WCS Event and Alarm Severities

Double-quotations enclose variables that are replaced with resource names when the message is displayed.

Critical Events and Alarms

1. The PoE controller has failed on the controller “{0}”.
2. AP “{0}”, interface “{1}” is down on controller “{2}”.
3. AP “{0}” disassociated from controller “{1}”
4. Controller “{0}”. RADIUS server(s) are not responding to authentication requests.
5. Port “{0}” is down on controller “{1}”.
6. Rogue AP “{0}” is on wired network.
7. User “{1}” with IP address “{0}” has made too many unsuccessful login attempts.
8. AP “{0}” with protocol “{1}” on controller “{2}” is contained as a rogue, preventing service.
9. Fake AP or other attack may be in progress. Rogue AP count on system “{0}” has exceeded the security warning threshold of “{1}”.
10. Fake AP or other attack may be in progress. Rogue AP count on AP with MAC address “{0}” associated with controller “{2}” has exceeded the security warning threshold of “{1}”.
11. Controller “{0}” detected duplicate IP address “{0}” being used by machine with MAC address “{1}”.
12. AP “{0}” on controller “{3}” detected duplicate IP address “{2}” being used by machine with MAC address “{1}”.
13. The AP “{0}” with protocol “{1}” received a message with a large NAV field and all traffic on the channel has been suspended. This is most likely a malicious DoS attack.
14. The AP “{1}” received a WPA MIC error on protocol “{2}” from Station “{0}”. Counter measures have been activated and traffic has been suspended for 60 seconds.
15. Controller “{0}” is unreachable.
16. IDS signature attack detected on controller “{0}”. The signature type is “{1}”, signature name is “{2}”, and signature description is “{3}”.
17. Transmitter failure detected on the “{0}” radio of AP “{1}” on controller “{2}”.
18. Receiver failure detected on the “{0}” radio of AP “{1}” on controller “{2}”.

19. AP impersonation with MAC “{0}” is detected by authenticated AP “{1}” on “{2}” radio and Slot ID “{3}”.
20. AP functionality has been disabled for key “{0}”, reason being “{1}” for feature set “{2}”.
21. AP “{1}” is unable to associate. The regulatory domain configured on it “{3}” does not match the controller “{0}” country code “{2}”.
22. CPU Receive Multicast Queue is full on controller “{0}”.
23. Failed to authorize AP “{0}”. Authorization entry does not exist in AP authorization list of controller “{1}” .
24. Failed to authorize AP “{0}”. AP’s authorization key does not match with SHA1 key in AP authorization list of controller “{1}” .
25. Failed to authorize AP “{0}”. Controller “{1}” could not verify the self-signed certificate from the AP.
26. Failed to authorize AP “{0}”. AP has a self-signed certificate, whereas the AP authorization list of controller “{1}” has manufactured installed certificate for this AP.
27. Radio with MAC address “{0}” and protocol “{1}” is down. The reason is “{2}”.
28. Radio with MAC address “{0}” and protocol “{1}” that has joined controller “{2}” has invalid interface. The reason is “{3}”.
29. The Cisco Intrusion Detection System “{0}” has detected a possible intrusion attack by the wireless client “{1}”.
30. Controller “{0}” is “{1}” with the central time server.
31. MFP configuration of the WLAN was violated by the radio interface “{0}” and detected by the radio interface “{1}” of the AP with MAC address “{2}”. The violation was “{3}”.
32. Guest user “{1}” deleted on controller “{0}”.

Major Events and Alarms

1. The radios associated with controller “{0}” exceeded license count “{1}”. The current number of radios on this controller is “{2}”.
2. The sensed temperature on the controller “{0}” is too high. The current sensed temperature is “{1}”.
3. The sensed temperature on the controller “{0}” is too low. The current sensed temperature is “{1}”.
4. The temperature sensor failed on the controller “{0}”. Temperature is unknown.
5. Adhoc rogue “{0}” was found and has been auto-contained as per WPS policy.
6. Rogue AP “{0}” was advertising the SSID and has been auto-contained as per WPS policy.
7. Trusted AP “{0}” has invalid encryption. It is using “{1}” instead of “{2}”. It has been auto-contained as per WPS policy.
8. Trusted AP “{0}” has invalid radio policy. It is using “{1}” instead of “{2}”. It has been auto-contained as per WPS policy.
9. Trusted AP “{0}” has invalid SSID. It has been auto-contained as per WPS policy.
10. Trusted AP “{0}” is missing or has failed.

11. Trusted AP "{0}" on controller "{3}" has invalid preamble. It is using "{1}" instead of "{2}". It has been auto-contained as per WPS policy.
12. Keepalive messages are lost between master and controller "{0}".

Minor Events and Alarms

1. AP "{0}", interface "{1}". Load threshold violated.
2. AP "{0}", interface "{1}". Noise threshold violated.
3. AP "{0}", interface "{1}". Interference threshold violated.
4. AP "{0}", interface "{1}". Coverage threshold of "{3}" is violated. Total number of clients is "{5}" and number failed clients is "{4}".
5. Controller "{0}". User authentication from controller "{0}" failed for user name "{1}" and user type "{2}".
6. Client "{0}", which was associated with AP "{1}", interface "{2}" is excluded. The reason code is "{3}".
7. IPsec IKE negotiation failure from remote IP address "{0}".
8. IPsec invalid cookie from remote IP address "{0}".
9. Rogue AP "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}". Radio type "{2}" with RSSI "{5}" and SNR "{6}".
10. The WEP key configured at the station may be wrong. Station MAC address is "{0}", AP MAC is "{1}", and Slot ID is "{2}".
11. AP "{0}" with static IP configured as "{2}" has fallen back to the working DHCP address "{1}".
12. Absence of <Element> with MAC <macAddress>, last seen at <timestamp>
13. <Element> with MAC <macAddress> is <In | Out> the Area <campus | building | floor | coverageArea>
14. <Element> with MAC <macAddress> has moved beyond <specifiedDistance> ft. of marker <MarkerName>, located at a range of <foundDistance> ft.

Clear Events and Alarms

1. AP "{0}", interface "{1}" is up.
2. AP "{0}", interface "{1}". Load changed to acceptable.
3. AP "{0}", interface "{1}". Noise changed to acceptable.
4. AP "{0}", interface "{1}". Interference changed to acceptable.
5. AP "{0}", interface "{1}". Coverage changed to acceptable.
6. Port "{0}" is up on controller "{1}".
7. Rogue AP "{0}" is removed; it was detected as rogue AP by AP "{1}". Radio type "{2}".
8. Rogue AP "{0}" is not able to connect to the wired network.
9. The temperature sensor is working now on the controller "{0}". The sensed temperature is "{1}".
10. Controller "{0}" is reachable.

11. Adhoc rogue “{0}” was found and was auto-contained. The alert state is clear now.
12. Rogue AP “{0}” was advertising the SSID and was auto-contained. The alert state is clear now.
13. Trusted AP “{0}” had invalid encryption. The alert state is clear now.
14. Trusted AP “{0}” had invalid radio policy. The alert state is clear now.
15. Trusted AP “{0}” had invalid SSID. The alert state is clear now.
16. Trusted AP “{0}” is missing or has failed. The alert state is clear now.
17. Controller “{0}” is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.
18. Transmitter failure cleared on the “{0}” radio of AP “{1}” on controller “{2}”.
19. Receiver failure cleared on the “{0}” radio of AP “{1}” on controller “{2}”.
20. Trusted AP ”{0}“ on controller ”{3}” had invalid preamble. The alert state is clear now.
21. Radio with MAC address “{0}” and protocol “{1}” is up. The reason is “{2}”.
22. Radar has been cleared on channel “{1}”, which was detected by AP base radio MAC “{0}” on radio 802.11a.
23. The Cisco Intrusion Detection System “{0}” has cleared the wireless client “{1}” from possibly having generated an intrusion attack.

Informational Events and Alarms

1. Controller “{0}”. Configuration saved in flash.
2. Controller “{0}”. Multiple users logged in.
3. Controller “{0}”. Cold start.
4. AP “{0}” associated with controller “{2}” on port number “{1}”.
5. AP “{0}”, interface “{1}”. Transmit power level changed to “{2}”.
6. AP “{0}”, interface “{1}”. Channel changed to “{2}”. Interference energy before update was “{3}” and after update is “{4}”.
7. RRM 802.11a grouping done; the new group leader MAC address is “{0}”.
8. RRM 802.11b/g grouping done; the new group leader MAC address is “{0}”.
9. Controller “{0}”. Authentication failure reported
10. Client “{0}” is associated with AP “{1}”, interface “{2}”.
11. Client “{0}” with user name “{3}” is authenticated with AP “{1}”, interface “{2}”.
12. Client “{0}” is disassociated from AP “{1}”, interface “{2}” with reason code “{3}”.
13. Client “{0}” is deauthenticated from AP “{1}”, interface “{2}” with reason code “{3}”.
14. Client “{0}” has failed authenticating with AP “{1}”, interface “{2}”. The reason code is “{3}”.
15. Client “{0}” failed to associate with AP “{1}”, interface “{2}”. The reason code is “{3}”.
16. Rogue AP “{0}” is cleared explicitly. It is not detected anymore.
17. Fake AP or other attack is cleared now. Rogue AP count on system “{0}” is within the threshold of “{1}”.

18. Fake AP or other attack on AP with MAC address “{0}” associated with controller “{2}” is cleared now. Rogue AP count is within the threshold of “{1}”.
19. Global “{1}” network status disabled on controller with IP address “{0}”.
20. Global “{1}” network status enabled on controller with IP address “{0}”.
21. Radio with MAC address “{0}” and protocol “{1}” has core dump on controller “{2}”.
22. AP “{0}” tried to join controller “{1}” and failed. The controller does not support this kind of AP.
23. Radar has been detected on channel “{1}” by AP base radio MAC “{0}” on radio 802.11a.