



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.11

July 18, 2006

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) 2.11.

These release notes detail:

- [“New Features” section on page 2](#)
- [“Product Documentation” section on page 2](#)
- [“Documentation Updates” section on page 5](#)
- [“Open and Resolved Caveats” section on page 5](#)
- [“Obtaining Documentation” section on page 14](#)
- [“Documentation Feedback” section on page 15](#)
- [“Cisco Product Security Overview” section on page 16](#)
- [“Obtaining Technical Assistance” section on page 17](#)
- [“Obtaining Additional Publications and Information” section on page 18](#)



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 2.11 supports:

- Deployment on platforms: 1130-19, 1130, and 1030
- Wizard for ease of deployment on access points
- The IDS feature set, which includes:
 - IDS profile
 - IDS faults
 - IDS summary
 - Excessive Management Frame Detection
 - MIC/Encryption Failures
 - EAPOL Flooding
 - MAC address spoofing
 - Protection failure per client
- Auto Radio Monitoring
- Frame Monitoring
- Support for third-party IDS servers through an XML interface
- DFS
- Radio Management configuration via XML
- Improved Switchport Tracing algorithm
- RSSI based Rogue detection
- Better Rogue/Friendly management
- Faster RPG computation
- Poll and Event-based Self Healing
- Location Manager enhancements
- Fault notification enhancement

Product Documentation

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

The following product documentation is available for the WLSE 2.11:

Table 1 *Product Documentation*

Document Title	Available Formats
<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: <ul style="list-style-type: none"> http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm Printed document available by order (part number DOC-7816778=)¹
<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: <ul style="list-style-type: none"> http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm Printed document available by order (part number DOC-7816779=)¹
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<p>Provides regulatory compliance and safety information for 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: <ul style="list-style-type: none"> http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Provides regulatory compliance and safety information for 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: <ul style="list-style-type: none"> http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes WLSE features and configuration. Available in the following formats:</p> <ul style="list-style-type: none"> From the WLSE online help. PDF on the WLSE Recovery CD-ROM. On Cisco.com: <ul style="list-style-type: none"> http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i>	<p>Describes the options available and how to upgrade to the WLSE system software to release 2.11. Available in the following formats:</p> <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_11/index.htm
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>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:</p> <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_11/index.htm
<i>Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes how to convert non-IOS access points to IOS. Available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	<p>Contains procedures for converting non-IOS access points to IOS access points. Available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Lists the devices supported by WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Lists the documents associated with this release of WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> Printed document included with product. PDF on the WLSE Recovery CD-ROM.

1. See [Obtaining Documentation](#), page 14.

Documentation Updates

The latest version of the online help and/or User Guide for the CiscoWorks Wireless LAN Solution Engine does not include additions and corrections to the following sections:

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

Product Overview

In this chapter, the rack mounting shelf should be listed as an optional component and not as part of the equipment included in the package.

Configuration File Reference

In this appendix, the Example .XML File section should contain the following text:

```
<ApplianceSettings sshProtocol="SSH1_SSH2" webTimeoutInSeconds="1800"
httpServerPort="1741" telnetEnabled="YES"/>
<CLIBlock>
  <CLI command="username admin password blender privilege 15"/>
  <CLI command="auth cli radius secret 192.168.2.131 192.168.2.132"/>
  <CLI command="http-server port 1741"/>
  <CLI command="auth http radius secret 192.168.2.131 192.168.2.132"/>
</CLIBlock>
  <SplashScreenMessage enabled="YES" message="*****Welcome to the NEW
mini-WLSE*****"/>
</Administration>
<APLocations>
```

Deployment Wizard

In the “Setting Up the WDS” section, the example given for the subnet address in Step 6 is incorrect. The subnet address in the example is 172.10.10.0/255.255.255.0. The correct format is 172.10.10.0/24.

In the “Deploying the Configuration” section, the Subnet field is incorrect. The following note should be removed: “You can assign only one subnet per configuration.”

Open and Resolved Caveats

Table 2 describes problems known to exist in this release. Table 3 describes problems resolved since the last release.



Note

To obtain more information about known problems, 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 in the WLSE

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	<p>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.</p> <p>Workaround: No known workaround.</p> <p>Note In the current release, only association times of a client are supported. Disassociation time of the client is not available in this release.</p>
CSCec41188	You cannot add an access point-based LEAP server to the WLSE if it is already managed by WLSE.	<p>The WLSE views it as a duplicate device.</p> <p>Workaround: No known workaround.</p>
CSCef90440	A database exception occurs when creating jobs in multiple WLSE sessions.	<p>When you try to create WLSE configuration templates in two separate browser windows simultaneously, one configuration template does not get saved.</p> <p>Workaround: Create templates in a single browser window, one at a time.</p>
CSCeg84720	The auto-manage criteria for access point 1210 needs to be modified when moving from release 2.7 to 2.9, and release 2.7 to 2.11.	<p>During an upgrade from release 2.7 to 2.9 and 2.7 to 2.11, The access point 1210 Device Type auto-manage criteria will not work for access point 1210 devices with a single radio after an upgrade from release 2.7 to 2.9 or an upgrade from 2.7 to 2.11. Device Type auto-manage criteria will work with devices with a dual radio.</p> <p>Workaround: Edit the auto-manage criteria for the auto manage template to include both access point 1210 (for dual radio) as well as access point 1210-SR (for single radio) device types.</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>
CSCeh36880	RPG progress bar should show total percentage (%) completed in the progress bar.	<p>Currently, there is only a progress bar which often gives the false impression that RPG is hung because it can take a very long time to complete the calculations.</p> <p>Workaround: No known workaround. Resolved in release 2.12.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCeh39607	Cannot disable fault polling on WEP Encryption per VLAN fault.	After you enable the fault polling on the <i>WEP Encryption per VLAN</i> fault, you cannot subsequently disable fault polling on this particular fault due to an error message that is generated. Workaround: No known workaround. Resolved in release 2.12.
CSCeh60102	Rogue AP Fault description before/after upgrade is incorrect.	During a 2.9.1 to 2.11 upgrade, the description for rogue access point faults changes: Before: "Device is rogue access point". After: "Device state is rogue access point". Workaround: No workaround required. Issue resolved in release 2.12.
CSCei04672	Exporting devices to CiscoWorks LMS 2.5 fails.	You cannot export devices to CiscoWorks LMA 2.5. When you try to export devices, you get the following error message: <code>Could not connect to CiscoWorks Server.</code> Workaround: No known workaround. Resolved in release 2.12.
CSCsa35554	Weekly and monthly data aggregation does not happen at the beginning of the week/month.	The first weekly/monthly aggregation does not start at the beginning of the week/month. The first aggregation might happen earlier than the beginning of the week/month. After the first weekly/monthly aggregation, all subsequent weekly/monthly aggregation occurs every 7 days for weekly or every 30 days for monthly aggregation from the first time the aggregation occurred. Workaround: No known workaround.
CSCsa45830	An access point is shown in Monitor mode after Scanner mode is disabled and inventory is done.	If an access point is converted from Scanner mode to any non-Scanner mode while Frame Monitoring is still requested from that access point, no Fault is generated to warn the administrator of this erroneous network configuration. Workaround: Place the access point back into Scanner mode or remove it from the Frame Monitoring list. Resolved in release 2.12.
CSCsa48733	Selecting a building from the device tree selects nothing.	When creating a Radio Manager job such as an AP Scan, if you select the building in which the access points reside as the <i>selected devices</i> , no devices are selected when the job is run. Devices are selected when the floor or an explicit access point is selected only. This occurs in AP Radio Scan, Assisted Configuration, and Radio Monitoring. Workaround: Select the explicit access points in the Select Devices step for Assisted Configuration and Radio Monitoring. Resolved in release 2.12.

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa57270	Access point 350 EMF does not always start when enabled on WLSE.	When WDS reboots, 350 access points might not start Excessive Management Frame (EMF) detection. Workaround: Perform one of these actions: <ul style="list-style-type: none"> • Locate the IDS profile where the device belongs and reapply EMF settings. • Remove the device and then add it back to the Radio Monitoring list to enable EMF.
CSCsa63479	After logging in, the WLSE GUI gets stuck on the Loading... window.	Because the tomcat process does not attempt to re-start, when you log in to the WLSE, the GUI gets stuck on the <i>Loading ...</i> window indefinitely. Workaround: Ensure the gateway is up, and reboot the WLSE. Issue resolved in release 2.12.
CSCsa67792	Backup schedule is not synchronized after a switchover.	The backup schedule does not synchronize after a switchover. Workaround: Set the backup schedules on both WLSE systems before enabling HA. The backup will then run from the active server when HA is enabled. Resolved in release 2.12.
CSCsa67922	Unable to import MAC address from file in Solaris.	In Japanese Solaris clients, the MAC address list can not be imported into the advanced Discover options. The problem doesn't occur in Windows client. Workaround: No known workaround. Resolved in release 2.12.
CSCsa68100	HA related faults are not generated when the standby becomes active.	When the Standby WLSE becomes the active WLSE, it fails to generate the corresponding HA (High Availability) related fault. However, the active WLSE can still generate all other non-HA related faults on the access points, switches, and routers. Workaround: No known workaround.
CSCsa68203	RPG parameters are not applied when they are scheduled using XML.	The RPG jobs that are created using XML are being executed, but the results are not applied. This only happens when RPG Jobs are created using XML. Workaround: Use MOM to schedule the jobs. Resolved in 2.12.

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa68758	Wizard: Need to add an error message for incorrect an WDS setting.	<p>There is no error message if you enter the incorrect WDS setting.</p> <p>Workaround: Make sure you enter the WDS MAC address and that the managed subnet is in the proper format, for example, <i>000b5f210426 192.168.3.0/24</i> where the first number is the WDS MAC address and the second number is the managed subnet address with a slash and the number of bits in the netmask. The example shows managed subnet of 192.168.3.0 with the number of bits in the netmask as 24.</p>
CSCsa68778	WLSE switchover time is not updated on consecutive switchovers.	<p>WLSE Switchover time is not updated on consecutive switch-overs.</p> <p>Workaround: No known workaround. Resolved in release 2.12.</p>
CSCsa71449	MIB walk on appliance returns the wrong values when the services stop.	<p>MIB walk on <i>chaRedundancyState</i> returns as <i>active</i> even after issuing the services stop command on the active WLSE.</p> <p>Workaround: Shut down the WLSE in a different way rather than issuing the services stop command. Resolved in release 2.1.2.</p>
CSCsa76310	Need to run Inventory after WLSE upgrade/restore from earlier release.	<p>After the upgrade/restore of WLSE from 2.7, 2.7.1, 2.9, or 2.9.1a to 2.11, all managed access points might not participate in Radio Management operations. Managed access points do show up in the HTML device selection lists, but they do not show up on the floors of Location Manager.</p> <p>Workaround: Manually start an inventory job on all managed devices after the upgrade is completed. Then you should verify that all the access points show up in Location Manager.</p>
CSCsa79473	Need to change the maximum transmit (Tx) power level based on the antenna for ETSI.	<p>The recommended transmit power by RPG and Self-Healing might potentially violate ETSI regulatory domain if you are using a high gain antenna, although it is not likely.</p> <p>Workaround: Set the maximum power in the RPG Constraints/Goals section as one of the following:</p> <ul style="list-style-type: none"> For 2.4 GHz: 25 mw (antenna gain 5.2 - 6 dB), 13 mw (antenna gain 6.1 - 9 dB), 8 mw (antenna gain 9.1 - 10 dB). For 5 GHz: 32 mw (antenna gain 6 - 7 dB), 13 mw (antenna gain 7.1 - 9.5 dB).

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
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 window.</p>
CSCsa78453	WLSE generates the PSPF disabled per radio interface fault when PSPF is configured per VLAN.	<p>When PSPF is configured per VLAN on an access point, WLSE needs to poll a different MIB object (<i>cd11IfVlanPsPacketForwardEnable</i>). WLSE does not take into account that PSPF is enabled per VLAN on an access point and still polls the MIB object <i>cd11IfPsPacketForwardEnable</i>, which corresponds to the PSPF configuration per radio interface. Consequently, WLSE erroneously generates a PSPF disabled per radio interface fault for an access point even though the PSPF is enabled per VLAN on that access point.</p> <p>Workaround: No known workaround.</p>
CSCsa80570	HA machines are in the starting state when the master file has the wrong password.	<p>After the master file is applied, the HA machines are in the <i>starting</i> state and when you log in, you see the Admin tab only.</p> <p>This occurs because the master file has an incorrect password for the redundancy settings. If the passwords do not match in the startup configuration file, then HA will not be configured.</p> <p>Workaround: Enable Redundancy again from the WLSE. Resolved in release 2.12.</p>
CSCsa83428	Devices do not appear in Location Manager if they are unreachable during an upgrade.	<p>After upgrading from WLSE 2.7 to WLSE 2.11, access points that appeared in the WLSE 2.7 Location Manager floor map do not show up in the WLSE 2.11 Location Manager. This happens to devices that are unreachable during the upgrade or devices that have a validation fault against them.</p> <p>Workaround: Before you upgrade, make sure there are no unreachable or validation faults against the devices.</p>
CSCsa83869	Packet errors do not show up in the trends graph.	<p>The real time reports show the percentage of packet errors, but in the trends graph the packet error percentage rate is zero.</p> <p>Workaround: View the packet error rate in the real time reports.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa84004	“Device not found” window appears even though rogue location is displayed.	<p>When the user selects View Location in Location Manager from the Rogue Report Details window, the message “device not found” is displayed while Location Manager is being launched (the launching functionality is not affected).</p> <p>Workaround: Ignore or close the window containing the “device not found” message. Resolved in release 2.12.</p>
CSCsa84440	Unknown Radio Location does not show probability of less than 30%.	<p>When a rogue is selected for the Unknown Radio Location display, no area in the map is highlighted for the location probability.</p> <p>If the estimated probability is less than 30%, it will not be displayed. This is due to the algorithm change in WLSE 2.11 that makes values lower than 30% more significant than in prior releases.</p> <p>Workaround: No known workaround. Resolved in release 2.12.</p>
CSCsa86661	RM Scan job runs and logs not preserved after upgrade.	<p>Radio scan job logs are not visible for historical runs when upgraded from release 2.7, 2.7.1, 2.9, or 2.9.1a to 2.11.</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>

Table 2 Open Caveats in the WLSE (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 might encounter the following problems:</p> <ul style="list-style-type: none"> • Some database tables are not trimmed, which might cause the database tables to grow very large over a period of time. The log file (swan.log/jobvm.log/tomcat.log) shows transaction log full messages. • Thousands of Unmanaged radios might appear and cannot be deleted. • Deleted floors are not cleared from some tables, which might cause the upgrade to fail. After upgrading, radio parameter generation, self healing, and auto re-site survey generate runtime errors. <p>To workaroud this problem, you must install the WLSE-2.x-CSCsa93623 patch before you upgrade 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 does not correct the root cause, but the patch eliminates the database inconsistency and allows 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>
CSCsb07984	WLSE fails to import devices from RME 4.0.	<p>You cannot import devices from CiscoWorks RME 4.0 to WLSE 2.11. When you try to import devices, you get an error message in the jobvm.log file.</p> <p>Workaround: No known workaround.</p>
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.	<p>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.</p>

Table 3 Resolved Caveats in the WLSE

Bug ID	Summary	Explanation
CSCed94324	Prior to this release, often a detach/IP address change event was reported after a roam event even when one did not occur.	<p>If you selected Reports > Wireless Clients > Client EAP UserName or MAC Address > Client Historical Association, an IP Address Change event often reported immediately after a roam event, even when no IP address change had occurred for the specified client. In addition, sometimes a Detach From WDS event was reported immediately after a Roam event, even though the specified client had not left the WDS indicated in the previous Roam event.</p> <p>This problem occurred for certain clients that were authenticated using LEAP and were not using the CCKM fast-roaming feature.</p>
CSCeg09569	Prior to this release, the template GUI did not check for incompatible encryption types.	<p>When you configured Authenticated Key Management options as <i>WPA</i> or <i>CCKM</i> from Configure > Templates > Security > SSID 802.11b/g/a, and you did not configure the Encryption Modes option as <i>Cipher</i> under Configure > Templates > Security > WEP 802.11b/g/a, the device reported the following error:</p> <p>Dot11Radio0 Error: Encryption mode cipher is not configured.</p>
CSCeg17204	Prior to this release, an incorrect CLI command was generated when the AAA group name included a space character.	<p>When the AAA group server name contained spaces, for example <i>aaa group server radius rad_eap</i> instead of <i>rad_eap</i>, the following incorrect CLI command is generated:</p> <pre>aaa group server radius aaa group server radius rad_eap</pre> <p>The correct group name “rad_eap” was required to generate following CLI command:</p> <pre>aaa group server radius rad_eap</pre>
CSCeg46075	Prior to this release, an incorrect IOS release was listed for 2.9 RM operations.	Radio Management operations in WLSE required the access points to be running the latest 12.3(2)JA IOS release. Older releases, including 12.2(15)JA, did not work.
CSCsa35793	Prior to this release, after entering the CLI command no http-server accept <ip> <mask> , WLSE redundancy failed.	When you entered the CLI commands http-server accept <ip> <mask> and no http-server accept <ip> <mask> and then configured the server as a <i>Redundancy Standby</i> server, the redundancy status on the server would get stuck in <i>starting</i> mode and could not connect via HTTP (however, it could be connected using HTTPS). The redundancy page showed the server as a <i>Standby</i> server, but with the <i>Manage Redundancy</i> option (which should only have displayed if the server was in <i>Active</i> server mode).

Table 3 Resolved Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa39732	Prior to this release, switches selected by a cursor would display radio port information.	If you selected Reports > Current > Device Type > Switches and pointed your cursor at the switches in that group, radio port information was displayed. The switches did not have radio ports and this information should not have displayed.
CSCsa39738	Prior to this release, the VxWorks template for dot11CurrentRxAntenna.2 generated errors.	When you created a VxWorks template and went to the 11b Radio Hardware page and selected Receive Antenna as Diversity, and saved the template, the following error message appeared: Following key-value(s), in the current configuration template, are not supported: Key: dot11CurrentRxAntenna.2 Value: diversity
CSCsa39854	Prior to this release, WLSE deleted lines with “!” in the template.	If you had an exclamation point (!) in the IOS command line interface (for example, <code>snmp-server community pub!!lic RO</code>), WLSE deleted the lines with the “!” character when importing the configuration or when the archived configuration file containing the “!” character was exported as a configuration template.
CSCsa41193	Prior to this release, the View Archive page showed access points running IOS as Non-IOS and attempts to export to a template failed when a (#) pound sign was incorporated in a CLI command.	If you had a pound sign (#) in the IOS configuration, for example, <code>snmp-server community pub#lic ro</code> , and you selected Configure > Archives > View Archive and selected Export to Template, the job failed and you got an error message. The View Archive window displayed the type as “non- IOS” even for access points that were running IOS images.
CSCsa42074	Prior to this release, TACACS + server configurations could not be saved by WLSE.	When you tried to save your TACACS+ server configuration, WLSE gave you the following error: Error processing configuration / No valid device versions supported.

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.

