Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico

Contenido

Introducción

En este documento se explica como Cisco implementa la autenticación Web y se muestra cómo configurar el Controlador (WLC) inalámbrico LAN (WLAN) Cisco Serie para que soporte la autenticación Web interna.

prerrequisitos

Requisitos

Este documento asume que ya tiene una configuración inicial en 4400 WLC.

Componentes Utilizados

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

hardware.

- WLC Serie 4400, versión 7.0.116.0
- Servidor de control de acceso (ACS) Cisco Secure, versión 4.2 instalado en un servidor Microsoft® Windows
- Punto de acceso liviano Cisco Aironet Serie 1131AG
- Adaptador inalámbrico Cisco Aironet .11 a/b/g CardBus, versión 4.0

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.

Autenticación Web

La autenticación Web es una función de seguridad de la capa 3 que hace que el controlador no permita el tráfico IP (excepto de los paquetes DHCP y DNS) de un cliente particular hasta que dicho cliente haya suministrado correctamente un nombre de usuario y una contraseña válidos. Es un método de autenticación simple sin la necesidad de un solicitante o de una utilidad de cliente. La autenticación Web es utilizada típicamente por los clientes que quieren implementar una red de acceso de invitados. Las instalaciones típicas pueden incluir ubicaciones “hot spot” tales como T-Mobile o Starbucks.

Considere que la autenticación Web no proporciona la cifrado de datos. La autenticación Web se utiliza típicamente como acceso simple de invitados para “hot spot” o ambiente de campus donde la conectividad es la única preocupación.

La autenticación Web se puede realizar mediante:

- ventana de login predeterminada en el WLC;
- versión modificada de la ventana de login predeterminada en el WLC;
- ventana de login personalizada configurada en un servidor web externo (autenticación web externa);
- ventana de login personalizada descargada en el controlador.

En este documento, se explican los pasos para configurar el controlador inalámbrico LAN para la autenticación del Web.

Proceso de Autenticación Web

Esto es lo que sucede cuando un usuario se conecta a un WLAN configurado para realizar una autenticación WEb:

- El usuario abre un navegador e ingresa una URL, por ejemplo, http://www.cisco.com. El cliente envía una solicitud DNS para que dicha URL obtenga la IP para el destino. El WLC desvía la solicitud DNS al servidor DNS y el servidor a su vez responde con una respuesta

DNS que contiene la dirección IP del destino www.cisco.com. Esto, a su vez, se remite a los clientes de red inalámbrica.

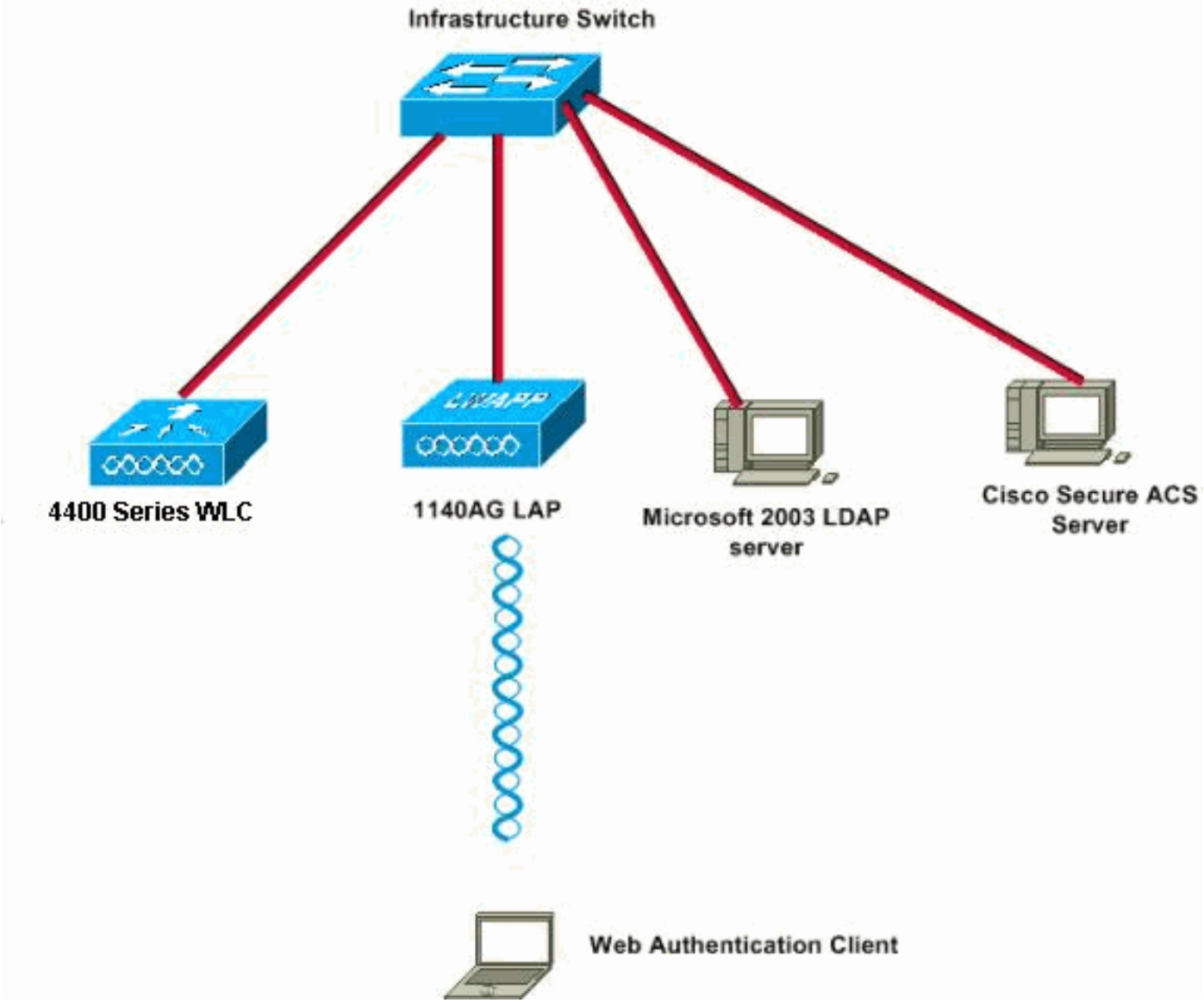
- El cliente entonces intenta abrir una conexión con el la dirección IP de destino. Envía un paquete TCP SYN destinado a la dirección IP de www.cisco.com.
- El WLC tiene reglas configuradas para el cliente y por lo tanto puede actuar como proxy para www.cisco.com. Devuelve un paquete TCP SYN-ACK al cliente con la fuente como la dirección IP de www.cisco.com. El cliente devuelve un paquete TCP ACK para completar la aceptación de contacto TCP de tres vías y la conexión TCP se establece completamente.
- El cliente envía un paquete HTTP GET destinado a www.cisco.com. El WLC intercepta este paquete y lo envía para el manejo de redireccionamiento. El aplicación HTTP gateway prepara a un cuerpo HTML y lo envía de vuelta como respuesta al HTTP GET solicitado por el cliente. Este HTML hace que el cliente vaya a la URL de la página Web predeterminada, por ejemplo, http:// /login.html.
- El cliente cierra la conexión TCP con la dirección IP, por ejemplo, www.cisco.com.
- Ahora el cliente quiere ir a http://1.1.1.1/login.html. Por lo tanto, el cliente intenta abrir una conexión TCP con la dirección IP virtual del WLC. Envía a paquete TCP SYN para 1.1.1.1 al WLC.
- El responde con un TCP SYN-ACK y el cliente devuelve un TCP ACK al WLC para completar la aceptación de contacto.
- El cliente envía un HTTP GET a /login.html destinado a 1.1.1.1 para solicitar acceso a la página de login.
- Esta solicitud llega al Servidor Web del WLC, y el servidor responde con la página de login predeterminada. El cliente recibe la página de login en la ventana del navegador donde el usuario puede continuar el inicio de sesión.

Aquí está un link a un vídeo en la comunidad del soporte de Cisco que explica el proceso de autenticación Web:

Autenticación Web en los controladores LAN inalámbricos Cisco (WLC)

Configuración de la red

En este documento, se utiliza esta configuración de red:



Configuración del Controlador para la Autenticación Web

En este documento, se muestra cómo configurar un WLAN para la autenticación Web y cómo asociarlo a una VLAN esclusiva. Estos son los pasos para configurar WLAN para la autenticación Web:

- Creación de una Interfaz VLAN
- Configuración de Autenticación Web Interna
- Agregado de una Instancia WLAN
- Configuración de un Tipo de Autentiación (Tres Maneras de Autenticar Usuarios durante la Autenticación Web)

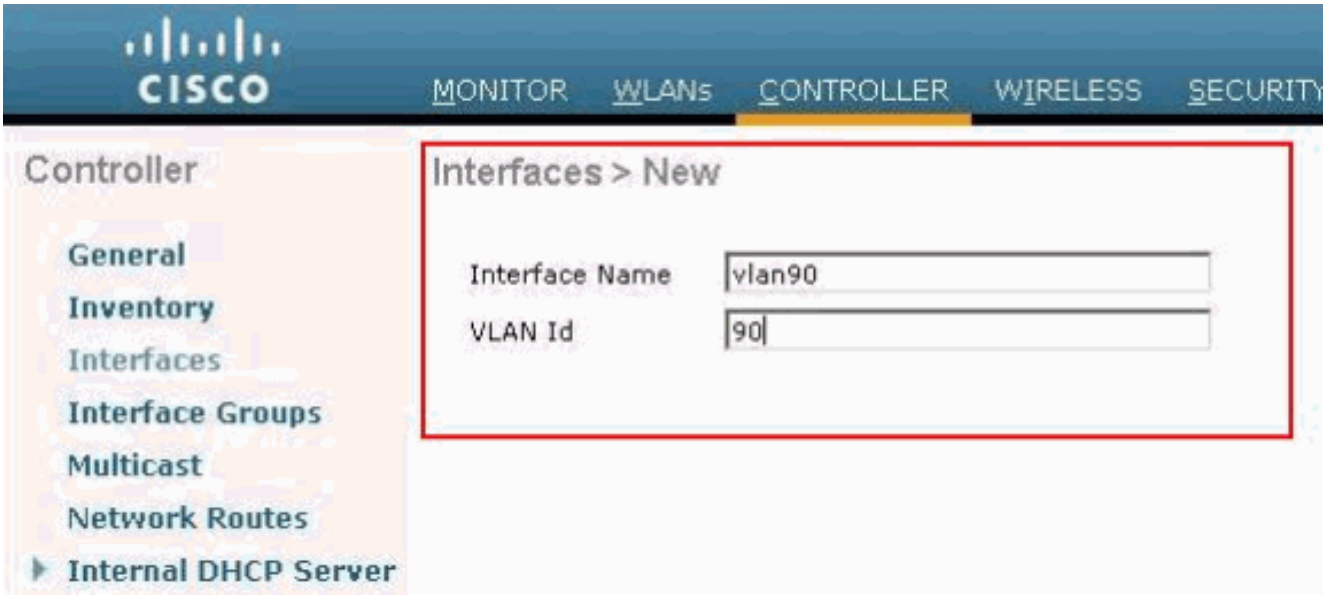
En esta sección, encontrará información para configurar el controlador para la autenticación Web.

Las siguientes son direcciones IP usadas en este documento:

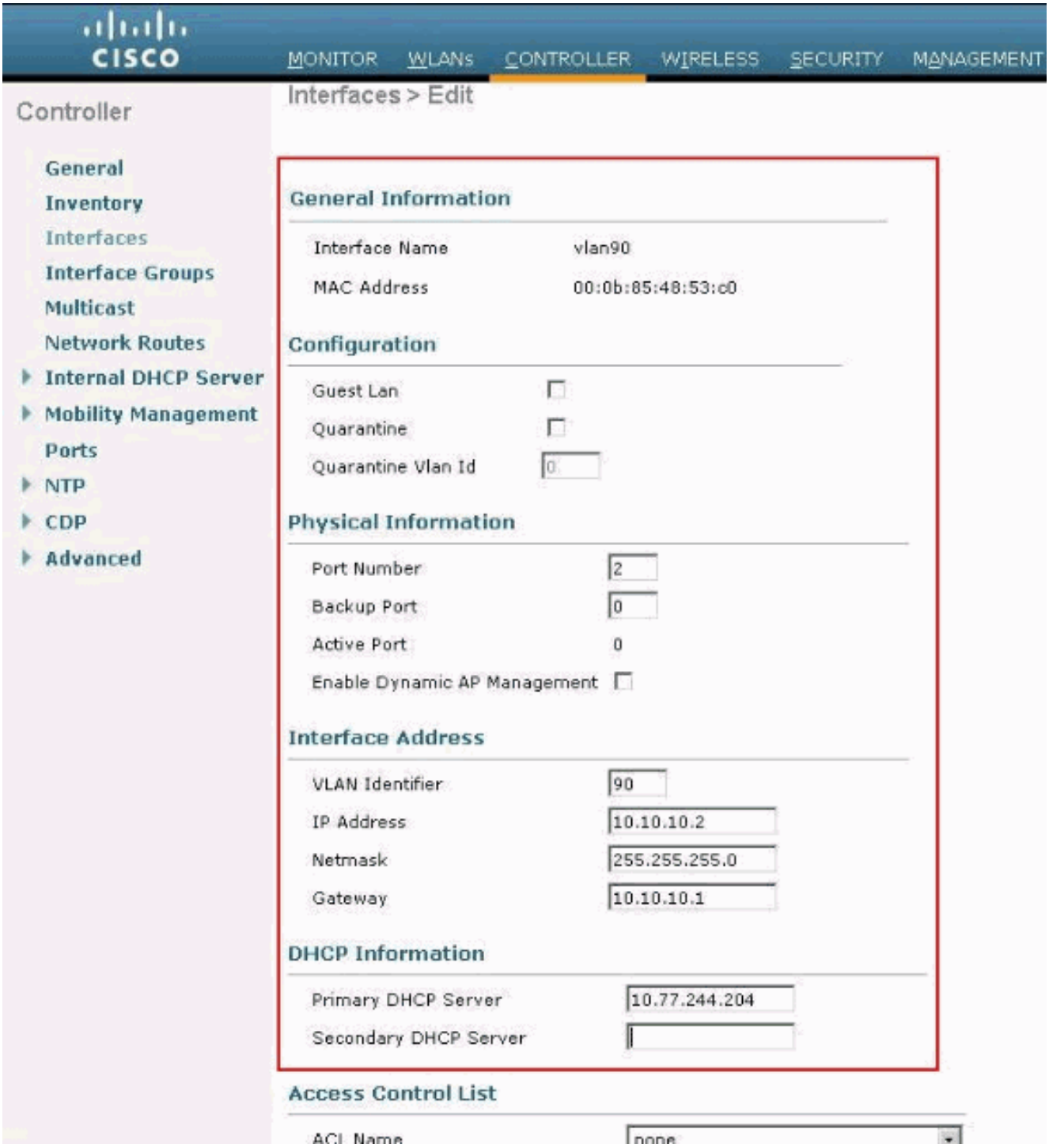
- La dirección IP del WLC es 10.77.244.204.
- La dirección IP del servidor ACS es 10.77.244.196.

Creación de una Interfaz VLAN

Complete estos pasos:

1. En la interfaz de usuario gráfica del controlador LAN inalámbrico, haga clic en la opción Controller en el menú superior, elija la opción Interfaces del menú a la izquierda, y haga clic en New en el extremo superior derecho de la ventana para crear una nueva interfaz dinámica.Se abrirá la ventana Interfaces > New. Este ejemplo utiliza Nombre de *Interfaz* con una VLAN ID de
90:


2. Haga clic en **Aplicar** para crear la interfaz VLAN.Se abrirá la ventana Interfaces > Edit, y se le solicitará que complete la información de interfaz específica.
3. Este documento utiliza estos parámetros:Dirección IP - 10.10.10.2Netmask - 255.255.255.0 (24 bits)Gateway - 10.10.10.1Número del puerto - 2Servidor DHCP primario - 10.77.244.204**Nota:** Este parámetro debe ser la dirección IP de su RADIO o servidor DHCP. En este ejemplo, se usa la dirección de administración del WLC como el servidor DHCP porque el alcance de DHCP interno se configura en el WLC.Servidor DHCP secundario - 0.0.0.0**Nota:** El ejemplo no tiene un servidor DHCP secundario, por eso usa 0.0.0.0. Si su configuración tiene un servidor DHCP secundario, agregue la dirección IP en este campo.Nombre ACL -
Ninguno



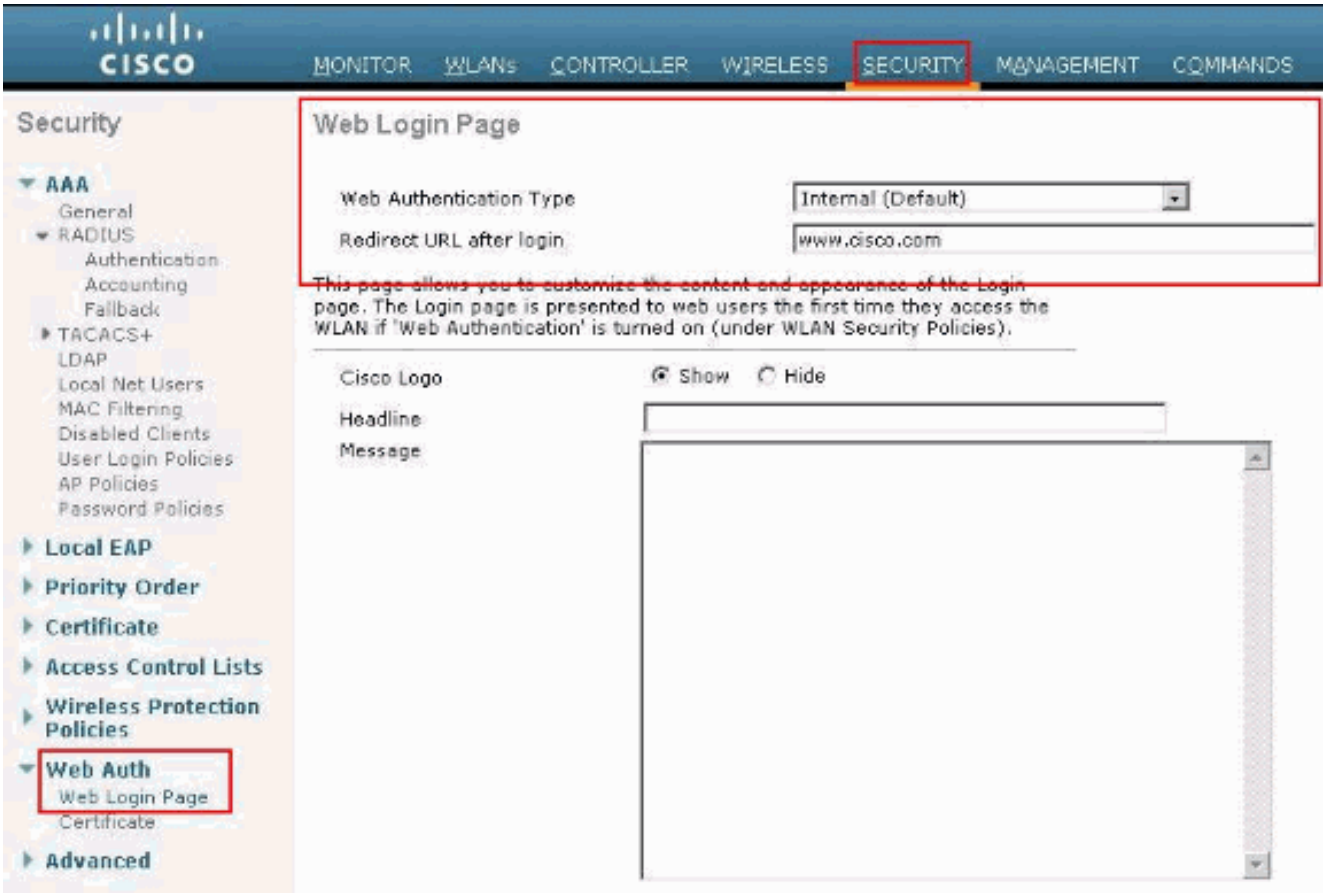
4. Haga clic en **Aply** para guardar los cambios.

Configuración de Autenticación Web Interna

El siguiente paso es configurar el WLC para la autenticación del Web interna. La autenticación Web interna es el tipo de autenticación Web predeterminada en los WLC. Si este parámetro no se ha cambiado, no se requiere ninguna configuración para habilitar la autenticación Web interna. Si el parámetro de la autenticación Web fue cambiado previamente, complete estos pasos para configurar el WLC para la autenticación Web interna:

1. En la interfaz gráfica de usuario del controlador, diríjase a **Security > Web Auth > Web Login** para acceder a la página de autenticación Web.
2. En el menú deplegable Web Authentication Type, elija Internal Web Authentication.
3. En el campo Redirect URL after login, ingrese la URL de la página a la cual se

redireccionará al cliente final tras una autenticación exitosa.

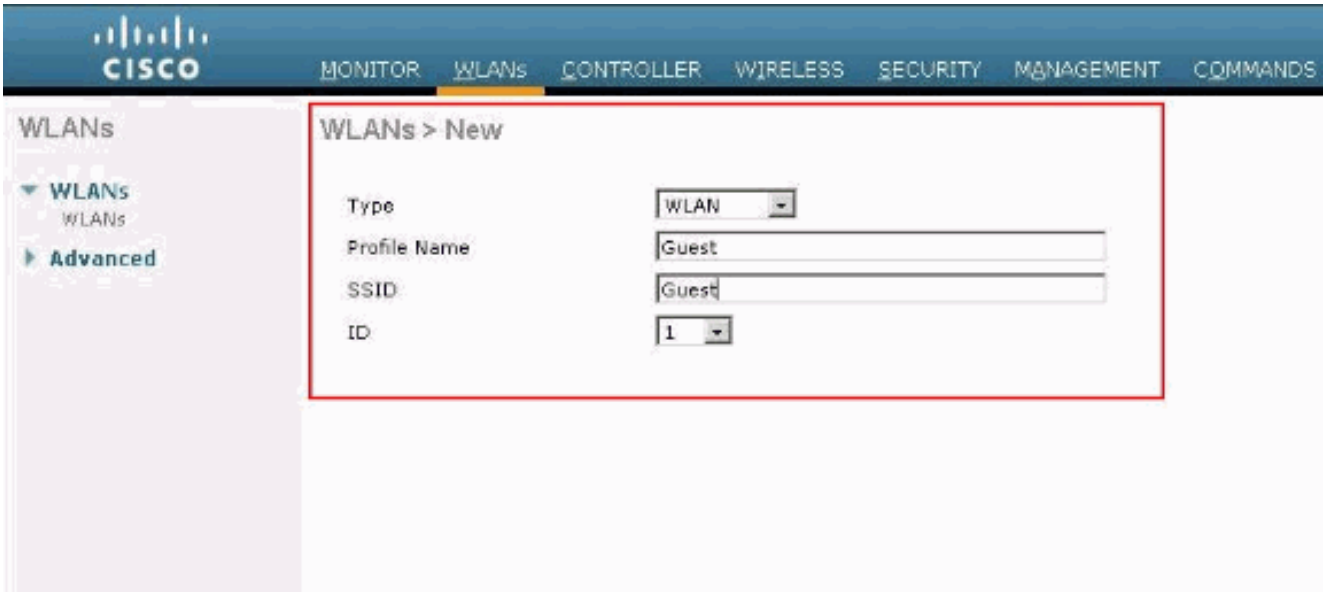


Nota: En las versión 5.0 y versiones subsiguientes del WLC, la página de cierre de sesión de la autenticación Web también se puede personalizar. Para obtener más información, consulte las secciones Asignar login, Error de login y Páginas de cierre de sesión correspondientes a WLAN de la Guía de configuración del controlador LAN inalámbrico, 5.2.

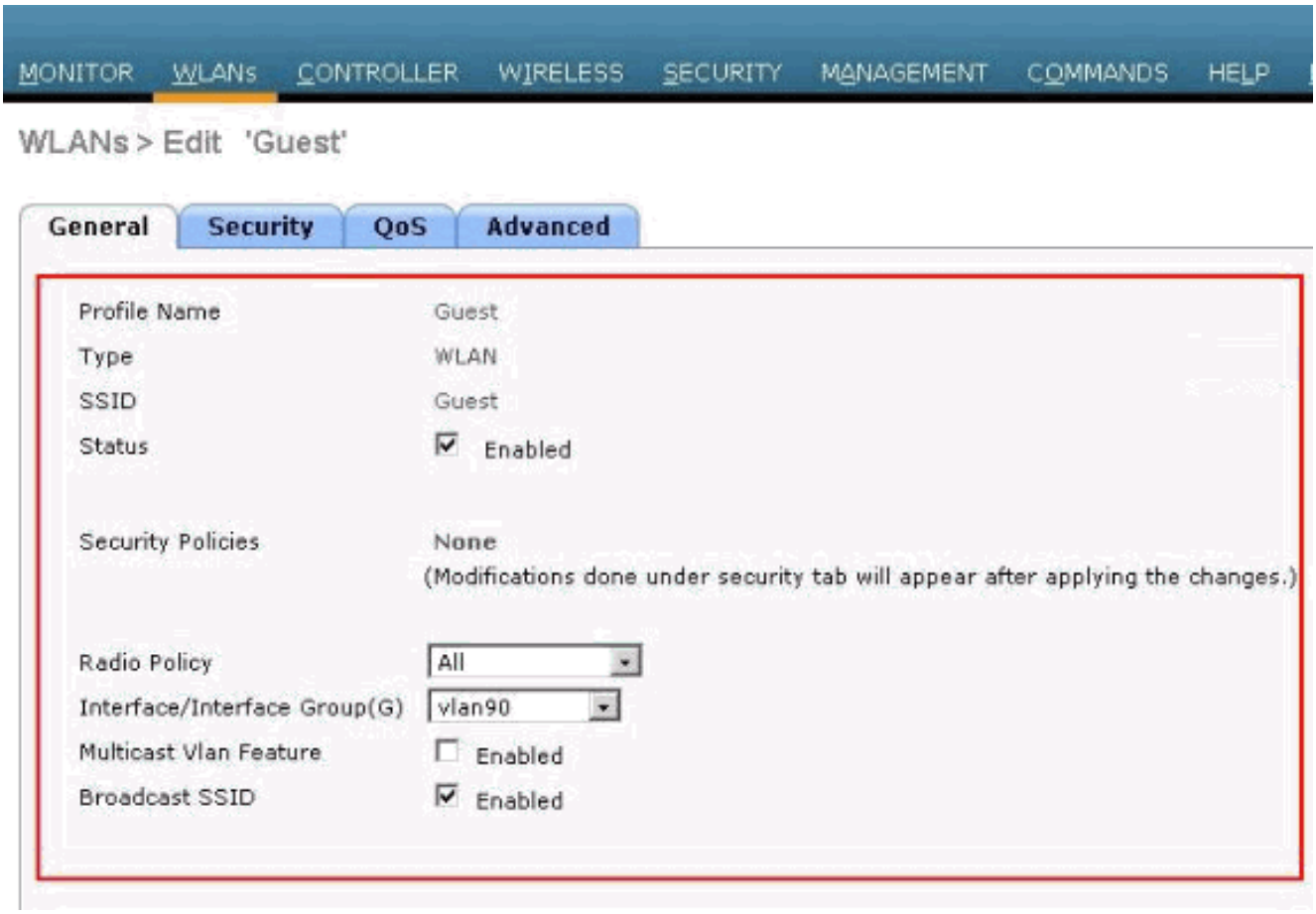
Agregado de una Instancia WLAN

Ahora que se ha habilitado la autenticación Web interna y hay una interfaz VLAN dedicada a la autenticación Web, debe proporcionar una WLAN/SSID nueva que sporte a los usuarios de la autenticación Web.

1. En la interfaz gráfica de usuario del WLC, haga clic en WLAN en el menú superior y luego en New en el extremo superior derecho.Elija **WLAN** como tipo. Elija un nombre del perfil y una WLAN SSID para la autenticación Web. Este ejemplo utiliza **Invitado** para el nombre del perfil y WLAN
SSID.

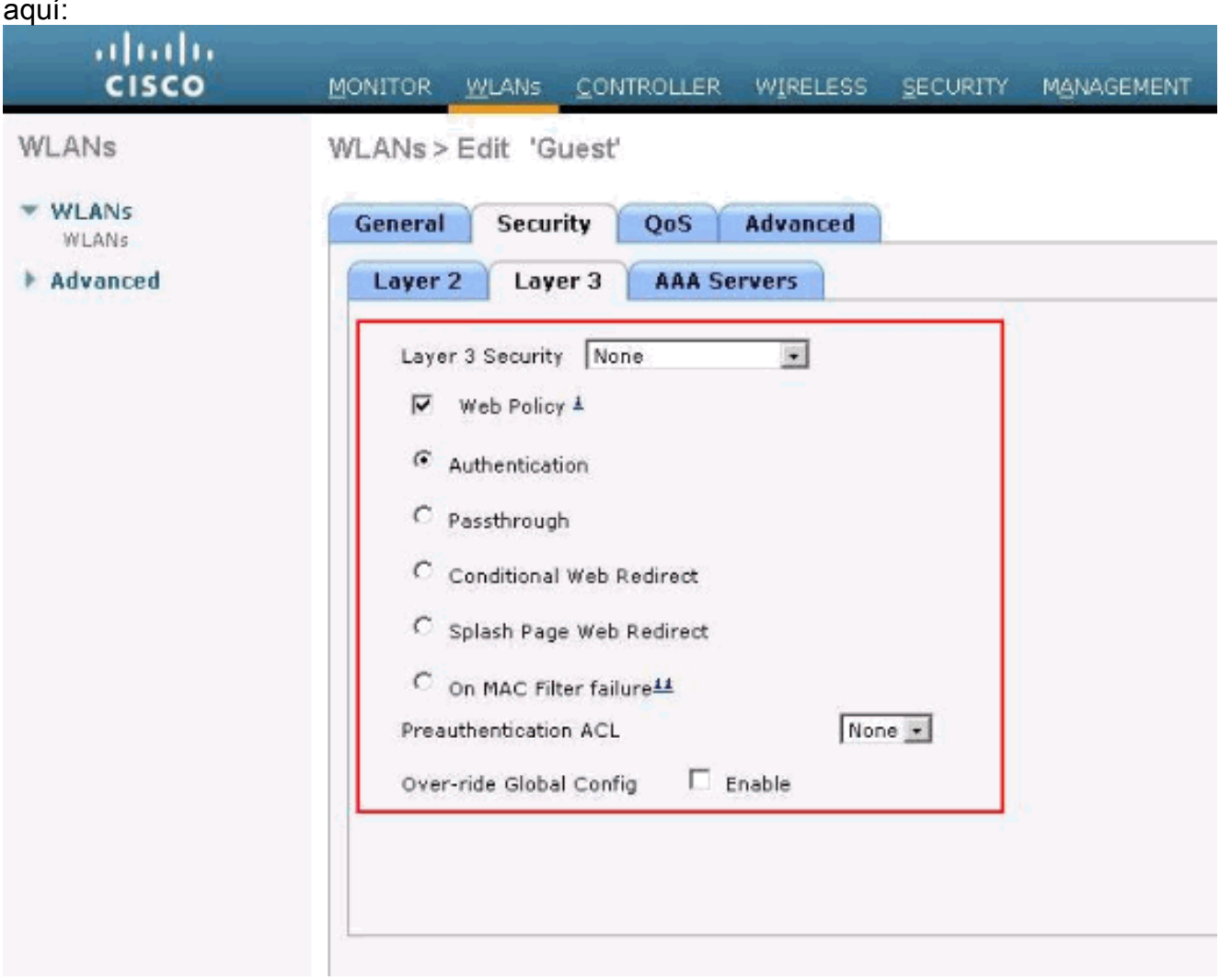


2. Haga clic en Apply (Aplicar).Se abrirá la ventana de edición de WLAN.



3. Verifique el cuadro de estado del WLAN para habilitar la WLAN. Del menú de la interfaz, seleccione el nombre de la interfaz VLAN que creó previamente. En este ejemplo, el nombre de la interfaz es *vlan90*.**Nota:** Deje el valor predeterminado para otros parámetros en esta pantalla.
4. Haga clic en la ficha Security (Seguridad).Complete estos pasos para configurar la autenticación Web:Haga clic en la pestaña Layer 2 y configure la seguridad como ***None***.**Nota:** No puede configurar el traspaso Web como seguridad de la capa 3 con 802.1x o WPA/WPA2 como seguridad de la capa 2 para un WLAN. Consulte Matriz de Compatibilidad de Seguridad de Capa 2 de Capa 3 del Wireless LAN Controller para más información sobre compatibilidad de seguridad del Wireless LAN Controller de Capa 2 y de Capa 3.Haga clic

en la pestaña Layer 3. Marque el cuadro Web Policy y elija la opción Authentication, como se muestra
aquí:



Haga clic en Aplicar para guardar el WLAN.Vuelve a la ventana Resumen de WLAN. Asegúrese de que Web-AUTH esté habilitado bajo la columna de las políticas de seguridad de la tabla WLAN para el invitado SSID.

Tres Maneras de Autenticar Usuarios durante la Autenticación Web

Hay tres maneras de autenticar usuarios cuando utiliza la autenticación Web. La autenticación local permite que autentique al usuario en el WLC de Cisco. También puede utilizar un servidor RADIUS externo o a un servidor LDAP como una base de datos back-end para autenticar a los usuarios.

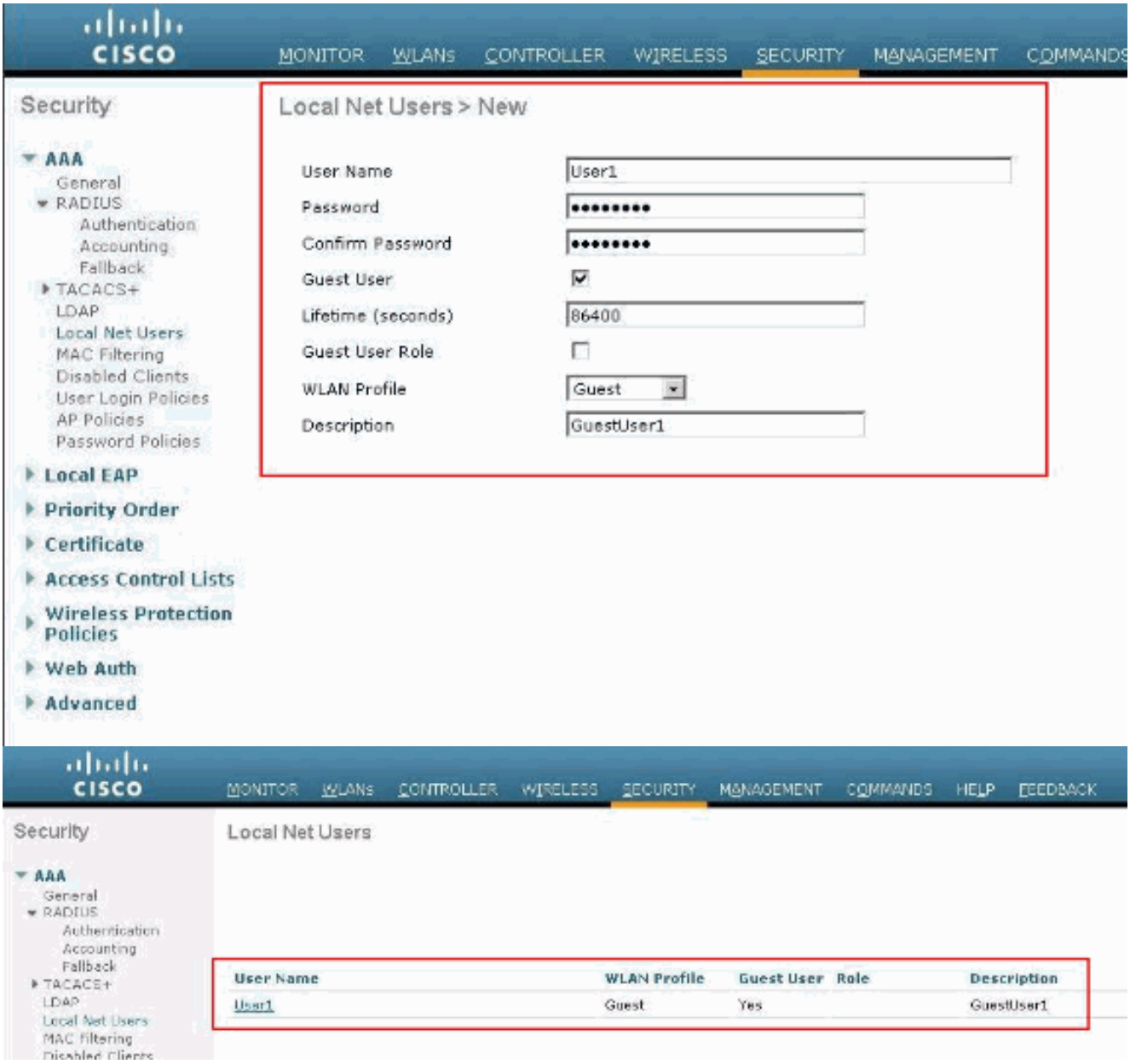
Este documento proporciona un ejemplo de configuración para los tres métodos.

Autenticación local

La base de datos de usuarios para los usuarios invitados se almacena en la base de datos local del WLC. El WLC autentica a los usuarios con esta base de datos.

1. En la interfaz gráfica de usuario del WLC, haga clic en Security.
2. Haga clic en Local Net Users en el menú a la izquierda.

3. Haga clic en New para crear a un usuario nuevo.Se abrirá una nueva ventana que le solicitará que ingrese una nombre de usuario y contraseña.
4. Ingrese un nombre de usuario y una contraseña para crear un usuario nuevo, después confirme la contraseña que desea utilizar.En este ejemplo se creará un usuario con nombre User1.
5. Agregue una descripción, si lo desea.En este ejemplo se utiliza el usuario invitado Guest User1.
6. Haga clic en **Aplicar** para guardar la configuración del usuario nuevo.



7. Repita los pasos 3-6 para agregar más usuarios a la base de datos.

Servidor de RADIUS para la autenticación Web

Este documento utiliza una red inalámbrica ACS en el servidor de Windows 2003 como el servidor RADIUS. Puede utilizar cualquier servidor de RADIUS disponible que implemente actualmente en su red.

Nota: El ACS se puede configurar en el Windows NT o Windows 2000 Server. Para descargar el ACS desde Cisco.com, consulte Centro de Software (Descargas) - Cisco Secure Software (clientes registrados solamente). Necesita una cuenta del Web de Cisco para descargar el software.

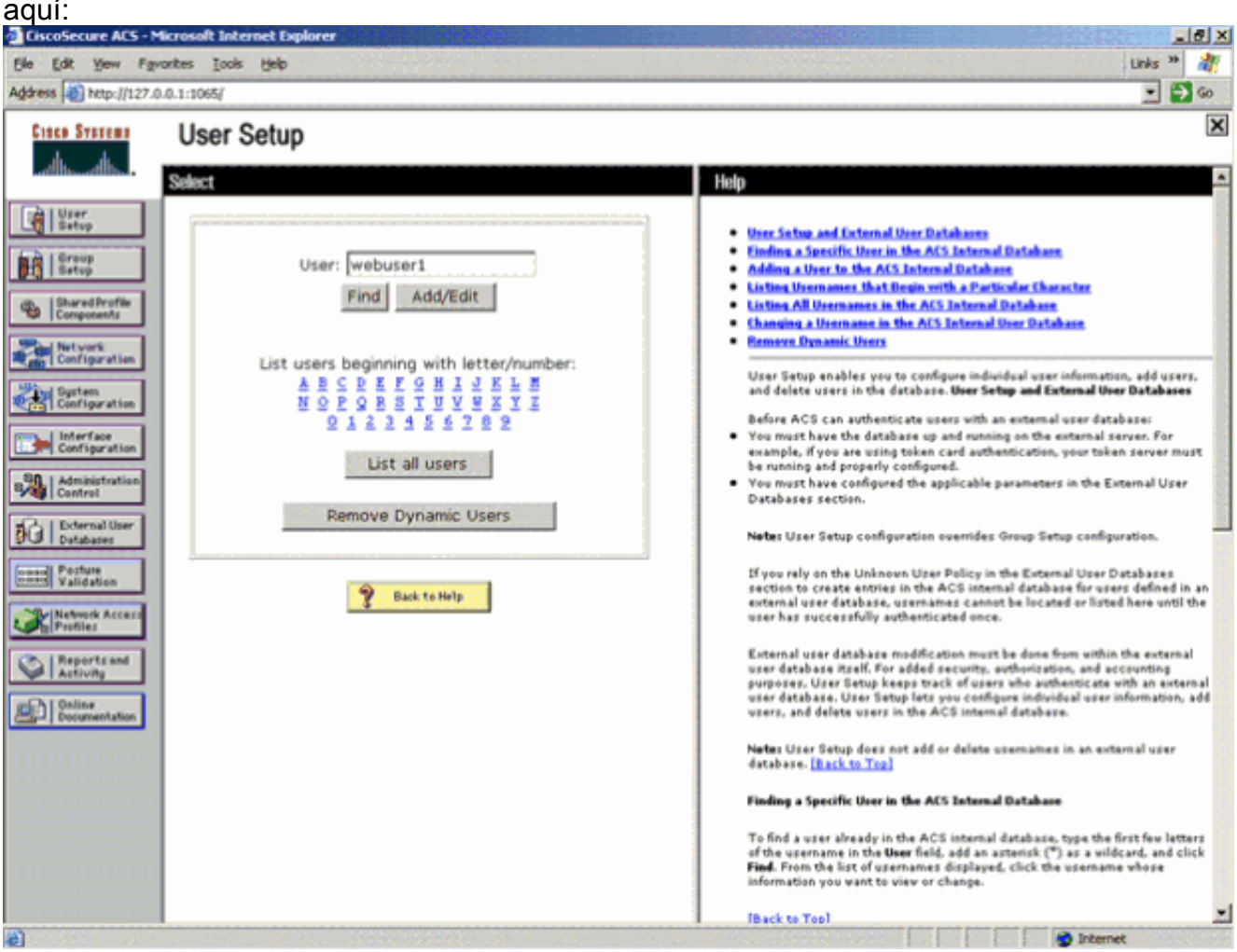
La sección Configuración ACS le muestra cómo configurar el ACS para el RADIUS. Debe tener red funcional a completamente - con un sistema de nombres del dominio (DN) y un servidor de RADIUS.

Configuración ACS

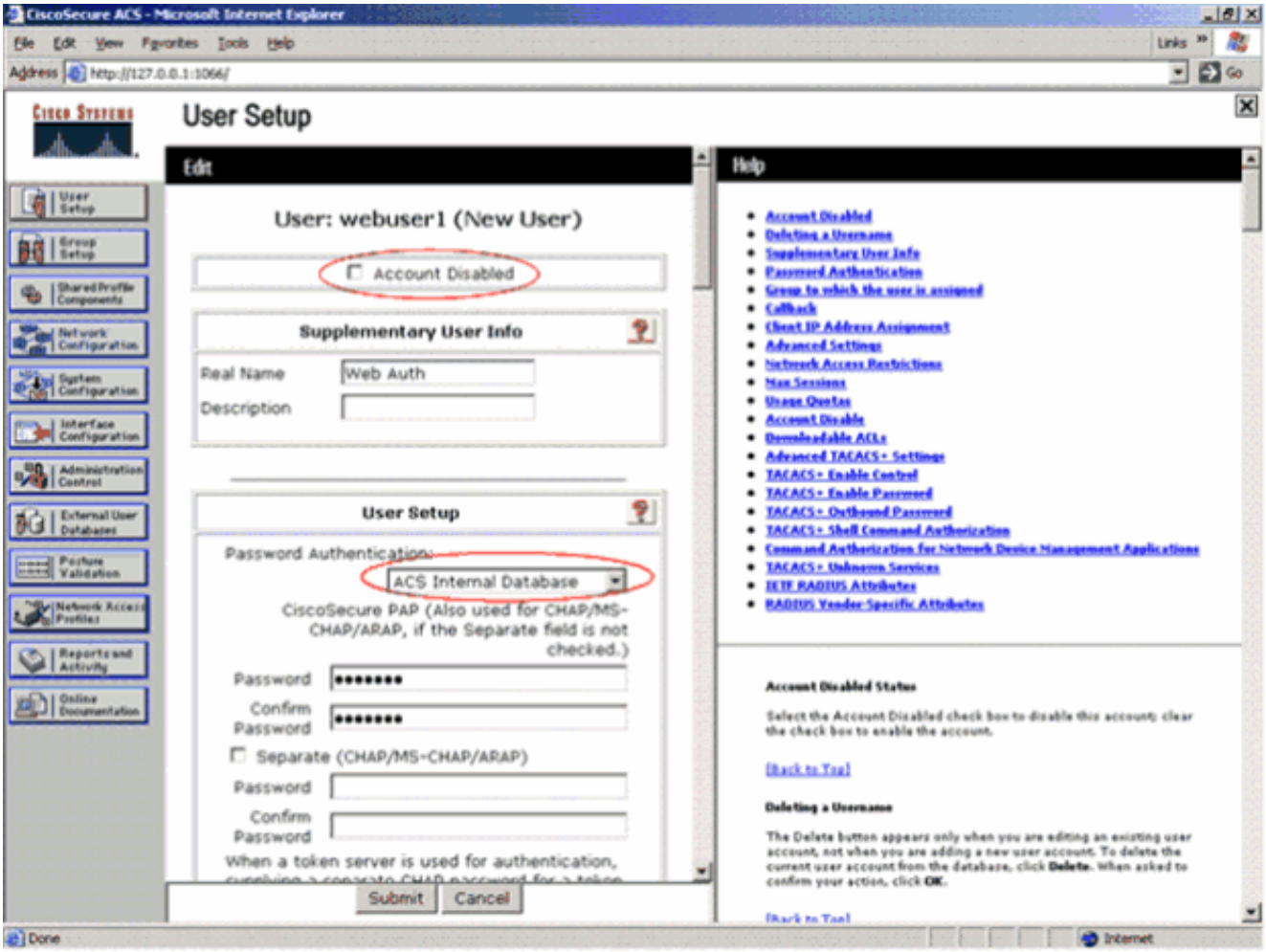
En esta sección, encontrará información para configurar el ACS para RADIUS.

Configure el ACS en su servidor y después complete estos pasos para crear a un usuario para la autenticación:

1. Cuando el ACS pregunte si desea abrir el ACS en una ventana del buscador para configurar, haga clic en **Yes**.**Nota:** Después de que configure el ACS, también tendrá un icono en su escritorio.
2. En el menú a la izquierda, haga clic en **Configuración de usuario** .Esta acción le lleva a la pantalla de configuración de usuario como se muestra
   aquí:



3. Ingrese el usuario que quieres utilizar para la autenticación Web, y haga clic en **Agregar/Editar**.Después de crear el usuario, se abrirá una segunda ventana como se muestra
   aquí:

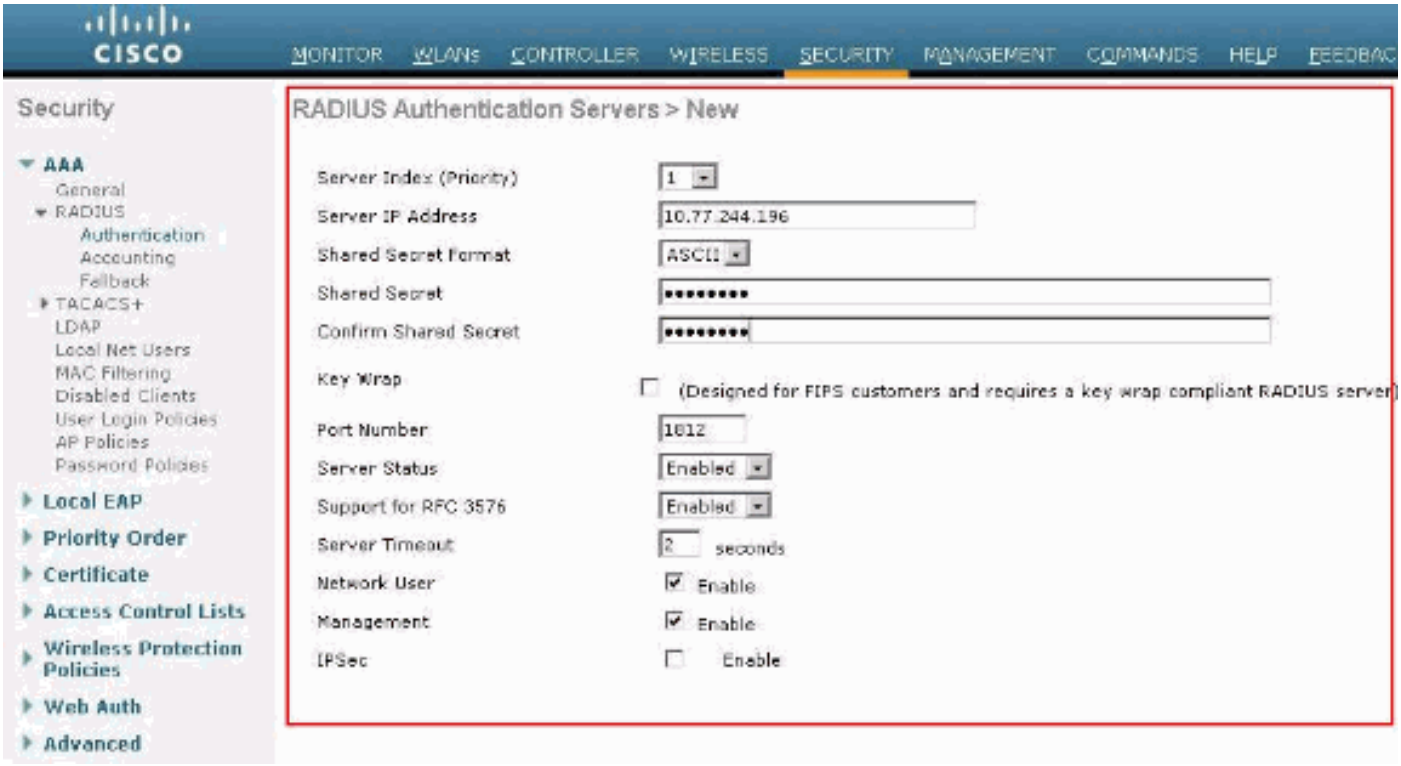


4. Asegúrese de que el cuadro Account Disabled en la parte superior no esté marcado.
5. Elija Internal Database para la opción Password Authentication.
6. Ingrese la contraseña. El Admin tiene la opción de configurar una autenticación PAP/CHAP o MD5-CHAP al agregar un usuario en la base de datos interna ACS. El PAP es el tipo de autenticación predeterminada para usuarios de autenticación Web en los controladores. El Admin tiene la flexibilidad para cambiar el método de autentificación a chap/md5-chap usando este comando CLI:
   ```
   config custom-web radiusauth <auth method>
   ```
7. Haga clic en Submit (Enviar).

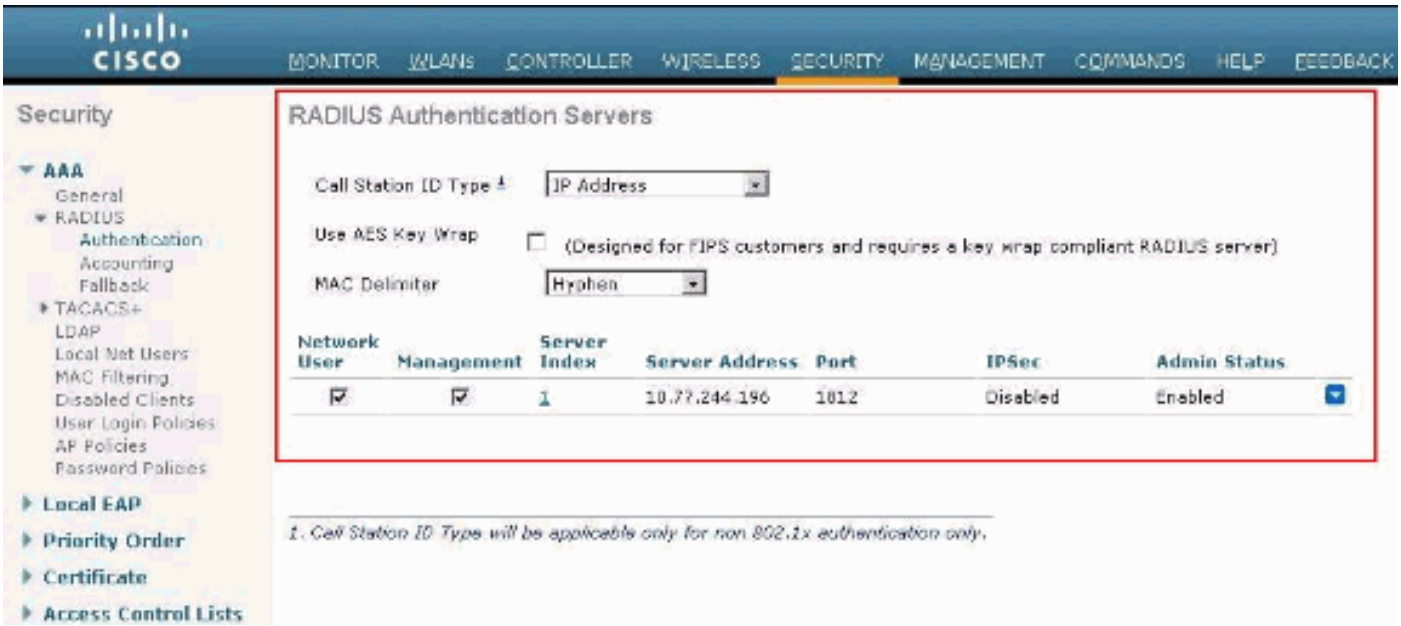
Ingrese su información del servidor de RADIUS en el WLC de Cisco

Complete estos pasos:

1. Haga clic en **Security** en la parte superior del menú.
2. Haga clic la **autenticación de RADIUS** en el menú a la izquierda.
3. Haga clic en **Nuevo**, e ingrese la dirección IP de tu ACS/RADIUS servidor. En este ejemplo, la dirección IP del servidor ACS es **10.77.244.196**.
4. Ingresa el secreto compartido para el servidor de RADIUS. Aseegurese que esta clave secreta sea igual a la que ingresó en el servidor RADIUS del WLC.
5. Deje el número del puerto en el valor predeterminado, 1812.
6. Asegúrese de que la opción del **estado del servidor** esté habilitada.
7. Marque el cuadro Network User Enable para utilizar este servidor RADIUS para autenticar a los usuarios de su red inalámbrica.
8. Haga clic en Apply (Aplicar).



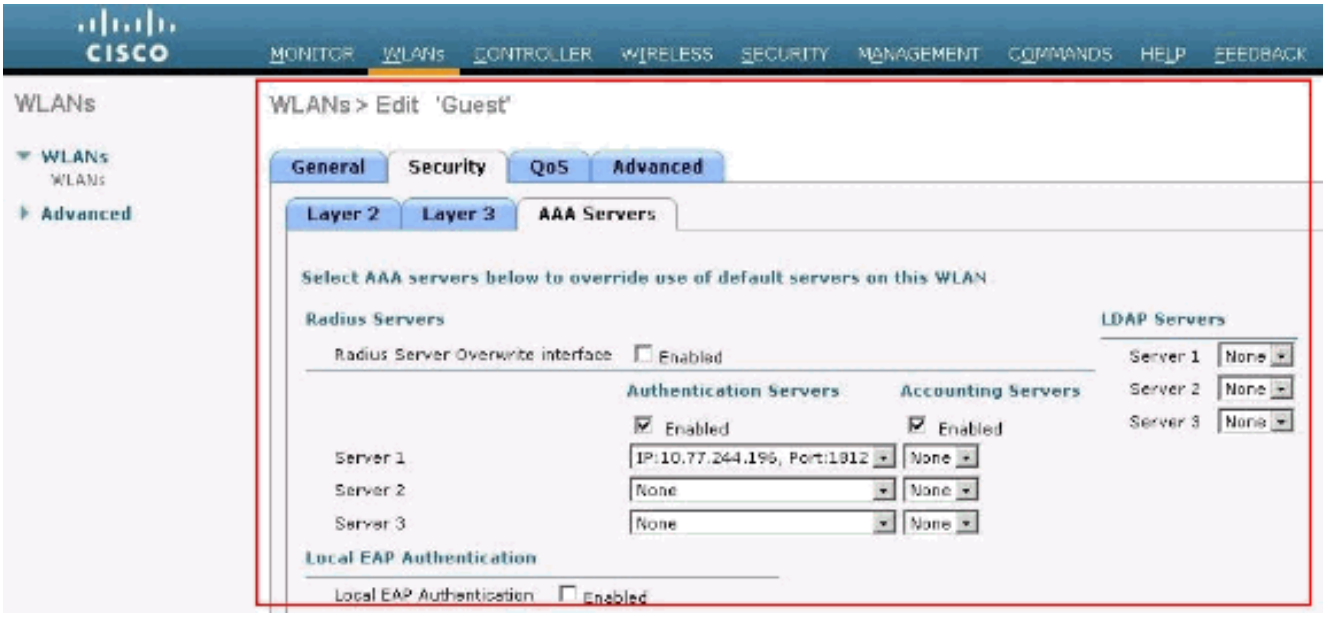
Asegúrese de que el cuadro Network User está marcado y de que la opción Admin Status esté habilitada.



Configuración de WLAN con el Servidor RADIUS

Ahora que el Servidor de RADIUS está configurado en el WLC, debe configurar el WLAN para utilizar este servidor de RADIUS para la autenticación Web. Complete estos pasos de progresión para configurar el WLAN con el servidor de RADIUS.

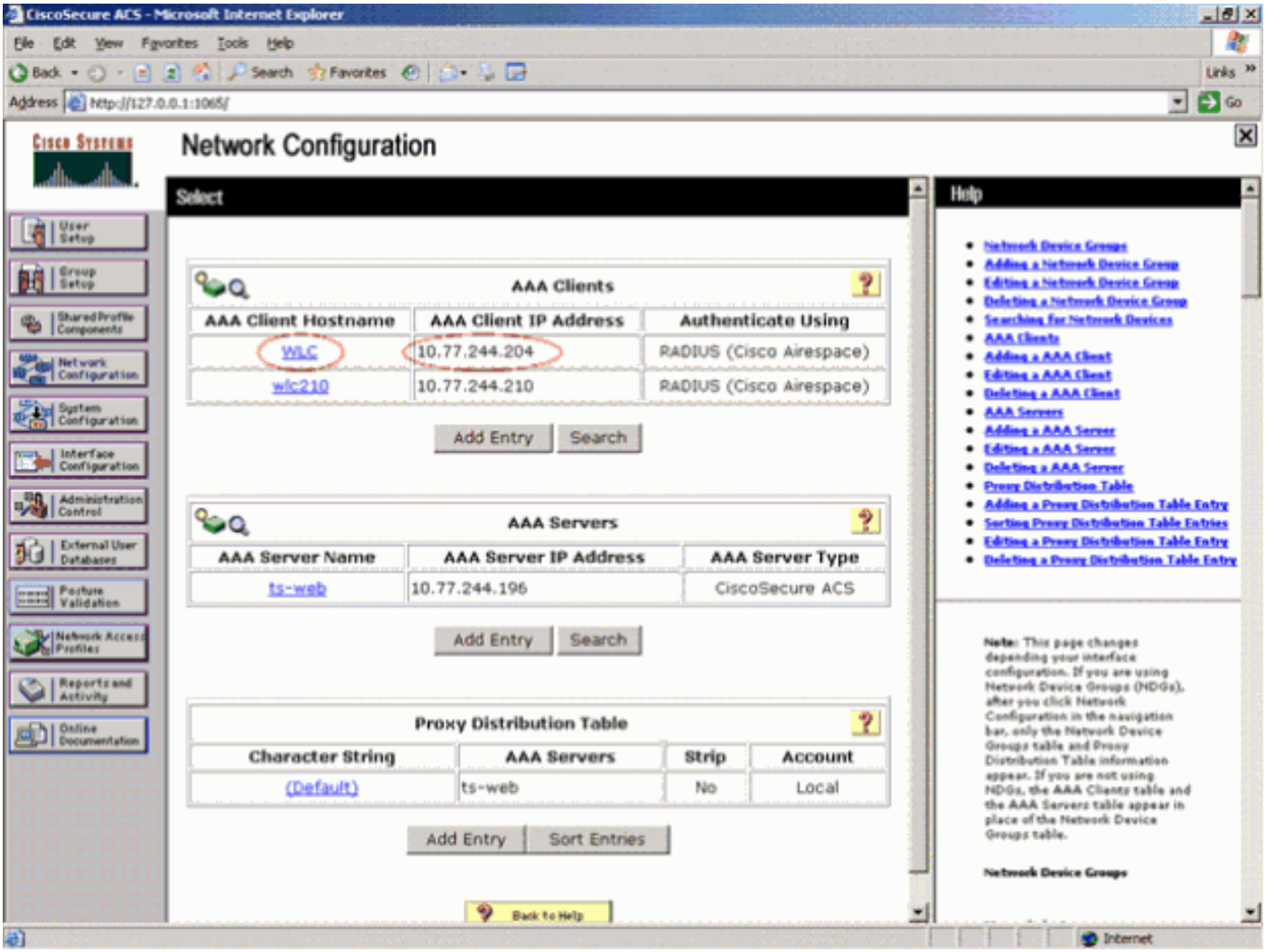
1. Abra su buscador WLC y haga clic en **WLAN**. Se mostrará la lista de WLAN configurados en el WLC. Seleccione el Invitado que creó para autenticación Web con un clic.
2. En la página WLANs > Edit, haga clic en Security MEnu. Haga clic en la pestaña AAA Servers en Security. Después, elija al servidor RADIUS, que en este ejemplo es 10.77.244.196.



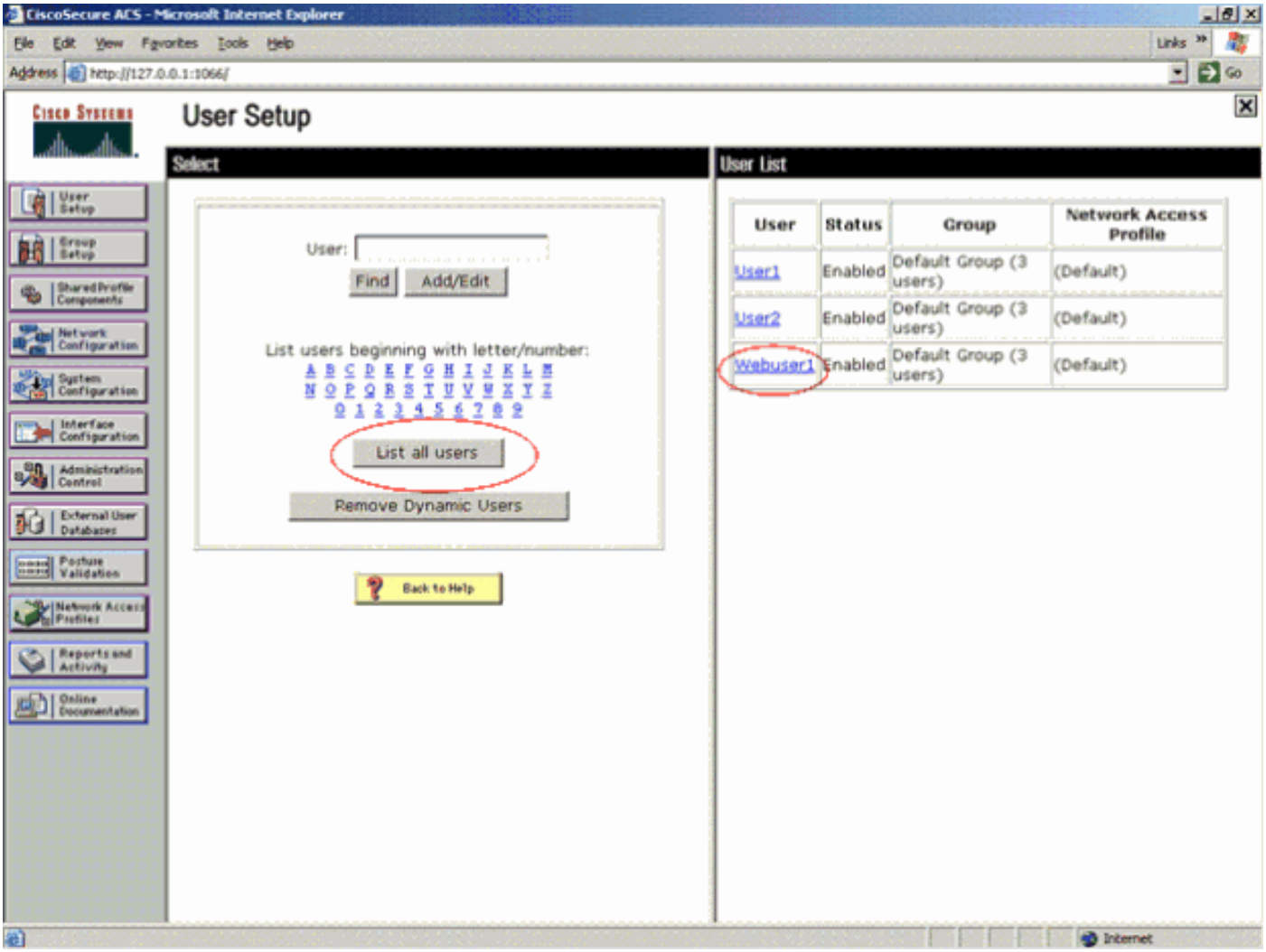
3. Haga clic en Apply (Aplicar).

Verificación de ACS

Al configurar el ACS, recuerde descargar los parches actuales y el último código. Esto debe solucionar los problemas inminentes. En caso de que usted esté utilizando la autenticación de RADIUS, asegúrese de que su WLC esté configurado como uno de los clientes AAA. Haga clic el menú Network Configuration en el lado izquierdo para marcar esta opción. Haga clic en el cliente AAA, después verifique la contraseña y el tipo de autenticación configurados. Consulte la sección Configuración de Clientes AAA de la Guía del Usuario para Cisco Secure Access Control Server 4.2 para más información sobre cómo configurar un cliente AAA.



Cuando elija User Setup, verifique otra vez que sus usuarios existan realmente. Haga clic en List All Users. Aparecerá una ventana como la que se muestra a continuación. Asegúrese de que el usuario que ha creado exista en la lista.

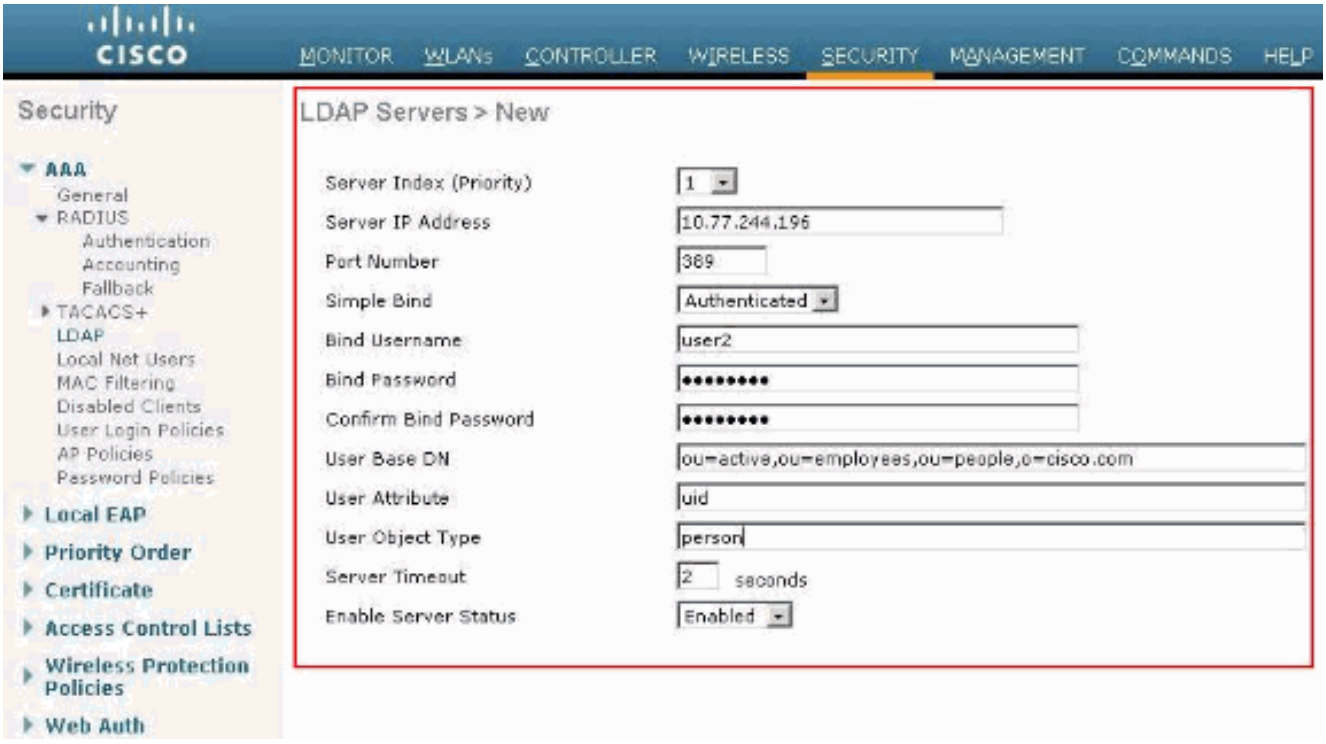


Servidor LDAP

En esta sección se explica cómo configurar un servidor de Protocolo de acceso a directorio liviano (LDAP) como base de datos back-end, similar a una base de datos RADIUS o a una base de datos de usuarios local. Una base de datos back-end LDAP permite que el controlador consulte un servidor LDAP para obtener las credenciales (nombre de usuario y contraseña) de un usuario determinado. Estas credenciales se utilizan para autenticar el usuario.

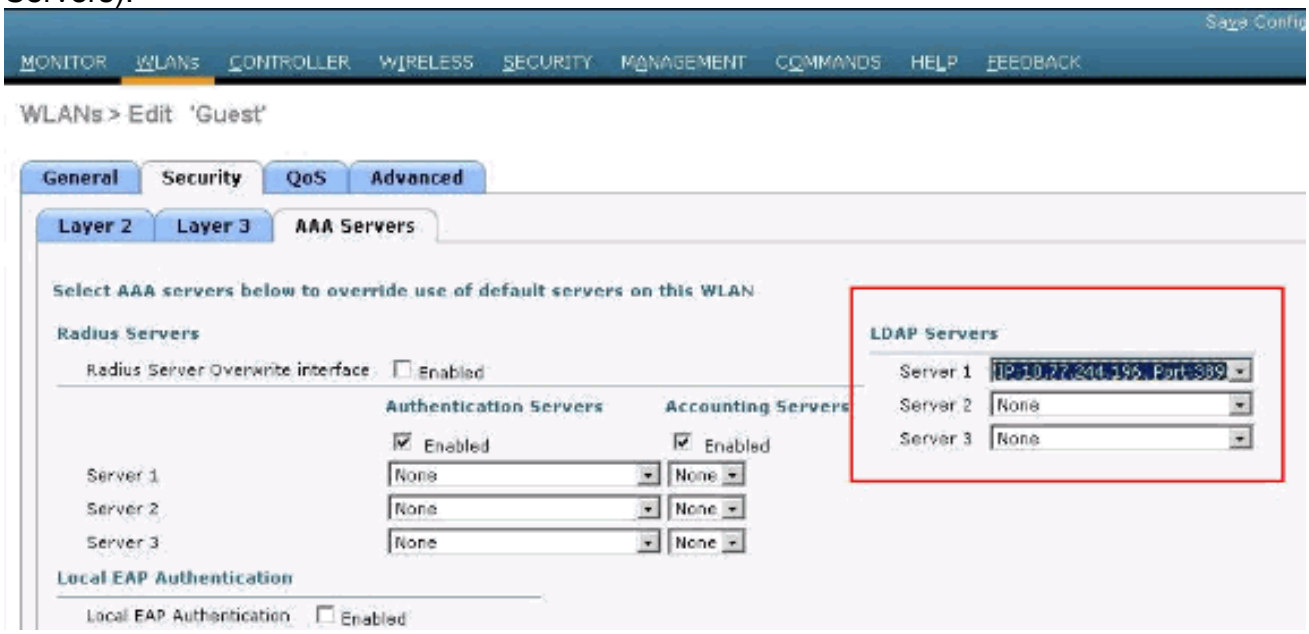
Complete estos pasos para configurar el LDPA mediante la interfaz gráfica de usuario del controlador:

1. Haga clic en Security > > para abrir a los servidores LDAP.Esta página enumera los servidores LDAP que ya se han configurado.Si desea borrar a un servidor LDAP existente, mueva su cursor sobre la flecha desplegable azul hasta encontrar dicho servidor y elija la opció Remove.Si desea asegurarse de que el controlador puede alcanzar un servidor determinado, desplace su cursor sobre la flecha desplegable azul hasta encontrar dicho servidor y elija la opción Ping.
2. Haga lo siguiente:Para editar a un servidor LDAP existente, haga clic en el número de índice de ese servidor. Se abrirá la ventana LDAP Servers > Edit.Para agregar a un servidor LDAP, haga clic en New. Se abrirá la ventana LDAP Servers >
   New.



3. Si desea agregar un nuevo servidor, elija un número del cuadro desplegable Server Index (Priority) para especificar el orden de prioridad de este servidor en relación con cualquier otro servidor LDAP configurado. Puede configurar hasta diecisiete servidores. Si el controlador no puede alcanzar el primer servidor, intentará comunicarse con el segundo de la lista y así sucesivamente.
4. Si desea agregar un nuevo servidor, ingrese el la dirección IP del servidor LDAP en el campo Server IP Address.
5. Si desea agregar un nuevo servidor, ingrese el número de puerto TCP del servidor LDAP en el campo Port Number. El intervalo válido es 1 a 65535, y el valor predeterminado es 389.
6. Marque el cuadro Enable Server Status para habilitar este servidor LDAP, o desmárquelo para inhabilitarlo. Se inhabilitará el valor predeterminado.
7. En el cuadro desplegable Simple Bind, elija Anonymous o Authenticated para especificar el método de vinculación de autenticación local para el servidor LDAP. El método Anonymous permite el acceso anónimo al servidor LDAP, mientras que el método Authenticated requiere un nombre de usuario y contraseña para un acceso seguro. El valor predeterminado es Anonymous.
8. Si eligió Authenticated en el paso 7, complete estos pasos:En el campo Bind Username, ingrese un nombre de usuario que se utilizará para la autenticación local al servidor LDAP.En los campos Bind Password y Confirm Bind Password, ingrese una contraseña que se utilizará para la autenticación local al servidor LDAP.
9. En el campo User Base DN, ingrese el nombre distintivo (DN) de la sub-estructura en el servidor LDAP que contiene una lista de todos los usuarios. Por ejemplo, ou=organizational unit, .ou=next organizational unit o o=corporation.com. Si la estructura que contiene los usuarios es la base DN, entonces el tipo o=corporation.com o dc=corporation, dc=com.
10. En el campo User Attribute, ingrese el nombre del atributo en el registro de usuarios que contiene el nombre de usuario. Puede obtener este atributo de su servidor de directorio.
11. En el campo User Object Type, ingrese el valor del atributo objectType del LDAP que identifica el registro como usuario. A menudo, los registros de usuario tienen varios valores para el atributo objectType, algunos de los cuales son únicos al usuario y otros son compartidos con otros tipos de objeto.

12. En el campo Server Timeout, ingrese el número de segundos entre las retransmisiones. El intervalo válido es de 2 a 30 segundos, y el valor predeterminado es 2 segundos.
13. Haga clic en Apply para aplicar sus cambios.
14. Haga clic en Save Configuration para guardar sus cambios.
15. Complete estos pasos si desea asignar servidores LDAP específicos a una WLAN:Haga clic en WLANs para abrir la ventana WLANs.Haga clic en el número de ID de la WLAN deseada.Cuando se abra la página WLANs > Edit, haga clic en las pestañas Security > AAA > Servers para abrir la ventana WLANs > Edit (Security > Servers).



En los cuadros desplegables DLAP Servers, elija los servidores LDAP que desea utilizar con esta WLAN. Puede elegir a hasta tres servidores LDAP, con los que se intentará conectar en orden de prioridad.Haga clic en Apply para aplicar sus cambios.Haga clic en Save Configuration para guardar sus cambios.

Configuración de Cliente WLAN para Usar la Autenticación Web

Una vez que se configura el WLC, el cliente debe ser configurado apropiadamente para la autenticación Web. En esta sección, encontrará información para configurar su Sistema Windows para la autenticación Web.

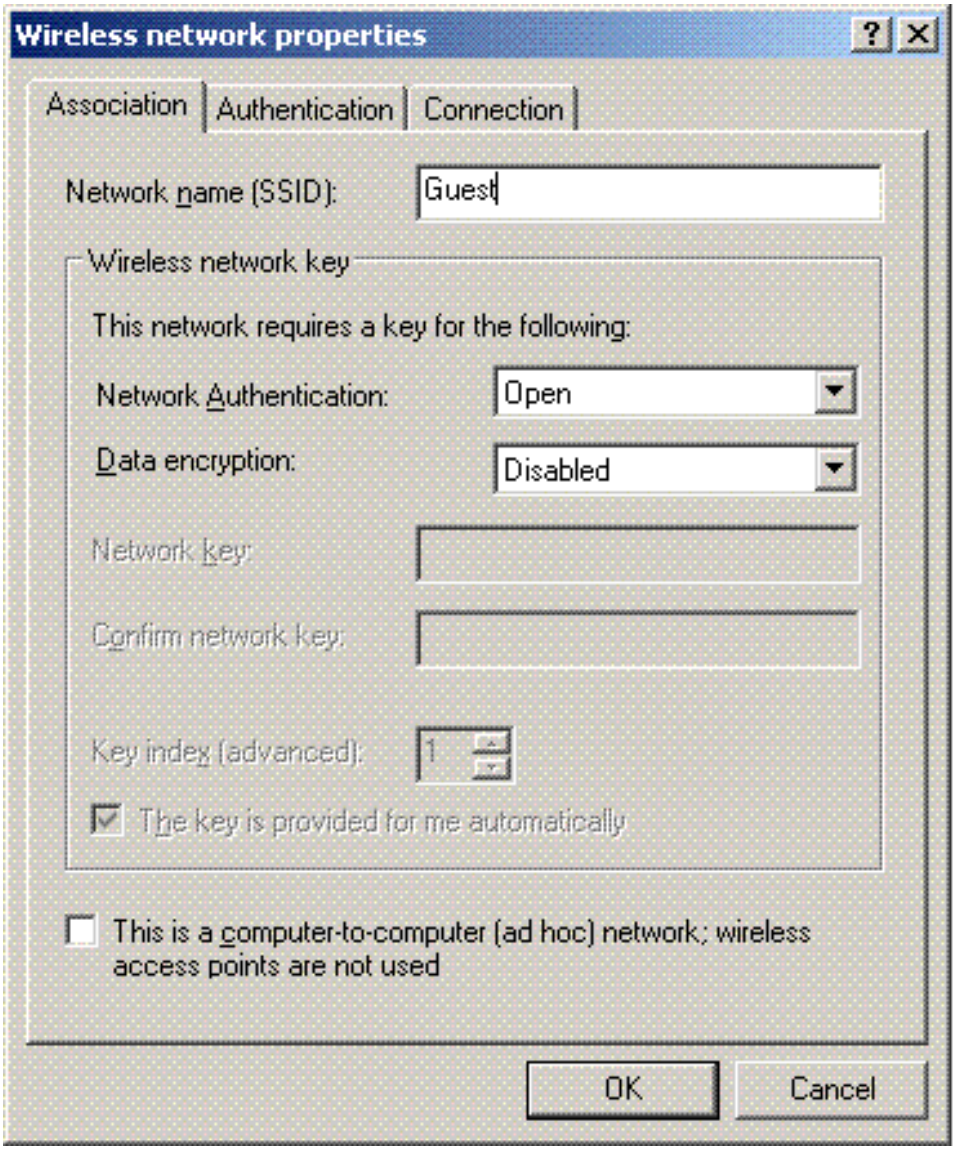
Configuración del Cliente

La configuración de cliente de red inalámbrica de Microsoft sigue sin modificarse para este suscriptor. Necesita agregar solamente información de configuración adecuada de WLAN/SSID. Complete estos pasos:

1. Del menú de Inicio de Windows, elija **Settings > Control Panel > Network and Internet Connections**.
2. Haga clic en el icono de **Network Connections**.
3. Haga clic en clic el botón derecho del mouse en el icono de **Conexión LAN** y elija la **inhabilitar**.
4. Haga clic con el botón derecho del mouse en el icono de **Wireless Connection** y elija **Enable**.
5. Haga clic con el botón derecho del mouse en el icono de **Wireless Connection** nuevamente y

elija **Properties**.

6. De la ventana Wireless Network Connection Properties, haga clic en la pestaña **Wireless Networks**.
7. En el área de redes preferidas, haga clic en **Agregar** para configurar la autenticación Web SSID.
8. Bajo la pestaña Association, ingrese el valor de Nombre de Red (WLAN/SSID) que desea utilizar para la autenticación
   Web.



   Nota: El Cifrado de Datos es Wired Equivalent Privacy (WEP) de forma predeterminada. Inhabilite Cifrado de Datos para que la autenticación Web funcione.
9. Haga clic en OK en la parte inferior de la ventana para guardar la configuración.Cuando usted se comunica con la WLAN, puede ver un icono beacon en el cuadro de Red Preferida.

Esto muestra una conexión de red inalámbrica exitosa en la autenticación Web. El WLC le ha proporcionado su cliente de red inalámbrica de Windows una dirección IP.

Nota: Si su cliente de red inalámbrica es también un punto extremo VPN y usted tiene autenticación Web configurada como función de seguridad para la WLAN, el túnel VPN no se establece hasta que usted atraviese el proceso de autenticación Web que aquí se explica. Para establecer un túnel VPN, el cliente debe primero pasar por el proceso de autenticación Web con el éxito. Después de este proceso, la tunelización VPN es satisfactoria.

Nota: Después de un inicio de sesión exitoso, si los clientes de red inalámbrica no se comunican con los otros dispositivos, dichos cliente serán de-autenticados después de un período de tiempo de inactividad. El período de agotamiento del tiempo de espera es de 300 segundos por defecto y se puede cambiar usando este comando CLI: config network usertimeout . &seconds>. Cuando esto ocurra, se eliminará la entrada del cliente del controlador. Si el cliente se asocia otra vez, se moverá de nuevo a un estado de Webauth_Reqd.

Nota: Si los clientes están inactivos después de un inicio de sesión satisfactorio, serán des-autenticados y es posible que la entrada se elimine del controlador después del período de agotamiento de tiempo de espera de la sesión configurado en la WLAN (por ejemplo, 1800 segundos por defecto, que pueden cambiarse usando el siguiente comando: config wlan session-timeout 6amp;WLAN ID> &seconds>). Cuando esto ocurra, se eliminará la entrada del cliente del controlador. Si el cliente se asocia otra vez, se moverá de nuevo a un estado de Webauth_Reqd.

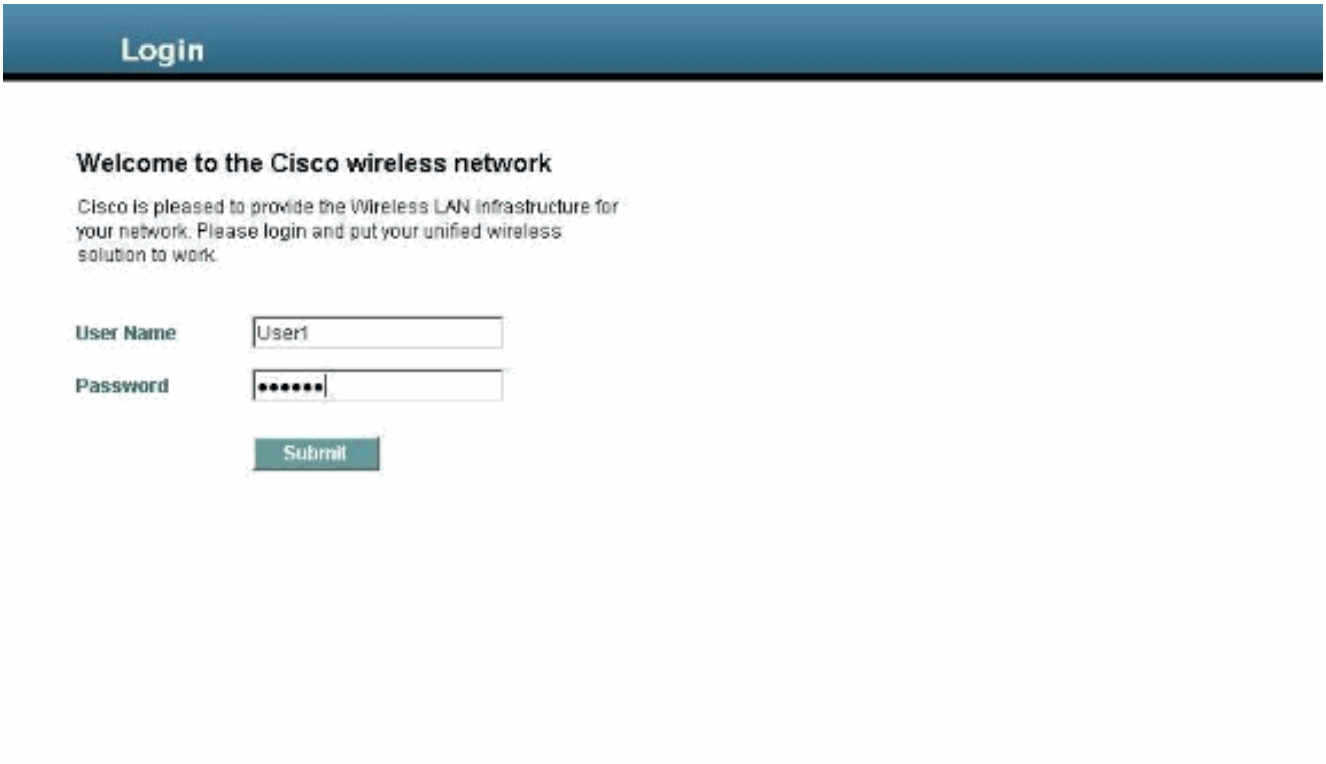
Sin importar si están activos o no, los clientes en estado de Webauth_Reqd serán des-autenticados una vez se agote el período de tiempo de espera de web-auth (por ejemplo, 300 segundos, que no pueden ser configurados por el usuario). Todo el tráfico del cliente (permitido vía el Pre-Auth ACL) será interrumpido. Si el cliente se asocia otra vez, se moverá de nuevo al estado de Webauth_Reqd.

Login del Cliente

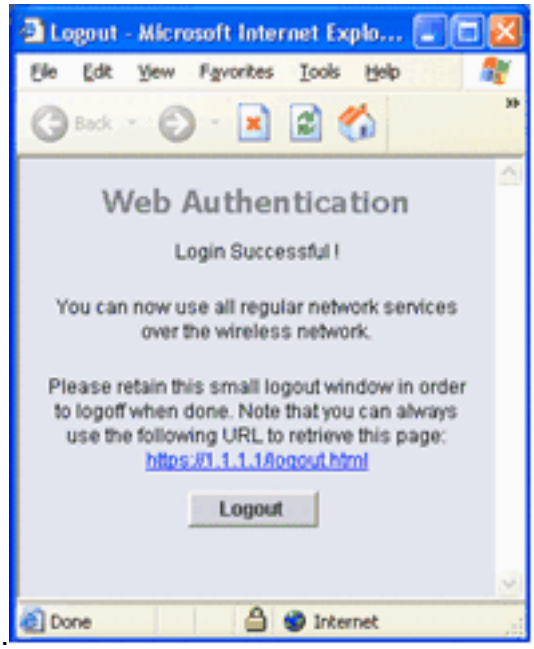
Complete estos pasos:

1. Abra un navegador e ingrese cualquier URL o dirección IP. Esto trae la página de autenticación Web al cliente.Si el regulador está funcionando con cualquier versión anterior a la 3.0, el usuario tiene que 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 de login, ingrese el nombre de usuario y contraseña del usuario de red local que usted
creó.



Si su login es correcto, podrá ver las dos ventanas del buscador. La ventana más grande indica un inicio de sesión exitoso, y puede utilizar esta ventana para navegar. Use la ventana más pequeña para cerrar la sesión cuando deje de usar la red del invitado.La captura de pantalla muestra un redireccionamiento exitoso a la página de autenticación Web.La captura de pantalla a continuación muestra la ventana de inicio de sesión exitoso que se muestra cuando ha ocurrido la autenticación.



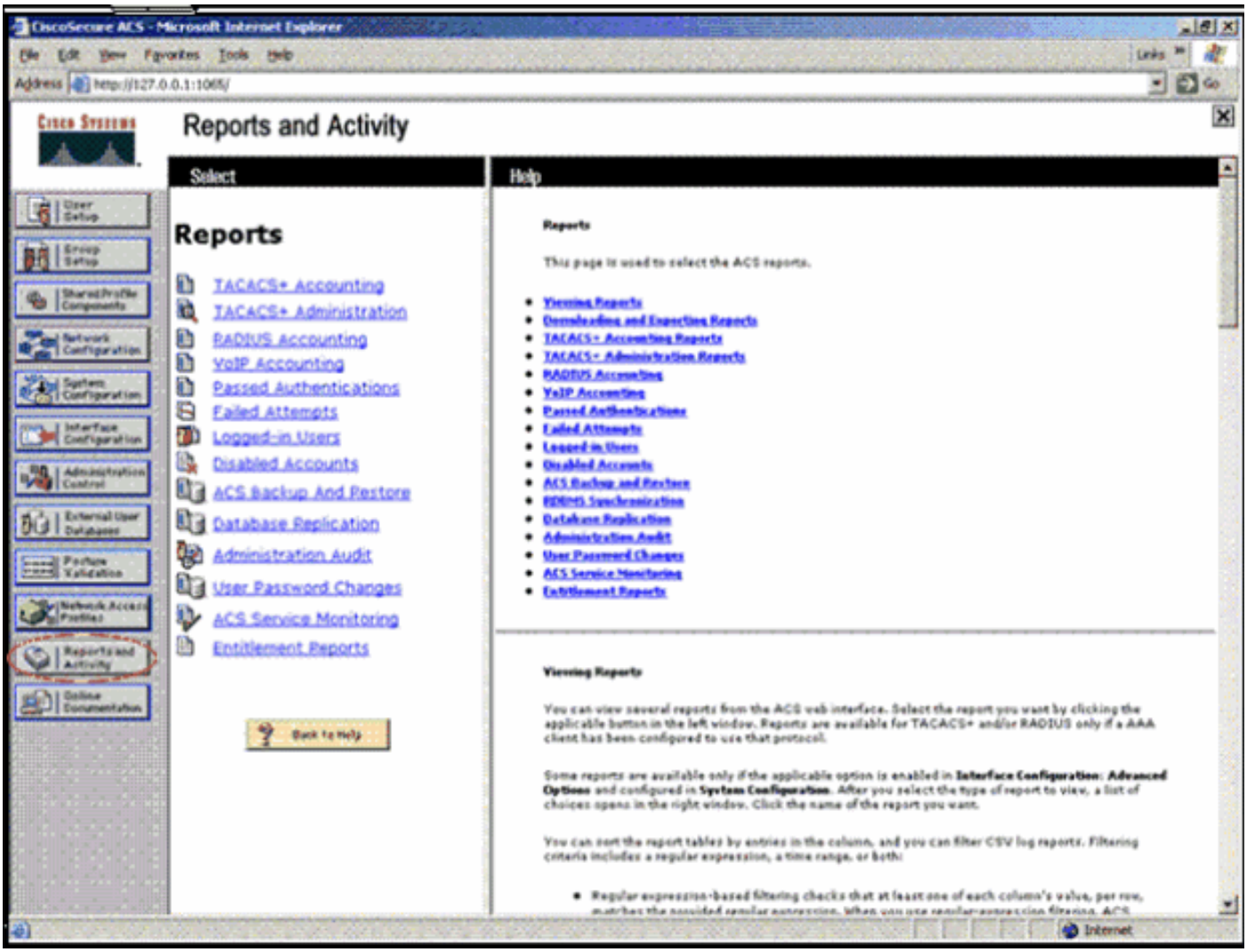
Los controladores Cisco 4404/WiSM pueden soportar 125 sesiones iniciadas en simultáneo de usuarios con autenticación Web, y esta cantidad puede aumentarse a 5000 clientes con autenticación Web.

Los reguladores Cisco 4404/WiSM pueden soportar 125 sesiones iniciadas en simultáneo de usuarios con autenticación Web.

Troubleshooting de Autenticación Web

Troubleshooting ACS

Si tiene problemas con la autenticación de contraseña, haga clic en **Informes y Actividad** en el lado izquierdo de ACS para abrir todos los informes disponibles. Después de que abra la ventana informes, tiene la opción de abrir Contabilidad de RADIUS, Intentos Fallidos para el login, Autenticaciones Aprobadas , Usuarios Registrado, y otros informes. Estos informes son archivos .csv, y puede abrir los archivos localmente en su equipo. Los informes ayudan a descubrir los problemas con la autenticación, tal como nombre de usuario o contraseña incorrectos. El ACS también viene con la documentación en línea. Si no está conectado con una red activa y no ha definido el puerto del servicio, el ACS utiliza la dirección IP de su acceso de Ethernet para su puerto del servicio. Si su red no está conectada, probablemente termine con la dirección IP predeterminada de Windows 169.254.x.x.



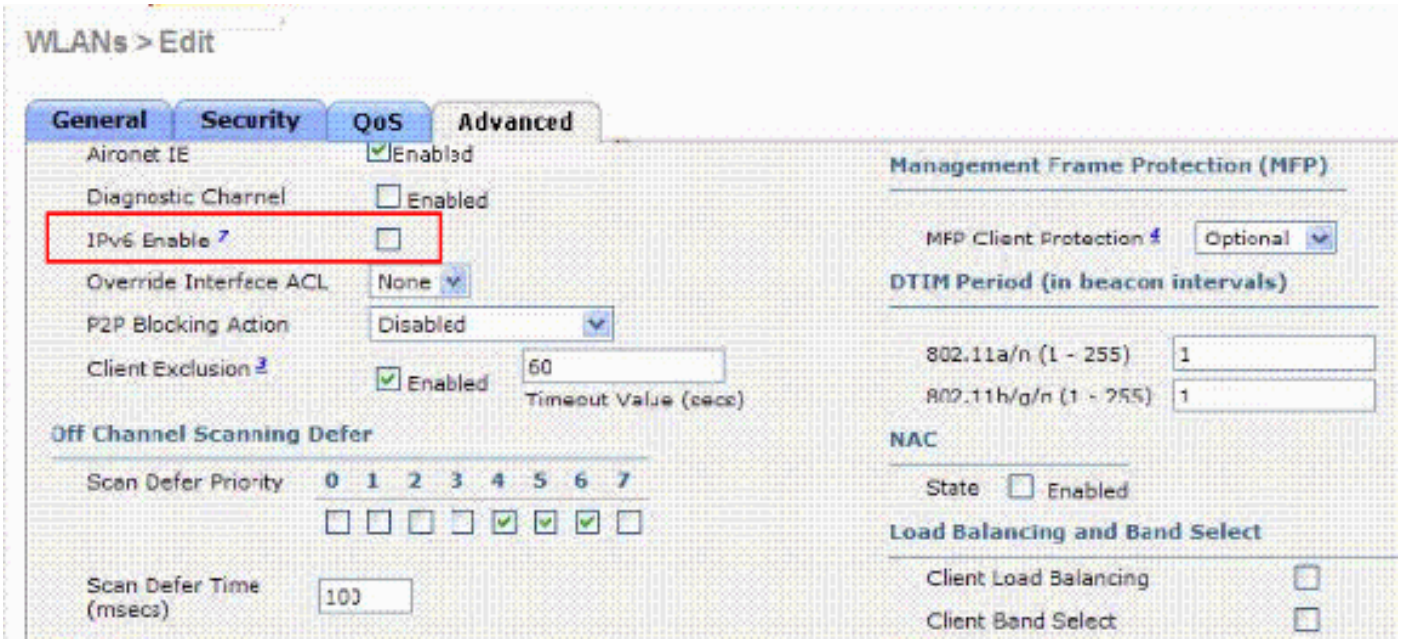
Nota: Si escribe en cualquier URL externa, el WLC se conecta automáticamente con la página de la autenticación web interna. Si la conexión automática no funciona, puede ingresar la dirección IP de administración del WLC en la barra de URL para resolver problemas. Lea el mensaje que le indica redirección para la autenticación Web en la parte superior del buscador.

Consulte Troubleshooting de Autenticación Web en Controladores LAN Inalámbricos (WLC) para obtener más información sobre troubleshooting de autenticación Web.

Autenticación Web con Puente IPv6

Para configurar una para el puente IPv6, diríjase a WLANs en la interfaz gráfica de usuario del controlador. Después, seleccione la WLAN deseada y elija Advanced en la página WLANs > Edit.

Seleccione la casilla de verificación IPv6 Enable si desea habilitar a los clientes que se conectan con esta WLAN para aceptar paquetes IPv6. Si no, deje la casilla de verificación no seleccionada, que es el valor predeterminado. Si usted inhabilita (o desmarca) la casilla de verificación IPv6, el IPv6 se permitirá solamente después de la autenticación. Habilitar el IPv6 significa que el controlador podrá pasar el tráfico del IPv6 sin la autenticación de cliente.



Para obtener información más detallada sobre puente IPv6 y las guías de uso de esta función, consulte la sección Configuración del Puente IPv6 de la Guía de configuración del controlados LAN inalámbrico Cisco, versión 7.0.

Información Relacionada

- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Troubleshooting de autenticación Web en controlador LAN inalámbrico
- Red Inalámbrica Cisco LAN
- Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers
- Guía de configuración del controlador LAN inalámbrico Cisco, versión 7.0: Administración de cuentas de usuario
- Autentificación del Administrador Lobby deWireless LAN Controller a través del Servidor RADIUS
- Soporte Técnico y Documentación - Cisco Systems