Alarms and Events

This chapter describes the type of events and alarms reported, how to view alarms and events by product or entity and severity, and how to view IDS signature attacks. It contains these sections:

- Using the Alarm Summary, page 16-1
- Monitoring Alarms, page 16-5
- Viewing Alarm Details, page 16-9
- Alarm and Event Dictionary, page 16-26

An event is an occurrence or detection of some condition in and around the network. For example, it can be a report about radio interference crossing a threshold, the detection of a new rogue access point, or a controller rebooting.

Events are not generated by a controller for each and every occurrence of a pattern match. Some pattern matches must occur a certain number of times per reporting interval before they are considered a potential attack. The threshold of these pattern matches is set in the signature file. Events can then generate alarms which further can generate e-mail notifications if configured as such.

An alarm is a Cisco WCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the WCS raises an alarm until the resulting condition no longer occurs. For example, an alarm may be raised while a rogue access point is detected, but the alarm terminates after the rogue has not been detected for several hours.

One or more events can result in a single alarm being raised. The mapping of events to alarms is their correlation function. For example, some IDS events are considered to be network wide so all events of that type (regardless of which access point the event is reported from) map to a single alarm. On the other hand, other IDS events are client-specific. For these, all events of that type for a specific client MAC address map to an alarm which is also specific for that client MAC address, regardless of whether multiple access points report the same IDS violation. If the same kind of IDS violation takes place for a different client, then a different alarm is raised.

A WCS administrator currently has no control over which events generate alarms or when they time out. On the controller, individual types of events can be enabled or disabled (such as management, SNMP, trap controls, etc.).

Using the Alarm Summary

When WCS receives an alarm message from a controller, it displays an alarm indicator at the top of the WCS page (see Figure 16-1).
Using the Alarm Summary

The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box. You must unselect the preference of hiding acknowledged alarms if you want acknowledged alarms to show on the WCS Alarm Summary and alarms lists page. By default, acknowledged alarms are not shown.

Critical (red), Major (orange) and Minor (yellow) alarms are shown in the alarm dashboard, left-to-right.

**Figure 16-1  WCS Alarm Summary**

Alarms indicate the current fault or state of an element that attention, and they are usually generated by one or more events. The alarm can be cleared but the event remains.

**Note**

Alarm counts refresh every 15 seconds.

**Note**

If an alarm is acknowledged, it does not appear on the alarm summary page by default. To change this setting, go to Administration > Settings > Alarms and deselect the Hide acknowledged alarms check box.

Alarms are color coded as follows:

- Red—Critical Alarm
- Orange—Major Alarm
- Yellow—Minor Alarm

The Alarm Summary displays the number of current critical, major, and minor alarms (see **Figure 16-2**).
Figure 16-2 Alarm Summary Page for WCS

Figure 16-3

Click the alarm count number link in the Alarm Summary page to view the Monitor > Alarms page for these alarms.

Click the blue down arrow in the Alarm Summary page to expand the alarm summary (see Figure 16-3).
Chapter 16      Alarms and Events

Using the Alarm Summary

The expanded summary includes alarm counts for the following:

- **Access Points**—Displays counts for AP alarms such as AP Disassociated from controller, Thresholds violation for Load, Noise or Interference, AP Contained as Rogue, AP Authorization Failure, AP regulatory domain mismatch, or Radio card Failure. See the “Monitoring Alarms” section on page 16-5 for more information.
- **Controllers**—Displays counts for controller alarms, such as reachability problems from WCS and other controller failures (fan failure, POE controller failure, AP license expired, link down, temperature sensor failure, and low temperature sensed). See the “Monitoring Alarms” section on page 16-5 for more information.
- **Coverage Hole**—Displays counts for coverage hole alarms generated for access points whose clients are not having enough coverage set by thresholds. See the “Monitoring Maps Overview” section on page 5-2 for more information.
- **Malicious AP**—Displays counts for malicious rogue access points alarms. See the “Monitoring Rogue Access Point Alarms” section on page 16-10 for more information.
- **Mesh Links**—Displays counts for mesh link alarms, such as poor SNR, console login, excessive parent change, authorization failure, or excessive association failure. See the “Monitoring Alarms” section on page 16-5 for more information.
- **Mobility**—Displays counts for location alarms such as reachability problems from WCS and location notifications (In/Out Area, Movement from Marker, or Battery Level). See the “Monitoring Alarms” section on page 16-5 for more information.
- **Security**—Displays counts for security alarms such as Signature Attacks, AP Threats/Attacks, and Client Security Events. See the “Monitoring Alarms” section on page 16-5 for more information.
- **Unclassified AP**—Displays counts for unclassified rogue access point alarms. See the “Monitoring Rogue Access Point Alarms” section on page 16-10 for more information.
- **WCS**—Displays counts for WCS alarms such as e-mail failures and license violation alarms.

**Customizing Alarm Summary Results**

If you click **Edit View** from the Alarm Summary page (shown in Figure 16-2), you can customize which results you want to appear in the Alarm Summary page.

Column names appear in one of the following lists:

- **Hide Information**—Lists columns that do not appear in the table. The **Hide** button points to this list.
- **View Information**—Lists columns that do appear in the table. The **Show** button points to this list.
To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the Shift or Control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

The Alarm Summary items to choose from are as follows:

- Owner
- Date/Time
- Message
- Acknowledged
- Category
- Condition

## Monitoring Alarms

This section provides information on the following:

- Monitoring Alarm Overview, page 16-5
- Using Edit View for Alarms, page 16-8
- Viewing Alarm Details, page 16-9
- Monitoring Rogue Access Point Alarms, page 16-10
- Using Advanced Search, page 16-12
- Viewing Rogue Access Point Details, page 16-14
- Acknowledging Alarms, page 16-16
- Monitoring Adhoc Rogue Alarms, page 16-19
- Rogue Access Point Location, Tagging, and Containment, page 16-21
- Monitoring Rogue Alarm Events, page 16-22
- Monitoring E-mail Notifications, page 16-23

## Monitoring Alarm Overview

Choose **Monitor > Alarms** to open the Alarms page. This page summarizes the controller alarms (see Figure 16-4).

**Note**

You can search for a specific alarm or type of alarm by using the WCS search feature. See “Using the Search Feature” section on page 2-31 for more information on searching for an alarm or alarm type.
This page displays a table of logged alarms. For more information, see Table 16-1.
Table 16-1  Monitor Alarms Page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Check box)</td>
<td>Enables you to select one or more alarms. You can take action on selected alarms using the Select a command drop-down list.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the alarm’s level of severity ranging from critical to minor.</td>
</tr>
<tr>
<td></td>
<td>• Red circle—Critical</td>
</tr>
<tr>
<td></td>
<td>• Orange downward triangle—Major</td>
</tr>
<tr>
<td></td>
<td>• Yellow upward triangle—Minor</td>
</tr>
<tr>
<td>Failure Source</td>
<td>Indicates the device that triggered the alarm.</td>
</tr>
<tr>
<td></td>
<td>Note When you move your mouse cursor over an individual failure source, additional information regarding the failure and its location displays. The same information appears in the Message column.</td>
</tr>
<tr>
<td>Owner</td>
<td>Displays the name of the person to whom this alarm is assigned, if one was entered.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Displays the date and time that the alarm occurred.</td>
</tr>
<tr>
<td>Message</td>
<td>Indicates the reason for the alarm.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
<tr>
<td>Category</td>
<td>Displays the alarm’s assigned category such as rogue AP, controller, switch, and security.</td>
</tr>
<tr>
<td></td>
<td>This column does not appear by default. You can add this column to the table in the Edit View page. To go to the Edit View page, click Edit View. See the “Using Edit View for Alarms” section on page 16-8 for more information.</td>
</tr>
<tr>
<td>Condition</td>
<td>Displays the current condition that caused the alarm.</td>
</tr>
<tr>
<td></td>
<td>This column does not appear by default. You can add this column to the table in the Edit View page. To go to the Edit View page, click Edit View. See the “Using Edit View for Alarms” section on page 16-8 for more information.</td>
</tr>
</tbody>
</table>

When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

To add, remove, or reorder columns in the table, click Edit View to go to the Edit View page.
Select a Command Menu

Using the Select a command drop-down list, you can make the following changes to the selected alarms:

- Assign to me—Assign the selected alarms to the current user.
- Unassign—Unassign the selected alarms.
- Delete—Delete the selected alarms.
- Clear—Clear the selected alarms.
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Opens the All Alarms > Email Notification page where you can view and configure e-mail notifications.

To make a change to a selected alarm, follow these steps:

**Step 1** Select an alarm by checking the check box.
**Step 2** From the command drop-down list, select a command.
**Step 3** Click Go.

Using Edit View for Alarms

The Edit View page allows you to add, remove, or reorder columns in the alarms table (see Figure 16-5).

**Figure 16-5 Edit View Page**

To edit the available columns in the alarms table, follow these steps:
Step 1  Choose Monitor > Alarms.

Step 2  Click Edit View.

Step 3  To add an additional column to the alarms table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the alarms table.

Step 4  To remove a column from the alarms table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. Not all items in the left column appear in the alarms table.

Step 5  Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

Step 6  Click Reset to restore the default view.

Viewing Alarm Details

In the Monitor > Alarms page, click an item under Failure Source to access the alarms details page (see Figure 16-6).

Figure 16-6  Alarm Details Page

This page provides the following information (Table 16-2):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Source</td>
<td>Device that generated the alarm.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of person to which this alarm is assigned, or blank.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
</tbody>
</table>
Viewing Alarm Details

Note

The General information may vary depending on the type of alarm. For example, some alarm details may include location and switch port tracing information.

- Annotations—Enter any new notes in this box and click Add to update the alarm. Notes appear in the “Annotations” display area.
- Messages—Displays information about the alarm.
- Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.
  Configuration audit alarms are generated when audit discrepancies are enforced on config groups.
  
  Note
  If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group.
  
  The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens you to the Monitoring Rogue Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

## Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more access points.

To open the Rogue AP Alarms page, do one of the following:

- Search for rogue Access Points. See the “Using Advanced Search” section on page 16-12 for more information about the search feature.
- In the WCS home page, click the Security tab. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.

### Table 16-2  General Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>The category of the alarm (for example, AP, Rogue AP, or Security).</td>
</tr>
<tr>
<td>Created</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm created.</td>
</tr>
<tr>
<td>Modified</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm last modified.</td>
</tr>
<tr>
<td>Generated By</td>
<td>Device that generated the alarm.</td>
</tr>
<tr>
<td>Severity</td>
<td>Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.</td>
</tr>
</tbody>
</table>
Click the **Malicious AP** number link in the Alarm Summary box. See the “Using the Alarm Summary” section on page 16-1 for more information.

**Note**

If there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Rogue AP Alarms page contains the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check box</td>
<td>Select the alarms on which you want to take action.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates the severity of the alarm: Critical, Major, Minor, Clear.</td>
</tr>
<tr>
<td>Rogue MAC Address</td>
<td>Indicates the MAC address of the rogue access points. See Monitor Alarms &gt; Rogue AP Details.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Rogue access point vendor name or Unknown.</td>
</tr>
<tr>
<td>Classification Type</td>
<td>Malicious, Friendly, or Unclassified.</td>
</tr>
<tr>
<td>Radio Type</td>
<td>Indicates the radio type for this rogue access point.</td>
</tr>
<tr>
<td>Strongest AP RSSI</td>
<td>Indicates the which signal strength indicator that was the strongest for this WCS (including all detecting access points for all controllers and across all detection times).</td>
</tr>
<tr>
<td>No. of Rogue Clients</td>
<td>Indicates the number of rogue clients associated to this access point.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Indicates the date and time that the alarm occurred.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates the state of the alarm. Includes Alert, Known or Removed.</td>
</tr>
<tr>
<td>SSID</td>
<td>Indicates the service set identifier being broadcast by the rogue access point radio. It is blank if SSID is not being broadcast.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Indicates the map location for this rogue access point.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
</tbody>
</table>

**Note**
The alarm remains in WCS, and you can search for all Acknowledged alarms using the alarm search functionality.

**Select a Command**

Select one or more alarms by checking their respective check boxes, select one of the following commands from the Select a Command drop-down list, and click **Go**.

- Assign to me—Assign the selected alarms to the current user.
- Unassign—Unassign the selected alarms.
- Delete—Delete the selected alarms.
- Clear—Clear the selected alarms.
• Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See the “Acknowledging Alarms” section on page 16-16 for more information.

Note

The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

• Unacknowledge—Unacknowledge an already acknowledged alarm.

• E-mail Notification—Opens the All Alarms > E-mail Notification page where you can view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.

Caution

Attempting to contain a rogue access point may lead to legal consequences. When you select any of the AP Containment commands, and click Go, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click OK if you are sure or click Cancel if you do not wish to contain any access points.

Using Advanced Search

When the access points on your wireless LAN are powered up and associated with controllers, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

Follow these steps to find rogue access point alarms using Advanced Search.

Step 1 Click Advanced Search in the top right-hand corner of the WCS main page.

Step 2 Choose Rogue Client from the Search Category drop-down list.

Step 3 (optional) You can filter the search even further with the other search criteria if desired.

Step 4 Click Search.

Step 5 The list of rogue clients appears (see Figure 16-7).

Figure 16-7 Rogue Clients Page

Step 6 Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears (see Figure 16-8).
Figure 16-8  Rogue Client Detail Page

<table>
<thead>
<tr>
<th>General</th>
<th>Location Information: Client is not detected by any WSE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC Address</td>
<td>&quot;00:13:02:86:e4:92&quot;</td>
</tr>
<tr>
<td>Number of Detecting APs</td>
<td>16</td>
</tr>
<tr>
<td>First Heard</td>
<td>Wed Apr 07 07:13:03 2009</td>
</tr>
<tr>
<td>Last Heard</td>
<td>Wed Apr 8 11:00:48 2009</td>
</tr>
<tr>
<td>Rogue AP MAC Address</td>
<td>00:13:02:86:e4:92</td>
</tr>
<tr>
<td>Status</td>
<td>Alert</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence: 0</td>
</tr>
<tr>
<td>Containment: 0</td>
</tr>
<tr>
<td>Distance: 0</td>
</tr>
<tr>
<td>All: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APs that detected this Rogue Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Radio Name</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
<tr>
<td>0157:5f:1d:8f:5d</td>
</tr>
</tbody>
</table>
Chapter 16      Alarms and Events

Viewing Alarm Details

Step 7 To modify the alarm, choose one of these commands from the Select a command drop-down list, and click Go.

- Set State to ‘Unknown-Alert’—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send dauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
- Map (High Resolution)—Displays the current calculated rogue location on the Maps > Building Name > Floor Name page.
- Location History—Displays the history of the rogue client location based on RF fingerprinting.

Note The client must be detected by an MSE for the location history to appear.

Configuring Alarm Severity

The Settings > Severity Configuration page allows you to change the severity level for newly generated alarms.

Note Existing alarms remain unchanged.

To reconfigure the severity level for a newly generated alarm, follow these steps:

Step 1 Choose Administration > Settings.
Step 2 From the left sidebar menu, select Severity Configuration.
Step 3 Select the check box of the alarm condition whose severity level you want to change.
Step 4 From the Configure Security Level drop-down list, select from the following severity levels:
  - Critical
  - Major
  - Minor
  - Warning
  - Informational
  - Reset to Default
Step 5 Click Go.
Step 6 Click OK to confirm the change or Cancel to leave the security level unchanged.

Viewing Rogue Access Point Details

Alarm event details for each rogue access point are available from the Rogue AP Alarms page.
Follow these steps to view alarm events for a rogue access point radio.

### Step 1
In the Rogue AP Alarms page, click an item under **Rogue MAC Address**.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by access points. The following information is available:

- **General**—
  - Rogue MAC Address—MAC address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.
  - Rogue Type—Indicates the rogue type such as AP.
  - On Network—Indicates whether or not the rogue access point is located on the network.
  - Owner—Indicates the owner or is left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue access point.
  - Containment Level—Indicates the containment level of the rogue access point or Unassigned.
  - Radio Type—Indicates the radio type for this rogue access point.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this access point.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - Event Details—Click to open the Monitor > Events page.
  - Switch Port Trace Status—Indicates the switch port trace status. See the **Switch Port Trace** section on page 18-60 or the **Using Switch Port Tracing** section on page 10-56 for additional information.

- Switch Port Tracing Details—Provides the most recent switch port tracing details. To view additional trace details, use the **Click here for more details** link.

- Rogue Client—Lists rogue clients for this access point including the client MAC address, the last date and time the client was heard, and the current client status.

- Message—Describes the alarm.

- Annotations—Lists current notes regarding this rogue access point. To add a new note, click **New Annotation**. Type the note and click **Post** to save and display the note or **Cancel** to close the page without saving the note.

- Location Notifications—Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
**Acknowledging Alarms**

You may want to remove certain alarms from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you may want to stop that access point from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, click the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, WCS will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

Any alarms, once acknowledged, will not show up on either the Alarm Summary page or any alarm list page. Also, no e-mails are generated for these alarms after you have marked them as acknowledged.

By default, acknowledged alarms cannot be found with any search criteria. To change this default, go to the **Administration > Settings > Alarms** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled (see Figure 16-9).

*Figure 16-9  Alarm Warning*

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. WCS automatically deletes cleared alerts that are more than seven days old; therefore, your results can show activity only for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which WCS has already generated an alarm.

**Monitoring Air Quality Alarms**

The Air Quality Alarms page displays air quality alarms on your network.

To access the air quality alarms page, do one of the following:

- Perform a search for Performance alarms.
- Click the Performance number link in the Alarm Summary dialog box. See “Using the Alarm Summary” for more information.

The Monitor Air Quality Alarms page contains the following parameters:
Viewing Alarm Details

- Severity—Indicates the severity of the alarm including:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Critical</td>
</tr>
<tr>
<td>🔴</td>
<td>Major</td>
</tr>
<tr>
<td>🔴</td>
<td>Minor</td>
</tr>
<tr>
<td>🔴</td>
<td>Warning</td>
</tr>
<tr>
<td>🟢</td>
<td>Info</td>
</tr>
<tr>
<td>🔴</td>
<td>Clear—Displays if the interferer is no longer detected by any access point.</td>
</tr>
</tbody>
</table>

- Failure Source—Device that generated the alarm.
- Owner—Name of the person to which this alarm is assigned, or blank.
- Date/Time—The time at which the alarm was generated.
- Message—The associated message displayed in the WCS alarm browser.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user. See “Acknowledging Alarms” for more information.

**Monitor Air Quality Alarms > Select a Command Menu**

Select one or more alarms by selecting their respective check boxes, choose one of the following commands from the Select a Command drop-down list, and click Go.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Delete—Delete the selected alarm(s)
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See “Acknowledging Alarms” for more information.

**Note** The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page where you can view and configure email notifications. See “Monitoring E-mail Notifications” for more information.
Monitoring CleanAir Security Alarms

The CleanAir Security Alarms page displays security alarms on your network.

To access the security alarms page, do one of the following:

- Perform a search for Security alarms.
- Click the Security number link in the Alarm Summary box. See “Using the Alarm Summary” for more information.

The Monitor CleanAir Security Alarms page contains the following parameters:

- Severity—Indicates the severity of the alarm including:
  - Failure Source—Device that generated the alarm.
  - Owner—Name of the person to which this alarm is assigned, or blank.
  - Date/Time—The time at which the alarm was generated.
  - Message—The associated message displayed in the WCS alarm browser.
  - Acknowledged—Displays whether or not the alarm is acknowledged by the user. See “Acknowledging Alarms” for more information.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Critical</td>
</tr>
<tr>
<td>🔄</td>
<td>Major</td>
</tr>
<tr>
<td>🔄</td>
<td>Minor</td>
</tr>
<tr>
<td>🔄</td>
<td>Warning</td>
</tr>
<tr>
<td>🔄</td>
<td>Info</td>
</tr>
<tr>
<td>🔄</td>
<td>Clear—Displays if the interferer is no longer detected by any access point.</td>
</tr>
</tbody>
</table>

- Monitor Security Alarms > Select a Command Menu

Select one or more alarms by checking their respective check boxes, select one of the following commands from the Select a Command drop-down list, and click Go.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Delete—Delete the selected alarm(s)
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary page. See “Acknowledging Alarms” for more information.
Note

The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page where you can view and configure email notifications. See “Monitoring E-mail Notifications” for more information.

### Monitoring Adhoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues.

To access the Adhoc Rogue Alarms page, do one of the following:

- Search for ad hoc rogue alarms. See the “Using the Search Feature” section on page 2-31 for more information.
- In the WCS home page, click the Security tab. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

The Adhoc Rogue Alarms page contains the following parameters:

| Parameter               | Description                                                                 |
|-------------------------|                                                                           |
| Check box               | Choose the alarms on which you want to take action.                      |
| Severity                | The severity of the alarm including Critical, Major, Minor, and Clear. These severity levels are color-coded. |
| Adhoc Rogue MAC Address | Indicates the MAC address of the ad hoc rogue.                           |
| Vendor                  | Indicates the ad hoc rogue vendor name or Unknown.                       |
| Classification Type     | Indicates the classification type of the ad hoc rogue including malicious, friendly, or unclassified. |
| Radio Type              | Indicates this ad hoc rogue’s radio type.                                |
| Strongest AP RSSI       | Indicates the strongest received signal strength indicator in dBm.       |
| No. of Rogue Clients    | Indicates the number of rogue clients associated to this ad hoc rogue.   |
| Owner                   | Indicates the owner of the ad hoc rogue.                                 |
| Date/Time               | Indicates the date and time that the alarm occurred.                    |
| State                   | Indicates the current state of the alarm including alert, known, or removed. |
| SSID                    | Service Set Identifier that is being broadcast by the ad hoc rogue radio. It is blank if there is no broadcast. |
| Map Location            | Indicates the map location for this ad hoc rogue.                       |
| Acknowledged            | Displays whether or not the alarm is acknowledged by the user.           |
Monitoring Adhoc Rogue Details

Alarm event details for each ad hoc rogue are available from the Adhoc Rogue Alarms page. Follow these steps to view the alarm events for an ad hoc rogue radio.

Step 1

In the Adhoc Rogue Alarms page, click an item under **Rogue MAC Address**.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco lightweight access points. The following information is available:

- **General**
  - Rogue MAC Address—Media Access Control address of the ad hoc rogue.
  - Vendor—Ad hoc rogue vendor name or Unknown.
  - On Network—Indicates whether or not the ad hoc rogue is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the ad hoc rogue radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the ad hoc rogue.
  - Containment Level—Indicates the containment level of the ad hoc rogue or Unassigned.
  - Radio Type—Indicates the radio type for this ad hoc rogue.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this ad hoc.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.

- Annotations—Enter any new notes in this box and click **Add** to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitor Alarms > Events page.
- Annotations—Lists existing notes for this alarm.
Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Find rogue access points.
- Receive new rogue access point notification, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Find the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment is done for individual rogue access points by MAC address or is mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security.
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security.
  - Tag rogue access points as unknown until they are eliminated or acknowledged.
  - Tag rogue access points as contained and discourage clients from disassociating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting Access Points

Click a Rogues alarm square in the Alarm Monitor (lower left-hand side of the screen) to access the Monitor Alarms > <failure object> page. In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access the Monitor Alarms > Rogue AP Details page, from the Select a command drop-down list choose Detecting APs, and click Go to access this page.

Choose Monitor > Alarms, then click New Search in the left sidebar. Choose Severity > All Severities and Alarm Category > Rogue AP, and click Go to access Monitor Alarms > <Failure Objects>.

In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access Monitor Alarms > Rogue AP Details. In the Monitor Alarms > Rogue - <vendor:MACaddr> page, from the Select a command drop-down list, choose Detecting APs to access this page.

This page enables you to view information about the Cisco lightweight access points that are detecting a rogue access point.

Click a list item to display data about that item:
- AP Name
- Radio
**Viewing Alarm Details**

- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

**Monitoring Rogue Alarm Events**

The Events page enables you to review information about rogue alarm events. Events list the sequence of occurrences for an element over a period of time.

To open the Rogue AP Alarms details page, follow these steps:

**Step 1**
To display the Rogue AP Alarms page, do one of the following:
- Search for rogue access points. See “Using the Search Feature” section on page 2-31 for more information about the search feature.
- In the WCS home page, click the **Security** tab. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box. See “Using the Alarm Summary” section on page 16-1 for more information.

**Step 2**
In the Rogue AP Alarms page, click the Rogue MAC Address for the appropriate rogue access point. The Rogue AP Alarm details page appears.

**Step 3**
From the Select a command drop-down list, click **Event History**.

**Step 4**
Click Go. The Rogue AP Events page appears.

**Note**
Any Airlink vendors appear as Alpha.

Click the title of each column to reorder the listings:
- Severity—Color coded display of the severity of the event.
- Rogue MAC Address—Click a list item to display information about the entry.
- Vendor—Name of rogue access point manufacturer.
- Type—AP or AD-HOC.
- On Network—Whether or not the rogue access point is on the same subnet as the associated Port.
- On 802.11a—Whether or not the rogue access point is broadcasting on the 802.11a band.
- On 802.11b—Whether or not the rogue access point is broadcasting on the 802.11b/802.11g band.
• Date/Time—Date and time of the alarm.
• Classification Type—Malicious, Friendly, or Unclassified
• State—State of the alarm, such as Alert and Removed.
• SSID—Service Set Identifier being broadcast by the rogue access point radio.

**Monitoring E-mail Notifications**

You can configure the delivery of e-mail notifications for specific alarm categories and severity levels.

To configure e-mail notifications, follow these steps:

1. Choose Monitor > Alarms.
2. From the Select a command drop-down list, choose E-mail Notification.
3. Click an Alarm Category to edit severity level and e-mail recipients for its e-mail notifications.
4. Choose the severity level check box(es) (Critical, Major, Minor, Warning) for which you want a notification sent.
5. Enter the notification recipient e-mail addresses in the To text box.
6. Click OK.
7. Click the Enabled check box for appropriate alarm categories to activate the delivery of e-mail notifications.
8. Click OK.

**Monitoring Severity Configurations**

You can change the severity level for newly generated alarms.

To change the severity level of newly-generated alarms, follow these steps:

1. Choose Administration > Setting.
2. Choose Severity Configuration from the left sidebar menu.
3. Choose the check box of the alarm condition for which you want to change the severity level.
4. From the Configure Severity Level drop-down list, choose the new severity level (Critical, Major, Minor, Warning, Informational, Reset to Default).
5. Click Go.
Viewing Alarm Details

Step 6 Click OK to confirm the change.

Monitoring CleanAir Air Quality Events

You can use Cisco WCS to view the events generated on the air quality of the wireless network. To view air quality events, follow these steps:

Step 1 Click Advanced Search in the top right of the main WCS page. The New Search page appears.

Step 2 In the New Search page, choose Events from the Search Category drop-down list.

Step 3 From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4 From the Event Category drop-down list, choose Performance.

Step 5 Click Go.

The air quality events page displays the following information:

- Severity—Indicates the severity of the alarm including:
  - Critical
  - Major
  - Minor
  - Warning
  - Info
  - Clear—Displays if the interferer is no longer detected by any access point.

- Failure Source—Device that generated the alarm.
- Date/Time—The time at which the alarm was generated.

Viewing Air Quality Event Details

To view air quality event details, follow these steps:

Step 1 In the Air Quality Events page, click an item under Failure Source to access the alarm details page. See Monitoring CleanAir Air Quality Events.

Step 2 The air quality event page displays the following information:
• Failure Source—Device that generated the alarm.
• Category—The category this event comes under. In this case, Performance.
• Created—The time stamp at which the event was generated.
• Generated by—The device that generated the event.
• Device IP Address—The IP address of the device that generated the event.
• Severity—The severity of the event.
• Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
• Message—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

You can use Cisco WCS to view the security events generated on your wireless network.

To view interferer security events, follow these steps:

Step 1  Click **Advanced Search** in the top right of the main WCS page.

The New Search page appears.

Step 2  In the New Search page, choose **Events** from the Search Category drop-down list.

Step 3  From the Severity drop-down list, choose the type of severity you want to search the air quality events.

Step 4  From the Event Category drop-down list, choose **Security**.

Step 5  Click **Go**.

The interferer security events page displays the following information:

• Severity—Indicates the severity of the alarm including:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Critical</td>
</tr>
<tr>
<td>▼</td>
<td>Major</td>
</tr>
<tr>
<td>⬤</td>
<td>Minor</td>
</tr>
<tr>
<td>⬤</td>
<td>Warning</td>
</tr>
<tr>
<td>🔴</td>
<td>Info</td>
</tr>
<tr>
<td>🔴</td>
<td>Clear—Displays if the interferer is no longer detected by any access point.</td>
</tr>
</tbody>
</table>

• Failure Source—Device that generated the alarm.
• Date/Time—The time at which the alarm was generated.
Viewing Interferer Security Risk Event Details

To view interferer security event details, follow these steps:

**Step 1**
In the Interferer Security Event details page, click an item under Failure Source to access the alarm details page. See Monitoring Interferer Security Risk Events.

**Step 2**
The air quality event page displays the following information:
- **Failure Source**—Device that generated the alarm.
- **Category**—The category this event comes under. In this case, Security.
- **Created**—The time stamp at which the event was generated.
- **Generated by**—The device that generated the event.
- **Device IP Address**—The IP address of the device that generated the event.
- **Severity**—The severity of the event.
- **Alarm Details**—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- **Message**—Describes the interferer device affecting the access point.

Alarm and Event Dictionary

This section describes the event and alarm notifications that the wireless LAN controller, access points, and location appliances can receive. In addition, specific actions an administrator can do to address these alarms and events are described.

**Note**
Not all traps which are seen on the WLC GUI are supported by WCS.

**Notification Format**

For each alarm and event notification, the following information is provided:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>The notification title is generally picked up from an event property file defined in the NMS.</td>
</tr>
<tr>
<td><strong>MIB Name</strong></td>
<td>The MIB Name is the name of the notification as defined in the management information base (MIB). In some cases, if the event is specific only to the NMS, this field is not relevant. You can define multiple events in WCS from the same trap based on the values of the variables present in the trap. In such cases, multiple subentries appear with the same MIB Name. In addition, this field displays the value of the variable that caused WCS to generate this event.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WCS Message</td>
<td>The WCS Message is a text string that reflects the message displayed in the WCS alarm or event browser associated with this event. Numbers such as &quot;{0}&quot; reflect internal WCS variables that typically are retrieved from variables in the trap. However, the order of the variables as they appear in the trap cannot be derived from the numbers.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This field displays the symptoms associated with this event.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>This field displays the severity assigned to this event in WCS.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>This field lists the probable causes of the notification.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>This field lists any actions recommended for the administrator managing the wireless network.</td>
</tr>
</tbody>
</table>
Traps Added in Release 2.0

**AP_BIG_NAV_DOS_ATTACK**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnApBigNavDosAttack.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The AP ”{0}” with protocol ”{1}” receives a message with a large NAV field and all traffic on the channel is suspended. This is most likely a malicious denial of service attack.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system detected a possible denial of service attack and suspended all traffic to the affected channel.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A malicious denial of service attack is underway.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the source of the attack in the network and take the appropriate action immediately.</td>
</tr>
</tbody>
</table>

**AP_CONTAINED_AS_ROGUE**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPContainedAsARogue.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP ”{0}” with protocol ”{1}” on Switch ”{2}” is contained as a Rogue preventing service.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point is reporting that it is being contained as a rogue.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Another system is containing this access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the system containing this access point. You may need to use a wireless sniffer.</td>
</tr>
</tbody>
</table>

**AP_DETECTED_DUPLICATE_IP**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDuplicateIpAddressReported.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP ”{0}” on Switch ”{3}” detected duplicate IP address ”{2}” being used by machine with mac address ”{1}”.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system detects a duplicate IP address in the network that matches that assigned to an access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Another device in the network is configured with the same IP address as an access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Correct the misconfiguration of IP addresses in the network.</td>
</tr>
</tbody>
</table>
**AP_HAS_NO_RADIOS**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnApHasNoRadioCards.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Not supported in WCS yet.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point is reporting that it has no radio cards.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>N/A.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Manufacturing fault or damage to the system during shipping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Call customer support.</td>
</tr>
</tbody>
</table>

**AP_MAX_ROGUE_COUNT_CLEAR**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnApMaxRogueCountClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Fake AP or other attack on AP with MAC address &quot;{0}&quot; associated with Switch &quot;{2}&quot; is cleared now. Rogue AP count is within the threshold of &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The number of rogues detected by a switch (controller) is within acceptable limits.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>N/A.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**AP_MAX_ROGUE_COUNT_EXCEEDED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnApMaxRogueCountExceeded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Fake AP or other attack may be in progress. Rogue AP count on AP with MAC address &quot;{0}&quot; associated with Switch &quot;{2}&quot; has exceeded the severity warning threshold of &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The number of rogues detected by a switch (controller) exceeds the internal threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes           | • There may be too many rogue access points in the network.  
• A fake access point attack may be in progress. |
| Recommended Actions       | Identify the source of the rogue access points. |

**AUTHENTICATION_FAILURE (From MIB-II standard)**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>AuthenticationFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. Authentication failure reported.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>There was an SNMP authentication failure on the switch (controller).</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>
Alarm and Event Dictionary

<table>
<thead>
<tr>
<th>Probable Causes</th>
<th>An incorrect community string is in use by a management application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Actions</td>
<td>Identify the source of the incorrect community string and correct the string within the management application.</td>
</tr>
</tbody>
</table>

### BSN_AUTHENTICATION_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAuthenticationFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. User authentication from Switch &quot;{0}&quot; failed for user name &quot;{1}&quot; and user type &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A user authentication failure is reported for a local management user or a MAC filter is configured on the controller.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Incorrect login attempt by an admin user from the controller CLI or controller GUI, or a client accessing the WLAN system.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>If the user has forgotten the password, the superuser may need to reset it.</td>
</tr>
</tbody>
</table>
### COLD_START (FROM MIB-II STANDARD)

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>coldStart.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. Cold start.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The switch (controller) went through a reboot.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>
| Probable Causes| • The switch (controller) has power-cycled.  
|                | • The switch (controller) went through a hard reset.  
|                | • The switch (controller) went through a software restart. |
| Recommended Actions | None.               |

### CONFIG_SAVED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnConfigSaved.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. Configuration saved in flash.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A configuration save to flash is performed on the switch (controller).</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The switch (controller) saves the configuration to the flash via a CLI command or entry via the controller GUI or WCS.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>If you change the configuration using the controller CLI or controller GUI, you may need to refresh the configuration.</td>
</tr>
</tbody>
</table>

### IPSEC_IKE_NEG_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnIpsecIkeNegFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>IPsec IKE Negotiation failure from remote IP address &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Unable to establish an IPsec tunnel between a client and a WLAN appliance.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Configuration mismatch.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Validate configuration, verify that authentication credentials match (preshared keys or certificates); and verify that encryption algorithms and strengths match.</td>
</tr>
</tbody>
</table>
### Alarm and Event Dictionary

#### IPSEC_INVALID_COOKIE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnIpsecInvalidCookieTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>IPsec Invalid cookie from remote IP address &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Cannot successfully negotiate an IPsec session.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Synchronization problem. The client believes a tunnel exists while the WLAN appliance does not. This problem often happens when the IPsec client does not detect a disassociation event.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Reset the IPsec client and then restart tunnel establishment.</td>
</tr>
</tbody>
</table>

#### LINK_DOWN  *(FROM MIB-II STANDARD)*

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>linkDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Port &quot;{0}&quot; is down on Switch &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The physical link on one of the switch (controller) ports is down.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes | • An access point or a port was manually disconnected from the network.  
                   • A port failure. |
| Recommended Actions | Troubleshoot physical network connectivity to the affected port. |

#### LINK_UP *(FROM MIB-II STANDARD)*

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>linkUp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Port &quot;{0}&quot; is up on Switch &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The physical link is up on a switch (controller) port.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A physical link to the switch (controller) is restored.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

#### LRAD_ASSOCIATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPAssociated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot; associated with Switch &quot;{2}&quot; on Port number &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point has associated with a switch (controller).</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>
| Probable Causes    | • A new access point has joined the network.  
                   • An access point has associated with a standby switch (controller) due to a failover.  
                   • An access point rebooted and reassociated with a switch (controller). |
| Recommended Actions| None. |
## LRAD_DISASSOCIATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPDisassociated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;[0]&quot; disassociated from Switch &quot;[1].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The switch (controller) is no longer detecting an access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• A failure in the access point.</td>
</tr>
<tr>
<td></td>
<td>• An access point is no longer on the network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check if the access point is powered up and has network connectivity to the switch (controller).</td>
</tr>
</tbody>
</table>

## LRADIF_COVERAGE_PROFILE_FAILED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPCoverageProfileFailed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;[0],&quot; interface &quot;[1].&quot; Coverage threshold of &quot;[3]&quot; is violated. Total no. of clients is &quot;[5]&quot; and no. failed clients is &quot;[4].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Number of clients experiencing suboptimal performance has crossed the configured threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Many clients are wandering to the remote parts of the coverage area of this radio interface with no handoff alternative.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>• If the configured threshold is too low, you may need to readjust it to a more optimal value.</td>
</tr>
<tr>
<td></td>
<td>• If the coverage profile occurs on a more frequent basis, you may need to provide additional radio coverage.</td>
</tr>
<tr>
<td></td>
<td>• If the power level of this radio can be manually controlled, you may need to boost it to increase the coverage area.</td>
</tr>
</tbody>
</table>

## LRADIF_COVERAGE_PROFILE_PASSED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPCoverageProfileUpdatedToPass.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;[0],&quot; interface &quot;[1].&quot; Coverage changed to acceptable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface that was reporting coverage profile failure has reverted to an acceptable level.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The number of clients on this radio interface with suboptimal performance has dropped below the configured threshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## LRADIF_CURRENT_CHANNEL_CHANGED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPCurrentChannelChanged.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0},&quot; interface &quot;{1}&quot;. Channel changed to &quot;{2}&quot;. Interference Energy before update was &quot;{3}&quot; and after update is &quot;{4}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The current channel assigned to a radio interface has automatically changed.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Possible interference on a channel has caused the radio management software on the controller to change the channel.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## LRADIF_CURRENT_TXPOWER_CHANGED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPCurrentTxPowerChanged.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0},&quot; interface &quot;{1}&quot;. Transmit Power Level changed to &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The power level has automatically changed on a radio interface.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The radio management software on the controller has modified the power level for optimal performance.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## LRADIF_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPIfDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0},&quot; interface &quot;{1}&quot; is down.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface is out of service.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical if not disabled, otherwise Informational.</td>
</tr>
</tbody>
</table>
| Probable Causes                 | • A radio interface has failed.  
                                 | • An administrator has disabled a radio interface.  
                                 | • An access point has failed and is no longer detected by the controller. |
| Recommended Actions             | If the access point is not administratively disabled, call customer support. |
### LRADF_INTERFERENCE_PROFILE_FAILED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPInterferenceProfileFailed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot; interface &quot;{1}&quot;. Interference threshold violated.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The interference detected on one or more channels is violated.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>There are other 802.11 devices in the same band that are causing interference on channels used by this system.</td>
</tr>
</tbody>
</table>
| Recommended Actions | • If the interference threshold is configured to be too low, you may need to readjust it to a more optimum value.  
• Investigate interference sources such as other 802.11 devices in the vicinity of this radio interface.  
A possible workaround is adding one or more access points to distribute the current load or slightly increasing the threshold of the access point which is displaying this message. To perform this workaround, follow the steps below:  
1. Choose **Configure > Controllers**.  
2. Click any IP address in that column of the All Controllers page.  
3. From the left sidebar menu, choose **802.11a/n** or **802.11b/g/n** and then **RRM Thresholds**.  
4. Adjust the Interference Threshold (%) in the Other Thresholds section. |

### LRADIF_INTERFERENCE_PROFILE_PASSED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPInterferenceProfileUpdatedToPass.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot; interface &quot;{1}&quot;. Interference changed to acceptable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface reporting interference profile failure has reverted to an acceptable level.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The interference on this radio interface has dropped below the configured threshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
**LRADIF_LOAD_PROFILE_FAILED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPLoadProfileFailed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot;, interface &quot;{1}&quot;. Load threshold violated.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface of an access point is reporting that the client load has crossed a configured threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>There are too many clients associated with this radio interface.</td>
</tr>
</tbody>
</table>
| Recommended Actions       | • Verify the client count on this radio interface. If the threshold for this trap is too low, you may need to readjust it.  
• Add new capacity to the physical location if the client count is a frequent issue on this radio. |

**LRADIF_LOAD_PROFILE_PASSED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPLoadProfileUpdatedToPass.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot;, interface &quot;{1}&quot;. Load changed to acceptable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface that was reporting load profile failure has reverted to an acceptable level.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The load on this radio interface has dropped below the configured threshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**LRADIF_NOISE_PROFILE_FAILED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPNoiseProfileFailed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot;, interface &quot;{1}&quot;. Noise threshold violated.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The monitored noise level on this radio has crossed the configured threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Noise sources that adversely affect the frequencies on which the radio interface operates.</td>
</tr>
</tbody>
</table>
| Recommended Actions       | • If the noise threshold is too low, you may need to readjust it to a more optimal value.  
• Investigate noise sources in the vicinity of the radio interface (for example, a microwave oven). |
**LRADIF_NOISE_PROFILE_PASSED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPNoiseProfileUpdatedToPass.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;[0],&quot; interface &quot;[1].&quot; Noise changed to acceptable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface that was reporting noise profile failure has reverted to an acceptable level.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The noise on this radio interface has dropped below the configured threshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**LRADIF_UP**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPIfUp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;[0],&quot; interface &quot;[1]&quot; is up.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio interface is back up.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• An administrator has enabled a radio interface.</td>
</tr>
<tr>
<td></td>
<td>• An access point has turned on.</td>
</tr>
<tr>
<td></td>
<td>• A new access point has joined the network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**MAX_ROGUE_COUNT_CLEAR**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnMaxRogueCountClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Fake AP or other attack is cleared now. Rogue AP count on system &quot;[0]&quot; is within the threshold of &quot;[1].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The number of rogues detected by a controller is within acceptable limits.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>N/A.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
**MAX_ROGUE_COUNT_EXCEEDED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnMaxRogueCountExceeded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Fake AP or other attack may be in progress. Rogue AP count on system &quot;{0}&quot; has exceeded the severity warning threshold of &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The number of rogues detected by a controller exceeds the internal threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes               | • There are too many rogue access points in the network.  
• A fake access point attack is in progress. |
| Recommended Actions           | Identify the source of the rogue access points. |

**MULTIPLE_USERS**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>multipleUsersTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. Multiple users logged in.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Multiple users with the same login ID are logged in through the CLI.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The same user has logged in multiple times through the CLI interface.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Verify that the expected login sessions for the same user are valid.</td>
</tr>
</tbody>
</table>

**NETWORK_DISABLED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnNetworkStateChanged (bsnNetworkState set to disabled).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Global &quot;{1}&quot; network status disabled on Switch with IP Address &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An administrator has disabled the global network for 802.11a/n and 802.11b/g/n.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Administrative command.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**NO_ACTIVITY_FOR_ROGUE_AP**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>This is a WCS-only event generated when no rogue activity is seen for a specific duration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Rogue AP &quot;{0}&quot; is cleared explicitly. It is not detected anymore.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A rogue access point is cleared from the management system due to inactivity.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A rogue access point is not located on any managed controller for a specified duration.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### POE_CONTROLLER_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnPOEControllerFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The POE controller has failed on the Switch &quot;{0}&quot;.</td>
</tr>
<tr>
<td>SYMPTOMS</td>
<td>A failure in the Power Over Ethernet (POE) unit is detected.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The power of the Ethernet unit has failed.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Call customer support. The unit may need to be repaired.</td>
</tr>
</tbody>
</table>

### RADIOS_EXCEEDED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRadiosExceedLicenseCount.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The Radios associated with Switch &quot;{0}&quot; exceeded license count &quot;{1}&quot;. The current number of radios on this switch is &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The number of supported radios for a switch (controller) has exceeded the licensing limit.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The number of access points associated with the switch (controller) has exceeded the licensing limits.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Upgrade the license for the switch (controller) to support a higher number of access points.</td>
</tr>
</tbody>
</table>

### RADIUS_SERVERS_FAILED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRADIUSServerNotResponding.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot;. RADIUS server(s) are not responding to authentication requests.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The switch (controller) is unable to reach any RADIUS server for authentication.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Network connectivity to the RADIUS server is lost or the RADIUS server is down.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Verify the status of all configured RADIUS servers and their network connectivity.</td>
</tr>
</tbody>
</table>
ROGUE_AP_DETECTED

MIB Name | bsnRogueAPDetected.
---|---
WCS Message | Rogue AP or ad hoc rogue "{0}" with SSID "{3}" and channel number "{4}" is detected by AP "{1}" Radio type "{2}" with RSSI "{5}" and SNR "{6}".
Symptoms | The system has detected a rogue access point.
WCS Severity | Minor if not on a wired network; Critical if on a wired network.
Probable Causes | • An illegal access point is connected to the network.
• A known internal or external access point unknown to this system is detected as rogue.
Recommended Actions | • Verify the nature of the rogue access point by tracing it using its MAC address or the SSID, or by using location features to locate it physically.
• If the access point is a known internal or external access point, acknowledge it or mark it as a known access point. Consider adding it to the known access point template within WCS.
• If the access point is deemed to be a severity threat, contain it using the management interface.

ROGUE_AP_ON_NETWORK

MIB Name | bsnRogueAPDetectedOnWiredNetwork
---|---
WCS Message | Rogue AP or ad hoc rogue "{0}" is on the wired network.
Symptoms | A rogue access point is found reachable through the wired network.
WCS Severity | Critical.
Probable Causes | An illegal access point was detected as reachable through the wired network.
Recommended Actions | • Determine if this is a known or valid access point in the system. If it is valid, place it in the known access point list.
• Contain the rogue. Prevent anyone from accessing it until the access point has been traced down using location or other features.
### ROGUE_AP_REMOVED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRogueAPRemoved.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Rogue AP or ad hoc rogue &quot;{0}&quot; is removed; it was detected as Rogue AP by AP &quot;{1}&quot; Radio type &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system is no longer detecting a rogue access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A rogue access point has powered off or moved away and therefore the system no longer detects it.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### RRM_DOT11_A_GROUPING_DONE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRrmDot11aGroupingDone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RRM 802.11a/n grouping done; the new group leader’s MAC address is &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The radio resource module is finished grouping for the A band, and a new group leader is chosen.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The older RRM group leader may have gone down.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### RRM_DOT11_B_GROUPING_DONE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRrmDot11bGroupingDone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RRM 802.11b/g/n grouping done; the new group leader’s MAC address is &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The radio resource module finished its grouping for the B band and chose a new group leader.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The older RRM group leader may have gone down.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### SENSED_TEMPERATURE_HIGH

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnSensedTemperatureTooHigh.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The sensed temperature on the Switch &quot;{0}&quot; is too high. The current sensed temperature is &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system's internal temperature has crossed the configured thresholds.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• Fan failure.</td>
</tr>
<tr>
<td></td>
<td>• Fault in the device.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>• Verify the configured thresholds and increase the value if it is too low.</td>
</tr>
<tr>
<td></td>
<td>• Call customer support.</td>
</tr>
</tbody>
</table>

### SENSED_TEMPERATURE_LOW

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnSensedTemperatureTooLow.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The sensed temperature on the Switch &quot;{0}&quot; is too low. The current sensed temperature is &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The internal temperature of the device is below the configured limit in the system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• Operating environment.</td>
</tr>
<tr>
<td></td>
<td>• Hardware fault.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>• Verify the configured thresholds and ensure that the limit is appropriate.</td>
</tr>
<tr>
<td></td>
<td>• Call customer support.</td>
</tr>
</tbody>
</table>

### STATION_ASSOCIATE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationAssociate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;{0}&quot; is associated with AP &quot;{1}&quot;, interface &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client has associated with an access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A client has associated with an access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### STATION_ASSOCIATE_FAIL

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationAssociateFail.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; failed to associate with AP &quot;[1],&quot; interface &quot;[2].&quot; The reason code is &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client station failed to associate with the system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The access point was busy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check whether the access point is busy and reporting load profile failures.</td>
</tr>
</tbody>
</table>

### STATION_AUTHENTICATE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationAssociate (bsnStationUserName is set).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; with user name &quot;[3]&quot; is authenticated with AP &quot;[1],&quot; interface &quot;[2].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client has successfully authenticated with the system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A client has successfully authenticated with the system.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### STATION_AUTHENTICATION_FAIL

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationAuthenticateFail.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; has failed authenticating with AP &quot;[1],&quot; interface &quot;[2].&quot; The reason code is &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system failed to authenticate a client.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Failed client authentication.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check client configuration and configured keys or passwords in the system.</td>
</tr>
</tbody>
</table>
STATION_BLACKLISTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationBlacklisted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; which was associated with AP &quot;[1],&quot; interface &quot;[2]&quot; is excluded. The reason code is &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client is in the exclusion list and is not allowed to authenticate for a configured interval.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
</tbody>
</table>
| Probable Causes     | • Repeated authentication or association failures from the client station.  
                      | • A client is attempting to use an IP address assigned to another device. |
| Recommended Actions | • Verify the configuration or the client along with its credentials.  
                      | • Remove the client from the exclusion list by using the management interface if the client needs to be allowed back into the network. |

STATION_DEAUTHENTICATE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationDeauthenticate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; is deauthenticated from AP &quot;[1],&quot; interface &quot;[2]&quot; with reason code &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client is no longer authenticated by the system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A client is no longer authenticated by the system.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

STATION_DISASSOCIATE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnDot11StationDisassociate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;[0]&quot; is disassociated from AP &quot;[1],&quot; interface &quot;[2]&quot; with reason code &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client has disassociated with an access point in the system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A station may disassociate due to various reasons such as inactivity timeout or a forced action from the management interface.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### STATION_WEP_KEY_DECRYPT_ERROR

**MIB Name**  
bsnWepKeyDecryptError.

**WCS Message**  
The WEP Key configured at the station may be wrong. Station MAC Address is 
"{0}," AP MAC is 
"{1}" and Slot ID is 
"{2}.

**Symptoms**  
A client station seems to have the wrong WEP key.

**WCS Severity**  
Minor.

**Probable Causes**  
A client has an incorrectly configured WEP key.

**Recommended Actions**  
Identify the client and correct the WEP key configuration.

### STATION_WPA_MIC_ERROR_COUNTER_ACTIVATED

**MIB Name**  
bsnWpaMicErrorCounterActivated.

**WCS Message**  
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.

**Symptoms**  
A client station has detected a WPA MIC error.

**WCS Severity**  
Critical.

**Probable Causes**  
A possible hacking attempt is underway.

**Recommended Actions**  
Identify the station that is the source of this threat.

### SWITCH_DETECTED_DUPLICATE_IP

**MIB Name**  
bsnDuplicateIpAddressReported.

**WCS Message**  
Switch 
"{0}" detected duplicate IP address 
"{0}" being used by machine with mac address 
"{1}.

**Symptoms**  
The system has detected a duplicate IP address in the network that is assigned to the switch (controller).

**WCS Severity**  
Critical.

**Probable Causes**  
Another device in the network is configured with the same IP address as that of the switch (controller).

**Recommended Actions**  
Correct the misconfiguration of IP addresses in the network.
### SWITCH_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>This is a WCS-only event.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;[0]&quot; is unreachable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A switch (controller) is unreachable from the management system.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• The switch (controller) has encountered hardware or software failure.</td>
</tr>
<tr>
<td></td>
<td>• There are network connectivity issues between the management station and the switch (controller).</td>
</tr>
<tr>
<td></td>
<td>• The configured SNMP community strings on the management station or the switch (controller) are incorrect.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>• Check if the switch (controller) is powered up and reachable through the web interface.</td>
</tr>
<tr>
<td></td>
<td>• Ping the switch (controller) from the management station to verify if there is IP connectivity.</td>
</tr>
<tr>
<td></td>
<td>• Check the community strings configured on the management station.</td>
</tr>
</tbody>
</table>

### SWITCH_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>This is a WCS-only event.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;[0]&quot; is reachable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A switch (controller) is now reachable from the management station.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A switch (controller) is reachable from the management station.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### TEMPERATURE_SENSOR_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTemperatureSensorClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The temperature sensor is working now on the switch &quot;[0].&quot; The sensed temperature is &quot;[1].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The temperature sensor is operational.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system is detecting the temperature sensor to be operational now.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
TEMPERATURE_SENSORFAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTemperatureSensorFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The temperature sensor failed on the Switch &quot;{0}&quot;. Temperature is unknown.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system is reporting that a temperature sensor has failed and the system is unable to report accurate temperature.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The temperature sensor has failed due to hardware failure.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Call customer support.</td>
</tr>
</tbody>
</table>

TOO_MANY_USER_UNSUCCESSFUL_LOGINS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTooManyUnsuccessLoginAttempts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>User &quot;{1}&quot; with IP Address &quot;{0}&quot; has made too many unsuccessful login attempts.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A management user has made too many login attempts.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes        | • An admin user has made too many login attempts.  
|                        | • A user attempted to break into the administration account of the management system. |
| Recommended Actions    | • Identify the source of the login attempts and take the appropriate action.  
|                        | • Increase the value of the login attempt threshold if it is too low. |

Traps Added in Release 2.1

ADHOC_ROGUE_AUTO_CONTAINED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAdhocRogueAutoContained.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Adhoc Rogue &quot;{0}&quot; was found and is auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system detected an ad hoc rogue and automatically contained it.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system detected an ad hoc rogue and automatically contained it as configured in the system’s wireless prevention policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the ad hoc rogue through the location application and take the appropriate action.</td>
</tr>
</tbody>
</table>
### ADHOC_ROGUE_AUTO_CONTAINED_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAdhocRogueAutoContained (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Adhoc Rogue &quot;[0]&quot; was found and was auto contained. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An ad hoc rogue that the system has detected earlier is now clear.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system no longer detects an ad hoc rogue.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### NETWORK_ENABLED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnNetworkStateChanged (bsnNetworkState set to enabled).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Global &quot;[1]&quot; network status enabled on Switch with IP Address &quot;[0].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An administrator has enabled the global network for 802.11a/n or 802.11b/g/n.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Administrative command.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### ROGUE_AP_AUTO_CONTAINED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRogueApAutoContained.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Rogue AP &quot;[0]&quot; is advertising our SSID and is auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has automatically contained a rogue access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system detected an ad hoc rogue and automatically contained it as configured in the system’s wireless prevention policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>• Track the location of the rogue and take the appropriate action.</td>
</tr>
<tr>
<td></td>
<td>• If this is a known valid access point, clear the rogue from containment.</td>
</tr>
</tbody>
</table>

### ROGUE_AP_AUTO_CONTAINED_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRogueApAutoContained (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Rogue AP &quot;[0]&quot; was advertising our SSID and was auto contained. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has cleared a previously contained rogue.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has cleared a previously contained rogue.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### TRUSTED_AP_INVALID_ENCRYPTION

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidEncryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;([0])&quot; is invalid encryption. It is using &quot;([1])&quot; instead of &quot;([2]).&quot; It is auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system automatically contained a trusted access point that has invalid encryption.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system automatically contained a trusted access point that violated the configured encryption policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the trusted access point and take the appropriate action.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_INVALID_ENCRYPTION_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidEncryption (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;([0])&quot; had invalid encryption. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has cleared a previous alert about a trusted access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The trusted access point has now conformed to the configured encryption policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_INVALID_RADIO_POLICY

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidRadioPolicy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;([0])&quot; has invalid radio policy. It is using &quot;([1])&quot; instead of &quot;([2]).&quot; It has been auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has contained a trusted access point with an invalid radio policy.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has contained a trusted access point connected to the wireless system for violating the configured radio policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the trusted access point and take the appropriate action.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidRadioPolicy (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;([0])&quot; had invalid radio policy. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has cleared a previous alert about a trusted access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The trusted access point has now conformed to the configured encryption policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### TRUSTED_AP_INVALID_SSID

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidSsid.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; has invalid SSID. It was auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has automatically contained a trusted access point for advertising an invalid SSID.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has automatically contained a trusted access point for violating the configured SSID policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Identify the trusted access point and take the appropriate action.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_INVALID_SSID_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidSsid (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; had invalid SSID. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has cleared a previous alert about a trusted access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The trusted access point has now conformed to the configured policy.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_MISSING

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApIsMissing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; is missing or has failed.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The wireless system no longer detects a trusted access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A trusted access point has left the network or has failed.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Track down the trusted access point and take the appropriate action.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_MISSING_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApIsMissing (bsnClearTrapVariable set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; is missing or has failed. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has found a trusted access point again.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has detected a previously missing trusted access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### Traps Added in Release 2.2

#### AP_IMPERSONATION_DETECTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPImpersonationDetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP Impersonation with MAC &quot;{0}&quot; is detected by authenticated AP &quot;{1}&quot; on &quot;{2}&quot; radio and Slot ID &quot;{3}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio of an authenticated access point has heard from another access point whose MAC address neither matches that of a rogue nor is it an authenticated neighbor of the detecting access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A severity breach related to access point impersonation may be under way.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Track down the MAC address of the impersonating access point in the network and contain it.</td>
</tr>
</tbody>
</table>

#### AP_RADIO_CARD_RX_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPRadioCardRxFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Receiver failure detected on the &quot;{0}&quot; radio of AP &quot;{1}&quot; on Switch &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio card is unable to receive data.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes           | • A radio card is experiencing reception failure.  
                          | • The antenna of the radio is disconnected.  |
| Recommended Actions       | • Check the access point’s antenna connection.  
                          | • Call customer support.  |

#### AP_RADIO_CARD_RX_FAILURE_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPRadioCardRxFailureClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Receiver failure cleared on the &quot;{0}&quot; radio of AP &quot;{1}&quot; on Switch &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio is no longer experiencing reception failure.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A malfunction in the access point has been corrected.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### AP_RADIO_CARD_TX_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPRadioCardTxFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Transmitter failure detected on the &quot;{0}&quot; radio of AP &quot;{1}&quot; on Switch &quot;{2}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio card is unable to transmit.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>- A radio card is experiencing transmission failure.</td>
</tr>
<tr>
<td></td>
<td>- The antenna of the radio may be disconnected.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>- Check the antenna of the access point.</td>
</tr>
<tr>
<td></td>
<td>- Call customer support.</td>
</tr>
</tbody>
</table>

### AP_RADIO_CARD_TX_FAILURE_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPRadioCardTxFailureClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Transmitter failure cleared on the &quot;{0}&quot; radio of AP &quot;{1}&quot; on Switch &quot;{2}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio is no longer experiencing transmission failure.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A malfunction in the access point has been corrected.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### SIGNATURE_ATTACK_CLEARED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnSignatureAttackDetected (bsnClearTrapVariable is set to True).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot; is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The switch (controller) no longer detects a signature attack.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The signature attack that the system previously detected has stopped.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### SIGNATURE_ATTACK_DETECTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnSignatureAttackDetected</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>IDS Signature attack detected on Switch &quot;{0}&quot;. The Signature Type is &quot;{1}&quot;. Signature Name is &quot;{2}&quot; and Signature description is &quot;{3}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The switch (controller) is detecting a signature attack. The switch (controller) has a list of signatures that it monitors. When it detects a signature, it provides the name of the signature attack in the alert it generates.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Someone is mounting a malevolent signature attack.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Track down the source of the signature attack in the wireless network and take the appropriate action.</td>
</tr>
</tbody>
</table>

### TRUSTED_AP_HAS_INVALID_PREAMBLE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidPreamble.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; on Switch &quot;{3}&quot; has invalid preamble. It is using &quot;{1}&quot; instead of &quot;{2}&quot;. It has been auto contained as per WPS policy.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has contained a trusted rogue access point for using an invalid preamble.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has detected a possible severity breach because a rogue is transmitting an invalid preamble.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Locate the rogue access point using location features or the access point detecting it and take the appropriate actions.</td>
</tr>
</tbody>
</table>

### TRUSTED_HAS_INVALID_PREAMBLE_CLEARED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnTrustedApHasInvalidPreamble (bsnClearTrapVariable is set to true).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Trusted AP &quot;{0}&quot; on Switch &quot;{3}&quot; had invalid preamble. The alert state is clear now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system has cleared a previous alert about a trusted access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The system has cleared a previous alert about a trusted access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
# Traps Added in Release 3.0

## AP_FUNCTIONALITY_DISABLED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPFunctionalityDisabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP functionality has been disabled for key &quot;{0},&quot; reason being &quot;{1}&quot; for feature-set &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system sends this trap out when the controller disables access point functionality because the license key has expired.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>When the controller boots up, it checks whether the feature license key matches the controller’s software image. If it does not, the controller disables access point functionality.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Configure the correct license key on the controller and reboot it to restore access point functionality.</td>
</tr>
</tbody>
</table>

## AP_IP_ADDRESS_FALLBACK

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPIPAddressFallback.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{0}&quot; with static-ip configured as &quot;{2}&quot; has fallen back to the working DHCP address &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This trap is sent out when an access point, with the configured static ip-address, fails to establish connection with the outside world and starts using DHCP as a fallback option.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>If the configured IP address on the access point is incorrect or obsolete, and if the AP Fallback option is enabled on the switch (controller), the access point starts using DHCP.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Reconfigure the access point’s static IP to the correct IP address if desired.</td>
</tr>
</tbody>
</table>
### AP_REGULATORY_DOMAIN_MISMATCH

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPRegulatoryDomainMismatch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP &quot;{1}&quot; is unable to associate. The Regulatory Domain configured on it &quot;{3}&quot; does not match the Controller &quot;{0}&quot; country code &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system generates this trap when an access point’s regulatory domain does not match the country code configured on the controller. Due to the country code mismatch, the access point will fail to associate with the controller.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes       | • If someone changes the controller’s country code configuration and some of the existing access points support a different country code, these access points fail to associate.  
                           • An access point on the controller’s network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating. |
| Recommended Actions   | Either remove the access points that are not meant for inclusion in the controller’s domain or correct the controller’s country code setting. |

### RX_MULTICAST_QUEUE_FULL

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRxMulticastQueueFull.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>CPU Receive Multicast Queue is full on Controller &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This trap indicates that the CPU’s Receive Multicast queue is full.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>An ARP storm.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
# Traps Added in Release 3.1

## AP_AUTHORIZATION_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPAuthorizationFailure</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Failed to authorize AP &quot;{0}&quot;. Authorization entry does not exist in Controllers &quot;{1}&quot; AP Authorization List.</td>
</tr>
<tr>
<td></td>
<td>• Failed to authorize AP &quot;{0}&quot;. AP’s authorization key does not match with SHA1 key in Controllers &quot;{1}&quot; AP Authorization List.</td>
</tr>
<tr>
<td></td>
<td>• Failed to authorize AP &quot;{0}&quot;. Controller &quot;{1}&quot; could not verify the Self Signed Certificate from the AP.</td>
</tr>
<tr>
<td></td>
<td>• Failed to authorize AP &quot;{0}&quot;. AP has a self signed certificate where as the Controllers &quot;{1}&quot; AP authorization list has Manufactured Installed Certificate for this AP.</td>
</tr>
</tbody>
</table>

**Symptoms**
An alert is generated when an access point fails to associate with a controller due to authorization issues.

**WCS Severity**
Critical.

**Probable Causes**
- The access point is not on the controller’s access point authorization list.
- The key entry in the controller's access point authorization list does not match the SHA1 key received from the access point.
- The access point self-signed certificate is not valid.
- The access point has a self-signed certificate and the controller's access point authorization list (for the given access point) references a manufactured installed certificate.

**Recommended Actions**
- Add the access point to the controller’s authorization list.
- Update the access point’s authorization key to match the controller’s access point key.
- Check the accuracy of the access point’s self-signed certificate.
- Check the certificate type of the access point in the controller’s access point authorization list.

## HEARTBEAT_LOSS_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>heartbeatLossTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Keepalive messages are lost between Master and Controller&quot;{0}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This trap is generated when the controller loses connection with the Supervisor Switch (in which it is physically embedded) and the controller cannot hear the heartbeat (keepalives) from the Supervisor.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>• Port on the WiSM controller could be down.</td>
</tr>
<tr>
<td></td>
<td>• Loss of connection with the Supervisor Switch.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### INVALID_RADIO_INTERFACE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>invalidRadioTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WCS Message</strong></td>
<td>Radio with MAC address “[0]” and protocol “[1]” that has joined controller “[2]” has invalid interface. The reason is “[3].”</td>
</tr>
<tr>
<td><strong>Symptoms</strong></td>
<td>If a Cisco access point joins the network but has unsupported radios, the controller detects this and generates a trap. This symptom propagates an alert in WCS.</td>
</tr>
<tr>
<td><strong>WCS Severity</strong></td>
<td>Critical.</td>
</tr>
<tr>
<td><strong>Probable Causes</strong></td>
<td>The radio hardware is not supported by the controller.</td>
</tr>
<tr>
<td><strong>Recommended Actions</strong></td>
<td>None.</td>
</tr>
</tbody>
</table>

### RADAR_CLEARED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRadarChannelCleared</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WCS Message</strong></td>
<td>Radar has been cleared on channel ”[1]” which was detected by AP base radio MAC ”[0]” on radio 802.11a/n.</td>
</tr>
<tr>
<td><strong>Symptoms</strong></td>
<td>Trap is generated after the expiry of a non-occupancy period for a channel that previously generated a radar trap.</td>
</tr>
<tr>
<td><strong>WCS Severity</strong></td>
<td>Informational.</td>
</tr>
<tr>
<td><strong>Probable Causes</strong></td>
<td>Trap is cleared on a channel.</td>
</tr>
<tr>
<td><strong>Recommended Actions</strong></td>
<td>None.</td>
</tr>
</tbody>
</table>

### RADAR_detected

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRadarChannelDetected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WCS Message</strong></td>
<td>Radar has been detected on channel ”[1]” by AP base radio MAC ”[0]” on radio 802.11a/n.</td>
</tr>
<tr>
<td><strong>Symptoms</strong></td>
<td>This trap is generated when radar is detected on the channel on which an access point is currently operating.</td>
</tr>
<tr>
<td><strong>WCS Severity</strong></td>
<td>Informational.</td>
</tr>
<tr>
<td><strong>Probable Causes</strong></td>
<td>Radar is detected on a channel.</td>
</tr>
<tr>
<td><strong>Recommended Actions</strong></td>
<td>None.</td>
</tr>
</tbody>
</table>
### RADIO_CORE_DUMP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>radioCoreDumpTrap</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Radio with MAC address “{0}” and protocol “{1}” has core dump on controller “{2}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When a Cisco radio fails and a core dump occurs, the controller generates a trap and WCS generates an event for this trap.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Radio failure.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Capture the core dump file using the controller’s command line interface and send to TAC support.</td>
</tr>
</tbody>
</table>

### RADIO_INTERFACE_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPIfDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Radio with MAC address “{0}” and protocol “{1}” is down. The reason is “{2}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When a radio interface is down, WCS generates an alert. Reason for the radio outage is also noted.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical if not manually disabled. Informational if radio interface was manually disabled.</td>
</tr>
</tbody>
</table>
| Probable Causes | • The radio interface has failed.  
                • The access point cannot draw enough power.  
                • The maximum number of transmissions for the access point is reached.  
                • The access point has lost connection with the controller heart beat.  
                • The admin status of the access point admin is disabled.  
                • The admin status of the radio is disabled. |
| Recommended Actions | None. |

### RADIO_INTERFACE_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPIfUp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Radio with MAC address “{0}” and protocol “{1}” is up. The reason is “{2}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When a radio interface is operational again, WCS clears the previous alert. Reason for the radio being up again is also noted.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>
| Probable Causes | • Admin status of access point is enabled.  
                • Admin status of radio is enabled.  
                • Global network admin status is enabled. |
| Recommended Actions | None. |
### UNSUPPORTED_AP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>unsupportedAPTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP “{0}” tried to join controller “{1}” and failed. The controller does not support this kind of AP.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When unsupported access points try to join 40xx/410x controllers or 3500 controller with 64 MB flash, these controllers generate a trap, and the trap is propagated as an event in WCS.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Access point is not supported by the controller.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### Traps Added in Release 3.2

### LOCATION_NOTIFY_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>locationNotifyTrap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Depending on the notification condition reported, the trap is sent out in an XML format and is reflected in WCS with the following alert messages:</td>
</tr>
<tr>
<td></td>
<td>• Absence of &lt;Element&gt; with MAC &lt;macAddress&gt;, last seen at &lt;timestamp&gt;.</td>
</tr>
<tr>
<td></td>
<td>• &lt;Element&gt; with MAC &lt;macAddress&gt; is &lt;In</td>
</tr>
<tr>
<td></td>
<td>• &lt;Element&gt; with MAC &lt;macAddress&gt; has moved beyond &lt;specifiedDistance&gt; ft. of marker &lt;MarkerName&gt;, located at a range of &lt;foundDistance&gt; ft.</td>
</tr>
<tr>
<td></td>
<td>For detailed info on the XML format for the trap content, consult the 2700 Location Appliance Configuration Guide.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A 2700 location appliance sends this trap out when the defined location notification conditions are met (such as element outside area, elements missing, and elements exceeded specified distance). WCS uses this trap to display alarms about location notification conditions.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor (under the Location Notification dashboard).</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The location notification conditions configured for a 2700 location appliance are met for certain elements on the network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### Traps Added In Release 4.0

#### CISCO_LWAPP_MESH_POOR_SNR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshPoorSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Poor SNR.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>SNR (signal-to-noise) ratio is important because high signal strength is not enough to ensure good receiver performance. The incoming signal must be stronger than any noise or interference that is present. For example, you can have high signal strength and still have poor wireless performance if there is strong interference or a high noise level.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The link SNR fell below 12 db. The threshold level cannot be changed. If poor SNR is detected on the backhaul link for a child or parent, the trap is generated and contains SNR values and MAC addresses.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

#### CISCO_LWAPP_MESH_PARENT_CHANGE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshParentChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Parent changed.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When the parent is lost, the child joins with another parent, and the child sends traps containing both old and new parent’s MAC addresses.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The child moved to another parent.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

#### CISCO_LWAPP_MESH_CHILD_MOVED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshChildMoved</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Child moved.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When the parent access point detects a child being lost and communication is halted, the child lost trap is sent to WCS, along with the child MAC address.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The child moved from the parent.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## CISCO_LWAPP_MESH_CONSOLE_LOGIN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshConsoleLogin</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Console login successful or failed.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The console port provides the ability for the customer to change the user name and password to recover the stranded outdoor access point. To prevent any unauthorized user access to the access point, WCS sends an alarm when someone tries to log in. This alarm is required to provide protection because the access point is physically vulnerable being located outdoors.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>A login is of critical severity.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>You have successfully logged in to the access point console port or failed on three consecutive tries.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshAuthorizationFailure</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Fails to authenticate with controller.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>WCS receives a trap from the controller. The trap contains the MAC addresses of those access points that failed authorization.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The access point tried to join the MESH but failed to authenticate because the MESH node MAC address was not on the MAC filter list.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
**CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshChildExcludedParent</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Parent AP being excluded by child AP.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When a child fails authentication at the controller after a fixed number of attempts, the child can exclude that parent. The child remembers the excluded parent so that when it joins the network, it sends the trap which contains the excluded parent MAC address and the duration of the exclusion period.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A child marked a parent for exclusion.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappMeshExcessiveParentChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Parent changed frequently.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When MAP parent-change-counter exceeds the threshold within a given duration, it sends a trap to WCS. The trap contains the number of times the MAP changes and the duration of the time. The threshold is user configurable.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The MESH access point changed its parent frequently.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**IDS_SHUN_CLIENT_TRAP**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-IDS-MIB. CLIdsNewShunClient.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The Cisco Intrusion Detection System &quot;{0}&quot; has detected a possible intrusion attack by the wireless client &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This trap is generated in response to a shun client clear alert originated from a Cisco IDS/IPs appliance &quot;{0}&quot; installed in the data path between the wireless client &quot;{1}&quot; and the site’s intranet.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The designated client is generating a packet-traffic pattern which shares properties with a well-known form of attack on the customer’s network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Investigate the designated client and determine if it is an intruder, a virus, or a false alarm.</td>
</tr>
</tbody>
</table>
### IDS_SHUN_CLIENT_CLEAR_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-IDS-MIB. cLIdsNewShunClientClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The Cisco Intrusion Detection System &quot;[0]&quot; has cleared the wireless client &quot;[1]&quot; from possibly having generated an intrusion attack.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This trap is generated in response to one of two things: 1) a shun client clear alert originated from a Cisco IDS/IPS appliance (&quot;[0]&quot;) installed in the data path between the wireless client (&quot;[1]&quot;) and the site's intranet, or 2) a scheduled timeout of the original IDS_SHUN_CLIENT_TRAP for the wireless client.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The designated client is no longer generating a suspicious packet-traffic pattern.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MFP_TIMEBASE_STATUS_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MFP-MIB. ciscoLwappMfpTimebaseStatus.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;[0]&quot; is &quot;[1]&quot; with the Central time server.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent to indicate when the synchronization of the controller's time base with the Central time base last occurred.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical (not in sync trap) and clear (sync trap).</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The controller's time base is not in sync with the Central time base.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### MFP_ANOMALY_DETECTED_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MFP-MIB. ciscoLwappMfpAnomalyDetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MFP configuration of the WLAN was violated by the radio interface &quot;{0}&quot; and detected by the radio interface &quot;{1}&quot; of the access point with MAC address &quot;{2}&quot;. The violation is &quot;{3}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the MFP configuration of the WLAN was violated by the radio interface cLApIfSmtDot11Bssid and detected by the radio interface cLApDot11IfSlotId of the access point cLApSysMacAddress. This violation is indicated by cLMfpEventType. When observing the management frame(s) given by cLMfpEventFrames for the last cLMfpEventPeriod time units, the controller reports the occurrence of a total of cLMfpEventTotal violation events of type cLMfpEventType. When the cLMfpEventTotal is 0, no further anomalies have recently been detected, and the NMS should clear any alarm raised about the MFP errors.</td>
</tr>
<tr>
<td>Note</td>
<td>This notification is generated by the controller only if MFP was configured as the protection mechanism through cLMfpProtectType.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The MFP configuration of the WLAN was violated. Various types of violations are invalidMic, invalidSeq, noMic, and unexpectedMic.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### GUEST_USER_REMOVED_TRAP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserRemoved.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Guest user &quot;{1}&quot; deleted on controller &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated when the lifetime of the guest user {1} expires and the guest user’s accounts are removed from the controller &quot;{0}&quot;.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>GuestUserAccountLifetime expired.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
Traps Added or Updated in Release 4.0.96.0

**AP_IMPERSONATION_DETECTED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPImpersonationDetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP Impersonation with MAC &quot;{0}&quot; using source MAC &quot;{1}&quot; is detected by authenticated AP &quot;{2}&quot; on &quot;{3}&quot; radio and slot ID &quot;{4}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio of an authenticated access point had communication with another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A security breach related to access point impersonation may be occurring.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Track down the MAC address of the impersonating access point and contain it.</td>
</tr>
</tbody>
</table>

**RADIUS_SERVER_DEACTIVATED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappAAARadiusServerGlobalDeactivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;{0}&quot; (port {1}) is deactivated.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server is deactivated in the global list.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server is deactivated in the global list.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**RADIUS_SERVER_ACTIVATED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappAAARadiusServerGlobalDeactivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;{0}&quot; (port {1}) is activated.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server is deactivated in the global list.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server is deactivated in the global list.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### RADIUS_SERVER_WLAN_DEACTIVATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;{0}&quot; (port {1}) is deactivated on WLAN &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server is deactivated on the WLAN.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server is deactivated on the WLAN.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### RADIUS_SERVER_WLAN_ACTIVATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanActivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;{0}&quot; (port {1}) is activated on WLAN &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server is activated on the WLAN.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server is activated on the WLAN.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### RADIUS_SERVER_TIMEOUT

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;{0}&quot; (port {1}) failed to respond to request from client &quot;{2}&quot; with MAC &quot;{3}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server failed to respond to a request from a client or user.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server fails to process the request from the client or user.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### DECRYPT_ERROR_FOR_WRONG_WPA_WPA2

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-DOT11-CLIENT-MIB. CiscoLwappDot11ClientKeyDecryptError.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Decrypt error occurred at AP with MAC &quot;{0}&quot; running TKIP with wrong WPA/WPA2 by client with MAC &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that a user is trying to connect with an invalid security policy for WPA/WPA2 types.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The user failed to authenticate and join the controller.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
Traps Added or Updated in Release 4.1

### AP_IMPERSONATION_DETECTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnAPImpersonationDetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>AP impersonation of MAC &quot;{0}&quot; using source MAC &quot;{1}&quot; is detected by an authenticated AP &quot;{2}&quot; on &quot;{3}&quot; radio and slot ID &quot;{4}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A radio of an authenticated access point received signals from another access point whose MAC address neither matches that of a rogue nor is an authenticated neighbor of the detecting access point.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A security breach related to access point impersonation has occurred.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Track down the MAC address of the impersonating access point and contain it.</td>
</tr>
</tbody>
</table>

### INTERFERENCE_DETECTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>COGNIO-TRAPS-MIB.cognioInterferenceDetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Interference detected by type {0} with power {1}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A Cognio spectrum agent detected interference over its configured thresholds.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Excessive wireless interference or noise.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### INTERFERENCE_CLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>COGNIO-TRAPS-MIB.cognioInterferenceClear</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Interference cleared.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The Cognio spectrum expert agent no longer detects an interference source over its configured threshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Previous excessive wireless interference or noise is gone.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
# ONE_ANCHOR_ON_WLAN_UP

**MIB Name**  
CISCO-LWAPP-MOBILITY-MIB.  
ciscoLwappMobilityOneAnchorOnWlanUp.

**WCS Message**  
Controller "{0}". An anchor of WLAN "{1}" is up.

**Symptoms**  
Successive EoIP and UDP ping to at least one anchor on the WLAN is up.

**WCS Severity**  
Clear.

**Probable Causes**  
At least one anchor is reachable from an EoIP/UDP ping.

**Recommended Actions**  
None.

# RADIUS_SERVER_DEACTIVATED

**MIB Name**  
CISCO-LWAPP-AAA-MIB.  
ciscoLwappAAARadiusServerGlobalDeactivated.

**WCS Message**  
RADIUS server "{0}" (port {1}) is deactivated.

**Symptoms**  
The controller detects that the RADIUS server is deactivated in the global list.

**WCS Severity**  
Major.

**Probable Causes**  
RADIUS server is deactivated in the global list.

**Recommended Actions**  
None.

# RADIUS_SERVER_ACTIVATED

**MIB Name**  
CISCO-LWAPP-AAA-MIB.  
ciscoLwappAAARadiusServerGlobalActivated.

**WCS Message**  
RADIUS server "{0}" (port {1}) is activated.

**Symptoms**  
The controller detects that the RADIUS server is activated in the global list.

**WCS Severity**  
Clear.

**Probable Causes**  
RADIUS server is activated in the global list.

**Recommended Actions**  
None.
### RADIUS_SERVER_WLAN_ACTIVATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalWlanActivated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;[0]&quot; (port [1]) is activated on WLAN &quot;[2].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server is activated on the WLAN.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>RADIUS server is activated on the WLAN.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### RADIUS_SERVER_TIMEOUT

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>RADIUS server &quot;[0]&quot; (port [1]) failed to respond to request from client &quot;[2]&quot; with MAC &quot;[3].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The controller detects that the RADIUS server failed to respond to a request from the client or user.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The RADIUS server fails to process the request from a client or user.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MOBILITY_ANCHOR_CTRL_PATH_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlPathDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;[0].&quot; Control path on anchor &quot;[1]&quot; is down.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>When successive ICMP ping attempts to the anchor fails, the anchor is conclusively down.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Anchor not reachable by ICMP ping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MOBILITY_ANCHOR_CTRL_PATH_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlUp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;[0].&quot; Control path on anchor &quot;[1]&quot; is up.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The ICMP ping to the anchor is restored, and the anchor is conclusively up.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The anchor is reachable by an ICMP ping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## MOBILITY_ANCHOR_DATA_PATH_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;{0}&quot;. Data path on anchor &quot;{1}&quot; is down.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Successive EoIP ping attempts to the anchor fails, and the anchor is conclusively down.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The anchor is not reachable by an EoIP ping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## MOBILITY_ANCHOR_DATA_PATH_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPathUp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;{0}&quot;. Data path on anchor &quot;{1}&quot; is up.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The EoIP ping to the anchor is restored, and the anchor is conclusively up.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Anchor is reachable by the EoIP ping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## WLAN_ALL_ANCHORS_TRAP_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAllAnchorsOnWlanDown.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller &quot;{0}&quot;. All anchors of WLAN &quot;{1}&quot; are down.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Successive EoIP ping attempts to all the anchors on WLAN is occurring.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Anchors are not reachable by the EoIP ping.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### MESH_AUTHORIZATIONFAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshAuthorizationFailure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; fails to authenticate with controller because &quot;{1}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A mesh access point failed to join the mesh network because its MAC address is not listed in the MAC filter list. The alarm includes the MAC address of the mesh access point that failed to join.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The mesh node MAC address is not in the MAC filter list, or a security failure from the authorization server occurred.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MESH_CHILDEXCLUDEDPARENT

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildExcludedParent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address &quot;{0},&quot; previous parent MAC address &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the controller after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the controller when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The child access point failed to authenticate to the controller after a fixed number of times.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MESH_PARENTCHANGE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentChange.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; changed its parent. AP current parent MAC address &quot;{1},&quot; previous parent MAC address &quot;{2}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The child access point has changed its parent.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
### MESH_CHILDMOVED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildMoved.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Parent AP lost connection to this AP. AP neighbor type is &quot;{0}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the parent access point loses connection with its child.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The parent access point lost connection with its child.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MESH_EXCESSIVEPARENTCHANGE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveParentChange.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; changes parent frequently.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent if the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the controller.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The child access point has frequently changed its parent.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### MESH_POORSNR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNR.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; has SNR on backhaul link as &quot;{1}&quot; which is lower then predefined threshold.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the child access point detects a signal-to-noise ratio below 12dB the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>SNR is lower then the threshold defined by c1MeshSNRThreshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## MESH_POORSNRCLEAR

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNRClear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; has SNR on backhaul link as &quot;{1}&quot; which is normal now.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent to clear ciscoLwappMeshPoorSNR when the child access point detects SNR on the backhaul link that is higher than the threshold defined by c1MeshSNRThreshold.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>SNR on the backhaul link is higher than the threshold defined by c1MeshSNRThreshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## MESH_CONSOLELOGIN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-MESH-MIB. ciscoLwappMeshConsoleLogin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>MESH &quot;{0}&quot; has console logged in with status &quot;{1}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when login on the MAP console is successful or when a failure occurred after three attempts.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Login on the MAP console was successful, or a failure occurred after three attempts.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## LRADIF_REGULATORY_DOMAIN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappApIfRegulatoryDomainMismatchNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Access Point &quot;{0}&quot; is unable to associate. The Regulatory Domain &quot;{1}&quot; configured on interface &quot;{2}&quot; does not match the controller &quot;{3}&quot; regulatory domain &quot;{4}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The system generates this trap when the regulatory domain configured on the access point radios does not match the country code configured on the controller.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>If the controller's country code configuration is changed, and some access points support a different country code, then these access points fail to associate. An access point on the controller's network sends join requests to the controller, but the regulatory domain is outside the domain in which the controller is operating.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Either remove the access points that are not meant for inclusion in the controller's domain or correct the controller's country code setting.</td>
</tr>
</tbody>
</table>
### LRAD_CRASH

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappApCrash</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Access Point &quot;[0]&quot; crashed and has a core dump on controller &quot;[1].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point has crashed.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Access point failure.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Capture the core dump file using the controller’s CLI and send it to TAC support.</td>
</tr>
</tbody>
</table>

### LRAD_UNSUPPORTED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappApUnsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Access Point &quot;[0]&quot; tried to join controller &quot;[1]&quot; and failed. Associate failure reason &quot;[2].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point tried to associate to a controller to which it is not supported.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The access point is not supported by the controller.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### Traps Added or Updated in Release 4.2

#### GUEST_USER_ADDED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserAdded</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Guest user &quot;[0]&quot; created on the controller &quot;[1].&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the GuestUser account is created successfully.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The guest user account was created on the agent by either CLI, Web UI, or WCS.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## GUEST_USER_AUTHENTICATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLogged</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Guest user &quot;{0}&quot; logged into controller &quot;{1}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when the GuestUser logged into the network through webauth successfully.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The guest user was successful with webauth authentication.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## IOSAP_LINK_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>linkUp</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Autonomous AP &quot;{0},&quot; Interface &quot;{1}&quot; is {2} up.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The physical link is up on an autonomous access point radio port.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A physical link has been restored to the autonomous access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## IOSAP_LINK_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>linkDown</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Autonomous AP &quot;{0},&quot; Interface &quot;{1}&quot; is {2} down.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The physical link is down on an autonomous access point radio port.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The radio port of an autonomous access point was disabled manually or a port failure occurred.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check the administrative status of the port. If the port administrative status is not down, check other port settings.</td>
</tr>
</tbody>
</table>
## Alarm and Event Dictionary

### IOSAP_UP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>The autonomous AP “{0}” is reachable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The autonomous AP is SNMP reachable.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The autonomous access point starts to respond to SNMP queries.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### IOSAP_DOWN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Autonomous AP “{0}” is unreachable.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The autonomous AP is SNMP unreachable.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
| Probable Causes | - Network connectivity to the autonomous access point is broken.  
- Ethernet port of the autonomous access point is down.  
- SNMP agent is not running in the autonomous access point.  
- SNMP credentials on the WCS do not match the SNMP credentials configured on the autonomous access point.  
- SNMP version on the WCS does not match the SNMP version configured on the autonomous access point. |
| Recommended Actions | First, check the IP connectivity to the access point. Next, check the port status of the access point. Finally, check SNMP credentials on both the WCS and the access point. |

### WCS_EMAIL_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>WCS with IP Address “{0}” failed to send e-mail.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when it fails to send e-mails.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The SNMP server is either not configured or not reachable from WCS.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check Administration &gt; Settings &gt; Mail Server settings. Send a test e-mail from the mail server settings to see if it is successful.</td>
</tr>
</tbody>
</table>
## AUDIT_STATUS_DIFFERENCE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Switch &quot;{0}&quot; Audit done at &quot;{1}&quot;. Config differences found between WCS and controller.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when audit differences are detected while auditing a controller during a network audit background task or per controller audit.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The WCS and controller configuration are not synchronized.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Refresh the configuration from the controller so that it synchronizes with the controller configuration on WCS.</td>
</tr>
</tbody>
</table>

## LRAD_POE_STATUS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappApPower</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Access point &quot;{0}&quot; draws low power from Ethernet. Failure reason: &quot;{1}&quot;</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated when the access point draws low power from the Ethernet connection.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The access point receives low power from the Ethernet connection.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check the power status of the access point and the device connected to the access point.</td>
</tr>
</tbody>
</table>

## ROGUE_AP_NOT_ON_NETWORK

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>bsnRogueAPDetectedOnWiredNetwork (bsnRogueAPOnWiredNetwork is set to false).</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Rogue AP or ad hoc rogue &quot;{0}&quot; is not able to connect to the wired network.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A rogue access point is no longer on the wired network.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The rogue access point is no longer reachable on the wired network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
## Traps Added or Updated in Release 5.0

### GUEST_USER_LOGOFF

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-WEBAUTH-MIB, cLWAGuestUserLoggedOut</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Guest user “{1}” logged out from the controller “{0}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when a GuestUser who was previously logged into the network logs out.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The GuestUser logs off from the network.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### WCS_NOTIFICATION_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>WCS with IP Address “{0}” failed to send notification.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when a notification sent to a northbound receiver fails. Currently only guest user related notifications (such as creation, deletion, log in, and log off) can be sent to a northbound receiver.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The notification receiver is either not configured or not reachable from WCS.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check Administration &gt; Settings &gt; Notification Receiver settings. Make sure the server IP is correct, and the server is reachable from WCS.</td>
</tr>
</tbody>
</table>

### WCS_LOW_DISK_SPACE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>WCS “{0}” does not meet the minimum hardware requirements for disk space. Available: “{3}.” Minimum requirement: “{4}” Mb.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when the free disk space where WCS is installed does not meet minimum hardware requirements. This event is of major severity if minimum requirements are not met. This event is of critical severity when the available disk space is less than half of the minimum requirement.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major/Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The disk is out of free space.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Free up disk space.</td>
</tr>
</tbody>
</table>
## WCS_OK_DISK_SPACE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>WCS &quot;{0}&quot; meets the minimum hardware requirements for disk space. Available: &quot;{3}&quot;. Minimum requirement: &quot;{4}&quot; Mb.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when the free disk space where WCS is installed has met the minimum hardware requirements.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A low disk space condition has been cleared.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## WCS_LOW_DISK_SPACE_BACKUP

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>WCS &quot;{0}&quot; does not have sufficient disk space in directory &quot;{1}&quot; for backup. Space needed: &quot;{2}&quot;, space free: &quot;{3}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when a previously created WCS_LOW_DISK_SPACE_BACKUP event is cleared or when the disk contains enough space for a backup.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Clear.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A low disk space condition has been cleared.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>

## STATION_ASSOCIATE_DIAG_WLAN

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-DOT11-CCX-CLIENT-MIB.cldccDiagClientAssociatedToDiagWlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client &quot;{0}&quot; is associated to diagnostic WLAN with reason &quot;{1}&quot;.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is sent by the agent when a v5 client associates to a diagnostic channel.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>When a CCXv5 client gets associated to the diagnostic channel WLAN on WLC, this trap is raised.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>If you wish to automatically perform client troubleshooting, you must enable Client Troubleshooting in Administration &gt; Settings &gt; client. After it is enabled, the series of V5 tests are carried out on the client upon trap arrival, and the client is updated with the test status via pop-up messages. The report is placed in the logs directory. The log filename is shown in the Client Details page in the Automated Troubleshooting Report section. You can export all automated troubleshooting logs.</td>
</tr>
</tbody>
</table>
# WLAN_SHUT_FAILED

**MIB Name** | None.
---|---
**WCS Message** | Wlan “{0}” shutdown failed on controller “{1}.”
**Symptoms** | This notification is generated by WCS during scheduled operations for a given WLAN Config object. It notifies the user that the WLAN status did not change at the scheduled time.
**WCS Severity** | Major.
**Probable Causes** | The controller for the selected WLAN is not reachable, or the WLAN object does not exist.
**Recommended Actions** | Check the WCS logs at the time of event generation and verify if the WLAN exists on the controller.

# WLAN_SHUT_SUCCESS

**MIB Name** | None.
---|---
**WCS Message** | Wlan “{0}” successfully shutdown on controller “{1}.”
**Symptoms** | This notification is generated by WCS during scheduled operation for each given WLAN configuration object. It notifies the user that the admin status has been successfully completed.
**WCS Severity** | Info.
**Probable Causes** | Verify the admin status for the displayed WLAN on the controller.
**Recommended Actions** | Remove the event from the event list page.
## RADIO_SHUT_FAILED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Radio shutdown failed for AP “{0}” connected to controller “{1}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS during a scheduled operation for a given list of access point radios. It notifies the user that the status for certain radios has failed to change.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Major.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The controllers for the selected access point are not reachable, or the radio configurations are changed on the controller.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Check the WCS logs at the time of event generation and verify that the access point is associated with the controller.</td>
</tr>
</tbody>
</table>

## RADIO_SHUT_SUCCESS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Radio successfully shutdown for AP “{0}” connected to controller “{1}.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS during scheduled operation for a given list of access point radios. It notifies the user that the admin status has been successfully changed.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Info.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>None.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Verify the status of the specified radio on the controller.</td>
</tr>
</tbody>
</table>
## Traps Added or Updated in Release 5.1

### CONFIGAUDITSET_ENFORCEMENT_SUCCESS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Successfully enforced Config Group “0” on controllers “1.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS during network audit when all the templates from the config group (which are opted to be enforced) are successfully enforced.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The config group (which are opted to be enforced) templates are not in sync with the device values.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Look at the controller audit report for the list of enforced values. An alarm is cleared when no enforcements are found during the next network audit cycle.</td>
</tr>
</tbody>
</table>

### CONFIGAUDITSET_ENFORCEMENT_FAIL

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Failed to enforce Config Group “0” on controllers “1.”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS during network audit when some failures are encountered during enforcement of the templates from the config groups (which as opted to be enforced).</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The config group (which are opted to be enforced) templates are not in sync with the device values.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Look at the controller audit report for the list of enforced values and for the failed enforcements. An alarm is cleared upon successful enforcements during the next network audit cycle.</td>
</tr>
</tbody>
</table>

## Traps Added or Updated in Release 6.0

### STATION_AUTHENTICATED

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappDot11ClientMovedToRunState</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client “(0)” is authenticated with interface “(2)” of AP “(1).”</td>
</tr>
<tr>
<td>Symptoms</td>
<td>A client has completed a security policy and has moved to Run state. It can start to send or receive data.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A client has completed security policy and moved to Run state.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>None.</td>
</tr>
</tbody>
</table>
**WCS_CLIENT_TRAP_DISABLED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Client traps are disabled on controller(s) {0}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>This notification is generated by WCS when required client traps are disabled in one or more controllers. These traps are needed for WCS to detect client sessions in a timely and efficient manner. The required traps are:</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Association</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Disassociation</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Authentication</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Deauthentication</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Failed Association</td>
</tr>
<tr>
<td></td>
<td>• 802.11 Failed Authentication</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>When a controller is added to WCS, WCS enables the required client traps. If WCS does not have the correct SNMP read-write community, it could fail. The trap controls can also be changed by pushing the SNMP trap control template or using controller GUI/CLI.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Use the WCS template to enable the required client traps on the controller list.</td>
</tr>
</tbody>
</table>

**WLC_LICENSE_NOT_ENFORCED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>clmgmtLicenseNotEnforced</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller {0} has AP with unlicensed feature {1} version {2} attempting to join.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>An access point with a licensed feature is trying to join a controller without the proper license.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>An access point with a WPLUS feature like indoor mesh or OfficeExtend AP is trying to join a controller without a WPLUS license.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>You must add a WPLUS license to the controller or fix the primary, secondary, or tertiary controller configuration to have controllers with WPLUS licenses.</td>
</tr>
</tbody>
</table>

**WLC_LICENSE_COUNT_EXCEEDED**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>clmgmtLicenseUsageCountExceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Controller {0} with license {1} version {2} and counted feature {4} with limit {3} has been exceeded {5}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The access point cannot join a controller.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
</tbody>
</table>
### Alarm and Event Dictionary

<table>
<thead>
<tr>
<th>Probable Causes</th>
<th>The controller has reached the maximum licensed access point capacity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Actions</td>
<td>Add a license capacity to the controller or move the access point to a controller with more capacity.</td>
</tr>
</tbody>
</table>

#### VOIP_CALL_FAILURE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>ciscoLwappVoipCallfailureNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>VoIP Call failure of {4} (Error Code {3}) occurred on Client {0} with phone number {5} calling {6} which was associated with AP {1} on interface {2}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>VoIP snooping is enabled on a WLAN.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Informational.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>A SIP error is detected by an access point.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>The actions depend on the type of error that is being reported. Errors can range from “dialed number does not exist,” “busy,” “service unavailable,” to “service timeout.”</td>
</tr>
</tbody>
</table>

#### MSE_EVAL_LICENSE

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Evaluation license for {0} is expired.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>The tracking for clients or tags stops, or service does not start.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>The evaluation period for the service has expired.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Add a permanent license for the service using License Center or the appropriate third-party vendor application.</td>
</tr>
</tbody>
</table>

#### MSE_LICENSING_ELEMENT_LIMIT

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>{0} limit for {1} is reached or exceeded.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Elements are not tracked beyond a certain limit.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Limit for the specified service has been reached.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Add a license with higher licensed capacity to the particular service.</td>
</tr>
</tbody>
</table>

### Traps Added or Updated in Release 7.0

- SI_AQ_TRAPS
- SI_SECURITY_TRAPS
- SI_SENSOR_CRASH_TRAPS
### SI_AQ_TRAPS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-SI-MIB.my</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Air Quality Index on Channel {0} is {1} (Threshold: {2}).</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Too Many interferers (Wi-Fi / non-Wi-Fi).</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Minor.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Air Quality Index has gone below the threshold.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Reduce interference.</td>
</tr>
</tbody>
</table>

### SI_SECURITY_TRAPS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-SI-MIB.my</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>Security-Risk Interferer {0} is detected by {3}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>Interferers detected which are defined as threat to the network.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>Interference detected by SI chip.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Reduce interference.</td>
</tr>
</tbody>
</table>

### SI_SENSOR_CRASH_TRAPS

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>CISCO-LWAPP-SI-MIB.my</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCS Message</td>
<td>CleanAir Sensor Status: {0} Error Code: {1}.</td>
</tr>
<tr>
<td>Symptoms</td>
<td>CleanAir Sensor Software stopped working.</td>
</tr>
<tr>
<td>WCS Severity</td>
<td>Critical.</td>
</tr>
<tr>
<td>Probable Causes</td>
<td>CleanAir sensor is not operational due to crash.</td>
</tr>
<tr>
<td>Recommended Actions</td>
<td>Reset AP to resolve the problem.</td>
</tr>
</tbody>
</table>

### Unsupported Traps

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- POWER_SUPPLY_STATUS_CHANGE: powerSupplyStatusChangeTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_AUTH_FAILURE: bsnIpsecEspAuthFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap
- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- IPSEC_SUITE_NEG_FAILURE: bsnIpsecSuiteNegFailure
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED: bsnDot11EssDeleted
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- WARM_START: warmStart
- LINK_FAILURE: linkFailureTrap