PEAP en UWN con ACS 5.1 y Windows 2003 Server

Contenido

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) 5.1 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 la tecnología inalámbrica segura, consulte el sitio web de Microsoft Wi-Fi y el plan inalámbrico de Cisco SAFE.

Prerequisites

Requirements

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

Para obtener información sobre la instalación y configuración iniciales de los controladores de la serie 5508 de Cisco, refiérase a la Guía de Instalación del Controlador de Red Inalámbrica de la Serie 5500 de Cisco. Para obtener información sobre la configuración e instalación inicial de los Cisco 2100 Series Controllers, consulte la Guía de inicio rápido: Cisco 2100 Series Wireless LAN Controller.

Puede encontrar las guías de instalación y configuración de Microsoft Windows 2003 en Instalación de Windows Server 2003 R2 .

Antes de comenzar, instale el sistema operativo Microsoft Windows Server 2003 con 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 actualizaciones de software más recientes.

Windows Server 2003 con SP1, Enterprise Edition se utiliza para configurar la inscripción automática de certificados de usuario y estación de trabajo para la autenticación PEAP. La inscripción automática y la renovación automática de certificados facilitan la implementación de certificados y mejoran la seguridad al expirar y renovar automáticamente los certificados.

Componentes Utilizados

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

- Cisco 2106 o 5508 Series Controller que ejecuta 7.0.98.0
- Punto de acceso de protocolo de punto de acceso ligero (LWAPP) Cisco 1142
- Windows 2003 Enterprise con Internet Information Server (IIS), autoridad certificadora (CA), DHCP y sistema de nombres de dominio (DNS) instalado
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional con SP (y Service Packs actualizados) y tarjeta de interfaz de red inalámbrica (NIC) (compatible con CCX v3) o un solicitante de terceros.
- Switch Cisco 3750

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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.

Configurar

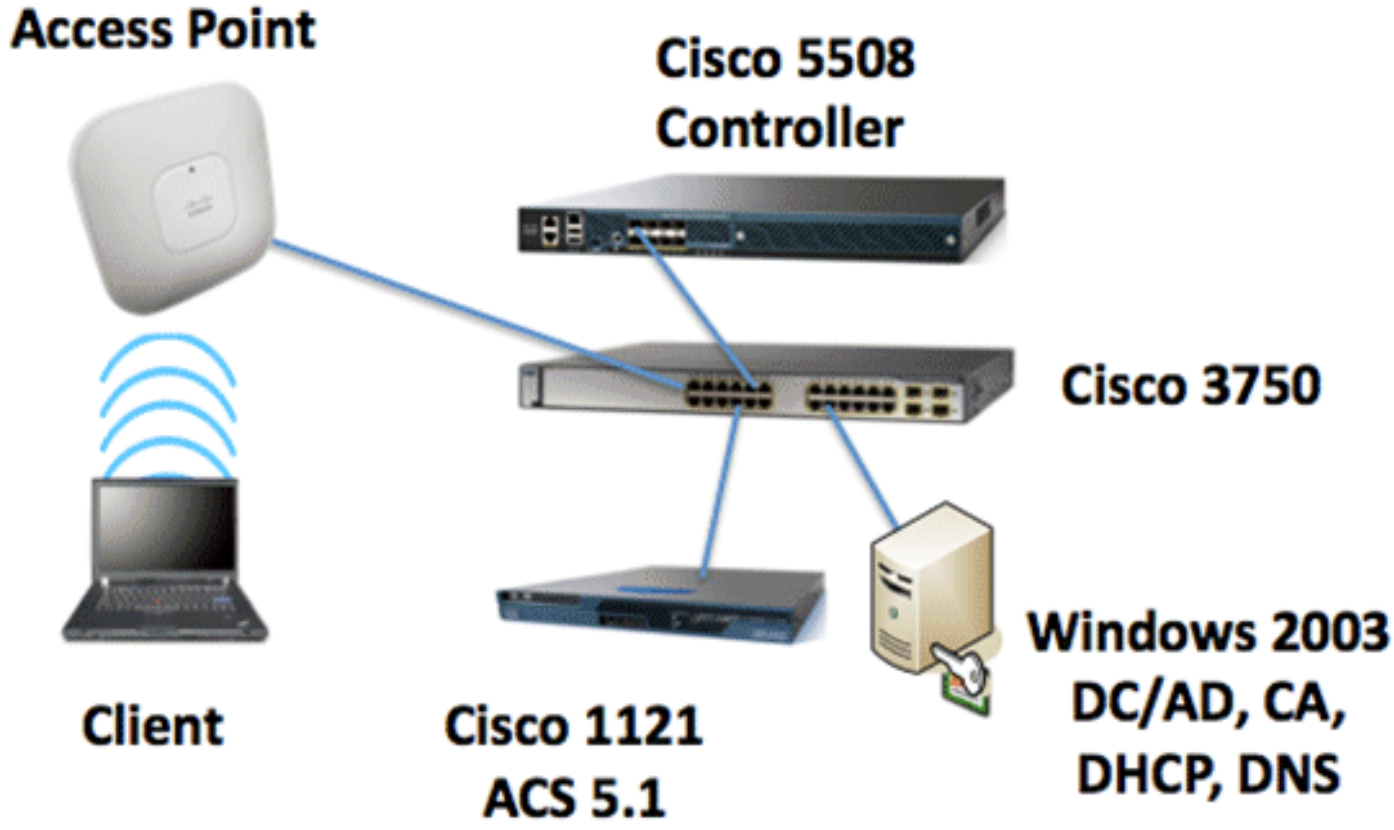
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Topología de Cisco Secure Wireless Lab



El objetivo principal de este documento es proporcionarle el procedimiento paso a paso para implementar PEAP en Redes inalámbricas unificadas con ACS 5.1 y el servidor Windows 2003 Enterprise. El énfasis principal está en la inscripción automática del cliente para que el cliente se inscriba automáticamente y tome el certificado del servidor.

Nota: Para agregar el acceso Wi-Fi protegido (WPA)/WPA2 con el protocolo de integridad de clave temporal (TKIP)/estándar de cifrado avanzado (AES) a Windows XP Professional con SP, consulte la actualización de WPA2/Wireless Provisioning Services Information Element (WPS IE)

para Windows XP con Service Pack 2 .

Instalación de Windows Enterprise 2003 con IIS, autoridad certificadora, DNS, DHCP (CA)

CA (democa)

CA es un equipo que ejecuta Windows Server 2003 con SP2, Enterprise Edition y realiza estas funciones:

- Un controlador de dominio para el dominio **demo.local** que ejecuta IIS
- Un servidor DNS para el dominio DNS **demo.local**
- Un servidor DHCP
- CA raíz de empresa para el dominio **demo.local**

Realice estos pasos para configurar la CA para estos servicios:

1. Realice una instalación y configuración básicas.
2. Configure el equipo como controlador de dominio.
3. Elevar 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 equipos al dominio.
8. Permitir el acceso inalámbrico a los equipos.
9. Agregue usuarios al dominio.
10. Permitir el acceso inalámbrico a los usuarios.
11. Agregue grupos al dominio.
12. Agregue usuarios al grupo de usuarios inalámbricos.
13. Agregue los equipos cliente al grupo de usuarios inalámbricos.

Instalación y configuración básicas

Siga estos pasos:

1. Instale Windows Server 2003 con SP2, Enterprise Edition, como servidor independiente.
2. Configure el protocolo TCP/IP con la dirección IP *10.0.10.10* y la máscara de subred *255.255.255.0*.

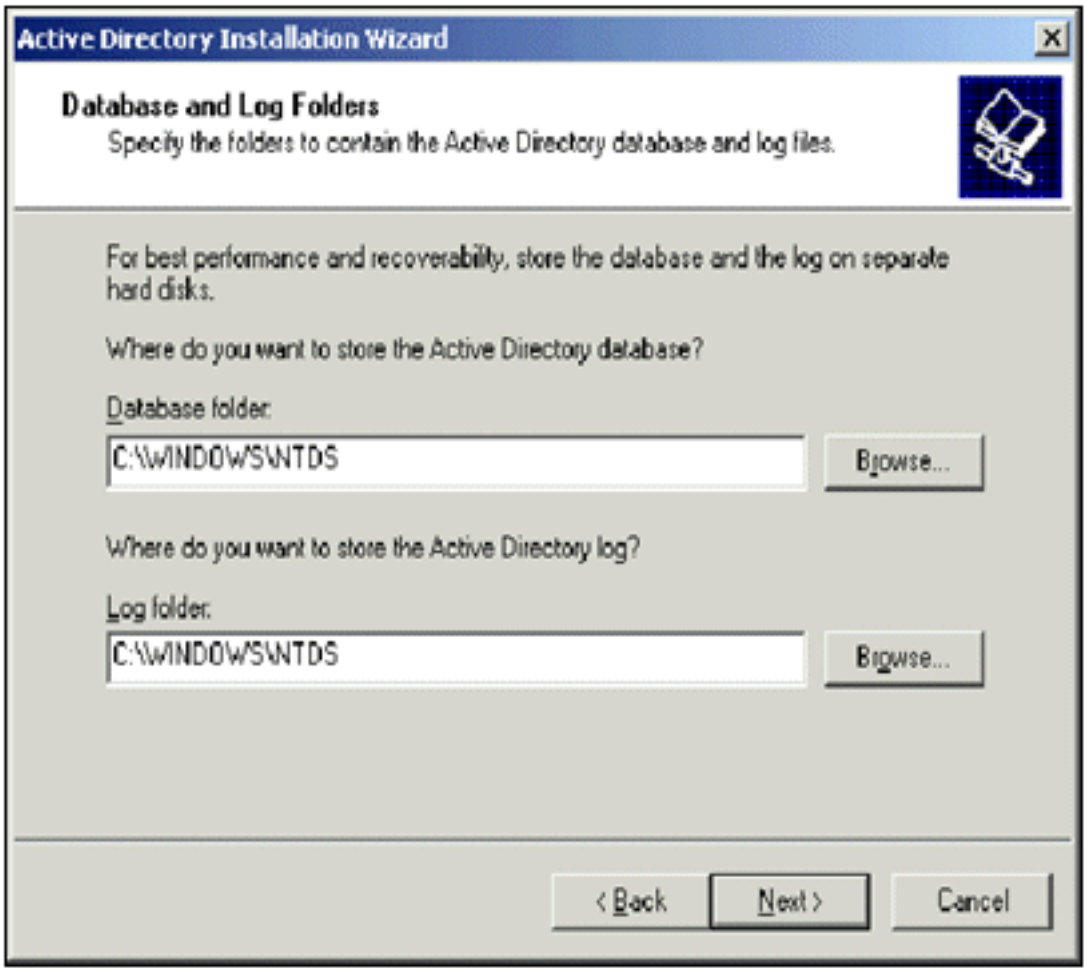
Configurar el equipo como controlador de dominio

Siga 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 Asistente para instalación de Active Directory, haga clic en **Siguiente**.
3. En la página Compatibilidad con el sistema operativo, haga clic en **Siguiente**.
4. En la página Tipo de controlador de dominio, seleccione **Controlador de dominio para un**

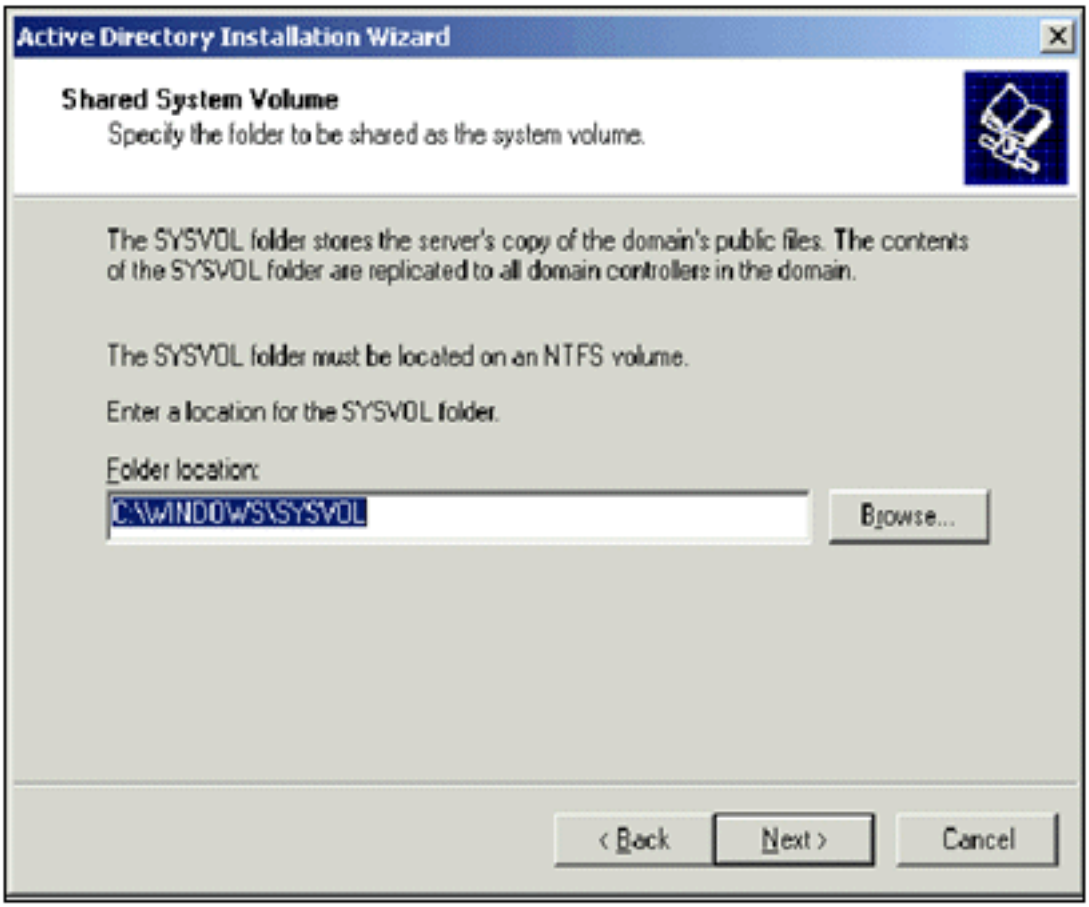
nuevo dominio y haga clic en **Siguiente**.

5. En la página Crear nuevo dominio, seleccione **Dominio en un nuevo bosque** y haga clic en **Siguiente**.
6. En la página Instalar o configurar DNS, seleccione **No, simplemente instale y configure DNS en este equipo** y haga clic en **Siguiente**.
7. En la página Nuevo nombre de dominio, escriba **demo.local** y haga clic en **Siguiente**.
8. En la página NetBIOS Domain Name (Nombre de dominio NetBIOS), introduzca el nombre NetBIOS del dominio como **demo** y haga clic en **Next** (Siguiente).
9. En la página Ubicaciones de la Base de Datos y las Carpetas de Registro, acepte los directorios predeterminados de la Base de Datos y las Carpetas de Registro y haga clic en



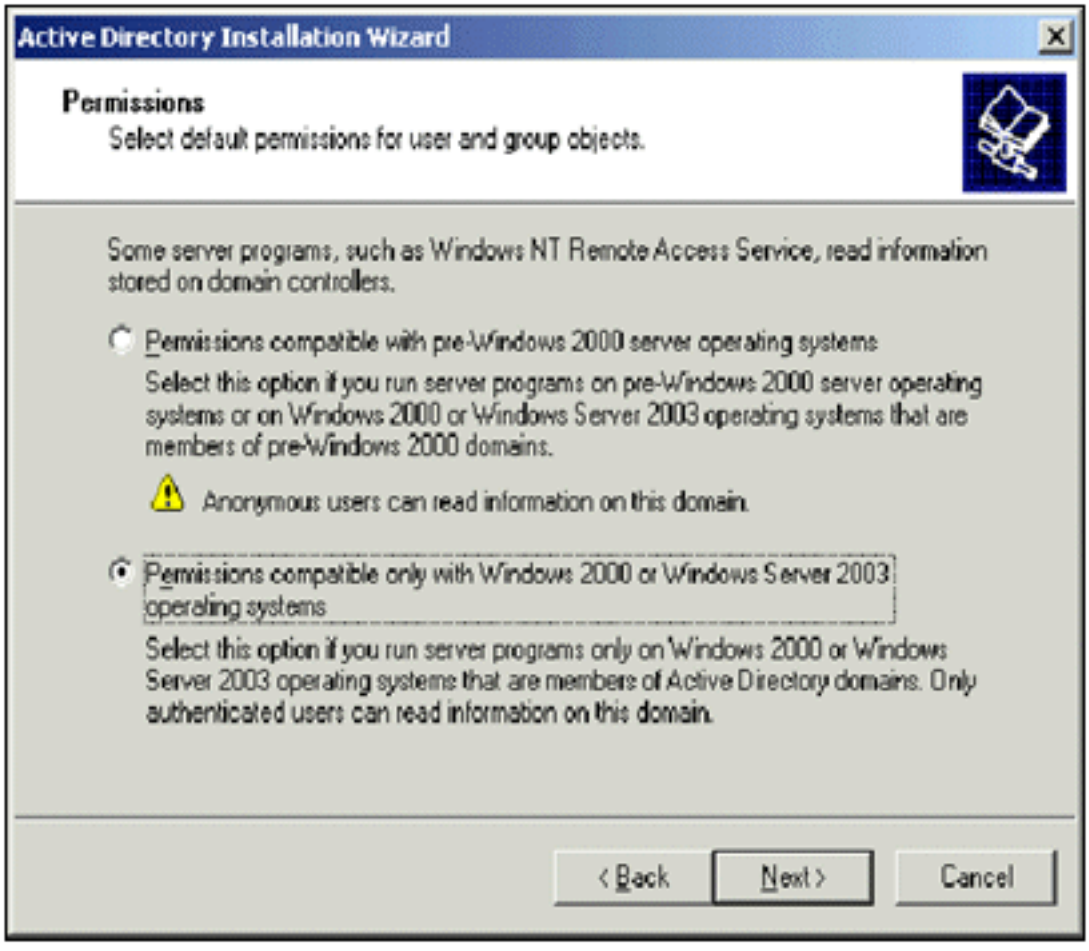
Siguiente.

10. En la página Volumen del sistema compartido, compruebe que la ubicación de la carpeta predeterminada es correcta y haga clic en



Siguiente.

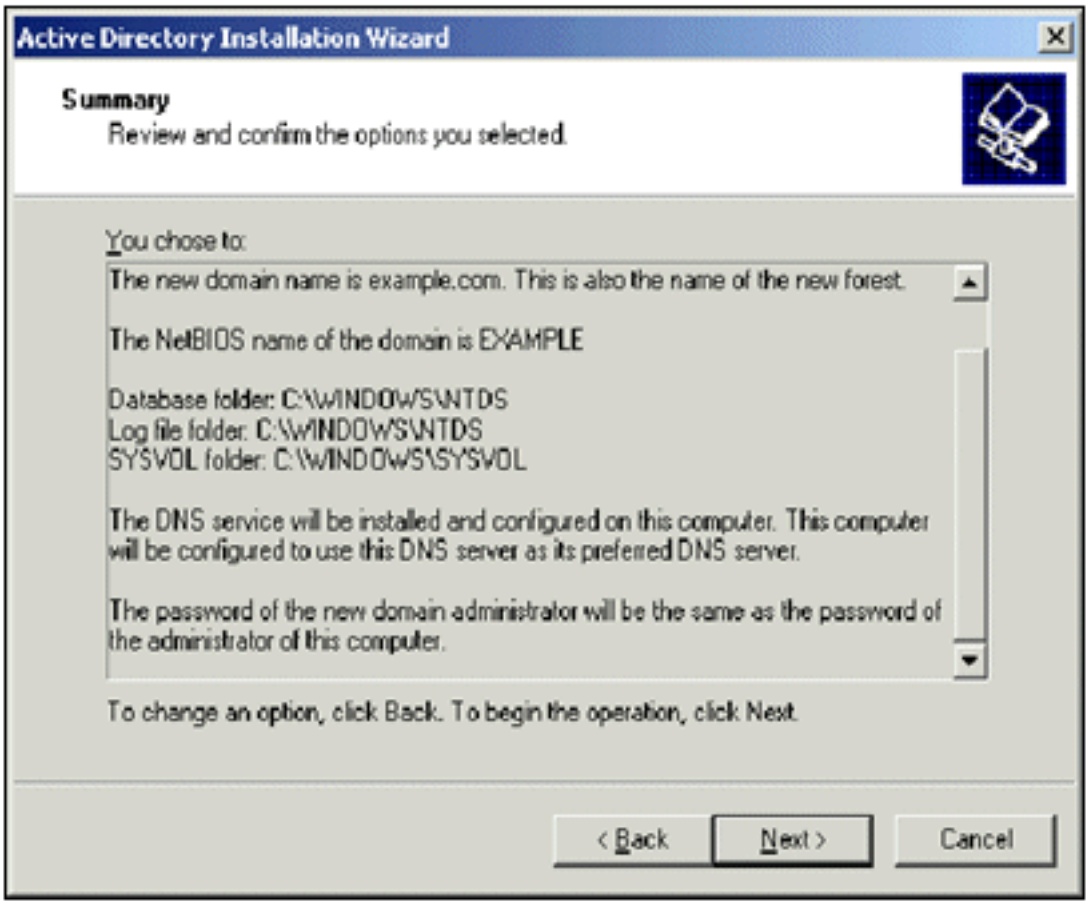
11. En la página Permisos, compruebe que la opción **Permisos compatibles sólo con los sistemas operativos Windows 2000 o Windows Server 2003** está seleccionada y haga clic



en **Siguiente**.

12. En la página Contraseña de administración del modo de restauración de servicios de directorio, deje los cuadros de contraseña en blanco y haga clic en **Siguiente**.

13. Revise la información en la página Resumen y haga clic en Siguiente.

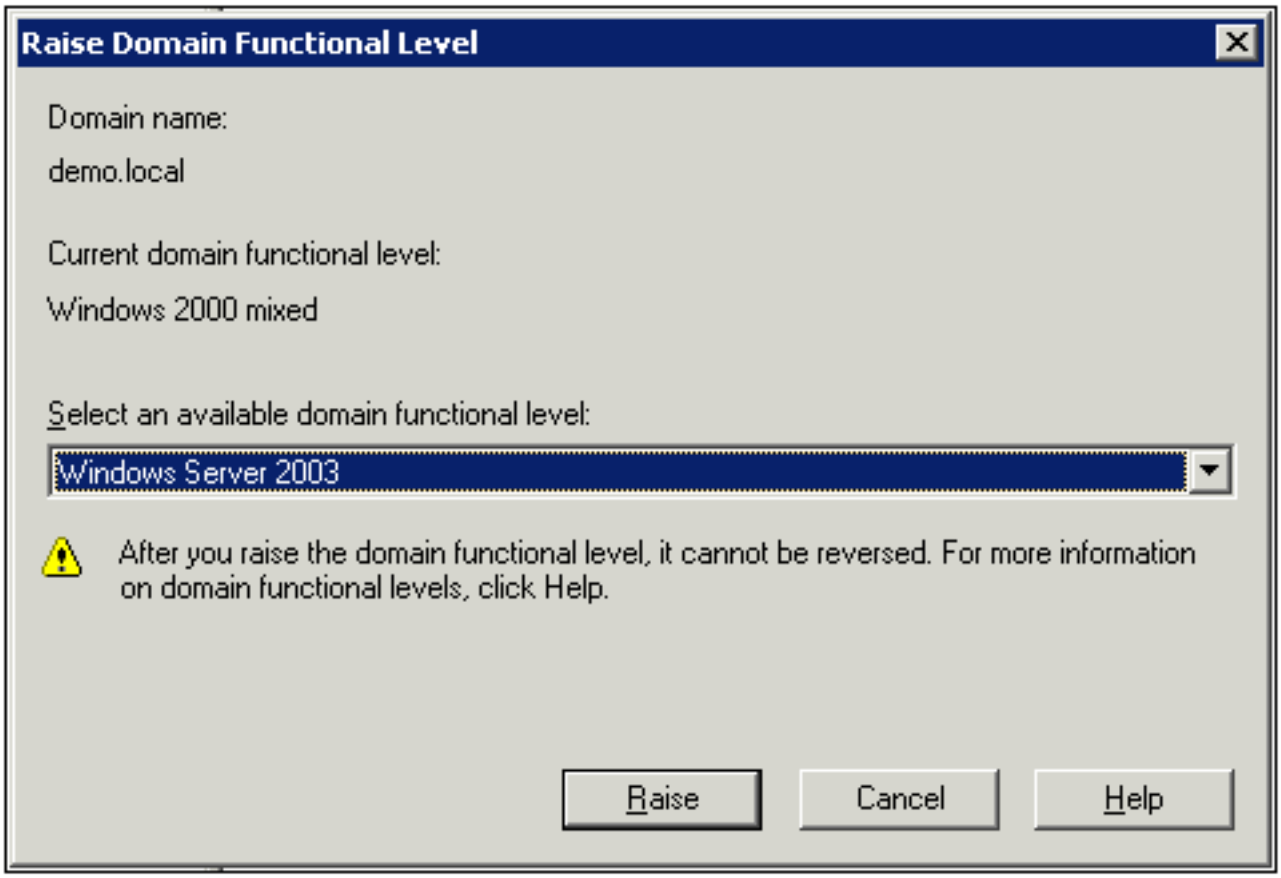


14. Cuando haya terminado con la instalación de Active Directory, haga clic en **Finalizar**.
15. Cuando se le solicite que reinicie el ordenador, haga clic en **Reiniciar ahora**.

Elevar el nivel funcional del dominio

Siga estos pasos:

1. Abra el complemento Dominios y confianzas de Active Directory desde la carpeta Herramientas administrativas (Inicio > Programas > Herramientas administrativas > **Dominios y confianzas de Active Directory**) y, a continuación, haga clic con el botón secundario del mouse en el equipo del dominio CA.demo.local.
2. Haga clic en **Elevar el nivel funcional del dominio** y, a continuación, seleccione **Windows Server 2003** en la página Elevar el nivel funcional del dominio.

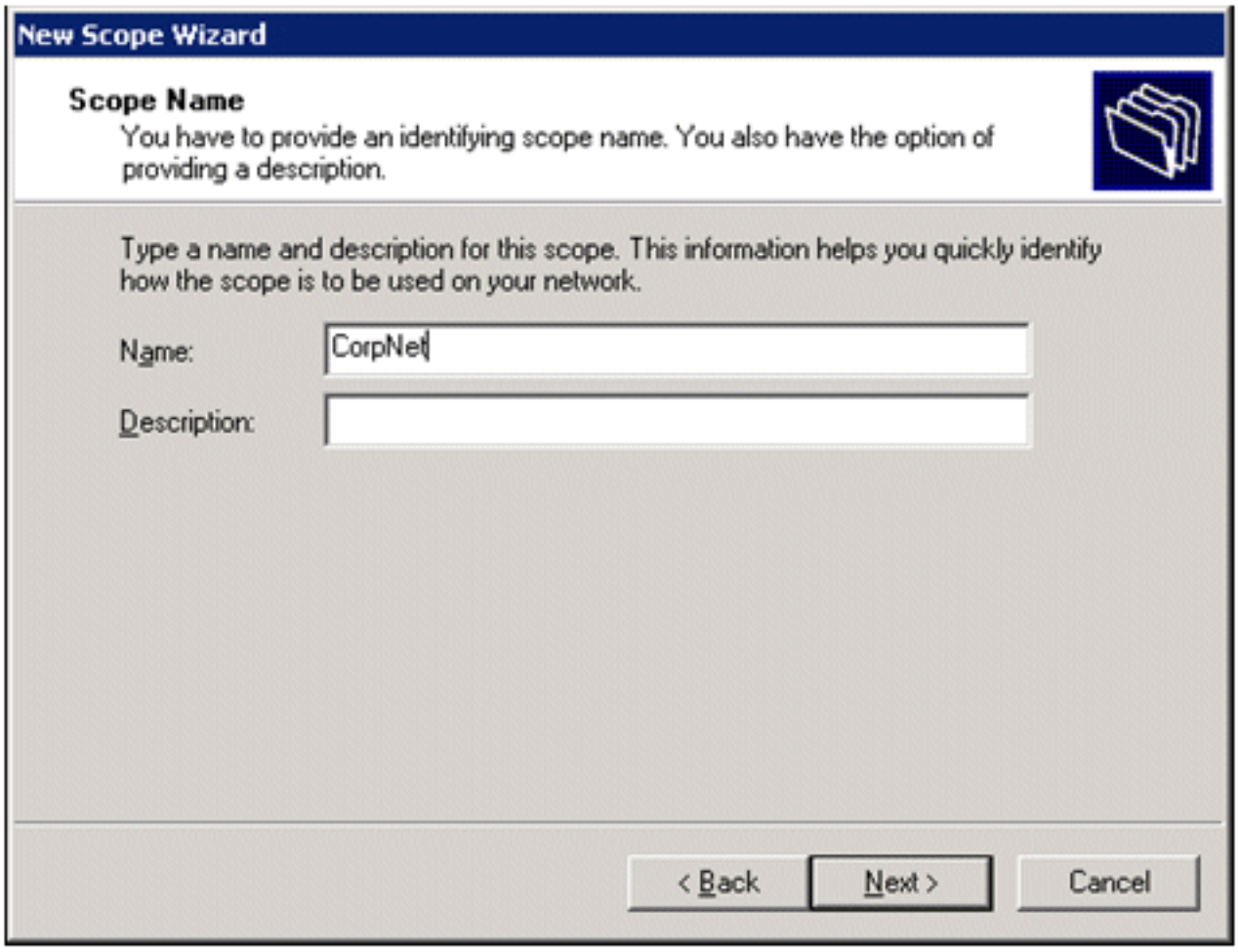


3. Haga clic en **Raise**, haga clic en **OK**, y luego haga clic en **OK** nuevamente.

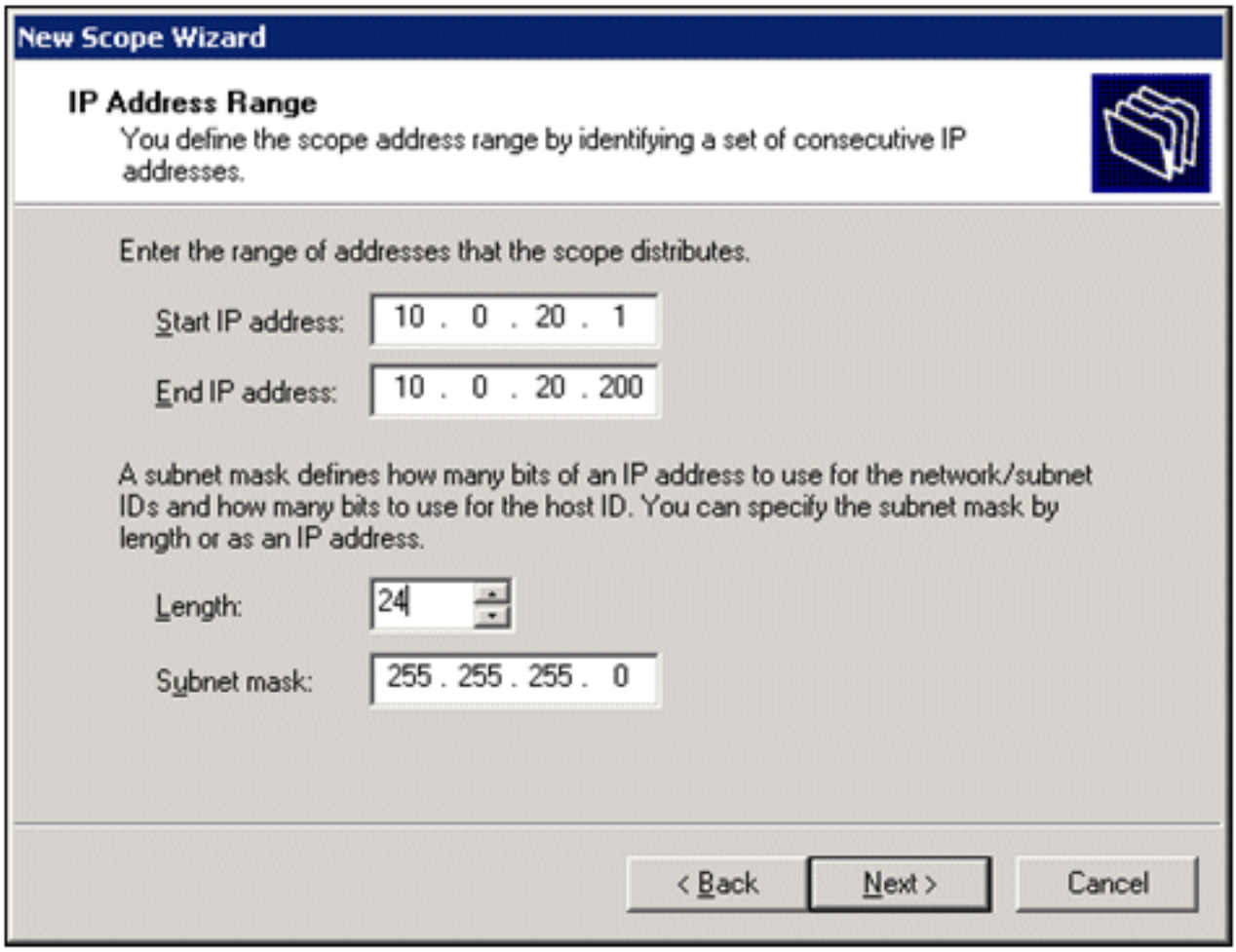
Instalación y configuración de DHCP

Siga estos pasos:

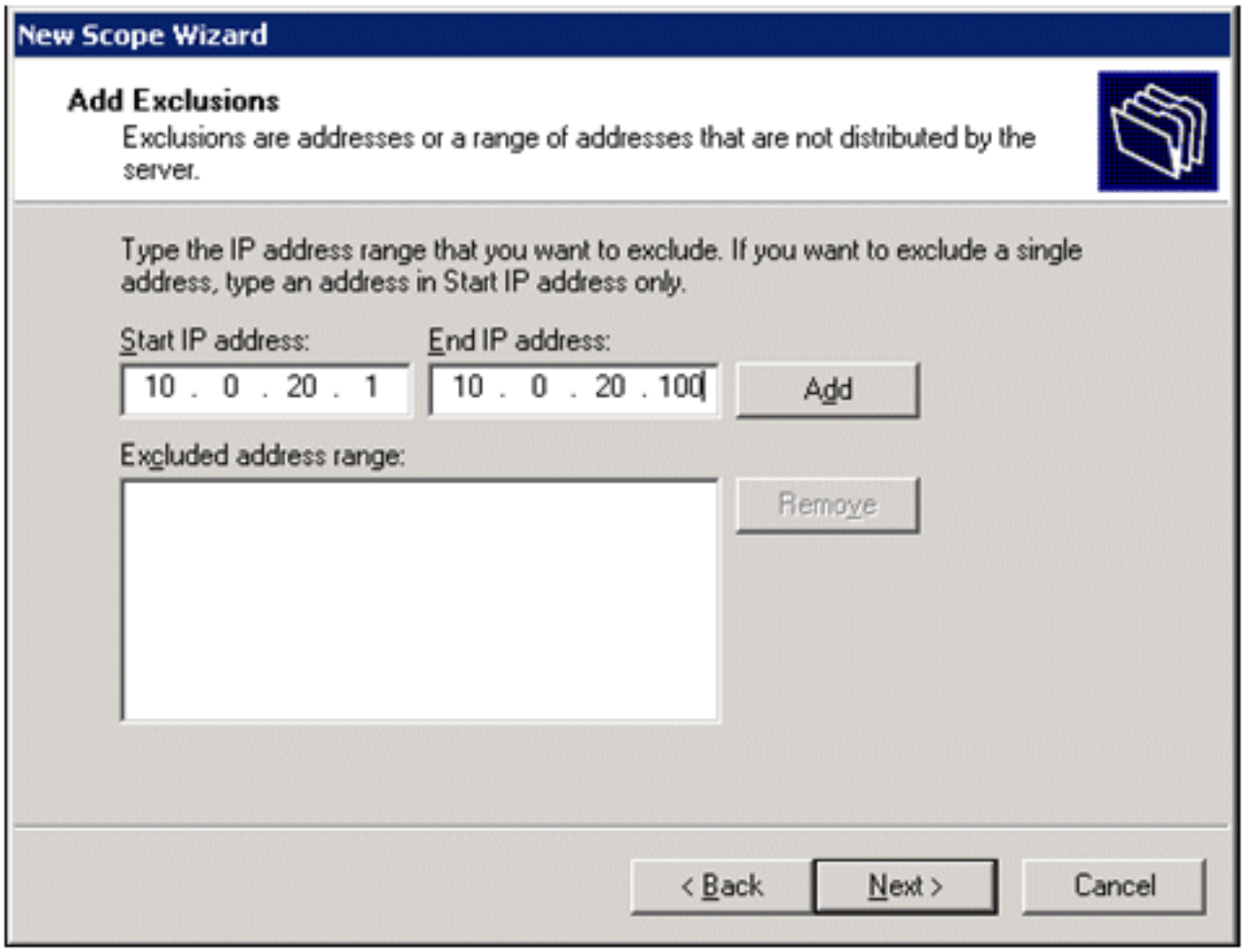
1. Instale el **Protocolo de configuración dinámica de host (DHCP)** como un componente del **Servicio de red** mediante **Agregar o quitar programas** en el Panel de control.
2. Abra el complemento DHCP desde la carpeta Herramientas administrativas (Inicio > Programas > Herramientas administrativas > **DHCP**) y, a continuación, resalte el servidor DHCP, CA.demo.local.
3. Haga clic en **Acción**, y después haga clic en **Autorizar** para autorizar el servicio DHCP.
4. En el árbol de consola, haga clic con el botón secundario en **CA.demo.local** y, a continuación, haga clic en **Ámbito nuevo**.
5. En la página de bienvenida del Asistente para ámbito nuevo, haga clic en **Siguiente**.
6. En la página Nombre del ámbito, escriba **CorpNet** en el campo Nombre.



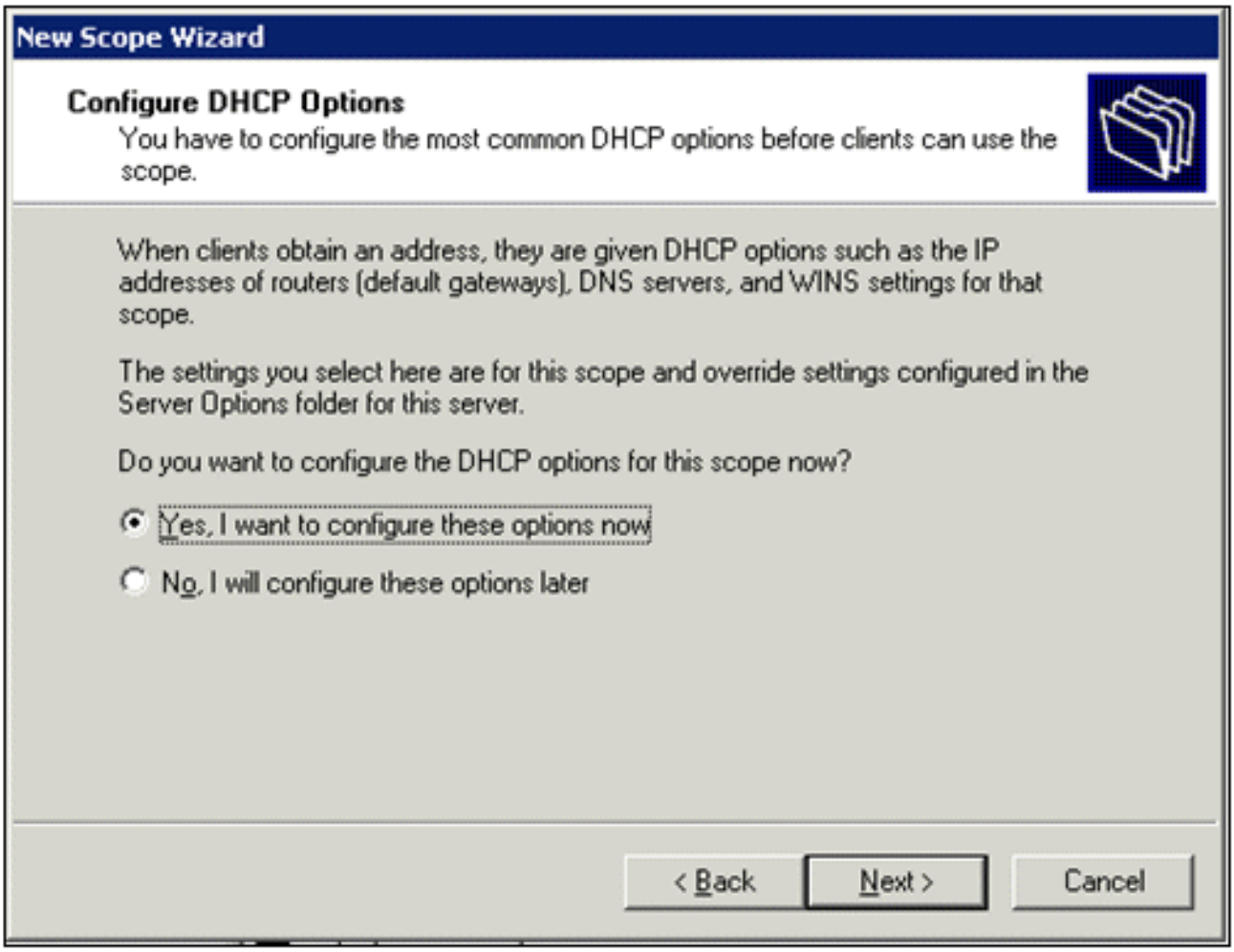
7. Haga clic en **Next** y rellene estos parámetros:Dirección IP inicial: **10.0.20.1**Dirección IP final: **10.0.20.200**Longitud: **24**Máscara de subred: **255.255.255.0**



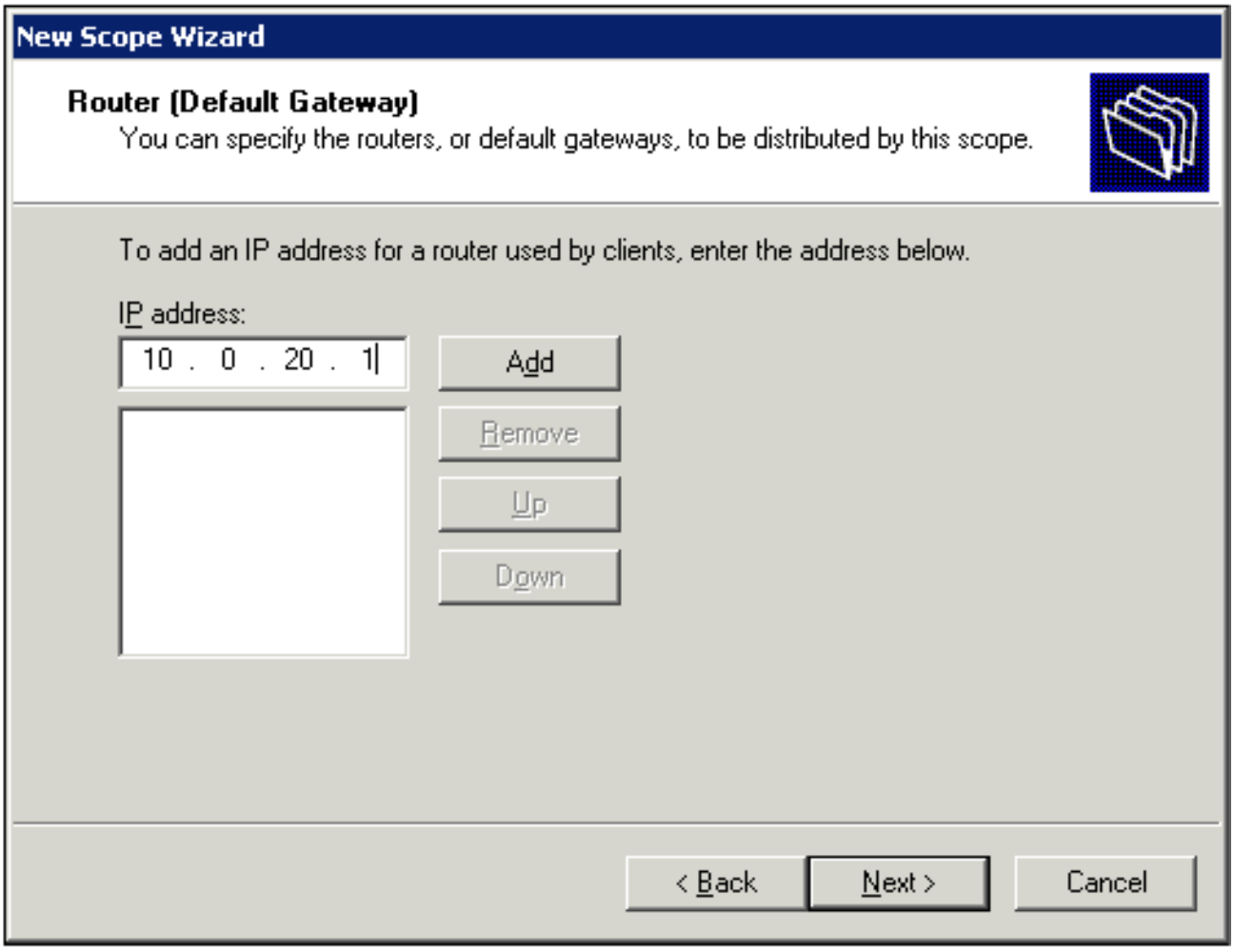
8. Haga clic en **Next** e ingrese *10.0.20.1* para la dirección IP inicial y *10.0.20.100* para la dirección IP final que se excluirá. Luego haga clic en Next (Siguiente). Esto reserva las direcciones IP en el rango de 10.0.20.1 a 10.0.20.100. El servidor DHCP no asigna estas direcciones IP de
reserva.



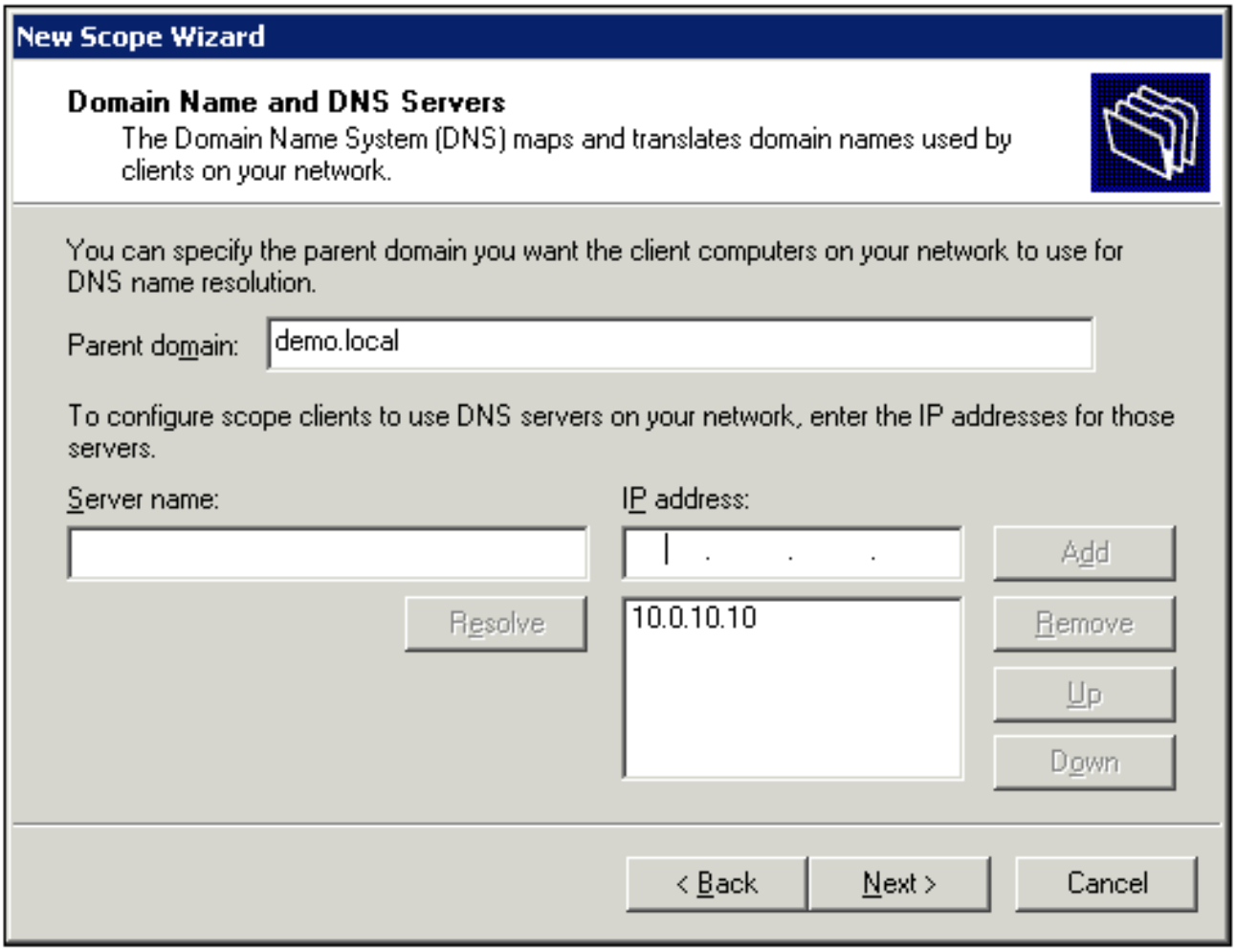
9. En la página Duración de la concesión, haga clic en **Siguiente**.
10. En la página Configure DHCP Options (Configurar opciones DHCP), seleccione **Yes, I want to configure these options now** (Sí, deseo configurar estas opciones ahora) y haga clic en **Next**.



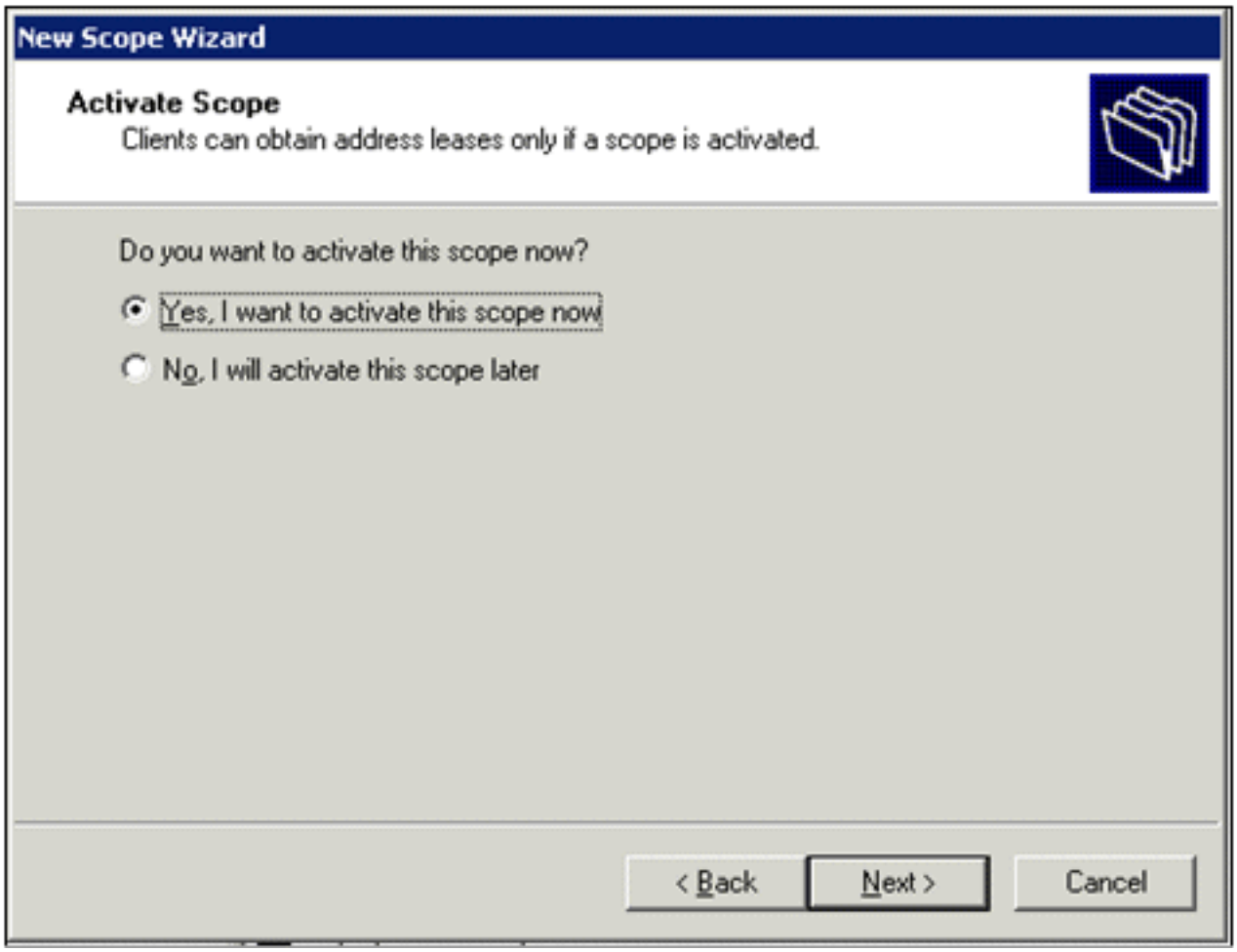
11. En la página Router (Default Gateway) (Router [Puerta de enlace predeterminada]), agregue la dirección predeterminada del router *10.0.20.1* y haga clic en **Next** (Siguiente).



12. En la página Nombre de dominio y servidores DNS, escriba *demo.local* en el campo Dominio principal, escriba *10.0.10.10* en el campo Dirección IP y, a continuación, haga clic en **Agregar** y en **Siguiente**.



13. En la página Servidores WINS, haga clic en **Siguiente**.
14. En la página Activar ámbito, elija **Sí, deseo activar este ámbito ahora** y haga clic en **Siguiente**.



15. Cuando termine con la página Asistente para ámbito nuevo, haga clic en **Finalizar**.

Instalar Servicios de Certificate Server

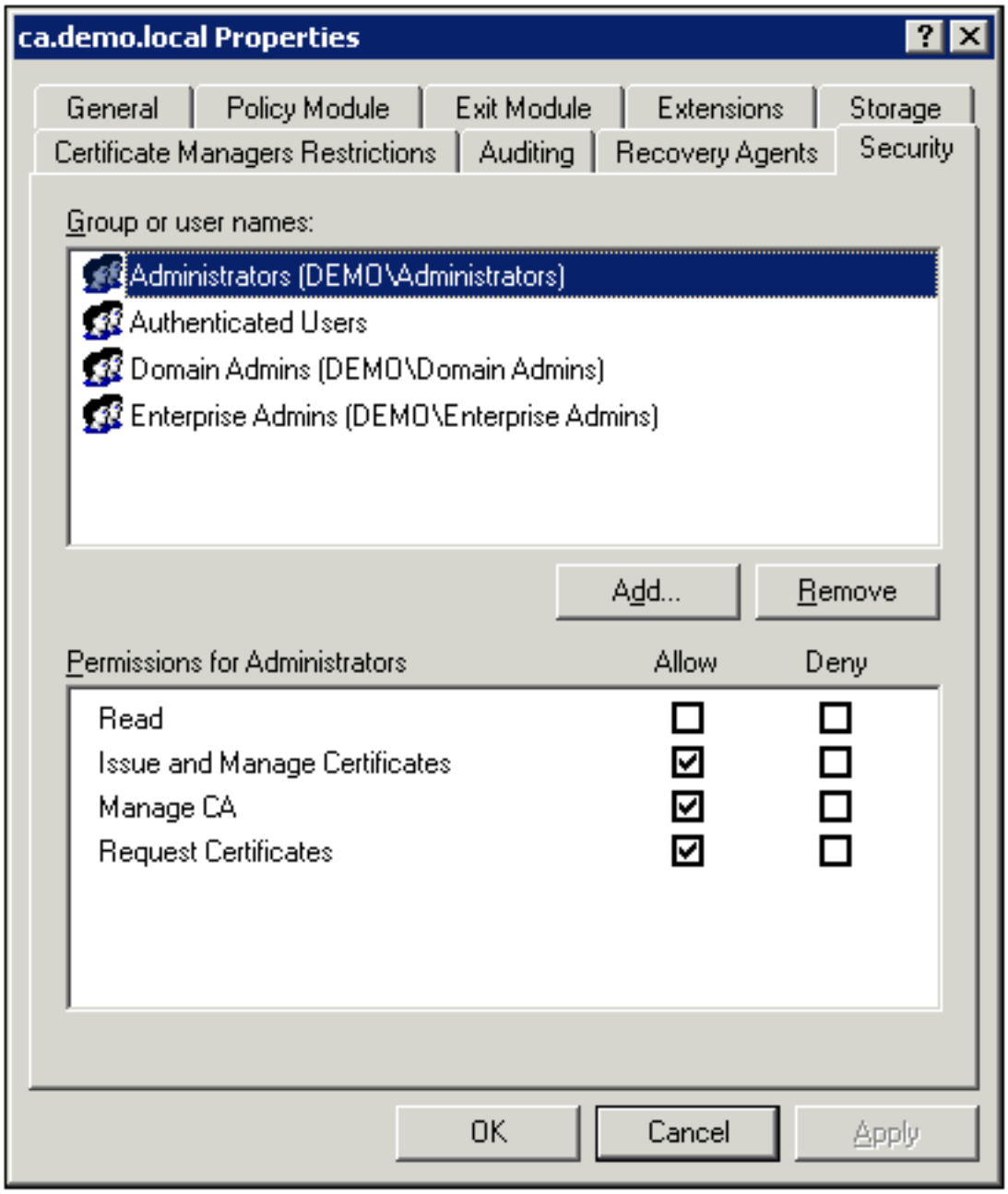
Siga estos pasos:

Nota: IIS debe estar instalado antes de instalar Servicios de Certificate Server y el usuario debe formar parte de la unidad organizativa de administración de empresas.

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 Certificate Server y, a continuación, haga clic en Siguiente.
3. En la página Tipo de CA, seleccione CA raíz de empresa y haga clic en Siguiente.
4. En la página Información de identificación de CA, escriba *democa* en el cuadro Nombre común para esta CA. También puede introducir los otros detalles opcionales. A continuación, haga clic en **Siguiente** y 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 **Finish**.
6. Haga clic en **Aceptar** después de leer el mensaje de advertencia sobre la instalación de IIS.

Comprobar permisos de administrador para certificados

Siga estos pasos:

1. Elija **Start > Administrative Tools > Certification Authority**.
2. Haga clic con el botón secundario en **democa CA** y, a continuación, haga clic en **Propiedades**.
3. En la ficha Seguridad, haga clic en **Administradores** en la lista Nombres de grupos o usuarios.
4. En la lista Permisos para administradores, compruebe que estas opciones están establecidas en **Permitir**:Emitir y administrar certificadosAdministrar CASolicitar certificadosSi alguna de estas opciones está establecida en Denegar o no está seleccionada, establezca los permisos en 

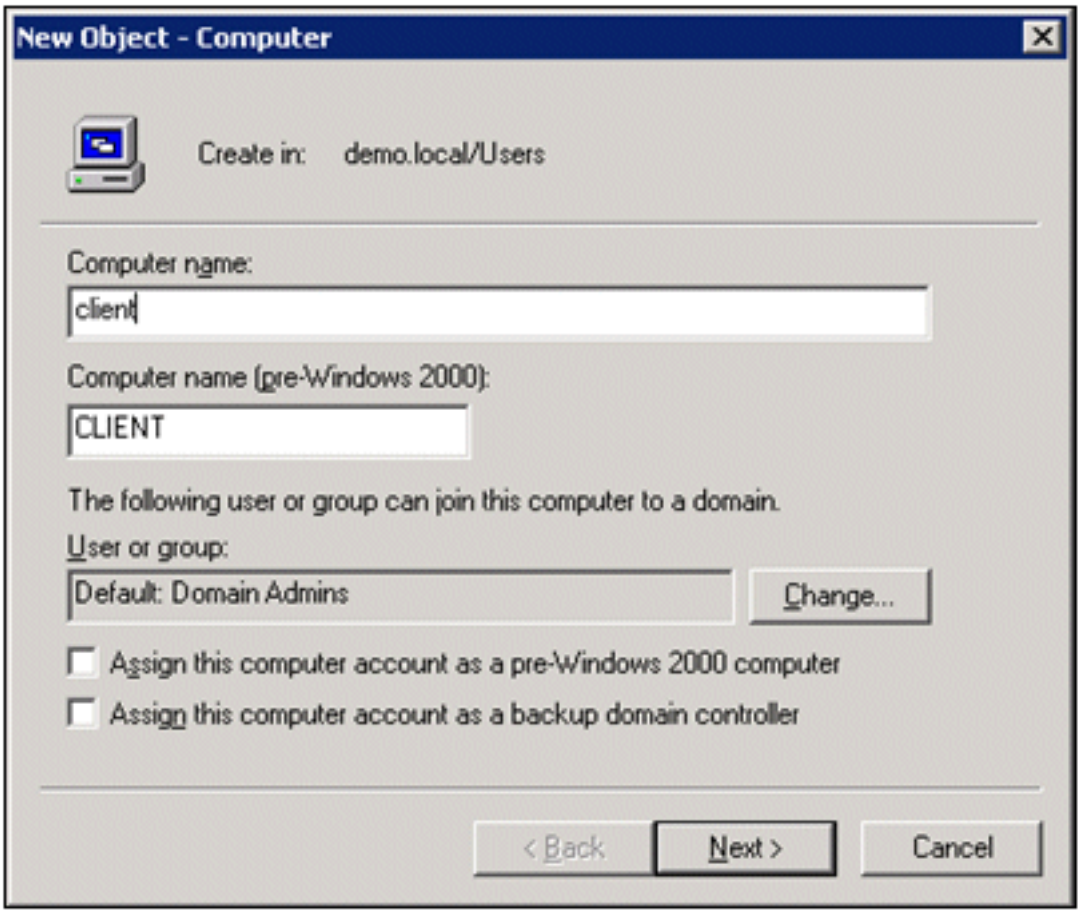
Permitir.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Propiedades de la entidad emisora de certificados democa y, a continuación, cierre Entidad emisora de certificados.

Agregar equipos al dominio

Siga 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 **demo.local**.
3. Haga clic con el botón secundario en **Equipos**, 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 de equipo y haga clic en **Siguiente**. En este ejemplo se utiliza el nombre de equipo *Client*.

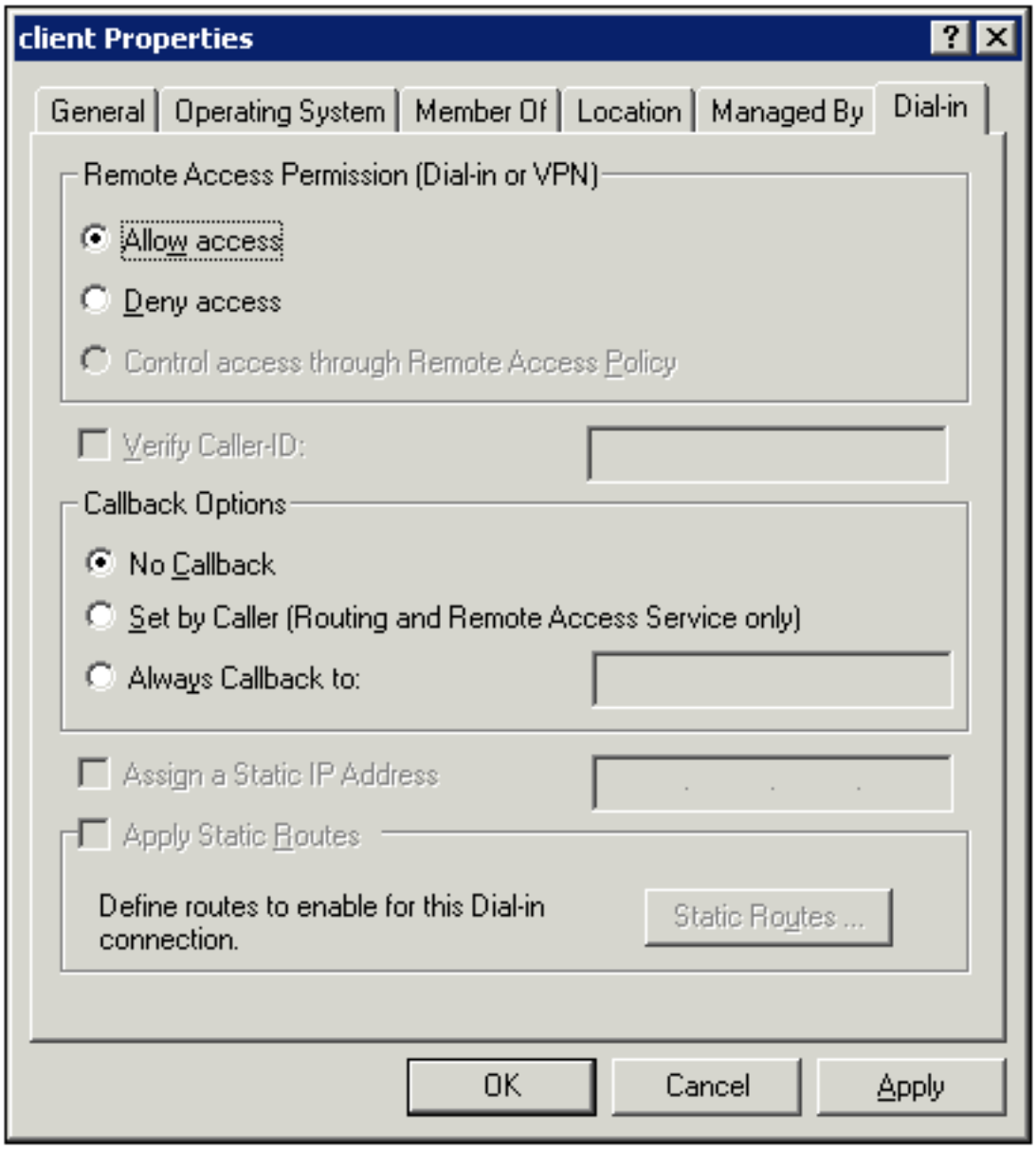


5. En el cuadro de diálogo Administrado, haga clic en **Siguiente**.
6. En el cuadro de diálogo Nuevo objeto - Equipo, haga clic en **Finalizar**.
7. Repita los pasos 3 a 6 para crear cuentas de equipo adicionales.

Permitir el acceso inalámbrico a ordenadores

Siga 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 secundario del mouse (ratón) en el equipo al que desea asignar acceso inalámbrico. Este ejemplo muestra el procedimiento con el equipo **Client** que agregó en el paso 7. Haga clic en **Properties** y, a continuación, vaya a la ficha **Dial-in**.
2. En el Permiso de acceso remoto, elija **Permitir acceso** y haga clic en

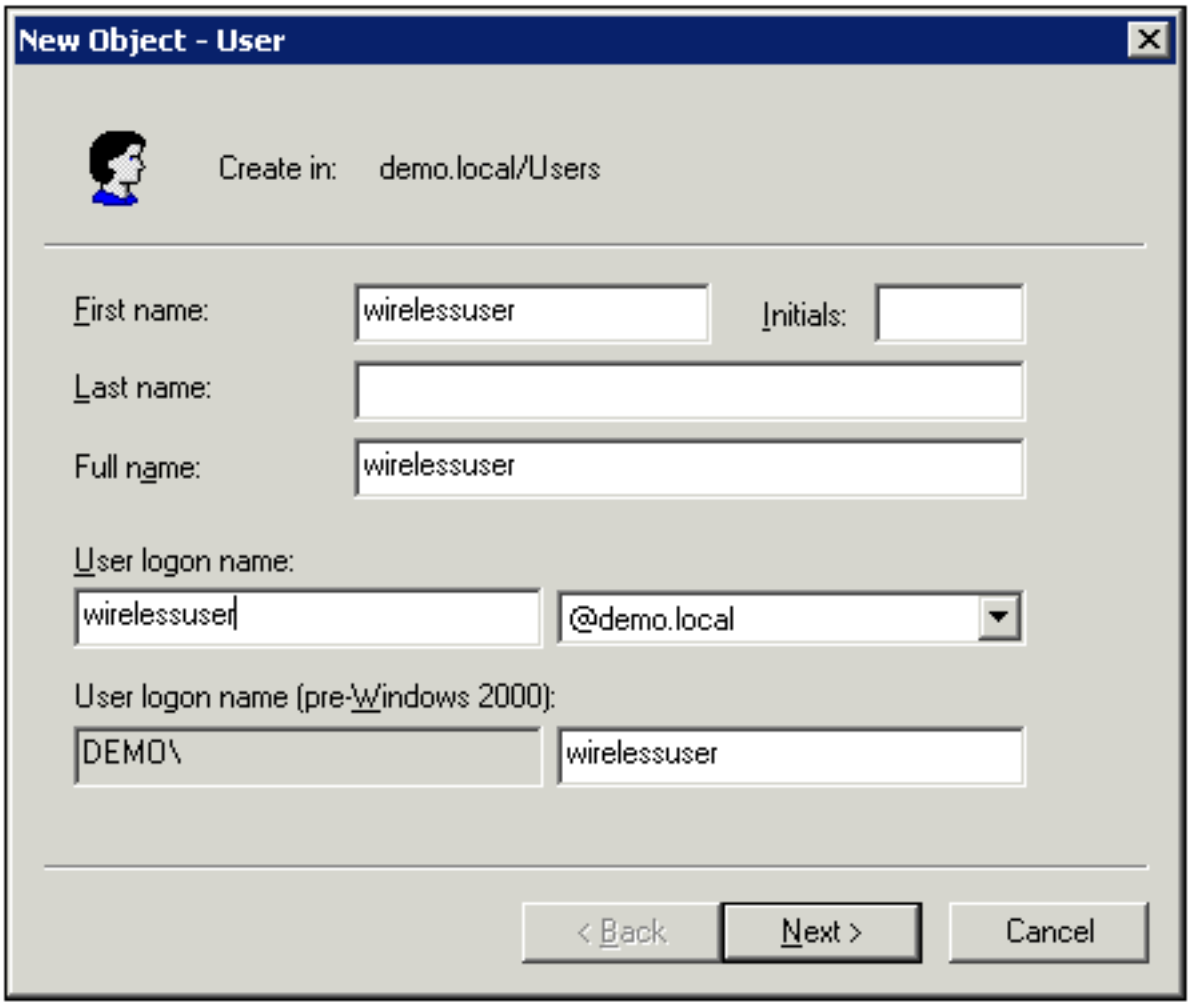


Aceptar.

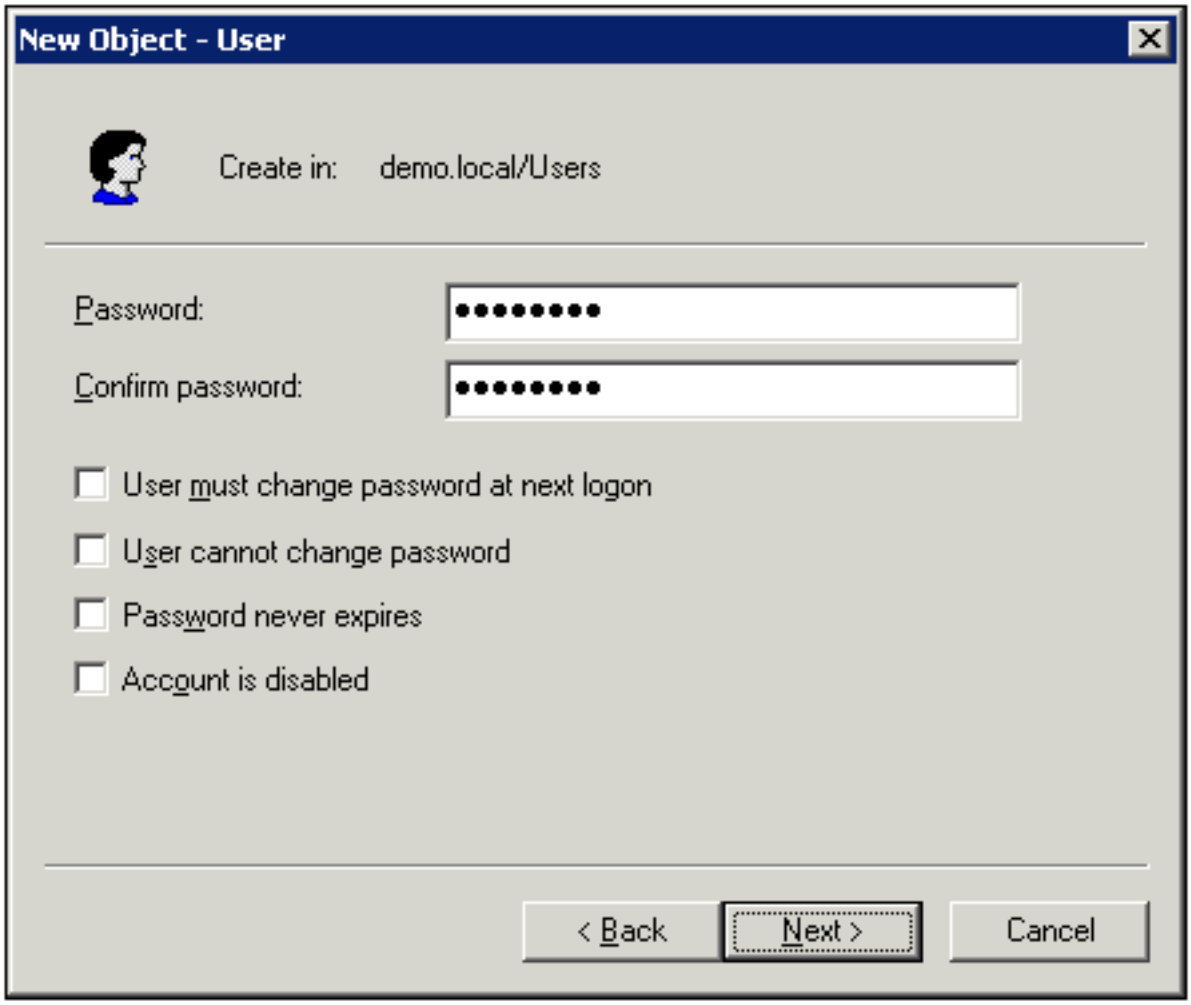
[Agregar usuarios al dominio]

Siga estos pasos:

1. En el árbol de consola Usuarios y equipos de Active Directory, haga clic con el botón secundario 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 (Nombre) y *wirelessuser* en el campo User logon name (Nombre de inicio de sesión de usuario). 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 la próxima vez que inicie sesión** y haga clic en **Siguiente**.



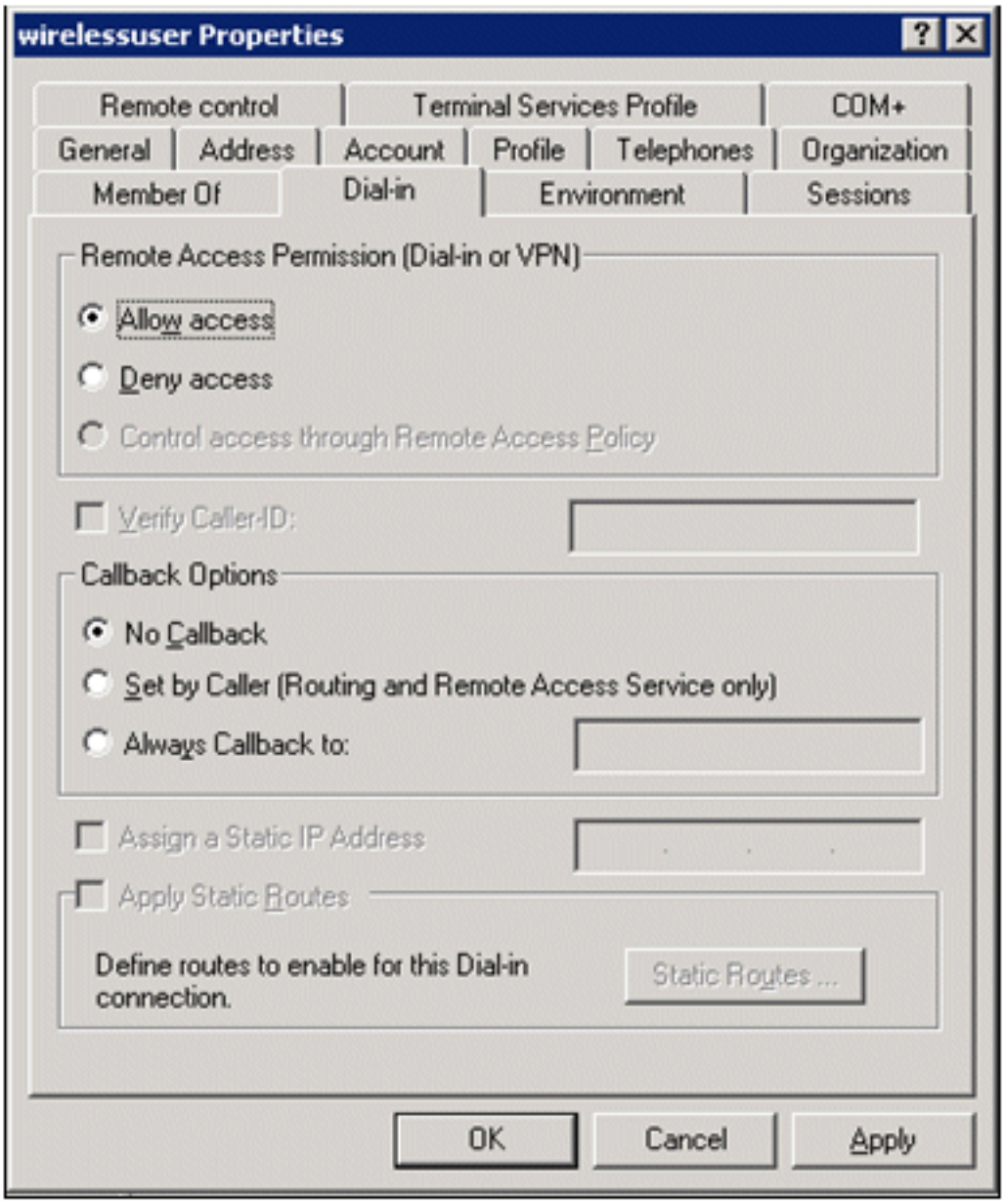
4. En el cuadro de diálogo Nuevo objeto - Usuario, haga clic en **Finalizar**.
5. Repita los pasos del 2 al 4 para crear cuentas de usuario adicionales.

Permitir el acceso inalámbrico a los usuarios

Siga 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 secundario en **Usuario inalámbrico**, haga clic en **Propiedades** y, a continuación, vaya a la pestaña **Marcado de entrada**.
2. En el Permiso de acceso remoto, elija **Permitir acceso** y haga clic en

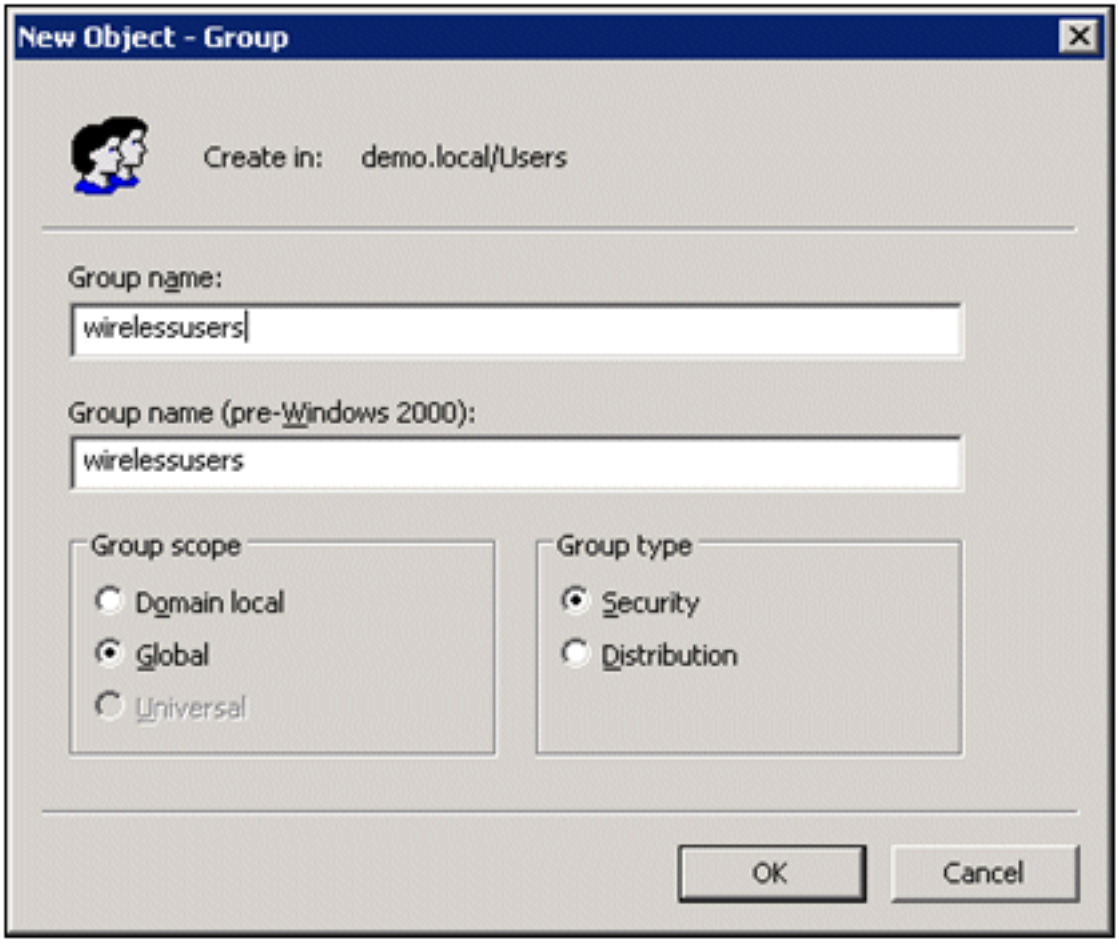
Aceptar.



[Agregar grupos al dominio]

Siga estos pasos:

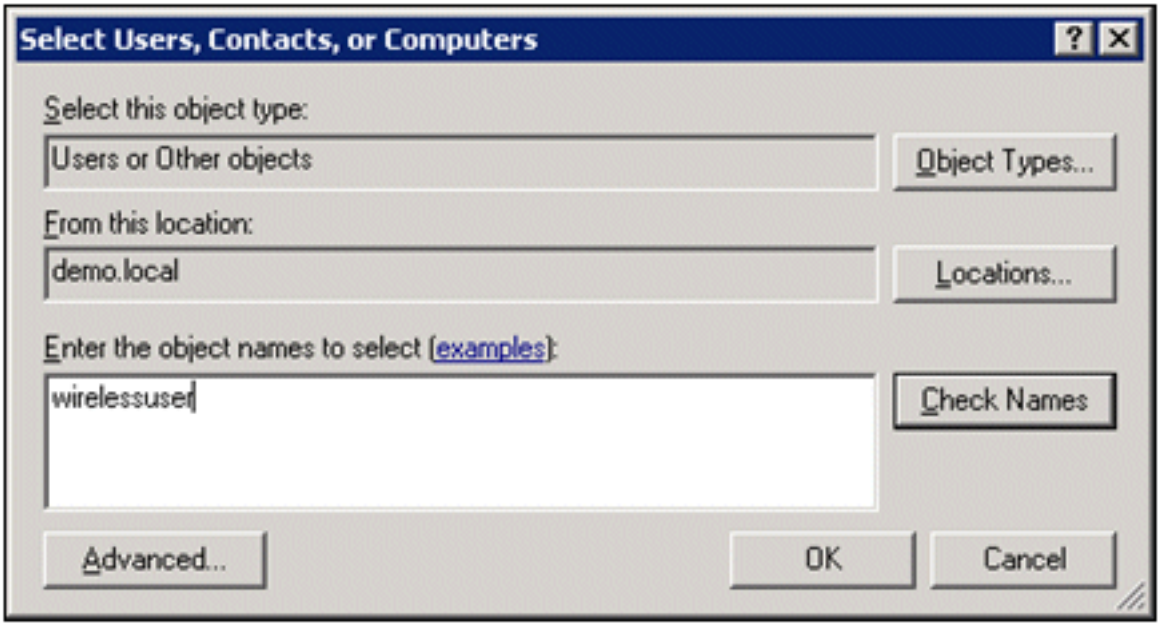
1. En el árbol de consola Usuarios y equipos de Active Directory, haga clic con el botón secundario en **Usuarios**, haga clic en **Nuevo** y, a continuación, haga clic en **Grupo**.
2. En el cuadro de diálogo Nuevo objeto - Grupo, escriba el nombre del grupo en el campo Nombre del grupo y haga clic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



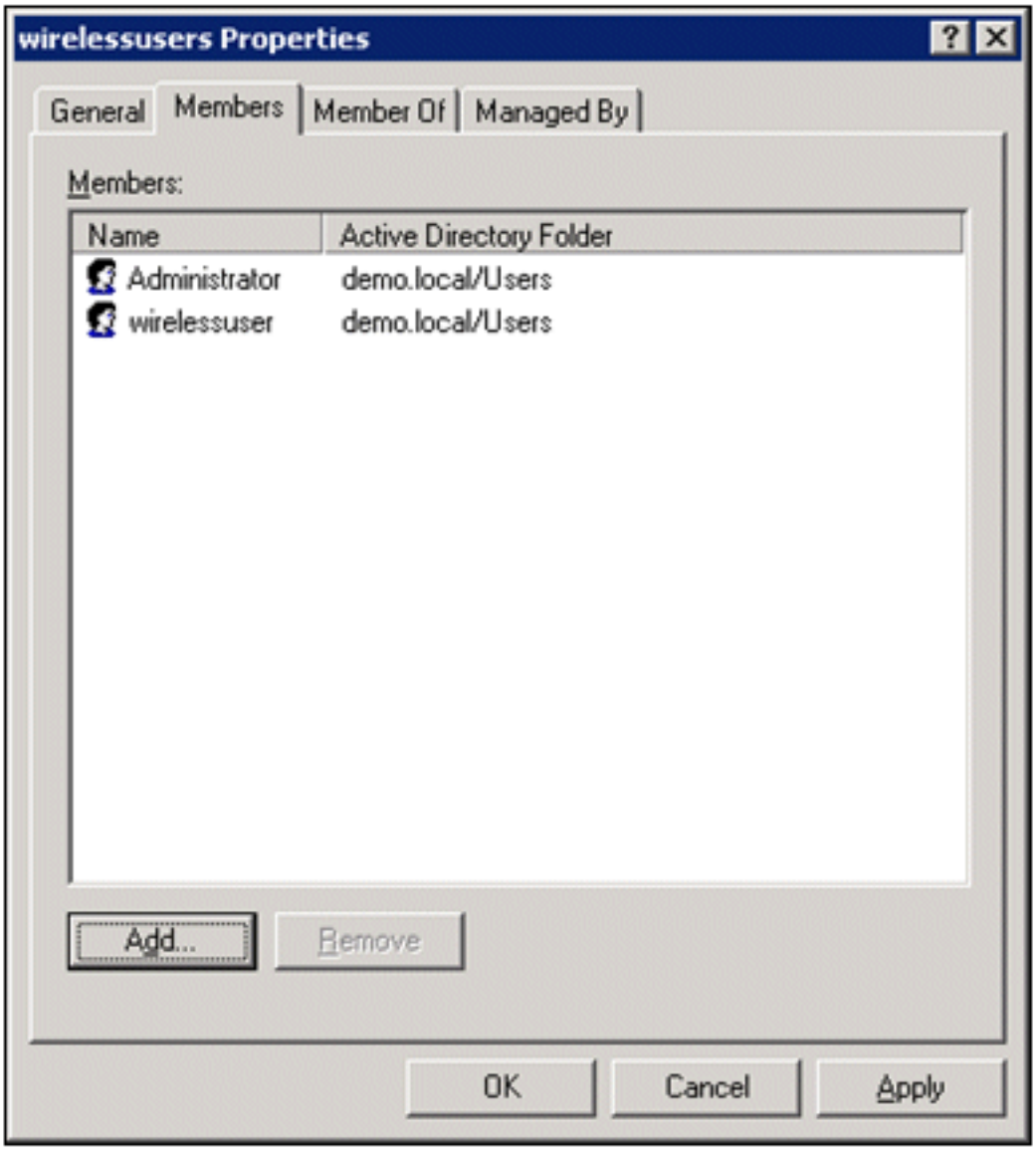
[Agregar usuarios al grupo de usuarios inalámbricos]

Siga estos pasos:

1. En el panel de detalles de Usuarios y equipos de Active Directory, haga doble clic en el grupo *UsuariosInalámbricos*.
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. En este ejemplo se muestra cómo agregar el usuario *wirelesuser* al grupo. Click OK.



4. En el cuadro de diálogo Se encontraron varios nombres, haga clic en **Aceptar**. La cuenta de usuario de usuarioinalámbrico se agrega al grupo de usuarioinalámbricos.

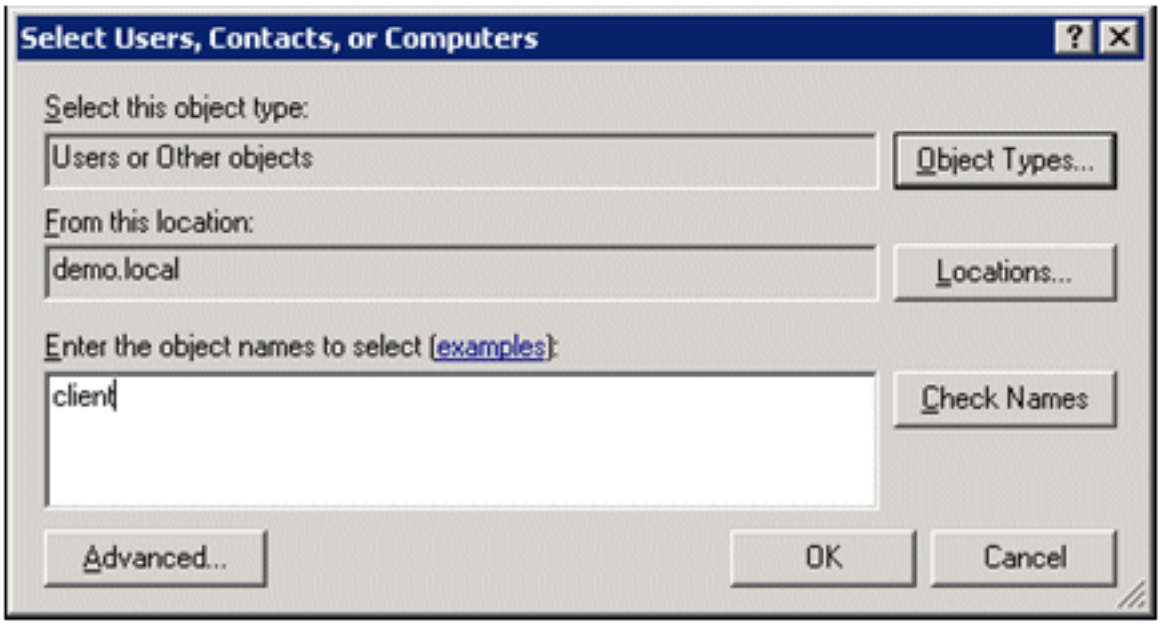


5. Haga clic en **Aceptar** para guardar los cambios en el grupo de usuarios inalámbricos.
6. Repita este procedimiento para agregar más usuarios al grupo.

Agregar equipos cliente al grupo de usuarios inalámbricos

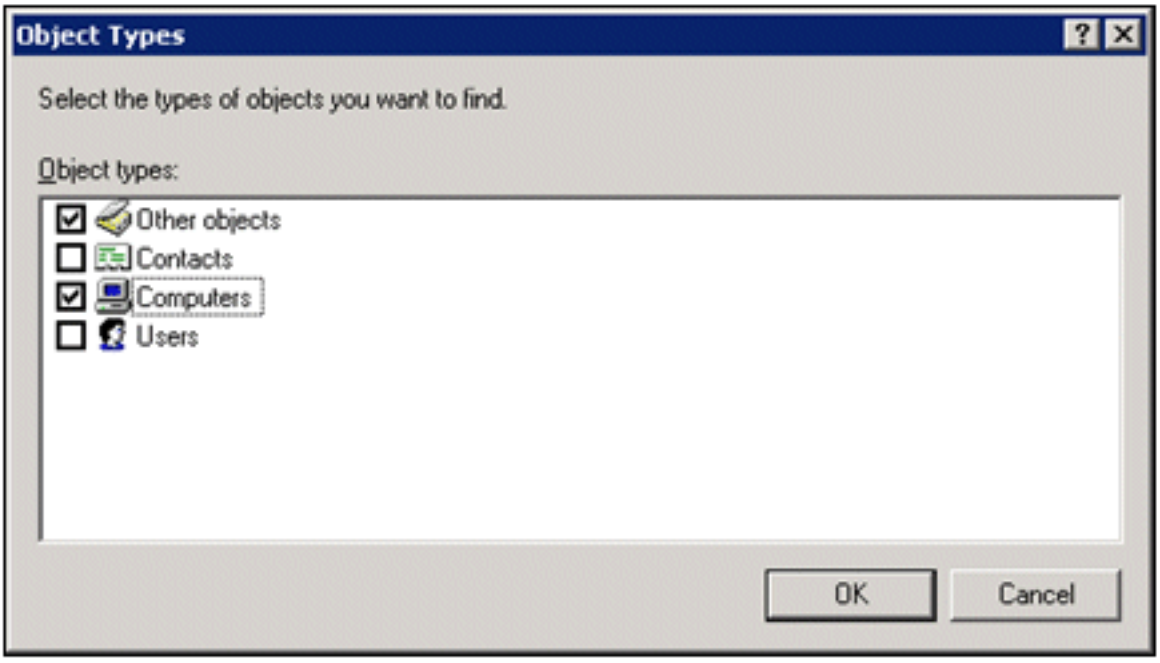
Siga estos pasos:

1. Repita los pasos 1 y 2 de 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. En este ejemplo se muestra cómo agregar el equipo denominado *client* al



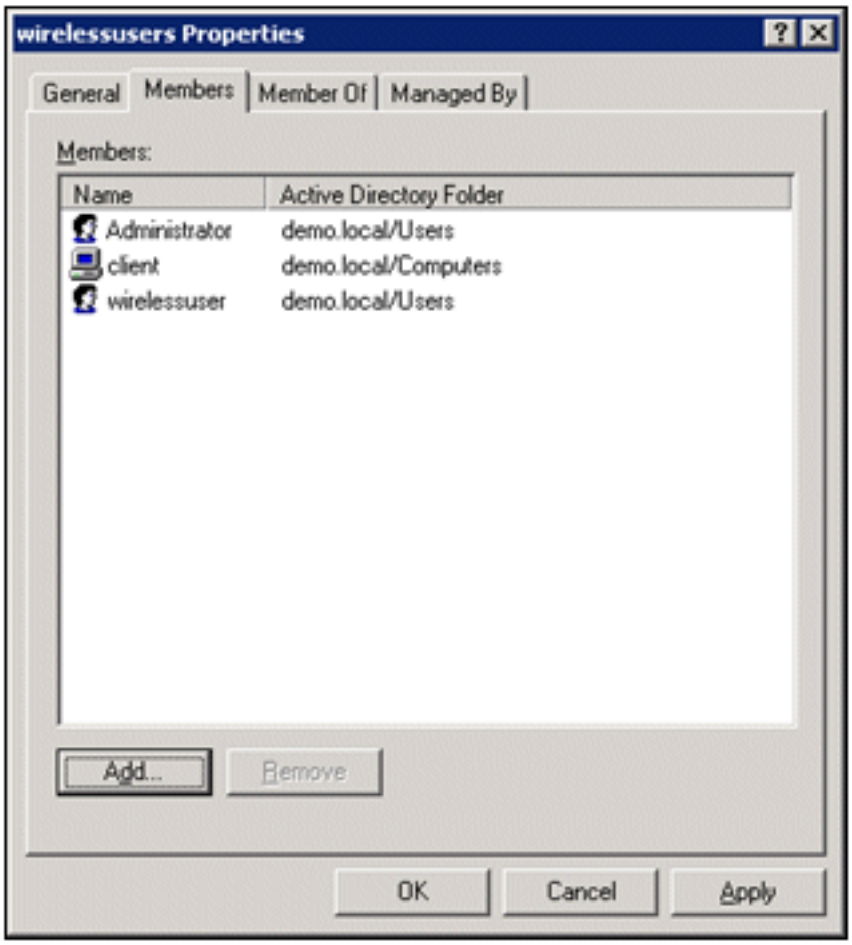
grupo.

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



Equipos.

4. Haga clic en OK dos veces. La cuenta de equipo CLIENTE se agrega al grupo de usuarios



inalámbricos.

5. Repita el procedimiento para agregar más equipos al grupo.

Cisco 1121 Secure ACS 5.1

Instalación mediante el dispositivo de la serie CSACS-1121

El dispositivo CSACS-1121 está preinstalado con el software ACS 5.1. Esta sección le brinda una descripción general del proceso de instalación y las tareas que debe realizar antes de instalar ACS.

1. Conecte el CSACS-1121 a la red y a la consola de dispositivos. Consulte el Capítulo 4, "Conexión de cables".
2. Encienda el dispositivo CSACS-1121. Consulte el Capítulo 4, "Encendido del dispositivo de la serie CSACS-1121".
3. Ejecute el comando **setup** en el indicador de comandos de la CLI para configurar las configuraciones iniciales para el servidor ACS. Consulte Ejecución del programa de instalación.

Instalación del servidor ACS

Esta sección describe el proceso de instalación del servidor ACS en el dispositivo de la serie CSACS-1121.

- Ejecutar el programa de instalación
- Verificar el proceso de instalación

- Tareas posteriores a la instalación

Para obtener información detallada sobre la instalación de Cisco Secure ACS Server, refiérase a la Guía de Instalación y Actualización para Cisco Secure Access Control System 5.1.

Configuración del controlador Cisco WLC5508

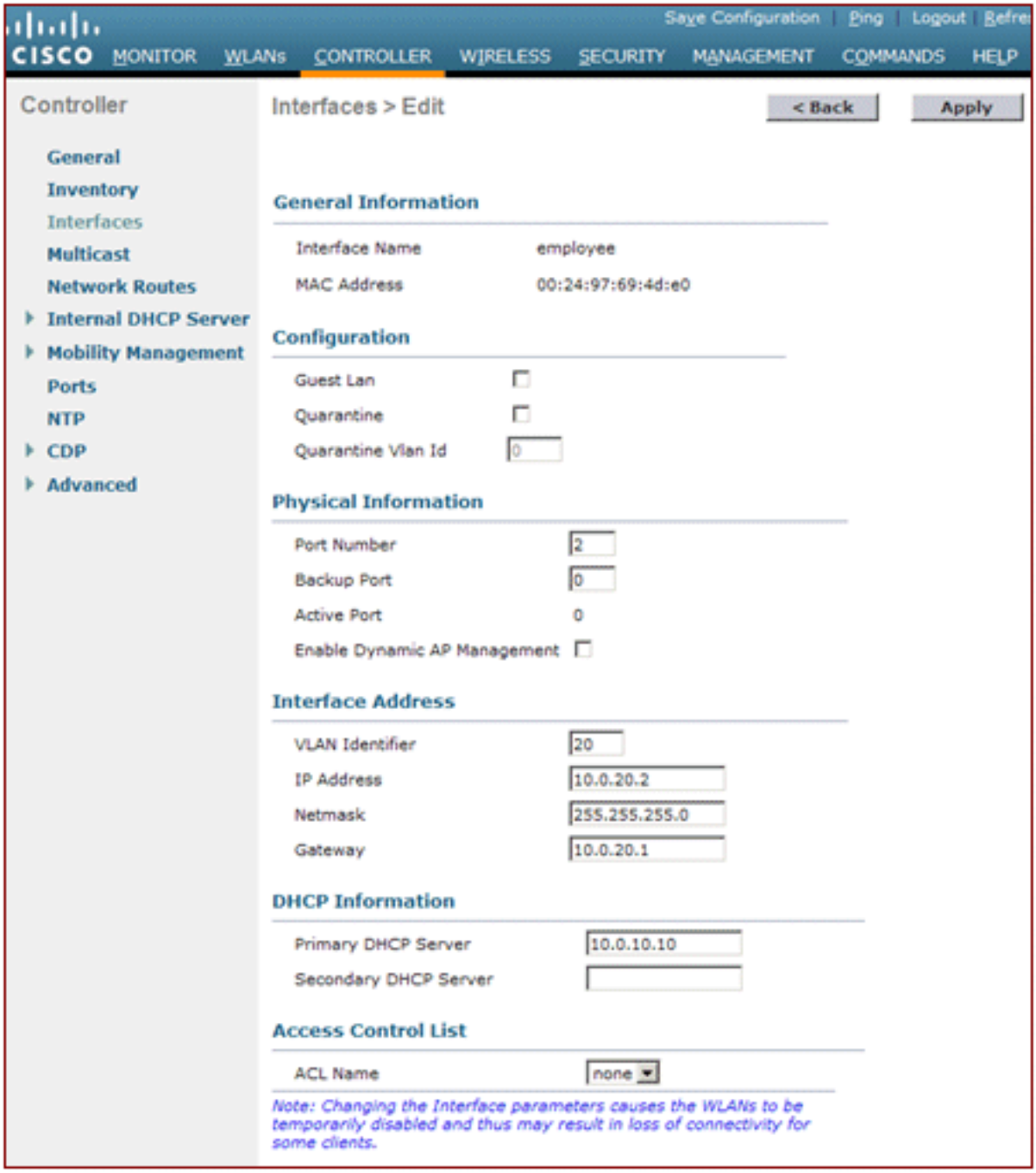
Cree la configuración necesaria para WPAv2/WPA

Siga estos pasos:

Nota: Se supone que el controlador tiene conectividad básica con la red y que el alcance IP de la interfaz de gestión es correcto.

1. Vaya a **https://10.0.1.10** 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 en el menú **Controlador**.
5. Haga clic en **Interfaces**.
6. Haga clic en **New**.
7. En el campo Interface name (Nombre de interfaz), introduzca *Employee*. (Este campo puede ser cualquier valor que desee.)
8. En el campo VLAN ID, ingrese *20*. (Este campo puede ser cualquier VLAN que se transporte en la red.)
9. Haga clic en Apply (Aplicar).
10. Configure la información como muestra esta ventana Interfaces > Edit:Dirección IP de la interfaz: **10.0.20.2**Máscara de red: **255.255.255.0**Gateway - **10.0.10.1**DHCP principal - **10.0.10.10**

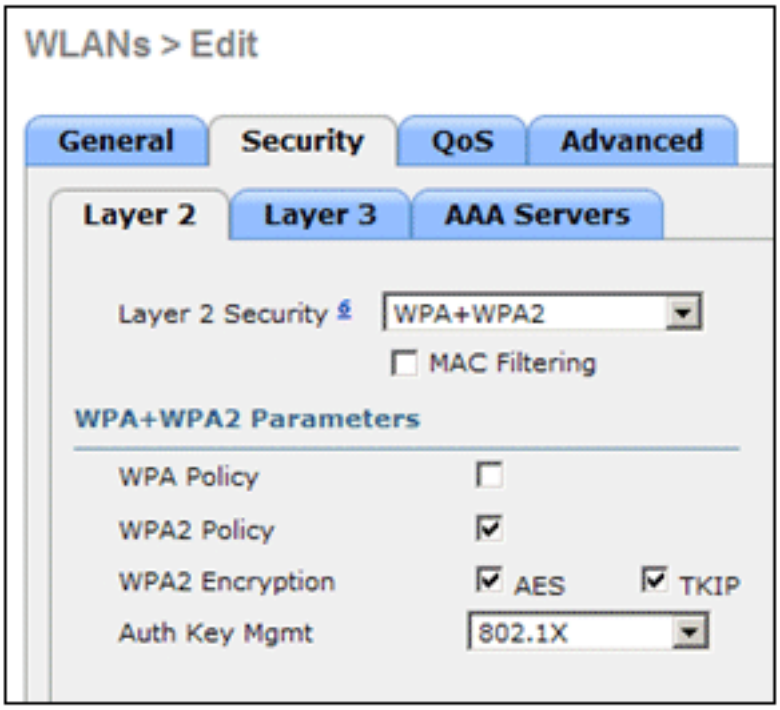


11. Haga clic en Apply (Aplicar).
12. Haga clic en la pestaña **WLANs**.
13. Elija **Create New**, y haga clic en **Go**.
14. Introduzca un nombre de perfil y, en el campo WLAN SSID, introduzca *Employee*.

15. Elija una ID para la WLAN y haga clic en **Apply**.

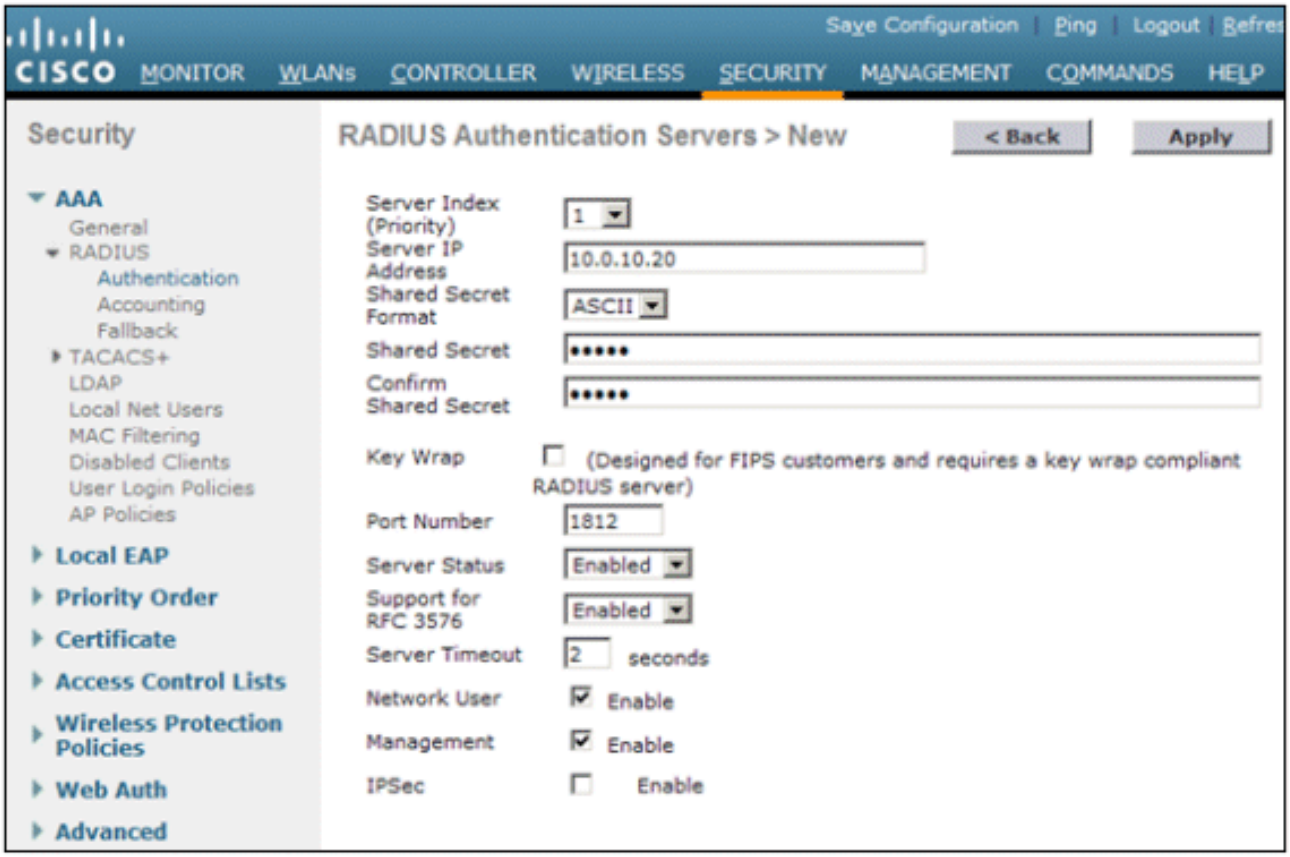
16. Configure la información para esta WLAN cuando aparezca la ventana WLANs > Edit .**Nota:** WPAv2 es el método de encriptación de capa 2 elegido para este laboratorio. Para permitir que WPA con clientes TKIP-MIC se asocie a este SSID, también puede marcar las casillas **WPA compatibility mode** y **Allow WPA2 TKIP Clients** o aquellos clientes que no admitan el método de cifrado AES 802.11i.
17. En la pantalla WLANs > Edit, haga clic en la ficha **General**.
18. Asegúrese de que la casilla Status (Estado) esté marcada para **Enabled** (Activado) y que se haya seleccionado la **Interface** (empleado) adecuada. Además, asegúrese de marcar la casilla de verificación **Enabled** para Broadcast SSID.

19. Haga clic en la ficha Security (Seguridad).
20. En el submenú Layer 2 (Capa 2), seleccione **WPA + WPA2** para Layer 2 Security (Seguridad de capa 2). Para la encriptación WPA2, verifique **AES + TKIP** para permitir los clientes TKIP.
21. Elija **802.1x** como método de



autenticación.

22. Omita el submenú de la capa 3, ya que no es necesario. Una vez configurado el servidor RADIUS, se puede seleccionar el servidor apropiado en el menú Authentication (Autenticación).
23. Las pestañas **QoS** y **Advanced** se pueden dejar en modo predeterminado a menos que se requiera alguna configuración especial.
24. Haga clic en el menú **Security** 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 (10.0.10.20) 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**.



28. La configuración básica ha finalizado 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 de equipo para los servidores ACS se puede utilizar para simplificar una implementación.

Para configurar el servidor de la CA para que proporcione la inscripción automática de los certificados de equipo y de usuario, complete los procedimientos de esta sección.

Nota: Microsoft ha cambiado la plantilla de servidor web con la versión de la CA de Windows 2003 Enterprise para que las claves ya no se puedan exportar y la opción esté atenuada. No hay otras plantillas de certificado suministradas con servicios de certificado que sean para la autenticación del servidor y permitan marcar claves como exportables que estén disponibles en el menú desplegable, por lo que debe crear una nueva plantilla que lo haga.

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

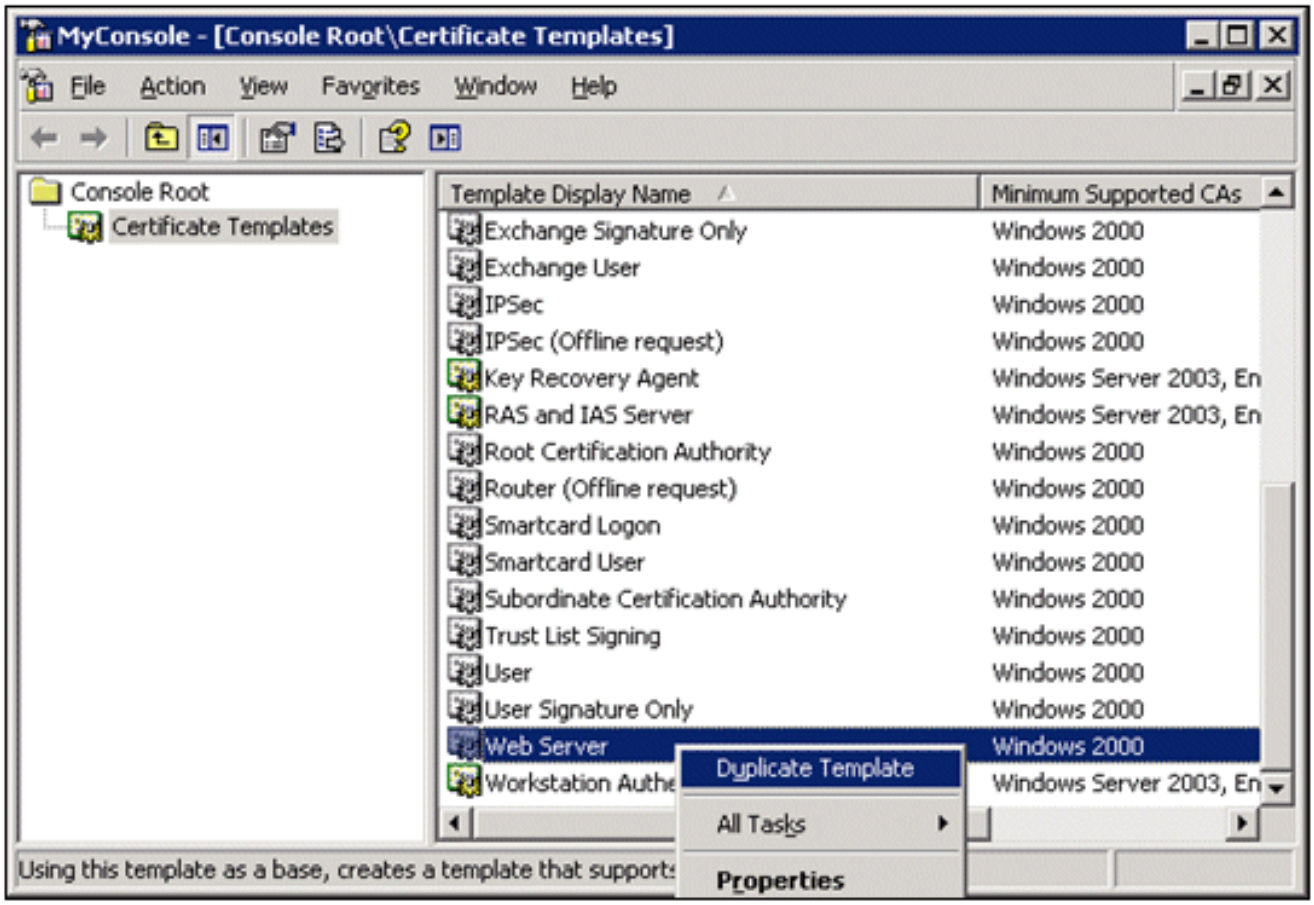
Instalar el complemento Plantillas de certificado

Siga estos pasos:

1. Elija **Start** > **Run**, ingrese *mmc*, y haga clic en **OK**.
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**.

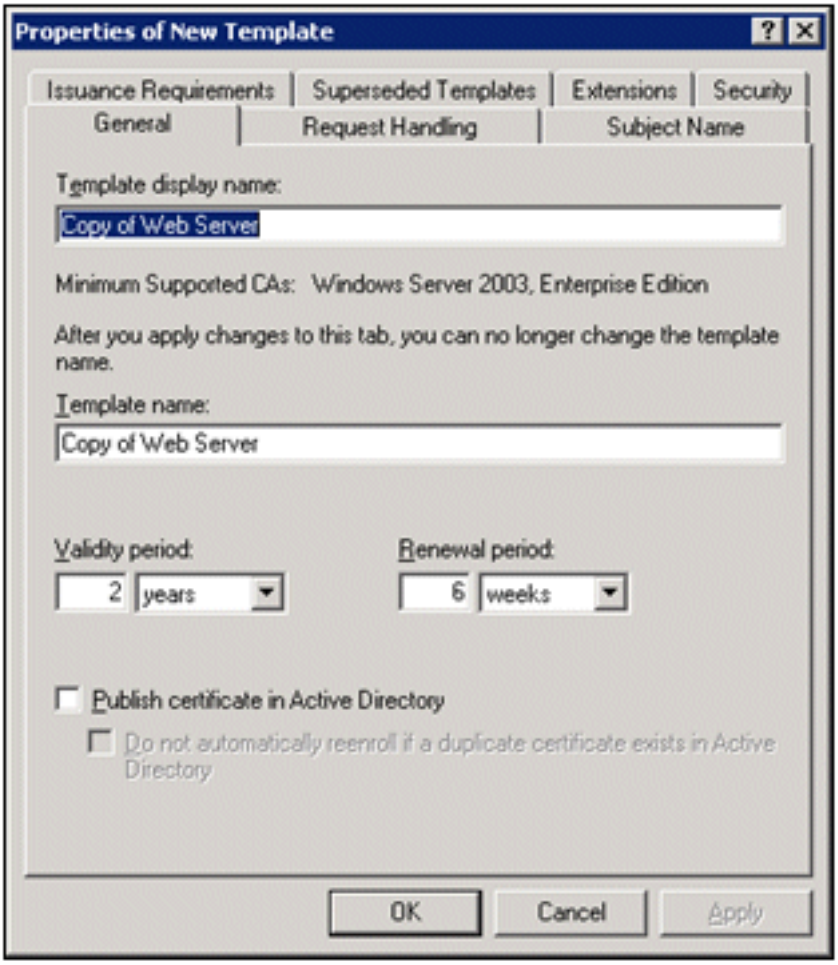
4. En el árbol de la consola, haga clic en **Plantillas de certificado**. Todas las plantillas de certificado aparecen en el panel Detalles.
5. Para omitir los pasos del 2 al 4, escriba *certtmpl.msc*, que abre el complemento Plantillas de certificado.



Crear la plantilla de certificado para el servidor web ACS

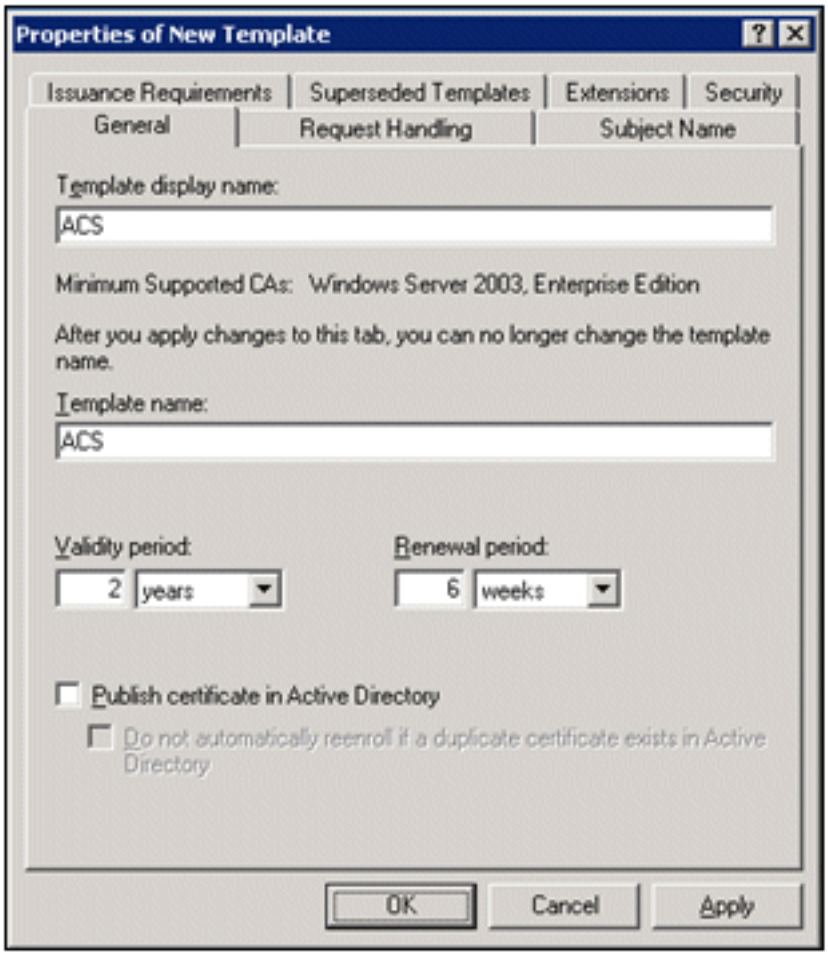
Siga estos pasos:

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.

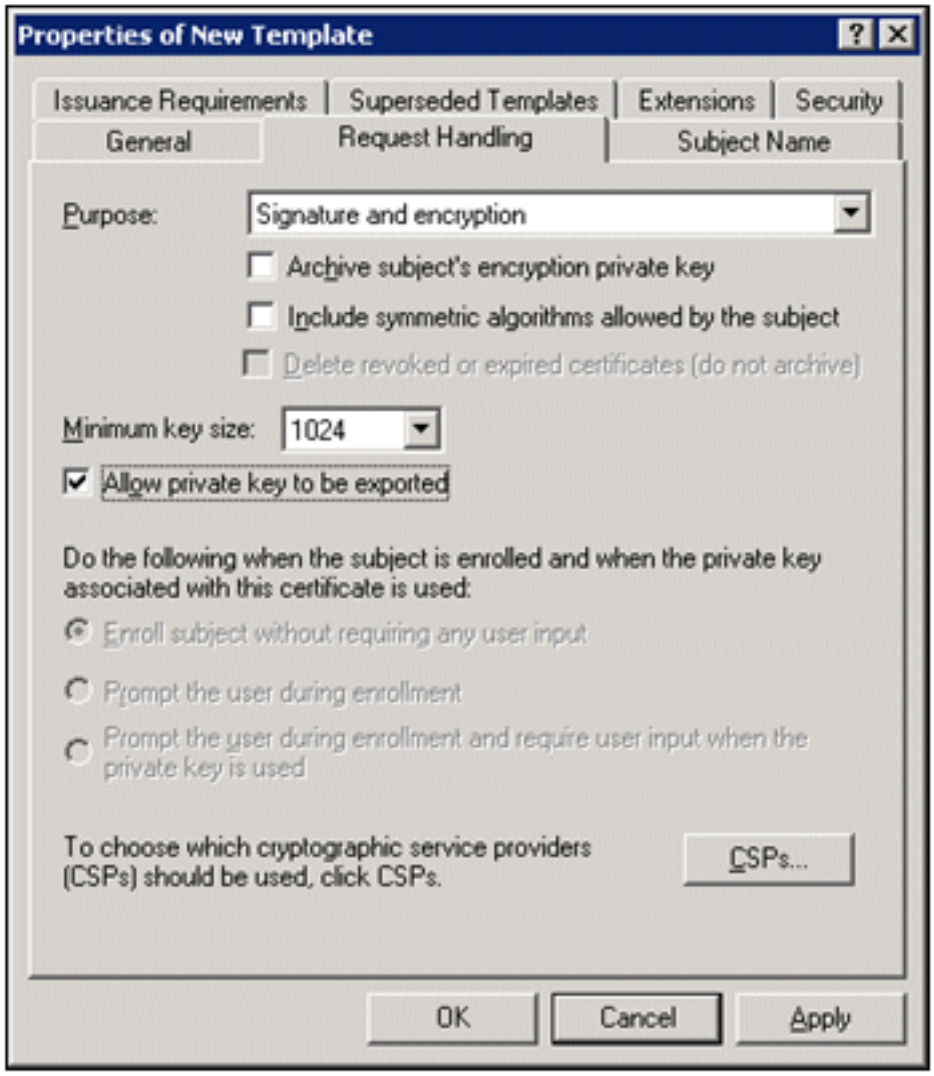
3. En el campo Template display name, ingrese



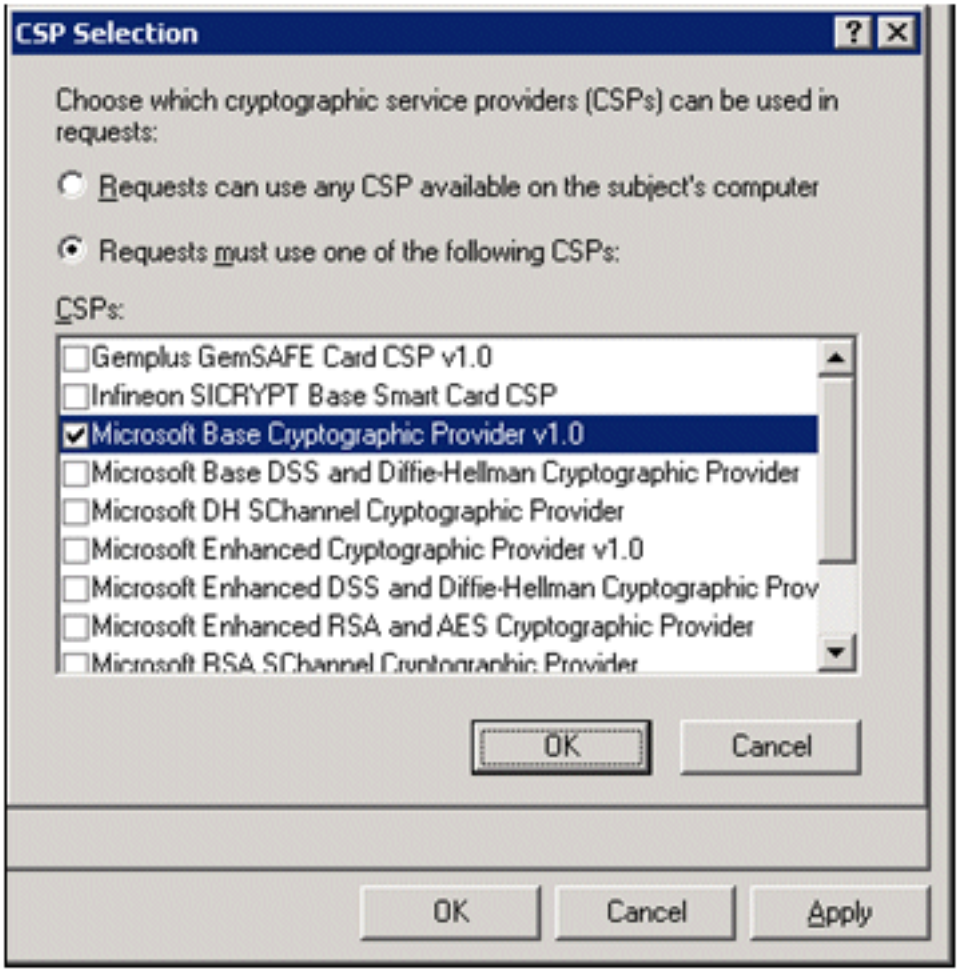
ACS.

4. Vaya a la ficha **Gestión de solicitudes** y marque **Permitir la exportación de claves privadas**.

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

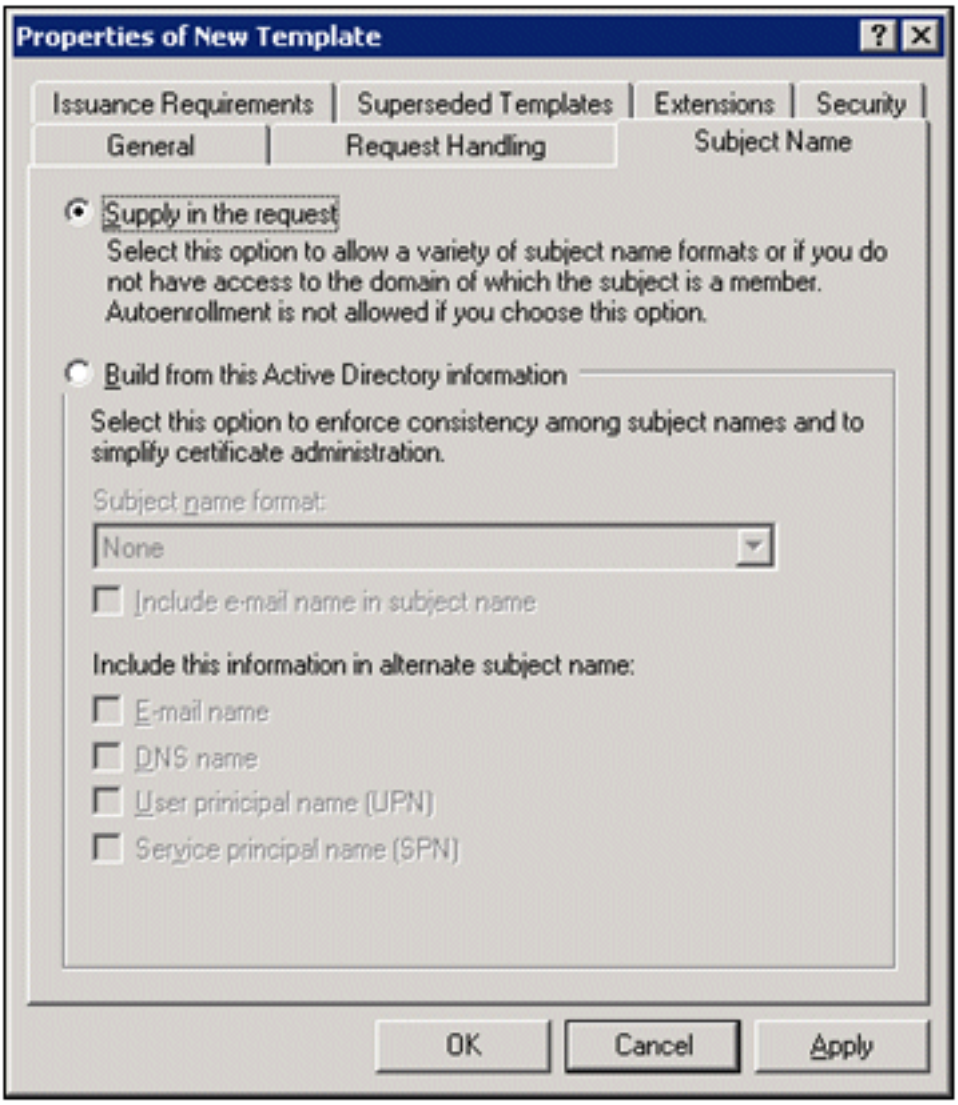


5. Elija **Solicitudes debe utilizar uno de los siguientes CSP** y marque **Proveedor criptográfico de base Microsoft v1.0**. Desmarque cualquier otro CSP que esté marcado y haga clic en



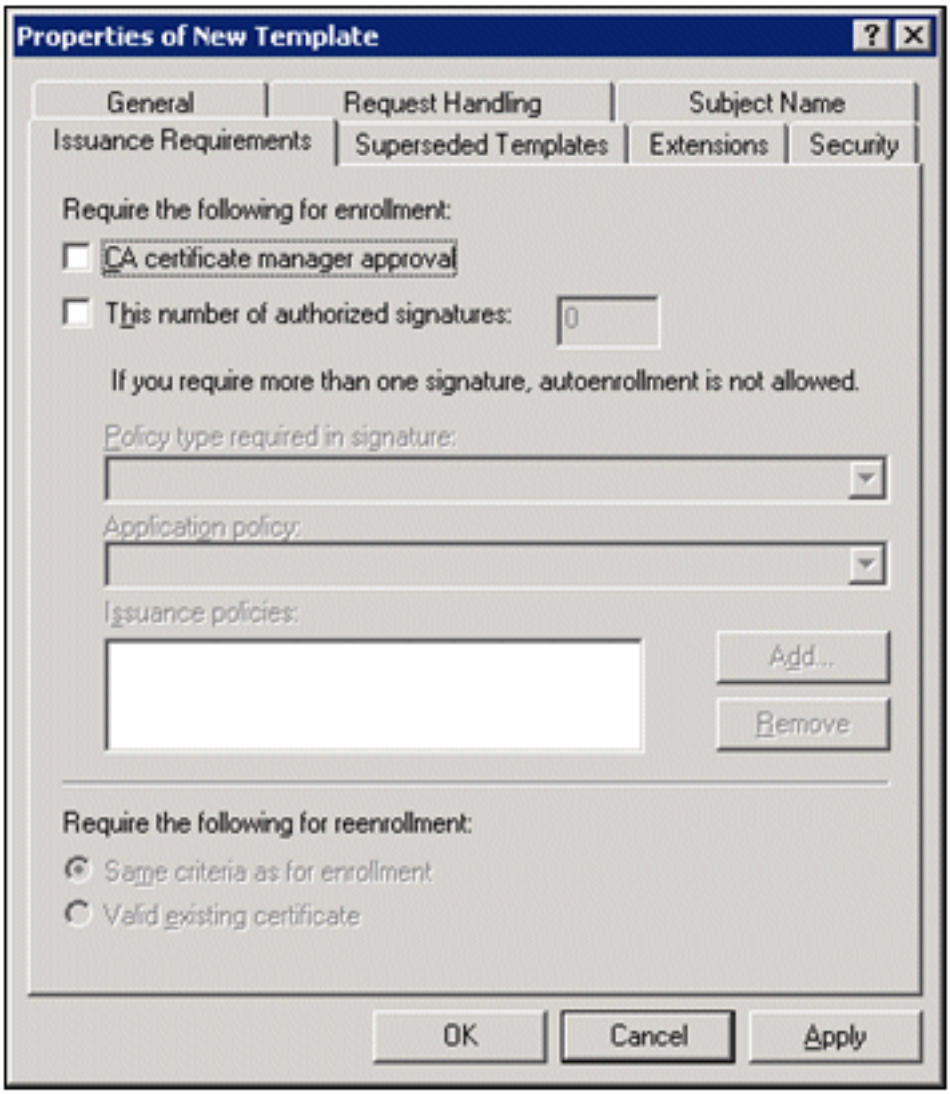
Aceptar.

6. Vaya a la pestaña **Subject Name**, elija **Supply** en la solicitud y haga clic en



OK.

7. Vaya a la pestaña **Security**, resalte el **Domain Admins Group** y asegúrese de que la opción **Enroll** esté marcada en Allowed.**Nota:** Si elige generar a partir de esta información de Active Directory, compruebe solamente el **Nombre principal de usuario (UPN)** y desmarque la opción **Incluir nombre de correo electrónico** en el nombre de asunto y el nombre de correo electrónico porque no se especificó un nombre de correo electrónico para la cuenta de usuario inalámbrico en el complemento Usuarios y equipos de Active Directory. Si no deshabilita estas dos opciones, la inscripción automática intentará utilizar el correo electrónico, lo que provocará un error de inscripción automática.
8. Existen medidas de seguridad adicionales si es necesario para evitar que los certificados se expulsen automáticamente. Puede encontrarlos en la pestaña Requisitos de emisión. Esto no se trata más adelante en este



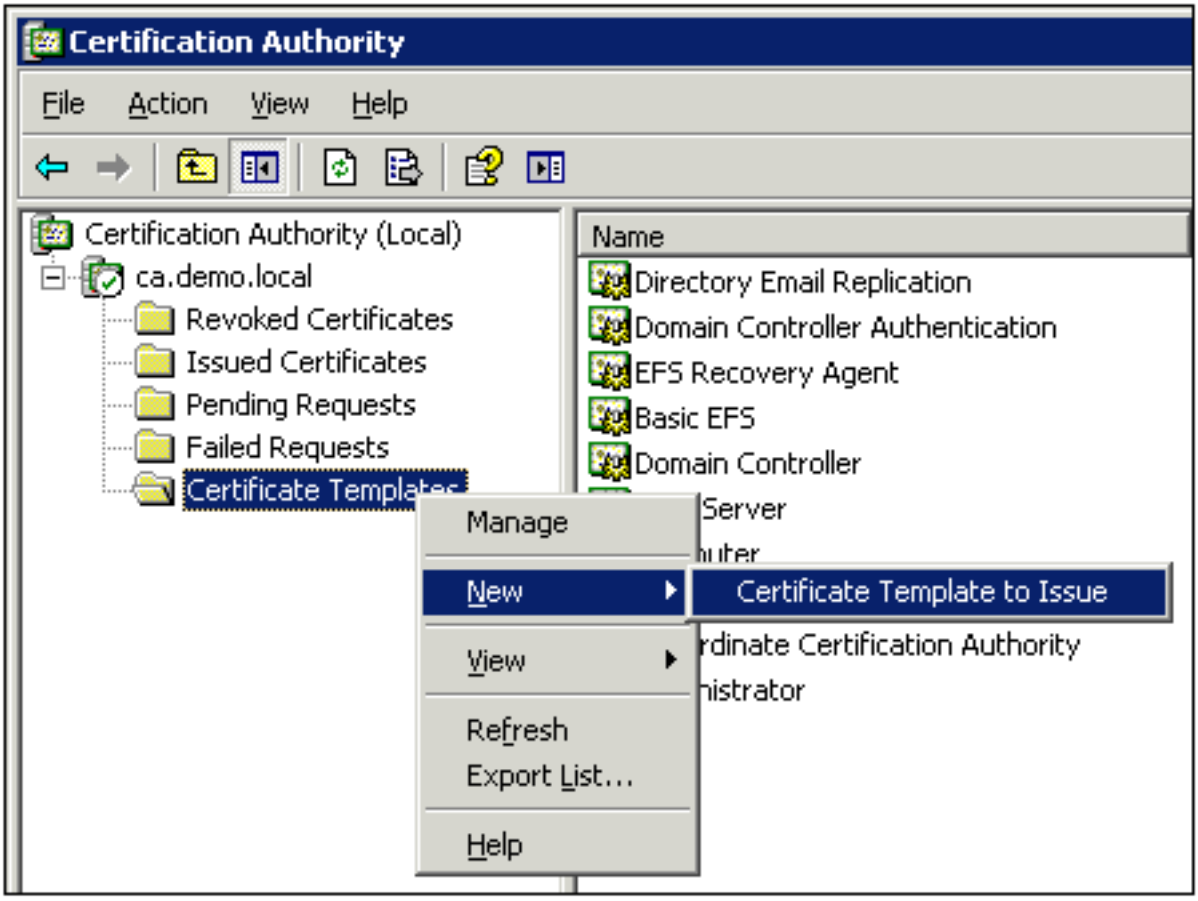
documento.

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

Habilitar la nueva plantilla de certificado de servidor web ACS

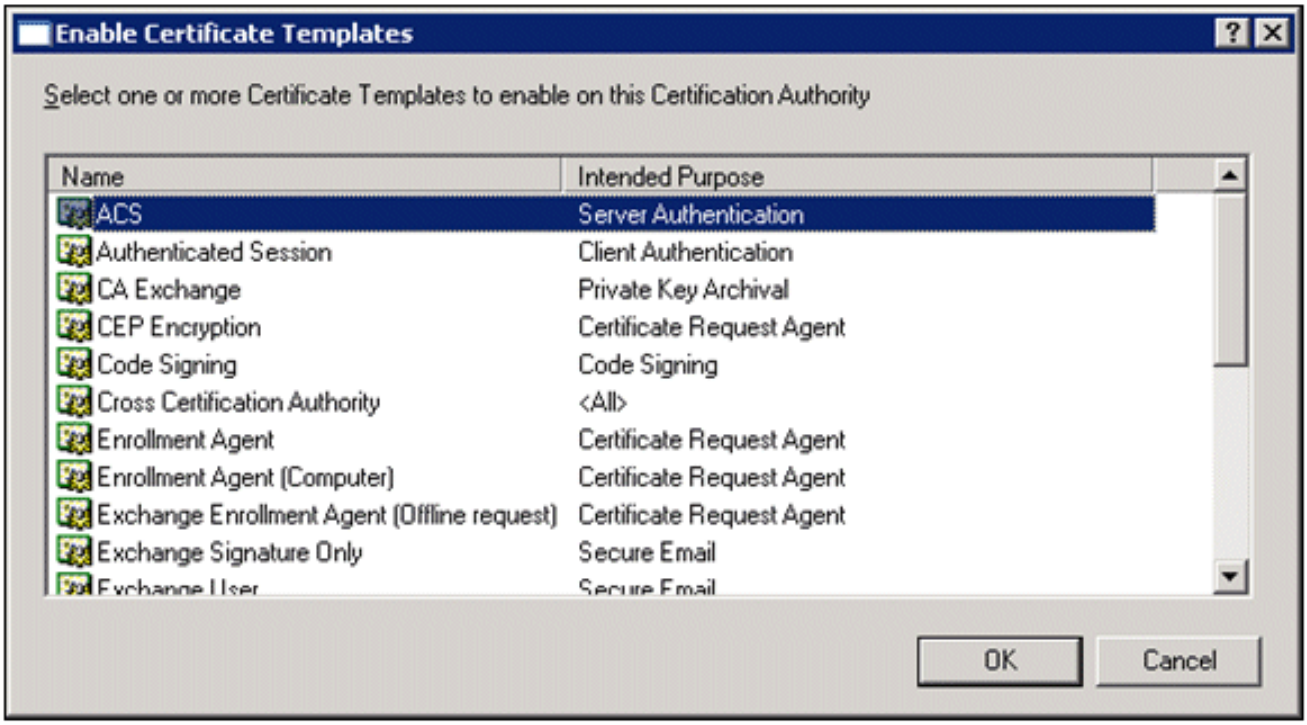
Siga estos pasos:

1. Abra el complemento Entidad de certificación. Realice los pasos del 1 al 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 Autoridad de certificación, expanda **ca.demo.local** y, a continuación, haga clic con el botón secundario en **Plantillas de certificado**.
3. Vaya a **Nuevo > Plantilla de certificado para**

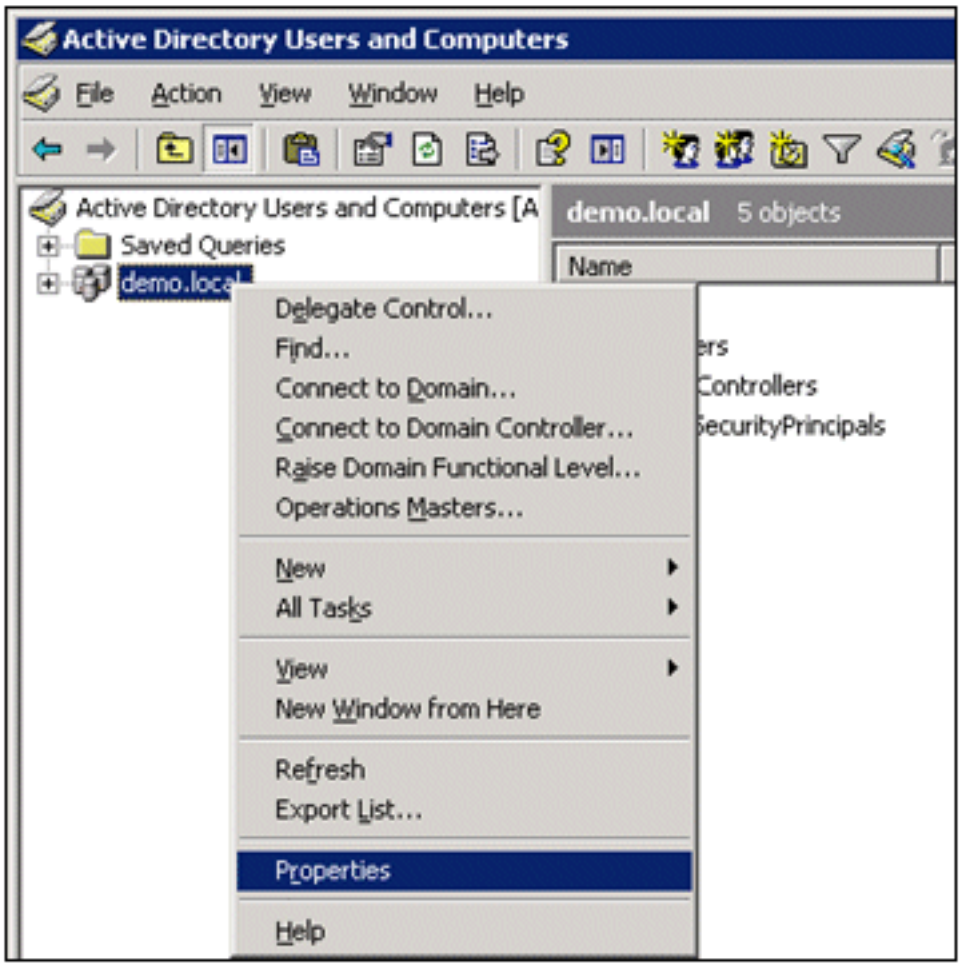


emitir.

4. Haga clic en la **Plantilla de certificado ACS**.

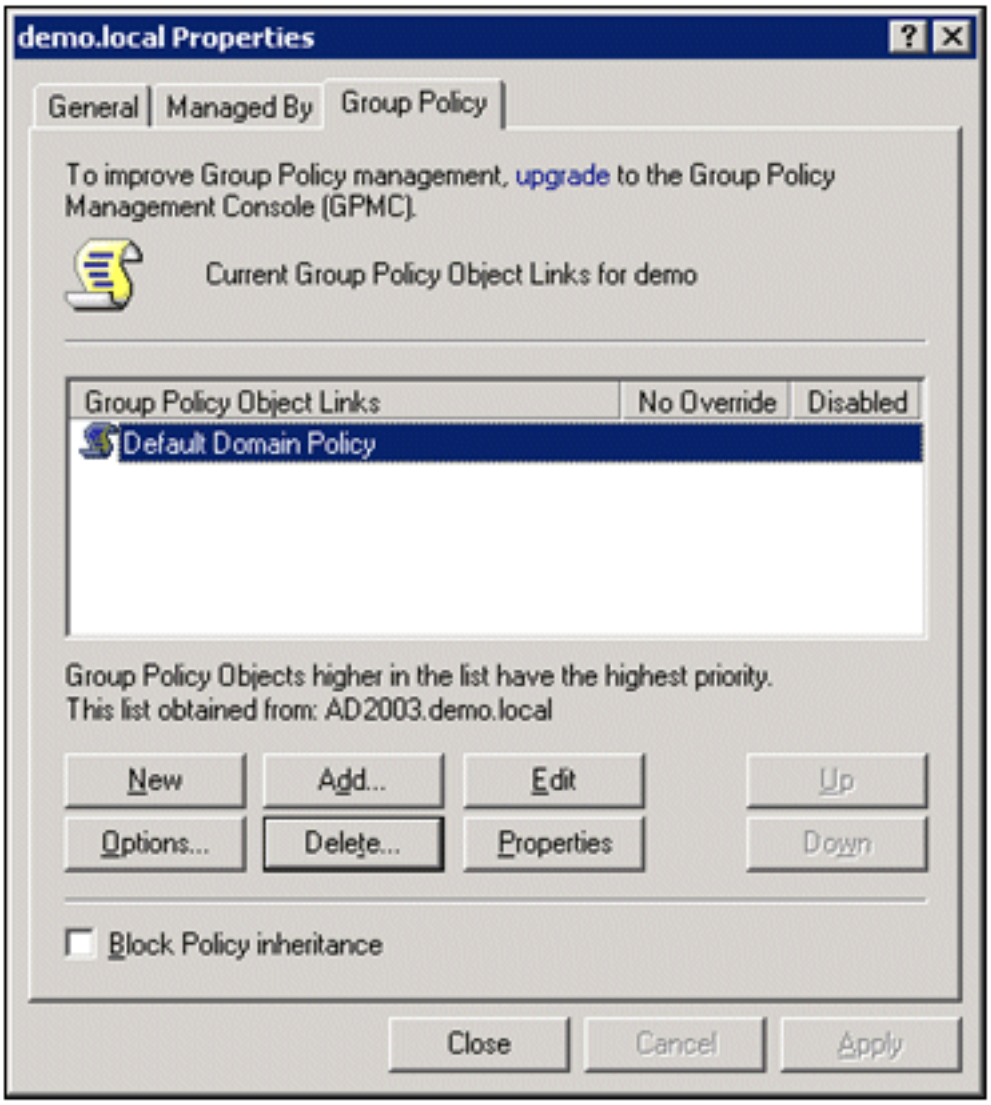


5. Haga clic en **Aceptar** y abra el **complemento Usuarios y equipos de Active Directory**.
6. En el árbol de la consola, haga doble clic en **Usuarios y equipos de Active Directory**, haga clic con el botón secundario en **demo.local** y, a continuación, haga clic en



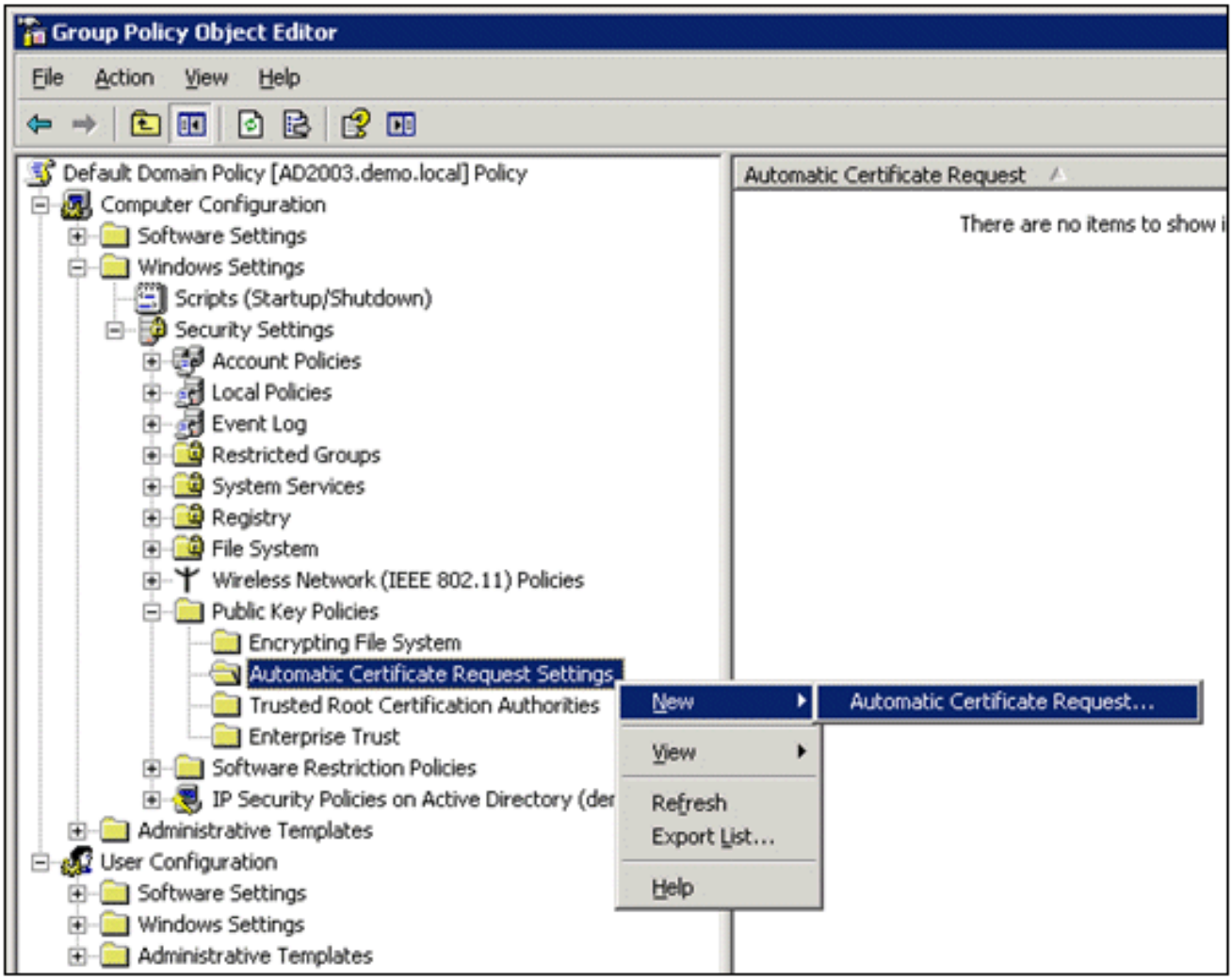
Propiedades.

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



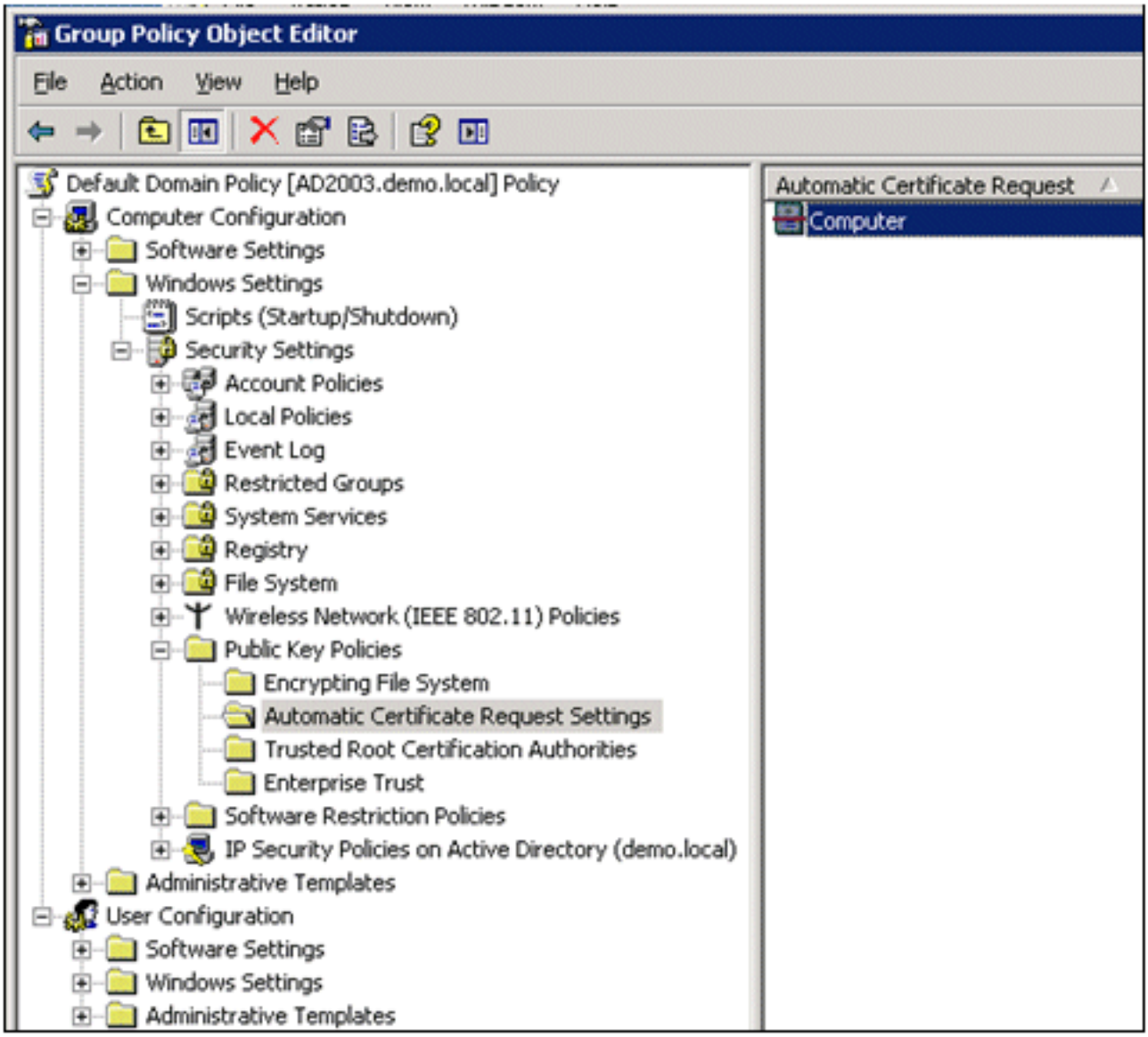
grupo.

8. En el árbol de la consola, expanda Configuración del equipo > **Configuración de Windows > Configuración de seguridad > Directivas de clave pública** y, a continuación, seleccione **Configuración automática de solicitud de certificado**.

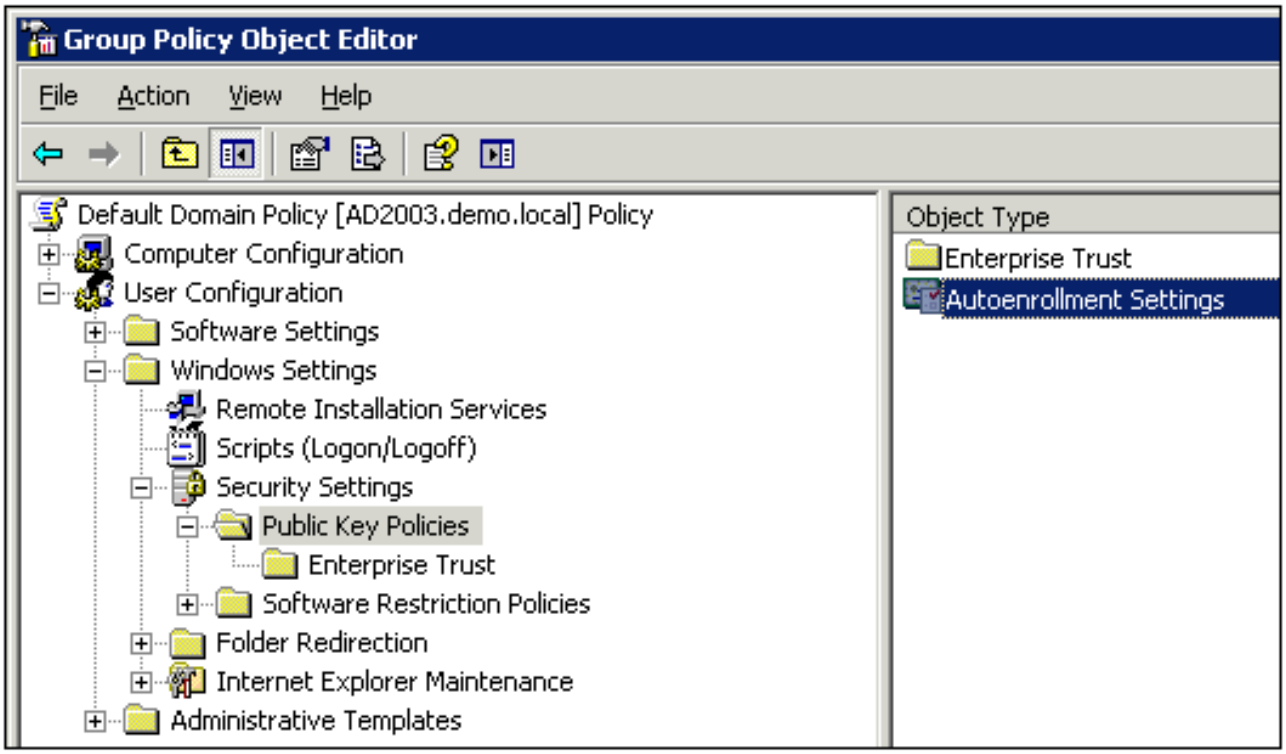


9. Haga clic con el botón derecho del mouse en **Configuración de Solicitud de Certificado Automático**, y elija **Nuevo > Solicitud de Certificado Automático**.
10. En la página Asistente para la instalación de la solicitud automática de certificados, haga clic en **Siguiente**.
11. En la página Plantilla de certificado, haga clic en **Equipo** y, a continuación, haga clic en **Siguiente**.

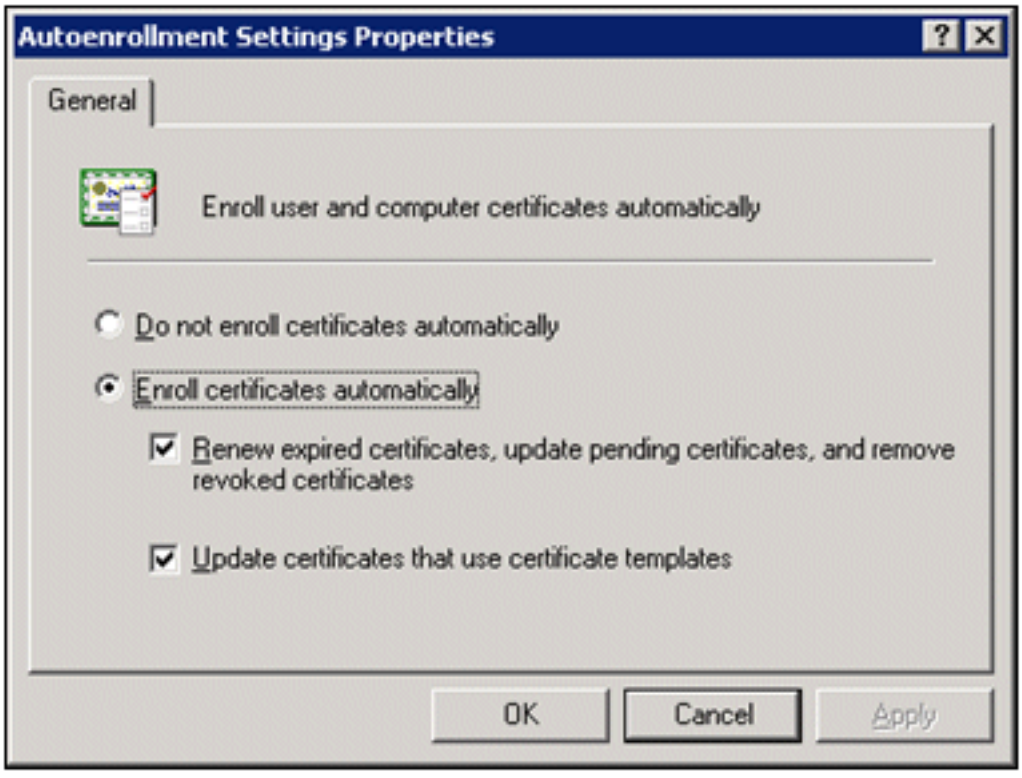
12. Cuando complete la página Asistente para la instalación de la solicitud automática de certificados, haga clic en **Finalizar**. El tipo de certificado Equipo aparece ahora en el panel de detalles del complemento Editor de objetos de directiva de grupo.



13. En el árbol de la consola, expanda **Configuración de usuario > Configuración de Windows > Configuración de seguridad > Directivas 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 quitar certificados revocados** y **Actualizar certificados que utilizan plantillas de certificados**.



16. Click OK.

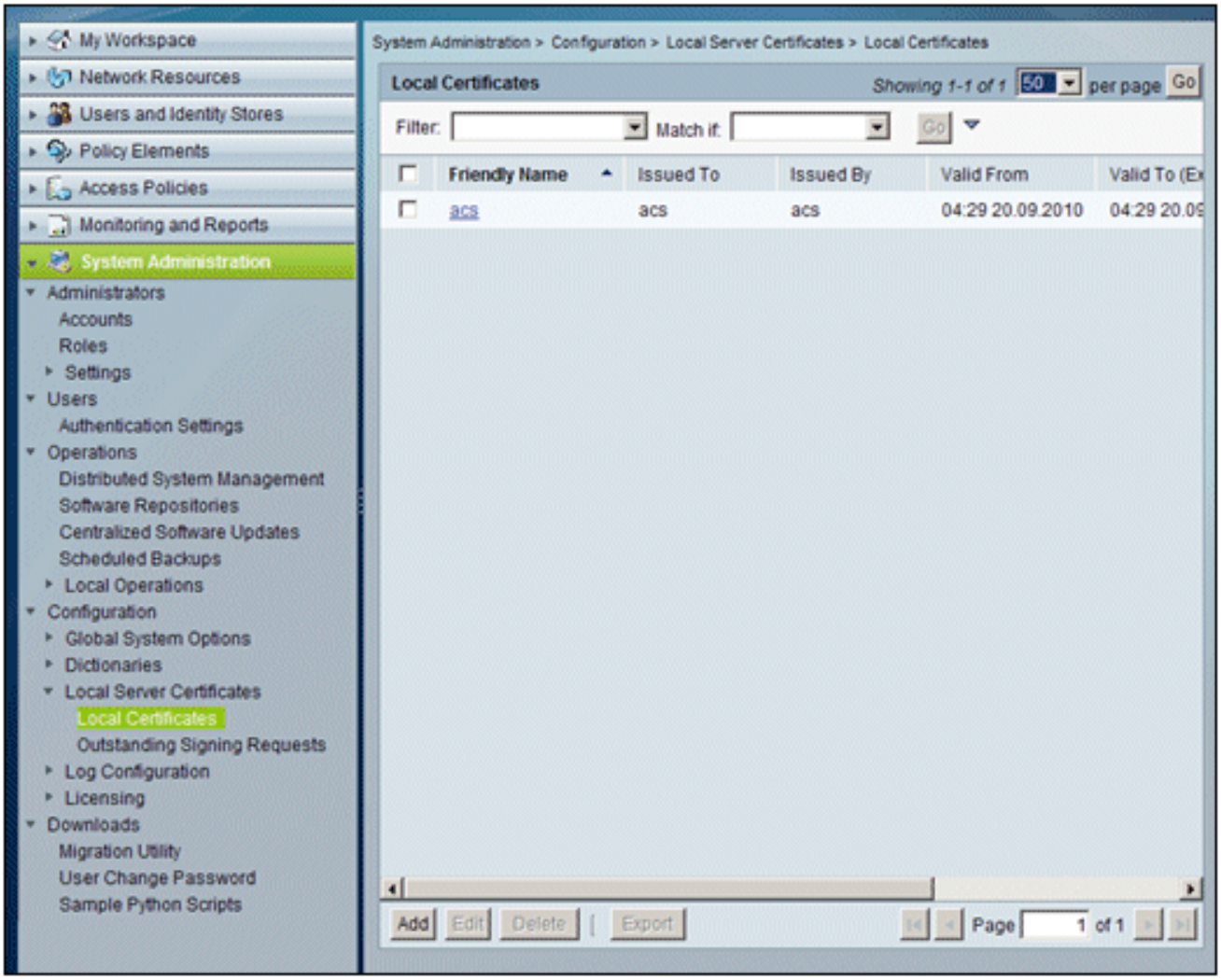
Configuración del certificado ACS 5.1

Configurar certificado exportable para ACS

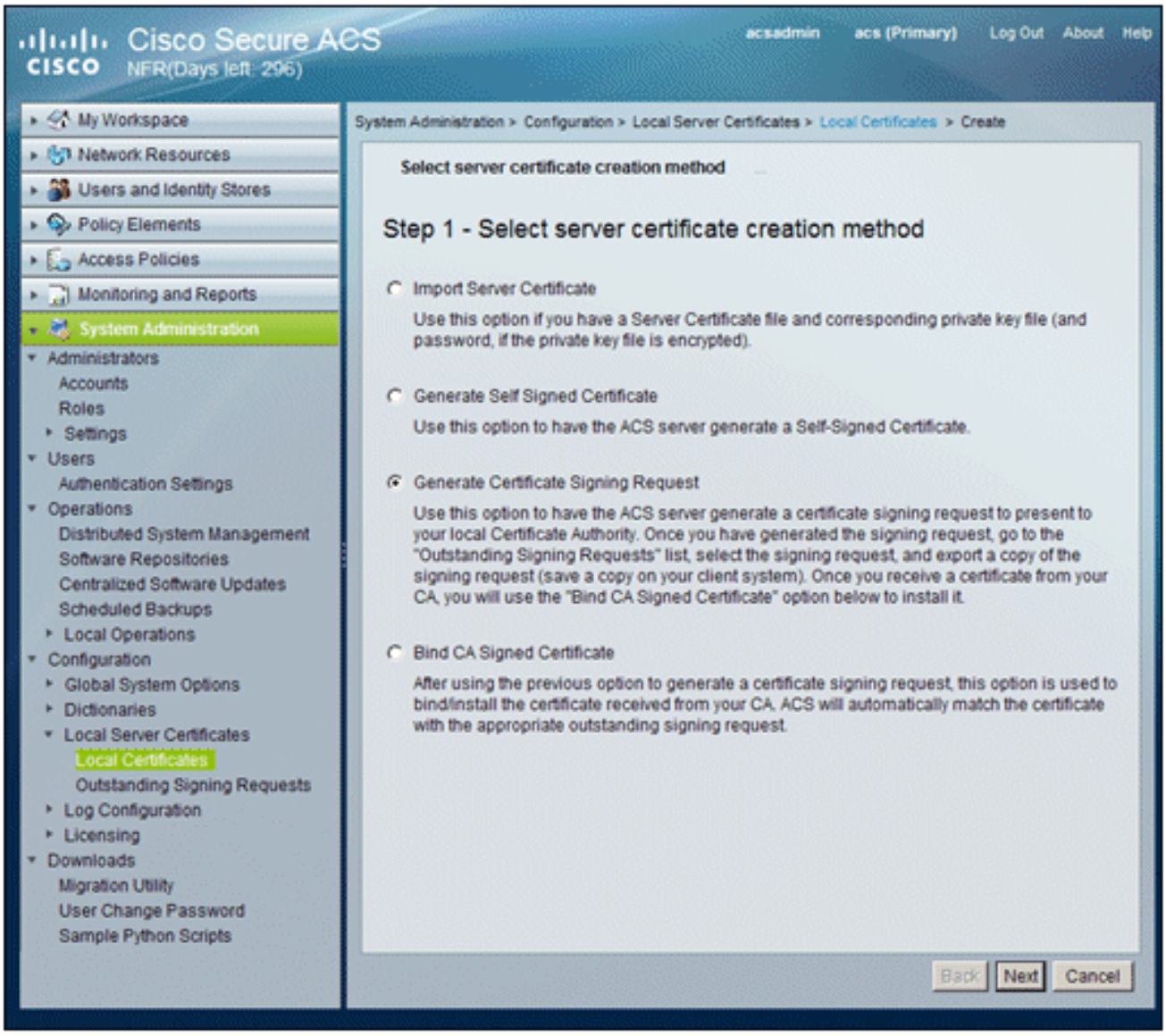
Nota: El servidor ACS debe obtener un certificado de servidor del servidor CA raíz de la empresa para autenticar un cliente WLAN PEAP.

Nota: Asegúrese de que el Administrador de IIS no esté abierto durante el proceso de instalación del certificado porque causa problemas con la información almacenada en caché.

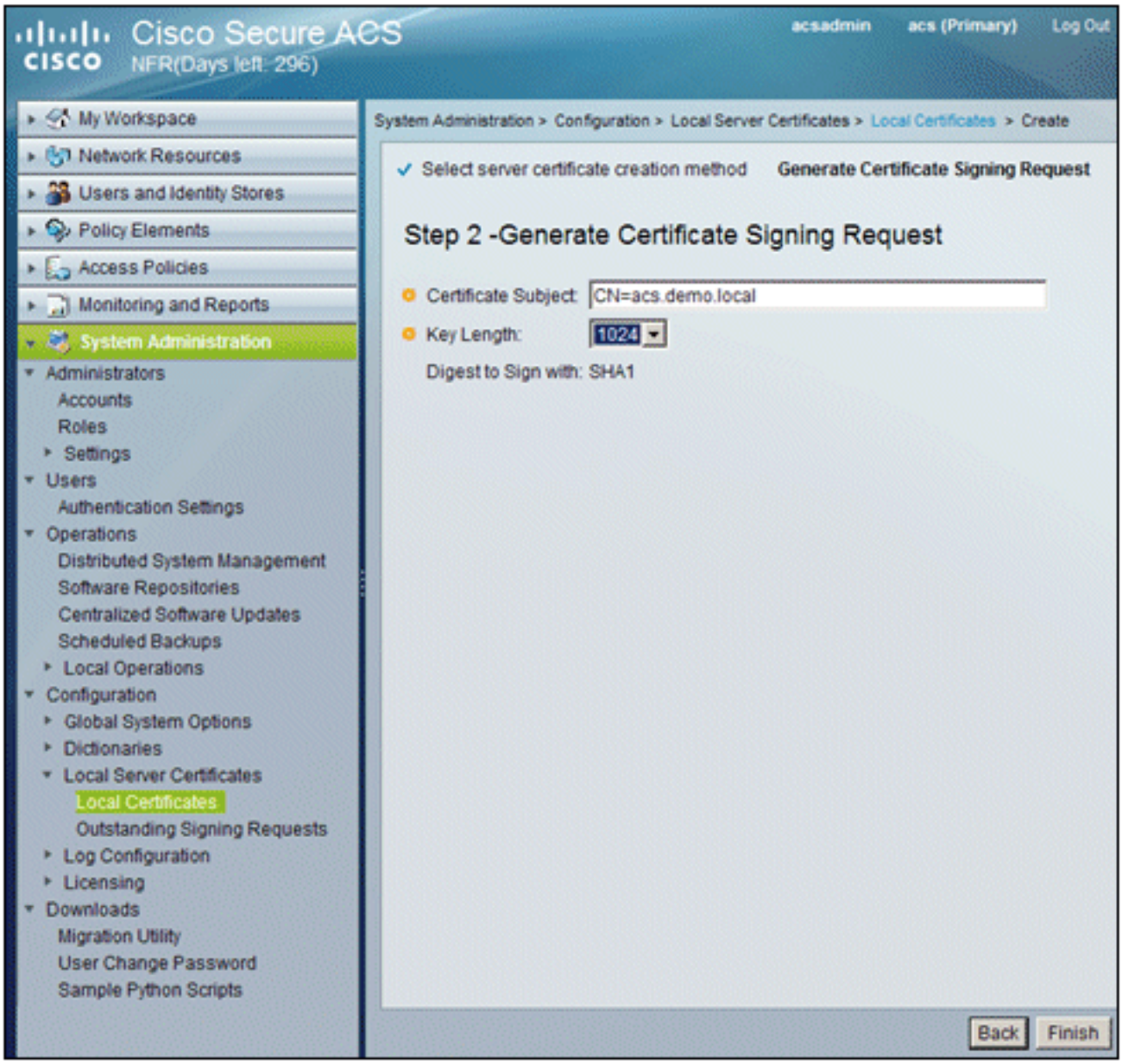
1. Inicie sesión en el servidor ACS con una cuenta de derechos de administrador.
2. Vaya a **Administración del sistema > Configuración > Certificados de servidor local**. Haga clic en Add
   (Agregar).



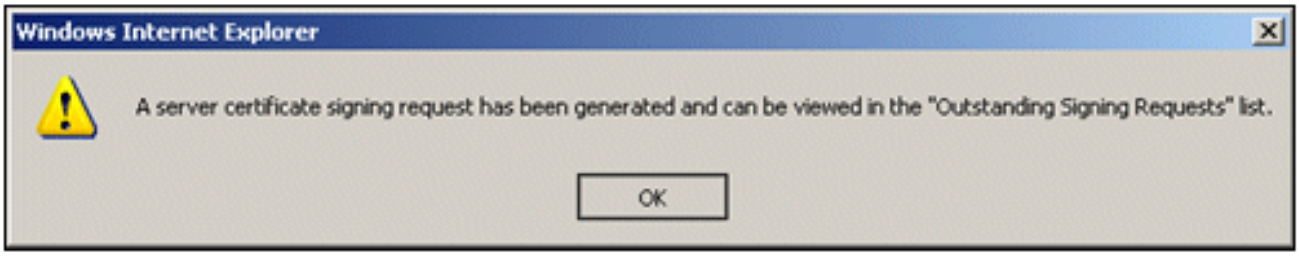
3. Cuando elija un método de creación de certificados de servidor, elija **Generar solicitud de firma de certificado**. Haga clic en Next
   (Siguiente).



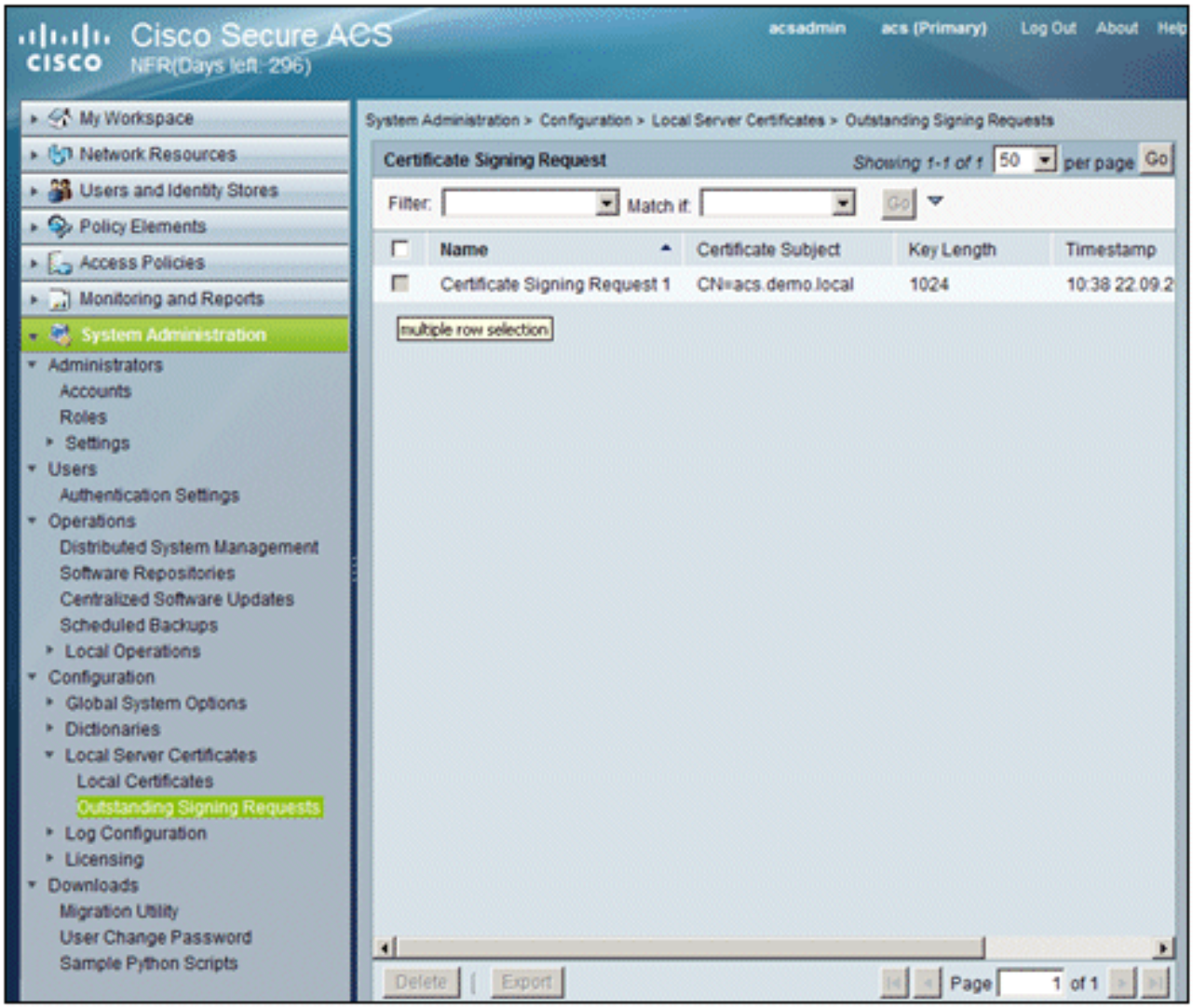
4. Ingrese un asunto de certificado y la longitud de clave como ejemplo, luego haga clic en **Finish**:Asunto del certificado: **CN=acs.demo.local**Longitud de clave: **1024**



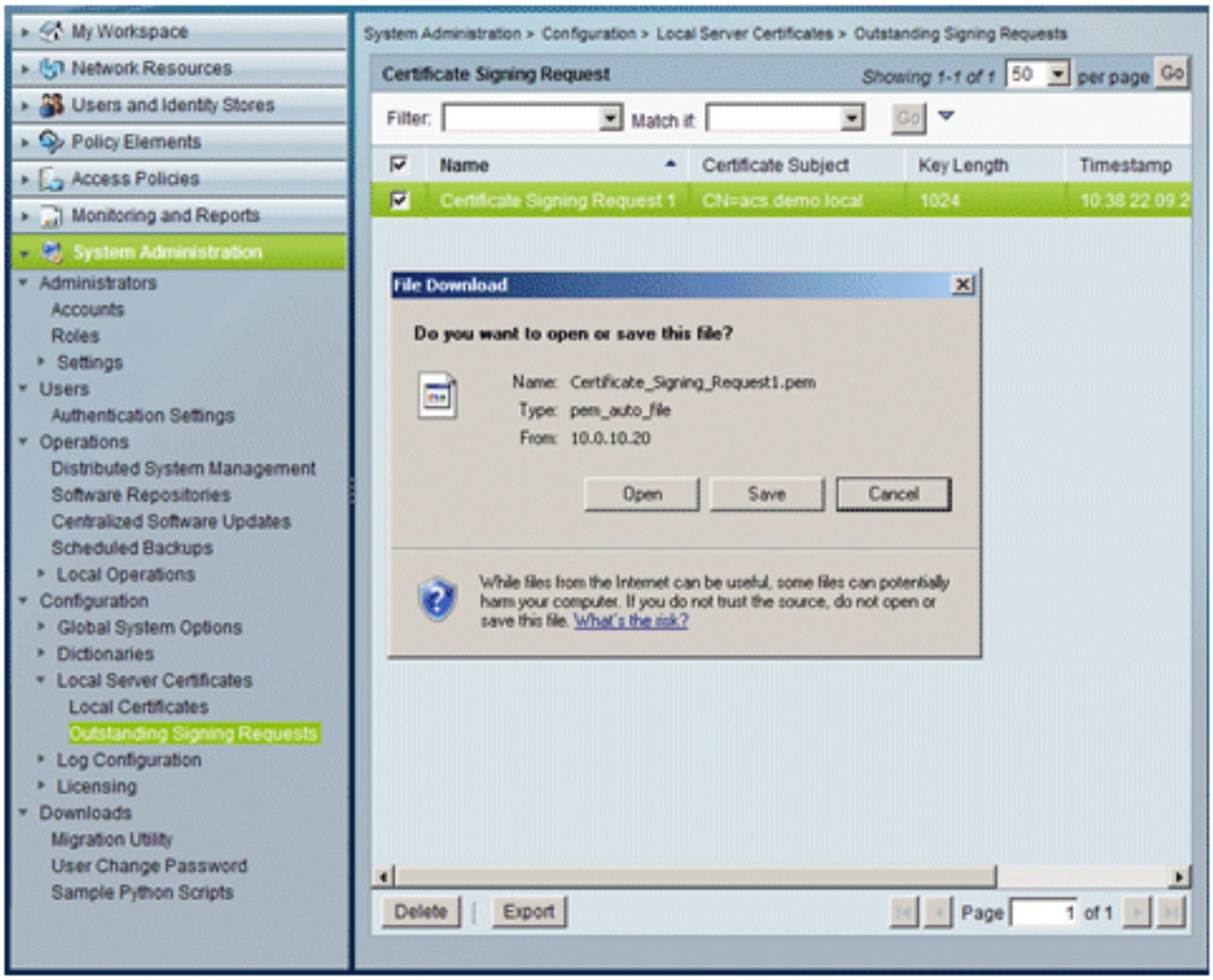
5. ACS solicitará que se genere una solicitud de firma de certificado. Click OK.



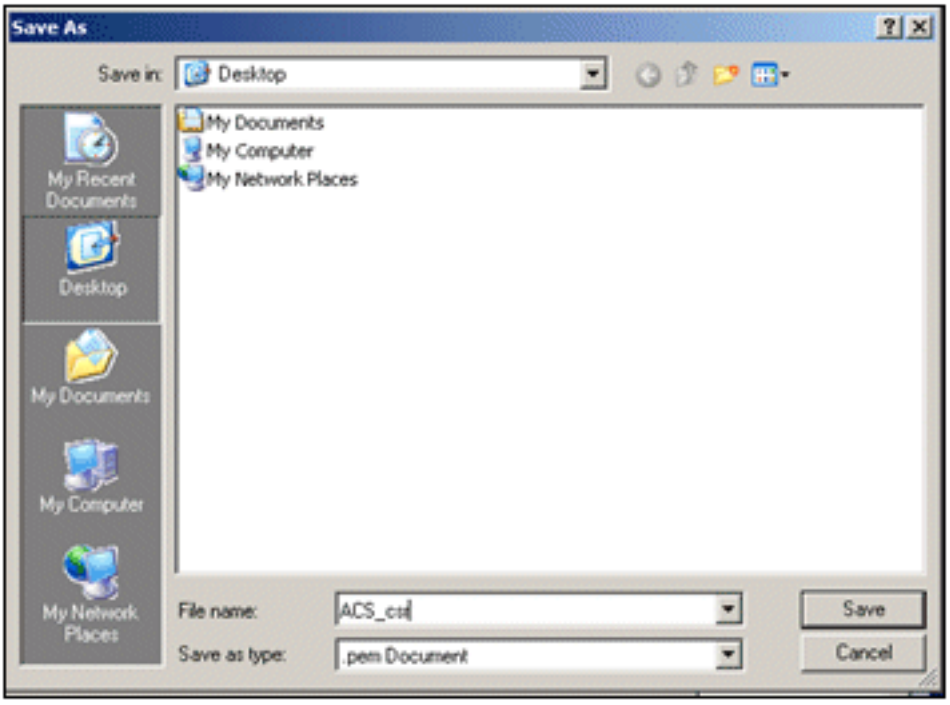
6. En Administración del sistema, vaya a **Configuración > Certificados de servidor local > Solicitudes de firma pendientes**.**Nota:** La razón de este paso es que Windows 2003 no permite claves exportables y necesita generar una solicitud de certificado basada en el certificado ACS que creó anteriormente que sí lo hace.



7. Elija la entrada **Solicitud de firma de certificado** y haga clic en **Exportar**.



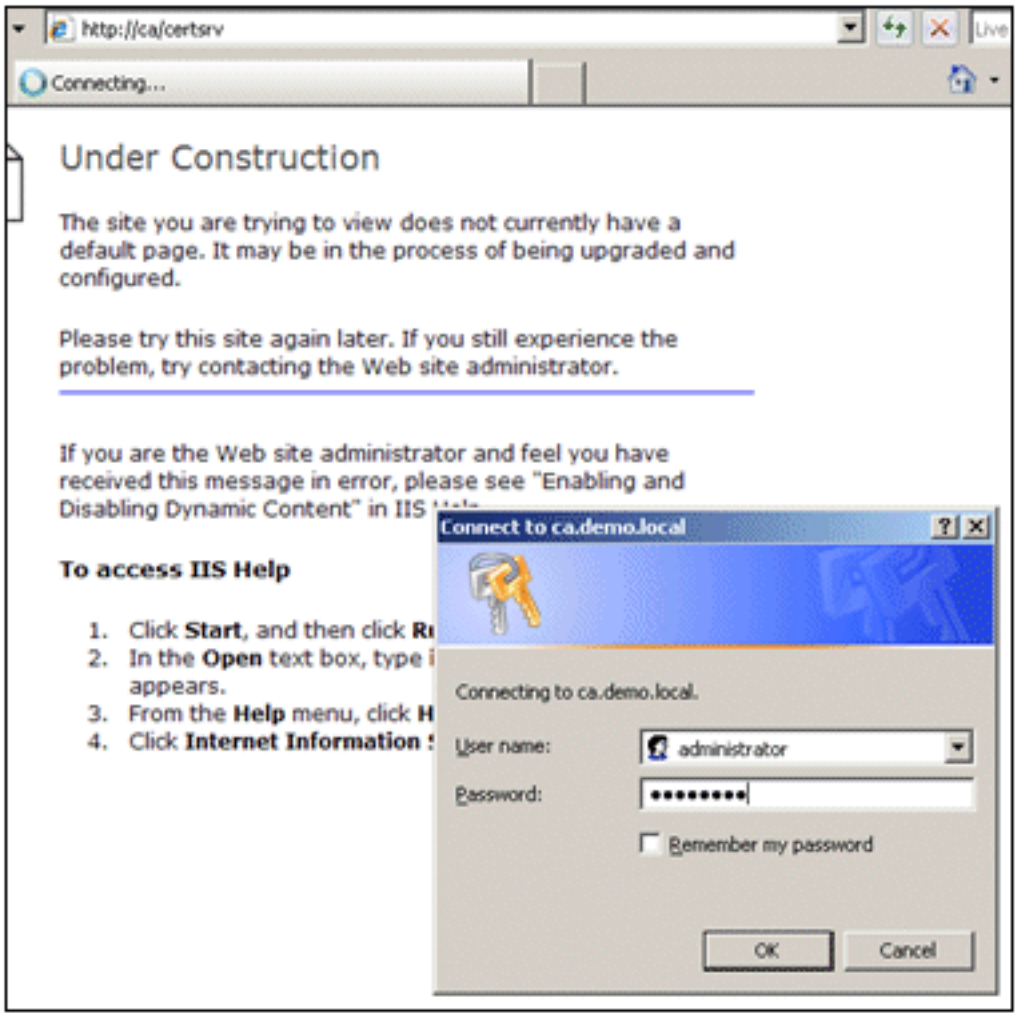
8. Guarde el archivo ACS certificate **.pem** en el escritorio.



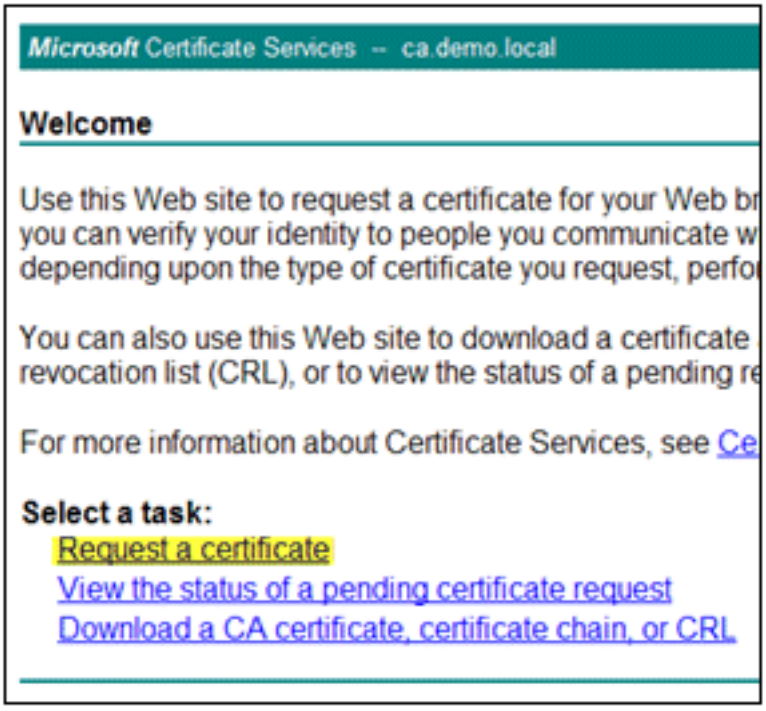
Instale el certificado en el software ACS 5.1

Siga estos pasos:

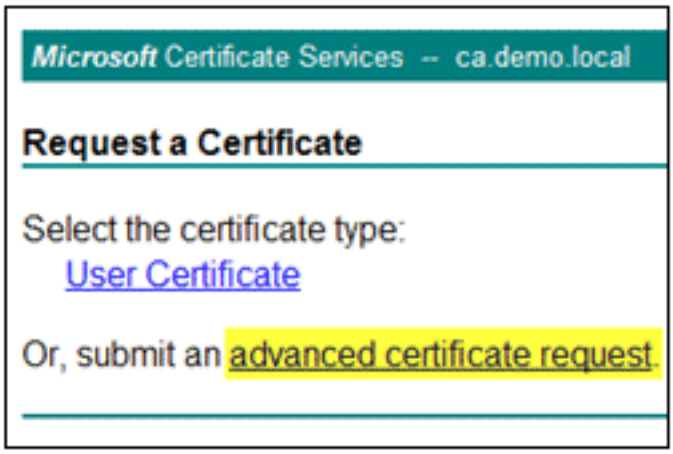
1. Abra un navegador y conéctese a la URL del servidor de la CA **http://10.0.10.10/certsrv**.



2. Aparece la ventana Servicios de Certificate Server de Microsoft. Elija **Solicitar un certificado**.

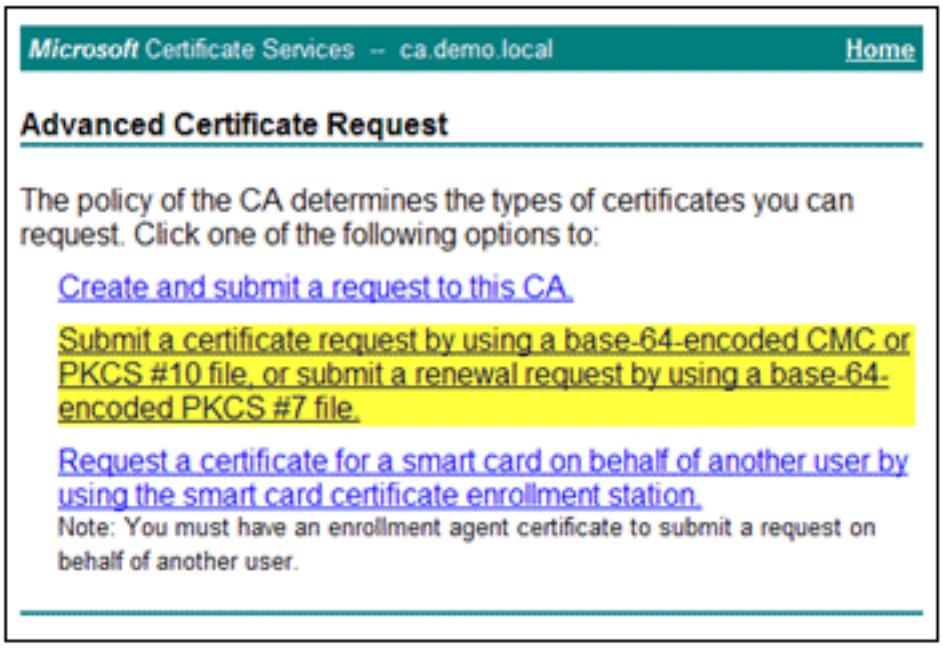


3. Haga clic para enviar una **solicitud de certificado**



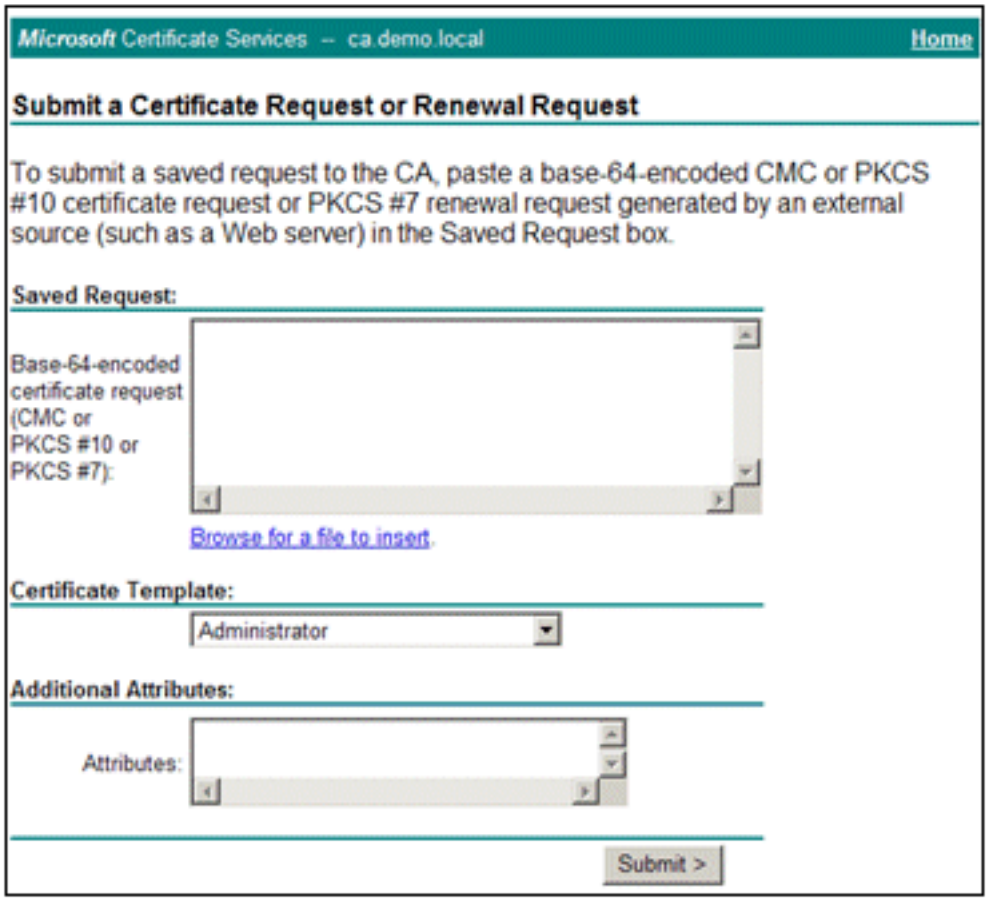
avanzada.

4. En la solicitud avanzada, haga clic en **Enviar una solicitud de certificado con una codificación**



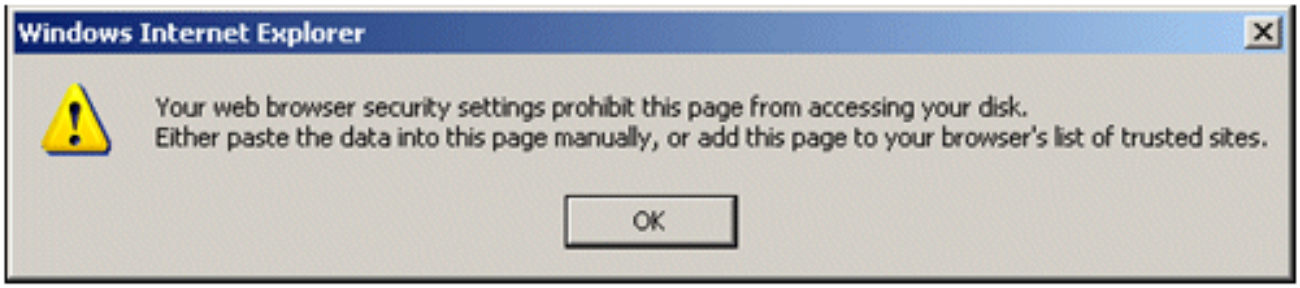
base-64...

5. En el campo Saved Request (Solicitud guardada), si la seguridad del navegador lo permite, busque el archivo de solicitud de certificado ACS anterior e

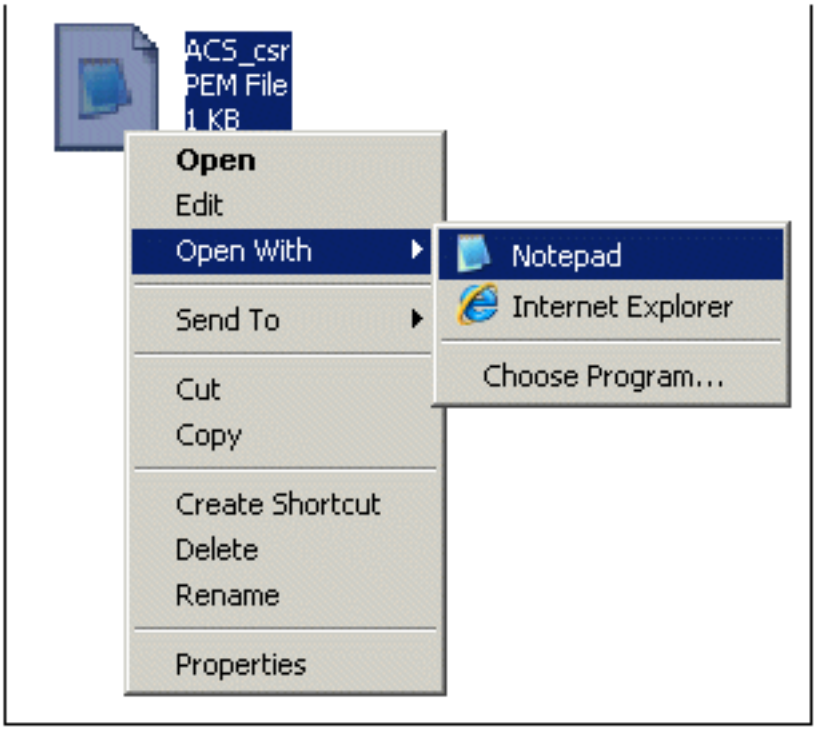


insértelo.

6. Es posible que la configuración de seguridad del explorador no permita el acceso al archivo en un disco. Si es así, haga clic en **Aceptar** para realizar una pegada manual.

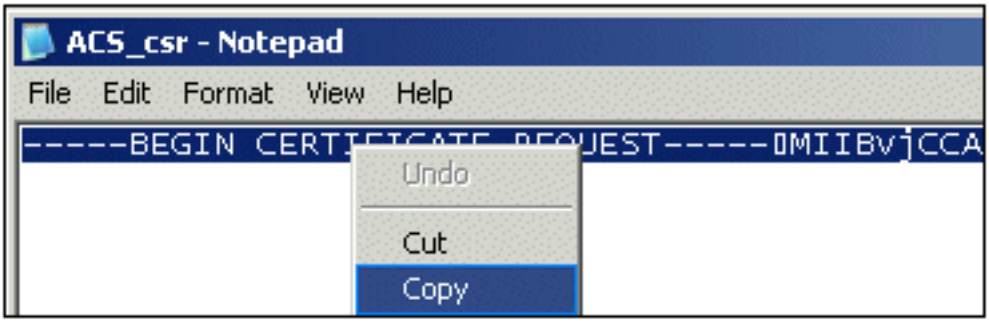


7. Localice el archivo ACS *.pem de la exportación ACS anterior. Abra el archivo con un editor de texto (por ejemplo, el Bloc de



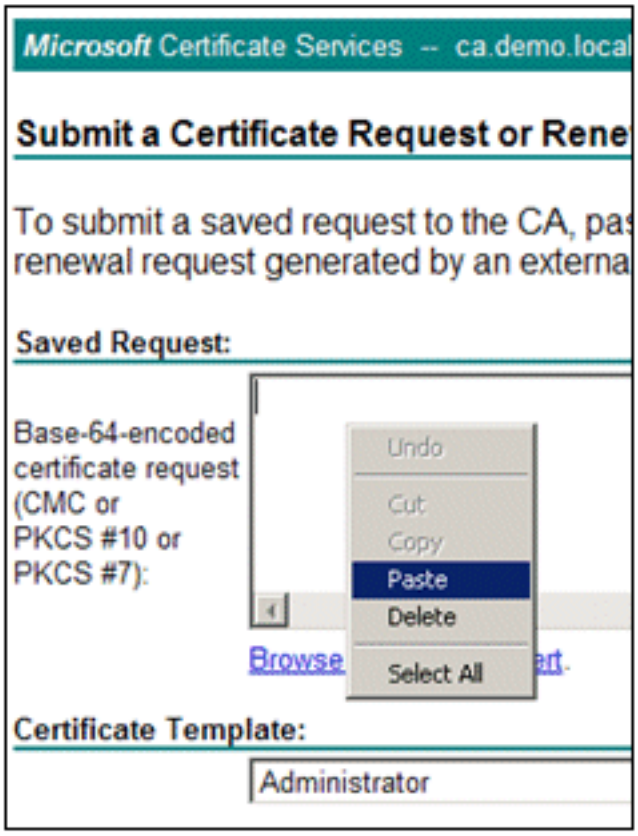
notas).

8. Resalte todo el contenido del archivo y haga clic en



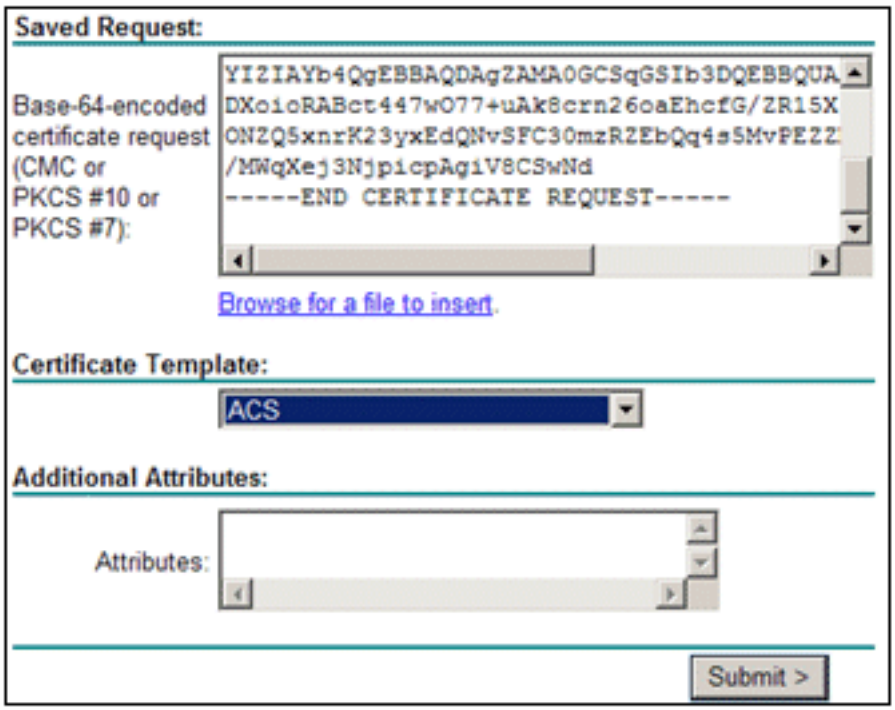
Copiar.

9. Vuelva a la ventana de solicitud de certificado de Microsoft. **Pegue** el contenido copiado en

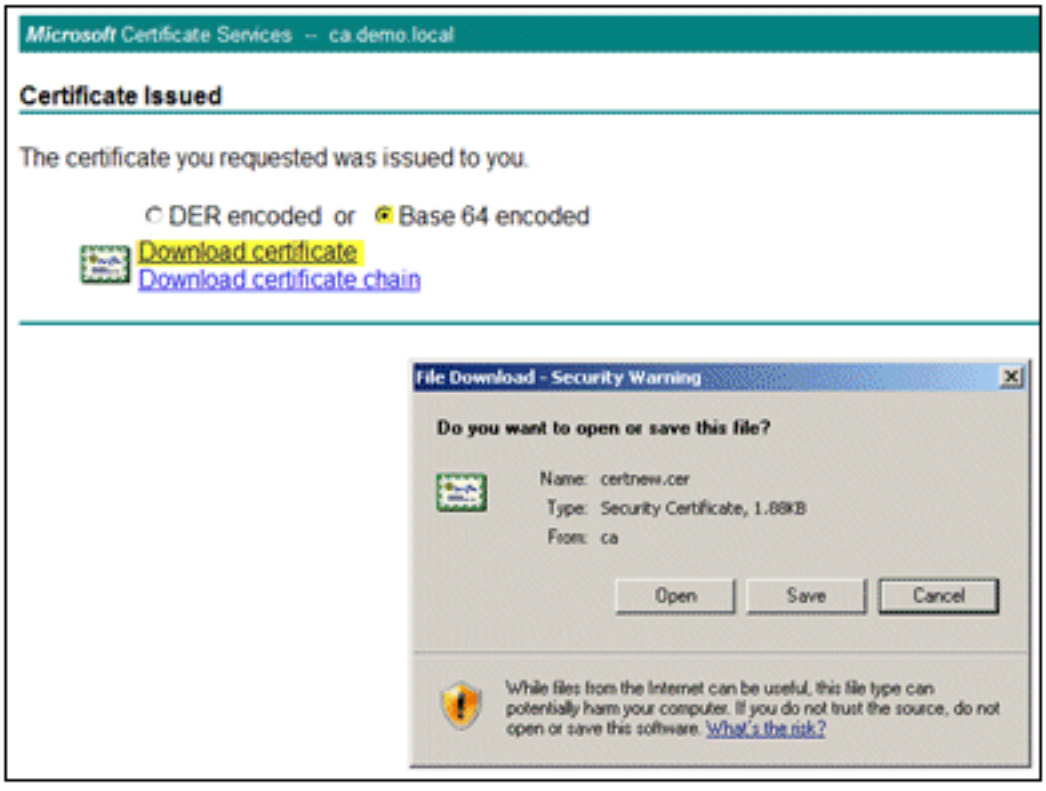


el campo Solicitud guardada.

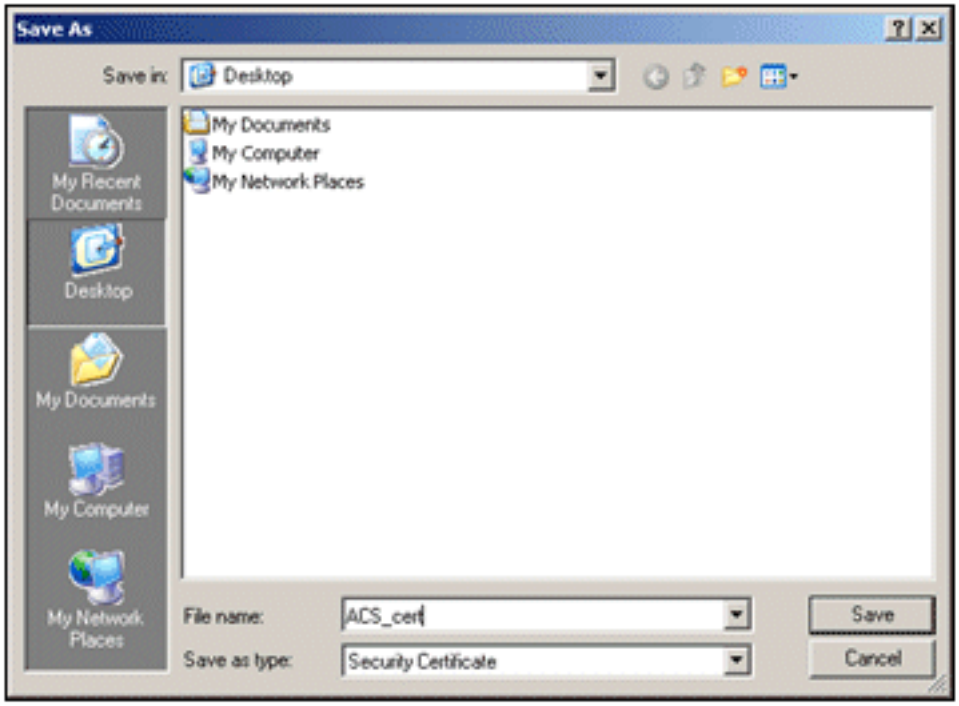
10. Elija **ACS** como la plantilla de certificado, y haga clic en **Submit**.



11. Una vez emitido el certificado, elija **Base 64 codificada** y haga clic en **Descargar certificado**.

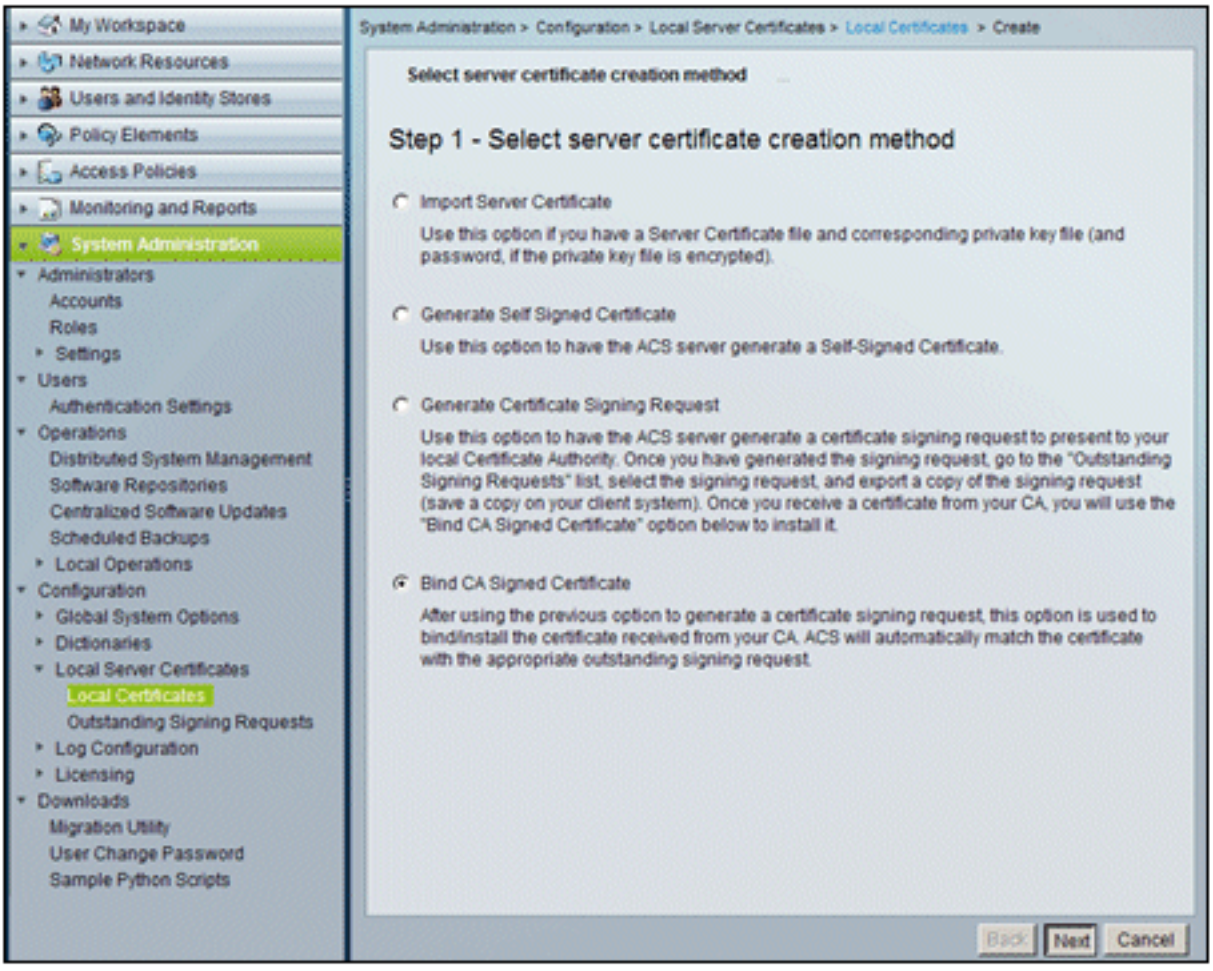


12. Haga clic en **Guardar** para guardar el certificado en el



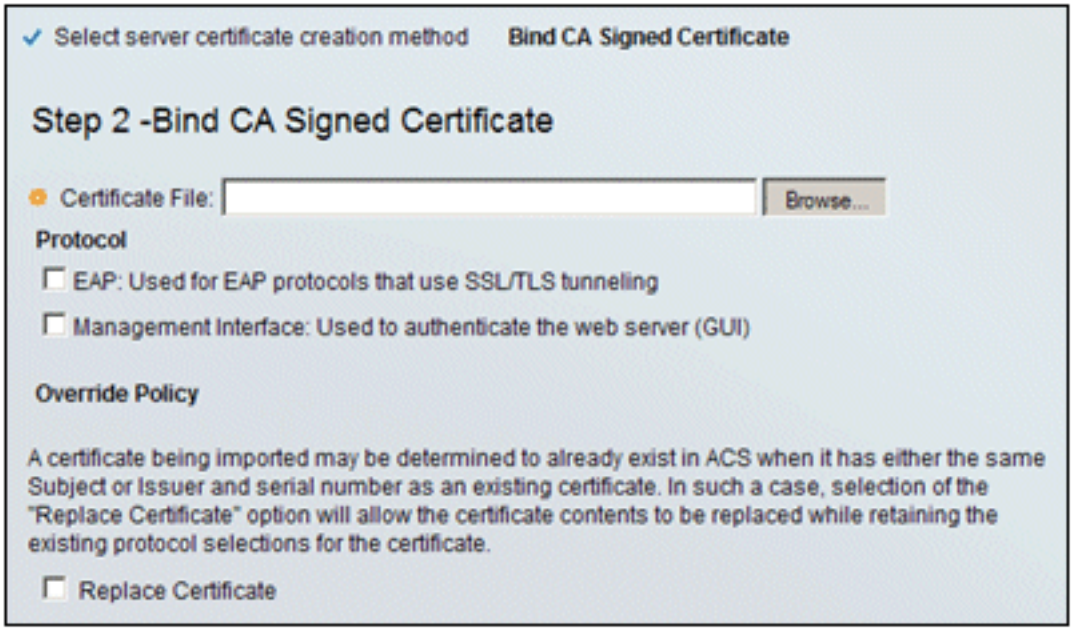
escritorio.

13. Vaya a **ACS > Administración del sistema > Configuración > Certificados de servidor local**. Elija **Bind CA Signed Certificate** y haga clic en



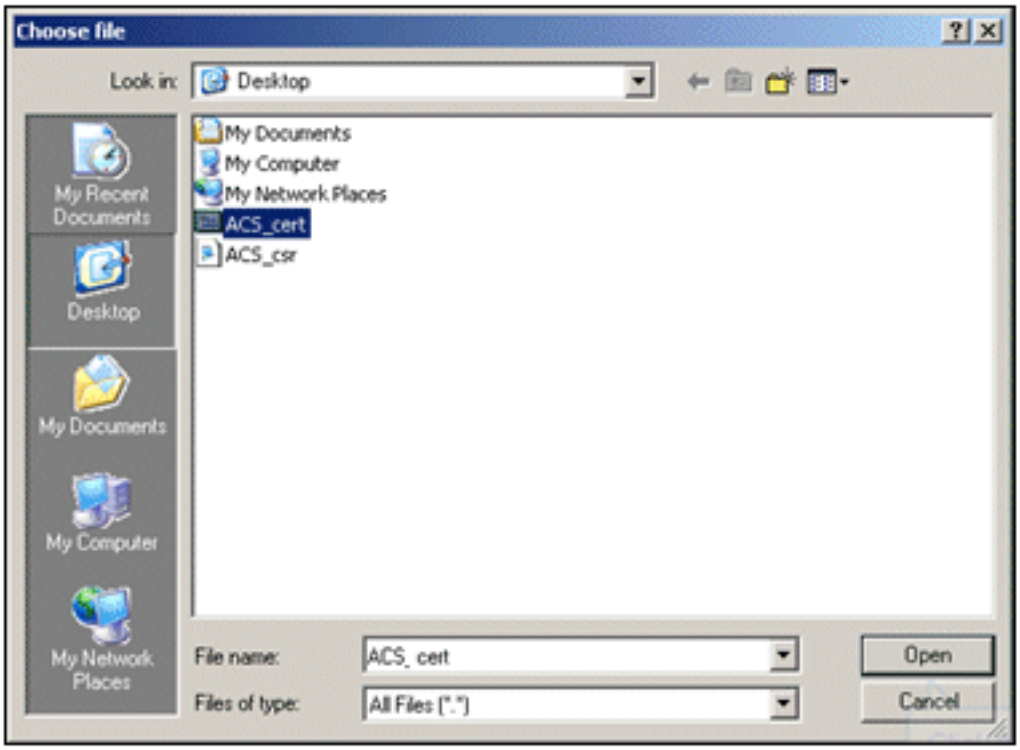
Next.

14. Haga clic en **Browse** y localice el certificado



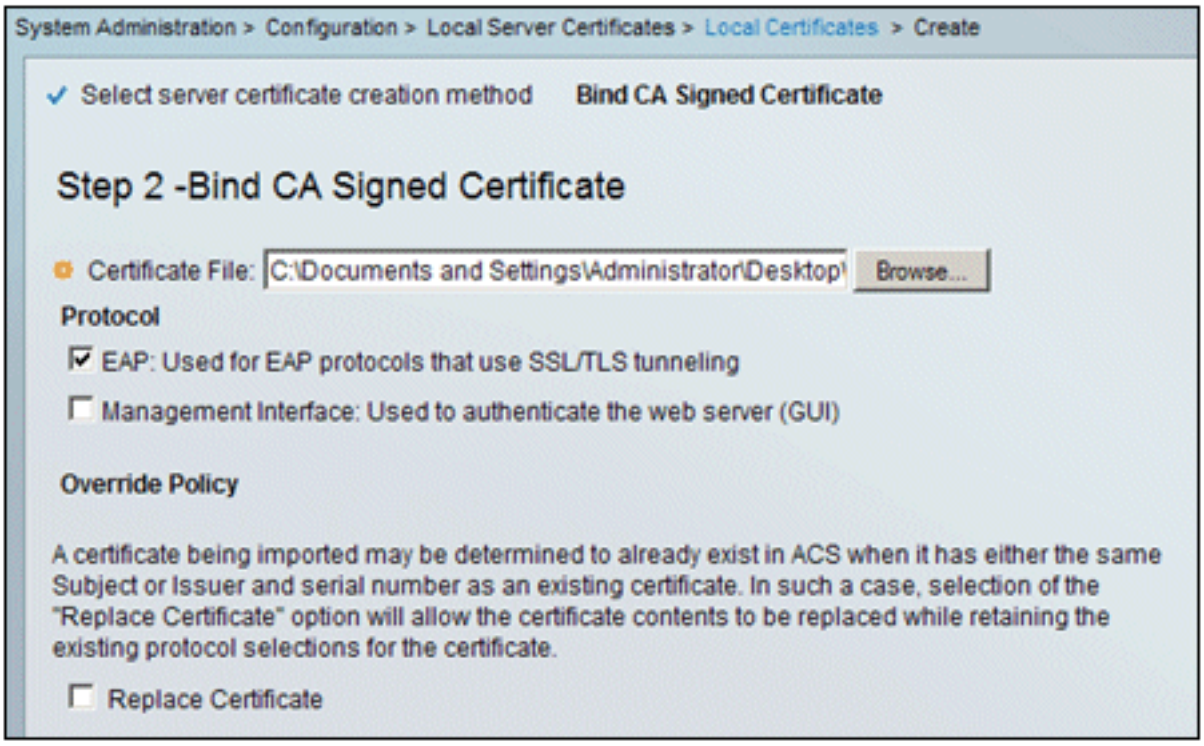
guardado.

15. Elija el certificado ACS emitido por el servidor CA y haga clic en

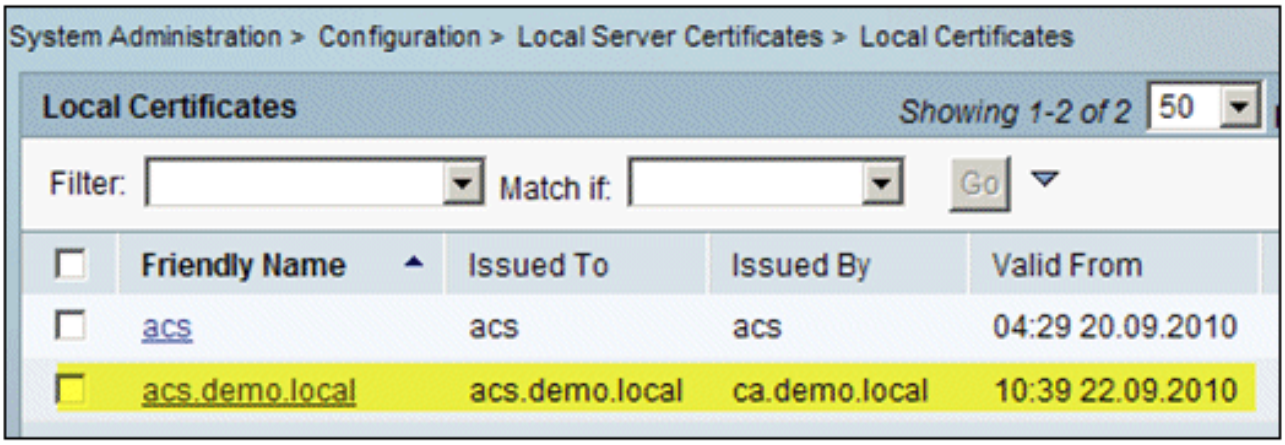


Abrir.

16. Además, marque la casilla Protocol para **EAP** y haga clic en **Finish**.



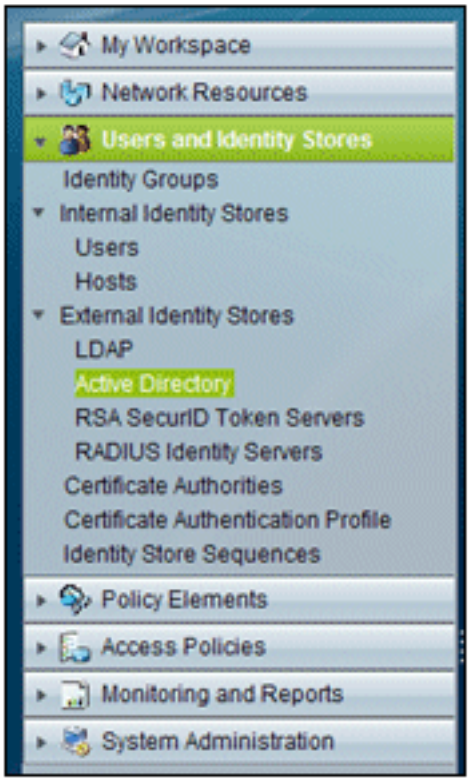
17. El certificado ACS emitido por la CA aparecerá en el certificado local ACS.



Configuración del almacén de identidades ACS para Active Directory

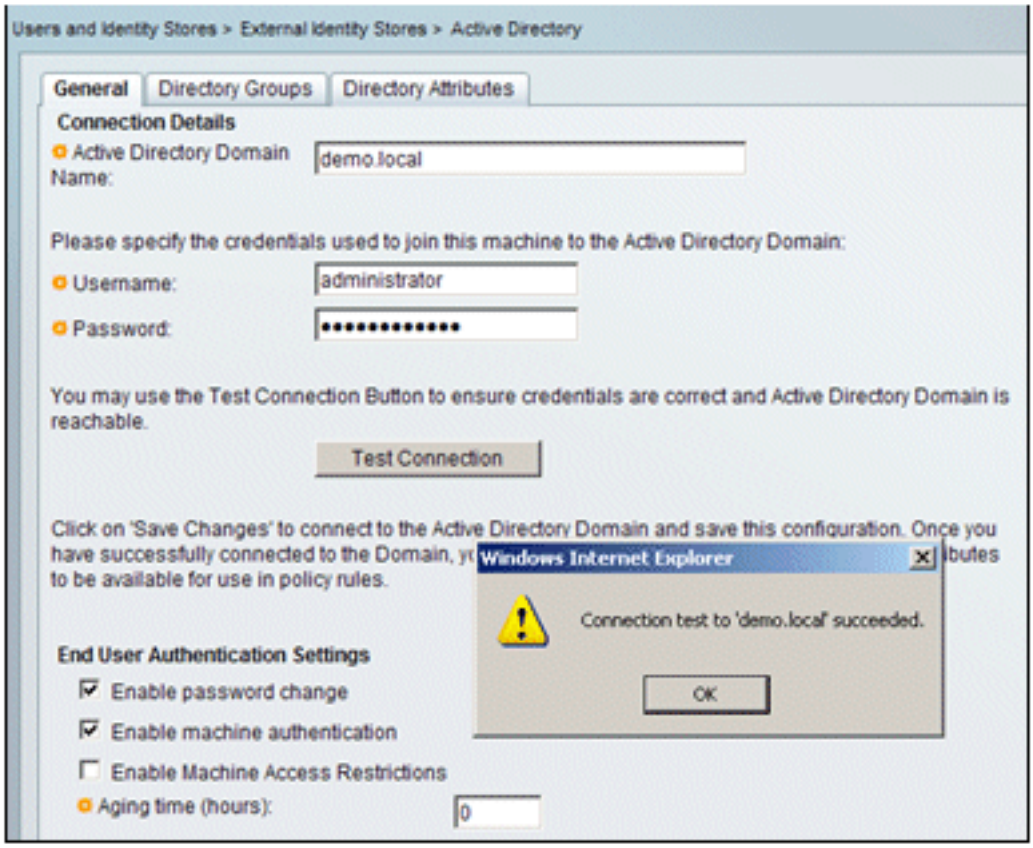
Siga estos pasos:

1. Conéctese a ACS e inicie sesión con la cuenta Admin.
2. Vaya a **Usuarios y almacenes de identidad > Almacenes de identidad externos > Active**



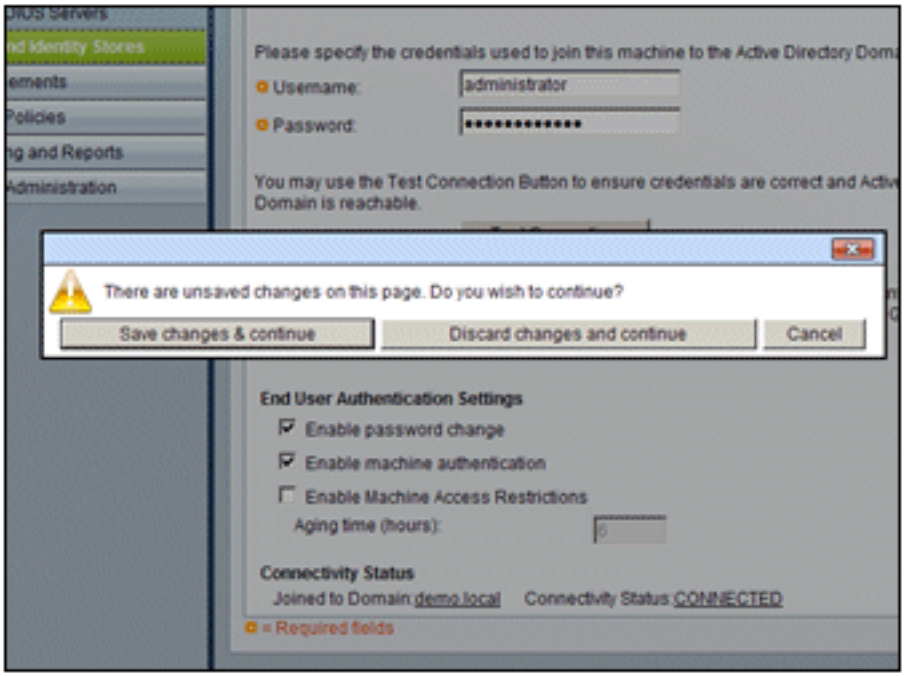
Directory.

3. Ingrese Active Directory Domain *demo.local*, ingrese la contraseña del servidor y haga clic en **Test Connection**. Haga clic en **Aceptar** para



continuar.

4. Haga clic en **Guardar**

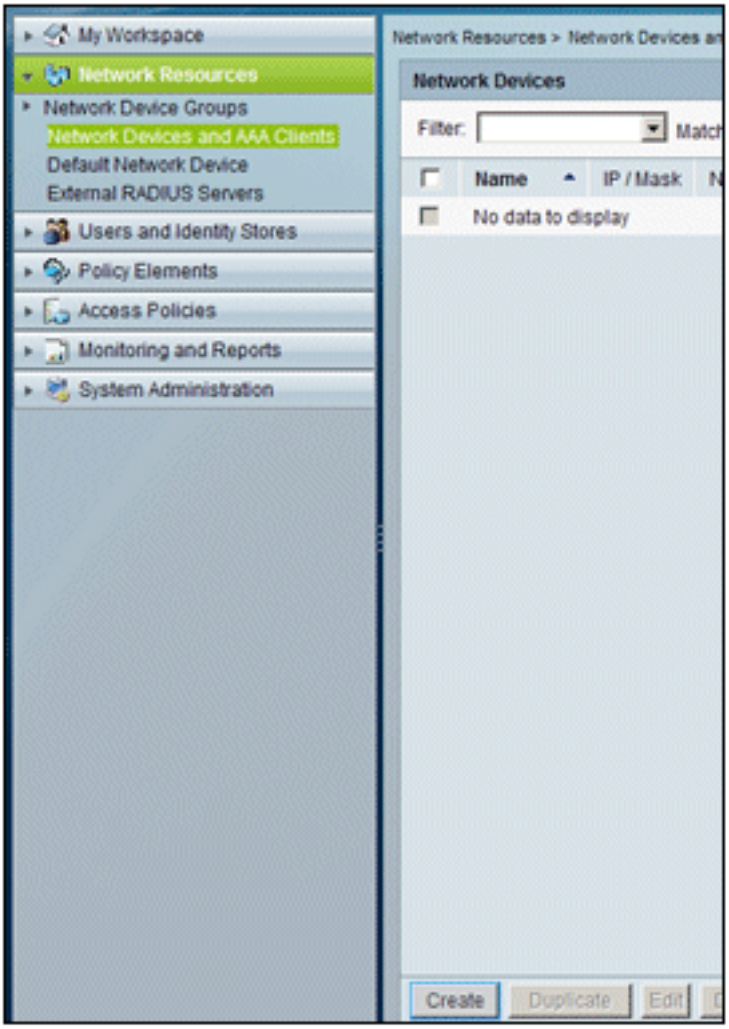
cambios. 

Nota: Para obtener más información sobre el procedimiento de integración de ACS 5.x, consulte Ejemplo de Configuración de ACS 5.x y versiones posteriores: Integración con Microsoft Active Directory.

Agregar un controlador a ACS como cliente AAA

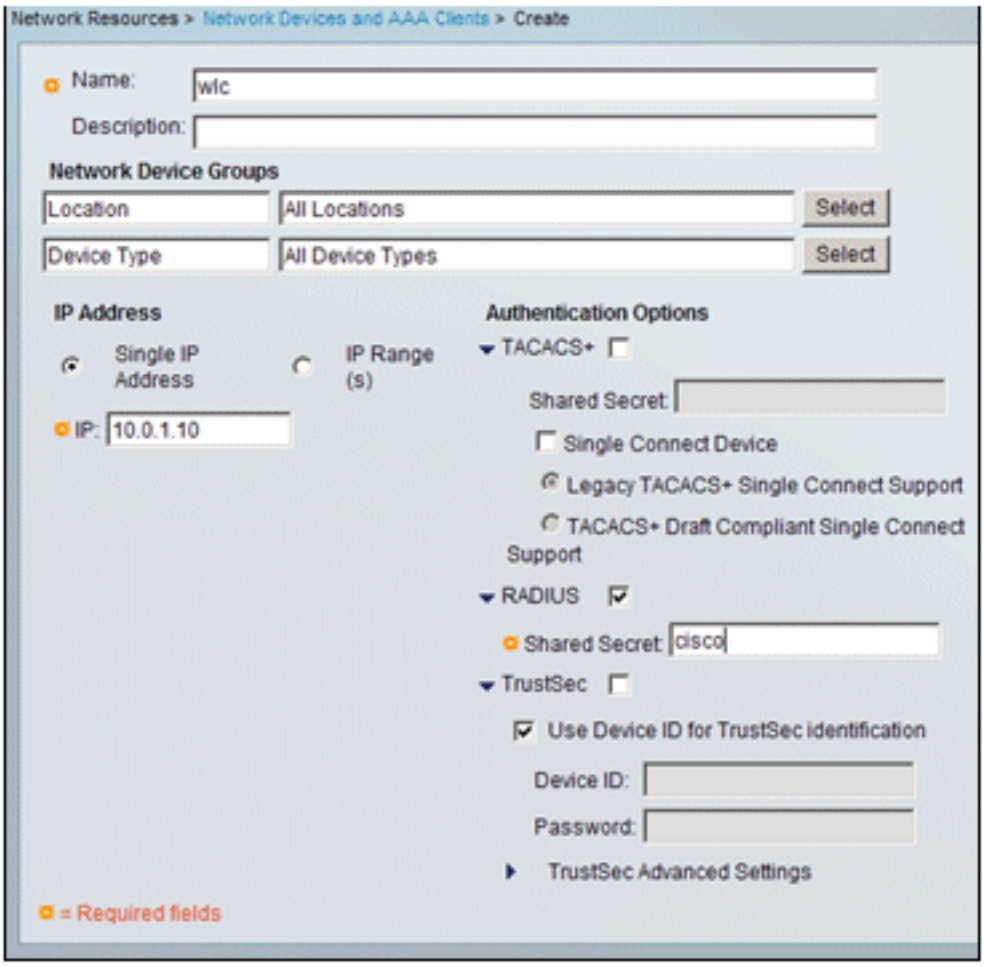
Siga estos pasos:

1. Conéctese a ACS y vaya a **Recursos de red > Dispositivos de red y clientes AAA**. Haga clic



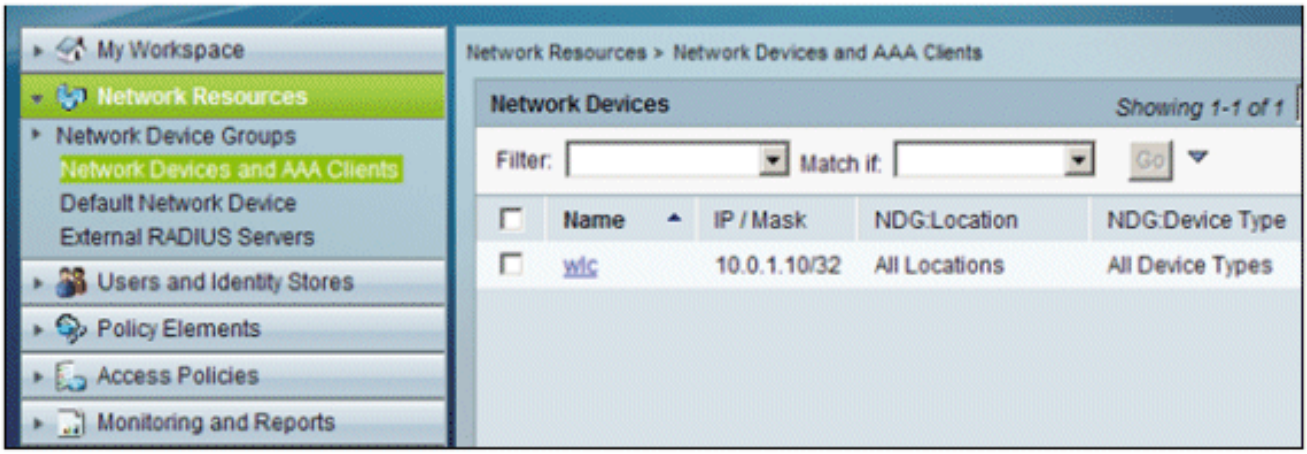
en **Crear**.

2. Escriba en estos campos:Nombre - **wlc**IP: **10.0.1.10**Casilla de verificación RADIUS: **activada**Secreto compartido:



Cisco

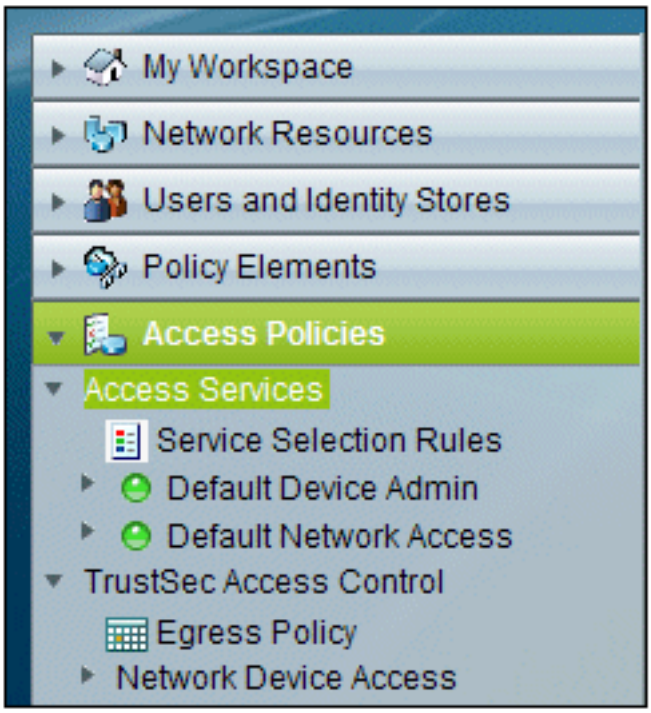
3. Haga clic en **Enviar** cuando haya terminado. El controlador aparecerá como una entrada en la lista de dispositivos de red
ACS.



Configuración de las Políticas de Acceso ACS para la Red Inalámbrica

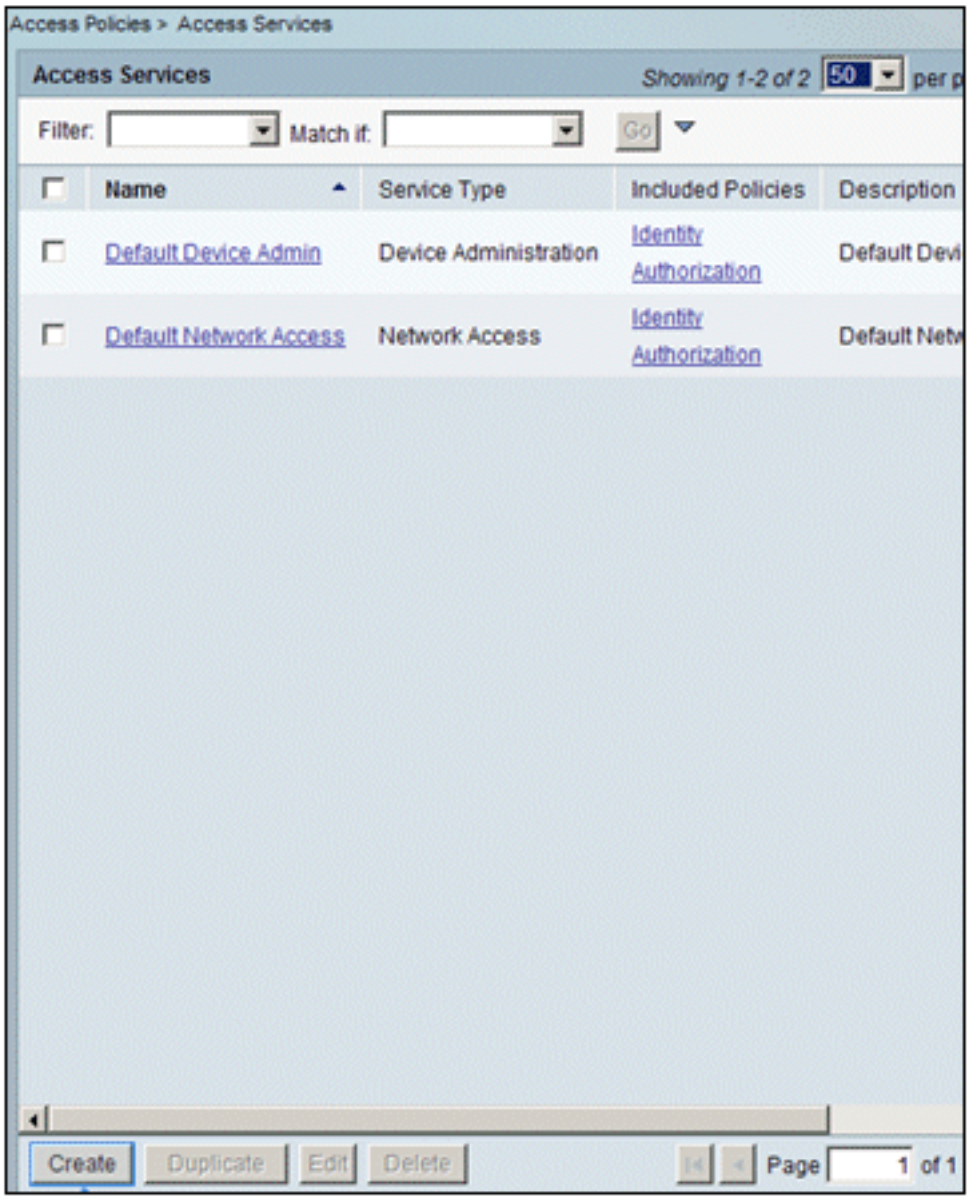
Siga estos pasos:

1. En ACS, vaya a **Políticas de acceso > Servicios de**



acceso.

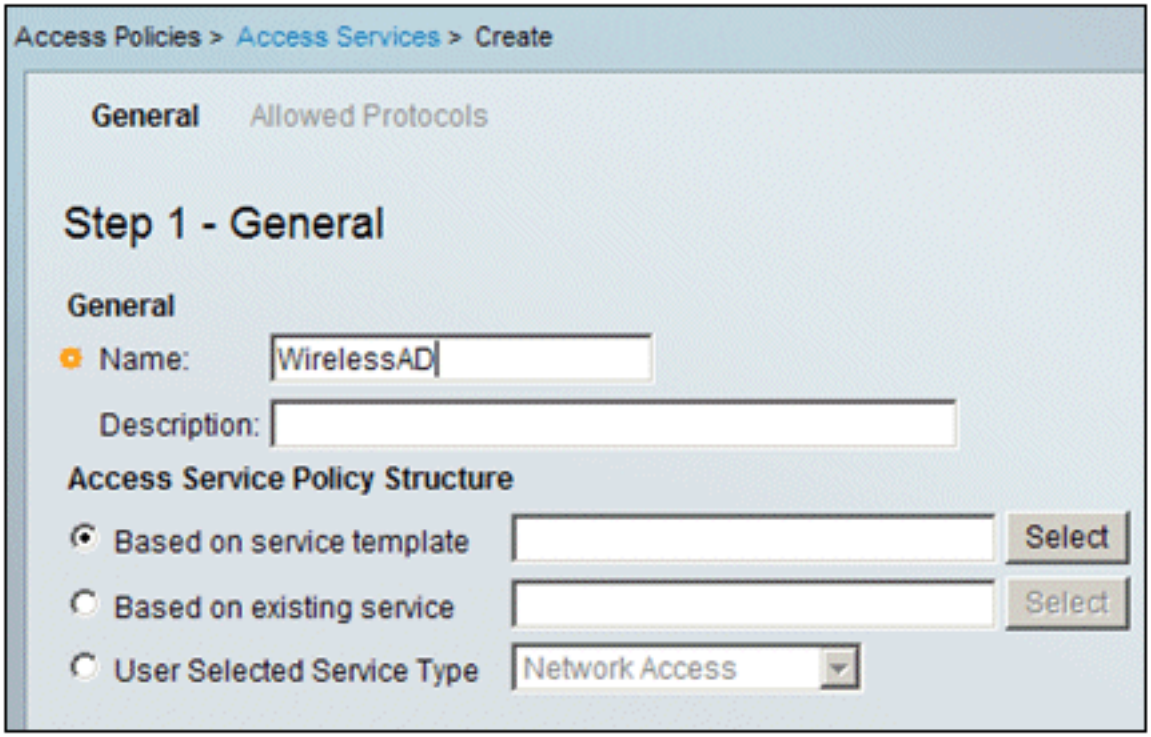
2. En la ventana Access Services, haga clic en



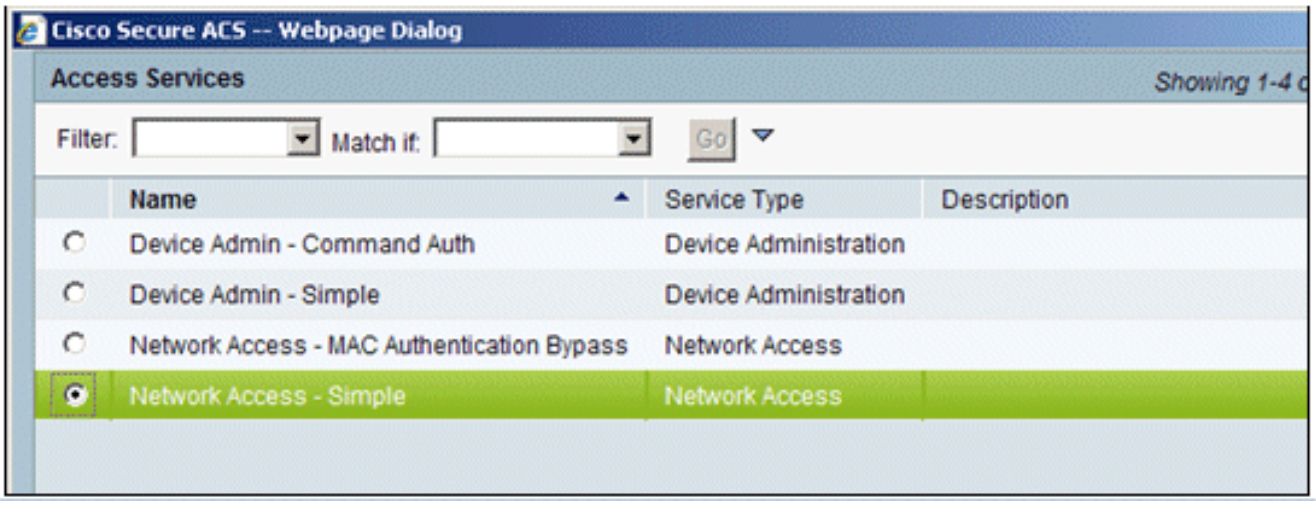
Create.

3. Cree un servicio de acceso e introduzca un nombre (por ejemplo, WirelessAD). Elija **Basado**

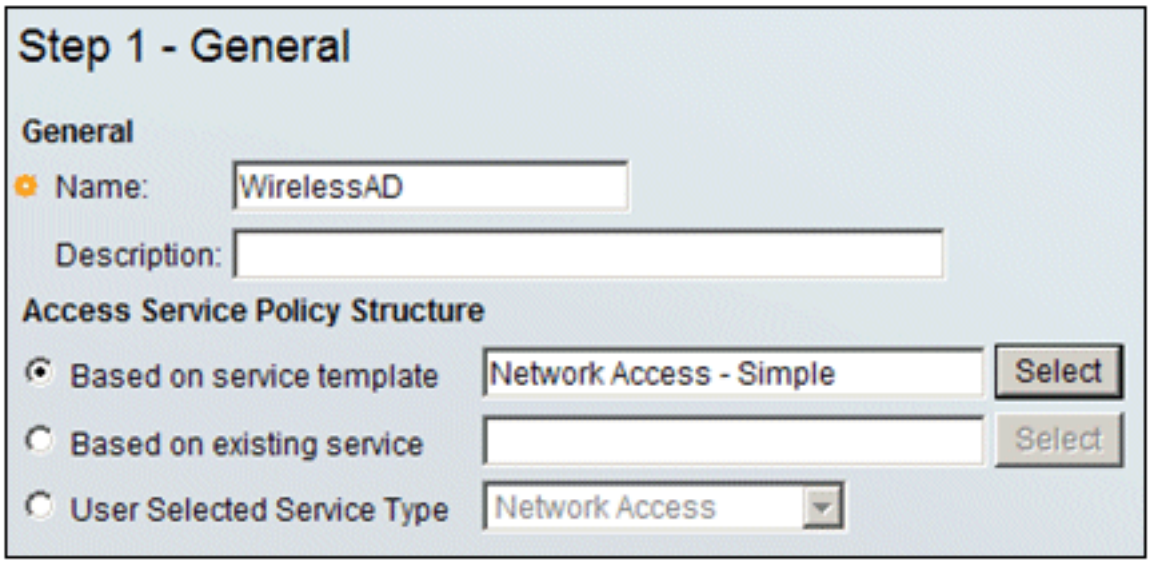
en plantilla de servicio y haga clic en **Seleccionar**.



4. En el cuadro de diálogo Página web, elija **Network Access - Simple**. Click OK.

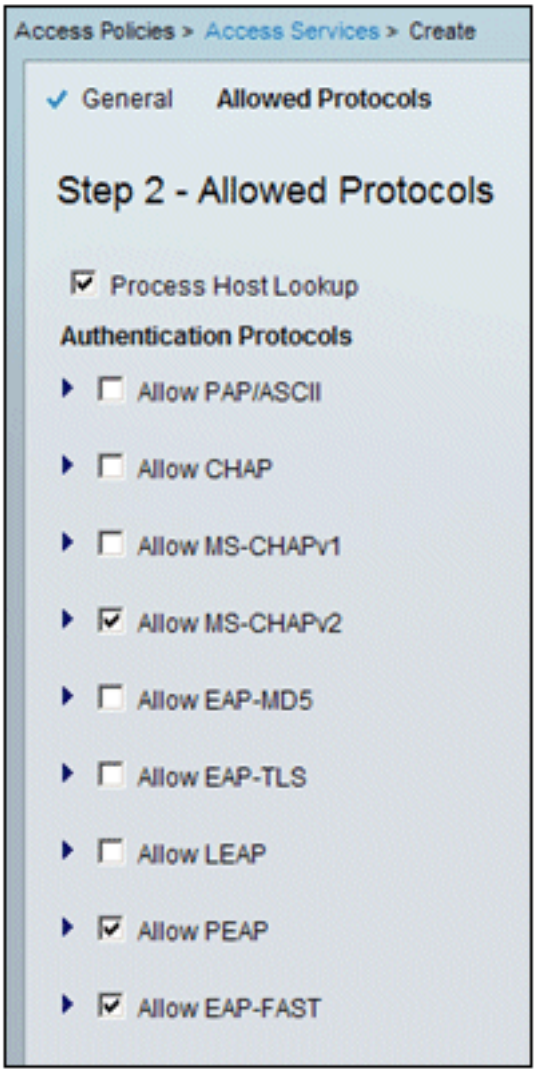


5. En el cuadro de diálogo Página web, elija **Network Access - Simple**. Click OK. Una vez seleccionada la plantilla, haga clic en



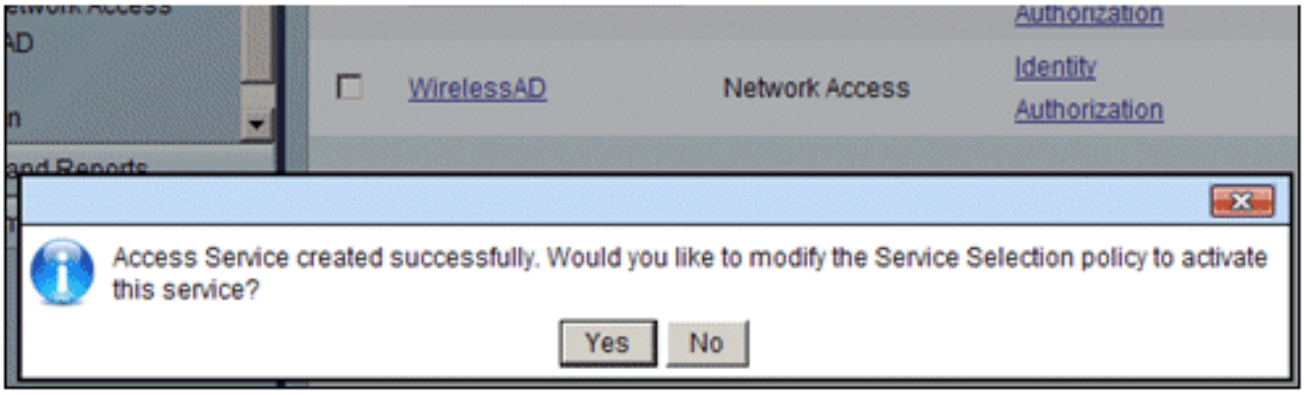
Next.

6. En Protocolos permitidos, active las casillas **Allow MS-CHAPv2** y **Allow PEAP**. Haga clic en

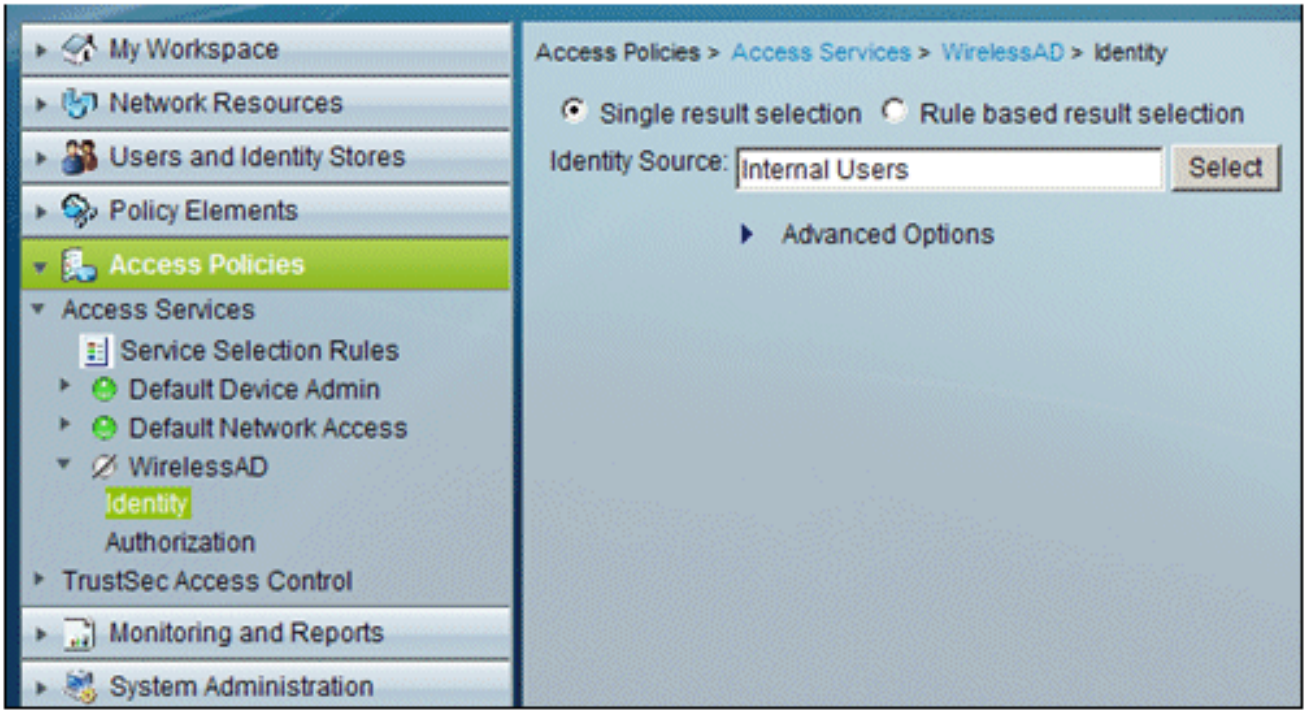


Finish (Finalizar).

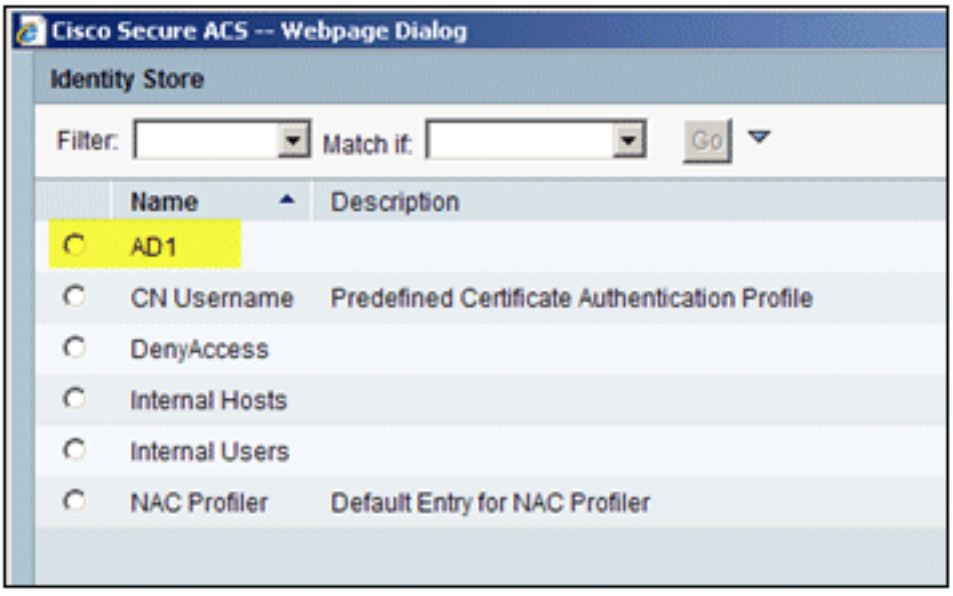
7. Cuando ACS le pida que active el nuevo servicio, haga clic en **Yes**.



8. En el nuevo servicio de acceso que se acaba de crear/activar, amplíe y seleccione **Identidad**. Para el origen de identidad, haga clic en **Select**.



9. Elija **AD1** para Active Directory que se configuró en ACS, haga clic en **OK**.



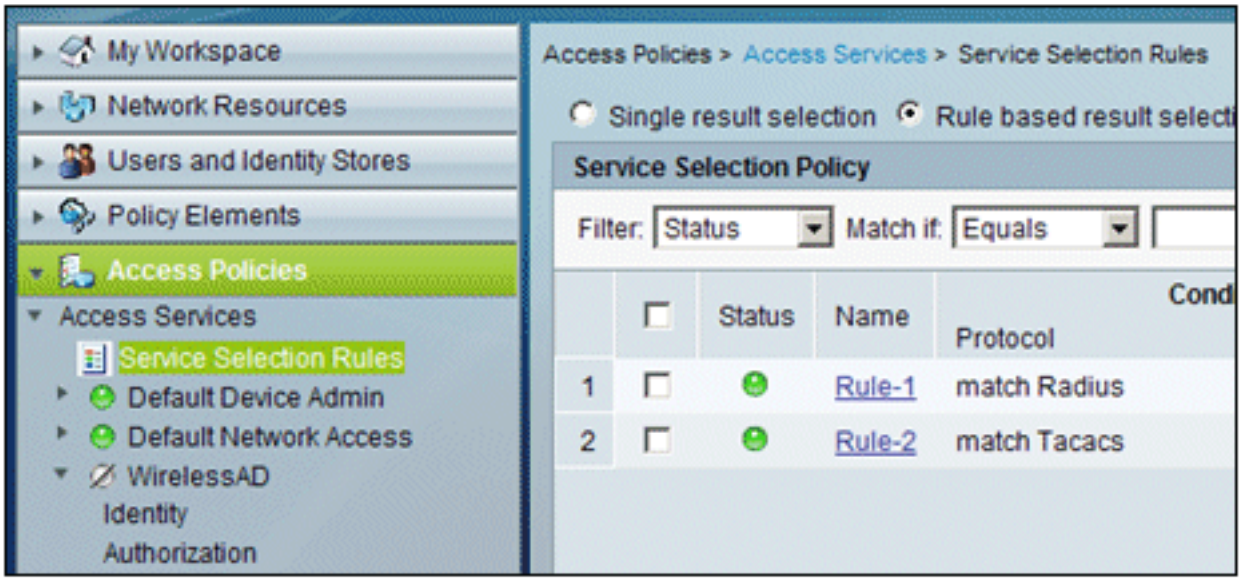
10. Confirme que el origen de identidad es AD1 y haga clic en **Guardar**

cambios.

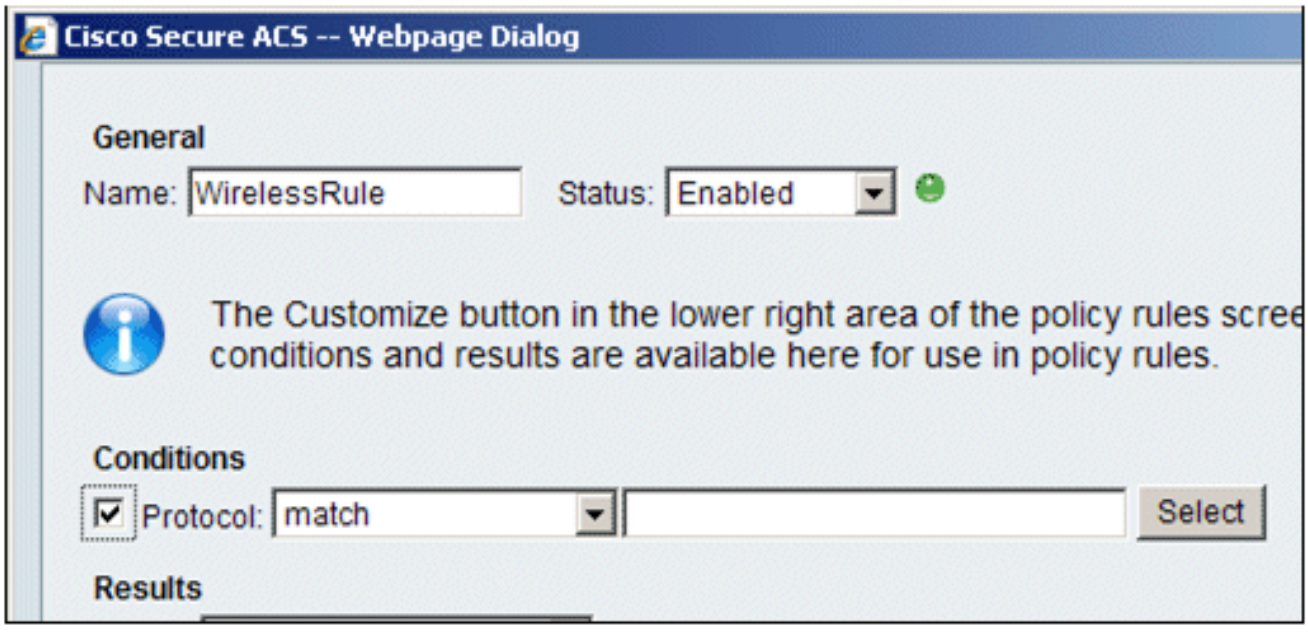
Crear política de acceso ACS y regla de servicio

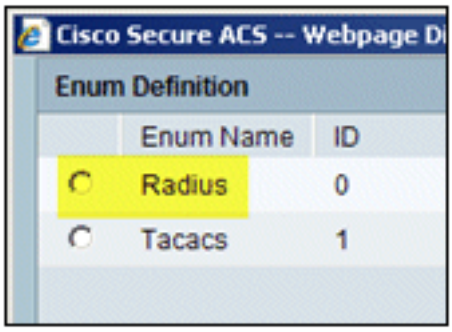
Siga estos pasos:

1. Vaya a **Políticas de acceso > Reglas de selección de servicio**.

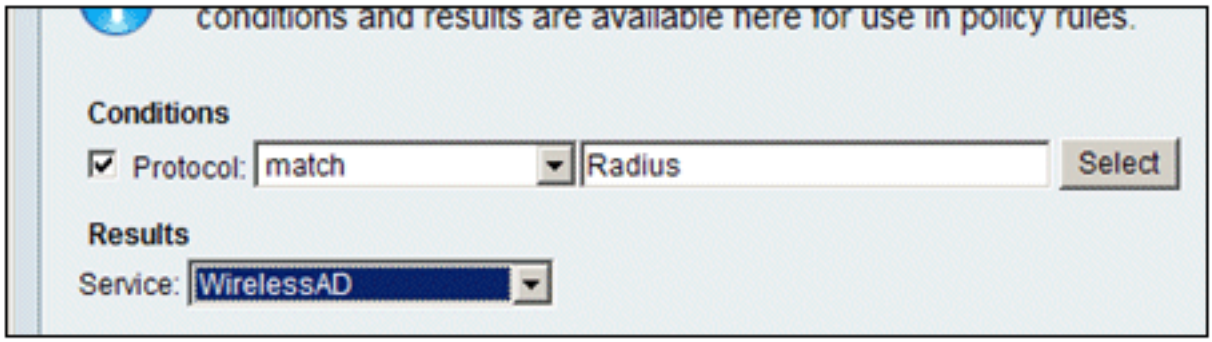


2. Haga clic en **Create** en la ventana Service Selection Policy . Asigne un nombre a la nueva regla (por ejemplo, *WirelessRule*). Marque la casilla para que **Protocol** coincida con **Radius**.

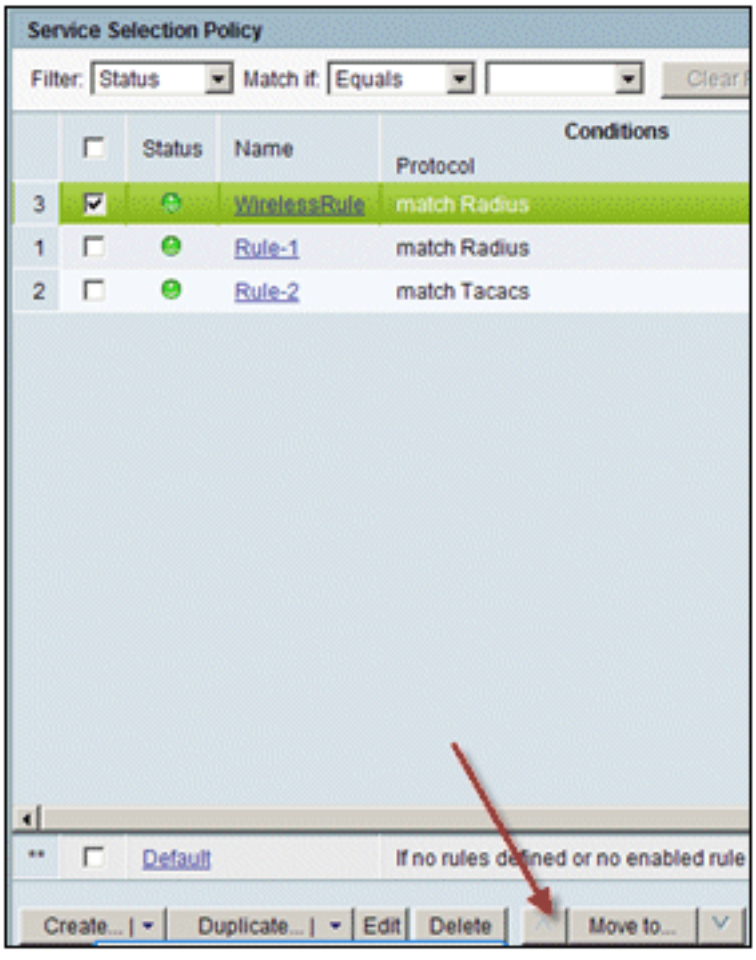




3. Elija **Radius**, y haga clic en **OK**.
4. En Resultados, elija **WirelessAD** para el servicio (creado en el paso anterior).



5. Una vez creada la nueva regla inalámbrica, elija y **Mueva** esta regla a la parte superior, que será la primera regla que identifique la autenticación del radio inalámbrico mediante Active Directory.



Configuración de CLIENTE para PEAP mediante Windows Zero Touch

En nuestro ejemplo, CLIENTE es un equipo que ejecuta Windows XP Professional con SP que actúa como cliente inalámbrico y obtiene acceso a los recursos de la intranet a través del punto de acceso inalámbrico. Complete los procedimientos de esta sección para configurar CLIENTE como cliente inalámbrico.

Realizar una instalación y configuración básicas

Siga estos pasos:

1. Conecte CLIENTE al segmento de red de la intranet mediante un cable Ethernet conectado al concentrador.
2. En CLIENTE, instale Windows XP Professional con SP2 como equipo miembro denominado CLIENTE del dominio demo.local.
3. Instale Windows XP Professional con SP2. Debe estar instalado para que PEAP sea compatible.**Nota:** Firewall de Windows se activa automáticamente en Windows XP Professional con SP2. No apague el firewall.

Instalación del adaptador de red inalámbrico

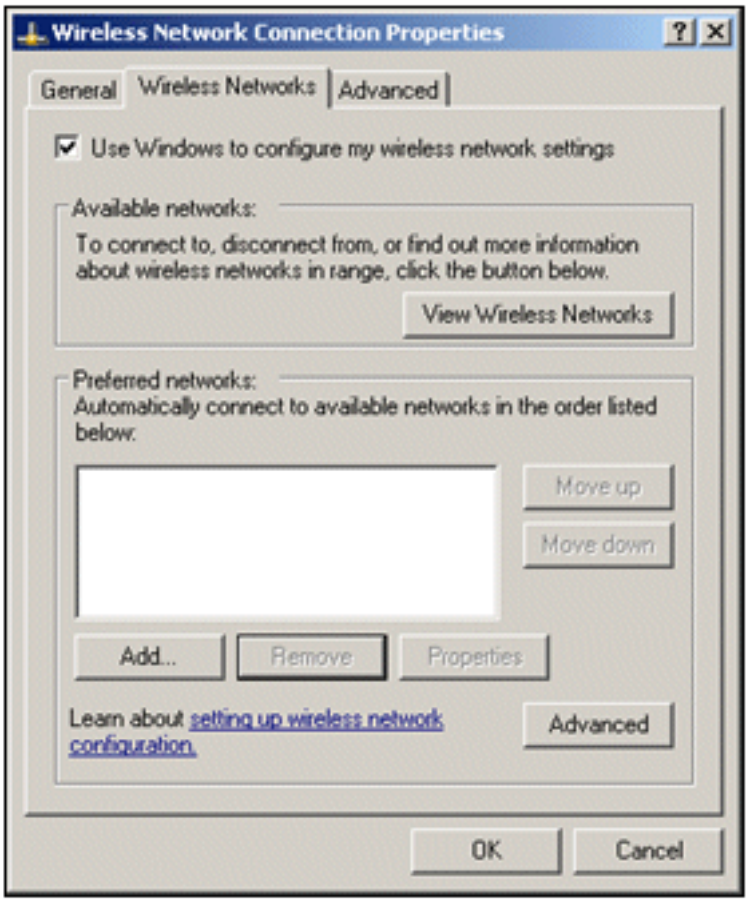
Siga estos pasos:

1. Apague el equipo CLIENTE.
2. Desconecte el equipo CLIENTE del segmento de red de la intranet.
3. Reinicie el equipo CLIENTE y, a continuación, inicie sesión con la cuenta de administrador local.
4. Instale el adaptador de red inalámbrico.**Nota:** No instale el software de configuración del fabricante para el adaptador inalámbrico. Instale los controladores del adaptador de red inalámbrico 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

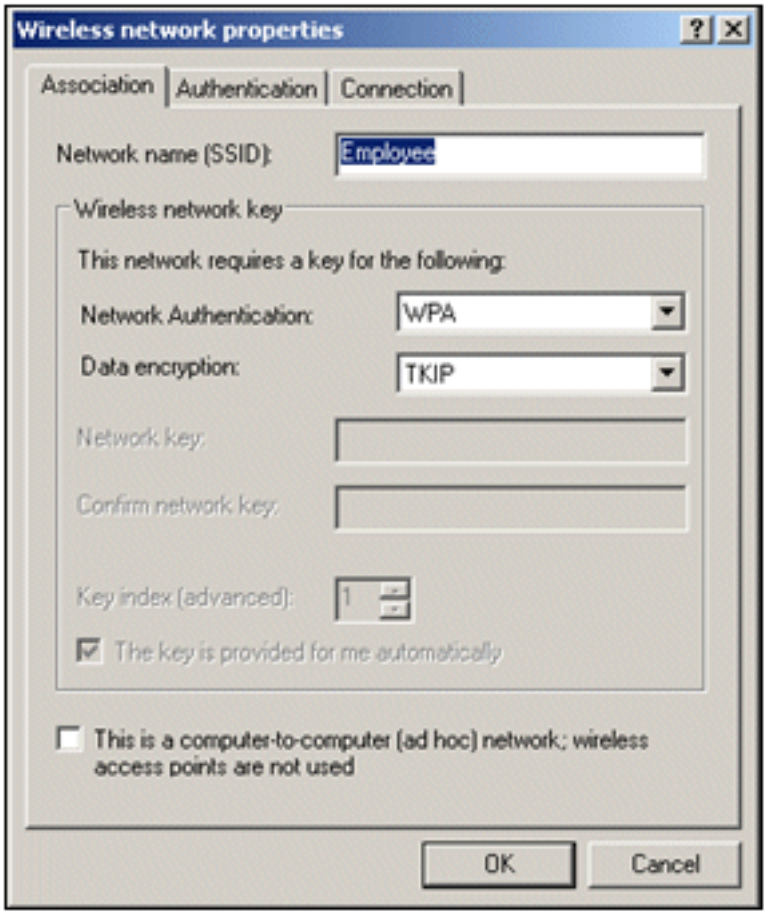
Siga estos pasos:

1. Cierre la sesión y, a continuación, inicie la sesión con la cuenta **WirelessUser** en el dominio **demo.local**.
2. Elija **Inicio > Panel de control**, haga doble clic en **Conexiones de red**, y luego haga clic derecho en **Conexión de red inalámbrica**.
3. Haga clic en **Properties**, vaya a la ficha **Wireless Networks** y asegúrese de que **Use Windows to configure my wireless network settings** esté



marcado.

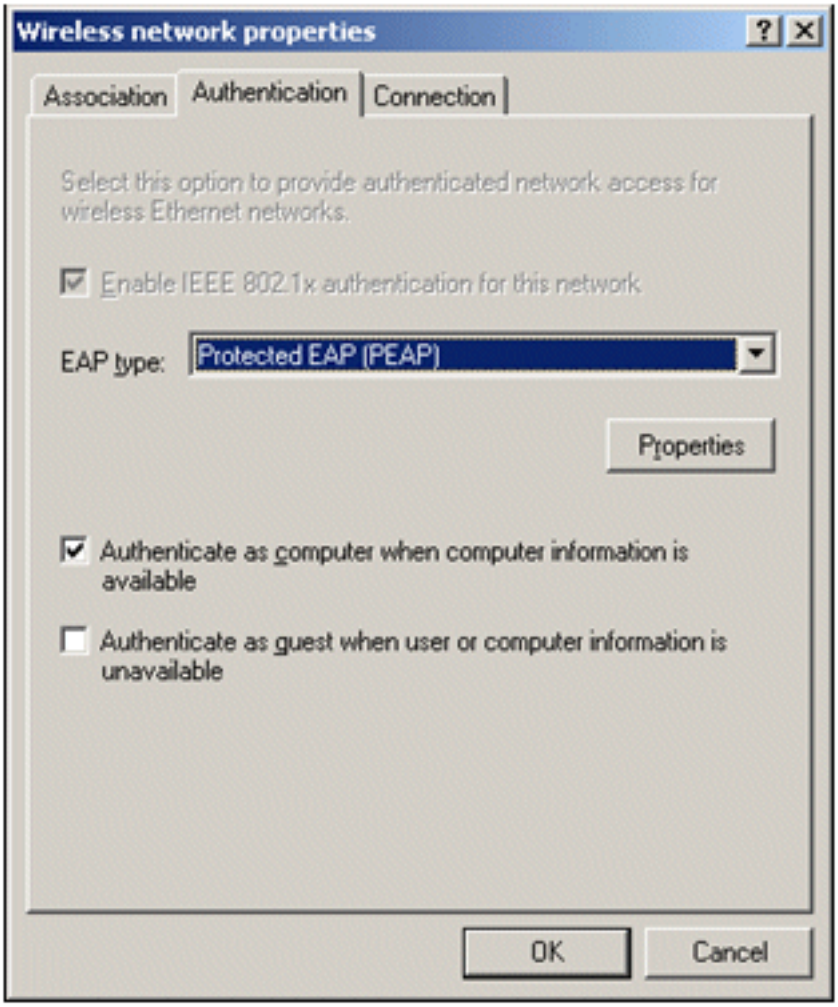
4. Haga clic en Add (Agregar).
5. En la ficha Asociación, introduzca *Empleado* en el campo Nombre de red (SSID).
6. Elija **WPA** para Network Authentication y asegúrese de que Data encryption esté



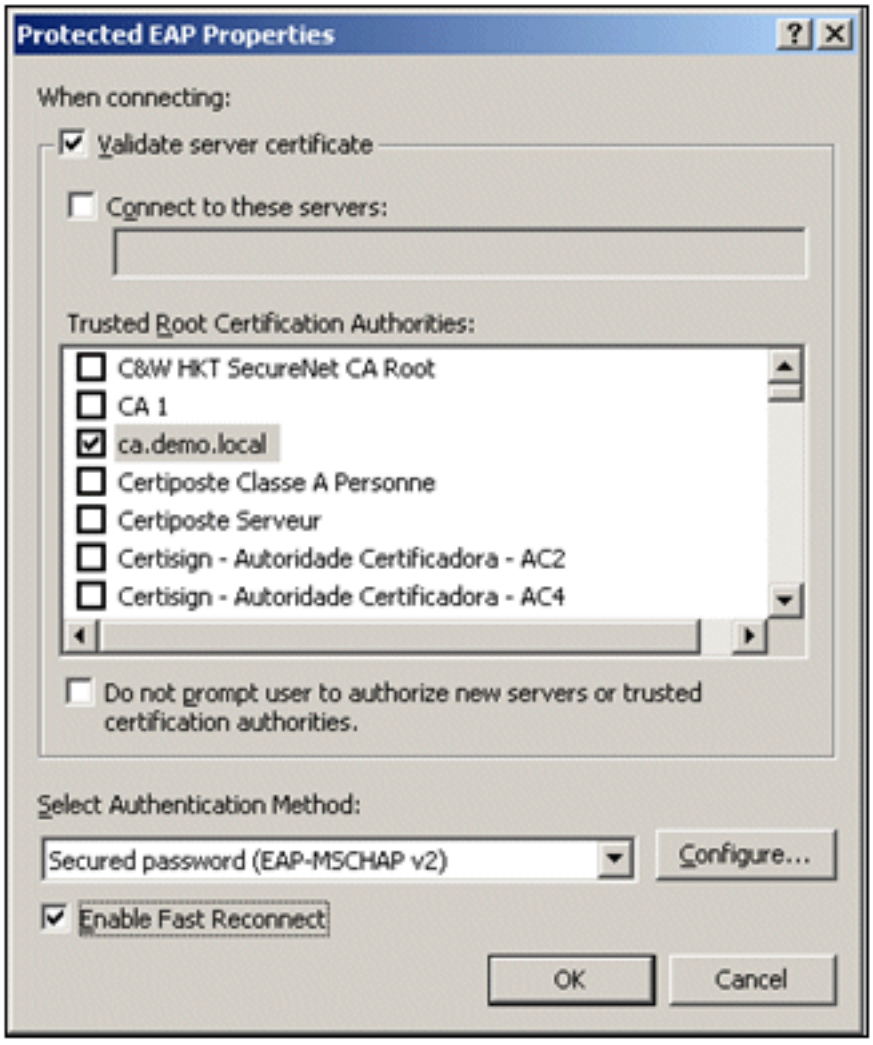
configurado en **TKIP**.

7. Haga clic en la pestaña **Authentication**.

8. Valide que el tipo de EAP esté configurado para utilizar **EAP protegido (PEAP)**. Si no es así, selecciónela en el menú desplegable.
9. Si desea que el equipo se autentique antes del inicio de sesión (lo que permite aplicar scripts de inicio de sesión o instrucciones de directiva 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 la opción **Validar certificado de servidor** esté activada. Además, asegúrese de que la CA que emitió el certificado ACS esté marcada en el menú Entidades de certificación raíz de confianza.
12. Elija **Contraseña segura (EAP-MSCHAP v2)** en Método de autenticación, ya que se utiliza



para la autenticación interna.

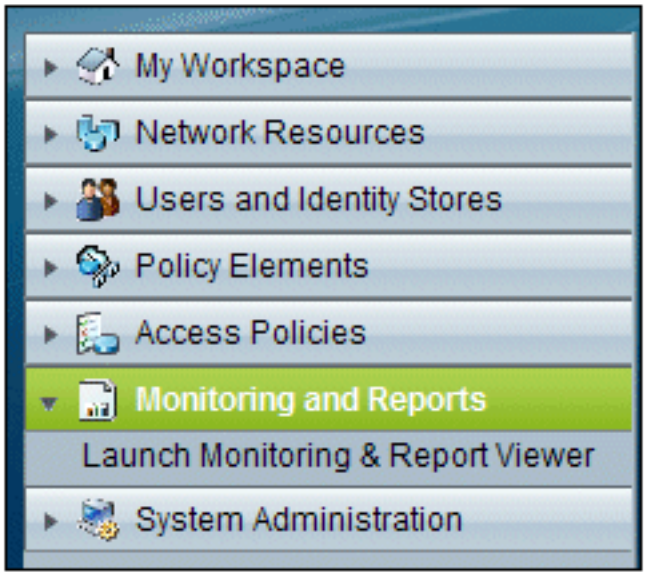
13. Asegúrese de que la casilla de verificación **Enable Fast Reconnect** esté marcada. A continuación, haga clic en **Aceptar** tres veces.
14. Haga clic con el botón secundario en el icono de conexión de red inalámbrica de la bandeja del sistema y, a continuación, haga clic en **Ver redes inalámbricas disponibles**.
15. Haga clic en la red inalámbrica Empleado y, a continuación, haga clic en **Conectar**. El cliente inalámbrico mostrará **Connected** si la conexión se realiza correctamente.

16. Una vez que la autenticación se haya realizado correctamente, compruebe la configuración de TCP/IP del adaptador inalámbrico mediante Conexiones de red. Debe tener un rango de direcciones de 10.0.20.100-10.0.20.200 desde el alcance DHCP o el alcance creado para los clientes inalámbricos CorpNet.
17. Para probar la funcionalidad, abra un navegador y navegue hasta **http://10.0.10.10** (o la dirección IP del servidor de la CA).

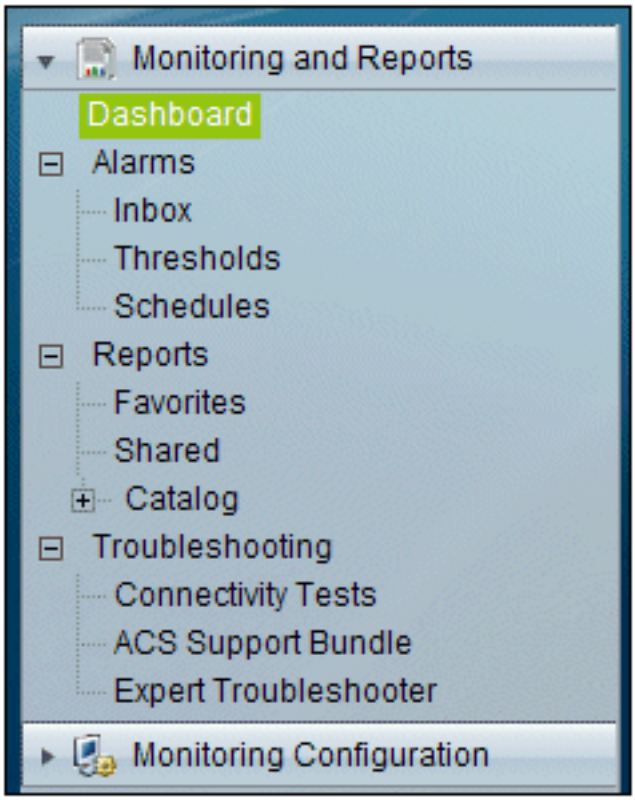
Troubleshooting de Autenticación Inalámbrica con ACS

Siga estos pasos:

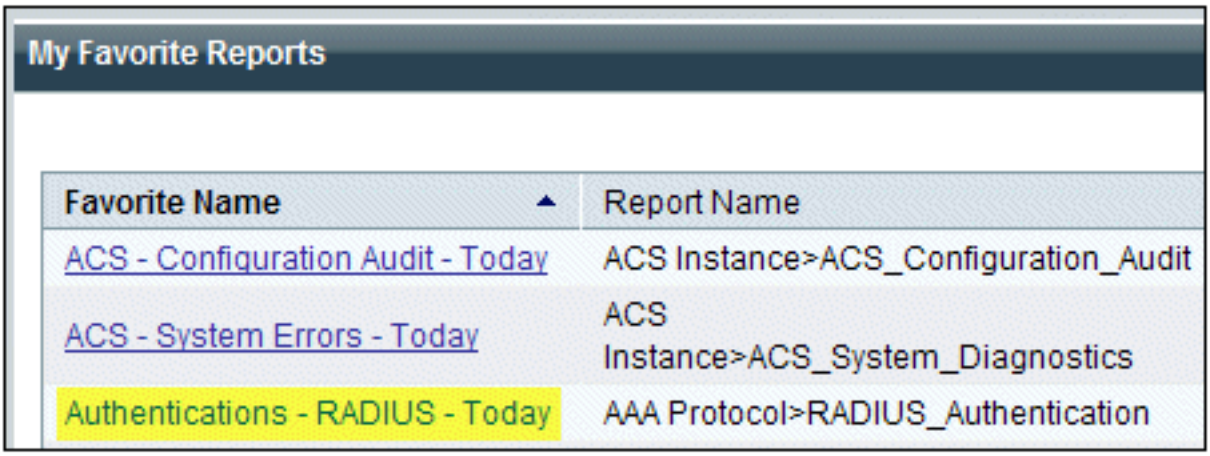
1. Vaya a **ACS > Supervisión e informes**, y haga clic en **Iniciar Supervisión y Visor de informes**.



2. Se abrirá una ventana ACS independiente. Haga clic en **Panel**.



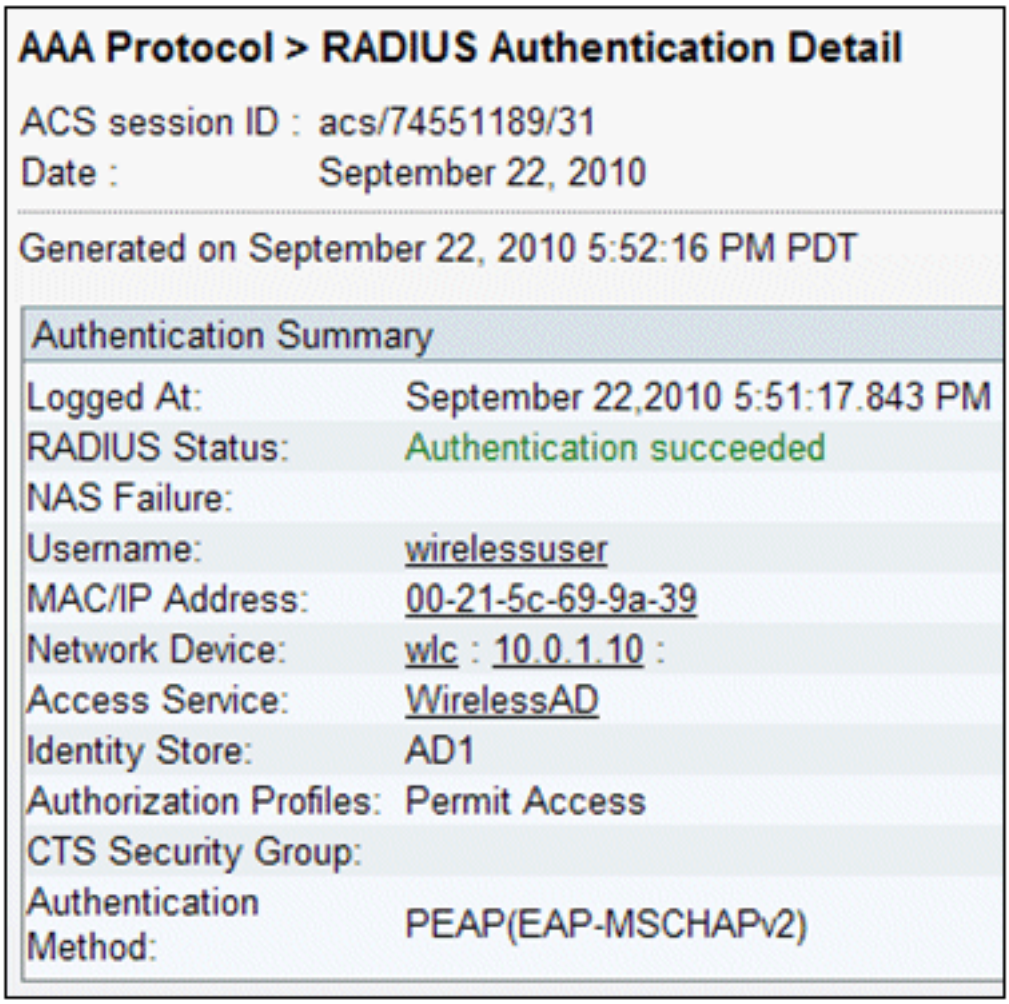
3. En la sección Mis informes favoritos, haga clic en **Autenticaciones - RADIUS -**



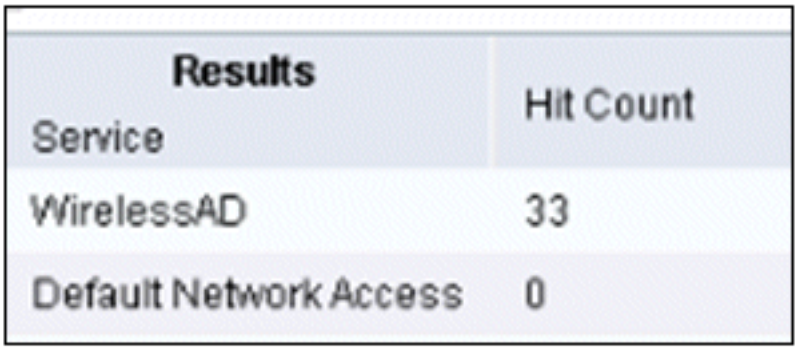
Hoy.

4. Un registro mostrará todas las autenticaciones RADIUS como Pass o Fail. Dentro de una entrada registrada, haga clic en el **icono de lupa** en la columna Detalles.

5. El detalle de autenticación RADIUS proporcionará mucha información sobre los intentos registrados.



6. El conteo de aciertos del servicio ACS puede proporcionar una descripción general de los intentos que coinciden con las reglas creadas en ACS. Vaya a **ACS > Access Policies > Access Services**, y haga clic en **Service Selection Rules**.



Results Service	Hit Count
WirelessAD	33
Default Network Access	0

Falla la autenticación PEAP con el servidor ACS

Cuando su cliente falle en la autenticación PEAP con un servidor ACS, verifique si encuentra el mensaje de error `NAS duplicate authentication try` en la opción **Intentos fallidos** en el menú **Informe y actividad** de ACS.

Es posible que reciba 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 IAS de Microsoft. En particular, el servidor RADIUS de Cisco (ACS) utiliza un método diferente para calcular el Id. de formato EAP-TLV (Extensible Authentication Protocol Type:Length:Value) que el que utiliza Windows XP. Microsoft ha identificado este defecto en el suplicante XP SP2.

Para obtener una revisión, póngase en contacto con Microsoft y consulte el artículo La autenticación PEAP no funciona correctamente cuando se conecta a un servidor RADIUS de terceros . El problema subyacente es que en el lado del cliente, con la utilidad de Windows, la opción de reconexión rápida está deshabilitada para PEAP de forma predeterminada. Sin embargo, esta opción está habilitada de forma predeterminada en el lado del servidor (ACS). Para resolver este problema, desmarque la opción Fast Reconnect en el servidor ACS (bajo Global System Options). También puede activar la opción Fast Reconnect en el lado del cliente para resolver el problema.

Realice estos pasos para habilitar la reconexión rápida en el cliente que ejecuta Windows XP con la utilidad de Windows:

1. Vaya a **Inicio > Configuración > Panel de control**.
2. Haga doble clic en el icono **Conexiones de red**.
3. Haga clic con el botón secundario en el icono **Conexión de red inalámbrica** y, a continuación, haga clic en **Propiedades**.
4. Haga clic en la ficha **Wireless Networks**.
5. Elija la opción **Use Windows to configure my wireless network settings** para habilitar Windows para configurar el adaptador del cliente.
6. Si ya ha configurado un SSID, elija el SSID y haga clic en **Properties**. Si no, haga clic en **Nuevo** para agregar una WLAN nueva.
7. Introduzca el SSID en la ficha Association (Asociación). Asegúrese de que Network Authentication (Autenticación de red) es **Open (Abierto)** y Data Encryption (Encriptación de datos) está configurado en **WEP**.

8. Haga clic en **Authentication**.
9. Elija la opción **Enable IEEE 802.1x authentication for this network**.
10. Elija **PEAP** como tipo de EAP y haga clic en **Properties**.
11. Elija la opción **Enable Fast Reconnect** en la parte inferior de la página.

Información Relacionada

- PEAP en Redes inalámbricas unificadas con ACS 4.0 y Windows 2003
- Ejemplo de Configuración de Cisco Wireless LAN Controller (WLC) y Cisco ACS 5.x (TACACS+) para la Autenticación Web
- Guía de instalación y actualización para Cisco Secure Access Control System 5.1
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).