



Release Notes for Cisco Unified Videoconferencing Manager Release 5.0

October 24, 2006

These release notes describe the new features and caveats for all versions of Cisco Unified Videoconferencing Manager release 5.0.

You can access the latest software upgrades and release notes for all versions of Cisco Unified Videoconferencing Manager on Cisco Connection Online (CCO) at the following URL:

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

Contents

These release notes discuss the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Related Documentation, page 3](#)
- [Resolved Caveats for Cisco Unified Videoconferencing Manager Release 5.0, page 3](#)
- [Open Caveats for Cisco Unified Videoconferencing Manager Release 5.0, page 6](#)
- [Documentation Updates, page 9](#)
- [Obtaining Documentation, page 11](#)
- [Documentation Feedback, page 12](#)
- [Cisco Product Security Overview, page 12](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 14](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco Unified Videoconferencing Manager is a single-installation product that contains the following components

- **Resource Manager**—A simple-to-use, web-based application for managing and monitoring visual communication in multi-site organization deployments. Resource Manager is deployed on your network to provide scheduling, monitoring and management of capacity, resources, and network devices for video and audio meetings.
- **Network Manager**—Provides a central management interface, enabling network administrators to easily and intuitively control, configure, and maintain Cisco-based collaborative communications networks. Backed by the Cisco track record for industry-leading innovation, Network Manager is the ideal choice to help you get the most out of your rich media network solutions.
- **Internal Gatekeeper**—A simple-to-use, ITU-T H.323 version 4-compliant gatekeeper application that is essential for the management of IP telephony and multimedia communication networks. Designed with the network manager in mind, the Internal Gatekeeper provides complete functionality for defining and controlling voice and video traffic management over IP networks. Network managers can configure, monitor and manage the activities of registered network users. Managers can set policies and control network resources such as bandwidth usage to ensure optimal implementation.

System Requirements

- Cisco Unified Videoconferencing Manager supports the English version of Windows 2000 Server, Windows 2000 Professional, and Windows 2003 platforms.

**Note**

Cisco support the Cisco Unified Videoconferencing Manager when installed on the Cisco MCS 7825 server operating system only. The Cisco MCS 7825 server operating system (based on Windows 2000) is shipped with the Cisco Unified Videoconferencing Manager software.

- Cisco Unified Videoconferencing Manager is supplied with a fully functional temporary license key which supports 30 concurrent ports and is valid for 30 days from the date of installation.
- Before installing Cisco Unified Videoconferencing Manager, make sure that port 1098 and 1099 are not occupied. The Cisco MCS 7825 server operating system comes configured with these ports open.
- If Windows 2003 Service Pack 1 Firewall is enabled on the designated server, make sure that in Windows Firewall > Exceptions, the following ports are added to the Programs and Services list
 - Web Server Port: TCP 8080 (by default)
 - ECS Authorization Port: TCP 7777 (by default)

The Cisco MCS 7825 server operating system comes configured with these security settings.

- Make sure that no previous MySQL version is installed.

- Cisco Unified Videoconferencing Manager uses the following predefined account details for the MySQL database connection: user name root and a null password.



Note Do not interrupt the installation procedure. After starting the service, allow several minutes for initialization of the server before logging in to the web user-interface.

- Cisco Unified Videoconferencing Manager is configured to use Active Directory Server as its user database, with security groups used for managing user roles. By default, all users except the administrator are given the role of Meeting Organizer. To modify this behavior, go to Advanced Settings > LDAP Configuration > Advanced and change the user-role mapping.
- After installation, log in as an administrator to configure the network and resources in the system.



Note To enable scheduling, meeting types must be downloaded from a specific MCU. If more than one MCU is present, upload Resource Manager meeting types from Resource Manager to those MCUs. To modify meeting type (service) settings, update the service parameters in a specific MCU, download the service to the Resource Manager, and then upload the service to all other MCUs.

Related Documentation

- *Cisco Unified Videoconferencing Manager Administrator Guide Release 5.0*
- *Cisco Unified Videoconferencing Manager User Guide Release 5.0*

Resolved Caveats for Cisco Unified Videoconferencing Manager Release 5.0

You can find the latest resolved caveat information for Cisco Unified Videoconferencing Manager release 5.0 by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.



Tip

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section includes the following topics:

- [Using Bug Toolkit, page 4](#)
- [Saving Bug Toolkit Queries, page 5](#)

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

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

To use Bug Toolkit, follow this procedure.



Note

Cisco CallManager is used in this procedure as an example. You will want to replace Cisco CallManager with the name of the product for which you are searching for bug information.

Procedure

- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. Log on with your Cisco.com user ID and password.
- Step 2** Click the **Launch Bug Toolkit** hyperlink.
- Step 3** If you are looking for information about a specific caveat, enter the ID number in the “Enter known bug ID:” field.
- To view all caveats for Cisco CallManager, go to the “Search for bugs in other Cisco software and hardware products” section, and enter **Cisco CallManager** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco CallManager**.
- Step 4** Click **Next**. The Cisco CallManager search window displays.
- Step 5** Choose the filters to query for caveats. You can choose any or all of the available options:
- Choose the Cisco CallManager version:
 - Choose the major version for the major releases (such as, 4.1, 4.0, 3.3).
A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.
 - Choose the revision for more specific information; for example, choosing major version 4.1 and revision version 3 queries for release 4.1(3) caveats.
A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.
 - Choose the Features or Components to query; make your selection from the “Available” list and click Add to place your selection in the “Limit search to” list.
 - To query for all Cisco CallManager caveats for a specified release, choose “All Features” in the left window pane.



Note

The default value specifies “All Features” and includes all of the items in the left window pane.

- To query only for Cisco CallManager-related caveats, choose “ciscocm” and then click **Add**.
- To query only for phone caveats, choose “ciscocm-phone” and then click **Add**.
- To query only for gateway caveats, choose “voice-gateway” and then click **Add**.

- c. Enter keywords to search for a caveat title and description, if desired.



Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- d. Choose the Set Advanced Options, including the following items:
- Bug Severity level—The default specifies 1-3.
 - Bug Status Group—Check the **Fixed** check box for resolved caveats.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.
- e. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.
- You can save your query for future use. See the [“Saving Bug Toolkit Queries” section on page 5](#).



Note

For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

- Step 1** Perform your search for caveats, as described in the [“Using Bug Toolkit” section on page 4](#).
- Step 2** In the search result window, click the **This Search Criteria** button that displays at the bottom of the window.
- A new window displays.
- Step 3** In the Name of saved search field, enter a name for the saved search.
- Step 4** Under My Bug Groups, use one of the following options to save your defects in a bug group:
- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
 - Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.



Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches, and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

- Step 5** Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:
- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
 - **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
 - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
 - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
 - **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.
- Step 6** To save your changes, click **Save**.
- Step 7** A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.
-

Open Caveats for Cisco Unified Videoconferencing Manager Release 5.0

Table 1 describes possible unexpected behaviors by Cisco Unified Videoconferencing Manager Release 5.0, sorted by component. Unless otherwise noted, these caveats apply to all Cisco Unified Videoconferencing Manager 5.0 releases up to and including Cisco Unified Videoconferencing Manager 5.0.



Tip

For more information about an individual defect, click the associated Identifier in **Table 1** to access the online record for that defect, including workarounds.

You can find the latest resolved caveat information for Cisco Unified Videoconferencing Manager Release 5.0 by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.



Tip

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 1 *Open Caveats for Cisco Unified Videoconferencing Manager*

Identifier	Severity	Component	Headline
CSCsg36772	2	CUVC M	MP unregisters without notification, MP Unregister needs to be alarm and not event http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg36772
CSCsg23242	3	CUVC M	Internal GK loses authorization connection with CUVC-M intermittently http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg23242
CSCsg36775	3	CUVC M	MP unregisters without notification, MP Unregister needs to be alarm and not event http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg36775

Additional Open Caveats

This section describes possible unexpected behaviors by Cisco Unified Videoconferencing Manager Release 5.0, sorted by component. Unless otherwise noted, these caveats apply to all Cisco Unified Videoconferencing Manager 5.0 releases up to and including Cisco Unified Videoconferencing Manager 5.0.

Cisco Unified Videoconferencing Manager known issues are included in the following categories:

- [Administration, page 7](#)
- [Network Manager, page 8](#)
- [Client for Microsoft Outlook, page 8](#)

Administration

- When scheduling a meeting, you can set the customized layout for the terminal participants when working with a version 4.x MCU. When using a version 5.x MCU, the layout of terminals changes dynamically when the meeting starts.
- Cisco Unified Videoconferencing Manager supports the use of its internal gatekeeper with one external Cisco IOS H.323 Gatekeeper.
- Since the MCU uses ** as a separator in dial string, terminal numbers which include the ** string cannot connect to a meeting.
- Gateways configured in Cisco Unified Videoconferencing Manager must have a service with 64Kbps (video or audio) bandwidth.
- Cisco Unified Videoconferencing Manager does not support the Force Conference PIN Protection field in MCU service definition.
- If the "No Self-See" property is selected for an MCU service, when dragging terminals to the layout box on the In-Meeting Control window, certain terminals will not display since they need to comply with the No Self-See restriction.
- Reporting on a large number of conferences (in the Upcoming tab or the History tab) may cause an out of memory error.
- Taking an MCU offline and causing a large number of conferences to be rescheduled may result in an out of memory error.

- Cisco Unified Videoconferencing Manager supports cascading only by using the same service on each MCU. Only simple cascading can take place between an MCU version 4.x and an MCU version 5.0.
- In a cascaded conference, the Sub Conf list in the In-Meeting Control window is displayed for all endpoints, but only endpoints registered to the main MCU can join a sub conference.
- Cisco MCU version 4.x features, such as Encryption and Qualivision, function properly with Resource Manager but are not displayed as meeting type information or in the In-meeting Control window.
- Adjusting the server clock disrupts the status of any recurring meetings that are scheduled.
- Resource Manager works with Exchange Server 2003 SP2. Some exchange servers use a mechanism that prevents rogue applications from sending spam e-mails through them. Resource Manager must be registered as a trusted party with each exchange server before gaining permission to send e-mails through this type of exchange server.
- When you change the settings for a terminal in the Resource Management section, the changes are not reflected on the Terminals tab of the Meeting Templates and My Meetings sections.
- If an MCU is taken offline, in-session meetings running on the MCU are cancelled. These meeting records are moved to the History tab in the All Meetings and My Meetings sections.
- In order to access the Resource Manager Configuration Tool and the Network Manager, you need JRE 5.0 installed on your machine.
- Each time you restart the application, allow a few minutes for the service to initialize correctly.
- Alarms 35, 36, 37 and 38:
 - 35=Serial cable mismatch in line 1. Gateway reset will fix the problem.
 - 36=Serial cable mismatch in line 2. Gateway reset will fix the problem.
 - 37=Serial cable mismatch in line 3. Gateway reset will fix the problem.
 - 38=Serial cable mismatch in line 4. Gateway reset will fix the problem.

Network Manager

- Web user interface access information for the EMP card is irrelevant. The EMP card does not support a web user interface.
- For a current conference, the MaxPart field sometimes displays 100. This is an erroneous value and should be disregarded.
- Network Manager does not support or manage the MCU in SCCP mode.

Client for Microsoft Outlook

- When using the Client for Microsoft Outlook, the meeting organizer is always included in the participant list regardless of whether or not in the My Profile section, the Don't include me in the meeting check box is checked or not checked.
- Modify meetings scheduled via Outlook in the Outlook interface only. Do not modify them via the Resource Manager web user-interface.

Documentation Updates

Setting Authorization Mode

- Authorization Mode enables Cisco Unified Videoconferencing Manager to monitor and authorize point-to-point calls routed via the Cisco Unified Videoconferencing Manager Internal Gatekeeper. Authorization Mode is enabled by default, and no additional configuration is required. The default authorization port is 7777.

Single Sign-on

- Single sign-on (SSO) enables users to access Cisco Unified Videoconferencing Manager web pages without the need to type a user name or password. Users are authenticated transparently using domain account/password credentials. To enable this feature, during installation, make sure that you check the Single Sign-on check box.
 - Cisco recommends that administrators provide users with a link to Cisco Unified Videoconferencing Manager that includes the necessary FDQN rather than only the Resource Manager IP address. Failure to provide the Cisco Unified Videoconferencing Manager FDQN may result in the user's browser failing to recognize Resource Manager as a local intranet site and cause an authentication dialog box pop up to appear.

An alternative solution is to configure the user's browser so that Cisco Unified Videoconferencing Manager is a local intranet site.
 - When working with the Client for Microsoft Outlook and SSO, leave the user ID, password and organization fields empty in the Client for Microsoft Outlook Meetings tab. Resource Manager automatically performs authentication using the domain account/password credentials.

Client for Microsoft Outlook

- After Client for Microsoft Outlook installation, go to **Tools > Options > Meetings** and enter the URL of your server in the Web Site field. For example, <http://server-cuvc/cuvc>.
- To prevent the standard Outlook 2003 pop-up message warning that another application is trying to access Outlook information, apply the following new registry key HKEY_CURRENT_USER\Software\Policies\Microsoft\Security\CheckAdminSettings to the Outlook client machine, and then set its value to 1. To modify this behavior from the exchange server side, refer to Microsoft documentation.
- Meetings scheduled from the Outlook client use the meeting organizer time zone setting from Cisco Unified Videoconferencing Manager. Meeting organizers should make sure that the time zone settings on their PCs match those in Cisco Unified Videoconferencing Manager. To change time zone settings, in Resource Manager, go to My Profile.



Note Cisco recommends that meetings created via the Outlook client application contain no more than 100 participants.

User Experience

If you enable Internet Explorer Pop-up Blocker when using Windows XP SP2 or Windows 2003 SP1, add the Cisco Unified Videoconferencing Manager site to the list of allowed sites via **Tools > Internet Options > Privacy > Pop-up Blocker Settings**. Add the Resource Manager site as `http://<Resource Manager IP address>`.

- Use the Next and Back buttons provided within the Cisco Unified Videoconferencing Manager screens to navigate between pages rather than the Internet Explorer browser navigation buttons (Back, Forward and Refresh).
- When scheduling recurring meetings via the Cisco Unified Videoconferencing Manager web user interface, occurrences are scheduled within the first 730 days (maximum limit). The 730-day time period is configurable in the Configuration Tool.
- When many meetings are terminated at the same time, there may be a short delay before they are cleared from the All Meetings list.
- If the gateway and the invited ISDN party are located in a different area within the same country, the area code for endpoint ad-hoc meetings should be added to the dialing string or in Cisco Unified Videoconferencing Manager, go to **Resource Management > Gateway**, check the **Always dial area code** check box.
- To ensure that web pages and pop-up windows are displayed normally, Cisco recommends that you set the screen resolution to standard resolutions such as 800 x 600 pixels, 1024 x 768 pixels and so on. The minimum recommended resolution is 800 x 600 pixels and the recommended font size is normal or large.
- Users deleted from the Address Book are not automatically removed from meeting templates.
- If you take control of a meeting via the Resource Manager In-meeting Control panel but leave Cisco Unified Videoconferencing Manager inactive for five minutes, your control status automatically ends.

Administration

- If the database is not available during Cisco Unified Videoconferencing Manager initiation, ensure that you restart the service when the database is ready. If the connection between the database and the Cisco Unified Videoconferencing Manager is lost after Cisco Unified Videoconferencing Manager initiation, Cisco Unified Videoconferencing Manager works normally when the database is operating.
- The MCU service template name and description, terminal name and gateway service prefix can only contain ASCII text. Unicode and other double-byte characters (such as Chinese, Japanese and Korean characters) cause device exception.
- Ensure that you define terminal area codes correctly, and omit domestic long distance prefixes.
- DID numbers are currently assigned on a per-endpoint basis rather than on a per-meeting basis. This is an internal configuration and cannot be changed via the Configuration Tool or the Cisco Unified Videoconferencing Manager web interface.

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

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

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

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

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

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

<http://www.ciscopress.com>

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

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

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

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

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

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

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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. (0705R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

