

Guida alla distribuzione dell'autenticazione Web esterna con switching locale FlexConnect

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Panoramica delle funzionalità](#)

[Informazioni correlate](#)

Introduzione

Questo documento spiega come utilizzare un server Web esterno con la commutazione locale FlexConnect per diversi criteri Web.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base dell'architettura FlexConnect e dei punti di accesso (AP)
- Informazioni su come configurare un server Web esterno
- Informazioni su come configurare i server DHCP e DNS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 7500 Wireless LAN Controller (WLC) con firmware versione 7.2.10.0
- Cisco serie 3500 Lightweight Access Point (LAP)
- Server Web esterno che ospita la pagina di accesso per l'autenticazione Web
- Server DNS e DHCP nel sito locale per la risoluzione degli indirizzi e l'allocazione degli indirizzi IP ai client wireless

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Sebbene per questa guida all'installazione venga utilizzato un WLC serie 7500, questa funzione è supportata sui WLC 2500, 5500 e WiSM-2. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Panoramica delle funzionalità

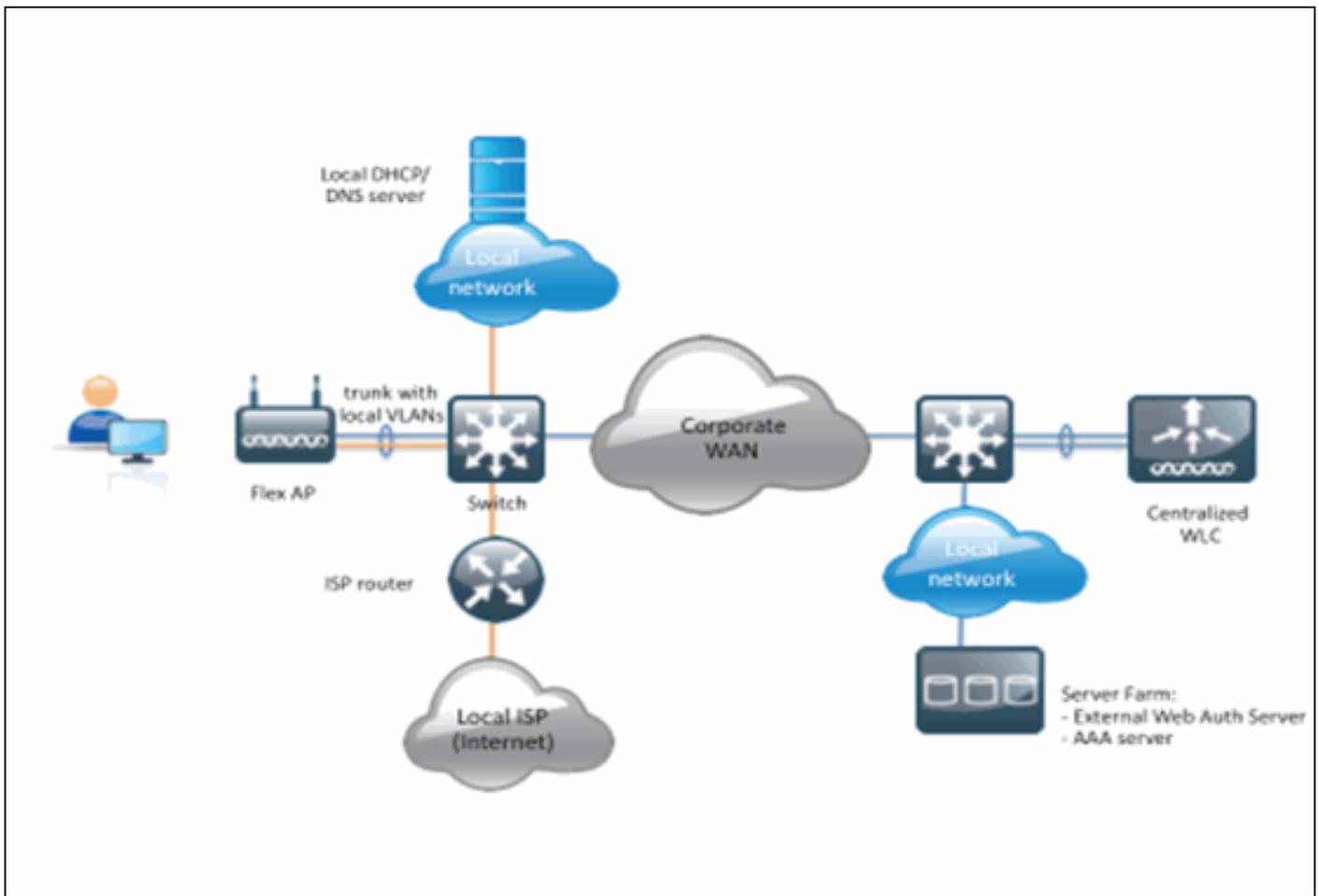
Questa funzionalità estende la funzionalità di autenticazione Web a un server Web esterno dall'access point in modalità FlexConnect, per le WLAN con traffico a commutazione locale (FlexConnect - Switching locale). Prima della versione 7.2.110.0 del WLC, l'autenticazione Web a un server esterno era supportata per i punti di accesso in modalità locale o in modalità FlexConnect per le WLAN con traffico a commutazione centrale (FlexConnect - Switching centrale).

Questa funzione, nota spesso come autenticazione Web esterna, estende la capacità della WLAN di switching locale FlexConnect di supportare tutti i tipi di sicurezza reindirizzamento Web di layer 3 attualmente forniti dal controller:

- Autenticazione Web
- Pass-through Web
- Reindirizzamento condizionale Web
- Reindirizzamento condizionale pagina iniziale

Se si prende in considerazione una WLAN configurata per l'autenticazione Web e per la commutazione locale, la logica alla base di questa funzionalità è la distribuzione e l'applicazione della lista di controllo dell'accesso (ACL) FlexConnect di preautenticazione direttamente a livello di access point anziché a livello di WLC. In questo modo, l'access point commuta localmente i pacchetti provenienti dal client wireless autorizzati dall'ACL. I pacchetti non consentiti vengono comunque inviati al WLC attraverso il tunnel CAPWAP. D'altra parte, quando l'access point riceve il traffico sull'interfaccia cablata, se autorizzato dall'ACL, lo inoltra al client wireless. In caso contrario, il pacchetto viene scartato. Dopo aver autenticato e autorizzato il client, l'ACL FlexConnect di preautenticazione viene rimosso e tutto il traffico di dati del client viene autorizzato e commutato localmente.

Nota: questa funzione si basa sul presupposto che il client possa raggiungere il server esterno dalla VLAN a commutazione locale.



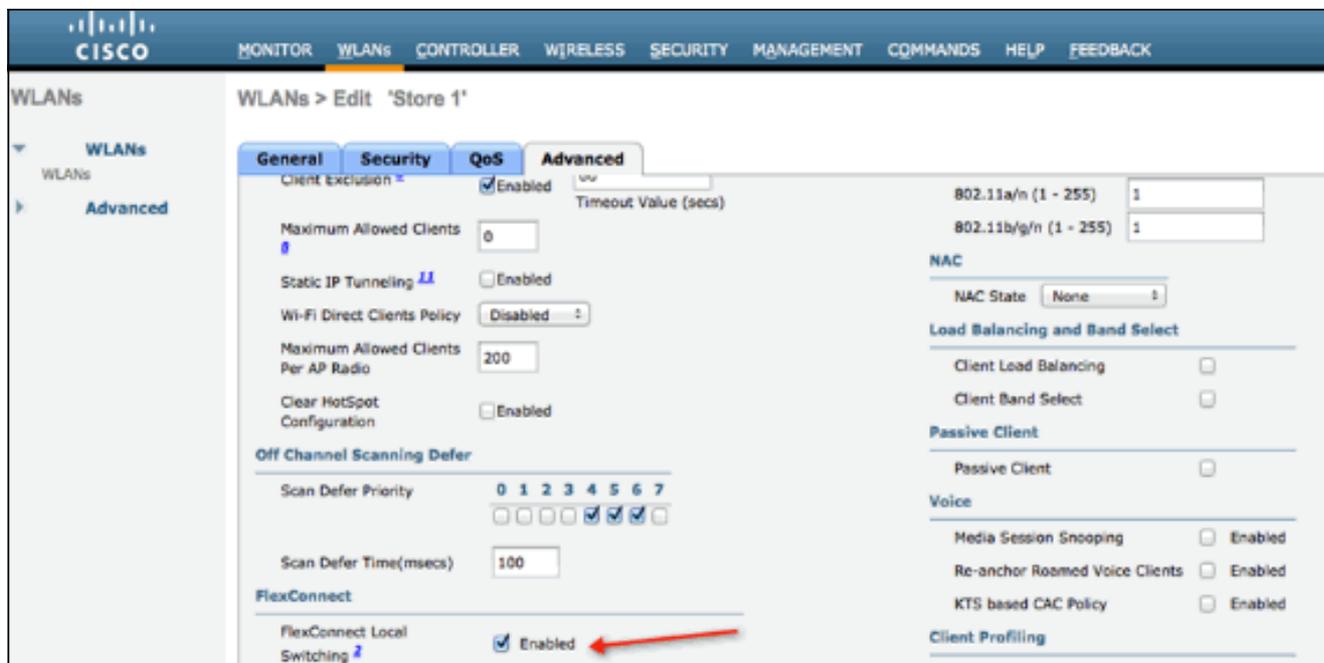
Riepilogo:

- WLAN configurata per switching locale FlexConnect e sicurezza L3
- Gli ACL FlexConnect verranno utilizzati come ACL di preautenticazione
- Una volta configurati, gli ACL FlexConnect devono essere inviati al database AP tramite Flex Group o un singolo AP, oppure possono essere applicati alla WLAN
- AP consente di commutare localmente tutto il traffico che corrisponde all'ACL di preautenticazione

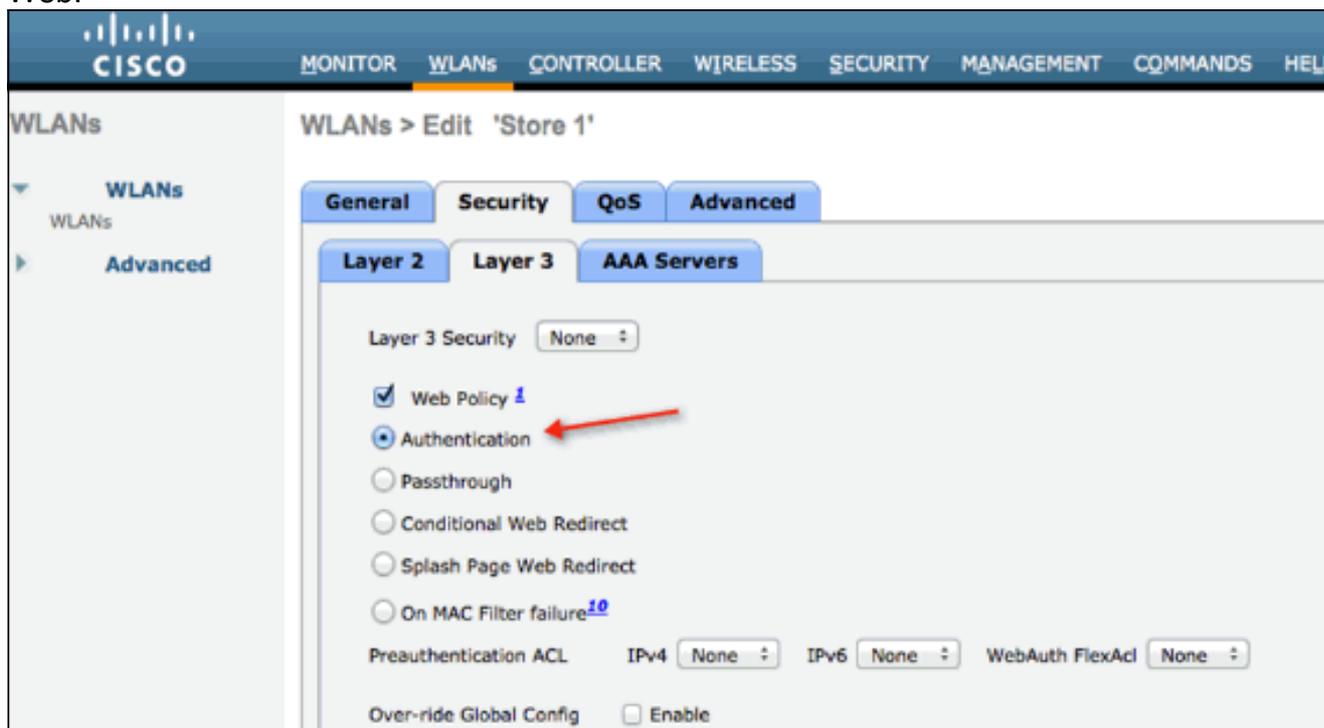
Procedura:

Per configurare questa funzionalità, completare la procedura seguente:

1. Configurare una WLAN per lo switching locale FlexConnect.



2. Per abilitare l'autenticazione Web esterna, è necessario configurare i criteri Web come criteri di sicurezza per la WLAN a commutazione locale. Questa opzione include una delle seguenti quattro opzioni: Autenticazione Pass-through, Reindirizzamento Web condizionale, Reindirizzamento Web pagina iniziale. In questo documento viene illustrato un esempio di autenticazione Web:



- I primi due metodi sono simili e possono essere raggruppati come metodi di autenticazione Web da un punto di vista della configurazione. I secondi due (Reindirizzamento condizionale e Pagina iniziale) sono criteri Web e possono essere raggruppati come metodi di criteri Web.
3. È necessario configurare l'ACL FlexConnect di preautenticazione in modo che i client wireless possano raggiungere l'indirizzo IP del server esterno. Il traffico ARP, DHCP e DNS è consentito automaticamente e non deve essere specificato. In Protezione > Lista di controllo di accesso, scegliere **ACL FlexConnect**. Quindi, fare clic su **Add** (Aggiungi) e definire i nomi e le regole come un normale ACL del controller.

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: È necessario creare ogni volta regole di inversione per il traffico.

4. Dopo aver creato gli ACL FlexConnect, occorre applicarli a diversi livelli: AP, FlexConnect Group e WLAN. L'ultima opzione (ACL Flex su WLAN) è valida solo per l'autenticazione Web e il pass-through Web per altri due metodi in Criteri Web, ad esempio Conditional e Splash Redirect. Gli ACL possono essere applicati solo all'access point o al Flex Group. Di seguito è riportato un esempio di ACL assegnato al livello AP. Andare su **Wireless > selezionare AP**, quindi fare clic sulla scheda

FlexConnect:

All APs > Details for 36001.0418

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

Fare clic sul collegamento **ACL di autenticazione Web esterna**. Quindi, scegliere l'ACL per l'ID WLAN specifico:

The screenshot displays the Cisco Wireless Management interface for an AP named 3600I.0418. The breadcrumb trail is "All APs > 3600I.0418 > ACL Mappings". The interface shows the following configuration sections:

- 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 (with an "Add" button below it).
- WLAN Table:** A table with columns "WLAN Id", "WLAN Profile Name", and "WebAuth ACL". The first row shows "1", "flex", and "AP-flex-ACL". A red arrow points to the "WebAuth ACL" dropdown menu in this row.
- WebPolicies:** WebPolicy ACL: AP-flex-ACL (with an "Add" button below it).

Analogamente, per l'ACL del criterio Web (ad esempio, il reindirizzamento condizionale o il reindirizzamento della pagina iniziale), sarà possibile selezionare l'ACL di Flex Connect in Criteri Web dopo aver fatto clic sullo stesso collegamento ACL di autenticazione Web esterna. Di seguito viene illustrato come eseguire questa operazione:

The screenshot shows the Cisco Wireless configuration interface for AP 36001.0418. The page is titled "All APs > 36001.0418 > 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:

- AP Information:** AP Name: 36001.0418, Base Radio MAC: 64:d9:89:42:0e:20.
- WLAN ACL Mapping:** WLAN Id: 0, WebAuth ACL: AP-flex-ACL, with an "Add" button.
- WLAN Profile Table:**

WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	AP-flex-ACL
- WebPolicies:** WebPolicy ACL: AP-flex-ACL, with an "Add" button. A red arrow points to this dropdown menu.

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

5. L'ACL può essere applicato anche a livello di gruppo FlexConnect. A tale scopo, andare alla scheda di **mappatura WLAN-ACL** nella configurazione del gruppo FlexConnect. Quindi, selezionare l'ID WLAN e l'ACL che si desidera applicare. Fare clic su **Add**. Ad esempio, per definire un ACL per un gruppo di access point.

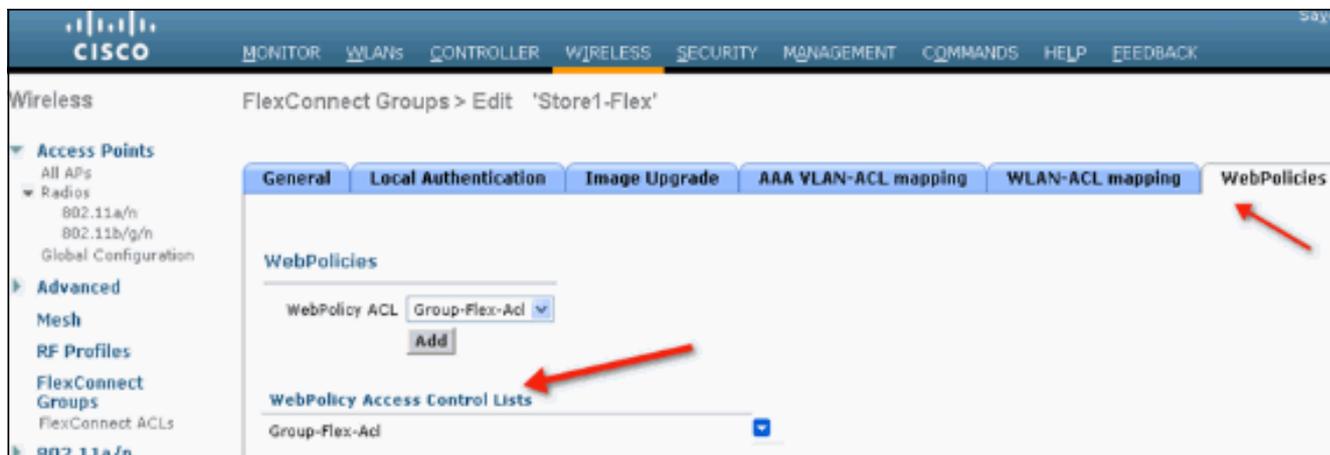
The screenshot shows the Cisco Wireless configuration interface for FlexConnect Group 'Store1-Flex'. The page is titled "FlexConnect Groups > Edit 'Store1-Flex'". The navigation menu on the left is similar to the previous screenshot. The main content area has several tabs: "General", "Local Authentication", "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 "WLAN ACL Mapping" section is visible, showing:

- WLAN Id: 0
- WebAuth ACL: AP-flex-ACL, with an "Add" button.
- WLAN Profile Table:**

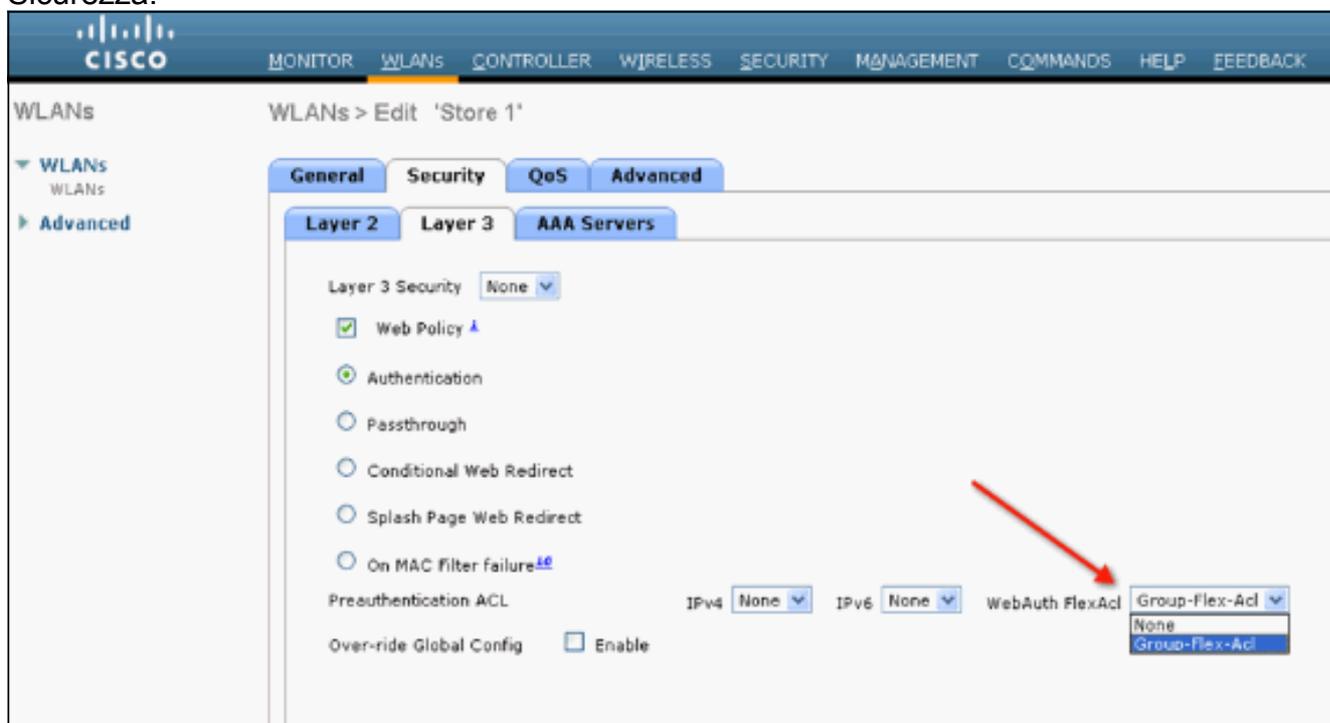
WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	Group-flex-ACL

A second red arrow points to the "Group-flex-ACL" dropdown menu in the table.

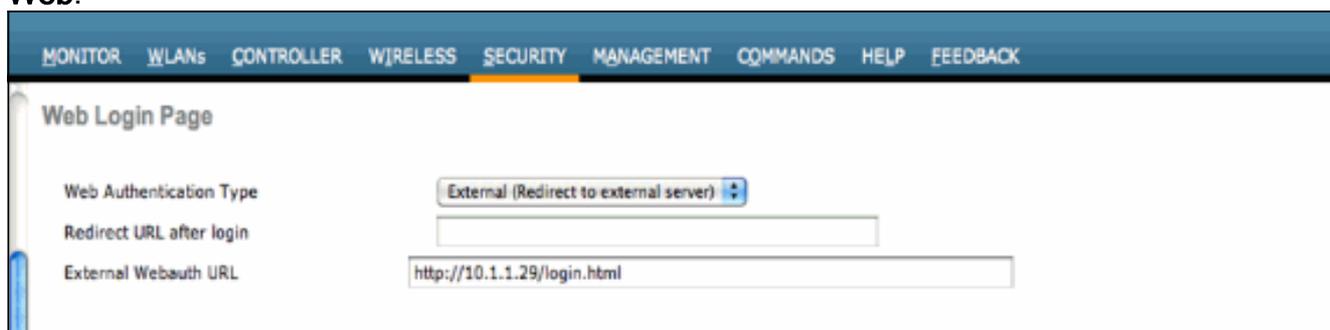
Analogamente, per l'ACL del criterio Web (per il reindirizzamento Web condizionale e della pagina iniziale), è necessario selezionare la scheda **Criteri Web**.



6. L'autenticazione Web e gli ACL Web Pass-through Flex possono essere applicati anche sulla WLAN. A tale scopo, scegliere l'ACL dall'elenco a discesa **WebAuth FlexACL** nella scheda Layer 3 in WLAN > Sicurezza.



7. Per l'autenticazione Web esterna, è necessario definire l'URL di reindirizzamento. Questa operazione può essere eseguita a livello globale o a livello di WLAN. Per il livello WLAN, fare clic sul segno di spunta **Override Global Config** (Ignora configurazione globale) e inserire l'URL. A livello globale, selezionare **Protezione > Web Auth > Pagina di accesso Web**:



Limitazioni: L'autenticazione Web (interna o verso un server esterno) richiede che l'access point Flex sia in modalità connessa. L'autenticazione Web non è supportata se Flex AP è in modalità standalone. L'autenticazione Web (interna o verso un server esterno) è supportata

solo con l'autenticazione centrale. Se una WLAN configurata per la commutazione locale è configurata per l'autenticazione locale, non è possibile eseguire l'autenticazione Web. Tutto il reindirizzamento Web viene eseguito a livello WLC e non a livello AP.

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)