



BeyondTrust

Privileged Remote Access Android Access Console 2.2.10

Table of Contents

Guide to the BeyondTrust Access Console for Android	3
Install the Access Console on Android	4
Log into the Access Console for Android	5
Log into the Android Access Console Using SAML for Mobile	5
Change Settings in the Android Access Console	8
Use Jump Items to Access Endpoints from the Android Access Console	9
End-User and Third-Party Authorization	9
Automatic Log On Credentials	11
Log into Endpoints Using Credential Injection in the Android Access Console	12
Install and Configure the Endpoint Credential Manager	12
Install and Configure the Plugin	14
Configure a Connection to Your Credential Store	15
Use Credential Injection to Access Endpoints	16
Use Team Chat to Chat with Other Users in the Android Access Console	18
View Access Sessions in the Android Access Console	19
Screen Share with the Endpoint from the Android Access Console	20
Screen Sharing Tools	20
Additional Screen Sharing Actions and Tools	21
Share a Session with Other Users from the Android Access Console	22
Invite An External User to Join a Session from the Android Access Console	23
Remove a Member from the Session in the Android Access Console	25
Open the Command Shell on an Remote Endpoint Using the Android Access Console	26
Command Shell Tools	27
View Endpoint System Information from the Android Access Console	28
View a Summary of the Access Session and Add Notes from the Android Access Console ..	29
Close the Session in the Android Access Console	30
Manage and Deploy Access Console App Using Intune	31

Guide to the BeyondTrust Access Console for Android

This guide is designed to help you install BeyondTrust onto your Android device and understand the features of the Android access console. BeyondTrust enables you to securely access your endpoints remotely by connecting to them through the support_button.

Note that although screenshots of an Android smartphone are used in this guide, the functionality is the same when using an Android tablet.

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](#). Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Install the Access Console on Android

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

To run the BeyondTrust access console on your device, your B Series Appliance must be running software version 15.2 or higher. The BeyondTrust access console is supported on Android phones running 2.3 and higher and Android tablets running 3.0 and higher.



Note: Only the BeyondTrust access console can be used with a Privileged Remote Access (PRA) site. The BeyondTrust representative console cannot be used to connect to a Privileged Remote Access site, nor can the BeyondTrust access console be used to connect to a BeyondTrust Remote Support site.



IMPORTANT!

Your B Series Appliance must be equipped with a valid SSL certificate signed by a certificate authority. BeyondTrust does not support using self-signed certificates for the Android access console.¹ 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 run the BeyondTrust access console on your device to access your endpoints from virtually anywhere.

¹Android devices with an operating system prior to 4.0 may encounter a certificate error when attempting to reach your BeyondTrust site. This issue results from a missing root SSL certificate in the Android device's certificate store. The issue is solely related to the Android operating system and not to the BeyondTrust software. To resolve this issue, either upgrade the Android device or contact the certificate authority to request another root SSL certificate which is compatible with the Android device.

Log into the Access Console for Android

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

For privileged users or vendors using the access console, you can choose to change the authentication method by touching the **Username/Password** label. Select **Access Invite Key** from the dropdown menu and enter the key you were provided.



Note: Your administrator might require you to be on an allowed network to log in to the console. This network restriction might apply the first time you log in or every time. This restriction does not apply to access invites.

Log into the Android Access Console Using SAML for Mobile

SAML for mobile provides an easy and secure method for authenticating to the Android access console. To learn more about SAML single sign-on, please see [Security Assertion Markup Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language) at https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language. Follow the steps below to log into the Android access console using SAML.



Note: Before attempting to log into the Android access console using SAML, verify that a SAML provider has been configured for your /login administrative environment by going to **Users & Security > Security Providers**. If SAML is not configured in /login, SAML is not available as an authentication method for the Android access console. To learn more about integrating SAML single sign-on into your BeyondTrust Privileged Remote Access environment, please see [Create and Configure the SAML Security Provider](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm) at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm.

1. Tap the access console app on your Android device.

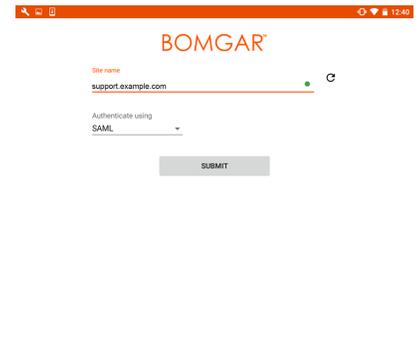
2. From the login screen, tap **Username and Password**.



3. Select **SAML**.

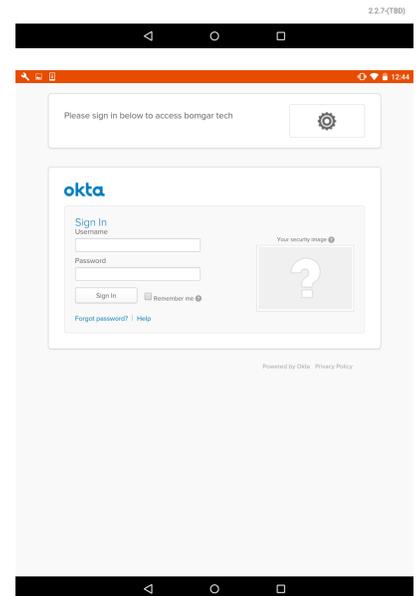


4. Tap **Submit**.



5. When directed to your SAML provider's page, enter your credentials.

6. Tap **Sign In** to access the console.



Change Settings in the Android Access Console

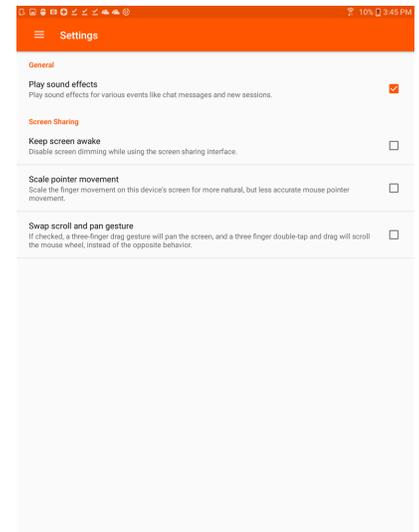
To change your settings, select **Settings** from the menu.

Play Sound Effects plays audible alerts for certain events that occur within the access console.

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 is more accurate.

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



Use Jump Items to Access Endpoints from the Android Access Console

To access an individual endpoint without end-user assistance, install a Jump Item on that system from the **Jump Clients** page of the /login administrative interface. Additionally, the following Jump Item types are supported by the mobile access console:

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

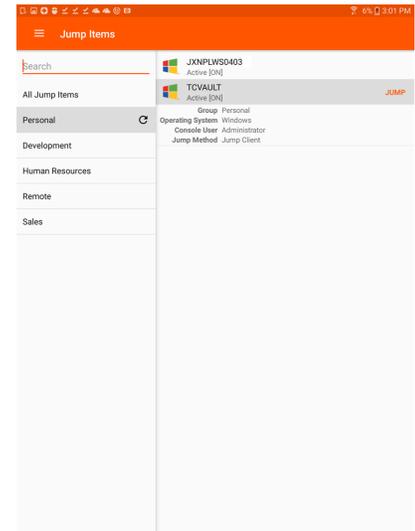
Jump Items are listed in Jump Groups. If you are assigned to one or more Jump Groups, you can access the Jump Items in those groups, with the permissions assigned by your admin.

Your personal list of Jump Items is primarily for your individual use, although your team leads, team managers, and users with permission to see all Jump Items may have access to your personal list of Jump Items. Similarly, if you are a team manager or lead with appropriate permissions, you may see team members' personal lists of Jump Items. Additionally, you may have permission to access Jump Items in Jump Groups you do not belong to and personal Jump Items for non-team members.

To locate a Jump Item, tap on the **Jump Items** option from the menu.

Select a location and touch the **Refresh** button. Once you have found the endpoint you wish to access, select the entry to view details.

Tap the **Jump** button to begin a session.



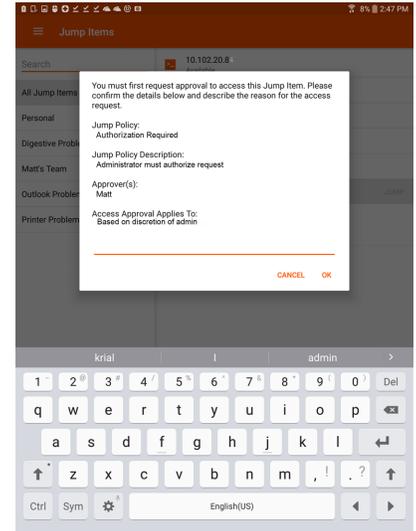
End-User and Third-Party Authorization

Depending on the configuration of Jump Items within the /login administrative interface, a Jump Item may have a Jump Policy associated with it, and the policy may define an authorization component that forces you to request permission from a third-party or an administrator before you are able to start an access session with the Jump Item.

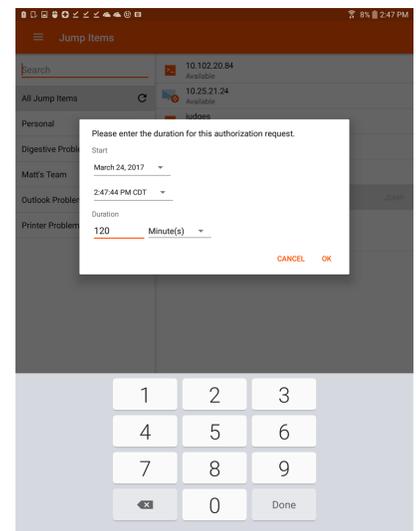


For more information about how to configure third party and end-user notifications and approval, please see [Jump Policies: Set Schedules, Notifications, and Approval for Jump Items](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm>.

After you have tapped the Jump button and requested access, a prompt appears, and you are required to enter a reason for wanting to access the system.



Next, you must indicate when and for how long you will be accessing the system.



Once the request has been submitted, the third party or person responsible for approving access requests is alerted through an email notification and has the opportunity to accept or deny the request. Although other approvers can see the email address of the person who approved or denied the request, the requestor cannot. After permission has been determined, an authorization notification appears within the Jump Item's information displaying either *approved* or *denied*. If access is granted, you can tap the Jump button to begin accessing the system.

Bomgar

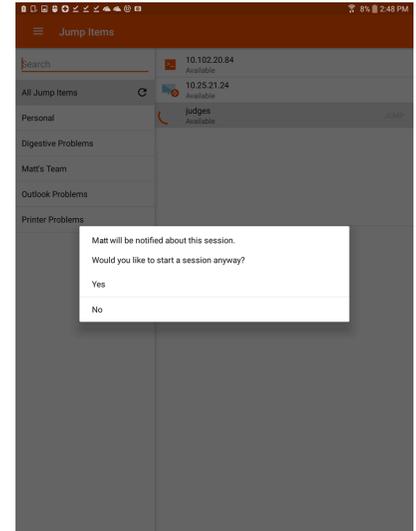
Your jump authorization request number 1 beginning at 05/31/49198 10:19:53 PM has been approved.

OK

After tapping the Jump button, you are presented with a message asking if you would like to begin an access session. If you choose to begin the session, the approving party's comments appear, and you can continue accessing the system.

If the user chooses to continue, the approving party's comments appear, and the user can begin working with the system.

For more information about how Jump Items work with Jump schedules, Ticked ID Workflow, etc., please see [Jump Interface: Use Jump Items to Access Remote Systems at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/jump-interface.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/jump-interface.htm).



Automatic Log On Credentials

Credentials from the **Endpoint Credential Manager** can be used for RDP and for performing Remote Jump. If a user selects to Jump to a Remote Jump or Remote RDP and no automatic log on credentials are available, a username and password must be entered into the prompt before the access session can begin with the endpoint. If the /login administrative interface has been configured with automatic log on credentials and returns only one set of credentials as being available for a particular user and Jump Item, the credential request is skipped, and the single credential is used to start the session. If there is more than one credential configured in the /login administrative interface, the user has the choice either to choose credentials from the credential store or to enter their own credentials manually.

i For more information on credential configuration and management, please see [Security: Manage Security Settings at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm).

Log into Endpoints Using Credential Injection in the Android Access Console

When accessing a Windows-based Jump Client via the mobile access console, you can use credentials from a credential store to log into 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 PRA, such as a password vault.

Install and Configure the Endpoint Credential Manager

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.



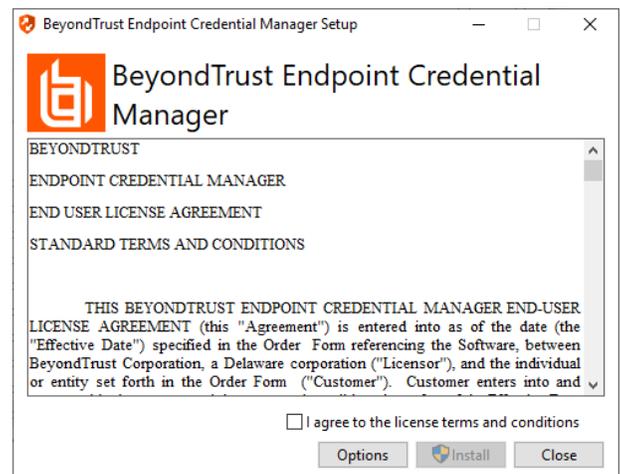
Note: The ECM must be installed in your network to enable the BeyondTrust ECM Service and to use credential injection in BeyondTrust PRA.

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from [BeyondTrust Support](https://www.beyondtrustcorp.com/service-now.com/csm) at [beyondtrustcorp.service-now.com/csm](https://www.beyondtrustcorp.com/service-now.com/csm).
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Check the box if you agree, and then click **Install**.

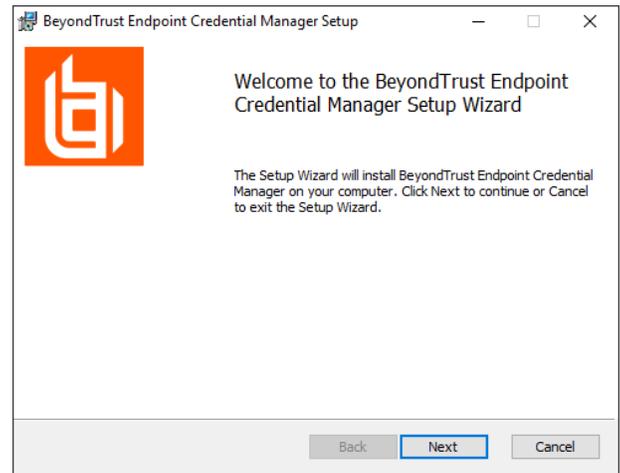
If you need to modify the ECM installation path, click the **Options** button to customize the installation location.



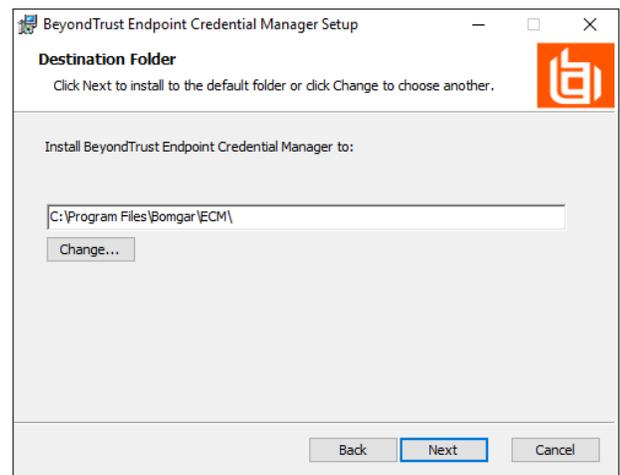
Note: You are not allowed to proceed with the installation unless you agree to the EULA.



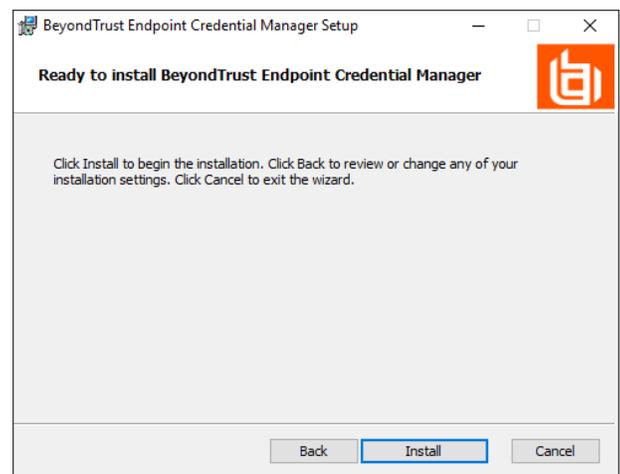
4. Click **Next** on the Welcome screen.



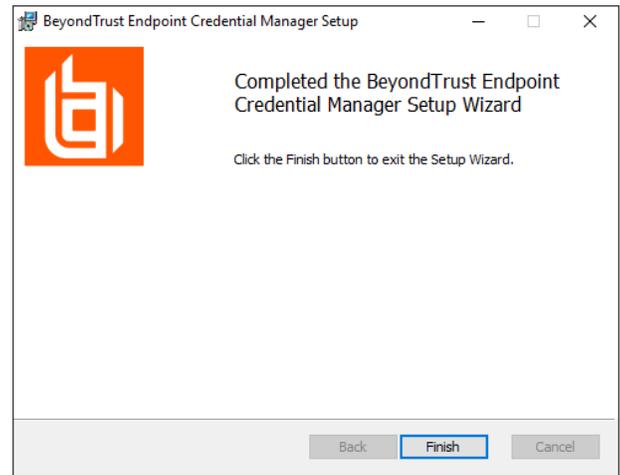
5. Choose a location for the credential manager, and then click **Next**.
6. On the next screen, you can begin the installation or review any previous step.



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



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



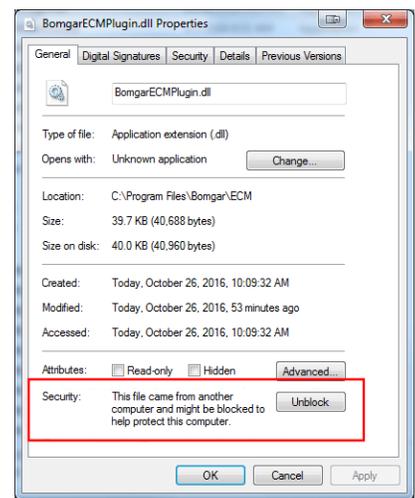
Note: To ensure optimal up-time, administrators can install up to three ECMs on different Windows machines to communicate with the same credential store. A list of the ECMs connected to the appliance site can be found at **/login > Status > Information > ECM Clients**.



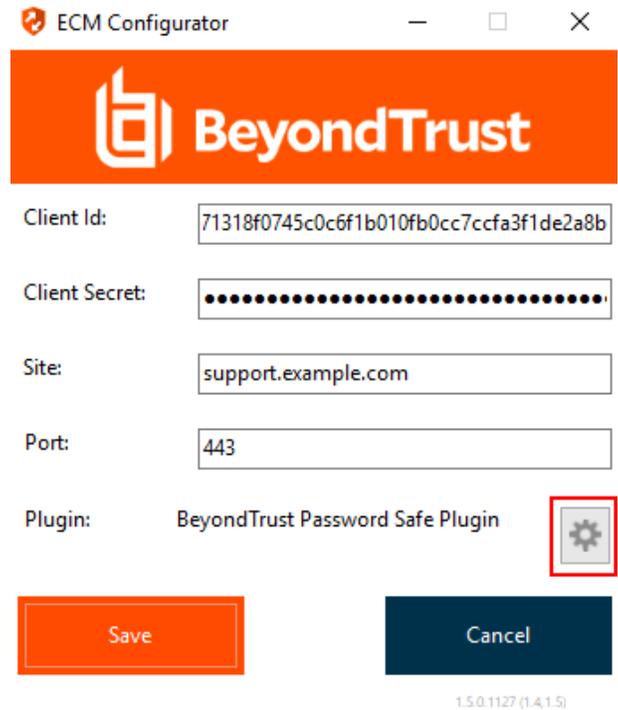
Note: When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Series routes requests to the ECM in the ECM Group that has been connected to the appliance the longest.

Install and Configure the Plugin

- Once the BeyondTrust ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
- Run the **ECM Configurator** to install the plugin.
- The Configurator should automatically detect the plugin and load it. If so, skip to step 4 below. Otherwise, follow these steps:
 - First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
 - On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
 - Repeat these steps for any other DLLs packaged with the plugin.
 - In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL.



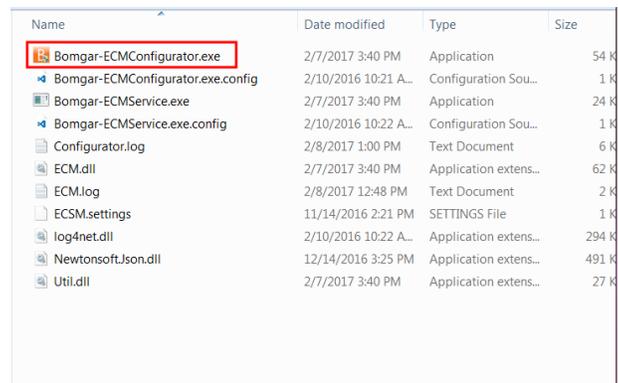
- Click the gear icon in the **Configurator** window to configure plugin settings.



Configure a Connection to Your Credential Store

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

- Locate the BeyondTrust ECM Configurator you just installed using the Windows Search entry field or by viewing your **Start** menu programs list.
- Run the program to begin establishing a connection.
- When the ECM Configurator opens, complete the fields. All fields are required.



Enter the following values:

Field Label	Value
Client ID	The ID for your credential store.
Client Secret	The 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.

Name	Date modified	Type	Size
ECM.dll	2/7/2017 3:40 PM	Application extens...	62 KB
log4net.dll	2/10/2016 10:22 A...	Application extens...	294 KB
Newtonsoft.Json.dll	12/14/2016 3:25 PM	Application extens...	491 KB
Util.dll	2/7/2017 3:40 PM	Application extens...	27 KB

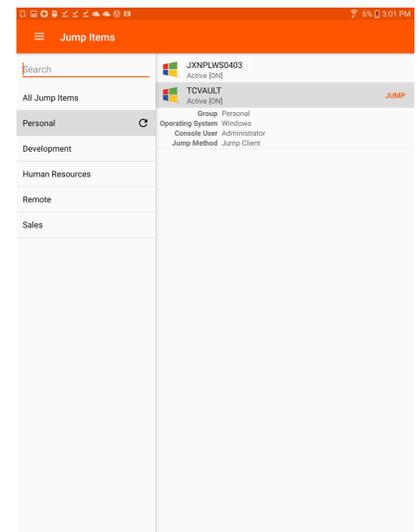


Note: If you are connecting to a password vault, more configuration at the plugin level may be needed. Plugin requirements vary based on the credential store that is being connected.

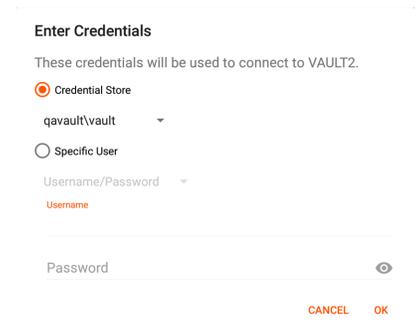
Use Credential Injection to Access Endpoints

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

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

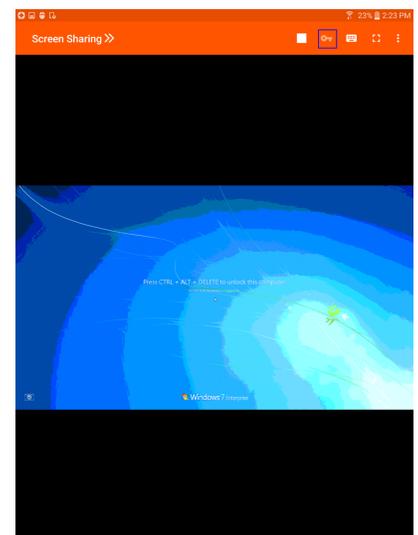
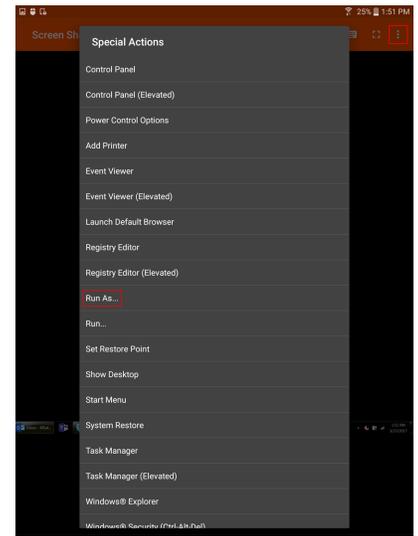


4. The **Enter Credentials** prompt appears. Tap **Credential Store**.
5. Tap the credentials you wish to use to access the system.
6. Tap **OK**.



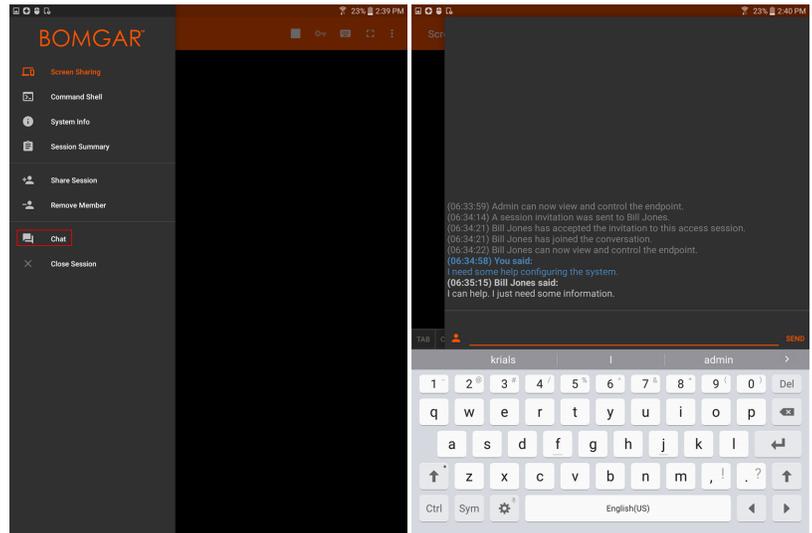
7. From within the session, tap the **Start** button to start screen sharing.
8. Tap the **Special Actions** option. Tap **Run as....**
9. Tap **Windows Security (Ctrl-Alt-Del)**.

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



Use Team Chat to Chat with Other Users in the Android Access Console

By tapping on the **Chat** option, you can chat with other logged-in team members. If you are a member of one or more teams, select whichever team you would like to chat with from the listing. You can chat with all members of that team or select a name from the list of members to chat with just that member.

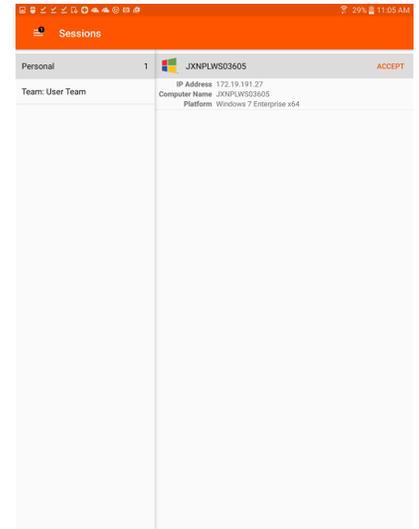


View Access Sessions in the Android Access Console

Within the access console, active access sessions are divided into team queues. When you tap the **Sessions** option on the menu, a listing of all configured queues appear. These queues reflect the teams that have been set up in the /login administrative interface. Once a team is defined, a queue becomes available in the **Sessions** area of the access console. .

The **Personal** queue contains sessions that have been shared with you specifically by another team member. The remaining queues represent specific teams of which you are a member.

Tap a team queue name to view any sessions that are in progress. The number beside the Session option indicates how many sessions are in progress in that queue.

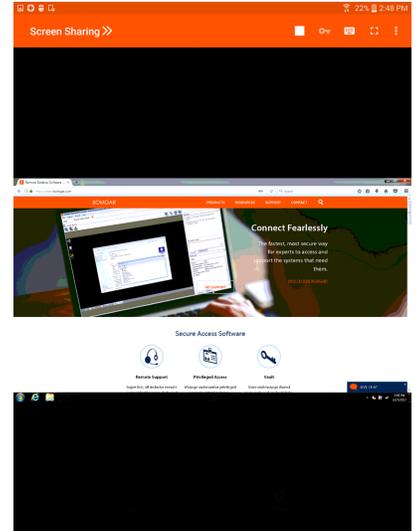


Note: If a session has been shared with you, tap the queue where the session resides. Then tap the session. Select **Accept**. Accepting a session causes it to open on your device.

Screen Share with the Endpoint from the Android Access Console

If screen sharing does not automatically start, touch the **Play** button at the top of the **Screen Sharing** page to request view and control of the remote system. You have full mouse and keyboard control of the remote system, enabling you to work on the remote computer as if you were really there.

- Tap once to left-click.
- Double-tap to double-click.
- Place your finger on the cursor or 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

 	Request or stop screen sharing.
	View additional actions available when screen sharing.
	Access the keyboard in order to type on the remote screen.



Options

Select from additional screen sharing actions and tools.



Full Screen

View the remote desktop in full screen mode.

Additional Screen Sharing Actions and Tools

Special Actions: Perform a special action on the remote system. Based on remote operating system and configuration, available tasks vary.

Paste to Clipboard: Paste items to the clipboard on your device.

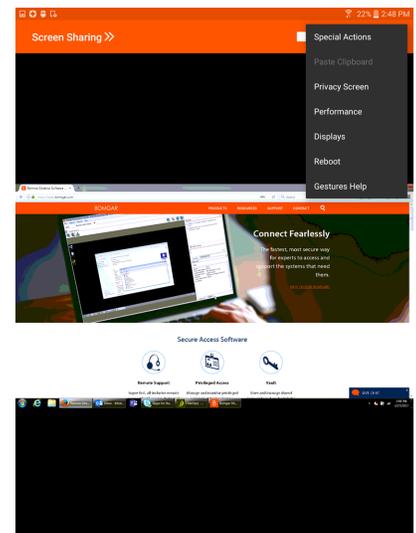
Privacy Screen: Disable the remote user's screen view, mouse, and keyboard input. Restricted endpoint interaction is available only when accessing macOS or Windows computers. Restricted customer interaction is available only when supporting Windows computers. In Windows Vista and above, the endpoint client must be elevated. On Windows 8, this feature is limited to disabling the mouse and keyboard.

Performance: 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.

Displays: Select an alternate remote monitor to display. The primary monitor is highlighted.

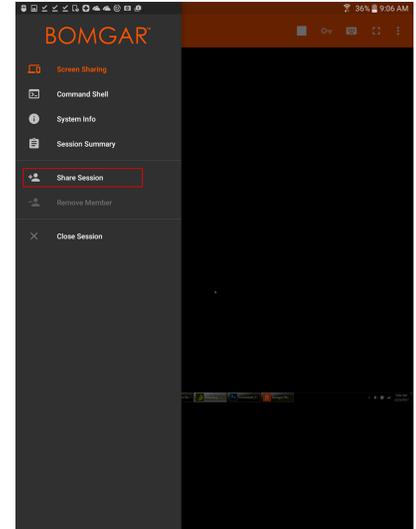
Reboot: Tap to reboot the remote system.

Gestures Help: Tap to receive tips for navigating the mobile access console.



Share a Session with Other Users from the Android Access Console

To share a session with another team member, touch the **Share Session** option from the menu.

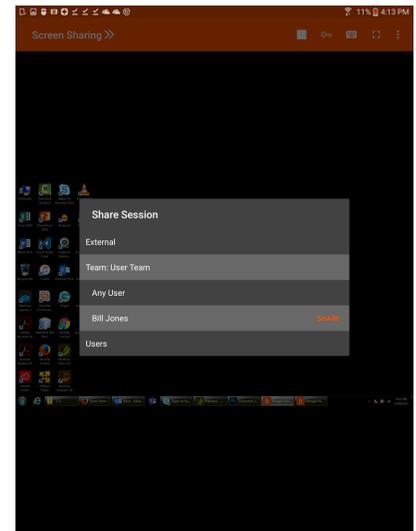


You can select a user listed in the teams displayed to invite them to join the session. You can send multiple invitations if you want more members from the team to join your session. Users are listed here only if they are logged into the access console or if they have extended availability enabled.

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 into the access console or if they have extended availability enabled.

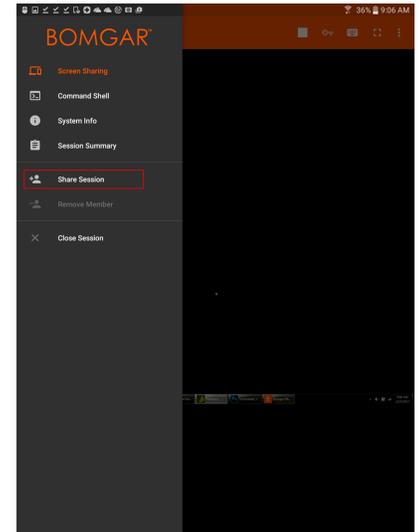
Only the session owner can send invitations. Invitations do not time out as long as you remain the session owner. Multiple active invitations cannot exist for the same user to join the same session. The invitation will disappear if:

- The inviting user cancels the invitation.
- The inviting user leaves the session.
- The session ends.
- The invited user accepts the invitation.

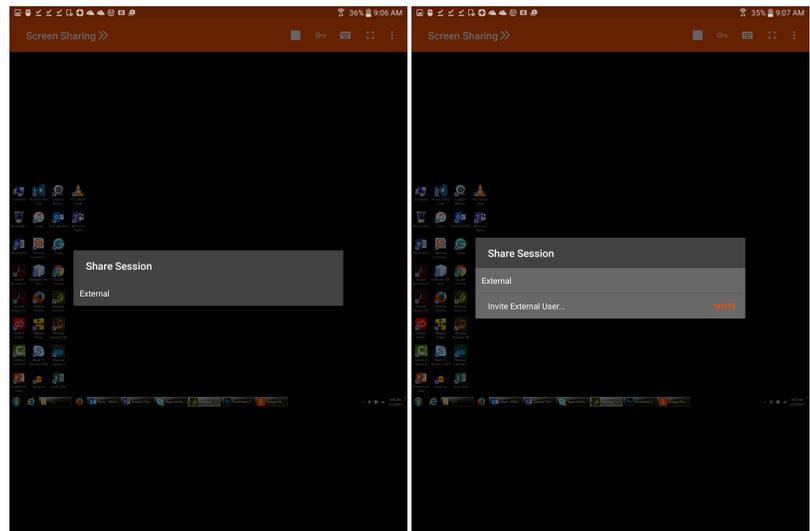


Invite An External User to Join a Session from the Android Access Console

Within a session, a user can request an external user to participate in a session one time only. The inviting user should tap the flyout menu and select **Share Session** menu.

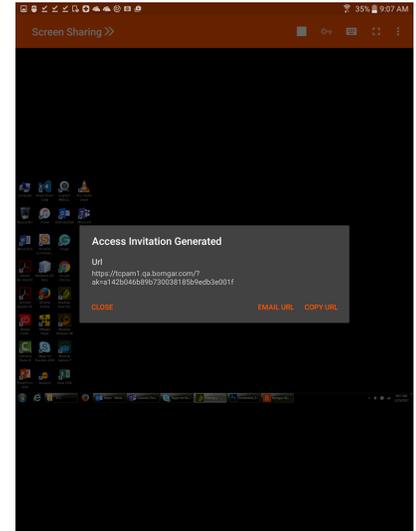


Select **External** and then **Invite External User**. Tap the **Invite** button to proceed.



Next, select a security policy. These policies are created in the administrative interface and determine the level of permission the external user has. When you select a policy, the full description displays below.

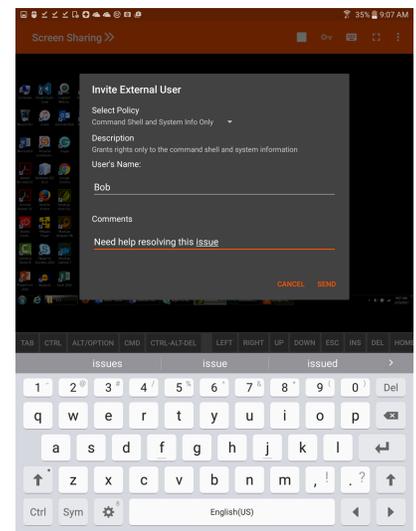
Enter the external user's name. This name appears in the chat window and in reports. Next, enter comments about why this user has been invited. Click **Send**, and a new dialog containing the invitation URL appears.



Depending on the options selected by your administrator, you may be able to send the invitation from your local email or from a server side email. You also can copy and paste the direct URL to the external user. The external user needs to download and run the access console installer, which is an abbreviated process from the full access console installation.

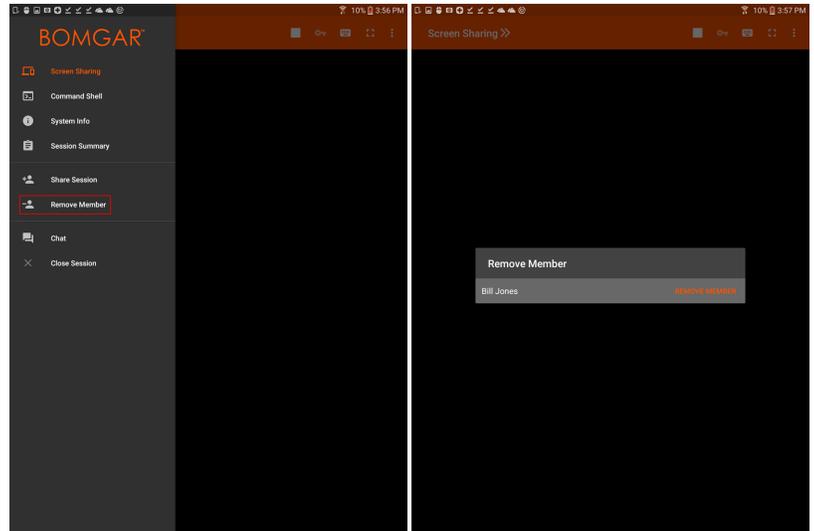
The external user has access only to the **Session** tab and has a limited set of privileges. The external user can never be the session owner. When the inviting user leaves the session, the external user is logged out.

You can invite more than one external user to a session.

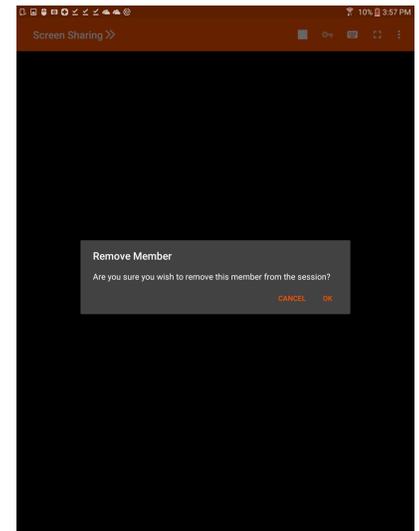


Remove a Member from the Session in the Android Access Console

You can remove another user from a shared session. Touch the **Remove Member** option from the menu.



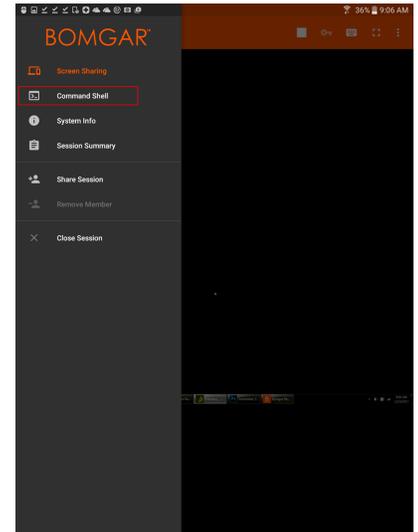
Select the participant you wish to remove. Then touch **Remove**. Tap **OK** on the following prompt. You must be the owner of the session to remove another member.



Open the Command Shell on an Remote Endpoint Using the Android Access Console

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

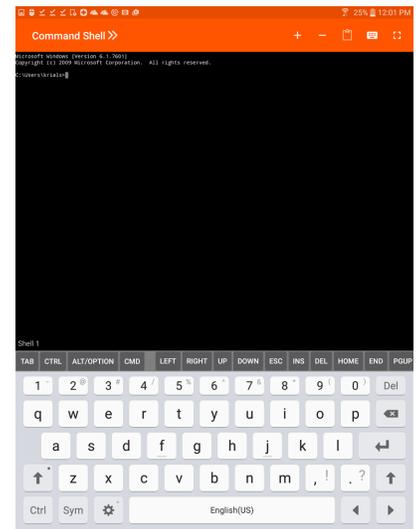
To access command shell, select **Command Shell** from the menu. Tap the **+** icon to open a new shell.



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. A set of additional keys 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.

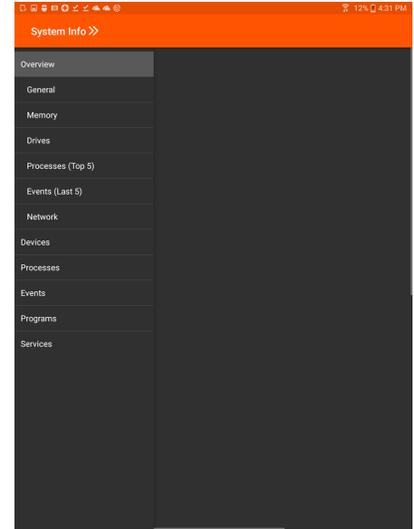


Command Shell Tools

	Open a new shell to run multiple instances of command prompt.
	Close the current command shell. Other open command shells continue to run.
	Access the keyboard to type commands in the command shell.
	Access the command shell menu to perform additional actions, such as viewing other shell sessions and toggling to full screen.

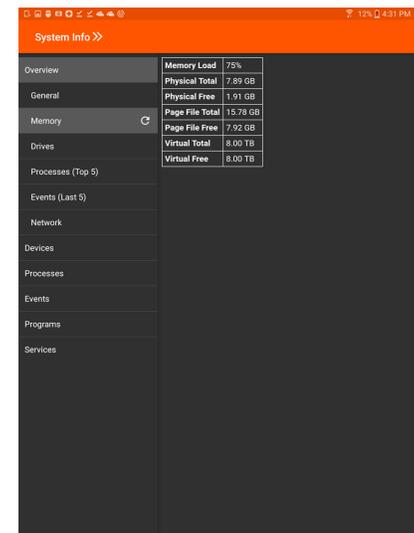
View Endpoint System Information from the Android Access Console

Users may view a complete snapshot of the endpoint'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.



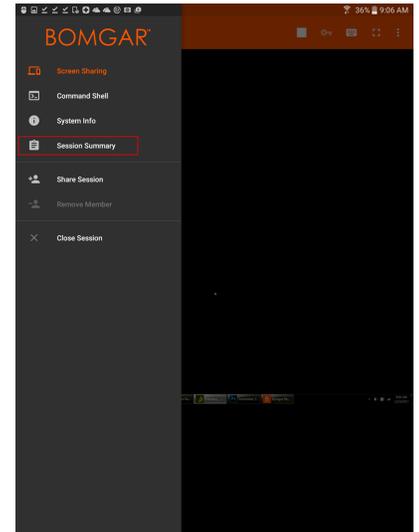
Select successive category names to access the data you wish to view.

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

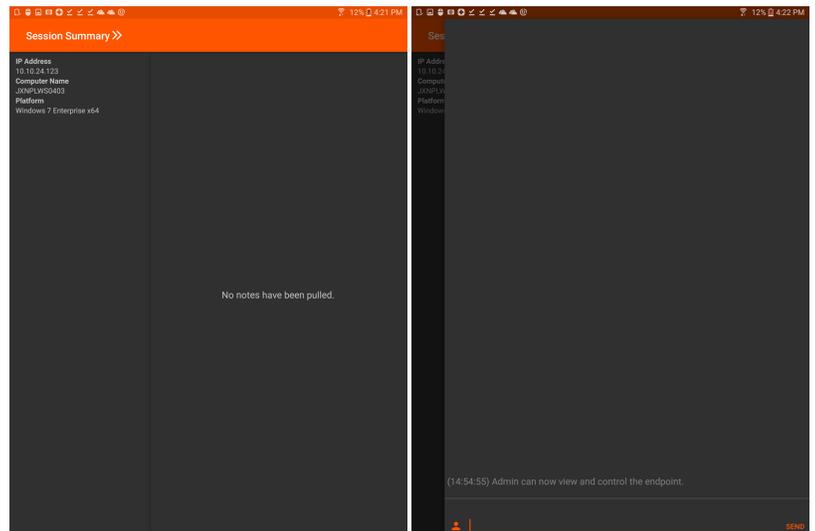


View a Summary of the Access Session and Add Notes from the Android Access Console

The **Summary** page gives an overview of the remote system being accessed.

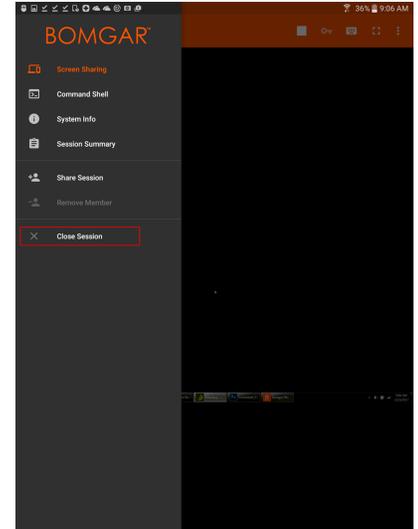


You can also add notes about the session by swiping left across the screen. Notes can be submitted by one user and recalled by another user for review. These notes are also available in the session report.



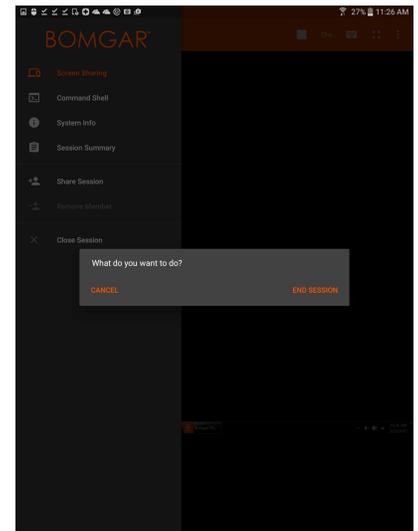
Close the Session in the Android Access Console

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



If you are the session owner, **End Session** closes the session page in your access console and removes any additional members who may be sharing the session.

If you are not the session owner, touching **Leave Session** removes you from the session. The session continues to be supported by the session owner. If any additional members are sharing the session, they remain in session.



Manage and Deploy Access 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](https://intune.microsoft.com/) 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](https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android) at <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android>.