Ejemplo de Configuración de Servidor EAP Local de Red Inalámbrica Unificada

Contenido

Introducción

Este documento describe la configuración de un servidor local de Extensible Authentication Protocol (EAP) en un Controlador de LAN de Red Inalámbrica Cisco (WLC) para la autenticación de los usuarios de red inalámbrica.

EAP local es un método de autenticación que permite autenticar a usuarios y clientes inalámbricos de forma local. Se ha diseñado para su uso en oficinas remotas que desean mantener la conectividad con clientes inalámbricos cuando el sistema back-end se interrumpe o el servidor de autenticación externo se desactiva. Cuando habilita el EAP local, el controlador funciona como el servidor de autenticación y la base de datos de usuario local, eliminando así 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 del protocolo ligero de acceso a directorios (LDAP) para autenticar a los usuarios. EAP local admite EAP ligero (LEAP), autenticación EAP-flexible a través de tunelación segura (EAP-FAST) y autenticación EAP-Transport Layer Security (EAP-TLS) entre el controlador y los clientes inalámbricos.

Observe que el servidor EAP local no está disponible si hay una configuración de servidor

RADIUS externo global en el WLC. Todas las solicitudes de autenticación se reenvían al RADIUS externo global hasta que el servidor EAP local esté disponible. Si el WLC pierde la conectividad con el servidor RADIUS externo, entonces el servidor EAP local se vuelve activo. Si no hay ninguna configuración de servidor RADIUS global, el servidor EAP local se activa inmediatamente. El servidor EAP local no se puede utilizar para autenticar clientes, que están conectados a otros WLC. En otras palabras, un WLC no puede reenviar su solicitud EAP a otro WLC para la autenticación. Cada WLC debe tener su propio servidor EAP local y una base de datos individual.

Nota: Use estos comandos para detener el WLC de enviar solicitudes a un servidor RADIUS externo .

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

El servidor local EAP admite estos protocolos en la versión 4.1.171.0 del software y posteriores:

- LEAP
- EAP-FAST (tanto nombre de usuario/contraseña como certificados)
- EAP-TLS

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar WLC y puntos de acceso ligeros (LAP) para el funcionamiento básico
- Conocimiento del protocolo de punto de acceso ligero (LWAPP) y de los métodos de seguridad inalámbrica
- Conocimiento básico de la autenticación EAP local.

Componentes Utilizados

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

- Windows XP con tarjeta de adaptador CB21AG y Cisco Secure Services Client versión 4.05
- Controlador de LAN inalámbrica Cisco 4400 4.1.171.0
- Microsoft Certification Authority en el servidor Windows 2000

Convenciones

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

Configuración de EAP local en el controlador de LAN inalámbrica

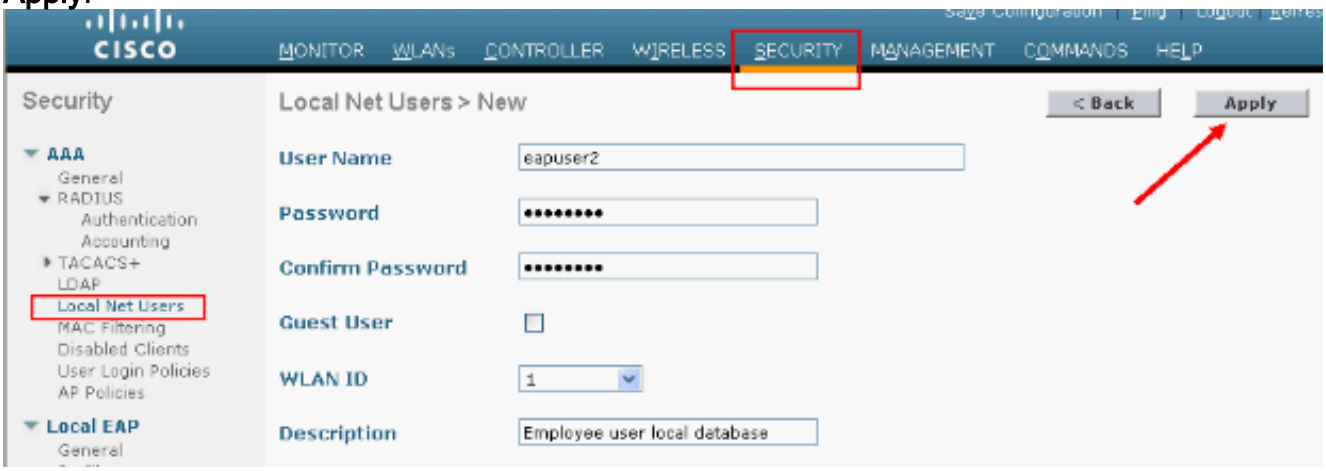
de Cisco

Este documento asume que la configuración básica del WLC ya está completa.

Configuración EAP local

Complete estos pasos para configurar el EAP local:

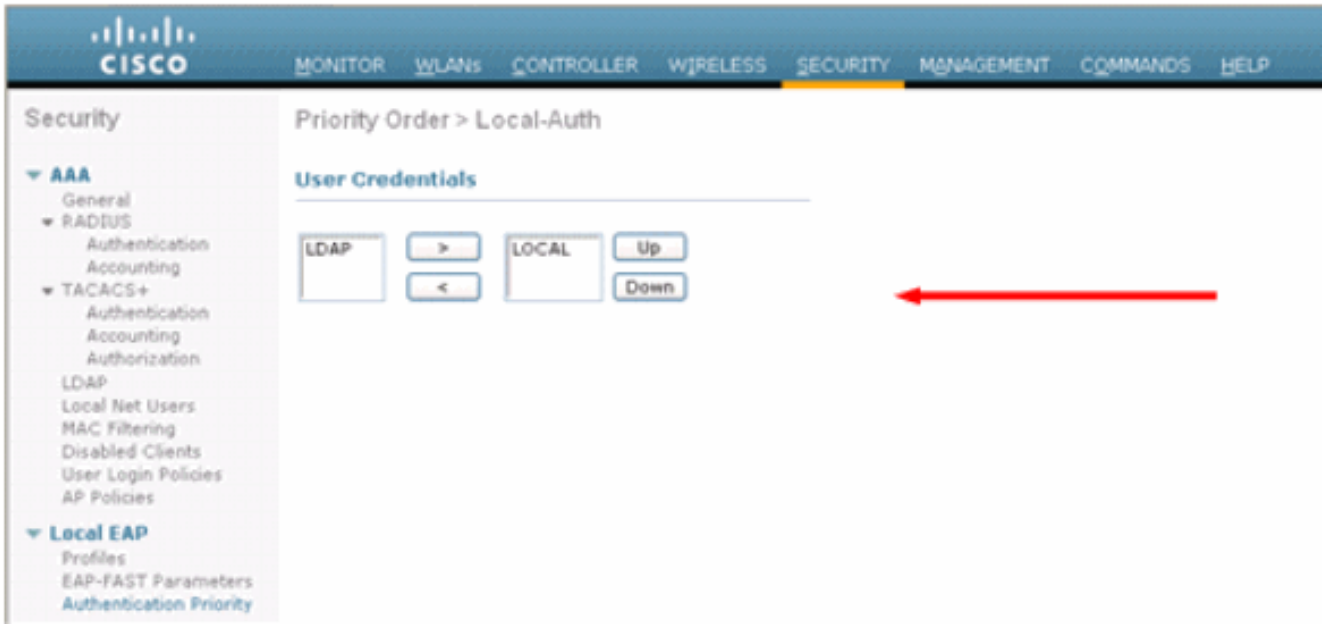
1. Agregar un usuario de red local:Desde la GUI. elija **Security > Local Net Users > New**, ingrese User Name, Password, Guest User, WLAN ID y Description y haga clic en **Apply**.



Desde la CLI, puede utilizar el comando **config netuser add** ***<username>*** ***<password>*** **<WLAN id>** ***<description>***:**Nota:** Este comando se ha reducido a una segunda línea por razones espaciales.

```
(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
```

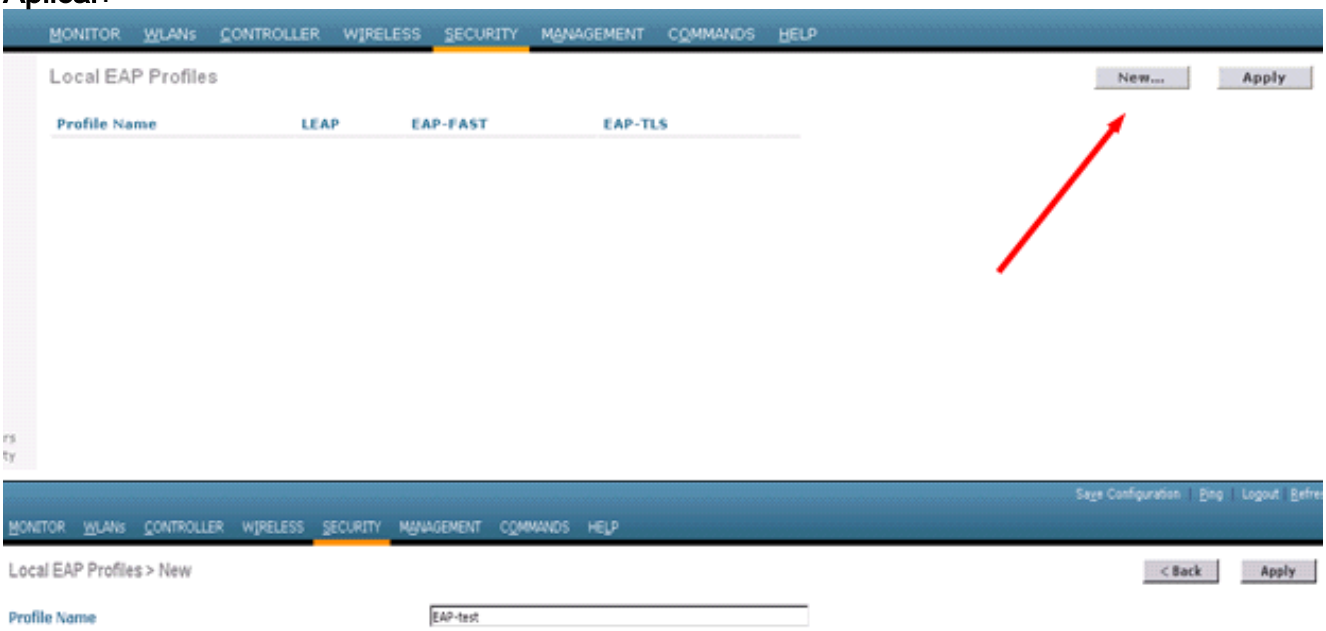
2. Especifique el orden de recuperación de credenciales de usuario.Desde la GUI, elija **Security > Local EAP > Authentication Priority**. A continuación, seleccione LDAP, haga clic en el **<"** botón y haga clic en **Aplicar**. Esto coloca primero las credenciales de usuario en la base de datos
local.



Desde la CLI:

```
(Cisco Controller) >config local-auth user-credentials local
```

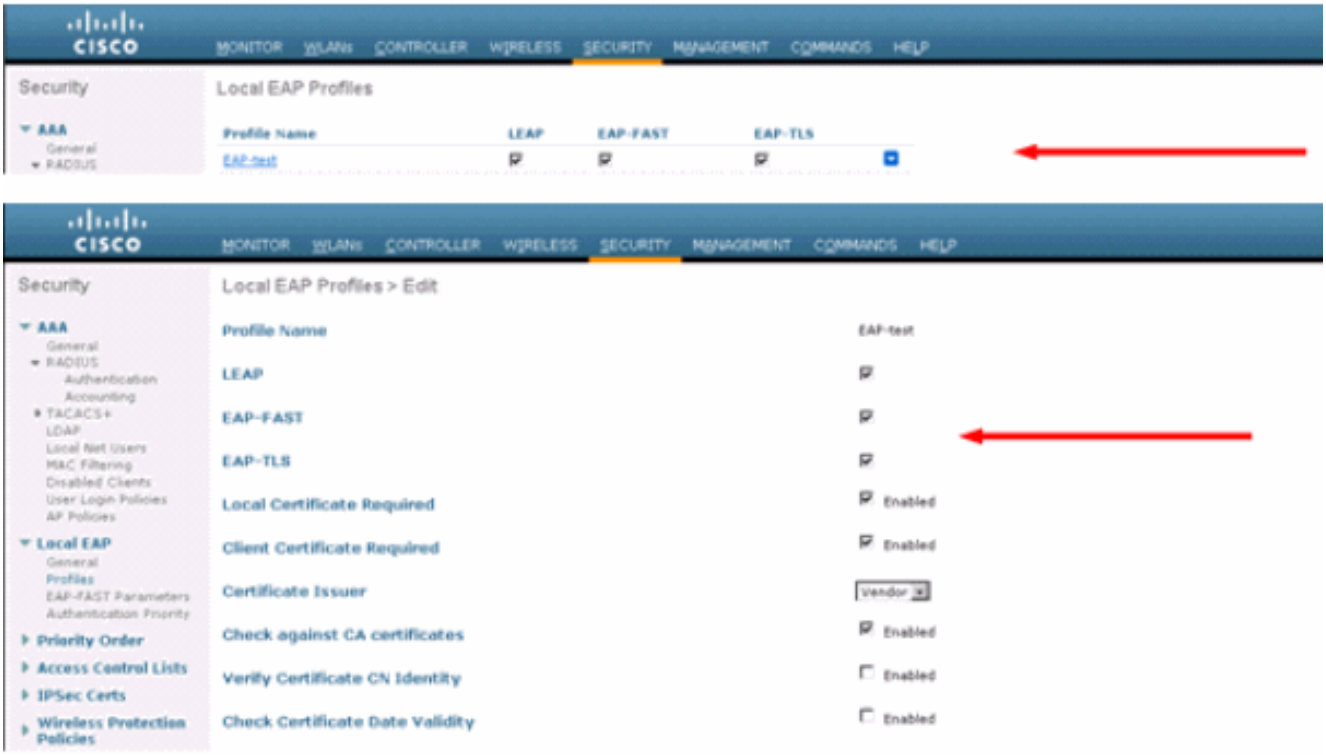
3. Agregar un perfil EAP:Para hacer esto desde la GUI, elija **Security > Local EAP > Profiles** y haga clic en **New**. Cuando aparezca la nueva ventana, escriba el nombre del perfil y haga clic en
Aplicar.



También puede hacer esto usando el comando CLI **config local-auth eap-profile add *<profile-name>*.** En nuestro ejemplo, el nombre del perfil es *EAP-test*.

```
(Cisco Controller) >config local-auth eap-profile add EAP-test
```

4. Agregue un método al perfil EAP.Desde la GUI elija **Security > Local EAP > Profiles** y haga clic en el nombre del perfil para el cual desea agregar los métodos de autenticación. Este ejemplo utiliza LEAP, EAP-FAST y EAP-TLS. Haga clic en **Aplicar** para establecer los métodos.

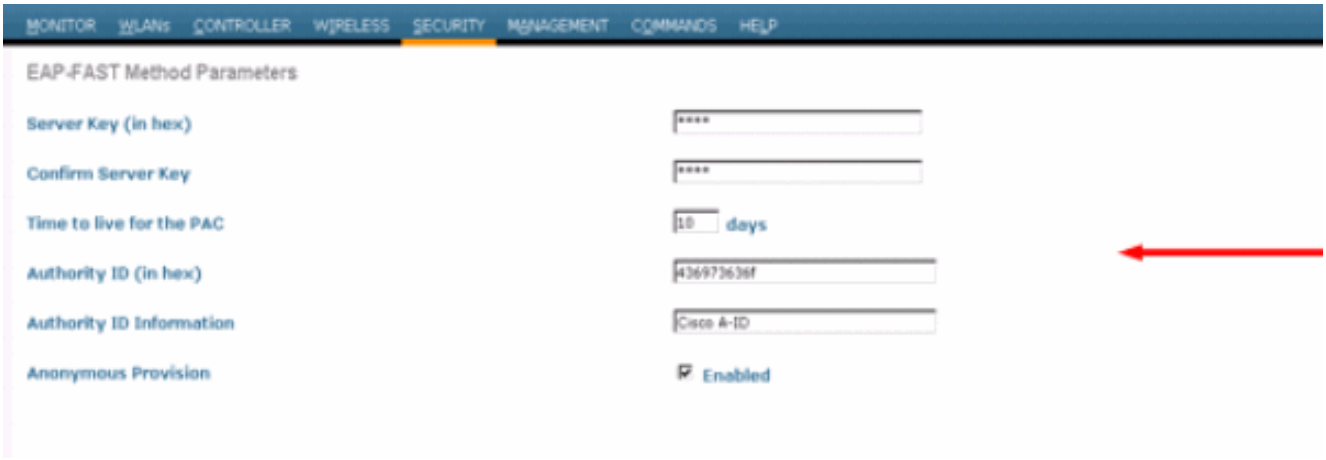


También puede utilizar el comando CLI **config local-auth eap-profile method add *<method-***

name><profile-name>. En nuestra configuración de ejemplo, agregamos tres métodos a la prueba EAP del perfil. Los métodos son LEAP, EAP-FAST y EAP-TLS cuyos nombres de método son *salto, rápido* y *tls* respectivamente. Este resultado muestra los comandos de configuración CLI:

```
(Cisco Controller) >config local-auth eap-profile method add leap EAP-test
(Cisco Controller) >config local-auth eap-profile method add fast EAP-test
(Cisco Controller) >config local-auth eap-profile method add tls EAP-test
```

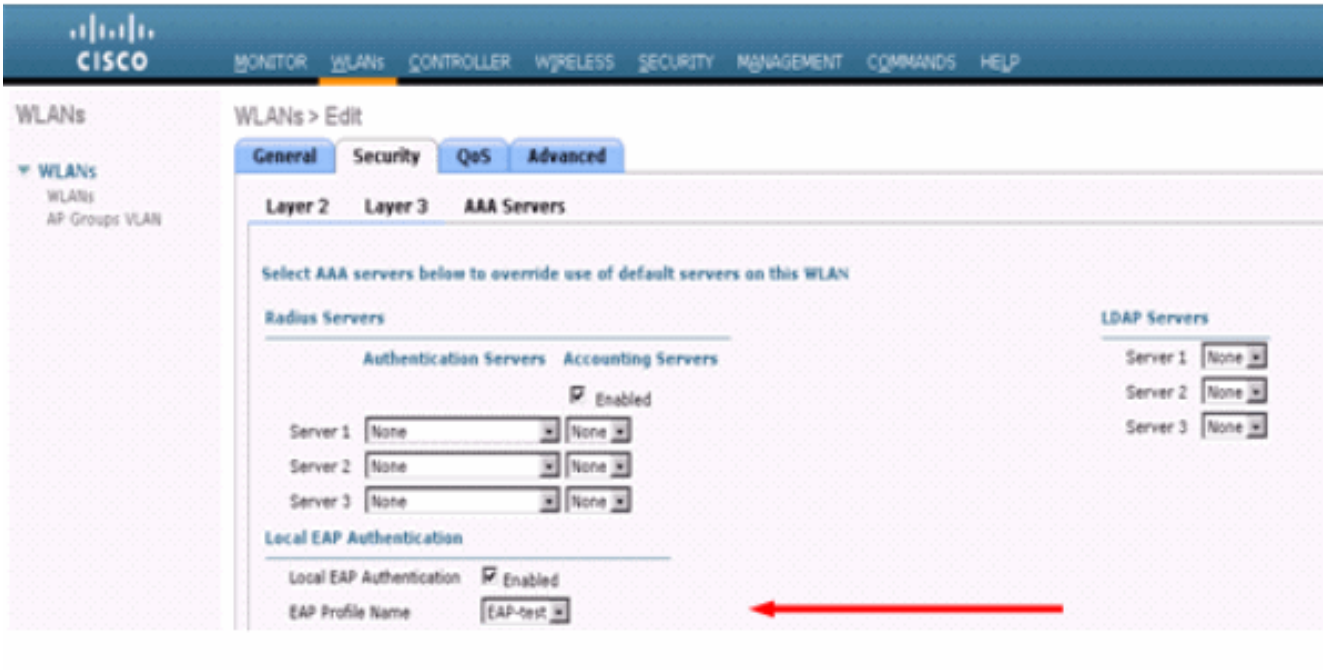
5. Configure los parámetros del método EAP. Esto sólo se utiliza para EAP-FAST. Los parámetros que se deben configurar son:**Server Key (Clave de servidor)**: clave de servidor para cifrar/descifrar las credenciales de acceso protegido (PAC) (en formato hexadecimal).**Tiempo de vida para PAC (pac-ttl)**: establece el tiempo de vida para el PAC.**ID de autoridad (ID de autoridad)** : establece el identificador de autoridad.**Disposición anónima (no probada)**: configura si se permite una provisión anónima. Esto se activa como opción predeterminada.Para la configuración a través de la GUI, elija **Security > Local EAP > EAP-FAST Parameters** e ingrese la clave del servidor, Time to live para los valores PAC, Authority ID (en hexadecimal) e Authority ID Information.



Estos son los comandos de configuración CLI que se deben utilizar para configurar estos parámetros para EAP-FAST:

```
(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

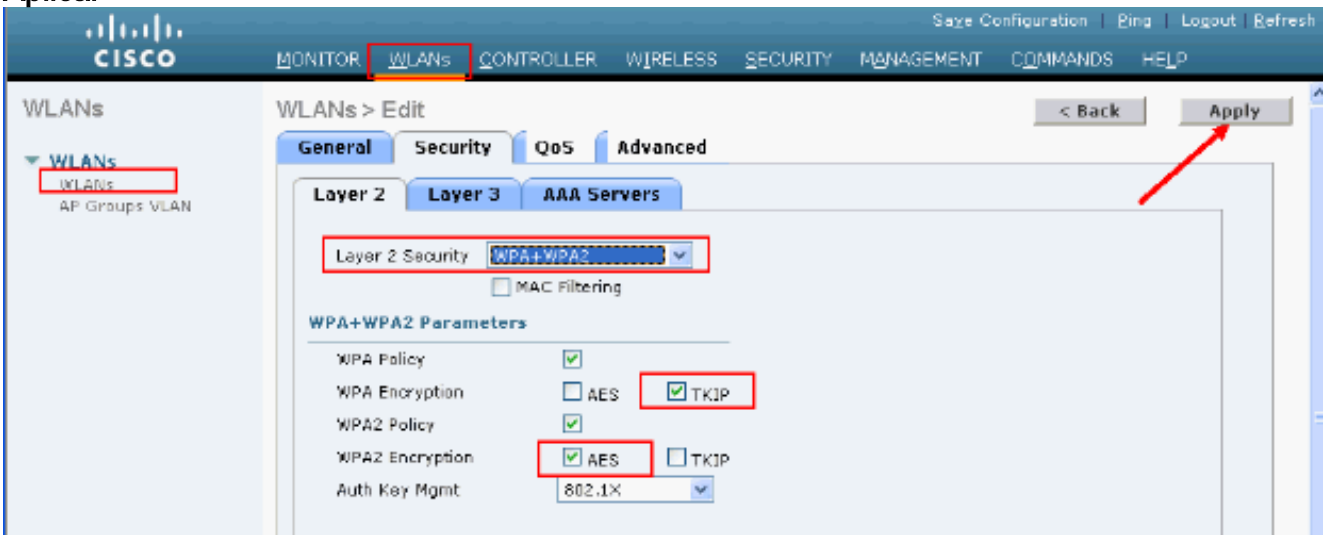
6. Habilitar autenticación local por WLAN:Desde la GUI elija **WLANs** en el menú superior y seleccione la WLAN para la cual desea configurar la autenticación local. Aparece una nueva ventana. Haga clic en las fichas **Seguridad > AAA**. Verifique la **autenticación** EAP **local** y seleccione el nombre de perfil EAP correcto en el menú desplegable como muestra este ejemplo:



También puede ejecutar el comando de configuración CLI **config wlan local-auth enable *<profile-name>* *<wlan-id>***, como se muestra a continuación:

```
(Cisco Controller) >config wlan local-auth enable EAP-test 1
```

7. Establezca los parámetros de seguridad de la capa 2.Desde la interfaz GUI, en la ventana WLAN Edit vaya a las pestañas **Security > Layer 2** y elija **WPA+WPA2** en el menú desplegable Layer 2 Security. En la sección Parámetros WPA+WPA2, establezca el cifrado WPA en **TKIP** y **AES** de cifrado WPA2. A continuación, haga clic en **Aplicar**.



Desde la CLI, utilice estos comandos:

```
(Cisco Controller) >config wlan security wpa enable 1
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

8. Verifique la configuración:

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................. Undefined

Configured EAP profiles:
    Name ........................................ EAP-test
```

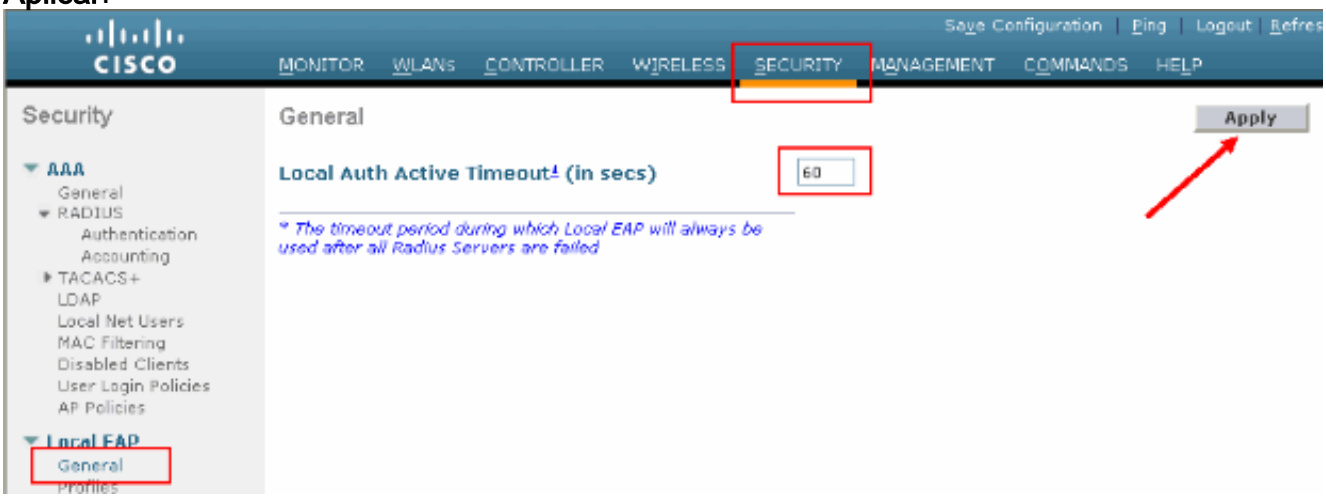
```
      Certificate issuer ..................... cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ......................... leap fast tls
      Configured on WLANs ..................... 1

EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key .............................. <hidden>
      TTL for the PAC ......................... 10
      Anonymous provision allowed ............. Yes
      Authority ID ............................ 43697369f10000000000000000000000
      Authority Information ................... CiscoA-ID
```

Puede ver parámetros específicos de wlan 1 con el comando **show wlan** *<wlan id>*:

```
(Cisco Controller) >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'EAP-test')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Enabled
         AES Cipher.............................. Disabled
      WPA2 (RSN IE)............................... Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                        Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
```

```
   CKIP ..................................... Disabled
   IP Security.............................. Disabled
   IP Security Passthru..................... Disabled
   Web Based Authentication................. Disabled
--More-- or (q)uit
   Web-Passthrough.......................... Disabled
   Conditional Web Redirect................. Disabled
   Auto Anchor.............................. Disabled
   Cranite Passthru......................... Disabled
   Fortress Passthru........................ Disabled
   H-REAP Local Switching................... Disabled
   Infrastructure MFP protection............ Enabled
                                          (Global Infrastructure MFP Disabled)
   Client MFP............................... Optional
   Tkip MIC Countermeasure Hold-down Timer.. 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

Hay otros parámetros de autenticación local que se pueden configurar, en particular el temporizador de tiempo de espera activo. Este temporizador configura el período durante el cual se utiliza el EAP local después de que todos los servidores RADIUS hayan fallado.Desde la GUI, elija **Security > Local EAP > General** y establezca el valor de tiempo. A continuación, haga clic en **Aplicar**.



Desde la CLI, ejecute estos comandos:

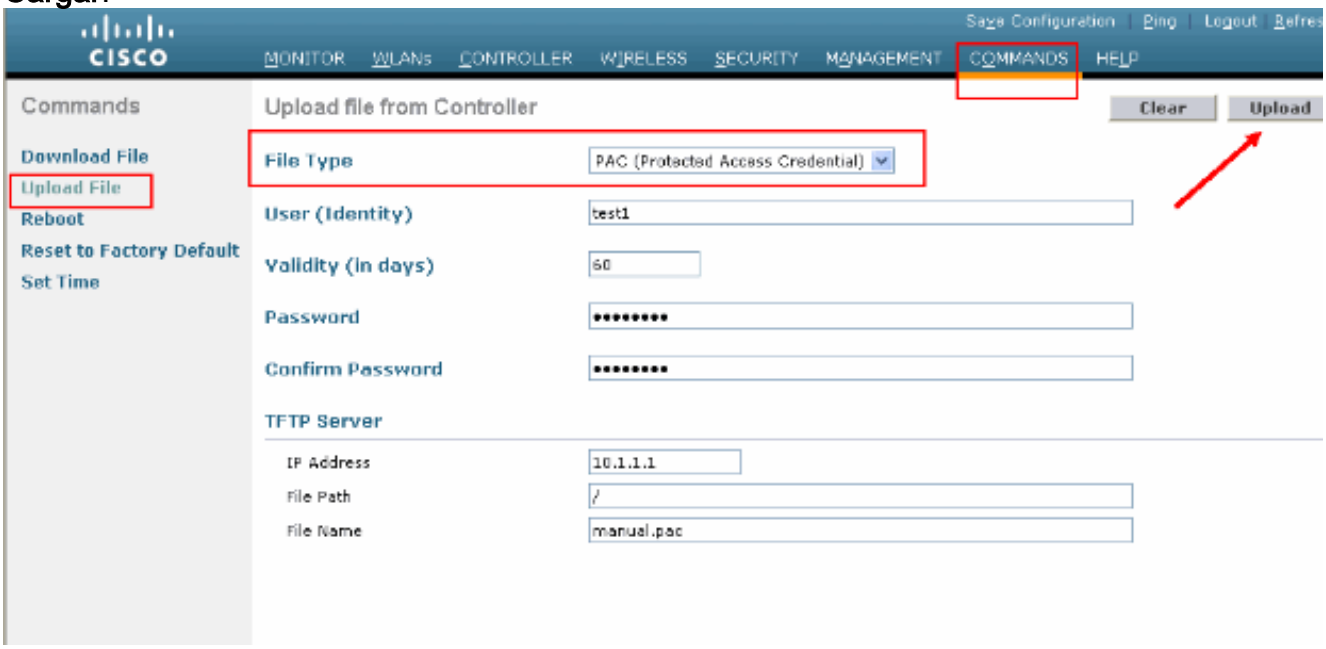
```
(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60
```

Puede verificar el valor al que se configura este temporizador cuando ejecuta el comando **show local-auth config**.

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................... 60

Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. Si necesita generar y cargar el PAC manual, puede utilizar la GUI o la CLI.Desde la GUI,

seleccione **COMANDOS** en el menú superior y elija **Cargar archivo** de la lista en el lado derecho. Seleccione **PAC (Credencial de acceso protegido)** en el menú desplegable Tipo de archivo. Introduzca todos los parámetros y haga clic en **Cargar**.



Desde la CLI, ingrese estos comandos:

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >transfer upload pac test1 60 cisco123

(Cisco Controller) >transfer upload serverip 10.1.1.1

(Cisco Controller) >transfer upload filename manual.pac

(Cisco Controller) >transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 10.1.1.1
TFTP Path................................................ /
TFTP Filename............................................ manual.pac
Data Type................................................ PAC
PAC User................................................. test1
PAC Validity............................................. 60 days
PAC Password............................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

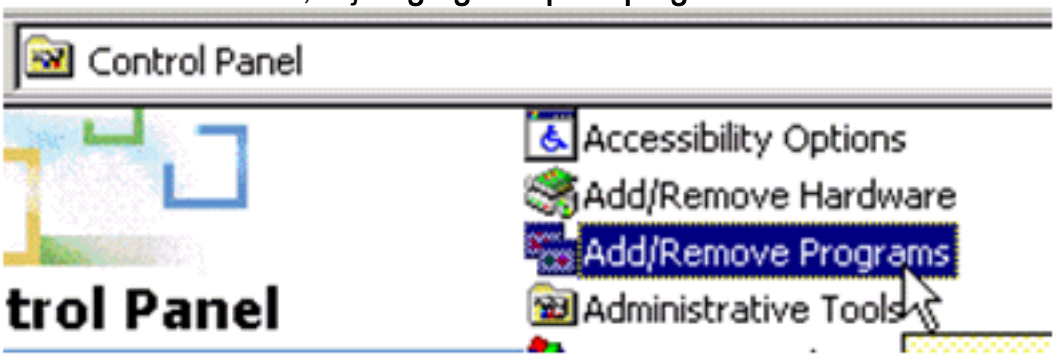
Microsoft Certification Authority

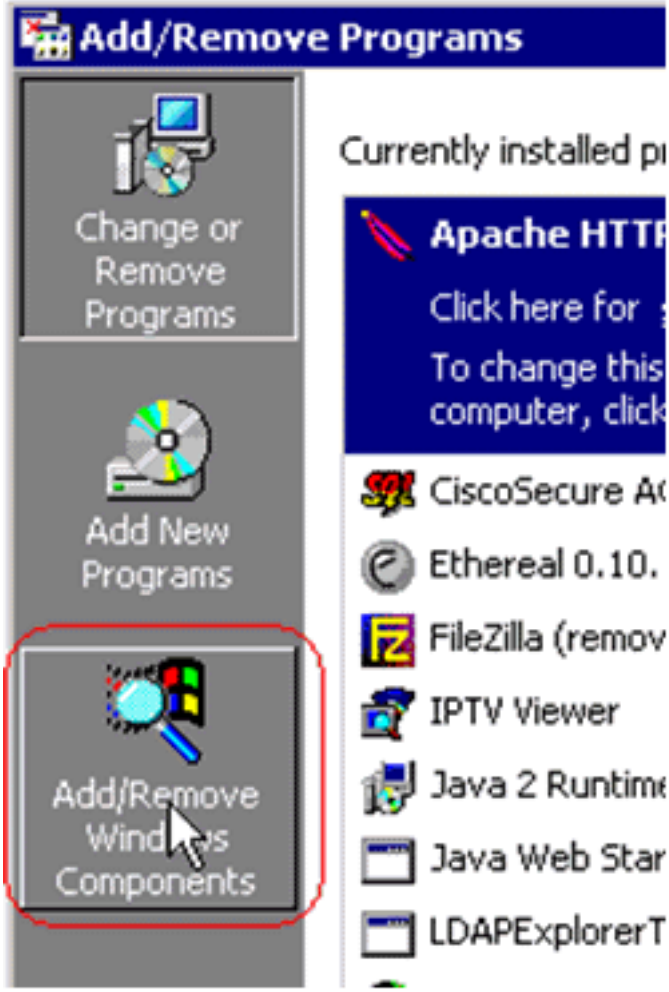
Para utilizar EAP-FAST versión 2 y autenticación EAP-TLS, el WLC y todos los dispositivos cliente deben tener un certificado válido y también deben conocer el certificado público de la Autoridad de certificación.

Instalación

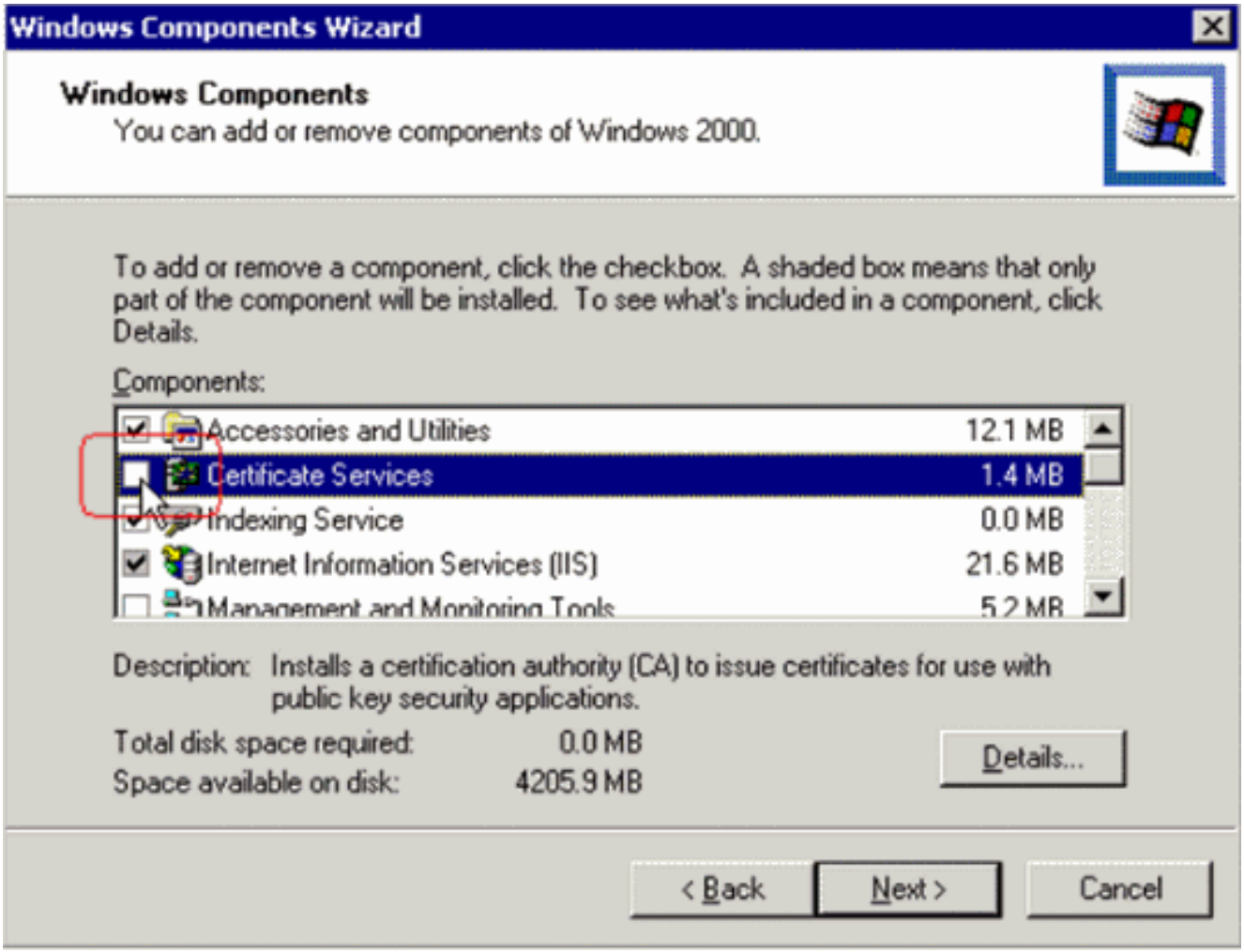
Si el servidor de Windows 2000 aún no tiene instalados los servicios de Certification Authority, debe instalarlo.

Complete estos pasos para activar Microsoft Certification Authority en un Windows 2000 Server:

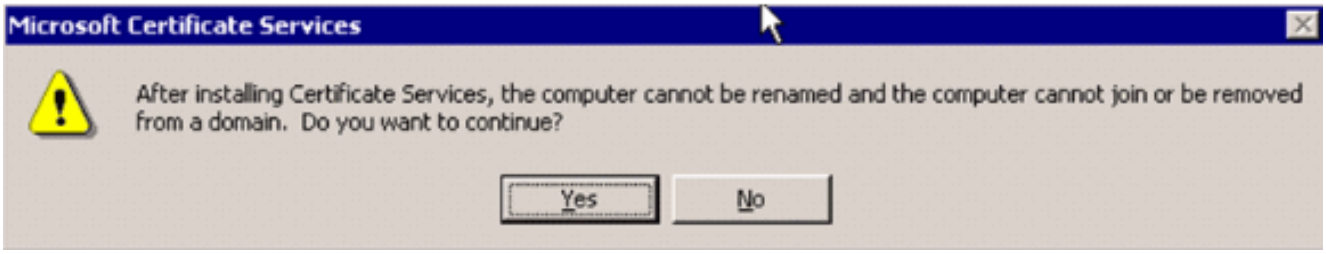
1. En el Panel de control, elija **Agregar o quitar programas**.


:
2. Seleccione **Add/Remove Windows Components** en el lado


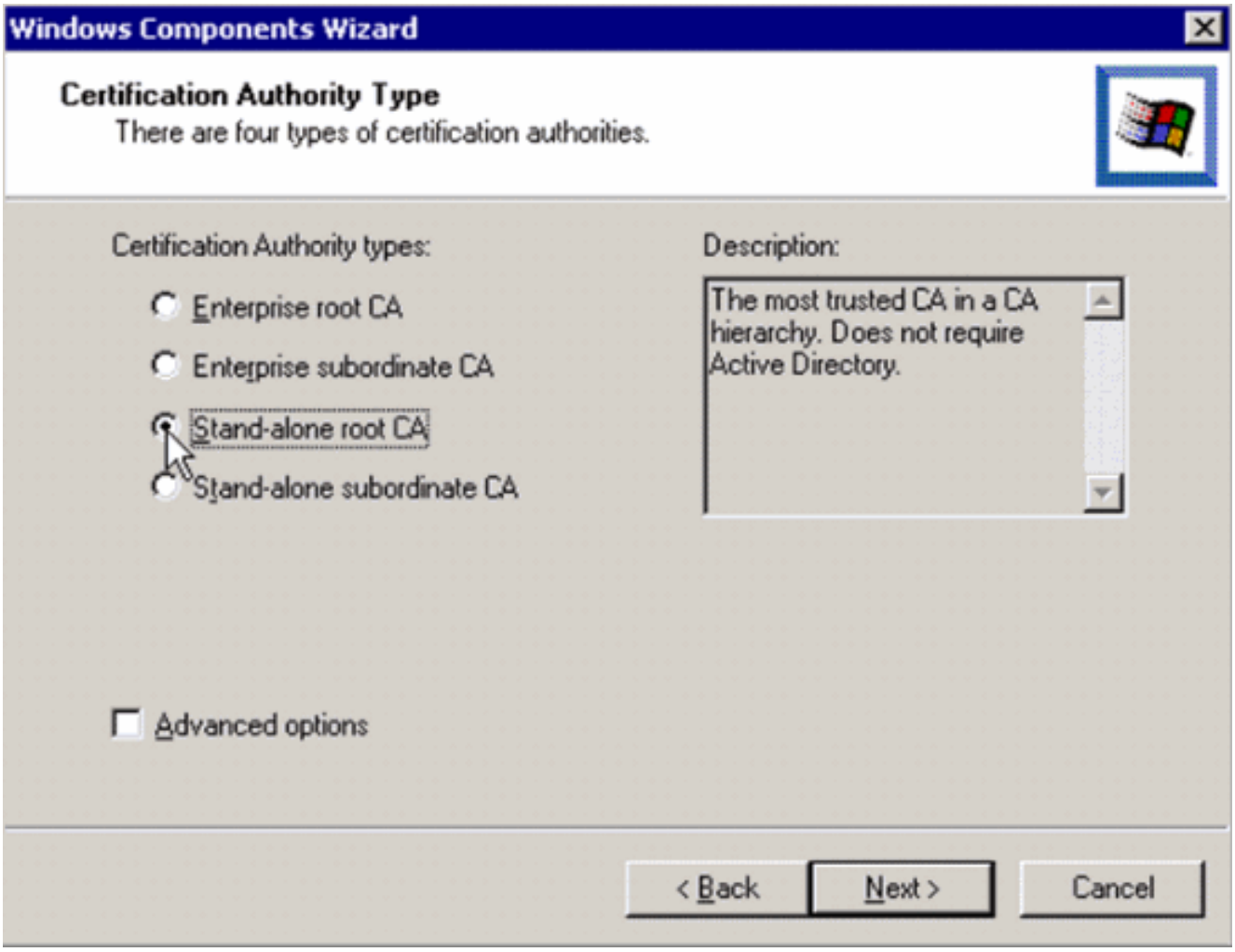
izquierdo.
3. Verifique **Servicios de Certificados**.



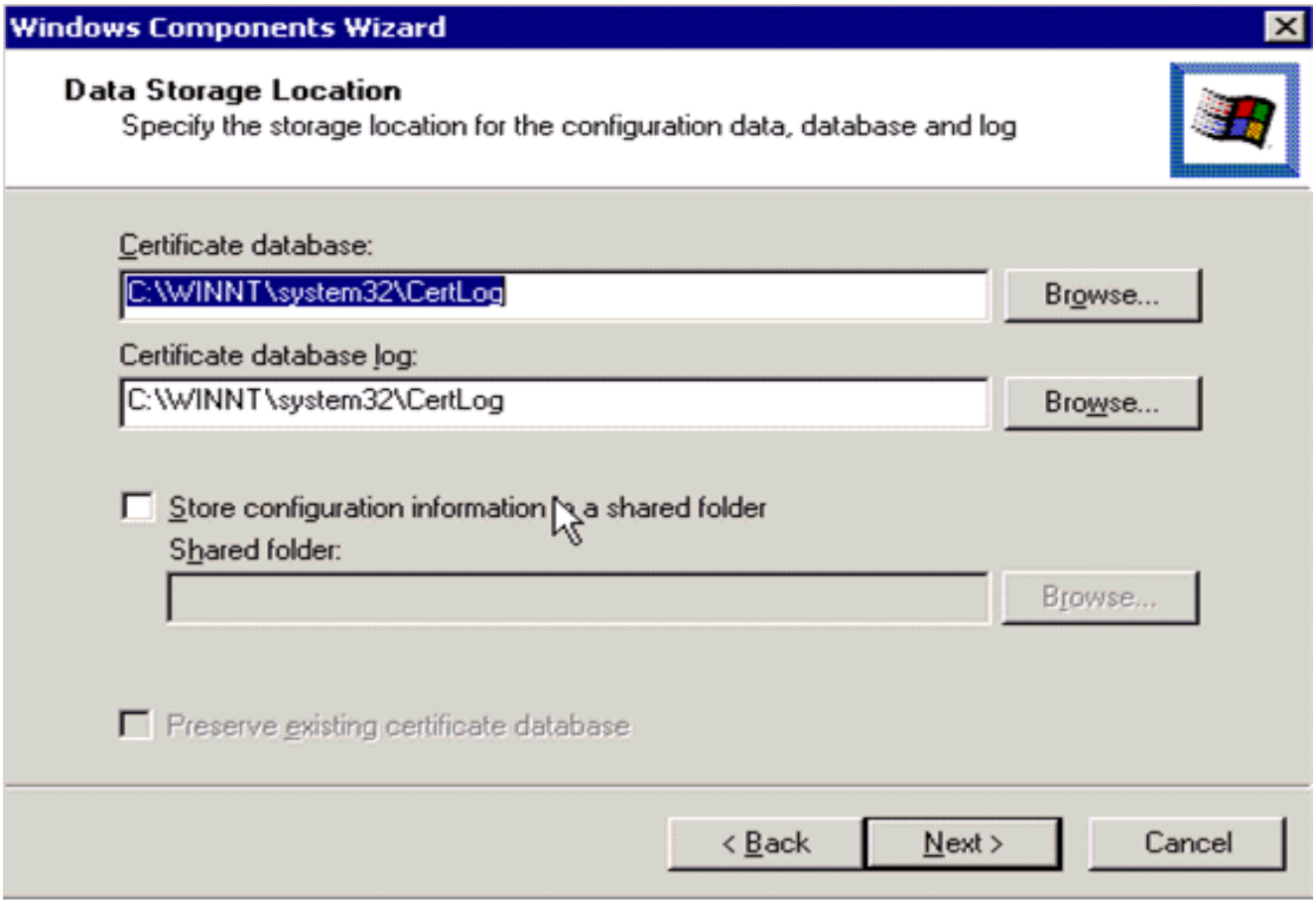
Revise esta advertencia antes de continuar:



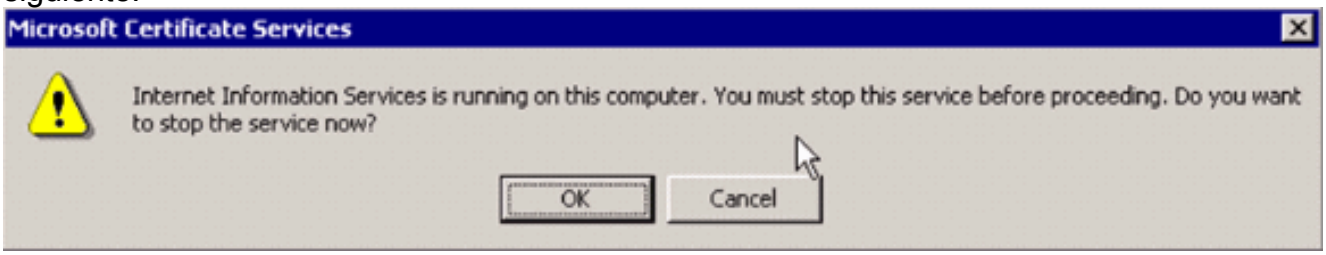
4. Seleccione el tipo de entidad de certificación que desea instalar. Para crear una autoridad independiente simple, seleccione **CA raíz independiente**.



5. Introduzca la información necesaria sobre la Autoridad de certificación. Esta información crea un certificado autofirmado para su Autoridad de Certificación. Recuerde el nombre de la CA que utiliza.La Autoridad de Certificación almacena los certificados en una base de datos. Este ejemplo utiliza la configuración predeterminada propuesta por Microsoft:



6. Los servicios de Microsoft Certification Authority utilizan IIS Microsoft Web Server para crear y administrar certificados de cliente y servidor. Debe reiniciar el servicio IIS para lo siguiente:



Microsoft Windows 2000 Server instala ahora el nuevo servicio. Debe tener el CD de instalación del servidor de Windows 2000 para instalar nuevos componentes de Windows.La Autoridad de certificación ya está instalada.

Instalación del certificado en el controlador de LAN inalámbrica de Cisco

Para utilizar EAP-FAST versión 2 y EAP-TLS en el servidor EAP local de un controlador LAN inalámbrico de Cisco, siga estos tres pasos:

1. Instale el certificado del dispositivo en el controlador de LAN inalámbrica.
2. Descargue un certificado de CA del proveedor al controlador de LAN inalámbrica.
3. Configure el Wireless LAN Controller para utilizar EAP-TLS.

Tenga en cuenta que en el ejemplo que se muestra en este documento, Access Control Server (ACS) se instala en el mismo host que Microsoft Active Directory y Microsoft Certification Authority, pero la configuración debe ser la misma si el servidor ACS se encuentra en un servidor diferente.

Instalación del certificado de dispositivo en el controlador de LAN inalámbrica

Complete estos pasos:

1. . Complete estos pasos para generar el certificado para importar al WLC:Vaya a **http://<serverIpAddr>/certsrv**.Elija **Request a Certificate** y haga clic en **Next**.Elija **Advanced Request** y haga clic en **Next**.Elija **Submit a certificate request to this CA using a form** y haga clic en **Next**.Elija **servidor Web** para la plantilla de certificados e introduzca la información pertinente. A continuación, marque las claves como **exportables**.Ahora recibirá un certificado que necesita instalar en su equipo.
2. Complete estos pasos para recuperar el certificado del equipo:Abra un explorador de Internet Explorer y elija **Herramientas > Opciones de Internet > Contenido**.Haga clic en **Certificados**.Seleccione el certificado recién instalado en el menú desplegable.Haga clic en **Exportar**.Haga clic en **Next** dos veces y elija **Yes export the private key**. Este formato es PKCS#12 (formato .PFX).Elija **Enable strong protection**.Escriba una contraseña.Guárdelo en un archivo <tme2.pfx>.
3. Copie el certificado en el formato PKCS#12 en cualquier equipo en el que tenga instalado Openssl para convertirlo al formato PEM.
```
openssl pkcs12 -in tme2.pfx -out tme2.pem
!--- The command to be given, -in Enter Import Password: !--- Enter the password given
previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase.
Verifying - Enter PEM pass phrase:
```
4. Descargue el certificado de dispositivo con formato PEM convertido en el WLC.
```
(Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password
!--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download
filename tme2.pem

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor Dev Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```
5. Una vez reiniciado, verifique el certificado.
```
(Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer ..................................... vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
  Device certificate:
```

```
Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
 Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
  Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

Descargue un certificado de CA del proveedor al controlador de LAN inalámbrica

Complete estos pasos:

1. Complete estos pasos para recuperar el Certificado CA del Proveedor:Vaya a **http://<serverIpAddr>/certsrv**.Elija **Recuperar el certificado de CA** y haga clic en **Siguiente**.Elija el certificado CA.Haga clic en **DER codificado**.Haga clic en **Descargar certificado de CA** y guarde el certificado como **rootca.cer**.
2. Convierta la CA del proveedor desde el formato DER en formato PEM con el **comando openssl x509 -en rootca.cer -report DER -out rootca.pem -outform PEM**.El archivo de salida es rootca.pem en formato PEM.
3. Descargue el certificado de la CA del proveedor:

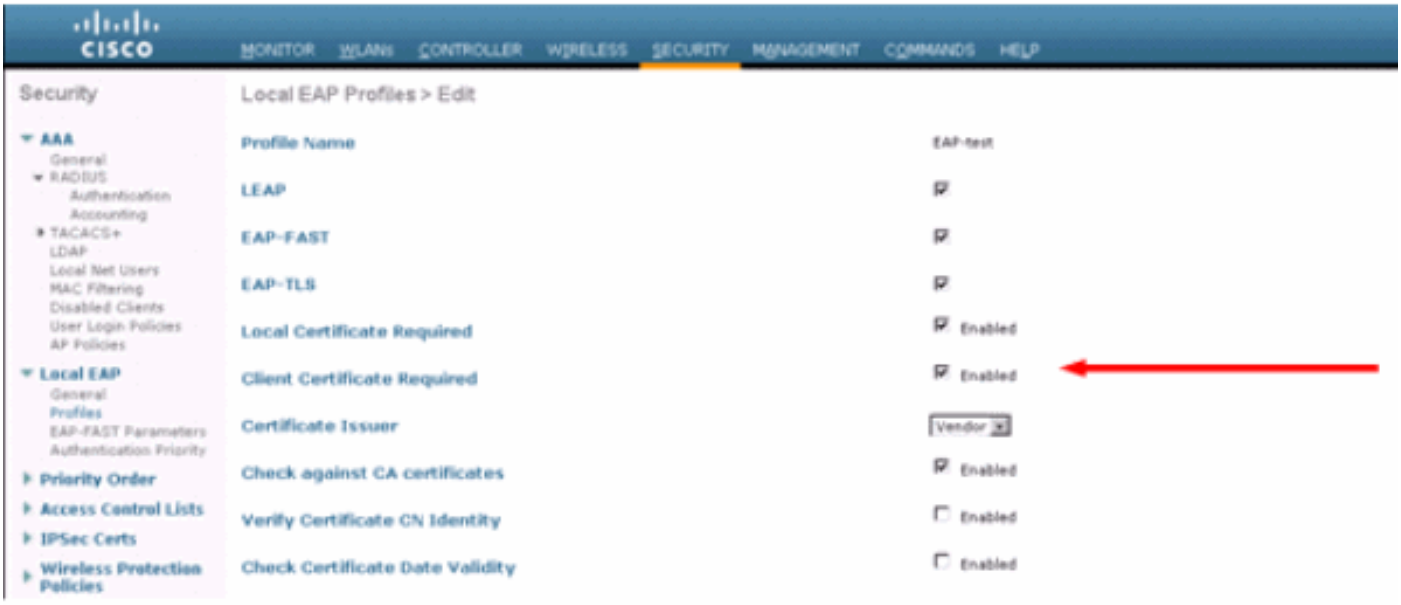
```
(Cisco Controller) >transfer download datatype eapcacert

(Cisco Controller) >transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.

(Cisco Controller) >transfer download filename rootca.pem

(Cisco Controller) >transfer download start ?

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor CA Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ rootca.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 new certificate.
```

Configure el Wireless LAN Controller para utilizar EAP-TLS

Complete estos pasos:

En la GUI, elija **Security > Local EAP > Profiles**, elija el perfil y verifique estas configuraciones:

- Se habilita el certificado local requerido.
- El certificado de cliente requerido está habilitado.
- El emisor del certificado es el proveedor.
- La comprobación en los certificados de CA está activada.



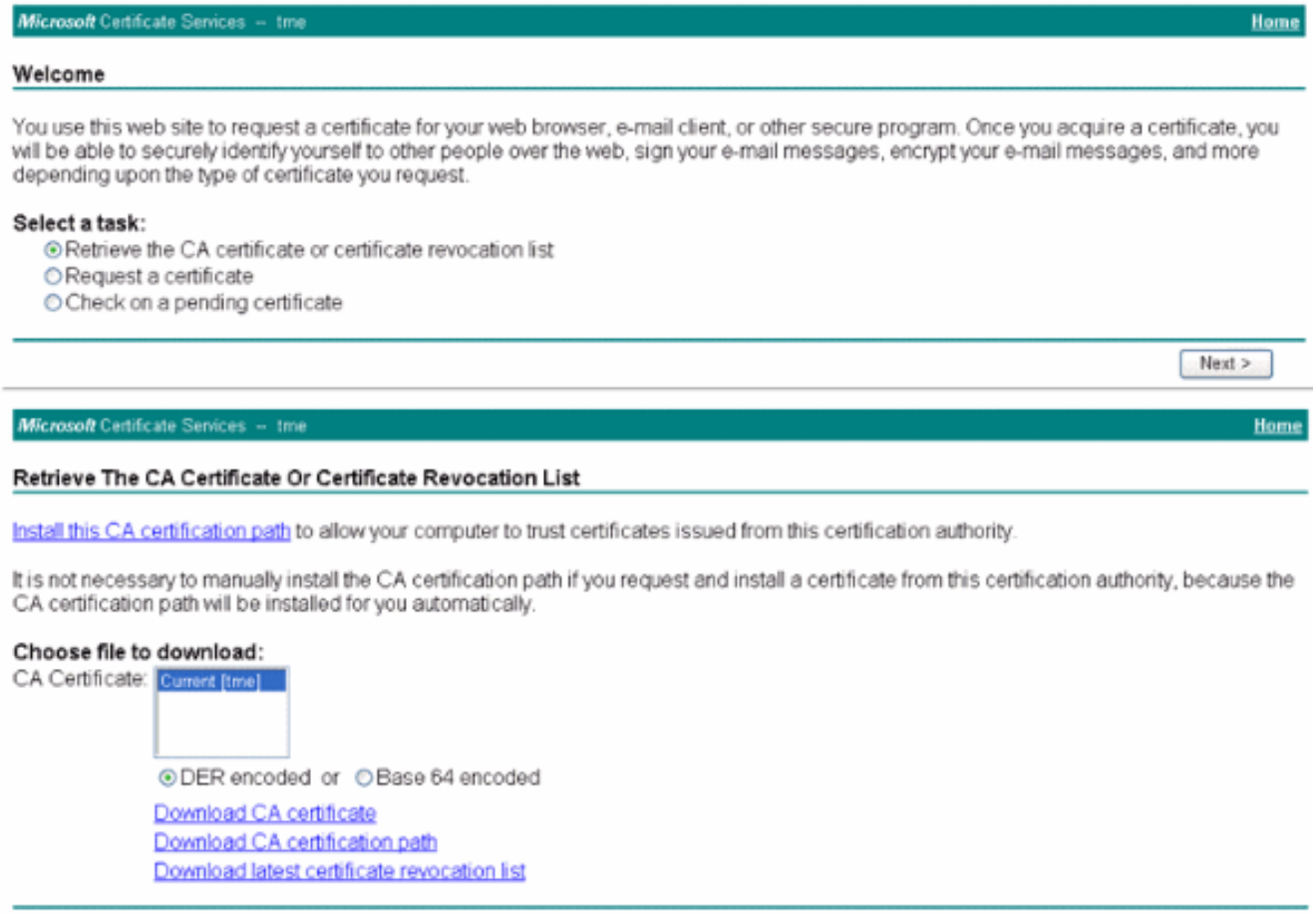
Instalación del Certificado de Autoridad de Certificación en el Dispositivo Cliente

Descargue e instale un certificado de CA raíz para el cliente

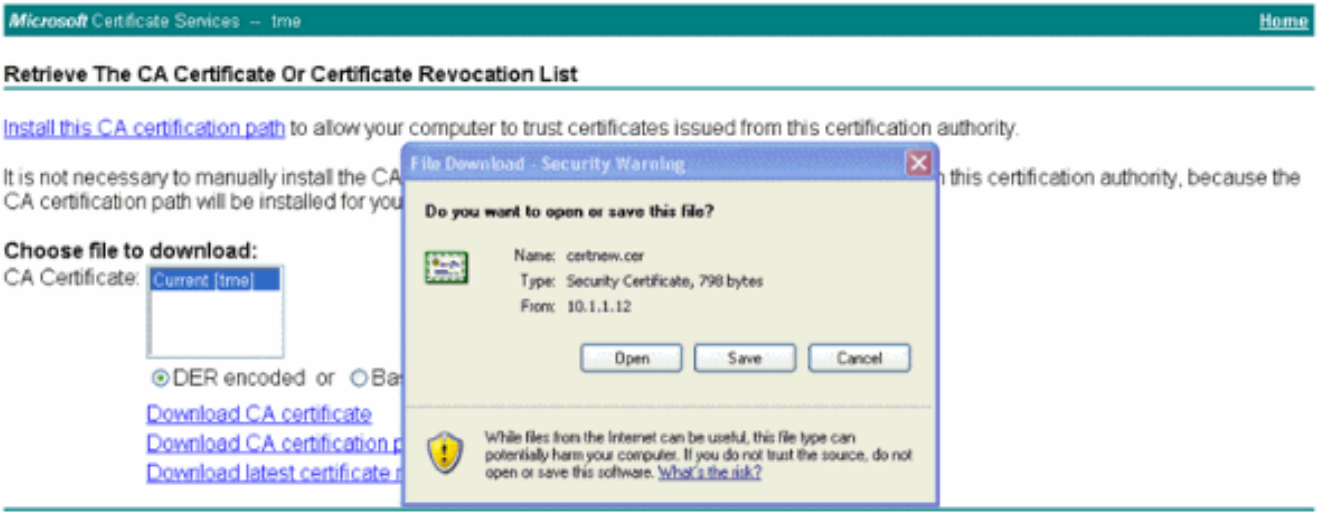
El cliente debe obtener un certificado CA raíz de un servidor de la Autoridad de certificación. Hay varios métodos que puede utilizar para obtener un certificado de cliente e instalarlo en el equipo de Windows XP. Para adquirir un certificado válido, el usuario de Windows XP debe iniciar sesión con su ID de usuario y debe tener una conexión de red.

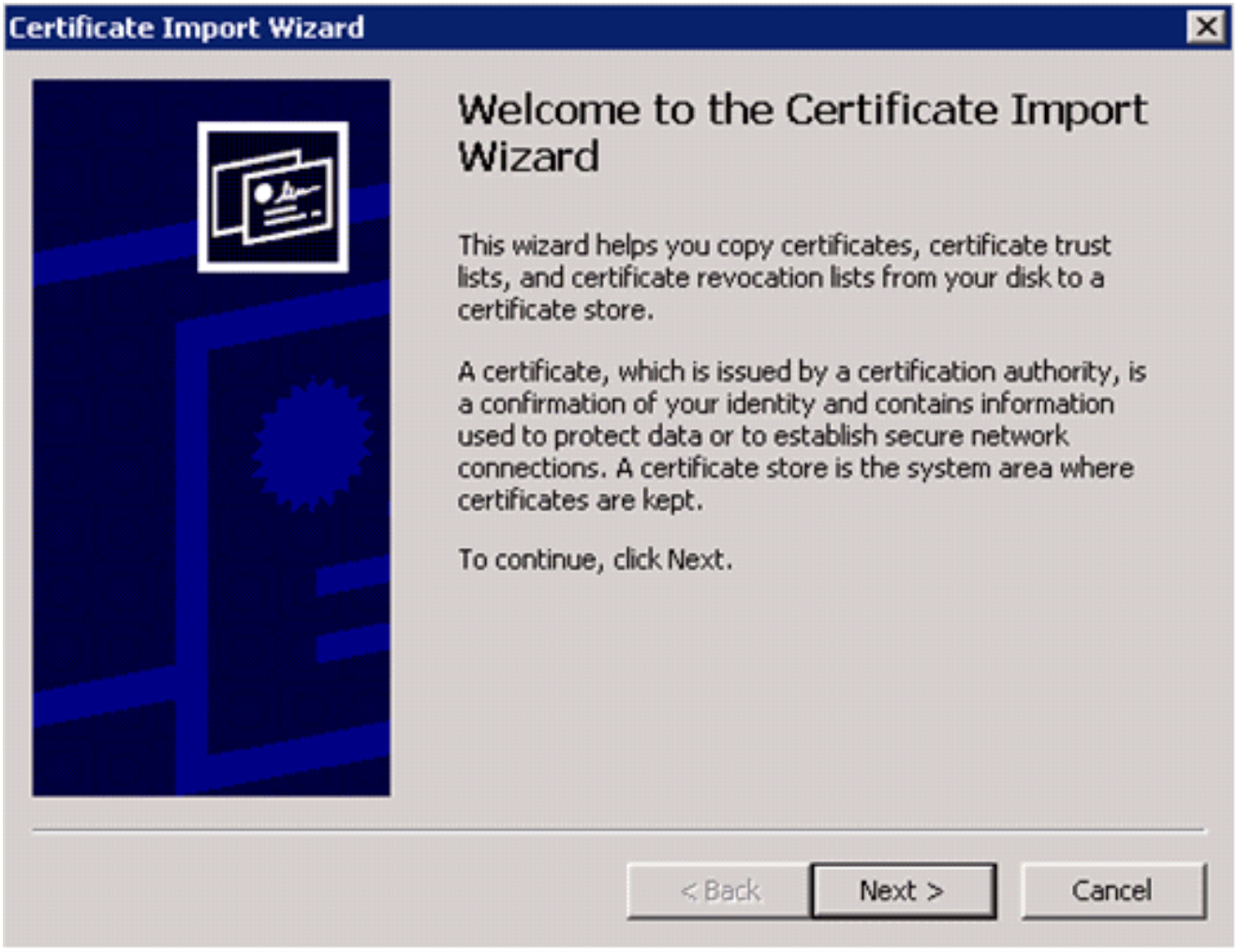
Se utilizó un explorador web en el cliente de Windows XP y una conexión por cable a la red para obtener un certificado de cliente del servidor de la autoridad de certificación raíz privada. Este procedimiento se utiliza para obtener el certificado de cliente de un servidor de Microsoft Certification Authority:

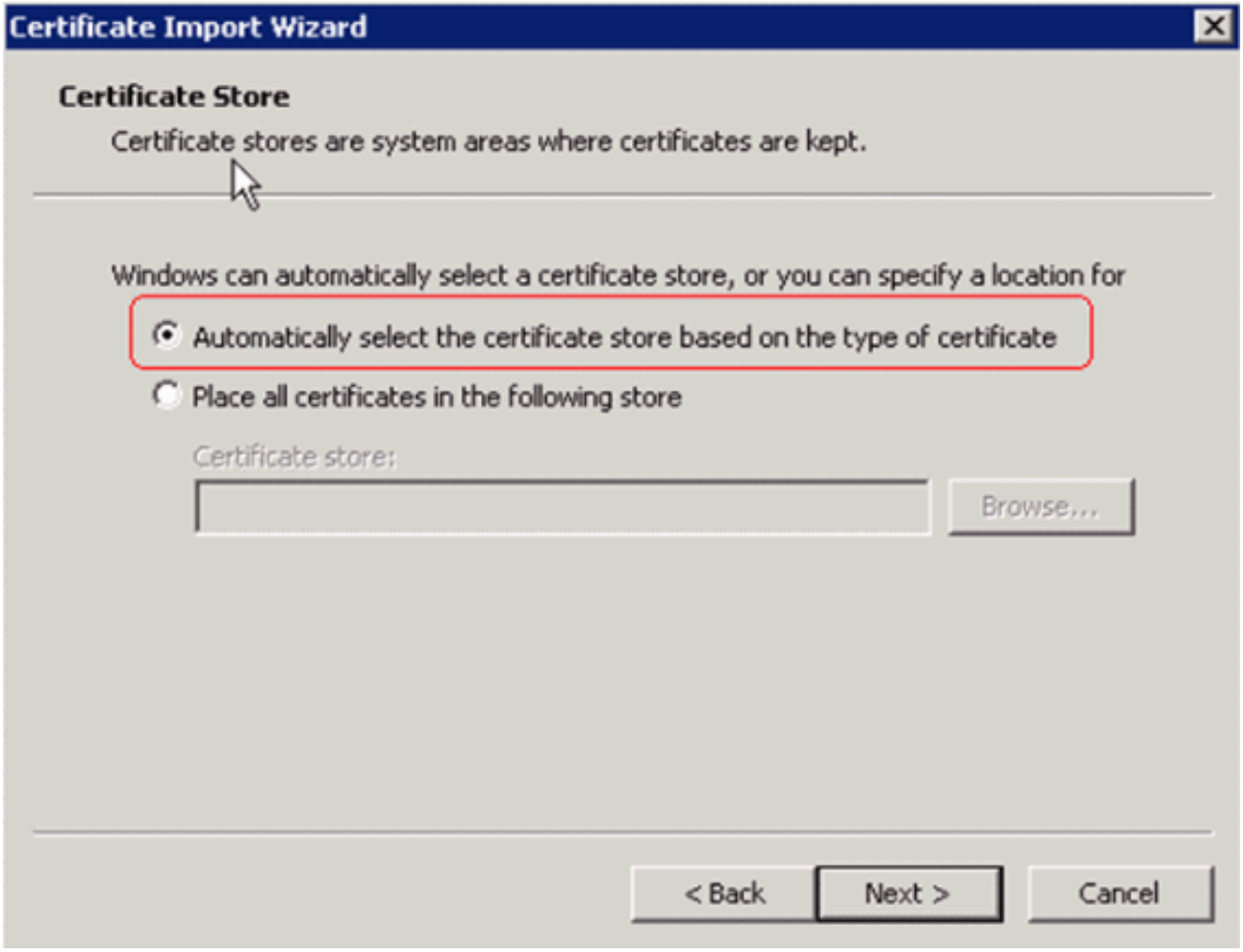
1. Utilice un explorador web en el cliente y señale el explorador al servidor de la Autoridad de certificación. Para hacerlo, ingrese **http://IP-address-of-Root-CA/certsrv**.
2. Inicie sesión con **Domain_Name\user_name**. Debe iniciar sesión utilizando el nombre de usuario de la persona que va a utilizar el cliente XP.
3. En la ventana de bienvenida, elija **Recuperar un certificado de CA** y haga clic en **Siguiente**.
4. Seleccione **Base64 Encoding** y **Download CA certificate**.
5. En la ventana Certificado emitido, haga clic en **Instalar este certificado** y haga clic en **Siguiente**.
6. Elija **Automáticamente seleccione el almacén de certificados** y haga clic en **Siguiente** para ver el mensaje de importación correcto.
7. Conéctese a la Autoridad de Certificación para recuperar el certificado de la Autoridad de Certificación:



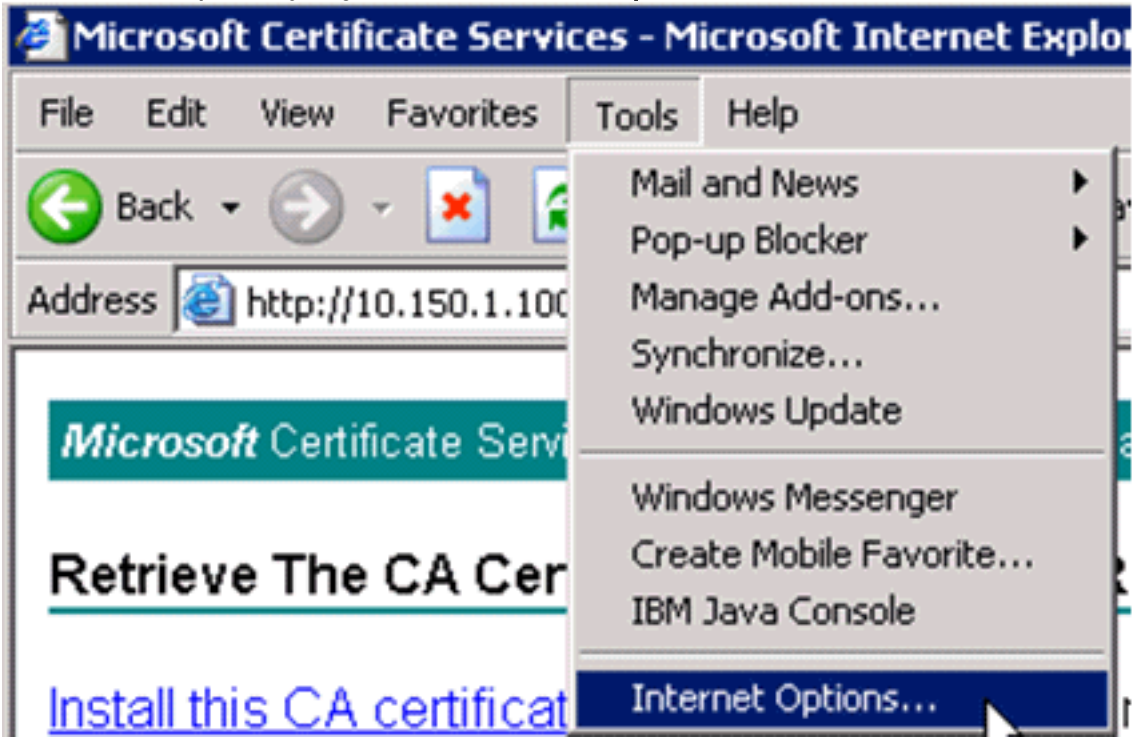
8. Haga clic en **Descargar certificado de CA**.

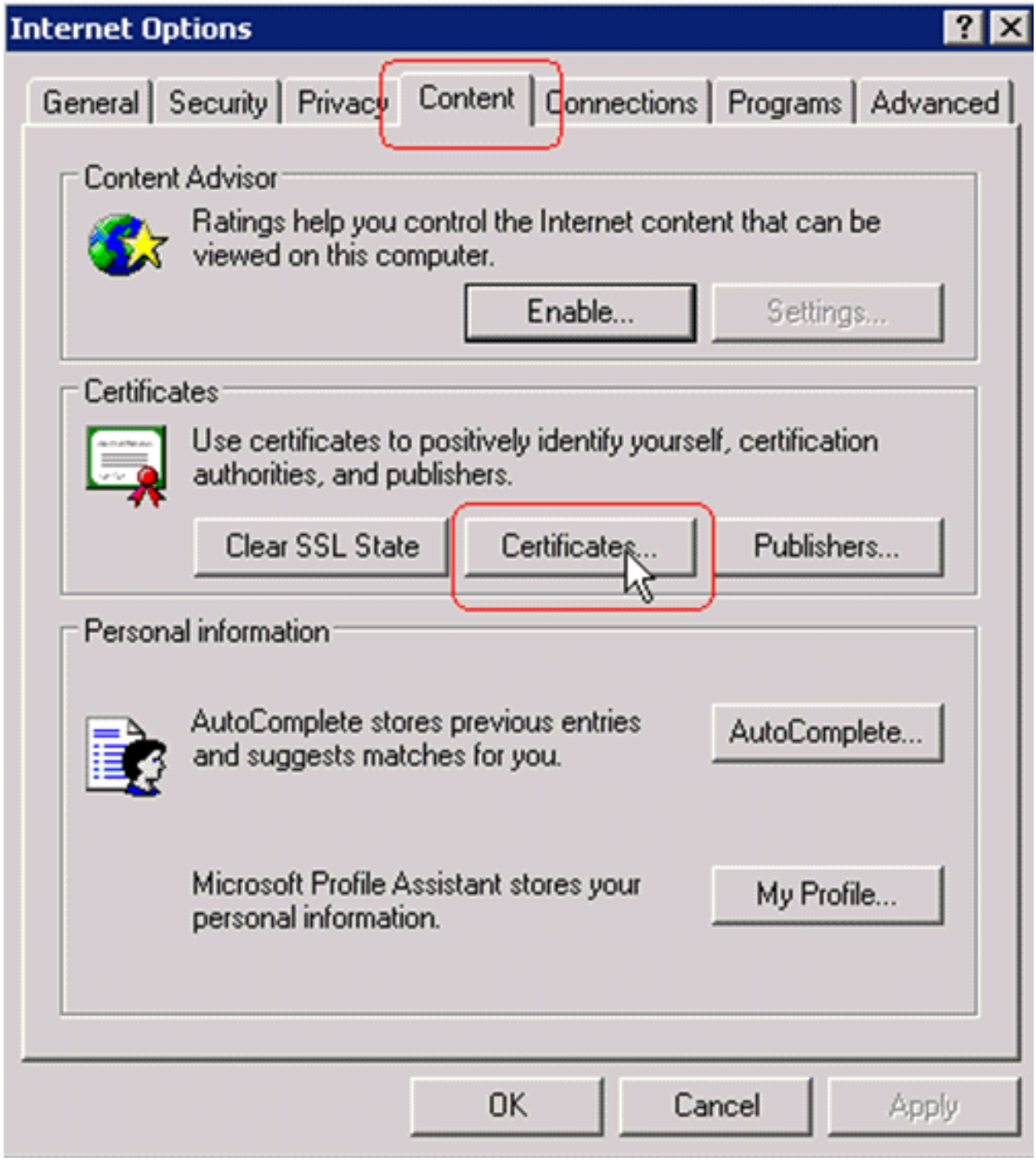



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

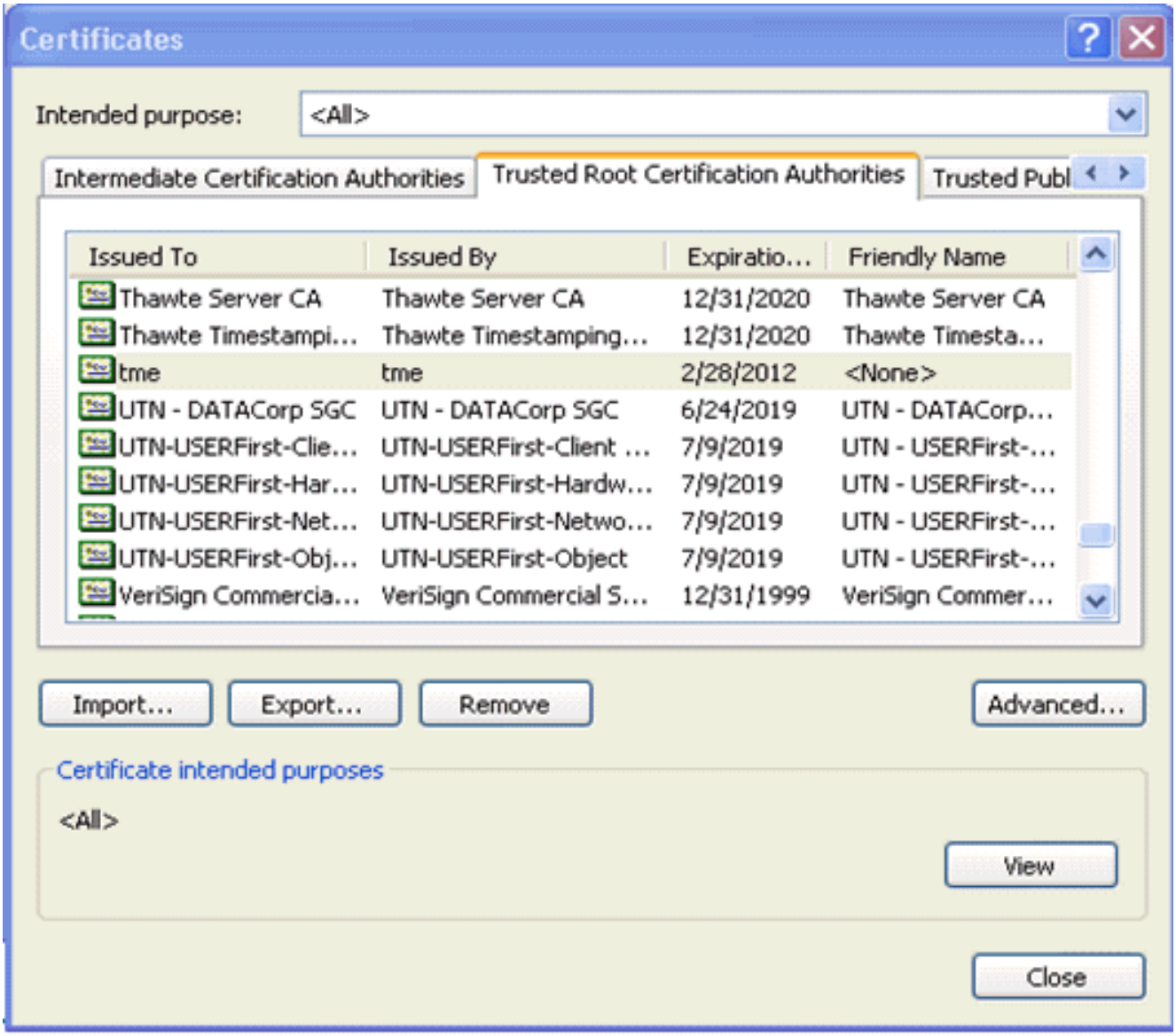

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

9. Para verificar que el certificado de la Autoridad de Certificación esté correctamente instalado, abra Internet Explorer y elija **Herramientas > Opciones de Internet > Contenido > Certificados**.





En Autoridad de certificación raíz de confianza, debe ver a su entidad de certificación recién instalada:



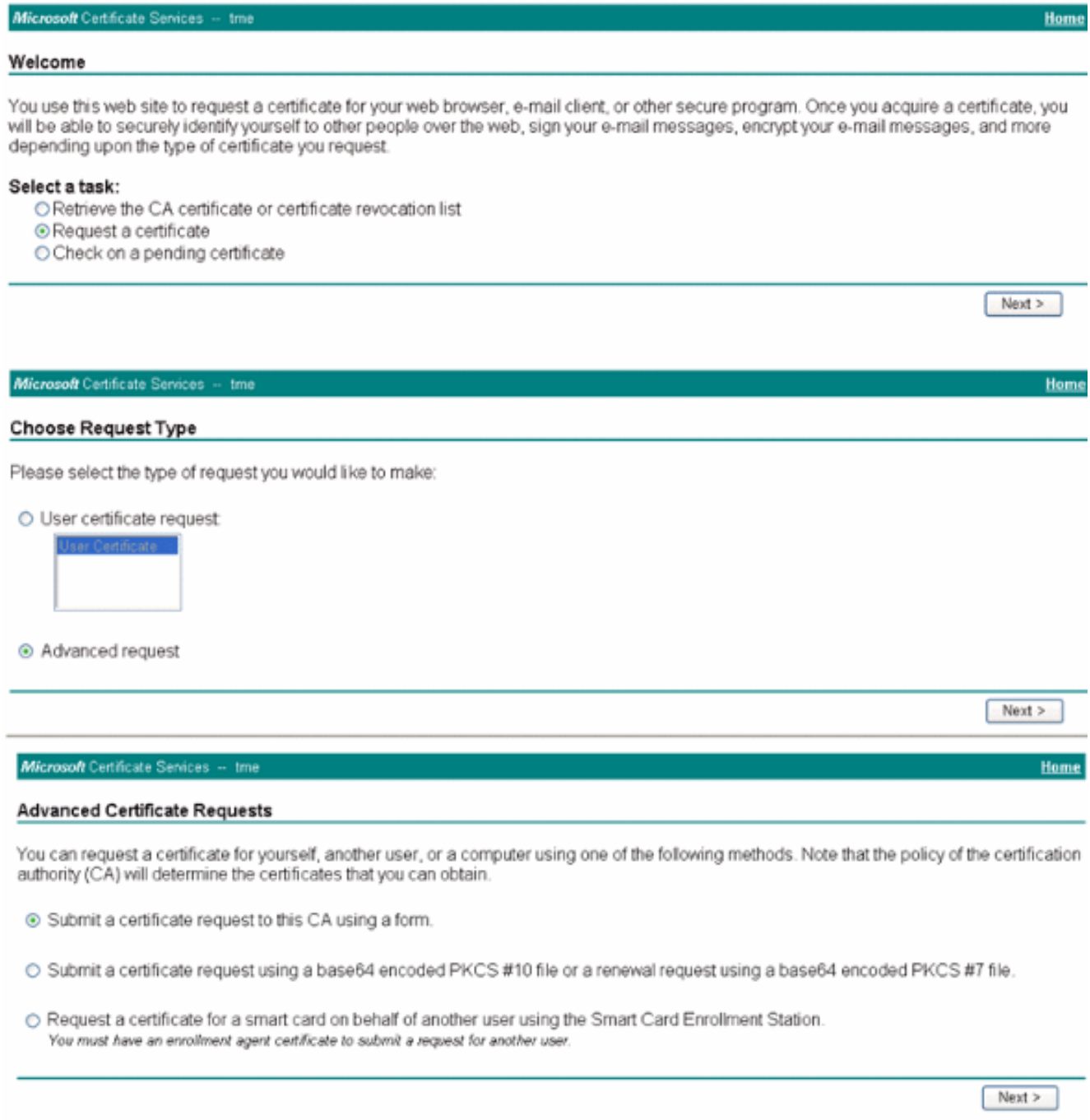
Generar un certificado de cliente para un dispositivo cliente

El cliente debe obtener un certificado de un servidor de la Autoridad de Certificación para que el WLC autentique un cliente WLAN EAP-TLS. Hay varios métodos que puede utilizar para obtener un certificado de cliente e instalarlo en el equipo de Windows XP. Para adquirir un certificado válido, el usuario de Windows XP debe iniciar sesión con su ID de usuario y debe tener una conexión de red (una conexión con cable o una conexión WLAN con seguridad 802.1x desactivada).

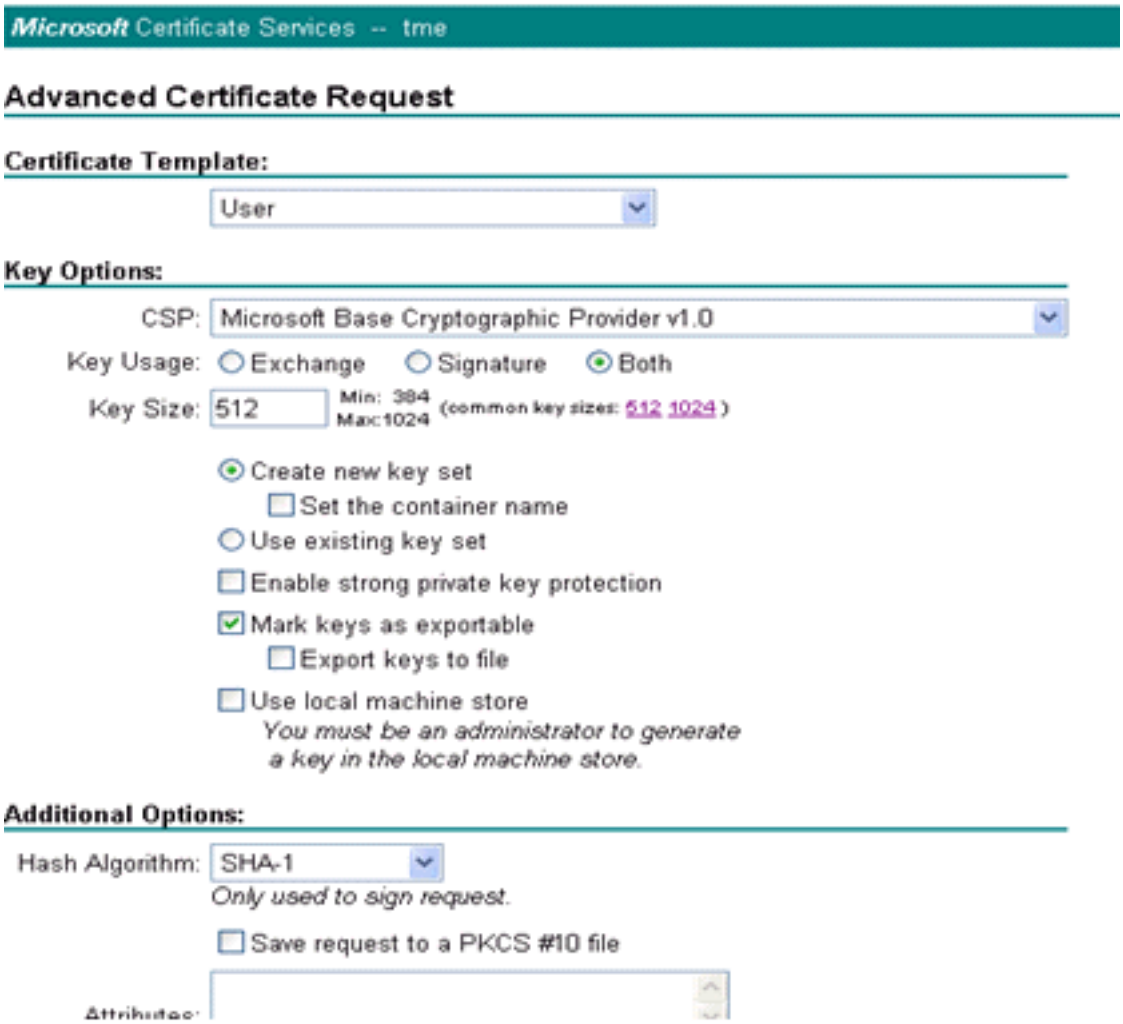
Se utiliza un explorador web en el cliente de Windows XP y una conexión por cable a la red para obtener un certificado de cliente del servidor de la autoridad de certificación raíz privada. Este procedimiento se utiliza para obtener el certificado de cliente de un servidor de Microsoft Certification Authority:

1. Utilice un explorador web en el cliente y señale el explorador al servidor de la Autoridad de certificación. Para hacerlo, ingrese **http://IP-address-of-Root-CA/certsrv**.
2. Inicie sesión con **Domain_Name\user_name**. Debe iniciar sesión utilizando el nombre de usuario de la persona que utiliza el cliente XP. (El nombre de usuario se incrusta en el certificado del cliente.)
3. En la ventana de bienvenida, elija **Solicitar un certificado** y haga clic en **Siguiente**.
4. Elija **Solicitud avanzada** y haga clic en **Siguiente**.

5. Elija **Submit a certificate request to this CA using a form** y haga clic en **Next**.
6. En el formulario de solicitud de certificado avanzado, elija la plantilla de certificado como **usuario**, especifique el tamaño de clave como **1024** y haga clic en **Enviar**.
7. En la ventana Certificado emitido, haga clic en **Instalar este certificado**. Esto da como resultado la instalación correcta de un certificado de cliente en el cliente de Windows XP.

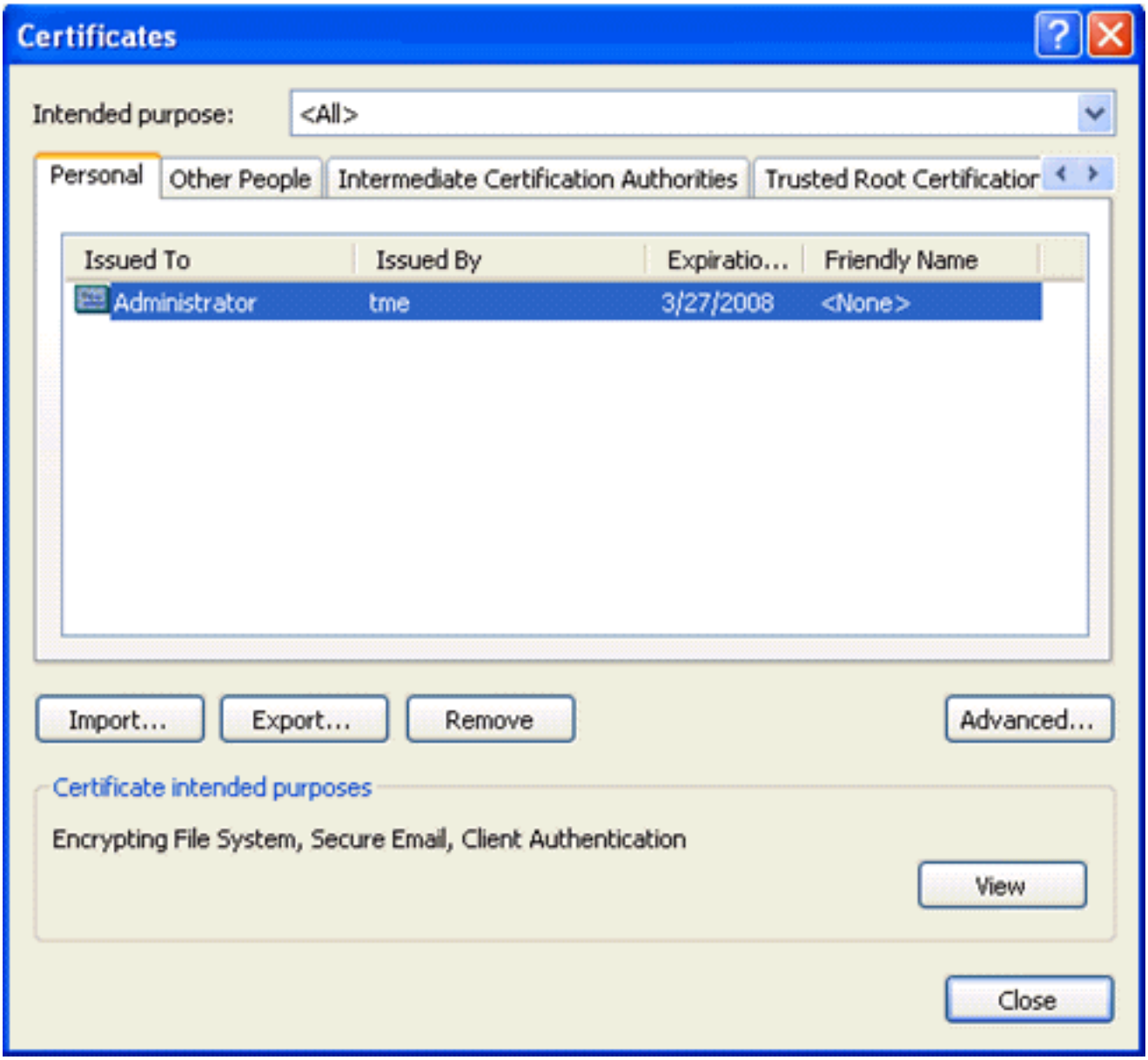


8. Seleccione **Certificado de autenticación de**



cliente. El certificado de cliente se ha creado.

9. Para verificar que el certificado está instalado, vaya a Internet Explorer y elija **Herramientas > Opciones de Internet > Contenido > Certificados**. En la ficha Personal, debe ver el certificado.

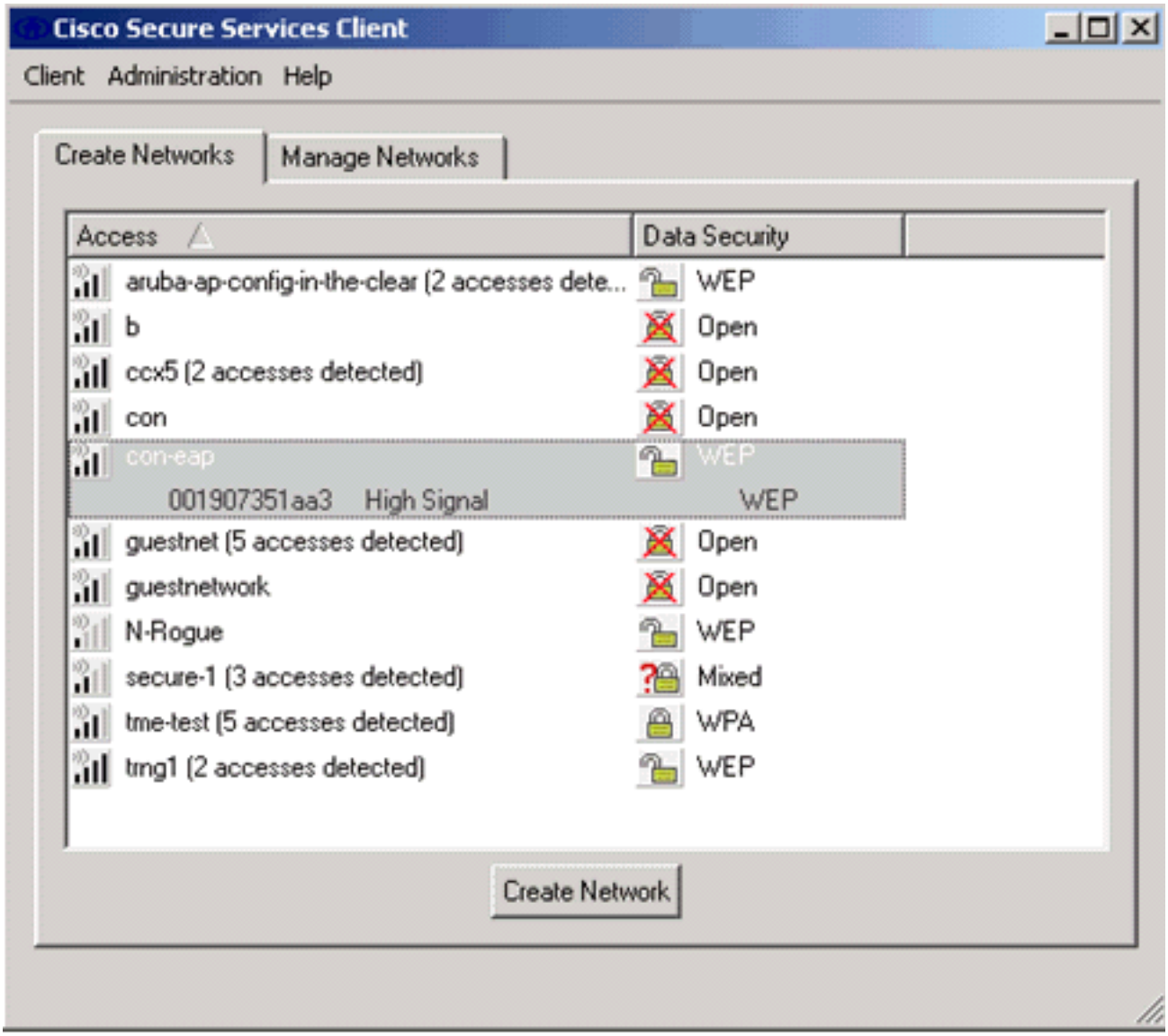


EAP-TLS con Cisco Secure Services Client en el dispositivo cliente

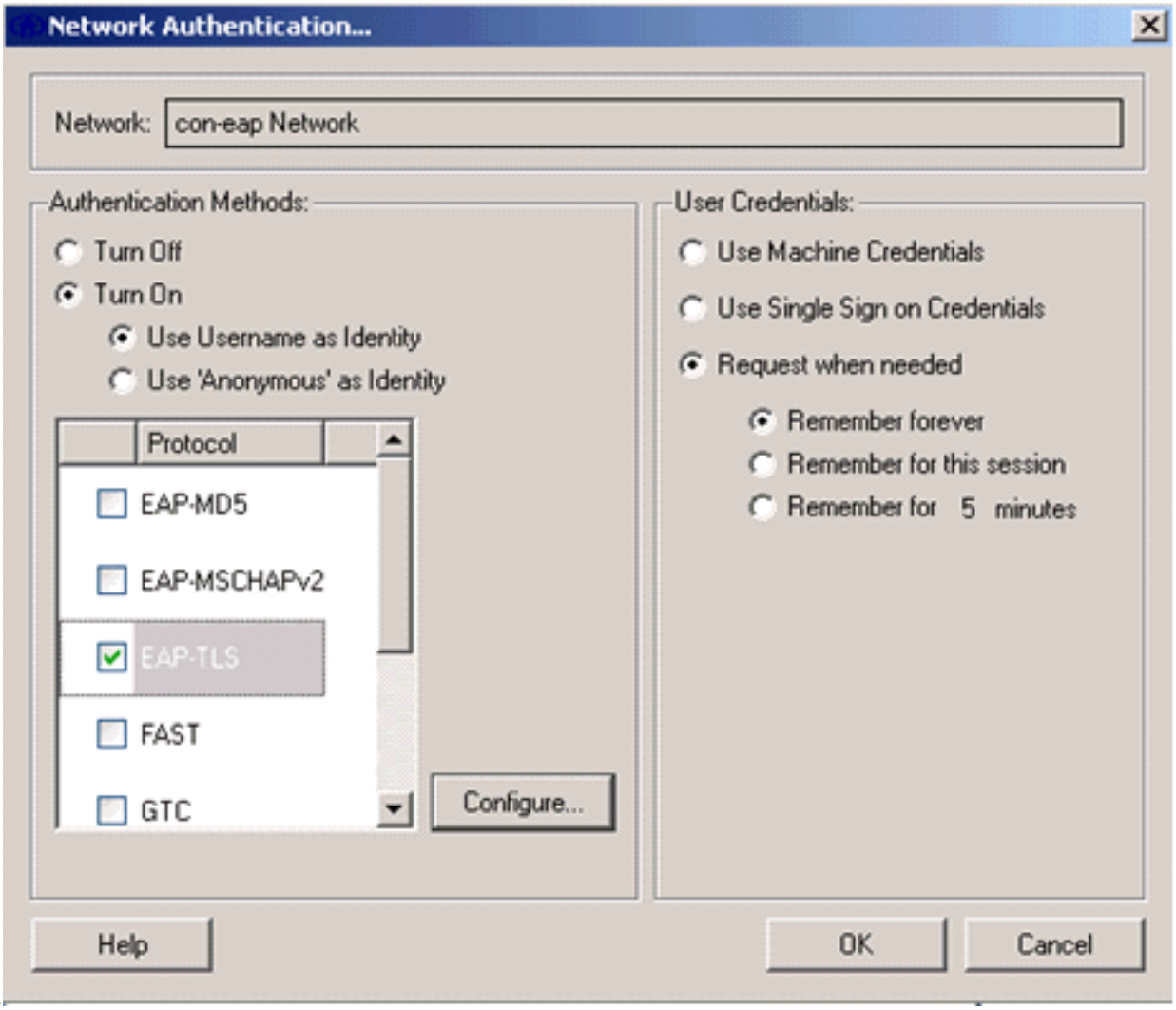
Complete estos pasos:

1. El WLC, de forma predeterminada, transmite el SSID, por lo que se muestra en la lista Crear Redes de SSID escaneados. Para crear un perfil de red, puede hacer clic en el SSID en la lista (Empresa) y hacer clic en **Crear red**.Si la infraestructura WLAN se configura con el SSID de broadcast inhabilitado, debe agregar manualmente el SSID. Para hacerlo, haga clic en **Agregar** en Dispositivos de acceso e introduzca manualmente el SSID adecuado (por ejemplo, Enterprise). Configure el comportamiento de la sonda activa para el cliente. Es decir, donde el cliente sondea activamente para su SSID configurado. Especifique **Búsqueda activa para este dispositivo de acceso** después de ingresar el SSID en la ventana Add Access Device .**Nota:** La configuración del puerto no permite modos empresariales (802.1X) si la configuración de autenticación EAP no se configura primero para el perfil.
2. Haga clic en **Crear red** para iniciar la ventana Perfil de red, que le permite asociar el SSID seleccionado (o configurado) con un mecanismo de autenticación. Asigne un nombre descriptivo al perfil.**Nota:** En este perfil de autenticación se pueden asociar varios tipos de

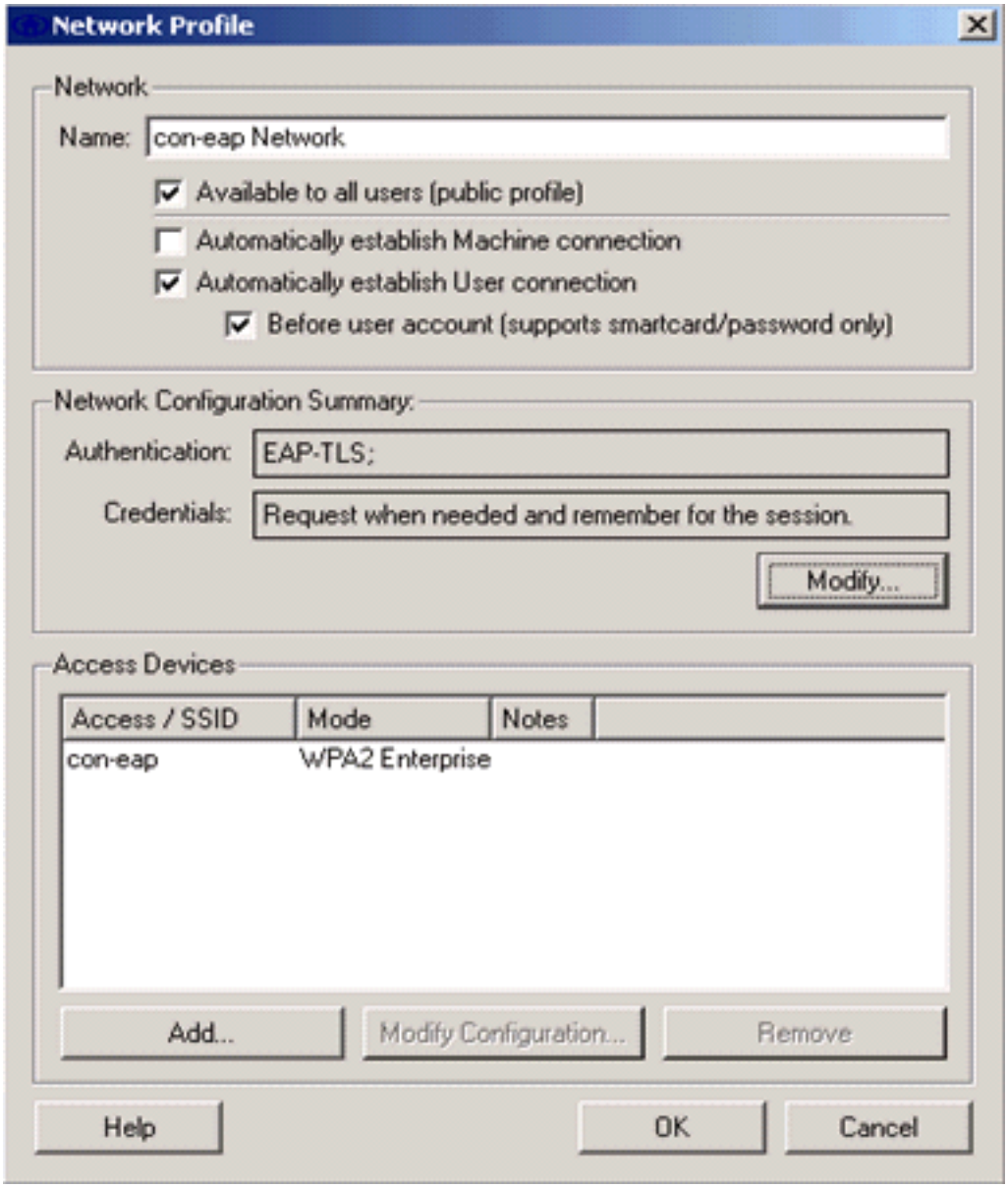
seguridad WLAN y/o
SSID.



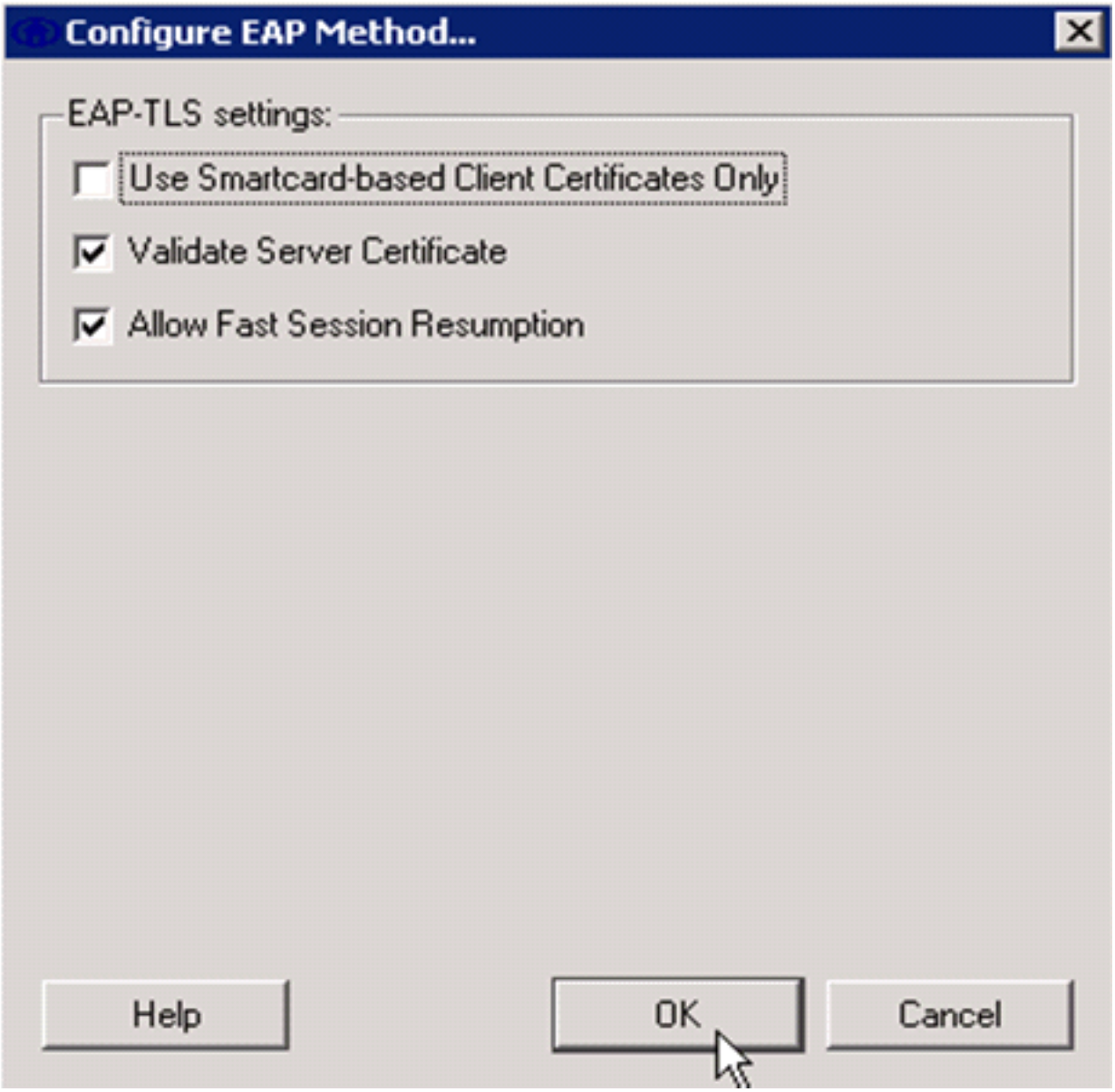
3. Active la autenticación y verifique el método EAP-TLS. A continuación, haga clic en **Configurar** para configurar las propiedades EAP-TLS.
4. En Resumen de configuración de red, haga clic en **Modificar** para configurar los parámetros EAP / credenciales.
5. Especifique **Activar autenticación**, elija **EAP-TLS** en Protocolo y elija **Nombre de usuario** como Identidad.
6. Especifique **Usar credenciales de inicio de sesión único** para utilizar las credenciales de inicio de sesión para la autenticación de red. Haga clic en **Configurar** para configurar los parámetros EAP-


Network Authentication...
Network:
con-eap Network
Authentication Methods:
Turn Off
Turn On
Use Username as Identity
Use 'Anonymous' as Identity
Protocol
EAP-MD5
EAP-MSCHAPv2
EAP-TLS
FAST
GTC
Configure...
User Credentials:
Use Machine Credentials
Use Single Sign on Credentials
Request when needed
Remember forever
Remember for this session
Remember for 5 minutes
Help
OK
Cancel

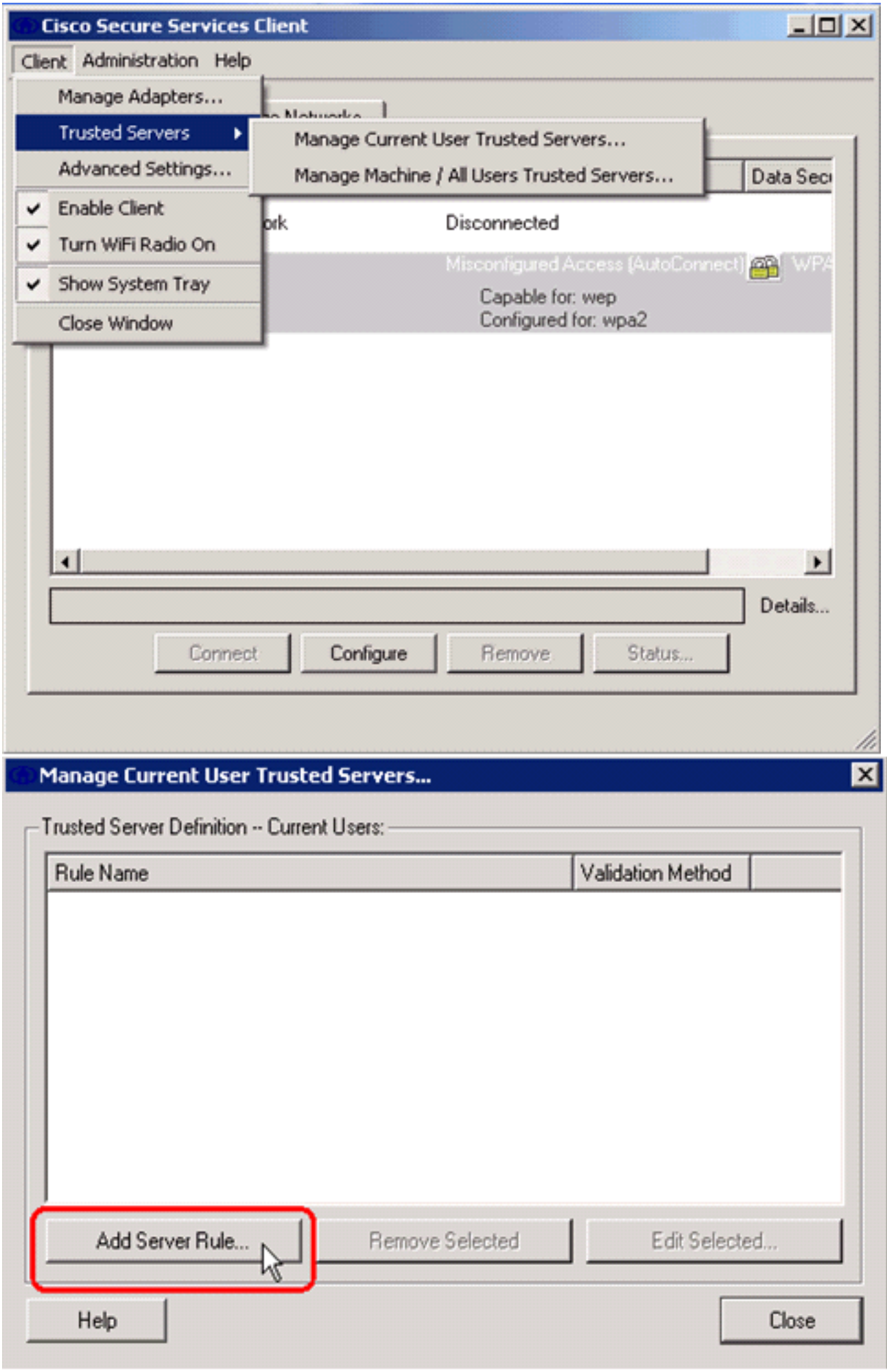
TLS.



7. Para tener una configuración EAP-TLS segura, debe verificar el certificado del servidor RADIUS. Para hacer esto, marque **Validar certificado de servidor**.

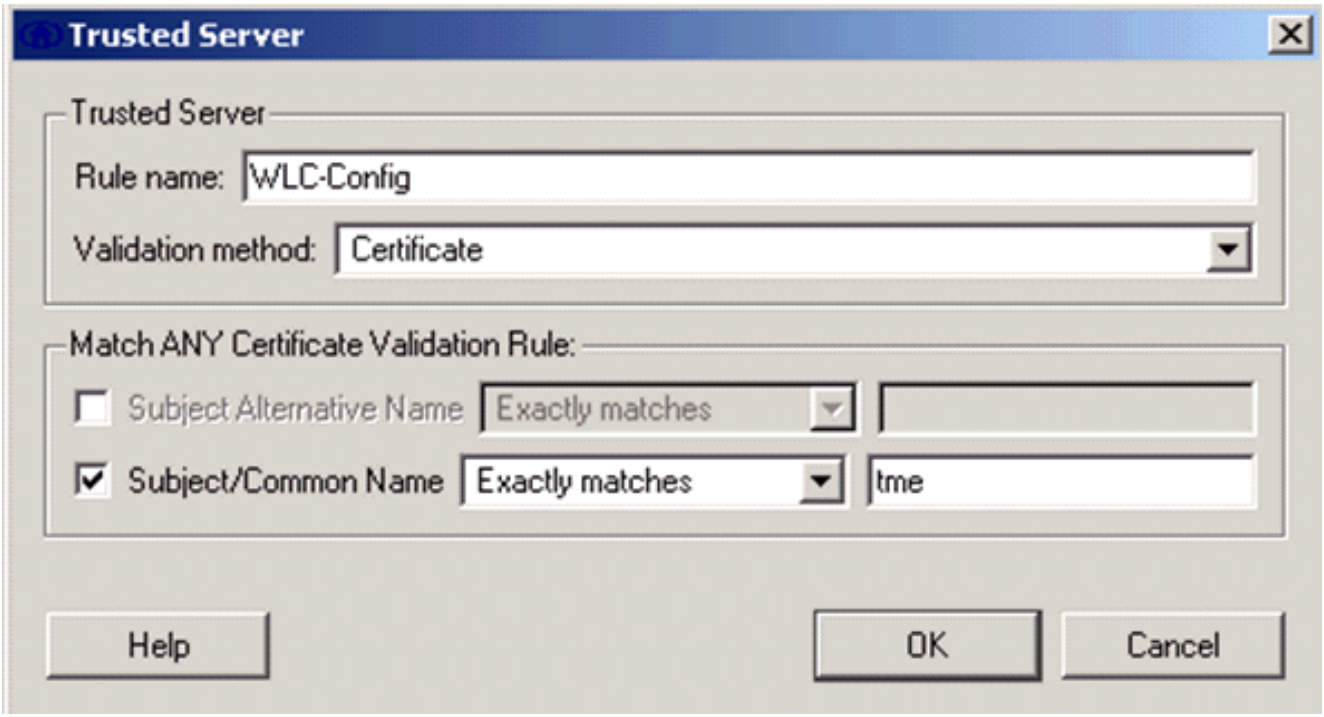


8. Para validar el certificado del servidor RADIUS, debe proporcionar información de Cisco Secure Services Client para aceptar solamente el certificado correcto. Elija **Client > Trusted Servers > Manage Current User Trusted Servers**.



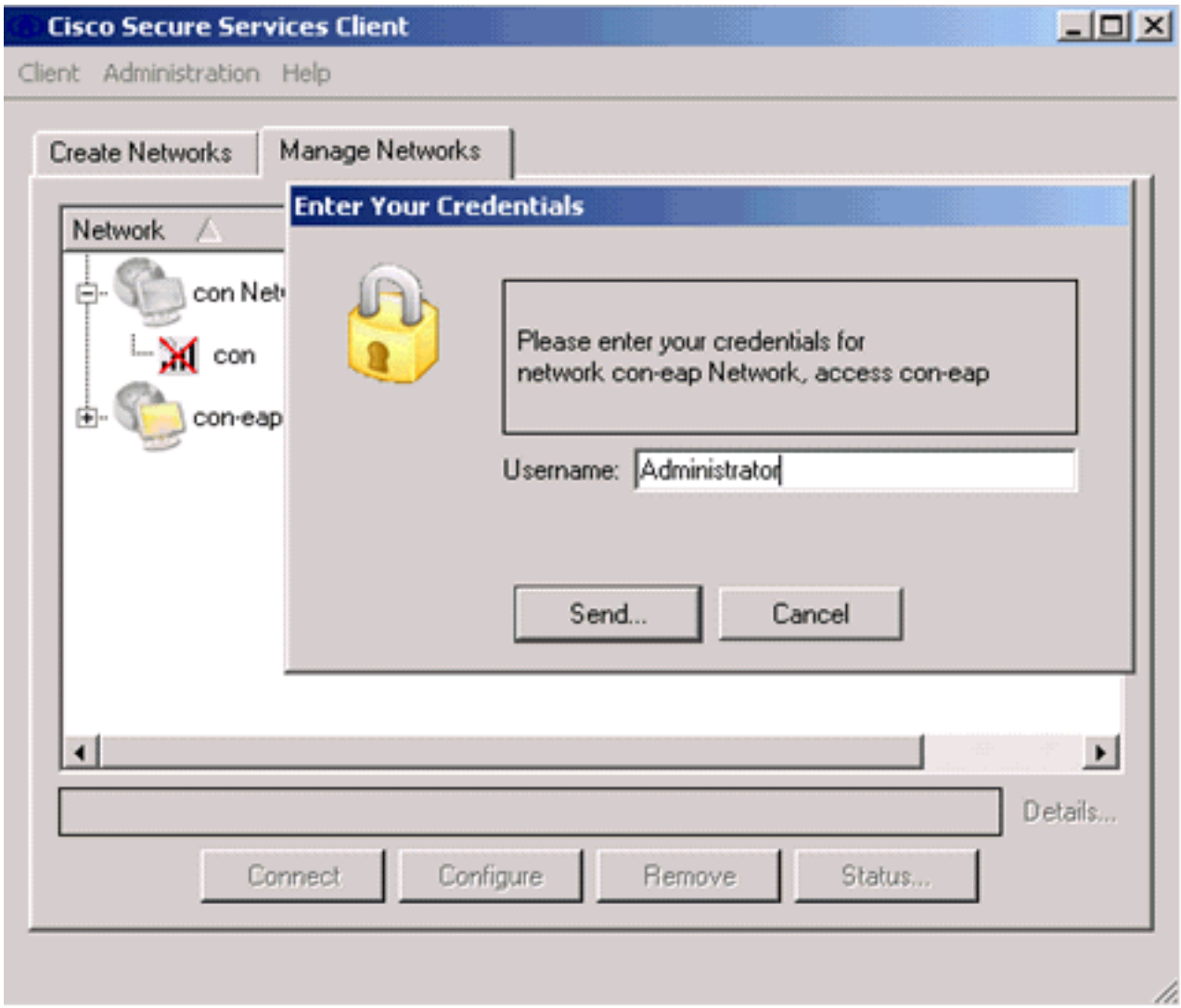
9. Asigne un nombre a la regla y verifique el nombre del certificado del

servidor.



La configuración EAP-TLS ha finalizado.

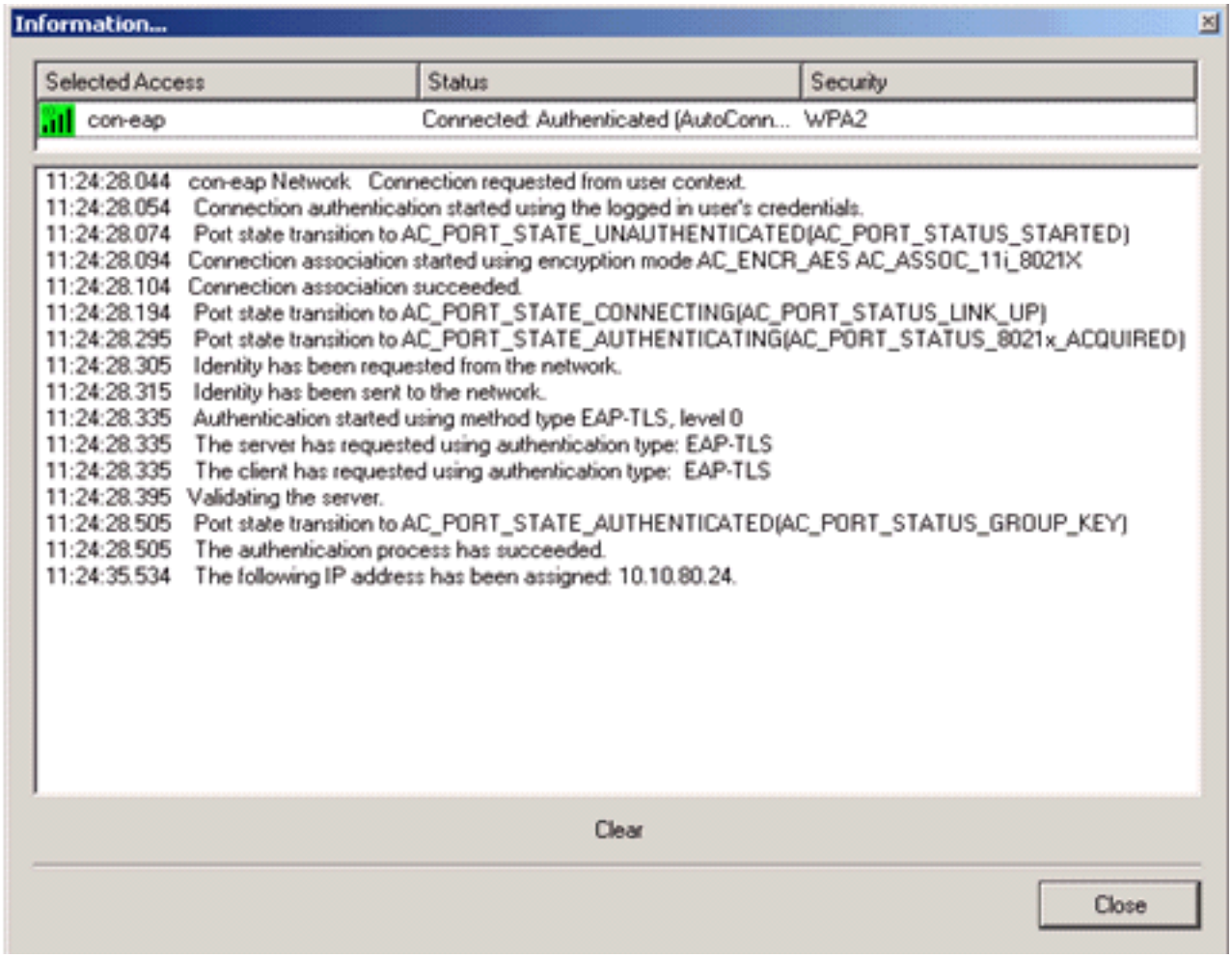
10. Conéctese al perfil de red inalámbrica. Cisco Secure Services Client solicita el inicio de sesión del
usuario:

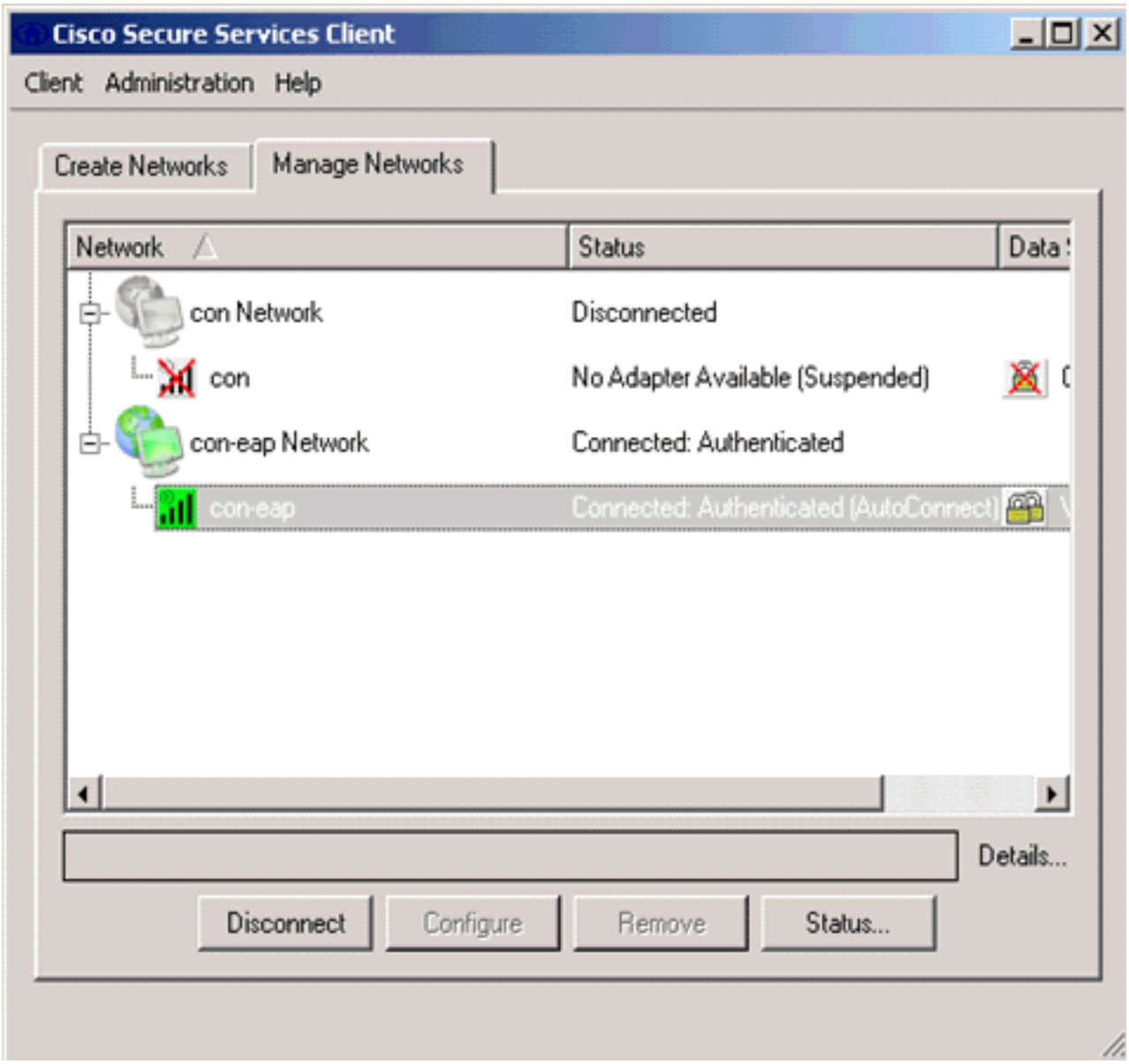


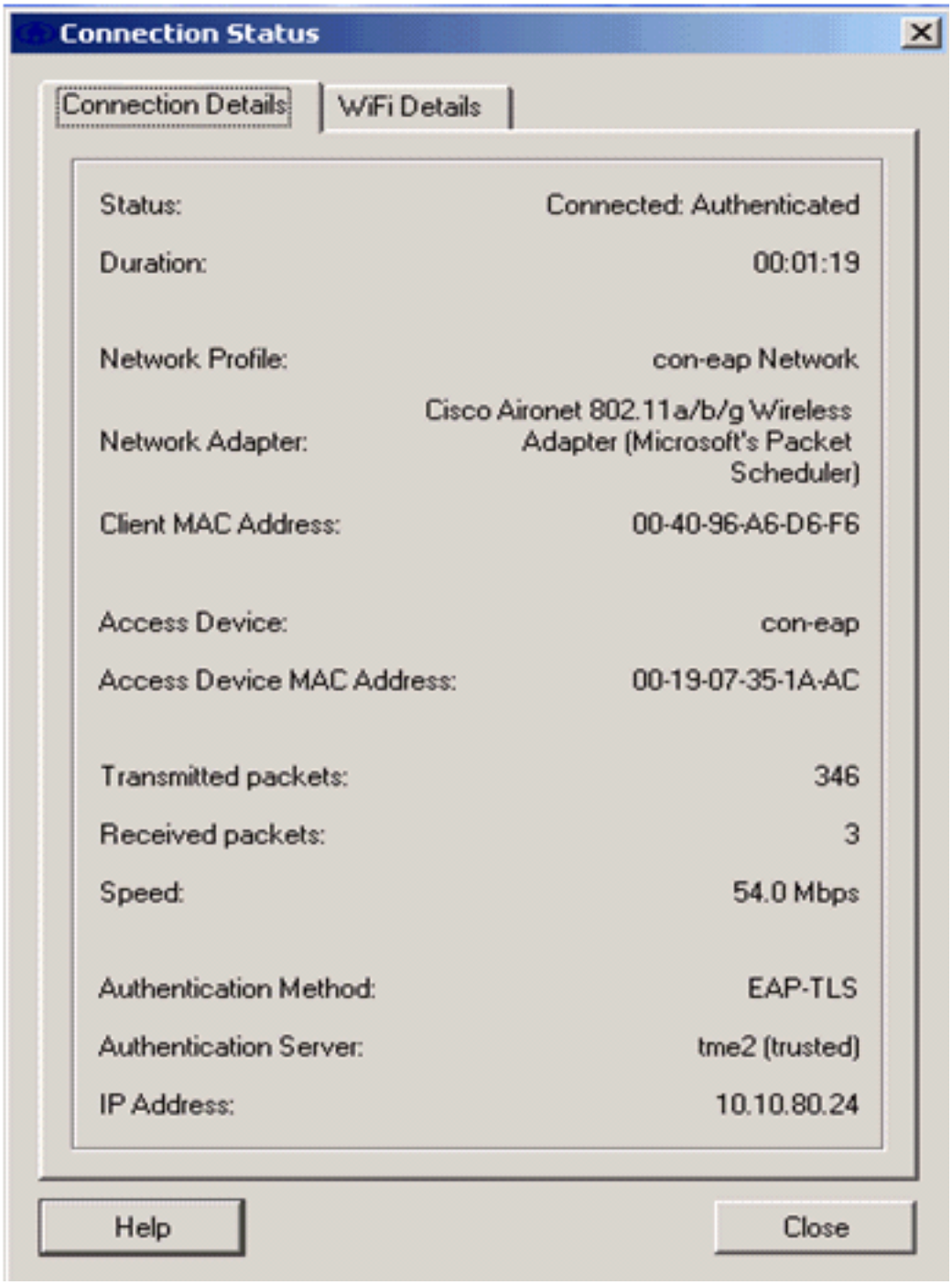
Ci

sco Secure Services Client recibe el certificado del servidor y lo verifica (con la regla configurada y la Autoridad de certificación instalada). A continuación, solicita que el certificado se utilice para el usuario.

11. Después de que el cliente se autentique, elija **SSID** en el Perfil en la pestaña Administrar redes y haga clic en **Estado** para consultar los detalles de la conexión.La ventana Detalles de la conexión proporciona información sobre el dispositivo cliente, el estado y las estadísticas de la conexión, y el método de autenticación. La ficha Detalles de WiFi proporciona detalles sobre el estado de la conexión 802.11, que incluye el canal RSSI, 802.11 y la autenticación/cifrado.




Cisco Secure Services Client
Client
Administration
Help
Create Networks
Manage Networks
Network
Status
Data
con Network
Disconnected
con
No Adapter Available (Suspended)
con-eap Network
Connected: Authenticated
con-eap
Connected: Authenticated (AutoConnect)
Details...
Disconnect
Configure
Remove
Status...



Comandos de Debug

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.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Estos comandos debug se pueden emplear en el WLC para monitorear el progreso del intercambio de autenticación:

- **debug aaa events enable**
- **debug aaa detail enable**
- **debug dot1x events enable**

- debug dot1x state enable
- debug aaa local-auth eap events enableO
- debug aaa all enable

Información Relacionada

- Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, versión 4.1
- Soporte de la Tecnología de la WLAN
- Soporte Técnico y Documentación - Cisco Systems