



Release Notes for Cisco Unified Videoconferencing 3500 MCU Release 5.0

Revised: June 11, 2006 OL-10587-01

These release notes describe the new features and caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0 for the following Cisco products:

- Cisco Unified Videoconferencing 3515 MCU12
- Cisco Unified Videoconferencing 3515 MCU24
- Cisco Unified Videoconferencing 3545 MCU
- Cisco Unified Videoconferencing 3545 EMP

Use these release notes with *Administrator Guide for Cisco Unified Videoconferencing 3515 MCU12 and MCU24 Release 5.0* and *Administrator Guide for Cisco Unified Videoconferencing 3545 MCU Release 5.0*.



Note

In this document, these products are referred to as Cisco Unified Videoconferencing 3500 MCU unless otherwise noted.



Note

To view the release notes for previous versions of Cisco Unified Videoconferencing 3500 MCU, go to: http://cisco.com/en/US/products/hw/video/ps1870/prod_release_notes_list.html

You can access the latest software upgrades and release notes for all versions of Cisco Unified Videoconferencing 3500 MCU on Cisco Connection Online (CCO) at the following URL:

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

Contents

These release notes include the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0, page 3](#)
- [Caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0, page 3](#)
- [Troubleshooting, page 5](#)
- [Tips, page 5](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation, page 6](#)
- [Documentation Feedback, page 7](#)
- [Cisco Product Security Overview, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 10](#)

Introduction

The Cisco Unified Videoconferencing 3500 MCU is a high performance multipoint video conferencing and media processing system that provides extensive audio and video processing capabilities and web-based conference monitoring and management. The Cisco Unified Videoconferencing 3500 MCU supports a wide range of telephony protocols and media communication networks and is fully interoperable with other video conferencing network devices.

System Requirements

This section includes the following topics:

- [Supported Upgrades, page 2](#)

Supported Upgrades

**Note**

Cisco Unified Videoconferencing 3500 MCU Release 5.0 only operates with the following products: Cisco Unified Videoconferencing 3515 MCU12, Cisco Unified Videoconferencing 3515 MCU24, Cisco Unified Videoconferencing 3545 MCU, and Cisco Unified Videoconferencing 3545 EMP. You cannot install version 5.0 on older IP\VC products, including the Cisco IP\VC 3511 and 3540 MCU.

Upgrading from a previous build of MCU version 5.x

- Step 1** Use the MCU Upgrade Utility to burn the latest version onto the MCU card.
After burning, the Upgrade Utility will reset the platform.
- Step 2** After reset, the latest version is installed on the MCU
-

Caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0

This section includes the following topics:

- [Open Caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0, page 3](#)

Open Caveats for Cisco Unified Videoconferencing 3500 MCU Release 5.0

This section lists possible unexpected behaviors by Cisco Unified Videoconferencing 3500 MCU Release 5.0.

MCU known issues are included in the following categories:

- [Endpoint Information Display in MCU Conference Control, page 3](#)
- [Local View, page 3](#)
- [H.243, page 3](#)
- [DTMF Conference Control, page 4](#)
- [Encryption, page 4](#)
- [Configuration, page 4](#)
- [Video Quality, page 4](#)
- [H.239, page 4](#)
- [Gateway Connectivity, page 4](#)
- [Cascading, page 5](#)
- [SCCP, page 5](#)
- [T.120, page 5](#)

Endpoint Information Display in MCU Conference Control

- The information icon for participants in child conferences does not function. Clicking on it does not perform any action.
- SIF resolutions appear as CIF resolutions on the statistics page.
- Connections with asymmetric resolution (4CIF/CIF) inaccurately show 4CIF for both directions.

Local View

- Local view, defined in the custom layouts section of the advanced video settings, does not appear in the conference control and cannot be used.

H.243

- If the H.323 registration mode is set to gateway when enabling H.243, then in cascaded conferences endpoints appear twice in the conference control. To resolve this, either disable H.243 or change H.323 registration mode to MCU.
- H.243 conference control may not function with some ISDN endpoints that are connected through a gateway.

- When H.243 is enabled, Far End Camera Control (FECC) to some TANDBERG endpoints may not function. To resolve this, disable H.243.

DTMF Conference Control

- In some cases, the MCU spontaneously announces the conference control menu. When this occurs, press '#' to exit the menu.

Encryption

- Encryption does not function with TANDBERG endpoints that support both AES and DES and that are configured to only enable DES. To resolve this, enable AES in the endpoint.
- Encryption and H.239 do not function together.

Configuration

- Using '0' as the service prefix causes unpredictable results. Refrain from using '0' as the service prefix.
- Using special characters ('<', '>', '&') in the service description causes unpredictable results. Refrain from using those characters in the service prefix.

Video Quality

- Joining more than 12 4CIF endpoints into a full-screen conference may result in significant delays.

H.239

- When working with H.264 and presentation view enabled services, some TANDBERG or Aethra endpoints may stop sending the main video when the presentation channel is opening. Use the relevant workaround for the following endpoints
 - TANDBERG MXP–Enable H.239 on the endpoint.
 - TANDBERG classic–Remove H.264 from the service or the endpoint.
 - Aethra–Remove H.264 from the service or the endpoint.
- In cascaded conferences with H.239, make sure that only one presenter is active at any given time. Having simultaneous presenters in a cascaded conference may result in the display of more than one presentation to participants. To immediately solve this issue, keep one presentation open and close all other presentations. For details about how to fix this issue permanently with an advanced command, contact Cisco Technical Support as described at [“Obtaining Technical Assistance” section on page 8](#).
- Some ISDN endpoints connected to the MCU via a gateway may fail to send the presentation channel when using H.239 XGA.
- When working with H.239 XGA in a conference including Sony and Polycom or Sony and TANDBERG endpoints, the presentation video from the Polycom or TANDBERG endpoint may not appear on the Sony endpoint.

Gateway Connectivity

- This version of the MCU does not function well with ISDN gateway downspeeding or resync. Make sure to disable downspeeding on the gateway.

Cascading

- In a cascaded conference, the conference control of the child conference does not indicate the identity of the active speaker. A workaround is to view the conference from the parent MCU that does display this correctly.

SCCP

- When connecting Sony PCS1 in SCCP mode using H.264, video may not open. A workaround is to use H.263 when connecting Sony PCS1 using SCCP.
- Using the TANDBERG Transfer button in an SCCP conference with only one participant results in a video freeze or no video. This does not happen in conferences with more than one participant.
- When adding a new SCCP service, an irrelevant error message may display. To resolve this issue, and enable the creation of the service, open the Advanced management and security dialog box, and then press OK.
- Configuring SCCP services to work in audio mode only may result in an MCU crash. Please note that this does not apply to a video SCCP service that can accept audio calls.

T.120

- T.120 does not function across cascaded conference
- The Join Data Conference button on the MCU conference control page allows users to join T.120 data conferences from the computer running the conference control. This button is currently not available in V5.0 and will be re-added in a later patch.

Troubleshooting

For troubleshooting information, see the Troubleshooting chapter in the *Administrator Guide for Cisco Unified Videoconferencing 3515 MCU12 and MCU24 Release 5.0* and *Administrator Guide for Cisco Unified Videoconferencing 3545 MCU Release 5.0* at the following URL:

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

Tips

- When the Windows **Start Navigation** sound is enabled, a continuous clicking sound is heard when the Conference Control interface automatically refreshes. Disable this sound in the **Sounds and Multimedia** configuration of the Control Panel.
- The Conference Control web interface operates in polling mode with updates every 10 seconds. To refresh information on the screen, reselect the tab you are currently viewing. Pressing the browser **Refresh** button causes you to exit from the Conference Control and displays the login screen.
- The Conference Control and Login screens are best viewed in full screen mode (1024 x 768 fps).
- The MCU allows you to open multiple Conference Control browser screens at the same time. It is recommended that you close screens in which you are not currently working to avoid confusion and performing operations on the wrong conference.

Related Documentation

- For administration documentation, see the *Administrator Guide for Cisco Unified Videoconferencing 3515 MCU12 and MCU24 Release 5.0* and *Administrator Guide for Cisco Unified Videoconferencing 3545 MCU 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. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you will find information about how to:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

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

- For Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

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

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

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

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

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

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

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

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

This document is to be used in conjunction with the documents listed in the “Related 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)

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.

