



Cisco IP Phone 7970G and 7971G-GE Release Notes for Firmware Release 7.0(3) for Cisco CallManager 3.3, 4.0, 4.1

February 9, 2006

Use these release notes with the Cisco IP Phone 7970G and 7971G-GE for firmware release 7.0(3) running on Cisco CallManager Versions 3.3(5) SR1, 4.0(2) SR2b, and 4.1(3) SR1.

Contents

These release notes provide the following information. You might need to notify your users about some of the information provided in this document.

- [Related Documentation](#)
- [Installation Notes](#)
- [Important Notes](#)
- [Caveats](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Related Documentation

Cisco IP Phone Documentation

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

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

Cisco CallManager Documentation

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

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

Installation Notes

This section contains these topics:

- [Firmware Information, page 2](#)
- [Supported CallManager Versions, page 3](#)
- [Cisco IP Phone Expansion Module 7914, page 3](#)

Firmware Information

The Cisco IP Phone 7970G and 7971G-GE firmware installation program is named **cmterm-7970_7971-sccp.7-0-3.exe**.

The readme file that contains installation instructions is named **cmterm-7970_7971-sccp.7-0-3-readme.htm**.

Both files can be downloaded from this location on Cisco.com:

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

Supported CallManager Versions

The Cisco IP Phone 7970G and 7971G-GE firmware release 7.0(3) is supported on these Cisco CallManager versions:

- Cisco CallManager version 3.3(5) SR1 or later
- Cisco CallManager version 4.0(2) SR2b or later
- Cisco CallManager version 4.1(3) SR1 or later

Cisco CallManager Device Packs

You should install the following device packs for these Cisco CallManager versions. You can download the device packs from this location on Cisco.com:

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

The device pack readme files provide installation information.

| Cisco CallManager Version | Device Pack |
|---------------------------|--------------------------------------|
| 3.3(5) SR1 | ciscocm.3-3-DevPack-64.exe, or later |
| 4.0(2) SR2b | ciscocm.4-0-DevPack-43.exe, or later |
| 4.1(3) SR1 | ciscocm.4-1-DevPack-23.exe, or later |

Cisco IP Phone Expansion Module 7914

The Cisco IP Phone Expansion Module 7914 is supported on the Cisco IP Phone 7970G and 7971G-GE.

If you are using the Cisco IP Phone Expansion Module 7914, you must upgrade the Expansion Module to firmware release S00104000100. You can download the installation program, which is named **cmterm-7914-sccp.4-0-1.exe**, and the readme file from Cisco.com at this location:

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

Important Notes

This section contains these topics:

- [Cisco CallManager Load Server Setting for Firmware Upgrades](#), page 4
- [Securing the Phone with a Cable Lock](#), page 5
- [Secure PC Log Off in an 802.1X Network](#), page 5

Cisco CallManager Load Server Setting for Firmware Upgrades

A setting that optimizes installation time for phone firmware upgrades is available in Cisco CallManager Administration.

**Note**

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

To view the load server setting, you must install the latest Cisco CallManager Device Pack (see the [“Cisco CallManager Device Packs”](#) section on page 3).

The Load Server setting is visible on the Phone Configuration page (Product Specific Configuration section) in the Cisco CallManager Administration application. This setting lets you specify another 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 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**.

Securing the Phone with a Cable Lock

You can secure the Cisco IP Phone 7970G and 7971G-GE to a desktop using a laptop cable lock. The lock connects to the security slot on the back of the phone and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm. Compatible laptop cable locks include the Kensington® laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

Secure PC Log Off in an 802.1X Network

Firmware release 7.0(3) provides support for a Cisco IP Phone 7970G or 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 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 IP Phone firmware release 7.0(2) or greater, be aware that you must re-authenticate a PC that is connected to a Cisco 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 6](#)
- [Resolved Caveats, page 7](#)
- [Open Caveats, page 12](#)

Using Bug Toolkit

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

You can get more information about the caveats in these release notes or search for caveats of any severity level by using the Cisco software called Bug Toolkit.

To access Bug Toolkit, you need a Cisco.com user ID and password.

To use Bug Toolkit, follow these steps:

Procedure

- Step 1** 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**.
-

Resolved Caveats

Table 1 lists severity 1, 2, and 3 defects that are resolved in firmware release 7.0(3) for the Cisco IP Phone 7970G and 7971G-GE.

Table 1 **Resolved Caveats**

| Identifier | Summary and Bug Toolkit Link |
|------------|---|
| CSCsb13507 | Domain Name field under Network Configuration menu can not be removed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb13507 |
| CSCsb13552 | The phone does not remove the default router configuration. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb13552 |
| CSCsb30771 | Phone crashes when sending a fragmented ICMP packet. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb30771 |
| CSCsb32965 | Phone UI locks after pressing Directory button. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb32965 |
| CSCsb40300 | Phone doesn't register when unable to resolve the Cisco CallManager name. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb40300 |
| CSCsb42411 | After a power outage, the phone is stuck at "Configuring IP". http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb42411 |
| CSCsb44304 | There is a race condition in CNU sockets when the same socket is accessed by multiple threads in the same process. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb44304 |
| CSCsb47829 | Phone still downloads files after a DHCP release. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb47829 |
| CSCsb50077 | After erase or reset, the phone sticks at "Configuring IP" and shows Cisco logo. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb50077 |
| CSCsb54419 | LED does not blink red while the DCP is busy. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb54419 |
| CSCsb60547 | Assigning same IP port to RX and TX socket causes one-way audio. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb60547 |

Table 1 **Resolved Caveats (continued)**

| Identifier | Summary and Bug Toolkit Link |
|------------|--|
| CSCsb60762 | Phone doesn't play Zip/ZipZip Tones toward network. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb60762 |
| CSCsb61918 | When the spanPCPort is enabled and the pcPort is disabled, the pcPort still displays messages. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb61918 |
| CSCsb62087 | Phone is stuck in a reboot loop. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb62087 |
| CSCsb66459 | SIP TNP: DSP debug seen when pressing Settings, Directories, or Services. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb66459 |
| CSCsb66487 | The phone is requesting a CTL file from a TFTP server that does not exist in the current CTL file on the phone. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb66487 |
| CSCsb67660 | File system formats on reset from Cisco CallManager. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb67660 |
| CSCsb68597 | Phone receives mcast pkts when port open for Mcast transmit. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb68597 |
| CSCsb68914 | Error Verifying Config Info after LSC install on secure phone. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb68914 |
| CSCsb70143 | If a DNS lookup fails because an FQDN was mis-configured, the code will still send out a message to IP address 0.0.0.0. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb70143 |
| CSCsb75176 | Phone displays wrong message when registration is rejected for security reason. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb75176 |
| CSCsb77225 | Phone is stuck at "Configuring IP" on the screen. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb77225 |
| CSCsb85540 | Ethernet Disconnected message does not appear when Ethernet unplugged. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb85540 |

Table 1 **Resolved Caveats (continued)**

| Identifier | Summary and Bug Toolkit Link |
|------------|--|
| CSCsb87704 | The syslogd does not write the log files in proper order. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb87704 |
| CSCsb88142 | After setting DHCP = No and attempting to set the TFTP2 address to 0.0.0.0, the phone stops sending packets. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb88142 |
| CSCsb88986 | Phone crashes due to buffer handling in net_input(). http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb88986 |
| CSCsb93321 | Race condition in __shutdown() function causes BugTrap. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb93321 |
| CSCsc03743 | Presence BLF lamp is not being displayed correctly on the phone. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc03743 |
| CSCsc08584 | Calls drop during Cisco CallManager Express failback. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc08584 |
| CSCsc24668 | cBarge Target phone changes focus when other party cBarges. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc24668 |
| CSCsc27685 | If fragmented IP packets are received on the phone, they are not reassembled to provide a complete message to the User Datagram Protocol (UDP) layer. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc27685 |
| CSCsc30810 | Problems when filename length == NAME_MAX. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc30810 |
| CSCsc31606 | Pressing the “.” soft key in the edit menu doesn’t force Kate String T/O. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc31606 |
| CSCsc36213 | Clicking noise is heard in encrypted call when duplicating packets. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc36213 |
| CSCsc36645 | Phone does not boot up and the line buttons continuously flash red. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc36645 |

Table 1 **Resolved Caveats (continued)**

| Identifier | Summary and Bug Toolkit Link |
|------------|--|
| CSCsc39509 | Call bubble does not disappear when there is no active call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc39509 |
| CSCsc40627 | High End Phones connect to CCM sub that is not present in the CTL file. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc40627 |
| CSCsc43827 | InsideDialTone could not be stopped after removing CFwdAll. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc43827 |
| CSCsc58105 | Phone reboots when secondary Cisco CallManager Express is inaccessible and keepalive is 10. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc58105 |
| CSCsc65503 | SIP Phone does not do a TLS session reuse after network failure. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc65503 |
| CSCsc70929 | When phones are upgraded to use Cisco CallManager development version 50-205 they got stuck in a reboot loop. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc70929 |
| CSCsc76402 | RMS Store must be deleted in order for phone to boot correctly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc76402 |
| CSCsc91001 | Answer softkey is not displayed for a new incoming call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc91001 |
| CSCsc72223 | Phone stuck after erase under Settings menu. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc72223 |
| CSCsd11037 | Two (2) meg file limit cause double boot when upgrading to 8.0 load. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd11037 |
| CSCeb52862 | No value for some items on Device Information page. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb52862 |
| CSCsa94528 | Cancel softkey has delayed response when looking up a bogus DNS address. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa94528 |

Table 1 **Resolved Caveats (continued)**

| Identifier | Summary and Bug Toolkit Link |
|------------|--|
| CSCsb54991 | 7970/7971 Touch Screen issue: Phone URL shows Delay. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb54991 |
| CSCsb72254 | Corporate directory search fails if username contains special characters. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb72254 |
| CSCsb56740 | Background Image thumbnails not displayed in correct order. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb56740 |
| CSCsc28515 | Services page text does not display properly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc28515 |
| CSCsd23065 | Display distorts, when held calls goes from three to two. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd23065 |
| CSCsb40406 | Phone resets randomly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb40406 |

Open Caveats

Table 2 lists severity 1, 2, and 3 caveats that are known to exist in firmware release 7.0(3) for the Cisco IP Phone 7970G and 7971G-GE.

Table 2 **Open Caveats**

| Identifier | Summary and Bug Toolkit Link |
|------------|--|
| CSCsd09502 | Phone does not send DHCP traffic to PC port. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09502 |
| CSCsd09043 | Two concurrent XML posts result in Error 0 or Error 6. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09043 |
| CSCsc23475 | Delayed audio connection on phone with Cisco CallManager Express. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc23475 |
| CSCsc85517 | Phone does not use DNS cache properly on subnet without a domain. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc85517 |
| CSCsc91398 | Performs unneeded ARP when Garp enabled. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc91398 |
| CSCsc67938 | Phone sends bad HTTP request to Cisco CallManager. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc67938 |
| CSCsc97119 | Phone is not resetting after Extension Mobility logout. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc97119 |
| CSCsd09298 | Phone is unable to disable the PC Port permanently. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09298 |
| CSCsc99161 | Phone does not go offhook except via softkey. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc99161 |
| CSCsd09123 | Phone displays time in GMT instead of GMT-4 when set to Caracas. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09123 |

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>

- *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>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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.