# Konfigurieren von Flexconnect ACLs auf dem WLC

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten ACL-Typen 1. VLAN-ACL ACL-Richtungen Überlegungen zur ACL-Zuordnung Überprüfen, ob die ACL auf den Access Point angewendet wird 2. Webauth-ACL 3. Webrichtlinien-ACL 4. Split-Tunnel-ACL Fehlerbehebung

# 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.

Wireless	FlexConnect Groups > Edit 'F	lex_Group'			
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> <li>Dual-Band Radios</li> <li>Global Configuration</li> </ul> </li> </ul>	General Local Authentication	Image Upgrade A	ACL Mapping	Central DHCP	WLAN VLAN mapping
Advanced	AAA VLAN ACL Mapping				
Mesh	Vlan Id 0				
▶ ATF	Ingress ACL ACL 1 +				
RF Profiles	Egress ACL ACL 1				
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN	Add		_		
Templates	Vlan Id Ingress ACL	Egress ACL			
OEAP ACLS	1 ACL_1 \$	ACL_1 \$			
Network Lists	10 localswitch_acl 🗘	localswitch_acl \$			
802.11a/n/ac	21 Policy_ACL \$	none 🗘			

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.

	cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANA	GEMENT COM
W	ïreless	All APs	> AP-380	2I > VLAN Ma	ppings			
+	Access Points All APs Radios	AP Name	AP	P-3802I				
	802.11a/n/ac	MAC	18	:80:90:21:e3:40				
	Dual-Band Radios Global Configuration	WLAN VL	AN Mappi	ing				
۲	Advanced	Make	AP Specific	\$ Go				
	Mesh	WLAN	SEID			VLAN	NAT-	Tabaritanca
1	AIF		3310			1	PAI	AP-concific
	RF Profiles	0.	Elev Local	ē		10	110	Group specifi
	FlexConnect Groups	04	Flex_Local	S		10	no	Group-specin
	FlexConnect ACLS FlexConnect VLAN	3	Flex_Test			21	no	Group-specifi
	Templates	4	Policyacl			1	no	AP-specific
	OEAP ACLs	6	webauth			6	no	Group-specifi
	Network Lists							
۲	802.11a/n/ac	Centrally	switched	Wlans				
Þ	802.11b/g/n	WLAN				VLAN		
Þ	Media Stream	Id	SSID			ID		
	Application Visibility And Control	5	Split acl			N/A		
	time Comme	AP level	VLAN ACL	. Mapping				
	Lync Server	Vlan Id	Ingres	S ACL	Egress ACL			
	Country	1	ACL_1		none	•		
	Timers							

#### 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.

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 APspezifische 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.

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROL	LER V	W <u>I</u> RELESS	SECURIT	Y M <u>a</u> na	GEMENT
Wireless	FlexConne	ect Gro	ups > Edi	t 'Fle	ex_Group	•		
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> </ul>	General	Local	Authentic	ation	Image	Upgrade	ACL M	apping
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	AAA VLA	AN-ACL	mapping	WLA	N-ACL ma	pping	Policies	
Advanced Mesh	Web Au	Ith ACL	Mapping	_				Loca
ATF     RF Profiles	WEAN	uth ACL (	ACL_1 Add	•				Lo
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	WLAN I	d WLA	N Profile Na uth	ime		WebAu	th ACL	WL/
OEAP ACLs								_

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.

	cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MA
W	ireless	All APs >	AP-380	2I >External V	VebAuth AC	CL Mapping	js
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> <li>Dual-Band Radios</li> <li>Global Configuration</li> </ul> </li> </ul>		AP Name Base Radio MAC	AP	9-3802I 9:80:90:21:e3:40			
		WLAN AC	L Mapp	ing			
*	Advanced Mesh ATF PE Profiles	WLAN Id WebAuth	0 ACL AC	CL_1 \$			
	FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	WLAN IdWI6we	LAN Prof bauth	ile Name	We	bAuth ACL	

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

cisco	MONITOR V	<u>V</u> LANs <u>C</u> ON	TROLLER	WIRELE	SS <u>S</u> ECL	IRITY M <u>a</u> na	GEMENT	COMMANDS	HELP
WLANs	WLANs > E	dit 'webau	uth'						
WLANS	General	Security	QoS	Policy-	Aapping	Advanced			
Advanced	Layer 2	Layer 3	AAA S	ervers					
WLANS WLANS Advanced	Layer 3 Auth Pass Conc Spla: On N Preauth Sleeping Over-rid	Security Well entication through ditional Web Re sh Page Web R MAC Filter failur entication ACL g Client Er le Global Config	b Policy edirect edirect re <sup>10</sup> IPv4 nable	None 🗘	IPv6 No	ne 🗘 WebAut	h FlexAcl 🤇	Policy_ACL	Ð

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 OFE 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:

	cisco	MONITOR	<u>W</u> LANs		R WIRELESS	SECURITY	MANAGE	MENT	C <u>O</u> MMANDS
W	ireless	FlexConn	ect Gro	ups > Edit	'Flex_Group	o'			
•	Access Points All APs Radios	General	Loca	Authenticat	on Image	Upgrade	ACL Mapp	ping	Central DHC
	802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	AAA VI	LAN-ACL	mapping	WLAN-ACL ma	apping	Policies		
•	Advanced	Policie	es						
	Mesh ATF	Polic	y ACL AC	:L_1 \$)					
	RF Profiles						_		
	FlexConnect Groups	Policy	Access Co	ontrol Lists					
	FlexConnect ACLs FlexConnect VLAN Templates	Policy_	ACL						

#### 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

	CISCO	MONITOR V	<u>V</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY
Wi	reless	All APs > A	P-380	2I >External V	VebAuth A	CL Mappings
*	Access Points	AP Name	AP-	38021		
*	Radios 802.11a/n/ac 802.11b/g/n	Base Radio MAC	18:	80:90:21:e3:40		
	Dual-Band Radios Global Configuration	WLAN ACL	Mappi	ng		
۲	Advanced	WI AN Id	0			
	Mesh	WebAuth A				
۲	ATF	WEDAULI A	Ad	d		
	RF Profiles		C.L.C.			
	FlexConnect Groups	WLAN Id	WLAN	Profile Name	WebA	uth ACL
	FlexConnect ACLs FlexConnect VLAN Templates	Policies				
	OEAP ACLs		_			
	Network Lists	Policy ACL	ACL_1	÷		
•	802.11a/n/ac		Add			
۲	802.11b/g/n	Policy Acces	s Contr	ol Lists		
۲	Media Stream	ACL_1				

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 APspezifisch 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.

CISCO	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMEN	IT COMMANDS HELP FEEDBACK	
Wireless	FlexConnect Groups > Edit 'Flex_Grou	p'		
Access Points     All APs     Padice	General Local Authentication Imag	e Upgrade ACL Mapping	Central DHCP WLAN VLAN m	apping WLAN AVC map
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	AAA VLAN-ACL mapping WLAN-ACL m	Policies		
Advanced	Web Auth ACL Mapping	Loc	cal Split ACL Mapping	
Mesh ATF RF Profiles	WLAN Id 0 WebAuth ACL ACL_1 +	1	ULAN Id 0	
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	WLAN Id WLAN Profile Name 6 webauth	WebAuth ACL W webauth_acl ‡	LAN Id WLAN Profile Name Split acl	LocalSplit ACL
OEAP ACLS				

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.

cisco	MONITOR	WLAN	is <u>C</u> ONT	ROLLER	WIRELESS	SECURITY	M	
Wireless	All APs	> AP-3	802l > Lo	ocal Spl	it ACL Map	pings		
Access Points     All APs     Padios	AP Name	AP Name AP-3802I						
802.11a/n/ac 802.11b/g/n	Base Rac MAC	lio	18:80:90:2	1:e3:40				
Dual-Band Radios Global Configuration	WLAN A	CL Map	ping					
Advanced Mesh	WLAN	Id	0					
ATE	Local-S	plit ACL	L ACL_1 \$					
RF Profiles			Add					
FlexConnect Groups FlexConnect ACLs	WLAN Id	WLAN Pr	ofile Name	2	Loc	al-Split ACL		
FlexConnect VLAN Templates	5 5	Split acl			AC	L_1 \$		

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.