Autenticación del Web externa con el ejemplo inalámbrico de la configuración de los reguladores LAN

Contenido

Introducción
Prerequisites
Requisitos
Componentes usados
Convenciones
Antecedentes
Proceso de autenticación del Web externa
Configuración de la red
Configurar
Cree un interfaz dinámico para los Usuarios invitados
Cree una Autenticación previa ACL
Cree una base de datos local en el WLC para los Usuarios invitados
Configure el WLC para la autenticación del Web externa
Configure la red inalámbrica (WLAN) para los Usuarios invitados
Verifique
Troubleshooting
Los clientes reorientados al servidor de la autenticación del Web externa reciben una advertencia del certificado
Error: la “página no puede ser visualizada”
Información Relacionada

Introducción

Este documento explica cómo utilizar un servidor Web externo para configurar un controlador de LAN inalámbrico (WLC) para la autenticación Web.

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

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

- Conocimiento básico del protocolo ligero del Punto de acceso (LWAPP) y control y aprovisionamiento de los untos de acceso de red inalámbrica (CAPWAP)
- Conocimiento en cómo poner y configurar a un servidor Web externo
- Conocimiento en cómo poner y configurar los servidores del DHCP y DNS

Componentes usados

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

- Cisco 4400 WLC que funciona con el firmware release/versión 7.0.116.0
- REVESTIMIENTO de las Cisco 1131AG Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con la versión 3.6 de los firmwares
- Servidor Web externo que recibe la página de registro de la autenticación Web
- Servidores DNS y del DHCP para el address resolution y la asignación de la dirección IP a los clientes de red inalámbrica

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

La 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. La autenticación Web es un método de autenticación simple sin la necesidad de un suplicante o de una utilidad de cliente.

La autenticación Web se puede realizar usando:

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

Este documento proporciona a un ejemplo de la configuración para explicar cómo configurar el WLC para utilizar un script de la clave de un servidor Web externo.

Proceso de autenticación del Web externa

Con la autenticación del Web externa, la página de registro usada para la autenticación Web se

salva en un servidor Web externo. Ésta es la Secuencia de eventos cuando un cliente de red inalámbrica intenta tener acceso a una red de la red inalámbrica (WLAN) que tenga autenticación del Web externa activada:

1. El cliente (usuario final) conecta con el WLAN y abre a un buscador Web y ingresa un URL, tal como www.cisco.com.
2. El cliente envía una petición DNS a un servidor DNS para resolver www.cisco.com a la dirección IP.
3. El WLC adelante la petición al servidor DNS que, a su vez, resuelve www.cisco.com a la dirección IP y envía una contestación DNS. El regulador adelante la contestación al cliente.
4. El cliente intenta iniciar una conexión TCP con la dirección IP de www.cisco.com enviando paquete TCP Syn a la dirección IP de www.cisco.com.
5. 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.
6. El cliente envía un HTTP CONSIGUE el paquete destinado a www.google.com. El WLC intercepta este paquete, 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 URL del valor por defecto del WLC, por ejemplo, http:// <Virtual-Server-IP>/login.html.
7. El cliente entonces enciende la conexión HTTPS a la reorientación URL que la envía a 1.1.1.1. Ésta es la dirección IP virtual del regulador. El cliente tiene que validar el certificado de servidor o ignorarlo para traer para arriba el túnel SSL.
8. Porque se activa la autenticación del Web externa, el WLC reorienta al cliente al servidor Web externo.
9. La clave auténtica URL del Web externa se añade al final del fichero con los parámetros tales como el AP_Mac_Address, el client_url (www.cisco.com) y el action_URL que el cliente necesita para entrar en contacto con al servidor Web del regulador.**Note**: El action_URL dice a servidor Web que el nombre de usuario y contraseña está salvado en el regulador. Las credenciales se deben devolver al regulador para conseguir autenticadas.
10. El servidor Web URL del externo lleva al usuario a una página de registro.
11. La página de registro toma la entrada de los credenciales de usuario, y envía la petición de nuevo al action_URL, ejemplo http://1.1.1.1/login.html, del servidor Web WLC.
12. El servidor Web WLC somete el nombre de usuario y contraseña para la autenticación.
13. El WLC inicia la petición del servidor de RADIUS o utiliza la base de datos local en el WLC y autentica al usuario.
14. Si la autenticación es acertada, el servidor Web WLC cualquiera adelante el usuario al configurado reorienta el URL o al URL el cliente comenzó con, por ejemplo www.cisco.com.
15. Si la autenticación falla, después el servidor Web WLC reorienta al usuario de nuevo a la clave URL del cliente.

Note: Para configurar el webauthentication externo para utilizar los puertos con excepción del HTTP y del HTTPS, publique este comando:

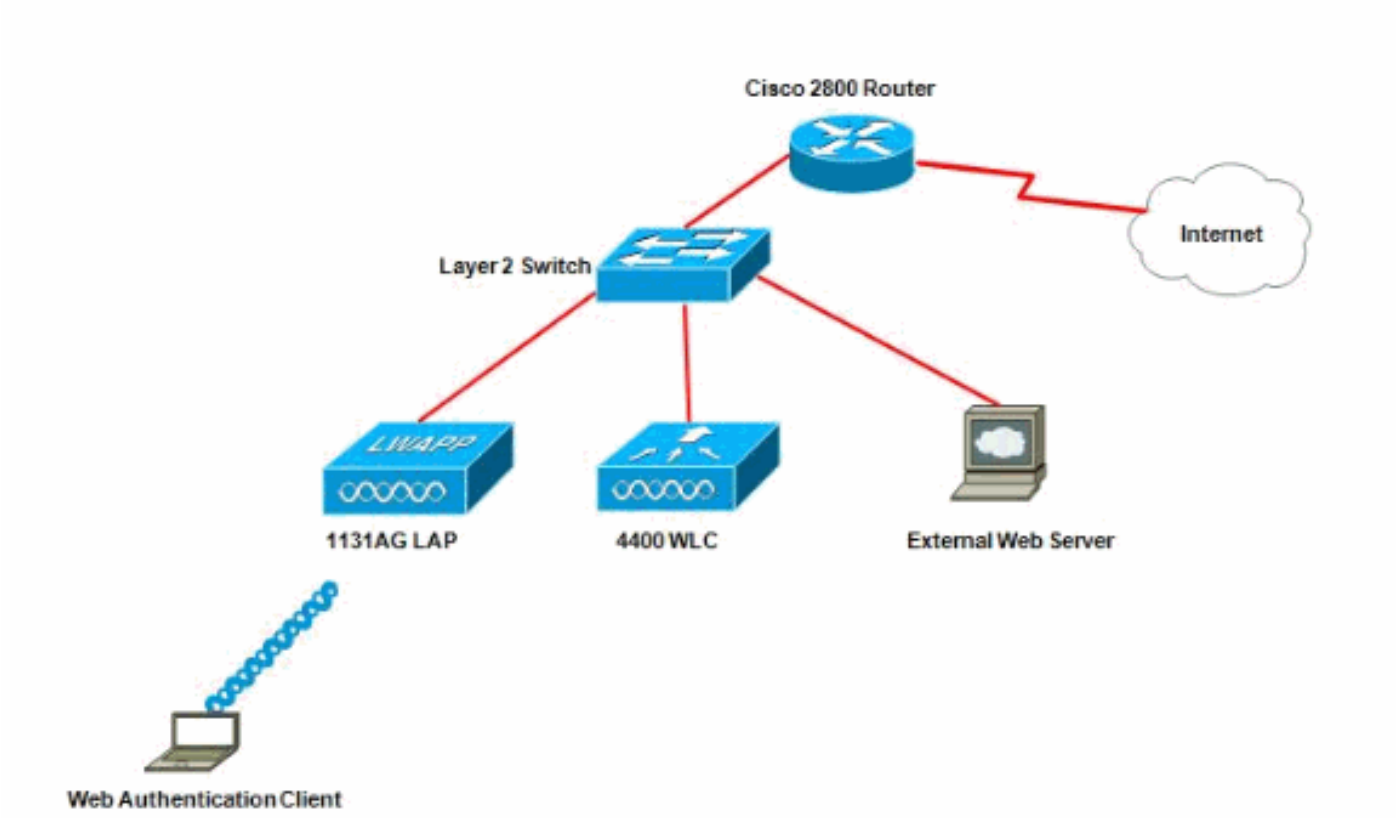
```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

Configuración de la red

El ejemplo de la configuración utiliza esta disposición. UN REVESTIMIENTO se registra al WLC. Usted necesita configurar a un **invitado de la** red inalámbrica (WLAN) para los Usuarios invitados y tuvo que activar la autenticación Web para los usuarios. Usted también necesita asegurarse de que el regulador reoriente al usuario al servidor Web externo URL (para la autenticación del Web externa). El servidor Web del externo recibe la página de registro de la red que se utiliza para la autenticación.

Los credenciales de usuario se deben validar contra la base de datos local mantenida en el regulador. Después de la autenticación satisfactoria, los usuarios deben no ser prohibidos el acceso al invitado de la red inalámbrica (WLAN). El regulador y los otros dispositivos necesitan ser configurados para esta disposición.

Note: Usted puede utilizar una versión personalizada del script de la clave, que serán utilizados para la autenticación Web. Usted puede descargar un script de la autenticación Web de la muestra de la página de las transferencias directas de software de Cisco. Por ejemplo, para los 4400 reguladores, navegue a los **Productos > a la Tecnología inalámbrica > regulador inalámbrico LAN > los Controladores autónomos > Cisco Wireless LAN Controllers de la serie 4400 > regulador > software LAN de la Tecnología inalámbrica de Cisco 4404 en el chasis > la autenticación Web inalámbrica Bundle-1.0.1 del regulador Lan** y descargue el **fichero webauth_bundle.zip**.



Note: El manojo auténtico personalizado de la red tiene un límite de hasta 30 caracteres para los nombres de fichero. Asegúrese de que no hay nombres de fichero dentro del manojo mayores de 30 caracteres.

Note: Este documento asume que configuran el DHCP, el DNS y a los servidores Web externos. Refiera a la documentación para información apropiada del otro vendedor en cómo configurar el DHCP, el DNS y al servidor Web externo.

Configurar

Antes de que usted configure el WLC para la autenticación del Web externa, usted debe configurar el WLC para la operación básica y registrar los revestimientos al WLC. Este documento asume que el WLC está configurado para la operación básica y que los revestimientos están registrados al WLC. Refiera al registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (WLC) si usted es usuario nuevo que intenta poner el WLC para la operación básica con los revestimientos.

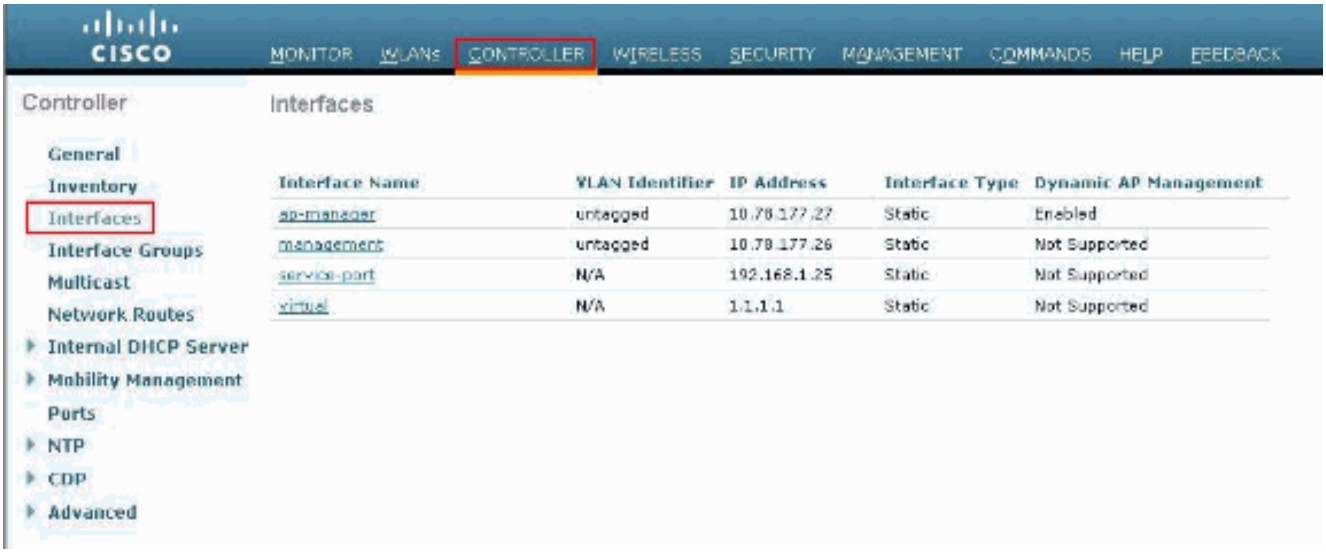
Complete estos pasos para configurar los revestimientos y el WLC para esta disposición:

1. Cree un interfaz dinámico para los Usuarios invitados
2. Cree una Autenticación previa ACL
3. Cree una base de datos local en el WLC para los Usuarios invitados
4. Configure el WLC para la autenticación del Web externa
5. Configure la red inalámbrica (WLAN) para los Usuarios invitados

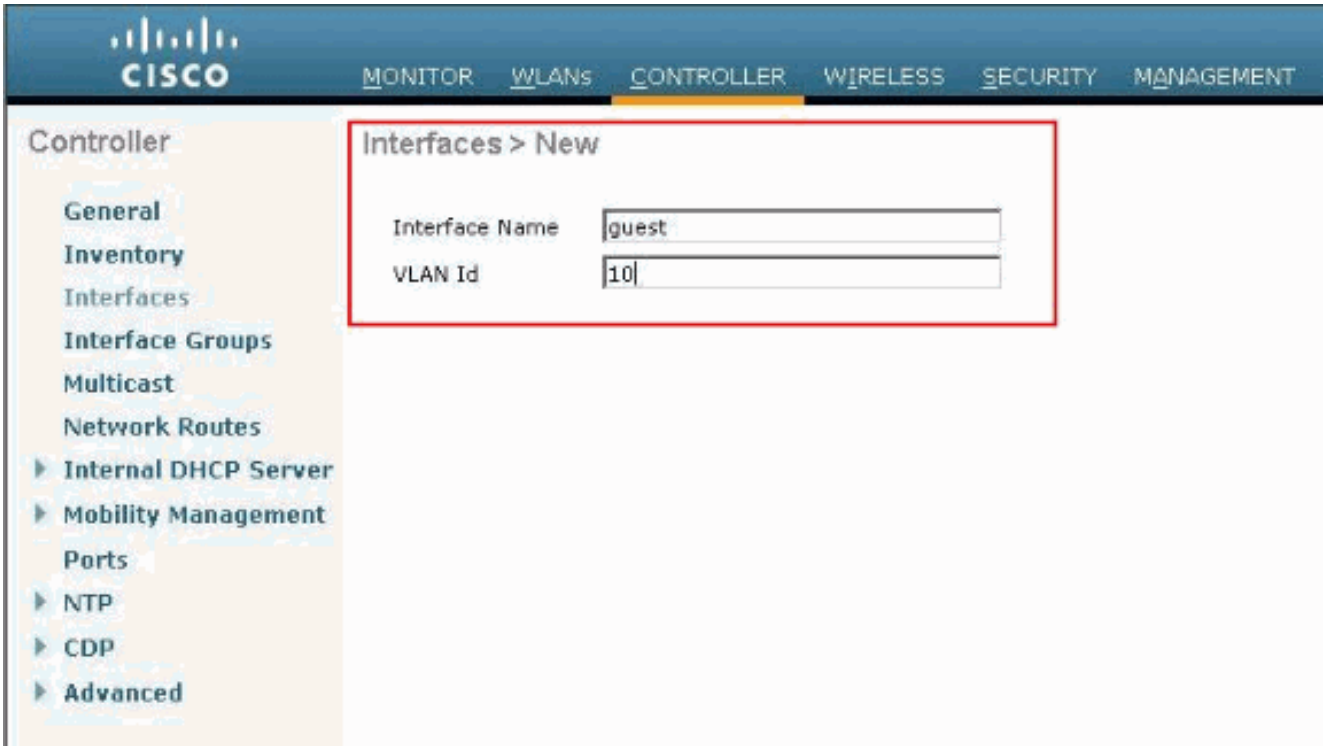
Cree un interfaz dinámico para los Usuarios invitados

Complete estos pasos para crear un interfaz dinámico para los Usuarios invitados:

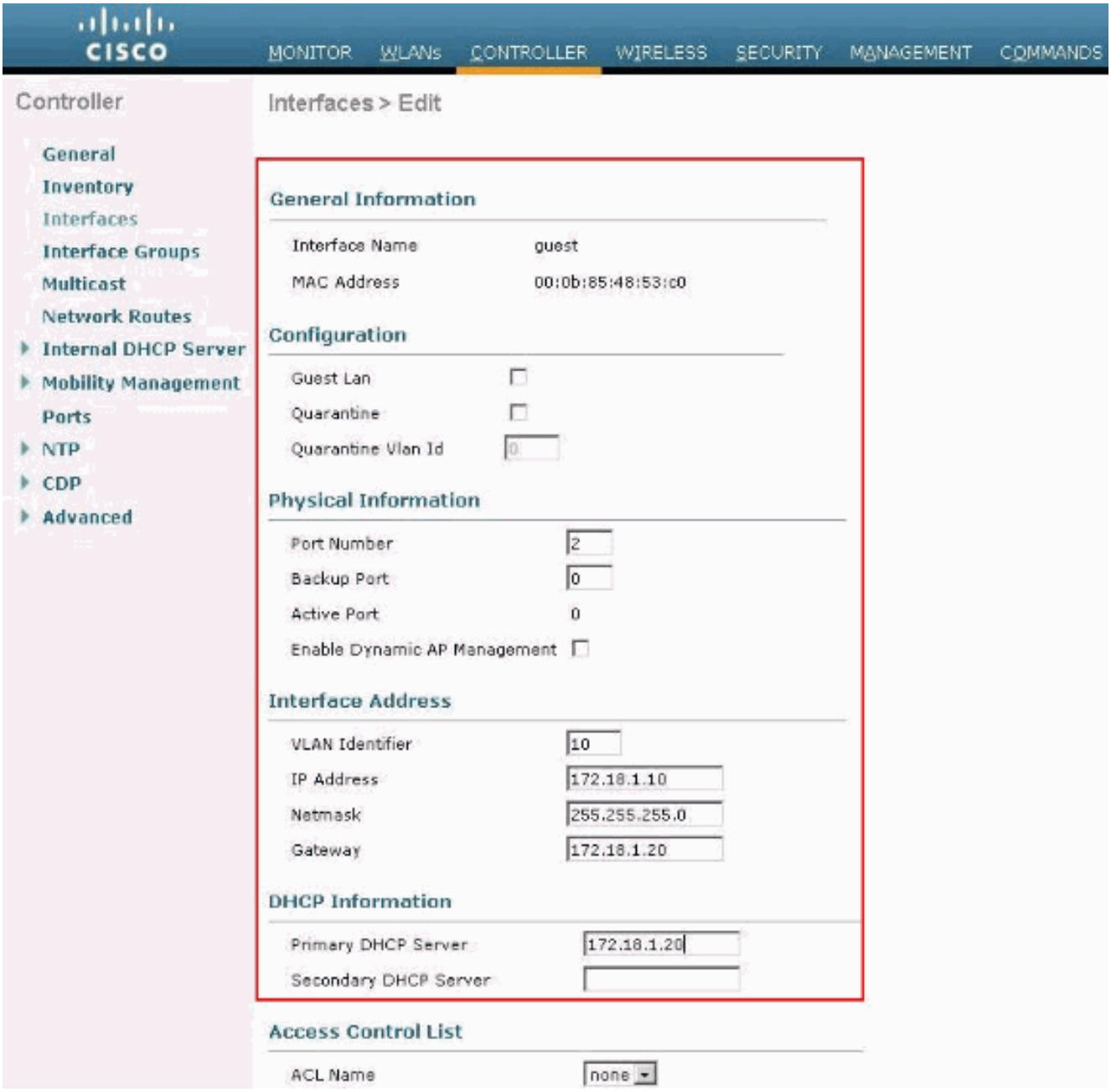
1. Del GUI WLC, elija los **reguladores > los interfaces**.La ventana de los interfaces aparece. Esta ventana enumera los interfaces que se configuran en el regulador. Esto incluye los interfaces del valor por defecto, que son la interfaz de administración, interfaz del ap-encargado, la interfaz virtual y la interfaz de puerto del servicio, y los interfaces dinámicos definidos por el
usario.



2. Haga clic **nuevo** para crear un nuevo interfaz dinámico.
3. En los **interfaces > la nueva ventana**, ingrese el nombre del interfaz y la identificación del VLA N. Entonces, el tecleo **se aplica**.En este ejemplo, el interfaz dinámico se nombra **invitado** y la identificación del VLA N se asigna
10.



4. En los **interfaces > corrija la** ventana, para el interfaz dinámico, ingrese el IP address, la máscara de subred, y el gateway de valor por defecto. Asígnelo a un puerto físico en el WLC, y ingrese el IP address del servidor del DHCP. Entonces, el tecleo **se aplica**.



Cree una Autenticación previa ACL

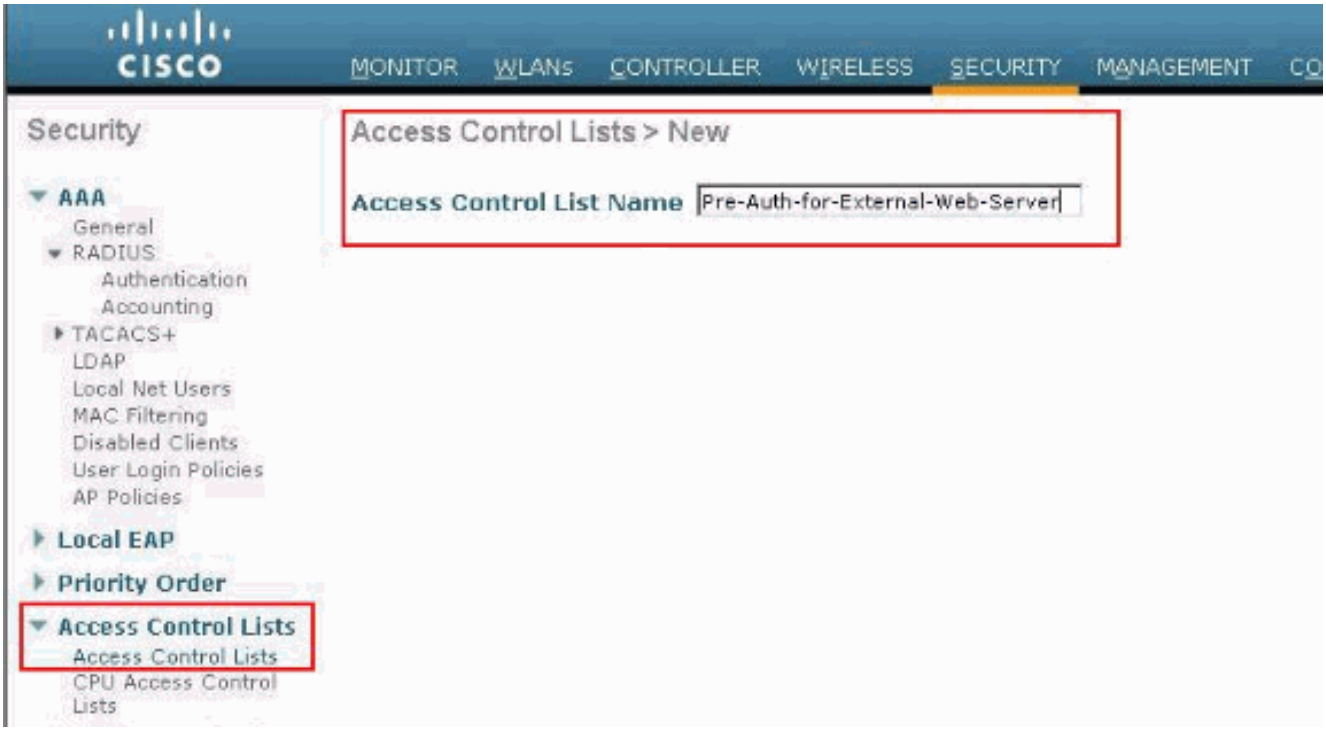
Al usar a un servidor Web externo para la autenticación Web, algunas de las Plataformas WLC necesitan una pre-autenticación ACL para el servidor Web externo (el regulador de las Cisco 5500 Series, las Cisco 2100 Series regulador, las Cisco 2000 Series y el módulo de red del regulador). Para las otras Plataformas WLC la pre-autenticación ACL no es obligatoria.

Sin embargo, es una práctica adecuada configurar una Autenticación previa ACL para el servidor Web externo al usar la autenticación del Web externa.

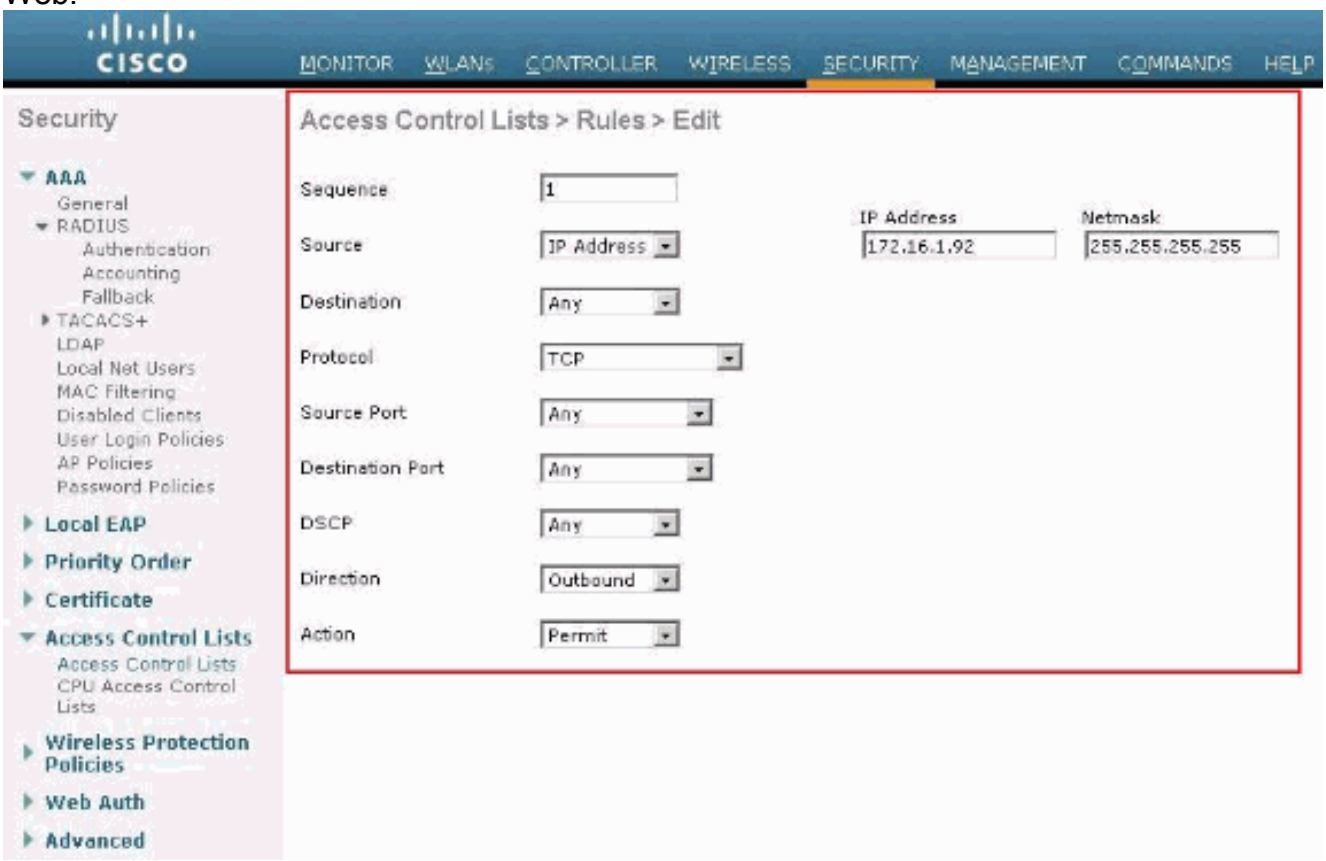
Complete estos pasos para configurar la Autenticación previa ACL para la red inalámbrica (WLAN):

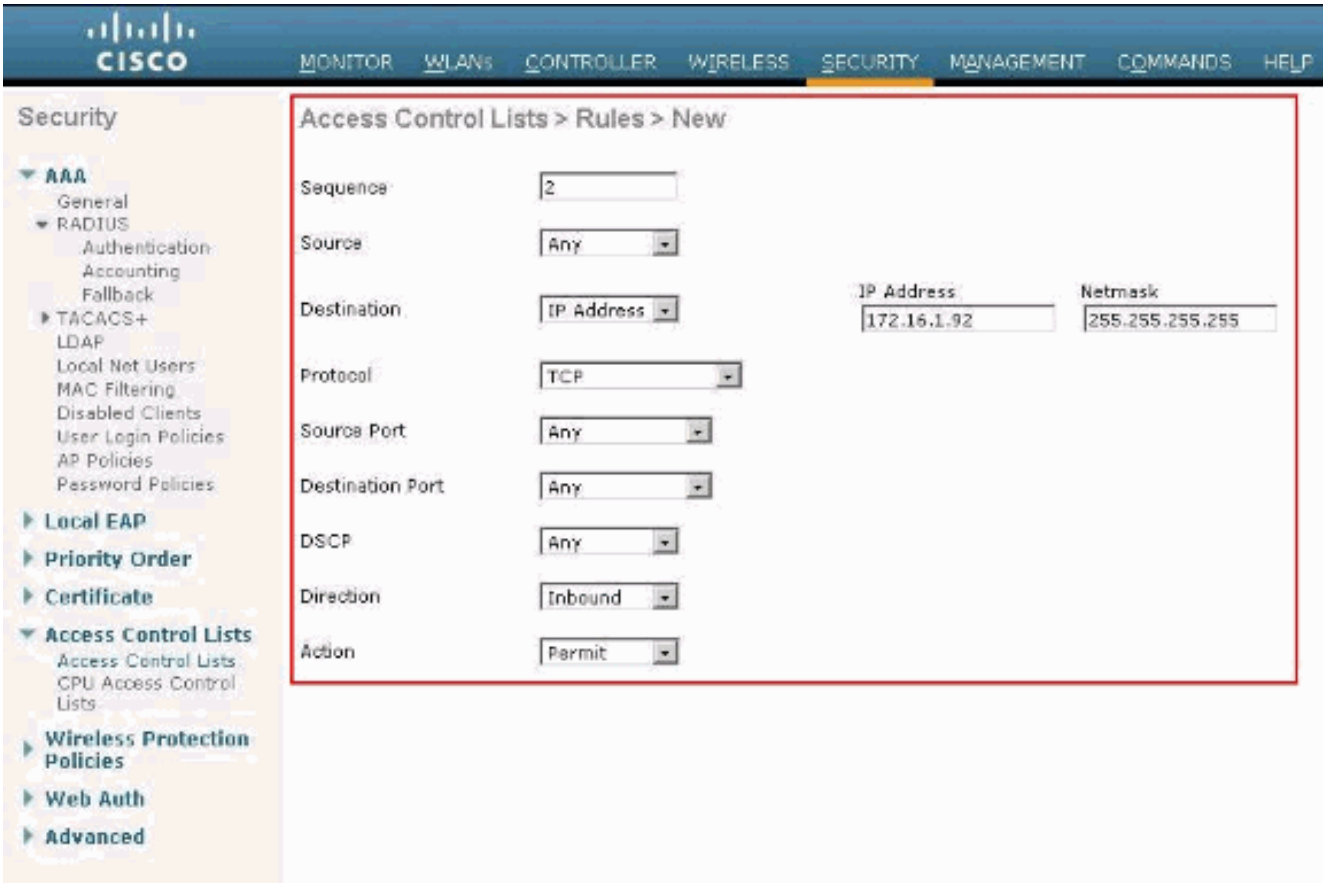
1. Del GUI WLC, elija la **Seguridad > las listas de control de acceso**.Esta ventana permite que usted vea los ACL actuales que son similares al Firewall estándar ACL.
2. Tecleo **nuevo** para crear un nuevo ACL.
3. Ingrese el nombre del ACL y del tecleo **se aplican**.En este ejemplo, el ACL se nombra Pre-

Auth-para-Externo-Red-
Servidor.

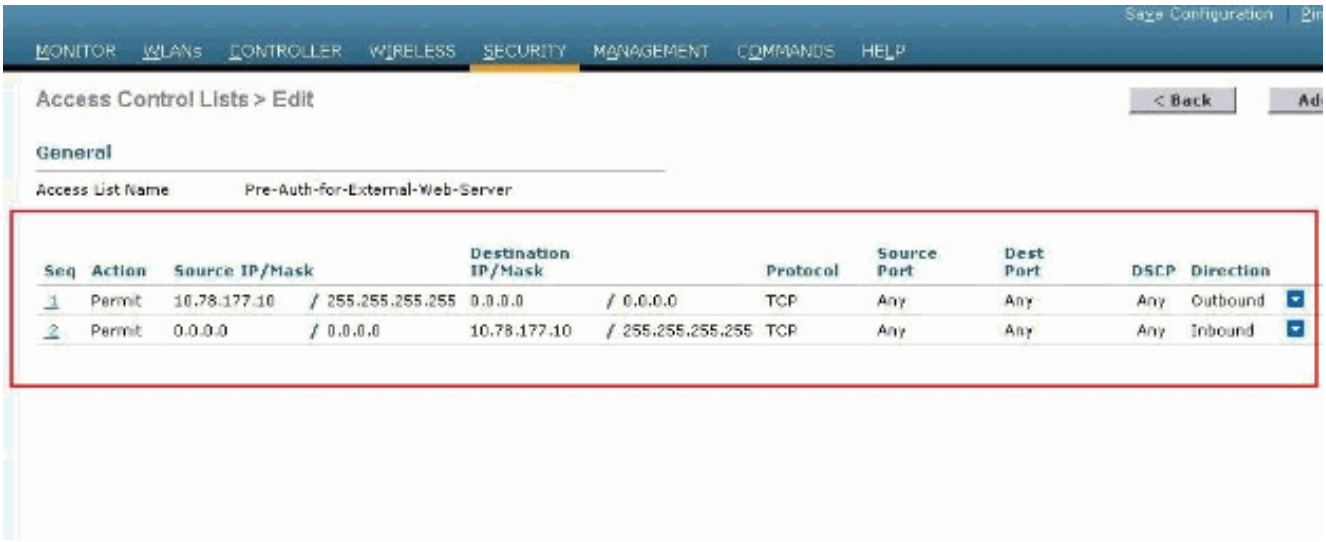


4. Para el nuevo ACL creado, el tecleo **corrige**.El ACL > corrige la ventana aparece. Esta ventana deja al usuario definir las nuevas reglas o modificar las reglas del ACL que existen.
5. El tecleo **agrega la nueva regla**.
6. Defina una regla ACL que permita el acceso para los clientes al servidor Web externo.En este ejemplo, 172.16.1.92 es la dirección IP externa del servidor Web.





7. El tecleo **se aplica** para confiar los cambios.



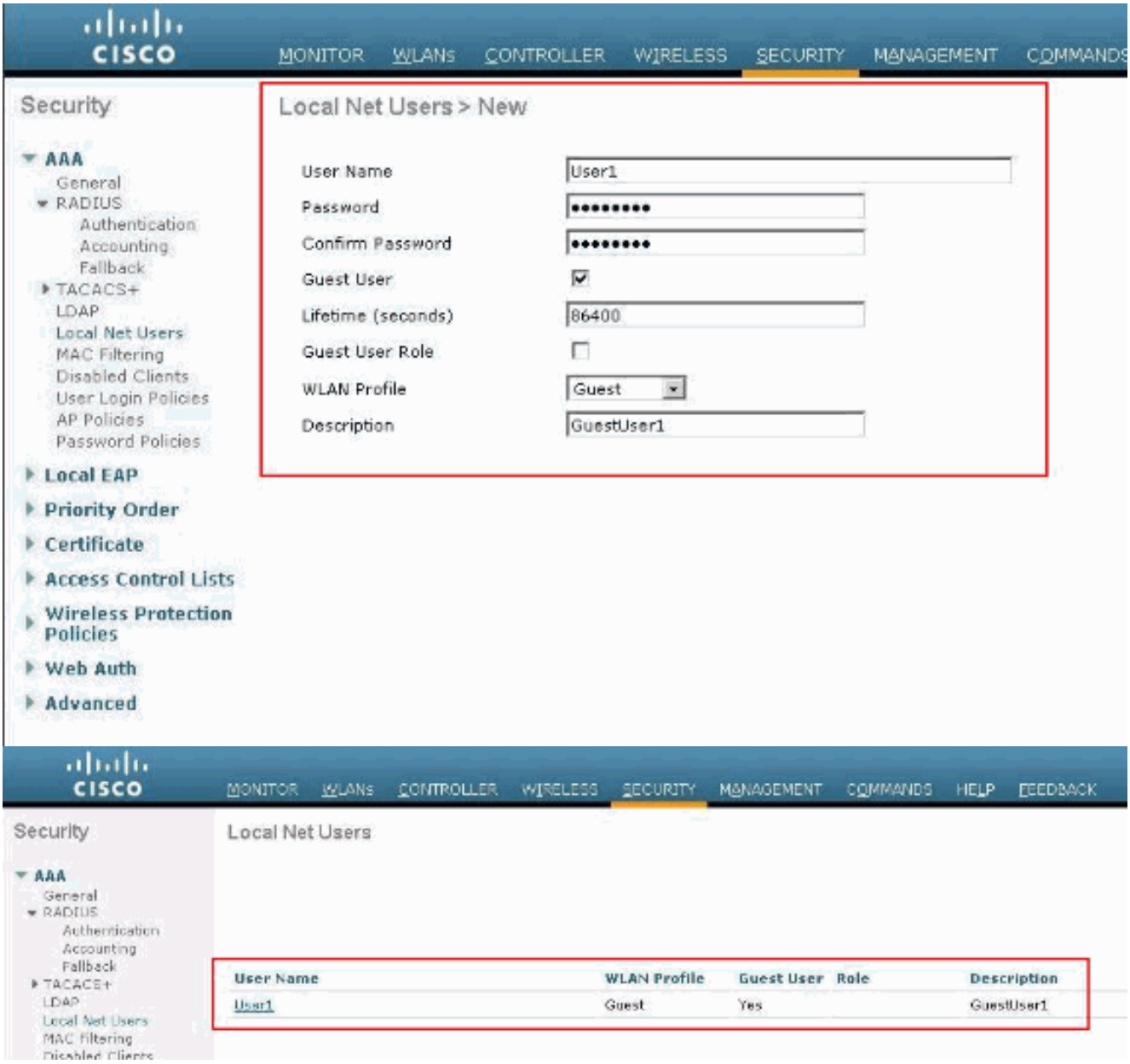
Cree una base de datos local en el WLC para los Usuarios invitados

La base de datos de usuarios para los Usuarios invitados se puede salvar en la base de datos local de la Tecnología inalámbrica del regulador LAN, o pudo ser externo salvado del regulador.

En este documento la base de datos local en el regulador se utiliza para autenticar a los usuarios. Usted debe crear a un usuario neto local y definir una contraseña para la clave del cliente de la autenticación Web. Complete estos pasos para crear la base de datos de usuarios en el WLC:

1. Del GUI WLC, elija la **Seguridad**.
2. Haga clic a los **usuarios netos locales 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 al **invitado User1**.
6. Haga clic en **Aplicar** para guardar la configuración del usuario nuevo.

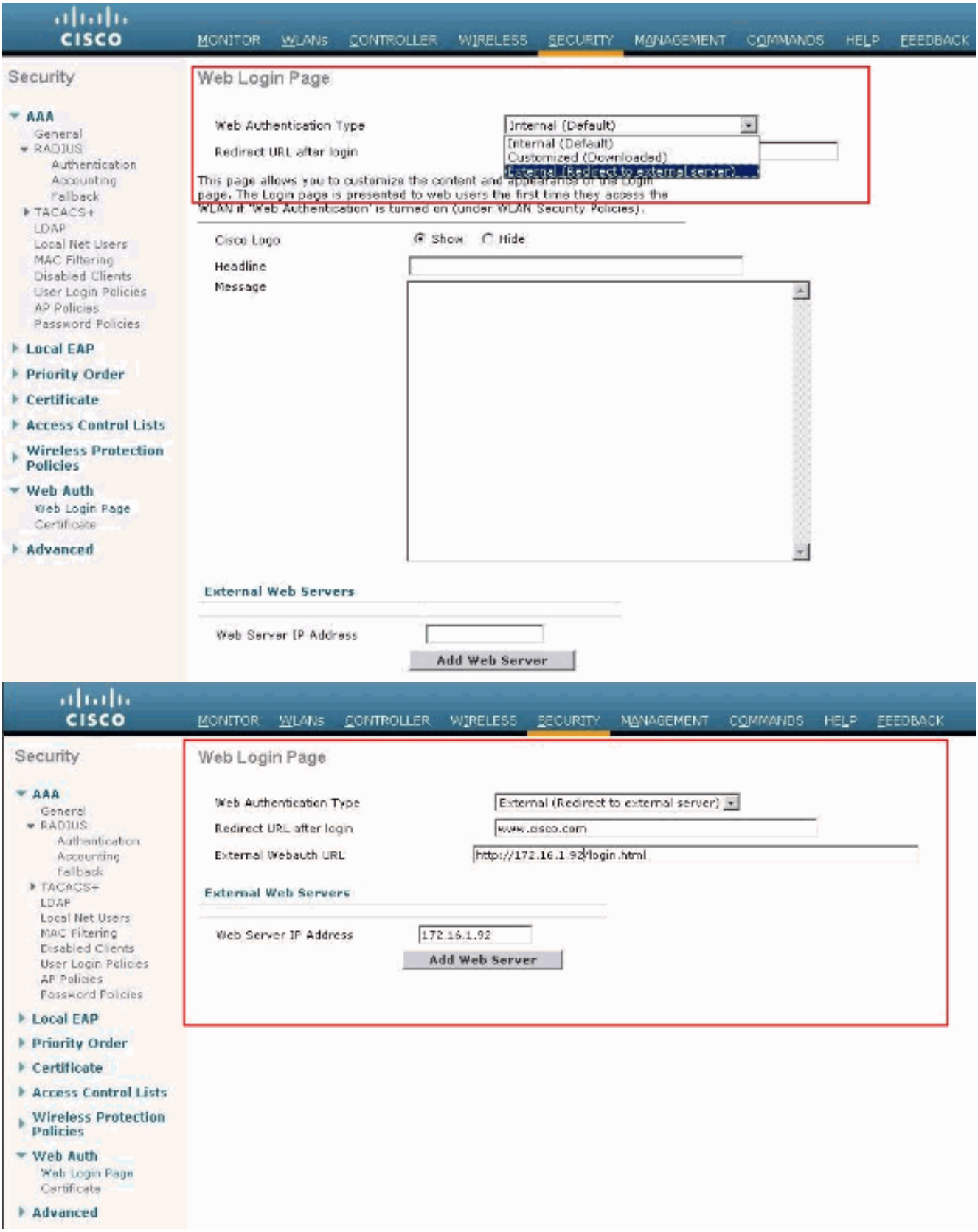


7. Relance los pasos 3-6 para agregar a más usuarios a la base de datos.

Configure el WLC para la autenticación del Web externa

El siguiente paso es configurar el WLC para la autenticación del Web externa. Complete estos pasos:

1. Del GUI del regulador, elija la **Seguridad > la red auténticas > página de registro de la red** para tener acceso a la página de registro de la red.
2. De la autenticación Web pulse la casilla desplegable, eligen el **externo (reoriente al servidor externo)**.
3. En la sección **externa del servidor Web**, agregue al nuevo servidor Web externo.
4. En el **URL de la reorientación después del** campo de la **clave**, ingrese el URL de la página a la cual reorientarán al usuario final sobre a la autenticación satisfactoria. En el campo **URL auténtico del Web externa**, ingrese el URL donde la página de registro se salva en el servidor Web
externo.



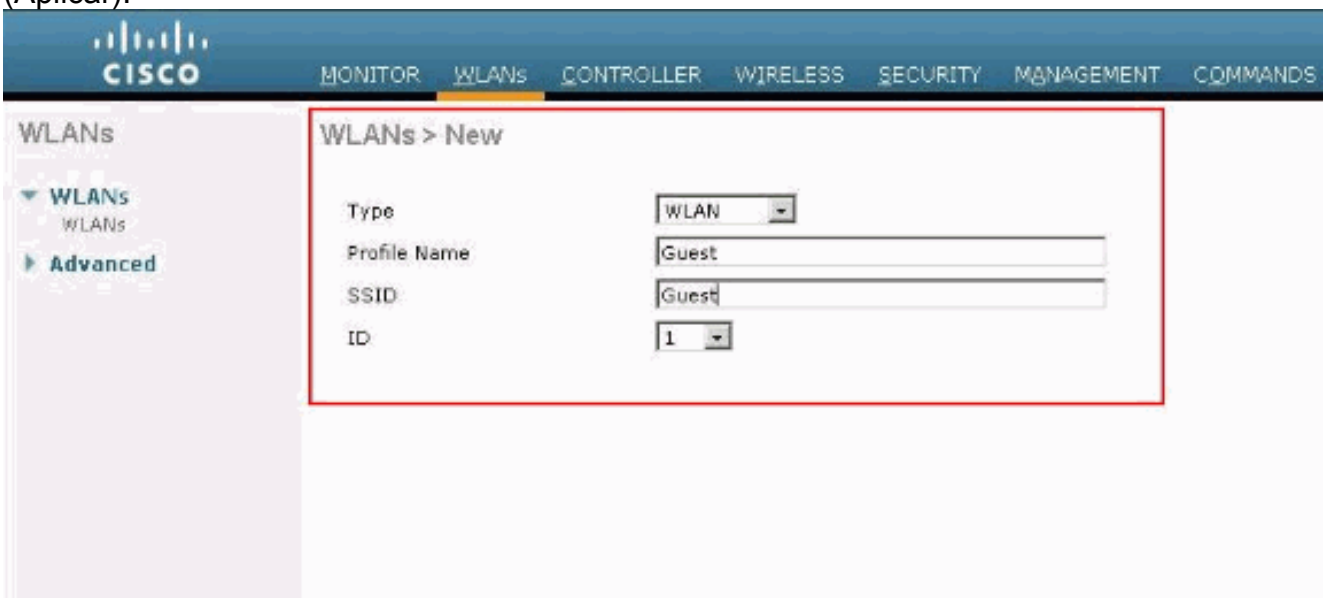
Note: En las versiones 5.0 WLC y más adelante, la página de la fin de comunicación para la autenticación Web puede también ser personalizada. Refiera a las páginas de la clave, de la falla de registro y de la fin de comunicación de la asignación por la sección de la red inalámbrica (WLAN) de la *configuración Guide,5.2 del regulador LAN de la Tecnología inalámbrica* para más información sobre cómo configurarla.

Configure la red inalámbrica (WLAN) para los Usuarios invitados

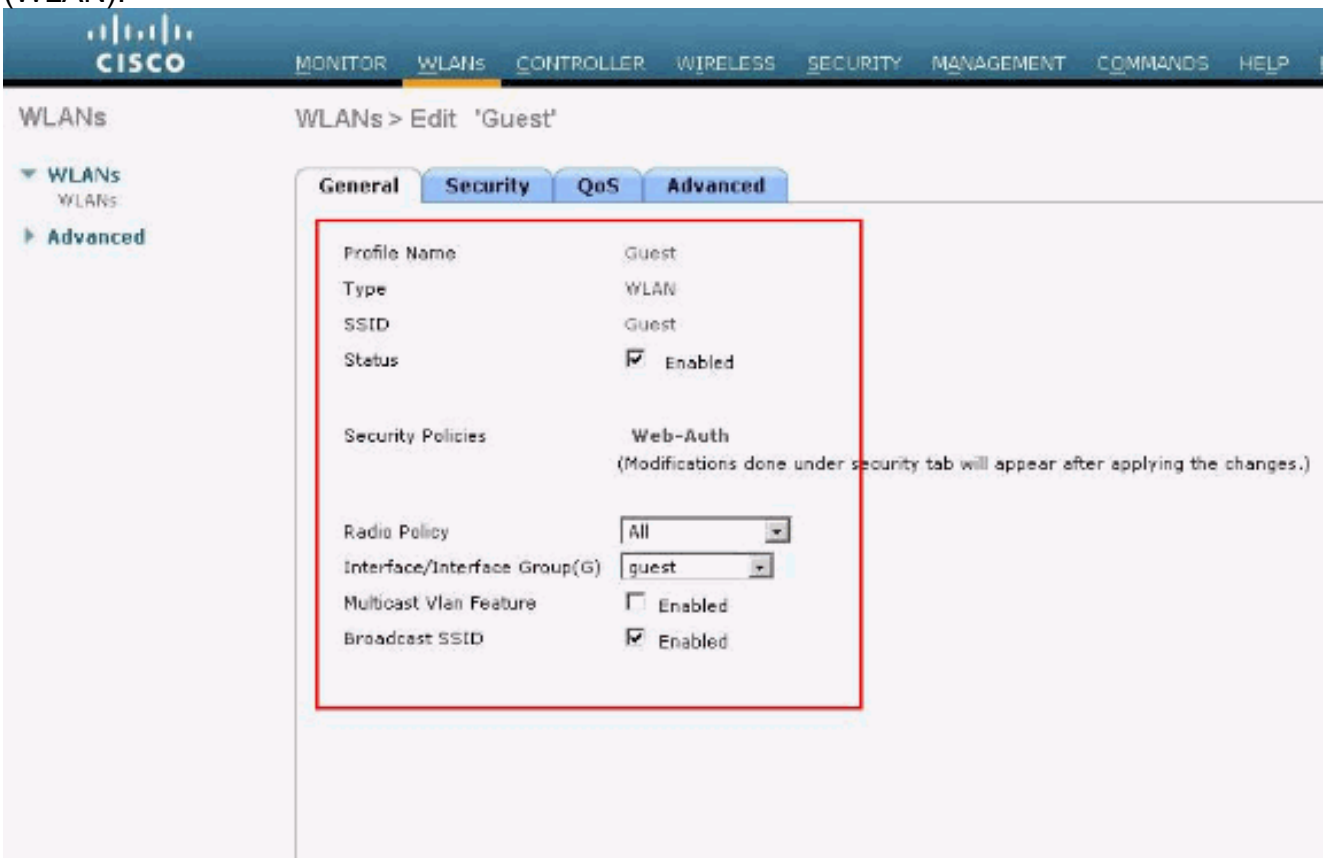
El último paso es crear las redes inalámbricas (WLAN) para los Usuarios invitados. Complete

estos pasos:

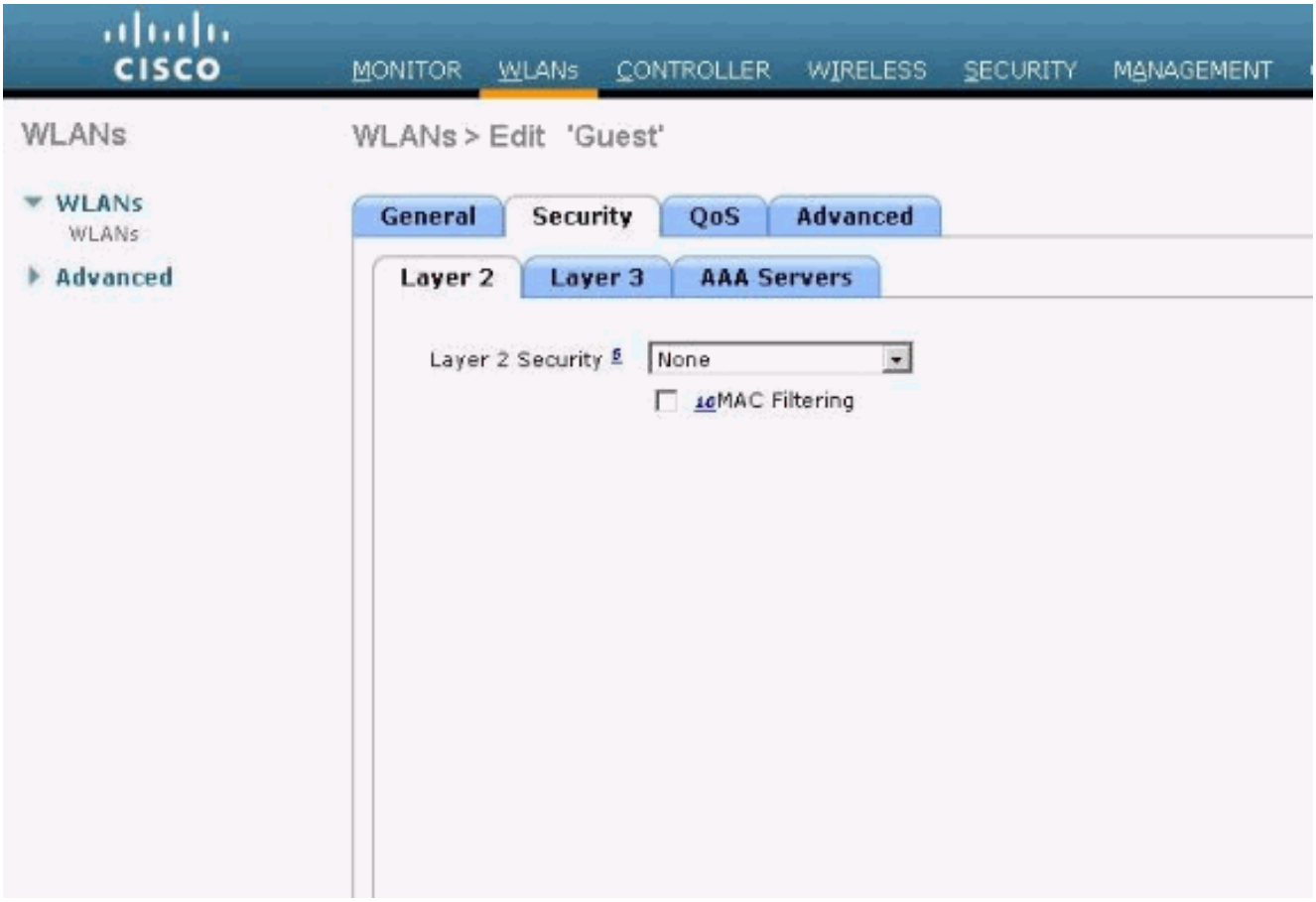
1. Haga clic las **redes inalámbricas (WLAN) del** GUI del regulador para crear una red inalámbrica (WLAN).La ventana de las redes inalámbricas (WLAN) aparece. Esta ventana enumera las redes inalámbricas (WLAN) configuradas en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra **Guest** y la identificación de la red inalámbrica (WLAN) es **1.**
3. Haga clic en Apply
   (Aplicar).



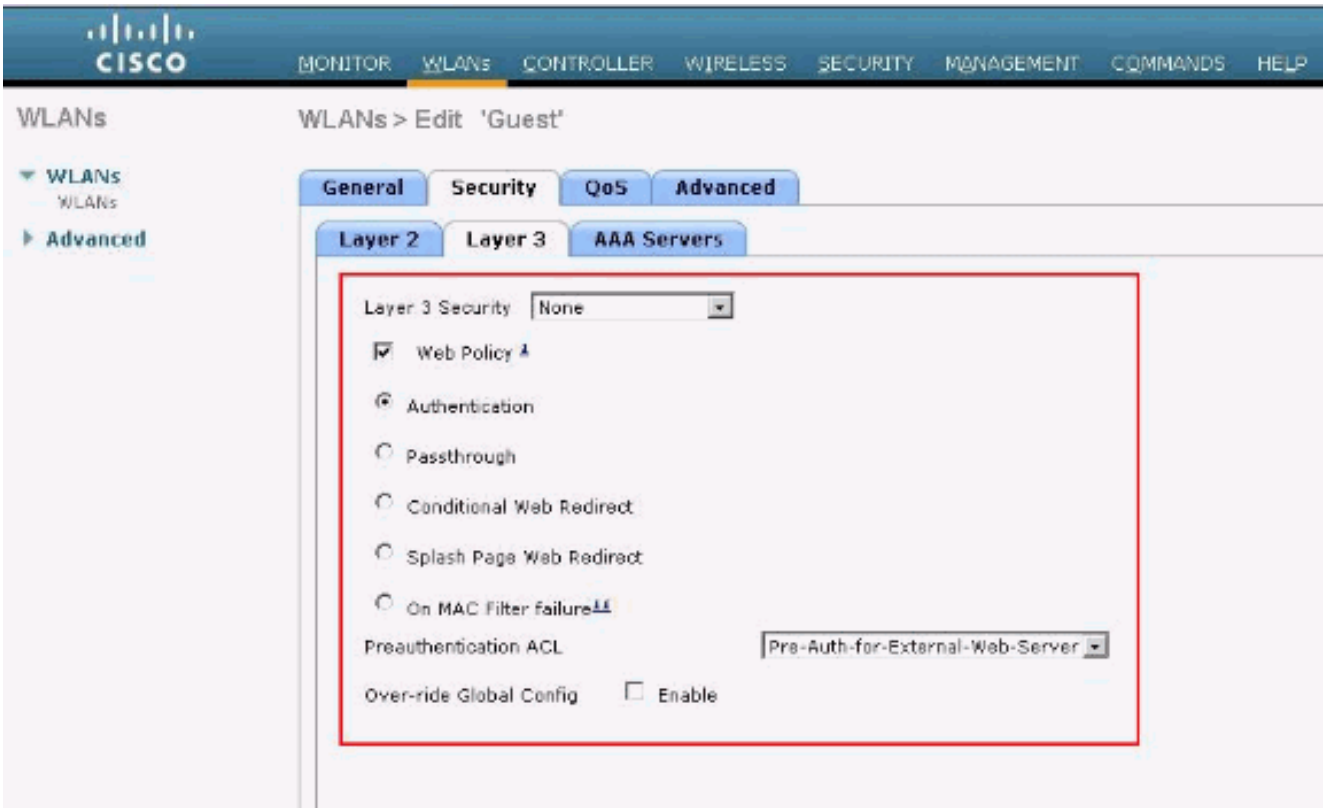
4. En la red inalámbrica (WLAN) **>** corrija la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).Para la red inalámbrica (WLAN) del invitado, en la ficha general, elija el interfaz apropiado del campo de nombre del interfaz.Este ejemplo asocia al **invitado** dinámico del interfaz que fue creado previamente al invitado de la red inalámbrica (WLAN).



Vaya a la **pestaña Seguridad**. Bajo Seguridad de la capa 2, no se selecciona **ninguno** en este ejemplo.**Note**: La autenticación Web no se utiliza con la autenticación del 802.1x. Esto significa que usted no puede elegir el 802.1x o a WPA/WPA2 con el 802.1x como la Seguridad de la capa 2 cuando usted utiliza la autenticación Web. La autenticación Web se utiliza con el resto de los parámetros de Seguridad de la capa
2.



En el campo de Seguridad de la capa 3, controle la casilla de verificación de la **directiva de la red** y elija la **opción de autenticación**.Se elige esta opción porque la autenticación Web se utiliza para autenticar a los clientes inalámbricos del invitado.Elija la Autenticación previa apropiada ACL del menú desplegable.En este ejemplo, se utiliza la Autenticación previa ACL que fue creada previamente.Haga clic en Apply
(Aplicar).

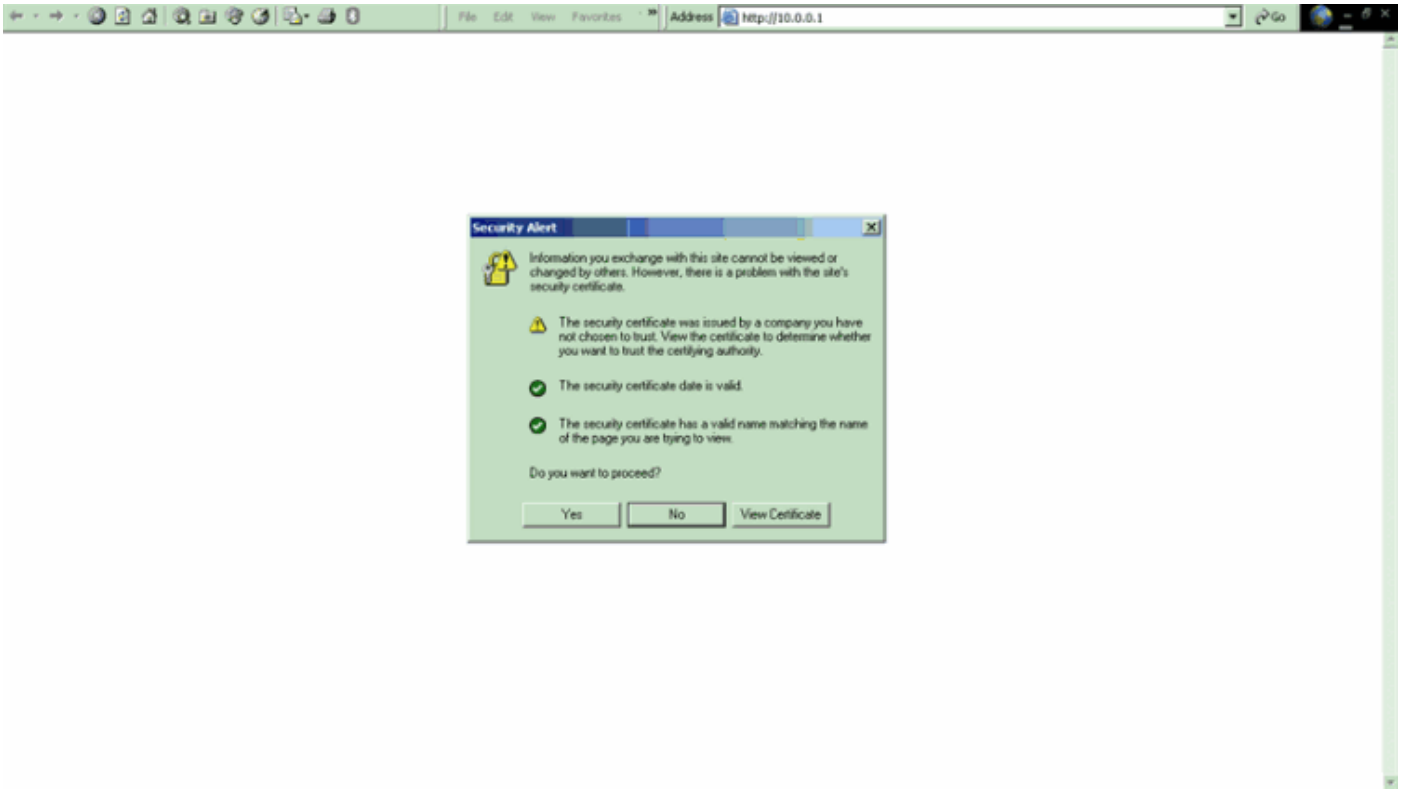


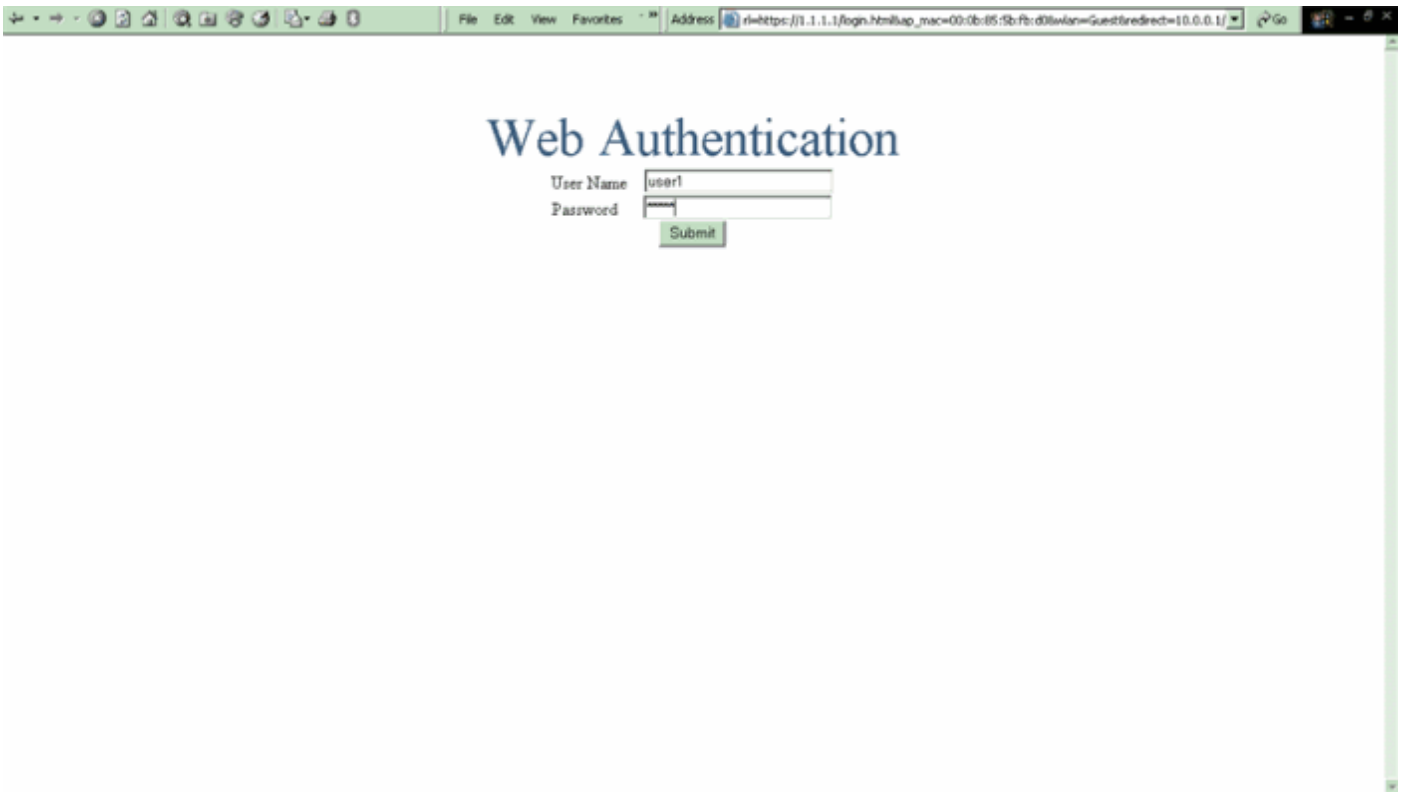
Verifique

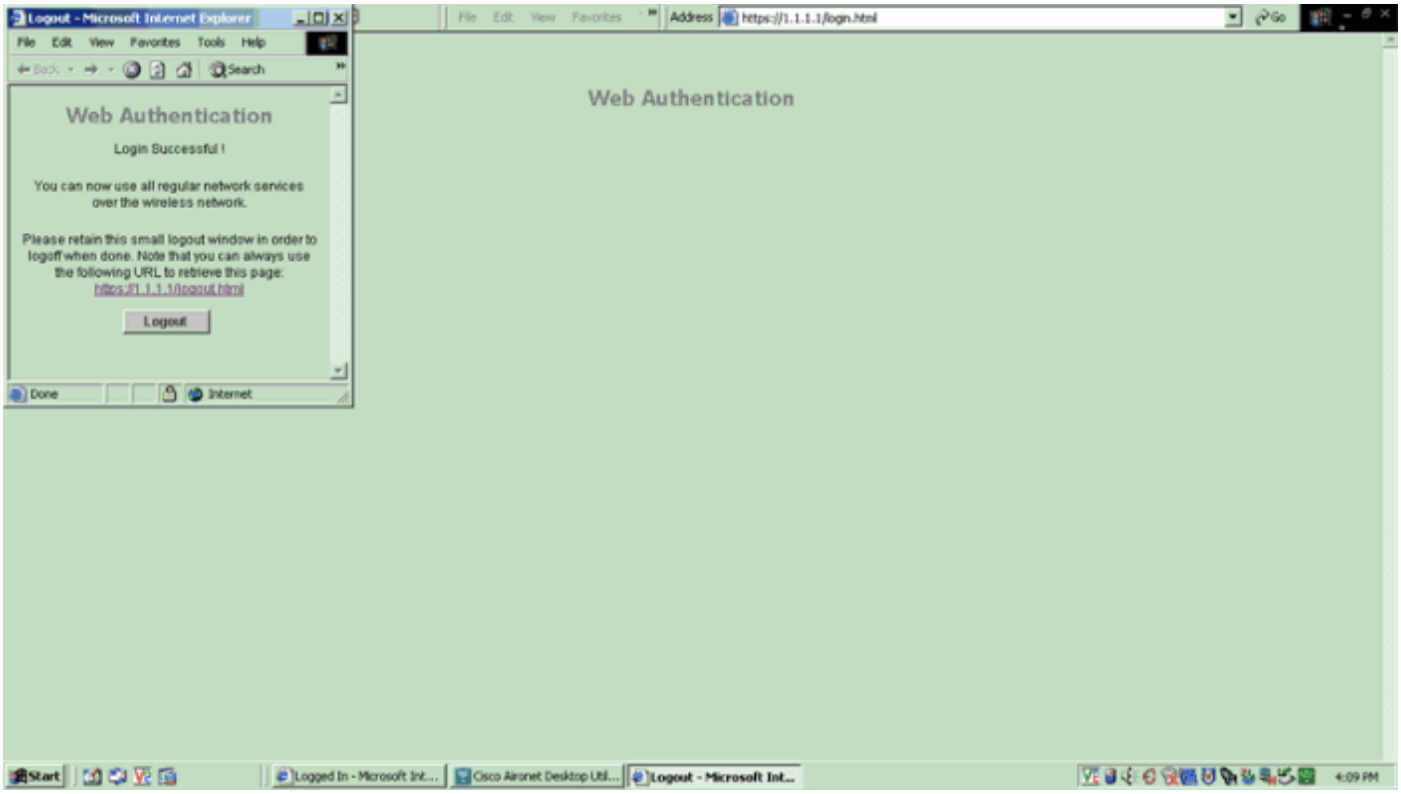
El cliente de red inalámbrica sube y el usuario ingresa el URL, tal como www.cisco.com, en el buscador Web. Porque no han autenticado al usuario, el WLC reorienta al usuario a la clave URL del Web externa.

Incitan al usuario para los credenciales de usuario. Una vez que el usuario somete el nombre de usuario y contraseña, la página de registro toma la entrada de los credenciales de usuario y encendido somete envía la petición de nuevo al ejemplo del action_URL, http://1.1.1.1/login.html, del servidor Web WLC. Se proporciona esto mientras que un parámetro de entrada al cliente reorienta el URL, donde está el direccionamiento 1.1.1.1 de la interfaz virtual en el conmutador.

El WLC autentica al usuario contra la base de datos local configurada en el WLC. Después de la autenticación satisfactoria, el servidor Web WLC cualquiera adelante el usuario al configurado reorienta el URL o al URL el cliente comenzó con, por ejemplo www.cisco.com.


File Edit View Favorites
Address http://10.0.0.1
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate


File Edit View Favorites
Address rl=https://1.1.1.1/login.html&ap_mac=00:0b:85:5b:fb:d0&wlan=Guest&redirect=10.0.0.1/
Web Authentication
User Name user1
Password
Submit



Troubleshooting

Utilice estos comandos debug para resolver problemas su configuración.

- ponga a punto el <client-MAC-direccionamiento xx addr del mac: xx: xx: xx: xx: xx>
- debug aaa all enable
- permiso del estado PEM de la depuración
- permiso de los eventos PEM de la depuración
- permiso del mensaje DHCP de la depuración
- permiso del paquete DHCP de la depuración
- permiso de la depuración P.M. SSH-appgw
- permiso de la depuración P.M. SSH-TCP

Use esta sección para resolver problemas de configuración.

Los clientes reorientados al servidor de la autenticación del Web externa reciben una advertencia del certificado

Problema: Cuando reorientan a los clientes al servidor de la autenticación del Web externa de Cisco, reciben una advertencia del certificado. Hay un certificado válido en el servidor, y si usted conecta con el servidor de la autenticación del Web externa directamente la advertencia del certificado no se recibe. ¿Es esto porque la dirección IP virtual (1.1.1.1) del WLC se presenta al cliente en vez de la dirección IP real del servidor de la autenticación del Web externa que se asocia al certificado?

Solución: Yes. Independientemente de si usted realiza la autenticación del local o del Web externa, usted todavía golpea al servidor Web interno en el regulador. Cuando usted reorienta a un servidor Web externo, usted todavía recibe la advertencia del certificado del regulador a menos que usted tenga un certificado válido en el regulador sí mismo. Si la reorientación se envía a los https, usted recibe la advertencia del certificado del regulador y del servidor Web externo, a

menos que ambos tengan un certificado válido.

Para librarse de las advertencias todas del certificado juntas, usted necesita tener un certificado del nivel de la raíz publicado y descargado sobre su regulador. El certificado se publica para un nombre de host y usted pone que nombre de host en el cuadro del nombre de host DNS bajo interfaz virtual en el regulador. Usted también necesita agregar el nombre de host a su servidor DNS local y señalarlo a la dirección IP virtual (1.1.1.1) del WLC.

Refiera a la generación del pedido de firma de certificado (CSR) para un certificado de tercera persona en un regulador de la red inalámbrica (WLAN) (WLC) para más información.

Error: la “página no puede ser visualizada”

Problema: Después de que el regulador se actualice a 4.2.61.0, la “página no puede ser” mensaje de error visualizado aparece cuando usted utiliza una página web descargada para la autenticación Web. Esto trabajada bien antes de la mejora. La página web interna del valor por defecto carga sin ningún problema.

Solución: De la versión 4.2 y posterior WLC se introduce una nueva función en donde usted puede tener páginas de registro cutomized múltiplo para la autenticación Web.

Para tener la carga de la página web correctamente, no es suficiente fijar el tipo de la autenticación Web según lo **personalizado** global en la **Seguridad > la red auténticas > página de registro de la red**. Debe también ser configurado en una red inalámbrica (WLAN) determinada. A tal efecto, complete estos pasos:

1. Registro en el GUI del WLC.
2. Haga clic en la tabulación de las **redes inalámbricas (WLAN)**, y tenga acceso al perfil de la red inalámbrica (WLAN) configurada para la autenticación Web.
3. En la red inalámbrica (WLAN) > corrija la página, hacen clic la **ficha de seguridad**. Entonces, elija la **capa 3.**
4. En esta página, no elija **ninguno** como la Seguridad de la capa 3.
5. Controle el cuadro de la **directiva de la red**, y elija la **opción de autenticación**.
6. Controle el cuadro del **permiso de la** configuración global de la invalidación, elija **personalizado (descargado)** como el tipo auténtico de la red, y seleccione la página de registro deseada del menú de **Pagepull de la clave** abajo. Haga clic en Apply (Aplicar).

Información Relacionada

- Ejemplo inalámbrico de la configuración de la autenticación Web del regulador LAN
- Vídeo: Autenticación Web en los reguladores inalámbricos LAN de Cisco (WLCs)
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soporte técnico y documentación - Cisco Systems