



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.12

July 10, 2006

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) 2.12.

These release notes detail:

- [New Features, page 2](#)
- [Product Documentation, page 2](#)
- [Documentation Updates, page 4](#)
- [Open and Resolved Caveats, page 5](#)
- [Obtaining Documentation, page 17](#)
- [Documentation Feedback, page 18](#)
- [Cisco Product Security Overview, page 19](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 21](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

New Features

WLSE 2.12 supports:

- Deployment on platforms: 1130, 1130-19, and 1030.
- Cisco IOS Release 12.3(7)JA.
- Cisco 1240 series access points.
- Link role flexibility.
- Device specific configuration.
- User tracking integration with LMS Campus Manager.
- Addition of access point serial number in the Device Details report.
- Conversion of friendly access points to rogue access points.


Note

WLSE 2.12 supports only IOS access points.

Product Documentation

You can access the WLSE online help by clicking the **Help** button in the top right corner of the screen or by selecting an option and then clicking the **Help** button. You can access the user guide from the online help by clicking the **View PDF** button.

The following product documentation is available for WLSE 2.12:

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Installation and Configuration Guide for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE Express. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm • Printed document available by order (part number DOC-17005=)¹
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm • Printed document available by order (part number DOC-=17301)¹

Table 1 **Product Documentation (continued)**

Document Title	Available Formats
<i>Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	Provides regulatory compliance and safety information for the WLSE Express. Available in the following formats: <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	Provides regulatory compliance and safety information for the WLSE. Available in the following formats: <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	Describes WLSE features and provides instructions for using it. Available in the following formats: <ul style="list-style-type: none"> • From the WLSE online help. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i>	Describes the options available and how to upgrade to the WLSE system software to release 2.12. Available in the following formats: <ul style="list-style-type: none"> • From the WLSE online help. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	Contains FAQs and troubleshooting information, and provides a table for all the faults displayed under Faults > Display Faults with explanations and possible actions. Available in the following formats: <ul style="list-style-type: none"> • From the WLSE online help. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	Contains procedures for converting non-IOS access points to IOS access points. Available in the following formats: <ul style="list-style-type: none"> • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm

Table 1 **Product Documentation (continued)**

Document Title	Available Formats
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	Lists the devices supported by WLSE. Available in the following formats: <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine</i>	Lists the documents associated with this release of WLSE. Available in the following formats: <ul style="list-style-type: none"> Printed document included with product. PDF on the WLSE Recovery CD-ROM.
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine Express</i>	Lists the documents associated with this release of WLSE. Available in the following formats: <ul style="list-style-type: none"> Printed document included with product. PDF on the WLSE Recovery CD-ROM.

1. See [Obtaining Documentation](#), page 17.

Documentation Updates

Please note the following additions to the WLSE user documentation.

Addition to the Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express

Product Overview Chapter

“The rack mounting shelf is an optional component. It is not part of standard equipment shipments.”

radiomanager Command in the Command Line Interface (CLI) Appendix

“Using the CLI command `radio manager disable` to disable Radio Management, the Radio Mgr and the Sites tabs does not gray-out the WLSE GUI as it should.”

Device Discovery and Management Chapter

In the “Managed Device Limit on the WLSE 1130 Series” section, the first paragraph should read:

- “The WLSE 1130 series can manage 2,500 access points and wireless bridges and up to 5,000 radios if you are using network management features only.”
- “If you are using radio management features, the WLSE can manage up to 1,800 access points and 3,600 radios.”
- “When you are only using the network management features (and not the radio management feature), a warning message is displayed each time an access point is added to the Managed folder *after* the initial threshold of 2,500 managed access points is met. A maximum of 2,550 devices can be added to the Managed folder . Device discovery continues after the absolute limit (2,550 access points) is reached, but no additional devices can be placed under management.

**Caution**

If you are also using radio management features, you will not get a warning message when you have exceeded 1,800 access points under management.

Open and Resolved Caveats

Table 2 describes outstanding caveats in WLSE 2.12. Table 3 describes caveats resolved since the previous release.

**Note**

To obtain more information about known caveats, access the Cisco Software bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

WLSE Caveats

Table 2 *Open Caveats*

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	The Client Historical Association report does not have information about the last time a client associated with the access point, the time it disconnected from the access point, the duration of the association, or the association state. Workaround: No known workaround. Note In the current release, only association times of a client are supported. Disassociation time of the client is not available in this release.
CSCec41188	You cannot add an access point-based LEAP server to the WLSE if it is already managed by WLSE.	You cannot add an access point-based LEAP/EAP-FAST server to WLSE if that access point is already being managed by WLSE. The WLSE views it as a duplicate device. Workaround: No known workaround.
CSCef90440	A database exception occurs when creating jobs in multiple WLSE sessions.	When you try to create WLSE configuration templates in two separate browser windows simultaneously, one configuration template does not get saved. Workaround: Create templates in a single browser window, one at a time.

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCeg43747	Unable to set EAP-FAST credential-lifetime using quotes.	<p>If you set the EAP-FAST credential lifetime value using double quotes (“”) from the CLI on a WLSE 1030, the following command fails:</p> <pre>aaa-server eap-fast credential-lifetime "8 days"</pre> <p>Workaround: Use the lifetime <i>forever</i> or set credential lifetime using the WLSE GUI. Resolved in release 2.13.</p>
CSCeh06754	Radio Monitoring is not enabled after rebooting a 350 access point.	<p>After rebooting a 350 access point, if you enter <i>show wlccp ap rm</i>, Radio Monitoring is not enabled on the access point even though it is enabled from WLSE.</p> <p>Workaround: Re-enable Radio Manager from WLSE.</p>
CSCeh77651	The configured Web Timeout value is not effective.	<p>If you select Admin > Appliance > TIME/NTP/NAME/WEBTIMEOUT and set the Web Timeout value to 300 seconds, the client browser session does not time out after 5 minutes even though you configured it to do so.</p> <p>Workaround: No known workaround.</p>
CSCsa60720	Location Manager loads with a previous version of jar file.	<p>Workaround: Close all instances of your browser to clear the Java cache. Then re-launch your browser and re-launch Location Manager.</p>
CSCsa75699	The installation wizard does not compare the WLSM version number.	<p>Step 4 of the installation wizard displays the software version numbers for access points and WLSM. If you select Compare known devices version, you get a list of access points that meet the recommended version requirement, but the list does not include WLSM. In addition, the recommended version numbers for WLSM are not accurate.</p> <p>Workaround: No known workaround. Resolved in release 2.13.</p>
CSCsa79506	If a switch has multiple IP addresses, port suppression may fail.	<p>If a switch has multiple IP addresses, port suppression might fail. In order for a switchport to be suppressed, the switch must be in the <i>Managed</i> state. If a switch has multiple IP addresses, WLSE stores only one IP address. If WLSE discovers the rogue on a different VLAN on the same switch with a different IP address (other than the one stored in WLSE), WLSE does not suppress the port because this IP address is not in the database.</p> <p>Workaround: Manually suppress the switchport from the Rogue Details screen.</p>

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCsa86661	RM Scan job runs and logs are not preserved after upgrade.	<p>Radio scan job logs are not visible for historical runs when upgrading from releases 2.9 or 2.9.1a to release 2.12.</p> <p>The job run and job log is not used for any Radio Management computation. The details help to determine when the job ran and if any errors occurred. The data that is lost does not impact any RM functionality run on WLSE 2.11 after an upgrade/restore.</p> <p>Workaround: No known workaround.</p>
CSCsa93652	Backup data fails occasionally due to database locks.	<p>The backup function occasionally does not work.</p> <p>Workaround:</p> <p>Stop the services by entering</p> <pre>services stop</pre> <pre>services status</pre> <p>Make sure the database is no longer running, and then restart the services by entering</p> <pre>services start</pre> <p>If the services do not restart after entering these commands, reboot the WLSE.</p> <p>After restarting the WLSE, log in to the WLSE and select Admin > Appliance > DIAGNOSTICS > Processes.</p> <p>Check WirelessSvcMgr and click Stop.</p> <p>Check WLSEjobvm and click Stop.</p> <p>Check WLSEFaults and click Stop.</p> <p>Make sure the processes actually stop; the green arrow pointing up should change to a red arrow pointing down.</p> <p>After the processes have been stopped, perform the backup.</p>

Table 2 **Open Caveats (continued)**

Bug ID	Summary	Explanation
CSCsa99224	The VM might crash in rare conditions.	<p>In rare conditions, the Tomcat or WLSEFaults virtual machine (VM) might crash. If any of the VMs crash in a redundancy environment, the standby WLSE takes over and becomes the Active WLSE and the system recovers. If the Tomcat VM crashes in a standalone environment, the WLSE GUI does not come up and the daemon manager tries to recover and restarts the services automatically. If the WLSEFault VM crashes in a standalone environment, a red ticker scrolls in the window displaying the message “WLSEFault process is down.” In some cases, the daemon manager does not know that the VM crashed and the process status still shows as “running”. If this happens, the system does not recover automatically.</p> <p>Workaround: Reboot the WLSE. Resolved in release 2.13.</p>
CSCsb25230	Sometimes disabling redundancy via the GUI on an active WLSE causes the database services to stop on the standby WLSE.	<p>If you use the GUI to disable redundancy on an active WLSE, the database services might stop on the standby WLSE. If this occurs, you see the “User role empty” message when you try to log in to the GUI of the standby WLSE.</p> <p>Workaround: Restart the database services on the standby WLSE by entering the following CLI commands:</p> <pre>services stop services start</pre> <p>Resolved in release 2.13.</p>
CSCsb28196	Exception occurs in tomcat.log file when tracing fails for a friendly access point.	<p>When you try to trace a friendly rogue access point that has no Client associated with it, the tracing fails to find the switch port and a nullpointer exception appears in the tomcat.log file.</p> <p>Workaround: No known workaround.</p>
CSCsb28236	Disabling rogue access point detection disables friendly-to-rogue reclassification.	<p>When you enable rogue detection, friendly-to-rogue and rogue port suppression should be disabled in the WLSE GUI for network-wide settings.</p> <p>Workaround: No known workaround.</p>

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCsb37387	WLSE time and date is not synchronizing with NTP server time.	<p>If you set the WLSE time or date to future date or time before you configure the NTP settings, WLSE does not synchronize with the NTP server date/time. However, if you set the date/time to a past date, WLSE does synchronize to the current date/time.</p> <p>Workaround: Use the CLI command to reset the clock to a past date and WLSE will synchronize with the NTP server. Resolved in release 2.13.</p>
CSCsb60195	Wizard Compare Known Devices Version cannot detect 350.	<p>If you select Wizard > Software, and click Compare Known Devices Version, the table does not display access point 350 when operating with release 12.3(7)JA.</p> <p>Workaround: No known workaround. Resolved in release 2.13.</p>
CSCsb65071	An SNMP timeout occurs during access point radio scan jobs.	<p>In some cases, you might get a “Not SNMP Accessible” error message on some access points during an access point Radio Scan even though the access point is SNMP reachable and the SNMP RW community string provided in WLSE is correct. During the start of the access point Radio Scan or in any of the following 8 power steps, WLSE gives an ERROR message indicating that a particular interface is not SNMP accessible. A corresponding SNMP Timeout exception appears in the swan.log for the same access points.</p> <p>Workaround: Do one of the following:</p> <ul style="list-style-type: none"> • Reduce the number of access points in the AP Radio Scan job and then re-run the job; or, • Create a new radio scan job and include the access points which had SNMP errors, select some neighboring access points (for example, from the same floor, one floor above, or one floor below), and then run the AP Radio Scan job.
CSCsb65711	Deleted and re-discovered devices do not get listed in Radio Monitoring.	<p>After an access point is deleted and then re-discovered, Radio Monitoring is not turned on for that access point.</p> <p>Workaround: Select Radio Mgr > Radio Monitoring, select the access point, and turn on Radio Monitoring.</p>

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCsb65889	Cannot access subtabs other than admin user.	<p>When you upgrade a WLSE from any pre-2.12 WLSE release to 2.12, you cannot access any subtabs in the WLSE GUI. If you log in as admin user, change the authentication module to Tacacs+, create a user with system admin roles, change the authentication module back to <i>local</i>, log out and log back in as the just-created user, click on any main tab (for example, Devices or Configure), and then click on any sub tab (for example, Discover or Group management).</p> <p>Workaround: On the active WLSE HA appliance, login as admin, go to <code>http://<wlse-ip>/debug/dbupdate.jsp</code> and follow these steps:</p> <ul style="list-style-type: none"> • Delete from <code>hsa_rolecodes</code> where <code>roleid=0</code> • Delete from <code>hsa_rolecodes</code> where <code>roleid=1</code> • Delete from <code>hsa_rolecodes</code> where <code>roleid=2</code> • Delete from <code>hsa_rolecodes</code> where <code>roleid=3</code> • Issue the following CLI commands on the HA standby box to prevent the standby from becoming active: <pre>services stop</pre> • Issue the following CLI commands on the active HA box: <pre>services stop services start</pre> • Issue the following CLI commands on the standby HA box: <pre>services start</pre>
CSCsb69261	The 802.11a maximum power is not displayed correctly unless native power is enabled.	<p>The 802.11a radio maximum transmit power for the UNII-2 (52-64) and UNII-3 (149-161) channels is incorrectly displayed as 30mW in the Location Manager GUI.</p> <p>Workaround: Enable <i>dot11 extension power native</i> on the 802.11a radio interface by entering the following configuration commands:</p> <pre>ap(config)# int d1 ap(config-if)# dot11 extension power native</pre>

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCsb70367	Location Manager floors do not get loaded after upgrading from WLSE 2.9 to WLSE 2.12.	After you upgrade from WLSE 2.9 to WLSE 2.12, the Location Manager window launches, but it gets stuck and displays the following message: Loading All Locations. Workaround: Reboot WLSE.
CSCsb70419	BR1310 crashes at the start of an AP Radio Scan job.	When you select a BR1310 to be included in an AP Radio Scan, the BR1310 might not be included in the AP Radio Scan. Workaround: No known workaround.
CSCsb72331	Fault notification email priority setting is not preserved after an upgrade.	After upgrading from WLSE 2.9 or 2.9.1a to WLSE 2.12, the fault notification email priority settings (for example, P1, P2, etc.) that you previously configured are not preserved in the upgraded WLSE 2.12. Workaround: No known workaround.
CSCsb73871	WLSM-WDS does not get discovered after being deleted.	After you delete WLSM-WDS from WLSE, subsequent manual discovery and auto-discovery of WLSM-WDS fails. Workaround: Reboot WLSE or stop and then start services.
CSCsb82715	Redundancy upgrade does not work if admin password changes.	If you change the admin password on one WLSE in a redundant environment while an upgrade to 2.12 is in progress, the upgrade will fail. Workaround: Do not change the admin password on either WLSE during the upgrade. Resolved in release 2.13.
CSCsb95162	Windows Domain Auth Server configuration is lost during upgrade.	When you upgrade a WLSE 1030 from WLSE 2.11 to WLSE 2.12, all data on the Windows Domain Authorization Server page, including host name, port, default domain, default AAA user group, and AAA user groups to windows groups attributes, is lost. Workaround: Re-enter the data. Resolved in release 2.13.

Table 2 Open Caveats (continued)

Bug ID	Summary	Explanation
CSCsc39117	Upgrading to WLSE 2.12 without adequate space may cause you to lose the database.	After upgrading to WLSE 2.12, the database does not start, but the web GUI does start and attempts to log in. You are not able to log in to WLSE successfully and a message appears in the upper right corner of the screen indicating the database did not respond correctly. Workaround: Always back up your database before performing a WLSE upgrade. If the upgrade fails, install WLSE from the recovery CD and restore your database. Resolved in release 2.13.
CSCse40868	When you try to access Real Time Graphs or Location Manager WLSE features, a warning message appears indicating that the Verisign certificate has or will be expiring.	Workaround: There are two workarounds for this outstanding caveat: (1) Click OK in the warning dialog box to continue working with the application -or- (2) Upgrade to WLSE release 2.13 or greater in which the caveat is resolved. Please contact technical support for recommended upgrade path.

Table 3 Resolved Caveats

Bug ID	Summary	Explanation
CSCeh36880	In the prior release, a RPG progress bar showing completion percentage (%) was not available often making the user wonder if the process was hanging.	The radio parameter generation function in WLSE now displays a percentage completion (for example, 10% complete) in the progress bar to indicate that it is running and not hanging. In the past, there was only a progress bar which often gave the false impression that RPG was hung because it could take a very long time to complete the calculations.
CSCeh39607	In the prior release, you could not disable fault polling on WEP Encryption per VLAN fault.	After you enabled the fault polling on the <i>WEP Encryption per VLAN</i> fault, you could not subsequently disable fault polling on the fault due to an error message that was generated.
CSCeh60102	In the prior release, rogue access point fault descriptions before and after an upgrade were different.	During a 2.9.1a to 2.11 upgrade, the description for rogue access point faults changed: Before: "Device is rogue access point". After: "Device state is rogue access point".

Table 3 **Resolved Caveats (continued)**

Bug ID	Summary	Explanation
CSCeh79045	In the prior release, after upgrading to WLSE 2.11, devices such as 1410 bridges, access point 1200s, and 350s showed this fault: Inconsistent states appeared in query “interface.radio.config.”	To resolve inconsistent configurations, several possibilities existed: <ul style="list-style-type: none"> • It was possible that the most recent Inventory failed for the device. Re-running inventory often cleared the condition. • If the configuration value being contested was user-editable, you corrected the problem using the WLSE templates, the AP/BR GUI, or the AP/BR CLI. • If the configuration value being contested was not user-editable, this it was probably an IOS error. You had to upgrade the affected AP/BR to the most recent IOS release.
CSCeh91256	In the prior release, the configuration job did not notify user that BR1310 did not support WDS.	No previously known workaround. It is resolved in the current release.
CSCei04672	In the prior release, exporting devices to CiscoWorks LMS 2.5 failed.	You could not export devices to CiscoWorks LMS 2.5. When you tried to export devices, you got the following error message: Could not connect to CiscoWorks Server.
CSCsa45830	In the prior release, an access point was shown in Monitor mode after Scanner mode was disabled and the inventory was done.	If an access point was converted from Scanner mode to any non-Scanner mode while Frame Monitoring was still requested from that access point, a <i>no Fault</i> was generated to warn the administrator of the erroneous network configuration.
CSCsa48733	In the prior release, selecting a building from the device tree selected nothing.	When creating a Radio Manager job such as an AP Scan, if you selected the building in which the access points resided as the <i>selected devices</i> , no devices were selected when the job was run. Devices were only selected when the floor or an explicit access point was selected. This occurred during AP Radio Scan, Assisted Configuration, and Radio Monitoring.
CSCsa63479	In the prior release, after logging in, the WLSE GUI got stuck on the Loading... screen.	Because the tomcat process did not attempt to restart, when you logged into the WLSE, the GUI got stuck on the <i>Loading ...</i> screen indefinitely.
CSCsa67792	In the prior release, backup schedule was not synchronized after a switchover.	The backup schedule did not synchronize after a switchover.

Table 3 **Resolved Caveats (continued)**

Bug ID	Summary	Explanation
CSCsa67922	In the prior release, you were unable to import MAC addresses from Japanese Solaris files.	In Japanese Solaris clients, the MAC address list could not be imported into the advanced Discover options. The problem did not occur in Windows client.
CSCsa68203	In the prior release, RPG parameters were not applied when they were scheduled using XML.	The RPG jobs were created using XML would execute, but the results would not apply. This only happened when RPG Jobs were created using XML.
CSCsa68758	In the prior release, there was a need for an error message to show an incorrect WDS setting.	There was no error message if you entered the incorrect WDS setting.
CSCsa68778	In the prior release, WLSE switchover time was not updated on consecutive switchovers.	WLSE Switchover time was not updated on consecutive switch-overs.
CSCsa68827	In the prior release, Fault Profile Summary showed AssociationErrorRate for Authentication	Workaround involved creating a profile under Faults > Manage Fault Settings that included Authentication Error Rate (available under Access Point/Bridge Thresholds > Radio 802.11a Thresholds). In the Summary page, this displayed as <i>Association ErrorRate</i> .
CSCsa71449	In the prior release, MIB walk on appliance returned the wrong values when the services stopped.	MIB walk on <i>chaRedundancyState</i> returned as <i>active</i> even after entering the services stop command on the active WLSE.
CSCsa78453	In the prior release, WLSE generated the PSPF disabled per radio interface fault when PSPF was configured per VLAN.	When PSPF was configured per VLAN on an access point, WLSE polled a different MIB object (<i>cd11IfVlanPsPacketForwardEnable</i>). WLSE did not take into account that PSPF was enabled per VLAN on an access point and still polled the MIB object <i>cd11IfPsPacketForwardEnable</i> , which corresponded to the PSPF configuration per radio interface. Consequently, WLSE erroneously generated a PSPF disabled per radio interface fault for an access point even though the PSPF was enabled per VLAN on that access point.
CSCsa79473	In the prior release, needed to change the maximum transmit (Tx) power level based on the antenna for ETSI.	The recommended transmit power by RPG and Self-Healing would potentially violate ETSI regulatory domain if you used a high gain antenna, although it was not likely.

Table 3 Resolved Caveats (continued)

Bug ID	Summary	Explanation
CSCsa80570	In the prior release, HA machines were in the starting state when the master file had the wrong password.	<p>After the master file was applied, the HA machines were in the <i>starting</i> state and when you logged in, you would only see the Admin tab.</p> <p>This occurred because the master file had an incorrect password for the redundancy settings. If the passwords did not match in the startup configuration file, then HA would not be configured.</p>
CSCsa83869	In the prior release, packet errors did not show up in the trends graph.	The real time reports showed the percentage of packet errors, but in the trends graph the packet error percentage rate appeared as zero.
CSCsa84004	In the prior release, the “Device not found” window appeared even though a rogue location was displayed.	When the user selected View Location in Location Manager from the Rogue Report Details window, the message “device not found” was displayed while Location Manager was being launched (the launching functionality was not affected).
CSCsa84440	In the prior release, Unknown Radio Location did not show probability of less than 30%.	<p>When a rogue was selected for the Unknown Radio Location display, no area in the map was highlighted for the location probability.</p> <p>If the estimated probability was less than 30%, it was not displayed. This was due to the algorithm change in WLSE 2.11 that made values lower than 30% more significant than in prior releases.</p>
CSCsa84786	In the prior release (WLSE 2.11), did not getting authenticated with ACS.	When using the command <code>show wlccp wnm st</code> from the access point, it replied “Authenticated”. It should have replied “security key setup”. Because the security keys were not getting set up, the other RM management options were not working either.
CSCsa92042	In the prior release, friendly-to-rogue access point reclassification happened immediately after the second try, irrespective of the configured no-observation period.	<p>Working as designed.</p> <p>The first time you moved a rogue access point to the friendly list and shut down its radio, after 5 minutes (in this case, this was the configured no-observation period) the access point would be moved to the rogue access point list.</p> <p>The second time you moved the same access point back to the friendly list it would immediately be moved to the rogue access point list.</p>

Table 3 Resolved Caveats (continued)

Bug ID	Summary	Explanation
CSCsa93623	Pre-patch before you upgrade to WLSE 2.11 from WLSE 2.7, 2.7.1, 2.9 and 2.9.1a.	<p>When you upgrade from WLSE 2.7, 2.7.1, 2.9 or 2.9.1a to WLSE 2.11, you could encounter the following problems:</p> <ul style="list-style-type: none"> • Some database tables were not trimmed, which could cause the database tables to grow very large over a period of time. The log file (swan.log/jobvm.log/tomcat.log) showed a transaction log full messages. • Thousands of Unmanaged radios could appear and could be deleted. • Deleted floors were not cleared from some tables, which could cause the upgrade to fail. After upgrading, radio parameter generation, self healing, and auto re-site survey generated runtime errors. <p>To workaroud this problem, you had to install the WLSE-2.x-CSCsa93623 patch before you upgraded to WLSE 2.11 from any of these WLSE releases: 2.7, 2.7.1, 2.9 or 2.9.1a.</p> <p>Running this patch did not correct the root cause, but the patch eliminated the database inconsistency and allowed you to upgrade to WLSE 2.11.</p> <p>Note We strongly recommend that you back up your database after installing the patch and <i>before</i> you upgrade to WLSE 2.11. Delete all old backups as they contain incorrect data.</p> <p>After you install the patch, if you continue to run WLSE 2.7, 2.7.1, 2.9, or 2.9.1, the issues addressed by the patch will recur.</p>
CSCsb02828	In the prior release, default memory utilization needed to be adjusted.	When an access point running Gallium access point firmware was acting as an AP/WDS, a fault was generated at 80% memory utilization. However, this appeared to be normal for Gallium IOS running as AP/WDS.
CSCsb05240	In the prior release, the Reports > Radio Manager > Channel Loading Report remained empty for all access points after a clean reinstall of the WLSE.	If this problem is encountered, select Radio Mgr > Radio Monitoring > Select Options > Enable History Data Collection , then select the Channel Loading Historical Report to display the data.

Table 3 **Resolved Caveats (continued)**

Bug ID	Summary	Explanation
CSCsb05274	In the prior release, Switch Port tracing displayed as failed in the Switch Port Tracing Results log.	Switch Port tracing showed as failed in Switch Port Tracing Results log. However, under WLSE Unknown AP Detail, switch port tracing did not show the correct switch port. There was no workaround, but you could ignore the failure message.
CSCsb05344	In the prior release, if you pushed a template to enable CDP it would work and then subsequent attempts did not work if Device Specific was checked.	The job failed if the Device Specific hostname was empty and the contact field was not empty. To prevent a failure when the contact field was <i>not</i> empty, a value was entered into the hostname field.
CSCsb54491	In the prior release, non-base mac-add BSSIDs displayed in the Rogue list if MBSSID was enabled.	If you had multiple VLANs/SSIDs setup on an access point and then turned on MBSSID, WLSE moved the non-base mac-add BSSIDs into the Rogue list. This happened if the WLSE discovery process ran after the rogue was detected.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- Non-emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.