

# Ejemplo de Configuración de Wireless LAN Controller Splash Page Redirect

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configuración de la red](#)

[Configurar](#)

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

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

[Paso 3. Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida.](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## [Introducción](#)

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

## [Prerequisites](#)

## [Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de las soluciones de seguridad LWAPP
- Conocimiento de cómo configurar Cisco Secure ACS

## [Componentes Utilizados](#)

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

- Controlador de LAN inalámbrica (WLC) de Cisco serie 4400 que ejecuta la versión 5.0 del firmware
- Punto de acceso ligero (LAP) Cisco serie 1232
- Cisco Aironet 802.a/b/g Wireless Client Adapter que ejecuta la versión 4.1 del firmware
- Servidor Cisco Secure ACS que ejecuta la versión 4.1
- Cualquier servidor web externo de terceros

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 Cisco para obtener más información sobre las convenciones del documento.](#)

## Antecedentes

La redirección web de la página de bienvenida es una función introducida con Wireless LAN Controller versión 5.0. Con esta función, el usuario es redirigido a una página web determinada después de que se haya completado la autenticación 802.1x. La redirección se produce cuando el usuario abre un navegador (configurado con una página de inicio predeterminada) o intenta acceder a una URL. Una vez completada la redirección a la página web, el usuario tiene acceso completo a la red.

Puede especificar la página de redirección en el servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). El servidor RADIUS debe configurarse para devolver el atributo RADIUS de redirección URL de par AV de Cisco al controlador de LAN inalámbrica tras una autenticación 802.1x correcta.

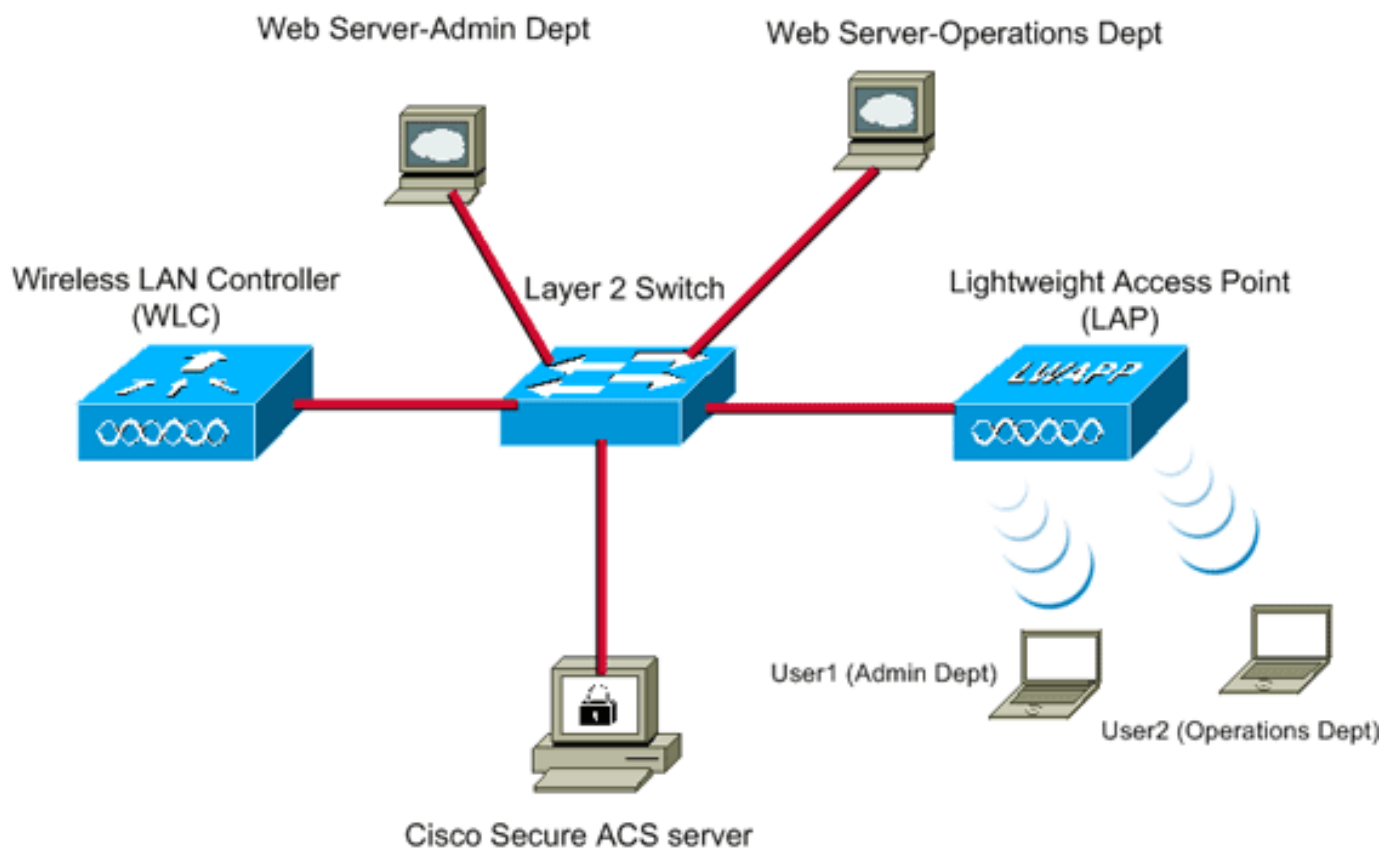
La función de redireccionamiento web de la página de bienvenida solo está disponible para las WLAN configuradas para la seguridad 802.1x o WPA/WPA2 de capa 2.

## Configuración de la red

En este ejemplo, un Cisco 4404 WLC y un Cisco 1232 Series LAP se conectan a través de un switch de capa 2. El servidor Cisco Secure ACS (que actúa como servidor RADIUS externo) también está conectado al mismo switch. Todos los dispositivos están en la misma subred.

El LAP se registra inicialmente en el controlador. Debe crear dos WLAN: una para los usuarios del **Departamento de Administración** y otra para los usuarios del **Departamento de Operaciones**. Ambas redes LAN inalámbricas utilizan WPA2/ AES (EAP-FAST se utiliza para la autenticación). Ambas WLAN utilizan la función Splash Page Redirect para redirigir a los usuarios a las URL de la página de inicio adecuada (en 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

En la siguiente sección se 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](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

Complete estos pasos para configurar los dispositivos para utilizar la función de redirección de página de bienvenida:

1. [Configure el WLC para la autenticación RADIUS a través del servidor ACS seguro de Cisco.](#)
2. [Configure las WLAN para los departamentos de administración y operaciones.](#)
3. [Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida.](#)

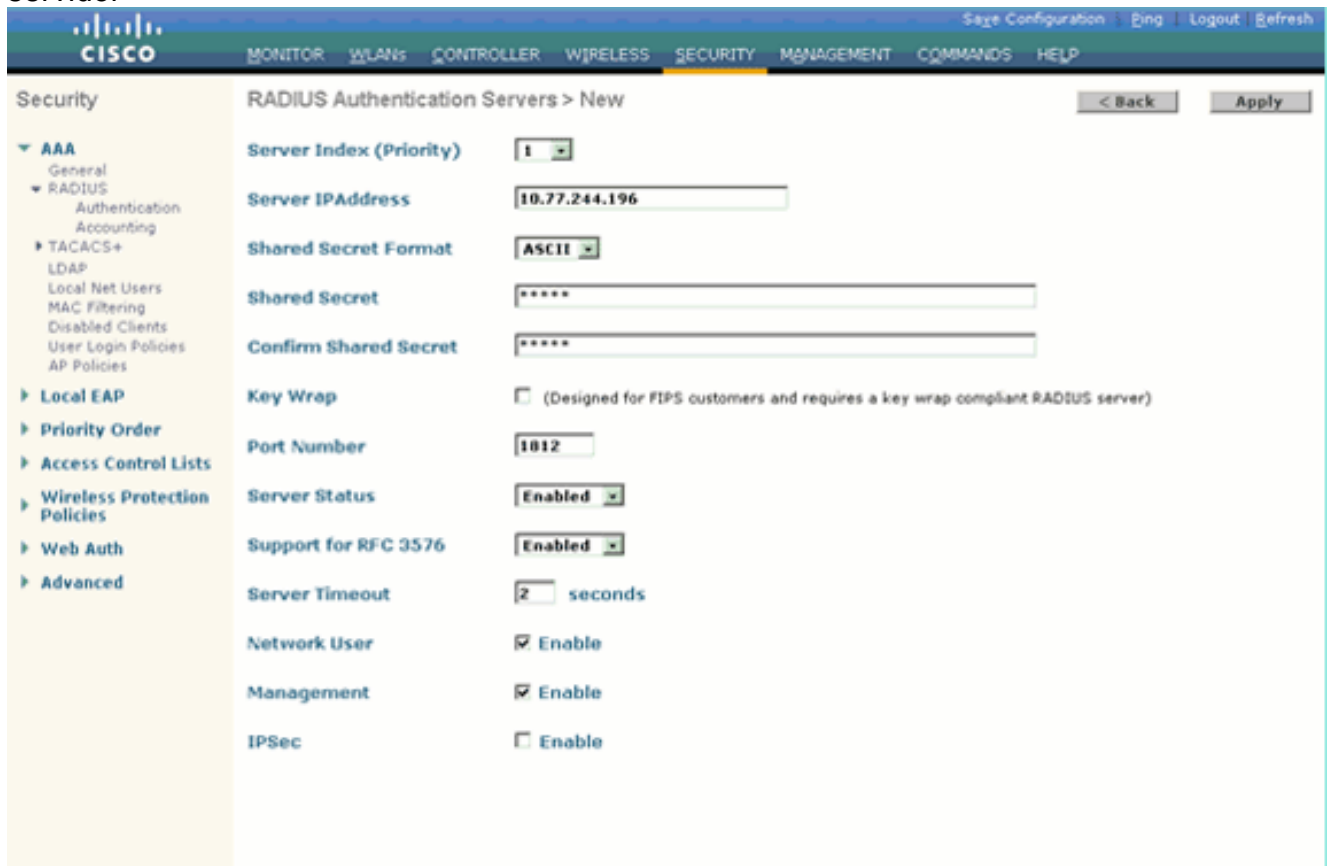
### Paso 1. Configure el WLC para la autenticación RADIUS a través del servidor ACS

## [seguro de Cisco.](#)

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo.

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

1. Elija **Security** y **RADIUS Authentication** de la GUI del controlador para mostrar la página RADIUS Authentication Servers.
2. Haga clic en **Nuevo** para definir un servidor RADIUS.
3. 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



The screenshot shows the Cisco WLC GUI configuration page for RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The left sidebar shows the navigation menu with "Security" selected. The main content area 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 el servidor ACS con una dirección IP de 10.77.244.196.

4. Haga clic en Apply (Aplicar).

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

En este paso, configure las dos WLAN (una para el departamento de administración y otra para el departamento de operaciones) que los clientes utilizarán para conectarse a la red inalámbrica.

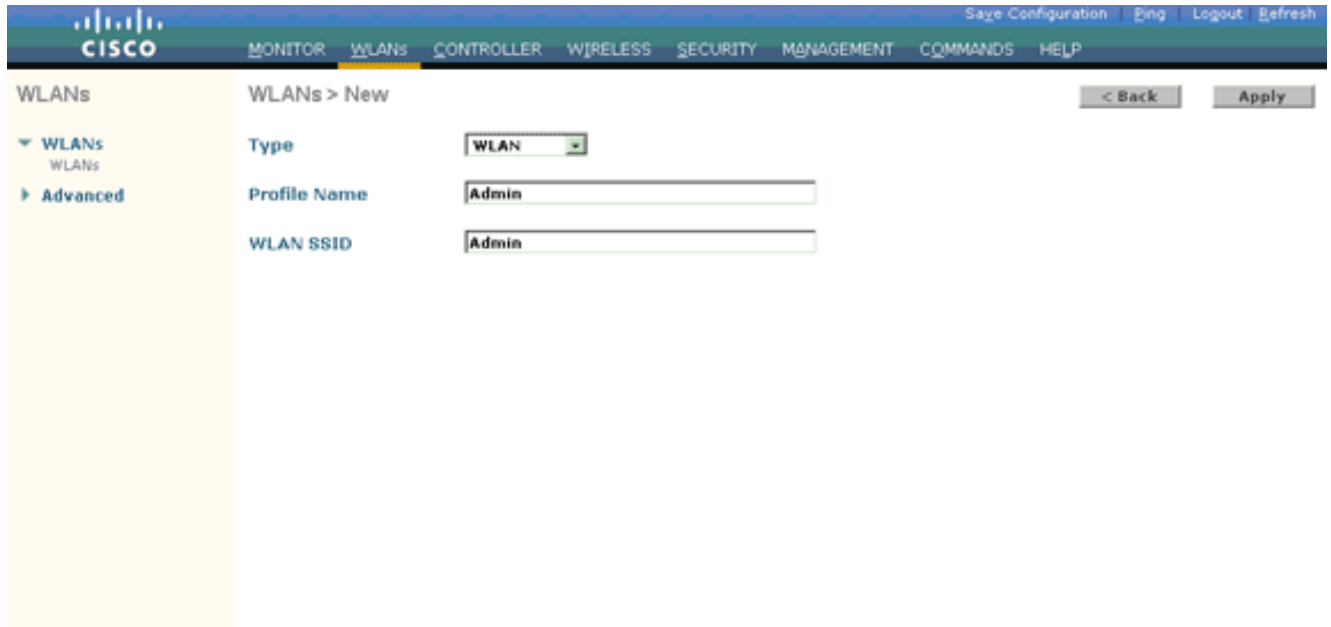
El SSID de WLAN para el departamento de administración será *Admin*. El SSID de WLAN para el departamento de operaciones será *Operations* (Operaciones).

Utilice la autenticación EAP-FAST para habilitar WPA2 como el mecanismo de seguridad de la capa 2 en ambas WLAN y la función de política web - Splash Page Web Redirect como el método

de seguridad de la capa 3.

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.

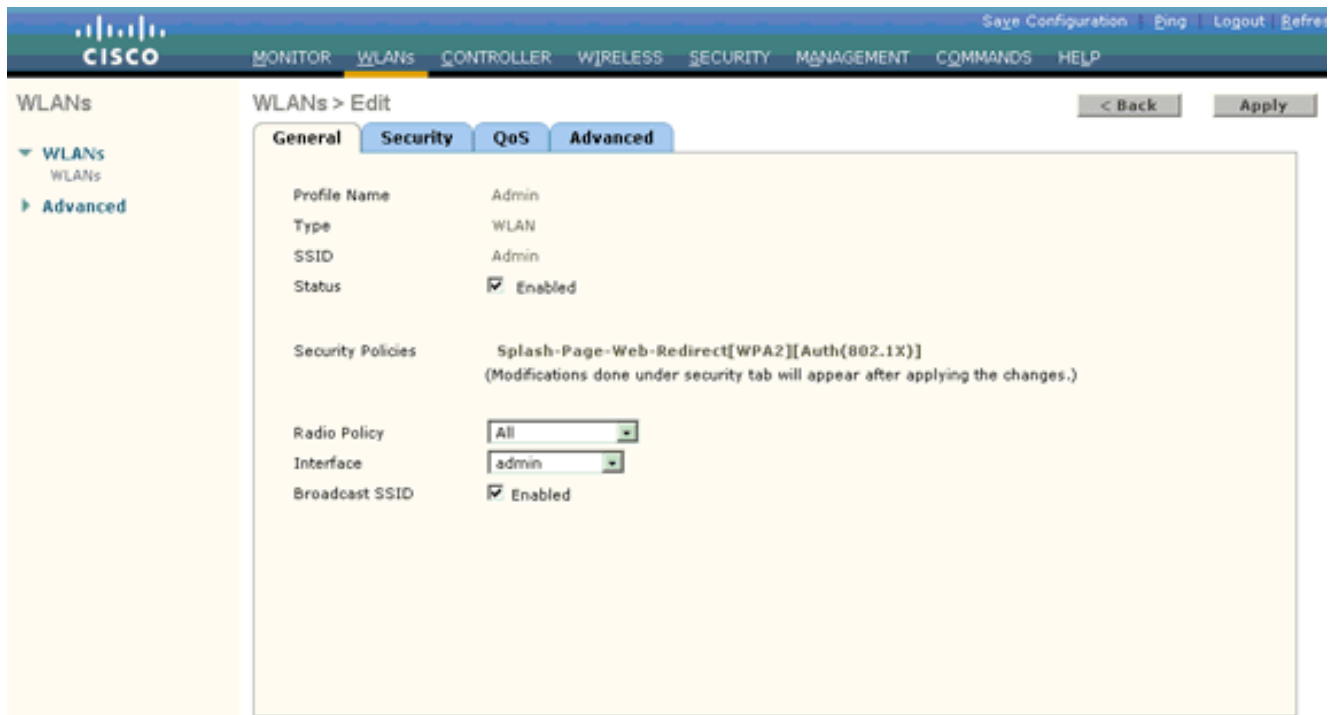


The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs' section is expanded, showing 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

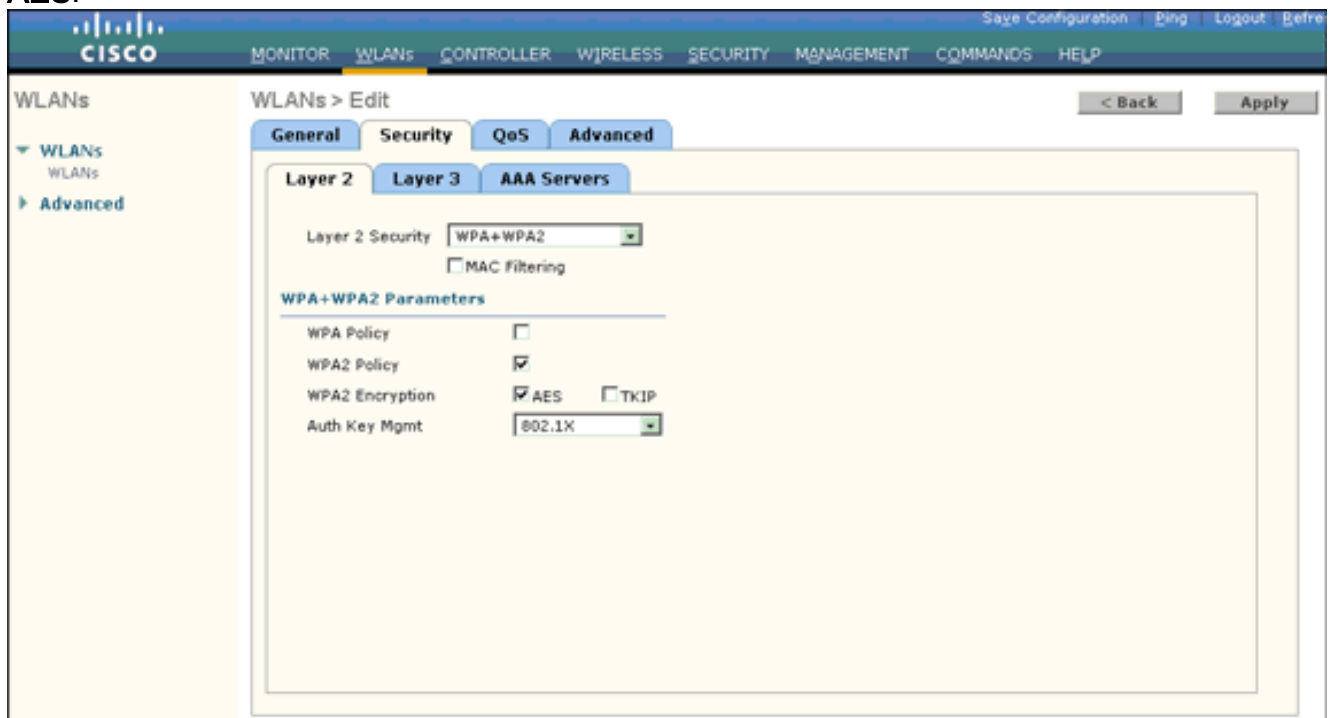
Type	WLAN
Profile Name	Admin
WLAN SSID	Admin

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

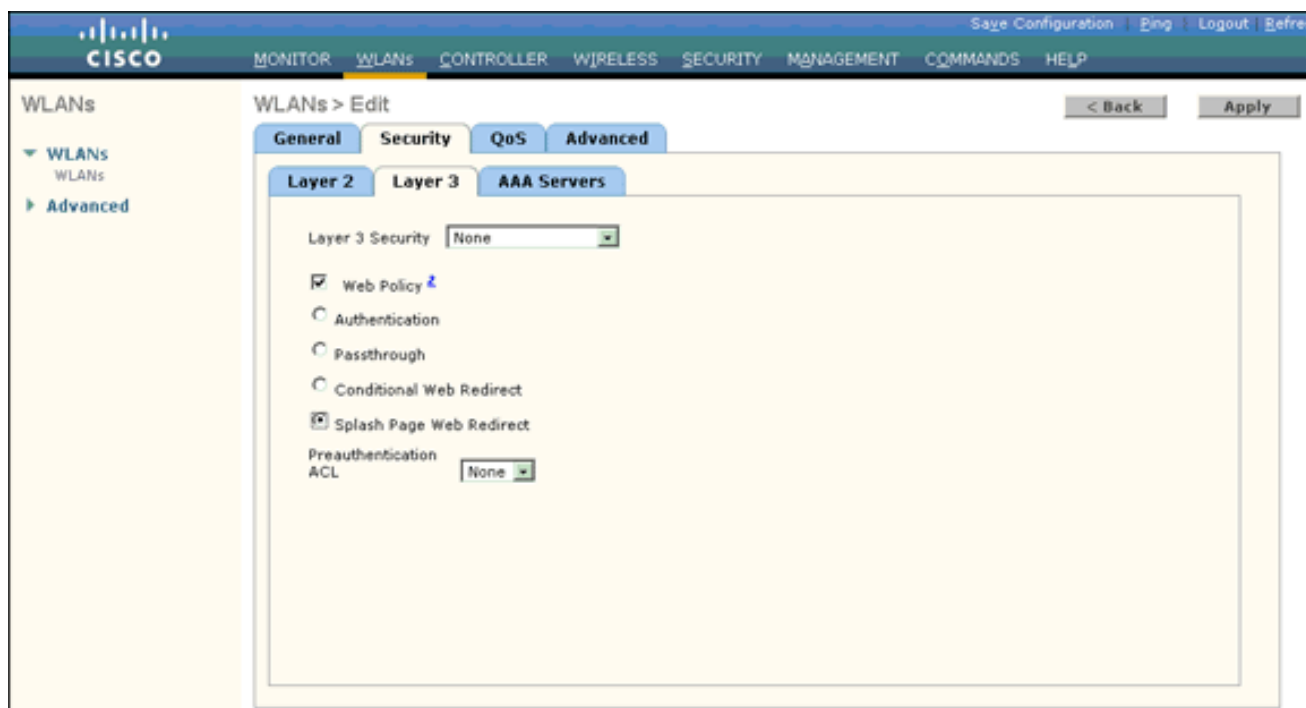
3. Introduzca el nombre SSID de WLAN y el nombre de perfil en la página WLAN > New (WLAN > Nuevo).
4. Haga clic en Apply (Aplicar).
5. En primer lugar, crearemos la WLAN para el departamento de administración. Una vez creada una nueva WLAN, aparece la página WLAN > Edit (WLAN > Editar) para la nueva 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.
6. En Políticas generales, marque la casilla de verificación **Status** para habilitar la WLAN.



7. Haga clic en la pestaña **Seguridad** y, a continuación, haga clic en la pestaña **Capa 2**.
8. Elija **WPA+WPA2** en la lista desplegable Layer 2 Security. Este paso activa la autenticación WPA para la WLAN.
9. En Parámetros WPA+WPA2, active las casillas de verificación **Política WPA2** y **Cifrado AES**.



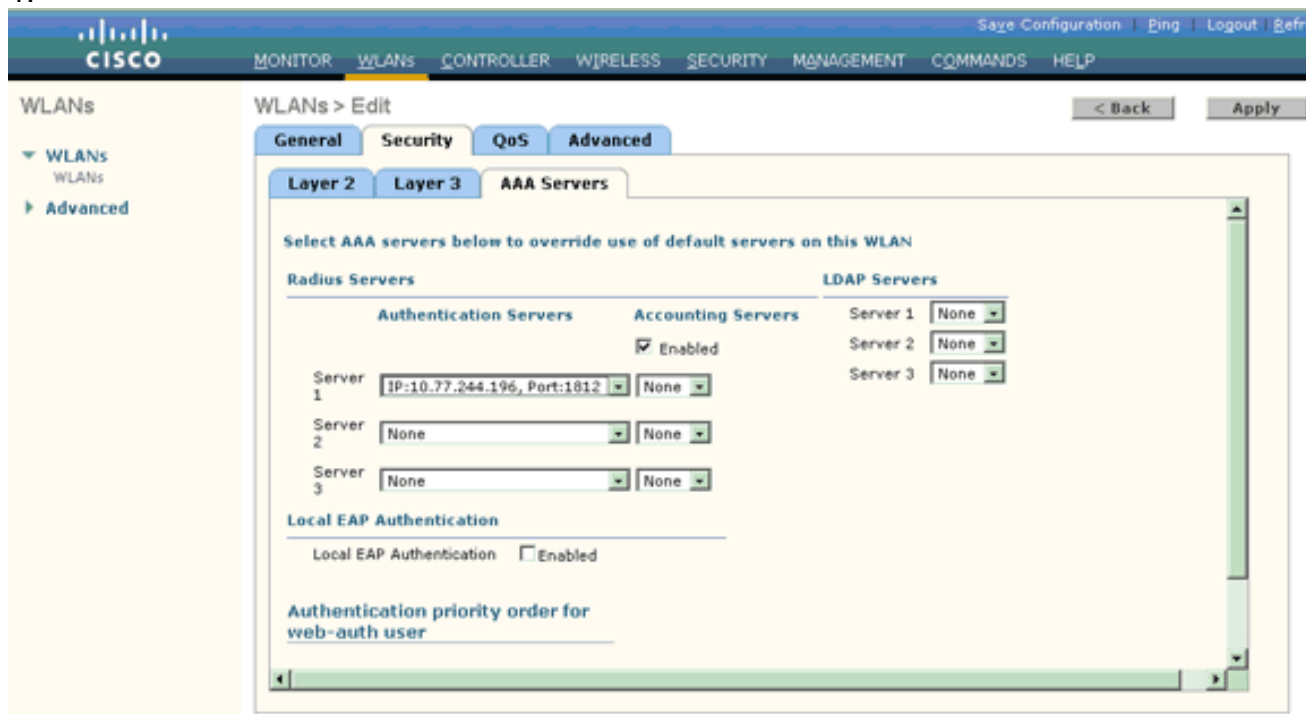
10. Elija **802.1x** en la lista desplegable Auth Key Mgmt. Esta opción habilita WPA2 con autenticación 802.1x/EAP y cifrado AES para la WLAN.
11. Haga clic en la pestaña **Layer 3 Security**.
12. Active la casilla **Web Policy** y, a continuación, haga clic en el botón de opción **Splash Page Web Redirect**. Esta opción activa la función de redireccionamiento web de la página de bienvenida.



13. Haga clic en la pestaña **AAA Servers**.

14. En Servidores de autenticación, elija la dirección IP del servidor correspondiente en la lista desplegable Servidor

1.



En este ejemplo, 10.77.244.196 se utiliza como servidor RADIUS.

15. Haga clic en Apply (Aplicar).

16. Repita los pasos del 2 al 15 para crear la WLAN para el departamento de operaciones. La página WLANs (WLANs) muestra las dos WLANs que ha creado.

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
<a href="#">Admin</a>	WLAN	Admin	Enabled	[WPA2][Auth(802.1X)], Splash-Page
<a href="#">Operations</a>	WLAN	Operations	Enabled	[WPA2][Auth(802.1X)], Splash-Page

Observe que las políticas de seguridad incluyen la redirección de la página de bienvenida.

### [Paso 3. Configure Cisco Secure ACS para que admita la función de redirección de páginas de bienvenida.](#)

El siguiente paso es configurar el servidor RADIUS para esta función. El servidor RADIUS necesita realizar una autenticación EAP-FAST para validar las credenciales del cliente y, tras una autenticación exitosa, redirigir al usuario a la URL (en el servidor web externo) especificada en el atributo RADIUS *url-redirect* de par AV de Cisco.

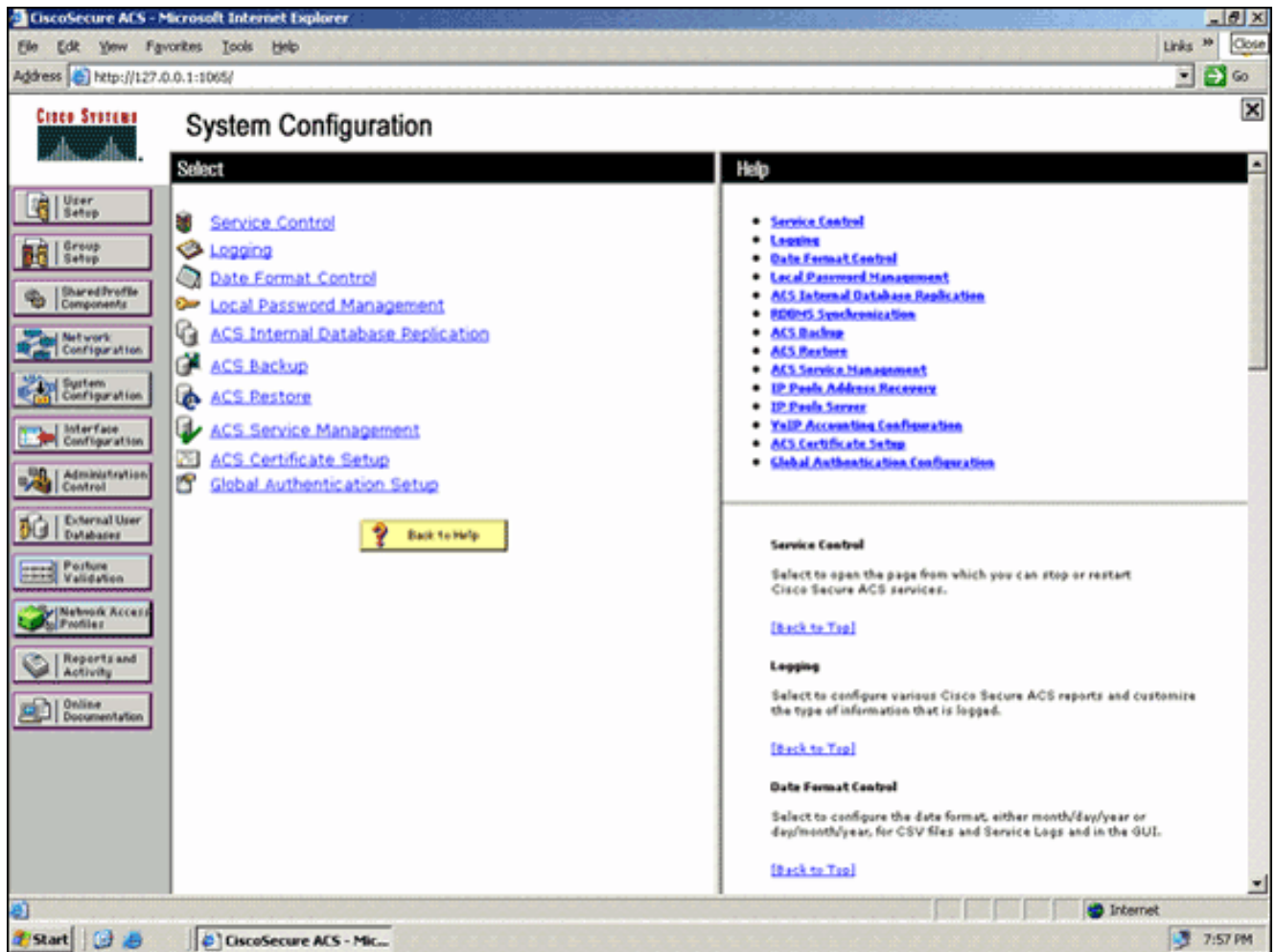
#### **Configuración de Cisco Secure ACS para la autenticación EAP-FAST**

**Nota:** Este documento asume que el controlador de LAN inalámbrica se agrega a Cisco Secure ACS como cliente AAA.

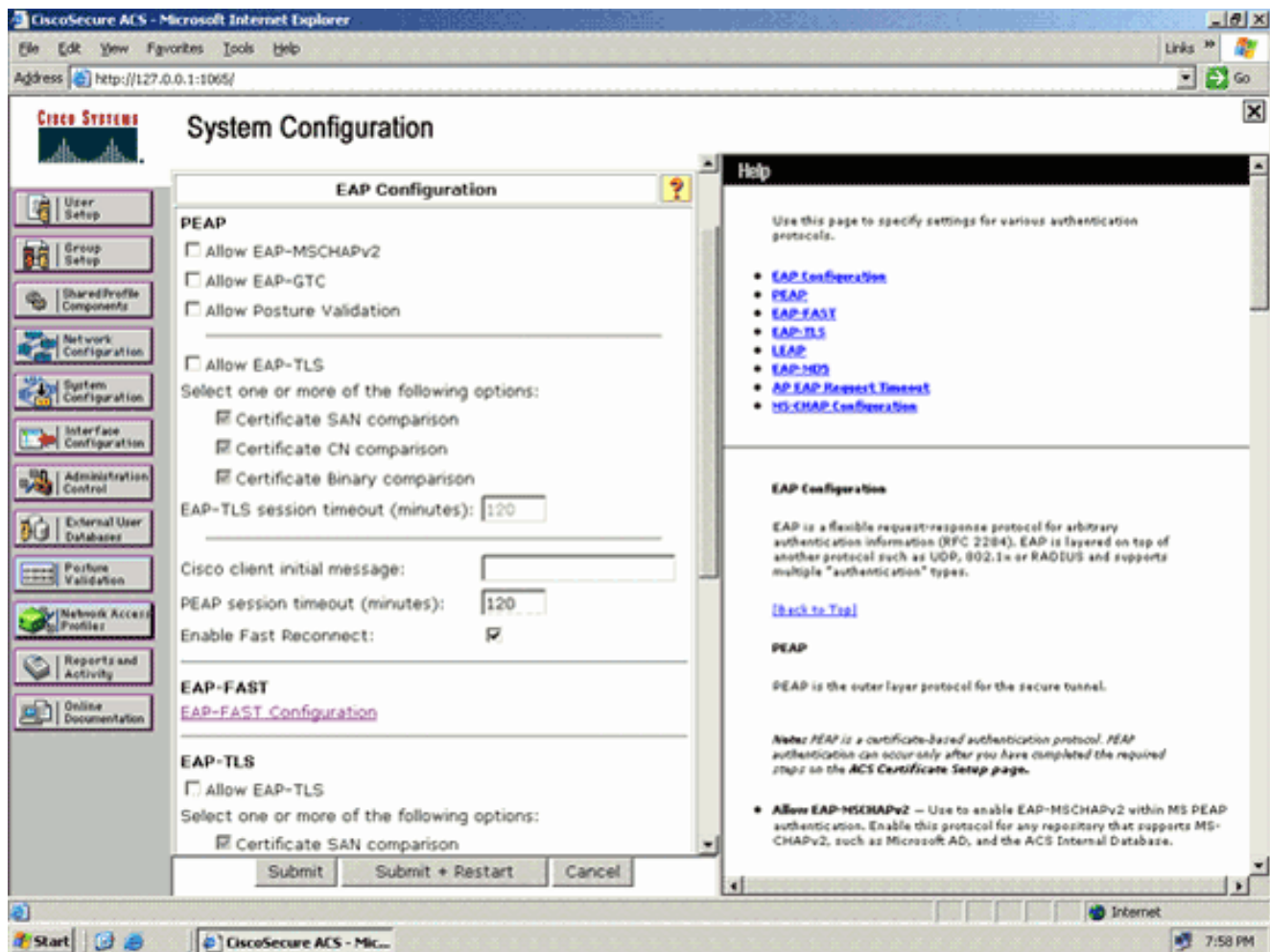
Complete estos pasos para configurar la autenticación EAP-FAST en el servidor RADIUS:

1. Haga clic en **Configuración del Sistema** de la GUI del servidor RADIUS y luego elija **Configuración de Autenticación Global** en la página Configuración del Sistema.

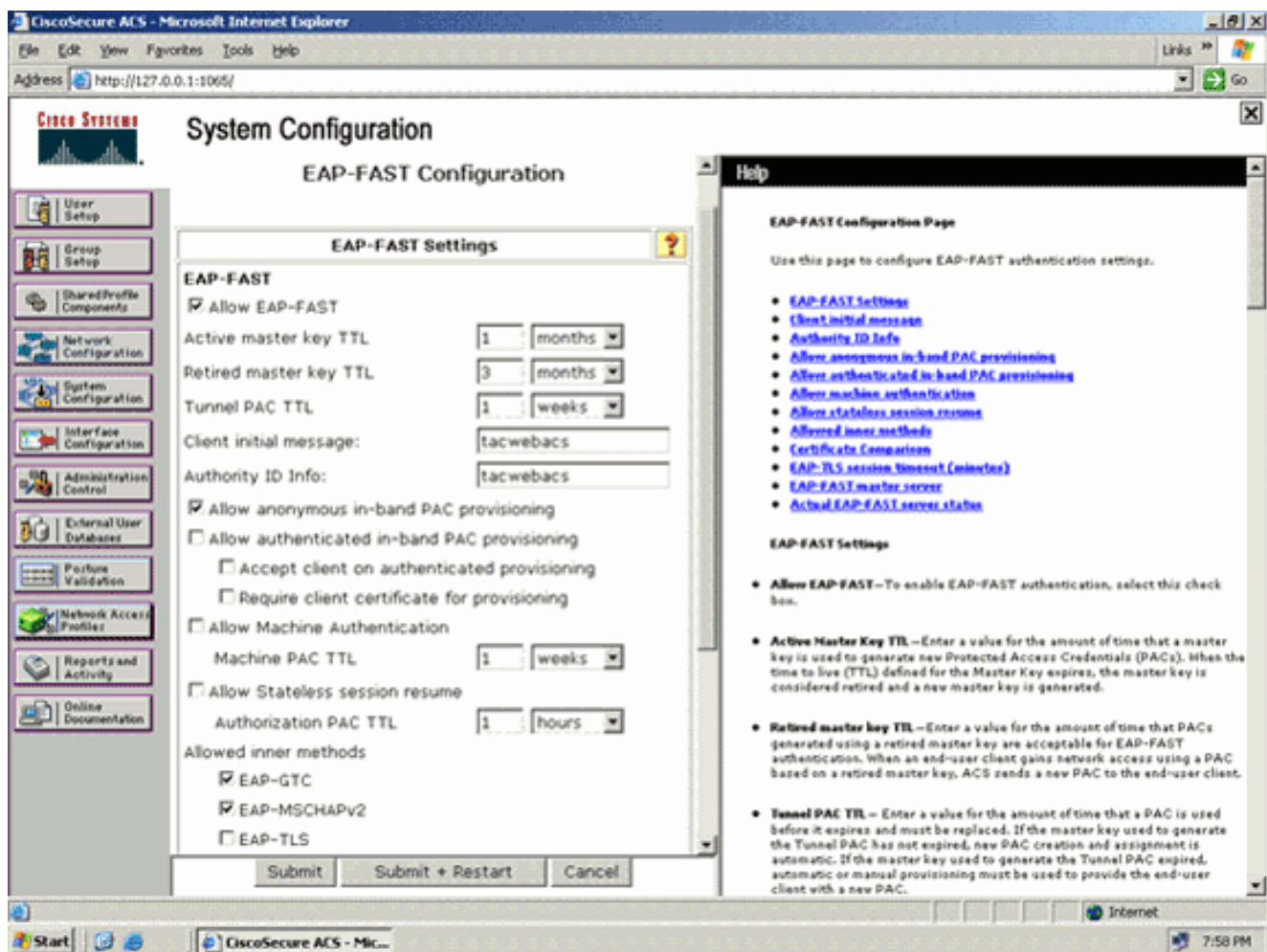




2. Desde la página de configuración de Autenticación Global, haga clic en **Configuración EAP-FAST** para ir a la página de configuración de EAP-FAST.



3. Desde la página EAP-FAST Settings, marque la casilla de verificación **Allow EAP-FAST** para habilitar EAP-FAST en el servidor RADIUS.



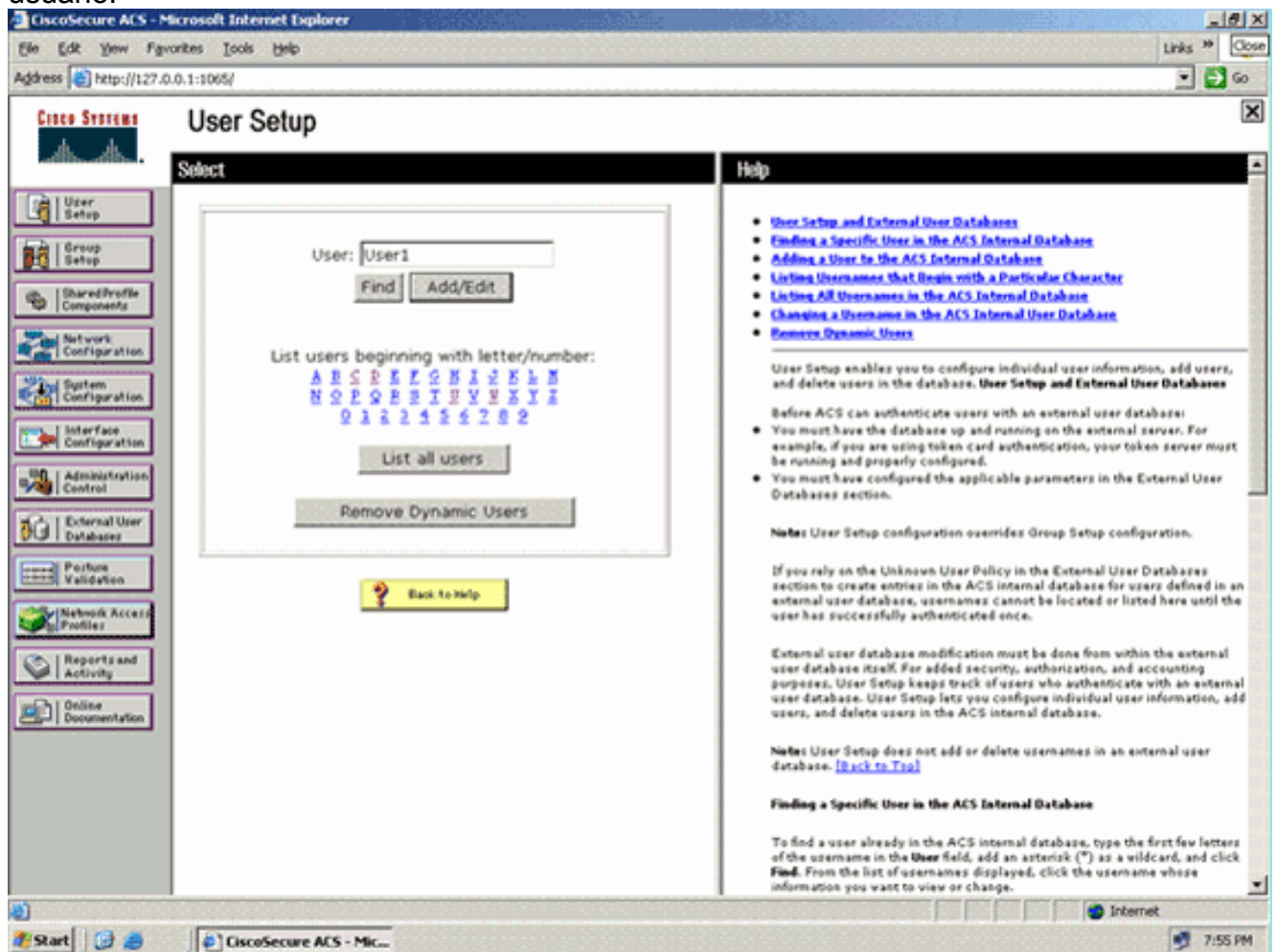
4. Configure los valores TTL (Time-to-Live) de clave maestra activa/retirada como desee o establézcalos en el valor predeterminado, como se muestra en este ejemplo. El campo Información de ID de autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar 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 autentican 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.
5. 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**.
6. La opción *Allowed inner methods* determina qué métodos EAP internos pueden ejecutarse 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).
7. Haga clic en Submit (Enviar). **Nota:** Para obtener información detallada y ejemplos sobre cómo configurar EAP-FAST con aprovisionamiento de PAC en banda anónimo y aprovisionamiento en banda autenticado, consulte [Ejemplo de Configuración de EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo](#).

### Configure la base de datos User y defina el atributo *url-redirect* RADIUS

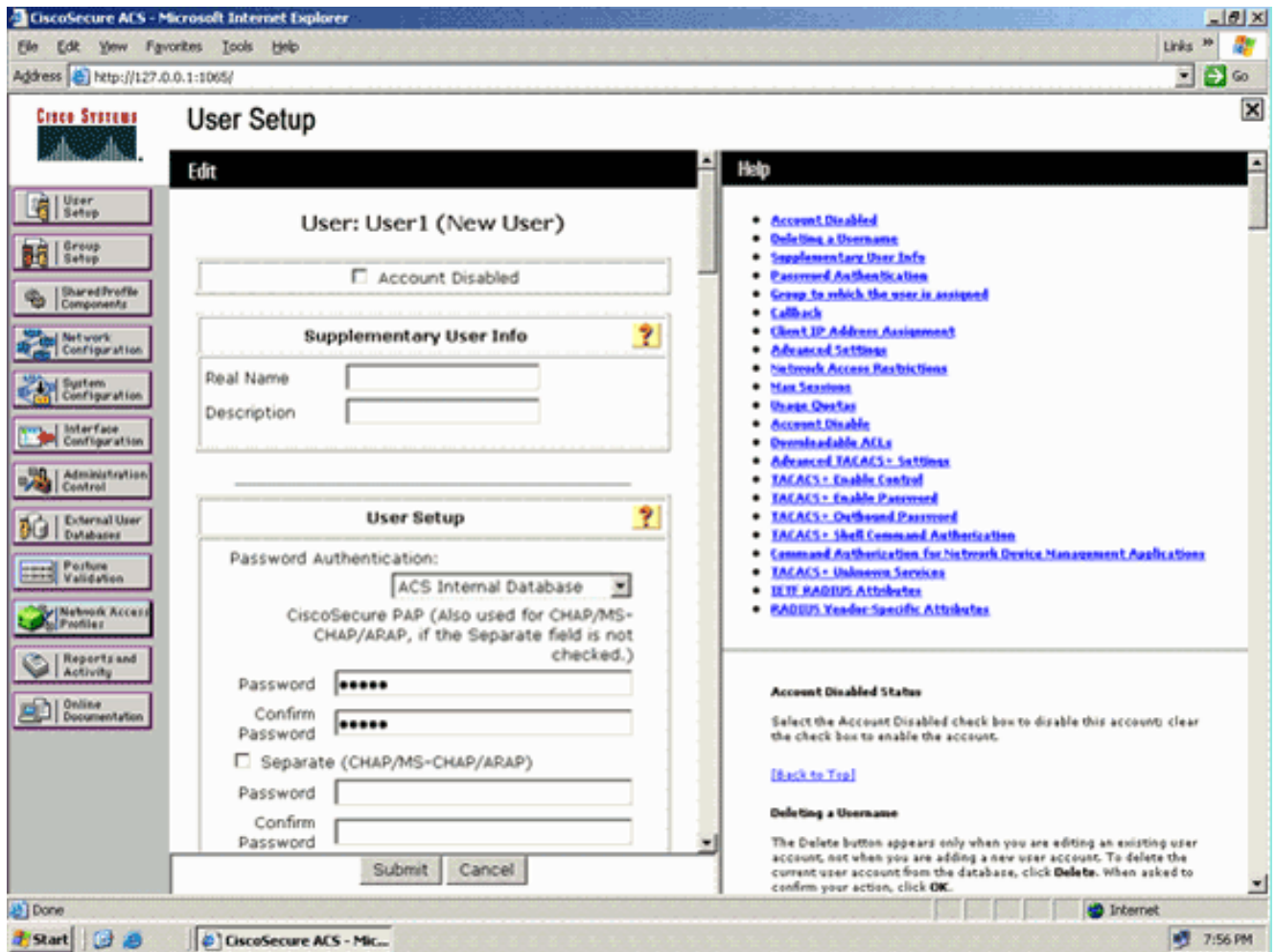
Este ejemplo configura el nombre de usuario y la contraseña del cliente inalámbrico como Usuario1 y Usuario1, respectivamente.

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

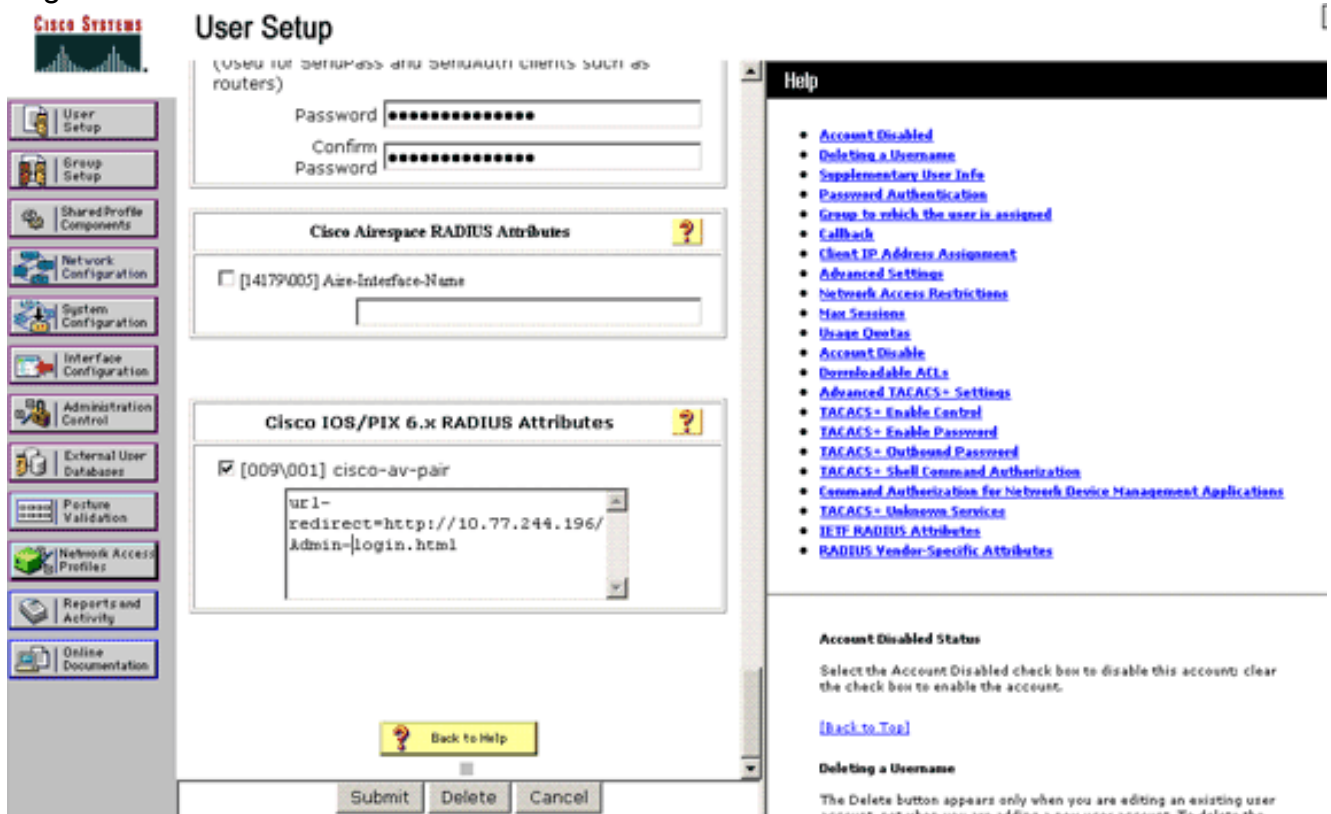
1. En la GUI de ACS en la barra de navegación, elija **User Setup**.
2. Cree un nuevo usuario inalámbrico, y luego haga clic en **Add/Edit** para ir a la página Edit de este usuario.



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



4. Desplácese hacia abajo en la página para modificar los atributos RADIUS.
5. Marque la casilla de verificación [009\001] cisco-av-pair.
6. Ingrese estos pares AV de Cisco en el cuadro de edición [009\001] cisco-av-pair para especificar la URL a la que se redirige al usuario: url-redirect=http://10.77.244.196/Admin-Login.html



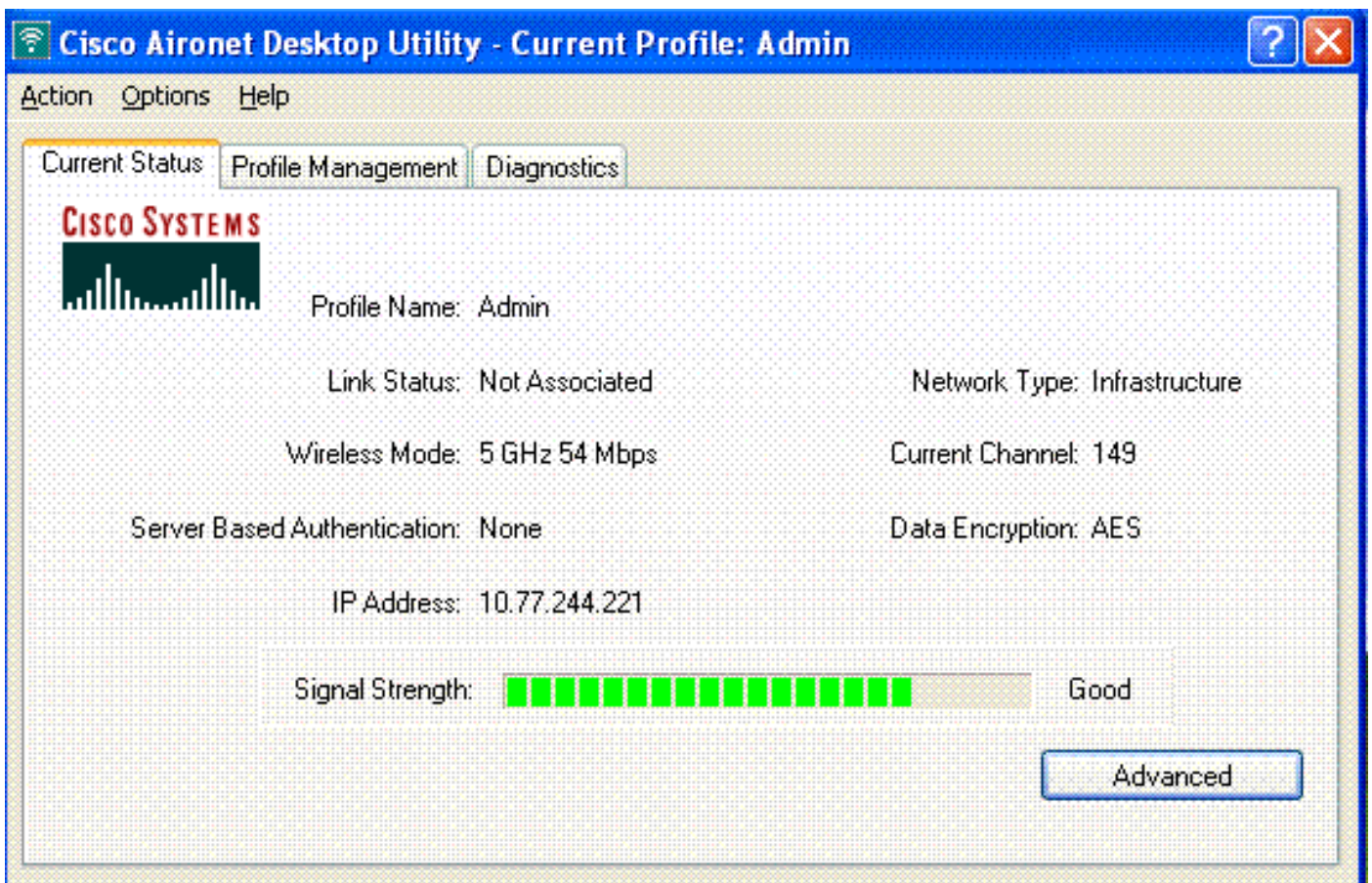
Esta es la página de inicio de los usuarios del departamento de administración.

7. Haga clic en Submit (Enviar).
8. Repita este procedimiento para agregar el usuario 2 (usuario del departamento de operaciones).
9. Repita los pasos del 1 al 6 para agregar más usuarios del departamento de administración y del departamento de operaciones a la base de datos. **Nota:** Los atributos RADIUS se pueden configurar en el nivel de usuario o de grupo en Cisco Secure ACS.

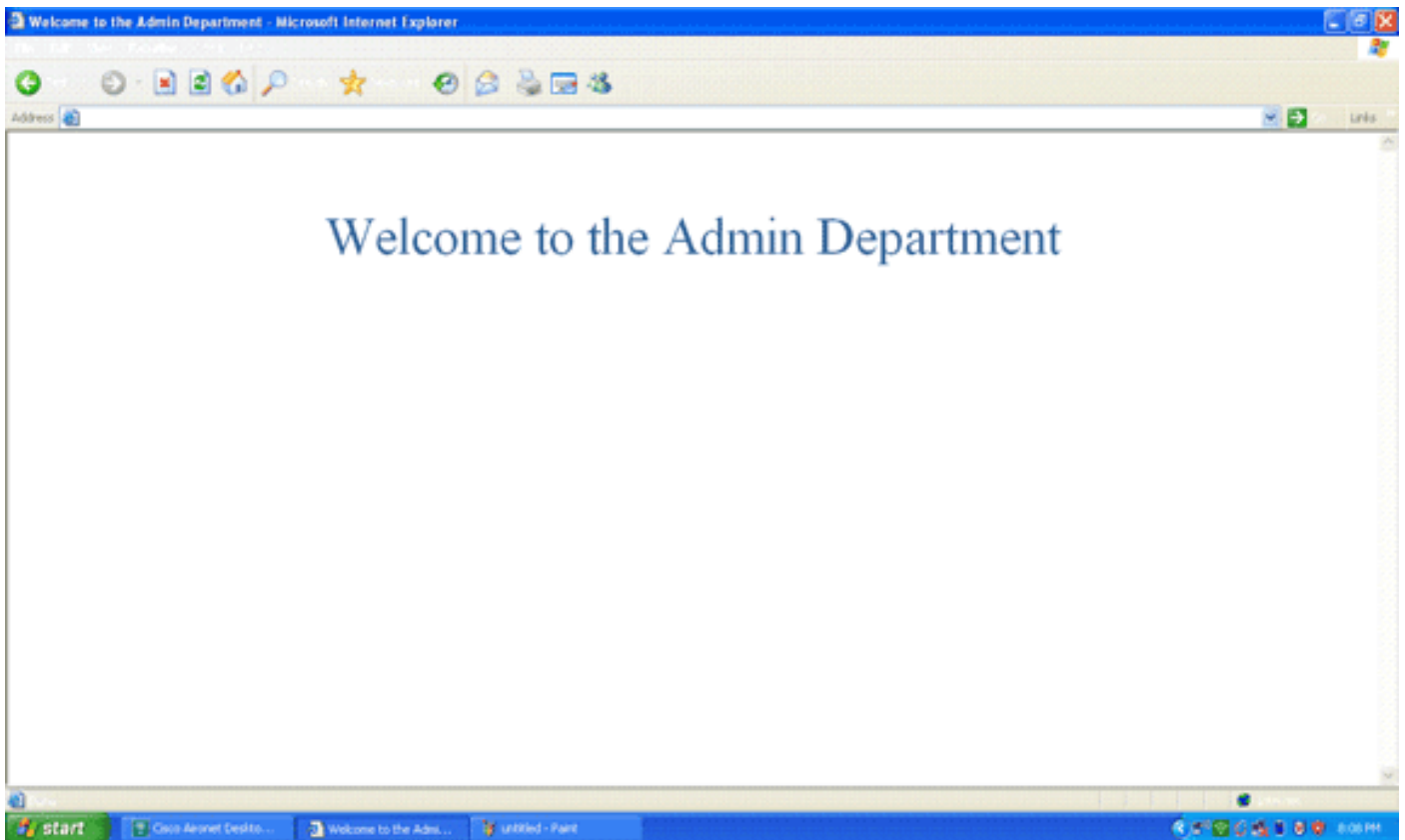
## Verificación

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

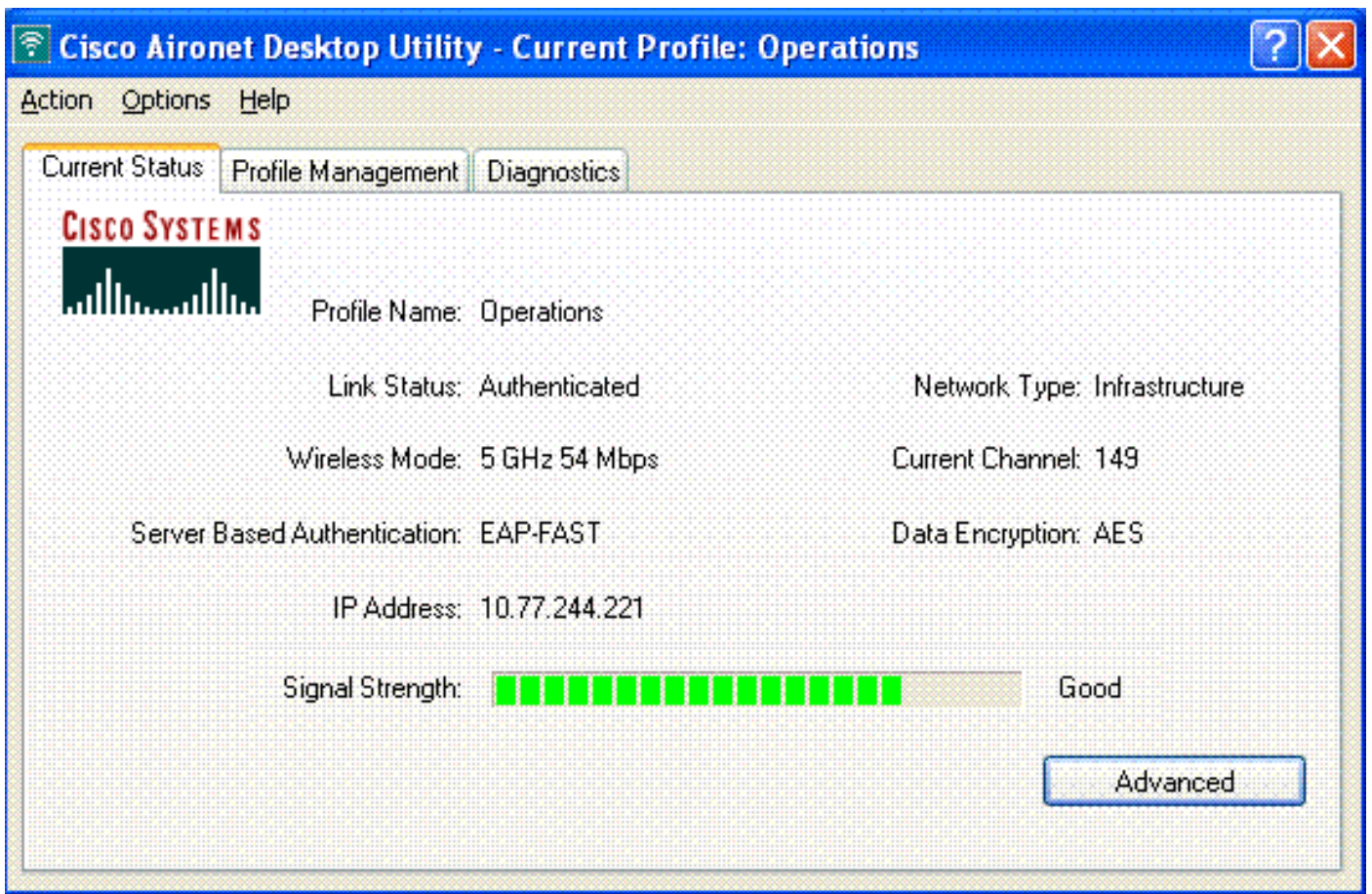
Cuando un usuario del departamento de administración se conecta con el administrador de LAN inalámbrica, se le solicitan credenciales 802.1x (credenciales EAP-FAST en nuestro caso). Una vez que el usuario proporciona las credenciales, el WLC pasa esas credenciales al servidor ACS seguro de Cisco. El servidor Cisco Secure ACS valida las credenciales del usuario contra la base de datos y, tras una autenticación satisfactoria, devuelve el atributo url-redirect al controlador de LAN inalámbrica. La autenticación se ha completado en esta etapa.

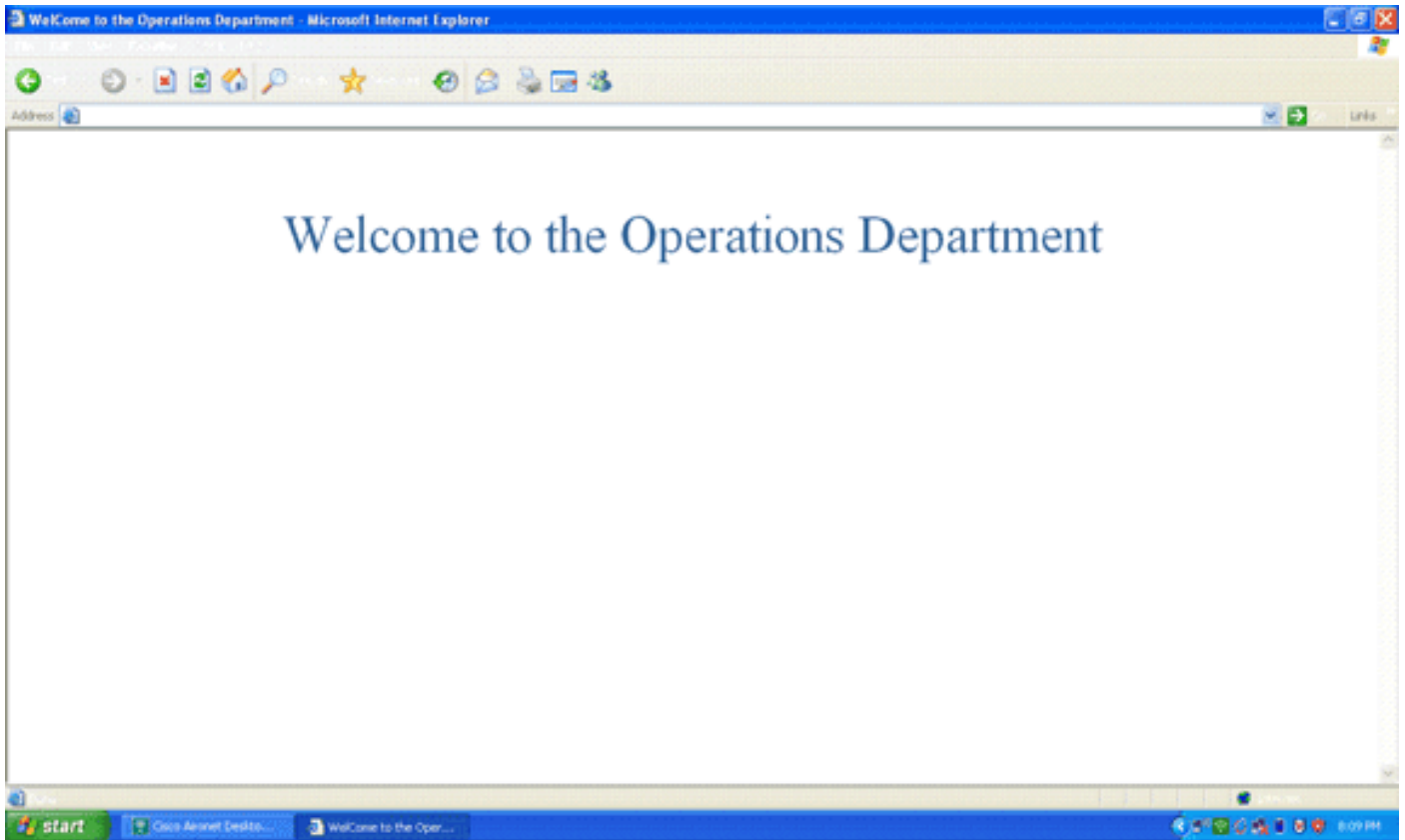


Cuando el usuario abre un navegador web, se le redirige a la URL de la página de inicio del departamento de administración. (Esta URL se devuelve al WLC a través del atributo cisco-av-pair). Después de la redirección, el usuario tiene acceso completo a la red. Estas son las capturas de pantalla:



Las mismas secuencias de eventos se producen cuando un usuario del departamento de operaciones se conecta a las operaciones de WLAN.





## Troubleshoot

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

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

Puede utilizar los siguientes comandos para solucionar problemas de configuración.

- **show wlan wlan\_id:** muestra el estado de las funciones de redirección web para una 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
```

- **debug dot1x events enable:** habilita la depuración de mensajes de paquetes 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 Id 16, 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

```

- **debug aaa events enable:** habilita la salida de depuración 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 de controlador de LAN inalámbrica de Cisco, versión 5.0](#)
- [Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico](#)
- [Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica](#)
- [Página de Soporte 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).