Common Wireless Event Log Messages

When monitoring your wireless environment, the event log (in the Dashboard at Monitor > Event log) can be an invaluable tool in gaining additional visibility into current activity. A list of the common wireless event log messages along with their origin and their potential causes can help to bring a better understanding of the wireless environment.

802.11 Event Log Messages

The 802.11 event log messages are from codes specified in the 802.11 wireless standard from the Institute of Electrical and Electronic Engineers (IEEE). The full list of specified 802.11 reason codes can be found in IEEE's documentation in this article (requires account) under "Table 9-45—Reason codes" in section "9.4.1.7 Reason Code field".

- **802.11 association** - Denotes the joining of a client to an AP on a specified channel with the current received signal strength indication (RSSI).

  Example:

  May 26 14:45:21 00:18:0a:00:00:01 101 IPAD2 802.11 association channel: 36, rssi: 45

Below is an example of the association process as specified by the 802.11 standard:

![Association Process Diagram](image)

- **802.11 disassociation: previous authentication expired** - A client that is attempting to join the service set identifier (SSID) is incorrectly entering the pre-shared key (PSK), or a client left the BSSID without sending a deauthentication frame (could be from a client shutting down or leaving the AP)

- **802.11 disassociation: client has left AP** - A client informed the AP that it should no longer keep the client in its association table. You may see this if the client has potentially gone into a hibernate state, a powered down state,
or the client may have chosen to roam to another AP.

Example:

May 26 14:51:35 00:18:0a:00:00:01 101 IPAD2 802.11 disassociation client has left AP

- **802.11 disassociation: Client association expired** - Client was disassociated due to inactivity. If a client is not heard from for 5 minutes, then the client will be disassociated.

- **802.11 disassociation: Client was deauthenticated** - Sending STA is leaving or has left Independent BSS or ESS. Client indicated to the AP that it's disconnecting from the wireless network. Could be from a client going into 'sleep' mode and disconnecting the WiFi radio for battery savings.

- **802.11 disassociation: unknown reason** - A client is no longer communicating with the AP, yet failed to notify the AP that it should be dropped from the association table. This problem is typically associated with wireless interference, but can be caused by any issue that would cause a client to suddenly stop being heard by an AP.

- **802.11 association rejected for load balancing** - A client that was attempting to join with an access point was rejected, as the access point in question was attempting to steer the client toward another access point in order to evenly distribute the client loads to another nearby access point

- **DFS Event Detected** - The access point detected a radar signal and dynamically took action as to not interfere with the radar. To read more about DFS events please refer to our guide on Dynamic Frequency Selection (DFS)

---

**WPA Event Log Messages**

- **WPA authentication** - Denotes that the client has successfully entered the pre-shared key (PSK) for the associated SSID.

Example:

May 26 14:54:16 00:18:0a:00:00:01 101 IPAD2 WPA authentication

- **WPA deauthentication** - Signifies that the secure session to the client (known by association ID or AID) has ended to the virtual access point (VAP aka SSID) on the listed radio number.

Example:

May 26 14:51:35 00:18:0a:00:00:01 101 IPAD2 WPA deauthentication vap: 0, radio: 1, aid: 1844047018

---

**802.1X/RADIUS Event Log Messages**

- SSIDs that use WP2-Enterprise for authenticating splash pages will have related 802.1X and RADIUS messages in the event log

- You may occasionally see 802.1X re-authentication messages at periodic intervals which is explained [here](#).

Example of a **successful** 802.1X sequence in the event logs (using Meraki-hosted RADIUS):
Example of a failed (due to incorrect password) 802.1X sequence in the event logs (using Meraki-hosted RADIUS):

May 26 15:29:34 00:18:0a:00:00:01 101 IPAD2 802.11 disassociation client has left AP
May 26 15:29:34 00:18:0a:00:00:01 101 IPAD2 802.1X deauthentication identity: caleb@meraki.com, vap: 0, radio: 1
May 26 15:29:34 00:18:0a:00:00:01 101 IPAD2 802.1X EAP failure identity: caleb@meraki.com, vap: 0, radio: 1
May 26 15:29:30 00:18:0a:00:00:01 101 IPAD2 802.11 association channel: 36, rssi: 46

Below is an example of the 802.1X authentication process as specified by the 802.11 standard (Supplicant = client, Authenticator = AP, AS = RADIUS server):

![Diagram of 802.1X authentication process](image)

**Air Marshal Event Log Messages**

- The Air Marshal capabilities of Meraki APs can provide detection and classification of potential attacks in the wireless environment.

- The frequency of the messages and the associated MAC address(es) can help to diagnose. More information on the Air Marshal product can be found [here](#).

- *Single or multiple device packet flood* - Denotes that an AP has detected that single or multiple client(s) have attempted to flood the wireless environment with a type of packet. These messages can indicate a malicious attack or temporary, client-based misbehavior.

Examples:
• **Channel scan** - When APs are not serving clients, they can scan channels on which they were previously serving clients to identify attacks.

Example:

May 26 13:52:03 00:18:0a:00:00:01 Channel scan channel: 36, clients: 0, active: 0