Konfigurieren von Flexconnect ACLs auf dem WLC

Inhalt

Einführung

In diesem Dokument werden die verschiedenen Zugriffskontrolllisten (ACLs) für FlexConnect beschrieben, und es wird erläutert, wie diese auf dem Access Point konfiguriert und validiert werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Wireless LAN Controller (WLC) mit Code 8.3 und höher
- Flexconnect-Konfiguration auf dem WLC

Verwendete Komponenten

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

- Der Cisco WLC der Serie 8540 mit Softwareversion 8.3.133.0.
- 3802- und 3702-APs, die im Flexconnect-Modus ausgeführt werden.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

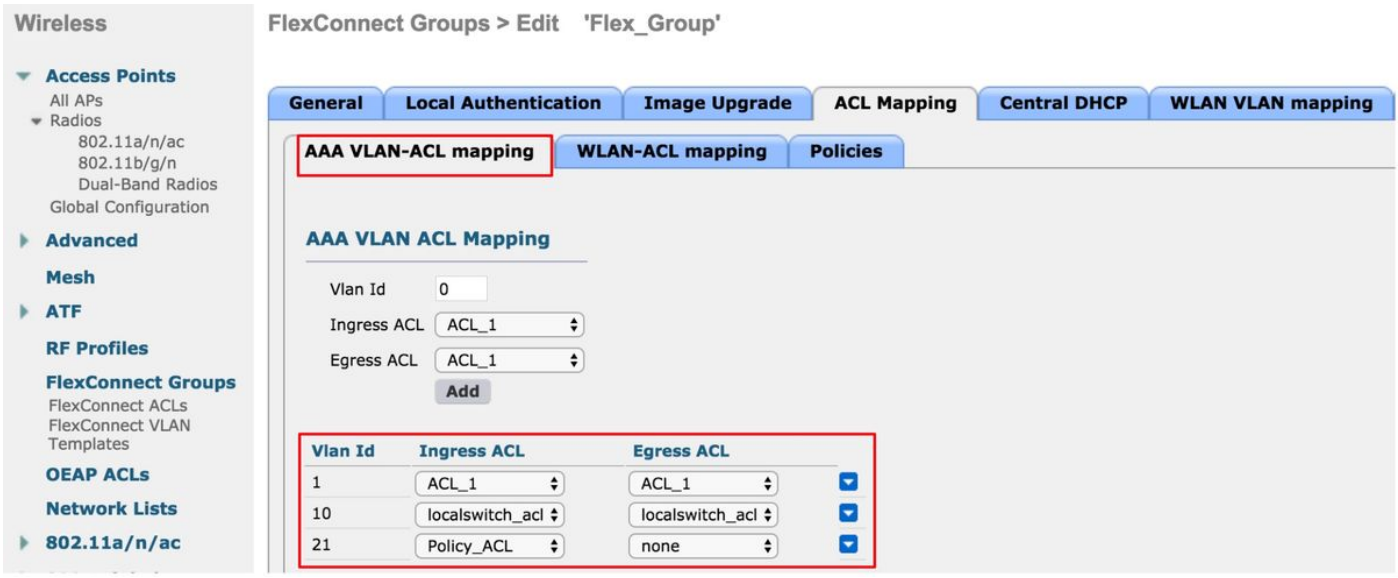
die potenziellen Auswirkungen eines Befehls verstehen.

ACL-Typen

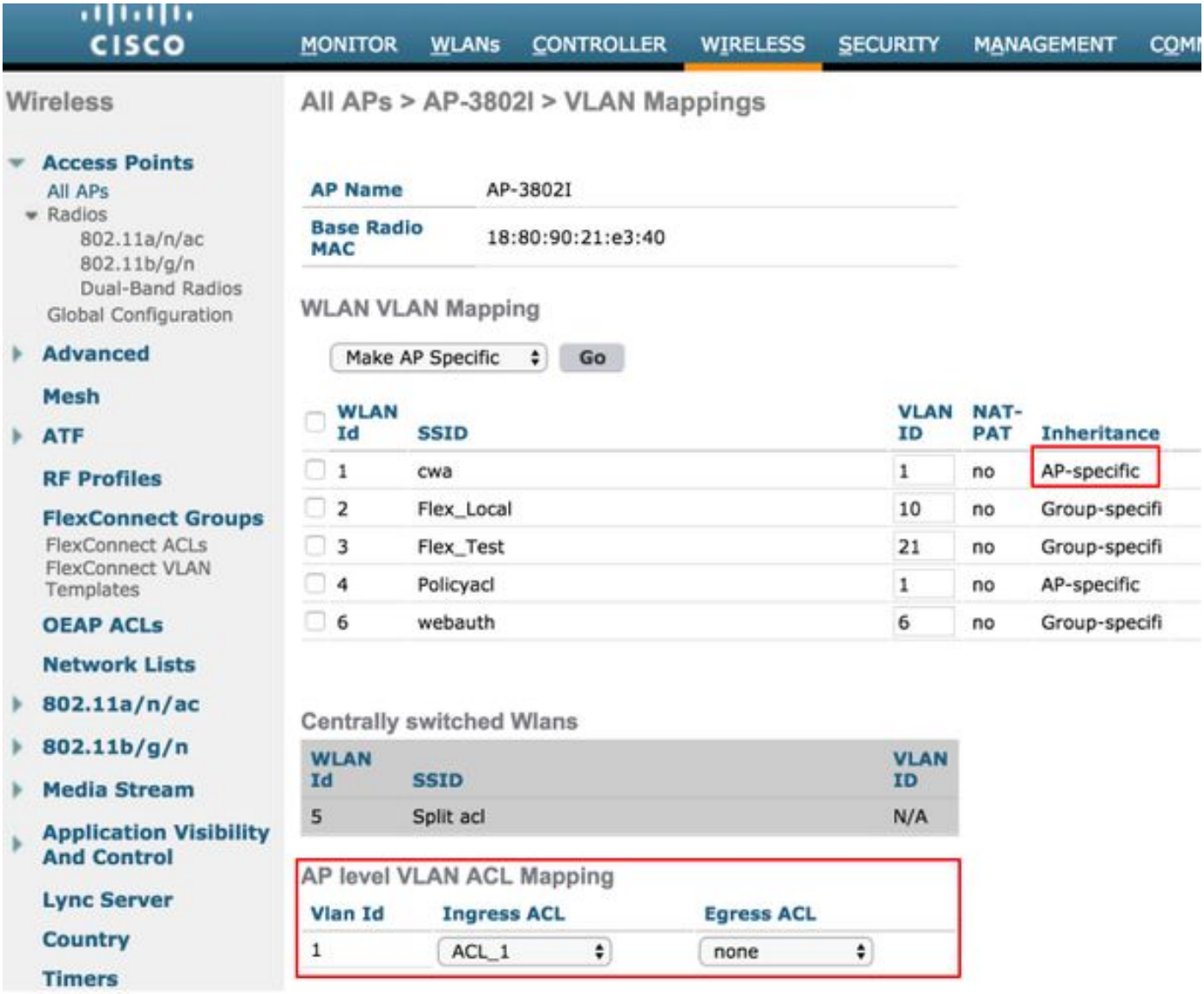
1. VLAN-ACL

VLAN-ACLs sind die am häufigsten verwendete ACL und ermöglichen die Steuerung des Client-Datenverkehrs, der ein- und ausgesendet wird.

Die ACL kann als die Flexconnect-Gruppe konfiguriert werden, die den Bereich für die **AAA-VLAN-ACL-**Zuordnung in **Wireless-FlexConnect Groups > ACL-Zuordnung >** AAA-VLAN-ACL-Zuordnung verwendet, wie im Bild gezeigt.



Sie kann auch auf AP-Ebene konfiguriert werden. Navigieren Sie zu **Wireless > All AP's > AP name > Flexconnect tab,** und klicken Sie auf **VLAN mappings** section. Hier müssen Sie zuerst den VLAN-Konfigurationszugangspunkt spezifisch definieren. Danach können Sie die VLAN-ACL-Zuordnung auf AP-Ebene wie im Bild gezeigt festlegen.



ACL-Richtungen

Sie können auch die Richtung angeben, in der die ACL angewendet wird:

- Eingehend (Eingehend bedeutet für den Wireless-Client)
- Ausgehend (zum DS oder LAN),
- beide oder keine.

Wenn Sie Datenverkehr, der zum Wireless-Client gerichtet ist, blockieren möchten, können Sie die Eingangsrichtung verwenden. Wenn Sie Datenverkehr blockieren möchten, der vom Wireless-Client stammt, können Sie die Ausgangsrichtung verwenden.

Die Option none wird verwendet, wenn Sie eine separate ACL mit der Verwendung von AAA-Überschreibung (Authentication, Authorization, and Accounting) übertragen möchten. In diesem Fall wird die vom Radius-Server gesendete ACL dynamisch auf den Client angewendet.

> **Hinweis**: Die ACL muss zuvor unter der Flexconnect ACL konfiguriert werden, ansonsten wird sie nicht angewendet.

Überlegungen zur ACL-Zuordnung

Wenn Sie VLAN-ACLs verwenden, ist es auch wichtig, diese Überlegungen in Bezug auf VLAN-Zuordnungen auf FlexConnect-APs zu verstehen:

- Wenn das VLAN für die Verwendung der FlexConnect-Gruppe konfiguriert ist, wird die entsprechende für die FlexConnect-Gruppe konfigurierte ACL angewendet.
- Wenn ein VLAN sowohl auf der FlexConnect-Gruppe als auch auf dem AP (als AP-spezifische Konfiguration) konfiguriert ist, hat die Konfiguration der Access Point-Zugriffskontrollliste Vorrang.
- Wenn die AP-spezifische ACL auf none konfiguriert ist, wird keine ACL angewendet.
- Wenn das vom AAA zurückgegebene VLAN im Access Point nicht vorhanden ist, kehrt der Client zum Standard-VLAN zurück, das für das Wireless LAN (WLAN) konfiguriert wurde, und alle diesem Standard-VLAN zugeordneten ACLs haben Vorrang.

Überprüfen, ob die ACL auf den Access Point angewendet wird

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. APs der Phase 2

Bei einem Access Point der Stufe 2 können Sie mithilfe des Befehls **show flexconnect vlan-acl** überprüfen, ob die ACL tatsächlich an den Access Point übertragen wird. Hier sehen Sie auch die Anzahl der weitergeleiteten und verworfenen Pakete für jede 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® APs

Auf AP-Ebene können Sie überprüfen, ob die ACL-Konfiguration auf zwei Arten an den Access Point weitergeleitet wurde:

- Verwenden Sie den Befehl **show access-lists**, der anzeigt, ob alle VLAN-ACLs auf dem Access Point konfiguriert sind:

```
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
```

Sie können auch die Aktivität jeder ACL überwachen, die detaillierte Ausgabe dieser ACL prüfen und die Trefferanzahl für jede Leitung anzeigen:

```
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)
```

- Da die VLAN-ACLs auf die Gigabit-Schnittstelle angewendet werden, können Sie überprüfen, ob die ACL korrekt angewendet wurde. Überprüfen Sie die Ausgabe der Subschnittstelle, wie hier gezeigt:

```
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
```

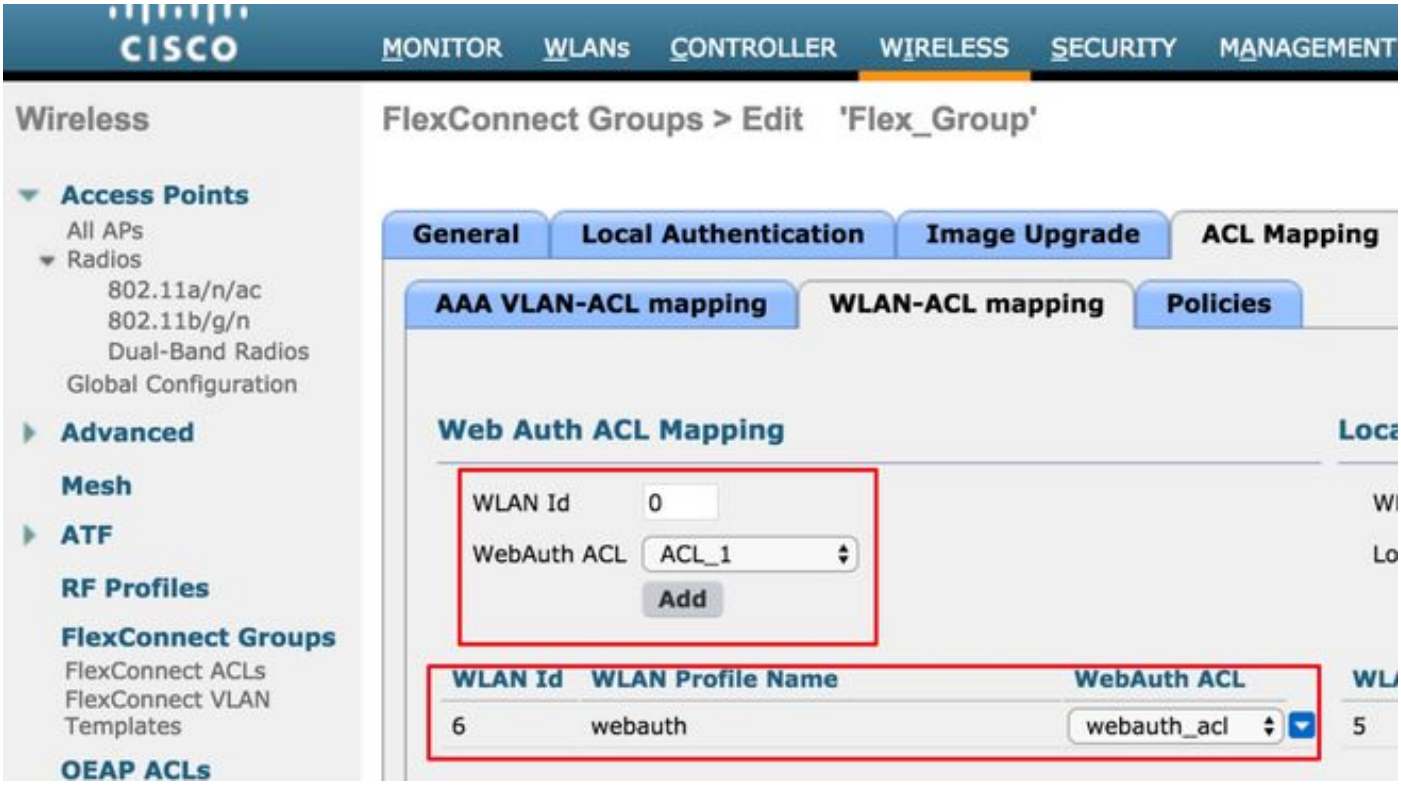
2. Webauth-ACL

Die Webauth-ACL wird bei einem Webauth/Webpassthrough Service Set Identifier (SSID) verwendet, der für das lokale FlexConnect-Switching aktiviert wurde. Diese wird als Pre-Authentication-ACL verwendet und ermöglicht den Client-Datenverkehr zum Umleitungsserver. Wenn die Umleitung abgeschlossen ist und sich der Client im **RUN-**Zustand befindet, wird die ACL beendet, um sie in Kraft zu setzen.

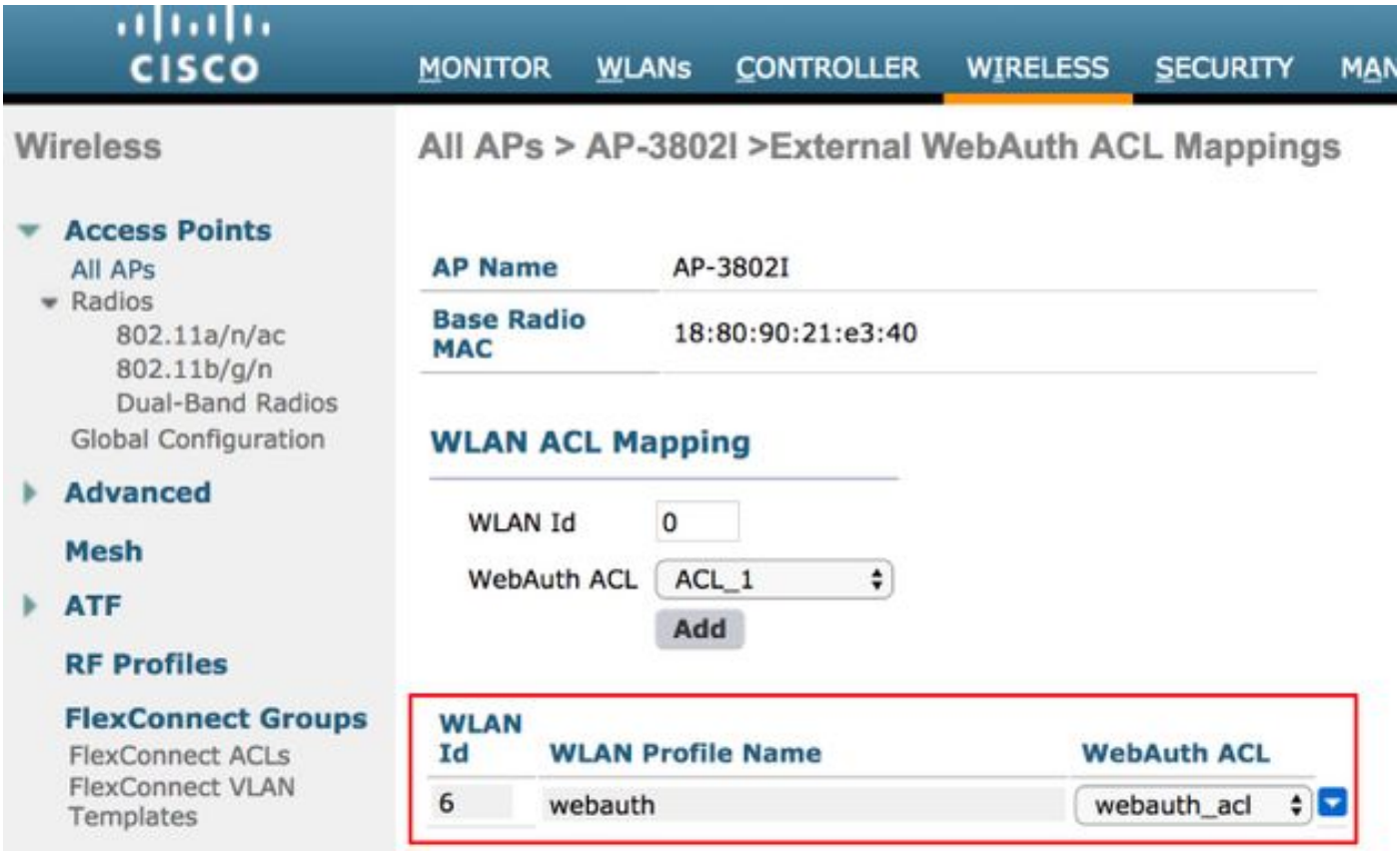
Die Webauth-ACL kann entweder auf WLAN-, AP- oder Flexconnect-Gruppenebene angewendet werden. Eine AP-spezifische ACL hat die höchste Priorität, die WLAN-ACL hingegen die niedrigste. Wenn alle drei Kriterien angewendet werden, hat AP-Specific Vorrang, gefolgt von Flex ACL und dann WLAN Global Specific ACL.

Es können maximal 16 Web-Auth-ACLs für einen Access Point konfiguriert werden.

Sie kann auf die Flexconnect-Gruppenebene angewendet werden. Navigieren Sie zu **Wireless > Flexconnect Groups > Wählen Sie die Gruppe aus, die konfiguriert werden soll > ACL-Zuordnung > WLAN-ACL-Zuordnung > Web Auth ACL-Zuordnung** wie im Bild gezeigt.



Die ACL kann auf AP-Ebene angewendet werden. Navigieren Sie zu **Wireless >Alle APs >AP-Name >Flexconnect-Registerkarte > Externe WebAuthentication ACLs > WLAN ACL,** wie im Bild gezeigt.



Die ACL kann auf WLAN-Ebene angewendet werden. Navigieren Sie zu **WLAN > WLAN_ID > Layer 3 > WebAuth FlexAcl,** wie im Bild gezeigt.

Auf dem Cisco IOS® AP können Sie überprüfen, ob die ACL auf den Client angewendet wurde. Überprüfen Sie die Ausgabe von **show controller dot11radio 0 client** (oder 1, wenn der Client eine Verbindung mit dem A-Radio herstellt) wie folgt:

```
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
```

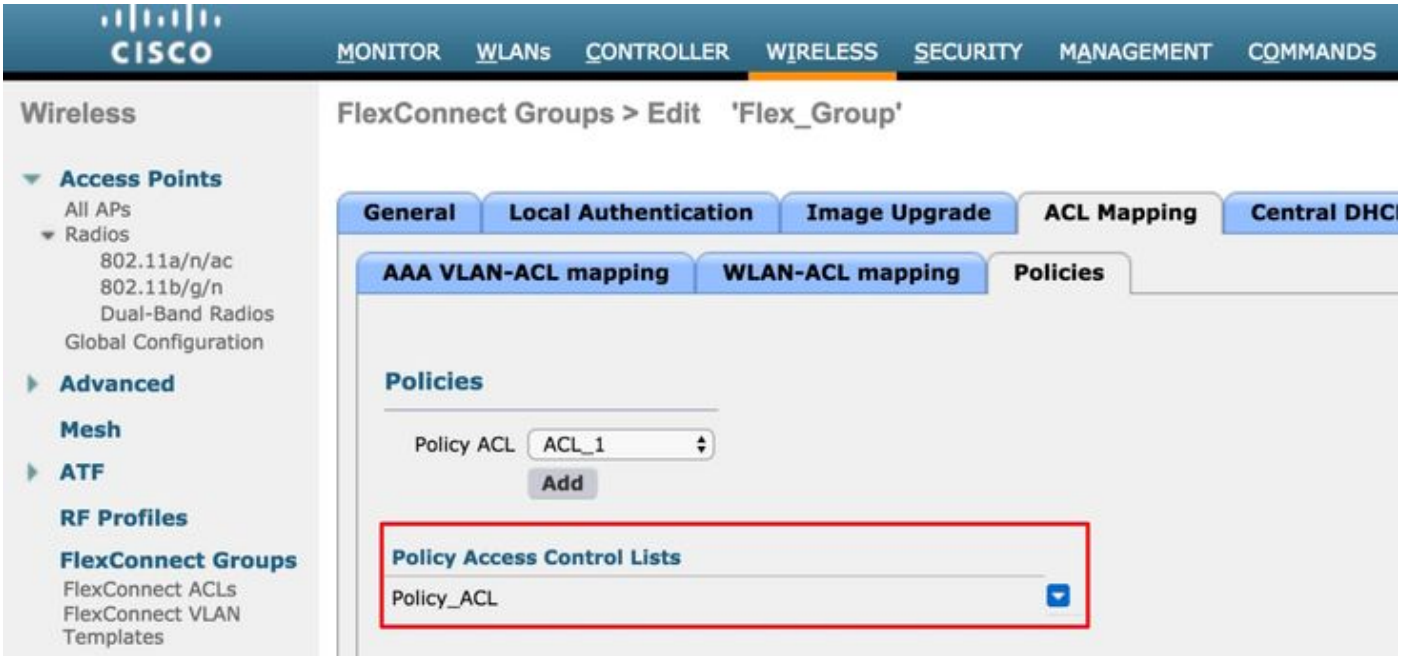
3. Webrichtlinien-ACL

Die WebPolicy-ACL wird für die bedingte Web-Umleitung, die Splash Page-Webumleitung und zentrale Webauth-Szenarien verwendet.

Für WebPolicy-WLANs mit Flex ACLs stehen zwei Konfigurationsmodi zur Verfügung:

1. Flexconnect-Gruppe

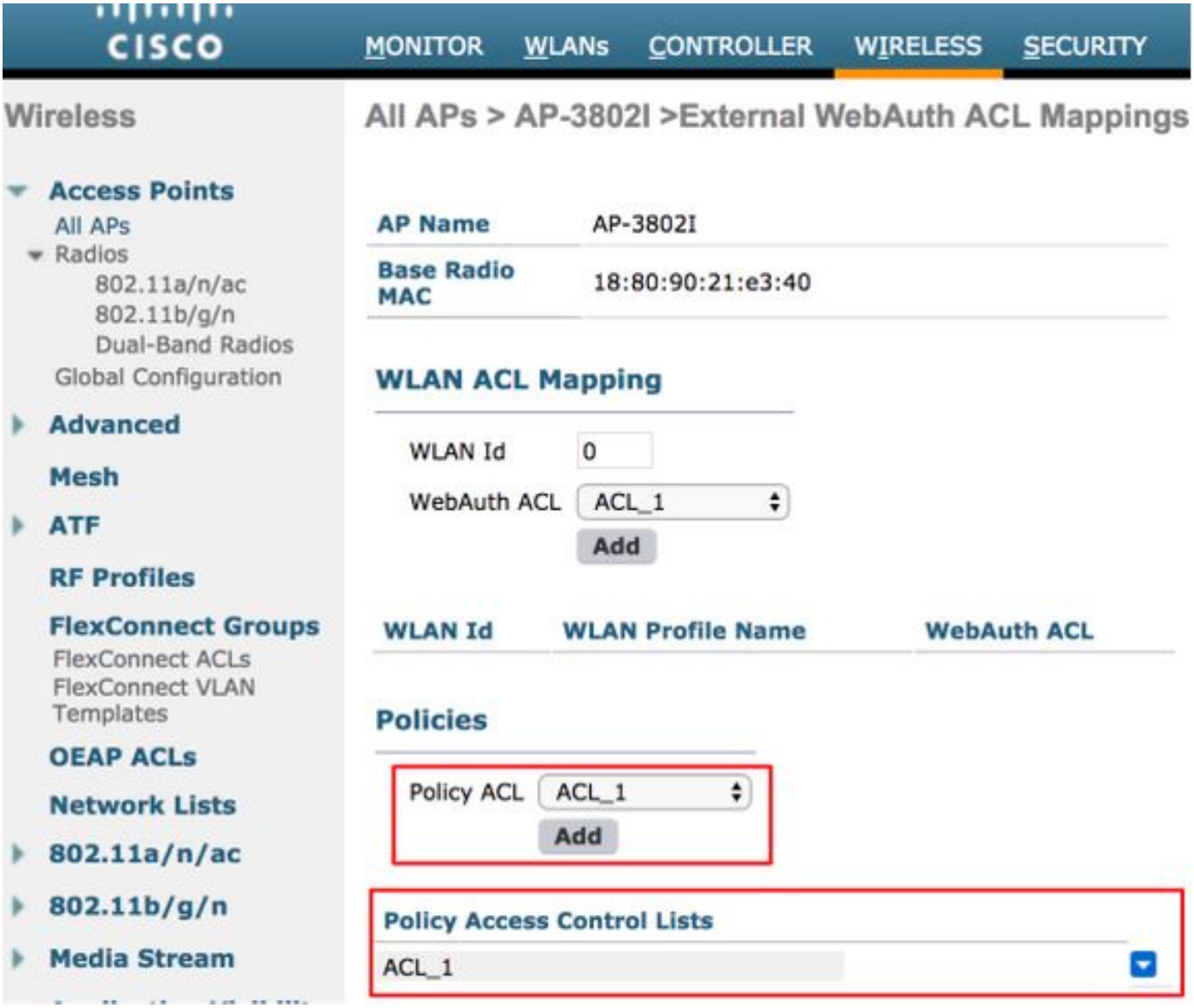
Alle APs in der FlexConnect-Gruppe erhalten die konfigurierte ACL. Dies kann konfiguriert werden, wenn Sie zu **Wireless-Flexconnect-Gruppen** navigieren **> Wählen Sie die Gruppe aus, die konfiguriert werden soll > ACL-Zuordnung > Richtlinien**, und fügen Sie den Namen der Richtlinie-ACL hinzu, wie im Bild gezeigt:



2. AP-spezifisch

Der Access Point, für den die Konfiguration erfolgt, empfängt die ACL, keine anderen Access Points sind betroffen. Dies kann konfiguriert werden, wenn Sie zu **Wireless > All APs > AP name >** navigieren.

Flexconnect-Registerkarte > External WebAuthentication ACLs > Policies (Richtlinien) wie im Bild dargestellt



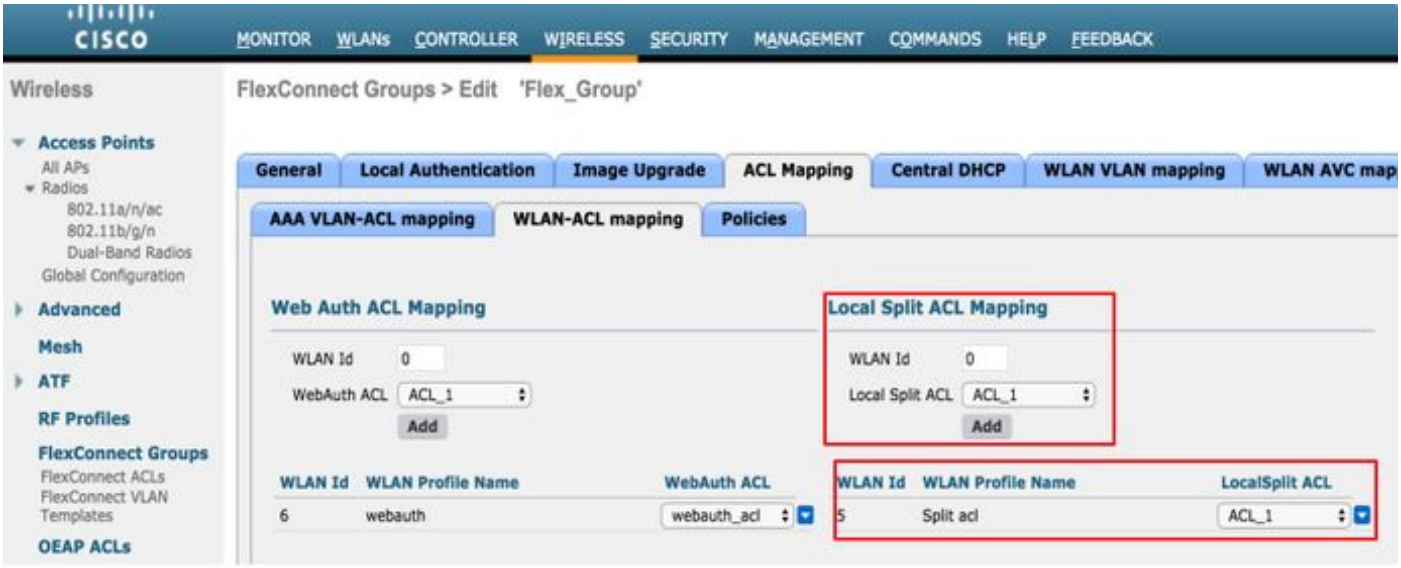
Wenn der Radius-Server nach einer erfolgreichen L2-Authentifizierung den ACL-Namen im AV-Paar für die Umleitung sendet, wird dieser direkt auf den Client auf dem Access Point angewendet. Wenn der Client in den **RUN-**Status wechselt, wird der gesamte Client-Datenverkehr lokal geswitcht, und der Access Point stoppt die Anwendung der ACL.

Es können maximal 32 WebPolicy-ACLs für einen Access Point konfiguriert werden. 16 AP-spezifisch und 16 FlexConnect-gruppenspezifisch

4. Split-Tunnel-ACL

Split Tunneling-ACLs werden mit zentral geswitchten SSIDs verwendet, wenn ein Teil des Client-Datenverkehrs lokal gesendet werden muss. Die Split Tunneling-Funktion bietet außerdem einen zusätzlichen Vorteil für Office Extend Access Point (OEAP)-Konfigurationen, bei denen Clients einer Unternehmens-SSID direkt mit Geräten in einem lokalen Netzwerk (Drucker, kabelgebundene Systeme an einem Remote-LAN-Port oder Wireless-Geräte an einem Personal-SSID) kommunizieren können, sobald sie als Teil der Split-Tunnel-ACL erwähnt werden.

Die Split Tunneling-ACLs können auf der Flexconnect-Gruppenebene konfiguriert werden. Navigieren Sie zu **Wireless-Flexconnect-Gruppen > Wählen Sie die Gruppe aus, die konfiguriert werden soll > ACL-Zuordnung > WLAN-ACL-Zuordnung > Lokale Split ACL-Zuordnung** wie im Bild gezeigt.



Sie können auch auf AP-Ebene konfiguriert werden. Navigieren Sie zu **Wireless > All AP's > AP name > Flexconnect tab > Local Split ACLs** und fügen Sie den Namen der Flexconnect ACL hinzu, wie im Bild gezeigt.

Split Tunneling-ACLs können den Multicast-/Broadcast-Verkehr nicht lokal überbrücken. Multicast-/Broadcast-Datenverkehr wird selbst dann zentral geswitcht, wenn er mit der FlexConnect-ACL übereinstimmt.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.