Cisco Secure Services Client con el ejemplo de configuración PEAP/GTC WPA

Contenido

Introducción

Este documento describe cómo configurar el Acceso protegido de Wi-Fi (WPA) protegido de la placa Token del protocolo extensible authentication (PEAP) /Generic (GTC) en el Cisco Secure Services Client.

prerrequisitos

Componentes Utilizados

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

- Versión 4.0 del Cisco Secure Services ClientEl Cisco Secure Services Client está disponible para la descarga del centro de software de Cisco.com (clientes registrados solamente).
- Windows XP SP2 o 2000 mínimos SP4

Convenciones

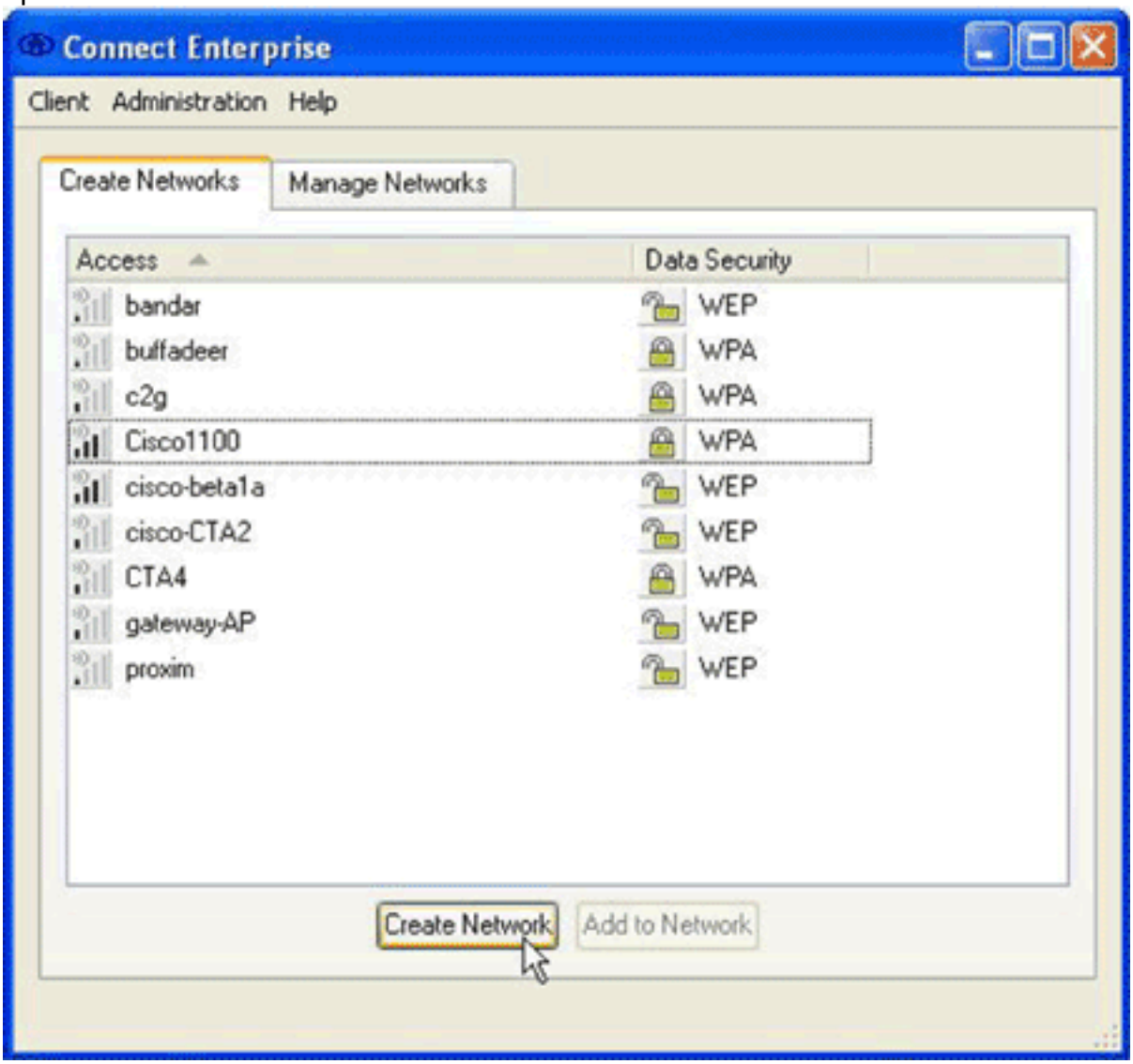
Para más información sobre las convenciones sobre documentos, consulte Convenciones sobre Consejos Técnicos de Cisco.

Configure al Cisco Secure Services Client con PEAP/GTC WPA

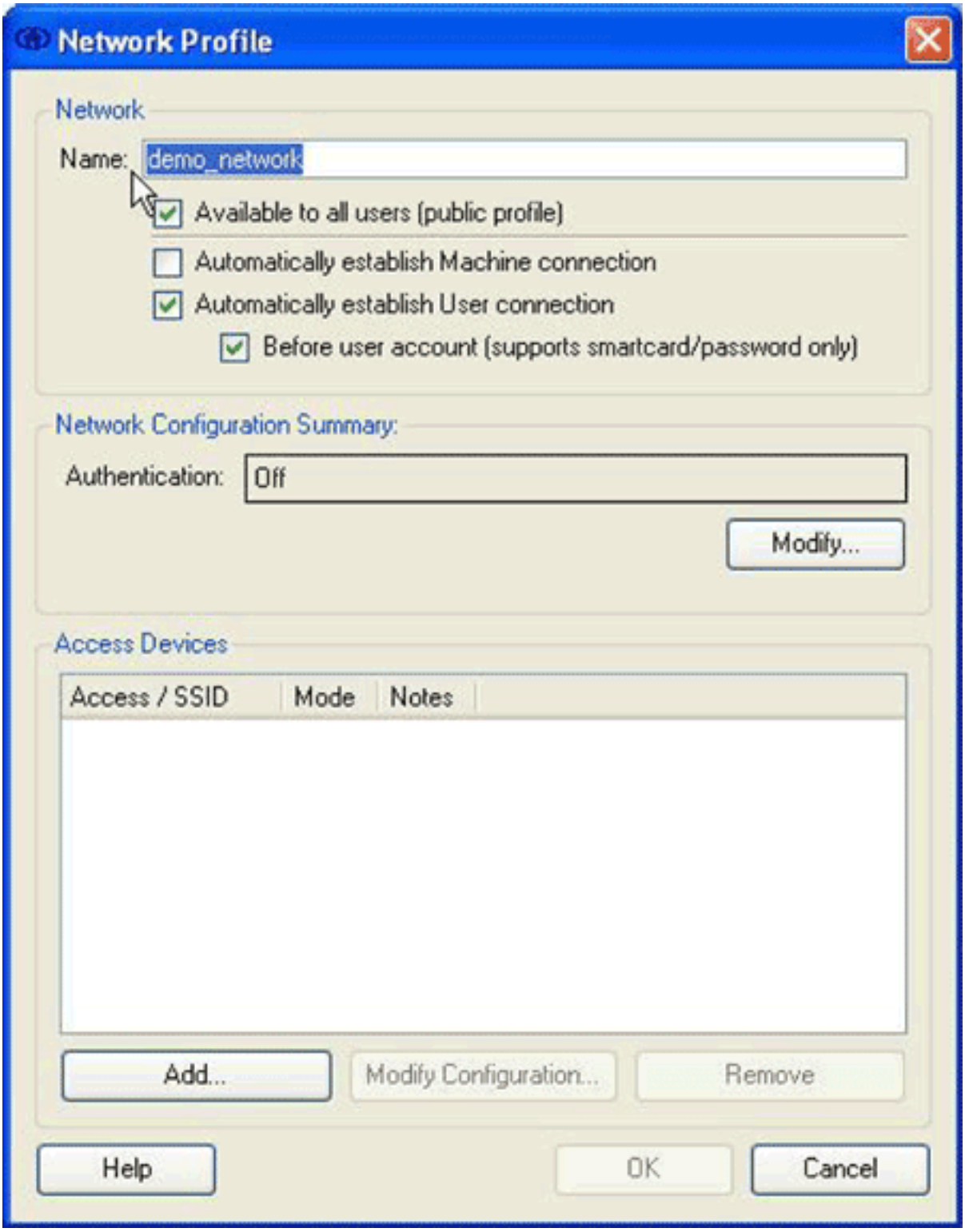
Para configurar al Cisco Secure Services Client con PEAP/GTC WPA, complete estos pasos:

1. Haga clic con el botón derecho del ratón el icono de bandeja del sistema del Cisco Secure Services Client, y elija **abierto**.**Nota:** Si usted no está conectado con una red, su icono de

bandeja del sistema es oscuro.El cuadro de diálogo de la empresa de la conexión aparece.



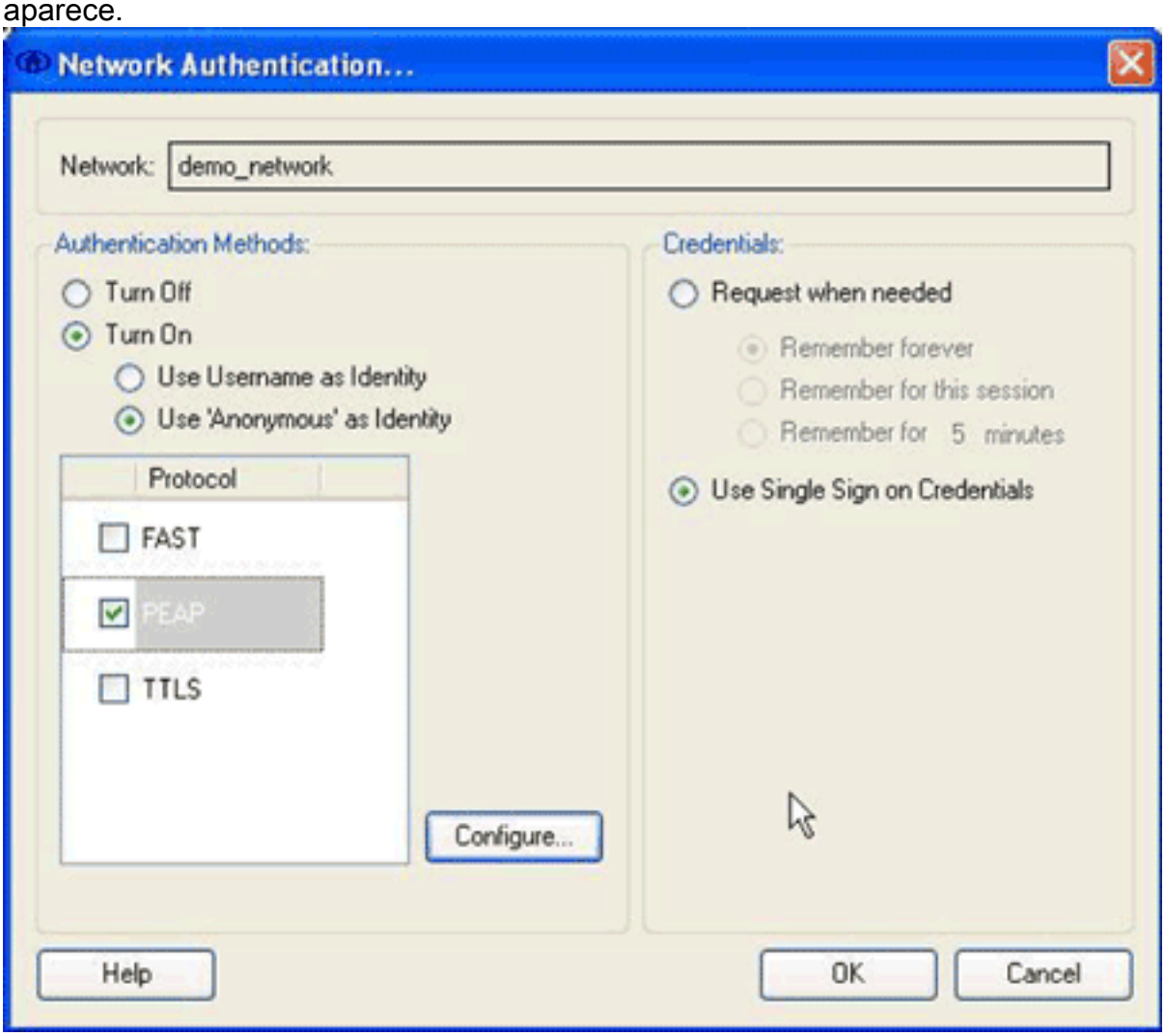
2. Haga clic la lengueta de las **redes del crear**.El área de las redes del crear visualiza las redes que transmiten su Service Set Identifier (SSID).
3. Haga clic el botón de la **red del crear**.El cuadro de diálogo del perfil de la red aparece.



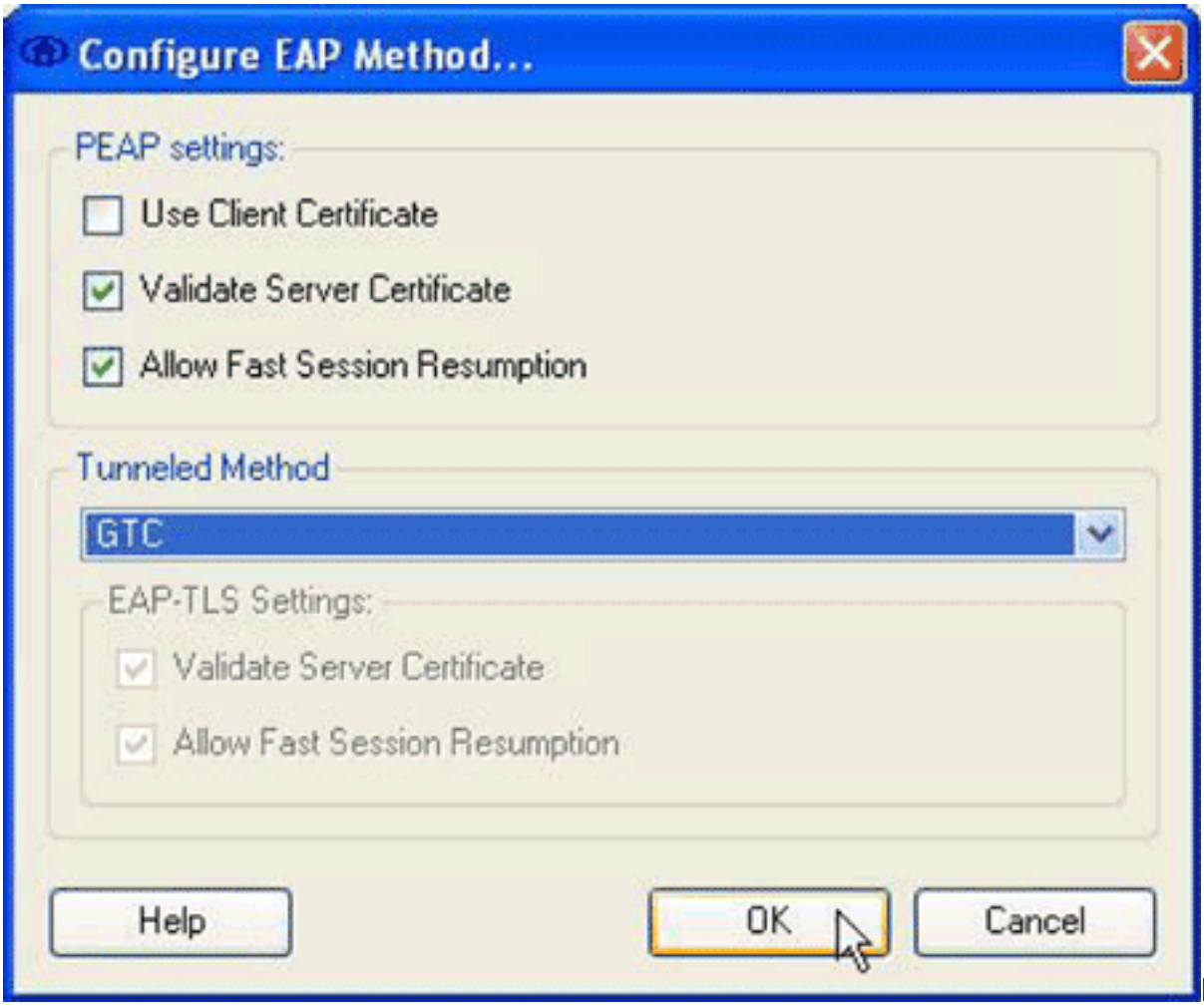
4. En la área de red, configure estas opciones:En el campo de nombre, ingrese un nombre para su red.Este nombre aparece como el SSID para esta red. Por este ejemplo, el nombre es *demo_network*.Marque el **disponible a toda la** casilla de verificación de los **usuarios (perfil público)**.Marque **automáticamente la** casilla de verificación de la **conexión del usuario del establecimiento**, y verifique la máquina del establecimiento casilla de verificación de conexión no se marca automáticamente.Marque **antes de la** casilla de verificación de la **cuenta de usuario (tarjeta inteligente/contraseña de los soportes solamente)**.**Nota:** Cuando **antes de que** se marque la casilla de verificación de la **cuenta de usuario (tarjeta inteligente/contraseña de los soportes solamente)**, la autenticación procede inmediatamente después que se ingresan las credenciales, pero antes de que ocurre el inicio de sesión del dominio. Si usted utiliza los Certificados de usuario, no marque **antes de la** casilla de verificación de la **cuenta de usuario (tarjeta inteligente/contraseña de los soportes**

solamente). Porque no están disponibles antes del inicio de Windows, usted no puede utilizar los Certificados de usuario con los inicios de sesión del dominio.

5. En el área sumaria de la configuración de red, haga clic el **botón Modify Button**.El cuadro de diálogo de la autenticación de red
aparece.

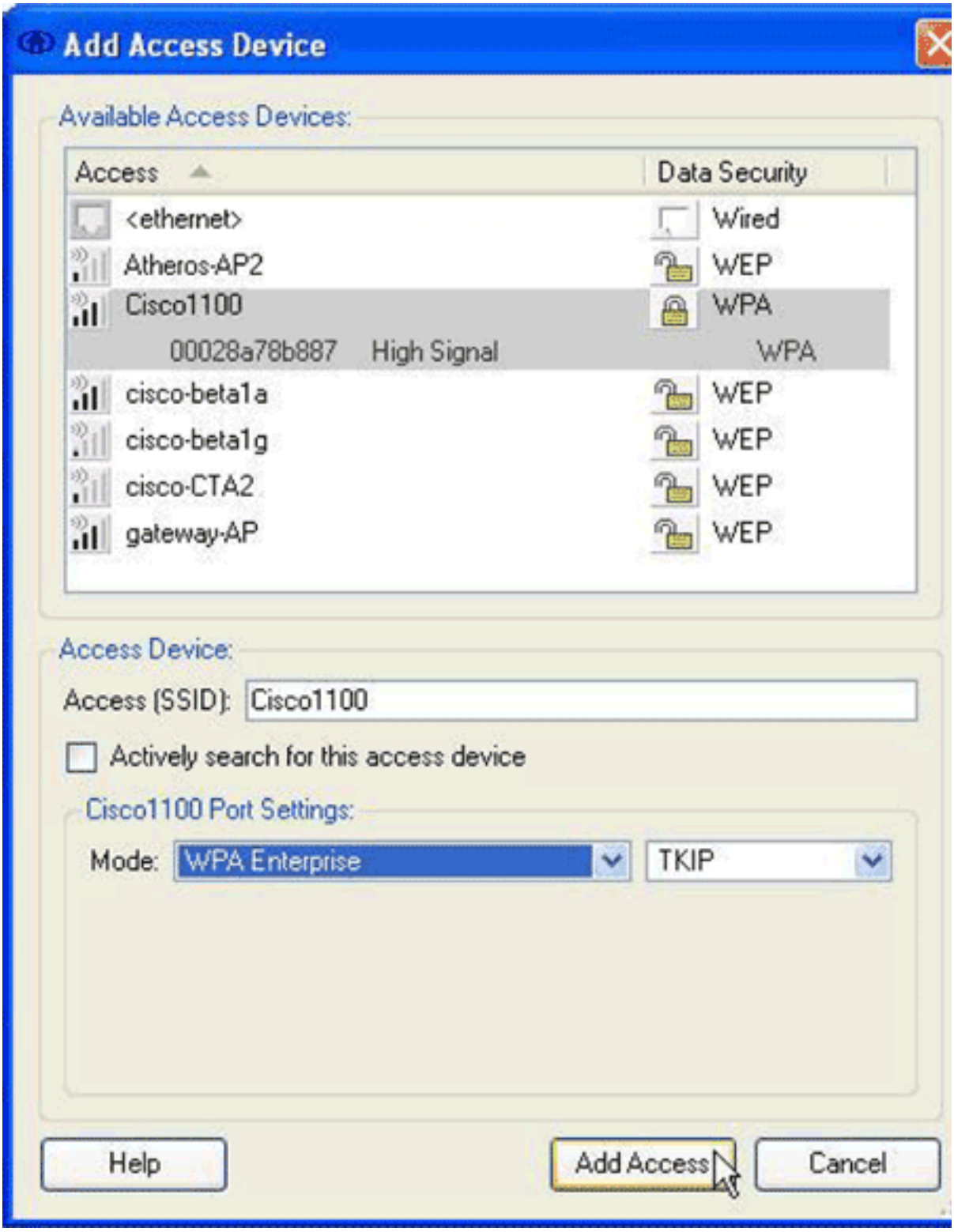


6. En el cuadro de diálogo de la autenticación de red, configure estas opciones:En el área de las credenciales, haga clic la **sola muestra del uso en el** botón de radio de las **credenciales**.En el área de los métodos de autentificación, haga clic la **vuelta en el** botón de radio, y después haga clic el **uso “anónimo” como identidad**.La vuelta en el botón de radio puebla la lista del protocolo visualizada en el área de los métodos de autentificación. El uso “anónimo” como botón de radio de la identidad limita la lista solamente a los Protocolos de autenticación tunneled.Marque la casilla de verificación **PEAP**, y después haga clic la **configuración**.El cuadro de diálogo del método EAP de la configuración
aparece.



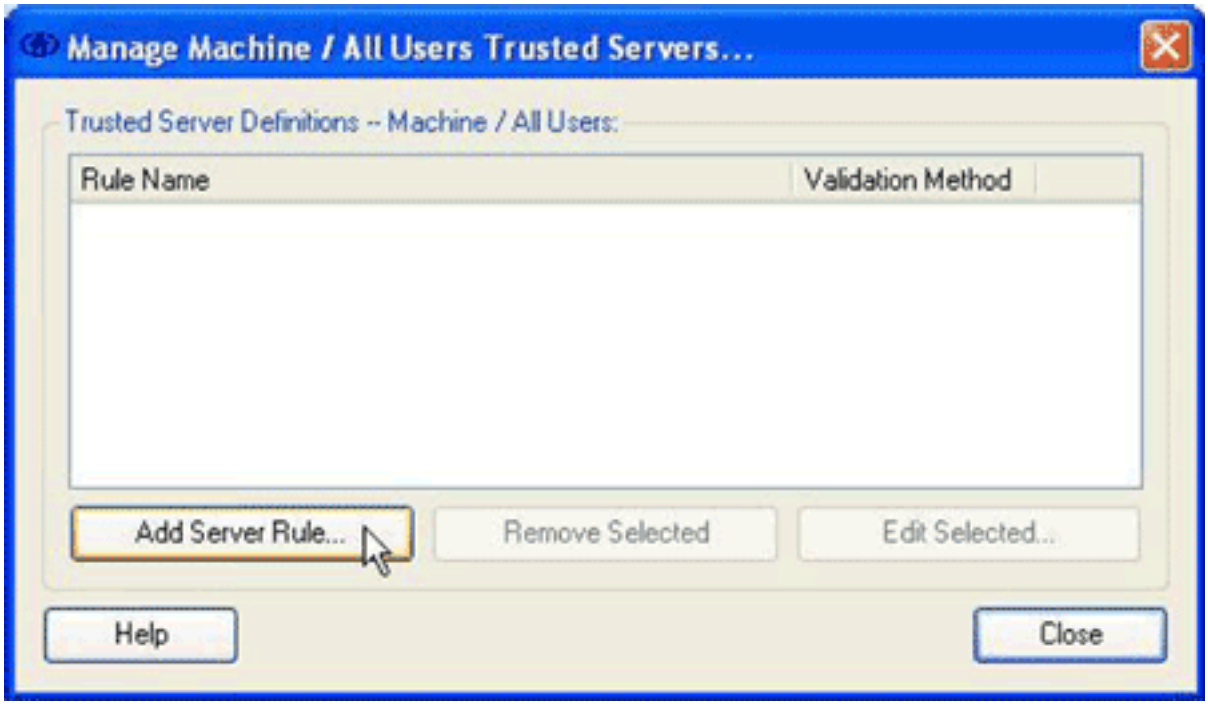
Desmarque la casilla de verificación del **certificado del cliente del uso**.Marque el **certificado de servidor del validar** y **permita las** casillas de verificación **rápidas de la reanudación de la sesión**.Del menú desplegable tunneled del método, elija el **GTC**.Haga Click en OK a volver al cuadro de diálogo de la autenticación de red, y después para hacer clic la **AUTORIZACIÓN** para volver al cuadro de diálogo del perfil de la red.

7. En el área de los dispositivos de acceso del cuadro de diálogo del perfil de la red, haga click en AddEl cuadro de diálogo del dispositivo de acceso del agregar aparece.

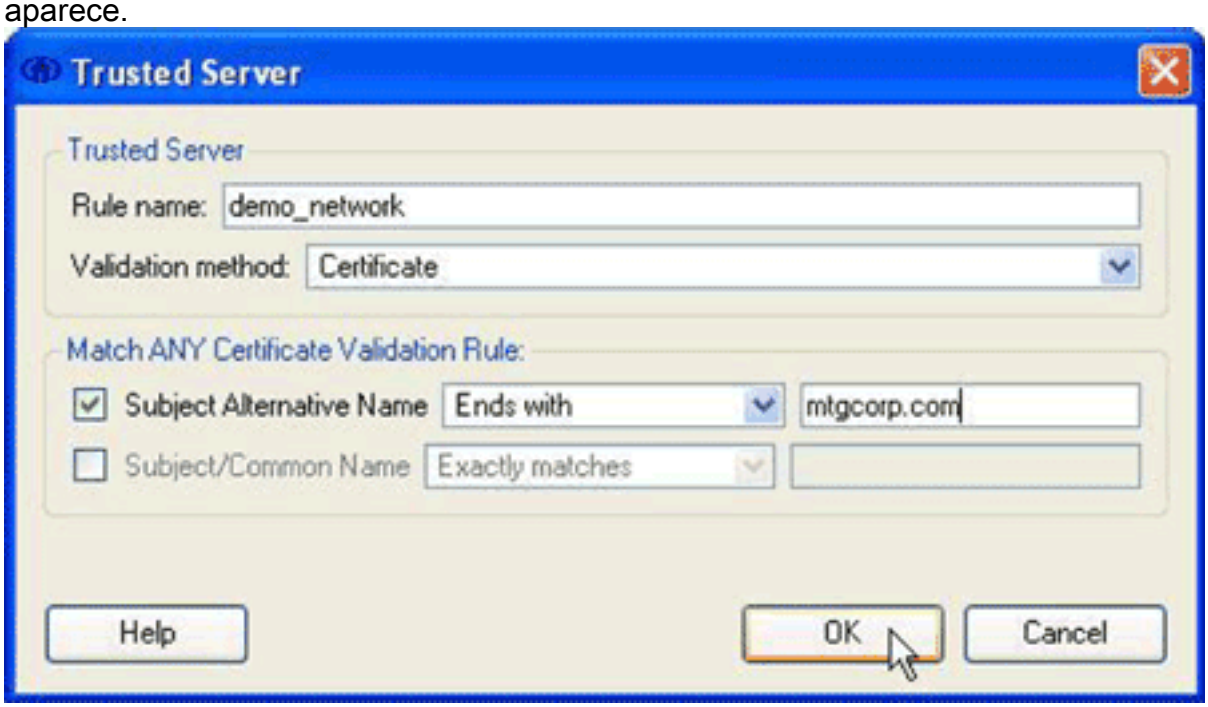


8. En el cuadro de diálogo de los dispositivos de acceso del agregar, elija el dispositivo que usted quiere configurar, y después haga clic **agregan el acceso**.**Nota:** Si el dispositivo que usted quiere configurar está dentro de rango, el SSID para ese dispositivo aparece en la lista de dispositivos de acceso disponible. Si no aparece el dispositivo, ingrese el SSID para el dispositivo en el campo del acceso (SSID), ingrese las configuraciones de puerto en el área de las configuraciones de puerto del Cisco 1100, y después haga clic **agregan el acceso**.
9. En el cuadro de diálogo del perfil de la red, **AUTORIZACIÓN del** tecleo a volver al cuadro de diálogo de la empresa de la conexión.
10. En el cuadro de diálogo de la empresa de la conexión, elija los **servidores de confianza > manejan la máquina/todos los servidores confiados en los usuarios del** menú del cliente.La máquina del manejo/todos los usuarios confiaba en que cuadro de diálogo aparecen de los

servidores.



11. El tecleo **agrega la regla del servidor**.El cuadro de diálogo de confianza del servidor aparece.



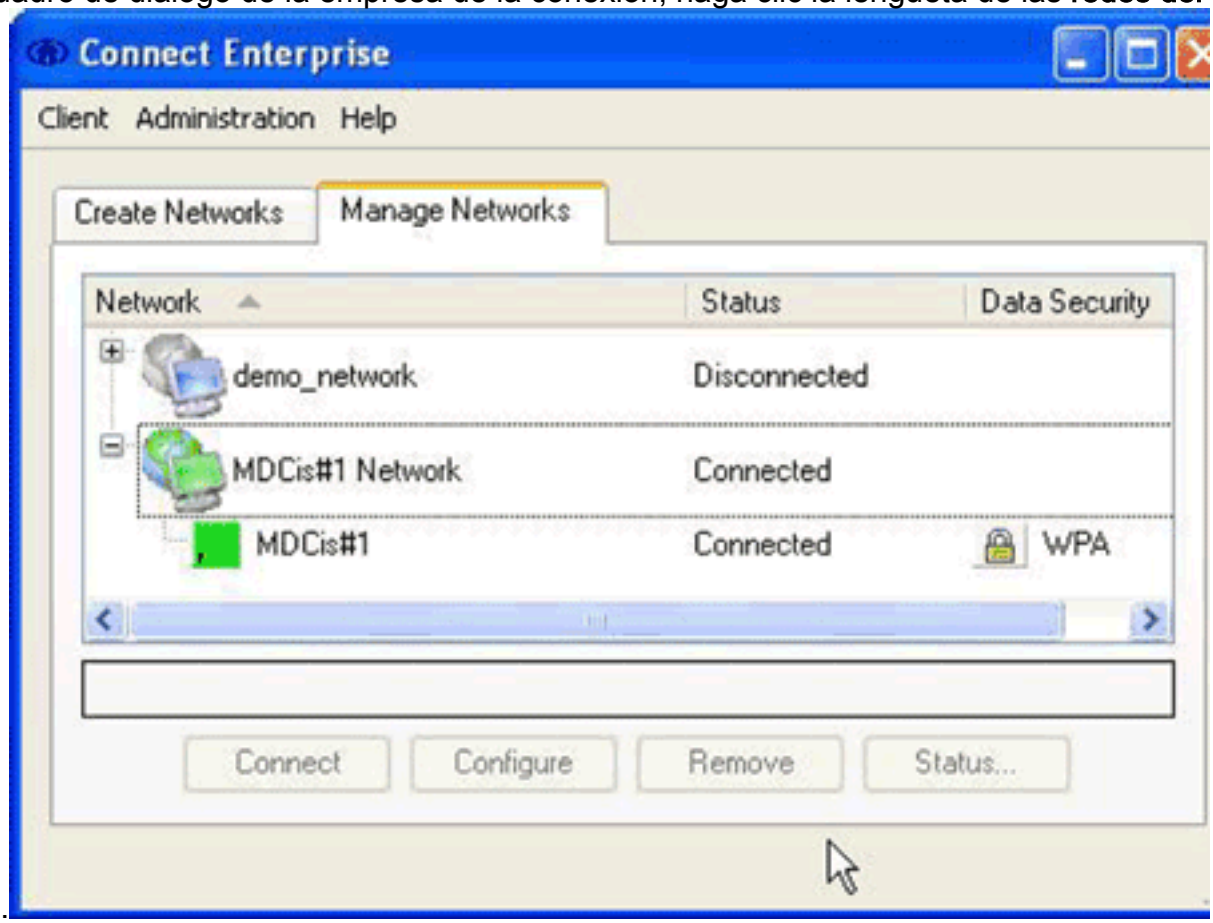
12. En el cuadro de diálogo de confianza del servidor, configure estas opciones:En el campo de nombre de la regla, ingrese un nombre para la regla.Del menú desplegable del método de la validación, elija el **certificado**.En la coincidencia CUALQUIER área de la regla de la validación de certificado, configura las opciones para la regla.Para construir una regla, usted debe saber que el contenido del certificado de servidor y ingresar esos valores en el emparejamiento CUALQUIER validación de certificado gobierna el área. Por ejemplo, si el nombre alternativo sujeto contiene el Domain Name de un servidor, *mtgcorpserver.mtgcorp.com*, elige los **extremos con del** menú desplegable alternativo sujeto del nombre, y después ingresa **mtgcorp.com** en el campo de texto.El Haga Click en OK a volver a la máquina del manejo/a todos los usuarios confiaba en el cuadro de diálogo de los servidores.
13. En la máquina del manejo/todos los usuarios confiaba en el cuadro de diálogo de los

servidores, hacen clic **cerca de la** vuelta al cuadro de diálogo de la empresa de la conexión. La configuración es completa, y

Conecte con la red

Para conectar con su nueva red, complete estos pasos:

1. En el cuadro de diálogo de la empresa de la conexión, haga clic la lengueta de las **redes del manejo**.



2. Desconecte de cualquier red que esté conectada con el adaptador usado por su nueva red.
3. De la lista de red, seleccione el nuevo perfil de la red, y el tecleo **conecta**.

Sobre la configuración exitosa y la conexión, las visualizaciones del icono de bandeja del sistema del Cisco Secure Services Client se ponen verde.

Nota: Si el Software de protección contra virus está instalado en su ordenador y se configura para analizar el directorio del registro del Cisco Secure Services Client, usted puede experimentar CPU elevada los ciclos con la autenticación de Cisco Secure Services Client. Para mejorar el funcionamiento, configure su Software de protección contra virus para excluir el directorio del registro del Cisco Secure Services Client.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems