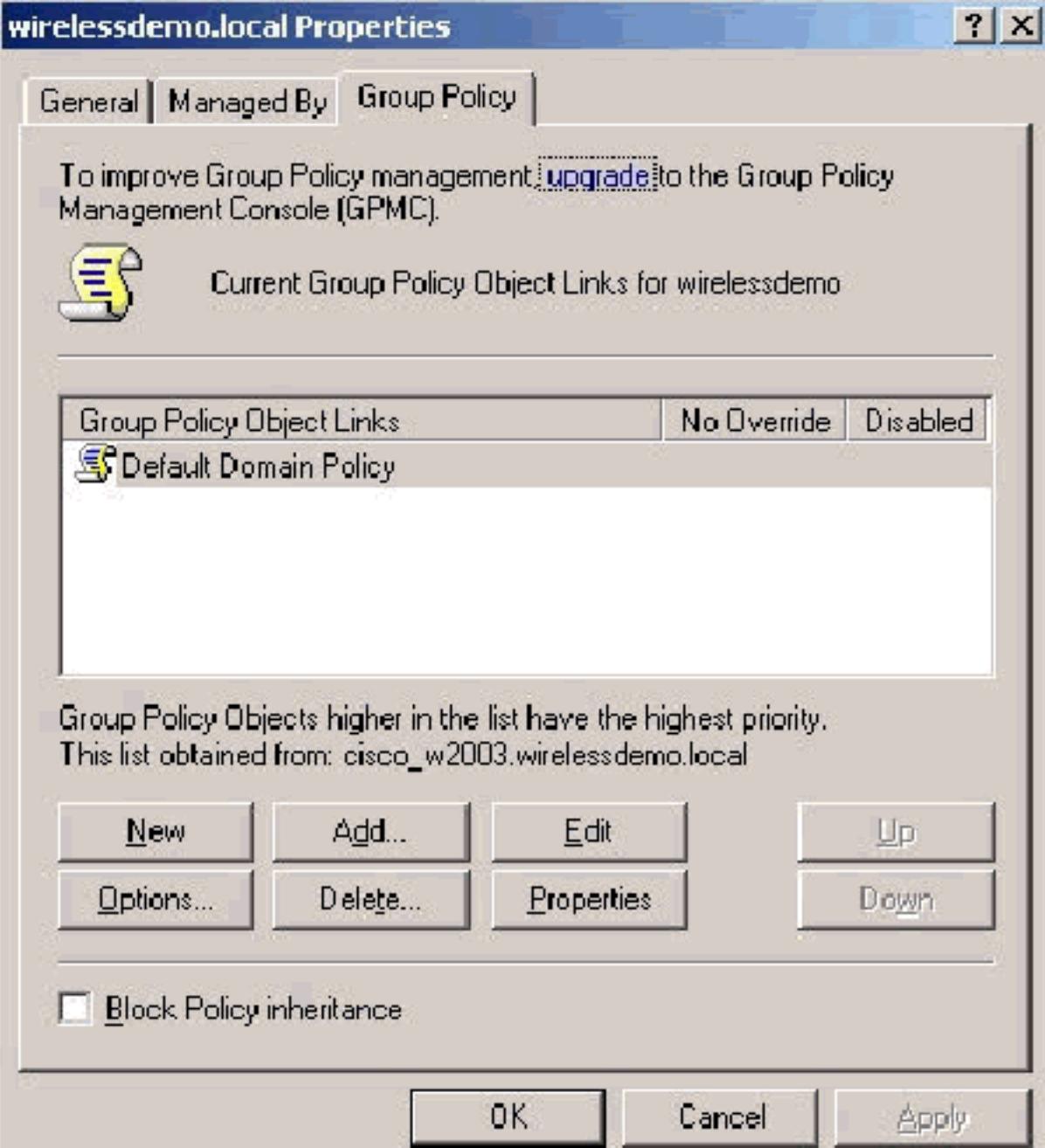


5. Haga clic en **Aceptar** y abra el complemento **Usuarios y equipos de Active Directory**.
6. En el árbol de la consola, haga doble clic en **Active Directory Users and Computers**, haga clic con el botón derecho en **wirelessdemo.local** y, a continuación, haga clic en



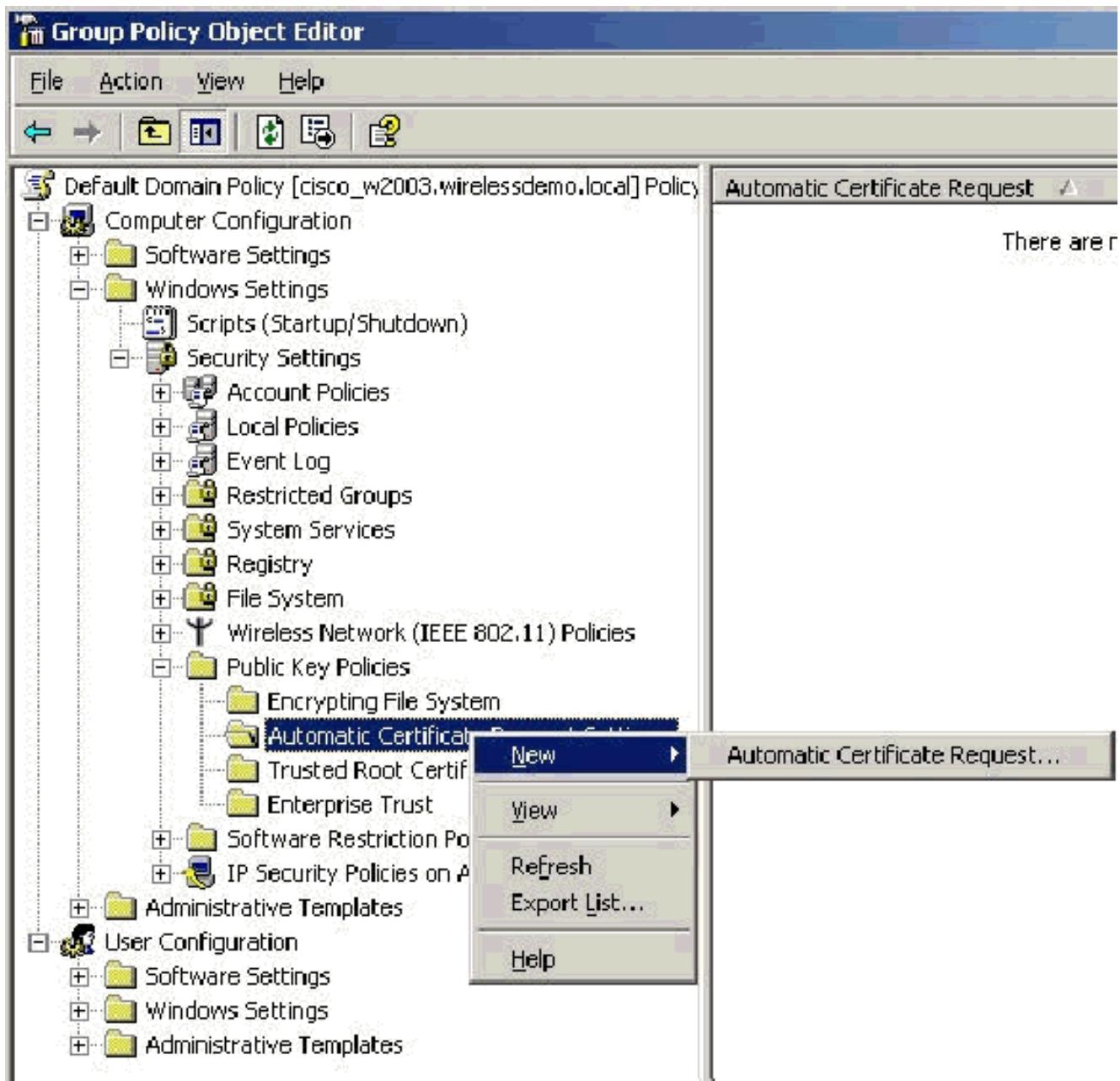
### Properties.

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**.

## Automatic Certificate Request Setup Wizard



### Certificate Template

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



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

Certificate templates:

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

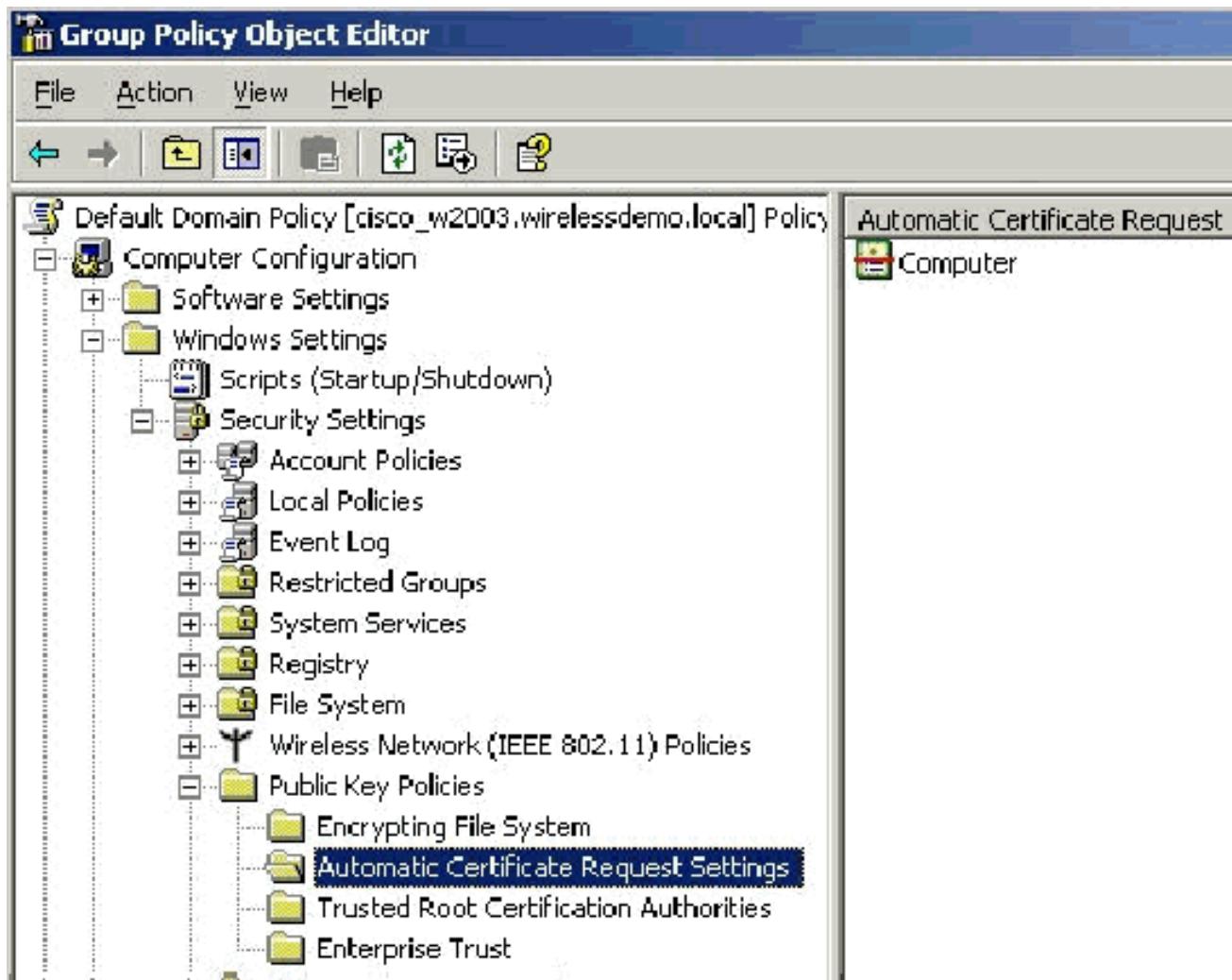


< Back

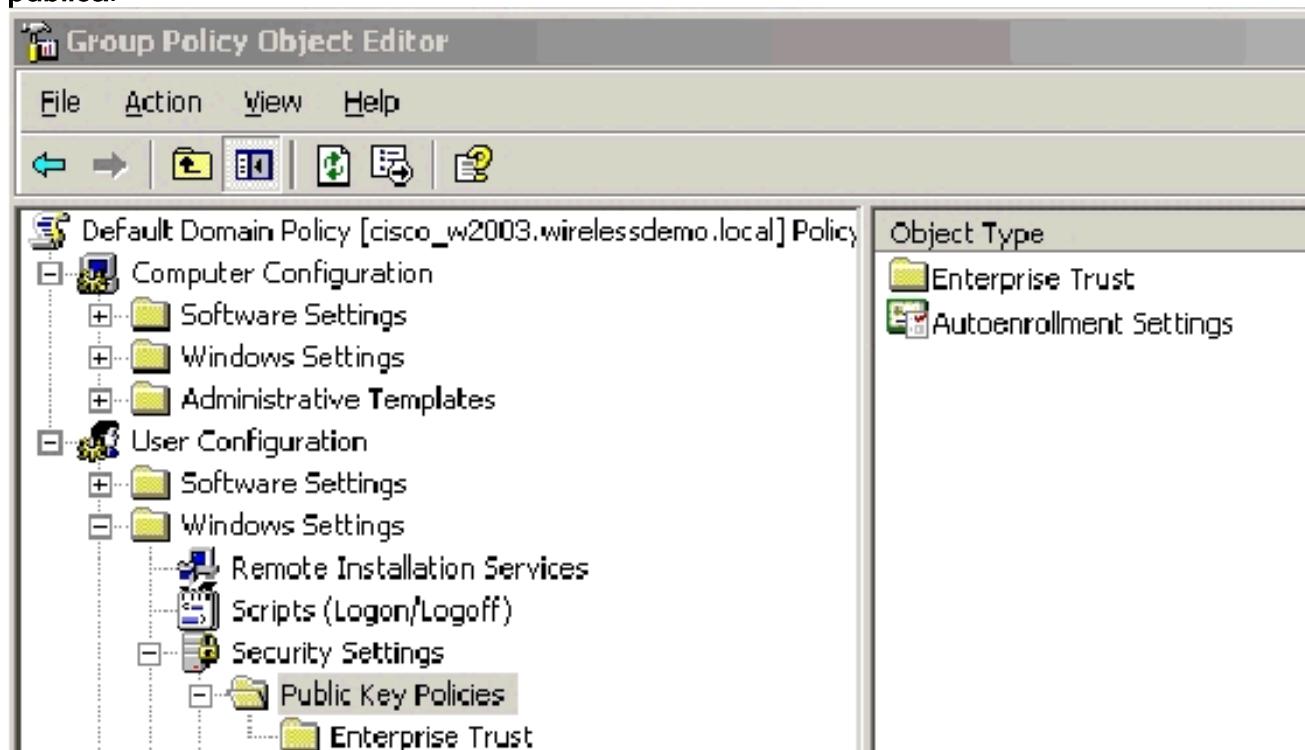
Next >

Cancel

12. Cuando complete la página Asistente para la configuración automática de solicitudes de certificados, 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.

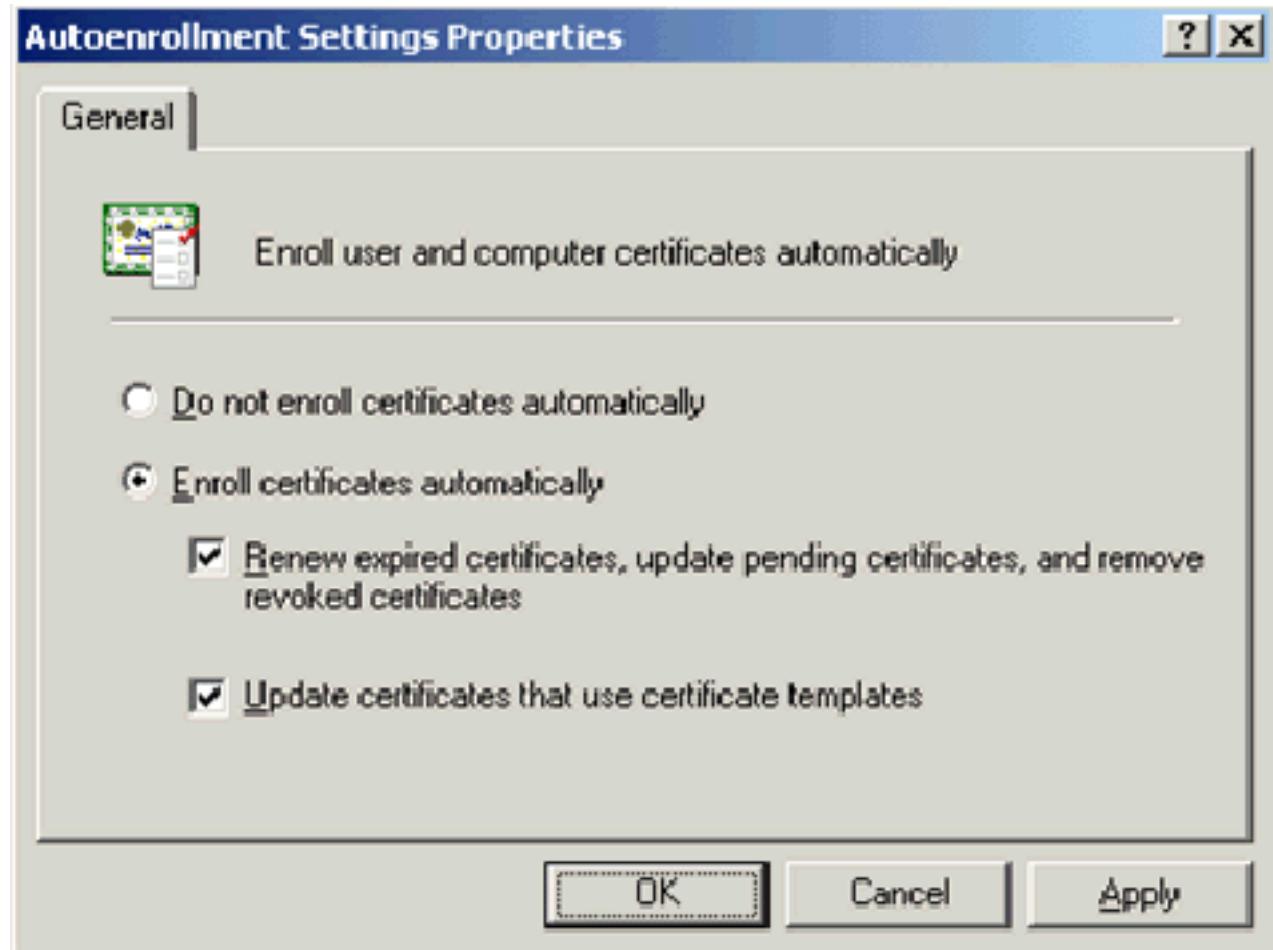


13. En el árbol de la consola, expanda Configuración de usuario > Configuración de Windows > Configuración de seguridad > Políticas de clave pública.



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 PEAP de WLAN.

**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.

This screenshot shows the Microsoft Certificate Services interface. The title bar reads "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar shows the URL "http://172.16.100.26/certsrv/certrqus.asp". The main content area has a teal header "Microsoft Certificate Services -- wirelessdemoca". Below it, a section titled "Welcome" contains text about requesting certificates for various purposes like email clients or servers. It also mentions certificate signing and encryption, and provides links for "View certificate details" and "View certificate status". A sidebar on the left says "Select a task:" with options for "Request a certificate", "View certificate details", and "View certificate status".

4. Elija Request a Certificate y haga clic en [Next](#).

This screenshot shows the "Request a Certificate" page. The title bar is "Microsoft Certificate Services - Microsoft Internet Explorer" and the address bar is "http://172.16.100.26/certsrv/certrqus.asp". The main content area has a teal header "Microsoft Certificate Services -- wirelessdemoca". Below it, the heading "Request a Certificate" is underlined. It says "Select the certificate type:" followed by a link "User Certificate". There is also a link "Or, submit an [advanced certificate request](#)".

5. Elija Advanced Request y haga clic en [Next](#).

This screenshot shows the "Advanced Certificate Request" page. The title bar is "Microsoft Certificate Services - Microsoft Internet Explorer" and the address bar is "http://172.16.100.26/certsrv/certreqas.asp". The main content area has a teal header "Microsoft Certificate Services -- wirelessdemoca". Below it, the heading "Advanced Certificate Request" is underlined. It contains instructions about certificate types and links for "Create and submit a request to this CA", "Submit a certificate request by using a base 64 encoded CMX or PKCS #10 file", "Submit a renewal request by using a base 64 encoded PKCS#12 file", and "Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment feature".

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.

Microsoft Certificate Services - wirelessdemo.local

## Advanced Certificate Request

**Certificate Template:**

Key Options:

Administrator  
Basic CPE  
EFS Recovery Agent  
User  
Wireless User Certificate Template  
**ACS**  
Subordinate Certification Authority  
Web Server  
Key Usage:  
Max 15884 (-----2 1024 2048 4096 8192 16384)

Automatic key container name    User specified key container name  
 Make keys exportable  
 Export keys to file  
 Enable sharing private key protocol  
 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

Activation:

Friendly Name:

7. Desde 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 Search Favorites

Address: <http://172.16.100.26/certsrv/certreqa.asp>

---

**Certificate Template:**

ACS

---

**Identifying Information For Offline Template:**

Name:   
 E-Mail:   
 Company:   
 Department:   
 City:   
 State:   
 Country/Region:

---

**Key Options:**

Create new key set    Use existing key set  
 CSP: Microsoft Base Cryptographic Providerv1.0

Key Usage:  Exchange  
 Key Size: 1024 Min:1024 Max:1024 (maximum key size: 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

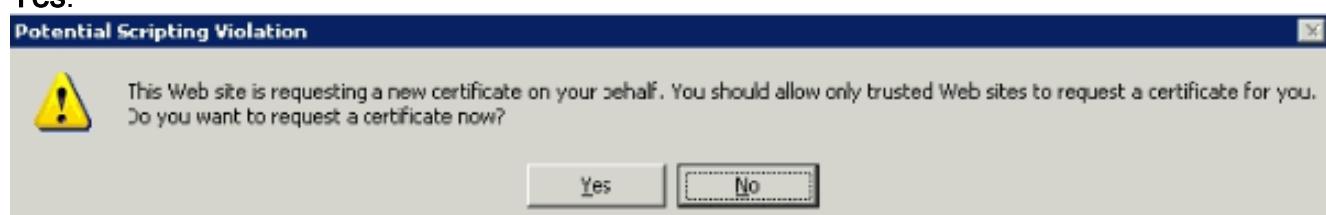
Attributes:

Friendly Name:

**Enviar.**

9. Aparece una ventana emergente en la que se advierte de una posible violación de la secuencia de comandos. Elija

**Yes.**



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

**Microsoft Certificate Services - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Search Favorites

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

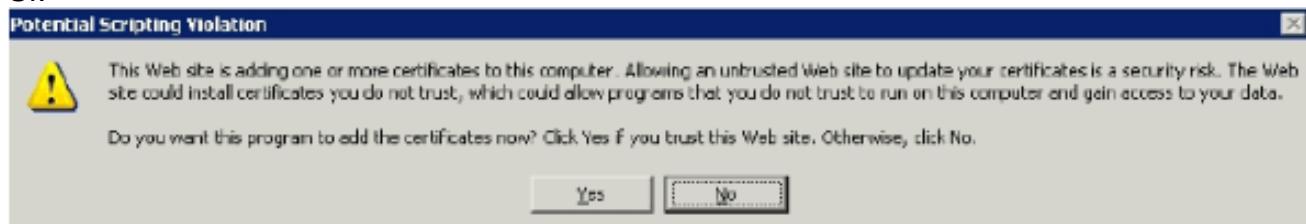
**Microsoft Certificate Services -- wirelessdemoca**

**Certificate Issued**

The certificate you requested was issued to you.

[Install this certificate](#)

11. Una ventana emergente aparece de nuevo y advierte sobre una posible violación de secuencias de comandos. Seleccione Sí.



12. Despues de hacer clic en Sí, se instala el

**Microsoft Certificate Services - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Search Favorites

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

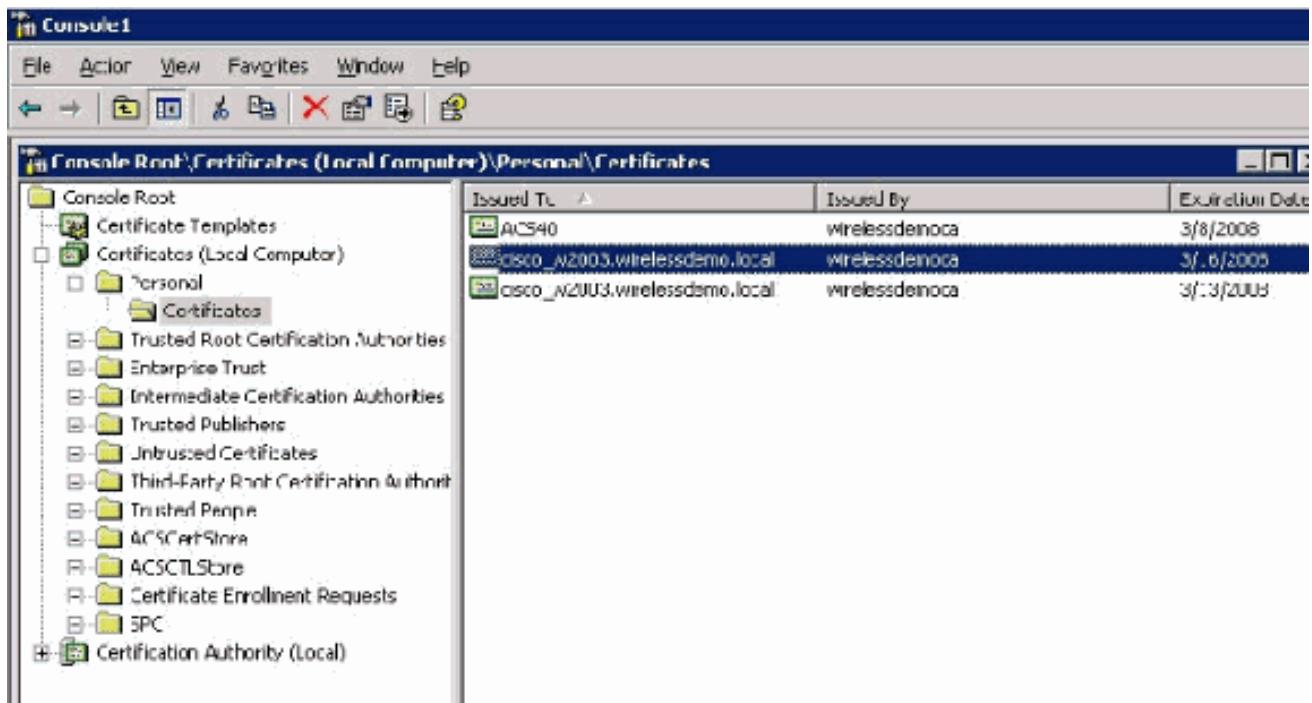
**Microsoft Certificate Services -- wirelessdemoca**

**Certificate Installed**

Your new certificate has been successfully installed

certificado.

13. En este momento, el certificado se instala en la MMC de certificados bajo **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 Refresh Search Favorites Home Address http://172.16.100.26/certs/v/certcert.cer

## **Microsoft Certificate Services -- wirelessdem0na**

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

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

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

#### **CA certificate:**

Client [wirelessdem0na]

Server

Root

#### **Encoding method:**

DER

Base64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

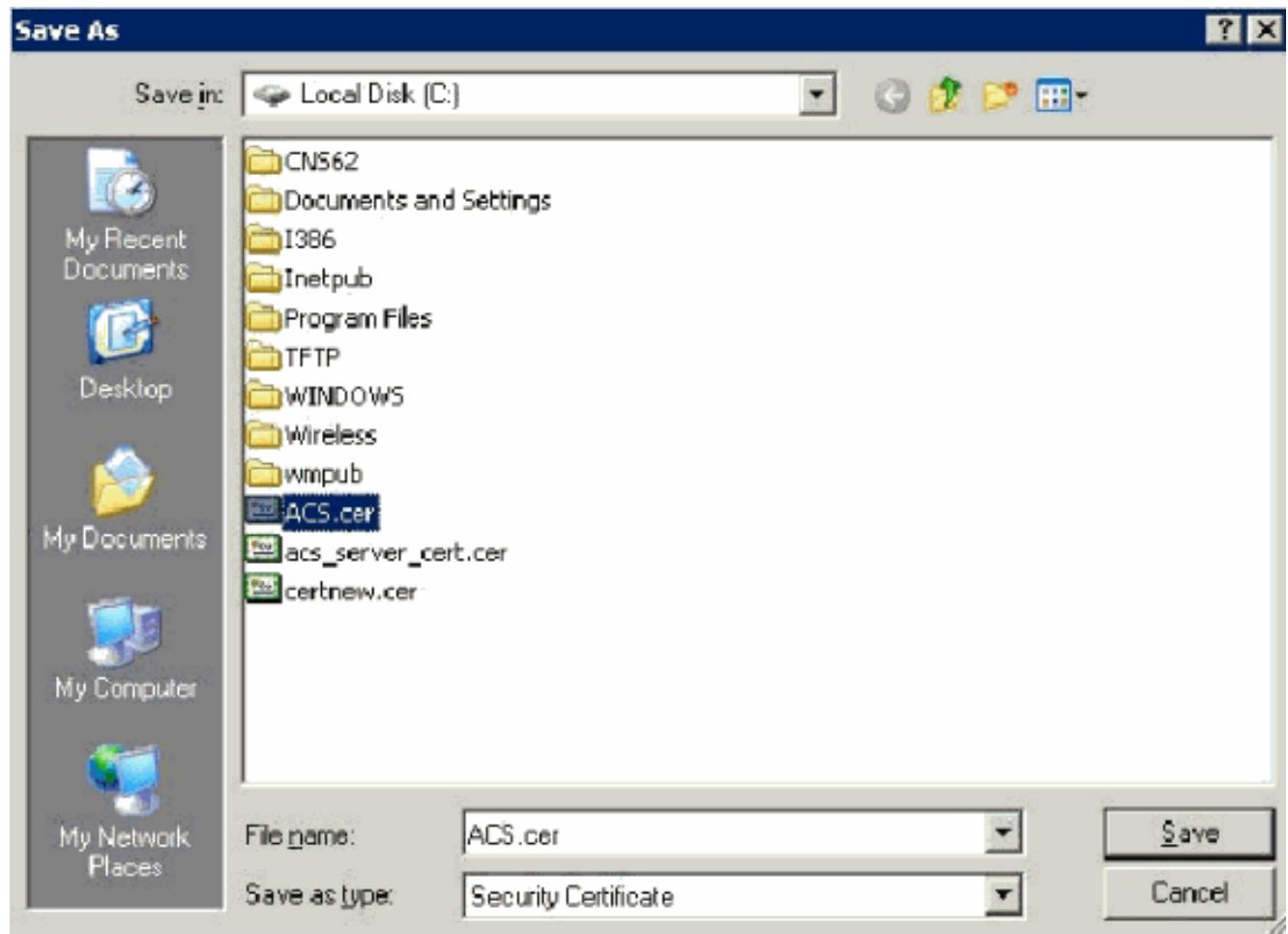
[Download latest delta CRL](#)

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

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://127.0.0.1:3809/

**CISCO SYSTEMS**

# System Configuration

**Select**

-  [User Setup](#)
-  [Group Setup](#)
-  [Shared Profile Components](#)
-  [Network Configuration](#)
-  [System Configuration](#)
-  [Interface Configuration](#)
-  [Administration Control](#)
-  [External User Databases](#)
-  [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.

8. 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

Read certificate from file  
Certificate file

Use certificate from storage  
Certificate CN

Private key file

Private key password

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

Read certificate from file  
Certificate file

Use certificate from storage  
Certificate CN  cisco\_w2003.wirelessde

Private key file   
Private key password

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

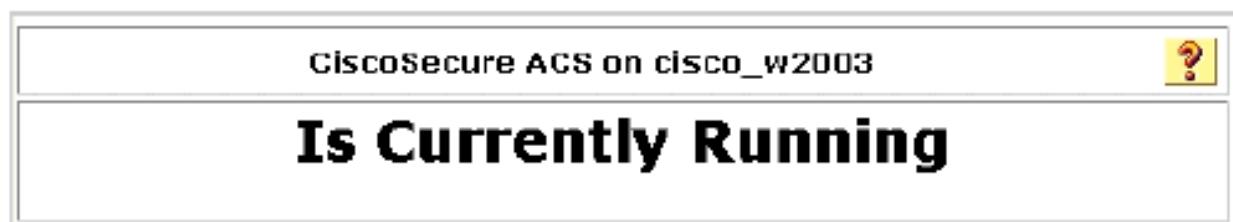
**The current configuration has been changed.  
Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.**

12. Haga clic en Configuración del sistema.  
13. Haga clic en Service Control y luego haga clic en

Restart.

## System Configuration

Select



The screenshot shows the "Services Log File Configuration" settings. It includes the following options:

- Level of detail:** Radio buttons for "None" (unchecked), "Low" (checked), and "Full" (unchecked).
- Generate New File:** Radio buttons for "Every day" (checked), "Every week" (unchecked), "Every month" (unchecked), and "When size is greater than" followed by a text input field containing "2048" and a unit "KB".
- Manage Directory:** A checkbox labeled "Manage Directory" is checked. Below it are two radio button options: "Keep only the last" followed by a text input field containing "7" and "files", and "Delete files older than" followed by a text input field containing "7" and "days".

Back to Help

14. Haga clic en Configuración del sistema.
15. Haga clic en Configuración de autenticación global.
16. Marque Allow EAP-MSCHAPV2 y Allow EAP-GTC.

# 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

Edit

## ACS Certification Authority Setup



### System Configuration

Edit

#### ACS Certification Authority Setup



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

CA certificate common name wirelessdemoca

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 PEAP con Windows Zero Touch

En nuestro ejemplo, CLIENT es un equipo que ejecuta Windows XP Professional con SP 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 hub.
2. En CLIENT, instale Windows XP Professional con SP2 como equipo miembro denominado CLIENT del dominio local wireless.demo.
3. Instale Windows XP Professional con SP2. Esto se debe instalar para tener soporte PEAP. **Nota:** Firewall de Windows se activa automáticamente en Windows XP Professional con SP2. No apague el firewall.

### Instalación del adaptador de red inalámbrico

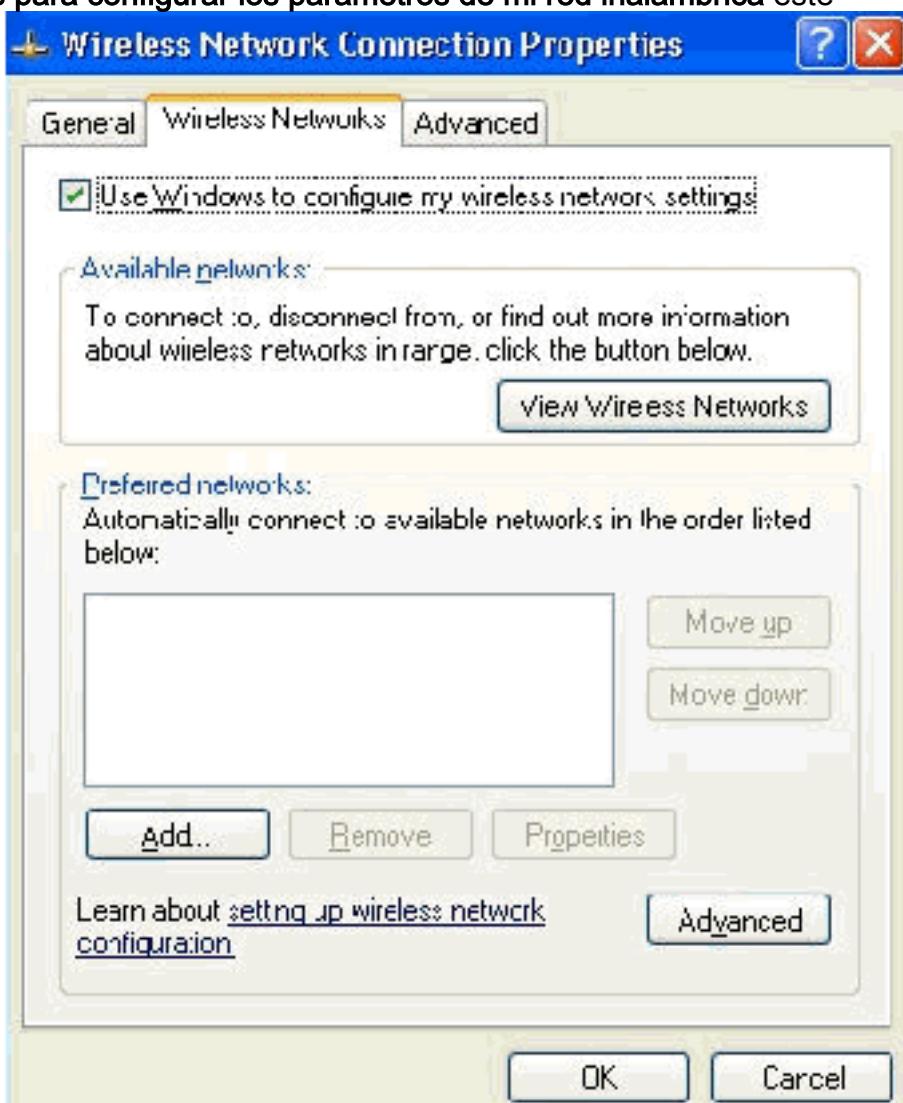
Complete estos pasos:

1. Apague el equipo CLIENTE.
2. Desconecte el equipo CLIENTE del segmento de red de la Intranet.
3. Reinicie el equipo CLIENT y, a continuación, inicie sesión con la cuenta de administrador local.
4. Instale el adaptador de red inalámbrico. **Importante:** No instale el software de configuración del fabricante para el adaptador inalámbrico. Instale los controladores del adaptador de red inalámbrica mediante el Asistente para agregar hardware. Además, cuando se le solicite, proporcione el CD proporcionado por el fabricante o un disco con controladores actualizados para su uso con Windows XP Professional con SP2.

## Configuración de la conexión de red inalámbrica

Complete estos pasos:

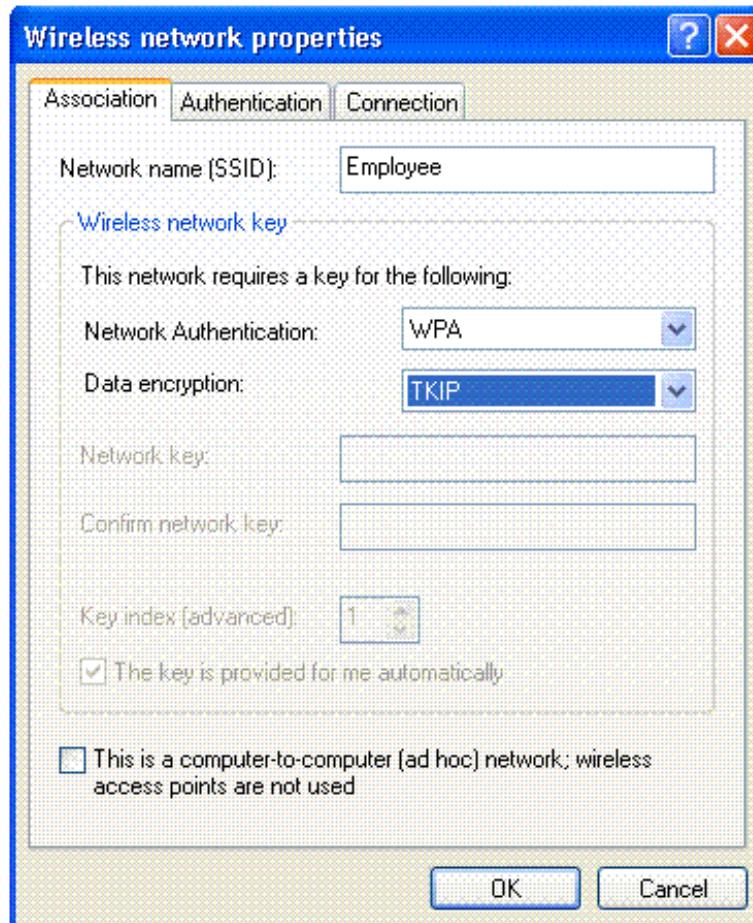
1. Cierre la sesión y, a continuación, conéctese utilizando la cuenta WirelessUser en el dominio wirelessdemo.local.
2. Elija **Inicio > Panel de control**, haga doble clic en **Conexiones de red** y, a continuación, haga clic con el botón derecho en **Conexión de red inalámbrica**.
3. Haga clic en **Propiedades**, vaya a la ficha Redes inalámbricas y asegúrese de que **Usar Windows para configurar los parámetros de mi red inalámbrica** esté



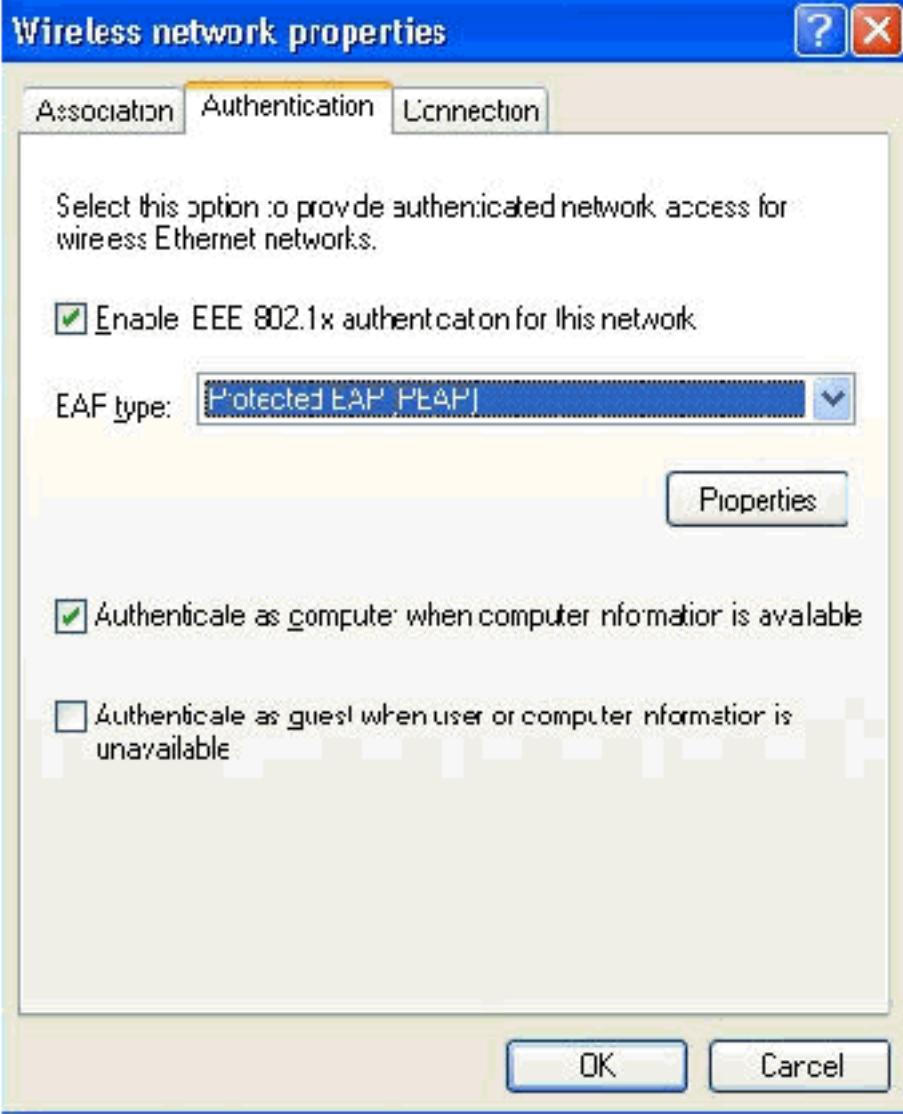
activado.

4. Haga clic en **Add (Agregar)**.
5. En la ficha Asociación, escriba **Empleado** en el campo Nombre de red (SSID).

6. Seleccione WPA para la autenticación de red y asegúrese de que el cifrado de datos esté configurado en TKIP.

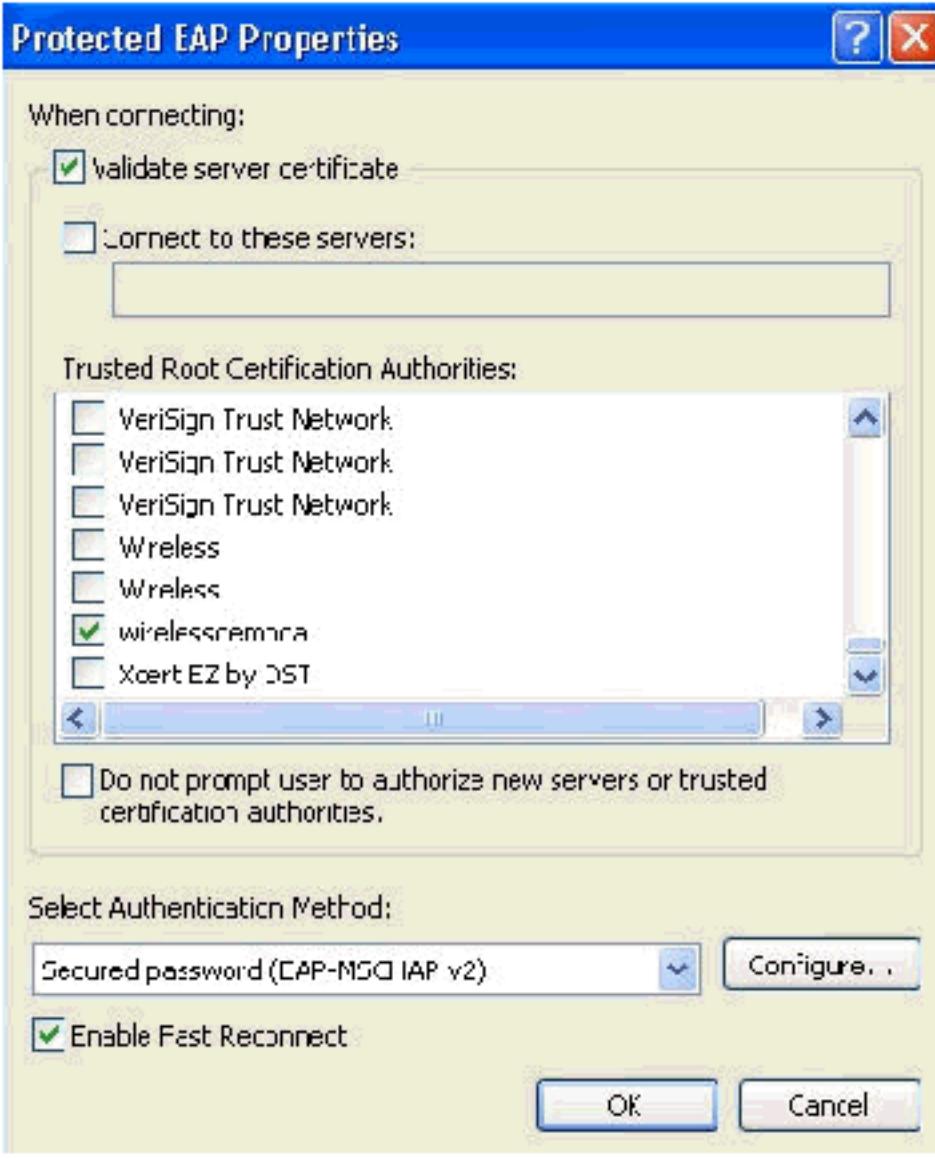


7. Vaya a la ficha Authentication (Autenticación).  
8. Valide que el tipo EAP esté configurado para utilizar **EAP protegido (PEAP)**. Si no es así, selecciónelo en el menú desplegable.  
9. Si desea que la máquina se autentique antes del inicio de sesión (que permite aplicar secuencias de comandos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



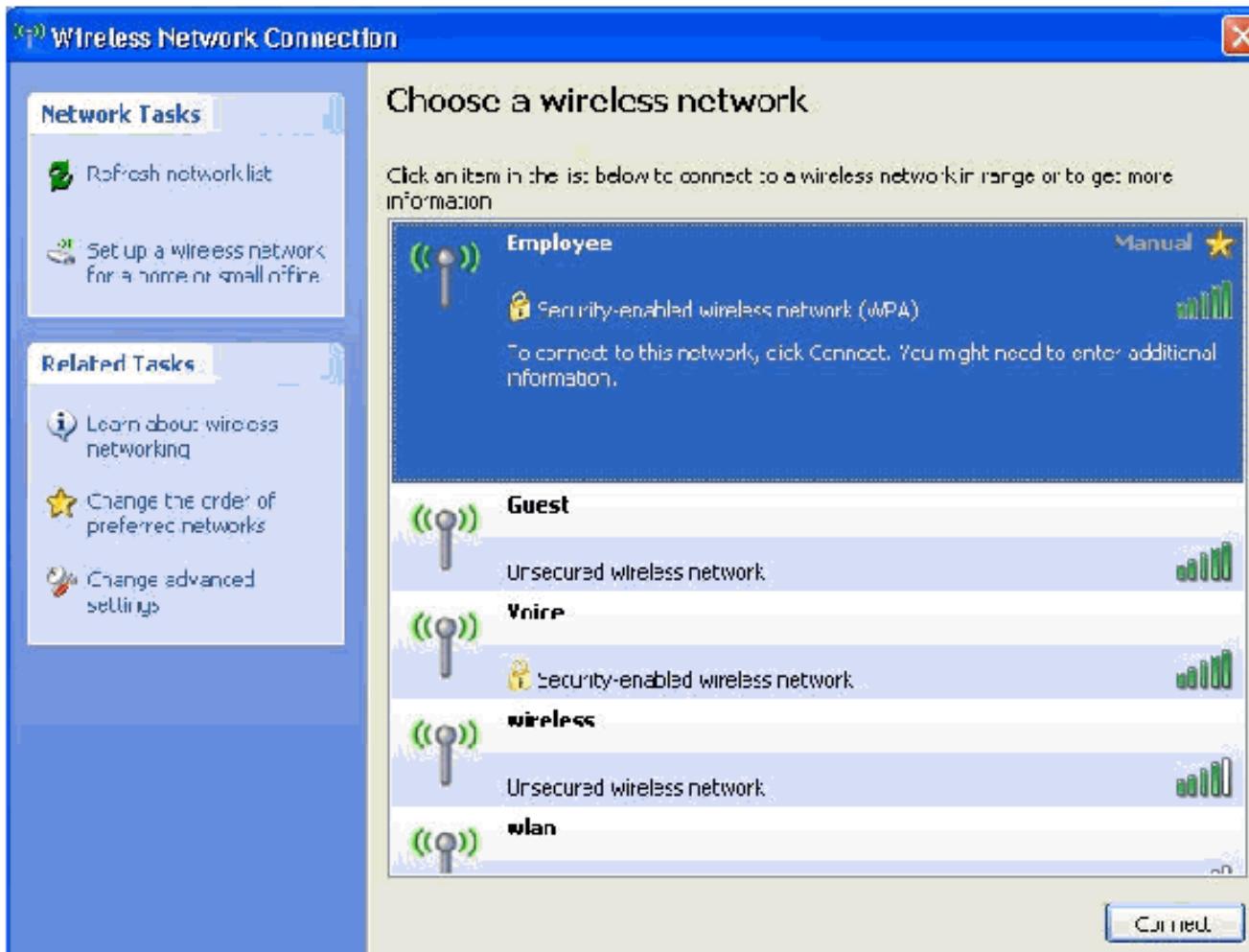
disponible.

10. Haga clic en Properties (Propiedades).
11. Dado que PEAP implica la autenticación del servidor por parte del cliente, asegúrese de que Validar certificado del servidor esté marcado. Además, asegúrese de que la CA que emitió el certificado ACS esté marcada en el menú *Autoridades de certificación raíz de confianza*.
12. Elija **Contraseña segura (EAP-MSCHAP v2)** en Método de autenticación, ya que se utiliza para la autenticación

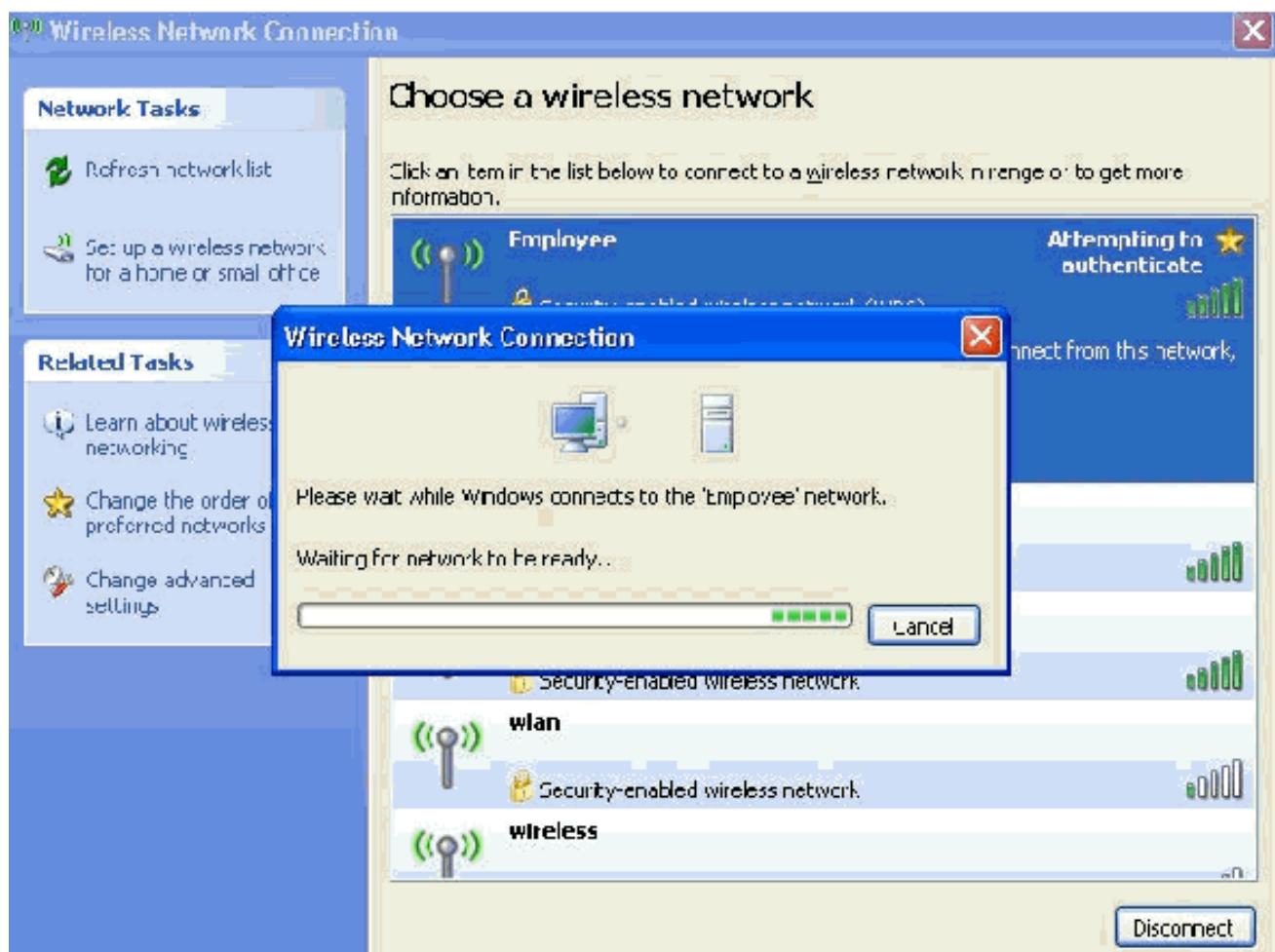
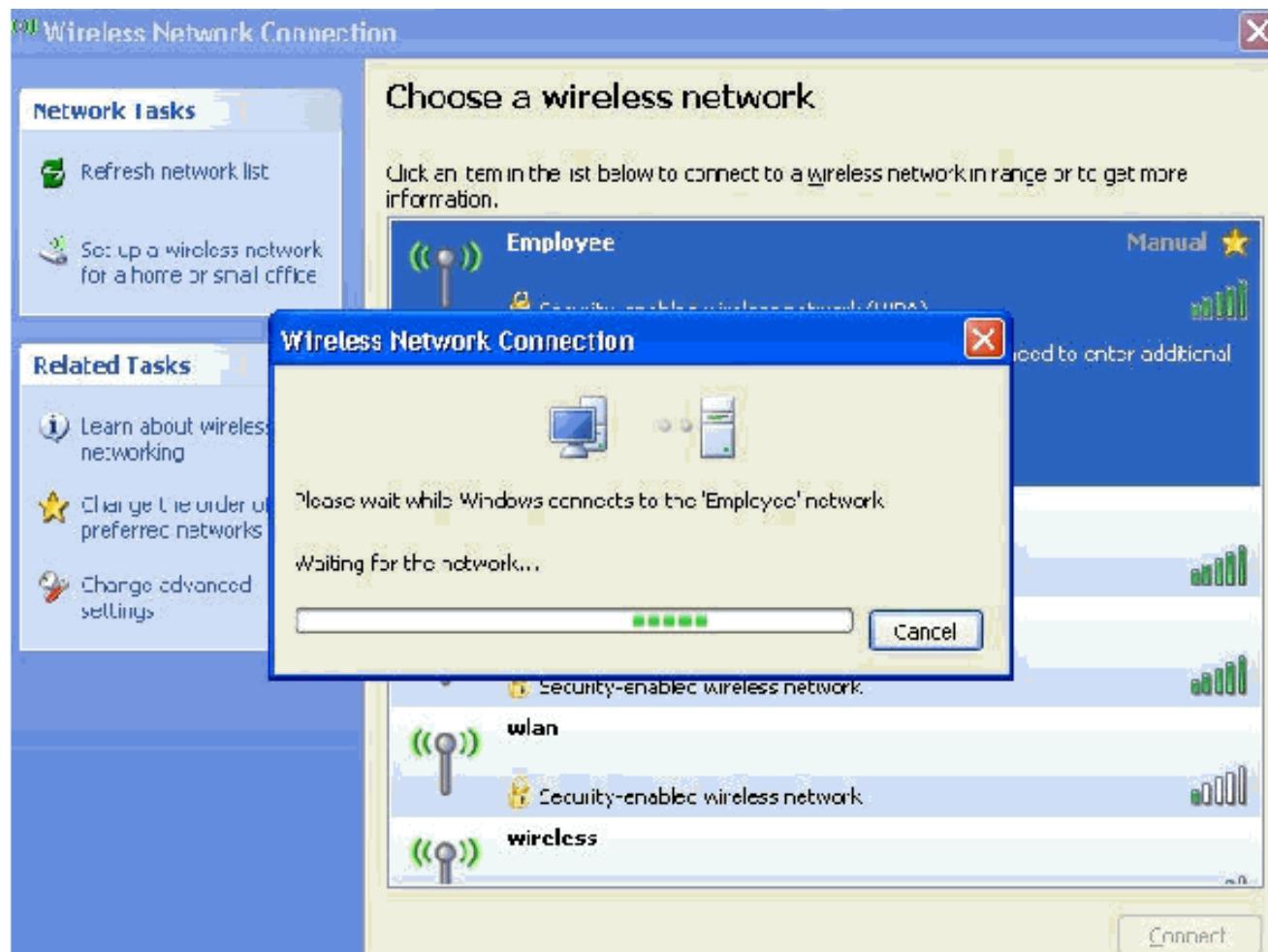


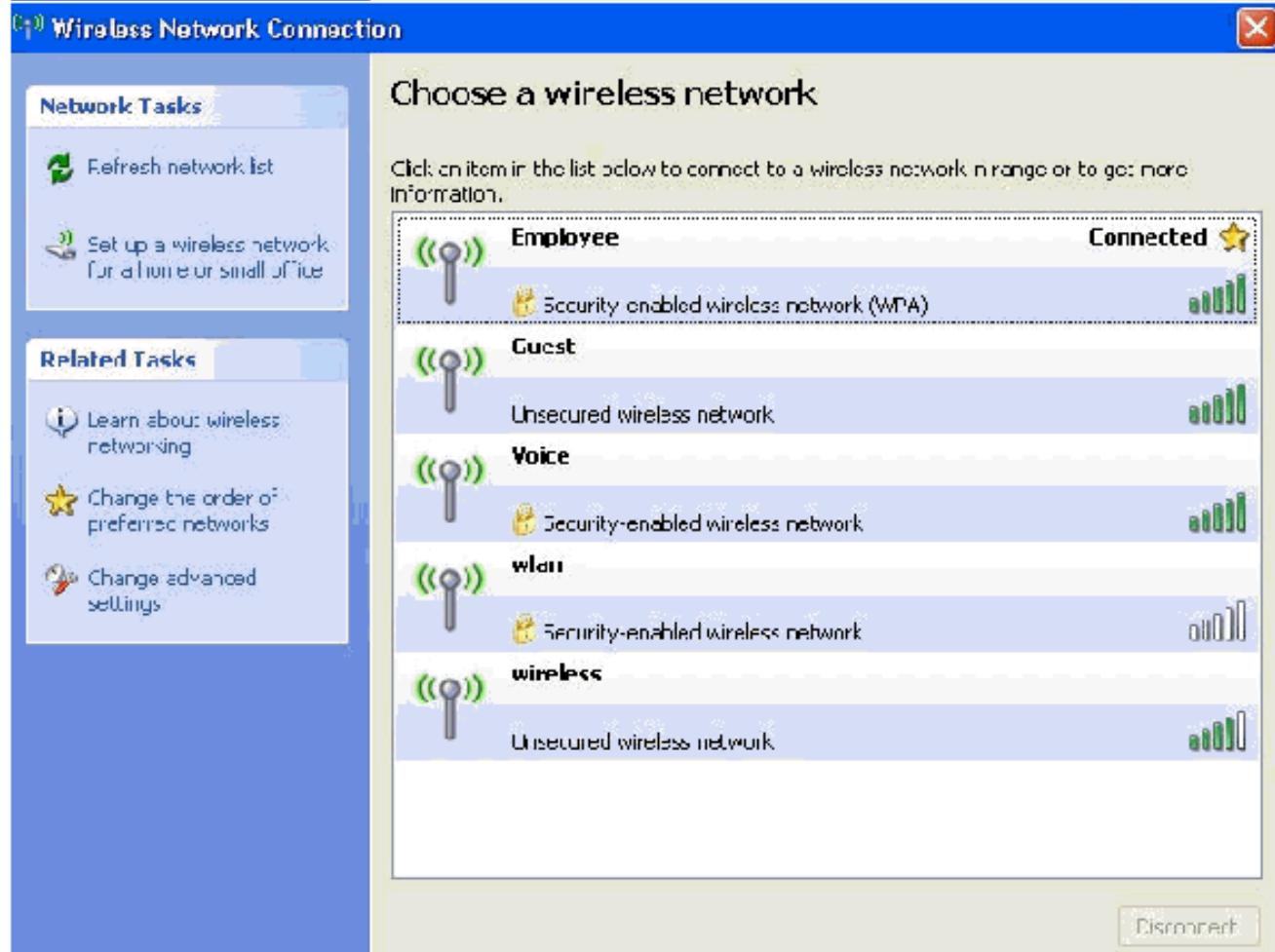
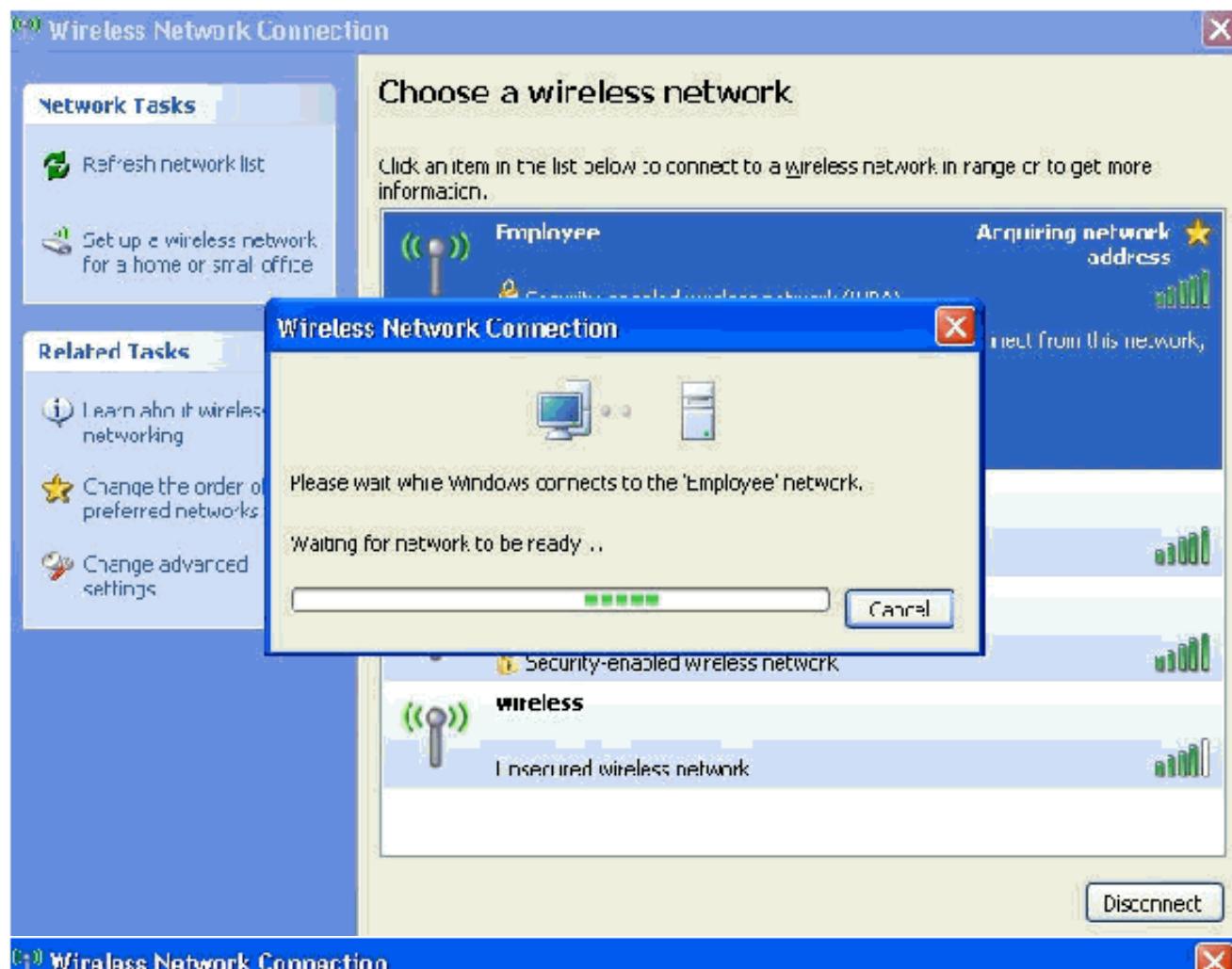
interna.

13. Asegúrese de que la casilla de verificación Habilitar reconexión rápida está marcada. A continuación, haga clic en **Aceptar** tres veces.
14. Haga clic con el botón derecho del ratón en el ícono de conexión de red inalámbrica del sistema y, a continuación, haga clic en **Ver redes inalámbricas disponibles**.
15. Haga clic en la red inalámbrica **Empleado** y haga clic en **Conectar**.



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





16. Después de que la autenticación se realice correctamente, compruebe 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.

17. Para probar la funcionalidad, abra un explorador y navegue hasta <http://wirelessdemoca> (o la dirección IP del servidor de CA de la empresa).

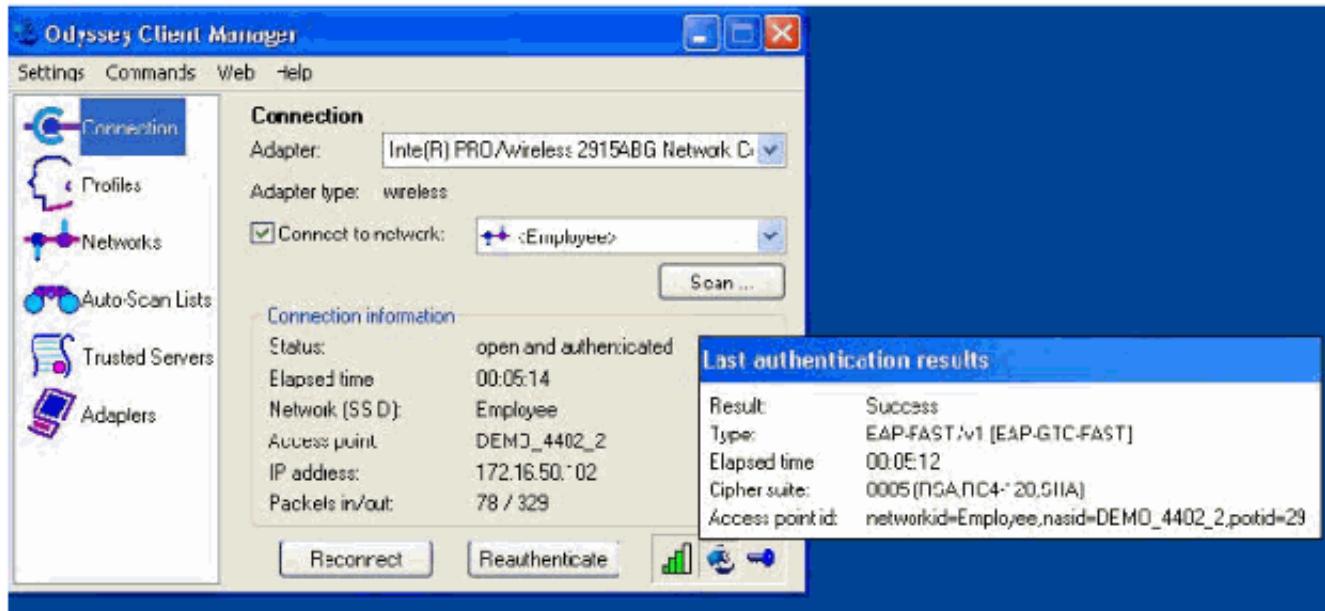
## Problema: El cliente Odyssey solicita tres veces la plataforma de autenticación Token

Este problema ocurre en todas las versiones de Windows y en la solución 2.x.

Normalmente, una configuración de servicios inalámbricos en XP hace que esto ocurra.

Complete estos pasos para corregir este problema:

1. Elija Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios.
2. Vaya a la parte inferior de la lista y busque Wireless Zero Configuration.
3. Haga doble clic en esta configuración.
4. Seleccione la opción para detener este servicio.
5. En la configuración para el tipo de inicio, seleccione **disable**.**Nota:** Si todo lo que hace es detener el servicio, se inicia de nuevo al reiniciar, por lo que debe desactivarlo para que este problema no vuelva a ocurrir.
6. Guarde los parámetros y cierre.



## La autenticación PEAP falla con el servidor ACS

Cuando su cliente falla la autenticación PEAP con un servidor ACS, verifique si encuentra el mensaje de error "*intento de autenticación duplicado NAS*" en la opción **Intentos fallidos** bajo el menú **Informe y actividad** del ACS.

Puede recibir este mensaje de error cuando Microsoft Windows XP SP2 esté instalado en el equipo cliente y Windows XP SP2 se autentique en un servidor de terceros que no sea un servidor Microsoft IAS. En particular, el servidor RADIUS de Cisco (ACS) utiliza un método

diferente para calcular la ID de formato EAP-TLV (Extensible Authentication Protocol Type:Length:Value) que el método que utiliza Windows XP. Microsoft ha identificado esto como un defecto en el suplicante XP SP2.

Para obtener una revisión, póngase en contacto con Microsoft y consulte el artículo [KB885453](#). El problema subyacente es que en el lado del cliente, con la *utilidad windows*, la opción **Fast Reconnect** está inhabilitada para PEAP de forma predeterminada. Sin embargo, esta opción está activada de forma predeterminada en el lado del servidor (ACS). Para resolver este problema, desmarque la opción **Fast Reconnect** en el servidor ACS y presione **enviar+reiniciar**. Alternativamente, puede habilitar la opción Fast Reconnect en el lado del cliente para resolver el problema.

Complete estos pasos para habilitar Fast Reconnect en el cliente que ejecuta Windows XP usando la utilidad de Windows:

1. Haga clic en **Inicio > Configuración > Panel de control**.
2. Haga doble clic en el ícono **Conexiones de red**.
3. Haga clic con el botón derecho del ratón en el ícono **Wireless Network Connection** y haga clic en **Properties**.
4. Haga clic en la pestaña **Redes inalámbricas**.
5. Marque la opción *Usar Windows para configurar los parámetros de mi red inalámbrica* para habilitar windows para configurar el adaptador del cliente.
6. Si ya ha configurado un SSID, elija el SSID y haga clic en **Propiedades**. Si no, haga clic en **Nuevo** para agregar una nueva WLAN.
7. Ingrese el SSID bajo la pestaña **Asociación**. Asegúrese de que la *Autenticación de Red* esté **Abierta** y de que el *Cifrado de Datos* esté configurado en **WEP**.
8. Haga clic en **Authentication**.
9. Marque la opción *Enable IEEE 802.1x authentication for this network*.
10. Elija el *tipo EAP* como **PEAP** y haga clic en **Propiedades**.
11. Marque la opción **Enable Fast Reconnect** en la parte inferior de la



página.

## 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](#)