Configuring Client Exclusion Policies

Configuring Client Exclusion Policies (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Client Exclusion Policies** to open the Client Exclusion Policies page.

Step 2 Select any of these check boxes if you want the controller to exclude clients for the condition specified. The default value for each exclusion policy is enabled.

- **Excessive 802.11 Association Failures**: Clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- **Excessive 802.11 Authentication Failures**: Clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- **Excessive 802.1X Authentication Failures**: Clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.

  Note In some configurations, 802.1X exclusion may not occur. For more information, see https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/214466-802-1x-client-exclusion-on-an-aireos-wlc.html.

- **Maximum 802.1x-AAA Failure Attempts**: Clients are excluded after a maximum number of 802.1X-AAA failure attempts with the RADIUS server. Valid range of maximum number of 802.1X-AAA failure attempts that you can configure is 1 to 10 with the default value being 3.
- **IP Theft or IP Reuse**—Clients are excluded if the IP address is already assigned to another device.
- **Excessive Web Authentication Failures**—Clients are excluded on the fourth web authentication attempt, after three consecutive failures.

Step 3 Save your configuration.

Configuring Client Exclusion Policies (CLI)

Step 1 Enable or disable the controller to exclude clients on the sixth 802.11 association attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-assoc {**enable** | **disable**}

Step 2 Enable or disable the controller to exclude clients on the sixth 802.11 authentication attempt, after five consecutive failures by entering this command:

config wps client-exclusion 802.11-auth {**enable** | **disable**}

Step 3 Enable or disable the controller to exclude clients on the fourth 802.1X authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion 802.1x-auth {**enable** | **disable**}

Step 4 Configure the controller to exclude clients after a maximum number of 802.1X-AAA failure attempts with the RADIUS server by entering this command:

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts *num-of-attempts*

Valid range for the maximum number of 802.1X-AAA failure attempts with the RADIUS is 1 to 10 with the default value being 3.

Step 5 Enable or disable the controller to exclude clients if the IP address is already assigned to another device by entering this command:

config wps client-exclusion ip-theft {**enable** | **disable**}

Step 6 Enable or disable the controller to exclude clients on the fourth web authentication attempt, after three consecutive failures by entering this command:

config wps client-exclusion web-auth {**enable** | **disable**}

Step 7 Enable or disable the controller to exclude clients for all of the above reasons by entering this command:

config wps client-exclusion all {**enable** | **disable**}

Step 8 Use the following command to add or delete client exclusion entries.

config exclusionlist {**add** *mac-addr description* | **delete** *mac-addr* | **description** *mac-addr description*}

- **add**: Creates a local exclusion-list entry.
- **delete**: Deletes a local exclusion-list entry.
- **description**: Sets the description for an exclusion-list entry.

Step 9 Save your changes by entering this command:

save config

Step 10 See a list of clients that have been dynamically excluded, by entering this command:

show exclusionlist

Information similar to the following appears:

```
Dynamically Disabled Clients
----------------------------
```

```
  MAC Address      Exclusion Reason     Time Remaining (in secs)
  -----------      ----------------     ------------------------

00:40:96:b4:82:55    802.1X Failure            51
```

Step 11 See the client exclusion policy configuration settings by entering this command:

show wps summary

Information similar to the following appears:

```
Auto-Immune
 Auto-Immune.............................. Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
  Maximum 802.1x-AAA failure attempts............ 3

Signature Policy
  Signature Processing....................... Enabled
```