Release Notes

3.5.1 | April 2016 | 3725-82877-018A

Polycom® RealPresence® Mobile for Android®

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.

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. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

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 3.5.1

Polycom announces the 3.5.1 release of the Polycom® RealPresence® Mobile software. This release includes new devices and Android OS support, bug fixes, and feature enhancements.

Android Version 6.x Support

Polycom RealPresence Mobile application now supports Android version 6.x.

Constant Bitrate (CBR) Adopted for Video Codecs

From version 3.5.1, the RealPresence Mobile application changes its video codecs encoding from Variable Bitrate (VBR) to CBR. This provides better video quality.

About Polycom® Concierge Solution Support

Starting in version 3.5, the RealPresence Mobile application adds support to Polycom® Concierge Solution for Android phones.

However, please note that Polycom Concierge requires Polycom® RealPresence® Web Suite 2.1 with a RealPresence Web Suite Pro license. Do not enable any Polycom Concierge features unless your video conferencing environment includes RealPresence Web Suite Pro. RealPresence Web Suite 2.1 is targeted for release and available for purchase in the Q2 of 2016, but subject to change. Polycom reserves the right to modify future product plans at any time. Products and/o r related specifications are not guaranteed and will be delivered on a when and if available basis.

Release History

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

Version	Release Date	Features
3.5.1	April 2016	Android version 6.x support New devices support Constant Bitrate (CBR) adopted for video codecs Bug fixes and feature enhancements
3.5	January 2016	Polycom® Concierge Solution support for Android phones TLSv2 support Simplified Chinese UI support for Android phones and tablets New devices support
3.4.2	August 2015	Fixed a known Android security vulnerability.
3.4.1	July 2015	Support for Cloud Services
3.4	June 2015	Profile Photo and Virtual Business Card Feature Mid-string Search of Favorites Support for Polycom® NoiseBlock™ In-call Toolbar User Interface Enhancement Device Support Changes

3.3	January 2015	Support for BroadSoft Device Management as Provisioning Server
		User Interface Improvements
		Standalone mode provides more features. See System Capabilities and Constraints 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

Version	Release Date	Features
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

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.

RealPresence Mobile v3.5 and later Android version doesn't support Android OS versions 4.1.0 or earlier.

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	4.4.3		
LG	Optimus G pro LG-F240L Phone	4.1.2		
Samsung	Galaxy SIII GT-I9300 Phone	4.1.2		
	Galaxy Tab S 10.5	5.0.2		
	Galaxy Tab 4 10.1	4.4.2		
	Galaxy Tab 3 7” SM-T217A Tablet	4.2.2		
	Galaxy Tab 3 8” SM-T311 Tablet	4.2.2		
	Galaxy Tab Pro Tablet	4.4.2		
	Galaxy Tab S2 T710	5.0.0		
	Galaxy S4 GT-I9500 Phone	5.0.1		
	Galaxy S5 Phone	5.0.0		
	Galaxy S6 Phone	5.1.1		
	Galaxy Note 4 Phone	5.1.1		
	Galaxy Note 5 Phone	5.1.0		
	Galaxy Note 8.0 GT-N5100 tablet	4.1.2		
	Galaxy Note Pro 12.2	4.4.2		
	Galaxy S7 Edge	6.0.1		
HUAWEI	Nexus 6P	6.0.1		
SONY	Xperia ZL L35h Phone	4.4.2		
	Xperia Z SGP312 Tablet	4.2.2		

To view yourAndroid system version:

- » Tap **Settings** and then **About device** and then **Android Version**.

Polycom® CMA® System and Polycom® 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 with 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.

Type	Product	Version
Gatekeeper, Gateways, External MCU, Bridges, Call Managers	Polycom® Distributed Media Application™ (DMA®) 7000	6.2, 6.3
	Polycom® RealPresence® Resource Manager	8.4, 9.0
	Polycom® RealPresence® Collaboration Server (RMX®) 4000/2000	8.5, 8.6
	Polycom® RealPresence® Collaboration Server (RMX®) 1500	8.6
	Polycom® RealPresence® Collaboration Server (RMX®) 1800	8.5, 8.6
	Polycom® RealPresence® Collaboration Server (RMX®) 1000C	2.5.1
	Polycom® RealPresence® Media Suite	2.1, 2.5
	Broadsoft SIP Server	r21
	Polycom® RealPresence® Web Suite	2.0, 2.1
NAT/Firewall/Border Controller	ACME Packet Net-Net 3820	Firmware SCX6.3.0 MR-5 Patch 2
	Polycom® VBP® 5300-ST	11.2.23
	Polycom® VBP-E	11.2.23
	Polycom® RealPresence® Access Director™	4.1, 4.2
Endpoints	Polycom® HDX® Series	3.1.7, 3.1.9
	Polycom® RealPresence® Mobile	3.5, 3.5.1 (iOS) 3.5, 3.5.1 (Android)
	Polycom® VVX®	5.3.0
	Polycom® RealPresence® Desktop	3.5, 3.5.1 (Windows)
		3.5, 3.5.1 (Mac)
	Polycom® RealPresence® Group Series	5.0, 5.1
Other	Polycom® People+Content IP	1.3 (PC only)
	Broadsoft environment	r21

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 to find the current Polycom Supported Products matrix.

Install and Uninstall RealPresence Mobile

This section explains how to install and uninstall RealPresence Mobile.

To install the RealPresence Mobile application:

1. Go to the Google Play application, search for **Polycom** or **video conferencing** to find the RealPresence Mobile application.
2. Tap **Free** and then **OK** to accept permission. The application downloads and installs automatically.

RealPresence Mobile will consume one more license after upgrading from 3.0 or earlier version to version 3.1 or later versions.To release the old license, you must remove the old license manually or set the license reclaim cycle to be a small value (for example five minutes) on RealPresence Resource Manager.

To uninstall the RealPresence Mobile application:

1. Go to the device's application list, tap **Settings** and then **Applications** and then **Manage applications.**
2. Tap  **Video** and then **Uninstall**.
3. When you are prompted to confirm, tap **OK.** Your user data is deleted when you uninstall this application.

System Capabilities and Constraints

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

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.

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® Lost Packet Recovery™ (LPR™)	Lost Packet Recovery
SIP	Session Initiation Protocol

Resolutions

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

Resolution and Frame Rate	Source
Up to 720p, 15 fps	Video sent from camera
Up to 720p, 30 fps	Video received from far end

Resolution and Frame Rate	Source
Up to 720p (1280x720), 5 fps	Content received from far end
Up to 720p (1280x720), 5 fps (Tablets only)	Content showing from the tablets

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.

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.

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 Control (H.245)
3230 - 3250 (UDP)	Media (RTP/RTCP)

Port	Function
3238 (UDP and TCP)	BFCP
5060 (UPD and TCP)	SIP

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 Control (H.245)
3230 - 3250 (UDP)	Media (RTP/RTCP)
3238 (UDP and TCP)	BFCP

Known Issues

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

Issue ID	Description	Workaround
SWEP-9146	If you are using Samsung Note 4 phone with low battery, the frame rate of a 720 p call is around 7 fps, instead of 15 fps.	None.
SWEP-9040	If your RealPresence Mobile application runs over Android 6.0 OS, for example, on HUAWEI Nexus 6P device, sometimes, the application crashes.	None.
SWEP-8990	If you enabled SIP but didn't register to an SIP proxy server, you cannot place calls using your far end's IP address.	None.
SWEP-8960	You cannot share pictures or PDF files from the Dropbox application in SVC calls.	None. This is the designed behavior.
SWEP-8947	You cannot find the 1024 kbps call rate option if your RealPresence Mobile application runs over Android 6.0 OS.	None.
SWEP-8942	(HUAWEI Nexus device only) If you are using HUAWEI Nexus device, with loud speaker turned on and audio unmuted, your far ends hear an echo of their voice when they speak.	None.
SWEP-8747	Polycom RealPresence Mobile application V3.5 or later cannot register with a VBP server that is using a Diffie-Hellman (DH) key smaller than 768 bit.	Increase your VBP server DH key to 768 bit or above.
SWEP-8716	When you place an H.323 point-to-point call from the RealPresence Mobile application, the video protocol shown in the call statistics shows H264SVCHigh.	This is the designed behavior. To improve user experience in bad network environments, people and content video are both encoded as SVC/SVC high instead of H264/H264 high for H.323 point-to-point calls.
SWEP-8626	When you receive a PSTN call, you hear the call audio always from your device speaker.	None.
SWEP-8581	Occasionally, when the RealPresence Mobile application is left idle for a while, you are prompted "Video is stopped".	None.
SWEP-7978	If you adjust the speaker volume of your RealPresence Mobile application to 80% or lower, the volume is barely audible.	Use earphones or move to a quieter place.

Resolved Issues

The following table lists the resolved issues in this release.

Issue ID	Description
SWEP-9050	After upgrading the RealPresence Mobile application to version 3.5, you cannot switch to the Japanese keyboard to enter search phrases in Japanese. This is now fixed.

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 (RealPresence Mobile 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
	On the Galaxy Tab 10.1" LTE SC-01D tablet, the user cannot control mute the speaker on the device. (SWEP-7254).	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 RealPresence Collaboration Server (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 RealPresence Collaboration Server (RMX) **Content Settings** to **Graphics**, and **Content Protocol** to **H.263 & H.264 Auto Selection**. • Set the call rate on RealPresence Mobile 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 names and passwords to sign in a Polycom CMA server and RealPresence Resource Manager or register to a gatekeeper or an SIP server.	Use an English user name and password.
	If you use an MPM+ media card in a call with a RealPresence Collaboration Server (RMX) system, a blue edge is displayed at the bottom of the video window.	Use an MPMX media card with the RealPresence Collaboration Server (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 on the internet may fail to call Telepresence m100 on the 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.
	RealPresence Desktop SIP call transfers by VVX systems may fail when the endpoints are not registered with a RealPresence DMA system.	Register the endpoints.

Enterprise Scalable Video Coding (SVC) 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.

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 four remote participants plus one content-sharing frame, and one 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 RealPresence DMA

Using SVC conference calls has following limitations:

- Does not support recording
- Does not support 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 RealPresence 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.

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.
Content Rate	Rate your system uses in content transmission.

Value	Description
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 RealPresence 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
   ```
4. You are about to be asked to enter information that will be incorporated into your certificate request.

   Enter the Distinguished Name (DN) information that will be incorporated into your certificate request. You can leave some of the fields 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.
   ```
5. 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
   ```
6. 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**.

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

8 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.

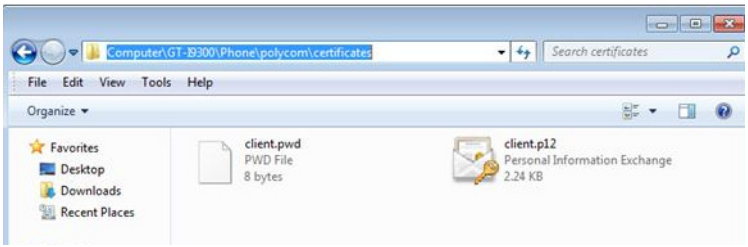
9 Encrypt the challenge password you set in Step 3:

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*.

10 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, 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.

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