



Disabling IP Learning in FlexConnect Mode

- [Information About Disabling IP Learning in FlexConnect Mode, on page 1](#)
- [Restrictions for Disabling IP Learning in FlexConnect Mode, on page 1](#)
- [Disabling IP Learning in FlexConnect Mode \(CLI\), on page 2](#)
- [Verifying MAC Entries from Database, on page 2](#)

Information About Disabling IP Learning in FlexConnect Mode

In FlexConnect local switching scenarios, where clients from the same sites may share the same address range, there is a possibility of multiple clients being allocated or registered with the same IP address. The controller receives IP address information from the AP, and if more than one client attempts to use the same IP address, the controller discards the last device trying to register an already-used address as an IP theft event, potentially resulting in client exclusion.

The Disabling IP learning in FlexConnect mode feature utilizes the **no ip mac-binding** command to ensure that no device tracking is done for clients, thus preventing the IP theft error.



Note

- This feature is applicable only for IPv4 addresses.
- Configuring **ip overlap** in FlexConnect Profile assists overlapping IP address support for clients across different sites in FlexConnect local switching.

Restrictions for Disabling IP Learning in FlexConnect Mode

- The **wireless client ip deauthenticate** command works by referring to the IP table binding entries directly. It does not work for client whose IPs are not learnt.
- Overlapping IP addresses within a single site tag and across different site tags require different settings. Furthermore, if a single site tag contains overlapping IP addresses, L3 web authentication is necessary. However, L3 web authentication relies on IP addresses, and ensuring the uniqueness of IP addresses cannot be guaranteed, making this combination incorrect.
- When IP Source Guard (IPSG) is enabled and multiple binding information is sent with the same IP and preference level (such as DHCP, ARP, and so on) to CPP, the CPP starts to ignore the later bindings

after the first binding creation. Hence, you should not configure IPSG and disable IP MAC binding together. If IPSG and **no ip mac-binding** are configured together then IPSG does not work.

Disabling IP Learning in FlexConnect Mode (CLI)

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | wireless profile policy <i>profile-policy-name</i> Example: Device(config)# wireless profile policy test-profile-policy | Configures the wireless profile policy. |
| Step 3 | shutdown Example: Device(config-wireless-policy)# shutdown | Disables the wireless policy profile. Note Disabling policy profile results in associated AP and client to rejoin. |
| Step 4 | no ip mac-binding Example: Device(config-wireless-policy)# no ip mac-binding | Disables IP learning in FlexConnect mode. |
| Step 5 | no shutdown Example: Device(config-wireless-policy)# no shutdown | Enables the wireless policy profile. |
| Step 6 | exit Example: Device(config-wireless-policy)# exit | Returns to privileged EXEC mode. |

Verifying MAC Entries from Database

To verify the MAC details from database, use the following command:

```
Device# show wireless device-tracking database mac
MAC VLAN IF-HDL IP
-----
6c96.cff2.889a 64 0x90000008 9.9.64.175
```