RADIUS Accounting

RADIUS accounting of AP events

RADIUS accounting of AP events is a network monitoring mechanism that

- Tracks the status transitions of APs within a wireless controller environment
- Records AP join and disjoin events
- Provides historical visibility into AP downtime and uptime through accounting messages sent to a RADIUS server.

Feature History

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 table

Feature Name	Release	Description
Device Ecosystem Data	Cisco IOS XE 17.10.1	This feature sends device analytics data that is present in the RADIUS accounting request to Cisco ISE to profile endpoints The command is introduced: • dot11-tlv-accounting

Feature Name	Release	Description
Chargeable User Identity in RADIUS Accounting	Cisco IOS XE 17.9.1	Chargeable User Identity (CUI) is a unique identifier for a client visiting a network. This attribute can be used as an alternative for the client's username as part of the authentication process. The command is introduced: • dot11-tlv-accounting
Improved Logging in RADIUS Accounting	Cisco IOS XE 17.1.1	Prior to Cisco IOS XE Amsterdam 17.1.1 release, the controller did not send accounting messages for AP join and disjoin events during network issues. From Cisco IOS XE Amsterdam 17.1.1 Release and later, the RADIUS server keeps a record of all APs that were down and have come up.

Configure accounting method-list for an AP profile

Define an accounting method list within an access point (AP) profile to enable or disable accounting for AP operations.

Use this task to specify how accounting is managed for an AP profile on your device. This allows tracking of AP events and assists with auditing and troubleshooting

Before you begin

- Identify the AP profile name you want to configure. The default AP profile name is `default-ap-profile`.
- Determine the accounting method list name you wish to apply.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP profile. The default AP join profile name is default-ap-profile.

Example:

```
Device(config)# ap profile ap-profile-name
```

Step 3 Configure the accounting method list for the AP profile.

Example:

```
Device(config-ap-profile)# [no] accounting method-list method-list-name
```

Use the **no** form of this command to disable the accounting method list.

The system associates the specified accounting method list with the AP profile, enabling or disabling accounting

Example

```
Device# configure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# [no] accounting method-list method-list-name
```

Verify AP accounting information

Verify the AP accounting information, including the MAC address, packets sent, packets received, and the method list.

```
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
```

View details for a method list configured for an AP profile.

```
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

Configure AAA accounting using default method list (CLI)

Use this task to monitor and record user command activity on devices through AAA accounting features.

Configure AAA accounting to track user commands executed on a controller, leveraging the default accounting method. This supports compliance and security needs.

Before you begin

- Confirm that AAA is enabled on the device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create an accounting method list and enables accounting.

Example:

```
Device(config)# aaa accounting commands 15 default start-stop group group-name
```

- *privilege_level*: AAA accounting level. The valid range is from zero to 15.
- *group-name*: AAA accounting group that supports only TACACS+ group.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The controller records user command activities according to the configured accounting method.

Configure HTTP command accounting using named method list (CLI)

Set up command accounting to track user actions on network devices via HTTP with a specified AAA method list using commands.

HTTP command accounting provides auditing and compliance by recording commands executed by users. Using a named method list offers flexibility for different accounting requirements.

Before you begin

- Ensure AAA accounting is enabled on your device.
- Have a predefined AAA accounting method list (if not, configure one).

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure HTTP command accounting using the named method list.

Example:

```
Device(config)# ip http accounting commands 1 oneacct
```

- *level*: The privilege value ranges from zero to 15. By default, the command privilege levels available on the controller are:
  - *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 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The device records user command activities in accordance with the configured accounting method.

Device ecosystem data

A device ecosystem data set is a collection of endpoint analytics that

- aggregates key attributes such as model number, OS version, and device type
- enables controllers to build comprehensive profiles of endpoints in a network, and
- supports integration with systems like Cisco Identity Services Engine (ISE) for security and policy management.

Feature history

Table 2: Feature History for Device ecosystem data

Feature	Release	Feature Information
Device ecosystem data	Cisco IOS XE 17.10.1	This feature includes device analytics data in the RADIUS accounting request sent to Cisco ISE. Cisco ISE uses this data to profile the endpoints.

Device ecosystem data uses device analytics to enhance DHCP and HTTP attribute sharing. This process provides richer endpoint profiling for access control and network management. For example, device ecosystem data can reveal an endpoint's operating system version and model. These insights enable more precise security policies in Cisco ISE.

Enable device ecosystem data

Enable the device ecosystem data feature so that the controller can send enhanced device analytics to ISE for improved endpoint profiling.

Before you begin

Before you proceed with the configuration, ensure that device classifier and accounting features are enabled.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a policy profile for wireless devices.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Disable the wireless policy profile.

Example:

```
Device(config-wireless-policy)# shutdown
```

Step 4 Configure client RADIUS profiling.

Example:

```
Device(config-wireless-policy)# radius-profiling
```

Step 5 Configure the controller to send device analytics data found in RADIUS accounting requests to Cisco ISE. This enables endpoint profiling.

Example:

```
Device(config-wireless-policy)# dot11-tlv-accounting
```

Use the **no** form of this command to disable the feature.

Step 6 Enable the wireless policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 7 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The controller now sends device analytics data found in RADIUS accounting requests to Cisco ISE for device profiling.

```
Device# configure terminal
Device(config)# wireless profile policy default-profile-policy
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# dot11-tlv-accounting
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

Verify device ecosystem data

Use this 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
.
.
.
```