



Cisco Unified IP Phone 7970G and 7971G-GE Release Notes for Firmware Release 8.0(3) for Cisco Unified CallManager 5.0, 4.2, 4.1, 4.0, and 3.3 (SCCP)

May 17, 2006

Use these release notes with a Cisco Unified IP Phone 7970G and 7971G-GE running SCCP firmware release 8.0(3) and Cisco Unified CallManager releases 5.0, 4.2, 4.1, 4.0, and 3.3.

You might need to notify your users about some of the information provided in this document.

Contents

These release notes provide the following information.

- [Related Documentation, page 2](#)
- [New and Changed Information, page 2](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 6](#)
- [Caveats, page 8](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 13](#)
- [Cisco Product Security Overview, page 13](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 16](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Related Documentation

Cisco Unified IP Phone Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified CallManager release. Navigate from the following documentation URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Cisco Unified CallManager Documentation

Refer to the Cisco Unified CallManager Documentation Guide and other publications specific to your Cisco Unified CallManager release. Navigate from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

New and Changed Information



Note

Cisco Unified IP Phone firmware release 8.0(3) supports several releases of Cisco Unified CallManager, including the latest releases—4.2 and 5.0. For a complete list of new and changed phone features introduced in these Cisco Unified CallManager releases, refer to the Release Notes for Cisco Unified CallManager 4.2 and the Release Notes for Cisco Unified CallManager 5.0. See the “[Related Documentation](#)” section on page 2 for help locating these documents.

The topics below contain new and changed information about features that are introduced in Cisco Unified IP Phone firmware release 8.0(3) for SCCP phones, but that are not documented in the latest release of the Cisco Unified IP Phone SCCP Administration Guide or User Guide for your phone model.

This section contains these topics:

- [DTMF Transport, page 2](#)
- [Hold Reversion, page 3](#)
- [Optimizing SCCP Messages, page 4](#)
- [Additional Device Information on the Web, page 4](#)
- [Call History Management Improvements, page 4](#)

DTMF Transport

Firmware release 8.0(3) supports DTMF Transport. DTMF Transport transmits RTP packets in band for each digit pressed during a call, according to RFC2833. This feature allows an SCCP endpoint to interwork with a SIP endpoint or gateway.

Hold Reversion

Feature Summary



Note

The Hold Reversion feature requires Cisco Unified CallManager release 4.2(1) SR1.

Firmware release 8.0(3) supports the Hold Reversion feature, which limits the amount of time that a call can be put on hold before reverting back to the phone that put the call on hold and alerting the user.

A reverting call can be distinguished from a new incoming call by the ring cadence, among other indicators. Reverting calls ring once, using the ring tone already set for that phone line. (If the line is configured to use another new call indicator, such as a flash or beep, the reverting call will be indicated according to the same setting.) If the reverting call continues to hold, the single ring repeats at intervals, as determined by the Hold Reversion Notification Interval setting (described below).

In addition, reverting calls are indicated by:

- The animated Hold Reversion icon—Displays in the call bubble of the held call.
- The “Hold Reversion” status line message—Appears for several seconds following each alert.
- A flashing amber line button—Occurs if the line state is reverting.

Administration Configuration Tips

Cisco Unified CallManager Administration provides these clusterwide system parameters:

- Hold Reversion Duration (0-1200 seconds)—Enables/disables Hold Reversion and determines how long a call can be placed on hold before reverting. The default value is 0. You must enter a value greater than 0 to enable Hold Reversion. You can also set this parameter for a specific directory number on the Directory Number Configuration window, which takes precedence over the system parameter.
- Hold Reversion Notification Interval (0-1200 seconds)—Enables/disables subsequent periodic alerts for a reverting call and determines the interval between alerts. The default setting is 30 seconds. (In this case, subsequent notification would occur every 30 seconds after the initial alert until the phone user resumed the call.) You must enter a value greater than 0 to enable subsequent periodic alerts.

With Cisco Unified CallManager release 4.2(1) SR1, the phone screen focus is configured to always display a new incoming call, even when a reverting call is present. On the phone, you can view the call focus setting by choosing Settings > Device Configuration > UI Configuration > Reverting Focus Priority. In this release, the value is “Lower,” indicating that the reverting call focus is a lower priority than the incoming call focus.

User Tips

When you put a call on hold, you have a limited time to resume the call before the Hold Reversion feature reverts the held call back to your phone and alerts you. The time limit is determined by your system administrator.

Your phone alerts you about a reverted held call by producing a single ring (or beep, flash, or other indicator, depending on how your phone normally indicates new calls on this line.) Your phone also displays an animated Hold Reversion icon next to the caller ID for the held call. If you do not answer the held call, the alert can repeat at intervals determined by your system administrator.

To resume the call on the currently displayed line, make sure the reverting call is highlighted, then pick up the handset or press any of the following: the **Resume** softkey, the speaker button (if unlit), or headset button (if unlit).

To resume the call on a different line, press the appropriate line button. If several reverting calls are holding on that line, your phone resumes the oldest reverting call.

If you use a shared line, Hold Reversion rings only on the phone that put the call on hold, not on the other phones that share the line.

Optimizing SCCP Messages

Firmware release 8.0(3) supports improved SCCP messaging to optimize bandwidth for customers who deploy large numbers of phones that share the same line. In SCCP Version 9, SCCP message structures are altered to allow variable length messages instead of a fixed length character-array that consumes bandwidth.

Additional Device Information on the Web

Firmware release 8.0(3) supports additional items in the Device Information area on the phone's web page, including Cisco Unique Device Identifier (UDI) information.

To view the phone's web page, open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone: `http://IP_address`.

[Table 1](#) shows the new Device Information items introduced in the 8.0(3) firmware load.

Table 1 Additional Device Information Area Items Supported by 8.0(3)

Item	Description
UDI	Displays the following Cisco Unique Device Identifier (UDI) information about the phone: Device Type—indicates hardware type. For example, <i>phone</i> displays for all phone models Device Description—displays the name of the phone associated with the indicated model type Device Model—specifies the phone model Device Version Identifier—represents the hardware version of the phone Device Serial Number—displays the phone's unique serial number
Time	Time obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs
Time Zone	Timezone obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs
Date	Date obtained from the Date/Time Group in Cisco Unified CallManager to which the phone belongs

Call History Management Improvements

Firmware release 8.0(3) supports several call history management improvements to give phone users more options for managing call logs. These improvements include:

- Line associations for missed, placed, and received calls—Allows phone users to see which phone line a missed or received call was intended for, and which phone line was used to place an outgoing call. This option is relevant for users who have multiple phone lines.
- Delete all records in a particular log—Allows phone users to delete all of the records in the displayed call log (Missed Calls, Placed Calls, or Received Calls).

- Delete an individual call record—Allows phone users to delete the highlighted call record in any call log.
- Call duration for placed and received calls—Allows phone users to see the call duration for the highlighted call record in the Placed and Received Calls logs.

User Tips

To use the new call history management features on your phone, do the following:

-
- Step 1** Press the **Directories** button.
- Step 2** Choose a call log (Missed, Placed, or Received).
- Step 3** Highlight a call record.
- Step 4** Choose one of the following softkeys to complete an action:
- **Clear**—Deletes all of the call records in the displayed log.
 - **Delete**—Deletes only the highlighted call record.
 - **Details**—Displays details for the highlighted call record, including called number, calling number, time of day, and call duration (for placed and received calls).



Note To access some of these softkeys, you might need to press the **more** softkey first.

Installation Notes

This sections contains these topics:

- [Firmware Upgrade Issues, page 5](#)
- [Cisco Unified IP Phone Expansion Module 7914, page 6](#)
- [Firmware Installation Procedure, page 6](#)

Firmware Upgrade Issues

Note the following firmware upgrade issues:

- If you are currently running firmware earlier than 6.0(2) on a Cisco Unified IP Phone 7970G and 7971G-GE and want to upgrade to 8.0(x), you must first install an intervening 7.0(x) load to prevent upgrade failure. Cisco recommends using the most recent 7.0(3) load as the intervening load to avoid lengthy upgrade times.
- If you are currently running firmware 6.0(2) to 7.0(2) on a Cisco Unified IP Phone 7970G and 7971G-GE and want to upgrade to 8.0(x), you can do so directly. However, expect the upgrade to take twice as long as usual.

Cisco Unified IP Phone Expansion Module 7914

If you are using the Cisco Unified IP Phone Expansion Module 7914, you must upgrade the expansion module to firmware release **S00105000200** before using the phone to support relevant 8.0(3) features on your expansion module.

You can download the installation program, which is named **cmterm-7914-sccp.5-0-2.exe**, and the readme file from Cisco.com at this location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>

Firmware Installation Procedure

Before using the Cisco Unified IP Phone 7970G and 7971G-GE with Cisco Unified CallManager release 3.3 or later, you must install the latest firmware on all Cisco Unified CallManager servers in the cluster.

Before You Begin

If you are upgrading from an earlier firmware version, see the “[Firmware Upgrade Issues](#)” section on [page 5](#).

To download and install the firmware, follow these steps:

Procedure

-
- Step 1** Go to the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>
- Step 2** To download the firmware for Cisco Unified IP Phone 7970G and 7971G-GE, click one of the following hyperlinks and follow the prompts:
- For Cisco Unified CallManager 4.2 and earlier:
cmterm-7970_7971-sccp.8-0-3.exe
 - For Cisco Unified CallManager 5.0 and later:
cmterm-7970_7971-sccp.8-0-3.cop
- Step 3** To download the Readme file, which contains installation instructions for the corresponding firmware, go back to the URL shown in [Step 1](#) and click the appropriate hyperlink.
cmterm-7970_7971-sccp.8-0-3-readme.htm
- Step 4** Follow the instructions in the Readme file to install the firmware.
-

Important Notes

This section contains these topics:

- [Cisco Unified CallManager Load Server Setting for Firmware Upgrades, page 7](#)
- [Secure PC Logoff in an 802.1X Network, page 7](#)

Cisco Unified CallManager Load Server Setting for Firmware Upgrades

Cisco Unified CallManager Administration contains a setting to optimize installation time for phone firmware upgrades.



Note

This setting is intended for future use, and is not yet a supported feature.

The Load Server setting is visible on the Phone Configuration page (Product Specific Configuration section) in the Cisco Unified CallManager Administration application. This setting lets you specify an external TFTP server IP address or name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for upgrades on the phones. When the Load Server is set, the phone contacts the designated server for the firmware upgrade.



Note

- If the firmware load is not found on the Load Server, the phone does not upgrade and is not redirected to the TFTP Server 1 or TFTP Server 2.
- On a factory reset or during a software recovery operation, the phone may fall back to using TFTP Server 1 or TFTP Server 2 to recover the phone load. In these scenarios, the phone will recover the phone load either via the term70.default.loads or term71.default.loads file, or it will attempt to recover the phone load based on its load.hist file.
- If the phone is auto-registering with Cisco Unified CallManager for the first time, the phone will request the phone load via TFTP Server 1 or TFTP Server 2. This will only occur once when the phone is first installed into the system. This can be mitigated by preloading the phones with the correct firmware so that no firmware upgrade is required in combination with the auto-registration, or by auto-registering the phones at the main site prior to deployment at a remote site.

You can view the Load Server setting on the phone from **Settings > Device Configuration > Network Configuration > Load Server**. If the value in the Load Server setting is invalid, a “Load Server is invalid” message is displayed on the phone in **Settings > Status > Status Messages**.

Secure PC Logoff in an 802.1X Network

Firmware release 8.0(3) provides support for the Cisco Unified IP Phone 7970G and 7971G-GE to monitor IEEE 802.1X messages between an authenticating switch and a connected PC (supplicant).

When a PC is disconnected from the Cisco Unified IP Phone, the phone issues an EAPOL-Logoff message on behalf of the PC to the authenticating switch. The proxy EAPOL-Logoff message causes the authenticating switch to set the port to an unauthenticated state.

If you have an 802.1X network and upgrade to Cisco Unified IP Phone firmware release 7.0(2) or greater, be aware that you must re-authenticate a PC that is connected to the Cisco Unified IP Phone 7970G and 7971G-GE.

For more information about 802.1X re-authentication, refer to the Cisco Catalyst switch configuration guides at:

http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html

Caveats

This section contains these topics:

- [Using Bug Toolkit, page 8](#)
- [Open Caveats, page 8](#)

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl . |
| Step 2 | Log on with your Cisco.com user ID and password. |
| Step 3 | Click the Launch Bug Toolkit hyperlink. |
| Step 4 | To look for information about a specific problem, enter the bug ID number in the “Enter known bug ID” field and click Search . |
-

Open Caveats

[Table 2](#) lists Severity 1, 2, and 3 defects that are open for Cisco Unified IP Phone 7970G and 7971G-GE for firmware release 8.0(3).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that [Table 2](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in the [“Using Bug Toolkit” section on page 8](#).

Table 2 *Open Caveats for Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(3)*

Identifier	Headline and Bug Toolkit Link
CSCsd64349	Invalid message URL causes the subsequent XML pushes to be not processed http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd64349
CSCsd65226	Empty Dial list is getting displayed on phone http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd65226
CSCsd65512	Phone User Preference > Rings window UI is (Overlapping) http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=SCsd65512
CSCsd78552	Lifting handset while in IPICS session plays dial tone http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd78552
CSCsd79623	Phone Continuously displays Requesting.... http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd79623
CSCsd84325	Mute button is enabled when phone Speaker button throws error pass limit http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd84325
CSCsd88089	Popping sound is heard when calling Cisco Unity IVR http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd88089
CSCsd88724	Focus should immediately shift when user action is involved http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd88724
CSCsd88756	Call back notification screen overlaps with received call list screen http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd88756
CSCsd91823	Multi-party call history—Transfer case— Received call from details http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd91823
CSCsd91853	Placed calls are not multi-party and should not show a multi-party call history http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd91853
CSCsd94168	No audible ring back on redial using Cisco Unified IP Phone 7970/7971/7961/7941/7911/7906 http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd94168
CSCsd95276	Phone discards DTMF digits A, B, C, D http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd95276
CSCsd96093	Duration runs cause problems events http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd96093
CSCsd97465	Phone UI behaves erroneously under certain conditions http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd97465
CSCsd97505	Unable to dial from external directory list after cancel edit dial http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd97505
CSCsd98820	Phone stops playing ring back when Mute button made on/off during ring out http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd98820

Table 2 Open Caveats for Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(3) (continued)

Identifier	Headline and Bug Toolkit Link
CSCse00577	revertPriority setting not used for first call after changing the setting http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse00577
CSCse03001	Status of BLF speed dial does not get updated http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse03001
CSCse05493	Kernel Shutdown bug code = 0x91 when performing upgrades/downgrades http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse05493
CSCse09491	UDI Time Zone not displaying string from phone configuration file http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse09491
CSCse10790	Phone display is not updated for multiple calls on shared line http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse10790

Resolved Caveats

Table 3 lists Severity 1, 2, and 3 defects that are resolved for Cisco Unified IP Phone 7970G and 7971G-GE for firmware release 8.0(3).

Table 3 Resolved Caveats for Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(3)

Identifier	Headline and Bug Toolkit Link
CSCsc34320	The headset icon does not wobble for ringing AG widget http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc34320
CSCsc78137	Phone stuck with prompt “Resetting” after load updates http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc78137
CSCsc80230	Cisco Unified IP Phone UDI compliance http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc80230
CSCsc83979	Volume in GL mode affects both speaker and handset http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc83979
CSCsc98903	SSH with Cisco Unified CallManager 5.x—performance hit during login http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc98903
CSCsc98937	Phone accepting duplicate IP http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc98937
CSCsd09502	Cisco Unified IP Phone 7941/7961/7970/7971 not sending DHCP traffic to PC port http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09502
CSCsd10839	Kernel shutdown bugcode = 0x95 with upgrade http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd10839
CSCsd13950	Phone can not boot up after RESET/power cycle http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd13950

Table 3 Resolved Caveats for Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(3) (continued)

Identifier	Headline and Bug Toolkit Link
CSCsd32588	Hardware compatibility http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd32588
CSCsd33424	Unable to disable PC port permanently http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd33424
CSCsd34361	Phone stops playing RingBack when second call comes http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd34361
CSCsd35011	Console log shows “SYSMSG: Kernel Shutdown bugcode = 0x67” http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd35011
CSCsd35541	LOADS filename extension displayed in upgrade UI http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd35541
CSCsd36392	ESPD: on no espd.conf, set logging=2 http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd36392
CSCsd36407	Hard factory reset should not erase rambox network settings http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd36407
CSCsd46848	Extra ESP messages on phone logs http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd46848
CSCsd49912	Bad propagation of debug flag http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd49912
CSCsd52709	my_name gets corrupted in dhcp.conf file http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd52709
CSCsd57320	DHCP recv socket error on bad address http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd57320
CSCsd57619	dsp ingress frame timestamp not following RTP RFC3550 http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd57619
CSCsd59892	“show inventory” CLI output not adhering to the specification http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd59892
CSCsd63834	Titan dsp host could 32-bit read between dsp firmware two 16-bit writes http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd63834
CSCsd64279	implement sched_yield() in DHCP http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd64279
CSCsd67218	F5CK stuck in deadlock with syslogd http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd67218
CSCsd67229	Handset volume is too high http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd67229
CSCsd74493	Cisco Unified IP Phone SLR needs adjustment http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd74493

Table 3 Resolved Caveats for Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(3) (continued)

Identifier	Headline and Bug Toolkit Link
CSCsd83812	mDoS tool icmpsic crashes phone on Bugtrap 0x93 http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd83812
CSCsd89584	Phone sends corrupted RFC2833 packets when SRTP enabled for call http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd89584

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

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

- For Nonemergencies—psirt@cisco.com

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

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

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

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

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

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.

