

# Externe Webauthentifizierung mit FlexConnect Local Switching - Bereitstellungsleitfaden

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Übersicht der Funktionen](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird die Verwendung eines externen Webservers mit FlexConnect Local Switching für verschiedene Web-Richtlinien erläutert.

## Voraussetzungen

### Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundlegendes Wissen über die FlexConnect-Architektur und Access Points (APs)
- Kenntnisse zum Einrichten und Konfigurieren eines externen Webservers
- Kenntnisse zum Einrichten und Konfigurieren von DHCP- und DNS-Servern

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 7500 Wireless LAN Controller (WLC) mit Firmware-Version 7.2.110.0
- Cisco Lightweight Access Point (LAP) der Serie 3500
- Externer Webserver, der die Anmeldeseite für die Webauthentifizierung hostet
- DNS- und DHCP-Server am lokalen Standort für die Adressauflösung und die Zuweisung von IP-Adressen an Wireless-Clients

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Obwohl für diesen Bereitstellungsleitfaden ein WLC der Serie 7500 verwendet wird, wird diese Funktion von WLCs der Serien 2500, 5500 und WiSM-2 unterstützt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Übersicht der Funktionen

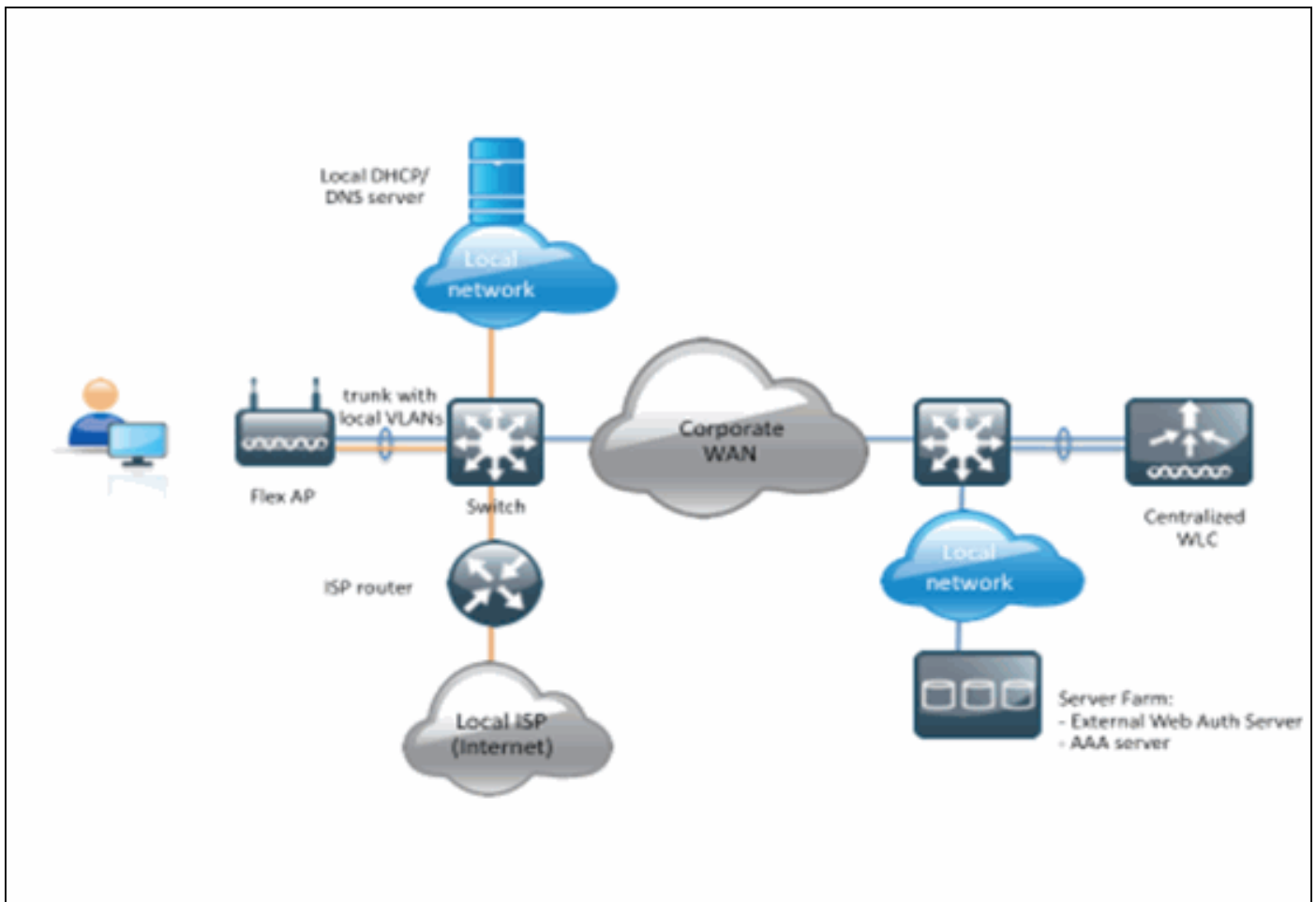
Diese Funktion erweitert die Möglichkeit zur Web-Authentifizierung auf einen externen Webserver vom Access Point im FlexConnect-Modus für WLANs mit lokalem Switched-Datenverkehr (FlexConnect - Local Switching). Vor der WLC-Version 7.2.110.0 wurde die Webauthentifizierung an einen externen Server für APs im Local-Modus oder im FlexConnect-Modus für WLANs mit zentralem Switched-Datenverkehr (FlexConnect - Central Switching) unterstützt.

Diese Funktion wird häufig als externe Webauthentifizierung bezeichnet und erweitert die Funktionalität für das FlexConnect Local Switching WLAN, um alle derzeit vom Controller bereitgestellten Sicherheitsarten für die Web-Umleitung auf Layer 3 zu unterstützen:

- Webauthentifizierung
- Web-Pass-Through
- Bedingte Webumleitung
- Bedingte Umleitung der Splash-Seite

Unter Berücksichtigung eines für die Webauthentifizierung und für lokales Switching konfigurierten WLAN besteht die Logik hinter dieser Funktion darin, die Pre-Authentication FlexConnect Access Control List (ACL) direkt auf der AP-Ebene anstatt auf der WLC-Ebene zu verteilen und anzuwenden. Auf diese Weise schaltet der Access Point die Pakete vom Wireless-Client, die von der ACL lokal zugelassen sind, um. Die nicht zulässigen Pakete werden weiterhin über den CAPWAP-Tunnel an den WLC gesendet. Wenn der Access Point jedoch den Datenverkehr über die kabelgebundene Schnittstelle empfängt (sofern dies durch die ACL zulässig ist), leitet er ihn an den Wireless-Client weiter. Andernfalls wird das Paket verworfen. Sobald der Client authentifiziert und autorisiert ist, wird die Pre-Authentication FlexConnect ACL entfernt, und der gesamte Datenverkehr des Clients wird zugelassen und lokal geschaltet.

**Hinweis:** Diese Funktion wird unter der Annahme verwendet, dass der Client den externen Server über das lokal geschaltete VLAN erreichen kann.



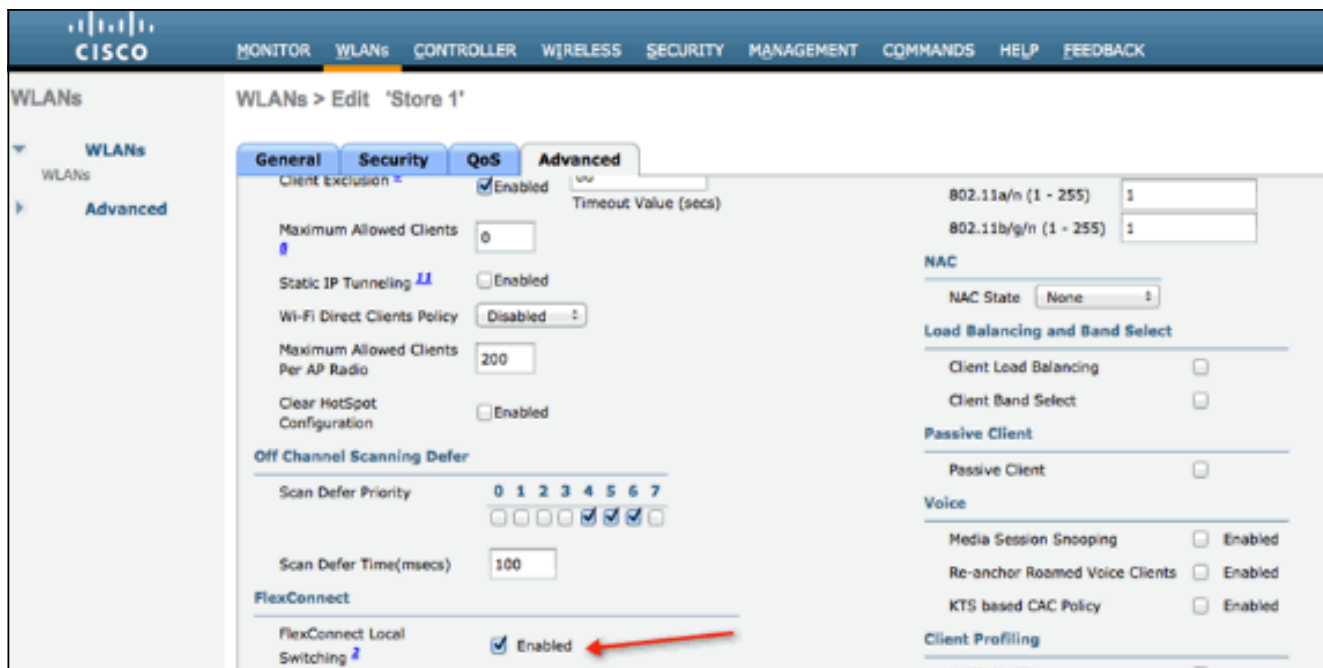
### Zusammenfassung:

- WLAN konfiguriert für FlexConnect Local Switching und L3 Security
- FlexConnect-ACLs werden als Pre-Authentication-ACLs verwendet.
- Nach der Konfiguration müssen FlexConnect-ACLs über Flex Group oder Individual AP in die AP-Datenbank übertragen werden oder können im WLAN angewendet werden.
- AP ermöglicht das lokale Umschalten des gesamten Datenverkehrs, der der Pre-Authentication ACL entspricht

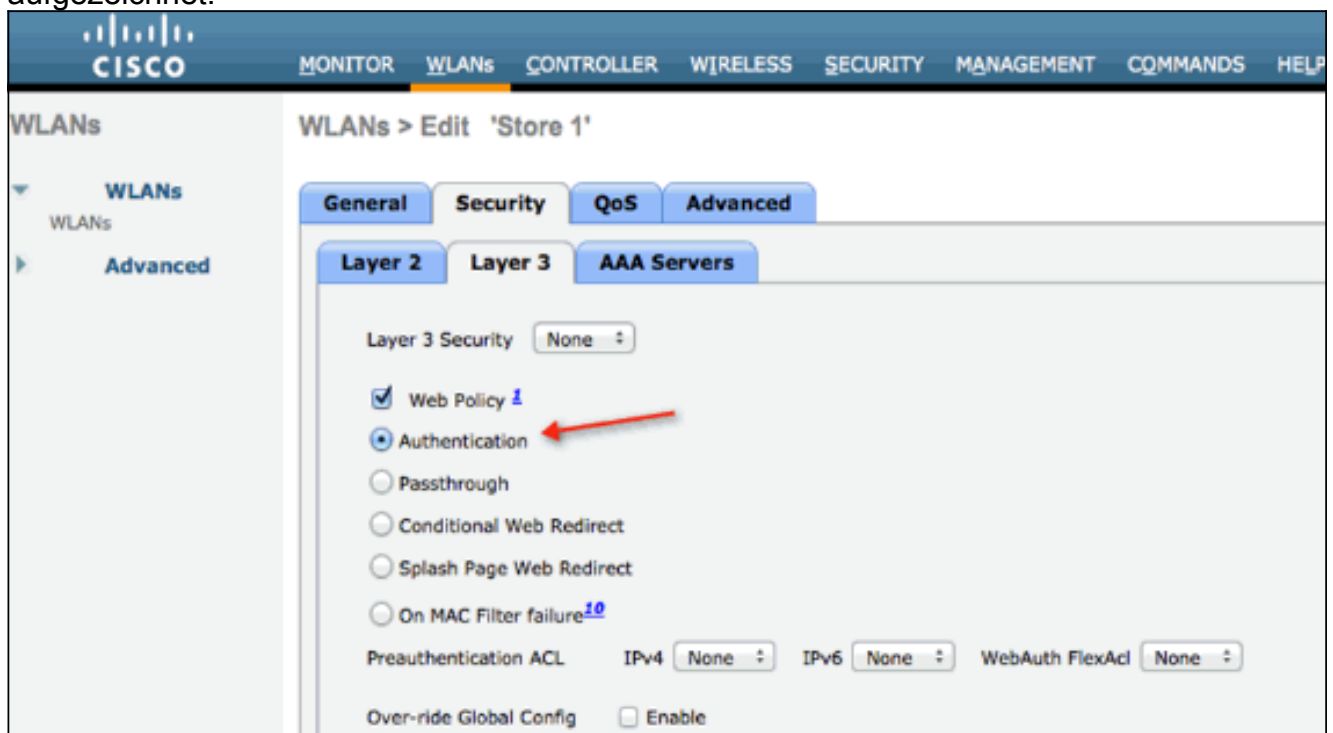
### Verfahren:

Gehen Sie wie folgt vor, um diese Funktion zu konfigurieren:

1. Konfigurieren eines WLAN für das lokale FlexConnect-Switching



2. Um die externe Webauthentifizierung zu aktivieren, müssen Sie die Webrichtlinie als Sicherheitsrichtlinie für das lokal geschaltete WLAN konfigurieren. Dazu gehören eine der folgenden vier Optionen: Authentifizierung, Passthrough, Bedingte Webumleitung, Splash Page, Webumleitung. In diesem Dokument wird ein Beispiel für die Webauthentifizierung aufgezeichnet:



Die ersten beiden Methoden sind ähnlich und können aus Konfigurationsperspektive als Web-Authentifizierungsmethoden gruppiert werden. Die beiden zweiten (Conditional Redirect and Splash Page) sind Webrichtlinien und können als Webrichtlinienmethoden gruppiert werden.

3. Die FlexConnect-ACL vor der Authentifizierung muss konfiguriert werden, damit die Wireless-Clients die IP-Adresse des externen Servers erreichen können. ARP-, DHCP- und DNS-Datenverkehr sind automatisch zulässig und müssen nicht angegeben werden. Wählen Sie unter Security > Access Control List (Sicherheit > Zugriffskontrollliste) die Option **FlexConnect ACLs aus**. Klicken Sie anschließend auf **Hinzufügen**, und definieren Sie die Namen und Regeln als normale Controller-

## 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

**Hinweis:** Sie müssen für den Datenverkehr jedes Mal umgekehrte Regeln erstellen.

4. Sobald FlexConnect-ACLs erstellt wurden, sollten sie angewendet werden, die auf verschiedenen Ebenen durchgeführt werden können: AP, FlexConnect Group und WLAN. Diese letzte Option (Flex ACL im WLAN) ist nur für die Webauthentifizierung und den Web-Pass-Through für die beiden anderen Methoden unter der Webrichtlinie (z. B. Conditional und Splash Redirect) vorgesehen. ACLs können nur auf die AP- oder Flex-Gruppe angewendet werden. Hier ein Beispiel für eine ACL, die auf AP-Ebene zugewiesen wurde. Gehen Sie zu **Wireless > wählen Sie AP** aus, und klicken Sie dann auf die Registerkarte **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**

Klicken Sie auf den Link **Externe Webauthentifizierungs-ACLs**. Wählen Sie anschließend die ACL für die jeweilige WLAN-ID aus:

**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    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](#)

Ebenso erhalten Sie für die Webrichtlinienzugriffskontrollliste (z. B. die bedingte Umleitung oder Splash-Seitenumleitung) die Option, die Flex Connect-Zugriffskontrollliste unter WebPolicies (Web-Richtlinien) auszuwählen, nachdem Sie auf denselben Link für externe WebAuthentication-Zugriffskontrolllisten geklickt haben. Hier sehen Sie:

**Wireless** All APs > 36001.0418 > 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** 36001.0418  
**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

**WebPolicies**

WebPolicy ACL

**WebPolicy Access Control Lists**

5. Die ACL kann auch auf FlexConnect-Gruppenebene angewendet werden. Gehen Sie dazu zur Registerkarte **WLAN-ACL-Zuordnung** in der FlexConnect Group-Konfiguration. Wählen Sie anschließend die WLAN-ID und die ACL aus, die Sie anwenden möchten. Klicken Sie auf **Hinzufügen**. Dies ist hilfreich, wenn Sie eine ACL für eine Gruppe von APs definieren möchten.

**Wireless** FlexConnect Groups > Edit 'Store1-Flex'

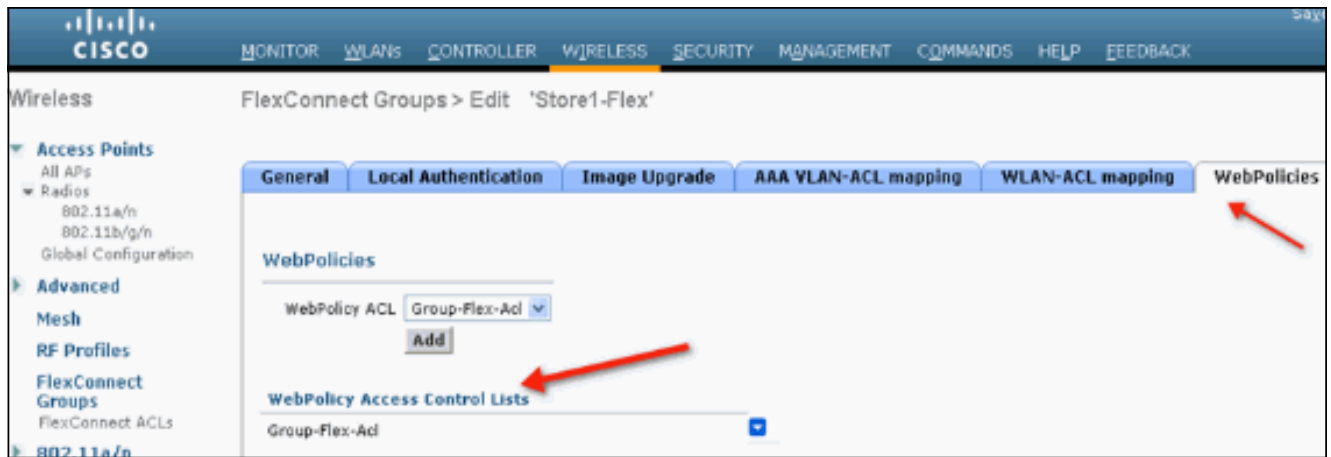
**General** **Local Authentication** **Image Upgrade** **VLAN-ACL mapping** **WLAN-ACL mapping** **WebPolicies**

**WLAN ACL Mapping**

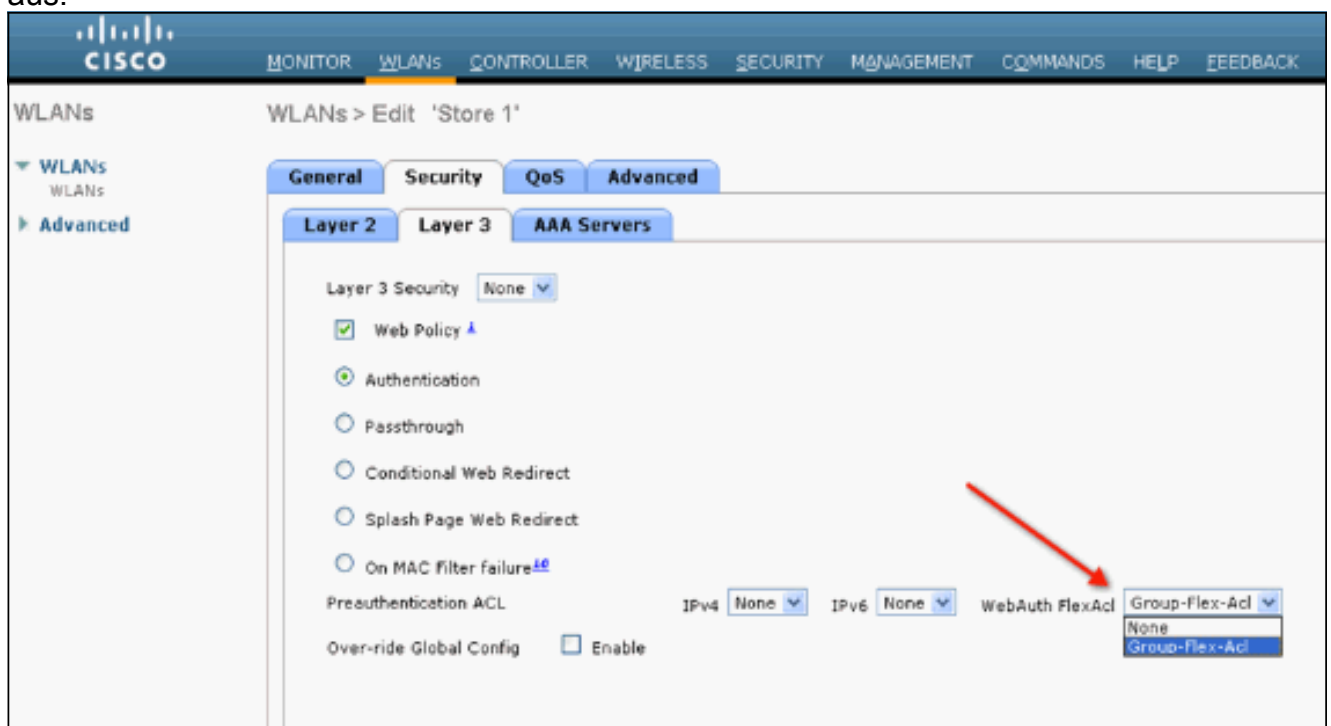
WLAN Id   
 WebAuth ACL

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

Ebenso müssen Sie für die Webrichtlinienzugriffskontrollliste (für die Web-Umleitung für Bedingung und Splash-Seite) die Registerkarte **WebPolicies** auswählen.



6. Web-Authentifizierung und Web-Pass-Through-Flex-ACLs können auch im WLAN angewendet werden. Wählen Sie dazu im Dropdown-Menü "WebAuth FlexACL" unter der Registerkarte "Layer 3" in WLAN > Security die ACL aus.



7. Für die externe Webauthentifizierung muss die Umleitungs-URL definiert werden. Dies kann auf globaler Ebene oder auf WLAN-Ebene erfolgen. Klicken Sie für die WLAN-Ebene auf das Kontrollkästchen **Globale Konfiguration außer Kraft setzen**, und fügen Sie die URL ein. Gehen Sie auf globaler Ebene zu **Security > Web Auth > Web Login**

Page:



**Einschränkungen:** Für die Webauthentifizierung (intern oder auf einem externen Server) muss sich der Flex AP im Connected-Modus befinden. Die Webauthentifizierung wird nicht unterstützt, wenn sich Flex AP im Standalone-Modus befindet. Die Webauthentifizierung



(intern oder auf einem externen Server) wird nur mit der zentralen Authentifizierung unterstützt. Wenn ein für lokales Switching konfiguriertes WLAN für die lokale Authentifizierung konfiguriert ist, können Sie keine Webauthentifizierung durchführen. Die gesamte Web-Umleitung erfolgt auf WLC-Ebene und nicht auf AP-Ebene.

## Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)