Ejemplo de configuración del servidor local unificado de la red inalámbrica EAP

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 los usuarios y a los clientes de red inalámbrica que se autenticarán localmente. Se diseña para el uso en las oficinas remotas que quieren mantener la Conectividad a los clientes de red inalámbrica cuando el sistema final se interrumpe o va el servidor externo de la autenticación abajo. Cuando usted activa EAP local, el regulador sirve como el servidor de la autenticación y la base de datos de usuarios locales, de tal modo quitando la dependencia de un servidor externo de la autenticación. EAP local extrae los credenciales de usuario de la base de datos de usuarios locales o de la base de datos del back-end del Lightweight Directory Access Protocol (LDAP) para autenticar a los usuarios. EAP local utiliza EAP ligero (SALTO), la autenticación adaptable de EAP vía el Tunelización seguro (EAP-FAST), y la autenticación de la Seguridad de la capa del EAP-transporte (EAP-TLS) entre el regulador y los clientes de red inalámbrica.

Observe que el servidor local EAP no está disponible si hay una configuración de servidor de RADIUS externa global en el WLC. Todas las peticiones de la autenticación se remiten al externo global RADIUS hasta que el servidor local EAP esté disponible. Si el WLC suelta la Conectividad al servidor de RADIUS externo, después el servidor local EAP llega a ser activo. Si no hay configuración de servidor de RADIUS global, el servidor local EAP llega a ser inmediatamente activo. El servidor local EAP no se puede utilizar para autenticar a los clientes, que están conectados con el otro WLCs. Es decir un WLC no puede remitir su petición EAP a otro WLC para la autenticación. Cada WLC debe tener su propio servidor local EAP y base de datos individual.

Note: Utilice estos comandos para parar WLC de enviar las peticiones a un servidor de RADIUS externo.

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

Los soportes de servidor locales EAP estos protocolos en la versión de software de 4.1.171.0 y más adelante:

- SALTO
- EAP-FAST (ambo username/contraseña, y Certificados)
- EAP-TLS

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar WLCs y los Puntos de acceso ligeros (revestimientos) para la operación básica
- Conocimiento de los métodos ligeros del protocolo (LWAPP) y de la seguridad de red inalámbrica del Punto de acceso
- Conocimiento básico de la autenticación local EAP.

Componentes usados

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

- Windows XP con la versión 4.05 del indicador luminoso LED amarillo de la placa muestra gravedad menor y del Cisco Secure Services Client del adaptador CB21AG
- Regulador 4.1.171.0 LAN de la Tecnología inalámbrica de Cisco 4400
- Autoridades de certificación de Microsoft encendido Windows 2000 Server

Convenciones

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

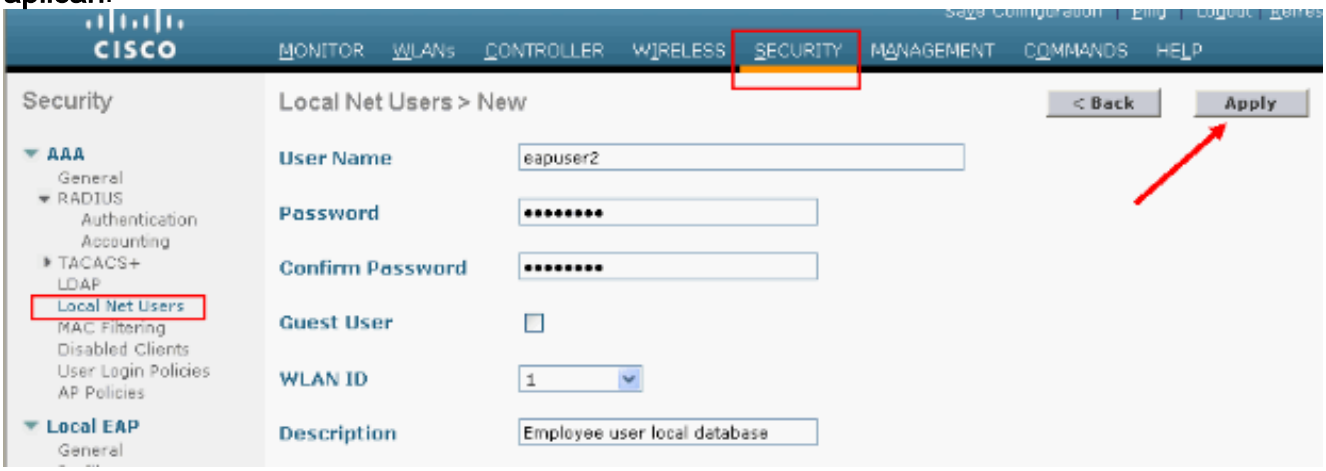
Configure EAP local en el regulador inalámbrico LAN de Cisco

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

Configuración local EAP

Complete estos pasos para configurar EAP local:

1. Agregue a un usuario neto local:Del GUI. elija la **Seguridad > los usuarios netos locales > nuevo**, ingrese el Nombre de usuario, contraseña, Usuario invitado, identificación WLAN, y la descripción y el tecleo **se aplican**.



Del CLI usted puede utilizar el **netuser de los config agrega el** comando del *<description> del id> del <password> <WLAN del <username>*:**Note**: Este comando se ha derribado a una segunda línea debido a las razones espaciales.

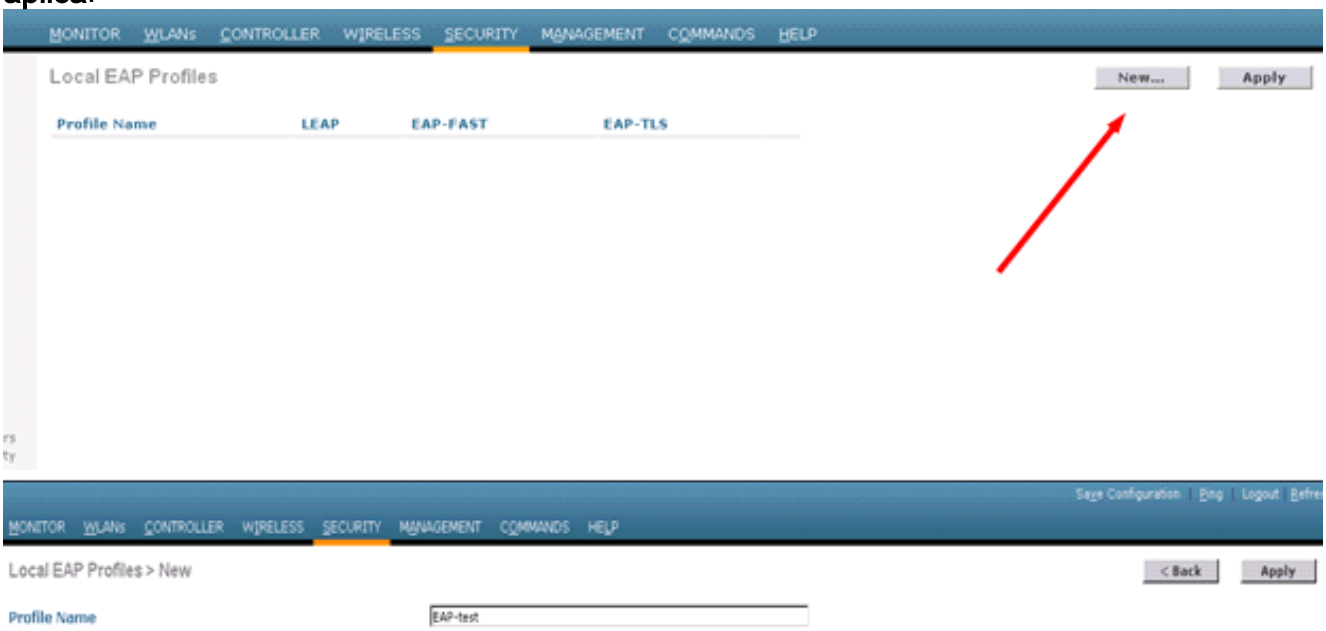
```
(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
```

2. Especifique la orden de extracción del credencial de usuario.Del GUI, elija la **Seguridad > local EAP > prioridad de la autenticación**. Entonces seleccione el LDAP, hacen clic "**<**" el botón y el tecleo **se aplica**. Esto pone los credenciales de usuario en la base de datos local primero.

Del CLI:

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

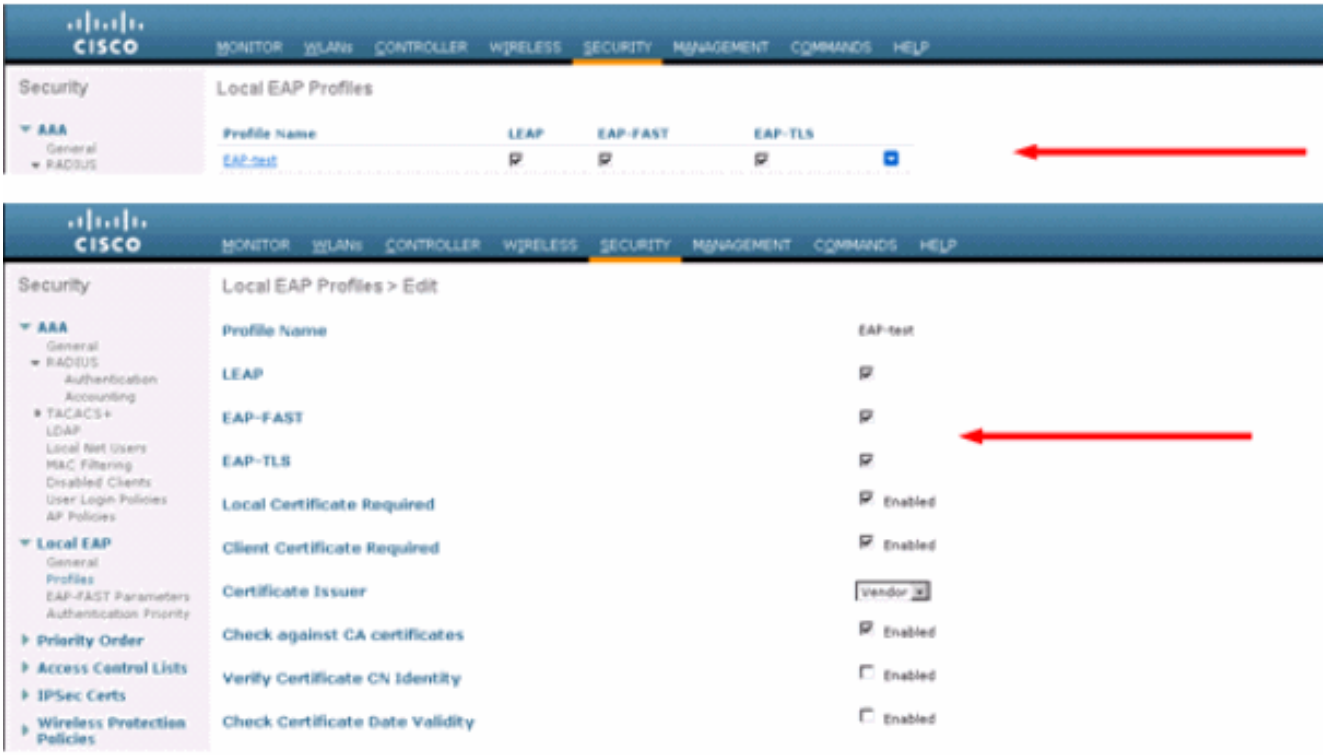
3. Agregue un perfil EAP:Para hacer esto del GUI, elija la **Seguridad > local EAP > los perfiles** y haga clic **nuevo**. Cuando aparece la nueva ventana, pulse el nombre del perfil y el tecleo **se aplica**.



Usted puede también hacer esto usando los **config del** comando CLI que el eap-**perfil local-auth agrega el *<profile-name>*.** En nuestro ejemplo, el nombre del perfil es EAP-*prueba*.

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

4. Agregue un método al perfil EAP.Del GUI elija la **Seguridad > local EAP > los perfiles** y haga clic en el nombre del perfil para el cual usted quiere agregar los métodos de autenticación. Este ejemplo utiliza el SALTO, el EAP-FAST, y el EAP-TLS. El tecleo **se aplica** para fijar los métodos.

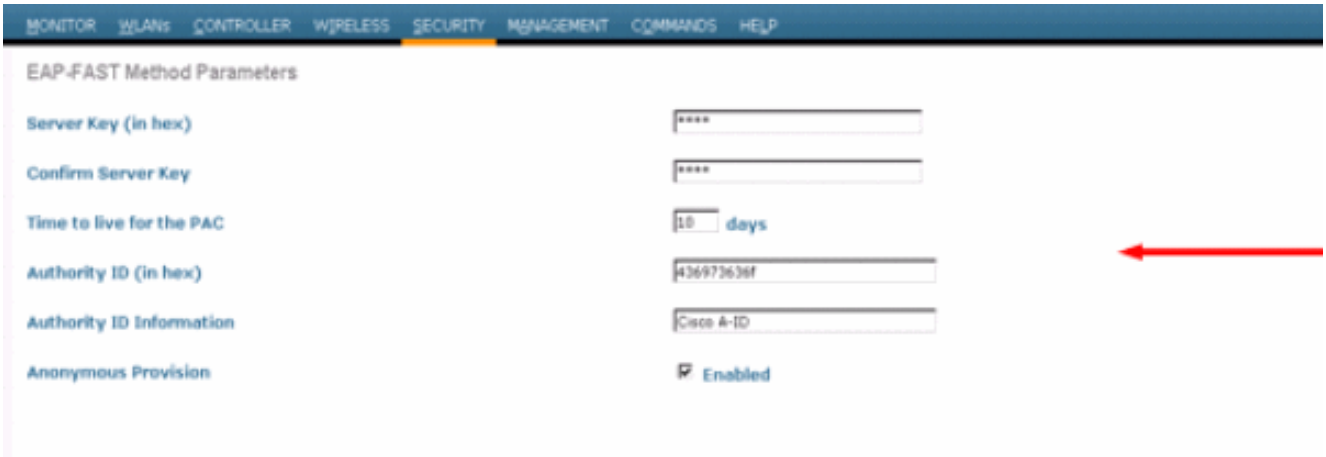


Usted puede también utilizar los **config del** comando CLI que el **método local-auth del eap-**

perfil agrega el ***<profile-name> del <method-name>***. En nuestro ejemplo de configuración agregamos tres métodos a la EAP-prueba del perfil. Los métodos son el SALTO, el EAP-FAST, y el EAP-TLS cuyos nombres del método son salto*, *rápido,* y *tls* respectivamente. Esta salida 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
```

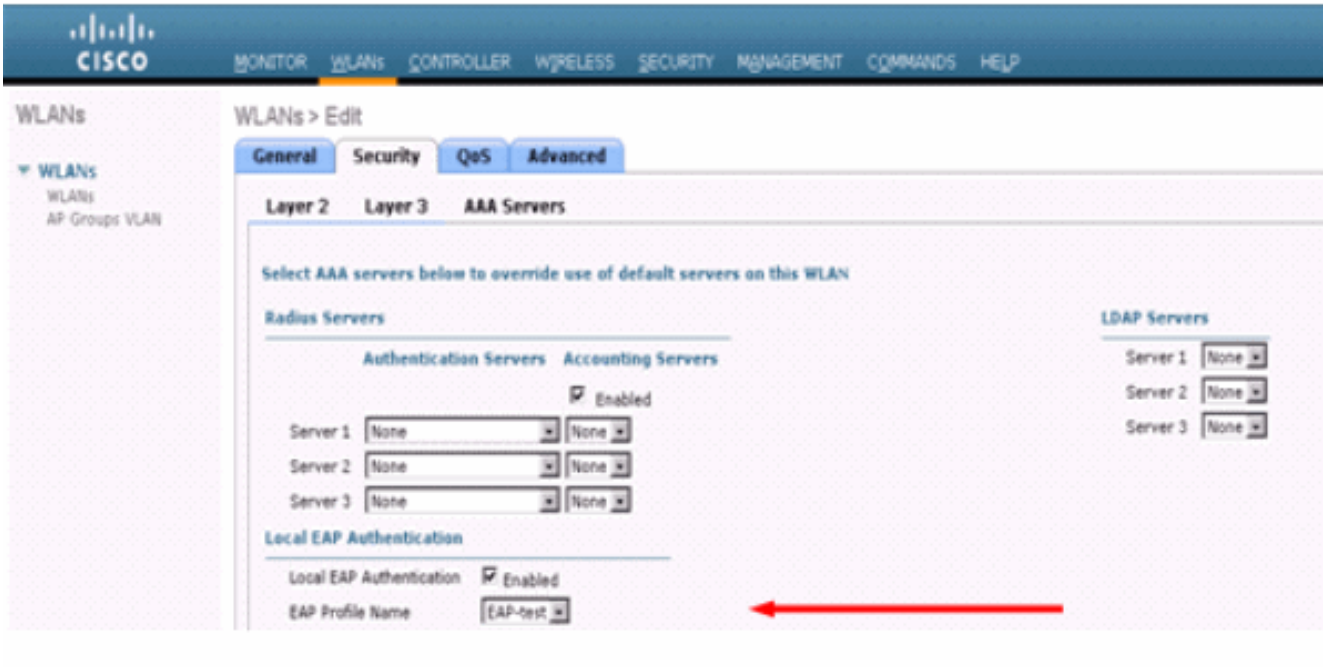
5. Configure los parámetros del método EAP. Esto se utiliza solamente para el EAP-FAST. Los parámetros que se configurarán son:**Clave del servidor (clave del servidor)** — Cifrar/de la clave del servidor credenciales protegidas decrypt del acceso (PACs) (en el hexadecimal).**Time to Live para PAC (pac-TTL)** — Fija el Time to Live para el PAC.**Identificación de la autoridad (autoridad-identificación)** — Fija el identificador de la autoridad.**Disposición de Annonymous (anon-provn)** — Configura si la disposición anónima está permitida. Esto se activa como opción predeterminada.Para la configuración a través del GUI, elija la **Seguridad > local los parámetros EAP > del EAP-FAST** y ingrese la clave del servidor, el Time to Live para el PAC, la identificación de la autoridad (en el maleficio), y los valores de información ID de la autoridad.



Éstos son los comandos de configuración CLI de utilizar para fijar estos parámetros para el 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
```

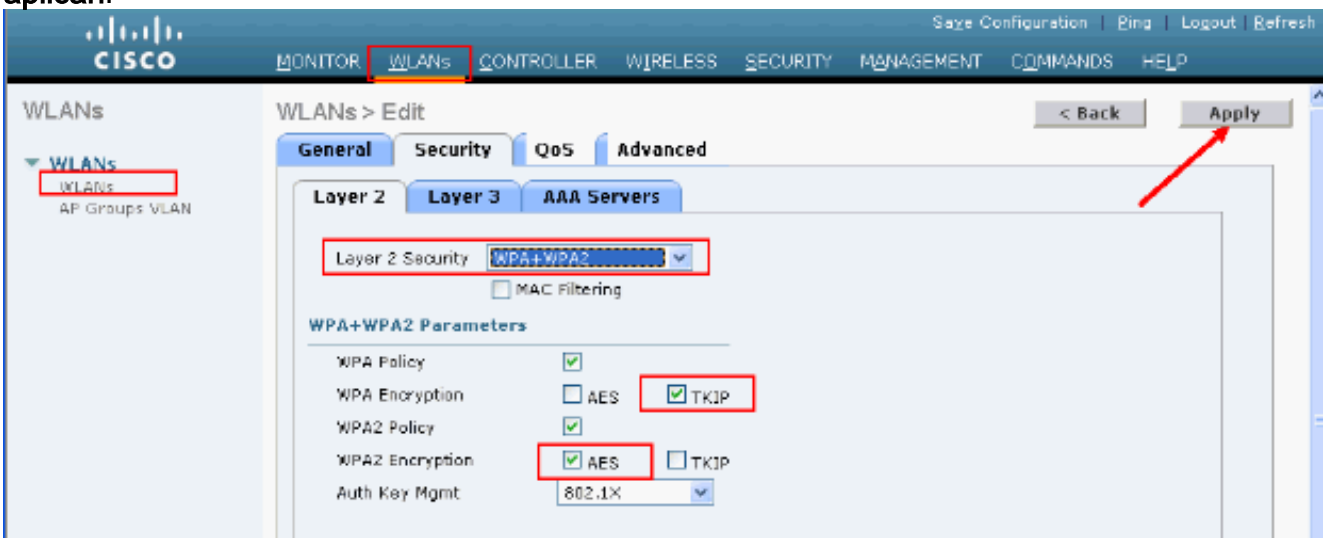
6. Autenticación local del permiso por la red inalámbrica (WLAN):Del GUI elija las **redes inalámbricas (WLAN)** en el menú superior y seleccione la red inalámbrica (WLAN) para la cual usted quiere configurar la autenticación local. Una nueva ventana aparece. Haga clic las tabulaciones de la **Seguridad >AAA**. Controle la **autenticación local EAP** y seleccione el nombre del perfil correcto EAP del menú desplegable como este ejemplo muestra:



Usted puede también publicar el comando configuration **local-auth wlan del *<wlan-id> del <profile-name> del* permiso de los config** CLI como se muestra aquí:

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

7. Fije los parámetros de Seguridad de la capa 2.Del interfaz GUI, en la red inalámbrica (WLAN) corrija la ventana van a las tabulaciones de la **Seguridad > de la capa 2** y eligió **WPA+WPA2 del** menú desplegable de la Seguridad de la capa 2. Bajo parámetros WPA+WPA2 seccione, fije el cifrado WPA **TKIP** y WPA2 al cifrado **AES**. Entonces haga clic **se aplican**.



Del 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:
```

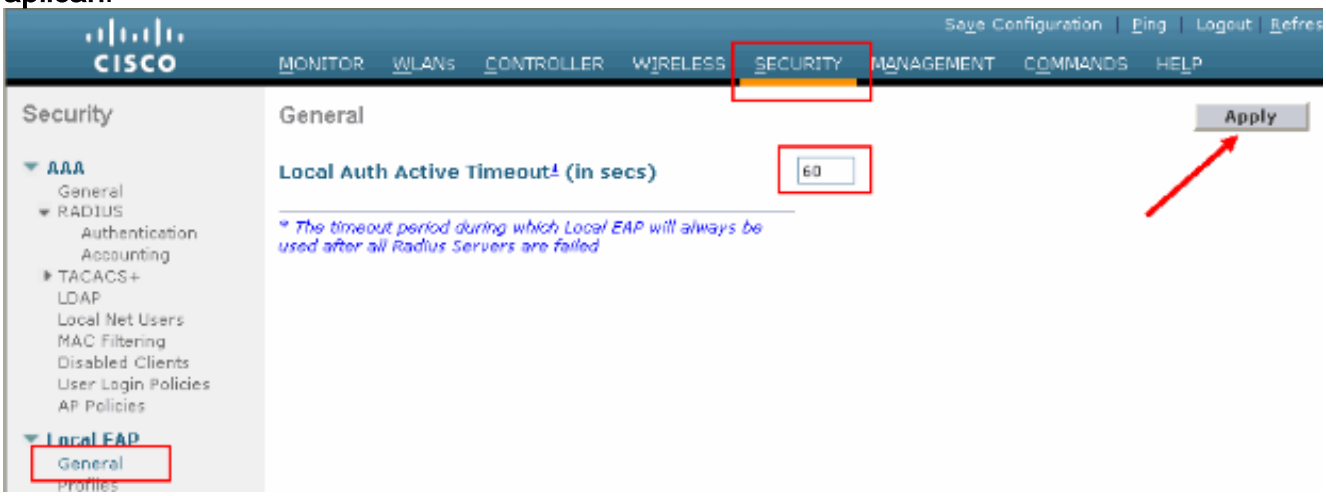
```
    Name ..................................... EAP-test
      Certificate issuer ..................... cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity ......... Disabled
        Check certificate date validity ......... 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
```

Usted puede ver los parámetros específicos de 1 wlan con el comando *<wlan **wlan del** id> de la **demostración***:

```
(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 la autenticación local que pueden ser configurados, particularmente el temporizador activo del descanso. Este temporizador configura el período durante el cual EAP local es después de todo servidores de RADIUS usados ha fallado.Del GUI, elija la **Seguridad > local EAP > general** y determinado el valor del tiempo. Entonces haga clic **se aplican**.



Del CLI, publique estos comandos:

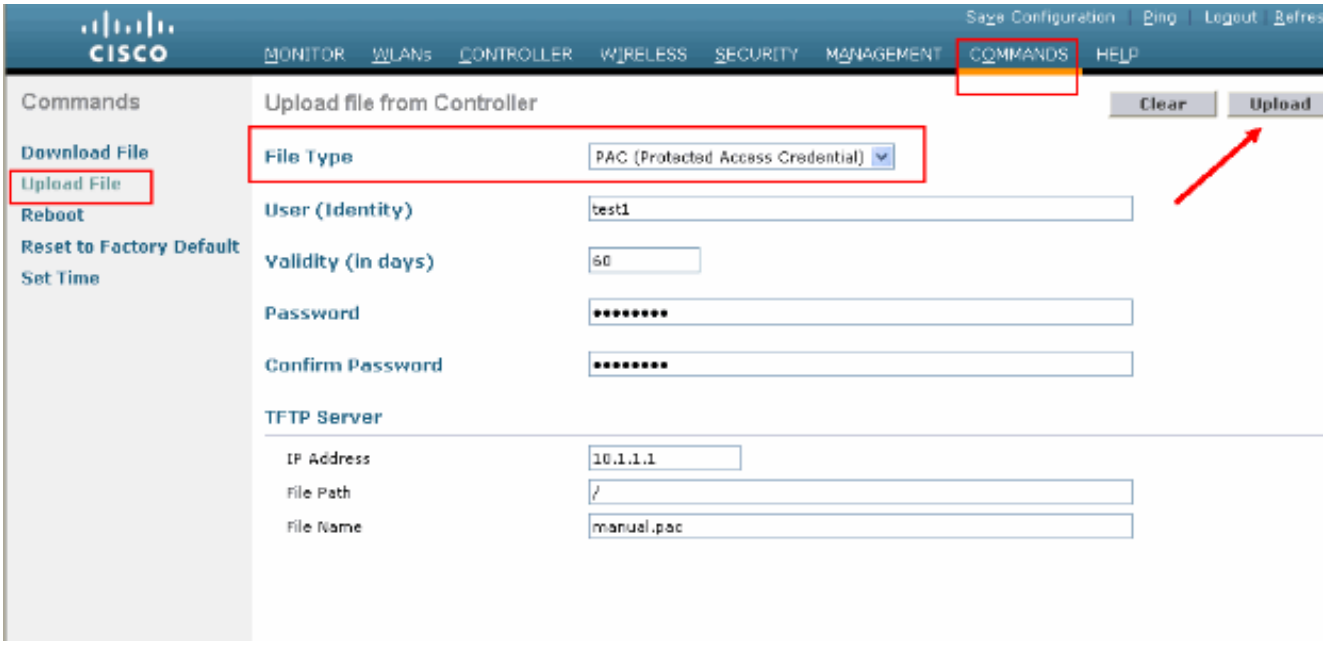
```
(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60
```

Usted puede verificar el valor al cual se pone este temporizador cuando usted publica el **comando config local-auth de la demostración**.

```
(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 usted necesita generar y cargar el PAC manual, usted puede utilizar el GUI o el CLI.Del

GUI, los **COMANDOS** selectos del menú superior y eligieron el **fichero de la carga por teletratamiento de la** lista en el Lado derecho. **PAC** selecto **(credenciales protegidos del acceso) del** menú desplegable del tipo de archivo. Ingrese todos los parámetros y haga clic encendido la **carga por teletratamiento**.



Del 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.
```

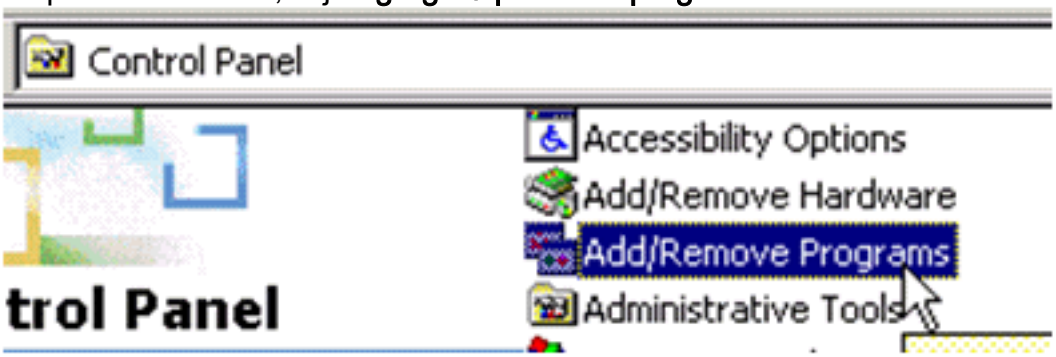
Autoridades de certificación de Microsoft

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

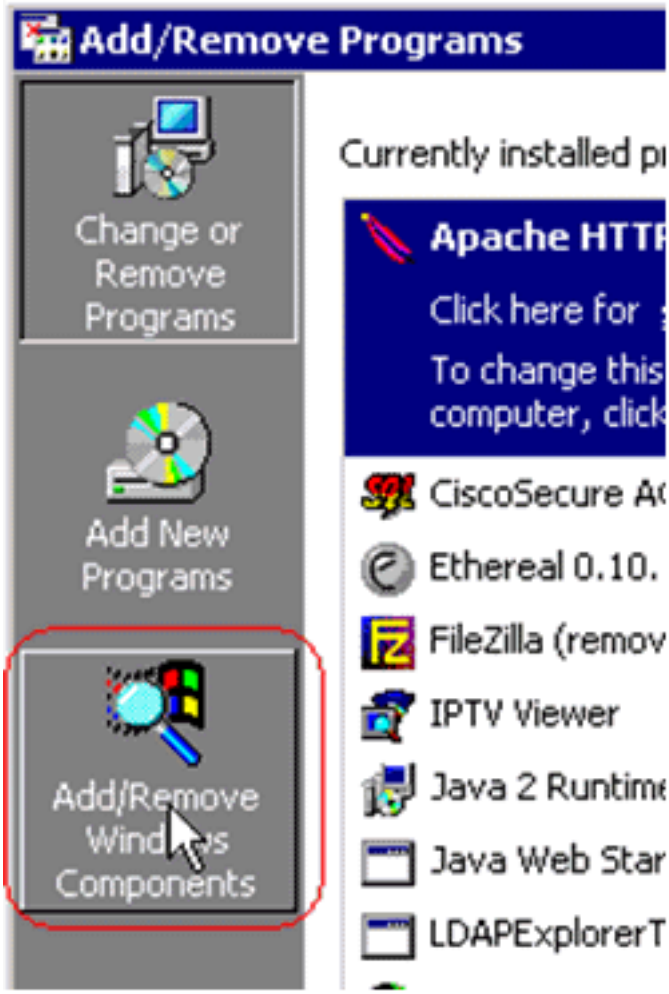
Instalación

Si Windows 2000 Server no tiene ya los servicios de las autoridades de certificación instalados, usted necesita instalarla.

Complete estos pasos para activar las autoridades de certificación de Microsoft en a Windows 2000 Server:

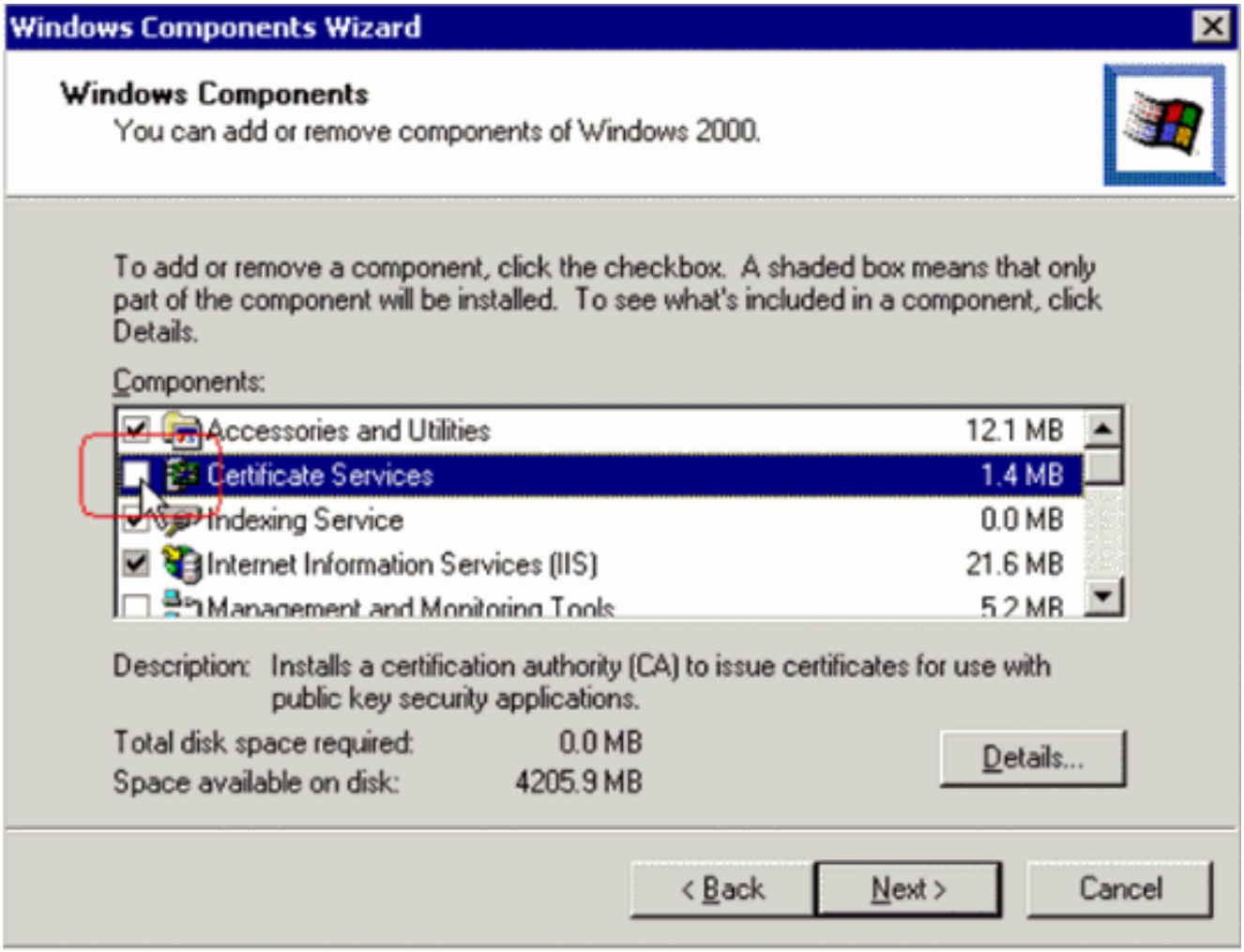
1. Del panel de control, elija **agregan/quitan los programas**.


:
2. Selecto **agregue/quite a los componentes de Windows** en el lado

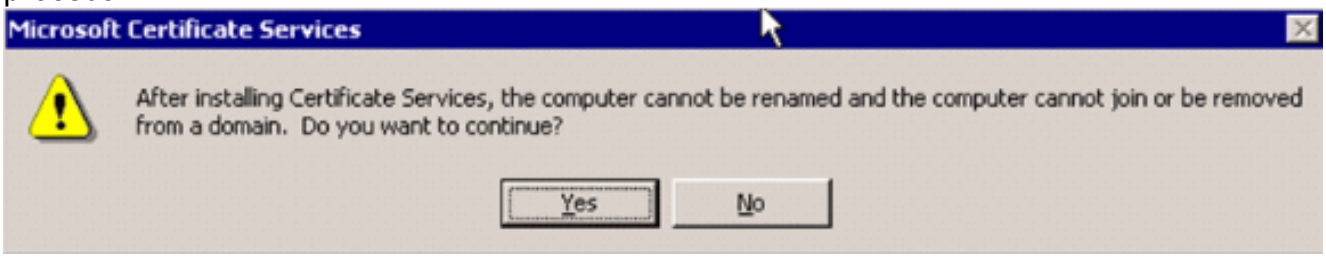


izquierdo.

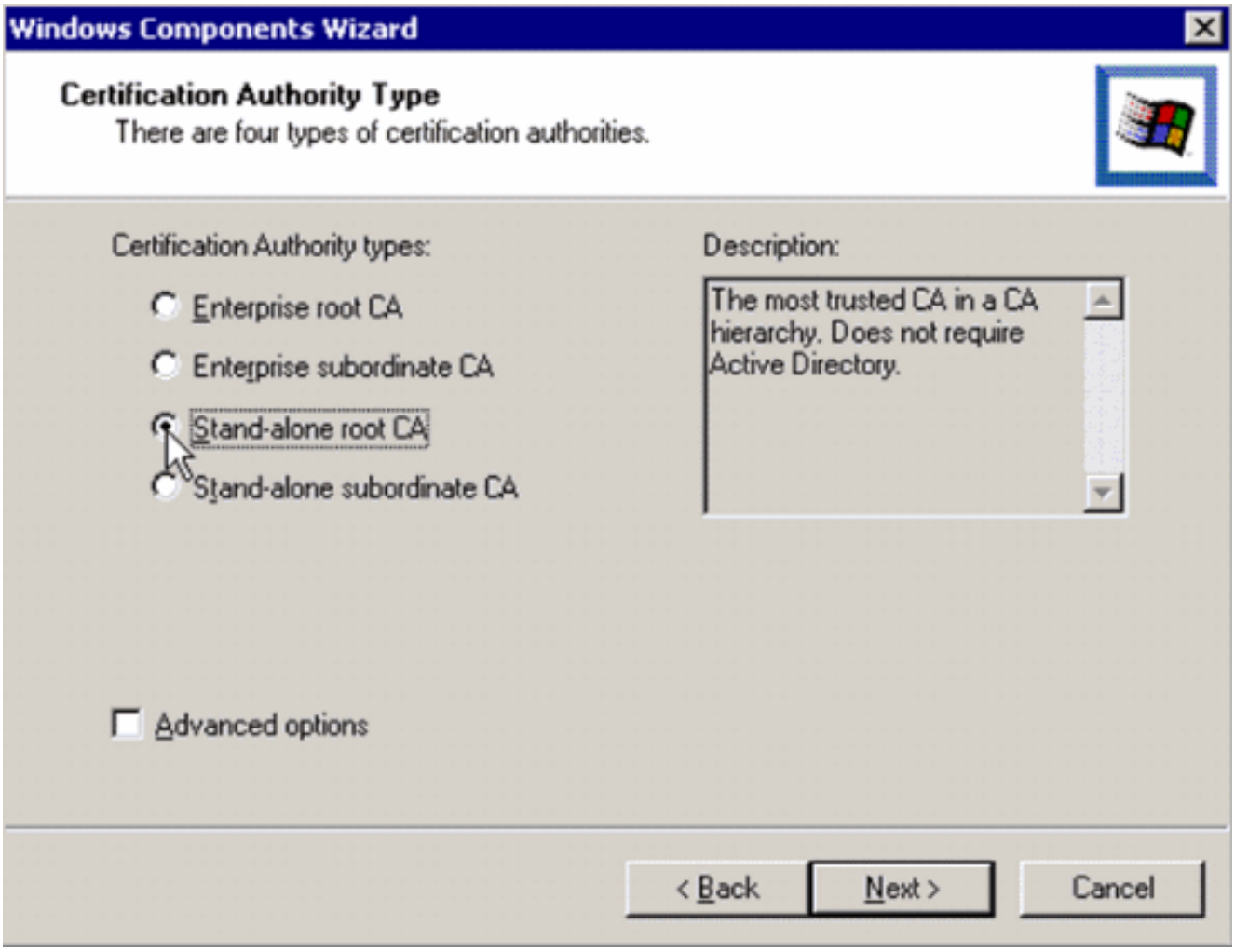
3. Controle los **servicios del certificado**.



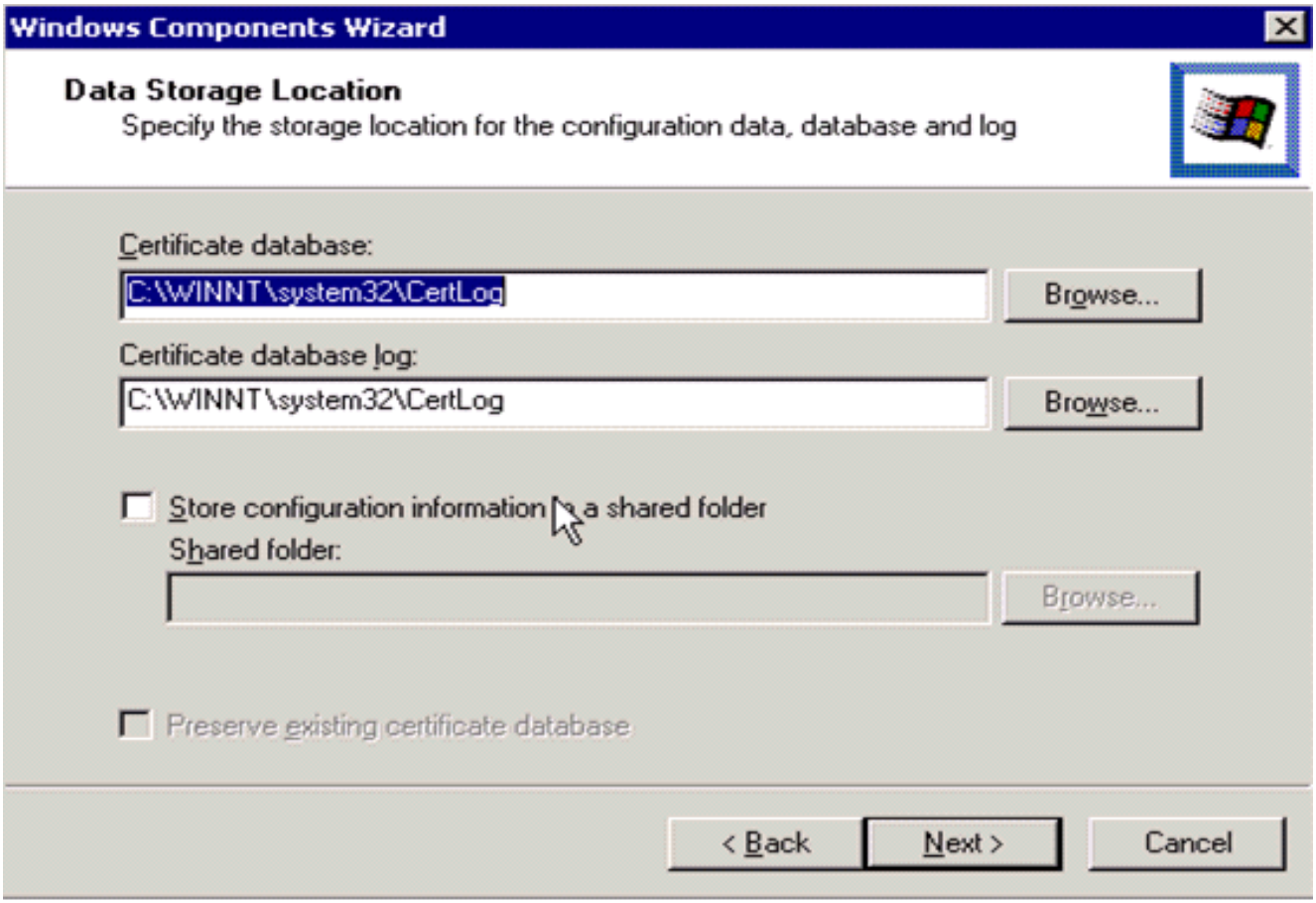
Revise esta advertencia antes de que usted proceda:



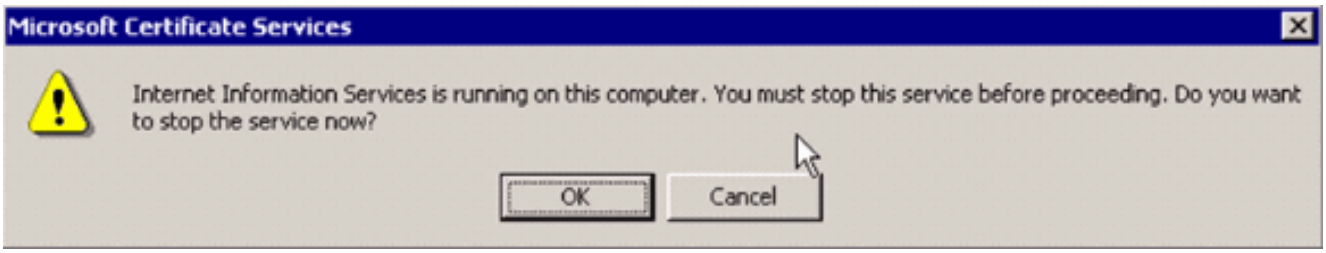
4. Seleccione que el tipo de autoridades de certificación usted quiere instalar. Para crear una autoridad independiente simple, seleccione **independiente raíz CA.**



5. Ingrese la información necesaria sobre las autoridades de certificación. Esta información crea un certificado autofirmado para sus autoridades de certificación. Recuerde el nombre CA que usted utiliza.Las autoridades de certificación salvan los Certificados en una base de datos. Este ejemplo utiliza la disposición del valor por defecto propuesta por Microsoft:



6. Los servicios de las autoridades de certificación de Microsoft utilizan al servidor Web IIS Microsoft para crear y manejar los Certificados de cliente y servidor. Necesita recomenzar el servicio IIS para
esto:



Microsoft Windows 2000 Server ahora instala el nuevo servicio. Usted necesita tener su Windows 2000 Server CD de instalación para instalar los componentes de las nuevas ventanas.Las autoridades de certificación ahora están instaladas.

Instale el certificado en el regulador inalámbrico LAN de Cisco

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

1. Instale el certificado del dispositivo en el regulador LAN de la Tecnología inalámbrica.
2. Descargue un certificado CA del vendedor al regulador LAN de la Tecnología inalámbrica.
3. Configure el regulador LAN de la Tecnología inalámbrica para utilizar el EAP-TLS.

Observe que en el ejemplo mostrado en este documento, el servidor del control de acceso (ACS) está instalado en el mismo host que el Microsoft Active Directory y las autoridades de certificación de Microsoft, pero la configuración debe ser lo mismo si el servidor ACS está en un diverso servidor.

Instale el certificado del dispositivo en el regulador LAN de la Tecnología inalámbrica

Complete estos pasos:

1. . Complete estos pasos para generar el certificado para importar al WLC:Vaya a **http://<serverIpAddr>/certsrv**.Elija la **petición un certificado** y haga clic **después**.Elija la **petición avanzada** y haga clic **después**.Elija **presentan una solicitud de certificado a este CA usando una forma** y hacen clic **después**.Elija al **servidor Web** para el Certificate Template plantilla de certificado y ingrese la información pertinente. Entonces marque las claves como **exportables**.Usted ahora recibe un certificado que usted necesite instalar en su máquina.
2. Complete estos pasos para extraer el certificado de la PC:Abra a un navegador del Internet Explorer y elija las **herramientas > las opciones de Internet > el contenido**.Haga clic los **Certificados**.Seleccione el certificado nuevamente instalado del menú desplegable.Haga clic la **exportación**.Haga clic **después** dos veces y elija **sí la exportación la clave privada**. Este formato es el PKCS#12 (formato .PFX).Elija la **protección fuerte del permiso**.Pulse una contraseña.Sálvela en un fichero <tme2.pfx>.
3. Copie el certificado en el formato PKCS#12 a cualquier ordenador donde usted hace Openssl instalar para convertirlo al formato PEM.

```
(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.
```

4. Descargue el certificado convertido del dispositivo de formato PEM sobre 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 que está reiniciado, controle 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 CA del vendedor al regulador LAN de la Tecnología inalámbrica

Complete estos pasos:

1. Complete estos pasos para extraer el certificado CA del vendedor:Vaya a **http://<serverIpAddr>/certsrv**.Elija **extraen el certificado CA** y hacen clic **después**.Elija el certificado CA.Haga clic **DER codificado**.Haga clic en el **certificado CA de la transferencia directa** y salve el certificado como **rootca.cer**.
2. Convierta al vendedor que el CA del formato DER en el formato PEM con el **openssl x509 - en rootca.cer - informa a DER - hacia fuera rootca.pem - comando del outform PEM**.El archivo saliente es rootca.pem en el formato PEM.
3. Descargue el certificado CA del vendedor:

```
(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
```

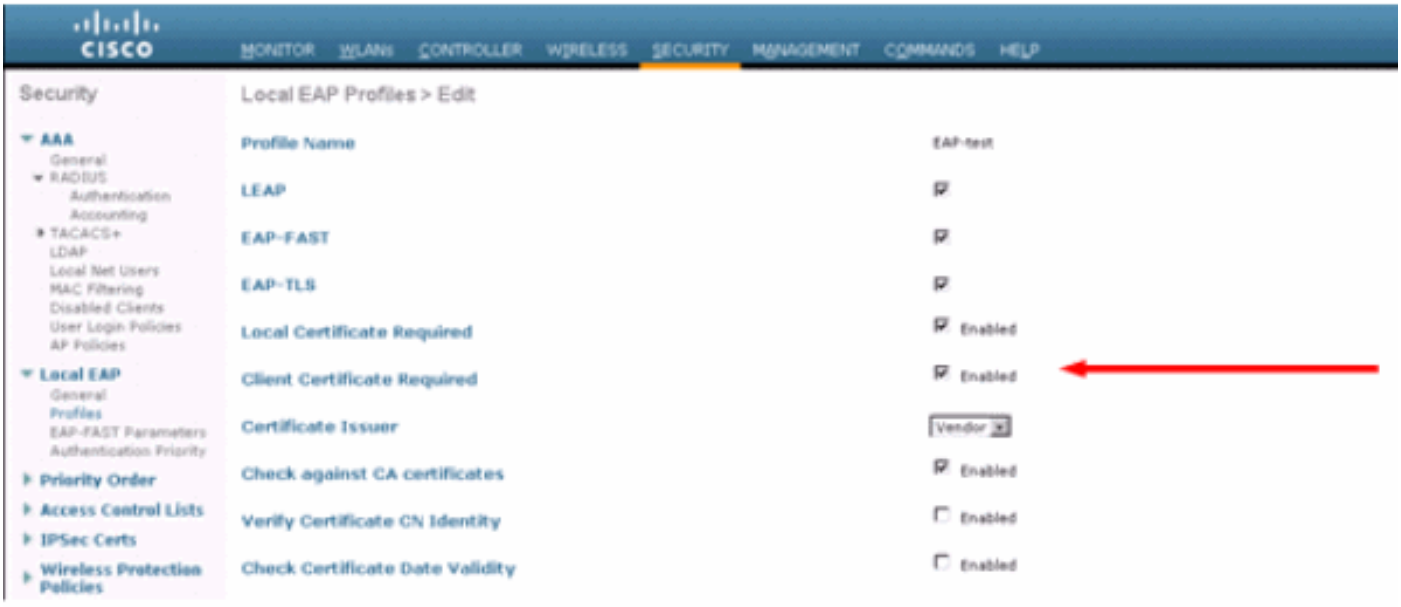
```
Mode..................................... TFTP
Data Type................................ Vendor CA Cert
TFTP Server IP........................... 10.1.1.12
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /
TFTP Filename............................ 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 regulador LAN de la Tecnología inalámbrica para utilizar el EAP-TLS

Complete estos pasos:

Del GUI, elija la **Seguridad > local EAP > los perfiles**, elija el perfil y controle para saber si hay estas configuraciones:

- El certificado local requerido se activa.
- El certificado del cliente requerido se activa.
- El emisor del certificado es vendedor.
- El control contra los Certificados CA se activa.



Instale el certificado de la autoridad de certificación en el dispositivo cliente

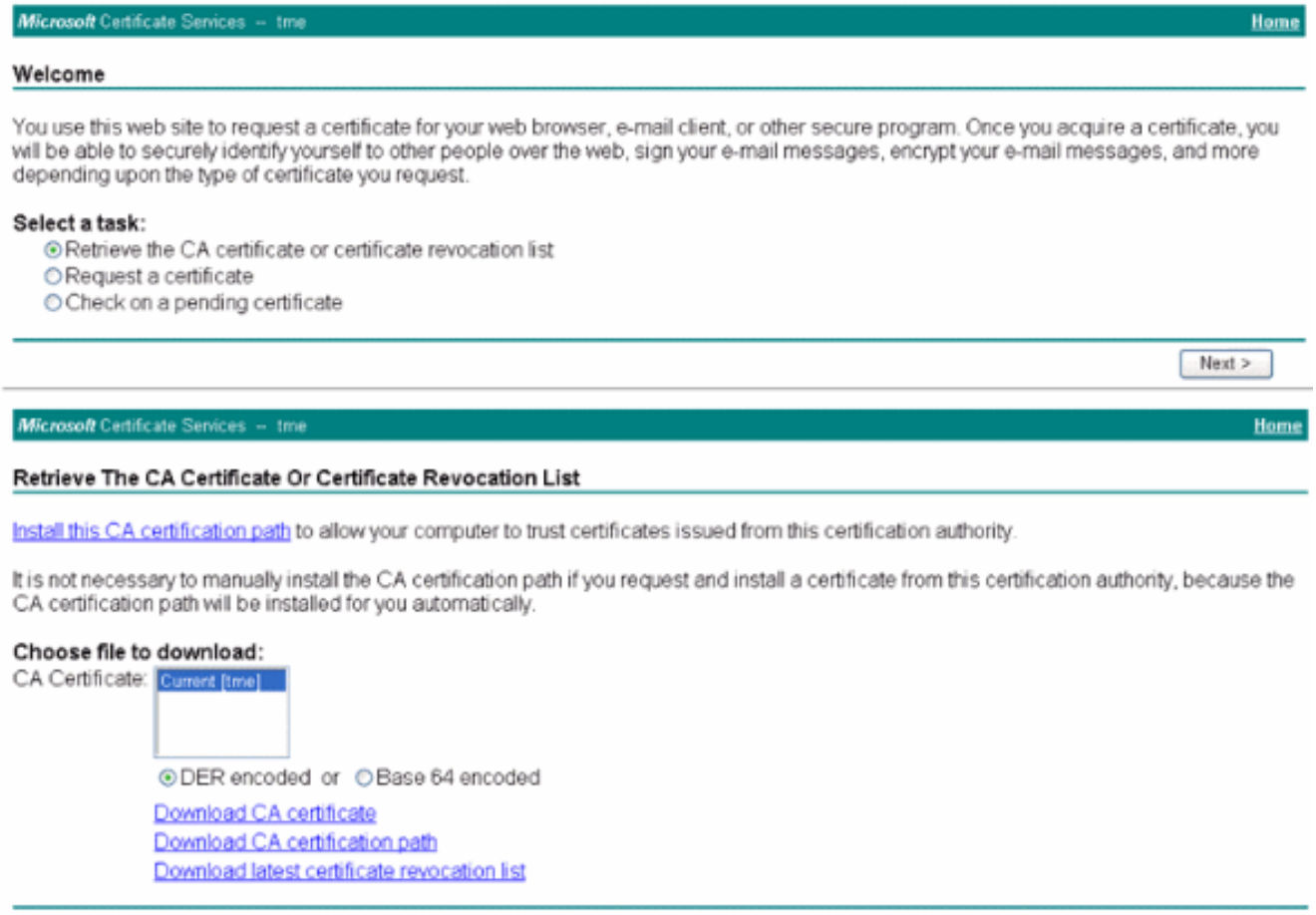
Descargue y instale a certificado raíz CA para el cliente

El cliente debe obtener a certificado raíz CA de un servidor de las autoridades de certificación. Hay varios métodos que usted puede utilizar para obtener un certificado del cliente y para instalarlo en la máquina de Windows XP. Para adquirir un certificado válido, el usuario de Windows XP tiene que ser abierto una sesión usando su identificación del usuario y debe tener

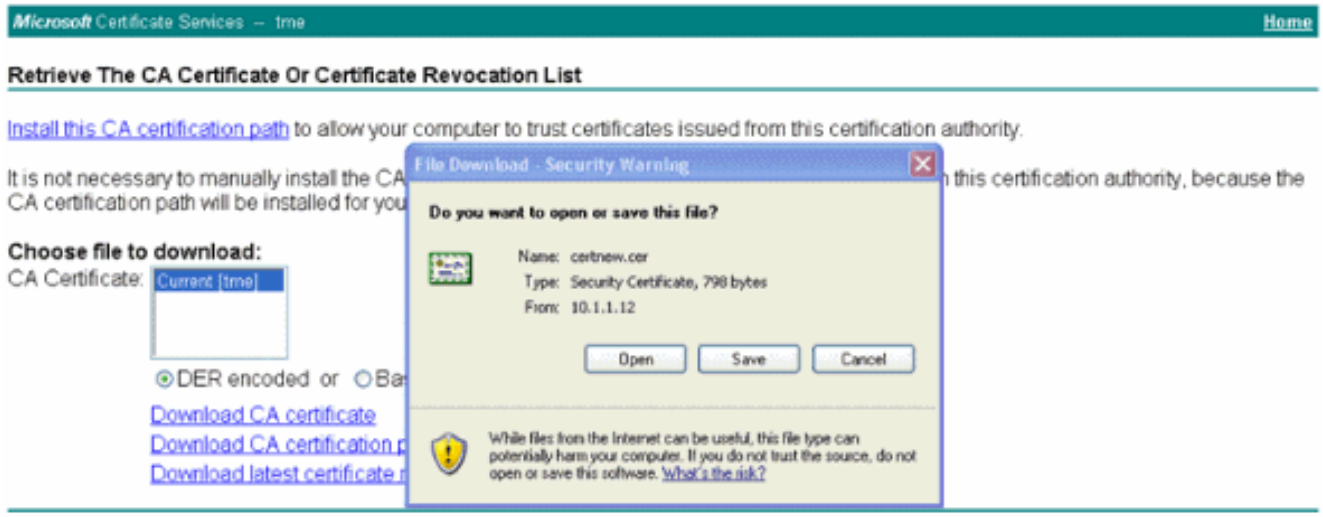
una conexión de red.

Utilizaron a un buscador Web en el cliente de Windows XP y una conexión alámbrica a la red para obtener un certificado del cliente del servidor privado de las autoridades de certificación raíz. Este procedimiento se utiliza para obtener el certificado del cliente de un servidor de las autoridades de certificación de Microsoft:

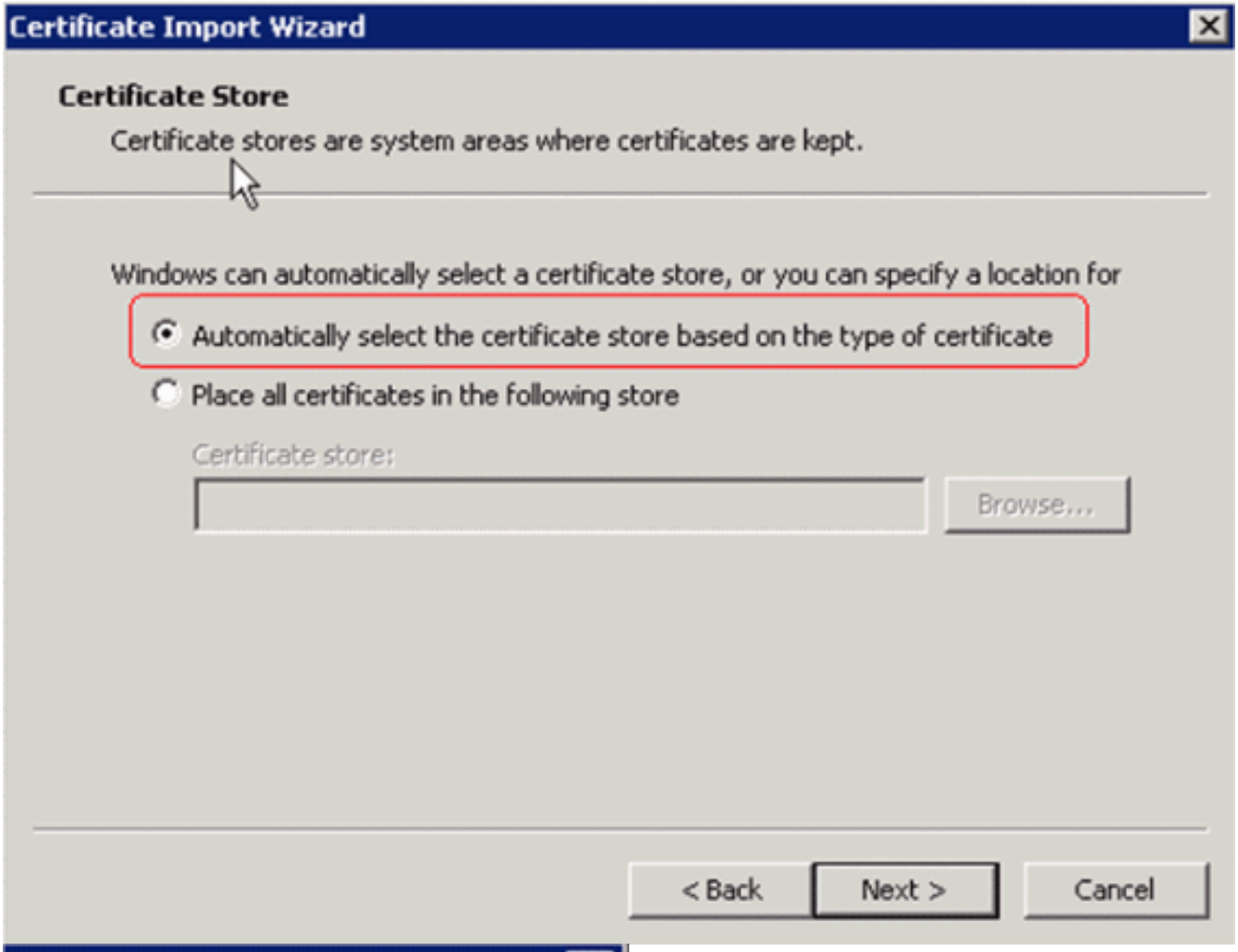
1. Utilice a un buscador Web en el cliente y señale al navegador al servidor de las autoridades de certificación. Para hacer esto, ingrese **http://IP-address-of-Root-CA/certsrv**.
2. Ábrase una sesión con **Domain_Name \ el user_name**. Usted debe abrirse una sesión usando el username del individuo que es utilizar al cliente de XP.
3. En la ventana agradable, elija **extraen un certificado CA** y hacen clic **después**.
4. Seleccione la **codificación Base64** y **descargue el certificado CA**.
5. En la ventana publicada certificado, el tecleo **instala este certificado** y hace clic **después**.
6. Elija **automáticamente selecto el almacén de certificados** y haga clic **después**, para el mensaje acertado de la importación.
7. Conecte con las autoridades de certificación para extraer el certificado de la autoridad de certificación:



8. Haga clic el **certificado CA de la transferencia directa**.

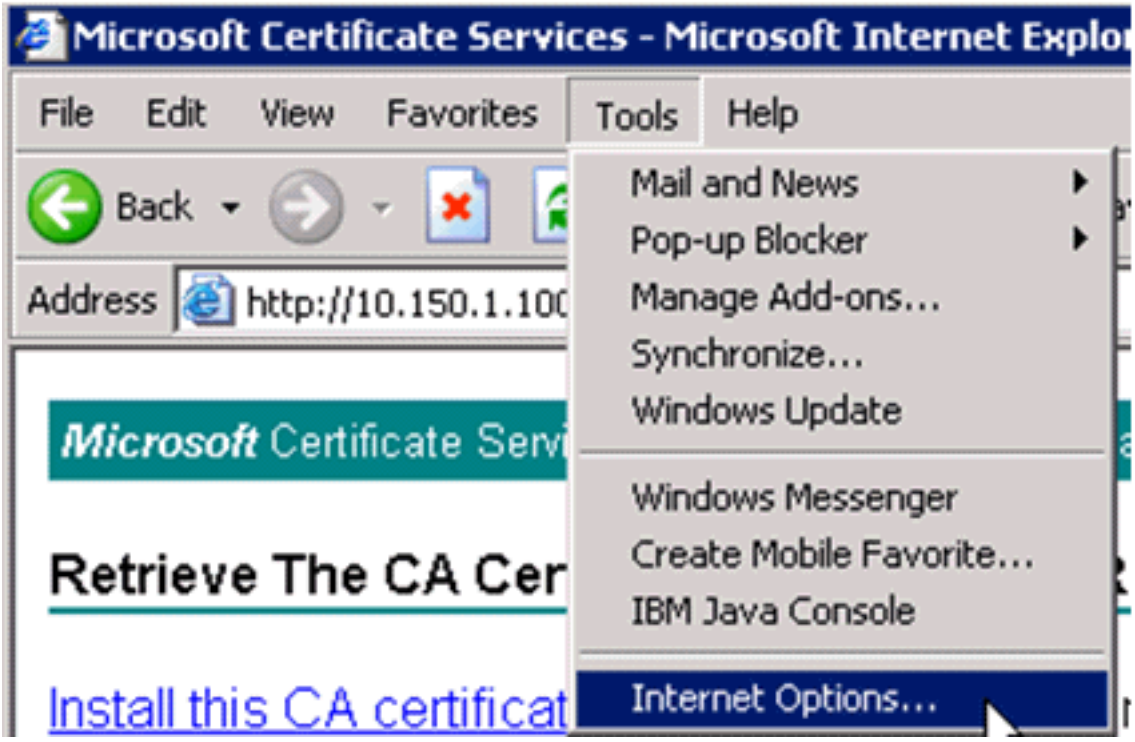

Microsoft Certificate Services -- tme
Home
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
It is not necessary to manually install the CA
this certification authority, because the
CA certification path will be installed for you
Choose file to download:
CA Certificate:
Current [tme]
DER encoded or
Download CA certificate
Download CA certification p
Download latest certificate r
File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 798 bytes
From: 10.1.1.12
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

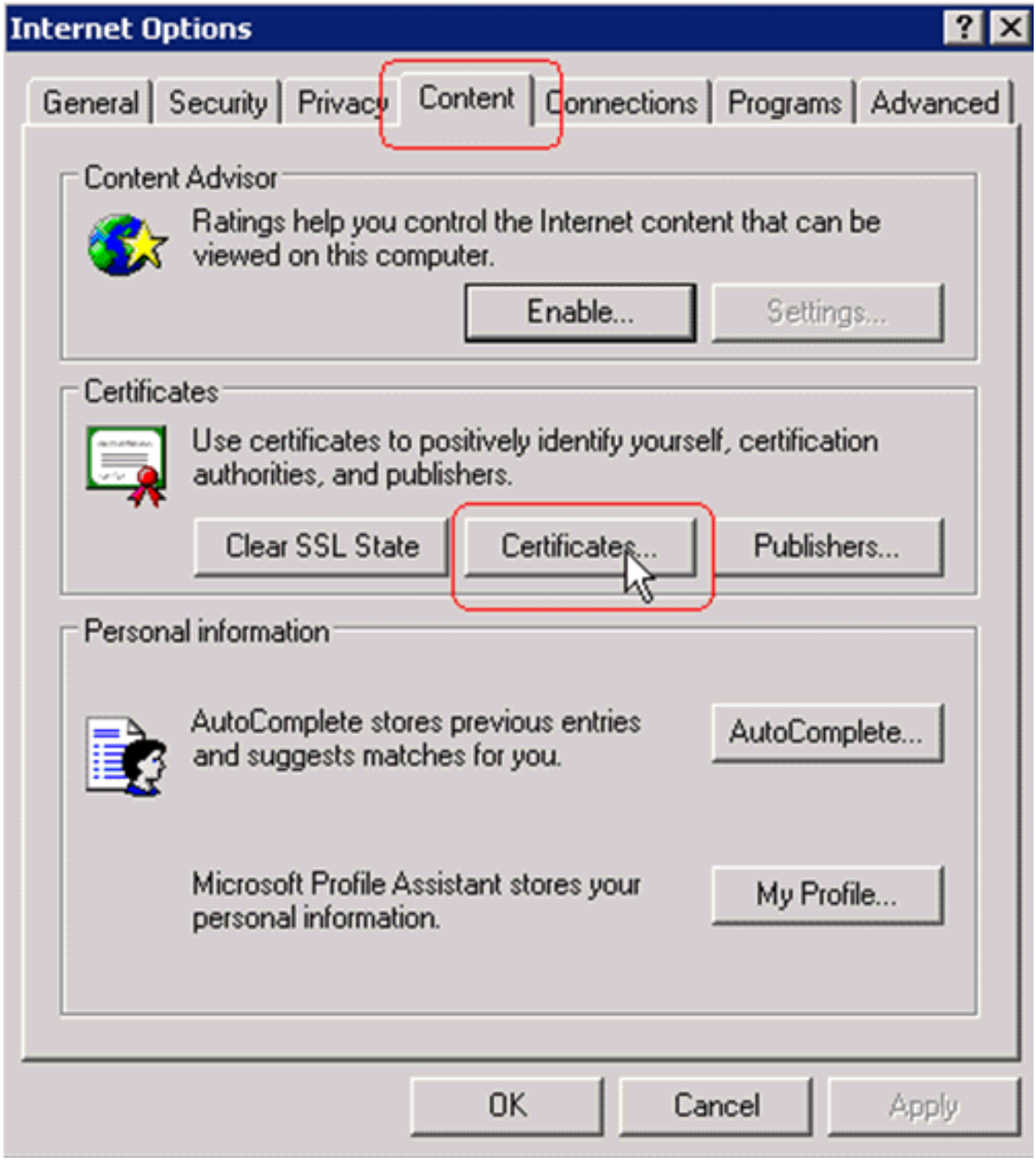

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity 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



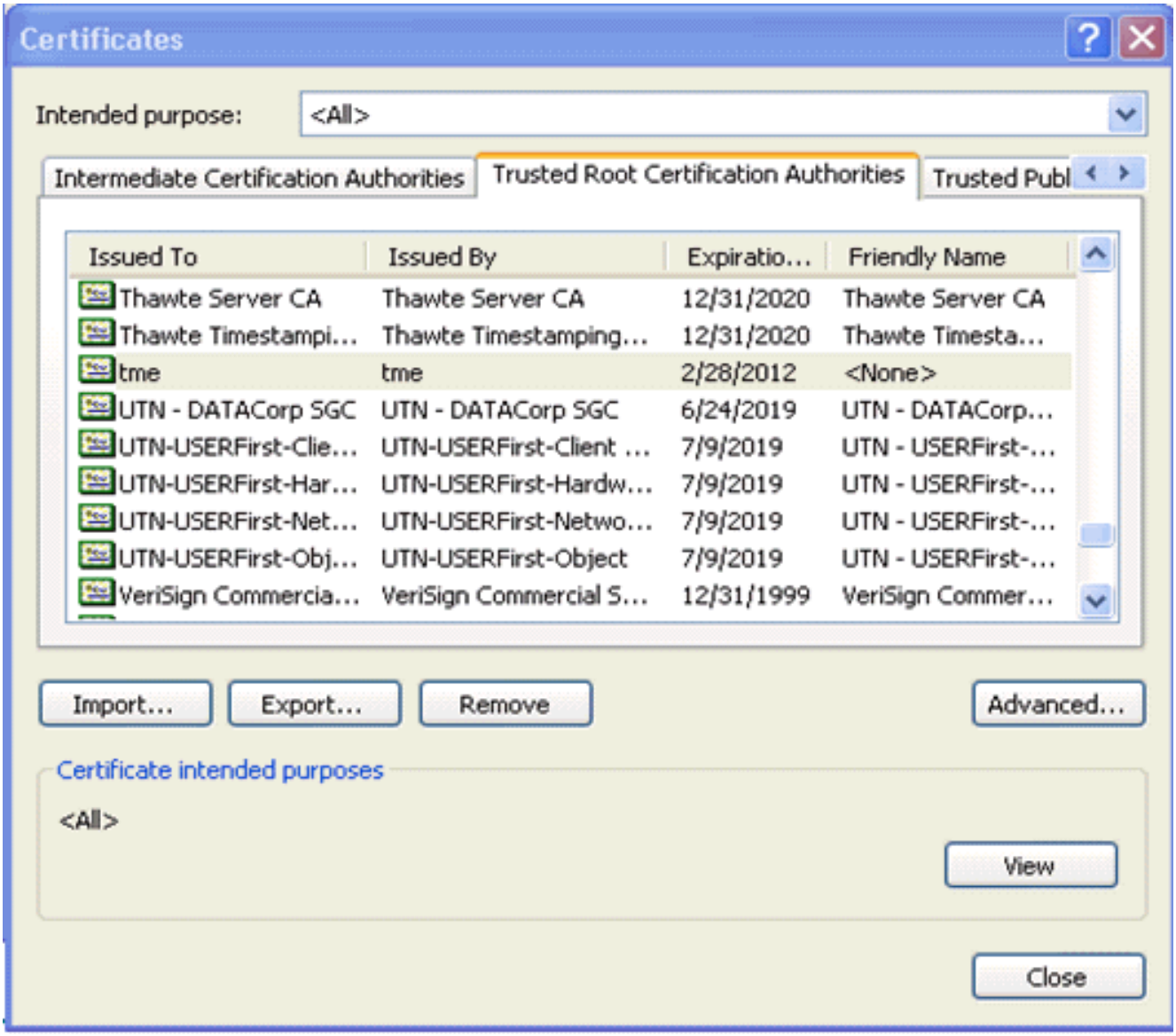
9. Para controlar que el certificado de la autoridad de certificación está instalado correctamente, Internet Explorer abierto y elegir las **herramientas > las opciones de Internet > el contenido > los**

Certificados.





En el Trusted Root Certification Authority, usted debe ver sus autoridades de certificación nuevamente
instaladas:



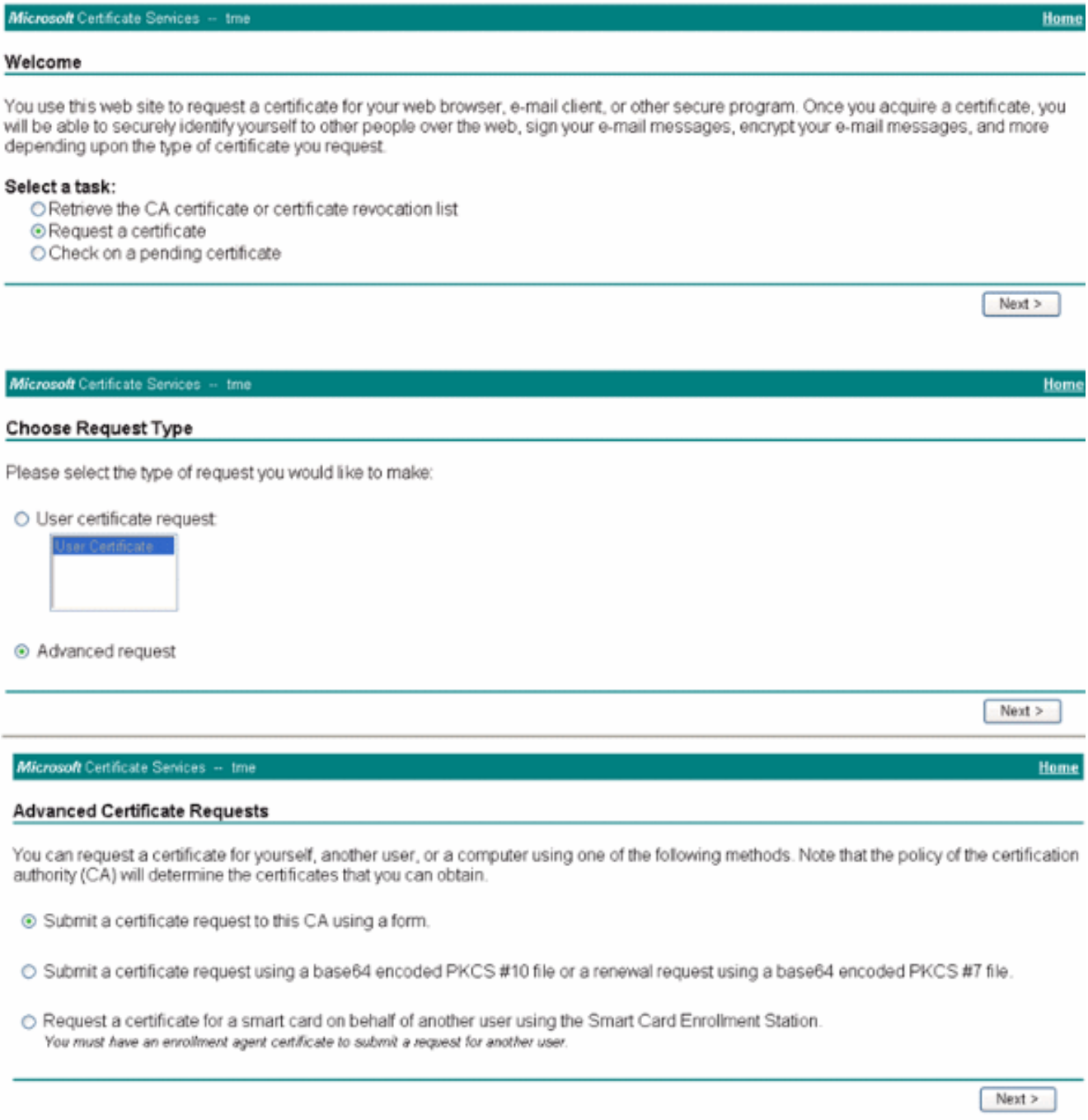
Genere un certificado del cliente para un dispositivo cliente

El cliente debe obtener un certificado de un servidor de las autoridades de certificación para que el WLC autentique a un cliente del EAP-TLS de la red inalámbrica (WLAN). Hay varios métodos que usted puede utilizar para obtener un certificado del cliente y instalarlo en la máquina de Windows XP. Para adquirir un certificado válido, el usuario de Windows XP tiene que ser abierto una sesión usando su identificación del usuario y debe tener una conexión de red (una conexión alámbrica o una conexión de la red inalámbrica (WLAN) con la Seguridad del 802.1x inhabilitada).

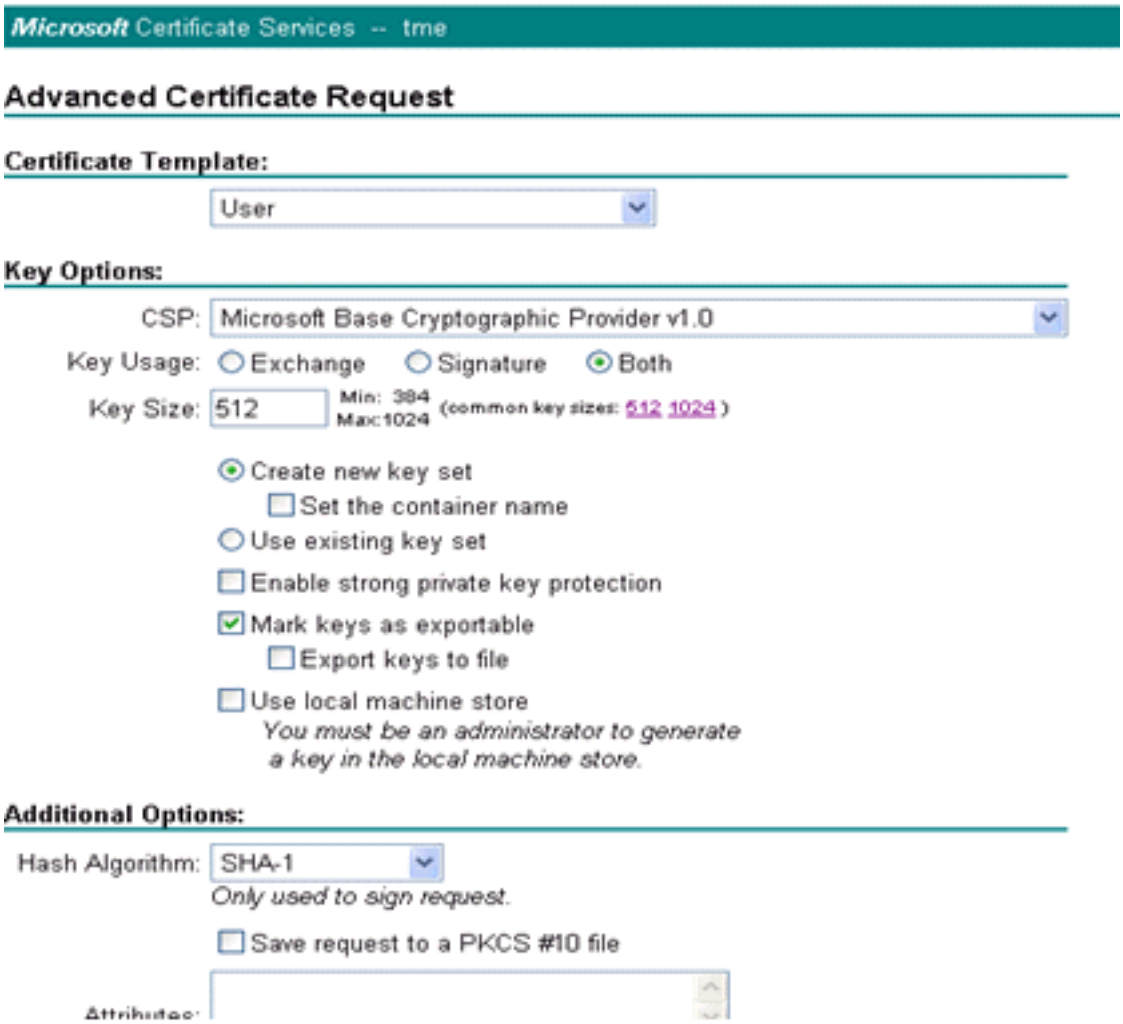
Utilizan a un buscador Web en el cliente de Windows XP y una conexión alámbrica a la red para obtener un certificado del cliente del servidor privado de las autoridades de certificación raíz. Este procedimiento se utiliza para obtener el certificado del cliente de un servidor de las autoridades de certificación de Microsoft:

1. Utilice a un buscador Web en el cliente y señale al navegador al servidor de las autoridades de certificación. Para hacer esto, ingrese **http://IP-address-of-Root-CA/certsrv**.
2. Ábrase una sesión con **Domain_Name \ el user_name**. Usted debe abrirse una sesión usando el username del individuo que utiliza al cliente de XP. (El username consigue integrado en el certificado del cliente.)
3. En la ventana agradable, elija la **petición un certificado** y haga clic **después**.
4. Elija la **petición avanzada** y haga clic **después**.

5. Elija **presentan una solicitud de certificado a este CA usando una forma** y hacen clic **después**.
6. En el formulario de solicitud de certificado avanzado, elija el Certificate Template plantilla de certificado como **usuario**, especifican el tamaño de clave como **1024** y el tecleo **somete**.
7. En la ventana publicada certificado, el tecleo **instala este certificado**. Esto da lugar a la instalación exitosa de un certificado del cliente en el cliente de Windows XP.

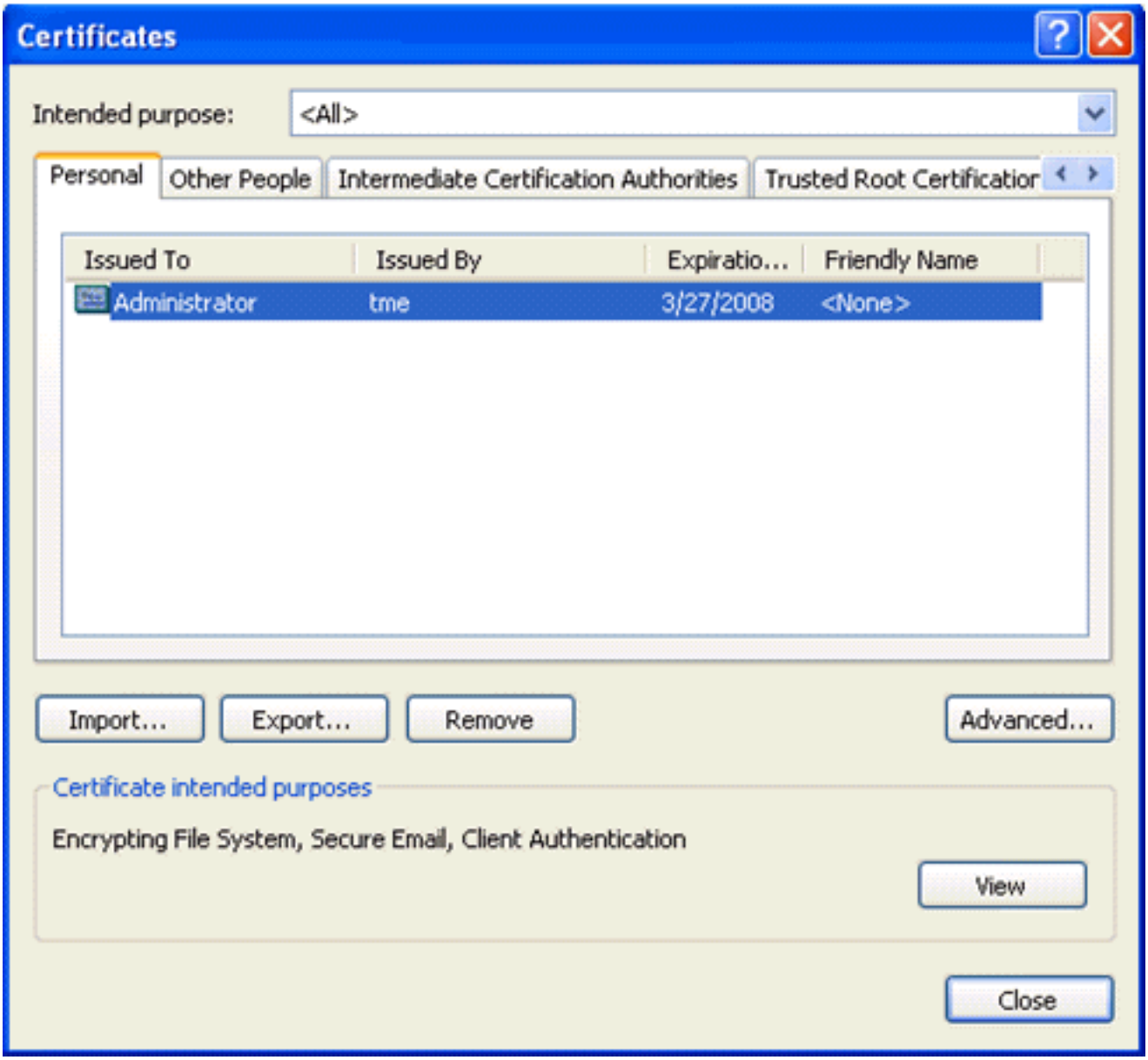


8. Seleccione el **Certificado de autenticación del**



cliente. El certificado del cliente ahora se crea.

9. Para controlar que el certificado está instalado, vaya al Internet Explorer y elija las **herramientas > las opciones de Internet > el contenido > los Certificados**. En la tabulación personal, usted debe ver el certificado.

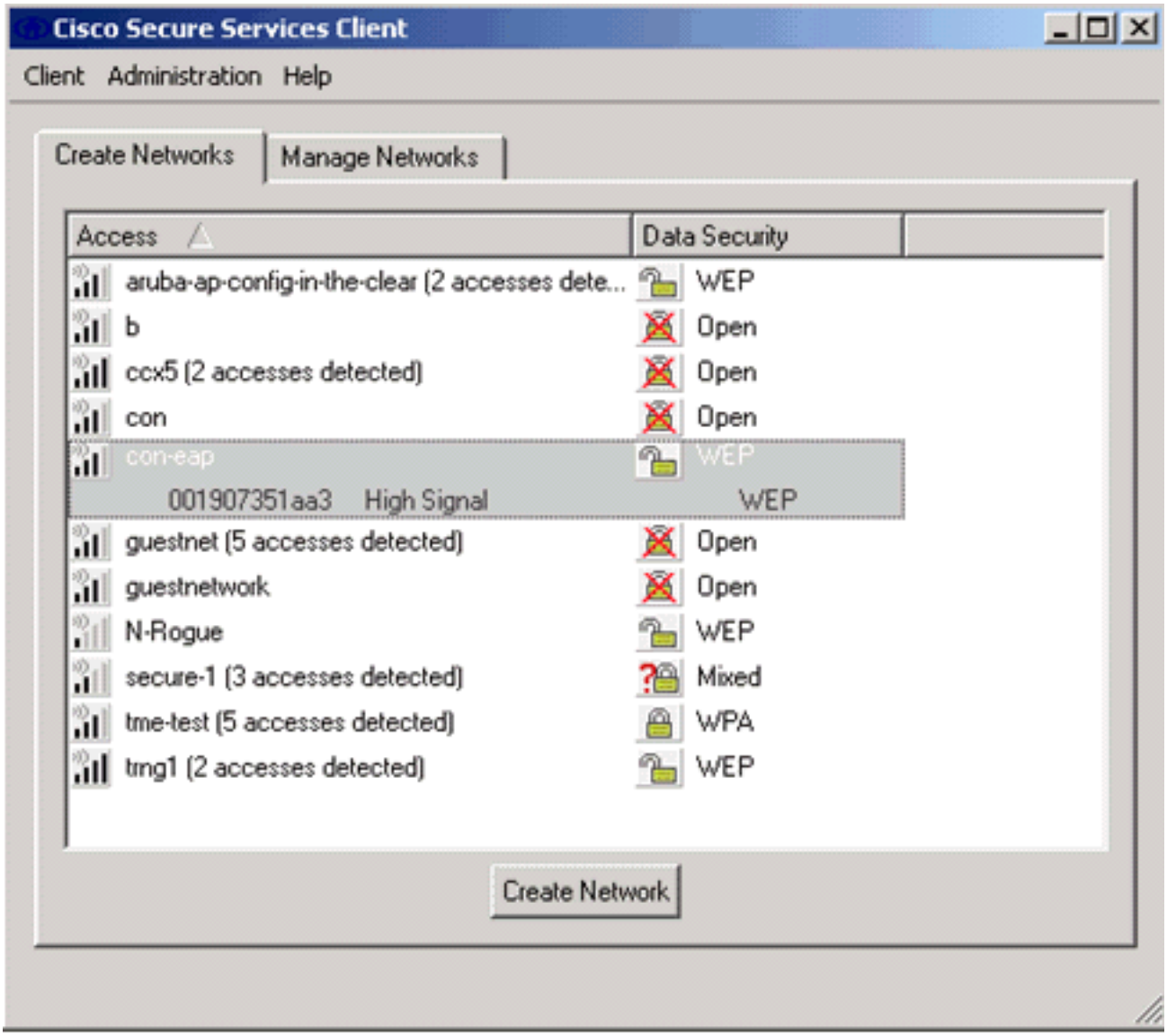


EAP-TLS con el Cisco Secure Services Client en el dispositivo cliente

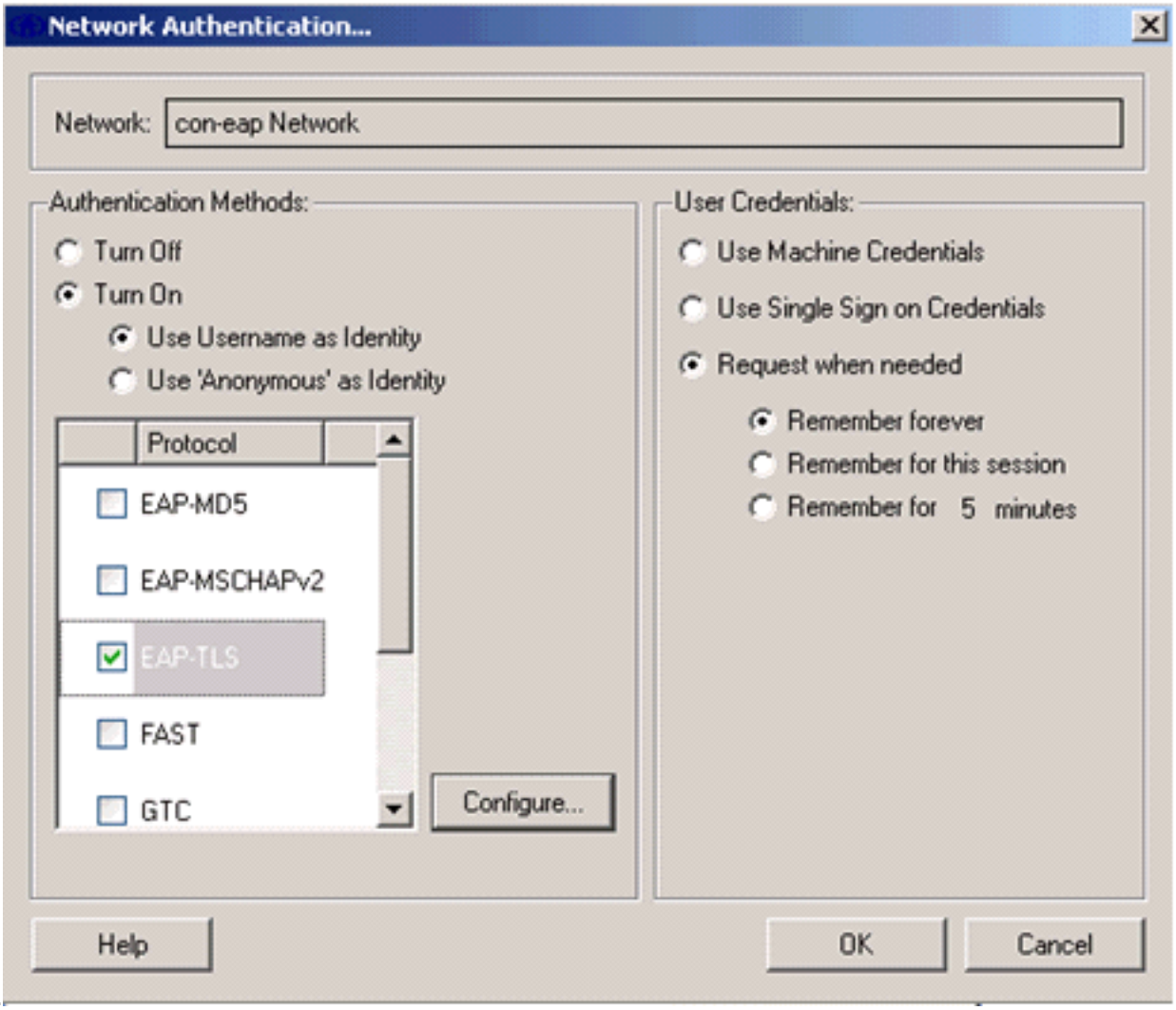
Complete estos pasos:

1. El WLC, por abandono, difunde el SSID, así que se muestra en la lista de las redes del crear de SSID analizados. Para crear un perfil de la red, usted puede hacer clic el SSID en la lista (empresa) y el tecleo **crea la red**.Si la infraestructura WLAN se configura con la difusión SSID inhabilitada, usted debe agregar manualmente el SSID. Para hacer esto, el tecleo **agrega** bajo dispositivos de acceso y ingresa manualmente el SSID apropiado (por ejemplo, empresa). Configure el comportamiento activo de la punta de prueba para el cliente. Es decir, donde el cliente sonda activamente para su SSID configurado. Especifique **activamente la búsqueda para este dispositivo de acceso** después de que usted ingrese el SSID en la ventana del dispositivo de acceso del agregar.**Note**: Las configuraciones de puerto no permiten los modos de la empresa (802.1x) si las configuraciones de la autenticación EAP no son primeras configuradas para el perfil.
2. El tecleo **crea la red** para lanzar la ventana del perfil de la red, que permite que usted asocie (o configurado) el SSID elegido a un mecanismo de autenticación. Asigne un nombre

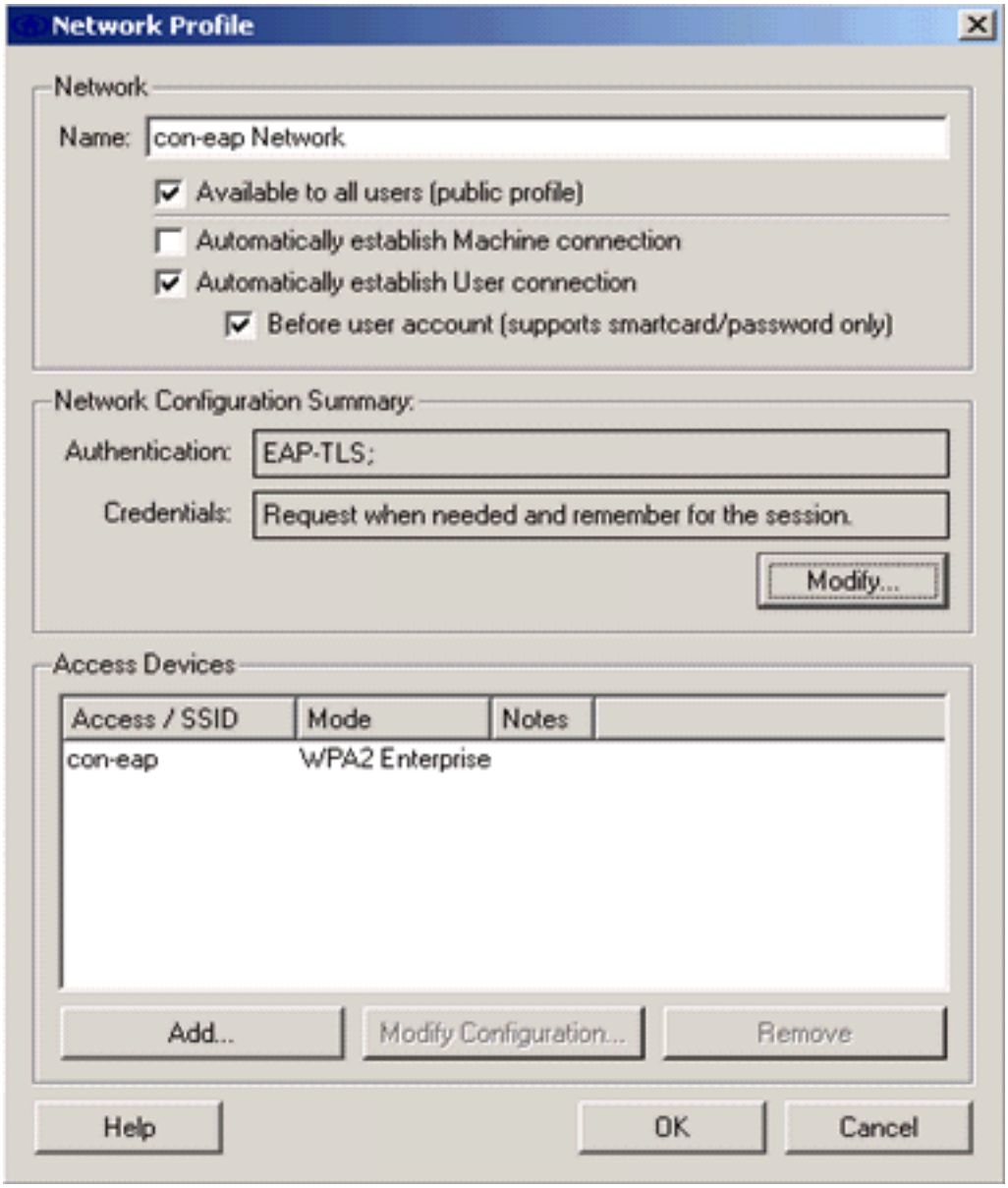
descriptivo para el perfil.**Note**: Los tipos múltiples de la Seguridad de WLAN y/o los SSID pueden ser asociados bajo este perfil de la autenticación.



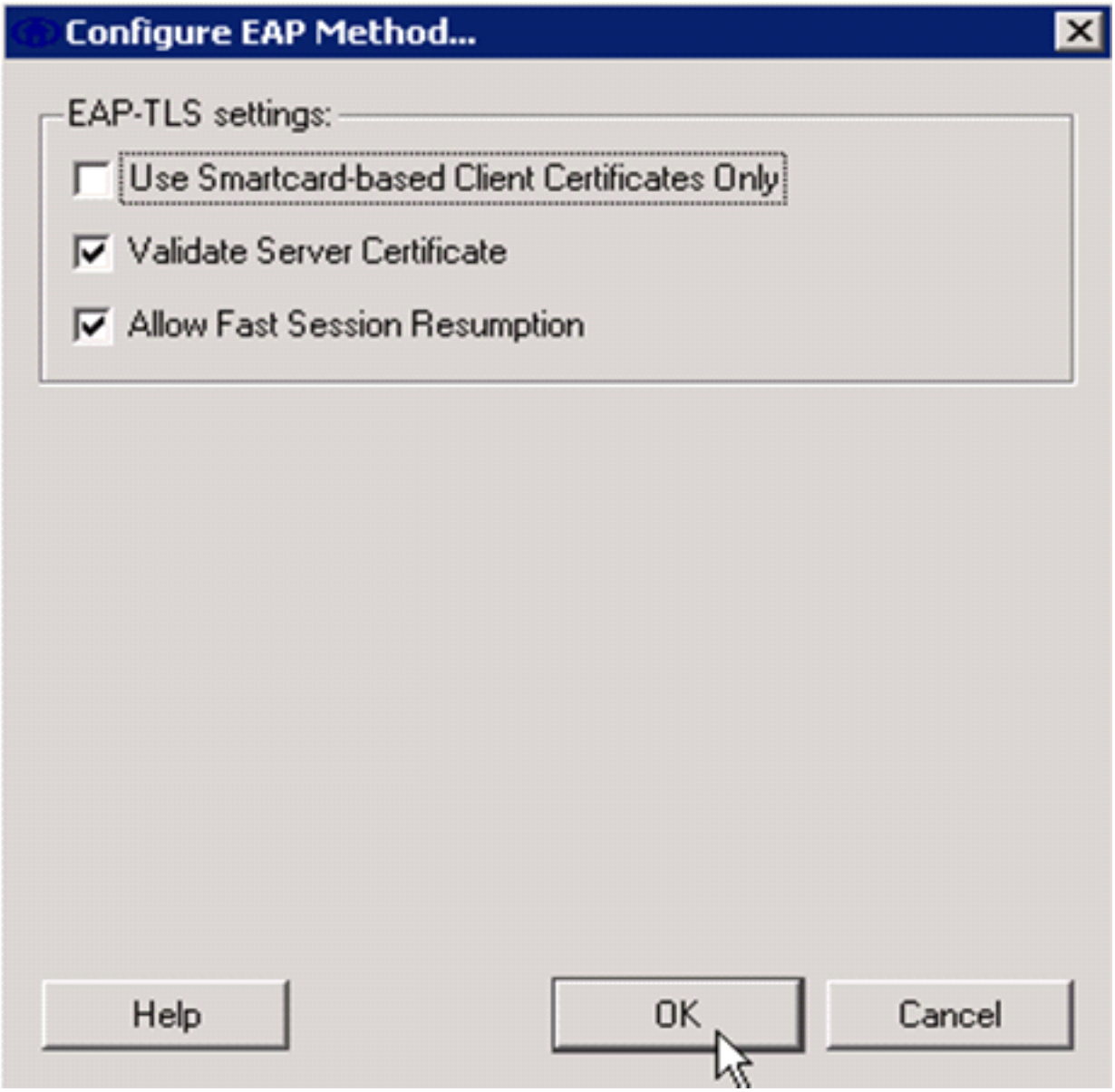
3. Gire la autenticación y controle el método del EAP-TLS. Entonces haga clic **configuran** para configurar las propiedades del EAP-TLS.
4. Bajo resumen de la configuración de red, el tecleo **se modifica** para configurar las configuraciones EAP/de las credenciales.
5. Especifique **giran la autenticación**, eligen el **EAP-TLS** bajo protocolo, y eligen el **username** como la identidad.
6. Especifique la **sola muestra del uso en las credenciales** de utilizar los credenciales de inicio de sesión para la autenticación de red. El tecleo **configura** para poner los parámetros del 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

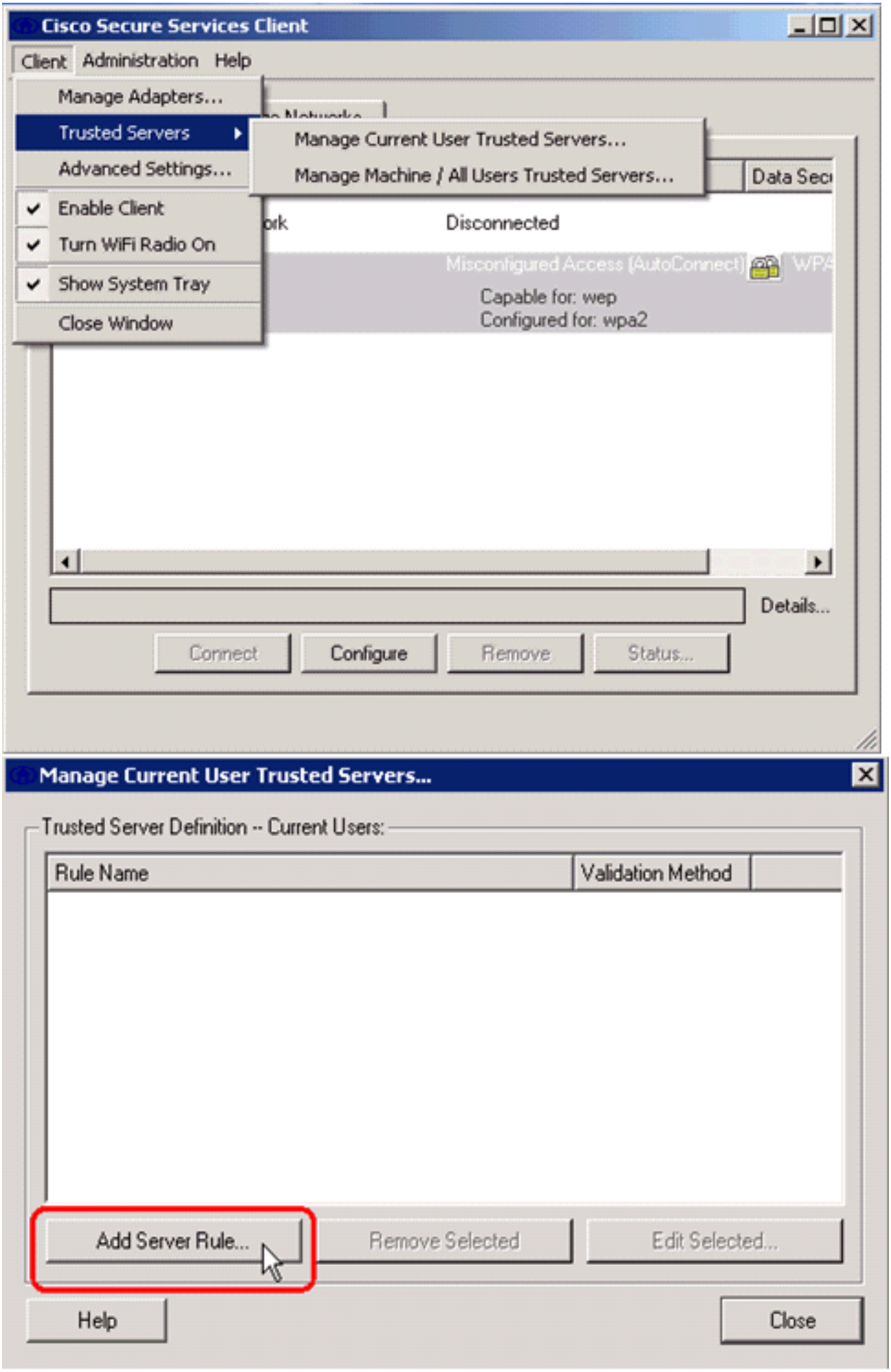
TLS.



7. Para tener una configuración asegurada del EAP-TLS que usted necesita controlar el certificado de servidor de RADIUS. Para hacer esto, el control **valida el certificado de servidor**.

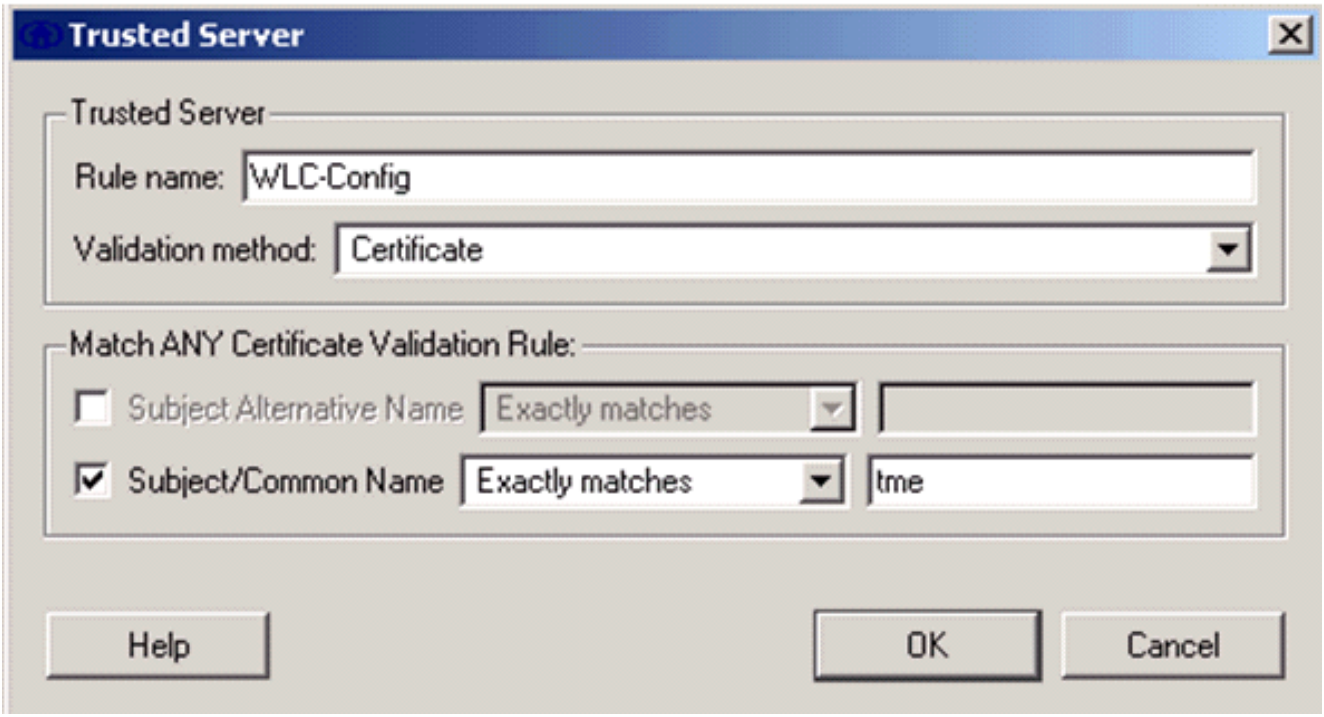


8. Para validar el certificado de servidor de RADIUS, usted necesita dar la información del Cisco Secure Services Client para validar solamente el certificado derecho. Elija al **cliente > confiaba en que los servidores > manejan los servidores confiados en Usuario usuario actual**.



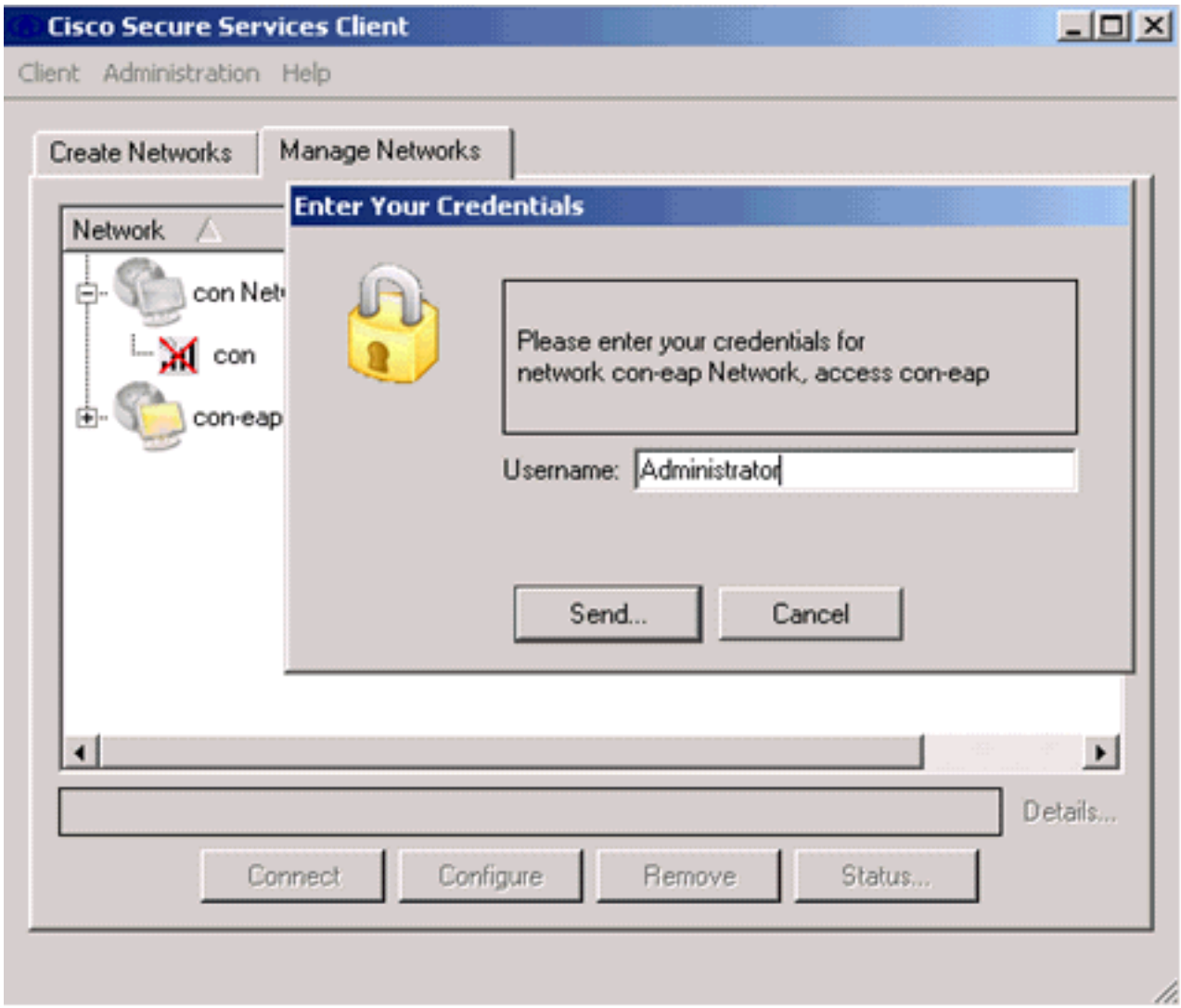
9. Dé un nombre para la regla y controle el nombre del certificado de

servidor.



Se acaba la configuración del EAP-TLS.

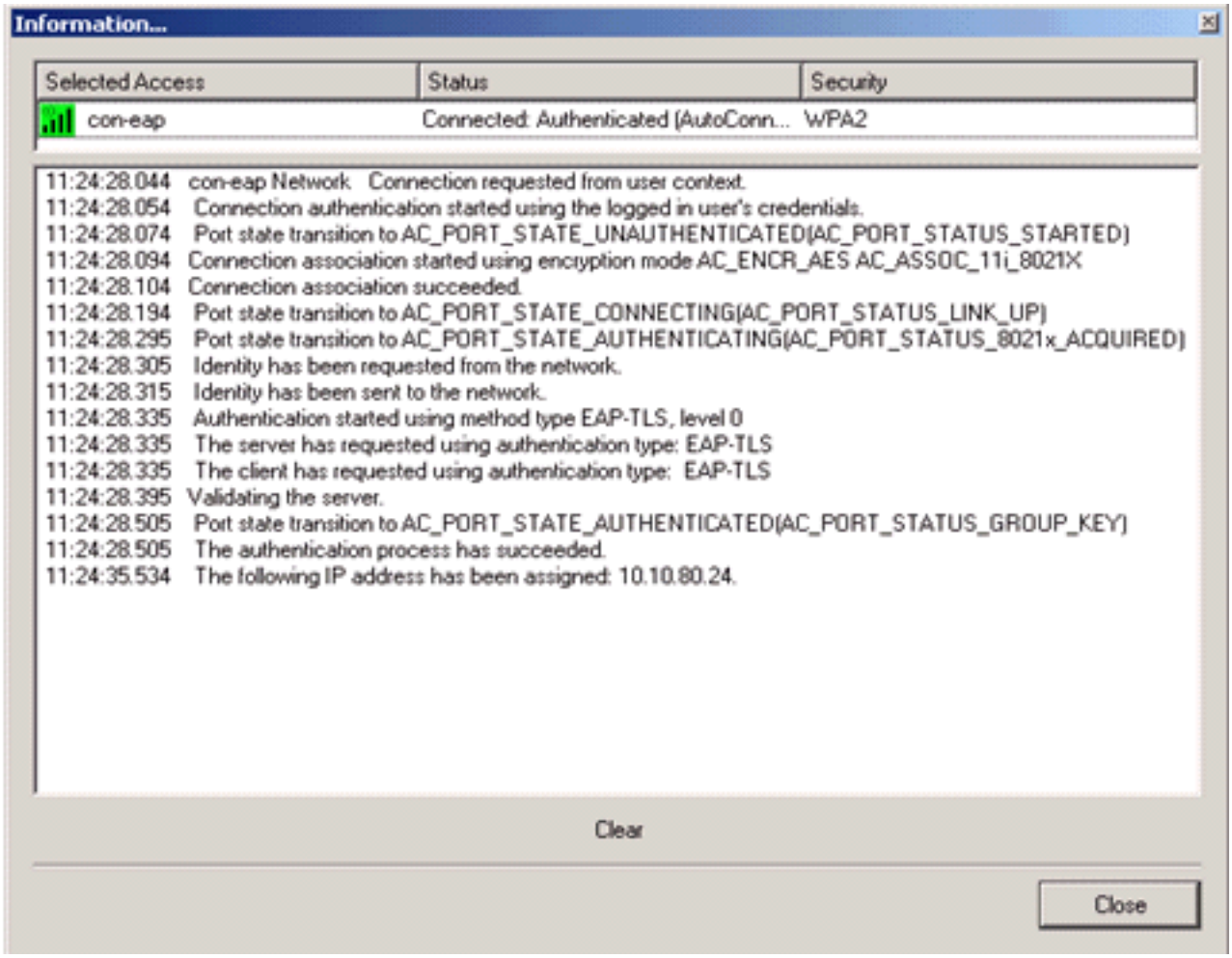
10. Conecte con el perfil de la red inalámbrica. El Cisco Secure Services Client pide el ingreso del usuario al sistema:

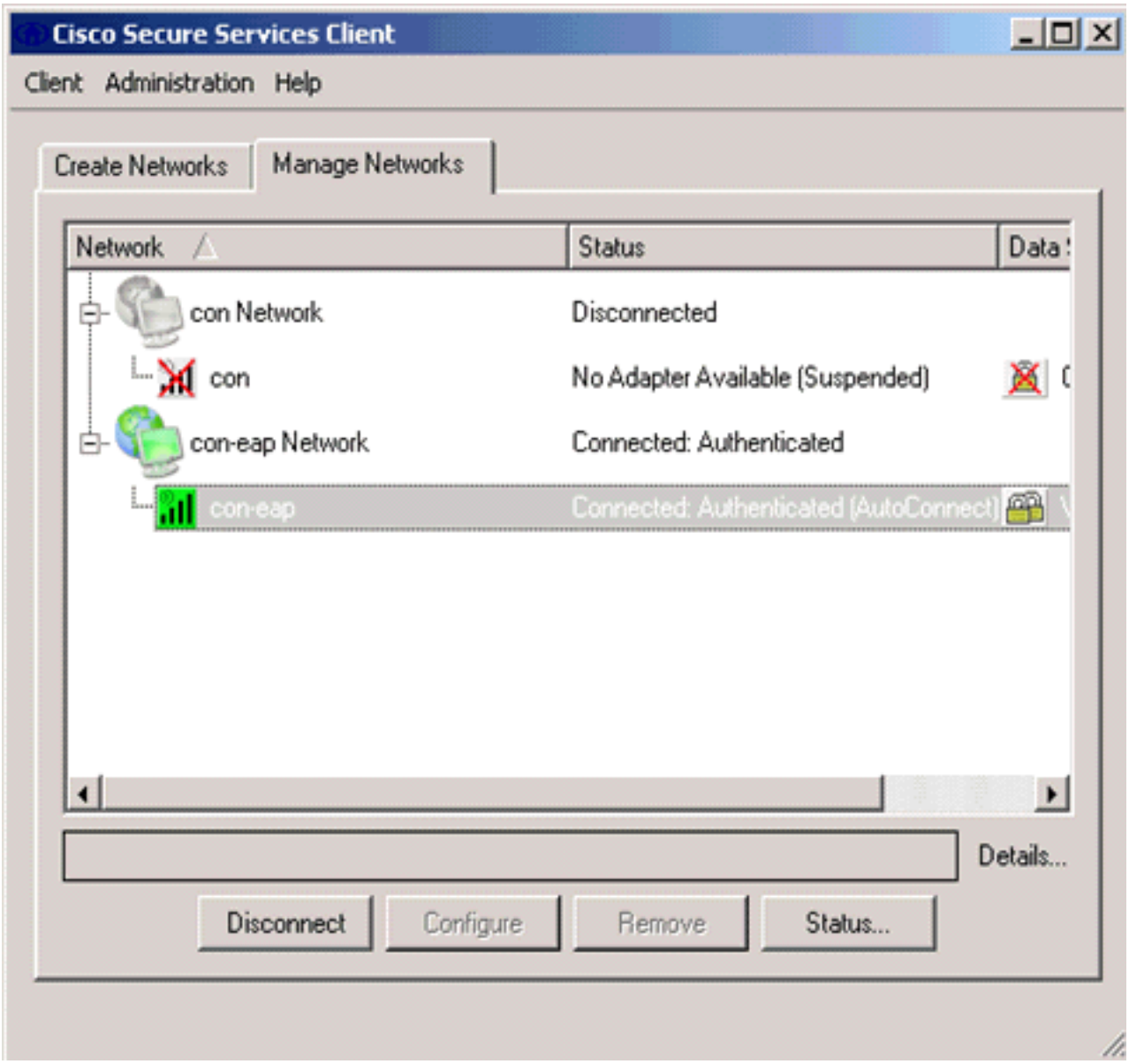


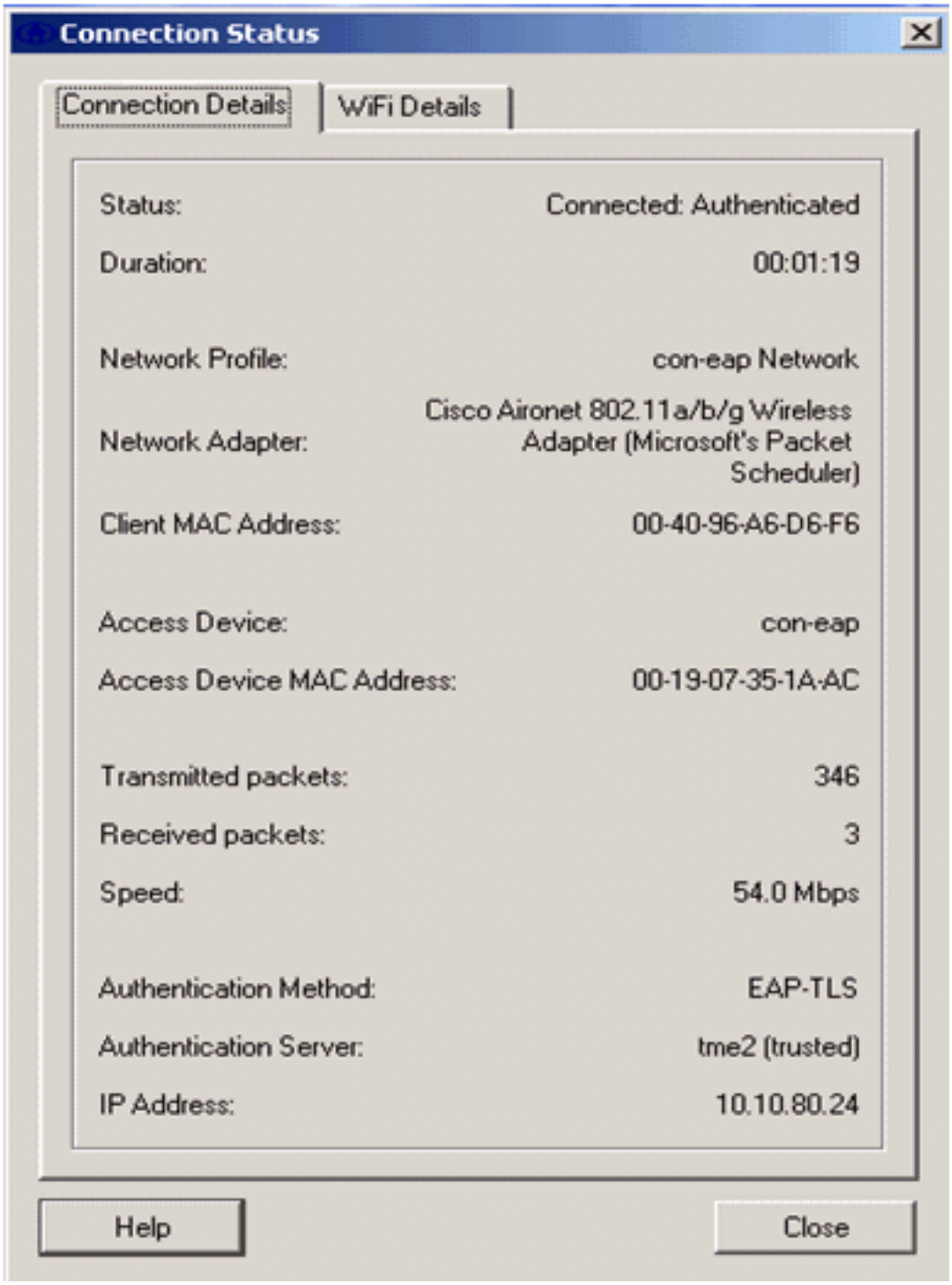
El

Cisco Secure Services Client recibe el certificado de servidor y lo controla (con la regla configurada y las autoridades de certificación instaladas). Entonces pide el certificado utilizar para el usuario.

11. Después de que el cliente autentique, elija el **SSID** bajo perfil en la tabulación de las redes del manejo y haga clic el **estatus** para preguntar los detalles de la conexión.La ventana de los detalles de la conexión proporciona a la información en el dispositivo cliente, el estado de la conexión y las estadísticas, y el método de autenticación. La tabulación de los detalles de WiFi proporciona a los detalles en el estado de la conexión del 802.11, que incluye el RSSI, el canal del 802.11, y la autenticación/el 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 el OIT para ver un análisis de la **salida del comando show**.

Note: Refiera a la información importante en los comandos Debug antes de que usted utilice los **comandos debug**.

Estos comandos debug pueden ser empleados en el WLC para vigilar el progreso del intercambio de la autenticación:

- **permiso de los eventos aaa de la depuración**
- **permiso del detalle aaa de la depuración**
- **permiso de los eventos de la depuración dot1x**

- permiso de los estados de la depuración dot1x
- permiso local-auth de los eventos del eap aaa de la depuraciónO
- 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