BeyondTrust

Privileged Remote Access
iOS Access Console 2.2.4

TC:9/2/2022

Table of Contents

Guide to the Access Console for iOS

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

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 iOS

The BeyondTrust access console for iOS is available for free download from the Apple App Store. From your iOS device, search the App Store for "BeyondTrust Access 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 access console app available through your Enterprise App Store.

To run the BeyondTrust access console on your device, your BeyondTrust software version must be 15.2 or higher, and the iOS device must be running iOS 7 and later.

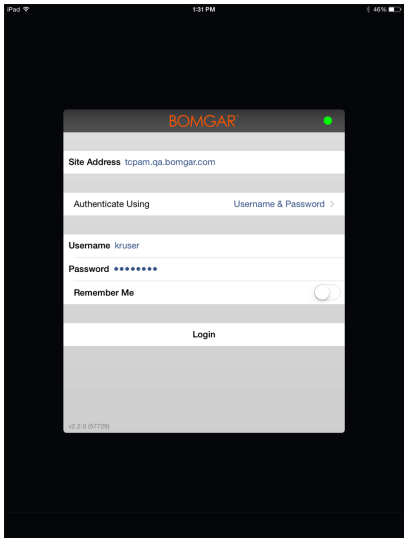
Note: *Only the BeyondTrust access console can be used with a Privileged Remote Access (PRA) site. The BeyondTrust representative console cannot be used to connect to a PRA site, nor can the BeyondTrust access console be used to connect to a BeyondTrust Remote Support site.*

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 access 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 access console on your device to access endpoints from virtually anywhere.

Log into the Access Console for iOS

From the login screen, enter your BeyondTrust site hostname, such as access.example.com. 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 tap **Login**.



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

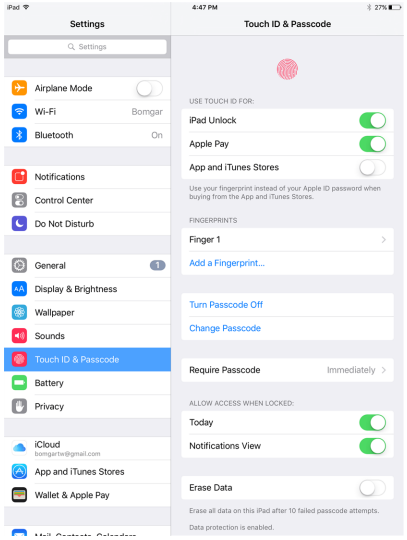
Alternatively, if you have been invited by another user to join an access session one time only, tap **Authenticate Using** and **Access Invite Key**.

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

Log into the BeyondTrust Privileged Remote Access Console for iOS Using Touch ID

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

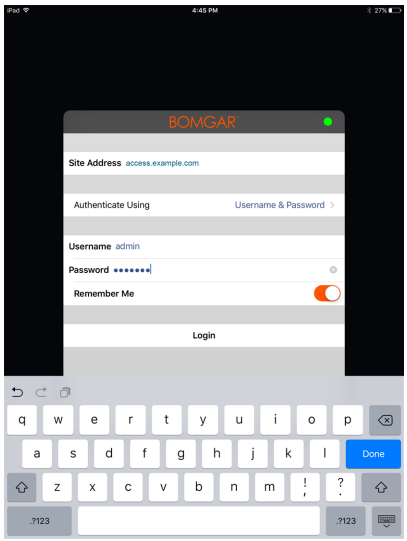
- **iPhone 5s or later**
- **iPad Pro**
- **iPad Air 2**
- **iPad Mini 3 or later**



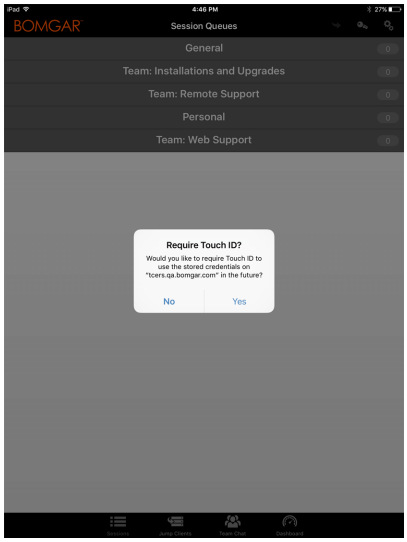
With this feature, you can unlock your device or authorize other actions from your iPhone or iPad using your fingerprint as a passcode. To learn more about Touch ID and how to enable it for your device, please see About Touch ID security on iPhone and iPad at https://support.apple.com/en-us/HT204587 and Use Touch ID on iPhone and iPad at https://support.apple.com/en-us/HT201371.

As of BeyondTrust Privileged Remote Access 16.1, you can use Touch ID to log into the mobile access console for iOS. The same fingerprint authentication used to unlock your device can be used to gain entry into your access console. Follow the steps below to enable ID authentication for your mobile access console.

1. Open the BeyondTrust mobile access console app.
2. Enter your BeyondTrust site hostname, such as access.example.com, along with your credentials.
3. Verify that the **Remember Me** option is enabled. Click **Login**.



4. Tap **Yes** on the Touch ID prompt that appears upon login.
5. Log out of the access console.



6. Tap the **Login with Touch ID** option that appears on the login screen.
7. Place your finger on the **Home** button of your device to finish logging into the representative console.

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

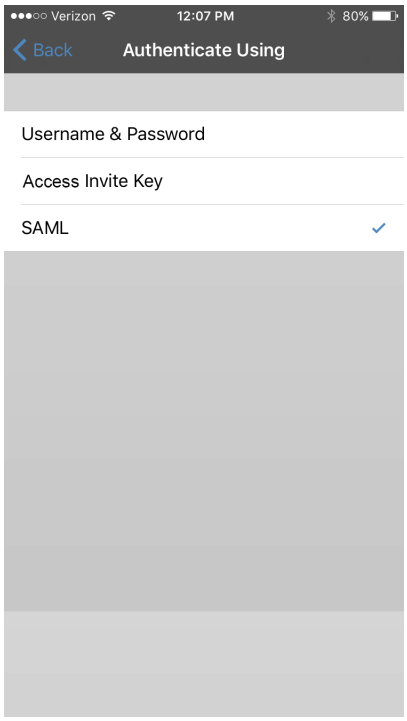
Log into the iOS Access Console Using SAML for Mobile

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

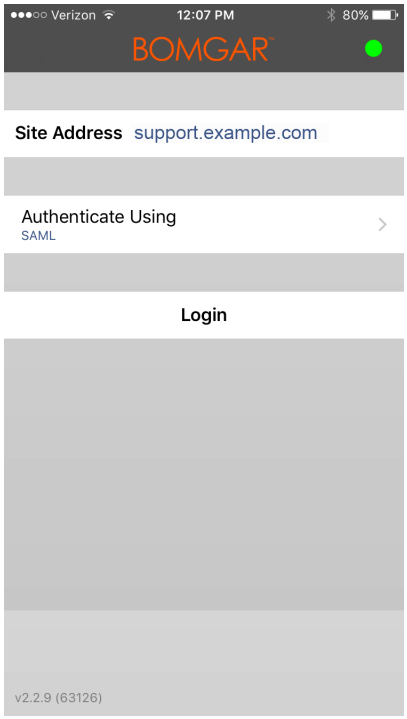
> ***Note:*** *Before attempting to log into the iOS access console using SAML, verify that a SAML provider has been configured for your /login administrative environment by going to* ***Users & Security > Security Providers****. If SAML is not configured in /login, SAML is not available as an authentication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

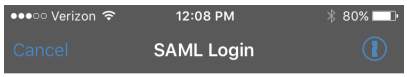
3. Select **SAML**.



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

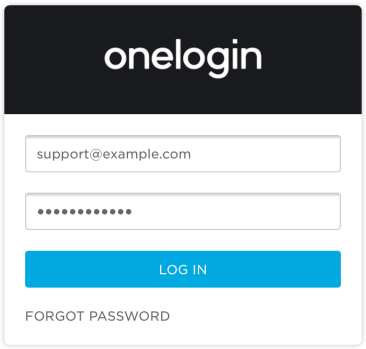


5. On your provider's page, enter your credentials.



> ***Note:*** *If you have a password vault configured on your device, you can tap the key lock icon in the top right to access your password vault and your credentials.*

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

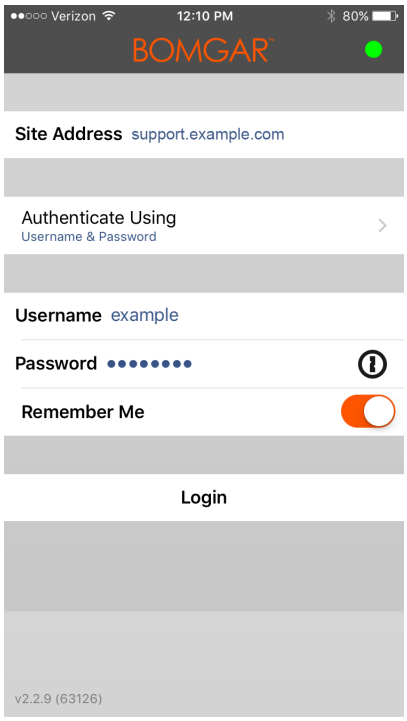


Log into the iOS Access Console Using a Password Manager

Password managers like 1Password and LastPass are an easy way to keep your passwords safe and confidential. To learn more about 1Password proprietary extension, please see Security is not just a feature. It's our foundation. at https://1password.com/security/. Follow the steps below to use 1Password or other password managers to access the BeyondTrust iOS access console.

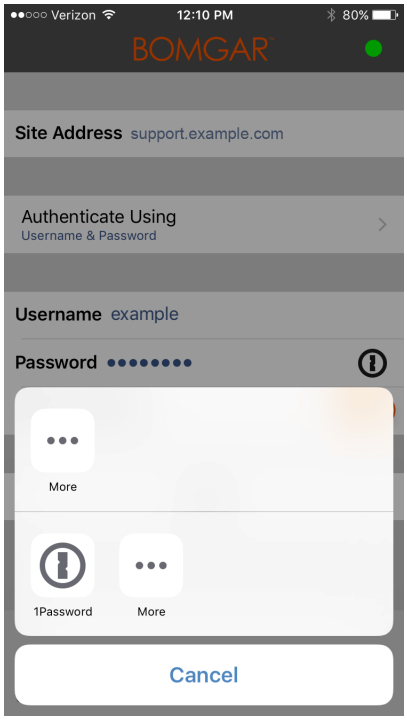
> ***Note:*** *Before using a password manager with the BeyondTrust iOS access console, make sure you have configured an account with the password manager and that the application is synced with your device.*

1. Open the access console app on your iOS device.
2. Tap the key lock icon found in the **Password** field.

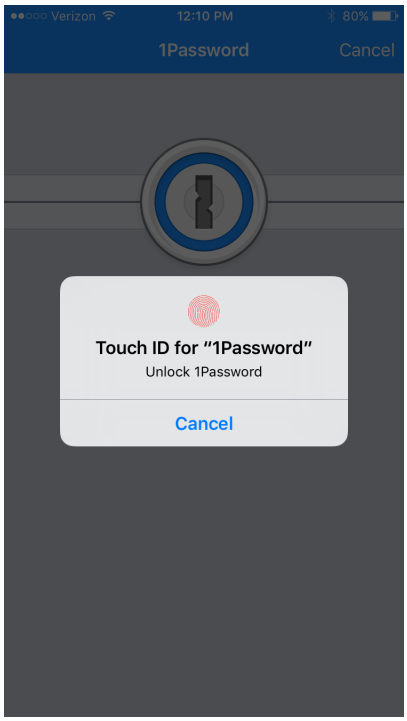


3. From the prompt, tap the password manager you wish to use, and you should be redirected to the password manager's login page.

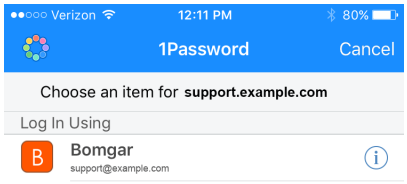
> ***Note:*** *If the password manager is not configured on the device, the key lock icon is not be visible.*



4. If TouchID is enabled, your device allows your fingerprint to be used for authentication to open the application. If TouchID is not enabled on your device, you must enter your password for authentication.



5. Once logged in, the password manager lists the accounts that can access the console. Tap the account you would like to use to access the console.

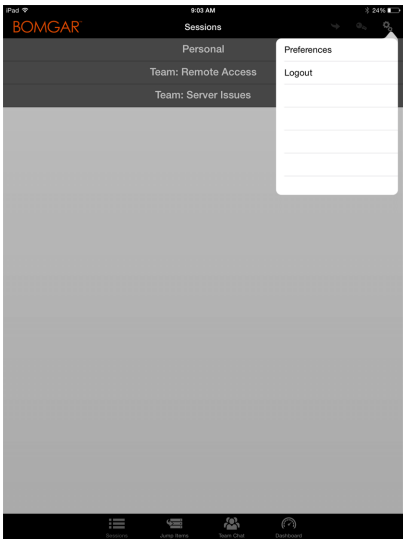


Set Preferences in the iOS Access Console

To change your preferences on an iPad, tap the **Gear** icon in the upper right corner of the screen.

To change your preferences on an iPhone, tap the **Menu** icon located in the upper right corner of the screen.

Next, tap **Preferences**.

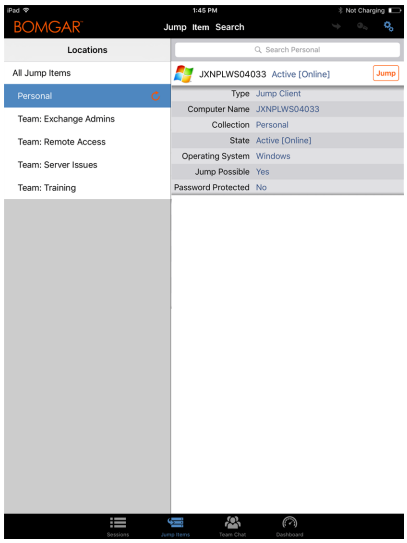


Audible Alerts	iPad and iPhone	If enabled, your device will play audible alerts for certain events that occur within the access console.
Absolute Mouse Pointer	iPad and iPhone	If disabled, you must place your finger on the mouse pointer and drag to move the mouse. Tap and hold to locate the mouse pointer when absolute positioning is turned off. If enabled, you can place the mouse pointer wherever your finger touches the screen. When absolute positioning is enabled, tap and hold to open a fly-out menu from which you can choose different click methods.
Shake device for help in session view	iPad only	If enabled, you can shake the device to generate the Screen Sharing Gestures guide while in an access session.

Use Jump Items to Access Endpoints from the iOS 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. 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** tab at the top of the screen.

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.

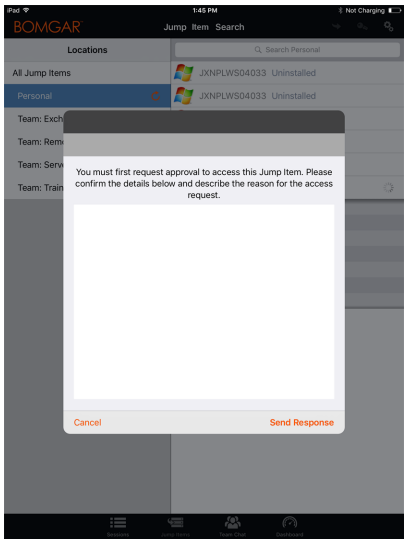
Depending on the permissions your administrator has set for your account, an end-user or third party may be prompted to accept or deny the session. If no response is received within a defined interval of time, the session will either start or cancel as set in your account permissions.

End-User and Third-Party Authorization

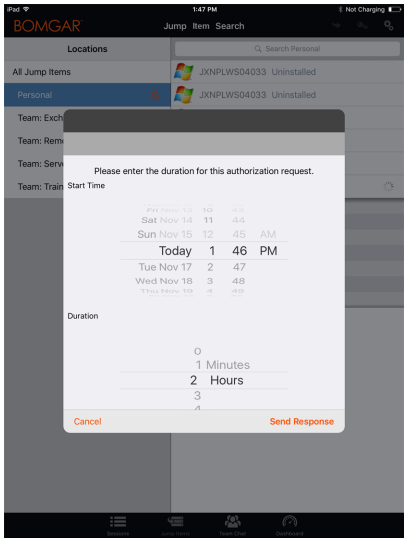
Depending on the configuration of Jump Items within the /login administrative interface, a Jump Item may have a Jump Policy associated with it, and the policy may define an authorization component that forces you to request permission from a third-party or an administrator before you are able to start 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 at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm.*

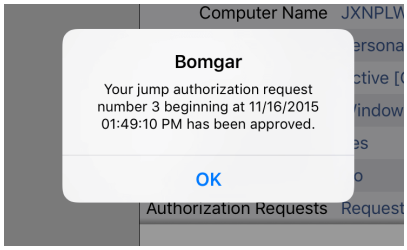
After you have tapped the Jump button and requested access, a prompt appears, and you are required to enter a reason for wanting to access the system.



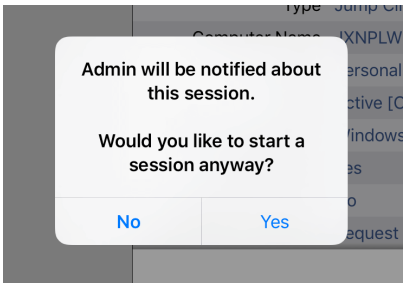
Next, you must indicate when and for how long you will be accessing the system.



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.



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.



Automatic Log On Credentials for the Mobile Access Console

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.

> *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.*

Log into Endpoints Using Credential Injection from the iOS 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

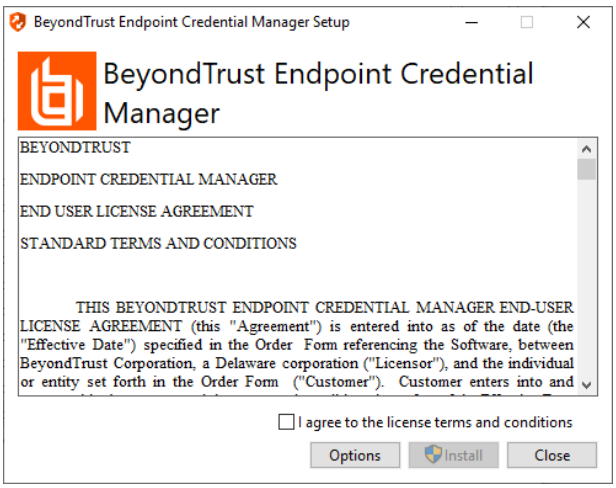
Before you can begin accessing Jump Items using credential injection, you must download, install, and configure the BeyondTrust Endpoint Credential Manager (ECM).

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

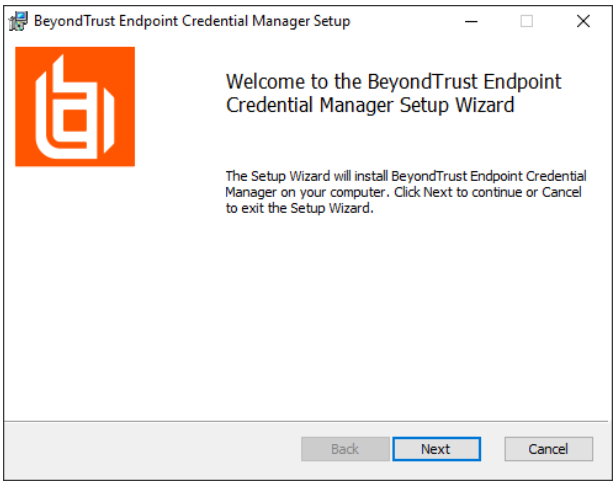
1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from BeyondTrust Support at beyondtrustcorp.service-now.com/csm.
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Check the box if you agree, and then click **Install**.

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

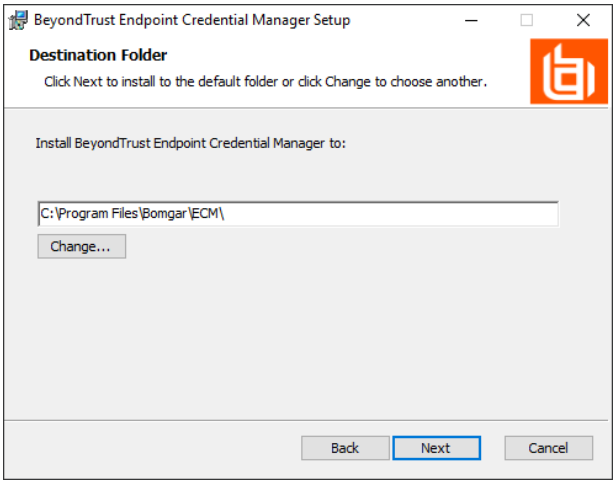
> ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*



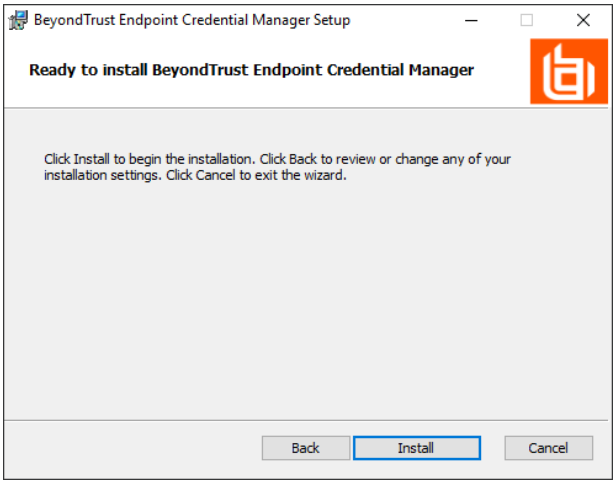
4. Click **Next** on the Welcome screen.



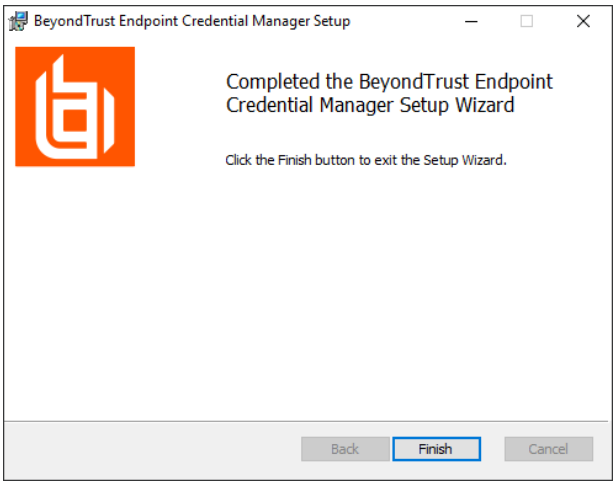
5. Choose a location for the credential manager, and then click **Next**.



6. On the next screen, you can begin the installation or review any previous step.
7. Click **Install** when you are ready to begin.



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

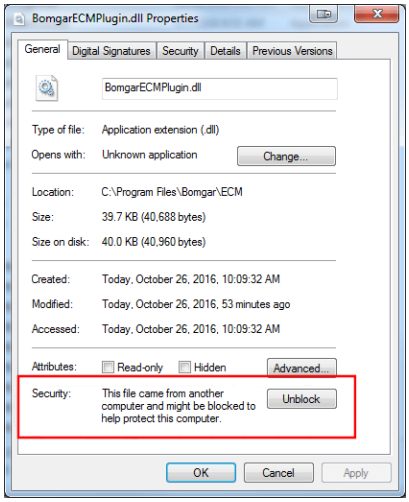


Note: *To ensure optimal up-time, administrators can install up to three ECMs on different Windows machines to communicate with the same credential store. A list of the ECMs connected to the appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

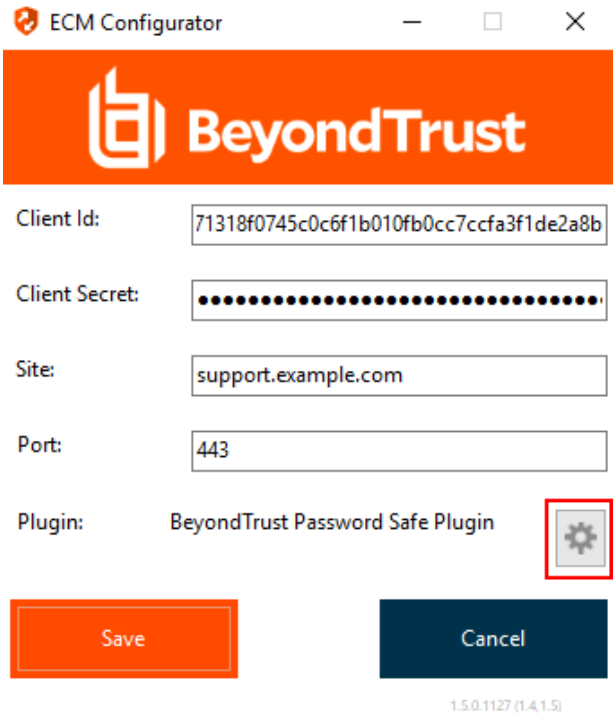
Note: *When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Seriesroutes requests to the ECM in the ECM Group that has been connected to the appliance the longest.*

Install and Configure the Plugin

1. Once the BeyondTrust ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
2. Run the **ECM Configurator** to install the plugin.
3. 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.



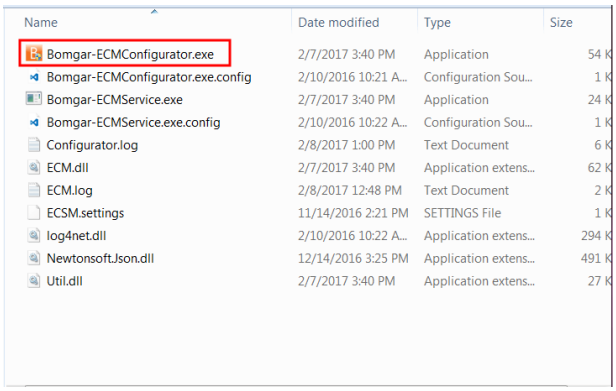
4. Click the gear icon in the **Configurator** window to configure plugin settings.



Configure a Connection to Your Credential Store

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

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.



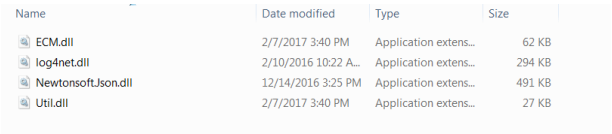
3. When the ECM Configurator opens, complete the fields. All fields are required.

Enter the following values:

Field Label	Value
Client ID	The ID for your credential store.
Client Secret	The secret key for your credential store.
Site	The URL for your credential store instance.

Field Label	Value
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.

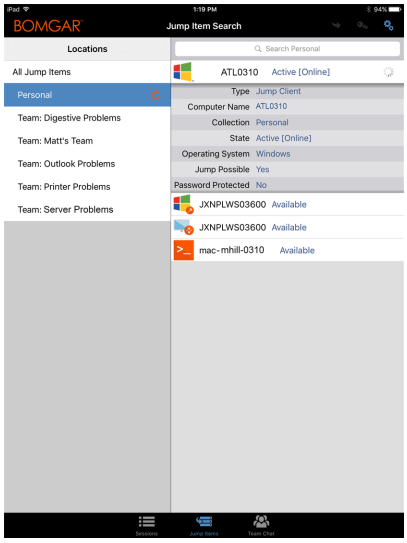


Note: *If you are connecting to a password vault, more configuration at the plugin level may be needed. Plugin requirements vary based on the credential store that is being connected.*

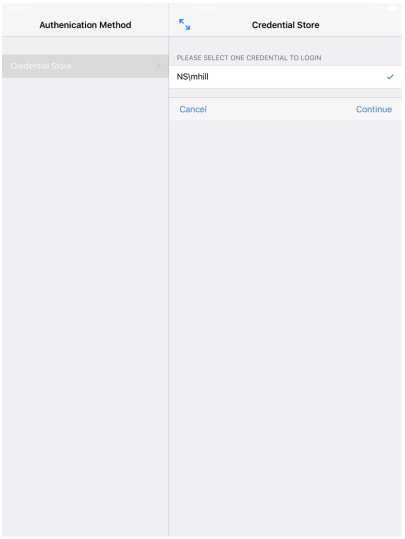
Use Credential Injection to Access Endpoints

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

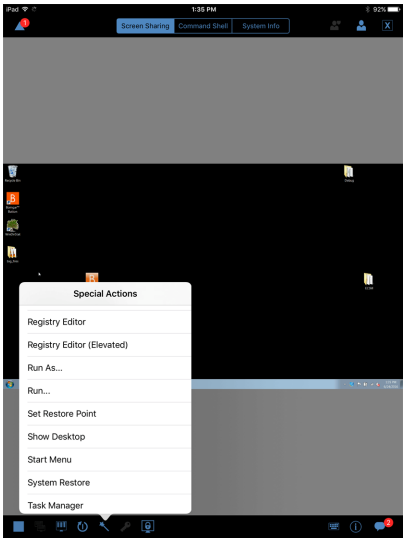
1. Go to your **Jump Items** list.
2. Tap the Jump Item you wish to access.
3. Tap **Jump**.



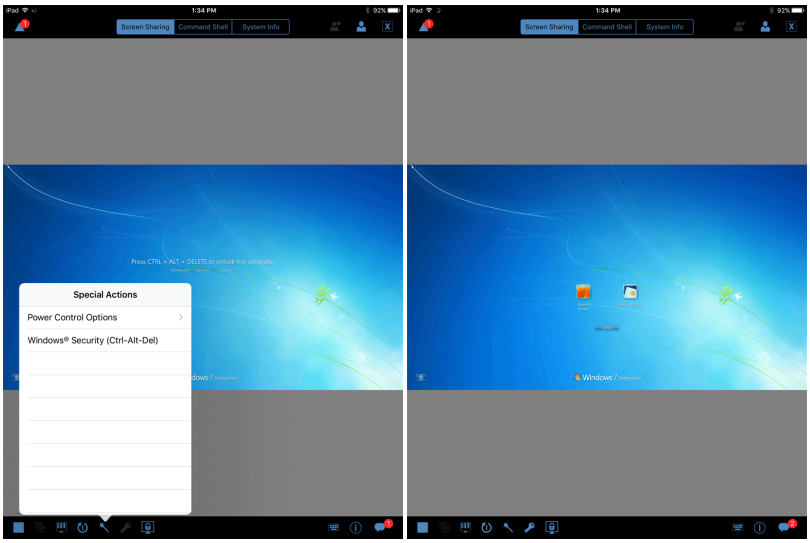
4. Tap **Credential Store**.
5. Tap the credentials you wish to use to access the system.
6. Tap **Continue**.



7. From within the session, tap the **Start** button to start screen sharing.
8. Tap the **Special Actions** option. Tap **Run as...**.



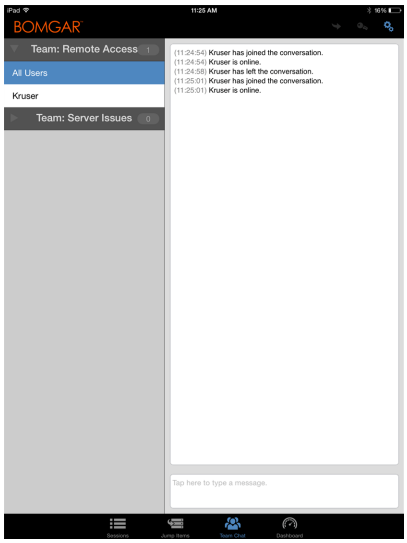
9. Tap **Windows Security (Ctrl-Alt-Del)**.

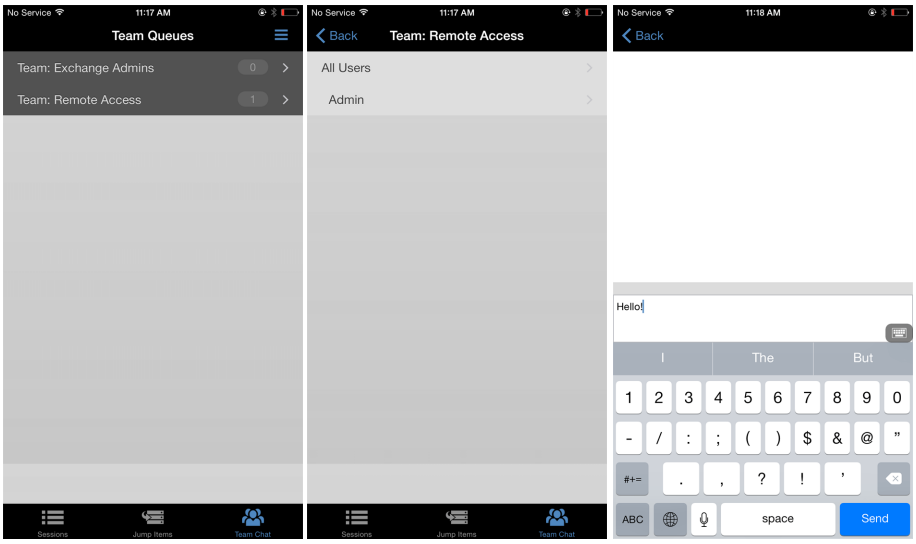


10. Tap the **Key** icon. The Key icon allows the system to view your stored credentials to gain entry into the endpoint.

Chat with Other Users in the iOS Access Console

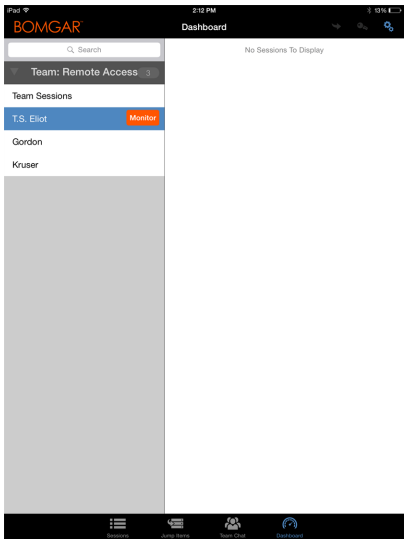
By tapping on the **Team Chat** icon located at the bottom of the screen, you can chat with other logged-in team members. If you are a member of one or more teams, select whichever team you would like to chat with from the listing. You can chat with all members of that team, or select a name from the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





Manage Team Members in the Dashboard (iPad Only)

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 **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 icon will appear at the bottom of the screen. On the dashboard, only logged-in team members of a lower role for the selected team will appear.

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.

Select the user whose screen you wish to view and then tap the **Monitor** button. This will open a new page in your access console, displaying either the user's entire computer screen or only the access console, depending on the administrative settings.

Within a team, a user can manage only those with roles lower than their own. Note, however, that roles apply strictly on a team-by-team basis, so that a user may be able to oversee another user in one team but not be able to oversee that same user in another team.

Use 3D Touch for Mobile Access

3D Touch is a pressure sensitive feature found in iPhone 6s and newer.

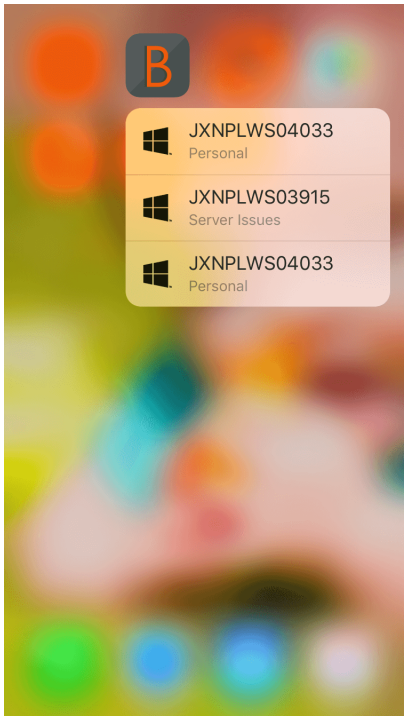
This feature allows you to apply different amounts of pressure to the screen display to make use of the Peek and Pop actions. These actions allow you to preview content and execute commands from your iPhone 6s/6s Plus device without having to fully open an application. To learn more about 3D Touch, Peek, and Pop, please see Take Advantage of 3D Touch at https://developer.apple.com/ios/3d-touch/.

As of BeyondTrust Privileged Remote Access 16.1, you can use 3D Touch to easily access Jump Items. Please see the sections below to learn more about the different ways that 3D Touch allows you to quickly access your critical systems.

Access Frequently Supported Jump Items Using 3D Touch

Using 3D Touch, you can quickly access up to three of your most frequently supported Jump Items from the iPhone Home display. Follow the steps below.

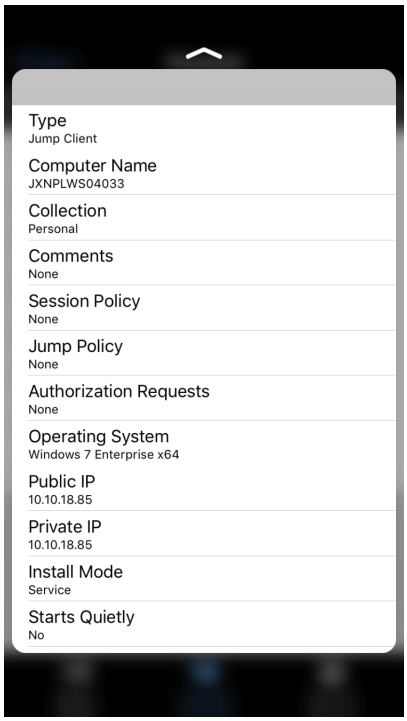
1. Press and hold the iOS mobile access console app icon, and a list of your frequently accessed Jump Items appears. Note that you will have to apply extra pressure to the screen to see the Jump Item options.
2. From the list, tap the Jump Item you wish to access.
3. Enter your login credentials.
4. A session with that Jump Item is iniated.



Preview Jump Item Information

To view Jump Item details before you launch a session, you can use the 3D Touch Peek and Pop actions. Follow the steps below to preview a session.

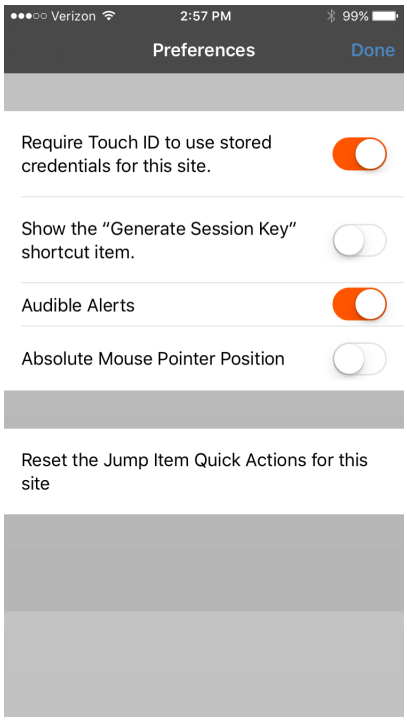
1. From the **Jump Items** page, select the queue where the Jump Item is located.
2. Once you have tapped the queue, a list of Jump Items appears. Tap and lightly press on your selection until the Jump Item's information comes into view.
3. While continuing to press on the screen, swipe upward to see the **Jump** action. Click Jump to initiate a session.



> ***Note:*** *If you do not press with enough force or for enough time, the preview will not appear, and instead, the* ***Session Information*** *page will appear.*

Set Preferences for 3D Touch

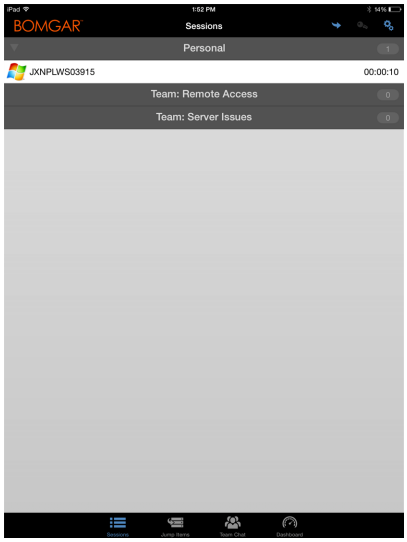
While in the iOS mobile access console, access the preferences menu by tapping the hamburger icon located in the top right corner of the screen and selecting **Preferences**. In the preferences, **Reset the Jump Item Quick Actions for this site** is specific to 3D Touch. When tapped, this preference allows you to clear the frequently used Jump Items list found when tapping and holding down the iOS mobile access console app icon.



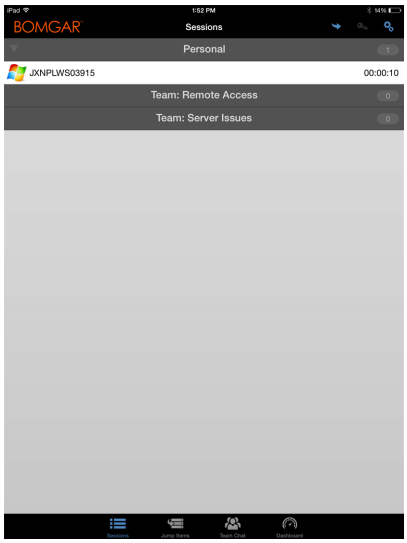
View Access Sessions in the iOS Access Console

Within the access console, active access sessions are divided into team queues. When you tap the **Sessions** icon located at the bottom of the screen, a listing of all configured queues appears. These queues are based upon the teams that you have set up in the /login administrative interface. Once a team is defined, a queue becomes available in the **Sessions** section of the access console. This queue is always displayed as long as at least one team member is logged into the access console.

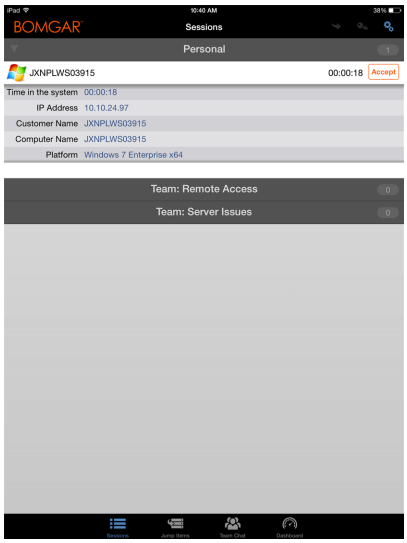
The **Personal** queue contains sessions that you currently have in progress or sessions that have been shared with you specifically by another member. The remaining queues are for specific teams of which you are a member.



Tap the queue name to view any sessions that are in progress. Tap a session entry to view details about the system or session. To navigate to a session, tap on the **Return** option.



> ***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 will cause it to appear on your screen.*



Screen Share with an Endpoint from the iOS Access Console

From the **Screen Sharing** page, tap the **Play** button to request view and control of the endpoint if screen sharing does start automatically. Once you have accessed the endpoint, it appears on your display. You will have full mouse and keyboard control of the endpoint, enabling you to work on it as if you were really there.

- 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 three fingers
- Tap 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.

> ***Note:*** *On an iPad, if enabled in your settings, shake the device for a quick reference of screen sharing gestures.*

On an iPad, all screen sharing actions are available at the bottom of the screen. On an iPhone, to access more screen sharing tools, tap the **Menu** icon located in the top right corner of the screen. Tap **View Gesture Help** for a quick reference of screen sharing gestures.

Screen Sharing Actions

	Begin screen sharing.
	Stop screen sharing.
	Select an alternate remote monitor to display. The primary monitor will be 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.
	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.
	Reboot the remote system without losing your connection to the access session.

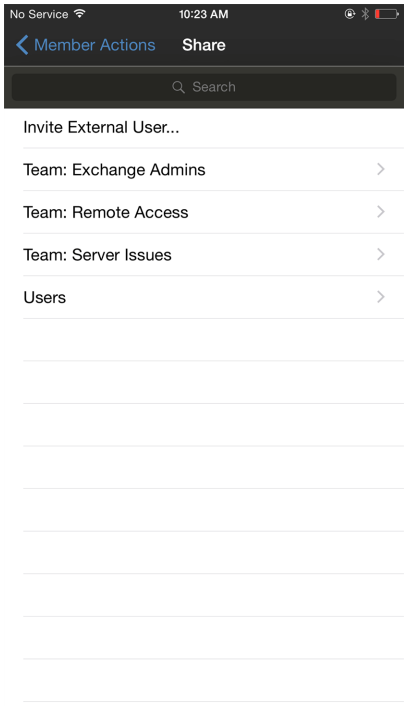
	Disable the remote user's screen view, mouse, and keyboard input. Restricted endpoint interaction is available only when accessing macOS or Windows computers. Restricted customer interaction is available only when supporting Windows computers. In Windows Vista and above, the endpoint client must be elevated.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

Share a Session with Other Members from the iOS Access Console

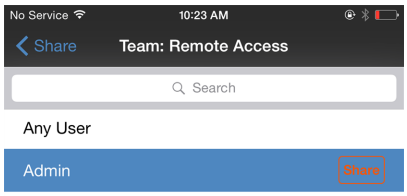
To share a session with another team member using an iPad, tap the person icon in the top right corner of the screen. When using an iPhone, tap on the **Action** icon located at the bottom of the screen. Tap on **Member Actions**.

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

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



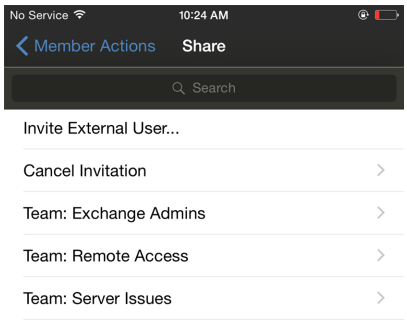
You can select a user listed in the teams displayed to invite them to join the session. You can send multiple invitations if you want more members from the team to join your session. Users are listed here only if they are logged into the access console or if they have extended availability enabled.



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 with extended availability enabled.

If you have sent an invitation and it is still active, you may revoke the invitation by selecting it from the **Cancel Invitation** menu. Next tap **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. The invitation disappears if:

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



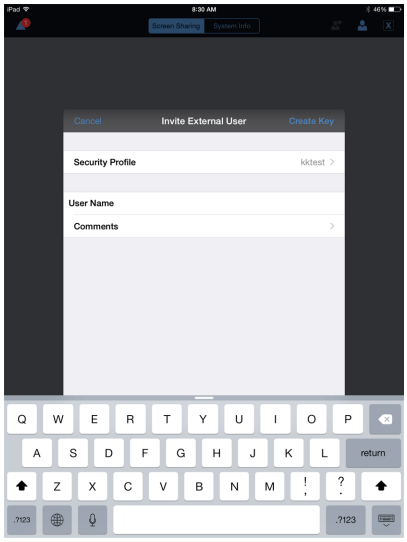
Invite an External User to Join a Session from the iOS Access Console

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

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

Tap **Invite External User**.

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

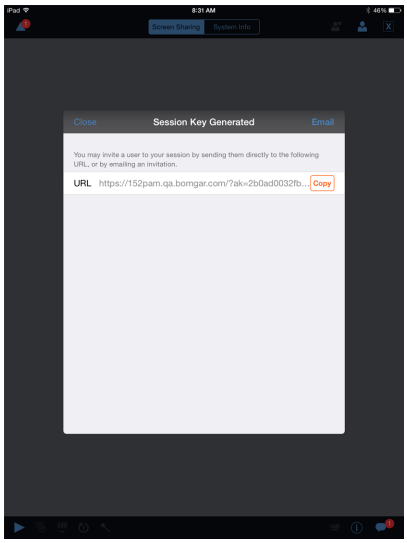


Tap **Security Profile** to access a list of available user profiles. These profiles are created in the administrative interface and determine the level of permission the external user will have. When you select a profile, the list will close.

Next, tap on the **Create Key** option located in the top right corner of the screen.

Once tapped, the **Session Key Generated** section will populate.

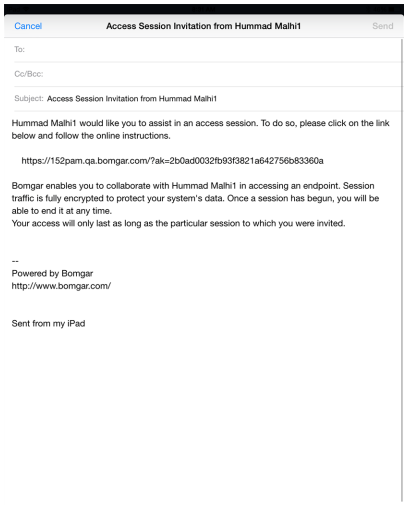
Tap the **Email** option located in the top right corner of the screen.



An email is generated. Make any necessary changes to the email.

When finished, tap **Send**.

> ***Note:*** *You also have the ability to copy the URL from the* ***Session Key Generated*** *section. Simply click the* ***Copy*** *option found beside the URL.*

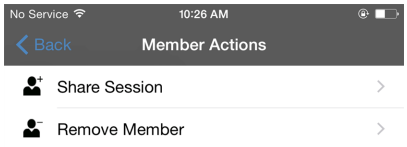


Once the external user has received the email, they must tap the **URL** found in the email. They are then taken to the **Access Portal**, where they are prompted to download the access console.

After the console has been downloaded, the login page to the access console appears with the access session key already populated. They must tap **Login** to access the console.

Remove a Member from the Session in the iOS Access Console

You can remove a user from a shared session. On an iPhone, tap the **Actions** icon located at the bottom of the screen. Select **Member Actions**. Tap **Remove Member**.



On an iPad, tap the person icon located in the top right corner of the screen. From the menu, select **Remove Member**.

Select the user you would like to remove. Then tap the **Remove** option.

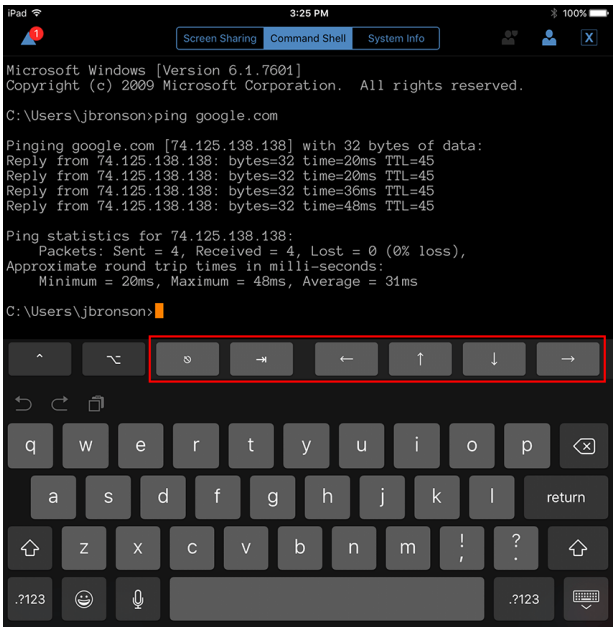
Open the Command Shell on the Remote Endpoint Using the Access Console (Apple iOS)

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.

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.



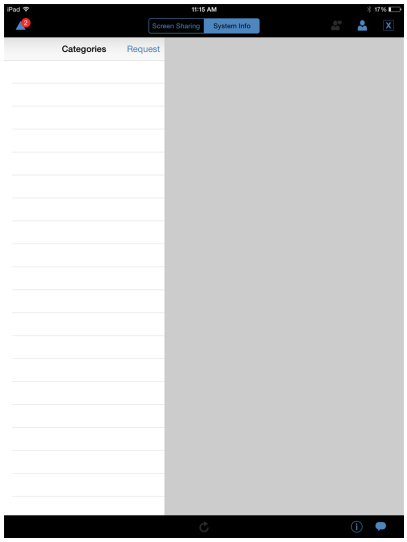
Command Shell Tools

	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 Access Console

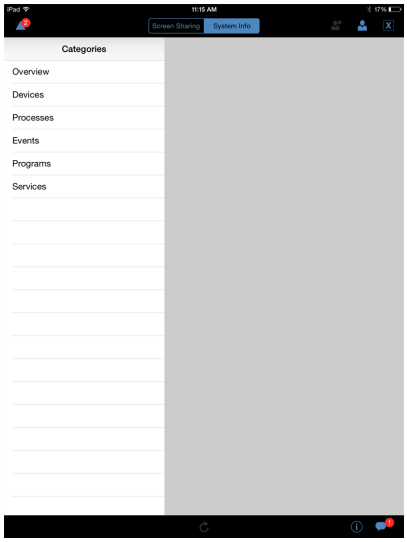
Privileged users may view a complete snapshot of the remote device's system information to reduce the time needed to diagnose and resolve issues. The system information available varies depending on the remote operating system and configuration.

To request a system's information, navigate to **System Information**. Tap **Request**.



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

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



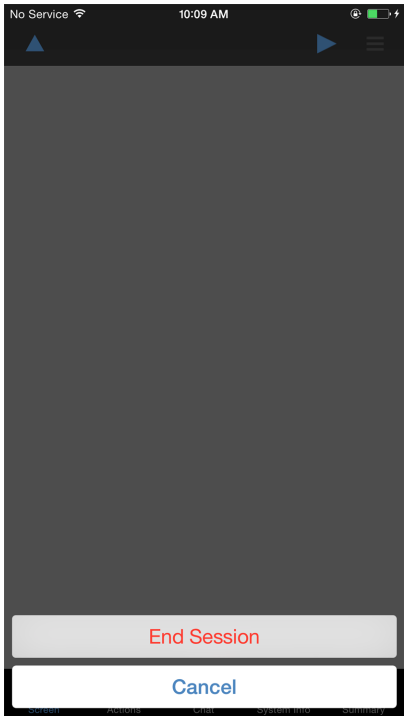
Review a Summary of an Access Session

The **Summary** page gives an overview of the remote system being accessed. Specifically, the **Summary** page outlines the following information about the remote system:

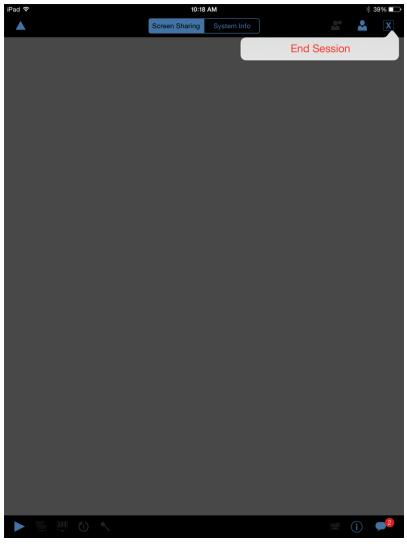
- **IP Address**
- **Customer Name**
- **Computer Name**
- **Platform**

Close an Access Session in the iOS Access Console

To exit a session on an iPhone, tap the triangle icon located in the top left corner of the screen.



To exit a session on an iPad, tap the **X** in the upper right corner of the screen.



> ***Note:*** *An* ***End Session*** *option is also available by tapping on the* ***Actions*** *icon located at the bottom of the screen.*

If you are the owner, **End Session** closes the session page in your access console and removes any additional users who may be sharing the session. However, it will not delete an installed Jump Item.

If you are not the session owner, tapping on the **X** icon and selecting **Leave Session** removes you from the session. However, the session continues to be accessed by the session owner and other users sharing the session.