Release Notes

Polycom® RealPresence® Mobile, Version 2.0 for Android® Devices

Polycom is pleased to announce this release of the Polycom® RealPresence® Mobile application.

This document provides the latest information about the RealPresence Mobile application, version 2.0, for Android-powered smart phones and tablet devices.

Software Version History

Version	Release Date	Features
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.
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.

November 2012
3725-82877-010/A

Hardware and Software Requirements

Manufacturer	Model	Android Version	Network Requirements	Optional Peripheral Devices
ASUS	Transformer Pad TF300T tablet	4.1.1	• Wireless Local Area Network (WLAN), 802.11 a/b/g/n • 3G or 4G network	• 3.5 mm headset • Stereo Bluetooth® headset
HTC	One X phone	4.0.4		
	One S phone	4.0.3		
	Jetstream tablet	3.1		
Motorola	XOOM tablet (Tegra 2-based)	4.1.2		
	DROID XYBOARD tablet	4.0.4		
Samsung	Galaxy Tab 8.9” SHV-E140S tablet	4.0.4		
	Galaxy Tab 10.1” GT-P7510/GT-P7500 tablet (Tegra 2-based)	4.0.4		
	Galaxy Tab 2 7” GT-P3110 tablet	4.0.3		
	Galaxy Tab 2 10” GT-P5100 tablet	4.0.3		
	Galaxy SII GT-I9100 phone	4.0.3		
	Galaxy SIII GT-I9300 phone	4.0.4		
	Galaxy Note 10.1” SHW-M480K tablet	4.0.4		
	Galaxy Note GT-I9220 phone	4.0.3		

To view your Android system version:

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

Interoperability

Polycom CMA® System and RealPresence Resource Manager System

The RealPresence Mobile application can register to the Polycom CMA® server version 6.2 and Polycom RealPresence Resource Manager server version 7.1. The CMA and RealPresence Resource Manager systems can schedule and perform limited monitoring of the RealPresence Mobile application, but cannot fully manage, provision, or update the application.

Products Tested with This Release

Polycom RealPresence Mobile systems are tested extensively with a wide range of products. The following list is not a complete inventory of compatible equipment. It simply indicates the products that have been tested for compatibility with this release.

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 http://support.polycom.com/PolycomService/support/us/support/service_policies.html to find the current Polycom Supported Products matrix.

Type	Product	Version
NAT/Firewall/Border Controller	ACME Packet Net-Net 3820	Firmware SCX6.3.0 F-2 GA
	Polycom VBP 5300-ST	11.2.13
	Polycom RealPresence Access Director	2.0.1

Type	Product	Version
Gatekeeper, Gateways, External MCU, Bridges, Call Managers	Polycom Distributed Media Application™ (DMA™) 7000	5.0, 5.1.0
	Polycom Converged Management Application™ (CMA) 4000/5000	6.0.1, 6.2
	Polycom RealPresence Resource Manager 5000	7.0.0, 7.1.0
	Polycom RMX® 4000/2000	7.7, 7.8
	Polycom RMX 1000 with Hardware Version C	2.4.2
	Polycom RSS™ 4000	8.0, 8.5
	Broadsoft SIP r17 Server	SP2
	DeltaPath	2.9.2
Endpoints	Polycom HDX® systems	3.0.5, 3.1.0
	Polycom RealPresence Mobile system	1.3.2, 2.0 (iOS) 1.3.1, 2.0 (Android)
	Polycom VVX systems	4.1.0
	Polycom Telepresence m100	1.0.4
	Polycom CMA Desktop	5.2.3
	Polycom RealPresence Desktop	2.0
	Polycom RealPresence Group Series	4.0.0
Content Sharing Applications	Polycom People+Content™ IP	1.2.3 (PC only)

Setting Up the RealPresence Mobile Application

Before you can use the RealPresence Mobile application, you need to configure network and server settings. You can register to a provisioning server to get the settings automatically, or enter settings manually.

You can use the RealPresence Mobile application without registering to a provisioning server. However, to use advanced features such as content sharing, AES, LDAP, and H.460 firewall traversal, you need to register to a provisioning server, called Provisioned mode.

To install the RealPresence Mobile application:

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

To uninstall the RealPresence Mobile application:

1. From your device's application list, touch **Settings > Applications > Manage applications,** and then touch  **Video**.
2. Touch **Uninstall**.
3. When you are prompted to confirm, touch **OK.**

Your user data is deleted when you uninstall the application.

Feature Overview

This table lists features available in version 2.0. Features marked with an asterisk (*) are enabled by the provisioning server.

Features	Android Phone Standalone	Android Phone Provisioned	Android Tablet Standalone	Android Tablet Provisioned
H.460 firewall traversal	✓	✓	✓	✓
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 + content during H.323 calls		✓		✓ (non-Tegra 2-based tablets)
Encrypting H.323 calls		✓		✓ *
Placing SIP calls	✓	✓ *	✓	✓ *
Enabling and disabling SIP calls	✓	✓ *	✓	✓ *

Features	Android Phone Standalone	Android Phone Provisioned	Android Tablet Standalone	Android Tablet Provisioned
Registering to SIP servers	✓	✓ *	✓	✓ *
Specifying SIP proxy servers	✓	✓ *	✓	✓ *
SIP digest authentication	✓	✓ *	✓	✓ *
Placing SIP calls over UDP	✓	✓ *	✓	✓ *
Placing SIP calls over TCP	✓	✓ *	✓	✓ *
Receiving H.264 content during SIP calls		✓		✓
Receiving H.263 + content during SIP calls		✓		✓ (non-Tegra 2-based tablets)
Selectable call rates between 64 kbps and 512 kbps Selectable call rates between 64 kbps and 1920 kbps (Tegra 2-based tablets)	✓	✓	✓	✓
For non-Tegra 2-based tablets and Android phones: • H.264 encode at up to 320x240 (video) • H.264 decode at up to 480x352 (video) For Tegra 2-based tablets: • H.264 encode at up to 720 p (video) • H.264 decode at up to 720 p (video)	✓	✓	✓	✓
H.264 decode at up to 720 p (content)		✓		✓
For non-Tegra 2-based tablets and Android phones: H.263+ decode at up to 720 p (content)		✓		✓
Automatic gain control	✓	✓	✓	✓
Acoustic echo cancellation	✓	✓	✓	✓
Automatic noise control	✓	✓	✓	✓
WLAN, 3G and 4G network support	✓	✓	✓	✓
Muting your audio during a call	✓	✓	✓	✓
Muting your video during a call	✓	✓	✓	✓
DTMF during a call	✓	✓	✓	✓
Viewing call statistics by touching	✓	✓	✓	✓

Features	Android Phone Standalone	Android Phone Provisioned	Android Tablet Standalone	Android Tablet Provisioned
Switching between the front and rear cameras	✓	✓	✓	✓
Adjusting volume during a call	✓	✓	✓	✓
Polycom Siren LPR	✓	✓	✓	✓
Provisioning service		✓		✓
Network quality indicator during a call	✓	✓	✓	✓
Local address book		✓		✓
LDAP service		✓		✓
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	✓	✓	✓	✓

New Features in Version 2.0

Version 2.0 provides the following new features:

- Support for H.460 firewall traversal in standalone mode.
- Ability to access Media Statistics by clicking .
- Support for Samsung Galaxy Note 10.1″ SHW-M480K tablet

Access to Media Statistics

To access media statistics, click the antenna icon .

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 its 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 frames per second. 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.

Value	Description
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.
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.

New Features in Previous Versions

Version 1.3.1

- 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

- Android 4.1 support for tablets that use hardware codecs

Version 1.3

- Ability to run on Android devices (HTC One S, HTC One X, HTC JetStream tablets)

Firewall/NAT Support

- Ability to keep RTP (Real-time Transport Protocol) NAT mapping alive during live streaming.
- Ability to support Secure Real-time Transport Protocol (SRTP) and Transport Layer Security (TLS) for the secure transmission of media.
- Ability to support Binary Floor Control Protocol (BFCP) over a UDP link. Control signaling can be forwarded using the best-effort traffic class in firewall and NAT traversal.
- Support the following dial strings when you place calls without registering to any server.

H.323	SIP
• name@domain • name@IP • extension@domain • extension@IP • IP##extension	• <name>@<domain> • <name>@<ipAddress:port> • <extension>@<domain> • <extension>@<ipAddress:port>

- Ability to verify server certificates by using installed root certificates (SIP, HTTPS, and LDAP) when establishing TLS connections.
- Ability to interoperate with ACME SBC systems.
- Support for SIP signaling FW/NAT traversal over TCP/TLS as defined in RFC5626.
- Ability to switch to a backup SIP server in case the primary server fails.

Version 1.1

For Galaxy, XOOM, and DROID XYBOARD:

- Ability to support Galaxy, XOOM, and DROID XYBOARD in one RealPresence Mobile application *.apk* file
- Usability enhancement

Version 1.0.4

For Galaxy and XOOM: Support for Android 4.0.

Version 1.0.3

For Galaxy and XOOM:

- Usability enhancement.
- Ability to disable H.323 calls.
- Ability to receive content using H.239 and BFCP when you are registered to a provisioning server.
- Ability to support AES encryption for H.323 calls when you are registered to a provisioning server.
- Support for H.460 firewall traversal when you are registered to a provisioning server.
- Support for muting your audio and video during a call.
- Ability to allow a provisioning server to supply configuration settings automatically when you are registered to the provisioning server.
- Ability to create a local address book when you are registered to a provisioning server.
- Ability to access LDAP (Lightweight Directory Access Protocol) service when you are registered to a provisioning server. With LDAP service, you can call contacts in your corporate directory or add them to your local address book.

Version 1.0.2.1

For DROID XYBOARD:

- Dual stack operation that enables the Polycom RealPresence Mobile application to connect to SIP or H.323 systems
- H.264 encode at up to QVGA, 15 fps
- Support for H.460 firewall traversal
- Video receiving at up to 480x352, 30 fps
- Support for Polycom Constant Clarity™ technology, such as Polycom® Siren™ Lost Packet Recovery, which can effectively improve the decreased audio quality caused by packet loss
- Configurable network and bandwidth settings that make the RealPresence Mobile application operate well in virtually any network
- Support for automatic gain control and echo cancellation
- Ability to view network quality during a call

Version 1.0.2

For Galaxy and DROID XYBOARD: Usability enhancements

Version 1.0

For Galaxy and DROID XYBOARD:

- Dual-stack operation that enables the Polycom RealPresence Mobile application to connect to SIP or H.323 systems.
- H.264 encode and decode at up to 720p, 30fps.
- Support for Polycom Constant Clarity™ technology, such as Polycom® Siren™ Lost Packet Recovery, which can effectively improve the decreased audio quality caused by packet loss.
- Support for automatic gain control and echo cancellation.
- Ability to view network quality during a call.

Corrected Issues in Version 2.0

Category	Issue ID	Description
Audio	SWEP-1904	In a call on the Galaxy Tab 8.9" SHV-E140S tablet, the RealPresence Mobile application cannot detect audio through the speaker. You must use a headset.
Calling	CMAD-9743	On the XOOM with Android 4.1.1, the system crashes when you press the video mute button while connecting to an IP address.
Calling	CMAD-9748	On the XOOM with Android 4.1.1, the far end cannot receive video during a call.
Calling	CMAD-9383	When you place a point-to-point call from a RealPresence Mobile Android device to a RealPresence Desktop system in a RealPresence Access Director environment, the screen goes black.
Call Control	CMAD-9824	A RealPresence Mobile system cannot hang up a call before the call is set up.
SIP	CMAD-9828	A RealPresence Mobile system in an external network cannot answer a SIP call from an internal network.
Uesr Interface	CMAD-8330	SIP registration fails before SRV lookup returns the record.

Corrected Issues in Previous Versions

Version 1.3.1

Category	Issue ID	Description
Call Control	CMAD-9021	The RealPresence Mobile application failed to send a keep-alive message with TCP when switched from registering to an RFC 5626 server to a non-RFC 5626 server. This issue has been corrected.
Calling	CMAD-8550	The RealPresence Mobile application did not send an authentication update when the SIP server authentication valid time expired. This issue has been corrected.
CMA Provisioning	CMAD-9024	Endcall callStatsMessage content was not correct. The callStatus should be ENDED in endcall message, not ACTIVE. This issue has been corrected.
Interoperability	CMAD-8588	The RealPresence Mobile application did not support PLI. This issue has been corrected.
Interoperability	CMAD-8590	An external participant appeared on the participant list in a conference-managed screen when monitoring an ad-hoc point-to-point call from CMA Desktop to the RealPresence Mobile application or the RealPresence Mobile application to the RealPresence Mobile application. This issue has been corrected.
Installation	CMAD-8597	The RealPresence Mobile application could not be launched on the Motorola XOOM tablet with Android version 4.1. This issue has been corrected.
Installation	CMAD-8977	You could not launch the RealPresence Mobile application after installing Samsung P7510, Android version 4.0.4 on a tablet device. This issue has been corrected.

Version 1.3

Category	Issue ID	Description
Interoperability: Polycom HDX systems	CMAD-5331	When you were in an H.323 call with a Polycom HDX 8000 system using the call rate 512 kbps, your people video froze often after a Polycom Telepresence m100 application joined the call. This issue has been corrected.
Interoperability	CMAD-4417	When you attempted to leave a video voice message to a contact that also supported video voice messaging, the recorded message contained only audio (no video). This issue has been corrected.

Category	Issue ID	Description
Interoperability: Polycom HDX systems	CMAD-4361	When you placed SIP calls to a Polycom HDX system, local video was unavailable. This issue has been corrected.
Interoperability: Polycom m100	CMAD-4519	When you and a Polycom m100 application joined a multipoint call hosted by a Polycom HDX 9006 system, local video froze after you were in the call for around 10 minutes. This issue has been corrected.
Interoperability	CMAD-8591	RealPresence Mobile did not send an authentication update when the SIP server authentication valid time expired, which caused authentication failure and disconnected the call. This issue has been corrected.

Version 1.1

Category	Issue ID	Description
Calling	CMAD-4438	When you call a contact who is already in a call, you get the message 'Unreachable', instead of 'Busy'.
Calling	CMAD-4946	When you call a Polycom CMA Desktop system while your tablet is connected to a monitor using an HDMI cable, your screen turns black for a while after either you or the far end hangs up.
Calling	CMAD-4945	When you place a SIP call with a Polycom HDX 8000 system, your far-end video is displayed with the 4:3 aspect ratio, instead of 16:9.
Content	CMAD-5645	When you are in a multipoint call hosted through a bridge, if two far sites send you content in short succession, you may receive the second content in wrong aspect ratio.
User Interface	CMAD-4951	When you place a call to another XOOM 2 which is in a call with a Polycom RMX system, you receive the message 'Far end hangs up', instead of 'Busy MSG'.
Video	CMAD-4953	When you place an H.323 call to a bridge with 128 kbps as the call rate, the screen turns black for several seconds.
Video	CMAD-3571	In SIP calls hosted by a Polycom RMX1500 system, people video is not displayed. In H.323 calls, people video can be displayed after a three-minute delay.

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
Audio	SWEP-2636	On the Samsung Galaxy Tab 8.9" and ASUS Transformer Pad TF300T tablets, you cannot adjust speaker volume by using the hardware Volume control.	
Audio	CMAD-8563	Far end can hear echo of its own voice if the RealPresence Mobile Android device is in the same conference and does not mute. (HTC One S)	Use earphones.
Audio	CMAD-9416	Loudspeaker volume is too low to be heard during a call. (HTC smart phones)	Use a headset.
Audio/Video	SWEP-2757	No media are shown or heard in the HDX system when the RealPresence Mobile application calls H.323 B2B through a SIP trunk to the H.323 HDX system in the other enterprise.	
Calling	CMAD-8460	H.323 registration fails with notification Configuration error, but provision is successful.	Sign out and sign in again, or force stop the application.
Content	CMAD-6203	On Tegra 2-based tablets, when you view content shared in a call, if you switch back and forth between the content and people windows, or if the far end stops the content showing, sometimes you get a message saying that the application does not respond.	

Known Issues Category	Issue ID	Description	Workaround
General	SWEP-2677	In very rare conditions, there may be something wrong with the application UI (provision status is not right, sign-out button and call button are grayed out) because it was not stopped properly the last time. This issue might occur when you update the operating system or force stop the RealPresence Mobile application in Settings.	Reboot the device.
General	CMAD-5818	After you closed the Polycom RealPresence Mobile application by stopping the **LogService** and **MainService** from **Settings** > **Applications** > **Running Services**, if you then try to launch the application again, you get a message saying that the application has stopped unexpectedly.	Always follow these steps to force close the RealPresence Mobile application: **1** From your tablet, touch **Settings**. **2** Touch **Applications** > **Manage Applications**. **3** Touch **Video**. **4** Touch **Force Stop**, and touch **OK** to confirm.
Interoperability	SWEP-2756	You cannot log in to a Polycom CMA system or RealPresence Resource Manager system by using a non-English account name.	Use an English account name to log in.
Provisioning	CMAD-6209	When you are signed in to a Polycom CMA server through a WiFi network, if you then switch to another WiFi network and try to search in your corporate directory, it takes a long time before you see an error message about provisioning failure.	
SIP	CMAD-7896	On some devices, placing SIP calls over UDP (Default) and SIP over TLS work well. Placing SIP calls over TCP may fail. 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.	Use SIP over UDP (Default) or SIP over TLS.

Known Issues Category	Issue ID	Description	Workaround
Video	SWEP-2693	On Tegra 2-based tablets with Android 4.1 or later installed, the RealPresence Mobile application has no 1920K call rate available in the WLAN Call Rate settings, and cannot send 720p video with the rear camera.	
Video	CMAD-6364	On Tegra 2-based tablets, when you are in a call hosted by a Polycom RMX 4000 or RMX 2000 system that has no MPMX cards inserted, other participants cannot see your video.	

Supported Capabilities, Protocols, Algorithms, and Ports

Capabilities

Call Rate	Video Capability
1920 kbps (Tegra 2-based tablets only)	720p
1024 kbps (Tegra 2-based tablets only) 768 kbps (Tegra 2-based tablets only)	VGA
512 kbps 384 kbps 256 kbps	QVGA
64 kbps	Audio only

Protocols

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

Protocol	Description
H.239	People and Content
H.323, V6	Signaling
H.460	Firewall traversal
SIP (Session Initiation Protocol)	Signaling
BFCP (Binary Floor Control Protocol)	Content

H.239, BFCP, and H.460 are supported only when you are registered to a provisioning server.

Resolutions

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

Resolution and Frame Rate	Source
Up to VGA, 15 fps (Tegra 2-based tablets only) Up to QVGA, 15 fps (non-Tegra 2-based tablets and all Android phones)	People video sent from front camera
Up to HD/720p, 30 fps (Tegra 2-based tablets only) Up to QVGA, 15 fps (non-Tegra 2-based tablets and all Android phones)	People video sent from rear camera
Up to HD/720p, 30 fps (Tegra 2-based tablets only) Up to CIF (480x360), 30 fps (non-Tegra 2-based tablets and all Android phones)	People video received from far end
Up to 720p, 5 fps	Content received from far end

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.

480x352 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.

Algorithm Type	Description
Audio	G.722.1 Annex C G.711u G.711a Siren™ LPR Acoustic Echo Cancellation (AEC) Automatic Gain Control (AGC)
Video	H.264
Encryption	AES for H.323 calls TLS for SIP calls

AES encryption is available only when you are registered to a provisioning server.

TLS encryption is available only when you are registered to a provisioning server.

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 Signaling
1719 (UDP)	Registration, Admission, and Status (RAS)
3230 - 3237 (UDP)	Media (RTP/RTCP)
5060	SIP
5061 (TCP)	SIP TLS signaling

Outbound Ports

Port	Function
443 (TCP)	Provisioning, Monitoring, Help Files, HTTPS
389 (TCP)	LDAP
5060	SIP
1720 (TCP)	H.323 Signaling
1719 (UDP)	Registration, Admission, and Status (RAS)
3230 - 3237 (UDP)	Media (RTP/RTCP)
5061 (TCP)	SIP TLS signaling

Preparing 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:
Open the Terminal from your Mac computer.

1. Generate the private key *client.key*. For example:
   ```
   Mike-MacBook-Pro:~ root# openssl genrsa  -out client.key 1024
   ```
2. 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.
Email Address []:pp@pp.com  ---CSR info.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234            -----see [Note1]
An optional company name []:poly
```

Please write down the challenge password. You will need it later in the procedure.

3 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/, then 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 text filed under **Saved Request** text field, then click **Submit**.

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

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

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

5 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 2.

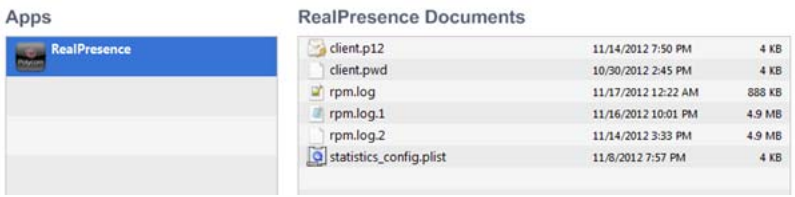
6 Encrypt the challenge password you set in Step 2:

   a Go to http://www.convertstring.com/EncodeDecode/Base64Encode.

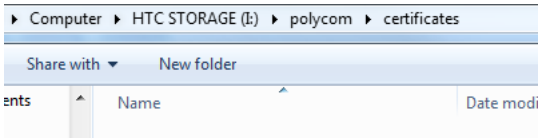
   b Enter the challenge password in the text field, and then click **Base64 Encode!**.

   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 CRL**.

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, 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.

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.

Polycom Notices

Copyright Information

Polycom, Inc.
6001 America Center Drive
San Jose, CA 95002
USA

Trademark Information

Patent Information