Ejemplo de Configuración de Autenticación EAP Local en el Controlador de LAN Inalámbrica con EAP-FAST y el Servidor LDAP

Contenido

Introducción

Este documento explica cómo configurar el protocolo de autenticación extensible (EAP) - autenticación flexible a través de tunelación segura (FAST) autenticación EAP local en un controlador LAN inalámbrico (WLC). Este documento también explica cómo configurar el servidor LDAP (Lightweight Directory Access Protocol) como la base de datos backend para que la EAP local obtenga los credenciales de usuario y autentique al usuario.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- WLC de la serie 4400 de Cisco que ejecuta firmware 4.2
- Punto de acceso ligero (LAP) Cisco Aironet serie 1232AG
- Servidor de Microsoft Windows 2003 configurado como controlador de dominio, servidor LDAP y servidor de autoridad certificadora.
- Adaptador de clientes Cisco Aironet 802.11 a/b/g que ejecuta firmware, versión 4.2
- Aironet Desktop Utility (ADU) de Cisco que ejecuta firmware, versión 4.2

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.

Antecedentes

La autenticación EAP local en controladores LAN inalámbricos se introdujo con la versión 4.1.171.0 del controlador LAN inalámbrico.

EAP local es un método de autenticación que permite que los usuarios y los clientes inalámbricos se autentiquen localmente en el controlador. Está diseñado para oficinas remotas que deseen mantener la conectividad con clientes inalámbricos cuando el sistema back-end se interrumpa o el servidor de autenticación externo deje de funcionar. Cuando habilita el EAP local, el controlador sirve como el servidor de autenticación y la base de datos de usuario local, por lo que elimina la dependencia de un servidor de autenticación externo. EAP local recupera las credenciales de usuario de la base de datos de usuario local o de la base de datos backend LDAP para autenticar usuarios. EAP local admite autenticación LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 y PEAPv1/GTC entre el controlador y los clientes inalámbricos.

EAP local puede utilizar un servidor LDAP como base de datos backend para recuperar las credenciales de usuario.

Una base de datos back-end LDAP permite que el controlador consulte un servidor LDAP para obtener las credenciales (nombre de usuario y contraseña) de un usuario determinado. Estas credenciales se utilizan para autenticar el usuario.

La base de datos backend LDAP soporta estos métodos EAP locales:

- EAP-FAST/GTC

- EAP-TLS
- PEAPv1/GTC.

LEAP, EAP-FAST/MSCHAPv2 y PEAPv0/MSCHAPv2 también son compatibles, **pero sólo si el servidor LDAP está configurado para devolver una contraseña de texto no cifrado**. Por ejemplo, Microsoft Active Directory no es compatible porque no devuelve una contraseña de texto no cifrado. Si no se puede configurar el servidor LDAP para que devuelva una contraseña de texto no cifrado, no se admiten LEAP, EAP-FAST/MSCHAPv2 y PEAPv0/MSCHAPv2.

Nota: Si se configura algún servidor RADIUS en el controlador, el controlador intenta autenticar los clientes inalámbricos utilizando primero los servidores RADIUS. Sólo se intenta el EAP local si no se encuentra ningún servidor RADIUS, ya sea porque los servidores RADIUS han agotado el tiempo de espera o porque no se ha configurado ningún servidor RADIUS. Si se configuran cuatro servidores RADIUS, el controlador intenta autenticar el cliente con el primer servidor RADIUS, luego el segundo servidor RADIUS y, a continuación, con EAP local. Si el cliente intenta volver a autenticarse manualmente, el controlador intenta el tercer servidor RADIUS, luego el cuarto servidor RADIUS y, a continuación, el EAP local.

Este ejemplo utiliza EAP-FAST como el método EAP local en el WLC, que a su vez está configurado para consultar las credenciales de usuario de un cliente inalámbrico en la base de datos backend LDAP.

Configurar

Este documento utiliza EAP-FAST con certificados tanto en el lado del cliente como en el lado del servidor. Para ello, la instalación utiliza el servidor **Microsoft Certificate Authority (CA)** para generar los certificados de cliente y de servidor.

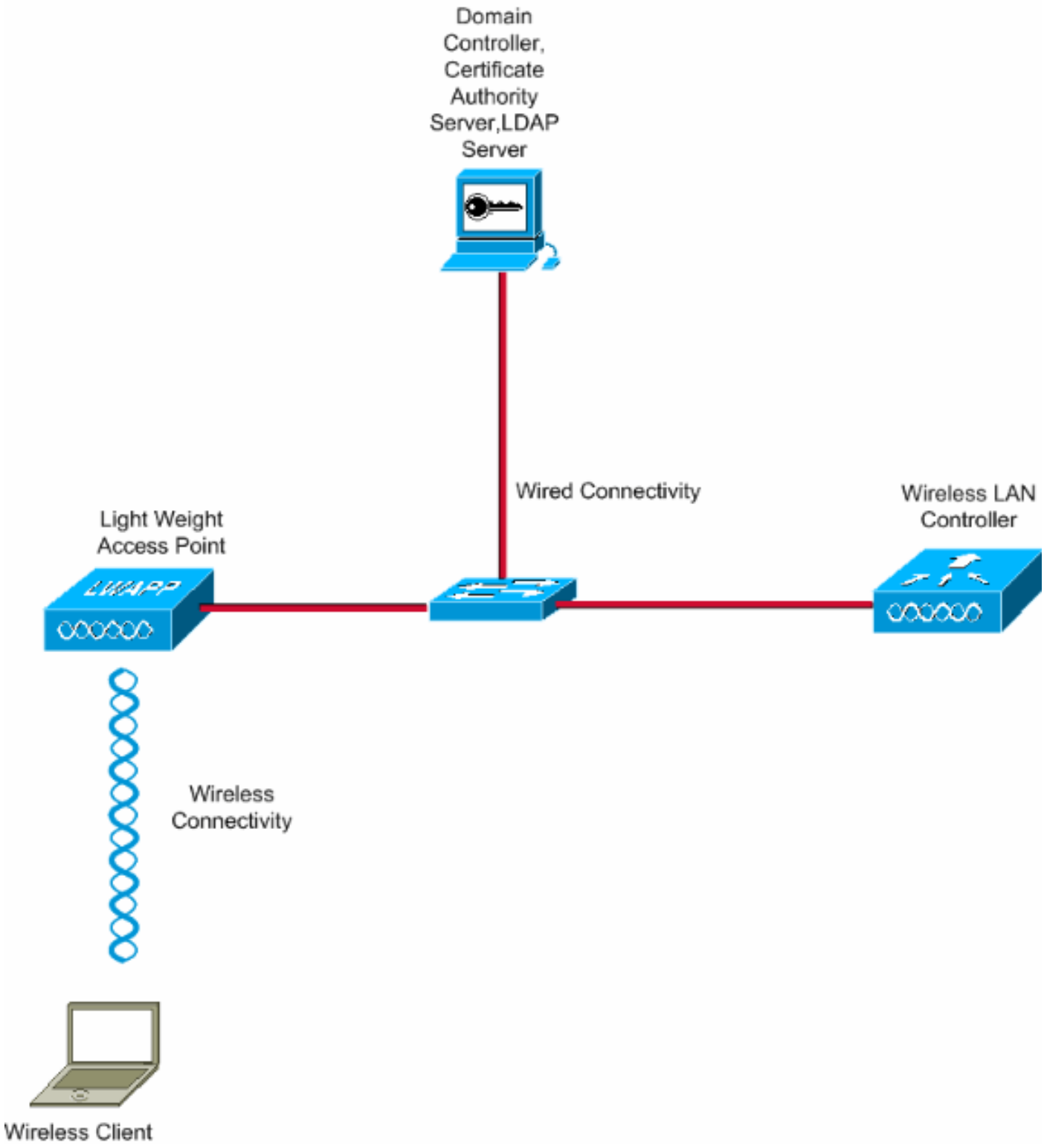
Las credenciales de usuario se almacenan en el servidor LDAP para que, una vez validada correctamente la certificación, el controlador consulte al servidor LDAP para recuperar las credenciales de usuario y autentique al cliente inalámbrico.

Este documento asume que estas configuraciones ya están en su lugar:

- Un LAP está registrado en el WLC. Refiérase a Registro de AP Ligero (LAP) a un Controlador de LAN Inalámbrica (WLC) para obtener más información sobre el proceso de registro.
- Se configura un servidor DHCP para asignar una dirección IP a los clientes inalámbricos.
- El servidor de Microsoft Windows 2003 está configurado como controlador de dominio y como servidor de la CA. En este ejemplo se utiliza **wireless.com** como dominio.Consulte Configuración de Windows 2003 como controlador de dominio para obtener más información sobre la configuración de un servidor de Windows 2003 como controlador de dominio.Consulte Instalación y Configuración de Microsoft Windows 2003 Server como Servidor de Autoridad de Certificación (CA) para configurar Windows 2003 Server como Servidor de CA Empresarial.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Complete estos pasos para implementar esta configuración:

- Configure EAP-FAST como método de autenticación EAP local en el WLC
- Configurar servidor LDAP
- Configurar cliente inalámbrico

Configure EAP-FAST como método de autenticación EAP local en el WLC

Como se mencionó anteriormente, este documento utiliza EAP-FAST con certificados tanto en el cliente como en el servidor como el método de autenticación EAP local. El primer paso es descargar e instalar los siguientes certificados en el servidor (WLC, en este caso) y el cliente.

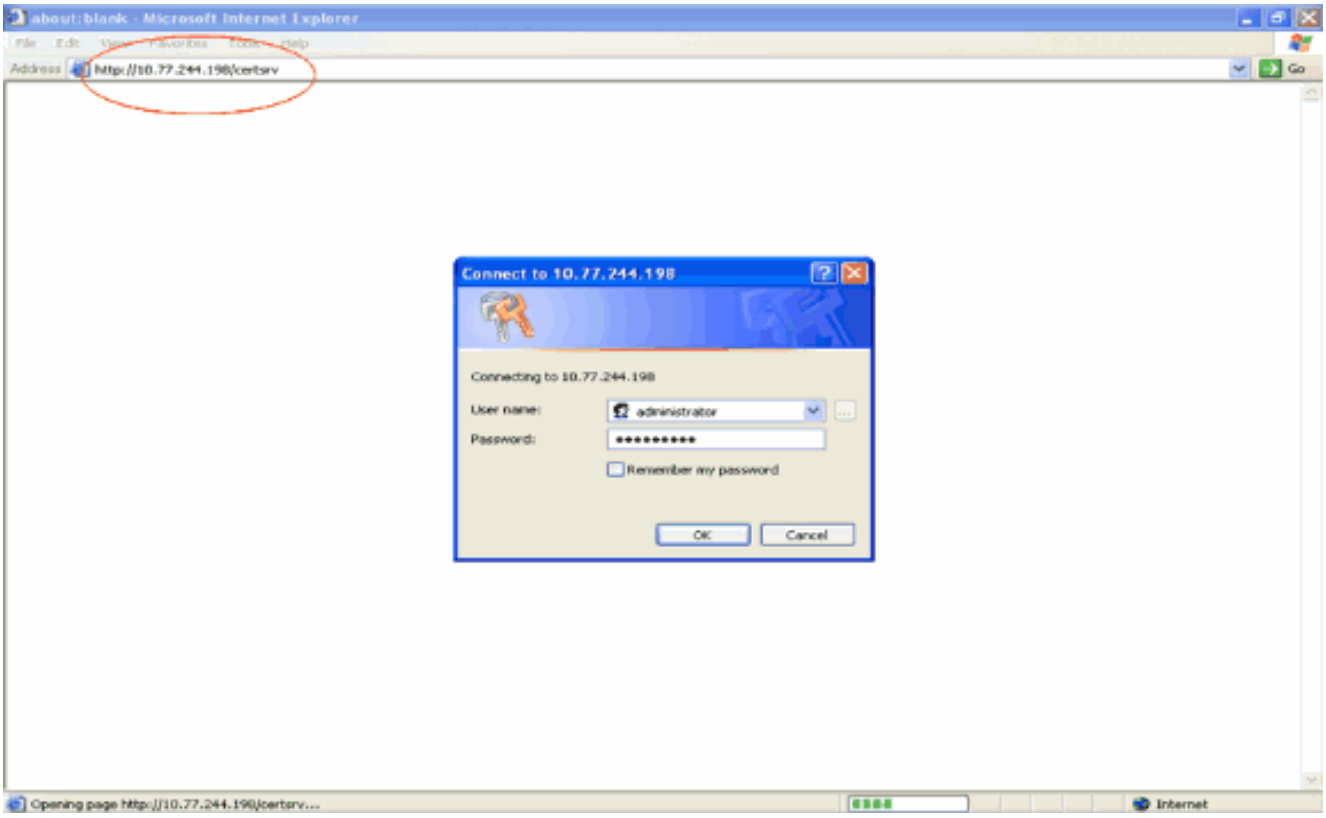
El WLC y el cliente necesitan cada uno estos certificados para ser descargados del servidor CA:

- Certificado del dispositivo (uno para el WLC y uno para el cliente)
- Certificado raíz de la infraestructura de clave pública (PKI) para el WLC y certificado de CA para el cliente

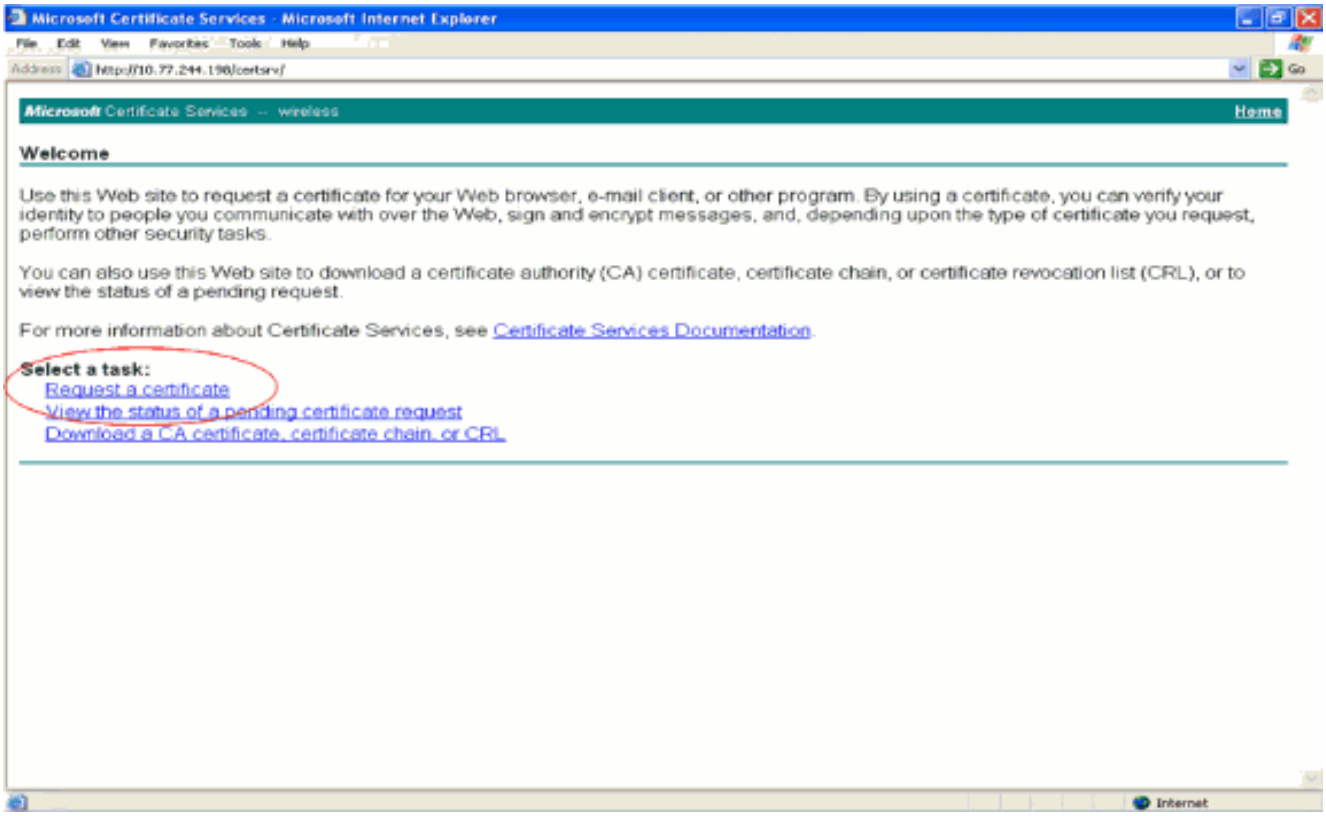
Generar un certificado de dispositivo para el WLC

Realice estos pasos para generar un certificado de dispositivo para el WLC del servidor CA. El WLC utiliza este certificado del dispositivo para autenticar al cliente.

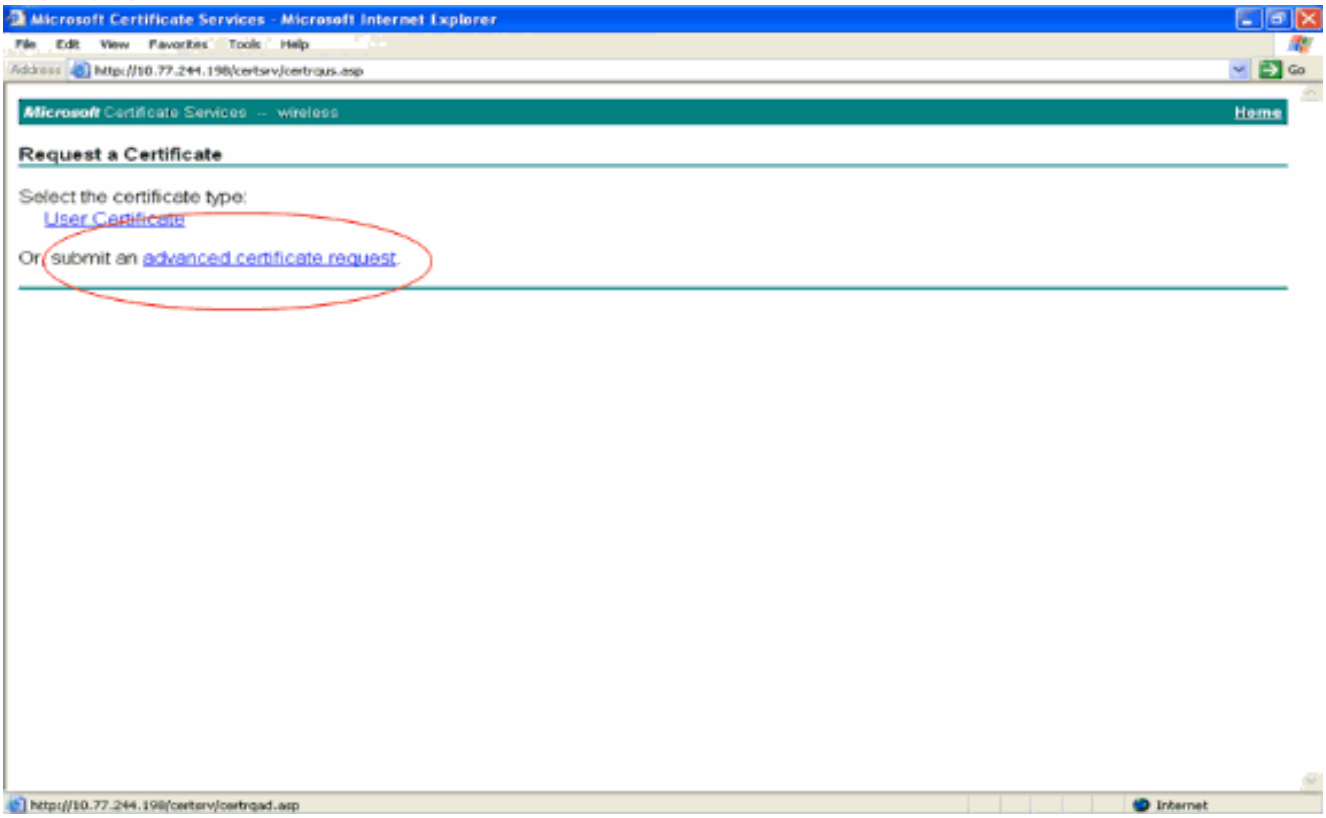
1. Vaya a **http://<dirección IP del servidor de la CA>/certsrv** desde su PC que tiene una conexión de red con el servidor de la CA. Inicie sesión como administrador del servidor de la CA.



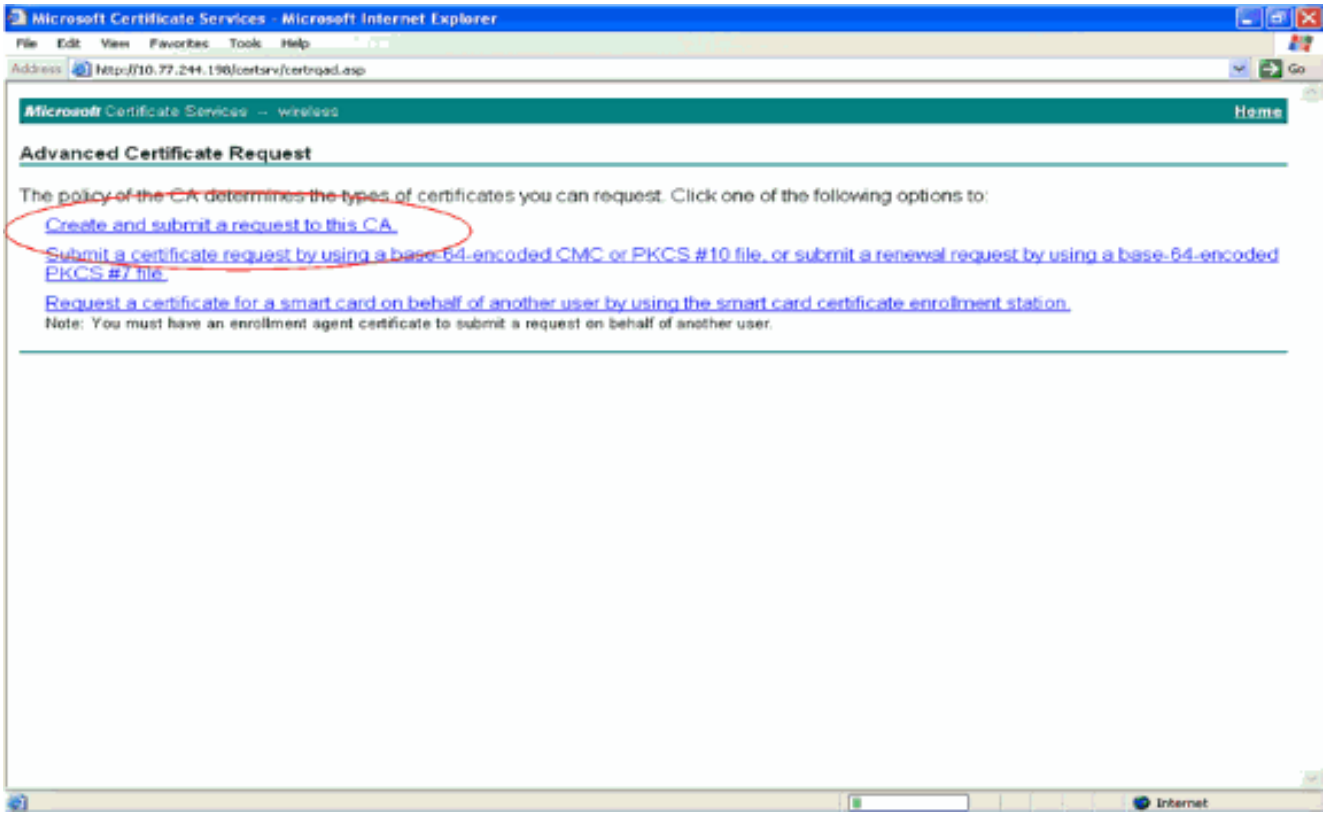
2. Seleccione **Solicitar un certificado**.



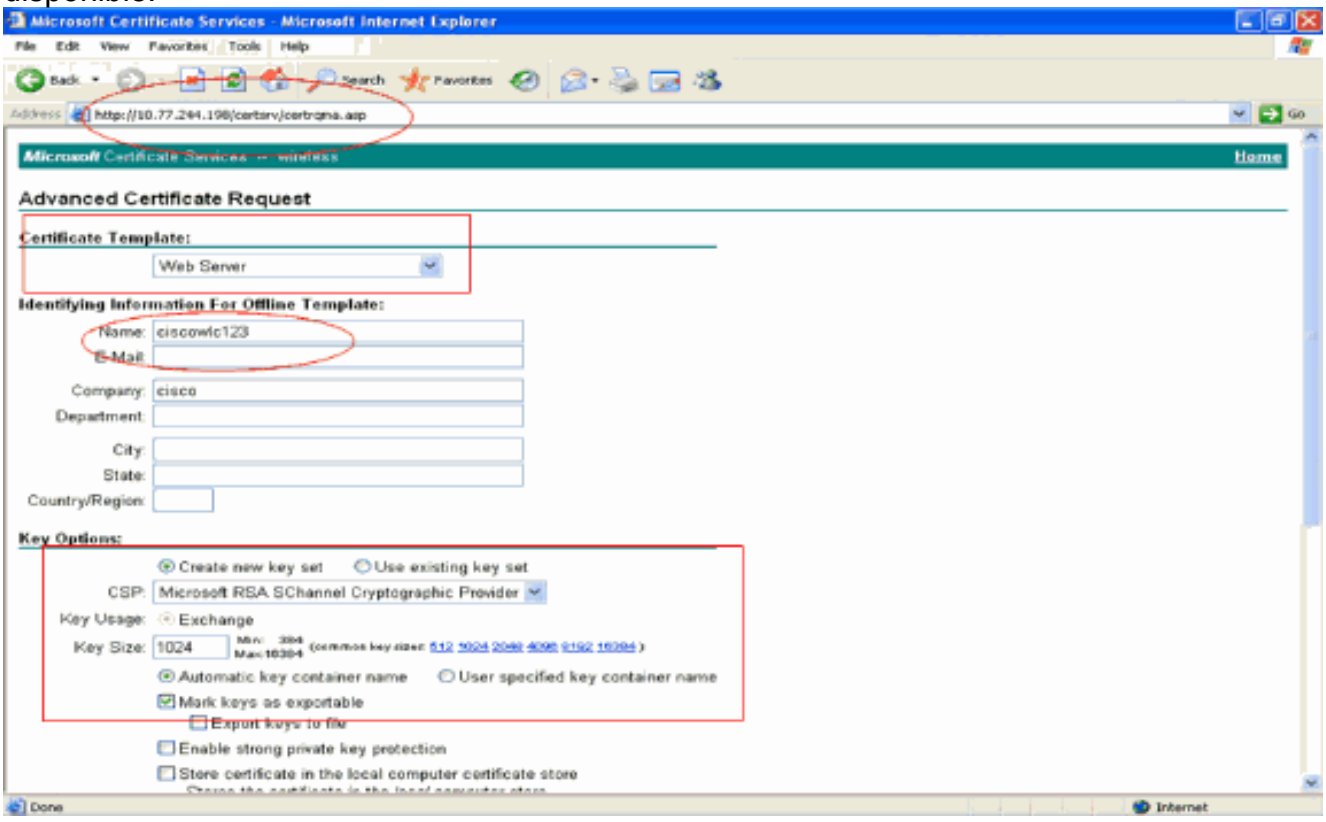
3. En la página Solicitar un certificado, haga clic en **Solicitud de certificado avanzada**.



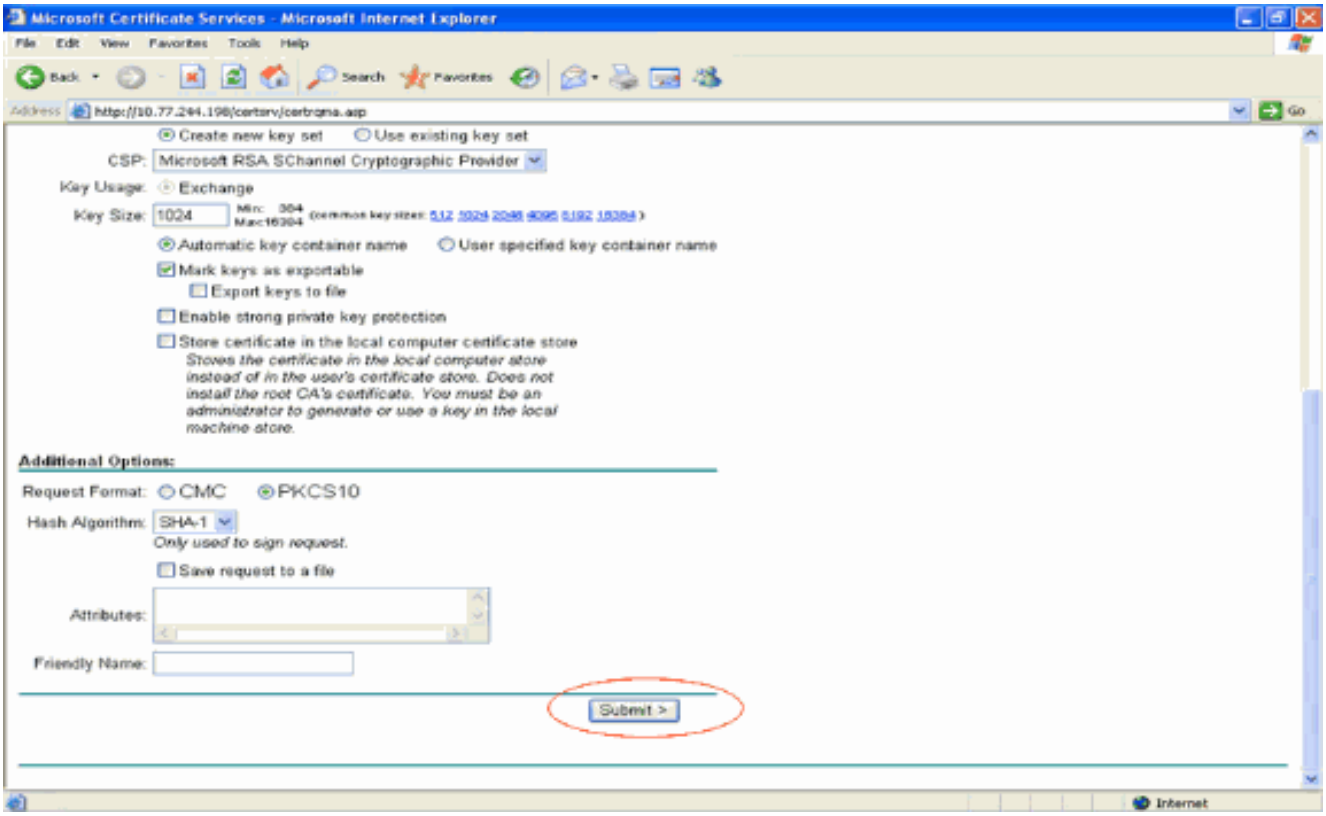
4. En la página Solicitud de certificado avanzada, haga clic en **Crear y enviar una solicitud a esta CA**. Esto lo lleva al formulario de solicitud de certificado avanzado.



5. En el formulario de solicitud de certificado avanzado, elija **Servidor Web** como plantilla de certificado. A continuación, especifique un nombre para este certificado de dispositivo.En este ejemplo se utiliza el nombre del certificado como ciscowlc123. Rellene la otra información de identificación según sus necesidades.
6. En la sección **Opciones de clave**, seleccione la opción **Marcar claves como exportables**. A veces, esta opción en particular aparecerá atenuada y no se puede habilitar ni deshabilitar si elige una plantilla de servidor Web. En estos casos, haga clic en **Atrás** en el menú del navegador para retroceder una página y volver a esta página. Esta vez, la opción Marcar claves como exportables debería estar disponible.

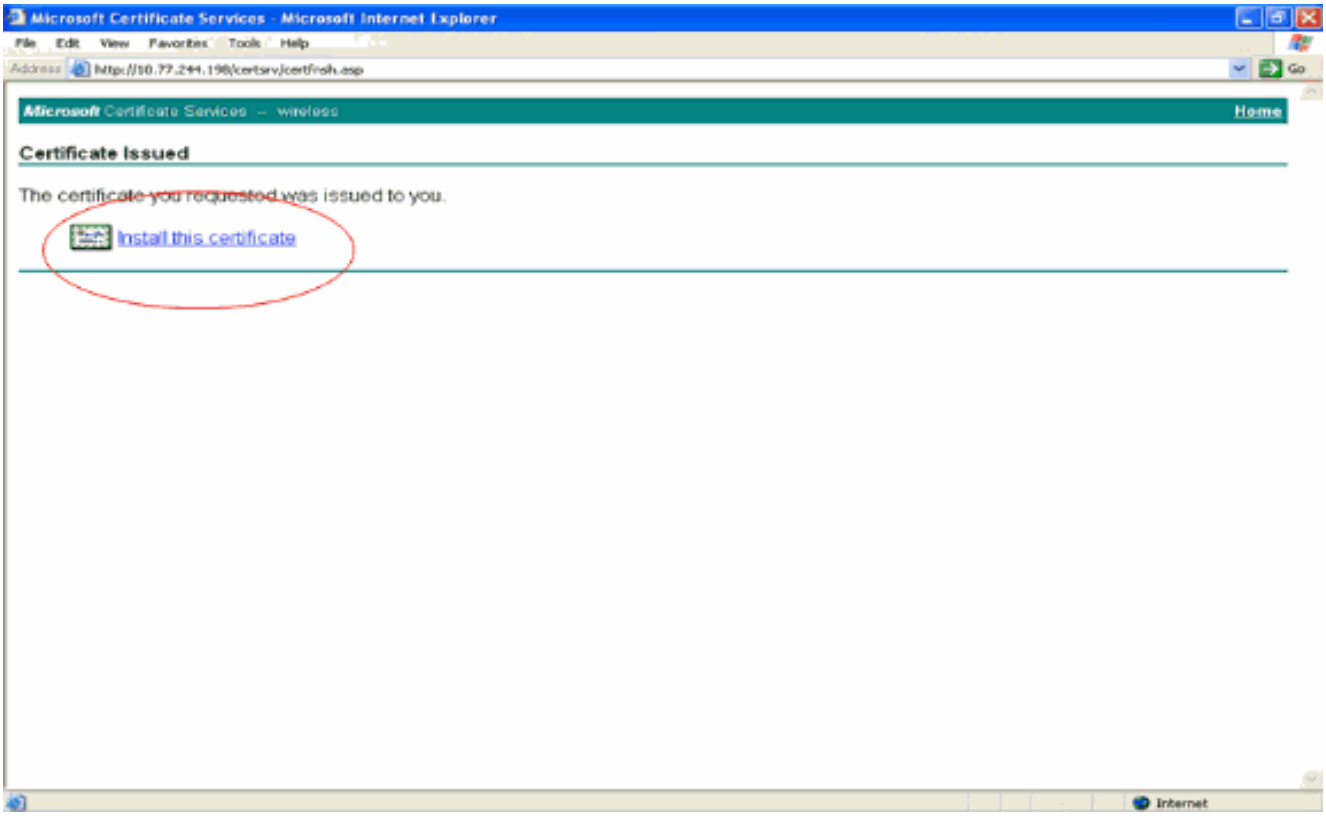


7. Configure todos los demás campos necesarios y haga clic en **Enviar**.

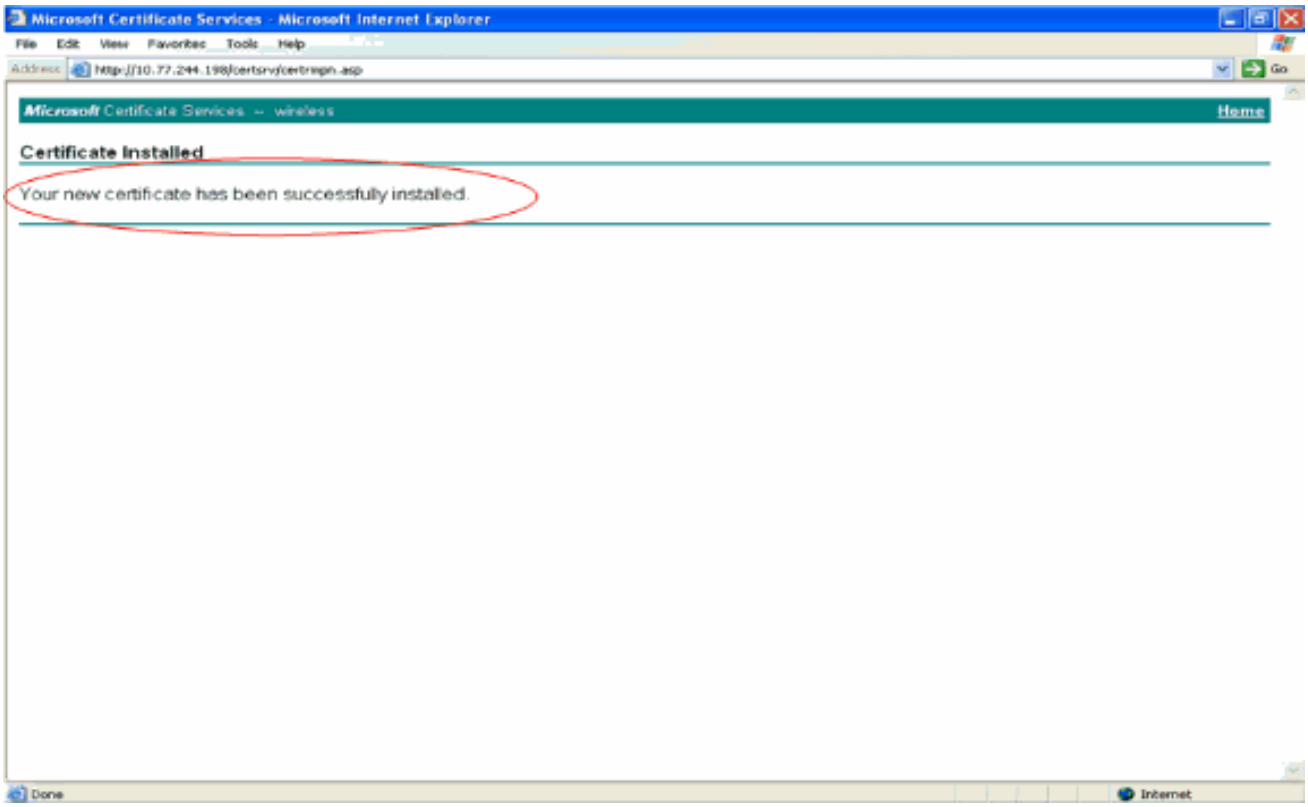


8. Haga clic en **Sí** en la siguiente ventana para permitir el proceso de solicitud de certificado.

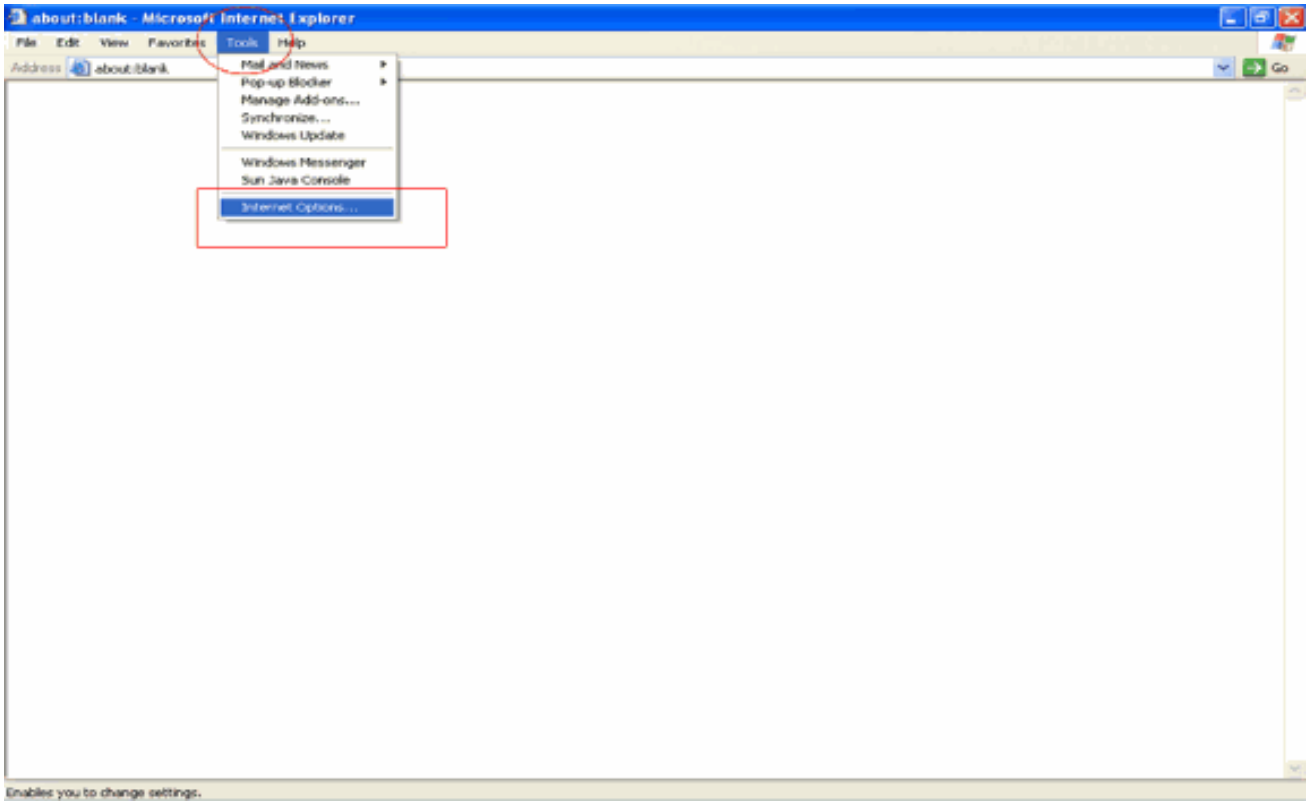
9. Aparecerá la ventana Certificado emitido, que indica que el proceso de solicitud de certificado se ha realizado correctamente. El siguiente paso es instalar el certificado emitido en el almacén de certificados de este equipo. Haga clic en Install this certificate (Instalar este certificado).



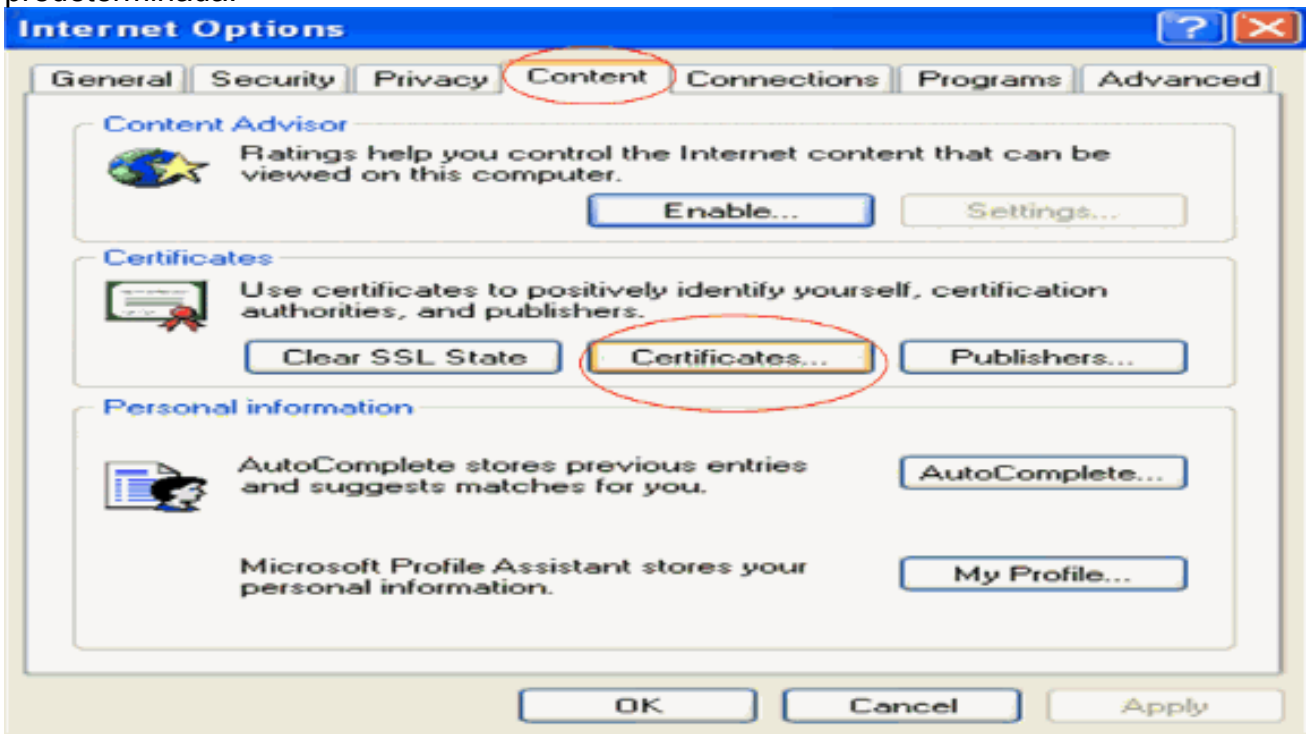
10. El nuevo certificado se ha instalado correctamente en el equipo desde el que se genera la solicitud al servidor de la CA.



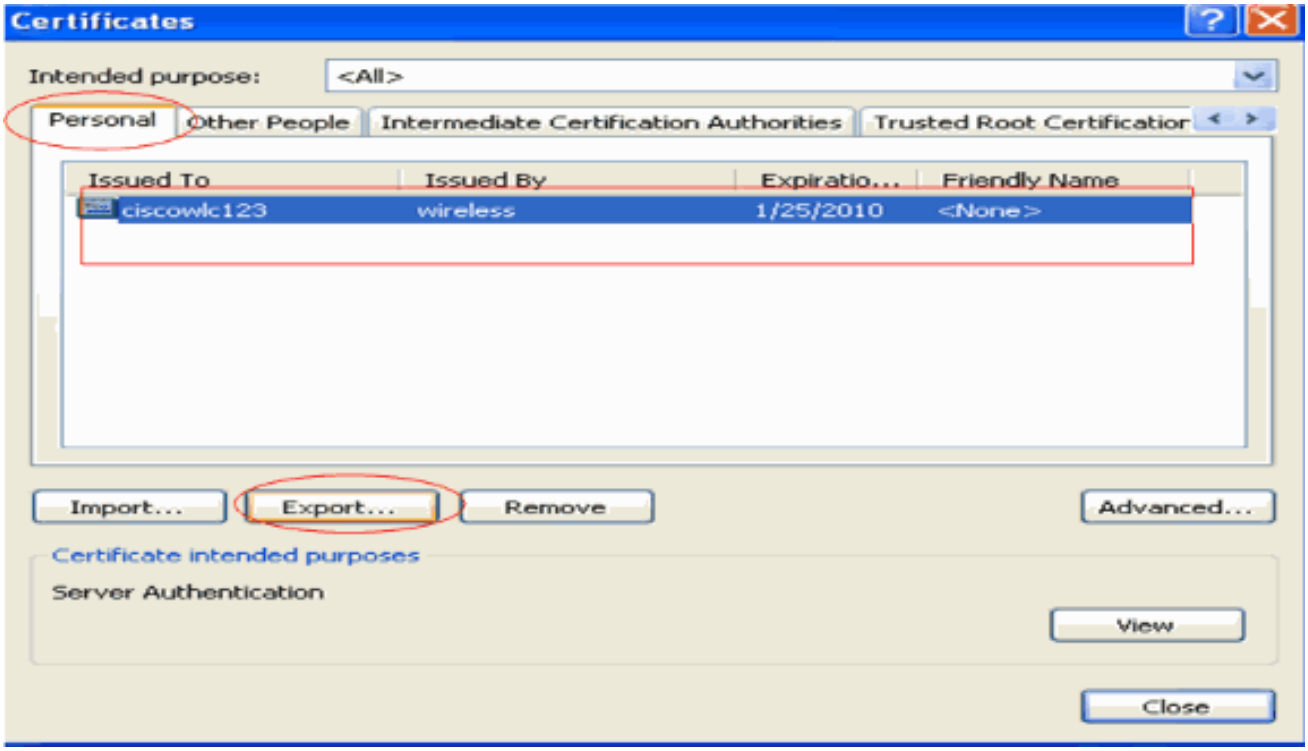
11. El siguiente paso es exportar este certificado desde el almacén de certificados al disco duro como un archivo. Este archivo de certificado se utilizará más adelante para descargar el certificado al WLC.Para exportar el certificado desde el almacén de certificados, abra el navegador Internet Explorer, luego haga clic en **Herramientas > Opciones de Internet**.



12. Haga clic en **Contenido > Certificados** para ir al almacén de certificados donde se instalan los certificados de forma predeterminada.

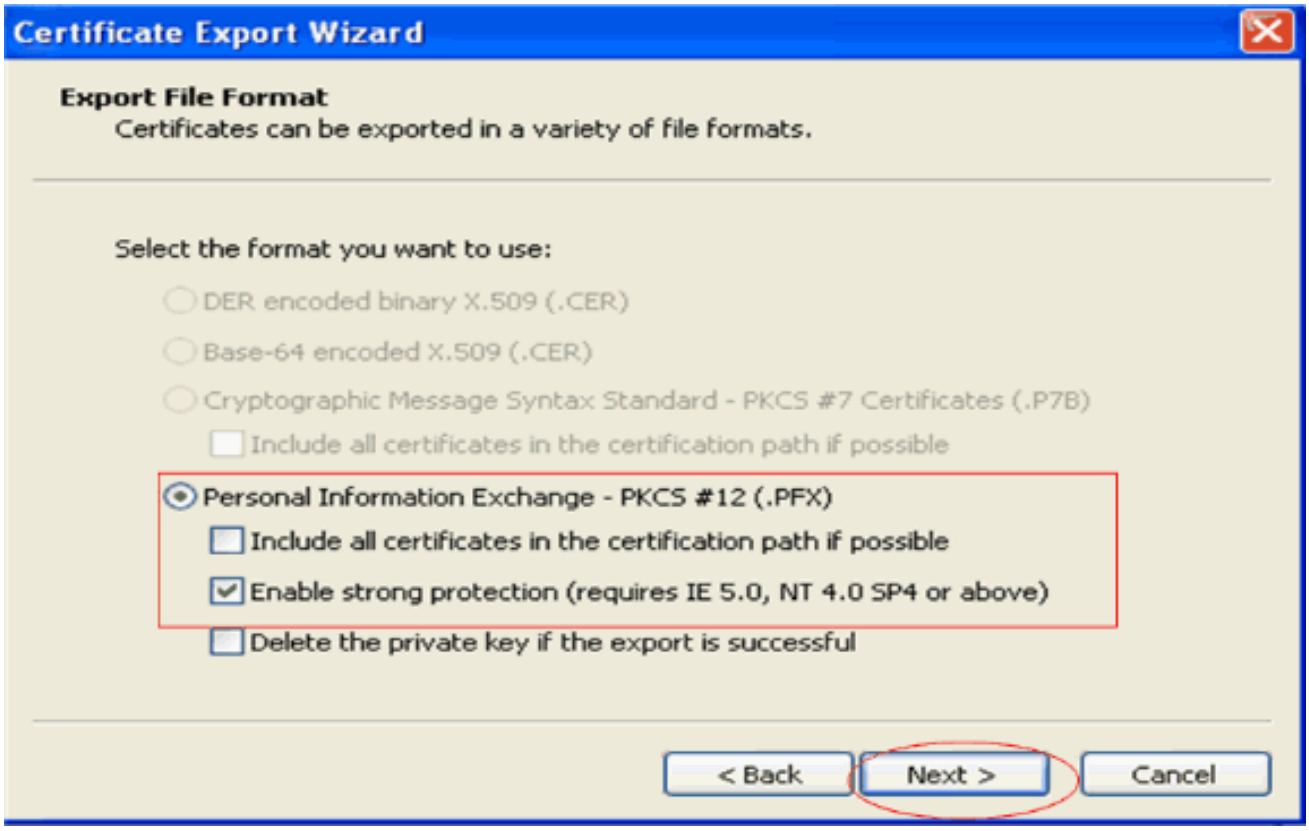


13. Los certificados de dispositivo se suelen instalar en la lista de certificados **personales**. Aquí debe ver el certificado recién instalado. Seleccione el certificado y haga clic en **Exportar**.

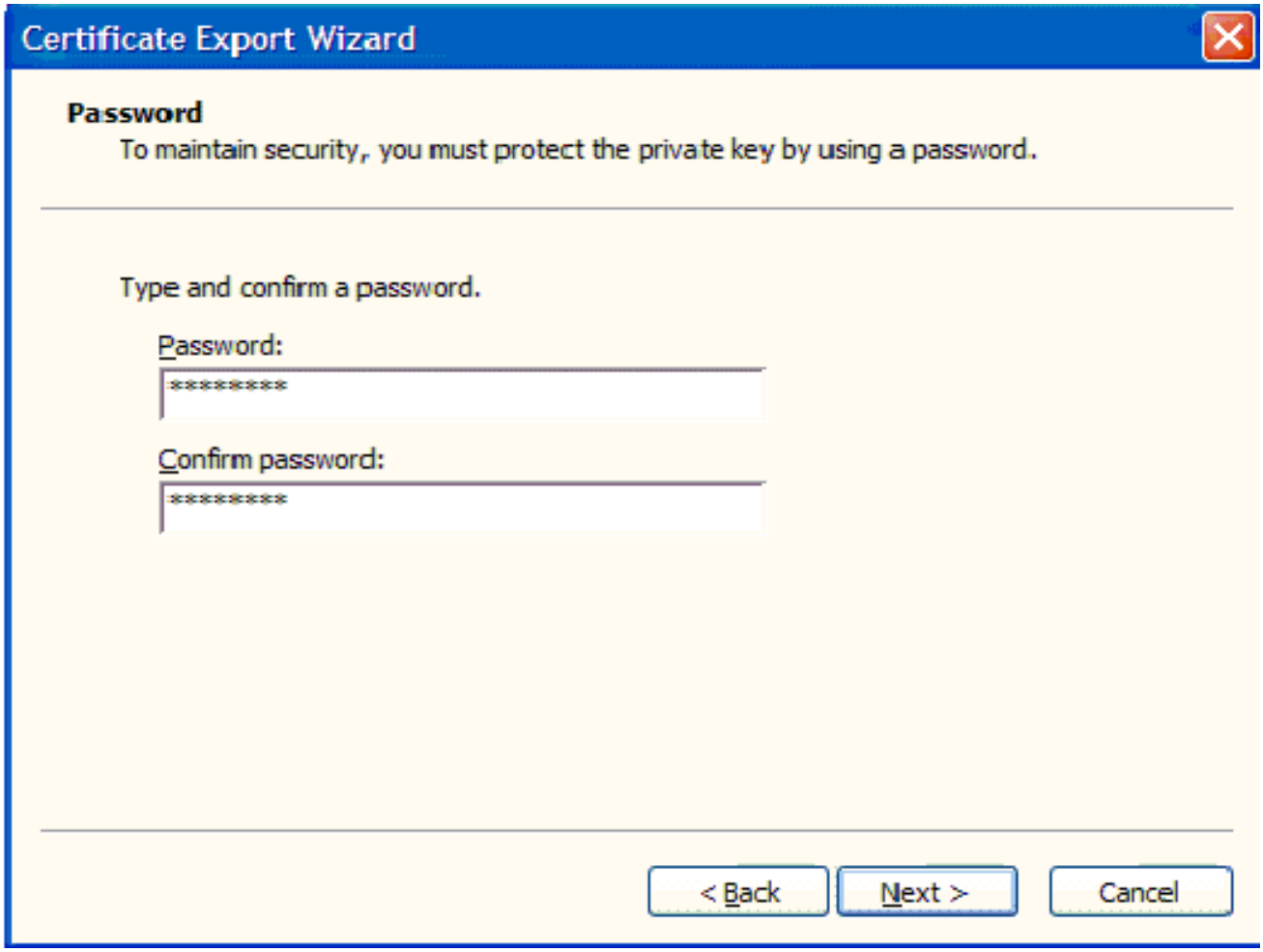


14. Haga clic en **Next** en las siguientes ventanas. Elija la opción **Yes, export the private key** en la ventana **Certificate Export Wizard**. Haga clic en Next (Siguiente).

15. Elija el formato de archivo de exportación como **.PFX** y elija la opción **Enable strong protection**. Haga clic en Next (Siguiente).

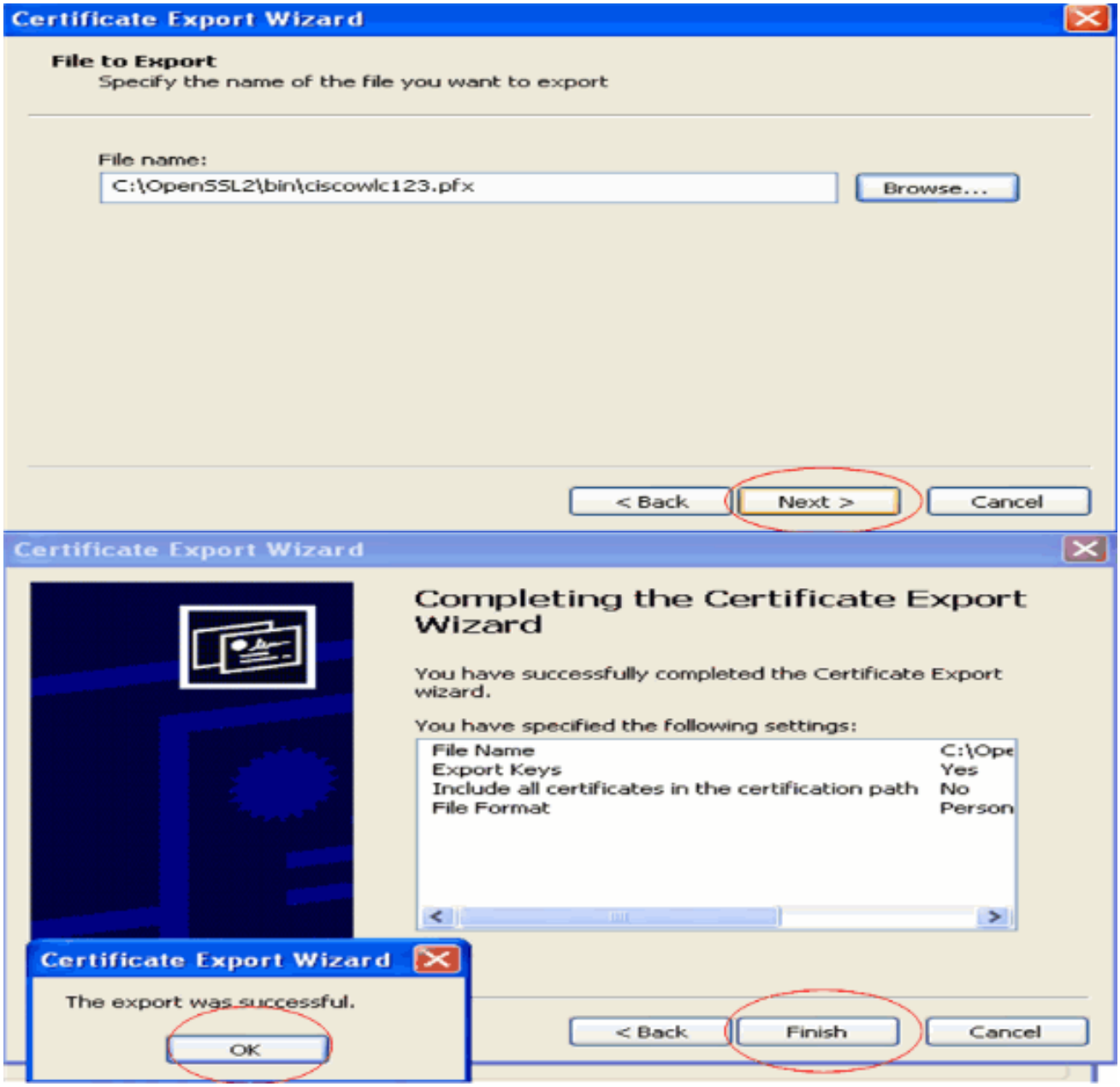


16. En la ventana Contraseña, introduzca una contraseña. En este ejemplo se utiliza **cisco** como
contraseña.



17. Guarde el archivo de certificado (archivo .PFX) en el disco duro. Haga clic en **Siguiente** y finalice el proceso de exportación

correctamente.



Descarga del certificado del dispositivo en el WLC

Ahora que el certificado del dispositivo del WLC está disponible como un archivo .PFX, el paso siguiente es descargar el archivo al controlador. Los WLC de Cisco aceptan certificados solamente en formato .PEM. Por lo tanto, primero debe convertir el archivo de formato .PFX o PKCS12 en un archivo PEM utilizando el programa openSSL.

Convierta el certificado en formato PFX a PEM utilizando el programa openSSL

Puede copiar el certificado en cualquier equipo en el que tenga instalado openSSL para convertirlo al formato PEM. Ingrese estos comandos en el archivo Openssl.exe en la carpeta bin del programa openSSL:

Nota: Puede descargar openSSL desde el sitio web de OpenSSL .

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
```

```
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

El archivo de certificado se convierte al formato PEM. El siguiente paso es descargar el certificado del dispositivo del formato PEM al WLC.

Nota: Antes de eso, necesita un software de servidor TFTP en su PC desde donde se descargará el archivo PEM. Este PC debe tener conectividad con el WLC. El servidor TFTP debe tener su directorio base y actual especificado con la ubicación donde se almacena el archivo PEM.

Descargue el certificado de dispositivo con formato PEM convertido al WLC

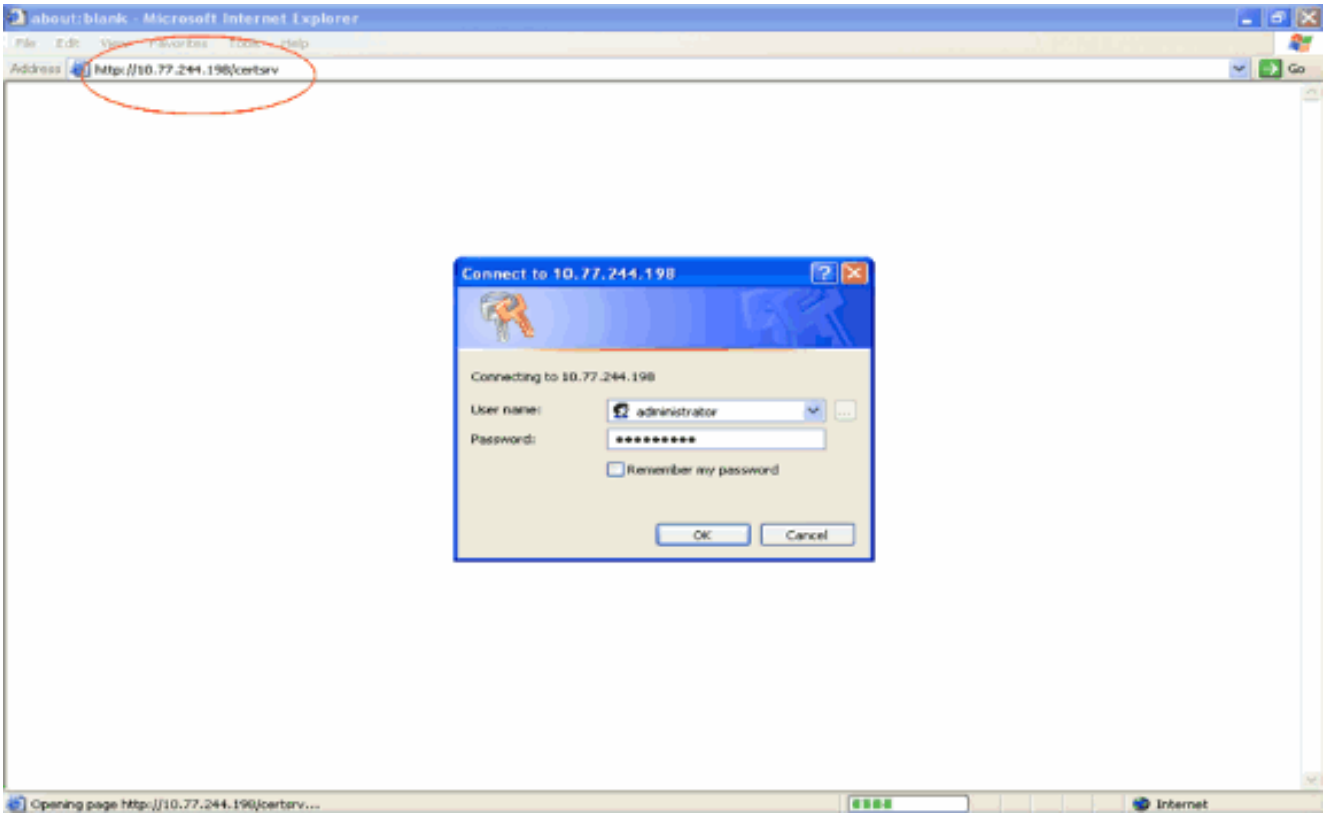
Este ejemplo explica el proceso de descarga a través de la CLI del WLC.

1. Inicie sesión en la CLI del controlador.
2. Ingrese el comando **transfer download datype eapdevcert**.
3. Ingrese el comando **transfer download serverip** ***10.77.244.196***.10.77.244.196 es la dirección IP del servidor TFTP.
4. Ingrese el comando **transfer download filename** ***ciscowlc.pem***.ciscowlc123.pem es el nombre de archivo utilizado en este ejemplo.
5. Ingrese el comando **transfer download certpassword** para establecer la contraseña para el certificado.
6. Ingrese el comando **transfer download start** para ver la configuración actualizada.A continuación, responda **y** cuando se le solicite que confirme la configuración actual e inicie el proceso de descarga.Este ejemplo muestra el resultado del comando download:
   ```
   (Cisco Controller) >transfer download start

   Mode..................................... TFTP
   Data Type................................ Vendor Dev Cert
   TFTP Server IP........................... 10.77.244.196
   TFTP Packet Timeout...................... 6
   TFTP Max Retries......................... 10
   TFTP Path.....................................
   TFTP Filename............................ ciscowlc.pem

   This may take some time.
   Are you sure you want to start? (y/N) y
   TFTP EAP CA cert transfer starting.
   Certificate installed.
   Reboot the switch to use the new certificate.
   Enter the reset system command to reboot the controller.
        The controller is now loaded with the device certificate.
   ```
7. Ingrese el comando **reset system** para reiniciar el controlador. El controlador se carga ahora con el certificado del dispositivo.

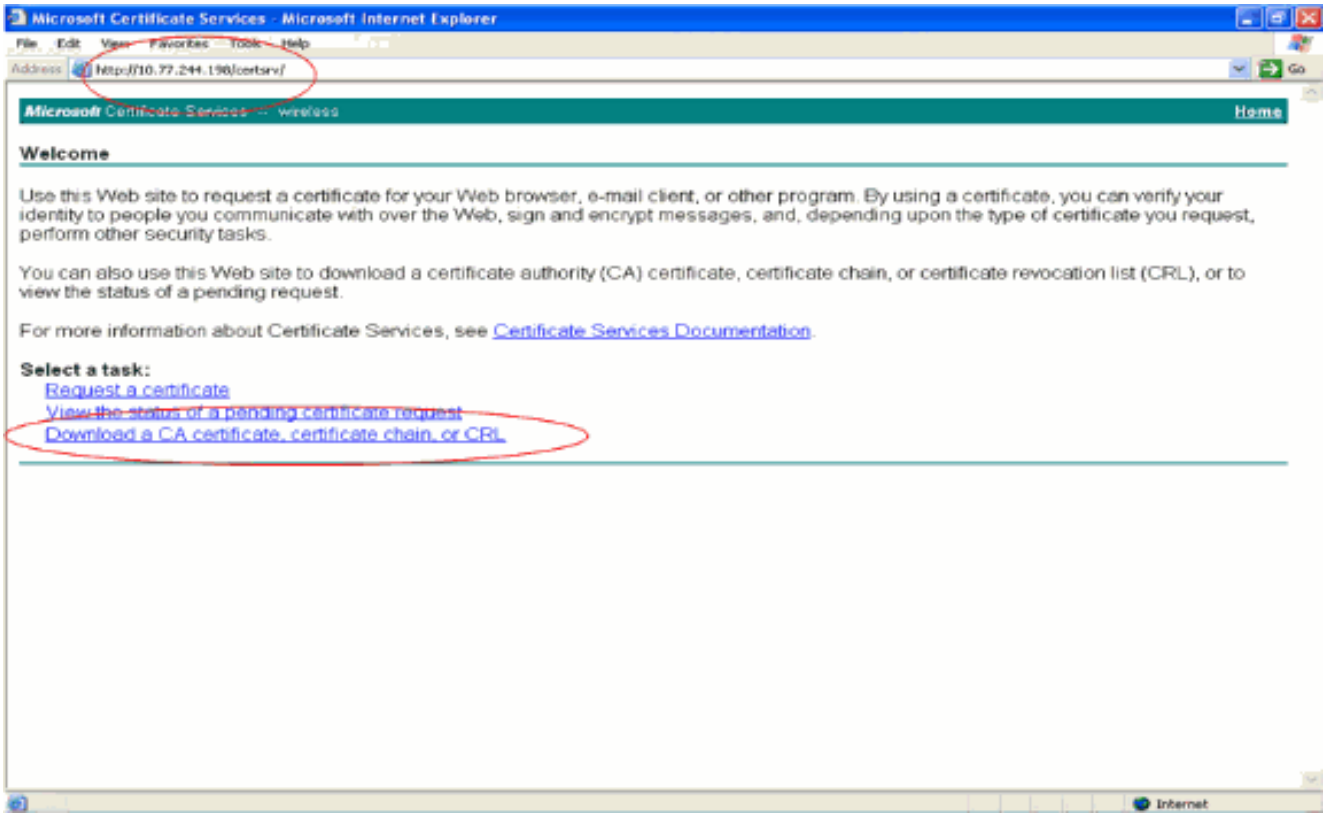
Instale el certificado raíz de PKI en el WLC

Ahora que el certificado del dispositivo está instalado en el WLC, el paso siguiente es instalar el certificado raíz del PKI al WLC del servidor CA. Siga estos pasos:

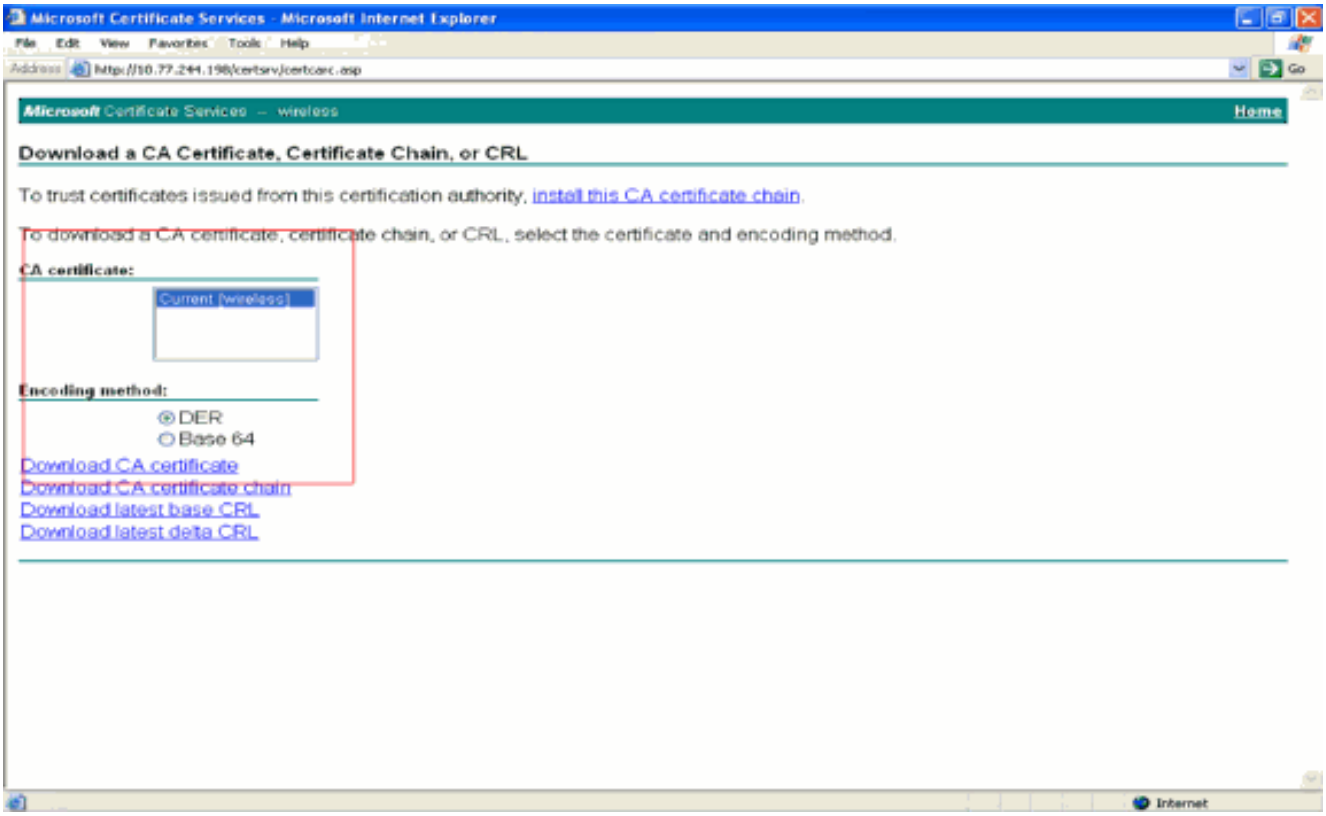
1. Vaya a **http://<dirección IP del servidor de la CA>/certsrv** desde su PC que tiene una conexión de red con el servidor de la CA. Inicie sesión como administrador del servidor de la CA.



2. Haga clic en **Descargar un certificado de CA, cadena de certificados o CRL**.



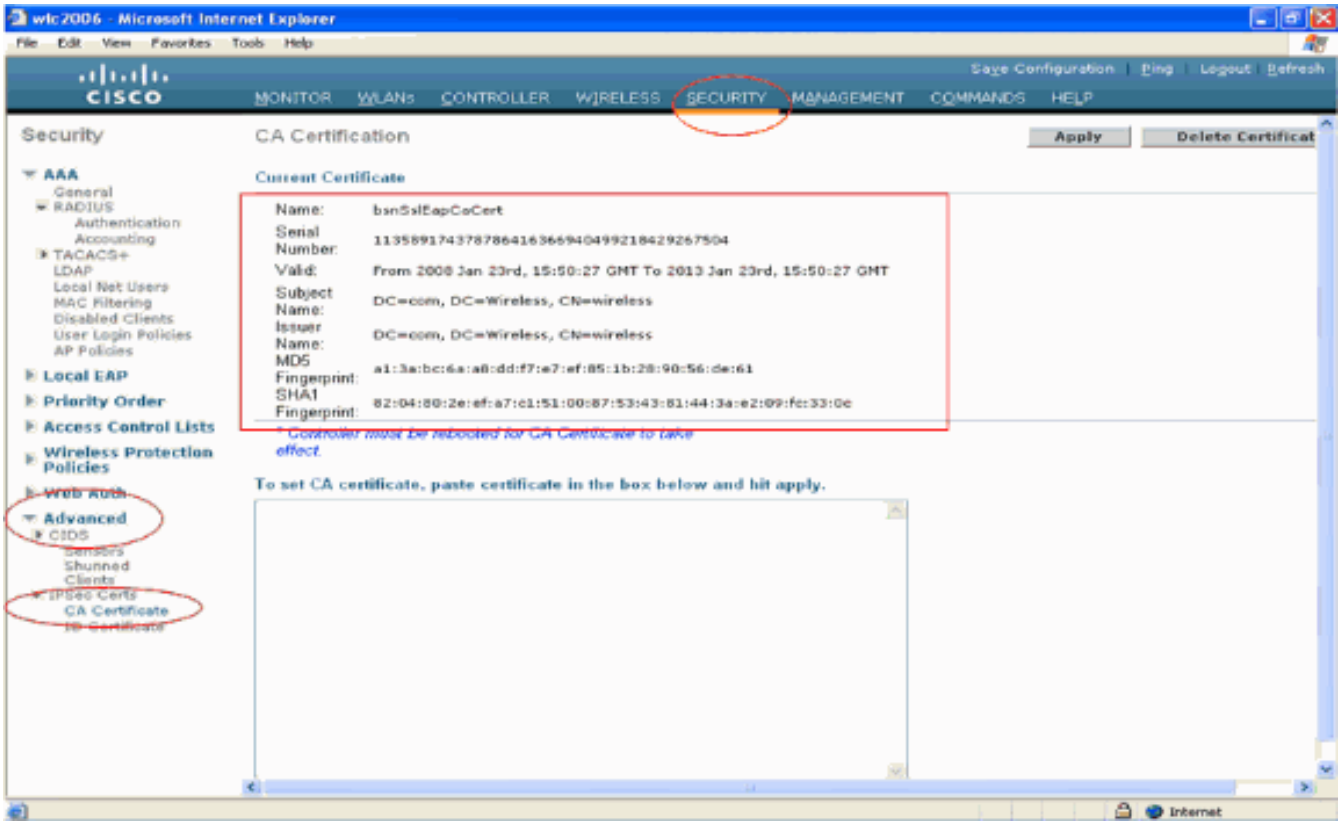
3. En la página resultante, puede ver los certificados de CA actuales disponibles en el servidor de CA en el cuadro **Certificado de CA**. Elija **DER** como método de codificación y haga clic en **Descargar certificado de CA**.



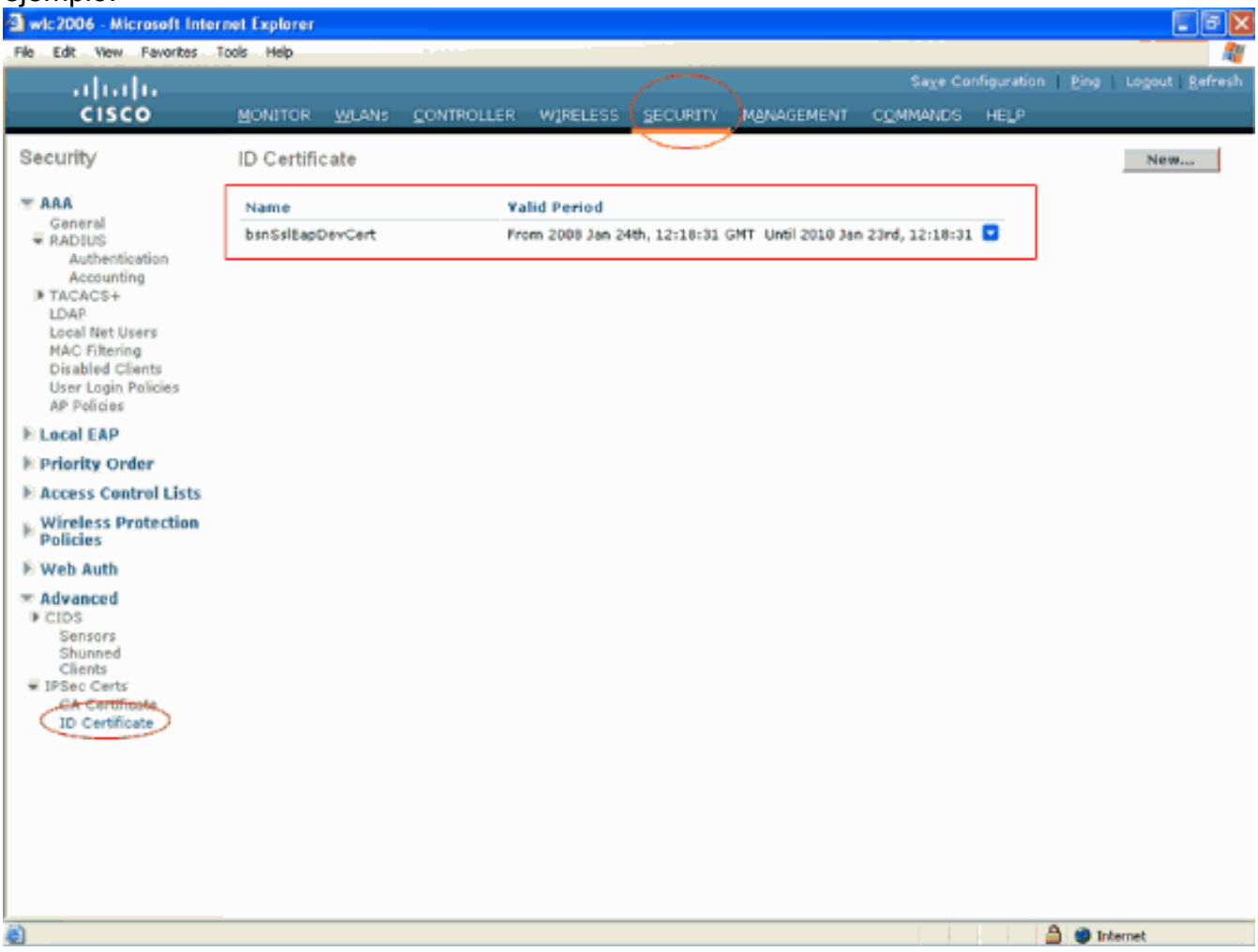
4. Guarde el certificado como un archivo **.cer**. En este ejemplo se utiliza **certnew.cer** como nombre de archivo.
5. El siguiente paso es convertir el archivo .cer al formato PEM y descargarlo al controlador. Para realizar estos pasos, repita el mismo procedimiento explicado en la sección Descarga del Certificado del Dispositivo al WLC con estos cambios:Los archivos openSSL "-in" y "-out" son **certnew.cer** y **certnew.pem**.Además, en este proceso no se requiere ninguna frase de contraseña PEM ni contraseñas de importación.Además, el comando openSSL para convertir el archivo **.cer** en el archivo **.pem** es:**x509 -in *certnew.cer* -inform DER -out *certnew.pem* -outform PEM**En el paso 2 de la sección Descargue el certificado de dispositivo de formato PEM convertido al WLC, el comando para descargar el certificado al WLC es:(Cisco Controller)**>transferir tipo de datos de descarga eapcacert**El archivo que se descargará al WLC es **certnew.pem**.

Puede verificar si los certificados están instalados en el WLC desde la GUI del controlador de la siguiente manera:

- Desde la GUI del WLC, haga clic en **Seguridad**. En la página Seguridad, haga clic en **Avanzadas > Certificados IPSec** en las tareas que aparecen a la izquierda. Haga clic en **CA Certificate** para ver el certificado de CA instalado. Este es el ejemplo:



- Para verificar si el certificado del dispositivo está instalado en el WLC, de la GUI del WLC, haga clic en **Seguridad**. En la página Seguridad, haga clic en **Avanzadas > Certificados IPSec** en las tareas que aparecen a la izquierda. Haga clic en **Certificado de ID** para ver el certificado de dispositivo instalado. Este es el ejemplo:

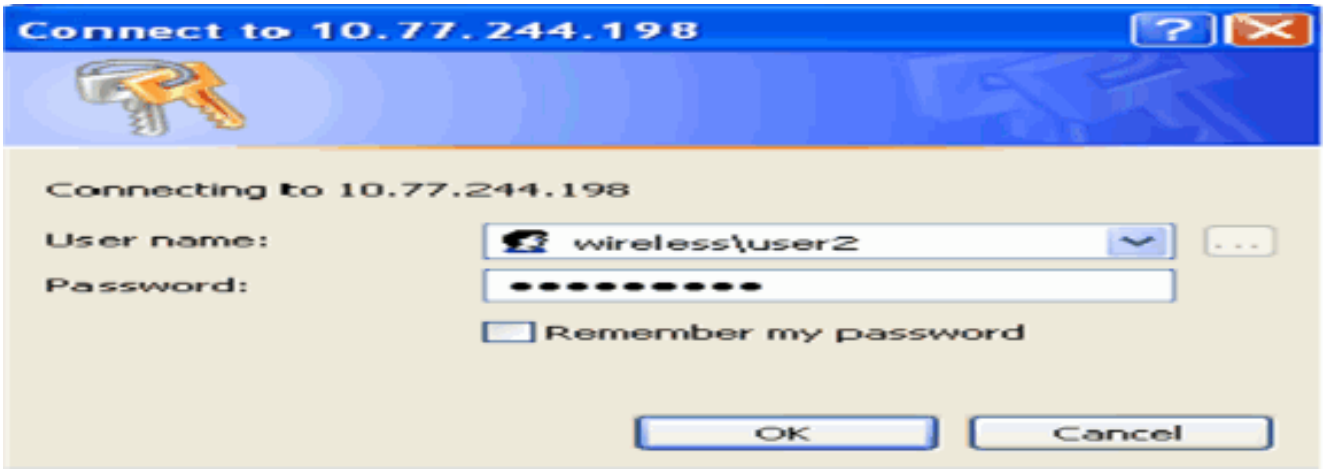


Generar un certificado de dispositivo para el cliente

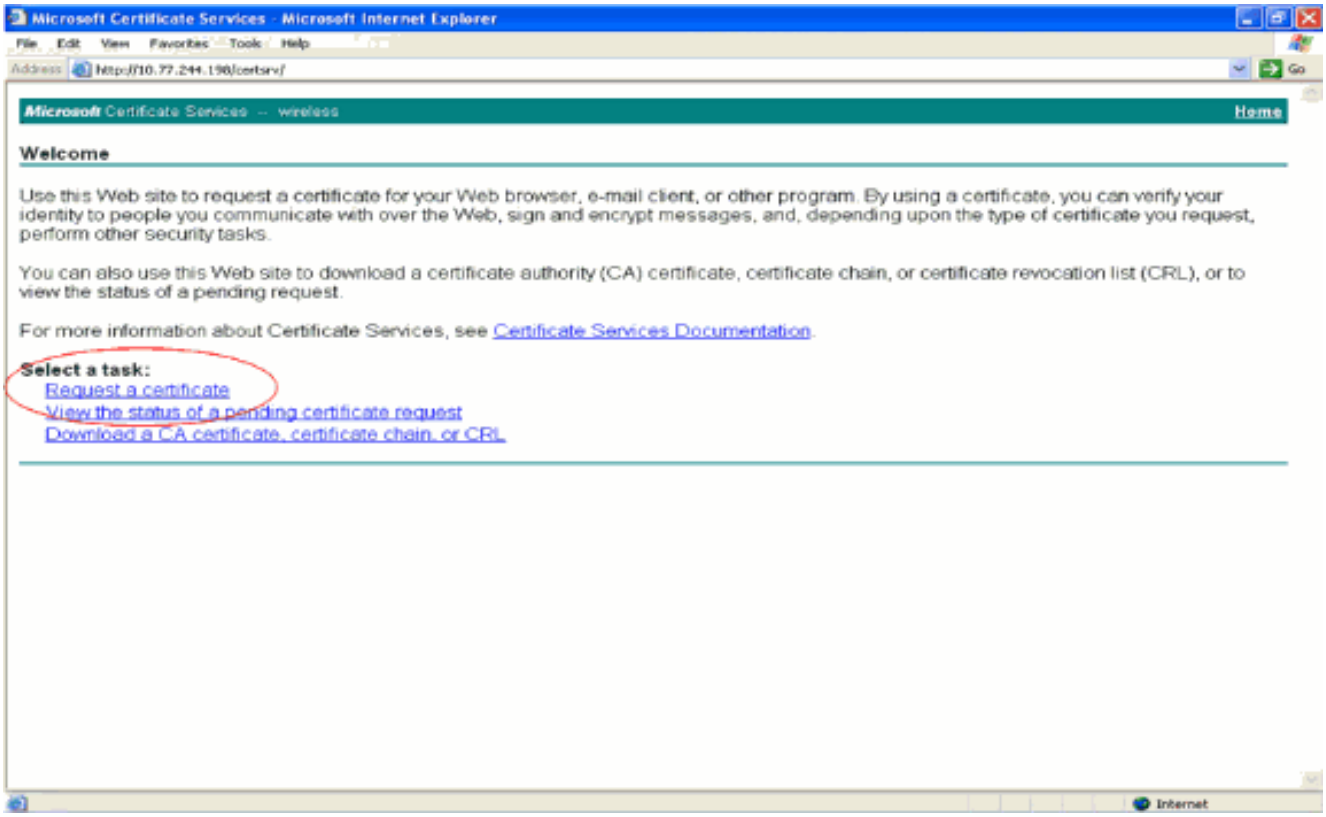
Ahora que el certificado del dispositivo y el certificado de CA están instalados en el WLC, el siguiente paso es generar estos certificados para el cliente.

Realice estos pasos para generar el certificado de dispositivo para el cliente. Este certificado será utilizado por el cliente para autenticar al WLC. Este documento explica los pasos necesarios para generar certificados para el cliente de Windows XP Professional.

1. Vaya a **http://<dirección IP del servidor de la CA>/certsrv** desde el cliente que requiere que se instale el certificado. Inicie sesión como nombre de dominio\nombre de usuario en el servidor de la CA. El nombre de usuario debe ser el nombre del usuario que está utilizando esta máquina XP, y el usuario ya debe estar configurado como parte del mismo dominio que el servidor
   CA.

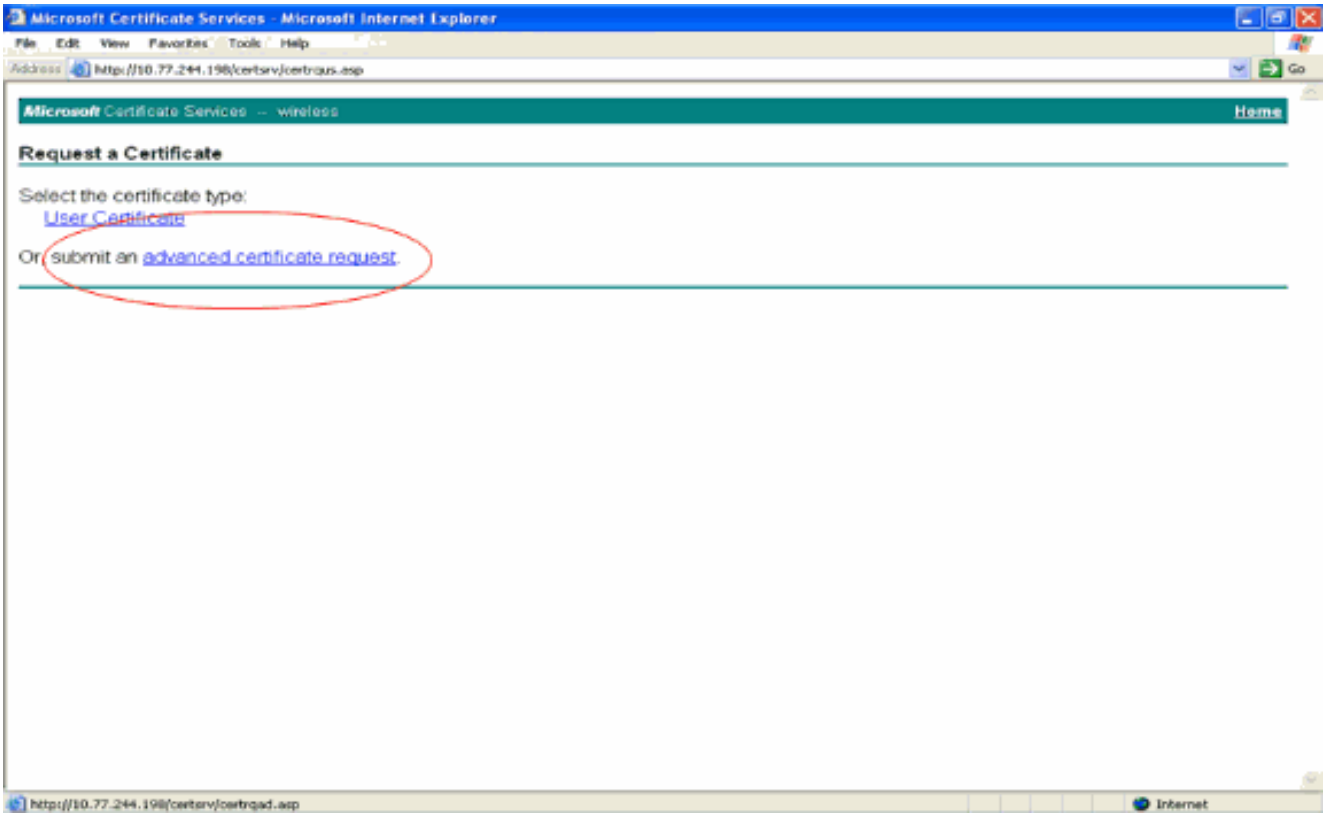


2. Seleccione **Solicitar un certificado**.

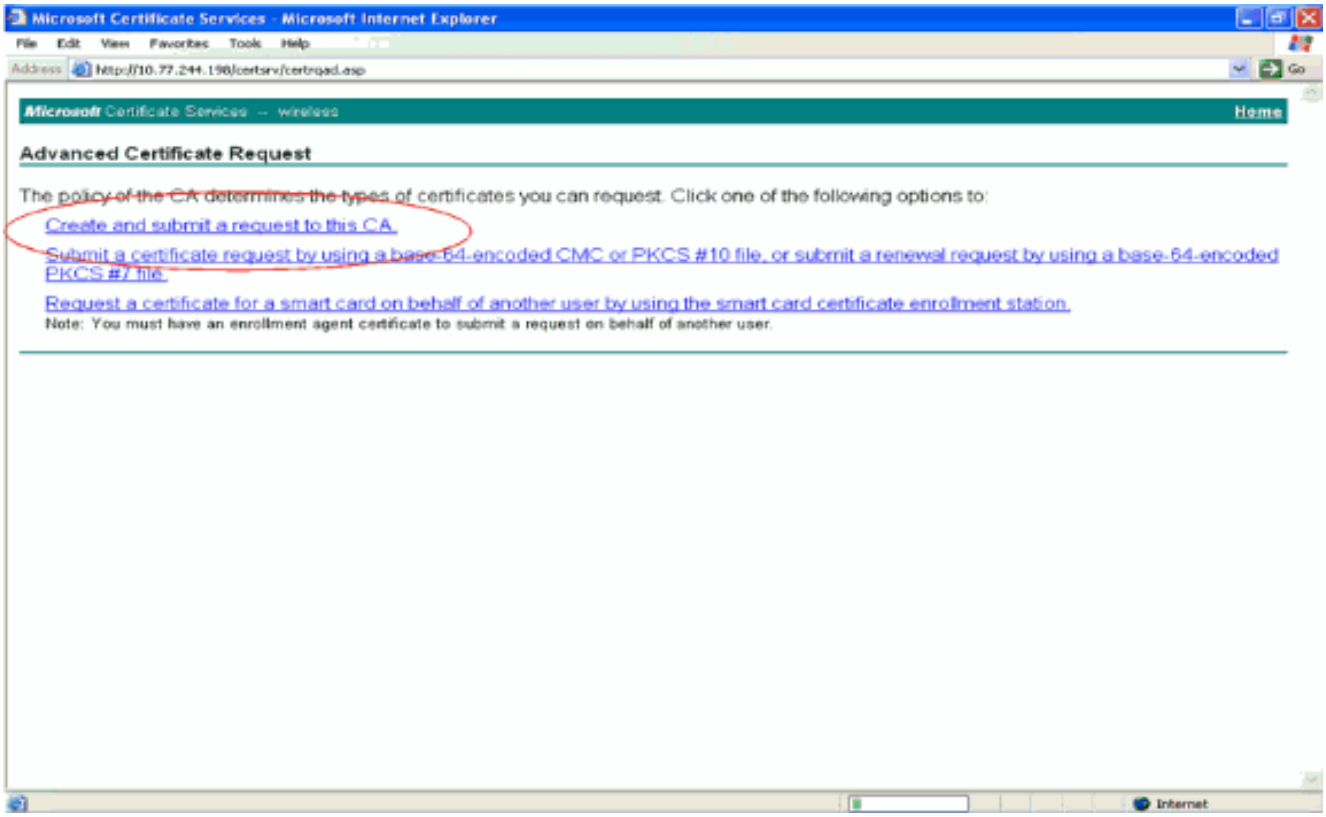


3. En la página Solicitar un certificado, haga clic en **Solicitud de certificado**

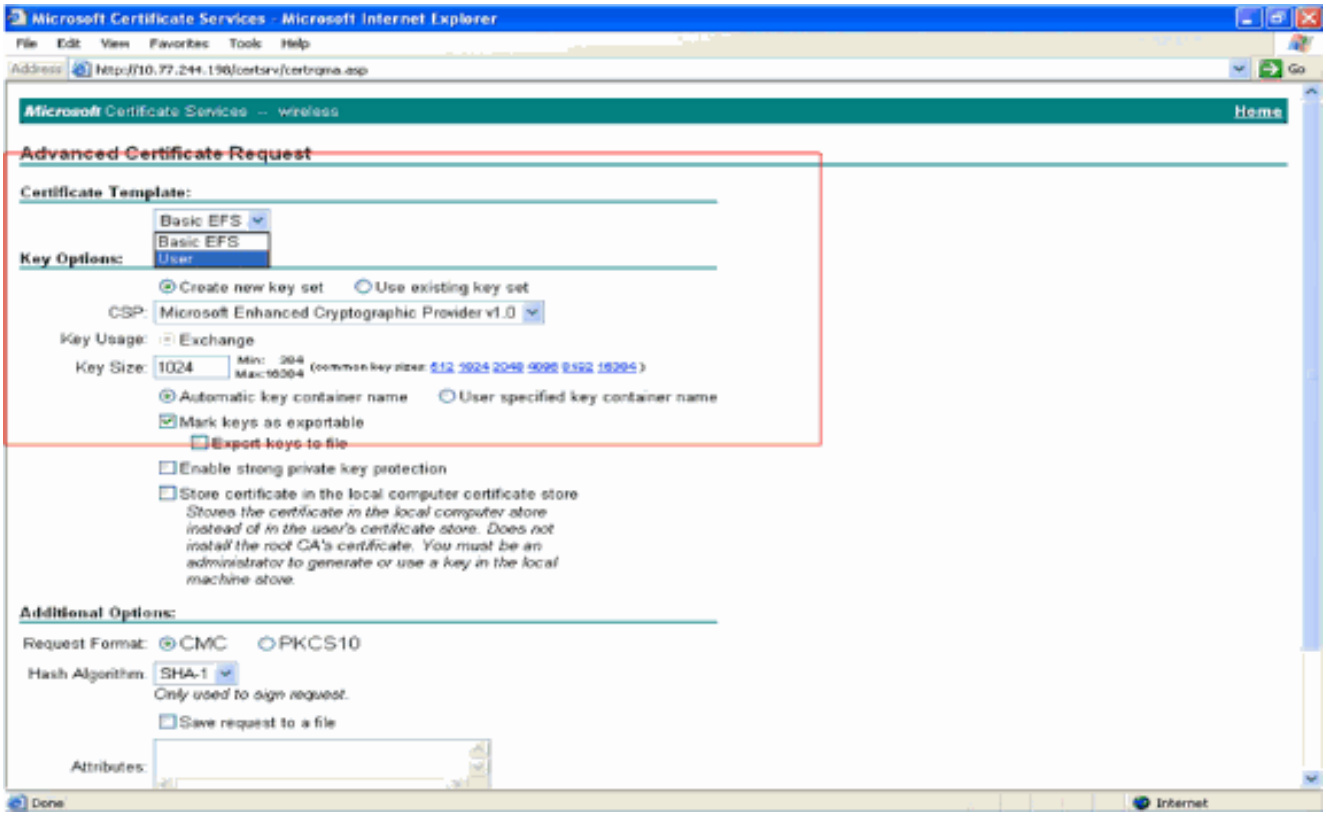
avanzada.



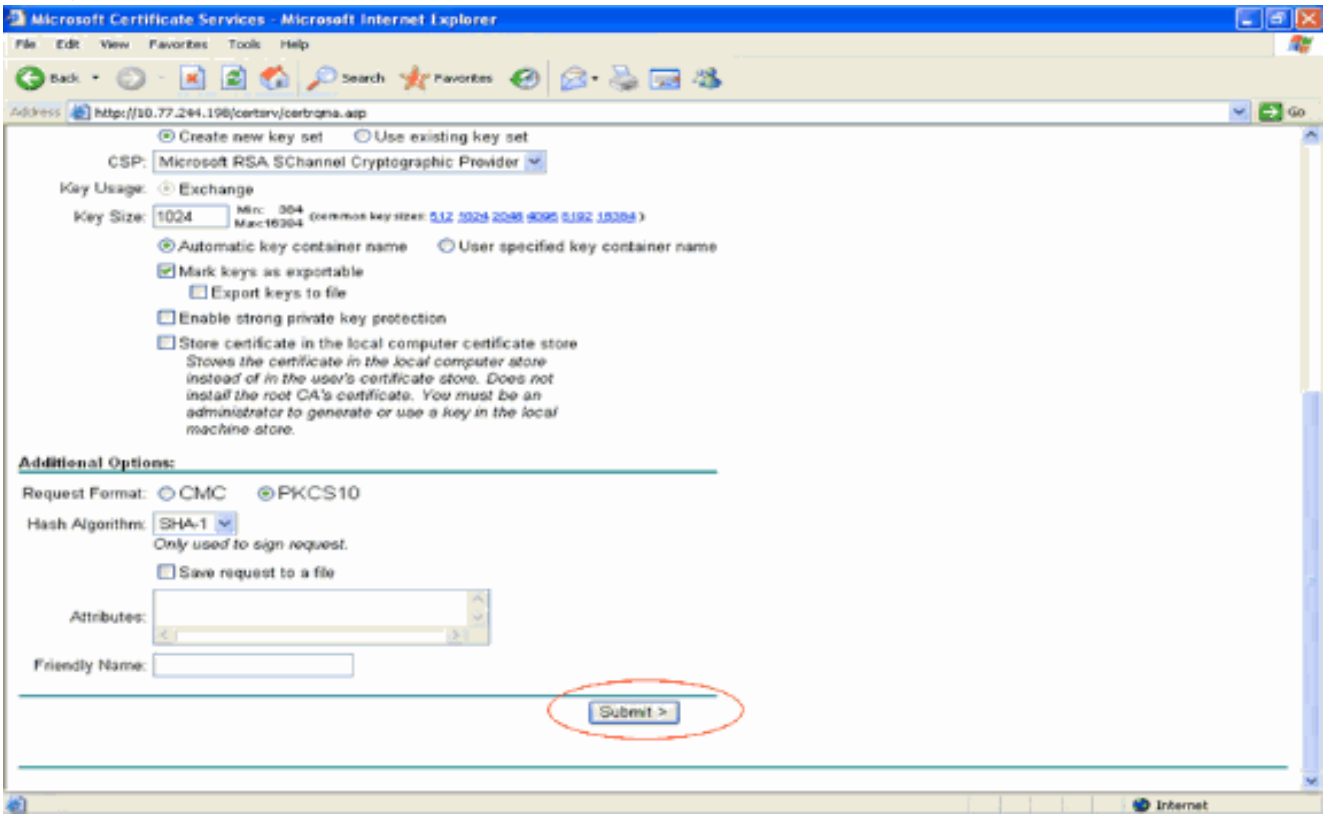
4. En la página Solicitud de certificado avanzada, haga clic en **Crear y enviar una solicitud a esta CA**. Esto lo lleva al formulario de solicitud de certificado avanzado.



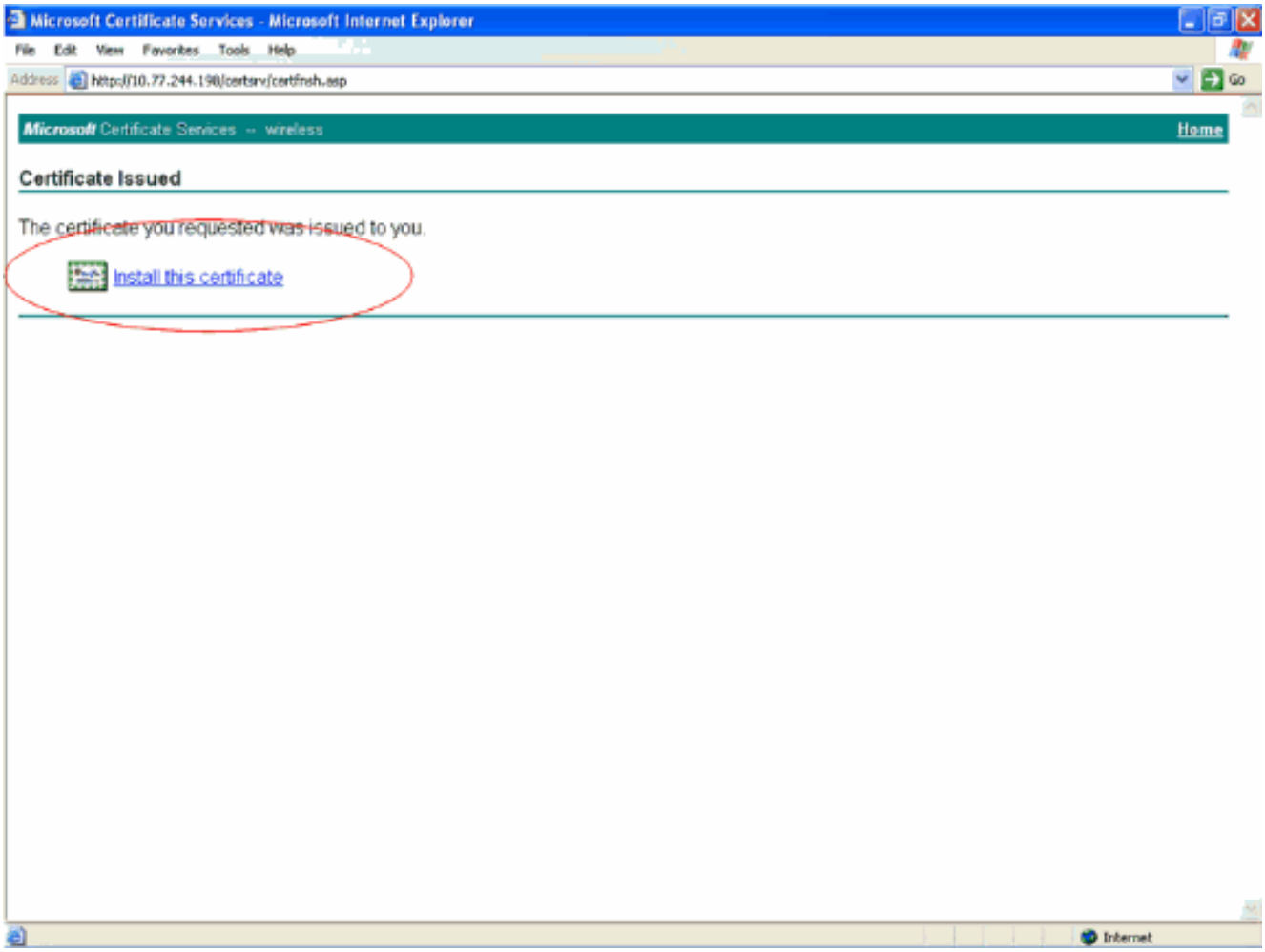
5. En el formulario de solicitud de certificado avanzado, elija **Usuario** en el menú desplegable Plantilla de certificado.En la sección Opciones de clave, elija estos parámetros:Introduzca el tamaño de clave en el campo Key Size (Tamaño de clave). Este ejemplo utiliza 1024.Marque la opción **Mark Keys as Exportable**.



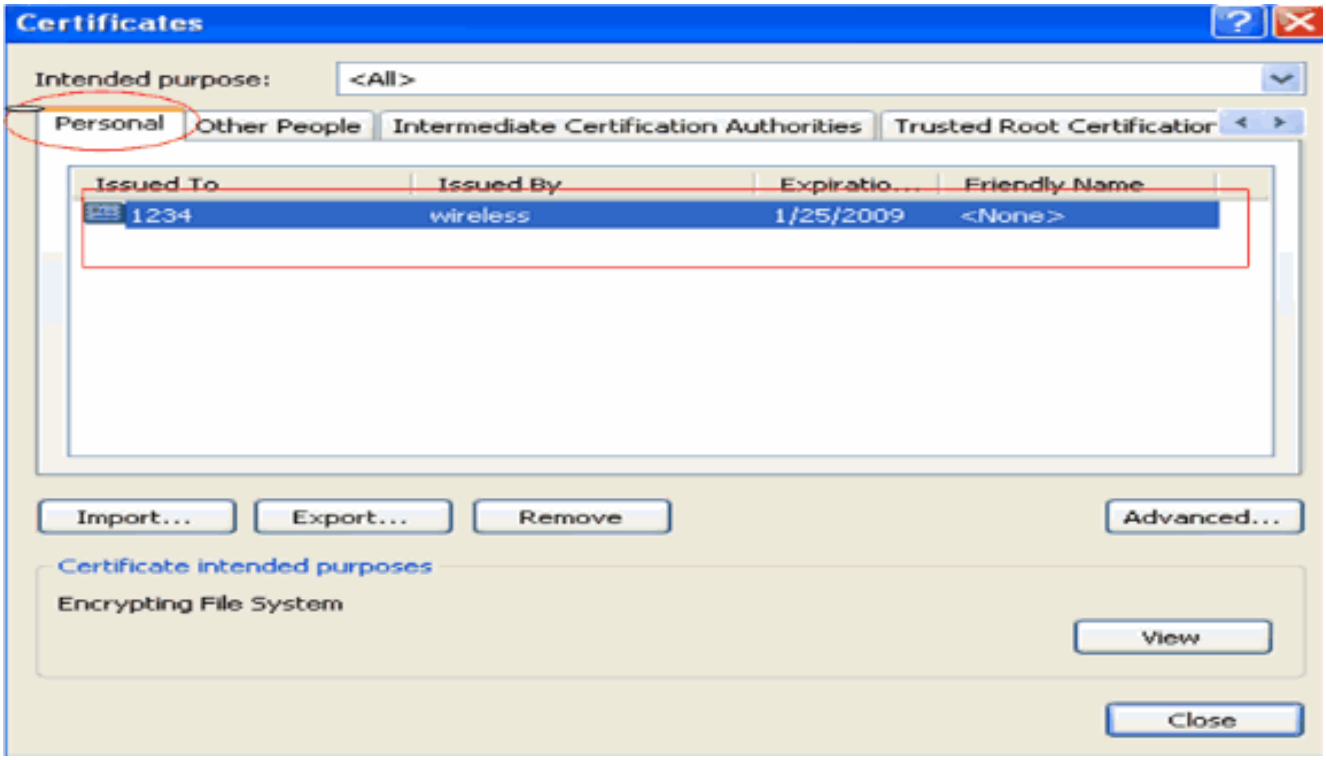
6. Configure todos los demás campos necesarios y haga clic en **Enviar**.



7. El certificado de dispositivo del cliente se genera ahora según la solicitud. Haga clic en **Instalar el certificado** para instalar el certificado en el almacén de certificados.



8. Debería poder encontrar el certificado de dispositivo del cliente instalado en la lista Personal certificate bajo **Tools > Internet Options > Content > Certificates** en el navegador IE del cliente.

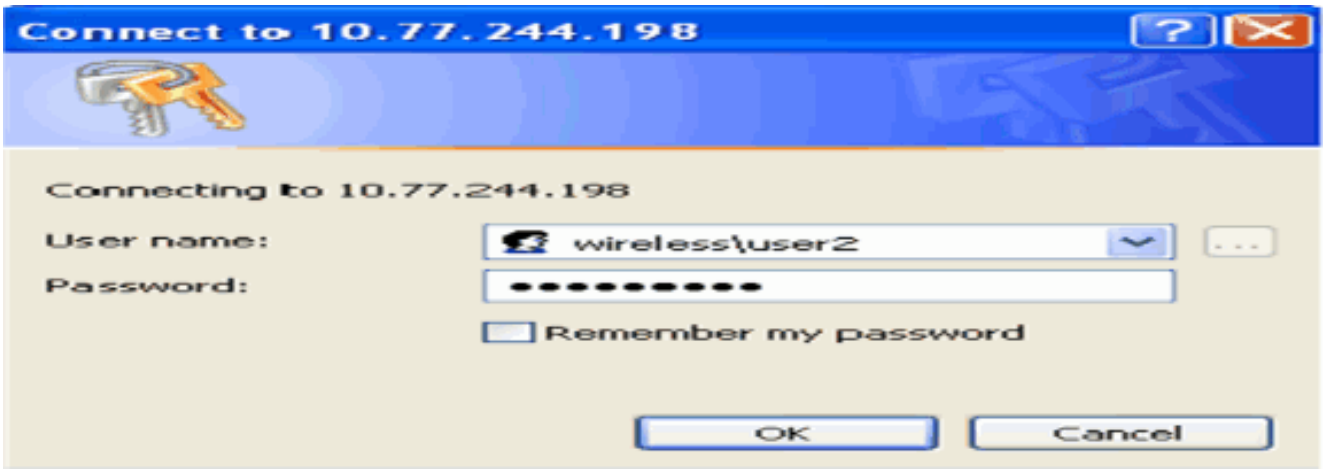


El certificado de dispositivo para el cliente está instalado en el cliente.

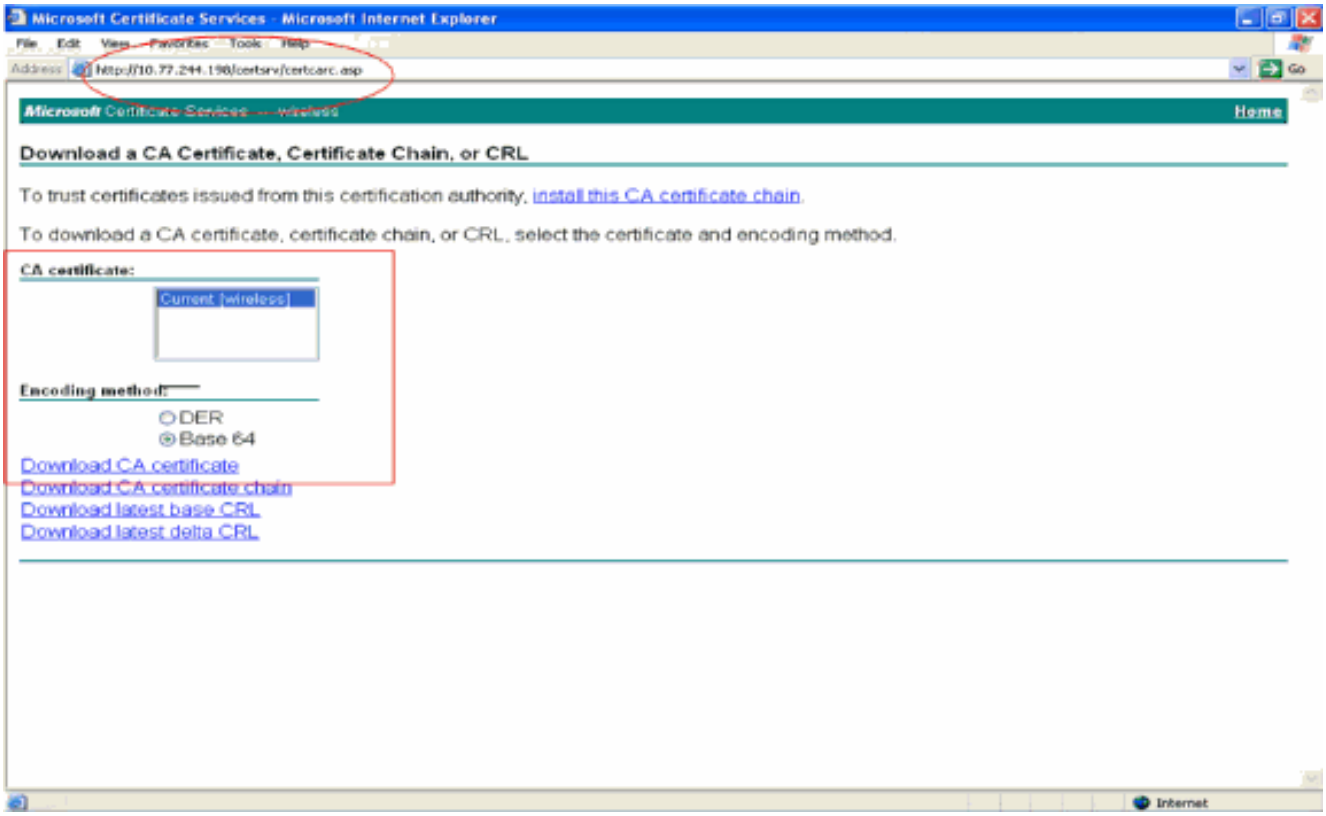
Generar el certificado de CA raíz para el cliente

El siguiente paso es generar el certificado de CA para el cliente. Complete estos pasos desde el PC cliente:

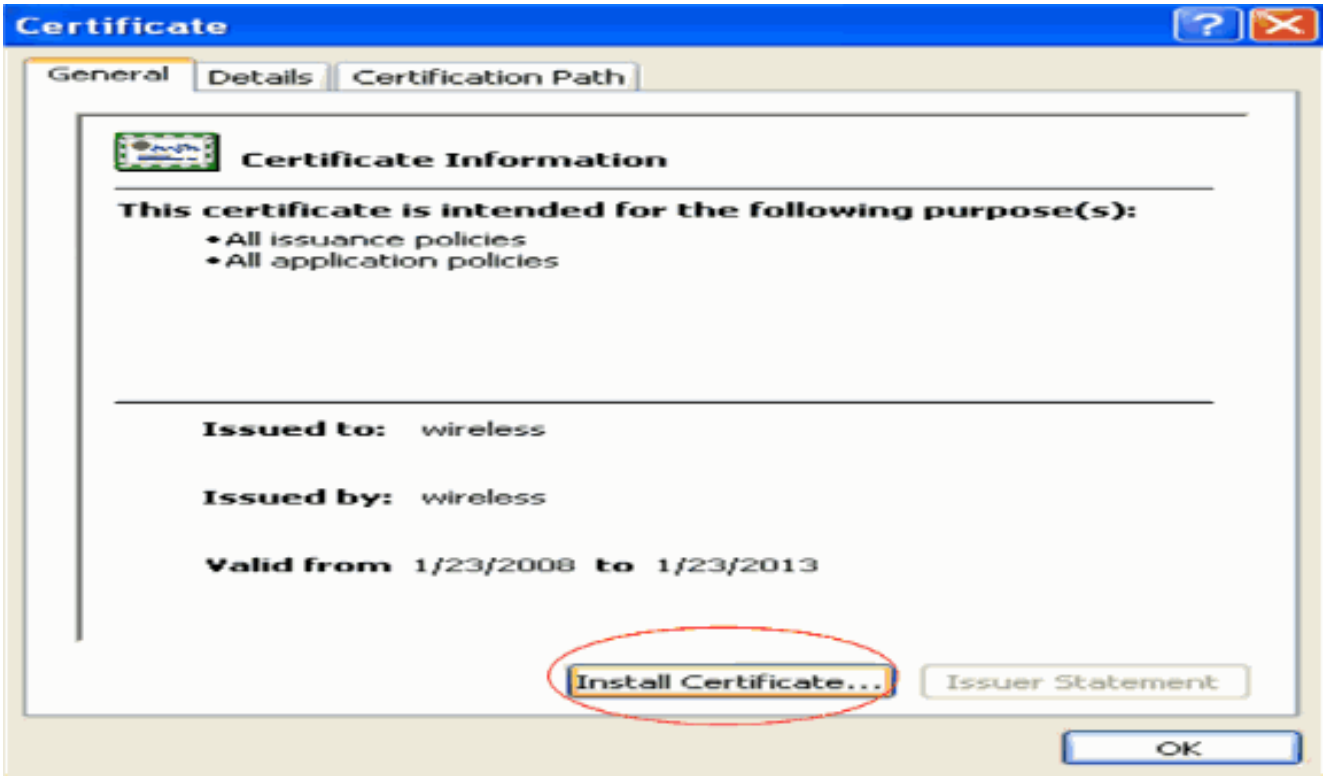
1. Vaya a **http://<dirección IP del servidor de la CA>/certsrv** desde el cliente que requiere que se instale el certificado. Inicie sesión como nombre de dominio\nombre de usuario en el servidor de la CA. El nombre de usuario debe ser el nombre del usuario que está utilizando esta máquina XP, y el usuario ya debe estar configurado como parte del mismo dominio que el servidor
CA.



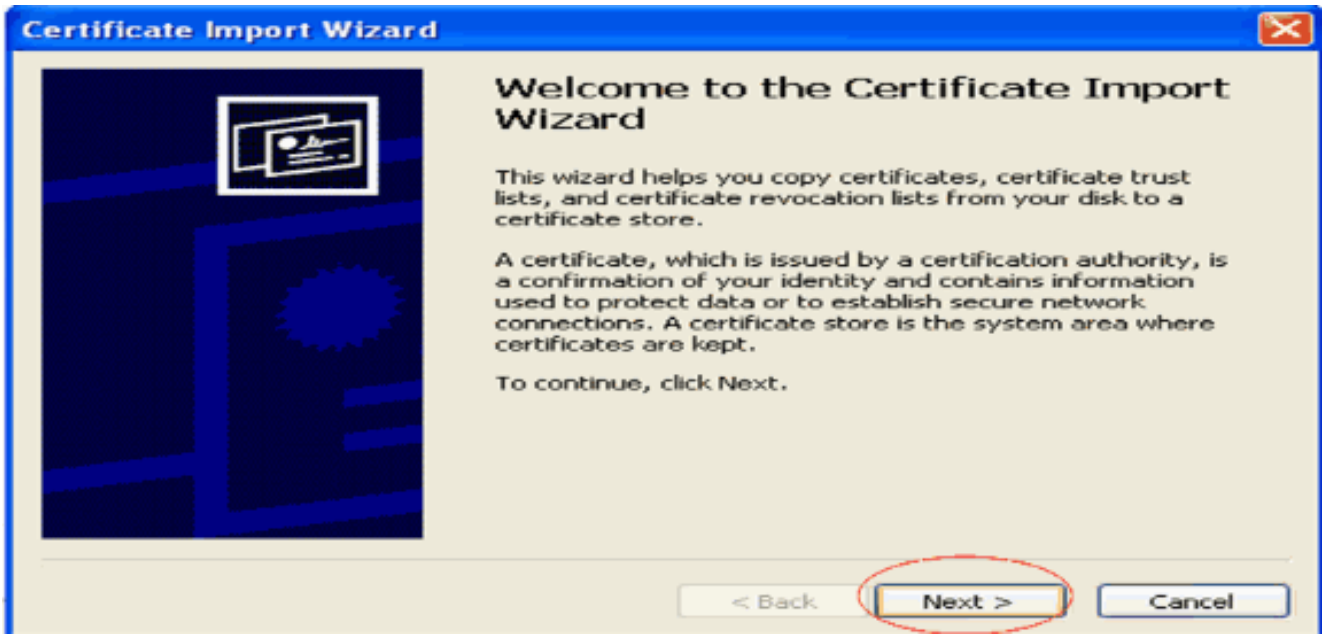
2. En la página resultante, puede ver los certificados de CA actuales disponibles en el servidor de CA en el cuadro **Certificado de CA**. Elija **Base 64** como método de codificación. A continuación, haga clic en **Descargar certificado de CA** y guarde el archivo en el equipo del cliente como un archivo **.cer**. Este ejemplo utiliza **rootca.cer** como nombre de archivo.



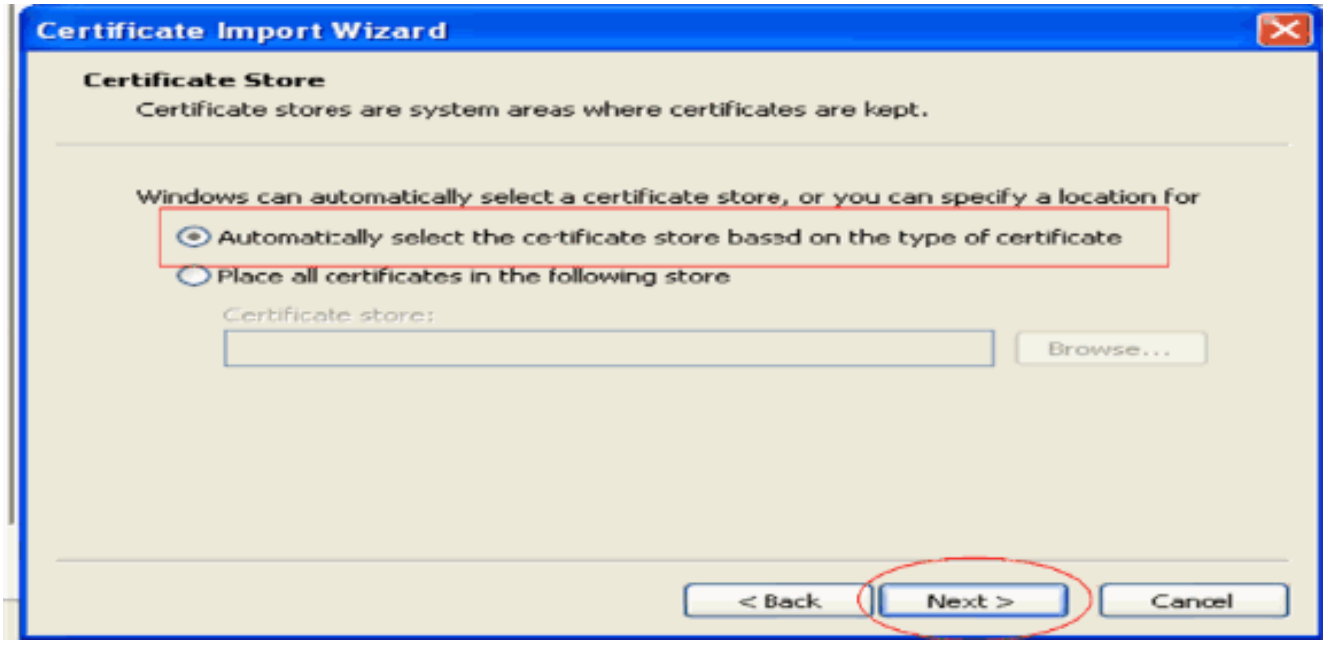
3. A continuación, instale el certificado de CA guardado en formato .cer en el almacén de certificados del cliente. Haga doble clic en el archivo rootca.cer y haga clic en **Install Certificate**.



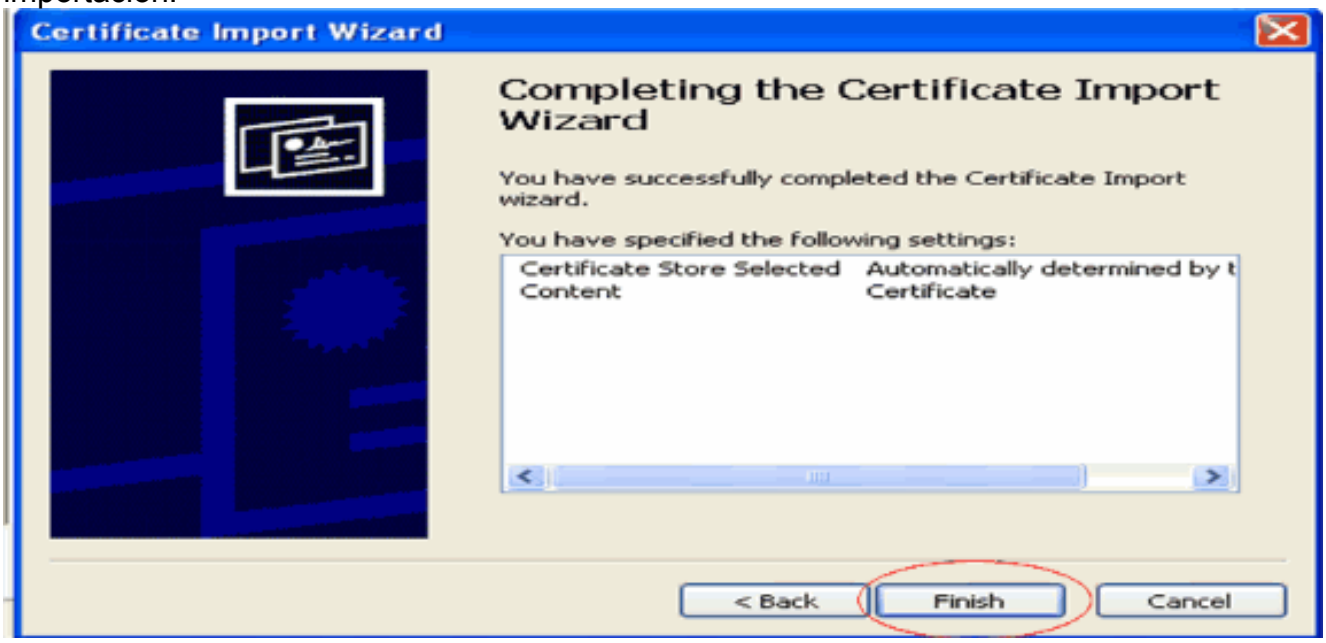
4. Haga clic en **Siguiente** para importar el certificado del disco duro del cliente al almacén de certificados.



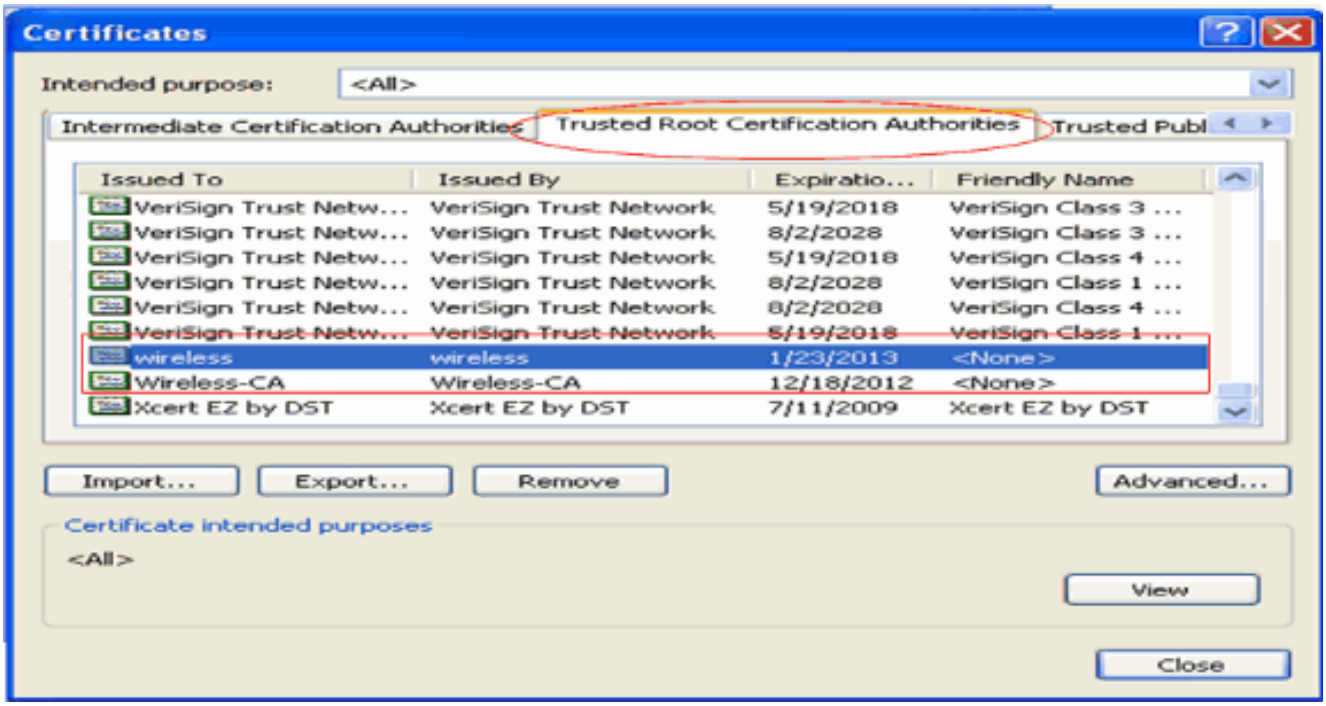
5. Elija **Automatically select the certificate store based on the type of certificate** y haga clic en **Next**.



6. Haga clic en **Finalizar** para terminar el proceso de importación.



7. De forma predeterminada, los certificados de CA se instalan en la lista Entidades de certificación raíz de confianza del explorador IE del cliente en **Herramientas > Opciones de Internet > Contenido > Certificados**. Este es el ejemplo:

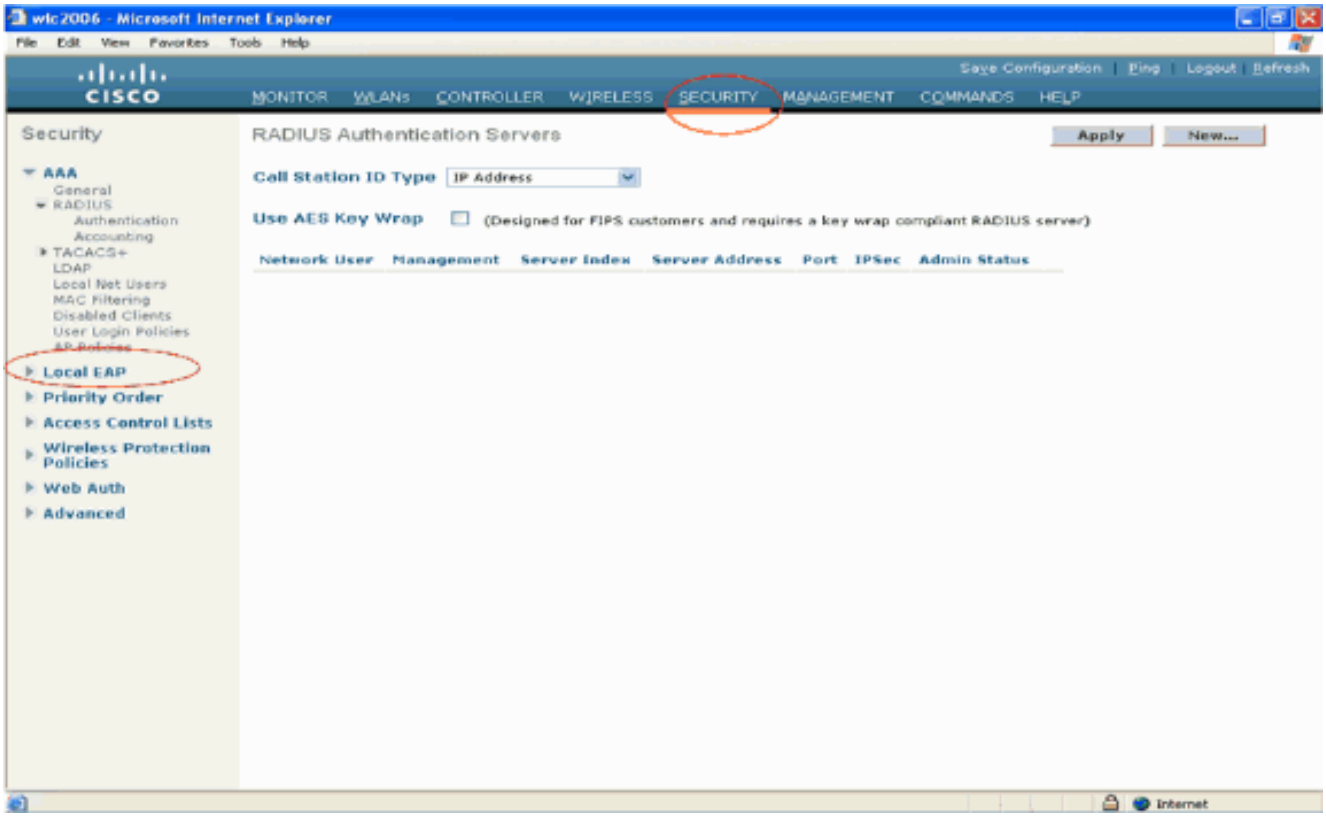


Todos los certificados requeridos se instalan en el WLC así como en el cliente para la autenticación EAP local EAP-FAST. El siguiente paso es configurar el WLC para la autenticación EAP local.

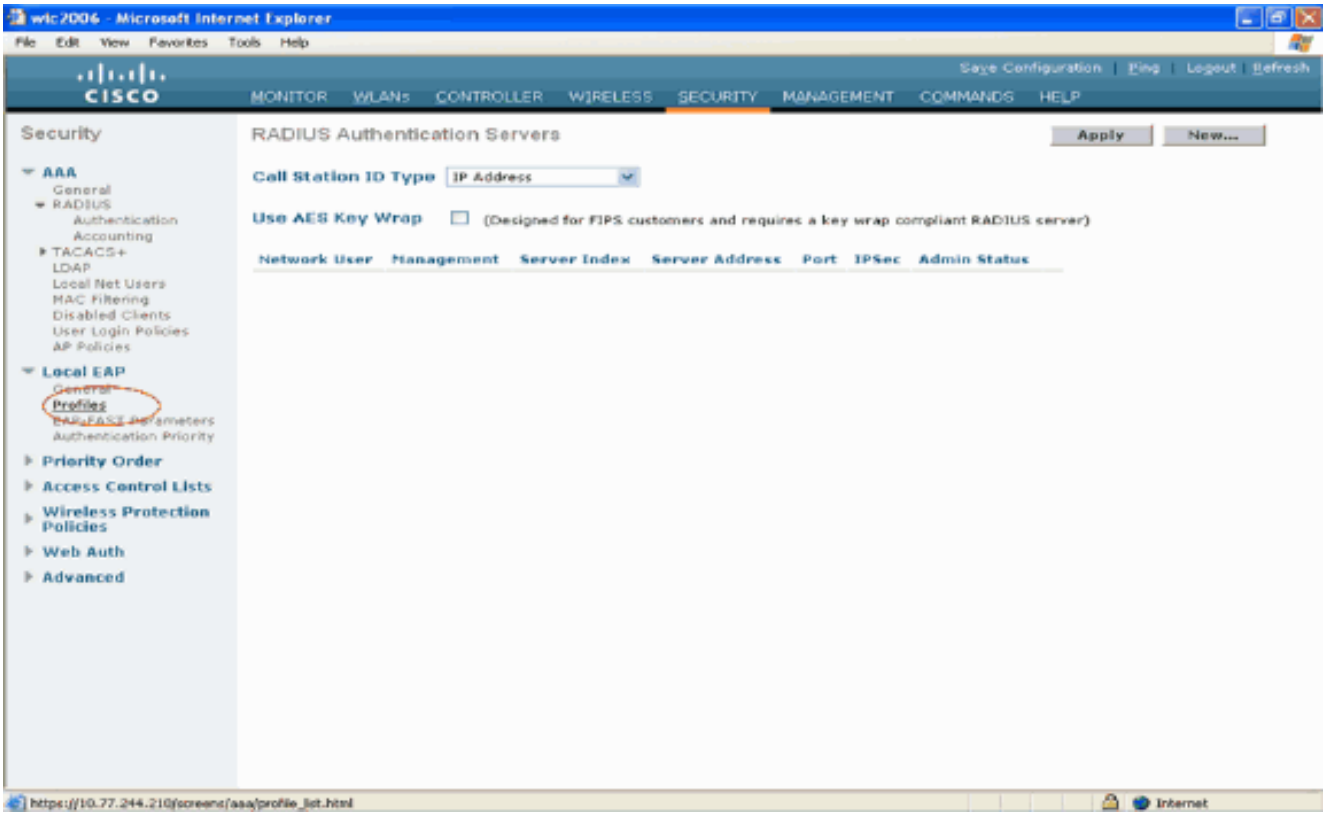
Configuración de EAP local en el WLC

Complete estos pasos del **modo GUI del WLC** para configurar la autenticación EAP local en el WLC:

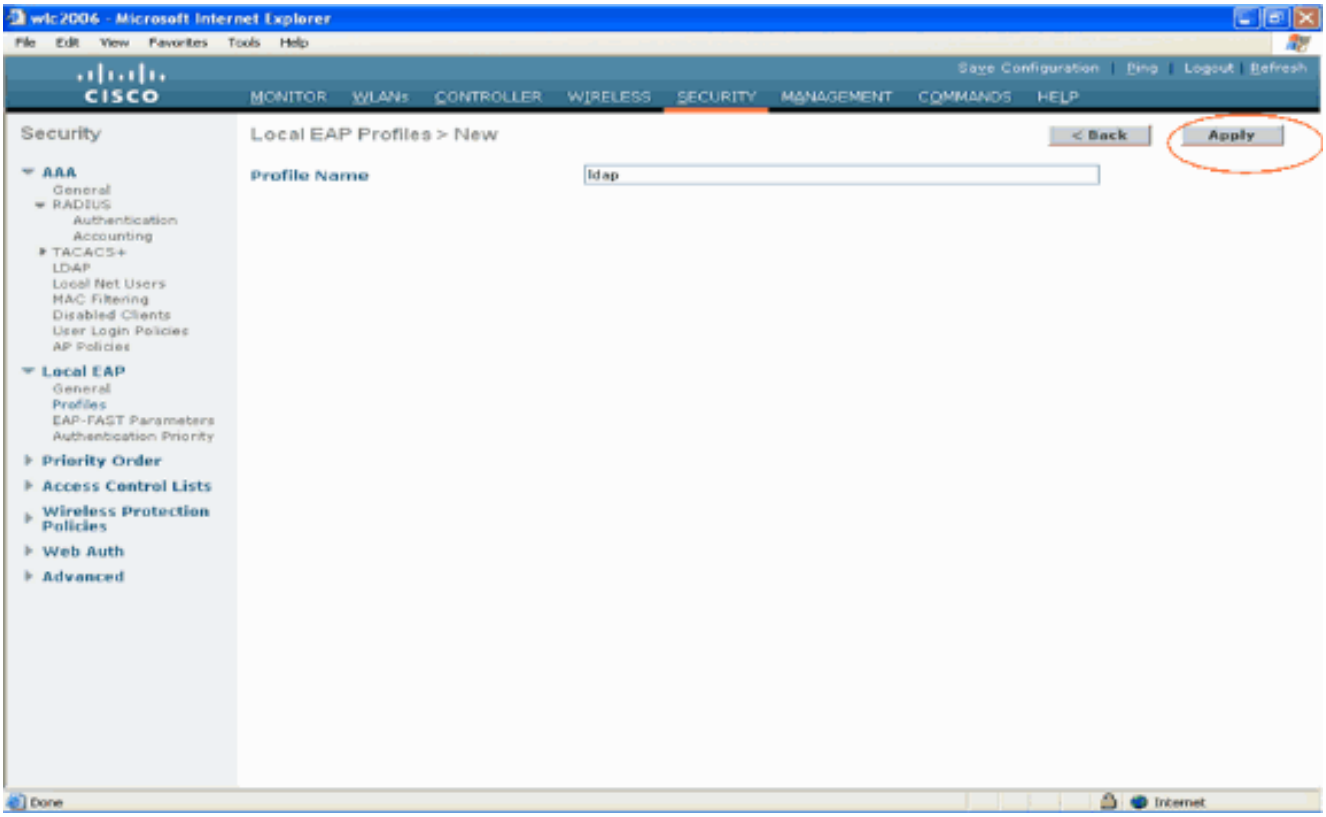
1. Haga clic en **Seguridad > EAP local**.



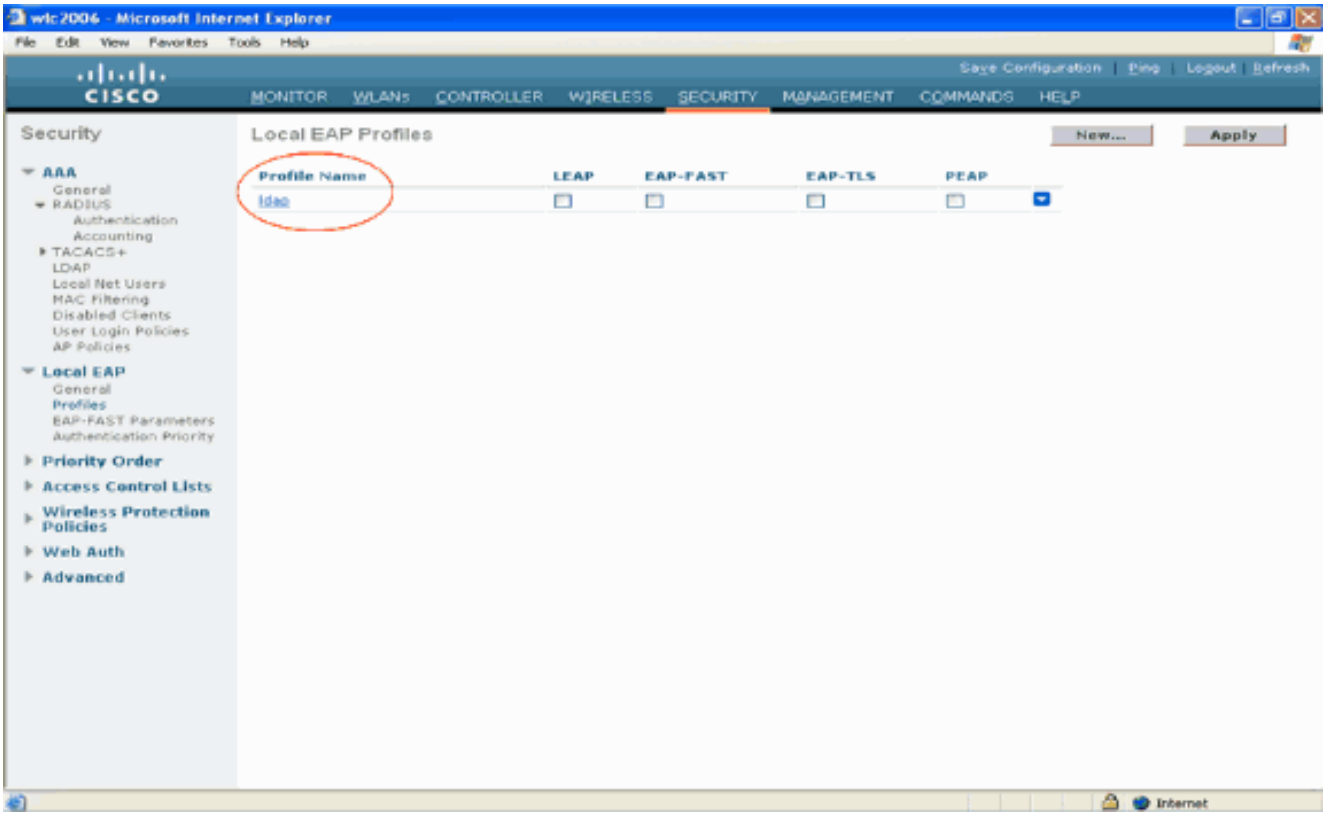
2. Bajo EAP local, haga clic en **Perfiles** para configurar el perfil EAP local.



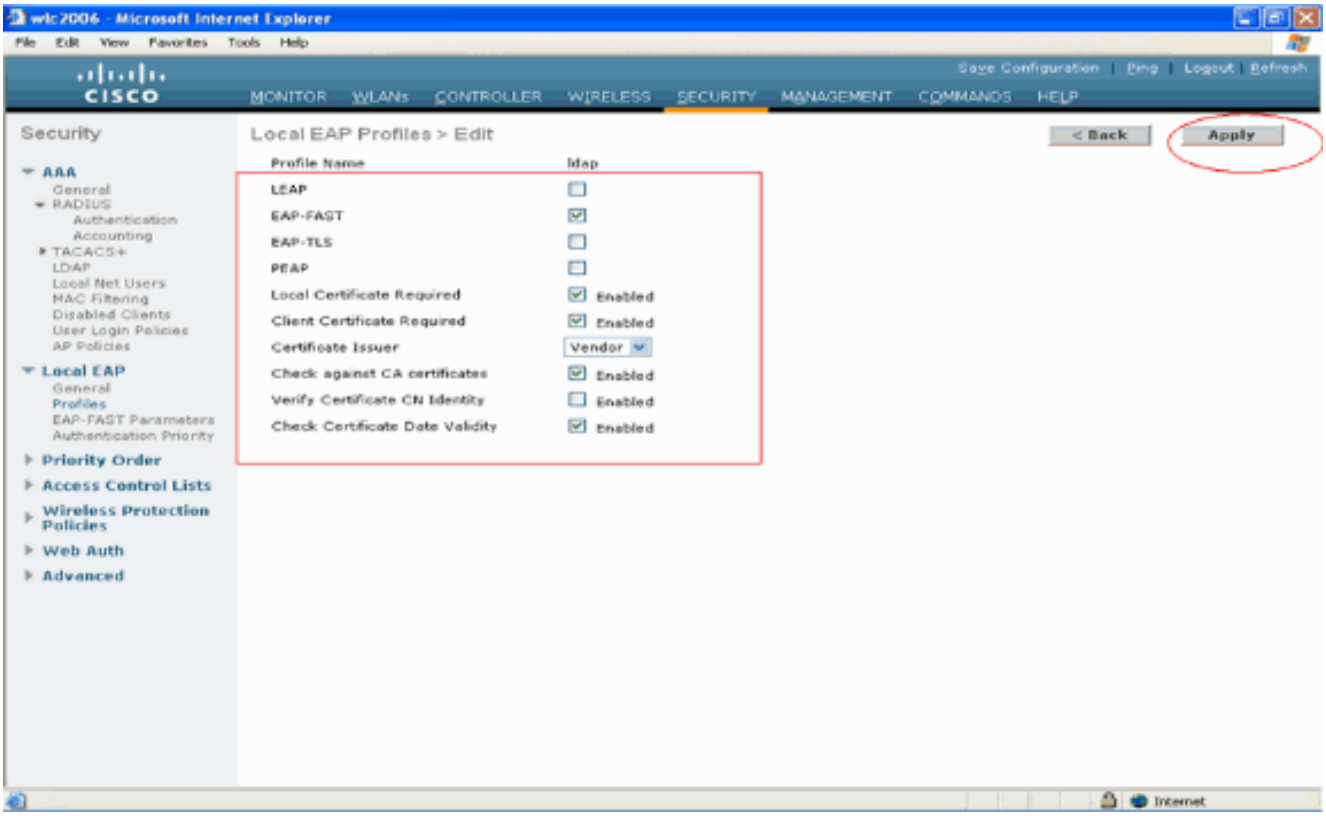
3. Haga clic en **Nuevo** para crear un nuevo perfil EAP local.
4. Configure un nombre para este perfil y haga clic en **Apply**. En este ejemplo, el nombre del perfil es **ldap**. Esto lo lleva a los perfiles EAP locales creados en el WLC.



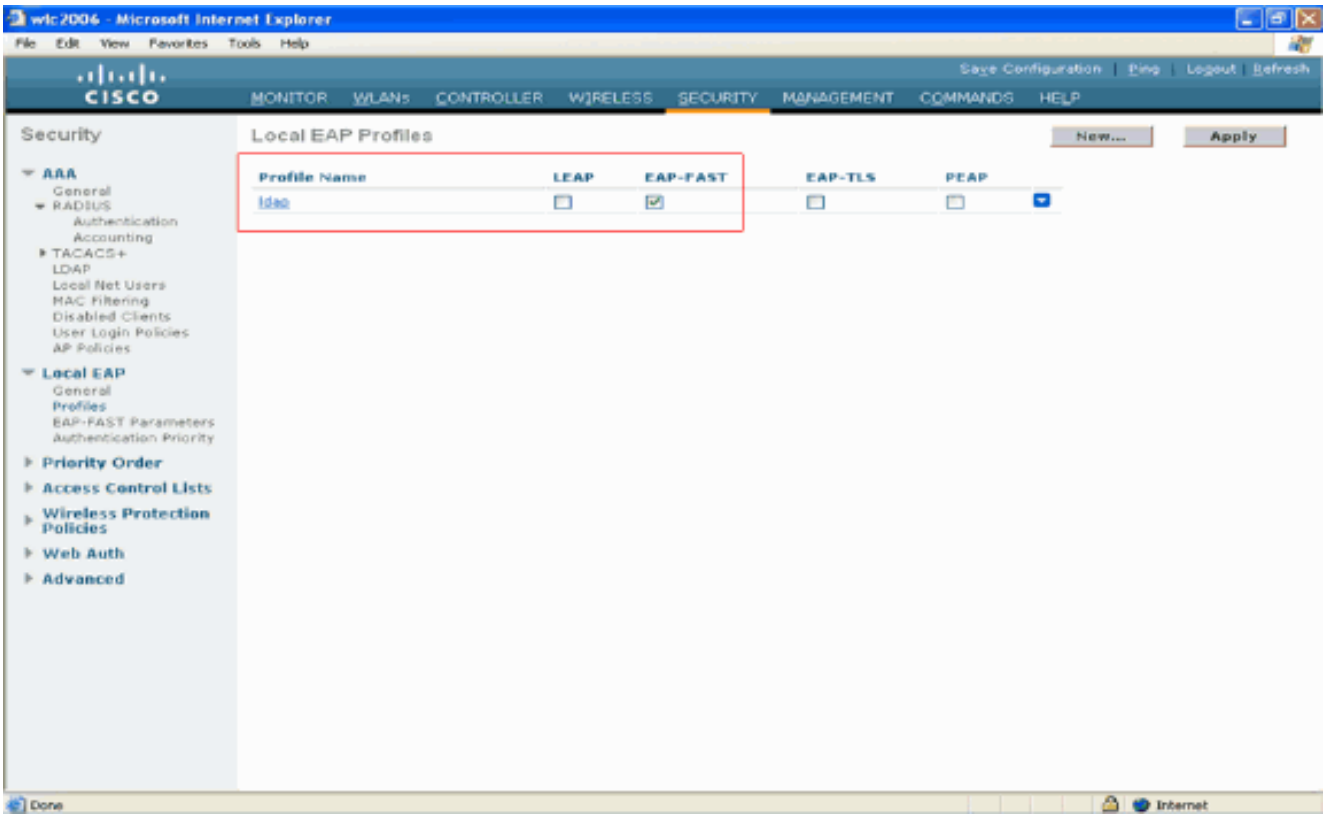
5. Haga clic en el perfil **ldap** que se acaba de crear, que aparece en el campo Profile Name (Nombre de perfil) de la página Local EAP Profiles (Perfiles EAP locales). Esto lo lleva a la página **Perfiles EAP locales > Editar**.



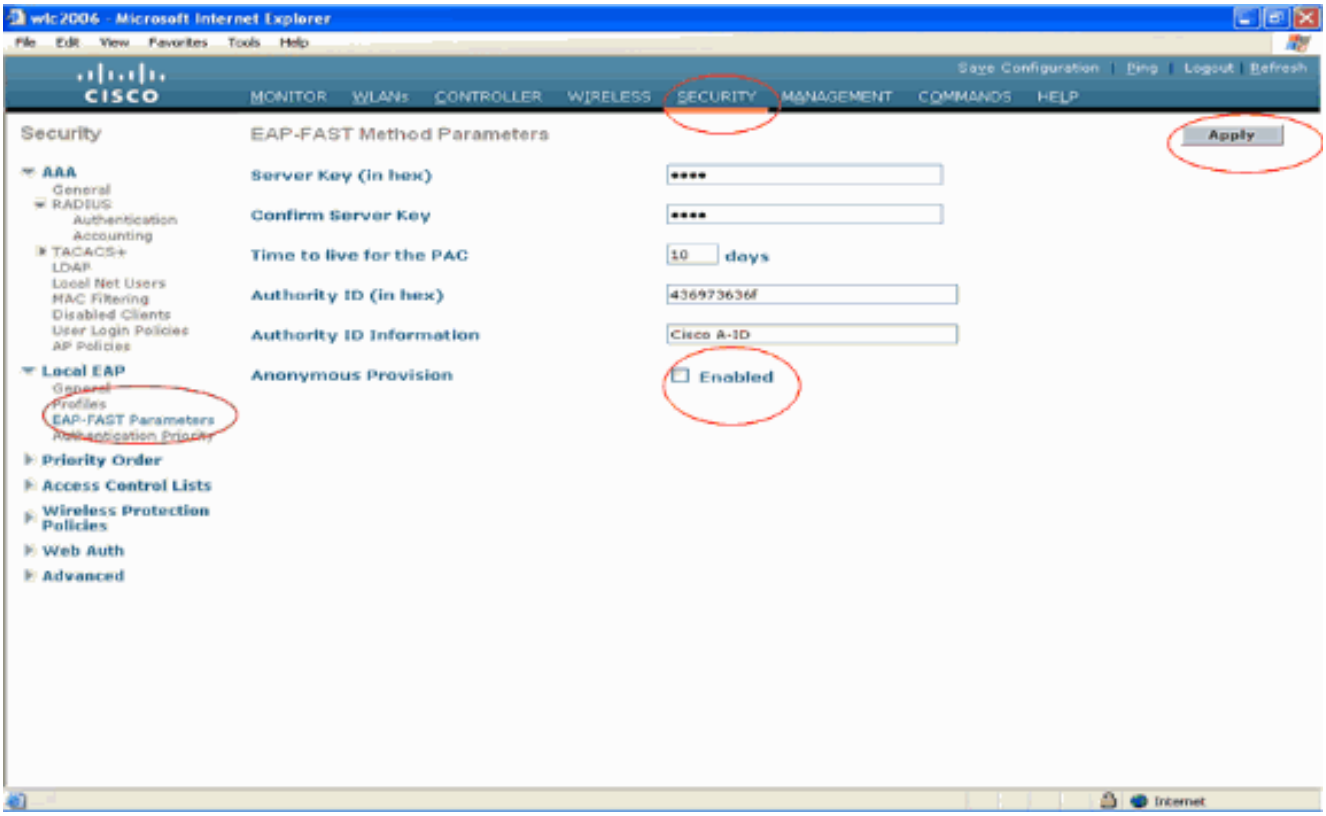
6. Configure los parámetros específicos para este perfil en la página **Perfiles EAP locales > Editar**.Elija **EAP-FAST** como el método de autenticación EAP local.Active las casillas de verificación junto a **Certificado local obligatorio** y **Certificado de cliente obligatorio**.Elija **Vendor** como emisor del certificado porque este documento utiliza un servidor CA de terceros.Habilite la casilla de verificación junto a **Verificar con certificados de CA** para permitir que el certificado entrante del cliente se valide con los certificados de CA en el controlador.Si desea que el nombre común (CN) del certificado entrante se valide con el CN de los certificados de CA en el controlador, marque la casilla de verificación **Verificar identidad CN del certificado**. La configuración predeterminada está desactivada. Para permitir que el controlador verifique que el certificado del dispositivo entrante sigue siendo válido y no ha caducado, marque la casilla de verificación **Verificar validez de fecha del certificado**.**Nota:** La validez de la fecha del certificado se comprueba con la hora UTC (GMT) actual configurada en el controlador. El desplazamiento de la zona horaria se ignora.Haga clic en Apply
(Aplicar).



7. El perfil EAP local con autenticación EAP-FAST se crea ahora en el WLC.



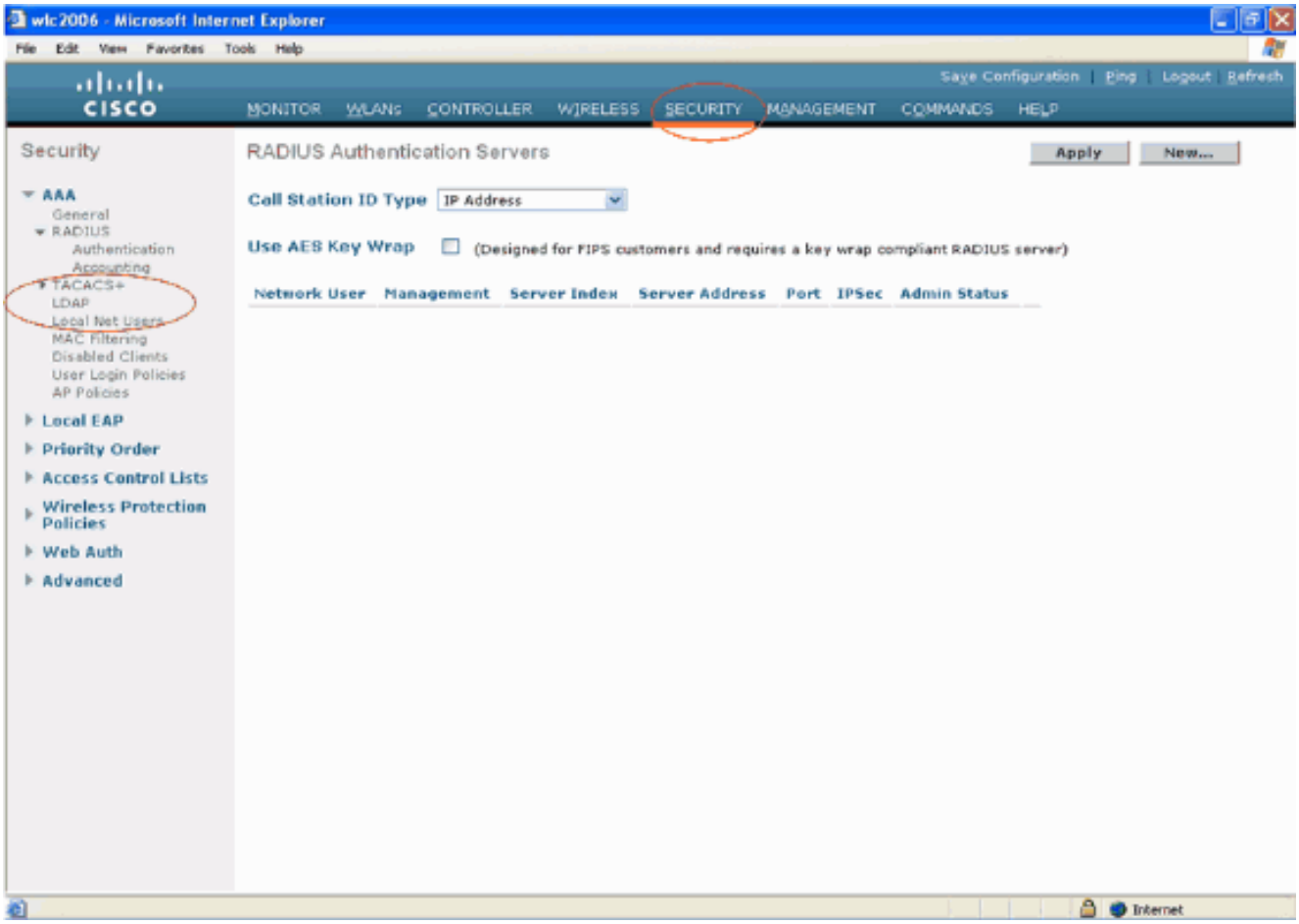
8. El siguiente paso es configurar los parámetros específicos de EAP-FAST en el WLC. En la página WLC Security, haga clic en **Local EAP > EAP-FAST Parameters** para moverse a la página EAP-FAST Method Parameters.Desmarque la casilla de verificación **Anonymous Provisioning** porque en este ejemplo se explica EAP-FAST mediante certificados. Deje el resto de los parámetros predeterminados. Haga clic en Apply (Aplicar).



Configuración de WLC con Detalles del Servidor LDAP

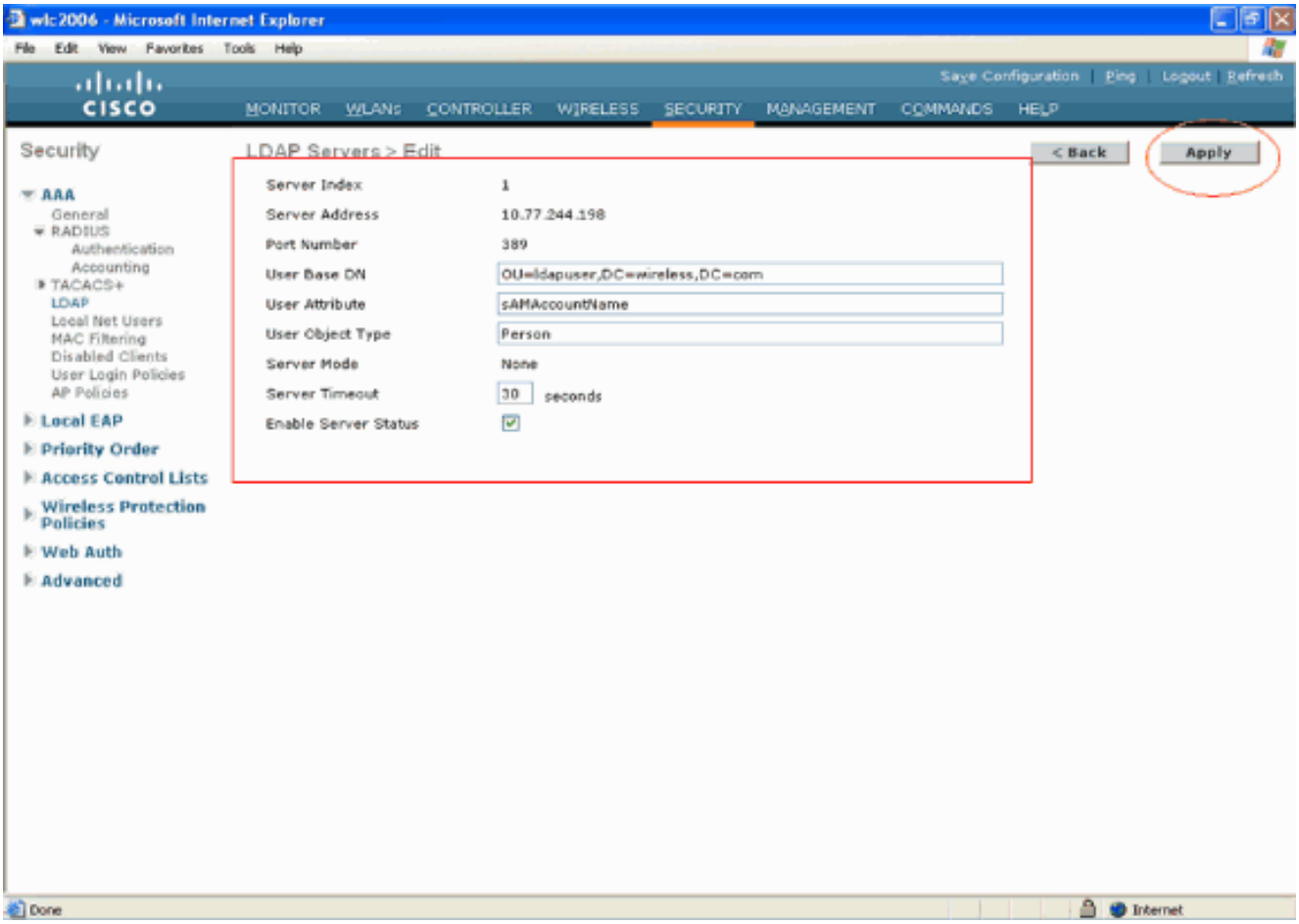
Ahora que el WLC se configura con el perfil EAP local y la información relacionada, el paso siguiente es configurar el WLC con los detalles del servidor LDAP. Complete estos pasos en el WLC:

1. En la página **Seguridad** del WLC, seleccione **AAA > LDAP** del panel de tareas del lado izquierdo para moverse a la página de configuración del servidor LDAP. Para agregar un servidor LDAP, haga clic en **New**. Se abrirá la ventana LDAP Servers > New.



2. En la página LDAP Servers Edit (Editar servidores LDAP), especifique los detalles del servidor LDAP, como la dirección IP del servidor LDAP, el número de puerto, el estado del servidor Enable (Habilitar), etc.Elija un número en el cuadro desplegable **Server Index (Priority)** para especificar el orden de prioridad de este servidor en relación con cualquier otro servidor LDAP configurado. Puede configurar hasta diecisiete servidores. Si el controlador no puede alcanzar el primer servidor, intenta el segundo en la lista y así sucesivamente.Ingrese la dirección IP del servidor LDAP en el campo **Server IP Address**.Ingrese el número de puerto TCP del servidor LDAP en el campo **Port Number**. El intervalo válido es 1 a 65535, y el valor predeterminado es 389.En el campo User Base DN, ingrese el nombre distintivo (DN) de la sub-estructura en el servidor LDAP que contiene una lista de todos los usuarios. Por ejemplo, ou=organizational unit, .ou=next organizational unit o o=corporation.com. Si el árbol que contiene usuarios es el DN base, introduzca o=corporation.com o dc=corporation, dc=com.En este ejemplo, el usuario se encuentra bajo el **ldapuser** de la unidad organizativa (OU) que, a su vez, se crea como parte del dominio **Wireless.com**.El DN base de usuario debe indicar la ruta completa en la que se encuentra la información de usuario (credencial de usuario según el método de autenticación EAP-FAST). En este ejemplo, el usuario se encuentra en el DN base OU=ldapuser, DC=Wireless, DC=com.En la sección Creación de Usuarios en el Controlador de Dominio de este documento se explican más detalles sobre OU, así como la configuración del usuario.En el campo User Attribute, ingrese el nombre del atributo en el registro de usuarios que contiene el nombre de usuario.En el campo User Object Type, ingrese el valor del atributo objectType del LDAP que identifica el registro como usuario. A menudo, los registros de usuario tienen varios valores para el atributo objectType, algunos de los cuales son únicos al usuario y otros son compartidos con otros tipos de objeto.**Nota:** Puede obtener el valor de estos dos campos desde el servidor de directorios con la utilidad de explorador LDAP, que se incluye como parte de las herramientas de soporte de Windows 2003. **Esta herramienta del**

navegador LDAP de Microsoft se llama LDP. Con la ayuda de esta herramienta, puede conocer los campos User Base DN, User Attribute y User Object Type de este usuario en particular. La información detallada sobre el uso de LDP para conocer estos atributos específicos del usuario se discute en la sección Uso de LDP para Identificar los Atributos del Usuario de este documento.Elija **Secure** en el cuadro desplegable Server Mode si desea que todas las transacciones LDAP utilicen un túnel TLS seguro. De lo contrario, elija **None**, que es la configuración predeterminada.En el campo **Server Timeout**, ingrese el número de segundos entre retransmisiones. El intervalo válido es de 2 a 30 segundos, y el valor predeterminado es 2 segundos.Marque la casilla de verificación **Enable Server Status** para habilitar este servidor LDAP, o desmárquela para inhabilitarlo. Se inhabilitará el valor predeterminado.Haga clic en Apply para aplicar sus cambios.A continuación se muestra un ejemplo ya configurado con esta
información:



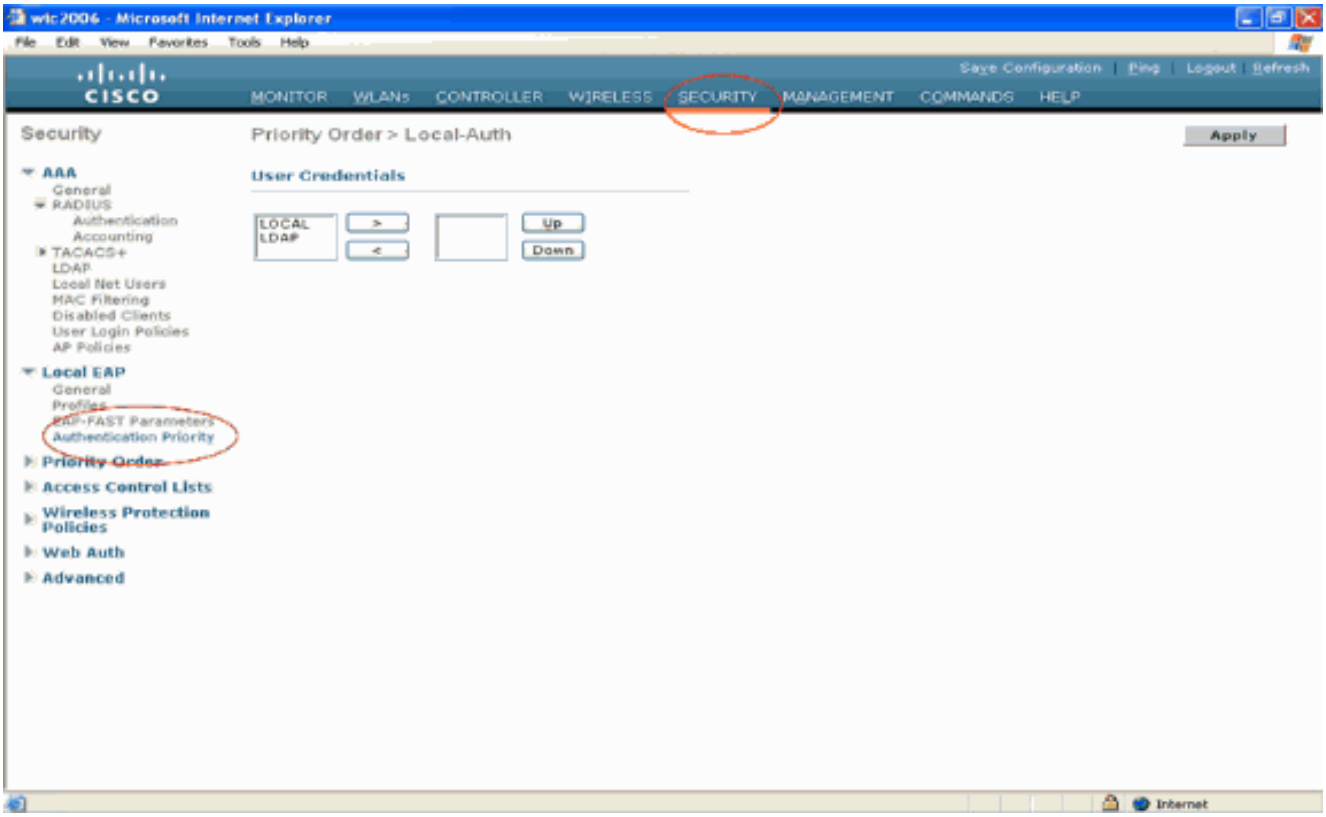
Ahora que los detalles sobre el servidor LDAP se configuran en el WLC, el paso siguiente es configurar LDAP como la base de datos backend prioritaria para que el WLC primero mire a la base de datos LDAP para las credenciales del usuario en lugar de cualquier otra base de datos.

Configuración de LDAP como la base de datos backend prioritaria

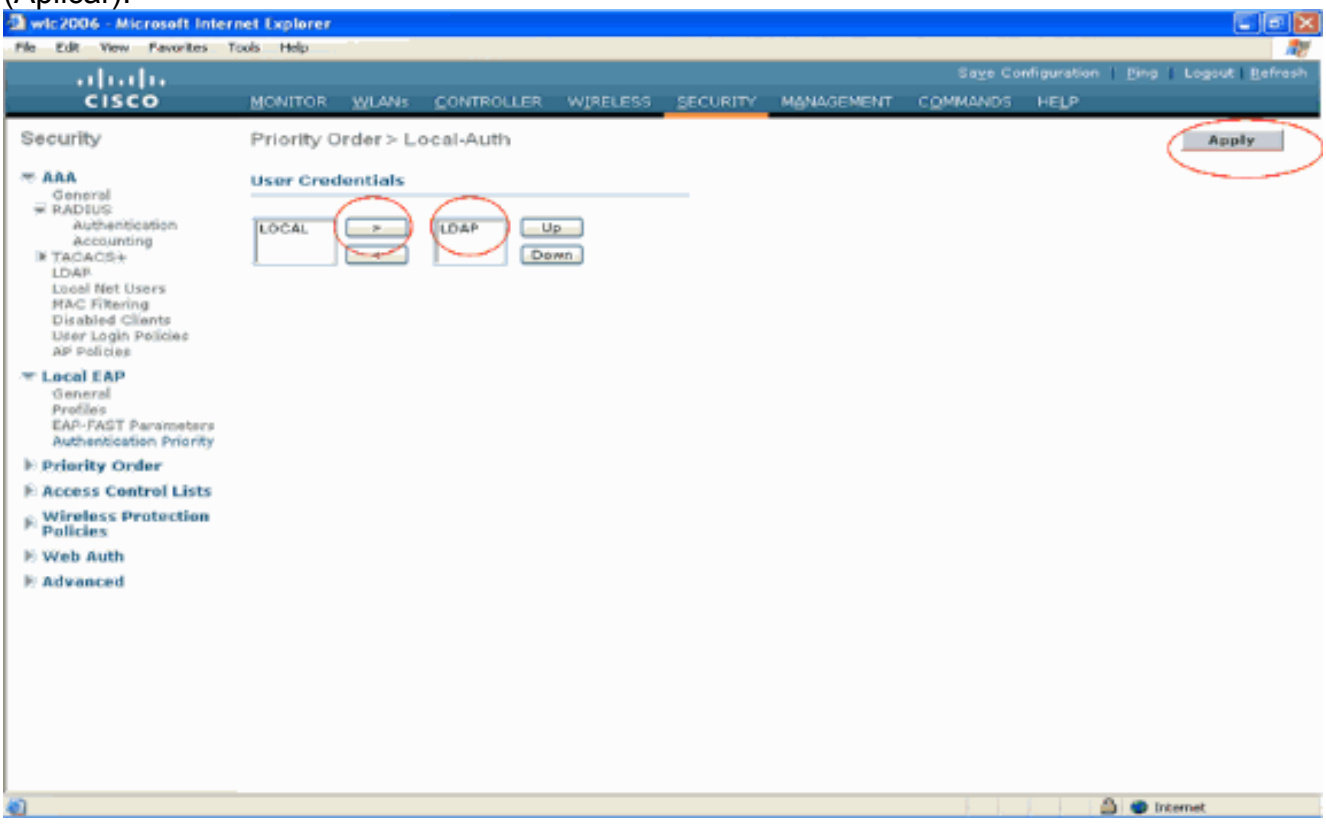
Complete estos pasos en el WLC para configurar LDAP como la base de datos backend de prioridad:

1. En la página Seguridad, haga clic en **EAP local > Prioridad de autenticación**. En la página Priority Order > Local-Auth , puede encontrar dos bases de datos (Local y LDAP) que pueden almacenar las credenciales del usuario.Para hacer que LDAP sea la base de datos

de prioridad, elija **LDAP** en el cuadro de credenciales de usuario del lado izquierdo y haga clic en el botón **>** para mover LDAP al cuadro de orden de prioridad del lado derecho.



2. Este ejemplo ilustra claramente que LDAP se elige en el cuadro del lado izquierdo y el botón **>** está seleccionado. Como resultado, LDAP se mueve al cuadro del lado derecho que decide la prioridad. La base de datos LDAP se elige como la base de datos de prioridad de autenticación.Haga clic en Apply (Aplicar).



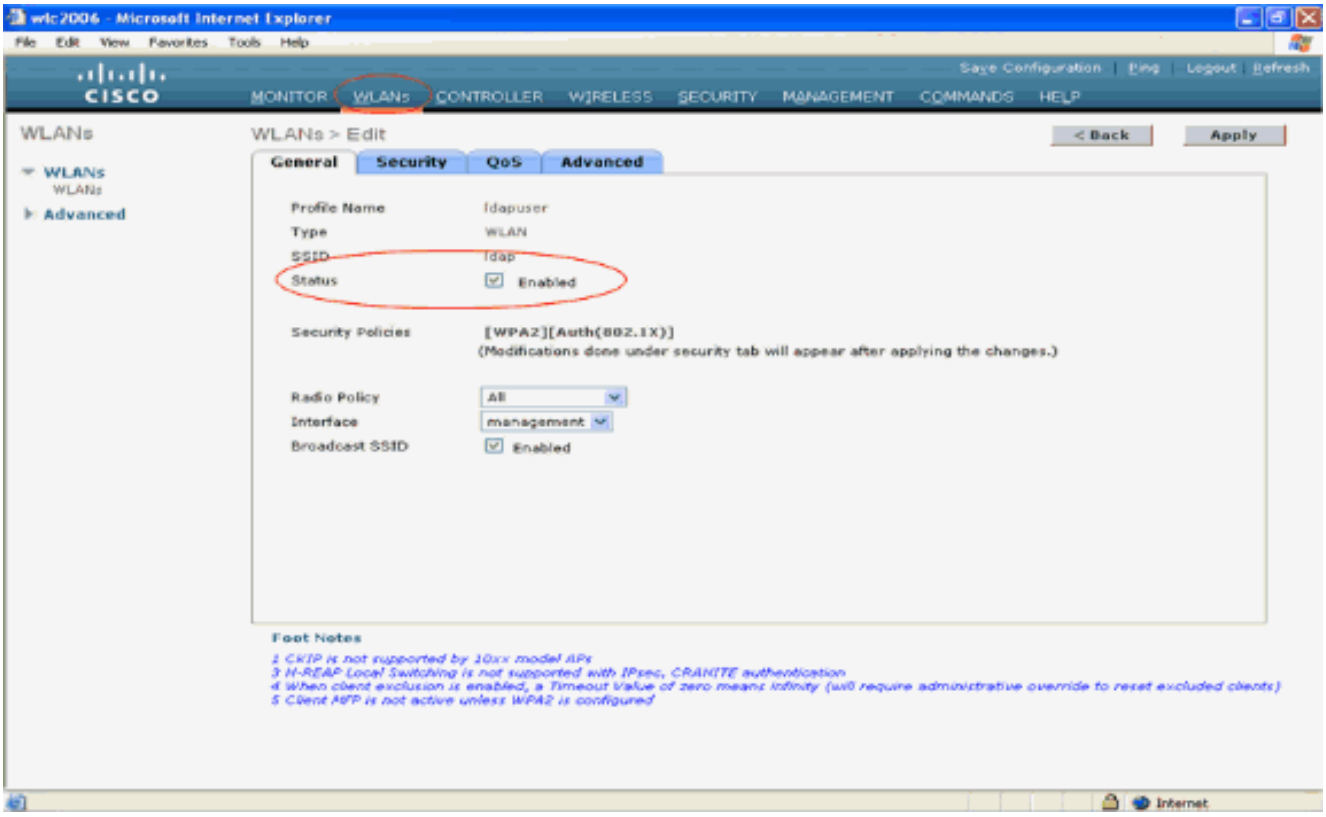
Nota: Si tanto LDAP como LOCAL aparecen en el cuadro Credenciales de usuario derecho

con LDAP en la parte superior y LOCAL en la inferior, EAP local intenta autenticar a los clientes utilizando la base de datos backend LDAP y conmuta por error a la base de datos de usuario local si no se puede acceder a los servidores LDAP. Si no se encuentra el usuario, se rechaza el intento de autenticación. Si LOCAL está en la parte superior, EAP local intenta autenticarse utilizando solamente la base de datos de usuarios local. No conmuta por error a la base de datos backend LDAP.

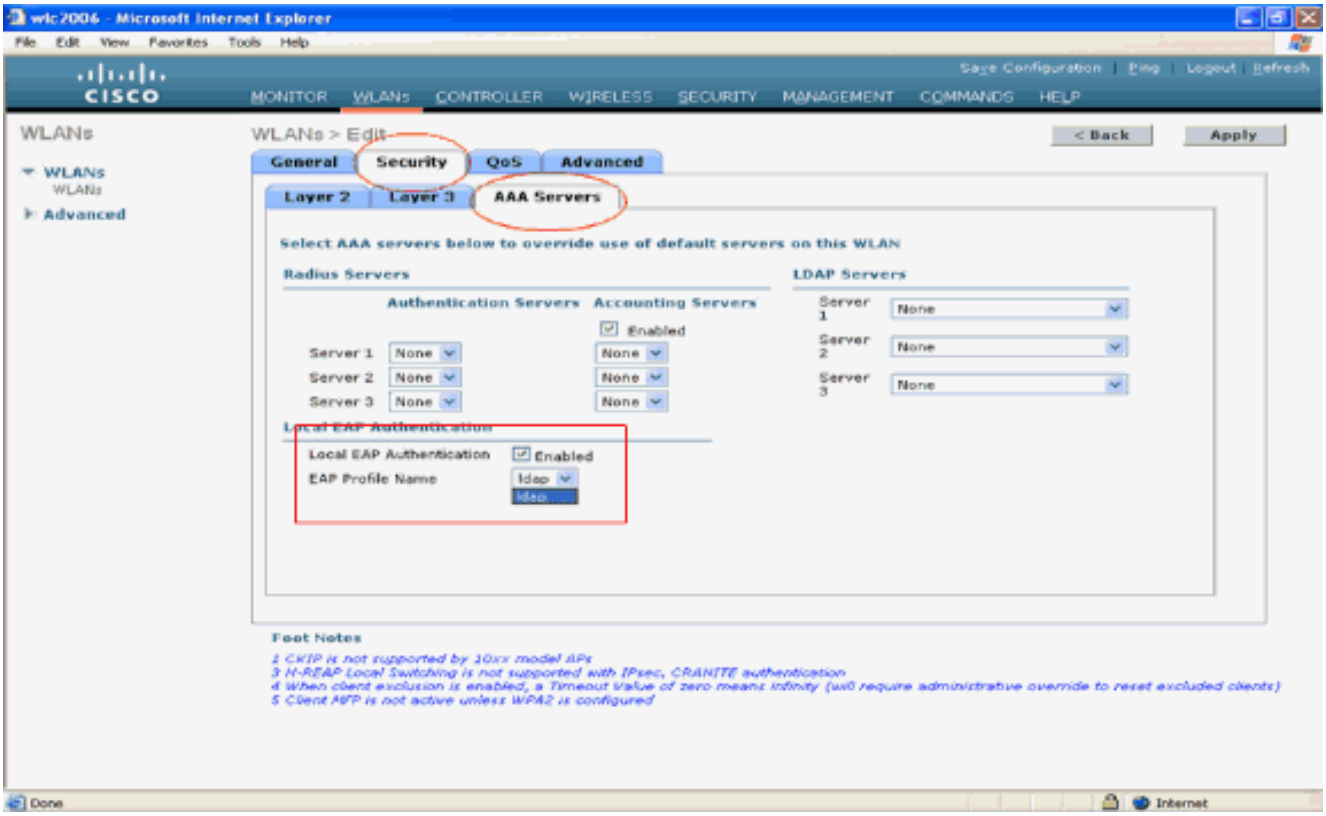
Configuración de WLAN en el WLC con autenticación EAP local

El último paso en el WLC es configurar un WLAN que utiliza el EAP local como su método de autenticación con el LDAP como su base de datos backend. Siga estos pasos:

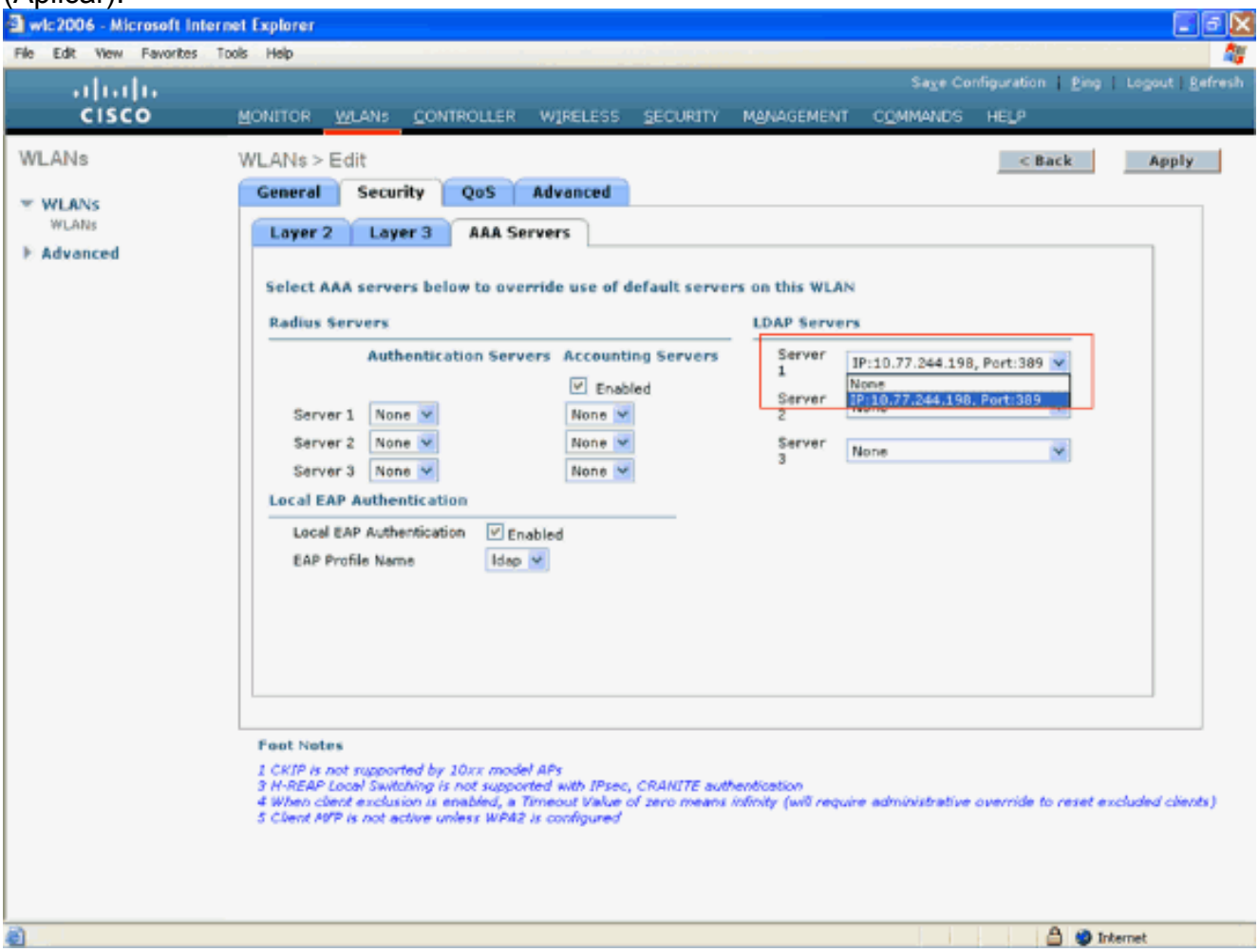
1. Desde el menú principal del controlador, haga clic en **WLANs** para moverse a la página de configuración de WLANs. En la página WLANs, haga clic en **New** para crear una nueva WLAN. Este ejemplo crea un nuevo **ldap** WLAN.Haga clic en **Apply** El siguiente paso es configurar los parámetros WLAN en la página WLANs > Edit .
2. En la página de edición de WLAN, habilite el estado de esta WLAN. Configure todos los demás parámetros
necesarios.



3. Haga clic en **Seguridad** para configurar los parámetros relacionados con la seguridad para esta WLAN. En este ejemplo se utiliza la seguridad de capa 2 como 802.1x con WEP dinámica de 104 bits.**Nota:** Este documento utiliza 802.1x con WEP dinámico como ejemplo. Se recomienda utilizar métodos de autenticación más seguros, como WPA/ WPA2.
4. En la página de configuración de Seguridad WLAN, haga clic en **la** ficha **Servidores AAA**. En la página de servidores AAA, habilite el método de autenticación EAP local y elija **ldap** en el cuadro desplegable que corresponde al parámetro EAP Profile Name. Este es el perfil EAP local creado en este
ejemplo.

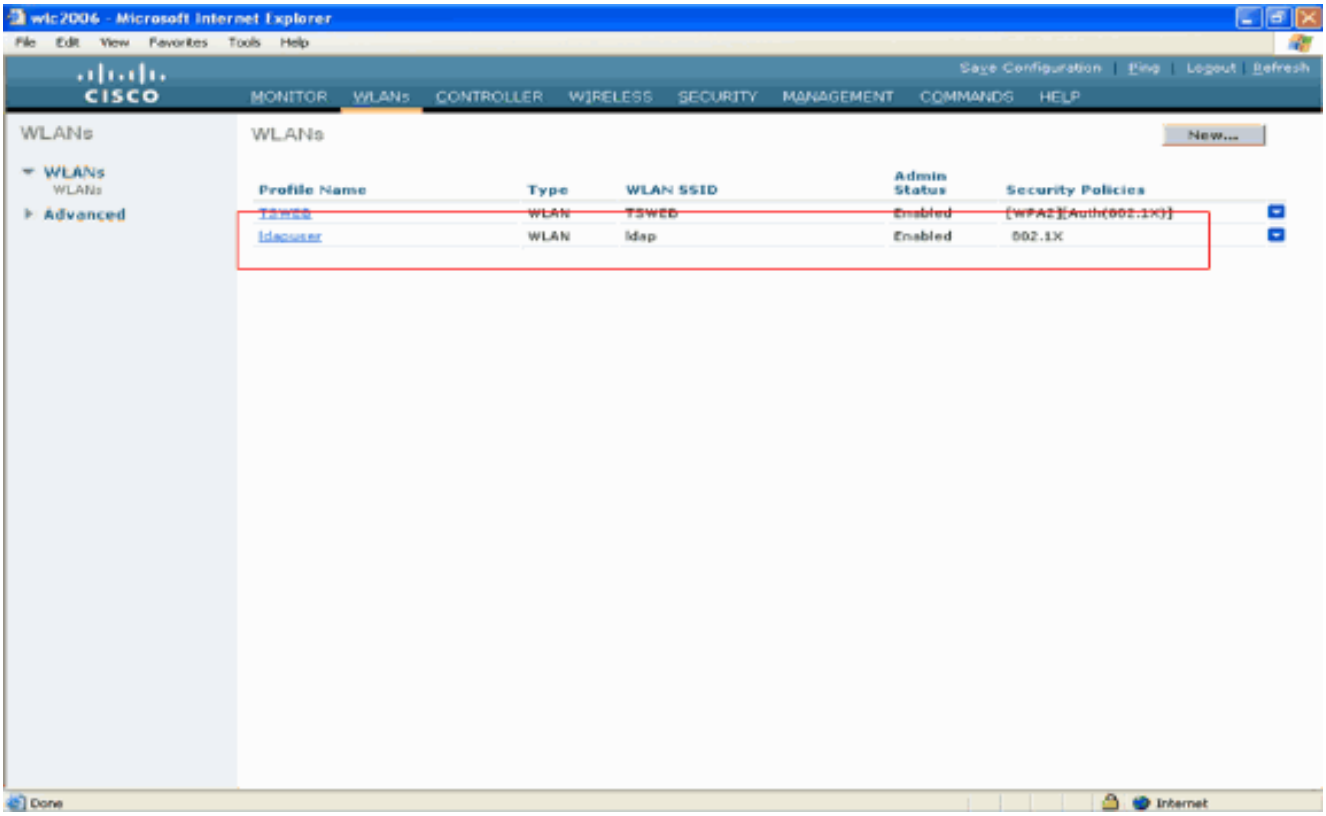


5. Elija el servidor LDAP (que fue configurado previamente en el WLC) del cuadro desplegable . Asegúrese de que el servidor LDAP es accesible desde el WLC.Haga clic en Apply (Aplicar).



6. El nuevo WLAN ldap se ha configurado en el WLC. Esta WLAN autentica a los clientes con autenticación EAP local (EAP-FAST en este caso) y consulta una base de datos backend

LDAP para la validación de credenciales de cliente.



Configurar servidor LDAP

Ahora que el EAP local está configurado en el WLC, el siguiente paso es configurar el servidor LDAP que sirve como una base de datos backend para autenticar los clientes inalámbricos después de la validación exitosa del certificado.

El primer paso en la configuración del servidor LDAP es crear una base de datos de usuario en el servidor LDAP para que el WLC pueda consultar esta base de datos para autenticar al usuario.

Creación de usuarios en el controlador de dominio

En este ejemplo, se crea un nuevo OU **ldapuser** y se crea el usuario **user2** en esta OU. Configurando este usuario para el acceso LDAP, el WLC puede consultar esta base de datos LDAP para la autenticación del usuario.

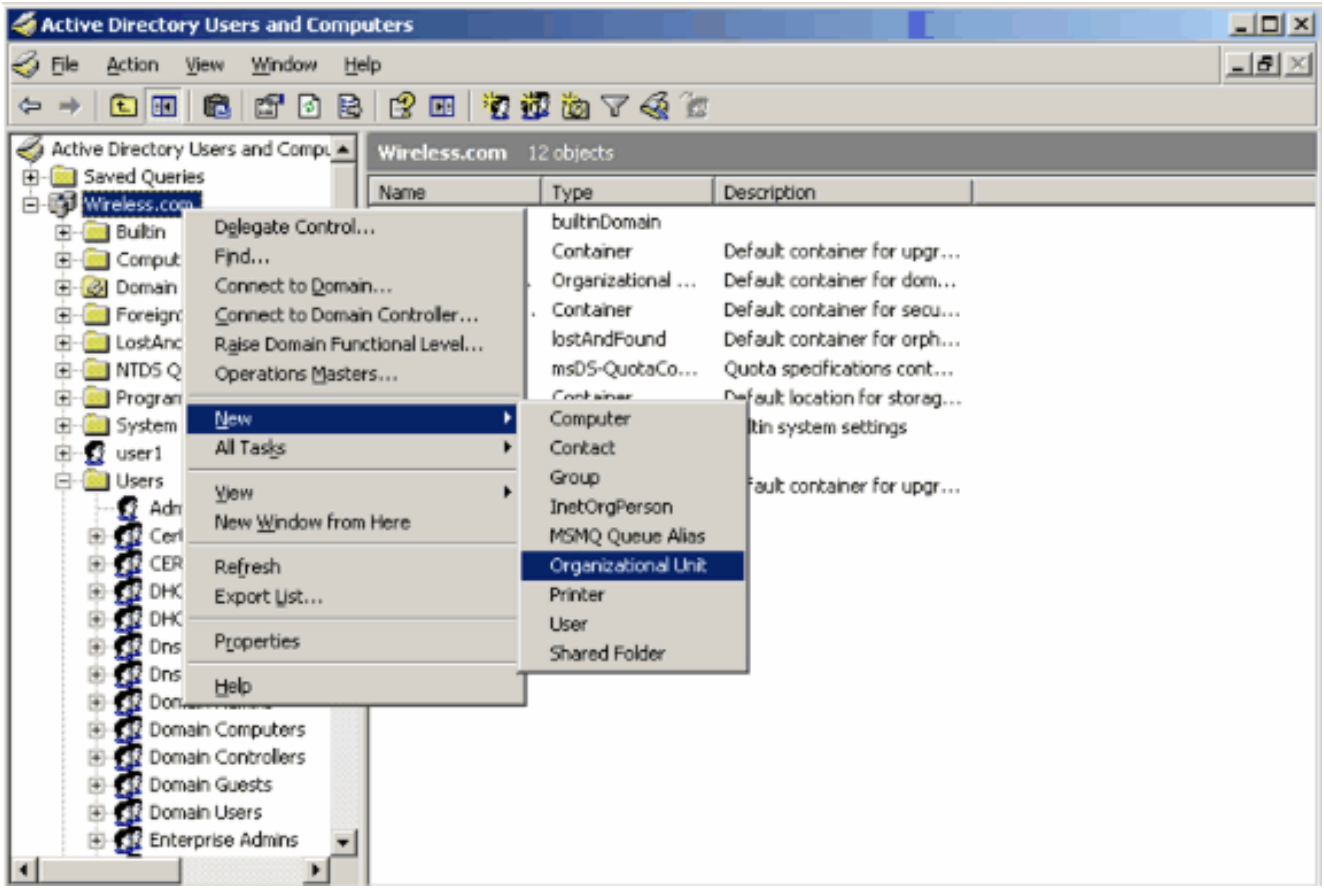
El dominio utilizado en este ejemplo es **wireless.com**.

Crear una base de datos de usuarios en una unidad organizativa

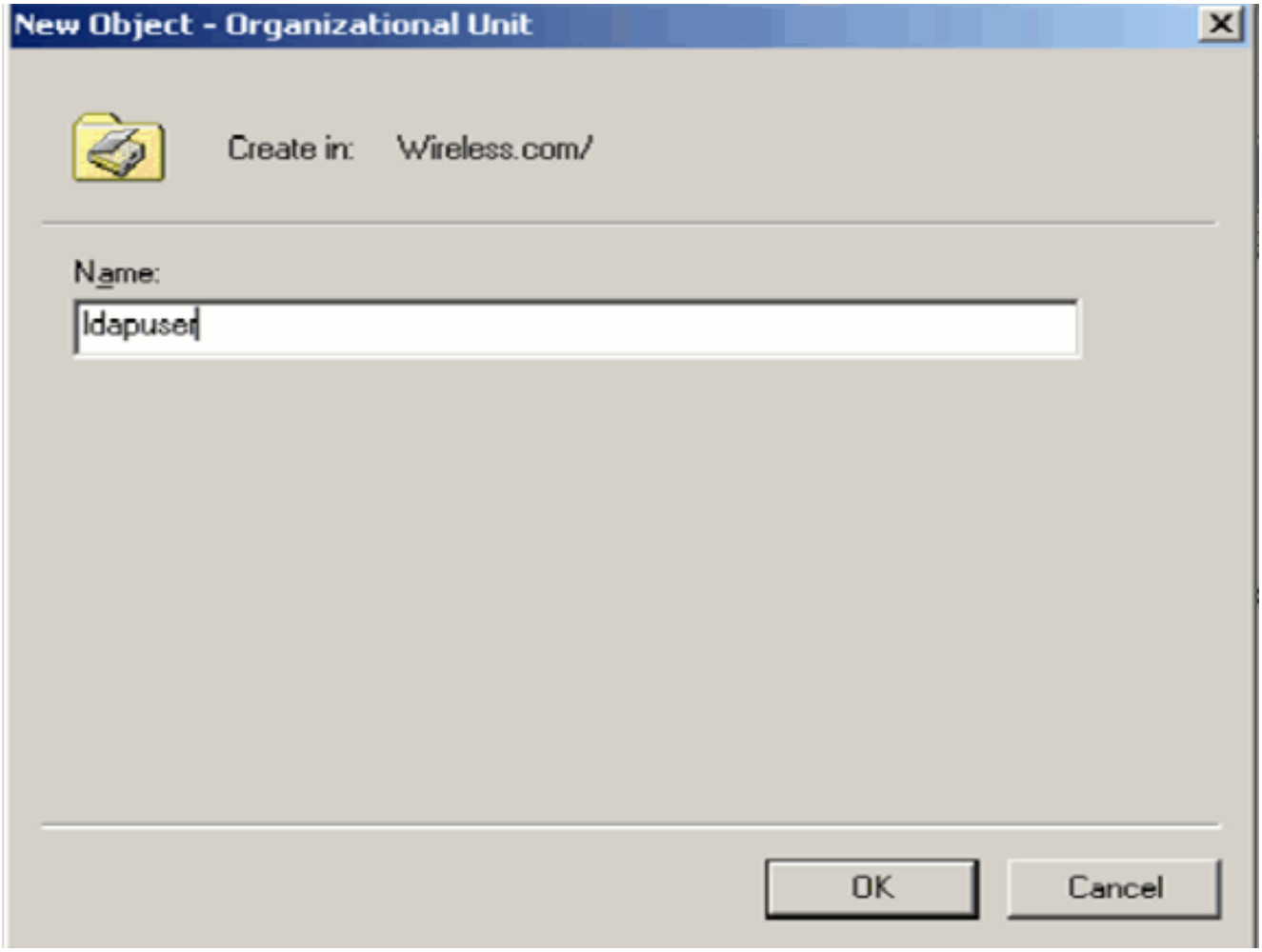
Esta sección explica cómo crear una nueva OU en su dominio y crear un nuevo usuario en esta OU.

1. En el controlador de dominio, haga clic en **Inicio > Programas > Herramientas administrativas > Usuarios y equipos de Active Directory** para iniciar la consola de administración de **Usuarios y equipos de Active Directory**.
2. Haga clic con el botón derecho en su nombre de dominio (wireless.com, en este ejemplo),

luego seleccione **Nuevo > Unidad organizacional** del menú contextual para crear una nueva OU.

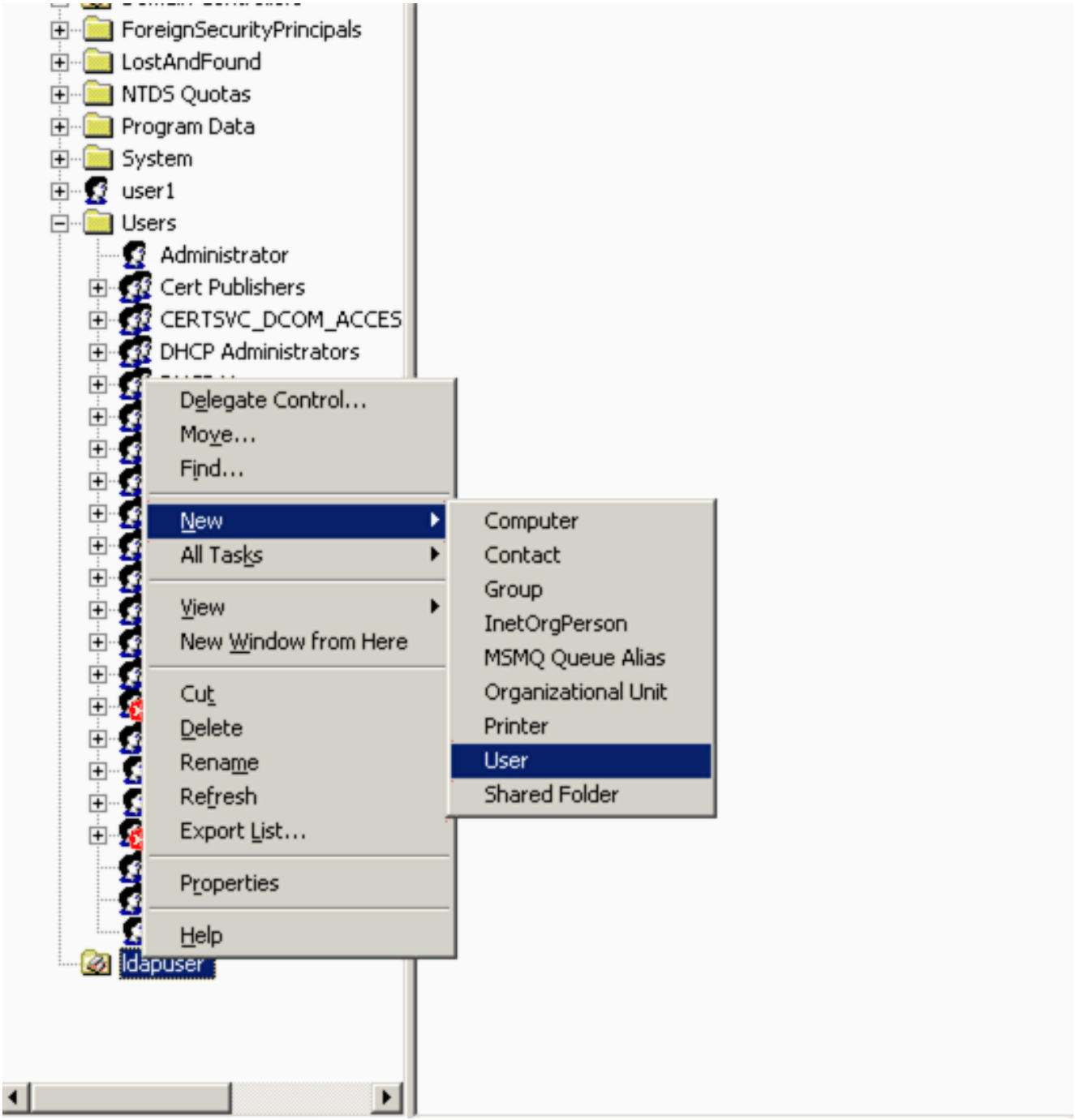


3. Asigne un nombre a esta unidad organizativa y haga clic en **Aceptar**.

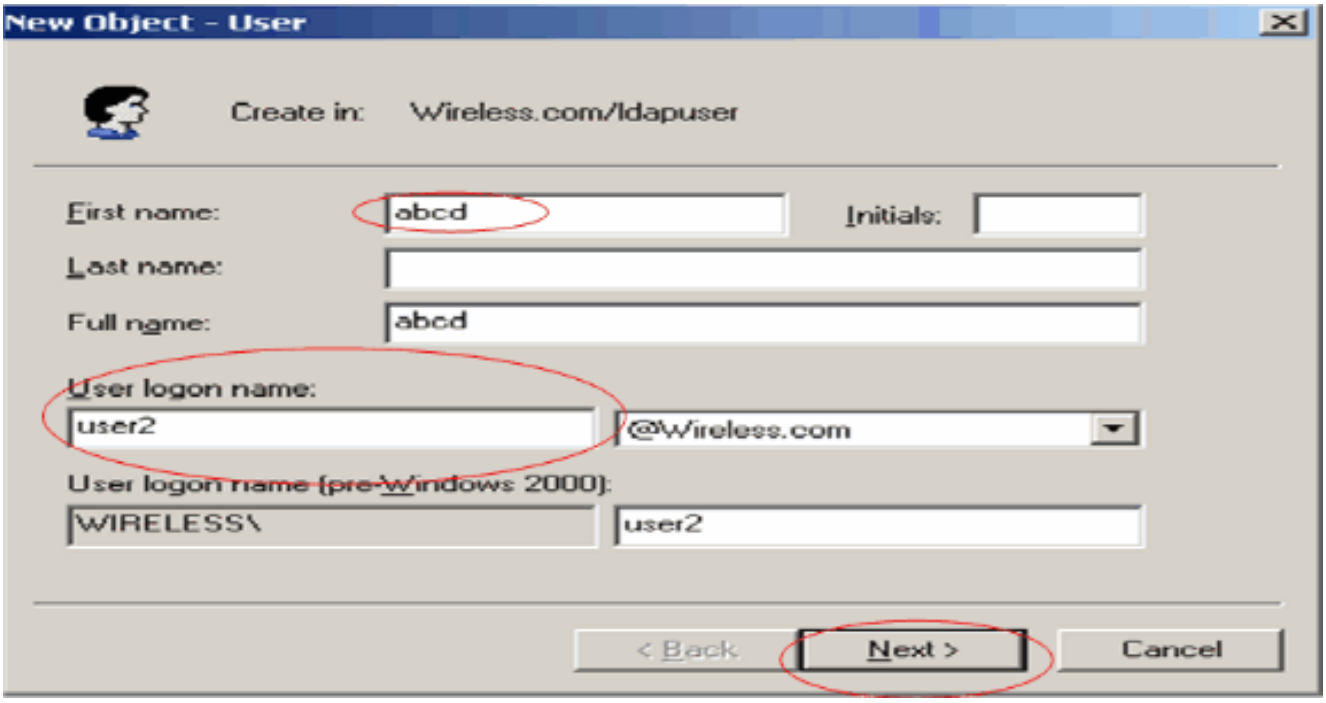


Ahora que el nuevo OU **ldapuser** se crea en el servidor LDAP, el siguiente paso es crear el usuario **user2** en esta OU. Para lograr esto, complete estos pasos:

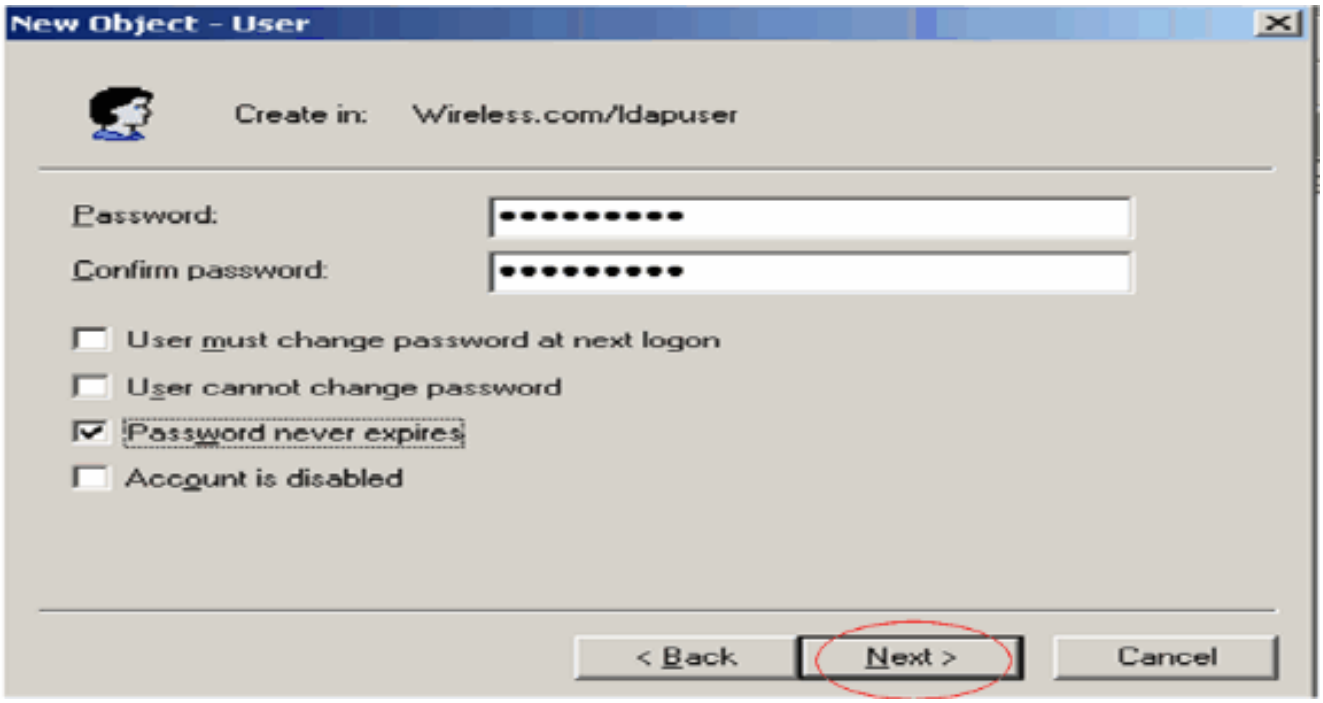
1. Haga clic con el botón derecho del ratón en la nueva unidad organizativa creada. Seleccione **New > User** en los menús contextuales resultantes para crear un nuevo usuario.



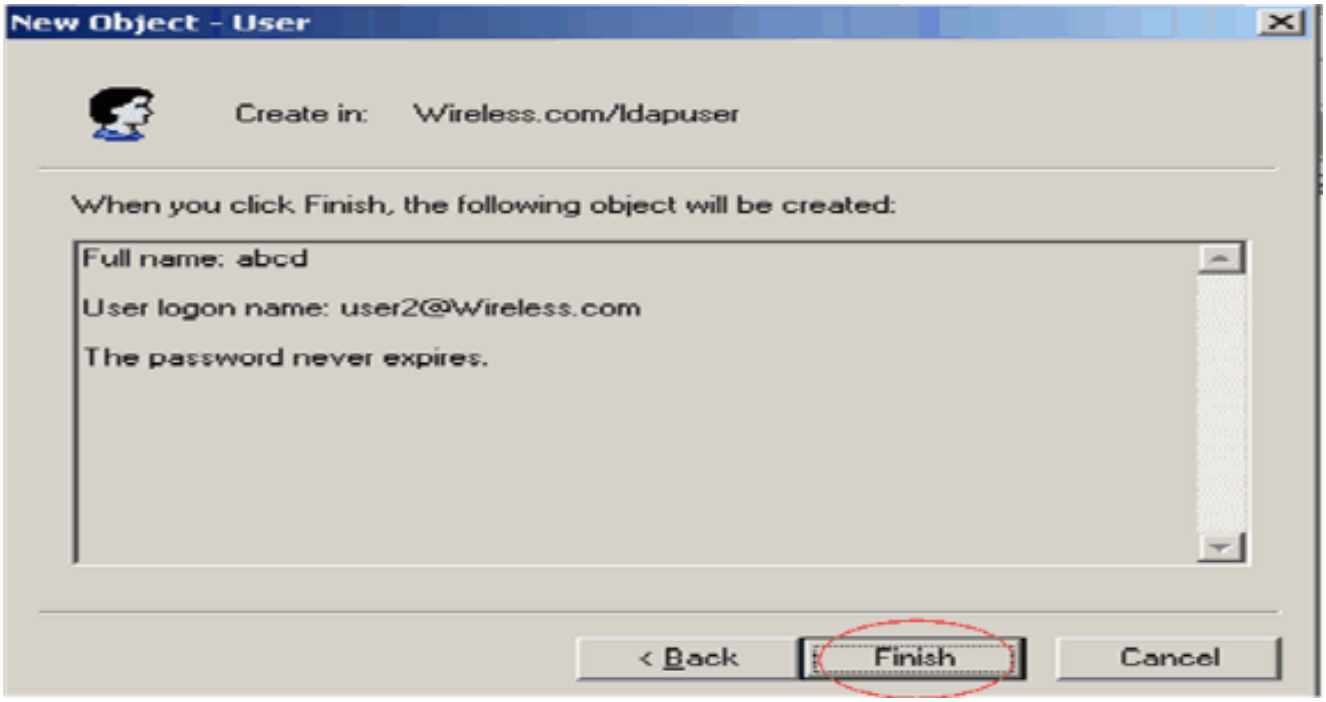
2. En la página Configuración de usuario, rellene los campos obligatorios como se muestra en este ejemplo. Este ejemplo tiene **user2** como nombre de inicio de sesión de usuario.Este es el nombre de usuario que será verificado en la base de datos LDAP para autenticar al cliente. Este ejemplo utiliza **abcd** como nombre y apellido. Haga clic en Next (Siguiente).



3. Introduzca una contraseña y confírmela. Elija la opción **Password never expires** y haga clic en
Next.



4. Haga clic en Finish (Finalizar).Se crea un nuevo usuario **user2** en OU **ldapuser**. Las credenciales de usuario son:nombre de usuario: **user2**contraseña: **Laptop123**



Ahora que se crea el usuario bajo una OU, el siguiente paso es configurar este usuario para el acceso LDAP.

Configuración del usuario para el acceso LDAP

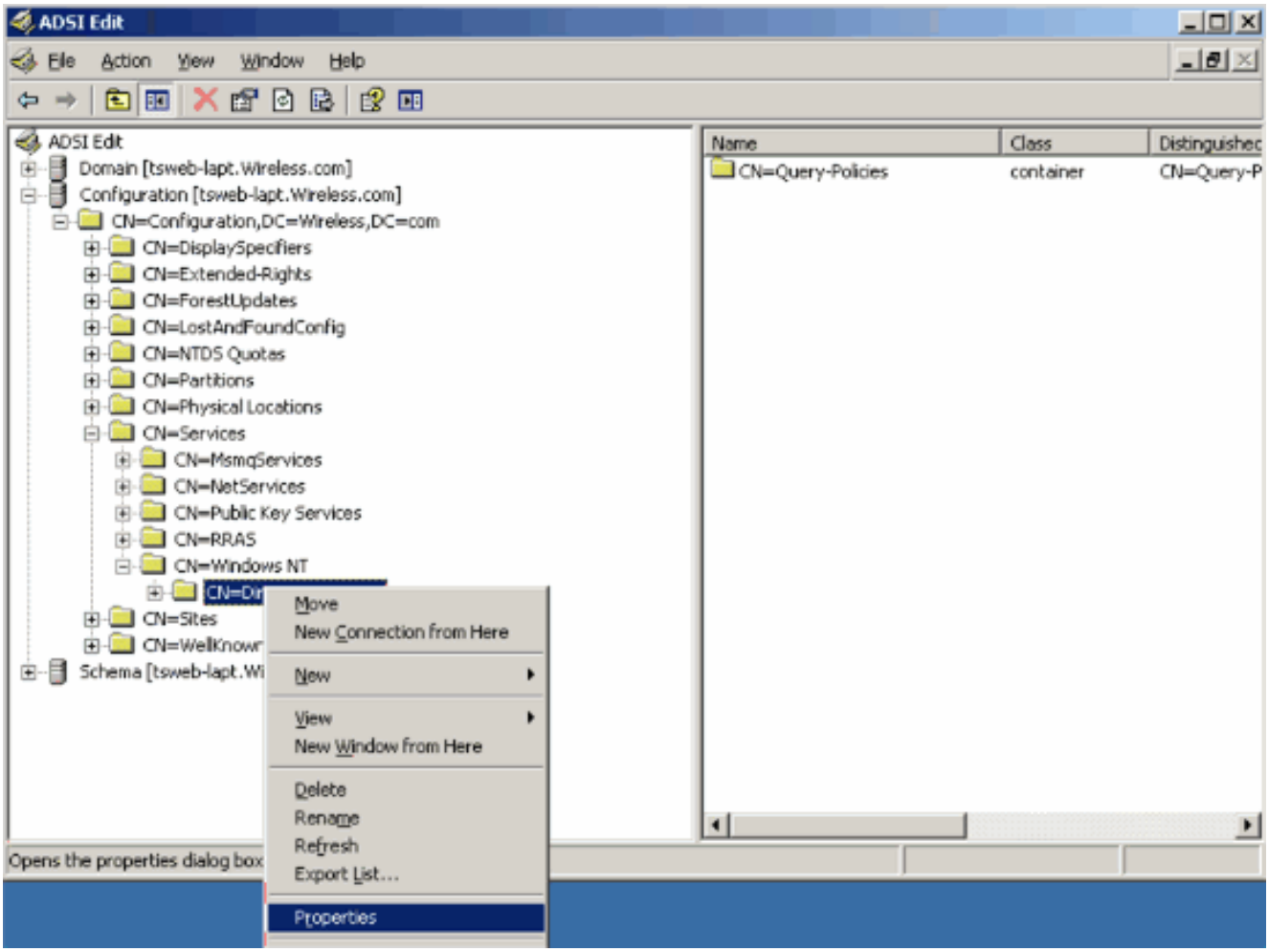
Realice los pasos de esta sección para configurar un usuario para el acceso LDAP.

Habilitar la característica de enlace anónimo en Windows 2003 Server

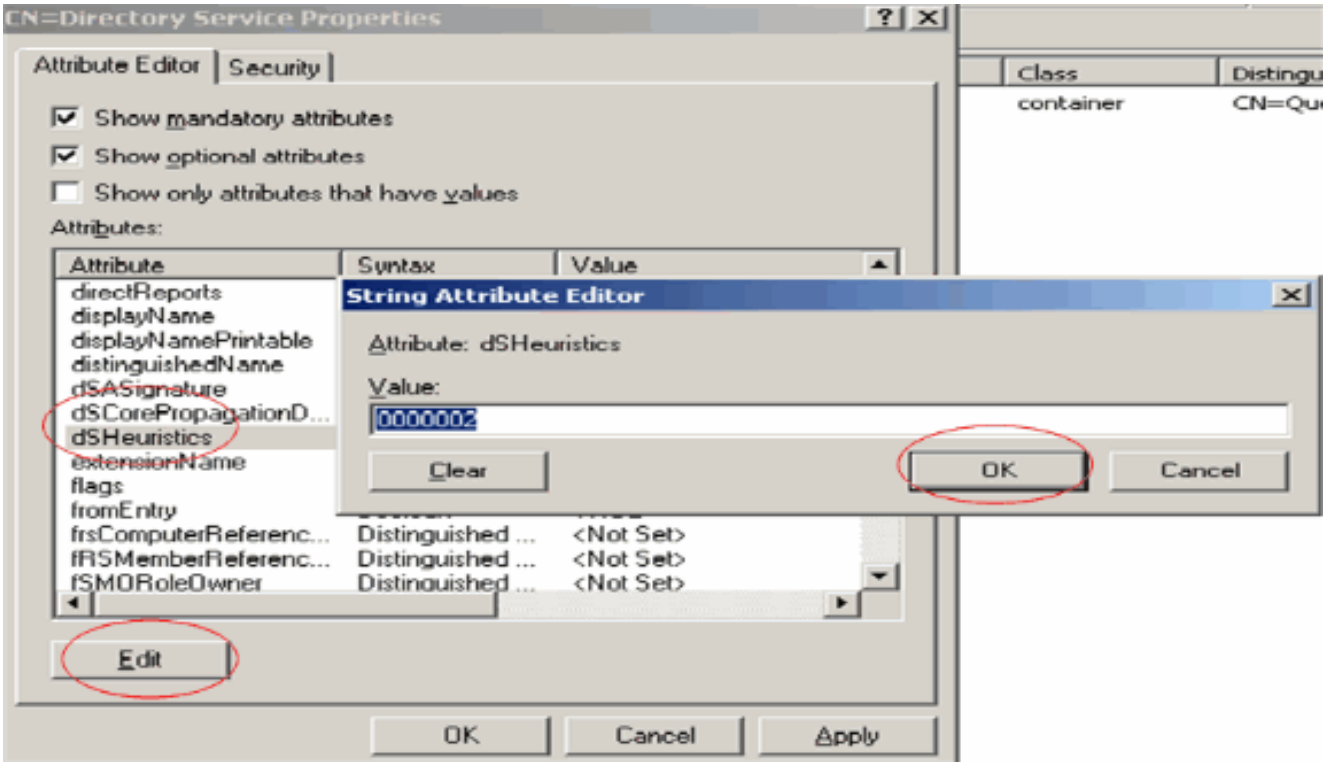
Para que las aplicaciones de terceros accedan a Windows 2003 AD en LDAP, la función de enlace anónimo debe estar habilitada en Windows 2003. De forma predeterminada, no se permiten operaciones LDAP anónimas en controladores de dominio de Windows 2003.

Realice estos pasos para habilitar la función Anonymous Bind:

1. Inicie la herramienta **ADSI Edit** desde la ubicación Start > Run > Type: **ADSI Edit.msc**. Esta herramienta forma parte de las herramientas de soporte técnico de Windows 2003.
2. En la ventana Editar ADSI, expanda el dominio raíz (Configuración [tsweb-lapt.Wireless.com]).Expanda **CN=Services > CN=Windows NT > CN=Directory Service**. Haga clic con el botón derecho del ratón en el contenedor **CN=Directory Service** y seleccione **propiedades** en el menú contextual.



3. En la ventana **CN=Directory Service Properties**, haga clic en el atributo **dsHeuristics** en el campo Attribute y elija **Edit**. En la ventana **String Attribute Editor** de este atributo, ingrese el valor **0000002** y haga clic en **Apply** y **OK**. La característica Enlace anónimo está habilitada en Windows 2003 Server.**Nota:** El último (séptimo) carácter es el que controla la forma en que se puede enlazar con el servicio LDAP. "0" o ningún séptimo carácter significa que las operaciones LDAP anónimas están inhabilitadas. **Si establece el séptimo carácter en "2", se habilita la función de enlace anónimo.**

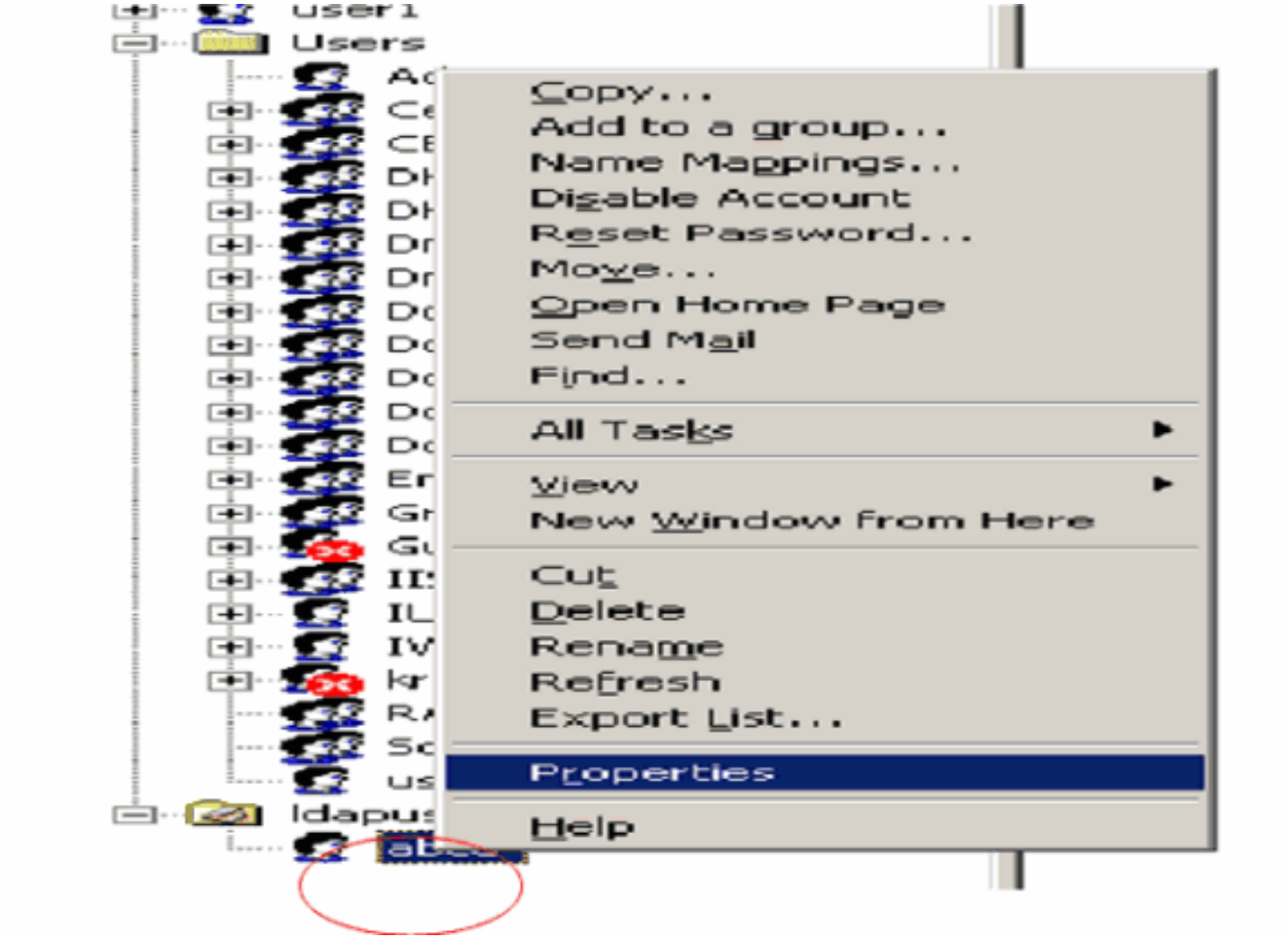


Nota: Si este atributo ya contiene un valor, asegúrese de que está cambiando sólo el séptimo carácter de la izquierda. Éste es el único carácter que debe cambiarse para habilitar los enlaces anónimos. Por ejemplo, si el valor actual es "0010000", tendrá que cambiarlo a "0010002". Si el valor actual es inferior a siete caracteres, tendrá que poner ceros en los lugares no utilizados: "001" se convertirá en "0010002".

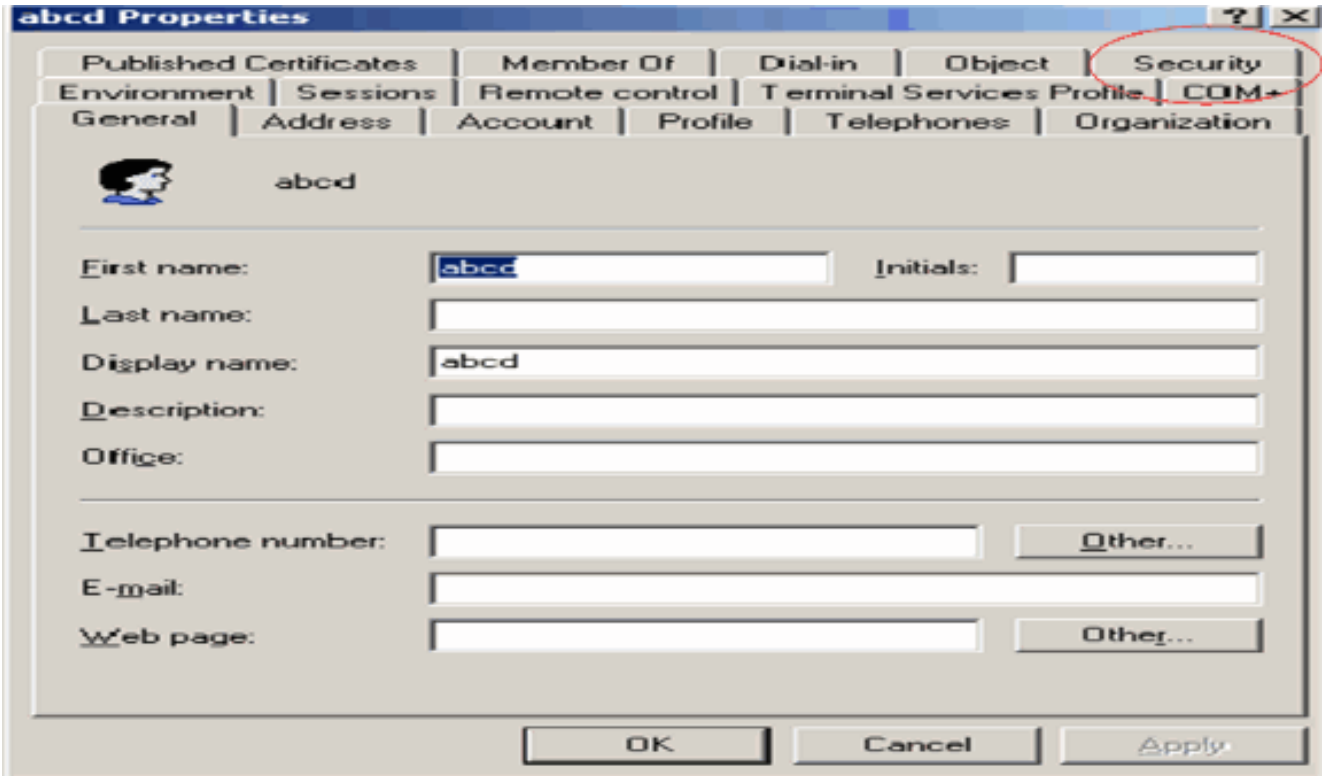
Concesión de acceso de INICIO DE SESIÓN ANÓNIMO al usuario "user2"

El siguiente paso es otorgar el acceso **ANONYMOUS LOGON** al usuario **user2**. Complete estos pasos para lograr esto:

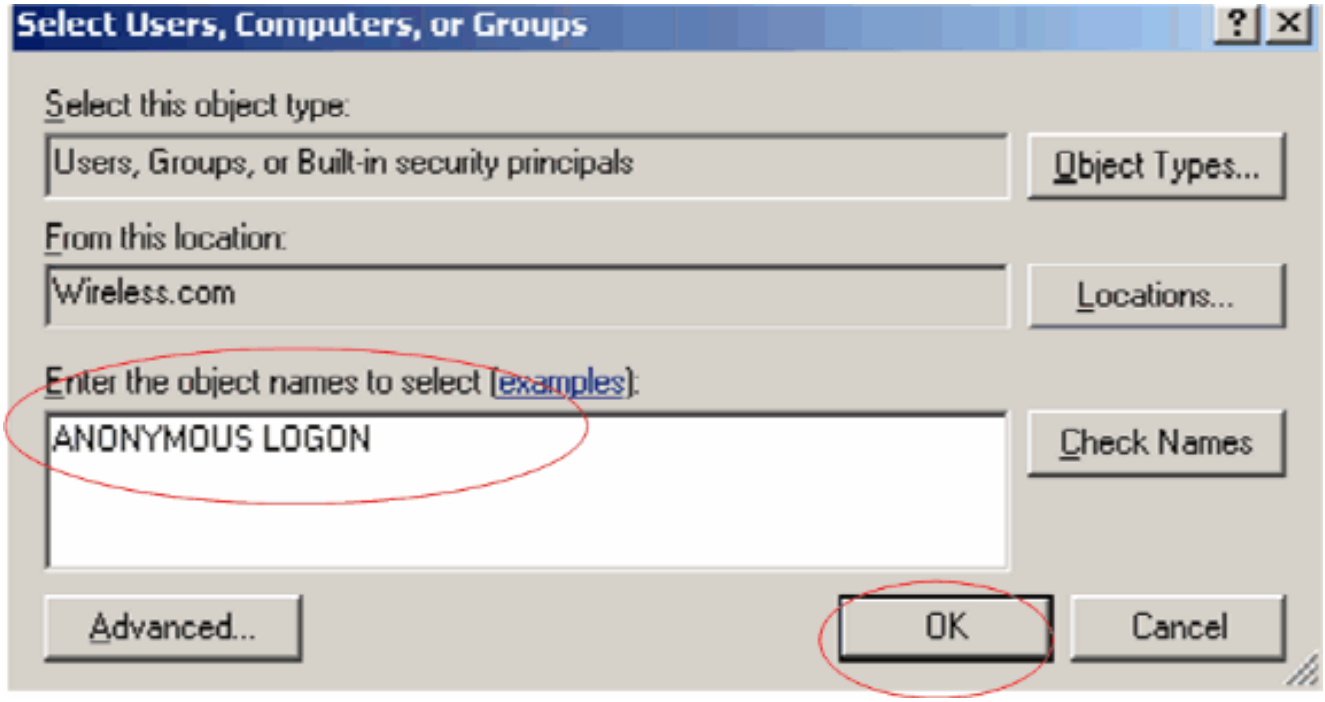
1. Abra **Usuarios** y **equipos de Active Directory**.
2. Asegúrese de que la opción **Ver funciones avanzadas** esté marcada.
3. Navegue hasta el usuario **user2** y haga clic con el botón derecho en él. Seleccione **Properties** en el menú contextual. Este usuario se identifica con el nombre "abcd".



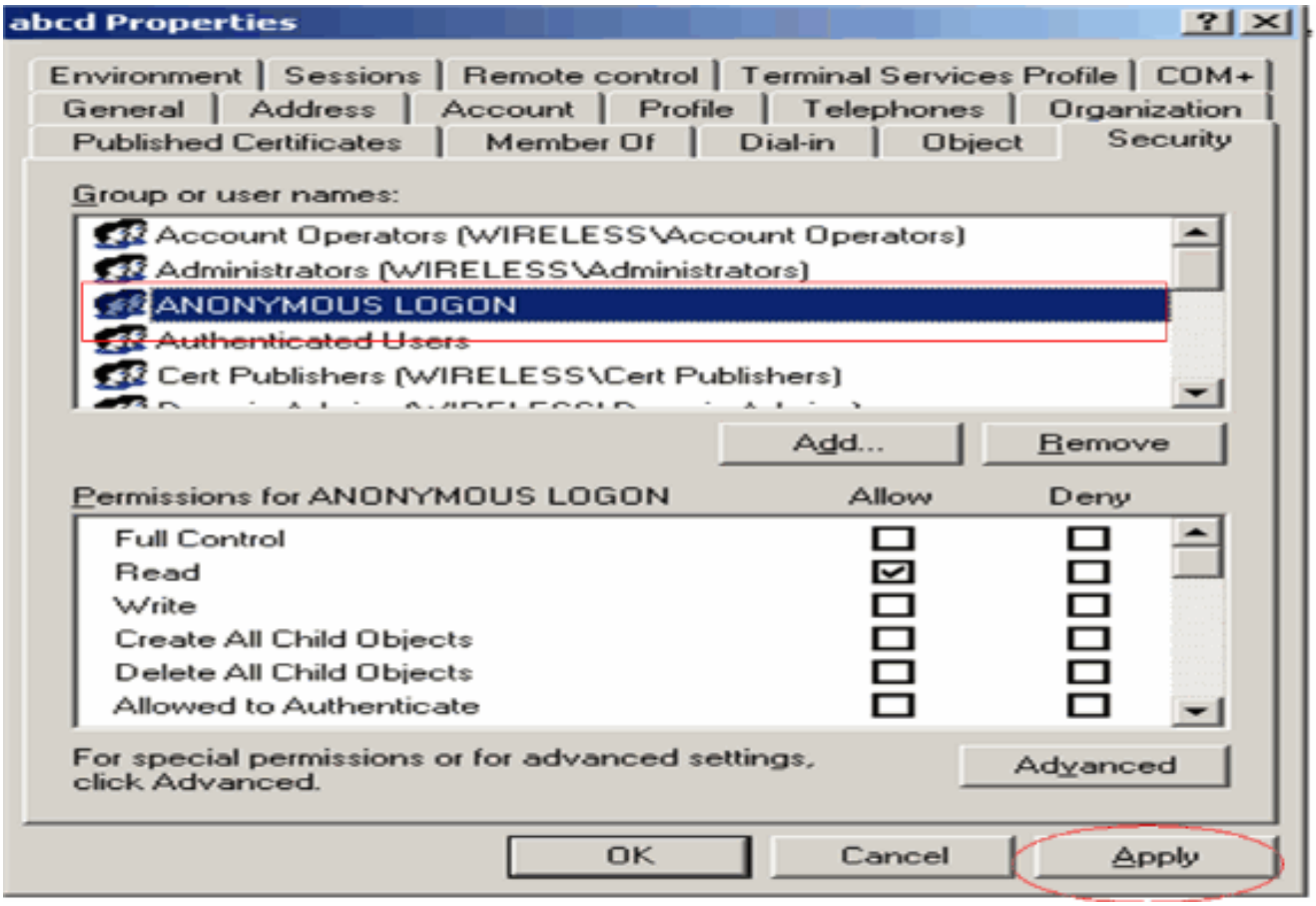
4. Vaya a **Seguridad** en la ventana Propiedades de abcd.



5. Haga clic en **Agregar** en la ventana resultante.
6. Ingrese **ANONYMOUS LOGON** en el cuadro **Ingrese los nombres de objeto a seleccionar** y confirme el diálogo.



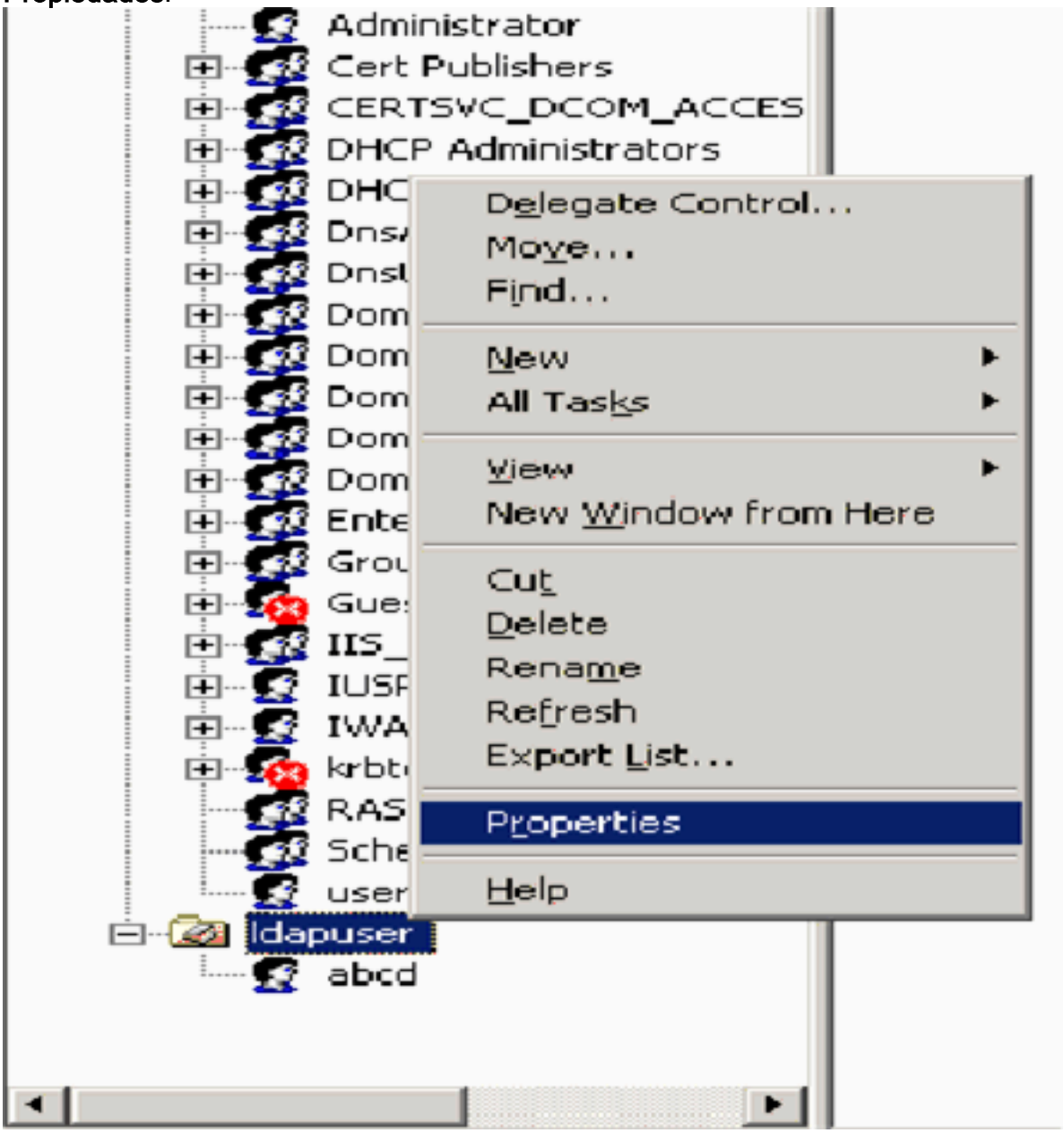
7. En la ACL, observará que **ANONYMOUS LOGON** tiene acceso a algunos conjuntos de propiedades del usuario. Click OK. El acceso de INICIO DE SESIÓN ANÓNIMO se concede a este
usuario.



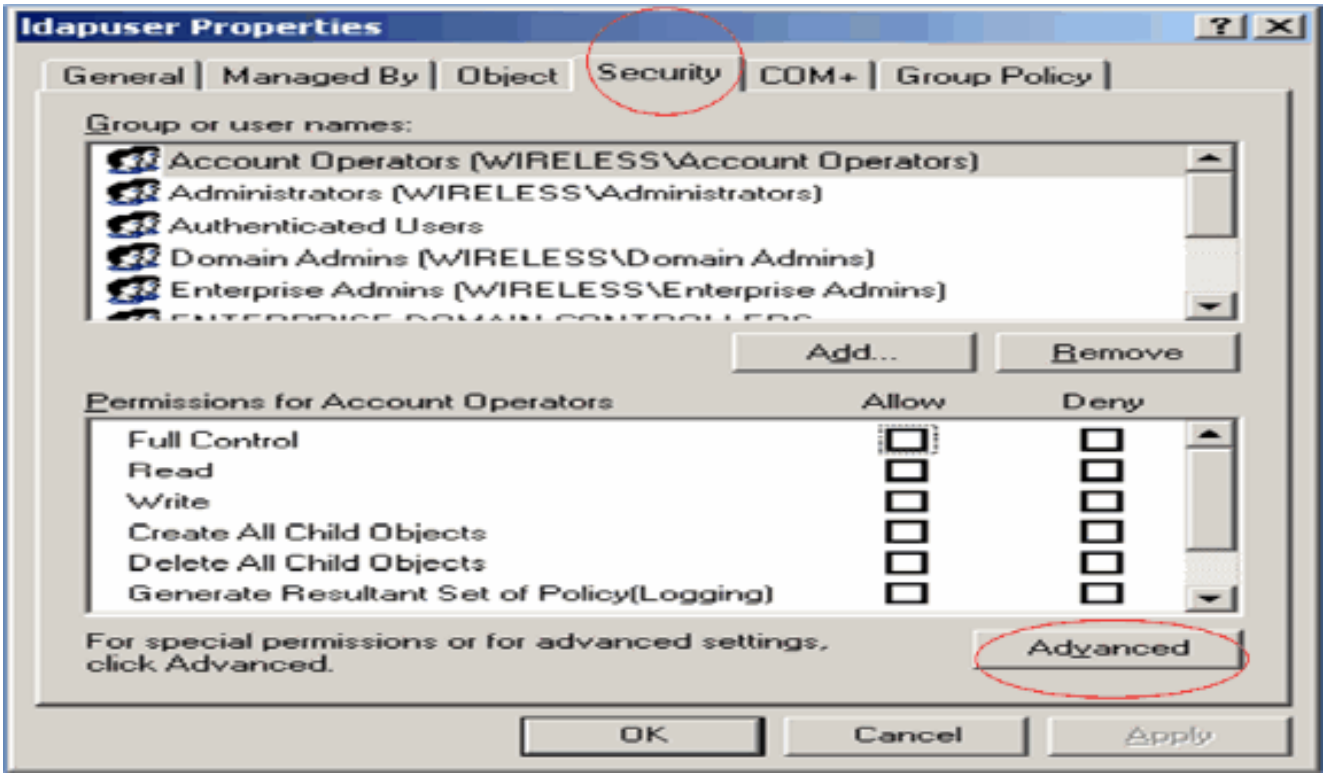
Concesión de permisos de contenido de lista en la unidad organizativa

El siguiente paso es otorgar al menos el permiso **List Contents** al **LOGON ANÓNIMO** en la OU en la que se encuentra el usuario. En este ejemplo, "user2" se encuentra en la unidad organizativa "ldapuser". Complete estos pasos para lograr esto:

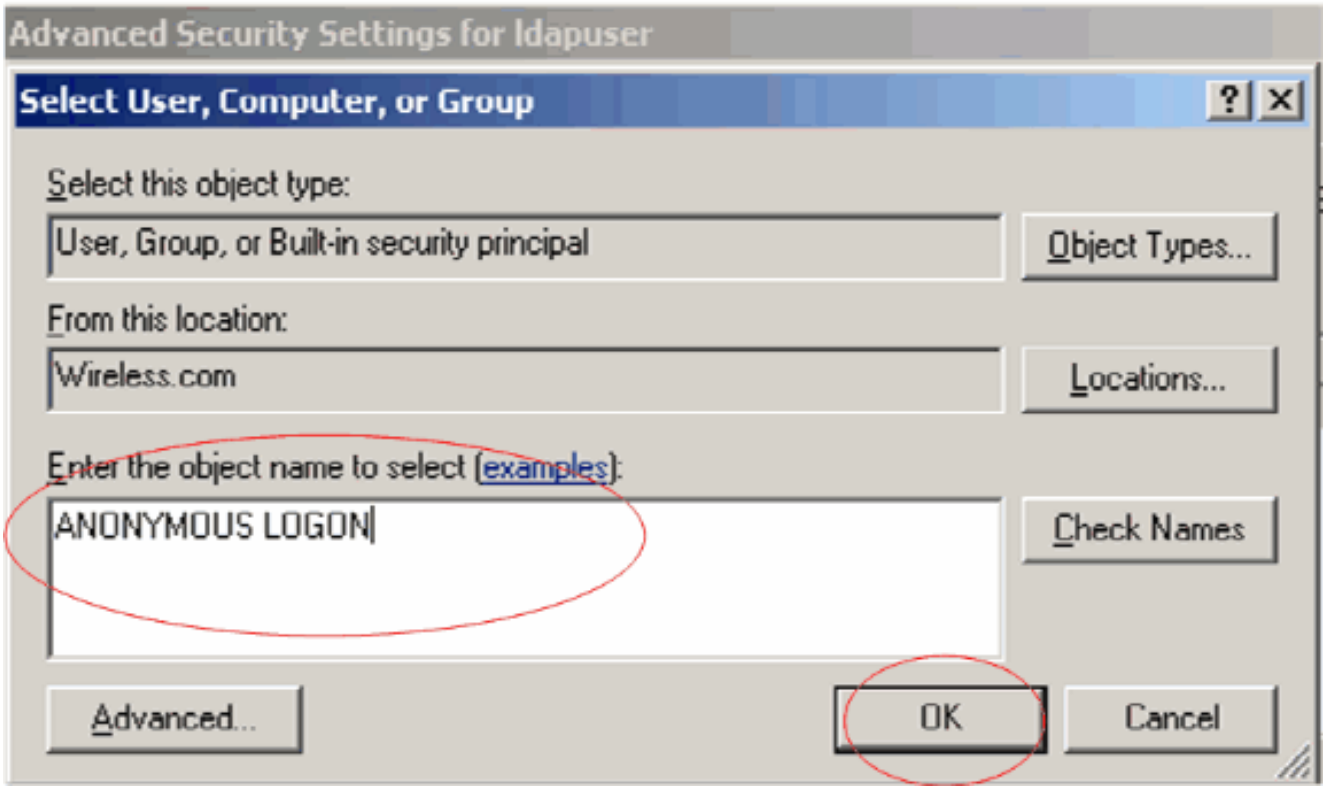
1. En Usuarios y equipos de Active Directory, haga clic con el botón secundario en OU **ldapuser** y elija **Propiedades**.



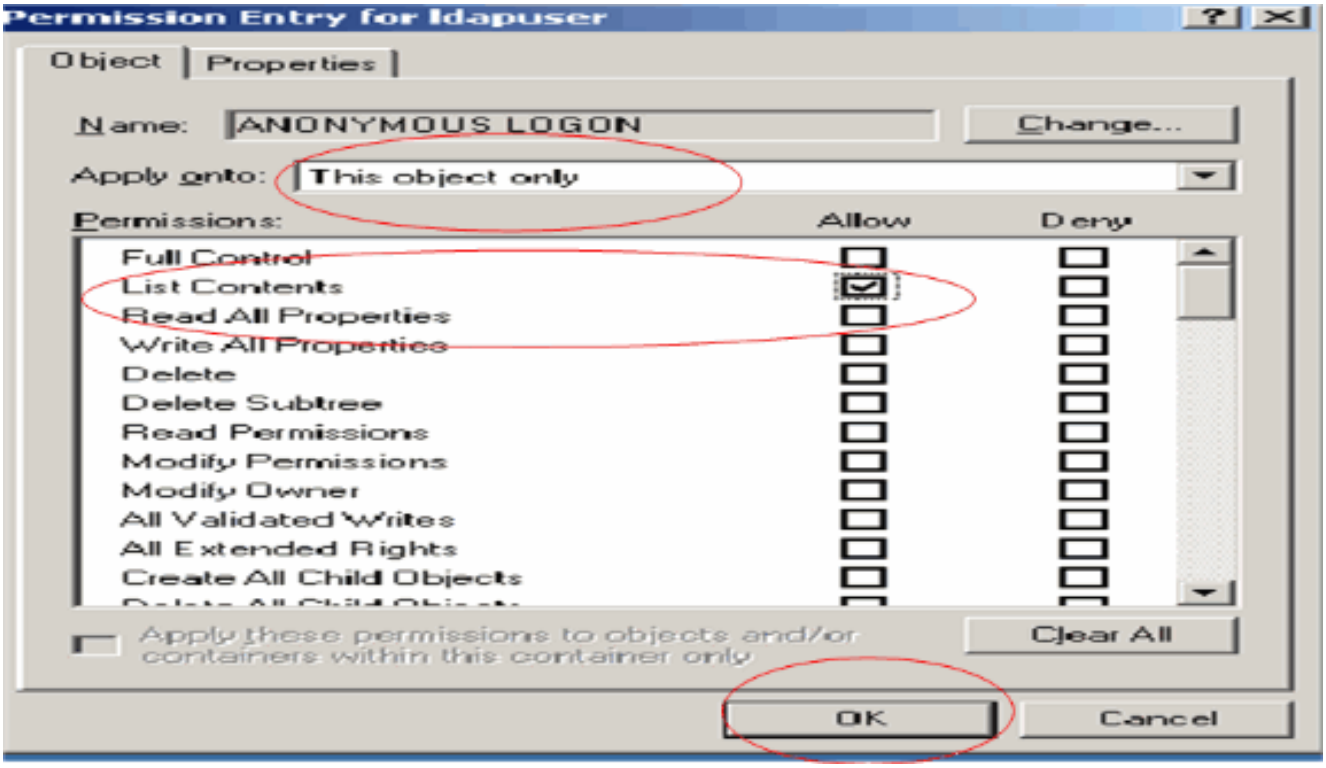
2. Haga clic en **Seguridad** y luego en **Avanzada**.



3. Haga clic en Add (Agregar). En el cuadro de diálogo que se abre, introduzca **ANONYMOUS LOGON**.



4. Reconozca el diálogo. Se abrirá una nueva ventana de diálogo.
5. En el cuadro desplegable **Aplicar en**, elija **Sólo este objeto** y active la casilla de verificación **Permitir contenido de lista**.

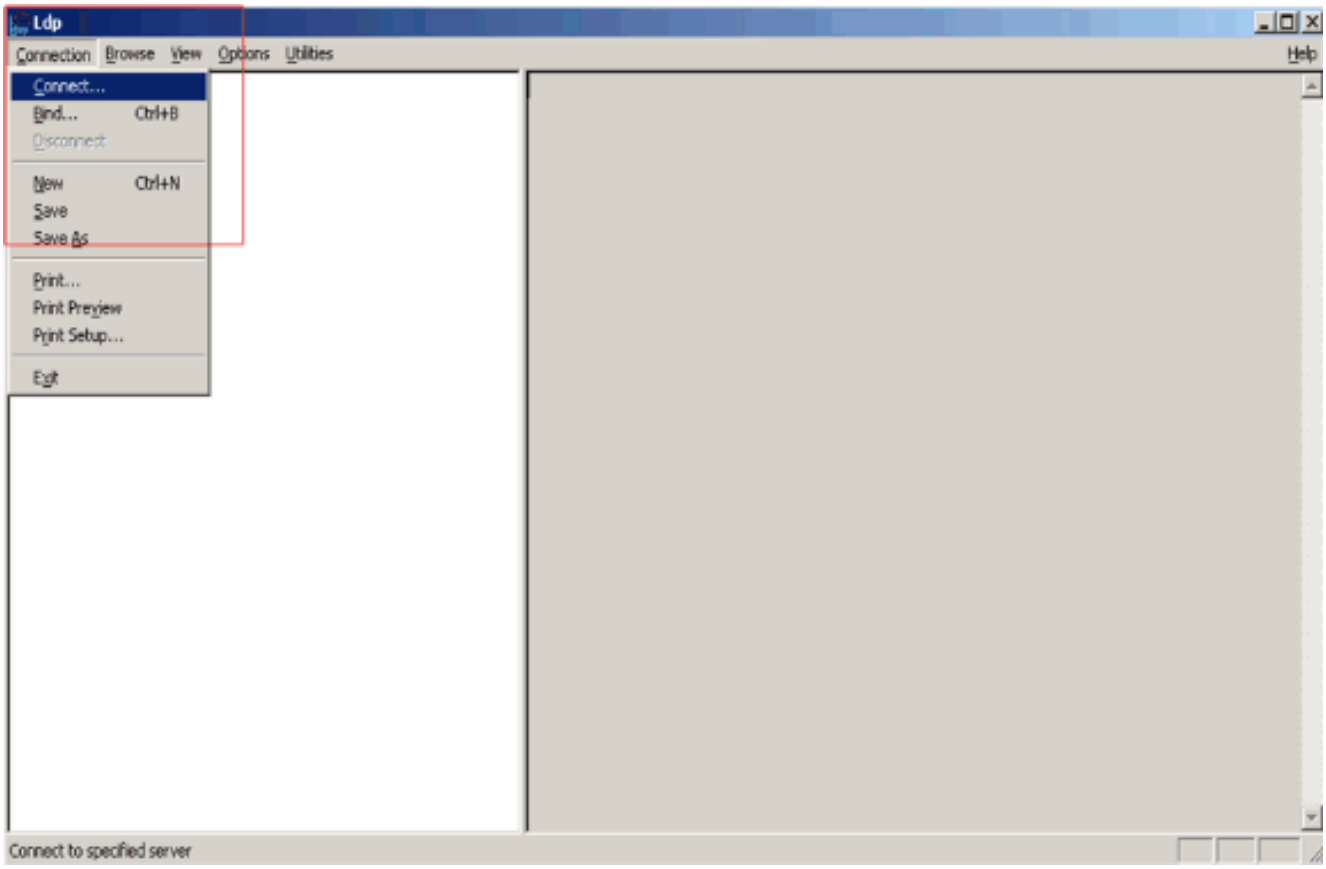


Uso de LDP para Identificar los Atributos de Usuario

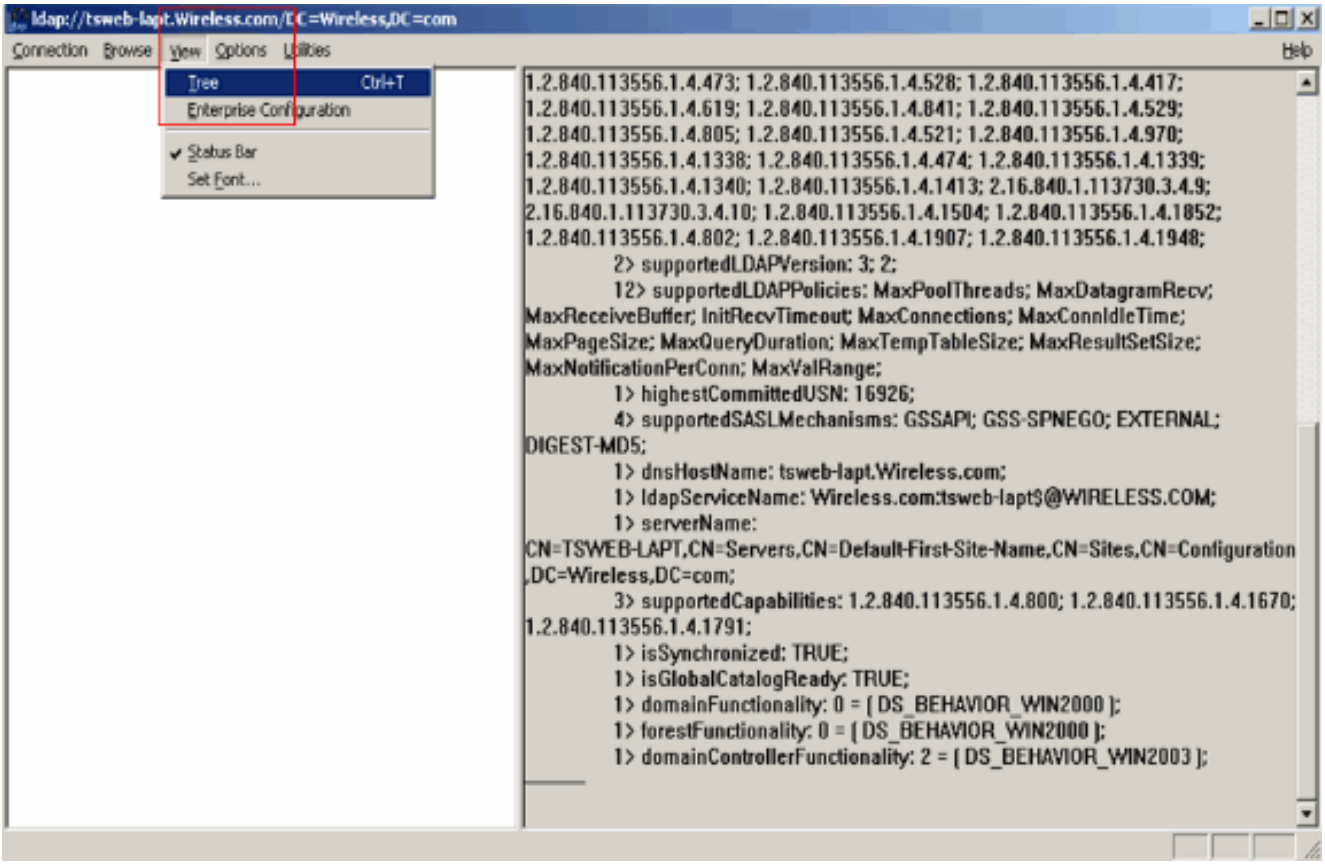
Esta herramienta GUI es un cliente LDAP que permite a los usuarios realizar operaciones (como conectar, enlazar, buscar, modificar, agregar, eliminar) en cualquier directorio compatible con LDAP, como Active Directory. LDP se utiliza para ver los objetos almacenados en Active Directory junto con sus metadatos, como los descriptores de seguridad y los metadatos de replicación.

La herramienta GUI de LDP se incluye al instalar las herramientas de soporte técnico de Windows Server 2003 desde el CD del producto. En esta sección se explica el uso de la utilidad LDP para identificar los atributos específicos asociados al usuario **user2**. Algunos de estos atributos se utilizan para rellenar los parámetros de configuración del servidor LDAP en el WLC, como el tipo de atributo de usuario y el tipo de objeto de usuario.

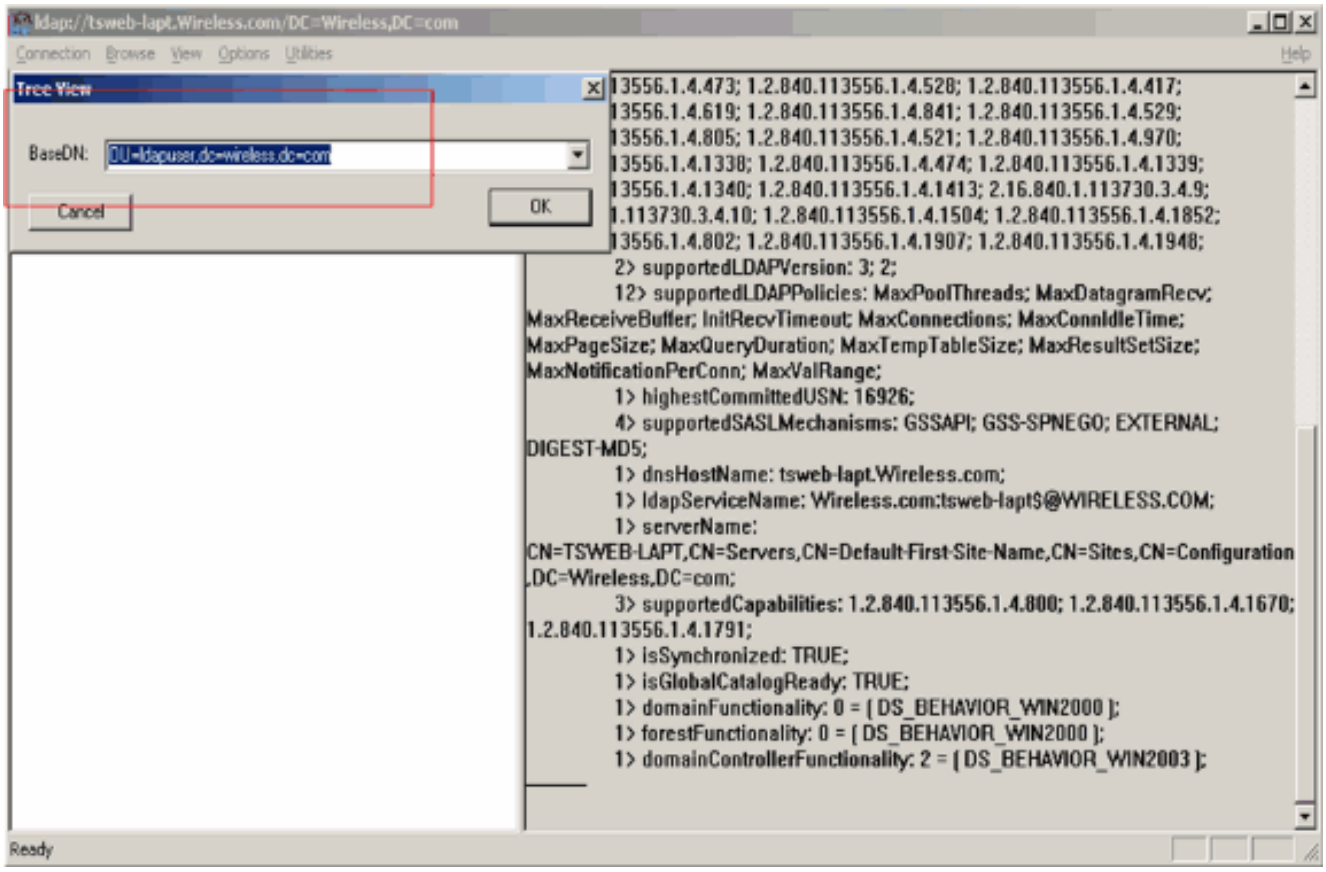
1. En el servidor Windows 2003 (incluso en el mismo servidor LDAP), haga clic en **Inicio > Ejecutar** e ingrese **LDP** para acceder al explorador LDP.
2. En la ventana principal de LDP, haga clic en **Connection > Connect** y conéctese al servidor LDAP ingresando la dirección IP del servidor
   LDAP.



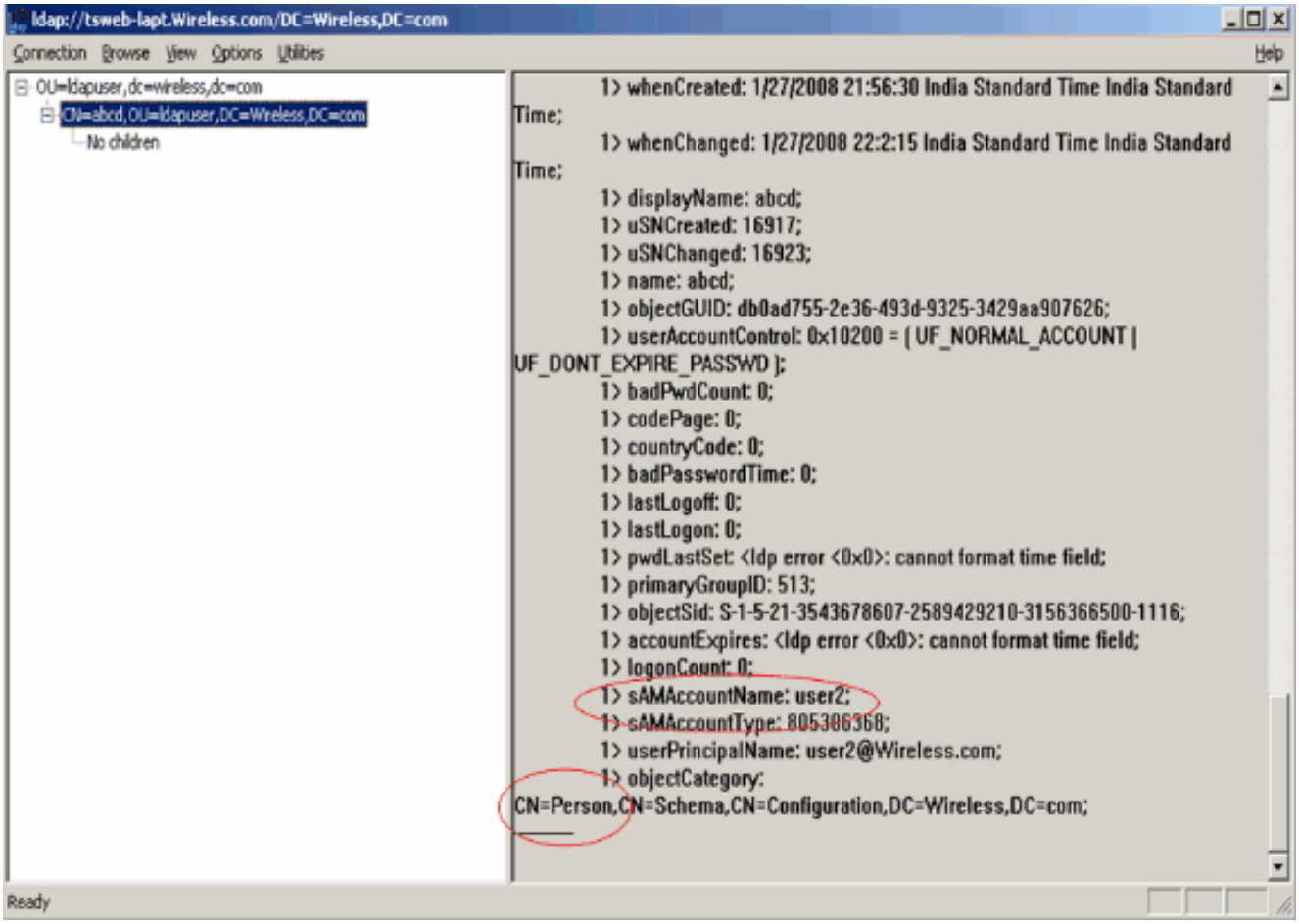
3. Una vez conectado al servidor LDAP, seleccione **View** en el menú principal y haga clic en **Tree**.



4. En la ventana Vista de árbol resultante, introduzca el DN base del usuario. En este ejemplo, **user2 se encuentra en la unidad organizativa "ldapuser" en el dominio Wireless.com**. Por lo tanto, el DN base para el usuario **user2** es **OU=ldapuser, dc=wireless, dc=com**. Click OK.



5. El lado izquierdo del navegador LDP muestra todo el árbol que aparece debajo del DN base especificado (**OU=ldapuser, dc=wireless, dc=com**). Expanda el árbol para localizar al usuario **user2**. Este usuario se puede identificar con el valor CN que representa el nombre del usuario. En este ejemplo, es **CN=abcd**. Haga doble clic en **CN=abcd**. En el panel derecho del navegador LDP, **LDP mostrará todos los atributos asociados con user2**. Este ejemplo explica este
paso:



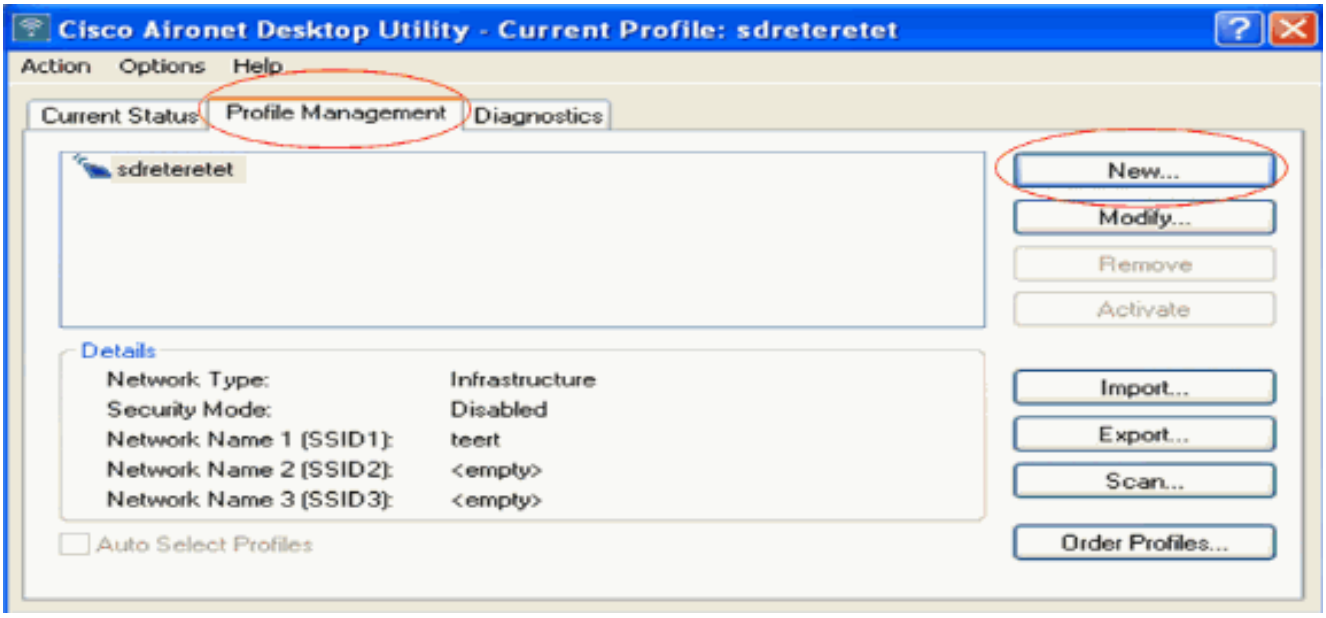
En este ejemplo, observe los campos rodeados de la derecha.

6. Como se mencionó en la sección Configure WLC with Details of LDAP Server de este documento, en el campo **User Attribute**, ingrese el nombre del atributo en el registro de usuario que contiene el nombre de usuario.En este resultado de LDP, puede ver que **sAMAccountName** es un atributo que contiene el nombre de usuario "user2". Por lo tanto, ingrese el atributo **sAMAccountName** que corresponde al campo **User Attribute** en el WLC.
7. En el campo User Object Type, ingrese el valor del atributo objectType del LDAP que identifica el registro como usuario. A menudo, los registros de usuario tienen varios valores para el atributo objectType, algunos de los cuales son únicos al usuario y otros son compartidos con otros tipos de objeto.En la salida LDP, **CN=Person** es un valor que identifica el registro como usuario. Por lo tanto, especifique **Person** como el atributo **User Object Type** en el WLC.

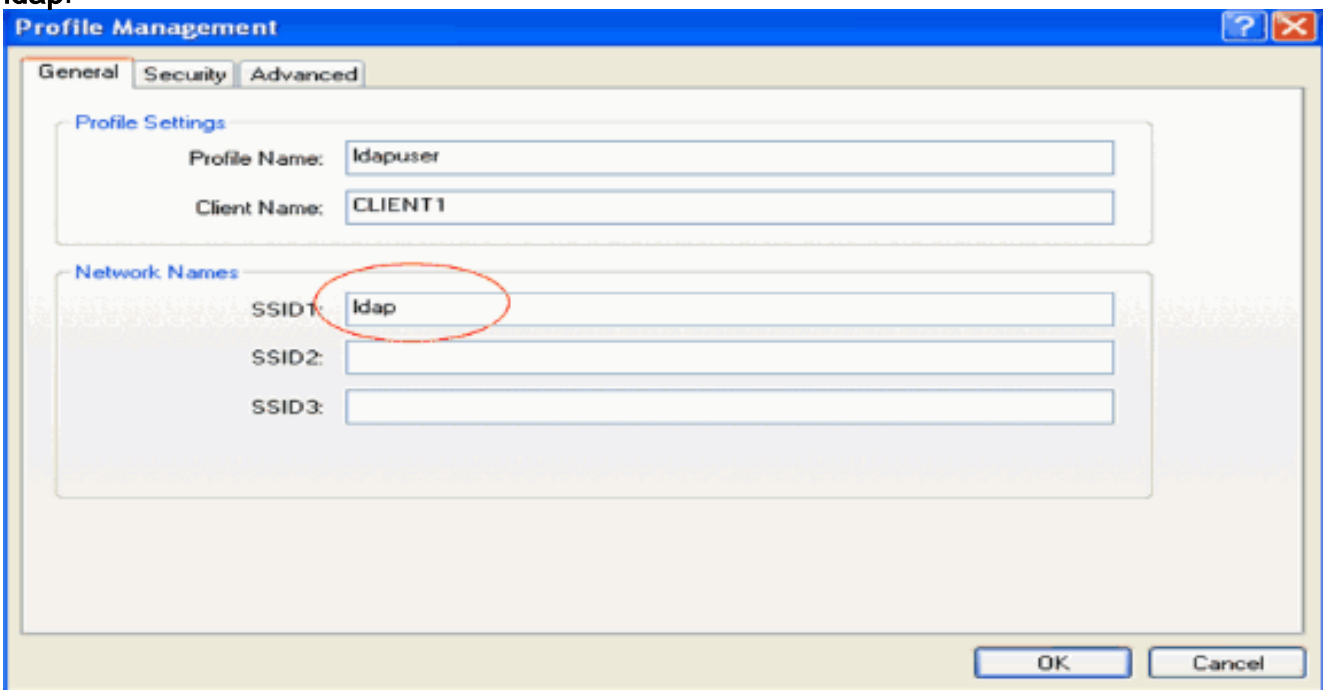
Configurar cliente inalámbrico

El último paso es configurar el cliente inalámbrico para la autenticación EAP-FAST con certificados de cliente y de servidor. Complete estos pasos para lograr esto:

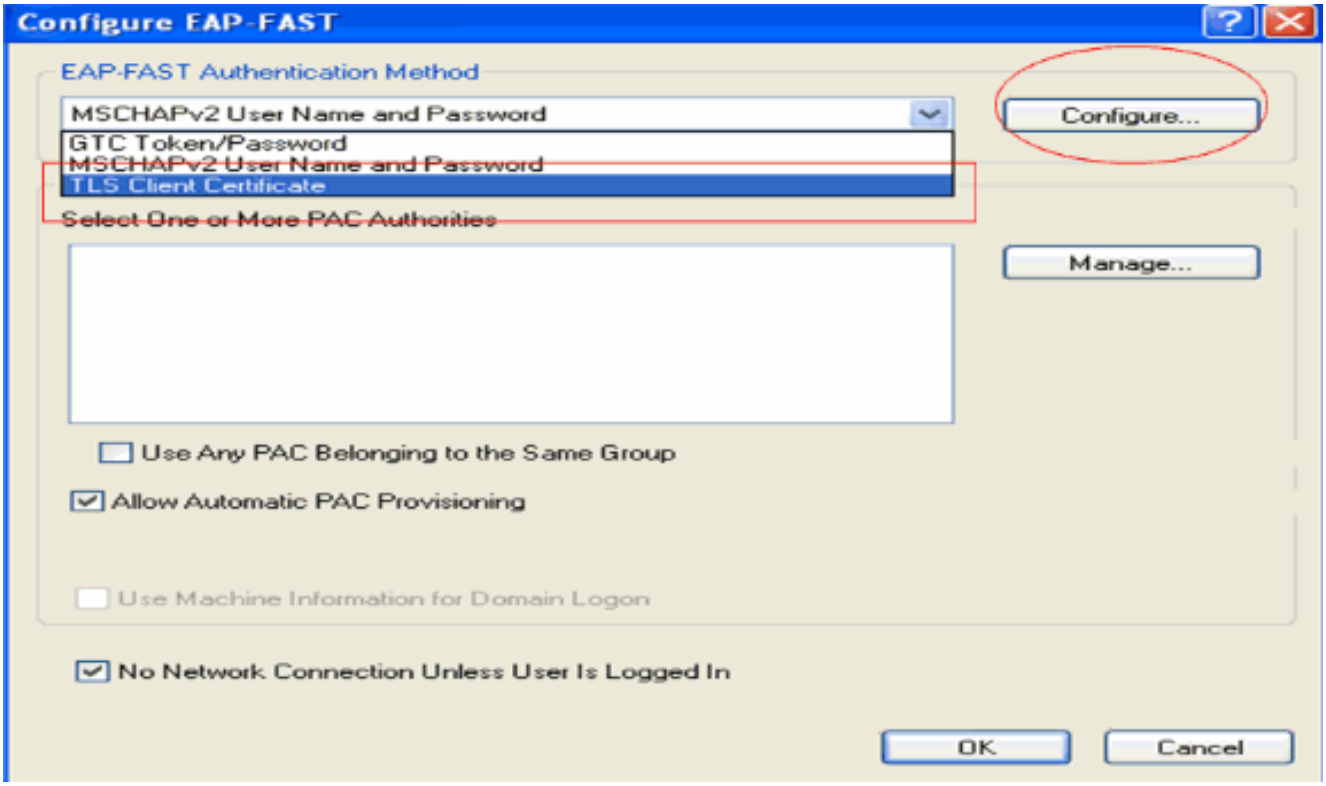
1. Inicie la **utilidad Cisco Aironet Desktop Utility** (ADU). En la ventana principal de ADU, haga clic en **Profile Management > New** para crear un nuevo perfil de cliente inalámbrico.



2. Especifique un nombre de perfil y asígnele un nombre SSID. Este nombre SSID debe ser el mismo configurado en el WLC. En este ejemplo, el nombre SSID es **ldap**.



3. Haga clic en la ficha **Security** y elija **802.1x/EAP** como Layer 2 Security. Elija **EAP-FAST** como el método EAP y haga clic en **Configure**.
4. En la página de configuración de EAP-FAST, elija **Certificado de cliente TLS** en el cuadro desplegable Método de autenticación EAP-FAST y haga clic en **Configurar**.



5. En la ventana de configuración del certificado de cliente TLS:Habilite la casilla de verificación **Validar identidad de servidor** y seleccione el certificado de CA instalado en el cliente (explicado en la sección Generar el certificado de CA raíz para el cliente de este documento) como Autoridad de certificación raíz de confianza.Seleccione el certificado de dispositivo instalado en el cliente (explicado en la sección Generación de un certificado de dispositivo para el cliente de este documento) como el certificado de cliente.Click OK.Este ejemplo explica este
paso:

Se crea el perfil del cliente inalámbrico.

Verificación

Realice estos pasos para verificar si su configuración funciona correctamente.

1. Active el **ldap** SSID en el ADU.

2. Haga clic en **Yes** o **OK**, según sea necesario, en las siguientes ventanas. Debería poder ver todos los pasos de la autenticación del cliente, así como la asociación para tener éxito en la ADU.

Use esta sección para confirmar que su configuración funciona correctamente. Utilice el modo CLI de WLC.

- Para verificar si el WLC puede comunicarse con el servidor LDAP y localizar al usuario, especifique el comando **debug aaa ldap enable** de la CLI del WLC. Este ejemplo explica un proceso de comunicación LDAP exitoso:**Nota:** Parte del resultado de esta sección se ha movido a la segunda línea debido a la consideración del espacio.(Cisco Controller) **>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

  De la información resaltada en esta salida de depuración, está claro que el servidor LDAP es consultado por el WLC con los atributos de usuario especificados en el WLC y el proceso LDAP es exitoso.
- Para verificar si la autenticación EAP local es exitosa, especifique el comando **debug aaa local-auth eap method events enable** desde la CLI del WLC. Aquí tiene un ejemplo:(Cisco Controller) **>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
```

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...

Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....

.....

.....

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....

.....

.....

.....
.

- El comando **debug aaa local-auth db enable** también es muy útil. Aquí tiene un ejemplo:(Cisco Controller) **>debug aaa local-auth db enable**

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsys

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

.....

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsys

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- Para ver los certificados instalados en el WLC que se utilizarán para la autenticación local, ejecute el comando **show local-auth certificates** desde la CLI del WLC. Aquí tiene un ejemplo:(Cisco Controller) **>show local-auth certificates**

```
Certificates available for Local EAP authentication:


Certificate issuer ............................ vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ............................ cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

              Not installed.
```

- Para ver la configuración de autenticación local en el WLC desde el modo CLI, ejecute el comando **show local-auth config**. Aquí tiene un ejemplo:(Cisco Controller) **>show local-auth config**

```
User credentials database search order:
```

```
    Primary ..................................... LDAP


Timer:

    Active timeout ............................. 300


Configured EAP profiles:

    Name ........................................ ldapuser

      Certificate issuer ....................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ........................... fast

      Configured on WLANs ....................... 2


EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key ................................ <hidden>

      TTL for the PAC ........................... 10

      Anonymous provision allowed ............... No

      ........................................

      ........................................

      Authority Information ..................... Cisco A-ID
```

Troubleshoot

Puede utilizar estos comandos para resolver problemas de su configuración:

- **debug aaa local-auth eap method events enable**
- **debug aaa all enable**

- debug dot1x packet enable

Información Relacionada

- Ejemplo de Configuración de Autenticación EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo
- PEAP bajo Redes Inalámbricas Unificadas con Microsoft Internet Authentication Service (IAS)
- Ejemplo de Configuración de Asignación de VLAN Dinámica con WLC Basada en ACS a Asignación de Grupos de Active Directory
- Guía de configuración del controlador de LAN inalámbrica de Cisco - Configuración de soluciones de seguridad
- Guía de configuración del controlador LAN inalámbrico de Cisco - Administración del software y las configuraciones del controlador
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Preguntas Frecuentes sobre el Diseño y las Funciones de Wireless LAN Controller (WLC)
- Cisco Secure Services Client con autenticación EAP-FAST
- Preguntas frecuentes sobre el controlador LAN inalámbrico (WLC)
- Preguntas frecuentes sobre mensajes del sistema y errores del controlador LAN inalámbrico (WLC) de controladores
- 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).