CHAPTER 13

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:

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 email notifications if configured as such.

An alarm is a 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 SNMP, client related traps, etc.).

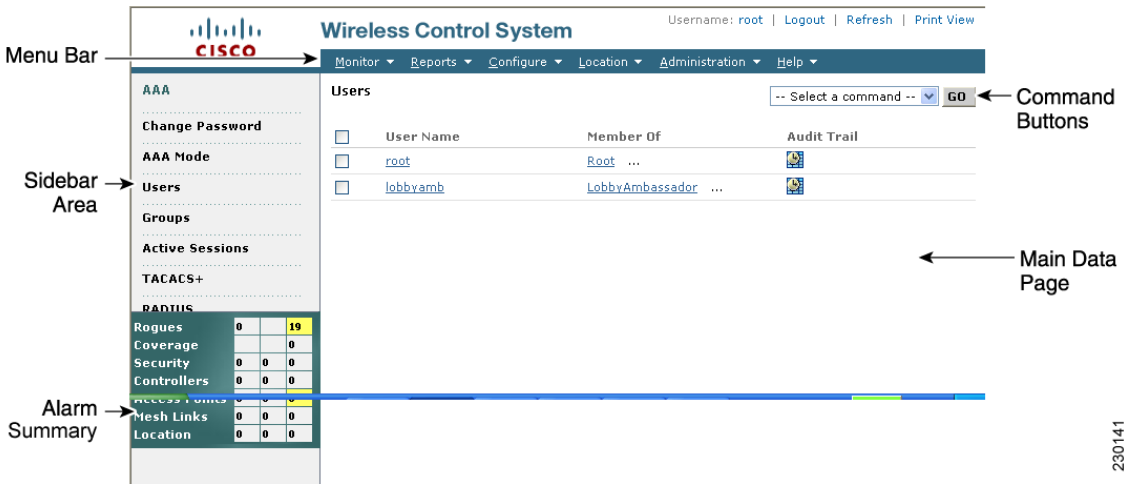
Alarm Dashboard

The number of active alarms for controllers, access points, location, and rogue elements as well as alarms associated with entities such as coverage, mesh, and security are actively displayed on the left-side of most WCS windows (see Figure 13-1).

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

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

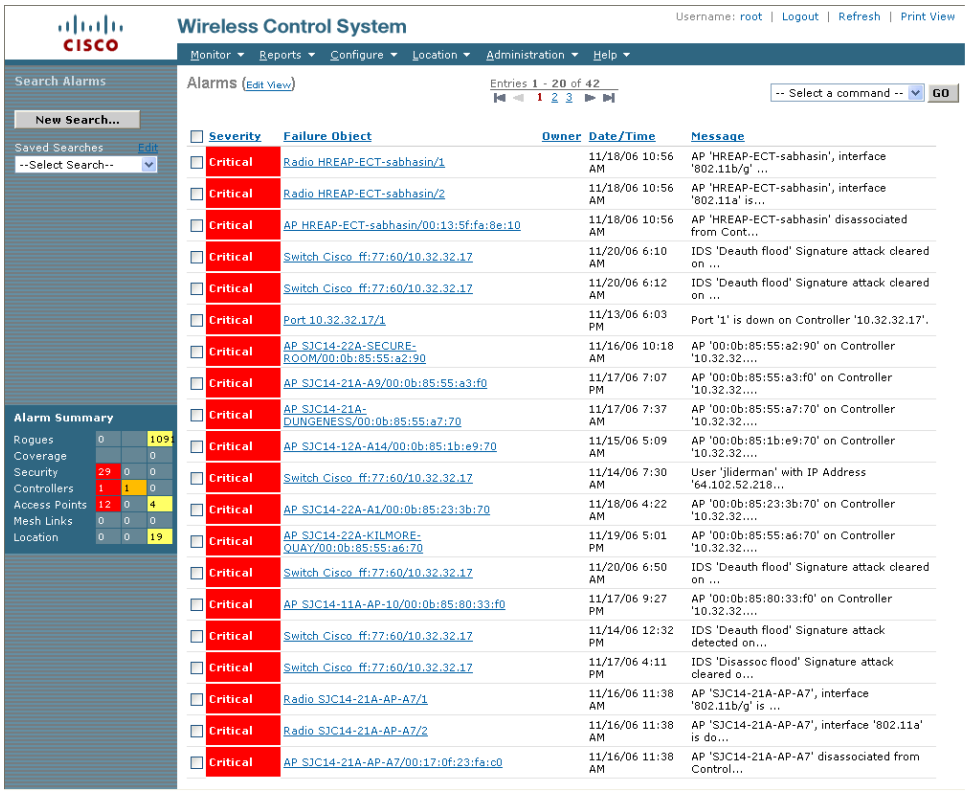
Figure 13-1 Alarm Summary Block



To view a listing of a specific type of alarm (critical, major, or minor) for a specific product or entity (such as coverage), click on the appropriate box within the alarm dashboard and a window displaying details for that alarm type and severity appears (see Figure 13-2).

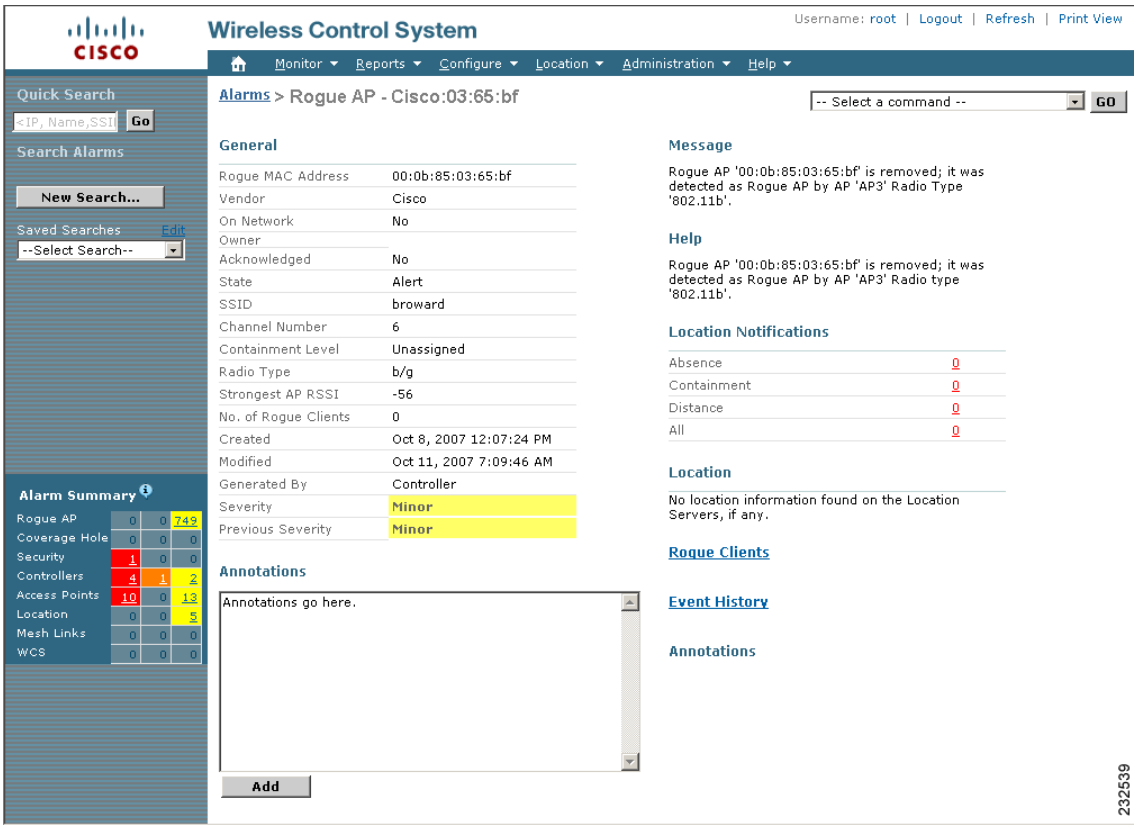
Note To search for additional alarms, click **New Search...** on the left panel of the page. For more details on conducting a search, refer to the "Setting Search Filters for Alarms" section on page 13-5.

Figure 13-2 Alarm Summary Page for WCS



Note You can click a box in the alarm dashboard to display alarm events for the entity and alarm type selected. For example, if you click on the minor alarms box for location, the Alarms page for that specific item appears (see Figure 13-2). For more details on a specific alarm listed on the Alarms page, click on the **Failure Object** link (see Figure 13-3).

Figure 13-3 Details for a Specific Failure Object (Alarm)



Note You can use the drop-down menu at the upper-right of the Alarms page to assign, unassign, delete, acknowledge, or clear the alarm. The event history of the alarm is also accessible from this menu.

Alarm Acknowledgement

You may want certain alarms to be removed 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 window or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, click the checkbox, 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 window 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 window or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged.

By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Adminstration > Settings > Alarms** window and disable the **Hide Acknowledged Alarms** perference.

You can separately search for all previously acknowledged alarms to reveal all active alarms that were acknowledged and cleared up to the seven days only. WCS automatically deletes cleared alerts that are more than seven days old. Once an alarm condition generates an alarm, no new alarms can be generated for that same condition until the existing alarm is deleted.

Setting Search Filters for Alarms

From the Monitor > Alarms page you can search for filters based on severity, category, and date range or search for rogue adhoc alarms.

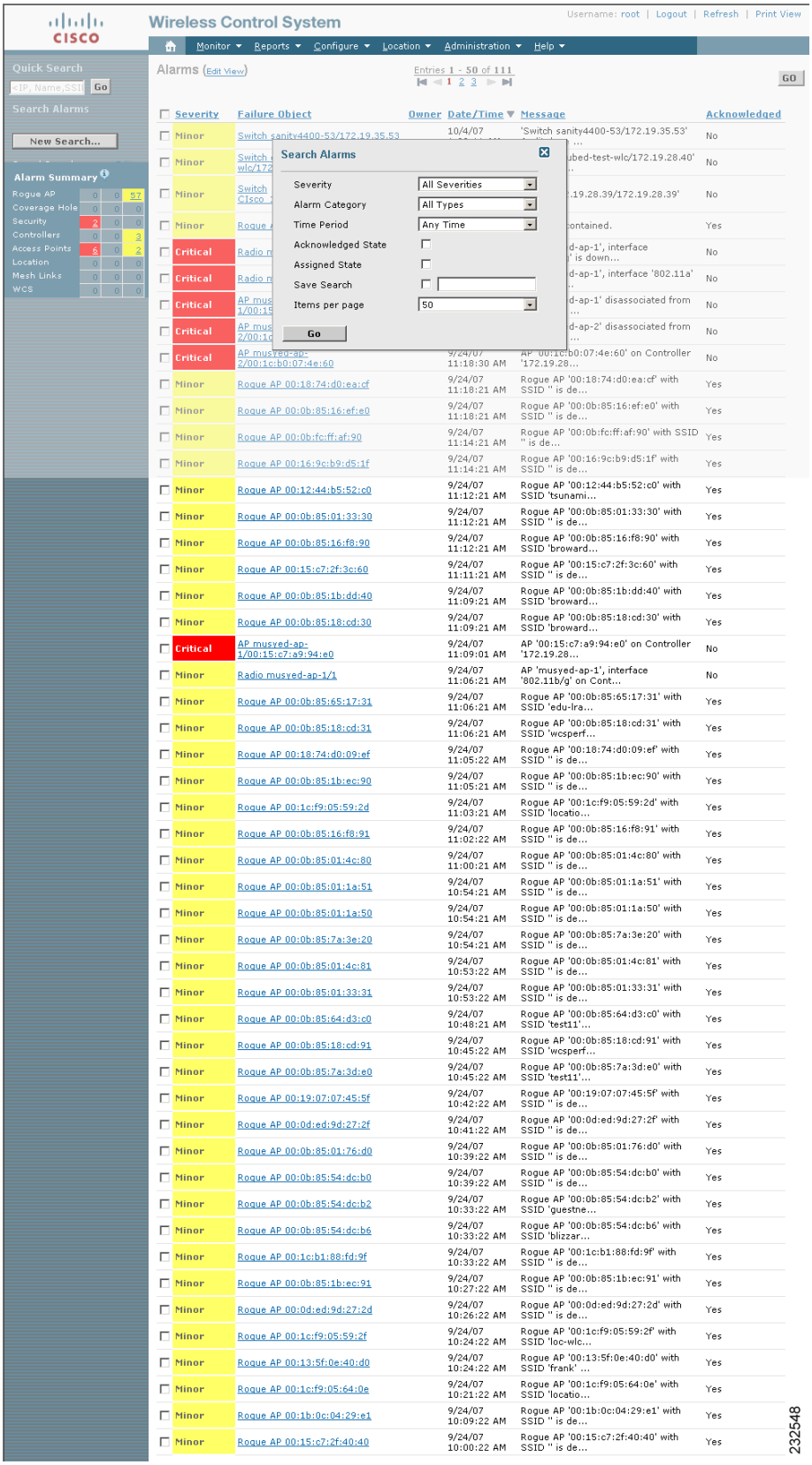
Step 1 Choose **Monitor > Alarms**. The Alarms window appears (see Figure 13-2). In the left-hand column, the saved searches that have been performed are listed.

Step 2 Use the controls in the left sidebar to create and save custom searches:

- **New Search** drop-down menu: Accesses the Search Alarms window. Use the Search Alarms window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

Step 3 If you want to run a new search, click the **New Search** link. A Search Alarms menu appears (see Figure 13-4).

Figure 13-4 Search Alarms Window



Step 4 Use the Severity drop-down menu to choose which level of severity to search for.

Note A user can modify the severities assigned to various system conditions, but the following definitions are general guidelines that will be used as the default.

- All Severities: Selects severities of every type.
- Critical: The system requires immediate attention and correction.
- Major: An error occurred and requires attention.
- Minor: A condition is noted and recorded, but it may not be an error.
- Warning: A warning message indicates a potential error condition. Warnings are not displayed in the alarm summary dashboard.
- Informational: An information message provides routine information on normal events, but an alarm is not generated.
- Clear: The existing alarm is cleared.

Step 5 Use the Alarm Category drop-down menu to choose which devices you want to limit in the search. The choices are all, access point, controller, WCS, security, coverage, rogue access point, rogue adhoc, mesh links, location servers, and location notifications.

Step 6 Use the Time Period drop-down menu to choose a time increment from Any Time to Last 7 days. The default is Any Time.

Step 7 Check Acknowledged State to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not checked, the acknowledged state is not considered in the search criteria.

Step 8 Check Assigned State to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not checked, the assigned state is not considered for search criteria.

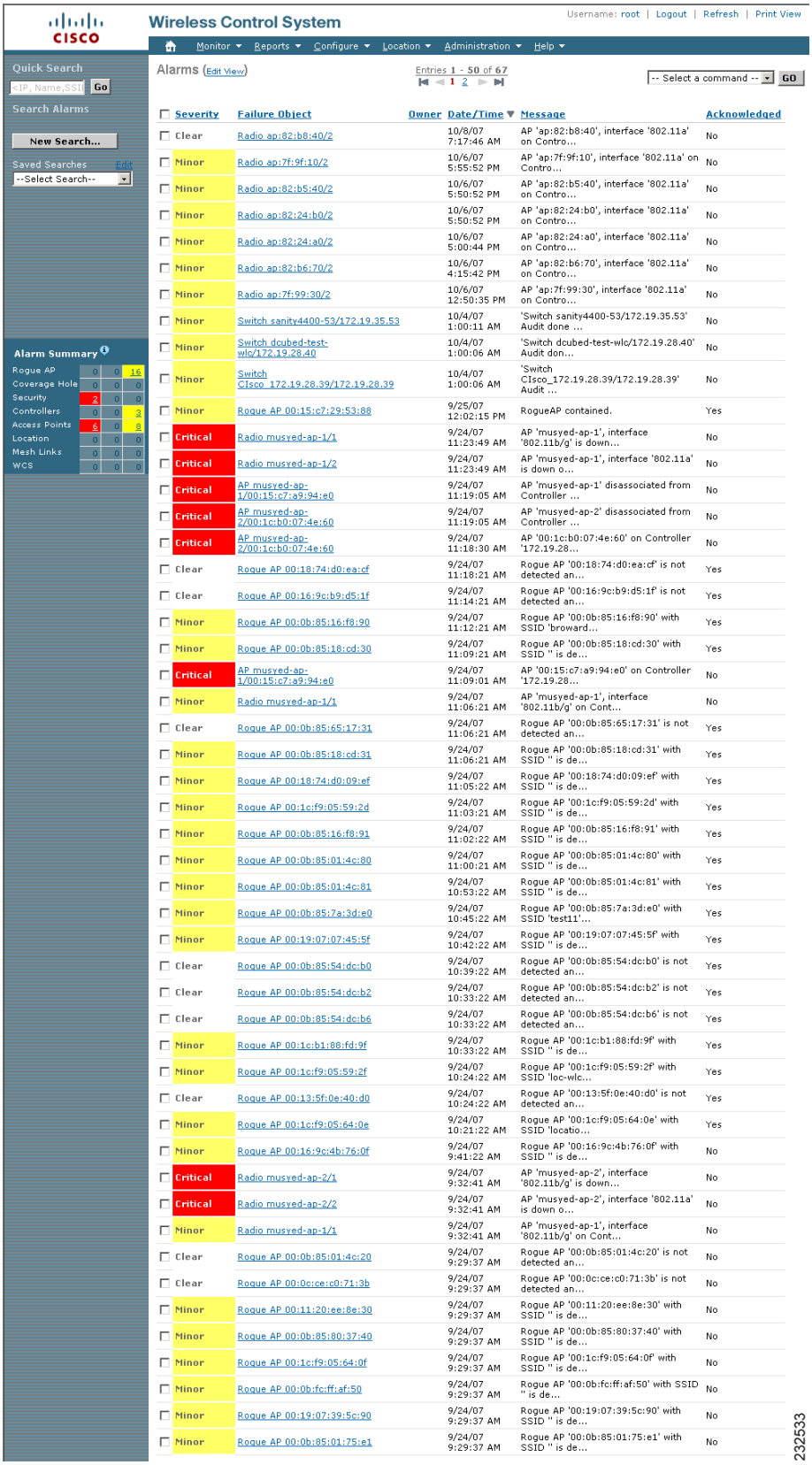
Note When you select Owner Name, type the owner name, if assigned.

Step 9 Click the **Save Search** check box if you want to save this search. You can then assign a name to this search.

Step 10 Choose the number of found items to display on the search results page. The default is 20.

Step 11 Click **GO**. The search begins, and the list of failed objects displays (see Figure 13-5). The date and time of the failure and a brief message about the failure is provided.

Figure 13-5 Alarms Displaying After Search



Step 12 The alarm search results reveal the following:

- Severity—Either Critical, Major, Minor, Warning, Clear, or Info.
- Failure Object—Clicking the title toggles between the name and the object in the message column.
- Owner—Name of person to whom this alarm is assigned or blank. Clicking the title toggles between ascending and descending order.
- Date/Time—When the alarm occurred. Clicking the title toggles between ascending and descending order.
- Message—Message explaining why the alarm occurred. Clicking the title toggles between ascending and descending order.
- Acknowledged—Indicates whether or not the alarm has been acknowledged.

Step 13 Click the failure object link to get more in depth information on this particular alarm.

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.

Notification Format

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

Table 13-1 Notification Format

Field	Description
Title	The notification title is generally picked up from an event property file defined in the NMS.
MIB Name	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.
WCS Message	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 "{0}" 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.
Symptoms	This field displays the symptoms associated with this event.
WCS Severity	This field displays the severity assigned to this event in WCS.
Probable Causes	This field lists the probable causes of the notification.
Recommended Actions	This field lists any actions recommended for the administrator managing the wireless network.

Traps Added in Release 2.0

AP_BIG_NAV_DOS_ATTACK

MIB Name	bsnApBigNavDosAttack.
WCS Message	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.
Symptoms	The system detected a possible denial of service attack and suspended all traffic to the affected channel.
WCS Severity	Critical.
Probable Causes	A malicious denial of service attack is underway.
Recommended Actions	Identify the source of the attack in the network and take the appropriate action immediately.

AP_CONTAINED_AS_ROGUE

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

AP_DETECTED_DUPLICATE_IP

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

AP_HAS_NO_RADIOS

MIB Name	bsnApHasNoRadioCards.
WCS Message	**Not supported in WCS yet**.

Symptoms	An access point is reporting that it has no radio cards.
WCS Severity	N/A.
Probable Causes	Manufacturing fault or damage to the system during shipping.
Recommended Actions	Call customer support.

AP_MAX_ROGUE_COUNT_CLEAR

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

AP_MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnApMaxRogueCountExceeded.
WCS Message	Fake AP or other attack may be in progress. Rogue AP count on AP with MAC address "{0}" associated with Switch "{2}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a switch (controller) exceeds the internal threshold.
WCS Severity	Critical.
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)

MIB Name	AuthenticationFailure.
WCS Message	Switch "{0}". Authentication failure reported.
Symptoms	There was an SNMP authentication failure on the switch (controller).
WCS Severity	Informational.
Probable Causes	An incorrect community string is in use by a management application.
Recommended Actions	Identify the source of the incorrect community string and correct the string within the management application.

BSN_AUTHENTICATION_FAILURE

MIB Name	bsnAuthenticationFailure.
WCS Message	Switch "{0}." User authentication from Switch "{0}" failed for user name "{1}" and user type "{2}."
Symptoms	A user authentication failure is reported for a local management user or a MAC filter is configured on the controller.
WCS Severity	Minor.
Probable Causes	Incorrect login attempt by an admin user from the controller CLI or controller GUI, or a client accessing the WLAN system.
Recommended Actions	If the user has forgotten the password, the superuser may need to reset it.

COLD_START (FROM MIB-II STANDARD)

MIB Name	coldStart.
WCS Message	Switch "{0}." Cold start.
Symptoms	The switch (controller) went through a reboot.
WCS Severity	Informational.
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

MIB Name	bsnConfigSaved.
WCS Message	Switch "{0}." Configuration saved in flash.
Symptoms	A configuration save to flash is performed on the switch (controller).
WCS Severity	Informational.

Probable Causes	The switch (controller) saves the configuration to the flash via a CLI command or entry via the controller GUI or WCS.
Recommended Actions	If you change the configuration using the controller CLI or controller GUI, you may need to refresh the configuration.

IPSEC_IKE_NEG_FAILURE

MIB Name	bsnIpsecIkeNegFailure.
WCS Message	IPsec IKE Negotiation failure from remote IP address "{0}."
Symptoms	Unable to establish an IPsec tunnel between a client and a WLAN appliance.
WCS Severity	Minor.
Probable Causes	Configuration mismatch.
Recommended Actions	Validate configuration, verify that authentication credentials match (preshared keys or certificates); and verify that encryption algorithms and strengths match.

IPSEC_INVALID_COOKIE

MIB Name	bsnIpsecInvalidCookieTrap.
WCS Message	IPsec Invalid cookie from remote IP address "{0}."
Symptoms	Cannot successfully negotiate an IPsec session.
WCS Severity	Minor.
Probable Causes	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.
Recommended Actions	Reset the IPsec client and then restart tunnel establishment.

LINK_DOWN (FROM MIB-II STANDARD)

MIB Name	linkDown.
WCS Message	Port "{0}" is down on Switch "{1}."
Symptoms	The physical link on one of the switch (controller) ports is down.
WCS Severity	Critical.
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)

MIB Name	linkUp.
WCS Message	Port "{0}" is up on Switch "{1}."
Symptoms	The physical link is up on a switch (controller) port.

WCS Severity	Informational.
Probable Causes	A physical link to the switch (controller) is restored.
Recommended Actions	None.

LRAD_ASSOCIATED

MIB Name	bsnAPAssociated.
WCS Message	AP "{0}" associated with Switch "{2}" on Port number "{1}."
Symptoms	An access point has associated with a switch (controller).
WCS Severity	Informational.
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

MIB Name	bsnAPDisassociated.
WCS Message	AP "{0}" disassociated from Switch "{1}."
Symptoms	The switch (controller) is no longer detecting an access point.
WCS Severity	Informational.
Probable Causes	• A failure in the access point. • An access point is no longer on the network.
Recommended Actions	Check if the access point is powered up and has network connectivity to the switch (controller).

LRADIF_COVERAGE_PROFILE_FAILED

MIB Name	bsnAPCoverageProfileFailed.
WCS Message	AP "{0}," interface "{1}." Coverage threshold of "{3}" is violated. Total no. of clients is "{5}" and no. failed clients is "{4}."
Symptoms	Number of clients experiencing suboptimal performance has crossed the configured threshold.
WCS Severity	Minor.

Probable Causes	Many clients are wandering to the remote parts of the coverage area of this radio interface with no handoff alternative.
Recommended Actions	• If the configured threshold is too low, you may need to readjust it to a more optimal value. • If the coverage profile occurs on a more frequent basis, you may need to provide additional radio coverage. • If the power level of this radio can be manually controlled, you may need to boost it to increase the coverage area.

LRADIF_COVERAGE_PROFILE_PASSED

MIB Name	bsnAPCoverageProfileUpdatedToPass.
WCS Message	AP "{0},” interface "{1}." Coverage changed to acceptable.
Symptoms	A radio interface that was reporting coverage profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The number of clients on this radio interface with suboptimal performance has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_CURRENT_CHANNEL_CHANGED

MIB Name	bsnAPCurrentChannelChanged.
WCS Message	AP "{0},” interface "{1}." Channel changed to "{2}." Interference Energy before update was "{3}" and after update is "{4}."
Symptoms	The current channel assigned to a radio interface has automatically changed.
WCS Severity	Informational.
Probable Causes	Possible interference on a channel has caused the radio management software on the controller to change the channel.
Recommended Actions	None.

LRADIF_CURRENT_TXPOWER_CHANGED

MIB Name	bsnAPCurrentTxPowerChanged.
WCS Message	AP "{0},” interface "{1}." Transmit Power Level changed to "{2}."
Symptoms	The power level has automatically changed on a radio interface.
WCS Severity	Informational.
Probable Causes	The radio management software on the controller has modified the power level for optimal performance.
Recommended Actions	None.

LRADIF_DOWN

MIB Name	bsnAPIfDown.
WCS Message	AP "{0}," interface "{1}" is down.
Symptoms	A radio interface is out of service.
WCS Severity	Critical if not disabled, otherwise Informational.
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

MIB Name	bsnAPInterferenceProfileFailed.
WCS Message	AP "{0}," interface "{1}." Interference threshold violated.
Symptoms	The interference detected on one or more channels is violated.
WCS Severity	Minor.
Probable Causes	There are other 802.11 devices in the same band that are causing interference on channels used by this system.
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 on 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

MIB Name	bsnAPInterferenceProfileUpdatedToPass.
WCS Message	AP "{0}," interface "{1}." Interference changed to acceptable.
Symptoms	A radio interface reporting interference profile failure has reverted to an acceptable level.
WCS Severity	Informational.

Probable Causes	The interference on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_LOAD_PROFILE_FAILED

MIB Name	bsnAPLoadProfileFailed.
WCS Message	AP "{0},” interface "{1}." Load threshold violated.
Symptoms	A radio interface of an access point is reporting that the client load has crossed a configured threshold.
WCS Severity	Minor.
Probable Causes	There are too many clients associated with this radio interface.
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

MIB Name	bsnAPLoadProfileUpdatedToPass.
WCS Message	AP "{0}," interface "{1}." Load changed to acceptable.
Symptoms	A radio interface that was reporting load profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The load on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_NOISE_PROFILE_FAILED

MIB Name	bsnAPNoiseProfileFailed.
WCS Message	AP "{0}," interface "{1}." Noise threshold violated.
Symptoms	The monitored noise level on this radio has crossed the configured threshold.
WCS Severity	Minor.
Probable Causes	Noise sources that adversely affect the frequencies on which the radio interface operates.
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

MIB Name	bsnAPNoiseProfileUpdatedToPass.
WCS Message	AP "{0}," interface "{1}." Noise changed to acceptable.
Symptoms	A radio interface that was reporting noise profile failure has reverted to an acceptable level.
WCS Severity	Informational.
Probable Causes	The noise on this radio interface has dropped below the configured threshold.
Recommended Actions	None.

LRADIF_UP

MIB Name	bsnAPIfUp.
WCS Message	AP "{0}," interface "{1}" is up.
Symptoms	A radio interface is back up.
WCS Severity	Informational.
Probable Causes	• An administrator has enabled a radio interface. • An access point has turned on. • A new access point has joined the network.
Recommended Actions	None.

MAX_ROGUE_COUNT_CLEAR

MIB Name	bsnMaxRogueCountClear.
WCS Message	Fake AP or other attack is cleared now. Rogue AP count on system "{0}" is within the threshold of "{1}."
Symptoms	The number of rogues detected by a controller is within acceptable limits.
WCS Severity	Informational.
Probable Causes	N/A.
Recommended Actions	None.

MAX_ROGUE_COUNT_EXCEEDED

MIB Name	bsnMaxRogueCountExceeded.
WCS Message	Fake AP or other attack may be in progress. Rogue AP count on system "{0}" has exceeded the severity warning threshold of "{1}."
Symptoms	The number of rogues detected by a controller exceeds the internal threshold.
WCS Severity	Critical.
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

MIB Name	multipleUsersTrap.
WCS Message	Switch "{0}." Multiple users logged in.
Symptoms	Multiple users with the same login ID are logged in through the CLI.
WCS Severity	Informational.
Probable Causes	The same user has logged in multiple times through the CLI interface.
Recommended Actions	Verify that the expected login sessions for the same user are valid.

NETWORK_DISABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to disabled).
WCS Message	Global "{1}" network status disabled on Switch with IP Address "{0}."
Symptoms	An administrator has disabled the global network for 802.11a/n and 802.11b/g/n.
WCS Severity	Informational.
Probable Causes	Administrative command.
Recommended Actions	None.

NO_ACTIVITY_FOR_ROGUE_AP

MIB Name	This is a WCS-only event generated when no rogue activity is seen for a specific duration.
WCS Message	Rogue AP "{0}" is cleared explicitly. It is not detected anymore.
Symptoms	A rogue access point is cleared from the management system due to inactivity.
WCS Severity	Informational.
Probable Causes	A rogue access point is not located on any managed controller for a specified duration.
Recommended Actions	None.

POE_CONTROLLER_FAILURE

MIB Name	bsnPOEControllerFailure.
WCS Message	The POE controller has failed on the Switch "{0}."
SYMPTOMS	A failure in the Power Over Ethernet (POE) unit is detected.
WCS Severity	Critical.
Probable Causes	The power of the Ethernet unit has failed.
Recommended Actions	Call customer support. The unit may need to be repaired.

RADIOS_EXCEEDED

MIB Name	bsnRadiosExceedLicenseCount.
WCS Message	The Radios associated with Switch "{0}" exceeded license count "{1}." The current number of radios on this switch is "{2}."
Symptoms	The number of supported radios for a switch (controller) has exceeded the licensing limit.
WCS Severity	Major.
Probable Causes	The number of access points associated with the switch (controller) has exceeded the licensing limits.
Recommended Actions	Upgrade the license for the switch (controller) to support a higher number of access points.

RADIUS_SERVERS_FAILED

MIB Name	bsnRADIUSServerNotResponding.
WCS Message	Switch "{0}." RADIUS server(s) are not responding to authentication requests.
Symptoms	The switch (controller) is unable to reach any RADIUS server for authentication.
WCS Severity	Critical.
Probable Causes	Network connectivity to the RADIUS server is lost or the RADIUS server is down.
Recommended Actions	Verify the status of all configured RADIUS servers and their network connectivity.

ROGUE_AP_DETECTED

MIB Name	bsnRogueAPDetected.
WCS Message	Rogue AP or rogue adhoc "{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 rogue adhoc "{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

MIB Name	bsnRogueAPRemoved.
WCS Message	Rogue AP or rogue adhoc "{0}" is removed; it was detected as Rogue AP by AP "{1}" Radio type "{2}."
Symptoms	The system is no longer detecting a rogue access point.
WCS Severity	Informational.
Probable Causes	A rogue access point has powered off or moved away and therefore the system no longer detects it.
Recommended Actions	None.

RRM_DOT11_A_GROUPING_DONE

MIB Name	bsnRrmDot11aGroupingDone.
WCS Message	RRM 802.11a/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module is finished grouping for the A band, and a new group leader is chosen.
WCS Severity	Informational.
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

RRM_DOT11_B_GROUPING_DONE

MIB Name	bsnRrmDot11bGroupingDone.
WCS Message	RRM 802.11b/g/n grouping done; the new group leader's MAC address is "{0}."
Symptoms	The radio resource module finished its grouping for the B band and chose a new group leader.
WCS Severity	Informational.
Probable Causes	The older RRM group leader may have gone down.
Recommended Actions	None.

SENSED_TEMPERATURE_HIGH

MIB Name	bsnSensedTemperatureTooHigh.
WCS Message	The sensed temperature on the Switch "{0}" is too high. The current sensed temperature is "{1}."
Symptoms	The system's internal temperature has crossed the configured thresholds.
WCS Severity	Major.
Probable Causes	• Fan failure. • Fault in the device.
Recommended Actions	• Verify the configured thresholds and increase the value if it is too low. • Call customer support.

SENSED_TEMPERATURE_LOW

MIB Name	bsnSensedTemperatureTooLow.
WCS Message	The sensed temperature on the Switch "{0}" is too low. The current sensed temperature is "{1}."
Symptoms	The internal temperature of the device is below the configured limit in the system.
WCS Severity	Major.
Probable Causes	• Operating environment. • Hardware fault.
Recommended Actions	• Verify the configured thresholds and ensure that the limit is appropriate. • Call customer support.

STATION_ASSOCIATE

MIB Name	bsnDot11StationAssociate.
WCS Message	Client "{0}" is associated with AP "{1}," interface "{2}."
Symptoms	A client has associated with an access point.
WCS Severity	Informational.
Probable Causes	A client has associated with an access point.
Recommended Actions	None.

STATION_ASSOCIATE_FAIL

MIB Name	bsnDot11StationAssociateFail.
WCS Message	Client "{0}" failed to associate with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	A client station failed to associate with the system.
WCS Severity	Informational.
Probable Causes	The access point was busy.
Recommended Actions	Check whether the access point is busy and reporting load profile failures.

STATION_AUTHENTICATE

MIB Name	bsnDot11StationAssociate (bsnStationUserName is set).
WCS Message	Client "{0}" with user name "{3}" is authenticated with AP "{1}," interface "{2}."
Symptoms	A client has successfully authenticated with the system.
WCS Severity	Informational.
Probable Causes	A client has successfully authenticated with the system.
Recommended Actions	None.

STATION_AUTHENTICATION_FAIL

MIB Name	bsnDot11StationAuthenticateFail.
WCS Message	Client "{0}" has failed authenticating with AP "{1}," interface "{2}." The reason code is "{3}."
Symptoms	The system failed to authenticate a client.
WCS Severity	Informational.
Probable Causes	Failed client authentication.
Recommended Actions	Check client configuration and configured keys or passwords in the system.

STATION_BLACKLISTED

MIB Name	bsnDot11StationBlacklisted.
WCS Message	Client "{0}" which was associated with AP "{1}," interface "{2}" is excluded. The reason code is "{3}."
Symptoms	A client is in the exclusion list and is not allowed to authenticate for a configured interval.
WCS Severity	Minor.
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

MIB Name	bsnDot11StationDeauthenticate.
WCS Message	Client "{0}" is deauthenticated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client is no longer authenticated by the system.
WCS Severity	Informational.
Probable Causes	A client is no longer authenticated by the system.
Recommended Actions	None.

STATION_DISASSOCIATE

MIB Name	bsnDot11StationDisassociate.
WCS Message	Client "{0}" is disassociated from AP "{1}," interface "{2}" with reason code "{3}."
Symptoms	A client has disassociated with an access point in the system.
WCS Severity	Informational.
Probable Causes	A station may disassociate due to various reasons such as inactivity timeout or a forced action from the management interface.
Recommended Actions	None.

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

MIB Name	This is a WCS-only event.
WCS Message	Switch "{0}" is unreachable.
Symptoms	A switch (controller) is unreachable from the management system.
WCS Severity	Critical.
Probable Causes	• The switch (controller) has encountered hardware or software failure. • There are network connectivity issues between the management station and the switch (controller). • The configured SNMP community strings on the management station or the switch (controller) are incorrect.
Recommended Actions	• Check if the switch (controller) is powered up and reachable through the web interface. • Ping the switch (controller) from the management station to verify if there is IP connectivity. • Check the community strings configured on the management station.

SWITCH_UP

MIB Name	This is a WCS-only event.
WCS Message	Switch "{0}" is reachable.
Symptoms	A switch (controller) is now reachable from the management station.
WCS Severity	Informational.
Probable Causes	A switch (controller) is reachable from the management station.
Recommended Actions	None.

TEMPERATURE_SENSOR_CLEAR

MIB Name	bsnTemperatureSensorClear.
WCS Message	The temperature sensor is working now on the switch "{0}." The sensed temperature is "{1}."
Symptoms	The temperature sensor is operational.
WCS Severity	Informational.
Probable Causes	The system is detecting the temperature sensor to be operational now.
Recommended Actions	None.

TEMPERATURE_SENSOR_FAILURE

MIB Name	bsnTemperatureSensorFailure.
WCS Message	The temperature sensor failed on the Switch "{0}." Temperature is unknown.
Symptoms	The system is reporting that a temperature sensor has failed and the system is unable to report accurate temperature.
WCS Severity	Major.
Probable Causes	The temperature sensor has failed due to hardware failure.
Recommended Actions	Call customer support.

TOO_MANY_USER_UNSUCCESSFUL_LOGINS

MIB Name	bsnTooManyUnsuccessLoginAttempts.
WCS Message	User "{1}" with IP Address "{0}" has made too many unsuccessful login attempts.
Symptoms	A management user has made too many login attempts.
WCS Severity	Critical.
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

MIB Name	bsnAdhocRogueAutoContained.
WCS Message	Adhoc Rogue "{0}" was found and is auto contained as per WPS policy.
Symptoms	The system detected an adhoc rogue and automatically contained it.
WCS Severity	Major.
Probable Causes	The system detected an adhoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	Identify the adhoc rogue through the location application and take the appropriate action.

ADHOC_ROGUE_AUTO_CONTAINED_CLEAR

MIB Name	bsnAdhocRogueAutoContained (bsnClearTrapVariable set to true).
WCS Message	Adhoc Rogue "{0}" was found and was auto contained. The alert state is clear now.
Symptoms	An adhoc rogue that the system has detected earlier is now clear.
WCS Severity	Informational.
Probable Causes	The system no longer detects an adhoc rogue.
Recommended Actions	None.

NETWORK_ENABLED

MIB Name	bsnNetworkStateChanged (bsnNetworkState set to enabled).
WCS Message	Global "{1}" network status enabled on Switch with IP Address "{0}."
Symptoms	An administrator has enabled the global network for 802.11a/n or 802.11b/g/n.
WCS Severity	Informational.
Probable Causes	Administrative command.
Recommended Actions	None.

ROGUE_AP_AUTO_CONTAINED

MIB Name	bsnRogueApAutoContained.
WCS Message	Rogue AP "{0}" is advertising our SSID and is auto contained as per WPS policy.
Symptoms	The system has automatically contained a rogue access point.
WCS Severity	Major.
Probable Causes	The system detected an adhoc rogue and automatically contained it as configured in the system's wireless prevention policy.
Recommended Actions	• Track the location of the rogue and take the appropriate action. • If this is a known valid access point, clear the rogue from containment.

ROGUE_AP_AUTO_CONTAINED_CLEAR

MIB Name	bsnRogueApAutoContained (bsnClearTrapVariable set to true).
Message	Rogue AP "{0}" was advertising our SSID and was auto contained. The alert state is clear now.
Symptoms	The system has cleared a previously contained rogue.
WCS Severity	Informational.
Probable Causes	The system has cleared a previously contained rogue.
Recommended Actions	None.

TRUSTED_AP_INVALID_ENCRYPTION

MIB Name	bsnTrustedApHasInvalidEncryption.
WCS Message	Trusted AP "{0}" is invalid encryption. It is using "{1}" instead of "{2}." It is auto contained as per WPS policy.
Symptoms	The system automatically contained a trusted access point that has invalid encryption.
WCS Severity	Major.
Probable Causes	The system automatically contained a trusted access point that violated the configured encryption policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_ENCRYPTION_CLEAR

MIB Name	bsnTrustedApHasInvalidEncryption (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid encryption. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_RADIO_POLICY

MIB Name	bsnTrustedApHasInvalidRadioPolicy.
WCS Message	Trusted AP "{0}" has invalid radio policy. It is using "{1}" instead of "{2}." It has been auto contained as per WPS policy.
Symptoms	The system has contained a trusted access point with an invalid radio policy.
WCS Severity	Major.
Probable Causes	The system has contained a trusted access point connected to the wireless system for violating the configured radio policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_RADIO_POLICY_CLEAR

MIB Name	bsnTrustedApHasInvalidRadioPolicy (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid radio policy. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured encryption policy.
Recommended Actions	None.

TRUSTED_AP_INVALID_SSID

MIB Name	bsnTrustedApHasInvalidSsid.
WCS Message	Trusted AP "{0}" has invalid SSID. It was auto contained as per WPS policy.
Symptoms	The system has automatically contained a trusted access point for advertising an invalid SSID.
WCS Severity	Major.
Probable Causes	The system has automatically contained a trusted access point for violating the configured SSID policy.
Recommended Actions	Identify the trusted access point and take the appropriate action.

TRUSTED_AP_INVALID_SSID_CLEAR

MIB Name	bsnTrustedApHasInvalidSsid (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" had invalid SSID. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The trusted access point has now conformed to the configured policy.
Recommended Actions	None.

TRUSTED_AP_MISSING

MIB Name	bsnTrustedApIsMissing.
WCS Message	Trusted AP "{0}" is missing or has failed.
Symptoms	The wireless system no longer detects a trusted access point.
WCS Severity	Major.
Probable Causes	A trusted access point has left the network or has failed.
Recommended Actions	Track down the trusted access point and take the appropriate action.

TRUSTED_AP_MISSING_CLEAR

MIB Name	bsnTrustedApIsMissing (bsnClearTrapVariable set to true).
WCS Message	Trusted AP "{0}" is missing or has failed. The alert state is clear now.
Symptoms	The system has found a trusted access point again.
WCS Severity	Informational.
Probable Causes	The system has detected a previously missing trusted access point.
Recommended Actions	None.

Traps Added in Release 2.2

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP Impersonation with MAC "{0}" is detected by authenticated AP "{1}" on "{2}" radio and Slot ID "{3}."
Symptoms	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.
WCS Severity	Critical.
Probable Causes	A severity breach related to access point impersonation may be under way.
Recommended Actions	Track down the MAC address of the impersonating access point in the network and contain it.

AP_RADIO_CARD_RX_FAILURE

MIB Name	bsnAPRadioCardRxFailure.
WCS Message	Receiver failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to receive data.
WCS Severity	Critical.
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

MIB Name	bsnAPRadioCardRxFailureClear.
WCS Message	Receiver failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing reception failure.
WCS Severity	Informational.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

AP_RADIO_CARD_TX_FAILURE

MIB Name	bsnAPRadioCardTxFailure.
WCS Message	Transmitter failure detected on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio card is unable to transmit.
WCS Severity	Critical.
Probable Causes	• A radio card is experiencing transmission failure. • The antenna of the radio may be disconnected.
Recommended Actions	• Check the antenna of the access point. • Call customer support.

AP_RADIO_CARD_TX_FAILURE_CLEAR

MIB Name	bsnAPRadioCardTxFailureClear.
WCS Message	Transmitter failure cleared on the "{0}" radio of AP "{1}" on Switch "{2}."
Symptoms	A radio is no longer experiencing transmission failure.
WCS Severity	Informational.
Probable Causes	A malfunction in the access point has been corrected.
Recommended Actions	None.

SIGNATURE_ATTACK_CLEARED

MIB Name	bsnSignatureAttackDetected (bsnClearTrapVariable is set to True).
WCS Message	Switch "{0}" is cleared from IDS signature attack. The wireless system is no longer detecting the intrusion.
Symptoms	The switch (controller) no longer detects a signature attack.
WCS Severity	Informational.
Probable Causes	The signature attack that the system previously detected has stopped.
Recommended Actions	None.

SIGNATURE_ATTACK_DETECTED

MIB Name	bsnSignatureAttackDetected
WCS Message	IDS Signature attack detected on Switch "{0}." The Signature Type is "{1}," Signature Name is "{2}," and Signature description is "{3}."
Symptoms	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.
WCS Severity	Critical.
Probable Causes	Someone is mounting a malevolent signature attack.
Recommended Actions	Track down the source of the signature attack in the wireless network and take the appropriate action.

TRUSTED_AP_HAS_INVALID_PREAMBLE

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

TRUSTED_HAS_INVALID_PREAMBLE_CLEARED

MIB Name	bsnTrustedApHasInvalidPreamble (bsnClearTrapVariable is set to true).
WCS Message	Trusted AP "{0}" on Switch "{3}" had invalid preamble. The alert state is clear now.
Symptoms	The system has cleared a previous alert about a trusted access point.
WCS Severity	Informational.
Probable Causes	The system has cleared a previous alert about a trusted access point.
Recommended Actions	None.

Traps Added in Release 3.0

AP_FUNCTIONALITY_DISABLED

MIB Name	bsnAPFunctionalityDisabled.
WCS Message	AP functionality has been disabled for key "{0}," reason being "{1}" for feature-set "{2}."
Symptoms	The system sends this trap out when the controller disables access point functionality because the license key has expired.
WCS Severity	Critical.
Probable Causes	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.
Recommended Actions	Configure the correct license key on the controller and reboot it to restore access point functionality.

AP_IP_ADDRESS_FALLBACK

MIB Name	bsnAPIPAddressFallback.
WCS Message	AP "{0}" with static-ip configured as "{2}" has fallen back to the working DHCP address "{1}."
Symptoms	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.
WCS Severity	Minor.
Probable Causes	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.
Recommended Actions	Reconfigure the access point's static IP to the correct IP address if desired.

AP_REGULATORY_DOMAIN_MISMATCH

MIB Name	bsnAPRegulatoryDomainMismatch.
WCS Message	AP "{1}" is unable to associate. The Regulatory Domain configured on it "{3}" does not match the Controller "{0}" country code "{2}."
Symptoms	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.
WCS Severity	Critical.
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

MIB Name	bsnRxMulticastQueueFull.
WCS Message	CPU Receive Multicast Queue is full on Controller "{0}."
Symptoms	This trap indicates that the CPU's Receive Multicast queue is full.
WCS Severity	Critical.
Probable Causes	An ARP storm.
Recommended Actions	None.

Traps Added in Release 3.1

AP_AUTHORIZATION_FAILURE

MIB Name	bsnAPAuthorizationFailure
WCS Message	• Failed to authorize AP “{0}." Authorization entry does not exist in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." AP’s authorization key does not match with SHA1 key in Controllers “{1}” AP Authorization List. • Failed to authorize AP “{0}." Controller “{1}” could not verify the Self Signed Certificate from the AP. • Failed to authorize AP “{0}." AP has a self signed certificate where as the Controllers “{1}” AP authorization list has Manufactured Installed Certificate for this AP.
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

MIB Name	heartbeatLossTrap.
WCS Message	Keepalive messages are lost between Master and Controller"{0}.”
Symptoms	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.
WCS Severity	Major.
Probable Causes	• Port on the WiSM controller could be down. • Loss of connection with the Supervisor Switch.
Recommended Actions	None.

INVALID_RADIO_INTERFACE

MIB Name	invalidRadioTrap.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” that has joined controller “{2}” has invalid interface. The reason is “{3}.”
Symptoms	If a Cisco access point joins the network but has unsupported radios, the controller detects this and generates a trap. This symptom propogates an alert in WCS.
WCS Severity	Critical.
Probable Causes	The radio hardware is not supported by the controller.
Recommended Actions	None.

RADAR_CLEARED

MIB Name	bsnRadarChannelCleared
WCS Message	Radar has been cleared on channel "{1}" which was detected by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	Trap is generated after the expiry of a non-occupancy period for a channel that previously generated a radar trap.
WCS Severity	Informational.
Probable Causes	Trap is cleared on a channel.
Recommended Actions	None.

RADAR_DETECTED

MIB Name	bsnRadarChannelDetected
WCS Message	Radar has been detected on channel "{1}" by AP base radio MAC "{0}" on radio 802.11a/n.
Symptoms	This trap is generated when radar is detected on the channel on which an access point is currently operating.
WCS Severity	Informational.
Probable Causes	Radar is detected on a channel.
Recommended Actions	None.

RADIO_CORE_DUMP

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

RADIO_INTERFACE_DOWN

MIB Name	bsnAPIfDown.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” is down. The reason is “{2}.”
Symptoms	When a radio interface is down, WCS generates an alert. Reason for the radio outage is also noted.
WCS Severity	Critical if not manually disabled. Informational if radio interface was manually disabled.
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

MIB Name	bsnAPIfUp.
WCS Message	Radio with MAC address “{0}” and protocol “{1}” is up. The reason is “{2}.”
Symptoms	When a radio interface is operational again, WCS clears the previous alert. Reason for the radio being up again is also noted.
WCS Severity	Informational.
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

MIB Name	unsupportedAPTrap.
WCS Message	AP "{0}" tried to join controller "{1}" and failed. The controller does not support this kind of AP.
Symptoms	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.
WCS Severity	Informational.
Probable Causes	Access point is not supported by the controller.
Recommended Actions	None.

Traps Added in Release 3.2

LOCATION_NOTIFY_TRAP

MIB Name	locationNotifyTrap.
WCS Message	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: • Absence of <Element> with MAC <macAddress>, last seen at <timestamp>. • <Element> with MAC <macAddress> is <In | Out> the Area <campus | building | floor | coverageArea>. • <Element> with MAC <macAddress> has moved beyond <specifiedDistance> ft. of marker <MarkerName>, located at a range of <foundDistance> ft. For detailed info on the XML format for the trap content, consult the *2700 Location Appliance Configuration Guide*.
Symptoms	A 2700 location appliance sends this trap out when the defined location notification conditions are met (such at element outside area, elements missing, and elements exceeded specified distance). WCS uses this trap to display alarms about location notification conditions.
WCS Severity	Minor (under the Location Notification dashboard).
Probable Causes	The location notification conditions configured for a 2700 location appliance are met for certain elements on the network.
Recommended Actions	None.

Traps Added In Release 4.0

CISCO_LWAPP_MESH_POOR_SNR

MIB Name	ciscoLwappMeshPoorSNR
WCS Message	Poor SNR.
Symptoms	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.
WCS Severity	Major.
Probable Causes	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.
Recommended Actions	None.

CISCO_LWAPP_MESH_PARENT_CHANGE

MIB Name	ciscoLwappMeshParentChange
WCS Message	Parent changed.
Symptoms	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.
WCS Severity	Info.
Probable Causes	The child moved to another parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_MOVED

MIB Name	ciscoLwappMeshChildMoved
WCS Message	Child moved.
Symptoms	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.
WCS Severity	Info.
Probable Causes	The child moved from the parent.
Recommended Actions	None.

CISCO_LWAPP_MESH_CONSOLE_LOGIN

MIB Name	ciscoLwappMeshConsoleLogin
WCS Message	Console login successful or failed.
Symptoms	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.
WCS Severity	A login is of critical severity.
Probable Causes	You have successfully logged in to the access point console port or failed on three consecutive tries.
Recommended Actions	None.

CISCO_LWAPP_MESH_AUTHORIZATION_FAILURE

MIB Name	ciscoLwappMeshAuthorizationFailure
WCS Message	Fails to authenticate with controller.
Symptoms	WCS receives a trap from the controller. The trap contains the MAC addresses of those access points that failed authorization.
WCS Severity	Minor.
Probable Causes	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.
Recommended Actions	None.

CISCO_LWAPP_MESH_CHILD_EXCLUDED_PARENT

MIB Name	ciscoLwappMeshChildExcludedParent
WCS Message	Parent AP being excluded by child AP.
Symptoms	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.
WCS Severity	Info.
Probable Causes	A child marked a parent for exclusion.
Recommended Actions	None.

CISCO_LWAPP_MESH_EXCESSIVE_PARENT_CHANGE

MIB Name	ciscoLwappMeshExcessiveParentChange
WCS Message	Parent changed frequently.
Symptoms	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.
WCS Severity	Major.
Probable Causes	The MESH access point changed its parent frequently.
Recommended Actions	None.

IDS_SHUN_CLIENT_TRAP

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

IDS_SHUN_CLIENT_CLEAR_TRAP

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

MFP_TIMEBASE_STATUS_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpTimebaseStatus.
WCS Message	Controller "{0}" is "{1}" with the Central time server.
Symptoms	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.
WCS Severity	Critical (not in sync trap) and clear (sync trap).
Probable Causes	The controller's time base is not in sync with the Central time base.
Recommended Actions	None.

MFP_ANOMALY_DETECTED_TRAP

MIB Name	CISCO-LWAPP-MFP-MIB. ciscoLwappMfpAnomalyDetected.
WCS Message	MFP configuration of the WLAN was violated by the radio interface "{0}" and detected by the radio interface "{1}" of the access point with MAC address "{2}." The violation is "{3}."
Symptoms	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. **Note** This notification is generated by the controller only if MFP was configured as the protection mechanism through cLMfpProtectType.
WCS Severity	Critical.
Probable Causes	The MFP configuration of the WLAN was violated. Various types of violations are invalidMic, invalidSeq, noMic, and unexpectedMic.
Recommended Actions	None.

GUEST_USER_REMOVED_TRAP

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserRemoved.
WCS Message	Guest user "{1}" deleted on controller "{0}."
Symptoms	This notification is generated when the lifetime of the guest user {1} expires and the guest user's accounts are removed from the controller "{0}."
WCS Severity	Critical.
Probable Causes	GuestUserAccountLifetime expired.
Recommended Actions	None.

Traps Added/Updated in Release 4.0.96.0

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP Impersonation with MAC "{0}" using source MAC "{1}" is detected by authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	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.
WCS Severity	Critical.
Probable Causes	A security breach related to access point impersonation may be occurring.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

RADIUS_SERVER_DEACTIVATED

MIB Name	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	ciscoLwappAAARadiusServerGlobalDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated.
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_WLAN_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanActivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
WCS Severity	Clear.
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
WCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from a client or user.
WCS Severity	Informational.
Probable Causes	RADIUS server fails to process the request from the client or user.
Recommended Actions	None.

DECRYPT_ERROR_FOR_WRONG_WPA_WPA2

MIB Name	CISCO-LWAPP-DOT11-CLIENT-MIB. CiscoLwappDot11ClientKeyDecryptError.
WCS Message	Decrypt error occurred at AP with MAC "{0}" running TKIP with wrong WPA/WPA2 by client with MAC "{1}."
Symptoms	The controller detects that a user is trying to connect with an invalid security policy for WPA/WPA2 types.
WCS Severity	Minor.
Probable Causes	The user failed to authenticate and join the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.1

AP_IMPERSONATION_DETECTED

MIB Name	bsnAPImpersonationDetected.
WCS Message	AP impersonation of MAC "{0}" using source MAC "{1}" is detected by an authenticated AP "{2}" on "{3}" radio and slot ID "{4}."
Symptoms	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.
WCS Severity	Critical.
Probable Causes	A security breach related to access point impersonation has occurred.
Recommended Actions	Track down the MAC address of the impersonating access point and contain it.

INTERFERENCE_DETECTED

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

INTERFERENCE_CLEAR

MIB Name	COGNIO-TRAPS-MIB. cognioInterferenceClear
WCS Message	Interference cleared.
Symptoms	The Cognio spectrum expert agent no longer detects an interference source over its configured threshold.
WCS Severity	Clear.
Probable Causes	Previous excessive wireless interference or noise is gone.
Recommended Actions	None.

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_DEACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerWlanDeactivated.
WCS Message	RADIUS server "{0}" (port {1}) is deactivated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is deactivated on the WLAN.
WCS Severity	Major.
Probable Causes	RADIUS server is deactivated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_WLAN_ACTIVATED

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusServerGlobalWlanActivated.
WCS Message	RADIUS server "{0}" (port {1}) is activated on WLAN "{2}."
Symptoms	The controller detects that the RADIUS server is activated on the WLAN.
WCS Severity	Clear.
Probable Causes	RADIUS server is activated on the WLAN.
Recommended Actions	None.

RADIUS_SERVER_TIMEOUT

MIB Name	CISCO-LWAPP-AAA-MIB. ciscoLwappAAARadiusReqTimedOut.
WCS Message	RADIUS server "{0}" (port {1}) failed to respond to request from client "{2}" with MAC "{3}."
Symptoms	The controller detects that the RADIUS server failed to respond to a request from the client or user.
WCS Severity	Informational.
Probable Causes	The RADIUS server fails to process the request from a client or user.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlPathDown.
WCS Message	Controller "{0}." Control path on anchor "{1}" is down.
Symptoms	When successive ICMP ping attempts to the anchor fails, the anchor is conclusively down.
WCS Severity	Major.
Probable Causes	Anchor not reachable by ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_CTRL_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorControlUp.
WCS Message	Controller "{0}." Control path on anchor "{1}" is up.
Symptoms	The ICMP ping to the anchor is restored, and the anchor is conclusively up.
WCS Severity	Clear.
Probable Causes	The anchor is reachable by an ICMP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPath-Down.
WCS Message	Controller "{0}." Data path on anchor "{1}" is down.
Symptoms	Successive EoIP ping attempts to the anchor fails, and the anchor is conclusively down.
WCS Severity	Major.
Probable Causes	The anchor is not reachable by an EoIP ping.
Recommended Actions	None.

MOBILITY_ANCHOR_DATA_PATH_UP

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAnchorDataPath-Up.
WCS Message	Controller "{0}." Data path on anchor "{1}" is up.
Symptoms	The EoIP ping to the anchor is restored, and the anchor is conclusively up.
WCS Severity	Clear.
Probable Causes	Anchor is reachable by the EoIP ping.
Recommended Actions	None.

WLAN_ALL_ANCHORS_TRAP_DOWN

MIB Name	CISCO-LWAPP-MOBILITY-MIB. ciscoLwappMobilityAllAnchorsOnW-lanDown.
WCS Message	Controller "{0}." All anchors of WLAN "{1}" are down.
Symptoms	Successive EoIP ping attempts to all the anchors on WLAN is occurring.
WCS Severity	Critical.
Probable Causes	Anchors are not reachable by the EoIP ping.
Recommended Actions	None.

MESH_AUTHORIZATIONFAILURE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshAuthorizationFailure.
WCS Message	MESH "{0}" fails to authenticate with controller because "{1}"
Symptoms	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.
WCS Severity	Minor.

Probable Causes	The mesh node MAC address is not in the MAC filter list, or a security failure from the authorization server occurred.
Recommended Actions	None.

MESH_CHILDEXCLUDEDPARENT

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildExcludedParent.
WCS Message	Parent AP being excluded by child AP due to failed authentication, AP current parent MAC address "{0}," previous parent MAC address "{1}."
Symptoms	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.
WCS Severity	Info.
Probable Causes	The child access point failed to authenticate to the controller after a fixed number of times.
Recommended Actions	None.

MESH_PARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshParentChange.
WCS Message	MESH "{0}" changed its parent. AP current parent MAC address "{1}," previous parent MAC address "{2}."
Symptoms	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.
WCS Severity	Info.
Probable Causes	The child access point has changed its parent.
Recommended Actions	None.

MESH_CHILDMOVED

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshChildMoved.
WCS Message	Parent AP lost connection to this AP. AP neighbor type is "{0}."
Symptoms	This notification is sent by the agent when the parent access point loses connection with its child.

WCS Severity	Info.
Probable Causes	The parent access point lost connection with its child.
Recommended Actions	None.

MESH_EXCESSIVEPARENTCHANGE

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshExcessiveParentChange.
WCS Message	MESH "{0}" changes parent frequently.
Symptoms	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.
WCS Severity	Major.
Probable Causes	The child access point has frequently changed its parent.
Recommended Actions	None.

MESH_POORSNR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNR.
WCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is lower then pre-defined threshold.
Symptoms	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.
WCS Severity	Major.
Probable Causes	SNR is lower then the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_POORSNRCLEAR

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshPoorSNRClear.
WCS Message	MESH "{0}" has SNR on backhaul link as "{1}" which is normal now.
Symptoms	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.
WCS Severity	Info.

Probable Causes	SNR on the backhaul link is higher than the threshold defined by c1MeshSNRThreshold.
Recommended Actions	None.

MESH_CONSOLELOGIN

MIB Name	CISCO-LWAPP-MESH-MIB. ciscoLwappMeshConsoleLogin.
WCS Message	MESH "{0}" has console logged in with status "{1}"
Symptoms	This notification is sent by the agent when login on the MAP console is successful or when a failure occurred after three attempts.
WCS Severity	Critical.
Probable Causes	Login on the MAP console was successful, or a failure occurred after three attempts.
Recommended Actions	None.

LRADIF_REGULATORY_DOMAIN

MIB Name	ciscoLwappApIfRegulatoryDomainMismatchNotif
WCS Message	Access Point "{0}" is unable to associate. The Regulatory Domain "{1}" configured on interface "{2}" does not match the controller "{3}" regulatory domain "{4}."
Symptoms	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.
WCS Severity	Critical.
Probable Causes	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.
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.

LRAD_CRASH

MIB Name	ciscoLwappApCrash
WCS Message	Access Point "{0}" crashed and has a core dump on controller "{1}."
Symptoms	An access point has crashed.
WCS Severity	Info.

Probable Causes	Access point failure.
Recommended Actions	Capture the core dump file using the controller's CLI and send it to TAC support.

LRAD_UNSUPPORTED

MIB Name	ciscoLwappApUnsupported
WCS Message	Access Point "{0}" tried to join controller "{1}" and failed. Associate failure reason "{2}."
Symptoms	An access point tried to associate to a controller to which it is not supported.
WCS Severity	Info.
Probable Causes	The access point is not supported by the controller.
Recommended Actions	None.

Traps Added or Updated in Release 4.2

GUEST_USER_ADDED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserAdded
WCS Message	Guest user "{0}" created on the controller "{1}."
Symptoms	This notification is sent by the agent when the GuestUser account is created successfully.
WCS Severity	Info.
Probable Causes	The guest user account was created on the agent by either CLI, Web UI, or WCS.
Recommended Actions	None.

GUEST_USER_AUTHENTICATED

MIB Name	CISCO-LWAPP-WEBAUTH-MIB. cLWAGuestUserLogged
WCS Message	Guest user "{0}" logged into controller "{1}."
Symptoms	This notification is sent by the agent when the GuestUser logged into the network through webauth successfully.
WCS Severity	Info.
Probable Causes	The guest user was successful with webauth authentication.
Recommended Actions	None.

IOSAP_LINK_UP

MIB Name	linkUp
WCS Message	Autonomous AP "{0}," Interface "{1}" is {2} up.
Symptoms	The physical link is up on an autonomous access point radio port.
WCS Severity	Clear.
Probable Causes	A physical link has been restored to the autonomous access point.
Recommended Actions	None.

IOSAP_LINK_DOWN

MIB Name	linkDown
WCS Message	Autonomous AP "{0}," Interface "{1}" is {2} down.
Symptoms	The physical link is down on an autonomous access point radio port.
WCS Severity	Critical.
Probable Causes	The radio port of an autonomous access point was disabled manually or a port failure occurred.
Recommended Actions	Check the administrative status of the port. If the port administrative status is not down, check other port settings.

IOSAP_UP

MIB Name	None.
WCS Message	The autonomous AP "{0}" is reachable.
Symptoms	The autonomous AP is SNMP reachable.
WCS Severity	Clear.
Probable Causes	The autonomous access point starts to respond to SNMP queries.
Recommended Actions	None.

IOSAP_DOWN

MIB Name	None.
WCS Message	Autonomous AP "{0}" is unreachable.
Symptoms	The autonomous AP is SNMP unreachable.
WCS Severity	Critical.

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

MIB Name	None.
WCS Message	WCS with IP Address “{0}” failed to send email.
Symptoms	This notification is generated by WCS when it fails to send emails.
WCS Severity	Major.
Probable Causes	The SNMP server is either not configured or not reachable from WCS.
Recommended Actions	Check Administration > Settings > Mail Server settings. Send a test email from the mail server settings to see if it is successful.

AUDIT_STATUS_DIFFERENCE

MIB Name	None.
WCS Message	Switch “{0}” Audit done at “(1).” Config differences found between WCS and controller.
Symptoms	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.
WCS Severity	Minor.
Probable Causes	The WCS and controller configuration are not synchronized.
Recommended Actions	Refresh the configuration from the controller so that it synchronizes with the controller configuration on WCS.

ROGUE_AP_NOT_ON_NETWORK

MIB Name	bsnRogueAPDetectedOnWiredNetwork (bsnRogueAPOnWiredNetwork is set to false).
WCS Message	Rogue AP or rogue adhoc "{0}" is not able to connect to the wired network.

Symptoms	A rogue access point is no longer on the wired network.
WCS Severity	Informational.
Probable Causes	The rogue access point is no longer reachable on the wired network.
Recommended Actions	None.

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

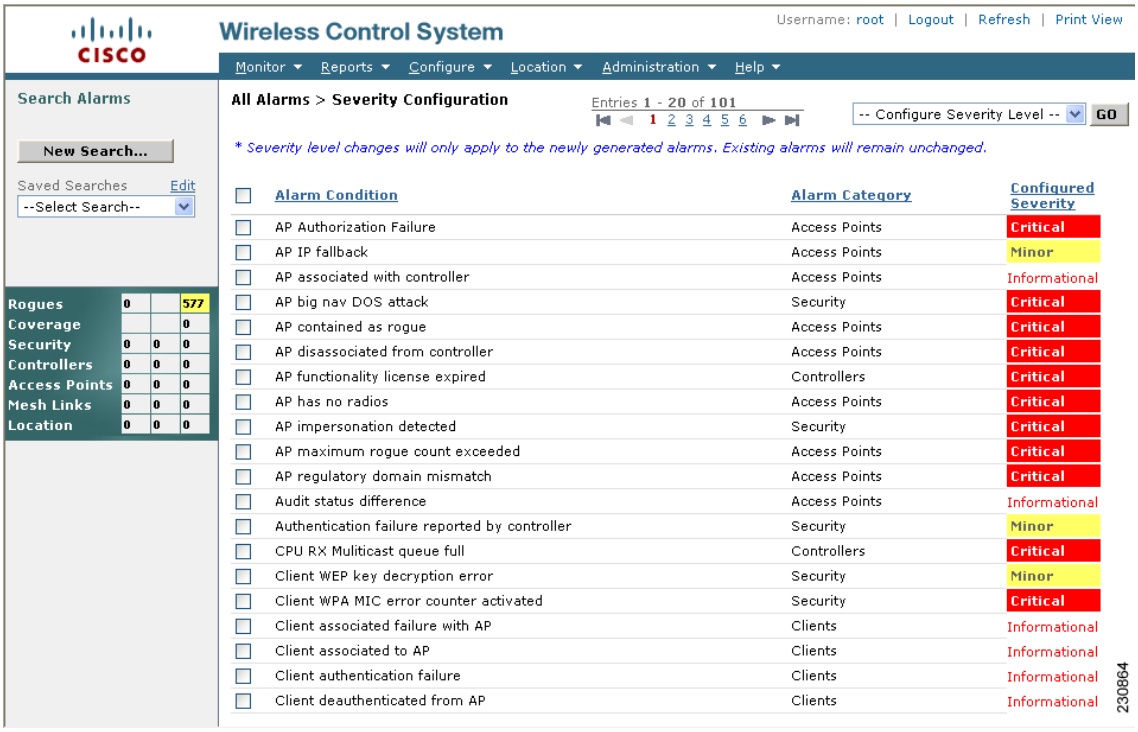
Configuring Alarm Severity

The severity levels are configurable for different alarms. You can view the severity levels for all WCS alarm conditions. Follow the steps below to configure alarm severity.

Step 1 Choose **Monitor > Alarms**.

Step 2 From the Select a command drop-down menu, choose **Severity Configuration** and click **GO**. The All Alarms > Severity Configuration window appears (see Figure 13-6).

Figure 13-6 All Alarms > Severity Configuration



Step 3 The alarm conditions along with the configured severity levels are listed. You can change the severity level. Select an alarm condition for which you would like to configure a different severity.

Step 4 From the drop-down menu in the upper right, make the severity level change and click **GO**.

Note You can also choose to reset to the default severity levels from the drop-down menu.

Note Severity levels for the existing alarms remain unchanged. Severity level changes only apply to the newly generated alarms.

Viewing MFP Events and Alarms

The 802.11 client devices generate Cisco Management Frame Protection (MFP) elements and validate which of the packets received contained MFP elements. The clients can then report back to the access point it is associated with and identify any anomalies. The most recent access point to report a similar anomaly is identified, and the most recent channel to record a similar event is also identified. If a rogue access point is detected through periodic polling of the controller, its channel number is not displayed. Upon detecting an excessive number of MFP errors from the current access point, a Cisco Compatible Client (version 5) can roam to another access point and report the MFP errors as the reason for roaming.

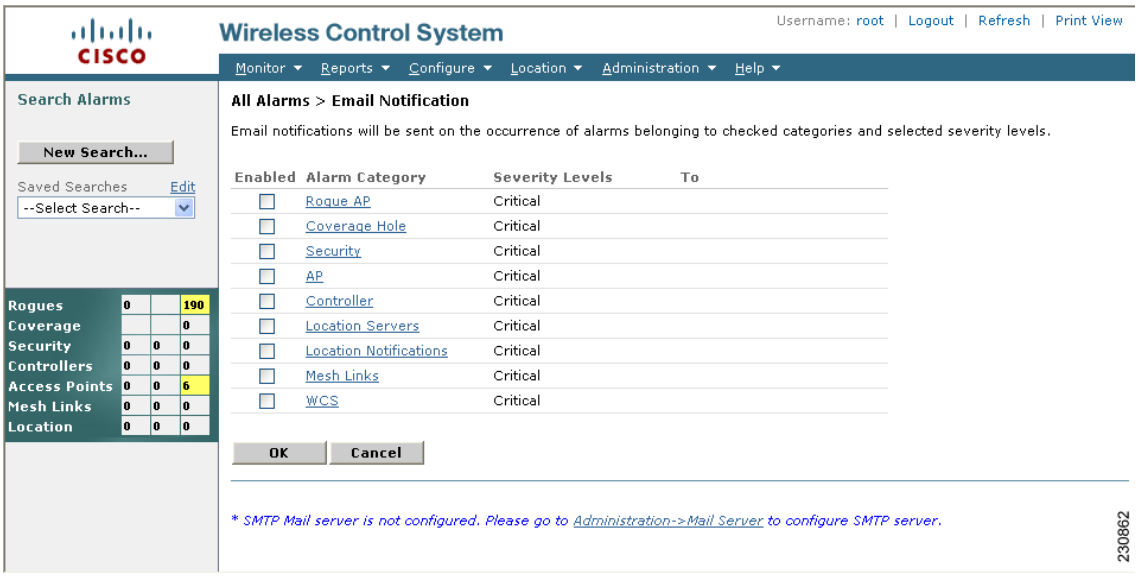
Alarm Emails

The email notification filter window allows you to notify a network operator when an alarm occurs. The severity level is set to critical by default when the alert category is enabled for email notifications, but you can choose a different severity level for the different categories. Email notifications are generated only for the severity levels that are configured. Refer to the "Mail Server" section on page 15-21 for further information.

Step 1 Choose **Monitor > Alarms**.

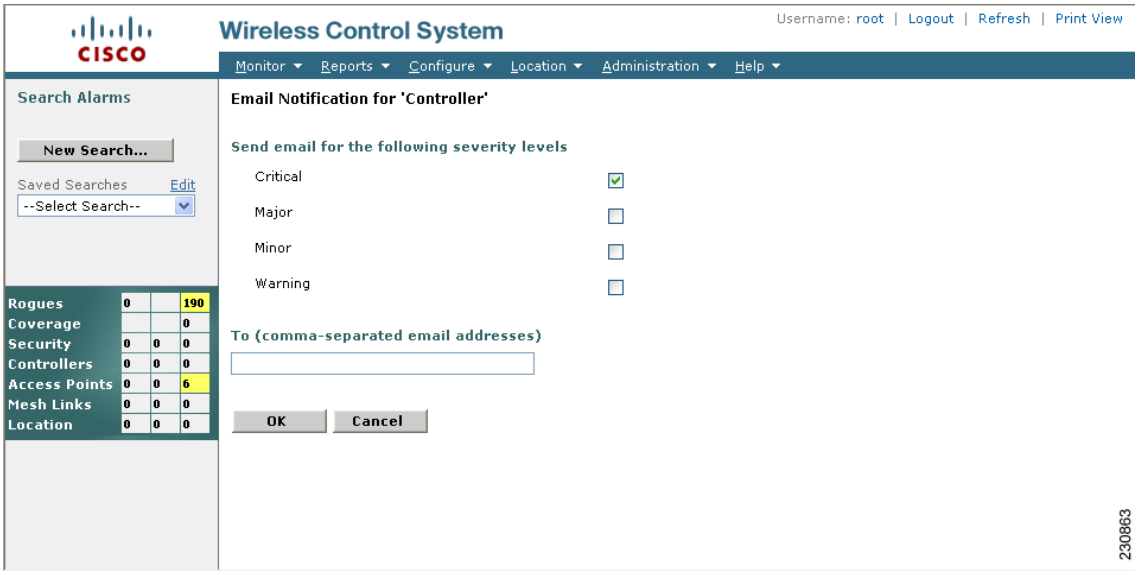
Step 2 From the Select a command drop-down menu, choose **Email Notification** and click **GO**. See the Email Notification window example in Figure 13-7.

Figure 13-7 Email Notification Window



Step 3 Click on a specific alarm category. An alarm category can be all types, access point, controller, mesh links, security, coverage, rogue access points, rogue adhocs, location servers, or location notifications. The detailed email notification window appears (see Figure 13-8).

Figure 13-8 Detailed Email Notification Window



Step 4 Check for which severity levels you want to send emails.

Step 5 Enter the email addresses that should receive the email notification. Insert a comma between email addresses.

Step 6 Click **OK**.

Note If you save the email notification setting for an alarm category, any later changes to the global mail server recipient list do not affect the filter settings. Refer to the "Mail Server" section on page 15-21 to make configuration changes.

Viewing IDS Signature Attacks

You can configure *IDS signatures*, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

When these attacks are detected, the controller is notified, and the client can be shut off if desired. WCS displays summaries and details about IDS/IPS exclusion events and alarms as soon as it is notified by a WLAN controller. The summary and details are available through the Security page with a severity level of critical. When a possible intrusion attack by a wireless client occurs, a message appears which states that the Cisco Intrusion Detection System has recognized a possible intrusion attack and that the client is not allowed access to the network.

To view the listing of all signature attacks that have been found, follow these steps.

Step 1 Choose **Monitor > Events** or **Monitor > Alarms**.

Step 2 Choose **Security** from the Event Category drop-down and click **Search**.

You will see a list of the failure objects, their level of severity, the date and time of the attack, and a descriptive message. For more information on signatures and how to edit, upload, and download them, refer to the "Configuring Intrusion Detection Systems (IDS)" section on page 3-9.

Wireless LAN IDS Event Correlation

If more than one controller hears the same attack, only one alarm is generated for that attack. If multiple rogue access points are generating the same kind of network-wide attack, only one alarm is generated. For example, if a signature attack report is classified as MAC-specific, all attacks of a given kind on the same channel from a given rogue access point are grouped together. In this way, more useful details without duplication are given to WCS administrators whenever more than one controller is managed by WCS.