RADIUS Accounting

Information About RADIUS Accounting of AP Events

This topic describes the configuration of a RADIUS server to monitor a network with regards to Access Points (APs). Prior to Cisco IOS XE Amsterdam 17.1.1 release, during times of network issues, the controller would not send accounting messages when APs join and disjoin from the controller. From Cisco IOS XE Amsterdam 17.1.1 release onwards, the RADIUS server keeps a record of all the APs that were down and have come up.

Configuring Accounting Method-List for an AP Profile

Procedure

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

Step 2	**ap profile** *ap-profile-name*
	
	Example:
	
	`Device(config)# ap profile`
	`ap-profile-name`
		Configures the AP profile. The default AP join profile name is *default-ap-profile*.

Step 3	**[no] accounting method-list** *method-list-name* **Example:**	Configures the accounting method list for the AP profile.

Command or Action	Purpose
`Device(config-ap-profile)# [no] accounting method-list method-list-name`	Use the **no** form of this command to disable the command.

Verifying the AP Accounting Information

To verify the AP accounting information, use the following command:

```
Device#show wireless stats ap accounting
Base MAC        Total packet Send   Total packet Received Methodlist
--------------------------------------------------------------------------------------
00b0.e192.0f20    4         3      abc
38ed.18cc.5788    8         8      ML_M
70ea.1ae0.af08    0         0      ML_A
```

To view the details of a method list that is configured for an AP profile, use the following command:

```
Device#show ap profile name Method-list detailed
AP Profile Name              : test-profile
Description                  :
.
.
.
Method-list name             : Method-list
Packet Sequence Jump DELBA   : ENABLED
Lag status                   : DISABLED
.
Client RSSI Statistics
  Reporting                  : ENABLED
  Reporting Interval         : 30 seconds
```

AAA Accounting

Configuring AAA Accounting Using Default Method List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa accounting commands** *privilege_level* **default start-stop group** *group-name* **Example:** `Device(config)# aaa accounting commands 15 default start-stop group group-name`	Creates an accounting method list and enables accounting. • *privilege_level*: AAA accounting level. The valid range is from 0 to 15. • *group-name*: AAA accounting group that supports only TACACS+ group.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring HTTP Command Accounting Using Named Method List (CLI)

Procedure

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

Step 2	**ip http accounting commands** *level named-accounting-method-list*
	
	Example:
	
	`Device(config)# ip http accounting commands 1 oneacct`
		Configures HTTP command accounting using the named method list.
		
		• *level*: Privilege value from 0 to 15. By default, the following command privilege levels are available on the controller:
		
		    • *0*: Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
		
		    • *1*: Includes all the user-level commands at the controller prompt (>).
		
		    • *15*: Includes all the enable-level commands at the controller prompt (>).
		
		• *named-accounting-method-list*: Name of the predefined command accounting method list.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Feature History for Device Ecosystem Data

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Device Ecosystem Data

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Device Ecosystem Data	This feature sends device analytics data in the RADIUS accounting request to Cisco ISE to profile the endpoints.

Information About Device Ecosystem Data

Edge analytics is the process of collecting, processing, and analyzing data from devices in a network. The controller learns about endpoint attributes, such as model number, operating system version, and other information from a set of endpoints using device analytics. The device analytics data is further shared with Cisco Identity Services Engine (ISE) to profile the endpoints. This information sharing is in addition to the DHCP and HTTP attributes already being shared with Cisco ISE using RADIUS accounting messages.

Enable Device Ecosystem Data

✎

Note Before proceeding with the configuration, ensure that device classifier and accounting features are enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a wireless policy profile.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile.
Step 4	**radius-profiling** **Example:** `Device(config-wireless-policy)# radius-profiling`	Configures client radius profiling.
Step 5	**dot11-tlv-accounting** **Example:**	Configures the controller to send device analytics data that is found in the RADIUS

	Command or Action	Purpose
	`Device(config-wireless-policy)# dot11-tlv-accounting`	accounting request to Cisco ISE in order to profile the endpoints. The **no** form of this command disables the feature.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 7	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Verify Device Ecosystem Data

Use the following command to verify device ecosystem data in RADIUS accounting configuration:

```
Device# show wireless profile policy detailed <name>
.
.
.
WLAN Local Profiling
  Subscriber Policy Name          : Not Configured
  RADIUS Profiling                : ENABLED
  HTTP TLV caching                : DISABLED
  DHCP TLV caching                : DISABLED
  DOT11 TLV accounting            : ENABLED
.
.
.
```