BeyondTrust

Remote Support
Android Rep Console 2.2.17

TC:8/10/2023

Table of Contents

Representative Console for Android

BeyondTrust enables you to support your customers remotely by connecting to them through the BeyondTrust Appliance B Series.This guide is designed to help you install BeyondTrust onto your Android device and understand the features of the Android representative console.

Use this guide only after an administrator has performed the initial setup and configuration of the B Series Appliance as detailed in the BeyondTrust Appliance B Series Hardware Installation Guide at www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware. Once BeyondTrust is properly installed, you can begin supporting customers immediately. Should you need any assistance, please contact at www.beyondtrust.com/support.

Note: *BeyondTrust Android support is limited to phones and tablets. Other devices running Android OS are not certified or tested for compatibility.*

Install the Representative Console on Android

The BeyondTrust representative console for Android is available for free download from Google Play. From your Android device, search Google Play for "BeyondTrust Representative Console" and then install the app.

To run the BeyondTrust representative console on your device, your Android device must be running 4.0+.

Configure Mobile Device Management for Android

BeyondTrust supports management of Android devices with mobile device management (MDM). The MDM configuration profile may be configured so that the URL of a support site is pre-populated in the **Site Address** field. The profile may also be configured to prevent this field from being edited.

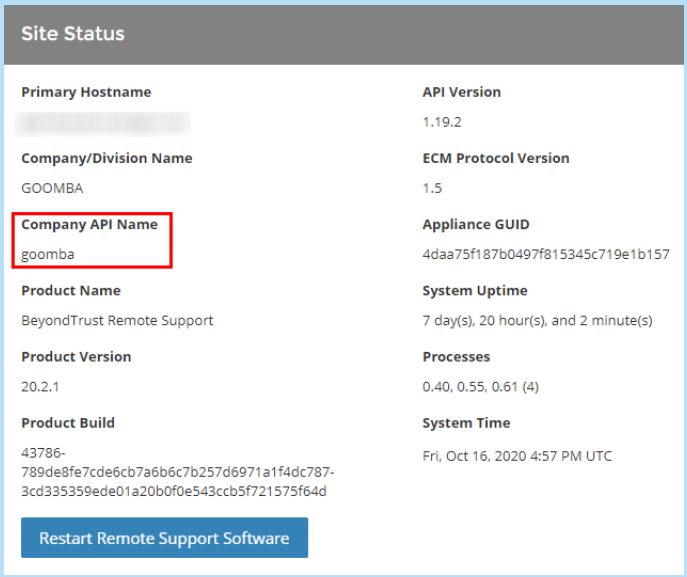
The method by which you configure your profile will vary depending on your MDM product. Consult your MDM documentation for exact steps.

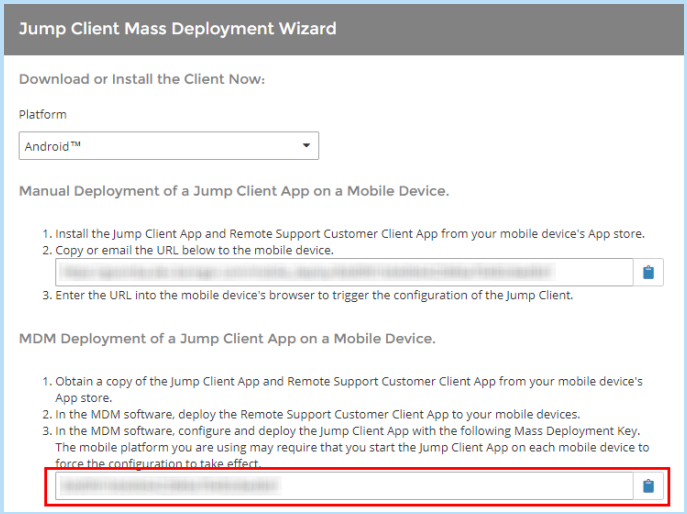
Below are the configurable keys that for the Android Customer Client and Android Jump Client you will need to add to your MDM payload:

Android Customer Client

Key	Type/Description
ApplianceURL	String: The BeyondTrust support site address. For example, support.example.com.
URLLocked	Boolean: If true, then editing the site address within the customer client is disabled.

Android Jump Client

Key	Type/Description
CompanyAPIName	String: The API name of the company or organization. ***Note:*** *The API name can be found in the* ***Site Status*** *section at* ***/login/status****.* 

Key	Type/Description
MassDeploymentKey	String: The ID of your Android Jump Client configuration. ***Note:*** *The Mass Deployment Key value can be found when deploying a Jump Client via* ***/login*** *and selecting the Android platform. The value appears in the MDM section.* 

Manage and Deploy Representative Console App Using Intune

These instructions are based on the Microsoft documentation for using Intune to manage Android devices.

Follow the steps below to create an app configuration policy.

1. Sign in to the Microsoft Intune admin center at https://intune.microsoft.com/.
2. Navigate to **Apps > App configuration policies > Add > Managed devices**.
3. On the **Basics** page, set the following details:
    - **Name**: The name of the profile that appears in the portal.
    - **Description**: The description of the profile that appears in the portal.
    - **Device enrollment type**: The type of device. Leave at the default setting, Managed devices.
4. Select **Android Enterprise** as the **Platform**.
5. Click **Select app** next to **Targeted app**. The **Associated app** pane is displayed.
6. On the **Associated app** pane, choose the BeyondTrust Support or Support+ app to associate with the configuration policy and click **OK**.
7. Click **Next** to display the **Settings** page.
8. Click **Add** to display the **Add permissions** pane.
9. Click the permissions that you want to override. The following permissions are requested by the app and we recommend using the Auto grant behavior:
    - READ_PHONE_STATE
    - READ_CONTACTS
    - GET_ACCOUNTS
    - CAMERA
    - WRITE_EXTERNAL_STORAGE
    - READ_EXTERNAL_STORAGE
10. The default support portal behavior can also be configured with the **Configuration settings format** dropdown if desired. Select **Use configuration designer**.
11. Click **Add**. Add and assign values to each configuration setting according to their descriptions.
12. Click **Next** to display the **Assignments** page.
13. In the dropdown box next to **Assign to**, select either **Add groups**, **Add all users**, or **Add all devices** to assign the app configuration policy. Once you've selected an assignment group, you can select a filter to refine the assignment scope when deploying app configuration policies for managed devices.
14. Click **Next** to display the **Review + create** page.
15. Click **Create** to add the app configuration policy to Intune.

For more information, please see Add app configuration policies for managed Android Enterprise devices at https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android.

Manage and Deploy Representative Console App For Zebra Devices using Intune

Full screen sharing and input injection for Zebra devices require access to specialized services on the devices. This access is granted by staging a configuration profile called a MX Profile at https://techdocs.zebra.com/stagenow/5-10/about/. The MX Profile is generated by StageNow Support at https://www.zebra.com/us/en/support-downloads/software/utilities/stagenow.html and distributed to a device through an Intune profile. This MX Profile is generated by development and must be provided to a customer so they can create a profile within Intune to push the configuration to their devices.

The BeyondTrust MX Profiles are below. There is one for the enterprise Support Plus release and another for the Play Store Support release.

BeyondTrust Plus.xml

```
<wap-provisioningdoc>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="1" />
    <parm name="ServiceIdentifier" value="com.zebra.remotedisplayservice" />
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="4" />
    <parm name="ServiceIdentifier" value="com.zebra.remotedisplayservice" />
    <parm name="CallerPackageName" value="com.beyondtrust.sra.scc.plus" />
    <parm name="CallerSignature"
value="MIIFdDCCA1ygAwIBAgIEThu3yzANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQGEwJVUzEUMBIGA1UECBMLTWlzc2lzc2
lwcGkxEjAQBgNVBAcTCVJpZGdlbGFuZDEbMBkGA1UEChMSQm9tZ2FyIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtEZXZlbG9wbWV
udDEQMA4GA1UEAxMHQW5kcm9pZDAeFw0xMTA3MTIwMjU2MTFaFw00NDA1MTkwMjU2MTFaMHwxCzAJBgNVBAYTAlVTMRQwEgYD
VQQIEwtNaXNzaXNzaXBwaTESMBAGA1UEBxMJUmlkZ2VsYW5kMRswGQYDVQQKExJCb21nYXIgQ29ycG9yYXRpb24xFDASBgNVB
AsTC0RldmVsb3BtZW50MRAwDgYDVQQDEwdBbmRyb2lkMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkqgwc8NDA6
vQVk2e6BHkTNqfsZxRVpZezibfv8U+/hr/uNgFvKE5EQRmjzfcqHim7YRfHzhvSK9kqrYCcxiNzKzFF2d8zcRlPMfWWpErt/L
cudP3NfnvtE0pCJRu29q4d2HTIx68M2e16hSXbBGeuUz7MUhzDcaTTVYX8zUOCjQcvms2juLWAuDzkVrfEaluFVGGQccyDMkU
47YQwHJ4p86mkOzIDoSx7kDtijyNZ+AiW1P7UHOLbl4o07b96VRl3VnMCMYVfFd92cibV5KLAjSySPIzM1OBhbM35DtRBDAGG
JddX5ipGScsALpn5JGlVq4yGjErV8JKBRdTT697qPk6deJDqf2gEBEUvLbNI8/wsLoo7sy2hJas2coset93qUCaH39I60X813
sPALpmraxXla8TlKIbReLWZpFnNGvgYQx3cgleLndY2UDRt1O4Gm76rb1zpTFS94zW4yc6DvFIE7xcWNR6zLpaXOeKK+avuHG
yK3kGtqCKI06x49JvlTm2lVV5zAZFjqWLEfA3HwUzUwks2wj5+xpxRV8XHm2XISTibnwctm7et9witziE2LDIzWE53ldjtFEO
UD1qg6qk7VSk0fAM+ntxtOaEKvRq1VZPjyrnFEZsJ05p6IwhviaIucbPhQmdSDjuNMQB3BGY1U1usdDQ7Mvg1JSeO9UCAwEAA
TANBgkqhkiG9w0BAQUFAAOCAgEAarSiV8z12JkgoLt17CY1MvBkAQStB1Ww9MpYbEspDxS3AnS3AIyqbG2EA0e6NwFoZItTmZ
C+6Jv1jwuyKL1Mc4kVDdmlhQ1lKRqsxwSvJQJHtOX5md+TcND3nkwjNhnLTcbnoH07WlOcuU7BVULYbPvGqxypxYmm46HVoH8
fzYxXJQvbQx8P/FaqMM2ZGzkXoYAUgo/RBptfJy6Kd+bWIPmFXssJIxsojHmueti7lrYt4kSDCYqgxMOXQQqG1fbvjrcc/n0z
MY6nEL8DuJtpzPrdB10vzjCruRCDUjtJgmUPtmc9OS/9s7fEpHDmgvvnkpVoabQw3+MnhI5mCyJsngkni9N5fZpa7bjnepkar
IqvT9v+V9NgelJE3bQ+W2X94Su6QvotAYuWSOe1NdkPXO6oErsA26wY+ogQEqwTZ+yMNgr9PhTruNI/88+Z+RDo6apt1nBXex
TvcjPj1BJM3f2TE7jfUUfH4So4JNWSPLeqLMW3VSLRw2ZSLVXZvk9EJBSPwicNfHV80k2rf1QRfpUXnb3FE3v7mMoAJgTEIN9
E3HuhcmOzR1kSv0ejwvvdMEnc5m9NWtzE5KR3xO3LYkpuY7uaNXdglEOYe/u5GWM5GvzsBj0cNI1X2nMju0dlqXpMdTKgMKA2
Q7JiA7uQfX9HzuklwTvQnKX11Cs85NE=" />
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="1" />
    <parm name="ServiceIdentifier" value="com.zebra.eventinjectionservice" />
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="4" />
    <parm name="ServiceIdentifier" value="com.zebra.eventinjectionservice" />
    <parm name="CallerPackageName" value="com.beyondtrust.sra.scc.plus" />
    <parm name="CallerSignature"
```

```
value="MIIFdDCCA1ygAwIBAgIEThu3yzANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQGEwJVUzEUMBIGA1UECBMLTWlzc2lzc2
lwcGkxEjAQBgNVBAcTCVJpZGdlbGFuZDEbMBkGA1UEChMSQm9tZ2FyIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtEZXZlbG9wbWV
udDEQMA4GA1UEAxMHQW5kcm9pZDAeFw0xMTA3MTIwMjU2MTFaFw00NDA1MTkwMjU2MTFaMHwxCzAJBgNVBAYTAlVTMRQwEgYD
VQQIEwtNaXNzaXNzaXBwaTESMBAGA1UEBxMJUmlkZ2VsYW5kMRswGQYDVQQKExJCb21nYXIgQ29ycG9yYXRpb24xFDASBgNVB
AsTC0RldmVsb3BtZW50MRAwDgYDVQQDEwdBbmRyb2lkMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkqgwc8NDA6
vQVk2e6BHkTNqfsZxRVpZezibfv8U+/hr/uNgFvKE5EQRmjzfcqHim7YRfHzhvSK9kqrYCcxiNzKzFF2d8zcRlPMfWWpErt/L
cudP3NfnvtE0pCJRu29q4d2HTIx68M2e16hSXbBGeuUz7MUhzDcaTTVYX8zUOCjQcvms2juLWAuDzkVrfEaluFVGGQccyDMkU
47YQwHJ4p86mkOzIDoSx7kDtijyNZ+AiW1P7UHOLbl4o07b96VRl3VnMCMYVfFd92cibV5KLAjSySPIzM1OBhbM35DtRBDAGG
JddX5ipGScsALpn5JGlVq4yGjErV8JKBRdTT697qPk6deJDqf2gEBEUvLbNI8/wsLoo7sy2hJas2coset93qUCaH39I60X813
sPALpmraxXla8TlKIbReLWZpFnNGvgYQx3cgleLndY2UDRt1O4Gm76rb1zpTFS94zW4yc6DvFIE7xcWNR6zLpaXOeKK+avuHG
yK3kGtqCKI06x49JvlTm2lVV5zAZFjqWLEfA3HwUzUwks2wj5+xpxRV8XHm2XISTibnwctm7et9witziE2LDIzWE53ldjtFEO
UD1qg6qk7VSk0fAM+ntxtOaEKvRq1VZPjyrnFEZsJ05p6IwhviaIucbPhQmdSDjuNMQB3BGY1U1usdDQ7Mvg1JSeO9UCAwEAA
TANBgkqhkiG9w0BAQUFAAOCAgEAarSiV8z12JkgoLt17CY1MvBkAQStB1Ww9MpYbEspDxS3AnS3AIyqbG2EA0e6NwFoZItTmZ
C+6Jv1jwuyKL1Mc4kVDdmlhQ1lKRqsxwSvJQJHtOX5md+TcND3nkwjNhnLTcbnoH07WlOcuU7BVULYbPvGqxypxYmm46HVoH8
fzYxXJQvbQx8P/FaqMM2ZGzkXoYAUgo/RBptfJy6Kd+bWIPmFXssJIxsojHmueti7lrYt4kSDCYqgxMOXQQqG1fbvjrcc/n0z
MY6nEL8DuJtpzPrdB10vzjCruRCDUjtJgmUPtmc9OS/9s7fEpHDmgvvnkpVoabQw3+MnhI5mCyJsngkni9N5fZpa7bjnepkar
IqvT9v+V9NgelJE3bQ+W2X94Su6QvotAYuWSOe1NdkPXO6oErsA26wY+ogQEqwTZ+yMNgr9PhTruNI/88+Z+RDo6apt1nBXex
TvcjPj1BJM3f2TE7jfUUfH4So4JNWSPLeqLMW3VSLRw2ZSLVXZvk9EJBSPwicNfHV80k2rf1QRfpUXnb3FE3v7mMoAJgTEIN9
E3HuhcmOzR1kSv0ejwvvdMEnc5m9NWtzE5KR3xO3LYkpuY7uaNXdglEOYe/u5GWM5GvzsBj0cNI1X2nMju0dlqXpMdTKgMKA2
Q7JiA7uQfX9HzuklwTvQnKX11Cs85NE=" />
  </characteristic>
</wap-provisioningdoc>
```

BeyondTrust.xml

```
<wap-provisioningdoc>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="1" />
    <parm name="ServiceIdentifier" value="com.zebra.remotedisplayservice" />
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="4" />
    <parm name="ServiceIdentifier" value="com.zebra.remotedisplayservice" />
    <parm name="CallerPackageName" value="com.bomgar.thinclient.android" />
    <parm name="CallerSignature"
value="MIIFdDCCA1ygAwIBAgIEThu3yzANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQGEwJVUzEUMBIGA1UECBMLTWlzc2lzc2
lwcGkxEjAQBgNVBAcTCVJpZGdlbGFuZDEbMBkGA1UEChMSQm9tZ2FyIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtEZXZlbG9wbWV
udDEQMA4GA1UEAxMHQW5kcm9pZDAeFw0xMTA3MTIwMjU2MTFaFw00NDA1MTkwMjU2MTFaMHwxCzAJBgNVBAYTAlVTMRQwEgYD
VQQIEwtNaXNzaXNzaXBwaTESMBAGA1UEBxMJUmlkZ2VsYW5kMRswGQYDVQQKExJCb21nYXIgQ29ycG9yYXRpb24xFDASBgNVB
AsTC0RldmVsb3BtZW50MRAwDgYDVQQDEwdBbmRyb2lkMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkqgwc8NDA6
vQVk2e6BHkTNqfsZxRVpZezibfv8U+/hr/uNgFvKE5EQRmjzfcqHim7YRfHzhvSK9kqrYCcxiNzKzFF2d8zcRlPMfWWpErt/L
cudP3NfnvtE0pCJRu29q4d2HTIx68M2e16hSXbBGeuUz7MUhzDcaTTVYX8zUOCjQcvms2juLWAuDzkVrfEaluFVGGQccyDMkU
47YQwHJ4p86mkOzIDoSx7kDtijyNZ+AiW1P7UHOLbl4o07b96VRl3VnMCMYVfFd92cibV5KLAjSySPIzM1OBhbM35DtRBDAGG
JddX5ipGScsALpn5JGlVq4yGjErV8JKBRdTT697qPk6deJDqf2gEBEUvLbNI8/wsLoo7sy2hJas2coset93qUCaH39I60X813
sPALpmraxXla8TlKIbReLWZpFnNGvgYQx3cgleLndY2UDRt1O4Gm76rb1zpTFS94zW4yc6DvFIE7xcWNR6zLpaXOeKK+avuHG
yK3kGtqCKI06x49JvlTm2lVV5zAZFjqWLEfA3HwUzUwks2wj5+xpxRV8XHm2XISTibnwctm7et9witziE2LDIzWE53ldjtFEO
UD1qg6qk7VSk0fAM+ntxtOaEKvRq1VZPjyrnFEZsJ05p6IwhviaIucbPhQmdSDjuNMQB3BGY1U1usdDQ7Mvg1JSeO9UCAwEAA
TANBgkqhkiG9w0BAQUFAAOCAgEAarSiV8z12JkgoLt17CY1MvBkAQStB1Ww9MpYbEspDxS3AnS3AIyqbG2EA0e6NwFoZItTmZ
C+6Jv1jwuyKL1Mc4kVDdmlhQ1lKRqsxwSvJQJHtOX5md+TcND3nkwjNhnLTcbnoH07WlOcuU7BVULYbPvGqxypxYmm46HVoH8
fzYxXJQvbQx8P/FaqMM2ZGzkXoYAUgo/RBptfJy6Kd+bWIPmFXssJIxsojHmueti7lrYt4kSDCYqgxMOXQQqG1fbvjrcc/n0z
MY6nEL8DuJtpzPrdB10vzjCruRCDUjtJgmUPtmc9OS/9s7fEpHDmgvvnkpVoabQw3+MnhI5mCyJsngkni9N5fZpa7bjnepkar
IqvT9v+V9NgelJE3bQ+W2X94Su6QvotAYuWSOe1NdkPXO6oErsA26wY+ogQEqwTZ+yMNgr9PhTruNI/88+Z+RDo6apt1nBXex
TvcjPj1BJM3f2TE7jfUUfH4So4JNWSPLeqLMW3VSLRw2ZSLVXZvk9EJBSPwicNfHV80k2rf1QRfpUXnb3FE3v7mMoAJgTEIN9
E3HuhcmOzR1kSv0ejwvvdMEnc5m9NWtzE5KR3xO3LYkpuY7uaNXdglEOYe/u5GWM5GvzsBj0cNI1X2nMju0dlqXpMdTKgMKA2
Q7JiA7uQfX9HzuklwTvQnKX11Cs85NE=" />
```

```
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="1" />
    <parm name="ServiceIdentifier" value="com.zebra.eventinjectionservice" />
  </characteristic>
  <characteristic version="9.3" type="AccessMgr">
    <parm name="ServiceAccessAction" value="4" />
    <parm name="ServiceIdentifier" value="com.zebra.eventinjectionservice" />
    <parm name="CallerPackageName" value="com.bomgar.thinclient.android" />
    <parm name="CallerSignature"
value="MIIFdDCCA1ygAwIBAgIEThu3yzANBgkqhkiG9w0BAQUFADB8MQswCQYDVQQGEwJVUzEUMBIGA1UECBMLTWlzc2lzc2
lwcGkxEjAQBgNVBAcTCVJpZGdlbGFuZDEbMBkGA1UEChMSQm9tZ2FyIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtEZXZlbG9wbWV
udDEQMA4GA1UEAxMHQW5kcm9pZDAeFw0xMTA3MTIwMjU2MTFaFw00NDA1MTkwMjU2MTFaMHwxCzAJBgNVBAYTAlVTMRQwEgYD
VQQIEwtNaXNzaXNzaXBwaTESMBAGA1UEBxMJUmlkZ2VsYW5kMRswGQYDVQQKExJCb21nYXIgQ29ycG9yYXRpb24xFDASBgNVB
AsTC0RldmVsb3BtZW50MRAwDgYDVQQDEwdBbmRyb2lkMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAkqgwc8NDA6
vQVk2e6BHkTNqfsZxRVpZezibfv8U+/hr/uNgFvKE5EQRmjzfcqHim7YRfHzhvSK9kqrYCcxiNzKzFF2d8zcRlPMfWWpErt/L
cudP3NfnvtE0pCJRu29q4d2HTIx68M2e16hSXbBGeuUz7MUhzDcaTTVYX8zUOCjQcvms2juLWAuDzkVrfEaluFVGGQccyDMkU
47YQwHJ4p86mkOzIDoSx7kDtijyNZ+AiW1P7UHOLbl4o07b96VRl3VnMCMYVfFd92cibV5KLAjSySPIzM1OBhbM35DtRBDAGG
JddX5ipGScsALpn5JGlVq4yGjErV8JKBRdTT697qPk6deJDqf2gEBEUvLbNI8/wsLoo7sy2hJas2coset93qUCaH39I60X813
sPALpmraxXla8TlKIbReLWZpFnNGvgYQx3cgleLndY2UDRt1O4Gm76rb1zpTFS94zW4yc6DvFIE7xcWNR6zLpaXOeKK+avuHG
yK3kGtqCKI06x49JvlTm2lVV5zAZFjqWLEfA3HwUzUwks2wj5+xpxRV8XHm2XISTibnwctm7et9witziE2LDIzWE53ldjtFEO
UD1qg6qk7VSk0fAM+ntxtOaEKvRq1VZPjyrnFEZsJ05p6IwhviaIucbPhQmdSDjuNMQB3BGY1U1usdDQ7Mvg1JSeO9UCAwEAA
TANBgkqhkiG9w0BAQUFAAOCAgEAarSiV8z12JkgoLt17CY1MvBkAQStB1Ww9MpYbEspDxS3AnS3AIyqbG2EA0e6NwFoZItTmZ
C+6Jv1jwuyKL1Mc4kVDdmlhQ1lKRqsxwSvJQJHtOX5md+TcND3nkwjNhnLTcbnoH07WlOcuU7BVULYbPvGqxypxYmm46HVoH8
fzYxXJQvbQx8P/FaqMM2ZGzkXoYAUgo/RBptfJy6Kd+bWIPmFXssJIxsojHmueti7lrYt4kSDCYqgxMOXQQqG1fbvjrcc/n0z
MY6nEL8DuJtpzPrdB10vzjCruRCDUjtJgmUPtmc9OS/9s7fEpHDmgvvnkpVoabQw3+MnhI5mCyJsngkni9N5fZpa7bjnepkar
IqvT9v+V9NgelJE3bQ+W2X94Su6QvotAYuWSOe1NdkPXO6oErsA26wY+ogQEqwTZ+yMNgr9PhTruNI/88+Z+RDo6apt1nBXex
TvcjPj1BJM3f2TE7jfUUfH4So4JNWSPLeqLMW3VSLRw2ZSLVXZvk9EJBSPwicNfHV80k2rf1QRfpUXnb3FE3v7mMoAJgTEIN9
E3HuhcmOzR1kSv0ejwvvdMEnc5m9NWtzE5KR3xO3LYkpuY7uaNXdglEOYe/u5GWM5GvzsBj0cNI1X2nMju0dlqXpMdTKgMKA2
Q7JiA7uQfX9HzuklwTvQnKX11Cs85NE=" />
  </characteristic>
</wap-provisioningdoc>
```

Since the MX Profile is provided by BeyondTrust, the customer must follow the process below to create a device configuration profile and use Zebra mobility extensions in Microsoft Intune:

1. Sign in to the Microsoft Intune admin center at https://intune.microsoft.com/.
2. Navigate to **Devices > Configuration profiles > Create profile**.
3. Enter the following properties:
    - **Platform**: Select **Android device administrator**.
    - **Profile**: **Select MX profile (Zebra only)**.
4. Click **Create**.
5. In **Basics**, enter the following properties:
6. **Name**: Enter a descriptive name for the new profile.
7. **Description**: Enter a description for the profile. This setting is optional, but recommended.
8. Click **Next**.
9. In **Configuration settings > Choose a valid Zebra MX XML file**, add the XML profile file provided by BeyondTrust. When done, click **Next**.
10. In **Assignments**, select the groups to receive this profile.
11. Select **Next**.

12. In **Review + create**, click **Create** when finished.
13. The profile is created and is displayed in the list.

To also apply a customer MX Profile, there are two options:

- Create two Intune profiles, one for the customer configuration and one for the BeyondTrust configuration, and then assign both to a device.
- Create a single Intune profile that contains a merged MX Profile.

To merge a profile, follow these steps:

1. Open the customer profile XML file as the destination, and the BeyondTrust profile XML file as the source in test editor.

Example: *A shorted version of the configuration structure for merging profiles:*

```
<wap-provisioningdoc>
  <characteristic ...
    ...
  </characteristic>
  <characteristic ...
    ...
  </characteristic>
</wap-provisioningdoc>
```

2. From the source file, copy the entire contents of the file except the opening and closing *<wap-provisioningdoc>* lines.
3. In the destination file, locate the last instance of a closing *</characteristic>* and paste the contents copied from the source file on the next line. This results in a longer list of *<characteristic>* entries that retain the same format as the example above.

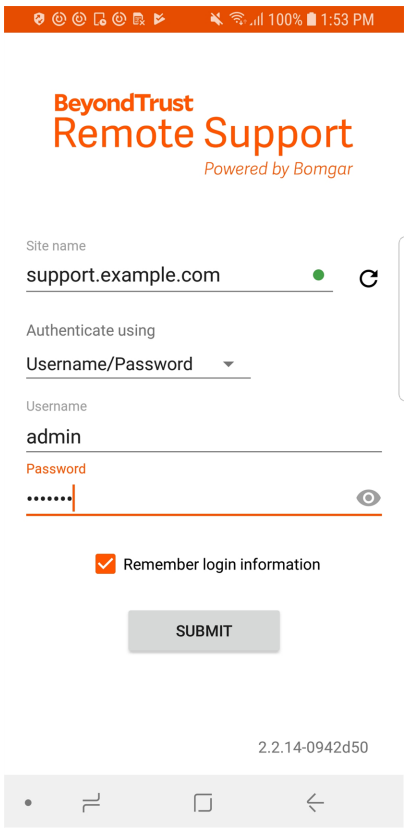
This resulting merged profile can be used to create Intune profiles to be pushed to devices.

For more information, please see the following:

- *Add app configuration policies for managed Android Enterprise devices at https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android*
- *Use and manage Zebra devices with Zebra Mobility Extensions in Microsoft Intune at https://learn.microsoft.com/en-us/mem/intune/configuration/android-zebra-mx-overview*
- *Assign policies in Microsoft Intune at https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign*

Log in to the Representative Console for Android

From the login screen, enter your BeyondTrust site hostname, such as support.example.com. Enter the username and password associated with your BeyondTrust user account. You can choose to have the BeyondTrust representative console remember your login credentials. Then touch **Login**.



> ***Note:*** *If you are using a local account and two-factor authentication has been enabled for it, enter the email code you have received. If you enter the email code incorrectly three consecutive times, you must re-enter your credentials and get a new email code.*

> ***Note:*** *Your administrator might require you to be on an unrestricted network to log in to the console. This network restriction might apply only the first time you log in or every time.*

Log in to the Android Representative Console Using SAML for Mobile

SAML for mobile provides an easy and secure method for authenticating to the Android representative console.

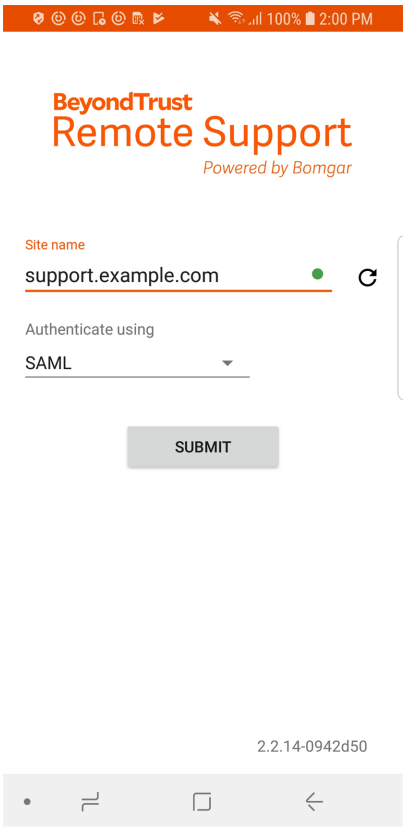
> *For more information about SAML single sign-on, please see Security Assertion Markup Language at https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language.*

Follow the steps below to log in to the mobile representative console using SAML.

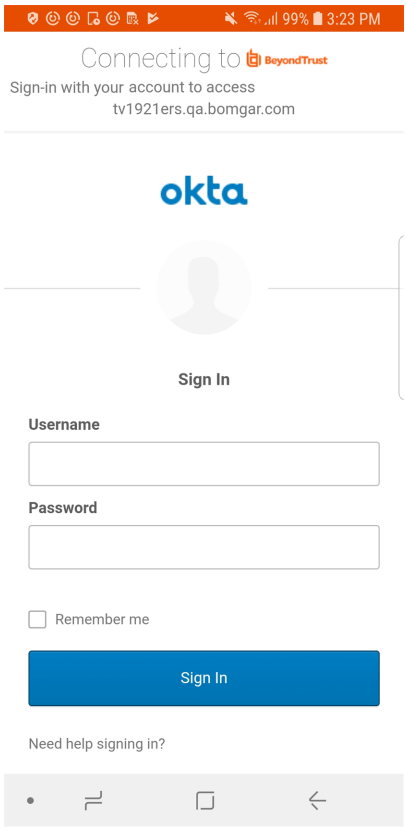
> ***Note:*** *Before attempting to log in to the Android representative console using SAML, verify that a SAML provider has been configured for your /login administrative environment by going to* ***Users & Security > Security Providers****. To learn more about integrating SAML single sign-on into your BeyondTrust Remote Support environment, please see Create and Configure the SAML Security Provider at www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/configure-settings.htm.*

1. Tap the representative console app on your Android device.
2. From the login screen, tap **Username and Password**.

3. Select **SAML**.
4. Tap **Submit**.



5. When directed to your SAML provider's page, enter your credentials.
6. Tap **Log In** to access the representative console.



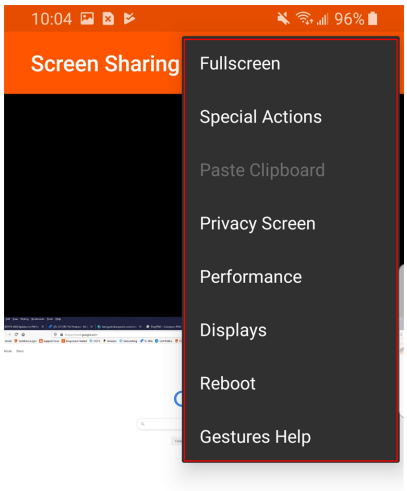
Change Settings and Preferences in the Android Rep Console

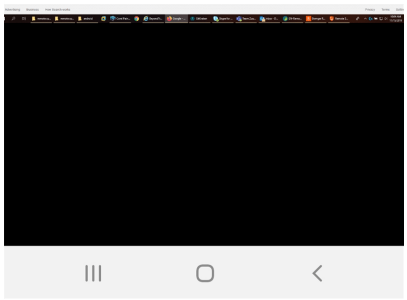
Change Preferences During a Session

To manage your preferences, touch the **Options** button in the upper right corner of the screen.

From the menu, the following preferences are available:

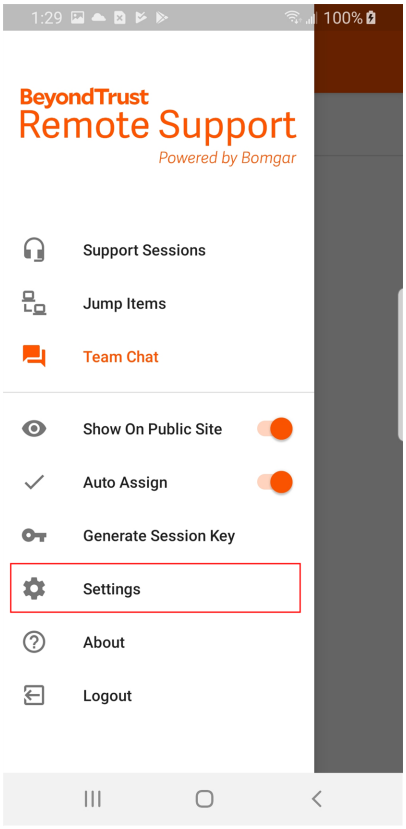
- **Fullscreen:**Hides the rep console UI and expands the display to fit the entire screen of the device. Tap the back button to exit fullscreen mode.
- **Special Actions:**Perform a special action on the remote system. Based on remote operating system and configuration, available tasks will vary. When operating in elevated mode, some actions can be run in System context. Alternatively, provide an administrative user's credentials to perform a special action in that user context. Canned scripts available to the user appear in a fly-out menu.
- **Paste Clipboard:** Allows you to paste items to the clipboard on your computer.
- **Privacy Screen:**If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The customer's view of the privacy screen clearly explains that the representative has disabled the customer's view. The customer can regain control at any time by pressing **Ctrl+Alt+Del**.
- **Performance:** Allows you to change the screen-sharing quality.
- **Displays:** Allows you to select the monitor you want to display to the customer.
- **Reboot:** Allows you to reboot the system that you are supporting.
- **Gestures Help:** Walks you through tips for navigating the mobile representative console.





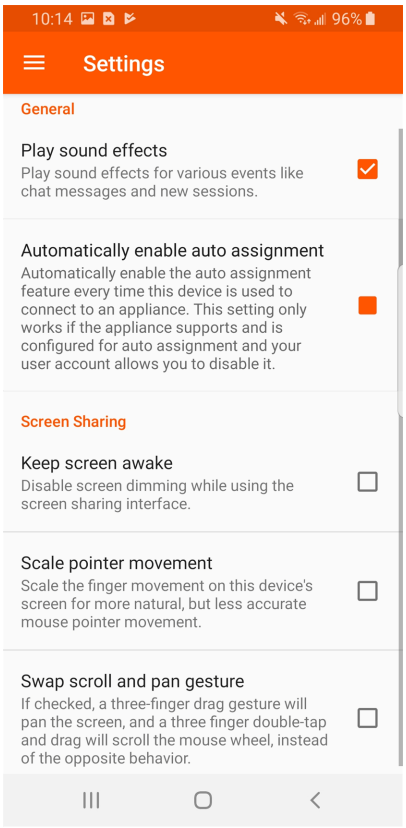
Change Your General and Screen-Sharing Settings

To manage your settings, tap **Settings** from the menu.



The **Play Sound Effects** setting allows you to play audible alerts for certain events that occur within the representative console.

If you have permission to opt out of session assignments, you may enable or disable auto assignment. Auto assignment is used with Equilibrium to route a session to the representative best qualified to handle the issue.



For more information about Equilibrium and session assignment, please see Equilibrium for Automatic Session Routing at www.beyondtrust.com/docs/remote-support/how-to/equilibrium/.

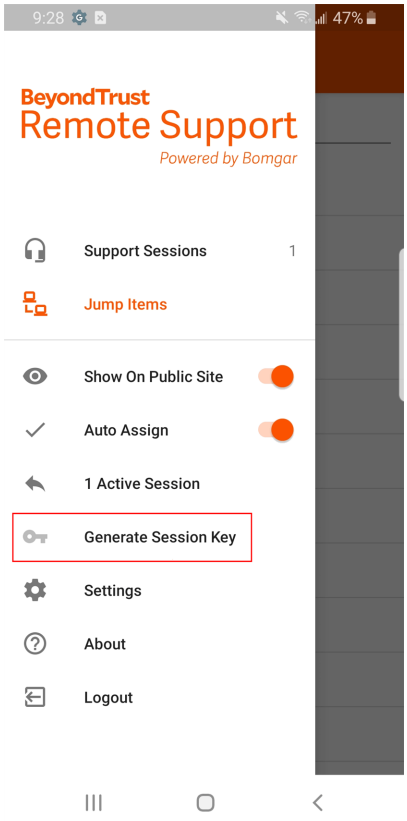
To prevent your screen from dimming during screen sharing, check **Keep screen awake**.

If **Scale pointer movement** is checked, the remote cursor matches your finger movement on the screen. If unchecked, the cursor may lag, but its position will be more accurate.

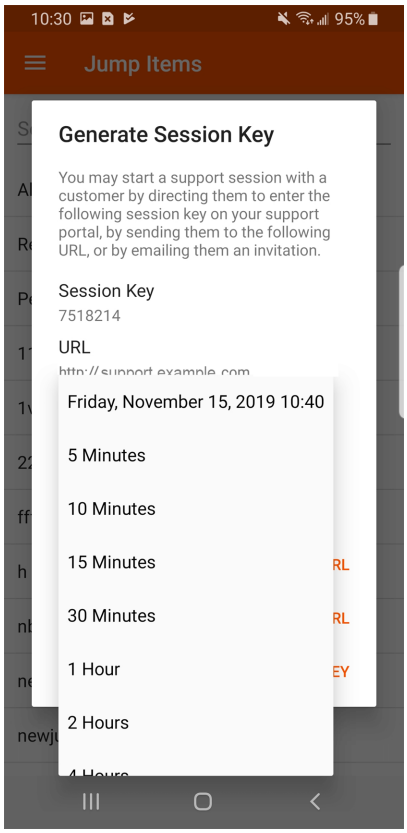
With **Swap scroll and pan gestures**, set which two gestures should scroll the remote mouse wheel and which should pan the screen.

Generate a Session Key to Start a Support Session in the Android Rep Console

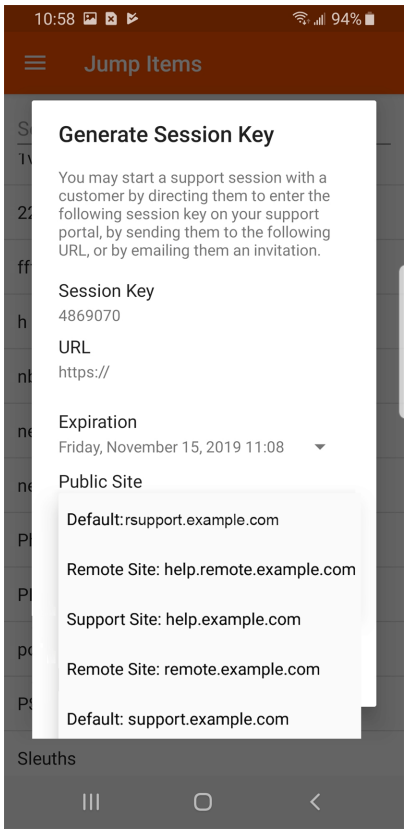
One method to start a support session is for your customer to submit a one-time, randomly generated session key on your public site. Depending upon your account permissions, you can generate session keys for this purpose. Touch the **Generate Session Key** option on the menu. This opens a menu from which you can edit the session key details.



Set how long you want this session key to remain valid. The expiration time applies only to the length of time the key can be used to start a session and does not affect the length of the session itself.



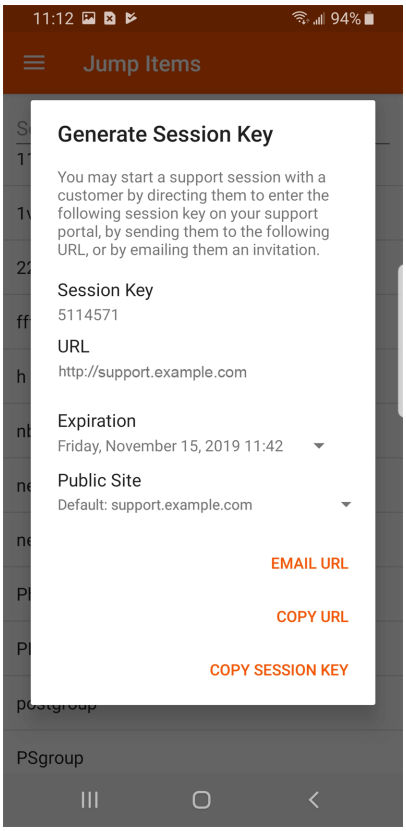
You can also select the public portal through which you want your customer to enter the session.



Direct your customer to go to either to the unique URL or to enter the session key on your public site. You can copy the URL to your clipboard to send it to your customer in a text message.

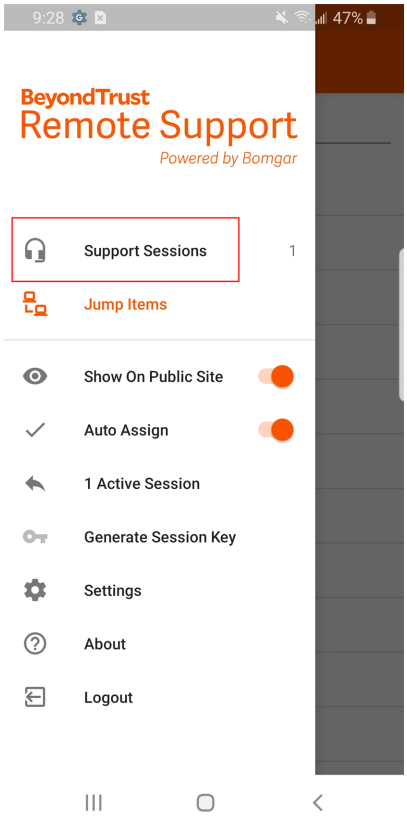
You can also send your customer an email invitation that contains the unique URL.

After running the customer client, the customer appears in your personal queue.



View Support Sessions in Queue in the Android Rep Console

Queues



Session queues provide information about and access to customers who are waiting for support. The **Personal** queue contains customers with whom you are currently in session or who are waiting for a session with you specifically. A waiting session appears in your personal queue if it was transferred to you, or if the customer initiated it by entering a session key you generated, by selecting your name from the public site, or by clicking a Support Button tied to you. This queue also contains invitations for you to join a shared session.

You also have queues for any teams of which you are a member. If a customer initiates a session by selecting an issue type from an issue submission form, that customer enters a specific team queue based on which team owns that issue. A customer also enters a team queue if they click a **Support Button** tied to a team. A session may also enter a queue if it is transferred intentionally or due to waiting session rules, or if the representative's connection is lost in the middle of a session. These queues also contain invitations for any representative in the team to join a shared session.

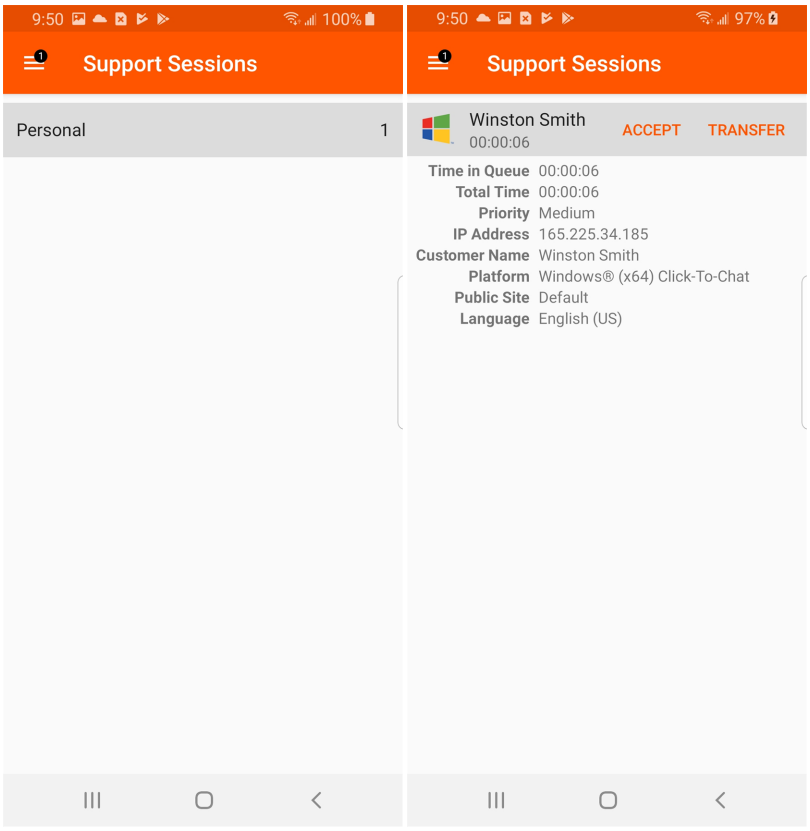
Click the star to the left of a team name to mark that queue as a favorite. If a team chat message is sent, an orange chat bubble appears in place of the star.

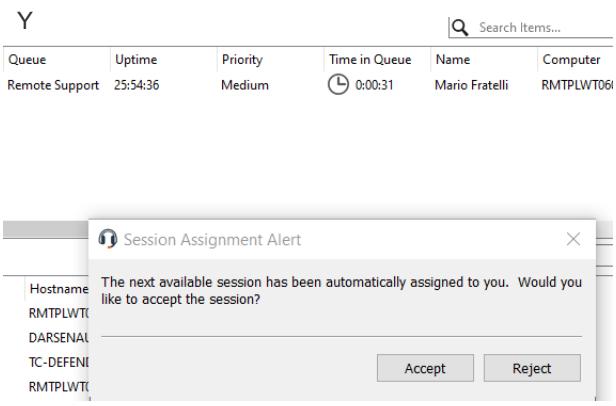
Customers can also request assistance directly from a web page which contains a help link. This initiates a browser sharing session, which allows a representative to chat and view the customer's web page. Administrators can generate custom links in order to direct browser sessions to the correct representative or team queue. In the queue, browser sharing sessions are identified by the **[Browser]** prefix next to the customer's name.

View Sessions

Touch a queue name to view its sessions. Touch a session entry to view details about the support request. To begin supporting the selected session, touch the **Accept** button. Accepting a session opens a new page for that session.

Session Assignment Rules





You can also accept sessions that are assigned using Equilibrium. When a session enters a queue that has Equilibrium enabled, that session is automatically assigned to the best qualified and least busy representative, based on matching skills, the number of sessions that representative is supporting, and how long they have been available.

When a session is assigned to you, you are given a prompt to accept or reject the session, along with an audible alert if enabled. If you reject the invitation or the invitation times out, the session is reassigned to the next best qualified and least busy representative in that queue.

A rejected session is never assigned to the same representative twice unless it is manually transferred into another queue for which that representative is available. If a session cycles through all available representatives for the queue and is not accepted, it remains in queue until someone manually accepts or transfers it.

Alternatively, if your administrator has set up a waiting session rule for this queue, the session gives out an audible alert when it is overdue, or it is transferred to an overflow queue. If that overflow queue has a waiting session rule set up that transfers the session back to the first queue, the session could potentially bounce back and forth between the queues until it is accepted.

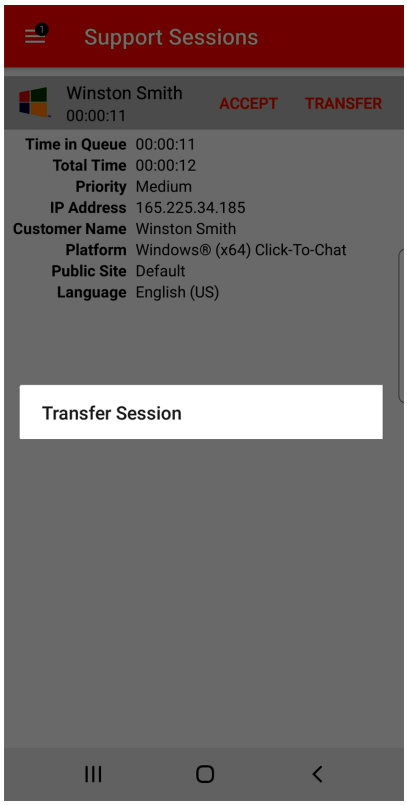
A session is not assigned to a representative if that representative is unavailable. Also, rules within the user permissions mark you as unavailable if you are participating in more than a set number of sessions or have been idle longer than a specified length of time. Finally, if you have permission to opt out of session assignments, you may choose not to receive automatic session assignments.

For more information, please see "Change Settings and Preferences in the Android Rep Console" on page 17.

Session Transfer

Alternatively, you can transfer a session to another queue. When viewing a session's details, touch the **Transfer** button. Browse the list of available teams. Select the queue to which you wish to move the session. Then tap **Transfer**.

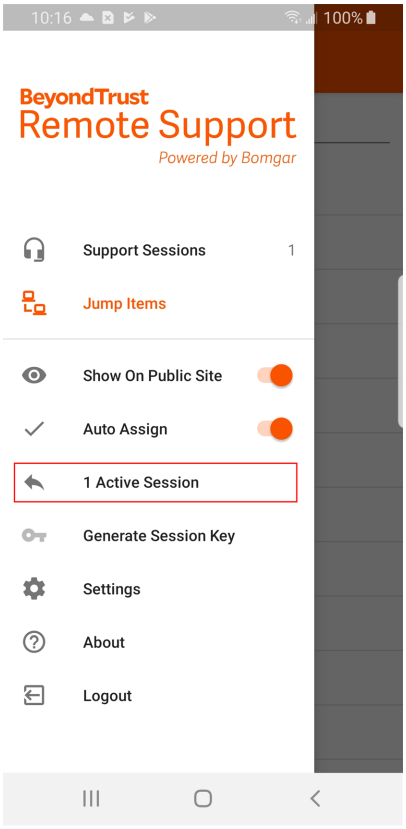
You may also transfer a session to another representative's personal queue. Touch the **Representative** button at the bottom of the menu. Locate the representative and select their name. Then touch the **Transfer Session** button.



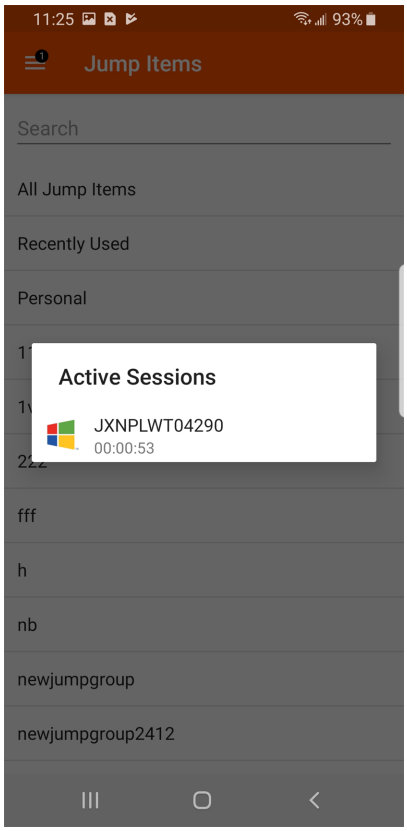
Return to an Active Session in the Android Representative Console

To return to a session you are already supporting, touch the menu icon.

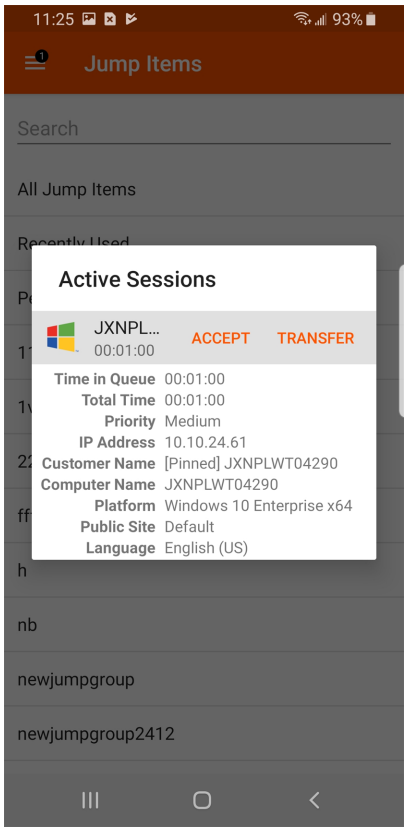
Tap **Active Session**.



Tap the active session you wish to return to from the list.

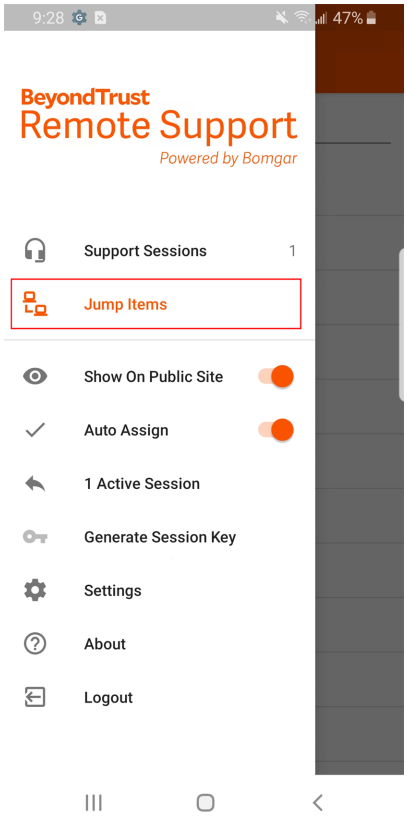


Tap **Accept**.



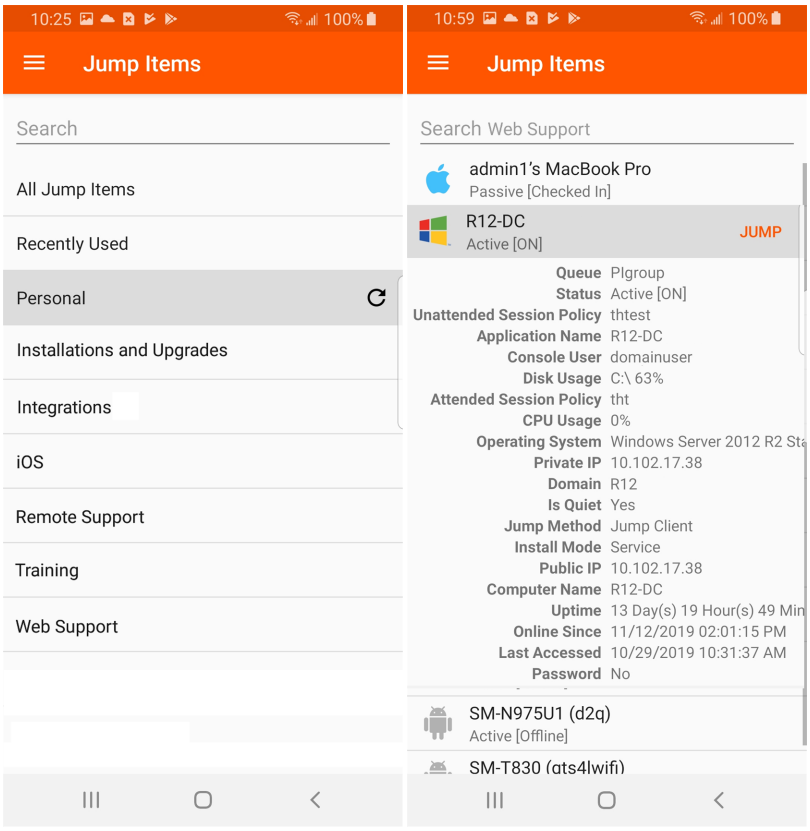
Use Jump Clients to Access Unattended Computers from the Android Rep Console

To access an individual computer without end-user assistance, install a Jump Client on that system either from within a session or from the **Jump Clients** page of the administrative interface. Your account settings determine what Jump Item permissions you have, including which Jump Groups you can access and which types of Jump Items you are allowed to use.



Jump Shortcuts are grouped according to who can access them - only the user who created them or members of a particular Jump Group. To locate a Jump Client, tap the menu and tap the **Jump Items** option. Select the queue where the Jump Client is located. Tap the refresh icon. You can use the **Search** feature to narrow your results. Once you have found the computer you wish to access, select the entry to view details.

Touch the **Jump** button to begin a session. Depending on the permissions your administrator has set for your account, the end-user may be prompted to accept or deny the session. If no response is received within a defined interval of time, the session either starts or is canceled as set in your account permissions.



***Note:** If you need to access Jump Items when no user is available, make sure the session permissions are set either to disable prompting or to default to **Allow** for unattended sessions.*

Jump Client Permissions

The following table offers a list of permissions required by the Android Jump Client app, as well as an explanation for each one.

API Permission Name	Permission Definition	Permission Explanation
android.permission.SYSTEM_ALERT_WINDOW	Allows an app to create windows shown on top of all other apps.	Although the app doesn't make direct use of this permission, it is needed to start the Support app from the background when a representative attempts to start a session through a Jump.
android.permission.RECEIVE_BOOT_COMPLETED	Allows an application to receive a broadcast after the system finishes booting.	The app is able to start itself after the device boots up in order to connect itself with this permission. Otherwise, the app would have to be opened manually after every restart in order to establish a connection to the appliance it is pinned to.
android.permission.INTERNET	Allows applications to open network sockets.	Allows the app to connect to an Appliance in order to start support sessions through the Support app.

API Permission Name	Permission Definition	Permission Explanation
android.permission.ACCESS_ NETWORK_STATE	Allows applications to access information about networks.	The app uses this to determine and show information about its connection status.
android.permission.ACCESS_WIFI_ STATE	Allows applications to access information about Wi-Fi networks.	The app can be configured to enable or disable itself based on certain network states, such as when it only has access to internet over a mobile data connection. This permission grants it access to that information.
android.permission.REQUEST_ IGNORE_BATTERY_ OPTIMIZATIONS	Allows the app to ask the user to ignore battery optimizations.	This is needed to ensure the app can maintain a consistent background connection to the appliance without service interruptions, from any battery saving behavior the operating system may try to impose otherwise.
android.permission.FOREGROUND_ SERVICE	Allows the app to start a foreground service.	A foreground service is required to maintain a consistent background connection to the appliance without service interruptions.
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 Jump Client 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 looks at the SIM card and attempts to gather some generic information about the device. This happens only when dealing with non-consumer devices.
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.	If the representative requests it, the app gathers some system information, including the phone state, and transfers the data to the representative console so that the representative can better deal with the customer's issue.

API Permission Name	Permission Definition	Permission Explanation
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 Jump Client 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 looks at the SIM card and attempts 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 Jump Client 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 looks at the SIM card and attempts to gather some generic information about the device.This happens only when dealing with non-consumer devices.

Use Jump Shortcuts to Access Unattended Computers from the Android Representative Console

To access an individual computer without end-user assistance, create a Jump Shortcut for that system within the representative console or from the **Jumpoint** page of the /login administrative interface. The following Jump Shortcuts are supported by the mobile representative console:

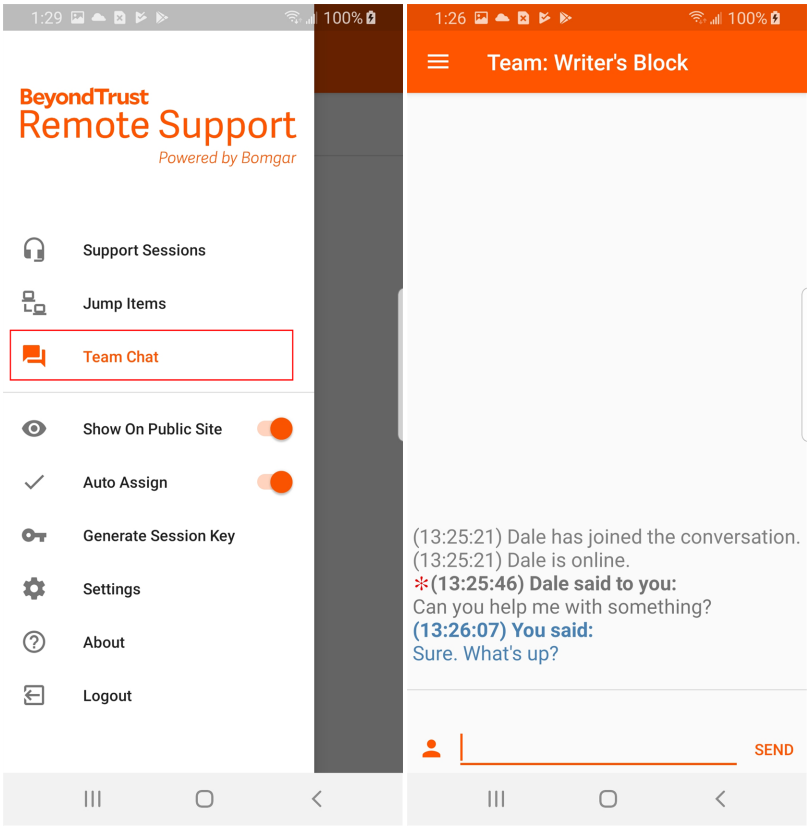
- **Remote Jump**
- **RDP**
- **VNC**
- **Shell Jump**

Jump Shortcuts are grouped according to who can access them - only the user who created them or members of a particular Jump Group.

1. To locate a Jump Shortcut, tap **Jump Items** from the menu.
2. Select a location and touch the **Refresh** icon.
3. Once you have found the system you wish to access, select the entry to view details.
4. Tap the **Jump** button to begin a session.

Use Team Chat to Chat with Other Representatives in the Android Rep Console

From the menu, tap **Team Chat** to chat with other logged-in representatives. If you are a member of one or more support teams, select the team you would like to chat with. You can chat with all members of that team or select a name from the list of representatives to chat with just that one.



Support Session Tools in the Android Rep Console

The support session page is your starting point for providing remote support.

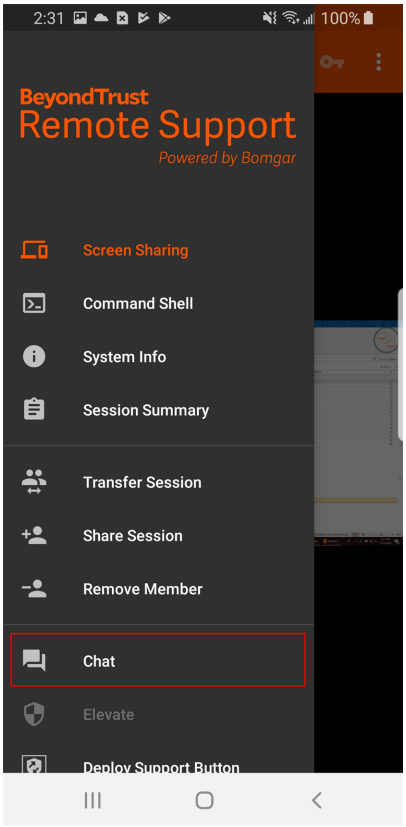
To access support session tools, touch the menu button.

Support Session Tools

Elevate	Elevating the customer client enables switching user accounts, deploying Jump Clients in service mode, and controlling protected windows and UAC dialog boxes. Elevation does not change the user context of the active user and is not the same as logging out the active user and logging back in as an administrator. Elevation to admin rights is currently available only for Windows and Mac computers. Administrators can set the customer client to automatically request elevation at session initiation on Windows systems.
Member Actions	Transfer control of the session to another team or representative. Alternatively, invite another representative to participate in a shared session. If you are the session owner of a shared session, you can remove another representative at any time.
Support Button	If permitted, install a **Support Button** on the remote desktop or remove a previously installed Support Button. The customer can click the **Support Button** to start a support session quickly and easily.
Pin Jump Client	If permitted, install a Jump Client on the remote computer, enabling you or your teammates to access that system later without end-user initiation. Uninstall the client if you no longer need unattended access to that system.
Close Session	Close your session page entirely. If you have ownership of the session, you can either uninstall the customer client from the remote machine or leave the session in queue.

Chat with the Remote Customer During a Session in the Android Representative Console

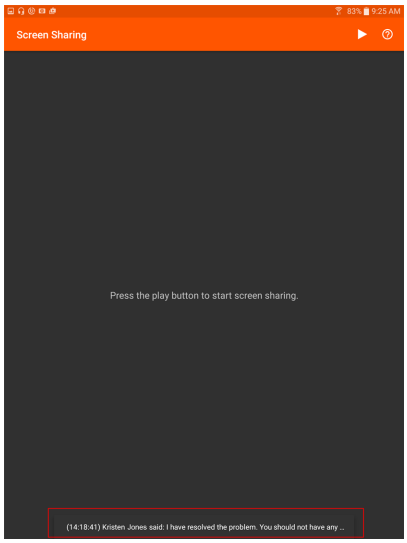
Throughout the support session, you can chat with your remote customer. You do not need to have screen sharing permissions before beginning a chat session. If you have uploaded your photo or any avatar image, it displays on the customer's chat window once the chat begins.



If one or more representatives are sharing the session, you can choose to chat with all participants or to chat privately with only the other representatives. When an additional user joins a shared session, they are able to see the entire chat history. From the menu, select chat members.

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

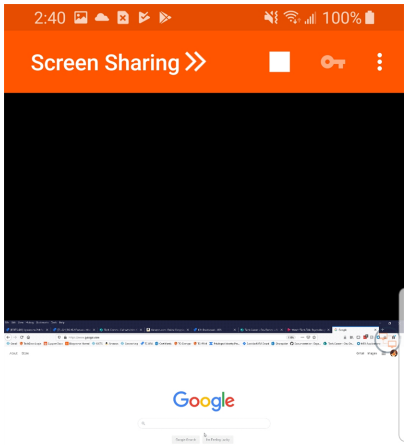
If you receive a message while the chat area is minimized, the message appears as a semi-transparent pop-up near the bottom of the screen.

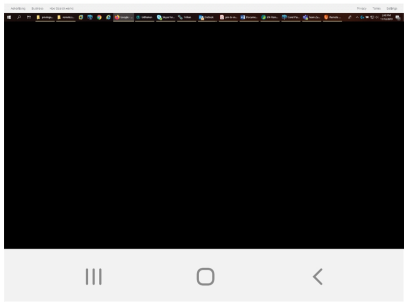


Screen Share with the Remote Computer from the Android Rep Console

From the **Screen Sharing** page, touch the **Play** button at the top of the screen to request view and control of the remote system. Once the customer has granted permission, the remote desktop appears in your display. You have full mouse and keyboard control of the remote system, enabling you to work on the remote computer as if you were physically present.

- Tap once to left-click.
- Double-tap to double-click.
- Place your finger on the cursor and drag to navigate the mouse.
- Double-tap an item and then drag to drag and drop.
- Pinch to view the remote screen at a scaled size or at its full resolution. Zoom occurs where the fingers are placed, regardless of the current pointer location.
- Tap with two fingers to right-click.
- Scroll the mouse wheel by dragging with three fingers.
- Tap with three fingers to toggle the keyboard.
- Tap and hold to locate the cursor.





Screen Sharing Tools

  **Screen Sharing**	Request or stop screen sharing.
 **Help**	View a quick reference of screen sharing gestures.
 **Keyboard**	Access the keyboard in order to type on the remote screen.

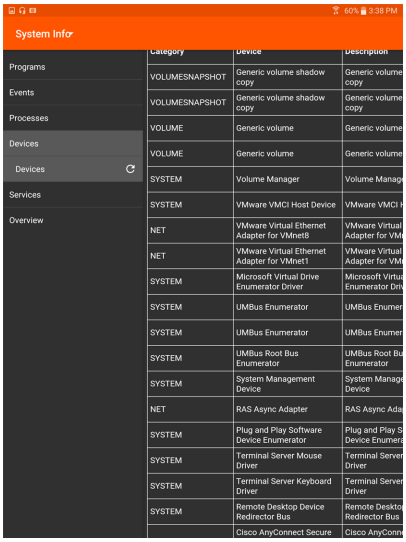
 **Special Actions**	Perform a special action on the remote system. Based on remote operating system and configuration, available tasks will vary. When operating in elevated mode, some actions can be run in System context. Alternatively, provide an administrative user's credentials to perform a special action in that user context. Canned scripts available to the user appear in a fly-out menu.
 **Full Screen**	View the remote desktop in full screen mode. To return to the interface view, touch the **Back** key.
 **Options**	Gain access to actions like setting the monitor display, selecting the screen sharing quality, rebooting remote systems, etc.

View Remote System Information from the Android Rep Console

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.

Select successive category names to access the data you wish to view.

Once the data has been populated, you can touch the **Refresh** icon to retrieve the most recent data.



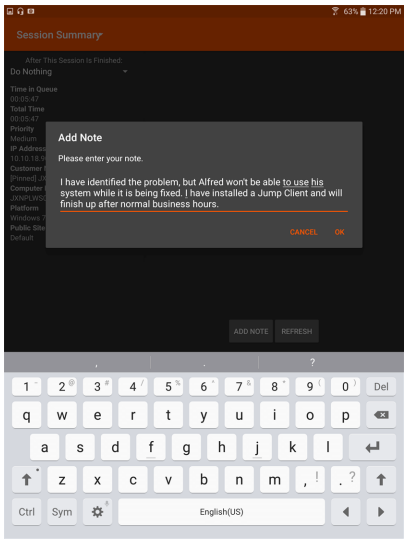
View a Summary of the Support Request and Add Notes from the Android Rep Console

The **Summary** page gives an overview of the remote system, including information like **IP Address**, **Customer Name**, **Computer Name**, and **Platform**.

Depending on your account permissions, you may have the option to log out the Windows user automatically or lock the remote computer when the session closes. When you have been working on an unattended system, for example, locking the computer is recommended to prevent unauthorized users from viewing private information.

Tap **After This Session Is Finished**, and then select the action to take at the end of the session.

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.



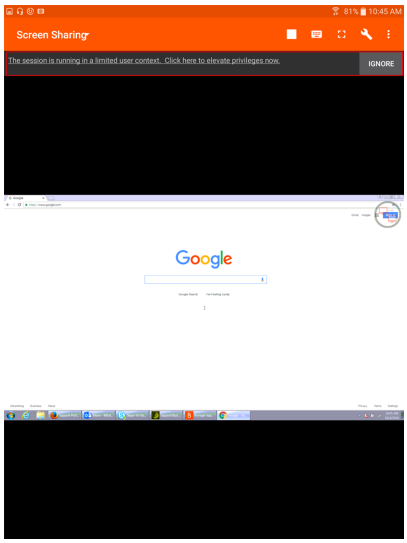
Elevate Rights in the Customer Client from the Android Representative Console

When a session starts in click-to-chat mode, only chat is available. If you wish to have access to more robust support features such as screen sharing, you must elevate the customer client.

Similarly, if the downloaded customer client is running in user mode, you may not have the depth of access you need. You can elevate the customer client to run with administrative rights, as a system service. Elevating the customer client enables switching user accounts, deploying Jump Clients in service mode, and controlling protected windows and UAC dialog boxes. Elevation does not change the user context of the active user and is not the same as logging out the active user and logging back in as an administrator.

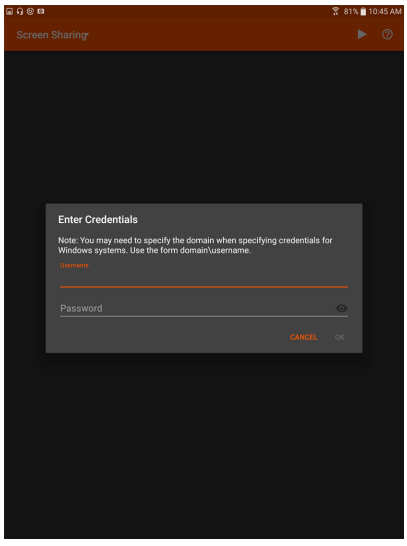
To elevate the customer client, touch the **Elevate** option from the menu.

When initiating a screen sharing session a message may appear at the top of the screen asking to elevate the session. Click the link in the message to receive the **Prompt Customer** and **Provide Credentials** options.



If you possess administrative credentials to the remote computer, select **Provide Credentials** to supply an administrative username and password. Touch **OK** to elevate the client.

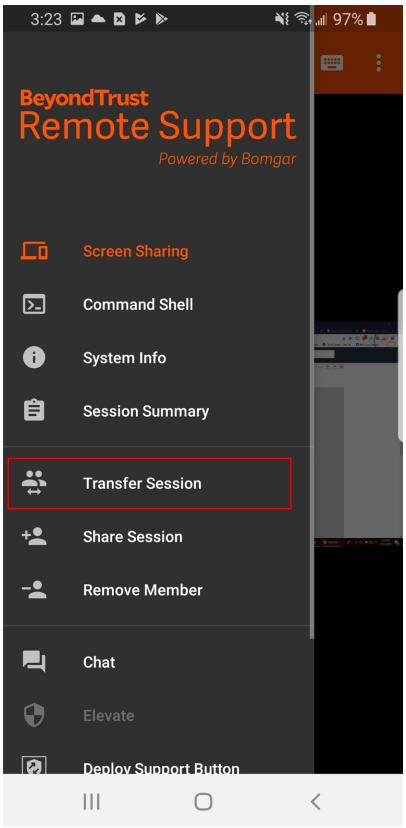
Alternatively, you can touch **Prompt Customer** to send a request to the customer to enter administrative credentials for their computer.



For more information about manual vs automatic elevation, please see the Representative Console Guide at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm.

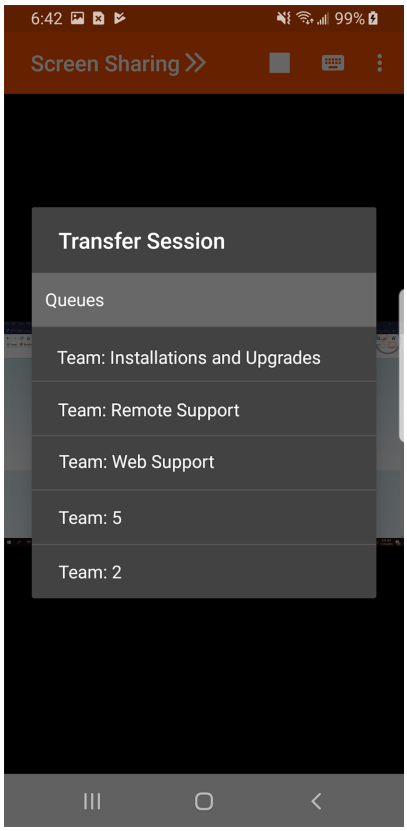
Transfer a Session to Another Representative or Team from the Android Rep Console

To transfer a session to another representative or team, touch **Transfer Session** from the menu.



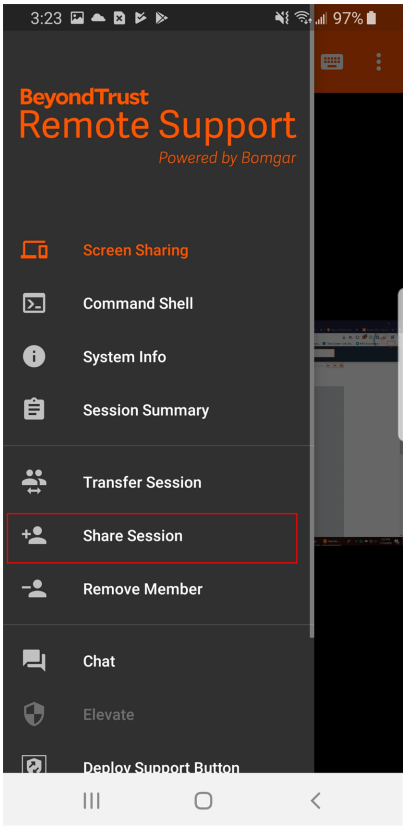
Browse the list of available teams. Select the queue to which you wish to move the session. Then tap **Transfer**.

You may also transfer a session to another representative's personal queue. Touch the **Representative** button at the bottom of the menu. Locate the representative and select their name. Then touch the **Transfer Session** button.



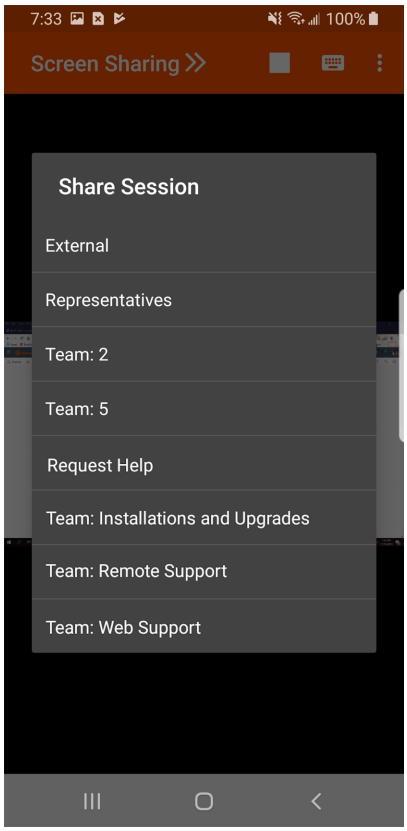
Share a Session with Other Representatives from the Android Rep Console

To share a session with another representative, select **Share Session** from the menu



There are several ways you can invite a representative to join a session. Only issues that have been configured to allow you to request help are displayed on this list.

Select the issue for which you wish to request help. Then tap **Request**.



Alternatively, locate the representative with whom you wish to share the session by first selecting a team to which the representative belongs. Select a team name to view its members.

You can select a user listed in the teams displayed to invite them to join the session.

If you select **Any Representative**, the invitation is sent to the team queue so that any single representative in the selected team can join the session. You can send multiple invitations if you want more representatives from the team to join your session.

Users are listed here only if they are logged into the console or have extended availability enabled.

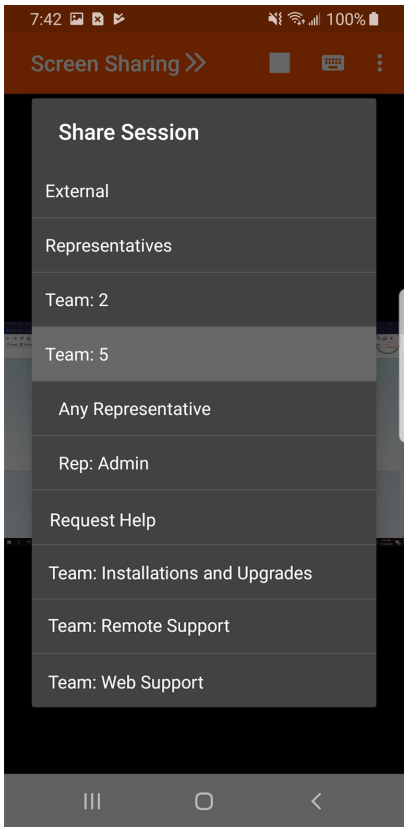
If you are permitted to share sessions with users who are not members of your teams, additional teams are displayed, provided that they contain at least one member logged in or with extended availability enabled.

When you invite a user with extended availability enabled, they receive an email notification.

If you have sent an invitation and it is still active, you may revoke the invitation by selecting it from the **Cancel Invitation** menu. Then touch the **Cancel** button. Only the session owner can send invitations. Invitations do not time out as long as you remain the session owner. Multiple active invitations cannot exist for the same user to join the same session.

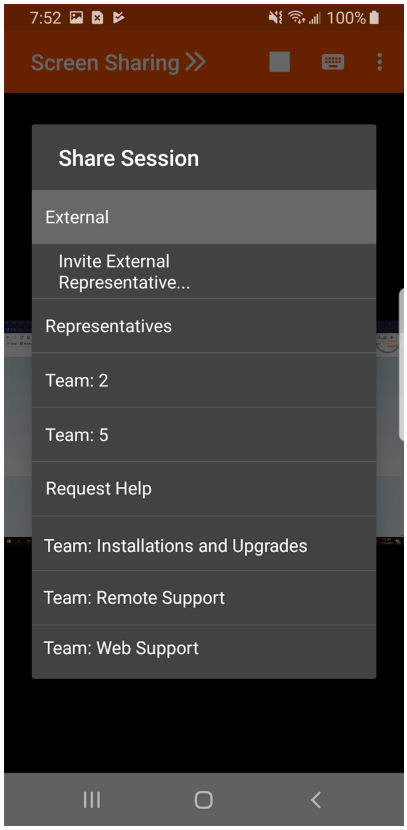
An invitation is made inactive when one of the following events occurs:

- The inviting user cancels the invitation
- The inviting user leaves or transfers ownership of the session
- The session ends
- The invited user accepts the invitation
- The invited user declines the invitation

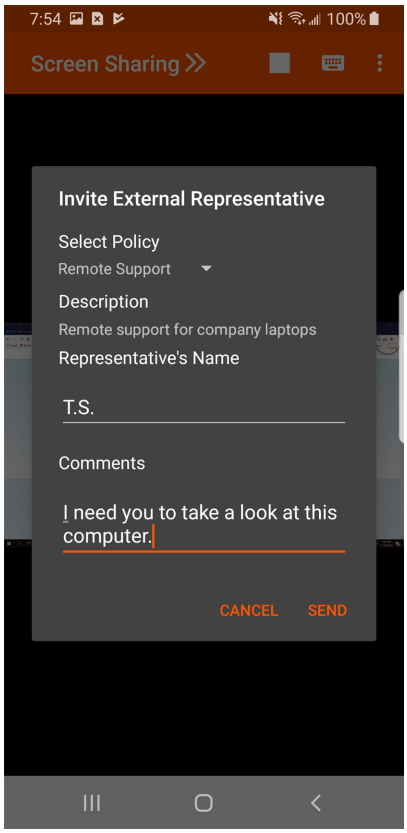


Invite an External Representative to Join a Session from the Android Representative Console

Within a session, a representative can send a one-time invitation to an external user who does not have an account in the BeyondTrust Appliance B Series. To send the invitation, tap the menu icon.

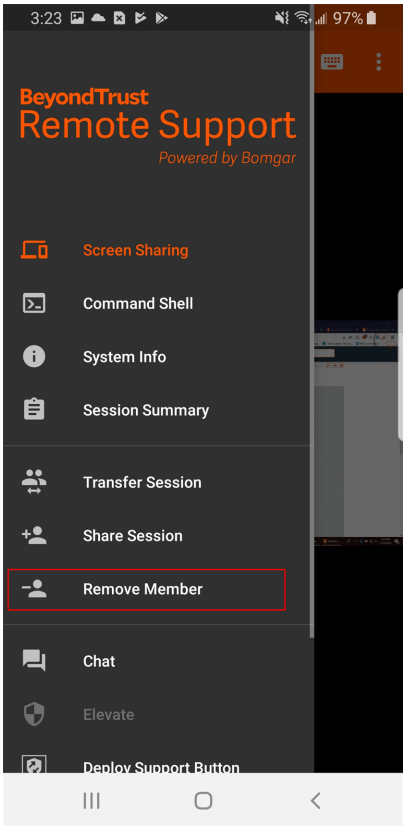


From the menu, select **Share Session**, and then tap **External > Invite External Representative > Invite**.

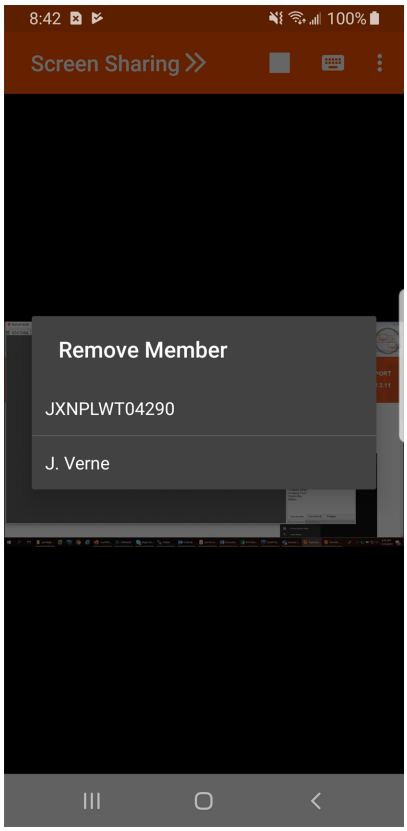


Remove a Member from the Session in the Android Rep Console

You can remove the customer or another user from a shared session. Tap **Remove Member** from the menu. Select the member you wish to remove.



Select the participant you wish to remove. Then touch the **Remove Member** button. Tap **OK** to confirm you want to remove the member. You must be the owner of the support session to remove another member.



Open the Command Shell on a Remote Endpoint Using the Android Representative Console

Remote command shell enables reps to open a virtual command line interface on remote systems. Users can then type locally but have the commands executed on the remote system. You can work from multiple shells.

Your administrator can also enable remote shell recording so that a video of each shell instance can be viewed from the session report. If shell recording is enabled, a transcript of the command shell is also available.

Additional keyboard commands and characters are available above the standard keyboard. The set of additional keys at the top right can be swiped left and right to reveal more options.

If multiple command shells are open, you can swipe the shell screen left and right to switch between the open shells. The name of the current shell is displayed in the lower left corner of the shell screen.

Command Shell Tools

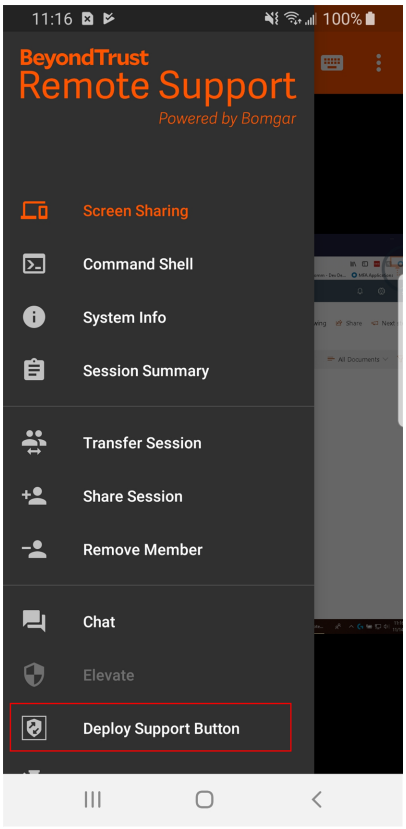
	Open a new shell to run multiple instances of command prompt.
	Close the current command shell. Other open command shells will continue to run.
	Access the keyboard to type commands in the command shell.
	View the command shell in full screen mode.
	Tap the menu icon to access Keyboard and Fullscreen options. The Shell Sessions option is visible if more than one shell session is in progress. Tap Shell Sessions, then the shell session you wish to access.

Add a Support Button to the Remote Computer from the Android Representative Console

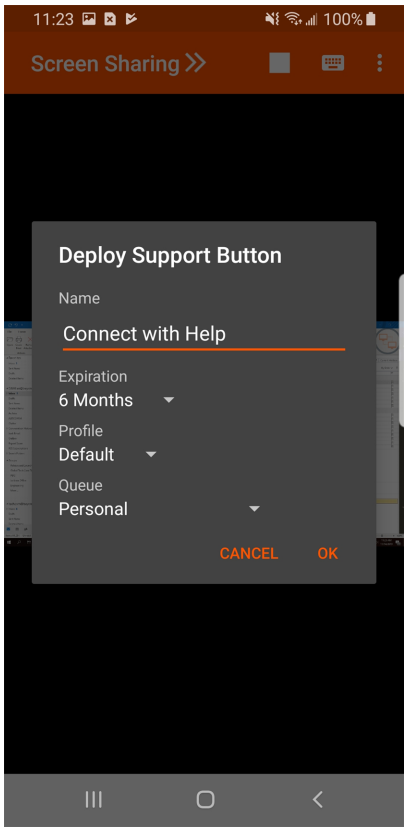
While in a session, you can deploy a Support Button to the remote computer, providing a quick method for your customer to request support.

To edit the name, tap the **Name** entry and modify the text.

To begin, tap the menu. Tap **Deploy Support Button**.

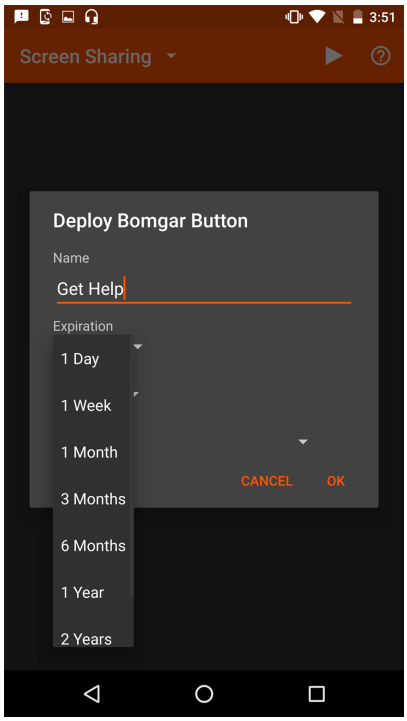


This opens a menu from which you can edit the Support Button's details.

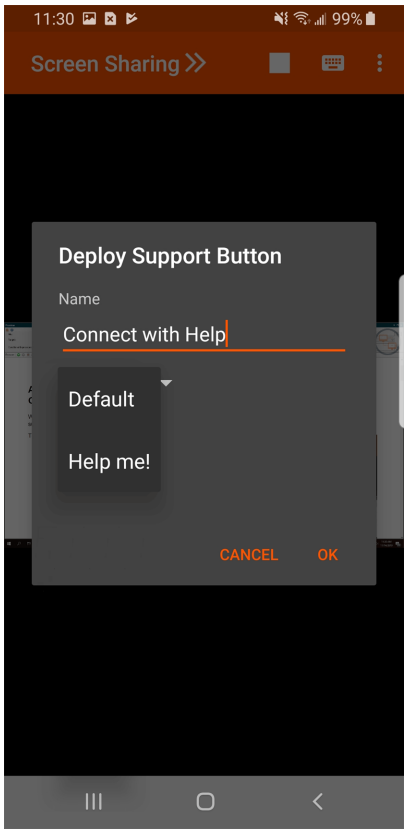


To edit the name, tap the **Name** entry and modify the text.

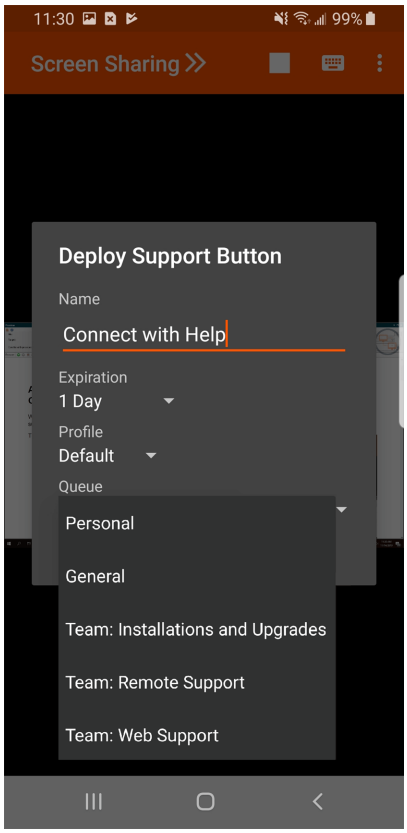
To set how long this Support Button should last, touch the **Expiration** date. The customer can use this button to start sessions only as long as specified. This time does NOT affect how long the installer remains active or how long a session can last.



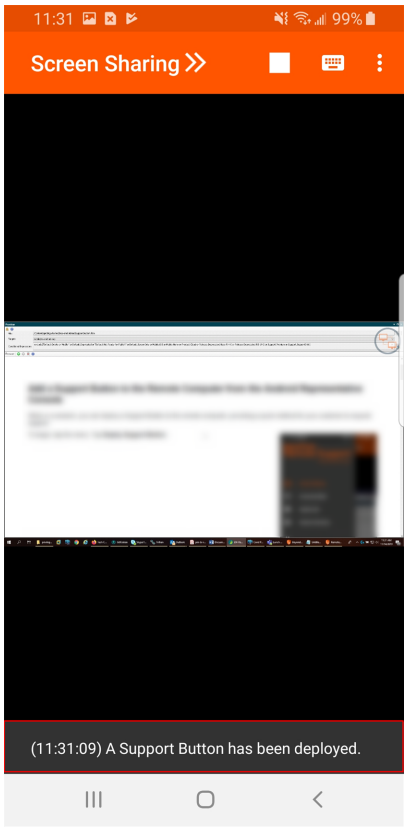
Touch the **Profile** entry to open a list of Support Button profiles from which you can select.



Next, touch the **Queue** entry to select the queue to which this Support Button should link. Once the Support Button is deployed, your customer can use it to directly enter the queue specified here.



After you have set the details for this Support Button, touch **OK**. This creates a Support Button on the remote user's system. Your customer can now use the Support Button to quickly request support.



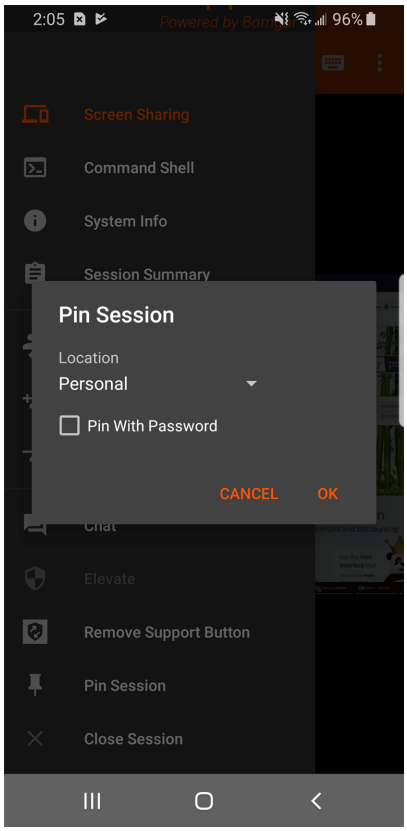
You also may delete the Support Button from the remote system. Touch the **Remove Support Button** icon. When prompted to confirm that you want to uninstall the Support Button, touch **Yes**.

Pin a Jump Client to the Remote Computer from the Android Rep Console

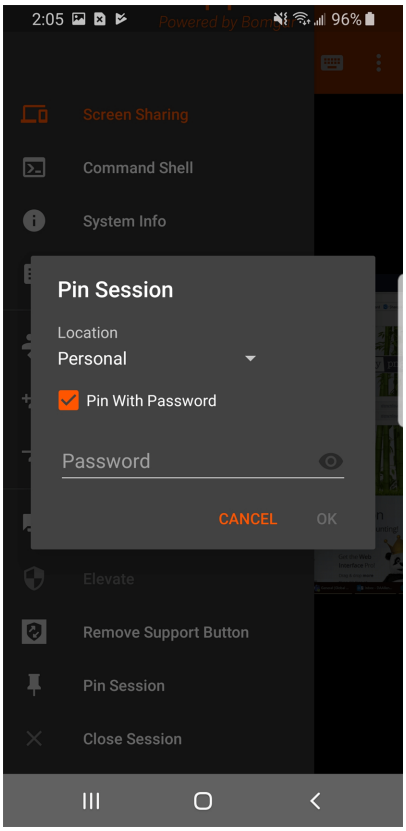
While in a session, you can pin a Jump Client to the remote computer, enabling later unattended access to that system. To begin, touch the **Pin Session** option from the menu.

Touch the **Location** entry to open a list of available Jump Groups, and select the group to which you wish to pin the Jump Client. Pinning the Jump Client to your personal list of Jump Items means that only you can access this remote computer through its Jump Client. You also can choose to pin the Jump Client to a specific Jump Group to allow access to members of that group.

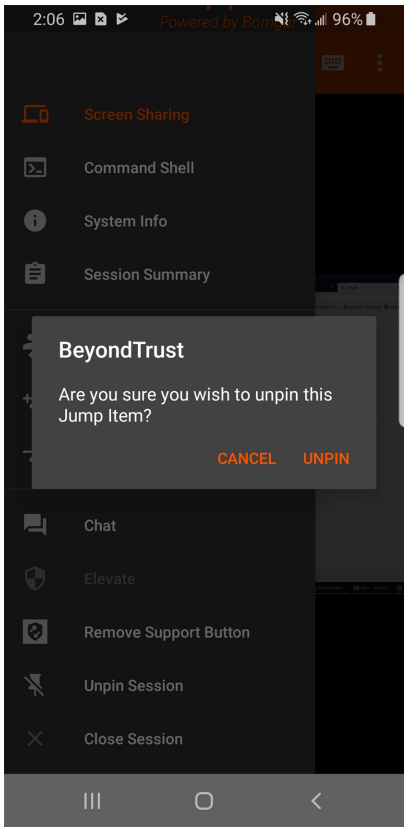
If you wish to pin the Jump Client without setting a password, touch **OK**.



Alternatively, you may set a password for this Jump Client. This will require anyone who wishes to access the Jump Client to enter the correct password before gaining access to the remote system. Enter the desired password and then touch **OK**.



If you no longer need unattended access to a remote system, you can remove the Jump Client. Touch the **Unpin Session** option from the menu. When prompted to confirm that you want to uninstall the Jump Client, touch **Yes**.



Log in to Remote Systems Using Credential Injection in the Android Representative Console

When accessing a Windows-based Jump Client via the mobile representative console, you can use credentials from a credential store to log in to the endpoint or to run applications as an admin.

Before using credential injection, make sure that you have a credential store available to connect to BeyondTrust Remote Support, such as a password vault.

Install and Configure the Endpoint Credential Manager

System Requirements

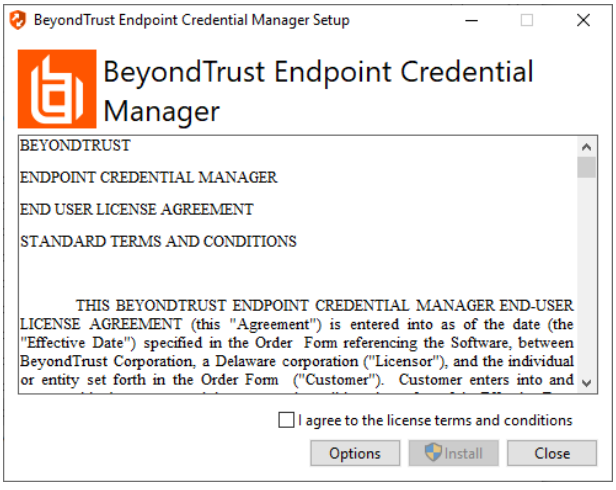
- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

Before you can begin accessing Jump Items using credential injection, you must download, install, and configure the BeyondTrust Endpoint Credential Manager (ECM). The BeyondTrust ECM allows you to quickly configure your connection to a credential store, such as a password vault.

> ***Note:*** *The ECM must be installed in your network to enable the BeyondTrust ECM Service and to use credential injection in BeyondTrust Remote Support.*

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from BeyondTrust Support at beyondtrustcorp.service-now.com/csm. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
2. Agree to the EULA terms and conditions. Mark the checkbox if you agree, and click **Install**.

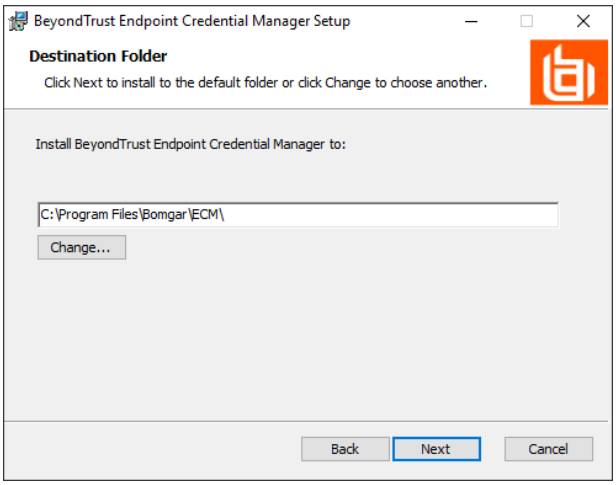
   If you need to modify the ECM installation path, click the **Options** button to customize the installation location.



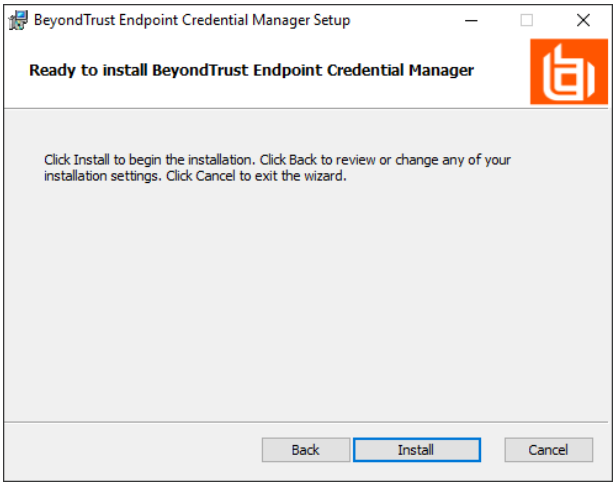
> ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*

3. Click **Install**.

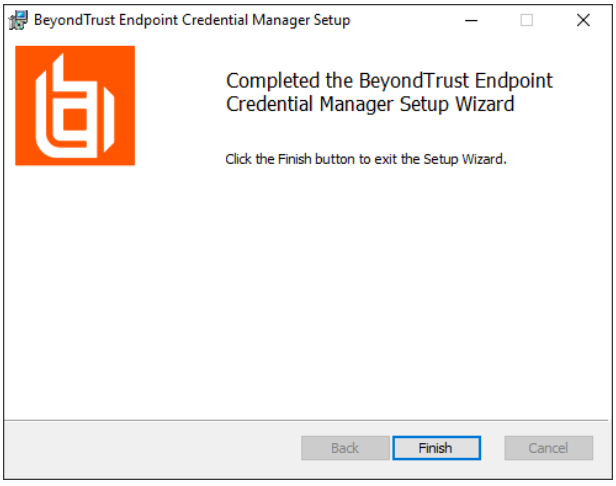
4. Choose a location for the credential manager and click **Next**.
5. On the next screen, you can begin the installation or review any previous step.



6. Click **Install** when you are ready to begin.



7. The installation takes a few moments. On the screen, click **Finish**.



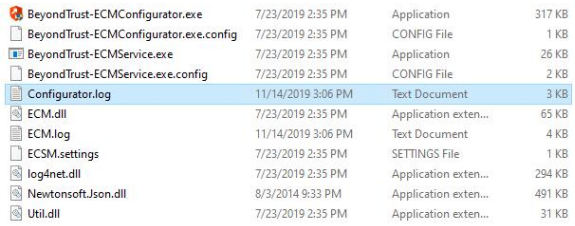
> ***Note:*** *To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the BeyondTrust Appliance B Series. A list of the ECMs connected to the B Series Appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

> ***Note:*** *When multiple ECMs are connected to a BeyondTrust site, the B Series Appliance routes requests to the ECM that has been connected to the B Series Appliance the longest.*

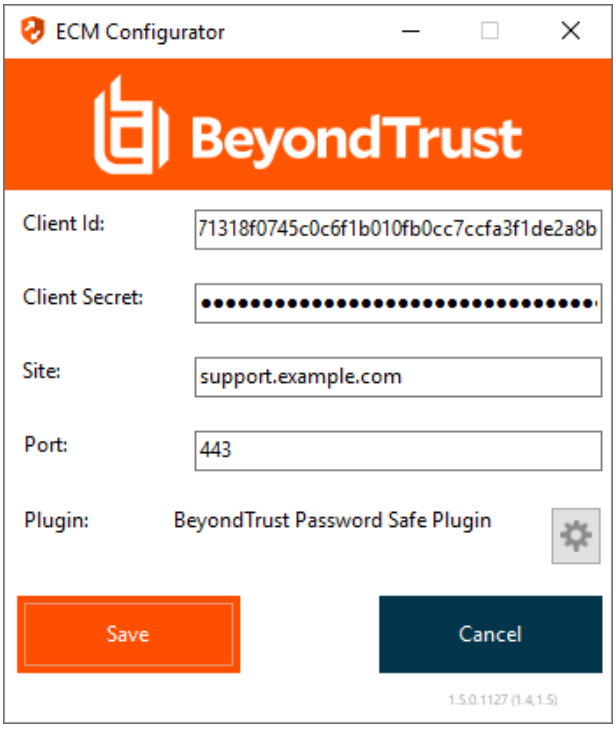
Configure a Connection to Your Credential Store

Using the ECM Configurator, set up a connection to your credential store.

1. Locate the BeyondTrust ECM Configurator you just installed using the Windows Search entry field or by viewing your **Start** menu programs list.
2. Run the program to begin establishing a connection.



3. When the ECM Configurator opens, complete the fields. All fields are required.



Enter the following values:

Field Label	Value
Client ID	The Admin ID for your credential store.
Client Secret	The Admin secret key for your credential store.
Site	The URL for your credential store instance.
Port	The server port through which the ECM connects to your site.
Plugin	Click the **Choose Plugin...** button to locate the plugin.

4. When you click the **Choose Plugin...** button, the ECM location folder opens.
5. Paste your plugin files into the folder.
6. Open the plugin file to begin loading.

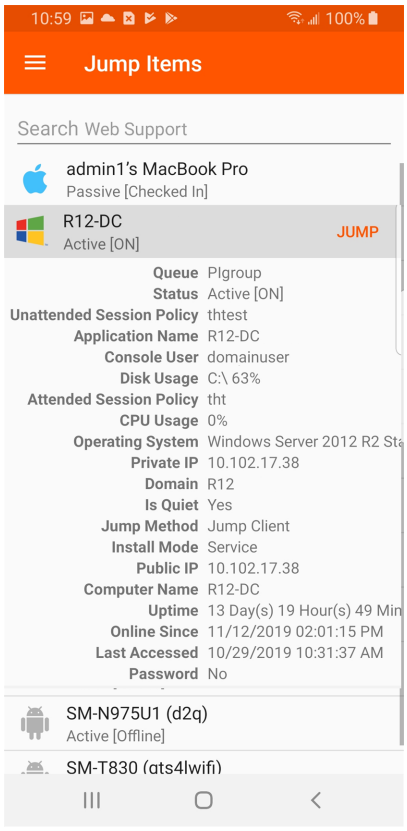
Note: *If you are connecting to a password vault, more configuration at the plugin level may be needed. Plugin requirements vary based on the credential store that is being connected.*

Use Credential Injection to Access Endpoints

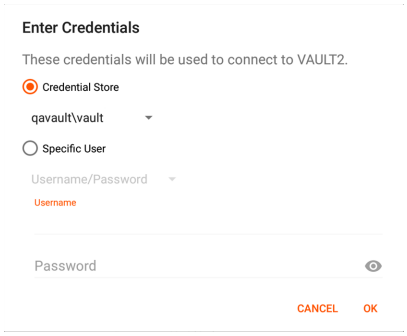
After the credential store has been configured and a connection established, BeyondTrust Remote Support can begin using credentials in the credential store to log in to endpoints.

1. Go to your **Jump Items** list.
2. Tap the Jump Item you wish to access.

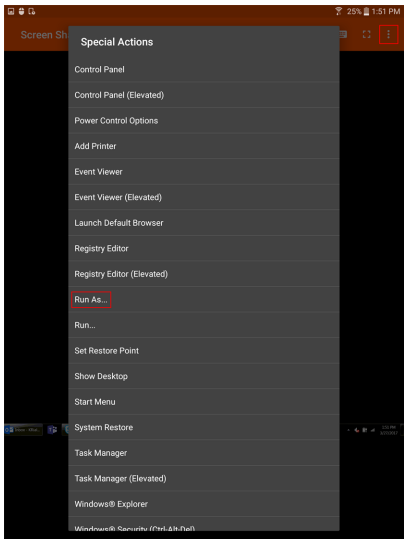
3. Tap **Jump**.



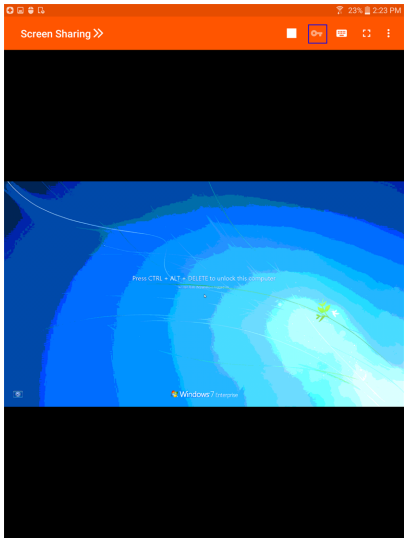
4. The **Enter Credentials** prompt appears. Tap **Credential Store**.
5. Tap the credentials you wish to use to access the system.
6. Tap **OK**.



7. From within the session, tap the **Start** button to start screen sharing.
8. Tap the **Special Actions** option. Tap **Run as...**.
9. Tap **Windows Security (Ctrl-Alt-Del)**.



10. Tap the **Key** icon. The key icon allows the system to view your stored credentials to gain entry into the endpoint.



Close the Session in the Android Representative Console

To exit a session, touch **Close Session** from the menu.

If you are the session owner, End Session closes the session page in your representative console and removes any additional representatives who may be sharing the session. It also uninstalls the customer client from the remote system. However, it does not delete an installed Jump Client.

If you choose **Hold Session**, your session page closes, but the session returns to your personal queue. If any additional representatives are sharing the session, they remain in session.

If you are not the session owner, touching **End Session** removes you from the session. The session continues to be supported by the session owner.