

Cisco Secure Services Client con la autenticación del EAP-FAST

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisito](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Parámetros de diseño](#)

[Base de datos](#)

[Cifrado](#)

[Escoja Muestra-en y las credenciales de la máquina](#)

[Diagrama de la red](#)

[Configure el servidor del control de acceso \(ACS\)](#)

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

[Configure ACS para preguntar la base de datos externa](#)

[Active la ayuda del EAP-FAST en el ACS](#)

[Regulador de la red inalámbrica \(WLAN\) de Cisco](#)

[Configure el regulador LAN de la Tecnología inalámbrica](#)

[Operación básica y registro del REVESTIMIENTO al regulador](#)

[Autenticación de RADIUS con Cisco ACS seguro](#)

[Configuración de los parámetros de la red inalámbrica \(WLAN\)](#)

[Verifique la operación](#)

[Appendix](#)

[Captura del sniffer para el intercambio del EAP-FAST](#)

[Depuración en el regulador de la red inalámbrica \(WLAN\)](#)

[Información Relacionada](#)

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 encriptación 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-activado 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 (Seguridad de LAN inalámbrica) del estándar 802.11i para activar la autenticación, la autorización, y las funciones de contabilidad basadas layer-2 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 ejecutada con el protocolo asegurado del túnel (EAP-FAST) como protocolo estándar-basado EAP disponible para el despliegue en las redes atadas con alambre y 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 (PACs) y se pueden distribuir automáticamente (aprovisionamiento automático o de la En-banda) o manualmente (aprovisionamiento manual o fuera de banda) a los dispositivos 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 menos del hace un uso intensivo del procesador EAP tipo más rápido y de los que proporcionen a 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 LAN inalámbrico 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
- Ayuda para la ejecución del script de la clave
- Ayuda del Acceso protegido de Wi-Fi (WPA) sin el suplicante 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, ayuda 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 cliente apropiado

[prerrequisitos](#)

Requisito

Hay una suposición que el instalador tiene conocimiento de la instalación básica de Windows 2003 y de la instalación de Cisco WLC 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 servidor 2000 de Microsoft Windows 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
- Cisco 1242 LWAPP AP
- Windows 2000 con el Active Directory
- Cisco Catalyst 3750G Switch
- Windows XP con la versión 4.05 del indicador luminoso LED amarillo de la placa muestra gravedad menor y del Cisco Secure Services Client del adaptador CB21AG

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 de la red inalámbrica (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 fichero 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 fichero PAC al cliente. Después de que el PAC provisioned con éxito, el fichero 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 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 utilice el formato MSCHAPv2 (tal como OTP, Novell, o LDAP), se requiere emplear un cierto otro mecanismo (es decir, aprovisionamiento manual o aprovisionamiento autenticado) para desplegar los ficheros PAC del usuario. 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 encriptación específico de la red inalámbrica (WLAN). Las capacidades del indicador luminoso LED amarillo de la placa muestra gravedad menor NIC del cliente determina al tipo de encriptación de la red inalámbrica (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 la red inalámbrica (WLAN) de Cisco permite la coexistencia del WPA2 y de los dispositivos del cliente WPA en un SSID común.

Si los dispositivos cliente no utilizan 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 encriptación 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 tarifas 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 tener acceso a las aplicaciones múltiples o a 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 una PC para la autenticación a la red inalámbrica (WLAN).

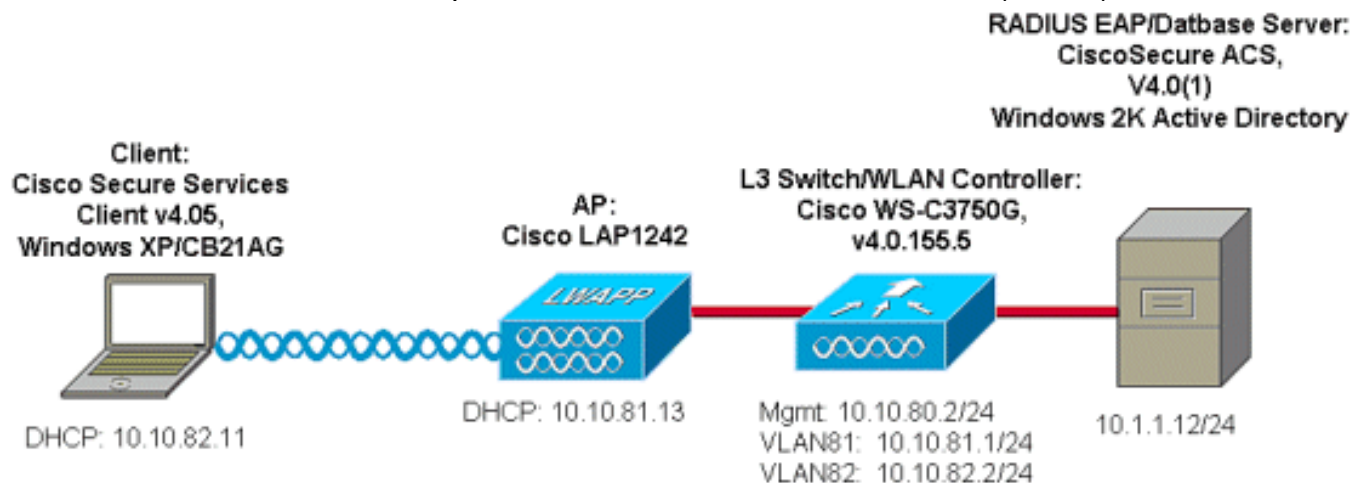
Con el Cisco Secure Services Client, es posible utilizar los credenciales de inicio de sesión de un usuario también para autenticar a la red de la red inalámbrica (WLAN). Si se desea para autenticar una PC a la red antes del inicio del usuario a la PC, se requiere para utilizar los credenciales de usuario 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 cargadores del programa inicial de la 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 inalámbrico integrado 3750G LAN del catalizador proporciona a la potencia sobre los switchports de los Ethernetes (POE), la transferencia L3, y la capacidad del regulador de la red inalámbrica (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 regulador de la red inalámbrica (WLAN).
3. La red 10.10.81.0 es la red donde residen los APs.
4. La red 10.10.82.0 se utiliza para los clientes de la red inalámbrica (WLAN).



[Configure el servidor del control de acceso \(ACS\)](#)

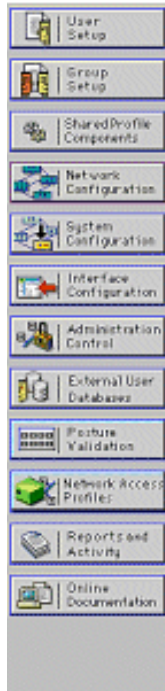
En esta sección encontrará la información para configurar las funciones descritas en este documento.

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 ACS](#)

Esta sección describe cómo configurar ACS para el EAP-FAST con el aprovisionamiento PAC de la en-banda 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 regulador de la red inalámbrica (WLAN), dirección IP, clave secreta compartida, y debajo autentiíquelo usando, elija el RADIUS (Cisco Airespace), que también incluye los atributos IETF RADIUS. **Nota:** Si se activan los grupos de dispositivos de red (NDG), primero elija el NDG apropiado y agregue el regulador de la red inalámbrica (WLAN) a él. Refiera a la guía de configuración ACS para más información sobre el NDG.
3. **Reinicio del teclado**
Submit+.



AAA Client Setup For ws-3750

AAA Client IP Address	<input type="text" value="10.10.80.3"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

[Back to Help](#)

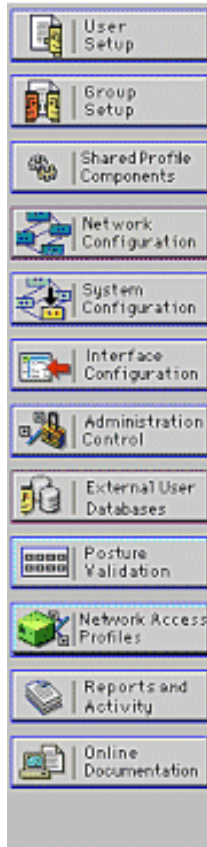
[Configure ACS para preguntar la base de datos externa](#)

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

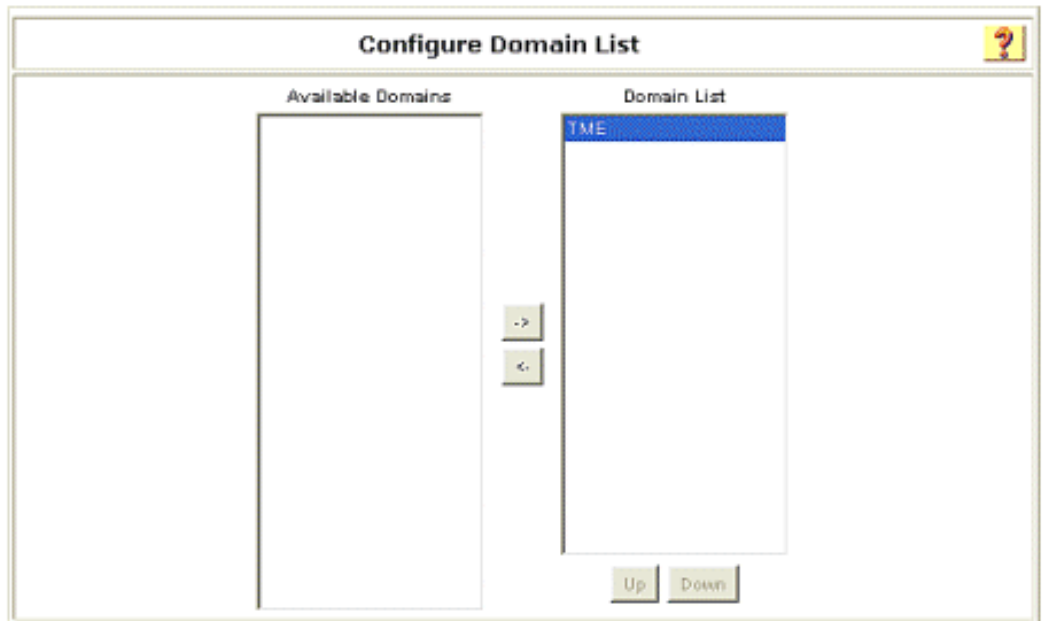
1. **La Base de datos de usuarios externa > la configuración de la base de datos > la base de datos de Windows del teclado > configuran.**
2. Bajo configure lista de dominio, los **dominios del** movimiento de los dominios disponibles a lista de dominio. **Nota:** El servidor que ejecuta el ACS debe tener conocimiento de estos dominios para que la aplicación ACS detecte y utilice esos dominios para los fines de autenticación.



External User Databases



If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you may enable this option.



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 Cisco ACS seguro 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 no--EAP MS-CHAP. Para activar la contraseña cambie conjuntamente con el EAP-FAST, él es necesario activar el cambio de la contraseña bajo configuraciones de Windows EAP.



External User Databases

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Windows EAP Settings

Enable password change inside PEAP or EAP-FAST.
 EAP-TLS Strip Domain Name.

Machine Authentication.

Enable PEAP machine authentication.
 Enable EAP-TLS machine authentication.
EAP-TLS and PEAP machine authentication name prefix:
 Enable machine access restrictions.
Aging time (hours):
Group map for successful user authentication without machine authentication:
User Groups that are exempt from passing machine authentication:

Available User Groups		Selected User Groups
Default Group		
Group 1		
Group 2		
Group 3		
Group 4		
Group 5		
Group 6		
Group 7		
Group 8		

These settings can be used to enable or disable specific Windows EAP functionality

- 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**.
- Mueva la base de datos de Windows desde las **bases de datos externas** a las **bases de datos seleccionadas**.
- Haga clic en **Submit** (Enviar). **Nota:** Desde aquí, el ACS controla el DB de Windows. 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 acceso-derechos necesitan ser configuradas en Windows. Refiera a la [guía de instalación para Cisco ACS seguro para el Servidor Windows](#) para los detalles.

External User Databases

Edit

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the ACS Internal Database.

Fail the attempt
 Check the following external user databases

External Databases	Selected Databases
	Windows Database@Wind...

The internal database.
 The database in which the user profile is held.

[Active la ayuda del EAP-FAST en el ACS](#)

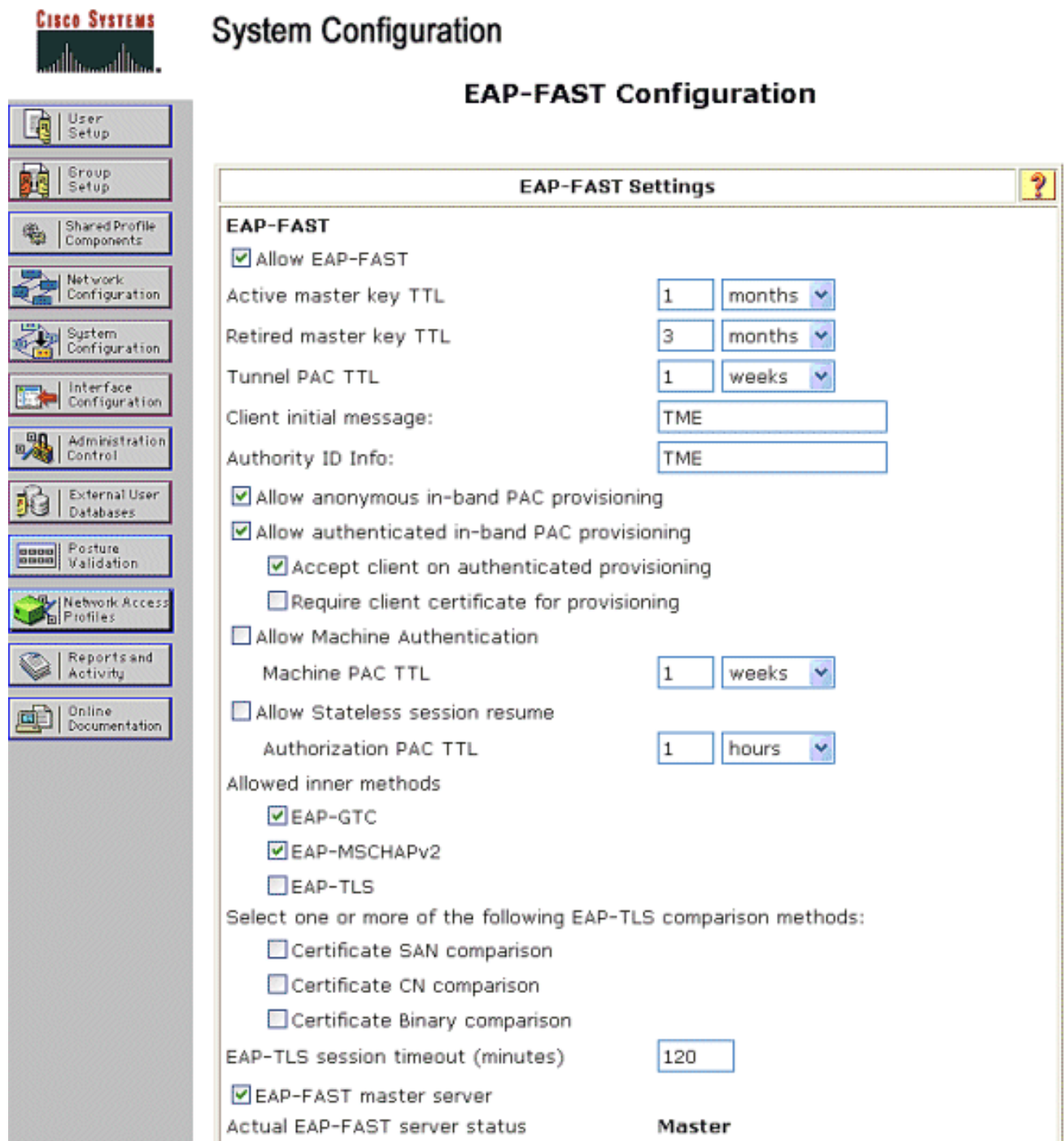
Esta sección describe cómo activar la ayuda del EAP-FAST en el ACS.

1. Va a la **configuración del sistema > la autenticación global puesta > 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 Cisco ACS seguro: 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 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 PAC de la en-banda de la permit**. Este campo activa el aprovisionamiento automático PAC para los clientes apropiado-activados 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 de los clientes del EAP-FAST v1 y del EAP-FAST v1a. (El Cisco Secure Services Client utiliza el EAP-FAST v1a.) Si no es necesario apoyar a los clientes del EAP-FAST v1, es solamente necesario activar EAP-MSCHAPv2 como método interno.

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

8. Haga clic

Submit+Restart.



The screenshot shows the Cisco System Configuration interface for EAP-FAST. On the left is a navigation menu with options like User Setup, Group Setup, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'EAP-FAST Configuration' and contains the 'EAP-FAST Settings' window. The settings include:

- Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: TME
- Authority ID Info: TME
- Allow anonymous in-band PAC provisioning
- Allow authenticated in-band PAC provisioning
 - Accept client on authenticated provisioning
 - Require client certificate for provisioning
- Allow Machine Authentication
 - Machine PAC TTL: 1 weeks
- Allow Stateless session resume
 - Authorization PAC TTL: 1 hours
- Allowed inner methods:
 - EAP-GTC
 - EAP-MSCHAPv2
 - EAP-TLS
- Select one or more of the following EAP-TLS comparison methods:
 - Certificate SAN comparison
 - Certificate CN comparison
 - Certificate Binary comparison
- EAP-TLS session timeout (minutes): 120
- EAP-FAST master server
- Actual EAP-FAST server status: **Master**

[Regulador de la red inalámbrica \(WLAN\) de Cisco](#)

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

Configure el regulador LAN de la Tecnología inalámbrica

Operación básica y registro del REVESTIMIENTO al regulador

Utilice al Asistente 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 Asistente de la configuración de inicio en el CLI.

Después de los cargadores del programa inicial WLC por primera vez, ingresa en el Asistente de la configuración de inicio. Utilice al asistente de configuración para configurar las configuraciones básicas. Usted puede tener acceso al Asistente a través del CLI o del GUI. Esta salida muestra un ejemplo del Asistente 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 pusieron 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 del interfaz del AP-encargado.

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 de WLCs de la Conmutación por falla del regulador de la red inalámbrica \(WLAN\) por el ejemplo de la configuración de los Puntos de acceso ligeros](#) para la información sobre cómo los APs ligeros se registran con el WLC. Para la referencia con este ejemplo de la configuración, los AP1240s se despliegan en una subred distinta (10.10.81.0/24) del regulador de la red inalámbrica (WLAN) (10.10.80.0/24), y la opción 43 del DHCP se utiliza para prever el descubrimiento del regulador.

[Autenticación de RADIUS con Cisco ACS seguro](#)

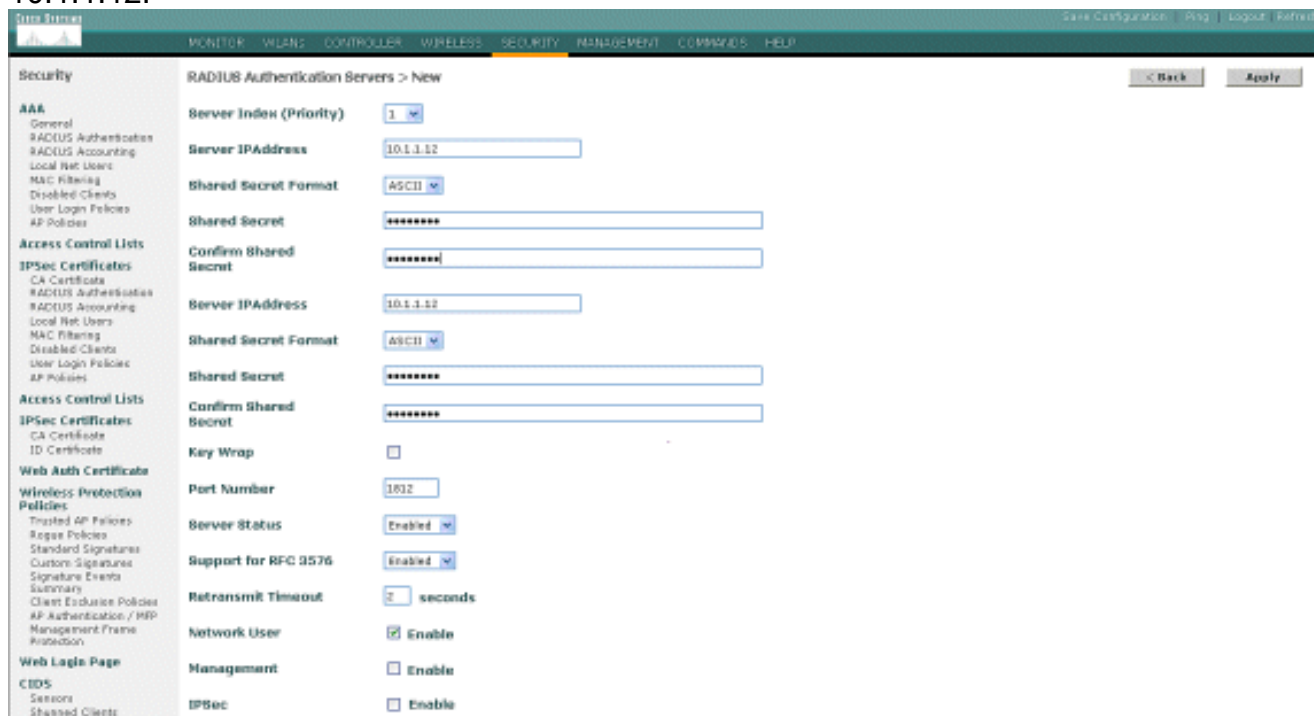
El WLC necesita ser configurado para remitir los credenciales de usuario a Cisco asegura al servidor ACS. El servidor ACS después valida los credenciales de usuario (a través de la base de datos de Windows configurada) y proporciona al acceso a los clientes de red inalámbrica.

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

1. Haga clic la **Seguridad** y la **autenticación de RADIUS** del GUI del regulador 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 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 de la red inalámbrica (WLAN)) y la Administración (es decir, usuarios administradores). El ejemplo de configuración utiliza Cisco ACS seguro como el servidor de RADIUS con la dirección IP 10.1.1.12:



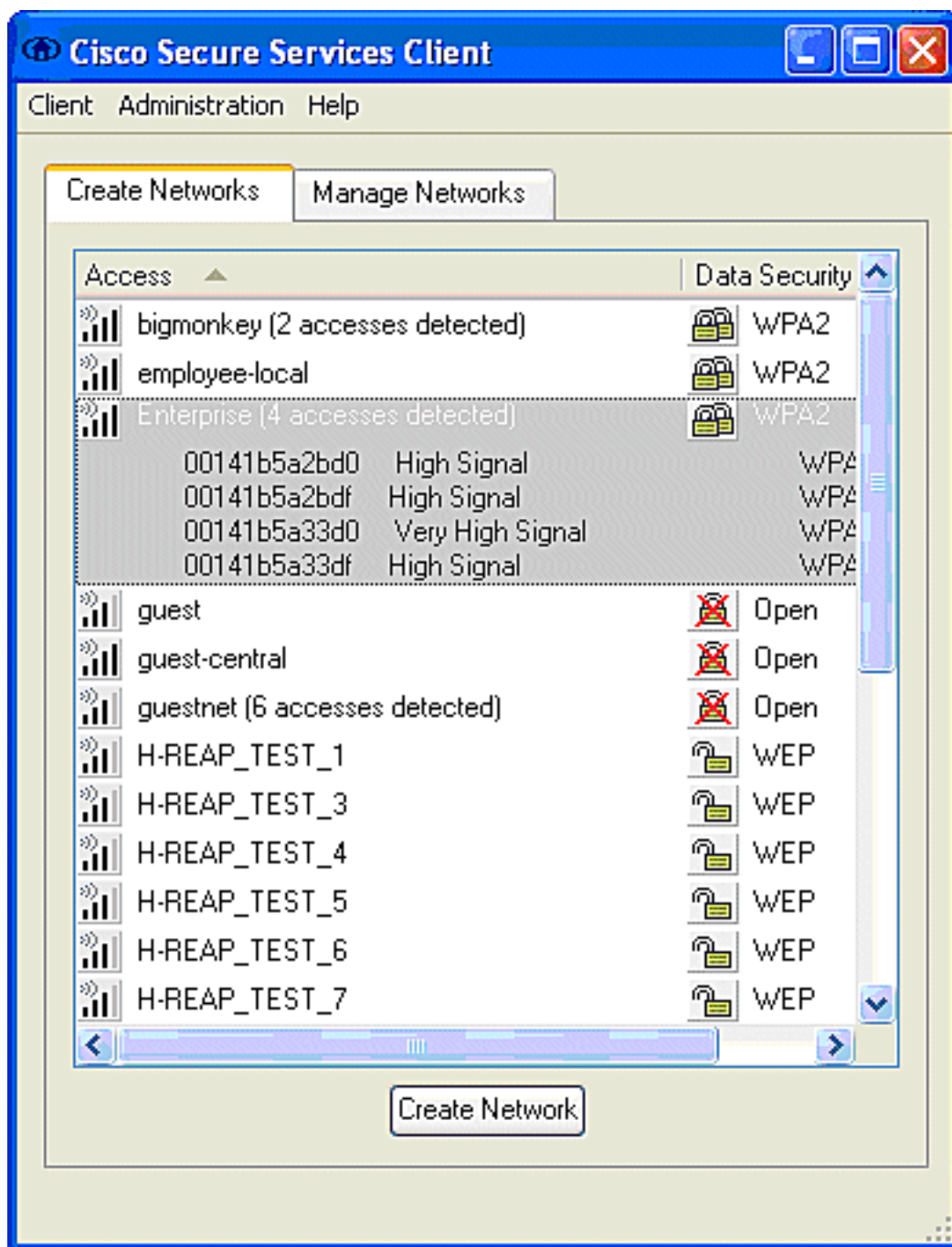
[Configuración de los parámetros de la red inalámbrica \(WLAN\)](#)

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 de Cisco CB21AG. 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 éstos disponibles.

Nota: CSSC inhabilita Windows cero Config.

Nota: Eso el SSID que se activa para la difusión es solamente visible.



Nota: El regulador de la red inalámbrica (WLAN), por abandono, difunde el SSID, así que se muestra en la lista de las redes del crear de SSID analizados. Para crear un perfil de la red, usted puede hacer clic simplemente el **SSID** en la lista (empresa) y el botón de radio de la **red del crear**.

Si la infraestructura WLAN se configura con la difusión SSID inhabilitada, 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 punta de prueba para el cliente, es decir, donde el cliente sonda activamente para su SSID configurado; especifique **activamente la búsqueda para este dispositivo de acceso** después de que usted ingrese el SSID en la ventana del dispositivo de acceso del agregar.

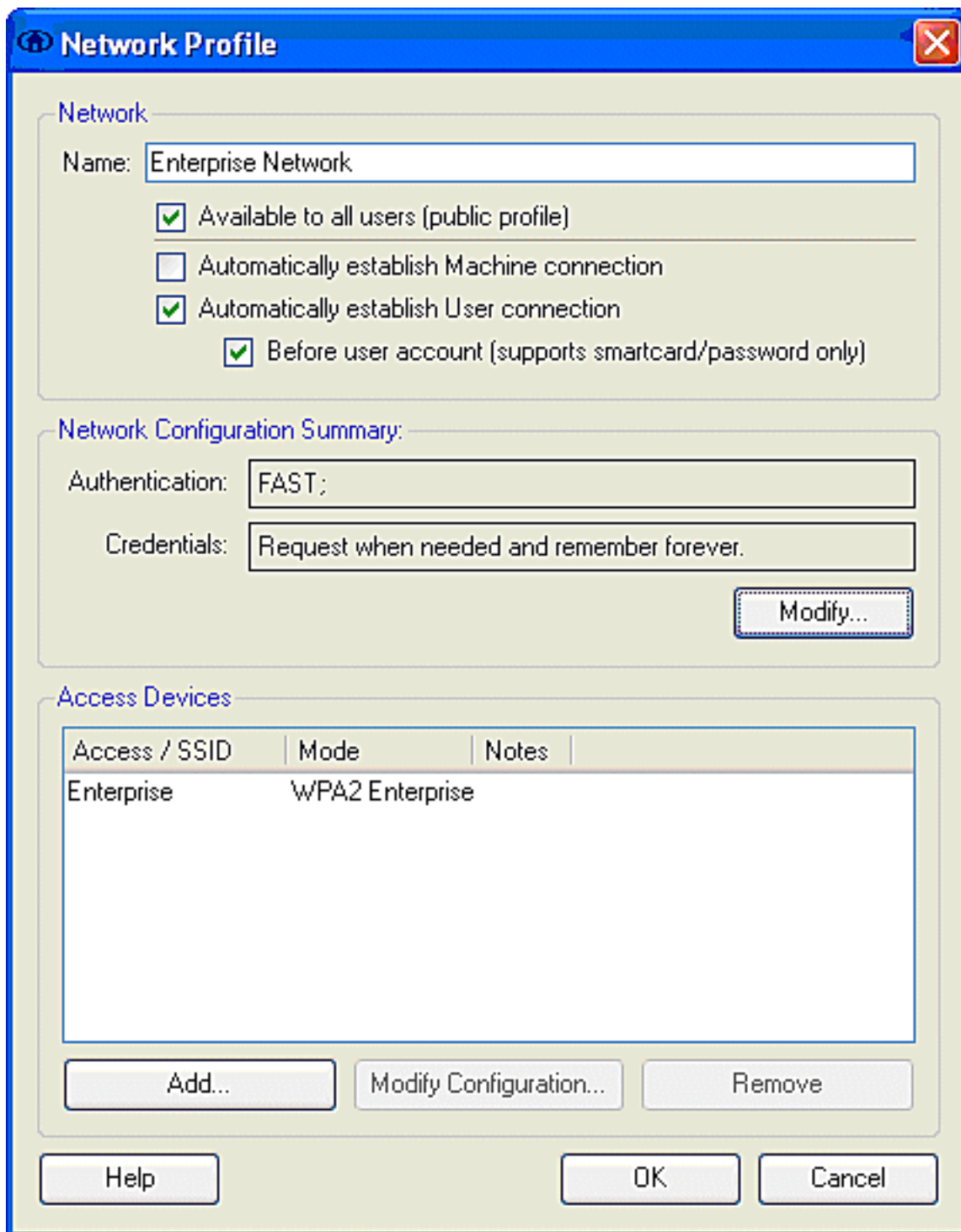
Nota: Las configuraciones de puerto no permiten los modos de la empresa (802.1x) si las configuraciones de la autenticación EAP no son primeras configuradas para el perfil.

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

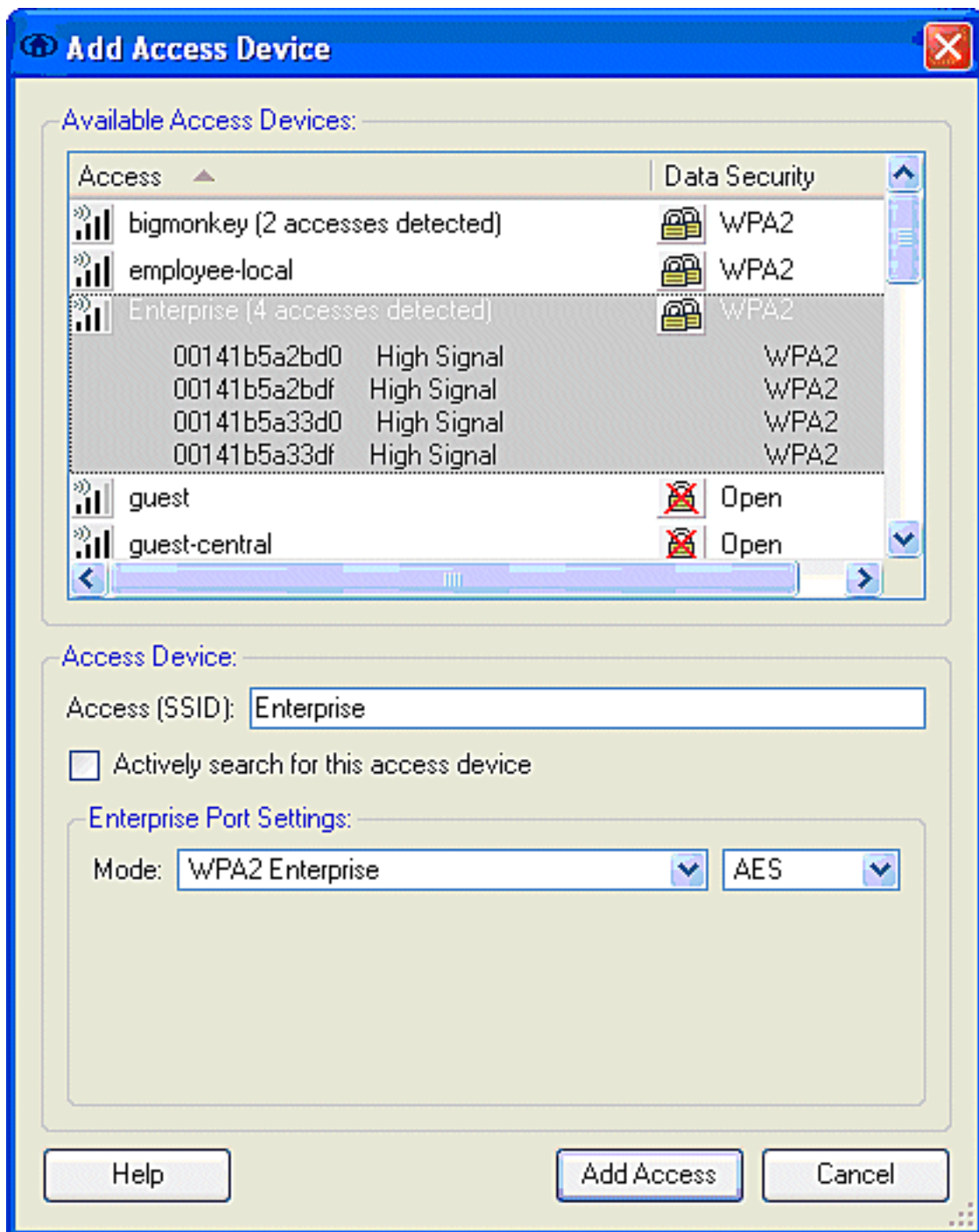
Nota: Los tipos múltiples de la Seguridad de WLAN y/o los SSID pueden ser asociados bajo este perfil de la autenticación.

Para tener el cliente para conectar automáticamente con la red cuando en el rango de la cobertura RF, elija **establecen automáticamente la conexión del usuario**. Uncheck **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**.

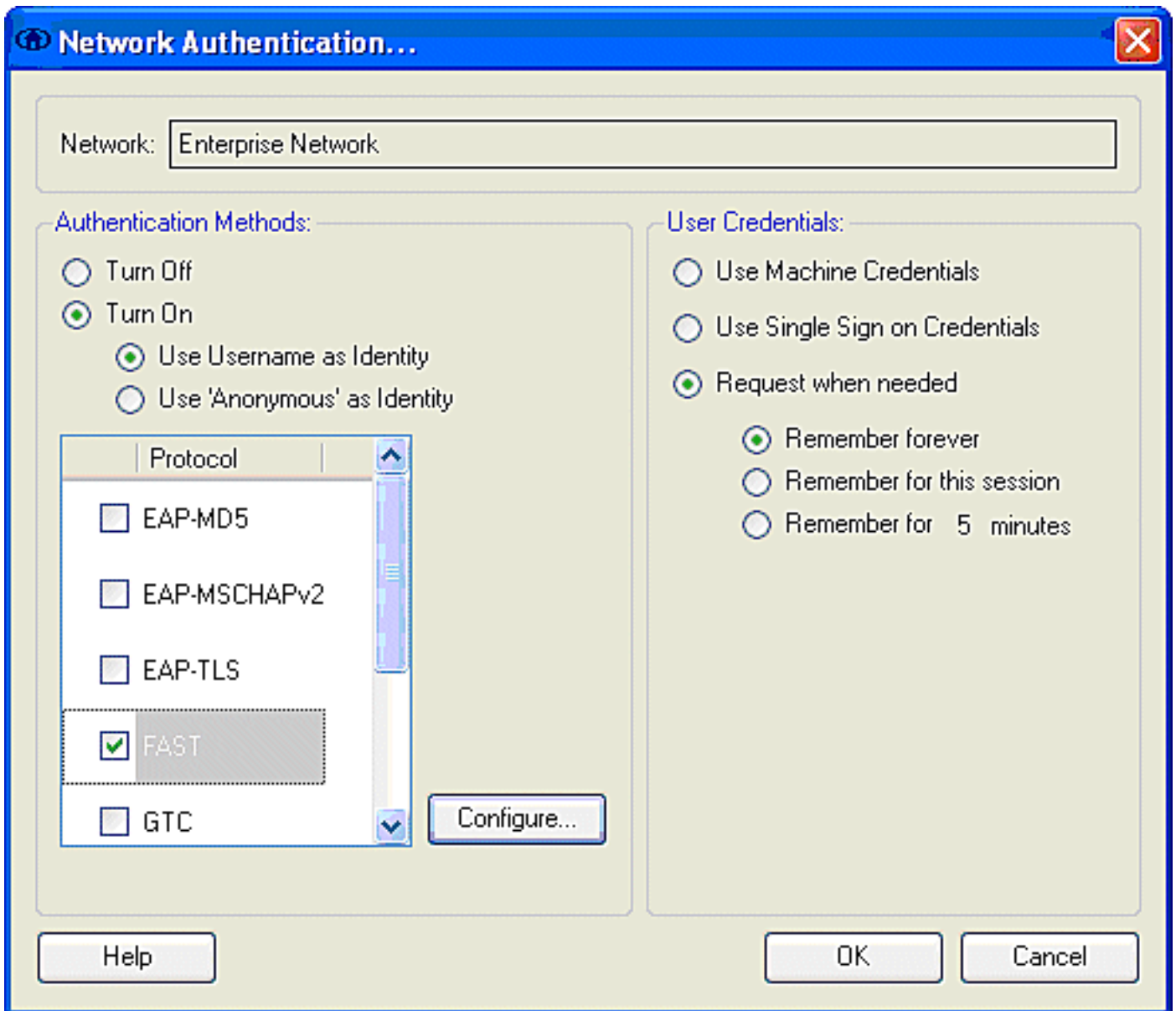
Si se desea para iniciar la conexión de la red inalámbrica (WLAN) antes del inicio del usuario, elija **antes de la cuenta de usuario**. Esto permite Solo-Muestra-en la operación con los credenciales de usuario guardados (contraseña o certificado/tarjeta inteligente cuando usted utiliza TLS dentro del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



Nota: Para la operación WPA/TKIP con el adaptador del cliente del Cisco Aironet de la serie 350, 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 WPA (el cerrar del por-paquete TKIP y control de la Integridad del mensaje), pero inhabilita la clave de autenticación inicial WPA.



Bajo resumen de la configuración de red, el teclado **se modifica** para configurar las configuraciones EAP/de las credenciales. Especifique **giran la** autenticación, eligen **RÁPIDAMENTE** bajo protocolo, y eligen **"anónimo" como identidad** (para no utilizar ningún username en la petición inicial EAP). Es posible utilizar el **username 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. El teclado **configura** para poner 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 a la protección para los dispositivos 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 de la autoridad de certificación de la raíz instalar. En este ejemplo, la validación del certificado de servidor no se activa.

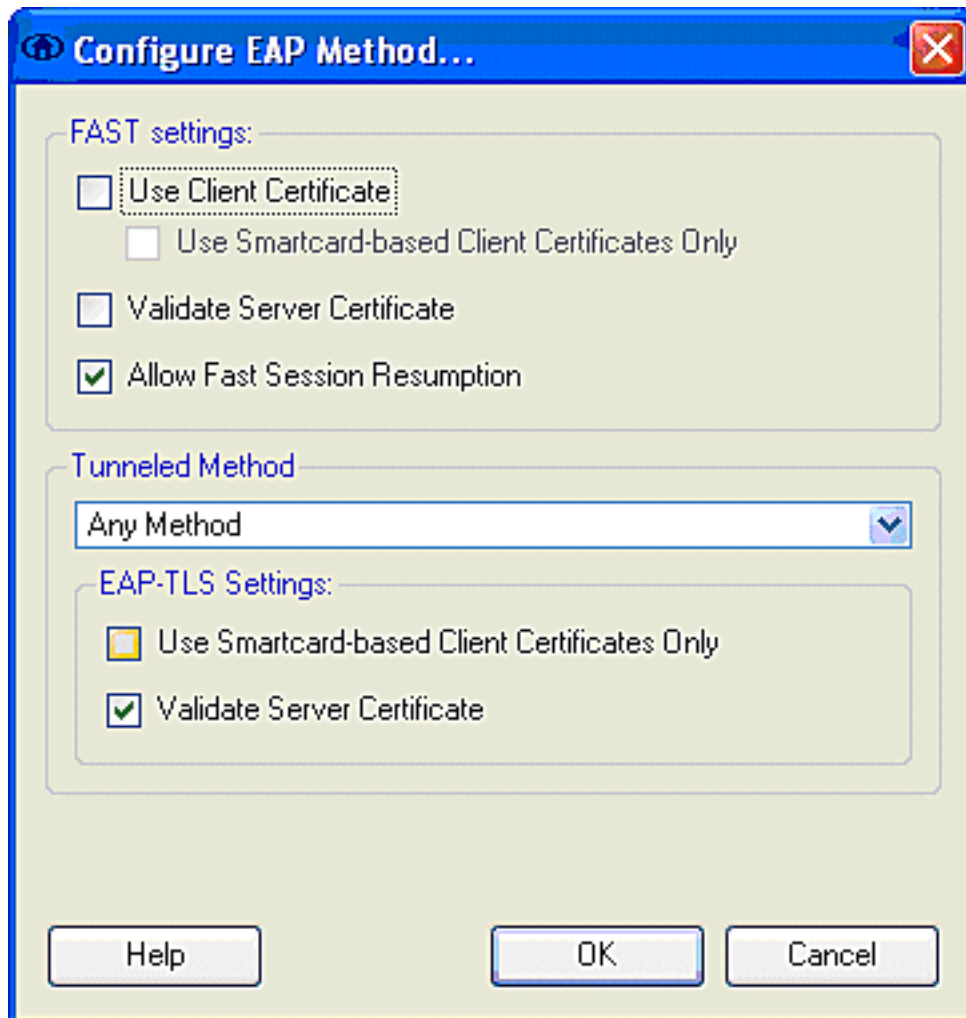
Bajo configuraciones RÁPIDAS, es posible especificar **permite la reanudación rápida de la sesión**, que permite la reanudación de una sesión del EAP-FAST basada sobre la información del túnel (sesión de TLS) bastante que el requisito de un reauthentication completo del EAP-FAST. Si el servidor y el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

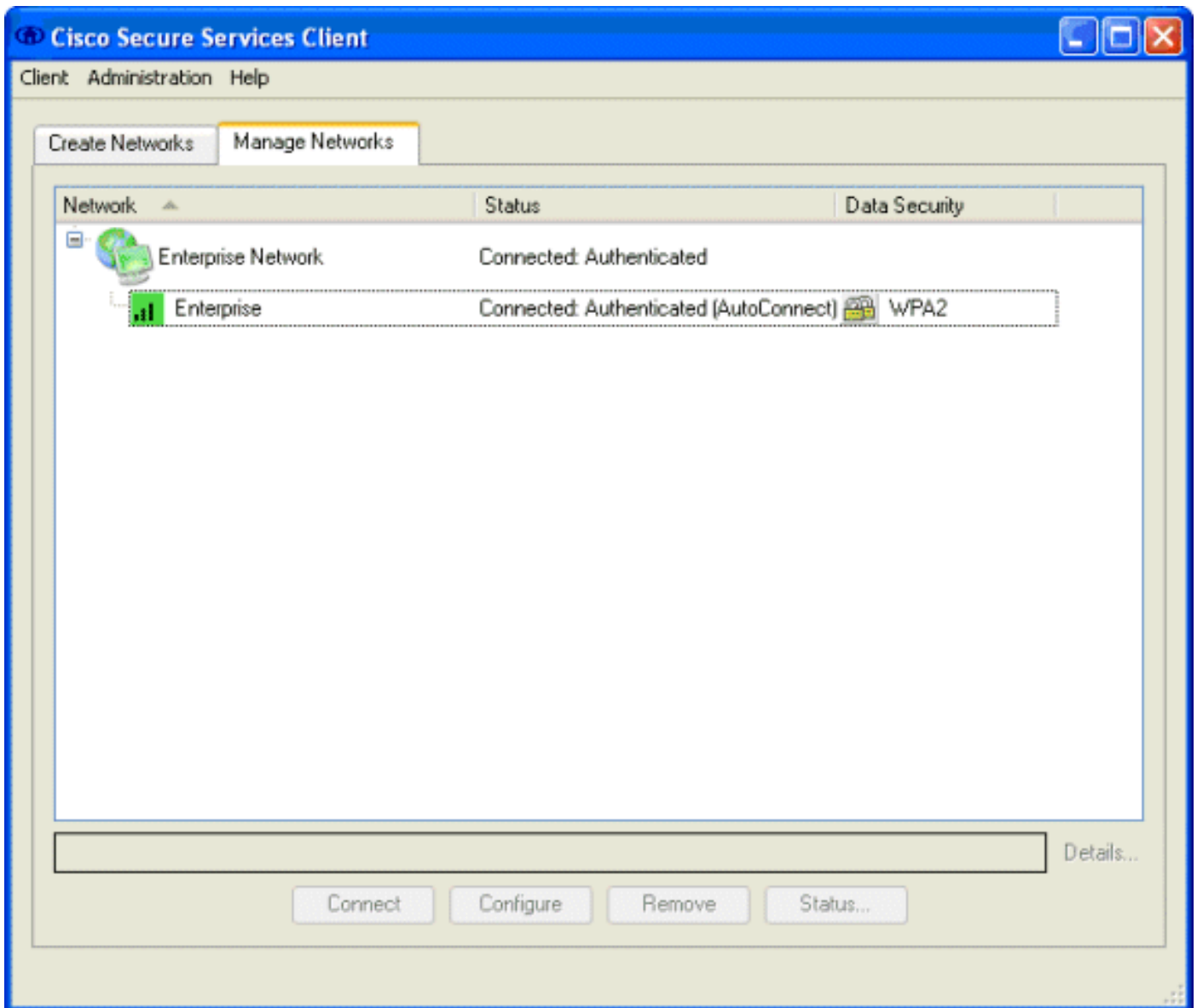
Bajo el método > configuraciones hechos un túnel del EAP-TLS, especifique **cualquier método** para permitir el EAP-MSCHAPv2 para la auto-disposición PAC y el EAP-GTC para la

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

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



AUTORIZACIÓN del teclado 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 tabulación 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 de 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 encriptación 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 tabulación de las redes del manejo y haga clic el **estatus** para preguntar los detalles de la conexión. La ventana de los detalles de la conexión proporciona a la información en el dispositivo cliente, el estado de la conexión y las estadísticas, y el método de autenticación. La tabulación de los detalles de WiFi proporciona a los detalles en el estado de la conexión del 802.11, que incluye el RSSI, el canal del 802.11, y la autenticación/el cifrado.

Connection Status



Connection Details

WiFi Details

Status: Connected: Authenticated

Duration: 00:00:47

Network Profile: Enterprise Network

Network Adapter: Cisco Aironet 802.11 a/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

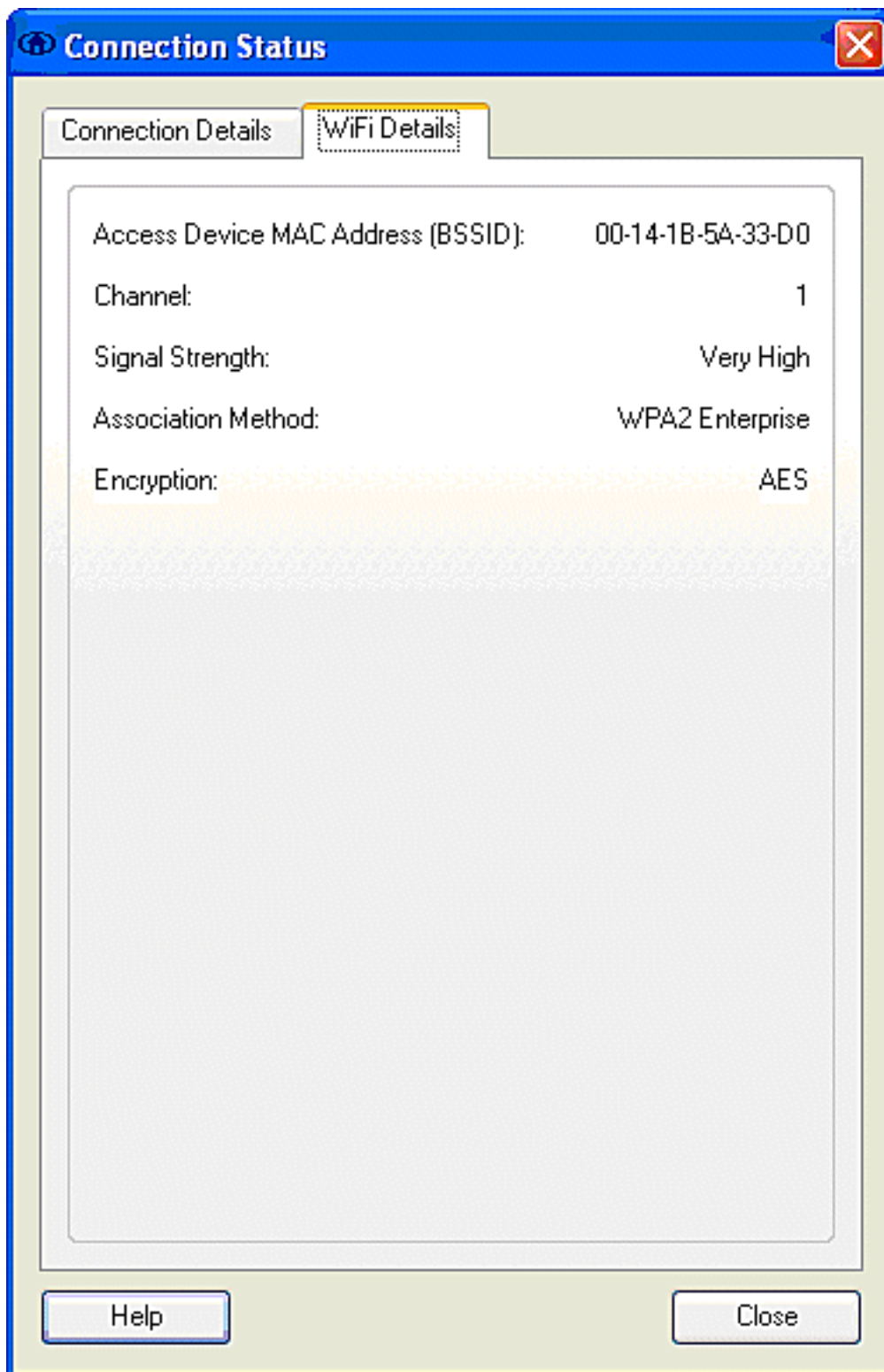
Authentication Method: FAST / GTC

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 desde el principio menú disponible 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 fichero de Microsoft al directorio con el archivo de informe comprimido. Dentro del fichero comprimido, la mayoría de los datos útiles están situados bajo el registro (log_current).

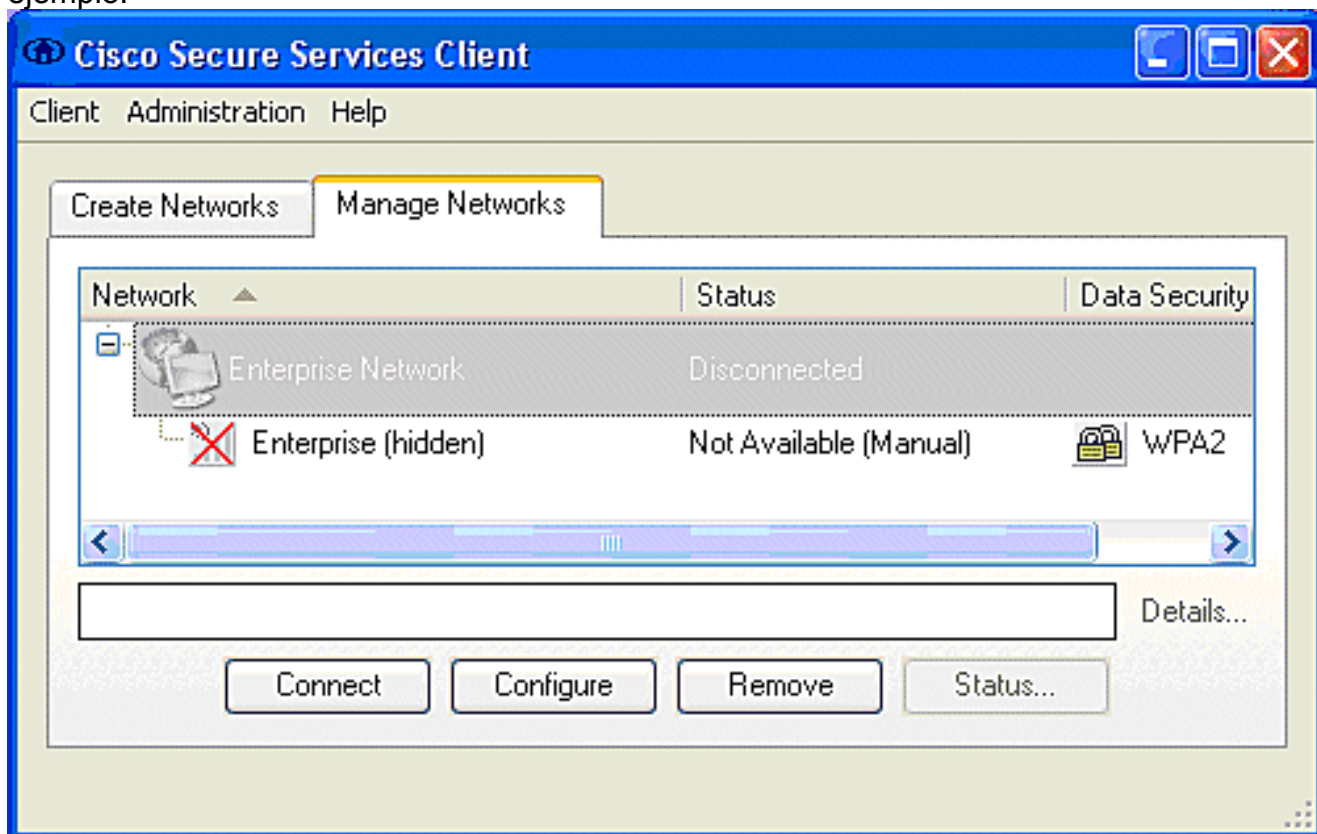
La utilidad da el estado actual de CSSC, interfaz, y los detalles del driver, junto con la información de la red inalámbrica (WLAN) (SSID detectado, estado de asociación, etc.). Esto puede ser útil, diagnosticar especialmente los problemas de la Conectividad entre CSSC y el adaptador de la red inalámbrica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

Verifique la operación

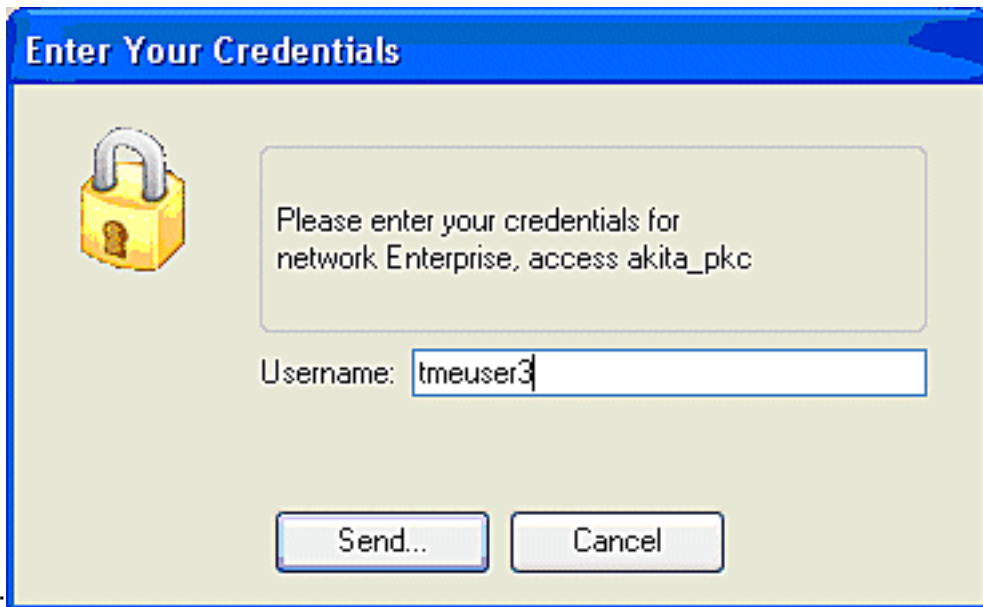
Después de que la configuración de Cisco asegure el servidor ACS, el regulador de la red inalámbrica (WLAN), el cliente CSSC, y la población probablemente correcta de la configuración y de la base de datos, la red de la red inalámbrica (WLAN) se configura para la autenticación del EAP-FAST y la Comunicación del cliente segura. Hay las puntas numerosas que se pueden vigilar para controlar el progreso/los errores para saber si hay una sesión segura.

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

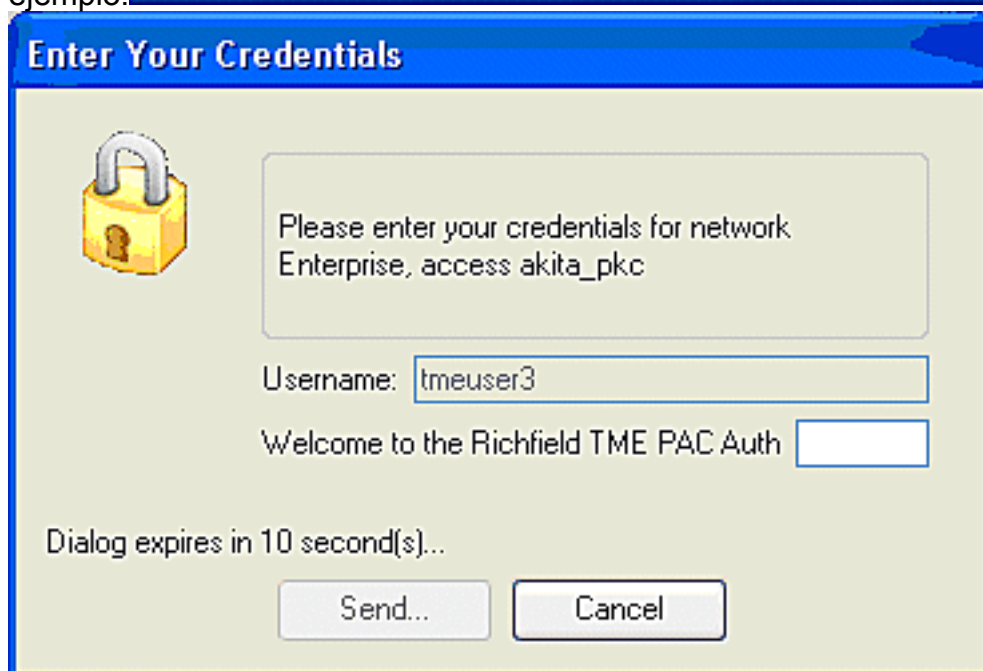
1. Si CSSC se configura para la Auto-conexión, el cliente intenta esta conexión automáticamente. Si no se configura para la Auto-conexión y escoge Muestra-en la operación, el usuario debe iniciar la conexión de la red inalámbrica (WLAN) a través del botón de radio de la **conexión**. Esto inicia el proceso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



2. Incitan al usuario posteriormente proporcionar al username y entonces a la contraseña para la autenticación del EAP-FAST (de la autoridad PAC del EAP-FAST 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 ACS seguro) para validar las credenciales. 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 al 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:

The screenshot shows the Cisco ACS Reports and Activity interface. On the left is a navigation menu with categories like 'Reports' and 'Configuration'. The main area displays a table of authentication reports for 'Passed Authentications active.csv'. The table includes columns for Date, Time, Message-Type, User-Name, Group-Name, CoS-ID, NAS-Port, NAS-IP-Address, Network Access Profile Name, Shared BAC, Downloadable ACL, System Posture-Token, Application Posture-Token, Reason, and EA Type.

Date	Time	Message-Type	User-Name	Group-Name	CoS-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System Posture-Token	Application Posture-Token	Reason	EA Type
08/22/2006	16:25:37	Authen OK	test	Default Group	00-40-96-ab-36-2f	29	10.10.80.3	(Default)	43
08/22/2006	16:09:51	Authen OK	test	Default Group	00-40-96-ab-36-2f	29	10.10.80.3	(Default)	43
08/22/2006	16:06:55	Authen OK	test	Default Group	00-40-96-ab-36-2f	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authen OK	test	Default Group	00-40-96-ab-36-2f	29	10.10.80.3	(Default)	43
08/22/2006	16:06:29	Authen OK	test	Default Group	00-40-96-ab-36-2f	29	10.10.80.3	(Default)	43

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

The screenshot shows the Cisco ACS Wireless Clients page. It features a search bar for MAC address and a table listing clients with columns for Client MAC Addr, AP Name, WLAN, Type, Status, and Auth Port. Each row includes links for 'Detail', 'LinkTest', 'Disable', and 'Remove'.

Client MAC Addr	AP Name	WLAN	Type	Status	Auth Port
88:0f:05:45:04:30	AP0004-0948-0504	Unknown	882.11b	Probing	No 29
88:00:76:a0:36:2f	AP0004-0948-0504	Enterprise	882.11g	Associated	Yes 29
88:00:76:ac:04:89	AP0004-0948-0480	Unknown	882.11b	Probing	No 29
88:00:76:a6:06:0b	AP0004-0948-0480	Enterprise	882.11g	Associated	No 29

Appendix

Además del diagnóstico y de la información de estatus, que está disponible en Cisco regulador ACS y de la red inalámbrica (WLAN) seguros 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 de la red inalámbrica (WLAN) o los intercambios el poner a punto EAP en el regulador de la red inalámbrica (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 Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Req	FC=...R...,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F...,SN=2868,FM= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T...,SN= 3,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T...,SN= 4,FM= 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,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T...,SN= 5,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T...,SN= 5,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T...,SN= 6,FM= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T...,SN= 6,FM= 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,FM= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T...,SN= 7,FM= 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...,SN=2875,FM= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T...,SN= 8,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F...,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F...,SN=2878,FM= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T...,SN= 9,FM= 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,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F...,SN=2879,FM= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T...,SN= 10,FM= 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.

```

Packet: 12
Frame Control Flags: 00000001 [1]
  0... .. Non-strict order
  .0... .. WEP Not Enabled
  ..0... .. No More Data
  ....0... .. Power Management - active mode
  ....0... .. This is not a Re-Transmission
  ....0... .. Last or Unfragmented Frame
  ....0... .. Not an Exit from the Distribution System
  ....1... .. To the Distribution System
Duration: 314 Microseconds [2-3]
BSSID: 00:14:1B:5A:33:D0 [4-9]
Source: 00:14:1B:5A:33:D0 [10-15]
Destination: 00:14:1B:5A:33:D0 [16-21]
Seq. Number: 3 [22-23 Hash 0x7770]
Frag. Number: 0 [22 Hash 0x07]
802.2 Logical Link Control (LLC) Header
  Dest. SRP: 0xAA SNAP [24]
  Source SRP: 0xAA SNAP [25]
  Command: 0x03 Unnumbered Information [26]
  Vendor ID: 0x000000 [27-29]
  Protocol Type: 0x808E 802.1x Authentication [30-31]
802.1x Authentication
  Protocol Version: 1 [32]
  Packet Type: 0 EAP - Packet [33]
  Body Length: 14 [34-35]
Extensible Authentication Protocol
  Code: 2 Response [36]
  Identifier: 1 [37]
  Length: 14 [38-39]
  Type: 1 Identity [40]
  Type-Data: anonymous [41-49]

```

Depuración en el regulador de la red inalámbrica (WLAN)

Estos comandos debug pueden ser empleados en el regulador de la red inalámbrica (WLAN) para vigilar el progreso del intercambio de la autenticación:

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

- permiso de los eventos de la depuración dot1x
- permiso de los estados de la depuración dot1x

Éste es un ejemplo del comienzo de una transacción de la autenticación entre el cliente CSSC y el ACS según lo vigilado en el regulador de la red inalámbrica (WLAN) con las depuraciones:

```
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.
```

Ésta es la terminación satisfactoria del intercambio EAP de la depuración del regulador (con la autenticación WPA2):

```
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.

[Información Relacionada](#)

- [Guía de instalación para Cisco ACS seguro para el Servidor Windows](#)
- [Guía de configuración para Cisco ACS seguro 4.1](#)
- [Restrinja el acceso de la red inalámbrica \(WLAN\) basado en el SSID con el ejemplo seguro de la configuración WLC y de Cisco ACS](#)
- [EAP-TLS bajo red inalámbrica unificada con ACS 4.0 y Windows 2003](#)
- [Asignación VLAN dinámica con el servidor de RADIUS y el ejemplo inalámbrico de la configuración del regulador LAN](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)