Cisco Secure Services Client con autenticación EAP-FAST

Contenido

Introducción

Este documento describe cómo configurar Cisco Secure Services Client (CSSC) con Wireless LAN Controllers, software Microsoft Windows 2000® y Cisco Secure Access Control Server (ACS) 4.0 mediante EAP-FAST. Este documento presenta la arquitectura EAP-FAST y proporciona ejemplos de implementación y configuración. CSSC es el componente de software de cliente que proporciona la comunicación de las credenciales de usuario a la infraestructura para autenticar un usuario para la red y asignar el acceso apropiado.

Estas son algunas de las ventajas de la solución CSSC, como se describe en este documento:

- Autenticación de cada usuario (o dispositivo) antes del permiso de acceso a WLAN/LAN con

protocolo de autenticación extensible (EAP)
- Solución de seguridad WLAN integral con componentes de servidor, autenticador y cliente
- Solución común para la autenticación por cable e inalámbrica
- Teclas de cifrado dinámicas por usuario derivadas en el proceso de autenticación
- No se requiere infraestructura de clave pública (PKI) ni certificados (la verificación de certificados es opcional)
- Asignación de políticas de acceso y/o marco EAP habilitado para NAC

Nota: Refiérase a Cisco SAFE Wireless Blueprint para obtener información sobre la implementación de tecnología inalámbrica segura.

El marco de autenticación 802.1x se ha incorporado como parte del estándar 802.11i (Wireless LAN Security) para habilitar funciones de autenticación, autorización y contabilidad basadas en capa 2 en una red LAN inalámbrica 802.11. Actualmente, hay varios protocolos EAP disponibles para su implementación en redes por cable e inalámbricas. Los protocolos EAP implementados habitualmente incluyen LEAP, PEAP y EAP-TLS. Además de estos protocolos, Cisco ha definido e implementado el protocolo EAP Flexible Authentication a través del túnel seguro (EAP-FAST) como un protocolo EAP basado en estándares disponible para su implementación en redes LAN por cable e inalámbricas. La especificación del protocolo EAP-FAST está disponible públicamente en el sitio de IETF.

Al igual que con otros protocolos EAP, EAP-FAST es una arquitectura de seguridad cliente-servidor que cifra las transacciones EAP dentro de un túnel TLS. Aunque es similar a PEAP o EAP-TTLS en este sentido, difiere en que el establecimiento de túnel EAP-FAST se basa en claves secretas compartidas seguras que son únicas para cada usuario en comparación con PEAP/EAP-TTLS (que utilizan un certificado X.509 de servidor para proteger la sesión de autenticación). Estas claves secretas compartidas se denominan Credenciales de acceso protegido (PAC) y se pueden distribuir automáticamente (aprovisionamiento automático o en banda) o manualmente (aprovisionamiento manual o fuera de banda) a los dispositivos cliente. Debido a que los apretones de manos basados en secretos compartidos son más eficientes que los apretones de manos basados en una infraestructura PKI, EAP-FAST es el tipo EAP más rápido y menos intensivo de procesador de aquellos que proporcionan intercambios de autenticación protegidos. EAP-FAST también está diseñado para facilitar la implementación, ya que no requiere un certificado en el cliente de LAN inalámbrica ni en la infraestructura RADIUS, pero incorpora un mecanismo de aprovisionamiento integrado.

Estas son algunas de las principales capacidades del protocolo EAP-FAST:

- Inicio de sesión único (SSO) con nombre de usuario/contraseña de Windows
- Compatibilidad con ejecución de secuencia de comandos de inicio de sesión
- Compatibilidad con acceso Wi-Fi protegido (WPA) sin suplicante de terceros (solo para Windows 2000 y XP)
- Implementación sencilla sin necesidad de infraestructura PKI
- Antigüedad de la contraseña de Windows (es decir, compatibilidad con vencimiento de la contraseña basada en servidor)
- Integración con Cisco Trust Agent para Network Admission Control con el software de cliente adecuado

Prerequisites

Requisito

Se supone que el instalador tiene conocimiento de la instalación básica de Windows 2003 y de la instalación de Cisco WLC, ya que este documento sólo cubre las configuraciones específicas para facilitar las pruebas.

Para obtener información de configuración e instalación inicial para los Cisco 4400 Series Controllers, refiérase a la Guía de Inicio Rápido: Controladores LAN inalámbricos Cisco de la serie 4400. Para obtener información de configuración e instalación inicial para los Cisco 2000 Series Controllers, refiérase a la Guía de Inicio Rápido: Controladores LAN inalámbricos Cisco de la serie 2000.

Antes de comenzar, instale Microsoft Windows Server 2000 con el software de Service Pack más reciente. Instale los controladores y los puntos de acceso ligeros (LAP) y asegúrese de que se configuran las últimas actualizaciones de software.

Componentes Utilizados

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

- Controlador de la serie Cisco 2006 o 4400 que ejecuta 4.0.155.5
- Cisco 1242 LWAPP AP
- Windows 2000 con Active Directory
- Switch Cisco Catalyst 3750G
- Windows XP con tarjeta de adaptador CB21AG y Cisco Secure Services Client versión 4.05

Convenciones

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

Parámetros de diseño

Base de datos

Cuando se implementa una red WLAN y se busca un protocolo de autenticación, normalmente se desea utilizar una base de datos actual para la autenticación de usuario/máquina. Las bases de datos típicas que se pueden utilizar son Windows Active Directory, LDAP o una base de datos de una contraseña única (OTP) (es decir, RSA o SecureID). Todas estas bases de datos son compatibles con el protocolo EAP-FAST, pero cuando planifica la implementación, hay algunos requisitos de compatibilidad que deben tenerse en cuenta. La implementación inicial de un archivo PAC en los clientes se realiza mediante el aprovisionamiento automático anónimo, el aprovisionamiento autenticado (a través del certificado X.509 del cliente actual) o el aprovisionamiento manual. A los efectos de este documento, se consideran el aprovisionamiento automático anónimo y el aprovisionamiento manual.

El aprovisionamiento automático de PAC utiliza el protocolo de acuerdo clave Diffie-Hellman autenticado (ADHP) para establecer un túnel seguro. El túnel seguro se puede establecer de forma anónima o a través de un mecanismo de autenticación del servidor. Dentro de la conexión de túnel establecida, MS-CHAPv2 se utiliza para autenticar al cliente y, tras la autenticación exitosa, para distribuir el archivo PAC al cliente. Una vez que el PAC se ha aprovisionado

correctamente, el archivo PAC se puede utilizar para iniciar una nueva sesión de autenticación EAP-FAST para obtener acceso seguro a la red.

El aprovisionamiento automático de PAC es relevante para la base de datos en uso porque, dado que el mecanismo de aprovisionamiento automático se basa en MSCHAPv2, la base de datos utilizada para autenticar a los usuarios debe ser compatible con este formato de contraseña. Si utiliza EAP-FAST con una base de datos que no admite el formato MSCHAPv2 (como OTP, Novell o LDAP), es necesario emplear algún otro mecanismo (es decir, aprovisionamiento manual o aprovisionamiento autenticado) para implementar archivos PAC de usuario. Este documento proporciona un ejemplo de aprovisionamiento automático con una base de datos de usuarios de Windows.

Cifrado

La autenticación EAP-FAST no requiere el uso de un tipo de encripción WLAN específico . El tipo de encripción WLAN que se va a utilizar viene determinado por las capacidades de la tarjeta NIC del cliente. Se recomienda emplear la encriptación WPA2 (AES-CCM) o WPA(TKIP), en función de las capacidades de la tarjeta NIC en la implementación específica. Tenga en cuenta que la solución WLAN de Cisco permite la coexistencia de dispositivos cliente WPA2 y WPA en un SSID común.

Si los dispositivos cliente no admiten WPA2 o WPA, es posible implementar la autenticación 802.1X con claves WEP dinámicas, pero, debido a las vulnerabilidades conocidas contra las claves WEP, no se recomienda este mecanismo de encriptación WLAN. Si se requiere para admitir clientes solo WEP, se recomienda emplear un intervalo de tiempo de espera de sesión, que requiere que los clientes deriven una nueva clave WEP en un intervalo frecuente. Treinta minutos es el intervalo de sesión recomendado para las velocidades de datos WLAN típicas.

Credenciales de inicio de sesión único y máquina

El inicio de sesión único hace referencia a la capacidad de un único usuario para iniciar sesión o introducir credenciales de autenticación para acceder a varias aplicaciones o a varios dispositivos. A los efectos de este documento, Inicio de sesión único se refiere al uso de las credenciales que se utilizan para iniciar sesión en un equipo para la autenticación en la WLAN.

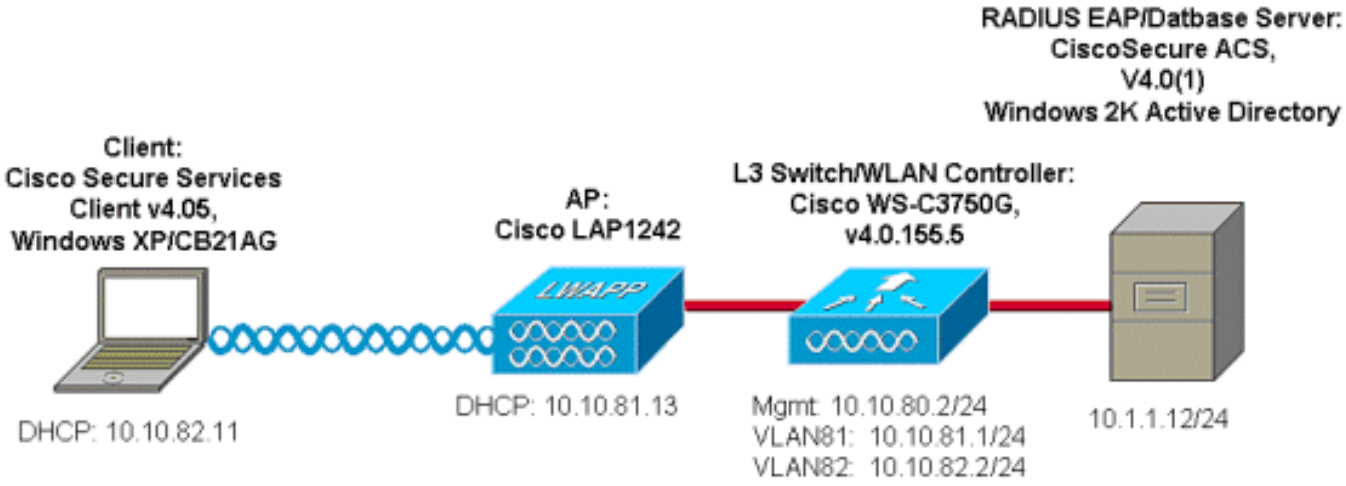
Con Cisco Secure Services Client, es posible utilizar las credenciales de inicio de sesión de un usuario para autenticarse también en la red WLAN. Si desea autenticar una PC en la red antes de que el usuario inicie sesión en la PC, es necesario utilizar las credenciales de usuario almacenadas o las credenciales vinculadas a un perfil de máquina. Cualquiera de estos métodos es útil en los casos en los que se desea ejecutar secuencias de comandos de inicio de sesión o asignar unidades cuando se inicia el PC, a diferencia de cuando un usuario inicia sesión.

Diagrama de la red

Este es el diagrama de red utilizado en este documento. En esta red, se utilizan cuatro subredes. Tenga en cuenta que no es necesario segmentar estos dispositivos en diferentes redes, pero esto ofrece la mayor flexibilidad para la integración con redes reales. El controlador de LAN inalámbrica integrado Catalyst 3750G proporciona puertos de switch Power Over Ethernet (POE), switching L3 y capacidad de controlador WLAN en un chasis común.

1. La red 10.1.1.0 es la red de servidor donde reside el ACS.

2. La red 10.10.80.0 es la red de administración utilizada por el controlador WLAN.
3. La red 10.10.81.0 es la red donde residen los AP.
4. La red 10.10.82.0 se utiliza para los clientes WLAN.



Configuración del servidor de control de acceso (ACS)

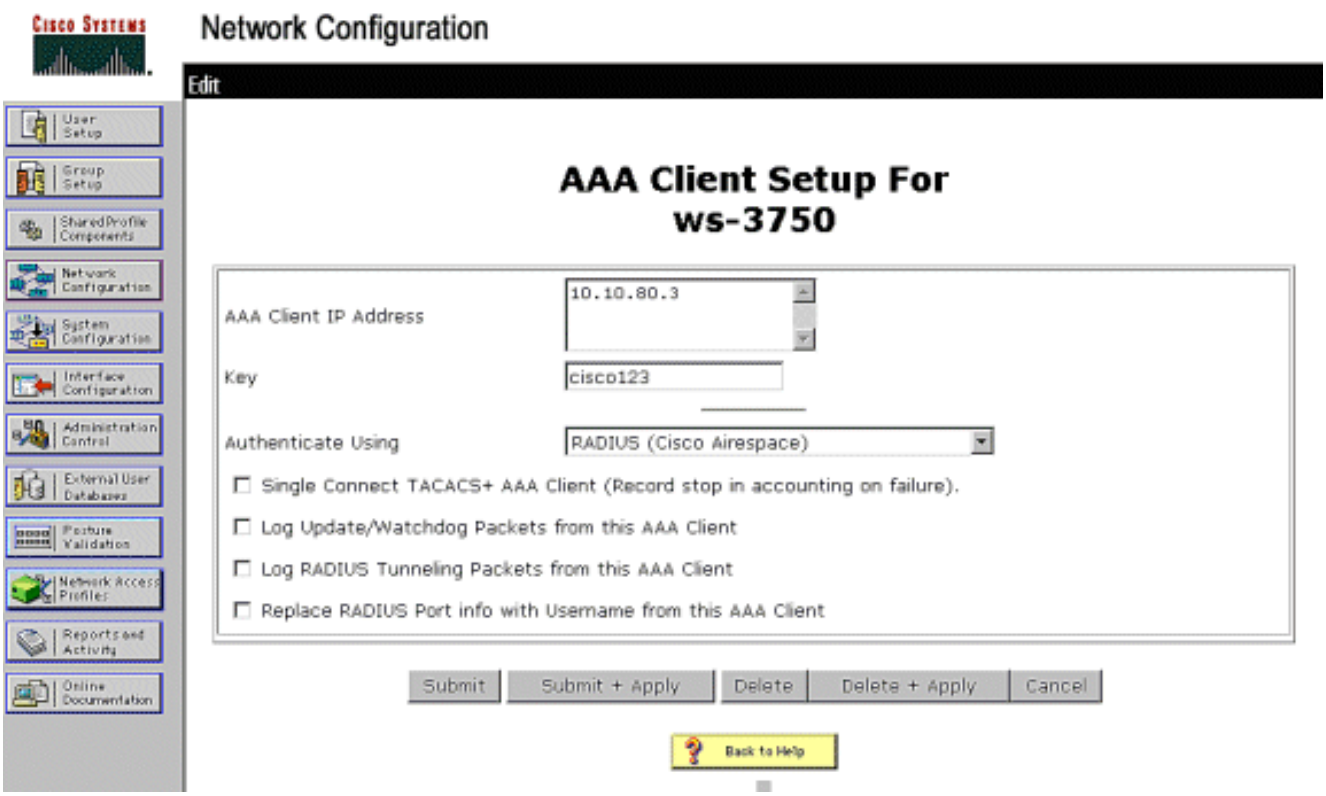
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Agregar punto de acceso como cliente AAA (NAS) en ACS

Esta sección describe cómo configurar ACS para EAP-FAST con aprovisionamiento PAC en banda con Windows Active Directory como base de datos externa.

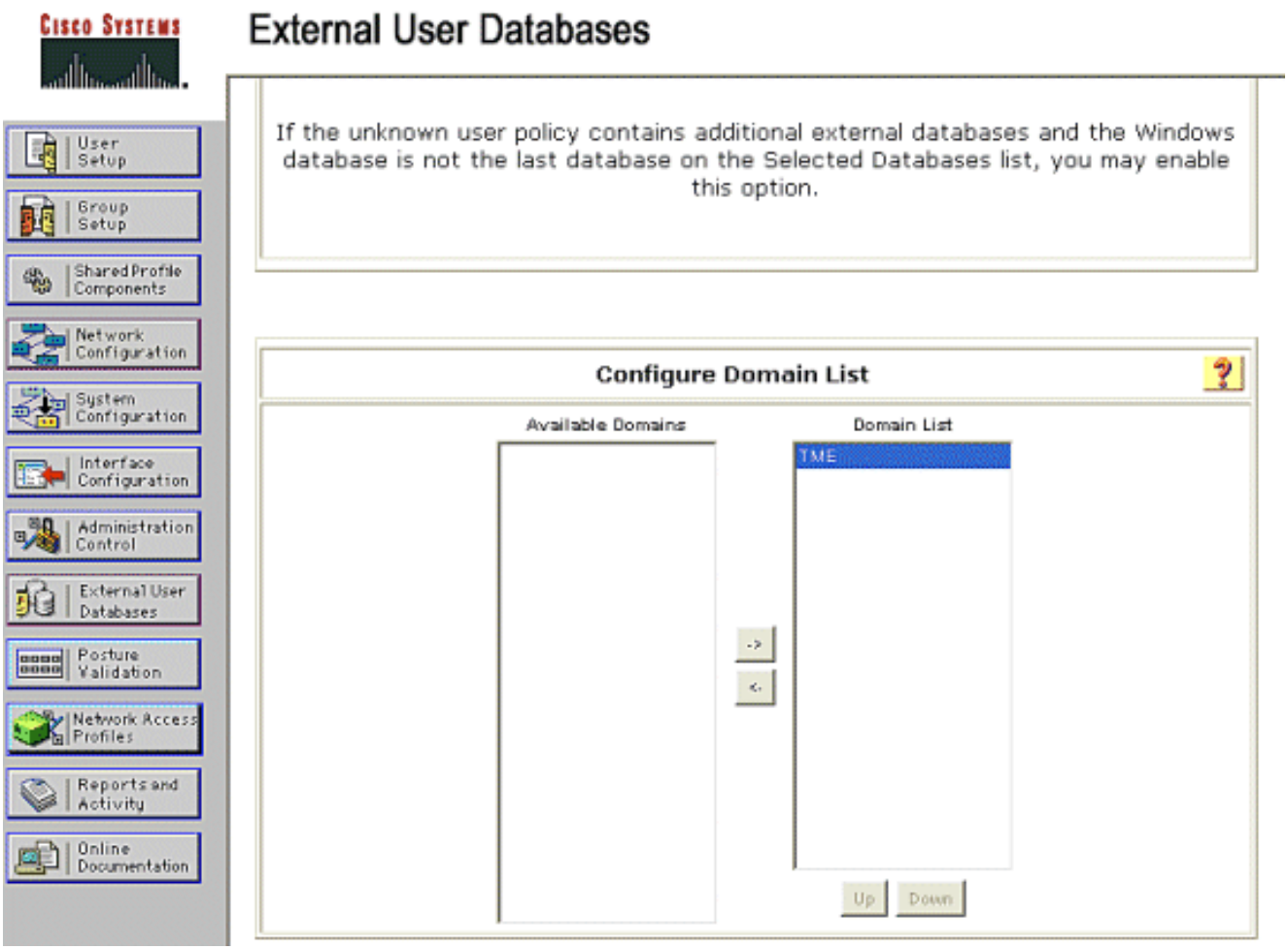
1. Inicie sesión en **ACS > Configuración de red** y haga clic en **Agregar entrada**.
2. Introduzca el nombre del controlador WLAN, la dirección IP, la clave secreta compartida y, en Autenticar mediante, seleccione RADIUS (Cisco Airespace), que también incluye los atributos RADIUS IETF.**Nota:** Si los grupos de dispositivos de red (NDG) están habilitados, primero elija el NDG adecuado y añada el controlador WLAN a él. Consulte la Guía de Configuración de ACS para obtener detalles sobre el NDG.
3. Haga clic en **Submit+**
   Restart.



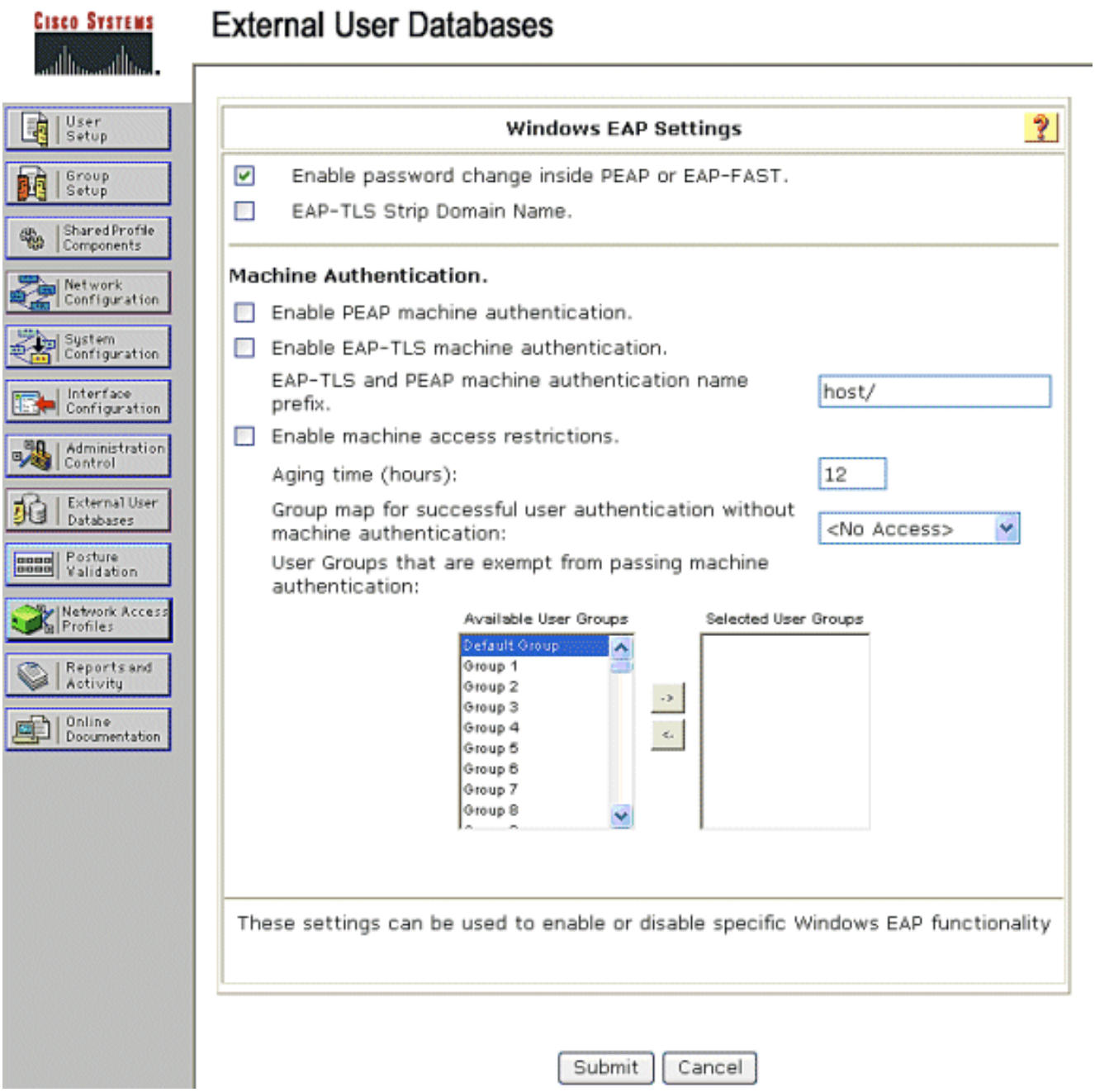
Configure ACS para consultar la base de datos externa

Esta sección describe cómo configurar el ACS para consultar la base de datos externa.

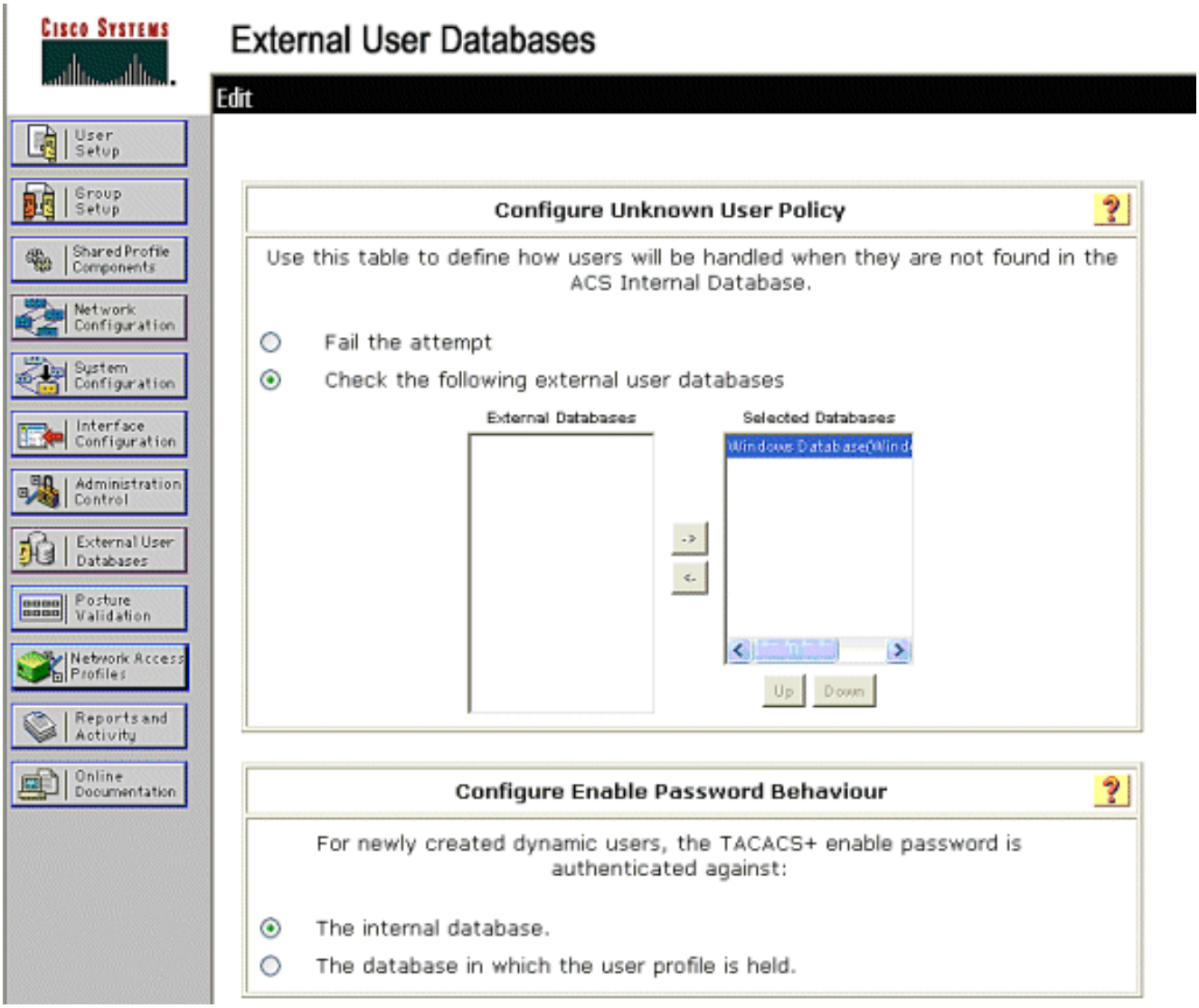
1. Haga clic en **Base de datos de usuario externa > Configuración de base de datos > Base de datos de Windows > Configurar**.
2. En Configure Domain List (Configurar lista de dominios), mueva **Domains** de Available Domains a Domain List (Lista de dominios disponibles).**Nota:** El servidor que ejecuta el ACS debe tener conocimiento de estos dominios para que la aplicación ACS detecte y use esos dominios con fines de
autenticación.



3. En Windows EAP Settings, configure la opción para permitir el cambio de contraseña dentro de la sesión PEAP o EAP-FAST. Refiérase a la Guía de Configuración de Cisco Secure ACS 4.1 para obtener más detalles sobre EAP-FAST y el envejecimiento de la contraseña de Windows.
4. Haga clic en Submit (Enviar).**Nota:** También puede habilitar la función de permiso de marcación para EAP-FAST en la configuración de base de datos de usuario de Windows para permitir que la base de datos externa de Windows controle el permiso de acceso. La configuración de MS-CHAP para el cambio de contraseña en la página de configuración de la base de datos de Windows sólo se aplica a la autenticación MS-CHAP no EAP. Para habilitar el cambio de contraseña junto con EAP-FAST, es necesario habilitar el cambio de contraseña en la Configuración EAP de
Windows.



5. Haga clic en **Base de datos de usuario externa > Directiva de usuario desconocida** y elija el botón de opción **Verificar las siguientes bases de datos de usuario externas**.
6. Mover la base de datos de Windows de **bases de datos externas** a **bases de datos seleccionadas**.
7. Haga clic en Submit (Enviar).**Nota:** A partir de este punto, el ACS verifica la base de datos de Windows. Si el usuario no se encuentra en la base de datos local ACS, coloca al usuario en el grupo predeterminado ACS. Consulte la documentación de ACS para obtener más detalles sobre las Asignaciones de Grupos de Bases de Datos.**Nota:** A medida que el ACS consulta la base de datos de Microsoft Active Directory para verificar las credenciales del usuario, es necesario configurar parámetros de derechos de acceso adicionales en Windows. Refiérase a la Guía de Instalación de Cisco Secure ACS para Windows Server para obtener
detalles.



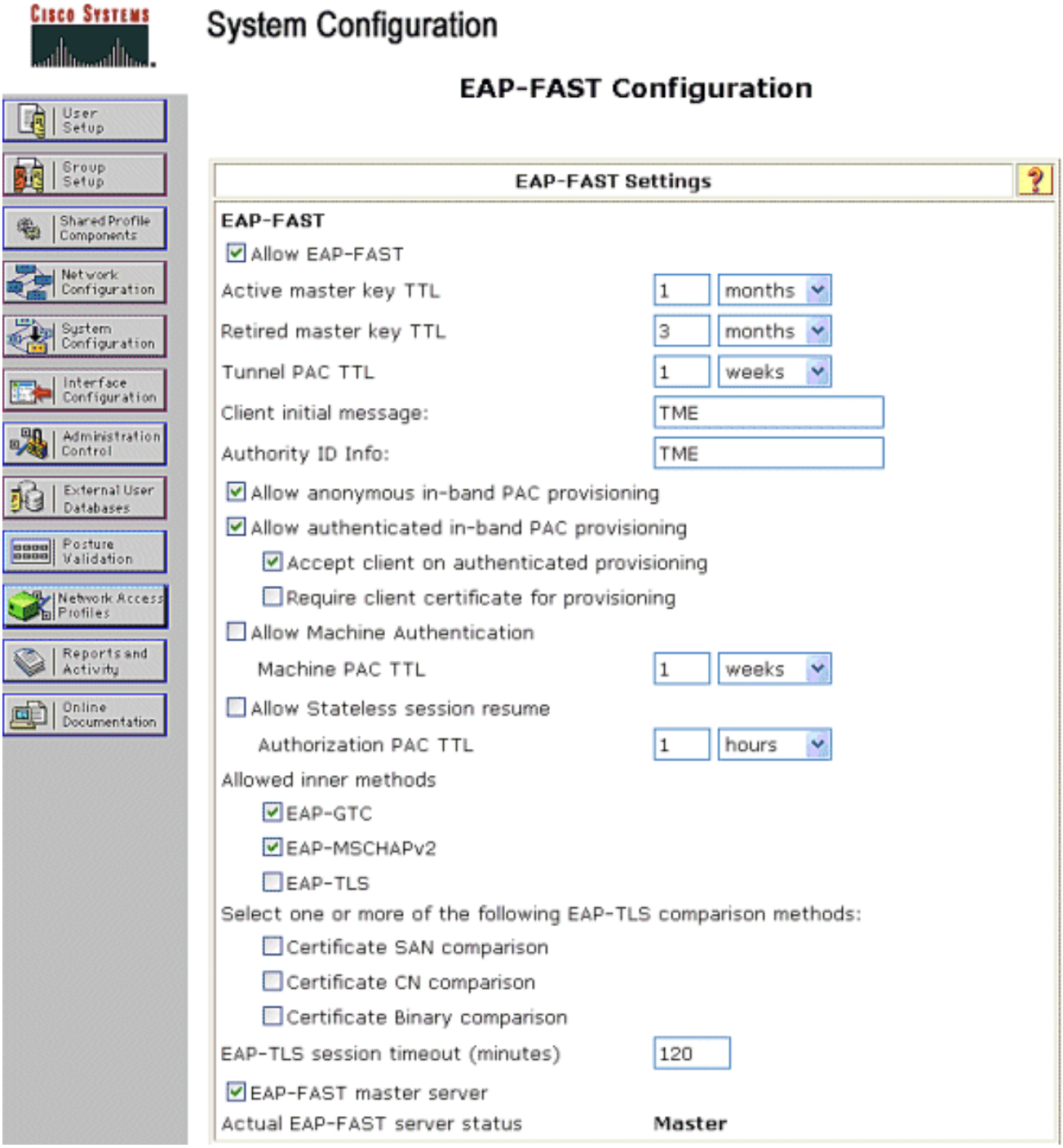
Habilite EAP-FAST Support en ACS

Esta sección describe cómo habilitar el soporte EAP-FAST en el ACS.

1. Vaya a **Configuración del sistema > Configuración de autenticación global > Configuración EAP-FAST**.
2. Elija **Allow EAP-FAST**.
3. Configure estas recomendaciones: Tecla maestra TTL/ Clave maestra retirada TTL/ PAC TTL. Estos parámetros se configuran de forma predeterminada en Cisco Secure ACS:Clave maestra TTL:1 mesTTL de clave retirada: 3 mesesTTL PAC: 1 semana
4. Rellene el campo **Información de ID de autoridad**. Este texto se muestra en algún software cliente EAP-FAST donde la selección de la Autoridad PAC es el controlador.**Nota:** Cisco Secure Services Client no emplea este texto descriptivo para la autoridad PAC.
5. Elija el campo **Permitir aprovisionamiento PAC en banda**. Este campo habilita el aprovisionamiento PAC automático para clientes EAP-FAST habilitados correctamente. Para este ejemplo, se utiliza el aprovisionamiento automático.
6. Elija **métodos internos permitidos**: EAP-GTC y EAP-MSCHAP2. Esto permite el funcionamiento de clientes EAP-FAST v1 y EAP-FAST v1a. (Cisco Secure Services Client es compatible con EAP-FAST v1a.) Si no es necesario admitir clientes EAP-FAST v1, sólo es necesario habilitar EAP-MSCHAPv2 como método interno.
7. Elija la casilla de verificación **EAP-FAST Master Server** para habilitar este servidor EAP-

FAST como maestro. Esto permite que otros servidores ACS utilicen este servidor como la autoridad PAC maestra para evitar el suministro de claves únicas para cada ACS en una red. Consulte la Guía de Configuración de ACS para obtener más detalles.

8. Haga clic en **Enviar+Reiniciar**.



Controlador WLAN de Cisco

A efectos de esta guía de implementación, se utiliza un controlador de LAN inalámbrica integrado (WLC) Cisco WS3750G con puntos de acceso ligeros (LAP) Cisco AP1240 para proporcionar la infraestructura de WLAN para las pruebas de CSSC. La configuración se aplica a cualquier controlador WLAN de Cisco. La versión de software empleada es 4.0.155.5.

Configuración del controlador de LAN inalámbrica

Funcionamiento básico y registro del LAP en el controlador

Utilice el asistente de configuración de inicio en la interfaz de línea de comandos (CLI) para configurar el WLC para el funcionamiento básico. Alternativamente, puede utilizar la GUI para configurar el WLC. Este documento explica la configuración en el WLC con el asistente de configuración de inicio en la CLI.

Después de que el WLC se inicie por primera vez, ingresa al asistente de configuración de inicio. Utilice el asistente de configuración para configurar los parámetros básicos. Puede acceder al asistente a través de la CLI o la GUI. Este resultado muestra un ejemplo del asistente de configuración de inicio en la CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

Estos parámetros configuran el WLC para el funcionamiento básico. En este ejemplo de configuración, el WLC utiliza **10.10.80.3** como la dirección IP de la interfaz de administración y **10.10.80.4** como la dirección IP de la interfaz del administrador de AP.

Antes de que se puedan configurar otras funciones en los WLC, los LAPs deben registrarse en el WLC. Este documento asume que el LAP está registrado en el WLC. Refiérase a la sección Registro del Lightweight AP al WLCs del Ejemplo de Configuración de Failover del Controlador WLAN para Puntos de Acceso Ligeros para obtener información sobre cómo los Lightweight APs se registran con el WLC. Para hacer referencia a este ejemplo de configuración, los AP1240 se implementan en una subred independiente (10.10.81.0/24) del controlador WLAN (10.10.80.0/24), y la opción DHCP 43 se utiliza para proporcionar la detección del controlador.

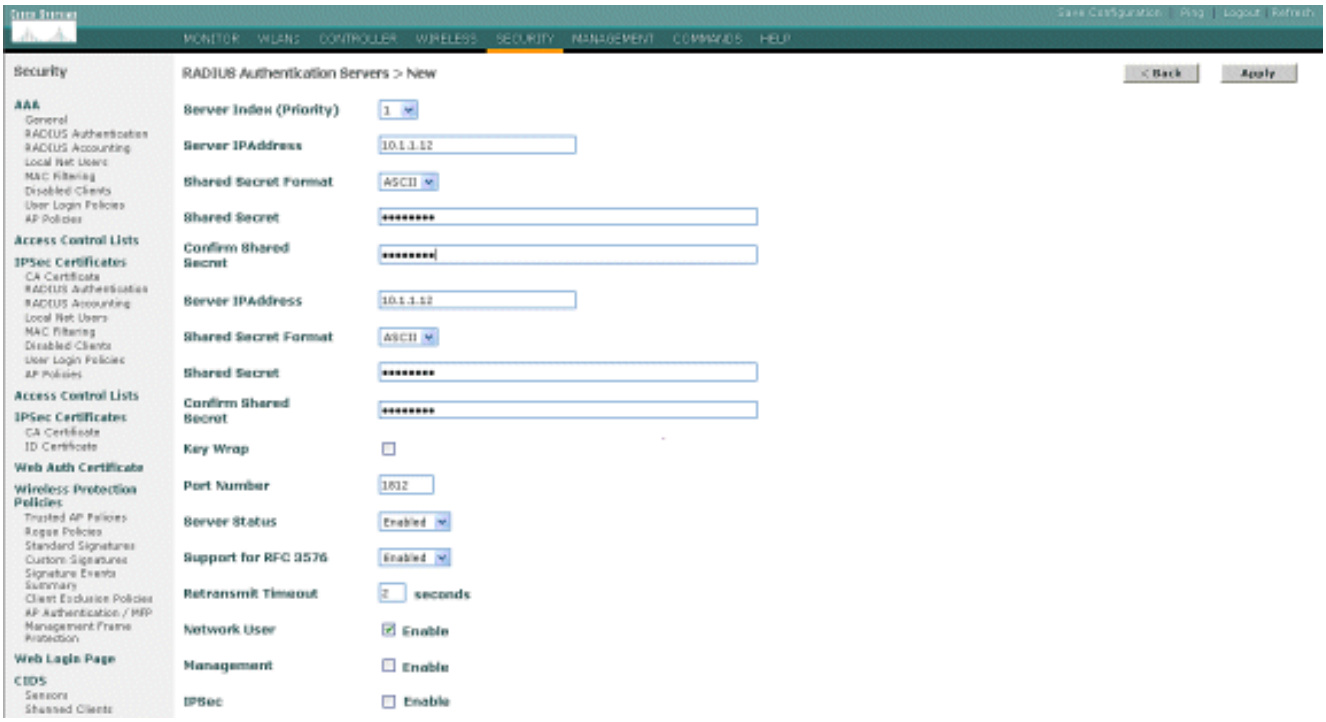
Autenticación RADIUS a través de Cisco Secure ACS

El WLC debe configurarse para reenviar las credenciales del usuario al servidor Cisco Secure

ACS. A continuación, el servidor ACS valida las credenciales del usuario (a través de la base de datos de Windows configurada) y proporciona acceso a los clientes inalámbricos.

Complete estos pasos para configurar el WLC para la comunicación con el servidor ACS:

1. Haga clic en **Seguridad** y **Autenticación RADIUS** desde la GUI del controlador para mostrar la página Servidores de Autenticación RADIUS. A continuación, haga clic en **New** para definir el servidor
   ACS.
   

2. Defina los parámetros del servidor ACS en la página RADIUS Authentication Servers > New . Estos parámetros incluyen la dirección IP ACS, el secreto compartido, el número de puerto y el estado del servidor.**Nota:** Los números de puerto 1645 o 1812 son compatibles con ACS para la autenticación RADIUS.Las casillas de verificación Usuario y administración de red determinan si la autenticación basada en RADIUS se aplica a los usuarios de red (por ejemplo, clientes WLAN) y a la administración (es decir, usuarios administrativos). El ejemplo de configuración utiliza Cisco Secure ACS como el servidor RADIUS con la dirección IP
   10.1.1.12:
   

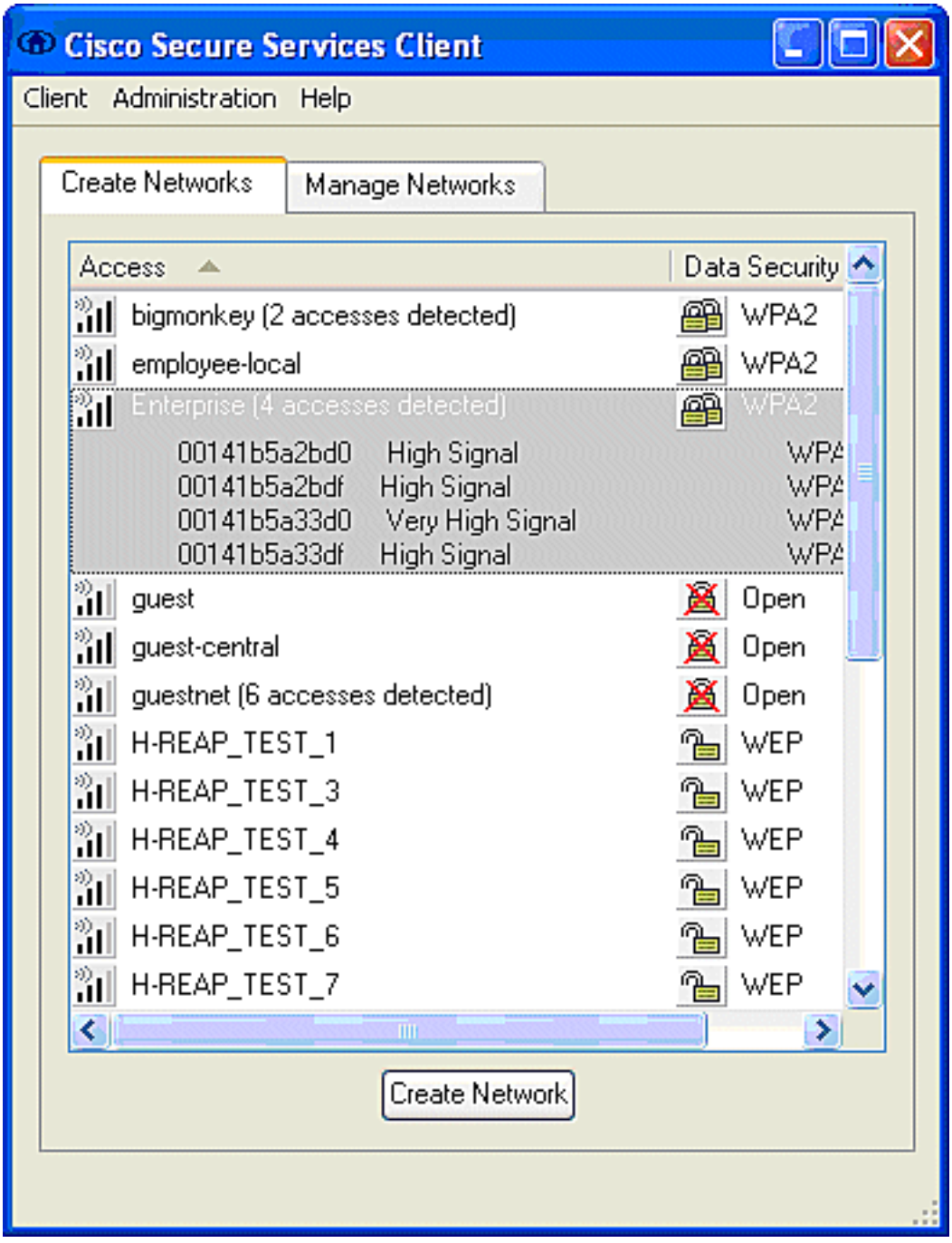
Configuración de los Parámetros WLAN

Esta sección describe la configuración de Cisco Secure Services Client. En este ejemplo, CSSC v4.0.5.4783 se utiliza con un adaptador de cliente Cisco CB21AG. Antes de instalar el software CSSC, verifique que sólo estén instalados los controladores para el CB21AG, no la Aironet Desktop Utility (ADU).

Una vez instalado el software y ejecutado como servicio, busca las redes disponibles y muestra las disponibles.

Nota: CSSC inhabilita Windows Zero Config.

Nota: Sólo se pueden ver los SSID habilitados para difusión.



Nota: El controlador WLAN transmite el SSID de forma predeterminada, por lo que se muestra en la lista Crear Redes de SSID escaneados. Para crear un perfil de red, simplemente puede hacer clic en el **SSID** en la lista (Enterprise) y el botón de radio **Create Network** .

Si la infraestructura WLAN se configura con el SSID de broadcast inhabilitado, debe agregar manualmente el SSID; haga clic en el botón de opción **Agregar** debajo de Dispositivos de acceso e introduzca manualmente el **SSID** adecuado (por ejemplo, Enterprise). Configure el comportamiento de 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 .

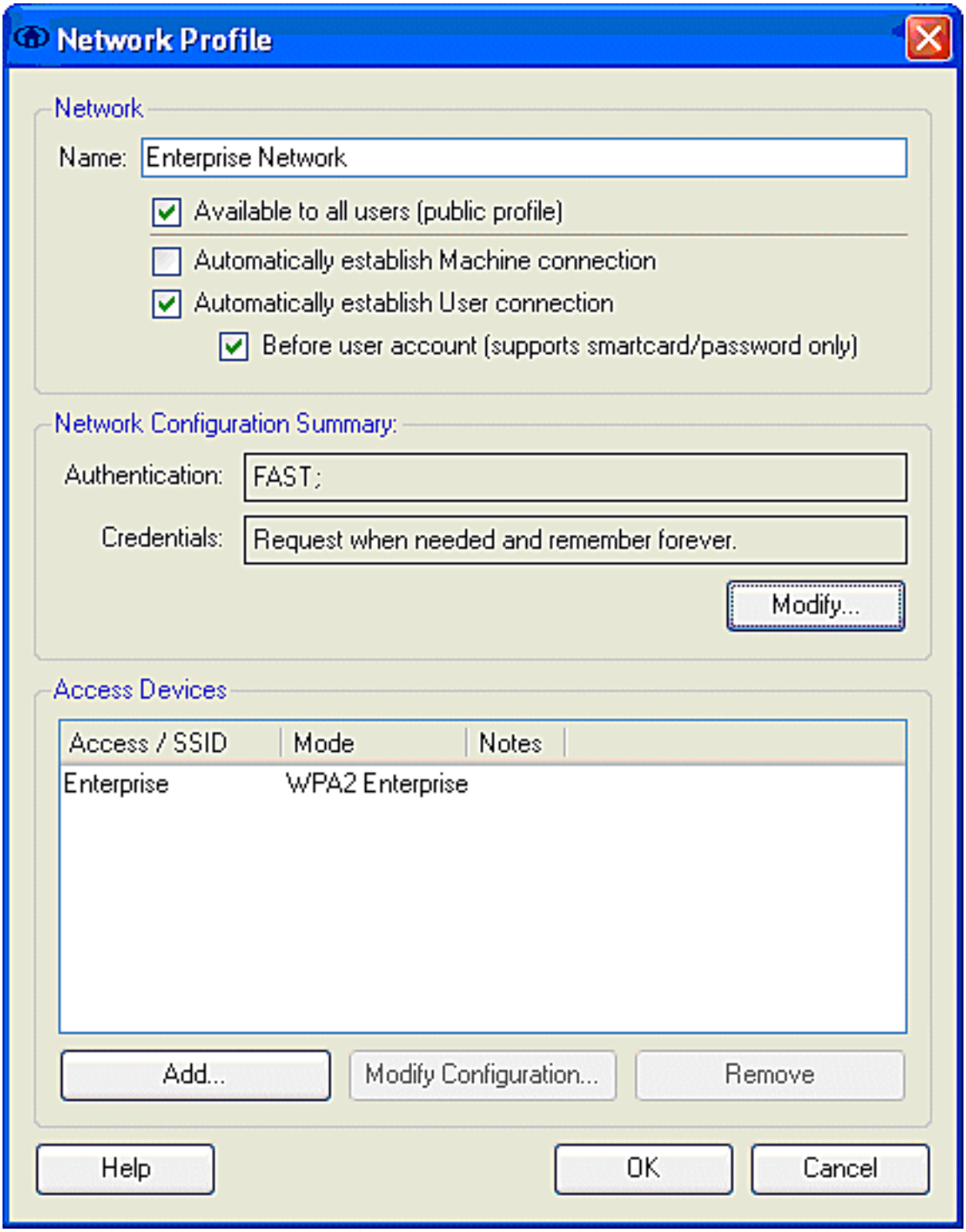
Nota: La configuración del puerto no permite modos empresariales (802.1X) si la configuración de autenticación EAP no se configura primero para el perfil.

El botón de opción **Crear red** inicia la ventana Perfil de red, que permite asociar el SSID seleccionado (o configurado) con un mecanismo de autenticación. Asigne un nombre descriptivo al perfil.

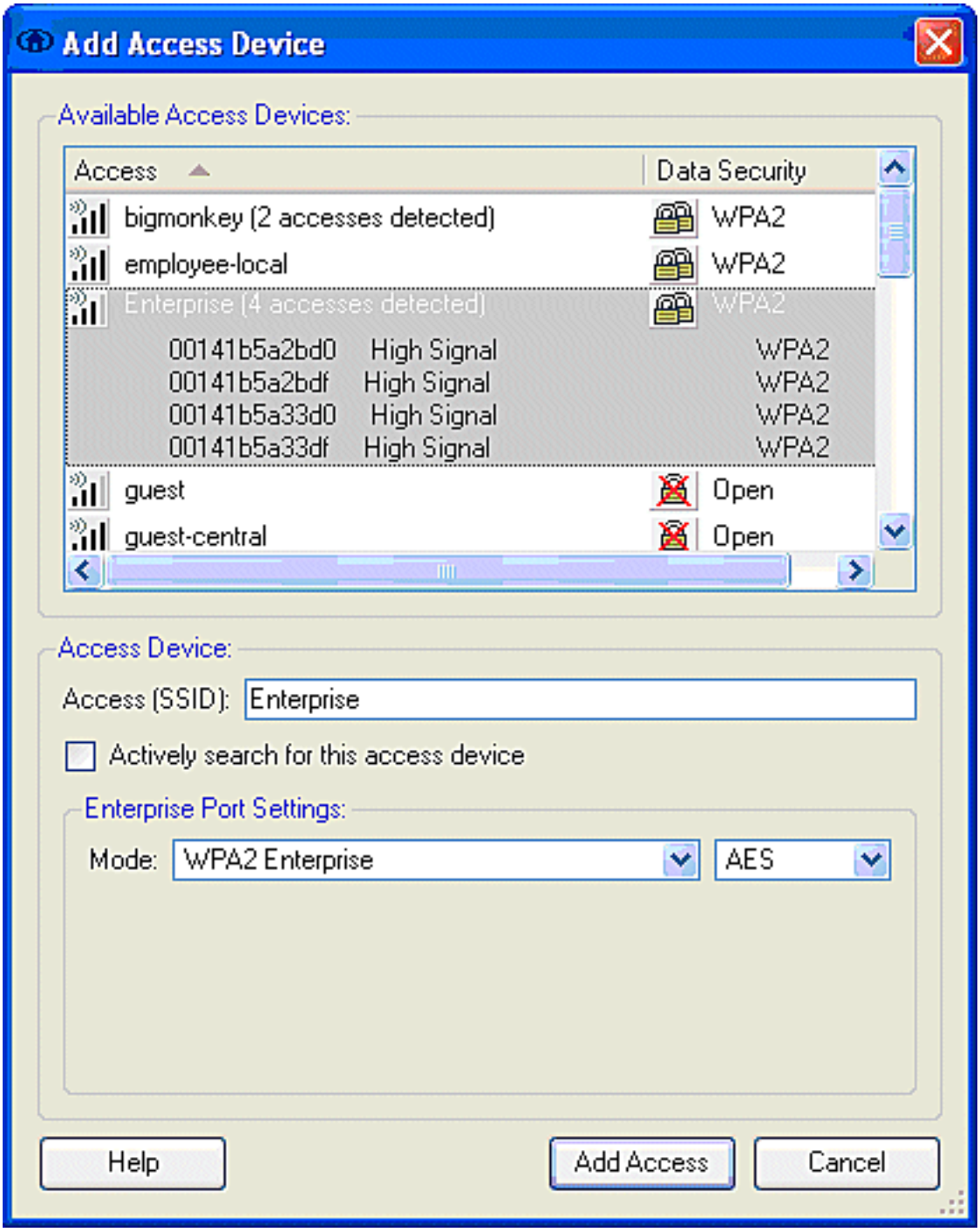
Nota: En este perfil de autenticación se pueden asociar varios tipos de seguridad WLAN y/o SSID.

Para que el cliente se conecte automáticamente a la red cuando esté en el rango de cobertura de RF, elija **Establecer automáticamente la conexión del usuario**. Desmarque **Disponible para todos los usuarios** si no es deseable utilizar este perfil con otras cuentas de usuario en el equipo. Si no se elige **Establecer automáticamente**, es necesario que el usuario abra la ventana CSSC e inicie manualmente la conexión WLAN con el botón de opción **Conectar**.

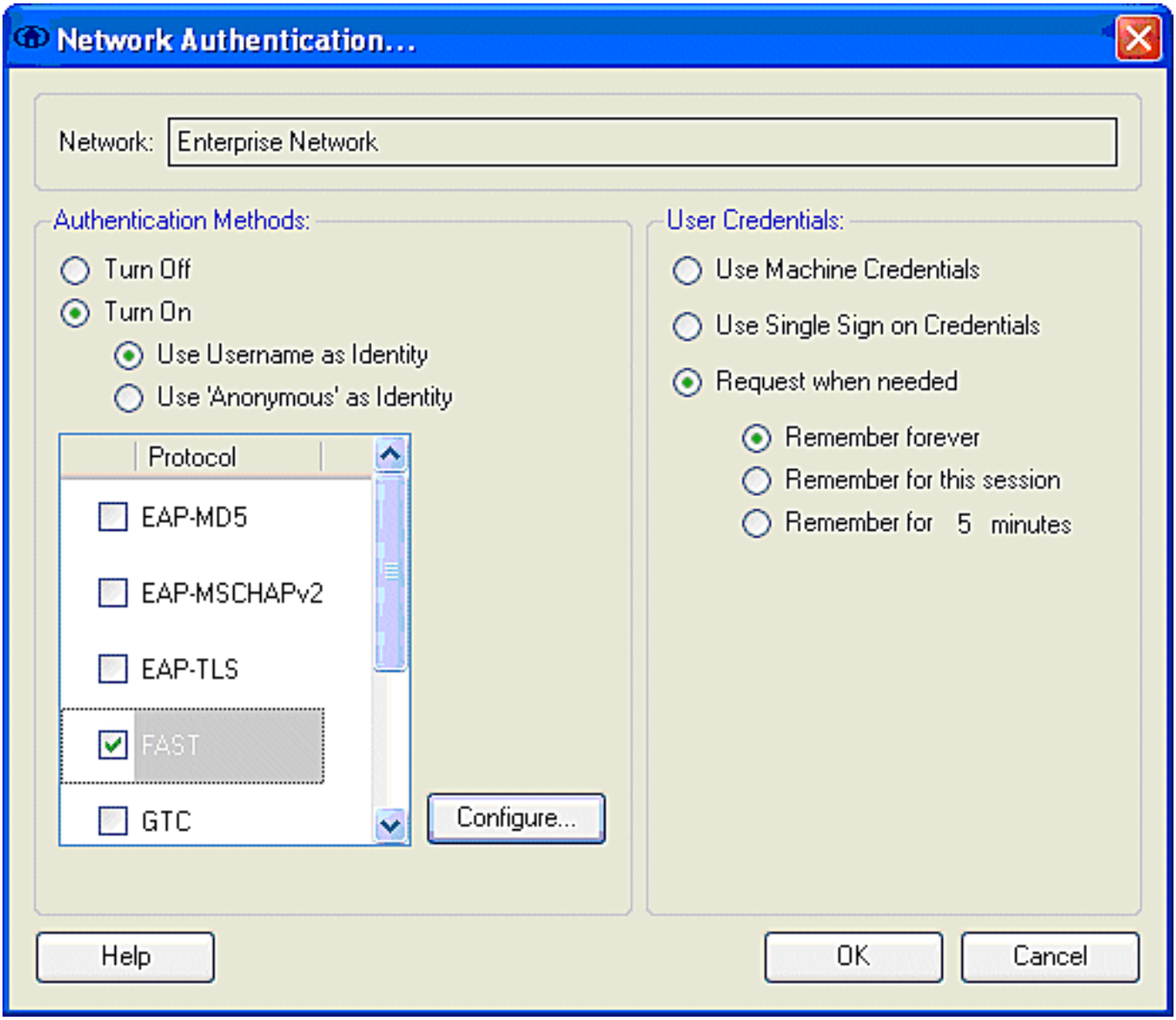
Si desea iniciar la conexión WLAN antes de que el usuario inicie sesión, elija **Antes de la cuenta de usuario**. Esto permite la operación de inicio de sesión único con credenciales de usuario guardadas (contraseña o certificado/Smartcard cuando se utiliza TLS dentro de EAP-FAST).



Nota: Para el funcionamiento de WPA/TKIP con el Cisco Aironet 350 Series Client Adapter, es necesario desactivar la validación del intercambio de señales WPA, ya que actualmente hay una incompatibilidad entre el cliente CSSC y 350 controladores con respecto a la validación del hash de intercambio de señales WPA. Esto se inhabilita en **Client > Advanced Settings > WPA/WPA2 Handshake Validation**. La validación del intercambio de señales desactivado sigue permitiendo las funciones de seguridad inherentes a WPA (clave TKIP por paquete y verificación de integridad del mensaje), pero desactiva la autenticación de clave WPA inicial.



En Resumen de configuración de red, haga clic en **Modificar** para configurar los parámetros EAP / credenciales. Especifique **Activar** autenticación, Elija **FAST** en Protocolo y elija **'Anonymous' como identidad** (para no utilizar ningún nombre de usuario en la solicitud EAP inicial). Es posible utilizar el **Usar nombre de usuario como** Identitas la identidad EAP externa, pero muchos clientes no desean exponer los ID de usuario en la solicitud EAP inicial no cifrada. 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-FAST.



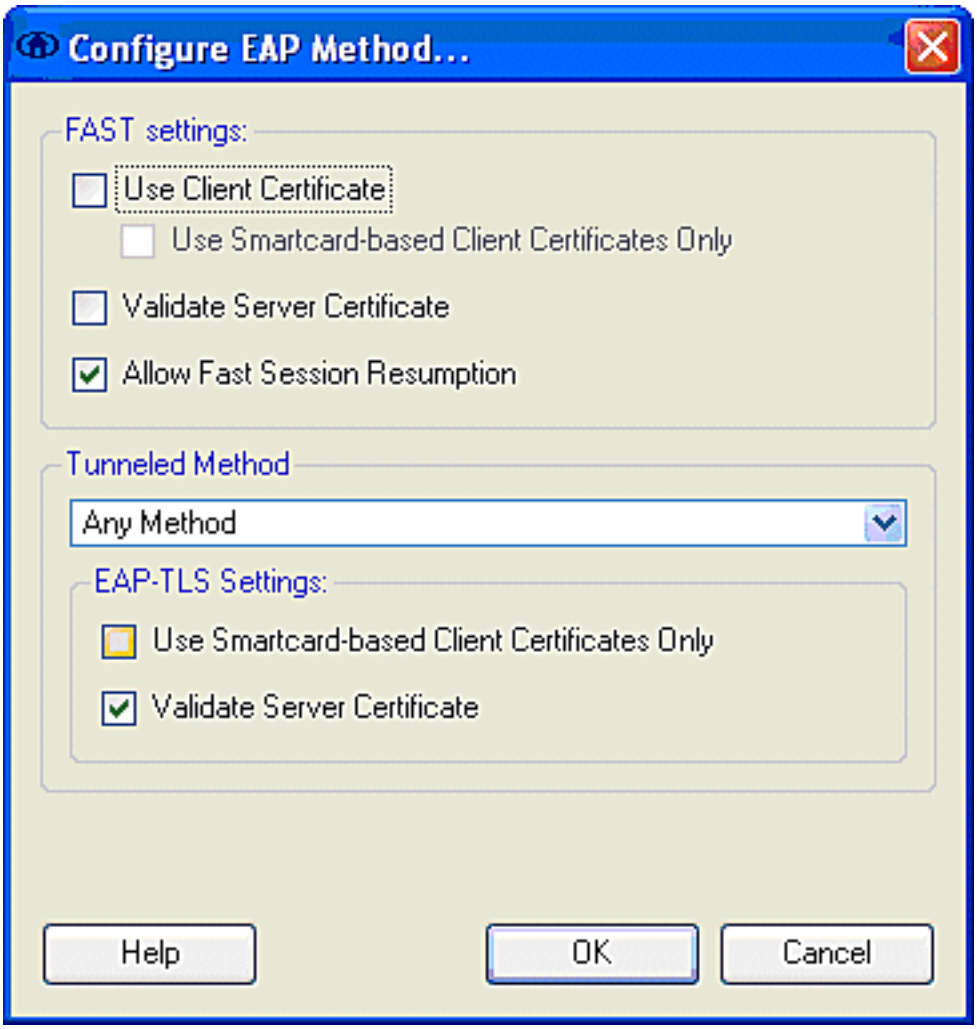
En la configuración de FAST, es posible especificar **Validar certificado de servidor**, que permite al cliente validar el certificado de servidor EAP-FAST (ACS) antes del establecimiento de una sesión EAP-FAST. Esto proporciona protección para los dispositivos cliente de la conexión a un servidor EAP-FAST desconocido o desconocido y el envío involuntario de sus credenciales de autenticación a un origen no confiable. Esto requiere que el servidor ACS tenga instalado un certificado y que el cliente también tenga instalado el certificado de autoridad de certificados raíz correspondiente. En este ejemplo, la validación del certificado del servidor no está habilitada.

En la configuración de FAST, es posible especificar **Permitir la reanudación rápida de la sesión**, que permite la reanudación de una sesión EAP-FAST basada en la información del túnel (sesión TLS) en lugar del requisito de una reautenticación EAP-FAST completa. Si el servidor EAP-FAST y el cliente tienen conocimiento común de la información de sesión TLS negociada dentro del intercambio de autenticación EAP-FAST inicial, puede producirse la reanudación de la sesión.

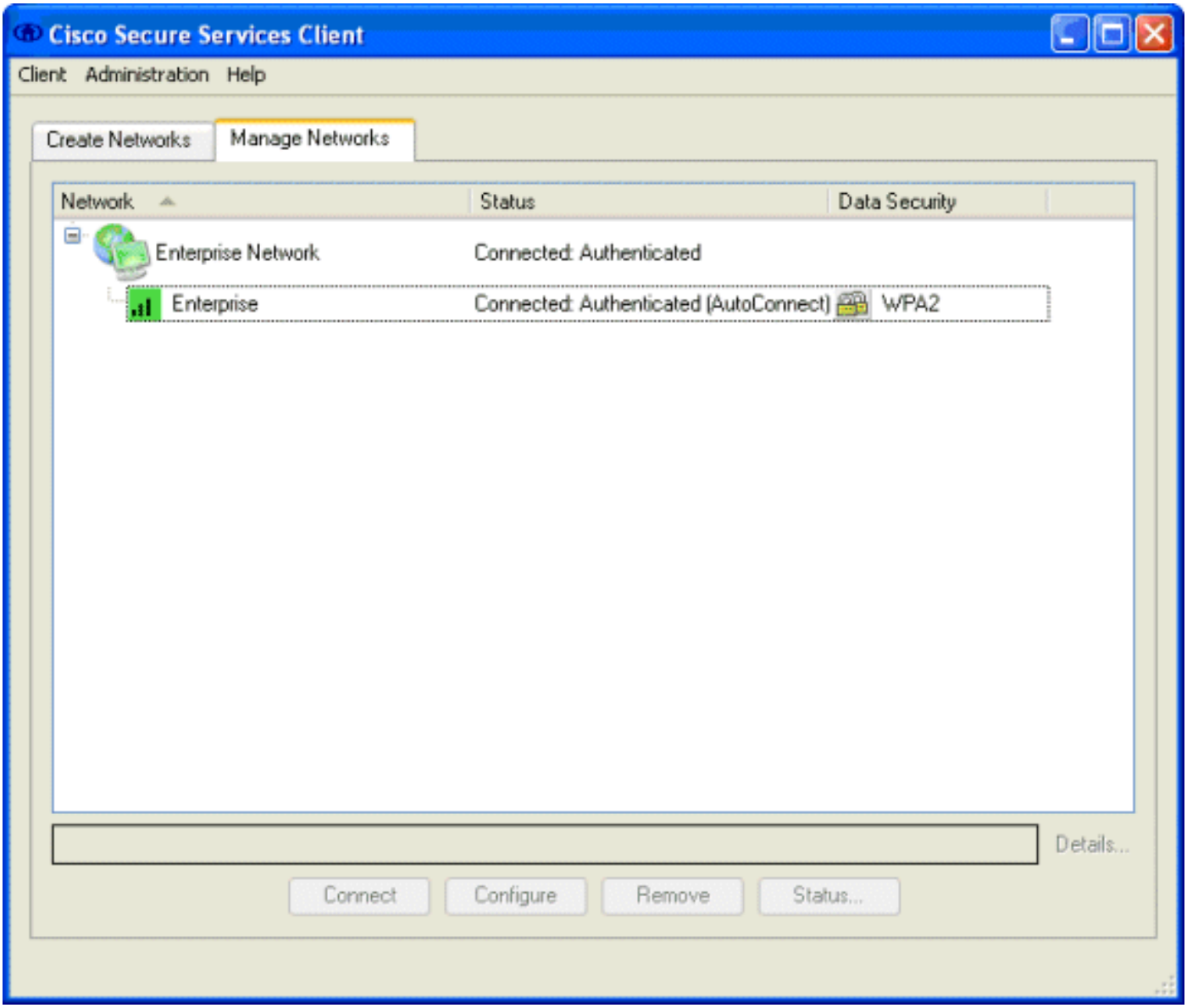
Nota: Tanto el servidor EAP-FAST como el cliente deben configurarse para que se reanude la sesión EAP-FAST.

En Tunneld Method > EAP-TLS Settings, especifique **Any Method** para permitir EAP-MSCHAPv2 para el aprovisionamiento automático PAC y EAP-GTC para la autenticación. Si utiliza una base de datos en formato Microsoft, como Active Directory, y si no admite ningún cliente EAP-FAST v1 en la red, también puede especificar el uso de sólo **MSCHAPv2** como método tunelado.

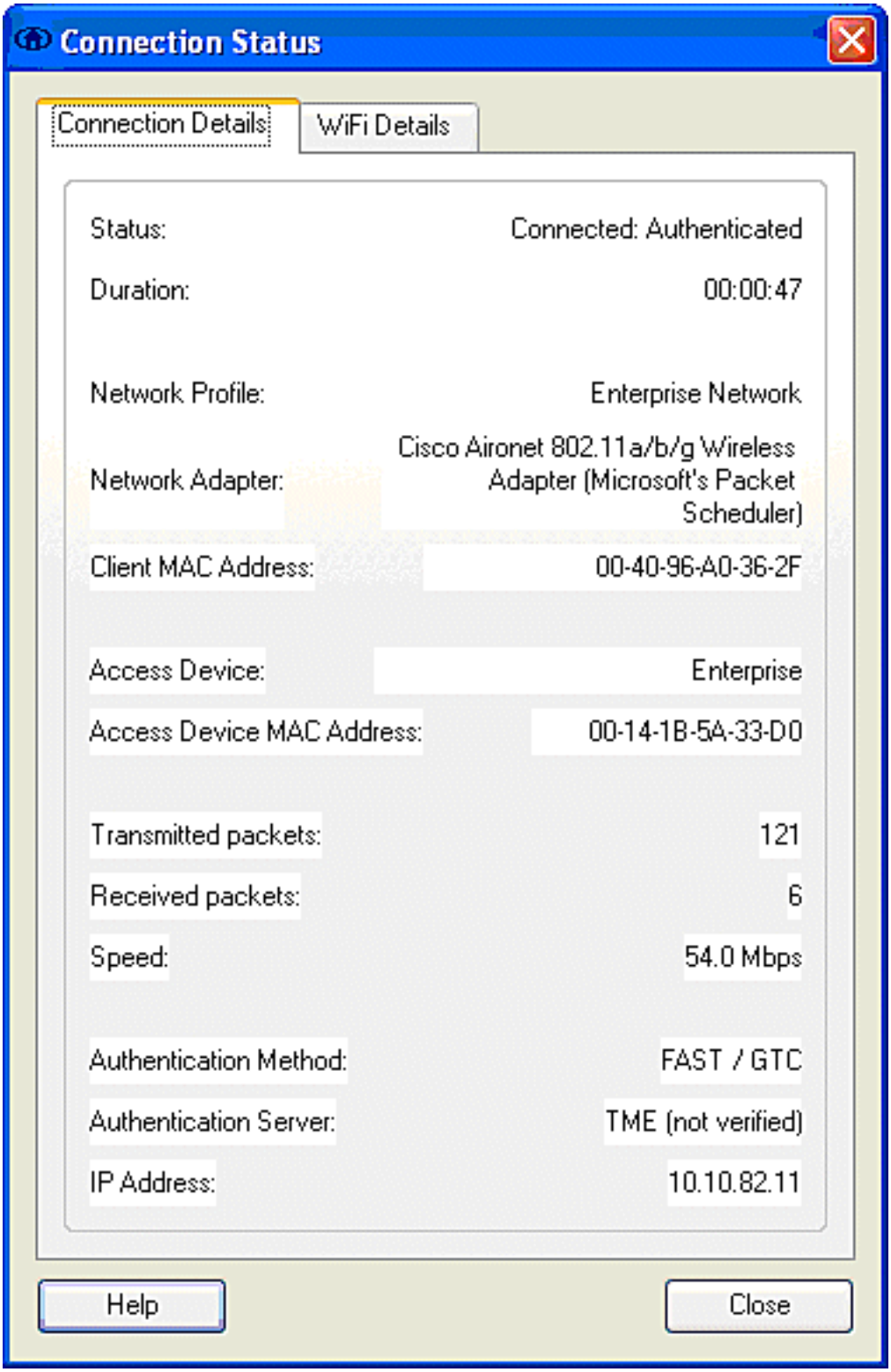
Nota: Validar certificado de servidor está habilitado de forma predeterminada bajo la configuración EAP-TLS en esta ventana. Dado que el ejemplo no utiliza EAP-TLS como método de autenticación interna, este campo no es aplicable. Si este campo está habilitado, permite al cliente validar el certificado del servidor además de la validación del servidor del certificado del cliente dentro de EAP-TLS.

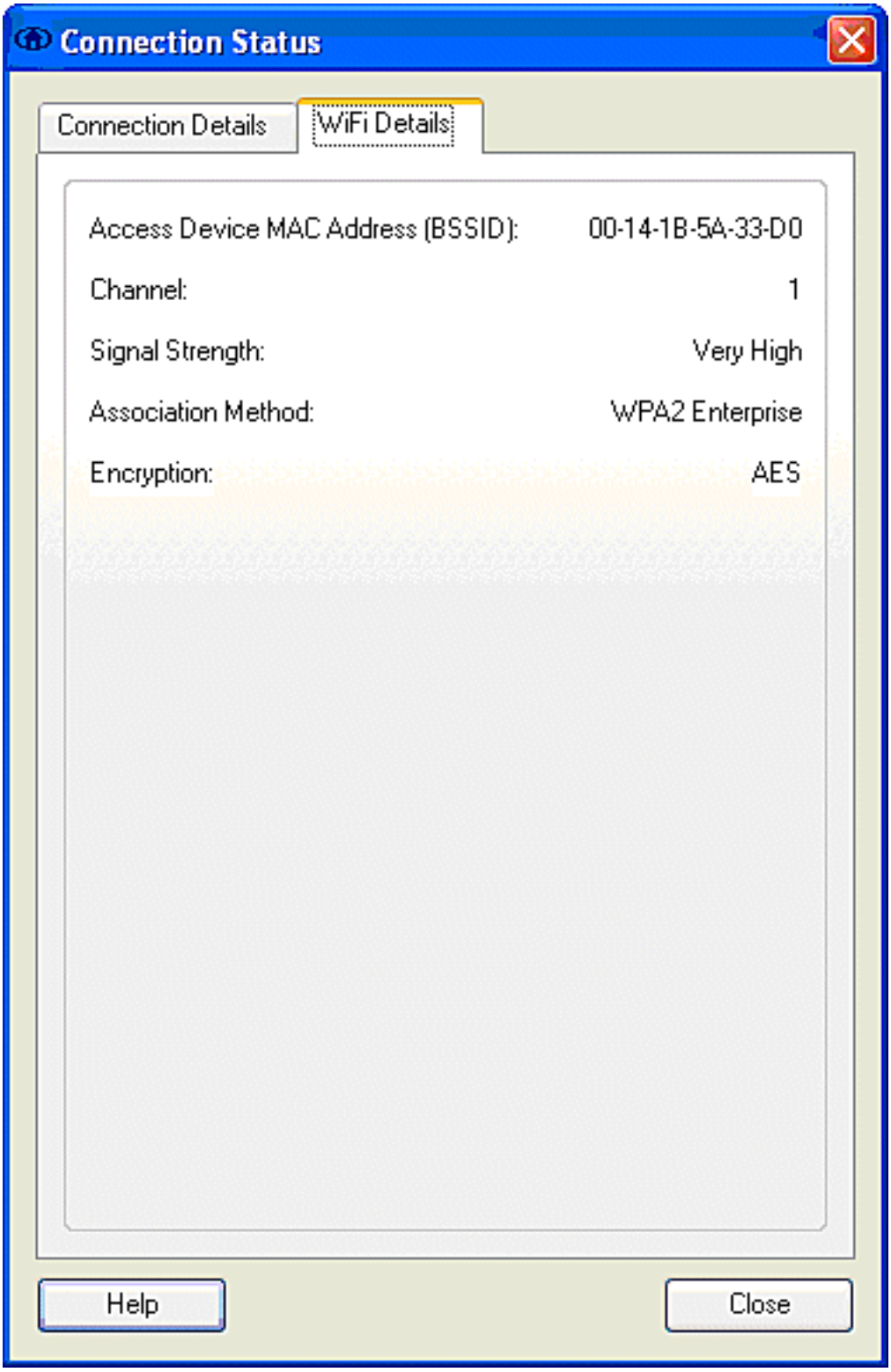


Haga clic en **Aceptar** para guardar la configuración EAP-FAST. Dado que el cliente está configurado para "establecer automáticamente" bajo perfil, inicia automáticamente la asociación/autenticación con la red. En la ficha Administrar redes, los campos Red, Estado y Seguridad de datos indican el estado de conexión del cliente. A partir del ejemplo, se observa que la red empresarial Profile está en uso y el dispositivo de acceso de red es el SSID Enterprise, que indica Connected:Authenticated y utiliza Autoconnect. El campo Seguridad de datos indica el tipo de encriptación 802.11 empleado, que, por este ejemplo, es WPA2.



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.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



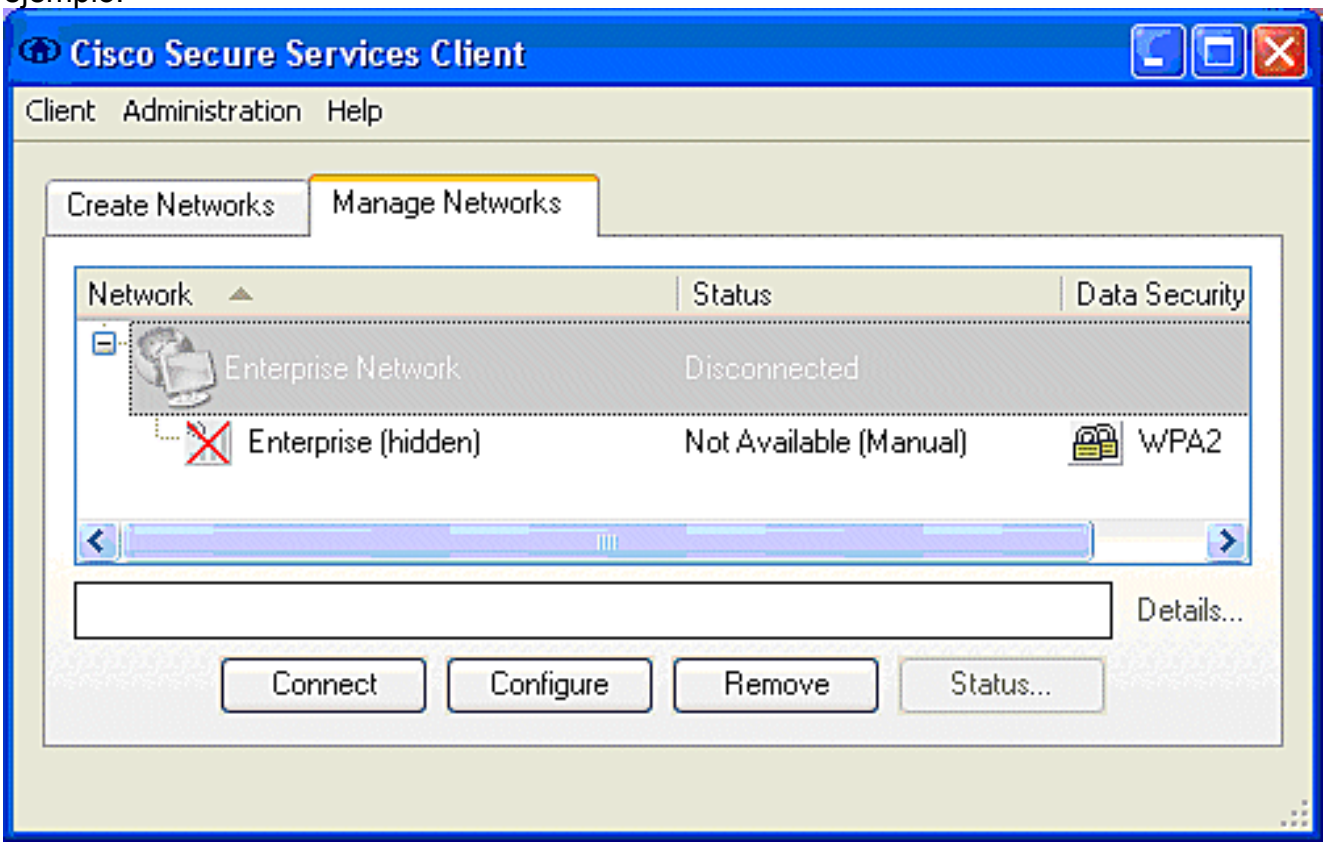
Como administrador del sistema, tiene derecho a la utilidad de diagnóstico Cisco Secure Services Client System Report, que está disponible con la distribución CSSC estándar. Esta utilidad está disponible en el menú de inicio o en el directorio CSSC. Para obtener datos, haga clic en **Recopilar datos > Copiar al portapapeles > Localizar archivo de informe**. Esto dirige una ventana de Microsoft File Explorer al directorio con el archivo de informe comprimido. Dentro del archivo comprimido, los datos más útiles se encuentran en log (log_current).

La utilidad proporciona el estado actual de CSSC, la interfaz y los detalles del controlador, junto con la información de WLAN (SSID detectado, estado de asociación, etc.). Esto puede ser útil, especialmente para diagnosticar problemas de conectividad entre CSSC y el adaptador WLAN.

Verificar operación

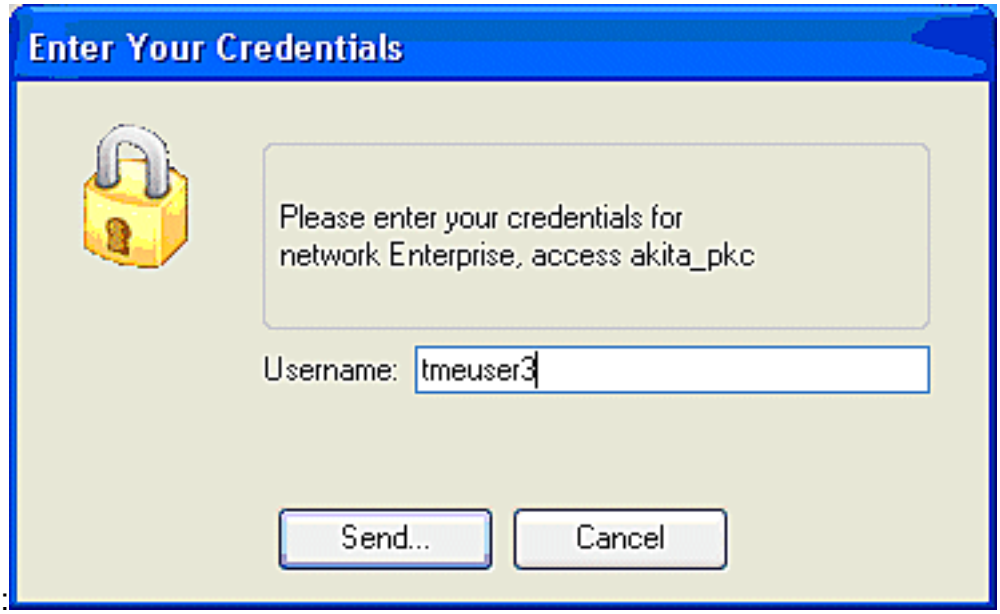
Después de la configuración del servidor Cisco Secure ACS, el controlador WLAN, el cliente CSSC y la configuración y población de base de datos presumiblemente correctas, la red WLAN se configura para la autenticación EAP-FAST y la comunicación de cliente segura. Hay numerosos puntos que se pueden supervisar para comprobar el progreso/los errores de una sesión segura.

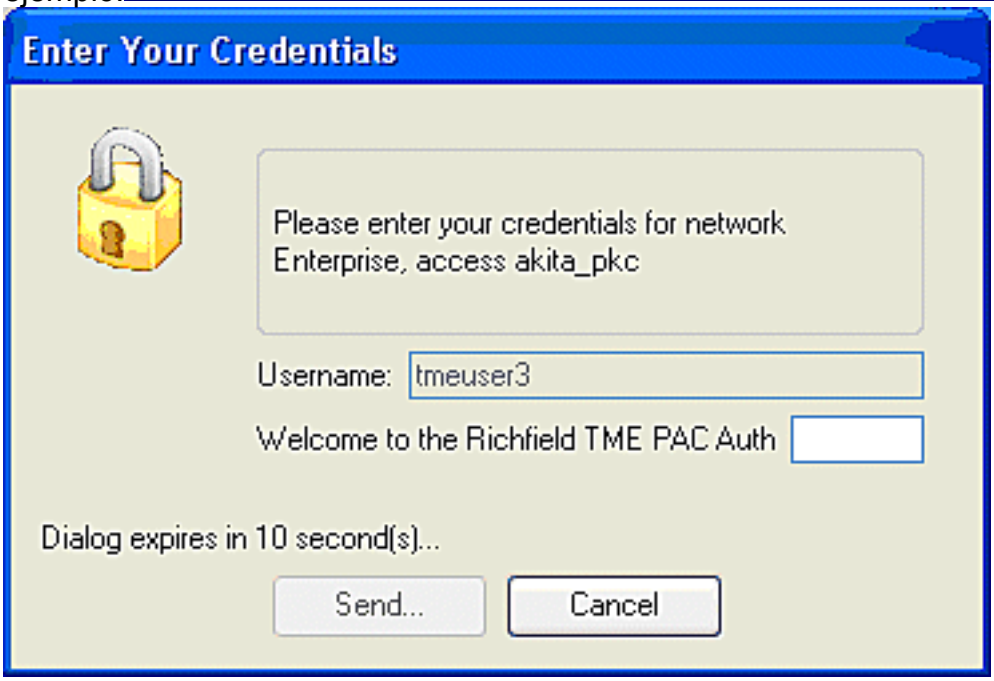
Para probar la configuración, intente asociar un cliente inalámbrico con el controlador WLAN con la autenticación EAP-FAST.

1. Si CSSC está configurado para la conexión automática, el cliente intenta esta conexión automáticamente. Si no está configurado para la conexión automática y el inicio de sesión único, el usuario debe iniciar la conexión WLAN a través del botón de opción **Connect**. Esto inicia el proceso de asociación 802.11 sobre el cual se produce la autenticación EAP.Aquí tiene un
ejemplo:


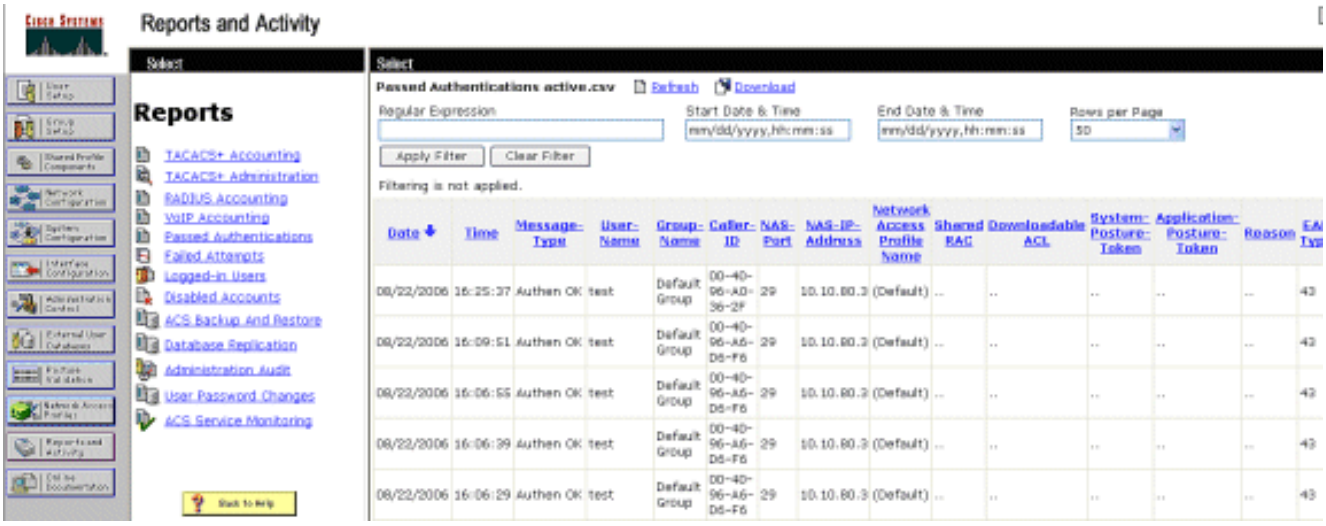
2. A continuación, se le solicita al usuario que proporcione el nombre de usuario y luego la contraseña para la autenticación EAP-FAST (de la Autoridad PAC EAP-FAST o ACS).Aquí tiene un

ejemplo:

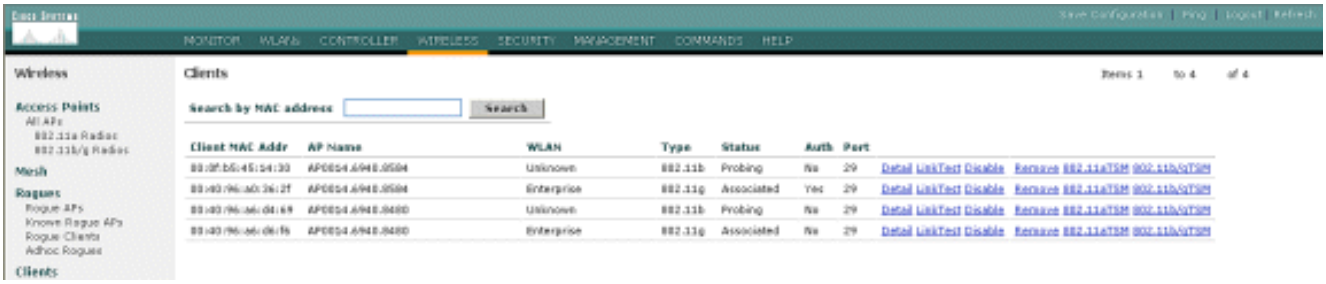




3. El cliente CSSC, a través del WLC, luego pasa las credenciales del usuario al servidor RADIUS (Cisco Secure ACS) para validar las credenciales. ACS verifica las credenciales del usuario con una comparación de los datos y la base de datos configurada (en la configuración de ejemplo, la base de datos externa es Windows Active Directory) y proporciona acceso al cliente inalámbrico siempre que las credenciales del usuario sean válidas. El informe de autenticaciones pasadas en el servidor ACS muestra que el cliente ha pasado la autenticación RADIUS/EAP.Aquí tiene un
ejemplo:



4. Tras la autenticación RADIUS/EAP correcta, el cliente inalámbrico (00:40:96:ab:36:2f en este ejemplo) se autentica con el controlador AP/WLAN.



Appendix

Además de la información de diagnóstico y estado, que está disponible en Cisco Secure ACS y Cisco WLAN Controller, hay puntos adicionales que se pueden utilizar para diagnosticar la autenticación EAP-FAST. Aunque la mayoría de los problemas de autenticación se pueden diagnosticar sin el uso de un rastreador WLAN o el debugging de los intercambios EAP en el controlador WLAN, este material de referencia se incluye para ayudar a resolver problemas.

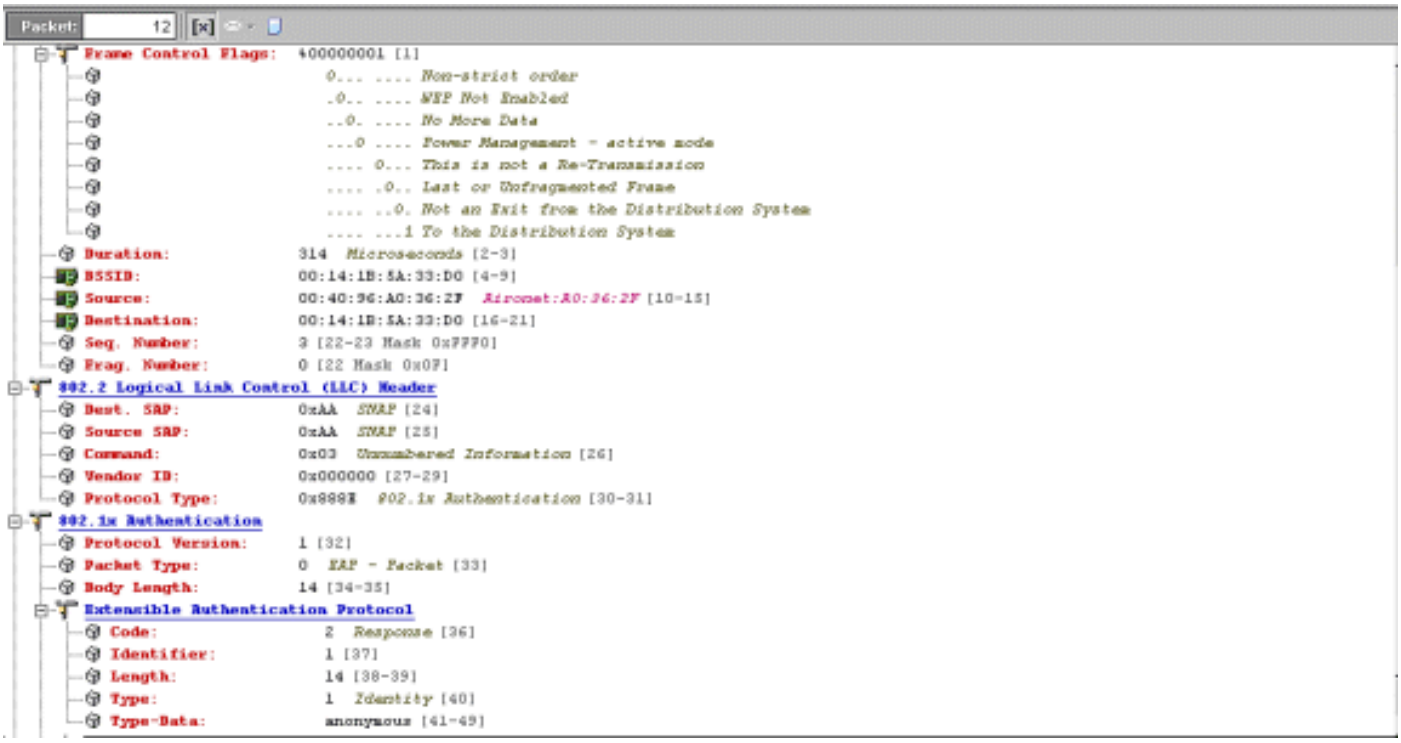
Captura de sabueso para EAP-FAST Exchange

Esta captura de sabueso 802.11 muestra el intercambio de autenticación.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

Este paquete muestra la respuesta EAP-FAST inicial.

Nota: Tal como se configuró en el cliente CSSC, anonymous se utiliza como la identidad EAP externa en la respuesta EAP inicial.



Depuración en el controlador WLAN

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

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

- debug dot1x events enable
- debug dot1x state enable

Este es un ejemplo del inicio de una transacción de autenticación entre el cliente CSSC y ACS como monitoreado en el controlador WLAN con los debugs:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

Esta es la finalización exitosa del intercambio EAP desde la depuración del controlador (con autenticación WPA2):

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
```

```
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
```

```
   Tunnel-Medium-Type.................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id....................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type...................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets..................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets.................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets.................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets................0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time..................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time....................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id.................10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id..................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

Información Relacionada

- Guía de instalación de Cisco Secure ACS para Windows Server
- Guía de Configuración de Cisco Secure ACS 4.1
- Ejemplo de Restringir Acceso WLAN Basado en SSID con WLC y Cisco Secure ACS Configuration
- EAP-TLS en Unified Wireless Network con ACS 4.0 y Windows 2003
- Ejemplo de Configuración de Asignación de VLAN Dinámica con Servidor RADIUS y Controlador de LAN Inalámbrico
- Soporte Técnico y Documentación - Cisco Systems