



Release Notes for Cisco Unified Videoconferencing Gateway Release 5.0.1

Revised: October 30, 2006 OL-11635-01

These release notes describe the new features and caveats for Cisco Unified Videoconferencing Gateway Release 5.0.1 for the following Cisco products:

- Cisco Unified Videoconferencing 3527 PRI Gateway
- Cisco Unified Videoconferencing 3522 BRI Gateway
- Cisco Unified Videoconferencing 3545 PRI Gateway
- Cisco Unified Videoconferencing 3545 Serial Gateway

You can access the latest software upgrades and release notes for all versions of gateway 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 2](#)
- [New and Changed Information, page 2](#)
- [Resolved Caveats for gateway Release 5.0.1, page 3](#)
- [Open Caveats for gateway Release 5.0.1, page 6](#)
- [Troubleshooting, page 7](#)
- [Obtaining Documentation, page 7](#)
- [Documentation Feedback, page 8](#)
- [Cisco Product Security Overview, page 8](#)
- [Product Alerts and Field Notices, page 9](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 11](#)

Introduction

The gateway enables audio, video and data communication between H.320 endpoints that connect through Integrated Services Digital Network (ISDN), and H.323 endpoints that connect through a packet-based network. For voice-over-IP, the gateway enables Public Switched Telephone Network (PSTN) voice callers to connect with IP voice callers.

System Requirements

- [Compatibility Matrix and Supported Upgrades, page 2](#)

Compatibility Matrix and Supported Upgrades

You can upgrade directly from gateway Release 4.x to Release 5.0.1.

Related Documentation

- *Administrator Guide for Cisco Unified Videoconferencing 3527 PRI Gateway and 3522 BRI Gateway Release 5.0*
- *Administrator Guide for Cisco Unified Videoconferencing 3545 PRI Gateway and 3545 Serial Gateway Release 5.0* at the following URL:

New and Changed Information

The following section describes new features and changes that are pertinent to this release of gateway.

- Full support for H.243 cascading with Cisco Unified Videoconferencing 3500 MCU and other vendor MCUs.
- Enhanced H.239 interoperability between Aethra ISDN endpoints and Cisco Unified Videoconferencing 3500 MCU via the gateway.
- The content of the Display field can be modified before being sent to the IP side in the SETUP message.
- Cisco Unified Videoconferencing 3545 3545 Serial Gateway offers enhanced interoperability with KG encryption devices.

Resolved Caveats for gateway Release 5.0.1

You can find the latest resolved caveat information for gateway Release 5.0.1 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.

Topics in this section include:

- [Resolved Caveats, page 3](#)
- [Using Bug Toolkit, page 3](#)
- [Saving Bug Toolkit Queries, page 5](#)

Resolved Caveats

The following issues have been resolved since Release 4.0:

- The web user interface correctly displays the Gateway location or IP address.
- When using the improved G.722.1, H.264 and H.239 capability policy, these capabilities are not published to the ISDN or to the IP legs to prevent some legacy equipment crashing.
- 2*B calls via the Gateway operate correctly.
- Interoperability with the Cisco IPVC 35xx MCU for calls using G.728 at 128 Kbps.
- Improved interoperability with ISDN Polycom VSX version 7.5.2.
- Improved clearing cause is sent to the IP endpoint in some cases.

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:

- a. 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.
- b. 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 3](#).
- 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 gateway Release 5.0.1

This section lists possible unexpected behaviors by gateway Release 5.0.1 and is sorted by gateway product.

All gateway Products

- Upgrade/downgrade problems may occur due to lack of memory. If the following message displays, “Upgrade process failed: The uploaded file size is larger than the maximum available memory” in the Upgrade Utility, manually reboot the board and retry the upgrade.
- When using TANDBERG 1500 MXP on the IP side, it may take about 20 seconds for the video channel to open from the MXP to the Gateway.
- The start of the IVR message is missing in calls from an ISDN Polycom VSX endpoint.
- Some H.239 interoperability issues may occur when working with eConf.
- Some H.239 interoperability issues occur in calls between a TANDBERG ISDN 990MXP endpoint and a Polycom VSX LAN endpoint.
- Some H.235 interoperability issues may occur when working with a TANDBERG 4.1 endpoint. The audio channel from the endpoint via the Gateway may fail to open as an encrypted channel. In such cases, the Gateway will disconnect the call.
- The H.239 codec supports only the H.263 codec in the second video channel. The H.264 codec is not supported.
- We recommend that you use an MVP when working with the MCU in H.239 mode.
- When working in Peer-to-Peer mode, the front Gatekeeper (GK) LED is always lit.
- Video may freeze in calls between ISDN Polycom FX and IP TANDBERG MXP.

Cisco Unified Videoconferencing 3527 PRI Gateway, 3522 BRI Gateway and 3545 PRI Gateway

- Difficulties may occur when using Fast Start. We recommend that you do not activate Fast Start.
- H.239 is not supported in 2*B calls.

Cisco Unified Videoconferencing 3545 Serial Gateway

- Connection problems occur in IP-to-IP calls via two Serial Gateways using Polycom VSX 7000.

Troubleshooting

- We recommend that you use Microsoft Explorer version 5.0 or later as your browser.
- Interoperability issues may occur with Aethra Maia384 on the ISDN. Solve the problem by sending the ChangeBondingCID advanced command with the parameter value "enable" to the Gateway.
- Calls may fail when using TANDBERG endpoints on the ISDN with the bit rate set to "Auto." Solve the problem by sending the ClearBondXflag advanced command with the parameter value "enable" to the Gateway.
- When making a 128 Kbps call from an ISDN Sony PCS-1, H.239 may not open correctly. Increasing the call bit rate solves this issue.
- H.239 interoperability issues may occur when working with Aethra endpoints on the ISDN when making a TCS4 or IVR call. Solve this issue by sending the SimulateVideoOff advanced command with the parameter value "enable".
- When working with VSX300 on the ISDN side, if using G.722.1 with H.263, there will be no video seen in the VSX. Disable the G.722.1 in the GW media modes in order to solve this issue.
- When using G.722.1 with H.263, video is lost on a Polycom VSX300 ISDN endpoint. Solve this problem by disabling G.722.1 in the Media Modes section of the Gateway Settings tab.
- Opening an H.239 channel to a TANDBERG MXP on the ISDN side may fail. Simply retry and the channel will open successfully.

For additional troubleshooting information, see the Troubleshooting chapter in the *Administrator Guide for Cisco IPVC-3527-GW1P and Cisco IPVC-3522-GW4B Release 5.0* and *Administrator Guide for Cisco IPVC-3545-GW2P and Cisco IPVC-3545-GW4S Release 5.0* at the following URL:

http://cisco.com/en/US/products/hw/video/ps1870/prod_maintenance_guides_list.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created monthly and is released in the middle of the month. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 do the following:

- 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



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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation**.radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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 channel product 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 magazine for Cisco networking professionals. 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 subscribe to *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 where networking professionals 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>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- 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 “Obtaining Documentation” section.

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)

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