



# Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.13

---

**July 10, 2006**

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) 2.13.

These release notes detail:

- [New Features, page 2](#)
- [Product Documentation, page 2](#)
- [Documentation Updates, page 6](#)
- [Open and Resolved Caveats, page 6](#)
- [Obtaining Documentation, page 13](#)
- [Documentation Feedback, page 14](#)
- [Cisco Product Security Overview, page 14](#)
- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 17](#)

# New Features

WLSE 2.13 supports:

- Deployment on platforms: 1130, 1130-19, and 1030.
- Cisco IOS Release 12.3(8)JA
- User role integration with ACS
- Enhanced support for WLSM faults, reports, discovery, and inventory
- IDS: Management Frame Protection (MFP)
- Voice (802.11e TSPEC CAC), GPR and the following features:
  - Traffic Stream Metrics
  - Enhanced radio parameter generation to support voice deployment
  - Voice profile to support consistency between self healing and radio parameter generation



**Note**

---

WLSE 2.13 supports only IOS access points.

---

## Product Documentation

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

The following product documentation is available for WLSE 2.13:

**Table 1 Product Documentation**

Document Title	Available Formats
<i>Installation and Configuration Guide for the 1030 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE Express. Available in the following formats:</p> <ul style="list-style-type: none"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html</a></li> <li>Printed document available by order (part number DOC-17252=)<sup>1</sup></li> </ul>
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html</a></li> <li>Printed document available by order (part number DOC-17251=)<sup>1</sup></li> </ul>
<p><i>Installation and Configuration Guide for the 1133 CiscoWorks Wireless LAN Solution Engine</i></p> <p>Details on WLSE 1133 hardware and hardware installation and initial software configuration.</p>	<ul style="list-style-type: none"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>Online: <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm</a></li> </ul>
<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"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html</a></li> </ul>
<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"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html</a></li> </ul>

Table 1 Product Documentation (continued)

Document Title	Available Formats
<p><i>Regulatory Compliance and Safety Information for the CiscoWorks 1133 Wireless LAN Solution Engine</i></p> <p>Translated safety warnings and compliance information.</p>	<ul style="list-style-type: none"> <li>Printed document included with the product.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>Online: <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_13/index.htm</a></li> </ul>
<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"> <li>From the WLSE online help.</li> <li>PDF on the WLSE Recovery CD-ROM.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html</a></li> </ul>
<p><i>Upgrading CiscoWorks Wireless LAN Solution Engine Software</i></p>	<p>Describes the options available and how to upgrade to the WLSE system software to 2.13. Available in the following formats:</p> <ul style="list-style-type: none"> <li>From the WLSE online help.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_install_and_upgrade.html</a></li> </ul>
<p><i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i></p>	<p>Contains FAQs and troubleshooting information, and provides a table for all the faults displayed under <b>Faults &gt; Display Faults</b> with explanations and possible actions. Available in the following formats:</p> <ul style="list-style-type: none"> <li>From the WLSE online help.</li> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html</a></li> </ul>
<p><i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i></p>	<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"> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html</a></li> </ul>
<p><i>Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine</i></p>	<p>Lists the devices supported by WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> <li>On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html</a></li> </ul>

**Table 1** Product Documentation (continued)

Document Title	Available Formats
<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"> <li>• Printed document included with product.</li> <li>• PDF on the WLSE Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_documentation_roadmaps_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_documentation_roadmaps_list.html</a></li> </ul>
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine Express</i>	<p>Lists the documents associated with this release of WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> <li>• Printed document included with product.</li> <li>• PDF on the WLSE Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/ps6379/products_documentation_roadmaps_list.html">http://www.cisco.com/en/US/products/ps6379/products_documentation_roadmaps_list.html</a></li> </ul>
<i>Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using Cisco Secure ACS</i>	<p>Describes the procedure to configure the CiscoWorks Wireless LAN Solution Engine (WLSE) using ACS as a TACACS+/RADIUS authentication module.</p> <ul style="list-style-type: none"> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html</a></li> </ul>
<i>WLSE Express AAA Server Certificate Configuration Guide</i>	<p>Provides information about public key infrastructure (PKI) and Rabin-Shamir-Adelmann (RSA) certificates, how to generate certificates to be used with the WLSE Express, and how to configure AAA certificates to be used on WLSE-Express.</p> <ul style="list-style-type: none"> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/products/ps6379/products_installation_and_configuration_guides_list.html">http://www.cisco.com/en/US/products/ps6379/products_installation_and_configuration_guides_list.html</a></li> </ul>

1. See [Obtaining Documentation](#), page 13.

# Documentation Updates

Please note the following additions to WLSE user documentation and online help:

## Rack Mounting Shelf not Included with WLSE Express

The *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express* incorrectly lists a rack mounting shelf as an item included with the WLSE Express. However, the rack mounting shelf is not included and must be ordered separately.

## Additions to the User Guide for the CiscoWorks Wireless LAN Solution Engine

### Supported Browsers

Section should include:

- “Java Plug-in release 1.5 is required. The Java Plug-in is used by certain WLSE features such as Location Manager and Real Time Graphs. The Java Plug-in can be installed from a third-party source such as Sun Microsystems.”
- “Mozilla should be replaced with Firefox release 1.06.”

### Deployment Wizard

Section should include:

- “The roles and privileges assigned to your login determine whether you can use the Deployment Wizard. Select **Admin > User Admin > Manage Roles**, and make sure that both the **Wizard > WLSE Wizard** and **Configure > Auto Update** options are checked.”

## Additions to Online Help

### Naming Guidelines

Should include:

- “The pound (#) signs should not be used in the shared secret for RADIUS or TACACS+ authentication modules, which are defined under **Admin > Appliance > Security > Authentication Modules**.”

## Open and Resolved Caveats



### Caution

---

Refer to Bug ID [CSCse02049](#) for important information regarding a patch needed after upgrading to WLSE 2.13 from WLSE 2.11 or 2.12.

---

- [Table 2](#) describes outstanding caveats in WLSE 2.13.
- [Table 3](#) describes caveats resolved since the previous 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.)

**Table 2** Open Caveats in the WLSE

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	The Client Historical Association report does not have information about the last time a client associated with the access point, the time it disconnected from the access point, the duration of the association, or the association state.  <b>Workaround:</b> No known workaround.  <b>Note</b> In the current release, only association times of a client are supported. Disassociation time of the client is not available in this release.
CSCec41188	You cannot add an access point-based LEAP server to the WLSE if it is already managed by WLSE.	You cannot add an access point-based LEAP/EAP-FAST server to WLSE if that access point is already being managed by WLSE. The WLSE views it as a duplicate device.  <b>Workaround:</b> No known workaround.
CSCef90440	A database exception occurs when creating jobs in multiple WLSE sessions.	When you try to create WLSE configuration templates in two separate browser windows simultaneously, one configuration template does not get saved.  <b>Workaround:</b> Create templates in a single browser window, one at a time.
CSCeh06754	Radio Monitoring is not enabled after rebooting a 350 access point.	Occasionally 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.  <b>Workaround:</b> Re-enable Radio Manager from WLSE.
CSCsa60720	Location Manager loads with a previous version of jar file.	<b>Workaround:</b> Close all instances of your browser to clear the Java cache. Then relaunch your browser and relaunch Location Manager.
CSCsa79506	If a switch has multiple IP addresses, port suppression may fail.	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.  <b>Workaround:</b> Manually suppress the switchport from the Rogue Details screen.

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa93652	Backup data fails occasionally due to database locks.	<p>The backup function occasionally does not work.</p> <p><b>Workaround:</b> Do the following:</p> <p>Stop the services by entering</p> <pre>services stop services status</pre> <p>Make sure the database is no longer running, and then restart the services by entering</p> <pre>services start</pre> <p>If the services do not restart after entering these commands, reboot the WLSE.</p> <p>After restarting the WLSE, log into the WLSE and select <b>Admin &gt; Appliance &gt; DIAGNOSTICS &gt; Processes</b>.</p> <p>Check WirelessSvcMgr and click <b>Stop</b>.</p> <p>Check WLSEjobvm and click <b>Stop</b>.</p> <p>Check WLSEFaults and click <b>Stop</b>.</p> <p>Make sure the processes actually stop; the green arrow pointing up should change to a red arrow pointing down.</p> <p>After the processes have been stopped, perform the backup.</p>
CSCsb64225	Replacement access point shows incorrect MAC address in Location Manager.	<p>If you replace an access point with a different access point that has the same management IP address (but different MAC addresses), after reinventory of that access point, all reports show the new access point's MAC addresses, but Location Manager still shows the old access point's MAC addresses.</p> <p><b>Workaround:</b> No known workaround.</p>
CSCsb65071	An SNMP timeout occurs during access point radio scan jobs.	<p>In some cases, you might get a "Not SNMP Accessible" error message on some access points during an access point radio scan even though the access point is SNMP reachable and the SNMP RW community string provided in WLSE is correct. During the start of the access point radio scan or in any of the following 8 power steps, WLSE gives an error message indicating that a particular interface is not SNMP accessible. A corresponding SNMP Timeout exception appears in the swan.log for the same access points.</p> <p><b>Workaround:</b> Do one of the following:</p> <ul style="list-style-type: none"> <li>• Reduce the number of access points in the access point radio scan job and then rerun the job; or,</li> <li>• Create a new radio scan job and include the access points that had SNMP errors, select some neighboring access points (for example, from the same floor, one floor above, or one floor below), then run the access point radio scan job.</li> </ul>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsb65711	Deleted and re-discovered devices do not get listed in Radio Monitoring.	After an access point is deleted then rediscovered, radio monitoring is not turned on for that access point. <b>Workaround:</b> Select <b>Radio Mgr &gt; Radio Monitoring</b> , select the access point, and turn on radio monitoring.
CSCsb69261	The 802.11a maximum power is not displayed correctly unless native power is enabled.	The 802.11a radio maximum transmit power for the UNII-2 (52-64) and UNII-3 (149-161) channels is incorrectly displayed as 30mW in the Location Manager GUI. <b>Workaround:</b> Enable <i>dot11 extension power native</i> on the 802.11a radio interface by entering the following configuration commands: <pre>ap(config)# int d1 ap(config-if)# dot11 extension power native</pre>
CSCsb73871	WLSM-WDS does not get discovered after being deleted.	After you delete WLSM-WDS from WLSE, subsequent manual discovery and auto-discovery of WLSM-WDS fails. <b>Workaround:</b> Reboot WLSE or stop and then start the services.
CSCsd01131	Telnet enable does not synchronize to standby WLSE.	After you enable Telnet on an active WLSE, the user interface of the standby WLSE incorrectly shows that Telnet is enabled on the standby WLSE. However, Telnet is not enabled. <b>Workaround:</b> You must use the Standby WLSE user interface to re enable Telnet.
CSCsd23516	Redundancy gets stuck in the pre-standby state after <i>reinitdb</i> .	The Standby WLSE server might remain in the pre-standby state for a long time, for example, more than 3 hours. <b>Workaround:</b> Log into the web server of the Active WLSE, navigate to <b>Admin &gt; Appliance &gt; Redundancy &gt; Manage Redundancy</b> , and click <b>Verify</b> . When asked if you want to apply the changes, click <b>Yes</b> . The Standby WLSE will request another backup from the Active WLSE. After the backup is restored on the Standby WLSE, the WLSE will go to the Standby state.
CSCsd23688	Changing the <i>webtimeout</i> value starts another instance of Tomcat.	When you change the timeout value under <b>Admin &gt; Appliance &gt; Time/NTP/Name/Web Timeout</b> , another set of Tomcat processes are started but the previous processes are not terminated. <b>Workaround:</b> Reload the WLSE after changing the web timeout value.

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsd33933	“Voice stream is rejected due to other reason” is not updated.	<p>When you generate a report under <b>Reports &gt; Voice &gt; AP Group Voice Stream Summary: Current</b>, the third column of the report displays “Voice Streams Rejected Due To Insufficient Bandwidth.” The last column of the report is supposed to display “Voice Streams Rejected Due To Other Reason,” which can be any one of the following reasons:</p> <ul style="list-style-type: none"> <li>• The SSID is blocked for Admission Control.</li> <li>• There is an incorrect PHY rate</li> <li>• There is a TSPEC violation.</li> </ul> <p>However, the report shows the voice streams rejected due to “TSPEC violation” only.</p> <p><b>Workaround:</b> Get the detailed reason for the voice stream rejections from the access point console using the CLI command <i>show dot11 cac</i>. This displays the CAC settings and statistics, including the reasons for the rejections.</p>
CSCsd38274	TSM QoS threshold settings that are modified in the GUI are overwritten.	<p>If you modify and save the TSM QoS Threshold settings under <b>Faults &gt; Voice QoS Settings</b>, and if for any reason, the WLSE is restarted (or the services are stopped and restarted), the TSM QoS threshold settings you modified are overwritten by the system default values. This happens only if and when the WLSE is restarted (or when the services are stopped and restarted).</p> <p><b>Workaround:</b> You need to reset the threshold values after the WLSE is restarted.</p>
CSCsd66542	The date on some reports shows “dddd” for users other than the admin.	<p>When a user other than <i>admin</i> accesses reports from the WLSE GUI, the date selection in Trend Reports and some of the Wireless Client Reports shows <i>dddd</i> for the year selection.</p> <p><b>Workaround:</b> Use the default <i>admin</i> user to view Trend and Historical Reports.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsd74705	Starting an upgrade from a WLSE 2.11, 2.12 or 2.13 base, on a slow link, and utilizing the MS Windows Repository method to upgrade may cause the upgrade to fail.	<p>The Microsoft Windows Repository method first downloads the upgrade image from the Windows Server to the WLSE appliance. If this first transaction takes more than 15 minutes to complete, the actual upgrade never starts. Under normal link speeds, the download occurs in less than 15 minutes. The upgrade then has a chance to shut down the idle daemon while the upgrade runs.</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>1. Follow steps 1-7 under the Microsoft Windows Server Repository section in the WLSE-2.13-K9.readme-V1.txt file.</li> <li>2. From the browser, manually disable the idle daemon before continuing with the upgrade as follows: <ol style="list-style-type: none"> <li>a. Select <b>Admin &gt; Appliance &gt; Diagnostics &gt; Processes</b>.</li> <li>b. Select <b>WLSEIdleServer</b>, then click <b>Stop</b> at the bottom of screen.</li> </ol> </li> <li>3. Continue with step 9 of the upgrade readme file.</li> </ol>
CSCsd89254	The authorization settings on a WLSE 2.13 with a restored 2.11 or 2.12 backup in which a remote service is configured, are set incorrectly.	<p>Restoring a WLSE 2.11 or 2.12 backup onto a WLSE 2.13 system does not correctly restore the authorization settings if they are set to a remote service. The settings are only partially restored and should work, but will be reported incorrectly as set to local.</p> <p><b>Workaround:</b> Re-run the <i>auth</i> command with the desired settings. This will correctly set all the needed parameters.</p>
CSCse02049	Apply patch after upgrading/restoring to WLSE 2.13 from 2.11 or 2.12.	<p>When you upgrade from WLSE 2.11 or 2.12 to WLSE 2.13, you might encounter the following problems:</p> <ul style="list-style-type: none"> <li>• RPG will not work if there are no floor images with Client Walkabout data.</li> <li>• For floors already present before the upgrade, RPG recommendation for power and channel will be suboptimal.</li> <li>• Self Healing might fail or will not provide optimized power recommendation.</li> <li>• ARSS might fail or raise false alarm.</li> </ul> <p><b>Workaround:</b> You must install the WLSE-2.13-CSCse02049 patch after you upgrade to WLSE 2.13 from the following WLSE releases: 2.11 or 2.12.</p> <p><b>Note</b> The patch does not need to be applied immediately after the upgrade.</p>

**Table 3 Resolved Caveats in the WLSE**

Bug ID	Summary	Explanation
CSCeg43747	In prior releases, you were unable to set the EAP-FAST credential-lifetime parameter with CLI when using quotes. <i>This problem applied to WLSE 1030 only.</i>	If you set the EAP-FAST credential lifetime value using double quotes (“ ”) from the CLI on a WLSE 1030, the following command failed:  <b>aaa-server eap-fast credential-lifetime "8 days"</b>
CSCsa75699	In prior releases, the installation wizard did not compare the WLSM release numbers.	Step 4 of the installation wizard displayed the software release numbers for access points and WLSM. If you selected <b>Compare known devices version</b> , you got a list of access points that met the recommended version requirement, but the list did not include WLSM. In addition, the recommended version numbers for WLSM were not accurate.
CSCsa99224	In prior releases, the VM would crash in rare conditions.	In rare conditions, the Tomcat or WLSE Faults virtual machine (VM) could crash. If any of the VMs crashed in a redundancy environment, the standby WLSE took over and became the Active WLSE and the system recovered. If the Tomcat VM crashed in a standalone environment, the WLSE GUI did not come up and the daemon manager tried to recover and restart the services automatically. If the WLSEFaults VM crashed in a standalone environment, a red ticker scrolled in the window and displayed the message “WLSEFault process is down.” In some cases, the daemon manager did not know that the VM crashed and the process status still showed as actively running. If this happened, the system did not recover automatically.
CSCsb25230	In prior releases, sometimes disabling redundancy via the GUI on an active WLSE would cause the database services to stop on the standby WLSE.	If you used the GUI to disable redundancy on an active WLSE, the database services often would stop on the standby WLSE. If this occurred, you would see the “User role empty” message when you tried to log into the GUI of the standby WLSE.
CSCsb37387	In prior releases, WLSE time and date was not synchronized with the NTP server time.	If you set the WLSE time or date to a future date or time before you configured the NTP settings, WLSE did not synchronize with the NTP server date/time. However, if you set the date/time to a past date, WLSE did synchronize to the current date/time.
CSCsb60195	In prior releases, the Wizard Compare Known Devices Version option could not detect the 350 access point.	If you selected <b>Wizard &gt; Software</b> , and then clicked <b>Compare Known Devices Version</b> , the table did not show the following access point 350 with the latest release, 12.3(7)JA.
CSCsb82715	In prior releases, redundancy upgrades did not work if you changed the admin password.	If you changed the admin password on one WLSE in a redundant environment while an upgrade to 2.12 was in progress, the upgrade failed.
CSCsb95162	In prior releases, the Windows Domain Auth Server configuration was lost during upgrade. <i>This problem applied to WLSE 1030 only.</i>	When you upgraded a WLSE 1030 from WLSE 2.11 to WLSE 2.12, all data on the Windows Domain Authorization Server page, including host name, port, default domain, default AAA user group, and AAA user groups to windows groups attributes, was lost.

**Table 3** Resolved Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsc39117	In prior releases, upgrading to WLSE 2.12 without adequate space would cause you to lose the database.	After upgrading to WLSE 2.12, the database did not start, but the web GUI did start and attempted to log in. You were not able to log in to WLSE successfully and a message appeared in the upper right corner of the screen indicating that the database did not respond correctly.
CSCsc50985	In prior releases, WLSE was unable to save SNMP community strings for an IP address range.	When you added SNMP community strings using an IP address range, for example 172.19.28.[2-80], WLSE did not save the community strings.
CSCse40868	In prior releases, when you tried to access Real Time Graphs or Location Manager WLSE features, a warning message appeared indicating that the Verisign certificate had or would be expiring.	There were two workarounds for this outstanding caveat: (1) Click <b>OK</b> in the warning dialog box to continue working with the application -or- (2) Upgrade to WLSE 2.13 or greater in which the caveat was resolved.

## 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](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](mailto: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](mailto: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](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](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](mailto: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](mailto: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](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.