

Autenticación Web Externa Usando un Servidor RADIUS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Convenciones](#)

[Autenticación web externa](#)

[Configurar la WLC](#)

[Configuración del WLC para Cisco Secure ACS](#)

[Configure el WLAN en el WLC para la autenticación Web](#)

[Configure la información del servidor Web en el WLC](#)

[Configuración de Cisco Secure ACS](#)

[Configuración de la información del usuario en Cisco Secure ACS](#)

[Configuración de la Información de WLC en Cisco Secure ACS](#)

[Proceso de autenticación de cliente](#)

[Configuración del Cliente](#)

[Proceso de conexión del cliente](#)

[Verificación](#)

[Verificación de ACS](#)

[Verificar WLC](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento explica cómo realizar la autenticación Web externa usando un servidor RADIUS externo.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de Lightweight Access Points (LAP) y Cisco WLC

- Conocimiento de cómo configurar un servidor web externo
- Conocimiento de cómo configurar Cisco Secure ACS

Componentes Utilizados

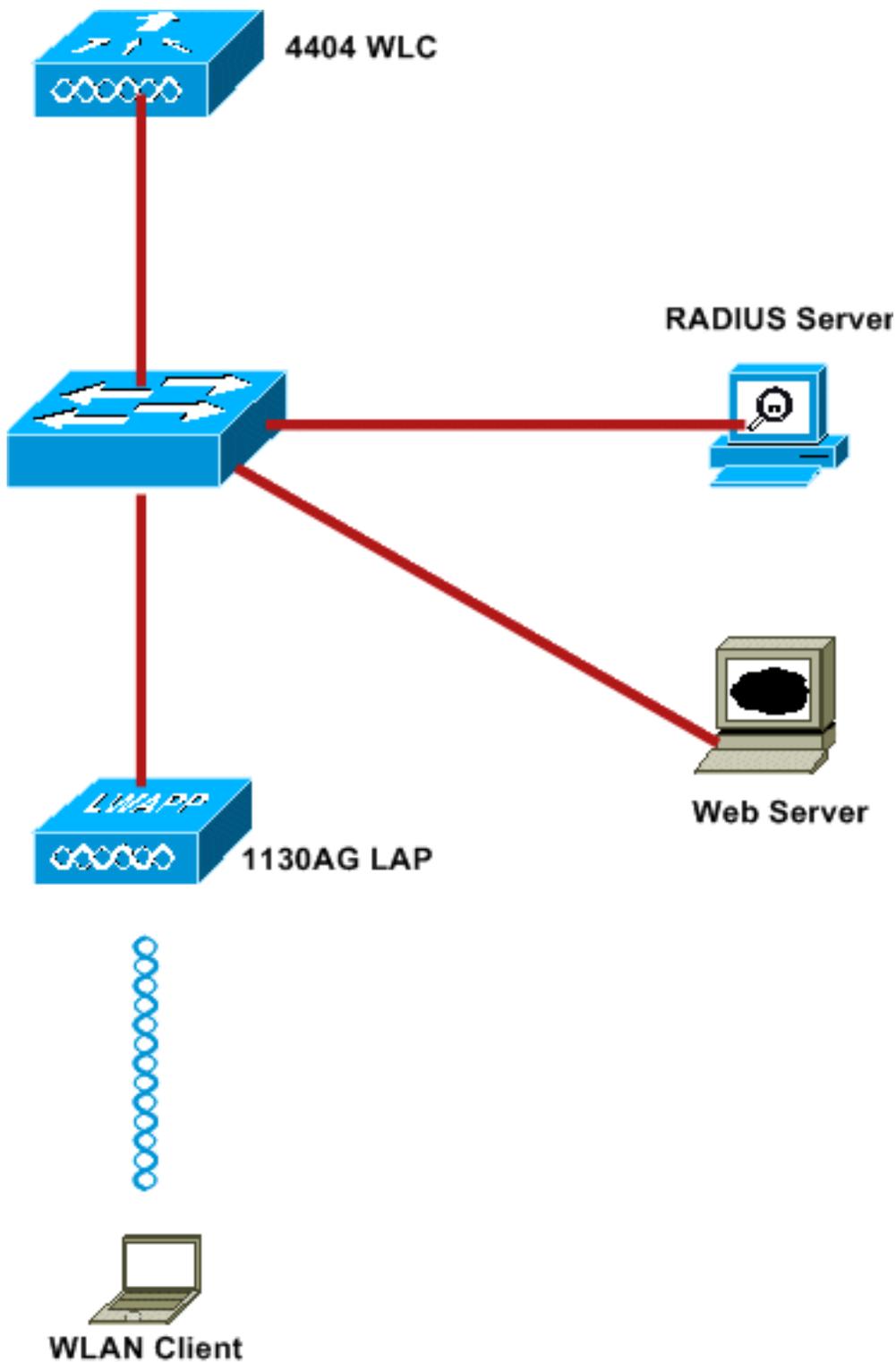
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador de LAN inalámbrica que ejecuta la versión de firmware 5.0.148.0
- LAP de la serie 1232 de Cisco
- Adaptador de cliente inalámbrico 802.11a/b/g de Cisco 3.6.0.61
- Servidor Web externo que aloja la página de inicio de sesión de autenticación Web
- Versión de Cisco Secure ACS que ejecuta la versión de firmware 4.1.1.24

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Las siguientes son direcciones IP usadas en este documento:

- El WLC utiliza la dirección IP 10.77.244.206
- El LAP se registra al WLC con la dirección IP 10.77.244.199
- El servidor web utiliza la dirección IP 10.77.244.210
- El servidor Cisco ACS utiliza la dirección IP 10.77.244.196
- El cliente recibe una dirección IP de la interfaz de administración asignada a la WLAN - 10.77.244.208

Convenciones

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

[Autenticación web externa](#)

La autenticación Web es un mecanismo de autenticación de capa 3 que se utiliza para autenticar a los usuarios invitados para el acceso a Internet. Los usuarios autenticados mediante este proceso no podrán acceder a Internet hasta que completen correctamente el proceso de autenticación. Para obtener información completa sobre el proceso de autenticación web externa, lea la sección [Proceso de autenticación web externa](#) del documento [Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica](#).

En este documento, vemos un ejemplo de configuración, en el cual la autenticación web externa se realiza usando un servidor RADIUS externo.

[Configurar la WLC](#)

En este documento, asumimos que el WLC ya está configurado y tiene un LAP registrado al WLC. Este documento asume además que el WLC se configura para el funcionamiento básico y que los LAPs se registran al WLC. Si usted es un nuevo usuario que intenta configurar el WLC para el funcionamiento básico con los LAPs, consulte [Registro ligero del AP \(LAP\) a un controlador del Wireless LAN \(WLC\)](#). Para ver los LAPs que se registran al WLC, navegue hasta **Wireless > All APs**.

Una vez que el WLC se configura para el funcionamiento básico y tiene uno o más LAPs registrados para él, usted puede configurar el WLC para la autenticación Web externa usando un servidor Web externo. En nuestro ejemplo, estamos utilizando una versión 4.1.1.24 de Cisco Secure ACS como servidor RADIUS. En primer lugar, configuraremos el WLC para este servidor RADIUS y luego buscaremos la configuración requerida en Cisco Secure ACS para esta configuración.

[Configuración del WLC para Cisco Secure ACS](#)

Realice estos pasos para agregar el servidor RADIUS en el WLC:

1. Desde la GUI del WLC, haga clic en el menú **SECURITY**.
2. En el menú **AAA**, navegue hasta el submenú **Radius > Authentication**.
3. Haga clic en **Nuevo**, e ingrese la dirección IP del servidor RADIUS. En este ejemplo, la dirección IP del servidor es *10.77.244.196*.
4. Introduzca el secreto compartido en el WLC. El secreto compartido debe configurarse igual en el WLC.
5. Elija **ASCII** o **Hex** para Shared Secret Format. El mismo formato debe ser elegido en el WLC.
6. **1812** es el número de puerto utilizado para la autenticación RADIUS.
7. Asegúrese de que la opción Estado del servidor está establecida en **Habilitado**.
8. Marque la casilla Network User **Enable** para autenticar a los usuarios de la red.
9. Haga clic en Apply
(Aplicar).

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

- Server Index (Priority): 2
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (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: Enable
- Management: Enable
- IPSec: Enable

[Configure el WLAN en el WLC para la autenticación Web](#)

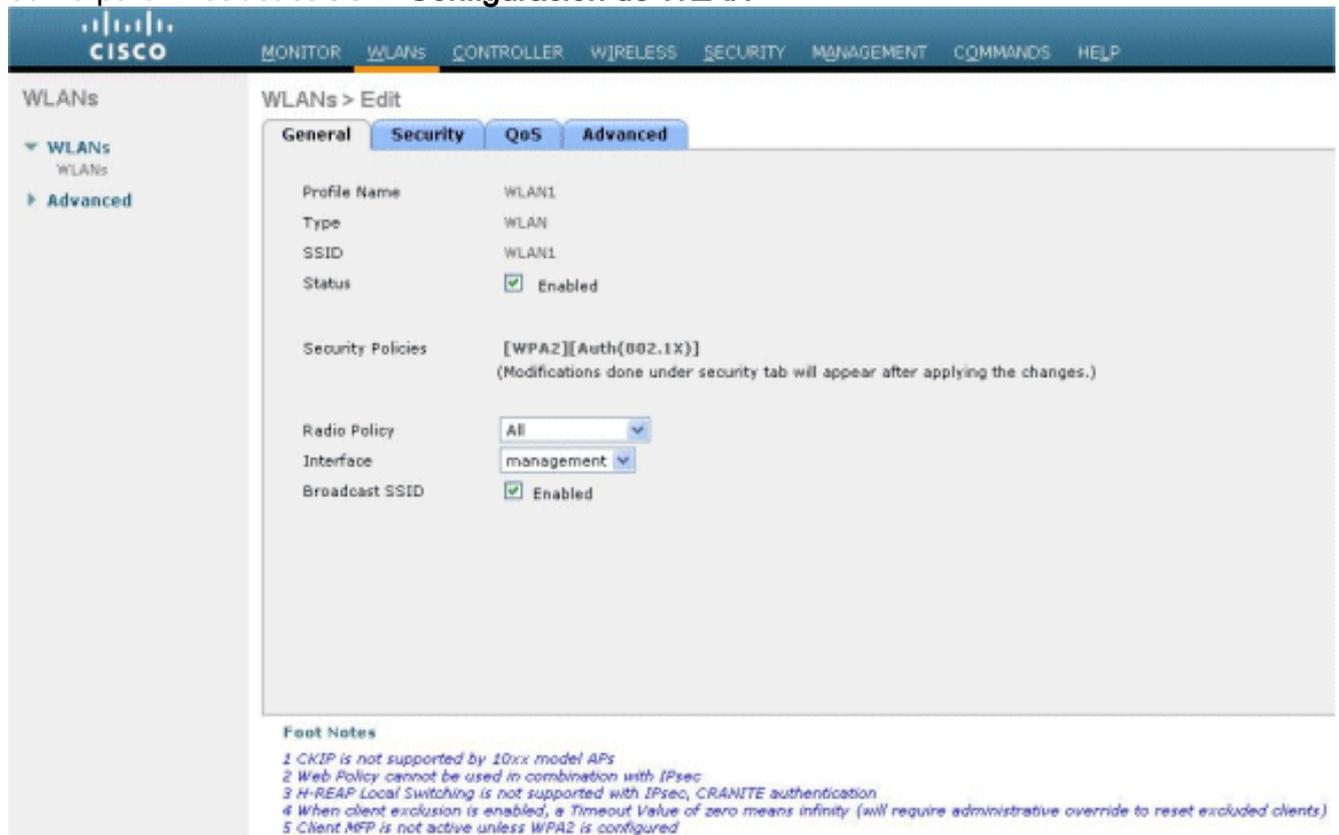
El siguiente paso es configurar el WLAN para la autenticación Web en el WLC. Realice estos pasos para configurar el WLAN en el WLC:

1. Haga clic en el menú **WLANs** de la GUI del controlador y elija **New**.
2. Elija **WLAN** para Type.
3. Ingrese un nombre de perfil y un SSID de WLAN de su elección, y haga clic en **Apply**. **Nota:** El SSID de WLAN distingue entre mayúsculas y minúsculas.

The screenshot shows the Cisco WLC configuration interface for a new WLAN. The left sidebar is under 'WLANs' with 'WLANs' expanded. The main area is titled 'WLANs > New' and contains the following fields:

- Type: WLAN
- Profile Name: WLAN1
- WLAN SSID: WLAN1

4. En la pestaña **General**, asegúrese de que la opción **Enabled** esté marcada tanto para Status como para Broadcast SSID. **Configuración de WLAN**



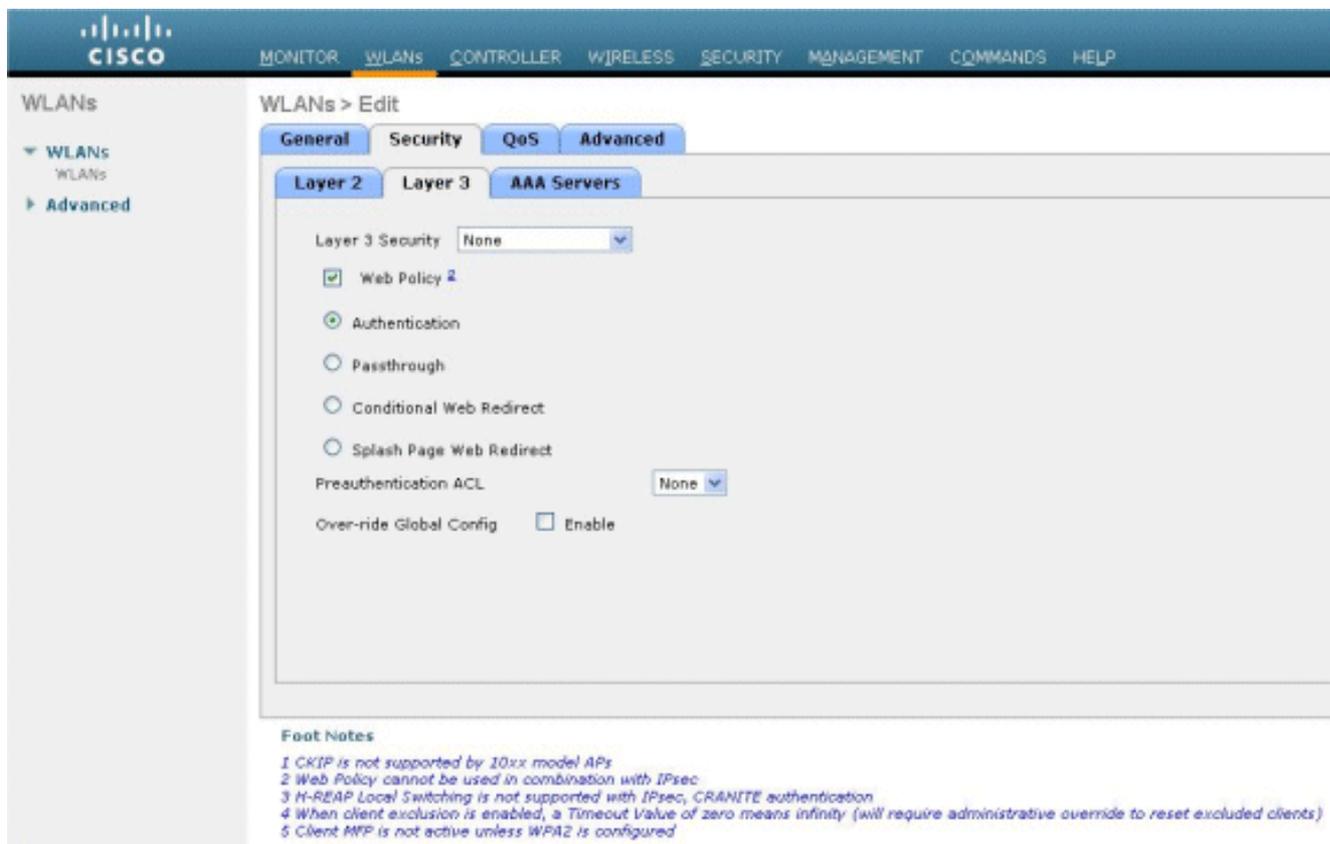
The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the WLANs menu with an 'Advanced' option selected. The main content area is titled 'WLANs > Edit' and has four tabs: General, Security, QoS, and Advanced. The 'General' tab is active, showing the following configuration:

| | |
|-------------------|---|
| Profile Name | WLAN1 |
| Type | WLAN |
| SSID | WLAN1 |
| Status | <input checked="" type="checkbox"/> Enabled |
| Security Policies | [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface | management |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |

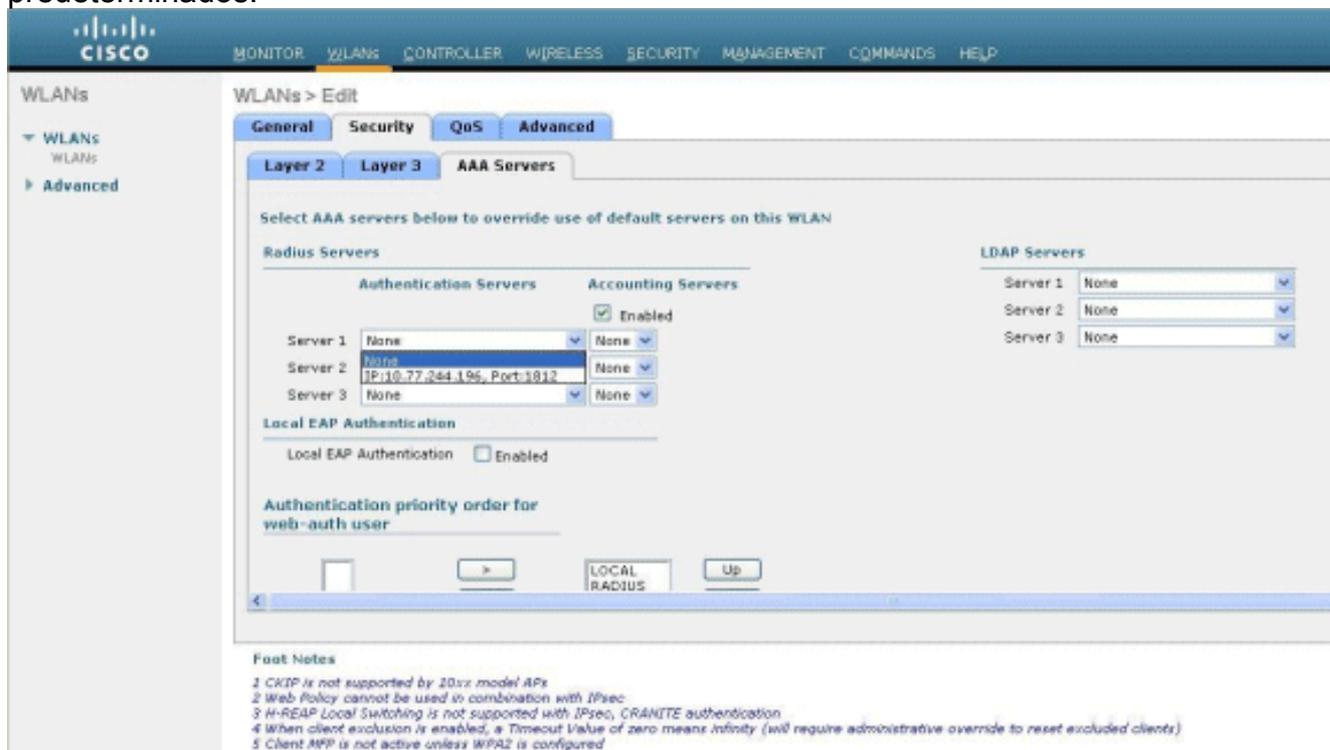
Below the configuration area, there are 'Foot Notes' with the following text:

- 1 CKIP 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

5. Elija una interfaz para la WLAN. Normalmente, una interfaz configurada en una VLAN única se asigna a la WLAN para que el cliente reciba una dirección IP en esa VLAN. En este ejemplo, utilizamos *management* para Interface.
6. Elija la pestaña **Security**.
7. En el menú **Layer 2**, elija **None** para Layer 2 Security.
8. En el menú **Layer 3**, elija **None** para Layer 3 Security. Marque la casilla de verificación **Web Policy** y elija **Authentication**.



9. En el menú **AAA servers**, para Authentication Server, elija el servidor RADIUS que se configuró en este WLC. Otros menús deben permanecer en los valores predeterminados.

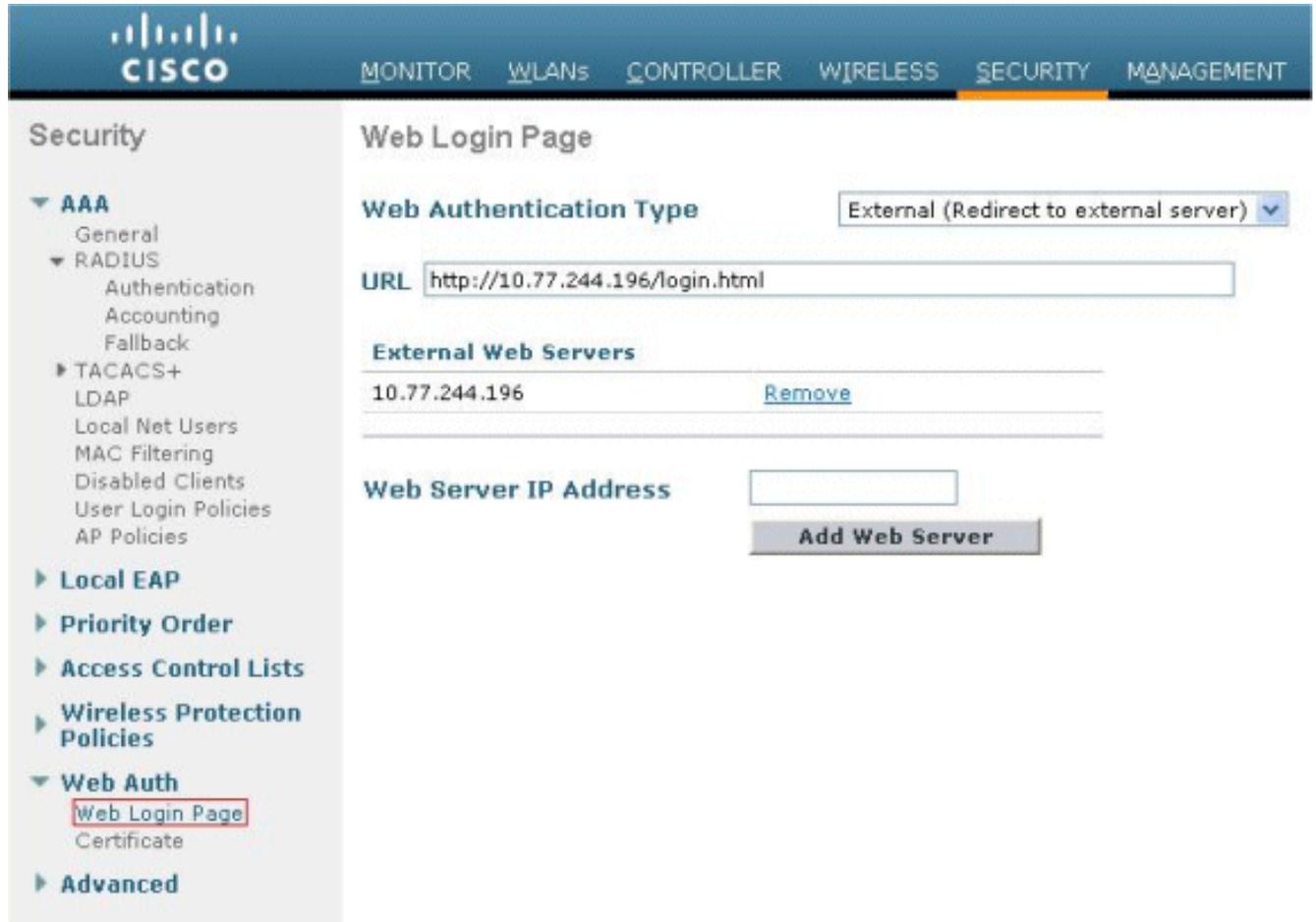


[Configure la información del servidor Web en el WLC](#)

El servidor web que aloja la página de autenticación Web debe configurarse en el WLC. Siga estos pasos para configurar el servidor Web:

1. Haga clic en la ficha Security (Seguridad). Vaya a **Web Auth > Web Login Page**.

2. Establezca el tipo de autenticación Web como **Externa**.
3. En el campo Dirección IP del servidor Web, introduzca la dirección IP del servidor que aloja la página Autenticación Web y haga clic en **Agregar servidor Web**. En este ejemplo, la dirección IP es *10.77.244.196*, que aparece en External Web Servers (Servidores web externos).
4. Introduzca la URL de la página de autenticación Web (en este ejemplo, *http://10.77.244.196/login.html*) en el campo URL.



[Configuración de Cisco Secure ACS](#)

En este documento, asumimos que Cisco Secure ACS Server ya está instalado y ejecutándose en una máquina. Para obtener más información sobre cómo configurar Cisco Secure ACS, consulte la [Guía de Configuración de Cisco Secure ACS 4.2](#).

[Configuración de la información del usuario en Cisco Secure ACS](#)

Realice estos pasos para configurar los usuarios en Cisco Secure ACS:

1. Elija **User Setup** de la GUI de Cisco Secure ACS, ingrese un nombre de usuario y haga clic en **Add/Edit**. En este ejemplo, el usuario es *user1*.



User Setup

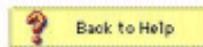
Select



User:

List users beginning with letter/number:

| | | | | | | | | | | | | |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | | | |



- De forma predeterminada, PAP se utiliza para autenticar clientes. La contraseña para el usuario se ingresa en **User Setup > Password Authentication > Cisco Secure PAP**. Asegúrese de elegir **ACS Internal Database** para la autenticación de contraseña.

CISCO SYSTEMS

User Setup

Edit

User: user1 (New User)

Account Disabled

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

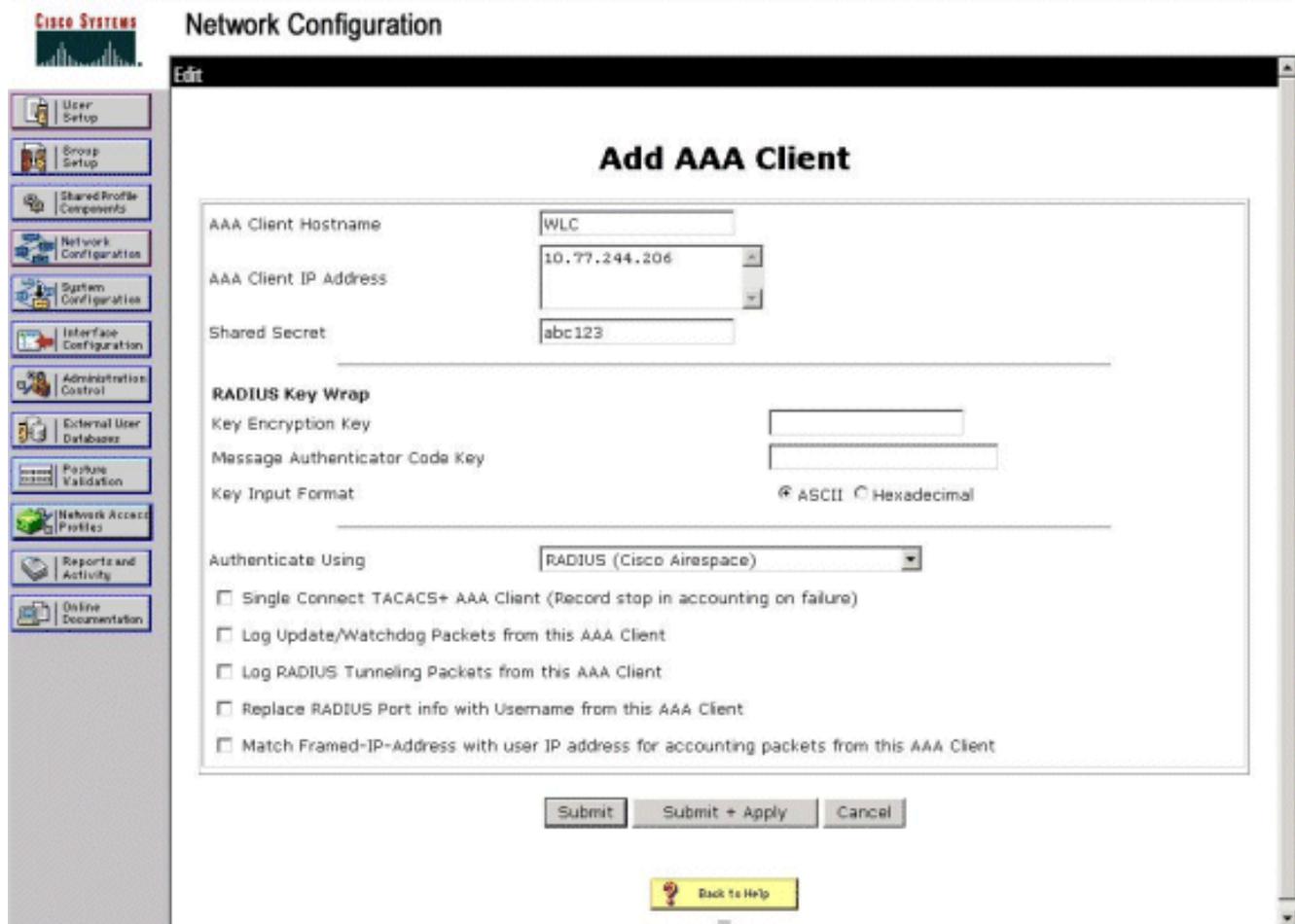
Group to which the user is assigned:

3. El usuario debe tener asignado un grupo al que pertenezca. Elija el **grupo predeterminado**.
4. Haga clic en Submit (Enviar).

[Configuración de la Información de WLC en Cisco Secure ACS](#)

Realice estos pasos para configurar la información del WLC en Cisco Secure ACS:

1. En la GUI de ACS, haga clic en la pestaña **Network Configuration**, y haga clic en **Add Entry**.
2. Aparecerá la pantalla Add AAA client (Agregar cliente AAA).
3. Introduzca el nombre del cliente. En este ejemplo, utilizamos *WLC*.
4. Introduzca la dirección IP del cliente. La dirección IP del WLC es *10.77.244.206*.
5. Introduzca la clave secreta compartida y el formato de la clave. Esto debe coincidir con la entrada hecha en el menú **Seguridad** del WLC.
6. Elija **ASCII** para el formato de entrada de la llave, que debe ser el mismo en el WLC.
7. Elija **RADIUS (Cisco Airespace)** para autenticar usando para fijar el protocolo utilizado entre el WLC y el servidor RADIUS.
8. Haga clic en **Enviar + Aplicar**.

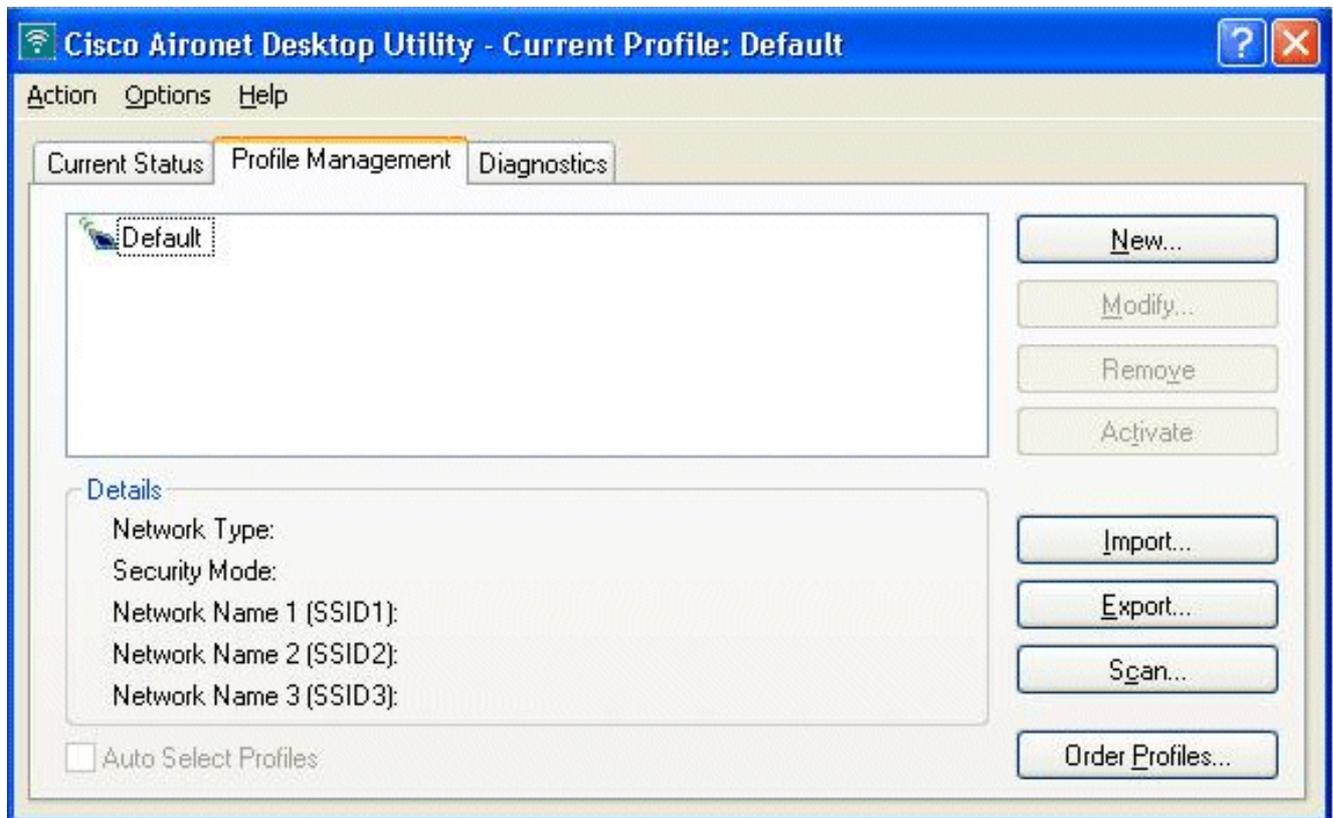


Proceso de autenticación de cliente

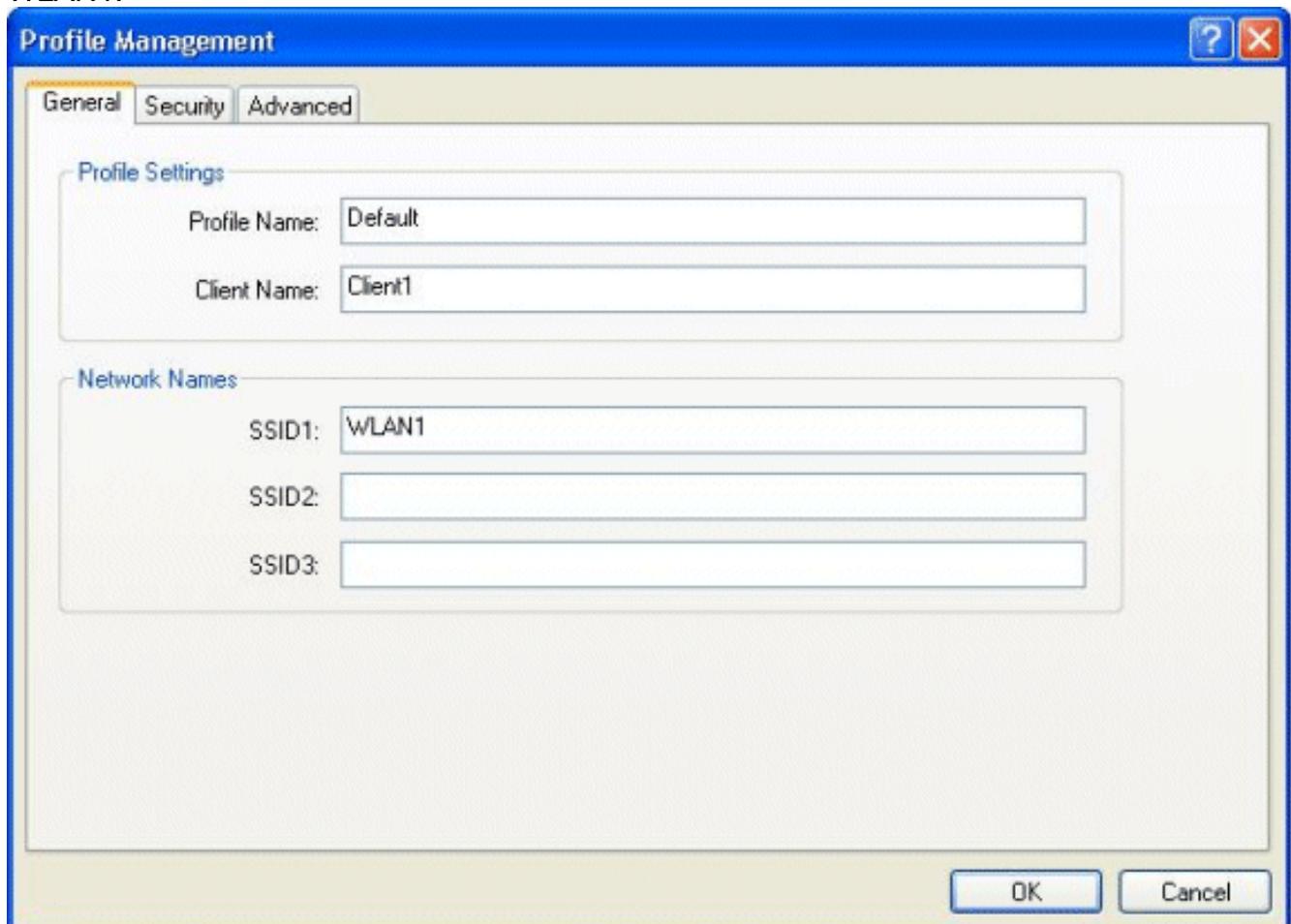
Configuración del Cliente

En este ejemplo, utilizamos Cisco Aironet Desktop Utility para realizar la autenticación web. Realice estos pasos para configurar Aironet Desktop Utility.

1. Abra Aironet Desktop Utility desde Inicio > Cisco Aironet > Aironet Desktop Utility.
2. Haga clic en la pestaña **Profile Management**.

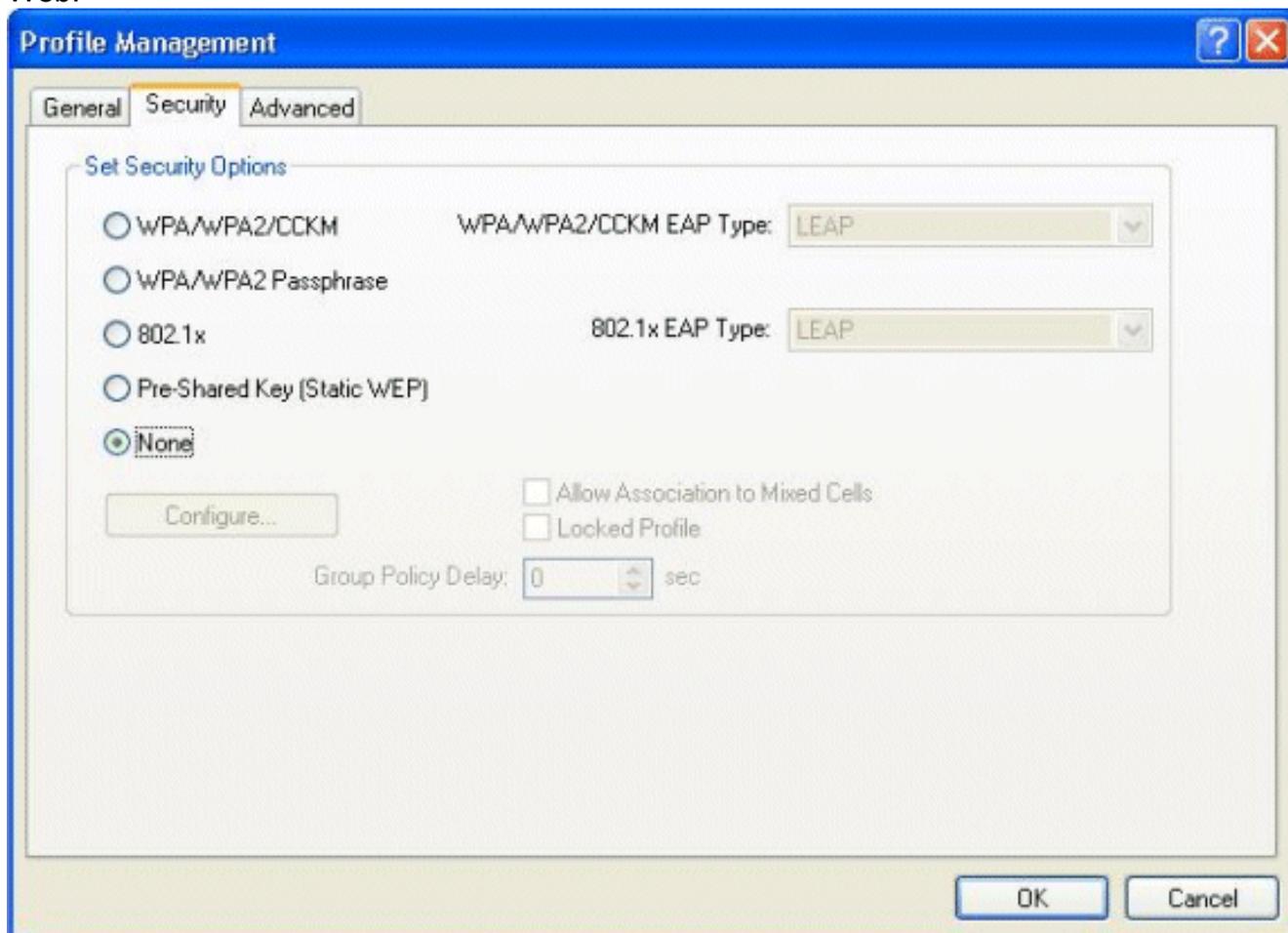


3. Elija el perfil **Default** y haga clic en **Modify**. Haga clic en la ficha **General**. Configure un nombre de perfil. En este ejemplo, se utiliza *Default*. Configure el SSID en Nombres de red. En este ejemplo, se utiliza *WLAN1*.

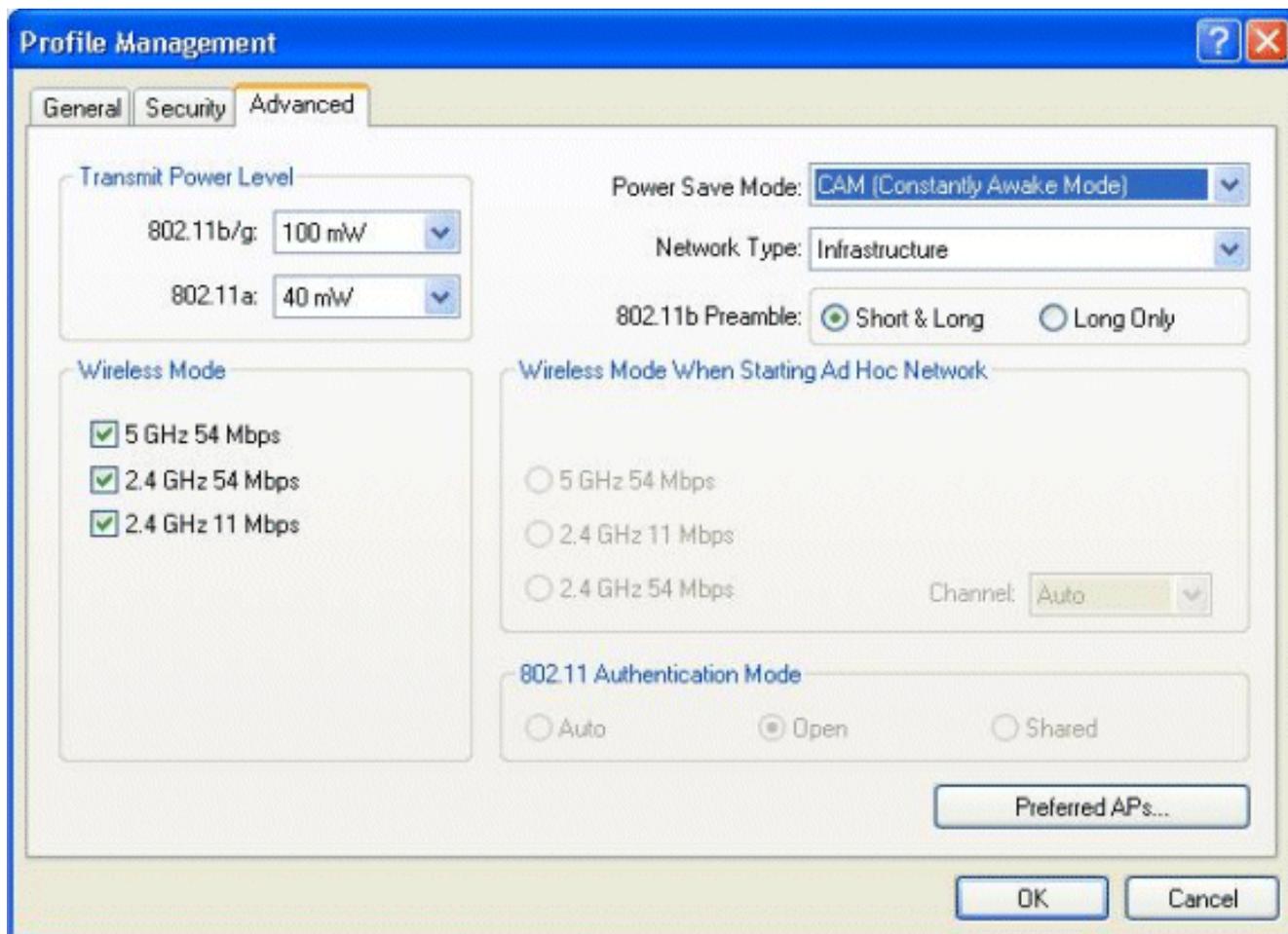


Nota: El SSID distingue entre mayúsculas y minúsculas y debe coincidir con la WLAN configurada en el WLC. Haga clic en la ficha Security (Seguridad). Elija **None** como Security

para la autenticación Web.



Haga clic en la ficha Advanced (Opciones avanzadas). En el menú **Wireless Mode**, elija la frecuencia en la que el cliente inalámbrico se comunica con el LAP. Bajo el **nivel de energía de transmisión**, elija la energía que se configura en el WLC. Deje el valor predeterminado para Modo de ahorro de energía. Elija **Infrastructure** como el tipo de red. Establezca el preámbulo 802.11b como **Short & Long** para una mejor compatibilidad. Click OK.



4. Una vez configurado el perfil en el software cliente, el cliente se asocia correctamente y recibe una dirección IP del conjunto de VLAN configurado para la interfaz de administración.

Proceso de conexión del cliente

Esta sección explica cómo ocurre el login del cliente.

1. Abra un navegador e ingrese cualquier URL o dirección IP. Esto trae la página de autenticación Web al cliente. Si el controlador está ejecutando alguna versión anterior a la 3.0, el usuario debe ingresar `https://1.1.1.1/login.html` para que aparezca la página de autenticación web. Se muestra una ventana de alerta de seguridad.
2. Haga clic en **Sí para continuar**.
3. Cuando aparezca la ventana Login, ingrese el nombre de usuario y la contraseña que está configurada en el servidor RADIUS. Si el inicio de sesión se realiza correctamente, verá dos ventanas del navegador. Una ventana más grande indica que el inicio de sesión se ha realizado correctamente y puede utilizar esta ventana para navegar por Internet. Use la ventana más pequeña para cerrar la sesión cuando deje de usar la red del



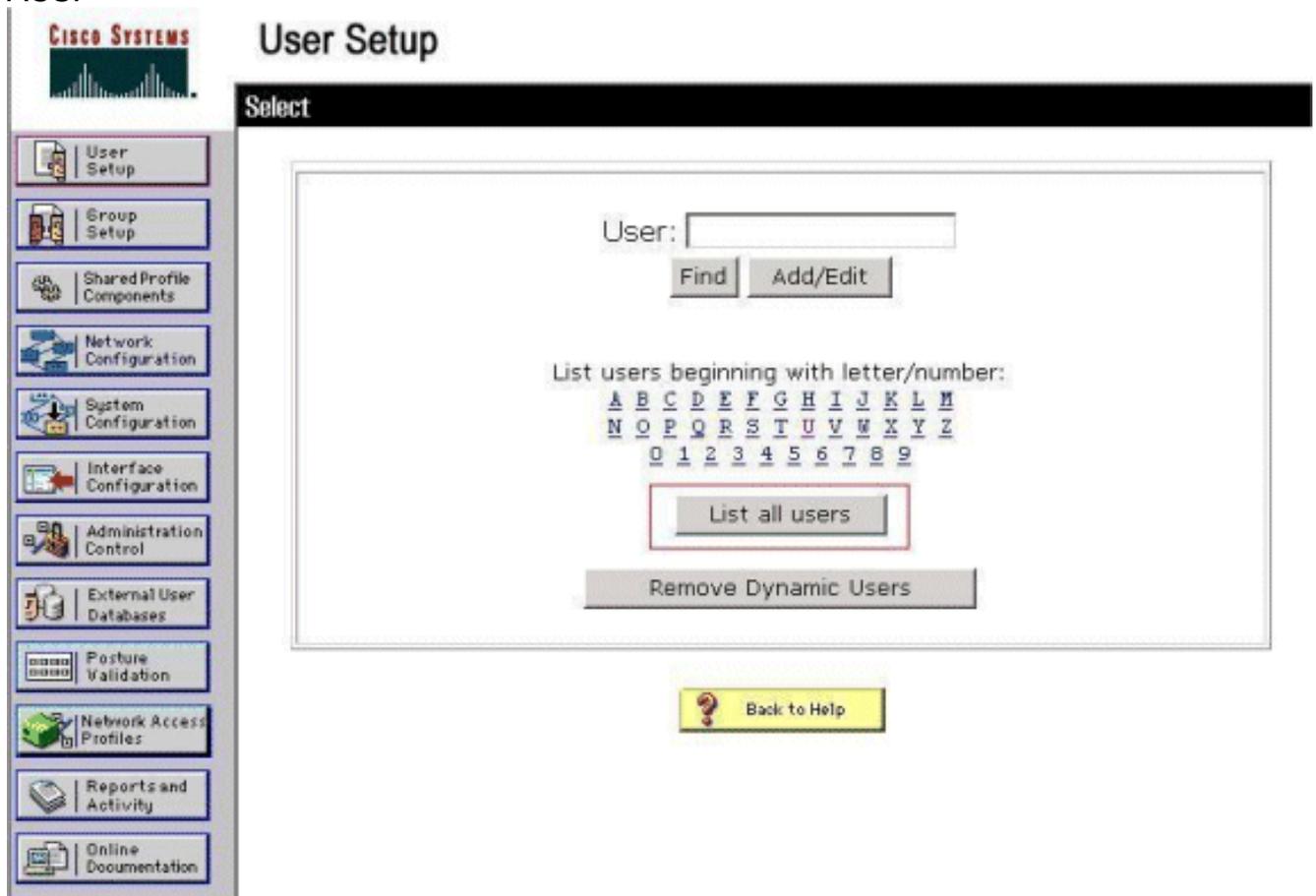
invitado.

Verificación

Para que la autenticación web sea correcta, debe comprobar si los dispositivos están configurados de forma adecuada. Esta sección explica cómo verificar los dispositivos utilizados en el proceso.

Verificación de ACS

1. Haga clic en **User Setup**, y luego haga clic en **List All Users** en la GUI de ACS.



Asegúrese de que el estado del usuario es *Habilitado* y que el grupo Predeterminado está asignado al usuario.

User List

| User | Status | Group | Network Access Profile |
|-----------------------|---------|-------------------------|------------------------|
| user1 | Enabled | Default Group (2 users) | (Default) |

- Haga clic en la pestaña **Network Configuration** y busque en la tabla **AAA Clients** para verificar que el WLC está configurado como un cliente AAA.

The screenshot shows the Cisco WLC Network Configuration page. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Profile Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and has a 'Select' dropdown. It contains three tables:

- AAA Clients:** A table with columns 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. It contains one entry: 'wlc1' with IP '10.77.244.206' and 'RADIUS (Cisco Airespace)'. Below the table are 'Add Entry' and 'Search' buttons.
- AAA Servers:** A table with columns 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type'. It contains one entry: 'TS-Web' with IP '10.77.244.196' and 'CiscoSecure ACS'. Below the table are 'Add Entry' and 'Search' buttons.
- Proxy Distribution Table:** A table with columns 'Character String', 'AAA Servers', 'Strip', and 'Account'. It contains one entry: '(Default)' with 'TS-Web', 'No', and 'Local'. Below the table are 'Add Entry' and 'Sort Entries' buttons.

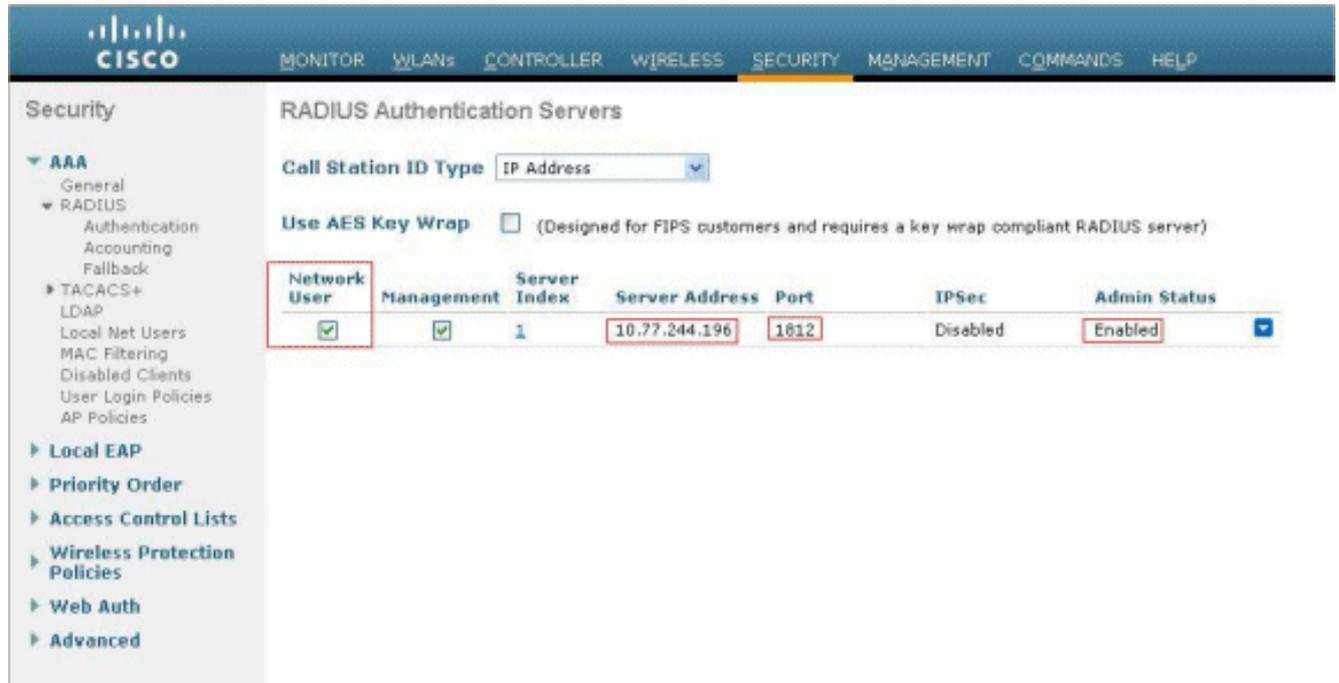
At the bottom of the main content area is a 'Back to Help' button.

Verificar WLC

- Haga clic en el menú **WLANs** de la GUI del WLC. Asegúrese de que la WLAN utilizada para la autenticación Web aparezca en la página. Asegúrese de que el estado del administrador para la WLAN esté *habilitado*. Asegúrese de que la Política de Seguridad para la WLAN muestre *Web-Auth*.

The screenshot shows the Cisco WLC GUI. The top navigation bar includes 'MONITOR', 'WLANs' (highlighted), 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with a dropdown arrow, 'WLANs', and 'Advanced'. The main content area is titled 'WLANs' and contains a table with columns 'Profile Name', 'Type', 'WLAN SSID', 'Admin Status', and 'Security Policies'. It contains one entry: 'WLAN1' with Type 'WLAN', WLAN SSID 'WLAN1', Admin Status 'Enabled', and Security Policies 'Web-Auth'. The 'WLAN1', 'Enabled', and 'Web-Auth' cells are highlighted with red boxes.

- Haga clic en el menú **SECURITY** de la GUI del WLC. Asegúrese de que Cisco Secure ACS (10.77.244.196) aparece en la página. Asegúrese de que la casilla Network User (Usuario de red) está activada. Asegúrese de que el puerto sea 1812 y que el estado del administrador sea *Enabled*.



Troubleshoot

Hay muchas razones por las que una autenticación web no es exitosa. El documento [Troubleshooting Web Authentication on a Wireless LAN Controller \(WLC\)](#) explica claramente esas razones en detalle.

Comandos para resolución de problemas

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

Telnet en el WLC y ejecute estos comandos para resolver problemas de autenticación:

- **debug aaa all enable**

```

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00 00 00 00 00 00 0
0 00 ...s.....
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73 65 72 31 02 12 93 c
3 66 .....user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010: structureSize.....89
Fri Sep 24 13:59:52 2010: resultCode.....0
Fri Sep 24 13:59:52 2010: protocolUsed.....0x0

```

```

0000001
Fri Sep 24 13:59:52 2010:      proxyState.....00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:      Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:      AVP[01] Framed-IP-Address.....
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[02] Class.....
.....CACs:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for station
00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
                qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:      Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:      AVP[01] User-Name.....
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:      AVP[02] Nas-Port.....
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[03] Nas-IP-Address.....
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[04] Framed-IP-Address.....
.....0x0a4df4c7 (172881095) (4 bytes)

```

- **debug aaa detail enable**

Los intentos de autenticación fallidos se enumeran en el menú ubicado en **Informes y Actividad > Intentos fallidos**.

[Información Relacionada](#)

- [Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico](#)
- [Troubleshooting de autenticación Web en controlador LAN inalámbrico](#)
- [Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica](#)
- [Ejemplo de Configuración de Autenticación Web Usando LDAP en Controladores LAN Inalámbricos \(WLCs\)](#)
- [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).