Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN

Contenido

Introducción

Este documento explica cómo Cisco implementa la autenticación Web y muestra cómo configurar un regulador del Wireless LAN de las Cisco 4400 Series (WLAN) (WLC) para soportar una autenticación del 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.

- Un WLC de las 4400 Series que funciona con la versión 7.0.116.0
- La versión 4.2 del Cisco Secure Access Control Server (ACS) instaló en un servidor de Windows 2003 del Microsoft®
- Lightweight Access Point de la serie del Cisco Aironet 1131AG
- Adaptador de red inalámbrica de CardBus del a/b/g del 802.11 del Cisco Aironet que funciona con la 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 al regulador no permitir el tráfico IP (excepto el DHCP y el DNS - los paquetes relacionados) de un cliente particular hasta que ese cliente haya suministrado correctamente un nombre de usuario válido y una contraseña. Es un método de autenticación simple sin la necesidad de un supplicant 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 usando:

- Ventana predeterminada del login en el WLC
- Versión modificada de la ventana predeterminada del login en el WLC
- Una ventana personalizada del login que usted configura en un servidor Web externo (autenticación del Web externa)
- Una ventana personalizada del login que usted descarga al regulador

En este documento, el regulador del Wireless LAN para la autenticación del Web interna se configura.

Proceso de autenticación Web

Esto es qué ocurre cuando un usuario conecta con una red inalámbrica (WLAN) configurada para la autenticación Web:

- El usuario abre a un buscador Web y ingresa un URL, por ejemplo, http://www.cisco.com. El cliente envía una petición DNS para que este URL consiga el IP para el destino. El WLC

desvía la petición DNS al servidor DNS y el servidor DNS responde detrás con una contestación DNS, que contiene la dirección IP del destino www.cisco.com. Esto, a su vez, se remite a los clientes de red inalámbrica.

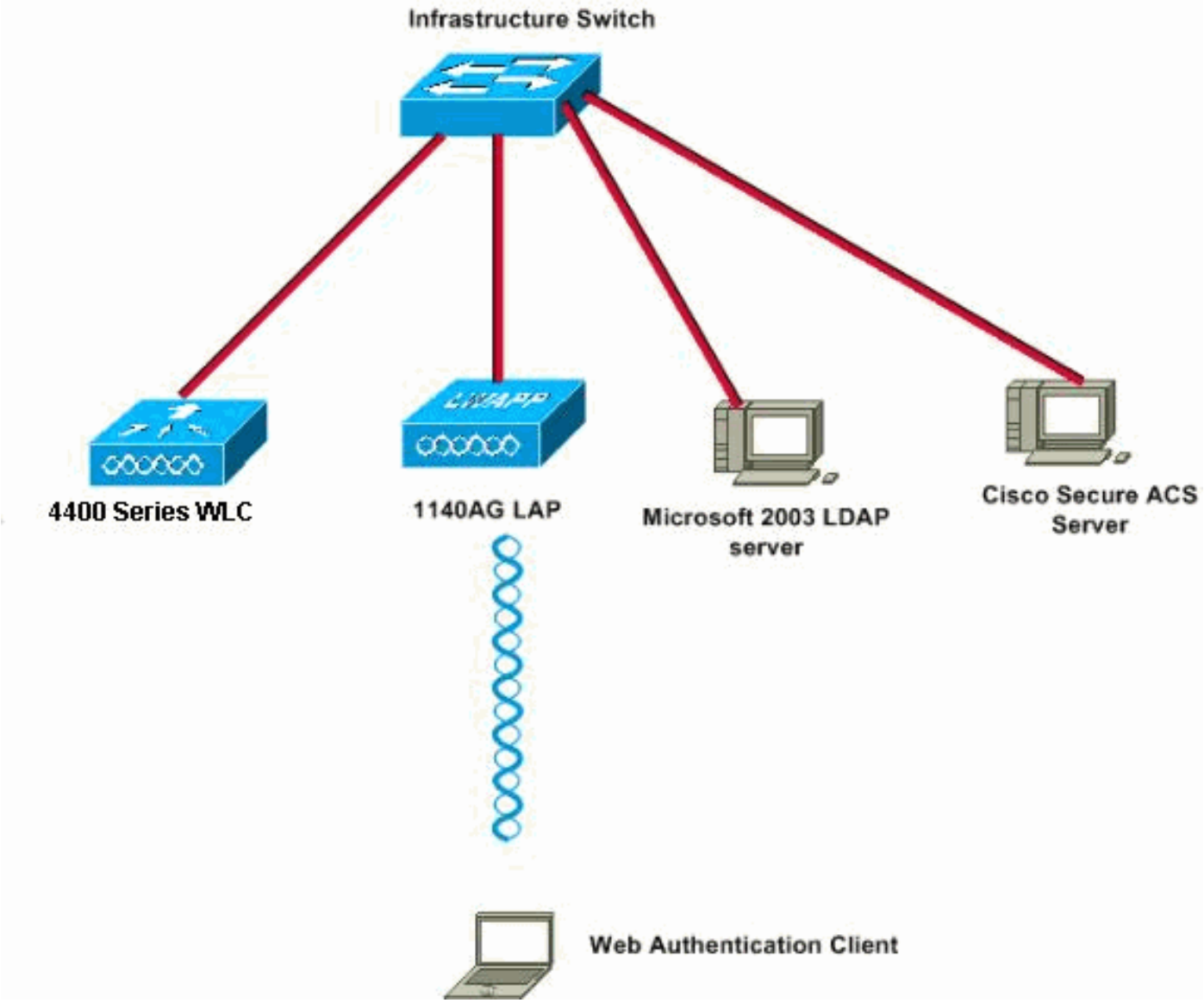
- El cliente entonces intenta abrir una conexión TCP con el IP Address de destino. Envía paquete TCP Syn un destinado a la dirección IP de www.cisco.com.
- El WLC tiene reglas configuradas para el cliente y por lo tanto puede actuar como proxy para www.cisco.com. Devuelve un paquete TCP SYN-ACK al cliente con la fuente como la dirección IP de www.cisco.com. El cliente devuelve un paquete ACK TCP para completar la aceptación decontacto con 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 la dirección del cambio de dirección. El gateway de aplicación HTTP prepara a un cuerpo del HTML y lo envía detrás como la contestación al HTTP GET pedido por el cliente. Este HTML hace que el cliente va a la página web predeterminada URL del WLC, por ejemplo, http:// <Virtual-Server-IP>/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 WLC responde detrás con un TCP SYN-ACK y el cliente devuelve un TCP ACK al WLC para completar el apretón de manos.
- El cliente envía un HTTP GET para /login.html destinó a 1.1.1.1 para petición la página de registro.
- Esta petición se permite hasta el servidor Web del WLC, y el servidor responde detrás con la página de registro predeterminada. El cliente recibe la página de registro en la ventana del buscador donde el usuario puede continuar y iniciar 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 de la tecnología inalámbrica de Cisco (WLCs)

Configuración de la red

En este documento, se utiliza esta configuración de red:



Configuración del Controlador para la Autenticación Web

En este documento, una red inalámbrica (WLAN) se configura para la autenticación Web y se asocia a un vlan dedicada. Éstos son los pasos implicados para configurar una red inalámbrica (WLAN) para la autenticación Web:

- Creación de una Interfaz VLAN
- Configure el WLC para la autenticación del Web interna
- Agregado de una Instancia WLAN
- Configure el tipo de autenticación (tres maneras de autenticar a los usuarios en la autenticación Web)

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

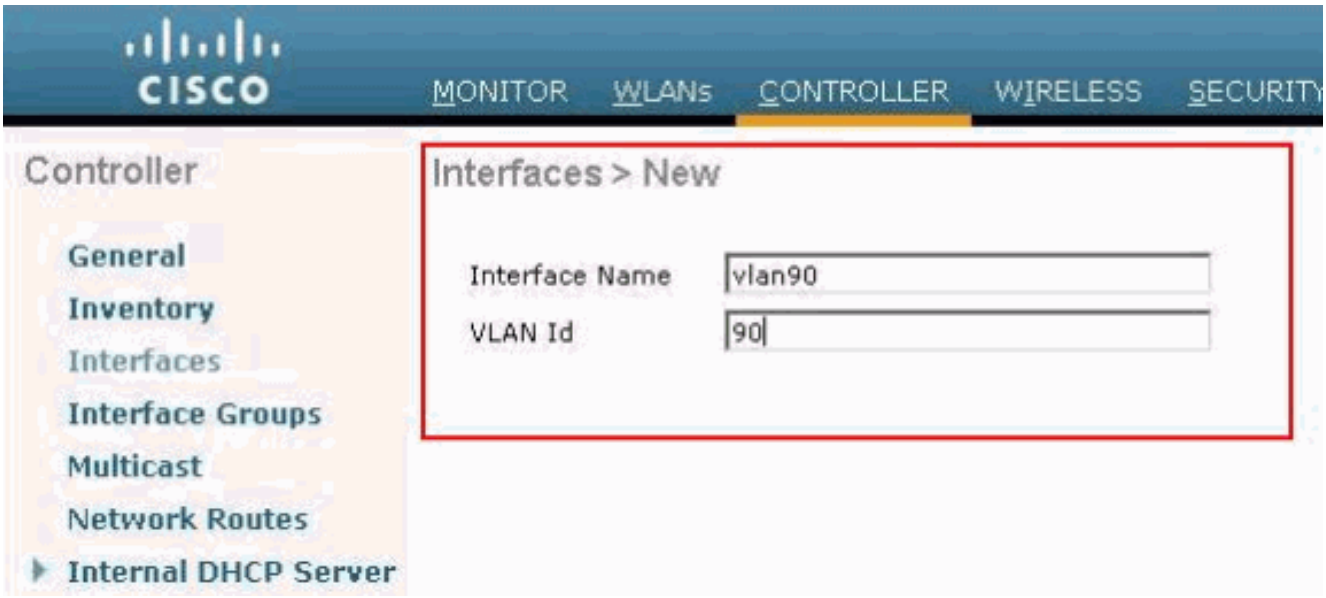
Las siguientes son direcciones IP usadas en este documento:

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

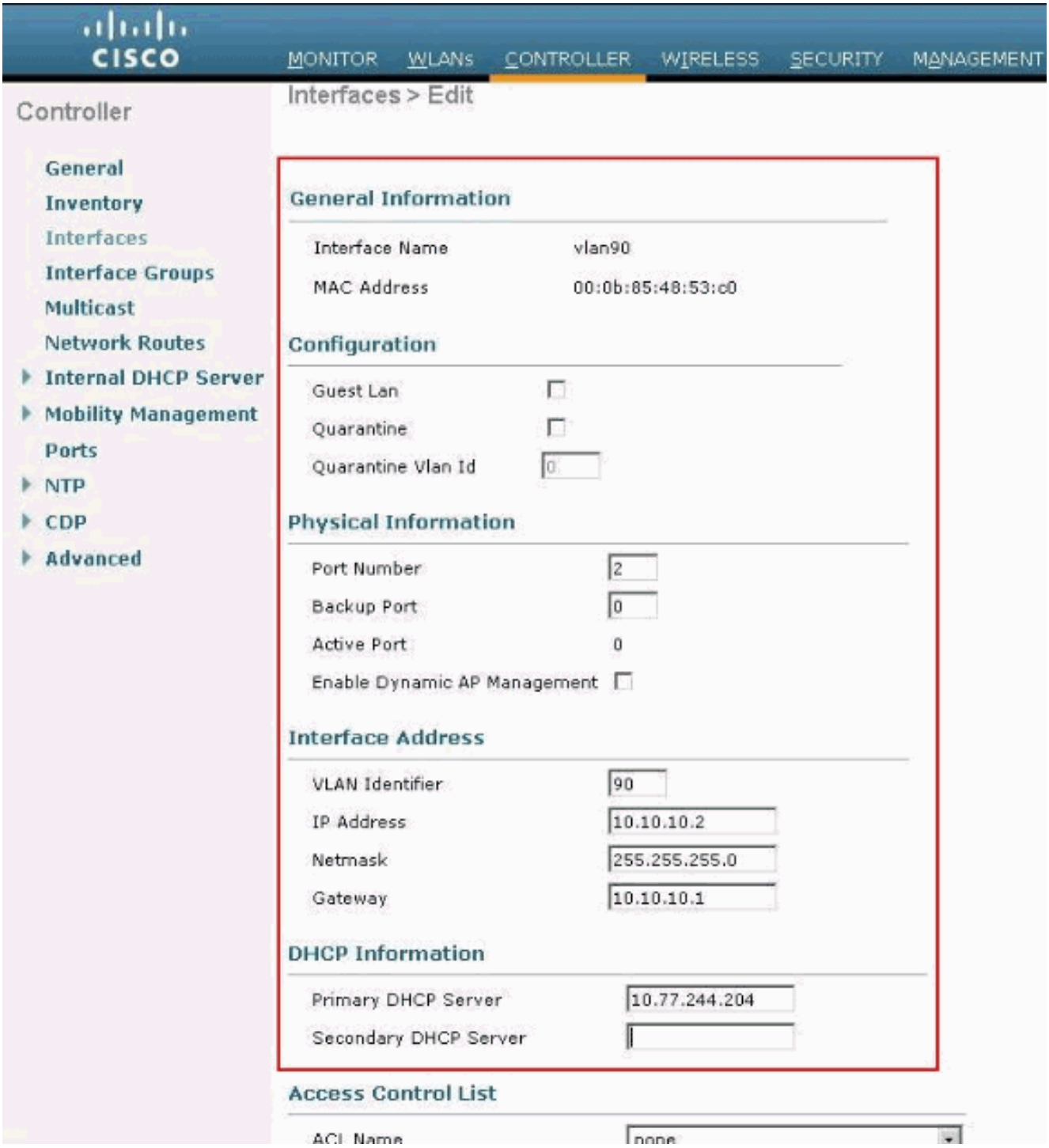
Creación de una Interfaz VLAN

Complete estos pasos:

1. Del regulador GUI del Wireless LAN, elija el **regulador del** menú en el top, elija las **interfaces del** menú a la izquierda, y haga clic **nuevo** en el extremo superior derecho de la ventana para crear una nueva interfaz dinámica.**Las interfaces > la nueva ventana** aparece. Este ejemplo utiliza Nombre de *Interfaz* con una VLAN ID de *90*:



2. Haga clic en **Aplicar** para crear la interfaz VLAN.**Las interfaces > editan la** ventana aparecen que pide que usted llene la información del específico de la interfaz.
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



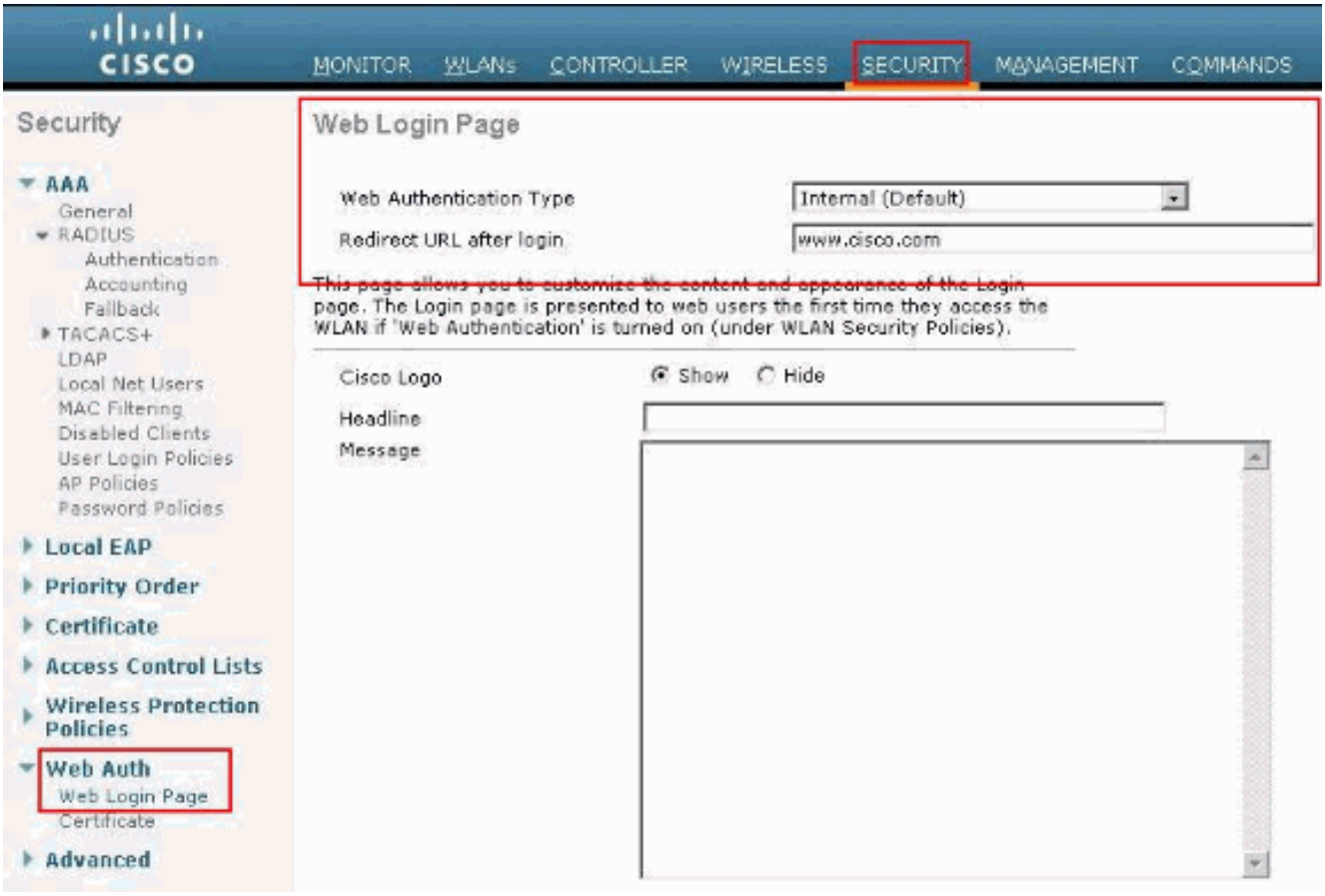
4. Haga clic en **Aply** para guardar los cambios.

WLC de la configuración para la autenticación del Web interna

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

1. Del regulador GUI, elija el **auth de la Seguridad** > de la **red** > la **página de registro de la red** para acceder la página de registro de la red.
2. De la casilla desplegable del tipo de la autenticación Web, elija la **autenticación del Web interna**.

3. En la **reorientación URL después del** campo del **login**, ingrese el URL de la página a la cual reorientarán al usuario final después de la autenticación satisfactoria.

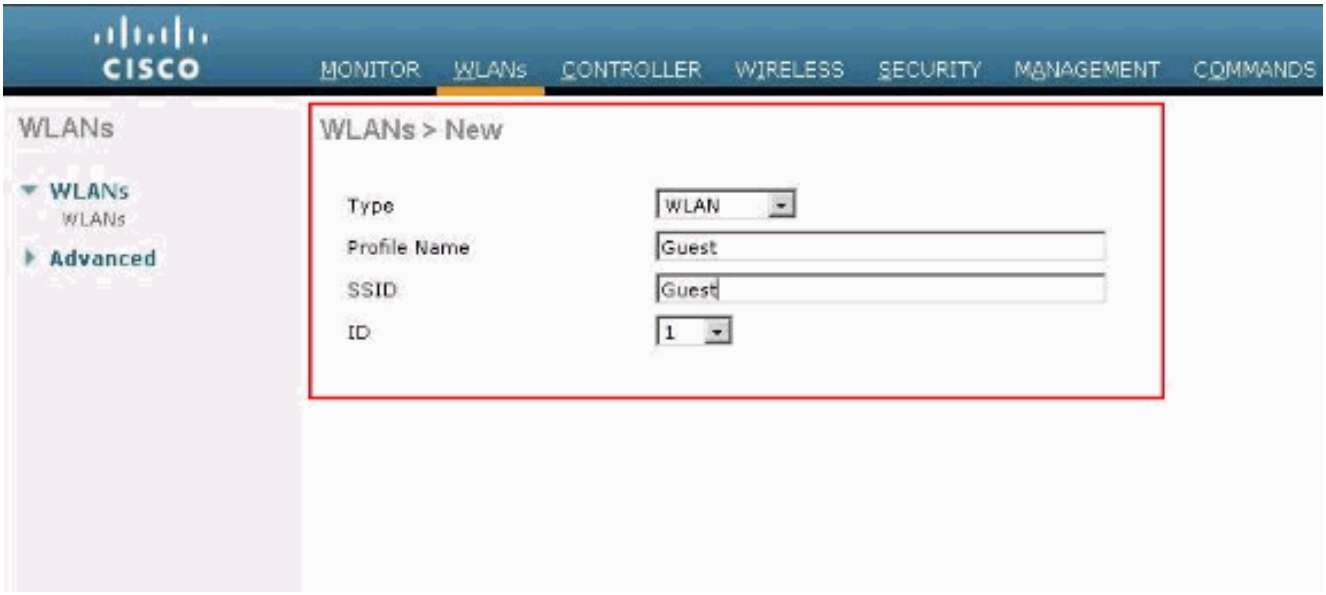


Nota: En las versiones 5.0 del WLC y posterior, la página del logout para la autenticación Web puede también ser personalizada. Refiera a las páginas del login, de la falla de registro y del logout de la asignación por la sección de la red inalámbrica (WLAN) de la *configuración de controlador Guide,5.2 del Wireless LAN* para más información sobre cómo configurarla.

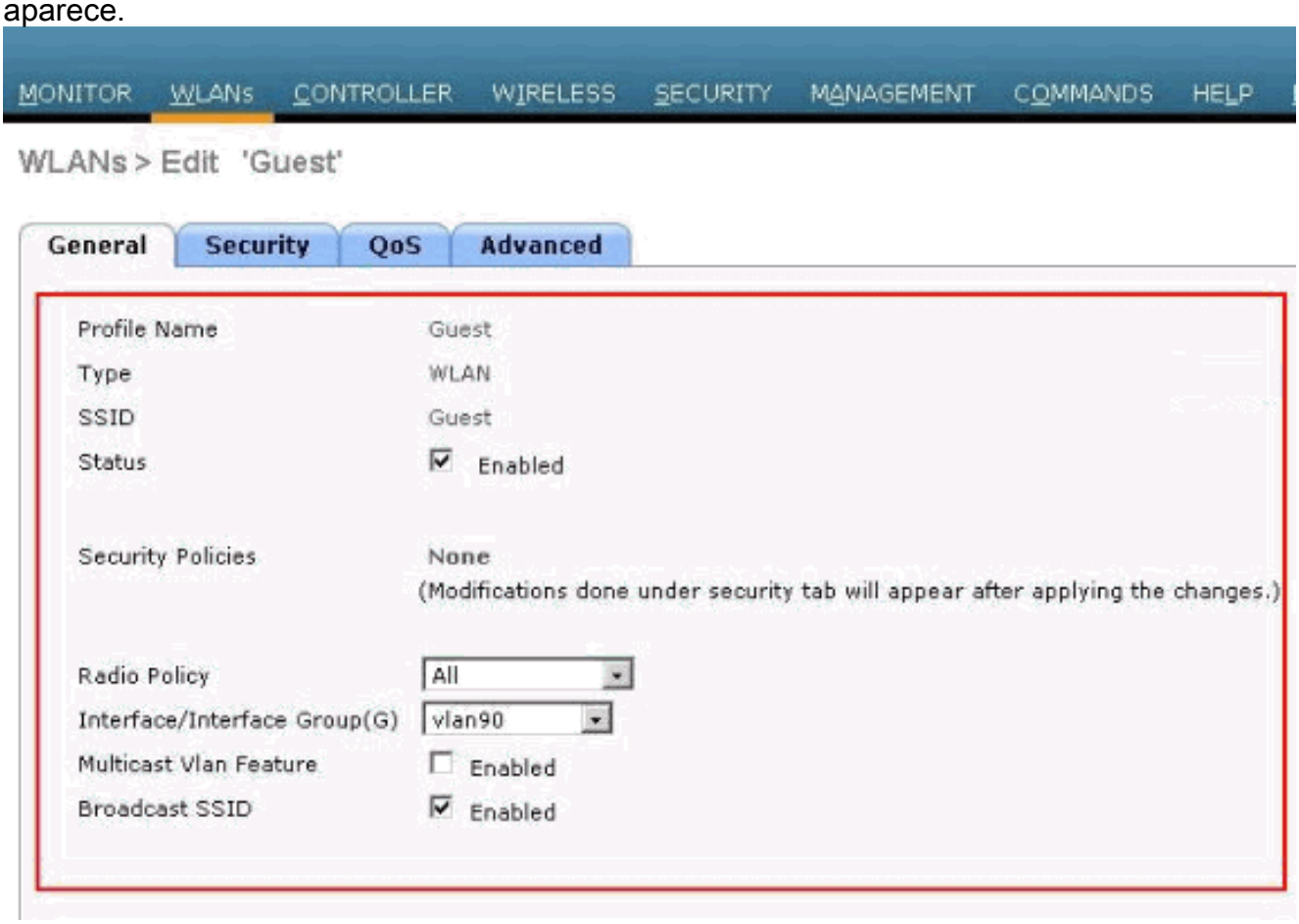
Agregado de una Instancia WLAN

Ahora que se ha habilitado la autenticación del Web interna y hay una interfaz VLAN dedicada para la autenticación Web, usted debe proporcionar un nuevo WLAN/SSID para apoyar a los usuarios de la autenticación Web.

1. Del WLC GUI, haga clic la **red inalámbrica (WLAN)** en el menú en el top, y haga clic **nuevo** 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.

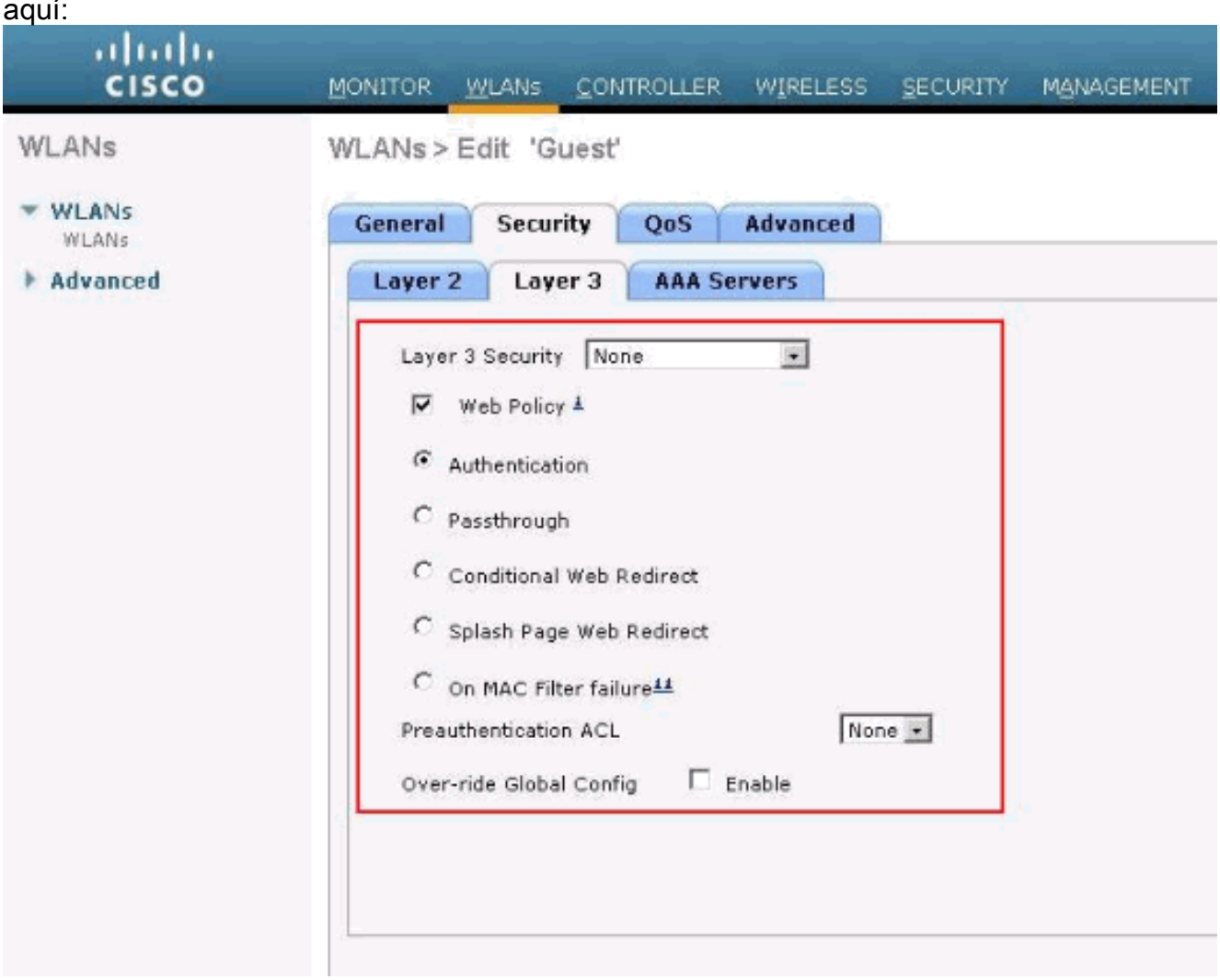


2. Haga clic en Apply (Aplicar).Un nuevo los WLAN > edita la ventana aparece.



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 de la **directiva de la red** y elija la ***opción de autenticación***, 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 a los usuarios en la autenticación Web

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

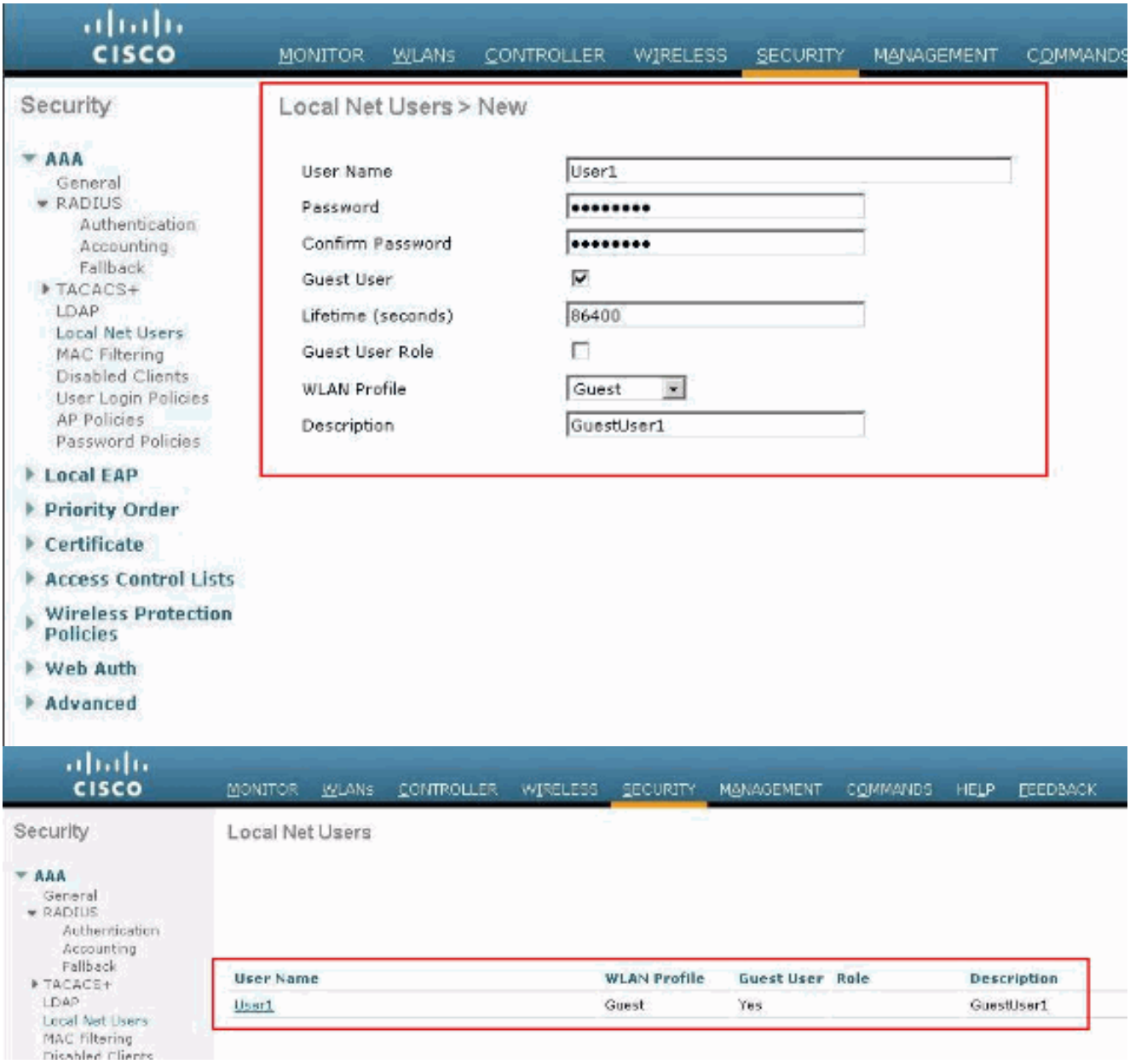
Este documento proporciona un ejemplo de configuración para los tres métodos.

Autenticación local

La base de datos de usuarios para los Usuarios invitados se salva en la base de datos local WLC. El WLC contra esta base de datos autentican a los usuarios.

1. Del WLC GUI, elija la **Seguridad**.
2. Haga clic a los **usuarios de red local del** menú AAA a la izquierda.

3. Haga clic **nuevo** para crear a un usuario nuevo.Visualizaciones de una nueva ventana que pide la información del nombre de usuario y contraseña.
4. Ingrese un Nombre de usuario y una contraseña para crear a un usuario nuevo, después confirme la contraseña que usted quiere utilizar.Este ejemplo crea al usuario nombrado **User1**.
5. Agregue una descripción, si lo desea.Este ejemplo utiliza el **user1 del invitado**.
6. Haga clic en **Aplicar** para guardar la configuración del usuario nuevo.



7. Relance los pasos 3-6 para agregar a 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.

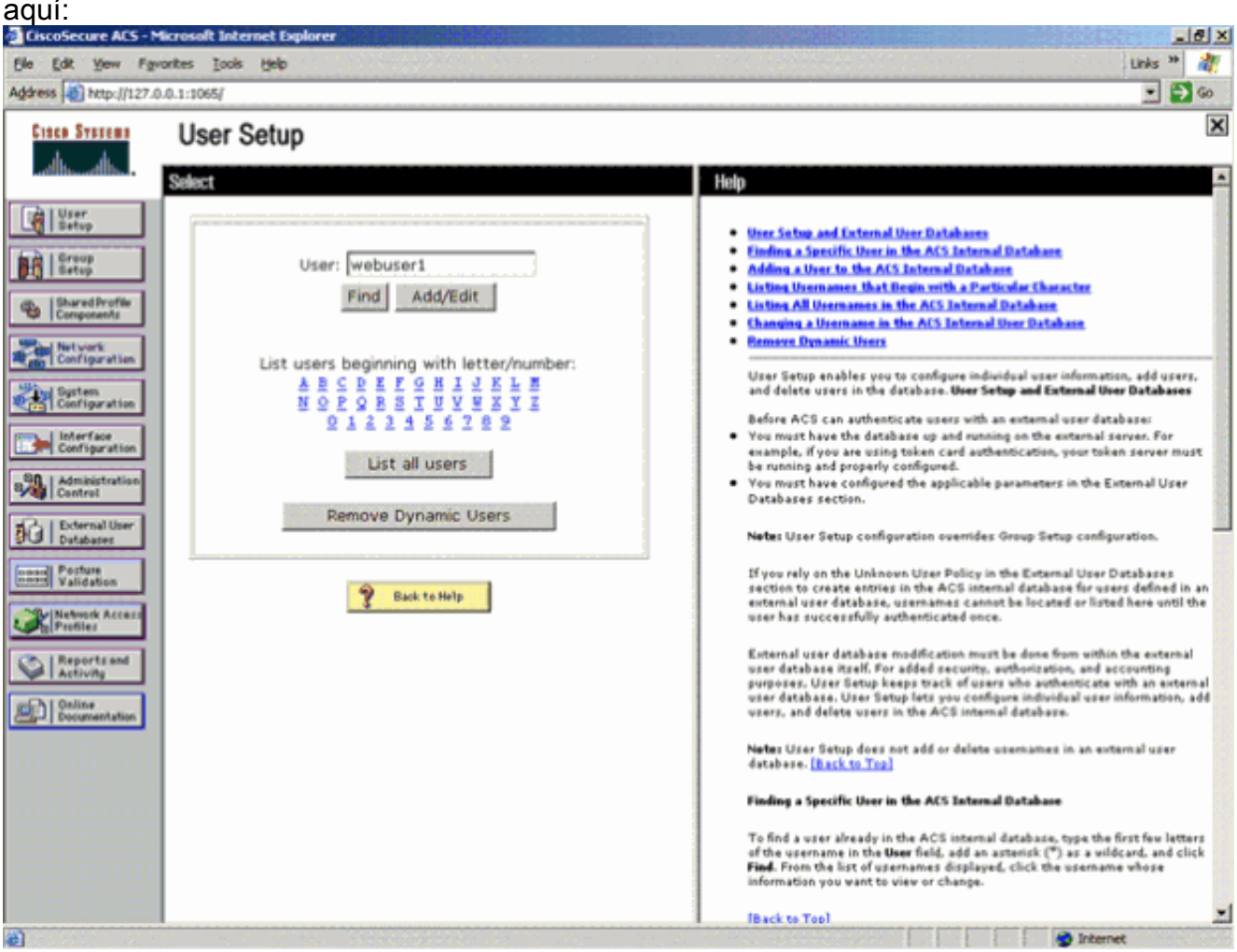
La sección Configuración ACS le muestra cómo configurar el ACS para el RADIUS. Debe tener red funcional a completamente - con un sistema de nombres del dominio (DN) y un servidor de RADIUS.

Configuración ACS

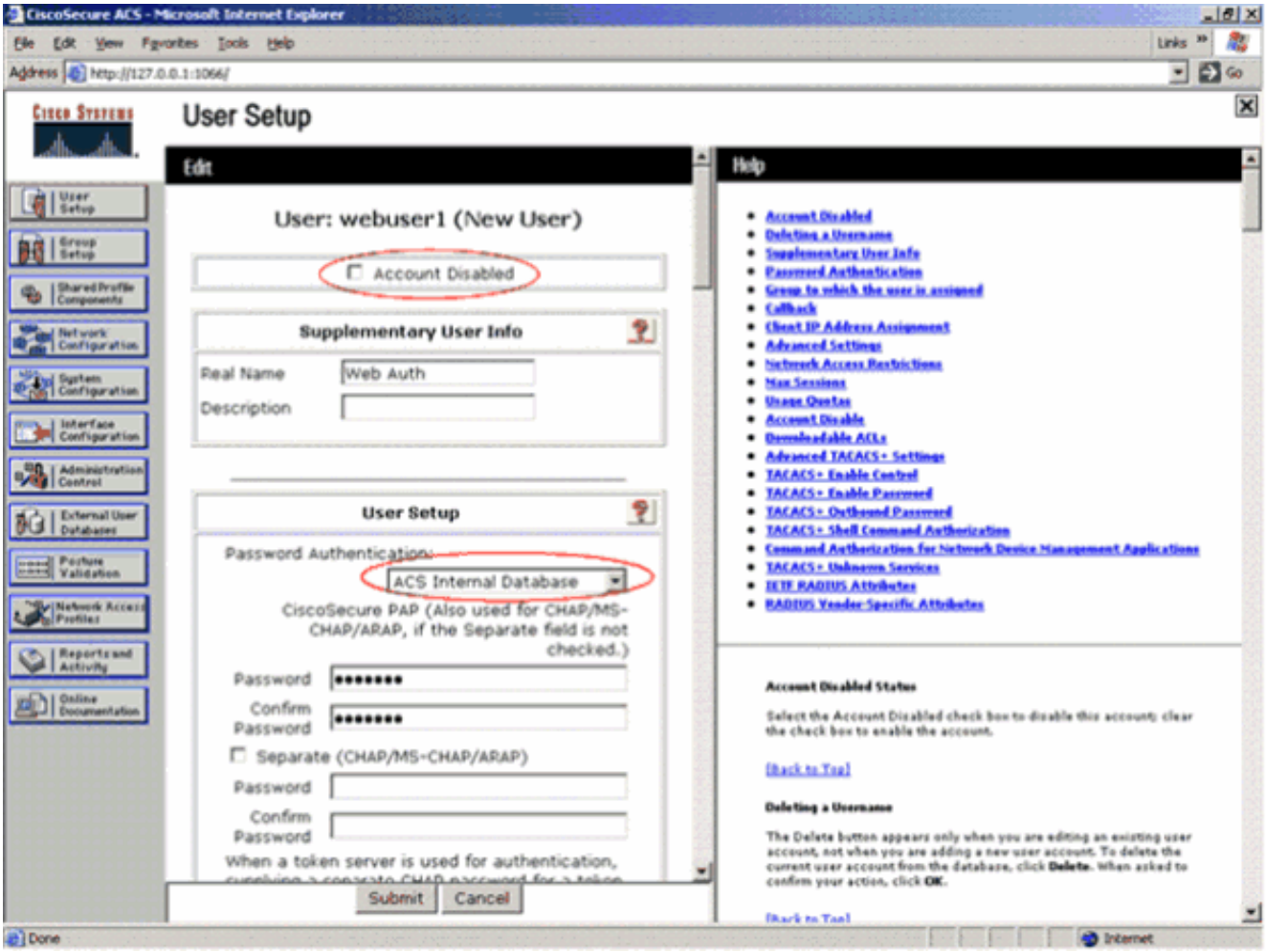
En esta sección, encontrará información para configurar el ACS para RADIUS.

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 que creen al usuario, una segunda ventana se abre como se muestra
   aquí:

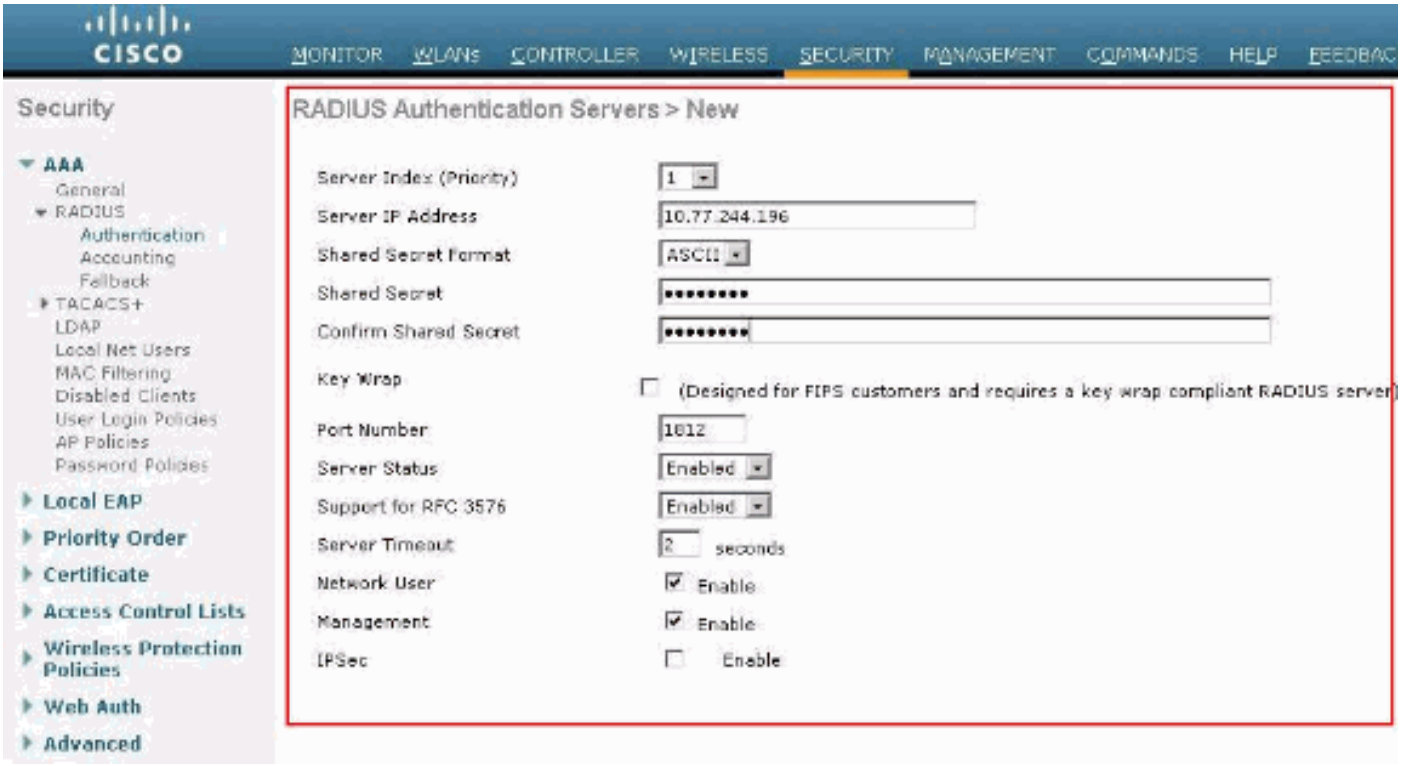


4. Asegúrese de que los **minusválidos de la cuenta** encajonen en el top no estén marcados.
5. Elija la **base de datos interna ACS** para la opción de la autenticación de contraseña.
6. Ingrese la contraseña. El Admin tiene una opción para configurar la autenticación PAP/CHAP o del MD5-CHAP mientras que agrega a un usuario en la base de datos interna ACS. El PAP es el tipo de la autenticación predeterminada para los usuarios del red-auth en los reguladores. 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).

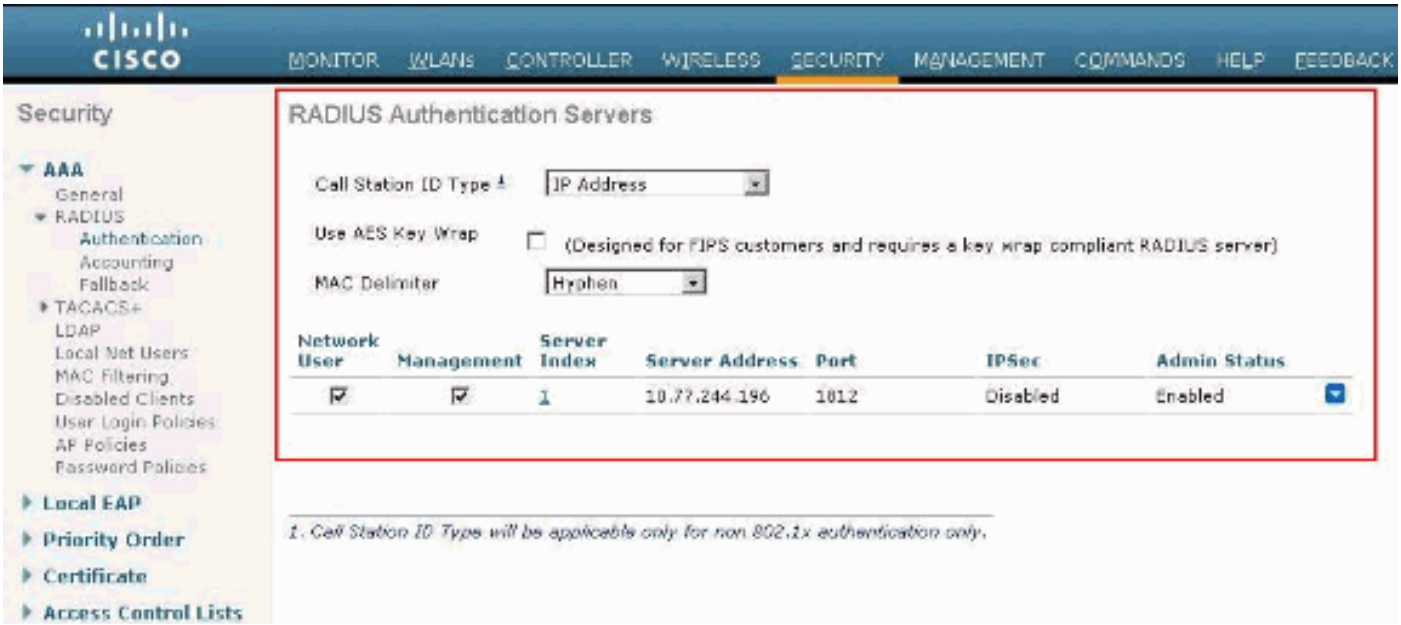
Ingrese su información del servidor de RADIUS en el WLC de Cisco

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 es lo mismo que la usted ingresó en el servidor de RADIUS para el 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 del **permiso del usuario de la red** para utilizar este servidor de RADIUS para los usuarios de autenticidad de su red inalámbrica.
8. Haga clic en Apply (Aplicar).



Aseegurese que el cuadro del *usuario de la red* está marcado y habilitan al *estado del administrador*.

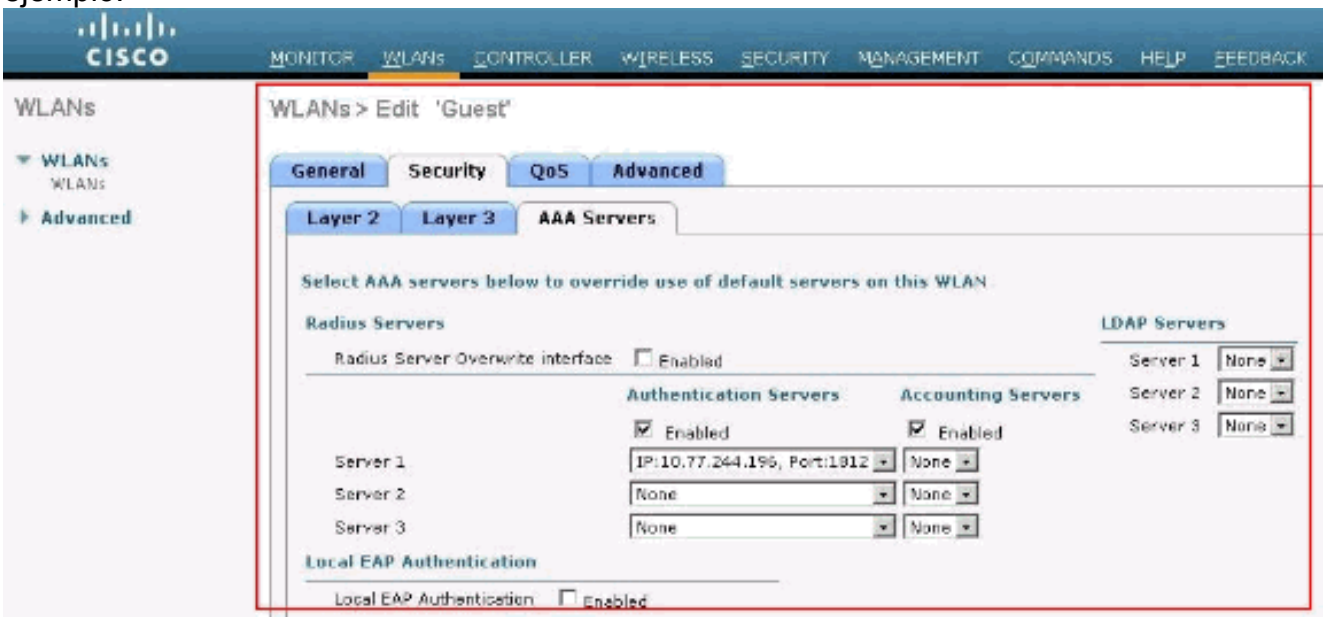


Configuración de WLAN con el Servidor RADIUS

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**. Esto visualiza la lista de WLAN configurados en el WLC. Haga clic al **invitado de la** red inalámbrica (WLAN) que fue creado para la autenticación Web.
2. En los **WLAN > editan el** tecleo de la página el **menú de seguridad**. Haga clic la lengueta de los **servidores de AAA** bajo Seguridad. Entonces, elija al servidor de RADIUS que es

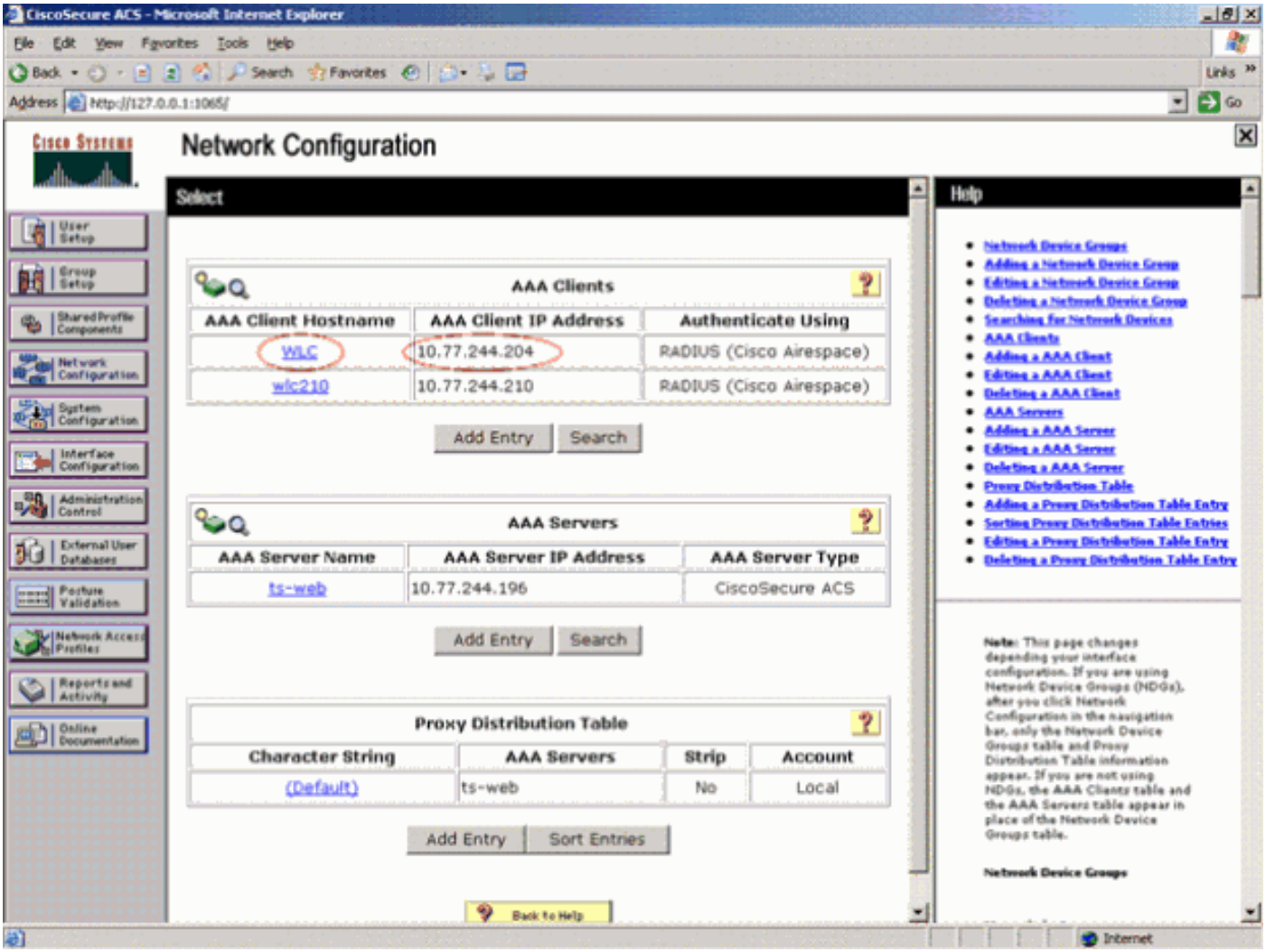
10.77.244.196 en este ejemplo:



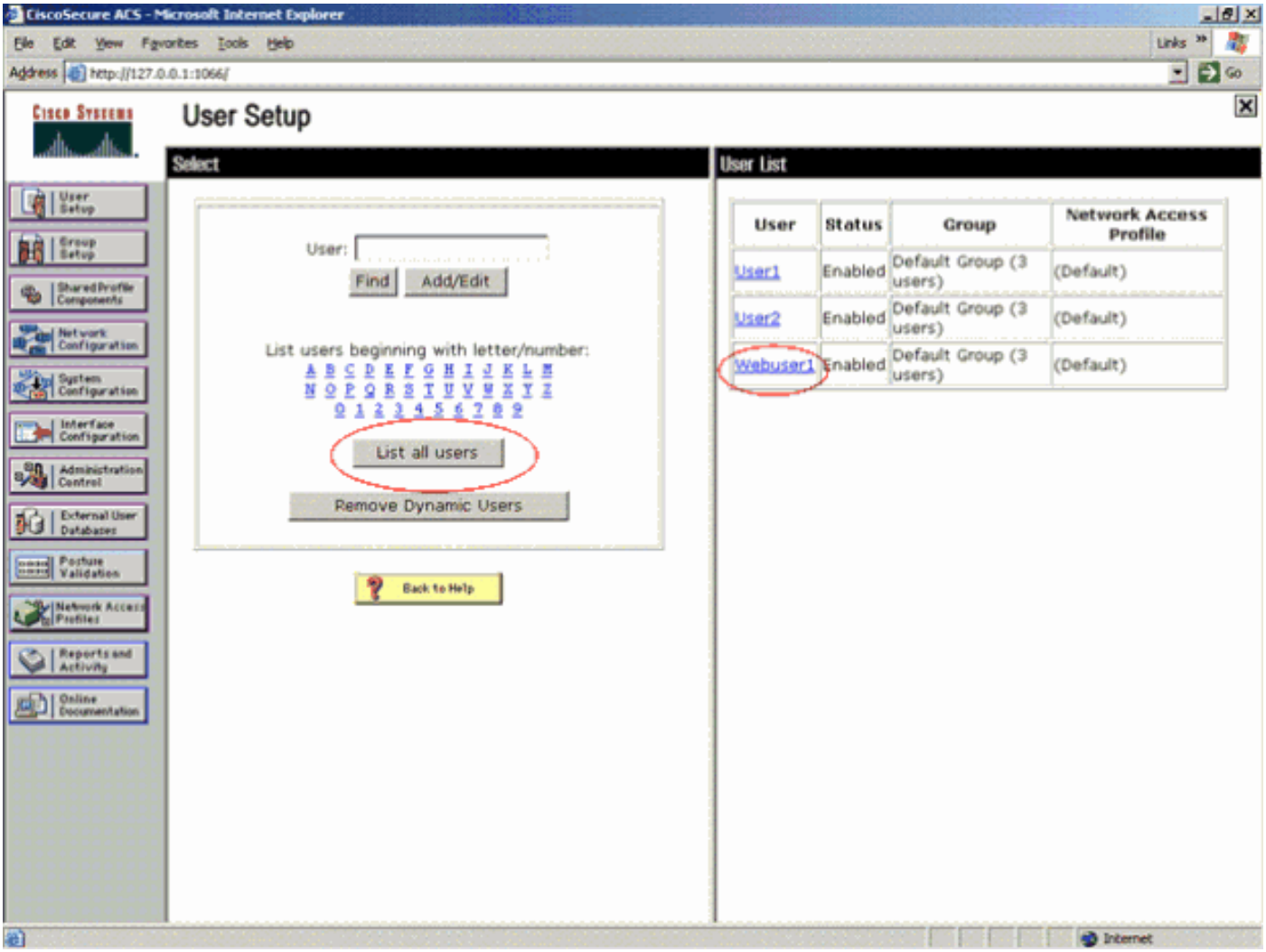
3. Haga clic en Apply (Aplicar).

Verificación de ACS

Cuando usted configura el ACS, recuerde descargar todas las correcciones actuales y último código. Esto debe solucionar los problemas inminentes. En caso de que usted esté utilizando la autenticación de RADIUS aseegurese que su WLC está enumerado como uno de los clientes AAA. Haga clic el menú de la **configuración de red** en el lado izquierdo para marcar esto. Haga clic al 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 usted elige la configuración de usuario, verifique otra vez que existan sus usuarios realmente. Haga clic la **lista todos los usuarios**. Una ventana como se muestra aparece. Asegúrese de que el usuario que ha creado exista en la lista.

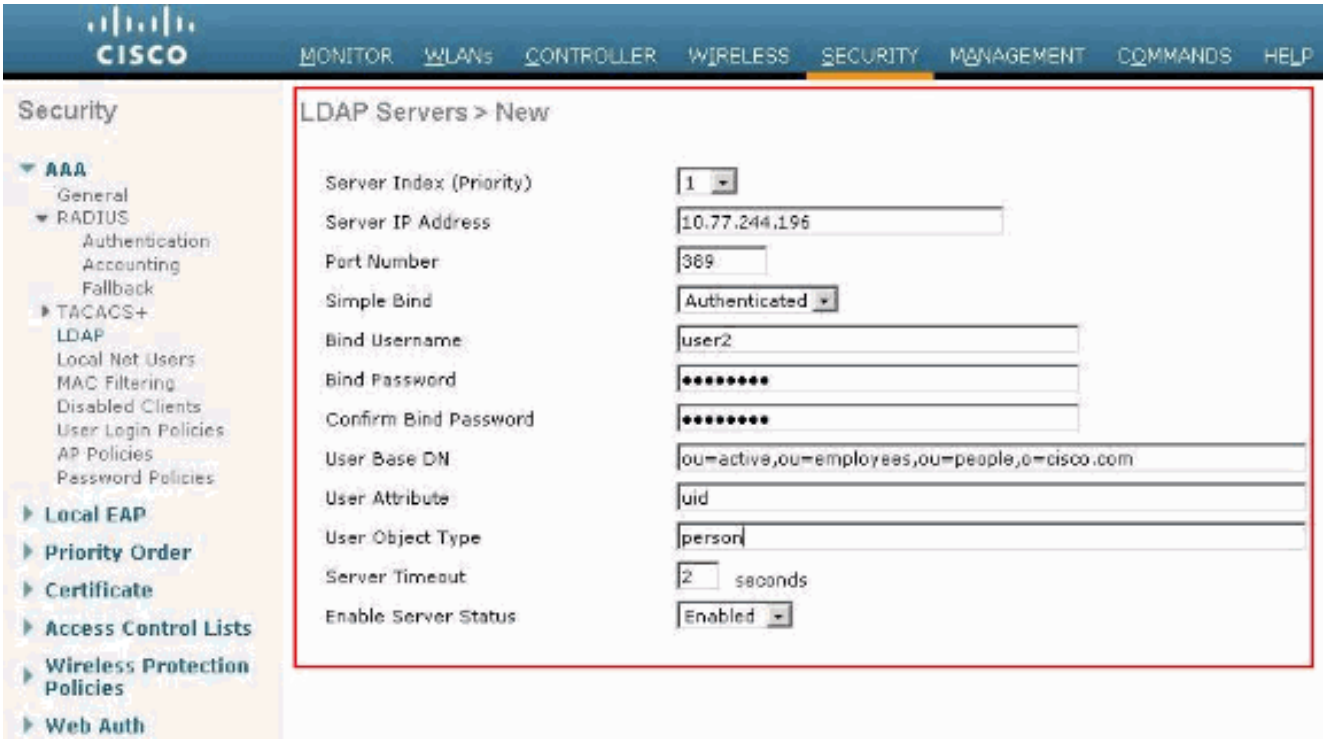


Servidor LDAP

Esta sección explica cómo configurar un servidor del Lightweight Directory Access Protocol (LDAP) como base de datos backend, similar a un RADIUS o a una base de datos de usuarios locales. Una base de datos de la parte LDAP permite que el regulador pregunte a un servidor LDAP para las credenciales (nombre de usuario y contraseña) de un usuario determinado. Estas credenciales entonces se utilizan para autenticar al usuario.

Complete estos pasos para configurar el LDAP usando el regulador GUI:

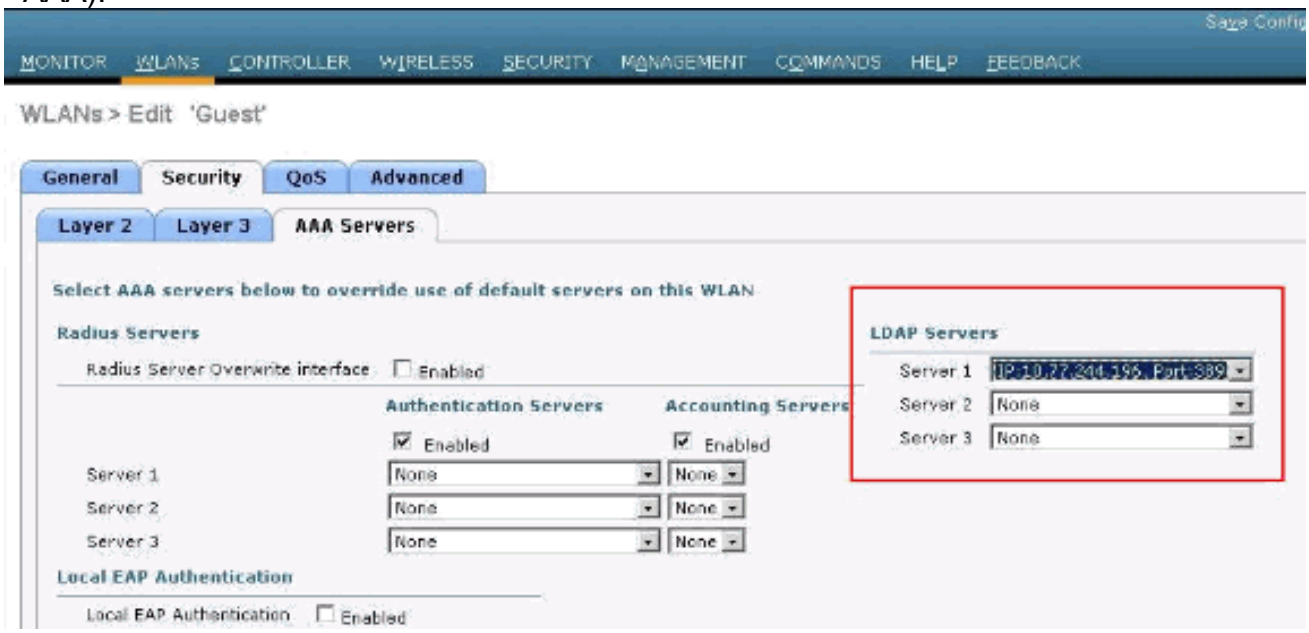
1. Haga clic la **Seguridad** >AAA > **LDAP** para abrir a los servidores LDAP.Esta página enumera a cualquier servidor LDAP que se haya configurado ya.Si usted quiere borrar a un servidor LDAP existente, mueva su cursor sobre la flecha desplegable azul para ese servidor y elija **quitan**.Si usted quiere aseegurarse que el regulador puede alcanzar a un servidor determinado, asoma su cursor sobre la flecha desplegable azul para ese servidor y elige el **ping**.
2. Realice uno del siguiente:Para editar a un servidor LDAP existente, haga clic el número del índice para ese servidor. Los servidores LDAP > editan la página aparecen.Para agregar a un servidor LDAP, haga clic **nuevo**. Los servidores LDAP > nueva página aparecen.



3. Si usted está agregando un nuevo servidor, elija un número de la casilla desplegable del índice del servidor (prioridad) para especificar la orden de la prioridad de este servidor en relación con cualquier otro servidor LDAP configurado. Usted puede configurar hasta diecisiete servidores. Si el regulador no puede alcanzar el primer servidor, después intenta segundo de la lista y así sucesivamente.
4. Si usted está agregando un nuevo servidor, ingrese el IP Address del servidor LDAP en el campo de dirección IP del servidor.
5. Si usted está agregando un nuevo servidor, ingrese el número del puerto TCP del servidor LDAP en el campo de número del puerto. El intervalo válido es 1 a 65535, y el valor predeterminado es 389.
6. Marque la casilla de verificación del **estado del servidor del permiso** para habilitar a este servidor LDAP, o desmarquela para inhabilitarla. Se inhabilita el valor predeterminado.
7. De la casilla desplegable simple del lazo, elija **anónimo** o **autenticado** para especificar el método bind de la autenticación local para el servidor LDAP. El método anónimo permite el acceso anónimo al servidor LDAP, mientras que el método autenticado requiere que un nombre de usuario y contraseña esté ingresado al acceso seguro. El valor predeterminado es anónimo.
8. Si usted eligió autenticado en el paso 7, complete estos pasos:En el campo de nombre de usuario del lazo, ingrese un nombre de usuario que se utilizará para la autenticación local al servidor LDAP.En la contraseña del lazo y confirme los campos de contraseña del lazo, ingresan una contraseña que se utilizará para la autenticación local al servidor LDAP.
9. En el campo de la Base del usuario DN, ingrese el Nombre distintivo (DN) de la sub-estructura en el servidor LDAP que contiene una lista de todos los usuarios. Por ejemplo, unidad del ou=organizational, unidad organizativa .ou=next, y o=corporation.com. Si el árbol que contiene a los usuarios es la base DN, el tipo o=corporation.com o dc=corporation, dc=com.
10. En el campo del atributo de usuario, ingrese el nombre del atributo en el registro del usuario que contiene el nombre de usuario. Usted puede obtener este atributo de su Servidor del directorio.
11. En el campo del tipo de objeto de usuario, ingrese el valor del atributo del objectType del

LDAP que identifica el expediente como usuario. A menudo, los registros del usuario tienen varios valores para el atributo del objectType, algunos de los cuales son únicos al usuario y comparten algunos de los cuales con otros tipos de objeto.

12. En el campo del tiempo de espera del servidor, ingrese el número de segundos entre las retransmisiones. El intervalo válido es 2 a 30 segundos, y el valor predeterminado es 2 segundos.
13. El tecleo **se aplica** para confiar sus cambios.
14. **Configuración de la salvaguardia del** tecleo para salvar sus cambios.
15. Complete estos pasos si usted desea asignar a los servidores LDAP específicos a una red inalámbrica (WLAN):Haga clic los **WLAN** para abrir la página WLAN.Haga clic el número de ID de la red inalámbrica (WLAN) deseada.Cuando los WLAN > editan la página aparece, hace clic las lenguetas de los **servidores de la Seguridad** >AAA abrir los WLAN > edita (la página de los servidores de la Seguridad >AAA).



De las casillas desplegables de los servidores LDAP, elija los servidores LDAP que usted quiere utilizar con esta red inalámbrica (WLAN). Usted puede elegir a hasta tres servidores LDAP, que se intentan en la orden de la prioridad.El tecleo **se aplica** para confiar sus cambios.**Configuración de la salvaguardia del** tecleo para salvar sus cambios.

Configure a su cliente WLAN para utilizar la autenticación Web

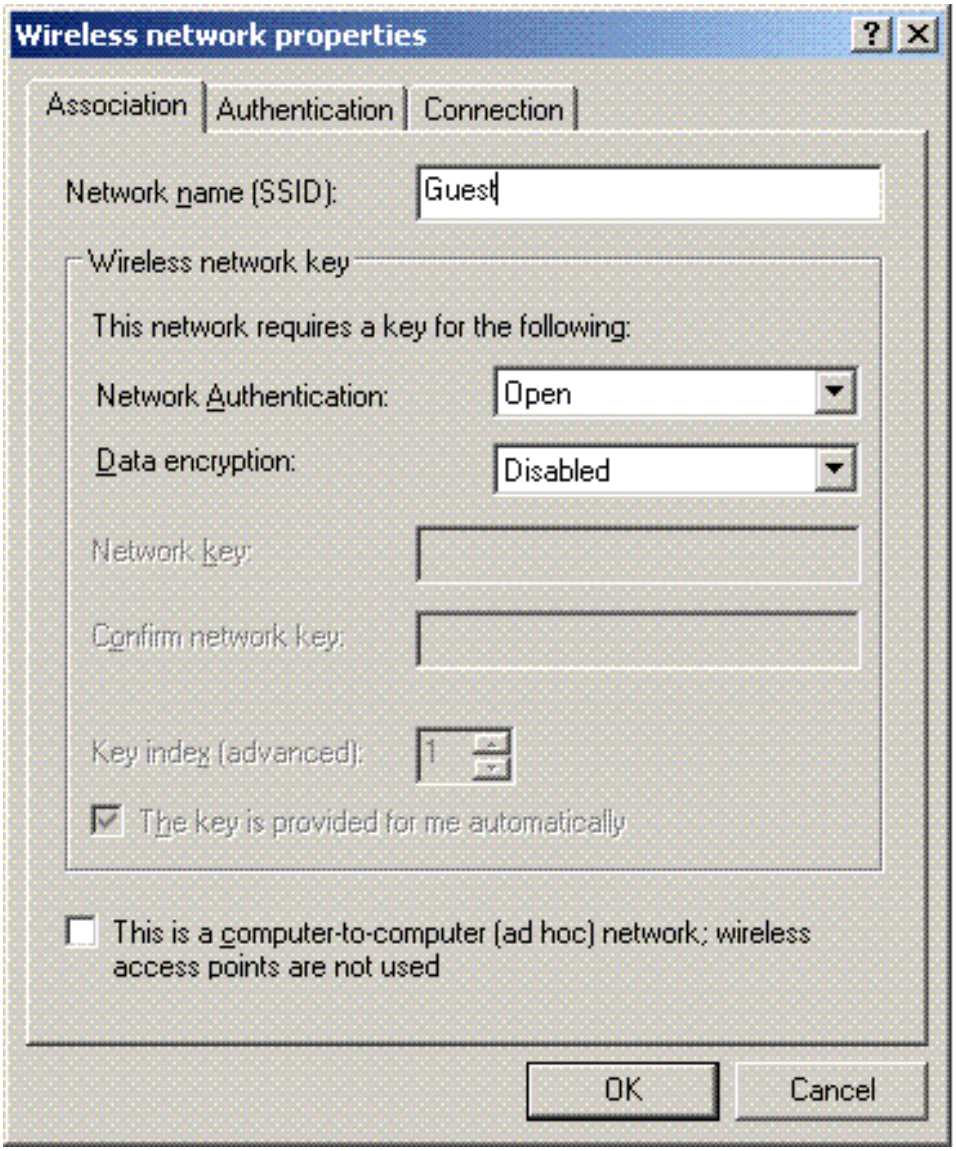
Una vez que se configura el WLC, el cliente debe ser configurado apropiadamente para la autenticación Web. En esta sección, encontrará información para configurar su Sistema Windows para la autenticación Web.

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 Click en OK en la parte inferior de la ventana para salvar 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 acertada a 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 red inalámbrica (WLAN), después el túnel VPN no se establece hasta que usted pase con el proceso de autenticación Web explicado aquí. Para establecer un túnel VPN, el cliente debe primero pasar con el proceso de la autenticación Web con el éxito. Después de este proceso, la tunelización VPN es satisfactoria.

Nota: Después de una registración satisfactoria, si los clientes de red inalámbrica son marcha lenta y no comunican con los otros dispositivos uces de los, de-autentican al cliente después de un período de tiempo de inactividad. El período de agotamiento del tiempo de espera es 300 segundos por abandono y se puede cambiar usando este comando CLI: `<seconds> del usertimeout de la red de los config`. Cuando ocurre esto, la entrada del cliente se quita del regulador. Si el cliente se asocia otra vez, se moverá de nuevo a un estado de Webauth_Reqd.

Nota: Si los clientes son activos después de la registración satisfactoria, conseguirán de-autenticados y la entrada se puede todavía quitar del regulador después del período de tiempo de espera de la sesión configurado en esa red inalámbrica (WLAN) (por los segundos example,1800 por abandono y puede ser cambiado usando este comando CLI: `<seconds> wlan del sesión-descanso <WLAN de los config ID>`). Cuando ocurre esto, la entrada del cliente se quita del regulador. Si el cliente se asocia otra vez, moverá hacia atrás en un estado de Webauth_Reqd.

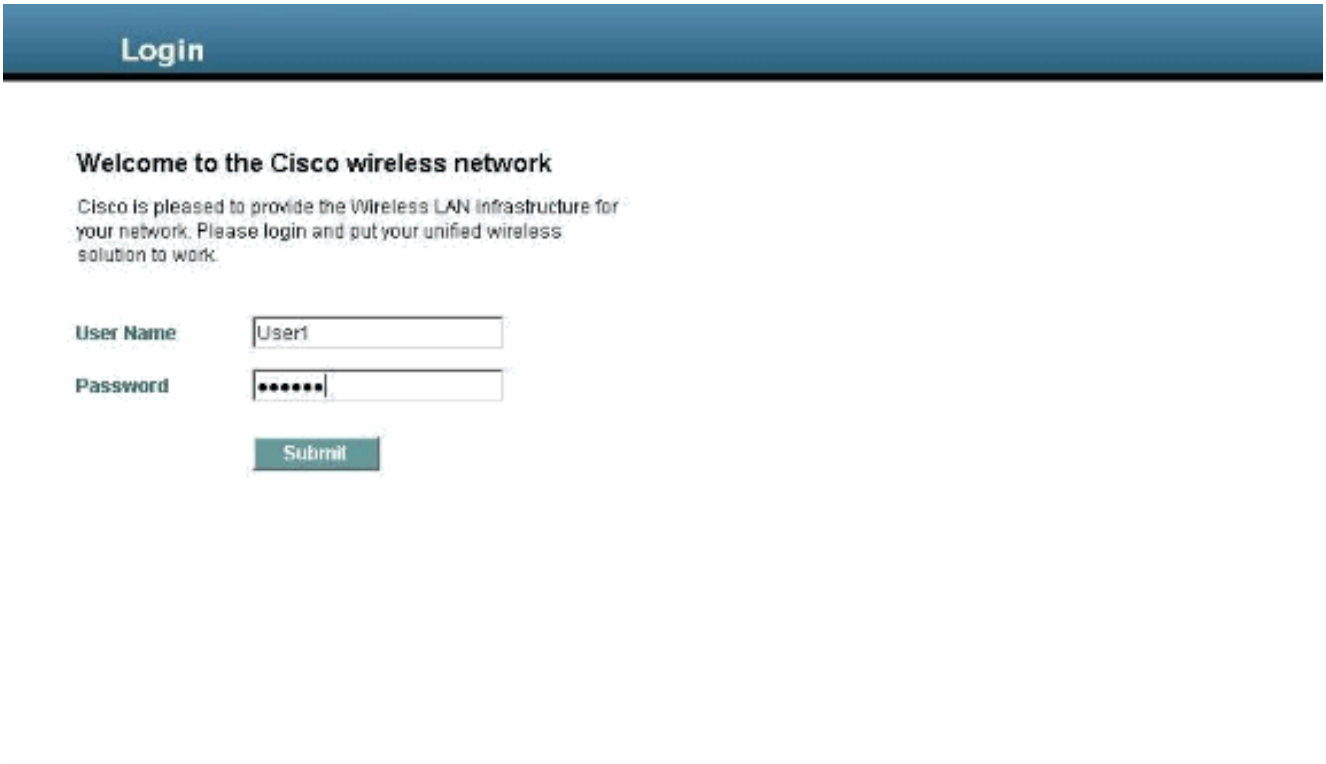
Si los clientes están en el estado de Webauth_Reqd, ninguna materia si están activos u ociosos, los clientes conseguirán de-autenticados después de que un red-**auth requiriera el período de agotamiento del tiempo de espera** (por ejemplo, 300 segundos y este vez es no utilizador configurable). Todo 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

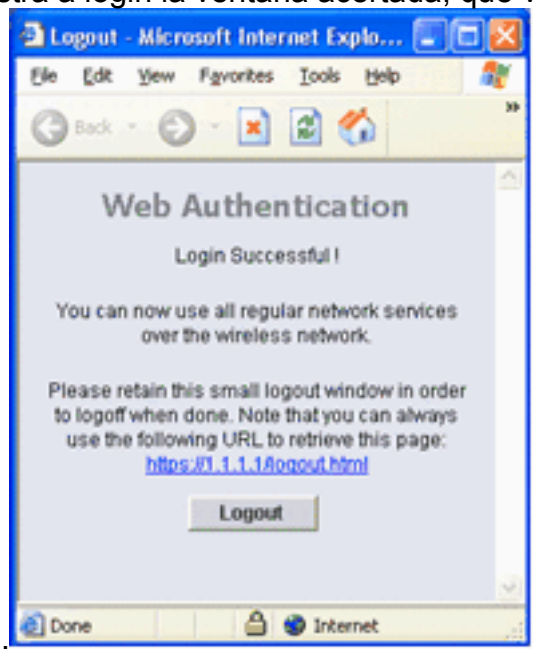
Complete estos pasos:

1. Abra 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 tiene que 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 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 que la registración satisfactoria y usted pueden esta ventana hojear Internet. Use la ventana más pequeña para cerrar la sesión cuando deje de usar la red del invitado.El tiro de pantalla muestra que un acertado reorienta para la autenticación Web.El tiro de siguiente pantalla muestra a login la ventana acertada, que visualiza cuando ha ocurrido la autenticación.



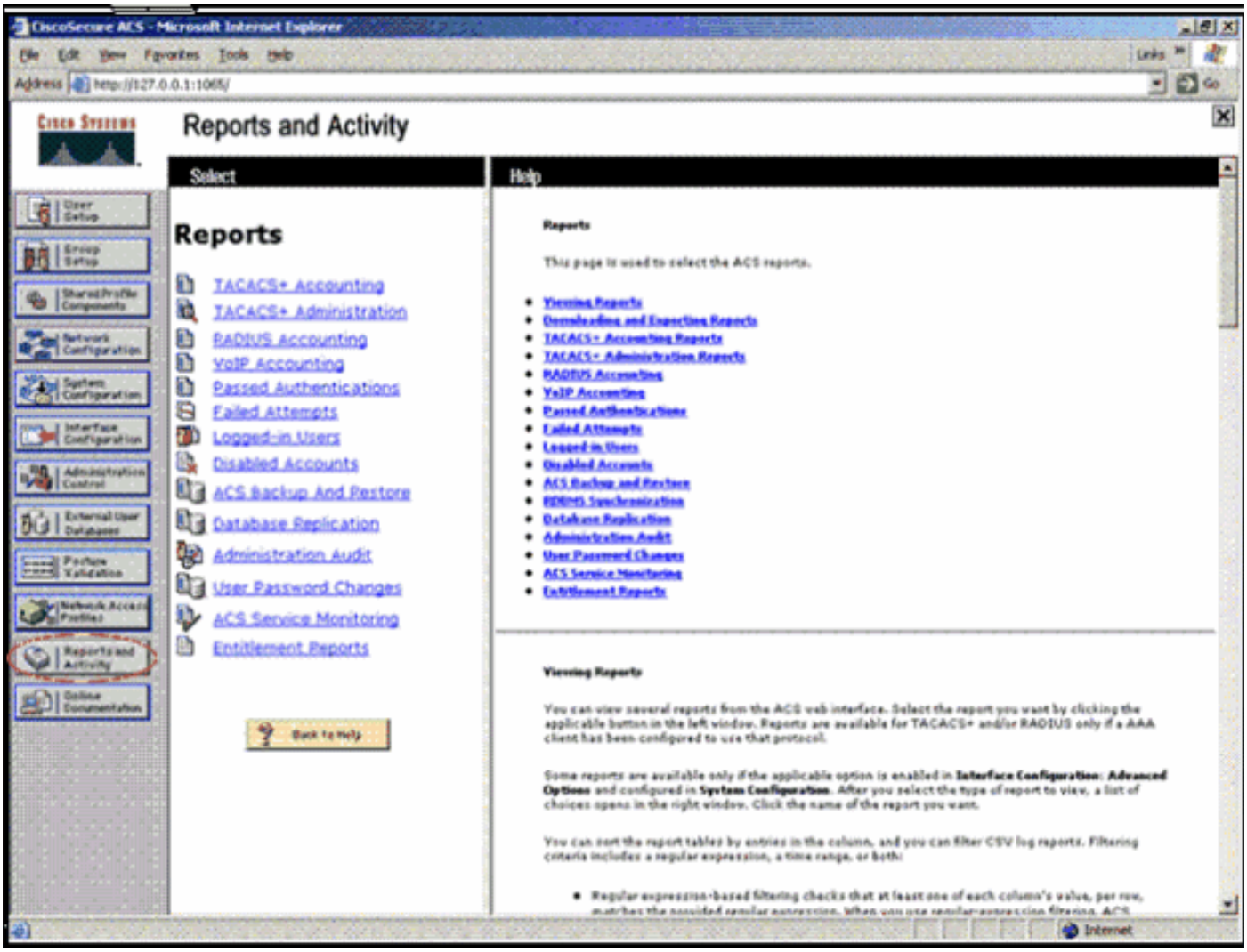
Los reguladores de Cisco 4404/WiSM pueden soportar 125 logines simultáneos de los usuarios del auth de la red, y escalan a hasta 5000 clientes del auth de la red.

Los reguladores del Cisco 5500 pueden soportar 150 logines simultáneos de los usuarios del auth de la red.

Autenticación Web del Troubleshooting

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.



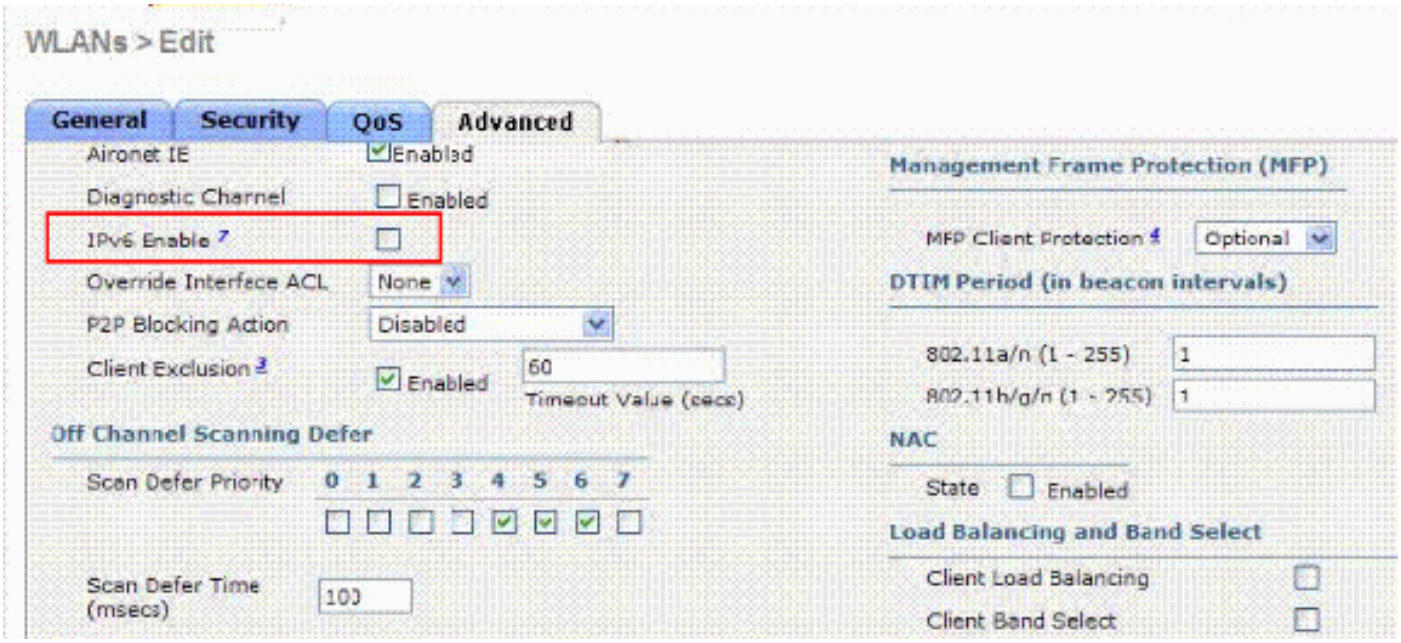
Nota: Si escribe en cualquier URL externa, el WLC se conecta automáticamente con la página de la autenticación web interna. Si la conexión automática no funciona, usted puede ingresar el IP Address de administración del WLC en la barra URL para resolver problemas. Lea el mensaje que le indica redirección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

Refiera a la autenticación Web del troubleshooting en un regulador del Wireless LAN (WLC) para más información sobre la autenticación Web del troubleshooting.

Auth de la red con interligar del IPv6

Para configurar una red inalámbrica (WLAN) para el IPv6 que interliga, del regulador GUI, navegue a los **WLAN**. Entonces, seleccione la red inalámbrica (WLAN) deseada y elija **avanzado del los WLAN > editan la** página.

Seleccione la casilla de verificación del **permiso del IPv6** si usted quiere habilitar a los clientes que conectan con esta red inalámbrica (WLAN) para validar los paquetes del IPv6. Si no, deje la casilla de verificación no seleccionada, que es el valor predeterminado. Si usted inhabilita (o desmarque) la casilla de verificación del IPv6, el IPv6 será permitido solamente después de la autenticación. Habilitar el IPv6 significa que el regulador puede pasar el tráfico del IPv6 sin la autenticación de cliente.



Para información más detallada sobre interligar del IPv6 y las **guías de consulta para usar esta característica**, refiera al IPv6 que configura que interliga la sección de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 7.0.

Información Relacionada

- Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN
- Resolviendo problemas la autenticación Web en un regulador del Wireless LAN (WLC)
- Red Inalámbrica Cisco LAN
- Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0 - Manejo de las cuentas de usuario
- Autentificación del Administrador Lobby deWireless LAN Controller a través del Servidor RADIUS
- Soporte Técnico y Documentación - Cisco Systems