RELEASE NOTES

Version 3.11.7 | September 2022 | 3725-82877-028A

Poly RealPresence Mobile for Android

Contents

What's New in This Release

Polycom RealPresence Mobile 3.11.7 is a maintenance release that includes bug fixes only.

Release History

This following table lists the release history of Poly RealPresence Mobile application.

Release History

Release	Release Date	Features
3.11.7	October 2022	Bug fixes
3.11.7	August 2022	Bug fixes
3.11.6	February 2022	Bug fixes
3.11.5	September 2021	Bug fixes
3.11.4	May 2021	Bug fixes
3.11.2	December 2020	Bug fixes
3.10.1	May 2019	New option for sharing customer information with Poly
3.10	April 2019	Support for clicking the URL of a new format that contains the user token to join a meeting Supports new devices Defect fixes
3.9.1	September 2018	Supports new devices Defect fixes
3.9	January 2018	Dropped support for automatic detection of Poly SmartPairing New device and OS support
3.8	September 2017	Support for receiving 1080p content Disable Remember Password feature Dropped support for Poly Concierge New device support
3.7	December 2016	Audio enhancement Video enhancements UI enhancements Support for Android device capability detection for 720p CallTo feature support Czech language support New device support New OS Support
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

Release	Release Date	Features
3.5	January 2016	Poly 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 Poly 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

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

Security Updates

Please refer to the Poly Security Center for information about known and resolved security vulnerabilities.

Hardware and Software Requirements

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

Manufacturer	Devices	Android Version	Network Requirements	Optional Peripheral Devices
Samsung	M Series, S Series, A Series, and Note Series devices that support Android 8 (Oreo) through Android 11.	8.0 - 11	Wireless Local Area Network (WLAN), 802.11 a/b/g/n. 3G or 4G network	3.5 mm headset Stereo Bluetooth headset
Google	Pixel devices that support Android 8 (Oreo) through Android 11.			
LG	Devices that support Android 8 (Oreo) through Android 11.			
Motorola	Devices that support Android 8 (Oreo) through Android 11.			
Realme	Realme XT			

Poly Clariti Manager System

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

Products Tested with This Release

The Poly RealPresence Mobile application is tested with other products. The following list isn't a complete inventory of compatible equipment. It indicates the products that have been tested for compatibility with this release.

Poly recommends that you upgrade your Poly devices with the latest software versions, as compatibility issues may already have been addressed by software updates. See the Current Poly Interoperability Matrix to match product and software versions.

Products Tested with This Release

Type	Product	Tested Versions
Gatekeeper, Gateways, External MCU, Bridges, Call Managers	Poly Clariti Core and Poly Clariti Edge	10.2.0.0-487888
	Poly Clariti Manager	10.10
	Poly RealPresence Collaboration Server 800s, Virtual Edition	8.10.0.4420
	Poly Clariti Relay	1.2.0_487520
Poly Endpoints	Poly RealPresence Desktop	Windows 10: 3.11.6 Mac 12.2.1: 3.11.6
	Poly RealPresence Mobile	Samsung Galaxy S9: Android 10 Samsung Galaxy Tab S6 lite: Android 11
	Poly Studio X30	3.7.1-354025
	Poly Clariti App	1.1

Install and Uninstall RealPresence Mobile

This section explains how to install and uninstall RealPresence Mobile.

The RealPresence Mobile user interface supports the following languages: English, Czech, Simplified Chinese, and Traditional Chinese.

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.

To uninstall the RealPresence Mobile application:

1. Go to the device's application list, tap **Settings** and then **App** 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 Constraints and Limitations

The following sections provide information on constraints and limitations when using Poly RealPresence Mobile application.

Capabilities

The following video capabilities are supported for RealPresence Mobile.

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
Poly 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
Up to 1080p, 15 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)
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

Resolved Issues

The following table lists the resolved issues in this release.

Issue #	Description
EN-230827	When you place a VMR call into Poly RealPresence Collaboration Server, the latter shows your **Display Name** as your E.164 or H.323 alias, instead of your **System Name**.
EN-219240	If you're using an unregistered RealPresence Mobile, the *url-ID* of H.323 calls via IP doesn't include domain name.
EN-225392	(V3.11.6 only) After you sign in to RealPresence Mobile and place the first call, if you end the call and then place another, the 2nd call gets stuck in the `Connecting` status.

Known Issues

The following table lists all known issues and suggested workarounds for Poly RealPresence Mobile application.

These release notes do not provide a complete listing of all known issues that are included in the software. Issues not expected to significantly impact customers with standard voice or video conferencing environments may not be included. In addition, the information in these release notes is provided as-is at the time of release and is subject to change without notice.

Known Issues

Issue ID	Description	Workaround
EN-129145	When SMB 2.0 is enabled on both of Clariti Manager and the Active Directory server, RealPresence Mobile may fail to connect to Clariti Manager if `SmbServerNameHardeningLevel` is not set to 0 on the Active Directory server.	Set `SmbServerNameHardeningLevel` to `0`.
EN-162035	During the enterprise user sign-in process, the application doesn't validate the IP format entered in the **Server** field.	None.
EN-200769	Some devices can't find the RealPresence Mobile phone application in the Google Play Store or can't install it. The error message is: **Your device is not compatible with this version**. The impacted devices include (but not limited to): Samsung Galaxy S21+ 5G, Samsung 21 Ultra 5g, Galaxy Note20, and Note20 5G models.	Download the RealPresence Mobile application from the Poly Online Support Center.
EN-206374	If you turn on or turn off the camera during a meeting, the call disconnects.	None.

Interoperability Issues

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

Interoperability Issues Related to the Android Versions and Devices

Description	Solution
Screen rotation doesn't work if Virtual Business Card is enabled on Android phones and tablets.	None.
If ACL is enabled on RealPresence Access Director, calls may fail due to provisioning data (configured by Clariti Manager) lost and timeout when Android phones or tablets enter the sleep mode.	None.
Google Pixel 3 and Samsung Galaxy Tab S4 fail in SIP registration over UDP.	Set the SIP registration over TCP.
As the RealPresence Mobile user, you cannot mute the speaker volume of some Android phones and tablets including Samsung Galaxy Note8 (SM-N950F), SHV-E140S, Galaxy S6 G9200, Galaxy Tab 2 (GT-P5100), Google Pixel, ASUS Transformer Pad (TF300T).	None.
The speaker's volume is a little low during a call on the following Samsung tablets: • Tab3 7" T217A • Tab3 8" T311	It is a limitation of the RealPresence Mobile application. Adjust the volume to the maximum on the tablets.
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.

Enterprise Scalable Video Coding (SVC) Solution

Limitation Type	Description	Solution
Limitations Related to Other Poly Products	If you create a Continuous Presence (CP) only conference call on Poly RealPresence Collaboration Server (RMX) 4000/2000 system and Poly RealPresence Collaboration Server 800s version 8.1 with default content settings (**Content Settings: HiResGraphics** and **Content Protocol: H.264 HD**), the RealPresence Mobile application can't 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.
	Poly VSX Visual Concert can't display 1024x576 content sent by RealPresence Mobile, whether or not they call each other directly.	Double-click the content to show the content in full screen, then RealPresence Mobile will send 1024x768 content, and the Poly VSX Visual Concert can display correctly.
	RealPresence Mobile may consume more than one license on Clariti Manager if you install and uninstall RealPresence Mobile several times.	Configure the reclaim period on Clariti Manager to a small value (for example five minutes).
	RealPresence Mobile supports only using English user names and password to sign in Poly CMA server and Clariti Manager, or to register to a gatekeeper or an SIP server.	Use English user name and password.
	In a motion mode conference, RealPresence Mobile receives video with a long 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.
	You may hear a short audio glitch on RealPresence Mobile when dialing in an SIP AVC encrypted conference created on the RealPresence Collaboration Server (RMX) 4000 with NGB.	None

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 **Statistics** . 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.
Content Rate Used	Actual bandwidth being used for the content transmission.
Content Frame Rate	Rate your system uses in content frame transmission.

Value	Description
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 Poly RealPresence DMA, CMA, or Clariti 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.

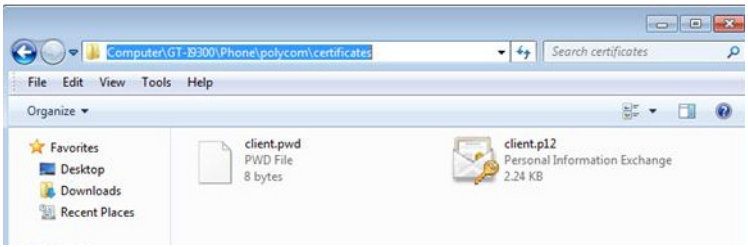
9 Encrypt the challenge password you set in Step 3:

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 Clariti Manager systems, these systems should also hold the CA root certificate and the system's certificates.

Get Help

For more information about installing, configuring, and administering Poly products or services, go to the Poly site, click Support, and choose the option best suited to your needs.

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Licensing & Product Registration, Self-Service, Account Management, Product-Related Legal Notices, and Documents & Software downloads.
- The Poly Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Poly Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The Poly Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration.

Copyright and Trademark Information

Plantronics, Inc. (Plantronics + Polycom, Now together as Poly)

345 Encinal Street

Santa Cruz, California

95060

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

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Poly up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Poly 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 Poly by email at OpenSourceVideo@Poly.com.

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

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