# Cisco Secure Services Client con la autenticación del 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.

Éstos son algunas de las ventajas de la solución CSSC de acuerdo con este documento:

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

con el Protocolo de Autenticación Extensible (EAP)
- Solución de punta a punta de la Seguridad de WLAN con el servidor, el authenticator, y los componentes del cliente
- Solución común para la autenticación atada con alambre y inalámbrica
- Dinámico, por las claves de encripción del usuario derivadas en el proceso de autenticación
- Ningún requisito para el Public Key Infrastructure (PKI) o los Certificados (verificación del certificado opcional)
- Asignación de la política de acceso y/o marco NAC-habilitado EAP

**Nota:** Refiera al Cisco SAFE que el modelo inalámbrico para la información sobre el despliegue de asegura la Tecnología inalámbrica.

El marco de autenticación del 802.1x se ha incorporado como parte del estándar 802.11i (seguridad de red inalámbrica LAN) para habilitar las funciones basadas capa 2 del autenticación, autorización y contabilidad en una red inalámbrica LAN del 802.11. Hoy, hay varios protocolos EAP disponibles para el despliegue en atado con alambre y las redes inalámbricas. Los protocolos comúnmente desplegados EAP incluyen el SALTO, el PEAP, y el EAP-TLS. Además de estos protocolos, Cisco ha definido y autenticación adaptable de EAP implementada con el protocolo asegurado del túnel (EAP-FAST) como protocolo basado en estándares EAP disponible para el despliegue en atado con alambre y las redes inalámbricas LAN. La especificación del protocolo del EAP-FAST está público - disponible en el sitio web IETF .

Como con algunos otros protocolos EAP, el EAP-FAST es una arquitectura de seguridad del servidor del cliente que cifra las transacciones EAP dentro de un túnel de TLS. Mientras que es similar al PEAP o al EAP-TTLS a este respecto, diferencia en ese establecimiento del túnel del EAP-FAST se basa sobre las claves secretas compartidas fuertes que son únicas a cada usuario contra PEAP/EAP-TTLS (que utilicen un certificado del servidor X.509 para proteger la sesión de la autenticación). Estas claves secretas compartidas se llaman las credenciales protegidas del acceso (PAC) y se pueden distribuir automáticamente (aprovisionamiento automático o de la En-banda) o manualmente (aprovisionamiento manual o fuera de banda) a los dispositivos del cliente. Porque los apretones de manos basados sobre los secretos compartidos son más eficientes que los apretones de manos basados sobre una infraestructura PKI, el EAP-FAST es el tipo más rápido y menos uso intensivo del procesador EAP de los que proporcionen los intercambios protegidos de la autenticación. El EAP-FAST también se diseña para la simplicidad del despliegue puesto que no requiere un certificado en el cliente del Wireless LAN o en la infraestructura RADIUS con todo incorpora un mecanismo incorporado del aprovisionamiento.

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

- Escoja muestra-en (SSO) con el nombre de usuario de Windows/la contraseña
- Soporte para la ejecución del script del login
- Soporte del Acceso protegido de Wi-Fi (WPA) sin el supplicant del otro vendedor (Windows 2000 y XP solamente)
- Despliegue simple sin el requisito para la infraestructura PKI
- Envejecimiento de la contraseña de Windows (es decir, soporte para el vencimiento de contraseña basado en el servidor)
- Integración con el Cisco Trust Agent para el control de admisión de red con el software de cliente apropiado

## prerrequisitos

## Requisito

Hay una suposición que el instalador tiene la instalación de Windows 2003 del conocimietno básico e instalación del WLC de Cisco puesto que este documento cubre solamente las configuraciones específicas para facilitar las pruebas.

Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 4400 Series, refiera a la guía de inicio rápido: Cisco Wireless LAN Controllers de la serie 4400. Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 2000 Series, refiera a la guía de inicio rápido: Cisco Wireless LAN Controllers de la serie 2000.

Antes de que usted comience, instale el Microsoft Windows server 2000 con el último software del Service Pack. Instale los reguladores y los Puntos de acceso ligeros (revestimientos) y asegúrese de que las actualizaciones de último software están configuradas.

## Componentes Utilizados

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

- Regulador de las Cisco o Series que funcionamientos 4.0.155.5
- LWAPP AP de Cisco 1242
- Windows 2000 con el Active Directory
- Cisco Catalyst 3750G Switch
- Windows XP con la versión 4.05 de la placa adaptadora y del Cisco Secure Services Client del CB21AG

## Convenciones

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

# Parámetros de diseño

## Base de datos

Cuando usted despliega una red WLAN y busca un protocolo de autenticación, se desea comúnmente para utilizar una base de datos actual para la autenticación del usuario/de la máquina. Las bases de datos típicas que pueden ser utilizadas son Active Directory de Windows, LDAP, o una base de datos de la contraseña de una vez (OTP) (es decir, RSA o SecureID). Todas estas bases de datos son compatibles con el protocolo del EAP-FAST, pero cuando usted planea para el despliegue, hay algunos requerimientos de compatibilidad que deben ser considerados. La implementación inicial de un archivo PAC a los clientes es realizada con el auto-aprovisionamiento anónimo, el aprovisionamiento autenticado (a través del certificado del cliente actual X.509), o el aprovisionamiento manual. Con el fin de este documento, se consideran el auto-aprovisionamiento anónimo y el aprovisionamiento manual.

El aprovisionamiento automático PAC utiliza el protocolo autenticado del acuerdo de la clave Diffie-Hellman (ADHP) para establecer un túnel seguro. El túnel seguro se puede establecer anónimo o a través de un mecanismo de autenticación de servidor. Dentro de la conexión del

túnel establecido, MS-CHAPv2 se utiliza para autenticar al cliente y, sobre la autenticación satisfactoria, para distribuir el archivo PAC al cliente. Después de que el PAC haya sido con éxito aprovisionado, el archivo PAC se puede utilizar para iniciar una nueva sesión de la autenticación del EAP-FAST para tener el acceso a la red seguro.

El aprovisionamiento automático PAC es relevante a la base de datos funcionando porque, puesto que el mecanismo del auto-aprovisionamiento confía en el MSCHAPv2, la base de datos usada para autenticar a los usuarios debe ser compatible con este formato de la contraseña. Si usted utiliza el EAP-FAST con una base de datos que no soporte el formato del MSCHAPv2 (tal como OTP, Novell, o LDAP), se requiere emplear un cierto otro mecanismo (es decir, aprovisionamiento manual o aprovisionamiento autenticado) para desplegar los archivos del usuario PAC. Este documento da un ejemplo del aprovisionamiento auto con una base de datos de usuario de Windows.

### Cifrado

La autenticación del EAP-FAST no requiere el uso un tipo de encripción específico de la red inalámbrica (WLAN). Las capacidades del indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente NIC determina al tipo de encripción WLAN que se utilizará. Se recomienda para emplear el cifrado WPA2 (AES-CCM) o WPA(TKIP), dependiente sobre las capacidades del indicador luminoso LED amarillo de la placa muestra gravedad menor NIC en el despliegue específico. Observe que la solución de Cisco WLAN permite la coexistencia del WPA2 y de los dispositivos del cliente WPA en un SSID común.

Si los dispositivos del cliente no soportan el WPA2 o el WPA, es posible desplegar la autenticación del 802.1x con las claves WEP dinámicas, pero, debido a los exploits bien conocidos contra las claves WEP, este mecanismo de encripción de la red inalámbrica (WLAN) no se recomienda. Si se requiere para apoyar a los clientes WEP-solamente, se recomienda para emplear un intervalo del sesión-descanso, que requiere que los clientes deriven una nueva clave WEP en un intervalo frecuente. Treinta minutos son el intervalo recomendado de la sesión para las velocidades de datos típicas de la red inalámbrica (WLAN).

### Escoja Muestra-en y las credenciales de la máquina

Escoja Muestra-en refiere a la capacidad de un único usuario muestra-en o de una entrada de los credenciales de autenticación de ser utilizado para acceder las aplicaciones múltiples o los dispositivos múltiples. Con el propósito de este documento, solo Muestra-en refiere al uso de las credenciales que se utilizan para abrir una sesión a un PC para la autenticación a la red inalámbrica (WLAN).

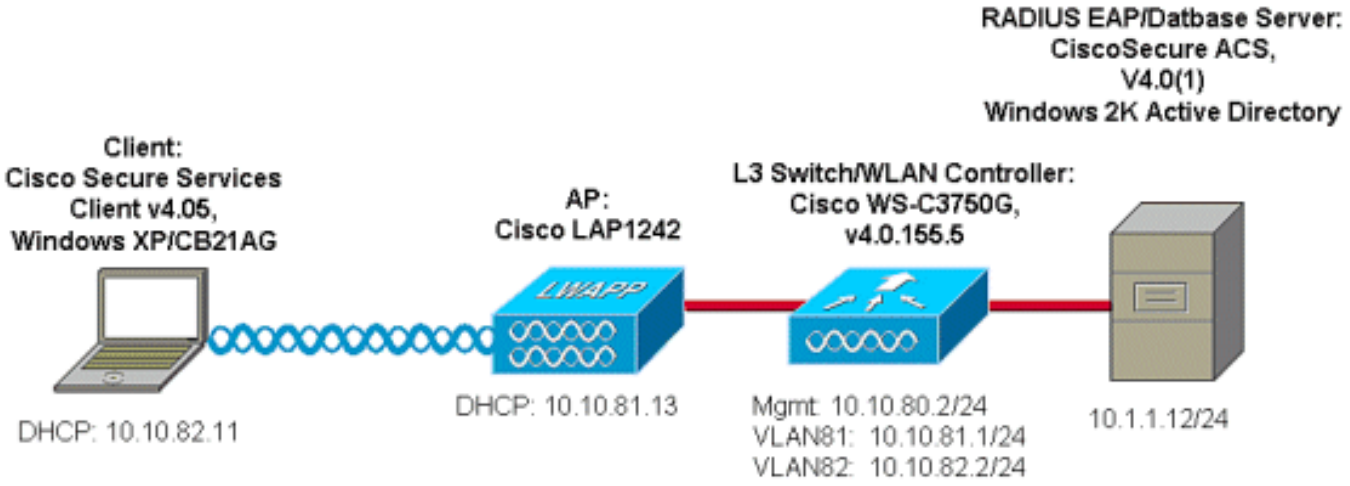
Con el Cisco Secure Services Client, es posible utilizar los credenciales de inicio de sesión de un usuario también para autenticar a la red WLAN. Si se desea para autenticar un PC a la red antes del inicio del usuario al PC, se requiere para utilizar los credenciales de usuario salvados o las credenciales atados a un perfil de la máquina. Cualquiera de estos métodos es útil en caso de que se desee para ejecutar las secuencias de comandos de inicio o las unidades de la correspondencia cuando los inicios PC para arriba, en comparación con cuando un usuario abre una sesión.

## Diagrama de la red

Éste es el diagrama de la red usado en este documento. En esta red, hay cuatro subredes

usadas. Observe que no es necesario dividir estos dispositivos en segmentos en diversas redes, pero éste permite la mayoría de la flexibilidad para la integración con las redes reales. El regulador integrado 3750G del Wireless LAN del Catalyst proporciona el poder sobre los switchports de los Ethernetes (POE), la transferencia L3, y la capacidad del controlador de WLAN en los comunes de chasis.

1. La red 10.1.1.0 es la red de servidores en donde reside el ACS.
2. La red 10.10.80.0 es la red de administración usada por el controlador de 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.




# Configure el Access Control Server (el ACS)

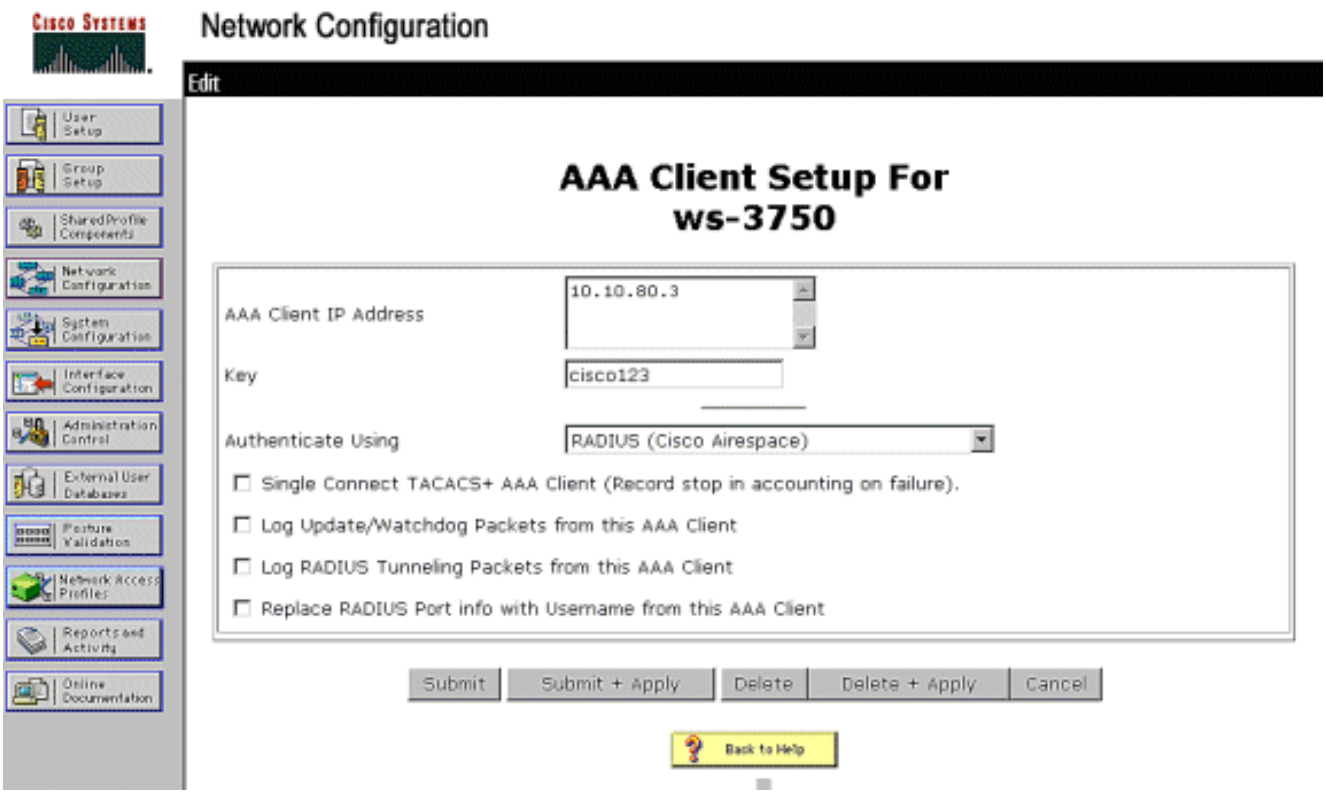
En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

## Agregue el Punto de acceso como cliente AAA (NAS) en el ACS

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

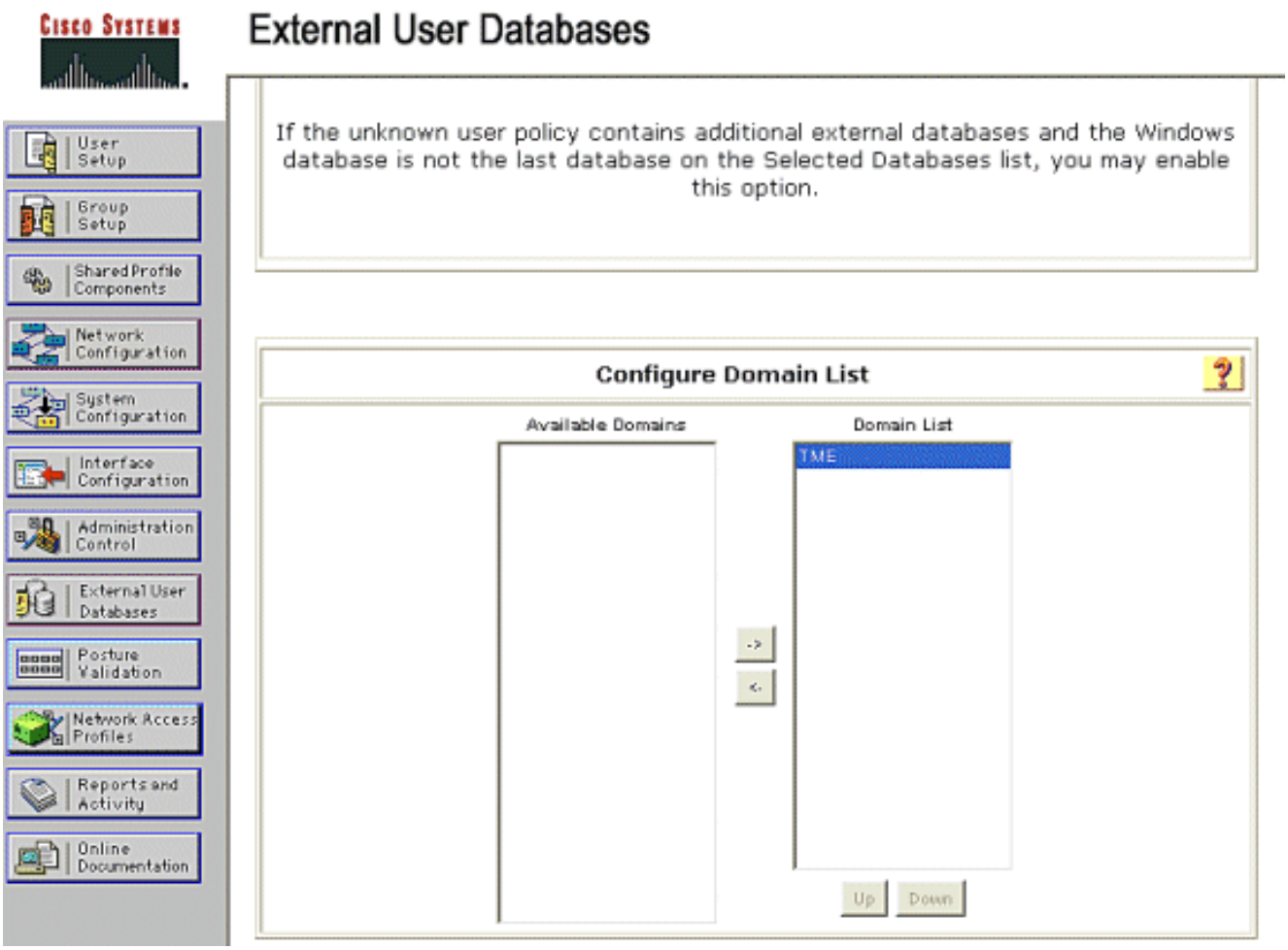
1. El inicio a **ACS > configuración de red** y tecleo **agrega la entrada**.
2. Complete el nombre del controlador de WLAN, dirección IP, clave secreta compartida, y debajo autentiqúelo usando, elija el RADIUS (Airespace de Cisco), que también incluye los atributos RADIUS IETF.**Nota:** Si se habilitan los grupos de dispositivos de red (NDG), primero elija el NDG apropiado y agregue el controlador de WLAN a él. Refiera a la guía de configuración de ACS para más información sobre el NDG.
3. **Reinicio del** tecleo
   **Submit+**.



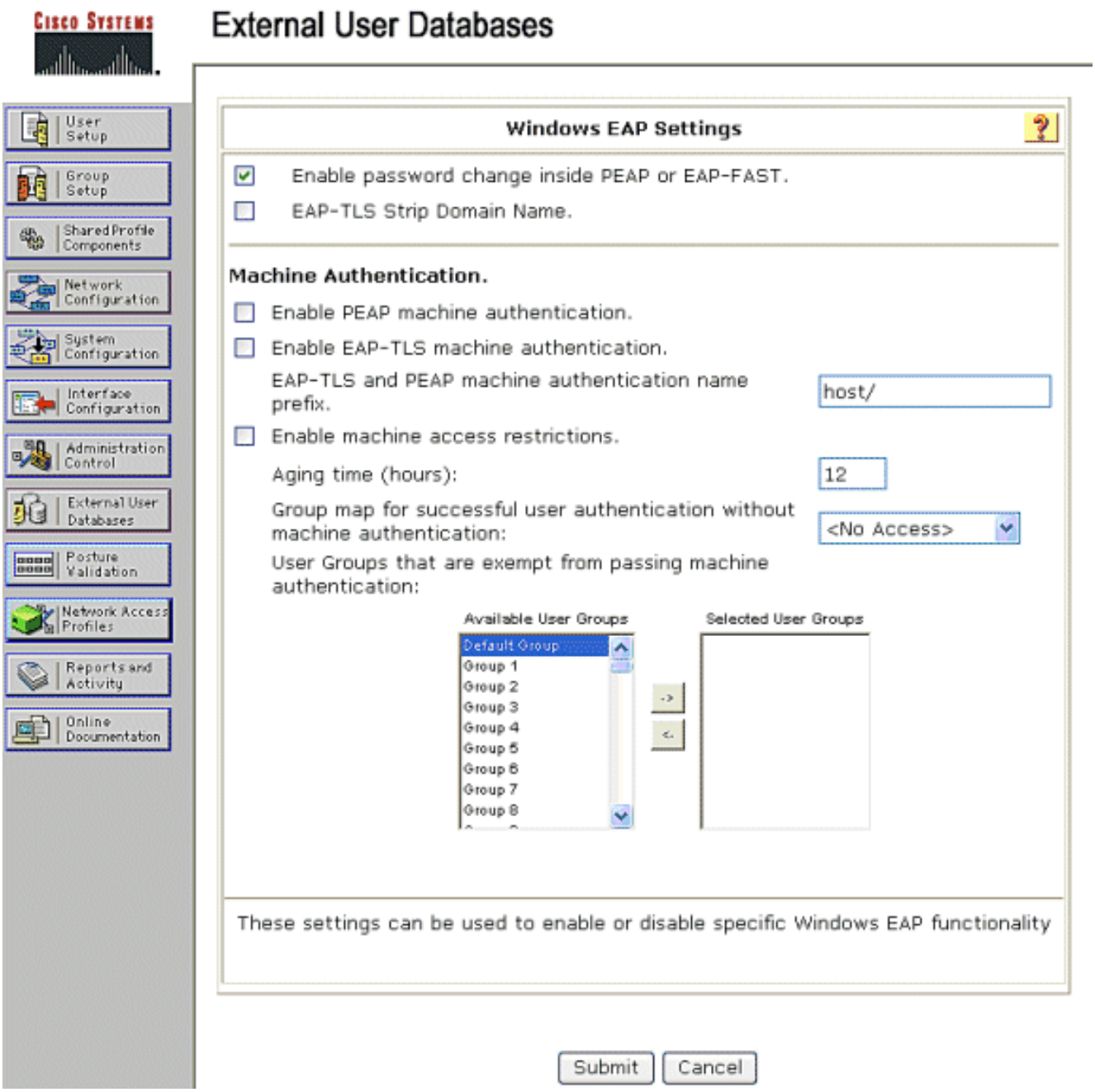

## Configuración ACS para preguntar la base de datos externa

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

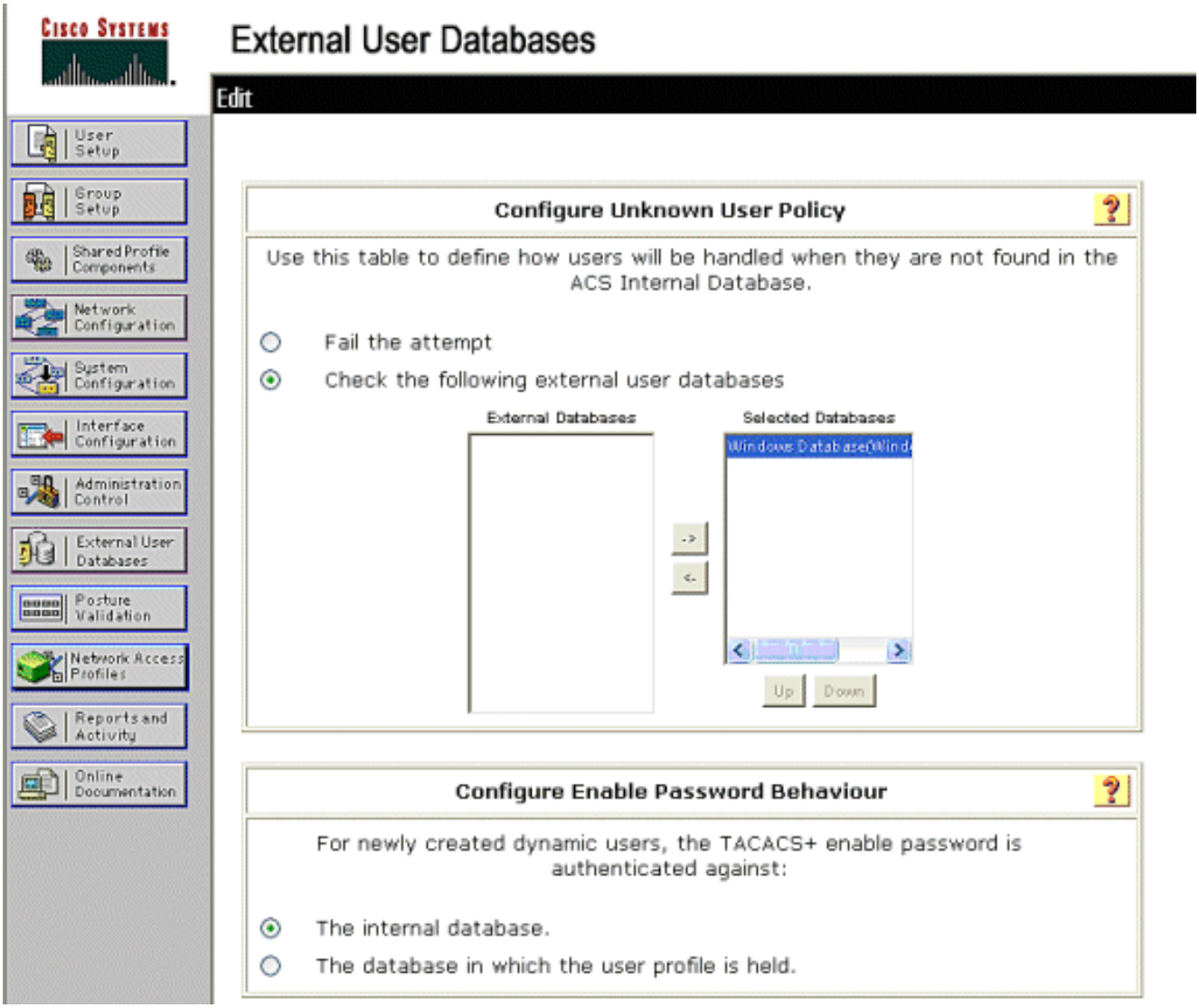
1. **Base de datos de usuarios externa > configuración de la base de datos > base de datos de Windows > configuración del** tecleo.
2. Bajo configuración lista de dominio, mueva los **dominios** desde los dominios disponibles a lista de dominio.**Nota:** El servidor que ejecuta el ACS debe tener conocimiento de estos dominios para que la aplicación ACS detecte y utilice esos propósitos de los dominios para autentificación.




3. Bajo configuraciones de Windows EAP, configure la opción para permitir el cambio de la contraseña dentro de la sesión PEAP o del EAP-FAST. Refiera a la guía de configuración para el Cisco Secure ACS 4.1 para conseguir más detalles sobre el envejecimiento del EAP-FAST y de la contraseña de Windows.
4. Haga clic en Submit (Enviar).**Nota:** Usted puede también permitir a la característica del permiso de marcado para el EAP-FAST bajo configuración de la base de datos del usuario de Windows para permitir que la base de datos externa de Windows controle el permiso de acceso. Las configuraciones MS-CHAP para el cambio de la contraseña en la página de configuración de la base de datos de Windows son solamente aplicables a la autenticación NON-EAP MS-CHAP. Para la contraseña habilitada cambia conjuntamente con el EAP-FAST, él es necesaria al cambio de la contraseña habilitada bajo configuraciones de Windows
EAP.




5. Haga clic la **Base de datos de usuarios externa > la Política de usuario desconocido** y elija el **control el** botón de radio **siguiente de las Bases de datos de usuarios externas**.
6. Mueva la base de datos de Windows desde las **bases de datos externas a las bases de datos seleccionadas**.
7. Haga clic en Submit (Enviar).**Nota:** Desde aquí, el ACS marca Windows DB. Si no encuentran al usuario en la base de datos local ACS, coloca al usuario en el grupo predeterminado ACS. Refiera a la documentación ACS para más detalles sobre los Mapeo de grupo de base de datos.**Nota:** Pues el ACS pregunta la base de datos del Microsoft Active Directory para verificar los credenciales de usuario, las configuraciones adicionales de los derechos de acceso necesitan ser configuradas en Windows. Refiera a la guía de instalación para el servidor del Cisco Secure ACS for Windows para los detalles.

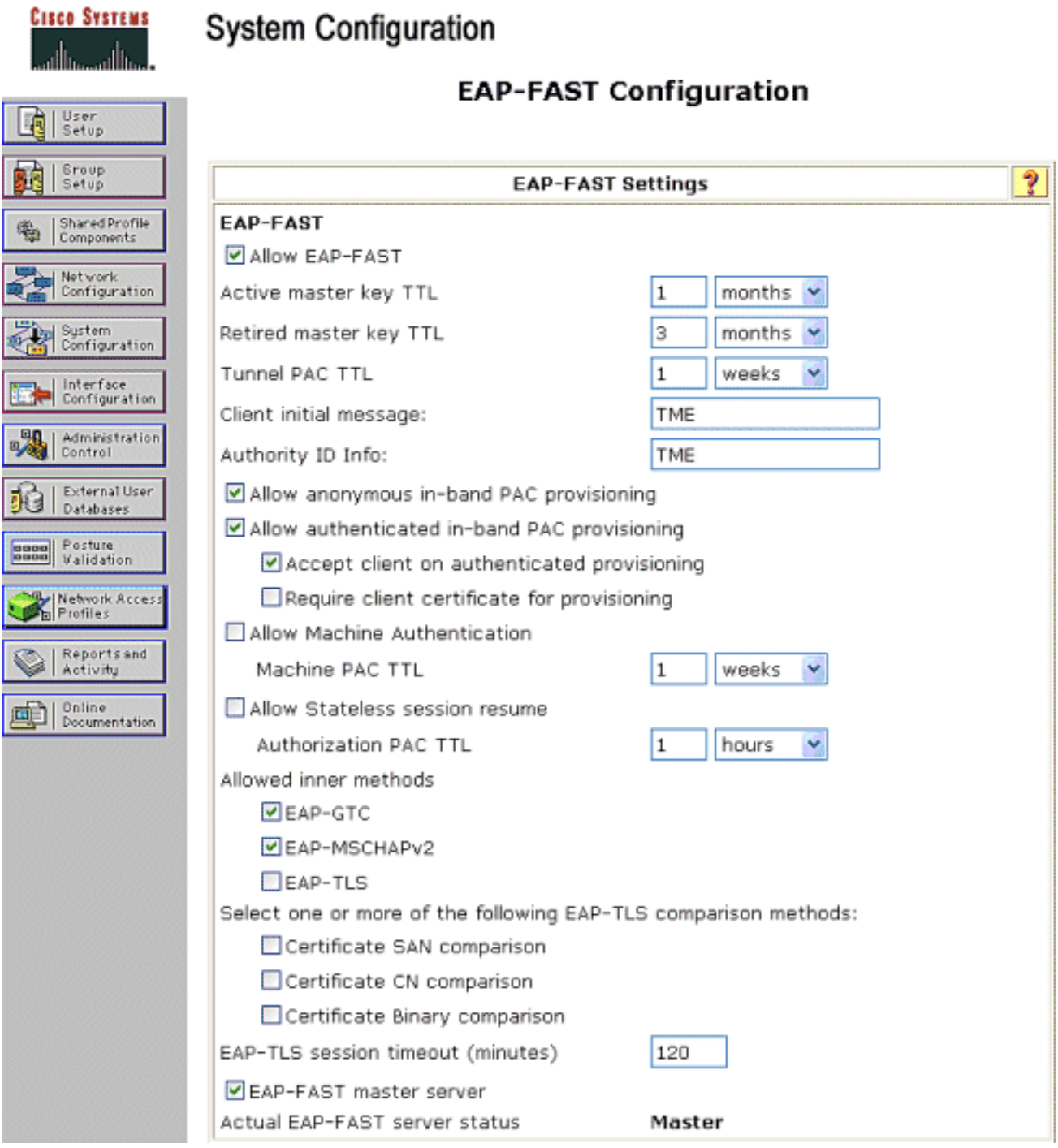



## Habilite el soporte del EAP-FAST en el ACS

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

1. Va a la **configuración del sistema > a la autenticación global puestas > la configuración del EAP-FAST**.
2. Elija **permiten el EAP-FAST**.
3. Configure estas recomendaciones: Clave principal jubilada TTL TTL PAC TTL de la clave principal. Estas configuraciones se configuran por abandono en el Cisco Secure ACS:Mes de la clave principal TTL:1TTL dominante jubilado: 3 mesesPAC TTL: 1 semana
4. Complete el campo de **información ID de la autoridad**. Este texto se muestra en un cierto software de cliente del EAP-FAST donde está el regulador la selección de la autoridad PAC.**Nota:** El Cisco Secure Services Client no emplea este texto descriptivo para la autoridad PAC.
5. Elija el campo del **aprovisionamiento de la en-banda PAC de la permit**. Este campo habilita el aprovisionamiento automático PAC para los clientes apropiado-habilitados del EAP-FAST. Por este ejemplo, se emplea el auto-aprovisionamiento.
6. Elija los **métodos internos permitidos**: EAP-GTC y EAP-MSCHAP2. Esto permite la operación del v1 del EAP-FAST y de los clientes del EAP-FAST v1a. (El Cisco Secure Services Client soporta el EAP-FAST v1a.) Si no es necesario apoyar a los clientes del v1 del EAP-FAST, es solamente necesario habilitar el EAP MSCHAPv2 como método interno.

7. Elija al **master del EAP-FAST casilla de selección del servidor** para habilitar este servidor del EAP-FAST como el master. Esto permite que otros servidores ACS utilicen este servidor como la autoridad del master PAC para evitar la disposición de las claves únicas para cada ACS en una red. Refiera a la guía de configuración de ACS para los detalles.
8. Haga clic
**Submit+Restart**.




## Controlador de WLAN de Cisco

Con el propósito de este Guía de despliegue, Cisco WS3750G regulador integrado del Wireless LAN (WLC) se utiliza con Cisco AP1240 AP ligeros (REVESTIMIENTO) para proporcionar la infraestructura WLAN para las pruebas CSSC. La configuración es aplicable para cualquier controlador de WLAN de Cisco. La versión de software empleada es 4.0.155.5.

# Configure el regulador del Wireless LAN

## Operación básica y registro del REVESTIMIENTO al regulador

Utilice al Asisitente de la configuración de inicio en el comando line interface(cli) para configurar el WLC para la operación básica. Alternativamente, usted puede utilizar el GUI para configurar el WLC. Este documento explica la configuración en el WLC con el Asisitente de la configuración de inicio en el CLI.

Después de que el WLC inicie por primera vez, ingresa en el Asisitente de la configuración de inicio. Utilice al asistente de configuración para configurar las configuraciones básicas. Usted puede acceder al Asisitente con el CLI o el GUI. Esta salida muestra un ejemplo del Asisitente de la configuración de inicio en el 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 la operación básica. 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 AP manager.

Antes de que cualquier otra función se pueda configurar en el WLCs, los revestimientos tienen que registrarse con el WLC. Este documento asume que el REVESTIMIENTO está registrado al WLC. Refiera al registro el AP ligero a la sección del WLCs de la Conmutación por falla del controlador de WLAN para el ejemplo de configuración de los Puntos de acceso ligeros para la información sobre cómo los AP ligeros se registran con el WLC. Para la referencia con este ejemplo de configuración, los AP1240s se despliegan en una subred distinta (10.10.81.0/24) del controlador de WLAN (10.10.80.0/24), y se utiliza la opción DHCP 43 de prever la detección del regulador.

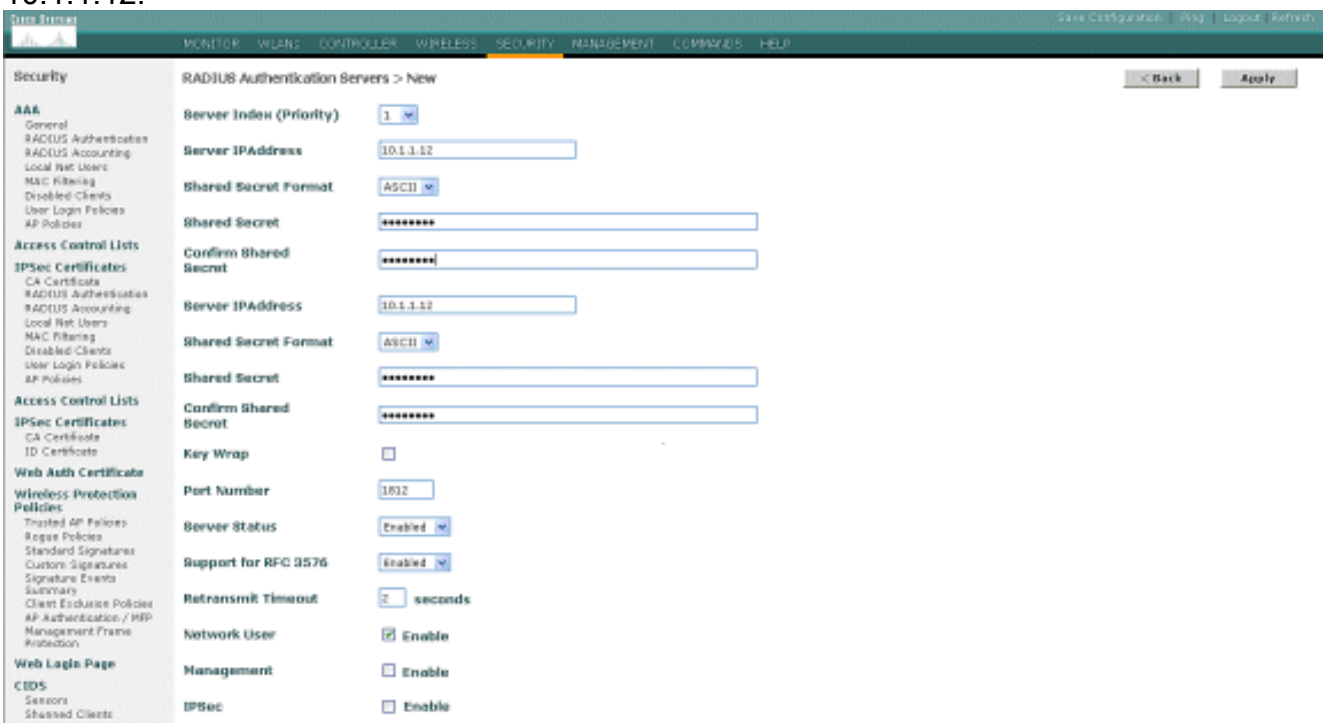
## Autenticación de RADIUS con el Cisco Secure ACS

El WLC necesita ser configurado para remitir los credenciales de usuario al servidor del Cisco Secure ACS. El servidor ACS después valida los credenciales de usuario (a través de la base de datos de Windows configurada) y proporciona el acceso a los clientes de red inalámbrica.

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

1. Haga clic la **Seguridad** y la **autenticación de RADIUS del** regulador GUI para visualizar la página de los servidores de autenticación de RADIUS. Entonces haga clic **nuevo** para definir al servidor
   ACS.


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



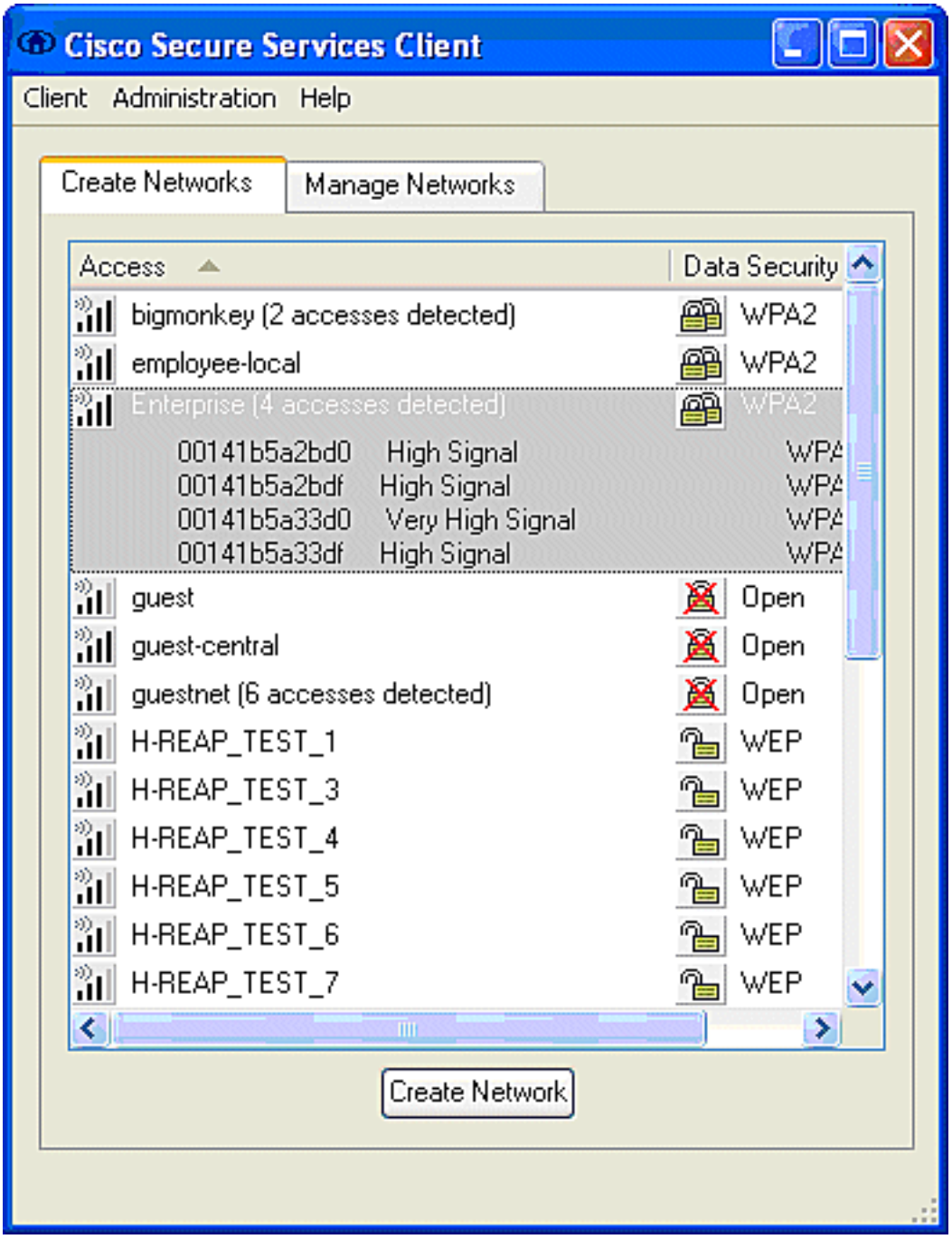

## Configuración de los parámetros de WLAN

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

Una vez que el software está instalado y se ejecuta como servicio, analiza para las redes disponibles y visualiza ésos disponibles.

**Nota:** CSSC inhabilita Windows cero Config.

**Nota:** Eso el SSID que se habilita para el broadcast es solamente visible.




**Nota:** El controlador de WLAN, por abandono, transmite 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 simplemente el **SSID** en la lista (empresa) y el botón de radio de la **red del crear**.

Si la infraestructura WLAN se configura con el broadcast SSID inhabilitado, usted debe agregar manualmente el SSID; haga clic el botón de radio del **agregar** bajo dispositivos de acceso y ingrese manualmente el **SSID** apropiado (por ejemplo, empresa). Configure el comportamiento activo de la sonda 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.

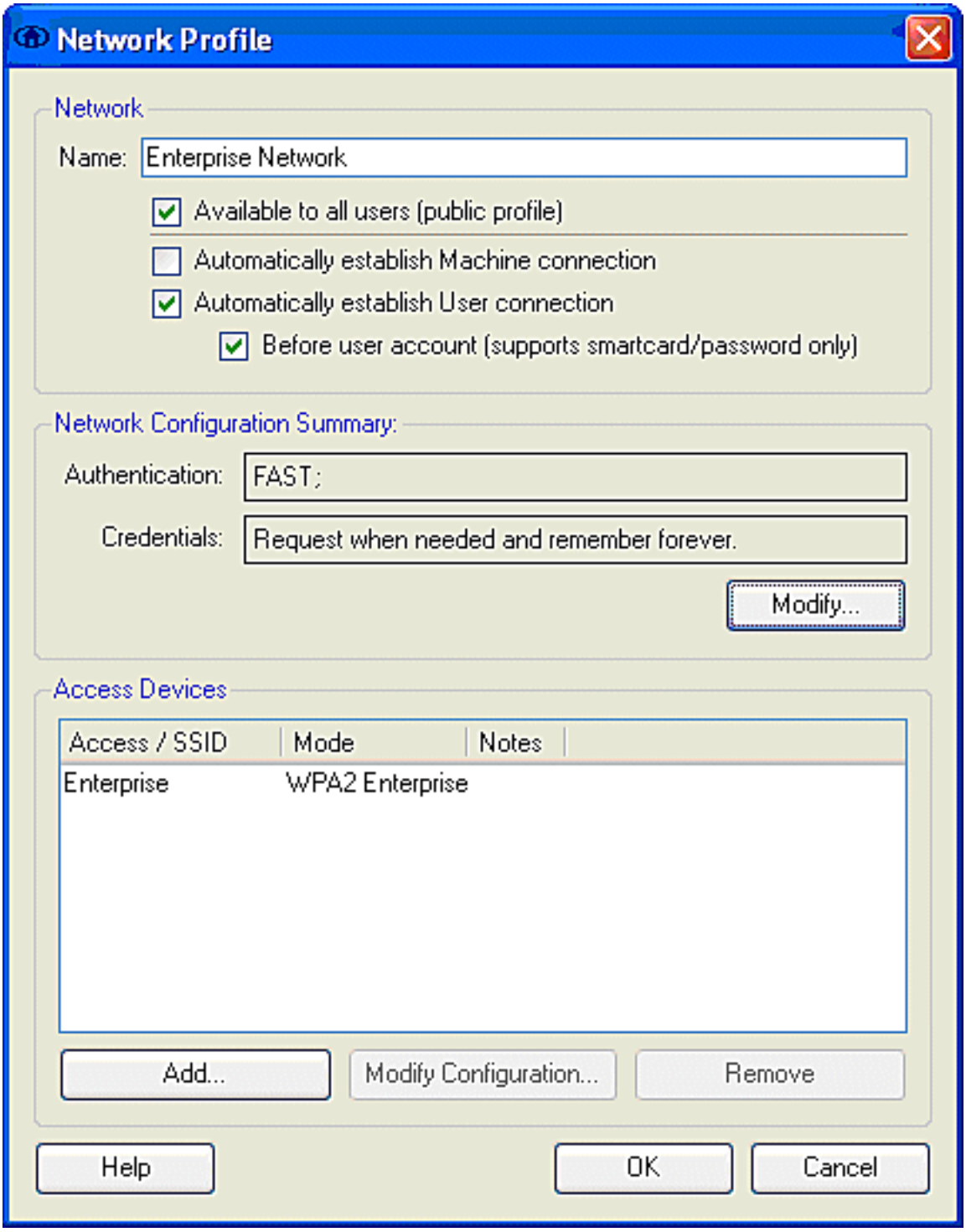
**Nota:** Las configuraciones de puerto no permiten a los modos de empresa (802.1x) si las configuraciones de la autenticación EAP no son primeras configuradas para el perfil.

El botón de radio de la **red del crear** inicia 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.

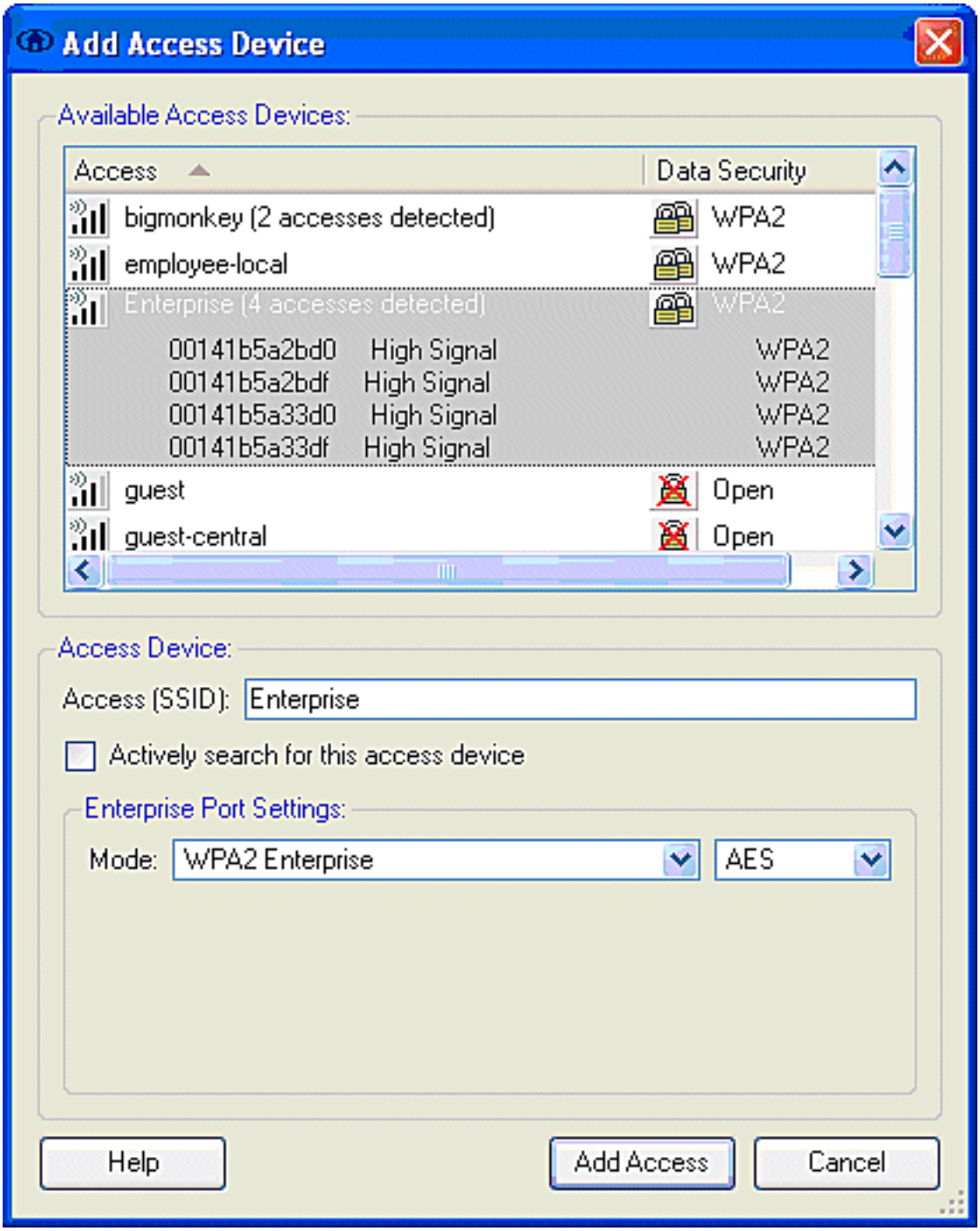
**Nota:** La Seguridad de WLAN múltiple teclea y/o los SSID pueden ser asociados bajo este perfil de la autenticación.

Para tener el cliente para conectar automáticamente con la red cuando en el intervalo de cobertura RF, elija **establecen automáticamente la conexión del usuario**. Desmarque **disponible a todos los usuarios** si no es deseable utilizar este perfil con otras cuentas de usuario en la máquina. Si **establezca automáticamente** no se elige, es necesario que el usuario abrir la ventana CSSC e inicie manualmente la conexión de la red inalámbrica (WLAN) con el botón de radio de la **conexión**.

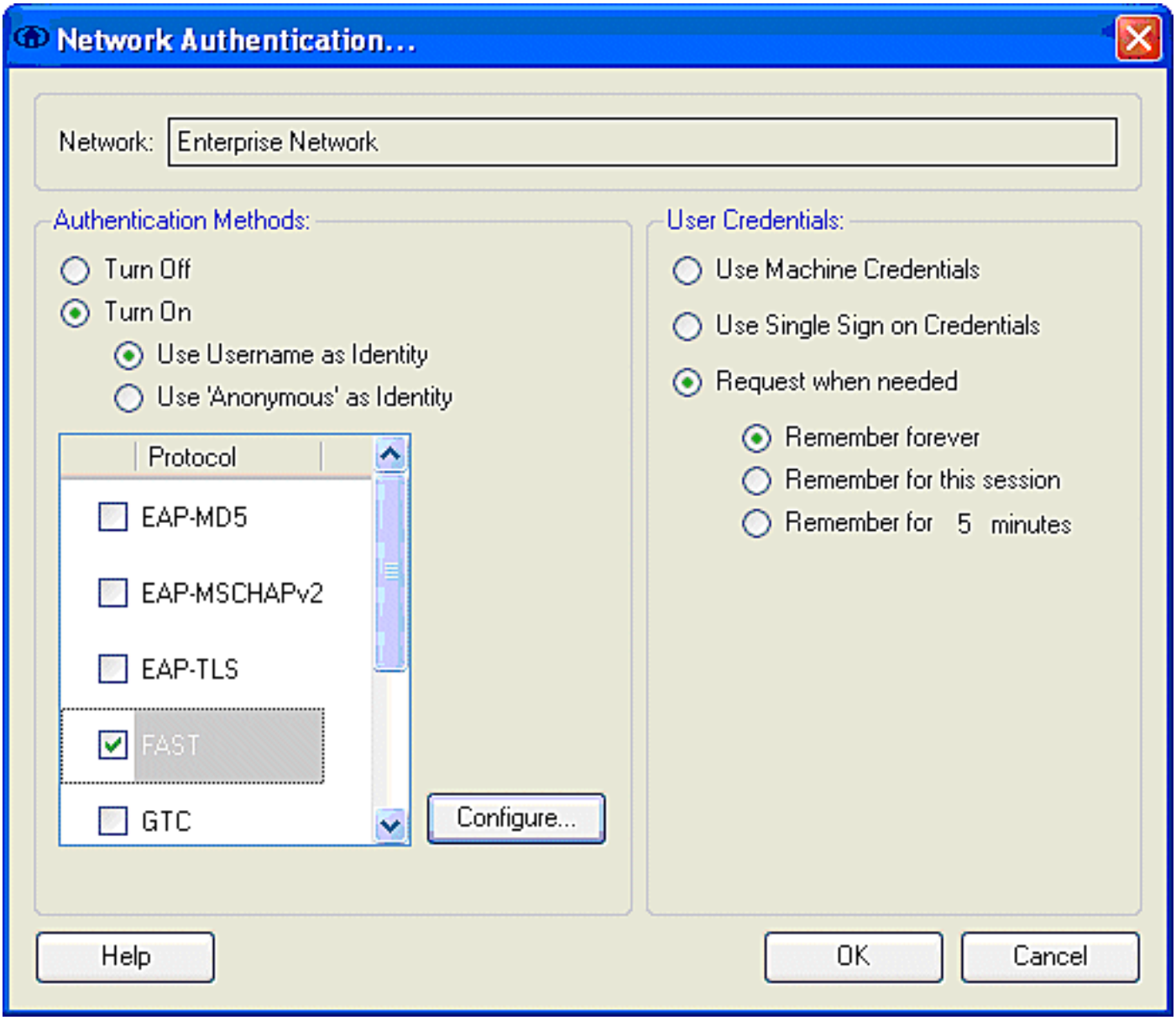
Si se desea para iniciar la conexión de la red inalámbrica (WLAN) antes del inicio del usuario, elija **antes de la cuenta de usuario**. Esto permite Solo-Muestra-en la operación con los credenciales de usuario guardados (contraseña o certificado/Smartcard cuando usted utiliza TLS dentro del EAP-FAST).



**Nota:** Para la operación WPA/TKIP con el adaptador del Cisco Aironet 350 Series Client, es necesario inhabilitar la validación del apretón de manos WPA puesto que hay actualmente una incompatibilidad entre el cliente CSSC y 350 drivers en cuanto al apretón de manos WPA desmenuce la validación. Esto se inhabilita bajo el **cliente > las configuraciones avanzadas > WPA/WPA2 validación del apretón de manos**. La validación discapacitada del apretón de manos todavía permite las funciones de seguridad inherentes en el WPA (el cerrar por paquete y Message Integrity Check TKIP), pero inhabilita la clave de autentificación inicial WPA.




Conforme al resumen de la configuración de red, el tecleo **se modifica** para configurar el EAP/las configuraciones de las credenciales. Especifique **giran la** autenticación, eligen **RÁPIDAMENTE** bajo protocolo, y eligen **"anónimo" como identidad** (para no utilizar ningún nombre de usuario en la petición inicial EAP). Es posible utilizar el **nombre de usuario del uso como Identityas la** identidad externa EAP, pero muchos clientes no desean exponer las identificaciones del usuario en la petición unencrypted inicial EAP. Especifique la **sola muestra del uso en las credenciales** de utilizar los credenciales de inicio de sesión para la autenticación de red. Haga clic la **configuración** para configurar los parámetros del EAP-FAST.




Bajo configuraciones RÁPIDAS, es posible especificar **valida el certificado de servidor**, que permite que el cliente valide el certificado del servidor del EAP-FAST (ACS) antes del establecimiento de una sesión del EAP-FAST. Esto proporciona la protección para los dispositivos del cliente contra la conexión a un servidor del EAP-FAST el desconocido o del granuja y el submittal inadvertido de sus credenciales de autenticación a una fuente untrusted. Esto requiere que el servidor ACS haga un certificado instalar y el cliente también hace el certificado correspondiente del Certificate Authority de la raíz instalar. En este ejemplo, la validación del certificado de servidor no se habilita.

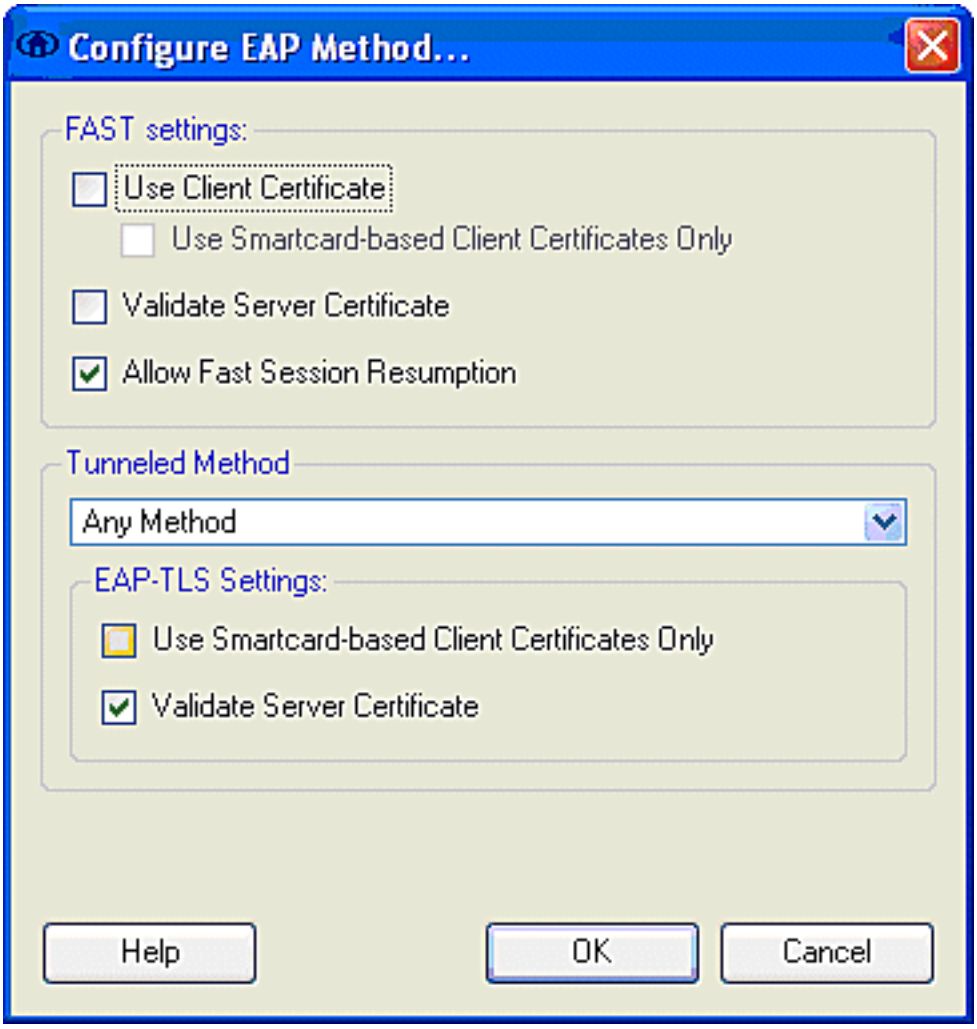
Bajo configuraciones RÁPIDAS, es posible especificar **permite la reanudación rápida de la sesión**, que permite la reanudación de una sesión del EAP-FAST basada sobre la información del túnel (sesión de TLS) bastante que el requisito de un reauthentication completo del EAP-FAST. Si el servidor y el cliente del EAP-FAST tienen vox populi de la información de la sesión de TLS negociada dentro del intercambio inicial de la autenticación del EAP-FAST, la reanudación de la sesión puede ocurrir.

**Nota:** El servidor y el cliente del EAP-FAST se deben configurar para el curriculum vitae de la sesión del EAP-FAST.

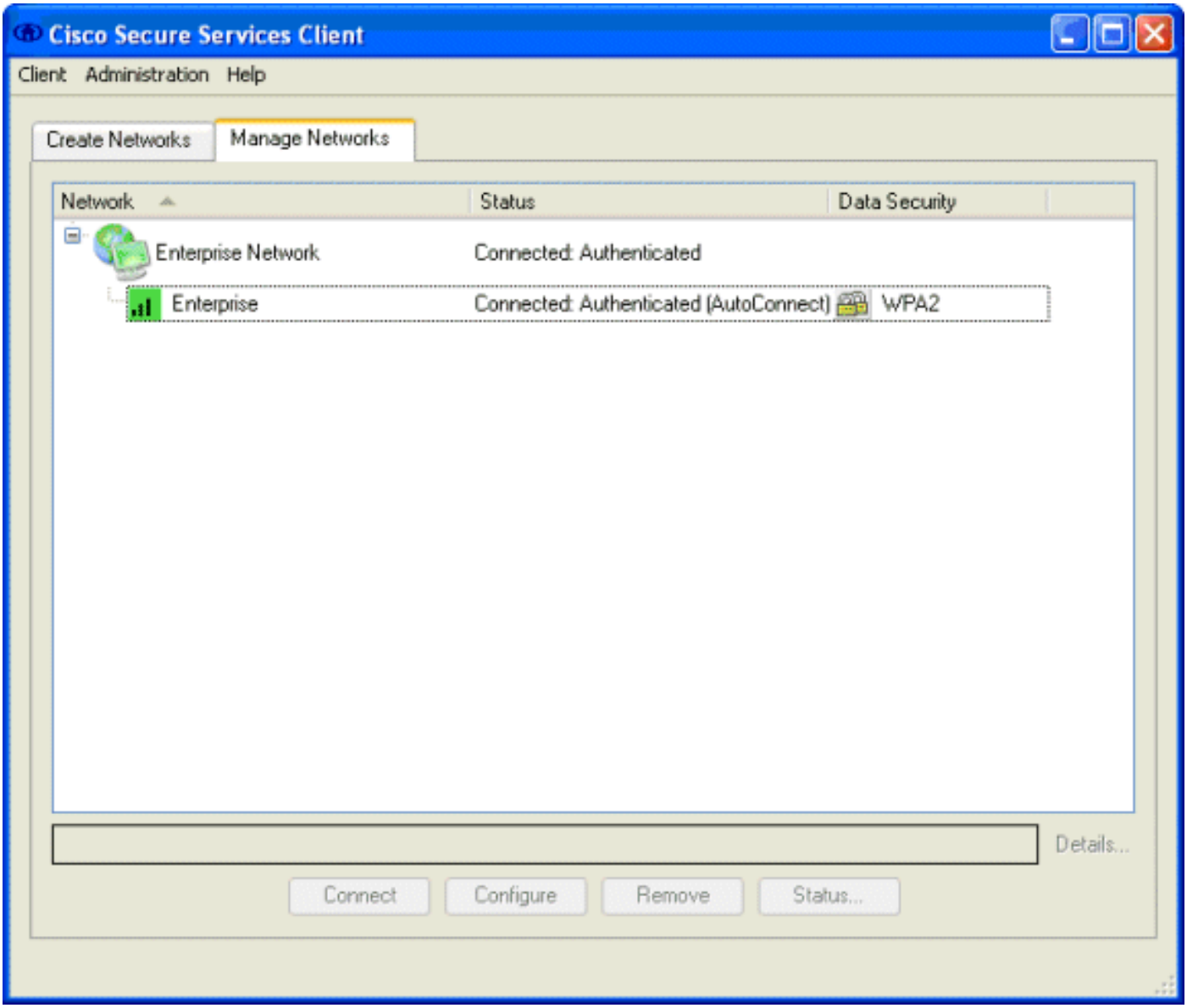
Bajo el método tunneled > configuraciones del EAP-TLS, especifique **cualquier método** para permitir el EAP MSCHAPv2 para la auto-disposición PAC y el EAP-GTC para la autenticación. Si

usted utiliza una base de datos del Microsoft-formato, tal como Active Directory, y si si no apoya a ninguna clientes del v1 del EAP-FAST en la red, usted puede también especificar el uso solamente del **MSCHAPv2** como el método tunneled.

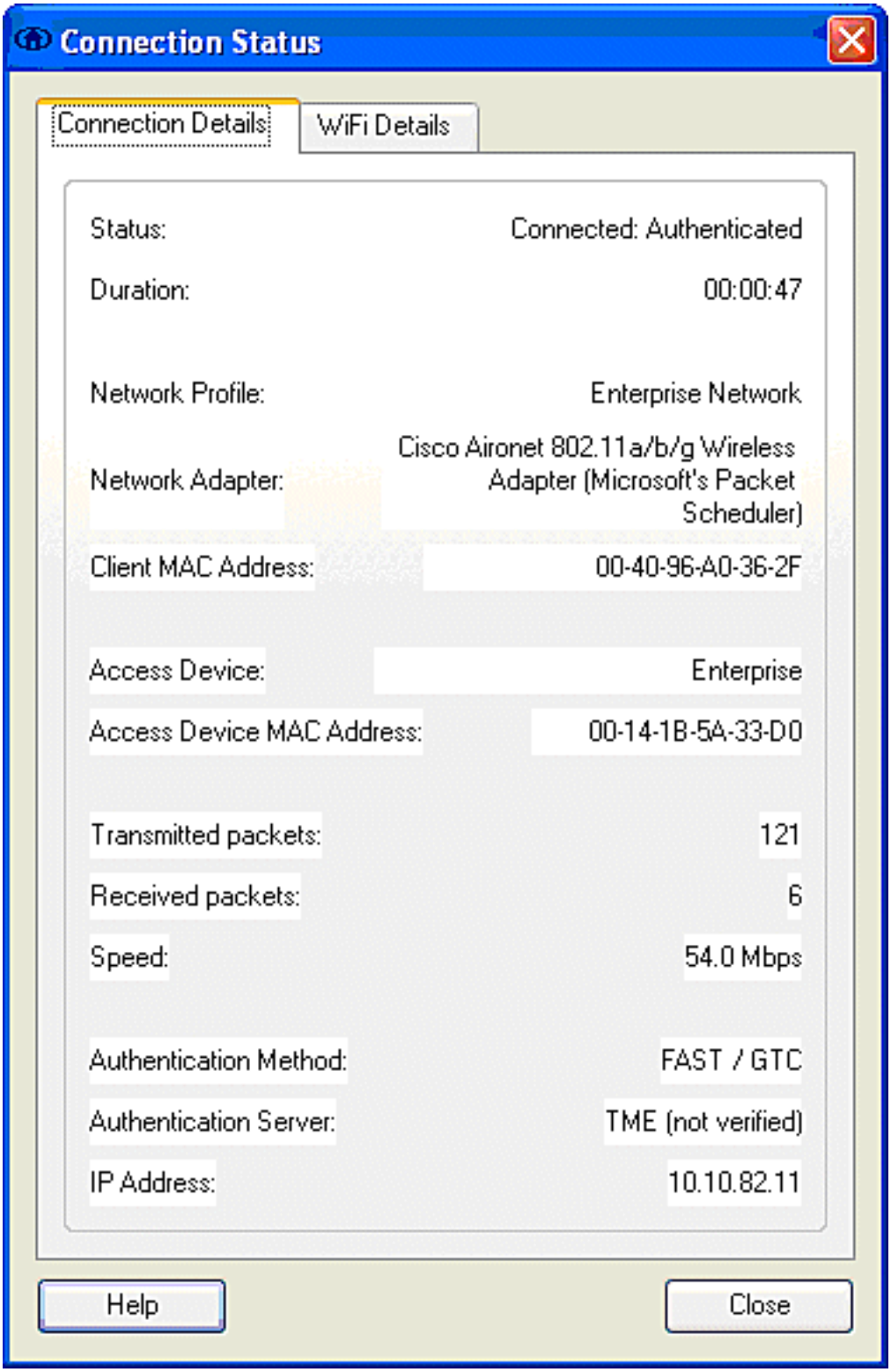
**Nota:** Valide el certificado de servidor se habilita por abandono bajo configuraciones del EAP-TLS en esta ventana. Puesto que el ejemplo no utiliza el EAP-TLS como el método de autentificación interno, este campo es no corresponde. Si se habilita este campo, permite al cliente para validar el certificado de servidor además de la validación del servidor del certificado del cliente dentro del EAP-TLS.

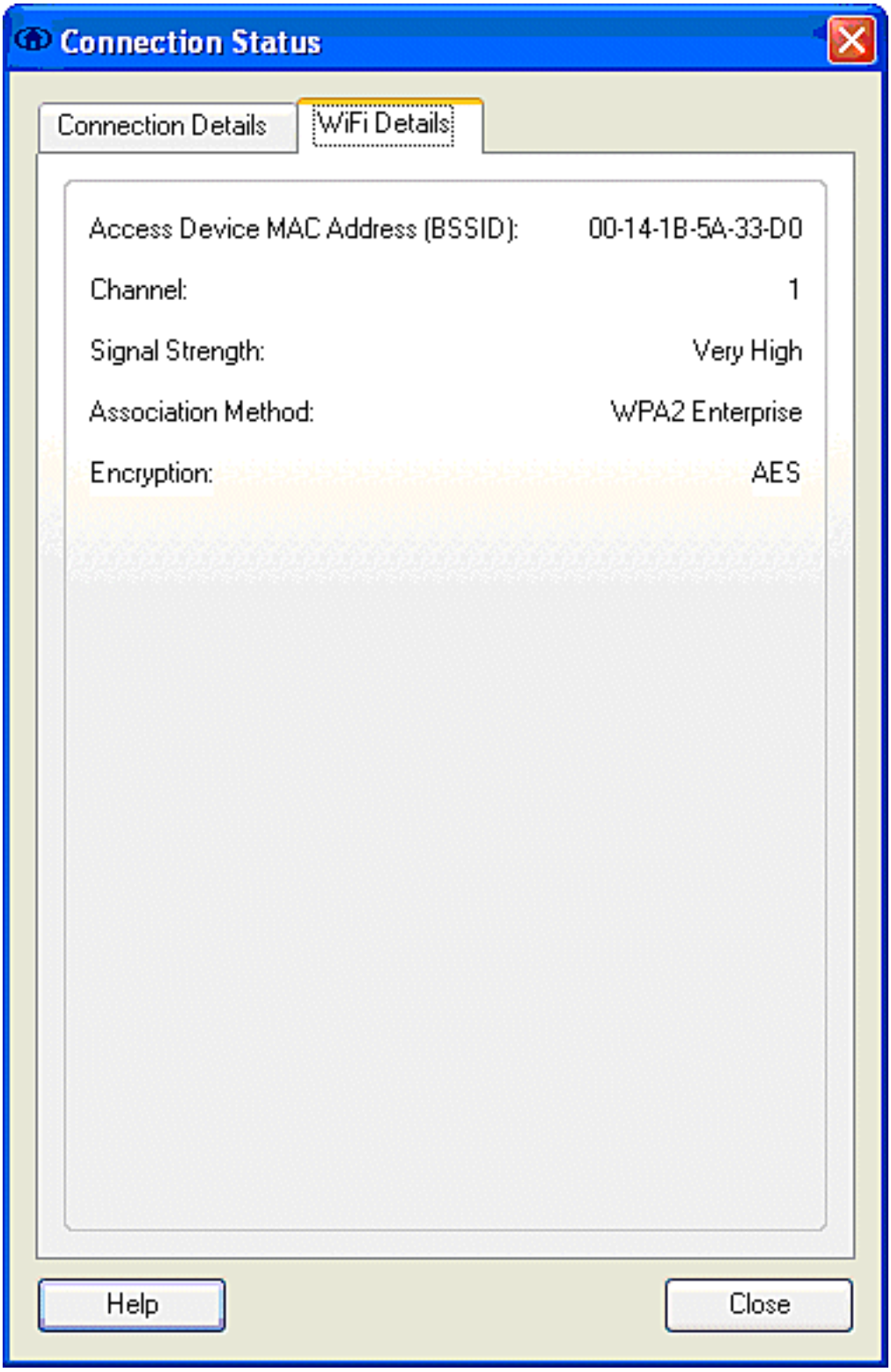



Haga Click en OK para salvar las configuraciones del EAP-FAST. Puesto que configuran al cliente para “automáticamente establezca” bajo perfil, él inicia automáticamente la asociación/la autenticación con la red. De la lengueta de las redes del manejo, los campos de la red, del estatus, y de seguridad de datos indican el estado de la conexión del cliente. Del ejemplo, se ve que la red para empresas del perfil es funcionando, y el dispositivo de acceso a la red es la empresa SSID, que indica conectado: Autenticado y las aplicaciones Autoconnect. El campo de seguridad de datos indica el tipo de encripción del 802.11 se emplea que, que, por este ejemplo, es WPA2.




Después de que el cliente autentique, elija el **SSID** bajo perfil en la lengueta 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 la información sobre el dispositivo del cliente, el estado de la conexión y las estadísticas, y el método de autentificación. La lengueta de los detalles de WiFi proporciona 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.


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 de sistema, le dan derecho a la utilidad de diagnóstico, el informe del sistema del Cisco Secure Services Client, que está disponible con la distribución estándar CSSC. Esta utilidad es disponible desde el menú Inicio o del directorio CSSC. Para obtener los datos, el tecleo **recoge los datos > la copia al tablero > localiza el archivo de informe**. Esto dirige una ventana del Explorador del archivo de Microsoft al directorio con el archivo de informe comprimido. Dentro del archivo comprimido, la mayoría de los datos útiles están situados bajo el registro (log_current).

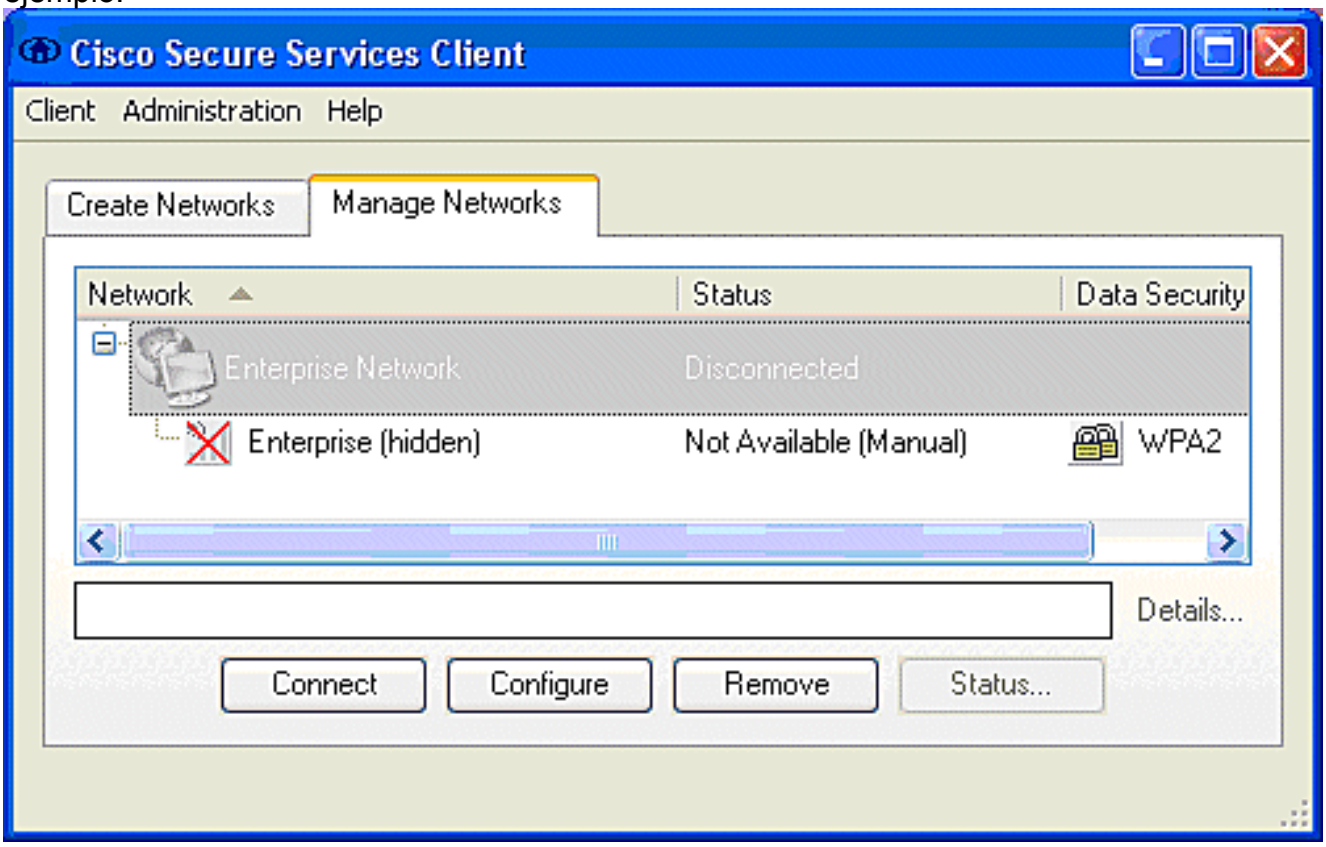
La utilidad da el estado actual de CSSC, interfaz, y los detalles del driver, junto con la información de la red inalámbrica (WLAN) (SSID detectado, estado de asociación, etc.). Esto puede ser útil, diagnosticar especialmente los problemas de conectividad entre CSSC y el adaptador WLAN.

# Verifique la operación

Después de la configuración del servidor del Cisco Secure ACS, del controlador de WLAN, del cliente CSSC, y de la población probablemente correcta de la configuración y de la base de datos, la red WLAN se configura para la autenticación del EAP-FAST y la Comunicación del cliente segura. Hay las puntas numerosas que se pueden monitorear para marcar el progreso/los errores para una sesión segura.

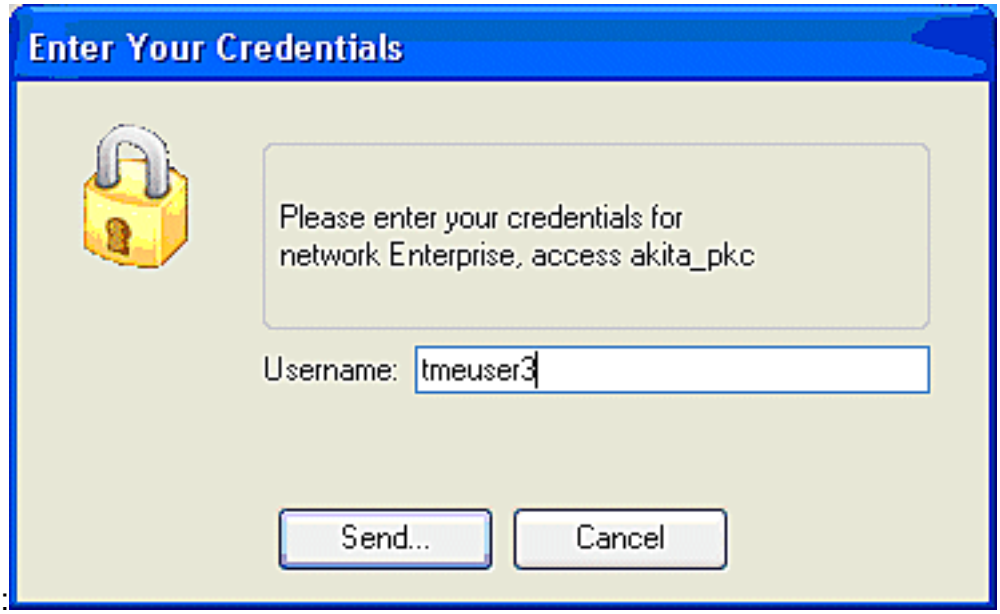
Para probar la configuración, intente asociar a un cliente de red inalámbrica al controlador de WLAN con la autenticación del EAP-FAST.

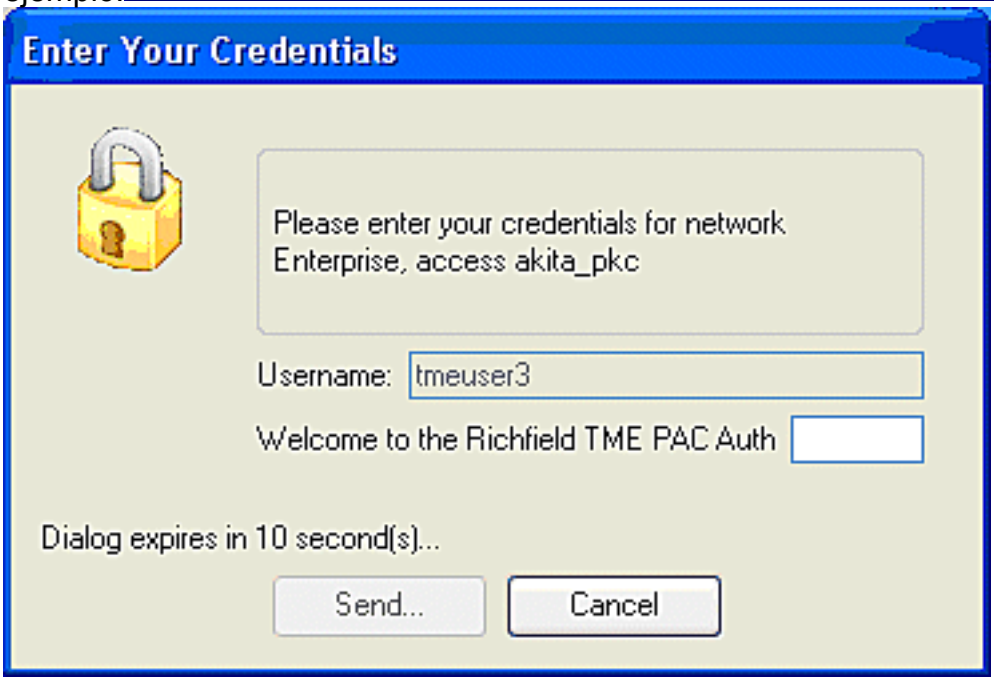
1. Si CSSC se configura para la Auto-conexión, el cliente intenta esta conexión automáticamente. Si no se configura para la Auto-conexión y escoge Muestra-en la operación, el usuario debe iniciar la conexión de la red inalámbrica (WLAN) a través del botón de radio de la **conexión**. Esto inicia el proceso de asociación del 802.11 sobre el cual la autenticación EAP ocurre.Aquí tiene un ejemplo:



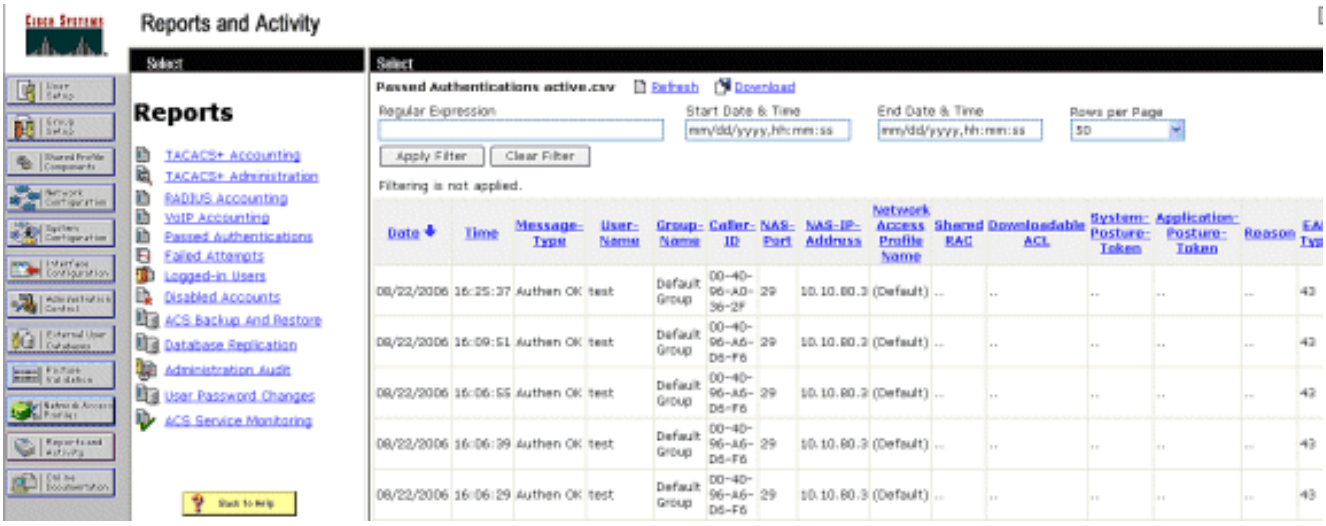

2. Se indica al usuario posteriormente que proporcione el nombre de usuario y entonces la contraseña para la autenticación del EAP-FAST (de la autoridad del EAP-FAST PAC o del ACS).Aquí tiene un

ejemplo:

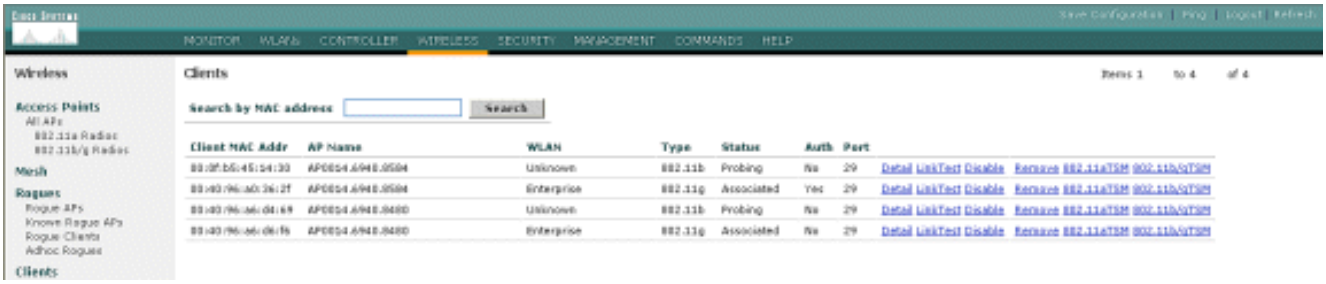



3. El cliente CSSC, por el WLC, entonces pasa los credenciales de usuario al servidor de RADIUS (Cisco Secure ACS) para validar las credenciales. El ACS verifica los credenciales de usuario con una comparación de los datos y de la base de datos configurada (en el ejemplo de configuración, la base de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




4. Sobre la autenticación acertada RADIUS/EAP, autentican al cliente de red inalámbrica (00:40:96:ab:36:2f en este ejemplo) con el controlador de WLAN AP/.




# Apéndice

Además del diagnóstico y de la información de estatus, que está disponible en el Cisco Secure ACS y el controlador de WLAN de Cisco, hay los puntos adicionales que se pueden utilizar para diagnosticar la autenticación del EAP-FAST. Aunque la mayoría de los problemas de la autenticación pueda ser diagnosticada sin el uso de un sniffer o de hacer el debug de la red inalámbrica (WLAN) los intercambios EAP en el controlador de WLAN, este material de referencia se incluye para ayudar a resolver problemas.

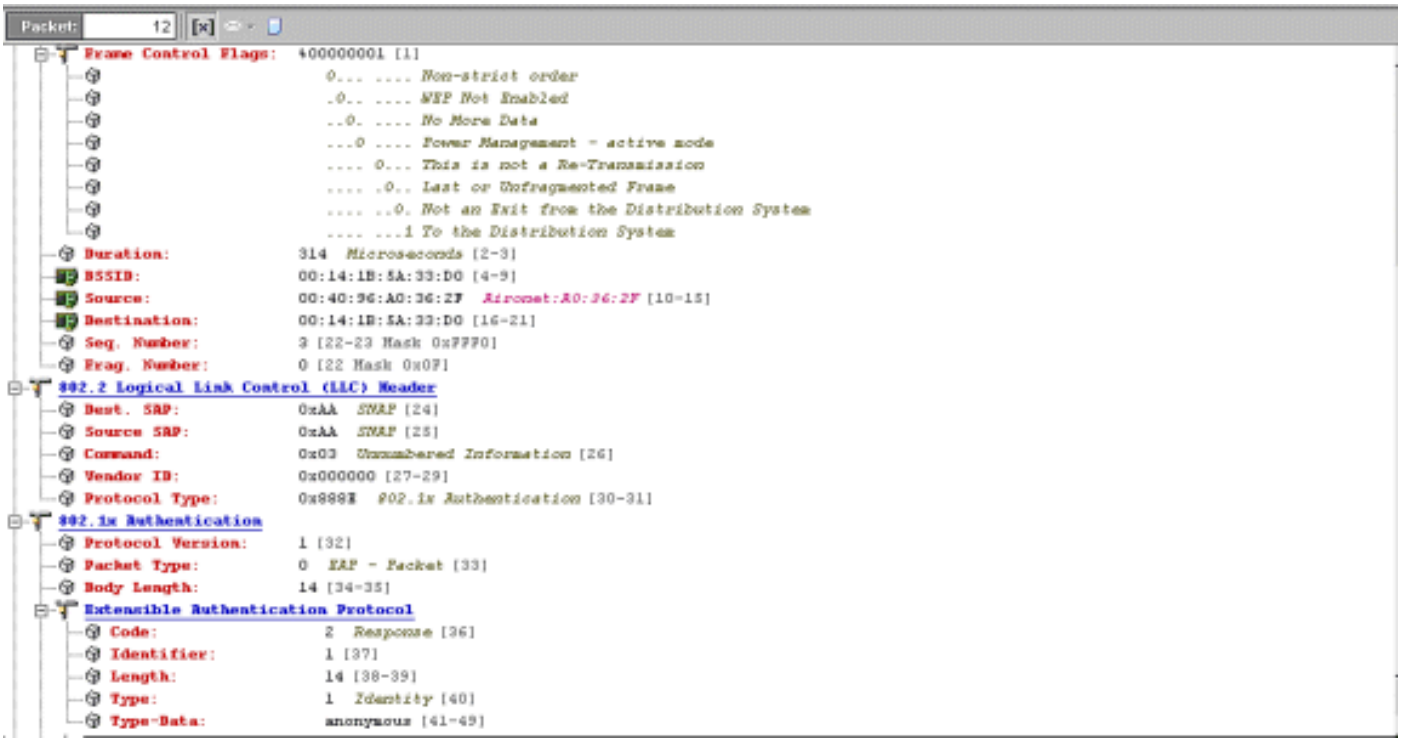
## Captura del sniffer para el intercambio del EAP-FAST

Esta captura del sniffer del 802.11 muestra el intercambio de la 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 inicial del EAP-FAST EAP.

**Nota:** Según lo configurado en el cliente CSSC, anónimo se utiliza como la identidad externa EAP en la respuesta inicial EAP.




## Debug en el controlador de WLAN

Estos comandos debug pueden ser empleados en el controlador de WLAN para monitorear el progreso del intercambio de la autenticación:

- **permiso de los eventos aaa del debug**
- **permiso del detalle aaa del debug**

- permiso de los eventos del dot1x del debug
- permiso de los estados del dot1x del debug

Éste es un ejemplo del comienzo de una transacción de la autenticación entre el cliente CSSC y el ACS según lo monitoreado en el controlador de 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)
```

Ésta es la terminación satisfactoria del intercambio EAP del debug del regulador (con la 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 para el servidor del Cisco Secure ACS for Windows
- Guía de configuración para el Cisco Secure ACS 4.1
- Restrinja el acceso de la red inalámbrica (WLAN) basado en el SSID con el WLC y el ejemplo de configuración del Cisco Secure ACS
- EAP-TLS bajo red inalámbrica unificada con ACS 4.0 y Windows 2003
- Asignación del VLAN dinámico con el servidor de RADIUS y el ejemplo de la configuración de controlador del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems