



# Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.9

---

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) Release 2.9.

These release notes provide:

- [New Features, page 2](#)
- [Product Documentation, page 3](#)
- [Documentation Updates, page 5](#)
- [Known Problems, page 6](#)
- [Obtaining Documentation, page 17](#)
- [Obtaining Technical Assistance, page 18](#)
- [Obtaining Additional Publications and Information, page 20](#)



---

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

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

# New Features

The WLSE Release 2.9 adds support for:

- Hardware platforms: BR1310 configured in AP mode
- Network management support for the AP 1130 802.11 a/b, a/g radios
- Network management support for the new 802.11a radio in the AP 1200 (support for AIR-RM21A 5-GHz radio module; these options are available for 5-GHz clients only.)
- Software support for firmware release 12.3(2)JA and 12.2(15)XR2 12.05 VxWorks
- IP Redirect
- EAP-FAST authentication and authorization protocol
- Fault email notification based on priority
- VLANs by name
- SSL
- WPA2/AES support
- Directional antennas
- Location Manager Building Tool wizard
- TKIP/MIC monitoring



---

**Note**

WLSE 2.9 software is supported on the 1130 and 1130-19 platforms only. WLSE 2.9 is not supported and cannot be installed on the 1105 platform.

---



---

**Note**

WLSE cannot monitor AP-based local AAA server running LEAP or EAP-FAST protocols if that AP is already being managed by WLSE.

---

# 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
<i>Installation and Configuration Guide for the 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"> <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/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a></li> <li>Printed document available by order (part number DOC-7816524=)<sup>1</sup></li> </ul>
<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"> <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/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a></li> </ul>
<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"> <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/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a></li> </ul>

**Table 1 Product Documentation (Continued)**

Document Title	Description
<i>FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine</i>	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: <ul style="list-style-type: none"> <li>• From the WLSE online help.</li> <li>• On Cisco.com:  <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a> </li> </ul>
<i>Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine, Release 2.9</i>	Describes how to convert non-IOS access points to IOS. Available in the following formats: <ul style="list-style-type: none"> <li>• From the WLSE online help.</li> <li>• On Cisco.com:  <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a> </li> </ul>
<i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine</i>	Contains procedures for converting non-IOS access points to IOS access points. Available in the following formats: <ul style="list-style-type: none"> <li>• On Cisco.com:  <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a> </li> </ul>
<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"> <li>• On Cisco.com:  <a href="http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm</a> </li> </ul>
<i>Finding Documentation for the CiscoWorks Wireless LAN Solution Engine</i>	Lists the documents associated with this release of WLSE. Available in the following formats: <ul style="list-style-type: none"> <li>• Printed document included with product.</li> <li>• PDF on the WLSE Recovery CD-ROM.</li> </ul>

1. See [Obtaining Documentation](#), page 17.

# 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:

When using the recovery CD to reimage the WLSE (using the WLSE's CD drive for the reimaging), the flash memory is not erased. Use the *erase config CLI* command, either before or after the reimaging.

## Displaying Wireless Client Reports

You cannot specify start and end dates for the following Wireless Client reports:

- Client Detail
- Client Statistics

## Assigning Self Healing Network Settings

The “Assigning Self Healing Network Settings” subsection in the “Managing Your Wireless LAN Radio Environment” section should be deleted.

## CLI Command Reference Chapter

The following corrections are for the “CLI Command Reference” chapter:

- The *show collectorlog* command should be removed.
- The *apptyp* command should be added. This command displays the type of WLSE hardware.
- For all of the commands that have the *page* option, use the following keys to control the output:
  - Press **Return** to display next line of output.
  - Press the **Space** bar to display the next screen of output.
  - Press **q** or **Q** to exit from paged output and return to the command prompt.

# Known Problems

Table 2 describes problems known to exist in this release. Table 3 describes problems fixed since the last release.


**Note**

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

## WLSE Problems

**Table 2** Known Problems in the WLSE

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	<p>The Client Historical Association report does not have information about the last time a client associated with the AP, the time it disconnected from the AP, the duration of the association, or the association state.</p> <p>There is no workaround for this problem.</p> <p><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.</p>
CSCec41188	You cannot add an AP-based LEAP server to the WLSE if it is already a managed by WLSE.	<p>You cannot add an AP-based LEAP/EAP-FAST server to WLSE if that AP is already being managed by WLSE. The WLSE views it as a duplicate device.</p> <p>There is no workaround for this problem.</p>

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

Bug ID	Summary	Explanation
CSCed94324	Detach/IP Address Change events during Roam event stress-2gclient.	<p>If you select <b>Reports &gt; Wireless Clients &gt; Client EAP UserName or MAC Address &gt; Client Historical Association</b>, sometimes an IP Address Change event is reported immediately after a Roam event, even though no IP address change has occurred for the specified client. In addition, sometimes a Detach From WDS event is reported immediately after a Roam event, even though the specified client has not left the WDS indicated in the previous Roam event.</p> <p>This problem occurs for certain clients that are authenticated using LEAP and are not using the CCKM fast-roaming feature.</p> <p>To work around this problem, ignore the IP Address Change and the Detach From WDS events if they occur immediately after a Roam event.</p>
CSCef90440	A database exception occurs when creating jobs in multiple WLSE sessions.	<p>When you try to create WLSE configuration templates in two separate browser windows simultaneously, one configuration template does not get saved.</p> <p>To work around this problem, create templates in a single browser window at one time.</p>
CSCef97944	Cannot select Bridge- Root and Install mode for 1310 bridges.	<p>When you select <b>Templates &gt; Basic Settings &gt; Radio0-802.11B/G</b>, click the radio button and check box for Bridge Non-Root and Install-Mode, and then click on any of the other links, the following popup message appears:</p> <p>Install mode is applicable for Bridge Root and Non-Root modes only.</p> <p>To work around this problem, apply the commands by using custom templates.</p>

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa35554	Weekly and monthly data aggregation does not happen at the beginning of the week/month.	<p>The first weekly/monthly aggregation does not start at the beginning of the week/month. The first aggregation might happen earlier than the beginning of the week/month.</p> <p>After the first weekly/monthly aggregation, all subsequent weekly/monthly aggregation occurs every 7 days for weekly or every 30 days for monthly aggregation from the first time the aggregation occurred.</p> <p>There is no workaround to this problem.</p>
CSCsa35793	After using the command <b>no http-server accept &lt;ip&gt; &lt;mask&gt;</b> , WLSE redundancy fails.	<p>When you issue the command line interface commands <b>http-server accept &lt;ip&gt; &lt;mask&gt;</b> and <b>no http-server accept &lt;ip&gt; &lt;mask&gt;</b> and then configure the server as a <i>Redundancy Standby</i> server, the redundancy status on the server gets stuck in <i>starting</i> mode from the command line interface and cannot be connected via http (however, it can be connected using https). The redundancy page shows the server as a <i>Standby</i> server, but with the Manage Redundancy option (which should show up if the server is in <i>Active</i> server mode only).</p> <p>There is no workaround to this problem.</p>
CSCsa36237	WLSE aborts active TFTP upgrade when the per-device timeout expires.	<p>WLSE aborts a firmware job when the timeout value expires.</p> <p>To work around this problem, configure the timeout value by selecting <b>Firmware &gt; Advanced Parameters</b> and changing the Per device job operation timeout value to a higher value.</p>

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

Bug ID	Summary	Explanation
CSCsa36966	Images imported for AP350 and AP1200 are missing the 12.05 link.	<p>The firmware images for version 12.05 are not listed for AP350 and AP1200 devices when you try to import from Cisco.com.</p> <p>To work around this problem, import the version 12.05 image from the desktop.</p>
CSCsa38974	QoS policies with WMM generate CLI with DISAB.	<p>When you create a new Services: QoS Policies 802.11b/g template under <b>Configure &gt; Templates</b>, if DISAB appears in the Transmit Opportunity column, you cannot apply the template to any devices.</p> <p>To work around this problem, remove the DISAB value from the Transmit Opportunity column before saving the configuration template.</p>
CSCsa39732	Switches, when pointed at, display radio port information.	<p>If you select <b>Reports &gt; Current &gt; Device Type &gt; Switches</b> and point your cursor at the switches in that group, radio port information is displayed. The switches do not have radio ports and this information should not be displayed.</p> <p>There is no workaround to this problem.</p>
CSCsa39738	The VxWorks template for dot11CurrentRxAntenna.2 is not handled well.	<p>When you create a Vxworks template and go to the 11b Radio Hardware page, select Receive Antenna as Diversity, and save the template, the following error message appears:</p> <p>Following key-value(s), in the current configuration template, are not supported:  Key: dot11CurrentRxAntenna.2  Value: diversity</p> <p>To work around this problem, add the configuration command in the custom template.</p>

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

Bug ID	Summary	Explanation
CSCsa39854	WLSE deletes lines with “!” in the template.	<p>If you have an exclamation point (!) in the IOS command line interface (for example, <code>snmp-server community pub!!lic RO</code>), WLSE deletes the lines with the “!” character when importing the configuration or when the archived configuration file containing the “!” character is exported as a configuration template.</p> <p>To work around this problem, edit the custom command section of the template by manually adding the lines containing the “!” character.</p>
CSCsa41193	Archive shows the type as Non-IOS and exporting the template fails.	<p>If you have a pound sign (#) in the IOS configuration, for example, <code>snmp-server community pub#lic ro</code>, and you select <b>Configure &gt; Archives &gt; View Archive</b> and select Export to Template, the job fails and you get an error message. The View Archive screen shows the type as non- IOS even for APs running IOS images.</p> <p>There is no workaround to this problem.</p>

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

Bug ID	Summary	Explanation
CSCsa42074	TACACS server configuration is not supported by WLSE	<p>When you try to save your TACACS+ server configuration, WLSE gives you the following error:</p> <pre>Error processing configuration / No valid device versions supported.</pre> <p>To work around this problem, copy the command line interface command from Preview, paste it into the Custom Configuration, then save the template.</p>
CSCeg84720	The AP 1210 automanage criteria needs a change from 2.7 to 2.9.	<p>During an upgrade from Release 2.7 to 2.9, the AP 1210 Device Type auto-manage criteria will not work for AP 1210 devices with a single radio.</p> <p>In the WLSE 2.9 release, AP 1210 device type criteria will match with devices with a dual radio only. There is a new criteria defined for AP 1210 devices with single radio AP 1210-SR.</p> <p>To work around this problem, Edit the auto manage criteria for the auto manage template to include both AP 1210 (for dual radio) as well as AP 1210-SR (for single radio) device types.</p>

**Table 3** Resolved Problems in WLSE

Bug ID	Summary	Summary
CSCed55402	When you set the WEP Enforced policy under <b>Faults &gt; Manage Faults</b> , 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).
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.

**Table 3 Resolved Problems in WLSE**

Bug ID	Summary	Summary
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.
CSCee33980	WLSE 2.5 configuration template shows WEP key in clear text.	The VxWorks export configuration template does not export the WEP key and the field is blank. When you type in the WEP key, because you need it to save the template, it shows what you are typing in clear text.
CSCee37875	CCO crypto download changes breaks image import from Cisco.com.	<p>When you select <b>Firmware &gt; Images &gt; Import &gt; From Cisco.com</b>, log in with your CCO account, and select any AP image, you get the following error message:</p> <p>Error while selecting or displaying image details. Please log into cisco.com at <a href="http://www.cisco.com/cgi-bin//Software/Crypto/crypto_main.pl">http://www.cisco.com/cgi-bin//Software/Crypto/crypto_main.pl</a> and make sure your username has acknowledged cryptography permissions for downloading IOS Aironet images.</p> <p>To work around this problem, download the image from outside WLSE, then use <b>Firmware &gt; Images &gt; Import &gt; From Desktop</b> to import the image into WLSE.</p>
CSCee44487	The user password in the GUI does not take special characters.	If you select <b>Administration &gt; User Admin &gt; Manage Users</b> and add a new user or modify an existing user, the user's password under the Change Password field does not accept any special characters such as, !@#\$\$%^&*(),.
CSCee70697	Community string *.*.* stays at the top in device credentials.	You cannot configure different community strings for the APs because the line *.*.* remains at the top and matches everything. You cannot remove or modify the line *.*.*, and whatever is added after it is ignored.

**Table 3 Resolved Problems in WLSE**

Bug ID	Summary	Summary
CSCee81819	Telnet login to the APs failed when configured with a long banner string.	<p>If an AP's configuration has a multiline banner, WLSE fails when you attempt to push a configuration change and you get the following error message:</p> <pre>Login failed [<i>Failed login</i>]. Error applying new configuration. Aborting configuration for device.</pre>
CSCee86956	Password change using the My Profile feature is not functional.	<p>If you log in as an administrator and create a user, assign the user the role of network administrator with CLI access <i>0</i> privilege <i>Now</i>, attempt to log in as the newly created user with administrator-assigned password, and then attempt to change the password, you will be informed it is successful. However, if you attempt to log in using the changed password, the login fails. You are unable to change the initial password assigned by the WLSE administrator.</p>
CSCee96424	The GUI Username field does not allow a backslash.	<p>You cannot have a backslash (\) in the Username field under <b>Administration &gt; User Admin &gt; Manage Users</b>.</p>
CSCef00829	WLSE produces an error when processing configurations. No valid device versions are supported.	<p>When you create and save an IOS configuration template, modify the template, and then click <b>Save</b>, you get the following error:</p> <pre>Error processing configuration. No valid device versions supported.</pre>
CSCef02875	Loading Devices operation freezes WLSE under rare circumstances.	<p>When selecting menus in WLSE which require the <i>Loading Devices</i> operation to execute, for example, <b>Devices &gt; Group Management</b> or <b>Reports &gt; Device Center</b>, the web interface might eventually freeze.</p>

**Table 3 Resolved Problems in WLSE**

Bug ID	Summary	Summary
CSCef14858	Authentication module settings not carried over to Standby HA box.	After a switchover operation, the configured settings in the HA active appliance do not get carried over to the newly active HA appliance.
CSCef24413	Loading devices and group add/delete is slow if there is a high number of groups.	When you have a high number of groups (for example, several hundred) in WLSE, the Loading Devices operation and the add/delete group operations are very slow. (Latency can range from 1 to 10 minutes.)
CSCef51482	<b>Reports &gt; Device Center</b> shows a red x for the backup WDS with no faults.	If you select <b>Reports &gt; Device Center</b> , a red x is displayed for the WDS Backup even after you have cleared any faults.
CSCef63314	Restore fails due to improper directory listing by the FTP server.	Backup/restore fails for WLSE 1105/1130 running 2.7.1 if you are using a nonstandard FTP application.
CSCsa12094	Configurations are lost when upgrading from converted IOS AP to IOS.	Configurations are lost when you use WLSE to upgrade from a converted IOS AP to IOS.
CSCsa13553	System Admin users are not authorized to use debug functions.	Only admin users can use the debug tools. System administration users other than admin cannot use debug tools.
CSCsa13569	Conversion adds a dot in front of domain name.	When converting an AP from VxWorks to IOS, a period gets added in front of the AP domain name.
CSCsa14926	TACACS+ secret does not accept the dollar sign.	You cannot use the dollar sign (\$) in the <b>auth</b> command.
CSCsa18431	Conversion hangs IOS AP due to native VLAN not being mapped to any SSID.	After converting an AP from VxWorks to IOS, the AP loses network connectivity because the native VLAN is not mapped to any SSID.
CSCsa20060	Registration error fault is not really disabled.	If you have an AP registered with an unmanaged WDS, 0.0.0.0 keeps getting generated even though the Registration error fault is disabled by default.

**Table 3** Resolved Problems in WLSE

Bug ID	Summary	Summary
CSCsa20490	Incomplete WDS configuration causes flood of <i>run now</i> 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.
CSCsa21669	The password needs to be reentered every time a user is modified.	When you modify a user, a pop window appears with the following message:  Password must only contain numbers, letters, or underscores.  You must re-enter the password.
CSCsa22255	Telnet/SSH credentials break if a backslash is used in the password.	If you use a backslash (\) in the Telnet password credentials in the WLSE telnet/ssh/user/password credentials, the credentials page is unusable. You are not able to add, delete, or modify any Telnet credential entries.
CSCsa23396	Upgrade should clean inconsistent SNMP community wildcards.	If you have multiple *.*.* entries in the SNMP credentials, and you upgrade the WLSE appliance to WLSE 2.7, the redundant entries cannot be deleted after the upgrade.
CSCsa25039	WLCCP password does not allow pound sign.	If the WLCCP password contains a pound sign (#), WLSE cannot authenticate to WDS. The ACS log displays the error:  Radius extension DLL rejected user.
CSCsa25784	You cannot schedule an import from a CiscoWorks job.	You cannot schedule an import from CiscoWorks, even though the option to schedule it is available in WLSE.

**Table 3 Resolved Problems in WLSE**

Bug ID	Summary	Summary
CSCsa26884	Webserver index.html page doesn't load with localhost.	<p>While upgrading the WLSE software, sometimes the browser does not open when it is launched.</p> <p>To work around this problem, in the URL, replace <i>localhost</i> with the IP address of the machine or 127.0.0.1.</p>
CSCsa29682	The /var /opt partition is full and there is no way to clean it up.	The /var or /opt directories are 100% full.
CSCsa30739	WLSE 1130 does not let you add more than 525 devices.	<p>In some cases, WLSE 1130 might not allow you to manage more than 525 devices. When you try to manage the 526th discovered device, you get the following message:</p> <p>Managed device limit has been reached. Unable to manage more devices.</p>
CSCsa32339	WLSE allows user creation starting with numeric character, but this should not be valid.	WLSE allows you to create a username that starts with a numeric character (for example, 1 or 2), however you cannot log in to WLSE using that username.
CSCsa32766	A username that starts with number cannot be added properly.	If you have a username that starts with a number, the username gets added but you cannot log into the WLSE GUI using the credentials. You get an error indicating the password is incorrect.
CSCsa33203	WLSE fails to deliver Multiline banner configuration to IOS APs.	When you create a multi-line banner configuration template, WLSE does not show the configuration under preview. Further, WLSE attempts to push the configuration to the extent that Telnet/ssh is successful and <i>config t</i> is entered. Beyond this point, nothing happens and WLSE reports that the job has successfully completed.

# 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](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

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

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

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

# Documentation Feedback

You can submit e-mail comments about technical documentation to [bug-doc@cisco.com](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.

## 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>

