



Configuring MAC Filtering for WLANs

- [Restrictions for MAC Filtering, on page 1](#)
- [MAC Filtering of WLANs, on page 1](#)
- [Enabling MAC Filtering, on page 1](#)

Restrictions for MAC Filtering

- MAC filtering cannot be configured for Guest LANs.
- Interface mapping and profile precedence—MAC filtering for the WLAN set to any WLAN/Interface requires a mandatory profile name, followed by the interface name for the traffic to work properly.

MAC Filtering of WLANs

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.

MAC Filtering with Centrally Authenticated WLANs

After the initial 802.11 authentication exchange between the AP and the clients, the AP sends the client association request in CAPWAP to the controller. If the controller is using a local MAC filter list, it will immediately send a successful or failed association response. If external RADIUS is used, the controller sends an Access-Request to the AAA server, and based on the response from RADIUS, sends its association response to the client.



Note

Wireless clients may time out their wait for association response within as little as 300 ms. Therefore, if you use an external RADIUS server with MAC filtering, ensure that the server responds within this timeframe.

Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

- Enable MAC filtering by entering the **config wlan mac-filtering enable wlan_id** command.
- Verify that you have MAC filtering enabled for the WLAN by entering the **show wlan** command.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

When a client tries to associate to a WLAN for the first time, the client gets authenticated with its MAC address from AAA server. If the authentication is successful, the client gets an IP address from DHCP server, and then the client is connected to the WLAN.

When the client roams or sends association request to the same AP or different AP and is still connected to WLAN, the client is not authenticated again to AAA server.

If the client is not connected to WLAN, then the client has to get authenticated from the AAA server.