Release Notes

3.3 | January 2015 | 3725-82877-016/A

Polycom® RealPresence® Mobile, for Android®

6001 America Center Drive
San Jose, CA 95002
USA

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

What's New in Release 3.3

Polycom RealPresence Mobile 3.3 includes the features and functionality of previous releases and includes these new features:

Note: Get the latest product information from Polycom Support
To view the latest Polycom product documentation, visit Polycom Support web site.

User Interface Improvements

RealPresence Mobile 3.3 has newly designed user interfaces and icons to consolidate the user interface across all Polycom endpoint products. The RealPresence Mobile and the RealPresence Desktop user interfaces share common icons such as Recent Calls, Address Book, Mute, Place a Call, and Hang Up.

Standalone Mode Supports More Features

Standalone mode provides features such as content sharing, FECC, TLS in SIP protocol, media encryption, and local contact on tablets. See Feature Overview for a complete list of feature capabilities on tablets and phones.

Support for BroadSoft Device Management as Provisioning Server

From this release, BroadSoft Device Management is supported to provision RealPresence Mobile. In standalone mode, RealPresence Mobile can register with a BroadSoft server to use provisioned features. Only LDAP search is not supported.

Set up BroadSoft Device Management to Provision RealPresence Mobile

To configure BroadSoft Device Management for provisioning RealPresence Mobile, the BroadSoft Device Management administrator must pay attention to the following:

- Review the sample RealPresence Mobile file named `ProvisionData-template.xml` released with RealPresence Mobile. The file `ProvisionData-template.xml` is published on Polycom Support.
- Decide what to be provisioned in the customer deployment.
- Create your RealPresence Mobile provisioning template by defining the customer TAG set and assigning default values to each customer TAG.
- When adding a new Device Profile Type for RealPresence Mobile in the BroadSoft Device Management system, set the parameters to the values as follows:
  - Set **Device Access Context Name** to **`dms`**.

  - Set **Device Access URI** to **`POLYCOM/RPM`**
  - Use the customer TAG set that you defined as **Default System Tag Set** and **Tag Set**.
- When adding a new Device Profile Type file for the new created Device Profile Type, set the parameters to the values as follows:
  - Set **Device Access File Format** to **`ProvisionData.xml`**.
  - Set **Repository File Format** to **`ProvisionData-%BWLOGIN-ID-1%.xml`**.
  - Set **File Category** to **`Dynamic Per-Device`**.
  - Set **File Customization** to **`Administrator and User`**.

  After creating this Device Profile Type file, create a device profile for it.
- When adding or editing existing users for RealPresence Mobile,
  - choose **Use Custom Credentials** in the **Authentication** panel. The custom credentials will be the sign-in credentials for RealPresence Mobile.
  - bind the created device profile to the user account.

  If necessary, you can specify the Custom TAGs of the user account for the provisioning. The new values will overwrite the default values specified in the template **`ProvisionData.xml`** file.

After the configuration is done and the SRV record `_dmsconfig_tcp` is set on the DNS server properly, RealPresence Mobile can detect the provisioning server automatically using users' e-mails. Users can also specify the server when signing in RealPresence Mobile. RealPresence Mobile assumes each BroadSoft user has its specific provisioning data. If an user signs in RealPresence Mobile on multiple devices with the same user account, all the devices will get the same provisioning data.

Support for High Video Resolution (720p)

RealPresence Mobile 3.3 has the capability to encode 720p video stream on powerful mobile devices such as Samsung S5, and Samsung Galaxy Tab Pro 8.4". The video quality will be improved significantly.

This feature is available in standalone mode and managed mode and is only for AVC point to point calls, AVC multi-points calls, and Scalable Video Coding (SVC) point to point calls.

Support for the SDP Size Adjustment Feature

Enable this feature to shorten Session Description Protocol (SDP) size to avoid call failure caused by SDP size limitation for some users. Enter `#001#` from the Dialpad to enable or disable this feature.

Note: Video content, FECC, H.264 high profile, RFC 2833 for DTMF, and SVC cannot be used

When you enable **SDP Size Adjustment**, video content, FECC, H.264 high profile, RFC 2833 for DTMF, and SVC cannot be used.

Devices Support Changes

RealPresence Mobile 3.3 adds the support for the following Android devices:

- Samsung Galaxy Tab Pro 8.4"
- Samsung Galaxy S5 Phone

RealPresence Mobile 3.3 drops the support for the following Android devices:

- HTC One X phone

- Samsung Galaxy SII GT-I9100 Phone

Release History

The following table shows the release history of the Polycom RealPresence Mobile application.

Release History

Version	Release Date	Features

3.3	January 2015	Support for BroadSoft Device Management as Provisioning Server
		User Interface Improvements
		Standalone mode provides more features. See Feature Overview for a complete list of feature capabilities.
		Support for high video Resolution (720p) on powerful mobile devices, such as Samsung S5, and Samsung Galaxy Tab Pro, for AVC point to point calls, AVC multi-points calls, and SVC point to point calls.
		Support for the SDP Size Adjustment Feature
		Device Support Changes
		• This release adds support for the following devices:
		  ◦ Samsung Galaxy Tab Pro 8.4”
		  ◦ Samsung Galaxy S5 Phone
		• This release drops the support for the following Android devices:
		  ◦ HTC One X phone
		  ◦ Samsung Galaxy SII GT-I9100 Phone

3.2.1	July 2014	The **Roster** display button is not shown in CloudAXIS 1.5 and earlier versions. Fixed an OpenSSL security vulnerability (CVE-2014-0224).
3.2	June 2014	Support for CloudAXIS HTTPs tunneling Support for roster display in a CloudAXIS meeting Support for log collector Support for Far-end Camera Control (FECC) on Android tablets in managed mode Support for sharing pictures on Android tablets in managed mode Support for the following new devices: • Samsung Galaxy Tab 3 7” SM-T217A Tablet • Samsung Galaxy Tab 3 8” SM-T311 Tablet
3.1.1	March 2014	Fixed the issue SWEP-5765. See Resolved Issues for details.
3.1	January 2014	Support for portrait mode in a call (Android only) Support for higher quality video on Tegra-3 tablets (test feature) Support for the following new Android devices: • Samsung Galaxy Tab 10.1" LTE SC-01D tablet • Samsung Galaxy Note II GT-N7100 phone • HTC One 801e phone

Release History

Version	Release Date	Features
3.0	July 2013	Support for H.264 high-profile calls (outgoing and incoming). Support for auto-answer incoming calls. When enabled, this feature allows users to choose to mute the audio or video of auto-answered calls. Support for the following devices: • Samsung Galaxy S4 GT-I9500 Phone • Samsung Galaxy Note 8.0 GT-N5100 Tablet • LG Optimus G pro LG-F240L Phone • Sony Xperia ZL L35h Phone • Sony Xperia Z SGP312 Tablet Enabled users to hide or display local self-view.
2.3	March 2013	Support for the Polycom RealPresence CloudAXIS™ solution.

2.2	February 2013	Support for the following new features on non-Tegra 2 Android tablets:
		• Polycom SmartPairing™ which enables you to control and swipe calls to Polycom HDX and Group Series devices from a tablet.
		• Content sharing
		  ◦ Supported only in the managed mode.
		  ◦ Only PDF files can be shared.
		Support for the enterprise SVC solution on non-Tegra 2 Android tablets and phones. IVR service in SVC calls is also supported.

2.1	December 2012	Bug fix.
2.0	November 2012	Support for H.460 firewall traversal in standalone mode. Access to media statistics. Support for Samsung Galaxy Note 10.1” SHW-M480K tablet.
1.3.1	August 2012	Support for the following devices: • Samsung Galaxy Tab 2 7” GT-P3110 tablet • Samsung Galaxy Tab 2 10” GT-P5100 tablet • Samsung Galaxy Note GT-I9220 phone • Samsung Galaxy SII GT-I9100 phone • Samsung Galaxy SIII GT-I9300 phone • ASUS Transformer Pad TF300T tablet Added Android 4.1 support for tablets that use hardware codecs.
1.3	June 2012	Ability to run on Android phone. Support for firewall/NAT.
1.1	February 2012	XOOM and Galaxy: Enhanced user interface experience. DROID XYBOARD: Added automatic provisioning support.
1.0.4	January 2012	XOOM and Galaxy: Added support for Android 4.0.
1.0.3	December 2011	XOOM and Galaxy: Enabled users to disable H.323 calls. User interface enhancements. Added support for server provisioning, AES for H.323 calls, and H.460 firewall traversal.

Release History

Version	Release Date	Features
1.0.2.1	November 2011	DROID XYBOARD: Software release specially for DROID XYBOARD.
1.0.2	October 2011	XOOM and Galaxy: Fixed some known issues.
1.0	October 2011	XOOM and Galaxy: Initial release.

Hardware and Software Requirements

The following hardware and software requirements were determined based on test scenarios. Your system's actual performance may vary based on software or hardware configurations.

Hardware and Software Requirements

Manufacturer	Model	Android Version	Network Requirements	Optional Peripheral Devices
ASUS	Transformer Pad TF300T tablet	4.2.1	• Wireless Local Area Network (WLAN), 802.11 a/b/g/n • 3G or 4G network	• 3.5 mm headset • Stereo Bluetooth headset
HTC	One 801e	4.4.2		
LG	Optimus G pro LG-F240L Phone	4.1.2		
Motorola	DROID XYBOARD tablet	4.0.4		
Samsung	Galaxy Tab 8.9" SHV-E140S tablet	4.0.4	• Wireless Local Area Network (WLAN), 802.11 a/b/g/n • 3G or 4G network	• 3.5 mm headset • Stereo Bluetooth headset
	Galaxy Tab 2 7" GT-P3110 tablet	4.1.1		
	Galaxy Tab 2 10" GT-P5100 tablet	4.1.2		
	Galaxy Tab 10.1" LTE SC-01D tablet	4.0.4		
	Galaxy Tab 3 7" SM-T217A Tablet	4.2.2		
	Galaxy Tab 3 8" SM-T311 Tablet	4.2.2		
	Galaxy Note 10.1" SHW-M480K tablet	4.1.2		
	Galaxy Tab Pro Tablet 8.4"	4.4.2		
	Galaxy SIII GT-I9300 phone	4.1.2		
	Galaxy S4 GT-I9500 Phone	4.4.2		
	Galaxy S5 Phone	4.4.2		
	Galaxy Note 8.0 GT-N5100 tablet	4.1.2		
	Galaxy Note II GT-N7100 phone	4.3		
SONY	Xperia ZL L35h Phone	4.2.2		
	Xperia Z SGP312 Tablet	4.3		

To view your Android system version:

» From your device, touch **Settings > About device > Android Version**.

Products Tested in This Release

Polycom RealPresence Mobile systems are tested extensively with a wide range of products. The following table does not provide a complete inventory of compatible equipment, but indicates the products that have been tested for compatibility with this release.

Note: Upgrade your Polycom products

You are encouraged to upgrade all your Polycom systems with the latest software before contacting Polycom support to ensure that the issue has not already been addressed by vendor software updates. Go to the Polycom support website to find the current Polycom Supported Products matrix.

Polycom CMA System and RealPresence Resource Manager System

The RealPresence Mobile application can register to the Polycom CMA Server and Polycom RealPresence Resource Manager server. Some management features have limitations relative to other Polycom endpoints. For example, software updates of RealPresence Mobile are not supported and the QOS monitoring is limited.

Products Tested in This Release

Type	Product	Version
NAT/Firewall/Border Controller	ACME Packet Net-Net 3820	Firmware SCX6.3.0 MR-5 Patch 2
	Polycom VBP® 5300-ST	11.2.19
	Polycom VBP-E	11.2.19
	Polycom RealPresence® Access Director™	4.0, 4.1
Gatekeeper, Gateways, External MCU, Bridges, Call Managers	Polycom Distributed Media Application™ (DMA®) 7000	6.1.0, 6.2.0
	Polycom Converged Management Application™ (CMA®) 4000/5000	6.2.5
	Polycom RealPresence Resource Manager	8.2, 8.3
	Polycom RMX® 4000/2000	8.4, 8.5
	Polycom RMX® 1500	8.5
	Polycom RealPresence® Collaboration Server 1800	8.4, 8.5
	Polycom RMX® 1000C	2.5.1
	Polycom RSS™ 4000	8.5.1
	Polycom RealPresence Capture Server	1.8
	Broadsoft SIP r19 Server	r19
	Polycom RealPresence CloudAXIS™ Suite	1.6, 1.6.1

Products Tested in This Release

Type	Product	Version
Endpoints	Polycom HDX® Series	3.1.4, 3.1.5
	Polycom RealPresence Mobile	3.2, 3.3(iOS) 3.2, 3.3(Android)
	Polycom VVX®	5.0.1
	Polycom CMA® Desktop	5.2.6
	Polycom Telepresence m100	1.0.7
	Polycom RealPresence Desktop	3.2, 3.3(Windows)
		3.2, 3.3(Mac)
	Polycom RealPresence Group Series	4.1.4, 4.2

Install and Uninstall RealPresence Mobile

This section explains how to install and uninstall RealPresence Mobile.

To install the RealPresence Mobile application:

1. From the Google Play application, search for **polycom** or **video conferencing** to find the RealPresence Mobile application.
2. Touch **Free**, and touch **OK** to accept permission. The application downloads and installs automatically.

To uninstall the RealPresence Mobile application:

1. From your device's application list, touch **Settings > Applications > Manage applications,** and touch  **Video**.
2. Touch **Uninstall**.
3. When you are prompted to confirm, touch **OK.** Your user data is deleted when you uninstall this application.

Feature Overview

The following table lists the available features. Features marked with an asterisk (*) are enabled by a provisioning server.

RealPresence Mobile Features

Category	Features	Android Phone Standalone Mode	Android Phone Managed Mode	Android Tablet Standalone Mode	Android Tablet Managed Mode
Call functions and capability	Enterprise SVC solution	✓	✓	✓	✓
	IVR service in SVC calls	✓	✓	✓	✓
	Placing H.323 calls	✓	✓	✓	✓
	Enabling and disabling H.323 calling	✓	✓ *	✓	✓ *
	Specifying H.323 gatekeepers	✓	✓ *	✓	✓ *
	Specifying internal or external gatekeepers	✓		✓	
	Receiving H.264 content during H.323 calls	✓	✓	✓	✓
	Receiving H.263 and H.263 + content during H.323 calls	✓	✓	✓	✓
	Registering to SIP servers	✓	✓ *	✓	✓ *
	Specifying SIP proxy servers	✓	✓ *	✓	✓ *
	Placing SIP calls over UDP	✓	✓ *	✓	✓ *
	Placing SIP calls over TCP	✓	✓ *	✓	✓ *
	Receiving H.264 content during SIP calls	✓	✓	✓	✓
	Receiving H.263 and H.263 + content during SIP calls	✓	✓	✓	✓

RealPresence Mobile Features

Category	Features	Android Phone Standalone Mode	Android Phone Managed Mode	Android Tablet Standalone Mode	Android Tablet Managed Mode
Call functions and capability	Selectable call rates between 64 kbps - 1 Mbps (high call rate is only supported on on high performance devices)	✓	✓	✓	✓
	H.264 content sending up to 720 p			✓	✓
	H.263 and H.263+ content sending up to XGA			✓	✓
	• H.264 encode at up to 1280 x 720 (video) • H.264 decode at up to 1280 x 720 (video)	✓	✓	✓	✓
	H.264 decode at up to 720 p (content)	✓	✓	✓	✓
	H.264 high profile calls (outgoing and incoming)	✓	✓	✓	✓
	H.263 and H.263+ decode at up to XGA (content)	✓	✓	✓	✓
	Automatic gain control	✓	✓	✓	✓
	Acoustic echo cancellation	✓	✓	✓	✓
	Automatic noise control	✓	✓	✓	✓
	Polycom Siren Lost Packet Recovery	✓	✓	✓	✓
	WLAN, 3G and 4G network support	✓	✓	✓	✓

RealPresence Mobile Features

Category	Features	Android Phone Standalone Mode	Android Phone Managed Mode	Android Tablet Standalone Mode	Android Tablet Managed Mode
Call control	Muting your audio during a call	✓	✓	✓	✓
	Pause your video during a call	✓	✓	✓	✓
	DTMF during a call	✓	✓	✓	✓
	Viewing call statistics by touching	✓	✓	✓	✓
	Switching between the front and rear cameras	✓	✓	✓	✓
	Adjusting volume during a call	✓	✓	✓	✓
	Network quality indicator during a call	✓	✓	✓	✓
	Portrait Mode	✓	✓	✓	✓
	Far-end Camera Control (FECC)			✓	✓
SmartPairing	SmartPairing			✓	✓
	Transferring calls to HDX or RealPresence Group systems			✓	✓
Security and Encryption	H.460 firewall traversal	✓	✓	✓	✓
	Encrypting H.323 calls	✓	✓	✓	✓ *
	SIP digest authentication	✓	✓ *	✓	✓ *
	RTP keep-alive	✓	✓	✓	✓
	TLS/SRTP support	✓	✓	✓	✓
	BFCP over UDP	✓	✓	✓	✓
	SIP dial string	✓	✓	✓	✓
	Certificate verification (Android 4.0 and later)		✓		✓
	SBC Interoperability	✓	✓	✓	✓
	SIP outbound proxy	✓	✓	✓	✓
	SIP fail-over	✓	✓	✓	✓

RealPresence Mobile Features

Category	Features	Android Phone Standalone Mode	Android Phone Managed Mode	Android Tablet Standalone Mode	Android Tablet Managed Mode
Professional features	Provisioning service		✓		✓
	Local address book	✓	✓	✓	✓
	LDAP service		✓		✓

System Capabilities and Constraints

The following protocols, resolutions, algorithms, and ports are supported for RealPresence Mobile.

Capabilities

Capabilities

Call Rate	Video Capability
1 Mbps	720p
512 kbps 384 kbps 256 kbps	360p
64 kbps	Audio only

Protocols

The following table lists the protocols supported in this version of the RealPresence Mobile application.

Protocols

Protocol	Description
DNS	Domain Name System
H.235	Security and Encryption
H.239	Token Management
H.323	Signaling
H.460	Firewall/NAT Traversal
LDAP, H.350	Directory Services
NTLMv2	Authentication
Polycom LPR™	Lost Packet Recovery
SIP	Session Initiation Protocol

Resolutions

The following table lists the resolutions supported in this version of the RealPresence Mobile application.

Resolutions and Frame Rate

Resolution and Frame Rate	Source
Up to 720p, 15 fps	Video sent from camera
Up to 720p, 30 fps	Video received from far end
Up to 720p, 7.5 fps	Content received from far end
Up to 720 p, 3 fps (Tablets only)	Content showing from the tablets

Note: Video capability
Actual transmitted video resolution is determined by several factors, such as camera capability, computer performance, network conditions, the far-end system's capabilities, and whether content is being received.
HD/720p 30 fps is the maximum video receiving capability. The actual resolution is based on the negotiation with the far end.

Algorithms

The following table lists the algorithms supported in this version of the RealPresence Mobile application.

Algorithms

Algorithm Type	Description
Audio	G.722.1 Annex C G.711u G.711a Siren LPR Acoustic Echo Cancellation (AEC) Automatic Gain Control (AGC) Scalable Audio Coding (SAC)
Video	H.264 SVC H.264 AVC H.264 high profile H.263 and H.263+ (for content only) **Note:** H.261 is not supported.
Encryption	AES-128 media encryption TLS for SIP calls

Inbound and Outbound Ports

The following table lists the inbound and outbound ports supported in this version of the RealPresence Mobile application.

Inbound Ports

Port	Function
1720 (TCP)	H.323 Call Signaling (H.225)
1719 (UDP)	H.323 Registration, Admission, and Status (RAS)
3230 - 3250 (TCP)	H.323 Call Signaling (H.245)
3230 - 3250 (UDP)	Media (RTP/RTCP)
3238 (UDP and TCP)	BFCP
5060 (UPD and TCP)	SIP

Outbound Ports

Port	Function
443 (TCP)	Provisioning, Monitoring, Help Files, HTTPS
389 (TCP)	LDAP
5060 (UDP and TCP)	SIP
5061 (TCP)	SIP TLS signaling
1720 (TCP)	H.323 Signaling (H.225)
1719 (UDP)	H.323 Registration, Admission, and Status (RAS)
3230 - 3250 (TCP)	H.323 Signaling (H.245)
3230 - 3250 (UDP)	Media (RTP/RTCP)
3238 (UDP and TCP)	BFCP

Interoperability Issues

You may encounter the following issues when using RealPresence Mobile with other products or on specific operating systems.

Interoperability Issues

Limitation Type	Description	Solution
Limitations Related to the Android Versions and Devices	The RealPresence Mobile log file on Android 4.4 may only catch 16 KB size logs.	It is a limitation of the Android 4.4 OS. You can use `adb logcat` to catch RealPresence Mobile logs.
	SmartPairing auto detection does not work on Sony tablets.	Use manual detection.
	The speaker's volume is a little low during a call on the following Samsung tablets: • Tab3 7" T217A • Tab3 8" T311	Adjust the volume to the maximum on the tablets.
	RealPresence Mobile Android version 3.0 and later cannot launch on Tegra-2 devices (XOOM tablet and Galaxy Tab 10.1" GT-P7510/GT-P7500 tablet).	To enjoy the full features (RPM 2.3 release) of this application on your Tegra-2 tablets, download **REALPRESENCE MOBILE - TEGRA 2** from **Google Play**.
	The following two issues are due to the system limitation on tables using Acoustic Echo Cancellation (AEC): • On the Samsung Galaxy Tab 8.9", Samsung Galaxy Tab 10.1" LTE SC-01D, and ASUS Transformer Pad TF300T tablets, you cannot adjust the speaker volume by using the hardware Volume control. • If a Transformer Pad TF300T tablet is close to Polycom HDX or Group Serial 500 systems which enable Ultrasound, you can hear noise from the far end.	This is a system limitation of the tablet. The tablet's system volume control is used for RealPresence Mobile. When a tablet uses AEC, the system volume control does not work.
	The far end can hear an echo if RealPresence Mobile running on Android device is in the same conference and does not mute. • Sony Xperia Z SGP312 Tablet • Transformer Pad TF300T Tablet • DROID XYBOARD Tablet • Galaxy Tab 2 10" GT-P5100 Tablet	This is a limitation of the tablet.The microphone and the speaker are placed very close. Use a headset or lower the speaker's volume.
	When you run RealPresence Mobile on HTC smart phones, the loudspeaker volume is too low to be heard during a call.	This is a limitation of the tablet. Use a headset.

Interoperability Issues

Limitation Type	Description	Solution
Limitations Related to the Android Versions and Devices	Placing SIP calls over TCP may fail on the following tablets: • Transformer Pad TF300T Tablet 4.1.1 and 4.2.1 • Samsung Tab2 7" GT-P3110 Tablet 4.0.3 • Samsung Tab2 10" GT-P5100 Tablet 4.0.3 • Samsung Galaxy Note GT-I9220 Phone 4.0.3 • SONY Xperia ZL L35h Phone 4.1.2, 4.2.2, and 4.3 • SONY Xperia Z SGP312 Tablet 4.1.2 and 4.2.2 Placing SIP calls over UDP (Default) and SIP over TLS on the above tablets works well. The root cause is TCP/IP stack on Android 4.0.3 will check SIP messages. If TCP packet size is larger than 1500 bytes, it may be dropped by the system.	Try one of the following: • Use SIP over UDP (Default) or SIP over TLS. • Change the UDP or TCP listening port to a non-standard port on the SIP server.
	When using Android tablets with Acoustic Echo Cancellers, SmartPairing fails with auto-detection. • On Transformer Pad TF300T tablets, auto detection does not work. • On Galaxy Tab 8.9” SHV-E140S, Galaxy Tab 10.1" LTE SC-01D, and Galaxy Tab 2 10” GT-P5100 tablets, auto detection does not work during calls. • On SONY Xperia Z SGP312 tablet, auto detection does not work.	You can manually add the room systems’ IP addresses to control the room systems on non-AEC tablets.
	On the Samsung Galaxy Tab2 PT-3110 tablet and Samsung Galaxy Tab2 PT-5100, received video is delayed on long calls, or when you are sharing content.	This is due to the low CPU capability of the tablets. To avoid performance issues, only 1x1 layout is supported in SVC meetings. Users can see only the active speaker during SVC meetings.
	On some Android devices with display ratio other than 16:9, you may see video distortion in a meeting.	None.

Interoperability Issues

Limitation Type	Description	Solution
Limitations Related to Other Polycom Products	If you create a Continuous Presence (CP) only conference call on Polycom RMX 4000/2000 systems and Polycom RealPresence Collaboration Server 800s version 8.1 with default content settings (**Content Settings: HiResGraphics** and **Content Protocol: H.264 HD**), the RealPresence Mobile application cannot send or receive content if call rate is set as 384 kbps or below.	• Change the RMX **Content Settings** to **Graphics**, and **Content Protocol** to **H.263 & H.264 Auto Selection**. • Set the call rate on RPM to above 384 kbps.
	Prior to version 4.1.0, Polycom VVX 1500 always reboots when the RealPresence Mobile application sends 320 x 180 video to a Polycom VVX 1500 system.	This issue was fixed in VVX 1500 4.1.0, upgrade to 4.1.0 or newer version when using RealPresence Mobile with VVX 1500.
	RealPresence Mobile supports only using English user name and password to sign in Polycom CMA server and RealPresence Resource Manager, or register to a gatekeeper or an SIP server.	Use English user name and password.
	If you use an MPM+ media card in a call with an RMX system, a blue edge is displayed at the bottom of the video window.	Use an MPMX media card with the RMX system.
	In a motion mode conference, RealPresence Mobile receives video with a large delay because the video is 60 fps.	Set a conference with sharpness mode on MCU.
	RealPresence Mobile in internet may fail to call Telepresence m100 in intranet.	Let Telepresence m100 call RealPresence Mobile.
	When VSX® Visual Concert™ calls RealPresence Mobile, only audio is connected.	Let RealPresence Mobile call VSX Visual Concert.

Known Issues

The following table lists the known issues for this release. If a workaround is available, it is noted in the table.

Known Issues

Category	Issue ID	Description	Workaround
Video	SWEP-6439	When you mute video in an AVC conference with the test feature enabled on an ASUS Android device, your video is frozen on far ends.	Disable the test feature.
Other	SWEP-6812	OpenSSL Memory Leak may occur. This issue impacts OpenSSL1.0.1 server implementations for both SSL or TLS and DTLS.	None.

Resolved Issues

The following table lists the resolved issues in version 3.3.

3.3 Resolved Issues

Category	Issue ID	Description
Content	SWEP-6290	You might see a mosaic screen when RealPresence Mobile joins a RMX conference which enables content transcoding, and there is packet loss to the H.264 content stream.
SVC	SWEP-6350	RealPresence Mobile may stop working after joining an SVC conference with more than 100 SVC participants.

The following table lists the resolved issues in version 3.2.

3.2 Resolved Issues

Category	Issue ID	Description
Content	SWEP-4932	(SIP Call only) When the call rate of Telepresence m100 is lower than the call rate of RealPresence Mobile and when M100 calls RealPresence Mobile, RealPresence Mobile cannot send content to M100.
Other	DSTC-1541	When you are trying to sign in RealPresence Mobile, RealPresence Mobile may incorrectly display a certificate warning for the intermediate CA issued certificate.
Video	SWEP-5592	RealPresence Mobile received video is stretched when RealPresence Mobile is inter-operating with VSX Visual Concert.

Version 3.1.1 fixed the issue SWEP-5765.

3.1.1 Resolved Issues

Category	Issue ID	Description
CloudAXIS	SWEP-5765	Android participants are not able to join CloudAXIS meetings.

The following table lists the resolved issues in version 3.0.

3.0 Resolved Issues

Category	Issue ID	Description
Video	SWEP-3772	When a telephone call is answered, the RealPresence Mobile application remained active and transferred audio to far end. This issue has been fixed.

Enterprise Scalable Video Coding Solution

SVC is a scalable media relay conferencing solution based on SVC and Scalable Audio Coding (SAC) codecs. It is an alternative to the Advanced Video Coding (AVC) mode that has traditionally been supported. Differences between the two modes are listed in the following table.

Differences between SVC and AVC

SVC Mode	AVC Mode
Each participant in the conference call is received by the client as a separate video stream.	The composite video image is determined by the bridge based on administrator configuration.
A Caller ID is indicated by text in the appropriate window, on display throughout the call.	Caller ID information is displayed intermittently.
Double-clicking or tapping on a participant's video, content video, or local preview expands that video to full screen. Double-clicking or tapping again reverts the display to the composite image. Pinch controls enable you to zoom in and out on a participant's video or content video.	Layout may typically be controlled by dialing **, and then selecting a format.

The SVC solution provides the following features:

- For video send and receive, support up to 720p on high performance devices under 1 Mbps call rate.
- For video send, support 7.5/15 fps
- For video receive, support 7.5/15 fps
- Support auto layouts of 1x1, 1+1 through 1+5.

  The maximum layout of 1+5 comprises 4 remote participants plus 1 content-sharing frame, and 1 local preview frame.
- Support for AVC content.
- Support for Scalable Audio Coding (SAC) with at least two quality layers.
- Ability to mix up to three different audio streams from the MCU.
- Ability to combine up to four different SVC video streams (call rate at 512kbps and above) from the MCUs.
- Support for SVC dial-out from DMA.

Using SVC conference calls has following limitations:

- Does not support recording.
- Far-end Camera Control (FECC)
- In a SIP call, when networks using UDP experience 10 percent packet loss, the screen layout on received devices can be incorrect.
- Does not support H.323 call
- In a poor network connection, sometimes a participant disconnects automatically from an SVC call. This can result in a frozen video stream of the participant. The RMX system will clear the frozen stream in 30 minutes.

Access Media Statistics

To access media statistics, click . The following table shows the meaning of each value.

Media Statistics

Value	Description
Call Type	SIP or H.323 call type.
Call Encryption	Indicates whether your call is encrypted.
Far Site Name	Name of the far site.
Far Site System	Type of video conferencing system at the far end and the software version.
Call Speed	Negotiated speed (bandwidth) for the call, which is usually the combined video and audio speeds in the call.
Video Protocol	ITU-C video algorithm and annexes used in the current call. The video protocol used depends on the capabilities of the system at the far end as well as on your system's configuration.
Video Format	Picture size currently in use.
Audio Protocol	Audio algorithm and annexes used in the current call. The audio protocol used depends on the capabilities of the system at the far end as well as on your system’s configuration.
Audio Rate	Bandwidth specified for the audio portion of the call. The proportion of the audio rate to the video rate depends on the protocol used.
Video Rate	Bandwidth specified for the video portion of the call. The proportion of the video rate to the audio rate depends on the protocol used.
Video Rate Used	Actual bandwidth being used for the video portion of the call. This is a real-time measurement, which normally fluctuates.
Video Frame Rate	Rate your system uses to update the picture seen at the far end. The system can send up to 15 fps. If the camera picks up large, continuous, or frequent motions, the software takes longer to assemble the data into video frames, and the frame rate drops. Changes in lighting also reduce the frame rate.
Video Packets Loss Percentage	Total video packet loss as a percentage of the total number of video packets transmitted by your system and those transmitted by the far end.
Video Jitter	Percentage of variation in the video transmission rate.
Audio Packet Lost	Number of audio data packets lost during the call, including transmitted packets and incoming packets. Packet loss indicates congestion or other problems on the network.
Audio Packets Loss Percentage	Total audio packet loss as a percentage of the total number of audio packets transmitted by your system and those transmitted by the far end.
Audio Jitter	Percentage of variation in the audio transmission rate.
Content Protocol	Format used for the recording, compression, and distribution of the content.
Content Format	Display resolution of the content.

Media Statistics

Value	Description
Content Rate	Rate your system uses in content transmission.
Content Rate Used	Actual bandwidth being used for the content transmission.
Content Frame Rate	Rate your system uses in content frame transmission.
Content Packets Lost	Number of content data packets lost during the call, including transmitted packets and incoming packets. Packet loss indicates congestion or other problems on the network.
Content Packets Loss Percentage	Total audio packet loss as a percentage of the total number of content packets transmitted by your system and those transmitted by the far end.

Prepare Your Device for Mutual Transport Layer Security

You can establish secure communications using Mutual Transport Layer Security (MTLS) with provisioning servers such as Polycom DMA, CMA, or RealPresence Resource Manager systems.

To establish MTLS connections, the client and server need to hold certificates issued from the same Certificate Authority (CA) and the root certificate of this CA.

To import certificates into your Android device, you need to generate a Certificate Request (CSR) first by using a computer that has installed the OpenSSL tool.

The following example uses Mac as the example.

To generate and import your certificate:

1. Open the Terminal from your Mac computer.
2. Generate the private key *client.key*. For example:
   ```
   Mike-MacBook-Pro:~ root# openssl genrsa  -out client.key 1024
   ```
3. Generate the certificate request *client.csr*. For example:
   ```
   Mike-MacBook-Pro:~ root# openssl req -new -key client.key -out client.csr
   ```
   You are about to be asked to enter information that will be incorporated into your certificate request.

   What you are about to enter is what is called a Distinguished Name or a DN.

   There are quite a few fields but you can leave some blank
   ```
   For som-----
   Country Name (2 letter code) [GB]:cn                 ---CSR info.
   State or Province Name (full name) [Berkshire]:bj  ---CSR info.
   Locality Name (eg, city) [Newbury]:bj      ---CSR info.
   Organization Name (eg, company) [My Company Ltd]:plcm  ---CSR info.
   Organizational Unit Name (eg, section) []:caqa   ---CSR info.
   Common Name (eg, your name or your server's hostname) []:caqa  ---CSR info.
   E-mail Address []:pp@pp.com  ---CSR info.
   ```

   Enter the following extra attributes to be sent with your certificate request. Write down the challenge password. You will need it later in the procedure
   ```
   A challenge password []:1234            -----see [Note1]
   An optional company name []:poly
   ```
4. Submit the certificate request to your CA:
   a. View the content of the file *client.csr* using the following command, then select and copy its content (from ---BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST---):
   ```
   Mike-MacBook-Pro:~ root# cat client.csr
   ```
   b. Go to your CA's web interface http://<CA's IP address>/certsrv/, and click **Request a certificate**.
   c. Click **Advanced certificate request**.

d Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

e Paste the content of the file **client.csr** to the **Saved Request** text field, and click **Submit**.

f Click **Base 64 encoded** and click **Download certificate.**

The file is saved as *certnew.cer* by default in the folder **Downloads**.

5 Move the generated **certnew.cer** file to your current directory.

6 Convert the file *ccertnew.cer* to a .p12 file by using the OpenSSL tool. For example:

```
Mike-MacBook-Pro:~ root#openssl pkcs12 -export -in certnew.cer -inkey
client.key -out client.p12 -name testp12
Enter Export Password:

Verifying - Enter Export Password:
```

The export password should be the same as the challenge password you set in step 3.

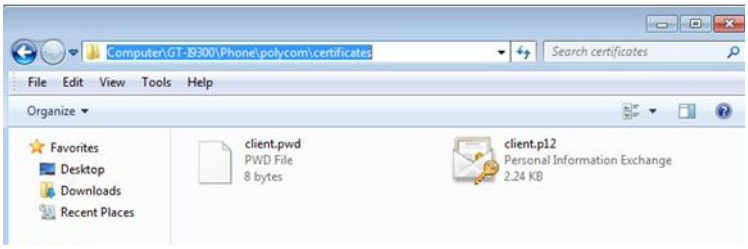
7 Encrypt the challenge password you set in Step 3:

a Go to Convert Strings.

b Enter the challenge password in the text field, and click **Base64 Encode!**.

c Copy the encoded text from the following text field, and save it as a .pwd file, for example, *client.pwd*.

8 Connect your Android phone or tablet to a PC using a USB cable, then copy file *client.p12* and *client.pwd* to your phone or tablet's internal storage, under the directory **/polycom/certificates**.



To import the root certificate of your CA into Android device:

1 Go to your CA's web address http://<CA's IP address>/certsrv/, click **Download a CA certificate, certificate chain, or CR**L.

2 Select **Base 64**, and then click **Download CA Certificate.**

3 Connect your Android phone or tablet to a PC using a USB cable.

4 From your Android phone or tablet, tap **Settings > Security > Install from Storage**.

5 Follow the screen prompt to enter, or set, the screen lock password.

6 Name the certificate, or accept the suggested name.

7 Click **OK** to install the certificate.

The certificate is now installed on your device.

Note: Hold CA root certificate and system's certificates on servers

To establish MTLS connection with servers such as Polycom DMA, CMA, or RealPresence Resource Manager systems, the Polycom DMA, CMA, or RealPresence Resource Manager system should also hold the CA root certificate and the system's certificates.