Configuring Client Profiling

Prerequisites for Configuring Client Profiling

- By default, client profiling will be disabled on all WLANs.
- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only a MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- To enable client profiling, you must enable the DHCP required flag and disable the local authentication flag.
- Client profiling uses pre-existing profiles in the controller.
- Profiling for Wireless clients are done based on MAC OUI, DHCP, HTTP User agent.

Note DHCP is required for DHCP profiling and Webauth for HTTP user agent.

Restrictions for Configuring Client Profiling

- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
  - Wired clients behind the WGB will not be profiled and policy action will not be done.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.
- While the controller parses the DHCP profiling information every time the client sends a request, the profiling information is sent to ISE only once.
- Custom profiles cannot be created for this release.
- This release contains 88 pre-existing policies where CLI is check only except if you create a policy.
- When local profiling is enabled radius profiling is not allowed on a particular WLAN.
- Only the first policy rule that matches is applied.
- Only 16 policies per WLAN can be configured and globally 16 policies can be allowed.
- Policy action is done only after L2/L3 authentication is complete or when the device sends http traffic and gets the device profiled. Profiling and policing actions will happen more than once per client.
- If AAA override is enabled and if you get any AAA attributes from the AAA server other than role type, configured policy does not apply since the AAA override attributes have a higher precedence.
- For Apple devices, the version and operating system information is displayed only for iPhone 7 and later models and iPads introduced in 2017 and later, provided the WLAN is not open. The version and operating system information is not displayed for older devices.

Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form. Local Client profiling (DHCP and HTTP) is enabled at WLAN level. Clients on the WLANS will be profiled as soon as profling is enabled.

Controller has been enhanced with some of these following capabilities:

- Controller does profiling of devices based on protocols like HTTP, DHCP, etc. to identify the end devices on the network.
- You can configure device-based policies and enforce per user or per device end points, and policies applicable per device.
- Controller displays statistics based on per user or per device end points, and policies applicable per device.

Profiling can be based on:

- Role, defining the user type or the user group to which the user belongs.
- Device type, such as Windows machine, Smart Phone, iPad, iPhone, Android, etc.
- Username/ password pair.
- Location, based on the AP group to which the endpoint is connected
- Time of the day, based on what time of the day the endpoint is allowed on the network.
- EAP type, to check what EAP method the client uses to get connected.

Policing is decided based on a profile which are:

- VLAN
- QoS Level
- ACL
- Session timeout value

This section contains the following subsections:

Configuring Client Profiling

Configuring Client Profiling (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID. The WLANs > Edit page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the RADIUS and Local Client Profiling area, do the following:

a) To profile clients based on DHCP, select the **DHCP Profiling** check box.

b) To profile clients based on HTTP, select the **HTTP Profiling** check box.

You can configure client profiling in both RADIUS mode and Local mode on the WLAN.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Client Profiling (CLI)

- Enable or disable client profiling for a WLAN based on DHCP by entering this command:

  config wlan profiling radius dhcp {**enable** | **disable**} *wlan-id*

- Enable or disable client profiling in RADIUS mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  config wlan profiling radius {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

  Note Use the **all** parameter to configure client profiling based on both DHCP and HTTP.

- Enable or disable client profiling in Local mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- To see the status of client profiling on a WLAN, enter the following command:

  show wlan *wlan-id*

- To enable or disable debugging of client profiling, enter the following command:

  debug profiling {**enable** | **disable**}