



Configuring and Applying Access Control Lists

- [Information about Access Control Lists, on page 1](#)
- [Guidelines and Restrictions on Access Control Lists, on page 1](#)
- [Configuring and Applying Access Control Lists \(GUI\), on page 2](#)
- [Configuring and Applying Access Control Lists \(CLI\), on page 6](#)
- [Configuring Layer 2 Access Control Lists, on page 8](#)

Information about 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). After ACLs are configured on the controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

You may also want to create a preauthentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

Both IPv4 and IPv6 ACL are supported. IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.



Note You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Guidelines and Restrictions on Access Control Lists

- You can define up to 64 ACLs, each with up to 64 rules (or filters) for both IPv4 and IPv6. Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet.
- When you apply CPU ACLs on a Cisco 5508 WLC or a Cisco WiSM2, you must permit traffic towards the virtual interface IP address for web authentication.
- 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 controller.

- If you are using an external web server with a Cisco 5508 WLC or a WLC network module, you must configure a preauthentication ACL on the WLAN for the external web server.
- Multicast traffic received from wired networks that is destined to wireless clients is not processed by WLC ACLs. Multicast traffic initiated from wireless clients, destined to wired networks or other wireless clients on the same controller, is processed by WLC ACLs.
- ACLs are configured on the controller directly or configured through Cisco Prime Infrastructure templates. The ACL name must be unique.
- You can configure ACL per client (AAA overridden ACL) or on either an interface or a WLAN. The AAA overridden ACL has the highest priority. However, each interface, WLAN, or per client ACL configuration that you apply can override one another.
- If peer-to-peer blocking is enabled, traffic is blocked between peers even if the ACL allows traffic between them.
- When you create an ACL, it is recommended to perform the two actions (create an ACL or ACL rule and apply the ACL or ACL rule) continuously either from CLI or GUI.
- Mobility pings on ports 16666 and 16667 are notable exemptions and these ports cannot be blocked by any ACL.
- When high priority for an ACL is enabled, two types of rules are possible as follows:
 - **Deny:** If you add the *Deny* rule, all the relevant services under the rule are blocked or disabled. This does not depend on the configuration status of the services.
 - **Permit:** If you add the *Permit* rule, all the relevant services might require more configuration that are based on the nature of the service, for the service to be functional. For example, Telnet/SSH do not require more configuration for their services to be functional, whereas HTTP/HTTPS do require more configuration for their services to be functional.
- ACLs do not affect the service ports of controllers.
- URL domain configuration for IPv6 ACLs is not supported. However, it is supported in the case of IPv4 ACLs.

Configuring and Applying Access Control Lists (GUI)

Configuring Access Control Lists (GUI)

-
- Step 1** Choose **Security > Access Control Lists > Access Control Lists** to open the Access Control Lists page.
- Step 2** If you want to see if packets are hitting any of the ACLs configured on your controller, select the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unselected, which is the default value. This feature is useful when troubleshooting your system.
- Note** If you want to clear the counters for an ACL, hover your cursor over the blue drop-down arrow for that ACL and choose **Clear Counters**.
- Step 3** Add a new ACL by clicking **New**. The Access Control Lists > New page appears.

- Step 4** In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.
- Step 5** Choose the ACL type. There are two types of ACL supported, IPv4 and IPv6.
- Step 6** Click **Apply**. When the Access Control Lists page reappears, click the name of the new ACL.
- Step 7** When the Access Control Lists > Edit page appears, click **Add New Rule**. The Access Control Lists > Rules > New page appears.
- Step 8** Configure a rule for this ACL as follows:
- The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, 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 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number for a rule, the sequence numbers for other rules adjust 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.
 - From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:
 - 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 text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.
 - 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 netmask of the destination in the text boxes. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination in the text boxes.
 - From the Protocol drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:
 - Any**—Any protocol (this is the default value)
 - TCP**—Transmission Control Protocol
 - UDP**—User Datagram Protocol
 - ICMP/ICMPv6**—Internet Control Message Protocol
Note ICMPv6 is only available for IPv6 ACL.
 - ESP**—IP Encapsulating Security Payload
 - AH**—Authentication Header
 - GRE**—Generic Routing Encapsulation
 - IP in IP**—Internet Protocol (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 text box. You can find the list of available protocols in the INAI website.

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

- e) If you chose TCP or UDP in the previous step, two additional parameters appear: Source Port and Destination Port. These parameters enable you to choose a specific source port and destination port or port ranges. 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.

Note Source and Destination ports based on the ACL type.

- 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 text box 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 edit box

- g) From the **Direction** drop-down list, choose one of these options to specify the direction of the traffic to which this ACL applies:

- **Any**—Any direction (this is the default value)
- **Inbound**—From the client
- **Outbound**—To the client

Note If you are planning to apply this ACL to the controller CPU, the packet direction does not have any significance, it is always 'Any'.

- h) 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.
- i) Click **Apply** to commit your changes. The **Access Control Lists > Edit** page reappears, showing the rules for this ACL.

The **Deny Counters** fields shows the number of times that packets have matched the explicit deny ACL rule. The **Number of Hits** field shows the number of times that packets have matched an ACL rule. You must enable ACL counters on the Access Control Lists page to enable these fields.

Note If you want to edit a rule, click the sequence number of the desired rule to open the **Access Control Lists > Rules > Edit** page. If you want to delete a rule, hover your cursor over the blue drop-down arrow for the desired rule and choose **Remove**.

- j) Repeat this procedure to add any additional rules for this ACL.

Step 9 Click **Save Configuration** to save your changes.

Step 10 Repeat this procedure to add any additional ACLs.

Applying an Access Control List to an Interface (GUI)

- Step 1** Choose **Controller > Interfaces**.
- Step 2** Click the name of the desired interface. The **Interfaces > Edit** page for that interface appears.
- Step 3** Choose the desired ACL from the ACL Name drop-down list and click **Apply**. The default is None.
- Note** IPv6 ACLs are supported only on management interface.
- Step 4** Click **Save Configuration** to save your changes.
-

Applying an Access Control List to the Controller CPU (GUI)

Before you begin

Before you apply ACL rules, ensure that you have explicitly set the following RRM ports to *allow* in the CPU ACL:

- 12124-12125
- 12134-12135

Also ensure that you add these ACL rules specifically at the top of the ACL list.

If you do not set these RRM ports to *allow*, the ports are blocked by default.

- Step 1** Choose **Security > Access Control Lists > CPU Access Control Lists** to open the CPU Access Control Lists page.
- Step 2** Select the **Enable CPU ACL** check box to enable a designated ACL to control the IPv4 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.
- Step 3** From the **ACL Name** drop-down list, choose the ACL that will control the IPv4 traffic to the controller CPU. *None* is the default value when the CPU ACL feature is disabled. If you choose *None* while the **Enable CPU ACL** check box is selected, an error message appears indicating that you must choose an ACL.
- Note** This parameter is available only if you have selected the **CPU ACL Enable** check box.
- Note** When CPU ACL is enabled, it is applicable to both wireless and wired traffic.
- Step 4** Select the **Enable CPU IPv6 ACL** check box to enable a designated ACL to control the IPv6 traffic to the controller CPU or unselect the check box to disable the CPU ACL feature and remove any ACL that had been applied to the CPU. The default value is unselected.
- Note** For CPU IPv6 ACL, along with permit rules for HTTP/Telnet, you must add a rule to allow ICMPv6 (NA/ND uses ICMPv6) for the CPU IPv6 ACLs to work.
- Step 5** From the **IPv6 ACL Name** drop-down list, choose the ACL that will control the IPv6 traffic to the controller CPU. *None* is the default value when the CPU ACL feature is disabled. If you choose *None* while the **Enable CPU IPv6 ACL** check box is selected, an error message appears indicating that you must choose an ACL.
- Step 6** Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Applying an Access Control List to a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Step 4 From the **Override Interface ACL** drop-down list, choose the IPv4 or IPv6 ACL that you want to apply to this WLAN. The ACL that you choose overrides any ACL that is configured for the interface. None is the default value.

Note To support centralized access control through AAA server such as ISE or ACS, IPv6 ACL must be configured on the controller and the WLAN must be configured with AAA override enabled feature.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Applying a Preauthentication Access Control List to a WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Security** and **Layer 3** tabs to open the **WLANs > Edit (Security > Layer 3)** page.

Step 4 Select the **Web Policy** check box.

Step 5 From the **Preauthentication ACL** drop-down list, choose the desired ACL and click **Apply**. None is the default value.

Step 6 Save the configuration.

Configuring and Applying Access Control Lists (CLI)

Configuring Access Control Lists (CLI)

Step 1 See all of the ACLs that are configured on the controller by entering this command:

```
show [ipv6] acl summary
```

Step 2 See detailed information for a particular ACL by entering this command:

```
show [ipv6] acl detailed acl_name
```

The Counter text box increments each time a packet matches an ACL rule, and the DenyCounter text box increments each time a packet does not match any of the rules.

Note If a traffic/request is allowed from the controller by a permit rule, then the response to the traffic/request in the opposite direction also is allowed and cannot be blocked by a deny rule in the ACL.

Step 3 Enable or disable ACL counters for your controller by entering this command:

```
config acl counter {start | stop}
```

Note If you want to clear the current counters for an ACL, enter the **clear acl counters** *acl_name* command.

Step 4 Add a new ACL by entering this command:

```
config [ipv6] acl create acl_name.
```

You can enter up to 32 alphanumeric characters for the *acl_name* parameter.

Note When you try to create an interface name with space, the controller CLI does not create an interface. For example, if you want to create an interface name int 3, the CLI will not create this since there is a space between int and 3. If you want to use int 3 as the interface name, you need to enclose within single quotes like 'int 3'.

Step 5 Add a rule for an ACL by entering this command:

```
config [ipv6] acl rule add acl_name rule_index
```

Step 6 Configure an ACL rule by entering **config [ipv6] acl rule** command:

Step 7 Save your settings by entering this command:

```
save config
```

Note To delete an ACL, enter the **config [ipv6] acl delete** *acl_name* command. To delete an ACL rule, enter the **config [ipv6] acl rule delete** *acl_name rule_index* command.

Applying Access Control Lists (CLI)

Step 1 Perform the following to apply an IPv4 ACL:

- To apply an ACL to the IPv4 data path, enter this command:

```
config acl apply acl_name
```

- To apply an ACL to the controller CPU to restrict the IPv4 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:

```
config acl cpu acl_name {wired | wireless | both}
```

Note To see the ACL that is applied to the controller CPU, enter the **show acl cpu** command. To remove the ACL that is applied to the controller CPU, enter the **config acl cpu none** command.

Note For 2504 and 4400 series WLC, the CPU ACL cannot be used to control the CAPWAP traffic. Use the access-list on the network to control CAPWAP traffic.

Step 2 Perform the following to apply an IPv6 ACL:

- To apply an ACL to an IPv6 data path, enter this command:

config ipv6 acl apply name

- To apply an ACL to the controller CPU to restrict the IPv6 type of traffic (wired, wireless, or both) reaching the CPU, enter this command:

```
config ipv6 acl cpu {name|none}
```

Step 3 To apply an ACL to a WLAN, enter this command:

- **config wlan acl** *wlan_id acl_name*

Note To see the ACL that is applied to a WLAN, enter the **show wlan** *wlan_id command*. To remove the ACL that is applied to a WLAN, enter the **config wlan acl** *wlan_id none* command.

Step 4 To apply a pre-authentication ACL to a WLAN, enter this command:

- **config wlan security web-auth acl** *wlan_id acl_name*

Step 5 Save your changes by entering this command:

```
save config
```

Configuring Layer 2 Access Control Lists

Layer 2 Access Control Lists

You can configure rules for Layer 2 access control lists (ACLs) based on the Ethertype associated with the packets. Using this feature, if a WLAN with central switching is required to support only PPPoE clients, you can apply Layer 2 ACL rules on the WLAN to allow only PPPoE packets after the client is authenticated and the rest of the packets are dropped. Similarly, if the WLAN is required to support only IPv4 clients or only IPv6 clients, you can apply Layer 2 ACL rules on the WLAN to allow only IPv4 or IPv6 packets after the client is authenticated and the rest of the packets are dropped. For a locally-switched WLAN, you can apply the same Layer 2 ACL either for the WLAN or a FlexConnect AP. AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs. The Layer 2 ACL that is applied to the FlexConnect AP takes precedence over the Layer 2 ACL that is applied to the WLAN.

In a mobility scenario, the mobility anchor configuration is applicable.

The following traffic is not blocked:

- Wireless traffic for wireless clients:
 - 802.1X
 - Inter-Access Point Protocol
 - 802.11
 - Cisco Discovery Protocol
- Traffic from a distributed system:
 - Broadcast

- Multicast
- IPv6 Neighbor Discovery Protocol (NDP)
- Address Resolution Protocol (ARP) and Gratuitous ARP Protection (GARP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)

Layer 2 ACL Mapping to WLAN

If you map a Layer 2 ACL to a WLAN, the Layer 2 ACL rules that you configure apply to all the clients that are associated with that WLAN.

When you map a Layer 2 ACL to a centrally switched WLAN, the rule to pass traffic based on the Ethertype is determined by Fast-Path for every client that is associated with the WLAN. Fast-Path looks into the Ethernet headers associated with the packets and forwards the packets whose Ethertype matches with the one that is configured for the ACL.

When you map a Layer 2 ACL to a locally switched WLAN, the rule to pass traffic based on the Ethertype is determined by the forwarding plane of the AP for every client that is associated with the WLAN. The AP forwarding plane looks into the Ethernet headers associated with the packets and forwards or denies the packets based on the action whose Ethertype matches with the one that is configured for the ACL.



Note Controllers configured to preform Central Switching and Centralized Authentication displays the name of the Layer-2 ACL being applied to roaming users incorrectly. The situation occurs when an authorized device preforms a Layer-3 roam from the anchor controller to a foreign controller. After roaming, if an administrator issues the **show acl layer2 summary** command on the CLI of the foreign controller the incorrect information is displayed. It is expected that the ACL applied by the anchor will follow the authenticated client as it roams from controller to controller.

This section contains the following subsections:

Restrictions on Layer 2 Access Control Lists

- You can create a maximum of 16 rules for a Layer 2 ACL.
- AP-specific Layer 2 ACLs can be configured only on FlexConnect APs. This is applicable only for locally-switched WLANs.
- You can create a maximum of 64 Layer 2 ACLs on a controller.
- A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.
- Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

Configuring Layer 2 Access Control Lists (CLI)

Procedure

- **config acl layer2 {create | delete} *acl-name***—Creates or deletes a Layer 2 ACL.
- **config acl layer2 apply *acl-name***—Applies a Layer 2 ACL to a data path.
- **config acl layer2 rule {add | delete} *acl-rule-name index***—Creates or deletes a Layer 2 ACL rule.
- **config acl layer2 rule change index *acl-rule-name old-index new-index***—Changes the index of a Layer 2 ACL rule.
- **config acl layer2 rule action *acl-rule-name index {permit | deny}***—Configures an action for a rule.
- **config acl layer2 rule etherType *name index ether-type-number-in-hex ether-type-mask-in-hex***—Configures the destination IP address and netmask for a rule.
- **config acl layer2 rule swap index *acl-rule-name index-1 index-2***—Swaps the index values of two rules.
- **config acl counter {start | stop}**—Starts or stops the ACL counter. This command is applicable for all types of ACLs. In an HA environment, the counters are not synchronized between the active and standby controllers.
- **show acl layer2 summary**—Shows a summary of the Layer 2 ACL profiles.
- **show acl layer2 detailed *acl-name***—Shows a detailed description of the Layer 2 ACL profile specified.
- **show client detail *client-mac-addr***—Shows the Layer 2 ACL rule that is applied to the client.

Mapping of Layer 2 ACLs with WLANs (CLI)

This is applicable to centrally switched WLANs and locally switched WLANs without FlexConnect access points.

Procedure

- **config wlan layer2 acl *wlan-id acl-name***—Maps a Layer 2 ACL to a centrally switched WLAN.
- **config wlan layer2 acl *wlan-id none***—Clears the Layer 2 ACLs mapped to a WLAN.
- **show wlan *wlan-id***—Shows the status of a Layer 2 ACL that is mapped to a WLAN.

Mapping of Layer 2 ACLs with Locally Switched WLANs Using FlexConnect Access Points (CLI)

This is applicable to locally switched WLANs that have FlexConnect access points.

Procedure

- **config ap flexconnect wlan l2acl add *wlan-id ap-name acl-name***—Maps a Layer 2 ACL to a locally switched WLAN.
- **config ap flexconnect wlan l2acl delete *wlan-id ap-name***—Deletes the mapping.
- **show ap config general *ap-name***—Shows the details of the mapping.