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 Access Control Lists, on page 7
- Configuring Layer 2 Access Control Lists, on page 9
- Configuring DNS-based Access Control Lists, on page 13
- Configuring URL Filtering, on page 16
- CNAME IPv6 Filtering, on page 23
- Domain-Based Filtering, on page 25

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 ACLs 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.

## Configuring and Applying Access Control Lists (GUI)

### Configuring Access Control Lists

#### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Security &gt; Access Control Lists &gt; Access Control Lists to open the Access Control Lists page.</th>
</tr>
</thead>
</table>
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:

a)  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.

b)  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.

c)  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.

d)  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.
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.

Related Topics
Configuring FlexConnect Access Control Lists (GUI)

Applying an Access Control List to an Interface

Procedure

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

Procedure

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.
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

**Procedure**

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

**Procedure**

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 Click Save Configuration to save your changes.
**Configuring Access Control Lists**

**Procedure**

**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

Procedure

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```
Information About Configuring 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
The 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.

WLC devices configured to perform Central Switching and Centralized Authentication display the name of the Layer-2 ACL being applied to roaming users incorrectly. The situation occurs when an authorized device performs 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.

### 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.

Configuring Layer 2 Access Control Lists (GUI)

**Procedure**

1. **Step 1** Choose Security > Access Control Lists > Layer2 ACLs to open the Layer2 Access Control Lists page.
2. **Step 2** Add a new ACL by clicking New. The Layer2 Access Control Lists > New page appears.
3. **Step 3** In the Access Control List Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.
4. **Step 4** Click Apply. When the Layer2 Access Control Lists page reappears, click the name of the new ACL.
5. **Step 5** When the Layer2 Access Control Lists > Edit page appears, click Add New Rule. The Layer2 Access Control Lists > Rules > New page appears.
6. **Step 6** Configure a rule for this ACL as follows:
   a) The controller supports up to 16 rules for each ACL. These rules are listed in order from 1 to 16. In the Sequence text box, enter a value (between 1 and 16) 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 15, 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.
   
   b) From the Ether Type drop-down list, choose any option from the following Ether type:
      - AppleTalk Address Resolution Protocol
      - VLAN-tagged Frame & Short Path Bridging
      - IPX (0x8137)
• IPX (0x8138)
• QNS Qnet
• Internet Protocol Version 6
• Ethernet Flow Control
• Slow Protocol
• CobraNet
• MPLS Unicast
• MPLS Multicast
• PPPoE Discovery Stage
• PPPoE Session Stage
• Jumbo Frames
• HomePlug 1.0 MME
• EAP over LAN
• PROFINET over Protocol
• HyperSCSI
• ATA over Ethernet
• EtherCAT Protocol

**Note** You can select any predefined Ether Types from the Ether Type drop-down list or enter your own Ether type value using the custom option from the Ether Type drop-down list.

c) 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.
d) Click **Apply** to commit your changes. The Layer2 Access Control Lists > Edit page reappears, showing the rules for this ACL.
e) Repeat this procedure to add any additional rules for this ACL.

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

**Step 8** Repeat this procedure to add any additional ACLs.

---

**Applying a Layer2 Access Control List to a WLAN (GUI)**

**Procedure**

**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 **Layer2 ACL** drop-down list, choose the ACL you have created.

**Step 5** Click **Apply**.

**Step 6** Click **Save Configuration**.
Applying a Layer2 Access Control List to an AP on a WLAN (GUI)

**Procedure**

**Step 1** Choose Wireless > Access Points > All APs to open the All APs page.

**Step 2** Click the name of the desired access point to open the All APs > Details page.

**Step 3** On the All APs > Details page, click the FlexConnect tab.

**Step 4** From the PreAuthentication Access Control Lists area, click the Layer2 ACLs link to open the ACL Mappings page.

**Step 5** From the Layer2 ACL drop-down list in the WLAN ACL Mapping area, choose the ACL you have created and click Add.

**Step 6** Save the configuration.

Configuring DNS-based Access Control Lists

**Information About DNS-based Access Control Lists**

The DNS-based ACLs are used for client devices such as Apple and Android devices. When using these devices, you can set pre-authentication ACLs on the controller to determine where devices have the right to go.

To enable DNS-based ACLs on the controller, you need to configure the allowed URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The controller is configured with the ACL name and that is returned by the AAA server for pre-authentication ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the controller, the CAPWAP payload is sent to the AP enabling DNS snooping on the client and the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the controller as a CAPWAP payload. The controller adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

In Release 8.0, support was added for DNS-based ACL with local web authentication.

**Restrictions on DNS-based Access Control Lists**

- In Release 8.2 and later releases, a maximum of 20 URLs can be allowed for an access control list.
- In Release 8.2 and later releases, on the controller, 40 IP addresses are allowed for one client.
• Local authentication is not supported for FlexConnect APs.
• DNS-based ACLs are not supported on FlexConnect APs with Local Switching.

**Note**
In Release 8.7, support was added in Cisco Wave 2 APs for DNS-based ACLs on FlexConnect APs with Local Switching.

• DNS-based ACLs are not supported on Cisco 1130 and 1240 series access points.
• If a client is anchored, be it auto-anchor or after roaming, DNS-based ACLs do not work.

### Configuring DNS-based Access Control Lists (CLI)

**Procedure**

**Step 1**
Specifies to create ACL. You can enter an IPv4 ACL name up to 32 alphanumeric characters.

```
config acl create name
```

**Example:**
(Cisco Controller) >> config acl create android

**Step 2**
Specifies to add a new URL domain for the access control list. URL domain name should be given in a valid format, for example, Cisco.com, bbc.in, or play.google.com. The hostname comparison is a sub string matched (wildcard based). You must use the ACL name that you have created already.

```
config acl url-domain add domain-name acl-name
```

**Example:**
(Cisco Controller) >> config acl url-domain add cisco.com android
(Cisco Controller) >> config acl url-domain add play.google.com android

**Step 3**
Specifies to delete an existing URL domain for the access control list.

```
config acl url-domain delete domain-name acl-name
```

**Example:**
(Cisco Controller) >> config acl url-domain delete cisco.com android

**Step 4**
Specifies to apply the ACL.

```
config acl apply acl-name
```

**Example:**
(Cisco Controller) >> config acl apply android

**Step 5**
Displays DNS-based ACL information by entering this command:

```
show acl summary
```

**Example:**
**Configure DNS-based Access Control Lists (CLI)**

1. **Step 6**
   Displays detailed DNS-based ACL information by entering this command:
   
   ```
   show acl detailed acl-name
   ```

   **Example:**
   
   ```
   (Cisco Controller) > show acl detailed android
   0 rules are configured for this ACL.
   DenyCounter : 0
   URLs configured in this ACL
   *.play.google.com
   *.store.google.com
   ```

2. **Step 7**
   Displays the IP addresses per client learned through DNS snooping (DNS-based ACL) by entering this command:
   
   ```
   show client detail mac-address
   ```

   **Example:**
   
   ```
   (Cisco Controller) > show client detail mac-address
   ```

3. **Step 8**
   Enables debugging of information related to DNS-based ACL.
   
   ```
   debug aaa events enable
   ```

   **Example:**
   
   ```
   (Cisco Controller) > debug aaa events enable
   ```

---

**Configuring DNS-based Access Control Lists (GUI)**

**Procedure**

1. **Step 1**
   Choose **Security > Access Control Lists > Access Control Lists** to open the Access Control Lists page.

2. **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**.

3. **Step 3**
   Add a new ACL by clicking **New**. The Access Control Lists > New page appears.
Configuring URL Filtering

Information About URL Filtering

URL filtering feature allows you to control access to internet websites. It does so by permitting or denying access to specific websites based on information contained in a URL access control list (ACL). The URL filtering then restricts access based on the ACL list.

Using location based filtering, APs are grouped under various AP groups and WLAN profiles separate trusted and non-trusted clients within the same SSID. This forces re-authentication and new VLAN when a trusted client moves to a non-trusted AP or vice-versa.

Controllers support up to 64 ACLs. These ACLs are configured to either permit or deny requests, and can be associated with different interfaces (ex: WLAN, LAN), thus increasing effective filtering. Policies can be implemented locally on a WLAN or an AP group that is different from the applied global policy.

The following is the policy priority order:

1. Policy
2. Interface
3. WLAN

The number of rules (URLs) supported in each ACL varies for different controllers:

- Cisco 5508 WLC and WiSM2 support 64 rules in one ACL.
- Cisco 5520, 8510, 8540 controllers support 100 rules in one ACL.

Restrictions for URL Filtering

- URL filtering is not supported in the following controllers:
  - Cisco 2504 Wireless Controller
• Cisco vWLC
• Cisco Mobility Express

• This feature is supported only on WLAN central switching and not local switching.
• Not supported in FlexConnect mode with local switching.
• The following types of URLs are not supported:
  • Wildcard URLs (ex: www.uresour*loc.com).
  • Sub-URL (ex: www.uresour*loc.com/support).
  • Sub-Domain (ex: reach.url.com or sub1.url.com)

• URL name is limited to 32 characters in length.
• No AVC Profile for the matched URLs. ACL Actions support for the Matched URLs.
• White list and Black list can be created using the "*" implicit rule in the ACL to permit or deny requests respectively.
• Only HTTP URLs are supported.
• RADIUS server returning URL filtering ACL name is not supported.
• ACL might fail to filter in the following situations:
  • URL is across fragmented packets.
  • IP packets are fragmented.
  • Direct IP address or proxy setup used instead of URL.

**Configuring URL Filtering (GUI)**

**Configuring Access Control Lists (GUI)**

To create or delete access control lists in an WLAN.

**Procedure**

**Step 1** Choose **Security > Access Control Lists > URL ACLs** to open the URL Access Control Lists page.

**Step 2** Select the **Enable URL Acl** check box to enable the URL ACL feature.

**Step 3** Add a new ACL by clicking **New**. The **URL Access Control Lists > New** page appears.

In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

**Step 4** Click **Apply**.

• Repeat this procedure to add any additional URL ACLs.
To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

**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**.

---

**Configuring an URL ACL List (GUI)**

Configuring rules in an URL ACL List.

**Procedure**

**Step 1** Choose **Security > Access Control Lists > URL ACLs** to open the URL Access Control Lists page.

**Step 2** Choose the URL ACL. **URL Access Control Lists > Edit** page appears.

**Step 3** Choose **Add New Rule**.

**Step 4** Configure a rule for this ACL from the drop-down menu.

- **Rule Index**—range between 1 and 100.
- **URL**—enter the URL address.
- **Action**—select Permit or Deny.

**Step 5** Click **Apply**.

Repeat this procedure to add any additional rules.

**Note** To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: Enter the URL as website.com:8080 and apply permit action.

---

**Applying a URL Filtering Access Control List Globally (GUI)**

Applying the URL ACL to the entire network.

**Procedure**

**Step 1** Choose **Security > Local Policies** to open the local policy page.

**Step 2** Choose the desired policy. **Policy > Edit** page appears.

**Step 3** Enter the **Match Role String** in the text box.

**Step 4** Select the URL ACL from the **URL ACL** drop-down list.
Step 5 Click Apply.

Note The Match Role String name should match the role name in Cisco AV pair.

---

**Applying a URL Filtering Access Control List to an Interface (GUI)**

Applying the URL ACL to an interface in the network.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Controller</strong> &gt; <strong>Interfaces</strong> to open the interface page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose the desired interface. The interface page for the selected interface appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the URL ACL from the <strong>URL ACL</strong> drop-down list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

---

**Applying a URL Filtering Access Control List for a WLAN (GUI)**

Applying the URL ACL to a WLAN in the network.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>WLANs</strong> to open the WLAN page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the ID number of the desired WLAN. The <strong>WLANs</strong> &gt; <strong>Edit</strong> page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the <strong>Advanced</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the <strong>URL ACL</strong> drop-down list, choose the ACL that you want to apply to this WLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

---

**Mapping the policy to a WLAN (GUI)**

Mapping the policy to a WLAN in the network.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>WLANs</strong> to open the WLAN page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the ID number of the desired WLAN. The <strong>WLANs</strong> &gt; <strong>Edit</strong> page appears.</td>
</tr>
</tbody>
</table>
To delete a Policy-Mapping in a WLAN (GUI)

This procedure helps delete the policy-mapping in a WLAN.

Procedure

Step 1 Choose WLANs to open the WLAN page.
Step 2 Click the ID number of the desired WLAN.
The WLANs > Edit page appears.
Step 3 Hover the mouse cursor over the blue drop-down arrow for that local policy
Step 4 Choose Remove
The confirmation box appears.
Step 5 Click OK.
Step 6 Click Apply.

Mapping the policy to an AP Group (GUI)

Mapping the policy to an AP Group in the network.

Procedure

Step 1 Choose WLANs to open the WLAN page.
Step 2 Choose Advanced > AP Groups.
Step 3 Choose the AP Group.
The AP Groups > Edit page appears.
Step 4 Choose the WLANs tab.
Step 5 Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select Policy-Mapping.
Step 6 In the AP Group > Policy > Mappings page.
1. Enter the Priority Index value.
2. Choose the local policy from the Local Policy drop-down list.
3. Click **Add**.

**Step 7**

Click **Apply**.

The WLAN and AP Group are Local Role based policies.

---

## Configuring URL Filtering (CLI)

### Configuring URL Filtering (CLI)

**Procedure**

**Step 1**

Configure the URL based Filtering feature by entering this command:

```plaintext
config acl url-acl { enabled | disable }
```

**Step 2**

Create or delete a URL ACL by entering this command:

```plaintext
config acl url-acl { create | delete } id-token
```

**Step 3**

Apply the URL ACL to the data path by entering this command:

```plaintext
config acl url-acl apply acl-name
```

**Step 4**

Configure an acl to an interface by entering this command:

```plaintext
config interface url-acl interface-name acl-name
```

**Step 5**

Configure an acl to a WLAN by entering this command:

```plaintext
config wlan url-acl wlan-id acl-name
```

---

## Configuring Access Control List Rules (CLI)

**Procedure**

**Step 1**

Create or delete a ACL by entering this command:

```plaintext
config acl url-acl rule { add | delete } acl-name index
```

**Step 2**

Configure the URL address in a valid format (example: www.cisco.com) by entering this command:

```plaintext
config acl url-acl rule url acl-name index url-name
```

**Step 3**

Configure the action of the rule by entering this command:

```plaintext
config acl url-acl rule action acl-name index { permit | deny }
```
To have seamless access to websites which use different port number instead of default port 80, you will need to create a rule which includes the port number in URL-name:Port format. Example: enter the URL as website.com:8080 and apply permit action.

Applying Local Policy (CLI)

Procedure

Step 1  Create or delete a local profiling policy by entering this command:
\texttt{config policy policy-name \{create | delete\}}

Step 2  Configure a match type to a policy by entering this command:
\texttt{config policy policy-name match role \{role-name| none\}}

Step 3  Configure an action to a policy by entering this command:
\texttt{config policy policy-name action url-acl \{enable | disable\} acl-name}

Step 4  Activate a local policy to a WLAN by entering this command:
\texttt{config wlan policy add priority-index policy-name wlan-id}

Step 5  Add or delete a local policy in an AP group in a WLAN by entering this command:
\texttt{config wlan apgroup policy \{add | delete\} priority-index policy-name ap-group-name wlan-id}

Viewing URL Filtering (CLI)

Procedure

- View ACL summary by entering this command:
  \texttt{show acl url-acl summary}
- View detailed URL ACL profile information by entering this command:
  \texttt{show acl url-acl detailed acl-name}
- View the details of a policy by entering this command:
  \texttt{show policy \{summary|policy-name\}}
- View client details by MAC address by entering this command:
  \texttt{show client detail mac-address}
- View the WLAN configuration details by entering this command:
  \texttt{show wlan wlan-id}
- View the interface details by entering this command:
  \texttt{show interface detailed interface-name}
- Clear the counters by entering this command:
Troubleshooting URL Filtering (CLI)

You can troubleshoot the URL Filtering feature by entering these commands:

**Procedure**

- `debug fastpath dump urlacldb aclid ruleindex dataplane`
- `debug fastpath dump stats dataplane`
  The dataplane options available are 0, 1, All.
- `debug fastpath dump scbldb`

CNAME IPv6 Filtering

**Information About CNAME IPv6 Filtering**

This feature enables the use of IPv6 address via FQDN in the network to authenticate the client traffic via controller and external AAA server. The client pre-authentication can be configured to use internal or external URL ACLs.

For the feature to function, you must set the SSID to central switching and the APs to local mode.

**Restrictions for CNAME IPv6 Filtering**

- Supported only on Cisco 3504, 5508, 8510, 5520, and 8540 WLCs
- Maximum supported ACLs are 64.
- Maximum supported rules in an ACL are 20.
- Total number of resolved IPs is 40.
- CNAME parsing in different packets is not supported.
- AP in FlexConnect mode is not supported.

Configuring CNAME URL ACL (GUI)

**Procedure**

**Step 1** Choose Security > Access Control Lists > URL ACLs to open the URL Access Control Lists page.

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

The URL Access Control Lists > New page appears. In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

**Step 3** Click the URL ACL name that you want to configure.
Step 4  **Note**  You can add the FQDN of the IPv6 server in the pre-authentication IPv4 ACL in the WLC so that the AAA server can allow or deny the requested traffic to the client.

Click **Add New Rule**.

Step 5  Configure a rule for this ACL from the drop-down list.

- **Rule Index**—range between 1 and 100.
- **URL**—enter the URL address.

**Note**  To use a IPv6 address, add the FQDN of the server address.

Step 6  Click **Apply**.

Repeat this procedure to add any additional rules in the URL ACL.

Step 7  To delete any rule within a URL ACL, in the **URL Access Control Lists > Edit** page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

Step 8  To delete any URL ACL, in the **URL Access Control Lists** page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose **Remove**.

Step 9  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**.

---

### Configuring Web Authentication for CNAME IPv6 Filtering on a WLAN (GUI)

**Procedure**

Step 1  Select **Security > Authentication** tab.

Step 2  Click **New** to add a new RADIUS server or click the **Server Index** of an existing server.

Step 3  Choose **Enable** from the **Support for CoA** drop-down list.

Step 4  Choose **WLAN > WLAN ID > Security > Layer 3** to open the Layer 3 page.

Step 5  Choose **Web Policy** from the **Layer 3 Security** drop-down list.

Step 6  Choose the URL ACL from the **Preauthentication ACL IPv4** drop-down list.

Step 7  Click **Apply**.

---

### Configuring Web Authentication for CNAME IPv6 Filtering Using External RADIUS Server (GUI)

**Procedure**

Step 1  Select **Security > Authentication** tab.

Step 2  Click **New** to add a new RADIUS server or click the **Server Index** of an existing server.
When adding a new RADIUS server, enter appropriate details in the fields.

**Step 3** Choose **Enable** from the **Support for CoA** drop-down list.

**Step 4** Choose **WLAN > WLAN ID > Advanced** to open the advanced page.

**Step 5** Choose **ISE NAC** from the **NAC State** drop-down list.

**Step 6** Click **Apply**.

### Configuring IPv6 CNAME Filtering (CLI)

**Procedure**

- Create a URL ACL by entering this command:
  ```plaintext
  config acl create acl-name
  ```
- Add a URL rule in a URL ACL by entering this command:
  ```plaintext
  config acl URL-domain add domain-name acl-name
  ```
- Enable a URL ACL by entering this command:
  ```plaintext
  config acl apply acl-name
  ```
- View the ACL summary by entering this command:
  ```plaintext
  show acl summary
  ```
- View detailed ACL profile statistics by entering this command:
  ```plaintext
  show acl detailed acl-name
  ```

### Domain-Based Filtering

#### Information About Domain Based Filtering

This feature allows you to control access to websites by permitting or denying access to websites using DNS-based access control list (ACL).

Cisco 3504, 5520, and 8540 Wireless Controllers (WLC) support up to 64 ACLs. These ACLs are configured to either permit or deny traffic based on whitelist or blacklist on any protocol. Hence when a URL request is blocked, access is denied regardless of the protocol. An ACL can either be a whitelist (permit) or a blacklist (deny). Rules with an independent permit or deny settings are not supported within an ACL. Each ACL supports up to 100 rules (URLs).

By default, all the URLs that do not match the applied ACL are denied.

ACLs can be associated with different interfaces (for example: WLAN, LAN, and so on) using the following priority:

1. Role-based Policy
2. Interface
3. WLAN

Note
Policies can be implemented locally on a WLAN or on an AP group that is different from the applied global policy.

Restrictions on Domain Based Filtering

- The following are not supported:
  - Cisco 2504 WLC
  - Cisco 5508 WLC
  - Cisco Flex 7510 WLC
  - Cisco 8510 WLC
  - WiSM2
  - vWLC
  - Mobility Express

- Supported only on WLAN Central Switching.
- Not supported on Local switching or FlexConnect mode with local switching.
- ACLs can have a maximum of 10 wildcard URLs (for example: *.example.com) and 5 sub-domains per wildcard (for example: sub.example.com).
- Sub-URL are not allowed (for example: www.example.com/support).
- URL name is limited to a maximum of 255 characters.
- Direct IP address access is blocked in the whitelist. However, it is not blocked in the blacklist.
- Layer 2 roaming is not supported.
- IPv6 is not supported.
- RADIUS server returning URL filtering ACL name is not supported.
- ACL may fail to filter in the following situations:
  - URL is across fragmented packets
  - IP packets are fragmented
Configuring Domain Based Filtering (GUI)

Configuring Access Control Lists (GUI)

Configuring rules in a URL ACL List.

Procedure

Step 1  Choose Security > Access Control Lists > URL ACLs to open the URL Access Control Lists page.
Step 2  Choose the URL ACL.  
URL Access Control Lists > Edit page appears.
Step 3  Choose Add New Rule.
Step 4  Configure a rule for this ACL as follows
   • Rule Index – Range between 1 and 100
   • URL—Enter the URL address.
   • Action—Select Permit or Deny.
Step 5  Click Apply.
Repeat this procedure to add any additional rules.

Note  To have seamless access to websites which use a different port number instead of the default port 80, create a rule which includes the port number in URL-name: Port format. Example: Enter the URL as website.com:8080 and apply permit action.

Creating a URL ACL List (GUI)

To create or delete access control lists in a WLAN.

Procedure

Step 1  Choose Security > Access Control Lists > URL ACLs to open the URL Access Control Lists page.
Step 2  Select the Enable URL Acl check box to enable the URL ACL feature.
Step 3  Add a new ACL by clicking New. The URL Access Control Lists > New page appears.
   In the URL ACL Name text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.
Step 4  Click Apply.
   • Repeat this procedure to add any additional URL ACLs.
   • To delete any URL ACL, in the URL Access Control Lists page, hover the mouse cursor over the blue drop-down arrow for that ACL and choose Remove.
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.

---

**Applying a URL Filtering Access Control List Globally (GUI)**

Applying the URL ACL to the entire network.

**Procedure**

1. **Step 1** Choose Security > Local Policies to open the local policy page.
2. **Step 2** Choose the desired policy.
3. **Policy > Edit** page appears.
4. **Step 3** Enter the Match Role String in the text box.
5. **Step 4** Select the URL ACL from the URL ACL drop-down list.
6. **Step 5** Click Apply.

**Note** The Match Role String name must match the role name in the Cisco AV pair.

---

**Applying a URL Filtering Access Control List to an Interface (GUI)**

Applying the URL ACL to an interface in the network.

**Procedure**

1. **Step 1** Choose Controller > Interfaces to open the interface page.
2. **Step 2** Choose the desired interface.
3. The interface page for the selected interface appears.
4. **Step 3** Select the URL ACL from the URL ACL drop-down list.
5. **Step 4** Click Apply.

---

**Applying a URL Filtering Access Control List for a WLAN (GUI)**

Applying the URL ACL to a WLAN in the network.

**Procedure**

1. **Step 1** Choose WLANs to open the WLAN page.
2. **Step 2** Click the ID number of the desired WLAN.
The WLANs > Edit page appears.

**Step 3** Choose the **Advanced** tab.
**Step 4** From the **URL ACL** drop-down list, choose the ACL that you want to apply to this WLAN.
**Step 5** Click **Apply**.

### Mapping the Policy to a WLAN (GUI)

Mapping the policy to a WLAN in the network.

**Procedure**

**Step 1** Choose **WLANs** to open the WLAN page.
**Step 2** Click the ID number of the desired WLAN. The **WLANs > Edit** page appears.
**Step 3** Choose the **Policy-Mapping** tab.
1. Enter the **Priority Index** value.
2. Choose the local policy from the **Local Policy** drop-down list.
3. Click **Add**.
**Step 4** Click **Apply**.

### To Delete a Policy-Mapping in a WLAN (GUI)

This procedure helps delete the policy-mapping in a WLAN.

**Procedure**

**Step 1** Choose **WLANs** to open the WLAN page.
**Step 2** Click the ID number of the desired WLAN. The **WLANs > Edit** page appears.
**Step 3** Hover the mouse cursor over the blue drop-down arrow for that local policy.
**Step 4** Choose **Remove**
The confirmation box appears.
**Step 5** Click **OK**.
**Step 6** Click **Apply**.
Mapping the Policy to an AP Group (GUI)

Mapping the policy to an AP Group in the network.

Procedure

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

**Step 2** Choose Advanced > AP Groups.

**Step 3** Choose the AP Group.

The AP Groups > Edit page appears.

**Step 4** Choose the WLANs tab.

**Step 5** Hover the mouse cursor over the blue drop-down arrow of the required WLAN, select Policy-Mapping.

**Step 6** In the AP Group > Policy > Mappings page.

1. Enter the Priority Index value.

2. Choose the local policy from the Local Policy drop-down list.

3. Click Add.

**Step 7** Click Apply.

The WLAN and AP Group are Local Role based policies.

---

Configuring DNS Filtering (CLI)

Configuring URL Filtering (CLI)

Procedure

**Step 1** Configure the URL-based Filtering feature by entering this command:
```
config acl url-acl { enabled | disable }
```

**Step 2** Create or delete a URL ACL by entering this command:
```
config acl url-acl { create | delete } id-token
```

**Step 3** Apply the URL ACL to the data path by entering this command:
```
config acl url-acl apply acl-name
```

**Step 4** Configure an acl to an interface by entering this command:
```
config interface url-acl interface-name acl-name
```

**Step 5** Configure an acl to a WLAN by entering this command:
```
config wlan url-acl wlan-id acl-name
```
Configuring Access Control List Rules (CLI)

Procedure

**Step 1**  Create or delete an ACL by entering this command:
```
config acl url-acl rule { add | delete } acl-name index
```

**Step 2**  Configure the URL address in a valid format (example: www.cisco.com) by entering this command:
```
config acl url-acl rule url acl-name index url-name
```

**Step 3**  Configure the action of the rule by entering this command:
```
config acl url-acl rule action acl-name index { permit | deny }
```

*Note*  To have seamless access to websites which use a different port number instead of the default port 80, create a rule which includes the port number in URL-name: Port format. Example: enter the URL as website.com:8080 and apply permit action.

**Step 4**  Configure the whitelist or blacklist ACL by entering this command:
```
config acl url-acl list-type acl-name { whitelist | blacklist }
```

**Step 5**  Configure the external server to the redirect the web page requests by entering this command:
```
config acl url-acl external-server-ip ip-address
```

**Related Topics**
- Configuring FlexConnect Access Control Lists (CLI)

Applying Local Policy (CLI)

Procedure

**Step 1**  Create or delete a local profiling policy by entering this command:
```
config policy policy-name { create | delete }
```

**Step 2**  Configure a match type to a policy by entering this command:
```
config policy policy-name match role { role-name | none }
```

**Step 3**  Configure an action to a policy by entering this command:
```
config policy policy-name action url-acl { enable | disable } acl-name
```

**Step 4**  Activate a local policy to a WLAN by entering this command:
```
config wlan policy add priority-index policy-name wlan-id
```

**Step 5**  Add or delete a local policy in an AP group in a WLAN by entering this command:
```
config wlan apgroup policy { add | delete } priority-index policy-name ap-group-name wlan-id
```
Viewing URL Filtering (CLI)

**Procedure**

- View ACL summary by entering this command:
  
  ```
  show acl url-acl summary
  ```

- View detailed URL ACL profile information by entering this command:
  
  ```
  show acl url-acl detailed acl-name
  ```

- View the details of a policy by entering this command:
  
  ```
  show policy { summary|policy-name }
  ```

- View client details by MAC address by entering this command:
  
  ```
  show client detail mac-address
  ```

- View the WLAN configuration details by entering this command:
  
  ```
  show wlan wlan-id
  ```

- View the interface details by entering this command:
  
  ```
  show interface detailed interface-name
  ```

- Clear the counters by entering this command:
  
  ```
  clear url-acl-counters
  ```

**Troubleshooting URL Filtering (CLI)**

You can troubleshoot the URL Filtering feature by entering these commands:

**Procedure**

- ```
  debug fastpath dump urlacldb aclid ruleindex dataplane
  ```

- ```
  debug fastpath dump stats dataplane
  ```
  
  The dataplane options available are 0, 1, All.

- ```
  debug fastpath dump scbdb
  ```