



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.7.1

July 18, 2006

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) 2.7.1.



Note

The Sun Java Cryptography Extension (JCE) 1.2.1 used in this release expired 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 detail:

- [“New Features” section on page 2](#)
- [“Product Documentation” section on page 2](#)
- [“Documentation Updates” section on page 4](#)
- [“Open and Resolved Caveats” section on page 7](#)
- [“Obtaining Documentation” section on page 15](#)
- [“Documentation Feedback” section on page 16](#)
- [“Cisco Product Security Overview” section on page 16](#)
- [“Obtaining Technical Assistance” section on page 17](#)
- [“Obtaining Additional Publications and Information” section on page 19](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

New Features

WLSE 2.7.1 supports:

- Firmware version 12.2(15)XR
- WLSM
- Firmware conversion of VxWorks version 12.04 to IOS software

Product Documentation

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

The following product documentation is available for WLSE:

Table 1 **Product Documentation**

Document Title	Description
<i>Installation and Configuration Guide for the 1130/1105 CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • Printed document available by order (part number DOC-7816194=)¹
<i>Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_7/index.htm • Printed document available by order (part number DOC-7816345=)¹

Table 1 **Product Documentation**

Document Title	Description
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<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=)¹
<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**

Document Title	Description
<i>Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine, Release 2.7.1</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 15.

Documentation Updates

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

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

Wireless LAN Services Module Acronym

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

Required Software for Access Points with 802.11g Radios

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

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 access point in each access point subnet; a backup WDS can also be defined in each access point subnet.”

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 access points:

- 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.

Required Software for Access Points with 802.11g Radios

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

Disable Pop-Up Blocker

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

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 read “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 a node’s originally configured IP address should remain the same. If you need to reconfigure a node’s IP address, first turn redundancy off, and then configure a node’s IP address.”

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 will fail and generate 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 reenabling 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: “Access point subnet” instead of “Layer-2 domain” so that the first sentence reads: “The WLSE must register with the WDS in each managed access point 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 wlcgp wds ap` command on the primary WDS in enable mode.”

Using Scanning-Only Access Points (APs)

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

Use a template-based configuration job to configure one or more access points as scanning-only access points (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 access points.
- Do not configure the scanning-only access point as an active/backup WDS (to serve fast roaming traffic).



Note Even though configuring *Scanning-Only APs* and configuring *WDS* are independent features, CPU contention occurs if both are enabled on the same access point. To make certain that Scanning-Only access point traffic does not affect the real time performance for fast roaming, *do not* configure a scanning-only access point 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 access points are 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, access points running in scanning-only mode may face sporadic connection loss and image upgrade failure. To resolve these problems, use the following access point configuration CLI commands to balance CPU time:”

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



Note

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.

Modifying Access Point Coverage Display Options

An additional step should appear after step 5. The new step should read: “Click **Display coverage for operational radio interfaces only** to display coverage for access points that are functional. If this box is checked (default), the coverage for radios that are determined to be down is not displayed.”

All other steps in this section are correct.

Additions to Online Help

Discovering WLSM

The online help should contain the following information:

“If you are using a WLSM, you need to configure the following command on the WLSM to point to the WLSE:”

```
wlccp wnm ip address <ip of wlse>
```

Specifying the Backup Location

The online help description for the **Clear Log** button in the **Administration > Backup and Restore > Configure** window is incorrect. The online help description of the **Clear Log** button should read: “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 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 access points in this group.”

Open and Resolved Caveats

Table 2 describes outstanding caveats known to exist in WLSE 2.7.1. Table 3 describes WLSE caveats resolved since the previous release.

Table 4 describes Resolved VxWorks to IOS Conversion Bugs in WLSE.



Note

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

WLSE Caveats

Table 2 Open Caveats in the WLSE

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	The Client Historical Association report does not have information about the last time a client associated with the access point, the time it disconnected from the access point, the duration of the association, or the association state. Workaround: No known workaround. Note In the current release, only association times of a client are supported. Disassociation time of the client is not available in this release.
CSCec41188	You cannot add an access point-based LEAP server to the WLSE if it is already a managed by WLSE.	The WLSE views it as a duplicate device. Workaround: No known workaround.
CSCed55402	When you set the WEP Enforced policy under Faults > Manage Faults the faults are not generated correctly.	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). Workaround: No known workaround.

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCed89308	RPG Stop Calculation does not work when a 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>Workaround: No known workaround.</p>
CSCee03323	Rogue PHY type is reported as 11a when it should be 11b.	<p>On cb21ag, pi21ag, and ti21ag client adapters, when a rogue access point client is detected, the rogue report might indicate the rogue is an 11a PHY type when it is an 11b PHY type.</p> <p>Workaround: No known workaround.</p>
CSCee09800 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 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>Workaround: There are two workarounds to this caveat: (1) Ignore the IP Address Change and the Detach From WDS events if they occur immediately after a Roam event or (2) Upgrade to release 2.11 or greater release in which it is resolved. Please consult with technical support BEFORE upgrading for recommended upgrade path.</p>
CSCee18557	Unable to include filters in policy groups.	<p>When you deploy policy groups to access point 1200s and access point 350s running VxWorks release 12.0(4), the filters associated with the policy groups cannot be included even though the policy group itself is deployed.</p> <p>Workaround: No known workaround.</p>
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>Workaround: Log in directly to the ACS server and look at the ACS Failed Login Report.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCee37875	CCO crypto download changes disrupt image import from Cisco.com	<p>When you select Firmware > Images > Import > From Cisco.com, log in with your CCO account, and select any access point 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>Workaround: Download the image from outside WLSE, then use Firmware > Images > Import > From Desktop to import the image into WLSE.</p>
CSCsa12061	Unable to schedule an IOS access point reload.	<p>You cannot reload an IOS access point via a Configuration template.</p> <p>Workaround: No known workaround.</p>
CSCsa12358	Wireless Client Detail Report sometimes does not show correct state.	<p>In the reports it shows it as <i>assocAndAuthenticated</i> when it should show it as <i>none</i>.</p> <p>Workaround: No known workaround; however, the Time Last Seen field, which indicates the last time the client was seen by WLSE as associated with the access point, is correct. If the client roams or reassociates to a different access point, the client details are updated appropriately to reflect the current association.</p>
CSCsa12833	Loading an unsupported image onto an access point crashes the access point.	<p>If you load a 12.2(11)JA image through WLSE to an access point 1100 with a 802.11g radio, the access point crashes. The 12.2(11)JA image is not supported on 802.11g radios.</p> <p>Workaround: No known workaround.</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>Workaround: 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 a search is initiated, a deleted device may appear in the Manage/Unmanage folder up to 24 hours after its deletion.</p> <p>Workaround: No known workaround.</p>
CSCsa13728	The wrong command is reported as failed when an IOS template job that has more than one command, fails.	<p>Workaround: Note the command previous to the one that reported as failed; that is the one that actually failed.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCse40868	When you try to access Real Time Graphs or Location Manager WLSE features, a warning message appears indicating that the Verisign certificate has or will be expiring.	<p>Workaround: There are two workarounds for this outstanding caveat: (1) Click OK in the warning dialog box to continue working with the application -or- (2) Upgrade to WLSE 2.13 or greater in which the caveat is resolved.Please consult technical support BEFORE upgrading for recommended upgrade path.</p>
CSCsa13929	Version checking error occurs if template has 802.11g and 802.11a radio parameters.	<p>When you create a template for a dual mode IOS access point 1210 that has any of the 802.11a interface parameters and has specific 802.11g parameters, the 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 802.11g 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>Workaround: There are two workarounds to this problem:</p> <ul style="list-style-type: none"> • Option 1: If you have an 802.11g 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 access point. • Option 2: 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: <p style="margin-left: 40px;">Currently selected configuration template does not have valid device version information. This template will not be validated against the selected devices.</p> <p>Click Save to save the job and the template will be applied to the access point.</p>
CSCsa14926	TACACS+ secret does not accept dollar sign.	<p>You cannot use the “\$” sign in the authentication password.</p> <p>Workaround: No known workaround.</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>Workaround: Create an on-demand inventory job for the access points that were successfully upgraded in the partially successful firmware job.</p>

Table 2 Open Caveats in the WLSE (continued)

Bug ID	Summary	Explanation
CSCsa16324	If you run CLI “services status” on the standby box, a database failure shows.	After you turn on Redundancy and telnet to the standby box and run CLI of “services status,” the failure message should say: SQL1117N A connection to or activation of database “WLSEDB” cannot be made. Workaround: No known workaround. You can ignore this message.
CSCsa20490	Incomplete WDS configuration causes flood of <i>run now</i> inventory jobs created.	Workaround: Before configuring WDS, you must make sure the access points in your network are discovered and managed in WLSE. If WLSE is unable to discover the WDS access point and the WDS access point is configured with the WLSE server, WLSE attempts to discover the access point that forwarded WDS packets, every 30 seconds.
CSCsa24492	WLSE cannot handle backslashes in some fields.	When using Microsoft Internet Explorer 6.0 on Windows XP, backslashes are not interpreted correctly. For example, if you select Devices > Discover > Credentials > WLCCP > Radius UserName and use a backslash in the user name, Internet Explorer does not remember the user name. Workaround: There is known workaround. This does not occur when using Netscape.
CSCsa26884	Webserver index.html page does not load with localhost.	While upgrading the WLSE software, sometimes the browser does not open when it is launched. Workaround: In the URL, replace <i>localhost</i> with the IP address of the machine or 127.0.0.1.

Table 3 Resolved Caveats in WLSE

Bug ID	Summary	Explanation
CSCee15196	Previous to this release, RM context did not reliably restart an access points when WDS was rebooted.	If a WDS device was rebooted while radio monitoring was turned on for access points registered to that WDS, Radio Monitoring for those access points did not restart.
CSCee30813	Previous to this release, self healing results were not visible until inventory was run.	After Self Healing applied changes to supported access points due to a downed access point, the results of the change were not visible in WLSE until after an inventory run.
CSCee32662	Previous to this release, Radio Manager sent the wrong RM request when non-WDS access points rebooted.	After you ran radio monitoring on a non-WDS access point for 802.11g/b radios and then rebooted the access point, the WLSE sent radio measurement requests for 802.11a radios as well as 802.11g/b radios.

Table 3 Resolved Caveats in WLSE

Bug ID	Summary	Explanation
CSCee39723	Previous to this release, Location Manager coverage was displayed regardless of its operational RIF status.	Location Manager did not display coverage for radios that had active faults on the following items: <ul style="list-style-type: none"> • RF Port Down • RF Port Down by Admin • Radio Down (Self-healing triggered)
CSCsa11677	Previous to this release, invalid selection caused a loop of error messages to be displayed.	When you selected Configure > Templates , entered a name and selected IOS, and clicked Create New Template > Categories > Network Interfaces > Radio 802.11b/g , and selected a channel for Default Radio Channel and clicked a channel from Least Congested Channel Search, an error message appeared saying that the default radio channel must be set to the least congested frequency to modify this field. When you clicked OK , the same error message came up immediately and the operation looped.
CSCsa15394	Previous to this release, WLSE 2.7.0 generated false WDS 0.0.0.0 faults when no WDS was configured.	If an access point was not registered with any WDS, WLSE generates a fault saying the access point 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 access point is registered with an Unmanaged WDS 0.0.0.0, this means the access point is not registered with any WDS.
CSCsa20580	Previous to this release, rogue location estimation failed if the rogue was detected by only one access point.	If you performed radio monitoring on one access point and a Rogue Access Point fault is generated, in Location Manager, the rogue access point location estimation fails.

Table 4 Resolved VxWorks to IOS Conversion Bugs in WLSE

Bug ID	Summary	Explanation
CSCed78655	Previous to this release, configuration conversion from VxWorks to IOS reported an incorrect value.	After converting an access point from Vxworks configuration to IOS configuration, the converted IOS configuration contained an incorrect value. If you tried to apply the converted configuration to an IOS access point, the job failed.
CSCee38616	Previous to this release, the MAC address format became bogus after converting from VxWorks to IOS.	After converting an access point from Vxworks to IOS, the MAC address format in the converted configuration file was incorrect.
CSCsa12094	Previous to this release, configurations were lost when upgrading from a converted IOS access point to IOS.	Configurations were lost when using WLSE to upgrade from converted IOS access points to IOS.

Table 4 Resolved VxWorks to IOS Conversion Bugs in WLSE (continued)

Bug ID	Summary	Explanation
CSCsa12085	Previous to this release, <i>awcDot11UseAWCExtensions = F</i> was not preserved in a VxWorks to IOS conversion.	When an access point was converted from VxWorks to IOS, WLSE did not preserve <i>awcDot11UseAWCExtensions = F</i> . If Aironet extensions were disabled in VxWorks prior to the conversion, after the conversion they were re-enabled.
CSCsa12593	Previous to this release, the authorization and authentication configuration was not synchronized.	In AAA configurations, if you enabled authentication, the following commands were created: <pre>aaa authentication login default group rad_admin aaa authorization exec default local group rad_admin</pre> The AAA authentication was configured to use only group <i>rad_admin</i> ; however, the authorization used <i>local</i> and then <i>rad_admin</i> , which broke login.
CSCsa13569	Previous to this release, VxWorks to IOS conversion added a dot in front of domain name.	When an access point was converted from VxWorks to IOS, a period was added to the beginning of the domain name.
CSCsa16787	Previous to this release, incomplete Eastern time zones were displayed.	For the Eastern time zone setting, the time zone names (-5 and recurring) were missing.
CSCsa17775	Previous to this release, the <i>awcDot11DesiredSSIDMic</i> algorithm was not converted.	MIC and Key-hash parameters were not converted in the encryption configuration.
CSCsa17779	Previous to this release, access point 350 conversions resulted in generation of dot 11 radio 1 commands.	After converting an access point 350, the startup configuration had dot 11 radio 1 commands.
CSCsa18431	Previous to this release, conversion would hang IOS access points if a native VLAN was not mapped to any SSID.	After conversion, the access point would lose network connectivity if a native VLAN was not mapped to any SSID.
CSCsa18948	Previous to this release, the class-map name was limited to 40 characters.	The class-map commands were missing for policy/protocol filter configurations.
CSCsa18954	Previous to this release, conversion added the default commands <i>login local</i> and <i>line con 0</i> .	After conversion, the commands <i>login local</i> and <i>line con 0</i> were generated by default.
CSCsa19914	Previous to this release, address filters were incorrectly converted during conversion.	After conversion, MAC filters were configured with the default value of <i>permit any</i> .
CSCsa20081	Previous to this release, EtherType filter default action could not always be <i>permit any</i> .	For the Ethertype filter, the converted configuration has <i>permit any</i> as the default.
CSCsa20084	Previous to this release, IP protocol faults default actions could not always be <i>permit any</i> .	For the protocol filter, the converted configuration has <i>permit any</i> as the default.

Table 4 Resolved VxWorks to IOS Conversion Bugs in WLSE (continued)

Bug ID	Summary	Explanation
CSCsa20102	Previous to this release, you could not Telnet to an IOS access point after converting from VxWorks.	When you created a conversion job and then tried to Telnet to the access point, the access point indicated that the Telnet lines were not configured with the Telnet line password.
CSCsa20273	Previous to this release, encryption mode was incorrectly set on VLANs after conversion.	VLAN encryption was set to <i>optional</i> instead of <i>mandatory</i> .
CSCsa20330	Previous to this release, WLSE would check free memory on an access point before starting VxWorks to IOS conversion.	If there was not enough available memory in the VxWorks access point, the conversion failed.
CSCsa20561	Previous to this release, a Hostname command with spaces would fail.	The <i>hostname</i> command was missing after conversion if the <i>sysname</i> contained any spaces.
CSCsa20622	Previous to this release, the AAA <i>authentication login default local</i> command was excluded as a result of the conversion if UsrMgr was enabled.	Whenever you converted a VxWorks access point that had the User Manager enabled and operated with at least one user who had all permissions, WLSE did not add the following command in the converted IOS configuration: aaa authentication login default local. Instead, WLSE added the command <i>ip http authentication aaa</i> because user manager was enabled.
CSCsa21112	Previous to this release, the Job Summary page had the wrong MIB variables for Username and User Manager.	After conversion, the MIB variables for Username and Enable User Manager were incorrectly listed in the “VxWorks To IOS Upgrade Security Check” section of the Job Summary page.
CSCsa21117	Previous to this release, Accounting Service Settings were not converted correctly.	The accounting server shared secret information that was not converted during the conversion process.
CSCsa21277	Previous to this release, SSID was disabled after conversion if the Infra-SSID VLAN was not native.	No additional notes.
CSCsa21732	Previous to this release, the HTTP disabled setting was not converted properly.	If the HTTP server setting was disabled under VxWorks and if web-based access to the access point was initially disabled as a security measure, then security could be compromised after the VxWorks to IOS conversion if the access point was web-accessible.
CSCsa22073	Previous to this release, there were confusing messages during repeater conversion failure.	When a repeater was converted, the following failure message was displayed: <i>Ethernet port is not configured as primary port.</i>

Table 4 **Resolved VxWorks to IOS Conversion Bugs in WLSE (continued)**

Bug ID	Summary	Explanation
CSCsa22766	Previous to this release, conversion did not proceed with a dual mode access point with v3 image if there was a memory issue.	Conversion of dual mode access points operating with a v3 image would fail.
CSCsa24586	Previous to this release, access point filters/policies were lost after conversion if the access point was on a slow link.	If an access point was on a slow WAN link, the created IP, IP Port, and EtherType filters and Policy Groups were not converted.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Non-emergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

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

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

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