在WLC上設定Flexconnect ACL

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[ACL型別](#)
[1. VLAN ACL](#)
[ACL方向](#)
[ACL對映注意事項](#)
[驗證ACL是否已應用於AP](#)
[2. Webauth ACL](#)
[3. Web策略ACL](#)
[4.分割通道ACL](#)
[疑難排解](#)

簡介

本檔案將說明各種Flexconnect存取控制清單(ACL)型別，以及在存取點(AP)上如何設定和驗證這些型別。

必要條件

需求

思科建議您瞭解以下主題：

- 執行8.3及更新版本的Cisco無線LAN控制器(WLC)
- WLC上的Flexconnect配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本8.3.133.0的Cisco 8540系列WLC。
- 在flexconnect模式下運行的3802和3702 AP。

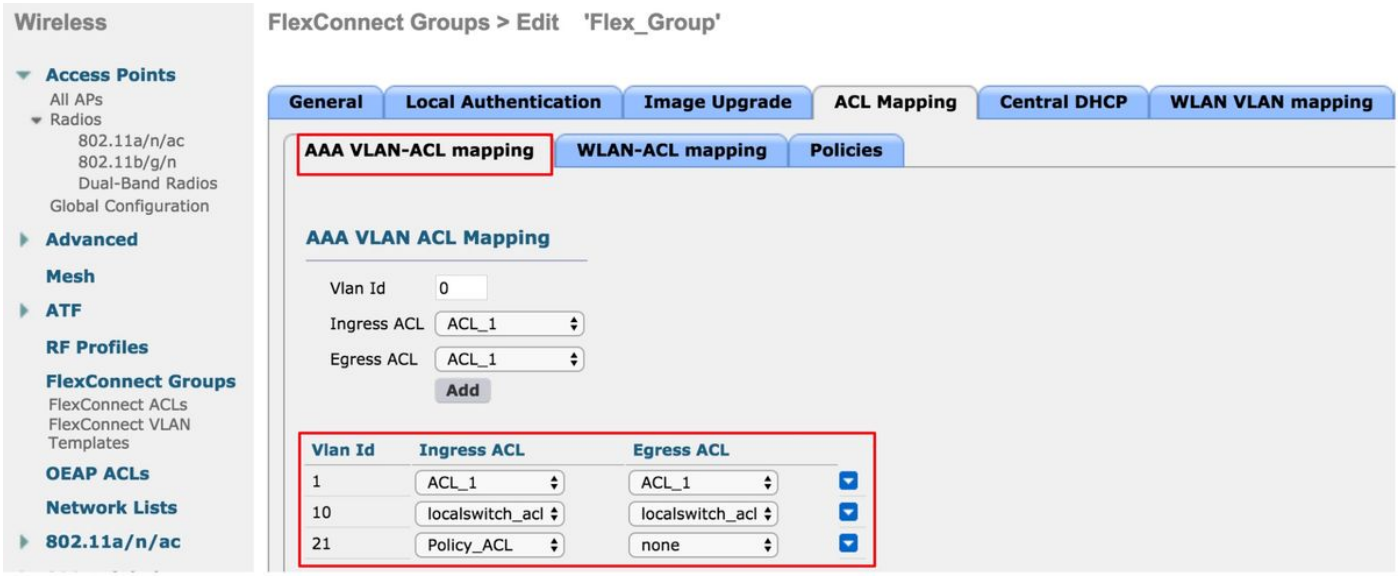
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

ACL型別

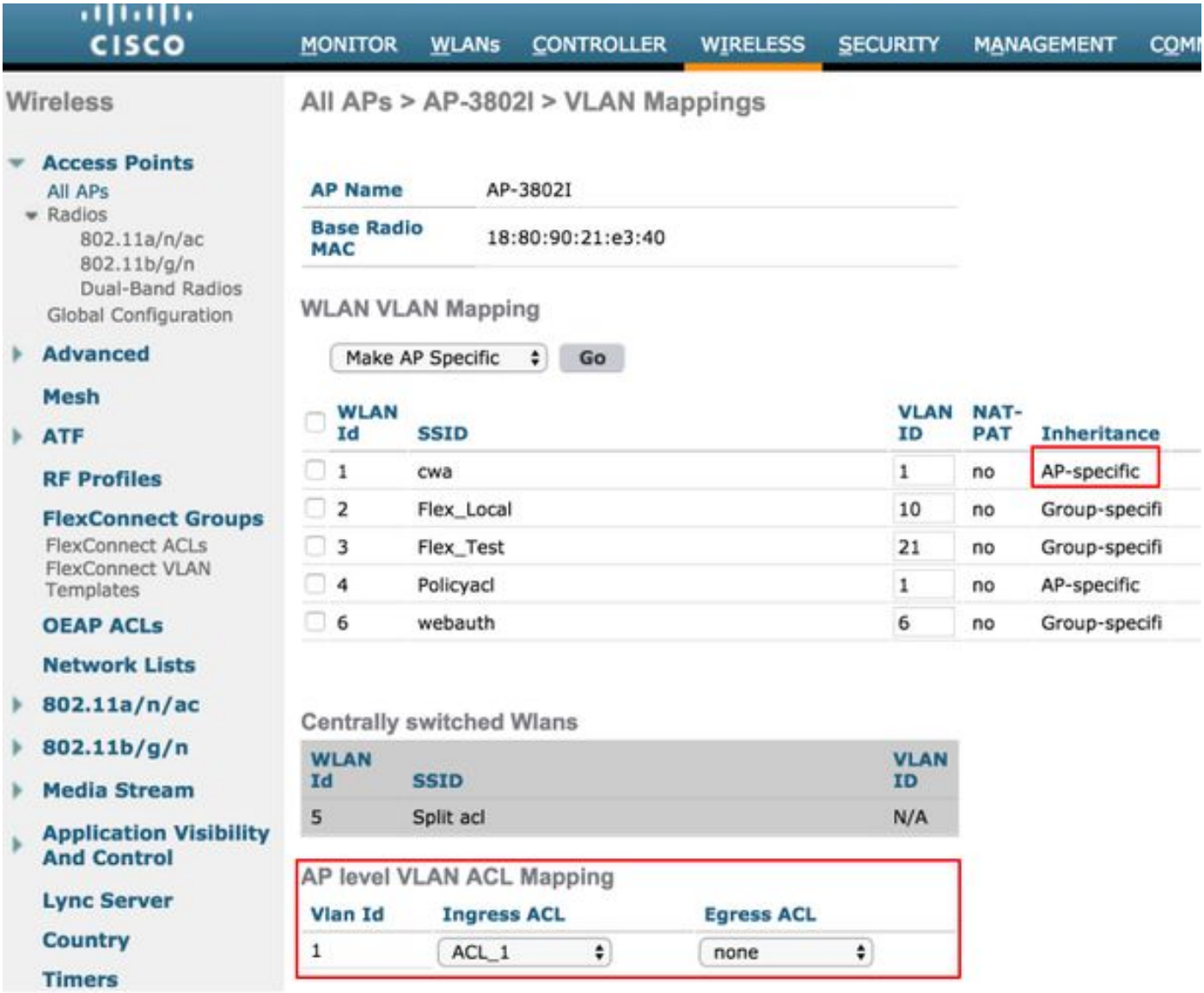
1. VLAN ACL

VLAN ACL是最常用的ACL，可用於控制進出該VLAN的客戶端流量。

您可以根據flexconnect組配置ACL，該組使用**無線 — Flexconnect組> ACL對映> AAA VLAN-ACL對映**中的**AAA VLAN-ACL對映部分，如下圖所示。**



也可以根據AP級別進行配置，導航到**無線>所有AP > AP名稱> Flexconnect頁籤**，然後按一下**VLAN對映**部分。在這裡，您需要首先使VLAN配置AP成為特定的AP，然後可以指定AP級別VLAN-ACL對映，如圖所示。



ACL方向

您還可以指定ACL的應用方向：

- Ingress（Ingress表示通向無線客戶端）
- 輸出（指向DS或LAN）、
- 兩者皆有或無。

因此，如果您想要封鎖目的地為無線使用者端的流量，可以使用輸入方向；如果您想要封鎖源自無線使用者端的流量，則可以使用輸出方向。

如果要使用驗證、授權及記帳(AAA)覆寫來推送獨立ACL，則會使用none選項。在這種情況下，由radius伺服器傳送的ACL會動態套用到使用者端。

> **附註**：ACL需要預先在Flexconnect ACL下配置，否則將不會應用。

ACL對映注意事項

使用VLAN ACL時，還必須瞭解flexconnect AP上VLAN對映的相關注意事項：

- 如果使用FlexConnect組配置VLAN，則會應用在FlexConnect組上配置的相應ACL。
- 如果在FlexConnect組和AP上配置了VLAN（作為AP特定配置），則AP ACL配置優先。
- 如果AP特定ACL配置為無，則不應用ACL。
- 如果AP上不存在從AAA返回的VLAN，則客戶端將回退到為無線LAN(WLAN)配置的預設VLAN，並且對映到該預設VLAN的任何ACL優先。

驗證ACL是否已應用於AP

使用本節內容，確認您的組態是否正常運作。

1.第2波無線接入點

在第2波AP上，可以使用**show flexconnect vlan-acl**命令驗證ACL是否實際被推送到AP。在這裡，您還可以看到每個ACL的已傳遞和已捨棄封包數量。

```
AP-3802I#show flexconnect vlan-acl
Flexconnect VLAN-ACL mapping-- ingress vlan     -----Listing ACL's in ingress direction
ACL enabled on ingress vlan

vlan_id: 10
ACL rules:
0: deny true and dst 10.1.1.0 mask 255.255.255.0,
1: deny true and dst 10.1.10.1 mask 255.255.255.255,
2: allow true,
the number of passed packets: 4
the number of dropped packets: 0

Flexconnect VLAN-ACL mapping-- egress vlan      -----Listing ACL's in egress direction
ACL enabled on egress vlan

vlan_id: 21
ACL rules:
0: allow true and dst 10.106.34.13 mask 255.255.255.255,
1: allow true and src 10.106.34.13 mask 255.255.255.255,
2: deny true,
the number of passed packets: 1
the number of dropped packets: 4
```

2. Cisco IOS® AP的

在AP級別，您可以通過兩種方式驗證ACL配置是否已推送到AP:

- 使用**show access-lists**命令，該命令會顯示是否在AP上配置了所有VLAN ACL:

```
AP-3702#sh access-lists
Extended IP access list Policy_ACL
    10 permit ip any host 10.106.34.13
    20 permit ip host 10.106.34.13 any
    30 permit udp any range 0 65535 any eq bootpc
    40 permit udp any eq bootps any range 0 65535
    50 deny ip any any
```

您還可以監控每個ACL上發生的活動，檢查該ACL的詳細輸出並檢視每行的命中數：

```
AP-3702#sh access-lists Policy_ACL
Extended IP access list Policy_ACL
    10 permit ip any host 10.106.34.13
    20 permit ip host 10.106.34.13 any
    30 permit udp any range 0 65535 any eq bootpc (6 matches)  -------------Shows the hit count
    40 permit udp any eq bootpc any range 0 65535
    50 deny ip any any (78 matches)
```

- 由於VLAN ACL應用在gigabit介面上，因此您可以驗證ACL應用是否正確。檢查子介面輸出，如下所示：

```
AP-3702#sh run interface GigabitEthernet0.10
Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10
 ip access-group localswitch_acl in --------Specifies that localswitch_acl has been applied in
ingress direction
 ip access-group localswitch_acl out -------Specifies that localswitch_acl has been applied in
egress direction
 bridge-group 6
 bridge-group 6 spanning-disabled
 no bridge-group 6 source-learning
```

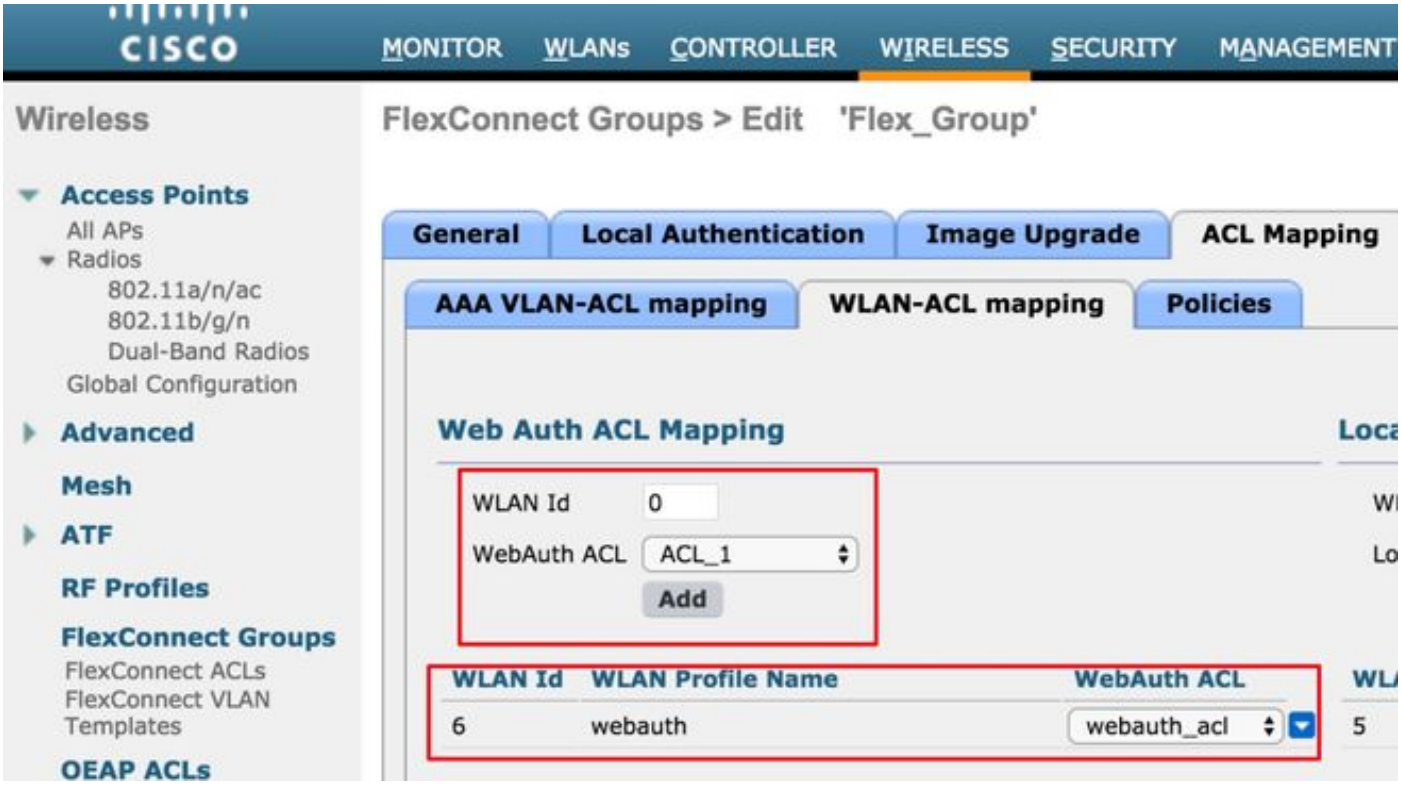
2. Webauth ACL

Webauth ACL用於已啟用flexconnect本機交換的Webauth/Webpassthrough服務組識別碼(SSID)。這用作預先驗證ACL，允許使用者端流量到達重新導向伺服器。重新導向完成且使用者端處於**RUN**狀態後，ACL會停止以使之生效。

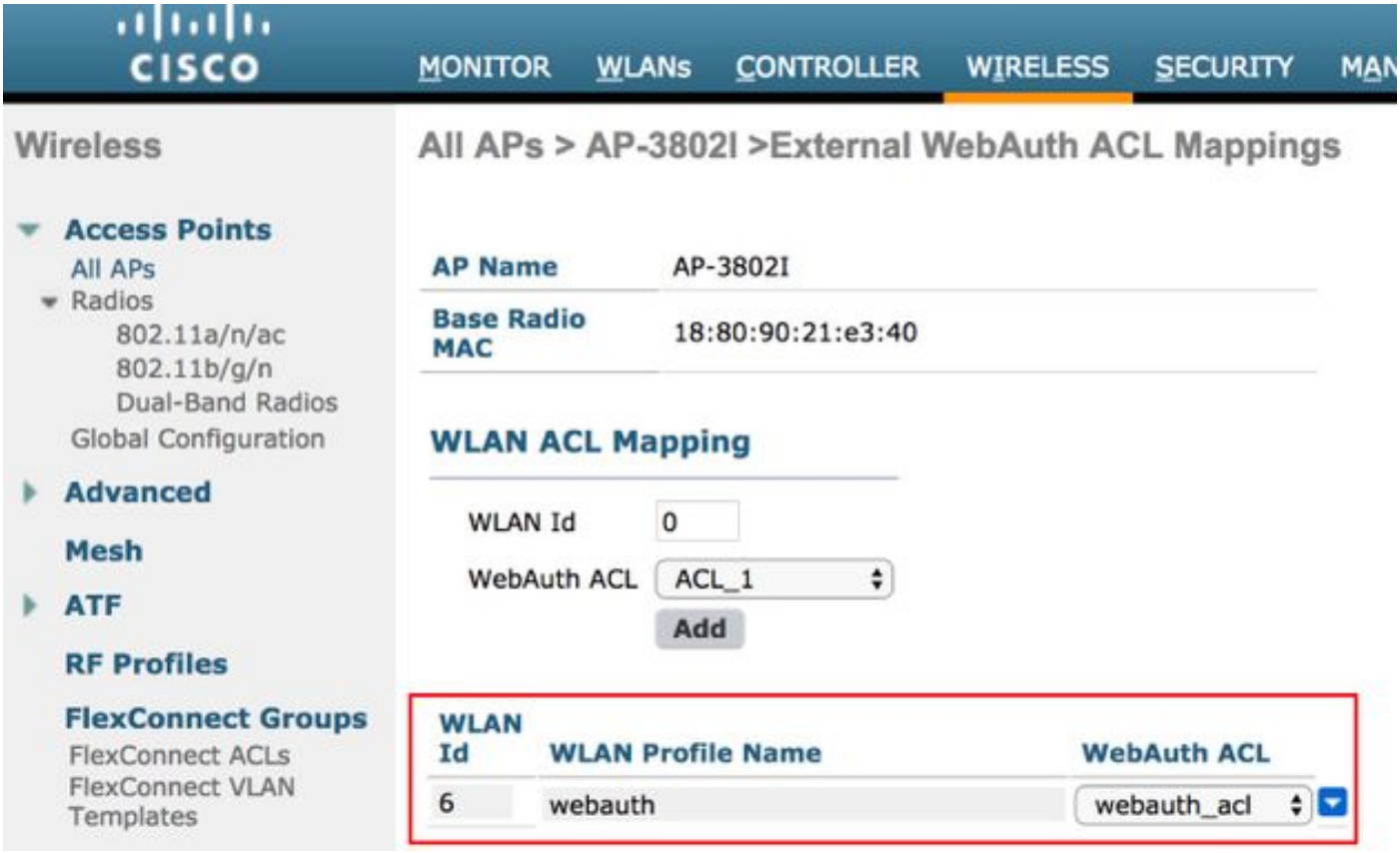
Webauth ACL可在WLAN層級、AP層級或flexconnect組層級應用。特定於AP的ACL的優先順序最高，而WLAN ACL的優先順序最低。如果應用所有這三種方法，則AP特定優先使用Flex ACL，然後是WLAN全域性特定ACL。

AP上最多可設定16個Web-Auth ACL。

可在flexconnect組級別應用，請導覽至**Wireless > Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping**，如下圖所示。



ACL可應用於AP級別，請導覽至**Wireless >All AP's >AP name >Flexconnect頁籤>External WebAuthentication ACLs > WLAN ACL**，如下圖所示。



ACL可應用於WLAN層級，導覽至**WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl**，如下圖所示。

在Cisco IOS® AP上，可以驗證該ACL是否已應用到客戶端。檢查**show controllers dot11radio 0 client**（如果客戶端連線到A無線電，則為1）的輸出，如下所示：

```
AP-3702#show controller dot11radio0 client
---Clients 0  AID VLAN Status:S/I/B/A Age TxQ-R(A) Mode Enc Key  Rate  Mask Tx   Rx
BVI   Split-ACL Client-ACL WebAuth-ACL L2-ACL
e850.8b64.4f45    1    4 30 40064 000 0FE 299  0-0 (0) 13B0 200 0-10 1EFFFFFF00000000000  020F
030 - - - webauth_acl       -     --------Specifies the name of the ACL that was applied
```

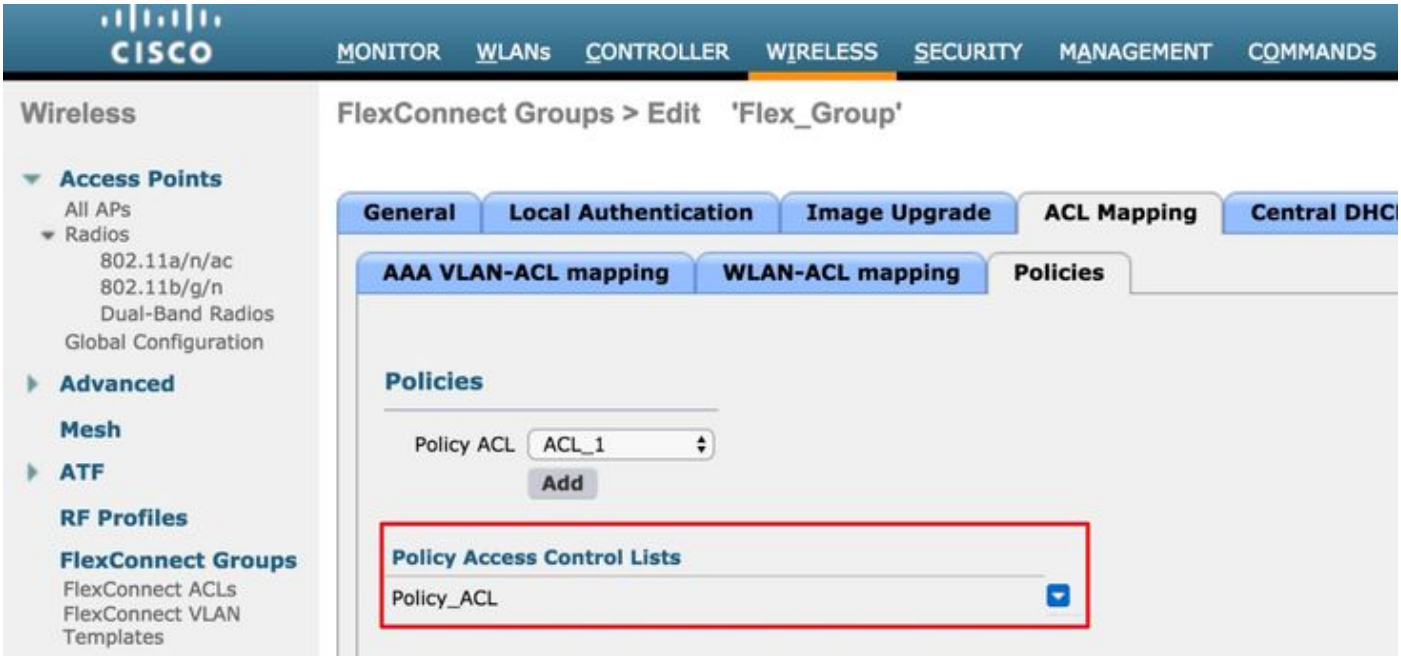
3. Web策略ACL

WebPolicy ACL用於條件式Web重新導向、啟動顯示頁面Web重新導向和中央Webauth案例。

使用Flex ACL的WebPolicy WLAN有兩種設定模式：

1. Flexconnect組

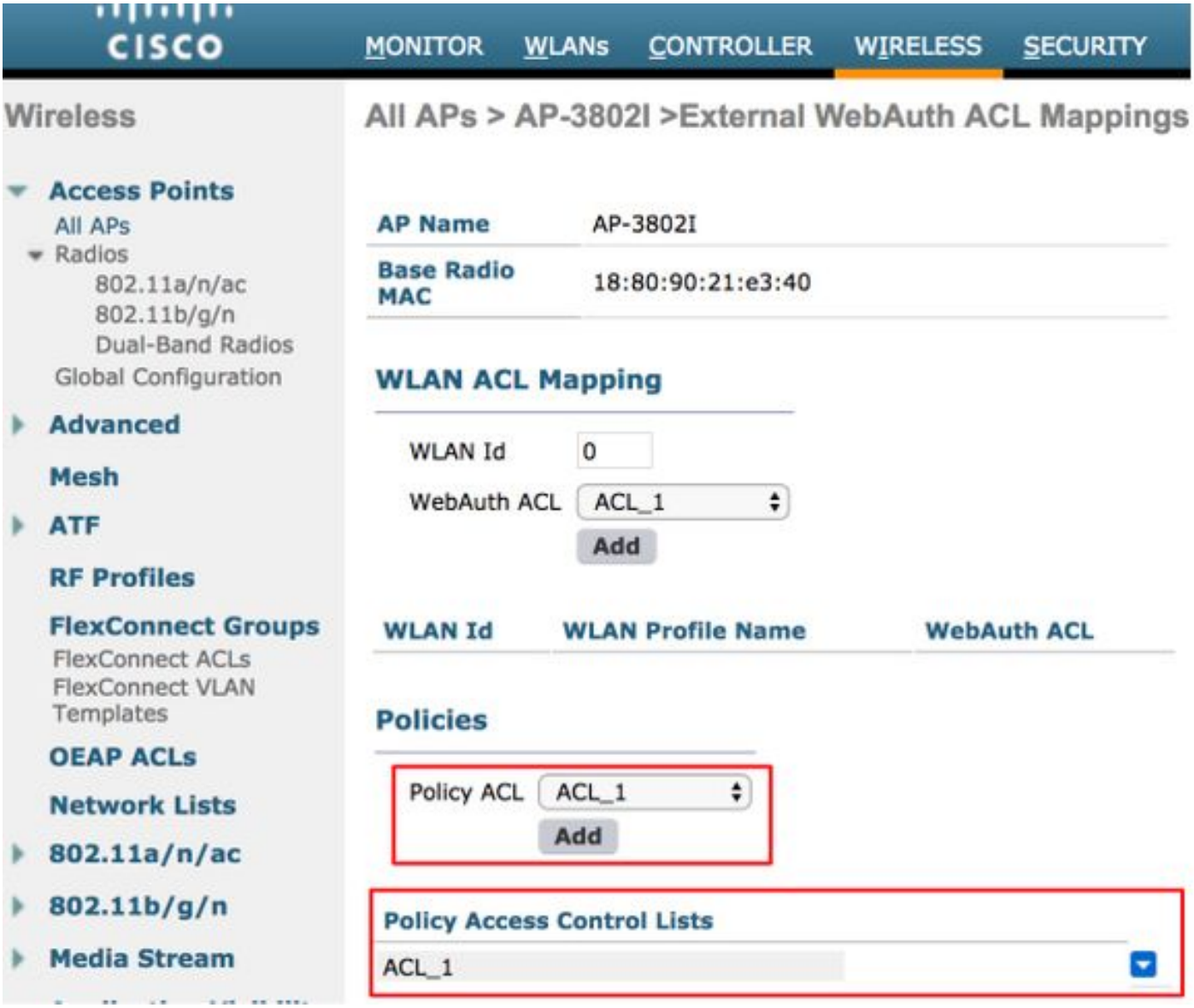
FlexConnect組中的所有AP都會收到已配置的ACL。您可以對此進行配置，導航到**Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > Policies**，然後新增策略ACL的名稱，如下圖所示：



2.特定於AP

完成配置的AP會收到ACL，但不會影響其他AP。您可以在導航到**無線>所有AP > AP名稱>**時進行配置

Flexconnect頁籤>外部Web驗證ACL >策略，如下圖所示。



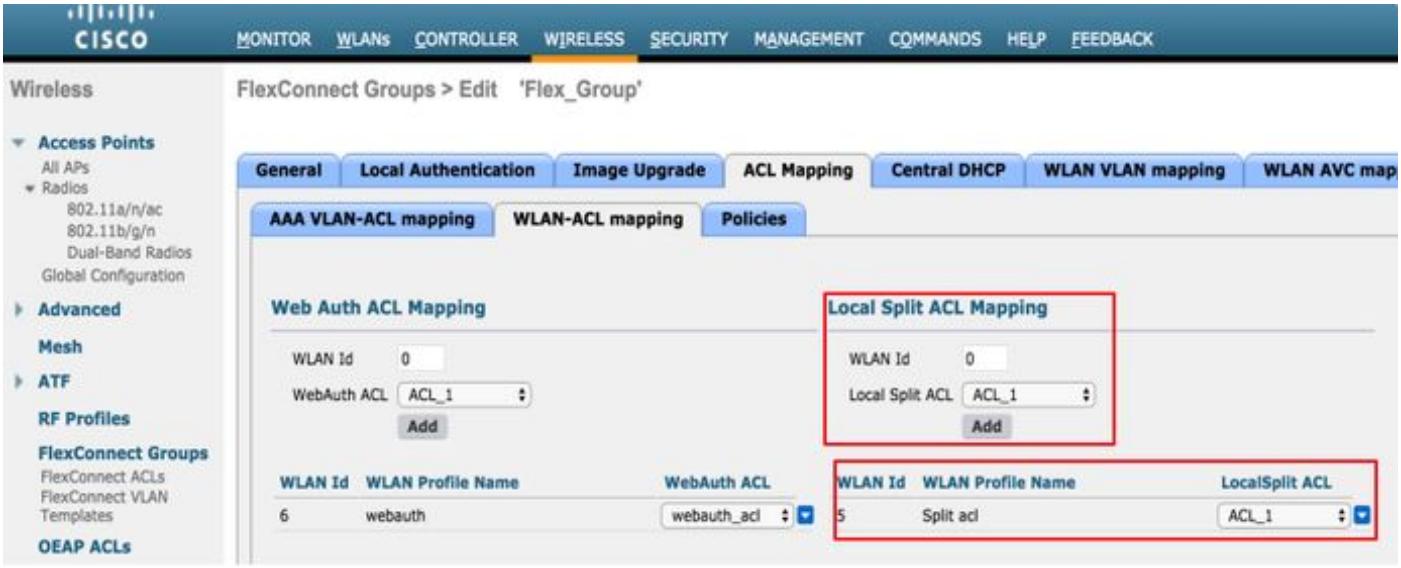
成功進行L2驗證後，當radius伺服器在redirect-acl AV配對中傳送ACL名稱時，此名稱會直接套用到AP上的使用者端。當客戶端進入**RUN**狀態時，所有客戶端流量都在本地交換，並且AP會停止以應用ACL。

一個AP上最多可以配置32個WebPolicy ACL。16個AP特定，16個FlexConnect組特定。

4.分割通道ACL

當部分客戶端流量需要通過本地傳送時，拆分隧道ACL與集中交換SSID一起使用。分割隧道功能也是Office Extend Access Point(OEAP)設定的一個額外優勢，在分割隧道ACL中提到企業SSID上的客戶端後，它們可以直接與本地網路中的裝置（印表機、遠端LAN埠上的有線電腦或個人SSID上的無線裝置）通訊。

您可以根據flexconnect組級別配置分割通道ACL，導航至**Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mapping**，如下圖所示。



也可以根據AP級別配置它們，導航到**Wireless > All AP's > AP name > Flexconnect頁籤>Local Split ACL**，然後新增flexconnect ACL的名稱，如下圖所示。

分割通道ACL無法在本地橋接組播/廣播流量。即使組播/廣播流量與FlexConnect ACL匹配，也會集中進行交換。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。