Avaya Aura® Communication Manager 6.3.2.1 (Service Pack 2)

Release Notes

Issue 1
November 6, 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com.

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processor up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User” means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/ThirdPartyLicense/

You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

"Avaya" and "Avaya Aura" are the registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux**"** is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Changes delivered to Avaya Aura® Communication Manager 6.3.2

Communication Manager 6.3.2 Release Notes

Communication Manager Release 6.3.1.0 and later uses the following service pack naming convention. This is a four digit number format as described in the following example:

Communication Manager 6.3.4.1, where

- 6 - major release field (Communication Manager Release 6)
- 3 - minor release field (Communication Manager Release 6.3)
- 4 - service pack field (Communication Manager Release 6.3 Service Pack 4)
- 1 - special release field, typically used for a re-issue of an existing service pack (Communication Manager 6.3 Service Pack 4.1)

Note that:

1. To avoid confusion, unused fields to the right might not be shown. For example, Communication Manager 6.3 will be used in documentation related to the minor release instead of Communication Manager 6.3.0.0.
2. The special release field may be used for atypical software releases other than service pack re-issues which will be explained in the documentation for the special release software (e.g. release notes or Product Correction Notices).
3. This naming change applies only to regular Communication Manager service packs and does not apply to special service packs such as Security Service Packs, Kernel Service Packs, Pre-Upgrade Service Packs and VMware Tools Service Packs.
4. Communication Manager service pack file names will be unaffected by this naming change. For example, Communication Manager 6.3 service packs will still have file names with the Communication Manager GA load string and a unique five digit identifier like: 03.0.124.0-12345.tar.
5. The service pack version information displayed on a running system will not change and will still show the Communication Manager service pack file name format like: 03.0.124.0-12345.
6. This naming change does not apply to service packs for Communication Manager Release 6.2 and earlier which will follow existing naming formats.

Communication Manager releases and service packs are cumulative, and all changes in 6.3.2.0 (Service Pack 2) are included in Communication Manager 6.3.2.1. Changes delivered to the Communication Manager 6.3.2.1 service pack are grouped as follows:

For the supported upgrade paths between Communication Manager releases and service packs, see the latest Communication Manager Software & Firmware Compatibility Matrix at http://support.avaya.com. The supported upgrade paths account for both Communication Manager internal data translation records as well as 100% inclusion of bug fixes.

For security purposes, Avaya recommends changing Communication Manager account passwords at regular intervals, staying current on the latest available Communication Manager Service Pack, and reinstalling Authentication Files periodically to change the local craft password.

Product Support Notices

Some problems are documented as Product Support Notices (PSN). To read the PSN descriptions online:

1. Go to http://support.avaya.com and enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOWNLOADS & DOCUMENTS** at the top of the page.
3. Begin to type **Communication Manager** into the **Enter Your Product Here** box and when **Avaya Aura® Communication Manager** appears as a selection below, select it.
4. Select **6.3.x** from the **Choose Release** pull-down menu to the right. Some PSNs are also found under the **Don't Know** release choice.
5. Check the box for **Product Support Notices** in the content filter to display the available PSN documents.
6. Click the PSN title links of interest to open the notices for viewing.

Communication Manager Messaging

For information regarding Communication Manager Messaging Service Packs (RFUs):

1. Go to http://support.avaya.com and enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOWNLOADS & DOCUMENTS** at the top of the page.
3. Begin to type **Messaging** in the **Enter Your Product Here** box and when **Avaya Aura®** **Communication Manager Messaging** appears as a selection below, select it.
4. Select **6.3.x** from the **Choose Release** pull-down menu to the right.
5. Click **View downloads** if necessary.
6. Available downloads for Communication Manager Messaging are displayed. Click the links to see the details.

Communication Manager Software

Communication Manager 6.3.2 software includes certain third party components including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 6.3 Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 6.3 Communication Manager Solution Templates DVD into the CD/DVD drive of a personal computer.
2. Browse the DVD content to find and open the folder D:\Licenses.
3. Within this folder are subfolders for Branch Gateway, Communication Manager, Installation Wizard, Session Manager, and Utility Services that contain the license text files for each application.
4. Right click the license text file of interest and select Open With => WordPad. This information is only accessible on the Communication Manager software DVD and is not installed or viewable on the Communication Manager Server.

Avaya Aura® Session Manager

For information regarding Session Manager updates:

1. Go to http://support.avaya.com and enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOWNLOADS & DOCUMENTS** at the top of the page.
3. Begin to type **Session** in the **Enter Your Product Here** box and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select **6.3.x** from the **Choose Release** pull-down menu to the right.
5. Click **View downloads** if necessary.
6. Available downloads for Session Manager are displayed. Click the links to see details.

Avaya Video Conferencing Solutions

Communication Manager 6.3 support for Avaya Video Conferencing Solutions including Radvision SCOPIA is documented in the Avaya Aura® Communication Manager SW and FW Compatibility Matrix and the Compatibility Matrix tool, both of which are available on http://support.avaya.com. Fixes and known issues for Avaya Video Conferencing Solutions including Radvision SCOPIA are included in the Communication Manager release notes.

System Platform

Communication Manager 6.x Releases and Service Packs are tested with specific versions and updates of System Platform 6.x. For more information, see Communication Manager Software & Firmware Compatibility Matrix at http://support.avaya.com or the appropriate Communication Manager Product Correction Notices.

Enhancements delivered to Communication Manager 6.3.2.0

Table 1: Enhancements delivered to Communication Manager 6.3.2.0 *1 of 2*

Problem	Keywords	Workaround
The Calling Party conversion screen is enhanced to introduce a new column named **Incoming number format**, and support to enter any in the **CPN Prefix** field has been added.		
A new field, Invoke ID for USNI Calling Name, is added to page 3 of the ISDN trunk-group screen. The system displays the new field when the trunk-group field is set to isdn with Carrier Medium set to pri/bri or atm, and the Supplemetary Service Protocol field is set to b. When the value of the new field is set to variable, then a new Invoke ID is selected each time the USNI Calling Name is sent to the far end. If the value of the new field is set to fixed-1, then the Invoke ID will be fixed as the number 1. This is required for interoperability with some equipment provided by other providers.	130481	
When Communication Manager runs in a VMware environment, each time Communication Manager VMware reboots, information about memory assigned to the VMware, CPU resources, and hard disk space assigned to the VMware is sent to the syslog and it shows up in the /var/log/messages folder.	130871	
Communication Manager, Call Center, and Communication Manager Messaging license usage data is now sent to WebLM.	130936, 131440.	
This is an enhancement to the GRIP 3587/4742 - Mute speakerphone when in shared control with One-X Communicator (1XC) feature that was delivered to Avaya Aura Feature Pack 1. With this enhancement, the deskphone is not muted in an ASAI initiated Single step conference while in the shared control mode with OneX Communicator.	131072	
When OPS mapping is created for a dual registered H.323 station, the call limit is synchronized with the number of call appearances administered for the station.	131109	

Table 1: Enhancements delivered to Communication Manager 6.3.2.0 *2 of 2*

Problem	Keywords	Workaround
This is an enhancement to the GRIP 3587/4742 - Mute speakerphone when in shared control with One-X Communicator (1XC) feature that was delivered to Avaya Aura Feature Pack 1. With this enhancement, the deskphone is not muted ASAI initiated Single step conference while in the shared control mode with OneX Communicator.	131422	
This is a new Message Tracer Analyzer version 6.4.5.3 that includes following: • Correction of CMS messages • Parsing of multi-digit r2mfc messages • Notifications of Internal Call Process and the Call Record fields • Parsing of the ASAI endpoint registration/ de-registration message	131744	

Problems fixed in Communication Manager 6.3.2.0

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *1 of 14*

Problem	Keywords	Workaround
DTMF could not be sent over a SIP trunk if the DTMF payload type was IN-BAND or Out-of-Band or RTP and PAUSE was required.	111735	
When a VDN service observer was observing a call and the call was transferred to a party that had the Can Be Service Observed? field set to no on the Class of Restriction screen, the service observer was not removed from the call.	120240	
Occasionally, there was one-way talk path on SIP calls that involved SRTP and EC500.	121260, 131438.	
There was wideband audio quality for calls made between Avaya SIP endpoints and Radvision XT endpoints. This was due to DTMF mode mismatch.	122111	
Orphaned TTI ports on the system caused the system to run out of ports. New TTI merges and PSA associates were denied because there were no ports available.	122983	
Occasionally, the **monitor bcms system** command did not show any data.	130157	Run the **monitor bcms system 1-8000** command.
Conference display was shown on a transferred call when SoftFlare was used to transfer a station to a held station.	130215	
The SIP network call redirection feature sent NCR REFER back to the party that initiated the transfer instead of the party that was on the call.	130223	
The display on bridged stations was not updated when a consult transfer was completed.	130261	
Call Admission Control did not apply for SIP to H.323 calls when Direct Media was enabled.	130315	
On a call made from Aastra to Communication Manager over Country Protocol 1b/1d (Telcordia), the endpoint on Communication Manager displayed the calling-party name and number. But on a call made from Communication Manager to Aastra over the same trunk, the endpoint on Aastra displayed only the calling-party number.	130361	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *2 of 14*

Problem	Keywords	Workaround
A Parallel-Forked Device could not be used to perform the following: • Deactivate Exclusion. • Bridge onto a Held call that had Exclusion deactivated The Parallel Forked Device was able to bridge onto a group-page call.	130383, 130580, 130885.	
A bridge appearance endpoint was unable to perform the Hold operation on the call when the call was already put on hold by the principal endpoint.	130395	
There was no video on a video call that was made from a One-X Communicator H.323 endpoint on Communication Manager to another One-X Communicator H.323 endpoint on another Communication Manager over a SIP trunk.	130430	
When the length of the calling-party number was greater than 13, Communication Manager truncated the calling-party number instead of removing the plus (+) sign.	130482	
The calling-party number was prefixed with an international access code from the trunk location when a station and a trunk were on different locations and the incoming call was of type national.	130506	
The value of the **Force Phones and Gateways to Active Survivable Servers** field on the **IP-Options System Parameters** screen could not be set to y. When the value of the field was already set to y, the changes could not be submitted to the Media Gateway screen. The system displayed the following error: `All MGs with the same BACKUP SERVER must have the same recovery rule`	130557	
Exclusion did not function properly on an endpoint when the 1XMobile SIP Dual Mode feature was activated.	130585	
After performing a Handoff to the cellular One-X Mobile, a user on an iOS could not release the call.	130606	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *3 of 14*

Problem	Keywords	Workaround
There was no talkpath for calls made between stations in different Stub Network Regions (SNR) with no common codec.	130632	Perform one of the following: • Use common codec from SNRs to CNR. • Remove the connectivity to CNR-1. • Remove Media resources from CNR-1.
A conference call involving bridged appearances of various parties dropped when one party in the call dropped and the remaining parties were put on hold.	130657	
Occasionally, Communication Manager did not send the ISDN Presentation Restricted when Per Station CPN - Send Calling Number was restricted.	130673	
The **SMI Network Configuration DNS Domain** field allowed invalid Domain Names to be inserted in the /etc/hosts file. This caused failures in failover instances on duplicated servers.	130768	
The logged-in agent hunt group audit could run only the first 1500 logged-in agents of a particular skill. When there were more than 1500 agents logged into a skill, the hunt group audit did not run properly.	130818	
On RadVision H.323 video endpoints, when a mid-call feature such as Hold, Transfer, or Conference is activated on video calls, video is not re-established on the call.	130831	
AACC could not dial Feature Access Codes that start with a pound (#) sign on the SIP station.	130879	
A dual registered (DR) Flare iOS endpoint and an H.323 endpoint were being used. The DR Flare iOS endpoint was used to make a video call to a SIP station. The DR H.323 endpoint then bridged onto the call. When the DR Flare iOS endpoint disconnected the call, the call dropped.	130893	
Communication Manager profiles were not properly restored during a migration from 5.2.1.	130901	
Communication Manager restarted when a 96xx SIP endpoint performed the Hold operation on a call.	130947	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *4 of 14*

Problem	Keywords	Workaround
When two or more Multiple Device Access (MDA) devices were on a call and one MDA device activated Exclusion, Communication Manager sent the BYE message followed by a PUBLISH (Dialog State Event Notification) message to the MDA device. When Session Manager received the the PUBLISH message before the BYE message, the MDA device that was dropped from the call displayed an idle call appearance instead of an active bridged call appearance.	130969	
The History Info messages generated in the invite message were different when the invite message had VOA and when the invite message did not have VOA.	130972	
After a Busyout followed by a Release operation on a DS1 board, Communication Manager sent a service acknowledgement message with an out-of-service indication on some of the PRI trunks right after the service-in service message had been sent. Even when Communication Manager sent additional Restart messages to the B channels, some vendor ISDN implementations did not process the requests properly. This rendered some trunks out-of-service until service and in-service messages were sent by Communication Manager.	131002	
Calls were stuck on the standby trunk when Digital Enhanced Cordless Telecommunications was forced back to the main server.	131053	
Occasionally, the CMS link dropped.	131065	
When encountering CAC limitations and call coverage on the called SIP station, the SIP caller did not hear call progress tones for around 50 seconds.	131077	
There was no talkpath on a SIP endpoint that was a whisper page group member.	131084	
An H.323 endpoint registered to an ESS got the incorrect IP address of the primary server in the Alternate Gatekeeper list. This caused the H.323 endpoint to fall back to the incorrect IP address.	131091	
A conference call hosted on an H.323 integrated multipoint control unit (MCU) was interrupted with MOH when one of the conference participants performed the Hold operation on the call.	131108	
Communication Manager reset on certain types of transfer operations, such as blind transfers.	131114	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *5 of 14*

Problem	Keywords	Workaround
A Flare endpoint was used to make a call to another Flare endpoint, and Music on Hold was enabled. One party on the call performed the Hold operation. The window of the endpoint that was used to perform the Hold operation still popped up allowing video operations. Ideally, after performing the Hold operation, the endpoint should not display the window.	131116	
The endpoint that was used to answer a pickup-group call displayed the trunk name instead of Anonymous when the incoming trunk call had no CPN.	131119	
Incoming Call Handling Treatment was applied to the calling numbers even when the SIP signaling group was administered to be in the Evolution Server mode.	131125	
Customer could not disable CDR1 and CDR2 on page 2 of the survivable-processor screen.	131128	
There was no video on video calls made between endpoints from unrecognized vendors or unrecognized video-endpoint models.	131129	
A SIP video endpoint was used to make a call to a Dual Registered (DR) extension. An audio-only DR H.323 endpoint was used to answer the call, and then a DR iOS Flare endpoint bridged onto the call. When iOS Flare escalated the call to video, there was no video on the call and the call dropped after 32 seconds.	131149	
Persistent intermittent port-network connectivity failures caused an overload condition that resulted in trunk groups going out-of-service.	131156	
Queued calls from ICR were not dropped automatically after the Session Establishment timer expired.	131157	
An outbound call transferred to an agent via hunt group showed only ANSWERED BY and no extension on the endpoint.	131165	
Occasionally, all ISDN PRI trunk calls failed due to internal software resource exhaustion.	131166	
When Communication Manager received two Hold REINVITE messages with a change in the SDP version, it did not send back the response.	131174	
Calls made from the attendant to an extension that were forwarded to the attendant overrid call forwarding when Chained Call Forwarding was active.	131189	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *6 of 14*

Problem	Keywords	Workaround
Occasionally, Communication Manager underwent **reload**.	131193	
Occasionally, attempting to send a call to an agent caused the CMS link to go down.	131195	
The **IMS Feature Sequencing** field was enabled when the station type was changed to a type that does not support IMS Feature Sequencing.	131210	
The display on a bridged appearance was not updated when a Facility Message with the Calling Party Name information was sent after a delay since the initial SETUP message.	131215	
An H.323 IP endpoint remained in the out-of-service state after a call on a media gateway went into the connection-reconstruct mode and then dropped.	131219	
A video SRTP-enabled SIP endpoint was used to make a call to a dual-registered (DR) extension. A video SRTP-enabled DR Flare endpoint was used to answer the call, and two-way video was observed on the call. A DR audio-only H.323 endpoint bridged on to the call. Depending on the SIP phones involved in the call, no video and one-way video was observed.	131228	
Occasionally, H.323 endpoints did not migrate to the ESS when the network region was disabled.	131233	
With the **Override ip-codec-set for SIP direct-media connections?** field on the **change system-parameters ip-options** screen set to y and only none given in the Media Encryption section of the ip-codec-set, calls between two Flare endpoints established with audio encryption, but no video encryption.	131236	
Call Admission Control did not apply to a call made from a SIP endpoint to an H.323 endpoint when Direct Media was enabled.	131240	
On Communication Manager, heavy call load on H.248 media gateways caused the gateways to become unstable, resulting in unpredictable call behavior.	131245	
There was a segmentation fault on Communication Manager during duplicate Processor Ethernet server interchange.	131248	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *7 of 14*

Problem	Keywords	Workaround
When a call has to be made from an H.323 One-X Communicator endpoint to an H.323 Radvision Elite 5000/6000 endpoint on an H.323 trunk, the caller can either dial into a video conference directly or via an IVR. There was audio and video on the call, but when mid-call operations such as hold were performed, the call was rendered audio-only.	131255, 131269, 131274.	
Calls were dropped when G.723-5.3K was configured, Shuffling was enabled, and Direct Media was disabled.	131256	
In a non-EAS environment, the hunt group members are unable to receive calls when a hunt group is changed from ACD to non-ACD.	131258	Remove the ACD hunt group and add it as non-ACD.
An ASAI redirection to a hunt group that is set up to be a SIP adjunct for MM was not acknowledged. But, it worked. The next request was denied because the domain control association was stuck.	131259	
XEN migration set is enabled on VE systems.	131260	
When an incoming R2MFC call that was made to an endpoint from a cellphone mapped to a EC500 station had ECF (Enhanced Call Forward) unconditional enabled to a SIP station, and if the SIP station did not answer the call, the call did not go to coverage of the endpoint that had ECF unconditional activated on it.	131268	
Any administration change using the change **ip-network-region** screen corrupted the backup server table on a previously administered server. This caused the Split Registration feature to not function correctly because the feature relies on the backup server tables for information to make network region auto disable and auto return decisions.	131285	
An SRTP call made to a TCP-registered CapNeg endpoint rang only on the bridged call appearances.	131286	
A meet-me paging call could not be answered from an IP trunk.	131298	
The SA8146 redirect display was incorrect for calls that were forwarded to a VDN with announcement vector steps.	131325	
Occasionally, large SIP messages were not parsed correctly. This resulted in truncated SIP headers.	131327	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *8 of 14*

Problem	Keywords	Workaround
When 128 simultaneous station firmware downloads occur, Communication Manager got into a state where new downloads requests were rejected. Phones that were rejected were not queued up again, and a station firmware download schedule did not complete successfully.	131339	
Administering the **Block Exclusion Event Notification** field on the Class of Restriction screen was blocked based on the Call Center Release number.	131346	
SA9124 enhancements did not work for ASAI 3PCC merge requests. The default trunk identifier was used.	131348	
For calls made over a SIP trunk to a VDN, the caller endpoint displayed the VDN name and number irrespective of the value of the ISDN/SIP Caller Display field in the hunt group screen.	131349	
Incoming trunk calls to a SAC station that was bridged on a DECT station failed to cover to MM.	131372	
An H.323 audio endpoint was used to make a call to a One-X Communicator SIP endpoint on Communication Manager. The H.323 endpoint then transferred the call to a Polycom HDX endpoint on another Communication Manager over a SIP trunk. The call dropped after the H.323 endpoint completed the transfer.	131386	
A SIP call answered on a bridged call appearance did not have talkpath when SA8965 was enabled.	131397	
Occasionally, due to data corruption, legacy port-networks such as G650s went out of service. Data corruption could be caused by running the **`list trace station`** or the **`status station`** command on an IP endpoint that was on a complex call, such as a large conference or a group page call.	131405	
There was no ringback tone on calls received on Communication Manager through Session Border Controller and Intelligent Customer Routing.	131409	
When the system reset and the first IPSI was added to translations, the IPSIs did not start functioning until after the next system restart of Communication Manager.	131412	
CDR failed to record the access code dialed for LAR calls.	131421	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *9 of 14*

Problem	Keywords	Workaround
The Service Observing Next Call Listen Only feature could not be activated remotely.	131425	
After a Session Manager failover, the SIP phones that were behind an SBC and on the call had stuck line appearances.	131427	
The VDN name in UUI was displayed incorrectly for AAEP call transfers.	131428	
VuStats did not check tenant calling permissions while deciding whether a user can view information regarding an agent, trunk group, VDN, or hunt group.	131433	
When Send All Calls and OneX Block All Calls was activated, the caller was unable to leave Voice Mail messages.	131435	
Supervisor Assist did not check tenant calling permissions while deciding whether an agent can call the supervisor.	131441	
Q-Stats (Q-Time and Q-Calls) did not check tenant calling permissions while deciding whether a user can view information from the hunt group.	131442	
The Hold operation could not be performed on SIP endpoints that were configured with multiple media encryption policies and Communication Manager was filtering out the top encryption policy.	131455	
Communication Manager stripped the crypto attribute from video calls when the port was set to 0. Hence, endpoints could not be used join the AAC calls.	131457	
The bridged call appearance could not drop the call after bridging onto a call when the primary endpoint had performed the Hold operation on the call.	131460	
A call made to an EAS agent when redirected on no answer to a VDN failed to cover to voice mail.	131469	
The One-X Client Enablement Services server could not be used with Communication Manager when it was routed via Session Manager Release 6.3 or later.	131470	
ASAI 3PMerge as part of CSTA SST (single step transfer) to a cellphone failed.	131479	
There was corrupted talk path on SIP calls when non-default packatization time was used for audio codecs.	131480	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *10 of 14*

Problem	Keywords	Workaround
When the second AES NICE logger observed the shared control endpoint, there was no talk path for the AES NIVE logger.	131501	
Calls made from a non-Avaya SIP endpoint dropped.	131519	
After a reset board command for a later vintage TN2602 board (Pacifica version), only half of the board's capability was used to set calls up.	131529	
When the second preference was chosen under the following conditions: • an EC500 or ONE-X call invoked ARS or AAR • the administered off-pbx number required a digit-conversion step • the first preference failed due to LAR then digit conversion did not occur, and the call was routed incorrectly.	131530	
The Genesys agent stopped functioning because an ASAI 3PCC answer request was not responded to. This happened because media resources were not available when the answer request was made.	131531	
While using a CTI application that included ASAI 3PCC commands on SIP endpoints, requests NACK'd with a CV of 111 - protocol error were observed.	131555	
A SoftFlare endpoint was used to make an audio call to an audio-only endpoint. After the answer was called, the SoftFlare endpoint escalated to video. The operation failed. When SoftFlare performed the Hold operation, it stopped functioning.	131556	
A trunk failure was observed, and the ASAI call offered message to a VDN was sent with no calling-party or called-party information.	131558	
Preserved H.323 trunk calls were dropped before the preservation time of two hours.	131559	
A Radvision XT 5000 endpoint was used to make a call to a LifeSize 1020 endpoint. The XT 5000 endpoint was then used to make a conference call between a LifeSize 1030 endpoint, a Flare endpoint, and a One-X Communicator H.323 endpoint. The One-X Communicator H.323 endpoint was dropped from the conference call after some time.	131568	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *11 of 14*

Problem	Keywords	Workaround
The system displayed the VE_BUF_FULL error when the collected-digit buffer was full.	131570	
Communication Manager restarted due to a limited SIP video memory leak.	131574	
Due to toll fraud restrictions (SA9122), Communication Manager blocked EC500 after answer when multiple trunks were present in the route-pattern to EC500.	131575	
The alerting message for a SIP endpoint logged in as an EAS agent did not follow VDN Override administration for the VDN that routed the call to the EAS agent.	131584	
On a SIP SRTP video call, the session type parameter was not sent during the Hold operation with Music on Hold enabled.	131587	
In media-gateway registration, announcement boards displayed `no board (list config media-gateway)` for several minutes after other boards were inserted.	131588	
Occasionally, calls made over a SIP trunk dropped when the SIP trunk was used for routing to a telecommuter destination.	131593	
When ROIF was enabled, Auto Exclusion did not remove the Service Observer for a manual-answer H.323 endpoint.	131595	
Communication Manager logs filled up with proc errors while using the ISAC (Internet Speech Audio Codec) codec, G.722.2, the iLBC (Internet Low Bitrate Codec), or the SILK codec developed by Skype.	131596	
A Communication Manager system (CM A) was routed to another Communication Manager system (CM B) through Session Manager, and the session refresh timer of CM A was less than the session refresh timer of CM B. CM B was connected to yet another Communication Manager system (CM C) by a SIP trunk that had Direct Media disabled. When an H.323 station (Station A) on CM A was used to make a call to another H.323 station (Station B) on CM B and Station B had an EC500 extension on CM C, both Station B and the EC500 extension alerted. When the call was answered on either Station B or the EC500 extension, the other stopped alerting and the call dropped.	131600	Enable Direct Media on the direct SIP trunk from CM B to CM C, or set the session refresh timer on CM A to a value greater than or equal to the value of the session refresh timer on CM B.

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *12 of 14*

Problem	Keywords	Workaround
There was only audio on a video call made from a Radvision XT-H.323 endpoint to a One-X Communicator SIP endpoint. The DTMF mode was RFC2833 for both the endpoints.	131624	
A SIP endpoint (SIP A) was used to call another SIP endpoint (SIP B). There was two-way talk path on the call. SIP A initiated attended transfer for an H.323 endpoint (H.323 C). Music On Hold was disabled. After SIP A completed the transfer, there was no talk path between SIP B and H.323 C.	131629	
When pound (#) is inserted before the digits of an outgoing call in a route pattern preference for a SIP trunk, the SIP INVITE has no digits.	131639	
VuStat values reset every 30 or 60 minutes depending on the administered measurement interval.	131644	
EC500 calls dropped when bridged appearances were administered on an IP DECT endpoint.	131645	
The endpoint displayed the name of an incoming SIP trunk call incorrectly when the username consisted of alphanumeric characters.	131648	
VP-MPP (Voice Portal) did not disconnect a call due to a lamp update received from Communication Manager. When VP changed its port to CTIACTIVE, and the port entered into CTI-only control mode, the call failed due to no CTI application.	131652	
Occasionally, Communication Manager reset during video calls on H.323 stations.	131654	
An SIP endpoint had features such as Bridged Call Appearance, Call Forward, Send Calls on an H.323 extension, and the Location field of the SIP endpoint on the IP Network Region screen was set to blank. During the button download of the H.323 endpoint, Communication Manager reset.	131657	
A SIP call could not be initiated because the CONN_M had a port in a bad state from a prior ASAI 3PCC merge involving a SIP endpoint that controlled the transfer.	131659	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *13 of 14*

Problem	Keywords	Workaround
A call was made from a One-X Communicator H.323 endpoint to a Radvision XT5000 SIP endpoint. The XT4200 SIP endpoint then was used to call a XT5000 SIP endpoint and a three-party conference took place. The One-X Communicator H.323 endpoint was dropped within three minutes.	131682	
Occasionally, there was no talk path on SIP calls that use SRTP.	131711	
Occasionally, a segmentation fault was observed on Communication Manager when an H.323 endpoint that had the EMU (Enterprise Mobility User) feature enabled had a bridged call appearance administered on the 24th button on the Station screen.	131714	
On a duplex server system, a system recovery that escalated to a Linux reboot did not complete and stopped before terminating all processes.	131720	
When an agent call with a bridged-call appearance was dropped, Communication Manager restarted due to an internal software trap.	131734	
There was no talkpath on incoming H.323 trunk calls. This happened when the signaling group of the trunk did not have Direct IP connections enabled.	131775	
When connection preservation was activated on call, a memory leak occurred and the transaction table filled up. Therefore, no more SIP processing could take place. This was observed only on systems that do not support UPDATE for session refreshes. This includes Communication Manager Release 6.0.1 systems. In Communication Manager Release 6.2, session refreshes are modified to use UPDATE instead of INVITE for refreshes. UPDATE handling does not encounter this problem.	131850	
When SIP downstream forking and reliable provisional responses were used simultaneously, the SIP transaction table filled up and SIP traffic was stopped.	131851	
A generic greeting was heard when a call that was made to a SIP endpoint covered to voice mail.	131959	

Table 2: Fixes delivered to Communication Manager 6.3.2.0 *14 of 14*

Problem	Keywords	Workaround
In a configuration where SIP messages associated with a call that was tandemed from a Communication Manager system to another over non-OPTIM SIP trunks, any one of the Communication Manager systems logged multiple UPDATE failures when the display name of the called party consisted of quotes. In some cases, the Communication Manager system reset.	131918	
ASAI Transfers and Conference operations from non-SIP stations that had EC500 or any other OPTIM feature enabled could not be performed.	131982	

Problems fixed in Communication Manager 6.3.2.1

Table 3: Fixes delivered to Communication Manager 6.3.2.1

Problem	Keywords	Workaround
When a principle station was active on a call and a bridged station attempted to originate another call, the bridged station was bridged on to the principle station's call.	132141	

Known problems

Known problems in Communication Manager 6.3.2.1

This release includes the following known issues in Communication Manager 6.3.2.1.

Table 4: Known problems in Communication Manager 6.3.2.1 *1 of 6*

Problem	Keywords	Workaround
If Communication Manager Messaging is configured for SRTP and the far-end doesn't offer SRTP, Communication Manager Messaging will not answer the call.	5336	Administer Communication Manager Messaging to RTP (non-SRTP) if far-end (endpoint, incoming trunk call from RTP environment) does not support SRTP.
In rotary analog stations, the inter-digit collection timer may expire too soon, preventing dialed calls from completing successfully. The workaround is the only solution to this issue since no Communication Manager software change has been planned.	101096	On the **`system-parameters features`** screen, page 6, there is a field called, **Short Interdigit Timer** (seconds). The default value of this field is 3 seconds. Increasing this value can fix this problem.
Communication Manager 6.x LSP servers cannot register with Communication Manager Main servers that are prior to the 5.2 release. If the LSP registers with a Communication Manager 5.1.2 or earlier Main server, you may need to enter the serial number of the media gateway to allow this LSP to register with the main server. To obtain a media gateway serial number, execute the **`list media-gateway`** SAT command on the main server and select one of the media gateway serial numbers displayed. Then configure the LSP with this serial number via the LSP SMI Server Role Web page. Note that this works as designed and no fix will be made in the Communication Manager software.	101016	

Table 4: Known problems in Communication Manager 6.3.2.1 *2 of 6*

Problem	Keywords	Workaround
A migration backup that was passphrase-protected on Communication Manager 5.2.1 where pre-upgrade patch 02.1.016.4-18793 was loaded could not be restored on Communication Manager 6.x unless quotes were put before and after the passphrase. This issue has been fixed in the latest pre-upgrade patch for upgrading from Communication Manager 5.2.1 to Communication Manager 6.x. The patch name is 02.1.016.4-19401.tar.gz, and it is available at http://support.avaya.com and PLDS.	111855	
Path Replacement does not work with Private numbering format for QSIG/SIP interworking. This also affects path replacement on a Communication Manager-Communication Manager Messaging QSIG trunk for the Messaging Transfer feature. The workaround is the only solution to this issue since no Communication Manager software change is planned.	113124	Change the numbering format from **Private** to **Unknown**.
After an interchange, the newly active server can experience call failures and occupancy spikes to overload levels. The occupancy prior to the interchange is 57% ST+CP or greater.	113197	
A call made from a 96xx SIP phone on Communication Manager 5.2.1 with RTP/SRTP enabled to a 96x1 SIP RTP phone on Communication Manager Release 6.2 or later with direct media enabled and CapNeg off drops immediately upon answer. This problem is resolved on the Communication Manager 5.2.1 side by applying service pack 12.01 (19751) or later.	101218, 120129, 120205.	Either turn off IP video on SIP signaling group to Session Manager on Communication Manager Release 6.2 and later, or remove 1-srtp from ip-codec-set on Communication Manager 5.2.1.
A 2004 IP phone on Communication Server 1000 calls an 1140 IP phone on a Business Communication Manager. If the 1140 IP phone blind transfers the call to a 96xx SIP phone, there is no talk path.	120170	

Table 4: Known problems in Communication Manager 6.3.2.1 *3 of 6*

Problem	Keywords	Workaround
S8300D main servers running Communication Manager with an unsupported medium or large memory configuration will be prevented from upgrading to Communication Manager Release 6.3 and later. S8300D survivable servers running Communication Manager in an unsupported medium or large memory configuration will automatically be converted to a small memory configuration during the upgrade to Communication Manager Release 6.3 and later. Medium and large memory configurations are not supported on an S8300D server, but previously administrators were not blocked from configuring these memory configurations. See PSN100127 for further information. **Note:** Survivable remote servers with a small survivable memory configuration can act as survivable servers for main servers with a large, medium or small memory configuration.	130445	All embedded (S8300D) Communication Manager main servers incorrectly configured with a large or medium memory configuration must be retranslated into small memory configuration before upgrading to, or having translations restored to, Communication Manager Release 6.3 and later.
IGAR is not supported on SIP endpoints.	130565, 130571, 130844.	
CM-A and CM-B have a QSIG trunk between them with **QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path?** set to yes and Diverted Party Identification set to principal for both switches. SIP phone A1 on CM-A calls B1 on CM-B which has call forward active to SIP phone A2 on CM-A. SIP phone A2 has cover-no-answer active to a sip-adjunct hunt-group which points to Avaya Aura Messaging or Communication Manager Messaging. If A2 does not answer the call forwarded from B1, the caller (A1) will reach the messaging mailbox for A2 instead of B1 as expected.	130582	

Table 4: Known problems in Communication Manager 6.3.2.1 *4 of 6*

Problem	Keywords	Workaround
Communication Manager should not allow endpoints to bridge onto a call when the Whisper Page feature is active. However, if Session Manager Multi-Device Access is in use, other SIP devices which are sharing an extension through parallel forking can bridge onto the whisper page call and have two way talk path with the paging extension.	130897	
When the ACB feature is administered on a parallel-forked extension, any attempt to invoke this feature on a busy extension will fail if the parallel-forked extension is active on another call.	131448	
Parallel Forked devices will not display detailed conference information on their call appearance.	131475	
If NCR is enabled, trunks can drop between multiple Communication Manager systems.	131829	Turn shuffling "on". If the customers want shuffling "off", then turn NCR "off". Turning NCR off is not serious as the only side effect is that a transfer involving intra-CM trunks may not drop instantly.
During deployment of the Communication Manager 6.3 Duplex vAppliance, the second vNIC labeled Asset is the Communication Manager duplication link and should be appropriately linked to the customer network. **Note:** After deployment this link can be found as "Network Adapter 2" within the Virtual Machine's properties and can be edited or linked from this location.	NA	

Table 4: Known problems in Communication Manager 6.3.2.1 *5 of 6*

Problem	Keywords	Workaround
The active server of a server pair running the Duplex Communication Manager Main/ Survivable Core Template can experience a service outage when System Platform is upgraded or updated on the standby server. **Note:** The basic steps outlined in the workaround are included in the connection preserving upgrade instructions for duplex servers in the document titled Upgrading to Avaya Aura® Communication Manager 6.3, which is available at http://support.avaya.com.	NA	Perform the pre-upgrade step on the active server. Busy out the standby server and upgrade/ update the System Platform. Release the standby server and verify the duplication state. Activate the Communication Manager Software update (service pack) on the standby server and again verify the duplication state. Perform a non-forced interchange of the Communication Manager servers. Busy out the previously active server which is now the standby and upgrade/update the System Platform. Release the standby server and verify the duplication state. Activate the Communication Manager Software update (service pack) on the standby server and again verify the duplication state.

Table 4: Known problems in Communication Manager 6.3.2.1 *6 of 6*

Problem	Keywords	Workaround
New features or feature options included in Communication Manager service packs are noted in the Enhancements section of the release notes. Often these new features or feature options have new administrative fields. Any changes added to the new administrative fields will be lost if the system is subsequently backed down to an earlier service pack that does not include the new administrative fields. This is the case even if translations that include the changes to the new fields are restored to the system following the activation of the earlier service pack that does not include the new administrative fields. Customers are required to back-up their systems before applying a new service pack so that translations that match the previous administrative fields are available, should the new service pack be removed and the system software restored to its previous state.	NA	
To avoid losing service, IP Softphone users should logoff, thereby, restoring their base phone to service prior to deactivating a Communication Manager service pack.	NA	

Known problems in Avaya Video Conferencing Solutions

This release includes the following known issues in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions..

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
Far End Camera Control (FECC) does not work on point-to-point calls between Radvision H.323 endpoints and Avaya SIP video endpoints that support FECC.	A28	
One-X® Communicator H.323 calls into Scopia Elite MCU over a SIP trunk gets no video.	A61/121975	Configure to use H.323 trunk as described in the Quick Setup Guide.

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
Video calls between Radvision VC240 and Flare Experience for Windows may result in low-resolution video.	A89/ SCAE-2403	On the Radvision VC240 web client, select **Configuration** > **Call Quality**, and set NetSense support to off.
Radvision MCU dialout calls to Avaya SIP endpoints using the H.323 protocol, for example, dialing the outbound call using a mismatched protocol type, results in the call flowing over the H.323 trunk to Communication Manager instead of the SIP trunk to Session Manager. Call flow results in an audio-only call.	A92	While creating terminals or endpoints on the iVIEW suite, be sure to properly assign the matching protocol type, SIP to SIP stations and H.323 to H.323 stations.
Radvision MCU dialout calls to an H.323 One-X® Communicator endpoint using the SIP protocol, for example, dialing the outbound call using a mismatched protocol type, results in the call flowing over the SIP trunk to Session Manager instead of the H.323 trunk to Communication Manager. Call flow results in CIF video.	A93	While creating terminals or endpoints on the iVIEW suite, be sure to properly assign the matching protocol type, SIP to SIP stations and H.323 to H.323 stations.
There is no content-sharing between Radvision XT and Avaya 1000 Series endpoints for point-to-point calls and calls made via Elite MCU.	R1	
SIP outdialing from Scopia Elite MCU uses the wrong SIP domain.	R4	Upgrade to iVIEW 8.2 or use this workaround to change default SIP domain on iVIEW 7.7: Manually add the default domain to the following file on the iVIEW ==> c:\ Program Files (x86)\ RADVISION\iVIEW Suite\iCM\jboss\bin\ vcs-core.properties "vnex.vcms.core.conference.defaultDomain=<domain>", where <domain> is the SIP domain for your system environment. Then restart the iVIEW Graphical User Interface.

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
SCOPIA Elite MCU shows SIP connection to iVIEW as down, but calls can be made successfully.	R6	Upgrade to iVIEW 8.2.
iVIEW does not strip the prefix digits for outbound calls from iVIEW to Communication Manager.	R13/ QC19493/ QC15404	Upgrade to iVIEW 8.2. For iVIEW 7.7, follow the admin steps in the Quick Setup Guide.
There is intermittent audio quality when Siren audio codecs are used for calls between Avaya 1000-series endpoints and the SCOPIA Elite MCU.	R14/AGS-289	Ensure that the Siren codecs are not in the Communication Manager ip-codec-set list.
Calls made from Radvision SCOPIA Elite MCU to Avaya SIP endpoints drop after 30 seconds.	R15	At the initial install, ensure that a functional FQDN is used for the Radvision iVIEW installation as per Radvision documentation. If FQDN is not configured, then reinstall it.
Avaya 1000-series calls made to Radvision XT1200 fail when G.729/G.729A is in the Communication Manager audio codec list other than the first position.	R75/ QC18567	Set G.729 and G.729A in the first position of the Communication Manager ip-codec-set list, or remove it from the ip-codec-set list.
(Avaya Video Conferencing Manager) AVCM allows endpoint discovery up to a /24 subnet (254 endpoints max or smaller subnet).	147	AVCM will not discover the endpoints, but instead manually enter them.
When upgrading the 1000 Series Endpoints "Upgrade License expired(15)" message may be displayed.	254	Ignore the message. Licensing is not required on the 1000 Series endpoints.
Sequential blind transfer of 10x0 endpoints may drop video.	255	If video is required after the transfers, drop and make a direct call.

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
After a Session Manager outage, 1010/1020 may take up to 30 minutes to re-register. Incoming calls are blocked while unregistered, but outgoing calls are accepted and immediately initiate registration.	260	When you see a red SIP box in the bottom right hand corner of the 1010/ 1020 screen, try manually registering by making an outgoing call or perform the following steps: 1. Log in to 1010/ 1020 as admin. 2. Select **Communications** . 3. Select **SIP** and enter your login credentials, and enter the IP address of the Session Manager system you have to register to. 4. Click **Register**.
1030/1040/1050 may transmit higher bandwidth than requested. Occasionally, this can cause 5+ party conferences to fail on 1050.	288	Administer 1040/1050 endpoints to send no more than 2M video.
Calls from Windows Flare Experience to ADVD with H.263 do not establish video. The hold and release operations drop the call.	130041	Enable H.264 on the ADVD endpoint in the ADVD Settings File.
HDX H.323 calls to AV10X0's is audio-only in a Multi Communication Manager configuration.	122851	Set DTMF rtp payload.
RMX dial-out to AV1010/20 leads to one-way video (Connect with Problem).	AVA-1551	Use dial-in on RMX.
ADVD may show severely distorted video with XT5000 embedded MCU.	A87/ ADVD-9909	This interop is currently not supported with FP2 and FP3.

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
No warning is currently given when a Zone Prefix is used on the iVIEW Gatekeeper administration screen for a Communication Manager entry that matches with either a Service Prefix or the leading digits of an assigned Virtual Room. Matching prefix entries can cause calls to route incorrectly and the call will fail.	R118/ QC20634	Ensure that Zone Prefix for the Communication Manager Gatekeeper entry does not match any of the Service Prefixes or the leading digits of any of the Virtual Rooms.
Parties joining an active conference call on the MCU that has **ALL** muted join the conference with active audio.	R123/ QC20032	
iVIEW8 does not show stats for SIP participants on initial view of the stats pop-up window.	R136/ QC21009	The screen can be updated by either closing the meeting room details pop-up window and bringing up a new one or by selecting "More Information..." under the "Action" drop down menu on the endpoint details.
Adding a new Communication Manager gatekeeper via Scopia Management may not update Scopia ECS.	R157/ QC21263	Manually update Scopia ECS to route calls to the new Communication Manager gatekeeper.
ADVD video calls made to a Radvision Elite MCU via an IVR result in audio-only connections for the ADVDs.	10012	ADVDs should dial directly into the virtual conference room instead of dialing in via the IVR.
When using Siren codecs on a Lifesize endpoint with **Override ip-codec-set for SIP direct-media connections** set to yes on page 2 of the **change sys ip-options** screen on Communication Manager, the 1050 can be limited to 4-party conferences if any of the Lifesize endpoints have Siren codecs above G.722 and G.711 in their priority list.	130531	Make sure Siren codecs are below G.722 and G.711 in the Lifesize codec priority list. The list is accessed on the Lifesize endpoint at **System Menu** > **Administrator Preferences** > **Audio** > **Audio Codec Order**.
One-X Communicator or ADVD blind transfers to HDX SIP fails to connect and drops after 30 seconds when BFCP (H.239) is enabled.	130722	Disable BFCP (H.239).

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
On Multi-Communication Manager audio calls between ADVD and One-X Communicator SIP, after performing the Hold operation twice on the ADVD, users have audio and video.	10078	
Flare video escalations from an audio-only call to Radvision H.323 XT endpoints going over an H.323 trunk remain audio-only.	130320	
One-X Communicator H.323 endpoints drop from a Lifesize 1050 conference call.	130321	Register the One-X Communicator endpoints as SIP endpoints instead of H.323.
XT5000 calls made to a bridged appearance on ADVD leads to an audio-only call.	130434	Currently, ADVD does not support bridging another station that is another ADVD.
Video SRTP calls to TLS registered HDX fail to connect.	131375	Use TCP signaling on the HDX.
If using Communication Manager CAC, the SAT **`status ip-network-region`** screen does not show the correct tally for the **# Times Exceed BW Hit Today** field for video calls that are denied due to bandwidth limits.	131466	Run the **`display events`** command, and select **denial** as the category. You can give a date to narrow down the results. Look for denial event **2373: No Video BW available** in the **Evnt Cnt** column to ascertain the number of times the bandwidth limit was reached for a given date range. Note that the event count is for the entire system and not listed as per ip-network-region.
Polycom VVX transfers to Lifesize 10x0's are not supported and result in transfer failures.	131661	
Multi-Communication Manager One-X Communicator H.323 calls in an XT MCU conference loses audio when video is stopped.	131684	Move the H.323 One-X Communicators to instead be SIP registered One-X Communicators.

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
Multi-CM transfers of Flare via One-X Communicator to an XT MCU may fail.	131689	
Mid-Call Features are not supported behind the DMA.	131696	
Poor video can occur if the second video line is used for video calls between One-X Communicator SIP and HDX H.323.	ONEXC-7691	
When a Polycom Gatekeeper is involved, all Polycom entities should be associated with the Polycom Gatekeeper (DMA/CMA).	AVA-1562	
Transfers from VVX SIP to 96x0 H.323 fail.	AVA-1576	
In a Multi-Communication Manager XT hosted conference, the One-X Communicator H.323 cannot become the active speaker.	QC23239	Stop the video and restart it.
One-X Communicator SIP in an XT MCU conference loses video when the XT dials out to a 96x0/96x1 endpoint.	QC23240	Have the 96x0 or the 96x1 endpoint dial into the XT MCU conference.
Flare dial in calls to RMX conference result in no audio.	NGUE-17174	Disable **override ip-codec set** and **limit audio codecs** to G.722 and G.711.
Radvision XT H.323 to Radvision XT H.323 calls end up with audio-only connection when any SIP endpoint transfers the call from one Radvision XT H.323 to another Radvision XT H.323.	131741	
Consulted transfers using SIP endpoints and a Radvision XT H.323 endpoint result in one-way video.	131746	Press hold/unhold or video stop/start to bring up two-way video.
Glare condition may occur when two Flare endpoints are on a call and press hold/resume simultaneously.	131901	Set Music On Hold (MOH) to "Yes" on Communication Manager.
There is no talkpath after transfer of a Multi-Communication Manager call involving a Polycom VVX endpoint and an H.323 endpoint.	131950	

Table 5: Known problems in Communication Manager 6.3.2.1 for Avaya Video Conferencing Solutions

Problem	Keywords	Workaround
There is one-way talkpath between a Polycom HDX and a 96xx SIP endpoint when H.239 is enabled on the Polycom HDX.	131951	Disable H.239 on the Polycom HDX.
Calls started as audio-only Multi-Communication Manager become audio and video calls after performing the Hold operation and then releasing them.	SCAE-3910	Set Music On Hold (MOH) to No on Communication Manager.
Flare clients cannot access MCU Meeting Room via IVR.	QC23513	Dial into the meeting room directly.

Technical Support

Support for Communication Manager is available through Avaya Technical Support.

If you encounter trouble with Communication Manager:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
   - Logging on to the Avaya Technical Support Web site http://www.avaya.com/support
   - Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

   You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Note:
If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to http://www.avaya.com for further information.

When you request technical support, provide the following information:

- Configuration settings, including Communication Manager configuration and browser settings.
- Usage scenario, including all steps required to reproduce the issue.
- Screenshots, if the issue occurs in the Administration Application, one-X Portal, or one-X Portal Extensions.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

Tip:
Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

For information about patches and product updates, see the Avaya Technical Support Web site http://www.avaya.com/support.

Appendix A: Acronyms

3PCC	Third Party Call Control
AAC	Avaya Aura Conferencing
AAR	Automatic Alternate Routing
ACD	Automatic Call Distribution
ACW	After-Call Work
ADVD	Avaya Desktop Video Device
AES	Application Enablement Services
APC	Avaya Performance Center
ARS	Automatic Route Selection
ASA	Avaya Site Administration
ASAI	Adjunct Switch Applications Interface
ATB	All Trunks Busy
ATM	Asynchronous Transfer Mode
AVP	Avaya Voice Portal
AWOH	Administered WithOut Hardware
BA	Bridge Appearance
BCMS	Basic Call Management System
BFCP	Binary Floor Control Protocol
BSR	Best Service Routing
BRI	Basic Rate Interface
BTD	Busy Tone Disconnect
CDR	Call Detail Record
CID	Caller Identification
CIE	Customer Interaction Express
CIF	Common Intermediate Format
CLI	Command Line Interface
CLAN	TN799 Control LAN circuit pack that controls TCP/IP signalling and firmware downloads
CMA	Call Management System
CMM	Communication Manager Messaging
CMS	Call Management System

CNC	Control Network C
COR	Class of Restriction
CPU	Central Processing Unit
CPN	Calling Party Number
CR	Call Recognition
CRV	Call Reference Value
CS1K	Communication Server 1000
CSS	Center Stage Switch
CTI	Computer Telephony Integration
CUCM	Cisco Unified Communications Manager
DAC	Direct Agent Calling
DC	Direct Current
DCP	Digital Communications Protocol
DCS	Distributed Communication System
DECT	Digitally Enhanced Cordless Telecommunications
DMCC	Device Media and Call Control
DPT	Dial Plan Transparency
DSP	Digital Signal Processor
DSCP	Differentiated Services Code Point
DTMF	Dual Tone Multi-Frequency
EAS	Expert Agent Selection
ECFB	Enhanced Call Forwarding Busy
ECFU	Enhanced Call Forwarding Unconditional
EMU	Enterprise Mobility Users
ES	Evolution Server
ESS	Enterprise Survivable Server
EWT	Expected Wait Time
ETSI	European Telecommunication Standards Institute
FAC	Feature Access Code
FNE	Feature Name Extension
FRL	Facility Restriction Level
FS	Feature Server
HDX	A Polycom high definition video room system
HEMU	Home Enterprise Mobility User

IAC	International Access Code
ICR	Intelligent Customer Routing
IDM	Initial Direct Media
IGAR	Inter-Gateway Alternate Routing
IP	Internet Protocol
IPSI	Internet Protocol Server Interface
ISDN	Integrated Services Digital Network
ISG	Integrated Services Gateway
IVR	Interactive Voice Response
J24	Avaya Digital Terminal for Japan
LAN	Local Area Network
LAI	Look Ahead Interflow
LAR	Look Ahead Routing
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LSP	Local Survivable Processor
OPTIM	Off-Premise Telephony Integration with MultiVantage
MCSNIC	Mask Calling Number/Station Name for Internal Calls
MCU	Multipoint Control Unit
MCH	Multiple Call Handling
MG	Media Gateway
MGC	Media Gateway Controller
MIA	Most Idle Agent
MIB	Management Information Base
MLDP	Multi-Location Dial Plan
MLPP	Multiple Level Precedence Preemption
MOH	Music on Hold
MPC	Maintenance Processor Complex
MST	Message Sequence Trace
MTA	Message Trace Analysis
MWI	Message Waiting Indication
NCR	Network Call Redirection
NIC	Network Interface Card
NR	Network Region

OEM Original Equipment Manufacturer
OPTIM Off-PBX-telephone Integration and Mobility
PAM Pluggable Authentication Modules
PBX Private Branch eXchange
PE Processor Ethernet
PRACK Provisional Response Acknowledgement
PROCR Processor Ethernet
PSA Personal Station Access
PSTN Public Switched Telephone Network
PCD Packet Control Driver
PCOL Personal Central Office Line
PN Port Network
PNC Port Network Connectivity
QSIG International Standard for inter-PBX feature transparency at the Q reference point
R2MFC Register Signaling 2 Multi Frequency Compelled
RDTT Reliable Data Transport Tool
RFC Request for Comments
RMB Remote Maintenance Board
RMX A Polycom media conferencing platform, used by CM as a video and audio bridge
ROIF Redirect on IP Failure
RONA Redirect on No Answer
RTCP RTP Control Protocol
RTP Real-Time Protocol
SAC Send All Calls
SAT System Access Terminal
SAL Secure Access Link
SAMP Server Access and Maintenance Processor
SBA Simulated Bridge Appearance
SBC Separation of Bearer and Signaling
SBS Separation of Bearer and Signaling
SDP Session Description Protocol
SEMT SIP Endpoint Managed Transfer
SES SIP Enablement Services
SIF Source Input Format

SIP	Session Initiation Protocol
SO	Service observer
SMI	System Management Interface
SSC	Single Step Conference
SSH	Secure Shell
SSHD	Secure Shell Daemon
STE	Secure Terminal Equipment
SVNS	Simple Voice Network Statistics
TAC	Trunk Access Code
TAE	Telecommuting Access Extension
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TEG	Terminating Extension Group
TLS	Transport Layer Security
TSC	Temporary Signaling Connection
TSP	Toshiba SIP Phone
TSRA	Time Slot Record Audit
TTI	Terminal Translation Initialization
TTS	Time To Service
UCID	Universal Call ID
URI	Uniform Resource Identifier
URN	Universal Resource Name
USNI	United States Network Interface
USB	Universal Serial Bus
UUI	User to User Information
VALU	Value-Added
VCS	Video Conferencing Server
VDN	Vector Directory Number
VEMU	Visitor Enterprise Mobility User
VLAN	Virtual Local Area Network
VOA	VDN of origin Announcement
VoIP	Voice over Internet Protocol
VP	Voice Portal
VSST	Virtual Server Synchronization Technology

VSX A Polycom standard definition video room system