Cisco Unified IP Phone 7911G Release Notes for Firmware Release 8.0(2) SR2 for Cisco Unified CallManager 5.0, 4.2, 4.1, 4.0, and 3.3 (SCCP)

March 31, 2006

Use these release notes with a Cisco Unified IP Phone 7911G running SCCP firmware release 8.0(2) SR2 and Cisco Unified CallManager version 5.0, 4.2, 4.1, 4.0, or 3.3.

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

Contents

These release notes provide the following information:

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

Related Documentation

Cisco Unified IP Phone Documentation

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

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

New and Changed Information

Cisco Unified IP Phone firmware release 8.0(2) SR2 supports the latest versions of Cisco Unified CallManager software—version 4.2 and version 5.0. For a list of new and changed phone features introduced in these Cisco Unified CallManager versions, 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.

DTMF Transport

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

Group Listen Mode

Cisco IP Phone firmware release 8.0(2) SR2 supports Group Listen mode on the Cisco Unified Phone 7911G. In Group Listen mode, both the handset and speaker can be active at the same time. During a call, one user can talk into the handset while other users can listen over the speaker.

Group Listen mode is disabled by default. To enable this mode, you must do so from the Phone Configuration page in Cisco CallManager Administration. If Group Listen mode is enabled, the Monitor feature softkeys are not available on the phone.

Group Listen softkeys are displayed if Group Listen mode is enabled by the administrator on Cisco CallManager. However, these softkeys cannot be configured by using the Cisco CallManager softkey template.

End-User Information

When Group Listen mode is activated, end-users can use Group Listen mode by pressing softkeys:

- **GListen**—Activates Group Listen on the phone. Users can deactivate Group Listen by hanging up the handset or by pressing **GLOff**.
- **GLOff**—Deactivates Group Listen on the phone.

Note If Group Listen mode is enabled, the **GListen** and **GLOff** softkeys replace the **Monitor** and **MonOff** softkeys on the phone.

Installation Notes

Before using the Cisco Unified IP Phone 7911G with Cisco Unified CallManager version 4.2 or version 5.0, you must install the latest firmware on all Cisco Unified CallManager servers in the cluster.

The firmware image name is: **SCCP11.8-0-2SR2S.loads**

To 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 Double-click one of the following hyperlinks, and follow the prompts to download the firmware:

- Cisco Unified CallManager 5.0: **cmterm-7911-sccp.8-0-2SR2.cop**
- Cisco Unified CallManager 4.2 and earlier:

  cmterm-7911-sccp.8-0-2SR2.exe

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-7911-sccp.8-0-2SR2-readme.htm

Step 4 Follow the instructions in the Readme file to install the firmware.

Important Notes

Review these important notes for this firmware release.

Cisco Unified CallManager Load Server Setting for Firmware Upgrades

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

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 term11.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(2) SR2 provides support for the Cisco Unified IP Phone 7911G to monitor IEEE 802.1X messages between an authenticating switch and a connected PC (supplicant).

When a PC is disconnected from the Cisco 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 8.0(2) SR2, be aware that you must re-authenticate a PC that is connected to the Cisco Unified IP Phone 7911G.

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

These release notes contain descriptions of open caveats of severity level 1 or 2 and significant severity level 3.

If you are a registered Cisco.com user, you can find the latest information about resolved, open, and closed caveats for the Cisco Unified IP Phone 7911G by using Bug Toolkit, an online tool that allows you to query caveats according to your own needs. By using Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides.

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 in this release.

Table 1 Open Caveats for Cisco Unified IP Phone 7911G for Firmware Release 8.0(2) SR2

Identifier	Headline and Bug Toolkit Link
CSCsc56616	The phone is sometimes unable to renew its DHCP IP address if the reserved IP address has changed on the DHCP server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc56616
CSCsc98937	The phone accepts a duplicate IP address. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc98937
CSCsd02273	Handset is not disabled when placed in cradle while in Group Listen mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd02273

Resolved Caveats

Table 2 lists Severity 1, 2, and 3 defects that are open in this release.

Table 2 Resolved Caveats for Cisco Unified IP Phone 7911G for Firmware Release 8.0(2) SR2

Identifier	Headline and Bug Toolkit Link
CSCsb70757	With Japanese locale, the Corporate Directory appears in English after the Personal Directory is displayed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb70757
CSCsc06398	The phone uses HTTP cookie received from CallManager while communicating with another server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc06398
CSCsc76316	Focus changes from a connected call to a ringing call before the 10-second inactivity timer expires. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc76316
CSCsc90123	Registration Rejected is not displayed when autoregistration is disabled. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc90123

Table 2 Resolved Caveats for Cisco Unified IP Phone 7911G for Firmware Release 8.0(2) SR2

Identifier	Headline and Bug Toolkit Link
CSCsc96369	Incorrect softkeys are displayed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc96369
CSCsc98903	Secure Shell SSH performance is slow during login. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc98903
CSCsc99030	Setting static IP addresses may cause the phone to reboot repeatedly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc99030
CSCsc99166	Initial voice clipping on SCCP and SIP phones. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc99166
CSCsd00199	The message waiting indicator light remains flashing after the Call Pickup notification. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd00199
CSCsd04472	The Dial URI with an active call does not invoke call options if no application is in focus. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd04472
CSCsc51724	Phone does not handle HTTP code 401 when the service URL is used. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc51724
CSCsc82221	Phones try to register to CallManager when CallManager service is stopped. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc82221
CSCsd03510	A time/date request to synchronize the clock causes skipping of one KeepAlive interval. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd03510
CSCsd02273	The handset is not disabled when placed in cradle while in Group Listen mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd02273
CSCsc83979	Volume in Group Listen mode affects both the speaker and handset. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc83979
CSCsd67229	Handset volume is too high. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd67229

Table 2 Resolved Caveats for Cisco Unified IP Phone 7911G for Firmware Release 8.0(2) SR2

Identifier	Headline and Bug Toolkit Link
CSCsd75616	The Cisco Unified IP Phone 7911G Group Listen mode SLR increases by 5 dB. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd75616
CSCsd81691	Cisco Unified IP Phone 7911G handset SLR is 5 dB soft. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd81691

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://ciscoiq.texterity.com/ciscoiq/sample/

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.