Configuring Local MAC Filters

Prerequisites for Configuring Local MAC Filters

You must have AAA enabled on the WLAN to override the interface name.

Local MAC Filters

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Configuring Local MAC Filters (CLI)

- Create a MAC filter entry on the controller by entering the **config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] command.

  The following parameters are optional:

  - *mac_addr*—MAC address of the client.

  - *wlan_id*—WLAN id on which the client is associating.

  - *interface_name*—The name of the interface. This interface name is used to override the interface configured to the WLAN.

  - *description*—A brief description of the interface in double quotes (for example, "Interface1").

  - *IP_addr*—The IP address which is used for a passive client with the MAC address specified by the mac addr value above.

- Assign an IP address to an existing MAC filter entry, if one was not assigned in the **config macfilter add** command by entering the **config macfilter ip-address** *mac_addr IP_addr* command.

- Verify that MAC addresses are assigned to the WLAN by entering the **show macfilter** command.

Note For ISE NAC WLANs, the MAC authentication request is always sent to the external RADIUS server. The MAC authentication is not validated against the local database. This functionality is applicable to Releases 8.5, 8.7, 8.8, and later releases via the fix for CSCvh85830.

Previously, if MAC filtering was configured, the controller tried to authenticate the wireless clients using the local MAC filter. RADIUS servers were attempted only if the wireless clients were not found in the local MAC filter.