

FlexConnect Security

- FlexConnect Access Control Lists, on page 1
- Authentication, Authorization, Accounting Overrides, on page 6

FlexConnect Access Control Lists

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs enable access control of network traffic. After ACLs are configured on the controller, you can apply them to the management interface, the AP-Manager interface, any of the dynamic interfaces, or a WLAN. ACLs enable you to control data traffic to and from wireless clients or to the controller CPU. You can configure ACLs on FlexConnect access points to enable effective usage and access control of locally switched data traffic on an access point.

The FlexConnect ACLs can be applied to VLAN interfaces on access points in both the Ingress and Egress mode.

Existing interfaces on an access point can be mapped to ACLs. The interfaces can be created by configuring a WLAN-VLAN mapping on a FlexConnect access point.

The FlexConnect ACLs can be applied to an access point's VLAN only if VLAN support is enabled on the FlexConnect access point.

Related Information

- To set up location authentication, see the FlexConnect chapter of the *Enterprise Mobility Design Guide*.
- Wireless BYOD for FlexConnect Deployment Guide

This section contains the following subsections:

Restrictions for FlexConnect Access Control Lists

- FlexConnect ACLs can be applied only to FlexConnect access points. The configurations applied are per AP and per VLAN.
- FlexConnect ACLs are supported on the native VLAN.

Note FlexConnect ACLs are not supported on native VLAN when setting comes from FlexConnect Group.

- You can configure up to 512 ACLs on a Cisco Wireless Controller. Each rule has parameters that affect its action. When a packet matches all the parameters pertaining to a rule, the action set pertaining to that rule is applied to the packet.
  - You can define 64 IPv4 address based rules in each ACL.
- Non-FlexConnect ACLs that are configured on the controller cannot be applied to a FlexConnect AP.
- FlexConnect ACLs do not support direction per rule. Unlike normal ACLs, Flexconnect ACLs cannot be configured with a direction. An ACL as a whole needs to be applied to an interface as ingress or egress.
- All ACLs have an implicit *deny all rule* as the last rule. If a packet does not match any of the rules, it is dropped by the corresponding access point.
- ACLs mapping on the VLANs that are created on an AP using WLAN-VLAN mapping, should be performed on a per-AP basis only. VLANs can be created on a FlexConnect group for AAA override. These VLANs will not have any mapping for a WLAN.
- ACLs for VLANs that are created on a FlexConnect group should be mapped only on the FlexConnect group. If the same VLAN is present on the corresponding AP as well as the FlexConnect group, AP VLAN will take priority. This means that if no ACL is mapped on the AP, the VLAN will not have any ACL, even if the ACL is mapped to the VLAN on the FlexConnect group.
- Ensure the FlexConnect ACL and the regular ACL names are not the same while configuring a WLAN for FlexConnect local switching.
- AAA client ACL support:
  - Before the AAA sends the client ACL, ensure that the ACL is created on a FlexConnect group or an AP. The ACL is not downloaded to the AP dynamically when the client gets associated with the AP.
  - A maximum of 96 ACLs can be configured on an AP. Each ACL can have a maximum of 64 rules.
  - FlexConnect ACLs do not have directions. The entire ACL is applied as ingress or egress.
  - The ACL returned by the AAA is applied on both ingress and egress on the 802.11 side of the client.
- Cisco Wave 2 and 802.11ax APs: When FlexConnect ACLs are applied to both wired and 802.11 interfaces, the client traffic honors only the ACL that is mapped to the 802.11 interface and not the ACL that is mapped to the wired interface.

Note A Local Switching WLAN is configured and ACL is mapped to a FlexConnect group with an ACL. The ACL has set of *deny and permit* rules. When you associate a client to the WLAN, the client needs to have DHCP permit rule added for getting the IP address.

Configuring FlexConnect Access Control Lists (GUI)

Procedure

Step 1 Choose **Security** > **Access Control Lists** > **FlexConnect Access Control Lists**.

The **FlexConnect ACL** page is displayed.

This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow that is next to the corresponding ACL name and choose **Remove**.

Step 2 Add a new ACL by clicking **New**.

The **Access Control Lists** > **New** page is displayed.

Step 3 In the **Access Control List Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

Step 5 Click the name of the new ACL after the **Access Control Lists** page is displayed again.

When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists** > **Rules** > **New** page is displayed.

Step 6 Configure an IP address based rule for a given FlexConnect ACL as follows:

a) Choose **IP Rule** to create an IP address based rule.

The **Access Control Lists** > **Rules** > **New** page is displayed.

b) The controller supports up to 64 rules for each IP address-based ACL. These rules are listed in order from 1 to 64. In the **Sequence** field, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

Note
If rules 1 to 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

c) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- **Any**—Any source (This is the default value.).
- **IP Address**—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding fields.

d) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- **Any**—Any destination (This is the default value.).

- **IP Address**—A specific destination. If you choose this option, enter the IP address and the details of the destination in the relevant fields.

e) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- **Any**—Any protocol (This is the default value.).
- **TCP**
- **UDP**
- **ICMP**—Internet Control Message Protocol
- **ESP**—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Permits or denies IP-in-IP packets
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note
If you choose Other, enter the number of the desired protocol in the **Protocol** field. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified.

If you choose TCP or UDP, two more parameters—Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

f) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header field that can be used to define the quality of service across the Internet.

- **Any**—Any DSCP (This is the default value.).
- **Specific**—A specific DSCP from 0 to 63, which you enter in the **DSCP** field.

g) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or **Permit** to cause this ACL to allow packets. The default value is **Deny**.

h) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

i) Repeat this procedure to add more rules, if required, for this ACL.

Related Topics

Configuring Access Control Lists (GUI)

Configuring FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to configure FlexConnect ACLs:

Procedure

- Create or delete an ACL on a FlexConnect access point by entering this command:

  config flexconnect acl { **create | delete** } *name*

  The IPv4 ACL name of up to 32 characters is supported.

- Associate a FlexConnect ACL to a WLAN.
  a) Enable web authentication by entering this command:

     config wlan security web-auth enable *wlan_id*

  b) Configure the FlexConnect ACL to a WLAN by entering this command:

     config wlan security web-auth flexacl *wlan_id acl_name*

- Configure an IP address based rule for an ACL
  a) Add an IP address based rule to the FlexConnect ACL by entering this command:

     config flexconnect acl rule add *acl-name rule-index*

  b) Configure a rule's source IP address and netmask by entering this command:

     config flexconnect acl rule source address *acl-name rule-index ipv4-addr subnet-mask*

  c) Configure a rule's source port range by entering this command:

     config flexconnect acl rule source port range *acl-name rule-index start-port end-port*

  d) Configure a rule's destination IP address and netmask by entering this command:

     IPv4—**config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask*

  e) Configure a rule's destination port range by entering this command:

     config flexconnect acl rule destination port range*acl-name rule-index start-port end-port*

  f) Configure the rule's IP protocol by entering this command:

     config flexconnect acl rule protocol *acl-name rule-index* **protocol**

     Specify an index value between 0 and 64. Specify the protocol value between 0 and 255 or 'any'. The default is 'any.'

  g) Specify the differentiated services code point (DSCP) value of the rule index by entering this command:

     config flexconnectacl rule dscp *acl-name rule-index dscp-value*

     DSCP is an IP header that can be used to define the quality of service across the Internet. Enter a value between 0 and 63 or the value **any**. The default value is **any**.

h) Set the Permit or deny action to the rule by entering this command:

config flexconnect acl rule actionacl-name *rule-index* **{permit |deny}**

i) Change the index value for an ACL rule by entering this command:

config flexconnectacl rule change index *acl-name old-index new-index*

j) Swap the index values between two rules by entering this command:

config flexconnect acl rule swap *acl-name index-1 index-2*

k) Delete a rule from the FlexConnect ACL by entering this command:

config flexconnect acl rule delete *name*

l) Apply an ACL to the FlexConnect access point by entering this command:

config flexconnect acl apply *acl-name*

- [Optional] Add a VLAN on a FlexConnect access point by entering this command:

  config ap flexconnect vlan add *acl vlan-id ingress-aclname egress-acl-name ap-name*

Related Topics

Configuring Access Control List Rules (CLI)

Viewing and Debugging FlexConnect Access Control Lists (CLI)

Use the following commands on the controller to view information related to FlexConnect ACLs:

Procedure

- **show flexconnect acl summary**—Displays a summary of the ACLs.
- **show client detail** *mac-address*—Displays AAA override ACL.
- **show flexconnect acl detailed acl-name**—Displays the detailed information about the ACL.
- **debug flexconnect acl {enable | disable}**—Enables or disables the debugging of FlexConnect ACL.
- **debug capwap reap**—Enables debugging of CAPWAP.

Authentication, Authorization, Accounting Overrides

The Allow Authentication, Authorization, Accouting (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.

There is an option to select the downstream rate limit through the QoS profile page. Users that already make use of QoS profiles functionality have additional granularity and capabilities.

The trade-off with configuring the rate limits under the QoS profile is that there are only four QoS profiles available. Thus, there are only four sets of configuration options to use.

Also, because the QoS profile is applied to all clients on the associated SSID, all clients connected to the same SSID will have the same rate limited parameters.

Table 1: 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

Important Guidelines

- Rate limiting is supported for APs in Local and FlexConnect mode (both Central and Local switching).
- When the controller is connected and central switching is used, the controller handles the downstream enforcement of per-client rate limit only.
- APs handle the enforcement of the upstream traffic and per-SSID rate limit for downstream traffic.

- For the locally switched environment, both upstream and downstream rate limits will be enforced on the AP. The enforcement on the AP will take place in the dot11 driver. This is where the current classification exists.
- In both directions, per-client rate limit is applied/checked first and per-SSID rate limit is applied/checked second.
- On virtual controller platforms, per-client downstream rate limiting is not supported in FlexConnect central switching.
- The WLAN rate limiting will always supercede the global QoS setting for WLAN and user.
- Rate limiting works only for TCP and UDP traffic. Other types of traffic (IPSec, GRE, ICMP, CAPWAP, etc) cannot be limited.
- Using AVC rule, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting. The per-client downstream rate limits takes precedence over the per-application rate limits.
- Bidirectional rate limiting (BDRL) configuration in a mobility Anchor-Foreign setup needs to be done both on Anchor and Foreign controller. As a best practice, we recommend that you do identical configuration on both the controllers to avoid breakage of any feature.
- Per WLAN BDRL is supported on these currently supported Cisco Wave1 APs: 1600, 2600, 3600, 1700, 2700, 3700, and 3500.
- For information about BDRL support on Cisco Wave 2 APs, see the *FlexConnect Feature Matrix* section in the Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points.
- BDRL is not supported in mesh platforms. On Cisco Virtual Wireless Controller (vWLC), per-client downstream rate limiting is not supported in FlexConnect central switching.
- In Release 8.5, in anchor-foreign scenario with Cisco Wave 2 APs, only per-client downstream works. The per-client upstream, per-SSID downstream, and per-SSID upstream are not supported. However, all of these are supported in Cisco Wave 1 APs.

  In Release 8.8 and later releases, in anchor-foreign scenarios with Cisco Wave 2 and 802.11ax APs, all of per-client upstream and downstream and per-SSID upstream and downstream are supported, provided that the configuration is the same in both and anchor and foreign controllers.

Related Documentation: Wireless Bi-Directional Rate Limiting Deployment Guide

This section contains the following subsections:

Restrictions on 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.

- The AAA ACLs and VLAN ACLs are applied on the client in the following order of precedence:
  - Wave 1 APs: Both the ACLs are active simultaneously on the client.
  - Wave 2 APs: AAA ACLs override the VLAN ACLs on the client.
- 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
  - 1700
  - 2600
  - 2700
  - 3500
  - 3600
  - 3700

  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 a 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.
- If you assign multiple VLAN names to a VLAN ID, the client display represents the first matching VLAN name that is assigned to the VLAN ID.

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

Procedure

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*