BeyondTrust

Remote Support
iOS Rep Console 3.1.3

TC:8/10/2023

Table of Contents

Representative Console for iOS

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 iOS device and understand the features of the iOS 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.

Install the Representative Console on iOS

The BeyondTrust representative console for iOS is available for free download from the Apple App Store. From your iOS device, search the App Store for "BeyondTrust Representative Console" and then install the app.

If your company uses an Enterprise App Store to distribute apps, contact BeyondTrust Technical Support to make the BeyondTrust representative console app available through your Enterprise App Store.

To run the BeyondTrust representative console on your device, your iOS device must be running iOS 14+.

Note: *Only the BeyondTrust representative console can be used with a Remote Support 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 iOS representative console. 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 representative console on your device to provide remote support from virtually anywhere.

Configure Mobile Device Management for Apple iOS

BeyondTrust supports management of iOS 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.

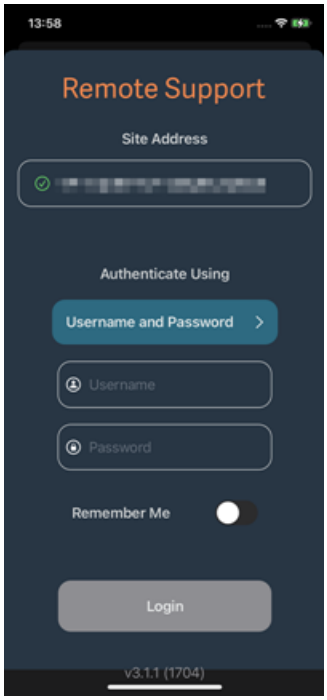
The method by which you configure your profile will vary depending on your MDM product. Consult your MDM documentation for exact steps.

Below are the configurable keys that you will need to add to your MDM payload:

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.

Log in to the Representative Console for iOS

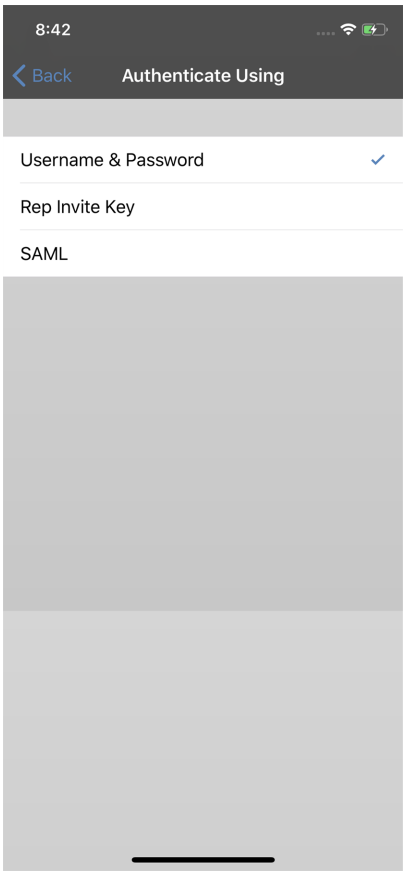
From the login screen, enter your BeyondTrust site hostname, such as support.example.com. Enter the username and password associated with your BeyondTrust user account. You can choose to have the BeyondTrust representative console remember your login credentials. Tap **Login**.



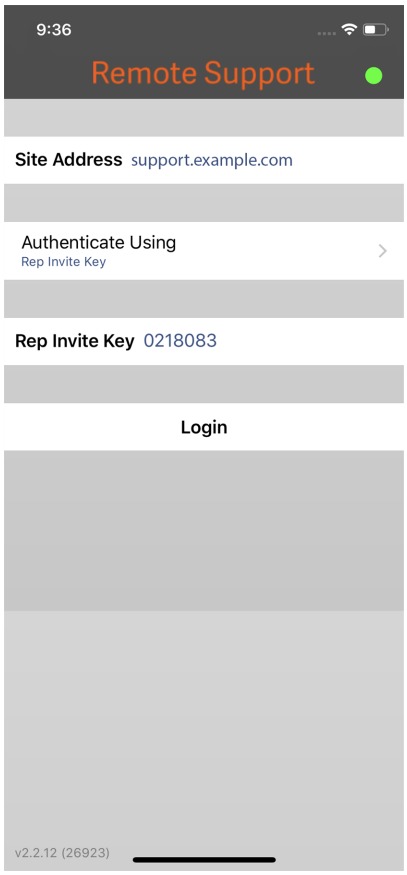
> ***Note:*** *If you are using a local account and two-factor authentication has been enabled for it, enter the email code you have received. If you enter the email code incorrectly three consecutive times, you must re-enter your credentials and get a new email code.*

> ***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.*

Alternatively, if you have been invited by another representative to join a session one time only, tap **Authenticate Using** and select **Rep Invite Key**.



Enter the rep invite key provided with your invitation and then tap **Login**.



Authentication Methods for the Remote Support iOS Representative Console

Log in to the iOS Representative Console Using Face ID

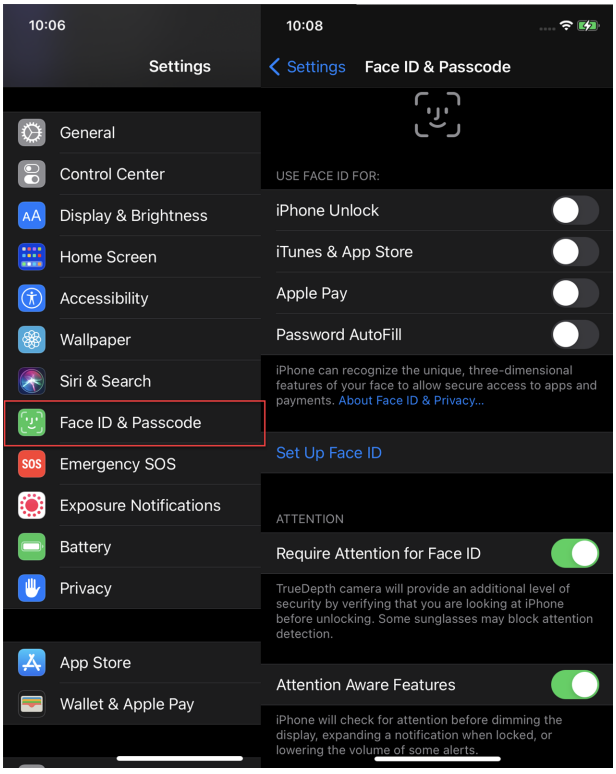
Face ID is a face recognition system found on the following iOS devices:

- **iPhone X, XR, XS, XS Max, 11, 11 Pro, 11 Pro Max, 12, 12 mini, 12 Pro, 12 Pro Max, 13, 13 mini, 13 Pro, 13 Pro Max**
- **iPad Pro 12.9** (3rd and 4th generation)
- **iPad Pro 11** (1st and 2nd generation)

Face ID allows you to unlock your device or authorize other actions on your iPhone or iPad using visual recognition as a passcode.

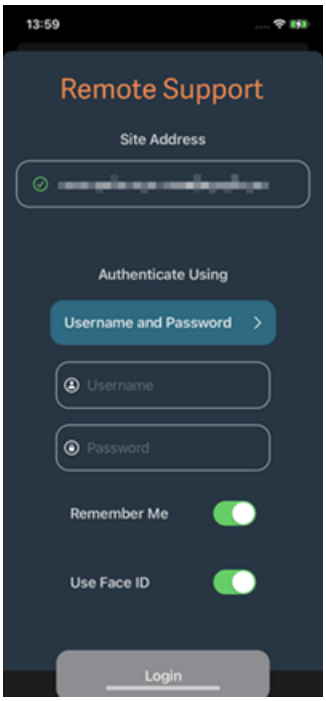
To set up **Face ID** on your device:

1. Go to **Settings > Face ID & Passcode**.
2. Select which devices and features you want to use **Face ID** for.
3. Check the **Require Attention for Face ID** and/or **Attention Aware Features** if you require those extra features.



4. Open the **BeyondTrust Mobile Representative Console** app.
5. Enter your BeyondTrust site hostname, such as **support.example.com**, as well as your credentials.

6. Verify that the **Remember Me** option is enabled.
7. Toggle the **Use Face ID** button to enable the feature.
8. Tap the **Login** button to finish logging into the representative console.

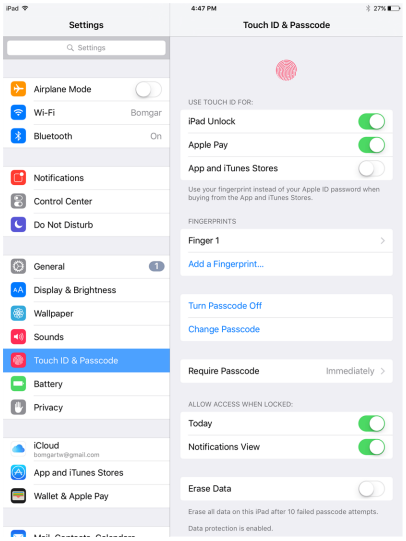


> *For more information about Face ID and how to enable it on your device, please see the following:*
>
> - *About Face ID advanced technology at https://support.apple.com/en-us/HT208108*
> - *Use Face ID on your iPhone or iPad Pro at https://support.apple.com/en-us/HT208109*

Log in to the iOS Representative Console Using Touch ID

Touch ID is the fingerprint identity sensor found in the following iOS devices:

- **iPhone 5s, 6, 6 Plus, 6s, 6s Plus, 7, 7 Plus, 8, 8 Plus, SE (all generations)**
- **iPad with a Home button**
- **iPad Air 4 or later**
- **iPad mini 6**



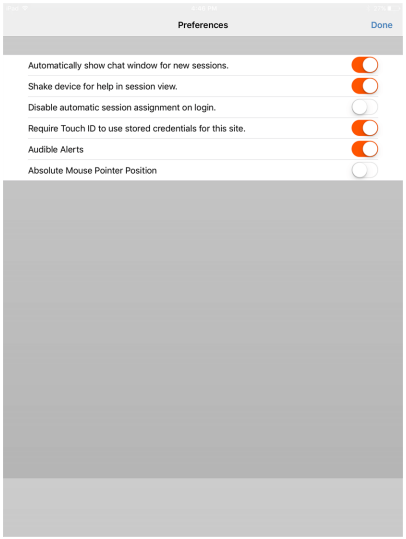
With this feature, you can unlock your device or authorize other actions on your iPhone or iPad using your fingerprint as a passcode.

If you are using one of the devices listed above, you can use **Touch ID** to log in to the mobile representative console.The same fingerprint authentication used to unlock your device can be used to gain entry into your representative console. Follow the steps below to enable Touch ID authentication for your mobile representative console.

1. Open the **BeyondTrust Mobile Representative Console** app.
2. Enter your BeyondTrust site hostname, such as **support.example.com**, as well as your credentials.
3. Verify that the **Remember Me** option is enabled.
4. Tap **Yes** on the Touch ID prompt that appears upon login.
5. Tap the **Login** button to finish logging into the representative console.

> ***Note:** At any time, you can log in using your username and password by tapping **Back to Login**.*

Note: *From the* ***Preferences*** *section of the mobile representative console, you can turn off the Touch ID functionality by disabling the* ***Require Touch ID to use stored credentials for this site*** *option.*



For more information about Touch ID and how to enable it on your device, please see the following:

- *About Touch ID security on iPhone and iPad at https://support.apple.com/en-us/HT204587*
- *Use Touch ID on iPhone and iPad at https://support.apple.com/en-us/HT201371*

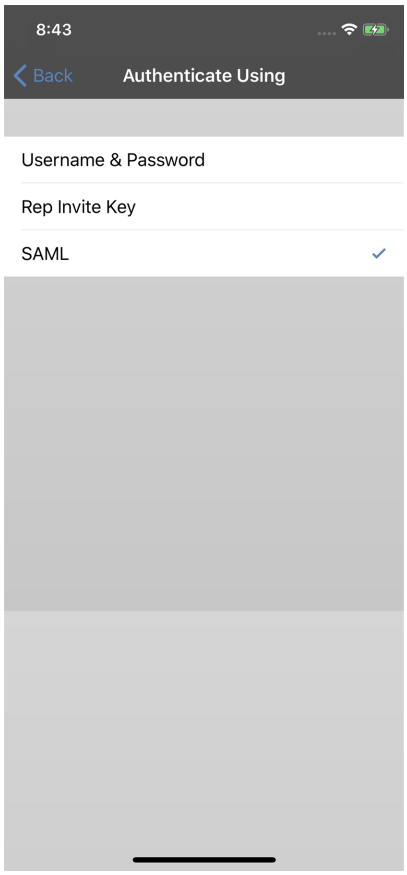
Log in to the iOS Representative Console Using SAML for Mobile

SAML for mobile provides an easy and secure method for authenticating to the mobile iOS representative console. Follow the steps below to log in to the mobile representative console using SAML.

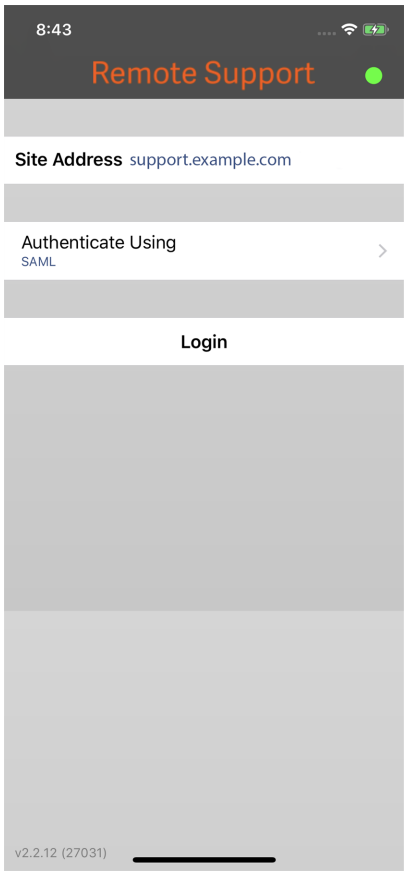
Note: *Before attempting to log in to the iOS representative console using SAML, verify that a SAML provider has been configured for your* ***/login*** *administrative environment by going to* ***Users & Security > Security Providers****. If SAML is not configured in* ***/login****, SAML is not available as an authentication method for the iOS rep console. 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 iOS device.
2. From the login screen, tap **Authenticate Using**.

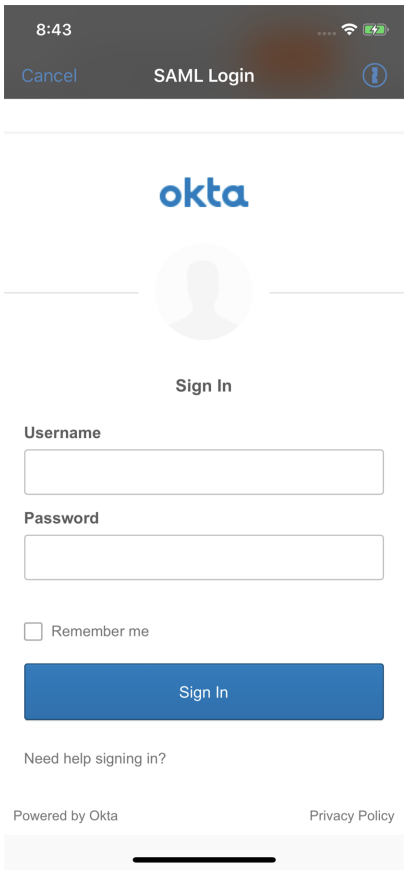
3. Select **SAML**.



4. Tap **Login**. You are then presented with your SAML provider's page.



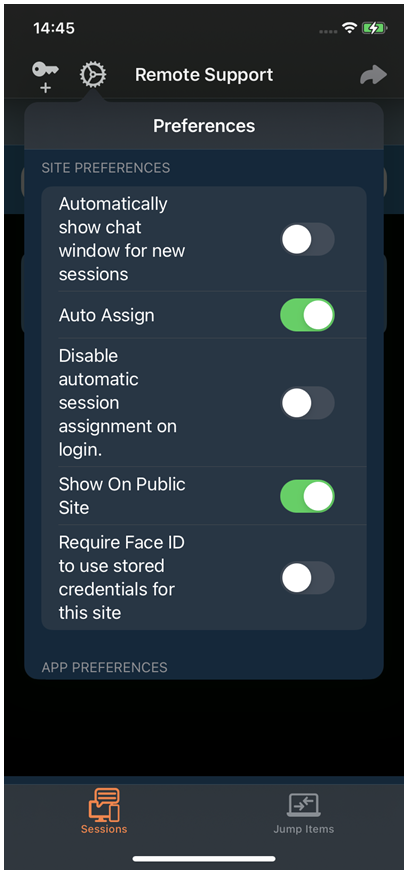
5. On your provider's page, enter your credentials.
6. Tap **Log In** to access the representative console.



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

Change Preferences in the iOS Rep Console

To change your preferences, tap the gear icon in the upper-left corner of the screen. It may be necessary to scroll down to see all the preferences.



Toggle preferences to enable or disable. Availability of some preferences depends on your device and your permissions. Preferences are organized by category.

Site Preferences

Auto Assign allows you to enable or disable auto assignment. You must have the user permission to opt out of session assignments for this option to be available. Auto assignment is used with Equilibrium to route a session to the representative best qualified to handle the issue.

You can choose if your display name should appear in the list of logged in representatives on the public site.You also can log out of the representative console.

> *For more information about Equilibrium and session assignment, see the following:*
>
> - *"View Queued Support Sessions in the iOS Rep Console" on page 20*
> - *Equilibrium for Automatic Session Routing at www.beyondtrust.com/docs/remote-support/how-to/equilibrium/.*

App Preferences

The **Audible Alerts** preference allows you to play audible alerts for certain events that occur within the representative console.

Mouse Pointer Preferences

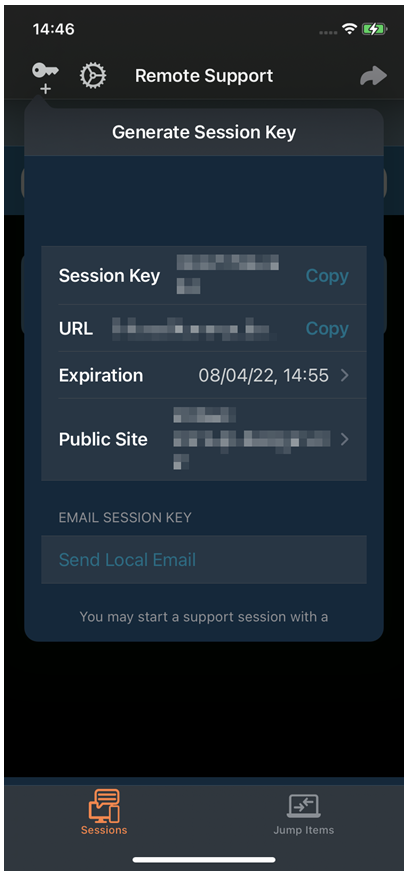
If **Absolute Mouse Pointer Position** is turned off, you must place your finger on the mouse pointer and drag to move the mouse. Tap and hold to locate the mouse pointer when absolute positioning is turned off. If it is turned on, you can place the mouse pointer wherever your finger touches the screen. When absolute positioning is turned on, tap and hold to open a fly-out menu from which you can choose to left-click, right-click, or double-click. Traditional click methods still apply.

> *For more information about Equilibrium and session assignment, see the following:*
>
> - *"View Queued Support Sessions in the iOS Rep Console" on page 20*
> - *Equilibrium for Automatic Session Routing at www.beyondtrust.com/docs/remote-support/how-to/equilibrium/.*

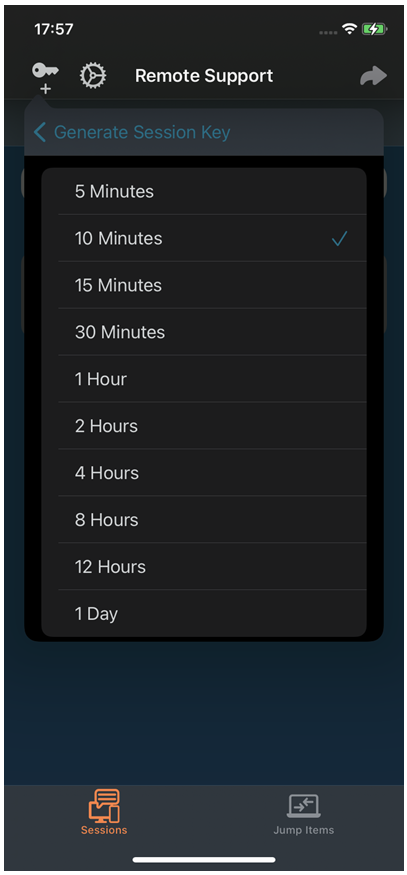
Generate a Session Key to Start a Support Session in the iOS Rep Console

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.

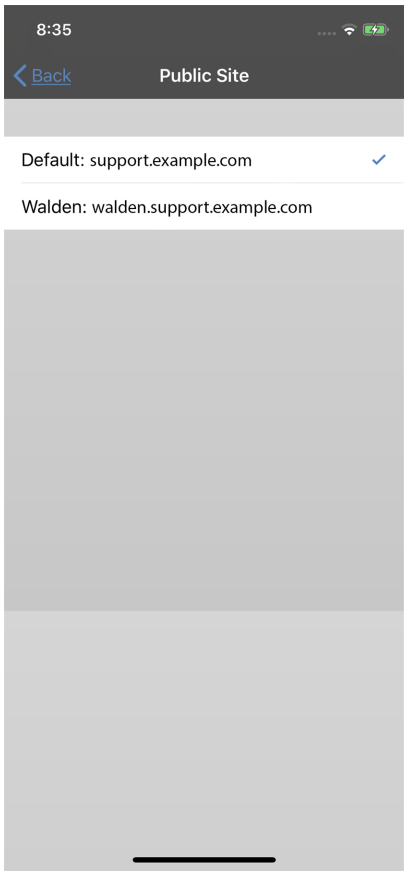
On your iPhone, tap the key icon at the top of the screen and then the **Generate Session Key button**. This opens a **Generate Session Key** menu from which you can edit the session key details.



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.



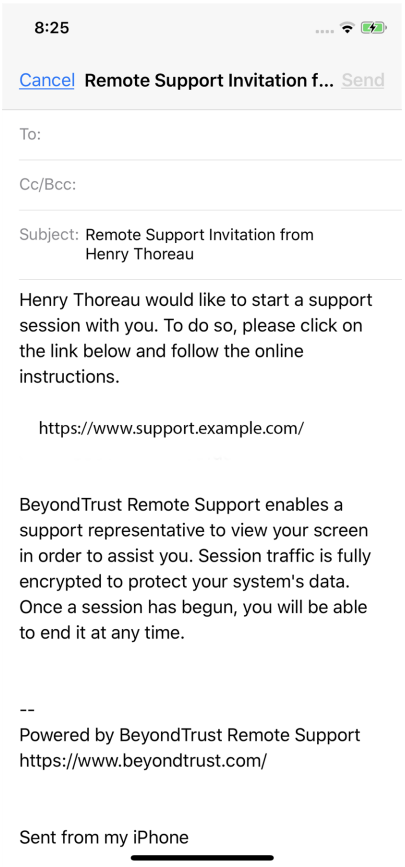
You can also select the public portal through which you want your customer to enter the session.



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.

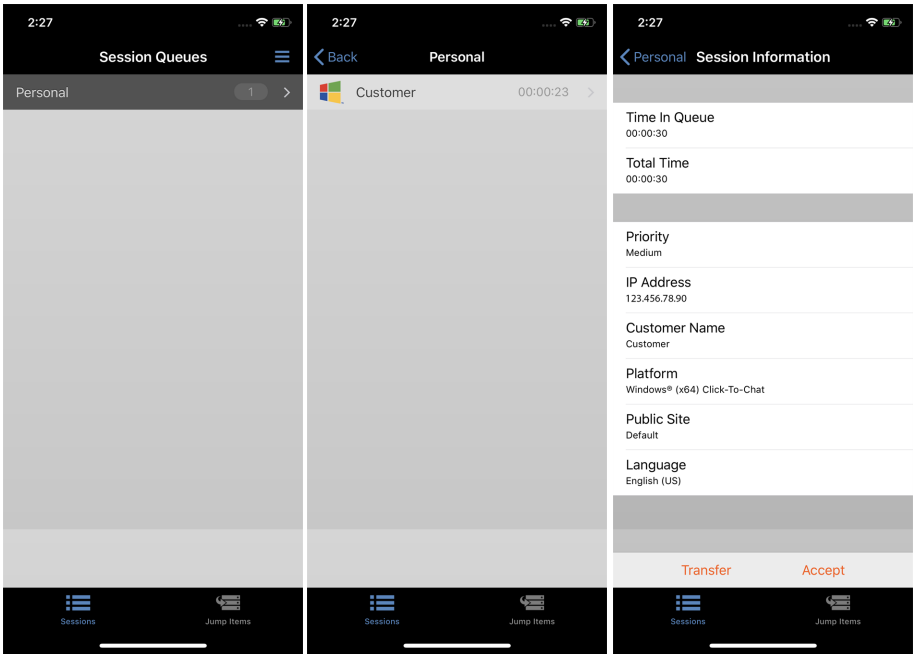
You can also send your customer an email invitation that contains the unique URL.

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



View Queued Support Sessions in the iOS 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.

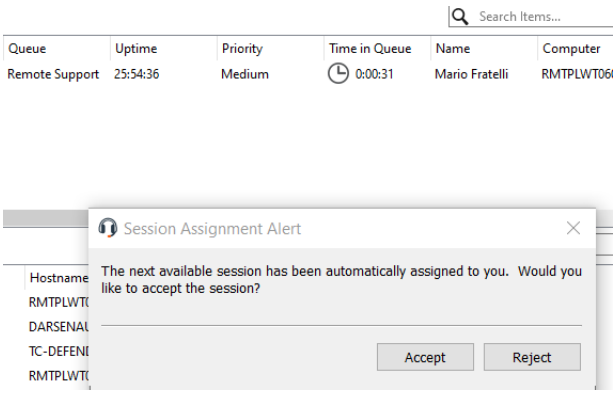
If allowed to use the feature, start supporting the oldest queued session from among your team queues by selecting the next session from the **Get Next** button.

View Sessions

Tap a queue name to view its sessions. Tap a session entry to view details about the support request. To begin supporting the selected session, tap 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.

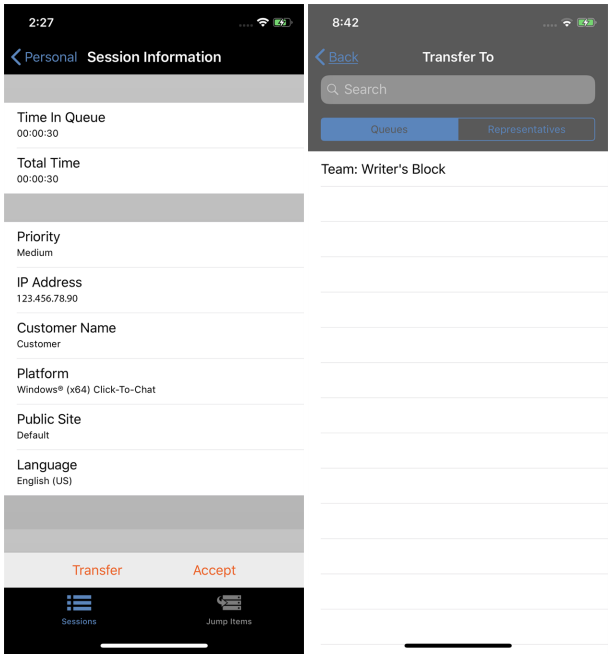
Alternatively, if your administrator has set up a waiting session rule for this queue, the session gives out an audible alert when it is overdue, or it is transferred to an overflow queue. If that overflow queue has a waiting session rule set up that transfers the session back to the first queue, the 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.

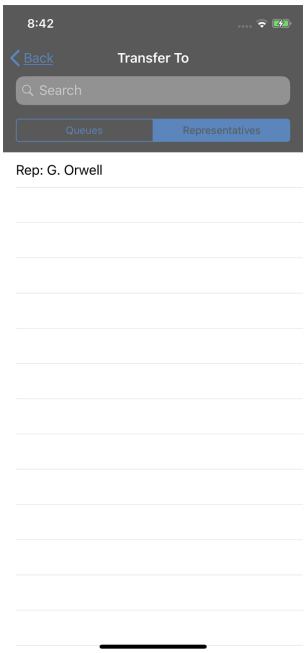
> *For more information about changing the rep console settings and preferences, please see "Change Preferences in the iOS Rep Console" on page 15.*

Session Transfer

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

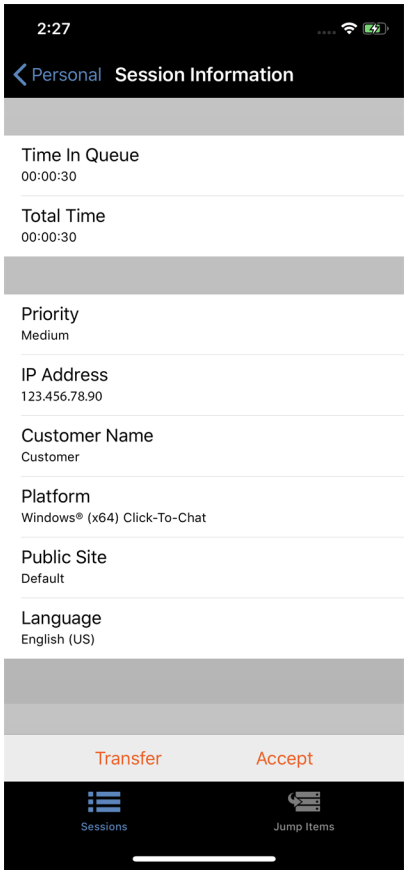


You may also transfer a session to another representative's personal queue. Tap the **Representative** button at the top of the menu. Locate the representative by browsing or searching, and select their name. Then tap the **Transfer** button.



Return to an Active Session in the iOS Representative Console

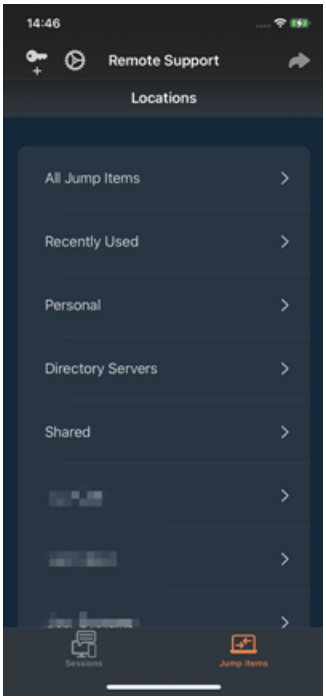
To return to a session you are already supporting, open your personal queue and select the session you wish to support. On an iPhone, tap **Accept**.



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

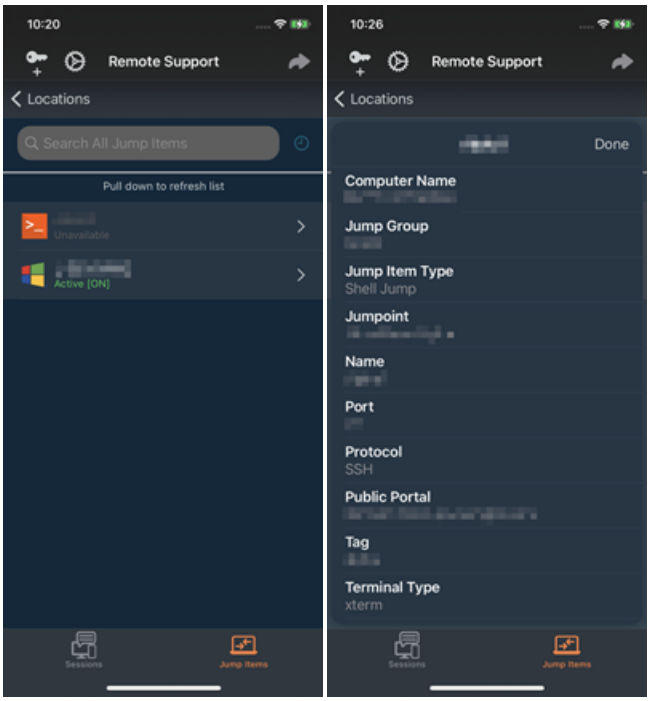
> ***Note:*** *If you need to access Jump Items when no user is available, make sure the session permissions are set either to disable prompting or to default to* ***Allow*** *for unattended sessions.*

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, select a location. 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.

Tap 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.



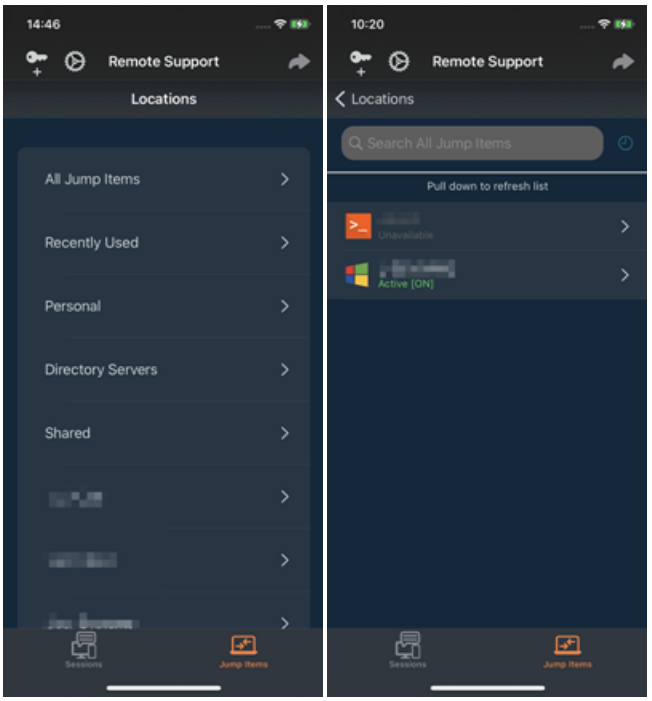
Use Jump Shortcuts to Access Unattended Computers from the iOS Representative Console

To access an individual computer without end-user assistance, install 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**

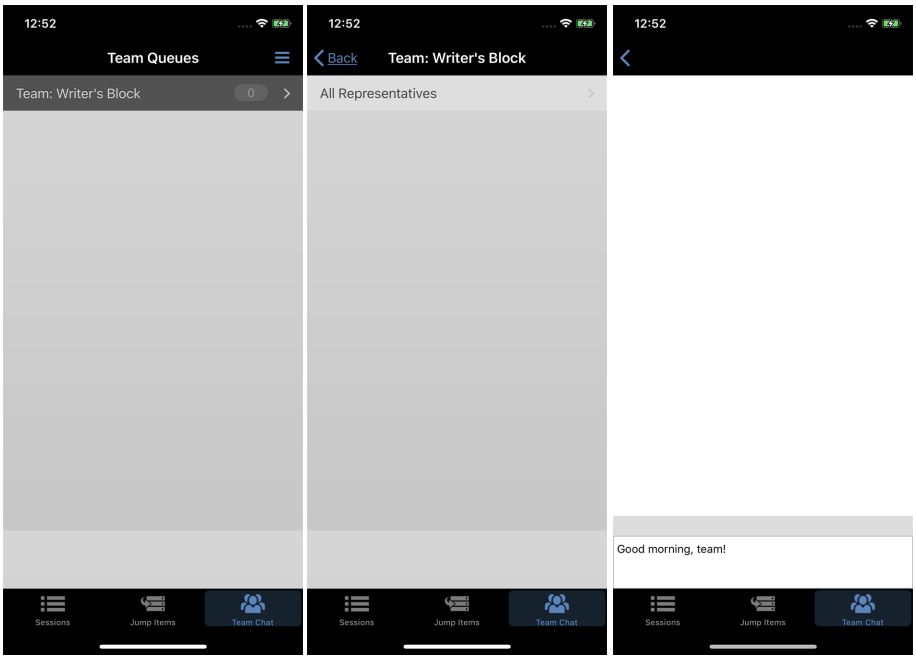
Jump Shortcuts are grouped according to who can access them — only the user who created them or members of a particular Jump Group.

1. To locate a Jump Shortcut, tap on the **Jump Items** at the bottom of the screen.
2. Select a location and touch the **Refresh** button.
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 iOS 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.



Monitor Team Members in the Dashboard

The dashboard feature enables privileged users to view and monitor ongoing sessions, enabling administrative oversight to help manage staff. Based on roles assigned from the **Support Teams** page of the administrative interface, team leads can monitor team members of a given team, and team managers can monitor both team leads and team members of that team.

If a user is a team manager or team lead of one or more teams, the dashboard pane appears beneath the queue selection pane on the **Home** tab of the console. This pane displays any logged-in team members of a lower role for the selected team.

Select a user from the dashboard pane to view any sessions they may be running. A Team Manager or Team Lead can take over a support session from another representative of that team by selecting the appropriate session from the queue and tapping the **Take Over** button. This transfers ownership of that session to the team manager or team lead, with the original user remaining in the session as a participant. A team manager or team lead can also transfer ownership of a support session from one user to another user or team.

It is also possible for a team manager to join a session in progress by clicking the **Join** button. The behavior is similar to joining a session via session invitation, except that no invitation is required.

Note: *The team lead can join or take over a team member's session only if the team lead has start session access to the Jump Item that was used to create the session, or the dashboard setting to allow join or take over without start session access is checked.*

Additionally, if configured in the **/login** interface, a team manager or team lead can monitor team members of a lower role even if there are no ongoing sessions, as long as those users are logged into the console.

A monitoring icon can be displayed in the corner of the user's desktop to indicate that monitoring is taking place. When the user moves the cursor near this icon, it moves to another corner to prevent obscuring the screen. Select the user whose screen you wish to view and then tap the **Monitor** button. This opens a new page in your console, displaying either the user's entire computer screen or only the console, depending on the administrative settings.

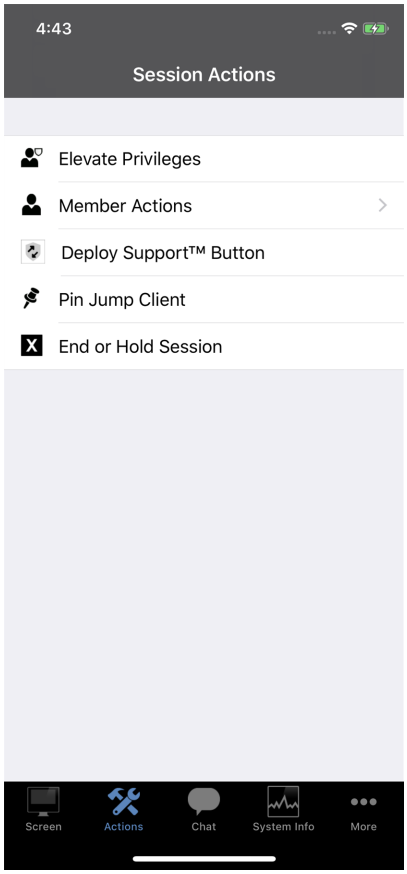
Within a team, a user can administrate only others with roles lower than their own.

Note: *Roles apply strictly on a team-by-team basis so that a user may be able to administrate another user in one team but not be able to administrate that same user in another team.*

Support Session Actions in the iOS Rep Console

When you first begin a support session, a new screen will open.

To access session actions on an iPhone, tap the **Menu** button at the top of the screen.

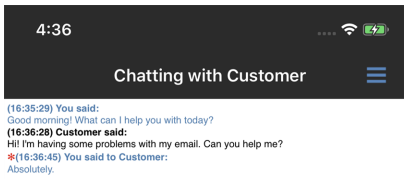


Support Session Actions

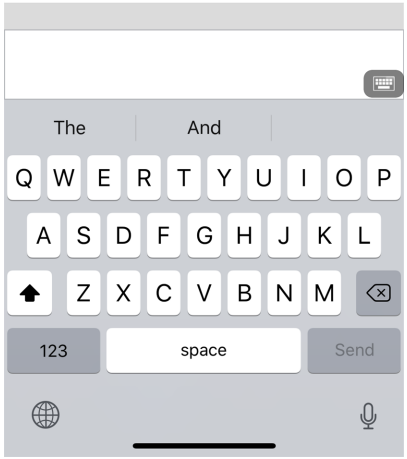
	Elevating the customer client enables switching user accounts, deploying Jump Clients in service mode, and controlling protected windows and UAC dialog boxes. Elevation does not change the user context of the active user and is not the same as logging out the active user and logging back in as an administrator. 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.
	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.
 	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.
 	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 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 Customer During a Session in the iOS 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.

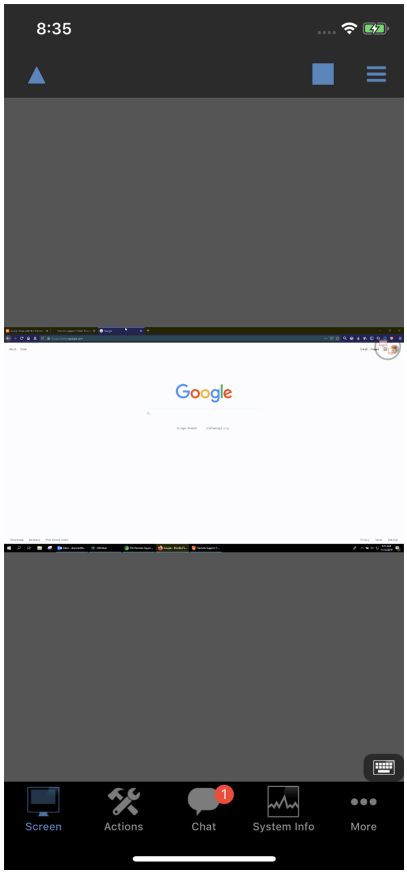


If you receive a message while chat is closed, the chat icon will display the number of messages waiting. On an iPad, the icon will also flash. Tap the chat button to open or close the chat area.



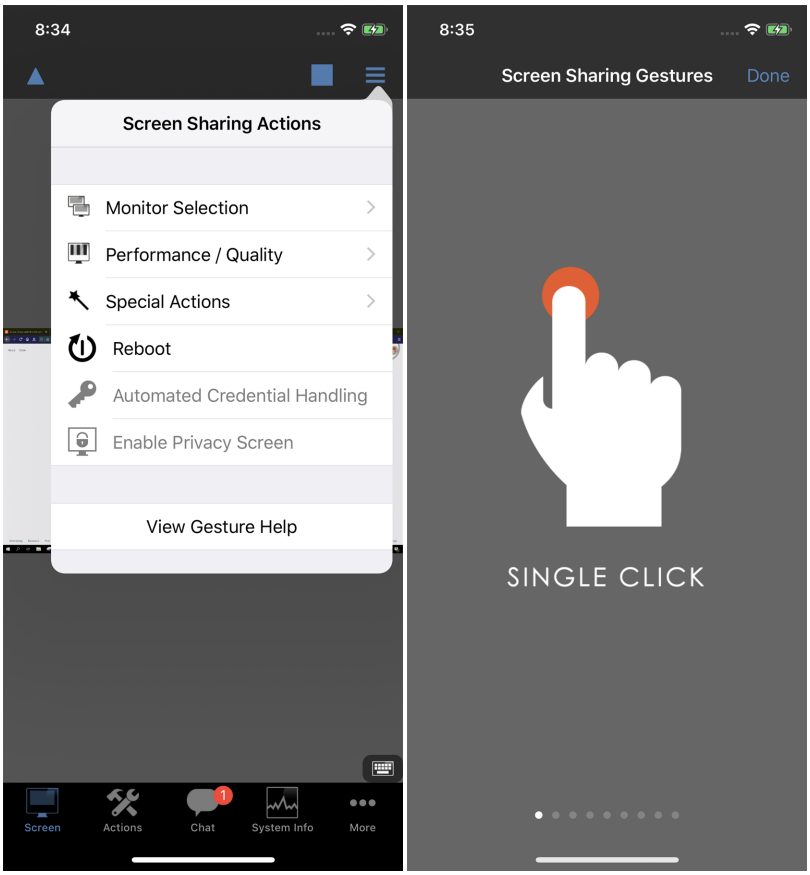
Screen Share with the Remote Computer from the iOS Rep Console

From the **Screen Sharing** page, tap the play button 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.
  OR
  If absolute mouse pointer position is turned on in your settings, place the mouse pointer wherever your finger touches the screen.
- 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.
  OR
  If absolute mouse pointer position is turned on in your settings, tap and hold to open a fly-out menu from which you can choose to left-click, right-click, or double-click.

On an iPhone, to access more screen sharing tools, tap the **Menu** button in the upper right corner of the screen. Tap **View Gesture Help** for a quick reference of screen sharing gestures.



Screen Sharing Actions

 	Request or stop screen sharing.
	Select an alternate remote monitor to display. The primary monitor is designated by a **P**.
	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.
	Reboot the remote computer without losing your connection to the support session.
	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.

	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**. Restricted customer interaction is available only when supporting macOS or Windows computers. In Windows Vista and above, the customer client must be elevated. On Windows 8, privacy screen is not available, and the representative can only disable the mouse and keyboard.
	Access the keyboard in order to type on the remote screen.

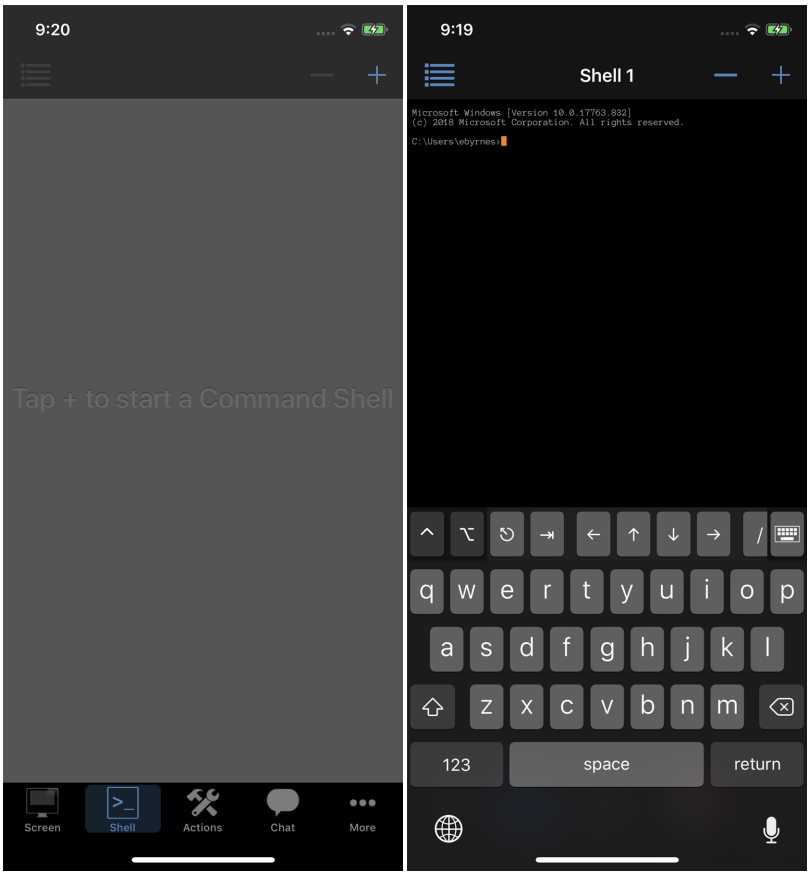
Open the Command Shell on the Remote Endpoint Using the Apple iOS Representative Console

Remote command shell enables reps to open on a virtual command line interface on remote system. 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 (highlighted in the image) 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.

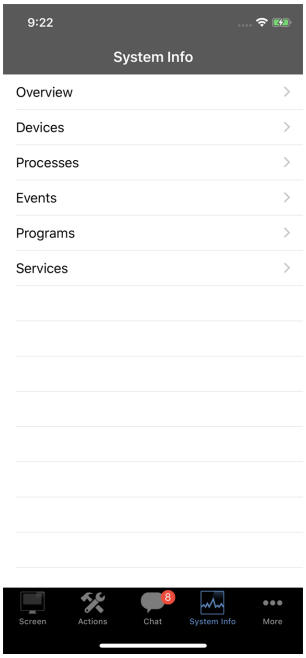


Command Shell Tools

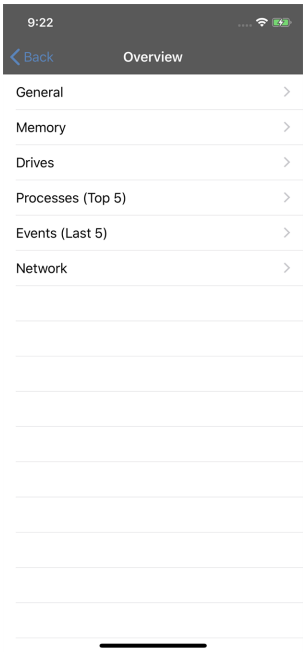
	Open a new shell to run multiple instances of command prompt.
	Close the current command shell. Other open command shells will continue to run.
	Close all open command shells.
	Display a list of currently open command shells. Tap an item in the list to access the corresponding command shell.

View Remote System Information from the iOS 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.



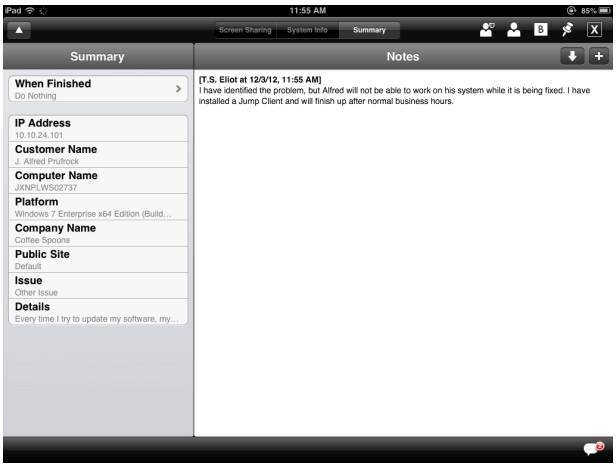
Select successive category names to access the data you wish to view. To return to the previous category, tap the **Back** button.



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

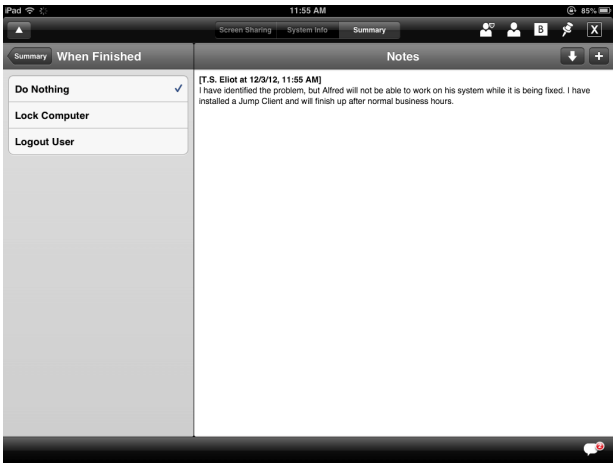
View a Summary of the Support Request and Add Notes from the iOS Rep Console

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.

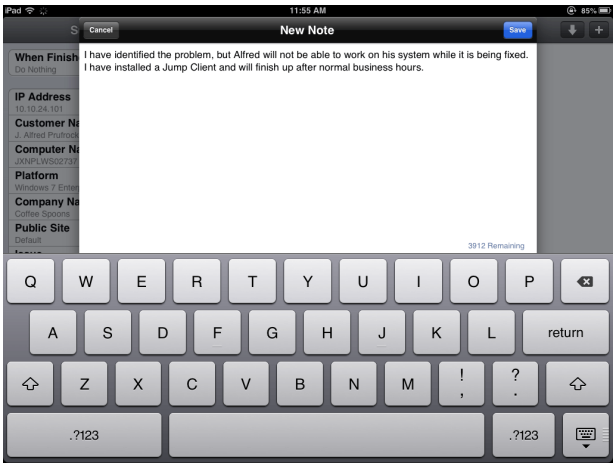
Tap **When Finished**, and then select the action to take at the end of the session.

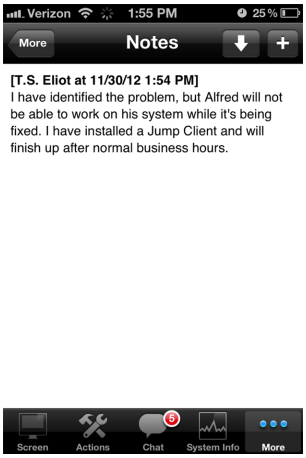


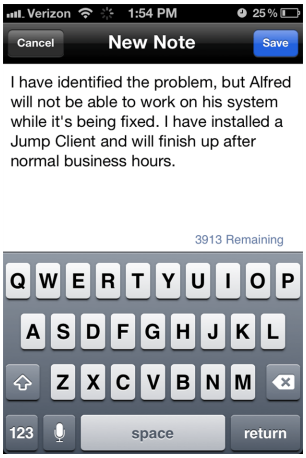
You can also add notes about the session. On an iPhone, you must first select the **Notes** page. If the session is shared or transferred, these notes can be submitted by one representative and pulled by another for a quick, private review of the situation. These notes are also available in the session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

To add a note, tap the **Add** button. When finished, tap **Save**.

To pull another representative's notes on the session, tap the **Pull** button.





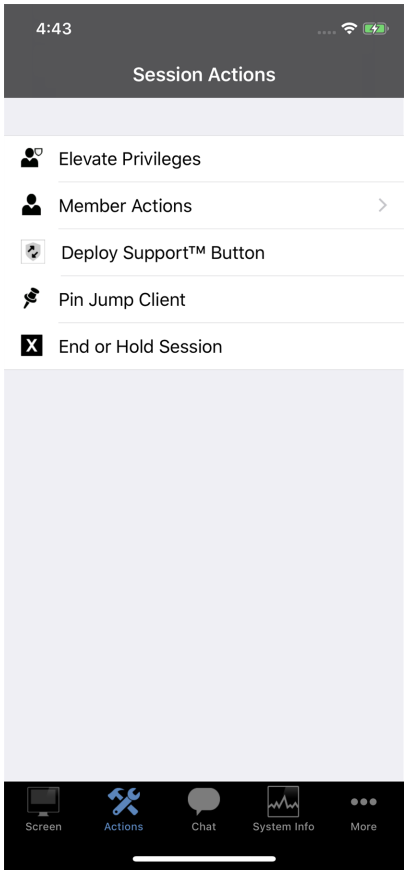


Elevate Rights in the Customer Client from the iOS Representative Console

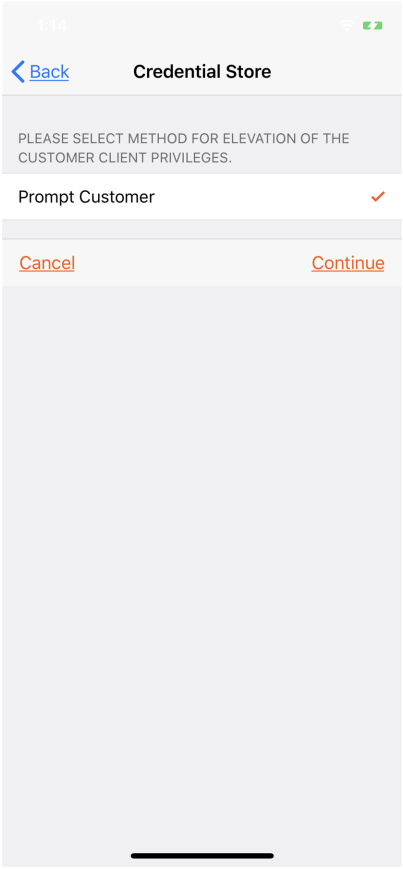
When a session starts in click-to-chat mode, only chat is available. If you wish to have access to more robust support features such as screen sharing, you must elevate the customer client.

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.

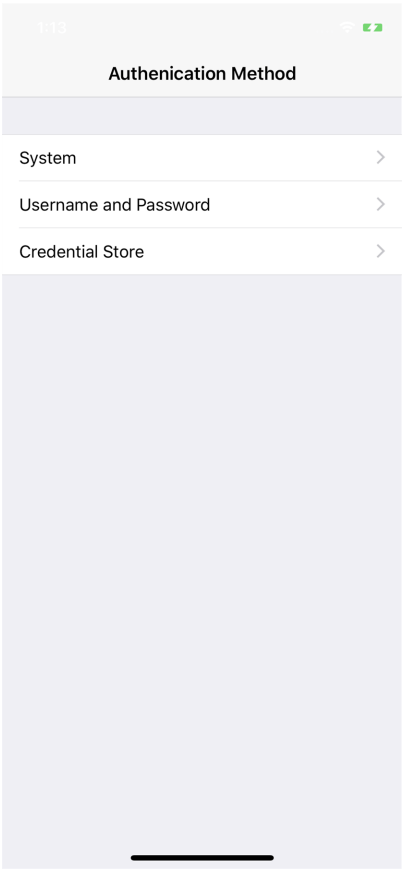
To elevate the customer client, tap the **Elevate** button. On an iPhone, access this button by tapping the **Menu** button first.



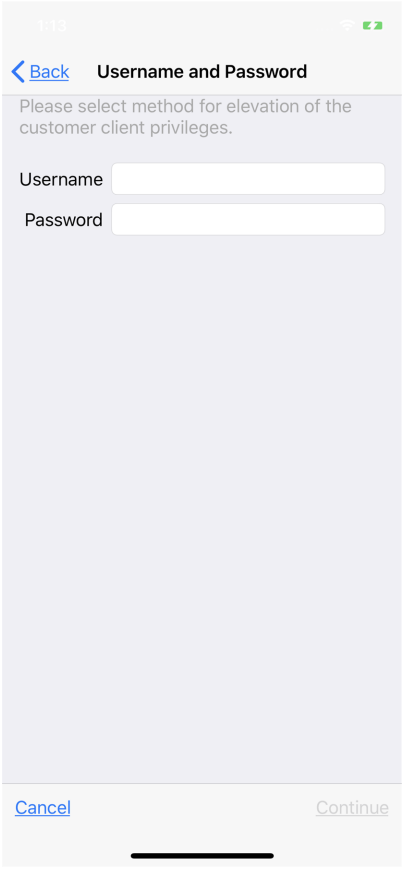
If **Prompt Customer** is selected, tap **OK** to send a request to the customer to enter administrative credentials for their computer.



To select an alternate means of elevation, tap **Elevation Method** and then select the method you wish to use.



If you possess administrative credentials to the remote computer, select **Specific User** to supply an administrative username and password yourself. Tap **OK** to elevate the client.

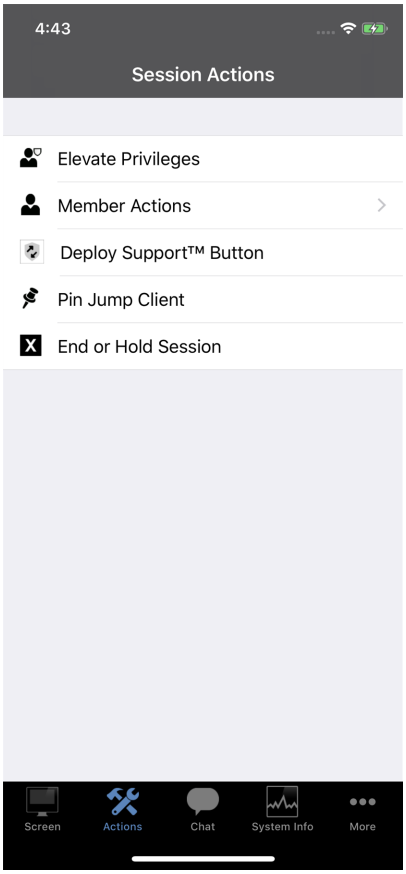


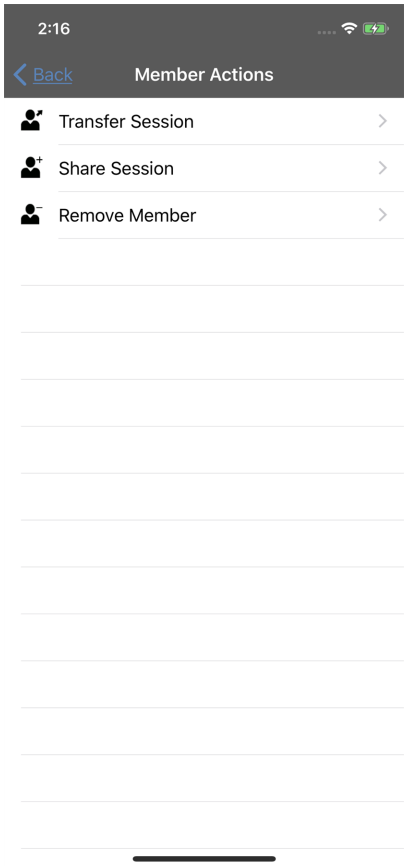
For more information about manual vs automatic elevation, please see the Representative Console Guide at https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm.

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

To transfer a session to another team or representative, tap the **Member Actions** button. On an iPhone, access this button by tapping the **Menu** button first.

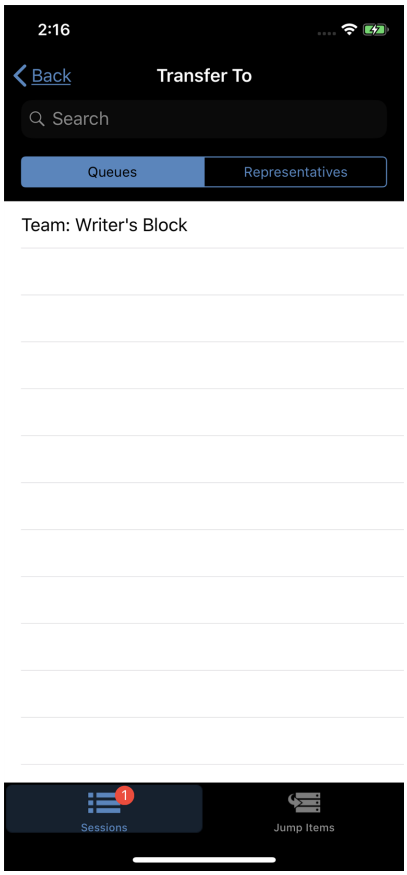
From the menu, select **Transfer Session**.





Browse the list of available teams or search for a specific team name. Select the queue to which you wish to move the session. Then tap the **Transfer** button.

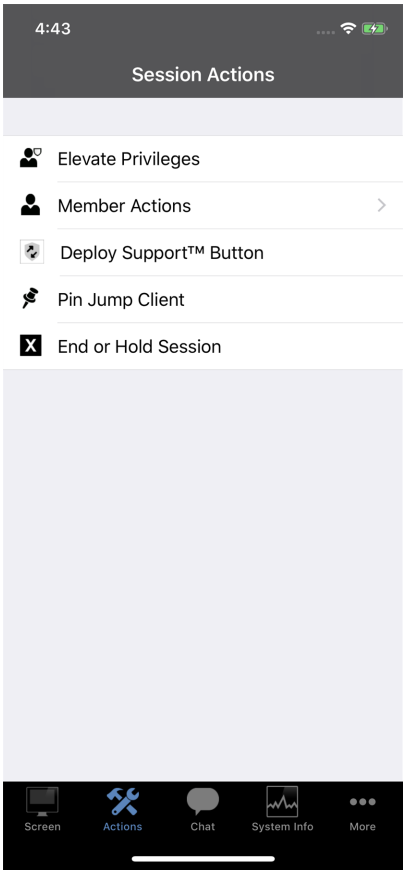
You may also transfer a session to another representative's personal queue. Tap the **Representative** button at the top of the menu. Locate the representative by browsing or searching, and select their name. Then tap the **Transfer** button.

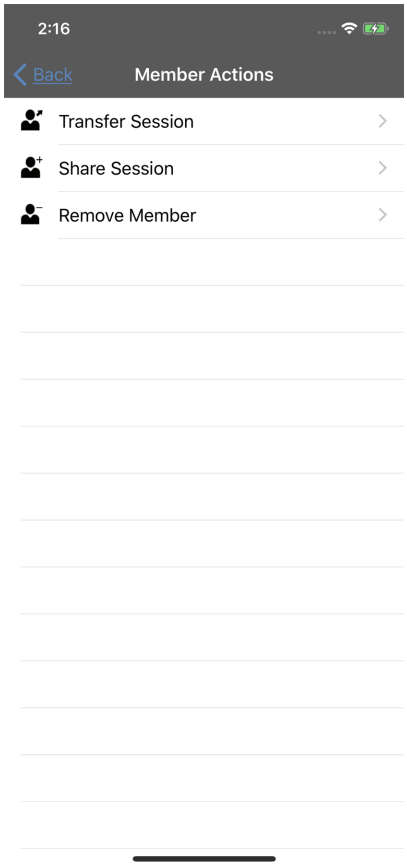


Share a Session with Other Representatives from the iOS Rep Console

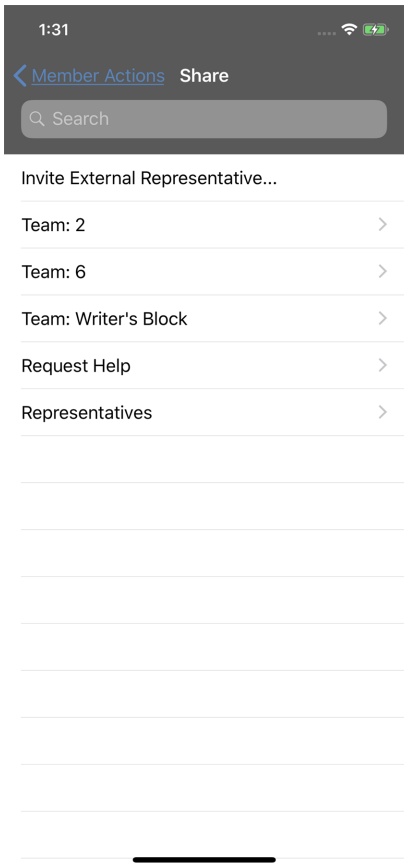
To share a session with another representative, tap the **Member Actions** button. On an iPhone, access this button by tapping the **Menu** button first.

From the menu, select **Share Session**.

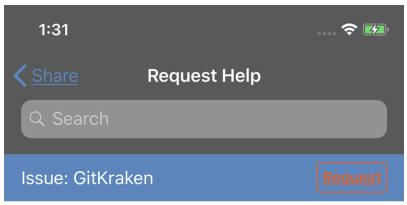




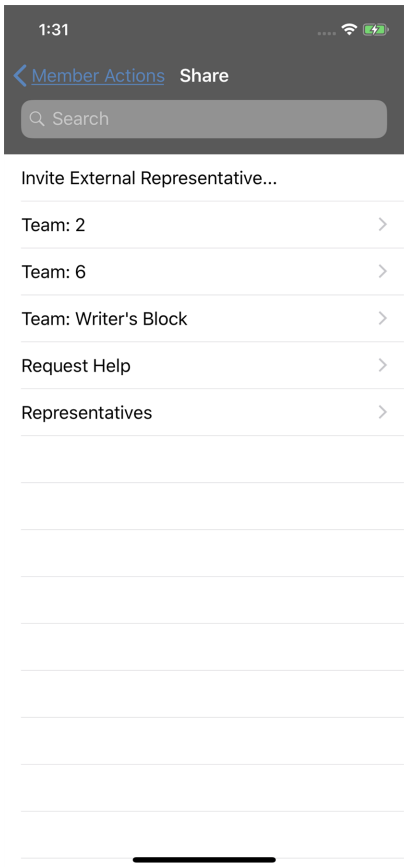
There are several ways you can invite a representative to join a session. Only issues that have been configured to allow you to request help are displayed on this list.



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



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.

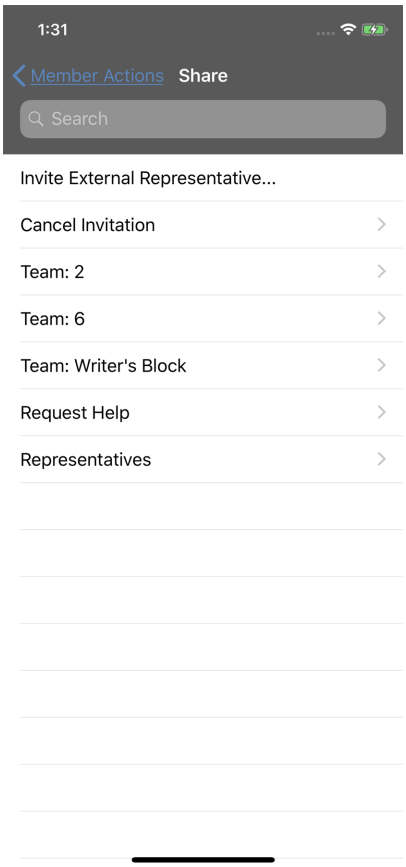
When you invite a user with extended availability enabled, they receive an email notification.

Rep: G. Orwell

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 tap 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:

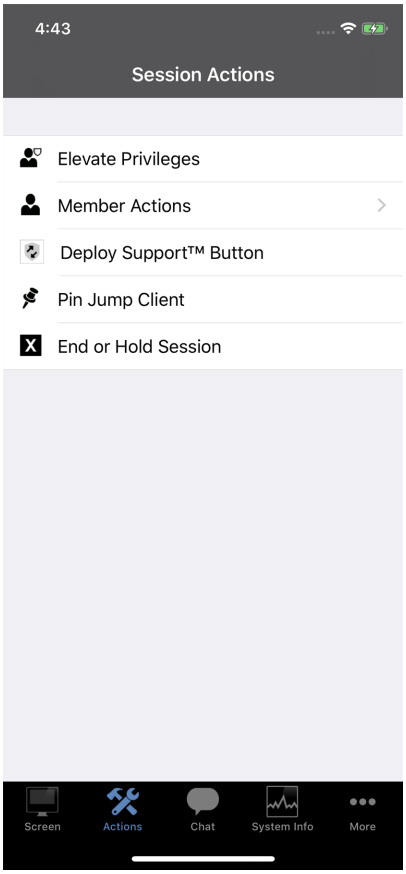
- The inviting user cancels the invitation
- The inviting user leaves or transfers ownership of the session
- The session ends
- The invited user accepts the invitation
- The invited user declines the invitation

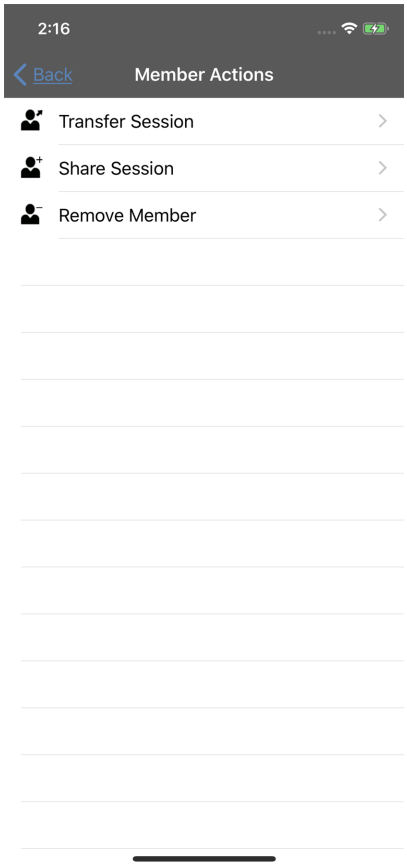


Invite an External Representative to Join a Session from the iOS Rep Console

Alternatively, you can share a session with a representative who does not have an account on your B Series Appliance. To invite an external representative to join a session one time only, tap the **Member Actions** button. On an iPhone, access this button by tapping the **Menu** button first.

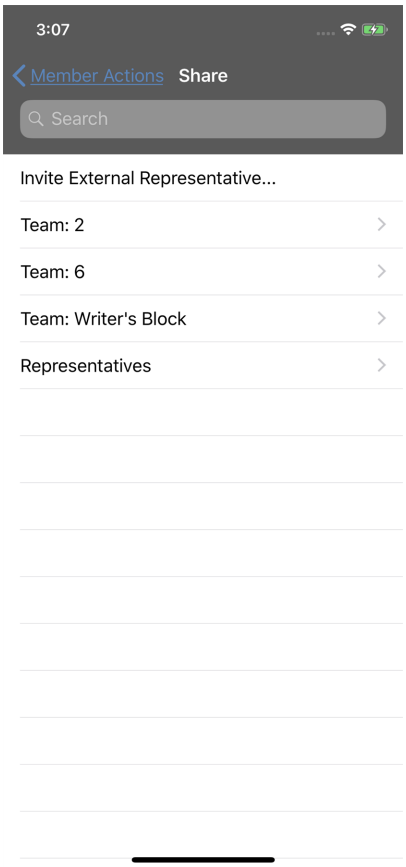
From the menu, select **Share Session**.





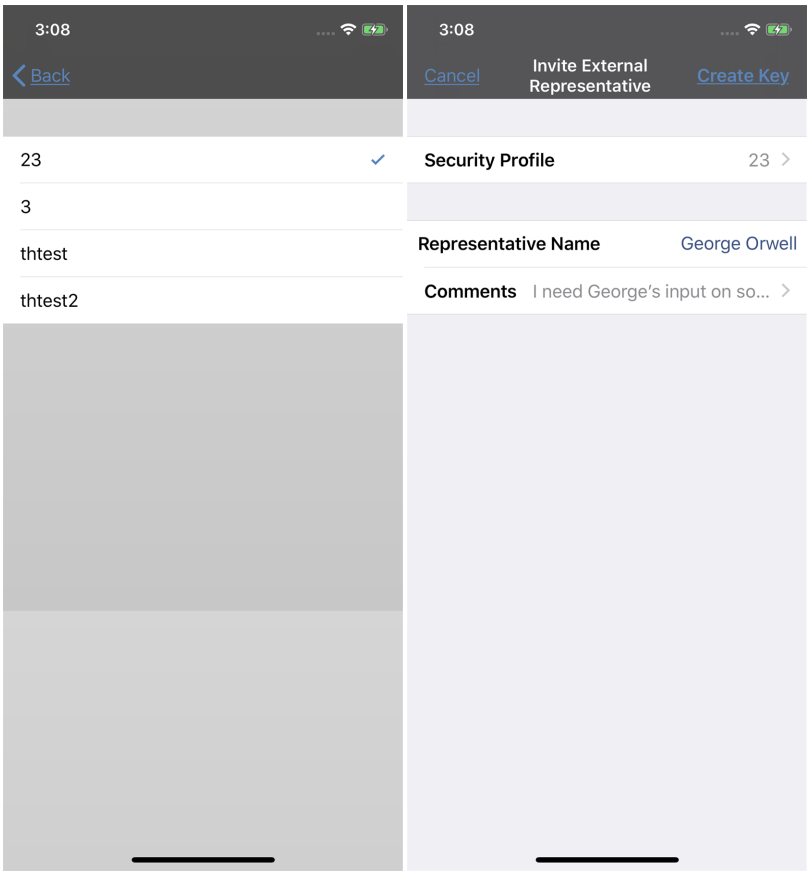
Tap **Invite External Representative**.

A menu will open, allowing you to customize the invitation and create a representative session key.



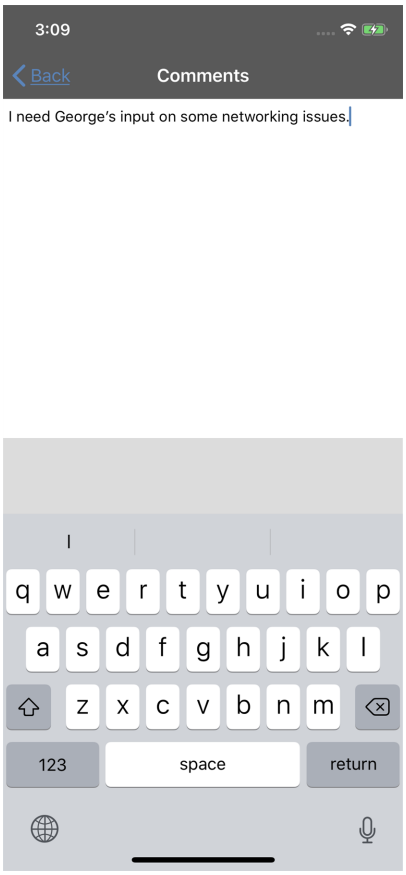
Tap **Security Profile** to access a list of available representative profiles. These profiles are created in the administrative interface and determine the level of permission the external representative will have. When you select a profile, the list will close, and the full description will display beneath the selected profile.

Enter the representative's name. This name will appear to the customer and in reports.



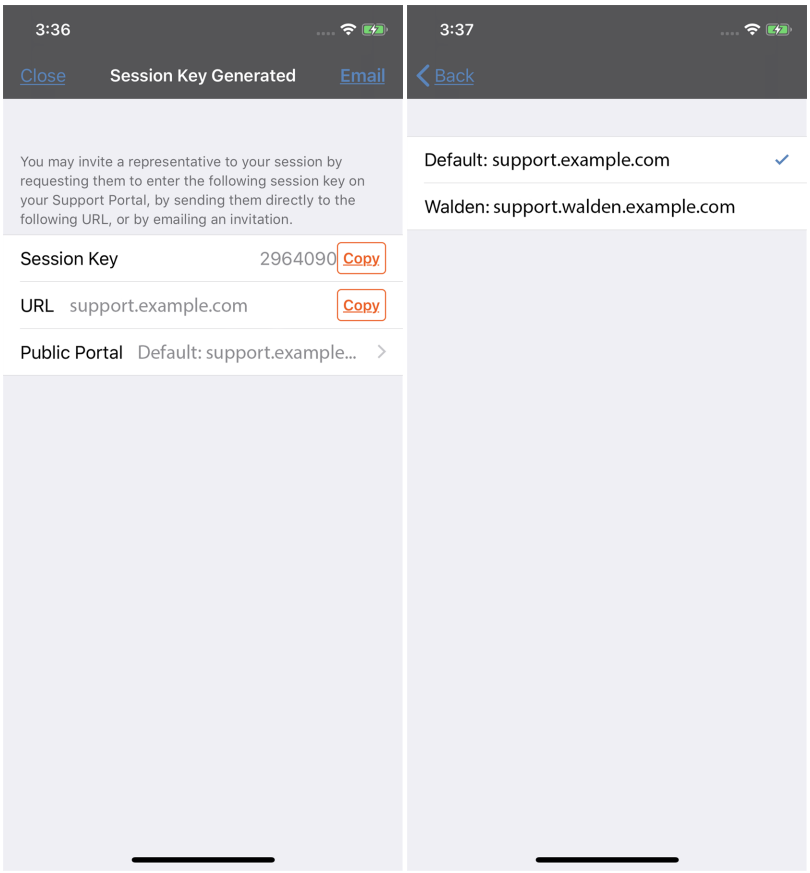
Next, tap **Comments** to enter details about why this representative has been invited.

When finished, tap **Create Key**.



A menu containing the session key and direct URL will appear.

To select the public site through which the external representative should connect, tap **Public Portal**.

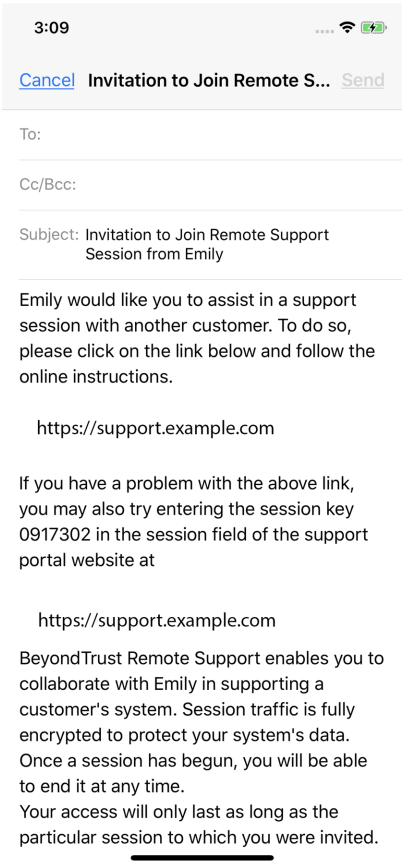


For the external representative to join the session, they will need to submit the session key on your public site or go to the direct URL.You can copy and paste the session key or the URL, or you can email the URL.

The external representative must download and run the representative console; this installation is an abbreviated process of the full representative console installation.

An invited representative has access only to the session tab and has a limited set of privileges. They can never be the session owner. If the primary representative leaves the session and no other licensed representatives are participating, the external representative is automatically logged out.

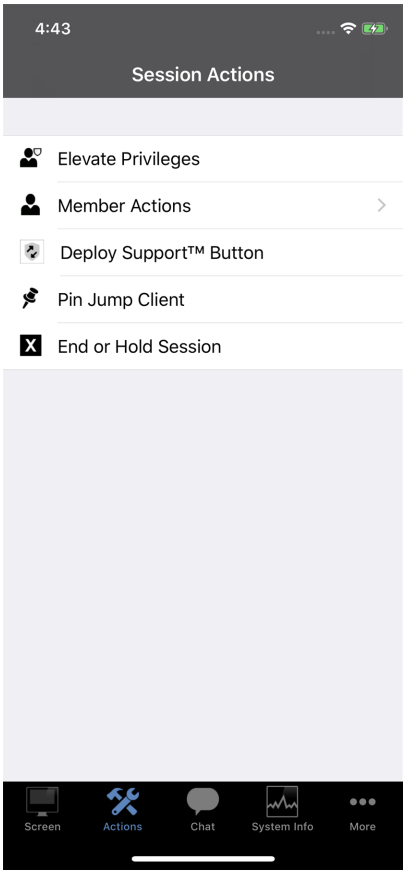
You can invite more than one external representative to a support session. Be aware that each external representative does allocate a BeyondTrust license.

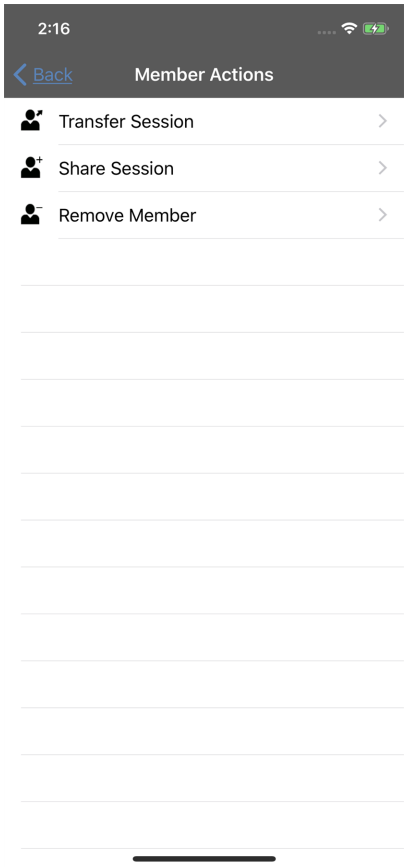


Remove a Member from the Session in the iOS Rep Console

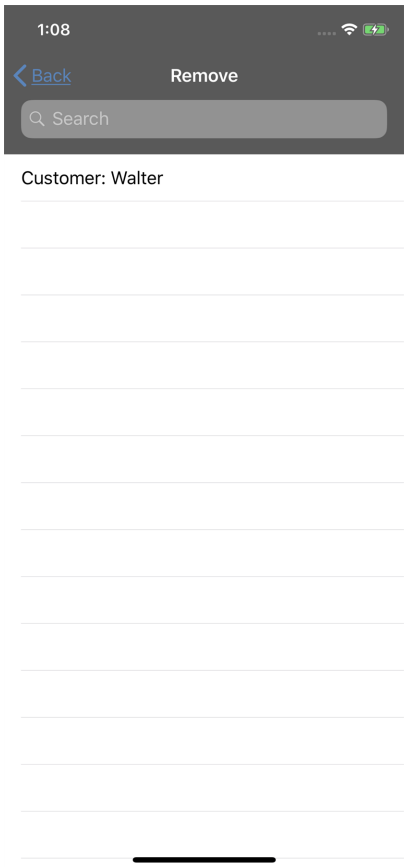
You can remove the customer or another user from a shared session. Tap **Remove Member** from the menu. Select the member you wish to remove. Tap the **Member Actions** button. On an iPhone, access this button by tapping the **Menu** button first.

From the menu, select **Remove Member**.





Select the participant you wish to remove. Then tap the **Remove** button. You must be the owner of the support session to remove another member.

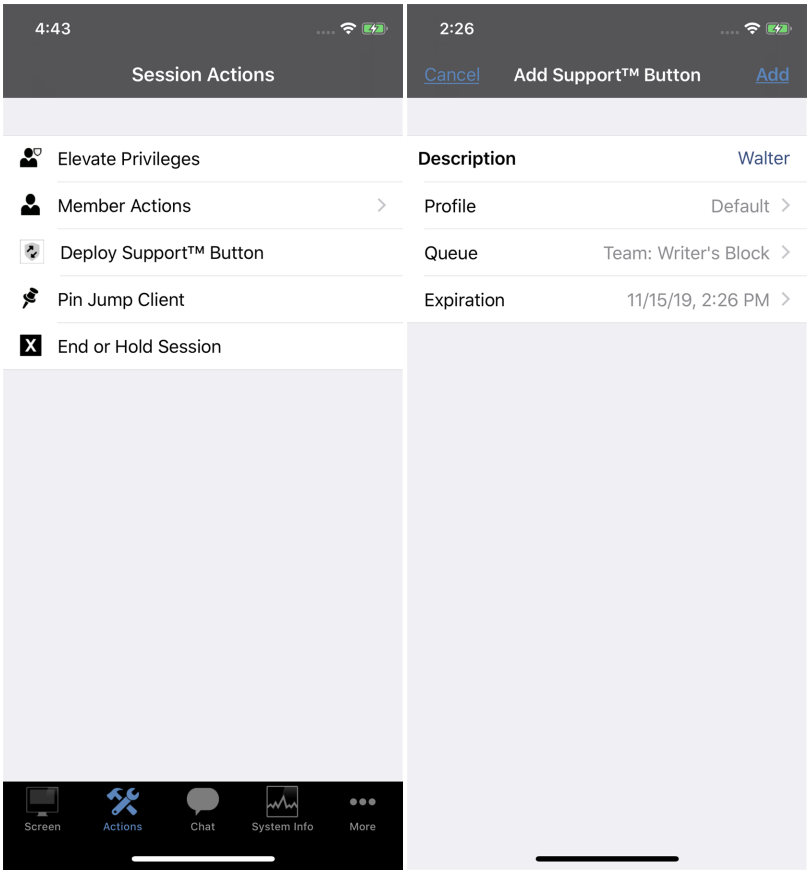


Add a Support Button to the Remote Computer from the iOS Rep Console

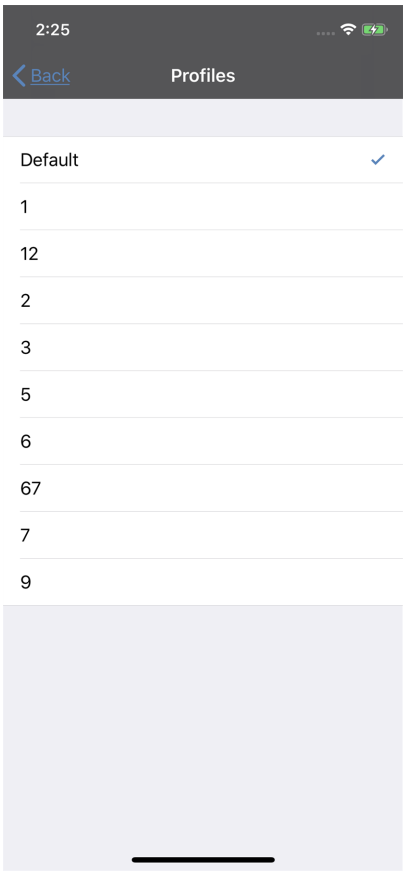
While in a session, you can deploy a Support Button to the remote computer, providing a quick method for your customer to request support.

To begin, tap the **Deploy Support Button** icon. On an iPhone, access this button by tapping the **Menu** button first.

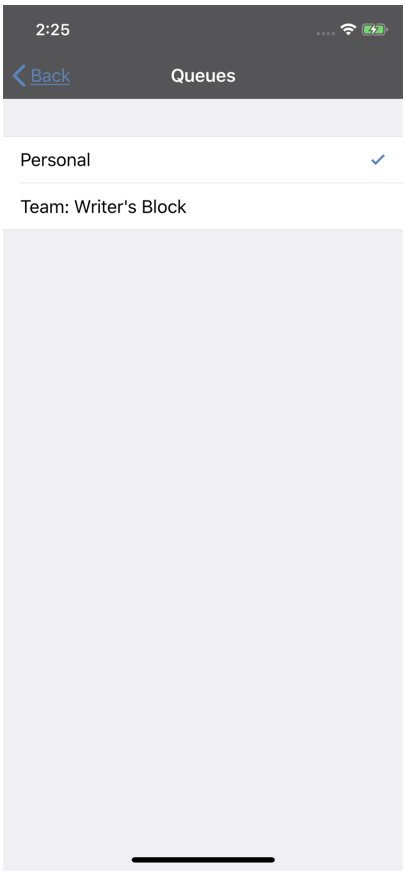
To edit the description, tap the **Description** entry and modify the text.



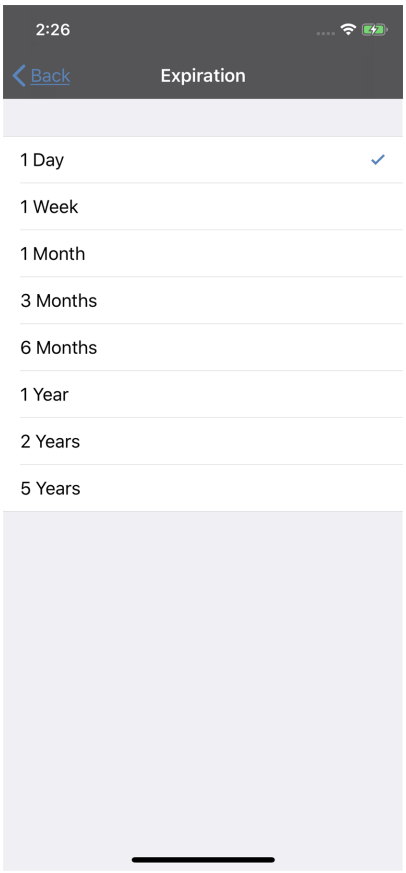
Tap the **Profile** entry to open a list of Support Button profiles from which you can select.



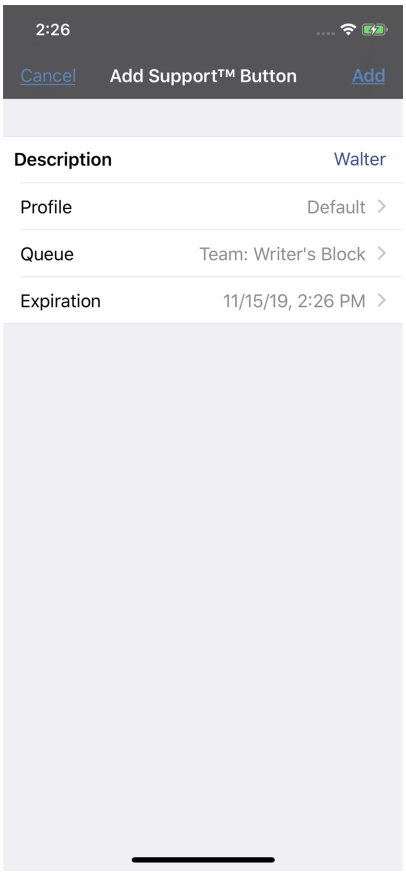
Next, tap **Queue** to select the queue to which this Support Button should link. Once the Support Button is deployed, your customer can use it to directly enter the queue specified here.



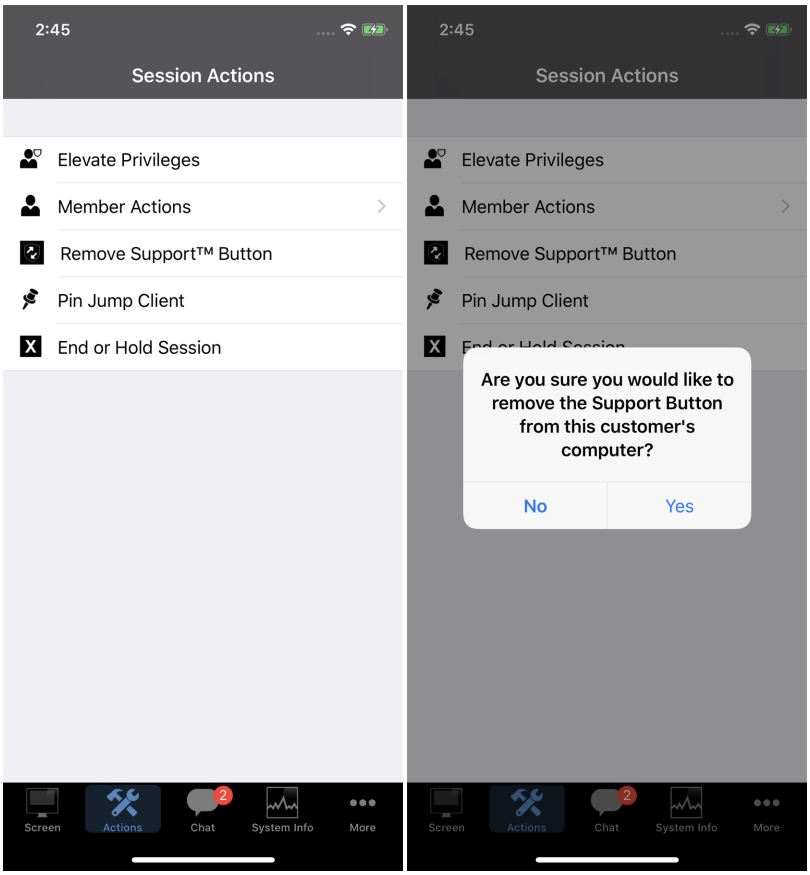
To set how long this Support Button should last, tap **Expiration**. The customer can use this button to start sessions only as long as specified. This time does NOT affect how long the installer remains active or how long a session can last.



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

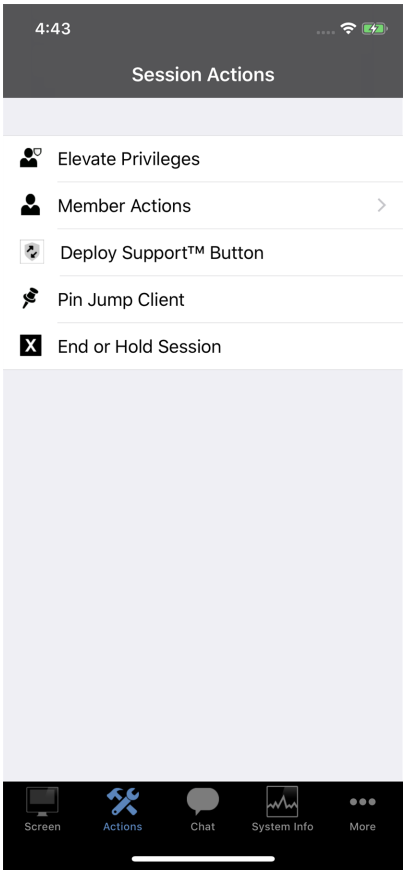


You also may delete the Support Button from the remote system. Tap the **Remove Support Button** icon. When prompted to confirm that you want to uninstall the Support Button, tap **Yes**.



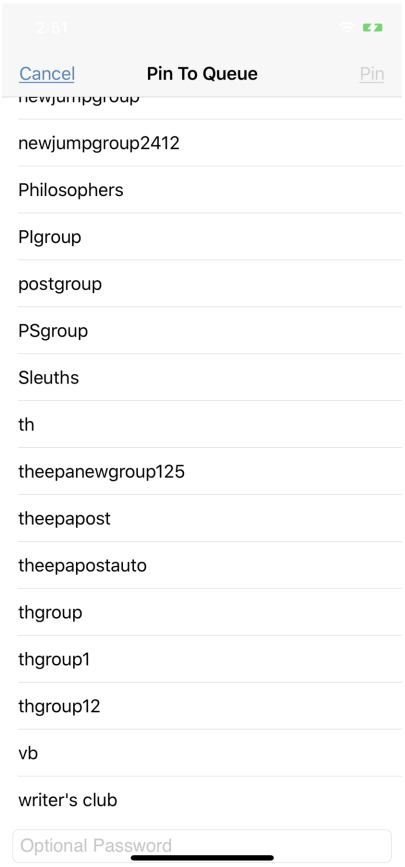
Pin a Jump Client to the Remote Computer from the iOS Rep Console

While in a session, you can pin a Jump Client to the remote computer, enabling later unattended access to that system. To begin, tap the **Pin Jump Client** button. On an iPhone, access this button by tapping the **Menu** button first.

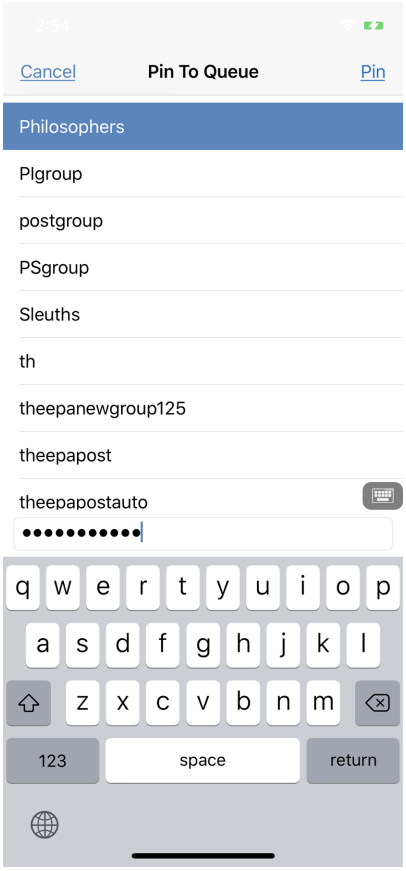


From the list of available Jump Groups, select the group to which you wish to pin the Jump Client. Pinning the Jump Client to your personal list of Jump Items means that only you can access this remote computer through its Jump Client. You also can choose to pin the Jump Client to a specific Jump Group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

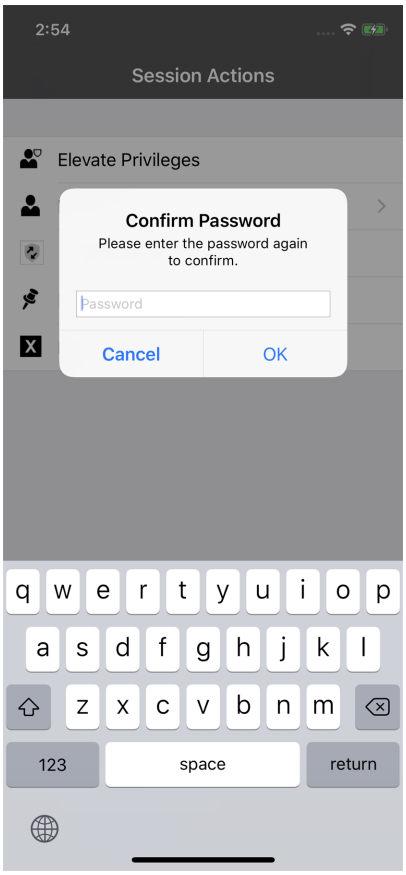
If you wish to pin the Jump Client without setting a password, you can tap **Pin** now.



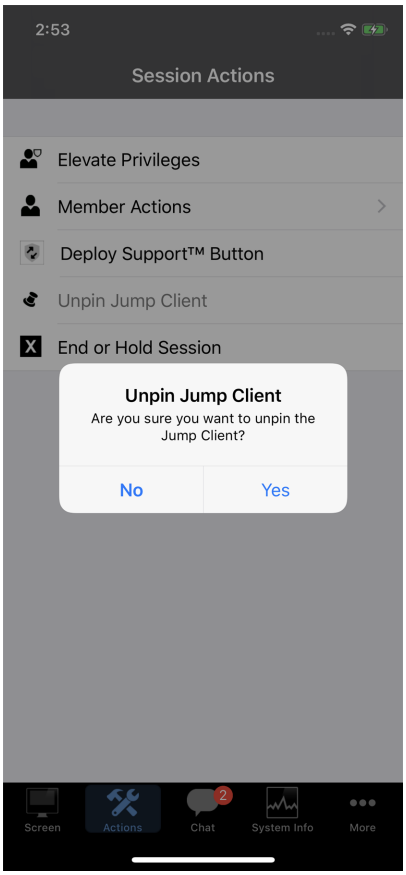
Alternatively, you may set a password for this Jump Client. This will require anyone who wishes to access the Jump Client to enter the correct password before gaining access to the remote system. Enter the desired password and then tap **Pin**.



Confirm the password you have set, and then tap **OK**.



If you no longer need unattended access to a remote system, you can remove the Jump Client. Tap the **Unpin Jump Client** button. On an iPhone, access this button by tapping the **Menu** button first.When prompted to confirm that you want to uninstall the Jump Client, tap **Yes**.



Log in to Remote Systems Using Credential Injection from the iOS 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.

System Requirements

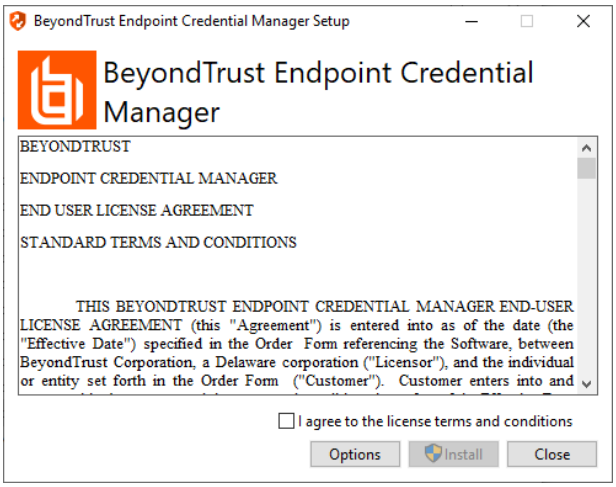
- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

Before you can begin accessing Jump Items using credential injection, you must download, install, and configure the BeyondTrust Endpoint Credential Manager (ECM).

> ***Note:*** *The ECM must be installed on your system 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**.

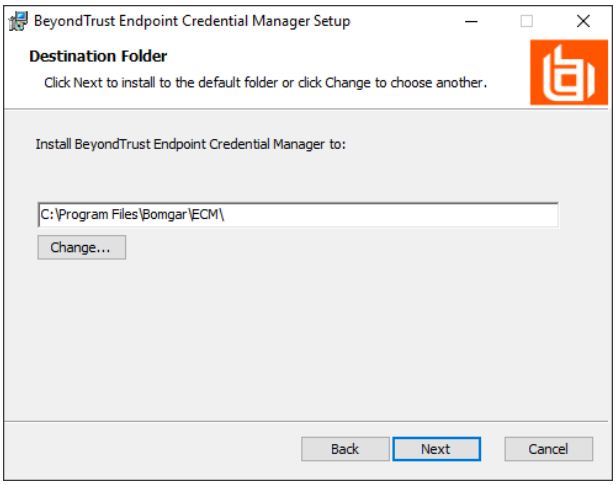
   If you need to modify the ECM installation path, click the **Options** button to customize the installation location.



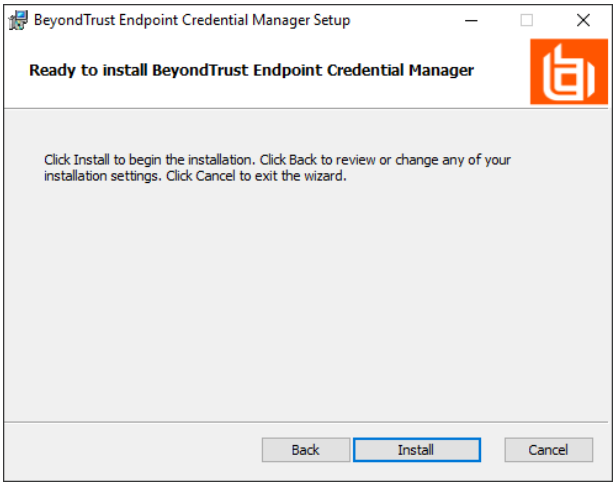
> ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*

3. Click **Install**.

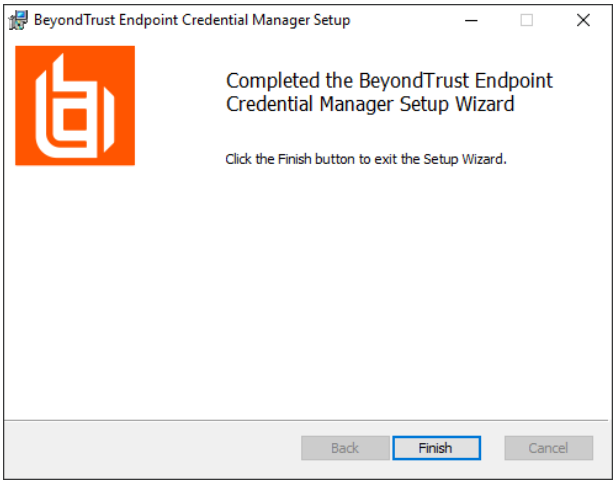
4. Choose a location for the credential manager and click **Next**.
5. On the next screen, you can begin the installation or review any previous step.



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



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



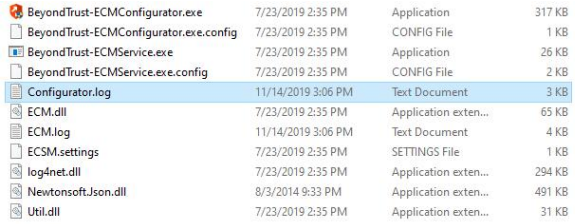
> ***Note:*** *To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the BeyondTrust Appliance B Series. A list of the ECMs connected to the B Series Appliance site can be found at* ***/login > Status > Information > ECM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

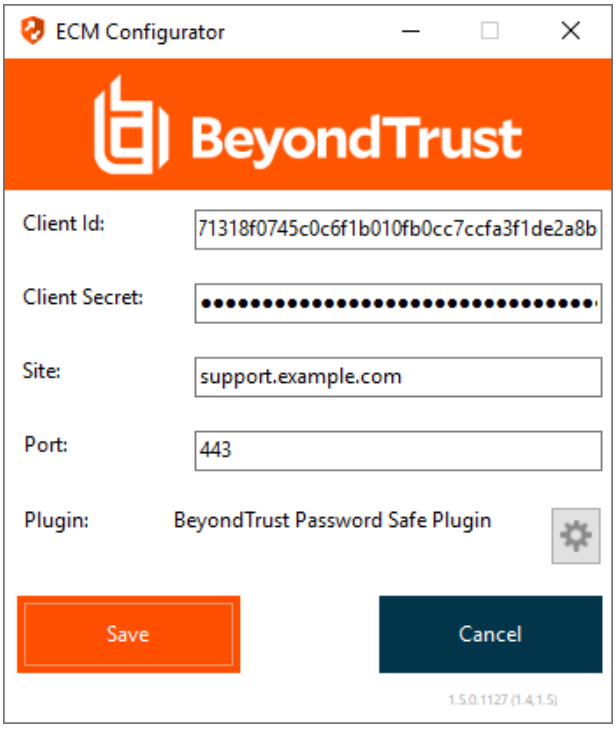
Configure a Connection to Your Credential Store

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.

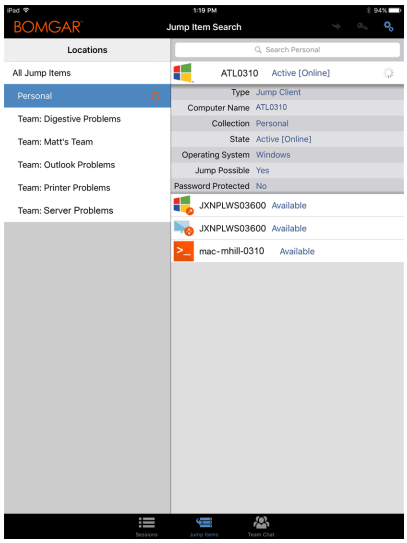
4. When you click the **Choose Plugin...** button, the ECM location folder opens.
5. Paste your plugin files into the folder.
6. Open the plugin file to begin loading.

> ***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.*

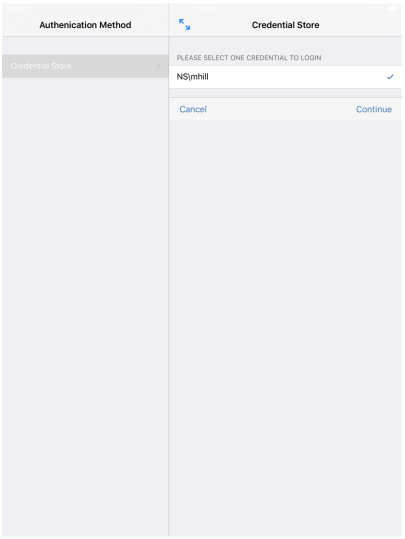
Use Credential Injection to Access Endpoints

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.

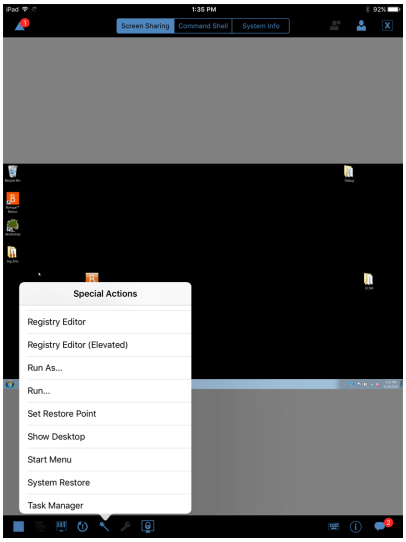
1. Go to your **Jump Items** list.
2. Tap the Jump Item you wish to access.
3. Tap **Jump**.



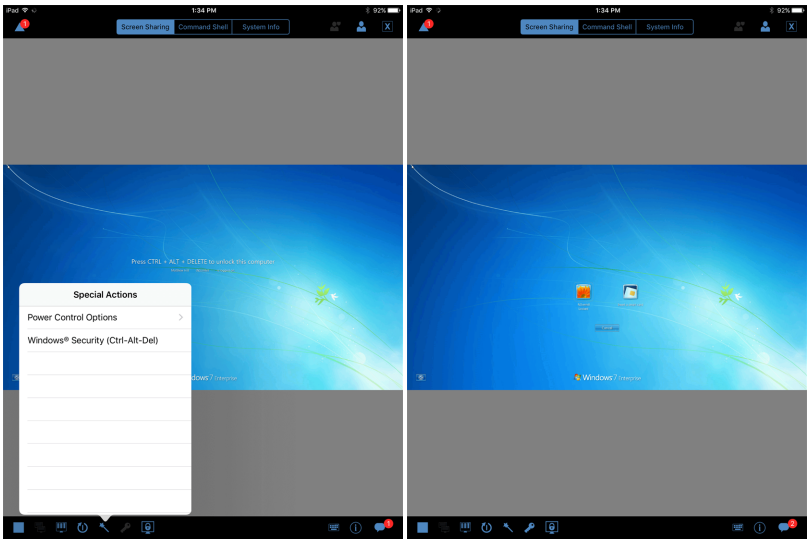
4. Tap **Credential Store**.
5. Tap the credentials you wish to use to access the system.
6. Tap **Continue**.



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.

Choose from Favorite Credentials for Injection

After you have used a set of credentials to log into an endpoint, the system stores your preferred credentials for the endpoint and the context in which they were used (to log in, to perform a special action, to elevate, or to push) in the B Series Appliance database. The next time you use a credential to access the same endpoint, the credential injection menu makes a recommendation for which credentials to use. The credentials are displayed at the top of the credentials list, under **Recommended Accounts**, followed by any remaining credentials. If no credential history exists for an endpoint, the B Series Appliance displays all possible credentials, grouped by accounts that are associated with the Jump Item and not associated with the Jump Item. Jump Item associations for accounts and account groups are configured in /login.

The credential list recommends no more than five credentials.

Close the Session in the iOS Representative Console

To exit a session on an iPhone, tap the **Actions** button, and then tap the **End or Hold Session** button at the bottom of 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.

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, tapping **Leave Session** removes you from the session. The session continues to be supported by the session owner.