

Guía de implementación de autenticación Web externa con switching local FlexConnect

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Descripción general de características](#)

[Información Relacionada](#)

Introducción

Este documento explica cómo utilizar un Servidor Web Externo con el FlexConnect Local Switching para diferentes Directivas Web.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimientos básicos sobre la arquitectura y los puntos de acceso (AP) de FlexConnect
- Conocimientos sobre cómo configurar y 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.

- Controlador de LAN inalámbrica (WLC) Cisco 7500 que ejecuta la versión de firmware 7.2.110.0
- Punto de acceso ligero (LAP) de la serie 3500 de Cisco
- Servidor web externo que aloja la página de inicio de sesión de autenticación web
- Servidores DNS y DHCP en el sitio local para la resolución de direcciones y la asignación de direcciones IP a clientes inalámbricos

The information in this document was created from the devices in a specific lab environment. Aunque se utiliza un WLC de la serie 7500 para esta guía de implementación, esta función se soporta en los WLC 2500, 5500 y WiSM-2. All of the devices used in this document started with a cleared (default) configuration. 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.](#)

Descripción general de características

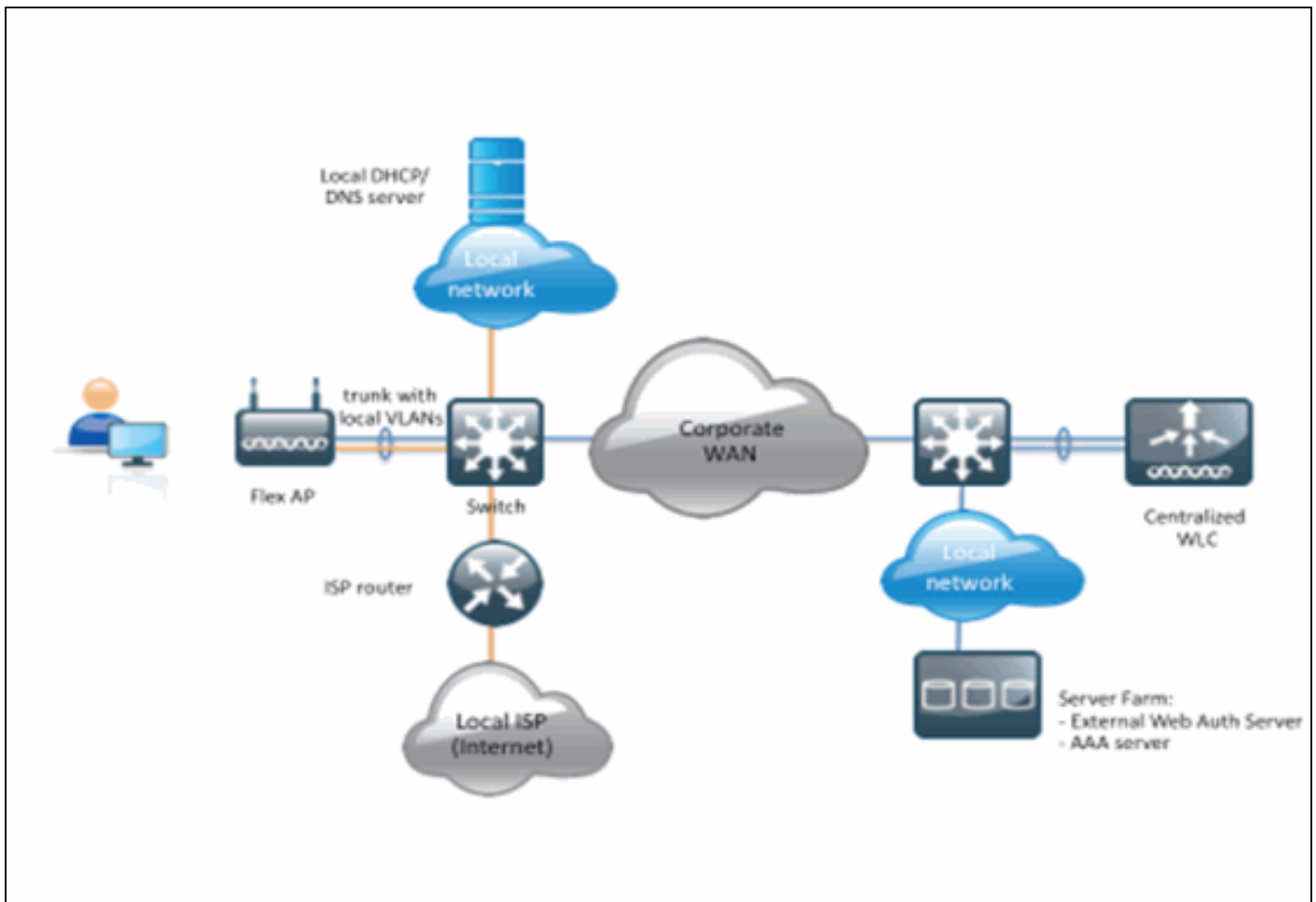
Esta función amplía la capacidad de realizar la autenticación Web a un servidor Web externo desde el AP en el modo FlexConnect, para las WLAN con tráfico conmutado localmente (FlexConnect - Local Switching). Antes de la versión 7.2.110.0 del WLC, la autenticación web a un servidor externo era soportada por AP en modo local o en modo FlexConnect para WLAN con tráfico conmutado centralmente (FlexConnect - Central Switching).

A menudo denominada Autenticación Web Externa, esta función amplía la capacidad de la WLAN de conmutación local de FlexConnect para admitir todos los tipos de seguridad de redirección web de capa 3 que actualmente proporciona el controlador:

- Autenticación Web
- Paso a través de la Web
- Redirección condicional a la Web
- Redirección condicional de la página de bienvenida

Teniendo en cuenta una WLAN configurada para la autenticación Web y para el switching local, la lógica detrás de esta función es distribuir y aplicar la Lista de control de acceso (ACL) FlexConnect de autenticación previa directamente en el nivel AP en lugar del nivel WLC. De esta manera, el AP conmutará los paquetes que vienen del cliente inalámbrico que son permitidos por la ACL, localmente. Los paquetes no permitidos todavía se envían a través del túnel CAPWAP al WLC. Por otra parte, cuando el AP recibe el tráfico a través de la interfaz cableada, si lo permite la ACL, lo reenviará al cliente inalámbrico. De no ser así, el paquete se pierde. Una vez que el cliente se autentica y autoriza, se elimina la ACL FlexConnect de autenticación previa y todo el tráfico de datos del cliente se permite y se conmuta localmente.

Nota: Esta función funciona bajo la suposición de que el cliente puede alcanzar el servidor externo desde la VLAN conmutada localmente.



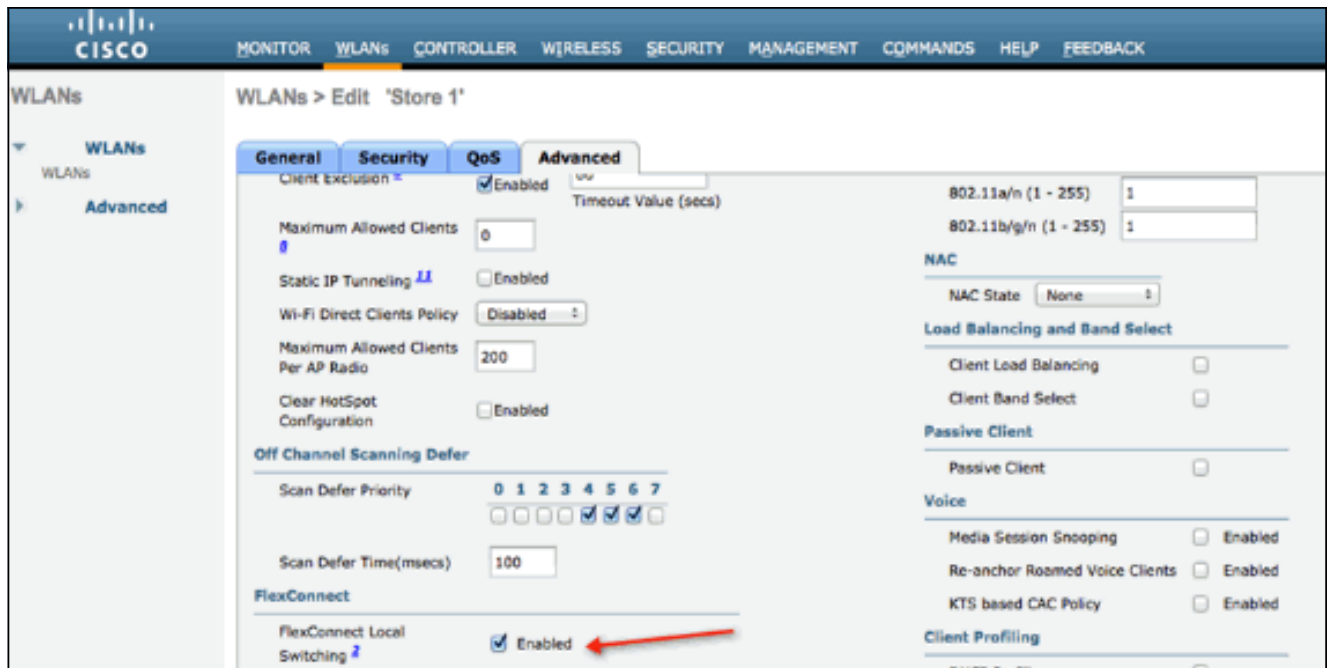
Resumen

- WLAN configurada para FlexConnect Local Switching y Seguridad L3
- Las ACL de FlexConnect se utilizarán como ACL de autenticación previa
- Las ACL de FlexConnect una vez configuradas deben enviarse a la base de datos de AP a través de Flex Group o a través de AP individual, o pueden aplicarse en la WLAN
- AP permite que todo el tráfico que coincide con la ACL de autenticación previa sea conmutado localmente

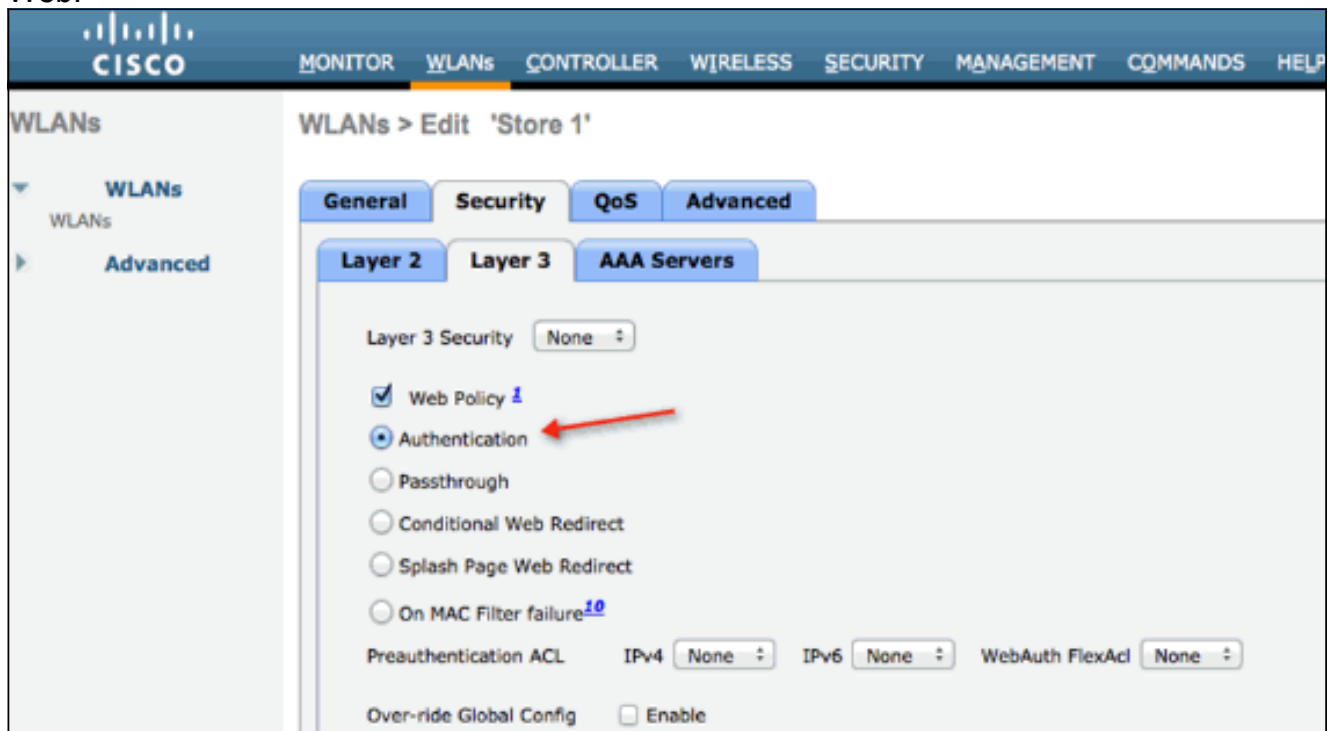
Procedimiento:

Complete estos pasos para configurar esta función:

1. Configure una WLAN para FlexConnect Local Switching.



2. Para habilitar la autenticación Web externa, debe configurar la política web como la política de seguridad para la WLAN conmutada localmente. Esto incluye una de estas cuatro opciones: Autenticación, Transferencia, Redirección web condicional, Redirección web de la página Splash. Este documento captura un ejemplo para la autenticación Web:



Los dos primeros métodos son similares y se pueden agrupar como métodos de autenticación Web desde un punto de vista de configuración. Los dos segundos (Redirección condicional y Página de bienvenida) son Políticas Web y se pueden agrupar como métodos de política Web.

3. La ACL FlexConnect de autenticación previa debe configurarse para permitir que los clientes inalámbricos alcancen la dirección IP del servidor externo. El tráfico ARP, DHCP y DNS se permite automáticamente y no es necesario especificarlo. En Security > Access Control List, elija **FlexConnect ACL**. Luego, haga clic en **Agregar** y defina los nombres y reglas como una ACL de controlador normal.

Access Control Lists > Edit

General

Access List Name: flex_pre_auth

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.1.1.29 / 255.255.255.255	Any	Any	Any	Any

Nota: Deberá crear reglas inversas para el tráfico cada vez.

4. Una vez creadas las ACL de FlexConnect, se debe aplicar lo que se puede hacer en diferentes niveles: AP, FlexConnect Group y WLAN. Esta última opción (Flex ACL en WLAN) es sólo para la autenticación Web y el paso a través de Web para otros dos métodos en Política Web, como Conditional y Splash Redirect. Las ACL sólo se pueden aplicar en el AP o en el Flex Group. Este es un ejemplo de una ACL asignada en el nivel AP. Vaya a **Wireless > seleccione AP** y luego haga clic en la **pestaña FlexConnect:**

All APs > Details for 3600I.0418

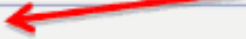
General | Credentials | Interfaces | High Availability | Inventory | **FlexConnect** | Advanced

VLAN Support

Native VLAN ID: **VLAN Mappings**

FlexConnect Group Name: Not Configured

PreAuthentication Access Control Lists

[External WebAuthentication ACLs](#) 

OfficeExtend AP

Enable OfficeExtend AP

Enable Least Latency Controller Join

Reset Personal SSID

Haga clic en el enlace **ACLs de autenticación WebExterna**. Luego, elija la ACL para el ID de WLAN particular:

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HE

Wireless All APs > 3600I.0418 > ACL Mappings

Access Points
 All APs
 Radios
 802.11a/n
 802.11b/g/n
 Global Configuration

Advanced
 Mesh
 RF Profiles
 FlexConnect Groups
 FlexConnect ACLs

802.11a/n
 802.11b/g/n
 Media Stream
 Country
 Timers
 QoS

AP Name 3600I.0418
Base Radio MAC 64:d9:89:42:0e:20

WLAN ACL Mapping

WLAN Id
 WebAuth ACL

WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	AP-flex-ACL <input type="button" value="Add"/>

WebPolicies

WebPolicy ACL

[WebPolicy Access Control Lists](#)

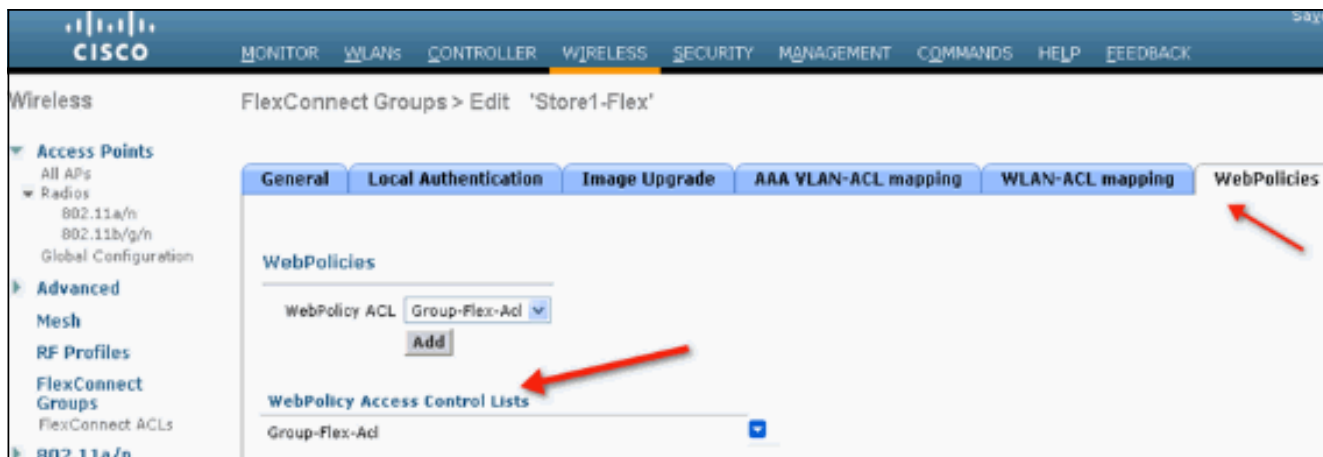
Del mismo modo, para la ACL de política web (por ejemplo, la redirección condicional o la redirección de página splash), recibirá una opción para seleccionar la ACL de Flex Connect en WebPolicies después de hacer clic en el mismo enlace ACL de autenticación Web externa. Esto se muestra aquí:

The screenshot shows the Cisco Wireless configuration interface. The breadcrumb trail is 'All APs > 3600I.0418 > ACL Mappings'. On the left, there is a navigation menu with sections like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and 'FlexConnect ACLs'. The main content area is divided into several sections: 'WLAN ACL Mapping' with fields for 'WLAN Id' (0) and 'WebAuth ACL' (AP-flex-ACL); a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL' containing one entry with '1', 'flex', and 'AP-flex-ACL'; and 'WebPolicies' with a 'WebPolicy ACL' dropdown set to 'AP-flex-ACL'. A red arrow points to this dropdown. At the bottom, there is a link for 'WebPolicy Access Control Lists'.

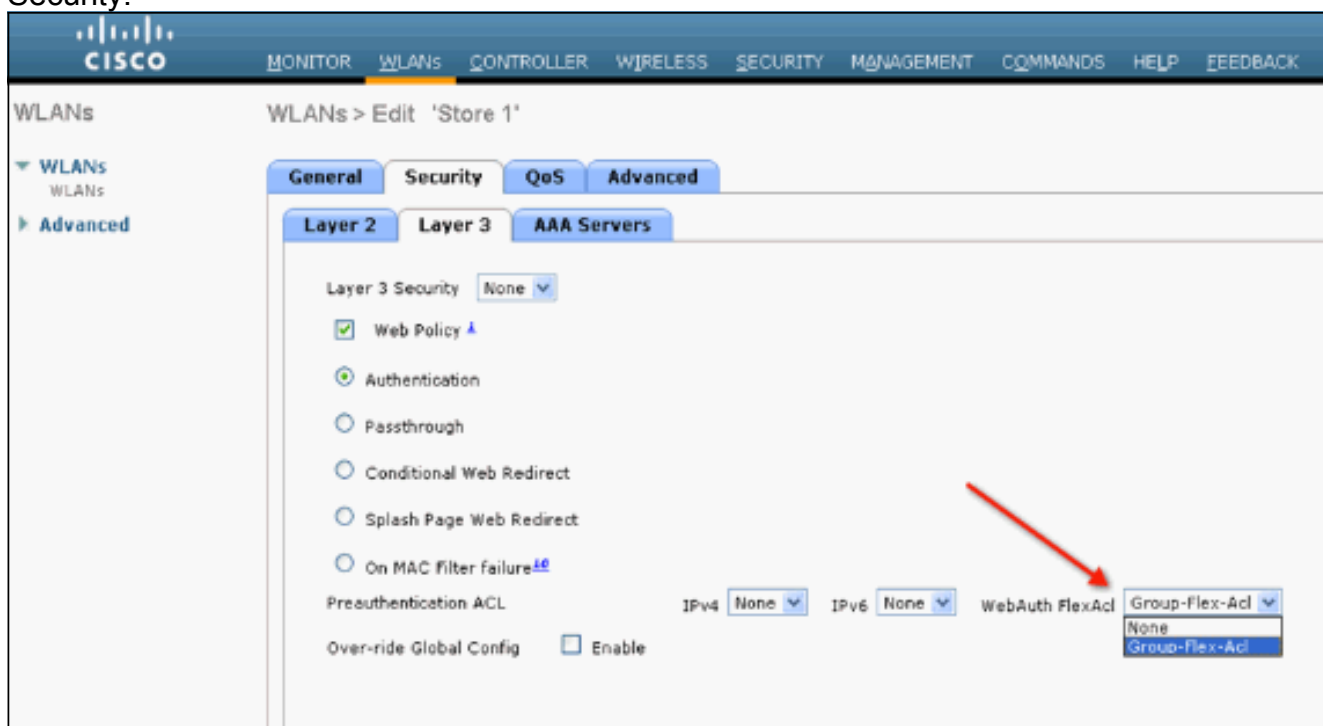
5. La ACL también se puede aplicar en el nivel del grupo FlexConnect. Para hacer esto, vaya a la pestaña **mapeo WLAN-ACL** en la configuración del grupo FlexConnect. A continuación, elija la ID de WLAN y la ACL que desea aplicar. Haga clic en Add (Agregar). Esto es útil cuando desea definir una ACL para un grupo de AP.

The screenshot shows the Cisco Wireless configuration interface for a FlexConnect Group named 'Store1-Flex'. The breadcrumb trail is 'FlexConnect Groups > Edit "Store1-Flex"'. The 'WLAN-ACL mapping' tab is selected, and a red arrow points to it. The configuration area shows 'WLAN ACL Mapping' with fields for 'WLAN Id' (0) and 'WebAuth ACL' (Group-flex-ACL). Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL' containing one entry with '1', 'flex', and 'Group-flex-ACL'. Another red arrow points to the 'WebAuth ACL' dropdown menu.

Del mismo modo, para la ACL de política web (para el Web Policy Redirect condicional y de página de presentación), debe seleccionar la ficha **WebPolicies**.

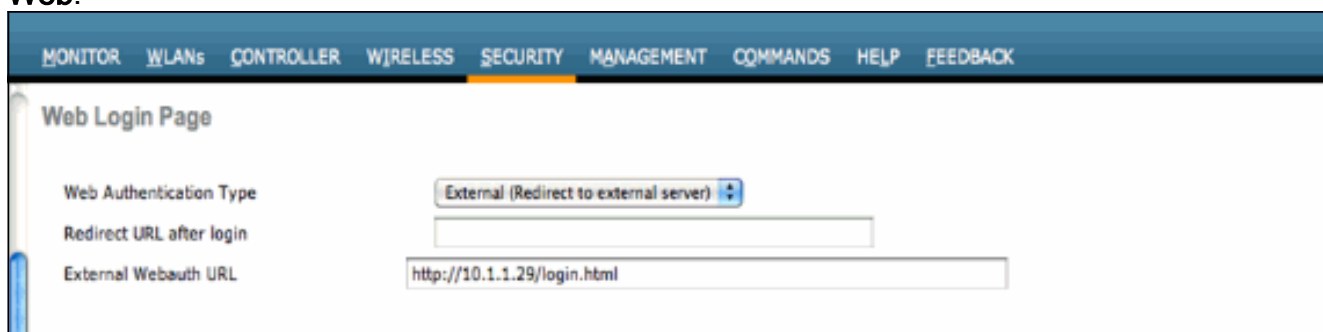


6. Las ACL Flex de Web Authentication y Web Pass-through también se pueden aplicar en la WLAN. Para hacer esto, elija la ACL en el menú desplegable **WebAuth FlexACL** bajo la pestaña Layer 3 en WLAN > Security.



7. Para la autenticación Web externa, es necesario definir la dirección URL de redirección. Esto se puede hacer a nivel global o a nivel de WLAN. Para el nivel WLAN, haga clic en la marca de verificación **Over-ride Global Config** e inserte la URL. A nivel global, vaya a **Seguridad > Autenticación Web > Página de inicio de sesión**

Web:



Limitaciones: La autenticación web (interna o a un servidor externo) requiere que el punto de acceso flexible esté en modo conectado. La autenticación web no se soporta si Flex AP está en modo autónomo. La autenticación Web (interna o a un servidor externo) sólo se admite

con la autenticación central. Si se configura una WLAN configurada para la conmutación local para la autenticación local, no puede realizar la autenticación Web. Todo el redireccionamiento web se realiza en el WLC y no en el nivel AP.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)