



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.7

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) Release 2.7.



Note

The Sun Java Cryptography Extension (JCE) 1.2.1 used in this release is set to expire at midnight on July 27th, 2005. Key functionality will stop working. Refer to the following field notice, then download and install the recommended patch: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_field_notice09186a00804cf5d3.shtml.

These release notes provide:

- [New Features, page 3](#)
- [Product Documentation, page 3](#)
- [Documentation Updates, page 6](#)
- [Known and Resolved Problems, page 9](#)
- [Obtaining Documentation, page 25](#)
- [Obtaining Technical Assistance, page 26](#)

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.

-
- [Obtaining Additional Publications and Information, page 28](#)

New Features

The WLSE Release 2.7 contains management support for:

- Hardware platforms: BR1300/1400 (Radio Manager functionality is not supported on these platforms.)
- Network management support for the following radios:
 - AP1200/AP1100 802.11 a and 802.11g radios
 - AP1200 dual mode radios 802.11a/802.11b and 802.11a/802.11g
 - BR1300 802.11g radios
- Software support for firmware release 12.2(15)JA
- Self healing APs (Available only on platforms with Radio Manager support.)
- WDS-based client tracking (Available only on platforms with Radio Manager support.)
- Real time reporting
- Location Manager enhancements
- WLSE cold standby redundancy
- Rogue AP switch port suppression
- Scanning only AP (Supported only on AP1100/AP1200.)
- Auto Re-site Survey (Available only on platforms with Radio Manager support.)

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:

Table 1 Product Documentation

Document Title	Description
<p><i>Installation and Configuration Guide for the 1130/1105 CiscoWorks Wireless LAN Solution Engine</i></p>	<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_7/index.htm • Printed document available by order (part number DOC-7816194=)¹
<p><i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i></p>	<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_7/index.htm • Printed document available by order (part number DOC-7816345=)²
<p><i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i></p>	<p>Describes WLSE features and provides instructions for using it. 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: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • Printed document available by order (part number DOC-7816193=)³

Table 1 Product Documentation (Continued)

Document Title	Description
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1130 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 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_7/index.htm
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1130-19 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 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_7/index.htm
<i>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_7/index.htm

Table 1 Product Documentation (Continued)

Document Title	Description
<i>Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine</i>	Describes how to convert non-IOS access points to IOS. 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_7/index.htm
<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_7/index.htm

1. See [Obtaining Documentation, page 25](#).
2. See [Obtaining Documentation, page 25](#).
3. See [Obtaining Documentation, page 25](#).

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:

Wireless LAN Services Module Acronym

The acronym for Wireless LAN Services Module should be WLSM and not WSM.

Required Software for APs with 802.11g Radios

If you are using WLSE to manage APs or bridges with 802.11g radios, the APs must be running Cisco IOS version 12.2.15JA or later. WLSE is unable to push configuration templates to APs with 802.11g radios that are running previous versions.

Disable Pop-Up Blocker

While using WLSE, you should disable pop-up blocking software or add WLSE to the “Allow” list.

What is WDS and Why Do I Need To Use It?

The second sentence in this section should read: The WDS provides control path technologies that must be active on an AP in each AP subnet; a backup WDS can also be defined in each AP subnet.

Specifying the Backup Location

The online help description for the **Clear Log** button in the **Administration > Backup and Restore > Configure** screen is incorrect. The online help description of the **Clear Log** button should say: Click the **Clear Log** button to delete from the View Log File window the backup.log file that was created during the previous backup or restore operation.

Displaying Current Reports

If you select **Reports > Current**, then click **Help**, in the Access Point Reports (IOS) section, the following two reports should be removed because they only apply to non-IOS APs:

- AP Filter Report
- AP Policy Report

Also, the hypertext links for the last two reports (EAP and MAC Failed Authentication Report and Failed Authentication and Login Attempt per AP Report) are incorrect.

Displaying Group Client Report

The description incorrectly describes the policy groups instead of the Group Client Report. The help topic should read: The Group Client Report lists all policy groups configured on each of the non-IOS APs in this group.

Checking Redundancy Settings

In the Redundancy Status Settings table, the description for the Turned Off redundancy status should be “Not configured.”

The description for Minutes Between Sync should be “Synchronization interval. (Data synchronized from the active node to the standby node.)”

Configuring Redundancy

The second paragraph should be replaced by the following text: Subsequent configuration changes can be done on whichever WLSE is in active mode, but the nodes' IP addresses should remain the same as when they were initially configured. If you need to reconfigure the nodes' IP addresses, first turn redundancy off, and then configure the nodes' IP addresses.

Changes in Backup and Restore and Redundancy Status

The documentation should include the following information:

- If redundancy is not enabled, backup and restore are allowed.
- If redundancy is in active mode, backup is allowed, but restore fails and generates an error message asking you to turn off redundancy first.
- When restoring, if the backup is performed when redundancy is in active mode, redundancy is automatically turned off after the restore, and you will need to reenable it.
- If redundancy is in standby mode, neither backup nor restore are allowed. If you are trying to run backup, a message appears asking you to run backup on an active node.

Managing Your WLAN Radio Environment

The Caution note should read AP subnet instead of Layer-2 domain so that the first sentence reads: The WLSE must register with the WDS in each managed AP subnet to receive Radio Manager data.

Getting Started with Radio Manager

The note in Step 2 is incorrect and should not appear in the documentation.

Step 5, part f should read: Verify that the WLSE to WDS Authentication Status column contains the string *KeysSetUpWithWDS* or *Authenticated*.

The last paragraph of Step 6 should read: You can also verify this setting by running the *show wlccp wds ap* command on the primary WDS in enable mode.

Using Scanning-Only APs

Step one in the “Using Scanning-Only APs” section should read:

Use a template-based configuration job to configure one or more APs as scanning-only APs (see “Using IOS Templates”). Follow these guidelines when you create the template:

- Keep the configuration simple. For example, do not configure VLAN/SSID for Scanning-Only APs.
- Do not configure the scanning-only AP as an active/backup WDS (to serve fast roaming traffic).



Note Even though configuring Scanning-Only APs and configuring WDS are independent features, they will contend with each other on the same CPU if both are enabled on the same AP. To make certain that Scanning-Only AP traffic does not affect the real time performance for fast roaming, *do not* configure a Scanning-Only AP to act as a WDS (active or backup) to support fast-roaming clients. However, if the subnet contains only Scanning-Only APs and no regular APs serving fast-roaming clients, you *can* configure one of the Scanning-Only APs to run WDS.

Also in the “Using Scanning-Only APs” section, Step 4 should read:

In a heavy-load environment, APs running in scanning-only mode may face sporadic connection loss and image upgrade failure. To resolve these problems, use the following AP configuration CLI commands to balance CPU time:

```
scheduler interval <100-xxx>
scheduler allocate <3000-xxx> <1000-xxx>
```

Many newer Cisco platforms use the command **scheduler allocate** instead of **scheduler interval**. The scheduler allocate command takes two parameters: a period in microseconds for the system to run with interrupts enabled, and a period in microseconds for the system to run with interrupts masked. Please refer to the IOS documentation for more information about these commands.

Known and Resolved Problems

Table 2 describes problems known to exist in this release. Table 3 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.)

WLSE 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 the 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>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 a LEAP server to the WLSE if it is already a managed access point.	<p>You cannot add an access point that is running the local RADIUS service and is managed as an access point by the WLSE as a LEAP server. The WLSE will view it as a duplicate device.</p> <p>There is no workaround for this problem.</p>
CSCed55402	When you set the WEP Enforced policy under Faults > Manage Faults the faults are not generated correctly.	<p>When the WEP Enforced policy is set for the radio interface of an IOS access point, sometimes the faults may not be generated due to an access point bug (see CSCed39748).</p> <p>There is no workaround for this problem.</p>
CSCed89308	RPG Stop Calculation does not work, only when job is rerun.	<p>If you are rerunning a radio parameter generation job, you cannot stop the parameter calculations once they have begun. Although the window displays “Stopping Calculations,” the process does not stop.</p> <p>If you are running radio parameter generation for the first time, this problem does not appear.</p> <p>There is no workaround for this problem.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCee03323	Rogue PHY type is reported as 11a when it should be 11b.	<p>On cb21ag, pi21ag, and ti21ag client adapters, when a rogue AP client is detected, the rogue report might indicate the rogue is an 11a PHY type when it is an 11b PHY type.</p> <p>There is no workaround for this problem.</p>
CSCee09800	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>These problems occur for certain clients that are authenticated using LEAP and are not using the CCKM fast-roaming feature.</p> <p>To workaround these problem, ignore the IP Address Change and the Detach From WDS events if they occur immediately after a Roam event.</p>
CSCee18557	Unable to include filters in policy groups.	<p>When you deploy policy groups to AP 1200's and AP 350's running VxWorks version 12.0(4), the filters associated with the policy groups cannot be included even though the policy group itself is deployed.</p> <p>There is no workaround for this problem.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCee26055	ACS Login Failed Report produces error message.	<p>When you click the ACS Failed Login Report link to launch the ACS Failed Login Report, an error message appears saying a URL has not been provided for this link.</p> <p>There is no workaround for this problem. You can log in directly to the ACS server and look at the ACS Failed Login Report.</p>
CSCee30813	Self healing results are not visible until inventory runs.	<p>After Self Healing applies changes to supporting APs due to a downed AP, the results of the changes are not visible in WLSE until after an inventory runs.</p> <p>To work around this problem, after receiving a fault for the downed AP, manually run an inventory for all APs on the same floor as the downed AP.</p>
CSCee37875	CCO crypto download changes breaks image import from Cisco.com	<p>When you select Firmware > Images > Import > From Cisco.com, log in with your CCO account, and select any AP image, you get the following error message:</p> <p>Error while selecting or displaying image details. Please log into cisco.com at http://www.cisco.com/cgi-bin//Software/Crypto/crypto_main.pl and make sure your username has acknowledged cryptography permissions for downloading IOS Aironet images.</p> <p>To work around this problem, download the image from outside WLSE, then use Firmware > Images > Import > From Desktop to import the image into WLSE.</p>
CSCsa10675	Reports have missing data for wireless clients with 11g and 11a radios.	<p>When you select Reports > Wireless clients and select a client associated to an AP with 11g or 11a radios, the report has missing data. (See CSCed19821.)</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa11295	AP and Bridge Performance Trends Report in graph and tabular form might have multiple data points with same timestamp.	<p>When there are changes to the aggregated columns like <i>ifDescr</i>, <i>ifIndex</i> and <i>IfType</i>, multiple rows with duplicate timestamps might be generated.</p> <p>There is no workaround for this problem.</p>
CSCsa11677	Invalid selection causes loop of error messages display.	<p>When you select Configure > Templates, enter a name and select IOS, then click Create New Template > Categories > Network Interfaces > Radio 802.11b/g, then select a channel for Default Radio Channel and click a channel from Least Congested Channel Search, an error message appears saying that the default radio channel must be set to the least congested frequency to modify this field. When you click OK, the same error message comes up immediately and this operation loops.</p> <p>To work around this problem, hit the Tab key to move the focus to Default Radio Channel and select Least Congested Frequency.</p>
CSCsa12358	Wireless Client Detail Report sometimes not showing correct state.	<p>Sometimes the wireless client detail report doesn't show the correct state of the client. In the reports it shows it as <i>assocAndAuthenticated</i> when it should show it as <i>none</i>.</p> <p>There is no workaround to this problem; however, the Time Last Seen field, which indicates the last time the client was seen by WLSE to be associated with the AP, is correct. If the client roams or reassociates to a different AP, the client details are updated appropriately to reflect the current association.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa12833	Pushing an unsupported image on AP breaks the AP.	<p>If you push a 12.2(11)JA image through WLSE to an AP 1100 with a g radio, the AP crashes. The 12.2(11)JA image not to supported on g radios.</p> <p>There is no workaround to this problem.</p>
CSCsa13094	Editing rule based groups is not recomputed.	<p>When you create a rule-based group and edit the group by changing any of its values, the group is not updated with the changes.</p> <p>To work around this problem, edit the group and change its name. The group will show the correct members. Edit the group again by changing the name back to the original name.</p>
CSCsa13695	Devices marked 'd'/Deleted show in Manage/Unmanage search.	<p>When you delete a device, the device still appears when you search in the Manage/Unmanage folder. The deleted devices continue to show in the manage/unmanage search until they are removed from WLSE, which could take up to 24 hours.</p> <p>There is no workaround to this problem.</p>
CSCsa13728	The wrong command is reported as failed when an IOS template job that has more than one command fails.	<p>If you create a template with more than one command, and one of the commands fails, the command that is reported as failed is not correct.</p> <p>To work around this problem, note the command previous to the one that is reported as failed; that is the one that has, in fact, failed.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa13929	Version checking error occurs if template has 11g plus any 11a radio parameters.	<p>When you create a template for a dual mode IOS AP1210 that has any of the 11a interface parameters and has specific 11g parameters, the version checking fails to process and gives you an error that no valid device versions are supported. This problem occurs only if you selected the following 11g specific parameters in the Radio-802.11b/g template:</p> <ul style="list-style-type: none"> • Data rates in for 11G • CCK Transmitter Power (mW) • OFDM Transmitter Power (mW) and • Short Slot-Time <p>There are two workarounds to this problem:</p> <ul style="list-style-type: none"> • If you have an 11g radio and want to set the 11g parameters above, create a separate template for these parameters, save the template, and then push it to the specific AP. • After you see the message “Error processing configuration / No valid device versions supported;” save the template. When creating the job with this template, during the final step of saving the job, the following message appears: <pre>Currently selected configuration template does not have valid device version information. This template will not be validated against the selected devices. Click Save to save the job and the template will be applied to the AP.</pre>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa13934	Scheduled email Client Historical Association Reports are blank.	<p>When the Client Historical Association Reports are scheduled to be exported by email, the received reports are blank.</p> <p>To work around this problem, use the export feature to display the Client Historical Association report.</p>
CSCsa14926	TACACS+ secret does not accept dollar sign.	<p>You cannot use the “\$” sign in the authentication password.</p>
CSCsa15394	WLSE 2.7 generates false WDS 0.0.0.0 faults when no WDS is configured.	<p>If an AP is not registered with any WDS, WLSE generates a fault saying the AP is registered with an unmanaged WDS (0.0.0.0) instead of generating a fault saying “AP is not registered with any WDS.” If you see a fault that says an AP is registered with an Unmanaged WDS 0.0.0.0, this means the AP is not registered with any WDS.</p> <p>There is no workaround to this problem.</p>
CSCsa15540	Inventory does not start for partially successful jobs.	<p>When a job is only partially successful, the inventory cycle does not start up, and the new information is not be displayed until the next regularly scheduled inventory.</p> <p>To work around this problem, create an on-demand inventory job for the access points that were successfully upgraded in the partially successful firmware job.</p>

Table 2 *Known Problems in the WLSE (Continued)*

Bug ID	Summary	Explanation
CSCsa16324	If you run CLI “services status” on the standby box, the database failure shows.	<p>After you turn on Redundancy and telnet to the standby box and run CLI of “services status,” the failure message should say:</p> <p>SQL1117N A connection to or activation of database “WLSEDB” cannot be made There is no workaround to this problem.</p>
CSCsa16787	Wrong clock time zone for Eastern time zone.	<p>For the Eastern time zone setting, the time zone names (-5 and recurring) are missing.</p> <p>To work around this problem, apply the following commands to the template and apply the template:</p> <pre>clock timezone R -5 clock summer-time R recurring</pre>

Table 3 Resolved Problems in WLSE

Bug ID	Summary	Explanation
CSCea91955	<p>Fault Notification Syslog messages from WLSE are displayed in a truncated form on the Resource Manager Essentials (RME) 3.4 Syslog Standard Report.</p>	<p>The RME 3.4 Syslog Standard Report displays fault notification syslog messages sent in XML message format or in plain text message format in a truncated form.</p> <p>To work around this problem and view the syslog messages in an untruncated form, see the following flat syslog file located in:</p> <ul style="list-style-type: none"> • On the Solaris 2.8 based RME 3.4 server: /var/log/syslog_info • On the Windows 2000 based RME 3.4 server: C:/Program Files/CSCOPx/log/syslog.log
CSCeb23307	<p>Entering dates under the Advanced Options for Device Discovery can generate an error message even if the dates are valid.</p>	<p>When you select Devices > Discover > Discover > Advanced Options, and set the Filters Valid From date, only the day and month are checked for validity, not the year. Therefore, if you enter a date range such as 12/30/2003 to 01/20/2004, you will get an error message stating that the "Start Date is greater than End Date," even though the date range is valid.</p> <p>To work around this problem, do not enter date interval values when using the MAC filtering option.</p>

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCeb23714	You will get an error if you use the pound (#) sign in the password for device Telnet credentials.	<p>When you use a pound (#) sign in the password field under Devices > Discover > Device Credentials > Telnet/SSH/User Password, a 500 Internal Server Error displays.</p> <p>To work around this problem, do not use pound (#) sign in the password.</p>
CSCec33330	A configuration job for a template which includes a banner command that spans multiple lines will not complete successfully.	<p>If the configuration template used in the configuration job has banner command spanning multiple lines in the Custom Values section, the job may either report a failure or continue to appear in a running state.</p> <p>To work around this problem either remove the banner command or make sure it spans only a single line, then run the configuration job again.</p>
CSCec38013	When you upgrade to Release 2.5, the fault "Ethernet BVII port is down" on IOS access points is not deleted.	<p>The IOS access point fault "Ethernet BVII port is down" in a Release 2.0 WLSE is not deleted after an upgrade to WLSE Release 2.5.</p> <p>To work around this problem, after you upgrade to Release 2.5:</p> <ol style="list-style-type: none"> 1. Disable fault polling for the access point Ethernet Port Status Threshold. 2. Manually clear the 'Ethernet BVII port is down' faults for the IOS access points.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCec42478	Dual band, non-IOS 1200 access points do not generate a Leap Disabled fault for the 802.11a RF port.	<p>When LEAP is disabled on the 802.11a RF port of a non-IOS, 1200 access point, it is not reported under Faults > Display Faults.</p> <p>This is a problem with the access point software, not the WLSE. Please refer to Bug ID CSCec47797.</p> <p>There is no workaround for this problem.</p>
CSCec52282	You cannot use the CLI command ip domain-name to reset your domain.	<p>The CLI command IP domain-name does not work correctly.</p> <p>To work around this problem, use the CLI command erase config to erase the previous WLSE configuration, then run the setup program and enter your network information.</p>
CSCec54430	There are no SSIDs listed under Faults > Manage Fault Profiles > Access Point Policies > EAP per SSID Enforced for non-IOS, dual band, 1200 access points.	<p>Dual band, non-IOS 1200 access points running version 12.03T, fail to list the Available SSIDs for Radio 802.11a in the EAP per SSID Enforced policy under Faults > Manage Fault Profiles.</p> <p>There is no workaround for this problem.</p>
CSCec57502	When you export trend report data in a CSV format, some of the attributes are incomplete.	<p>When you use CSV format to export trend report data, the data in the CSV file is incomplete.</p> <p>There is no workaround for this problem.</p>

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCec59512	Duplicate EAP Disabled per SSID faults are generated for the 11b radio of dual band 1200 access point.	Dual band, 1200 access points generate duplicate EAP Disabled per SSID faults under Faults > Display Faults. There is no workaround for this problem.
CSCec64486	Firmware conversion jobs are reported as successful even though they are not.	Sometimes firmware conversions from non-IOS to IOS are terminated quickly and display as successful. However, the Job Run log indicates an error downloading the non-IOS configuration. To work around this problem, increase the SNMP timeout and retries for those devices, then run the job again.
CSCec70880	Disabling Interference Detection causes hung Radio Management processes.	If you disable the Interference Detection fault setting (Faults>Manage Network-Wide Settings>Interference Detection), this can result in hung Radio Management operations (for example, radio scan). To work around this problem, never disable Interference Detection. If you are not interested in the interference faults, set the fault settings to the maximum values to reduce the number of interference faults generated.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCec70915	<p>“SNMP unreachable” APs can cause Client Walkabout to never stop.</p>	<p>If any APs included in a client walkabout session are “SNMP unreachable,” client walkabout does not stop. This prevents other jobs (for example, radio scan and other client walkabout tasks) from running. The user interface indicates that the task has stopped, but the task is still running in the background.</p> <p>To work around this problem, make sure all APs you select for a client walkabout session are SNMP reachable before starting the client walkabout. If the client walkabout never stops, you need to restart WLSE.</p>

Table 3 *Resolved Problems in WLSE (Continued)*

Bug ID	Summary	Explanation
CSCec72920	After converting an non-IOS access point to an IOS access point, the correct native VLAN may not be configured.	<p>If you convert from a non-IOS access point to an IOS access point, and the non-IOS access point does not have a native VLAN configured, a VLAN will be automatically assigned as the native VLAN. However, the assigned native VLAN may not be correct.</p> <p>To work around this problem, log in to the access point and change the native VLAN to the correct one.</p>

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa08621	<p>When you use the CLI command interface to set the WLSE to half-duplex, the WLSE crashes.</p>	<p>Setting the WLSE interface duplex mode may cause a catastrophic segmentation fault that corrupts the WLSE flash.</p> <p>There is no workaround for setting the duplex mode.</p> <p>Recovery requires erasing WLSE configuration in flash and rerunning the setup script.</p> <p>To recover, do the following:</p> <ol style="list-style-type: none"> 1. Connect to the WLSE console port. 2. Power cycle the WLSE. 3. When the WLSE powers up, wait for the GRUB loader to present you with OS options. 4. At the GRUB loader, select CiscoBreR. This boots you in to the recovery image and presents you with a Linux shell prompt. 5. At the shell prompt, type the command erase config. This erases the flash (leaving the WLSE database intact), then reboot the WLSE. 6. When WLSE reboots, you will be forced to rerun the setup script.

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>

