



## Setting the Client Count per WLAN

---

- [Restrictions for Setting Client Count for WLANs, on page 1](#)
- [Client Count per WLAN, on page 1](#)
- [Configuring the Client Count per WLAN \(GUI\), on page 2](#)
- [Configuring the Maximum Number of Clients per WLAN \(CLI\), on page 2](#)
- [Configuring the Maximum Number of Clients for each AP Radio per WLAN \(GUI\), on page 2](#)
- [Configuring the Maximum Number of Clients for each AP Radio per WLAN \(CLI\), on page 3](#)
- [Deauthenticating Clients \(CLI\), on page 3](#)

## Restrictions for Setting Client Count for WLANs

- The maximum number of clients for each WLAN feature is not supported when you use FlexConnect local authentication.
- The maximum number of clients for each WLAN feature is supported only for access points that are in connected mode.
- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.
- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.



---

**Note**

For more information about the number of clients that are supported, see the product data sheet of your controller.

---

## Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users

(employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

This section contains the following subsections:

## Configuring the Client Count per WLAN (GUI)

---

- Step 1** Choose **WLANs** to open the WLANs page.
  - Step 2** Click the ID number of the WLAN for which you want to limit the number of clients. The **WLANs > Edit** page appears.
  - Step 3** Click the **Advanced** tab.
  - Step 4** In the **Maximum Allowed Clients** text box, enter the maximum number of clients that are to be allowed.
  - Step 5** Click **Apply**.
  - Step 6** Click **Save Configuration**.
- 

## Configuring the Maximum Number of Clients per WLAN (CLI)

---

- Step 1** Determine the WLAN ID for which you want to configure the maximum clients by entering this command:  
**show wlan summary**  
Get the WLAN ID from the list.
  - Step 2** Configure the maximum number of clients for each WLAN by entering this command:  
**config wlan max-associated-clients *max-clients* *wlan-id***
- 

## Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI)

---

- Step 1** Choose **WLANs** to open the WLANs page.
  - Step 2** Click the ID number of the **WLAN** for which you want to limit the number of clients. The **WLANs > Edit** page appears.
  - Step 3** In the **Advanced** tab, enter the maximum allowed clients for each access point radio in the Maximum Allowed Clients Per AP Radio text box. You can configure up to 200 clients.
  - Step 4** Click **Apply**.
-

## Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI)

- 
- Step 1** Determine the WLAN ID for which you want to configure the maximum clients for each radio by entering this command:
- show wlan summary**
- Obtain the WLAN ID from the list.
- Step 2** Configure the maximum number of clients for each WLAN by entering this command:
- config wlan max-radio-clients** *client\_count*
- You can configure up to 200 clients.
- Step 3** See the configured maximum associated clients by entering the **show 802.11a** command.
- 

## Deauthenticating Clients (CLI)

Using the controller, you can deauthenticate clients based on their user name, IP address, or MAC address. If there are multiple client sessions with the same user name, you can deauthenticate all the client sessions based on the user name. If there are overlapped IP addresses across different interfaces, you can use the MAC address to deauthenticate the clients.



---

**Note** It is not possible to deauthenticate clients using the controller GUI.

---

### Procedure

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}

