Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.11

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE) Release 2.11.

These release notes provide:

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

New Features

The WLSE Release 2.11 contains support for:

- Deployment on the following hardware platforms: 1130-19, 1130, and 1030
- Wizard for ease of deployment on APs
- Software support for:
  - IDS feature set, which includes:

    IDS profile

    IDS faults

    IDS summary

    Excessive Management Frame Detection

    MIC/Encryption Failures

    EAPOL Flooding

    MAC address spoofing

    Protection failure per client
  - Auto Radio Monitoring
  - Frame Monitoring
  - Support for third-party IDS servers through an XML interface
  - DFS
  - Radio Management configuration via XML
  - Improved Switchport Tracing algorithm
  - RSSI based Rogue detection
  - Better Rogue/Friendly management
  - Faster RPG computation
  - Poll- and event-based Self Healing
  - Location Manager enhancements
  - Fault notification enhancements

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 the WLSE Release 2.11:

Table 1 Product Documentation

Document Title	Available Formats
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_11/index.htm • Printed document available by order (part number DOC-7816778=)[1]
Installation and Configuration Guide for the 1030CiscoWorks Wireless LAN Solution Engine Express	Describes how to install and configure the WLSE Express. 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_11/index.htm • Printed document available by order (part number DOC-7816779=)[2]

Table 1 Product Documentation (Continued)

Document Title	Available Formats
Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine	Provides regulatory compliance and safety information for 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_11/index.htm
Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express	Provides regulatory compliance and safety information for the WLSE Express. 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_11/index.htm
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_11/index.htm
Upgrading CiscoWorks Wireless LAN Solution Engine Software	Describes the options available and how to upgrade to the WLSE system software to release 2.11. 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_11/index.htm

Table 1 Product Documentation (Continued)

Document Title	Available Formats
FAQ and 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_11/index.htm
Converting Access Points to IOS, CiscoWorks Wireless LAN Solution Engine	Describes how to convert non-IOS access points to IOS. Available in the following formats: • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm
Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine	Contains procedures for converting non-IOS access points to IOS access points. Available in the following formats: • On Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/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_11/index.htm
Finding Documentation for the CiscoWorks Wireless LAN Solution Engine	Lists the documents associated with this release of WLSE. Available in the following formats: • Printed document included with product. • PDF on the WLSE Recovery CD-ROM.

1. See Obtaining Documentation, page 20.
2. See Obtaining Documentation, page 20.

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:

Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express

In the "Product Overview" chapter, the rack mounting shelf should be listed as an optional component and not as part of the equipment included in the package.

In the "Configuration File Reference" appendix, the Example .XML File section should contain the following text:

```
<ApplianceSettings sshProtocol="SSH1_SSH2" webTimeoutInSeconds="1800"
httpServerPort="1741" telnetEnabled="YES"/>
<CLIBlock>
  <CLI command="username admin password blender privilege 15"/>
  <CLI command="auth cli radius secret 192.168.2.131 192.168.2.132"/>
  <CLI command="http-server port 1741"/>
  <CLI command="auth http radius secret 192.168.2.131 192.168.2.132"/>
</CLIBlock>
        <SplashScreenMessage enabled="YES" message="*****Welcome to
the NEW mini-WLSE*****"/>
    </Administration>
    <APLocations>
```

Deployment Wizard

In the "Setting Up the WDS" section, in Step 6, the example given for the subnet address is incorrect. The subnet address in the example is 172.10.10.0/255.255.255.0. The correct format is 172.10.10.0/24.

In the "Deploying the Configuration" section, the Subnet field is incorrect. The following note should be removed: "You can assign only one subnet per configuration."

Known Problems

Table 2 describes problems known to exist in this release. Table 3 describes problems resolved 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/EAP-FAST 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.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCeg84720	AP 1210 automanage criteria needs a change from 2.7 to 2.9, and 2.7 to 2.11.	During an upgrade from Release 2.7 to 2.9 and 2.7 to 2.11, the AP 1210 Device Type auto-manage criteria will not work for AP 1210 devices with a single radio. In the WLSE 2.9 and 2.11 releases, 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. 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.
CSCef90440	A database exception occurs when creating jobs in multiple WLSE sessions.	When you try to create WLSE configuration templates in two separate browser windows simultaneously, one configuration template does not get saved. To work around this problem, create templates in a single browser window at one time.
CSCeh06754	Radio Monitoring is not enabled after rebooting a 350 AP.	After rebooting a 350 AP, if you do *show wlccp ap rm*, Radio Monitoring is not enabled on the AP even though it is enabled from WLSE. To work around this problem, re-enable Radio Manager from WLSE.
CSCeh36880	RPG progress bar should show % completion progress as well.	The radio parameter generation function in WLSE should display a percentage completion (for example, 10% complete) in the progress bar to indicated that it is running and not hanging. Currently, there is only a progress bar which often gives a false impression that RPG is hung because it can take a very long time to complete the calculations. There is no workaround to this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCeh39607	Cannot disable fault polling on WEP Encryption per VLAN fault.	After you enable the fault polling on the *WEP Encryption per VLAN* fault, you cannot subsequently disable fault polling on this particular fault due to an error message that is generated. There is no workaround to this problem.
CSCei04672	Exporting devices to CiscoWorks LMS 2.5 fails.	You cannot export devices to CiscoWorks LMA 2.5. When you try to export devices, you get the following error message: `Could not connect to CiscoWorks Server.` There is no workaround to this problem.
CSCsa35554	Weekly and monthly data aggregation does not happen at the beginning of the week/month.	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. 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. There is no workaround to this problem.
CSCsa45830	AP is shown in Monitor mode after Scanner mode is disabled and inventory is done.	If an AP is converted from Scanner mode to any non-Scanner mode while Frame Monitoring is still requested from that AP, no Fault is generated to warn the administrator of this erroneous network configuration. To work around this problem, place the AP back into Scanner mode or remove it from the Frame Monitoring list.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa48733	Selecting a building from the device tree selects nothing.	When creating a Radio Manager job such as an AP Scan, if you select the building in which the APs reside as the *selected devices*, no devices are selected when the job is run. Devices are selected when the floor or an explicit AP is selected only. This occurs in AP Radio Scan, Assisted Configuration, and Radio Monitoring. To work around this problem, select the explicit APs in the Select Devices step for Assisted Configuration and Radio Monitoring.
CSCsa57270	AP350 EMF does not always start when enabled on WLSE.	When WDS reboots, 350 APs might not start Excessive Management Frame (EMF) detection. To work around this problem, perform one of these actions: • Locate the IDS profile where the device belongs and reapply EMF settings. • Remove the device and then add it back to the Radio Monitoring list to enable EMF.
CSCsb07984	WLSE fails to import devices from RME 4.0.	You cannot import devices from CiscoWorks RME 4.0 to WLSE 2.11. When you try to import devices, you get an error message in the jobvm.log file. There is no workaround to this problem.
CSCeh60102	Rogue AP Fault description before/after upgrade is incorrect.	During a 2.9.1a to 2.11 upgrade, the description for rogue AP faults changes: Before: “Device is rogue access point”. After: “Device state is rogue access point”. No workaround is required.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa63479	After logging in, the WLSE GUI gets stuck on the Loading... screen.	Because the tomcat process does not attempt to re-start, when you log in to the WLSE, the GUI gets stuck on the *Loading ...* screen indefinitely. To work around this problem, ensure the gateway is up, and reboot the WLSE.
CSCsa67792	Backup schedule is not synced up after a switchover.	The backup schedule does not sync up after a switchover. To work around this problem, set the backup schedules on both WLSE systems before enabling HA. The backup will then run from the active server when HA is enabled.
CSCsa67922	Unable to import MAC address from file in Solaris.	In Japanese Solaris clients, the MAC address list can not be imported into the advanced Discover options. The problem doesn't occur in Windows client. There is no workaround to this problem.
CSCsa68100	HA related faults are not generated when the standby becomes active.	When the Standby WLSE becomes the active WLSE, it fails to generate the corresponding HA (High Availability) related fault. However, the active WLSE can still generate all other non-HA related faults on the APs, switches, and routers. There is no workaround to this problem.
CSCsa68203	RPG parameters are not applied when they are scheduled using XML.	The RPG jobs that are created using XML are being executed, but the results are not applied. This only happens when RPG Jobs are created using XML. To work around this problem, use MOM to schedule the jobs.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa68758	Wizard: Need to add an error message for incorrect an WDS setting.	There is no error message if you enter the incorrect WDS setting. To work around this problem, make sure you enter the WDS MAC address and that the managed subnet is in the proper format, for example, *000b5f210426 192.168.3.0/24* where the first number is the WDS MAC address and the second number is the managed subnet address with a slash and the number of bits in the netmask. The example shows managed subnet of 192.168.3.0 with the number of bits in the netmask as 24.
CSCsa68778	WLSE switchover time is not updated on consecutive switchovers.	WLSE Switchover time is not updated on consecutive switch-overs. There is no workaround to this problem.
CSCsa71449	MIB walk on appliance returns the wrong values when the services stop.	MIB walk on c*haRedundancyState* returns as *active* even after issuing the **services stop** command on the active WLSE. To work around this problem, shut down the WLSE in a different way rather than issuing the **services stop** command.
CSCsa76310	Need to run Inventory after WLSE upgrade/restore from earlier version	After the upgrade/restore of WLSE from 2.7, 2.7.1, 2.9, or 2.9.1a to 2.11, all managed APs might not participate in Radio Management operations. Managed APs do show up in the HTML device selection lists, but they do not show up on the floors of Location Manager. The workaround is to manually start an inventory job on all managed devices after the upgrade is completed. Then you should verify that all the APs show up in Location Manager.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa79473	Need to change the maximum transmit (Tx) power level based on the antenna for ETSI.	The recommended transmit power by RPG and Self-Healing might potentially violate ETSI regulatory domain if you are using a high gain antenna, although it is not likely. To work around this problem, set the maximum power in the RPG Constraints/Goals section as one of the following: • For 2.4 GHz: 25 mw (antenna gain 5.2 - 6 dB), 13 mw (antenna gain 6.1 - 9 dB), 8 mw (antenna gain 9.1 - 10 dB). • For 5 GHz: 32 mw (antenna gain 6 - 7 dB), 13 mw (antenna gain 7.1 - 9.5 dB).
CSCsa79506	If a switch has multiple IP addresses, port suppression may fail.	If a switch has multiple IP addresses, port suppression might fail. In order for a switchport to be suppressed, the switch must be in the *Managed* state. If a switch has multiple IP addresses, WLSE stores only one IP address. If WLSE discovers the rogue on a different VLAN on the same switch with a different IP address (other than the one stored in WLSE), WLSE does not suppress the port because this IP address is not in the database. To work around this problem, manually suppress the switchport from the Rogue Details screen.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa78453	WLSE generates the PSPF disabled per radio interface fault when PSPF is configured per VLAN.	When PSPF is configured per VLAN on an AP, WLSE needs to poll a different MIB object (*cd11IfVlanPsPacketForwardEnable*). WLSE does not take into account that PSPF is enabled per VLAN on an AP and still polls the MIB object *cd11IfPsPacketForwardEnable*, which corresponds to the PSPF configuration per radio interface. Consequently, WLSE erroneously generates a PSPF disabled per radio interface fault for an AP even though the PSPF is enabled per VLAN on that AP. There is no workaround to this problem.
CSCsa80570	HA machines are in the starting state when the master file has the wrong password.	After the master file is applied, the HA machines are in the *starting* state and when you log in, you see the Admin tab only. This occurs because the master file has an incorrect password for the redundancy settings. If the passwords do not match in the startup configuration file, then HA will not be configured. To work around this problem, enable Redundancy again from the WLSE.
CSCsa83428	Devices do not appear in Location Manager if they are unreachable during an upgrade.	After upgrading from WLSE 2.7 to WLSE 2.11, APs that appeared in the WLSE 2.7 Location Manager floor map do not show up in the WLSE 2.11 Location Manager. This happens to devices that are unreachable during the upgrade or devices that have a validation fault against them. To work around this problem, before you upgrade, make sure there are no unreachable or validation faults against the devices.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa83869	Packet errors do not show up in the trends graph.	The real time reports show the percentage of packet errors, but in the trends graph the packet error percentage rate is zero. To work around this problem, view the packet error rate in the real time reports.
CSCsa84004	"Device not found" window appears even though rogue location is displayed.	When the user selects **View Location in Location Manager** from the Rogue Report Details window, the message "device not found" is displayed while Location Manager is being launched (the launching functionality is not affected). The workaround to this problem is to ignore or close the window containing the "device not found" message.
CSCsa84440	Unknown Radio Location does not show probability of less than 30%.	Symptom: When a rogue is selected for the Unknown Radio Location display, no area in the map is highlighted for the location probability. If the estimated probability is less than 30%, it will not be displayed. This is due to the algorithm change in WLSE 2.11 that makes values lower than 30% more significant than in prior releases. There is no workaround to this problem.
CSCsa86661	RM Scan job runs and logs not preserved after upgrade.	Radio scan job logs are not visible for historical runs when upgraded from 2.7, 2.7.1, 2.9, or 2.9.1a to 2.11. The job run and job log is not used for any Radio Management computation. The details help to determine when the job ran and if any errors occurred. The data that is lost does not impact any RM functionality run on WLSE 2.11 after an upgrade/restore. There is no workaround to this problem.

Table 2 Known Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa93623	Pre-patch before you upgrade to WLSE 2.11 from WLSE 2.7, 2.7.1, 2.9 and 2.9.1a.	When you upgrade from WLSE 2.7, 2.7.1, 2.9 or 2.9.1a to WLSE 2.11, you might encounter the following problems: • Some database tables are not trimmed, which might cause the database tables to grow very large over a period of time. The log file (swan.log/jobvm.log/tomcat.log) shows transaction log full messages. • Thousands of Unmanaged radios might appear and cannot be deleted. • Deleted floors are not cleared from some tables, which might cause the upgrade to fai1. After upgrading, radio parameter generation, self healing, and auto re-site survey generate runtime errors. To workaround this problem, you must install the WLSE-2.x-CSCsa93623 patch before you upgrade to WLSE 2.11 from any of these WLSE releases: 2.7, 2.7.1, 2.9 or 2.9.1a. Running this patch does not correct the root cause, but the patch eliminates the database inconsistency and allows you to upgrade to WLSE 2.11. **Note** We strongly recommend that you back up your database after installing the patch and *before* you upgrade to WLSE 2.11. Delete all old backups as they contain incorrect data. After you install the patch, if you continue to run WLSE 2.7, 2.7.1, 2.9, or 2.9.1, the issues addressed by the patch will recur.

Table 3 Resolved Problems in the WLSE

Bug ID	Summary	Explanation
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.
CSCeg09569	The template GUI does not check for incompatible encryption type.	When you configure Authenticated Key Management options as *WPA* or *CCKM* from **Configure > Templates > Security > SSID 802.11b/g/a**, and you do not configure the Encryption Modes option as *Cipher* under **Configure > Templates > Security > WEP 802.11b/g/a**, the device reports the following error: `Dot11Radio0 Error: Encryption mode cipher is not configured.`

CSCeg17204	Incorrect CLI command is generated when the AAA group name has a space character.	When the AAA group server name contains spaces, for example *aaa group server radius rad_eap* instead of *rad_eap*, the following incorrect CLI command is generated:
		
		`aaa group server radius aaa group server radius rad_eap`
		
		The correct group name should be “rad_eap” to generate following CLI command:
		
		`aaa group server radius rad_eap`

Table 3 Resolved Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCeg46075	Incorrect IOS version is listed for 2.9 RM operations.	Radio Management operations in WLSE require the APs to be running the latest 12.3(2)JA IOS version. Older versions, including 12.2(15)JA, do not work.
CSCsa35793	After using the command **no http-server accept <ip> <mask>**, WLSE redundancy fails.	When you issue the command line interface commands **http-server accept <ip> <mask>** and **no http-server accept <ip> <mask>** and then configure the server as a *Redundancy Standby* server, the redundancy status on the server gets stuck in *starting* 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 *Standby* server, but with the Manage Redundancy option (which should show up if the server is in *Active* server mode only).
CSCsa39732	Switches, when pointed at, display radio port information.	If you select **Reports > Current > Device Type > Switches** 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.

CSCsa39738	The VxWorks template for dot11CurrentRxAntenna.2 is not handled well.	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:
		`Following key-value(s), in the current configuration template, are not supported:`
		`Key: dot11CurrentRxAntenna.2`
		`Value: diversity`

Table 3 Resolved Problems in the WLSE (Continued)

Bug ID	Summary	Explanation
CSCsa39854	WLSE deletes lines with "!" in the template.	If you have an exclamation point (!) in the IOS command line interface (for example, `snmp-server community pub!!lic RO`), 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.
CSCsa41193	Archive shows the type as Non-IOS and exporting the template fails.	If you have a pound sign (#) in the IOS configuration, for example, `snmp-server community pub#lic ro`, and you select **Configure > Archives >View Archive** 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.
CSCsa42074	TACACS + server configuration is not supported by WLSE	When you try to save your TACACS+ server configuration, WLSE gives you the following error: `Error processing configuration / No valid device versions supported.`

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/univercd/home/home.htm

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

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/

- 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 1 800 553-NETS (6387).

Documentation Feedback

You can send 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.

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
- Non emergencies—psirt@cisco.com

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 that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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

- *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

- 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