La página inalámbrica del chapoteo del regulador LAN reorienta el ejemplo de la configuración

Contenido

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 de la Seguridad LWAPP
- Conocimiento de cómo configurar Cisco ACS seguro

Componentes Utilizados

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

- El regulador inalámbrico LAN de las Cisco 4400 Series (WLC) ese funciona con la versión de firmware 5.0
- Punto de acceso ligero de las Cisco 1232 Series (REVESTIMIENTO)
- Adaptador de red inalámbrica de cliente de Cisco Aironet 802.a/b/g que funciona con la versión de firmware 4.1
- Cisco asegura al servidor 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 inalámbrica del regulador 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 de valor por defecto) o los intentos para tener acceso a 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 LAN de la Tecnología inalámbrica sobre la autenticación acertada del 802.1x.

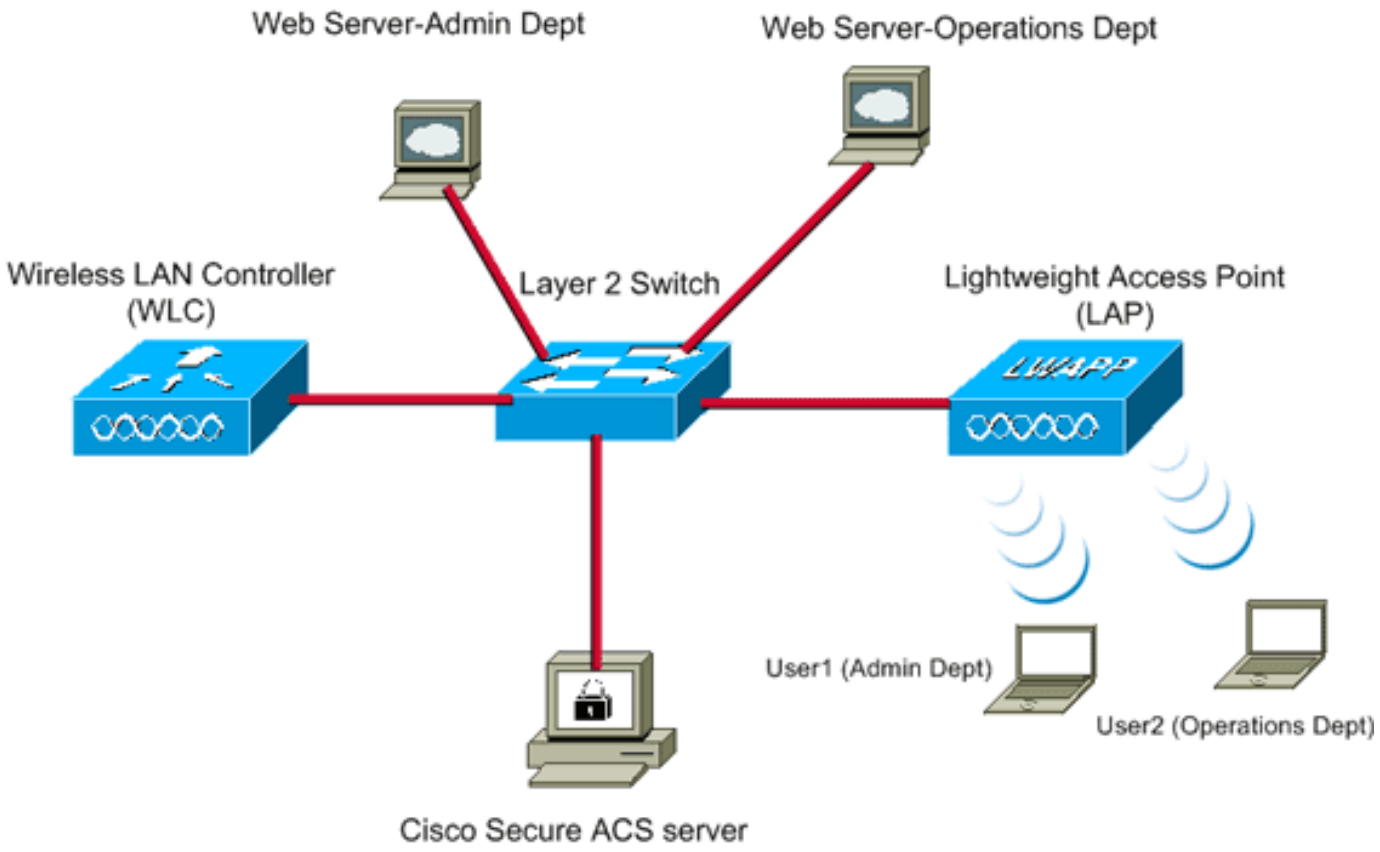
La red de la página del chapoteo reorienta la característica está disponible solamente para las redes inalámbricas (WLAN) configuradas para el 802.1x o WPA/WPA2 acoda la Seguridad 2.

Configuración de la red

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

El REVESTIMIENTO se registra inicialmente al regulador. Usted debe crear dos redes inalámbricas (WLAN): uno para los usuarios del **departamento Admin** y el otro para los usuarios del **departamento de operaciones**. Ambo uso inalámbrico WPA2/ AES de LANs (el EAP-FAST se utiliza para la autenticación). Ambas redes inalámbricas (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 disposición.

Configurar

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

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

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

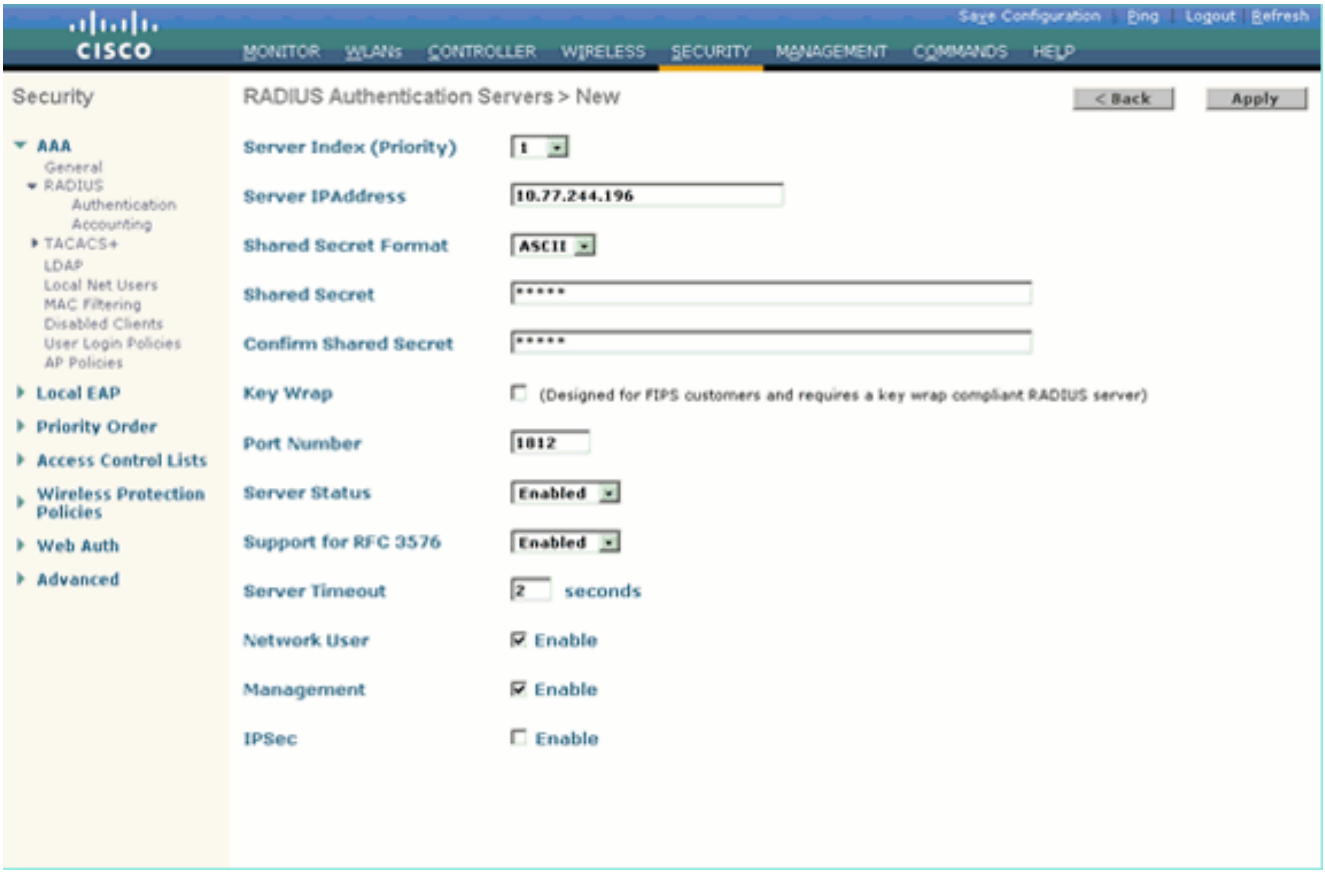
1. Configure el WLC para la autenticación de RADIUS con Cisco aseguran al servidor ACS.
2. Configure las redes inalámbricas (WLAN) para los departamentos Admin y de operaciones.
3. Configure Cisco ACS seguro para utilizar la página del chapoteo reorientan la característica.

Paso 1. Configure el WLC para la autenticación de RADIUS con Cisco aseguran al servidor ACS.

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

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

1. Elija la **Seguridad** y la **autenticación de RADIUS del** GUI del regulador 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 RADIUSsecreto compartidoNúmero del puertoEstado del servidor



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

4. Haga clic en Apply (Aplicar).

Paso 2. Configure las redes inalámbricas (WLAN) para el departamento Admin y de operaciones.

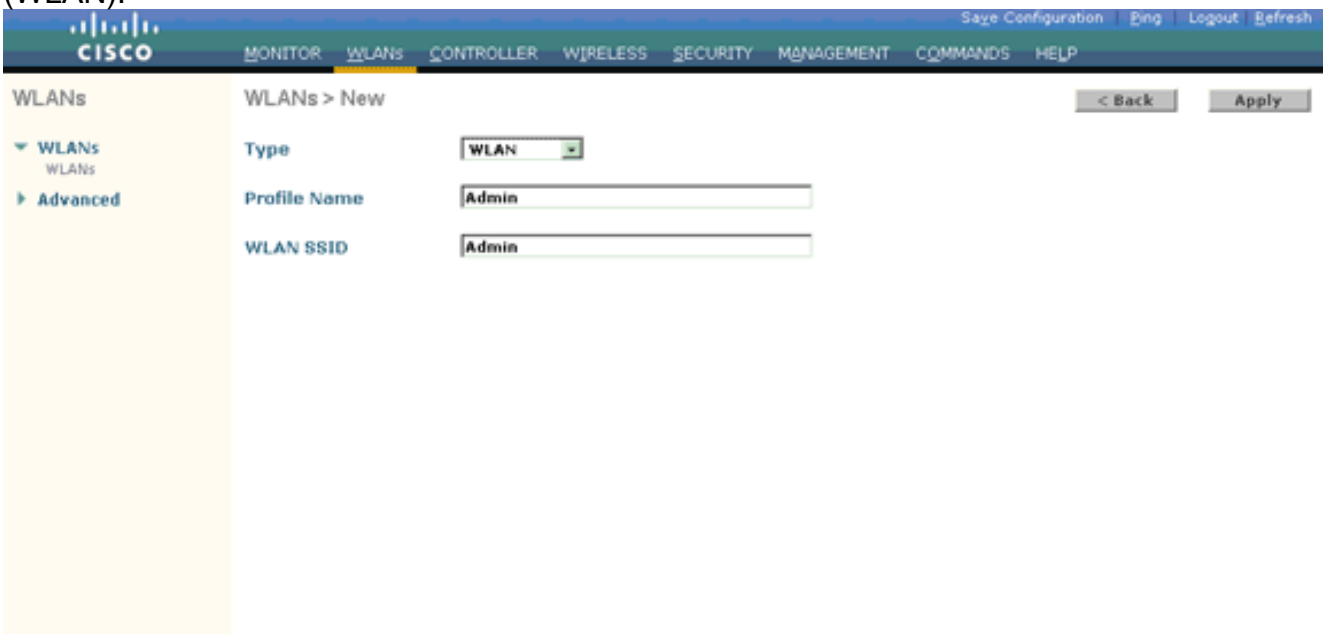
En este paso, usted configura las dos redes inalámbricas (WLAN) (una para el departamento Admin y la otra para el departamento de operaciones) que los clientes utilizarán para conectar con la red inalámbrica.

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

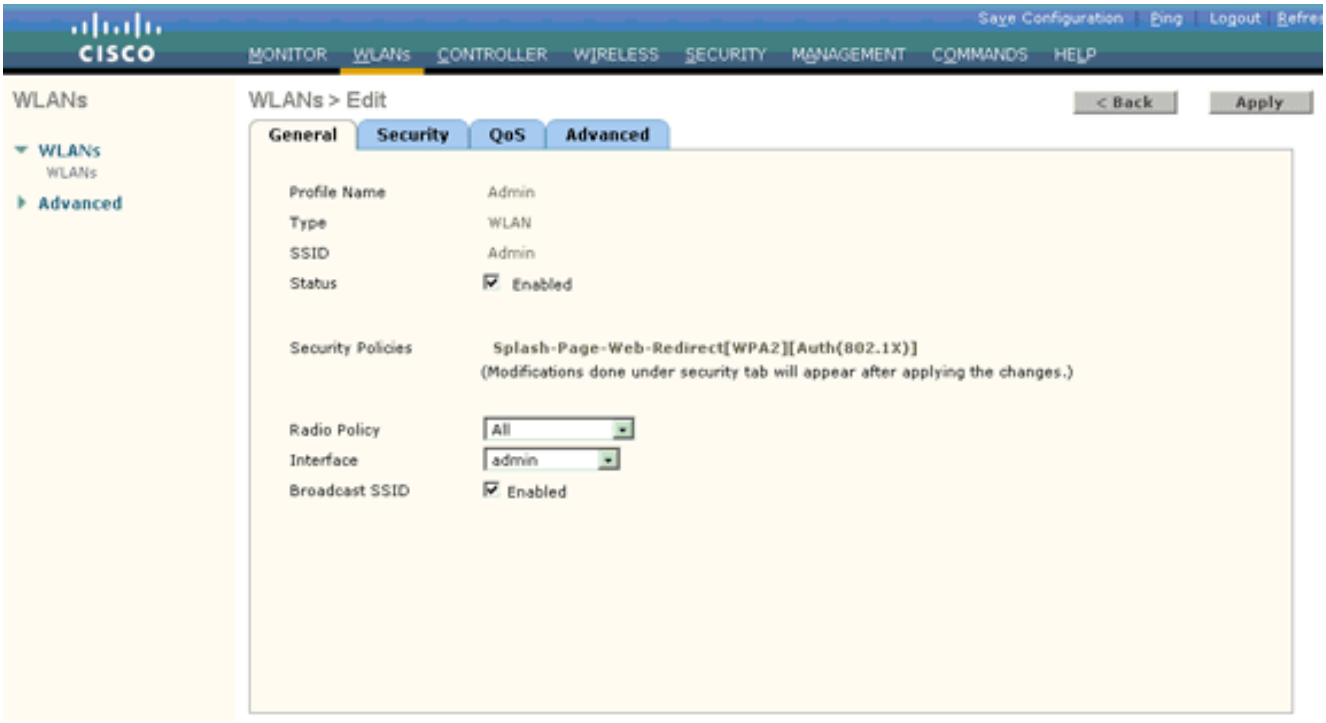
Utilice la autenticación del EAP-FAST para activar el WPA2 como el mecanismo de seguridad de la capa 2 en ambas redes inalámbricas (WLAN) y la directiva de la red - la red de la página del chapoteo reorienta la característica como el método de seguridad de la capa 3.

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

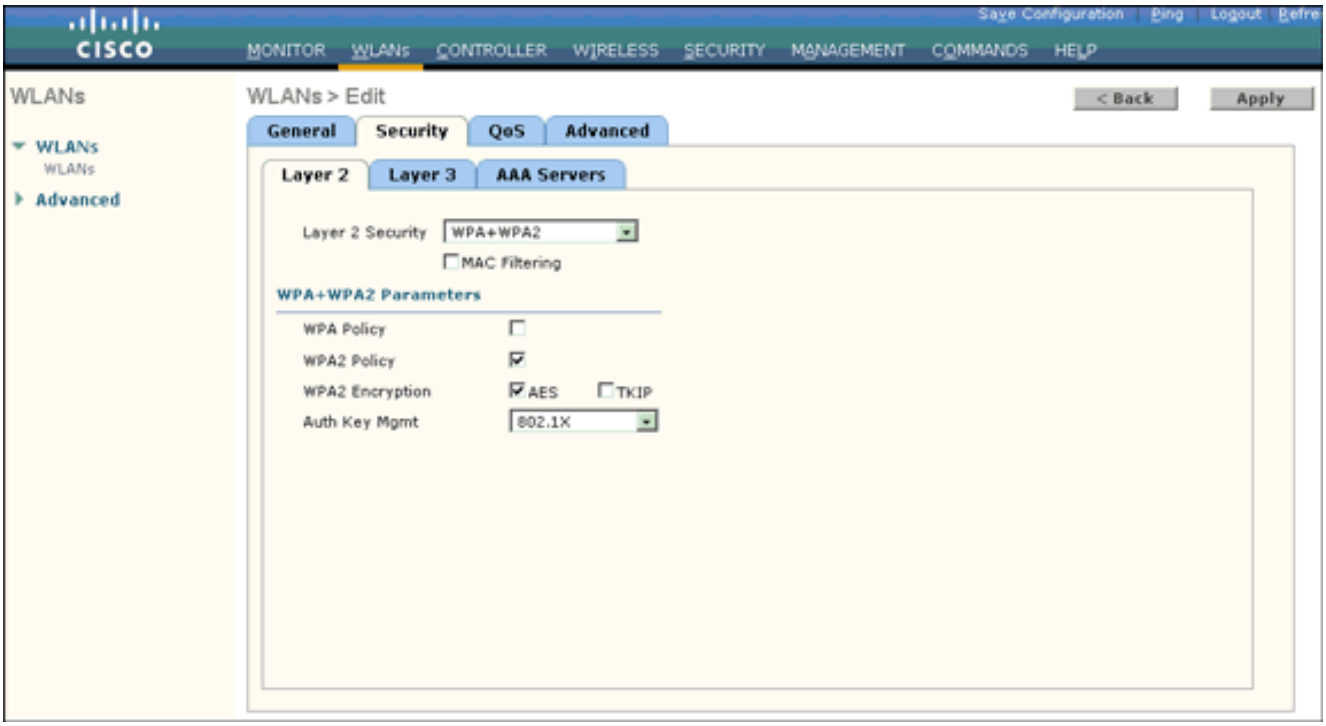
1. Haga clic las **redes inalámbricas (WLAN) del** GUI del regulador para visualizar la página de las redes inalámbricas (WLAN).Esta página enumera las redes inalámbricas (WLAN) que existen en el regulador.
2. Tecleo **nuevo** para crear una nueva red inalámbrica (WLAN).



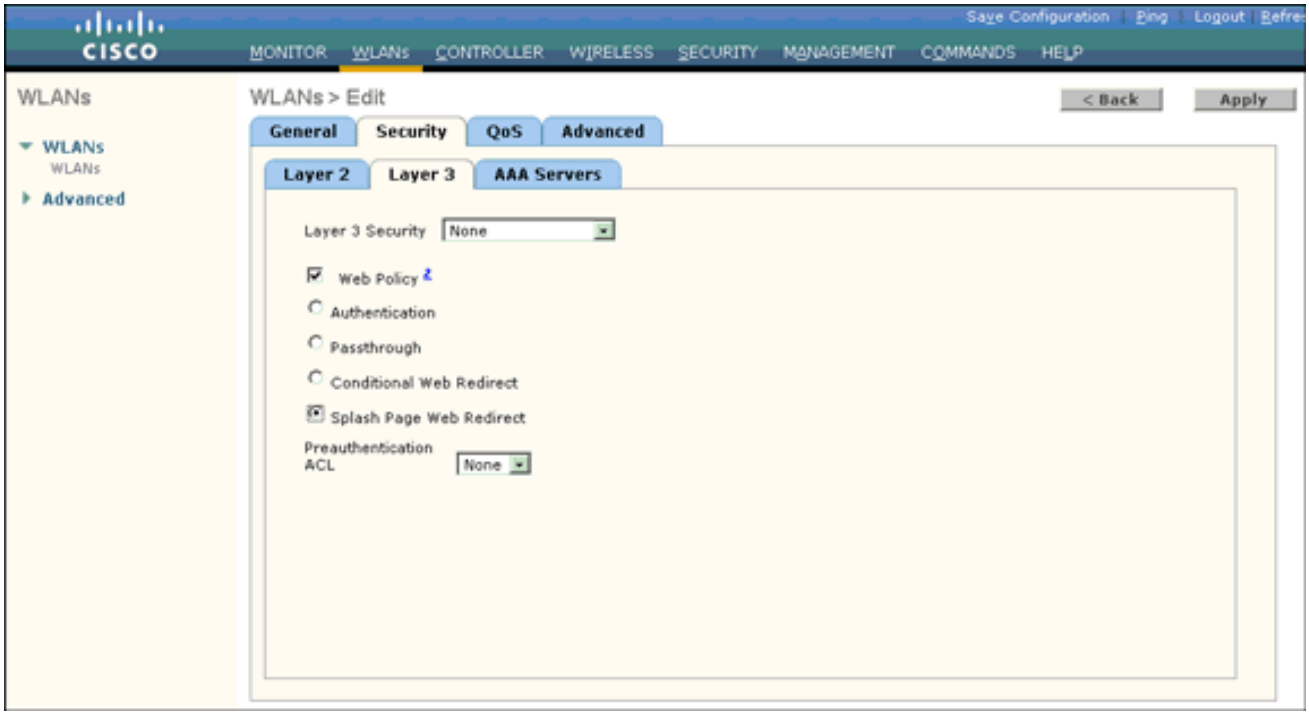
3. Ingrese el nombre WLAN SSID y el nombre del perfil en el WLANs > nueva página.
4. Haga clic en Apply (Aplicar).
5. Primero déjenos crean la red inalámbrica (WLAN) para el departamento Admin.Una vez que usted crea una nueva red inalámbrica (WLAN), la red inalámbrica (WLAN) > corrige la página para 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, controle el cuadro de **revisión de estado** para activar la red inalámbrica (WLAN).



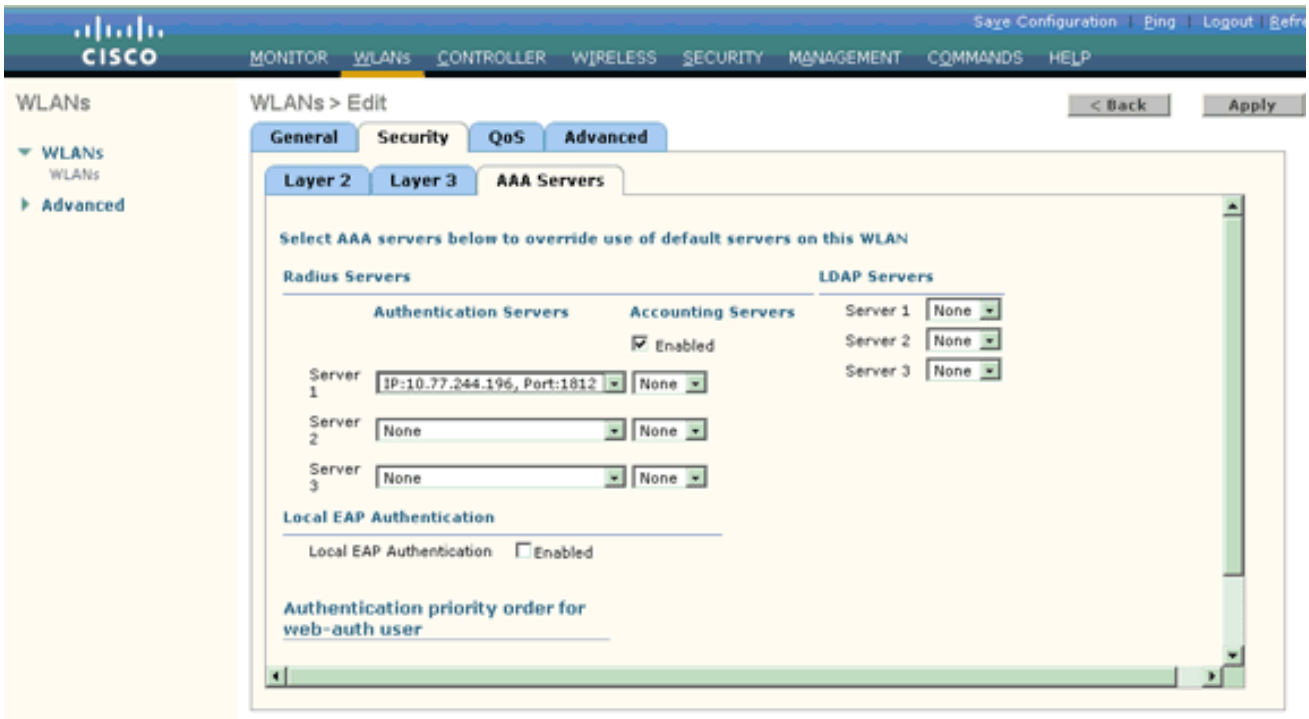
7. Haga clic la **ficha de seguridad**, y después haga clic la **capa 2** cuadro.
8. Elija **WPA+WPA2 de la** lista desplegable de la Seguridad de la capa 2.Este paso activa la autenticación WPA para la red inalámbrica (WLAN).
9. Bajo parámetros WPA+WPA2, controle las casillas de verificación de la **directiva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



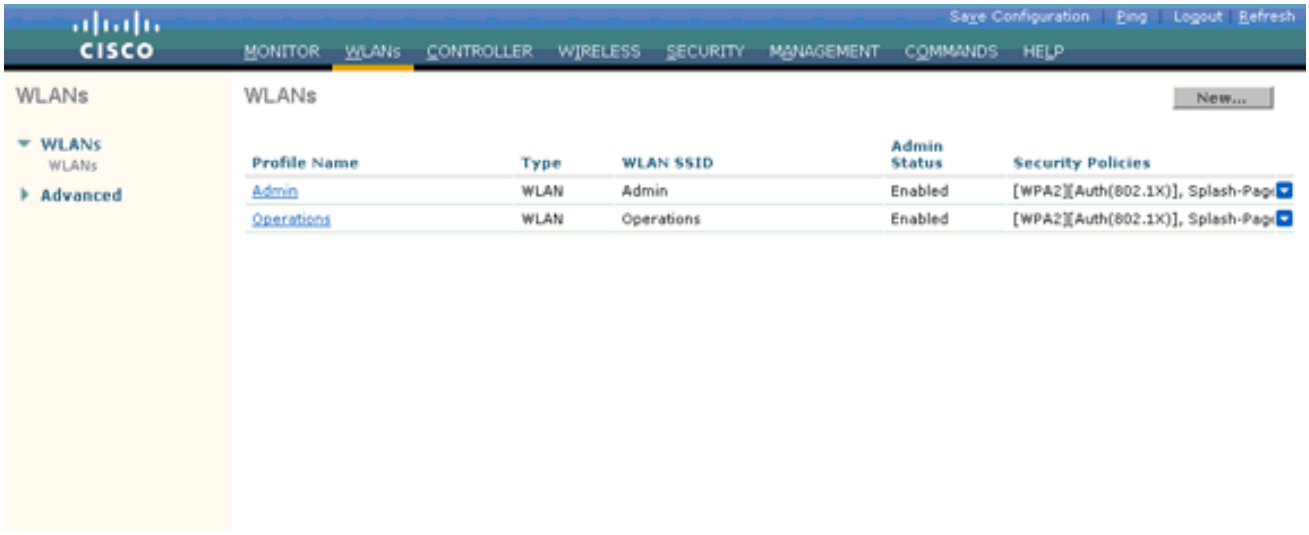
10. Elija el **802.1x de la** lista desplegable dominante auténtica de Mgmt. Esta opción activa el WPA2 con la autenticación 802.1x/EAP y la encripción AES para la red inalámbrica (WLAN).
11. Haga clic la **ficha de seguridad de la capa 3**.
12. Controle el cuadro de la **directiva de la red**, y después haga clic la **red de la página del chapoteo reorientan el** botón de radio.Esta opción activa la red de la página del chapoteo reorienta la
característica.



13. Haga clic los **servidores** cuadro **AAA**.
14. Bajo los servidores de la autenticación, elija la dirección IP apropiada del servidor de la lista desplegable del servidor
    1.



    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.Las redes inalámbricas (WLAN) paginan las listas las dos redes inalámbricas (WLAN) que usted
    creó.



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

Paso 3. Configure Cisco ACS seguro para utilizar la página del chapoteo reorientan la característica.

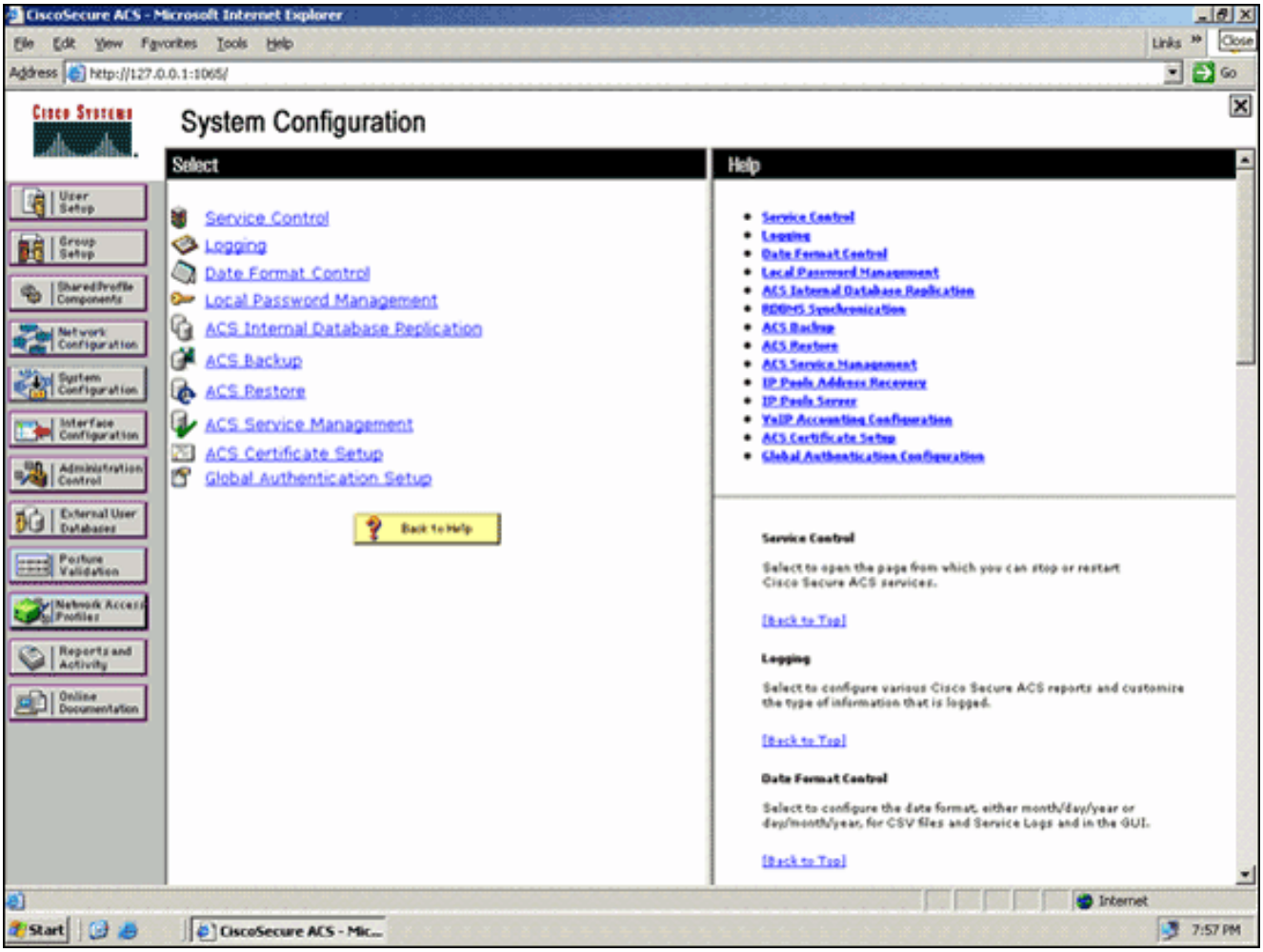
El siguiente paso es configurar al servidor de RADIUS para esta característica. El servidor de RADIUS necesita realizar la autenticación del EAP-FAST para validar las credenciales del cliente, y sobre la autenticación satisfactoria, reorientar al usuario al URL (en el servidor Web externo) especificada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

Configure Cisco ACS seguro para la autenticación del EAP-FAST

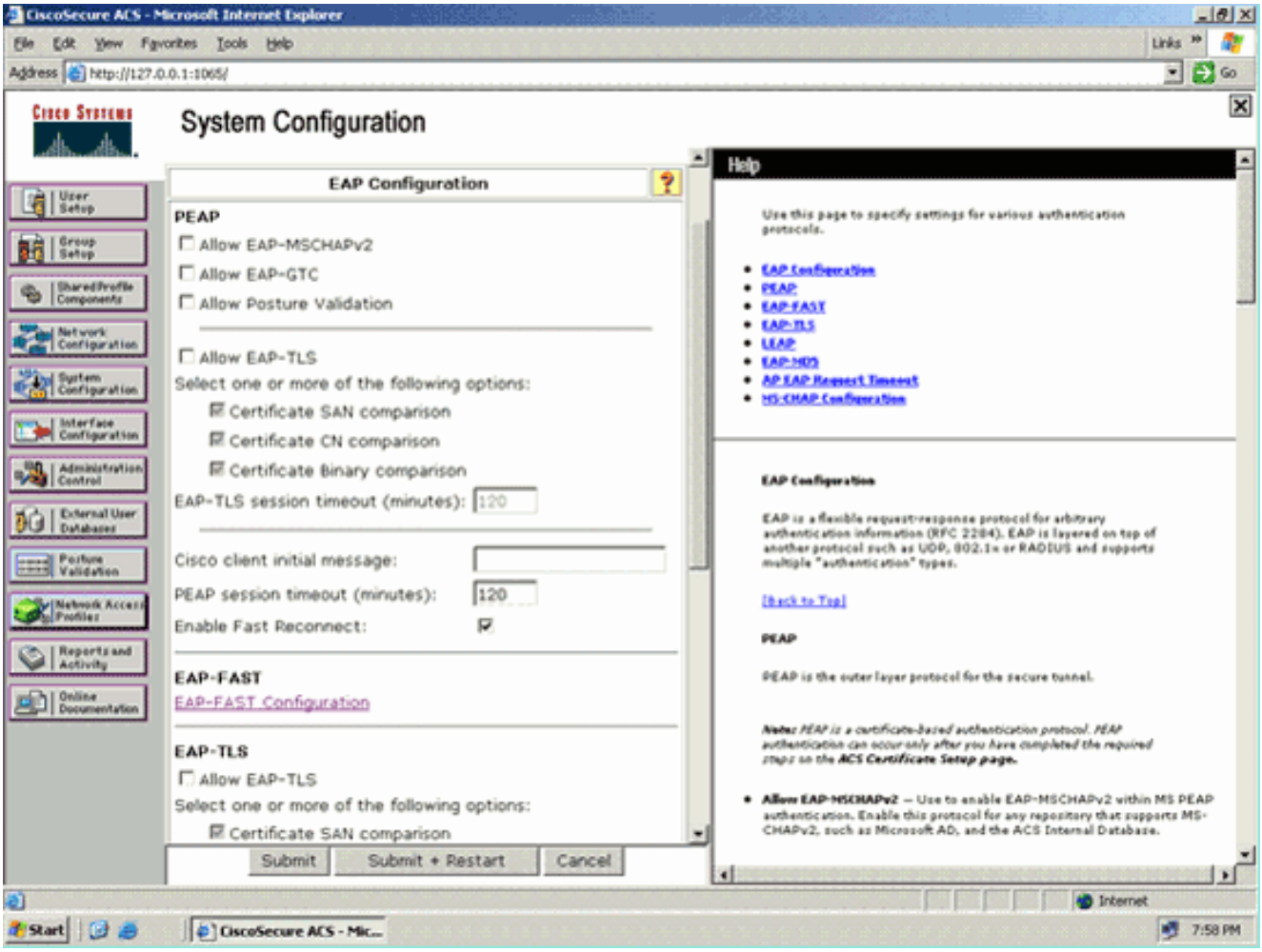
Nota: Este documento asume que el regulador LAN de la Tecnología inalámbrica está agregado a Cisco ACS seguro como cliente AAA.

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

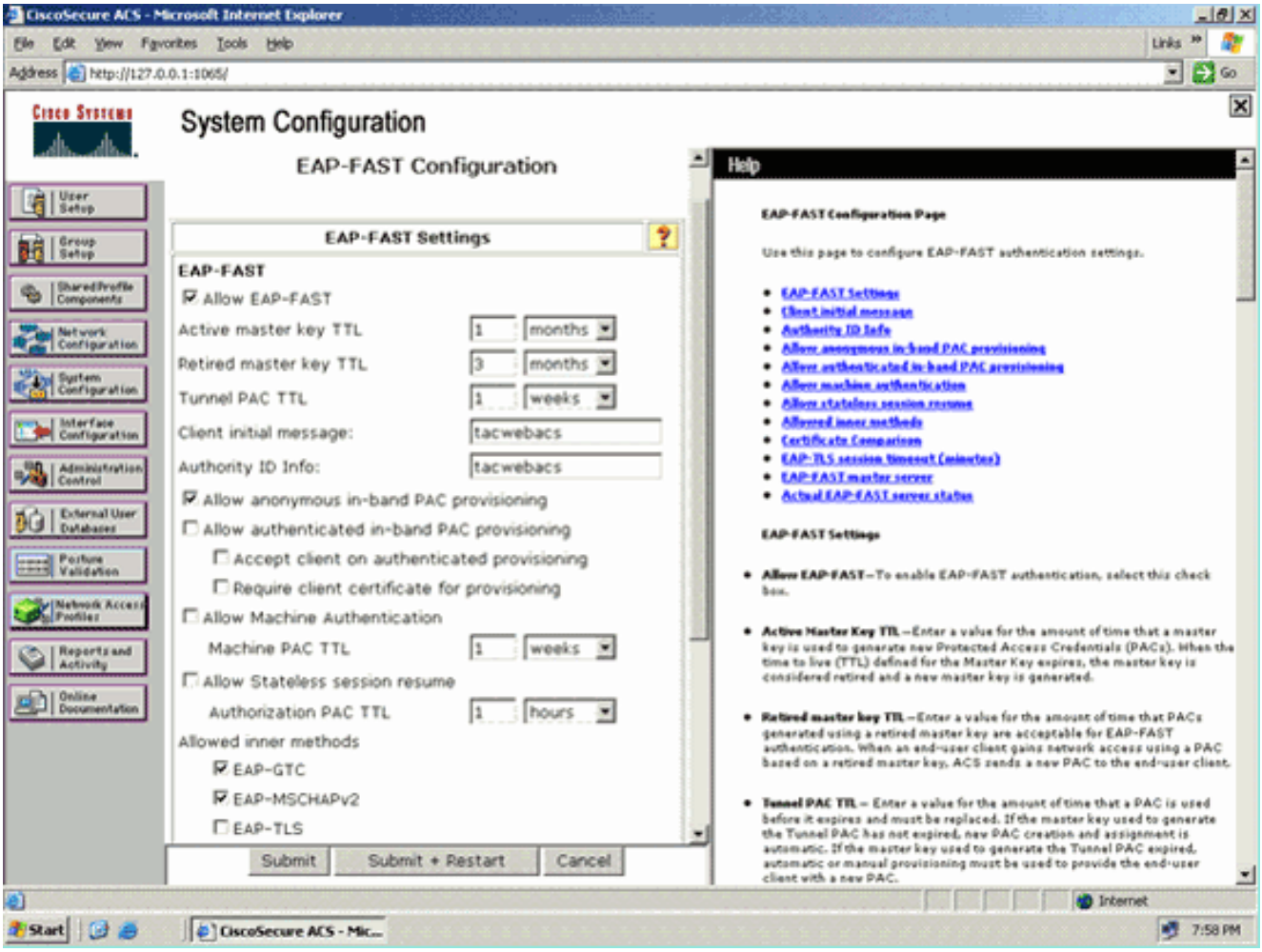
1. Haga clic la **configuración del sistema del** GUI del servidor de RADIUS, y después elija eligen la **disposición global de la autenticación de la** página de la configuración del sistema.



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



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



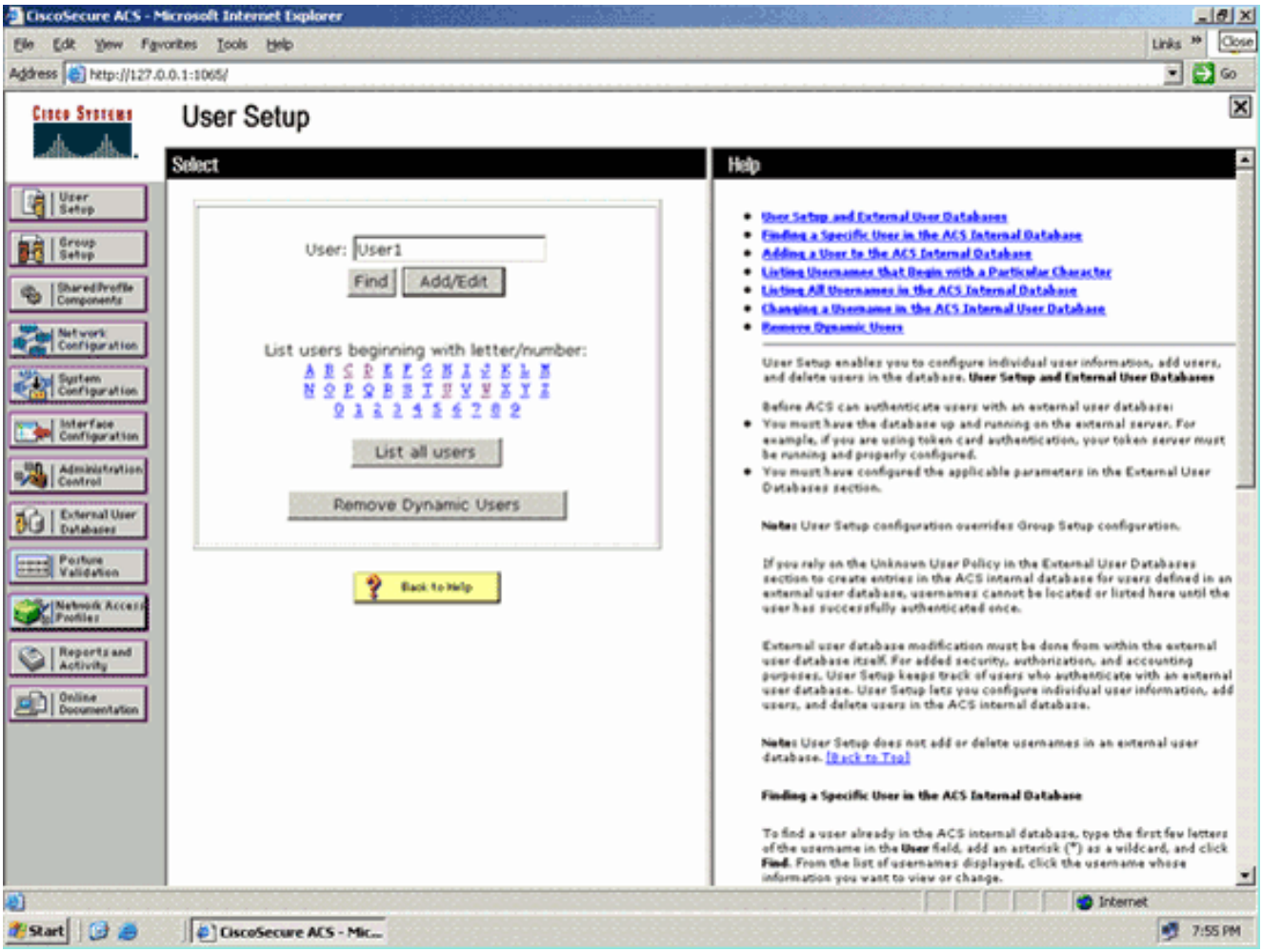
4. Configure el Active/los valores jubilados de TTL de la clave principal (Time to Live) según lo deseado, o fíjelos al valor predeterminado tal y como se muestra en de este ejemplo.El campo de información ID de la autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar contra qué 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 el cliente del usuario final utiliza la visualización.
5. Si usted quisiera que el ACS realizara el aprovisionamiento anónimo PAC de la en-banda, controle la casilla de verificación **anónima del aprovisionamiento PAC de la en-banda de la permit**.
6. La opción *interna permitida de los métodos* determina qué métodos EAP internos pueden ejecutarse dentro del túnel de TLS del EAP-FAST. Para el aprovisionamiento anónimo de la en-banda, usted debe activar el EAP-GTC y EAP-MS-CHAP para la compatibilidad con versiones anteriores. Si usted selecciona permita el aprovisionamiento anónimo PAC de la en-banda, 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 EAP AYUNE con el aprovisionamiento anónimo PAC de la En-banda y el aprovisionamiento autenticado de la En-banda, refiere a la autenticación del EAP-FAST con los reguladores inalámbricos LAN y el ejemplo externo de la configuración de servidor de RADIUS.

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

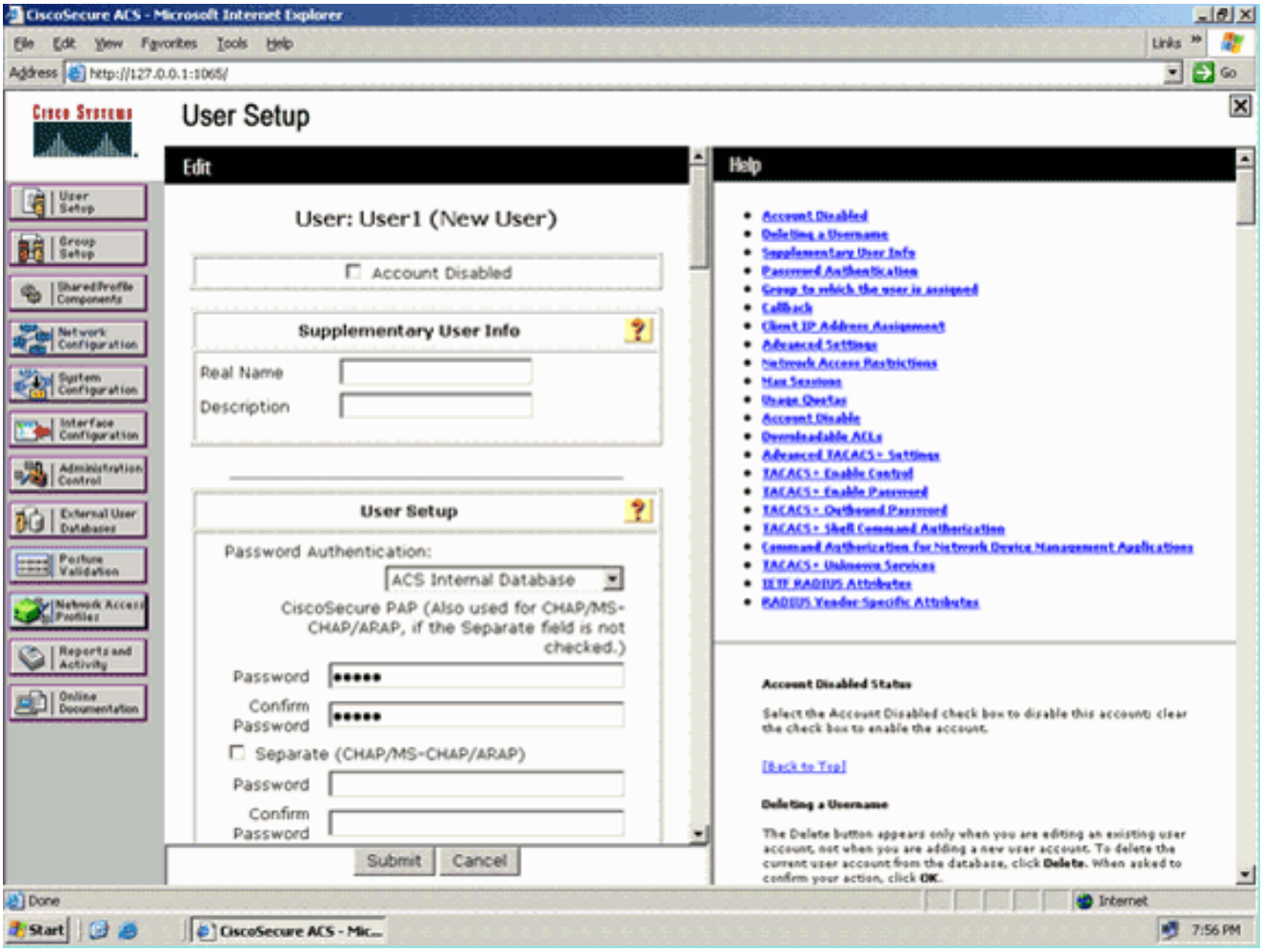
Este ejemplo configura el nombre de usuario y contraseña del cliente de red inalámbrica como User1 y User1, respectivamente.

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

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



3. De la configuración de usuario corrija la página, configure el Nombre real y la descripción, 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. Enrolle abajo la página para modificar los atributos de RADIUS.
5. Controle 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

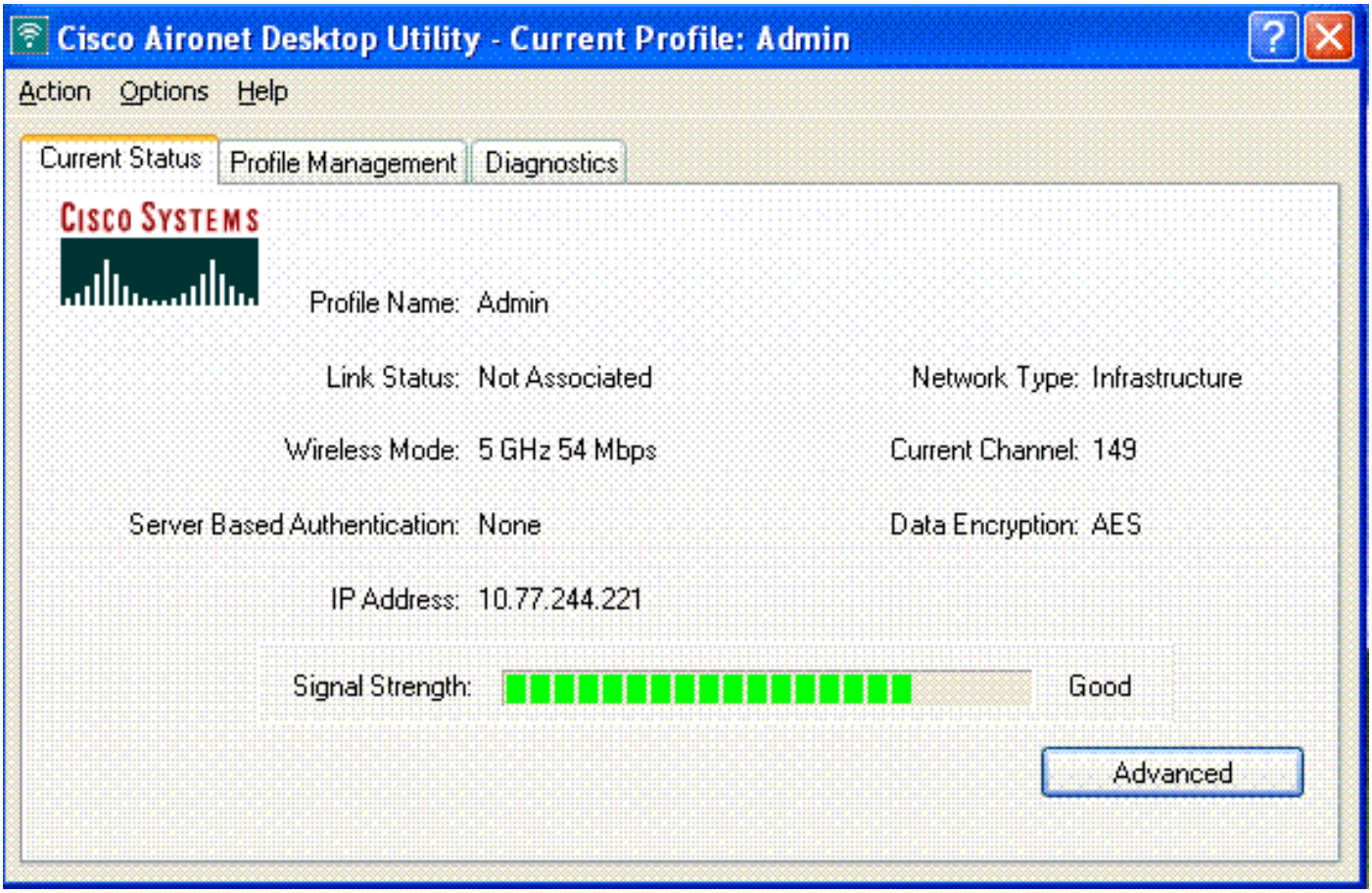
Éste es el Home Page de los usuarios del departamento Admin.

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 a más usuarios de los usuarios del departamento Admin y del departamento 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 Cisco ACS seguro.

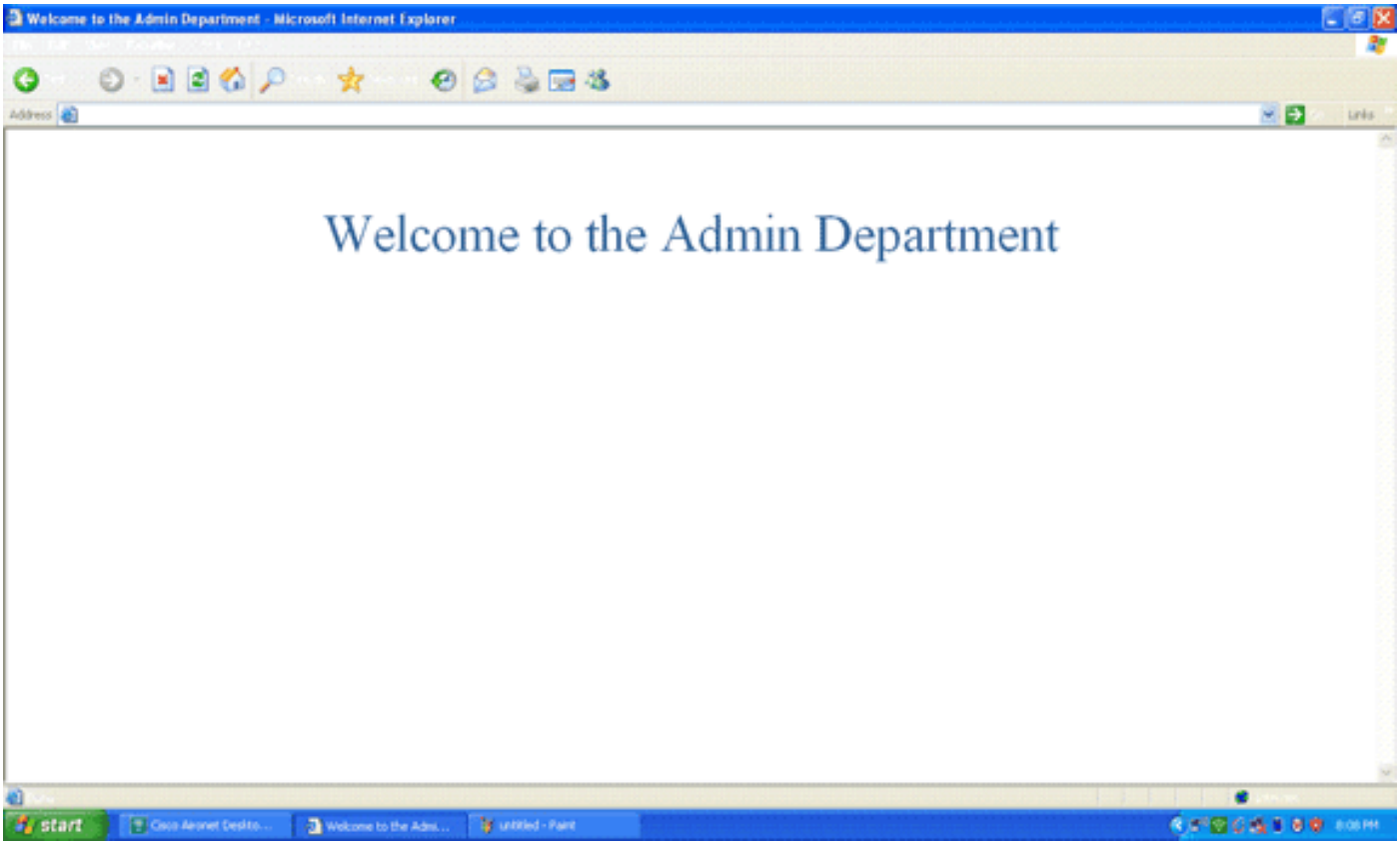
Verificación

Para verificar la configuración, asocie a un cliente de WLAN del departamento Admin y del departamento de operaciones a sus redes inalámbricas (WLAN) apropiadas.

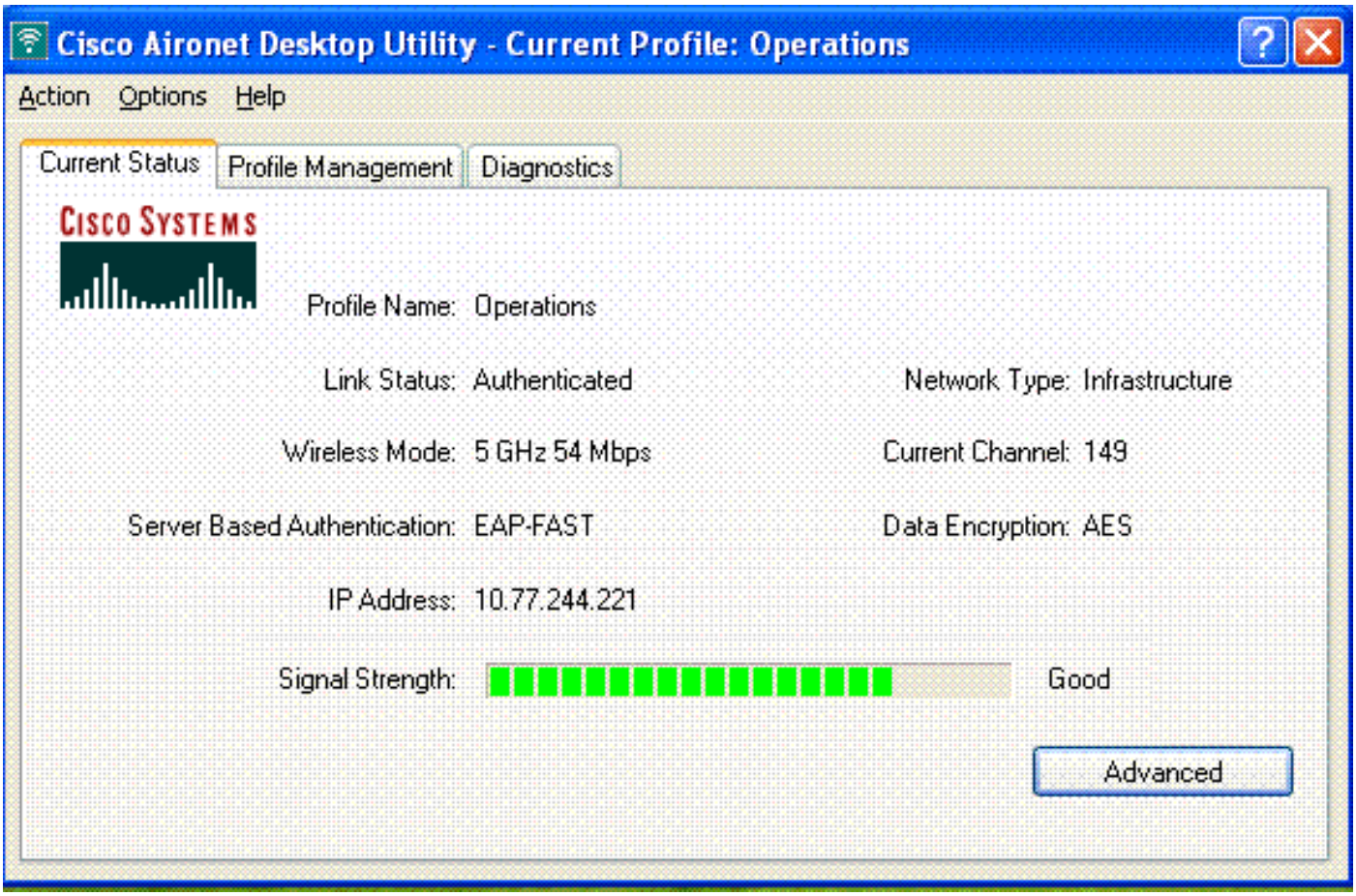
Cuando un usuario del departamento Admin conecta con el LAN Admin de la Tecnología inalámbrica, incitan al usuario para las credenciales del 802.1x (credenciales del EAP-FAST en nuestro caso). Una vez que el usuario proporciona a las credenciales, el WLC pasa esas credenciales a Cisco asegura al servidor ACS. Cisco asegura al servidor 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 LAN de la Tecnología inalámbrica. La autenticación es completa en esta etapa.

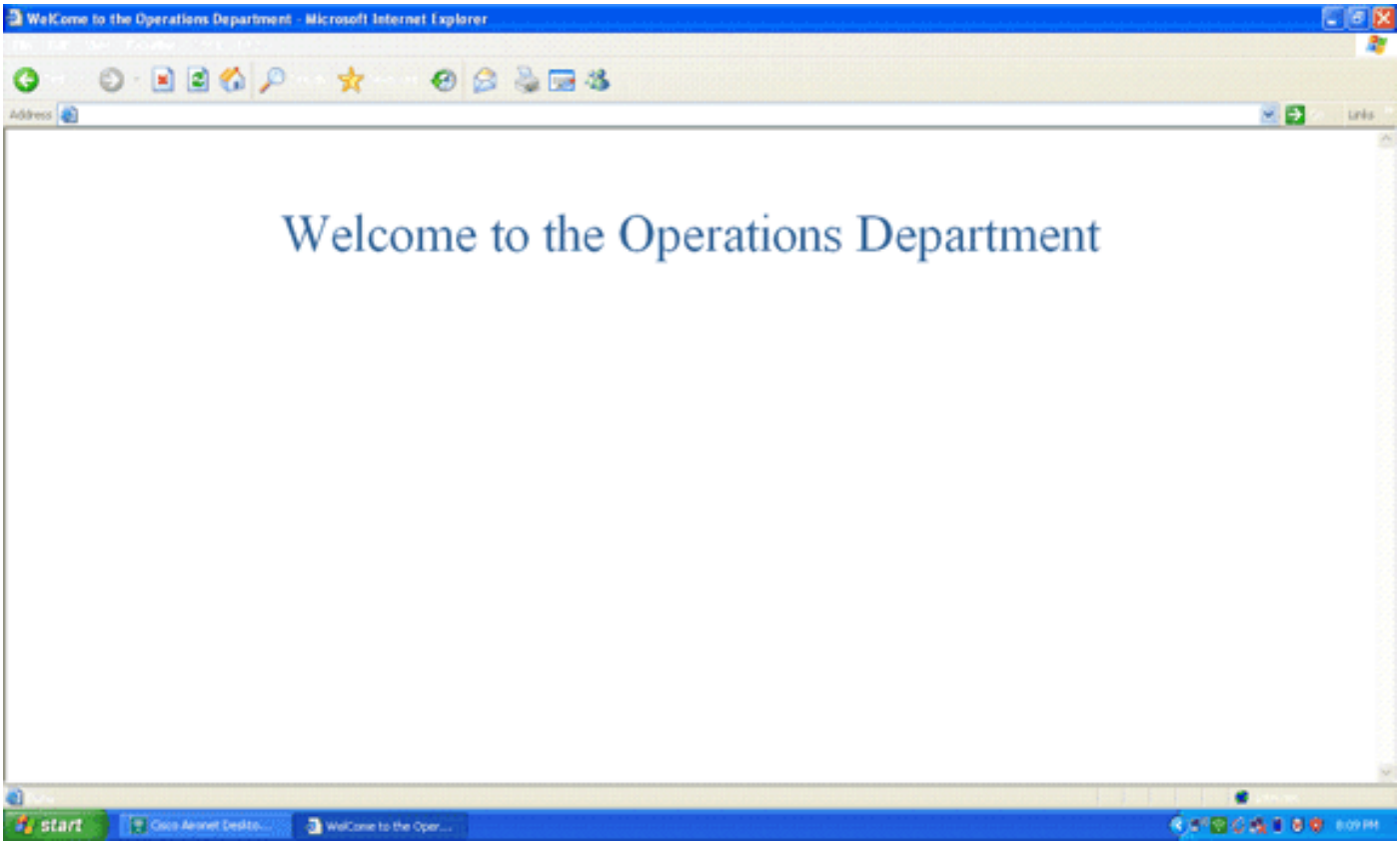


Cuando el usuario abre a un buscador Web, reorientan al usuario al Home Page URL del departamento Admin. (Este URL se vuelve al WLC con el atributo del cisco av-pair). Después de que la reorientación, el usuario tenga acceso total a la red. Aquí están las capturas de pantalla:



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 comandos siguientes 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 de la depuración dot1x** — Activa la depuración 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 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
```

- **permiso de los eventos aaa de la depuración** — Activa la salida de la 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 inalámbrica del regulador LAN 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