



## System Messages and Access Point LED Patterns

---

This appendix lists system messages that can appear on the Cisco Unified Wireless Network Solution interfaces and describes the LED patterns on lightweight access points. It contains these sections:

- [System Messages, page D-2](#)
- [Using Client Reason and Status Codes in Trap Logs, page D-4](#)
- [Using Lightweight Access Point LEDs, page D-6](#)

# System Messages

Table D-1 lists system messages and descriptions.

**Table D-1 System Messages and Descriptions**

Error Message	Description
STATION_DISASSOCIATE	Client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	Client may have intentionally terminated usage or it could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch or other configuration issues.
STATION_ASSOCIATE_FAIL	Check load on the Cisco Radio or signal quality issues.
LRAD_ASSOCIATED	The associated Cisco 1000 Series lightweight access point is now managed by this Cisco Wireless LAN Controller.
LRAD_DISASSOCIATED	Cisco 1000 Series lightweight access point may have associated with a different Cisco Wireless LAN Controller or may have become completely unreachable.
LRAD_UP	Cisco 1000 Series lightweight access point is operational, no action required.
LRAD_DOWN	Cisco 1000 Series lightweight access point may have a problem or is administratively disabled.
LRADIF_UP	Cisco Radio is UP.
LRADIF_DOWN	Cisco Radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	Client density may have exceeded system capacity.
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceed configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel -- check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	Possible coverage hole detected - check Cisco 1000 Series lightweight access point history to see if common problem - add Cisco 1000 Series lightweight access points if necessary.
LRADIF_LOAD_PROFILE_PASSED	Load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	Detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	Detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	Number of clients receiving poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.

**Table D-1 System Messages and Descriptions (continued)**

<b>Error Message</b>	<b>Description</b>
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue. Use maps and trends to investigate.
ROGUE_AP_REMOVED	Detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	Port may have a problem or is administratively disabled.
LINK_FAILURE	Port may have a problem or is administratively disabled.
AUTHENTICATION_FAILURE	Attempted security breach. Investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPSec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for attempt to spoof IP Address.
IPSEC_ESP_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for IPSec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for IPSec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	Maximum number of supported Cisco Radios exceeded. Check for controller failure in the same Layer 2 network or add another controller.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning and/or other cooling arrangements.

**Table D-1 System Messages and Descriptions (continued)**

Error Message	Description
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor ASAP.
TEMPERATURE_SENSOR_CLEAR	Temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check ports — possible serious failure detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
SWITCH_UP	Controller is responding to SNMP polls.
SWITCH_DOWN	Controller is not responding to SNMP polls, check controller and SNMP settings.
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the controller.
CONFIG_SAVED	Running configuration has been saved to flash - will be active after reboot.
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor Cisco Wireless LAN Controller temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for power-supply malfunction.
COLD_START	Cisco Wireless LAN Controller may have been rebooted.
WARM_START	Cisco Wireless LAN Controller may have been rebooted.
The Radios associated with Controller A.B.C.D <sup>1</sup> exceeded license count of 36. The current number of radios on the controller is 36.	Indicates the user is trying to add more access points than the license count allows.

1. A.B.C.D represents the controller MAC address.

## Using Client Reason and Status Codes in Trap Logs

The WCS Clients > Detail page lists the reason and status codes that you are likely to encounter when reviewing the trap logs. [Table D-2](#) lists client reason codes and descriptions. [Table y](#) lists client status codes and descriptions.

### Client Reason Codes

This table lists client reason codes.

**Table D-2** *Client Reason Code Descriptions and Meanings*

<b>Client Reason Code</b>	<b>Description</b>	<b>Meaning</b>
0	noReasonCode	Normal operation.
1	unspecifiedReason	Client associated but no longer authorized.
2	previousAuthNotValid	Client associated but not authorized.
3	deauthenticationLeaving	The access point went offline, deauthenticating the client.
4	disassociationDueToInactivity	Client session timeout exceeded.
5	disassociationAPBusy	The access point is busy, performing load balancing, for example.
6	class2FrameFromNonAuthStation	Client attempted to transfer data before it was authenticated.
7	class2FrameFromNonAssStation	Client attempted to transfer data before it was associated.
8	disassociationStaHasLeft	Operating System moved the client to another access point using non-aggressive load balancing.
9	staReqAssociationWithoutAuth	Client not authorized yet, still attempting to associate with an access point.
99	missingReasonCode	Client momentarily in an unknown state.

## Client Status Codes

This table lists client status codes.

**Table D-3** *Client Status Code Descriptions and Meanings*

<b>Client Status Code</b>	<b>Description</b>	<b>Meaning</b>
0	idle	Normal operation — no rejections of client association requests.
1	aaaPending	Completing an AAA transaction.
2	authenticated	802.11 authentication completed.
3	associated	802.11 association completed.
4	powersave	Client in powersave mode.
5	disassociated	802.11 disassociation completed.
6	tobedeleted	To be deleted after disassociation.

**Table D-3 Client Status Code Descriptions and Meanings (continued)**

Client Status Code	Description	Meaning
7	probing	Client not associated or authorized yet.
8	disabled	Automatically disabled by Operating System for an operator-defined time.

## Using Lightweight Access Point LEDs

This table describes the meaning of LED patterns on lightweight access points.

**Table D-4 Cisco 1000 Series Lightweight Access Point LED Conditions and Status**

LED Conditions				Status
Power	Alarm	2.4 GHz	5 GHz	
Green on	off	on or off	on or off	Controller found, code OK, normal status.
Green on	off	Yellow on	on or off	802.11b/g activity.
Green on	off	on or off	Amber on	802.11a activity.
off	Red on	off	off	Lightweight access point starting up.
All LEDs cycle back and forth				Lightweight access point searching for controller. Stops when controller and DHCP server are found.
All LEDs blink on and off together				Controller found, code upgrade in process.
off	Red flashing	off	off	Duplicate lightweight access point IP address.