Autenticación del Web externa usando un servidor de RADIUS

Contenido

Introducción

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

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los Puntos de acceso ligeros (revestimientos) y

del WLCs de Cisco
- Conocimiento de cómo configurar y configurar a un servidor Web externo
- Conocimiento de cómo configurar el Cisco Secure ACS

Componentes Utilizados

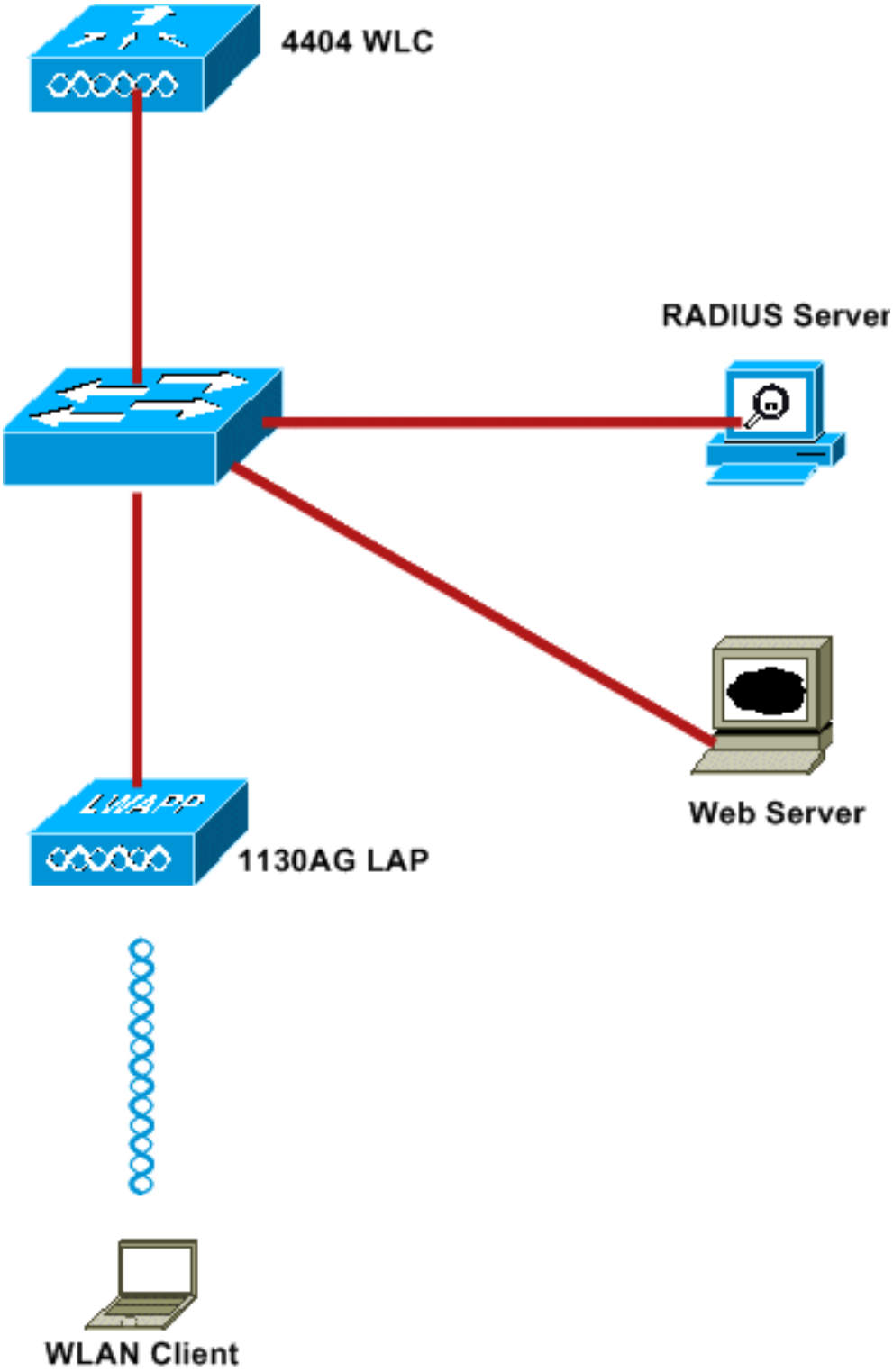
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Regulador del Wireless LAN que funciona con la versión de firmware 5.0.148.0
- REVESTIMIENTO de las Cisco 1232 Series
- Adaptador de red inalámbrica de cliente 3.6.0.61 de Cisco 802.11a/b/g
- Servidor Web externo que recibe la página de registro de la autenticación Web
- Versión del Cisco Secure ACS que funciona con 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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 REVESTIMIENTO 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 ACS de Cisco utiliza la dirección IP 10.77.244.196
- El cliente recibe una dirección IP de la interfaz de administración que se asocia a la red inalámbrica (WLAN) - 10.77.244.208

Convenciones

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

Autenticación del Web externa

La autenticación Web es un mecanismo de autenticación de la capa 3 usado para autenticar a los Usuarios invitados para el acceso a internet. Los usuarios autenticados usando este proceso no podrán acceder Internet hasta que completen con éxito el proceso de autenticación. Para toda la información sobre el proceso de autenticación del Web externa, lea el proceso de autenticación del Web externa de la sección de la autenticación del Web externa del documento con el ejemplo de configuración de los reguladores del Wireless LAN.

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

Configure el WLC

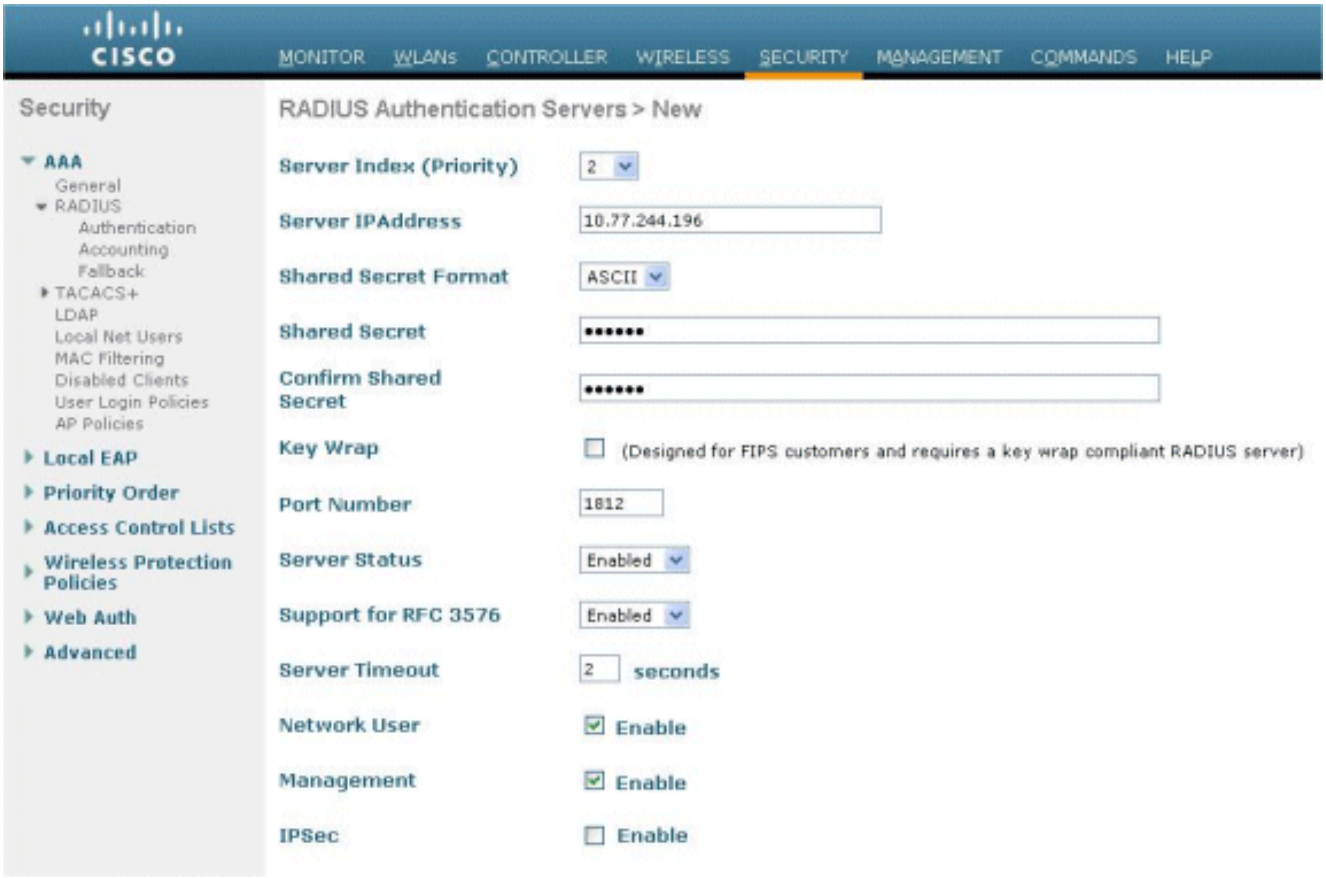
En este documento, asumimos que el WLC está configurado y tiene ya un REVESTIMIENTO registrado al WLC. Este documento más futuro asume que el WLC está configurado para la operación básica y que los revestimientos están registrados al WLC. Si usted es usuario nuevo que intenta configurar el WLC para la operación básica con los revestimientos, refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC). Para ver los revestimientos que se registran al WLC, navegue a la **Tecnología inalámbrica > todos los AP**.

Una vez que el WLC se configura para la operación básica y tiene uno o más revestimientos registradoes a ella, usted puede configurar el WLC para la autenticación del Web externa usando un servidor Web externo. En nuestro ejemplo, estamos utilizando una versión 4.1.1.24 del Cisco Secure ACS como el servidor de RADIUS. Primero, configuraremos el WLC para este servidor de RADIUS, y entonces miraremos la configuración requerida en el Cisco Secure ACS para esta configuración.

Configure el WLC para el Cisco Secure ACS

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

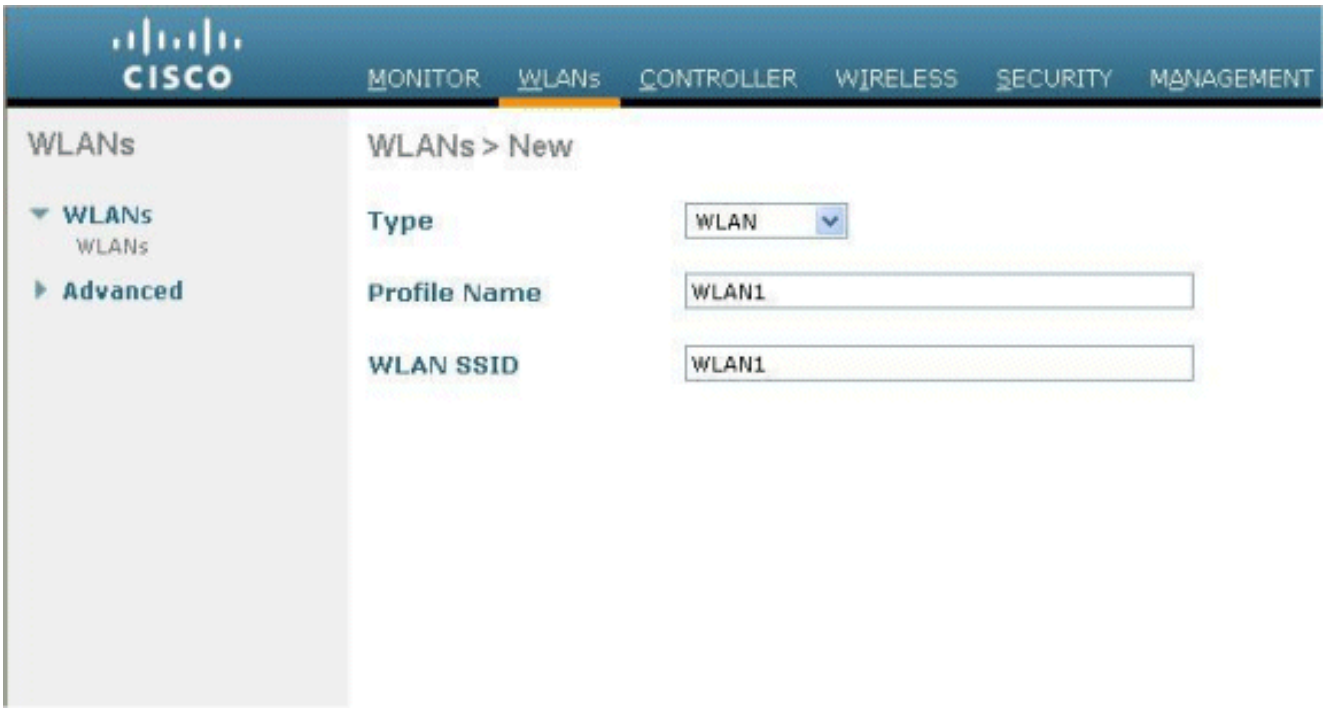
1. Del WLC GUI, haga clic el **menú de seguridad**.
2. Bajo **menú AAA**, navegue al submenú del **radio >** de la **autenticación**.
3. Haga clic **nuevo**, y ingrese el IP Address del servidor de RADIUS. En este ejemplo, la dirección IP del servidor es *10.77.244.196*.
4. Ingrese el secreto compartido en el WLC. El secreto compartido se debe configurar lo mismo en el WLC.
5. Elija el **ASCII** o **embruje** para el formato del secreto compartido. El mismo formato necesita ser elegido en el WLC.
6. **1812** es el número del puerto usado para la autenticación de RADIUS.
7. Asegúrese de que la opción del estado del servidor esté fijada a **habilitado**.
8. Marque el cuadro del **permiso del** usuario de la red para autenticar a los usuarios de la red.
9. Haga clic en Apply
   (Aplicar).



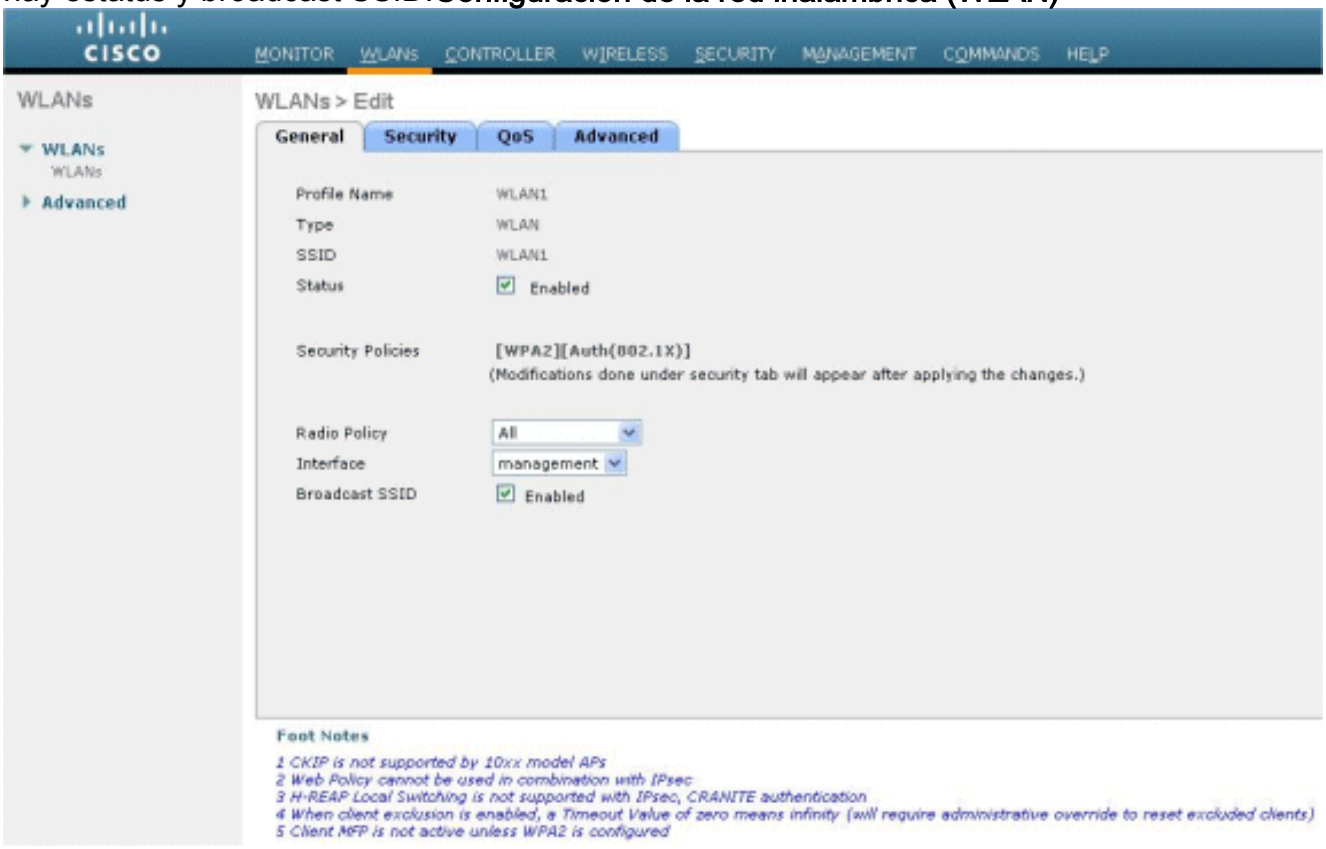
Configure la red inalámbrica (WLAN) en el WLC para la autenticación Web

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

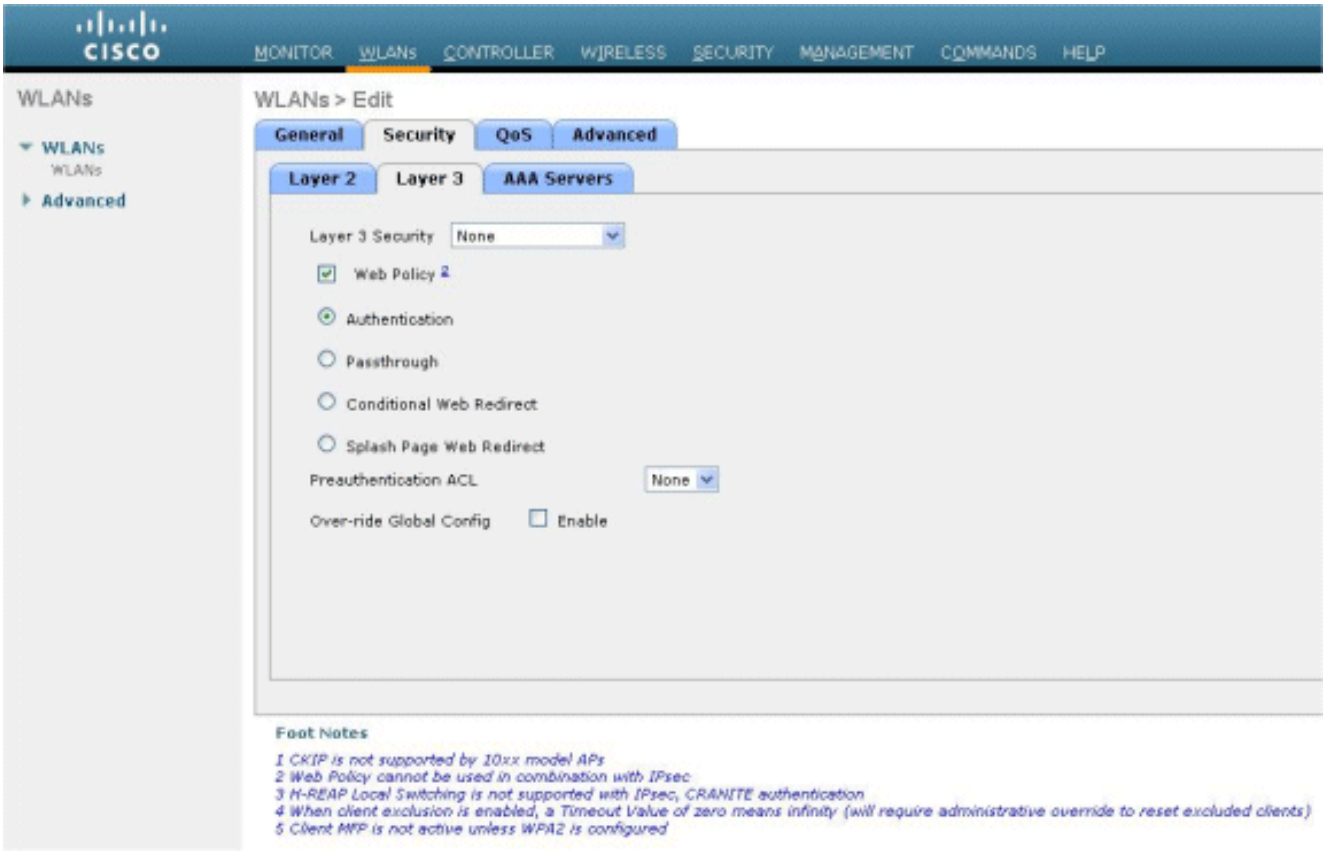
1. Haga clic el menú **WLAN del** regulador GUI, y elija **nuevo**.
2. Elija la **red inalámbrica (WLAN)** para el tipo.
3. Ingrese un nombre del perfil y un WLAN SSID de su opción, y el tecleo **se aplica**.**Note**: La red inalámbrica (WLAN) SSID es con diferenciación entre mayúsculas y minúsculas.



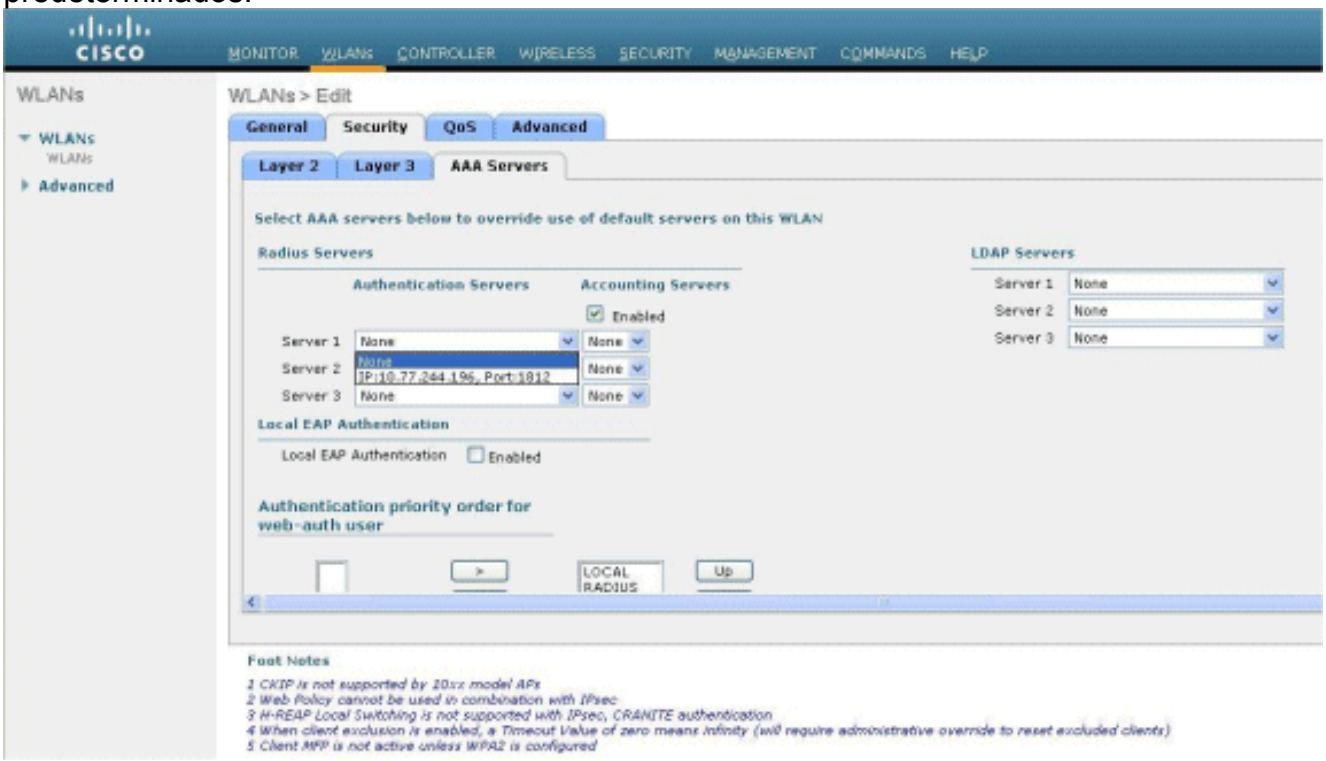
4. Conforme a la **ficha general**, aseegurese que la opción **habilitada** está marcada para saber si hay estatus y broadcast SSID.**Configuración de la red inalámbrica (WLAN)**



5. Elija una interfaz para la red inalámbrica (WLAN). Típicamente, una interfaz configurada en un VLA N único se asocia a la red inalámbrica (WLAN) de modo que el cliente reciba una dirección IP en ese VLA N. En este ejemplo, utilizamos la *Administración* para la interfaz.
6. Elija la **ficha de seguridad**.
7. Bajo menú de la **capa 2**, no elija **ninguno** para la Seguridad de la capa 2.
8. Bajo menú de la **capa 3**, no elija **ninguno** para la Seguridad de la capa 3. Marque la **casilla de verificación Web Policy**, y elija la **autenticación**.



9. Bajo menú de los **servidores de AAA**, para el servidor de autenticación, elija al servidor de RADIUS que fue configurado en este WLC. Otros menús deben permanecer en los valores predeterminados.

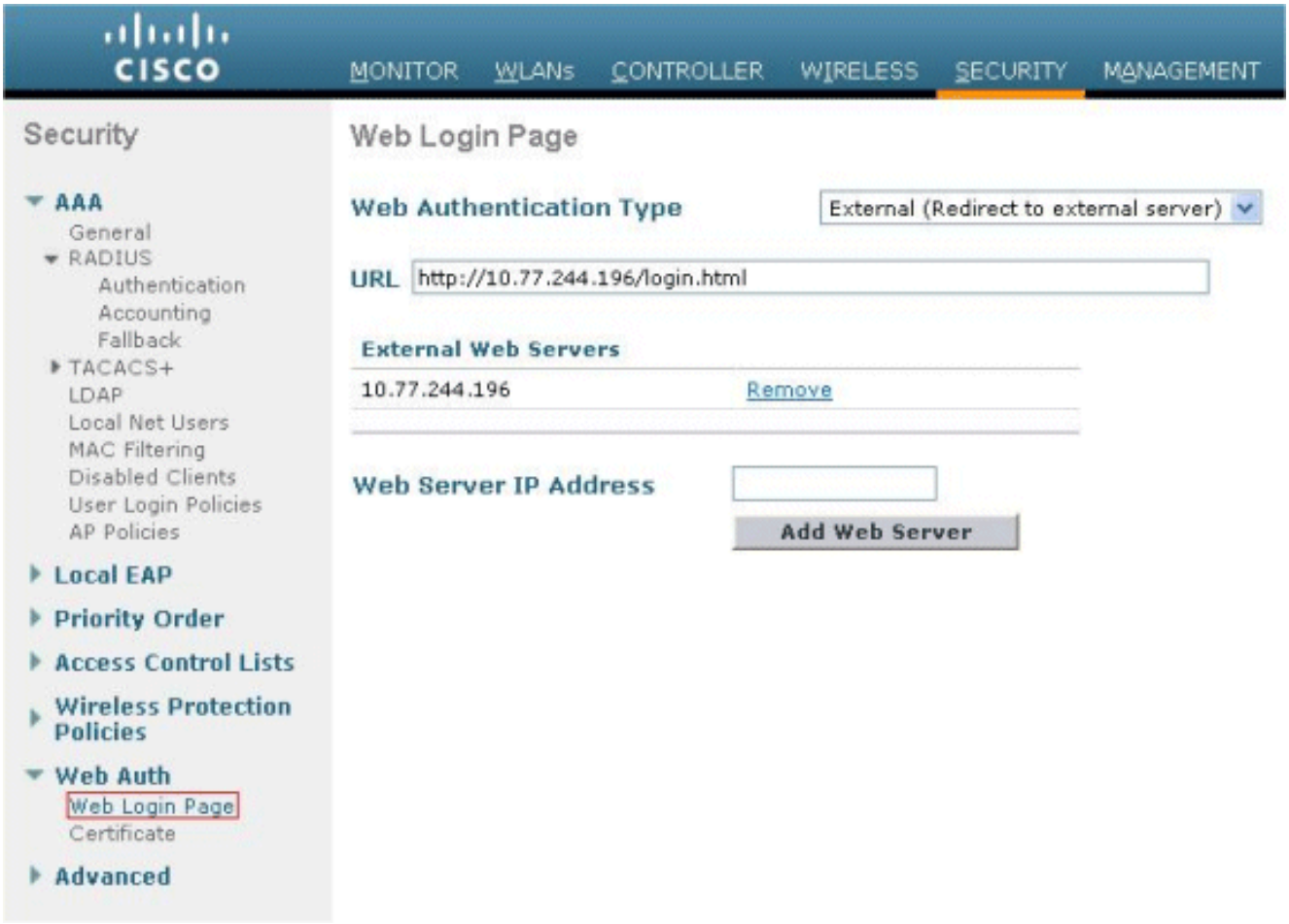


Configure la información del servidor Web sobre el WLC

El servidor Web que recibe la página de la autenticación Web debe ser configurado en el WLC. Realice estos pasos para configurar al servidor Web:

1. Haga clic la **Seguridad** cuadro van al **auth de la red >** a la **página de registro de la red**.

2. Fije el tipo de la autenticación Web como **externo**.
3. En el campo del IP Address del servidor Web, ingrese el IP Address del servidor que recibe la página de la autenticación Web, y el tecleo **agrega al servidor Web**. En este ejemplo, la dirección IP es *10.77.244.196*, que aparece bajo los servidores Web externos.
4. Ingrese el URL para la página de la autenticación Web (en este ejemplo, *http://10.77.244.196/login.html)* en el campo URL.



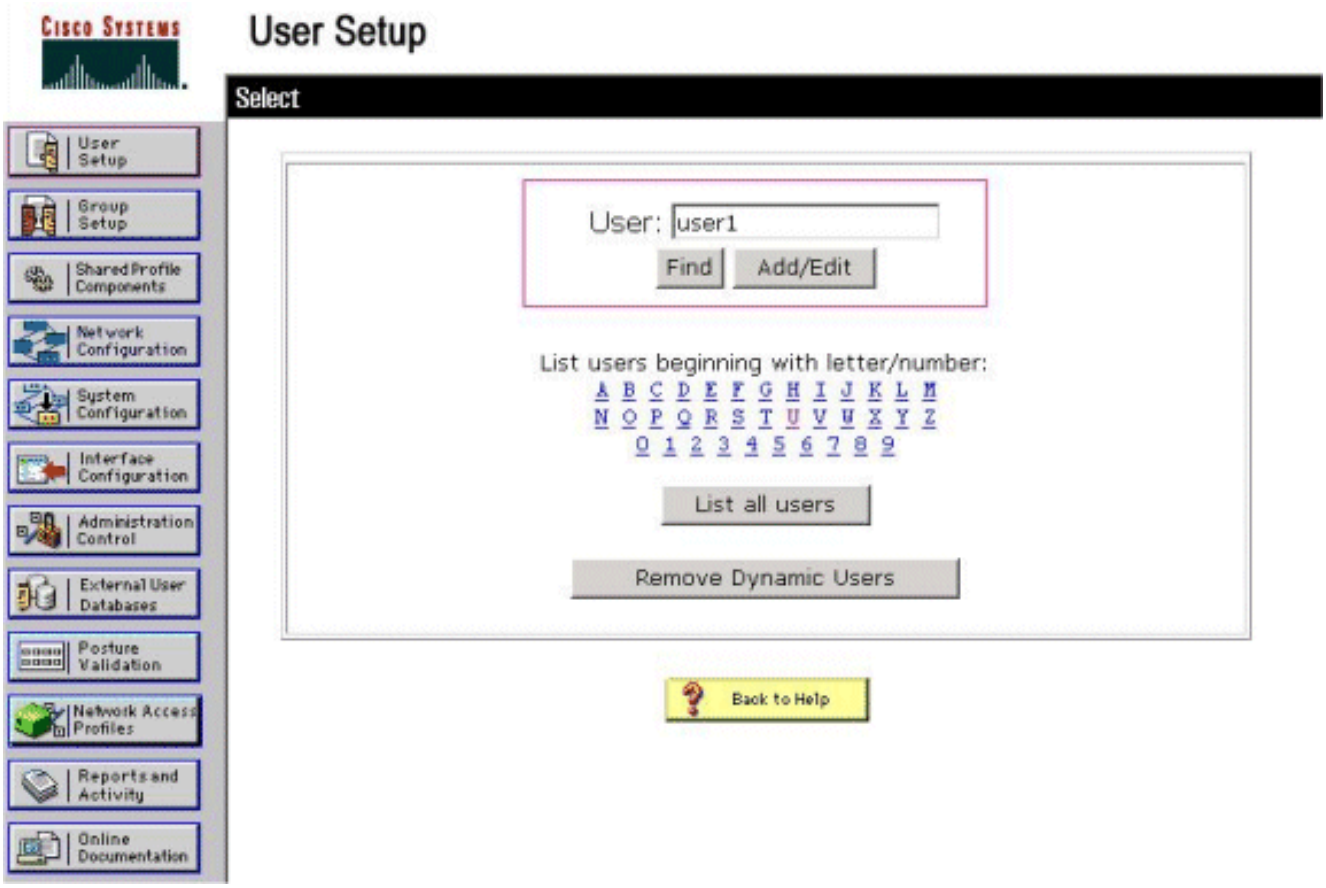
Configure el Cisco Secure ACS

En este documento asumimos que el servidor del Cisco Secure ACS es instalado ya y que se ejecuta en una máquina. Para más información cómo poner el Cisco Secure ACS refiera a la guía de configuración para el Cisco Secure ACS 4.2.

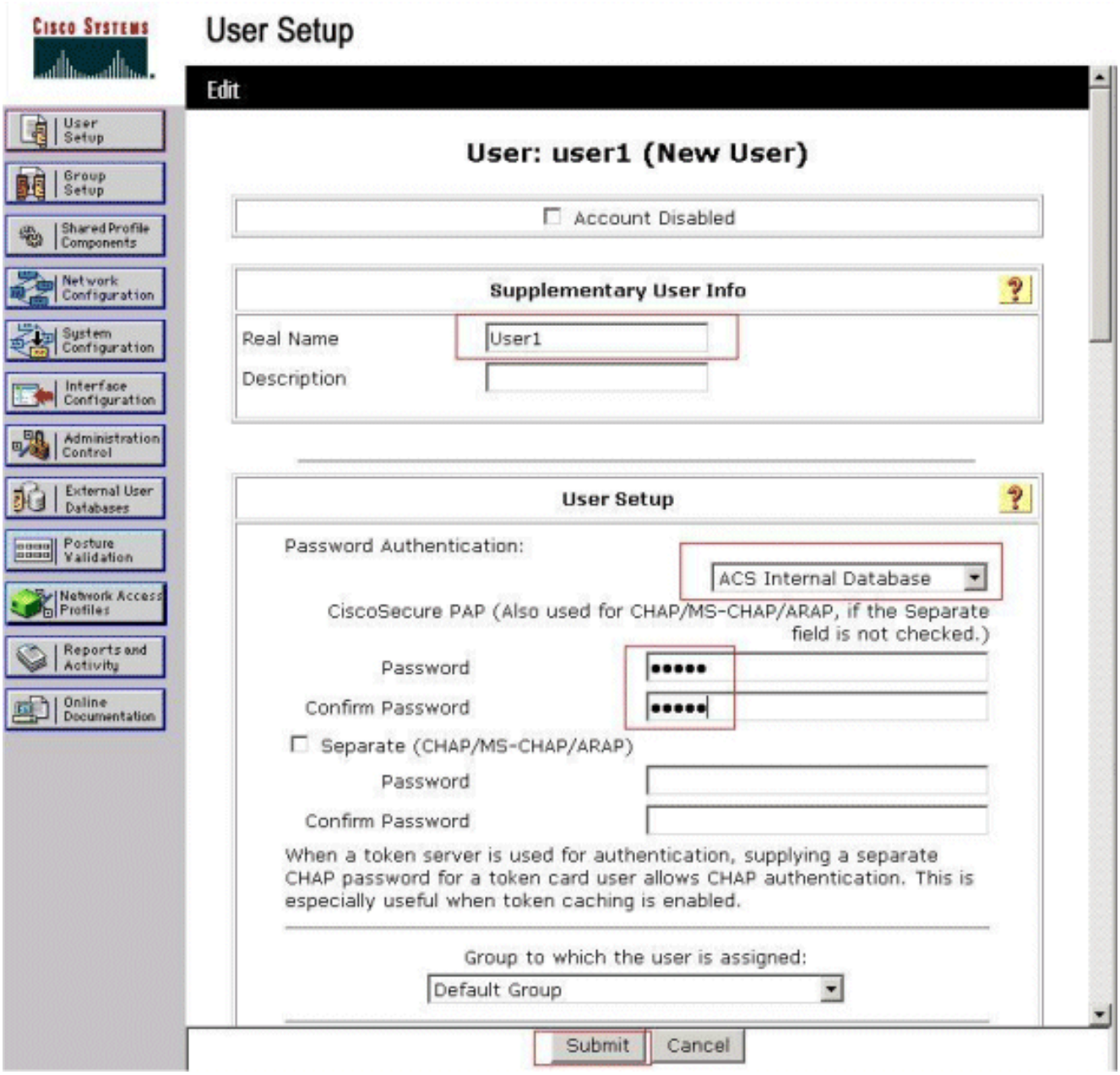
Configure la información del usuario en el Cisco Secure ACS

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

1. Elija la **configuración de usuario del** Cisco Secure ACS GUI, ingrese un nombre de usuario, y el tecleo **agrega/edita**. En este ejemplo, el usuario es *user1*.



2. Por abandono, el PAP se utiliza para los clientes de autenticidad. La contraseña para el usuario se ingresa bajo la **configuración de usuario** > la **autenticación de contraseña > Cisco PAP seguro**. Aseegurese le elegir la **base de datos interna ACS** para la autenticación de contraseña.



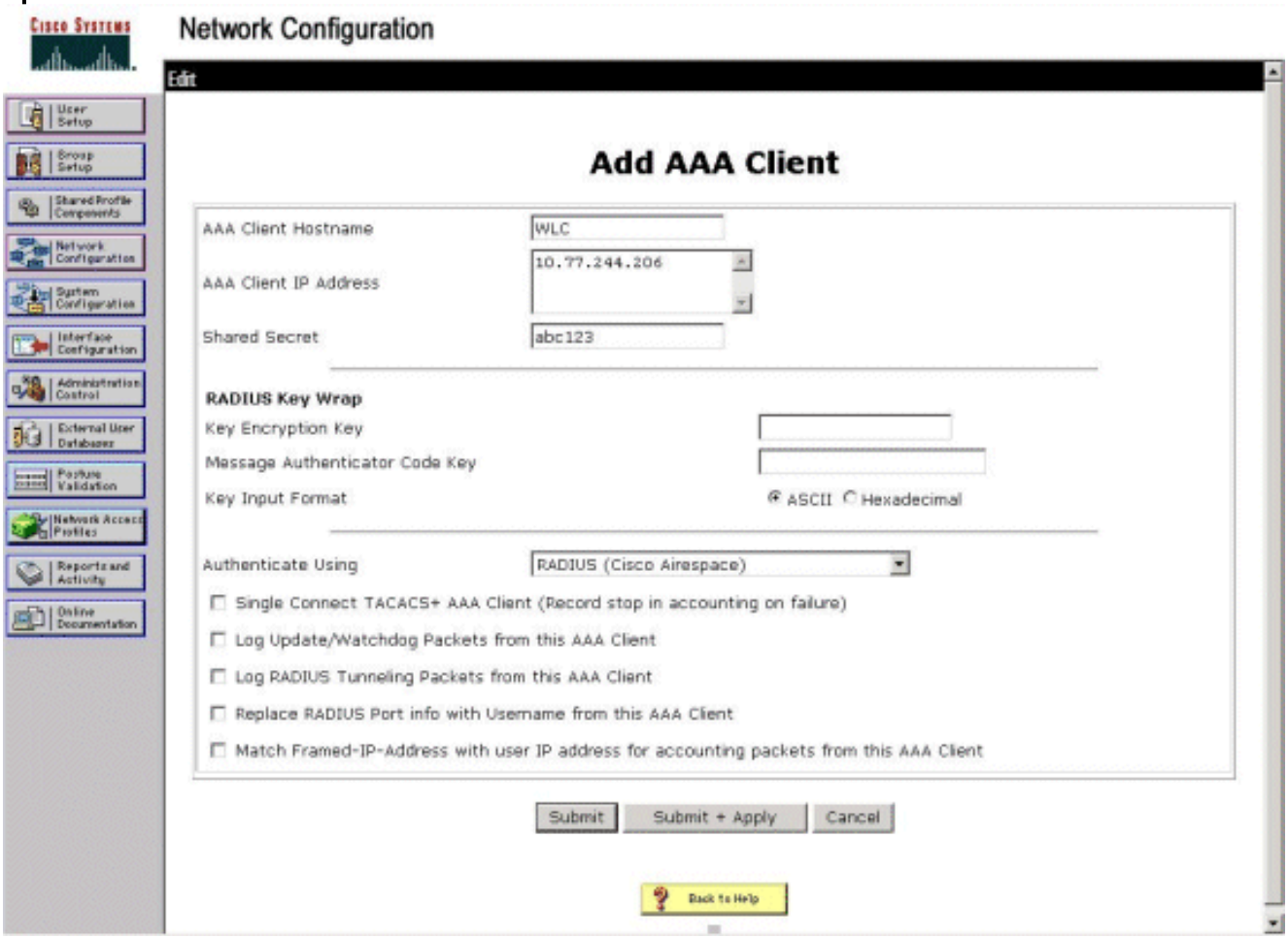
3. El usuario necesita ser asignado un grupo a quien el usuario pertenece. Elija al **grupo predeterminado**.
4. Haga clic en Submit (Enviar).

Configure la información del WLC sobre el Cisco Secure ACS

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

1. En el ACS GUI, haga clic la lengueta de la **configuración de red**, y el tecleo **agrega la entrada**.
2. La pantalla del cliente AAA del agregar aparece.
3. Ingrese el nombre del cliente. En este ejemplo, utilizamos el *WLC*.
4. Ingrese el IP Address del cliente. La dirección IP WLC es *10.77.244.206*.
5. Ingrese la clave secreta compartida y el formato dominante. Esto debe hacer juego la entrada hecha en el **menú de seguridad** WLC.
6. Elija el **ASCII** para el formato de la entrada dominante, que debe ser lo mismo en el WLC.
7. Elija **RADIUS (Airespace de Cisco)** para Authenticate usando para fijar el protocolo utilizado entre el WLC y el servidor de RADIUS.

8. El tecleo **somete + se aplica**.

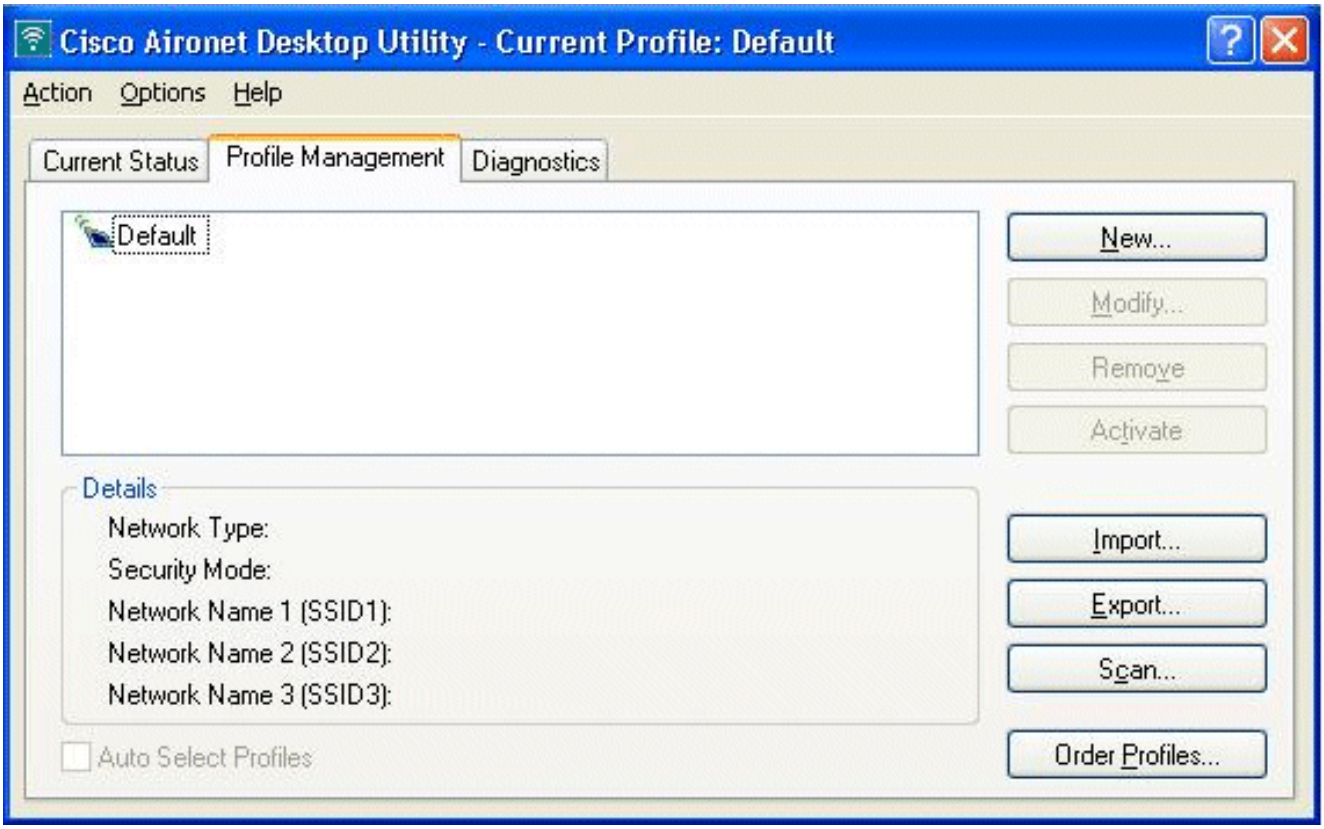


Proceso de autenticación de cliente

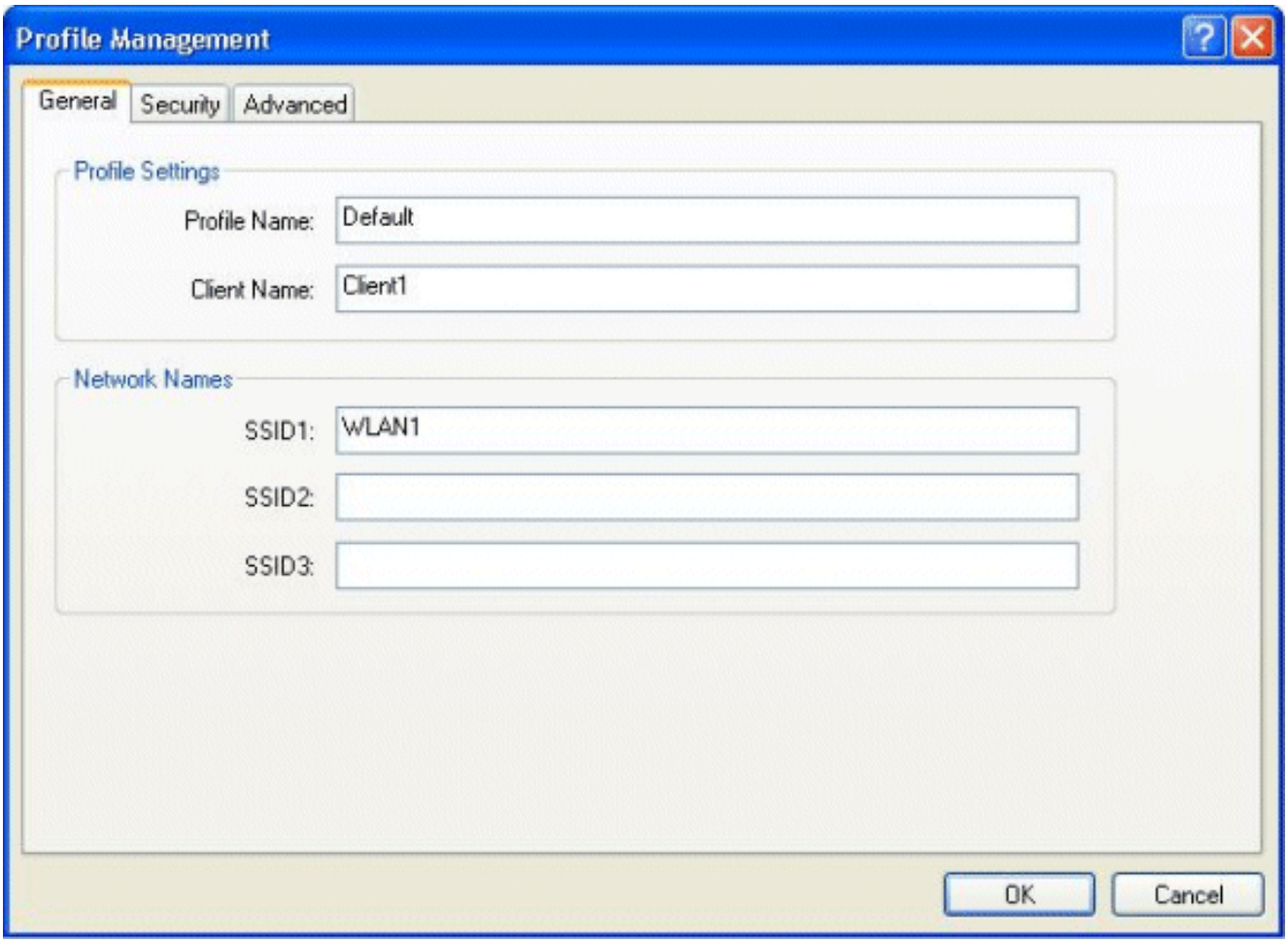
Configuración del Cliente

En este ejemplo, utilizamos la utilidad de escritorio del Cisco Aironet para realizar la autenticación Web. Realice estos pasos para configurar utilidad Aironet Desktop.

1. Abra utilidad Aironet Desktop del **comienzo** > del **Cisco Aironet** > **utilidad Aironet Desktop**.
2. Haga clic en la lengueta de la **Administración del perfil**.

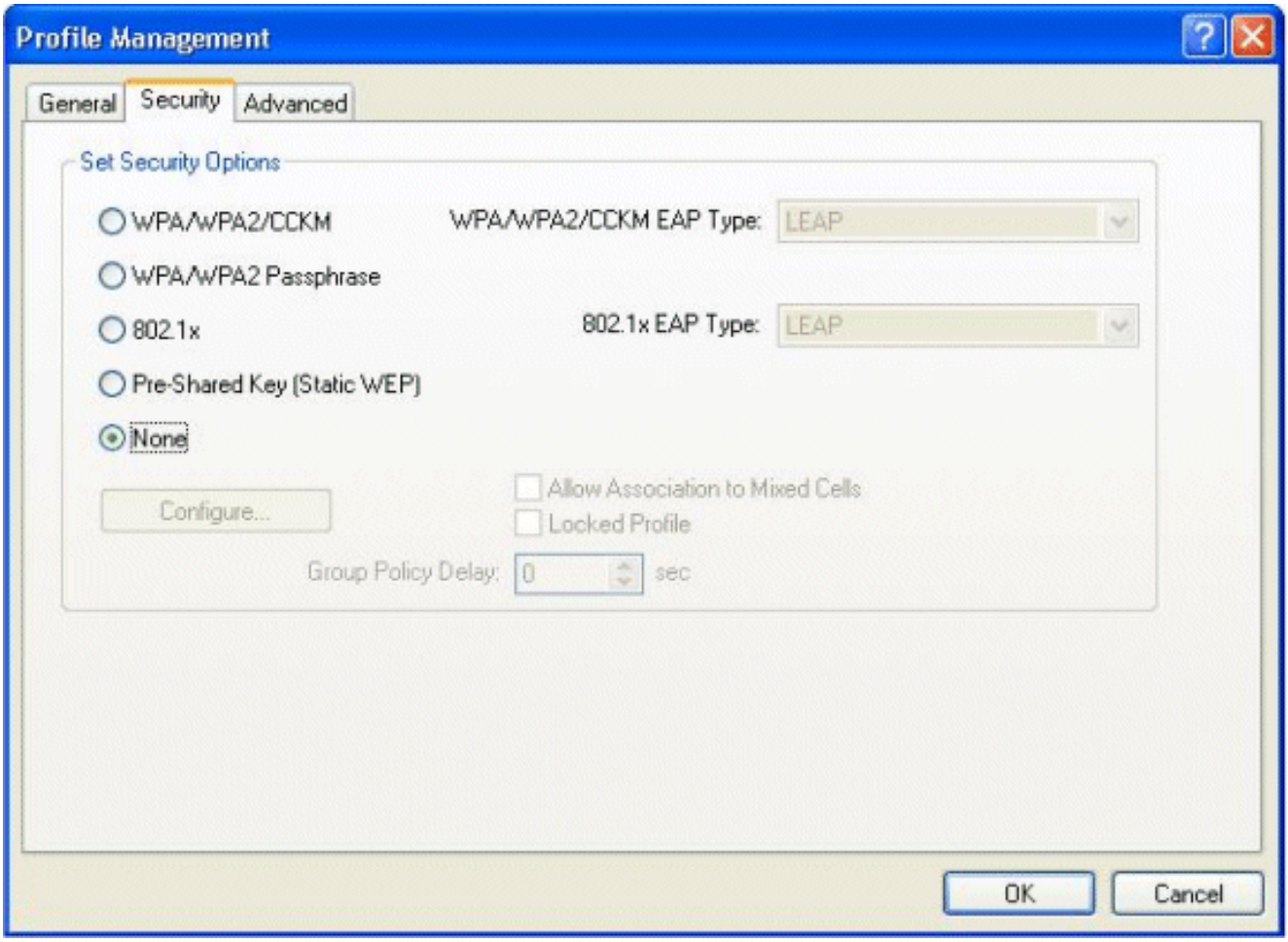


3. Elija el **perfil predeterminado**, y el tecleo **se modifica**.Haga clic la **ficha general**.Configure un nombre del perfil. En este ejemplo, se utiliza el *valor por defecto*.Configure el SSID bajo nombres de red. En este ejemplo, se utiliza *WLAN1*.

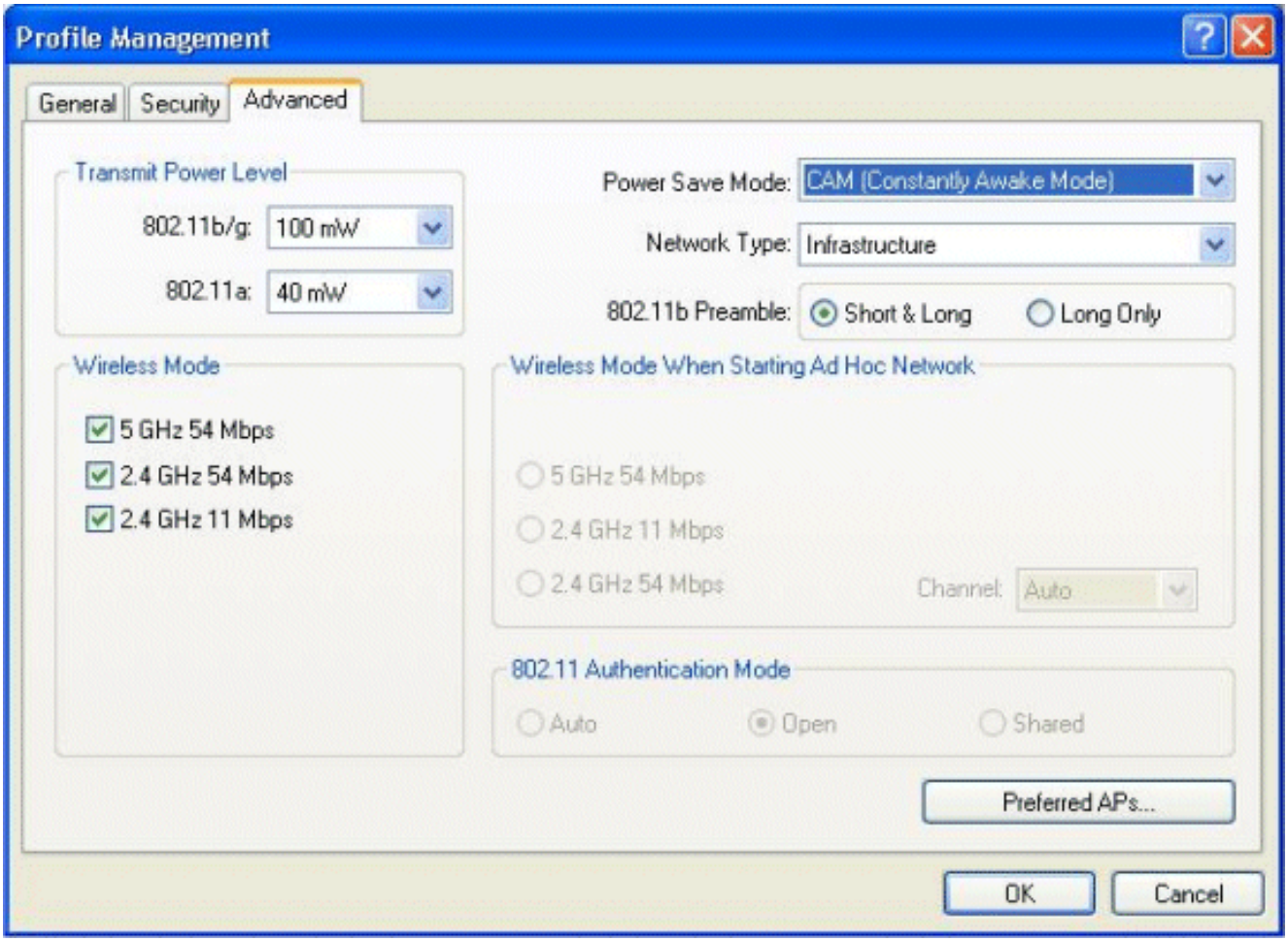


Note: El SSID es con diferenciación entre mayúsculas y minúsculas y debe hacer juego la red inalámbrica (WLAN) configurada en el WLC.Haga clic en la ficha Security

(Seguridad).No elija **ninguno** como Seguridad para la autenticación Web.



Haga clic en la ficha Advanced (Opciones avanzadas).Bajo menú **inalámbrico del modo**, elija la frecuencia en la cual el cliente de red inalámbrica comunica con el REVESTIMIENTO.Bajo **nivel de potencia de transmisión**, elija el poder que se configura en el WLC.Deje el valor predeterminado para el modo de ahorro de energía.Elija la **infraestructura** como el tipo de red.Fije el preámbulo del 802.11b como **cortocircuito y largo** para una mejor compatibilidad.Click OK.



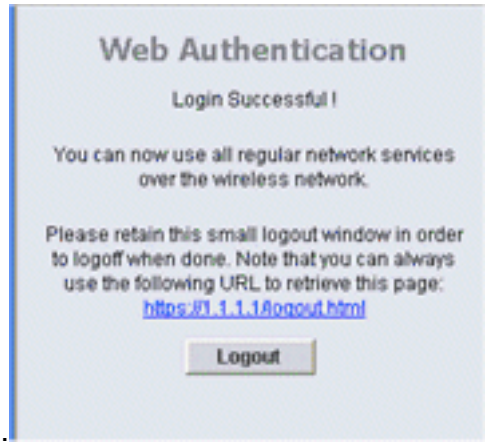
4. Una vez que el perfil se configura en el software de cliente, asocian con éxito y recibe al cliente una dirección IP del pool del VLA N configurado para la interfaz de administración.

Proceso de la conexión con el sistema cliente

Esta sección explica cómo ocurre la conexión con el sistema cliente.

1. Abra una ventana del buscador y ingrese cualquier URL o IP Address. Esto trae la página de la autenticación Web al cliente. Si el regulador está funcionando con cualquier versión anterior que el 3.0, el usuario debe ingresar *https://1.1.1.1/login.html* para traer para arriba la página de la autenticación Web. Se muestra una ventana de alerta de seguridad.
2. Haga clic en **Sí** para continuar.
3. Cuando aparece la ventana del login, ingrese el nombre de usuario y contraseña que se configura en el servidor de RADIUS. Si su login es acertado, usted verá dos ventanas del buscador. La ventana más grande indica la registración satisfactoria, y le puede esta ventana hojear Internet. Use la ventana más pequeña para cerrar la sesión cuando deje de

usar la red del invitado.

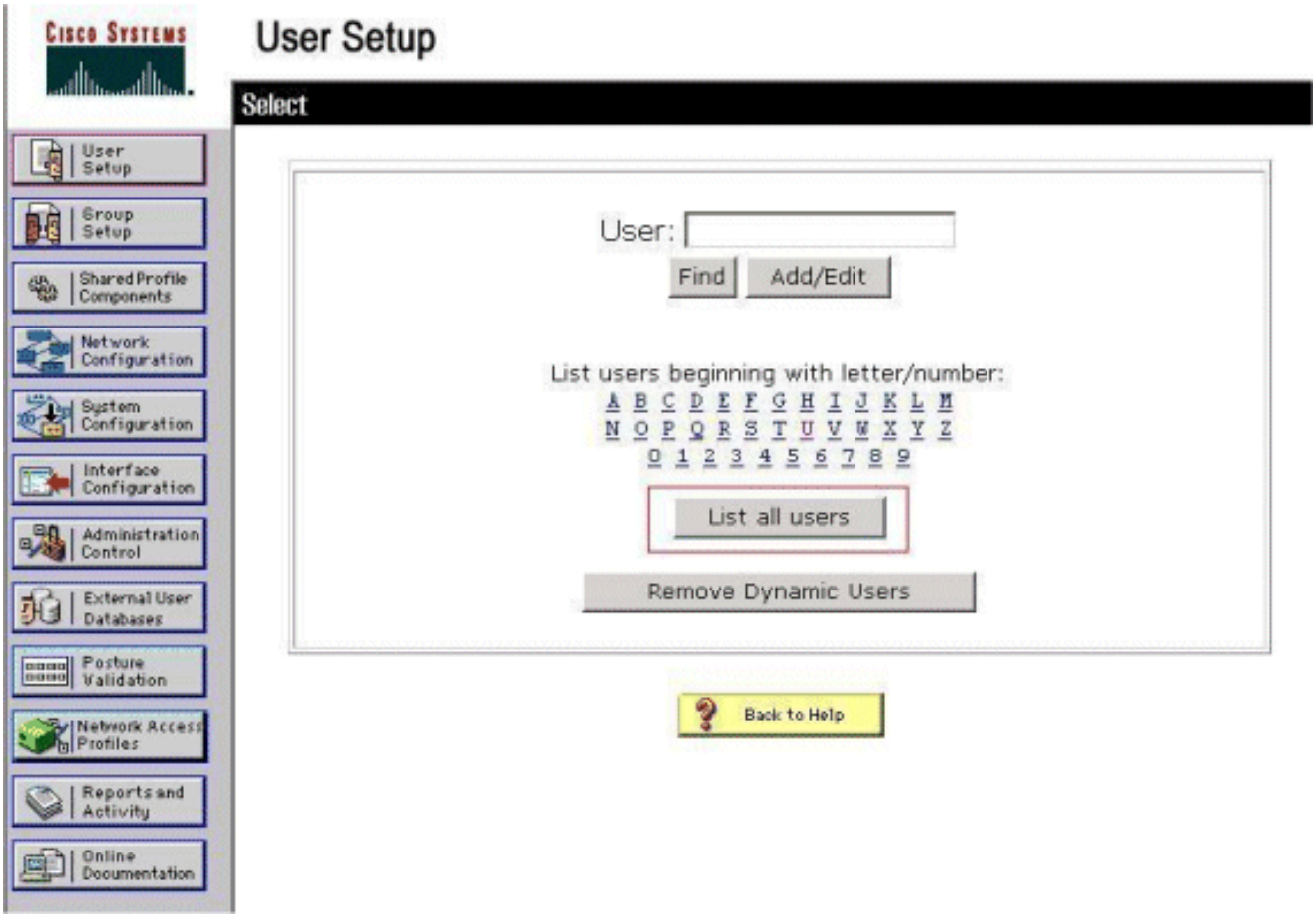


Verificación

Para una autenticación Web acertada, usted necesita marcar si los dispositivos se configuran de una manera apropiada. Esta sección explica cómo verificar los dispositivos usados en el proceso.

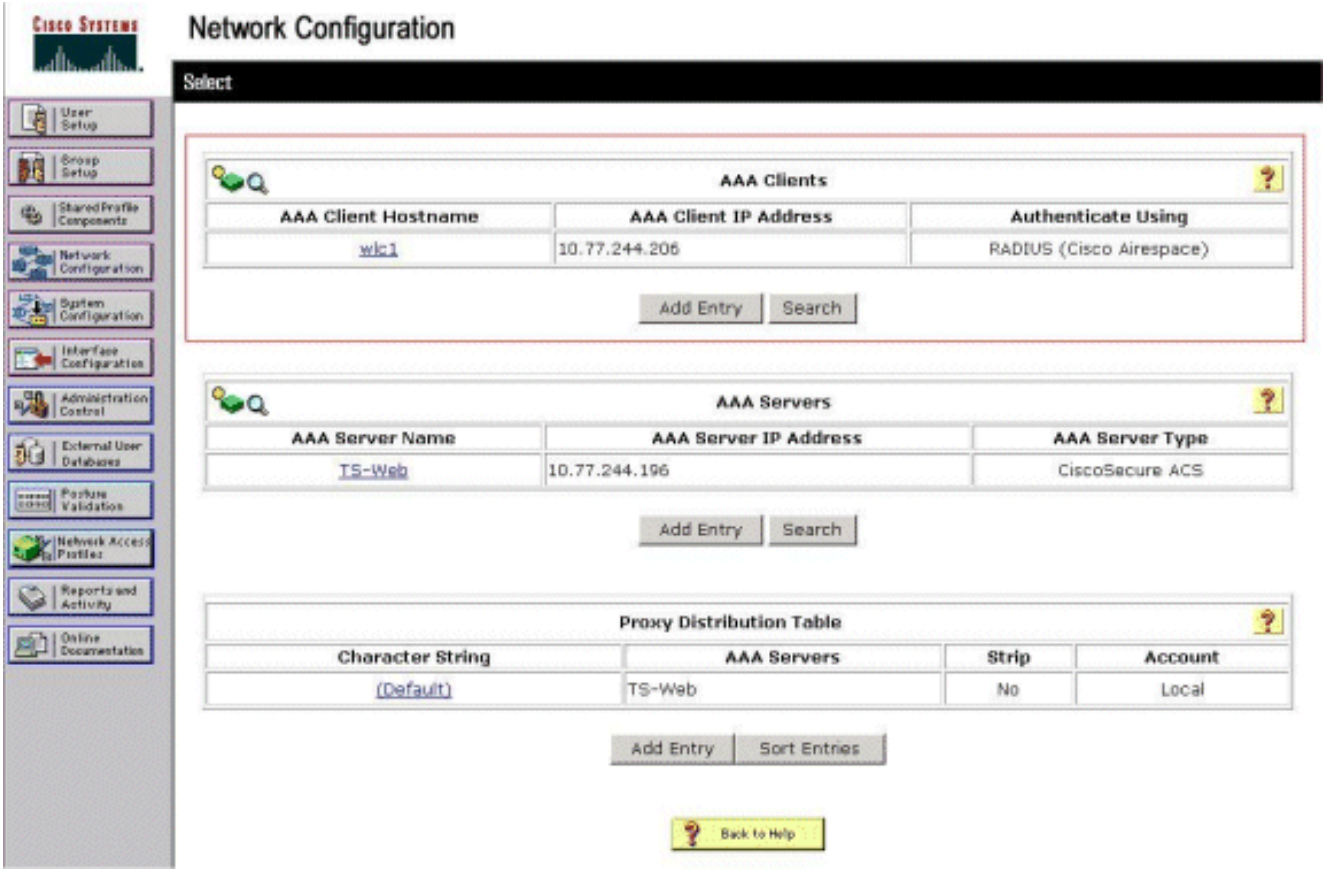
Verificación de ACS

1. Haga clic la **configuración de usuario**, y después haga clic la **lista todos los usuarios** en el ACS
GUI.



Aseegurese el estatus del usuario *se habilita* y eso el grupo predeterminado se asocia al usuario.

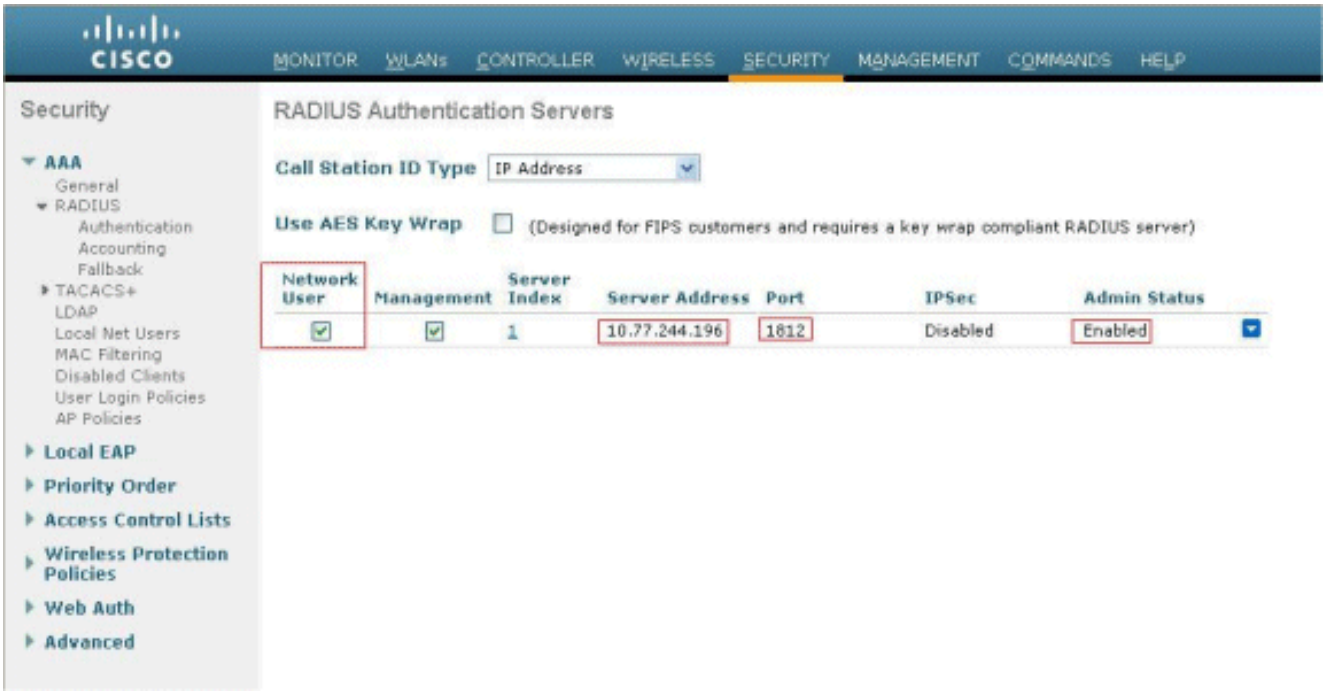
2. Haga clic la lengueta de la **configuración de red**, y la mirada en la tabla de los **clientes AAA** para verificar que el WLC está configurado como cliente AAA.



Verifique el WLC

1. Haga clic el menú **WLAN del** WLC GUI.Aseegurese la red inalámbrica (WLAN) usada para la autenticación Web se enumera en la página.Aseegurese el estado del administrador para la red inalámbrica (WLAN) *se habilita*.Aseegurese la política de seguridad para el Red-*auth de las* demostraciones de la red inalámbrica (WLAN).

2. Haga clic el **menú de seguridad del** WLC GUI.Aseegurese el Cisco Secure ACS (10.77.244.196) se enumera en la página.Aseegurese al usuario de la red que se marca el cuadro.Aseegurese el puerto es *1812* y *se habilita* eso el estado del administrador.



Troubleshooting

Hay muchas razones por las que una autenticación Web no es acertada. La autenticación Web del troubleshooting del documento en un regulador del Wireless LAN (WLC) explica claramente esas razones detalladamente.

Comandos para resolución de problemas

Note: Refiera a la información importante en los comandos Debug antes de que usted utilice estos **comandos debug**.

Telnet en el WLC y publica estos comandos de resolver problemas la 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 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 statio
n 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)
```

- **permiso del detalle aaa del debug**

Las tentativas de la autenticación fallida se enumeran en el menú situado en los **informes y la actividad** > los **intentos fallidos**.

Información Relacionada

- Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN
- Resolviendo problemas la autenticación Web en un regulador del Wireless LAN (WLC)
- Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN
- Autenticación Web usando el LDAP en el ejemplo de configuración de los reguladores del Wireless LAN (WLCs)
- Soporte Técnico y Documentación - Cisco Systems