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

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

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:

CISCO SYSTEMS

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

New Features

The WLSE Release 2.7.1 contains:

- Software support for firmware release 12.2(15)XR.
- Support for WLSM.
- Support for Firmware conversion VxWorks version 12.04 to IOS.

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
Installation and Configuration Guide for the 1130/1105 CiscoWorks Wireless LAN Solution Engine	Describes how to install and configure the WLSE. Available in the following formats: • 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]
Installation and Configuration Guide for the 1130-19 CiscoWorks Wireless LAN Solution Engine	Describes how to install and configure the WLSE. Available in the following formats: • 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]
User Guide for the CiscoWorks Wireless LAN Solution Engine	Describes WLSE features and provides instructions for using it. Available in the following formats: • 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
Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine	Provides regulatory compliance and safety information for the WLSE. Available in the following formats: • 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
Regulatory Compliance and Safety Information for the CiscoWorks 1130-19 Wireless LAN Solution Engine	Provides regulatory compliance and safety information for the WLSE. Available in the following formats: • 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
Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine	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: • 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
Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine, Release 2.7.1	Describes how to convert non-IOS access points to IOS. Available in the following formats: • 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
Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine	Lists the devices supported by WLSE. Available in the following formats: • 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 24.
2. See Obtaining Documentation, page 24.
3. See Obtaining Documentation, page 24.

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 or WAM.

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>
```

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 be 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.

Modifying AP 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 APs that are functional. If this box is checked (default), the coverage for radios that are determined to be down are not displayed.

All other steps in this section are correct.

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.	The Client Historical Association report does not have information about the last time a client associated with the AP, the time it disconnected from the AP, the duration of the association, or the association state. There is no workaround for this problem. **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 AP-based LEAP server to the WLSE if it is already a managed by WLSE.	You cannot add an AP-based Leap server to WLSE if that AP is already being managed by WLSE. The WLSE views it as a duplicate device. There is no workaround for this problem.
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). There is no workaround for this problem.
CSCed89308	RPG Stop Calculation does not work, only when job is rerun.	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. If you are running radio parameter generation for the first time, this problem does not appear. There is no workaround for this problem.

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.	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. There is no workaround for this problem.
CSCee09800 CSCed94324	Detach/IP Address Change events during Roam event stress-2gclient.	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. This problem occurs for certain clients that are authenticated using LEAP and are not using the CCKM fast-roaming feature. To work around this problem, ignore the IP Address Change and the Detach From WDS events if they occur immediately after a Roam event.
CSCee18557	Unable to include filters in policy groups.	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. There is no workaround for this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCee26055	ACS Login Failed Report produces error message.	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. There is no workaround for this problem. You can log in directly to the ACS server and look at the ACS Failed Login Report.
CSCee37875	CCO crypto download changes breaks image import from Cisco.com	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: `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.` To work around this problem, download the image from outside WLSE, then use **Firmware** > **Images** > **Import** > **From Desktop** to import the image into WLSE.
CSCsa12061	Unable to schedule an IOS AP reload.	You cannot reload an IOS AP via a Configuration template. There is no workaround for this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa12358	Wireless Client Detail Report sometimes not showing correct state.	Sometimes the wireless client detail report doesn't show the correct state of the client. In the reports it shows it as *assocAndAuthenticated* when it should show it as *none*. 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.
CSCsa12833	Pushing an unsupported image on AP breaks the AP.	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. There is no workaround to this problem.
CSCsa13094	Editing rule based groups is not recomputed.	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. 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.
CSCsa13695	Devices marked 'd'/Deleted show in Manage/Unmanage search.	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. There is no workaround to this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa13728	The wrong command is reported as failed when an IOS template job that has more than one command fails.	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. 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.

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.	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:
		• Data rates in for 11G
		• CCK Transmitter Power (mW)
		• OFDM Transmitter Power (mW) and
		• Short Slot-Time
		There are two workarounds to this problem:
		• 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:
		`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.

CSCsa14926	TACACS+ secret does not accept dollar sign.	You cannot use the “$” sign in the authentication password. There is no workaround to this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa15540	Inventory does not start for partially successful jobs.	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. 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.
CSCsa16324	If you run CLI "services status" on the standby box, the 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` There is no workaround to this problem. You can ignore this message.
CSCsa20490	Incomplete WDS configuration causes flood of *run now* inventory jobs created.	Before configuring WDS, you must make sure the APs in your network are discovered and managed in WLSE. If WLSE is unable to discover the WDS AP and the WDS AP is configured with the WLSE server, WLSE attempts to discover the AP from whom it heard WDS packets every 30 seconds. There is no workaround to this problem, except to ensure the device community strings are configured correctly.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa24492	WLSE cannot handle backslashes in the 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. There is no workaround to this problem. This does not occur when using Netscape.
CSCsa26884	Webserver index.html page doesn't load with localhost.	While upgrading the WLSE software, sometimes the browser does not open when it is launched. To work around this problem, in the URL, replace *localhost* with the IP address of the machine or 127.0.0.1.

Table 3 Resolved Problems in WLSE

Bug ID	Summary	Explanation
CSCee15196	RM context is not reliably restarted on APs when WDS is rebooted.	If a WDS device is rebooted while radio monitoring is turned on for APs registered to that WDS, after the WDS comes back up, Radio Monitoring for those APs might not restart.
CSCee30813	Self healing results are not visible until inventory runs.	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.
CSCee32662	Radio Manager sends wrong RM request when non-WDS AP reboots.	After you run radio monitoring on a non-WDS AP for radios 11g/b only and then reboot the AP, when the AP comes up, WLSE sends radio measurement requests for both the interface 11g/b and 11a.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCee39723	Location Manager coverage is displayed regardless of operational RIF status.	When there is no radio measurement data (for example, before running Radio Scan, you delete Radio Monitoring or measurement data), coverage display is estimated with the default path-loss model and the transmit power configuration parameter. Location Manager does not display Coverage for radios that have active faults on following items: • RF Port Down • RF Port Down by Admin • Radio Down (Self-healing triggered) **Note** This requires faults to be enabled through the WLSE Fault page. In addition, make sure "Display Coverage for operational radio interfaces only" is checked (default) in Location Manager's Coverage Display Options.
CSCsa11677	Invalid selection causes loop of error messages display.	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.

Table 3 Resolved Problems in WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa15394	WLSE 2.7 generates false WDS 0.0.0.0 faults when no WDS is configured.	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.
CSCsa20580	Rogue location estimation fails if the rogue is detected by only one AP.	If you perform radio monitoring on one AP and a Rogue AP fault is generated, in Location Manager, the Rogue AP location estimation fails.

Table 4 Resolved VxWorks to IOS Conversion Bugs in WLSE

Bug ID	Summary	Explanation
CSCed78655	Configuration conversion from VxWorks to IOS has wrong value.	After converting an AP from Vxworks configuration to IOS configuration, the converted IOS configuration contains an incorrect value. If you try to apply the converted configuration to an IOS AP, the job fails.
CSCee38616	The MAC address format becomes bogus after converting from Vxworks to IOS.	After converting an AP from Vxworks to IOS, the MAC address format becomes bogus in the converted configuration file.
CSCsa12094	Configurations lost when upgrading from converted IOS AP to IOS.	Configurations are lost when using WLSE to upgrade from converted IOS AP to IOS.
CSCsa12085	*awcDot11UseAWCExtensions = F* is not preserved in VxWorks to IOS conversion.	When an AP is converted from VxWorks to IOS, WLSE does not preserve *awcDot11UseAWCExtensions = F*. If Aironet extensions were disabled in VxWorks, after the conversion, they are re-enabled.

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

Bug ID	Summary	Explanation
CSCsa12593	Authorization and authentication are not configured in sync.	In AAA configurations, if you enable authentication, the following commands are created: *aaa authentication login default group rad_admin* *aaa authorization exec default local group rad_admin* The AAA authentication is configured to use only group *rad_admin*; however, the authorization uses *local* and then *rad_admin*, which breaks the login.
CSCsa13569	Conversion adds a dot in front of domain name	When converting an AP from VxWorks to IOS, a period is added to the beginning of the domain name.
CSCsa16787	Wrong clock time zone for Eastern time zone.	For the Eastern time zone setting, the time zone names (-5 and recurring) are missing.
CSCsa17775	awcDot11DesiredSSIDMic algorithm is not converted.	MIC and Key-hash parameters are not converted in the encryption configuration.
CSCsa17779	For AP 350, dot 11 radio 1 commands are generated.	After converting an AP350, the startup configuration has the dot 11 radio 1 commands.
CSCsa18431	Conversion hangs IOS AP if native VLAN is not mapped to any SSID.	After conversion, the AP might lose network connectivity if a native VLAN is not mapped to any SSID.
CSCsa18948	Limit the class-map name to 40 characters.	The class-map commands are missing for policy/protocol filter configurations.
CSCsa18954	Conversion adds the default command login local and line con 0.	After conversion, the commands *login local* and *line con 0* are generated by default.
CSCsa19914	Address Filters are incorrectly converted after conversion.	After conversion, MAC filters have *permit any* as the default.
CSCsa20081	EtherType filter default action cannot always be permit any	For the Ethertype filter, the converted configuration has *permit any* as the default.

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

Bug ID	Summary	Explanation
CSCsa20084	IP protocol faults default action cannot always be permit any.	For the protocol filter, the converted configuration has *permit any* as the default.
CSCsa20102	Cannot telnet to IOS AP after converting from VxWorks.	When you create a conversion job and then try to telnet to the AP, the AP indicates that the telnet lines are not configured with the telnet line password.
CSCsa20273	Encryption mode is incorrectly set after conversion on VLANs.	VLAN encryption is set to *optional* instead of *mandatory.*
CSCsa20330	WLSE should check free memory on an AP before starting VxWorks to IOS conversion.	If there is not enough available memory in the VxWorks AP, the conversion fails.
CSCsa20561	Hostname command with spaces will fail.	The *hostname* command is missing after conversion if the *sysname* contains any spaces.
CSCsa20622	Missing AAA authentication login default local command if UsrMgr is enabled.	Whenever you convert a VxWorks AP that has the User Manager enabled with at least one user who has all permissions, WLSE does not add the following command in the converted IOS configuration: `aaa authentication login default local.` Instead, WLSE adds the command *ip http authentication aaa* because user manager is enabled.
CSCsa21112	The Job Summary page has the wrong MIB variables for Username and User Manager.	After conversion, on the Job Summary page in the “VxWorks To IOS Upgrade Security Check” section, the MIB variables for Username and enable User Manager are incorrectly listed.
CSCsa21117	Accounting Service Settings are not converted correctly.	The accounting server shared secret information is not converted during the conversion process.

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

Bug ID	Summary	Explanation
CSCsa21277	SSID is disabled after conversion if Infra-SSID VLAN is not native.	To work around this problem: 1. Make sure the SSID that is mapped to the Native VLAN is set as infrastructure SSID before starting the conversion. 2. If the conversion has already completed, use WLSE to create an IOS configuration template to remove the command *infrastructure-ssid* from the SSID that is not the Native VLAN SSID.
CSCsa21732	HTTP disabled setting is not converted properly.	Because the HTTP server setting is not converted properly if it is disabled under VxWorks, if web-based access to the AP was initially disabled as a security measure, security could be compromised after conversion if the AP becomes web-accessible.
CSCsa22073	Confusing messages during repeater conversion failure.	When converting a repeater, the following failure message is displayed: `Ethernet port is not configured as primary port.`
CSCsa22766	Conversion does not proceed with a dual mode AP with v3 image if there is a memory issue.	Conversion fails when converting a dual mode AP running a v3 image because of memory issues.
CSCsa24586	Filters/Policies are lost for the AP after conversion if the AP is across a slow link.	If you are using a slow WAN link, after converting an AP from VxWorks to IOS, the created IP, IP Port, and EtherType filters and Policy Groups are 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 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_inpck/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