PEAP bajo Redes Inalámbricas Unificadas con Microsoft Internet Authentication Service (IAS)

Contenido

Introducción

Este documento proporciona un ejemplo de configuración para configurar Protected Extensible Authentication Protocol (PEAP) mediante la autenticación MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) versión 2 en una red Cisco Unified Wireless con el Servicio de autenticación de Internet de Microsoft (IAS) como servidor RADIUS.

Prerequisites

Requirements

Se asume que el lector 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.

Nota: Este documento pretende dar a los lectores un ejemplo sobre la configuración requerida en el servidor MS para la autenticación PEAP - MS CHAP. La configuración del servidor de Microsoft presentada en esta sección se ha probado en el laboratorio y funciona según lo esperado. Si tiene problemas para configurar el servidor de Microsoft, póngase en contacto con Microsoft para obtener ayuda. Cisco TAC no admite la configuración del servidor de Microsoft Windows.

Para obtener información sobre la configuración e instalación inicial de los Cisco 4400 Series Controllers, consulte la Guía de inicio rápido: Cisco 4400 Series Wireless LAN Controllers.

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.

Componentes Utilizados

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

- Cisco 4400 Series Controller que ejecuta firmware versión 4.0
- Punto de acceso de protocolo de punto de acceso ligero (LWAPP) Cisco 1131
- Windows 2003 Enterprise Server (SP1) con los servicios Internet Authentication Service (IAS), Certificate Authority (CA), DHCP y Domain Name System (DNS) instalados
- Windows XP Professional con SP2 (y Service Packs actualizados) y tarjeta de interfaz de red inalámbrica (NIC) Cisco Aironet 802.11a/b/g
- Aironet Desktop Utility Versión 4.0
- Switch Cisco 3560

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.

Descripción general de PEAP

PEAP utiliza la Seguridad de nivel de transporte (TLS) para crear un canal cifrado entre un cliente PEAP de autenticación, como un equipo portátil inalámbrico, y un autenticador PEAP, como el

Servicio de autenticación de Internet de Microsoft (IAS) o cualquier servidor RADIUS. PEAP no especifica un método de autenticación, pero proporciona seguridad adicional para otros protocolos de autenticación EAP, como EAP-MSCHAPv2, que pueden funcionar a través del canal cifrado TLS proporcionado por PEAP. El proceso de autenticación PEAP consta de dos fases principales:

PEAP fase uno: canal cifrado TLS

El cliente inalámbrico se asocia con el AP. Una asociación basada en IEEE 802.11 proporciona una autenticación de sistema abierto o clave compartida antes de crear una asociación segura entre el cliente y el punto de acceso (LAP). Después de que la asociación basada en IEEE 802.11 se establezca con éxito entre el cliente y el punto de acceso, la sesión TLS se negocia con el AP. Una vez completada correctamente la autenticación entre el cliente inalámbrico y el servidor IAS, la sesión TLS se negocia entre ellos. La clave derivada en esta negociación se utiliza para cifrar todas las comunicaciones posteriores.

Fase dos de PEAP: comunicación autenticada mediante EAP

La comunicación EAP, que incluye la negociación EAP, se produce dentro del canal TLS creado por PEAP dentro de la primera etapa del proceso de autenticación PEAP. El servidor IAS autentica el cliente inalámbrico con EAP-MS-CHAP v2. El LAP y el controlador sólo reenvían mensajes entre el cliente inalámbrico y el servidor RADIUS. El WLC y el LAP no pueden descifrar estos mensajes porque no es el punto final de TLS.

Después de que se produzca la primera etapa de PEAP y se cree el canal TLS entre el servidor IAS y el cliente inalámbrico 802.1X, para un intento de autenticación correcto en el que el usuario haya proporcionado credenciales válidas basadas en contraseña con PEAP-MS-CHAP v2, la secuencia de mensajes RADIUS es la siguiente:

1. El servidor IAS envía un mensaje de solicitud de identidad al cliente: EAP-Request/Identity.
2. El cliente responde con un mensaje de respuesta de identidad: EAP-Response/Identity.
3. El servidor IAS envía un mensaje de desafío MS-CHAP v2: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Challenge).
4. El cliente responde con un desafío y una respuesta MS-CHAP v2: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. El servidor IAS devuelve un paquete correcto MS-CHAP v2 cuando el servidor ha autenticado correctamente el cliente: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (correcto).
6. El cliente responde con un paquete de éxito MS-CHAP v2 cuando el cliente ha autenticado correctamente el servidor: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (correcto).
7. El servidor IAS envía un EAP-TLV que indica una autenticación correcta.
8. El cliente responde con un mensaje de estado de éxito EAP-TLV.
9. El servidor completa la autenticación y envía un mensaje EAP-Success usando texto sin formato. Si las VLAN se implementan para el aislamiento del cliente, los atributos de VLAN se incluyen en este mensaje.

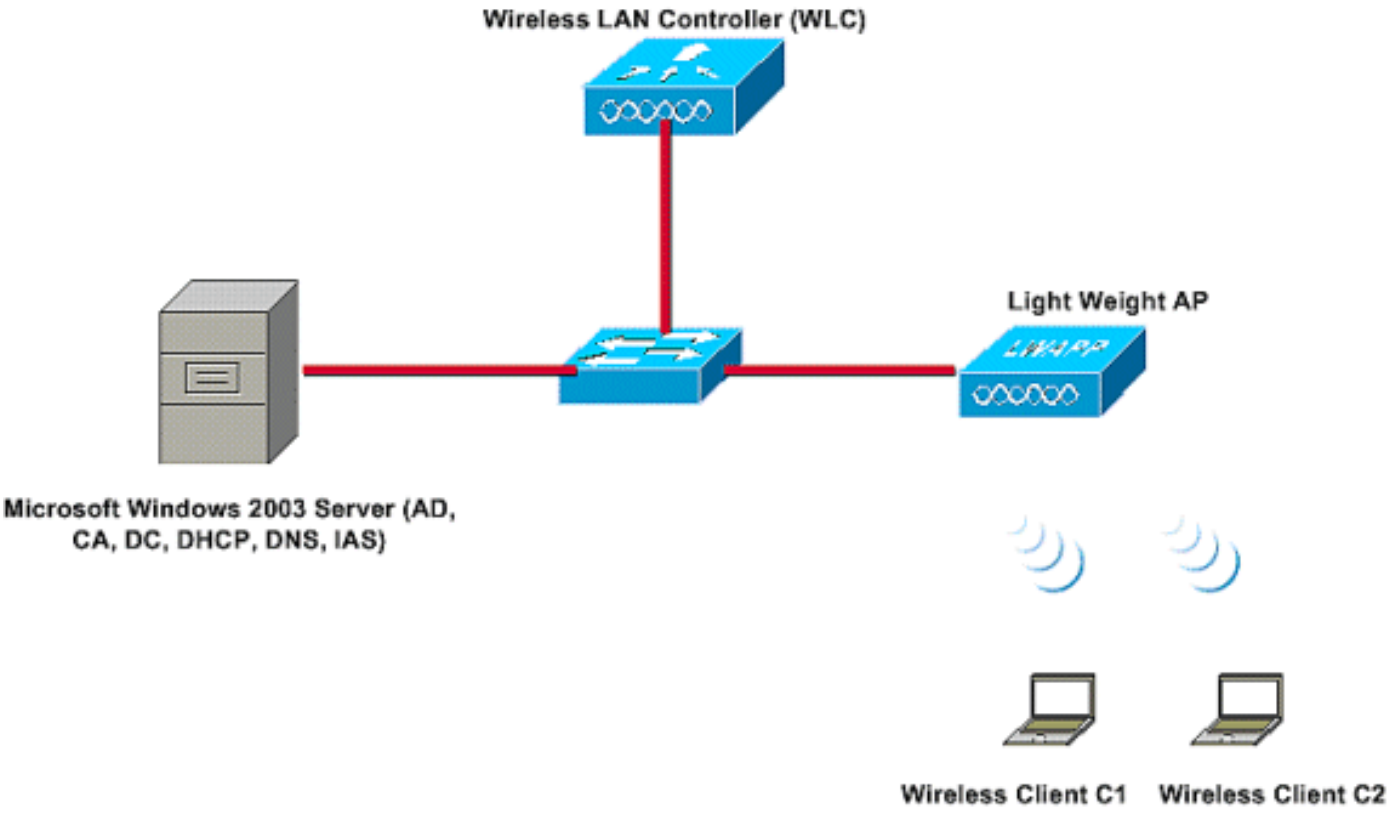
Configurar

Este documento proporciona un ejemplo para la configuración de PEAP MS-CHAP v2.

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:



En esta instalación, un servidor de Microsoft Windows 2003 realiza estas funciones:

- Controlador de dominio para el dominio **Wireless.com**
- Servidor DHCP/DNS
- Servidor de autoridad certificadora (CA)
- Active Directory: para mantener la base de datos de usuarios
- Internet Authentication Service (IAS): para autenticar a los usuarios inalámbricos

Este servidor se conecta a la red con cables a través de un switch de capa 2, como se muestra en la imagen.

El controlador de LAN inalámbrica (WLC) y el LAP registrado también se conectan a la red a través del switch de capa 2.

Los clientes inalámbricos C1 y C2 utilizarán autenticación PEAP MSCHAP v2 (acceso Wi-Fi protegido 2, WPA2) para conectarse a la red inalámbrica.

El objetivo es configurar el servidor de Microsoft 2003, el controlador de LAN inalámbrica y el punto de acceso ligero para autenticar los clientes inalámbricos con autenticación PEAP MSCHAP v2.

En la siguiente sección se explica cómo configurar los dispositivos para esta configuración.

Configuraciones

Esta sección analiza la configuración necesaria para configurar la autenticación PEAP MS-CHAP v2 en esta WLAN:

- Configuración de Microsoft Windows 2003 Server
- Configuración del controlador de LAN inalámbrica (WLC) y los puntos de acceso ligeros
- Configuración de los clientes inalámbricos

Comience con la configuración del servidor de Microsoft Windows 2003.

Configuración de Microsoft Windows 2003 Server

Configuración de Microsoft Windows 2003 Server

Como se ha mencionado en la sección Configuración de red, utilice el servidor de Microsoft Windows 2003 en la red para realizar estas funciones.

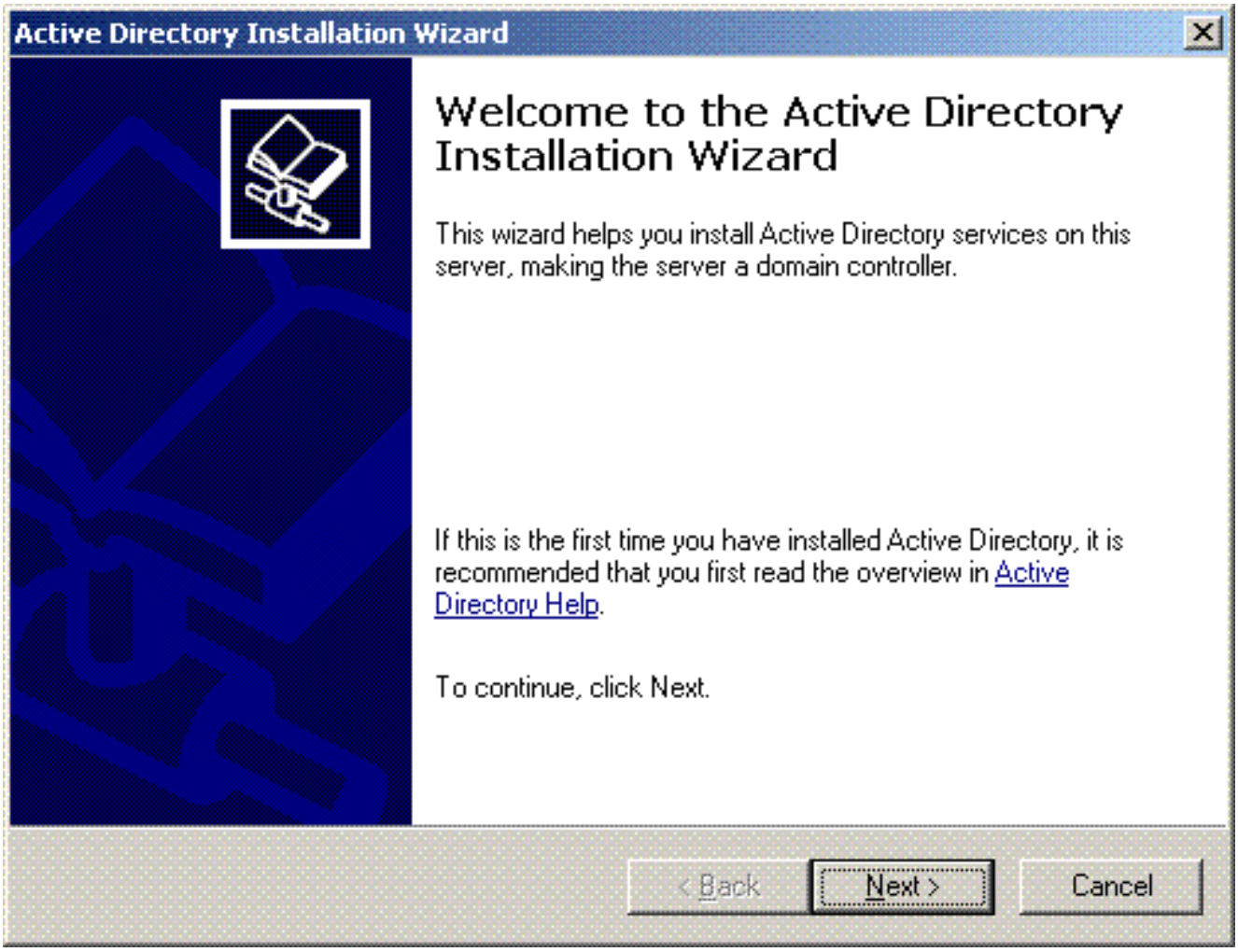
- **Controlador de dominio**: para el dominio **inalámbrico**
- **Servidor DHCP/DNS**
- **Servidor de autoridad certificadora (CA)**
- **Internet Authentication Service (IAS)**: para autenticar a los usuarios inalámbricos
- **Active Directory**: para mantener la base de datos de usuarios

Configure el servidor de Microsoft Windows 2003 para estos servicios. Comience con la configuración del servidor de Microsoft Windows 2003 como controlador de dominio.

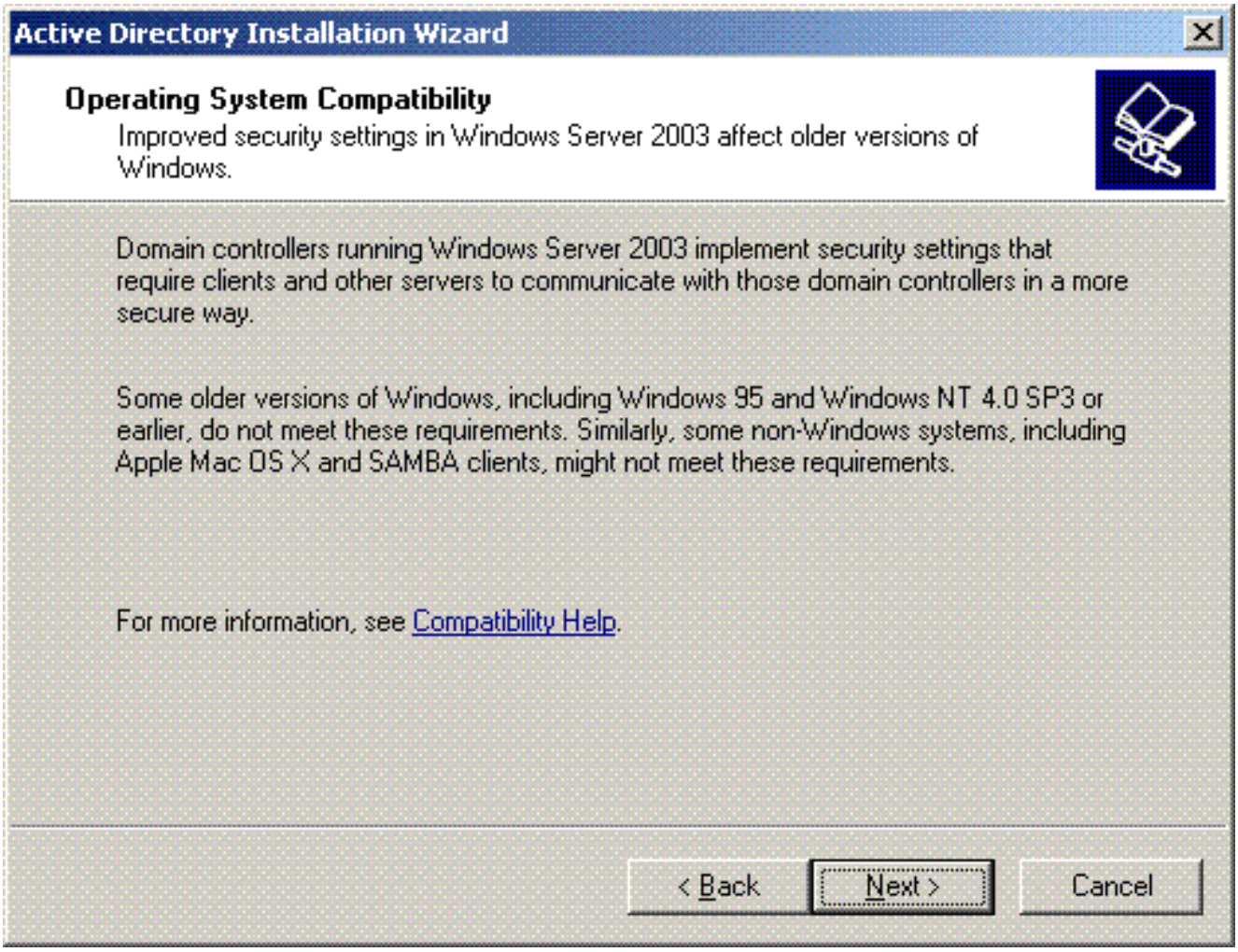
Configurar el servidor de Microsoft Windows 2003 como controlador de dominio

Para configurar el servidor de Microsoft Windows 2003 como controlador de dominio, siga estos pasos:

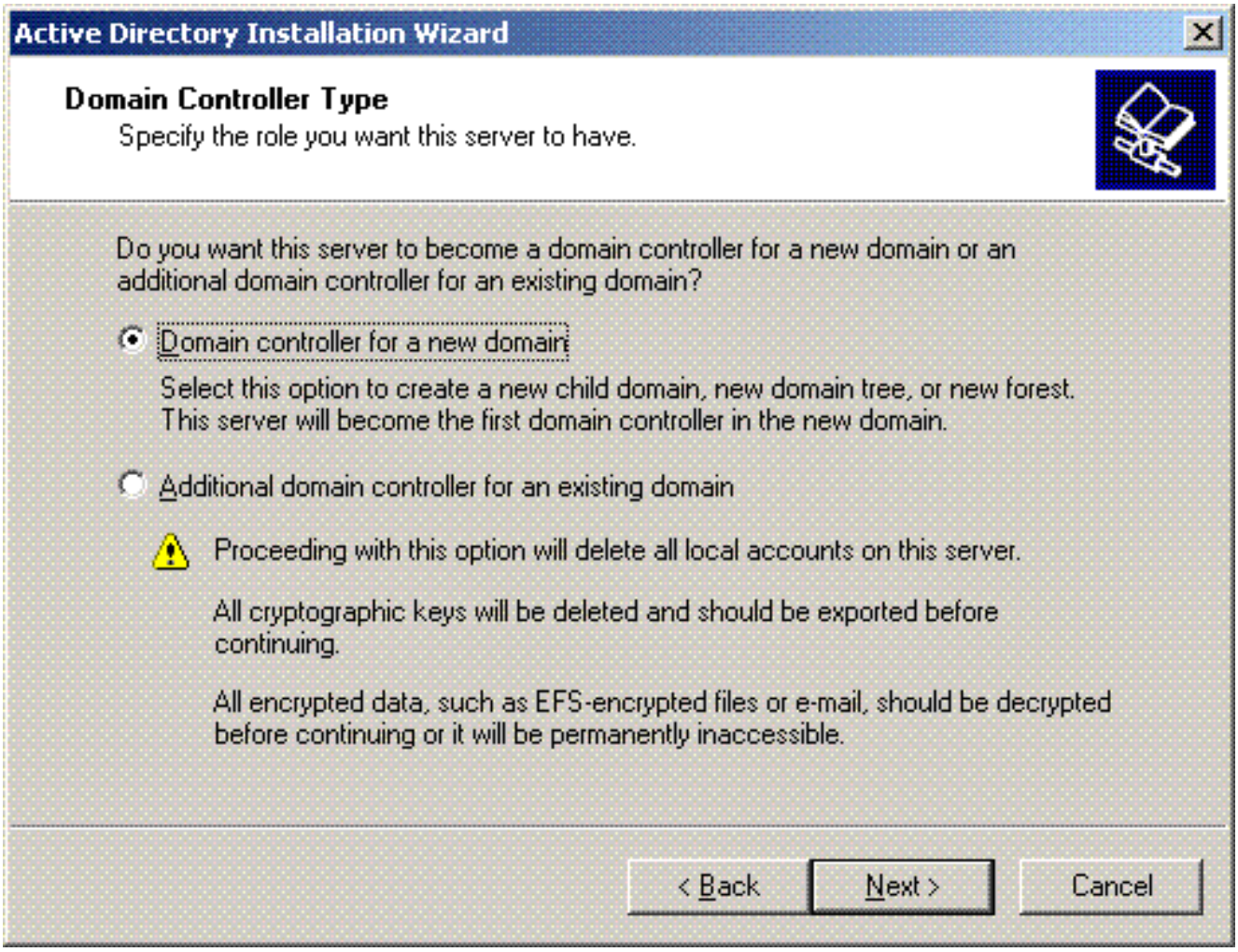
1. Haga clic en **Inicio**, haga clic en **Ejecutar**, escriba **dcpromo.exe** y, a continuación, haga clic en **Aceptar** para iniciar el Asistente para instalación de Active Directory.



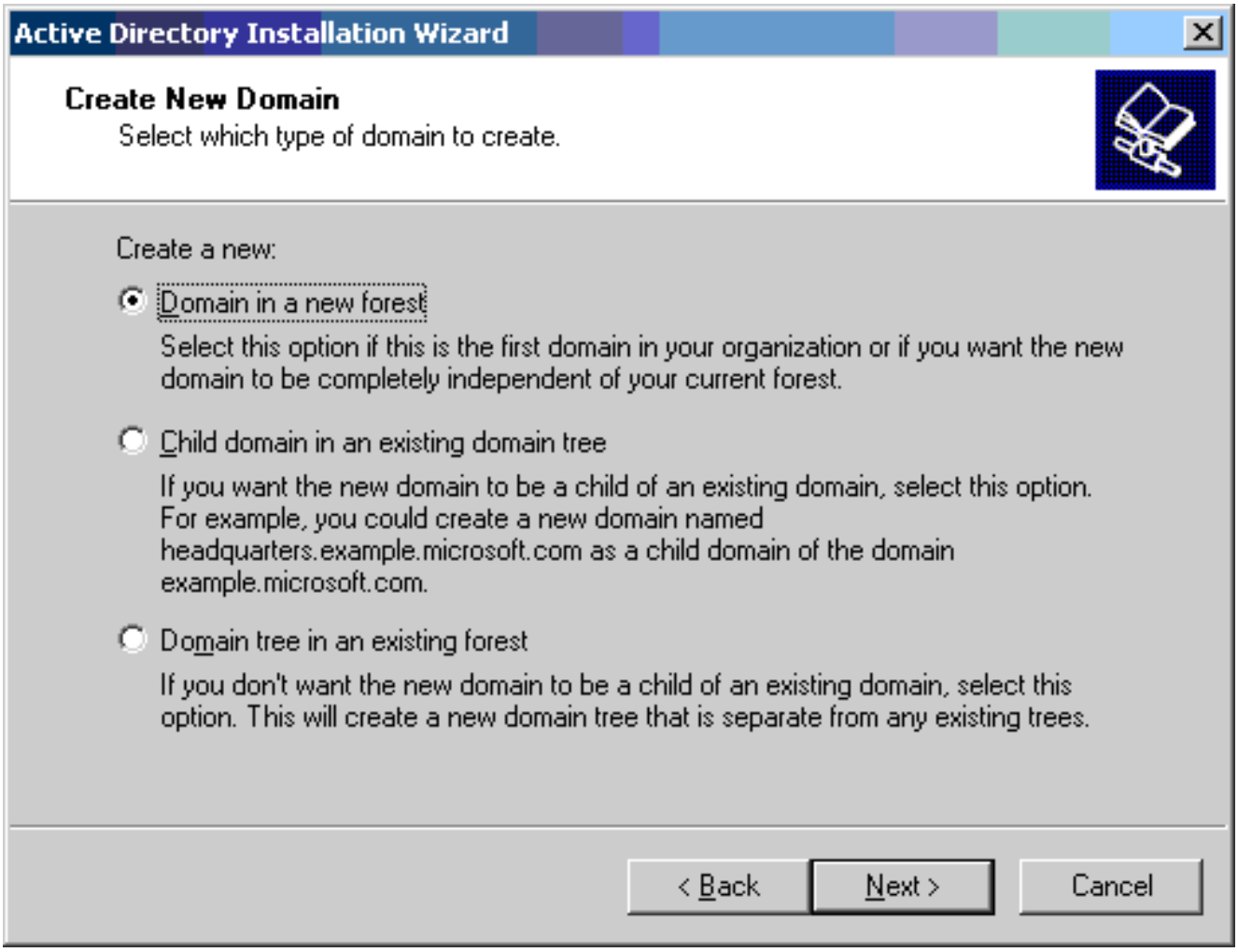
2. Haga clic en **Siguiente** para ejecutar el Asistente para instalación de Active Directory.



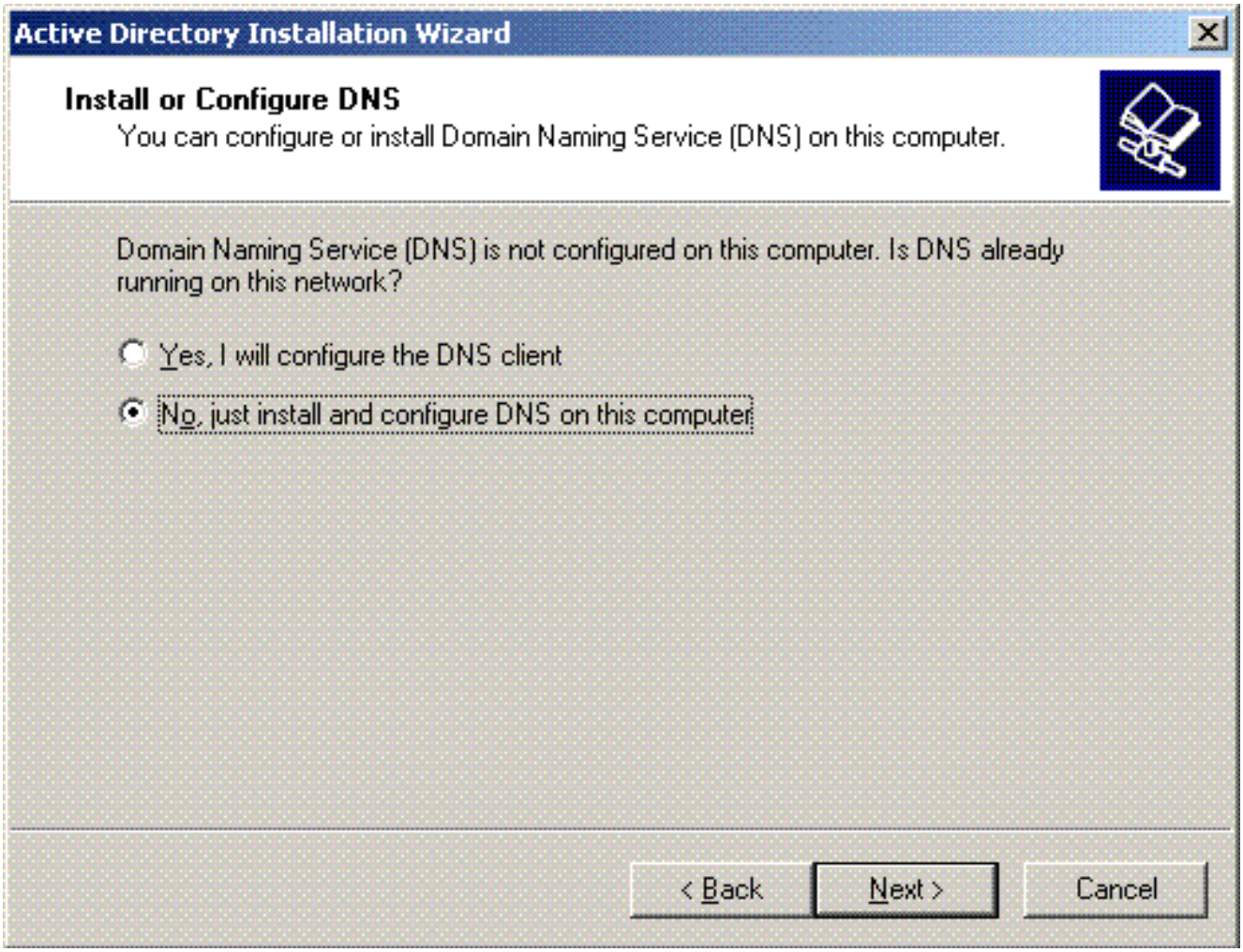
3. Para crear un nuevo dominio, elija la opción **Domain Controller** para un nuevo dominio.



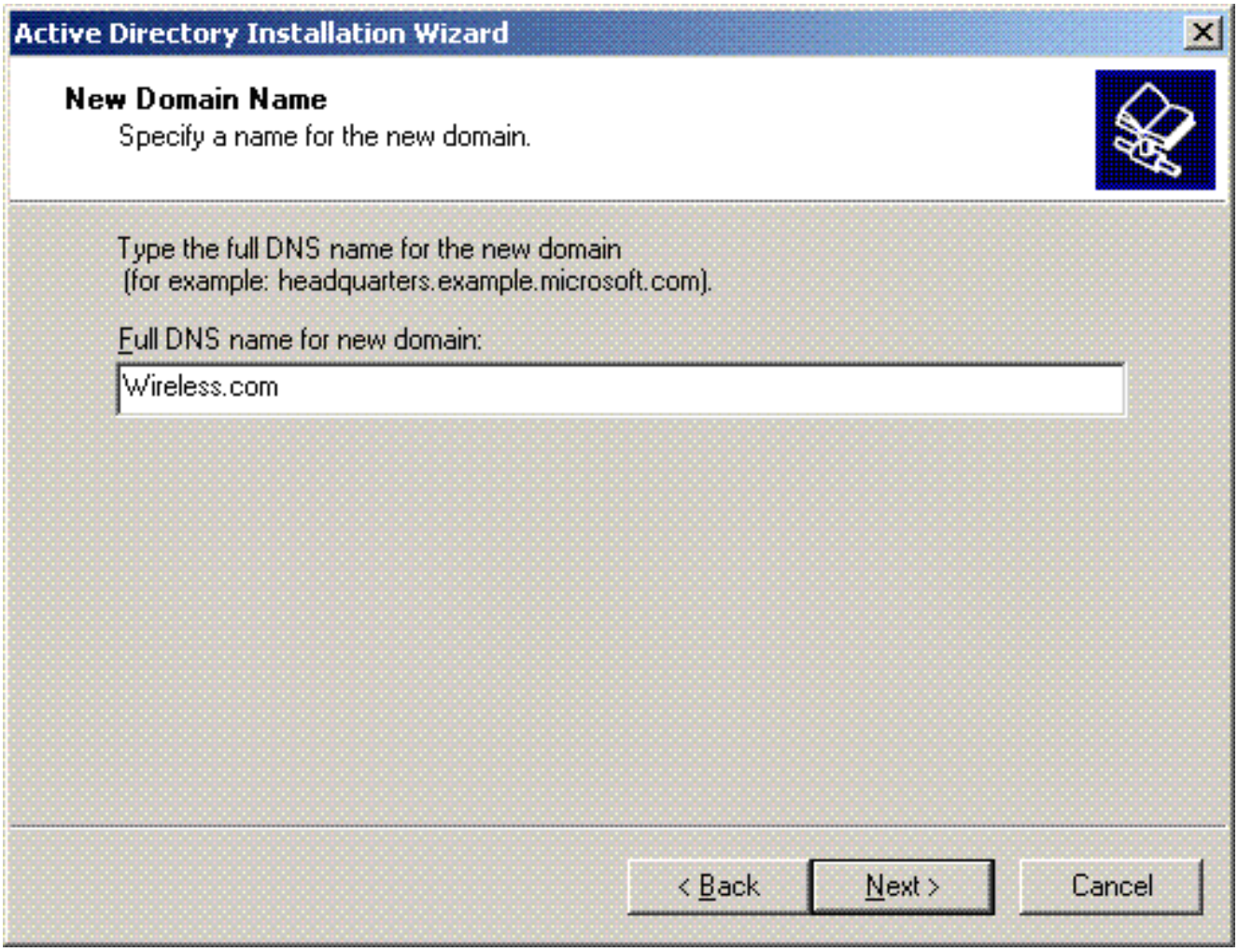
4. Haga clic en **Siguiente** para crear un nuevo bosque de árboles de dominio.



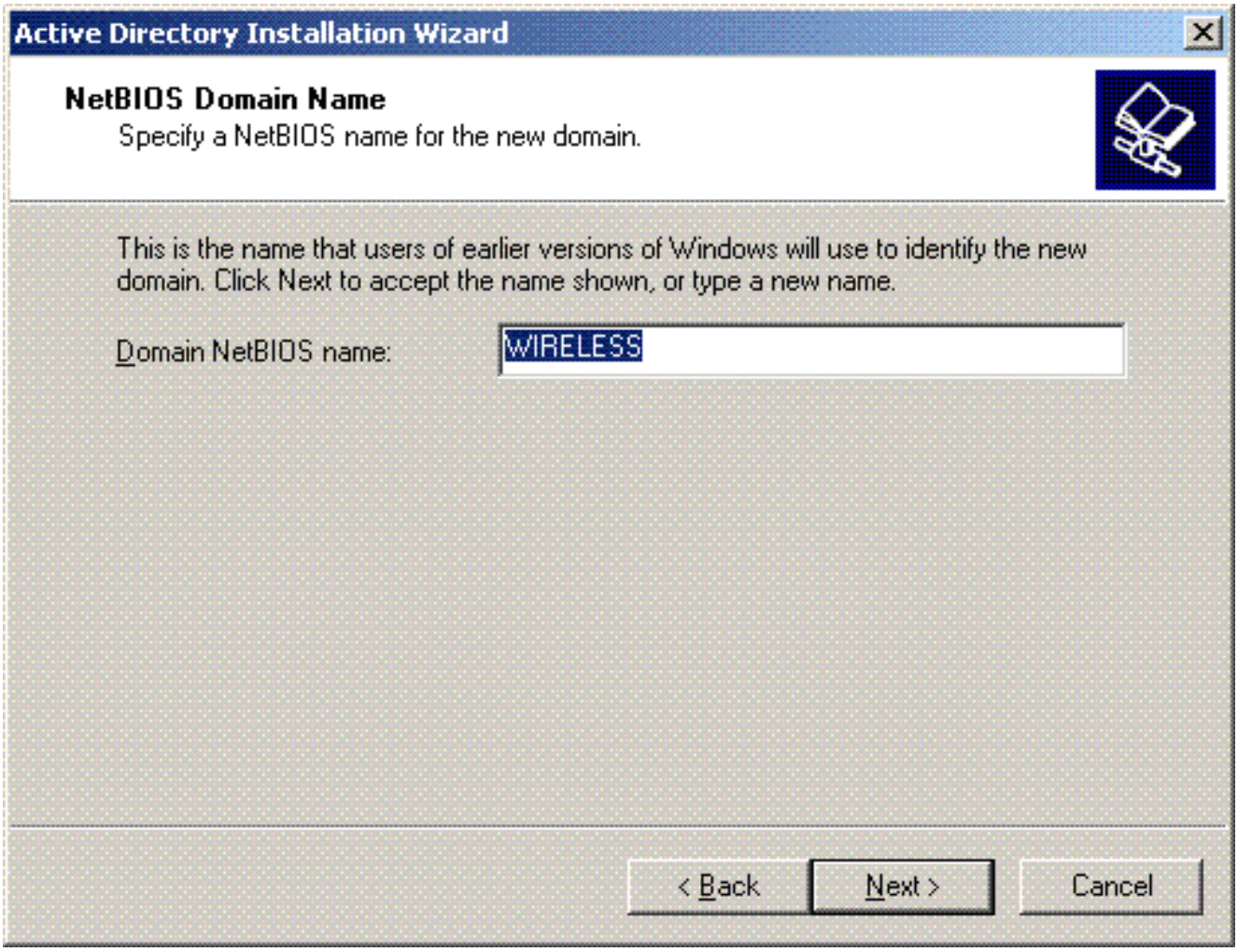
5. Si DNS no está instalado en el sistema, el asistente le proporciona opciones para configurar DNS. Elija **No, Just Install and Configure DNS** en este equipo. Haga clic en Next (Siguiente).



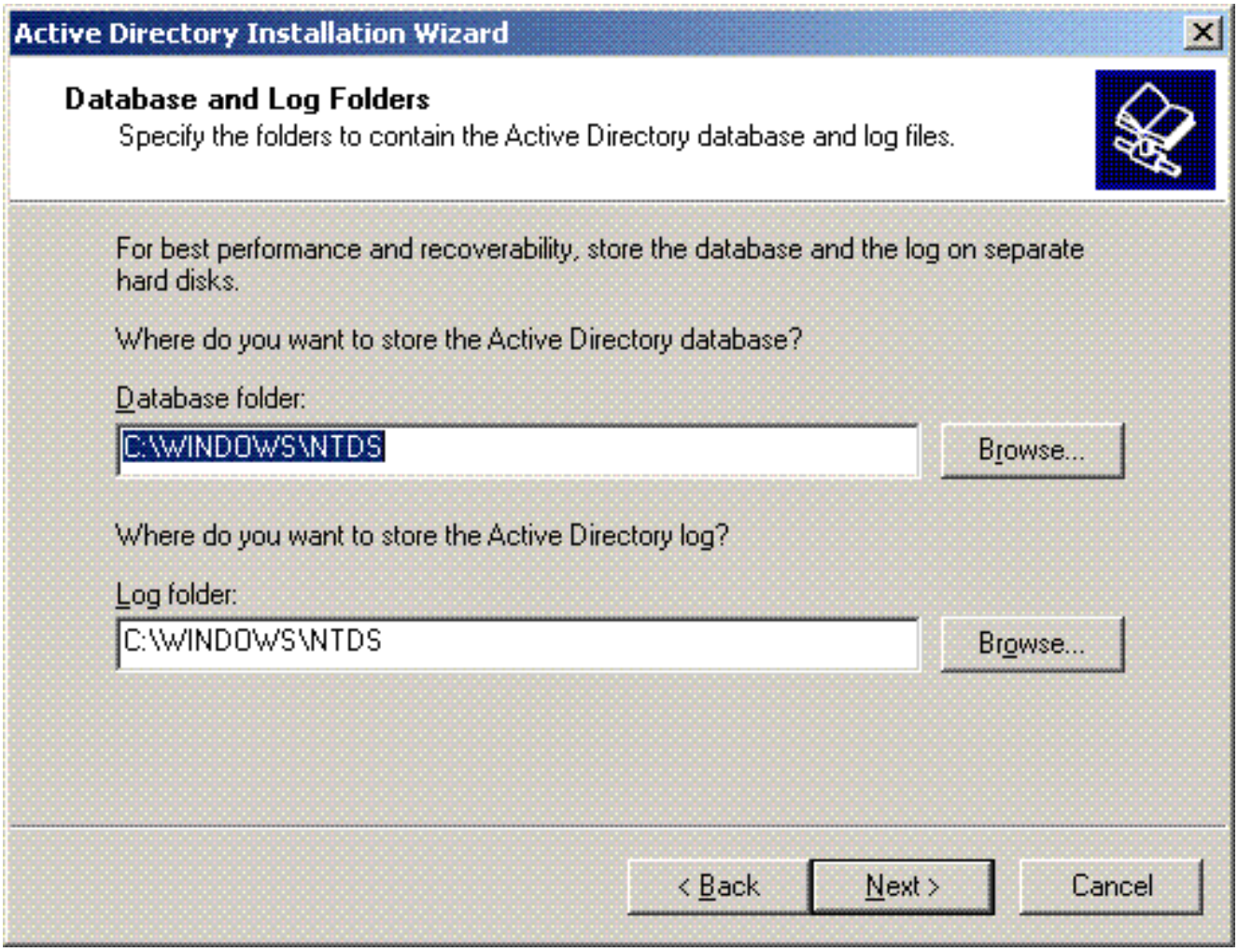
6. Escriba el nombre DNS completo del nuevo dominio. En este ejemplo, se utiliza **Wireless.com** y haga clic en **Next**.



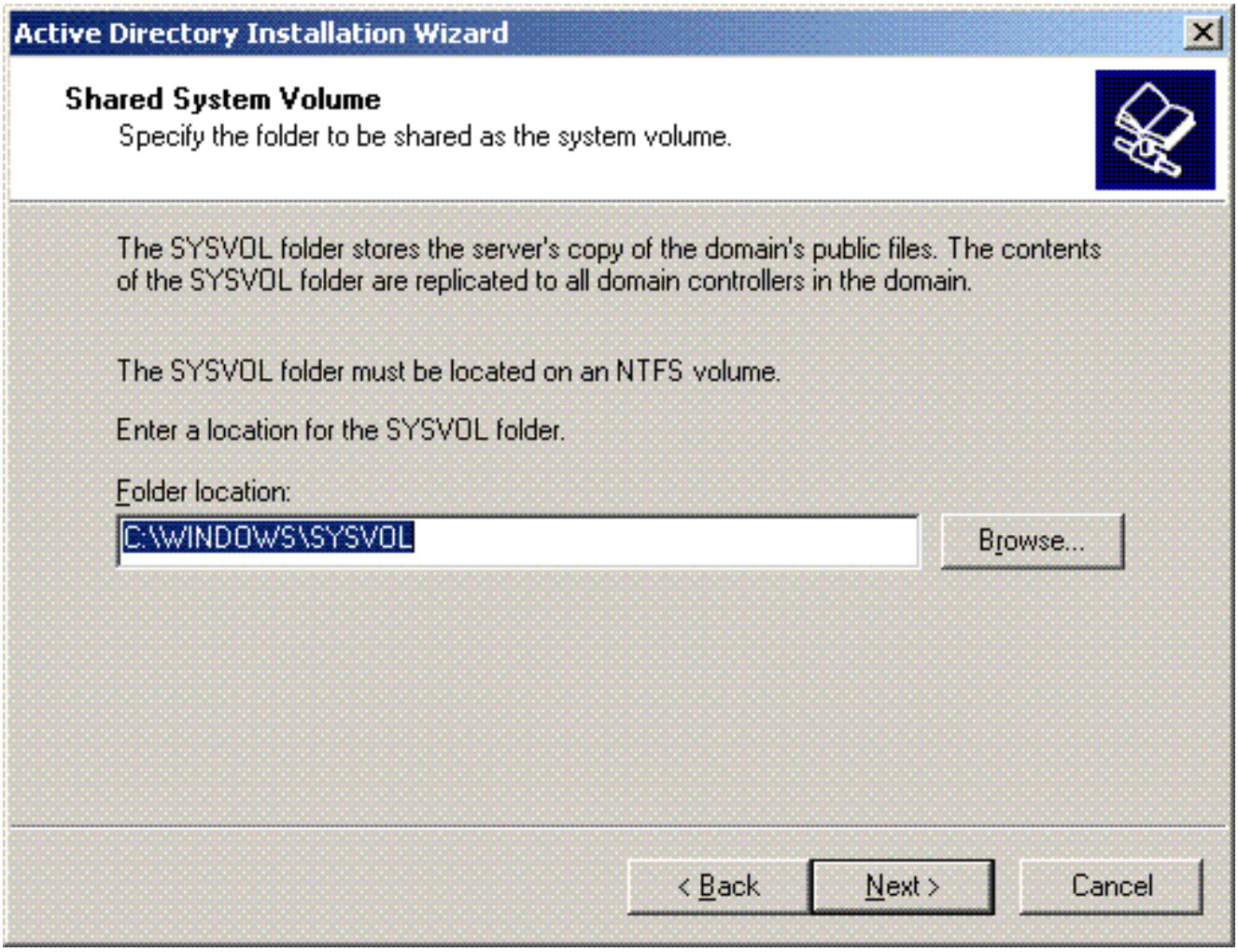
7. Ingrese el nombre NETBIOS para el dominio y haga clic en **Next**. Este ejemplo utiliza **WIRELESS**.



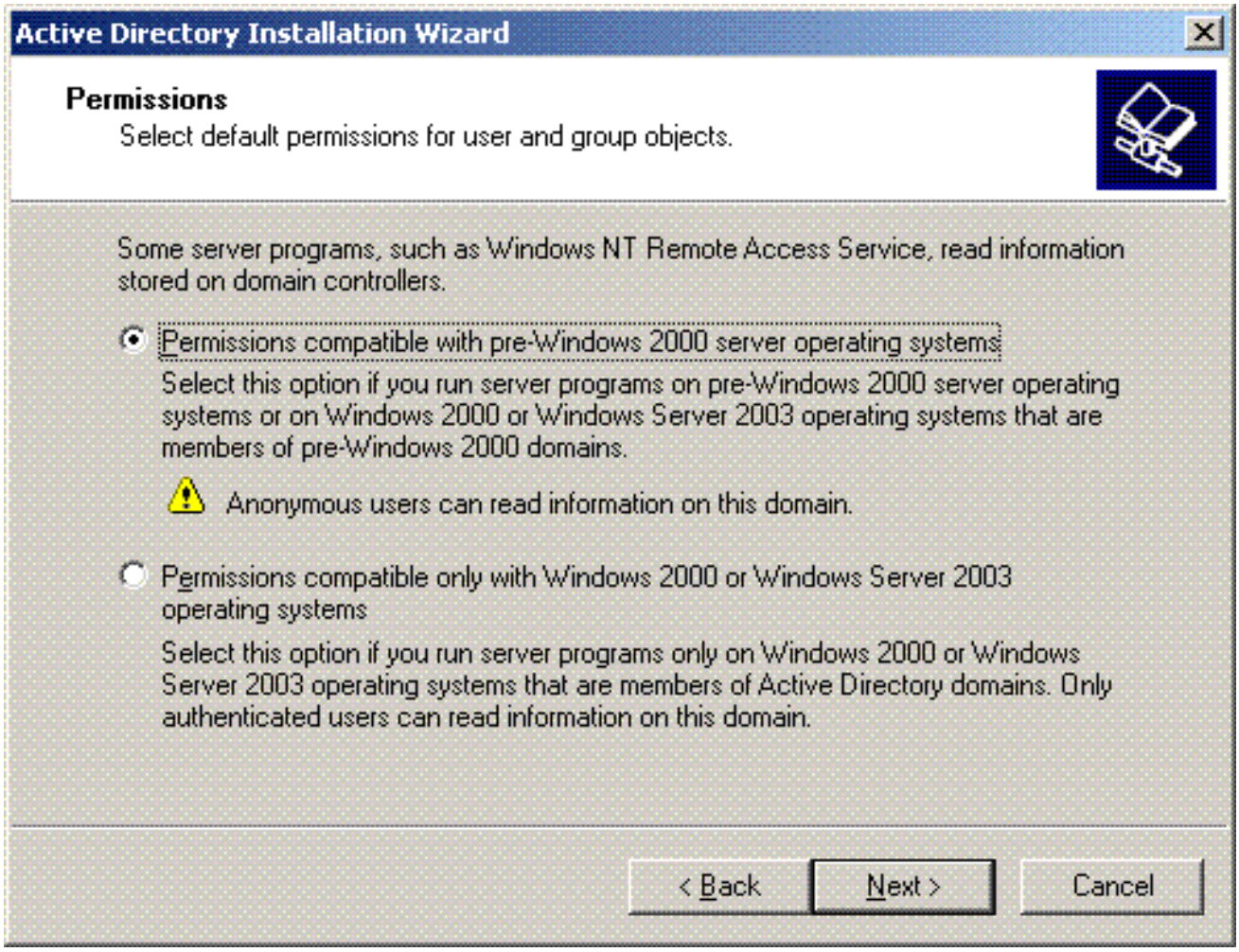
8. Elija las ubicaciones de la base de datos y del registro para el dominio. Haga clic en Next (Siguiente).



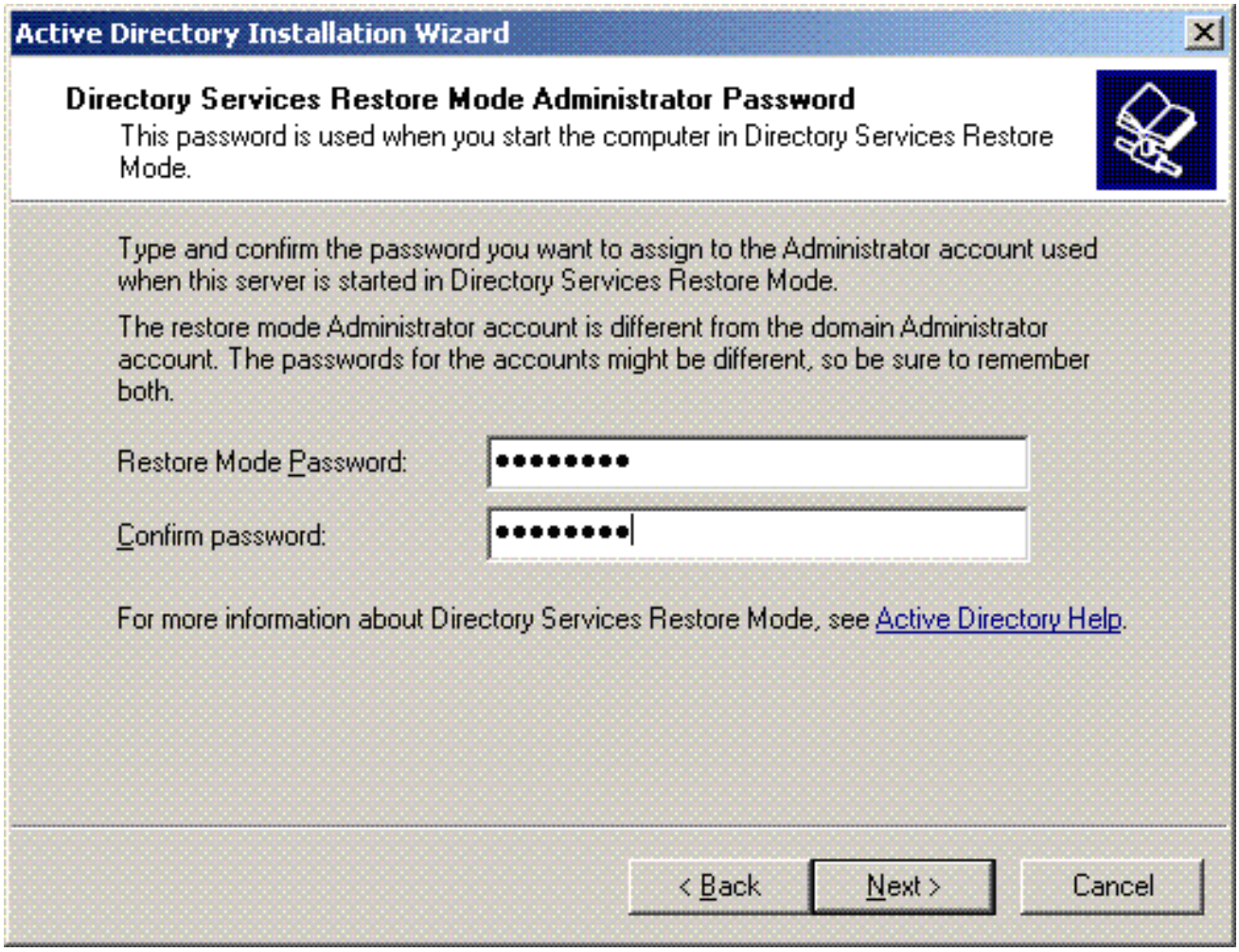
9. Elija una ubicación para la carpeta Sysvol. Haga clic en Next (Siguiente).



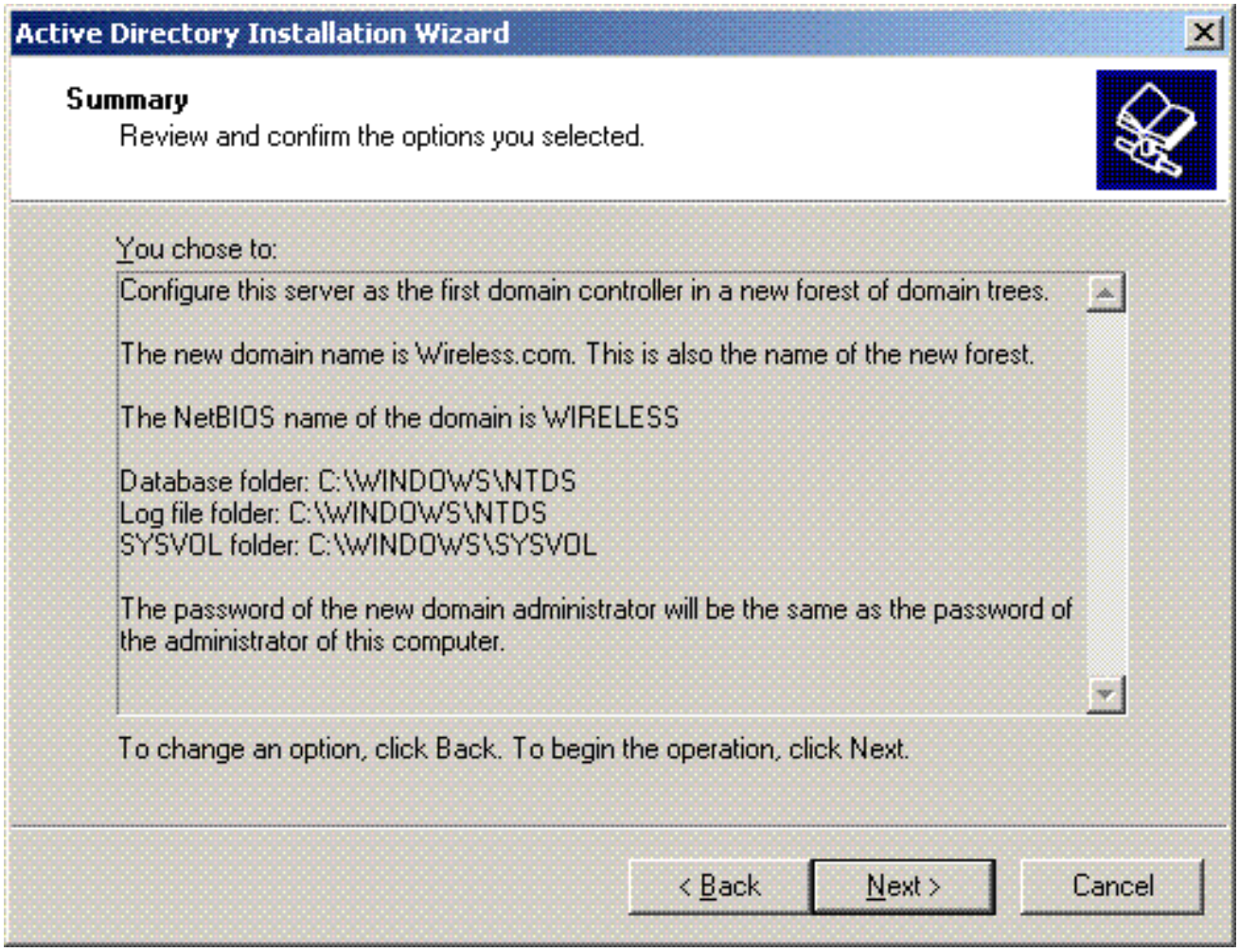
10. Elija los permisos predeterminados para los usuarios y grupos. Haga clic en Next (Siguiente).



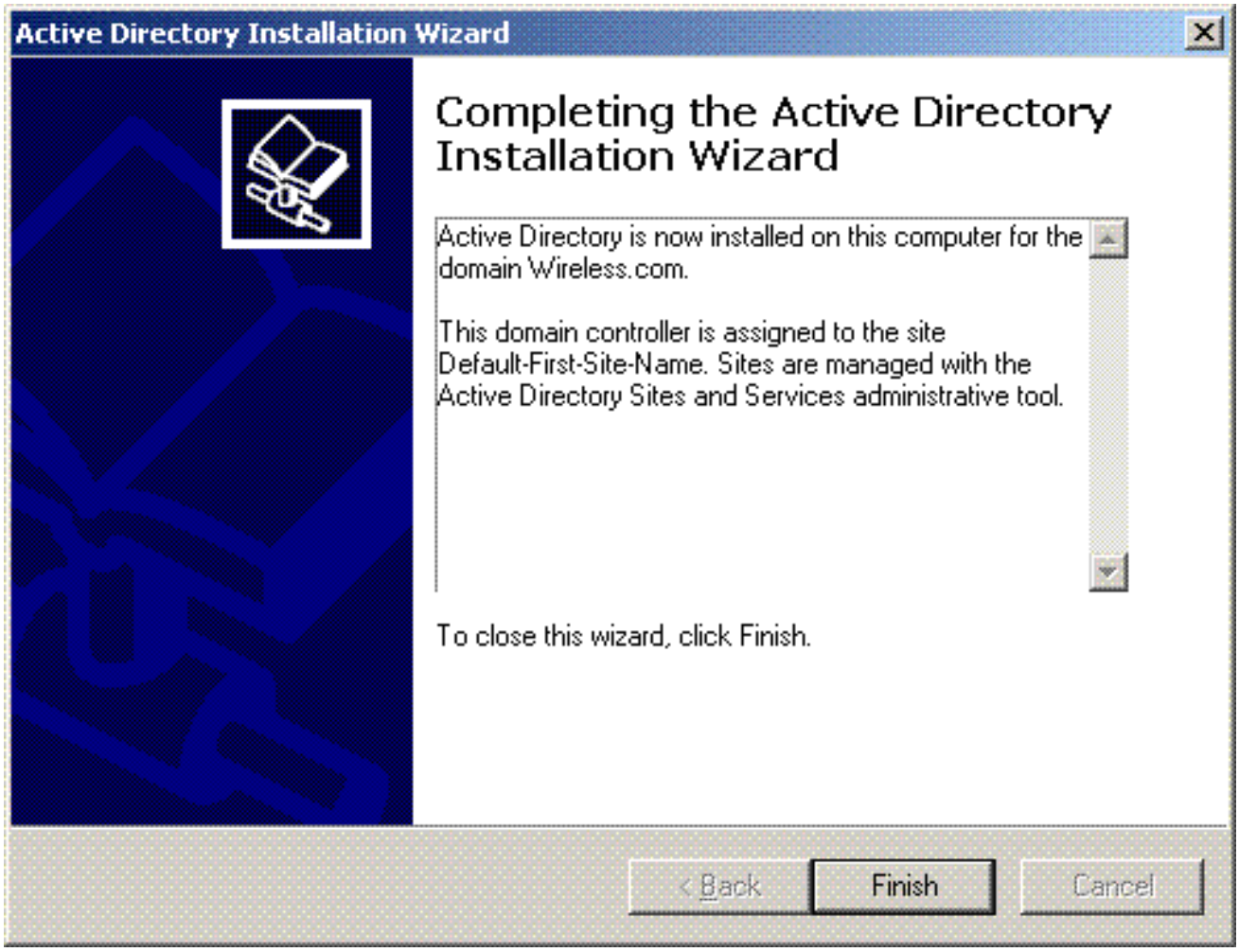
11. Establezca la contraseña de administrador y haga clic en **Next**.



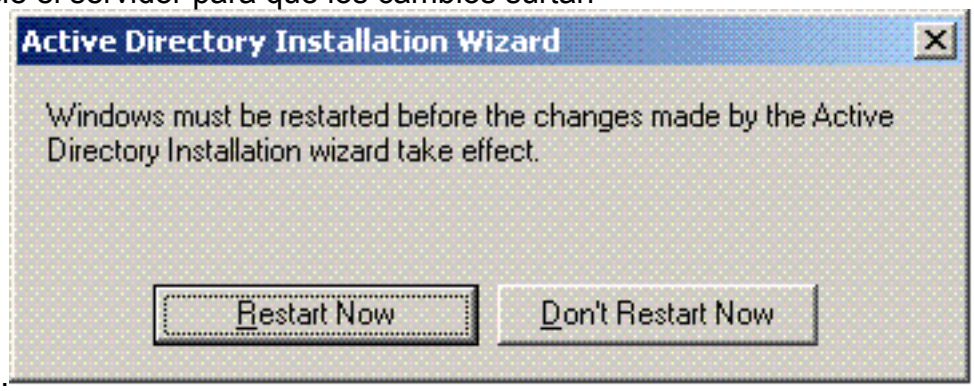
12. Haga clic en **Next** para aceptar el conjunto de opciones de dominio previamente establecido.



13. Haga clic en **Finalizar** para cerrar el Asistente para instalación de Active Directory.



14. Reinicie el servidor para que los cambios surtan efecto.

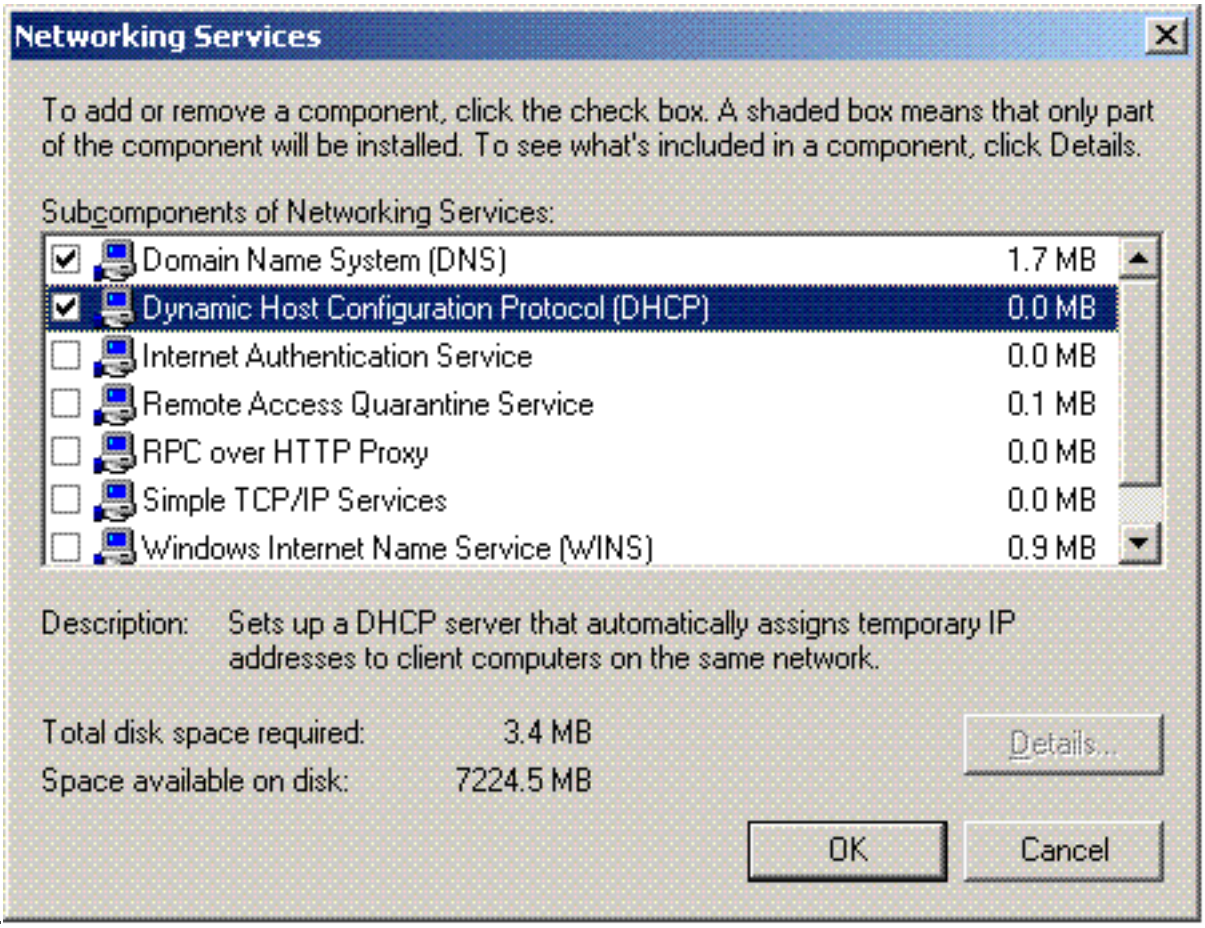


Con este paso, ha configurado el servidor de Microsoft Windows 2003 como controlador de dominio y ha creado un nuevo dominio **Wireless.com**. A continuación, configure los servicios DHCP en el servidor.

Instalar y configurar servicios DHCP en Microsoft Windows 2003 Server

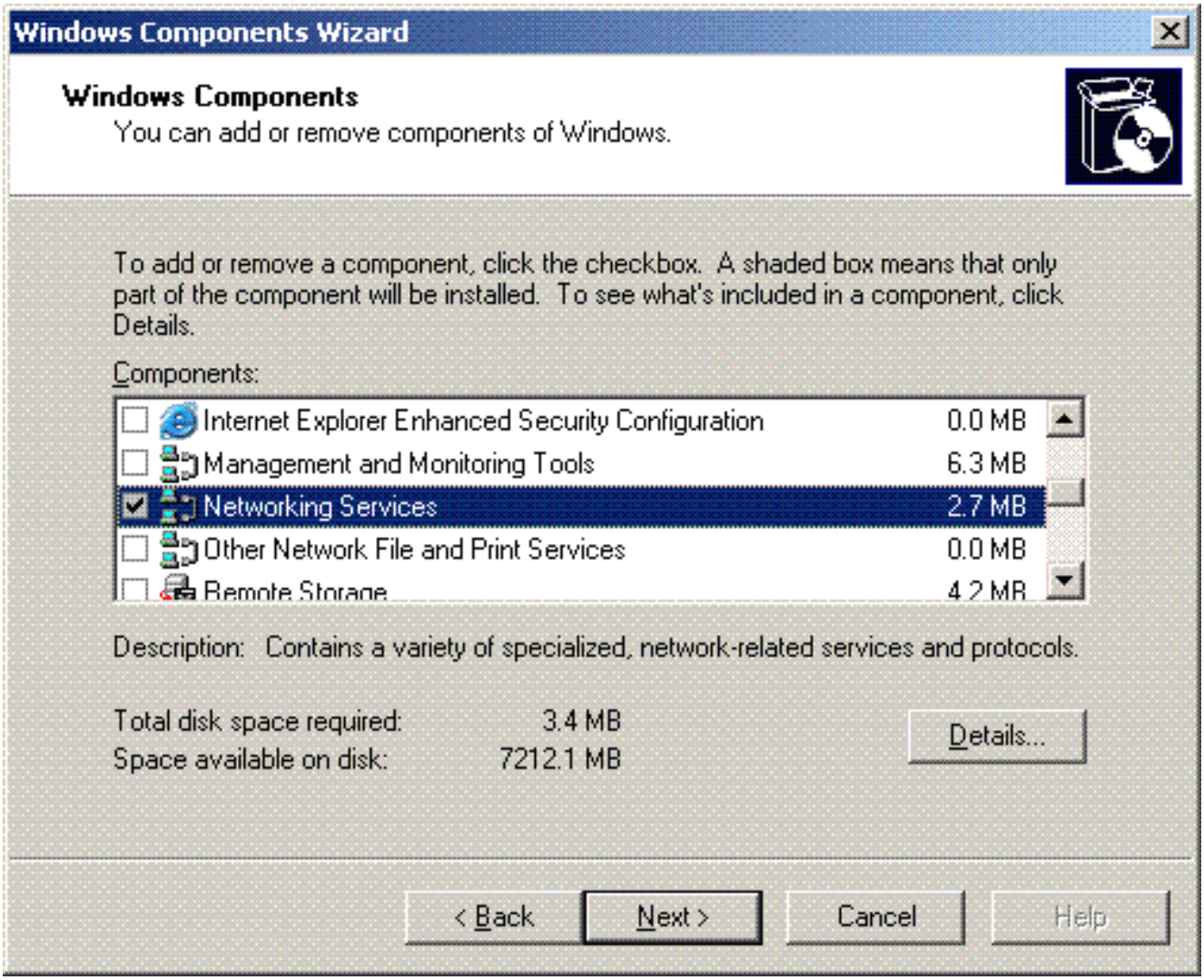
El servicio DHCP del servidor Microsoft 2003 se utiliza para proporcionar direcciones IP a los clientes inalámbricos. Para instalar y configurar los servicios DHCP en este servidor, complete estos pasos:

1. Haga clic en **Agregar o quitar programas** en el Panel de control.
2. Haga clic en **Agregar o quitar componentes de Windows**.
3. Elija **Networking Services** y haga clic en **Details**.
4. Elija **Dynamic Host Configuration Protocol (DHCP)** y haga clic en

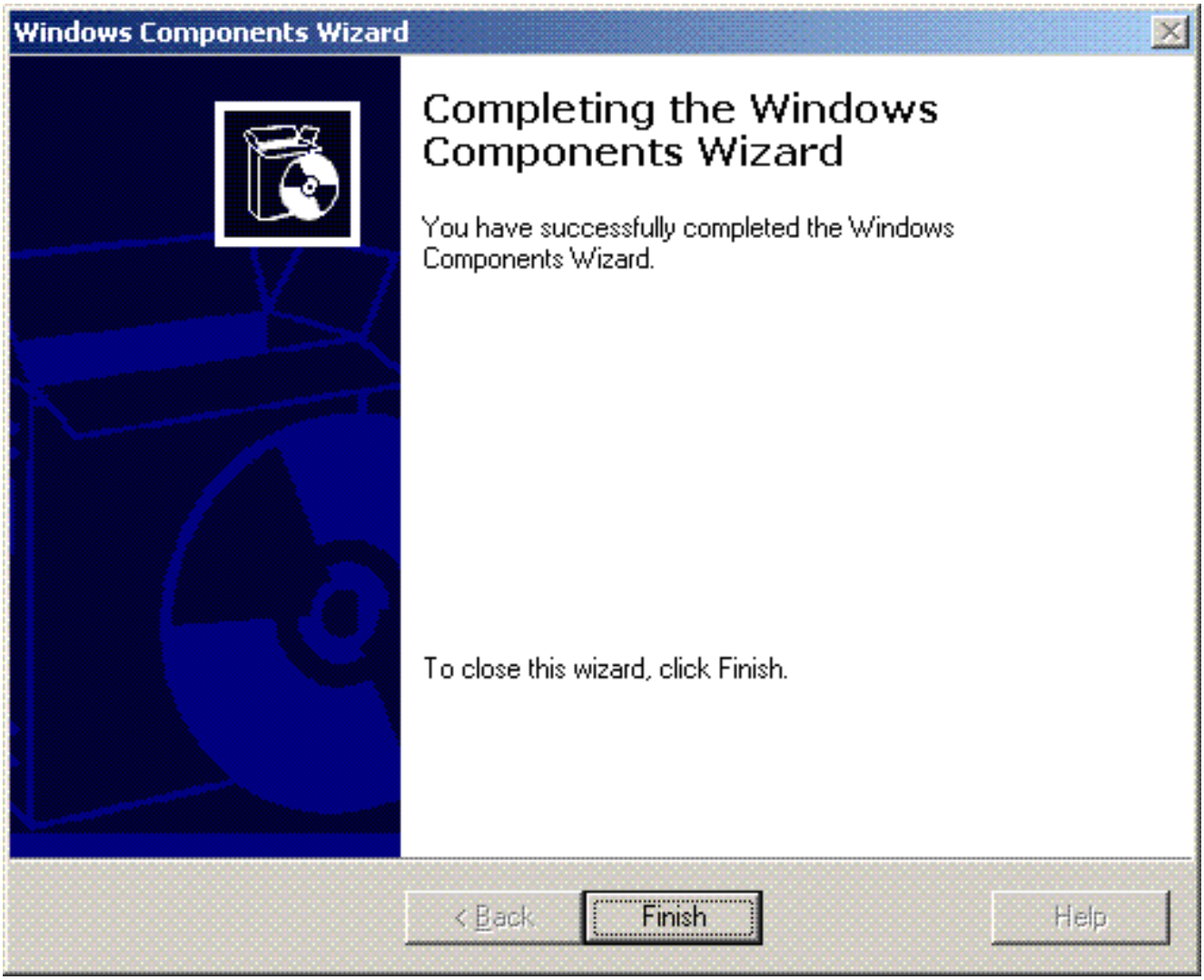


OK.

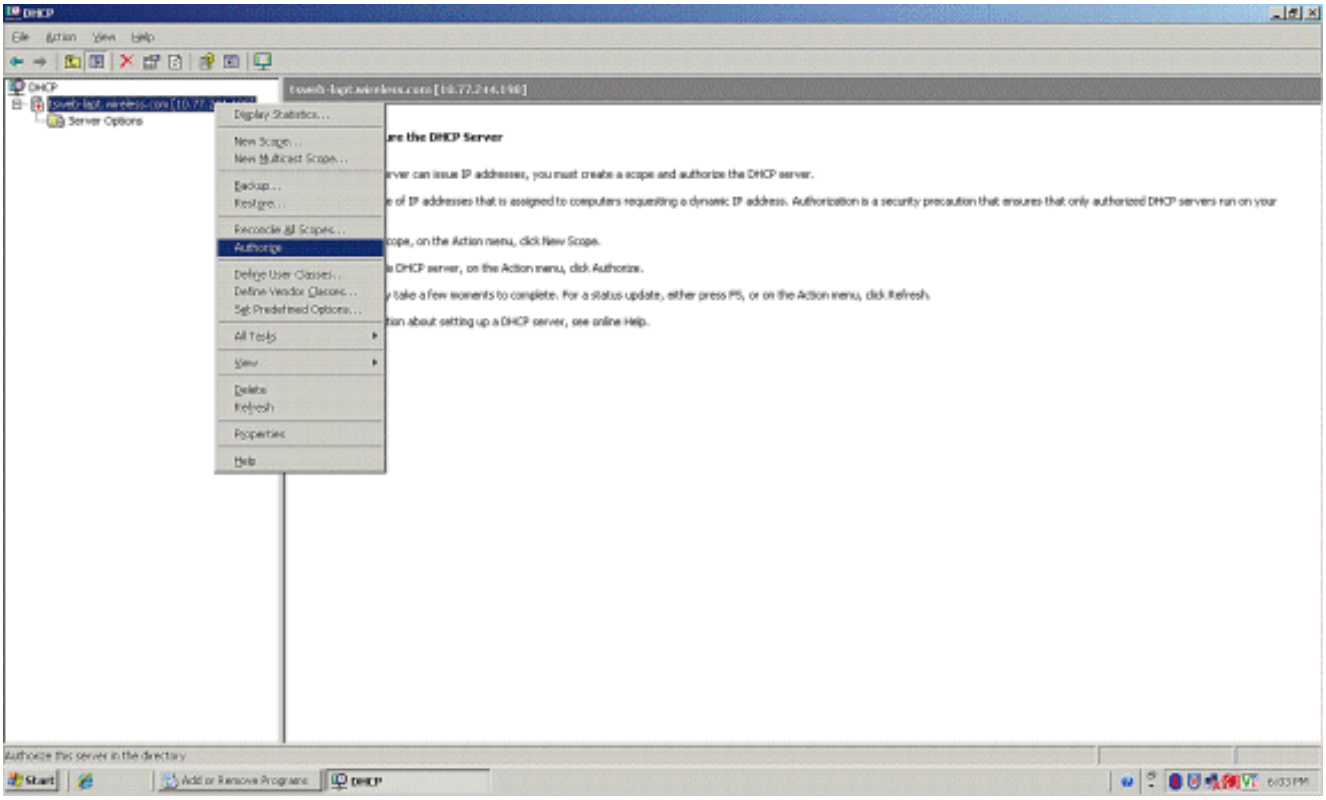
5. Haga clic en **Next** para instalar el servicio DHCP.



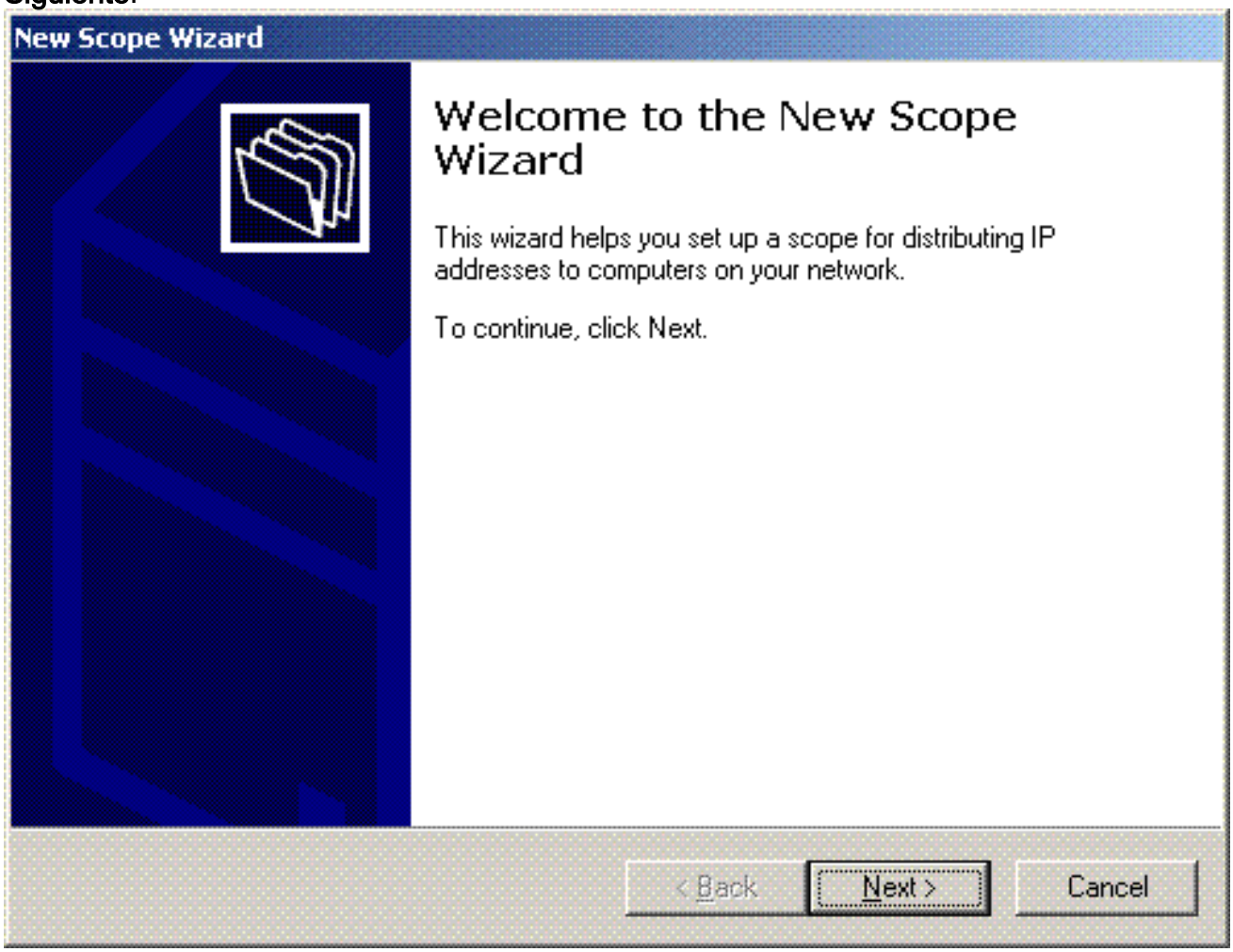
6. Haga clic en **Finish para completar la instalación.**



7. Para configurar los servicios DHCP, haga clic en **Inicio > Programas > Herramientas administrativas** y haga clic en el complemento **DHCP**.
8. Elija el servidor DHCP - **tsweb-lapt.wireless.com** (en este ejemplo).
9. Haga clic en **Action** y luego haga clic en **Authorize** para autorizar el servicio DHCP.

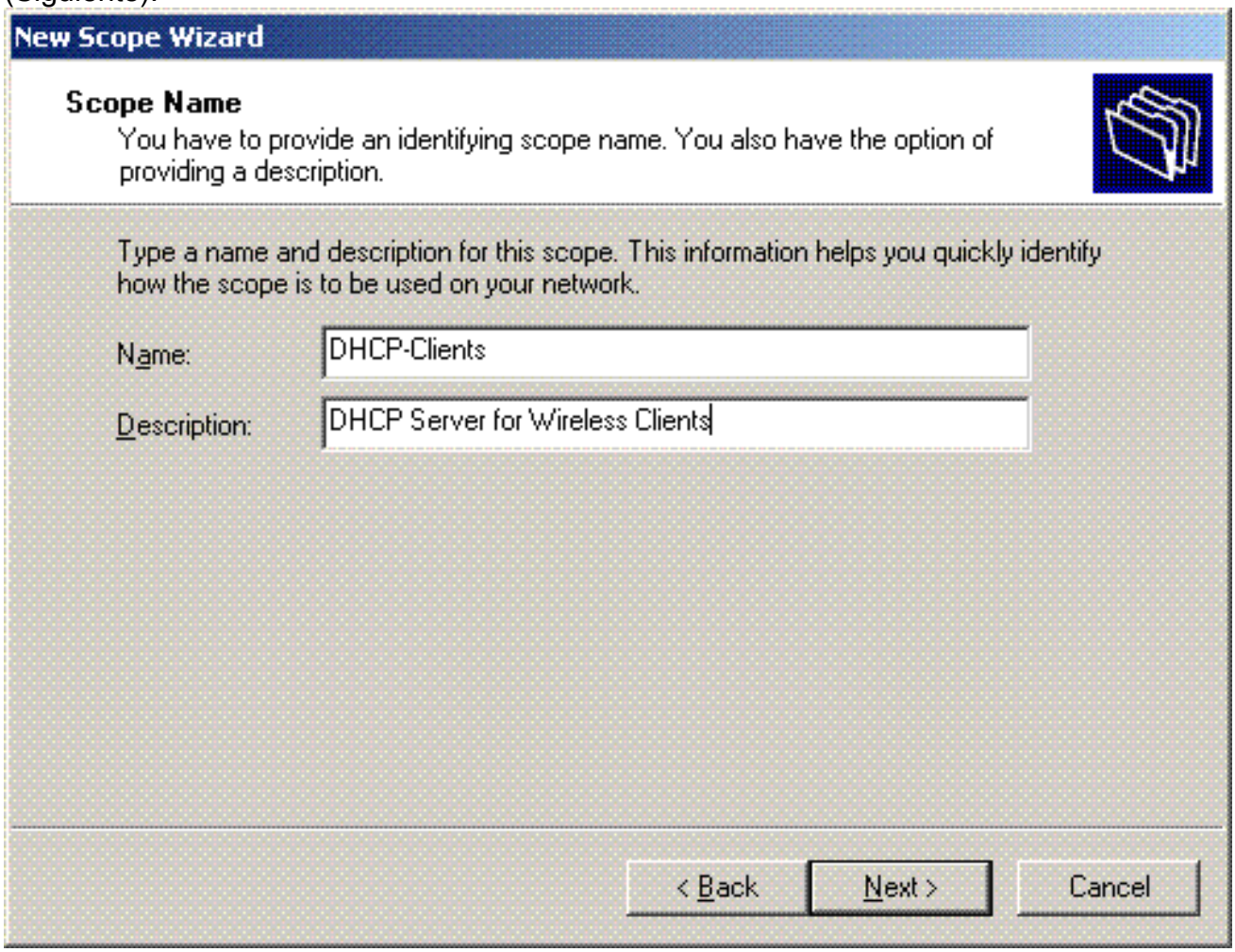


10. En el árbol de la consola, haga clic con el botón derecho en **tsweb-lapt.wireless.com** y, a continuación, haga clic en **Nuevo ámbito** para definir un intervalo de direcciones IP para los clientes inalámbricos.
11. En la página Asistente para ámbito nuevo del Asistente para ámbito nuevo, haga clic en **Siguiente**.

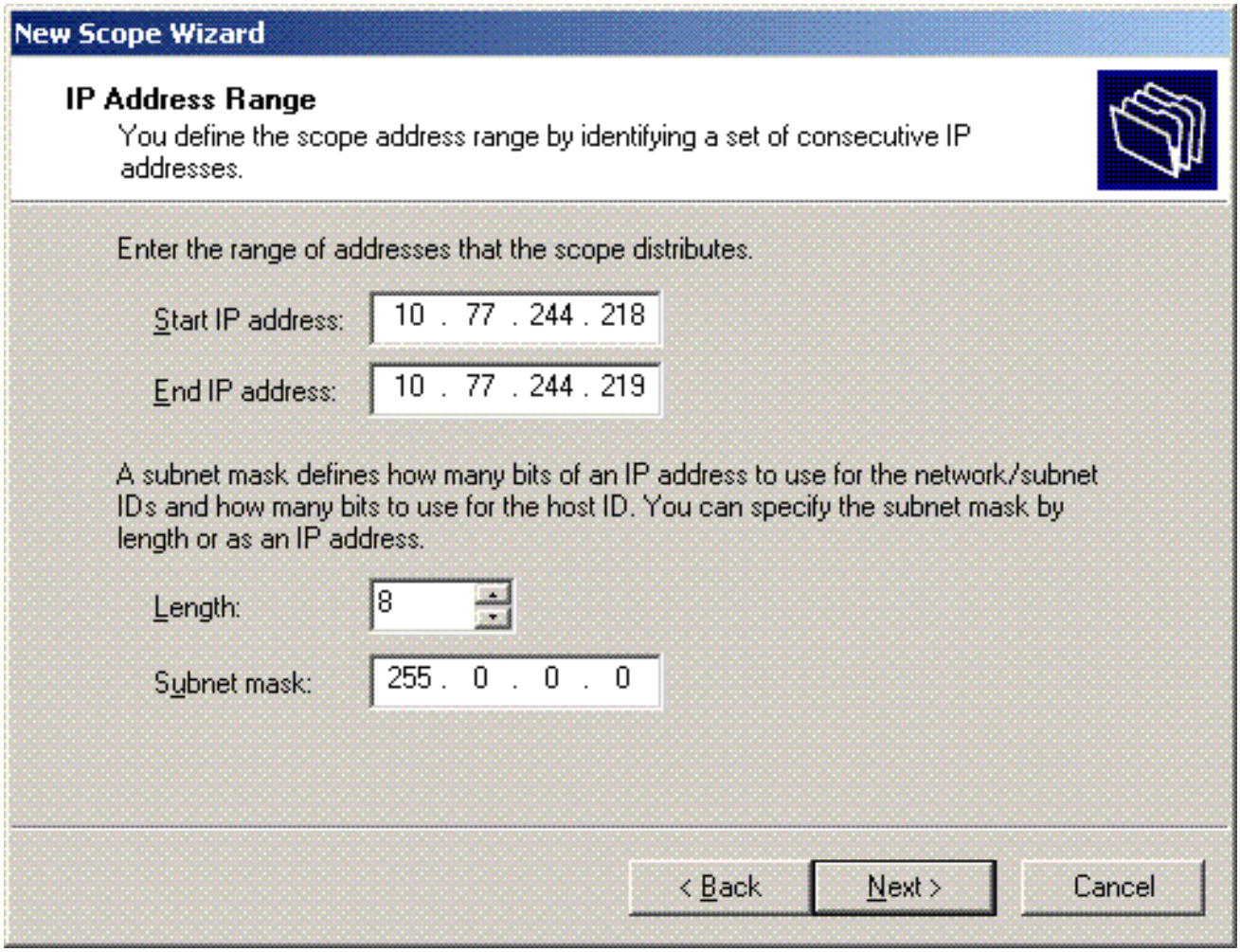


12. En la página Nombre del ámbito, escriba el nombre del ámbito DHCP. En este ejemplo,

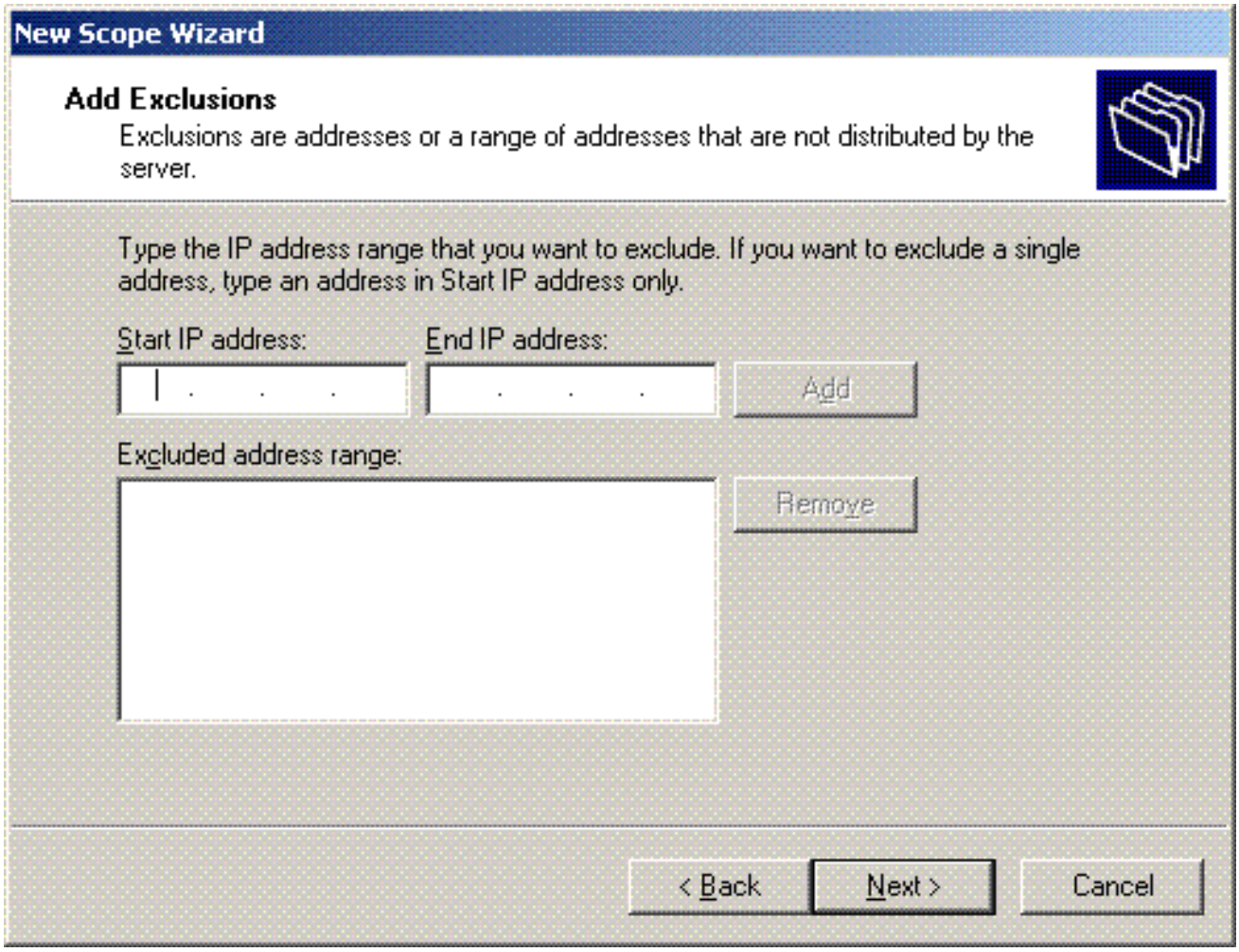
utilice **DHCP-Clients** como nombre de ámbito. Haga clic en Next (Siguiente).



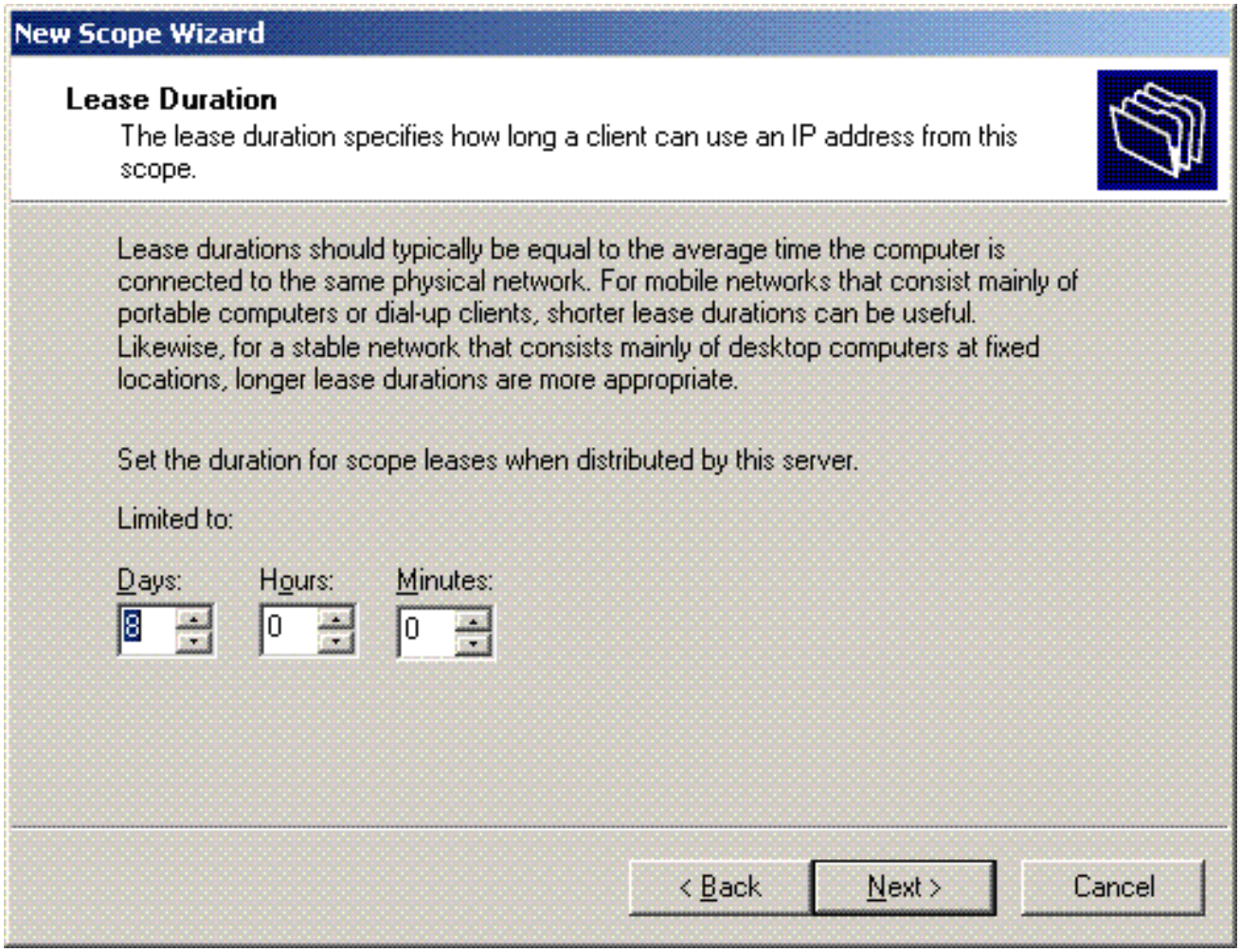
13. En la página Intervalo de direcciones IP, escriba las direcciones IP inicial y final del ámbito y haga clic en **Siguiente**.



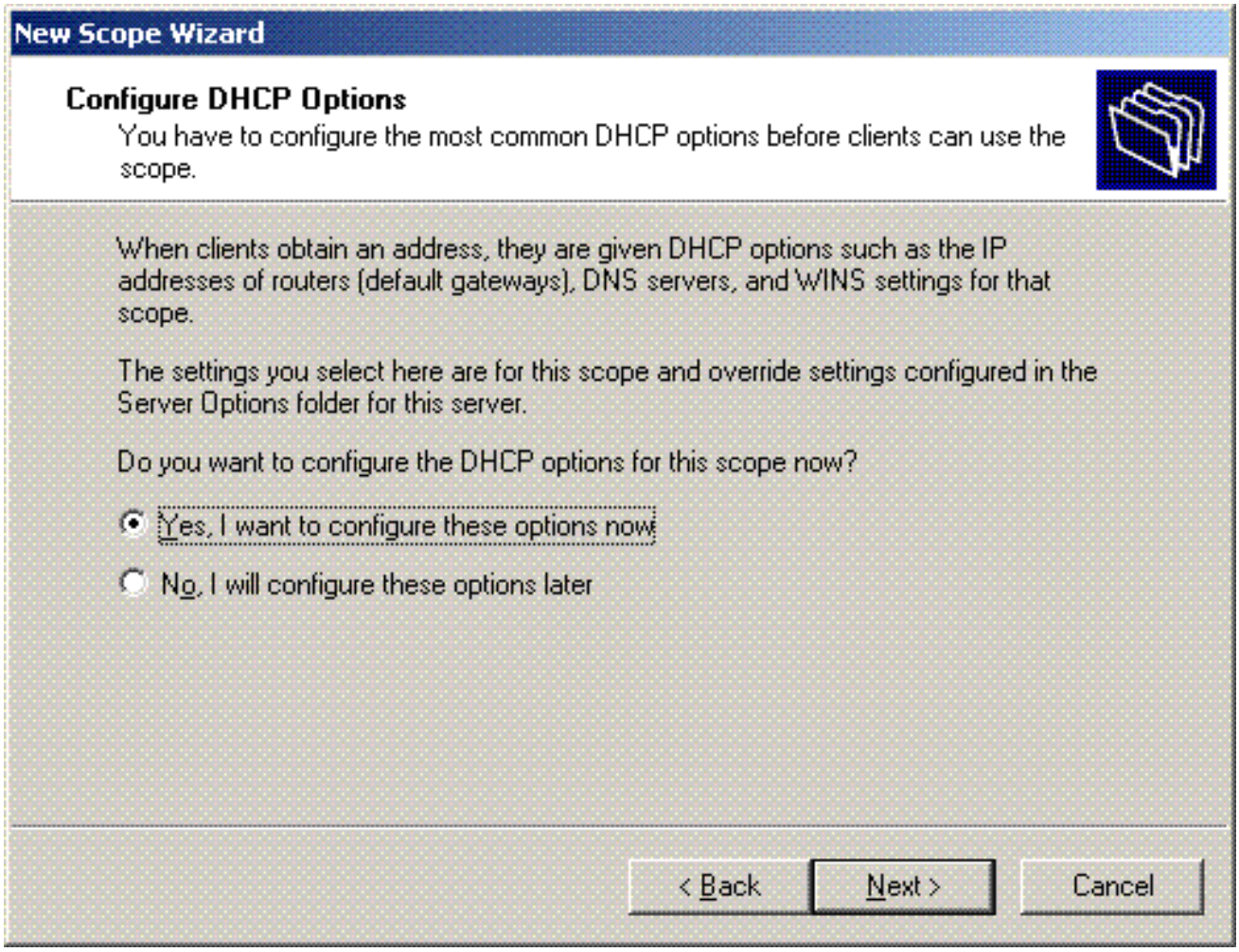
14. En la página Add Exclusions (Agregar exclusiones), indique la dirección IP que desea reservar/excluir del ámbito DHCP. Haga clic en Next (Siguiente).



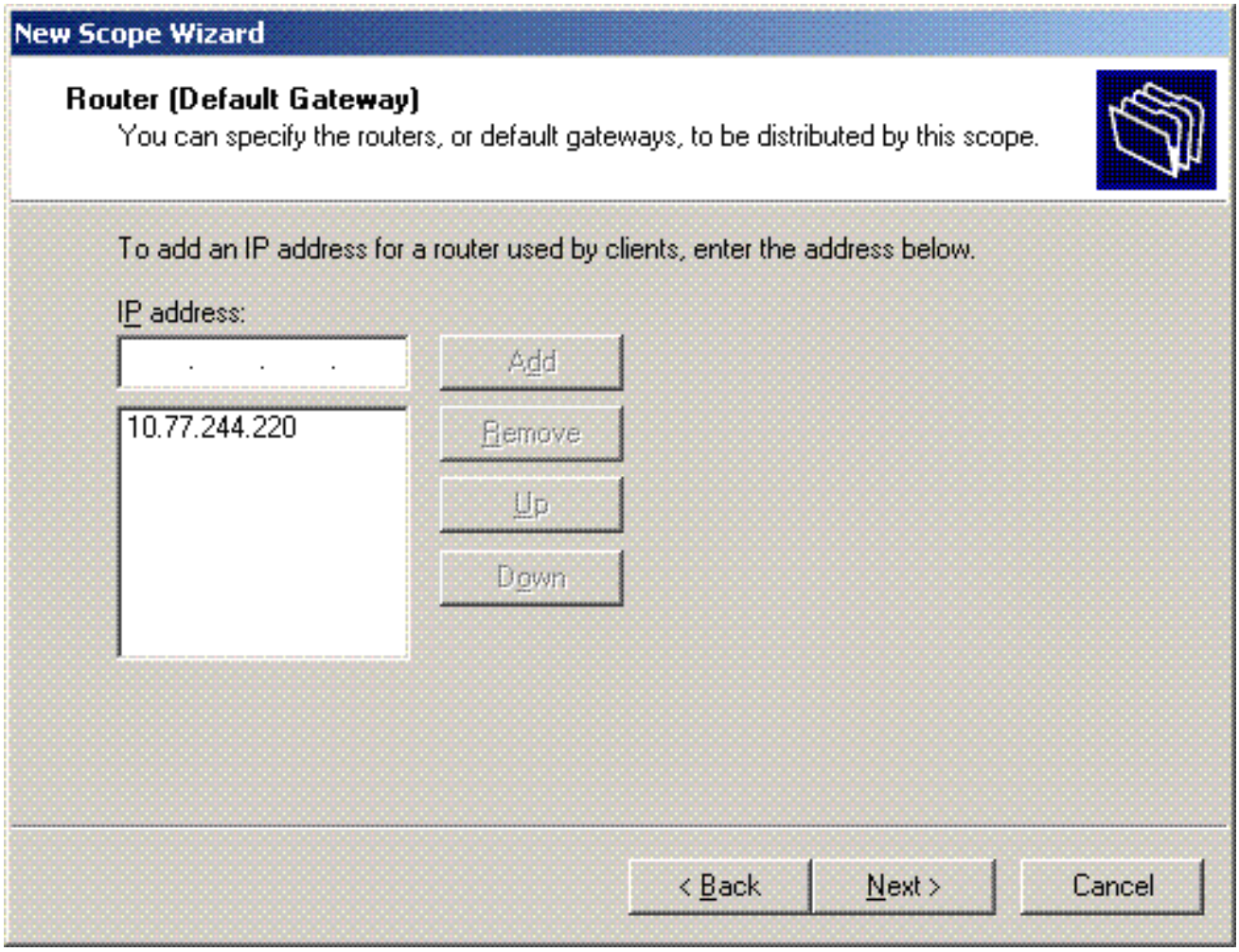
15. Mencione la duración de la concesión en la página Duración de la concesión y haga clic en **Siguiente**.



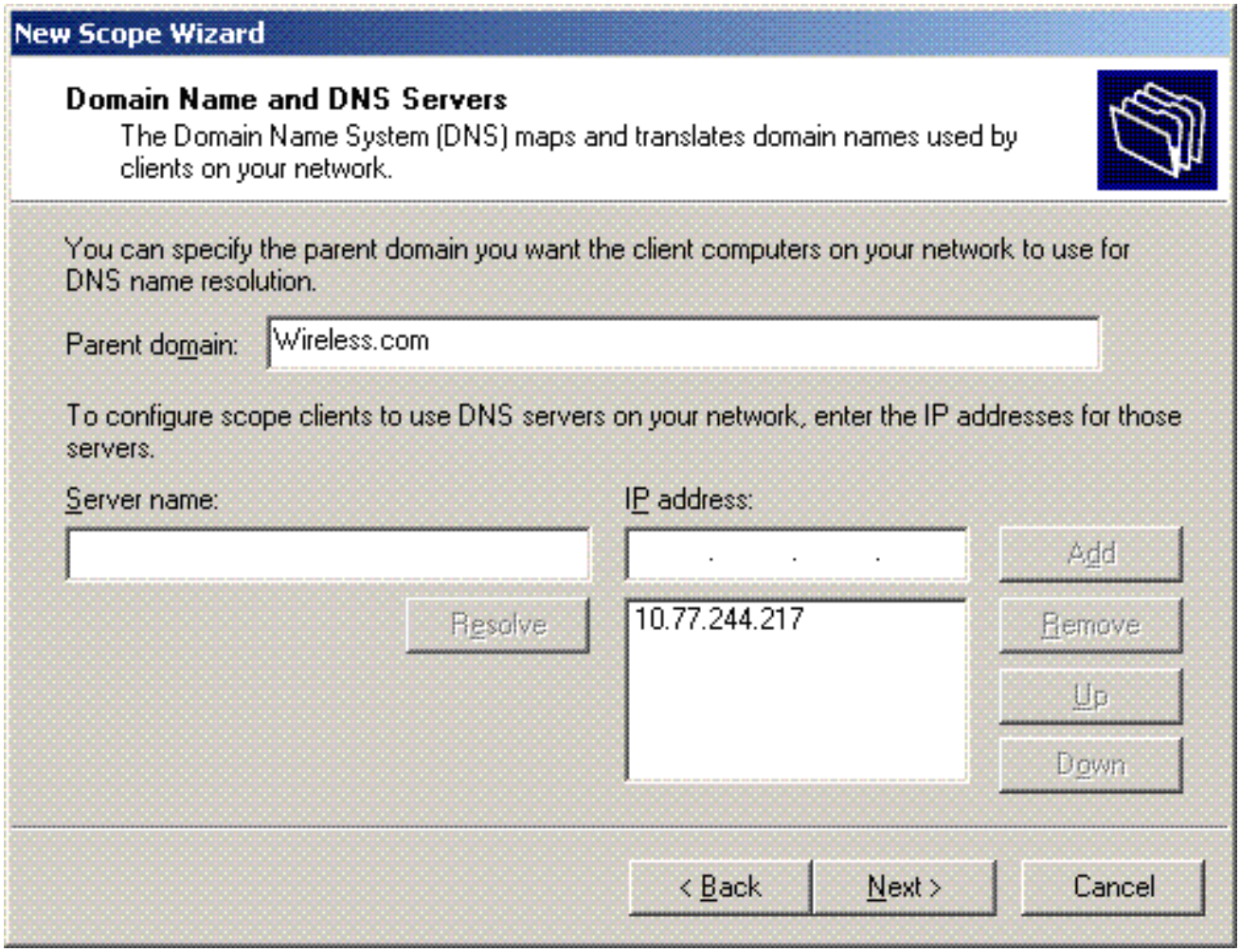
16. En la página Configure DHCP options (Configurar opciones DHCP), elija **Yes, I want to configure DHCP Option now** (Sí, deseo configurar la opción DHCP ahora) y haga clic en **Next**.



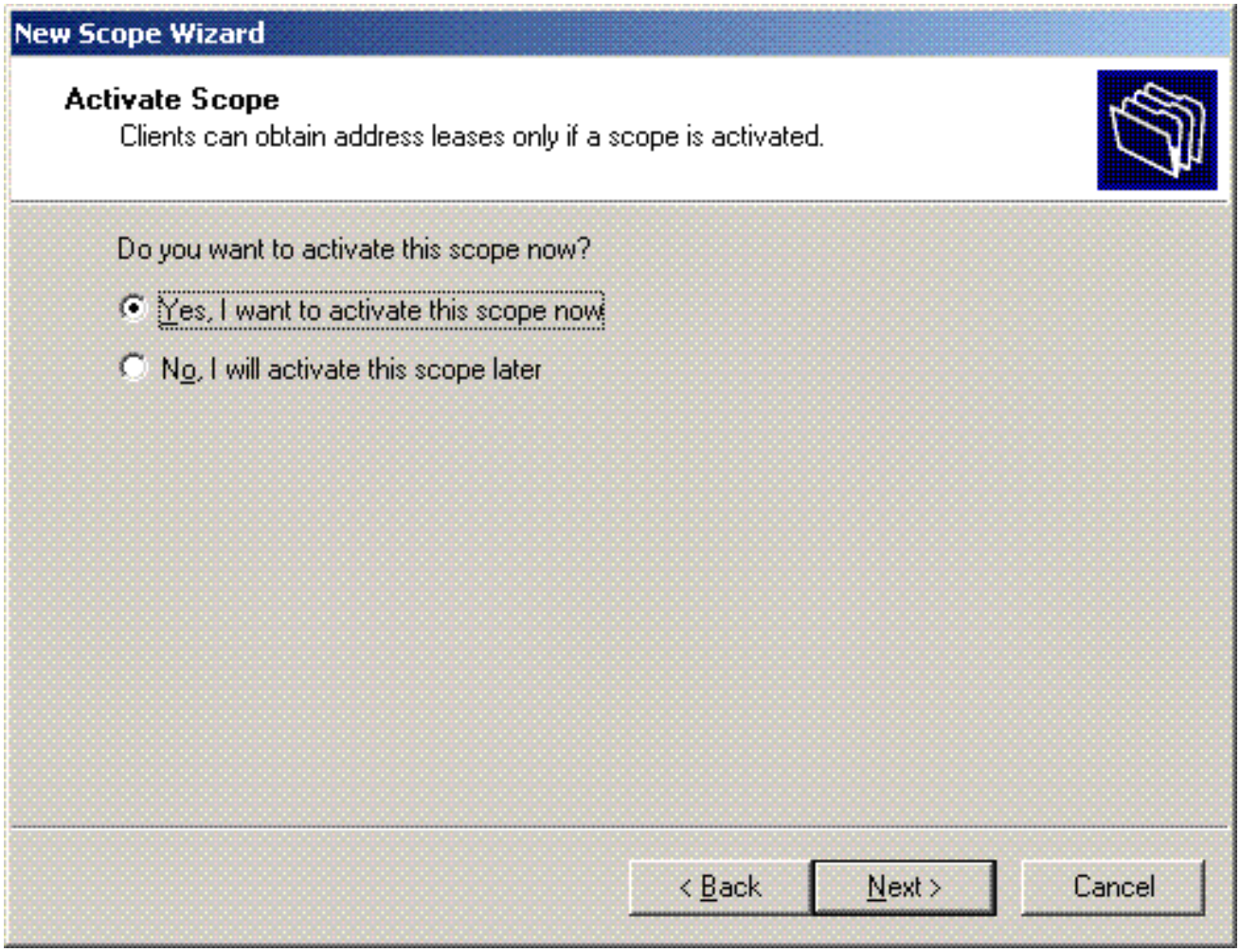
17. Si hay un router de gateway predeterminado, indique la dirección IP del router de gateway en la página Router (Default Gateway) (Router (Default Gateway)) y haga clic en **Next** (**Siguiente)**.



18. En la página Nombre de dominio y servidores DNS, escriba el nombre del dominio configurado anteriormente. En el ejemplo, utilice **Wireless.com**. Introduzca la dirección IP del servidor. Haga clic en Add
(Agregar).

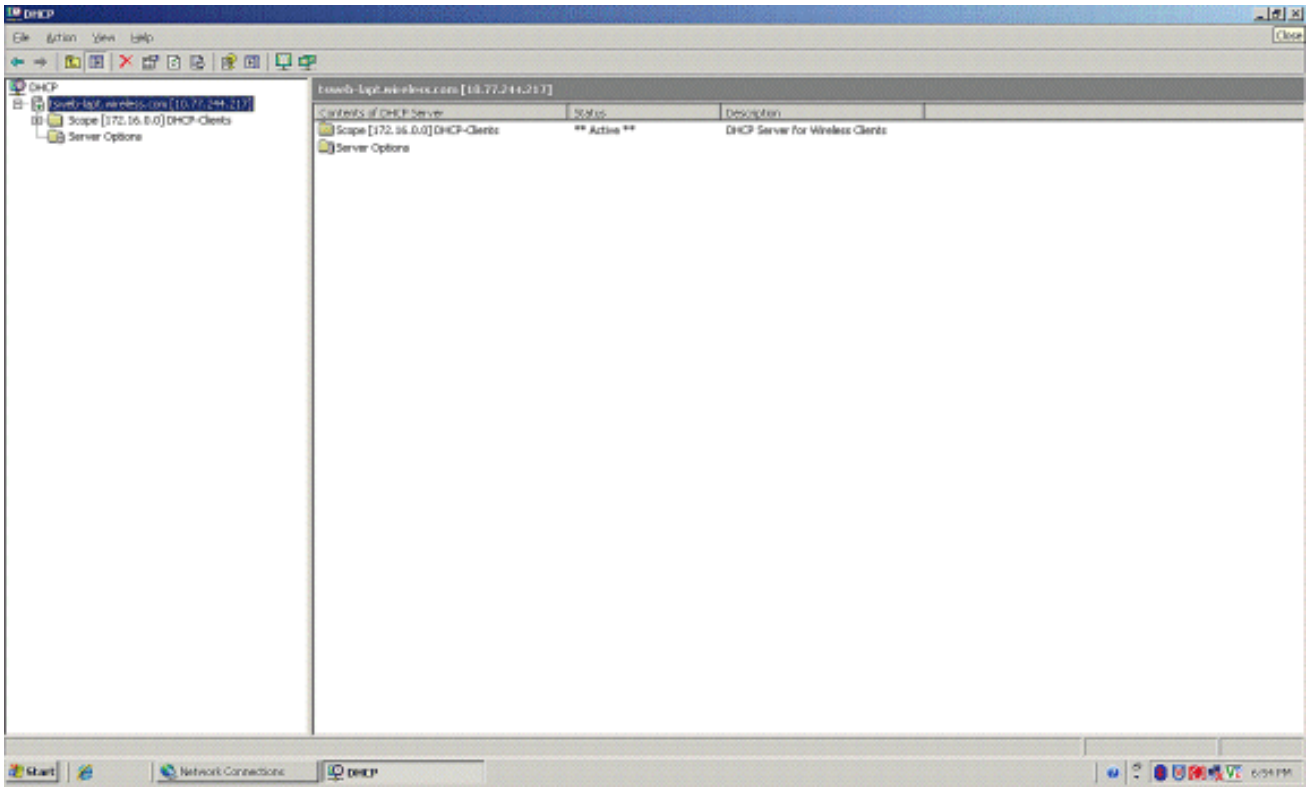


19. Haga clic en Next (Siguiente).
20. En la página Servidor WINS, haga clic en **Siguiente**.
21. En la página Activar ámbito, elija **Sí, deseo activar el ámbito ahora** y haga clic en **Siguiente**.



22. Al finalizar el Asistente para ámbito nuevo, haga clic en **Finalizar**.

23. En la ventana Complemento DHCP, compruebe que el ámbito DHCP creado está activo.



Ahora que DHCP/ DNS está activado en el servidor, configure el servidor como un servidor de la Autoridad de Certificación (CA) empresarial.

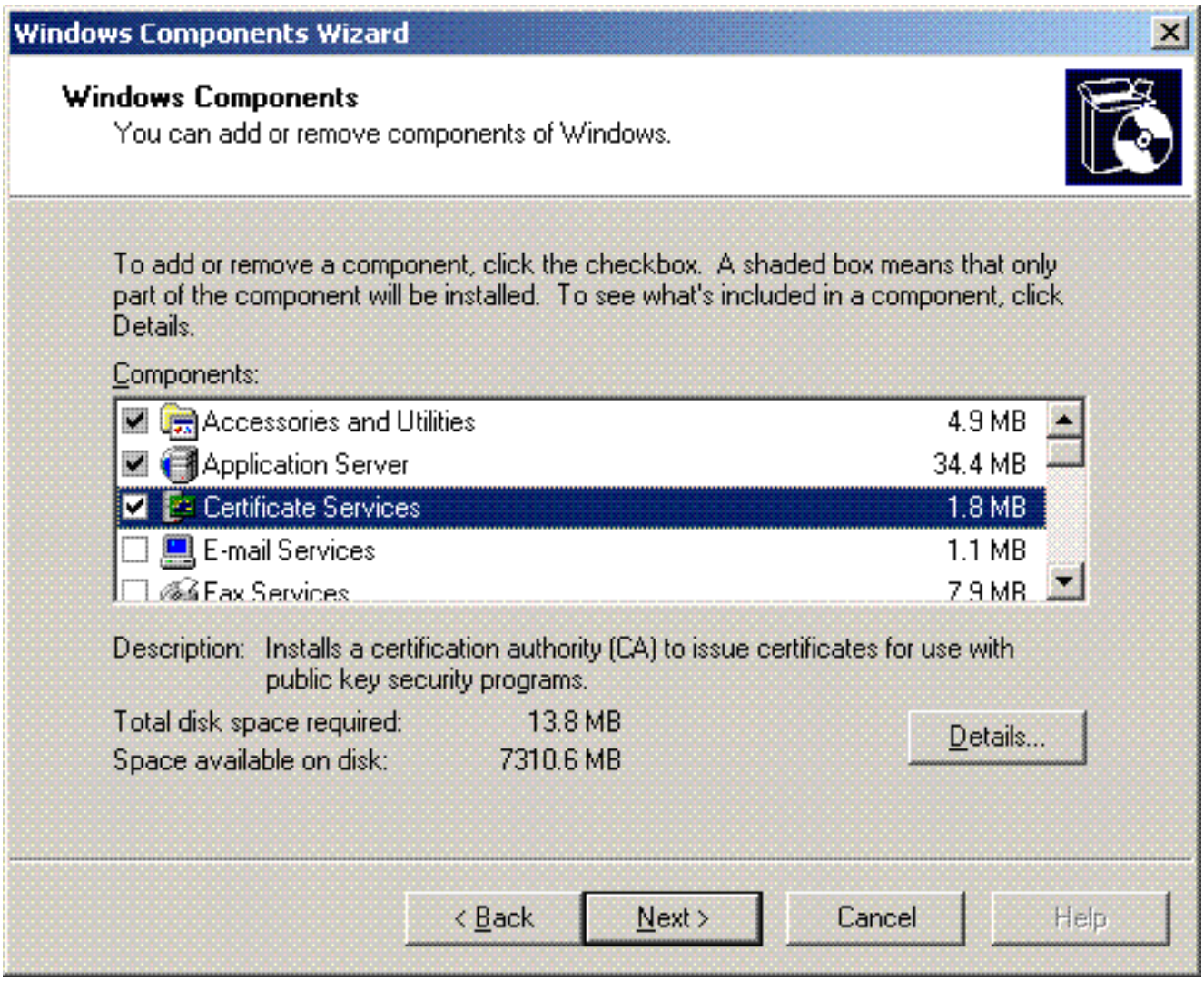
[Instalar y configurar Microsoft Windows 2003 Server como servidor de la autoridad]

[certificadora (CA)]

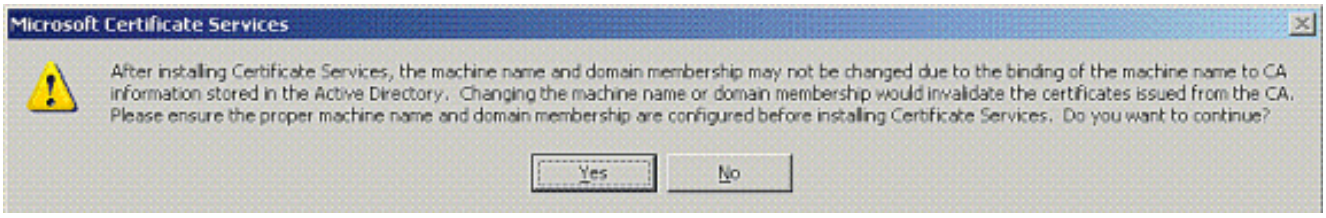
PEAP con EAP-MS-CHAPv2 valida el servidor RADIUS basándose en el certificado presente en el servidor. Además, el certificado de servidor debe ser emitido por una entidad de certificación (CA) pública en la que confíe el equipo cliente (es decir, el certificado de CA pública ya existe en la carpeta Entidad de certificación raíz de confianza en el almacén de certificados del equipo cliente). En este ejemplo, configure el servidor de Microsoft Windows 2003 como una entidad emisora de certificados (CA) que emite el certificado al Servicio de autenticación de Internet (IAS).

Para instalar y configurar los servicios de certificados en el servidor, complete estos pasos:

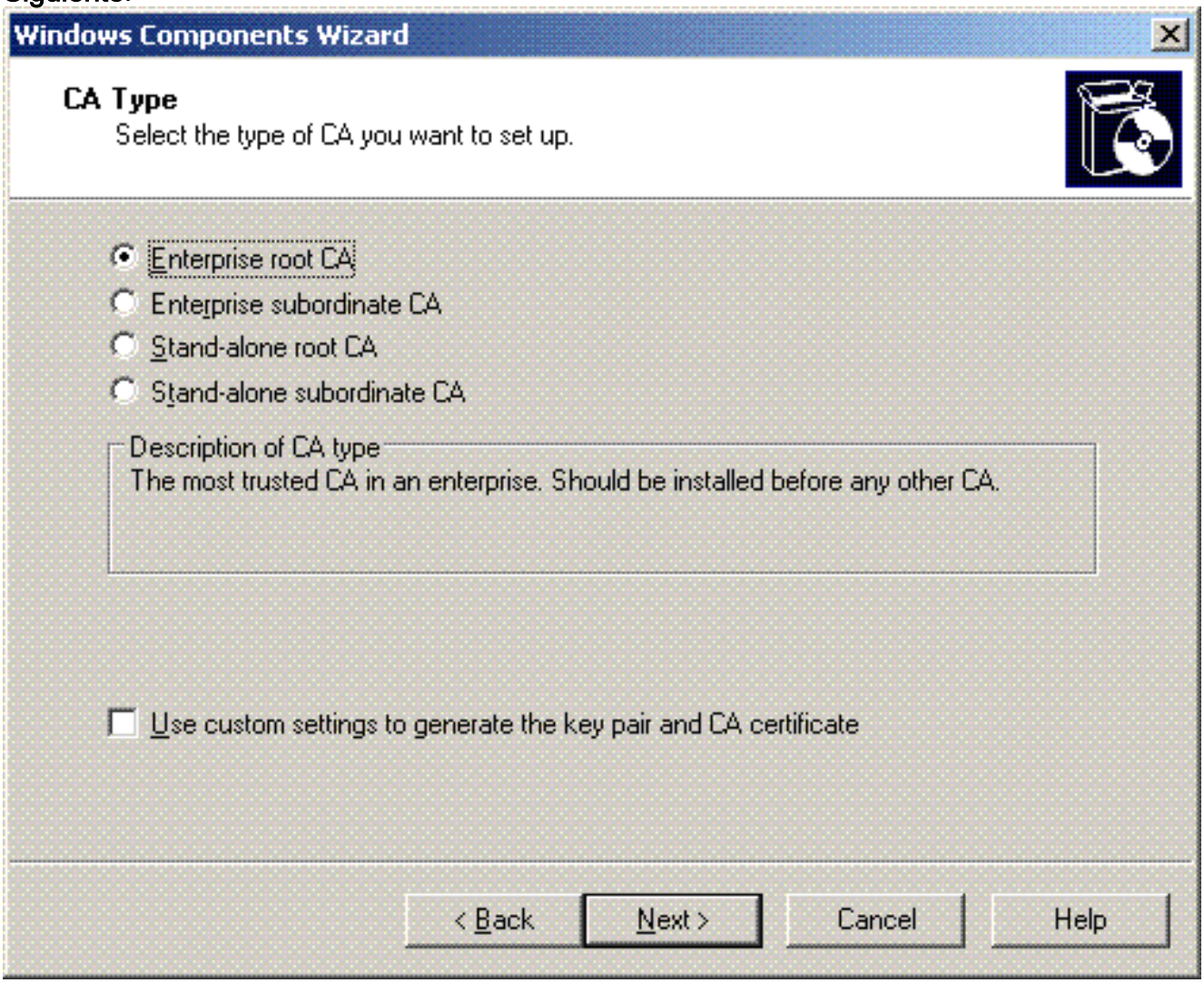
1. Haga clic en **Agregar o quitar programas en el Panel de control**.
2. Haga clic en **Agregar o quitar componentes de Windows**.
3. Haga clic en **Servicios de Certificate Server**.



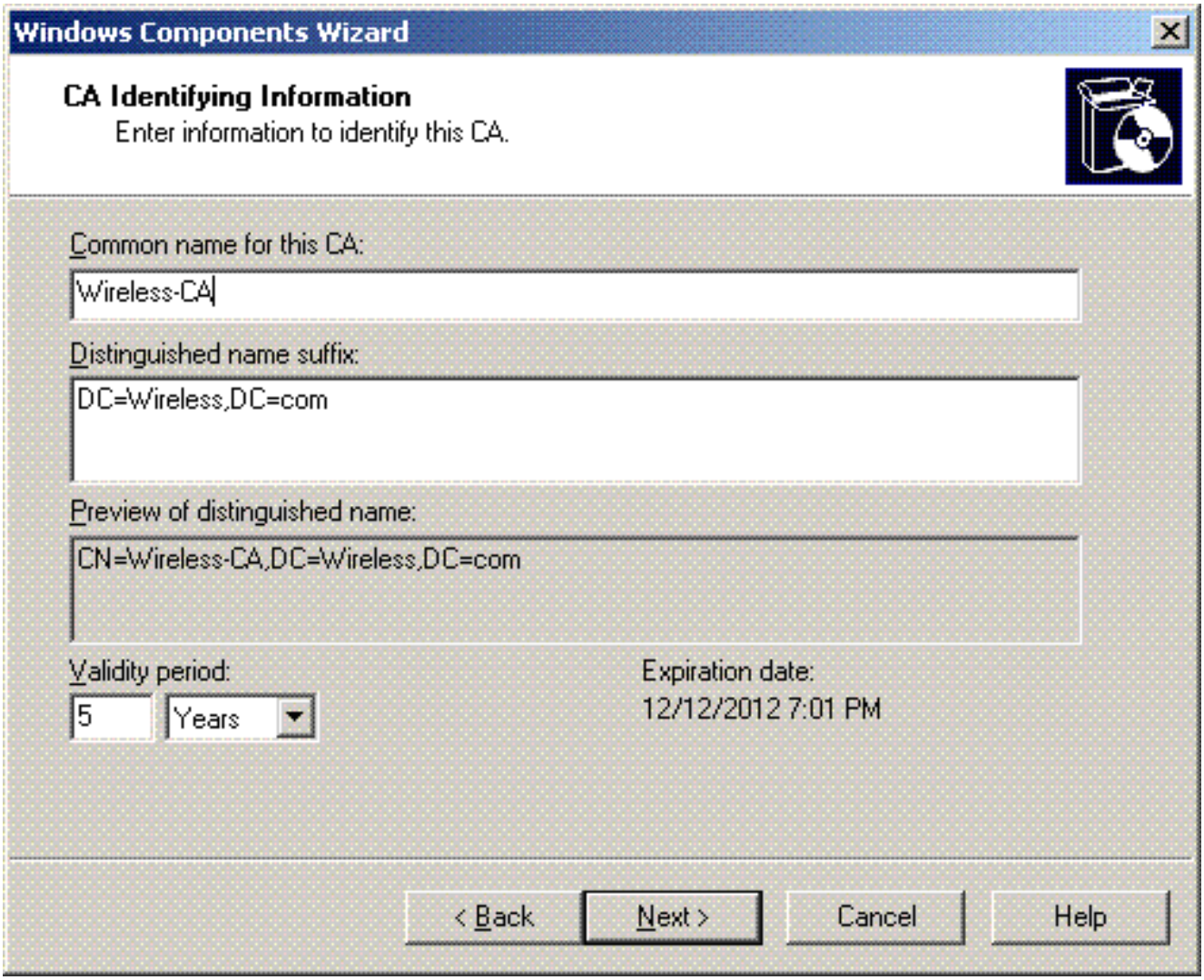
4. Haga clic en **Sí** para ver el mensaje de advertencia, **Después de instalar Servicios de Certificate Server, no se puede cambiar el nombre del equipo y el equipo no se puede unir a un dominio ni se puede quitar de él. ¿Desea continuar?**



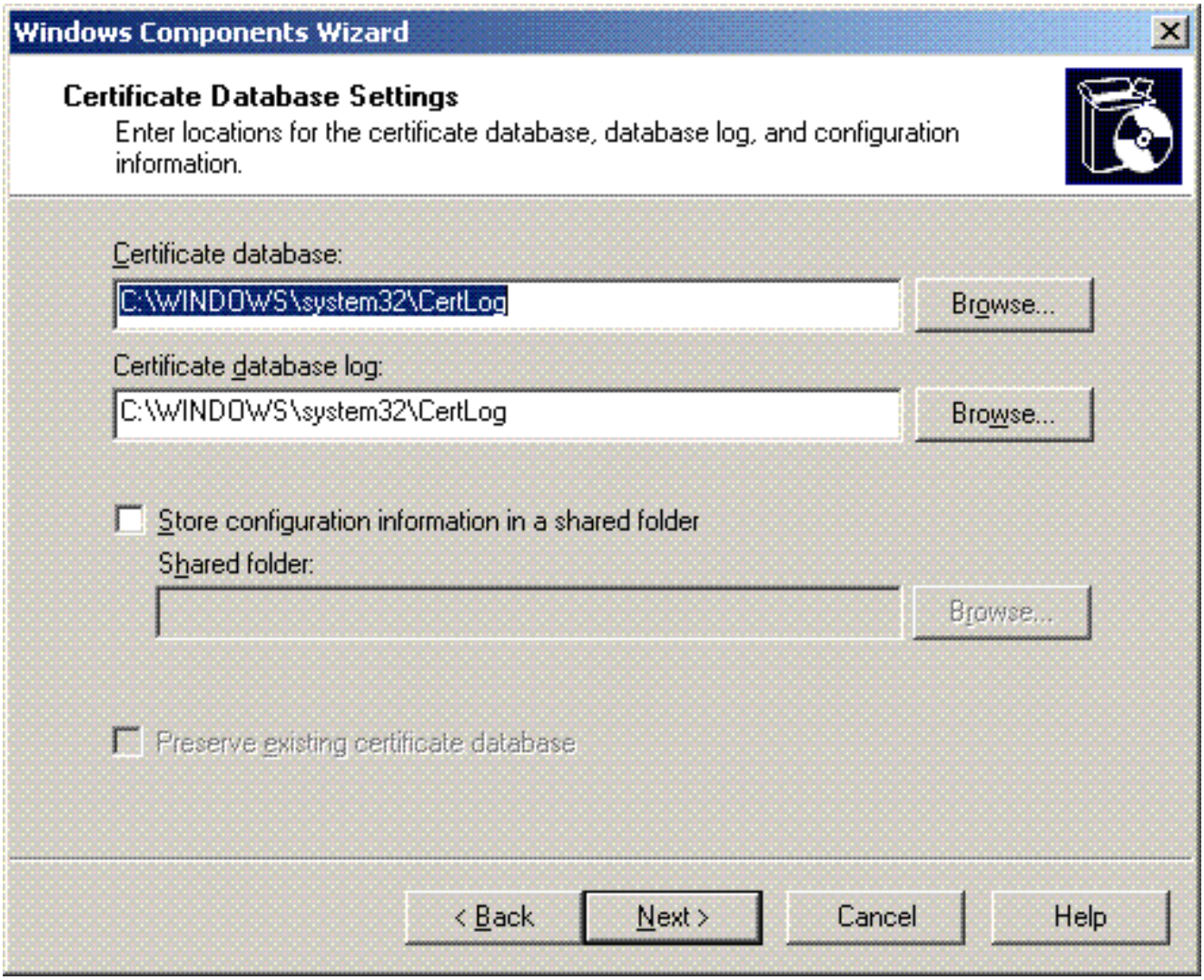
5. En Tipo de autoridad certificadora, elija **CA raíz de empresa** y haga clic en **Siguiente**.



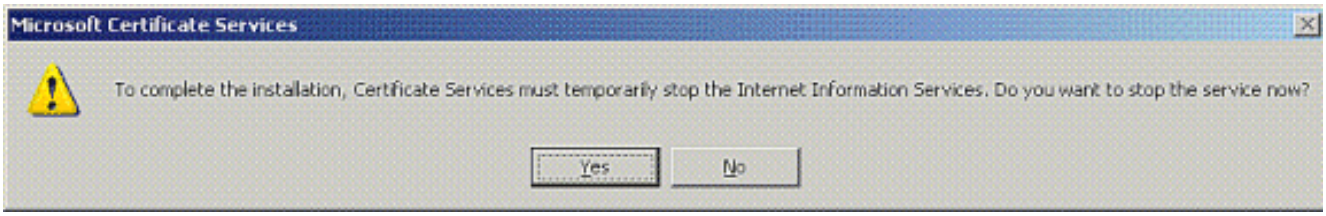
6. Introduzca un nombre para identificar la CA. Este ejemplo utiliza **Wireless-CA**. Haga clic en Next
(Siguiente).



7. Se crea un directorio "Registro de certificados" para el almacenamiento de la base de datos de certificados. Haga clic en Next
(Siguiente).



8. Si IIS está habilitado, debe detenerse antes de continuar. Haga clic en **Aceptar** para ver el mensaje de advertencia que indica que IIS debe detenerse. Se reinicia automáticamente después de instalar la
CA.



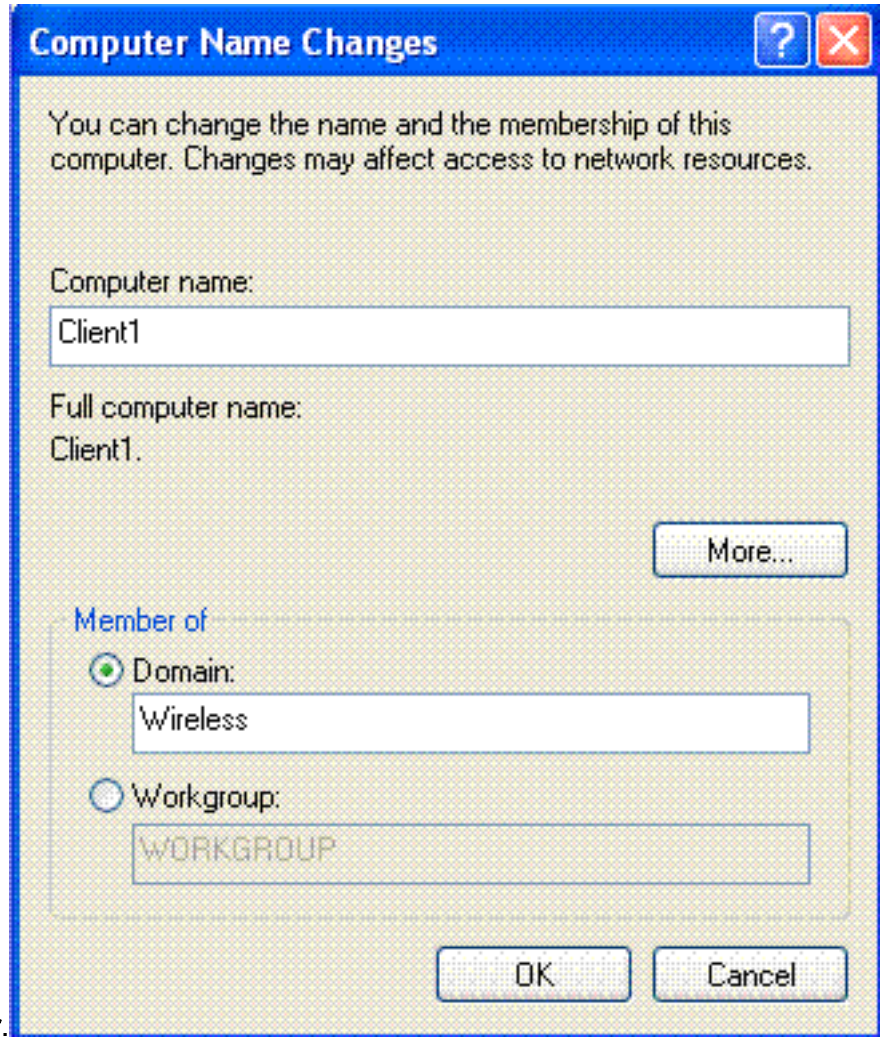
9. Haga clic en **Finalizar** para completar la instalación de los servicios de la autoridad certificadora
(CA).

El siguiente paso es instalar y configurar el Servicio de autenticación de Internet en el servidor de Microsoft Windows 2003.

Conectar clientes al dominio

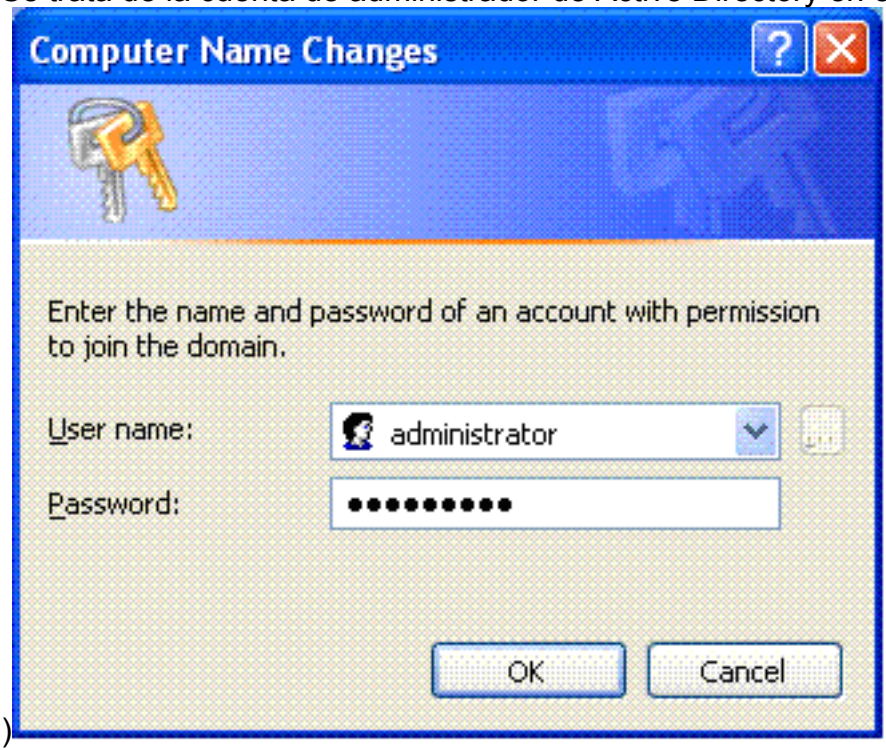
El siguiente paso es conectar los clientes a la red por cable y descargar la información específica del dominio del nuevo dominio. En otras palabras, conecte los clientes al dominio. A tal efecto, complete estos pasos:

1. Conecte los clientes a la red con cables mediante un cable Ethernet directo.
2. Inicie el cliente e inicie sesión con el nombre de usuario/ contraseña del cliente.
3. Haga clic en **Inicio**; haga clic en **Ejecutar**; escriba **cmd**; y haga clic en **Aceptar**.
4. En el símbolo del sistema, escriba **ipconfig** y haga clic en **Enter** para verificar que DHCP funciona correctamente y que el cliente recibió una dirección IP del servidor DHCP.
5. Para unir el cliente al dominio, haga clic con el botón derecho en **Mi PC**, y elija **Propiedades**.
6. Haga clic en la ficha **Nombre de equipo**.
7. Haga clic en **Cambiar**.
8. Haga clic en **Dominio**; escriba **wireless.com**; y haga clic en



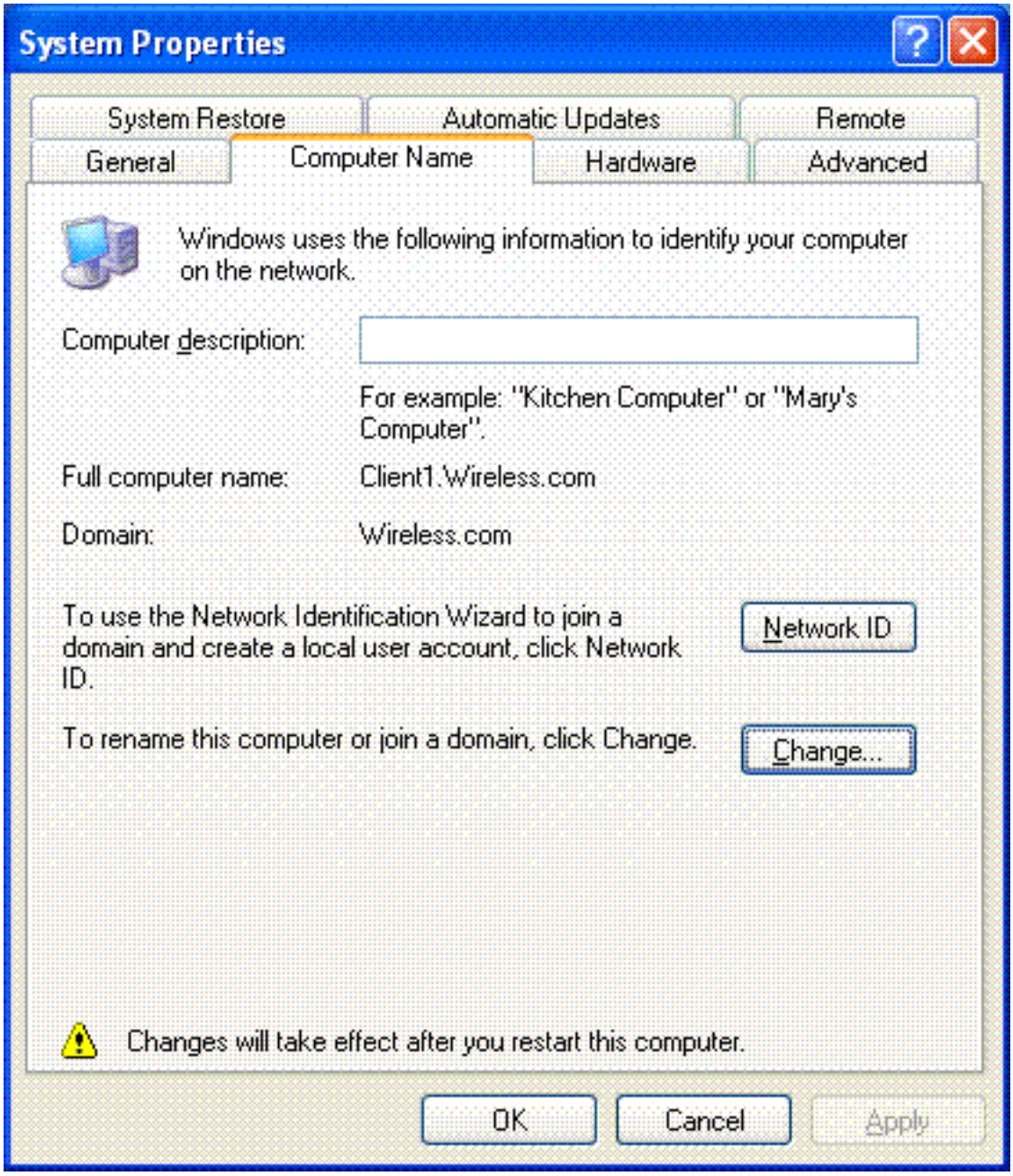
Aceptar.

9. Escriba **Username Administrator** y la contraseña específica del dominio al que se une el cliente. (Se trata de la cuenta de administrador de Active Directory en el



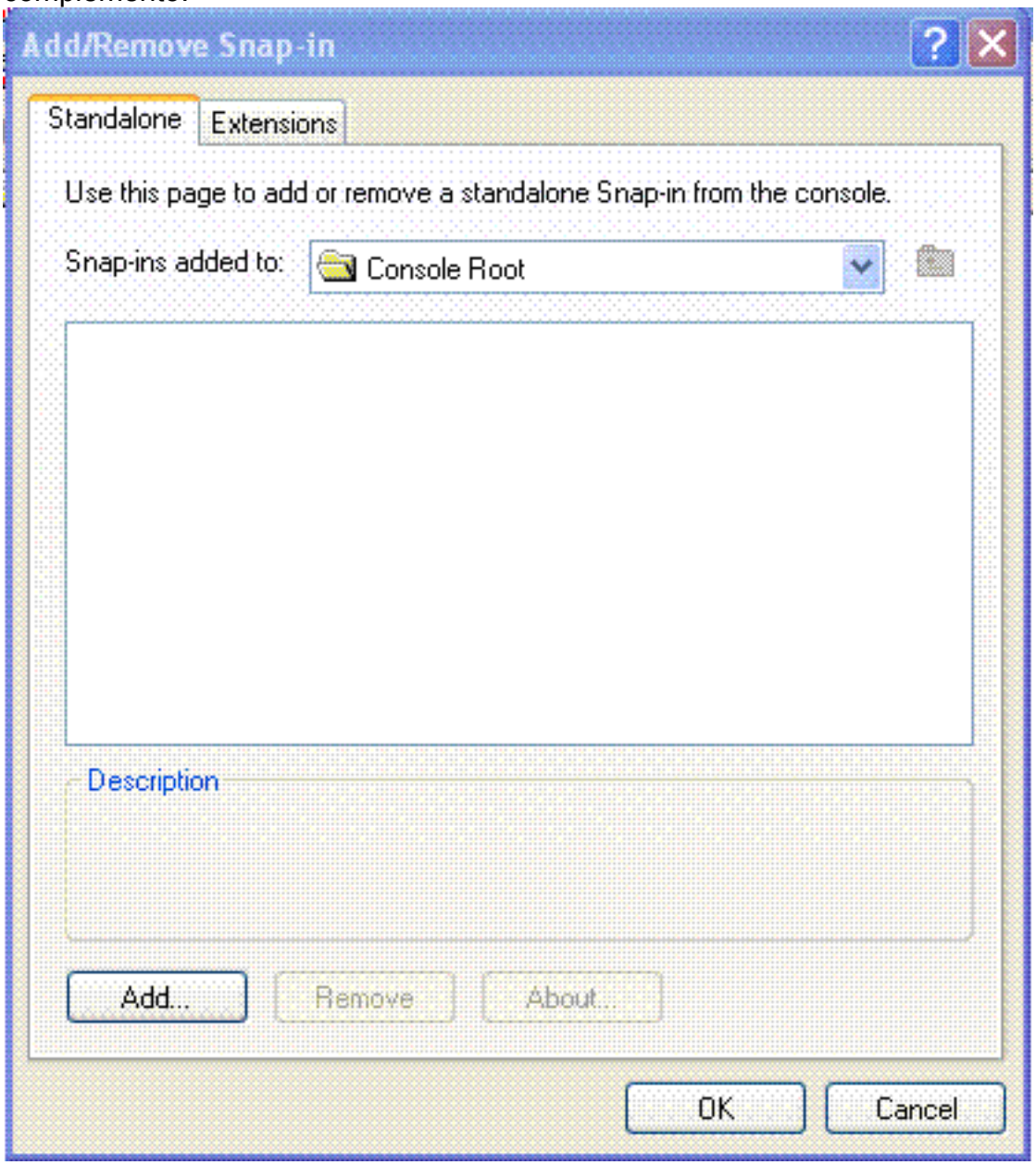
servidor.)

10. Click OK.
11. Haga clic en **Yes** para reiniciar el equipo.
12. Una vez reiniciado el equipo, inicie sesión con esta información: Nombre de usuario = **Administrador**; Contraseña = **<contraseña de dominio>**; Dominio = **Inalámbrico**.
13. Haga clic con el botón derecho en **Mi PC** y haga clic en **Propiedades**.
14. Haga clic en la ficha **Nombre de equipo** para comprobar que se encuentra en el dominio Wireless.com.

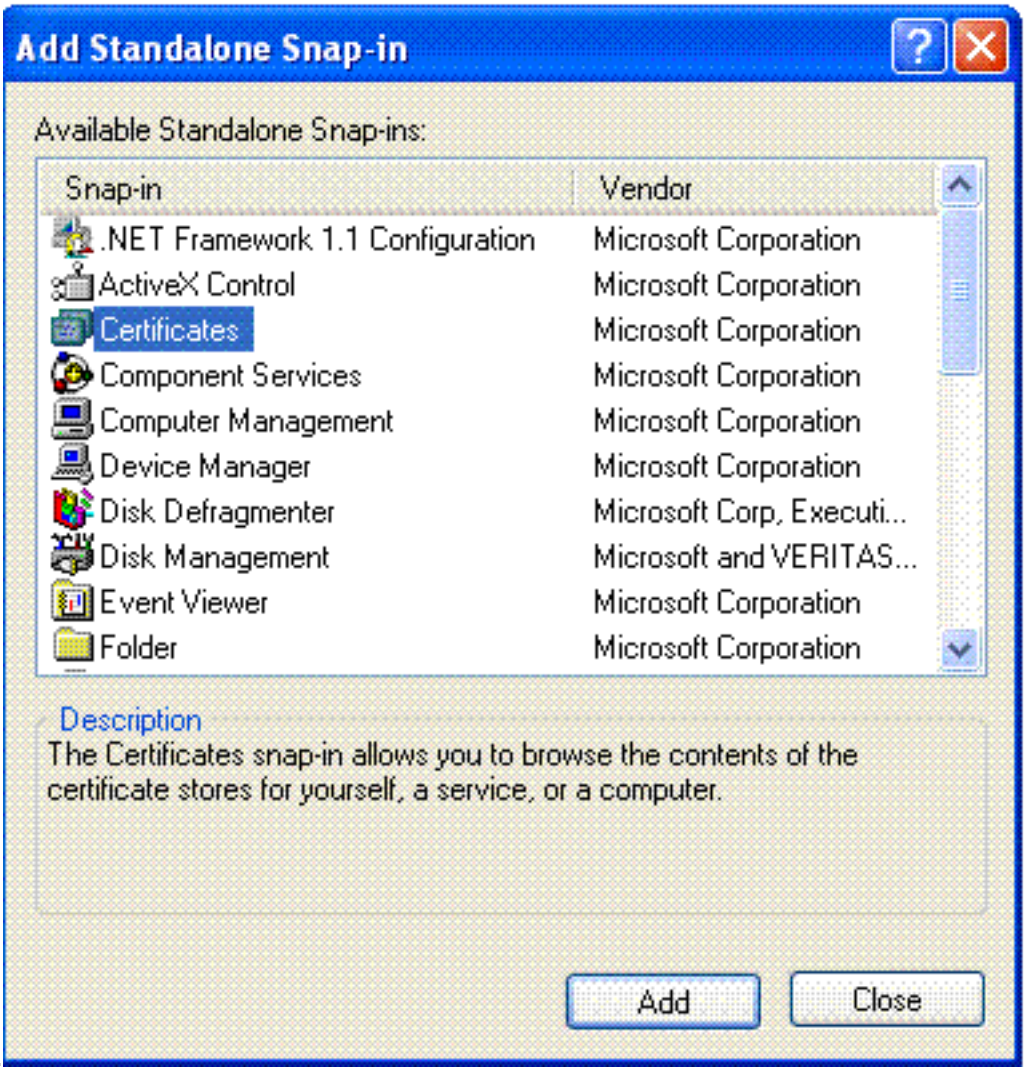


15. El siguiente paso consiste en comprobar que el cliente recibió el certificado de CA (confianza) del servidor.
16. Haga clic en **Inicio**; haga clic en **Ejecutar**; escriba **mmc**, y haga clic en **Aceptar**.

17. Haga clic en **Archivo** y haga clic en **Agregar o quitar** complemento.

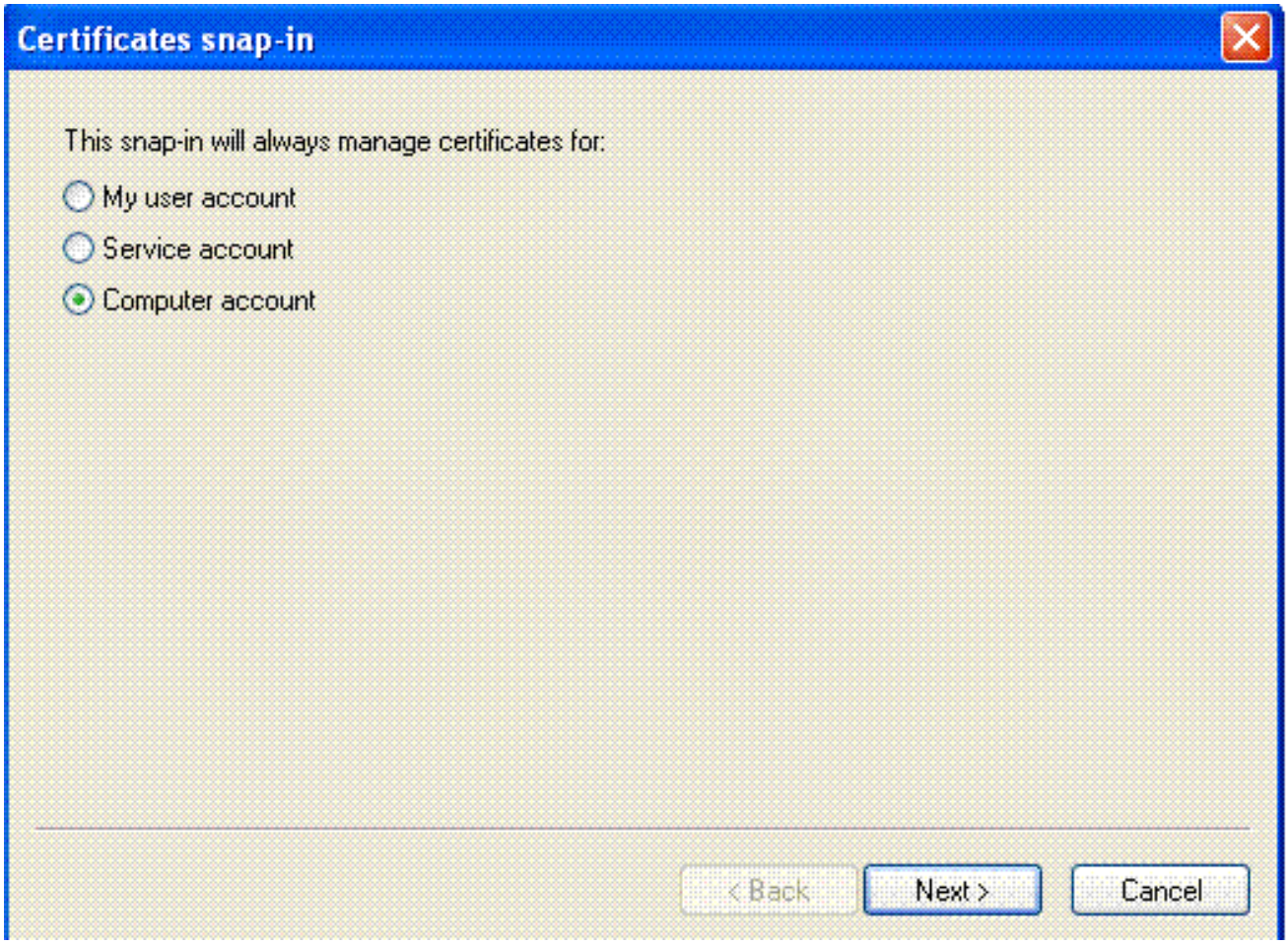


18. Haga clic en Add (Agregar).
19. Elija **Certificate**, y haga clic en

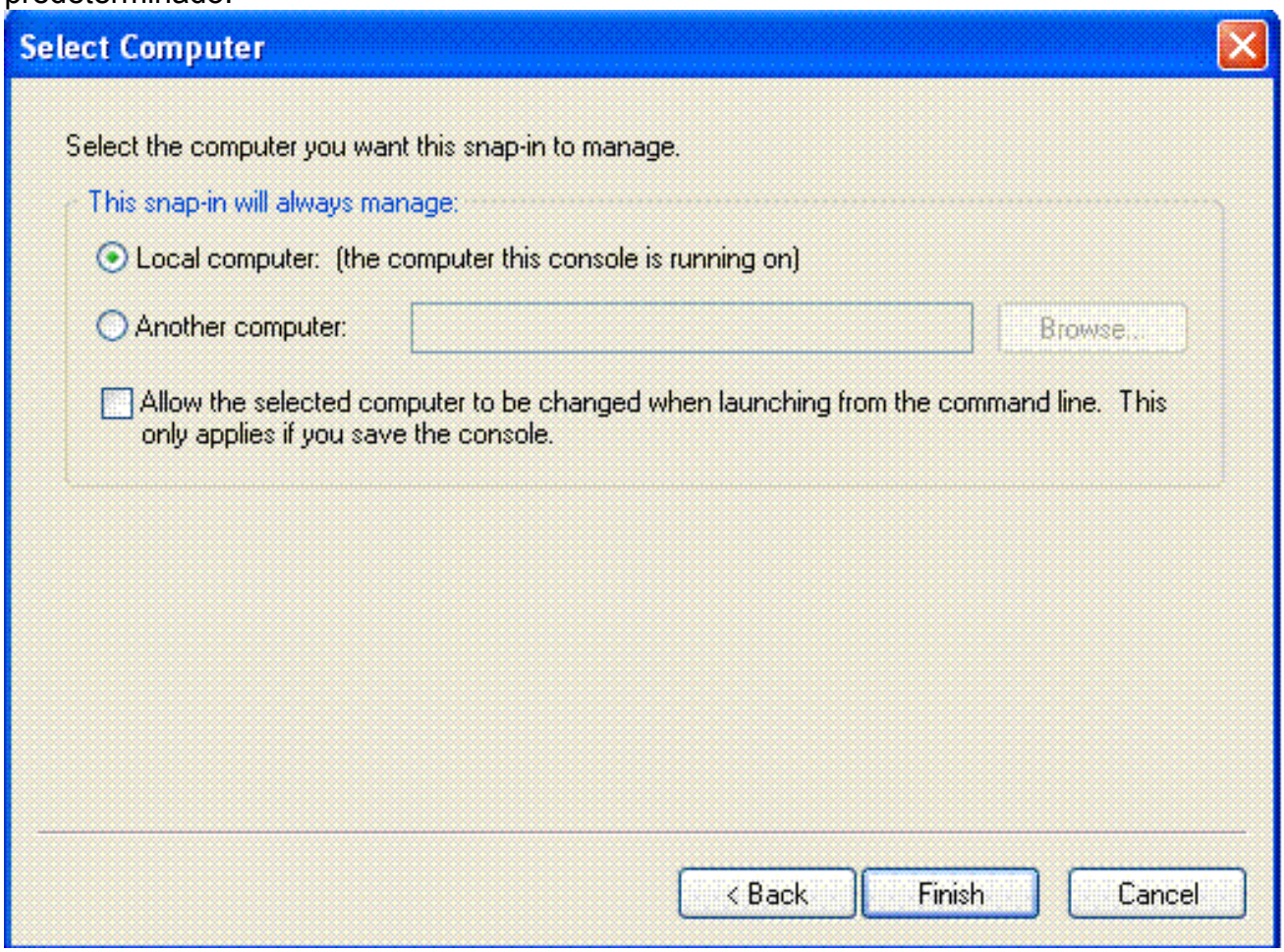


Add.

20. Elija **Computer Account**, y haga clic en **Next**.

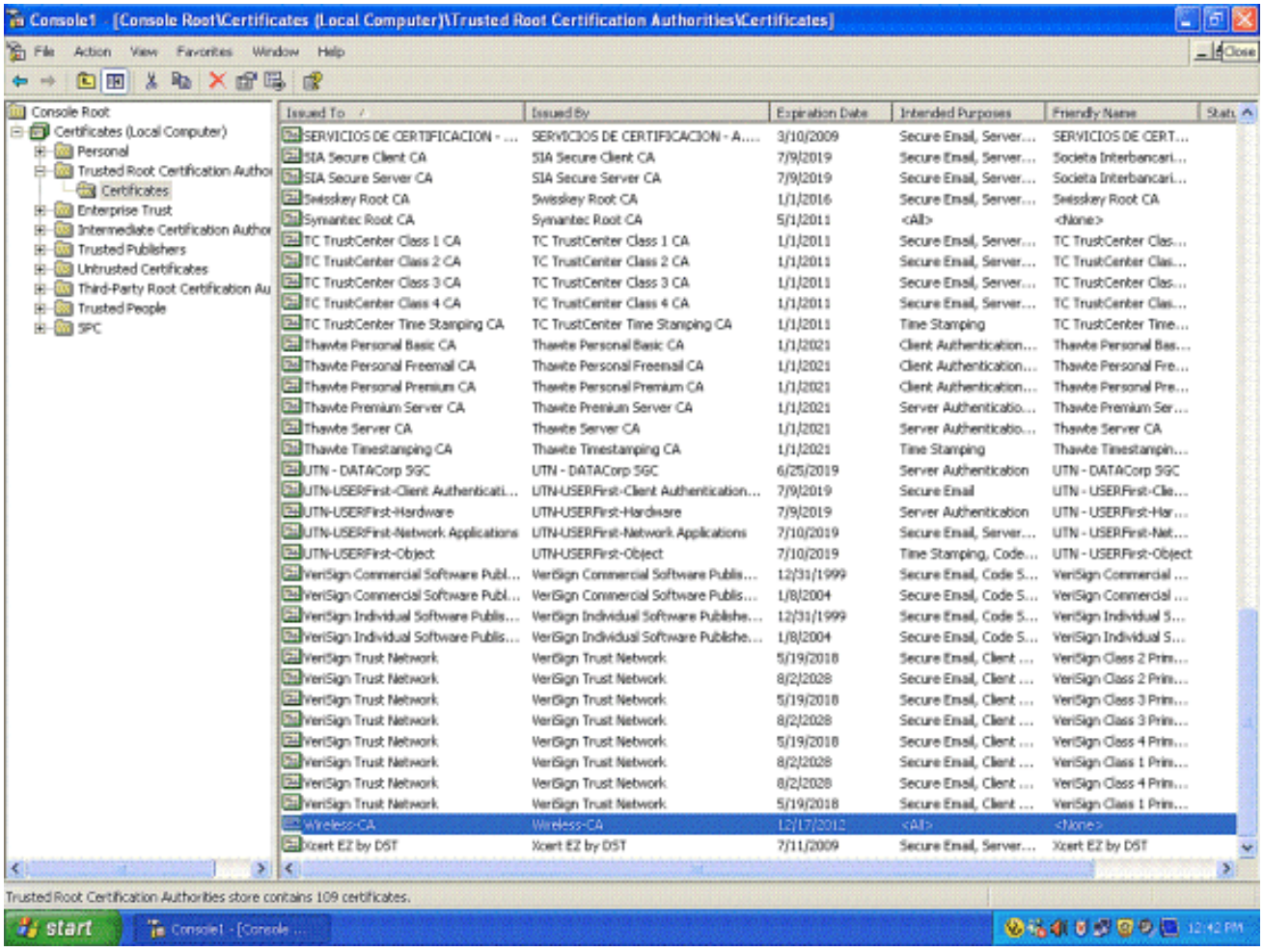


21. Haga clic en **Finalizar** para aceptar el equipo local predeterminado.



22. Haga clic en **Cerrar** y luego en **Aceptar**.

23. Expanda **Certificados (Equipo local)**; expanda **Entidades de certificación raíz de confianza**; y haga clic en **Certificados**. Busque **Wireless** en la lista.



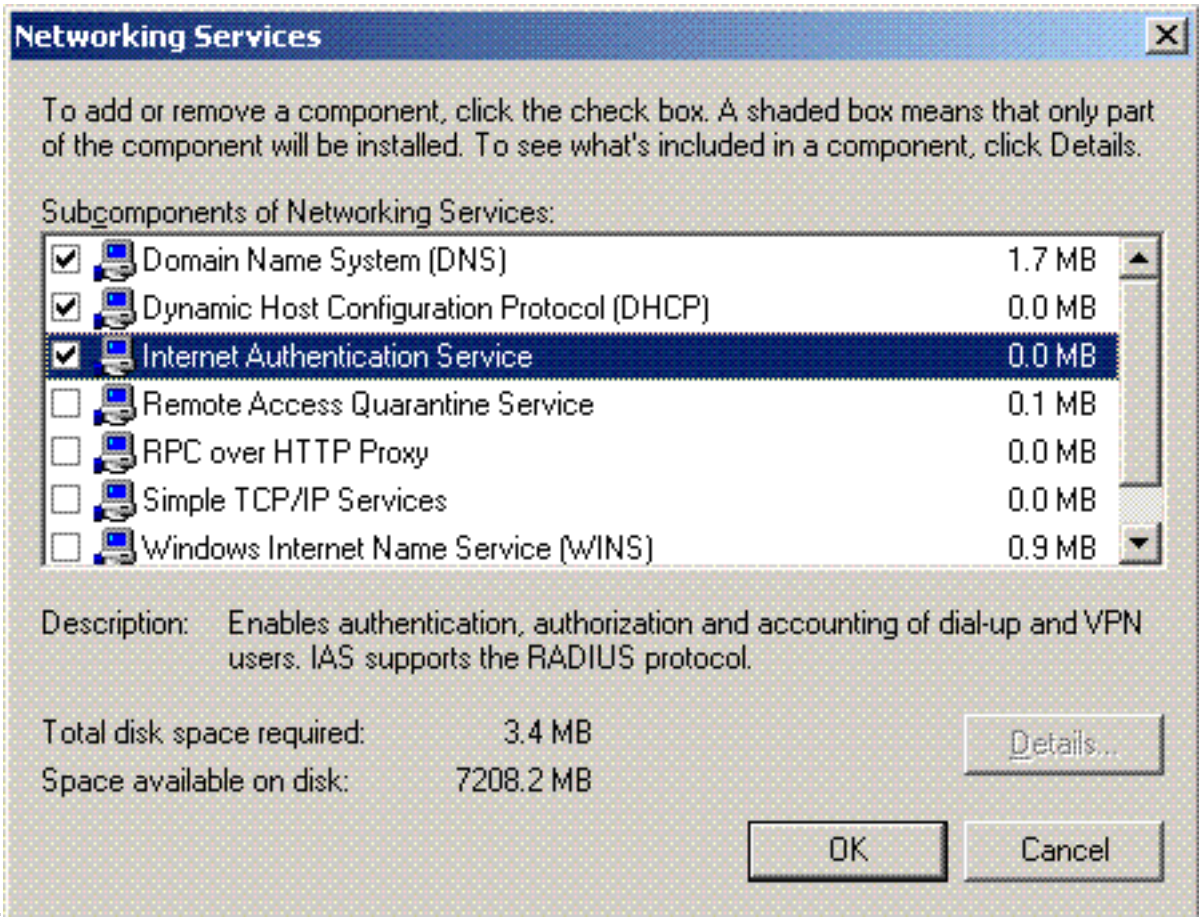
24. Repita este procedimiento para agregar más clientes al dominio.

Instalar el Servicio de autenticación de Internet en Microsoft Windows 2003 Server y Solicitar un certificado

En esta configuración, el Servicio de autenticación de Internet (IAS) se utiliza como servidor RADIUS para autenticar clientes inalámbricos con autenticación PEAP.

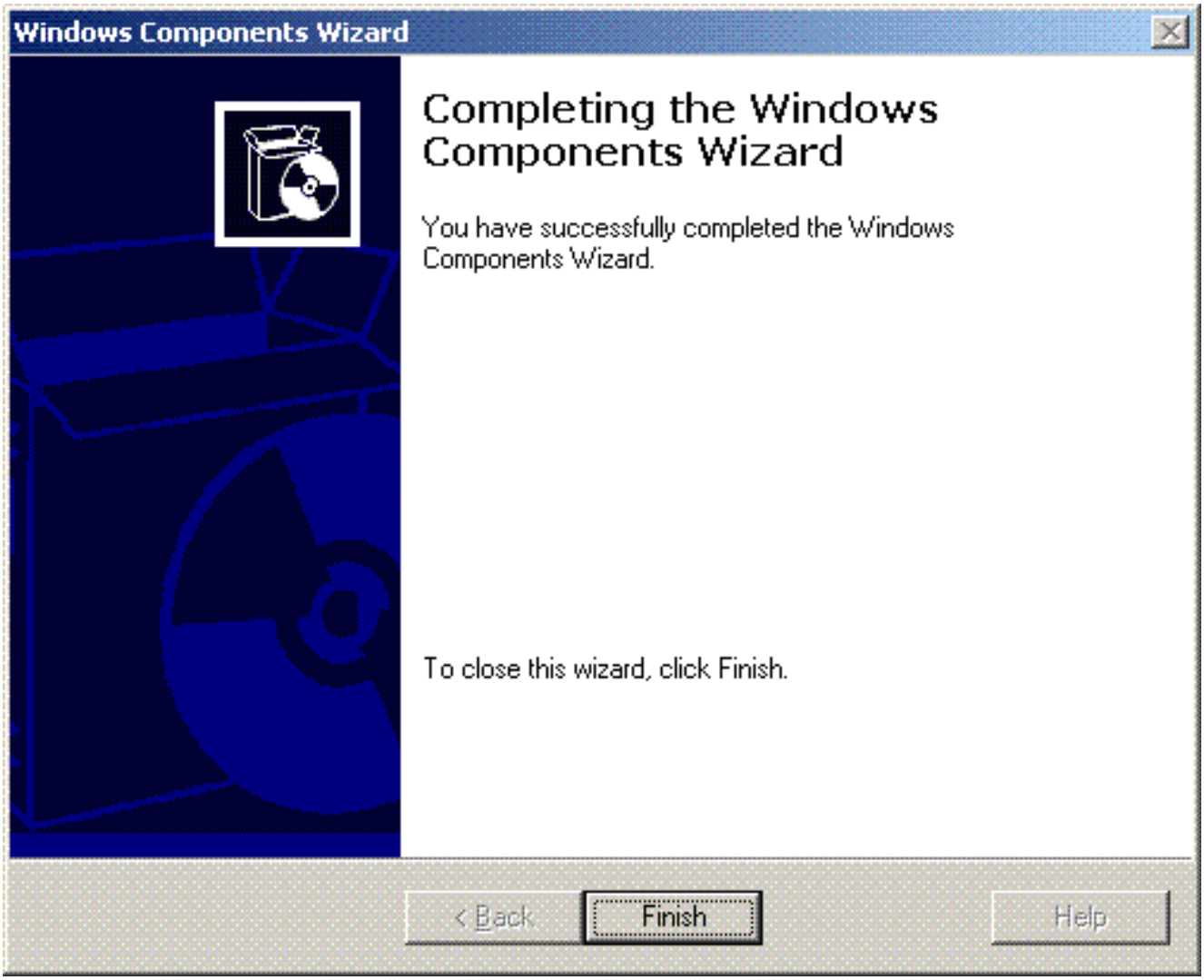
Complete estos pasos para instalar y configurar IAS en el servidor.

1. Haga clic en **Agregar o quitar programas** en el Panel de control.
2. Haga clic en **Agregar o quitar componentes de Windows**.
3. Elija **Networking Services** y haga clic en **Details**.
4. Elija **Internet Authentication Service**; haga clic en **OK**; y haga clic en

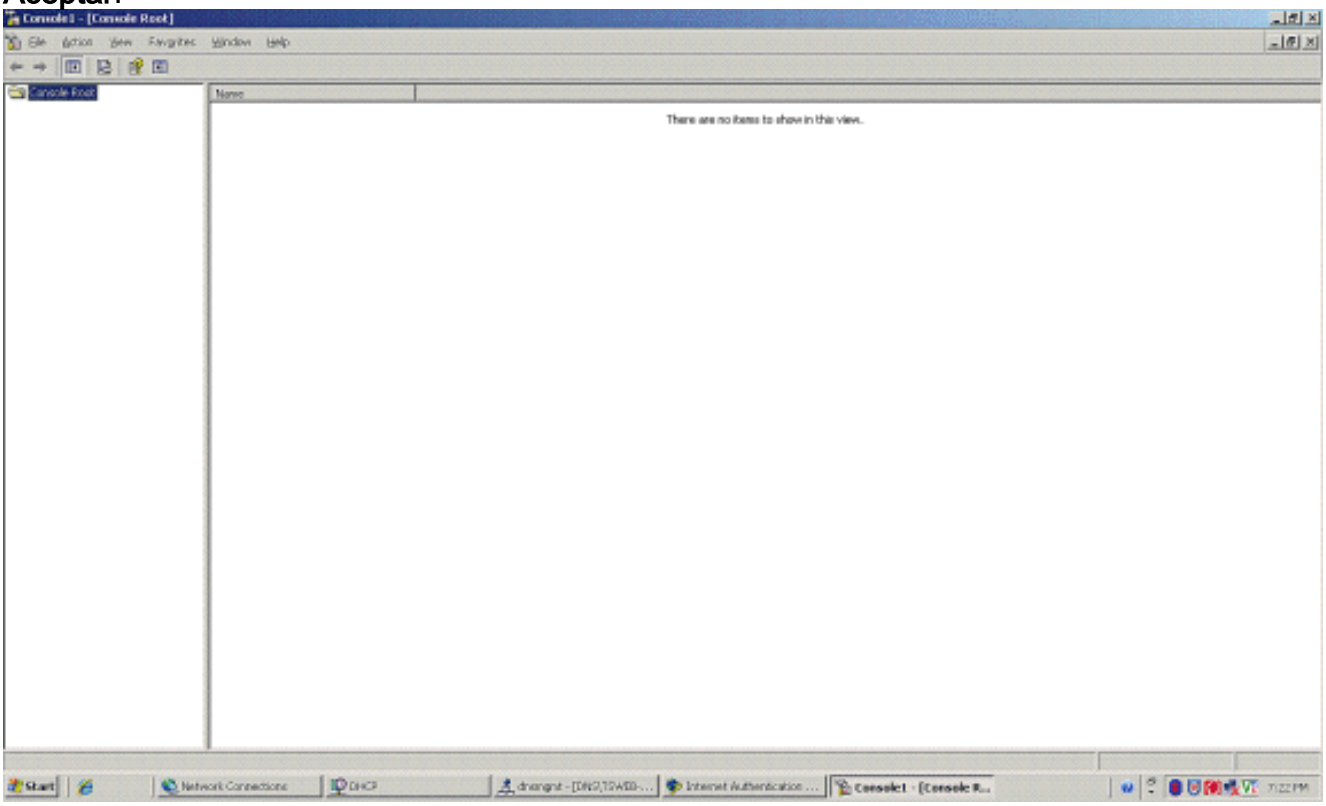


Next.

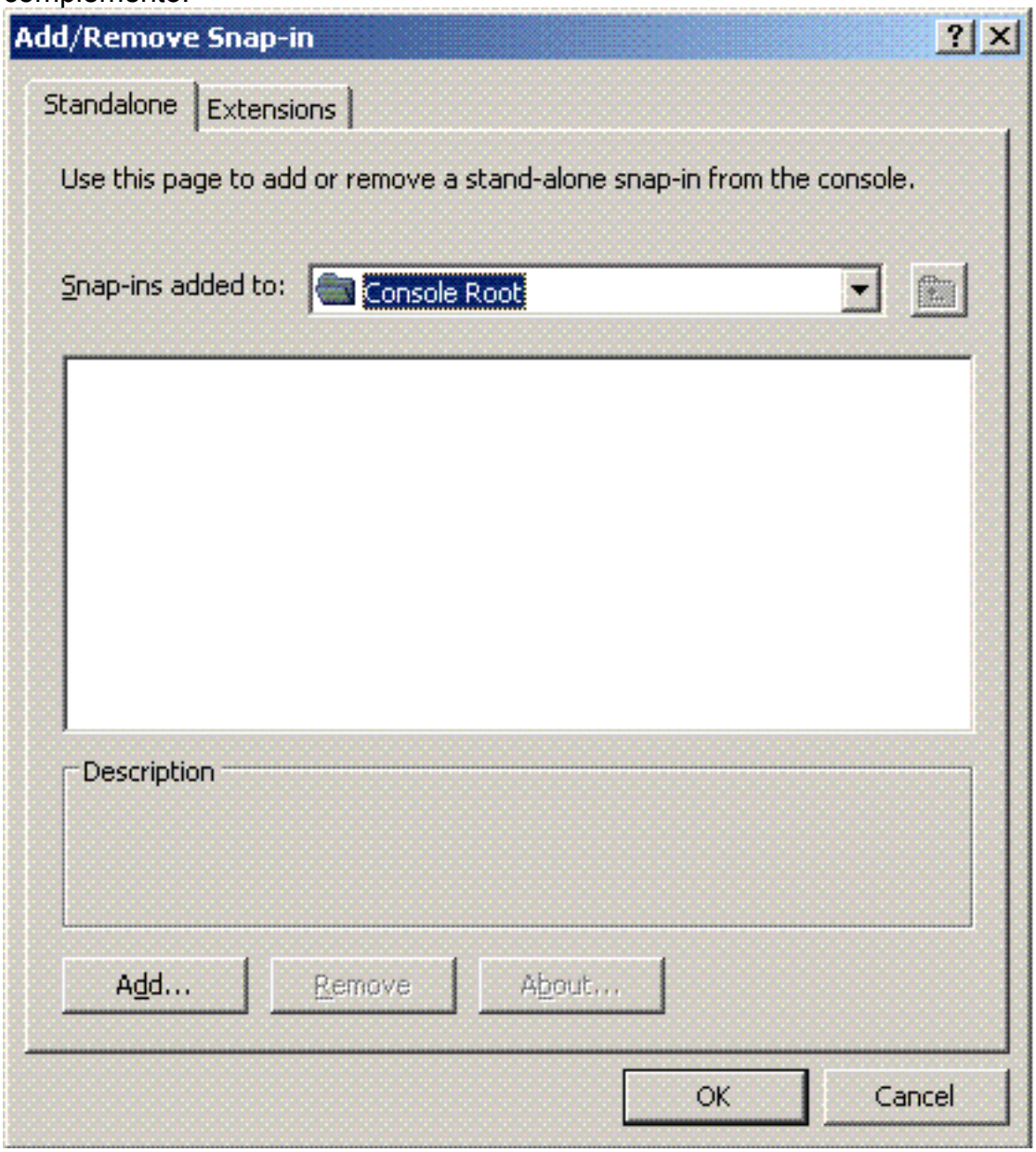
5. Haga clic en **Finalizar** para completar la instalación de IAS.



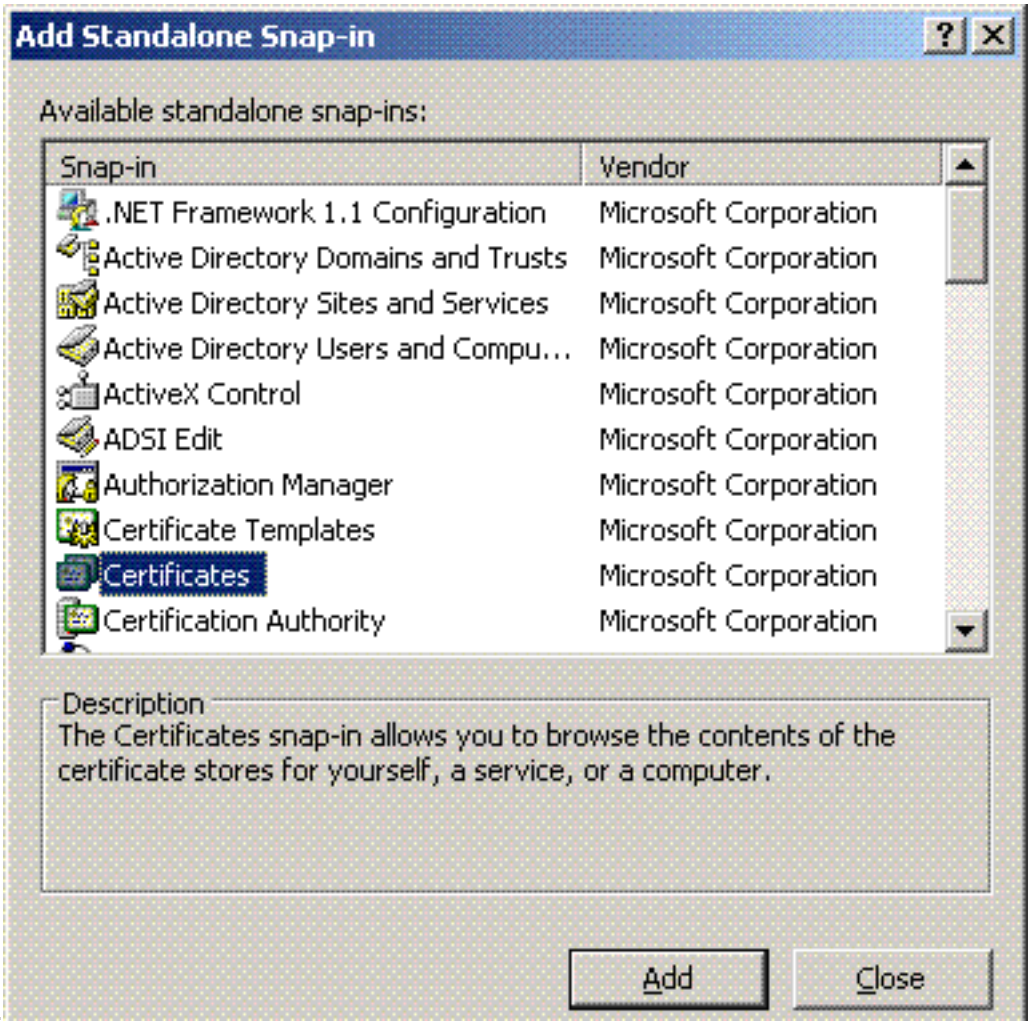
6. El paso siguiente es instalar el certificado de equipo para el Servicio de autenticación de Internet (IAS).
7. Haga clic en **Inicio**; haga clic en **Ejecutar**; escriba **mmc**; y haga clic en **Aceptar**.



8. Haga clic en **Consola** en el menú de archivos y, a continuación, elija **Agregar o quitar** complemento.
9. Haga clic en **Agregar** para agregar un complemento.

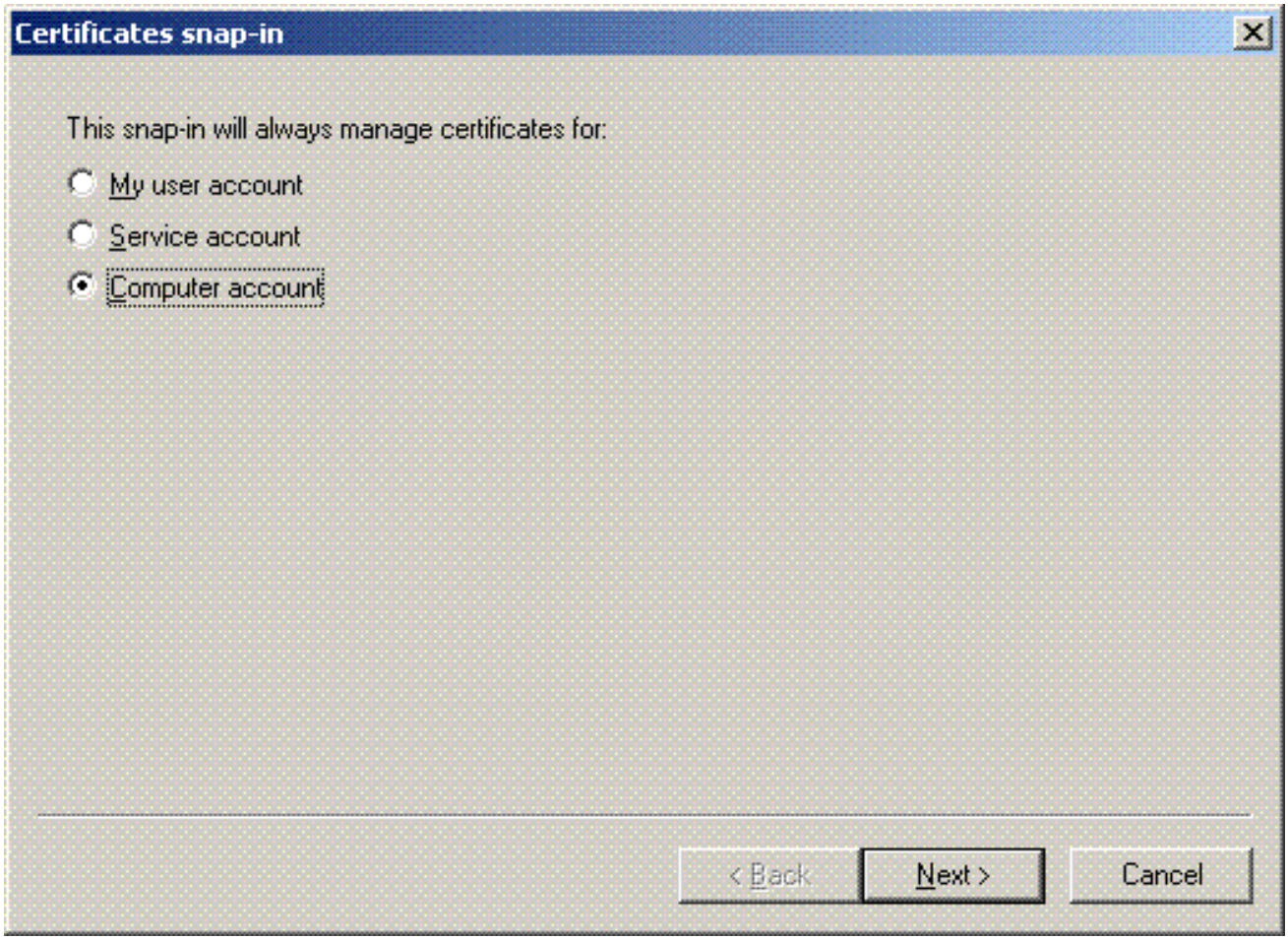


10. Elija **Certificados** en la lista de complementos y haga clic en

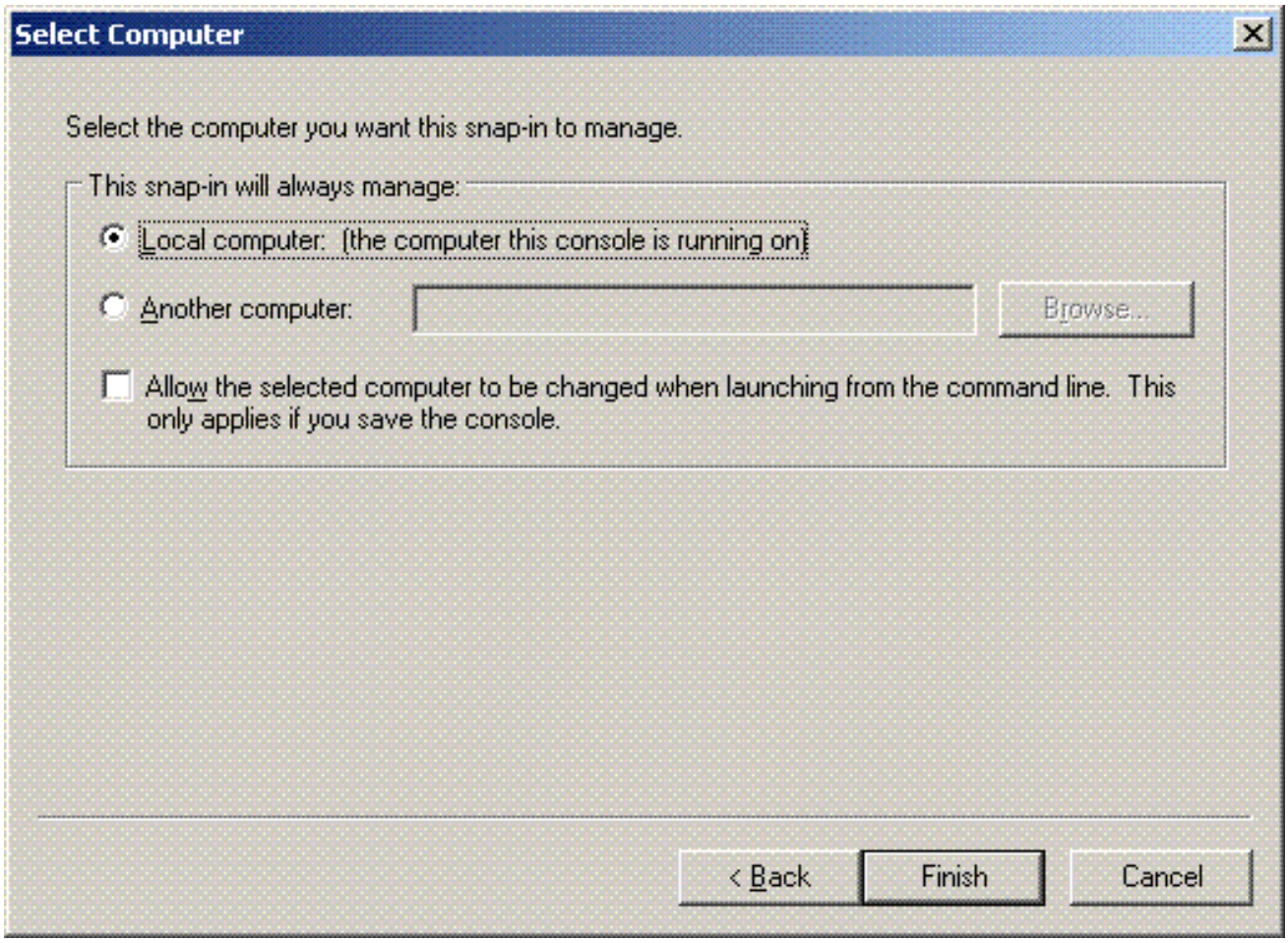


Agregar.

11. Elija **Computer account**, y haga clic en **Next**.

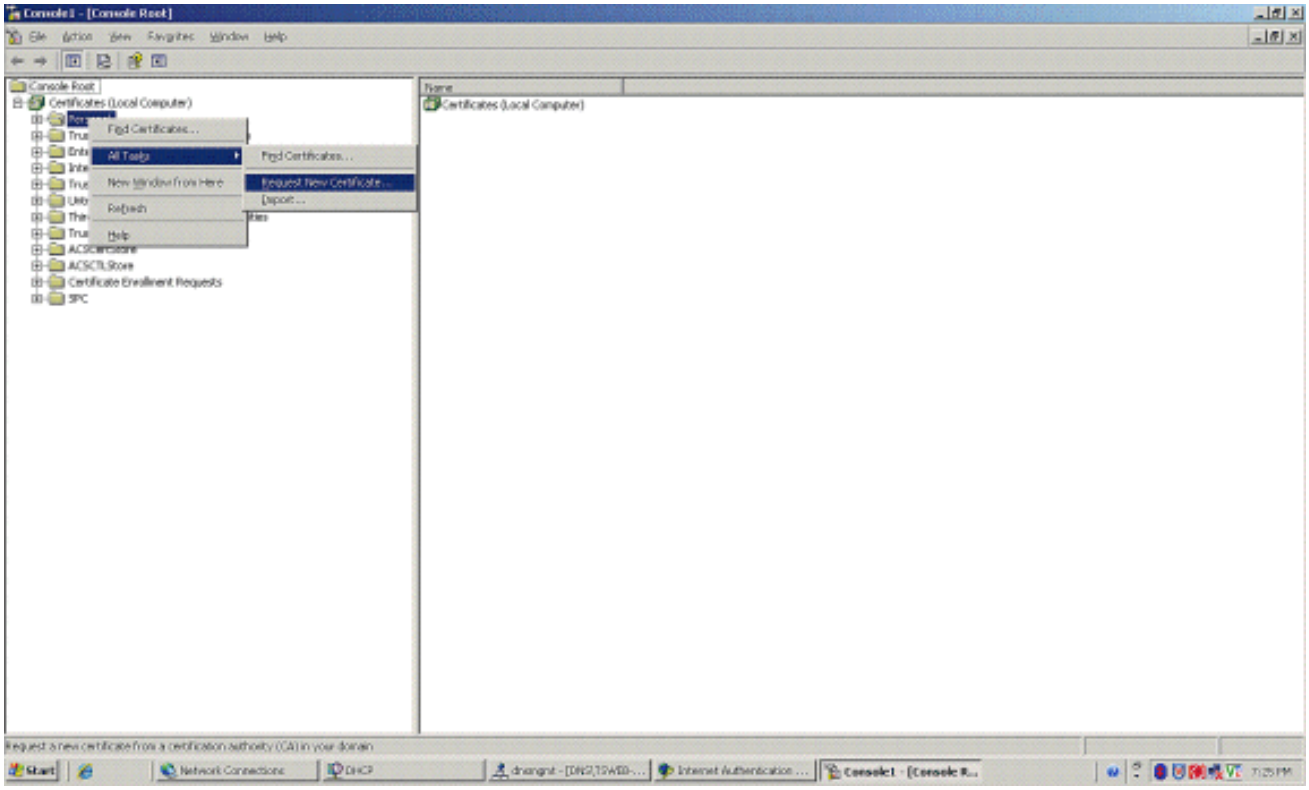


12. Elija **Local computer**, y haga clic en **Finish**.



13. Haga clic en **Cerrar** y luego en **Aceptar**.

14. Expanda **Certificados (Equipo local)**; haga clic con el botón derecho en **Carpeta personal**; elija **Todas las tareas** y después **Solicitar nuevo certificado**.

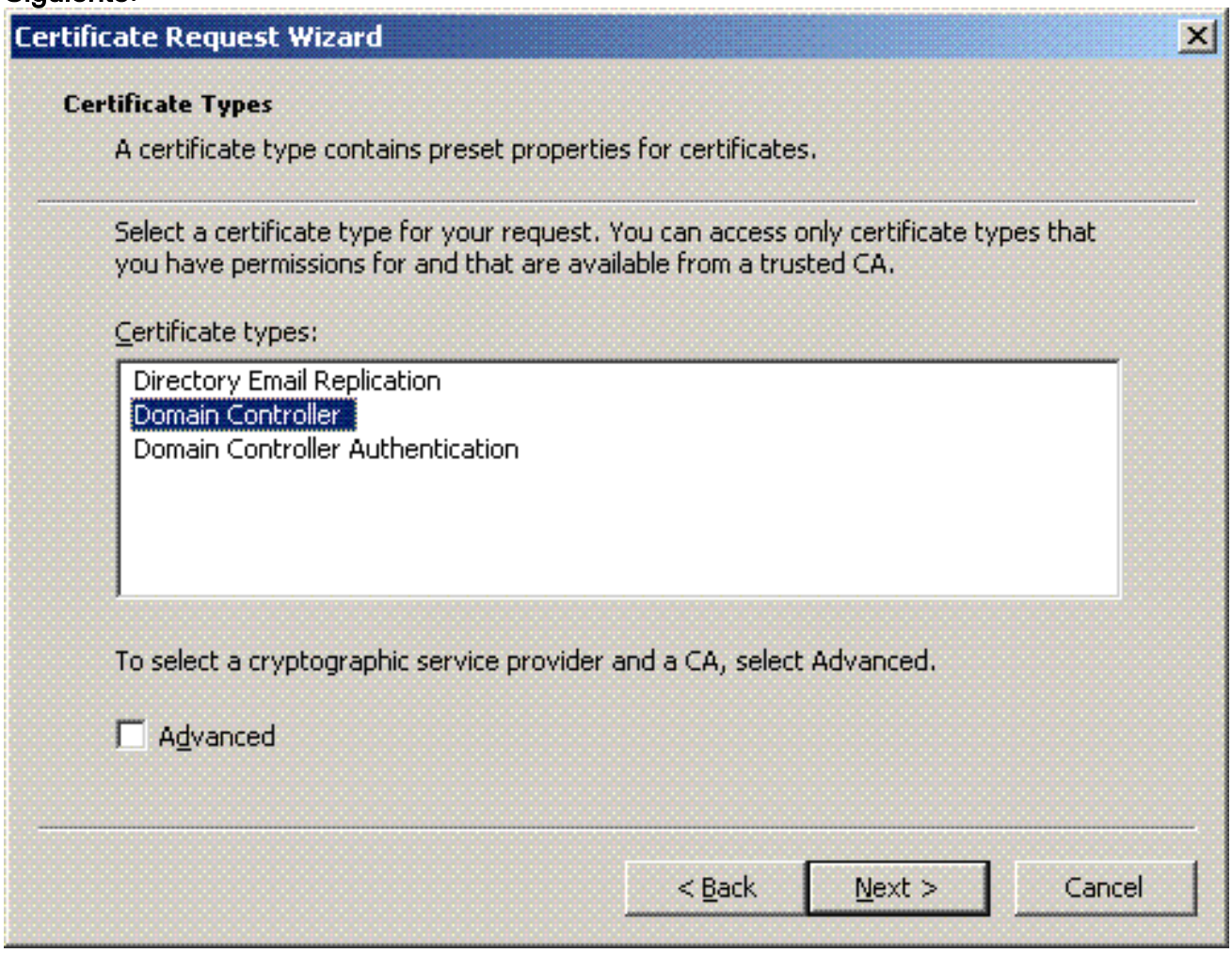


15. Haga clic en **Siguiente** en el ***Bienvenido al Asistente para solicitud de certificados***

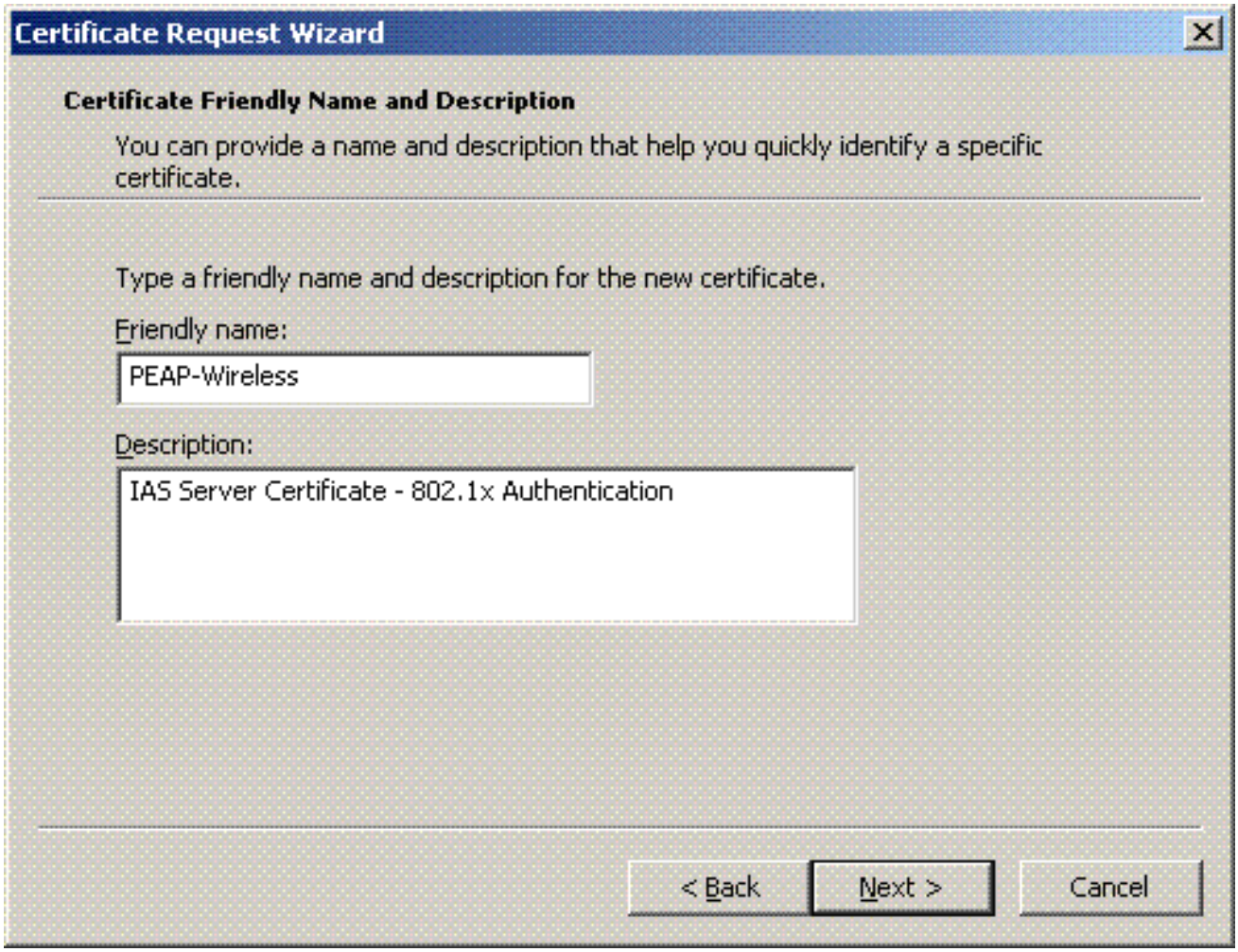
.

16. Elija la plantilla de certificado **Controlador de dominio** (si solicita un certificado de equipo en

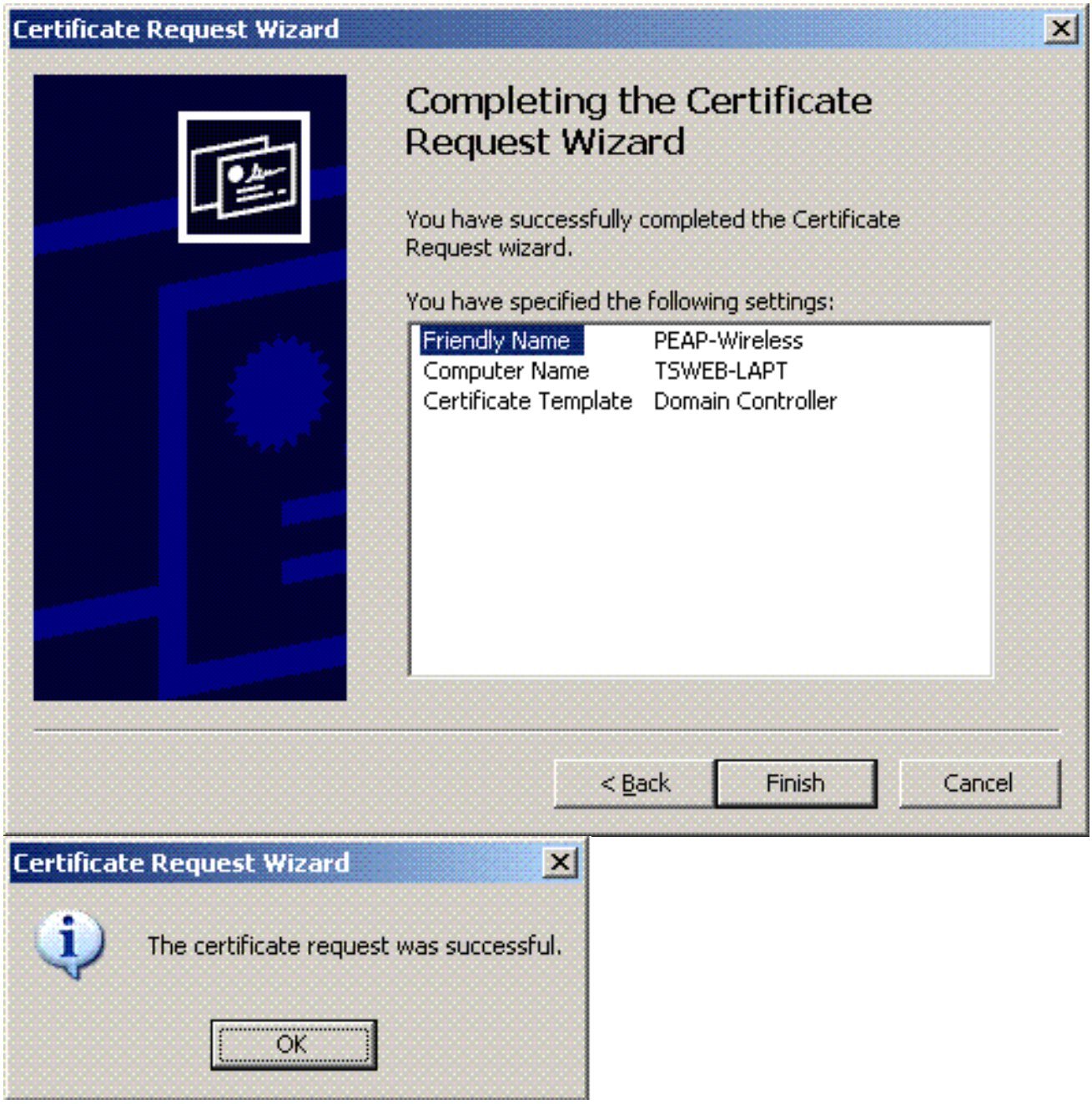
un servidor que no sea el DC, elija una plantilla de certificado de **equipo**) y haga clic en **Siguiente**.



17. Escriba un nombre y una descripción para el certificado.



18. Haga clic en **Finalizar** para completar el asistente para solicitud de certificación.

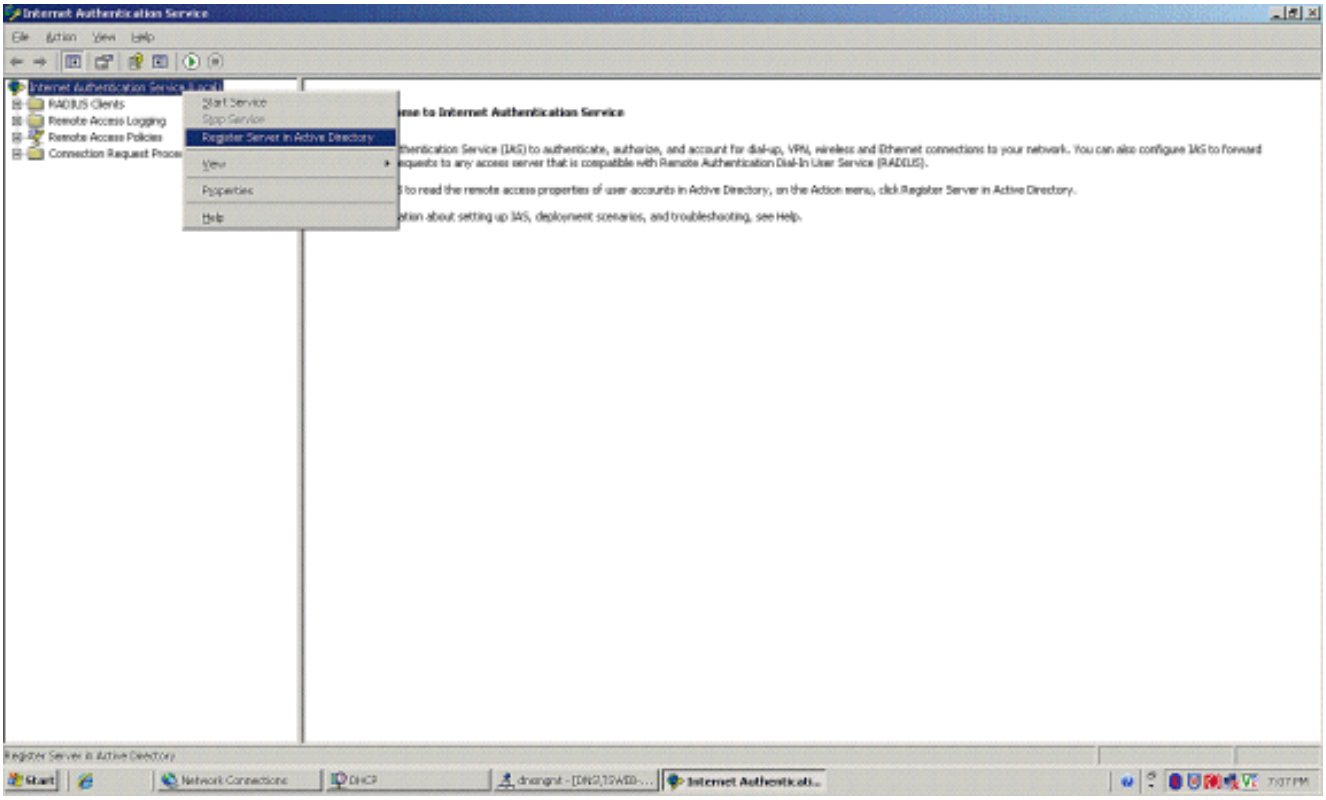


Configuración del servicio de autenticación de Internet para la autenticación PEAP-MS-CHAP v2

Ahora que ha instalado y solicitado un certificado para el IAS, configure el IAS para la autenticación.

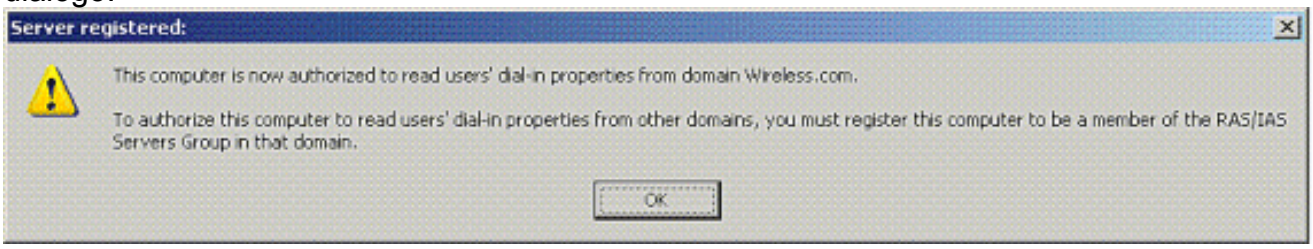
Complete estos pasos:

1. Haga clic en **Inicio > Programas > Herramientas administrativas**, y haga clic en **Servicio de autenticación de Internet** complemento.
2. Haga clic con el botón secundario en **Servicio de autenticación de Internet (IAS)** y, a continuación, haga clic en **Registrar servicio en Active Directory**.

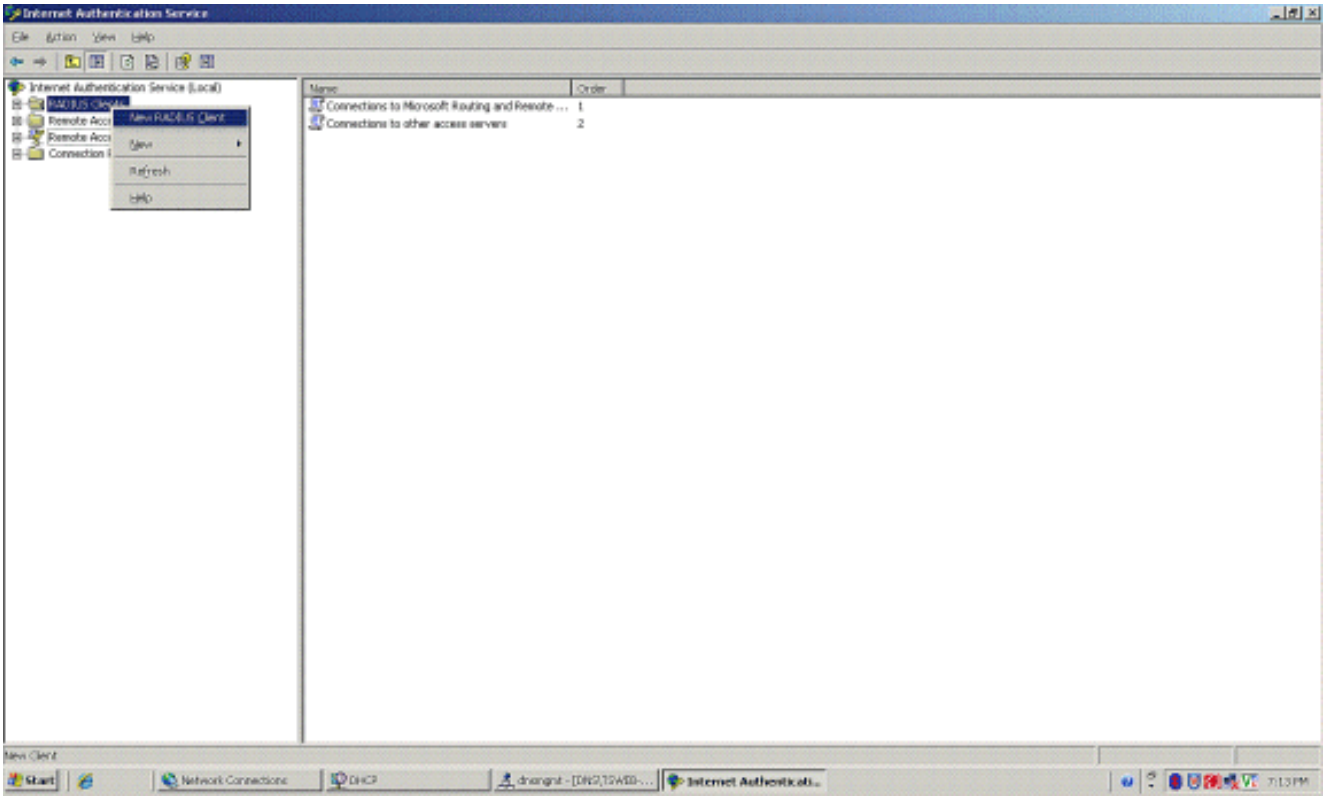


3. Aparecerá el cuadro de diálogo **Registrar servicio de autenticación de Internet en Active Directory**; haga clic en **Aceptar**. Esto permite a IAS autenticar a los usuarios en Active Directory.

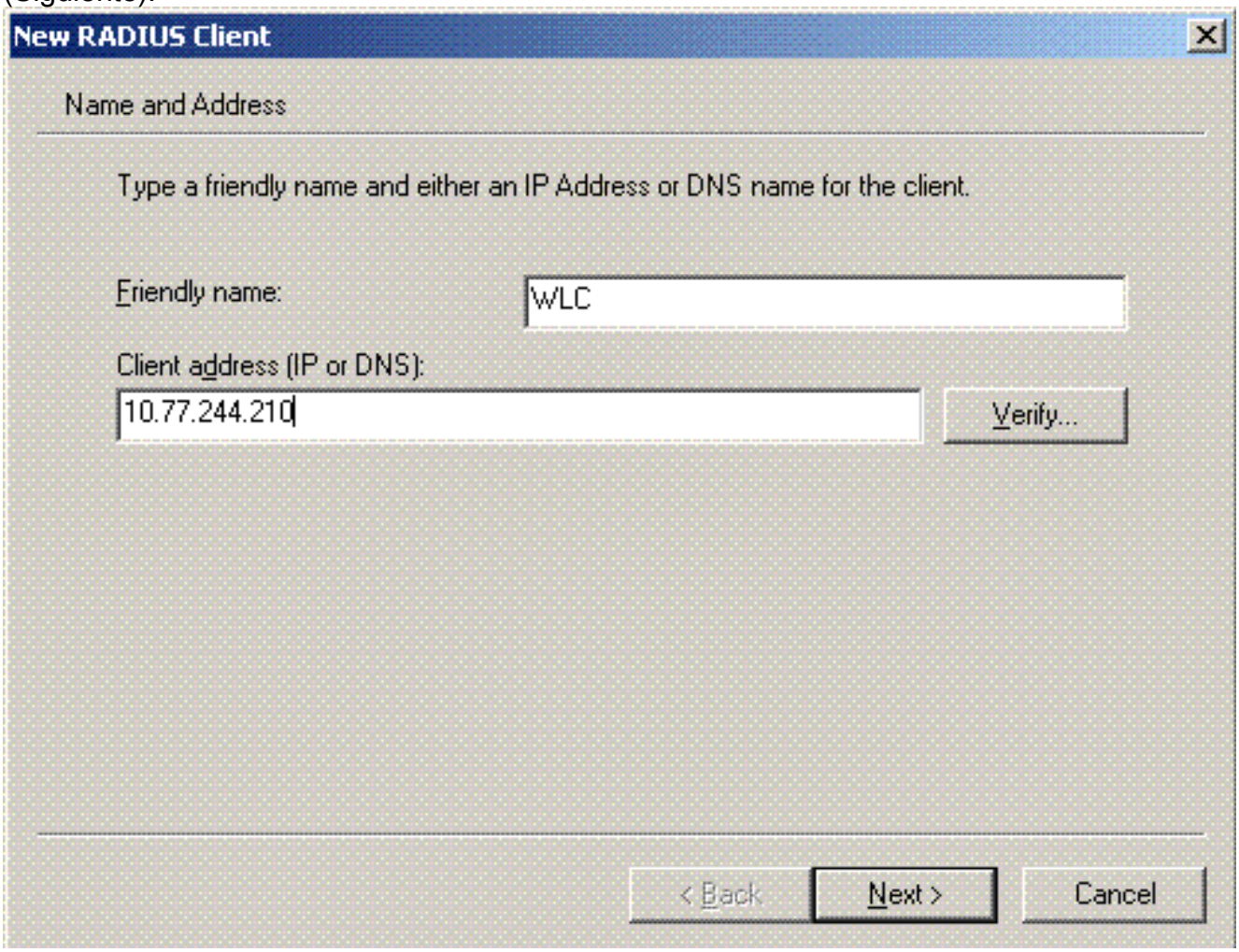
4. Haga clic en **Aceptar** en el siguiente cuadro de diálogo.



5. Agregue el controlador de LAN inalámbrica como cliente AAA en el servidor MS IAS.
6. Haga clic con el botón derecho del mouse en **RADIUS Clients**, y elija **New RADIUS Client**.

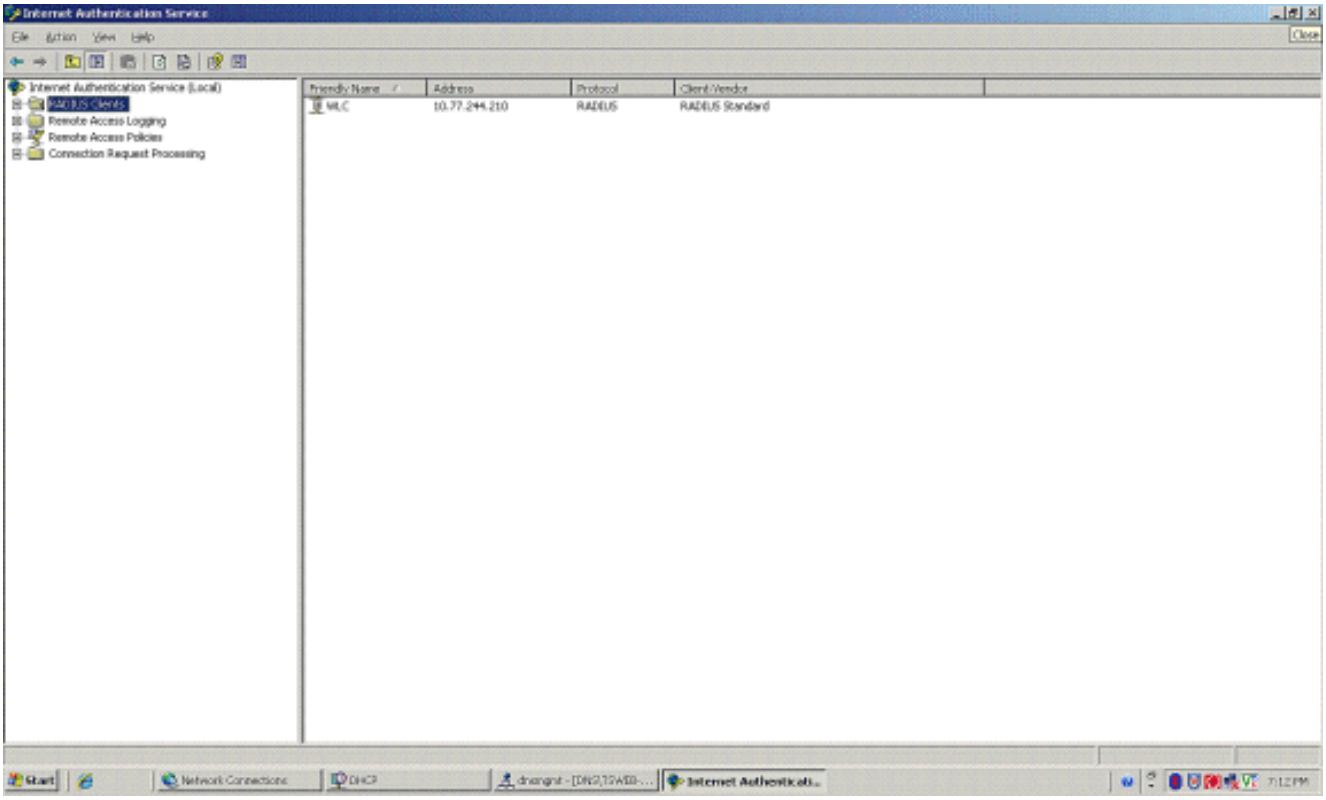


7. Escriba el nombre del cliente (WLC en este caso), e ingrese la dirección IP del WLC. Haga clic en Next
(Siguiente).

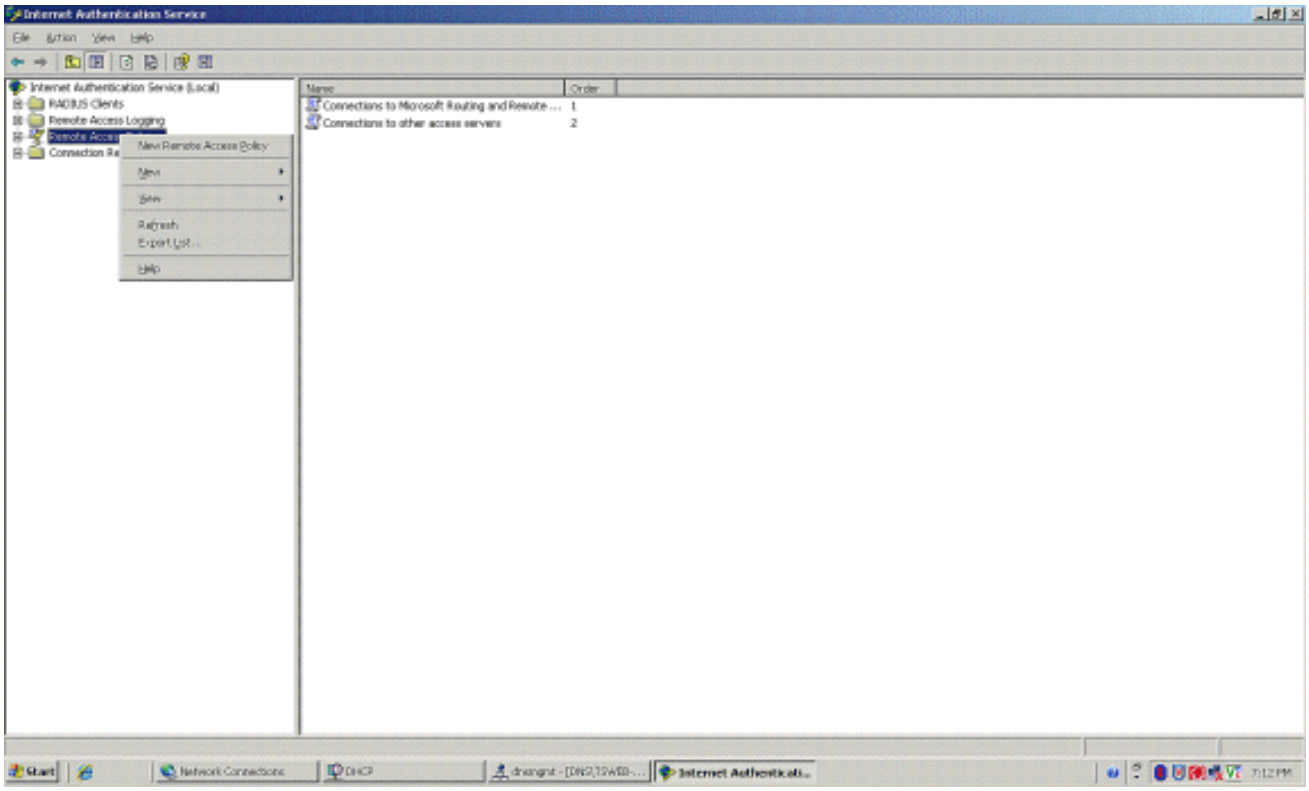


8. En la página siguiente, en Cliente-Proveedor, elija **Estándar RADIUS**, introduzca el secreto compartido y haga clic en **Finalizar**.

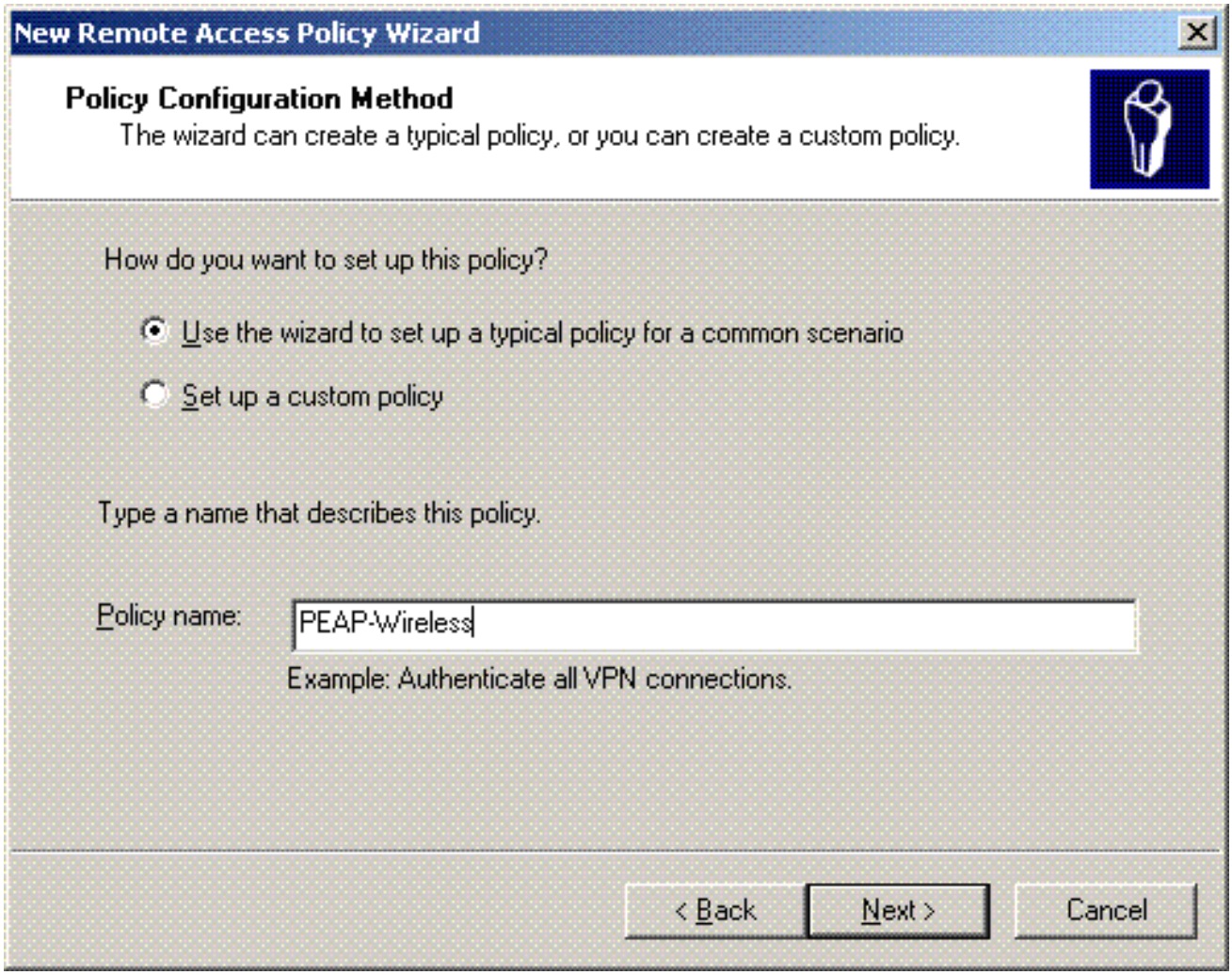
9. Observe que el WLC se agrega como un cliente AAA en el IAS.



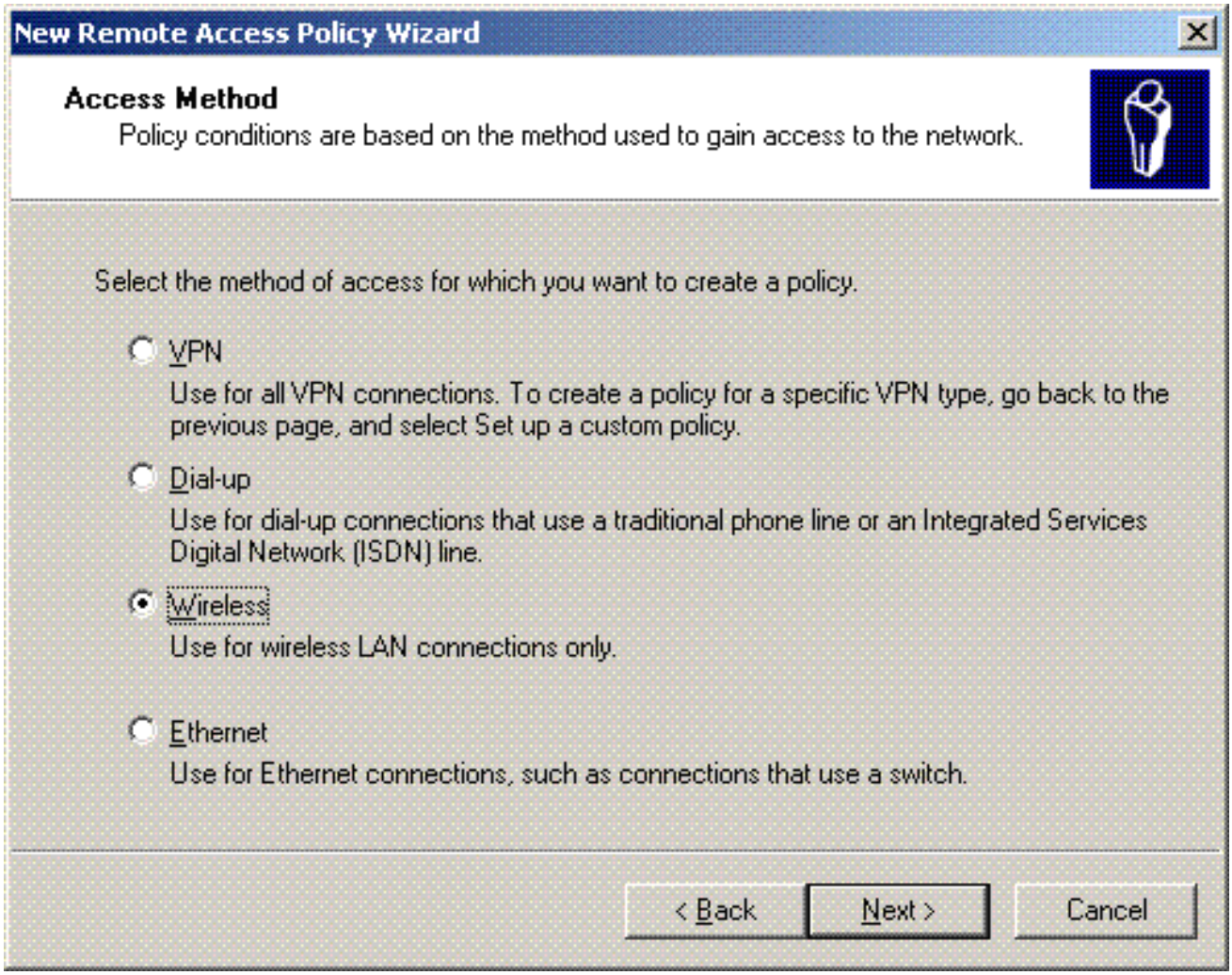
10. Cree una directiva de acceso remoto para los clientes.
11. Para hacerlo, haga clic con el botón derecho del mouse en **Directivas de acceso remoto**, y elija **Nueva directiva de acceso remoto**.



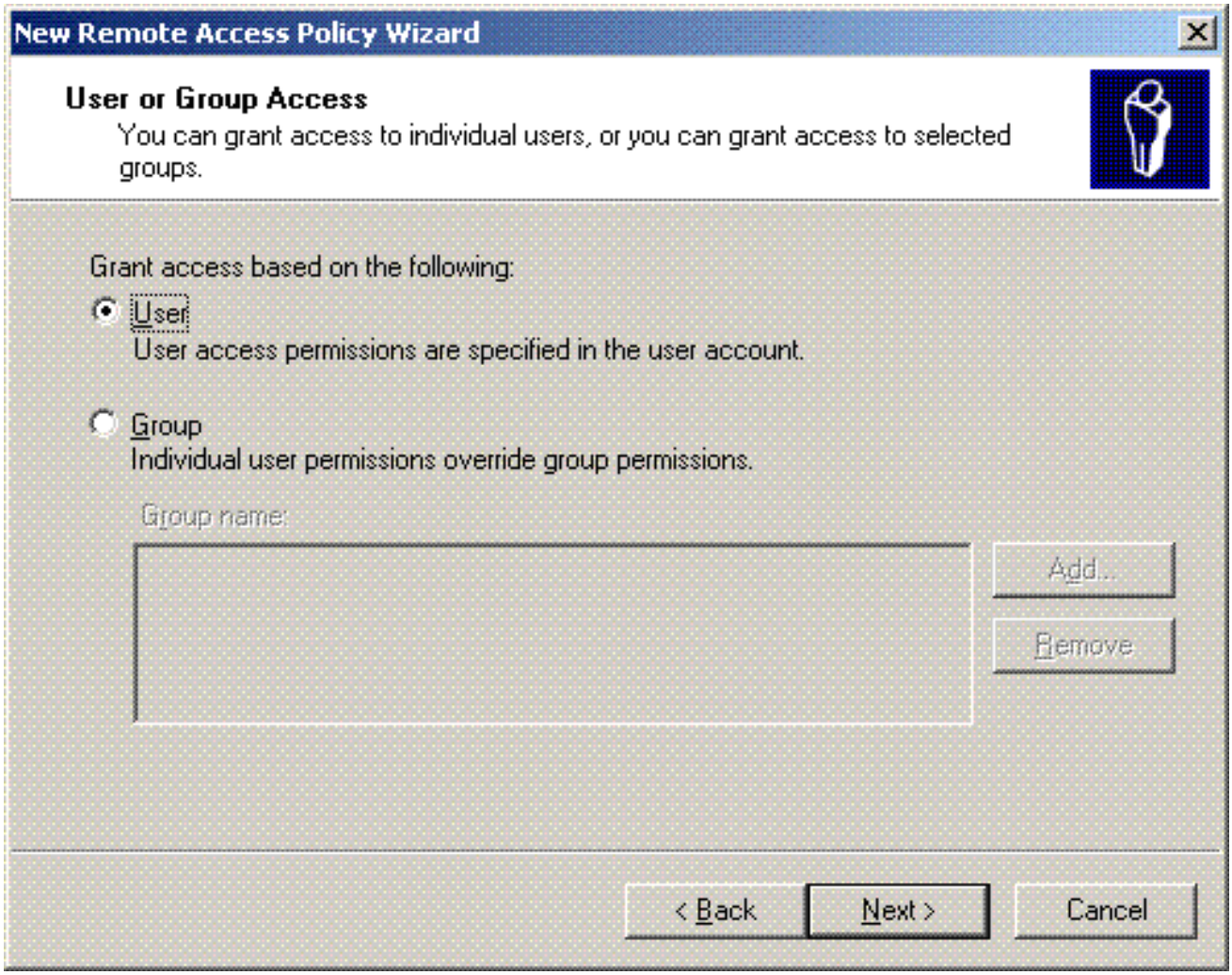
12. Escriba un nombre para la directiva de acceso remoto. En este ejemplo, utilice el nombre **PEAP**. Luego haga clic en Next (Siguiente).



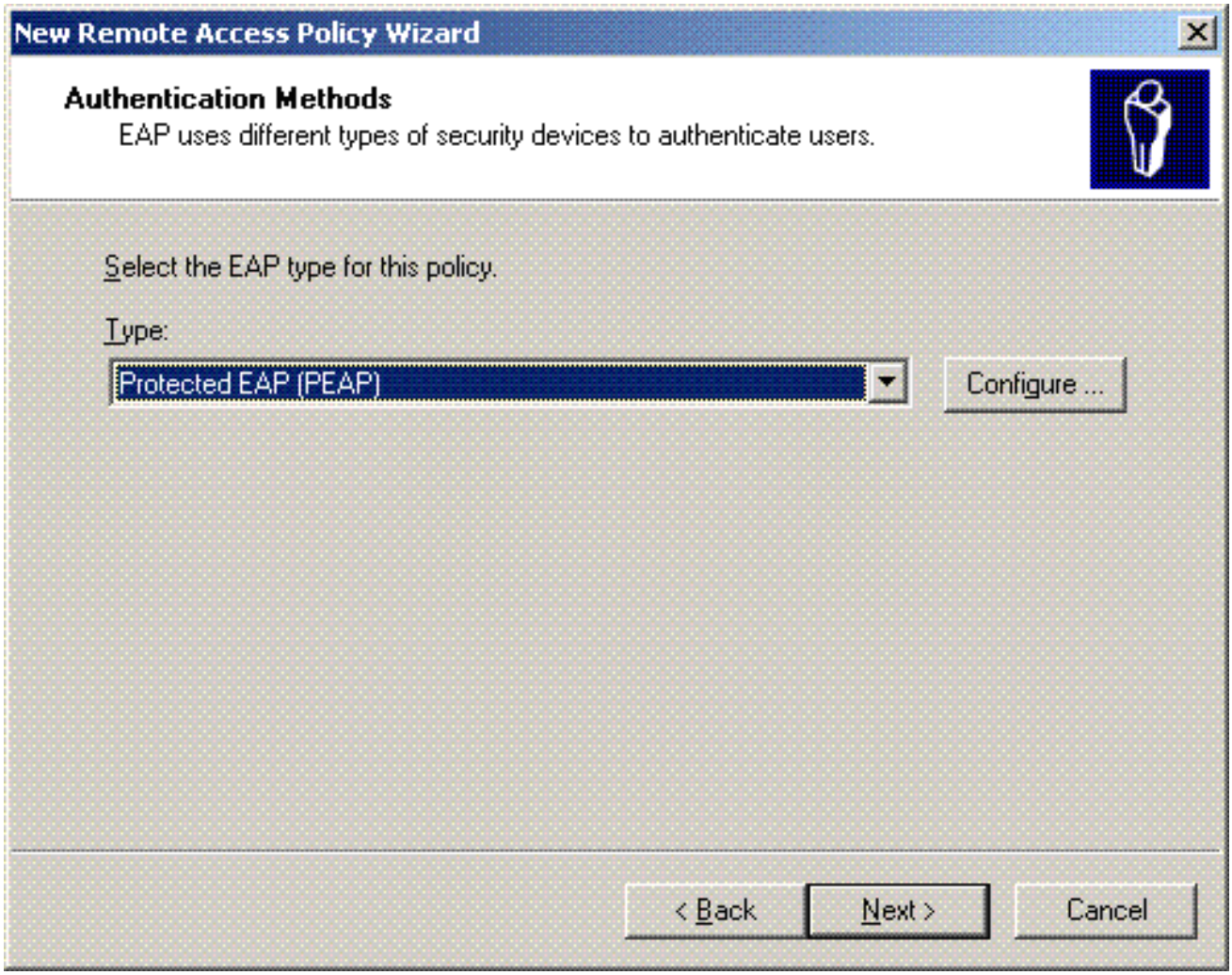
13. Elija los atributos de la política en función de sus requisitos. En este ejemplo, elija **Wireless**.



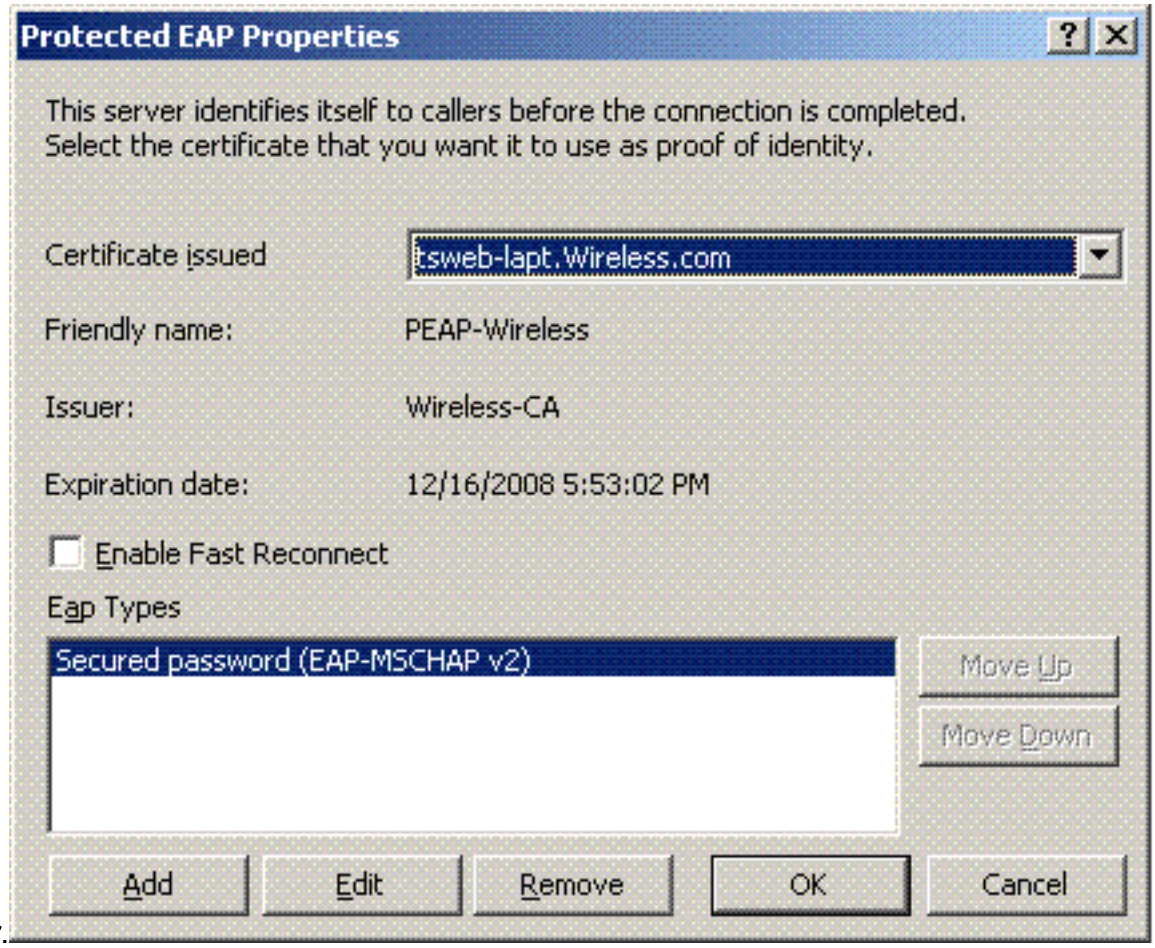
14. En la página siguiente, elija **Usuario** para aplicar esta directiva de acceso remoto a la lista de
usuarios.



15. En Métodos de autenticación, elija **EAP protegido (PEAP)** y haga clic en **Configurar**.

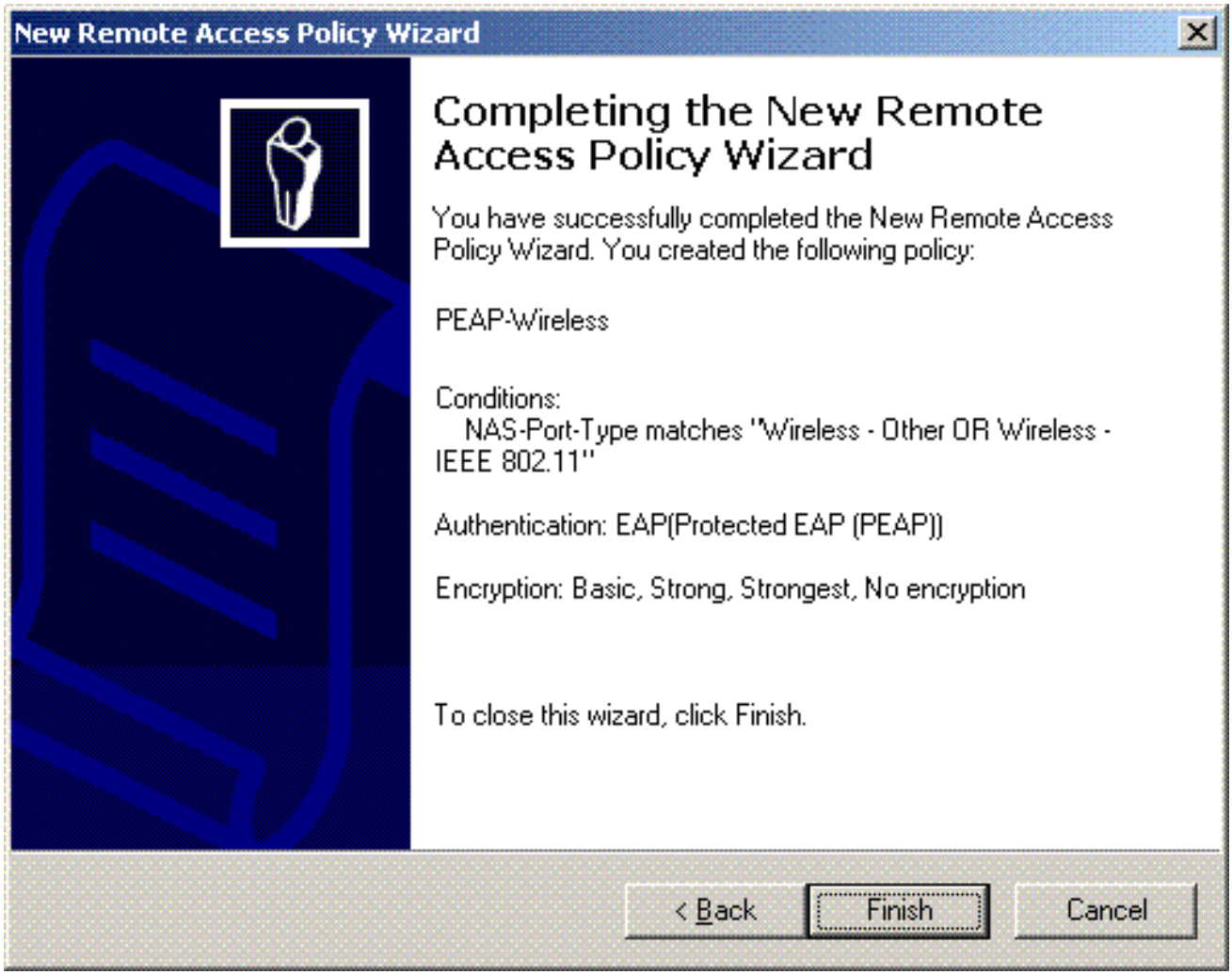


16. En la página **Propiedades de EAP protegido**, elija el certificado adecuado en el menú desplegable Certificado emitido y haga clic en

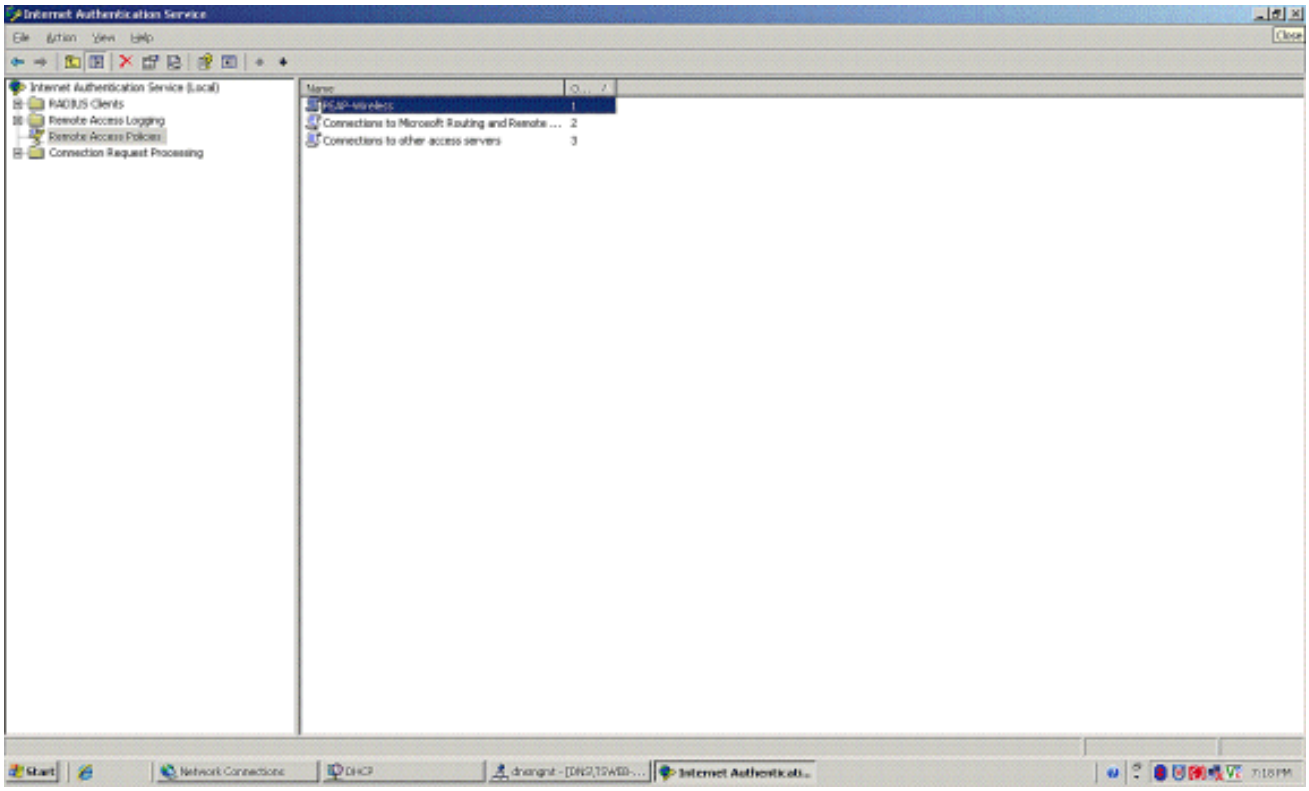


Aceptar.

17. Compruebe los detalles de la directiva de acceso remoto y haga clic en **Finalizar**.

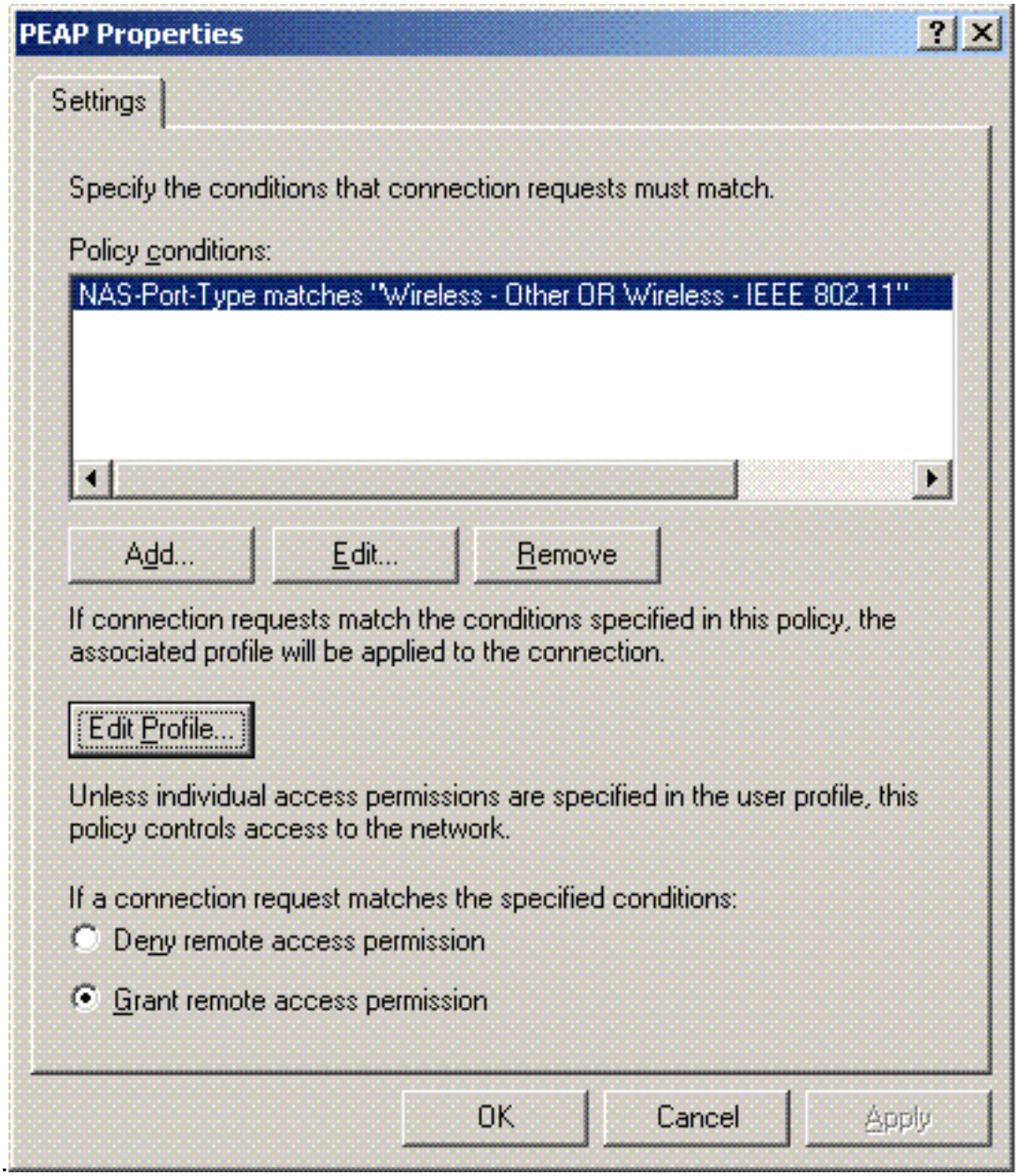


18. La directiva de acceso remoto se ha agregado a la lista.



19. Haga clic con el botón secundario en la directiva y haga clic en **Propiedades**. Elija **"Conceder permiso de acceso remoto"** en **"Si una solicitud de conexión coincide con las condiciones**

especificadas".

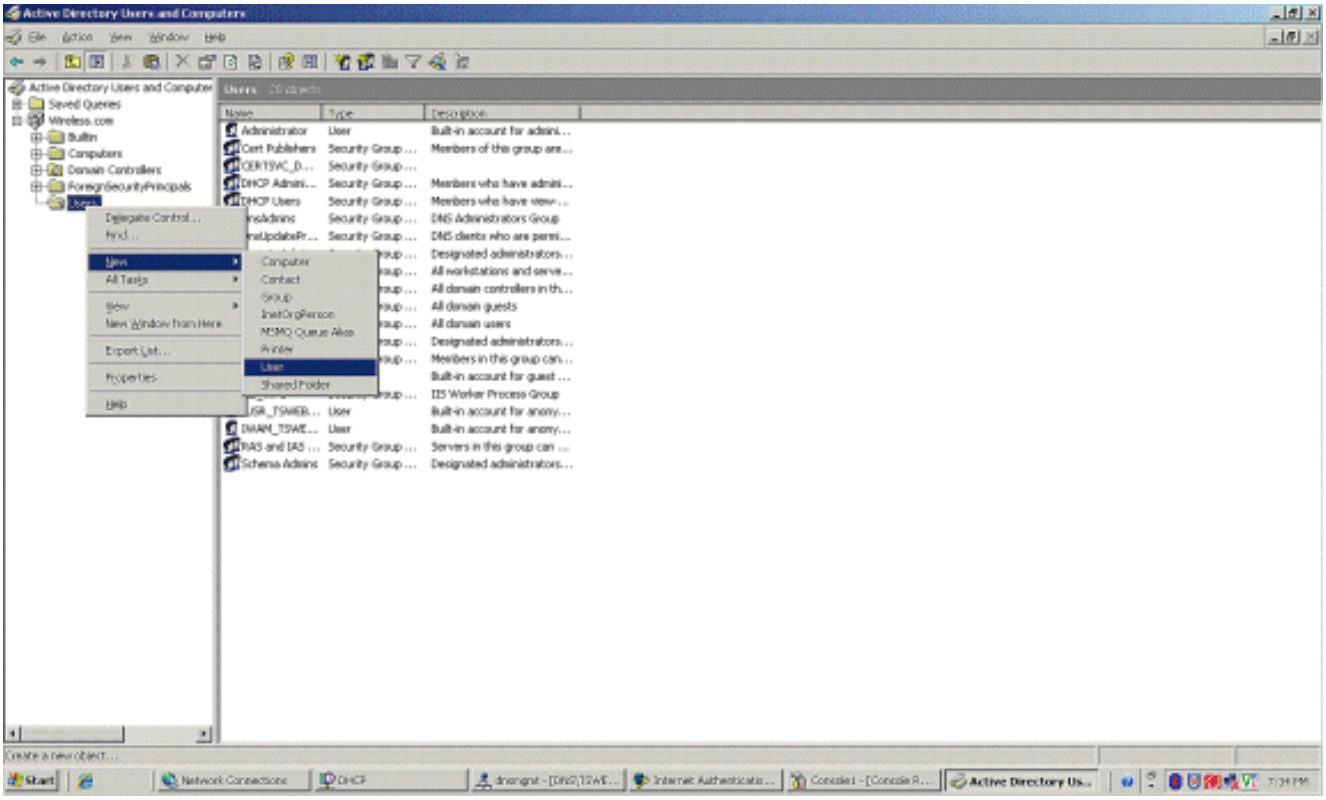


Agregar usuarios a Active Directory

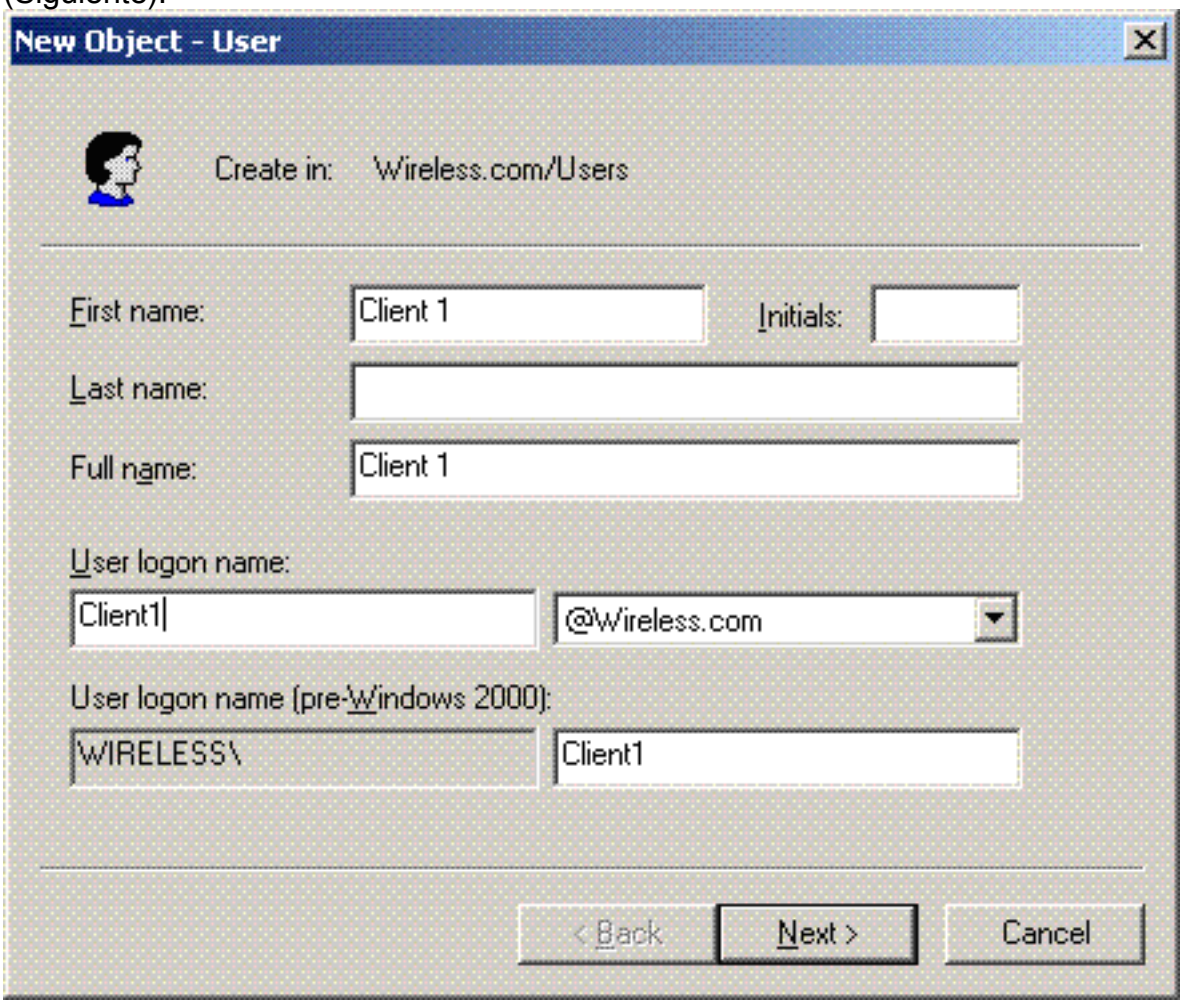
En esta configuración, la base de datos de usuarios se mantiene en Active Directory.

Para agregar usuarios a la base de datos de Active Directory, 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**.

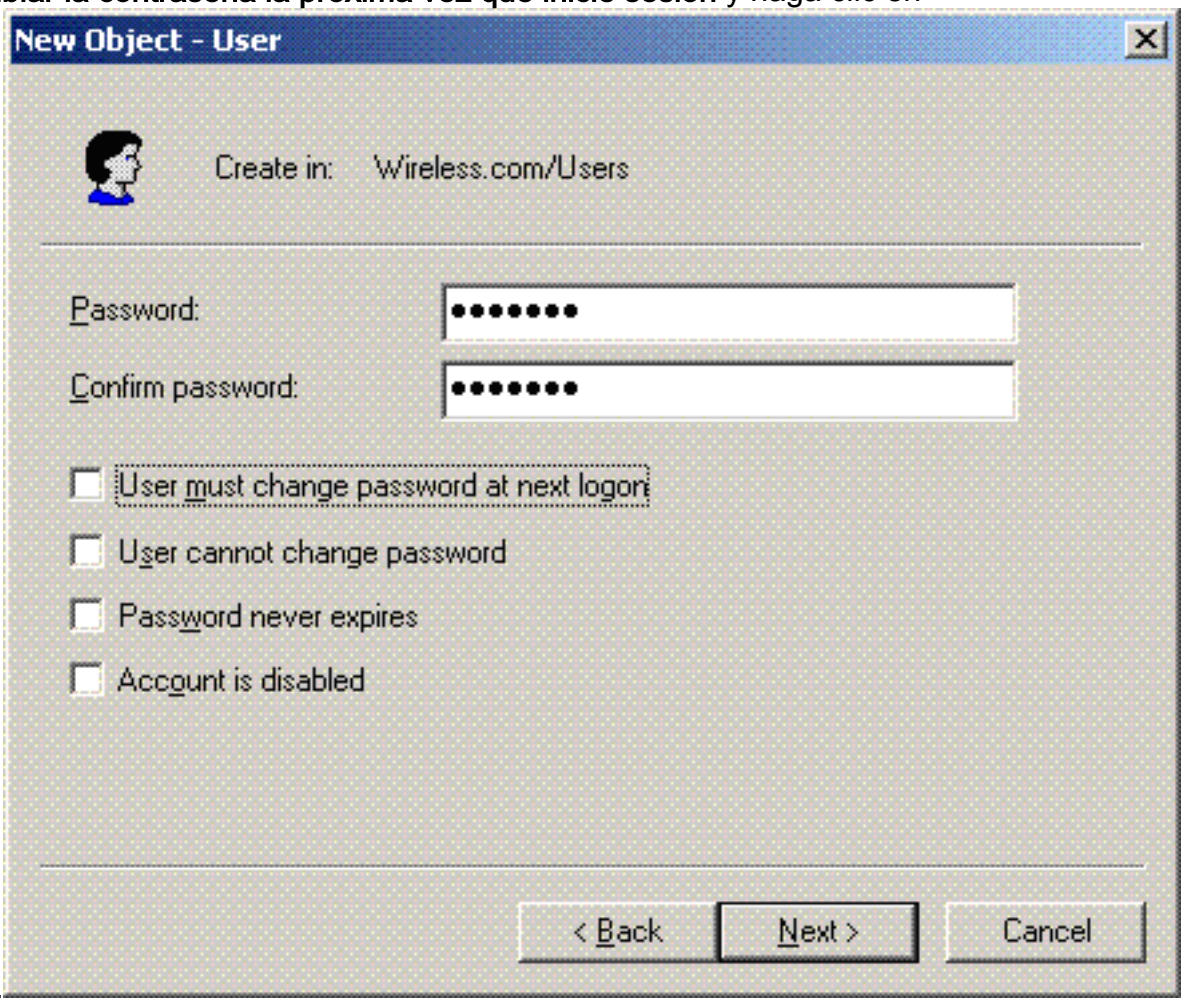


2. En el cuadro de diálogo Nuevo objeto - Usuario, escriba el nombre del usuario inalámbrico. En este ejemplo se utiliza el nombre **WirelessUser** en el campo First name (Nombre) y **WirelessUser** en el campo User logon name (Nombre de inicio de sesión de usuario). Haga clic en Next
(Siguiente).

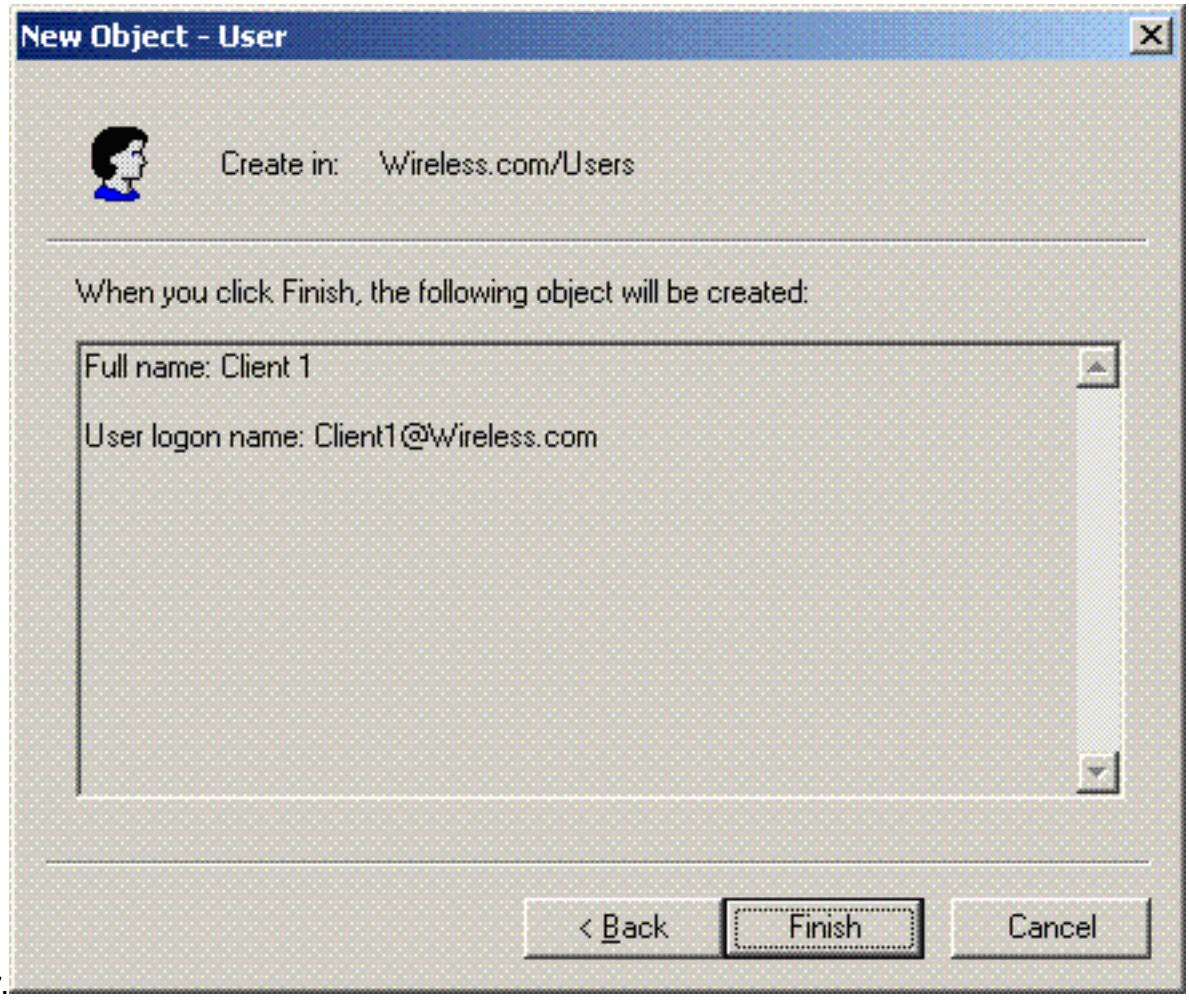


3. En el cuadro de diálogo Nuevo objeto - Usuario, escriba la contraseña que desee en los

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.

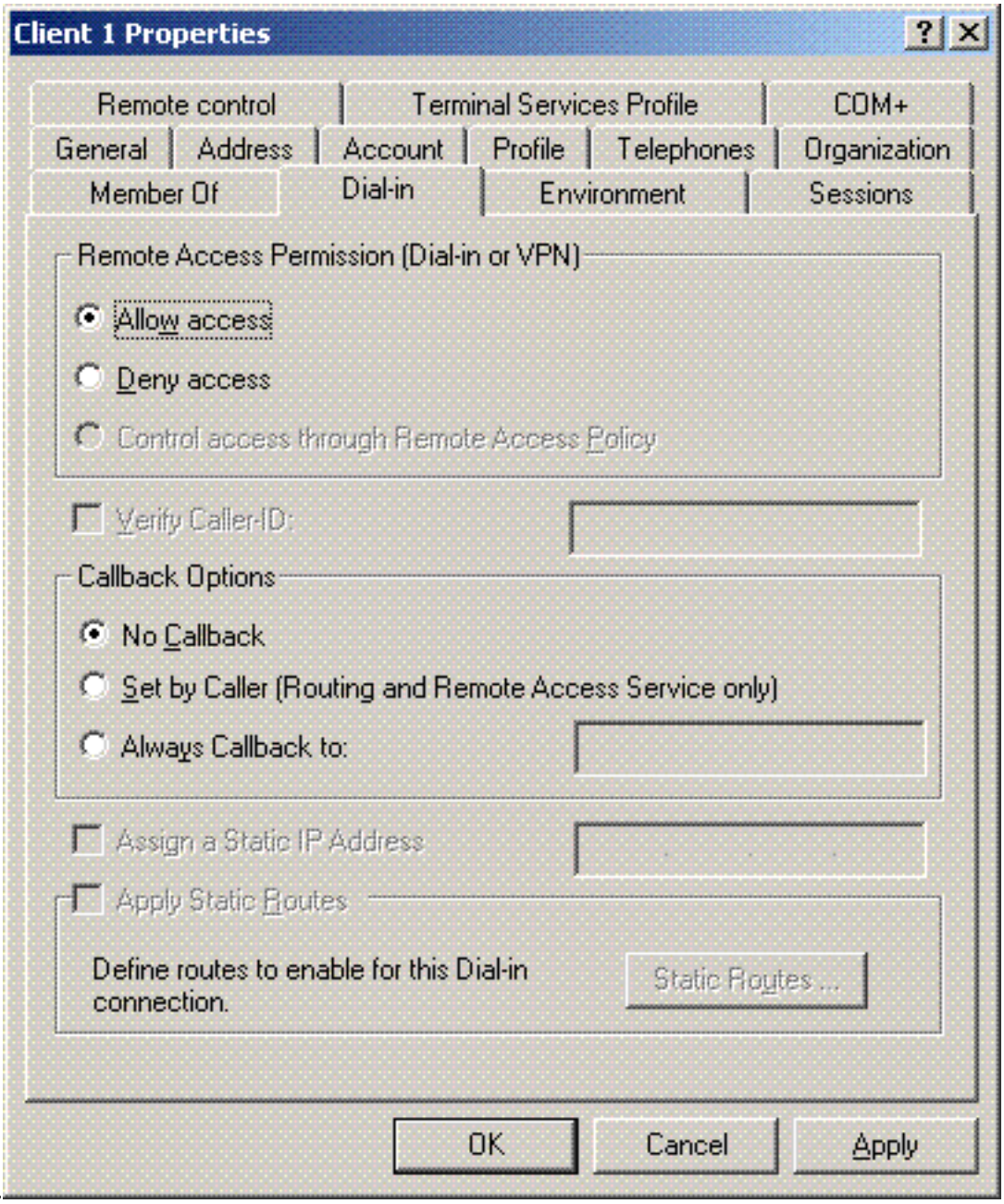
5. Repita los pasos del 2 al 4 para crear cuentas de usuario adicionales.

Permitir el acceso inalámbrico a los usuarios

Complete estos pasos:

1. En el árbol de consola de Usuarios y equipos de Active Directory, haga clic en la carpeta **Usuarios**; haga clic con el botón secundario del mouse en **WirelessUser**; haga clic en **Propiedades** y, a continuación, vaya a la pestaña **Marcado de entrada**.
2. Elija **Allow access**, y haga clic en

OK.



Configuración del controlador de LAN inalámbrica y los puntos de acceso ligeros

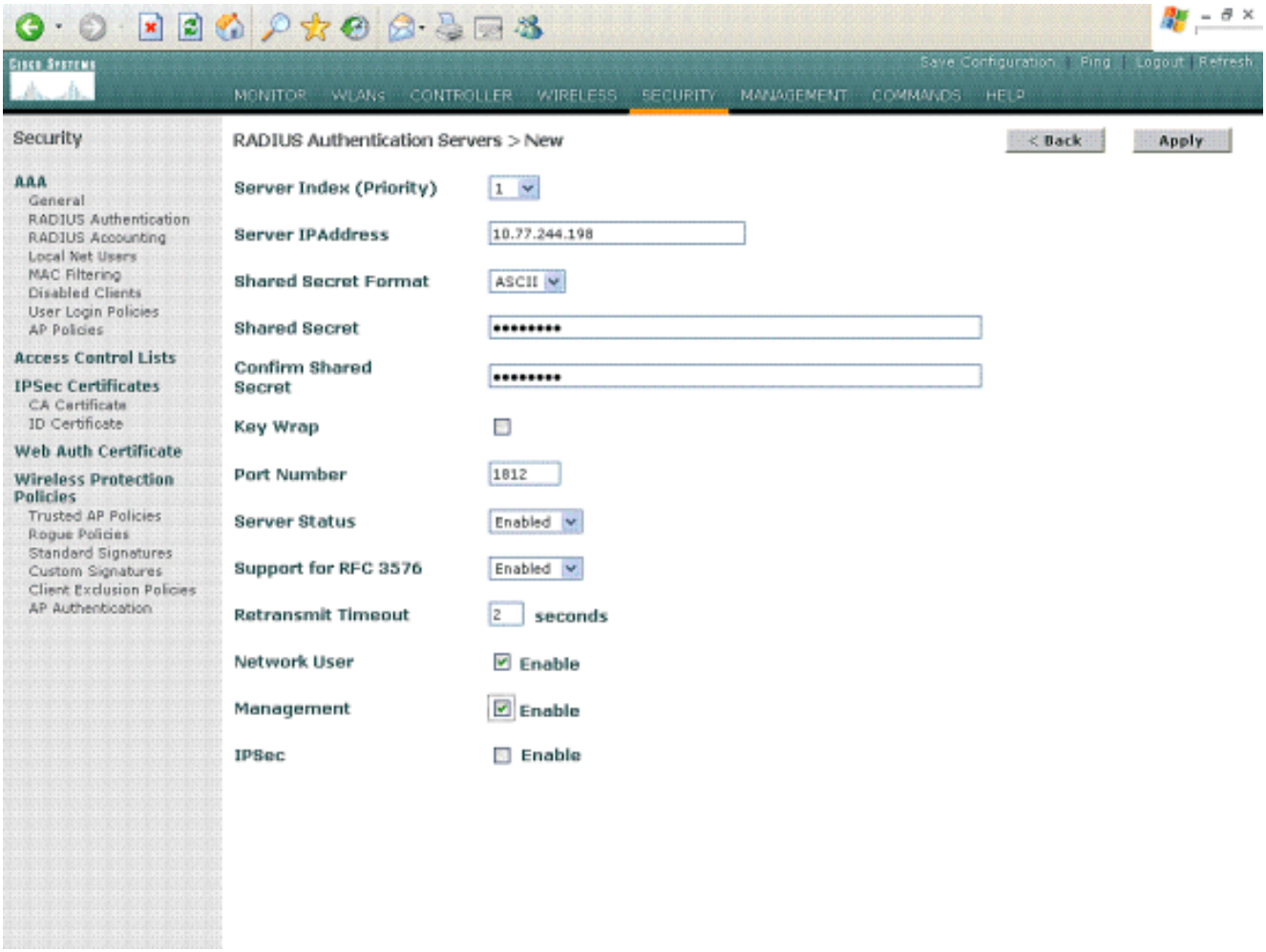
Ahora configure los dispositivos inalámbricos para esta configuración. Esto incluye la configuración de los controladores de LAN inalámbrica, los puntos de acceso ligeros y los clientes inalámbricos.

Configure el WLC para la autenticación RADIUS a través del servidor RADIUS de MS IAS

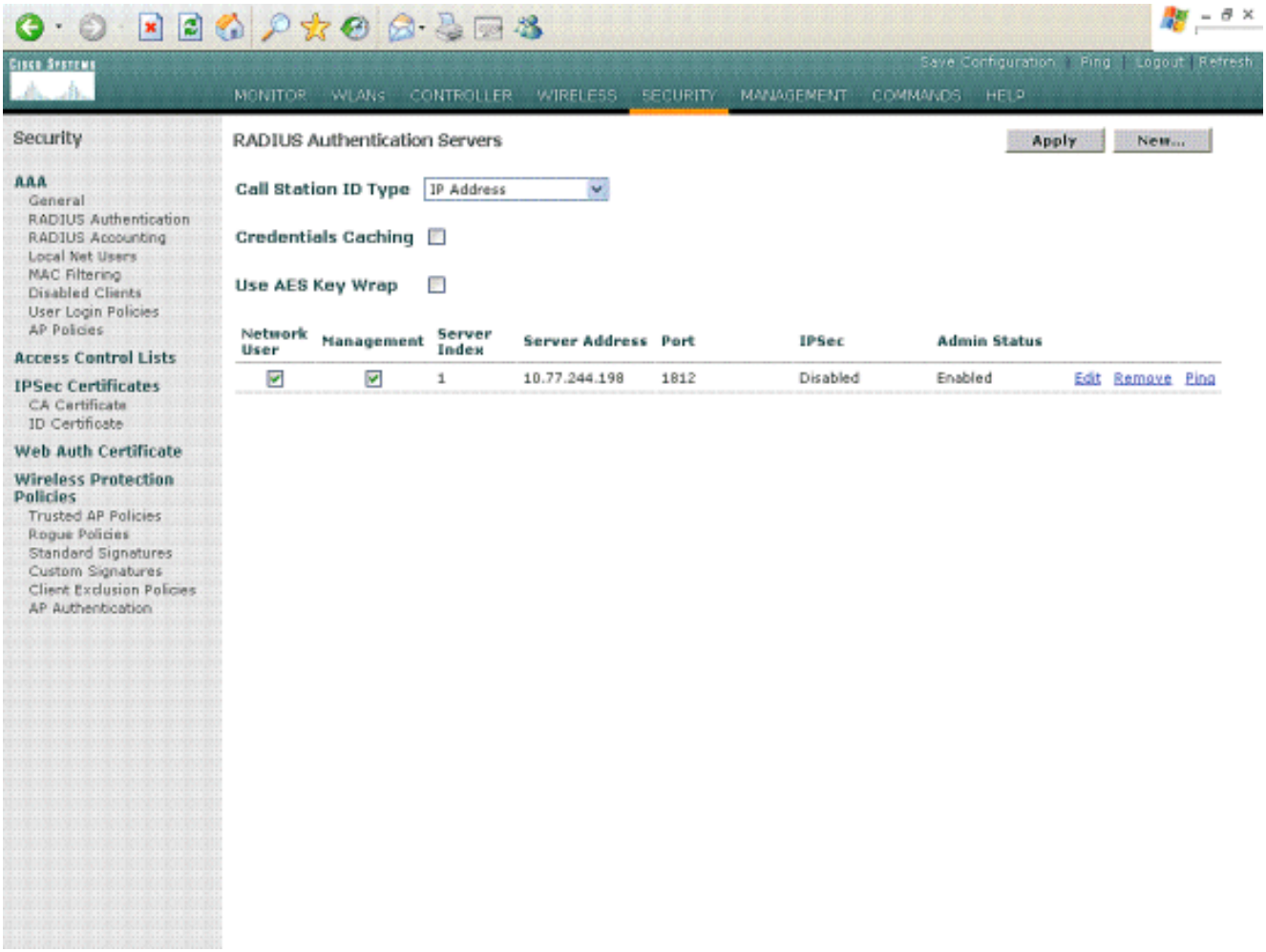
Primero configure el WLC para utilizar MS IAS como el servidor de autenticación. El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario y proporciona acceso a los clientes inalámbricos. Para ello, agregue el servidor MS IAS como servidor RADIUS en la página **Seguridad > Autenticación RADIUS**.

Complete estos pasos:

1. Elija **Security** y **RADIUS Authentication** de la GUI del controlador para mostrar la página RADIUS Authentication Servers. Luego haga clic en **Nuevo** para definir un servidor RADIUS.



2. Defina los parámetros del servidor RADIUS en la página **RADIUS Authentication Servers > New**. Estos parámetros incluyen la dirección IP del servidor RADIUS, el secreto compartido, el número de puerto y el estado del servidor. Las casillas de verificación Administración y usuario de red determinan si la autenticación basada en RADIUS se aplica a la administración y a los usuarios de red. Este ejemplo utiliza MS IAS como servidor RADIUS con la dirección IP
10.77.244.198.



3. Haga clic en Apply (Aplicar).
4. El servidor MS IAS se ha agregado al WLC como un servidor Radius y se puede utilizar para autenticar clientes inalámbricos.

Configuración de una WLAN para los clientes

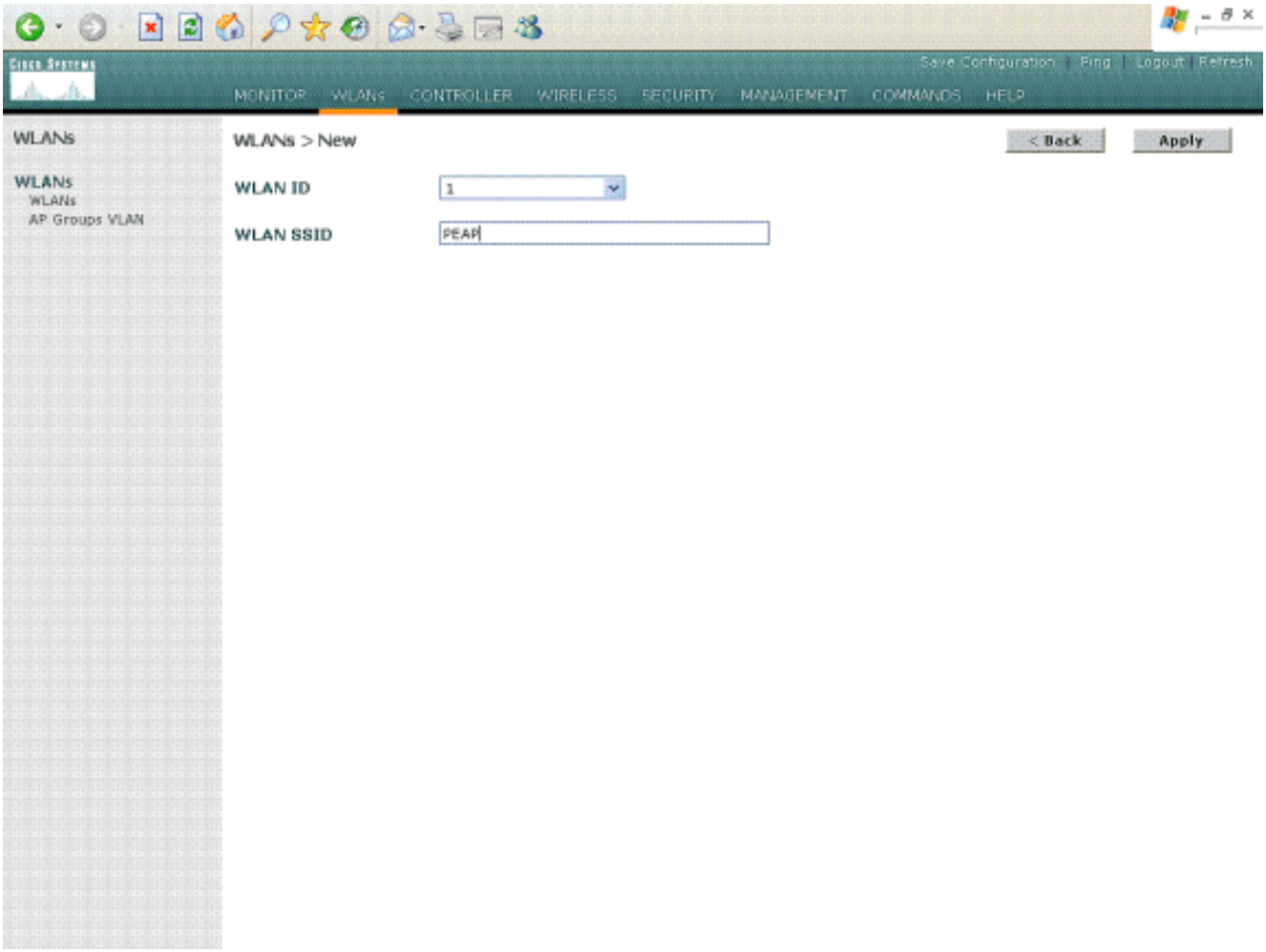
Configure el SSID (WLAN) al que se conectan los clientes inalámbricos. En este ejemplo, cree el SSID y denomínelo **PEAP**.

Defina la autenticación de capa 2 como WPA2 para que los clientes realicen la autenticación basada en EAP (PEAP-MSCHAPv2 en este caso) y utilicen AES como mecanismo de cifrado. Deje el resto de valores predeterminados.

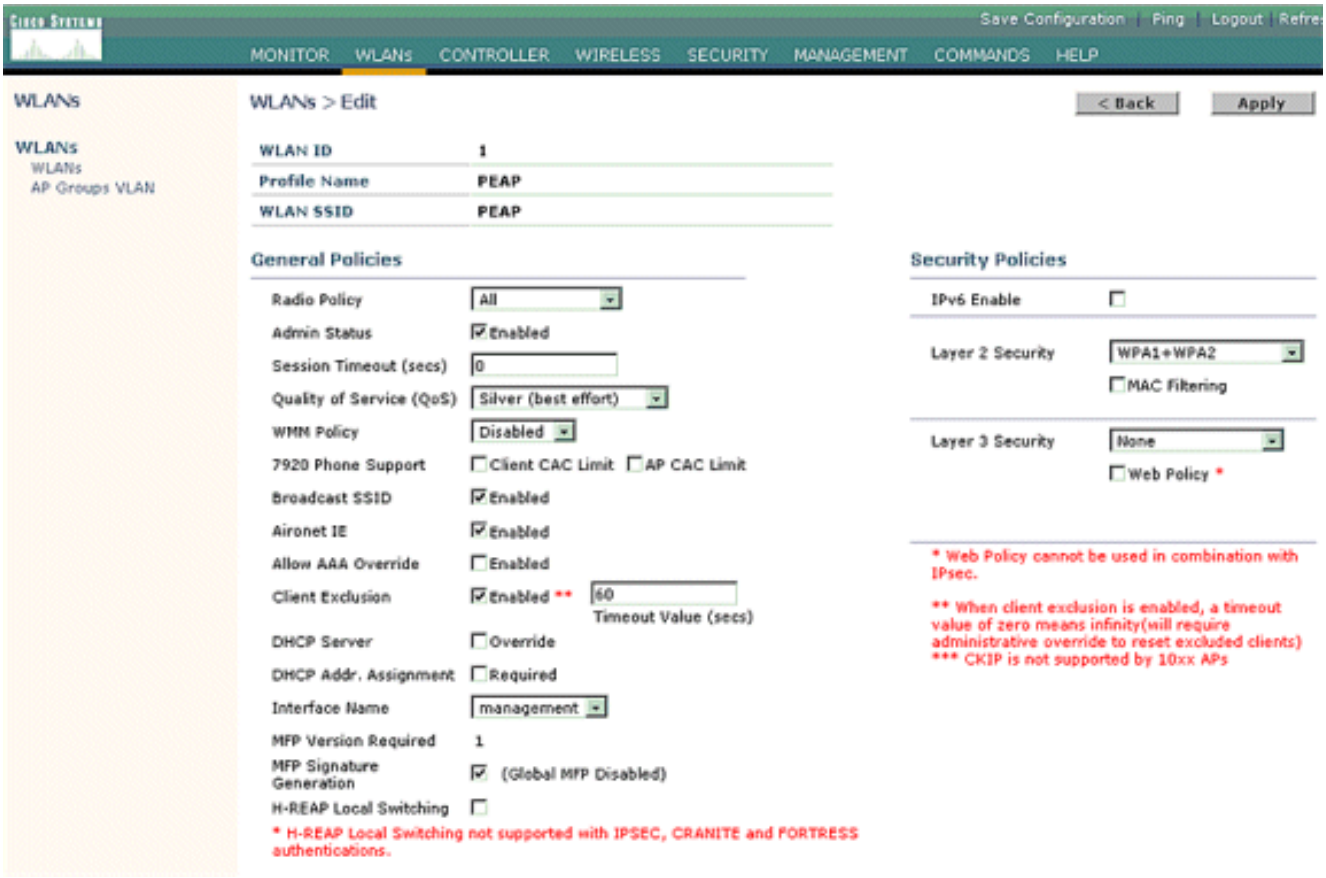
Nota: Este documento enlaza la WLAN con las interfaces de administración. Cuando tiene varias VLAN en la red, puede crear una VLAN independiente y enlazarla al SSID. Para obtener información sobre cómo configurar las VLAN en los WLC, consulte Ejemplo de Configuración de VLAN en Controladores de LAN Inalámbricos.

Para configurar una WLAN en el WLC complete estos pasos:

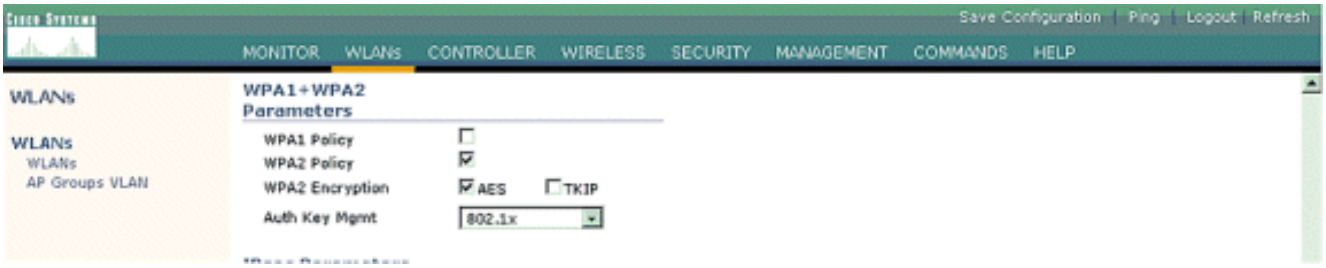
1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs. Esta página enumera las WLANs que existen en el controlador.
2. Elija **New** para crear una nueva WLAN. Introduzca el ID de WLAN y el SSID de WLAN para la WLAN y haga clic en
Apply.



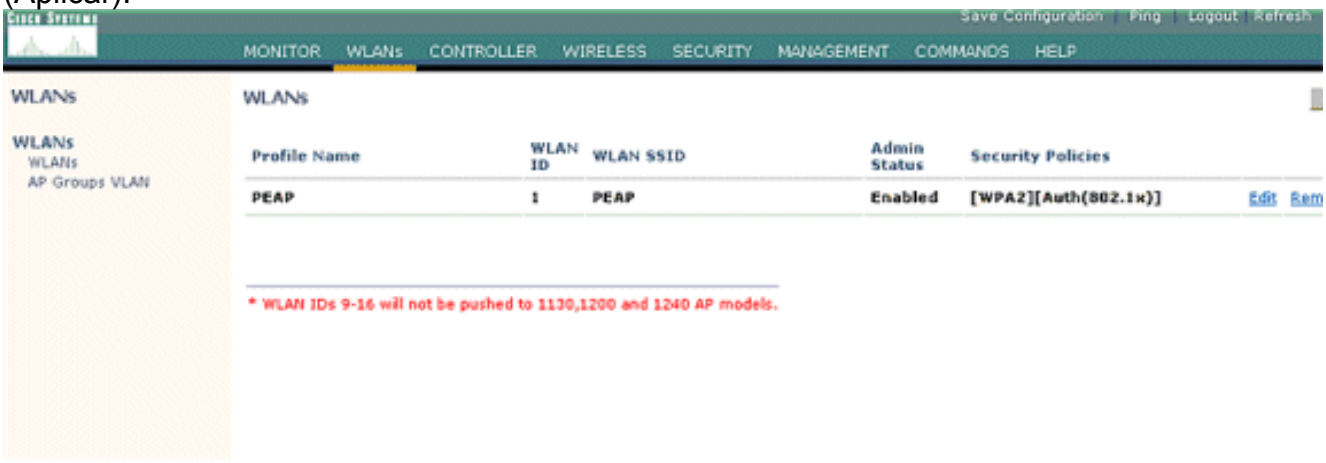
3. Una vez que haya creado una nueva WLAN, aparecerá la página **WLAN > Edit** para la nueva WLAN. En esta página puede definir varios parámetros específicos de esta WLAN que incluyen políticas generales, servidores RADIUS, políticas de seguridad y parámetros 802.1x.



4. Marque **Admin Status** en General Policies para habilitar la WLAN. Si desea que el AP difunda el SSID en sus tramas de baliza, marque **Broadcast SSID**.
5. En Layer 2 Security, elija **WPA1+WPA2**. Esto activa WPA en la WLAN. Desplácese hacia abajo por la página y seleccione la política WPA. Este ejemplo utiliza encriptación WPA2 y AES. Elija el servidor RADIUS apropiado en el menú desplegable bajo Servidores RADIUS. En este ejemplo, utilice **10.77.244.198** (dirección IP del servidor MS IAS). Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN.



6. Haga clic en Apply (Aplicar).



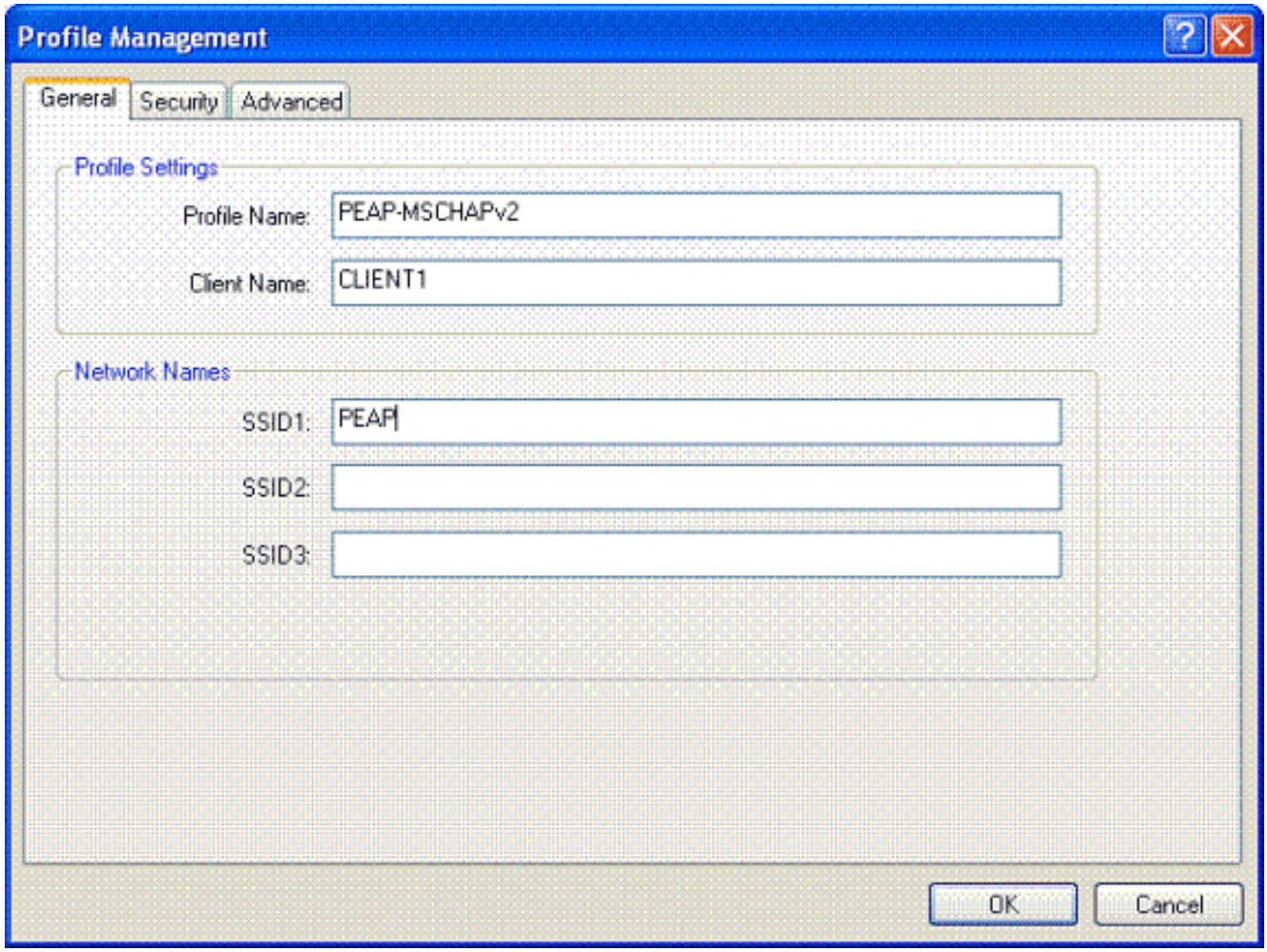
Configuración de los clientes inalámbricos

Configuración de clientes inalámbricos para autenticación PEAP-MS CHAPv2

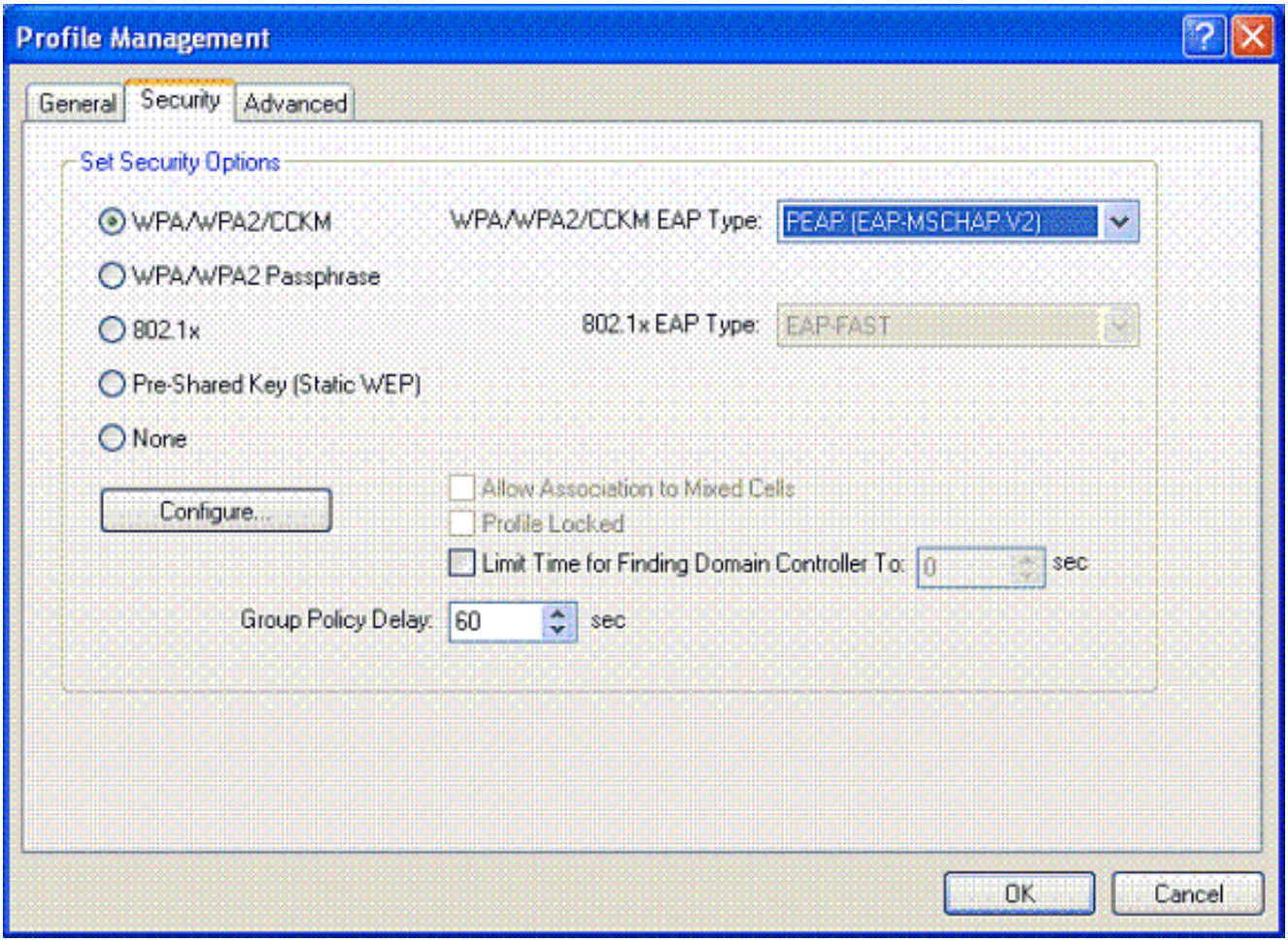
Este ejemplo proporciona información sobre cómo configurar el cliente inalámbrico con Cisco Aironet Desktop Utility. Antes de configurar el adaptador del cliente, asegúrese de que se utiliza la última versión del firmware y la utilidad. Encontrará la última versión del firmware y las utilidades en la página de descargas inalámbricas de Cisco.com.

Para configurar el adaptador de cliente inalámbrico Cisco Aironet 802.11 a/b/g con el ADU, siga estos pasos:

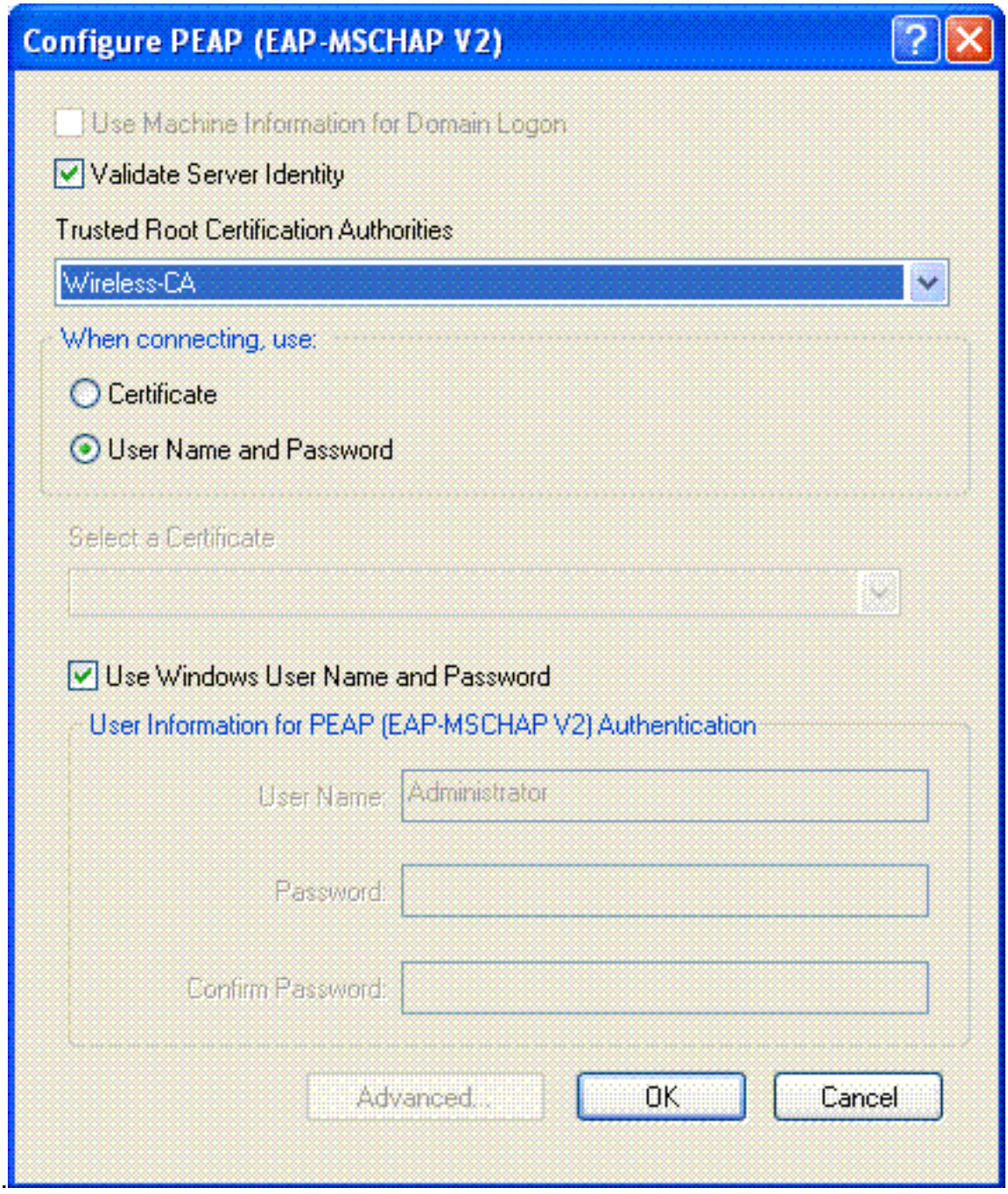
1. Abra Aironet Desktop Utility.
2. Haga clic en **Profile Management**, y haga clic en **New** para definir un perfil.
3. En la ficha General, introduzca el nombre del perfil y el SSID. En este ejemplo, utilice el SSID que configuró en el WLC (PEAP).



4. Elija la ficha Seguridad; elija **WPA/WPA2/CCKM**; en WPA/WPA2/CCKM EAP, escriba choose **PEAP [EAP-MSCHAPv2]** y haga clic en **Configurar**.



5. Elija **Validate Server Certificate**, y elija **Wireless-CA** en el menú desplegable Trusted Root Certificate

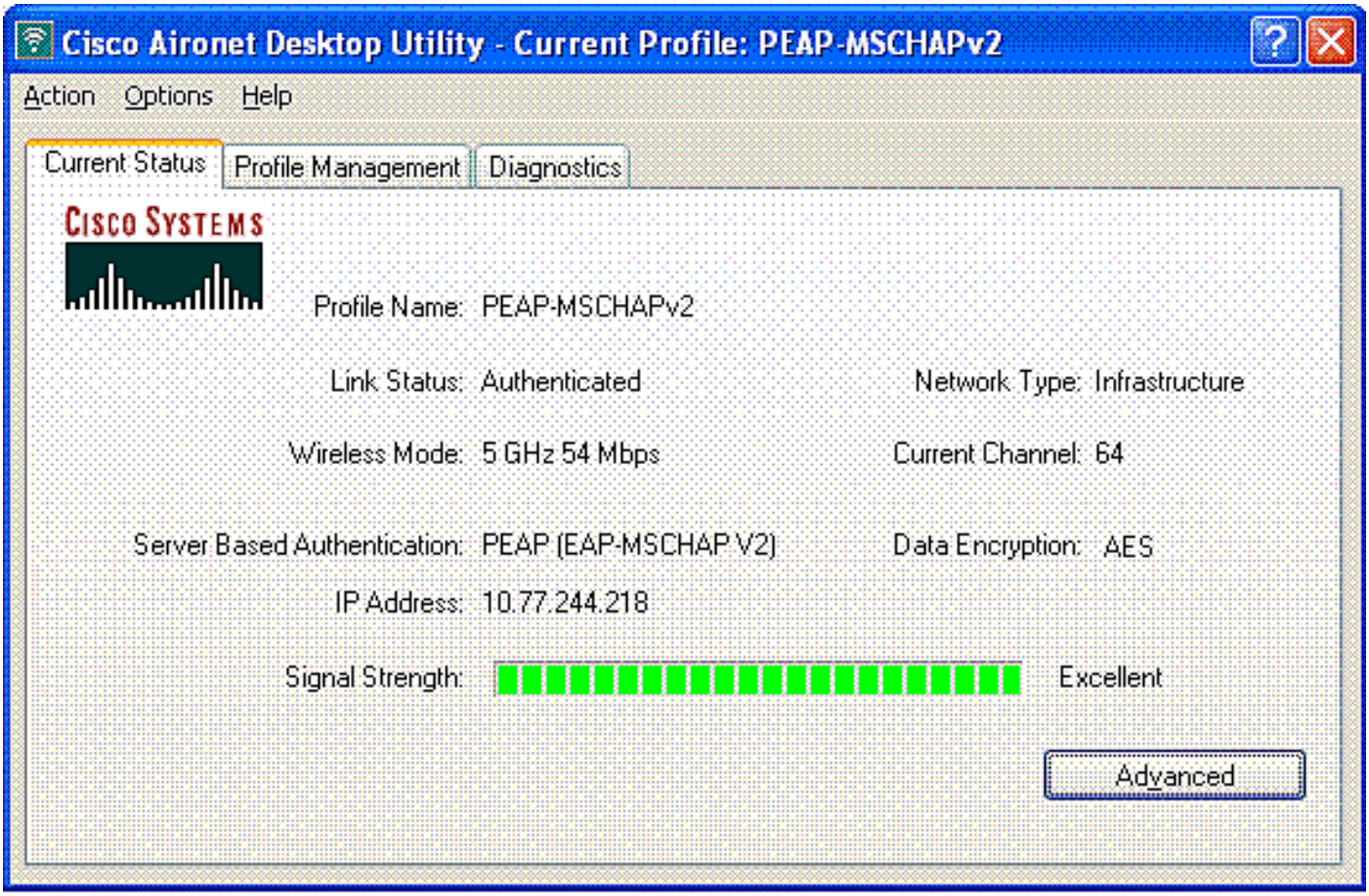


Authorities.

6. Haga clic en **Aceptar** y active el perfil.**Nota:** Cuando utilice EAP protegido-Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (PEAP-MSCHAPv2) con Microsoft XP SP2 y la tarjeta inalámbrica esté administrada por la configuración inalámbrica rápida de Microsoft (WZC), debe aplicar la revisión KB885453 de Microsoft. Esto evita varios problemas de autenticación relacionados con la reanudación rápida de PEAP.

Verificación y resolución de problemas

Para verificar si la configuración funciona según lo esperado, active el perfil PEAP-MSCHAPv2 en el cliente inalámbrico Client1.



Una vez activado el perfil PEAP-MSCHAPv2 en ADU, el cliente realiza la autenticación abierta 802.11 y, a continuación, realiza la autenticación PEAP-MSCHAPv2. Este es un ejemplo de autenticación PEAP-MSCHAPv2 exitosa.

Utilice los comandos debug para comprender la secuencia de eventos que ocurren.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Estos comandos debug en el controlador de LAN inalámbrica son útiles.

- **debug dot1x events enable** : para configurar la depuración de eventos 802.1x
- **debug aaa events enable** : para configurar la depuración de eventos AAA
- **debug mac addr <mac address>** : para configurar la depuración MAC, utilice el comando debug mac
- **debug dhcp message enable** —Para configurar el debug de los mensajes de error DHCP

Estos son los resultados de ejemplo del comando **debug dot1x events enable** y del comando **debug client <mac address>**.

debug dot1x events enable:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
   mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
```

mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to**

```
   mobile 00:40:96:ac:e6:57 (EAP Id 13)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending default RC4 key to
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending Key-Mapping RC4 key to
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received Auth Success while in
   Authenticating state for mobile 00:40:96:ac:e6:57
```

debug mac addr <MAC Address>:

```
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Association received from
   mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 -
   rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
   Change state to START (0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0)
   Initializing policy
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 START (0)
   Change state to AUTHCHECK (2)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)
   Change state to 8021X_REQD (3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)
   Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
   mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of
   Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to
   station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for
   mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving
   mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP-
   Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAPOL START from
   mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 EAP State update from
   Connecting to Authenticating for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x -
   moving mobile 00:40:96:ac:e6:57 into Authenticating state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
```

```
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached PLUMBFASTPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Replacing Fast Path rule
  type = Airespace AP Client
```

```
  on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
  Card = 0 (slot 0), InHandle = 0x00000000,
   OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
   Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
   while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
   moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

Nota: Si utiliza el Suplicante de Microsoft para autenticarse con un ACS seguro de Cisco para la autenticación PEAP, el cliente posiblemente no se autentique correctamente. En ocasiones, la conexión inicial puede autenticarse correctamente, pero los intentos de autenticación de conexión rápida subsiguientes no se conectan correctamente. Este es un problema conocido. Los detalles de este problema y la solución para el mismo están disponibles aquí .

Información Relacionada

- PEAP en Redes inalámbricas unificadas con ACS 4.0 y Windows 2003
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Actualización de software del controlador de LAN inalámbrica (WLC) a las versiones 3.2, 4.0 y 4.1
- Guías de configuración de Cisco 4400 Series Wireless LAN Controllers
- 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).