

# Guia de implantação de autenticação da Web externa com switching local FlexConnect

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Visão geral do recurso](#)

[Informações Relacionadas](#)

## Introduction

Este documento explica como usar um servidor web externo com switching local FlexConnect para políticas de web diferentes.

## Prerequisites

## Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico sobre a arquitetura e os access points (APs) FlexConnect
- Conhecimento sobre como configurar e configurar um servidor Web externo
- Conhecimento sobre como configurar e configurar servidores DHCP e DNS

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 7500 Wireless LAN Controller (WLC) que executa o firmware versão 7.2.110.0
- Access Point (LAP) Lightweight Cisco 3500 Series
- Servidor Web externo que hospeda a página de login da autenticação da Web
- Servidores DNS e DHCP no local para resolução de endereços e alocação de endereços IP para clientes sem fio

The information in this document was created from the devices in a specific lab environment. Embora uma WLC 7500 Series seja usada para este guia de implantação, esse recurso é suportado nas WLCs 2500, 5500 e 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.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

## Visão geral do recurso

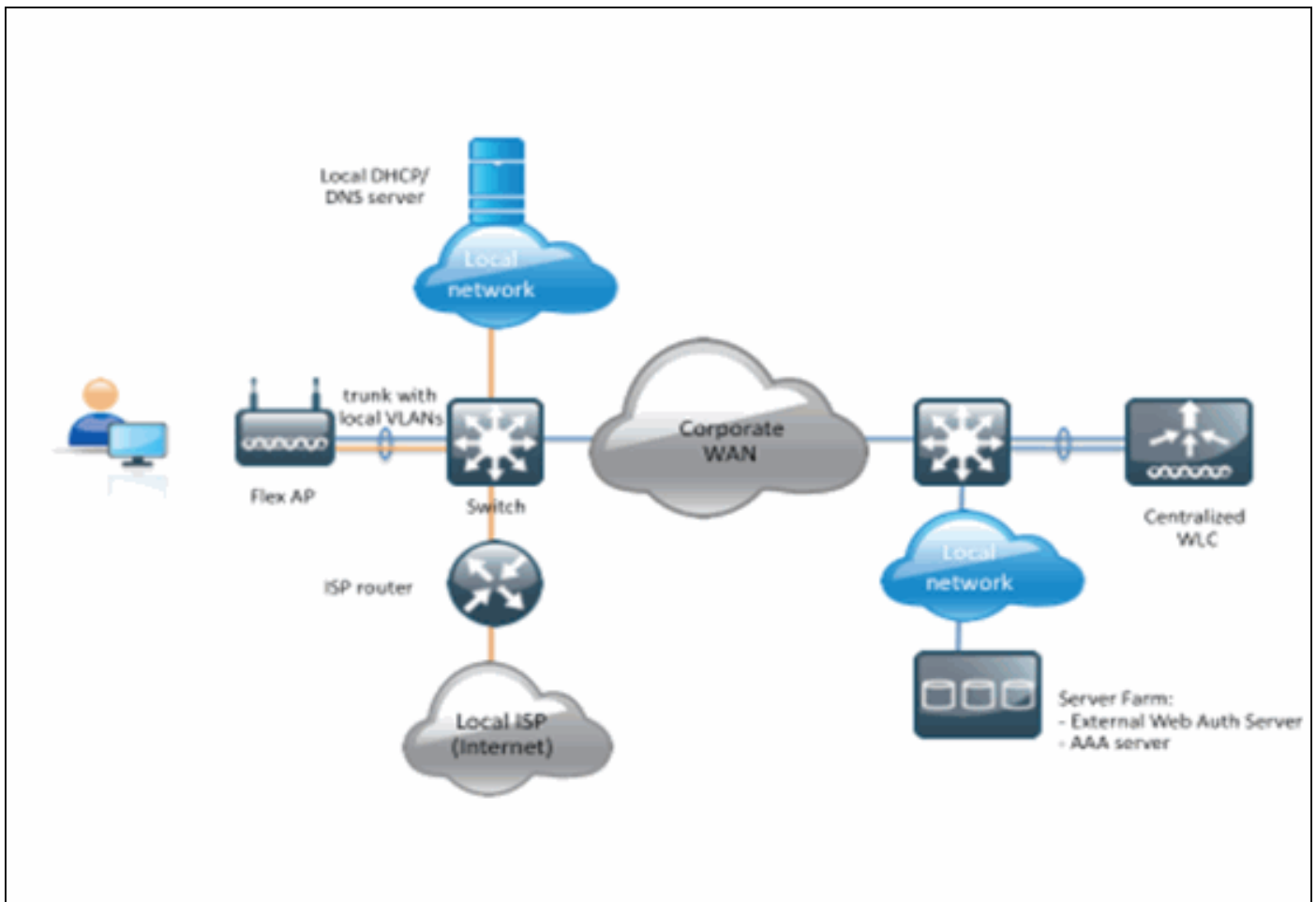
Esse recurso estende a capacidade de executar a autenticação da Web para um servidor Web externo a partir do AP no modo FlexConnect, para as WLANs com tráfego comutado localmente (FlexConnect - Switching local). Antes do WLC Versão 7.2.110.0, a Autenticação da Web para um servidor externo era suportada para APs no modo Local ou no modo FlexConnect para WLANs com tráfego comutado centralmente (FlexConnect - Central Switching).

Frequentemente conhecido como Autenticação externa da Web, esse recurso amplia a capacidade da WLAN de switching local do FlexConnect para suportar todos os tipos de segurança de redirecionamento da Web de Camada 3 fornecidos atualmente pelo controlador:

- Autenticação da Web
- Passagem da Web
- Redirecionamento condicional da Web
- Redirecionamento Condicional da Página de Apresentação

Considerando uma WLAN configurada para autenticação da Web e para switching local, a lógica por trás desse recurso é distribuir e aplicar a ACL (Pre-Authentication FlexConnect Access Control List) diretamente no nível do AP em vez do nível do WLC. Dessa forma, o AP irá comutar localmente os pacotes provenientes do cliente sem fio permitidos pela ACL. Os pacotes não permitidos ainda são enviados pelo túnel CAPWAP para a WLC. Por outro lado, quando o AP recebe o tráfego sobre a interface com fio, se permitido pela ACL, ele o encaminha para o cliente sem fio. Caso contrário, o pacote será perdido. Quando o cliente é autenticado e autorizado, a ACL FlexConnect de pré-autenticação é removida e todo o tráfego de dados do cliente é permitido e comutado localmente.

**Observação:** esse recurso funciona sob o pressuposto de que o cliente pode acessar o servidor externo a partir da VLAN comutada localmente.



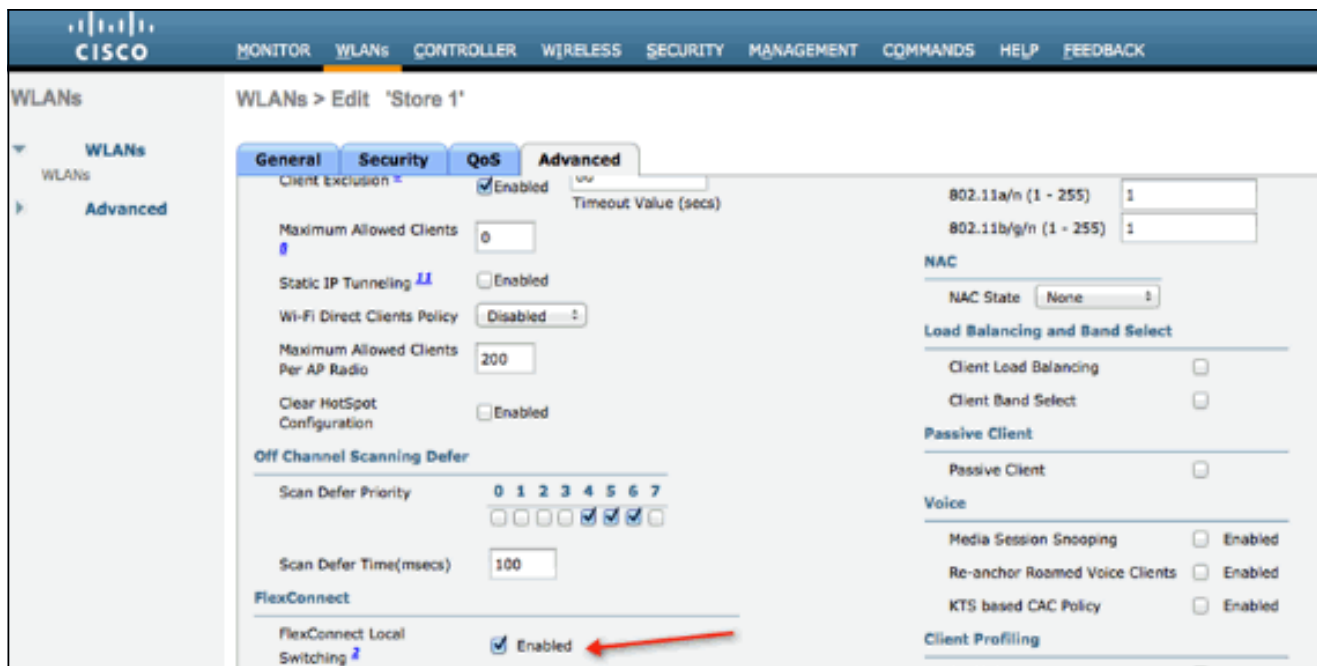
## Resumo:

- WLAN configurada para switching local FlexConnect e segurança L3
- As ACLs FlexConnect serão usadas como ACLs de pré-autenticação
- Depois de configuradas as ACLs FlexConnect devem ser enviadas para o banco de dados de AP por meio do Flex Group ou por meio do AP Individual, ou podem ser aplicadas na WLAN
- O AP permite que todo o tráfego que corresponde à ACL de pré-autenticação seja comutado localmente

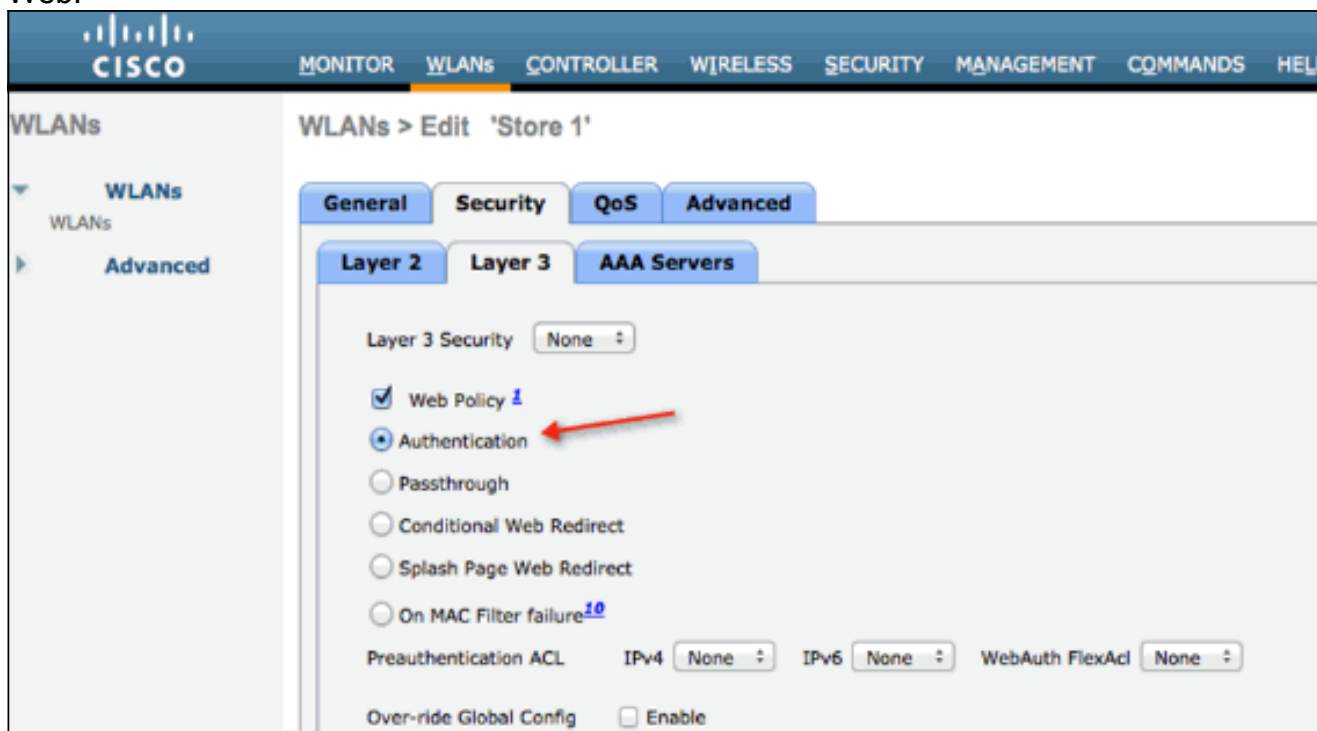
## Procedimento:

Conclua estes passos para configurar este recurso:

1. Configure uma WLAN para o FlexConnect Local Switching.



2. Para habilitar a Autenticação da Web externa, você precisa configurar a Política da Web como a política de segurança para a WLAN comutada localmente. Isso inclui uma destas quatro opções: Autenticação Passagem Redirecionamento condicional da Web Redirecionamento da Web da página inicial Este documento captura um exemplo de Autenticação da Web:



Os dois primeiros métodos são semelhantes e podem ser agrupados como métodos de autenticação da Web do ponto de vista da configuração. Os dois segundos (Redirecionamento condicional e Página inicial) são Políticas da Web e podem ser agrupados como métodos de Política da Web.

3. A ACL FlexConnect de pré-autenticação precisa ser configurada, permitindo que os clientes sem fio acessem o endereço IP do servidor externo. O tráfego ARP, DHCP e DNS são permitidos automaticamente e não precisam ser especificados. Em Security > Access Control List, escolha **FlexConnect ACLs**. Em seguida, clique em **Adicionar** e defina os nomes e as regras como uma 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

**Note:** Você precisará criar regras reversas para o tráfego cada vez.

4. Uma vez criadas as ACLs FlexConnect, elas devem ser aplicadas, o que pode ser feito em níveis diferentes: AP, Grupo FlexConnect e WLAN. Esta última opção (Flex ACL na WLAN) é somente para autenticação da Web e passagem da Web para outros dois métodos em Política da Web, como Condicional e Redirecionamento de abertura. As ACLs só podem ser aplicadas no AP ou no Grupo Flex. Aqui está um exemplo de uma ACL atribuída no nível do AP. Vá para **Sem fio > selecione AP** e clique na guia

**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**

Clique no link **External Web Authentication ACLs** (ACLs externas de autenticação da Web). Em seguida, escolha a ACL para a ID de WLAN específica:

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HE

Wireless All APs > 3600I.0418 > ACL Mappings

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

**WLAN ACL Mapping**

WLAN Id 0  
WebAuth ACL AP-flex-ACL  
Add

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

**WebPolicies**

WebPolicy ACL AP-flex-ACL  
Add

WebPolicy Access Control Lists

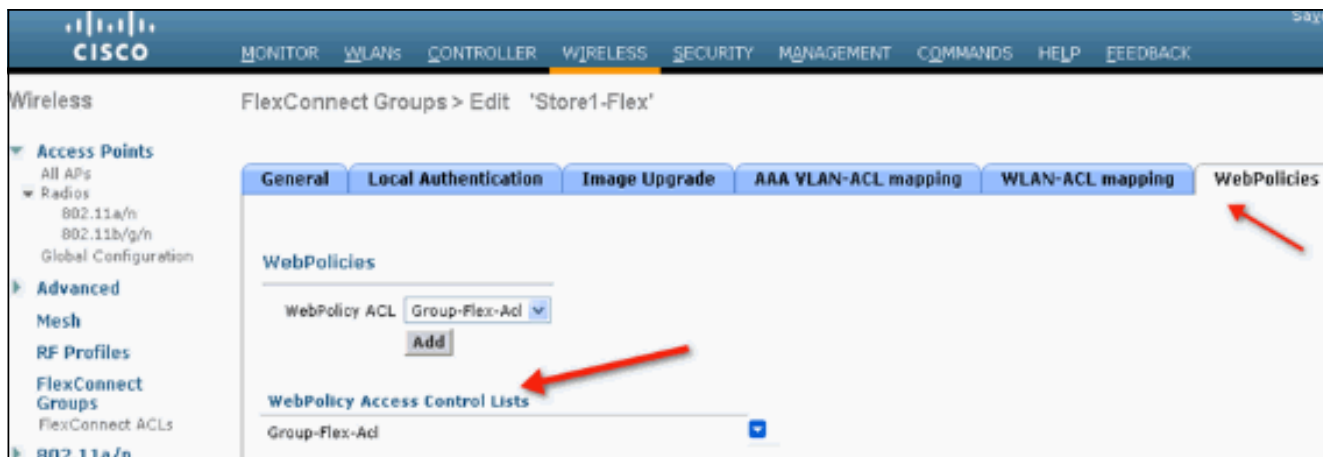
Da mesma forma, para a ACL de política da Web (por exemplo, redirecionamento condicional ou redirecionamento de página inicial), você receberá uma opção para selecionar a ACL do Flex Connect em WebPolicies depois de clicar no mesmo link External WebAuthentication ACLs. Isso é mostrado aqui:

The screenshot shows the Cisco Wireless configuration interface for an AP. The breadcrumb trail is 'All APs > 3600I.0418 > ACL Mappings'. On the left, there is a navigation menu with options 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 sections: 'WLAN ACL Mapping' and 'WebPolicies'. In the 'WLAN ACL Mapping' section, there is a 'WLAN Id' field with '0' and a 'WebAuth ACL' dropdown set to 'AP-flex-ACL'. Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. The table contains one entry: '1' for WLAN Id, 'flex' for WLAN Profile Name, and 'AP-flex-ACL' for WebAuth ACL. In the 'WebPolicies' section, there is a 'WebPolicy ACL' dropdown set to 'AP-flex-ACL' and an 'Add' button. A red arrow points to the 'WebPolicy ACL' dropdown.

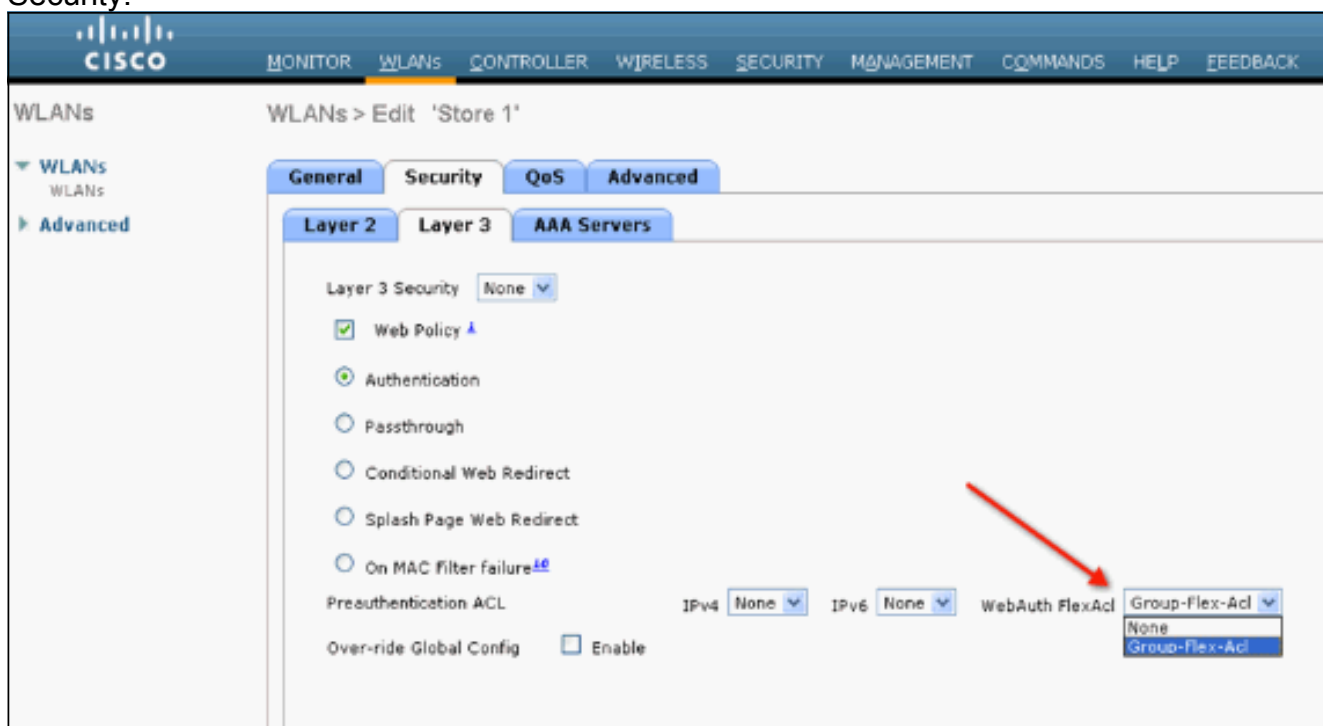
5. A ACL também pode ser aplicada no nível do grupo FlexConnect. Para fazer isso, acesse a guia **WLAN-ACL mapping** na configuração do grupo FlexConnect. Em seguida, escolha a ID da WLAN e a ACL que deseja aplicar. Clique em Add. Isso é útil quando você deseja definir uma ACL para um grupo de APs.

The screenshot shows the Cisco Wireless configuration interface for a FlexConnect Group. The breadcrumb trail is 'FlexConnect Groups > Edit "Store1-Flex"'. The page has several tabs: 'General', 'Local Authentication', 'Image Upgrade', 'VLAN-ACL mapping', 'WLAN-ACL mapping', and 'WebPolicies'. The 'WLAN-ACL mapping' tab is selected. In this tab, there is a 'WLAN ACL Mapping' section with a 'WLAN Id' field with '0' and a 'WebAuth ACL' dropdown set to 'AP-flex-ACL'. Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. The table contains one entry: '1' for WLAN Id, 'flex' for WLAN Profile Name, and 'Group-flex-ACL' for WebAuth ACL. A red arrow points to the 'WLAN-ACL mapping' tab, and another red arrow points to the 'WebAuth ACL' dropdown.

Da mesma forma, para a ACL de política da Web (para o Redirecionamento da Web de página condicional e de abertura), você precisa selecionar a guia **Web Policies**.

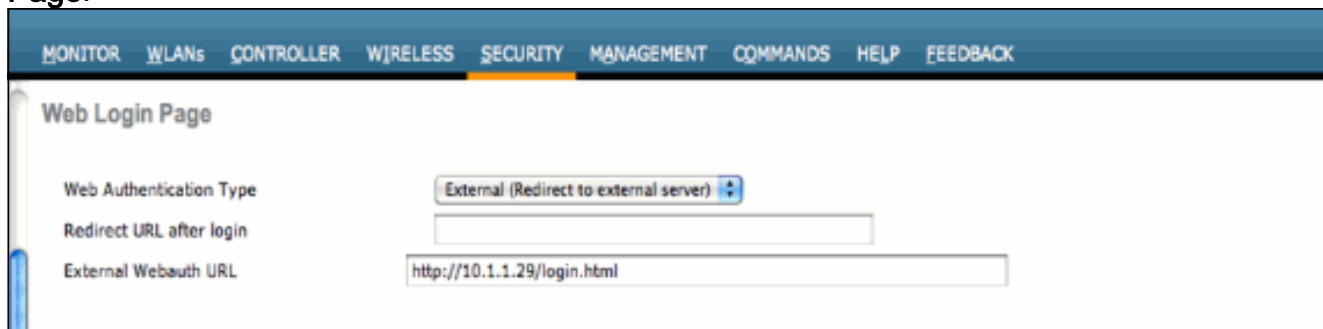


6. A autenticação da Web e as ACLs flexíveis de passagem da Web também podem ser aplicadas na WLAN. Para fazer isso, escolha a ACL na lista suspensa **WebAuth FlexACL** na guia Layer 3 em WLAN > Security.



7. Para a Autenticação da Web externa, o URL de redirecionamento precisa ser definido. Isso pode ser feito em um nível global ou no nível da WLAN. Para o nível de WLAN, clique na marca de seleção **Over-ride Global Config** e insira o URL. No nível global, vá para **Security > Web Auth > Web Login**

Page:



**Limitações:**A Autenticação da Web (interna ou para um servidor externo) exige que o AP Flex esteja no modo Conectado. A autenticação da Web não é suportada se o AP Flex estiver no modo independente.A autenticação da Web (interna ou para um servidor externo)



só é suportada com a autenticação central. Se uma WLAN configurada para comutação local estiver configurada para Autenticação local, você não poderá executar a Autenticação da Web. Todo o redirecionamento da Web é realizado na WLC e não no nível do AP.

## Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)