Configure Flexconnect ACL's on WLC

Contents

Introduction

This document describes the various flexconnect Access Control List (ACL) types and how they can be configured and validated on the Access Point (AP).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless LAN Controller (WLC) that runs code 8.3 and higher
- Flexconnect configuration on the WLC

Components Used

The information in this document is based on these software and hardware versions:

- The Cisco 8540 Series WLC that runs software Release 8.3.133.0.
- 3802 and 3702 AP's that runs in flexconnect mode.

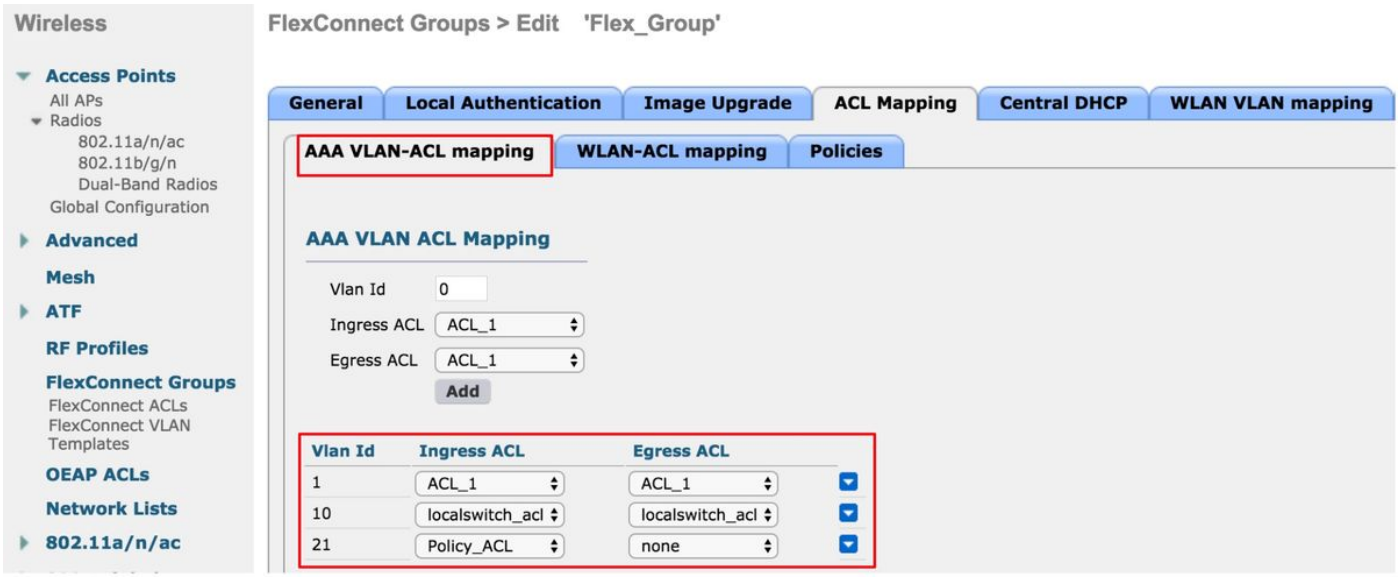
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

ACL Types

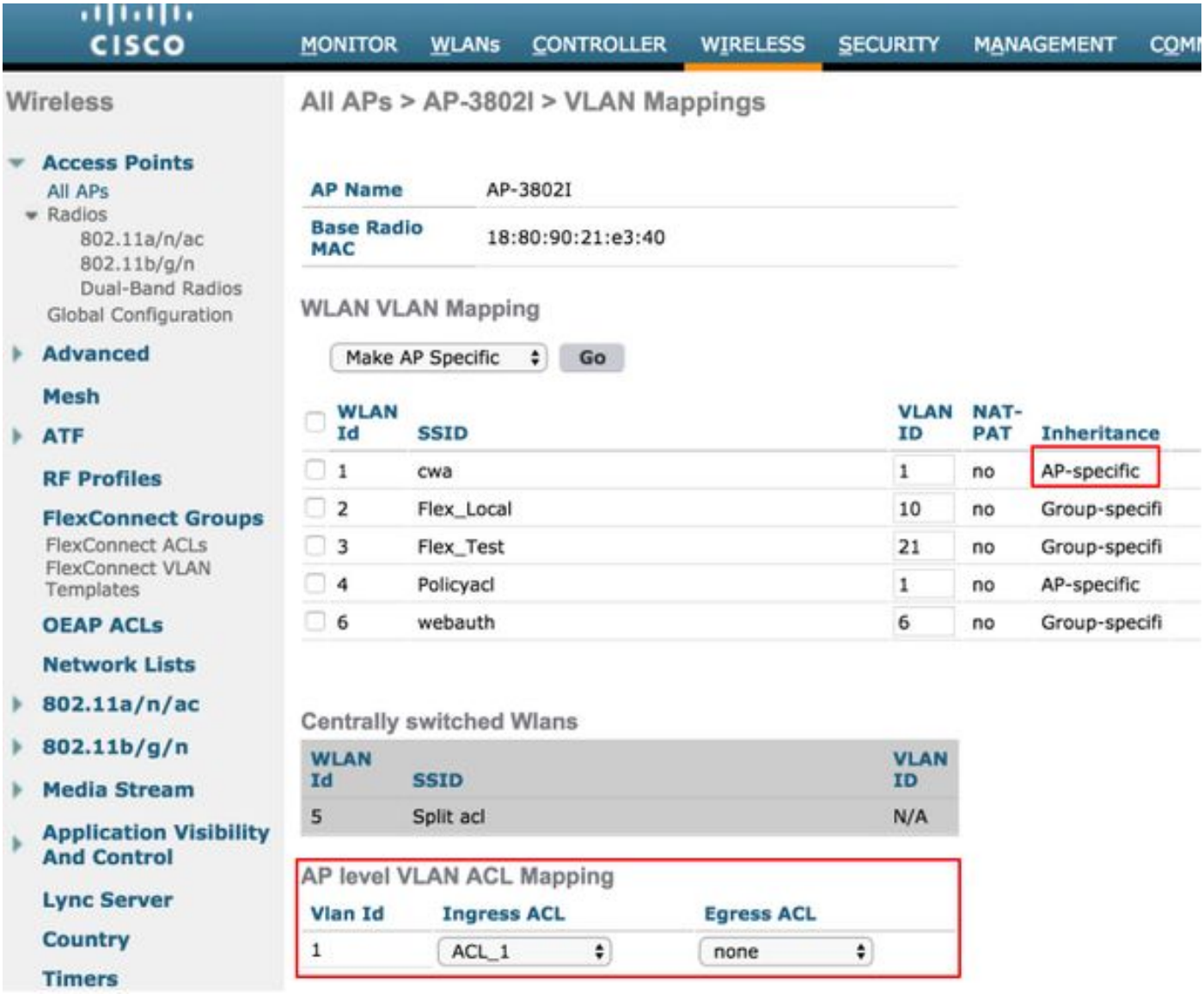
1. VLAN ACL

VLAN ACL are the most commonly used ACL and it lets you control client traffic that is sent in and out of the VLAN.

The ACL can be configured as per the flexconnect group which uses the **AAA VLAN-ACL** mapping section in **Wireless-Flexconnect Groups > ACL mapping > AAA VLAN-ACL mapping** as shown in the image.



It can also be configured as per the AP level, navigate to **Wireless > All AP's > AP name > Flexconnect tab** and click **VLAN mappings** section. Here, you need to make the VLAN config AP specific first, after which you can specify the AP level VLAN-ACL mapping as shown in the image.



ACL Directions

You can also specify the direction in which the ACL gets applied:

- Ingress (Ingress means towards the wireless client)
- Egress (towards theDS or LAN),
- both or none.

So, if you would like to block traffic destined towards the wireless client then you can use ingress direction and if you would like to block traffic sourced by the wireless client, you can use the egress direction.

The option none is used when you would like to push a separate ACL with the use of Authentication, Authorization, and Accounting (AAA) override. In this case, the ACL sent by the radius server is applied dynamically to the client.

> **Note**: The ACL needs to be configured under Flexconnect ACL beforehand, otherwise it does not get applied.

ACL Mapping Considerations

When you use VLAN ACL's, it is also important to understand these considerations with respect to VLAN mappings on flexconnect AP's:

- If the VLAN is configured with the use of the FlexConnect group, the corresponding ACL configured on the FlexConnect group is applied.
- If a VLAN is configured on both the FlexConnect group and also on the AP (as a AP specific configuration), then the AP ACL configuration takes precedence.
- If the AP specific ACL is configured to none, then no ACL is applied.
- If the VLAN that was returned from the AAA is not present on the AP, the client falls back to the default VLAN configured for the Wireless LAN (WLAN) and any ACL mapped to that default VLAN takes precedence.

Verify if ACL is Applied on AP

Use this section in order to confirm that your configuration works properly.

1. Wave 2 AP's

On a wave 2 AP, you can verify if the ACL actually gets pushed to the AP with the command **show flexconnect vlan-acl**. Here, you can also see number of passed and dropped packets for each ACL.

```
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's

At the AP level, you can validate if the ACL configuration has been pushed to the AP with two ways:

- Use the **show access-lists** command which shows if all the VLAN ACL's are configured on the AP:

```
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
```

You can also monitor the activity that happens on each ACL, check the detailed output of that ACL and see the hit count for each line:

```
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)
```

- Since the VLAN ACL's are applied on the gigabit interface, you can validate if the ACL is applied correctly. Check the sub interface output as shown here:

```
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
```

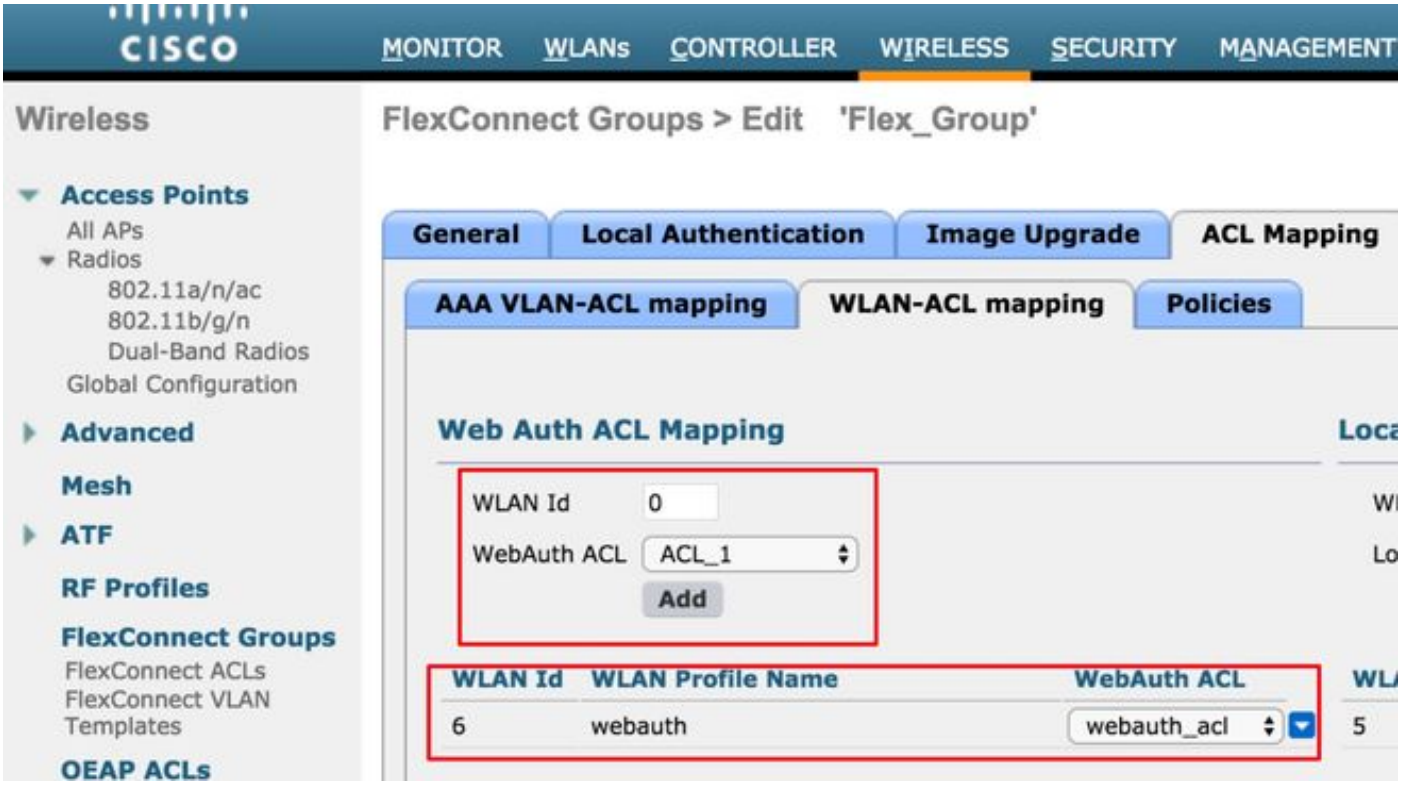
2. Webauth ACL

Webauth ACL is used in the case of a Webauth/Webpassthrough Service Set Identifier (SSID) which has been enabled for flexconnect local switching. This is used as a pre-authentication ACL and allows client traffic to the redirect server. Once the redirection is complete and the client is in **RUN** state, the ACL stops to take it into effect.

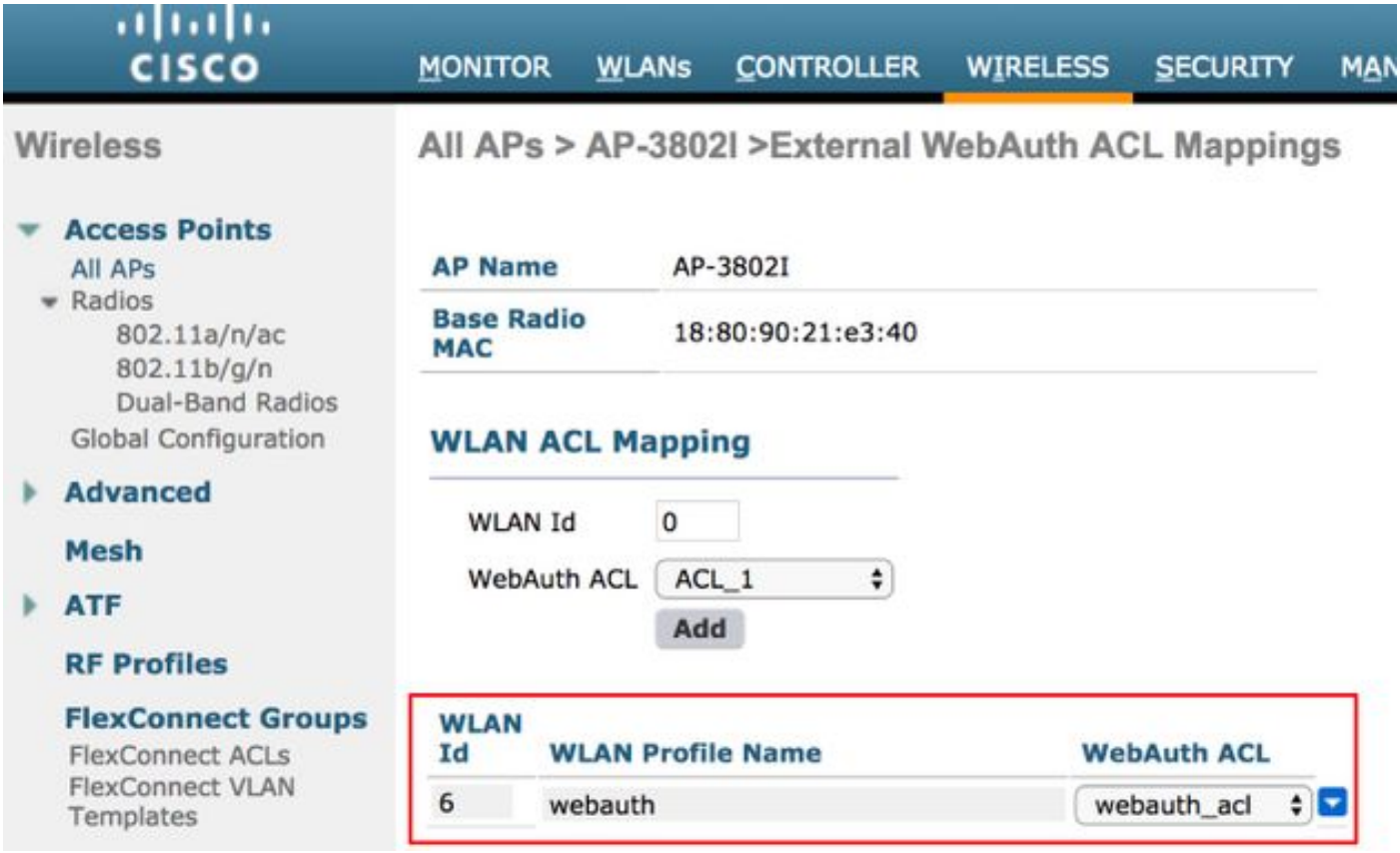
Webauth ACL can be applied either at the WLAN level, AP level or flexconnect group level. An AP specific ACL has the highest priority, whereas the WLAN ACL has the lowest. If all three are applied, AP Specific takes precedence followed by Flex ACL and then WLAN Global Specific ACL.

There can be a maximum of 16 Web-Auth ACLs configured on an AP.

It can be applied at the flexconnect group level, navigate to **Wireless > Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Web Auth ACL Mapping** as shown in the image.



The ACL can be applied at the AP level, navigate to **Wireless >All AP's >AP name >Flexconnect tab > External WebAuthentication ACLs > WLAN ACL** as shown in the image.



The ACL can be applied at the WLAN level, navigate to **WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl** as shown in the image.

On the Cisco IOS® AP, you can verify if the ACL was applied to the client. Check the output of **show controllers dot11radio 0 client** (or 1 if the client connects to the A radio) as shown here:

```
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
```

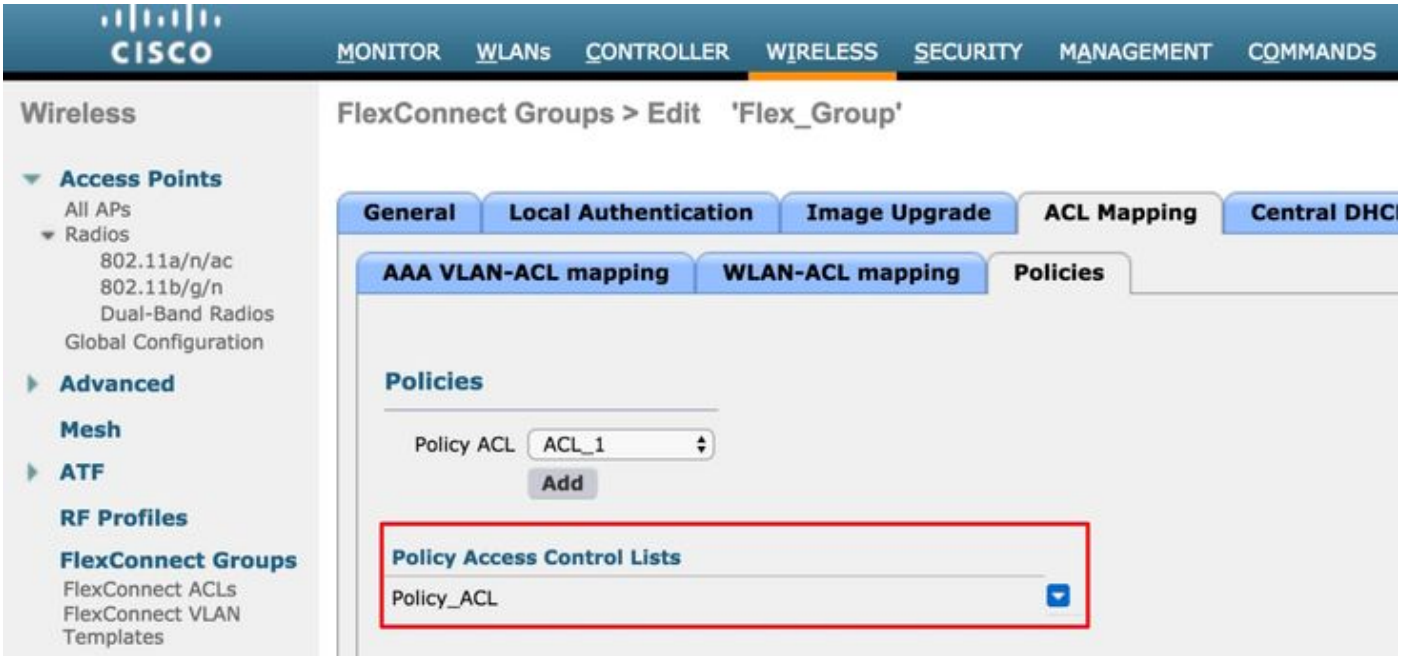
3. Web Policy ACL

WebPolicy ACL is used for Conditional Web Redirect, Splash Page Web Redirect and Central Webauth scenarios.

There are two modes of configuration available for WebPolicy WLANs with Flex ACLs:

1. Flexconnect Group

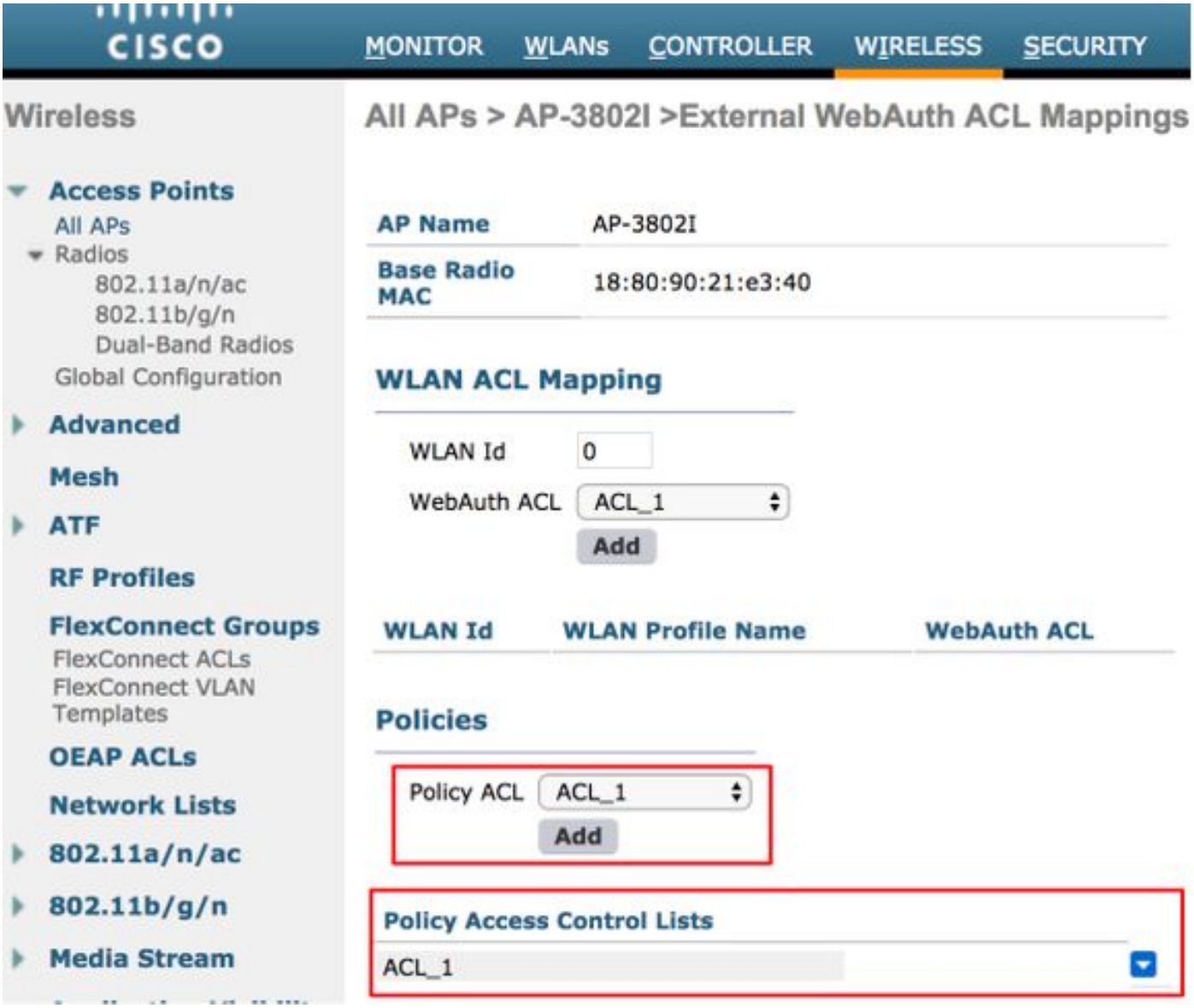
All the APs in the FlexConnect group receive the ACL that is configured. This can be configured as you navigate to **Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > Policies**, and add the name of the Policy ACL as shown in the image:



2. AP Specific

The AP for which the configuration is done receives the ACL, no other APs are impacted. This can be configured as you navigate to **Wireless > All APs > AP name >**

Flexconnect tab > External WebAuthentication ACLs > Policies as shown in the image.



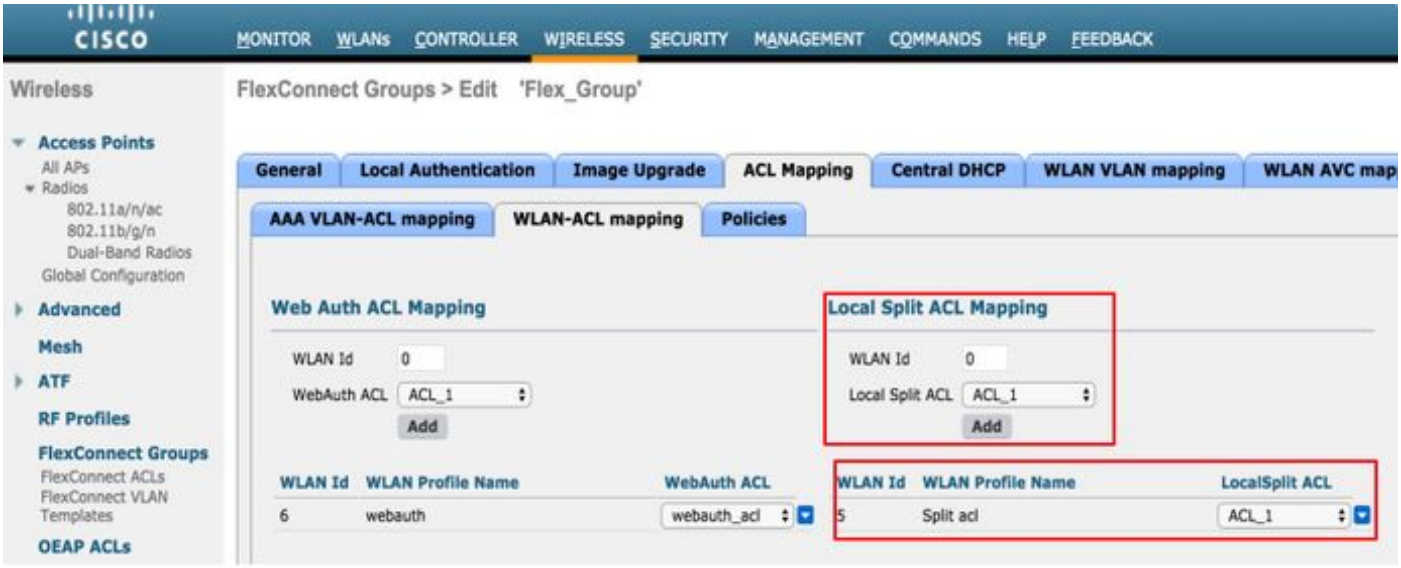
After a successful L2 authentication, when the radius server sends the ACL name in the redirect-acl AV pair, this gets applied directly for the client on the AP. When the client moves into **RUN** state, all client traffic is switched locally and the AP stops to apply ACL.

There can be a maximum or 32 WebPolicy ACLs configured on an AP. 16 AP specific and 16 FlexConnect group specific.

4. Split Tunnel ACL

Split Tunneling ACL's are used with centrally switched SSID's when some of the client traffic needs to be sent over locally. The Split Tunneling functionality is also an added advantage for Office Extend Access Point (OEAP) setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly once they are mentioned as part of the split tunnel ACL.

The Split Tunneling ACL's can be configured on as per the flexconnect group level, navigate to **Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mapping** as shown in the image.



They can also be configured at as per AP level, navigate to **Wireless > All AP's > AP name > Flexconnect tab > Local Split ACLs** and add the name of the flexconnect ACL as shown in the image.

Split Tunneling ACL's cannot locally bridge Multicast/Broadcast traffic. Multicast/Broadcast traffic is switched centrally even if it matches the FlexConnect ACL.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.