Configuring Per-WLAN RADIUS Source Support

- Prerequisites for Per-WLAN RADIUS Source Support, on page 1
- Per-WLAN RADIUS Source Support, on page 1
- Configuring Per-WLAN RADIUS Source Support (CLI), on page 2
- Monitoring the Status of Per-WLAN RADIUS Source Support (CLI), on page 2

Prerequisites for Per-WLAN RADIUS Source Support

- You must implement appropriate rule filtering on the new identity for the authentication server (RADIUS) because the controller sources traffic only from the selected interface.

Per-WLAN RADIUS Source Support

The sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the Dynamic interfaces. If a RADIUS server is reachable via a Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

To filter WLANs, use the callStationID that is set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

This section contains the following subsections:

Configuring Per-WLAN RADIUS Source Support (CLI)

Step 1 Enter the **config wlan disable** *wlan-id* command to disable the WLAN.

Step 2 Enter the following command to enable or disable the per-WLAN RADIUS source support:

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan-id*

Note When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN. When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

Step 3 Enable either an AP group's interface or a WLAN's interface for RADIUS packet routing by entering these commands:

- AP group's interface—**config wlan radius_server overwrite-interface apgroup** *wlan-id*
- WLAN's interface—**config wlan radius_server overwrite-interface wlan** *wlan-id*

Note Valid WLAN ID range is between 1 and 16.

Step 4 Enter the **config wlan enable** *wlan-id* command to enable the WLAN.

Note You can filter requests on the RADIUS server side using CiscoSecure ACS. You can filter (accept or reject) a request depending on the NAS-IP-Address attribute through a Network Access Restrictions rule. The filtering to be used is the CLI/DNIS filtering.

Monitoring the Status of Per-WLAN RADIUS Source Support (CLI)

To see if the feature is enabled or disabled, enter the following command:

show wlan *wlan-id*

Example

The following example shows that the per-WLAN RADIUS source support is enabled on WLAN 1.

show wlan *1*

Information similar to the following is displayed:

```
WLAN Identifier.................................. 4
Profile Name..................................... example
Network Name (SSID).............................. example
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
```

```
...
Radius Servers
   Authentication.............................. Global Servers
   Accounting.................................. Global Servers
   Overwrite Sending Interface................. Enabled
Local EAP Authentication........................ Disabled
```