

# WLCでのFlexconnect ACLの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ACLタイプ](#)

[1. VLAN ACL](#)

[ACLの方向](#)

[ACLマッピングの考慮事項](#)

[ACLがAPに適用されているかどうかを確認する](#)

[2. Webauth ACL](#)

[3. WebポリシーACL](#)

[4. スプリットトンネルACL](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、さまざまなFlexconnectアクセスコントロールリスト(ACL)タイプについて説明し、アクセスポイント(AP)で設定および検証する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- コード8.3以降を実行するCisco Wireless LAN Controller(WLC)
- WLCでのFlexconnectの設定

### 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。

- ソフトウェア リリース 8.3.133.0 を実行する Cisco 8540 シリーズ WLC.
- Flexconnectモードで動作する3802および3702 AP。

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。

## ACLタイプ

# 1. VLAN ACL

VLAN ACLは最も一般的に使用されるACLで、VLANに出入りするクライアントトラフィックを制御できます。

ACLは、図に示すように、[Wireless-Flexconnect Groups] > [ACL mapping] > [AAA VLAN-ACL mapping]の[AAA VLAN-ACL mapping]セクションを使用するflexconnectグループごとに設定できます。

The screenshot shows the configuration page for FlexConnect Groups, specifically the 'AAA VLAN-ACL mapping' section. The page has a sidebar on the left with navigation options like 'Access Points', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', and 'Network Lists'. The main content area has tabs for 'General', 'Local Authentication', 'Image Upgrade', 'ACL Mapping', 'Central DHCP', and 'WLAN VLAN mapping'. Under 'ACL Mapping', there are sub-tabs for 'AAA VLAN-ACL mapping', 'WLAN-ACL mapping', and 'Policies'. The 'AAA VLAN-ACL mapping' sub-tab is active and shows a form with 'Vlan Id' set to 0, 'Ingress ACL' set to 'ACL\_1', and 'Egress ACL' set to 'ACL\_1'. Below this is an 'Add' button and a table with columns 'Vlan Id', 'Ingress ACL', and 'Egress ACL'. The table contains three rows: Vlan Id 1 with Ingress ACL 'ACL\_1' and Egress ACL 'ACL\_1'; Vlan Id 10 with Ingress ACL 'localswitch\_acl' and Egress ACL 'localswitch\_acl'; and Vlan Id 21 with Ingress ACL 'Policy\_ACL' and Egress ACL 'none'. Each row has a blue checkmark icon in the right column.

Vlan Id	Ingress ACL	Egress ACL
1	ACL_1	ACL_1
10	localswitch_acl	localswitch_acl
21	Policy_ACL	none

APレベルに応じて設定することもできます。[Wireless] > [All AP's] > [AP name] > [Flexconnect]タブに移動し、[VLAN mappings]セクションをクリックします。ここで、最初にVLAN設定APを特定する必要があります。その後、図に示すように、APレベルのVLAN-ACLマッピングを指定できます。

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COM

Wireless

All APs > AP-3802I > VLAN Mappings

AP Name AP-3802I

Base Radio MAC 18:80:90:21:e3:40

WLAN VLAN Mapping

Make AP Specific Go

WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
<input type="checkbox"/> 1	cwa	1	no	AP-specific
<input type="checkbox"/> 2	Flex_Local	10	no	Group-specifi
<input type="checkbox"/> 3	Flex_Test	21	no	Group-specifi
<input type="checkbox"/> 4	Policyacl	1	no	AP-specific
<input type="checkbox"/> 6	webauth	6	no	Group-specifi

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
5	Split acl	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
1	ACL_1	none

## ACLの方向

ACLを適用する方向を指定することもできます。

- 入力 ( 入力はワイヤレスクライアントに対する意味 )
- 出力 ( DSまたはLANに対して )、
- 両方またはなし

そのため、ワイヤレスクライアント宛てのトラフィックをブロックする場合は入力方向を使用でき、ワイヤレスクライアントから送信されたトラフィックをブロックする場合は出力方向を使用できます。

オプションnoneは、認証、許可、アカウントティング(AAA)オーバーライドを使用して別のACLをプッシュする場合に使用します。この場合、radiusサーバから送信されたACLはクライアントに動的に適用されます。

注：ACLはFlexconnect ACLの下で事前に設定する必要があります。設定しないと適用されません。

## ACLマッピングの考慮事項

VLAN ACLを使用する場合は、flexconnect APのVLANマッピングに関する次の考慮事項を理解することも重要です。

- VLANがFlexConnectグループを使用して設定されている場合、FlexConnectグループに設定されている対応するACLが適用されます。
- VLANがFlexConnectグループとAPの両方に設定されている場合（AP固有の設定として）、AP ACLの設定が優先されます。
- AP固有のACLがnoneに設定されている場合、ACLは適用されません。
- AAAから返されたVLANがAPに存在しない場合、クライアントはワイヤレスLAN(WLAN)に設定されたデフォルトVLANにフォールバックし、そのデフォルトVLANにマッピングされたACLが優先されます。

## ACLがAPに適用されているかどうかを確認する

ここでは、設定が正常に機能しているかどうかを確認します。

### 1. Wave 2 AP

Wave 2 APでは、**show flexconnect vlan-acl**コマンドを使用して、ACLが実際にAPにプッシュされたかどうかを確認できます。ここでは、各ACLの通過パケットと廃棄パケットの数も確認できます。

```
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

APレベルでは、ACL設定が次の2つの方法でAPにプッシュされたかどうかを確認できます。

- **show access-lists**コマンドを使用します。このコマンドは、すべてのVLAN ACLがAPに設定されているかどうかを示します。

```
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
```

また、各ACLで発生するアクティビティを監視し、そのACLの詳細出力をチェックして、各行のヒットカウントを確認することもできます。

```
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)
```

- VLAN ACLはギガビットインターフェイスに適用されるため、ACLが正しく適用されているかどうかを確認できます。次に示すように、サブインターフェイスの出力を確認します。

```
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は、Flexconnectローカルスイッチングが有効になっているWebauth/Webpassthrough Service Set Identifier(SSID)の場合に使用されます。これは事前認証ACLとして使用され、リダイレクトサーバへのクライアントトラフィックを許可します。リダイレクションが完了し、クライアントがRUN状態になると、ACLは停止して有効になります。

Webauth ACLは、WLANレベル、APレベル、またはflexconnectグループレベルで適用できます。AP固有のACLのプライオリティは最も高く、WLAN ACLのプライオリティは最も低くなります。3つすべてが適用されている場合、AP固有が優先され、その後にFlex ACLが続き、次にWLANグローバル固有ACLが続きます。

1つのAPに最大16のWeb認証ACLを設定できます。

図に示すように、Flexconnectグループレベルで適用でき、[Wireless] > [Flexconnect Groups] > [Select the group you want configure] > [ACL mapping] > [WLAN-ACL mapping] > [Web Auth ACL Mapping]に移動します。

Wireless

FlexConnect Groups > Edit 'Flex\_Group'

General Local Authentication Image Upgrade ACL Mapping

AAA VLAN-ACL mapping WLAN-ACL mapping Policies

Web Auth ACL Mapping

WLAN Id 0

WebAuth ACL ACL\_1

Add

WLAN Id	WLAN Profile Name	WebAuth ACL
6	webauth	webauth_acl

ACLはAPレベルで適用できます。図に示すように、[Wireless] > [All AP's] > [AP name] > [Flexconnect]タブ> [External WebAuthentication ACLs] > [WLAN ACL]に移動します。

Wireless

All APs > AP-3802I > External WebAuth ACL Mappings

AP Name AP-3802I

Base Radio MAC 18:80:90:21:e3:40

WLAN ACL Mapping

WLAN Id 0

WebAuth ACL ACL\_1

Add

WLAN Id	WLAN Profile Name	WebAuth ACL
6	webauth	webauth_acl

ACLはWLANレベルで適用できます。図に示すように、[WLAN] > [WLAN\_ID] > [Layer 3] > [WebAuth FlexAcl]に移動します。



The screenshot displays the Cisco FlexConnect Groups configuration interface. The main content area is titled 'FlexConnect Groups > Edit 'Flex\_Group''. The 'Policies' tab is active, showing a 'Policy ACL' dropdown menu set to 'ACL\_1' and an 'Add' button. Below this, a table titled 'Policy Access Control Lists' is highlighted with a red box, containing one entry: 'Policy\_ACL' with a blue checkmark icon. The left sidebar shows the 'Wireless' menu with 'FlexConnect Groups' expanded, listing 'FlexConnect ACLs', 'FlexConnect VLAN', and 'Templates'.

## 2. AP固有

設定を行ったAPはACLを受信しますが、他のAPは影響を受けません。これは、[Wireless] > [All APs] > [AP name] >

図に示すように、[Flexconnect]タブ> [External WebAuthentication ACLs] > [Policies]を選択します

。

The screenshot shows the Cisco Wireless Controller configuration interface. The breadcrumb navigation is "All APs > AP-3802I > External WebAuth ACL Mappings". The left sidebar shows the navigation menu with "Wireless" selected. The main content area is divided into sections:

- AP Information:** AP Name: AP-3802I, Base Radio MAC: 18:80:90:21:e3:40.
- WLAN ACL Mapping:** WLAN Id: 0, WebAuth ACL: ACL\_1. There is an "Add" button below the dropdown.
- Policies:** Policy ACL: ACL\_1. There is an "Add" button below the dropdown.
- Policy Access Control Lists:** A table listing ACL\_1 with a dropdown arrow on the right.

L2認証が成功した後、radiusサーバがredirect-acl AVペアでACL名を送信すると、これはAP上のクライアントに直接適用されます。クライアントがRUN状態になると、すべてのクライアントトラフィックがローカルにスイッチングされ、APはACLの適用を停止します。

1つのAPに最大または32個のWebPolicy ACLを設定できます。16個のAP固有および16個のFlexConnectグループ固有です。

#### 4. スプリットトンネルACL

スプリットトンネリングACLは、クライアントトラフィックの一部をローカルに送信する必要がある場合に、中央でスイッチングされるSSIDとともに使用されます。スプリットトンネリング機能は、スプリットトンネルACLの一部として指定された企業SSID上のクライアント（プリンタ、リモートLANポート上の有線マシン、またはパーソナルSSID上の無線デバイス）がローカルネットワーク上のデバイスと直接通信できるOffice Extend Access Point(OEAP)設定のこの機能です。

スプリットトンネリングACLは、Flexconnectグループレベルに従って設定できます。図に示すように、Wireless-Flexconnect Groups > Select the group you want configure > ACL mapping > WLAN-ACL mapping > Local Split ACL Mappingに移動します。

FlexConnect Groups > Edit 'Flex\_Group'

General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC map

AAA VLAN-ACL mapping WLAN-ACL mapping Policies

Web Auth ACL Mapping

WLAN Id 0  
WebAuth ACL ACL\_1  
Add

Local Split ACL Mapping

WLAN Id 0  
Local Split ACL ACL\_1  
Add

WLAN Id	WLAN Profile Name	WebAuth ACL	LocalSplit ACL
6	webauth	webauth_acl	
5	Split acl		ACL_1

これらはAPレベルで設定することも可能で、Wireless > All AP's > AP name > Flexconnect tab > Local Split ACLsに移動して、図に示すようにflexconnect ACLの名前を追加します。

All APs > AP-3802I > Local Split ACL Mappings

AP Name AP-3802I

Base Radio MAC 18:80:90:21:e3:40

WLAN ACL Mapping

WLAN Id 0  
Local-Split ACL ACL\_1  
Add

WLAN Id	WLAN Profile Name	Local-Split ACL
5	Split acl	ACL_1

スプリットトンネリングACLでは、マルチキャスト/ブロードキャストトラフィックをローカルでブリッジすることはできません。マルチキャスト/ブロードキャストトラフィックは、FlexConnect ACLと一致する場合でも、中央でスイッチングされます。

## トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。