

FlexConnect ローカル スイッチングを使用した外部 Web 認証の導入ガイド

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[機能の概要](#)

[関連情報](#)

概要

このドキュメントでは、さまざまな Web ポリシーに対して、外部 Web サーバと FlexConnect ローカル スイッチングを使用する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- FlexConnect アーキテクチャとアクセス ポイント (AP) に関する基本的な知識
- 外部 Web サーバのセットアップと設定の方法に関する知識
- DHCP サーバと DNS サーバのセットアップと設定の方法に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア リリース 7.2.110.0 が稼働する Cisco 7500 シリーズ ワイヤレス LAN コントローラ (WLC)
- Cisco 3500 シリーズ Lightweight アクセス ポイント (LAP)
- Web 認証ログイン ページをホストする外部 Web サーバ
- ワイヤレス クライアントに対するアドレス解決と IP アドレス割り当てに使用するローカル サイト上の DNS サーバおよび DHCP サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。この導入ガイドでは 7500 シリーズ WLC が使用されますが、この機能は 2500、5500、WiSM-2 のそれぞれの WLC でサポートされます。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

機能の概要

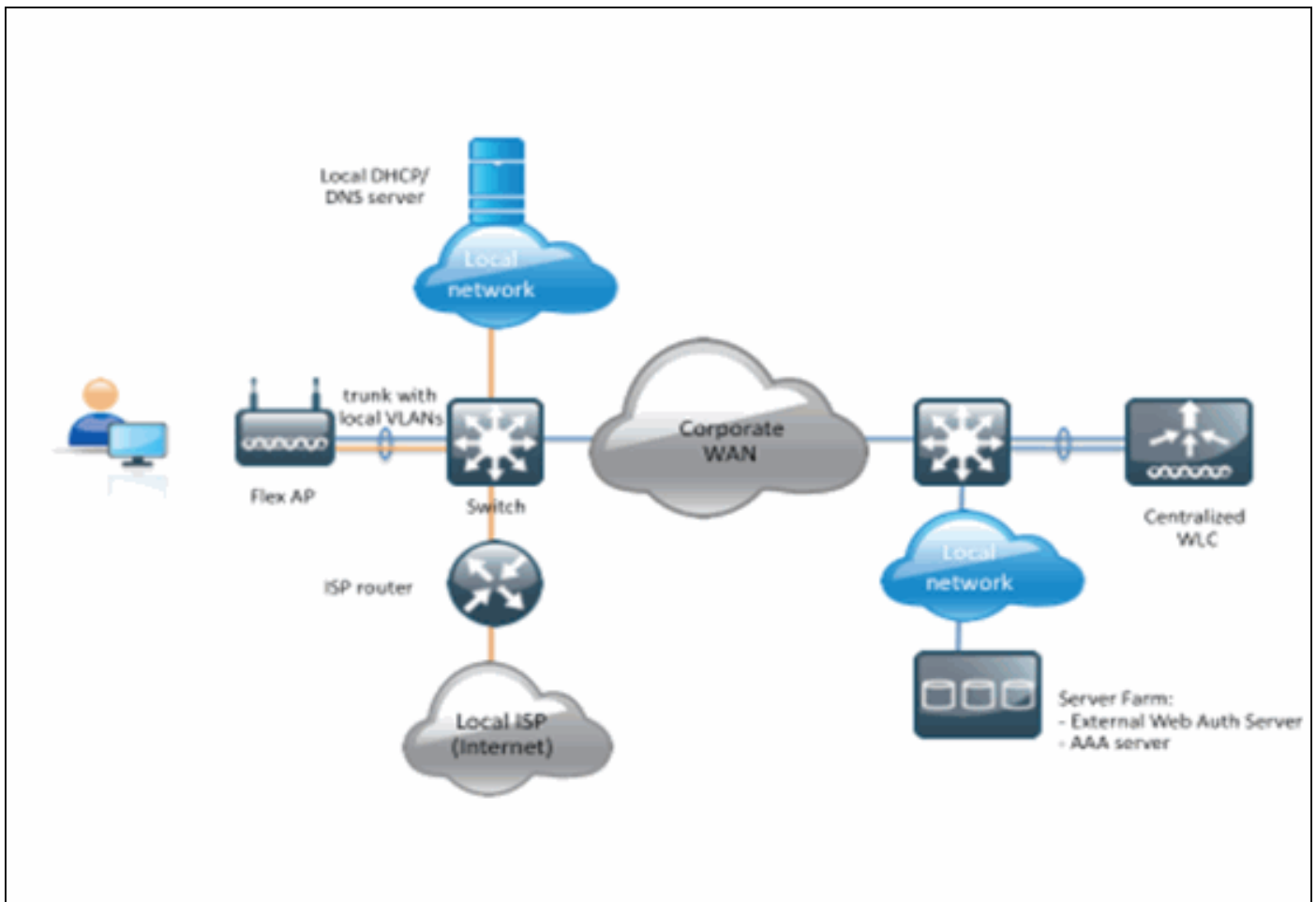
この機能は、FlexConnect モードで AP から外部 Web サーバに対して Web 認証を実行する機能を、ローカルにスイッチングされるトラフィックを持つ WLAN (FlexConnect – ローカル スイッチング) を対象に拡張します。WLC リリース 7.2.110.0 以前は、外部サーバに対する Web 認証は、一元的にスイッチングされるトラフィックを持つ WLAN (FlexConnect – 一元的スイッチング) を対象として、ローカル モードまたは FlexConnect モードの AP に対してサポートされていました。

外部 Web 認証としても知られるこの機能は、FlexConnect ローカル スイッチング WLAN を対象に機能を拡張してコントローラが現在提供しているすべてのレイヤ 3 Web リダイレクト セキュリティ タイプをサポートしています。

- Web 認証
- Web パススルー
- 条件付き Web リダイレクト
- スプラッシュ ページ Web リダイレクト

Web 認証とローカル スイッチング用に設定した WLAN について考えると、この機能の背景には、認証前用の FlexConnect アクセス コントロール リスト (ACL) を WLC レベルではなく AP レベルで直接配布および適用するというロジックがあります。この方法で、AP は、ACL によってローカルに許可されるワイヤレス クライアントから発信されるパケットをスイッチします。許可されないパケットは、CAPWAP トンネル経由で WLC に送信されます。一方、AP が有線インターフェイス経由でトラフィックを受信するとき、ACL が許可する場合は、ワイヤレス クライアントにそのトラフィックが転送されます。設定されている場合、パケットはドロップされます。クライアントが認証済みおよび承認済みになると、認証前用の FlexConnect ACL は削除され、すべてのクライアント データトラフィックが許可され、ローカルでスイッチングされます。

注：この機能は、クライアントがローカルにスイッチされる VLAN から外部サーバに到達できることを前提として動作します。



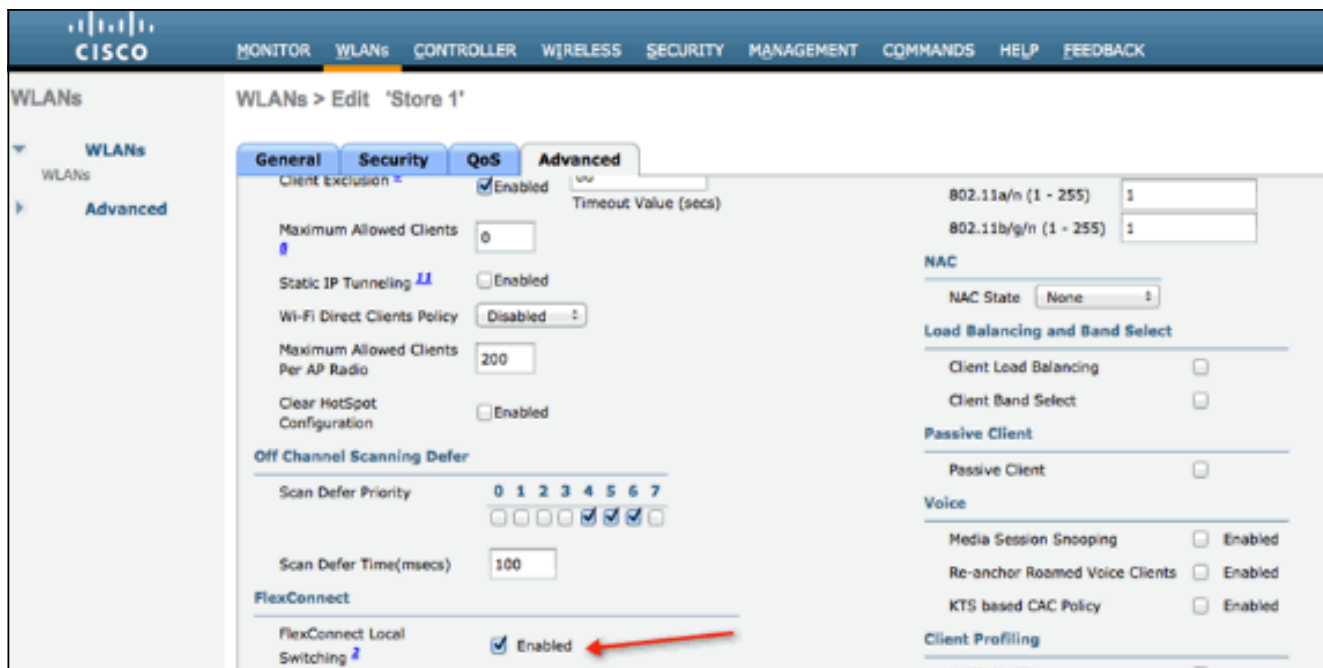
要約：

- FlexConnect ローカル スイッチングと L3 のセキュリティのために設定された WLAN
- FlexConnect ACL は認証前用の ACL として使用されます。
- FlexConnect ACL を設定したら、Flex グループまたは個々の AP 経由で AP データベースにプッシュする必要があります。または、WLAN に適用することができます。
- AP は、認証前用の ACL と一致するすべてのトラフィックをローカルにスイッチングすることを許可します。

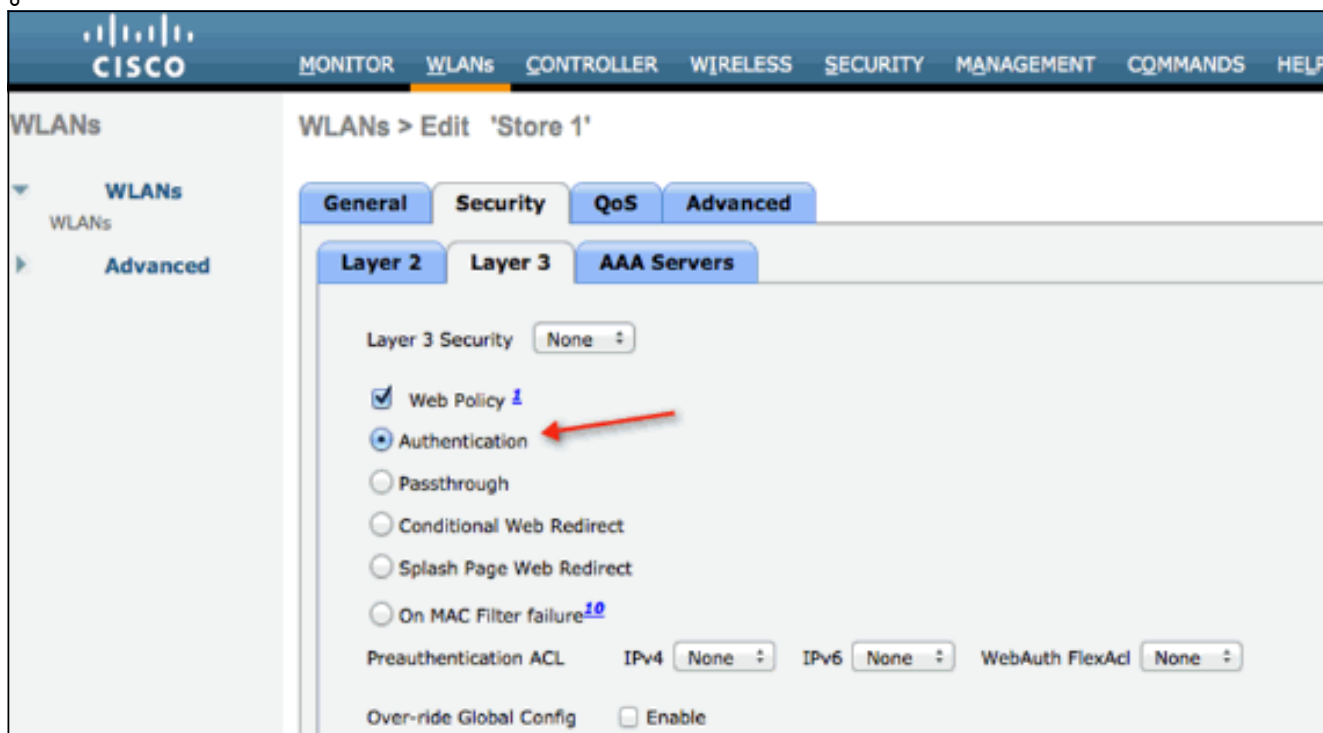
手順：

この機能を設定するには、次の手順を実行します。

1. FlexConnect ローカル スイッチング用に WLAN を設定します。



2. 外部 Web 認証を有効にするには、ローカルにスイッチングされる WLAN のセキュリティポリシーとして Web ポリシーを設定する必要があります。これには次の 4 つのオプションのうちの 1 つが含まれます。[Authentication]パススルー条件付き Web リダイレクトスプラッシュ ページ Web リダイレクトこのドキュメントでは、次の Web 認証の例で説明します。



最初の 2 つの方式は類似しており、設定の観点から見て、Web 認証方式としてグループ化できます。その後の 2 つ (条件付きリダイレクトおよびスプラッシュ ページ リダイレクト) は、Web ポリシーであり、Web ポリシー方式としてグループ化できます。

3. ワイヤレス クライアントが外部サーバの IP アドレスに到達することを許可するように、認証前用の FlexConnect ACL を設定する必要があります。ARP、DHCP、および DNS トラフィックは自動的に許可されるため、指定する必要はありません。[Security] > [Access Control List] で、[FlexConnect ACLs]を選択します。次に、[Add]をクリックし、通常のコントローラ ACL として名前とルールを定義します。

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

注：トラフィックのリバースルールを毎回作成する必要があります。

4. FlexConnect ACL を作成したら適用する必要があります。これは、次の異なるレベルで適用できます。AP、FlexConnect グループおよび WLAN。最後のオプション (WLAN レベルでの Flex ACL) は、条件付きリダイレクトやスプラッシュ リダイレクトなどの Web ポリシー下における他の 2 つの方式の Web 認証と Web パススルー専用です。ACL は AP または Flex グループに適用できます。AP のレベルで割り当てられる ACL の例を次に示します。
 [Wireless] > [Select AP] を選択し、[FlexConnect] タブをクリックします。

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](#)

[External WebAuthentication ACLs]のリンクをクリックします。次に、特定の WLAN ID として ACL を選択します。

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

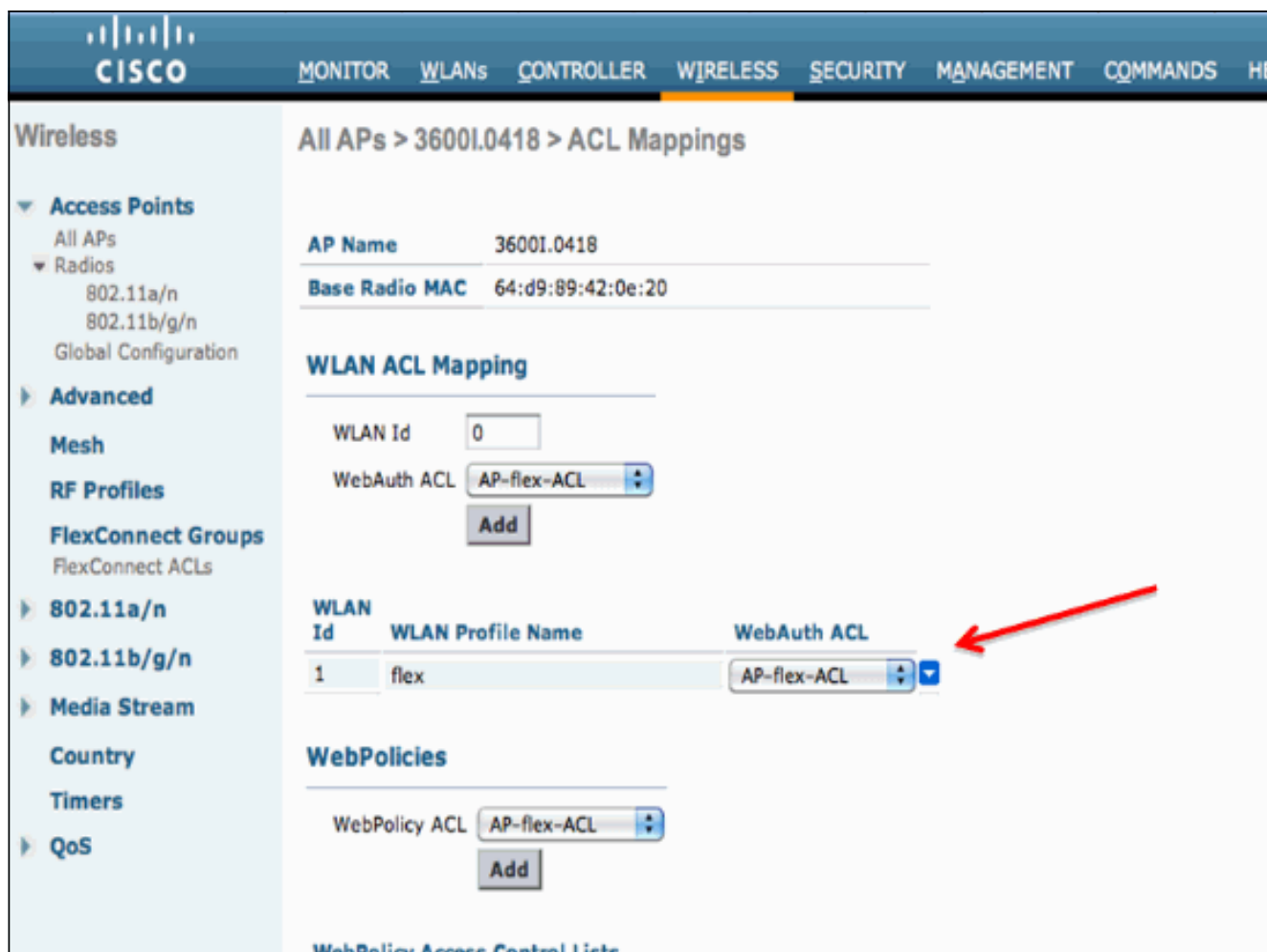
WLAN Id 0
WebAuth ACL AP-flex-ACL
Add

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

WebPolicies

WebPolicy ACL AP-flex-ACL
Add

WebPolicy Access Control Lists



同様に、Web ポリシーの ACL (たとえば、条件付きリダイレクトまたはスプラッシュ ページ リダイレクト) については、同じ [External WebAuthentication ACLs] リンクをクリックした後に、[WebPolicies] で [Flex Connect ACL] を選択します。これは、以下に示されています。

The screenshot shows the Cisco Wireless configuration interface for an AP named 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. There is an "Add" button below.
- WLAN Profile Table:**

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

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

5. ACL は、FlexConnect グループ レベルでも適用できます。これを行うには、[FlexConnect Group] の設定画面で、[WLAN-ACL mapping]タブを選択します。次に、適用したい WLAN ID と ACL を選択します。[Add] をクリックします。これは、AP のグループの ACL を定義するときに便利です。

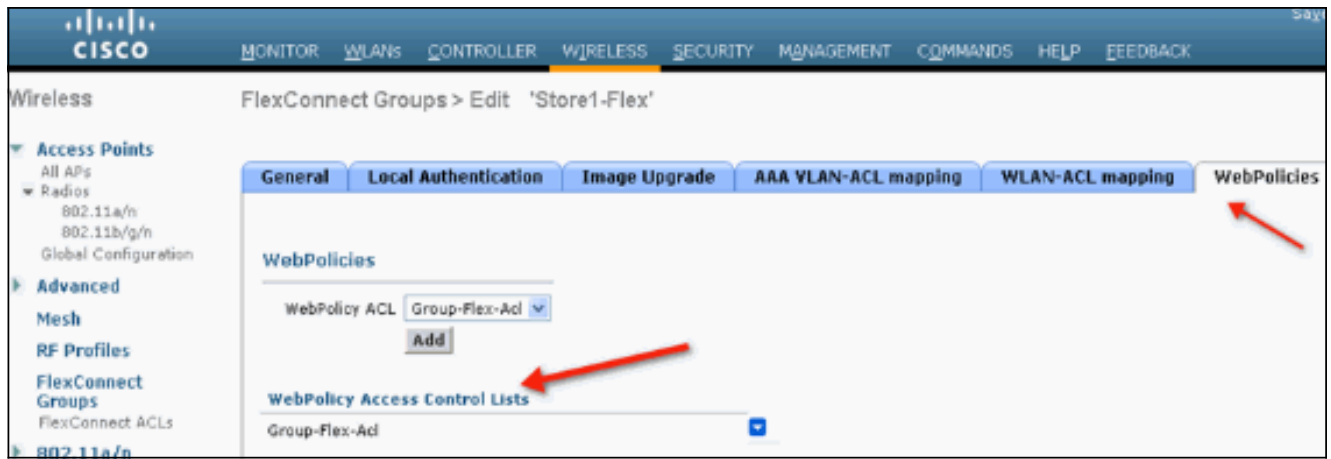
The screenshot shows the Cisco Wireless configuration interface for a FlexConnect Group named "Store1-Flex". The page is titled "FlexConnect Groups > Edit 'Store1-Flex'". The navigation menu on the left is similar to the previous screenshot. The main content area has several tabs: "General", "Local Authentication", "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:** WLAN Id: 0, WebAuth ACL: AP-flex-ACL. There is an "Add" button below.
- WLAN Profile Table:**

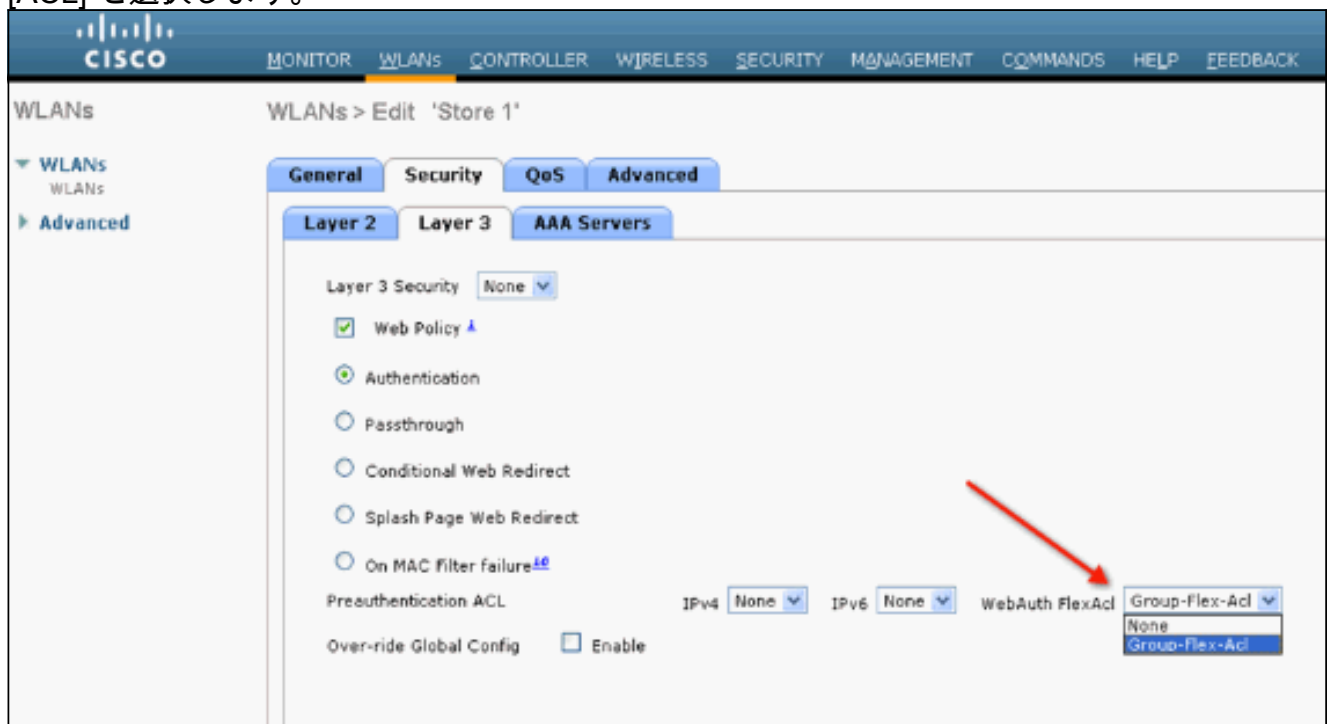
WLAN Id	WLAN Profile Name	WebAuth ACL
1	flex	Group-flex-ACL

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

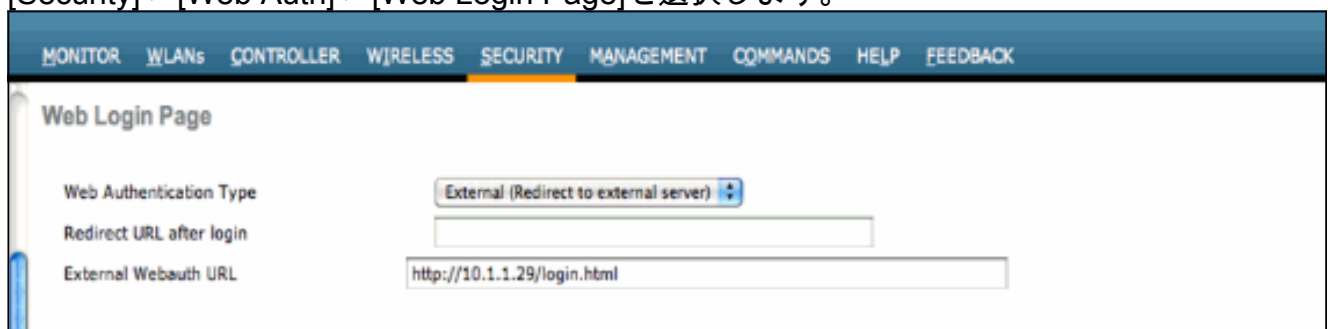
同様に、Web ポリシーの ACL (条件付きおよびスプラッシュページ Web リダイレクト) については、[WebPolicies]タブを選択する必要があります。



6. Web 認証および Web パススルーの Flex ACL は、WLAN にも適用できます。これを行うには、[WLAN] > [Security] の [Layer 3] タブで [WebAuth FlexACL]のドロップダウンから [ACL] を選択します。



7. 外部 Web 認証については、リダイレクト URL を定義する必要があります。これはグローバルレベルまたは WLAN レベルでできます。WLAN レベルの場合は、[Over-ride Global Config]のチェックマークをクリックし、URL を挿入します。グローバルレベルでは、[Security] > [Web Auth] > [Web Login Page]を選択します。



制限： Web 認証（内部または対外部サーバ）では、Flex AP が接続モードである必要があります。Web 認証は Flex AP がスタンドアロン モードの場合サポートされません。Web 認証（内部または対外部サーバ）は、中央認証でのみサポートされます。ローカルスイッチング用に設定された WLAN にローカル認証が設定されている場合は、Web 認証を実行できません。すべての Web リダイレクションは WLC レベルで実行され、AP レベルでは実行され

ません。

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)