



## Configuring AAA Overrides for FlexConnect

- [Information About Authentication, Authorization, Accounting Overrides, page 1](#)
- [Restrictions for AAA Overrides for FlexConnect, page 2](#)
- [Configuring AAA Overrides for FlexConnect on an Access Point \(GUI\), page 3](#)
- [Configuring VLAN Overrides for FlexConnect on an Access Point \(CLI\), page 4](#)

## Information About Authentication, Authorization, Accounting Overrides

The Allow Authentication, Authorization, Accounting (AAA) Override option of a WLAN enables you to configure the WLAN for authentication. It enables you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

AAA overrides for FlexConnect access points introduce a dynamic VLAN assignment for locally switched clients. AAA overrides for FlexConnect also support fast roaming (Opportunistic Key Caching [OKC]/ Cisco Centralized Key management [CCKM]) of overridden clients.

VLAN overrides for FlexConnect are applicable for both centrally and locally authenticated clients. VLANs can be configured on FlexConnect groups.

If a VLAN on the AP is configured using the WLAN-VLAN, the AP configuration of the corresponding ACL is applied. If the VLAN is configured using the FlexConnect group, the corresponding ACL configured on the FlexConnect group is applied. If the same VLAN is configured on the FlexConnect group and also on the AP, the AP configuration, with its ACL takes precedence. If there is no slot for a new VLAN from the WLAN-VLAN mapping, the latest configured FlexConnect group VLAN is replaced.

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 WLAN.

Before configuring a AAA override, the VLAN must be created on the access points. These VLANs can be created by using the existing WLAN-VLAN mappings on the access points, or by using the FlexConnect group VLAN-ACL mappings.

### AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override

attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled. The AAA attribute for an IPv6 ACL is *Airespace-IPv6-ACL-Name* similar to the *Airespace-ACL-Name* attribute used for provisioning an IPv4-based ACL. The AAA attribute returned contents should be a string that is equal to the name of the IPv6 ACL as configured on the controller.

### AAA Overrides of Bidirectional Rate Limiting on an AP and Controller

You can have AAA overrides for FlexConnect APs to dynamically assign QoS levels and/or bandwidth contracts for both locally switched traffic on web-authenticated WLANs and 802.1X-authenticated WLANs. Both upstream and downstream parameters are sent to the corresponding AP.

This table shows the bidirectional rate limiting implementation:

**Table 1: Bidirectional Rate-Limiting Implementation**

Upstream/Downstream	Local Mode	FlexConnect Central Switching	FlexConnect Local Switching	FlexConnect Standalone
Per-Client Downstream	Controller	Controller	AP	AP
Per-Client Upstream	AP	AP	AP	AP

This table shows the order of preference for local and FlexConnect central switching:

**Table 2: Rate-Limiting Parameters**

AAA	QoS Profile of AAA	WLAN	QoS Profile of WLAN	Applied to Client
100 Kbps	200 Kbps	300 Kbps	400 Kbps	100 Kbps
X	—	—	—	200 Kbps
X	X	—	—	300 Kbps
X	X	X	—	400 Kbps
X	X	X	X	Unlimited

## Restrictions for AAA Overrides for FlexConnect

- Before configuring a AAA override, VLANs must be created on the access points. These VLANs can be created by using the existing WLAN-VLAN mappings on the access points, or by using the FlexConnect group VLAN-ACL mappings.
- At any given point, an AP has a maximum of 16 VLANs. First, the VLANs are selected as per the AP configuration (WLAN-VLAN), and then the remaining VLANs are pushed from the FlexConnect group in the order that they are configured or displayed in the FlexConnect group. If the VLAN slots are full, an error message is displayed.
- VLAN, ACL, QoS, Rate limiting are supported with local and central switching WLAN.

- Dynamic VLAN assignment is not supported for web authentication from a controller with Access Control Server (ACS).
- AAA override of bidirectional rate limiting on an AP and the controller is supported on all the following 802.11n nonmesh access points:
  - 1040
  - 1140
  - 1250
  - 1260
  - 1600
  - 2600
  - 3500
  - 3600

This feature is not supported on the mesh and legacy AP platforms:

- 1130
  - 1240
  - 1520
  - 1550
- For bidirectional rate limiting:
    - If bidirectional rate limiting is not present, AAA override cannot occur.
    - The QoS profile of a client can be Platinum even if the QoS profile of the corresponding WLAN is Silver. The AP allows the client to send packets in voice queue. However, Session Initiation Protocol (SIP) snooping is disabled on the WLAN to ensure that the traffic for a SIP client does not go to the voice queue.
    - The ISE server is supported.
    - The upstream rate limit parameter is equal to the downstream parameter, from AAA override.
    - Local authentication is not supported.

## Configuring AAA Overrides for FlexConnect on an Access Point (GUI)

---

### Step 1

Choose **Wireless > All > APs**.

The **All APs** page is displayed. This page lists the access points associated with the controller.

- Step 2** Click the corresponding AP name.
- Step 3** Click the **FlexConnect** tab.
- Step 4** Enter a value for **Native VLAN ID**.
- Step 5** Click the **VLAN Mappings** button to configure the AP VLANs mappings. The following parameters are displayed:
- **AP Name**—The access point name.
  - **Base Radio MAC**—The base radio of the AP.
  - **WLAN-SSID-VLAN ID Mapping**—For each WLAN configured on the controller, the corresponding SSID and VLAN IDs are listed. Change a WLAN-VLAN ID mapping by editing the VLAN ID column for a WLAN.
  - **Centrally Switched WLANs**—If centrally switched WLANs are configured, WLAN-VLAN mapping is listed.
  - **AP Level VLAN ACL Mapping**—The following parameters are available:
    - **VLAN ID**—The VLAN ID.
    - **Ingress ACL**—The Ingress ACL corresponding to the VLAN.
    - **Egress ACL**—The Egress ACL corresponding to the VLAN.
- Change the ingress ACL and egress ACL mappings by selecting the mappings from the drop-down list for each ACL type.
- **Group Level VLAN ACL Mapping**—The following group level VLAN ACL mapping parameters are available:
    - **VLAN ID**—The VLAN ID.
    - **Ingress ACL**—The ingress ACL for this VLAN.
    - **Egress ACL**—The egress ACL for this VLAN.
- Step 6** Click **Apply**.
- 

## Configuring VLAN Overrides for FlexConnect on an Access Point (CLI)

To configure VLAN overrides on a FlexConnect access point, use the following command:

```
config ap flexconnect vlan add vlan-id acl ingress-acl egress-acl ap_name
```