System Release Notes for IP Telephony: Cisco Unified Communications System, Release 5.1(1)

Contents

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

Overview

It is standard methodology for Cisco Systems to perform system-wide testing of the Cisco Unified Communications family of products, supplementing the product-level testing performed on each Cisco Unified Communications product. This document provides release notes for the testing conducted on systems composed of Cisco voice gateways, routers, Catalyst switches, firewalls, IP phones and the following components:

- Cisco Unified CallManager and Cisco Unified CallManager Express
- Cisco Customer Response Solutions (Cisco Unified Contact Center Express)
- Cisco SIP Proxy Server
- Cisco Unified Presence Server
- Cisco Unified Survivable Remote Site Telephony (SRST)
- Cisco Unity (with Microsoft Exchange 2000/2003 and IBM/Lotus Domino), Cisco Unity Connection and Cisco Unity Express
- Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express
- Cisco Emergency Responder
- Cisco Fax Server
- Cisco Unified Videoconferencing multipoint control units (MCUs)
- Network management tools such as Cisco Unified Operations Manager and CiscoWorks Resource Manager Essentials

The focus of this document is on the IP telephony components of Cisco Unified Communications system testing. IP contact center components have also been tested. For additional information on contact center components, please see:
http://www.cisco.com/iam/unified/ipcc3/index.htm

A major deliverable of the System Release and Cisco Unified Communications testing is a recommendation of compatible software releases that have been verified by the test for customers. The recommendations are not exclusive and are in addition to interoperability recommendations for each of the individual voice application or voice infrastructure products. See System Requirements, page 12 for more information.

Tested Functionality

The system-wide testing of IP telephony functionality for Cisco Unified Communications Release 5.1(1) included the following:

- Testing on two distinct upgrade paths for North America IP telephony main components:
  - Multistage upgrade from IP Communications System Test Release 4.2 versions to Cisco Unified Communications Release 5.1(1) versions. For a list of the base Release 4.2 versions, see the *Systems Release Notes for North America IPT: IP Communications Systems Test Release 4.2* at: http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/gblink/system/gbtst4x/4_2/rng42nip.htm
  - Single stage upgrade from Cisco Unified Communications Release 5.0(2) versions Cisco Unified Communications Release 5.1(1) versions. For a list of the base Release 5.0(2) versions, see the *System Release Notes for IP Telephony: Cisco Unified Communications System, Release 5.0(2)* at: http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc502/relnotes/rnipt502.htm

Note For a list of the target Cisco Unified Communications Release 5.1(1) versions that the main components were upgraded to, see Software Version Matrix, page 14.

- Testing on a Multisite Distributed deployment topology, including changes to the following site models since Cisco Unified Communications Release 5.0:
  - Redesignated the Raleigh (RDU) site as the Medium Site (North America) site model
  - Added a new Roxboro (RXB) site as the Small Site (North America) site model
  - Added Cisco Unified MeetingPlace Express servers to the Very Large Campus with Clustering over the WAN (SJC-RFD) North American site model
  - Added two Survivable Remote Site Telephony (SRST) remote sites to the Large SIP Site (DFW) North American site model
  - Replaced SRST routers in the Paris (CDG) remote sites with Unified CallManager Express servers to support Unified CallManager fallback
- Interoperability testing of Cisco Unified Personal Communicator with Unified MeetingPlace Express.
- Testing of new Unified MeetingPlace Express features, such as ah-hoc videoconferencing and integration with Microsoft Outlook.
- Testing Unified CallManager phones falling back to a Cisco Unified CallManager Express server following a WAN outage (similar to fallback to an SRST router).
- Video call testing involving new releases and components, such as Cisco Unified Video Advantage 2.0(2), Cisco Unified Videoconferencing 5.0(1) running on MCU 3545 hardware, and Cisco Unified Personal Communicator as a SIP video client.
- Testing of a new 3rd party component, the Berbee InformaCast system that supports audio and text message broadcasting to IP phones.
- Expanded testing of Cisco Unified Operations Manager for network management and the addition of Cisco Unified Service Monitor for voice quality monitoring.

New and Changed Features

This release of Cisco Unified Communications includes the following new or upgraded significant components since Release 5.0(2):

- Cisco Unified CallManager 5.1(1)
- Cisco Unified CallManager Express 4.0(2)
- Cisco Emergency Responder 1.3(2)
- Cisco Unified Presence Server 1.0(3)
- Cisco Unified MeetingPlace 5.4
- Cisco Unified MeetingPlace Express 1.2(1)
- Cisco Unity Connection 1.2(1)
- Cisco Unified Operations Manager 2.0
- Cisco Unified Service Monitor 2.0
- Cisco Unified Personal Communicator 1.1(2)/1.1(3)
- Cisco IOS 12.4(11)T

The following sections list the features of each new or upgraded component tested in this release.

Cisco Unified CallManager

Unified CallManager Release 5.1(1) includes the following changes and updates to functionality since Release 5.0(4):

- Cisco Unified CallManager Administration enhancements including:
  - DirSync service synchronizes information from additional types of corporate directories, such as Microsoft Active Directory or Netscape/iPlanet Directory, to the Cisco Unified CallManager database
  - TFTP Service Parameter no longer offers the Enable Caching of Configuration Files option
  - The Basic and Advanced Third-Party SIP Phone Configuration windows include a check box called Require DTMF Reception
- New service parameters have been added for the following features:
  - Immediate Divert (iDivert): Use Legacy iDivert, Allow QSIG During iDivert, iDivert User Response Timer
  - Music On Hold: Multicast MOH Direction Mode for SIP
- A new enterprise parameter, Advertise G.722 Codec, was added to determine whether Cisco Unified IP Phones will advertise the G.722 codec to the Cisco Unified CallManager. This parameter only applies to Cisco Unified IP Phone models 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE.
- Installation updates to the Cisco Unified Real Time Monitoring Tool (RTMT) plug-ins, such as the Cisco Unified CallManager Real-Time Monitoring Tool-Linux and Cisco Unified CallManager Real-Time Monitoring Tool-Windows
- Several security feature changes, including an ExcludeDigest Credentials option for encrypted files supported by Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960 only.

- New menus in the Bulk Administration Tool include a Region Matrix menu to populate and depopulate the region matrix.
- Enhanced reporting, troubleshooting, phone and softkey features.

For a detailed description of these features and functionality, see *Cisco Unified CallManager Release 5.1(1) New and Changed Information Guide* at:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a0080731b6c.html

and *Release Notes for Cisco Unified CallManager Release 5.1(1)* at:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_note09186a008079a217.html

Cisco Unified CallManager Express

Unified CallManager Express Release 4.0(2) includes the following changes and updates to functionality since Release 3.4(0):

- FXO trunk enhancements—The following FXO trunk enhancements are introduced to improve the keyswitch emulation behavior of PSTN lines in a Cisco Unified CallManager Express system:
  - FXO port monitoring—Allows the line button on IP phones to reliably show the status of an FXO port when the port is in use. The status indicator, either a lamp or an icon, depending on the phone model, accurately displays the status of the FXO port during the duration of the call, even after the call is forwarded or transferred. The same FXO port can be monitored by multiple phones using multiple trunk ephone-dns.
  - Transfer recall—If a transfer-to phone does not answer after a specified timeout, the call is returned to the phone that initiated the transfer and it resumes ringing on the FXO line button. The ephone-dn must be dual-line and must have the huntstop channel command configured.
  - Transfer-to button optimization—When an FXO call is transferred to a private extension button on another phone, and that phone has a shared line button for the FXO port, after the transfer is committed and the call is answered, the connected call displays on the FXO line button of the transfer-to phone. This frees up the private extension line on the transfer-to phone. The ephone-dn must be dual-line and it must have the huntstop channel command configured.
  - Dual-line ephone-dns— Ephone-dns for FXO trunk lines can now be configured for dual-line to support the FXO monitoring, transfer recall, and transfer-to button optimization features.
- An enhancement to the automatic line selection feature allows incoming calls to be automatically answered on a specific line. The line associated with a specified button is selected automatically for both incoming and outgoing calls when the auto-line command is used with the button argument and answer-incoming keyword.
- The behavior of silent ringing, configured on the phone by using the s keyword with the button command, is suppressed when used with the night service feature. Silent ringing is overridden and the phone audibly rings during designated night-service periods.
- Support for Cisco IP Communicator with Cisco Unified Video Advantage on the same computer.
- Support for Unified CallManager phones to fall back to a Cisco Unified CallManager Express server following a WAN outage (similar to falling back to an SRST router) with full Unified CallManager Express functionality.

For a detailed description of these features and functionality, see *Cisco Unified CallManager Express New Features* at:

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_feature_guide09186a00806401f7.html

Cisco Emergency Responder

Cisco Emergency Responder Release 1.3(2) includes the following changes and updates to functionality since Release 1.3(1a):

- Detection of changes in the switch-port association of wired Cisco Unified IP Phones. An incremental or full discovery cycle detects Cisco Unified IP Phones that have changed switch-port associations or are newly discovered. Cisco Unified IP Phones that become missing during a complete discovery are also reported. Cisco Emergency Responder notifies the system administrator of these changes by email.
- Support for Cisco Unified CallManager Release 5.1(1) in addition to the previously-supported Cisco Unified CallManager releases 5.0, 4.2, 4.1, 4.0, and 3.3.
- Support for Cisco IP Communicator 2.0.

For a detailed description of these features and functionality, see the *Release Notes for Cisco Emergency Responder 1.3(2)* available at:

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_release_note09186a008077aa78.html

Cisco Unified Presence Server

Unified Presence Server Release 1.0(3) includes the following changes and updates to functionality since Release 1.0(1):

- A new *Cisco Unified Presence Server Deployment Guide* is available, which documents how to integrate Cisco Unified Presence Server with Cisco Unified CallManager, as well as with the required Microsoft servers and products, including
  - Microsoft Office Live Communications Server 2005 with Service Pack 1 (SP1)
  - Microsoft Windows Server 2003 Active Directory
  - Microsoft Office Communicator 2005
- The new Configuration Troubleshooter can diagnose configuration issues after the initial configuration of the Cisco Unified Presence Server or whenever changes are made. The Troubleshooter performs a set of tests on both the Cisco Unified Presence Server cluster and on the Cisco Unified CallManager cluster to validate the Cisco Unified Presence Server configuration.
- Ability to locate users with Microsoft Office Communicator (MOC) installed on their computer
- Ability to configure Computer Telephony Interface (CTI) gateways
- Expanded System Status display which now shows the following items:
  - Number of end users
  - Number of phone devices
  - Number of licensed Cisco Unified Presence Server end users
  - Number of licensed Cisco Unified Personal Communicator end users
  - Number of assigned Microsoft Office Communicator end users

For a detailed description of these features and functionality, see the *Release Notes for Cisco Unified Presence Server Release 1.0(3)* at:

http://www.cisco.com/en/US/docs/voice_ip_comm/cups/1_0_3/rel_notes/release/notes/cps103rn.pdf

Cisco Unified MeetingPlace

Unified MeetingPlace Release 5.4 includes the following changes and updates to functionality since Release 5.3:

- Expanded support for video conferencing provided by additional fields in the database, MeetingTime, and applicable reports.
- New fields in MeetingTime for reservationless meetings to set the following options:
  - Internet access during meetings
  - Growth limits for ports that can be set independently of those settings for scheduled meetings
- In Unified MeetingPlace for Outlook, for single and recurring meetings that are scheduled through Outlook, an assistant can be delegated to schedule a meeting and invite participants. An invitee can also delegate an assistant to accept or reject the meeting invitation.
- Video participants can now join a continuous meeting on an ad hoc basis, provided there are adequate video resources.
- Cisco Unified MeetingPlace Video Integration now allows:
  - Users to schedule video-only meetings. If no audio ports are scheduled, the audio link between the Cisco Unified Videoconferencing MCU and the Cisco Unified MeetingPlace Audio Server is not established. Audio for the meeting can be provided only by the video MCU.
  - A new User Profile Type—"video terminal"—which represents video endpoints. Video terminal profiles are created in Video Administration for Cisco Unified MeetingPlace and are then synchronized to Cisco Unified MeetingPlace Web Conferencing by using the Replication Service. Having the profile information in both components enables the scheduling, reporting, and displaying of video endpoints for video conferences.
- Cisco Unified MeetingPlace Video Integration now includes and requires the Video Administration for Cisco Unified MeetingPlace component. The Video Administration component provides the following features:
  - Managing and monitoring video conference devices—Manage the resource usage of video
  - Scheduling and managing meetings—Schedule future conferences and endpoint-initiated ad hoc conferences. Monitor in-session conferences and control them via in-conference control APIs. Display and manage scheduled and ad hoc meetings.
  - Network management—Define IP network topology to allow intelligent management of an IP network and to save valuable network resources. Define ISDN network topology to schedule ISDN calls via a least-cost routing mechanism.
  - Virtual MCU—Transparently manage a pool of MCU ports. Provide a single conference ID to end users for a meeting hosted across multiple MCUs with different physical conference IDs.
  - Cascading video conferences—Cisco Unified MeetingPlace video conferences are no longer limited to a single MCU. The new Video Administration component enables Cisco Unified MeetingPlace to communicate with multiple MCUs transparently. If there are multiple MCUs in the same conference, the Video Administration component designates one of the MCUs as the primary MCU for that conference; the rest of the MCUs are designated secondary MCUs. Cisco Unified MeetingPlace establishes an audio link with only the primary MCU. The secondary MCUs all connect to the primary MCU.

Note Note Cisco Unified MeetingPlace does not support a mixed environment of both Cisco Unified Videoconferencing MCU Release 4.0 and Release 5.0. When using Release 4.0, the cascading video meeting feature is not available.

  – Dynamic cascading—If a conference is scheduled to have "local first" priority, endpoints connect to a local MCU first, and then the local MCU cascades to the master MCU to form a larger conference. Ad hoc conferences are created with "local first" priority, and therefore support dynamic cascading.

- Cisco Unified MeetingPlace Web Conferencing now supports scheduling recurring meetings.

For a detailed description of these features and functionality, see the Release Notes for various Unified MeetingPlace components available at:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html

Cisco Unified MeetingPlace Express

Unified MeetingPlace Express Release 1.2(1) includes the following changes and updates to functionality since Release 1.1(2):

- The Cisco Unified MeetingPlace Express VT offering provides ad hoc voice, video, and web conferencing capabilities for video telephony using Cisco Unified CallManager. Ad hoc conferences are initiated through the end-user interfaces of products other than Cisco Unified MeetingPlace Express. For example, you can initiate either a voice-only or a voice-and-video ad hoc conference by using the "Meet-Me" button or the "Conf" button on Cisco Unified IP Phones that are registered to Cisco Unified CallManager. You can also initiate voice, video, and web conferences through Cisco Unified Personal Communicator.
- When Cisco Unified MeetingPlace Express is integrated with Microsoft Outlook, end users can schedule, reschedule, and cancel meetings from the Microsoft Outlook calendar. Microsoft Outlook notifications can be sent whether the meetings were scheduled, rescheduled, or canceled from the Microsoft Outlook calendar or from the Cisco Unified MeetingPlace Express end-user web interface. When end users accept an invitation, the meeting information and a click-to-attend link become available from their Microsoft Outlook calendar.
- Voice meeting recordings are now included in the archiving process. As files that are external to the database, voice meeting recordings and user name recordings are not included in the L0, L1, or L2 database backup files, which are stored on the Cisco Unified MeetingPlace Express server. Nevertheless, both voice meeting recordings and user name recordings are included in the archiving process, in which the database backup files and critical external files are copied to a remote server. End users may also download meeting recordings, rename them, and save them on their PCs.

For a detailed description of these new and enhanced features and functionality, see *Release Notes for Cisco Unified MeetingPlace Express Release 1.2* at:

http://www.cisco.com/en/US/products/ps6533/prod_release_note09186a008075557d.html

Cisco Unity Connection

Unity Connection Release 1.2(1) includes the following changes and updates to functionality since Release 1.1:

- A new license tag, LicRegionIsUnrestricted, added to the Connection license file is required to upgrade from Unity Connection Release 1.1 to 1.2.

- New languages are available for additional localization support. Also, with a Cisco Unity Connection multilingual system, users and administrators have the option of providing greetings in multiple languages so that callers can hear the greeting in their own language.
- Cisco Unity Connection users with the voice-recognition option can now:
  - Delete all messages in the Deleted Items folder by phone by saying “Empty Deleted Items folder” at the Main menu
  - Send messages to public and private distribution lists by phone by saying the name of a distribution list when addressing a message.
  - Play, record, enable, and disable their greetings by using voice commands.
- With a Cisco Unity Connection system using the voice-recognition option, administrators can create voice-type directory handlers so that callers can say the first name and last name of a Connection user they want to reach. In addition to searching by first and last names, a voice directory handler includes alternate names in searches.
- A new Voice Recognition Confirmation Confidence Threshold setting allows administrators to adjust the likelihood that Cisco Unity Connection will prompt voice-recognition users to confirm an intended action.
- The Cisco Unity Connection Administration interface has been changed to improve usability.
- Message counts are no longer truncated in SMS (SMPP) message notifications.
- Message notifications to text devices (SMTP, SMS, text pager, or the Cisco Unity Inbox web tool) now include Calling Line ID (CLID) information when the Include Caller Information check box is checked.

For a detailed description of these new and enhanced features and functionality, see *Release Notes for Cisco Unity Connection Release 1.2(1)* at:

http://www.cisco.com/en/US/products/ps6509/prod_release_note09186a00806b7bfb.html

Cisco Unified Operations Manager

Unified Operations Manager Release 2.0 includes the following changes and updates to functionality since Release 1.1:

- Trunk group modeling; performance, capacity and availability monitoring.
- Support for video endpoint discovery, monitoring and reporting.
- Acceptance testing, phone feature testing, dial-plan validation, and phone-to-phone testing.
- New device support:
  - Cisco Unified CallManager Release 5.1(1)
  - Cisco Unified Presence Server
  - Cisco SIP Proxy Server
  - Cisco Unity Express Release 2.3
- Feature-based licensing. There are two levels of functionality that you can purchase for Cisco Unified Operations Manager: Premium Edition and Standard Edition.
  - Premium Edition—Full feature Unified Operations Manager
  - Standard Edition—Limited feature Unified Operations Manager
- Enhancements to:

- Device monitoring
- Synthetic testing
- Phone reporting
- Performance graphing

For a detailed description of these features and functionality, see the *Release Notes for Cisco Unified Operations Manager Release 2.0* at:

http://www.cisco.com/en/US/products/ps6535/prod_release_note09186a008077a5d8.html

Cisco Unified Service Monitor

Unified Service Monitor Release 2.0 includes the following changes and updates to functionality since Release 1.1:

- Cisco Unified CallManager support—Service Monitor can monitor calls from Cisco Unified CallManager clusters solely or, in conjunction with monitoring calls from sensors.
- Cluster and sensor management—You can suspend and resume clusters and sensors from monitoring.
- Cisco 1040 Sensor management—The following changes have been introduced:
  - TFTP servers—Instead of just one TFTP server, multiple TFTP servers can be added to Service Monitor. Service Monitor now automatically copies any updated sensor configuration files to the TFTP servers if permitted by the security settings on them.
  - Sensor IDs—MAC addresses replace the naming scheme formerly used for sensor IDS; in addition, you can add a descriptive name for a sensor.
  - Sensor-calculated MOS—When there is voice activity on an endpoint, sensors send data to Service Monitor every 60 seconds without determining whether a threshold has been violated.
  - Trap suppression—Service Monitor 2.0 introduces a setting to reduce the number of traps that Service Monitor sends for each endpoint.
  - Failover from Primary Service Monitor—Sensor failover to a secondary Service Monitor is still supported; the ability to define and fail over to a tertiary Service Monitor is no longer supported.
- Reports—Service Monitor reports display MOS, endpoints involved in voice activity and other details obtained from sensors and clusters during the last 30 days. Service Monitor supplies separate sensor and Cisco Voice Transmission Quality (CVTQ) reports.
- Threshold for each codec—Service Monitor supplies a set of global thresholds that enable you to set a MOS threshold value for each supported codec. You can selectively override global thresholds by creating sensor threshold groups and CVTQ threshold groups.
- Licensing—Specifies the number of phones that Service Monitor can monitor; in releases earlier than 2.0, licensing specified the number of sensors that could register with Service Monitor.
- SNMP trap changes—The MOS violation trap TT field now specifies whether the trap was generated for sensor-based data or cluster-based data. The trap definition includes new fields for each type of data:
  - Cluster-based data—Concealment seconds, concealment ratios, and other cluster-specific information.
  - Sensor-based data—Number of traps that were suppressed, if any, and the time when Service Monitor started and stopped suppressing traps for the endpoint.

For a detailed description of these features and functionality, see the *Release Notes for Cisco Unified Service Monitor Release 2.0* at:

http://www.cisco.com/en/US/products/ps6536/prod_release_note09186a0080797e38.html

Cisco Unified Personal Communicator

Unified Personal Communicator Release 1.1(2) for Mac OS/Windows OS includes the following changes and updates to functionality since Release 1.1:

- Cisco Unified Personal Communicator Release 1.1(2) now supports Apple Mac OS X. This release provides the same features and functionality as that provided in Cisco Unified Personal Communicator Release 1.1(2) for Windows OS:
  - View real-time availability of other people who use Cisco Unified Personal Communicator.
  - Click-to-call from the contact list within Cisco Unified Personal Communicator instead of dialing telephone numbers
  - Use either the integrated soft phone or an associated Cisco Unified IP Phone.
  - Exchange ideas face-to-face by using a video display on your computer screen.
  - Add communication methods during a session; for example, you can add video to an existing audio session or add web conferencing to an existing video session.
  - Create conference calls by simply merging conversation sessions.
  - View, play back, sort, and delete voice-mail messages, all from the same client application.

  Cisco Unified Personal Communicator for Mac OS X also has these features:
  - Select the text of a phone number in almost any application and use the OS X Services menu (or key combination to that menu) to cause Cisco Unified Personal Communicator to dial the selected number.
  - From within the Apple Address Book application, dial phone numbers through Cisco Unified Personal Communicator. This capability is provided through integration with the Address Book.
- In the Windows version of Cisco Unified Personal Communicator, the new Cisco Unified Problem Reporting Tool can be used to automate the trace and crash-dump collection process on the client PC. The tool collects installation, application, and client PC system information. It also creates a dump file in the event that the application crashes.

For a detailed description of these features and functionality, see the *Release Notes for Cisco Unified Personal Communicator* at:

http://www.cisco.com/en/US/products/ps6844/prod_release_note09186a00805f6b3f.html

Cisco IOS

IOS Software Release 12.4(11)T includes the following changes and updates to functionality since Release 12.4(6)T1:

- Out-of-band Dual Tone Multi Frequency (DTMF) using Key Press Stimulus (KPML)—Enables SIP Phones (TNP Phones only) to report digits collected during the signaling phase as well as when the call is connected (Out-of-band DTMF) with KPML. This feature is available on SIP gateways for non-conferencing dialogs and for interoperability between SIP products such as Unified CallManager and Unified SIP IP Phones. The main functionality includes Out-of-band DTMF digit reporting using KPML for SIP gateway non-conferencing SIP calls and SIP dialpeer configuration of KPML as a DTMF relay method.

- SIP session timer—Enables IOS gateways as well as the SIP Portable common stack to comply with the latest IETF Session Timer RFC 4028. This feature helps call stateful proxies as well as user agents to determine if the SIP session is still active. From the user agent standpoint, this feature is needed by devices like Unified CallManager that do not handle media streams. For IOS gateways, RTP/RTCP activity can also help determine if a SIP session is alive or not.
- High-density voice feature card—Supports up to six PVDM2-64 C5510 DSP SIMM modules on the Dial Feature Card (DFC) form factor on the AS5xx0XM voice gateways. This increases the density of the Feature Card to 384 Low Complexity (192 Medium Complexity) VoIP calls.
- Media preservation for H.323 VoIP calls—Supports H.323 call preservation for calls between an endpoint controlled by Unified CallManager and an IOS voice gateway when the TCP connection between Unified CallManager and the gateway is lost. It also includes preserving calls in other scenarios where the signaling and media paths are different and the connection loss occurs on the signaling path.
- SIP MWI NOTIFY - QSIG translation—Enhances MWI functionality to include SIP-MWI-NOTIFY-to-QSIG-MWI translation between Cisco gateways or routers over a LAN or WAN and extends message waiting indicator (MWI) functionality for SIP MWI and QSIG MWI interoperation to enable sending and receiving MWI over QSIG to a PBX. When the SIP Unsolicited NOTIFY is received from voice mail, the Cisco router translates this event to activate QSIG MWI to the PBX, via PSTN. The PBX will switch on, or off, the MWI lamp on the corresponding IP phone

For a detailed description of these and other new and enhanced features and functionality, see *Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 3: New Feature Descriptions and Important Notes* at:

http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19ae.html

System Requirements

This section provides information about the software versions of the Cisco and third-party components and the firmware versions of the Cisco Unified IP phones used in system-wide testing of Cisco Unified Communications Release 5.1(1). This section contains the following information:

End-of-Sale Components

The following components have reached end-of-sale (EOS) status but are still supported, and since they may be present in existing customer deployments, remained installed in the test bed sites for this Cisco Unified Communications release:

- Cisco MCS-7825-H1
- Cisco MCS-7825I-3000
- Cisco MCS-7845H-2400
- Cisco 2611
- Cisco 2621

- Cisco 2651
- Cisco switch/router modules:
  - WS-X6624-FXS Analog Interface Module
  - NM-HDV High Density Voice Network Module
  - NM-1V/2V Low-Density Analog Interface Module
  - VIC-2FXO/2FXS Low Density Voice/Fax Network Module
- Analog Telephone Adaptor models ATA186-I1/I2 and ATA188-I1/I2
- Cisco VT Advantage (CVT-ADV-E1)
- Unified Videoconferencing 3526 PRI Videoconferencing Gateway
- Unified Videoconferencing Multipoint Control Unit 3511

The EOS date is the last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale. There is also an end-of-life (EOL) cycle that is a process that guides the final business operations associated with the product life cycle.

The EOL process consists of a series of technical and business milestones and activities that, once completed, make a product obsolete. Once obsolete, the product is not sold, manufactured, improved, repaired, maintained, or supported.

For information about recommended replacements, see the comprehensive list of announcements at End-of-Life and End-of-Sale Products at the following URL:

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

For information on specific products, choose a product from the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html. Then click on the End-of-Life and End-of-Sale Notices link in the Product Literature box.

For an overview of the Products and Services EOL policy, see the information at the following URL:

http://www.cisco.com/en/US/products/products_end-of-life_policy.html

Deployment Considerations

The tables in this section list the recommended software and firmware releases based on Cisco Unified Communications Release 5.1(1). Note that not every rebuild is tested as part of Cisco Unified Communications. Therefore, additional regression testing in a customer or Cisco-specific certification lab is recommended before deployment.

When deploying IP Communications in a customer environment, please remember the following:

- At the minimum, customers should deploy the software release recommended in these tables.
- For CSA, customers should use the latest engine and policy release. CSA software is available at:

  http://www.cisco.com/cgi-bin/tablebuild.pl/csa
- For other software components, customers should use the most current rebuild of a maintenance release. For IOS, information about the latest releases, including deferral advisories, is available at:

  http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml
- If the recommended release has been deferred to a subsequent release, customers should use the subsequent release.

- Before deploying a release, examine the open caveats in the chosen release to determine if any will impact your implementation. Open caveats can be viewed through the Bug Toolkit, located at:

  http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

- In system upgrades, deploy the chosen release in a lab environment that uses the same product components as the customer's product components before moving it to a production environment.

Software Version Matrix

Table 1 lists the software release versions of both Cisco and third-party components used in the Cisco Unified Communications Release 5.1(1) system test.

Table 1 Software Release Versions in Cisco Unified Communications Release 5.1(1) for IP Telephony

Component	Release Version
Cisco Unified CallManager	5.1(1)
Cisco Unified CallManager—Operating System	Bundled with Unified CallManager
Cisco Customer Response Solutions (Cisco Unified Contact Center Express)	4.5(2)
Cisco Customer Response Solutions—Operating System	2000.4.3aSR6
Cisco Emergency Responder	1.3(2)
Cisco Emergency Responder—Cisco IP Telephony Operating System	2000.4.3aSR6
Cisco Unified Presence Server	1.0(3)
Cisco Unity, TSP	4.2(1) ES27, 8.1(2)
Cisco Unity—Microsoft Exchange Server	Microsoft Exchange 2003 SP2 (on Cisco Unity and partner Exchange servers), Microsoft Exchange 2000 Post-SP3 Update Rollup (on other message store servers)
Cisco Unity—IBM Lotus Domino[1]	6.5 with DUC 1.2.3
Cisco Unified MeetingPlace Audio Server	5.4.0.15
Cisco Unified MeetingPlace IP Gateway	5.2.2.5
Cisco Unified MeetingPlace Web Conferencing	5.4.70.0
Cisco Unified MeetingPlace Gateway SIM	5.2.0.60
Cisco Unified MeetingPlace Video Integration	5.4.58.0
Cisco Unified MeetingPlace Video Administration Server	5.4.0.104
Cisco Unified MeetingPlace for Outlook	5.4.12.0
Cisco Unified MeetingPlace MeetingTime	5.4.0.14
Cisco Unified CallManager Express	4.0(2)/IOS 12.4(11)T
Cisco Unity Express	2.3(3)
Cisco Unity Connection	1.2(1)
Cisco Unified MeetingPlace Express	1.2(1)
Cisco Unified Survivable Remote Site Telephony (SRST)	4.0(2)/IOS 12.4(11)T
Cisco Unified Videoconferencing 3515 MCU[1]	5.0.58

Table 1 Software Release Versions in Cisco Unified Communications Release 5.1(1) for IP Telephony (continued)

Component	Release Version
Cisco Unified Videoconferencing 3540 MCU	4.2.10
Cisco Unified Videoconferencing 3545 MCU	5.0.1.0.12
Cisco Unified Videoconferencing Enhanced Media Processor (EMP) Module	5.0.64
Cisco Unified Videoconferencing 3521 BRI Gateway[1]	5.0.22
Cisco Unified Videoconferencing 3526 PRI Gateway[1]	5.0.22
Cisco 1760 (voice/data gateway)[1]	12.4(11)T
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691 (router)	12.4(11)T
Cisco 2801, 2821, 2851, 3825, 3845 (router, voice/data gateway)	12.4(11)T
Cisco 3745 (gatekeeper)	12.4(11)T
Cisco 3745 (IP-to-IP gateway)[1]	12.4(11)T
Cisco 3725, 3745 (voice/data gateway)	12.4(11)T
Cisco 3725, 3745, 3825 (SRTP[2] and Secure SRST gateways)	12.4(11)T
Cisco 7206 (voice/data gateway)	12.4(11)T
Cisco Catalyst 3500 XL Series (access switch)	12.0(5)WC15
Cisco Catalyst 3550 (access switch)	12.2(25)SEE2
Cisco Catalyst 3560 (access switch)	12.2(25)SEE2
Cisco Catalyst 3750 (data center switch)	12.2(25)SEE2
Cisco Catalyst 4506 (access switch)[1]	12.2(25)EWA6
Cisco Catalyst 6506, 6509 (voice access switch, Supervisor Engine 2/MSFC2)	CatOS 8.5(6) / 12.2(18)SXF6
Cisco Catalyst 6506, 6509 (core switch, Supervisor Engine 720)	12.2(18)SXF6 (native-mode)
Cisco Catalyst Communications Media Module (CMM)	12.4(11)T
Cisco Catalyst 6500 Series Firewall Services Module (FWSM)	3.1(4)
Cisco Catalyst 6608, 6624 (voice gateway)	Bundled with Unified CallManager See Firmware Version Matrix, page 16
Cisco VG224 (analog voice gateway)	12.4(11)T
Cisco VG248 (analog voice gateway)	1.3(1)ES8.2
Cisco ATA 186,188 (analog telephony adaptor)	Bundled with Unified CallManager See Firmware Version Matrix, page 16
Cisco Security Agent—Unified CallManager	4.5.1(657-2)
Cisco Security Agent—Cisco Emergency Responder	5.0.0.194-3.0.2
Cisco Security Agent—Cisco Customer Response Solutions	5.0.0.194-3.0.2
Cisco Security Agent—Cisco Unity	4.5.1.639-2.0.3
Cisco Fax Server	9.0
Cisco PIX 535 Security Appliance	7.2(2)
Cisco SIP Proxy Server	2.2.1.11
Cisco Unified MobilityManager	1.2(2)
Cisco Unified Operations Manager	2.0

Table 1 Software Release Versions in Cisco Unified Communications Release 5.1(1) for IP Telephony (continued)

Component	Release Version
Cisco Unified Service Monitor	2.0
Cisco Resource Management Essentials (RME)	4.0.3
Cisco Unified IP Phones models 7905G, 7911G, 7912G, 7920, 7935, 7940G, 7941G 7960G, 7961G, 7970G, 7971G, 7985	Bundled with Unified CallManager See Firmware Version Matrix, page 16
Cisco Unified Video Advantage	2.0(2)
Cisco Aironet Access Point (AP) 1200G	12.3(8)JA2
Cisco IP Communicator	2.0(2)
Cisco Unified Personal Communicator	1.1(2)
Berbee Informacast Overhead Paging System (OHPS)	5.0.4
McAfee Anti-virus	Enterprise 8.0.0 Patch Version: 11

1. Tested in EUEM site models only during Cisco Unified Communications Release 5.1(1) system testing.
2. SRTP supported for MGCP and H.323 gateways only (not on SIP gateways).

Firmware Version Matrix

Table 2 lists the firmware versions of the Cisco Unified IP Phones, analog adaptors, voice gateways and conference bridges used in the Cisco Unified Communications Release 5.1(1) system test.

Table 2 Firmware Versions for Cisco Devices in Cisco Unified Communications Release 5.1(1) for IP Telephony

Component	SCCP Firmware Version	SIP Firmware Version
Cisco Unified IP Phone 7902G[1]	CP7902080002SCCP060817A	—
Cisco Unified IP Phone 7905G[2]	CP7905080002SCCP060817A	CP7905080001SIP060412A
Cisco Unified IP Phone 7911G[2]	SCCP11.8-2-0-55S	SIP11.8-2-0-55S
Cisco Unified IP Phone 7912G[2]	CP7912080002SCCP060817A	CP7912080001SIP060412A
Cisco Unified IP Phone 7920[2]	CMTERM_7920.4.0-03-00	—
Cisco Unified IP Phone 7935[2]	P00503021500	—
Cisco Unified IP Phone 7936[2]	CMTERM_7936.3-3-12-0	—
Cisco Unified IP Phone 7940G	P00308000400	P0S3-08-5-00
Cisco Unified IP Phone 7941G-GE[3]	SCCP41.8-2-0-55S	SIP41.8-2-0-55S
Cisco Unified IP Phone 7960G	P00308000400	P0S3-08-5-00
Cisco Unified IP Phone 7961G-GE	SCCP41.8-2-0-55S	SIP41.8-2-0-55S
Cisco Unified IP Phone 7970G	SCCP70.8-2-0-55S	SIP70.8-2-0-55S
Cisco Unified IP Phone 7971G-GE	SCCP70.8-2-0-55S	SIP70.8-2-0-55S
Cisco Unified IP Phone 7985	CMTERM_7985.4-1-2-0	—
Cisco ATA 186, 188 (analog telephony adaptor)[2]	ATA030203SCCP051201A	—
Cisco Catalyst 6608 (voice gateway)[2]	D00404000028[4]	
Cisco Conference Bridge WS-X6608[2]	C00104000001[4]	

1. Phone model tested in EUEM site models only during Cisco Unified Communications Release 5.1(1) system testing.
2. Device not tested for SRST failover during Cisco Unified Communications Release 5.1(1) system testing.
3. SRST failover tested on phone model with SIP firmware load installed only, not with SCCP firmware load.
4. Only endpoints such as IP phones and analog telephone adaptors have separate firmware loads to support SCCP or SIP protocols; gateways and conference bridges do not.

Related Documentation

The following URLs provide access to documentation for related products:

- Cisco Unified Communications:
  http://www.cisco.com/go/unified-techinfo
- Voice documentation:
  http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html
- Cisco Unified CallManager:
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Cisco Unified CallManager Express:
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html
- Cisco Customer Response Solutions (Cisco Unified Contact Center Express Edition):
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
- Cisco Unified MobilityManager:
  http://www.cisco.com/en/US/products/ps6567/tsd_products_support_series_home.html
- Cisco Unified Presence Server
  http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html
- Cisco Unified Survivable Remote Site Telephony (SRST):
  http://www.cisco.com/en/US/products/sw/voicesw/ps2169/tsd_products_support_series_home.html
- Cisco Emergency Responder:
  http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- Cisco Unity:
  http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- Cisco Unity Express:
  http://www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html
- Cisco Unity Connection:
  http://www.cisco.com/en/US/products/ps6509/tsd_products_support_series_home.html
- Cisco Unified MeetingPlace:
  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html
- Cisco Unified MeetingPlace Express:
  http://www.cisco.com/en/US/products/ps6533/tsd_products_support_series_home.html
- Cisco Security Agents:
  http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html

- Cisco Unified Operations Manager:
  http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html
- Cisco Unified Service Monitor:
  http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html
- CiscoWorks Remote Management Essentials:
  http://www.cisco.com/en/US/products/sw/cscowork/ps2073/
  tsd_products_support_series_home.html
- Cisco Fax Server:
  http://www.cisco.com/en/US/products/ps6178/tsd_products_support_series_home.html
- Cisco Secure PIX Firewall Servers:
  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/
  tsd_products_support_series_home.html
- Cisco SIP Proxy Server:
  http://www.cisco.com/en/US/products/sw/voicesw/ps2157/
  tsd_products_support_series_home.html
- Cisco Unified Videoconferencing products:
  http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html
- Cisco 2600 Series Routers:
  http://www.cisco.com/en/US/products/hw/routers/ps259/tsd_products_support_series_home.html
- Cisco 2800 Series Routers/Voice Gateways:
  http://www.cisco.com/en/US/products/ps5854/tsd_products_support_series_home.html
- Cisco 3700 Series Voice Gateways/Gatekeepers:
  http://www.cisco.com/en/US/products/hw/routers/ps282/tsd_products_support_series_home.html
- Cisco 7200 Series Voice Gateways:
  http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html
- Cisco Catalyst 3550 Series Access Switches:
  http://www.cisco.com/en/US/products/hw/switches/ps646/tsd_products_support_series_home.html
- Cisco Catalyst 3560 Series Access Switches:
  http://www.cisco.com/en/US/products/hw/switches/ps5528/
  tsd_products_support_series_home.html
- Cisco Catalyst 3750 Series Data Center Switches:
  http://www.cisco.com/en/US/products/hw/switches/ps5023/
  tsd_products_support_series_home.html
- Cisco Catalyst 6500 Series Switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/
  tsd_products_support_series_home.html
- Cisco Catalyst 6600 Series Voice Gateways:
  http://www.cisco.com/en/US/products/hw/switches/ps700/
  tsd_products_support_eol_series_home.html
- Cisco VG224/248 Analog Voice Gateways:
  http://www.cisco.com/en/US/products/hw/gatecont/ps2250/
  tsd_products_support_series_home.html
- Cisco ATA 186/188 Analog Telephone Adaptors:
  http://www.cisco.com/en/US/products/hw/gatecont/ps514/
  tsd_products_support_series_home.html

- Cisco Unified IP Phone 7900 Series:
  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- Cisco Aironet 1200 Series Access Points:
  http://www.cisco.com/en/US/products/hw/wireless/ps430/tsd_products_support_series_home.html
- Cisco IP Communicator:
  http://www.cisco.com/en/US/products/sw/voicesw/ps5475/tsd_products_support_series_home.html
- Cisco Unified Personal Communicator:
  http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html
- Cisco Unified Video Advantage:
  http://www.cisco.com/en/US/products/sw/voicesw/ps5662/tsd_products_support_series_home.html
- Cisco IOS Software Release 12.4 T:
  http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.html

Install and Upgrade Notes

The components in these release notes, including the platforms tested, are discussed in the Technical Information site at:
http://www.cisco.com/iam/unified/ipt3/Install_and_Configure_System_Components.htm

See this content for the specific versions of the components tested and links to relevant documentation for installation and configuration procedures.

Upgrade information for components that have been tested and verified during system testing is discussed in the *System Upgrade Manual* at:
http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc511/sum/su511.pdf

For additional information on specific hardware recommendations or bills of material for each product, see the System Requirements section.

Latest Software Upgrades and Licenses

The following are links to the latest software upgrades and licenses for Cisco Unified Communications Release 5.1(1) components:

- Go to http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml to download the software for the following products:
  - Cisco Unified CallManager and Cisco Unified CallManager Express
  - Cisco Unified Presence Server
  - Unified Survivable Remote Site Telephony (SRST)
  - Cisco Customer Response Solutions (Cisco Unified Contact Center Express Edition)
  - Cisco Emergency Responder
  - Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express
  - Cisco Unity, Cisco Unity Connection and Cisco Unity Express
  - Cisco Unified MobilityManager

  - Voice/video endpoints such as Unified IP Phones, Analog Telephone Adaptors (ATAs), Cisco IP Communicator, Cisco Unified Personal Communicator and Cisco Unified Video Advantage
- Cisco IOS routers and gateways: http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml
- Catalyst switches: http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches
- Wireless products: http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml
- Firewalls and security modules: http://www.cisco.com/kobayashi/sw-center/sw-ciscosecure.shtml
- Network management software: http://www.cisco.com/kobayashi/sw-center/cw2000/lan-planner.shtml
- Cisco Agent Desktop Web Licensing Site: http://209.46.83.138/sws/WebLicensingInitial/InitialLicensePage.html
- Cisco Unity Connection License Files: http://www.cisco.com/en/US/products/ps6509/products_installation_guide_chapter09186a008055e1f6.html#wp1041859
- Product Upgrade Tool (for ordering CD's of new major/minor releases): http://tools.cisco.com/gct/Upgrade/jsp/index.jsp

Limitations and Restrictions

This section includes the following topics:

- Important Notes, page 20
- Resolved Caveats, page 34
- Open Caveats, page 35

If you are a Cisco partner or a registered Cisco.com user with a Cisco service contract, you can use the Bug Toolkit to find caveats of any severity for any release. To access the Bug Toolkit, go to this URL: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Important Notes

This section includes important notes related to the testing of Cisco Unified Communications System Release 5.1(1) for IP telephony.

Unified CallManager TFTP issues in large scale Cisco Unified IP Phones 7900 Series deployments (CSCdv21481)

Symptom:

If a large number of Cisco Unified IP Phones 7900 Series endpoints simultaneously request configuration files, their TFTP server may return a DISKFULL, RETRY, or other TFTP error. Some errors cause phones to continue to boot and log the error, while others cause phones to constantly reset. The current implementation defaults to the last saved settings if there is a TFTP timeout. Since Cisco Unified IP phones rely heavily on the TFTP configuration files received for configuration, softkeys, dial plans, and so forth, there is a possibility for the phones to be out of date with the TFTP server.

Conditions:

This issue can occur when all Cisco Unified IP Phones 7900 Series phones in a cluster are upgraded or restarted following a power outage. This problem may also occur on SIP phones after a complete Unified CallManager cluster restart on a medium size cluster when the phones lose connection to all Unified CallManager nodes and try to re-register on an interval. While the cluster is restarting, the Unified CallManager service may initialize faster than TFTP service can rebuild all the configuration files and return to service. This leads to a problem with SIP TNP phones that must download their Softkey template files. If the TFTP service is not ready, their attempts to download these files time out but they continue to register with the Unified CallManager node. In this case, the SIP TNP phones no longer support KPML events and only send enbloc SIP Invite messages to their Unified CallManager node.

Workaround:

None.

Unified CallManager in call throttling mode still accepts incoming calls (CSCea82559)

Symptom:

If an IP phone is registered with a Unified CallManager that is operating in call throttling mode, and a second IP phone registered with another Unified CallManager dials that first phone, the call is successfully established. The same scenario applies for any call destined for the first IP phone and placed through MGCP gateways or intercluster trunks (ICTs).

Condition:

Normal Unified CallManager operation.

Workaround:

None.

Cisco Unified CallManager does not support static codec G.726r32 on a SIP trunk (CSCsb92419)

Symptom:

Calls made to Unified CallManager fail if the audio codec type selected is G.726r16, G.726r24, or G.726r32.

Conditions:

This can happen when G.726 is selected as the codec type in the *voip dial-peer* for the following gateways: H.323, SIP, or MGCP.

Workaround:

Select another codec type such as G.711ulaw, G.711alaw, G.729, or G.723.

BAT.xlt Device and Line fields should match the Cisco Unified CallManager phone fields (CSCsb96065)

Symptom:

BAT.xlt does not exactly match the Device and Line fields that are listed on the Cisco Unified CallManager Administration page.

Conditions:

This occurs when you have to add multiple phone devices using the Bulk Administration Tool (BAT).

Workaround:

When adding phones using BAT, check the Cisco Unified CallManager Administration page to verify that you are adding the correct data to the appropriate fields.

Job Configuration Page does not automatically update (CSCsb96526)

Symptom:

When verifying the status of a scheduled BAT job, the Job configuration status page does not automatically get updated.

Conditions:

Whenever the Bulk Administration Tool is used to schedule a BAT job.

Workaround:

Press the Refresh button on the web browser page.

Shut down and power off behavior is different from previous CallManager Release 4.x conditions (CSCsc00895)

Symptom:

Power off and shut down behavior on a Unified CallManager node is different from previous CallManager release 4.x conditions.

Conditions:

When executing **utils system shutdown** from the command line interface (CLI) on the Unified CallManager server, the server does not power off completely after shutting down the active processes. While the system console displays the “Power Down” message, the Ethernet connection remains up and all the LEDs remain lit.

When you use the power button to physically power down the server on an MCS server (such as the MCS-7845-H1s), another major change from the Windows OS 2000.2.7 behavior is that the power shuts down immediately, without a grace period.

Workaround:

None. You must use the power button to physically power down the server. You should also be aware of the above changes in behavior to prevent accidental outages.

Real-Time Monitoring Tool Graphs do not have the capability to highlight nodes and counters (CSCsc12008)

Symptom:

Real-Time Monitoring Tool (RTMT) graph line color codes are not easily distinguishable on large clusters with more than ten nodes, especially when some of them overlap with each other.

Conditions:

When using RTMT to monitor a Unified CallManager cluster or analyzing a performance log saved by the Alert Manager and Collector (AMC) or Real-Time information System Data Collector (RISDC), you cannot highlight a node or a counter to distinguish it clearly from other color-coded lines. This problem applies to all graphs that display multiple nodes or counters with color codes.

Workaround:

None.

Multicast Music-On-Hold not supported by SIP gateway (CSCsc30731)

Symptom:

In the current release of IOS, the SIP gateway does not support multicast music- on-hold (MOH). The SIP gateway cannot stream RTP traffic when MOH is configured to multicast. When examining the traffic, it is observed that the SIP gateway receives the pre-allocated MTP information, but does not create a new MediaConnect to connect with the MOH server.

Conditions:

Call Flow: PSTN > SIP Gateway (Multicast MOH and MTP enabled) > IP Phone > Hold

When the call flow is as above and:

1. Multicast MOH is enabled on the Unified CallManager and the call is placed on hold; after a period of silence, the call is terminated.
2. Media Termination Point (MTP) is enabled and the MTP receives an ICMP (port unreachable) error from the SIP gateway; the RTP stream is terminated on the MTP.

Workaround:

None. The multicast feature for IOS will be supported in a future release.

Migration of Cisco Unified IP 7960 Phones from SCCP to SIP requires phone power cycle (CSCsc67031)

Symptom:

When SCCP Unified 7960 IP Phones are converted to SIP, the phones do not register properly and migration from SCCP to SIP does not occur. The phones are unable to locate the SEPmac.CNF.XML file and get stuck in a loop and registration as SIP phones is rejected.

Conditions:

The SCCP Unified 7960 IP Phones are converted to SIP using the BAT and the Unified CallManager cluster is rebooted. The SCCP load on the phones prior to migration is 8.0(0.21).

Workaround:

Power down and then power up the SCCP Unified IP 7960 Phones. Once the phones are power cycled, they register as SIP phones successfully.

Unity Connection needs an adaptive packet interval algorithm (CSCsc79956)

Symptom:

Remote endpoint sends RTP packets at a different packet interval than requested by Unity Connection. Unity Connection appears to record a message, but no message is actually recorded. Unity Connection discards the RTP packets and voicemail is not saved.

Conditions:

Unity Connection and remote endpoints are configured to send and receive RTP packets at different packet intervals. This problem is seen with remote endpoints that only send RTP packets at one interval or do not use the requested interval time.

Workaround:

Manually configure the remote endpoints and Unity Connection to have an identical packet interval time.

Default number of ports do not override maximum number of ports for Reservationless meeting (CSCsc82982)

Symptom:

The user is able to schedule Reservationless meetings with more users than specified in the “Maximum ports per meeting for Reservationless” parameter in the System Configuration > Meeting Configuration page in the Unified MeetingPlace Express Administration Center.

Conditions:

Even though the maximum number of ports for a Reservationless meeting are set to less than the default number of ports per meeting, the default number of ports are still available for use by the user.

Workaround:

The administrator should set the default number of ports per meeting to a value that will limit the maximum number of ports used for the Reservationless meeting.

Cisco Emergency Responder does not display phone protocol information under Phone Type (CSCsc99954)

Symptom:

The phones being tracked in Cisco Emergency Responder do not display the phone protocol type under the Phone Type field in Switch Port Details under ERL Membership on the Cisco Emergency Responder Administration Page.

Conditions:

This happens when polling the phones being tracked in the Cisco Emergency Responder.

Workaround:

Check the phone type in the Unified CallManager Administration > Device > Phone Page.

Support SIP video pass through with audio transcoder (CSCsd27125)

Symptom:

A SIP video call does not receive video when an audio transcoder is allocated, even if the audio transcoder supports video pass through. Currently, video pass through is disabled for a SIP call if an audio transcoder is allocated.

Conditions:

Whenever a pass through-capable transcoder is allocated for a SIP video call.

Workaround:

None.

No email notification when disconnecting standby Cisco Emergency Responder from network (CSCsd33512)

Symptom:

When the standby Cisco Emergency Responder server is disconnected from the network; the primary Cisco Emergency Responder realizes this because of the heart-beat miss; but does not inform the network administrator of the disconnected status via an email.

Conditions:

The standby Cisco Emergency Responder is disconnected in the network.

Workaround:

Manually monitor the Event Viewer logs or system-generated logs for email to verify that the standby Cisco Emergency Responder is connected and operational in the network.

Stopping meeting room music when using Cisco Unified MeetingPlace Express with SIP Integration to Cisco Unified CallManager (CSCsd35417)

Symptom:

When dialing in via SIP integration with Unified CallManager and the first user in a meeting presses the star (*) key once, the meeting room music restarts after stopping.

Conditions:

A user dials into a meeting using SIP integration with Unified MeetingPlace Express and Unified CallManager.

Workaround:

If the user happens to be the first user in the meeting, they must press the star (*) key on the phone twice to stop the meeting room music.

IPT Platform Administration CLI does not have ability to search folders by disk usage (CSCsd41441)

Symptom:

A LogPartitionHighWaterMarkExceeded alarm is received from a Unified CallManager node indicating that the server is running out of disk space under the common partition.

Condition:

If you enable too many traces for reporting purposes, the common partition may fill up and the server could run out of disk space. It is not easy to determine which trace levels or settings to reduce or which files to delete in order to prevent this situation. An IPT Platform Administration CLI command should be provided to examine which folders are using the most disk space and which files to delete.

Workaround:

None.

Cisco Unified CallManager/Cisco Unified CallManager Express calls via IP-to-IP Gateway with/without ECS support (CSCsd42645)

Symptom:

When an IP-to-IP gateway is configured without ECS support, calls made from an Unified CallManager to an Unified CallManager Express via the IP-to-IP gateway, which are then forwarded or transferred to another Unified CallManager or Unified CallManager Express, are successful.

However, when a call from an Unified CallManager forwards or transfers via the IP-to-IP gateway to an Unified CallManager Express or another Unified CallManager, the call fails on transfer. If ECS support is turned on in the IP-to-IP gateway, the Unified CallManager forwarded or transferred call works; but the Unified CallManager Express forwarded or transferred call fails.

Conditions:

Unified CallManager in this case uses QSIG Path replacement after the call has been transferred or forwarded. H.450 is used between Unified CallManager Express and the IP-to-IP gateways.

Workaround:

In Unified CallManager, configure MTP as “required” on the H.225 trunk to the Gatekeeper and IP-to-IP gateway. In the IP-to-IP gateway, remove the “emptycapability” parameter.

Note Use the above workaround if video calls are not used between Unified CallManager clusters via the IP-to-IP gateways.

If video calls between Unified CallManager clusters are required, implement the following procedures for each cluster in addition to the above workaround:

1. Add a second gatekeeper-controlled H.225 trunk to the gatekeeper and configure the second trunk the same identically to the first trunk.
2. Disable MTP on the second trunk and choose an alternate tech prefix.
3. Configure Unified CallManager to route all video calls through this second trunk.
4. Configure the gatekeeper to support the new tech prefix without routing the call via the IP-to-IP gateway. The gatekeeper should route all calls from remote zones to the new trunk using the new tech prefix.
5. Make sure that you perform the above procedures for each Unified CallManager cluster.
6. If RSVP is enabled between the Unified CallManager clusters, provide additional, similarly configured IP-to-IP gateways (include the "emptycapability" CLI parameter).
7. Configure the gatekeeper to route all video calls using the new tech prefix via the new IP-to-IP gateways.

No hold tone returned to SIP phone across QSIG inter-cluster trunk when call is put on hold (CSCsd43480)

Symptom:

During calls between SIP phones over QSIG inter-cluster trunks, the caller may only hear silence (no hold music) if the call is put on hold or a transferred by the called party.

Conditions:

The problem occurs when a SIP phone calls another SIP IP phone on another Cisco Unified CallManager cluster across a QSIG inter-cluster trunk, and the call is answered and put on hold. If there is no music on hold (MOH) configured on the incoming QSIG inter-cluster trunk itself or on the trunk's device pool, the caller does not hear hold music.

Workaround:

Configure MOH on either the incoming QSIG inter-cluster trunk or the device pool that contains the trunk.

Resetting CFwdALL on Cisco Unified IP Phones does not produce correct tone (CSCsd56104)

Symptom:

When the CFwdALL setting on the Cisco Unified IP Phone is reset, the two short beeps that indicate that the redirected number has been released are not heard. However, the redirected number correctly disappears from the phone display.

Conditions:

This happens with the current release of SIP Cisco Unified IP Phones 7941, 7961, and 7971.

Workaround:

None.

Certificate Authority Proxy Function (CAPF) logging requires service restart (CSCsd62658)

Symptom:

CAPF detailed trace is not available.

Conditions:

Platform serviceability logging level is set to “Detailed” for troubleshooting purposes.

Workaround:

Stop and restart the CAPF service via the Platform Serviceability interface.

Bulk Administration Tool (BAT) should support more than 12,000 records per transaction (CSCsd64029)

Symptom:

The Bulk Administration Tool (BAT) recommends limiting any transaction for inserts/updates/deletes to a maximum of 12,000 records. This limit should be removed. BAT should support over 12,000 record changes reliably.

Conditions:

This limitation applies to BAT transactions with over 12,000 records only.

Workaround:

In the case of a query-based transaction, if the selected number of records exceed 12,000, then administrator should refine the query to select fewer records. In the case of comma-separated value (CSV) based transactions, the administrator must split records across CSV files such that each file contains less than12,000 records and schedule multiple transactions.

Unified CallManager passthrough call TCS deadlock on Call Forward All (CFA) transfer to Unified CallManager Express via an IP-to-IP Gateway (CSCsd75497)

Symptom:

When a call from across a QSIG inter-cluster trunk is call forwarded (CFA) to Cisco Unified CallManager Express through an IP-to-IP Gateway, the call released but the destination hears hold tone generated by Unified CallManager Express. The call must be rerouted through a PBX.

Conditions:

The Unified CallManager fails to negotiate the Terminal Capabilities Set (TCS) value with the IP-to-IP Gateway in this passthrough situation; the Unified CallManager remains in a deadlock condition waiting for TCS on both sides of the call.

Workaround:

None.

Cisco Unified IP Phone 7985 phone gets stuck in No Video state with H.264 video call with Cisco Unified Video Advantage (CSCsd87718)

Symptom:

A Cisco Unified IP Phone 7985 loses video on a H.264 video call with Cisco Unified Video Advantage and then remains in a “no video available” state. The screen remains blank during any subsequent attempts to establish a video call from the phone (either H.263 or H.264).

Conditions:

The problem occurs when a simple audio call is established between any Cisco IP phone and a Cisco Unified IP Phone 7985. Mid-way through the call, if the user launches Cisco Unified Video Advantage on the PC connected to the Unified IP Phone 7985, an H.264 video call is established between the two endpoints. The Unified IP Phone 7985 displays a “Mute Video” indication at first and then the phone starts showing streaming live video of the near end for 1-2 seconds; after that the Unified IP Phone 7985 displays a “Mute Video” indication and loses the video portion of the call.

Workaround:

The only way to recover is to reboot the Cisco Unified IP Phone 7985.

No protection for limiting number of active nailed up callers (CSCse06753)

Symptom:

Cisco Unified CallManager service runs out of memory and unexpectedly restarts.

Conditions:

Under certain stress conditions when there are very large number of concurrent active calls present on a single call processing node, Unified CallManager service could run out of memory even on a Cisco MCS-7845-based Unified CallManager server equipped with 4 GB of RAM.

Workaround:

None.

Real-Time Monitoring Tool (RTMT) Critical Service Down alert is raised when backing up CDR_CAR (CSCse22377)

Symptom:

During a scheduled Cisco Disaster Recover System (DRS) backup, the Real-Time Monitoring Tool (RTMT) displays alerts indicating that critical services are down.

Conditions:

When backing up the CDR_CAR feature during a scheduled or manual DRS backup, the Cisco CAR Scheduler service and Cisco CAR Web Service are taken down during the backup process. The RTMT detects each service going down and triggers critical service down alerts.

Workaround:

These alerts can be ignored as they are normal during a backup process.

Large scale phone unregistrations leads to Unified CallManager Code Yellow entry (CSCse26225)

Symptom:

Cisco Unified CallManager service goes in to Code Yellow state unexpectedly and starts rejecting new calls from all devices.

Conditions:

When a large number of phones unregister from their primary Unified CallManager node, that particular node could go in to Code Yellow state for a period of time. During this time, all new calls are rejected. This situation could occur in centralized call processing deployment models with large SRST remote sites. If the connectivity between the remote and central sites is lost, Unified CallManager servers in the central site could go into Code Yellow state.

Workaround:

None.

Cisco Communications Media Module port loopback tests fail in special circumstances (CSCse80723)

Symptom:

A Cisco Communications Media module (CMM) fails to come back online after a reload, a power cycle, or an unexpected crash. The module status shows an incorrect value. The command **show test module** indicates that the loopback test on port#1 of the module has failed as shown below:

```
Loopback Status [Reported by Module 1] :
  Ports 1  2  3  4  5
  --------------------
        F  N  N  N
```

Conditions:

This happens to a CMM operating under a Cisco Catalyst 6000 Supervisor 2 module running version CatOS 8.5(5). The loopback test fails and the CMM does not come back online after the module has been reloaded or power cycled, or has crashed more than three times.

Workaround:

Issue a **clear cam dynamic** command to reset the faulty module.

No counters to track call throttling over an H.323 trunk (CSCsf10917)

Symptom:

When inter-cluster trunk (ICT) call throttling occurs, Unified CallManager raises an alarm and logs it in the Unified CallManager traces; but does not display the number of H.323 calls being throttled.

Conditions:

Unified CallManager has an ICT call throttling mechanism that enables it to reject additional H.323 calls. However, there is no performance counter associated with the throttling mechanism that records and displays the number of calls it throttles.

Workaround:

None.

Real-Time Monitoring Tool Performance Log Viewer does not display sorted remote log files (CSCsf20296)

Symptom:

The Real-Time Monitoring Tool (RTMT) Performance Log Viewer does not display sorted remote log files.

Conditions:

When viewing remote performance log files (either Alert Manager and Collector (AMC) or Real-Time information System Data Collector (RISDC)) using RTMT Performance Log Viewer, the list of files displayed is not sorted.

Workaround:

Manually sort the listed files and choose the log file that you need.

Disaster Recovery restore attempt on a first node fails (CSCsf28239)

Symptom:

Restoring data on a first node using the Disaster Recovery System (DRS) tool fails and an error in the Unified CallManager database displays.

Conditions:

The Unified CallManager multi-node cluster is running the same version as the DRS backup file. The restore attempt fails when trying to restore the first node or the Unified CallManager database to the previously saved version using the DRS tool. The DRS log files on the Unified CallManager database indicate the following error:

```
CCMDB Restore failed, installdb failed
425: Database is currently opened by another user
```

Workaround:

Shut down all the subsequent nodes in the Unified CallManager cluster and then attempt to restore the first node.

Default view should be given the option to enable or disable (CSCsg14500)

Symptom:

In the Cisco Unified Operations Manager, users are allowed to define their own views, logical groupings of devices that appear in the Monitoring Dashboard displays. However, the All IP Communications Devices view is enabled by default and automatically included in the user’s Service Level View, and there is no method for turning off this view.

Conditions:

In the Manage Views page, there is no option to disable the All IP Communications Devices view in the Service Level View. Users can select which customized views will appear in Service Level View by placing a checkmark next to each view name in the Topology column. However, the Service Level View display automatically includes the All IP Communications Devices view showing the entire network topology, in addition to the views selected by the user. Users may find this behavior unexpected.

Workaround:

None.

When a PIX firewall is operating in transparent mode, explicit routing configuration is required to support VoIP calls (CSCsg28343)

Symptom:

Cisco PIX 500 series security appliances may fail to allow VoIP traffic or H.323, SIP, or SCCP signaling packets through to “arbitrary” hosts.

Conditions:

When the Cisco PIX 500 is operating in transparent firewall mode, and the hosts participating in a VoIP call are not directly connected to the firewall and there are no routes configured for them in the Cisco PIX 500.

Workaround:

Configure routes in the Cisco PIX 500 for hosts behind the firewall that are involved in VoIP calls.

Cisco Unified CallManager Release 5.x to Unified CallManager Release 4.x via IOS gateway SIP trunk incompatibility not in documentation (CSCsg50227)

Symptom:

Calls from a Unified CallManager Release 5.x cluster over a SIP trunk with TCP transport to a Unified CallManager Release 4.1 or 4.2 cluster cannot be answered. After going off hook at the destination cluster running Unified CallManager Release 4.1 or 4.2, the originator continues to ring and after a period of time the call is cleared. Similar symptom could be observed when using an IOS PSTN gateway with TCP SIP trunks terminating at Unified CallManager Release 4.1 or 4.2 clusters.

Conditions:

Unified CallManager Release 5.x cluster with a SIP trunk Security Profile Outgoing Transport Type set to TCP a trunk destination to a Unified CallManager Release 4.x cluster. When placing concurrent calls, after the first call is established the consecutive calls cannot be connected. The problem occurs due to TCP reuse differences between the SIP protocol stacks in these products. If the side with TCP reuse capability calls to a side without the same capability, consecutive calls will fail. A similar condition applies to IOS PSTN gateways with SIP trunks terminating at Unified CallManager because IOS Release 12.3(8)T changes to TCP reuse from no TCP reuse.

Workaround:

Due to the SIP protocol stack incompatibilities between these components when using TCP transport, use UDP transport to ensure compatibility.

Cisco Unified CallManager Release 5.x to Unified CallManager Release 4.x via IOS gateway SIP trunk incompatibility not in documentation (CSCsg50227)

Symptom:

Voice security on MGCP gateways is enabled but not applied. For instance, running the voice gateway command **show rtpspi call** reveals that the SRTP column displays a zero (0) value.

Conditions:

This situation occurs when configuring voice security features on a Cisco IOS MGCP gateway. The Configuring Voice Security Features on Cisco IOS MGCP Gateways topic in the *Media and Signaling Authentication and Encryption Feature on Cisco IOS MGCP Gateways* document is missing information in the configuration procedures.

Workaround:

To ensure that voice security configuration changes are applied, you should first stop and restart the MGCP service before you exit the configuration mode. Listed below is a summary of the configuration steps required to enable and apply the voice security features:

1. Enable
2. Configure terminal
3. mgcp package-capability srtp-package
4. mgcp validate call-agent source-ipaddr (optional command)
5. no mgcp (this command stops the mgcp service)
6. mgcp (this command restarts the mgcp service)
7. Exit

SMTP Server Configuration Not Populated After a Fresh Unified MeetingPlace Express Install (CSCsg62534)

Symptom:

During the operating system installation of Unified MeetingPlace Express, the user is asked to enter SMTP server information. However, this information does not appear on the System Configuration -> E-Mail Service Configuration -> SMTP Server Configuration page on the Administration page after the installation is complete.

Conditions:

When a user enters an SMTP server while installing Unified MeetingPlace Express Release 1.2(1).

Workaround:

User must re-enter the SMTP information in the System Configuration -> E-Mail Service Configuration -> SMTP Server Configuration page on the Administration page following the installation.

No calls made via H.323 Gateway appear in Real Time Monitoring Tool (RTMT) Summary View for active gateways, ports, and channels (CSCsg71038)

Symptom:

Calls made via H.323 gateways are not visible in the Real Time Monitoring Tool Summary view for active gateways, ports and channels.

Conditions:

When using RTMT with Cisco Unified CallManager Release 5.0 or later.

Workaround:

Use the Call Process - Gateway Activity view to monitor calls of this type.

Unified MeetingPlace IP Gateway does not support G.722 codec (CSCsg73799)

Symptom:

The G.722 codec is not negotiated when it is configured in the Unified MeetingPlace Audio Server.

Conditions:

The G.722 codec is currently not supported by the Unified MeetingPlace IP Gateway.

Workaround:

Use another codec for Unified MeetingPlace conferences.

Unified Operations Manager fails to properly alert on Unified CallManager related service outage (CSCsg96469)

Symptom:

Cisco Unified CallManager related service outages are not properly identified by the Unified Operations Manager.

Conditions:

This has been observed in normal operating conditions. Currently when a Unified CallManager service outage occurs the event generated by Unified Operations Manager indicates a HeartBeat Threshold value has been exceeded. This is the same event if the heart beat actually falls below the configured threshold of 24 ticks per minute. The event details do not specify that the heart beat actually dropped to 0.

Workaround:

None.

Resolved Caveats

This section lists severity 1, 2, and selected 3 caveats that are resolved now but are *not* included in the recommended component versions of Cisco Unified Communications System Release 5.1(1) for IP telephony.

Note For information on the caveats that were resolved in specific versions of each component, refer to the appropriate release notes for each component.

To determine the software version that includes the fix, click on the linked caveat number in the Identifier column in Table 3 to go to the Bug Toolkit.

Table 3 Resolved Caveats Not Included in Cisco Unified Communications Release 5.1(1)

Identifier	Headline
CSCsb99980	Unified CallManager may try to insert extra unnecessary Media Termination Point (MTP) for DTMF due to Music on Hold (MoH) connection
CSCse80723	Cisco Communications Media Module port loopback tests fail in special circumstances
CSCse96864	No video between two Unified Video Advantage enabled endpoints
CSCsf10917	No counter to track call throttling over an H.323 trunk
CSCsf26578	Cisco Unified Video Advantage endpoint does not display remote video when calling into conference provided by Release 5.0 Unified Videoconferencing MCU
CSCsg00283	Simultaneous Real-Time Monitoring Tool (RTMT) trace collection download sends trace data to wrong folders
CSCsg46679	Cannot delete administrator-created folders in the Cisco Unified CallManager TFTP folder
CSCsg47594	Crosstalk observed in calls across FXO ports on Cisco Catalyst switch

Table 3 Resolved Caveats Not Included in Cisco Unified Communications Release 5.1(1) (continued)

Identifier	Headline
CSCsg47834	NACK message received in response to Open Voice Channel command sent by IOS
CSCsg67610	Unified CallManager auto configuration attempt does not fail when enough DSP resources are not available

Open Caveats

This section lists known severity 1, 2, and selected 3 caveats related to the testing of IP telephony components in Cisco Unified Communications Release 5.1(1) and previous releases, which were not resolved at the time this document was written.

For additional information on each defect, click on the linked caveat number in the Identifier column in Table 4 to go to the Bug Toolkit.

Table 4 Open Caveats in Cisco Unified Communications Release 5.1(1)

Identifier	Headline
CSCds25257	Cannot delete or clear gatekeeper endpoint registration
CSCsa59830	Unified 7970 IP Phone interface dead-ends after Call Me
CSCsb27177	Annotations and chat frozen temporarily
CSCsb46040	Unified MeetingPlace IP gateway has a possible 1 MB memory leak
CSCsb71648	Upgrade from Cisco CallManager 4.1(3) to Cisco Unified CallManager 5.0 requires excessive database migration time
CSCsc97966	Unified MeetingPlace Express will not register to a specific zone in gatekeeper
CSCsc97977	Direct meeting dial-in does not work with gatekeeper
CSCsd05236	Cisco Unity Domino: Message Store Configuration Wizard (MSCW) does not verify service account creation properly
CSCsd22921	Cisco Unified Videoconferencing MCU SCCP service with dual video codec prefers the wrong transmit codec
CSCsd27288	Cisco 2600 router crashes after booting with **boot flash** command
CSCsd29723	UserID search cannot find first user when scheduling a meeting via Unified MeetingPlaceWeb
CSCsd46211	Cisco Unified 7920 wireless phones cannot be tracked using IP SUBNET tracking in Cisco Emergency Responder
CSCse22877	Unified CallManager 5.0 Database Layer Monitor (dbmon) restarts and generates a core dump file
CSCse23371	Real-Time Monitoring Tool (RTMT) device search results timestamps do not match server logs if the servers are located in a different timezone
CSCse28611	Trace collection caused a core dump
CSCse43150	Real-Time Monitoring Tool (RTMT) core dumpfile trace collection generates very high CPU IOWait percentage
CSCse72089	Serial Advanced Technology Attachment (SATA) software RAID disk array I/O starvation causes Unified CallManager core dump
CSCse95242	Unified Videoconferencing Multipoint Control Unit (MCU) with four Enhanced Media Processor (EMP) modules cannot create a service prefix that shows the maximum 96 ports available

Table 4 Open Caveats in Cisco Unified Communications Release 5.1(1) (continued)

Identifier	Headline
CSCsf00288	Tandberg H.320 video endpoint does not update the video in a Cisco Unified Video Advantage’s remote window in a timely manner
CSCsf27257	Cisco Unified CallManager installation should not allow setting Network Interface Card (NIC) speed to 1000BaseT
CSCsf98457	Cisco IOS routers crash after running out memory from ISDN L2 process
CSCsg07605	Cisco Unified CallManager Disaster Recovery System (DRS) backup puts Cisco Unified CallManager database in read-only mode
CSCsg08547	Fax transmission fails when making a fax call over IP-to-IP Gateways
CSCsg21296	IPT Platform cannot detect and log duplicate IP addresses
CSCsg23247	Unprovisioned VG224 gateway prevents new phone registrations and impacts change notifications
CSCsg28343	When a PIX firewall is operating in transparent mode, explicit routing configuration is required to support VoIP calls
CSCsg29465	No video on Cisco Unified Personal Communicator on calls transferred from Cisco Unified IP Phone 7985
CSCsg31970	Cisco Unified CallManager Install DVD causes disk problems when used on an IBM laptop
CSCsg39825	Cisco Unified CallManager calls to registered SIP phones immediately generate reorder DMPidErr error message
CSCsg42281	H.323 to SIP interworking on Unified Videoconferencing MCU only shows one-way video
CSCsg49814	Video remains frozen on Cisco Unified Personal Communicator (without a camera) after holding and then resuming a call to Cisco Unified Video Advantage
CSCsg51225	Video channel between Cisco Unified Personal Communicator and Cisco Unified Video Advantage is not re-established after both endpoints put the video call on hold and then resume the call
CSCsg52269	No video on either end when a user starts Cisco Unified Video Advantage application after answering a call from Cisco Unified Personal Communicator, even when the call has been put on hold by the Unified Personal Communicator and then resumed after Unified Video Advantage has started
CSCsg56910	Unified Videoconferencing SCCP conference bridge runs out of resources after failover
CSCsg57002	SIP timer tree corruption causes SIP gateway to crash under heavy traffic load
CSCsg64964	No Switch-port Change Reporting email alert sent for new phones when Unified CallManager auto-registration is disabled
CSCsg65683	High CPU usage due to voice conferencing on Cisco 2600XM used as SIP gateway
CSCsg67493	Cisco Emergency Responder: Cisco IP Communicator movement generates e-mail report
CSCsg76544	Cisco Unified Video Advantage displays a mix of multiple simultaneous video streams
CSCsg86540	Unified Service Monitor backup operation continues indefinitely
CSCsg95361	New Cisco Unified IP Phone 7936 fails to upgrade and register with proper server in Unified CallManager Release 5.x cluster
CSCsg97738	Cisco Unified CallManager unable to save phone changes if Cisco Extension Mobility user is logged in
CSCsg98070	Cisco CallManager service parameter Asynchronous SDL Logging Enabled must be left at default disabled setting

Troubleshooting

For important troubleshooting information, tips, and recommendations related to Cisco Unified Communications System Release 5.1(1) for IP telephony, see the troubleshooting information at: http://www.cisco.com/iam/unified/ipt3/Introduction_to_Troubleshooting.htm.

Documentation Updates

- Technical Information Sites—The Unified Communications Technical Information Sites available by typing www.cisco.com/go/unified-techinfo are your one-stop location for all system-level documentation, resources, and training. These sites provide information on tested deployment models and sites, topology diagrams, and call flows. The sites specific to IP telephony or contact center system applications for Unified Communications Release 5.1(1) are:
  - Cisco Unified Communications System for IP Telephony Release 5.1(1): http://www.cisco.com/iam/unified/ipt3/index.htm
  - Cisco Unified Communications System for Contact Center Release 5.1(1): http://www.cisco.com/iam/unified/ipcc3/index.htm
- *System Upgrade Manual*—The content has been updated to reflect the new upgrade path to Cisco Unified Communications System Release 5.1(1). The content also discusses new upgrade strategies and upgrade considerations to be aware of for various components as you perform the upgrade. This document is available at: http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc511/sum/su51.pdf
- *System Test Results for IP Telephony: Cisco Unified Communications Release 5.1(1)*—Test results of the IP telephony system testing are available at: http://www.cisco.com/iam/unified/ipt3/System_Test_Results.htm

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_inpck/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.