

Autenticación del Web externa con el Guía de despliegue del Local Switching de FlexConnect

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[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

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico sobre el (APS) de la arquitectura y de los Puntos de acceso de FlexConnect
- Conocimiento en cómo configurar y configurar a un servidor Web externo
- Conocimiento en cómo configurar y configurar el DHCP y a los servidores DNS

Componentes Utilizados

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

- El regulador del Wireless LAN del Cisco 7500 (WLC) ese funciona con la versión de firmware 7.2.110.0
- Lightweight Access Point de las Cisco 3500 Series (REVESTIMIENTO)
- Servidor Web externo que recibe la página de registro de la autenticación Web
- DNS y servidores DHCP en el sitio local para el address resolution y la asignación de IP Address 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. Aunque un WLC de las 7500 Series se utilice para este Guía de despliegue, esta característica se soporta en 2500, 5500, y el WLCs WiSM-2. 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 Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

Descripción general de características

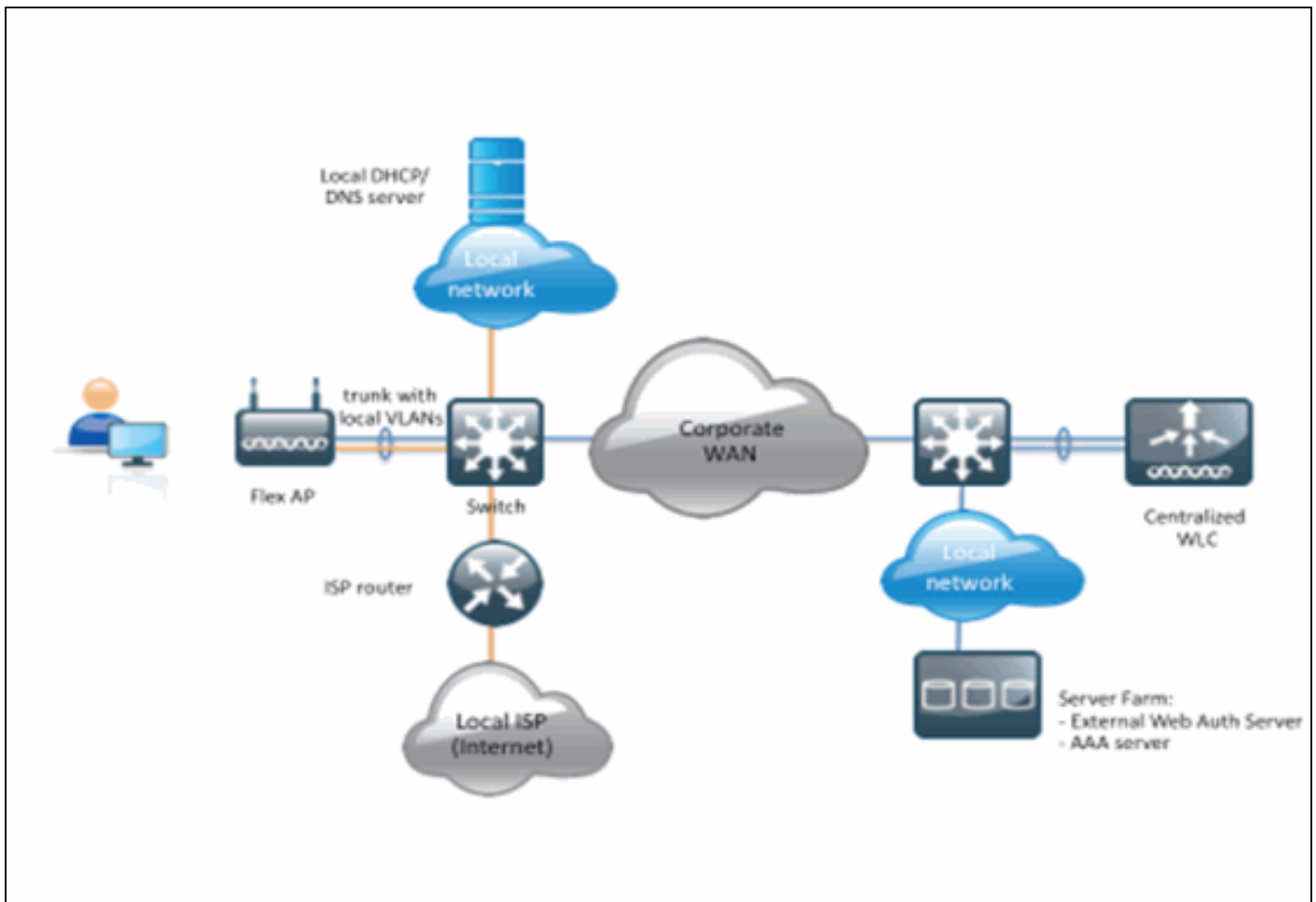
Esta característica amplía la capacidad de realizar la autenticación Web a un servidor Web externo del AP en el modo de FlexConnect, para los WLAN con localmente el tráfico conmutado (FlexConnect – Local Switching). Antes de que la versión 7.2.110.0 del WLC, la autenticación Web a un servidor externo fuera soportada para los AP en el modo local o el modo de FlexConnect para los WLAN con centralmente el tráfico conmutado (FlexConnect – transferencia central).

Designado a menudo la autenticación del Web externa, esta característica amplía la capacidad para que la red inalámbrica (WLAN) del Local Switching de FlexConnect soporte toda la red de la capa 3 reorienta los tipos de la Seguridad proporcionados actualmente por el regulador:

- Autenticación Web
- Paso de la red
- La red condicional reorienta
- La página del chapoteo condicional reorienta

En vista de que una red inalámbrica (WLAN) configurada para la autenticación Web y para el Local Switching, la lógica detrás de esta característica es distribuir y aplicar la lista de control de acceso (ACL) de FlexConnect de la PRE-autenticación directamente en el nivel AP en vez del WLC llano. De esta manera, el AP conmutará los paquetes que vienen del cliente de red inalámbrica que son permitidos por el ACL, localmente. Los paquetes no permitidos todavía se envían sobre el túnel CAPWAP al WLC. Por otra parte, cuando el AP recibe el tráfico sobre la interfaz atada con alambre, si es permitido por el ACL, lo remitirá al cliente de red inalámbrica. De no ser así, el paquete se pierde. Una vez que autentican y se autorizan al cliente, se quita la PRE-autenticación FlexConnect ACL, y todo el tráfico de datos del cliente se permite y se conmuta localmente.

Note: Esta característica trabaja bajo suposición que el cliente puede alcanzar al servidor externo del VLA N localmente conmutado.



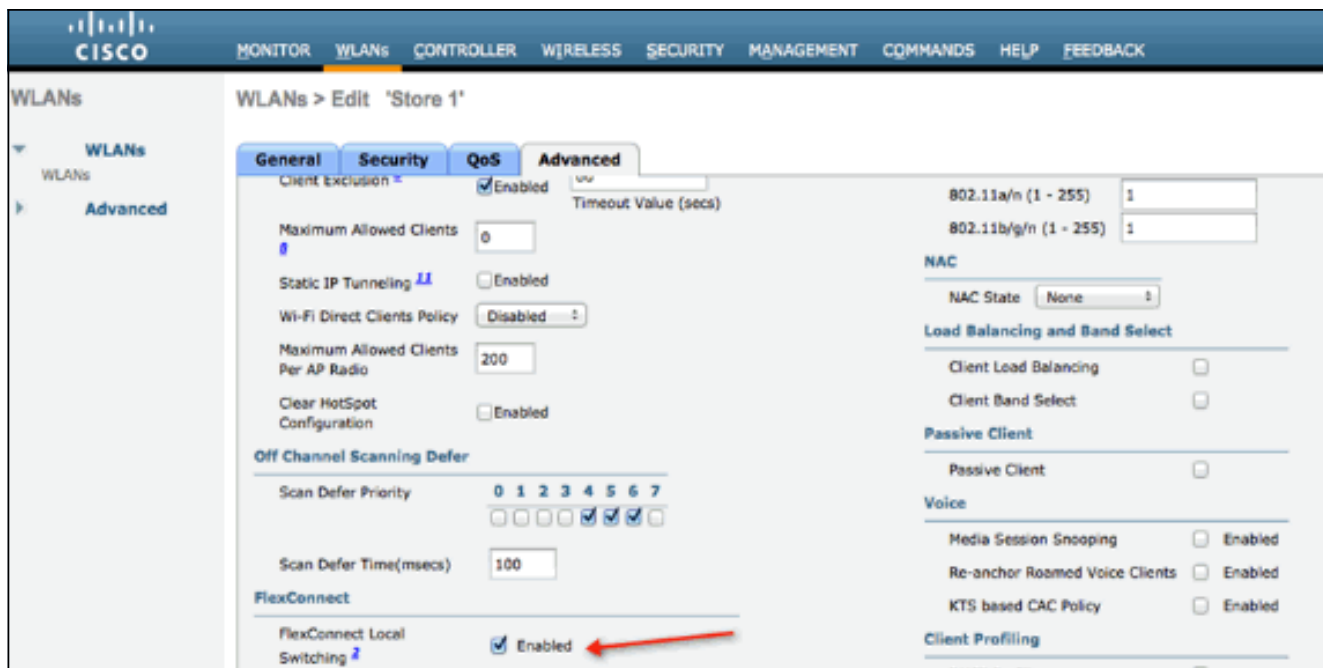
Resumen

- red inalámbrica (WLAN) configurada para el Local Switching de FlexConnect y la Seguridad L3
- FlexConnect ACL será utilizado como PRE-autenticación ACL
- FlexConnect ACL configurado una vez se debe avanzar a la base de datos AP vía el grupo de la flexión o vía el AP individual, o se puede aplicar en la red inalámbrica (WLAN)
- El AP permite todo el tráfico que hace juego la PRE-autenticación ACL que se conmutará localmente

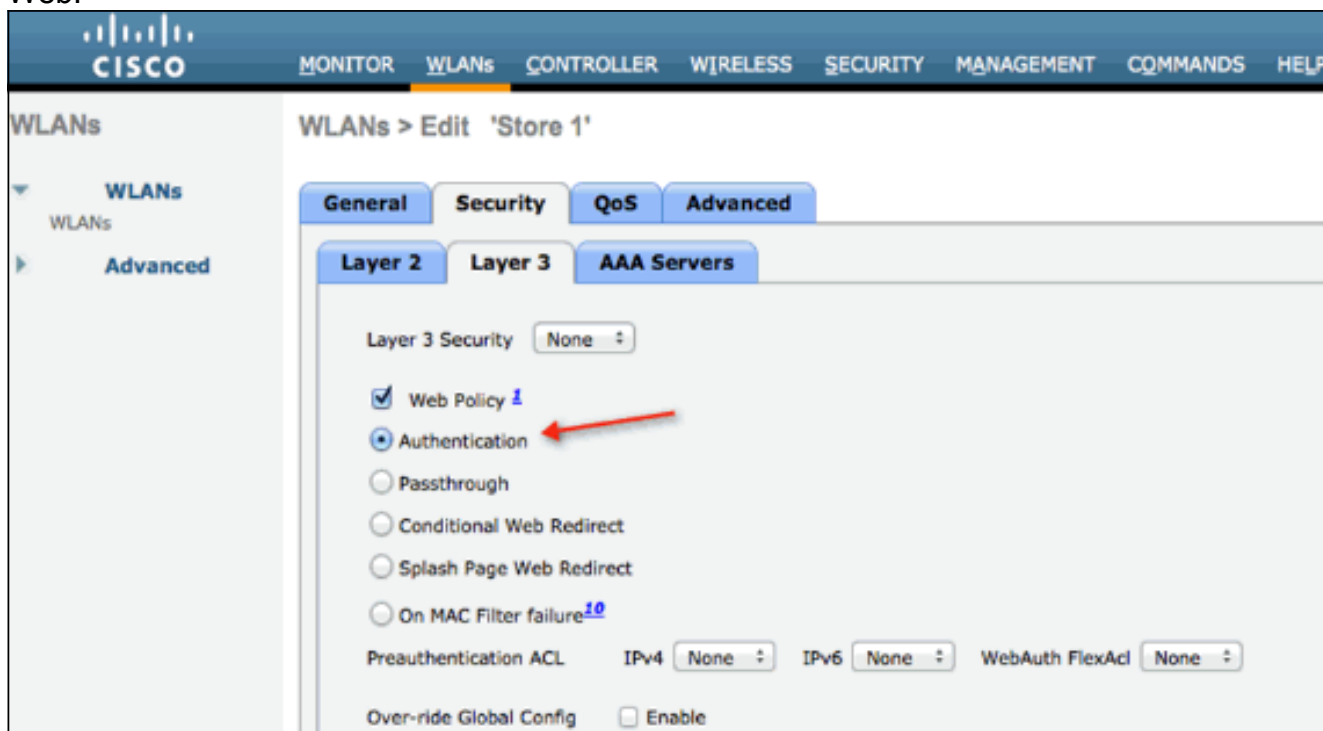
Procedimiento:

Complete estos pasos para configurar esta característica:

1. Configure una red inalámbrica (WLAN) para el Local Switching de FlexConnect.



2. Para habilitar la autenticación del Web externa, usted necesita configurar la directiva de la red como la política de seguridad para la red inalámbrica (WLAN) localmente conmutada. Esto incluye una de estas cuatro opciones: Autenticación Paso La red condicional reorienta La red de la página del chapoteo reorienta Este documentos contiene un ejemplo para la autenticación Web:



Los primeros dos métodos son similares y se pueden agrupar como métodos de autenticación Web desde un punto de vista de la configuración. Los segundos dos (condicional reorienta y página del chapoteo) son directivas de la red y se pueden agrupar como métodos de la Red-directiva.

3. La PRE-autenticación FlexConnect ACL necesita ser configurada permitiendo que los clientes de red inalámbrica alcancen la dirección IP del servidor externo. El tráfico ARP, del DHCP y DNS se permite y no necesita automáticamente ser especificado. Conforme a la Seguridad > a la lista de control de acceso, elija **FlexConnect ACL**. Entonces, el tecleo **agrega** y define los nombres y las reglas como regulador normal

ACL.

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

Note: Usted necesitará crear las reglas reversas para el tráfico cada vez.

4. Una vez que se crea FlexConnect ACL debe ser aplicado que se puede hacer en diversos niveles: AP, grupo de FlexConnect y red inalámbrica (WLAN). Esta última opción (flexión ACL en la red inalámbrica (WLAN)) está solamente para el paso de la autenticación Web y de la red para otros dos métodos bajo directiva de la red, tal como condicional y chapoteo reorienta. Los ACL pueden ser aplicados en el AP o doblar solamente al grupo. Aquí está un ejemplo de un ACL asignado en el nivel AP. Va a la **Tecnología inalámbrica > el AP selecto**, después hace clic la lengüeta de

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 el link de **WebAuthentication ACL del externo**. Entonces, elija el ACL para el ID de WLAN determinado:

The screenshot shows the Cisco Wireless configuration interface for an AP (3600I.0418). The main heading is "All APs > 3600I.0418 > ACL Mappings".

AP Information:

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

WLAN ACL Mapping:

- WLAN Id: 0
- WebAuth ACL: AP-flex-ACL
- Buttons: Add

WLAN Table:

WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	AP-flex-ACL

A red arrow points to the dropdown menu in the "WebAuth ACL" column of the table row with WLAN Id 1.

WebPolicies:

- WebPolicy ACL: AP-flex-ACL
- Buttons: Add

WebPolicy Access Control Lists:

Semejantemente, para la directiva ACL de la red (por ejemplo, el condicionales reorientan o la página del chapoteo reorienta), usted recibirá una opción para seleccionar la flexión conecta el ACL bajo WebPolicies después de que usted haga clic el mismo link de WebAuthentication ACL del externo. Esto se muestra aquí:

The screenshot shows the Cisco Wireless configuration interface for an AP named 3600I.0418. The page is titled "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", "802.11a/n", "802.11b/g/n", "Media Stream", "Country", "Timers", and "QoS". The main content area is divided into several sections:

- WLAN ACL Mapping:** Contains a "WLAN Id" field with the value "0" and a "WebAuth ACL" dropdown menu set to "AP-flex-ACL". There is an "Add" button below it.
- Table:** A table with columns "WLAN Id", "WLAN Profile Name", and "WebAuth ACL". It contains one row with "1" in the first column, "flex" in the second, and "AP-flex-ACL" in the third.
- WebPolicies:** Contains a "WebPolicy ACL" dropdown menu set to "AP-flex-ACL" and an "Add" button below it. A red arrow points to this dropdown menu.

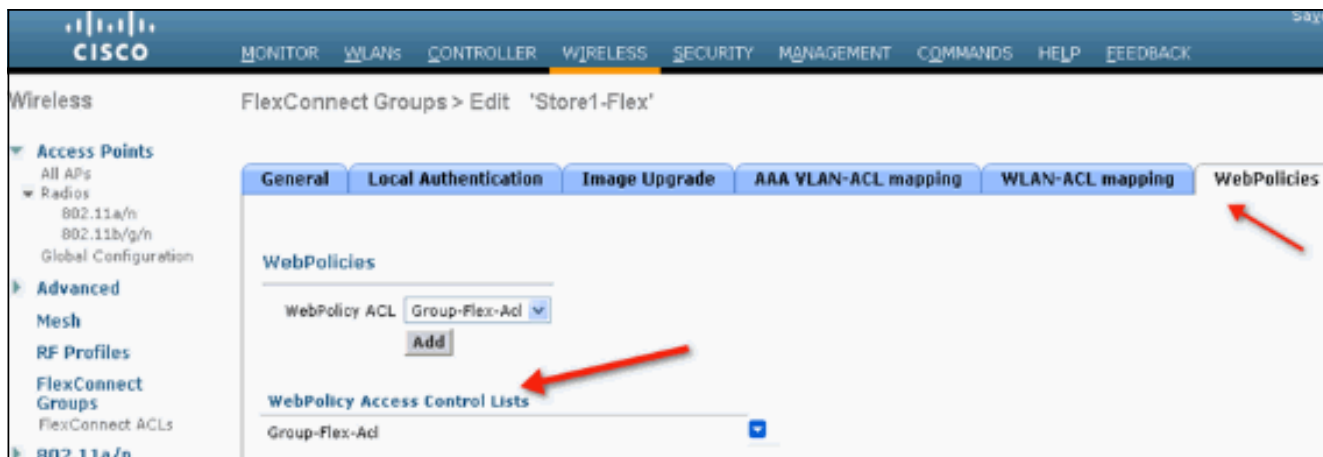
At the bottom of the page, there is a link for "WebPolicy Access Control Lists".

5. El ACL puede también ser aplicado en el nivel de grupo de FlexConnect. Para hacer esto, vaya a la lengüeta de la **asignación WLAN-ACL** en la configuración de grupo de FlexConnect. Entonces, elija el ID de WLAN y el ACL que usted quiere aplicarse. Haga clic en Add (Agregar). Esto es útil cuando usted quiere definir un ACL para un grupo de AP.

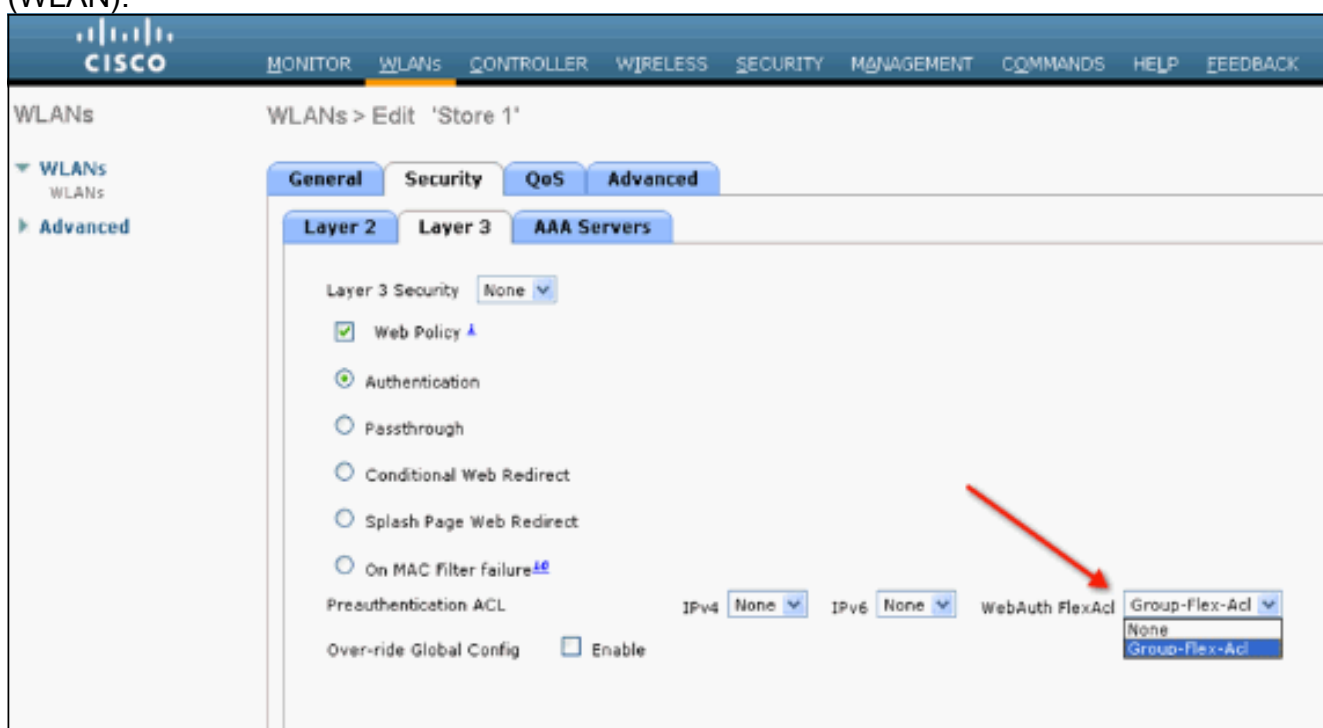
The screenshot shows the Cisco Wireless configuration interface for a FlexConnect Group named "Store1-Flex". The page is titled "FlexConnect Groups > Edit 'Store1-Flex'". The navigation menu on the left is similar to the previous screenshot. The main content area has several tabs: "General", "Local Authentication", "Image Upgrade", "VLAN-ACL mapping", "WLAN-ACL mapping", and "WebPolicies". The "WLAN-ACL mapping" tab is selected, and a red arrow points to it. The content under this tab is:

- WLAN ACL Mapping:** Contains a "WLAN Id" field with the value "0" and a "WebAuth ACL" dropdown menu set to "AP-flex-ACL". There is an "Add" button below it.
- Table:** A table with columns "WLAN Id", "WLAN Profile Name", and "WebAuth ACL". It contains one row with "1" in the first column, "flex" in the second, and "Group-flex-ACL" in the third. A red arrow points to the "WebAuth ACL" dropdown menu in this row.

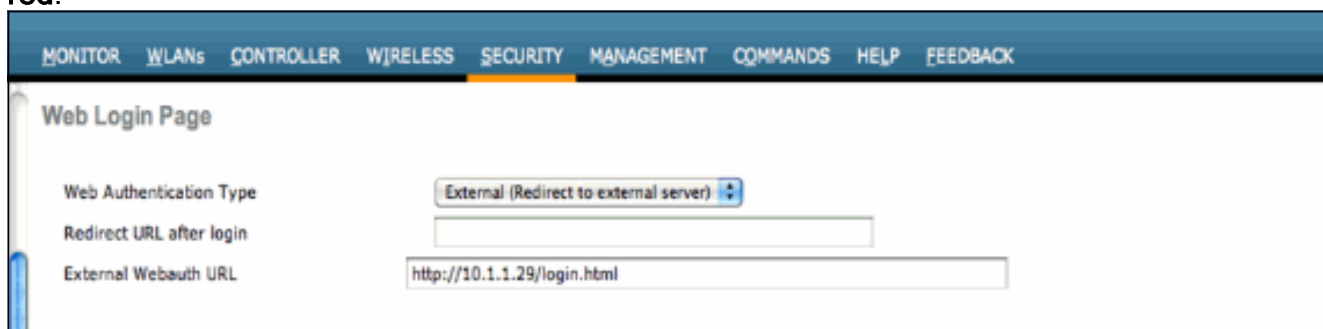
Semejantemente, porque la directiva ACL de la red (para la red condicional y del chapoteo de la página reorienta), usted necesita seleccionar la lengüeta de **WebPolicies**.



6. La flexión ACL del paso de la autenticación Web y de la red se puede también aplicar en la red inalámbrica (WLAN). Para hacer esto, elija el ACL del descenso-abajo de **WebAuth FlexACL** bajo lengüeta de la capa 3 en el > Security (Seguridad) de la red inalámbrica (WLAN).



7. Para la autenticación del Web externa, la reorientación URL necesita ser definida. Esto se puede hacer en un nivel global o en el nivel de la red inalámbrica (WLAN). Para el nivel de la red inalámbrica (WLAN), haga clic la marca de cotejo de la **configuración global de la invalidación** e inserte el URL. En el nivel global, vaya al **auth de la Seguridad > de la red > a la página de registro de la red:**



Limitaciones:La autenticación Web (interna o a un servidor externo) requiere la flexión AP estar en el modo conectado. La autenticación Web no se soporta si la flexión AP está en el

modo autónomo. La autenticación Web (interna o a un servidor externo) se soporta solamente con la autenticación central. Si una red inalámbrica (WLAN) configurada para el Local Switching se configura para la autenticación local, usted no puede realizar la autenticación Web. Todo el cambio de dirección de la red se realiza en el WLC y no en el nivel AP.

Información Relacionada

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