

La página del chapoteo del regulador del Wireless LAN reorienta el ejemplo de configuración

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configuración de la red](#)

[Configurar](#)

[Paso 1. Configure el WLC para la autenticación de RADIUS a través del servidor del Cisco Secure ACS.](#)

[Paso 2. Configure los WLAN para el departamento Admin y de operaciones.](#)

[Paso 3. Configure el Cisco Secure ACS para soportar la página del chapoteo reorientan la característica.](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la función de redireccionamiento de la página de presentación en los Controladores de LAN Inalámbricos.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de las soluciones acerca de la seguridad del LWAPP
- Conocimiento de cómo configurar el Cisco Secure ACS

Componentes Utilizados

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

- El regulador del Wireless LAN de las Cisco 4400 Series (WLC) ese funciona con la versión de firmware 5.0
- Lightweight Access Point de las Cisco 1232 Series (REVESTIMIENTO)
- Adaptador de red inalámbrica de cliente del Cisco Aironet 802.a/b/g que funciona con la versión de firmware 4.1
- Servidor del Cisco Secure ACS que funciona con la versión 4.1
- Cualquier servidor Web externo de tercera persona

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

[Antecedentes](#)

La red de la página del chapoteo reorienta es una característica introducida con la versión 5.0 del regulador del Wireless LAN. Con esta característica, reorientan al usuario a una página web determinada después de que la autenticación del 802.1x haya completado. La reorientación ocurre cuando el usuario abre un navegador (configurado con un Home Page predeterminado) o los intentos para acceder un URL. Después de que la reorientación a la página web sea completa, el usuario tiene acceso total a la red.

Usted puede especificar la página de la reorientación en el servidor del Remote Authentication Dial-In User Service (RADIUS). El servidor de RADIUS debe ser configurado para volver el cisco av-pair URL-reorienta el atributo de RADIUS al regulador del Wireless LAN sobre la autenticación acertada del 802.1x.

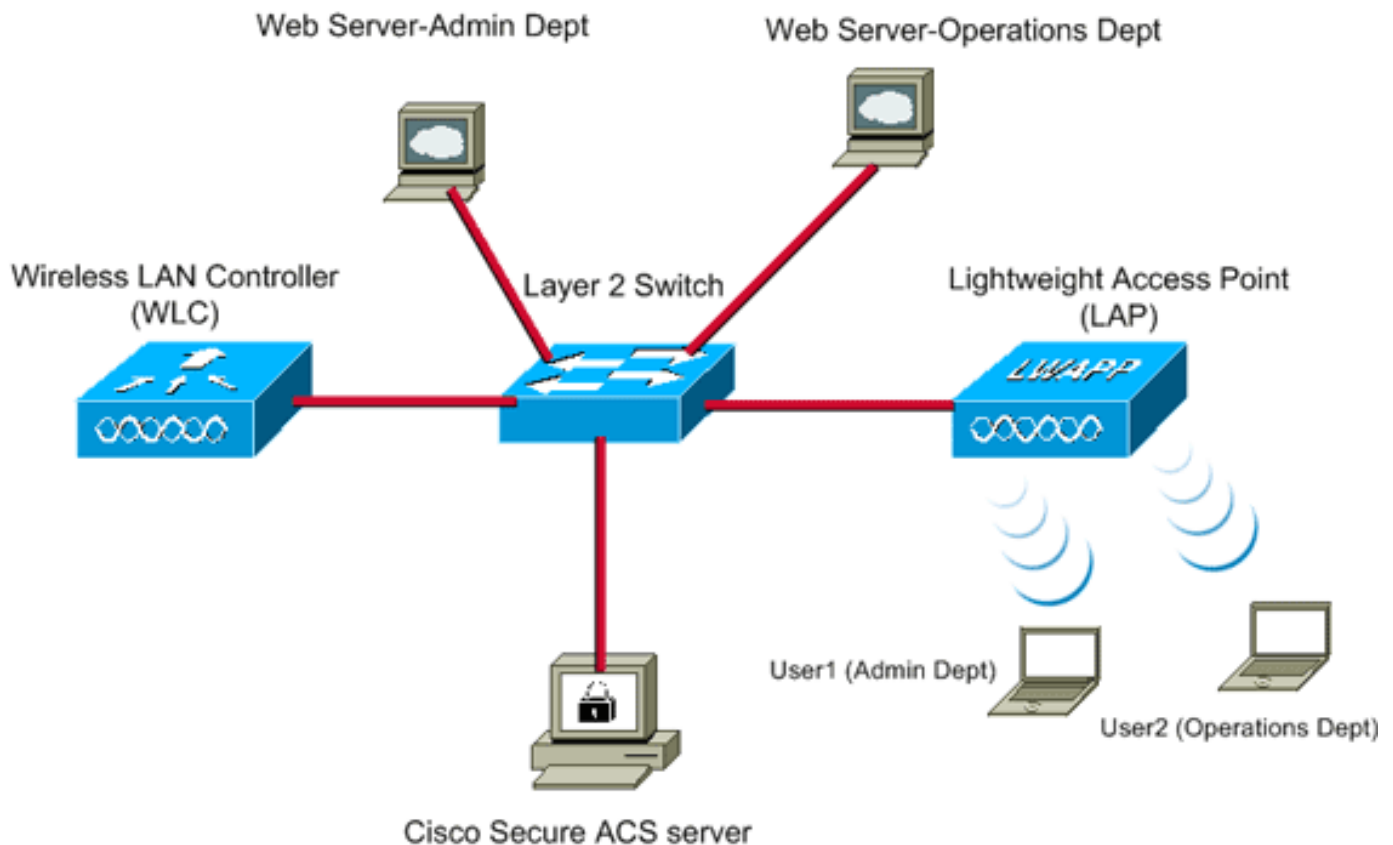
La red de la página del chapoteo reorienta la característica está disponible solamente para los WLAN configurados para el 802.1x o WPA/WPA2 acoda la Seguridad 2.

[Configuración de la red](#)

En este ejemplo, un WLC de Cisco 4404 y un REVESTIMIENTO de las Cisco 1232 Series están conectados a través de un 2 Switch de la capa. El servidor del Cisco Secure ACS (que actúa como servidor RADIUS externo) también está conectado con el mismo Switch. Todos los dispositivos están en la misma subred.

El REVESTIMIENTO se registra inicialmente al regulador. Usted debe crear dos WLAN: uno para los **usuarios del departamento administrativos** y el otro para los usuarios del **departamento de operaciones**. Ambos uso WPA2/ AES de la Tecnología inalámbrica LAN (el EAP-FAST se utiliza para la autenticación). Ambos WLAN utilizan la página del chapoteo reorientan la característica para reorientar a los usuarios al Home Page apropiado URL (en los servidores Web externos).

En este documento, se utiliza esta configuración de red:



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

La siguiente sección explica cómo configurar los dispositivos para esta configuración.

Configurar

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

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Complete estos pasos para configurar los dispositivos para utilizar la página del chapoteo reorientan la característica:

1. [Configure el WLC para la autenticación de RADIUS a través del servidor del Cisco Secure ACS.](#)
2. [Configure los WLAN para los departamentos Admin y de operaciones.](#)
3. [Configure el Cisco Secure ACS para soportar la página del chapoteo reorientan la característica.](#)

[Paso 1. Configure el WLC para la autenticación de RADIUS a través del servidor del Cisco Secure ACS.](#)

El WLC necesita ser configurado para remitir los credenciales de usuario a un servidor RADIUS externo.

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

1. Elija la **Seguridad** y la **autenticación de RADIUS** del regulador GUI para visualizar la página de los servidores de autenticación de RADIUS.
2. Haga clic **nuevo** para definir a un servidor de RADIUS.
3. Defina los parámetros del servidor de RADIUS en los servidores de autenticación de RADIUS > nueva página. Estos parámetros incluyen: Dirección IP del servidor de RADIUS, secreto compartido, número de puerto, Estado del servidor

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The left sidebar shows the navigation menu with 'Security' expanded to 'RADIUS'. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Field	Value
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

Este documento utiliza al servidor ACS con una dirección IP de 10.77.244.196.

4. Haga clic en Apply (Aplicar).

[Paso 2. Configure los WLAN para el departamento Admin y de operaciones.](#)

En este paso, usted configura los dos WLAN (uno para el departamento de administración y el otro para el departamento de operaciones) que los clientes utilizarán para conectar con la red inalámbrica.

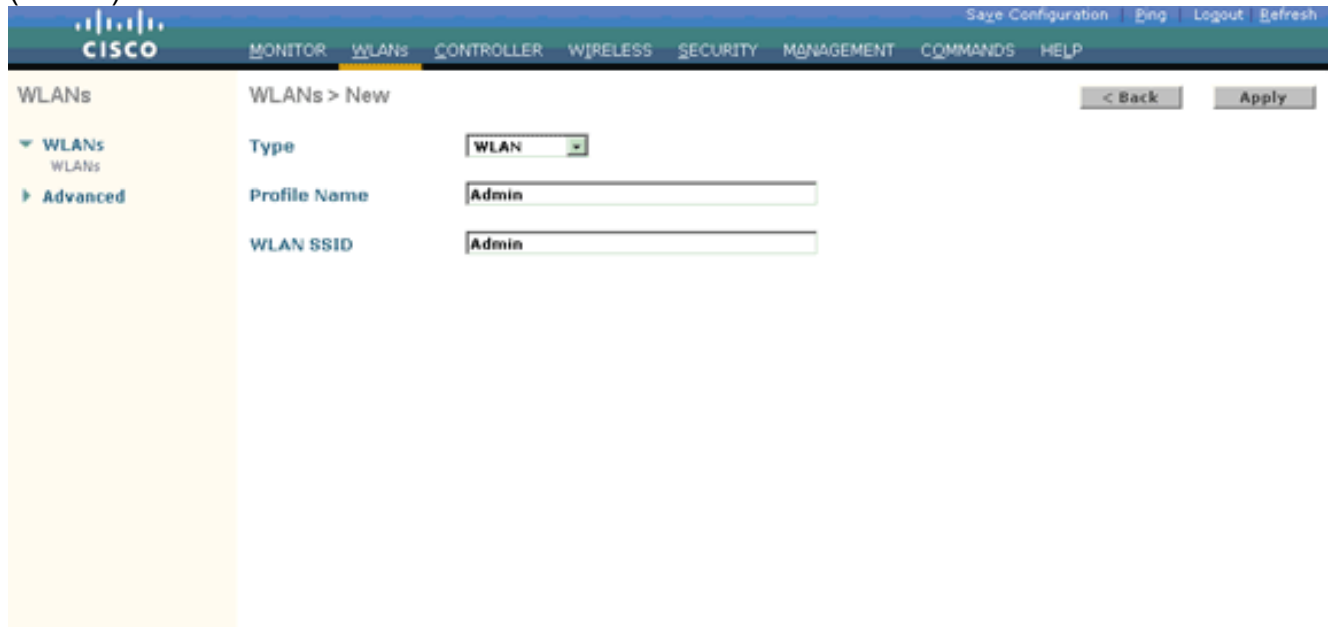
La red inalámbrica (WLAN) SSID para el departamento de administración será *Admin*. La red inalámbrica (WLAN) SSID para el departamento de operaciones será *operaciones*.

Utilice la autenticación del EAP-FAST para habilitar el WPA2 como el mecanismo de seguridad de

la capa 2 en ambos WLAN y la directiva de la red - la red de la página del chapoteo reorienta la característica como el método de seguridad de la capa 3.

Complete estos pasos para configurar la red inalámbrica (WLAN) y sus parámetros relacionados:

1. Haga clic los **WLAN** del GUI del regulador para visualizar la página WLAN. Esta página enumera los WLAN que existen en el regulador.
2. Tecleo **nuevo** para crear una nueva red inalámbrica (WLAN).

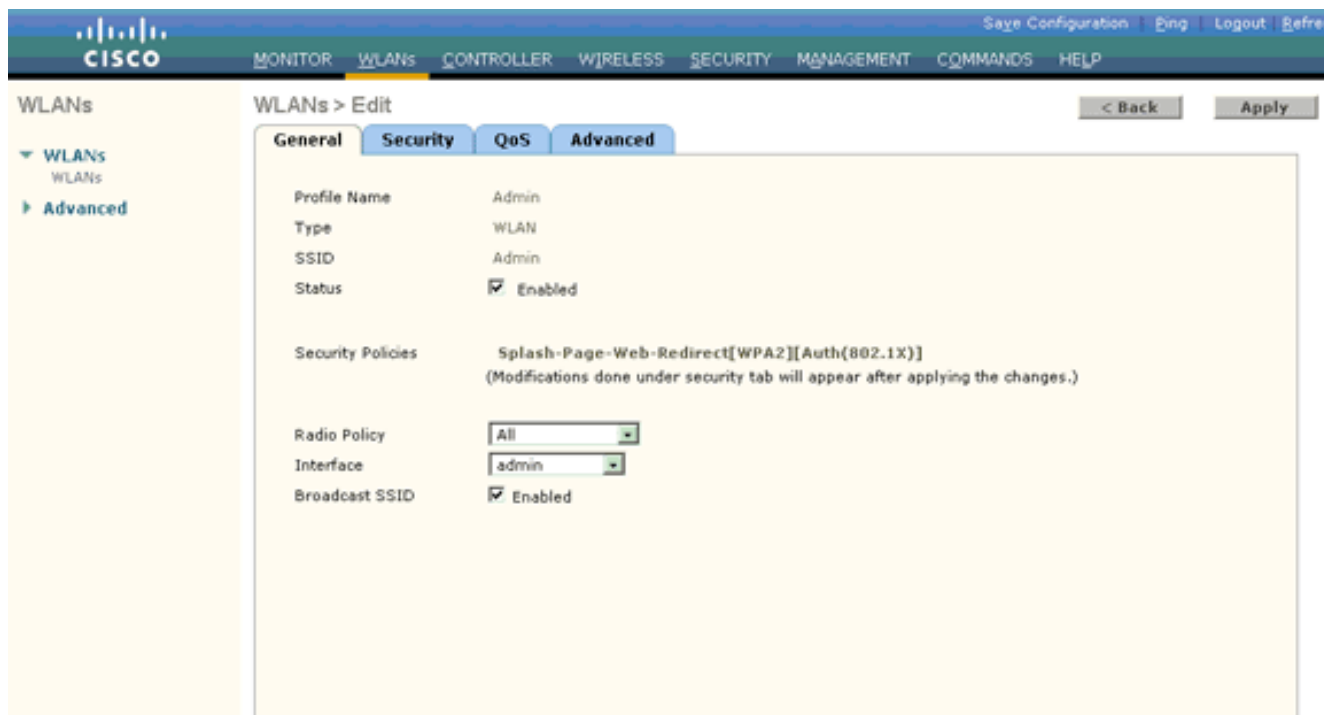


The screenshot shows the Cisco GUI for configuring WLANs. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs' section is active, and the 'New' page is displayed. The form fields are as follows:

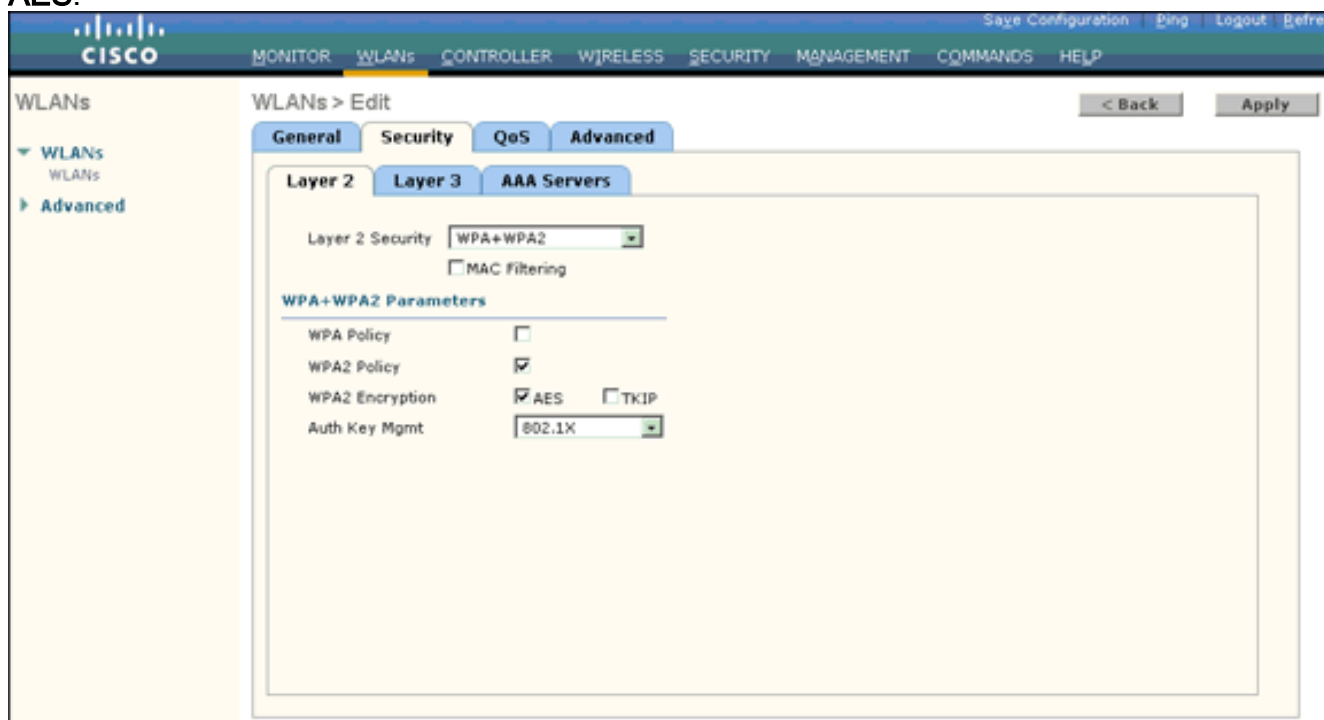
Field	Value
Type	WLAN
Profile Name	Admin
WLAN SSID	Admin

Buttons for '< Back' and 'Apply' are visible at the top right of the form area.

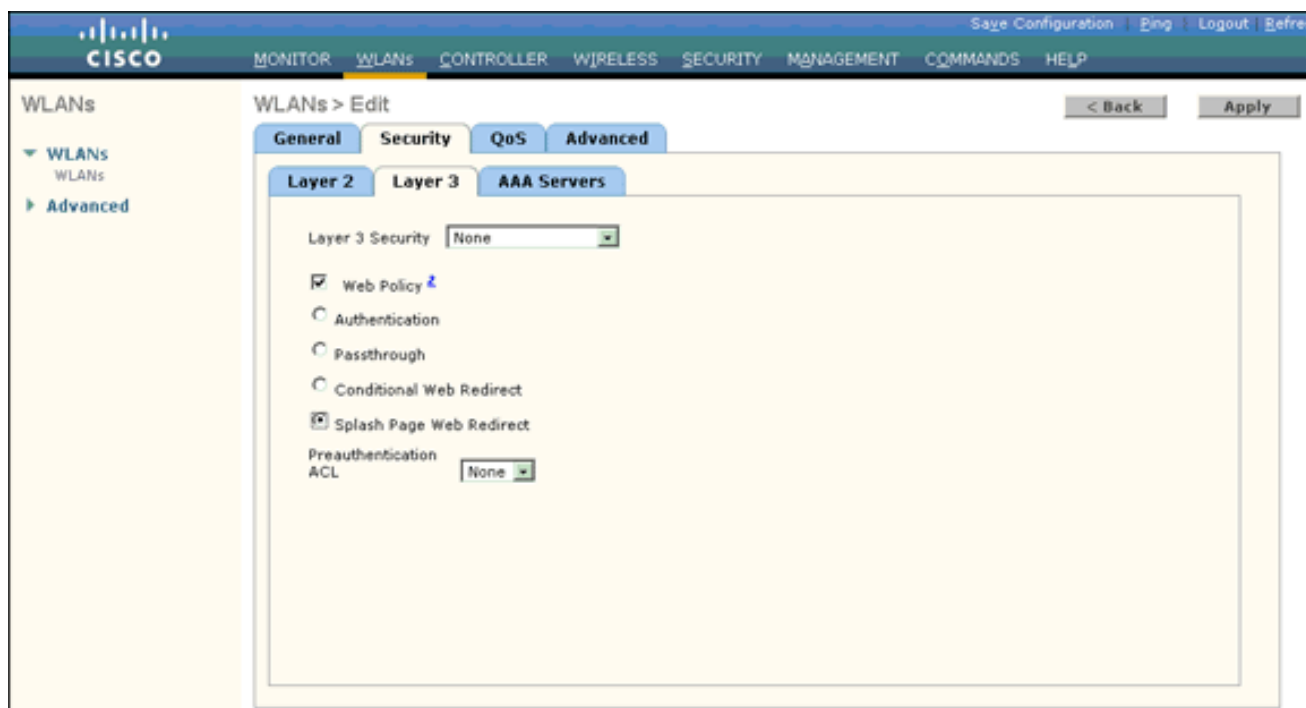
3. Ingrese el nombre WLAN SSID y el nombre del perfil en los WLAN > nueva página.
4. Haga clic en Apply (Aplicar).
5. Primero déjenos crear la red inalámbrica (WLAN) para el departamento de administración. Una vez que usted crea una nueva red inalámbrica (WLAN), la red inalámbrica (WLAN) > edita la página para la nueva red inalámbrica (WLAN) aparece. En esta página, usted puede definir los diversos parámetros específicos a esta red inalámbrica (WLAN). Esto incluye las políticas generales, las políticas de seguridad, las directivas QOS, y los parámetros avanzados.
6. Bajo políticas generales, marque el cuadro de **revisión de estado** para habilitar la red inalámbrica (WLAN).



7. Haga clic la **ficha de seguridad**, y después haga clic la lengüeta de la **capa 2**.
8. Elija **WPA+WPA2** de la lista desplegable de la Seguridad de la capa 2. Este paso habilita la autenticación WPA para la red inalámbrica (WLAN).
9. Bajo parámetros WPA+WPA2, marque las casillas de verificación de la **directiva WPA2** y de la **encriptación AES**.

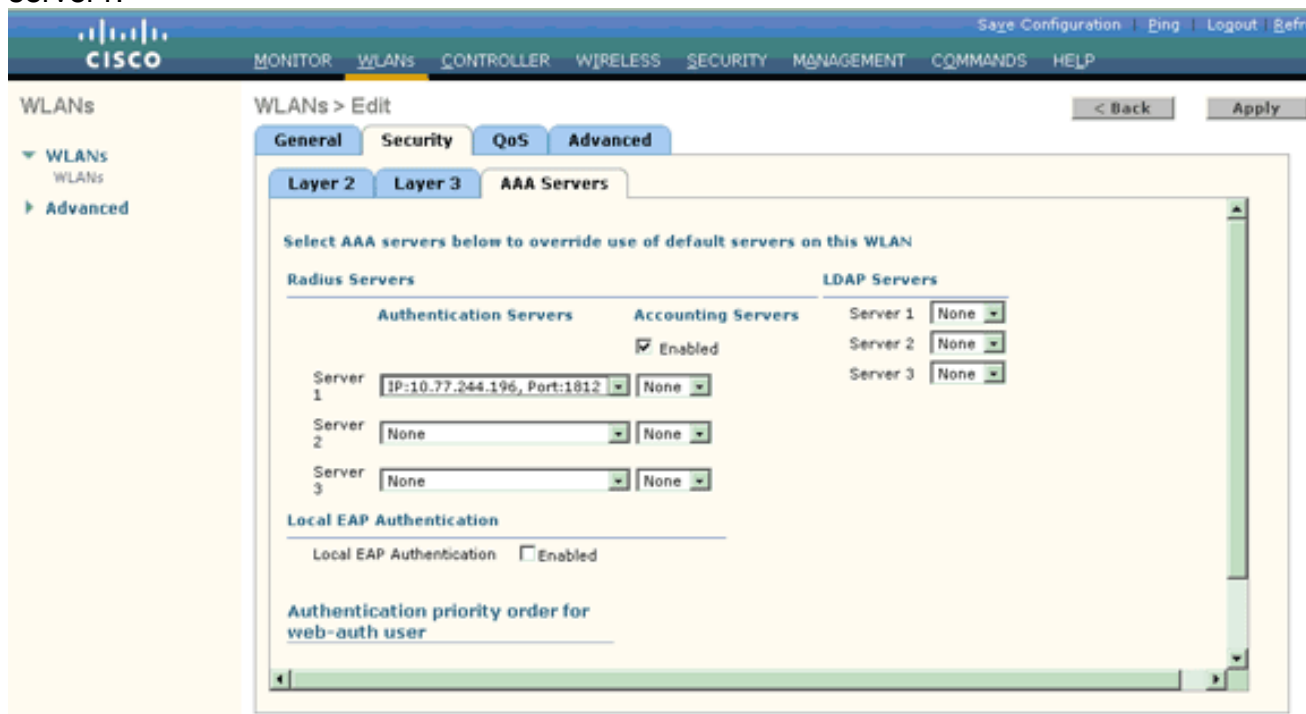


10. Elija el **802.1x** de la lista desplegable del mgmt de la clave del auth. Esta opción habilita el WPA2 con la autenticación 802.1x/EAP y la encriptación AES para la red inalámbrica (WLAN).
11. Haga clic la **ficha de seguridad de la capa 3**.
12. Marque el cuadro de la **directiva de la red**, y después haga clic la **red de la página del chapoteo reorientan** el botón de radio. Esta opción habilita la red de la página del chapoteo reorienta la característica.



13. Haga clic la lengüeta de los **servidores de AAA**.

14. Bajo los servidores de autenticación, elija el dirección IP del servidor apropiado de la lista desplegable del server1.



En este ejemplo, 10.77.244.196 se utiliza como el servidor de RADIUS.

15. Haga clic en Apply (Aplicar).

16. Relance los pasos 2 a 15 para crear la red inalámbrica (WLAN) para el departamento de operaciones. Los WLAN pagan las listas los dos WLAN que usted creó.

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
Admin	WLAN	Admin	Enabled	[WPA2][Auth(802.1X)], Splash-Page
Operations	WLAN	Operations	Enabled	[WPA2][Auth(802.1X)], Splash-Page

Note que las políticas de seguridad incluyen la página del chapoteo reorientan.

[Paso 3. Configure el Cisco Secure ACS para soportar la página del chapoteo reorientan la característica.](#)

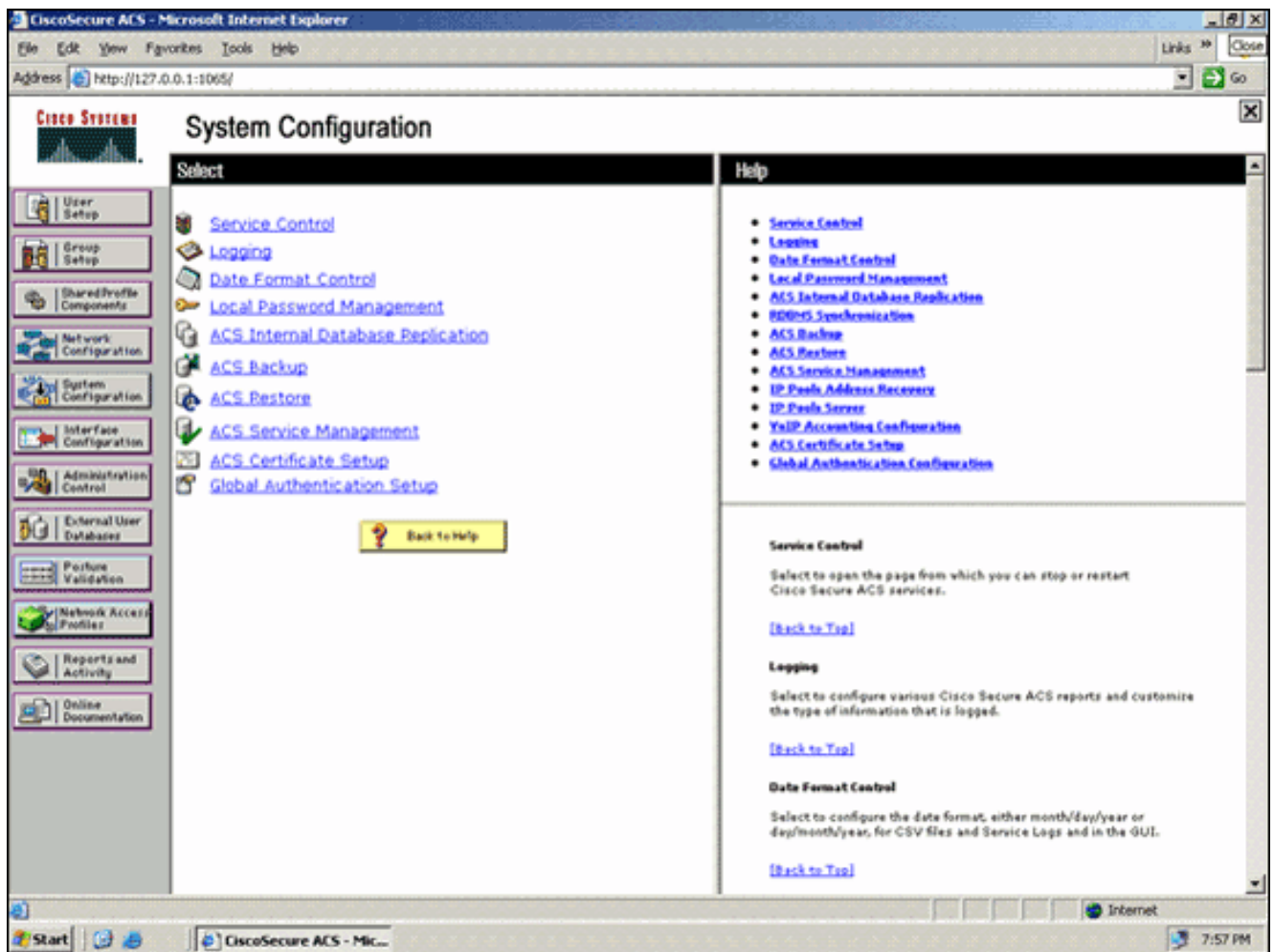
El siguiente paso es configurar al servidor de RADIUS para esta característica. El servidor de RADIUS necesita realizar la autenticación del EAP-FAST para validar las credenciales del cliente, y sobre la autenticación satisfactoria, reorientar al usuario al URL (en el servidor Web externo) especificada en el cisco av-pair URL-*reorienta el* atributo de RADIUS.

Configure el Cisco Secure ACS para la autenticación del EAP-FAST

Nota: Este documento asume que el regulador del Wireless LAN está agregado al Cisco Secure ACS como cliente AAA.

Complete estos pasos para configurar la autenticación del EAP-FAST en el servidor de RADIUS:

1. Haga clic la **configuración del sistema del** servidor de RADIUS GUI, y después elija eligen la **configuración de la autenticación global de la** página de la configuración del sistema.



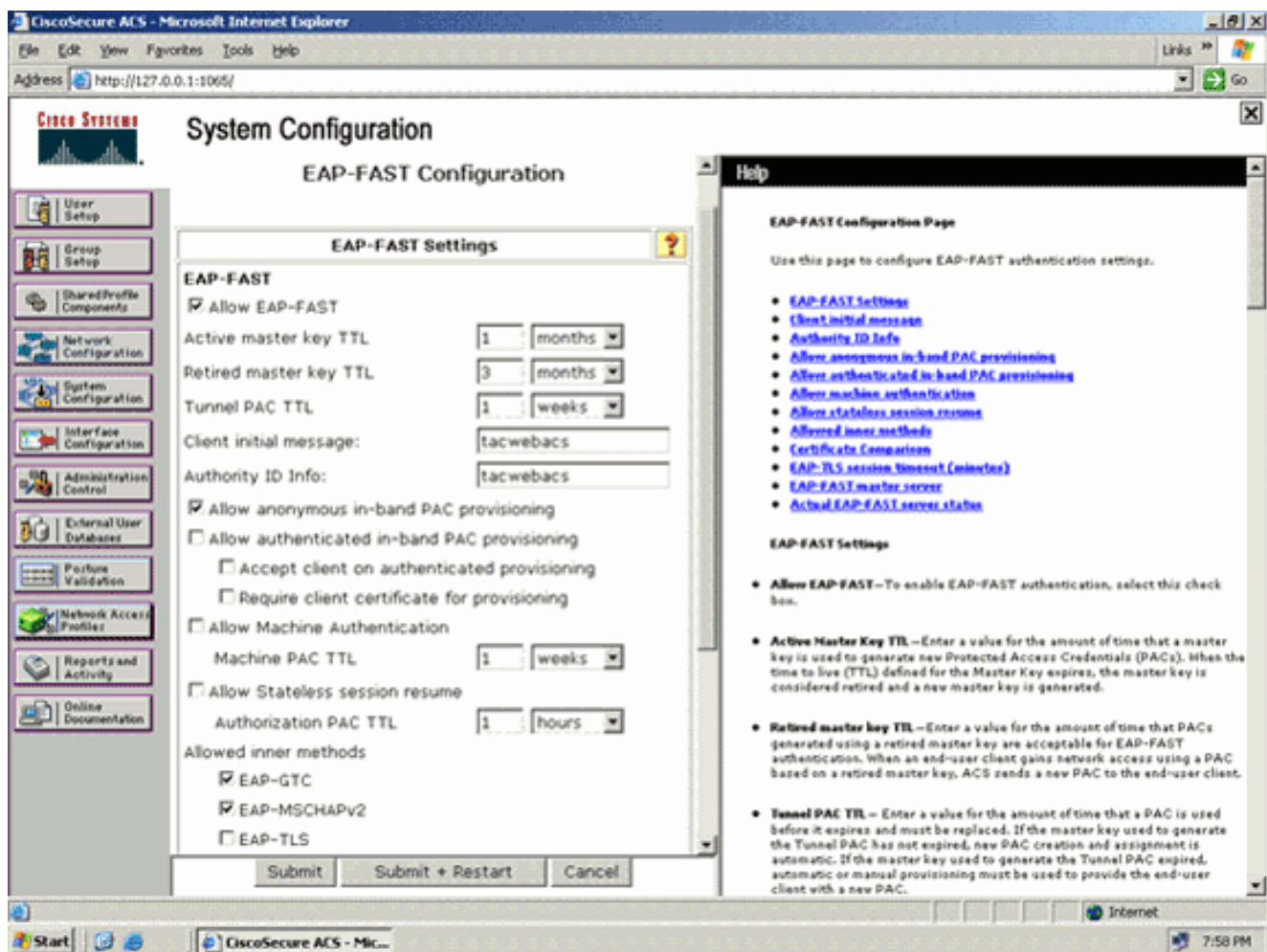
2. De la página de configuración de la autenticación global, haga clic la configuración del EAP-FAST para ir a la página de las configuraciones del EAP-FAST.

The screenshot shows the CiscoSecure ACS System Configuration page in Microsoft Internet Explorer. The address bar shows the URL <http://127.0.0.1:1005/>. The page title is "System Configuration". The left sidebar contains navigation links for various configuration areas: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Database, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "EAP Configuration" and contains the following sections:

- PEAP**
 - Allow EAP-MSCHAPv2
 - Allow EAP-GTC
 - Allow Posture Validation
 - Allow EAP-TLS
- Select one or more of the following options:
 - Certificate SAN comparison
 - Certificate CN comparison
 - Certificate binary comparison
- EAP-TLS session timeout (minutes):
- Cisco client initial message:
- PEAP session timeout (minutes):
- Enable Fast Reconnect:
- EAP-FAST**
 - [EAP-FAST Configuration](#)
- EAP-TLS**
 - Allow EAP-TLS
- Select one or more of the following options:
 - Certificate SAN comparison

At the bottom of the configuration area are buttons for "Submit", "Submit + Restart", and "Cancel". A "Help" window is open on the right side of the page, providing information about EAP and PEAP protocols. The help text includes a list of links for various EAP protocols and a detailed description of EAP and PEAP.

- De la página Configuración del EAP-FAST, marque la casilla de verificación del **EAP-FAST** de la permit para habilitar el EAP-FAST en el servidor de RADIUS.



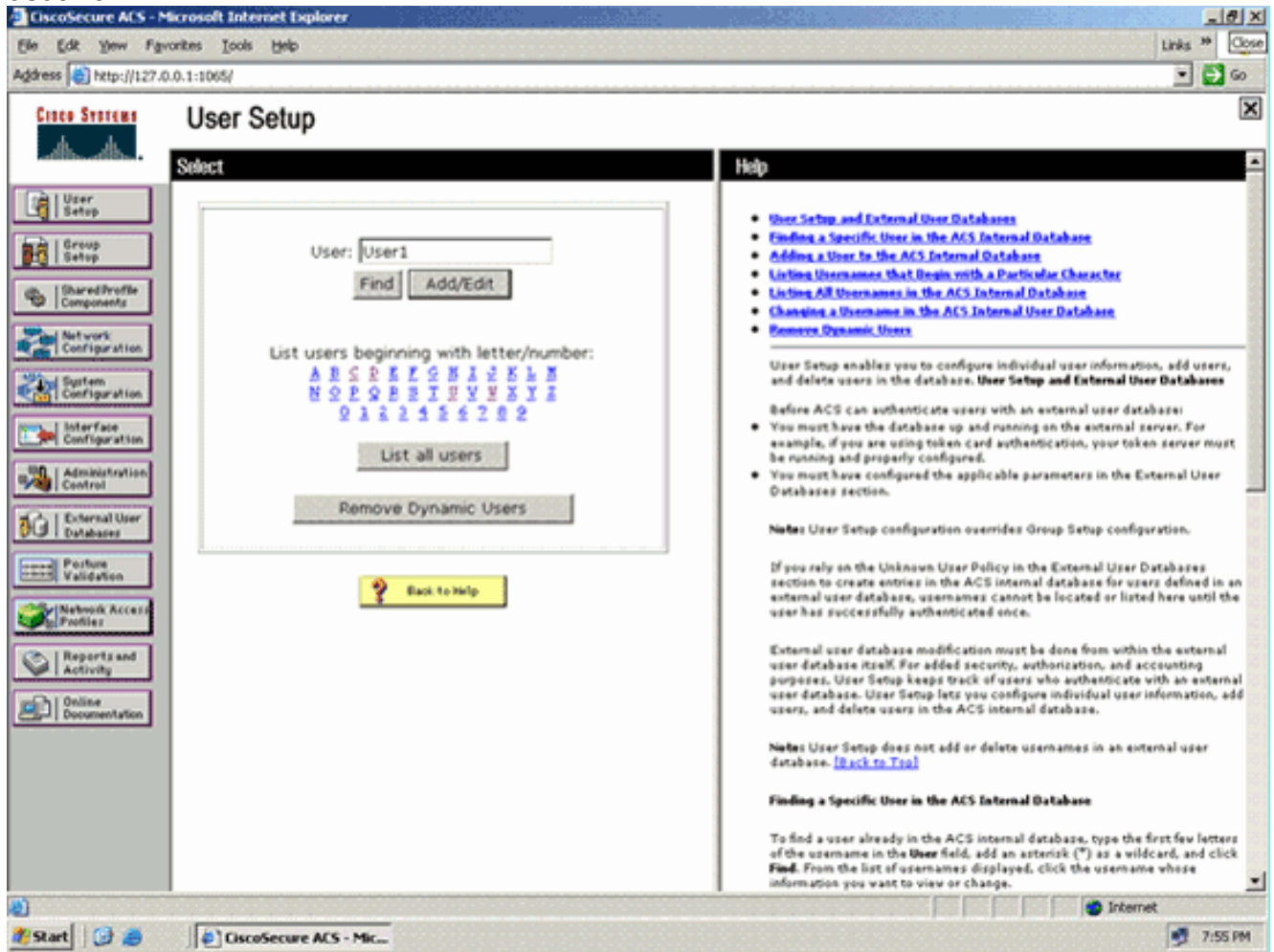
4. Configure el Active/los valores jubilados de TTL de la clave principal (Tiempo para vivir) según lo deseado, o fíjelos al valor predeterminado tal y como se muestra en de este ejemplo. El campo de información ID de la autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar contra quien servidor ACS que se autenticará. El completar este campo es obligatorio. El campo del mensaje de la visualización de la inicial del cliente especifica un mensaje que se enviará a los usuarios que autentican con un cliente del EAP-FAST. El Largo máximo es 40 caracteres. Un usuario verá el mensaje inicial solamente si los soportes de cliente del usuario final la visualización.
5. Si usted quisiera que el ACS realizara el aprovisionamiento anónimo de la en-banda PAC, marque la casilla de verificación **anónima del aprovisionamiento de la en-banda PAC de la permit**.
6. La opción *interna permitida de los métodos* determina que los métodos EAP internos pueden ejecutar dentro del túnel del EAP-FAST TLS. Para el aprovisionamiento anónimo de la en-banda, usted debe habilitar el EAP-GTC y EAP-MS-CHAP para la compatibilidad descendente. Si usted selecciona permita el aprovisionamiento anónimo de la en-banda PAC, usted debe seleccionar EAP-MS-CHAP (fase cero) y EAP-GTC (fase dos).
7. Haga clic en Submit (Enviar). **Nota:** Para la información detallada y los ejemplos sobre cómo configurar el EAP AYUNE con el aprovisionamiento anónimo de la En-banda PAC y el aprovisionamiento autenticado de la En-banda, refiere a la [autenticación del EAP-FAST con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN](#).

Configure la base de datos de usuarios y defina el atributo de RADIUS de la URL-*reorientación*

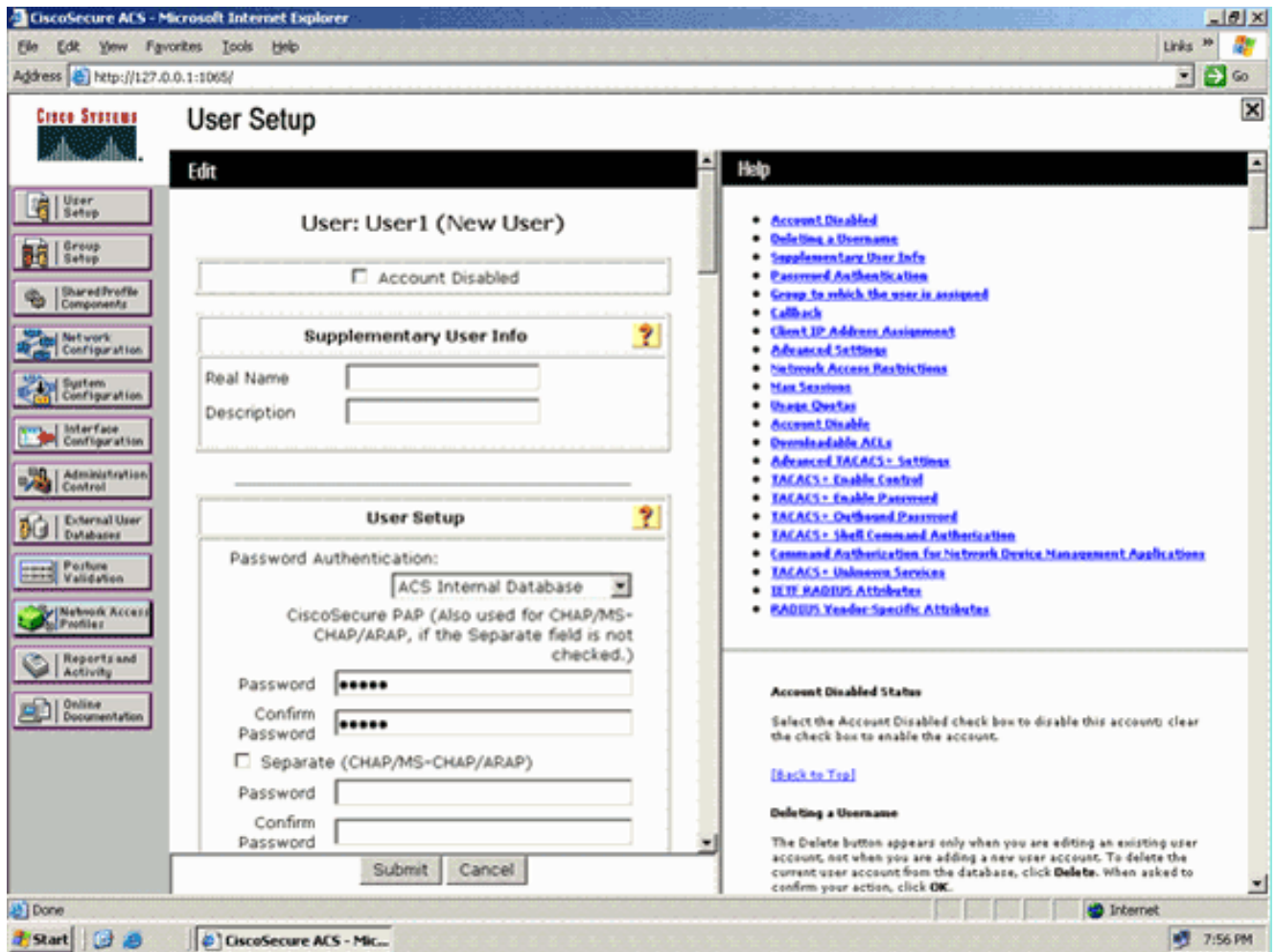
Este ejemplo configura el nombre de usuario y contraseña del cliente de red inalámbrica como el user1 y user1, respectivamente.

Complete estos pasos para crear una base de datos de usuarios:

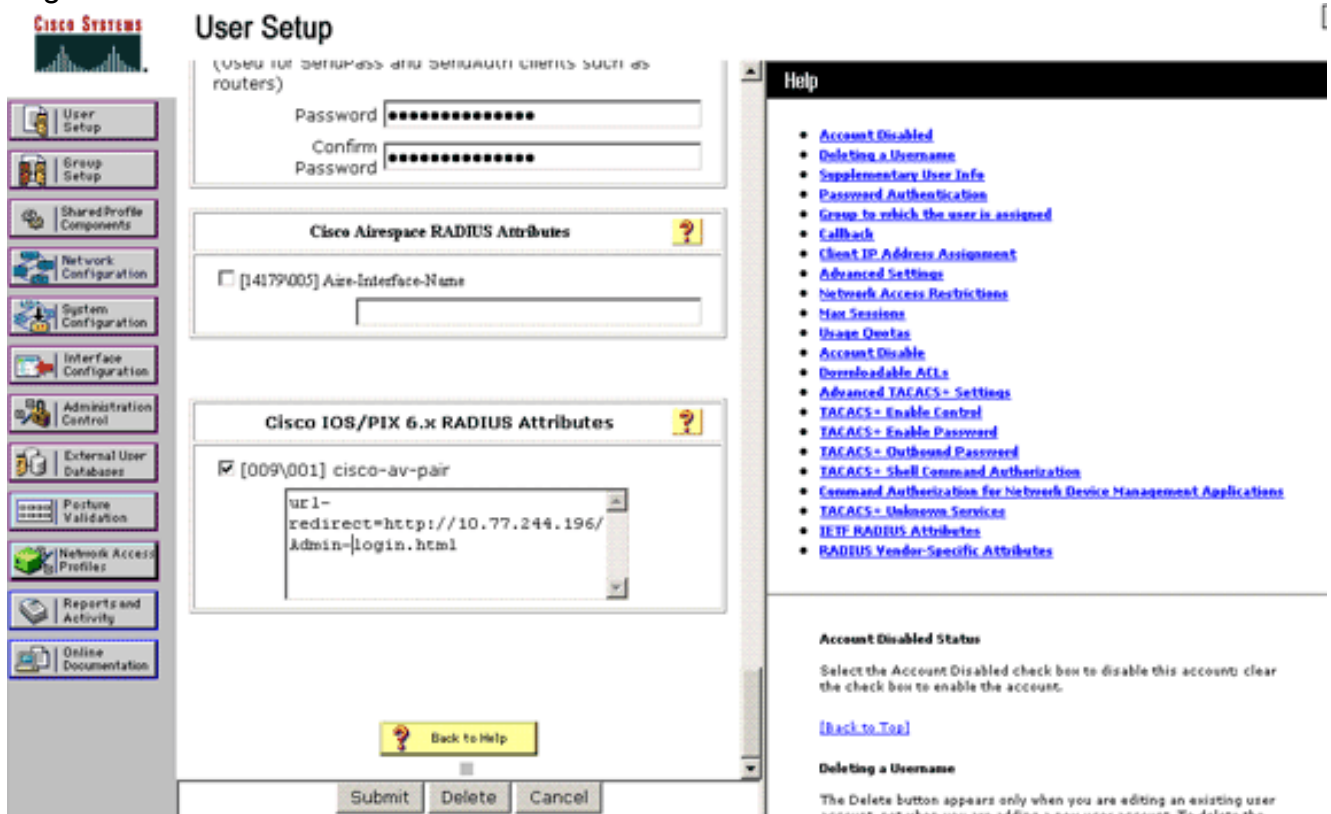
1. Del ACS GUI en la barra de navegación, elija la **configuración de usuario**.
2. Cree una Tecnología inalámbrica del usuario nuevo, y después haga clic **agregar/editar** para ir a la página del editar de este usuario.



3. De la configuración de usuario edite la página, Nombre real y descripción de la configuración, así como las configuraciones de la contraseña, tal y como se muestra en de este ejemplo. Este documento utiliza la base de datos interna ACS para la autenticación de contraseña.



4. Navegue hacia abajo la página para modificar los atributos de RADIUS.
5. Marque la casilla de verificación del Cisco-av-pair [009\001].
6. Ingrese estos cisco av-pair en el recuadro de edición del Cisco-av-pair [009\001] para especificar el URL al cual reorientan al usuario: url-redirect=http://10.77.244.196/Admin-Login.html



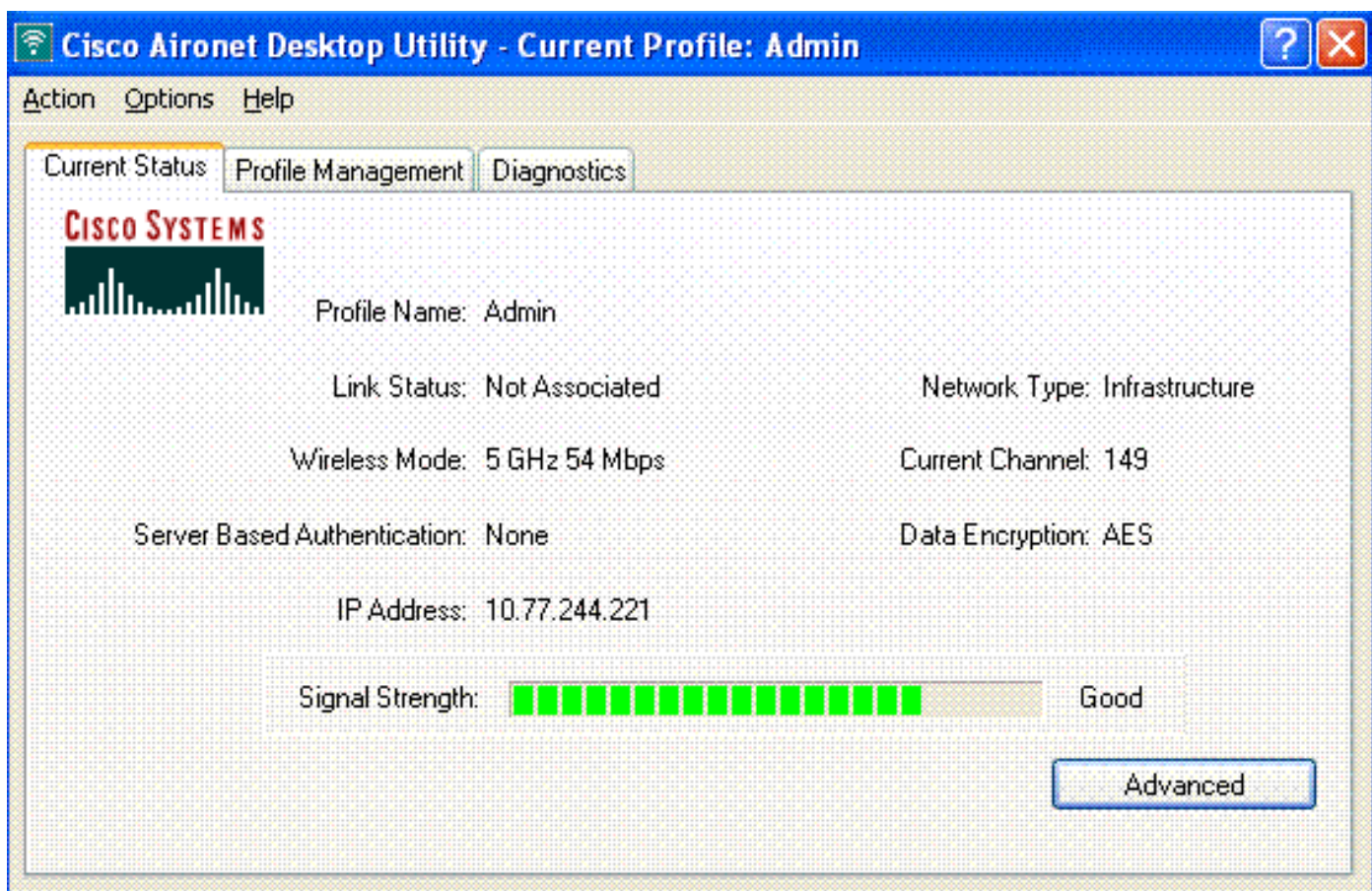
Éste es el Home Page de los usuarios del departamento administrativos.

7. Haga clic en Submit (Enviar).
8. Relance este procedimiento para agregar User2 (usuario del departamento de operaciones).
9. Relance los pasos 1 a 6 para agregar los usuarios de más departamento de los usuarios del departamento administrativos y de operaciones a la base de datos. **Nota:** Los atributos de RADIUS se pueden configurar en el nivel del usuario o el nivel de grupo en el Cisco Secure ACS.

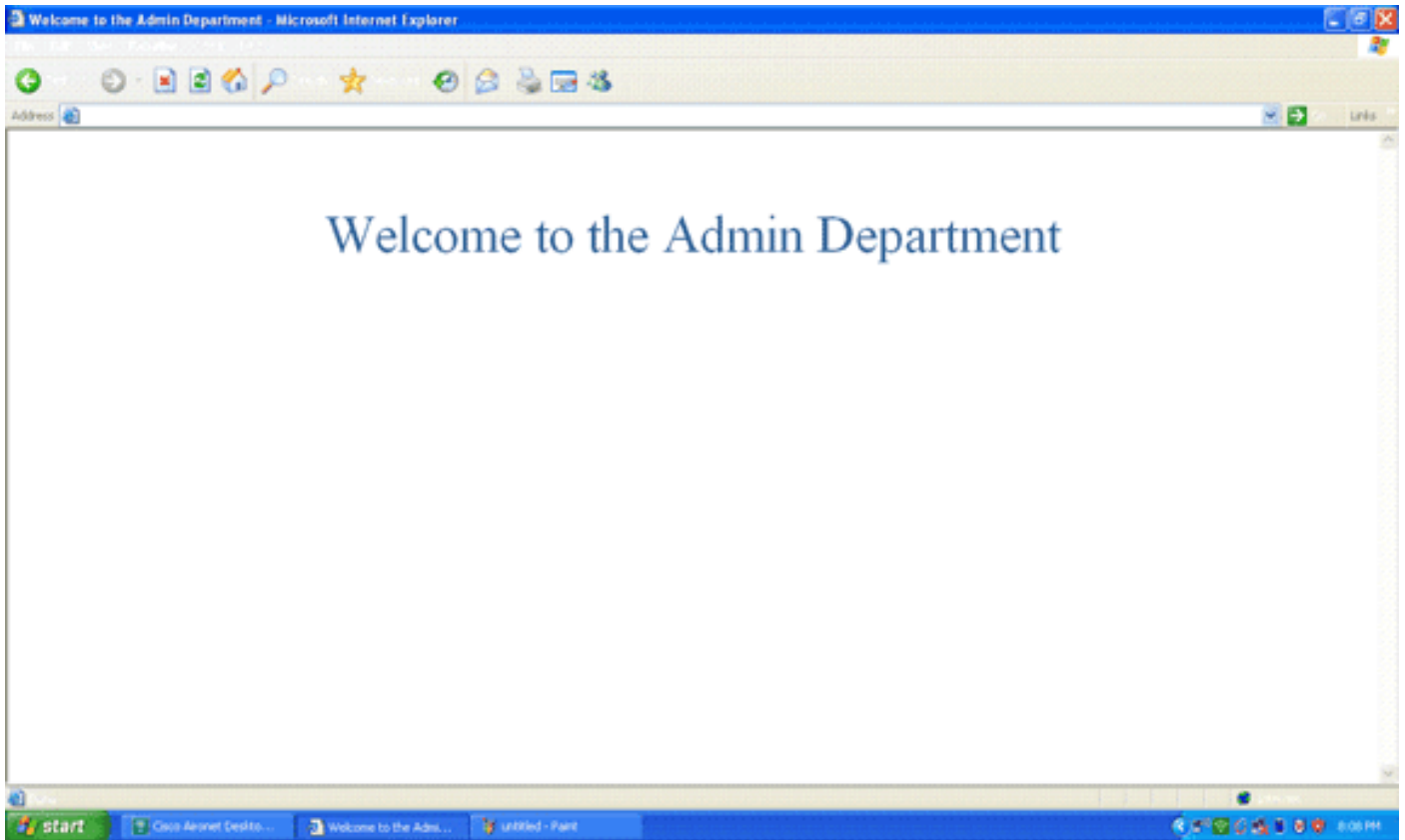
Verificación

Para verificar la configuración, asocie a un cliente de WLAN del departamento de administración y del departamento de operaciones a sus WLAN apropiados.

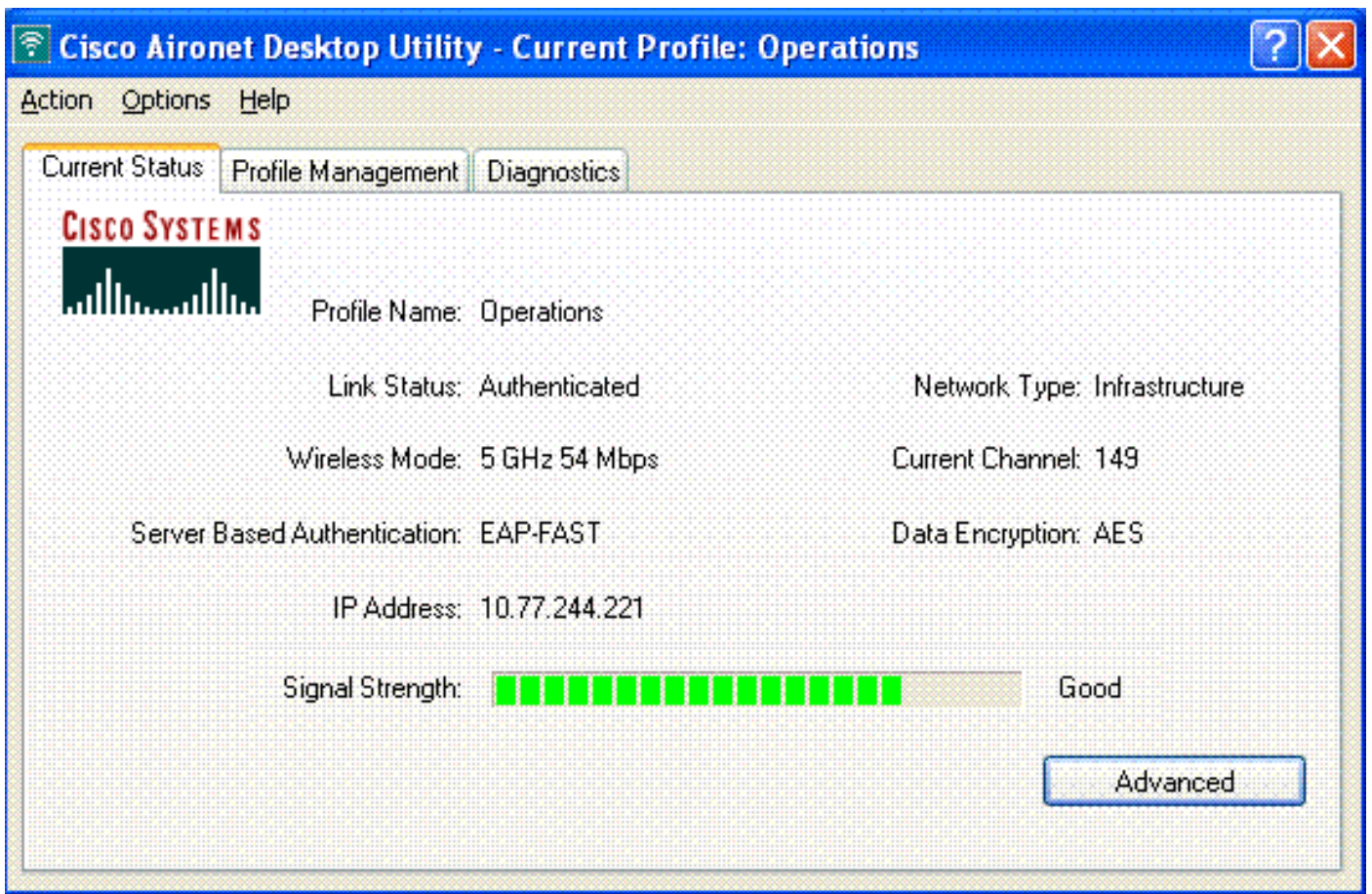
Cuando un usuario del departamento de administración conecta con el Wireless LAN Admin, indican al usuario para las credenciales del 802.1x (credenciales del EAP-FAST en nuestro caso). Una vez que el usuario proporciona las credenciales, el WLC pasa esas credenciales al servidor del Cisco Secure ACS. El servidor del Cisco Secure ACS valida las credenciales del usuario contra la base de datos, y sobre la autenticación satisfactoria, vuelve el atributo de la URL-reorientación al regulador del Wireless LAN. La autenticación es completa en esta etapa.

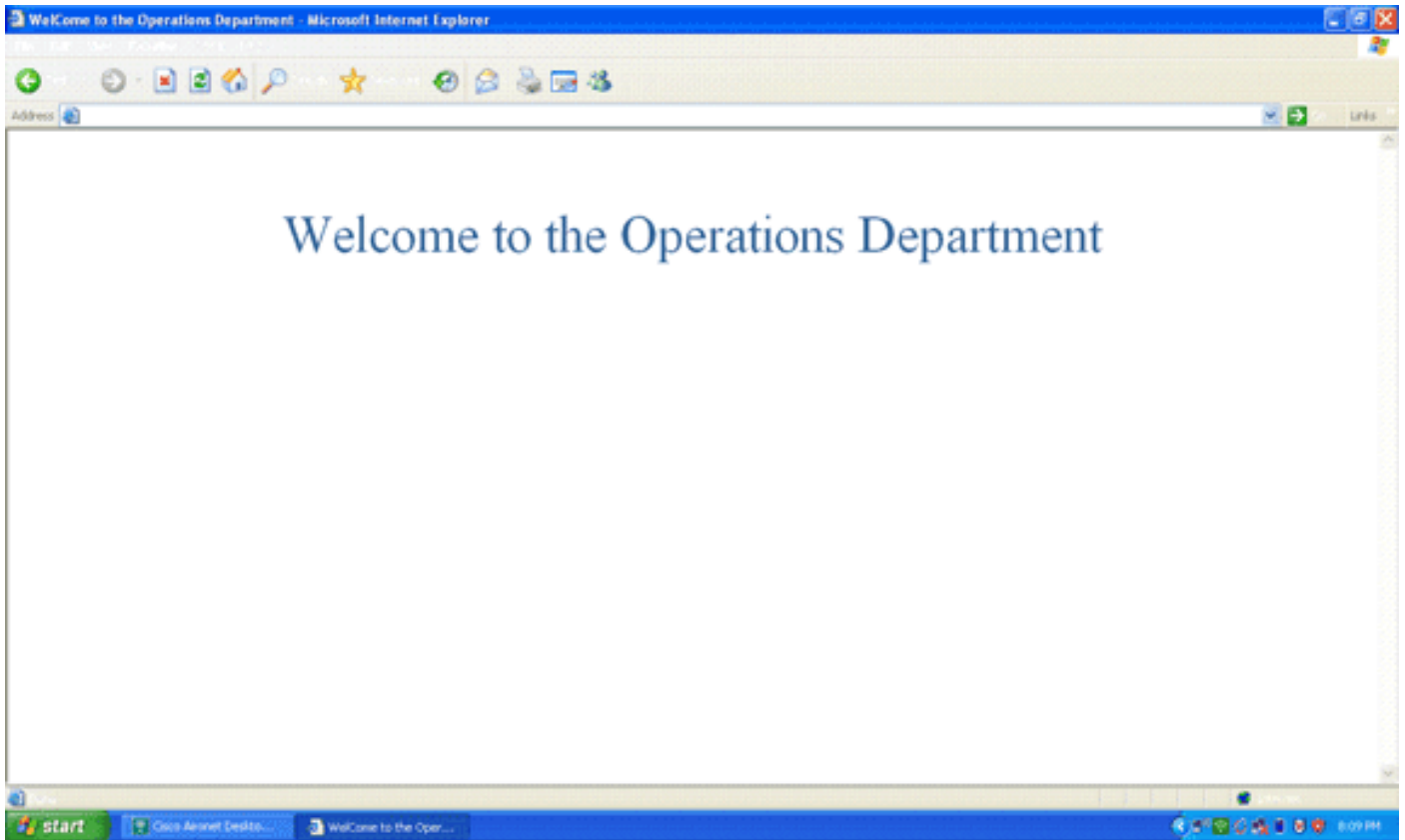


Cuando el usuario abre a un buscador Web, reorientan al usuario al Home Page URL del departamento de administración. (Este URL se vuelve al WLC con el atributo del Cisco-av-pair). Después de que la reorientación, el usuario tenga acceso total a la red. Aquí está el screenshots:



Las mismas Secuencias de eventos ocurren cuando un usuario del departamento de operaciones conecta con las operaciones de la red inalámbrica (WLAN).





Troubleshooting

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

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

Usted puede utilizar los siguientes comandos de resolver problemas su configuración.

- **muestre el wlan_id wlan** — Visualiza el estatus de la red reorientan las características para una red inalámbrica (WLAN) determinada. Aquí tiene un ejemplo:

```
WLAN
Identifier..... 1
Profile Name..... Admin
Network Name (SSID)..... Admin
...
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Enabled
```
- **permiso de los eventos del dot1x del debug** — Habilita el debug de los mensajes de paquete del 802.1x. Aquí tiene un ejemplo:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP
Request from AAA to mobile 00:40:96:ac:dd:05 (EAP Id 16) Fri Feb 29 10:27:16 2008:
00:40:96:ac:dd:05 Received EAPOL EAPPKT from mobile 00:40:96:ac:dd:05 Fri Feb 29 10:27:16
2008: 00:40:96:ac:dd:05 Received EAP Response from mobile 00:40:96:ac:dd:05 (EAP
Type 43) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile
00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to
1800 seconds, got from WLAN config. Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station
00:40:96:ac:dd:05 setting dot1x reauth timeout = 1800 Fri Feb 29 10:27:16 2008:
00:40:96:ac:dd:05 Creating a new PMK Cache Entry for station 00:40:96:ac:dd:05 (RSN 2) Fri
Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf to PMKID cache for
station 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: New PMKID: (16) Fri Feb 29 10:27:16
```



```
2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008:
00:40:96:ac:dd:05 Disabling re-auth since PMK lifetime can take care of same. Fri Feb 29
10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile 00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16) Fri Feb 29 10:27:16 2008: [0000] 79 ee
88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05
Sending EAPOL-Key Message to mobile 00:40:96:ac:dd:05 state INITPMK (message 1), replay
counter 00.00.00.00.00.00.00.00 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth
Success while in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **permiso de los eventos aaa del debug** — Habilita la salida de los debugs de todos los eventos

```
aaa.Aquí tiene un ejemplo:Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful
transmission of Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
00:40:96:ac:dd:05-00:00 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages:
response code=11 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from RADIUS server
10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3 Thu Feb 28 07:55:18 2008:
00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 104) to
10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00 Thu Feb 28 07:55:18 2008: ****Enter
processIncomingMessages: response code=2 Thu Feb 28 07:55:18 2008: ****Enter
processRadiusResponse: response code=2 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-
Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
'http://10.77.244.196/Admin-login.html' set Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05
Applying new AAA override for station 00:40:96:ac:dd:05 Thu Feb 28 07:55:18 2008:
00:40:96:ac:dd:05 Override values for station 00:40:96:ac:dd:05 source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1,
rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: '
```

[Información Relacionada](#)

- [Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 5.0](#)
- [Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN](#)
- [Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)