

Configuración de la Autenticación Web Externa con WLC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Proceso de autenticación Web externa](#)

[Configuración de la red](#)

[Configurar](#)

[Crear una interfaz dinámica para los usuarios invitados](#)

[Crear una ACL de autenticación previa](#)

[Cree una base de datos local en el WLC para los usuarios invitados](#)

[Configuración del WLC para la Autenticación Web Externa](#)

[Configuración de la WLAN para usuarios invitados](#)

[Verificación](#)

[Troubleshoot](#)

[Los clientes redirigidos al servidor de autenticación web externo reciben una advertencia de certificado](#)

[Error: "no se puede mostrar la página"](#)

[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](#)

[Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de Lightweight Access Points (LAP) y Cisco WLC
- Conocimientos básicos sobre el protocolo de punto de acceso ligero (LWAPP) y control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP)
- Conocimientos sobre cómo configurar un servidor web externo

- Conocimientos sobre cómo configurar y configurar servidores DHCP y DNS

Componentes Utilizados

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

- Cisco 4400 WLC que ejecuta la versión 7.0.116.0 del firmware
- LAP de Cisco 1131AG Series
- Adaptador de cliente inalámbrico Cisco 802.11a/b/g que utiliza firmware versión 3.6
- Servidor Web externo que aloja la página de inicio de sesión de autenticación Web
- Servidores DNS y DHCP para la resolución de direcciones y la asignación de direcciones IP a clientes inalámbricos

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Antecedentes

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

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.

Este documento proporciona un ejemplo de configuración para explicar cómo configurar el WLC para utilizar una secuencia de comandos de inicio de sesión de un servidor web externo.

Proceso de autenticación Web externa

Con la autenticación Web externa, la página de inicio de sesión utilizada para la autenticación Web se almacena en un servidor Web externo. Esta es la secuencia de eventos cuando un cliente inalámbrico intenta acceder a una red WLAN que tiene habilitada la autenticación web externa:

1. El cliente (usuario final) se conecta a la WLAN, abre un navegador web e ingresa una URL, como www.cisco.com.

2. El cliente envía una solicitud DNS a un servidor DNS para resolver `www.cisco.com` a la dirección IP.
3. El WLC reenvía la solicitud al servidor DNS que, a su vez, resuelve `www.cisco.com` a la dirección IP y envía una respuesta DNS. El controlador reenvía la respuesta al cliente.
4. El cliente intenta iniciar una conexión TCP con la dirección IP `www.cisco.com` enviando el paquete SYN TCP a la dirección IP `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 TCP ACK para completar la aceptación de contacto TCP de tres vías y la conexión TCP se establece completamente.
6. El cliente envía un paquete HTTP GET destinado a `www.google.com`. El WLC intercepta este paquete, lo envía para la gestión de la redirección. 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`.
7. A continuación, el cliente inicia la conexión HTTPS con la URL de redirección que la envía a `1.1.1.1`. Ésta es la dirección IP virtual del controlador. El cliente tiene que validar el certificado del servidor o ignorarlo para activar el túnel SSL.
8. Debido a que la autenticación Web externa está habilitada, el WLC redirige al cliente al servidor Web externo.
9. La URL de inicio de sesión de autenticación web externa se anexa con parámetros como `AP_Mac_Address`, `client_url` (`www.cisco.com`) y `action_URL` que el cliente necesita para comunicarse con el servidor web del controlador. **Nota:** `Action_URL` indica al servidor web que el nombre de usuario y la contraseña se almacenan en el controlador. Las credenciales se deben enviar de vuelta al controlador para que se autenticuen.
10. La URL del servidor Web externo lleva al usuario a una página de inicio de sesión.
11. La página de login toma la entrada de las credenciales del usuario, y envía la solicitud de vuelta a `action_URL`, ejemplo `http://1.1.1.1/login.html`, del servidor web del WLC.
12. El servidor web del WLC envía el nombre de usuario y la contraseña para la autenticación.
13. El WLC inicia la solicitud del servidor RADIUS o utiliza la base de datos local en el WLC y autentica al usuario.
14. Si la autenticación es exitosa, el servidor web del WLC reenvía al usuario a la URL de redireccionamiento configurada o a la URL con la que el cliente comenzó, como `www.cisco.com`.
15. Si la autenticación falla, entonces el servidor Web del WLC redirige al usuario de nuevo a la URL de login del cliente.

Nota: Para configurar la autenticación webexterna para utilizar puertos que no sean HTTP y HTTPS, ejecute este comando:

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

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

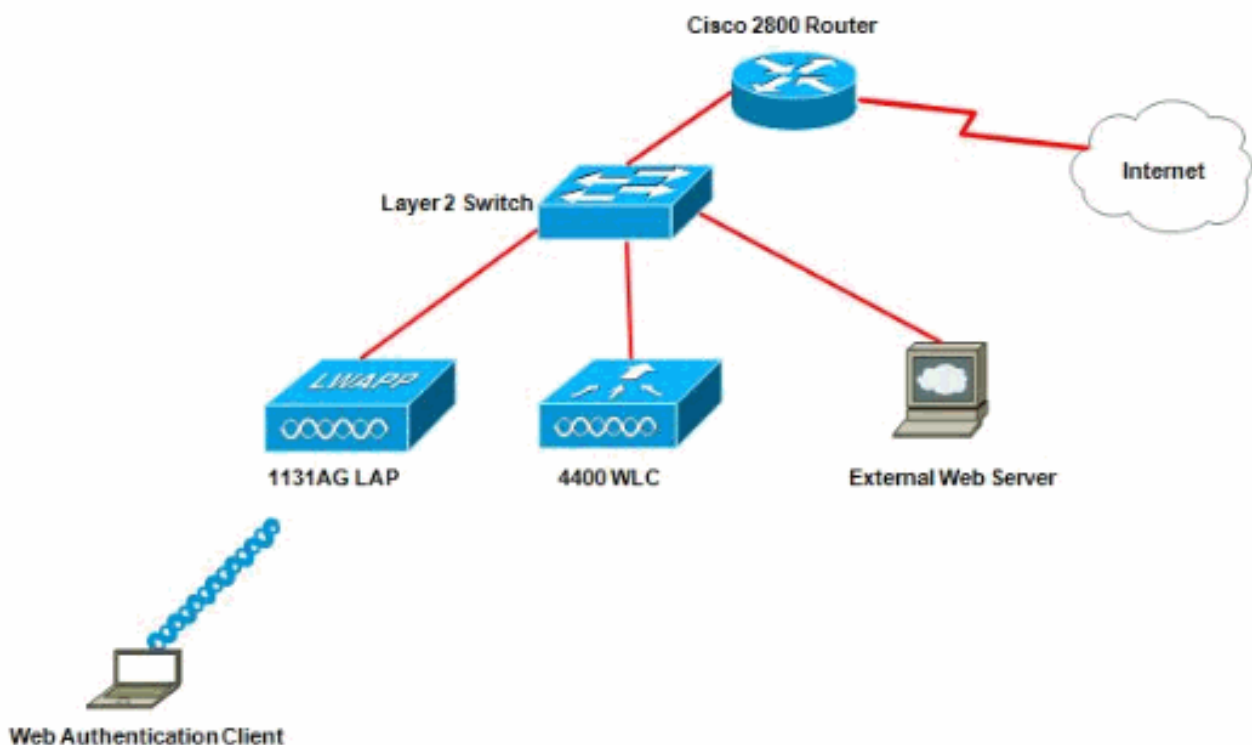
[Configuración de la red](#)

El ejemplo de configuración utiliza esta configuración. Un LAP está registrado en el WLC. Debe configurar un **invitado WLAN para los usuarios invitados y debe habilitar la autenticación web para los usuarios**. También debe asegurarse de que el controlador redirige al usuario a la URL del

servidor web externo (para la autenticación web externa). El servidor web externo aloja la página de inicio de sesión web que se utiliza para la autenticación.

Las credenciales de usuario deben validarse con la base de datos local mantenida en el controlador. Después de la autenticación exitosa, los usuarios deben tener acceso al invitado WLAN. El controlador y otros dispositivos deben configurarse para esta configuración.

Nota: Puede utilizar una versión personalizada del archivo de comandos de inicio de sesión, que se utilizará para la autenticación Web. Puede descargar un script de autenticación Web de ejemplo desde la página [Descargas de Software de Cisco](#). Por ejemplo, para los controladores 4400, navegue hasta **Productos > Inalámbrico > Controlador de LAN inalámbrica > Controladores independientes > Cisco 4400 Series Wireless LAN Controllers > Cisco 4404 Wireless LAN Controller > Software on Chassis > Wireless LAN Controller Web Authentication Bundle-1.0.1** y descargue el archivo `webauth_bundle.zip`.



Nota: El paquete de autenticación web personalizado tiene un límite de hasta 30 caracteres para los nombres de archivo. Asegúrese de que ningún nombre de archivo del paquete tiene más de 30 caracteres.

Nota: Este documento asume que los servidores DHCP, DNS y web externos están configurados. Consulte la documentación de terceros correspondiente para obtener información sobre cómo configurar el servidor web externo, DNS y DHCP.

[Configurar](#)

Antes de configurar el WLC para la autenticación Web externa, debe configurar el WLC para el funcionamiento básico y registrar los LAPs al WLC. Este documento supone que el WLC se configura para el funcionamiento básico y que los LAPs se registran al WLC. Consulte [Registro del Lightweight AP \(LAP\) a un Wireless LAN Controller \(WLC\)](#) si usted es un nuevo usuario que intenta configurar el WLC para el funcionamiento básico con los LAPs.

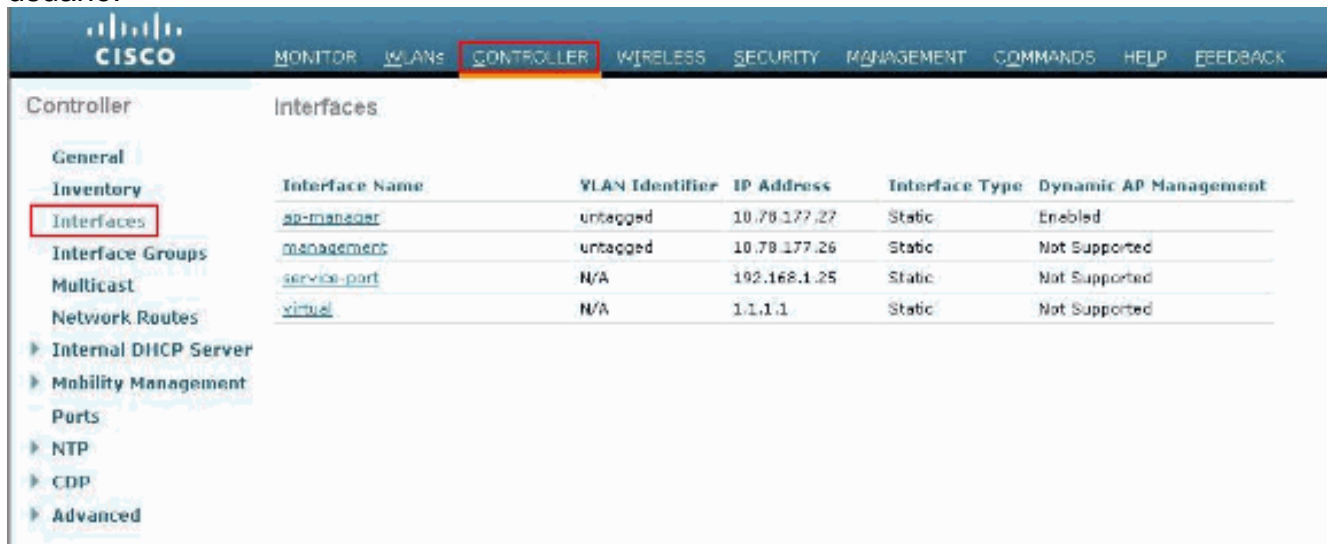
Complete estos pasos para configurar los LAPs y el WLC para esta configuración:

1. [Crear una interfaz dinámica para los usuarios invitados](#)
2. [Crear una ACL de autenticación previa](#)
3. [Cree una base de datos local en el WLC para los usuarios invitados](#)
4. [Configuración del WLC para la Autenticación Web Externa](#)
5. [Configuración de la WLAN para usuarios invitados](#)

[Crear una interfaz dinámica para los usuarios invitados](#)

Complete estos pasos para crear una interfaz dinámica para los usuarios invitados:

1. en la GUI de WLC, elija **Controladores > Interfaces**. Aparece la ventana Interfaces. Esta ventana muestra las interfaces que están configuradas en el controlador. Esto incluye las interfaces predeterminadas, que son la interfaz de administración, la interfaz de administrador de AP, la interfaz virtual y la interfaz de puerto de servicio, así como las interfaces dinámicas definidas por el usuario.



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.78.177.27	Static	Enabled
management	untagged	10.78.177.26	Static	Not Supported
service-port	N/A	192.168.1.25	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

2. Haga clic en **Nuevo para crear una nueva interfaz dinámica**.
3. En la ventana **Interfaces > New**, ingrese el nombre de la interfaz y el ID de VLAN. Luego, haga clic en **Apply**. En este ejemplo, la interfaz dinámica se denomina **guest** y el ID de VLAN se asigna a **10**.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- ▶ Internal DHCP Server
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ Advanced

Interfaces > New

Interface Name

VLAN Id

4. En la ventana Interfaces > Editar, para la interfaz dinámica, ingrese la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Asígnela a un puerto físico del WLC e introduzca la dirección IP del servidor DHCP. A continuación, haga clic en **Aplicar**.

The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. The left sidebar lists various configuration options, with 'Interfaces' highlighted. The main area displays the configuration for the 'guest' interface, which is highlighted with a red border. The configuration is organized into several sections:

- General Information:** Interface Name: guest; MAC Address: 00:0b:85:48:53:c0
- Configuration:** Guest Lan: ; Quarantine: ; Quarantine Vlan Id: 0
- Physical Information:** Port Number: 2; Backup Port: 0; Active Port: 0; Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 10; IP Address: 172.18.1.10; Netmask: 255.255.255.0; Gateway: 172.18.1.20
- DHCP Information:** Primary DHCP Server: 172.18.1.20; Secondary DHCP Server: (empty)
- Access Control List:** ACL Name: none

[Crear una ACL de autenticación previa](#)

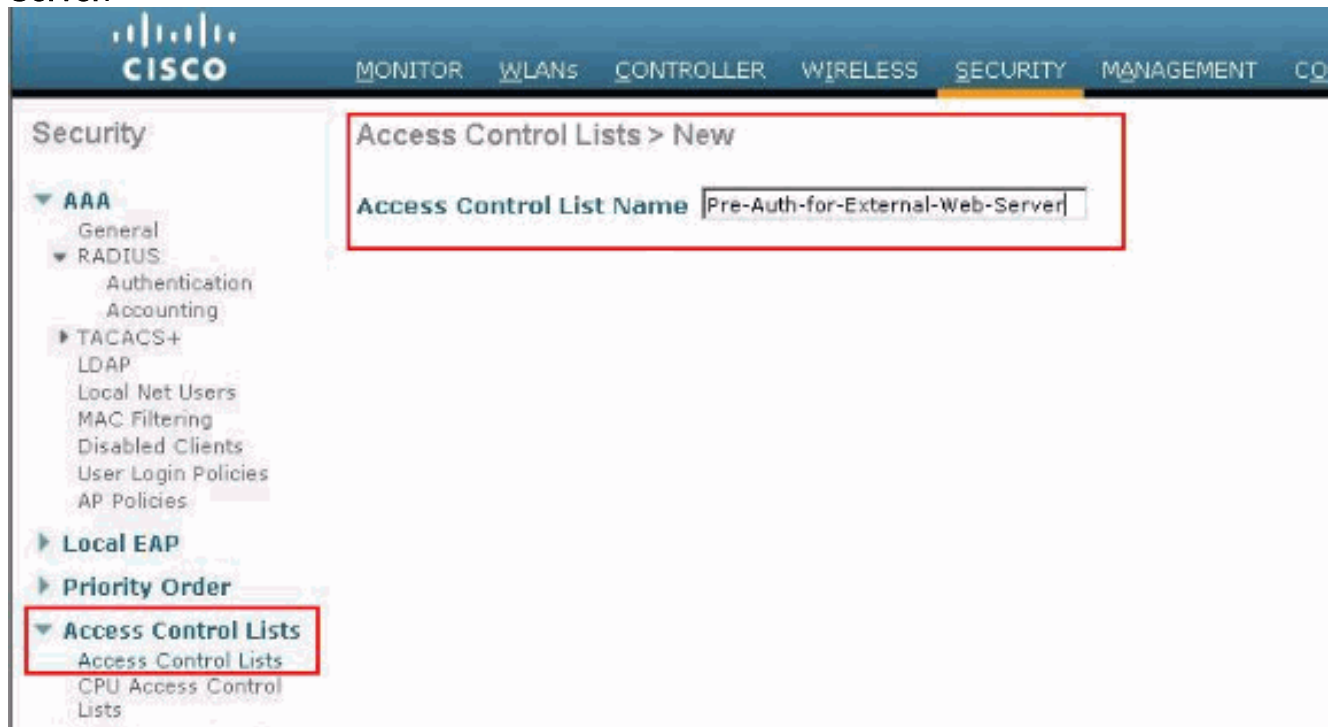
Cuando se utiliza un servidor web externo para la autenticación web, algunas de las plataformas WLC necesitan una ACL de autenticación previa para el servidor web externo (el Cisco 5500 Series Controller, un Cisco 2100 Series Controller, Cisco 2000 Series y el módulo de red del controlador). Para las otras plataformas del WLC la ACL de la pre-autenticación no es obligatoria.

Sin embargo, se recomienda configurar una ACL de autenticación previa para el servidor web externo cuando se utiliza la autenticación web externa.

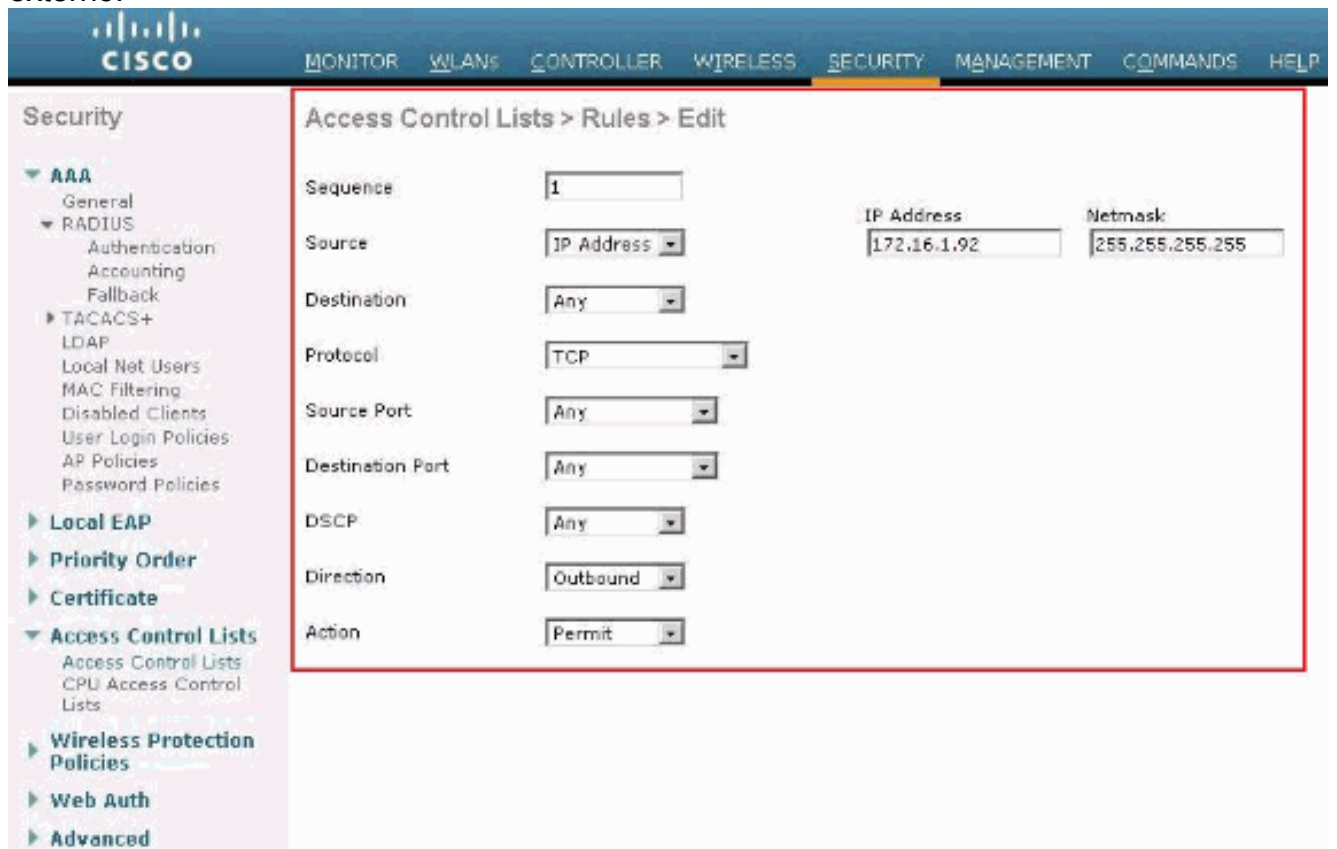
Complete estos pasos para configurar la ACL de autenticación previa para la WLAN:

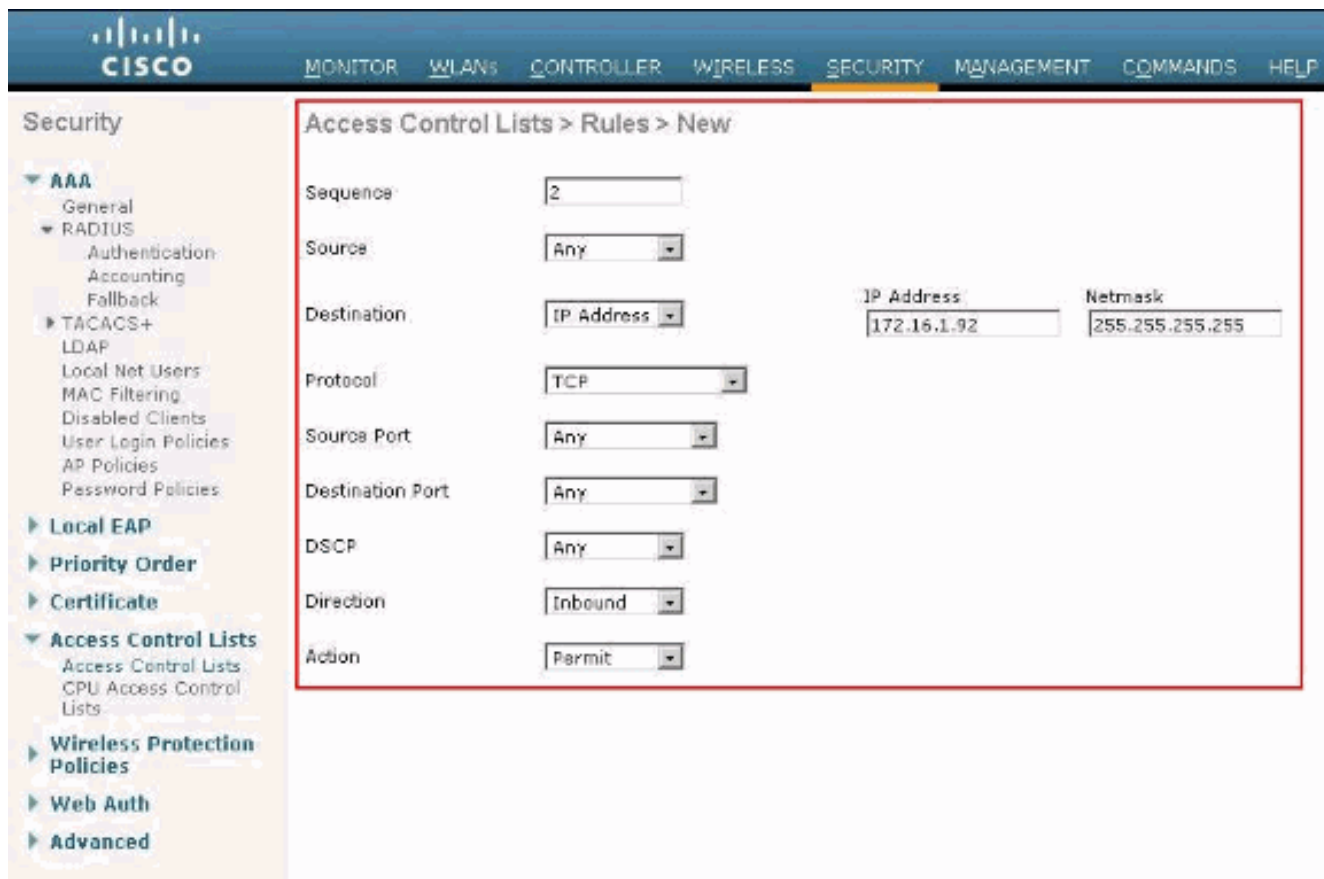
1. Desde la GUI del WLC, elija **Security > Access Control Lists**. Esta ventana permite ver las ACL actuales que son similares a las ACL de firewall estándar.
2. Haga clic en **Nuevo** para crear una nueva ACL.
3. Introduzca el nombre de la ACL y haga clic en **Apply**. En este ejemplo, la ACL se denomina **Pre-Auth-for-External-Web-**

Server.

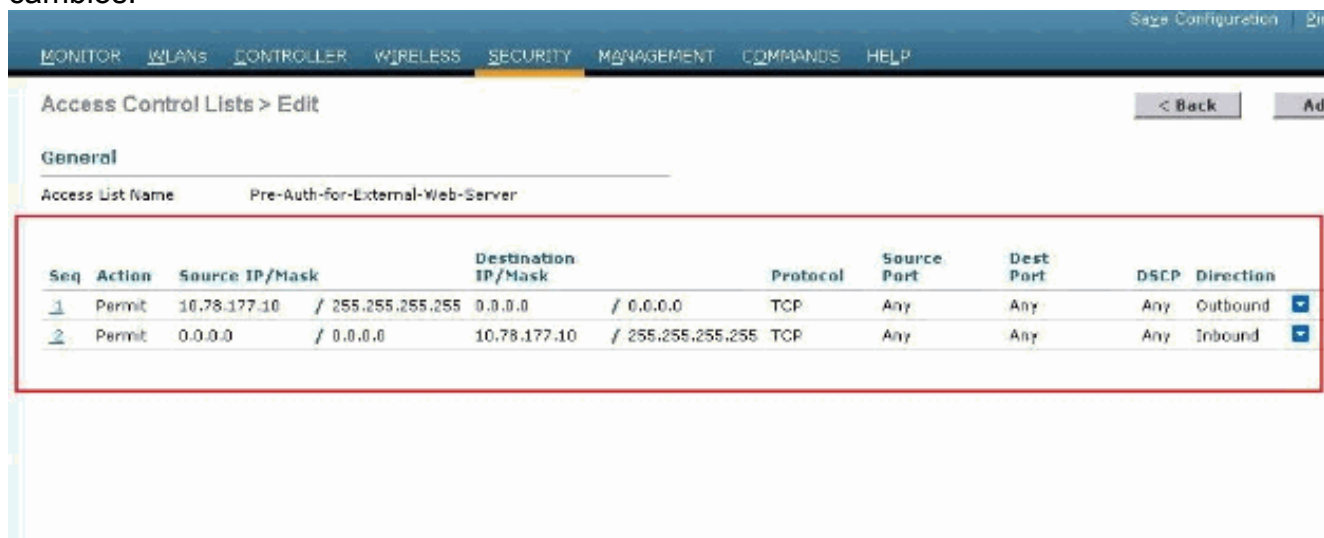


4. Para la nueva ACL creada, haga clic en **Edit**. Aparecerá la ventana ACL > Edit. Esta ventana permite al usuario definir nuevas reglas o modificar las reglas de la ACL existentes.
5. Haga clic en **Agregar nueva regla**.
6. Defina una regla ACL que permita el acceso de los clientes al servidor Web externo. En este ejemplo, 172.16.1.92 es la dirección IP del servidor Web externo.





7. Haga clic en **Aplicar** para aplicar 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 almacenar en la base de datos local del controlador de LAN inalámbrica o se puede almacenar fuera del controlador.

En este documento, la base de datos local en el controlador se utiliza para autenticar a los usuarios. Debe crear un usuario de red local y definir una contraseña para el inicio de sesión del cliente de autenticación web. Complete estos pasos para crear la base de datos del usuario en el WLC:

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.

The screenshot shows the Cisco Security configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the Security menu with AAA expanded, and Local Net Users highlighted with a red box. The main content area is titled 'Local Net Users' and contains a table with the following headers: User Name, WLAN Profile, Guest User, Role, and Description.

3. Haga clic en New para crear a un usuario nuevo. Se abrirá una nueva ventana que le solicitará que ingrese un 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.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, and COMMANDS. The left sidebar shows the 'Security' menu with options like AAA, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The main content area is titled 'Local Net Users > New' and contains the following form fields:

- User Name: User1
- Password: [masked]
- Confirm Password: [masked]
- Guest User:
- Lifetime (seconds): 86400
- Guest User Role:
- WLAN Profile: Guest
- Description: GuestUser1

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the 'Security' menu with options like AAA, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients. The main content area is titled 'Local Net Users' and contains a table with the following data:

User Name	WLAN Profile	Guest User	Role	Description
User1	Guest	Yes		GuestUser1

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

[Configuración del WLC para la Autenticación Web Externa](#)

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

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 cuadro desplegable Tipo de autenticación Web, elija **Externa (Redirigir a servidor externo)**.
3. En la sección **Servidor Web externo**, agregue el nuevo servidor Web externo.
4. En el campo **Redirigir URL después de iniciar sesión**, introduzca la URL de la página a la que se redirigirá al usuario final tras una autenticación correcta. En el campo **External Web Auth URL**, ingrese la URL donde se almacena la página de login en el servidor web externo.

Web Login Page

Web Authentication Type: (Dropdown menu open showing: Internal (Default), Internal (Default), Customized (Downloaded), External (Redirect to external server) [highlighted])

Redirect URL after login:

This page allows you to customize the content and appearance of the login page. The Login page is presented to web users the first time they access the WLAN if "Web Authentication" is turned on (under WLAN Security Policies).

Cisco Logo: Show Hide

Headline:

Message:

External Web Servers

Web Server IP Address:

Web Login Page

Web Authentication Type:

Redirect URL after login:

External Webauth URL:

External Web Servers

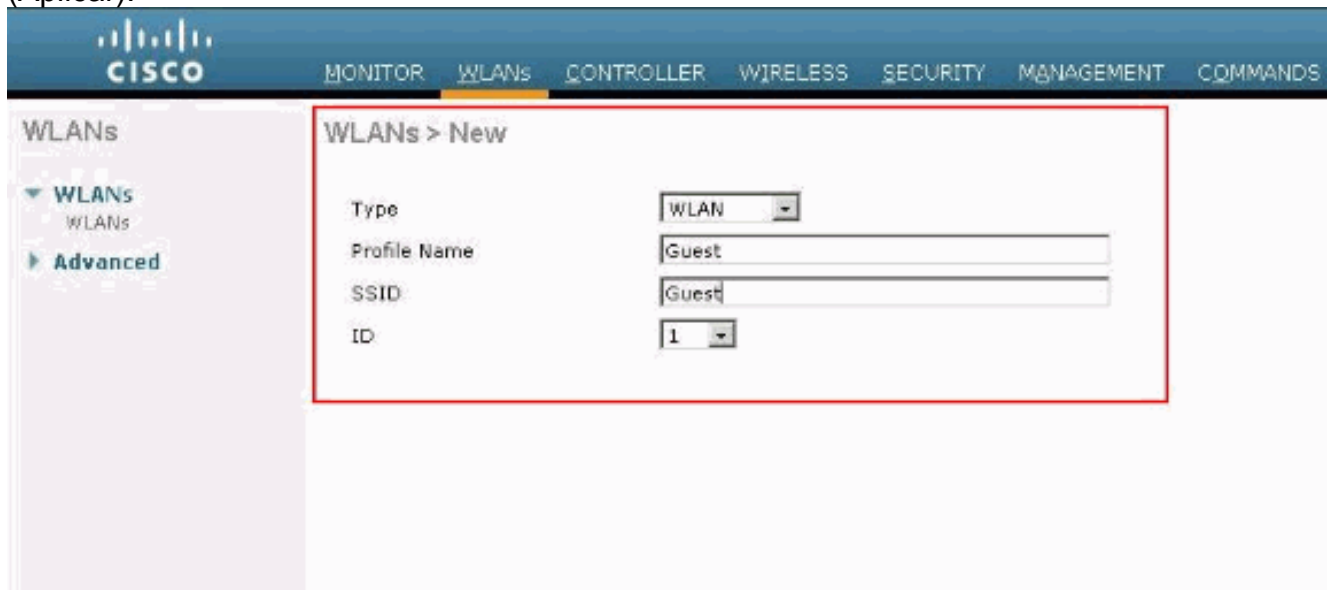
Web Server IP Address:

Nota: En las versiones 5.0 y posteriores del WLC, la página de logout para la autenticación Web también se puede personalizar. Consulte la sección [Asignar Login , Login failure and Logout pages per WLAN](#) de la *Guía de Configuración del Controlador de LAN Inalámbrica, 5.2* para obtener más información sobre cómo configurarlo.

[Configuración de la WLAN para usuarios invitados](#)

El paso final es crear WLANs para los usuarios invitados. Complete estos pasos:

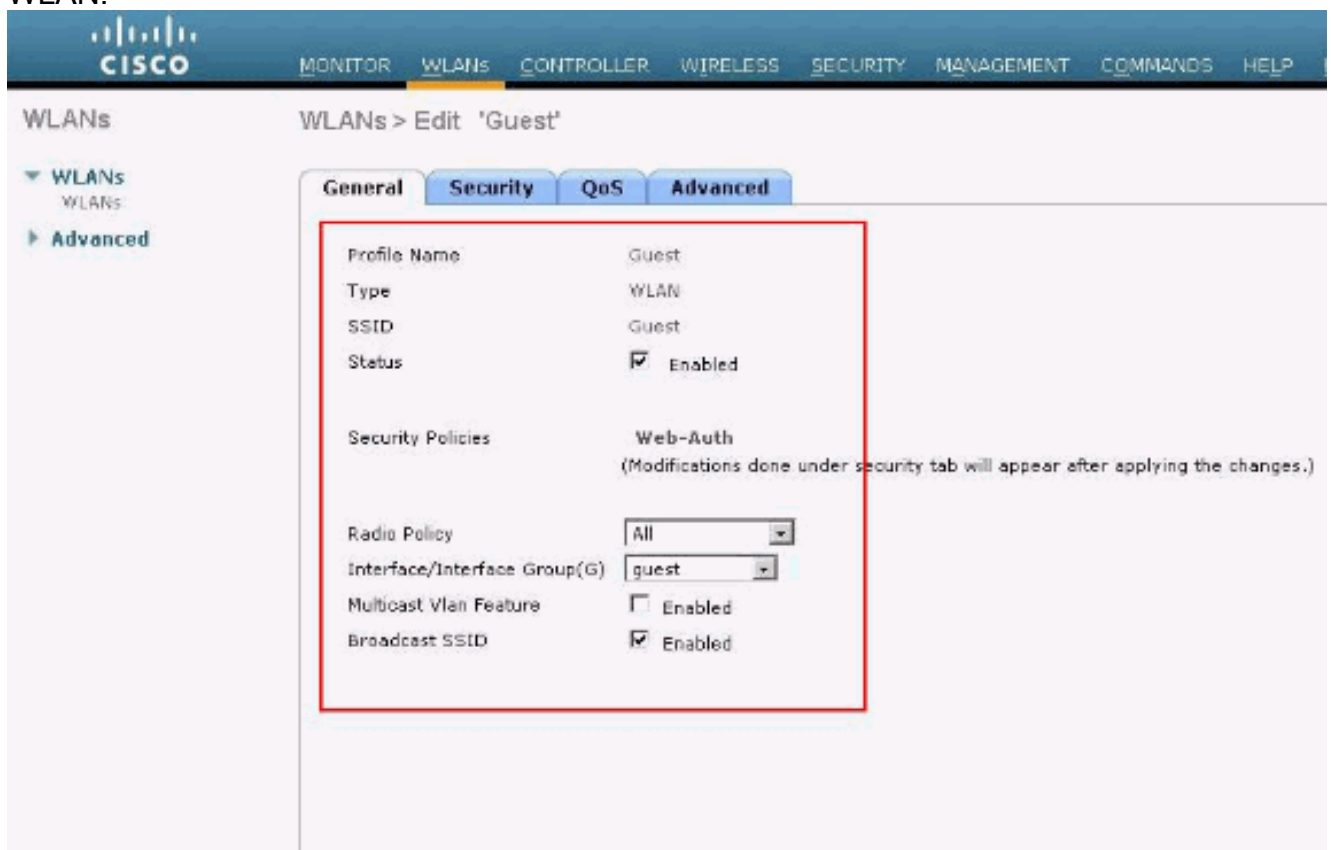
1. Haga clic en **WLAN** en la GUI para crear una WLAN. Aparece la ventana WLAN. Esta ventana enumera las WLAN configuradas en el controlador.
2. Haga clic en **Nuevo para configurar una WLAN nueva**. En este ejemplo, la WLAN se denomina **Guest** y el **Id. de WLAN es 1**.
3. Haga clic en **Apply** (Aplicar).



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains a form with the following fields:

Type	WLAN
Profile Name	Guest
SSID	Guest
ID	1

4. En la ventana **WLAN > Edit**, defina los parámetros específicos de la WLAN. Para la WLAN de invitado, en la ficha General, elija la interfaz adecuada del campo **Interface Name** (Nombre de interfaz). Este ejemplo asigna el **invitado de interfaz dinámica** que se creó previamente al invitado WLAN.



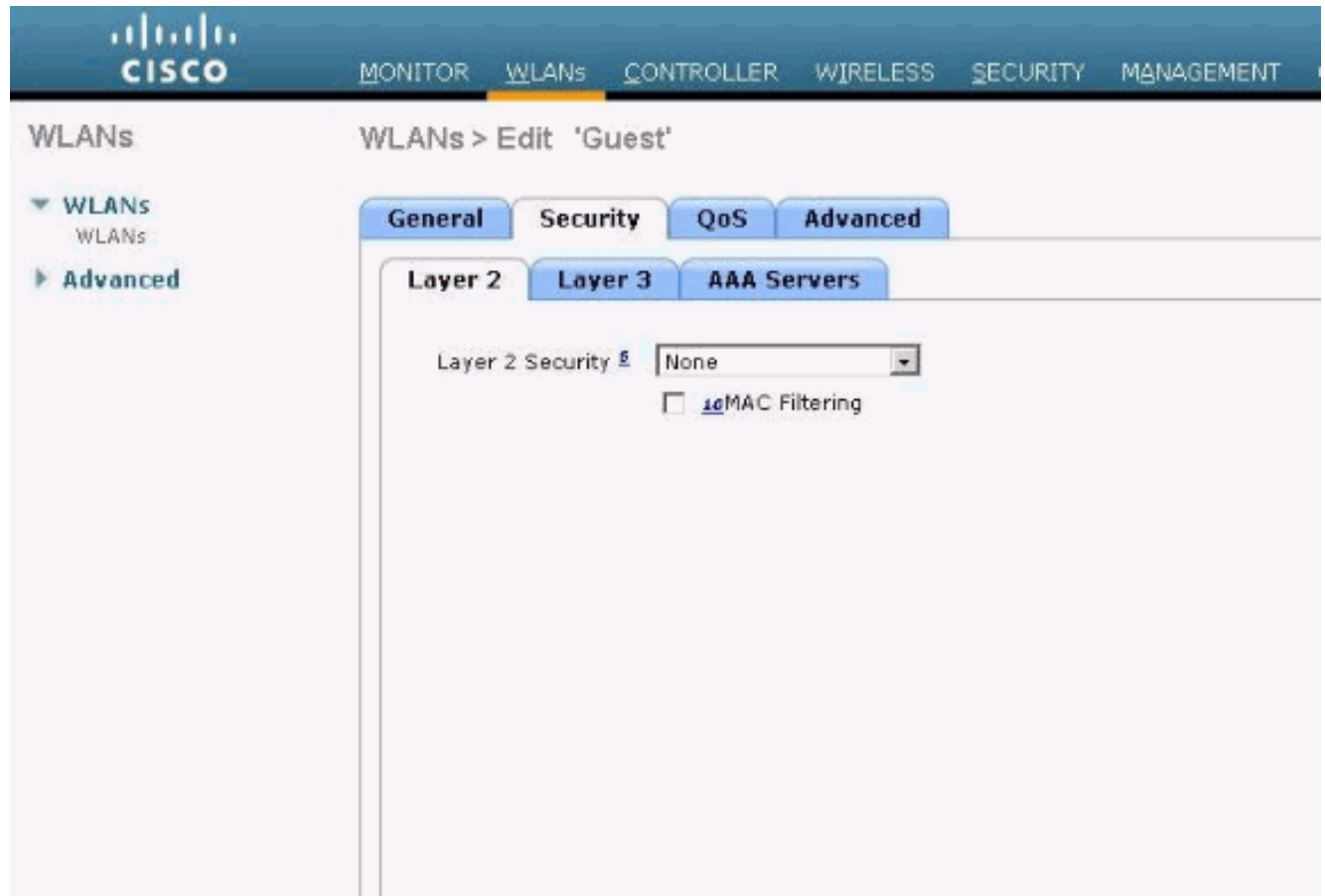
The screenshot shows the Cisco WLAN configuration interface for editing the 'Guest' WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Guest'' and contains a form with the following fields:

Profile Name	Guest
Type	WLAN
SSID	Guest
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	guest
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

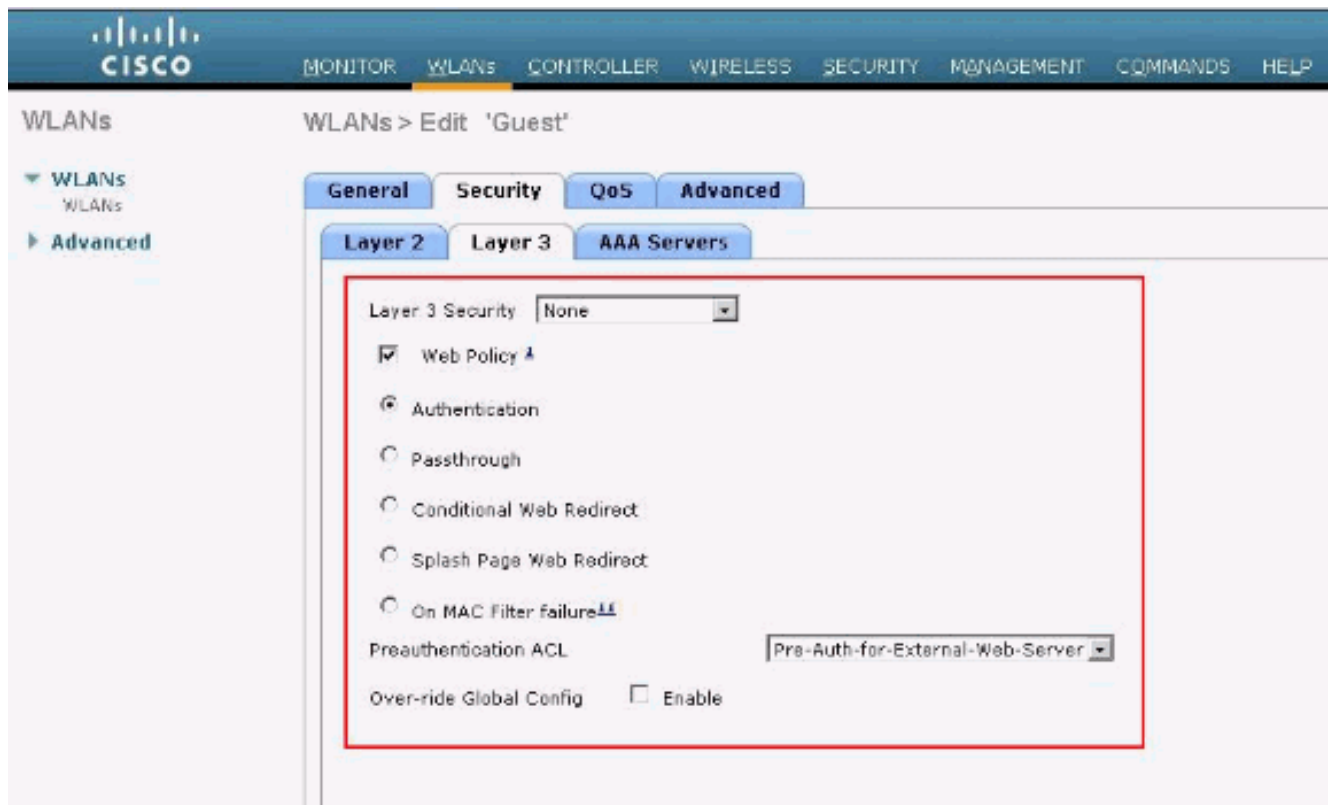
Vaya a la pestaña Seguridad. En Seguridad de la capa 2, **None** se selecciona en este ejemplo. **Nota:** la autenticación Web no es compatible con la autenticación 802.1x. Esto significa que no puede elegir 802.1x o un WPA/WPA2 con 802.1x como seguridad de capa 2

cuando utiliza la autenticación web. La autenticación web es compatible con todos los demás parámetros de seguridad de capa

2.



En el campo Layer 3 Security, marque la casilla de verificación **Web Policy** y elija la opción **Authentication**. Esta opción se elige porque la autenticación Web se utiliza para autenticar los clientes invitados inalámbricos. Elija la ACL de autenticación previa adecuada en el menú desplegable. En este ejemplo, se utiliza la ACL de autenticación previa que se creó previamente. Haga clic en Apply (Aplicar).



Verificación

El cliente inalámbrico se activa y el usuario introduce la URL, como www.cisco.com, en el navegador web. Debido a que el usuario no ha sido autenticado, el WLC redirige al usuario a la URL de login web externa.

Se le solicitarán al usuario las credenciales de usuario. Una vez que el usuario envía el nombre de usuario y la contraseña, la página de login toma la entrada de las credenciales del usuario y en el envío envía la solicitud de nuevo al ejemplo `action_URL`, `http://1.1.1.1/login.html`, del servidor web del WLC. Esto se proporciona como un parámetro de entrada a la URL de redirección del cliente, donde 1.1.1.1 es la dirección de la interfaz virtual en el switch.

El WLC autentica al usuario contra la base de datos local configurada en el WLC. Después de la autenticación exitosa, el servidor web del WLC reenvía al usuario a la URL de redireccionamiento configurada o a la URL con la que el cliente comenzó, como www.cisco.com.

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.

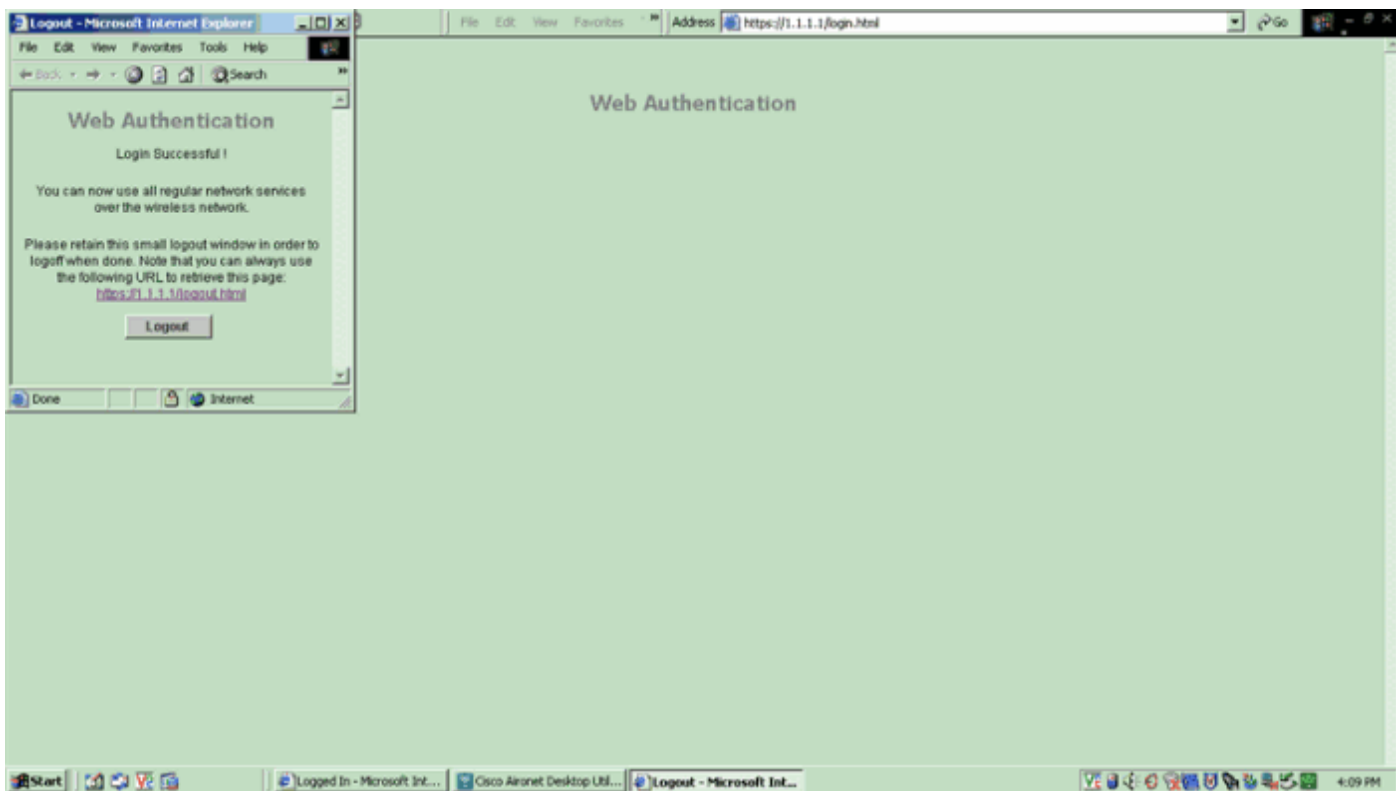
- ⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- ✔ The security certificate date is valid.
- ✔ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Web Authentication

User Name

Password



Troubleshoot

Utilice estos comandos debug para resolver problemas de su configuración.

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

Use esta sección para resolver problemas de configuración.

Los clientes redirigidos al servidor de autenticación web externo reciben una advertencia de certificado

Problema: cuando los clientes son redirigidos al servidor de autenticación web externo de Cisco, reciben una advertencia de certificado. Hay un certificado válido en el servidor, y si se conecta al servidor de autenticación web externo directamente, la advertencia del certificado no se recibe. ¿Se debe esto a que la dirección IP virtual (1.1.1.1) del WLC se presenta al cliente en lugar de la dirección IP real del servidor de autenticación web externo que está asociado con el certificado?

Solución: Sí. Independientemente de si realiza o no la autenticación web local o externa, aún puede acceder al servidor web interno en el controlador. Al redirigir a un servidor Web externo, el controlador le sigue advirtiéndole de que el certificado no es válido, a menos que tenga un certificado válido en el propio controlador. Si la redirección se envía a https, recibirá la advertencia del certificado del controlador y del servidor web externo, a menos que ambos tengan un certificado válido.

Para deshacerse de todas las advertencias de certificado, debe tener un certificado de nivel raíz emitido y descargado en su controlador. El certificado se emite para un nombre de host y se coloca ese nombre de host en el cuadro Nombre de host DNS debajo de la interfaz virtual en el controlador. También debe agregar el nombre de host a su servidor DNS local y señalarlo a la dirección IP virtual (1.1.1.1) del WLC.

Consulte [Generación de Solicitud de Firma de Certificado \(CSR\) para un Certificado de Terceros en un Controlador WLAN \(WLC\)](#) para obtener más información.

Error: "no se puede mostrar la página"

Problema: Después de actualizar el controlador a la versión 4.2.61.0, aparece el mensaje de error "page cannot be played " (la página no se puede mostrar) cuando utiliza una página Web descargada para la autenticación Web. Esto funcionaba bien antes de la actualización. La página web interna predeterminada se carga sin ningún problema .

Solución: A partir de la versión 4.2 y posterior del WLC se introduce una nueva característica en la que usted puede tener múltiples páginas de login personalizadas para la autenticación Web.

Para que la página web se cargue correctamente, no es suficiente configurar el tipo de autenticación web como **personalizado** globalmente en la página **Security > Web Auth > Web login**. También se debe configurar en una WLAN particular . A tal efecto, complete estos pasos:

1. Inicie sesión en la GUI del WLC.
2. Haga clic en la ficha **WLANs** y acceda al perfil de WLAN configurado para la autenticación Web.
3. En la página WLAN > Edit, haga clic en la pestaña **Security**. A continuación, seleccione **Capa 3**.
4. En esta página, elija **None** como Layer 3 Security.
5. Marque la casilla **Web Policy** y elija la opción **Authentication**.
6. Marque la casilla Override Global Config **Enable**, elija **Customized (Downloaded)** como tipo de autenticación web y seleccione la página de inicio de sesión deseada del menú desplegable **Login** . Haga clic en Apply (Aplicar).

Información Relacionada

- [Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico](#)
- [Vídeo: Autenticación web en controladores LAN inalámbricos \(WLC\) de Cisco](#)
- [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](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).