

Ejemplo de configuración de acceso Wi-Fi protegido (WPA) en una red inalámbrica unificada de Cisco

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Compatibilidad con WPA y WPA2](#)

[Configuración de la red](#)

[Configuración de los dispositivos para el modo WPA2 Enterprise](#)

[Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo](#)

[Configuración de la WLAN para el modo de funcionamiento empresarial de WPA2](#)

[Configuración del servidor RADIUS para la autenticación de modo empresarial WPA2 \(EAP-FAST\)](#)

[Configuración del cliente inalámbrico para el modo de funcionamiento de WPA2 Enterprise](#)

[Configuración de los dispositivos para el modo WPA2 Personal](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el acceso Wi-Fi protegido (WPA) en una red inalámbrica unificada de Cisco.

Prerequisites

Requirements

Asegúrese de tener conocimientos básicos de estos temas antes de intentar esta configuración:

- WPA
- Soluciones de seguridad para redes LAN inalámbricas (WLAN)**Nota:** Consulte [Descripción general de la seguridad de LAN inalámbrica de Cisco](#) para obtener información sobre las soluciones de seguridad de WLAN de Cisco.

Componentes Utilizados

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

- Punto de acceso ligero (LAP) Cisco serie 1000
- Controlador de LAN inalámbrica (WLC) Cisco 4404 que ejecuta el firmware 4.2.61.0
- Adaptador de cliente Cisco 802.11a/b/g que ejecuta firmware 4.1
- Aironet Desktop Utility (ADU) que ejecuta firmware 4.1
- Servidor Cisco Secure ACS versión 4.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Compatibilidad con WPA y WPA2

Cisco Unified Wireless Network es compatible con las certificaciones Wi-Fi Alliance WPA y WPA2. WPA fue introducido por Wi-Fi Alliance en 2003. WPA2 fue introducido por Wi-Fi Alliance en 2004. Todos los productos con certificación Wi-Fi para WPA2 deben ser interoperables con productos con certificación Wi-Fi para WPA.

WPA y WPA2 ofrecen un alto nivel de garantía a los usuarios finales y los administradores de red de que sus datos seguirán siendo privados y de que el acceso a sus redes estará restringido a los usuarios autorizados. Ambos tienen modos de funcionamiento personal y empresarial que satisfacen las distintas necesidades de los dos segmentos de mercado. El modo empresarial de cada uno utiliza IEEE 802.1X y EAP para la autenticación. El modo personal de cada uno utiliza una clave precompartida (PSK) para la autenticación. Cisco no recomienda el modo personal para implementaciones empresariales o gubernamentales porque utiliza una PSK para la autenticación de usuarios. PSK no es seguro para entornos empresariales.

WPA aborda todas las vulnerabilidades WEP conocidas en la implementación de seguridad IEEE 802.11 original, lo que aporta una solución de seguridad inmediata a las WLAN en entornos empresariales y de pequeña oficina/oficina doméstica (SOHO). WPA utiliza TKIP para la encriptación.

WPA2 es la última generación en seguridad Wi-Fi. Es la implementación interoperable de la Wi-Fi Alliance del estándar IEEE 802.11i ratificado. Implementa el algoritmo de cifrado AES recomendado por el Instituto Nacional de Normas y Tecnología (NIST) mediante el modo de recuento con el protocolo de código de autenticación de mensajes en cadena para el bloqueo de cifrado (CCMP). WPA2 facilita el cumplimiento gubernamental de FIPS 140-2.

Comparación de los tipos de modo WPA y WPA2

	WPA	WPA2
Modo empresarial (empresas, gobierno, educación)	<ul style="list-style-type: none">• Autenticación: IEEE 802.1X/EA	<ul style="list-style-type: none">• Autenticación: IEEE 802.1X/EA

	P • Cifrado: TKIP/MIC	P • Cifrado: AES- CCMP
Modo personal (SOHO, doméstico/personal)	• Autenticación: PSK • Cifrado: TKIP/MIC	• Autenticación: PSK • Cifrado: AES- CCMP

En el modo de funcionamiento empresarial, tanto WPA como WPA2 utilizan 802.1X/EAP para la autenticación. 802.1X proporciona a las WLAN una autenticación sólida y mutua entre un cliente y un servidor de autenticación. Además, 802.1X proporciona claves de cifrado dinámicas por usuario y por sesión, lo que elimina la carga administrativa y los problemas de seguridad relacionados con las claves de cifrado estáticas.

Con 802.1X, las credenciales utilizadas para la autenticación, como las contraseñas de inicio de sesión, nunca se transmiten sin cifrar o sin cifrado a través del medio inalámbrico. Aunque los tipos de autenticación 802.1X proporcionan una autenticación sólida para las LAN inalámbricas, se necesitan TKIP o AES para el cifrado, además de 802.1X, ya que el cifrado WEP 802.11 estándar es vulnerable a los ataques a la red.

Existen varios tipos de autenticación 802.1X, cada uno de los cuales proporciona un enfoque diferente de la autenticación, al tiempo que se basa en el mismo marco y EAP para la comunicación entre un cliente y un punto de acceso. Los productos Cisco Aironet admiten más tipos de autenticación EAP 802.1X que cualquier otro producto WLAN. Entre los tipos admitidos se incluyen:

- [Cisco LEAP](#)
- [EAP-autenticación flexible a través de tunelación segura \(EAP-FAST\)](#)
- EAP-seguridad de la capa de transporte (EAP-TLS)
- [Protocolo de autenticación extensible protegido \(PEAP\)](#)
- EAP-TLS con túnel (EAP-TTLS)
- EAP-módulo de identidad del suscriptor (EAP-SIM)

Otra ventaja de la autenticación 802.1X es la gestión centralizada de los grupos de usuarios de WLAN, incluida la rotación de claves basada en políticas, la asignación de claves dinámicas, la asignación de VLAN dinámica y la restricción de SSID. Estas funciones giran las claves de cifrado.

En el modo de funcionamiento personal, se utiliza una clave previamente compartida (contraseña) para la autenticación. El modo personal sólo requiere un punto de acceso y un dispositivo cliente, mientras que el modo empresarial normalmente requiere un servidor RADIUS u otro servidor de autenticación en la red.

Este documento proporciona ejemplos para configurar WPA2 (modo Enterprise) y WPA2-PSK (modo Personal) en una red Cisco Unified Wireless.

[Configuración de la red](#)

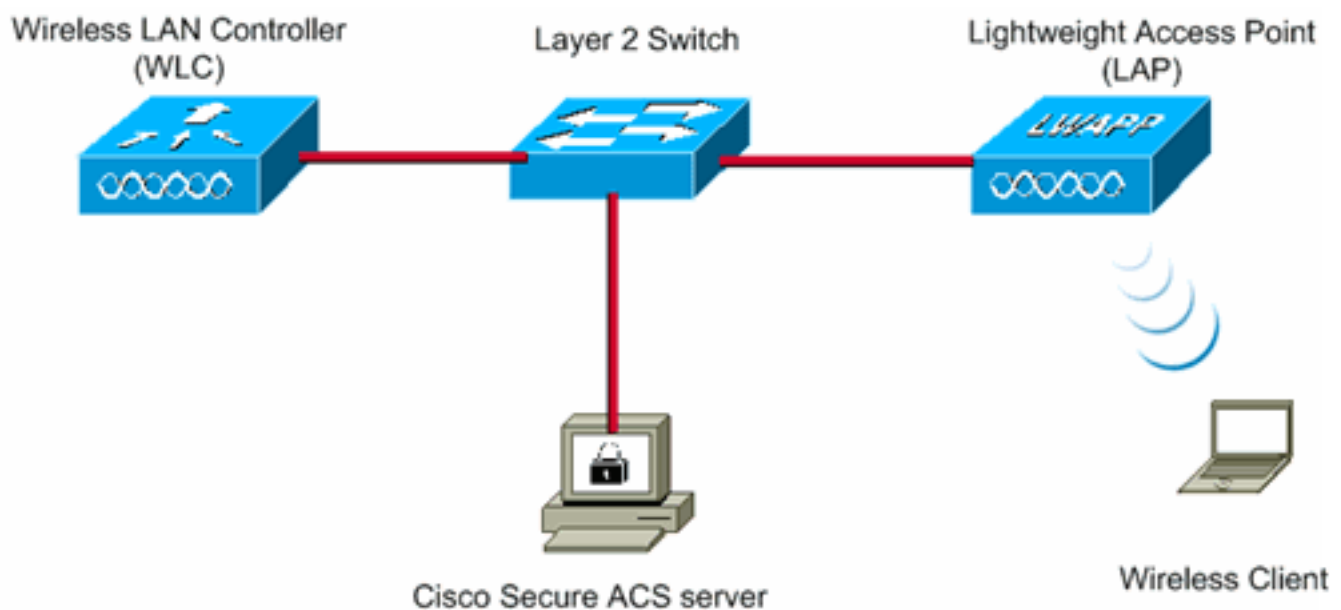
En esta configuración, un Cisco 4404 WLC y un Cisco 1000 Series LAP se conectan a través de

un switch de capa 2. Un servidor RADIUS externo (Cisco Secure ACS) también está conectado al mismo switch. Todos los dispositivos están en la misma subred. El punto de acceso (LAP) se registra inicialmente en el controlador. Es necesario crear dos LAN inalámbricas, una para el modo WPA2 Enterprise y otra para el modo WPA2 Personal.

La WLAN en modo WPA2-Enterprise (SSID: WPA2-Enterprise) utilizará EAP-FAST para autenticar los clientes inalámbricos y AES para el cifrado. El servidor Cisco Secure ACS se utilizará como servidor RADIUS externo para autenticar los clientes inalámbricos.

La WLAN en modo WPA2-Personal (SSID: WPA2-PSK) utilizará WPA2-PSK para la autenticación con la clave previamente compartida "abcdefghijk".

Debe configurar los dispositivos para esta configuración:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

[Configuración de los dispositivos para el modo WPA2 Enterprise](#)

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

Siga estos pasos para configurar los dispositivos para el modo de funcionamiento de WPA2 Enterprise:

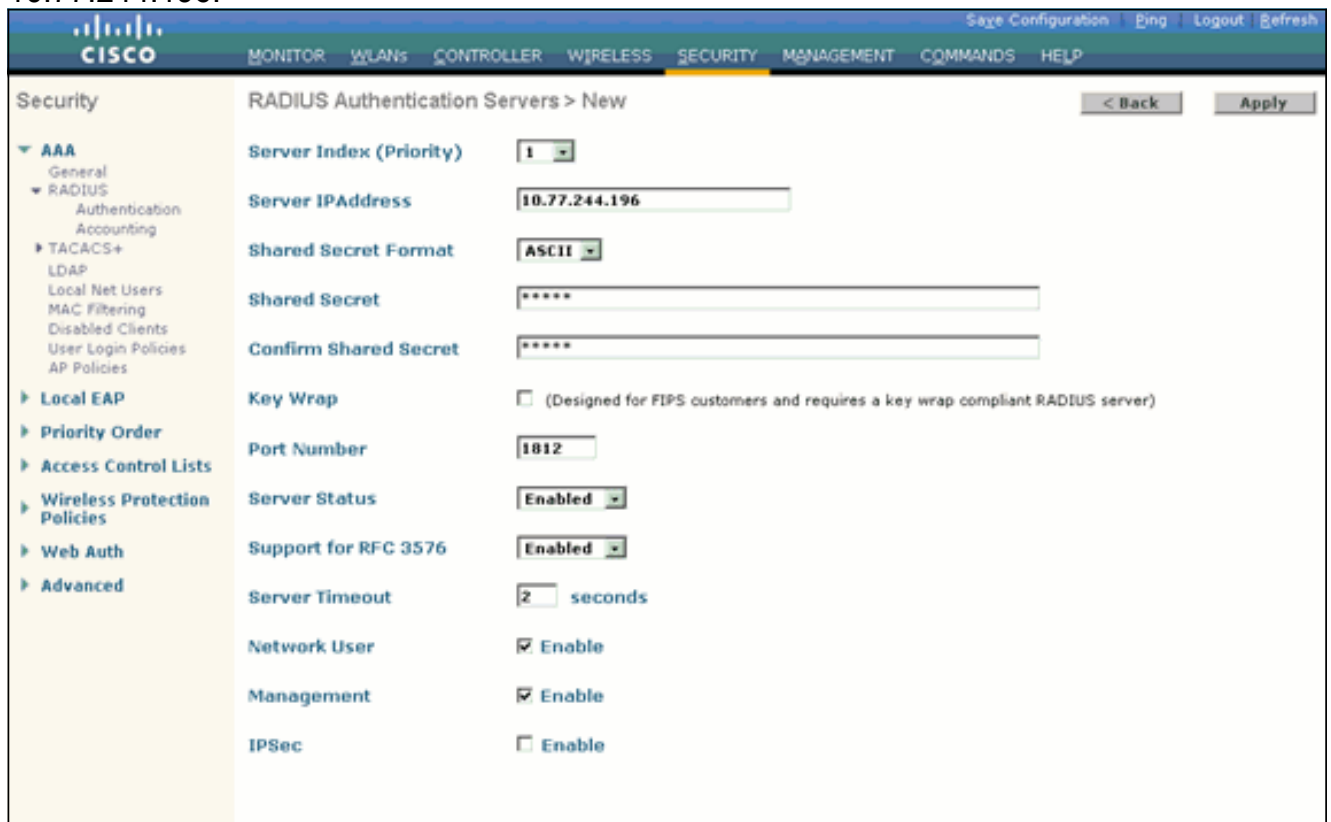
1. [Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo](#)
2. [Configuración de la WLAN para la autenticación de modo empresarial WPA2 \(EAP-FAST\)](#)
3. [Configuración del cliente inalámbrico para el modo WPA2 Enterprise](#)

[Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo](#)

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario mediante EAP-FAST y proporciona acceso a los clientes inalámbricos.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

1. Elija **Seguridad y Autenticación RADIUS** en la GUI del controlador para mostrar la página Servidores de Autenticación RADIUS. Luego, haga clic en **Nuevo** para definir un servidor RADIUS.
2. Defina los parámetros del servidor RADIUS en la página **RADIUS Authentication Servers > New**. Estos parámetros incluyen: Dirección IP de servidor RADIUS, secreto compartido, número de puerto, Estado del servidor. Este documento utiliza el servidor ACS con una dirección IP de 10.77.244.196.



The screenshot shows the Cisco WLC GUI with the 'SECURITY' tab selected. The left sidebar shows a tree view with 'RADIUS' expanded under 'AAA'. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Server Index (Priority)	1
Server IP Address	10.77.244.196
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

3. Haga clic en **Apply** (Aplicar).

[Configuración de la WLAN para el modo de funcionamiento empresarial de WPA2](#)

A continuación, configure la WLAN que utilizarán los clientes para conectarse a la red inalámbrica. El SSID de WLAN para el modo empresarial WPA2 será WPA2-Enterprise. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN y sus parámetros relacionados:

1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs. Esta página enumera las WLANs que existen en el controlador.
2. Haga clic en **Nuevo** para crear un nuevo WLAN.

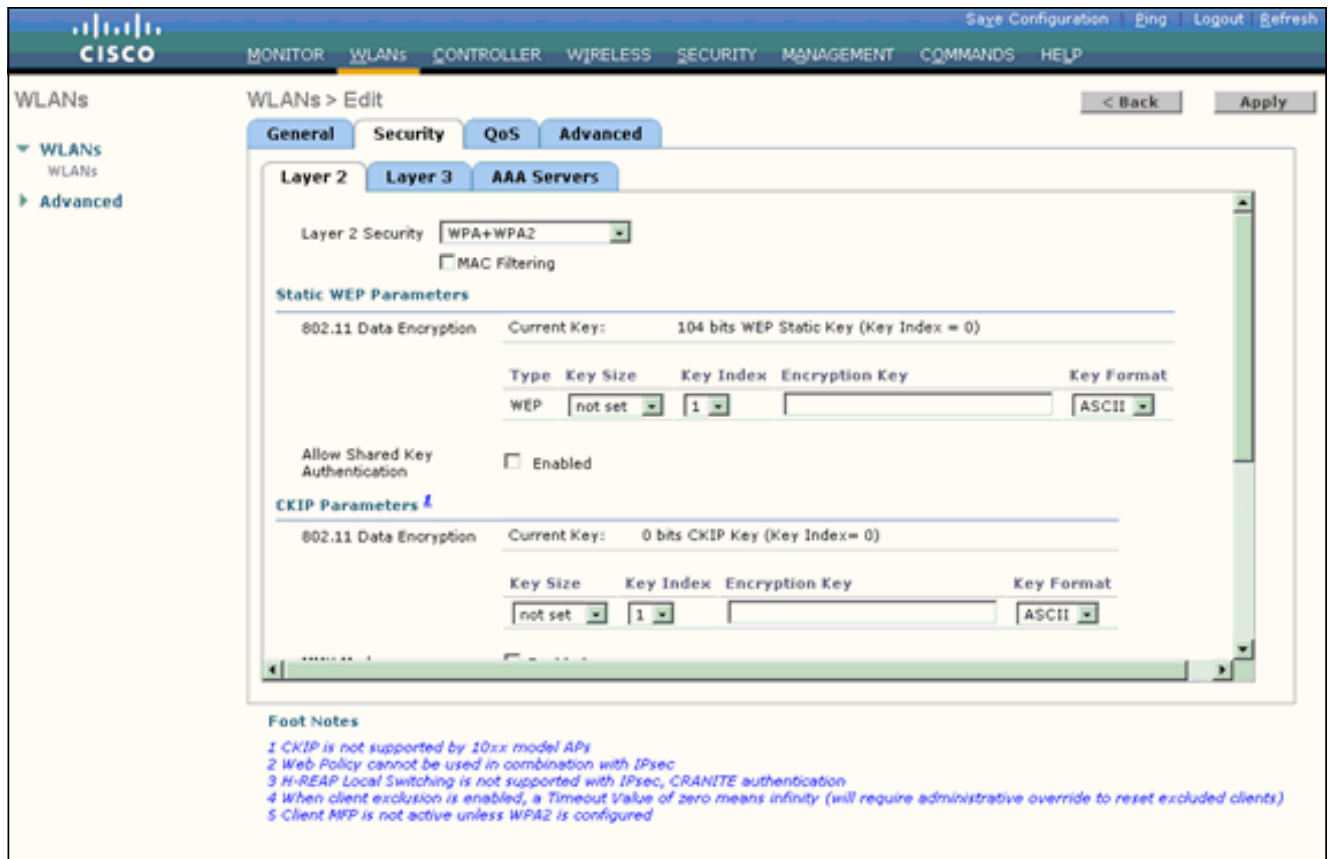
- Introduzca el nombre SSID de WLAN y el nombre Profile en la página **WLANs > New**. A continuación, haga clic en **Aplicar**. Este ejemplo utiliza **WPA2-Enterprise** como SSID.

The screenshot shows the Cisco configuration interface for creating a new WLAN. The page title is 'WLANs > New'. On the left, there is a navigation menu with 'WLANs' and 'Advanced' options. The main content area contains three input fields: 'Type' is a dropdown menu set to 'WLAN'; 'Profile Name' is a text box containing 'WPA2-Enterprise'; and 'WLAN SSID' is a text box also containing 'WPA2-Enterprise'. At the top right, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. At the bottom right, there are buttons for '< Back' and 'Apply'.

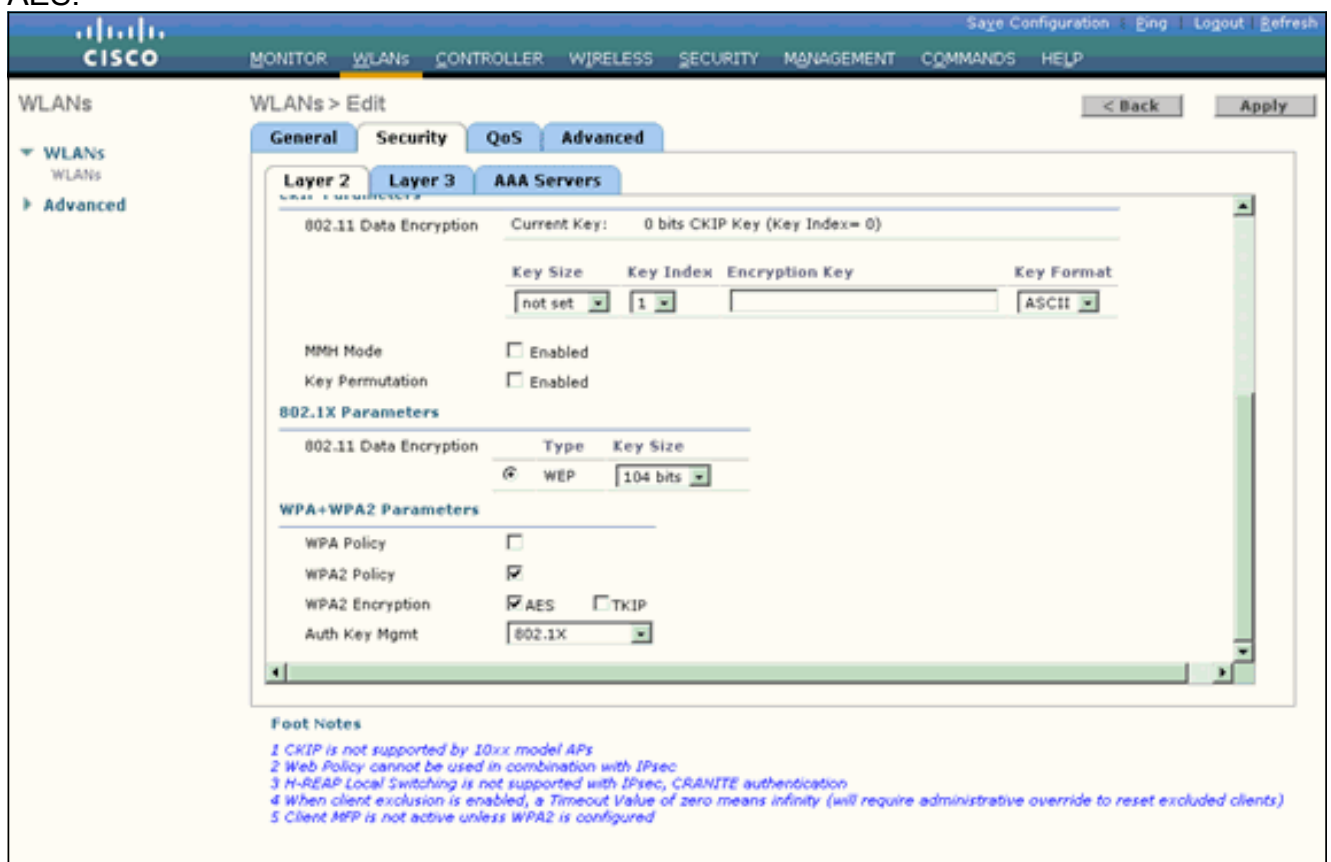
- Una vez que haya creado una nueva WLAN, aparecerá la página **WLAN > Edit** para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, políticas de seguridad, políticas de QoS y parámetros avanzados.
- En Políticas generales, marque la casilla de verificación **Status** para habilitar la WLAN.

The screenshot shows the Cisco configuration interface for editing an existing WLAN. The page title is 'WLANs > Edit'. On the left, there is a navigation menu with 'WLANs' and 'Advanced' options. The main content area has four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is active, showing the following fields: 'Profile Name' (WPA2-Enterprise), 'Type' (WLAN), 'SSID' (WPA2-Enterprise), 'Status' (checkbox checked, 'Enabled'), 'Security Policies' ([WPA2][Auth(802.1X)]), 'Radio Policy' (dropdown set to 'All'), 'Interface' (dropdown set to 'management'), and 'Broadcast SSID' (checkbox checked, 'Enabled'). At the bottom, there is a 'Foot Notes' section with five numbered notes. At the top right, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'. At the bottom right, there are buttons for '< Back' and 'Apply'.

- Si desea que el AP difunda el SSID en sus tramas de baliza, marque la casilla de verificación **Broadcast SSID**.
- Haga clic en la ficha Security (Seguridad). En Layer 2 Security, elija **WPA+WPA2**. Esto activa la autenticación WPA para la WLAN.



8. Desplácese hacia abajo por la página para modificar los parámetros **WPA+WPA2**. En este ejemplo, se seleccionan la política WPA2 y el cifrado AES.



9. En Administración de claves de autenticación, elija **802.1x**. Esto habilita WPA2 usando autenticación 802.1x/EAP y cifrado AES para la WLAN.

10. Haga clic en la pestaña **AAA Servers**. En Servidores de autenticación, elija la dirección IP del servidor correspondiente. En este ejemplo, 10.77.244.196 se utiliza como servidor

RADIUS.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers		LDAP Servers	
Authentication Servers	Accounting Servers	Server 1	Server 2
Server 1: IP:10.77.244.196, Port:1812	None	None	None
Server 2: None	None	None	None
Server 3: None	None	None	None

Local EAP Authentication

Local EAP Authentication Enabled

Foot Notes

1 CRIP is not supported by 10xx model APs
2 Web Policy cannot be used in combination with IPsec
3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

11. Haga clic en Apply (Aplicar). **Nota:** Éste es el único parámetro EAP que debe configurarse en el controlador para la autenticación EAP. Todas las demás configuraciones específicas de EAP-FAST deben realizarse en el servidor RADIUS y en los clientes que deben autenticarse.

[Configuración del servidor RADIUS para la autenticación de modo empresarial WPA2 \(EAP-FAST\)](#)

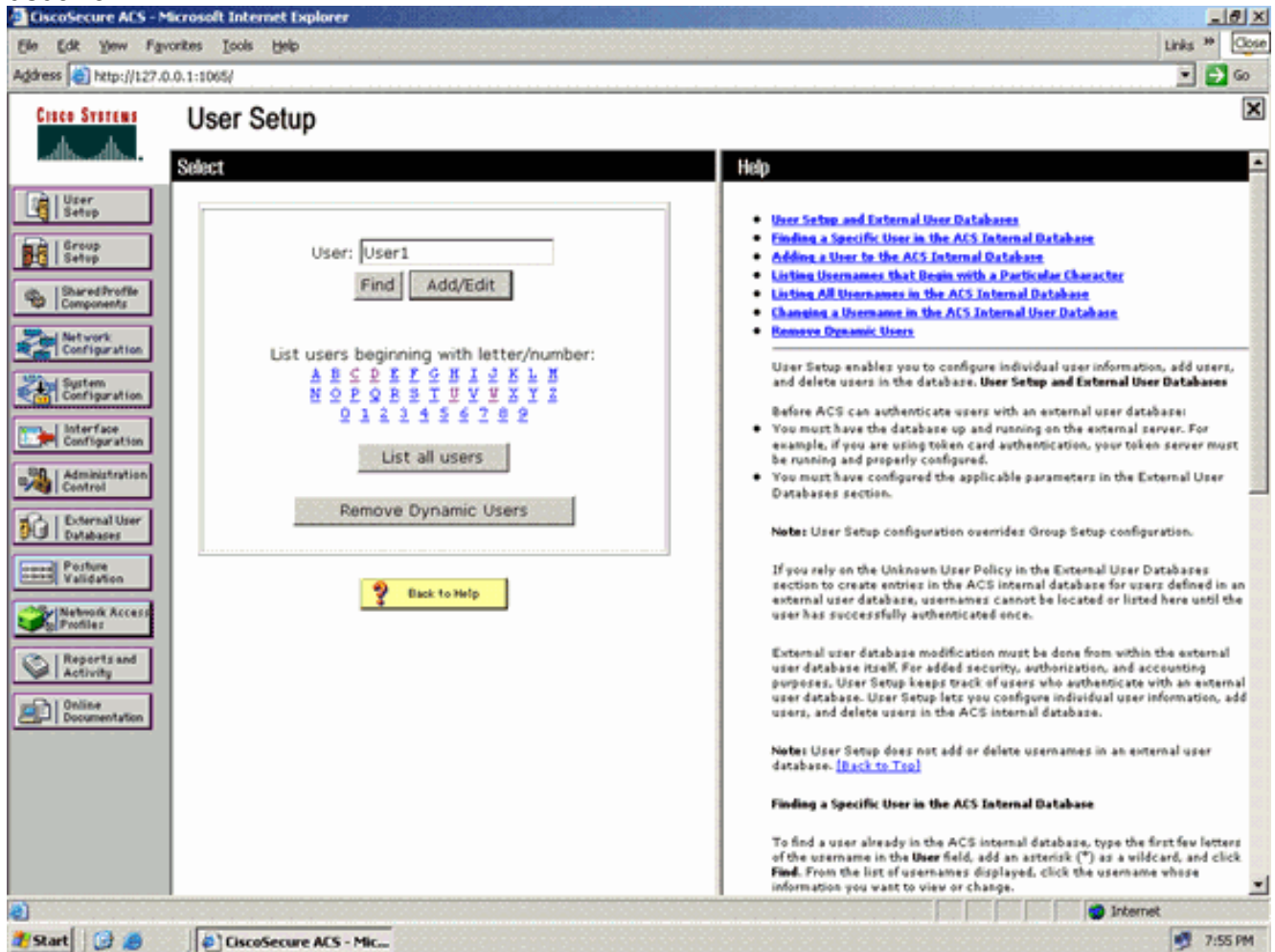
En este ejemplo, Cisco Secure ACS se utiliza como servidor RADIUS externo. Realice estos pasos para configurar el servidor RADIUS para la autenticación EAP-FAST:

1. [Crear una base de datos de usuarios para autenticar clientes](#)
2. [Agregue el WLC como cliente AAA al servidor RADIUS](#)
3. [Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con el Aprovisionamiento de PAC en banda anónimo](#) **Nota:** EAP-FAST se puede configurar con aprovisionamiento de PAC en banda anónimo o con aprovisionamiento de PAC en banda autenticado. En este ejemplo se utiliza el aprovisionamiento de PAC en banda anónimo. Para obtener información detallada y ejemplos sobre la configuración de EAP FAST con aprovisionamiento de PAC en banda anónimo y aprovisionamiento en banda autenticado, consulte [Ejemplo de Configuración de Autenticación EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo](#).

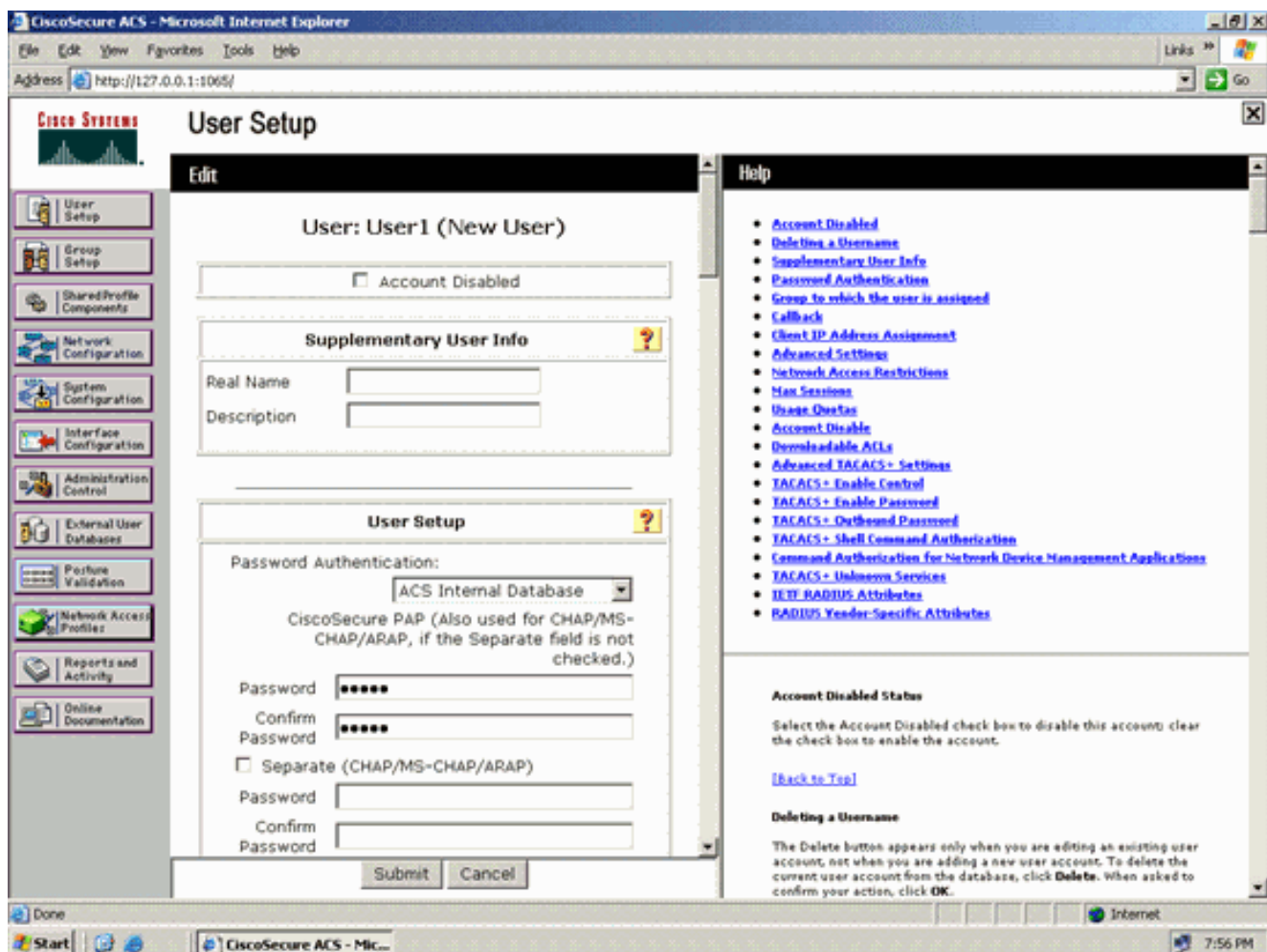
[Creación de una Base de Datos de Usuario para Autenticar Clientes EAP-FAST](#)

Complete estos pasos para crear una base de datos de usuario para los clientes EAP-FAST en ACS. Este ejemplo configura el nombre de usuario y la contraseña del cliente EAP-FAST como Usuario1 y Usuario1, respectivamente.

1. En ACS GUI en la barra de navegación, seleccione **User Setup**. Cree un nuevo usuario inalámbrico, y luego haga clic en **Add/Edit** para ir a la página Edit de este usuario.



2. En la página User Setup Edit (Edición de la configuración de usuario), configure Real Name (Nombre real) y Description (Descripción), así como los parámetros de Password (Contraseña), como se muestra en este ejemplo. Este documento utiliza **ACS Internal Database** para la autenticación de contraseña.

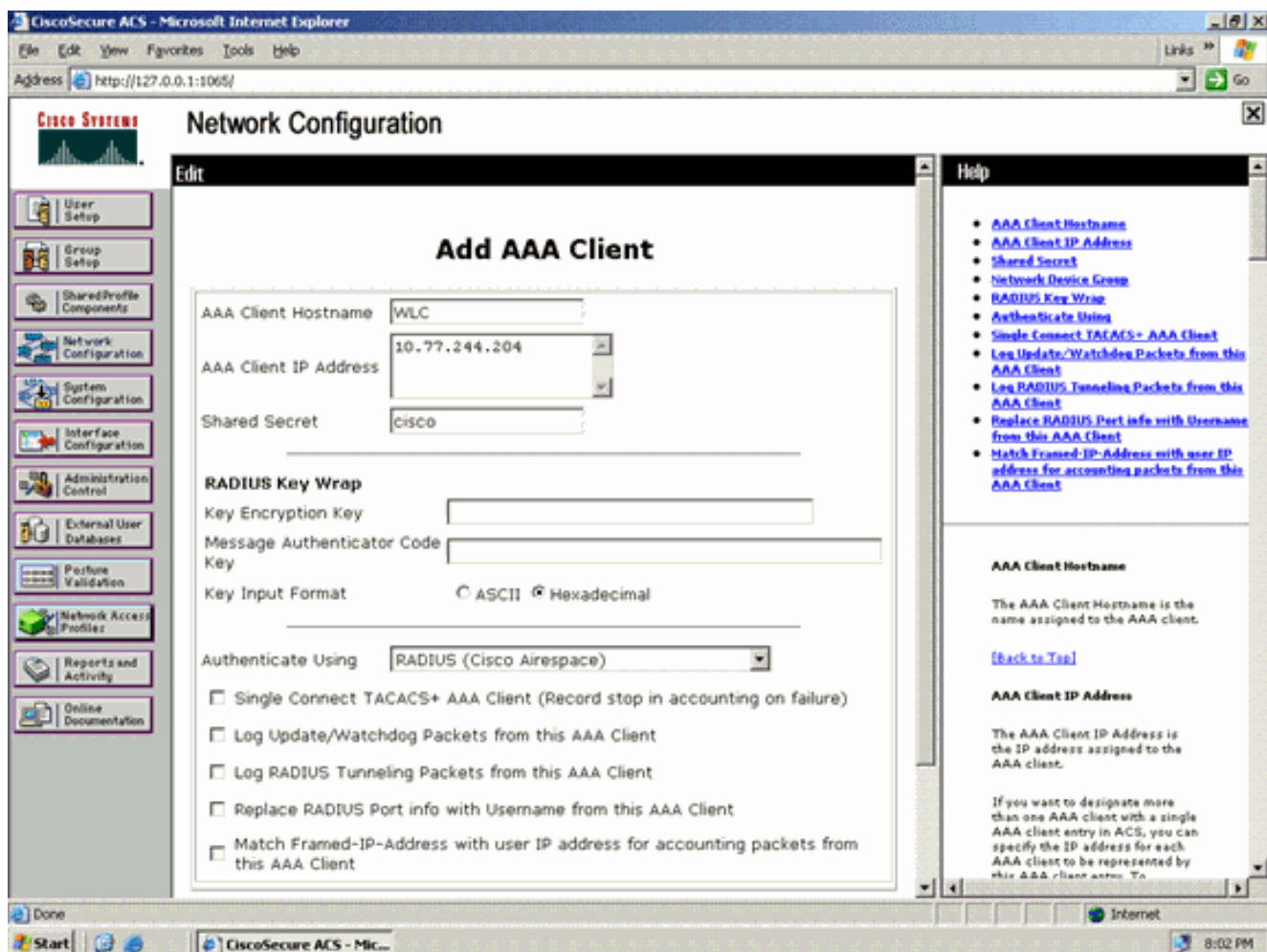


3. Elija **ACS Internal Database** del cuadro desplegable Password Authentication.
4. Configure todos los demás parámetros requeridos y haga clic en **Submit**.

[Agregue el WLC como cliente AAA al servidor RADIUS](#)

Complete estos pasos para definir el controlador como un cliente AAA en el servidor ACS:

1. Haga clic en **Network Configuration** desde la GUI de ACS. Bajo la sección Add AAA client de la página Network Configuration, haga clic en **Add Entry** para agregar el WLC como cliente AAA al servidor RADIUS.
2. En la página AAA Client (Cliente AAA), defina el nombre del WLC, la dirección IP, el secreto compartido y el método de autenticación (RADIUS/Cisco Airespace). Consulte la documentación del fabricante para otros servidores de autenticación no ACS.



Nota: La clave secreta compartida que configure en el WLC y el servidor ACS deben coincidir. El secreto compartido distingue entre mayúsculas y minúsculas.

3. Haga clic en **Enviar+Aplicar**.

[Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con el Aprovisionamiento de PAC en banda anónimo](#)

Aprovisionamiento anónimo en banda

Este es uno de los dos métodos de aprovisionamiento en banda en los que el ACS establece una conexión segura con el cliente de usuario final con el fin de proporcionar al cliente una nueva PAC. Esta opción permite un intercambio de señales TLS anónimo entre el cliente de usuario final y ACS.

Este método funciona dentro de un túnel de protocolo de acuerdo de clave Diffie-Hellman (ADHP) autenticado antes de que el par autentique el servidor ACS.

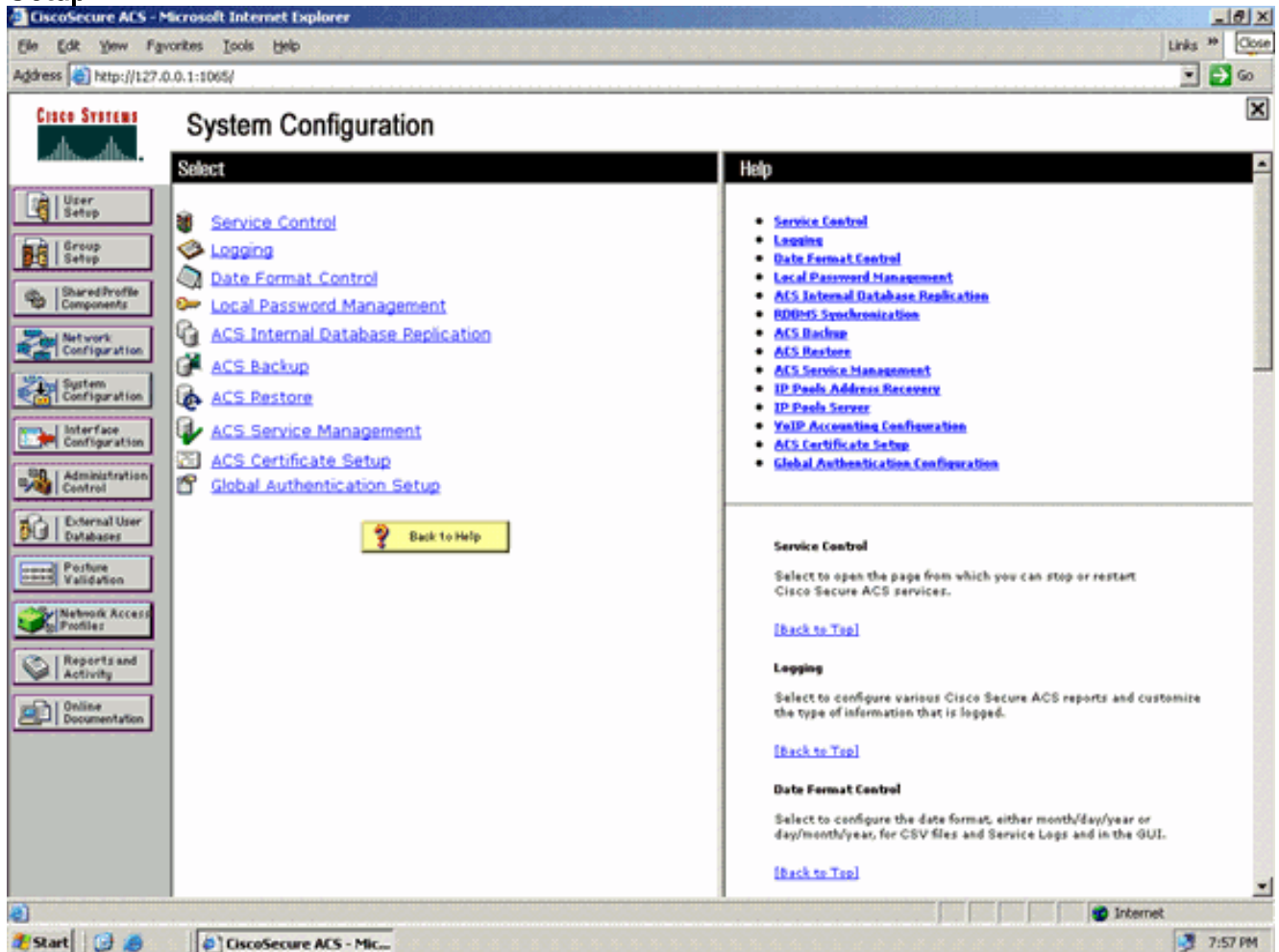
Entonces, el ACS requiere la autenticación EAP-MS-CHAPv2 del usuario. Cuando la autenticación de usuario es exitosa, el ACS establece un túnel Diffie-Hellman con el cliente de usuario final. El ACS genera una PAC para el usuario y la envía al cliente de usuario final en este túnel, junto con información sobre este ACS. Este método de aprovisionamiento utiliza EAP-MSCHAPv2 como método de autenticación en la fase cero y EAP-GTC en la fase dos.

Dado que se ha aprovisionado un servidor no autenticado, no es posible utilizar una contraseña de texto sin formato. Por lo tanto, sólo se pueden utilizar las credenciales MS-CHAP dentro del túnel. MS-CHAPv2 se utiliza para probar la identidad del par y recibir una PAC para sesiones de

autenticación adicionales (EAP-MS-CHAP se utilizará sólo como método interno).

Complete estos pasos para configurar la autenticación EAP-FAST en el servidor RADIUS para el aprovisionamiento anónimo en banda:

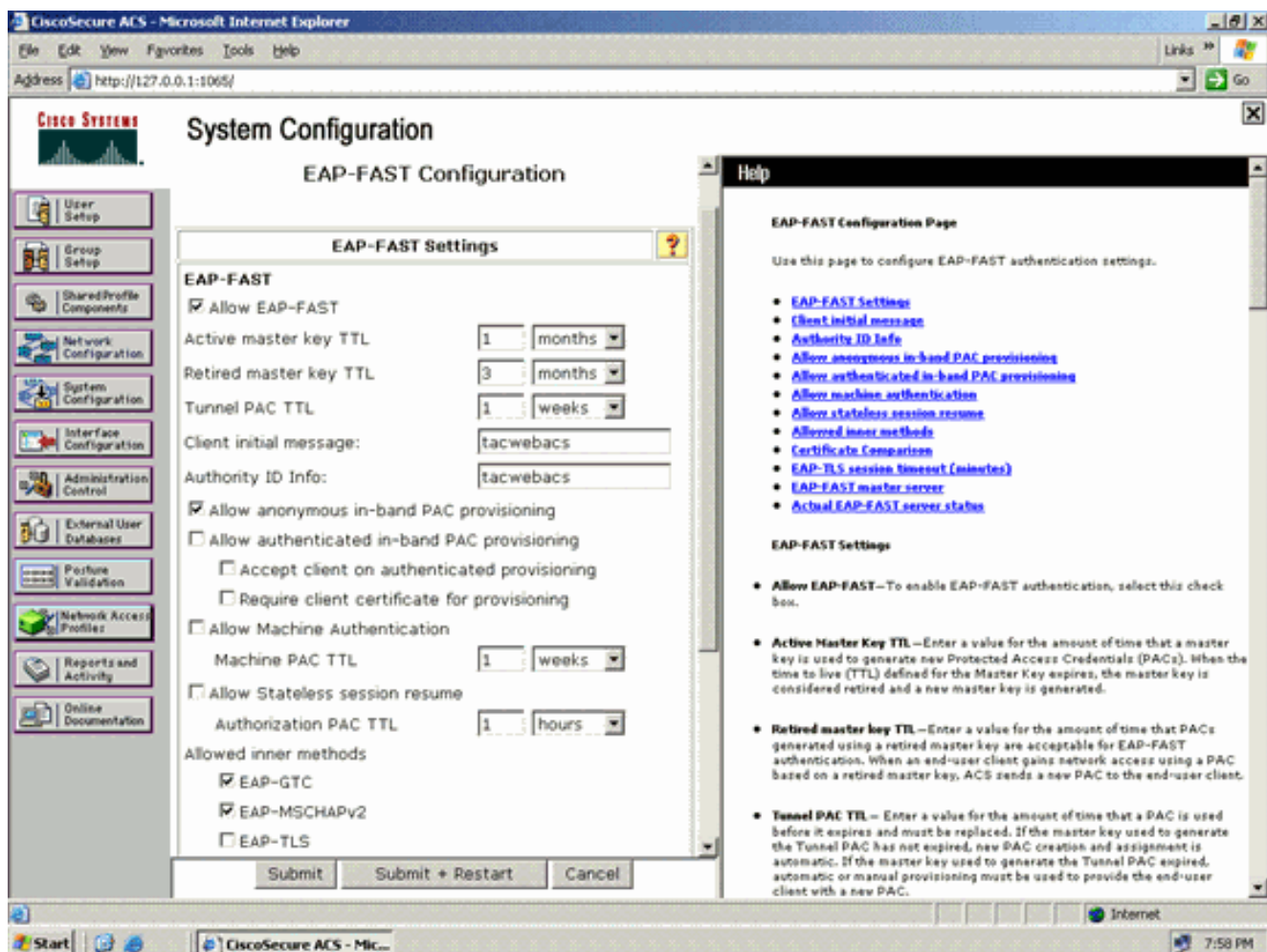
1. Haga clic en **System Configuration** de la GUI del servidor RADIUS. En la página System Configuration , elija **Global Authentication Setup**.



2. Desde la página de configuración de Autenticación Global, haga clic en **Configuración EAP-FAST** para ir a la página de configuración de EAP-FAST.

The screenshot shows the CiscoSecure ACS System Configuration page in Microsoft Internet Explorer. The browser address bar shows <http://127.0.0.1:1005/>. The page title is "System Configuration". On the left, there is a navigation menu with options like "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", and "Online Documentation". The main content area is titled "EAP Configuration" and contains sections for PEAP, EAP-FAST, and EAP-TLS. The PEAP section has checkboxes for "Allow EAP-MSCHAPv2", "Allow EAP-GTC", and "Allow Posture Validation", all of which are currently unchecked. Below these are options for "Allow EAP-TLS" and "Certificate SAN comparison", "Certificate CN comparison", and "Certificate Binary comparison", all of which are checked. The "EAP-TLS session timeout (minutes)" is set to 120. The "Cisco client initial message" field is empty. The "PEAP session timeout (minutes)" is set to 120, and "Enable Fast Reconnect" is checked. The EAP-FAST section has a link for "EAP-FAST Configuration". The EAP-TLS section has a checkbox for "Allow EAP-TLS" which is unchecked, and a checked checkbox for "Certificate SAN comparison". At the bottom of the configuration area are "Submit", "Submit + Restart", and "Cancel" buttons. On the right, there is a "Help" panel with a list of links including "EAP Configuration", "PEAP", "EAP-FAST", "EAP-TLS", "LEAP", "EAP-MD5", "AP EAP Request Timeout", and "MS-CHAP Configuration". Below the links, there is a section titled "EAP Configuration" with a description of EAP as a flexible request-response protocol. Below that is a section titled "PEAP" with a description of PEAP as the outer layer protocol for the secure tunnel. At the bottom of the help panel, there is a note: "Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page." and a bullet point: "• Allow EAP-MSCHAPv2 - Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database."

3. En la página EAP-FAST Settings (Parámetros de EAP-FAST), marque la casilla de verificación **Allow EAP-FAST** para activar EAP-FAST en el servidor RADIUS.



- Configure los valores TTL (Time-to-Live) de clave maestra activa/retirada como desee o establézcalos en el valor predeterminado, como se muestra en este ejemplo. Consulte Claves Maestras para obtener información sobre las claves Maestras Activas y Retiradas. Consulte también las claves maestras y los TTL PAC para obtener más información. El campo Información de ID de autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar con qué servidor ACS se autenticará. Rellenar este campo es obligatorio. El campo Mensaje de visualización inicial del cliente especifica un mensaje que se enviará a los usuarios que se autentiquen con un cliente EAP-FAST. La longitud máxima es de 40 caracteres. Un usuario sólo verá el mensaje inicial si el cliente de usuario final admite la visualización.
- Si desea que ACS realice el aprovisionamiento de PAC en banda anónimo, marque la casilla de verificación **Permitir el aprovisionamiento de PAC en banda anónimo**.
- Métodos internos permitidos:** esta opción determina qué métodos EAP internos se pueden ejecutar dentro del túnel EAP-FAST TLS. Para el aprovisionamiento en banda anónimo, debe habilitar EAP-GTC y EAP-MS-CHAP para la compatibilidad con versiones anteriores. Si selecciona Permitir el aprovisionamiento de PAC en banda anónimo, debe seleccionar EAP-MS-CHAP (fase cero) y EAP-GTC (fase dos).

[Configuración del cliente inalámbrico para el modo de funcionamiento de WPA2 Enterprise](#)

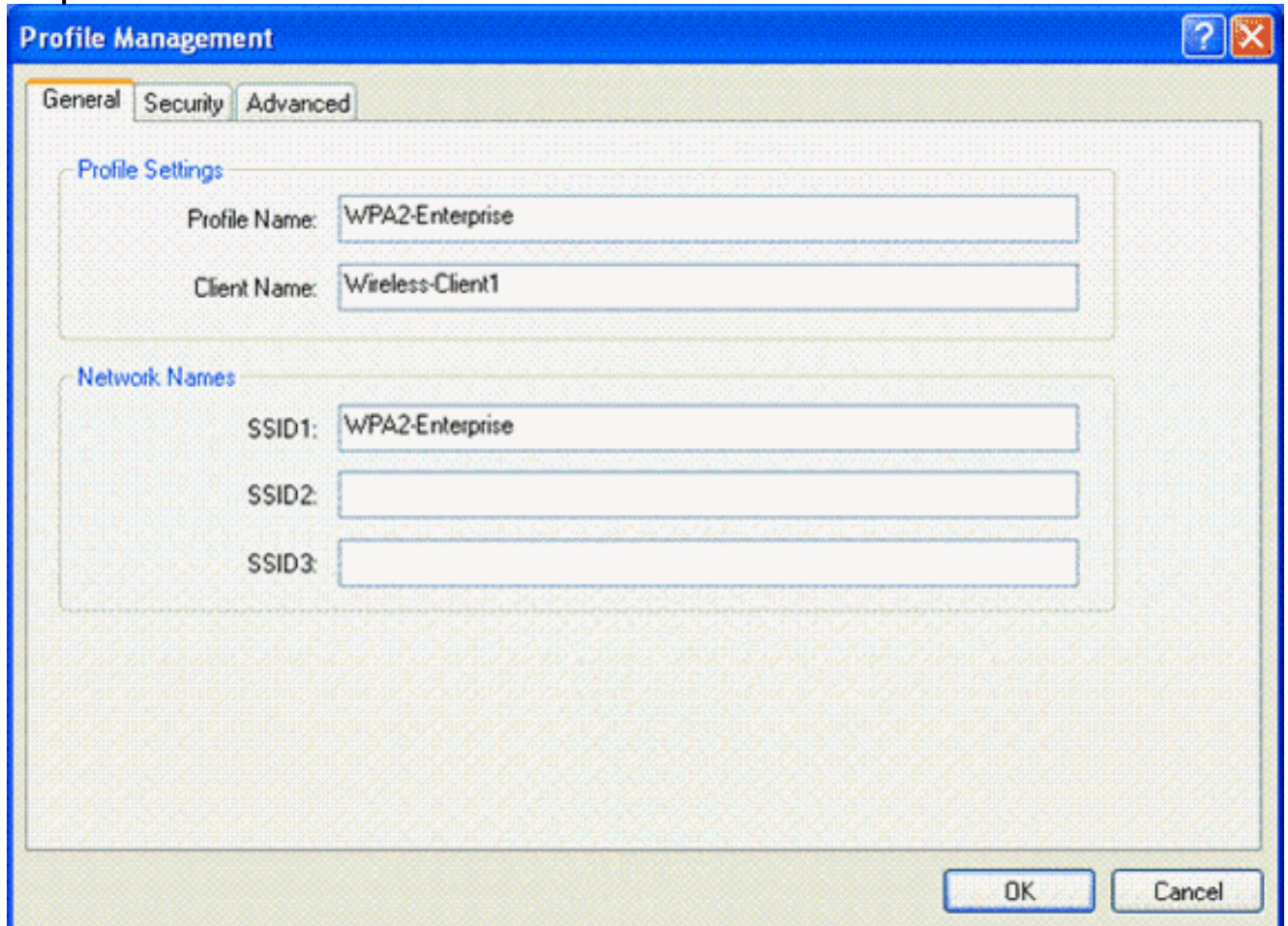
El siguiente paso consiste en configurar el cliente inalámbrico para el modo de funcionamiento WPA2 Enterprise.

Complete estos pasos para configurar el cliente inalámbrico para el modo WPA2 Enterprise.

1. Desde la ventana Aironet Desktop Utility, haga clic en **Profile Management > New** para crear un perfil para el usuario WLAN WPA2-Enterprise. Como se mencionó anteriormente, este documento utiliza el nombre WLAN/SSID como **WPA2-Enterprise** para el cliente inalámbrico.
2. Desde la ventana Profile Management, haga clic en la pestaña **General** y configure el nombre del perfil, el nombre del cliente y el nombre SSID como se muestra en este ejemplo.

A continuación, haga clic en

Aceptar

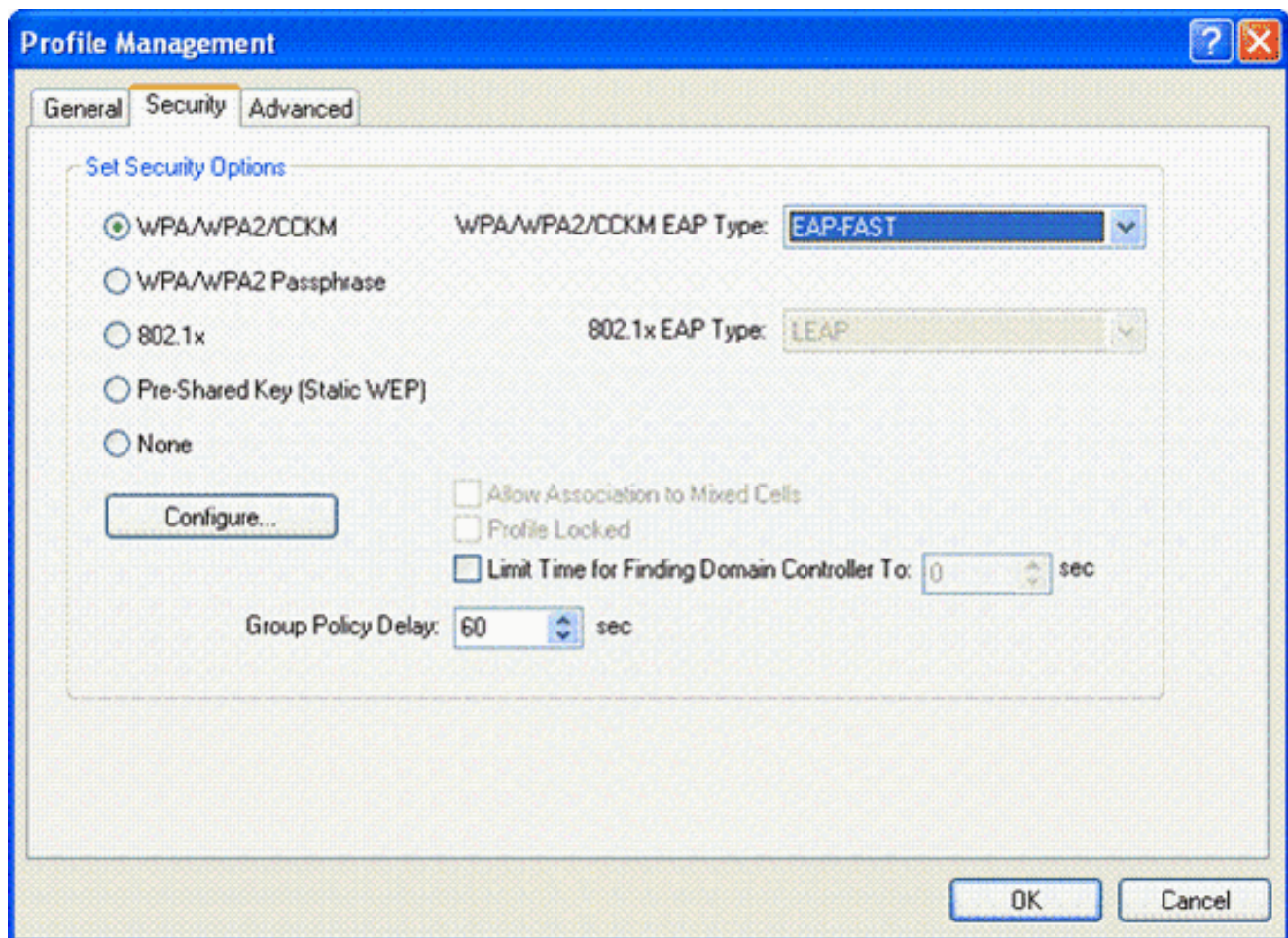


The screenshot shows the 'Profile Management' dialog box with the following fields:

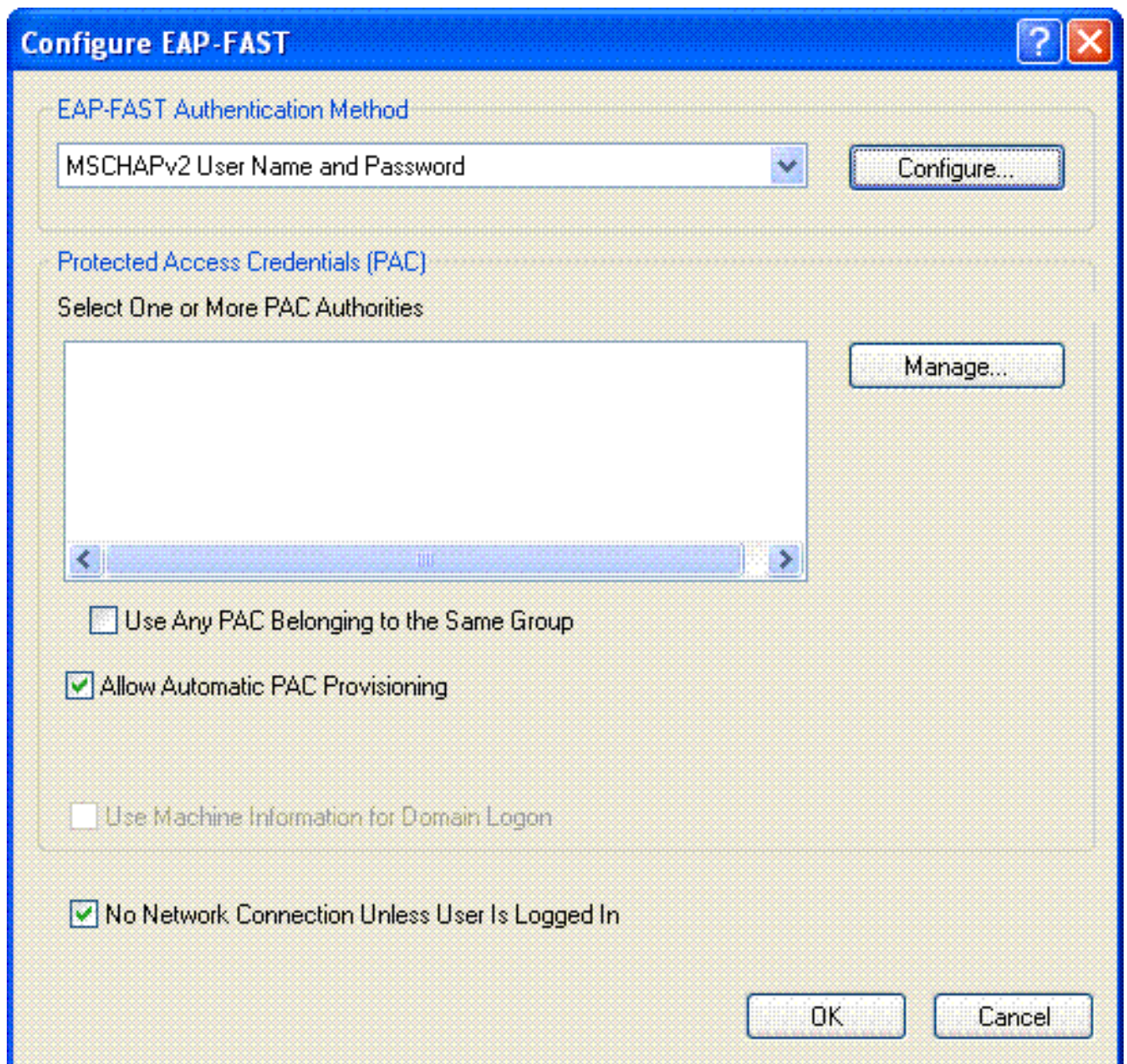
- Profile Settings:**
 - Profile Name: WPA2-Enterprise
 - Client Name: Wireless-Client1
- Network Names:**
 - SSID1: WPA2-Enterprise
 - SSID2: (empty)
 - SSID3: (empty)

Buttons: OK, Cancel

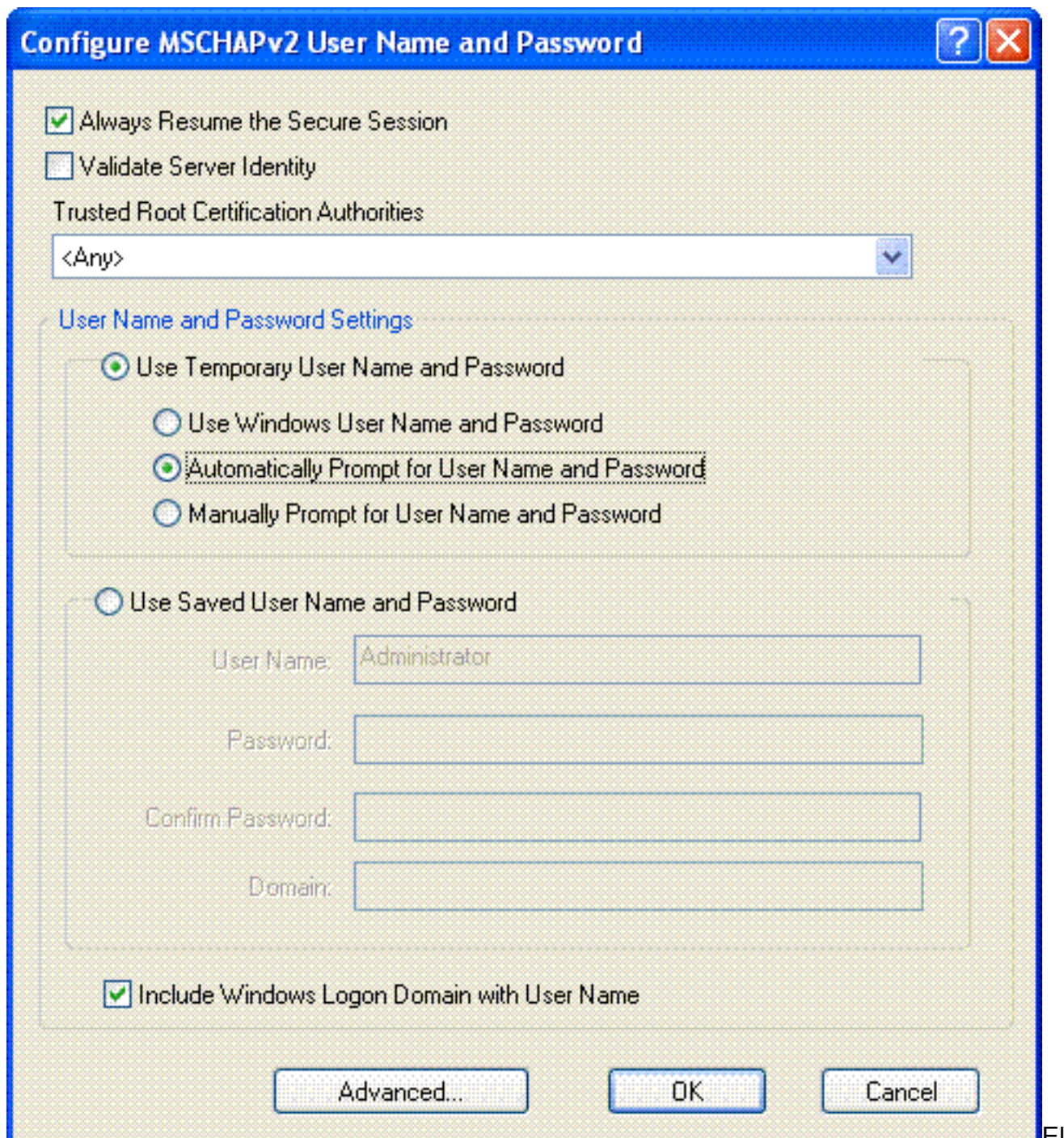
3. Haga clic en la ficha **Security** y seleccione **WPA/WPA2/CCKM** para activar el modo de funcionamiento de WPA2. En WPA/WPA2/CCKM EAP Type (Tipo de EAP WPA/WPA2/CCKM), seleccione **EAP-FAST**. Haga clic en **Configure** para configurar el ajuste EAP-FAST.



4. En la ventana Configure EAP-FAST, marque la casilla de verificación **Allow Automatic PAC Provisioning**. Si desea configurar el aprovisionamiento de PAC anónimo, EAP-MS-CHAP se utilizará como el único método interno en la fase cero.



5. Elija Nombre de usuario y Contraseña MSCHAPv2 como método de autenticación en el cuadro desplegable Método de autenticación EAP-FAST. Haga clic en Configurar (Configurar).
6. En la ventana Configurar nombre de usuario y contraseña de MSCHAPv2, elija la configuración de nombre de usuario y contraseña adecuada. En este ejemplo se elige **Pedir automáticamente nombre de usuario y contraseña**.



mismo nombre de usuario y la misma contraseña deben registrarse en ACS. Como se mencionó anteriormente, este ejemplo utiliza User1 y User1 respectivamente como nombre de usuario y contraseña. Además, tenga en cuenta que se trata de un aprovisionamiento en banda anónimo. Por lo tanto, el cliente no puede validar el certificado del servidor. Debe asegurarse de que la casilla de verificación Validar identidad de servidor no está activada.

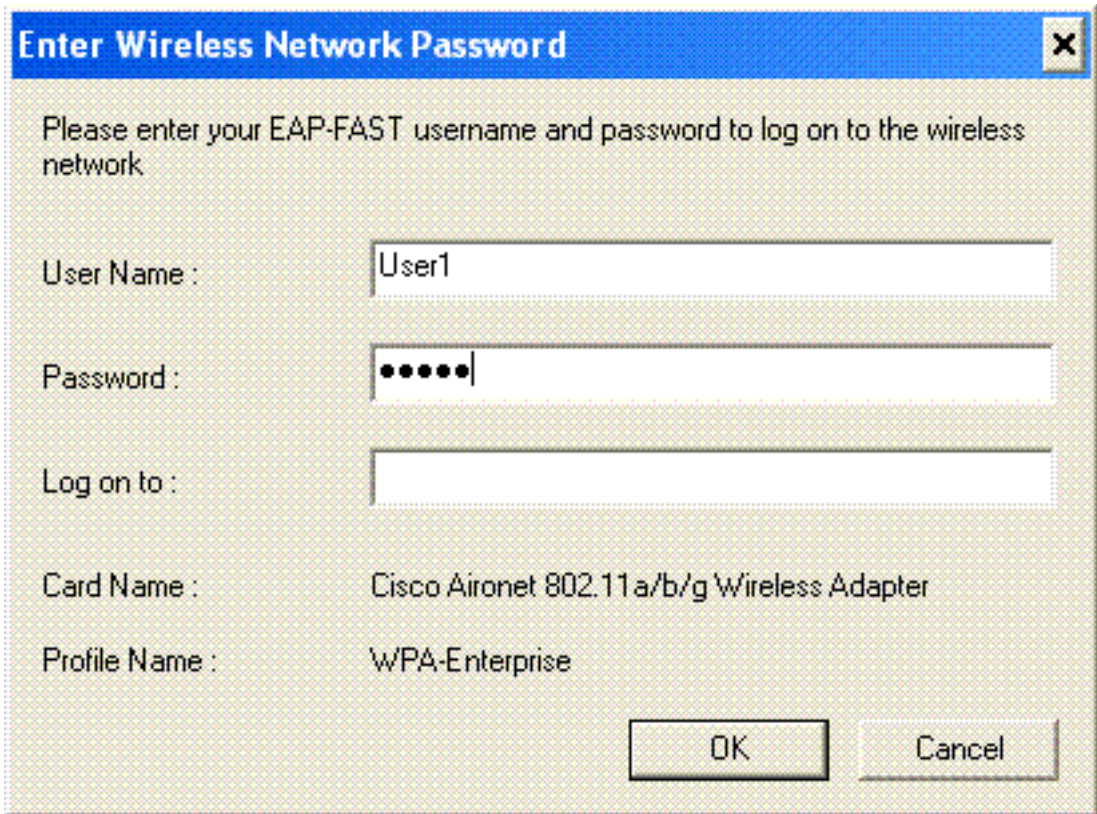
7. Click OK.

[Verificación del modo de funcionamiento de WPA2 Enterprise](#)

Complete estos pasos para verificar si su configuración del modo WPA2 Enterprise funciona correctamente:

1. En la ventana Aironet Desktop Utility, seleccione el perfil **WPA2-Enterprise** y haga clic en **Activate** para activar el perfil del cliente inalámbrico.
2. Si ha habilitado MS-CHAP ver2 como su autenticación, el cliente solicitará el nombre de

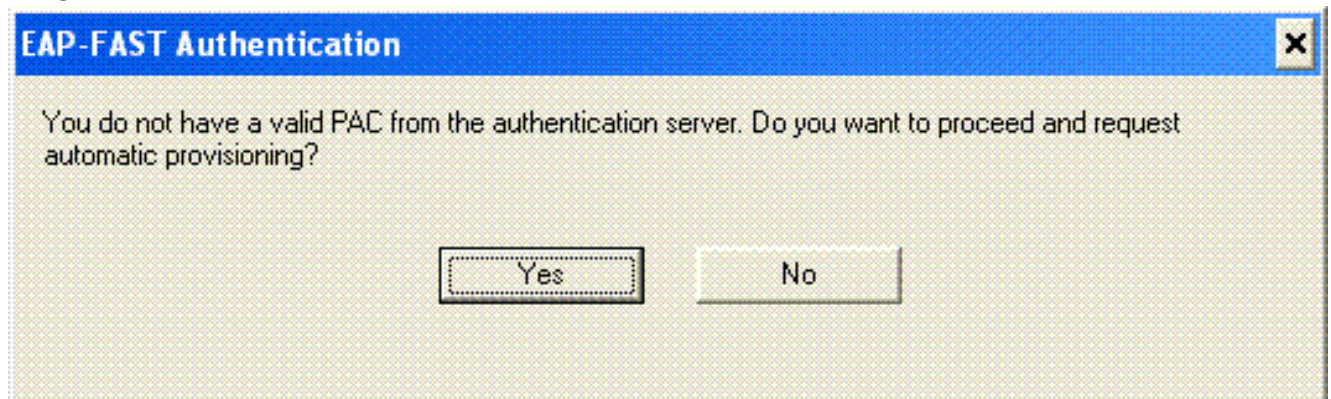
usuario y la



The screenshot shows a dialog box titled "Enter Wireless Network Password". The text inside reads: "Please enter your EAP-FAST username and password to log on to the wireless network". There are three input fields: "User Name" containing "User1", "Password" containing six dots, and "Log on to" which is empty. Below the input fields, the "Card Name" is "Cisco Aironet 802.11 a/b/g Wireless Adapter" and the "Profile Name" is "WPA-Enterprise". At the bottom right, there are "OK" and "Cancel" buttons.

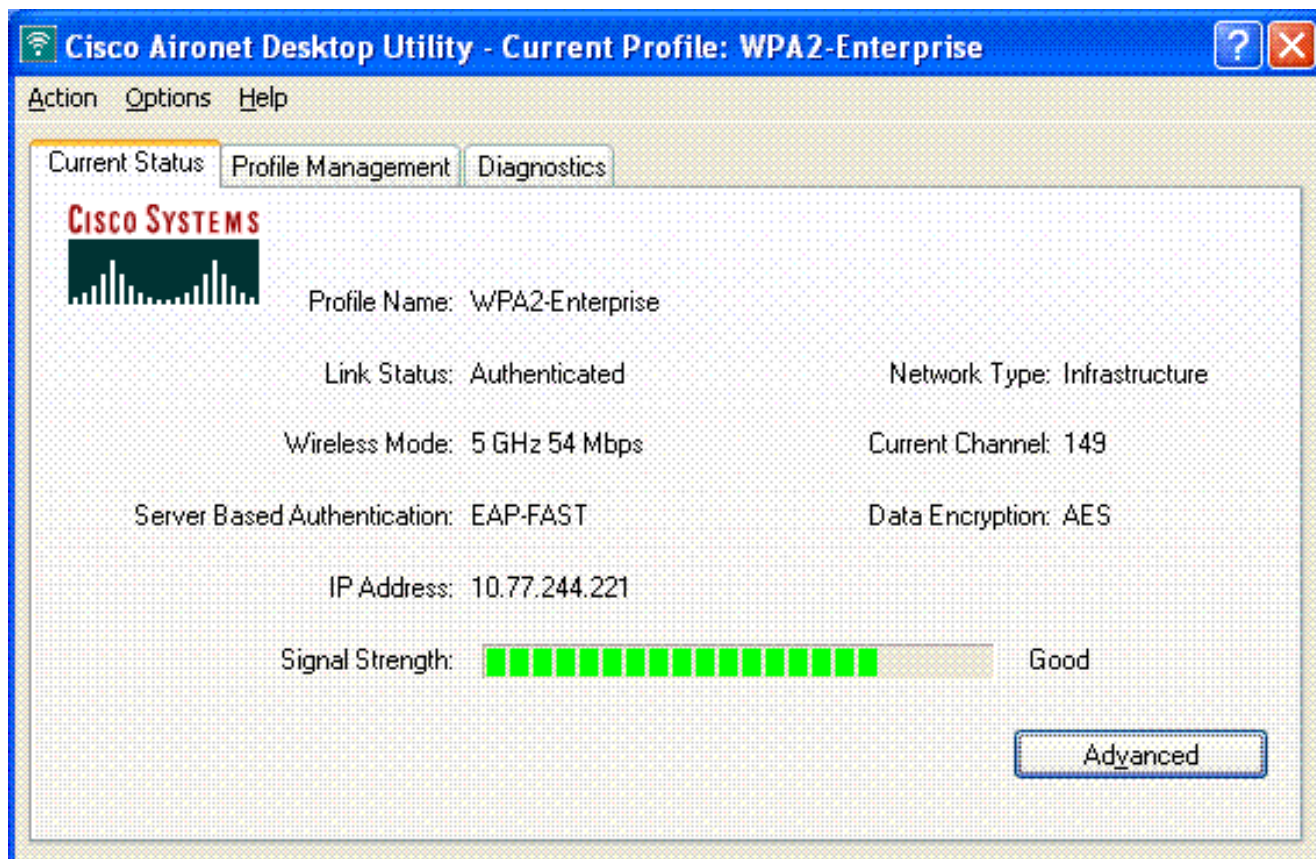
contraseña.

3. Durante el procesamiento EAP-FAST del usuario, el cliente le pedirá que solicite PAC del servidor RADIUS. Al hacer clic en **Sí**, se inicia el aprovisionamiento de PAC.



The screenshot shows a dialog box titled "EAP-FAST Authentication". The text inside reads: "You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?". At the bottom, there are "Yes" and "No" buttons.

4. Después del aprovisionamiento correcto de PAC en la fase cero, se siguen las fases uno y dos, y tiene lugar un procedimiento de autenticación correcto. Una vez realizada la autenticación correctamente, el cliente inalámbrico se asocia a WLAN WPA2-Enterprise. Esta es la captura de pantalla:



También puede verificar si el servidor RADIUS recibe y valida la solicitud de autenticación del cliente inalámbrico. Verifique los informes Passed Authentications and Failed Attempts en el servidor ACS para lograr esto. Estos informes están disponibles en Informes y actividades en el servidor ACS.

[Configuración de los dispositivos para el modo WPA2 Personal](#)

Siga estos pasos para configurar los dispositivos para el modo de funcionamiento WPA2-Personal:

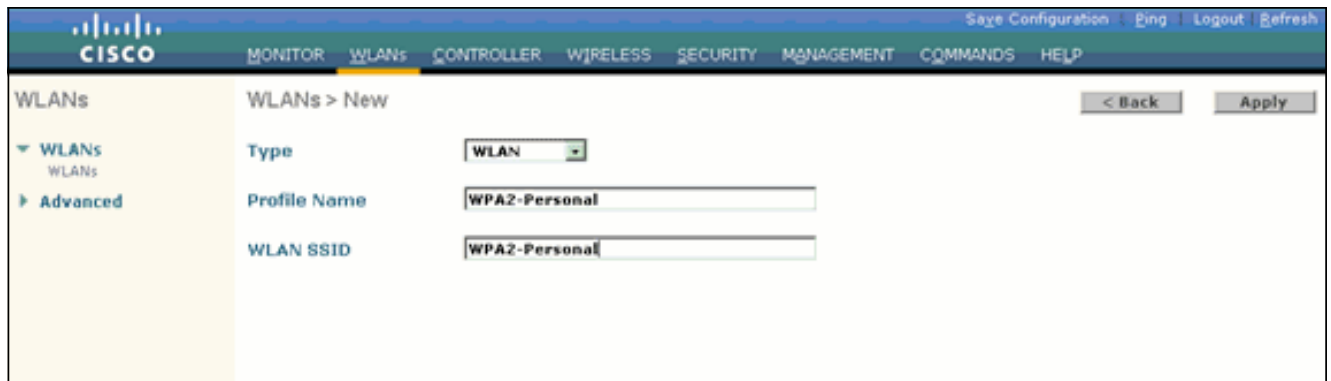
1. [Configuración de la WLAN para la autenticación en modo WPA2 Personal](#)
2. [Configuración del cliente inalámbrico para el modo WPA2 Personal](#)

[Configuración de la WLAN para el modo de funcionamiento WPA2 Personal](#)

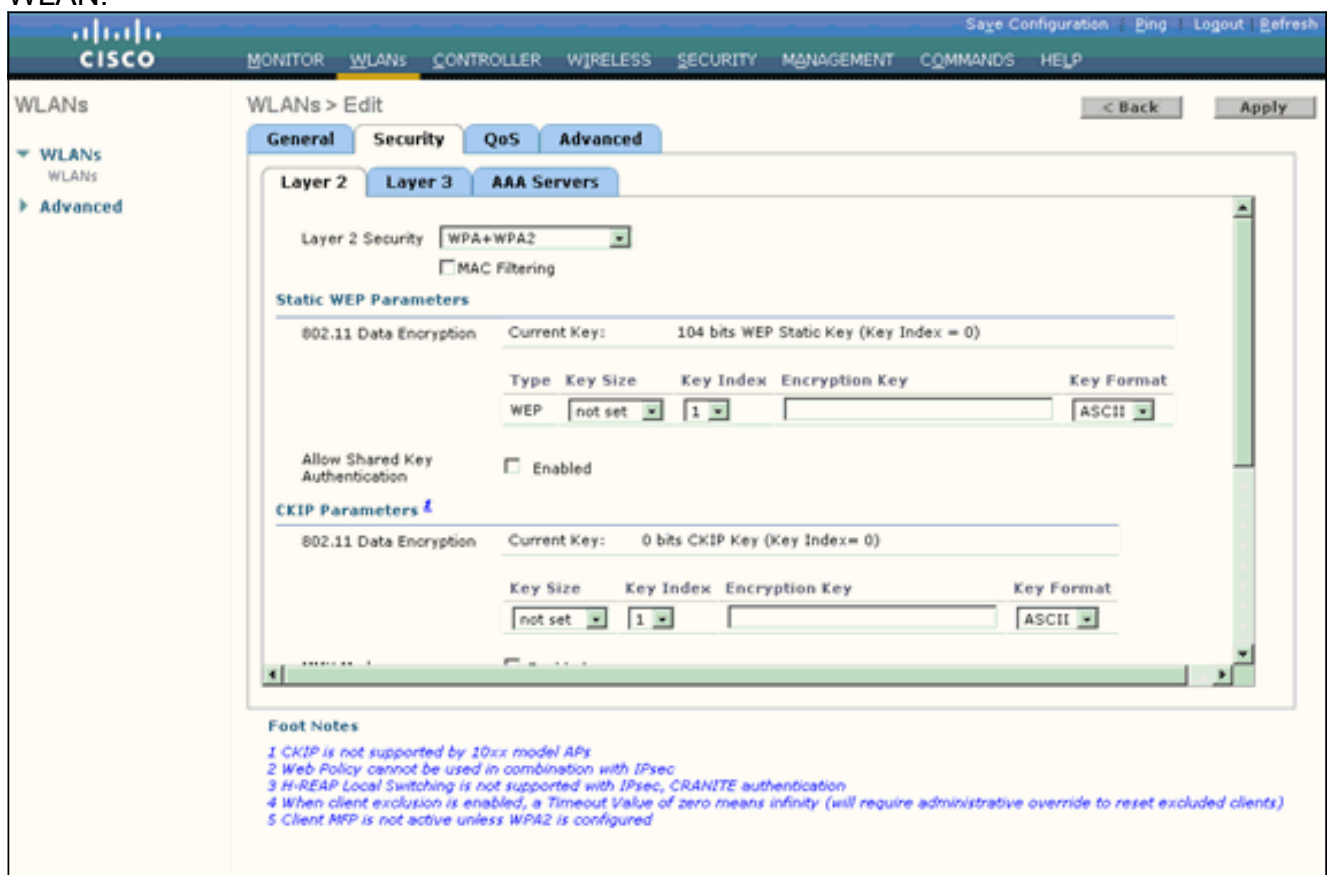
Debe configurar la WLAN que los clientes utilizarán para conectarse a la red inalámbrica. El SSID de WLAN para el modo WPA2 Personal será WPA2-Personal. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN y sus parámetros relacionados:

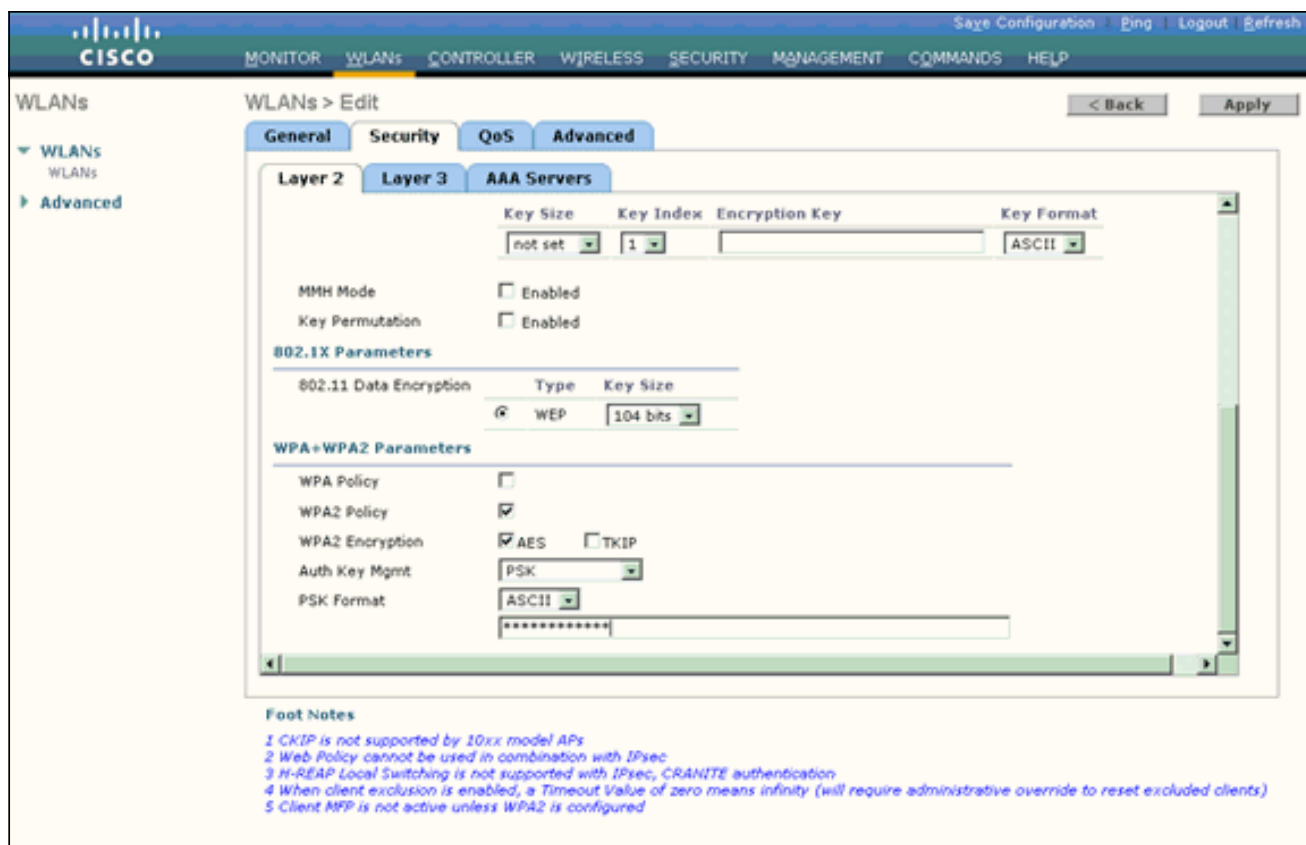
1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs. Esta página enumera las WLANs que existen en el controlador.
2. Haga clic en **Nuevo** para crear un nuevo WLAN.
3. Introduzca el nombre SSID de WLAN, el nombre de perfil y la ID de WLAN en la página WLAN > New (WLAN > Nuevo). A continuación, haga clic en **Aplicar**. Este ejemplo utiliza **WPA2-Personal** como SSID.



4. Una vez que haya creado una nueva WLAN, aparecerá la página **WLAN > Edit** para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, políticas de seguridad, políticas de QoS y parámetros avanzados.
5. En Políticas generales, marque la casilla de verificación **Status** para habilitar la WLAN.
6. Si desea que el AP difunda el SSID en sus tramas de baliza, marque la casilla de verificación **Broadcast SSID**.
7. Haga clic en la ficha Security (Seguridad). En Layer Security, seleccione **WPA+WPA2**. Esto activa la autenticación WPA para la WLAN.



8. Desplácese hacia abajo por la página para modificar los parámetros **WPA+WPA2**. En este ejemplo, se seleccionan la política WPA2 y el cifrado AES.
9. En Auth Key Mgmt, elija **PSK** para habilitar WPA2-PSK.
10. Introduzca la clave precompartida en el campo correspondiente, como se muestra a continuación.



Nota: La clave previamente compartida utilizada en el WLC debe coincidir con la configurada en los clientes inalámbricos.

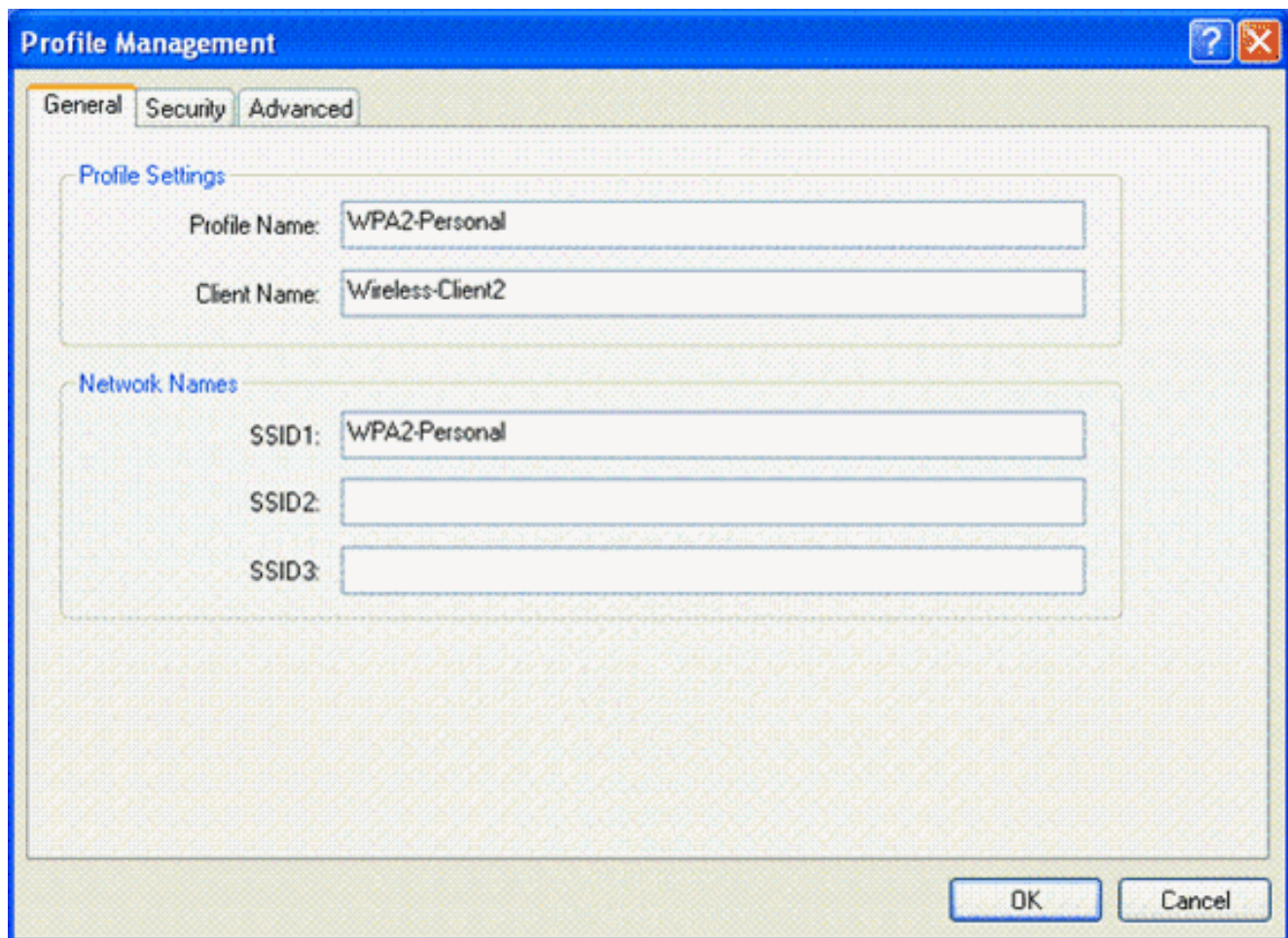
11. Haga clic en Apply (Aplicar).

[Configuración del cliente inalámbrico para el modo WPA2 Personal](#)

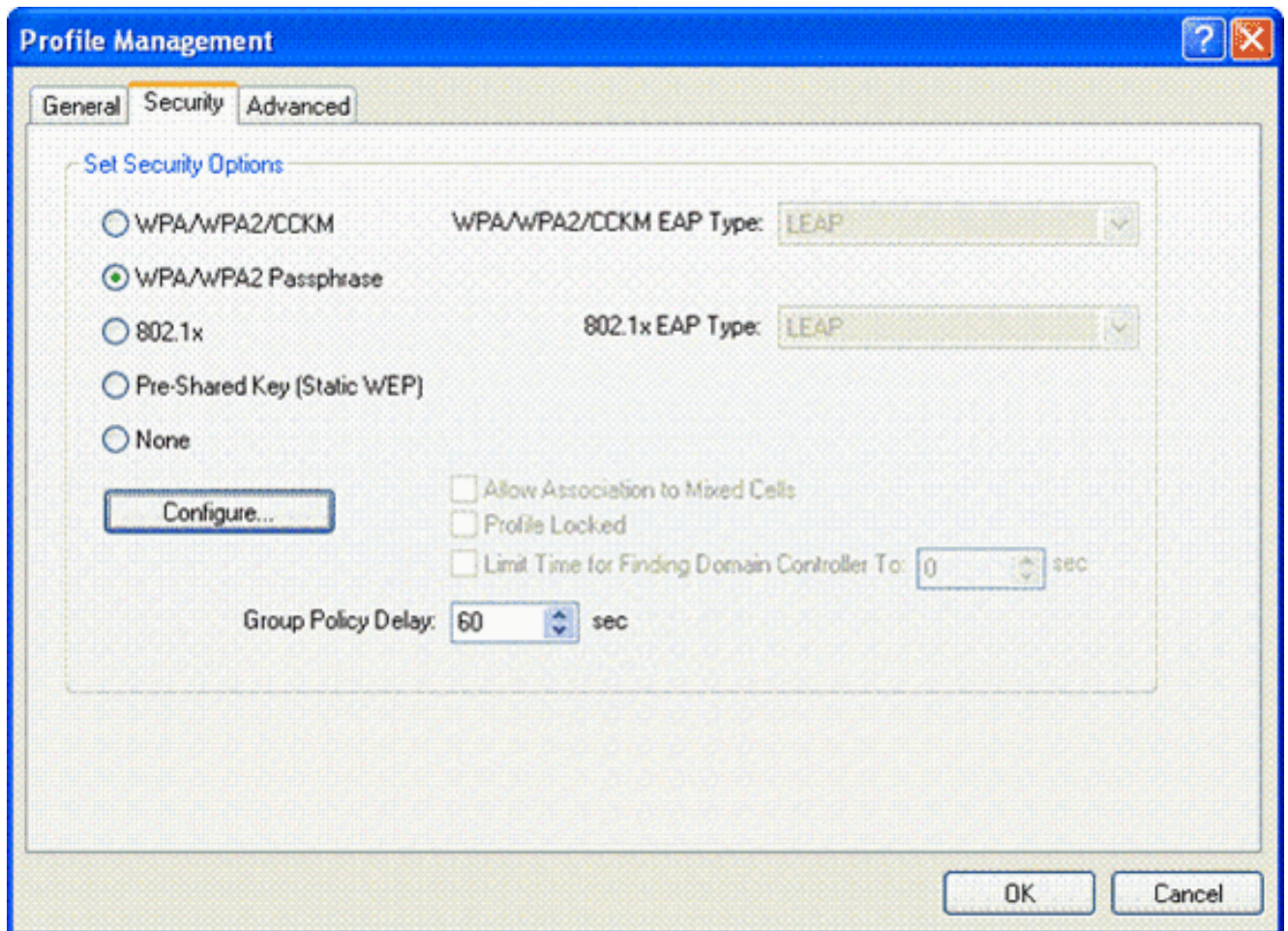
El siguiente paso consiste en configurar el cliente inalámbrico para el modo de funcionamiento WPA2-Personal.

Complete estos pasos para configurar el cliente inalámbrico para el modo WPA2-Personal:

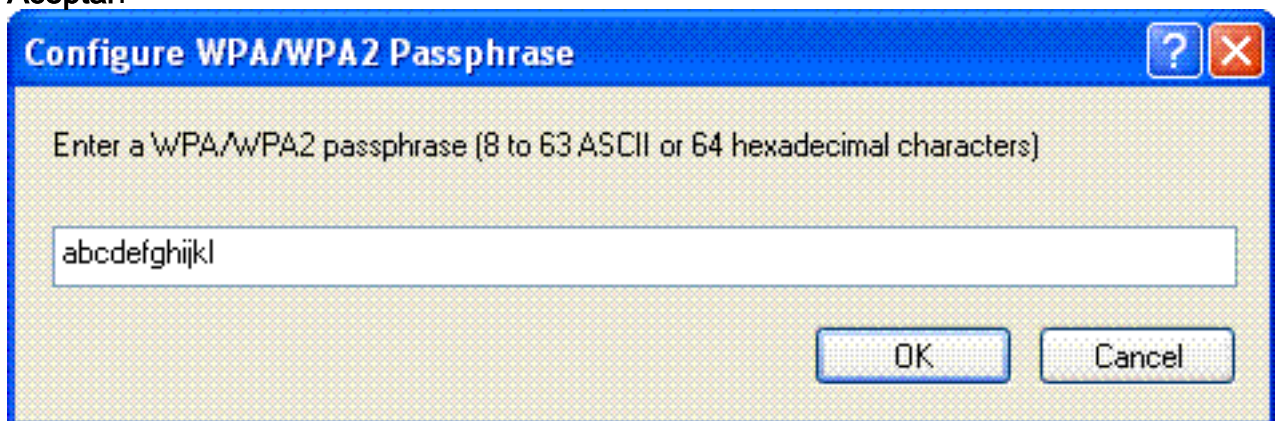
1. Desde la ventana Aironet Desktop Utility, haga clic en **Profile Management > New** para crear un perfil para el usuario WLAN WPA2-PSK.
2. Desde la ventana Profile Management, haga clic en la pestaña **General** y configure el nombre del perfil, el nombre del cliente y el nombre SSID como se muestra en este ejemplo. A continuación, haga clic en **Aceptar**.



3. Haga clic en la ficha **Security** y seleccione **WPA/WPA2 Passphrase** para activar el modo de funcionamiento de WPA2-PSK. Haga clic en **Configure** para configurar la clave previamente compartida WPA-PSK.



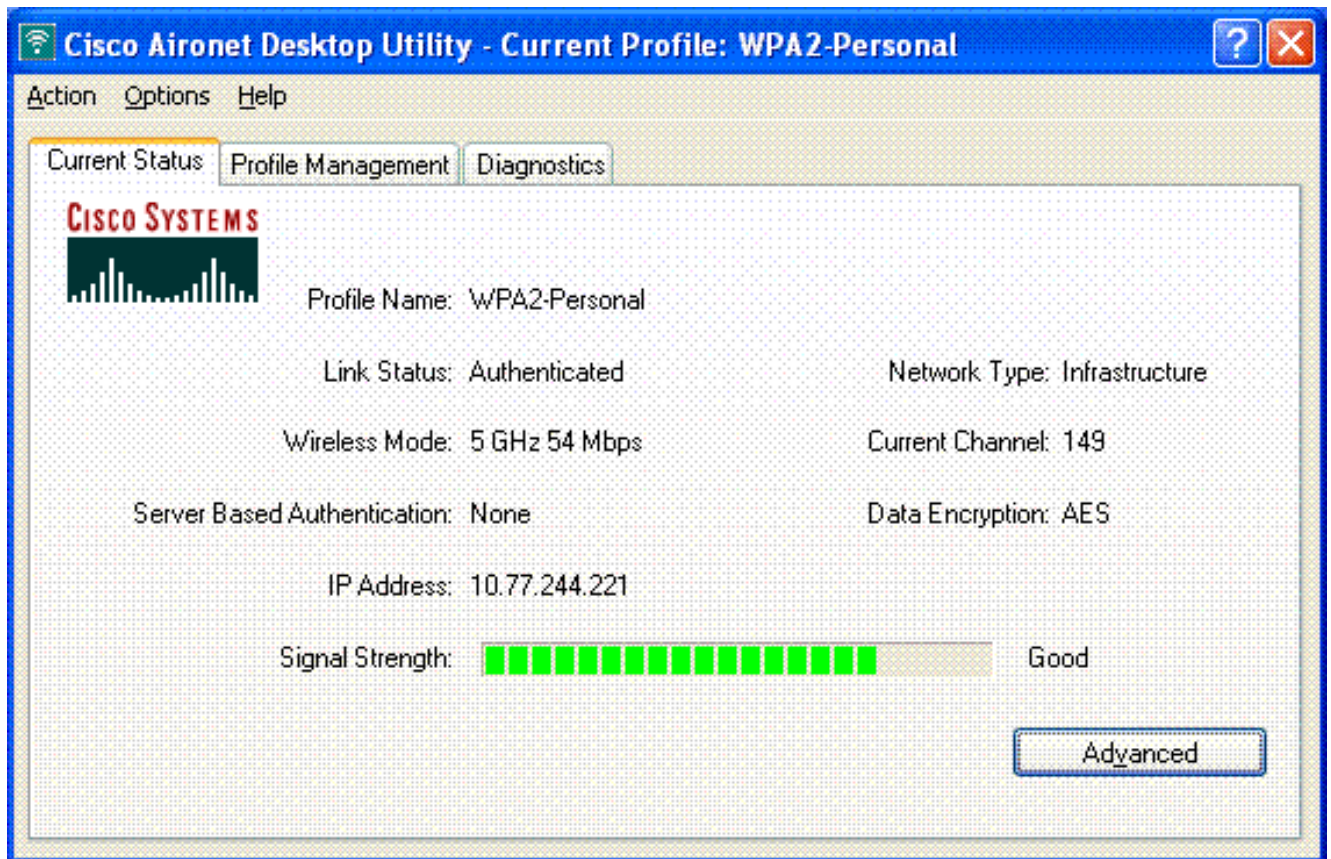
4. Introduzca la clave previamente compartida y haga clic en **Aceptar**.



Verificación del modo de funcionamiento de WPA2-Personal

Complete estos pasos para verificar si su configuración del modo WPA2-Enterprise funciona correctamente:

1. Desde la ventana de Aironet Desktop Utility, seleccione el perfil **WPA2-Personal** y haga clic en **Activar** para activar el perfil del cliente inalámbrico.
2. Una vez que se activa el perfil, el cliente inalámbrico se asocia a la WLAN tras una autenticación exitosa. Esta es la captura de pantalla:



Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Estos comandos **debug** serán útiles para resolver problemas de configuración:

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos **debug**.

- **debug dot1x events enable:** habilita la depuración de todos los eventos dot1x. A continuación se presenta un ejemplo de resultado de depuración basado en una autenticación exitosa:**Nota:** Algunas de las líneas de esta salida se han movido a la segunda línea debido a limitaciones de espacio.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....
.....
.....
.....
```

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)**

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)**

Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)**

Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0

Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0

Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1

Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ==> 19 for STA 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from

mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for
mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to
mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ==>
20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ==>
24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge
for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 25)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for**

mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0)**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25)**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending default RC4 key to mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received Auth Success while in Authenticating state for mobile 00:40:96:af:3e:93**

- **debug dot1x packet enable**: habilita la depuración de mensajes de paquetes 802.1x.
- **debug aaa events enable**: habilita la salida de depuración de todos los eventos aaa.

[Información Relacionada](#)

- [WPA2: acceso Wi-Fi protegido 2](#)
- [Ejemplo de Configuración de Autenticación EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo](#)
- [Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN \(WLC\)](#)
- [Introducción a la configuración WPA](#)
- [Soporte de Productos de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).