Disabling Clients with Random MAC Address

Information About Disabling Clients with Random MAC Addresses

Wireless clients used to associate with a wireless network using the MAC address that is assigned, for the Wi-Fi network interface card (NIC), during manufacture. This globally unique MAC address assigned by the manufacturer is also known as burn-in address (BIA). BIA tracks end users with the help of the MAC address of the Wi-Fi. To improve the privacy of end user products, a locally enabled random MAC address is enabled for Wi-Fi operations.

Prior to Cisco IOS XE Bengaluru 17.5.1 Release, clients joining a wireless network using a random MAC address could not be tracked with ease. From Cisco IOS XE Bengaluru 17.5.1 Release onwards, the controller is equipped with a knob that denies the entry of clients with a random MAC address into the network. When the *local-admin-mac deny* knob is enabled on the controller, the association of a client joining the network with a random MAC address is rejected. By default, this feature is disabled on the controller.

This feature is not supported in Cisco Wave 1 access points.

Configuring Random MAC Address Deny (CLI)

To stop the entry of clients with a random MAC addresses from joining a wireless network, enable the random MAC address deny knob, by following the steps given below.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan-profile-name <1-4096> SSID-network-name* **Example:** `Device(config)# wlan wlan-profile-name 8 ssid-network-name`	Configures the WLAN policy profile.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Shuts down the WLAN.
Step 4	**[no] local-admin-mac deny** **Example:** `Device(config-wlan)# local-admin-mac deny`	Enables the random MAC address deny knob. Use the **no** form of this command to disable the feature.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.

Verifying Denial of Clients with a Random MAC Address

To verify the denial of a client with a random MAC address, run the **show wlan name** *wlan-profile-name* | **begin locally** command:

```
Device# show wlan name laa | begin locally
Locally Administered Address Configuration
Deny LAA clients                          : Enabled
```

To verify if a client address is a random MAC address, run the **show wireless client mac-address** *MAC-address* **detail** command:

```
Device# show wireless client mac-address 72xx.38xx.2axx detail
Client MAC Address : 72xx.38xx.2axx
Client MAC Type    : Locally Administered Address
Client IPv4 Address      : 9.1.1.1
Client IPv6 Addresses    : fexx::71xx:27xx:a7xx:efxx
Client Username          : 72xx.38xx.2axx
```

To verify how many random MAC clients are present in the system, run the **show wireless stats client detail** command:

```
Device# show wireless stats client detail
Client Summary
------------------------------
Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
```

```
Anchor Clients  : 0
Local Clients   : 1
Idle Clients    : 0
Locally Administered MAC Clients: 1
```

To display the statistics of a specific client, run the **show wlan id** *<1-4096>* **client stats** command:

```
Device# show wlan id 8 client stats
Wlan Profile Name: wlan-profile, Wlan Id: 8
Current client state statistics:
------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  WebAuth Pending        : 0
  Run                    : 1
Locally Administered MAC Clients         : 1
```

Note Run the **show configuration wlan wlan-name** command on an AP, to view the status of the locally administered address (LAA) on the WLAN.