Remote Support

Android Customer Client 2.2.18

TC:2/1/2023

Table of Contents

Support Android Devices with BeyondTrust 3

What Your Customer Sees: The Android Customer Client 4

Start a Click-to-Chat Session on an Android Device 5

Download the BeyondTrust Support Client and BeyondTrust Jump Client Apps 7

Initiate an Android Support Session 8

Start a Session through the Support Portal 8

Enter a Session Key to Start an Android Support Session 9

Join a Support Session through Email 10

Use Jump Clients to Access Unattended Android Devices 11

How a Support Session Looks on an Android Device 13

Screen Sharing 13

Stream Video Using BeyondTrust InSight 13

The Android Device Support Session 15

Representative Console 15

Chat with the Android User During a Session 15

Screen Share with the Android Device 18

File Transfer To and From the Android Device 20

View the Android Device System Information 22

End the Android Support Session 24

Android Permissions Required by the Customer Client App 25

Support Android Devices with BeyondTrust

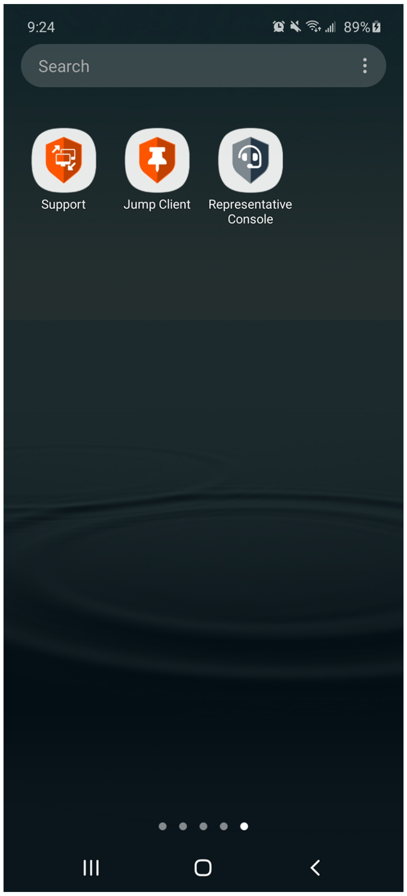
With BeyondTrust Remote Support, support representatives can help users of Android-powered devices resolve issues. This guide provides instructions for supporting Android devices through BeyondTrust Remote Support.

***Note:** BeyondTrust Android support is limited to phones, tablets, and Zebra devices. Other Android-powered devices are not certified or tested for compatibility.*

The minimum device requirement is Android version 6.0. Depending on the version and device implementation, some features may not be available, may require additional confirmation, or may appear slightly different from the screen shots in this manual.

When supporting devices, full screen sharing and control is possible. The remote user can also chat and share their device's screen in a view-only support session. The representative can transfer files to the remote device and view its system information.

Web-based click-to-chat is available on Android devices. Click-to-chat allows you to easily chat with the remote user without requiring them to download or run the BeyondTrust Remote Support client app. To use click-to-chat, the remote user must be using an up-to-date browser supported by BeyondTrust.



IMPORTANT!

To support Android devices, your B Series Appliance must be equipped with a valid SSL certificate signed by a certificate authority. Android devices will not accept a self-signed certificate when downloading the BeyondTrust customer client. Once you have applied a CA-signed SSL certificate to your B Series Appliance, contact BeyondTrust Technical Support. Your support representative will create a new software build that integrates your SSL certificate. With this updated build installed on your B Series Appliance, you can support Android devices.

App developers can use the BeyondTrust Embedded Mobile App Support SDK to embed BeyondTrust's remote support technology into Android applications. This allows you to support your mobile applications remotely by offering in-app remote screen viewing, custom special actions, custom system information, and file transfer to help resolve application or training issues your users are experiencing. The SDK is not covered in this document. If you develop your own apps and are interested in supporting those apps, contact your BeyondTrust Technical Support representative or submit a support request at www.beyondtrust.com/support.

What Your Customer Sees: The Android Customer Client

Customers on Android phones and tablets interact with support reps primarily through the BeyondTrust customer client application, called **BeyondTrust Support.**

They may also see prompts and messages in the context of the public site or support portal. This section details the customer-facing elements of a BeyondTrust remote support session on a mobile device.

For details on supporting other devices, including Apple iOS, please visit www.beyondtrust.com/docs/index.htm.

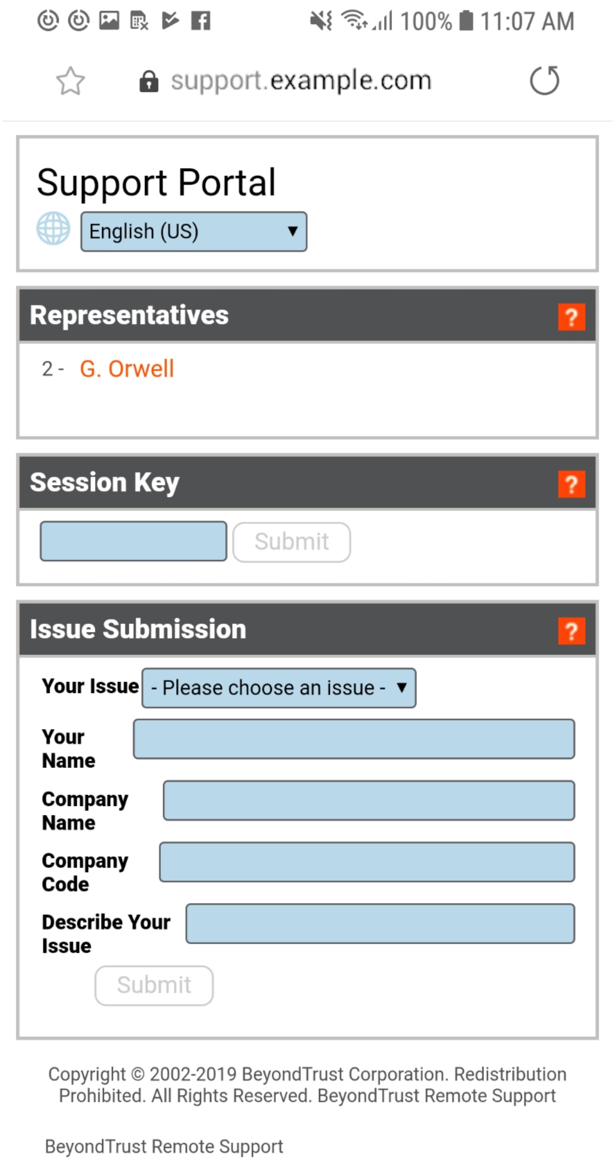
Start a Click-to-Chat Session on an Android Device

Users of Android mobile devices benefit from chatting with your professional support team. BeyondTrust enables you to start web-based click-to-chat support sessions with users on Android devices. You may begin this type of Android device support via a representative-initiated support invitation or from your BeyondTrust support portal.

Use Click-to-Chat for Web-Based Chat on an Android Device without a Download

To start a session with click-to-chat, your customer does not need to download the BeyondTrust customer client app. Instead, direct your customer to your public site. Your customer must use a modern browser supported by BeyondTrust.

For click-to-chat to be available, your administrator must have enabled the click-to-chat option for at least one of the session start methods available from your public site. Click-to-chat is enabled from **/login > Public Portals > Public Sites**.



100% 11:07 AM

support.example.com

Support Portal

English (US)

Representatives

2 - G. Orwell

Session Key

Submit

Issue Submission

Your Issue - Please choose an issue -

Your Name

Company Name

Company Code

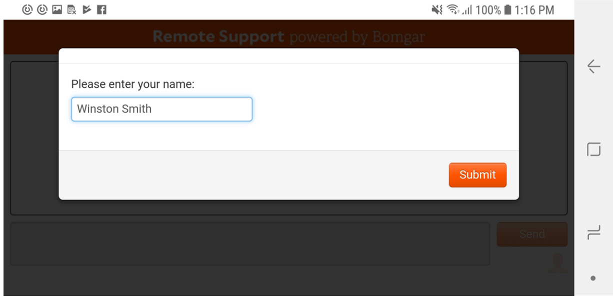
Describe Your Issue

Submit

Copyright © 2002-2019 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved. BeyondTrust Remote Support

BeyondTrust Remote Support

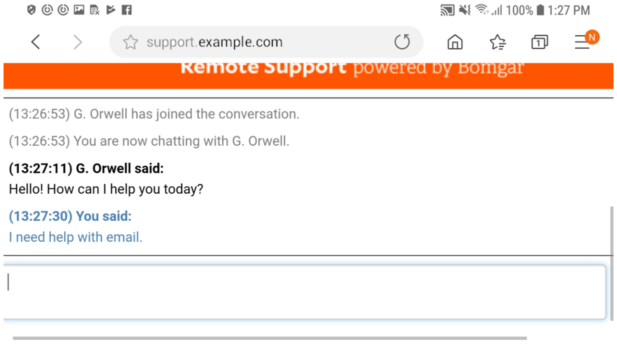
When your customer starts a session using a method that has click-to-chat enabled, a web-based chat session is initiated.



Please enter your name:

Winston Smith

After your customer enters their name, accepts the prompt to allow chat with a representative, and chooses to allow or refuse screen recording, a support request enters a queue in the representative console. Accept the session to chat with your customer.



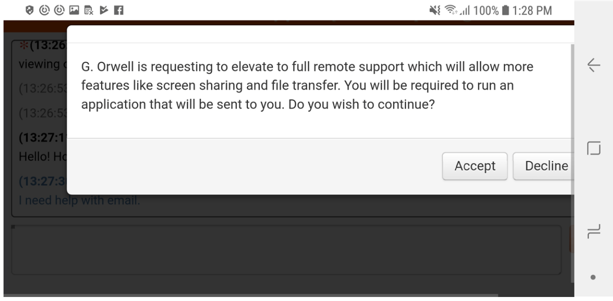
(13:26:53) G. Orwell has joined the conversation.

(13:26:53) You are now chatting with G. Orwell.

(13:27:11) G. Orwell said:
Hello! How can I help you today?

(13:27:30) You said:
I need help with email.

If you need to provide support at a level deeper than chat allows, you can request your customer to elevate to the BeyondTrust customer client app. Accepting the elevation request attempts to open the BeyondTrust customer client app. If the BeyondTrust app is already installed, the session will immediately become available. If the app needs to be downloaded, your customer is taken to Google Play to download the free BeyondTrust app. The session then continues as detailed in the next section of this guide.



G. Orwell is requesting to elevate to full remote support which will allow more features like screen sharing and file transfer. You will be required to run an application that will be sent to you. Do you wish to continue?

Note: *For Android 11 and later, file transfer is available only with the BeyondTrust Support+ Client app. This is available by logging into the BeyondTrust Customer Portal at https://www.beyondtrust.com/support.*

*The Support+ Client includes all the features of the Support Client. However, devices can have both clients installed. If both clients are installed, users must select **Support** or **Support+** when using a link to enter the support portal. Select **Support+** to enable file transfer.*

Download the BeyondTrust Support Client and BeyondTrust Jump Client Apps

To receive support, customers can download the BeyondTrust Support Client and BeyondTrust Jump Client apps for free from the Google Play Store.

1. Have the customer search in Google Play, from their Android device, for the BeyondTrust Support and BeyondTrust Jump Client. Select the application.
2. Alternately, customers can go directly to these links:
   - BeyondTrust Support at https://play.google.com/store/apps/details?id=com.bomgar.thinclient.android
   - BeyondTrust Jump Client at https://play.google.com/store/apps/details?id=com.bomgar.thinpin.android
3. Click Install.
4. Once the application has installed, the customer should open the application and accept the required permissions.

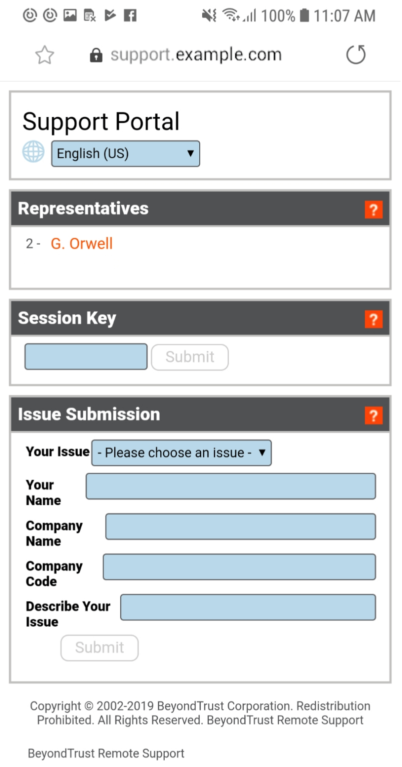
> ***Note:** For Android 11 and later, file transfer is available only with the BeyondTrust Support+ Client app. This is available by logging into the BeyondTrust Customer Portal at https://www.beyondtrust.com/support.*
>
> *The Support+ Client includes all the features of the Support Client. However, devices can have both clients installed. If both clients are installed, users must select **Support** or **Support+** when using a link to enter the support portal. Select **Support+** to enable file transfer.*

Initiate an Android Support Session

Users of Android mobile devices benefit from access to your professional support team. BeyondTrust enables you to support Android devices via a representative-initiated support invitation or from your BeyondTrust support portal.

Start a Session through the Support Portal

1. To initiate a support session, the customer must navigate to your organization's support portal, for example, support.example.com. From this page, the customer chooses how they wish to start the session. The options available on the page are determined by the permissions set within the /login administrative interface.
2. After a session start method has been chosen, the session starts.



100% 11:07 AM

support.example.com

Support Portal

English (US)

Representatives

2 - G. Orwell

Session Key

Submit

Issue Submission

Your Issue - Please choose an issue -

Your Name

Company Name

Company Code

Describe Your Issue

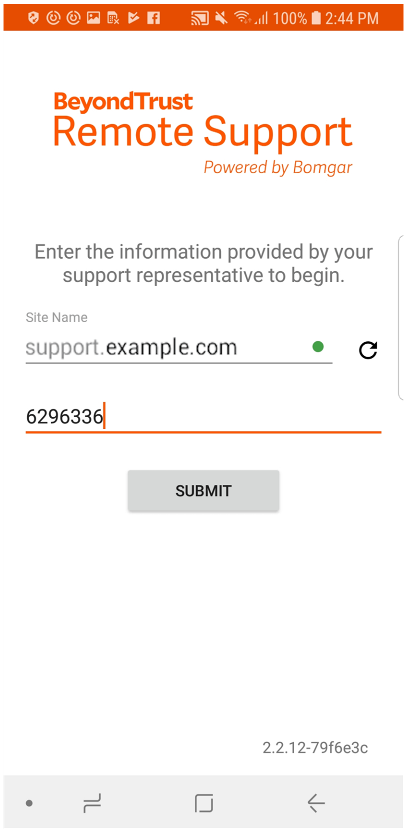
Submit

Copyright © 2002-2019 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved. BeyondTrust Remote Support

BeyondTrust Remote Support

Enter a Session Key to Start an Android Support Session

1. To start a session directly from the BeyondTrust Customer Client app, your customer must enter your support site address, which is automatically verified, along with a unique session key you have generated from the representative console. You can provide these values to the customer verbally, via email, or via SMS.
2. Once your customer clicks the **Submit** button, the connection is initiated. The customer may be prompted to accept an agreement and/or allow session recordings before joining the session.



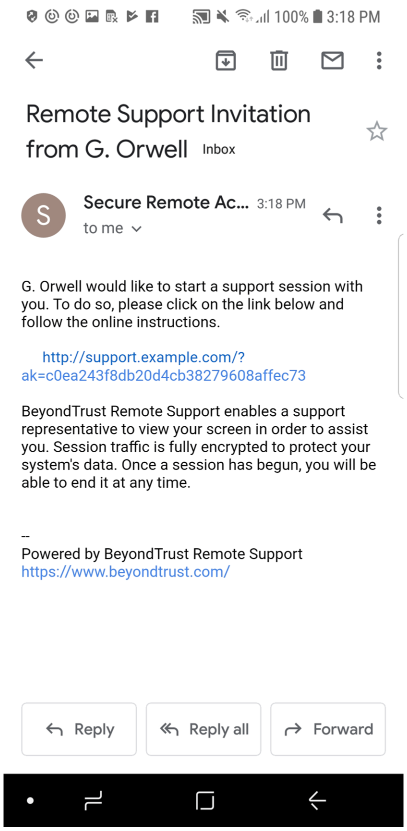
Enter the information provided by your support representative to begin.

Site Name: support.example.com

6296336

Join a Support Session through Email

1. You can send an email invitation from the representative console. The email contains an invitation to join a support session along with a unique session key URL.
2. After receiving the email invite, your customer must tap the link within the email. The link takes them to a page where they can choose to begin a session by tapping the **Start Session** button.
3. If the customer has the BeyondTrust Customer Client app installed on their Android device, they may tap **Start Session** to begin a session. However, if the customer does not have the app installed, the Google Play Store opens, allowing the customer to download the Customer Client app.



Remote Support Invitation from G. Orwell

Secure Remote Ac... 3:18 PM
to me

G. Orwell would like to start a support session with you. To do so, please click on the link below and follow the online instructions.

http://support.example.com/?ak=c0ea243f8db20d4cb38279608affec73

BeyondTrust Remote Support enables a support representative to view your screen in order to assist you. Session traffic is fully encrypted to protect your system's data. Once a session has begun, you will be able to end it at any time.

--
Powered by BeyondTrust Remote Support
https://www.beyondtrust.com/

Use Jump Clients to Access Unattended Android Devices

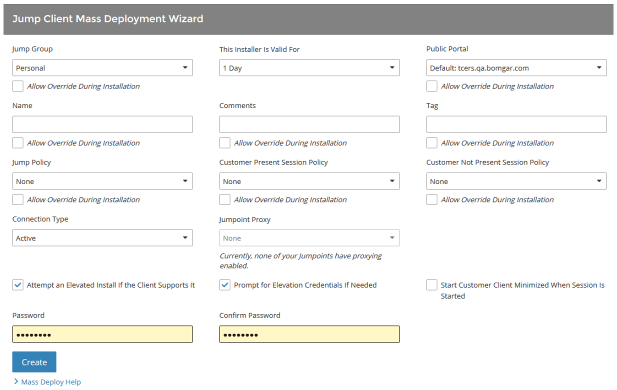
A persistent connection can be established with an Android device by pinning a Jump Client to the device. This provides the ability to have unattended support sessions with Android devices. You can deploy Jump Clients using the method below.

> ***Note:*** *Bandwidth usage and battery life are minimally affected by establishing a persistent connection.*
>
> *Persistent connections to an unattended Android device can occur only when the devices have both the* ***BeyondTrust Support Client App*** *and* ***BeyondTrust Jump Client App*** *installed from the Google Play Store. To learn more, please see* *Download the BeyondTrust Support Client and BeyondTrust Jump Client Apps* *at* *https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-download-app.htm*.

> ***Note:*** *Full screen sharing (capturing video of the device while the Support app is in the background) is supported only on Samsung and Zebra devices.*

Email a Link from the /login Interface

1. From the /login interface, navigate to **Jump > Jump Clients > Jump Client Mass Deployment Wizard**.
2. Complete the information needed for your Jump Client, such as **Jump Group**, **Name**, etc.
3. Click **Create**.



Jump Client Mass Deployment Wizard

Jump Group: Personal
□ Allow Override During Installation

This Installer Is Valid For: 1 Day

Public Portal: Default: tcers.qa.bomgar.com
□ Allow Override During Installation

Name:
□ Allow Override During Installation

Comments:
□ Allow Override During Installation

Tag:
□ Allow Override During Installation

Jump Policy: None
□ Allow Override During Installation

Customer Present Session Policy: None
□ Allow Override During Installation

Customer Not Present Session Policy: None
□ Allow Override During Installation

Connection Type: Active

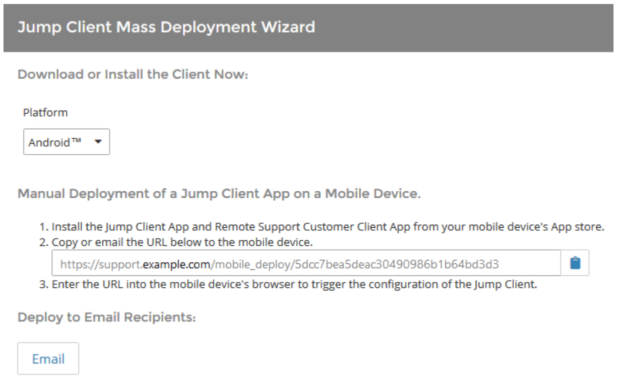
Jumpoint Proxy: None
Currently, none of your Jumpoints have proxying enabled.

☑ Attempt an Elevated Install If the Client Supports It
☑ Prompt for Elevation Credentials If Needed
□ Start Customer Client Minimized When Session Is Started

Password: ••••••••

Confirm Password: ••••••••

4. From the **Download or Install the Client Now** section, choose **Android** as your platform.
5. Verify that the **BeyondTrust Jump Client** app is installed on the Android device. If not, navigate to the Google Play Store to download the app.
6. To download the Jump Client to the device, open a browser on the Android device and go to the URL provided by the mass deployment wizard.
7. The application must be opened so that required permissions can be accepted.



Jump Client Mass Deployment Wizard

Download or Install the Client Now:

Platform: Android™

Manual Deployment of a Jump Client App on a Mobile Device.

1. Install the Jump Client App and Remote Support Customer Client App from your mobile device's App store.
2. Copy or email the URL below to the mobile device.
   https://support.example.com/mobile_deploy/5dcc7bea5deac30490986b1b64bd3d3
3. Enter the URL into the mobile device's browser to trigger the configuration of the Jump Client.

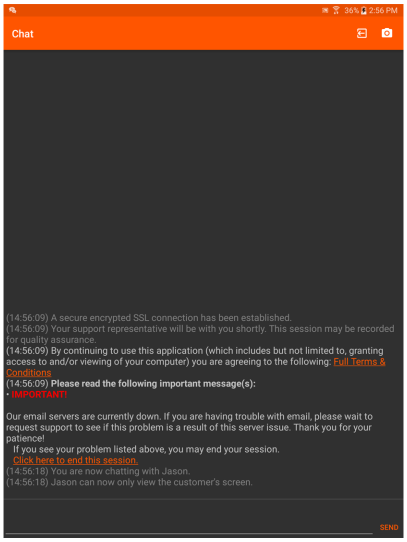
Deploy to Email Recipients:

Note: *You can also email the URL to the Android device by clicking on the* ***Email*** *link located in the* ***Deploy to Email Recipients*** *section.*

How a Support Session Looks on an Android Device

Once a session is established, the BeyondTrust chat interface opens, and a BeyondTrust indicator icon appears at the bottom of the device's display. While a session is running, the icon remains in the indicator area even if your customer is not in the BeyondTrust app itself.

You may continue to access files and system information while the customer is doing other things. If you send a chat message to the customer, the message will appear as a pop-up at the bottom of the device's screen.



(14:56:09) A secure encrypted SSL connection has been established.
(14:56:09) Your support representative will be with you shortly. This session may be recorded for quality assurance.
(14:56:09) By continuing to use this application (which includes but not limited to, granting access to and/or viewing of your computer) you are agreeing to the following: Full Terms & Conditions
(14:56:09) **Please read the following important message(s):**
- **IMPORTANT!**

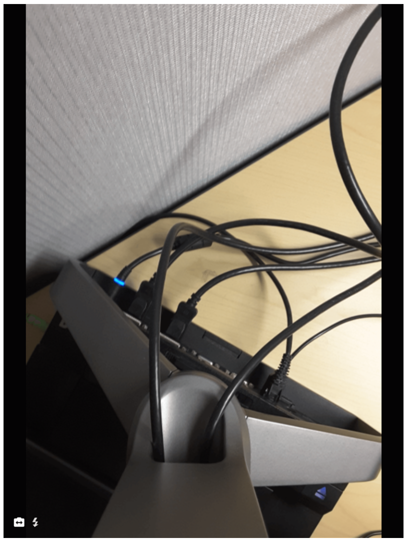
Our email servers are currently down. If you are having trouble with email, please wait to request support to see if this problem is a result of this server issue. Thank you for your patience!
If you see your problem listed above, you may end your session.
Click here to end this session.
(14:56:18) You are now chatting with Jason.
(14:56:18) Jason can now only view the customer's screen.

Screen Sharing

If you are in a screen sharing session, remember that any action the customer takes, such as entering passwords or accessing private information, can be seen by the representative and is recorded if session recording is turned on. To prevent private information being seen and recorded, you can stop screen sharing when the customer enters information and resume afterward.

Stream Video Using BeyondTrust InSight

By tapping on the **Camera** icon in the top right of the chat window, the customer can stream live video with VP9 technology to the representative from their mobile device. Sharing live video footage of a desktop, device, appliance, kiosk, etc. while an issue is taking place provides the representative with an additional way to assist the customer in finding a resolution to their problem.



To view the customer's live stream, the representative must first be screen sharing with the customer's device. Then, the customer must tap the **Camera** icon in the BeyondTrust customer client app. It is not possible for the representative to initiate BeyondTrust InSight within the Android customer client app.

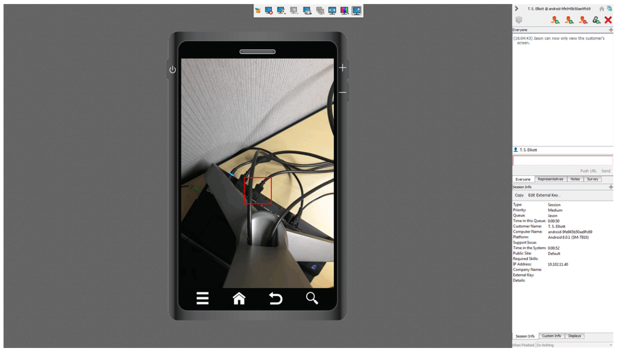
When the customer's screen appears in the representative console, the representative can select the video quality from the **Select Quality** dropdown.

***Note:** For best results, use the **More Colors** or **Full Color** quality options.*

While streaming, the customer can use the native Android camera controls to enhance the screen sharing experience. For example, the customer can switch between the front and rear cameras, turn on the camera's LED flash, and adjust the zoom level.

While viewing the footage, the representative can make annotations on a frame using the **Annotations** dropdown from the representative console. When the representative makes an annotation, the frame freezes, allowing the customer to view the annotation and take any necessary action. Once the representative clicks on the **Clear** option from the **Annotations** dropdown, the video begins streaming again.

***Note:** Annotations are not available in the web rep console or the mobile rep console.*



To end the session, the customer can tap the screen and then tap the **X** button that appears in the upper right corner of the screen, or they can tap the **Back** button. This prompts the end-user to confirm that they want to end the support session.

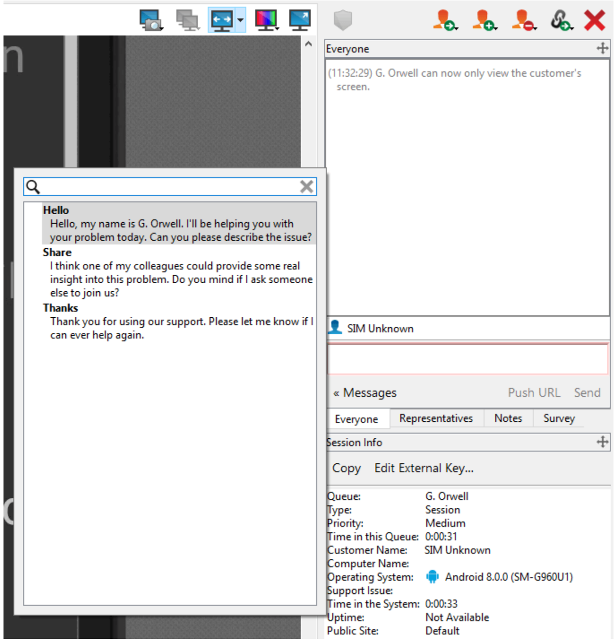
The Android Device Support Session

Representative Console

Once connected to a remote Android device through the representative console, you can chat with and support the customer, transfer files, and see Android device system information. If permission is granted by the customer, you can view and control the device.

Chat with the Android User During a Session

Throughout the support session, you can chat with your remote customer. You do not need to have screen sharing permissions before beginning a chat session. If you have uploaded your photo or any avatar image, it displays on the customer's chat window once the chat begins.



(11:32:29) G. Orwell can now only view the customer's screen.

Hello
Hello, my name is G. Orwell. I'll be helping you with your problem today. Can you please describe the issue?

Share
I think one of my colleagues could provide some real insight into this problem. Do you mind if I ask someone else to join us?

Thanks
Thank you for using our support. Please let me know if I can ever help again.

Queue:	G. Orwell
Type:	Session
Priority:	Medium
Time in this Queue:	0:00:31
Customer Name:	SIM Unknown
Computer Name:	
Operating System:	Android 8.0.0 (SM-G960U1)
Support Issue:	
Time in the System:	0:00:33
Uptime:	Not Available
Public Site:	Default

Click the arrow icon at the top left of the sidebar to collapse the sliding sidebar. If the sidebar is collapsed, hover over the arrow by the hidden window to reveal it. Click the pin icon that replaces the arrow icon at the top left of the sidebar to re-pin the sliding sidebar.

When typing in English, misspelled words are underlined in red. Right-click to view spelling suggestions or to ignore that spelling for the current console login.

If your administrator has configured canned messages, you can on the **Messages** button at the lower left of the chat input area to insert previously written messages into the chat. Click the arrow to the left of a category name to see its messages and subcategories. Type in the search box to find a specific message.

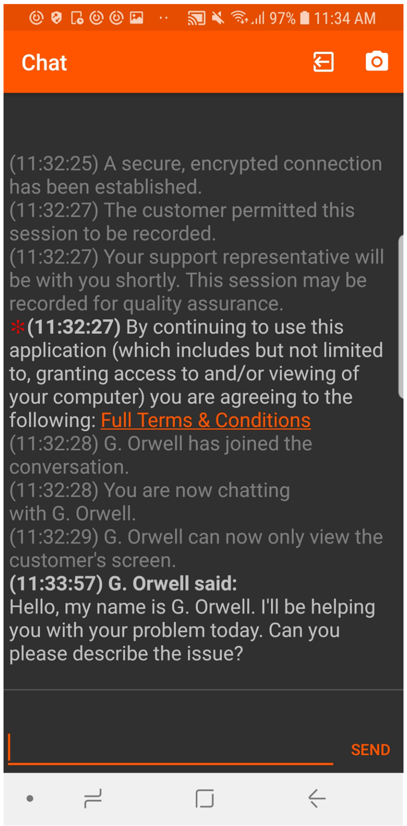
Messages appear as plain text in the chat input area. You can add or edit BBCode tags within a message to add text formatting. Formatting is applied when the message is sent.

The chat window records not only the messages and the time they are sent; it also serves as a running log of everything that happens throughout the session, including files transferred and permissions granted.

Pushing a URL through the chat interface automatically opens the designated site. Depending on the device, the site opens in the default browser or the **Web** view of the BeyondTrust support client. In order to push a URL, the web address must be the only text in the field.

You can also add notes about the session. If the session is shared or transferred, these notes can be submitted by one representative and pulled by another for a quick, private review of the situation. These notes are also available in the session report. Notes can be added both during the session and also after the remote connection has been terminated.

At the bottom right of the session window is information about the remote system along with any other information the customer may have provided in the issue submission form. This can include the following:



(11:32:25) A secure, encrypted connection has been established.
(11:32:27) The customer permitted this session to be recorded.
(11:32:27) Your support representative will be with you shortly. This session may be recorded for quality assurance.
***(11:32:27)** By continuing to use this application (which includes but not limited to, granting access to and/or viewing of your computer) you are agreeing to the following: Full Terms & Conditions
(11:32:28) G. Orwell has joined the conversation.
(11:32:28) You are now chatting with G. Orwell.
(11:32:29) G. Orwell can now only view the customer's screen.
(11:33:57) G. Orwell said:
Hello, my name is G. Orwell. I'll be helping you with your problem today. Can you please describe the issue?

- **Type**: The session type.
- **Priority**: The priority level (Low, Medium (default), or High) of the request, depending on the support issues defined by your BeyondTrust administrator.
- **Queue**: The Personal queue of the representative who owns the session.
- **Session Status**: Waiting (no rep has joined), In Progress (rep and customer have joined), or Customer Absent (rep has joined but customer has left).
- **Customer Name**: This is either the name entered by the customer when starting the session, the username of the logged-in user, the hostname of the customer machine (for pushed and pinned sessions), or service (for elevated sessions).
- **Computer Name**: The hostname of the customer's machine as reported in System Settings.
- **Platform**: The operating system of the customer’s machine
- **Support Issue**: If an issue was selected, this reports the name of the issue the customer selected.
- **Time in the System**: This tracks the amount of time from the moment the session entered its first queue.
- **Public Site**: Typically, this is listed as Default; however, if non-default sites are present, other sites may be available.
- **Required Skills**: Skills associated with the specific issue selected by the customer. Skills are created and associated with issues by the BeyondTrust administrator from the BeyondTrust /login interface.
- **IP Address**: The public and/or private IP address of the customer’s local system.

If your administrator has enabled the XML API, you may designate an external key for use in session reports. Any custom session attributes enabled by your administrator will appear in a **Custom Info** tab. Click **Copy** to copy all information to your clipboard.

You may continue to access files and system information while the customer is doing other things. If you send a chat message to the customer, the message appears as a pop-up at the bottom of the device's screen.

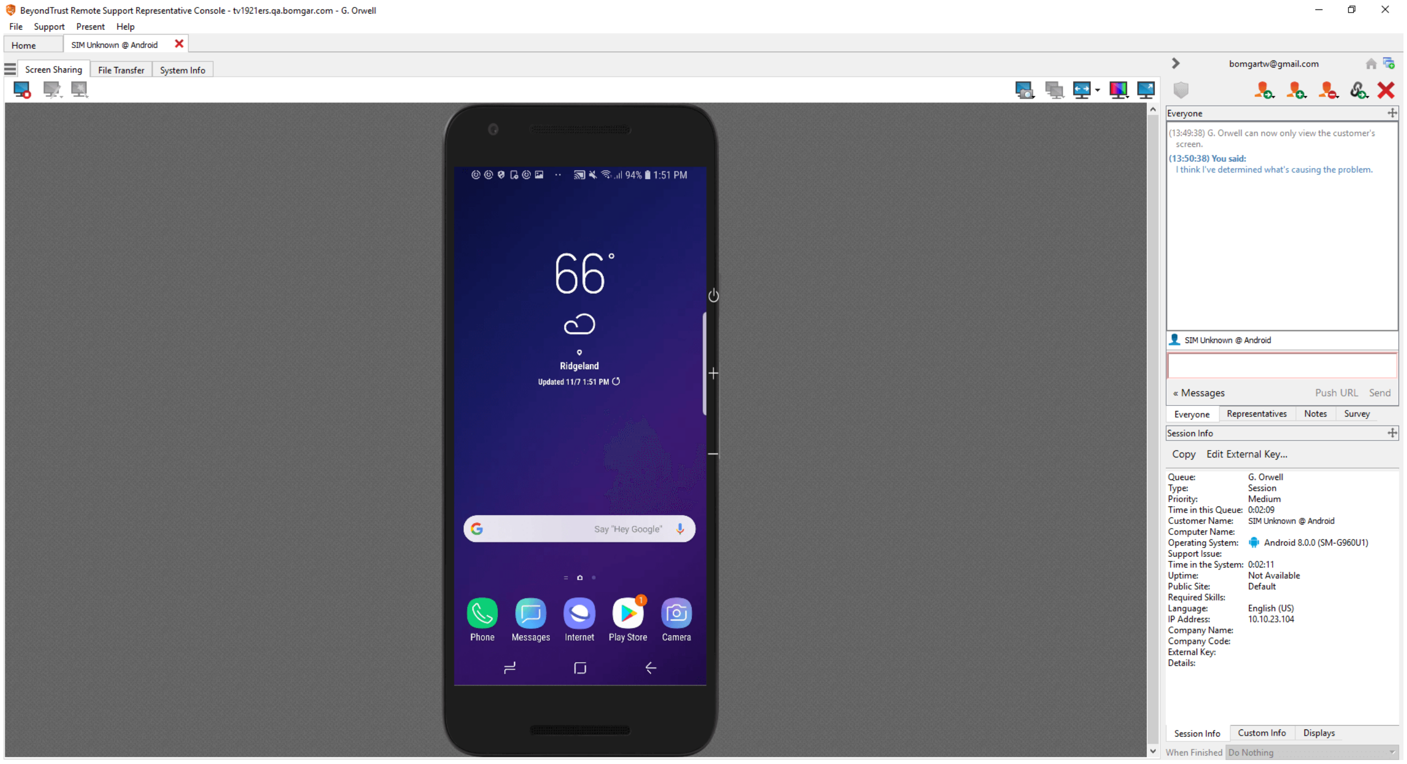
If you are in a screen sharing session, remember that any action the customer takes, such as entering passwords or accessing private information, can be seen by the representative and is recorded if session recording is turned on. To prevent private information being seen and recorded, you can stop screen sharing when the customer enters information and resume afterward.

Screen Share with the Android Device

From the session window, click the **Screen Sharing** button to request to view the remote device. Once the customer has granted permission, the remote device appears in your window.

To begin screen sharing, customers may need to accept a unique system prompt. View-only screen sharing allows no control of the device and restricts the representative to a limited set of support tools.

Your customer can choose to grant you view-only access or, if your permissions allow, full control of the pointer and keyboard, enabling you to work on the remote device as if you were physically present. You can request to elevate your permission level at any time during the session. The screen sharing tool bar provides a number of helpful features for support representatives.



(13:49:38) G. Orwell can now only view the customer's screen.

(13:50:38) You said:
I think I've determined what's causing the problem.

SIM Unknown @ Android

Queue:	G. Orwell
Type:	Session
Priority:	Medium
Time in this Queue:	0:02:09
Customer Name:	SIM Unknown @ Android
Computer Name:	
Operating System:	Android 8.0.0 (SM-G960U1)
Support Issue:	
Time in the System:	0:02:11
Uptime:	Not Available
Public Site:	Default
Required Skills:	
Language:	English (US)
IP Address:	10.10.23.104
Company Name:	
Company Code:	
External Key:	
Details:	

> ***Note:*** *Full screen sharing (capturing video of the device while the Support app is in the background) is supported only on Samsung and Zebra devices.*

Screen-sharing Tools

	Stop screen sharing.
	While viewing your customer's device, request or stop control of your customer's keyboard and pointer.

📷	While screen sharing, capture a screenshot of the remote screen or screens at their full resolution, saved in PNG format. Save the image file to your local system or to your clipboard. The capture action is recorded in the chat log with a link to a locally saved image. The link remains active even after the customer has left the session, but it does not persist in the BeyondTrust session report. You can adjust the directory where screenshots are saved by going to the **File > Settings > Support Tools** menu in the representative console. This feature works on Mac, Windows, and Linux.
↔	View the remote screen at actual or scaled size.
🌈	Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select **Video Optimized**; otherwise select between **Black and White** (uses less bandwidth), **Few Colors**, **More Colors**, or **Full Color** (uses more bandwidth). Both **Video Optimized** and **Full Color** modes allow you to view the actual desktop wallpaper.
⤢	View the remote desktop in full screen mode or return to the interface view.

File Transfer To and From the Android Device

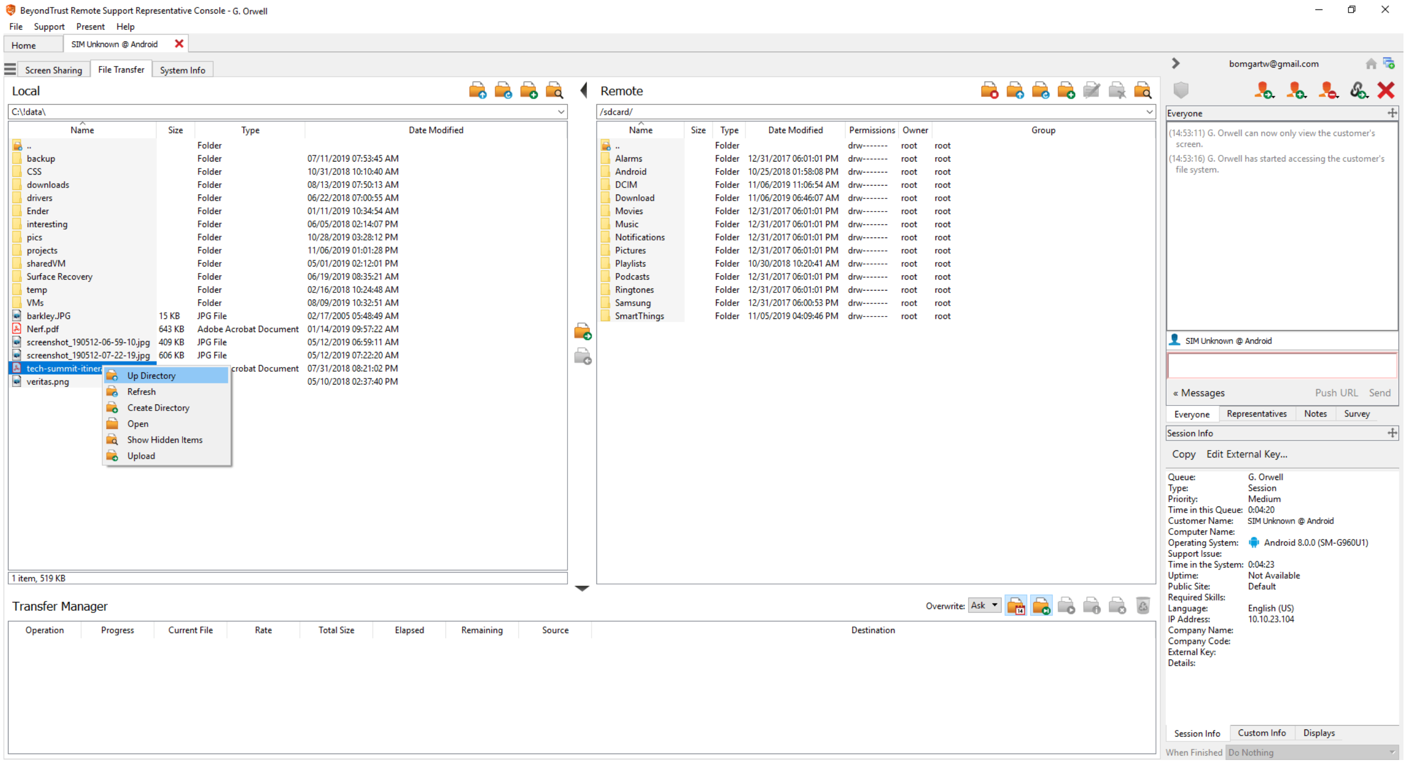
> ***Note:*** *For Android 11 and later, file transfer is available only with the BeyondTrust Support+ Client app. This is available by logging into the BeyondTrust Customer Portal at https://www.beyondtrust.com/support.*
>
> *The Support+ Client includes all the features of the Support Client. However, devices can have both clients installed. If both clients are installed, users must select **Support** or **Support+** when using a link to enter the support portal. Select **Support+** to enable file transfer.*

During a session, representatives with appropriate privileges can transfer files and directories to and from the remote device, with read privileges for the Android file system and read/write privileges on the SD card. You do not require full control of the customer's device in order to transfer files.

> ***Note:*** *Newer versions of the Android OS restrict access to some file paths.*

Depending upon the permissions your administrator has set for your account, you may be allowed only to upload files to the remote system or to download files to your local computer. File system access may also be restricted to certain paths on the remote or local system, thereby enforcing that uploads or downloads occur only in certain directories.

Transfer files by using the upload and download buttons or by dragging and dropping files. Right clicking on a file brings up a context sensitive menu from where you can, among other things, create a new directory; rename, open, or delete the file; or download it directly to your machine.



C:\!data\

Name	Size	Type	Date Modified
..		Folder	
backup		Folder	07/11/2019 07:53:45 AM
CSS		Folder	10/31/2018 10:10:40 AM
downloads		Folder	08/13/2019 07:50:13 AM
drivers		Folder	06/22/2018 07:00:55 AM
Ender		Folder	01/11/2019 10:34:54 AM
interesting		Folder	06/05/2018 02:14:07 PM
pics		Folder	10/28/2019 03:28:12 PM
projects		Folder	11/06/2019 01:01:28 PM
sharedVM		Folder	05/01/2019 02:12:01 PM
Surface Recovery		Folder	06/19/2019 08:35:21 AM
temp		Folder	02/16/2018 10:24:48 AM
VMs		Folder	08/09/2019 10:32:51 AM
barkley.JPG	15 KB	JPG File	02/17/2005 05:48:49 AM
Nerf.pdf	643 KB	Adobe Acrobat Document	01/14/2019 09:57:22 AM
screenshot_190512-06-59-10.jpg	409 KB	JPG File	05/12/2019 06:59:11 AM
screenshot_190512-07-22-19.jpg	606 KB	JPG File	05/12/2019 07:22:20 AM
tech-summit-itiner		crobat Document	07/31/2018 08:21:02 PM
veritas.png			05/10/2018 02:37:40 PM

1 item, 519 KB

/sdcard/

Name	Size	Type	Date Modified	Permissions	Owner	Group
..		Folder		drw-------	root	root
Alarms		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Android		Folder	10/25/2018 01:58:08 PM	drw-------	root	root
DCIM		Folder	11/06/2019 11:06:54 AM	drw-------	root	root
Download		Folder	11/06/2019 06:46:07 AM	drw-------	root	root
Movies		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Music		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Notifications		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Pictures		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Playlists		Folder	10/30/2018 10:20:41 AM	drw-------	root	root
Podcasts		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Ringtones		Folder	12/31/2017 06:01:01 PM	drw-------	root	root
Samsung		Folder	12/31/2017 06:00:53 PM	drw-------	root	root
SmartThings		Folder	11/05/2019 04:09:46 PM	drw-------	root	root

(14:53:11) G. Orwell can now only view the customer's screen.

(14:53:16) G. Orwell has started accessing the customer's file system.

SIM Unknown @ Android

Queue:	G. Orwell
Type:	Session
Priority:	Medium
Time in this Queue:	0:04:20
Customer Name:	SIM Unknown @ Android
Computer Name:	
Operating System:	Android 8.0.0 (SM-G960U1)
Support Issue:	
Time in the System:	0:04:23
Uptime:	Not Available
Public Site:	Default
Required Skills:	
Language:	English (US)
IP Address:	10.10.23.104
Company Name:	
Company Code:	
External Key:	
Details:	

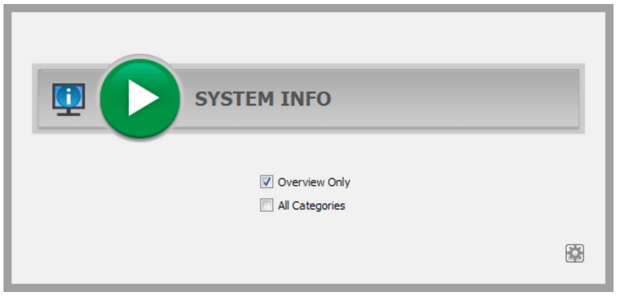
File Transfer Tools

	Stop access to the remote device's file system when it is no longer needed.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Create a new directory.
	Rename a directory or file.
	Delete a directory or file. Note that deleting a file or folder permanently deletes it. It is not sent to the recycle bin.
	Show hidden files.
	Select one or more files or directories and then click the appropriate button to upload the files to the remote system or download to your local system. You can also drag and drop files to transfer.
Ask ▾	If a file of the same name already exists in the location to which you are attempting to transfer a file, choose whether to respond by automatically overwriting the existing file, canceling the transfer, or prompting for each file of identical name. Note that if the content of the files is identical, the upload will be skipped and will result in a warning message.
14	Preserving file information will keep the file's original timestamp. If this option is disabled, the file's timestamp will reflect the date and time when it was transferred.
	If automatic file transfer is enabled, transfers will begin as soon as the upload or download button is clicked or a file is dragged from one file system to the other.
	If automatic file transfer is not enabled, select from the transfer manager the files you wish to transfer and then click the **Start** button to begin the transfer.
	From the transfer manager, select a file and then click the **Details** button to view information such as the date and time of the transfer, the origin and destination of the files, and the number of bytes transferred.
	Select one or more files from the transfer manager and then click **Cancel** to stop the transfer from completing.
	Clear all information from the transfer manager.

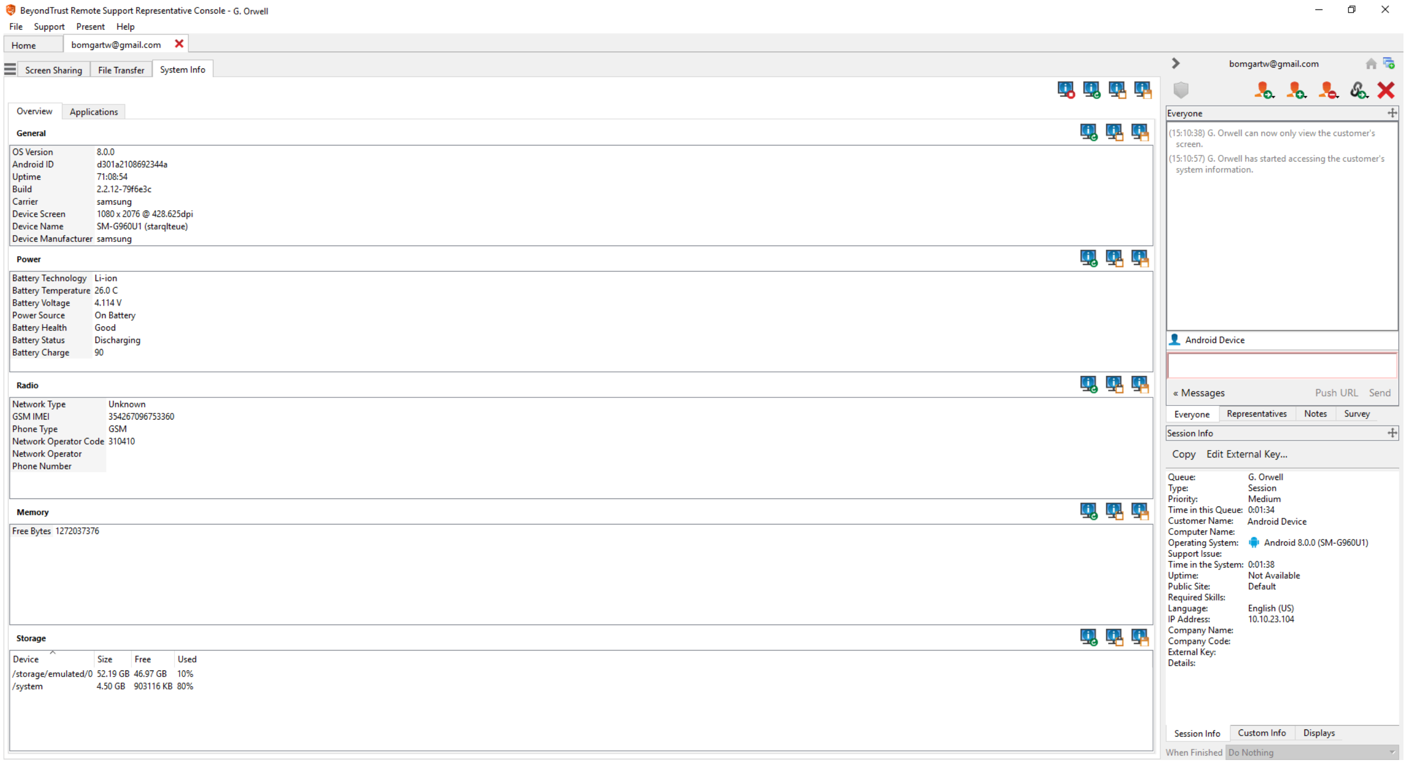
View the Android Device System Information

Privileged users may view a complete snapshot of the remote device's or computer's system information to reduce the time needed to diagnose and resolve the issue. The system information available varies depending on the remote operating system and configuration. Representatives with appropriate permissions may also kill processes and uninstall apps.

Because the large amount of data that can be pulled may result in slow transmission times, you can choose to start your view with only the **Overview** tab or to pull data for all tabs. If you choose to start with **Overview Only**, you can gather data from the other tabs by going to the section you need to view and clicking the **Refresh** button at the top of that section.



☑ Overview Only
□ All Categories



General

OS Version	8.0.0
Android ID	d301a2108692344a
Uptime	71:08:54
Build	2.2.12-79f6e3c
Carrier	samsung
Device Screen	1080 x 2076 @ 428.625dpi
Device Name	SM-G960U1 (starqlteue)
Device Manufacturer	samsung

Power

Battery Technology	Li-ion
Battery Temperature	26.0 C
Battery Voltage	4.114 V
Power Source	On Battery
Battery Health	Good
Battery Status	Discharging
Battery Charge	90

Radio

Network Type	Unknown
GSM IMEI	354267096753360
Phone Type	GSM
Network Operator Code	310410
Network Operator	
Phone Number	

Memory

Free Bytes	1272037376

Storage

Device	Size	Free	Used
/storage/emulated/0	52.19 GB	46.97 GB	10%
/system	4.50 GB	903116 KB	80%

(15:10:38) G. Orwell can now only view the customer's screen.

(15:10:57) G. Orwell has started accessing the customer's system information.

Queue:	G. Orwell
Type:	Session
Priority:	Medium
Time in this Queue:	0:01:34
Customer Name:	Android Device
Computer Name:	
Operating System:	Android 8.0.0 (SM-G960U1)
Support Issue:	
Time in the System:	0:01:38
Uptime:	Not Available
Public Site:	Default
Required Skills:	
Language:	English (US)
IP Address:	10.10.23.104
Company Name:	
Company Code:	
External Key:	
Details:	

When Finished: Do Nothing

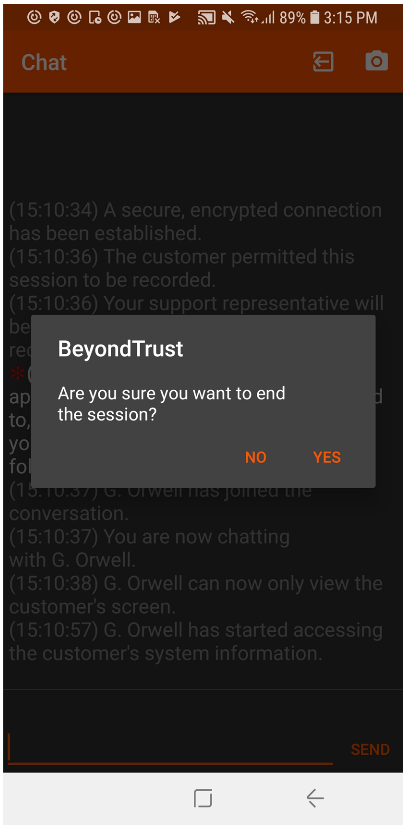
System Information Tools

	Stop pulling information about the remote system. Stopping will leave the last updated information available to view but will not pull current data.
	Refresh your view of system information or pull information for tabs to which you did not initially request access. Refresh can take place for individual sections or for all sections of the selected tab.
	Auto-refresh a category of system information.
	Copy the information to your clipboard. Copy individual sections or all sections of the selected tab.
	Save a text file of the system information to your local computer. You can save individual sections or all sections of the selected tab.
	End a running process on the remote system.
	Uninstall an app on the remote system.

End the Android Support Session

To end the session, your customer can tap the **Back** button. This prompts the user to confirm that they want to end the support session.

When the session is ended by either the customer or the representative, an alert will notify the customer that the representative can no longer access their device. The BeyondTrust support client app does remain installed after the termination of a support session so that if the customer needs support at a later time, the BeyondTrust app does not need to be reinstalled.

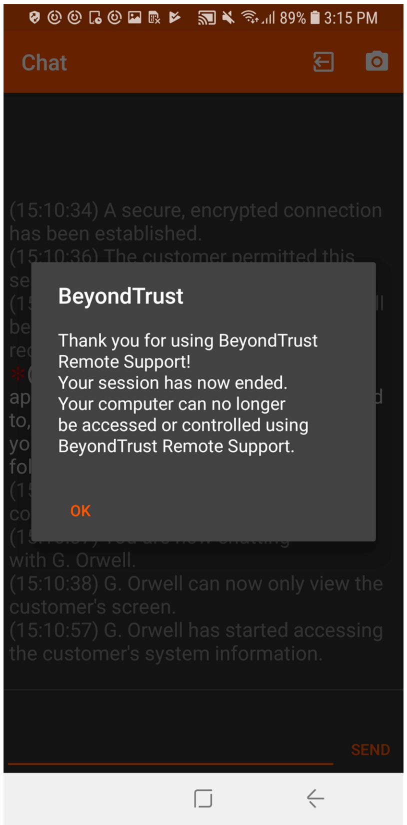


(15:10:34) A secure, encrypted connection has been established.
(15:10:36) The customer permitted this session to be recorded.
(15:10:36) Your support representative will

BeyondTrust

Are you sure you want to end the session?

(15:10:37) G. Orwell has joined the conversation.
(15:10:37) You are now chatting with G. Orwell.
(15:10:38) G. Orwell can now only view the customer's screen.
(15:10:57) G. Orwell has started accessing the customer's system information.



(15:10:34) A secure, encrypted connection has been established.

BeyondTrust

Thank you for using BeyondTrust Remote Support!
Your session has now ended.
Your computer can no longer be accessed or controlled using BeyondTrust Remote Support.

with G. Orwell.
(15:10:38) G. Orwell can now only view the customer's screen.
(15:10:57) G. Orwell has started accessing the customer's system information.

Android Permissions Required by the Customer Client App

The Android customer client for BeyondTrust requests a series of permissions during installation. The client prompts for certain permissions upon installing, but others are requested only when needed. Google Play lists the permissions used by apps, including the BeyondTrust Android customer client, but this list of permissions may not provide a satisfactory level of detail for all users. The following table offers a list of all permissions, as well as an explanation for each one.

API Permission Name	Permission Definition	Permission Explanation
android.permission. ACCESS_SURFACE_ FLINGER	Allows an application to use SurfaceFlinger's (involved with the display frame processor) low level features.	The representative may request screen sharing of the device's screen in order to provide more efficient support. This permission is necessary for the app to share the device's screen to the representative console.
android.permission.KILL_BACKGROUND_ PROCESSES	Allows an application to call killBackgroundProcesses (String).	A representative that is viewing the device's screen, may wish to perform actions on behalf of the user, such as keystrokes or touch events, in order to provide more efficient support. This permission is necessary for that functionality to work.
android.permission.GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.	The app uses this permission in an effort to find the device user's name when the support session is presented to a representative. Previous versions of the app used the phone number, but that is not as user-friendly or as personal. Given that the user name could be stored in multiple locations, the app first attempts to locate it in the **You** contact; if unsuccessful it looks for a Google account on the device. If finding the user's name is not possible, the app will look at the SIM card and attempt to gather some generic information about the device (this happens only when dealing with non-consumer devices).
android.permission.READ_CONTACTS	Allows an application to read the user's contacts data.	The app uses this permission in an effort to find the device user's name when the support session is presented to a representative. Previous versions of the app used the phone number, but that is not as user-friendly or as personal. Given that the user name could be stored in multiple locations, the app first attempts to locate it in the **You** contact; if unsuccessful it looks for a Google account on the device. If finding the user's name is not possible, the app will look at the SIM card and attempt to gather some generic information about the device (this happens only when dealing with non-consumer devices).
android.permission.INTERNET	Allows applications to open network sockets.	The app connects to a B Series Appliance in order to receive all requests from the technical representative and to send data such as chat messages, screen sharing updates, file transfers, and system information.

API Permission Name	Permission Definition	Permission Explanation
android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.	The representative can request the app to write data to the user's SD card as a way of sharing data files and applications that the user may need.
android.permission.INJECT_EVENTS	Allows the app to deliver its own input events (key presses, etc.) to other apps.	A representative that is viewing the device's screen may wish to perform actions on behalf of the user, such as keystrokes or touch events, in order to provide more efficient support. This permission is necessary for that functionality to work.
android.permission.WAKE_LOCK	Allows using PowerManager WakeLocks to keep the processor from sleeping or the screen from dimming.	Since the app keeps a constant connection to the B Series Appliance during a session and the user may be requested to respond to a chat message from the representative, the app requests a wake lock during the session to keep the device from going to sleep.
android.permission.READ_FRAME_BUFFER	Allows an application to take screen shots and more generally get access to the frame buffer data.	The representative may request screen sharing of the device's screen in order to provide more efficient support. This permission is necessary for the app to share the device's screen to the representative console.
android.permission.READ_PHONE_STATE	Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.	The app, upon the representative requesting it, will gather some system information including the phone state and transfer the data to the representative console so that the representative can better access the issue of the customer.
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage.	The app, upon the representative requesting it, can read data from the user's SD card as a way of capturing device and application data and logs that may be needed to diagnose issues.
android.permission.READ_PROFILE	Allows an application to access the device user's personally-identifying data.	The app uses this permission in an effort to find the device user's name when the support session is presented to a representative. Previous versions of the app used the phone number, but that is not as user-friendly or as personal. Given that the user name could be stored in multiple locations, the app first attempts to locate it in the **You** contact; if unsuccessful it looks for a Google account on the device. If finding the user's name is not possible, the app will look at the SIM card and attempt to gather some generic information about the device (this happens only when dealing with non-consumer devices).
android.permission.CAMERA	Required to be able to access the device's camera.	The representative may request remote camera sharing and video annotations using BeyondTrust InSight. This permission is required to perform this functionality.

API Permission Name	Permission Definition	Permission Explanation
android.permission.ACCESS_NETWORK_STATE	Allows applications to access information about networks.	The app shows a specific error message if the user attempts to connect to a B Series Appliance and the Wi-Fi and mobile data connectivity are disabled. This permission is required to perform this functionality.
android.permission.FOREGROUND_SERVICE	Starting with Android 9.0, this permission gives the application a higher priority for system resources and enforces that the app creates a notification while the service is in use.	The app uses this permission while it is connected to a B Series Appliance to ensure that the connection is consistently maintained by the host operating system. Without this permission, the app could be ended at any time by the host operating system, leading to service interruptions.
android.permission.CAPTURE_VIDEO_OUTPUT	This permission is used to capture the screen on older versions of Android. It requires special levels of access and is usually only allowed on 3rd party devices such as Samsung and Zebra devices.	The app uses this permission on certain devices to allow it to capture the screen for use in remote support sessions. Without it, the representative would be unable to see the remote device.
android.permission.CLEAR_APP_USER_DATA	This permission allows the app to clear the user-specific data from another app on the device. This permission in only granted on certain devices.	The app uses this permission in a remote support session as part of the system information tool. The representative can use that tool to view the installed apps on the remote device and clear the user data from the app, resetting it to its default state. This can be useful as a method for fixing an app that is misbehaving.
android.permission.REAL_GET_TASKS	This permission allows the app to obtain information about other processes running on the device. This permission in only granted on certain devices.	The app uses this permission in a remote support session as part of the system information tool. The representative can use that tool to view the running processes on the remote device and end those processes as needed. This can be useful as a method for fixing an app that is misbehaving.
com.samsung.android.knox.permission.KNOX_REMOTE_CONTROL	This permission, which is specific to Samsung devices, allows screen capture and input injection.	The app uses this permission in support sessions running on Samsung devices to allow the representative to remotely control the device by seeing their display injecting input from their console to solve the user’s issue.