



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.9.1a

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) Release 2.9.1a.



Note

We recommend that you download and view the 2.9.1a Readme for installation and other important information. The Readme can be found at the following URL: <http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>.

These release notes provide:

- [Product Documentation, page 2](#)
- [Known and Resolved Problems, page 4](#)
- [Obtaining Documentation, page 15](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 18](#)

CISCO SYSTEMS



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

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, Release 2.9:

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm
<i>Converting Access Points to IOS</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm
<i>Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<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_9/index.htm
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<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_9/index.htm

Table 1 Product Documentation (Continued)

Document Title	Available Formats
<i>Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<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_9/index.htm
<i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i>	<p>On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</p>
Context-sensitive online help	Select an option from the WLSE navigation tree, then click Help .
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<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_9/index.htm

Known and Resolved Problems

- [Known Problems, page 4](#) describes problems known to exist in this release.
- [Resolved Problems, page 7](#) describes problems solved 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.)

Known Problems

Table 2 *Known Problems 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 AP, the time it disconnected from the AP, the duration of the association, or the association state.</p> <p>There is no workaround for this problem.</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 AP-based LEAP server to the WLSE if it is already a managed by WLSE.	<p>You cannot add an AP-based LEAP/EAP-FAST server to WLSE if that AP is already being managed by WLSE. The WLSE views it as a duplicate device.</p> <p>There is no workaround for this problem.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCed94324	Detach/IP Address Change events during Roam event stress-2gclient.	<p>If you select Reports > Wireless Clients > Client EAP UserName or MAC Address > Client Historical Association, sometimes an IP Address Change event is reported immediately after a Roam event, even though no IP address change has occurred for the specified client. In addition, sometimes a Detach From WDS event is reported immediately after a Roam event, even though the specified client has not left the WDS indicated in the previous Roam event.</p> <p>This problem occurs for certain clients that are authenticated using LEAP and are not using the CCKM fast-roaming feature.</p> <p>To work around this problem, ignore the IP Address Change and the Detach From WDS events if they occur immediately after a Roam event.</p>
CSCef90440	Database exception while creating templates 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>To work around this problem, create templates in a single browser window at one time.</p>
CSCsa35554	Weekly and monthly data aggregation does not happen at the beginning of the week/month.	<p>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.</p> <p>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.</p> <p>There is no workaround to this problem.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa39854	WLSE deletes lines with “!” in the template.	<p>If you have an exclamation point (!) in the IOS command line interface (for example, <code>snmp-server community pub!lic RO</code>), WLSE deletes the lines with the “!” character when importing the configuration or when the archived configuration file containing the “!” character is exported as a configuration template.</p> <p>To work around this problem, edit the custom command section of the template by manually adding the lines containing the “!” character.</p>
CSCsa41193	Archive shows the type as Non-IOS and exporting the template fails.	<p>If you have a pound sign (#) in the IOS configuration, for example, <code>snmp-server community pub#lic ro</code>, and you select Configure > Archives > View Archive and select Export to Template, the job fails and you get an error message. The View Archive screen shows the type as non- IOS even for APs running IOS images.</p> <p>There is no workaround to this problem.</p>
CSCeg84720	The AP 1210 automanage criteria needs a change from 2.7 to 2.9.	<p>During an upgrade from Release 2.7 to 2.9, the AP 1210 Device Type auto-manage criteria will not work for AP 1210 devices with a single radio.</p> <p>In the WLSE 2.9 release, AP 1210 device type criteria will match with devices with a dual radio only. There is a new criteria defined for AP 1210 devices with single radio AP 1210-SR.</p> <p>To work around this problem, Edit the auto manage criteria for the auto manage template to include both AP 1210 (for dual radio) as well as AP 1210-SR (for single radio) device types.</p>

Resolved Problems

Table 3 Resolved Problems in WLSE

Bug ID	Summary	Explanation
CSCee62677	Device Center shows Red for AP1210 whose faults are cleared.	Under Reports > Device Center, an AP1210 appears red, not green, after the P1 and P2 faults for that device are cleared.
CSCef97944	Cannot select bridge non-root/install mode for 1310 bridge.	When you select Configure > Templates > IOS > Basic Settings > Radio0-802.11B/G, click the radio button and check box for Bridge Non-Root and Install-Mode, and then click on any of the other links, the following popup message appears: Install mode is applicable for Bridge Root and Non-Root modes only.
CSCeg09569	Template GUI does not check for incompatible encryption type.	Under Configure > Templates > Security > SSID 802.11b/g/a, when you enter the Authenticated Key Management options as WPA or CCKM, without configuring the Encryption Modes option as Ciphers under Configure > Templates > Security > WEP 802.11b/g/a., the device reports the following error: Dot11Radio0 Error: Encryption mode cipher is not configured.
CSCeg17204	Incorrect CLI command is generated when AAA group name has space characters.	When the AAA group server name contains spaces, for example “aaa group server radius rad_eap” instead of “rad_eap” the following incorrect CLI command is generated: <code>aaa group server radius aaa group server radius rad_eap</code> The correct group name should be “rad_eap” to generate the following CLI command: <code>aaa group server radius rad_eap</code>
CSCeg46839	WLSE autonegotiating even with speed/duplex hard coded.	The WLSE cannot detect a full duplex setting on the switch port, falls back to a half duplex setting, and causes a duplex mismatch.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCeg55064	Verifier check for AP registration with HSRP WDS needs fix.	<p>Under Location Manager the AP's registration is checked for AP-WDS and non-redundant WLSM-WDS.</p> <p>However, it does not check HSRP for redundant WLSM-WDS correctly.</p>
CSCeg55576	Radio Management will not function when an AP is replaced with a different model but the same IP.	<p>If an AP is replaced with a new AP of a different model, but using the same IP address, the old device (which has a different MAC address than the new one) shows up under "Duplicate IP" devices. If "daemons.log" is opened in WLSE under Admin > Appliance > Status > View Log File, the following exceptions are seen:</p> <pre> java.lang.ClassCastException: com.cisco.swan.co.EthernetInterface at com.cisco.swan.nmif.DeviceRelationManager. processDevice(DeviceRelationManager.java:13 4) at com.cisco.swan.nmif.NmDbApi.refreshDevices (NmDbApi.java:379) at com.cisco.swan.nmif.NmDbApi.refreshDevice(NmDbApi.java:388) at com.cisco.swan.nmif.MsgProcessor.processRef reshMessage(MsgProcessor.java:161) at com.cisco.swan.nmif.MsgProcessor.run(MsgPr ocessor.java:50) </pre>
CSCeg70679	Radio monitoring does not work when a new access point is added to the WLSE.	When new access points are added to the WLSE, radio monitoring does not detect them and will not function.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCeg89231	EAP Username is missing in client reports.	The EAP username column is missing from the client reports.
CSCsa35793	After using the command no http-server accept <ip> <mask> , WLSE redundancy fails.	<p>When you issue the command line interface commands http-server accept <ip> <mask> and no http-server accept <ip> <mask>, then the server will block HTTP access.</p> <p>If the server has redundancy configured, then the server will remain in a starting state indefinitely because the HTTP access is blocked.</p> <p>HTTPS access will still function and the redundancy feature can be disabled.</p>
CSCsa36237	WLSE aborts active TFTP upgrade when per device timeout expires.	<p>When the WLSE tries to push a firmware image to an AP over a WAN connection, sometimes the firmware job fails. This is due to an insufficient default timeout value for “Per device job operation timeout,” which is set to 600 seconds under the Firmware > Advanced Parameters.</p> <p>With the “Per device job operation timeout” value increased to 7200 seconds, there is enough time for a firmware upgrade for each device over a WAN connection.</p>
CSCsa36862	An IOS template with dual radio configuration fails for APs with single radio, such as AP 1210.	An IOS configuration template containing configurations for both radio 11b/g and radio 11a fails when applied to dual radio capable APs such as the 1210 with single radio.
CSCsa36966	Images import for AP350 and AP1200 missing 12.05 link.	The firmware images for version 12.05 are not listed for AP350 and AP1200 devices when you try to import from Cisco.com.
CSCsa37758	Need to find root cause analysis of why /opt is getting 100% full.	The /opt partition in WLSE fills up with database dump files which prevents proper operation of the WLSE.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa38974	QoS policies with WMM generate CLI with DISAB.	When you create a new Services: QoS Policies 802.11b/g template under Configure > Templates > IOS, if DISAB appears in the Transmit Opportunity column, you cannot apply the template to any devices.
CSCsa39508	AAA reports should report meaningful information when no records are returned.	If you do not enable AAA server response time under Faults > Manage Faults the following message is shown for AAA under Reports > Trends: INFO: Graph will be available only after inventory runs twice. The error message needs to provide the steps to correct the problem.
CSCsa39732	Switches, when pointed at, highlight the radio port information.	If you select Reports > Current > Device Type > Switches and point your cursor at the switches in that group, radio port information is displayed. The switches do not have radio ports and this information should not be displayed.
CSCsa39738	A non-IOS template with Receive Antenna as diversity gives error message.	When you create a non-IOS template by selecting the 11b Radio Hardware, and select Receive Antenna as Diversity, then save the template, the following error message appears: Following key-value(s), in the current configuration template, are not supported: Key: dot11CurrentRxAntenna.2 Value: diversity
CSCsa42074	TACACS server configuration is not supported by WLSE	When you try to save your IOS TACACS+ server configuration, the WLSE displays the following error: Error processing configuration / No valid device versions supported.
CSCsa42391	Standby WLSE can take over the VIP address.	When you have redundant WLSEs, and you Telnet or log in using VIP address, you might access the standby rather than the active WLSE.

Table 3 *Resolved Problems in WLSE (Continued)*

Bug ID	Summary	Explanation
CSCsa42474	Image push using SNMP is not successful.	Using an incompatible image naming convention causes the upload to fail and erases the flash. A validation while importing the image from desktop or while editing the image details needs to check if the image name is in the proper format.
CSCsa44285	The 3560 switches are not yet supported in WLSE 2.9.	When these switches are not supported in WLSE, the WLSE does not contain any information about them. Without this, there is no provision in WLSE to indicate which APs are connected to which switch.
CSCsa45411	Lost standby message sent out during data synchronization.	In a redundant operation, where the standby WLSE response is slow during data synchronization, the active WLSE might not get a response in the required time and it will send out a “lost standby” message.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa46081	Self-healing sometimes triggered when no radio has failed.	<p>Self Healing may be triggered on a radio that is in fact operational. Self Healing monitors a radio by using other radios in the same building to validate that the monitored radio is transmitting. Some false healing may occur in dense deployments or those experiencing interference.</p> <p>For self-healing to work satisfactorily, the monitored APs on a floor should have at least two other APs (vouching APs) in the building such that the vouching APs can hear the monitored AP reliably and consistently.</p> <p>If a monitored AP has only one other AP that fluctuates between being able and not able to hear the monitored radio, self healing compensation (and fault) will occur.</p> <p>Either the radio should have at least two radios that can hear its beacons or none. In the case of none then we will monitor the AP via the WDS registration. This issue is when a monitored AP fluctuates between being heard and not being heard. Interference can cause this as well.</p>
CSCsa46147	Redundancy email address cannot contain hyphens.	The email address used to for notifications in a redundant WLSE environment cannot contain a hyphen '-' in the hostname portion of the address.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa46167	With 2 APs reporting about a rogue, the WLSE reports the rogue location incorrectly.	<p>For rogue detection to work properly, the following are critical pre-requisites:</p> <ul style="list-style-type: none"> • All APs must be running software version 12.2(15)JA or later • On a per floor basis, there needs to be an adequate number of APs for Radio Management tasks (in addition to serving wireless clients) • Floor plan information must be accurate <p>When the pre-requisites are not met, the results can be skewed.</p> <p>For example, when only two APs report the existence of a rogue AP, the WLSE incorrectly indicates, with a 90 to 100% certainty, its the rogue's location.</p> <p>When more than two APs report the rogue's presence, the results are more accurate as to the location of the rogue AP.</p>
CSCsa46173	Participating clients have too many additional lines in ad-hoc networks.	<p>When you select Faults > Display Faults, then view the “Ad-hoc network creation detected” fault, a list of participating clients (if available) is shown.</p> <p>One hundred lines are shown when you display this page, even if only 50 participating clients are listed.</p>
CSCsa47230	An AAA server added to the wlse shows up as %hostname%.	After adding an AAA server to the WLSE, it appears as %hostname% in various UI displays in the WLSE (Reports, Devices, etc.).
CSCsa47363	The WLSE is not sending WEP commands to multiple devices.	When a template containing WEP key configuration is uploaded to multiple devices, only one device receives the configuration. However, all the other commands in the template are applied to all the devices.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa48103	No old record deletion from radio management database tables.	The radio management database records are not deleted which could fill the disk with records.
CSCsa52814	WLSE 2.9 email notification may not work after upgrade	Although faults are displayed under Faults > Display Faults, email notifications of those faults may not be sent.
CSCsa53633	Admin Access configuration should be sent last.	When you use the following templates: <ul style="list-style-type: none"> • Configure > Template > Security > Server Manager • Configure > Template > Security > Admin Access the access point becomes inaccessible because the Server Manager configuration overwrites the Admin Access commands.
CSCsa63599	500 Error in Radio Monitor after upgrade to WLSE 2.9.1.	After upgrading to WLSE 2.9.1, a 500 error may occur when you select Radio Manager > Radio Monitoring.

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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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, and logo merchandise. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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 online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- *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>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

