



BeyondTrust

Remote Support 21.3 Web Rep Console

Table of Contents

Web Rep Console Guide	3
Web Rep Console Requirements	4
Launch the Web Rep Console	5
Log in Directly to the Web Rep Console Using SAML	6
Authenticate to the Web Rep Console from the Client Scripting API	7
Join a Session as an External Representative Using the Web Rep Console	8
Download the Desktop Representative Console from the Web Rep Console	9
View Support Sessions in Queue in the Web Rep Console	10
Start a New Session with a Session Key in the Web Rep Console	11
Use Jump Items to Support Remote Systems in the Web Rep Console	12
Log in to Remote Systems Using Credential Injection from the Web Rep Console	13
Manage Multiple Support Sessions in the Web Rep Console	18
Return to an Active Session	18
Support Session Actions in the Web Rep Console	19
Support Session Actions	19
-Control the Remote System with Screen Sharing in the Web Rep Console	21
Access the Command Shell on the Remote System through the Web Rep Console	24
Use the Web Rep Console to Transfer Files to and from Remote Systems	26
Add a Support Button from the Web Rep Console	29
Pin a Jump Client from the Web Rep Console	30
Elevate the Session in the Web Rep Console	31
Transfer a Session to Another Representative or Team from the Web Rep Console	32
Share a Session with Other Users Using the Web Rep Console	33
Remove a Member from a Web Rep Console Session	35
Chat with the Remote User from the Web Rep Console	36
Close the Web Rep Console Session	37

Web Rep Console Guide

With the BeyondTrust web rep console, support representatives can support customers and remote systems, even when those reps do not have the ability to install software within their own desktop environments. Instead, they can support customers and remote systems through the web-based representative console.

In this guide, we discuss how the browser-based web rep console supports customers and performs other necessary functions while ensuring that the highest level of security is maintained.



Note: 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/docs/index.htm#support.

Web Rep Console Requirements

To run the web rep console on your system, your BeyondTrust Appliance B Series must be running software version 16.2 or higher. On the **/login > Management > Security** page, the permission **Allow Mobile Representative Console and Web Rep Console to Connect** must be enabled. The web rep console is supported on the following platforms and browsers:

Platforms

- Windows
- Mac
- Linux

Browsers

- Chrome 46+
- Firefox 42+
- Internet Explorer 11+
- Safari 8+
- Windows Edge



IMPORTANT!

Your BeyondTrust Appliance B Series must be equipped with a valid SSL certificate signed by a certificate authority. 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 access your endpoints from virtually anywhere.

Launch the Web Rep Console

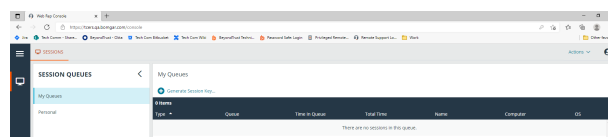
The web rep console enables you to use a web-based representative console to securely support customers and access remote systems by connecting to them remotely through the B Series Appliance. To begin using the web rep console to support customers, follow the steps outlined below.



Note: By default, the **web rep console** button is not available. You must navigate to **Management > Security** and check **Allow Mobile Representative Console** and **Web Rep Console to Connect** to activate the console.

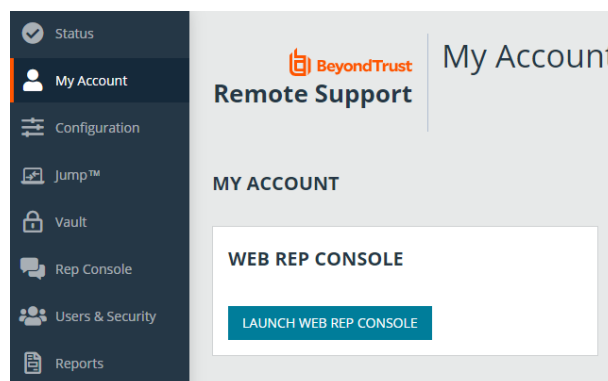
Launch the Web Rep Console Using /console

1. In the address bar of your browser, enter your BeyondTrust site host name followed by **/console** (support.example.com/console, for example).
2. Enter the username and password associated with your BeyondTrust user account.
3. Click **Login** to start your web-based representative console session.



Launch the Web Rep Console Using /login

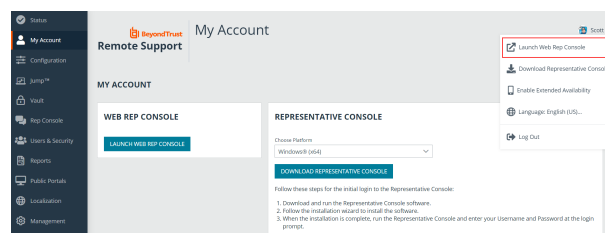
1. In the address bar of your browser, enter your BeyondTrust site host name followed by **/login** (support.example.com/login, for example).
2. Enter the username and password associated with your BeyondTrust user account.
3. Click **Login**.
4. Once you have logged into the /login administrative interface, click **My Account**.
5. Click the **Launch Web Rep Console** button.
6. The web rep console opens in a new tab, and you can begin supporting remote systems.



Note: Representatives using a Chrome OS device to support customers must use the web rep console.

Launch the Web Rep Console from the User Dropdown Menu

You can also launch the web rep console from the User dropdown menu located on the upper-right corner of the UI. This menu is accessible from any tab location in the administrative site.





Note: If you have more than one language enabled on your site, you can change the language used in the web rep console by clicking on the **Languages** link in the User dropdown menu and selecting the language you want. This language is applied to both the /login site and the web rep console.

Log in Directly to the Web Rep Console Using SAML

It is possible to configure an application or tile in a SAML identity provider (IdP), (like the tiles used to log into Okta and similar applications) that takes you directly to the web rep console rather than to /login. To configure this, you must:

- Set up application in the IdP as you would for /login
- Change the **RelayState** parameter to the word *console* (lowercase, no /, etc.)

There are two parts to the SAML configuration: the IdP and service provider (SP). In this instance you are the SP, and the SAML service is the IdP (OneLogin, Okta, and similar). Currently, you can export metadata from the SAML security provider on /login (in the Service Provider section), which you can then import into the IdP to help configure the SAML side. If, as part of this configuration, you set the **RelayState** parameter to **console**, then any login initiated from the IdP (for example, clicking the tile in Okta) sends you to the web rep console rather than to /login.

Authenticate to the Web Rep Console from the Client Scripting API

This feature allows users to log in to the web rep console and Jump to an endpoint using the [Remote Support Client Scripting API](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm) (<https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm>).

The Client Scripting API URL follows the format of **https://support.example.com/api/client_script**, where support.example.com is your B Series Appliance hostname.

The API accepts a client type (**web_console**), an operation to perform (**execute**), and a command (**start_jump_item_session**). No other commands are supported for the **web_console** client type.

If the user is logged into the desktop representative console when the Client Scripting API URL is accessed with **type=web_console**, then the user is logged into the web rep console and disconnected from the desktop representative console. If this behavior is not desired, then the user must use a Client Scripting API URL with **type=rep** instead of **type=web_console**.

Conversely, if the user is logged into the web rep console and the API calls **type=rep**, the user is logged into the desktop representative console and disconnected from the web rep console.

Here is an example of a valid Client Scripting API request:

```
https://support.example.com/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEF02
```

If the user is already logged into the web rep console, the above request runs the command in the browser tab running the web rep console. In this case, the command starts a session with the Jump Client whose hostname, comments, public IP, or private IP matches the search string "ABCDEF02."

If the user is not already logged into the web rep console, the above request opens a new browser tab and directs the user to /login to authenticate (this step is skipped if the user is already logged in to /login). The user is then redirected to the web rep console, and the command starts a session with the Jump Client whose hostname, comments, public IP, or private IP matches the search string "ABCDEF02."

In both cases, if more than one Jump Item matches the search criteria, the user must select the correct Jump Item from a list. If no Jump Items match the search criteria, the web rep console shows an error message to the user.

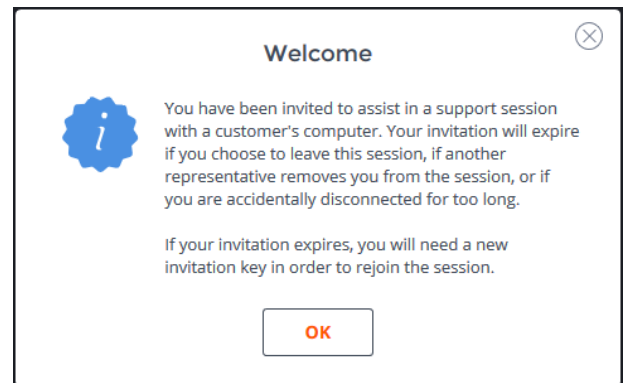
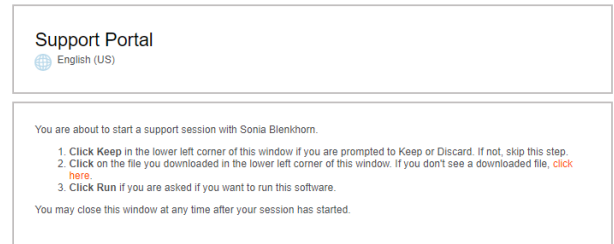
All of the search criteria for the **start_jump_item_session** command are supported with **type=web_console**, including:

- jump.method
- search_string
- client.hostname
- client.comments
- client.tag
- client.public_ip
- client.private_ip
- session.custom.<attribute code name>

Join a Session as an External Representative Using the Web Rep Console

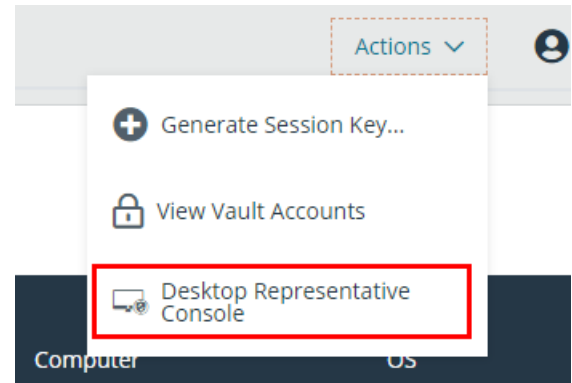
From the native representative console, a representative can invite an external user to participate in a session one time only. When the external representative clicks the rep invite URL, they are given the option to join the session using the web rep console or to download and install the desktop representative console. Once they have selected the web rep console or desktop representative console, they can join the session.

When the external representative joins the session, they are greeted with a welcome message. They have access only to the session they were invited to and have a limited set of privileges. The invited user can never be the session owner. If the inviting representative leaves the session without another session owner, the external representative is logged out.



Download the Desktop Representative Console from the Web Rep Console

While working in the web rep console, you can choose at any time to switch to working in the desktop representative console. Click on the **Desktop Representative Console** menu item located under the **Actions** menu in the top-right corner of the screen.



Note: Representatives using Chrome OS devices cannot download and use the desktop rep console.

If you already have the desktop representative console installed, run the BeyondTrust Representative Console Script to open and log in to the representative console. Any sessions active in the web rep console open in the desktop representative console. You are automatically signed out of the web rep console.

If you do not already have the desktop representative console installed, you must first follow the link to the **My Account** page to download and install the desktop representative console. You may then run the BRCS file.



Note: On a Linux system, you must save the file to your computer and then open it from its download location. Do not use the **Open** link that appears after downloading a file from some browsers.

RUN REPRESENTATIVE CONSOLE

1. If you have not already, download & install the Representative Console for your platform from your [My Account](#) page.
2. A file with a ".brcs-techcomm_ers" extension should download in your browser momentarily. [If not, click here.](#)
3. Open the ".brcs-techcomm_ers" file to launch the desktop Representative Console.

DISMISS

View Support Sessions in Queue in the Web 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.

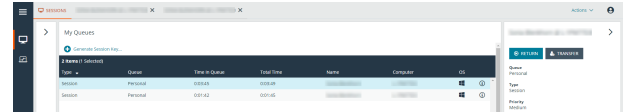
Click the star to the left of a team name to mark that queue as a favorite. If a team chat message is sent, an orange chat bubble appears in place of the star.

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.

Additionally, when a new session enters one of your queues, a popup alert appears in the lower-left corner of your screen. You can click the **View** button to see the session details in queue.

Click a queue name to view its sessions. Click a session entry to view details about the support request. To begin supporting the selected session, click the **Accept** button. Accepting a session switches your view to session view. You can run multiple sessions simultaneously.

Alternatively, you can transfer a session to another queue. Click the **Transfer** button. Choose **Support Teams** or **Representatives**. Select the queue to which you wish to move the session and then click the **TRANSFER** button.



New Session

Your Personal Queue has a new session. [View](#) [Dismiss](#)

TRANSFER SESSION

Support Teams

Team: Remote Support

Team: General

Representatives

Rep:

CANCEL

TRANSFER

Start a New Session with a Session Key in the Web 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. Click the **Generate Session Key** button at the top right of the screen. This opens a menu from which you can edit the session key details.

 [Generate Session Key...](#)

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 either to go to the unique URL or to enter the session key on your public site. Click on the session key or the URL to copy it to your clipboard.

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.

SUPPORT SESSION KEY

You may start a support session with a customer by directing them to enter the following session key on your Support Portal, by sending them directly to the following URL, or by emailing an invitation.

Session Key

9932 3793 7275 

URL

<https://tcers.qa.bomgar.com/?ak=80556a15d00ccc1> 

Expires in

10 Minutes 

August 26, 2021, 10:00:03 AM

Public Portal

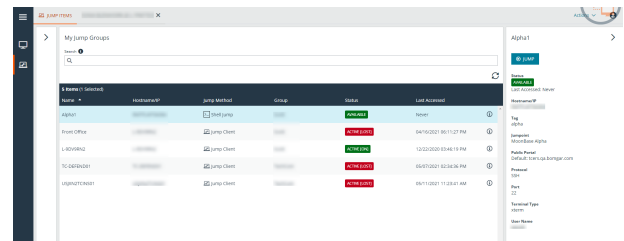
Default: tcers.qa.bomgar.com 

[CLOSE](#) [SEND LOCAL EMAIL](#)

Use Jump Items to Support Remote Systems in the Web Rep Console

BeyondTrust Jump Technology enables privileged users to connect to an unattended remote system to start a session without end-user assistance.

Jump Items can be installed from the **Jump Clients** page of the /login interface or from the native representative console.



Note: 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 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 view details about a Jump Item, click the plus sign beside the Jump Item's name. To start a session with a Jump Item, click the **Jump** button at the right of the Jump Item entry.



Note: The **Frequently Used Jump Items** list displays all of the Jump Items that you access on a regular basis. To start a session with a frequently accessed system, hover your mouse over the item and click **Start Session**.



Note: The Jump Items list can only display a maximum of 50 Jump Items.

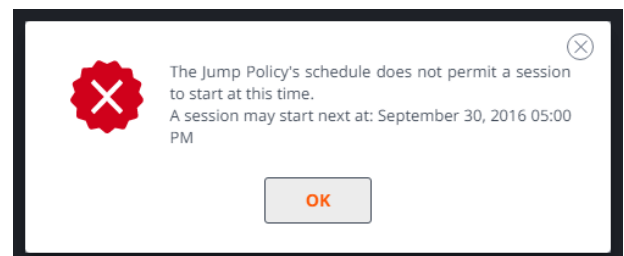


Note: If you need to access Jump Items when no user is available, make sure the session permissions are set either to disable prompting or to default to **Allow** for unattended sessions.

If a Jump Policy enforces a schedule for this Jump Item, an attempt to access the Jump Item outside of its permitted schedule prevents the Jump. A prompt informs you of the policy restrictions and provides the date and time when this Jump Item is next available for access.



Note: If you have permission to modify Jump Policies, the prompt gives you the option to override the schedule and start a session anyway.



Log in to Remote Systems Using Credential Injection from the Web Rep Console

When accessing a Windows-based Jump Item via the web rep 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 or password vault available to connect to BeyondTrust Remote Support.

Install and Configure the Endpoint Credential Manager

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



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

System Requirements

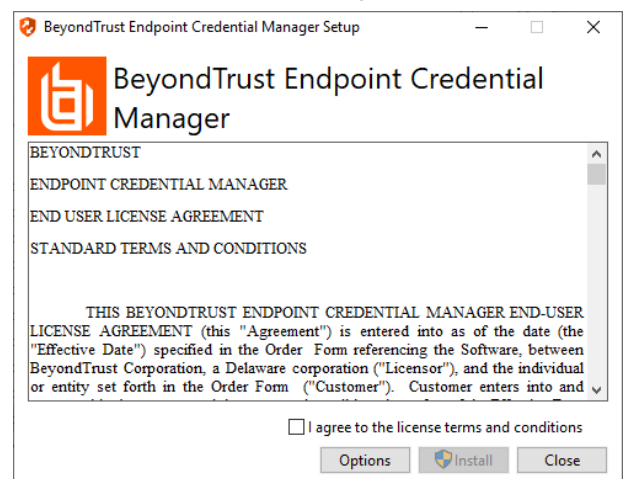
- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from [BeyondTrust Support](https://www.beyondtrust.com/docs/index.htm#support) at <https://www.beyondtrust.com/docs/index.htm#support>. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
2. Agree to the EULA terms and conditions. Check the box if you agree, and click **Install**. If you wish to modify the installation path, click the **Options** button to customize the installation location.

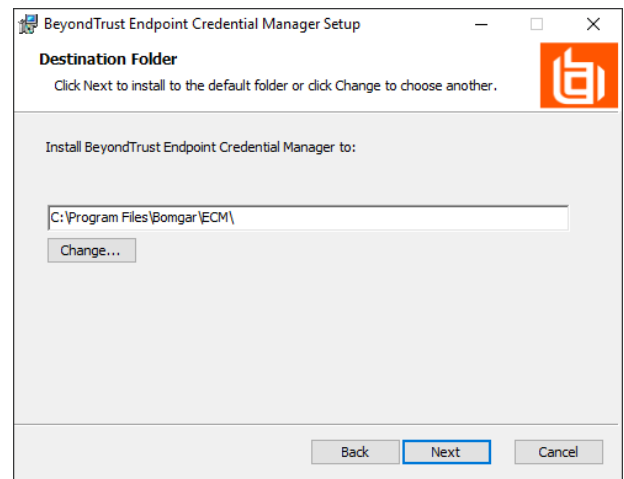


Note: You are not allowed to proceed with the installation unless you agree to the EULA.

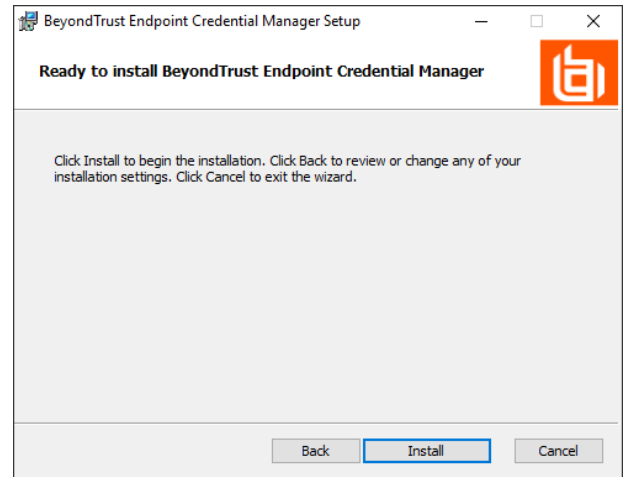
3. Click **Install**.



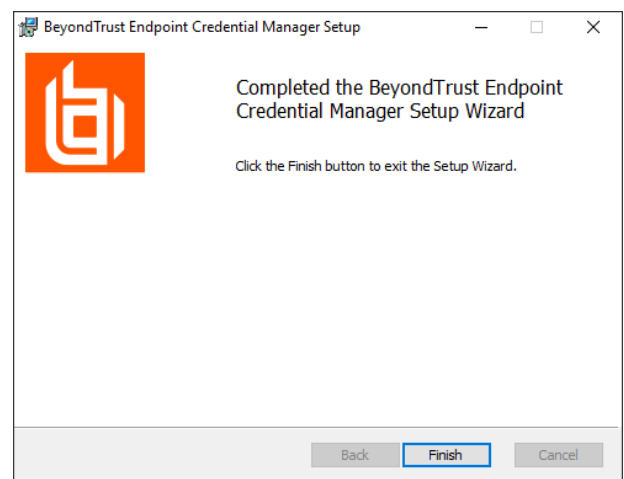
4. Choose a location for the Credential Manager and click **Next**.
5. On the next screen, you can begin the installation or review any previous step.



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



7. The installation will take 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.



Note: If you get a Windows plugin error during installation, locate and unblock **BomgarVaultRestPlugin.dll**.

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.

BeyondTrust-ECMConfigurator.exe	7/23/2019 2:35 PM	Application	317 KB
BeyondTrust-ECMConfigurator.exe.config	7/23/2019 2:35 PM	CONFIG File	1 KB
BeyondTrust-ECMService.exe	7/23/2019 2:35 PM	Application	26 KB
BeyondTrust-ECMService.exe.config	7/23/2019 2:35 PM	CONFIG File	2 KB
Configurator.log	11/14/2019 3:06 PM	Text Document	3 KB
ECM.dll	7/23/2019 2:35 PM	Application exten...	65 KB
ECM.log	11/14/2019 3:06 PM	Text Document	4 KB
ECM.settings	7/23/2019 2:35 PM	SETTINGS File	1 KB
log4net.dll	7/23/2019 2:35 PM	Application exten...	294 KB
Newtonsoft.Json.dll	8/3/2014 9:33 PM	Application exten...	491 KB
Util.dll	7/23/2019 2:35 PM	Application exten...	31 KB


BeyondTrust

Client Id:

71318f0745c0c6f1b010fb0cc7ccfa3f1de2a8b

Client Secret:

.....

Site:

support.example.com

Port:

443

Plugin:

BeyondTrust Password Safe Plugin



Save

Cancel

1.5.0.1127 (1.4.1.5)

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.

1. When you click the **Choose Plugin...** button, the ECM location folder opens.
2. Paste your plugin files into the folder.
3. 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.



IMPORTANT!

To apply new settings in the configuration, restart the ECM service.

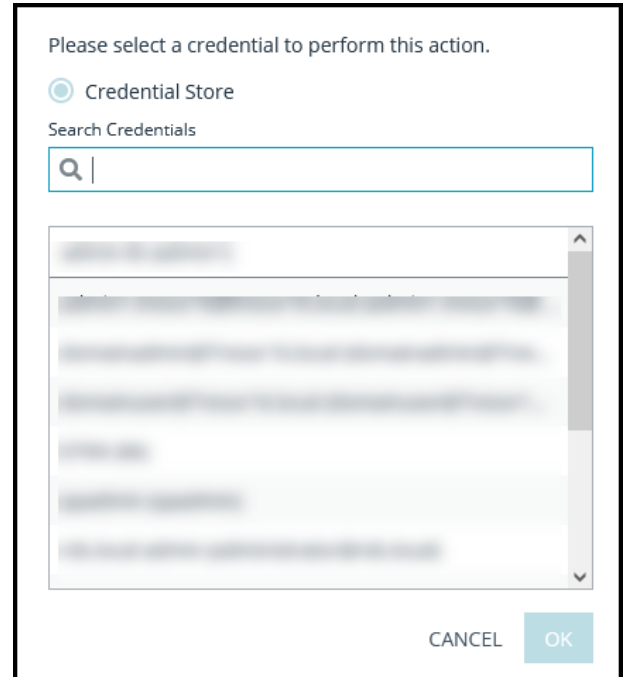
Use Credential Injection to Access Remote Systems

After the credential store has been configured and a connection established, the web rep console can begin using credentials in the credential store to log in to remote systems.

1. Log in to the web rep console.
2. Jump to a remote system with a Jump Item installed as an elevated service on a Windows machine.
3. Click the **Play** button to begin screen sharing with the remote system. If the remote system is at the Windows login screen, the **Inject Credentials** button is highlighted.
4. Click the **Inject Credentials** button. A pop-up credential selection dialog appears, listing the credentials available from the ECM.



5. Select the appropriate credentials to use from the ECM. The system retrieves the credentials from the ECM and injects them into the Windows login screen.
6. The representative is logged in to the remote system.



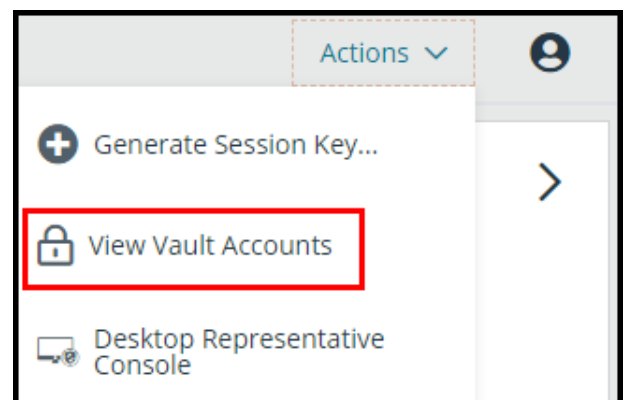
Note: When using BeyondTrust Vault, the maximum number of credentials that can display in the dropdown menu is 2,000. When using the ECM, the limit is 200.

Check In and Check Out Credentials

From the web rep console, you can easily access the BeyondTrust Vault in the **/login** interface to check out and check in credentials when necessary, either during a session or on your local machine.

To access the Vault, click the **View Vault Accounts** menu item located under the **Actions** menu at the top-right of the screen. You are taken directly to the **Vault > Accounts** page in the **/login** interface, once logged in.

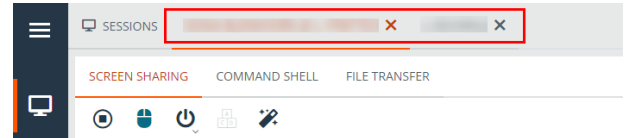
You can then locate and check out or check in a Vault account.



Manage Multiple Support Sessions in the Web Rep Console

Return to an Active Session

If you have multiple support sessions in progress, you have the ability to return to any other session at any time. To return to a system you are already accessing in another session, click on the desired support session at the top of the screen.



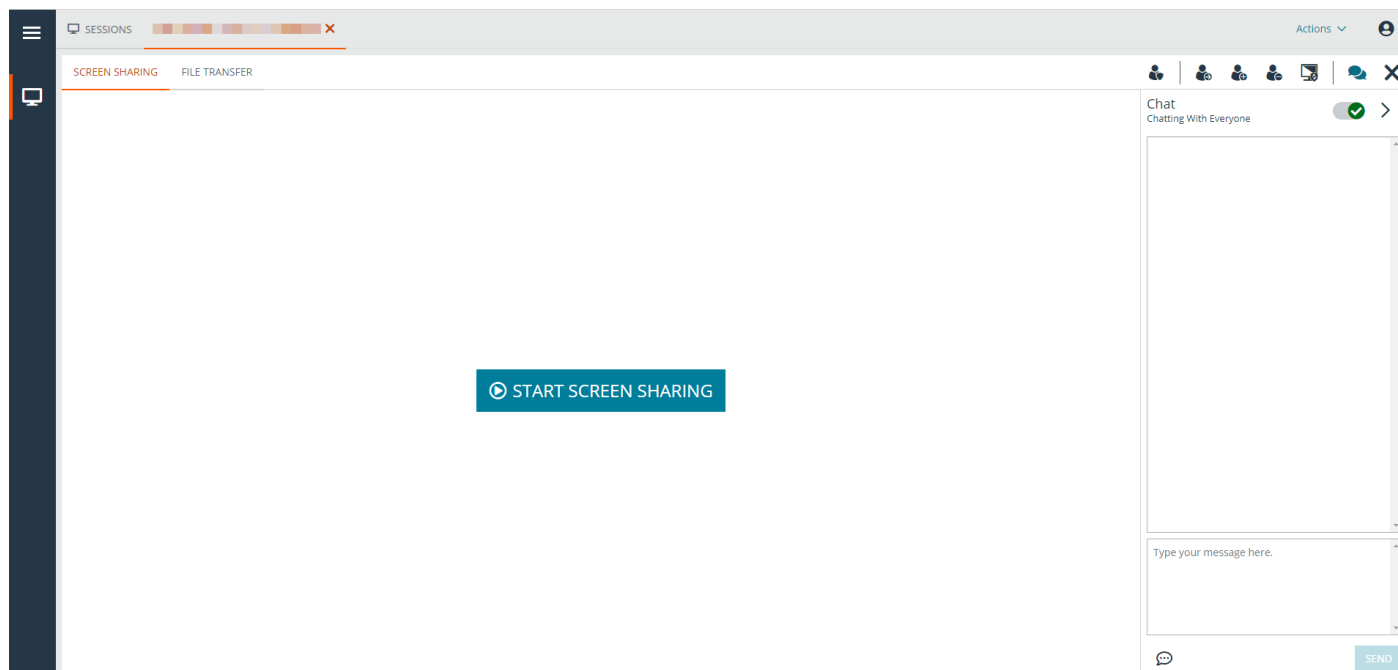
When a new session enters one of your queues, a popup alert appears in the lower-left corner of your screen. You can click **View** to see the session details in queue.



Note: When supporting a mobile client, the web representative console provides View Only support.

Support Session Actions in the Web Rep Console

In a support session, chat with the customer, start a screen sharing session, or start a command shell session. The button at the top-left of the session interface gives you access to the remote system, while the buttons at the top-right of the session interface allow you to manage the session as a whole.



Support Session Actions

	When a compatible iOS device is detected, the Special Actions icon appears, allowing the representative to push iOS screen sharing instructions to the device.
 	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.

	Elevate a click-to-chat session to the full customer client, or elevate the customer client to have administrative rights by clicking the shield button. Select Prompt Customer to request admin credentials from the remote user. If you possess administrative credentials to the remote computer, select Specific User and supply an administrative username and password. 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.
	Should you decide someone else is better suited to handle a session, transfer control of that session to another team or user. Remain as a participant or close your tab to leave the session with its new owner. Once you have transferred the session to a new owner, your Transfer, Share, and Remove icons become gray, and you are no longer able to perform these actions, as you are no longer the session owner. The session persists until the new owner of the session closes the session.
	Invite another user to participate in a shared session. You maintain ownership of the session but can receive input from one or more teammates.
	The session owner can remove another user from a shared session. Additionally, you can disconnect the customer but remain in the session tab.
	Show or hide the chat bar.
	Pin or unpin the chat bar.
	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.



For more information on iOS screen sharing, please see [Screen Share with the iOS Device](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm) at <https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm>.

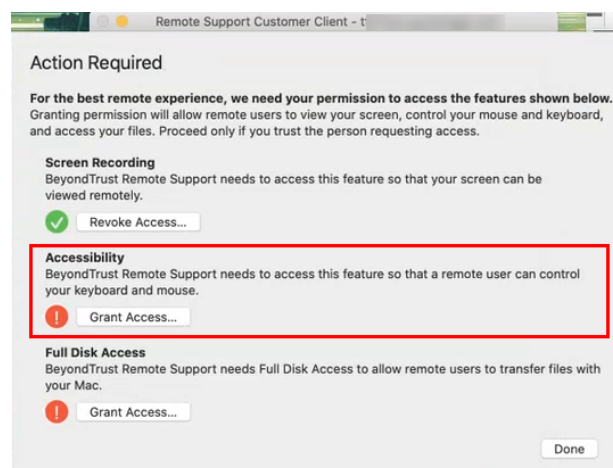
-Control the Remote System with Screen Sharing in the Web Rep Console

To view and control a customer's screen, use the screen sharing action while in a support session.

From the session window, click the **Start Screen Sharing** button to begin accessing the system.



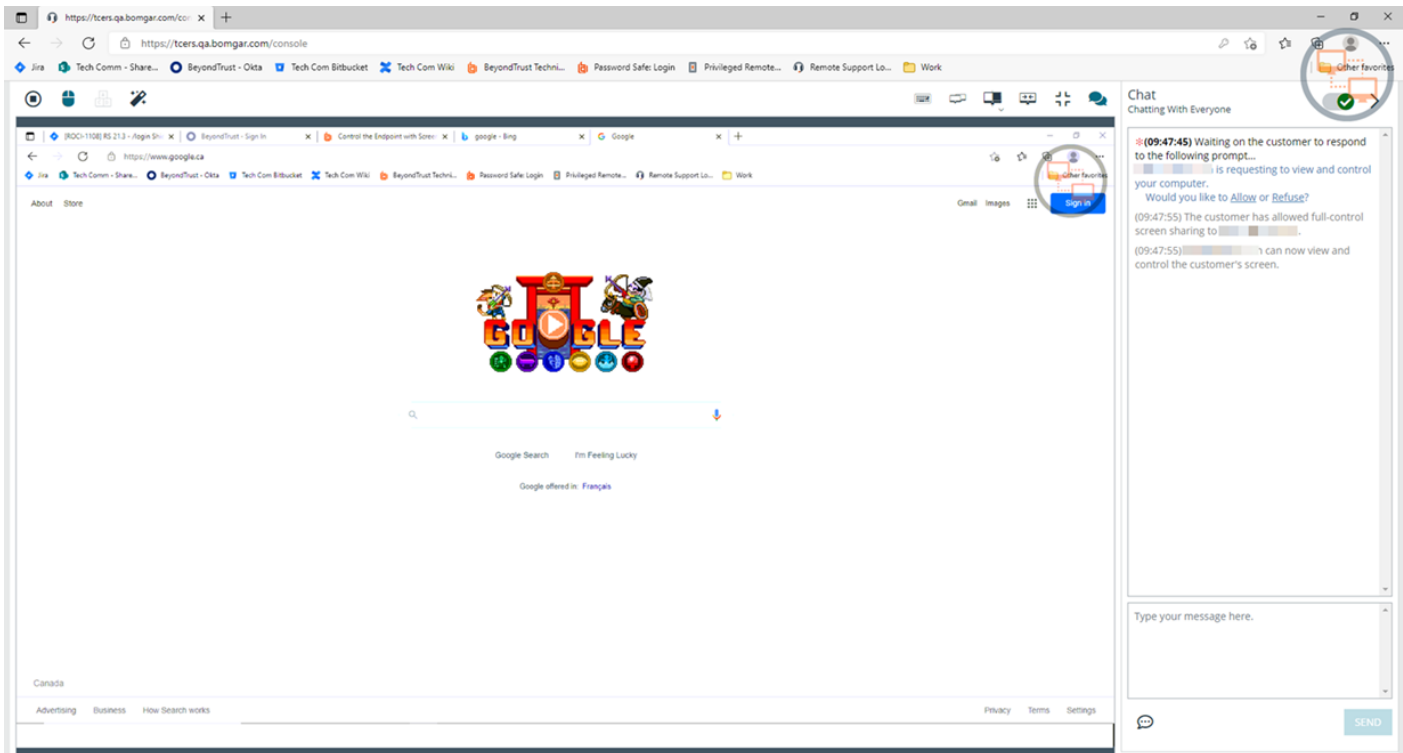

Note: For macOS Catalina (10.15)+ systems, if remote control is not enabled, click the link at the top of the **Screen Sharing** page to prompt the customer for permissions. The customer can then grant access when prompted in the Customer Client, and the representative is directed to the correct panes in **Settings** to update the permissions.



Use any of the following actions while in a session to perform different functions.

Screen Sharing Tools

	Stop screen sharing.
	While viewing the remote computer, start or stop control of the remote keyboard and mouse.
	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.
	Send a Ctrl-Alt-Del command to the remote computer.
	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.
	Toggle the virtual keyboard.
	Select an alternate remote monitor to display. The primary monitor is designated by a P .
	View the remote screen at actual or scaled size.
	Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select Video Optimized ; otherwise select between Black and White (uses less bandwidth), Few Colors , More Colors , or Full Color (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.
 	View the remote desktop in full screen mode or return to the interface view. When in full screen mode, special keys are passed through to the remote system. This includes but is not limited to modifier keys, function keys, and the Windows Start key. Note that this does not apply to the Ctrl-Alt-Del command.



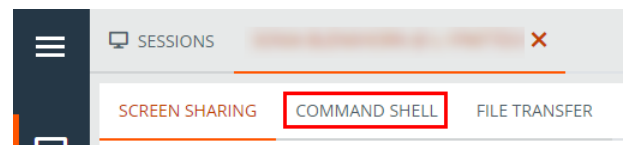
Access the Command Shell on the Remote System through the Web Rep Console

Remote command shell enables a privileged representative to open a virtual command line interface to the remote computer. The user can then type locally but have the commands executed on the remote computer. You can work from multiple shells.

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

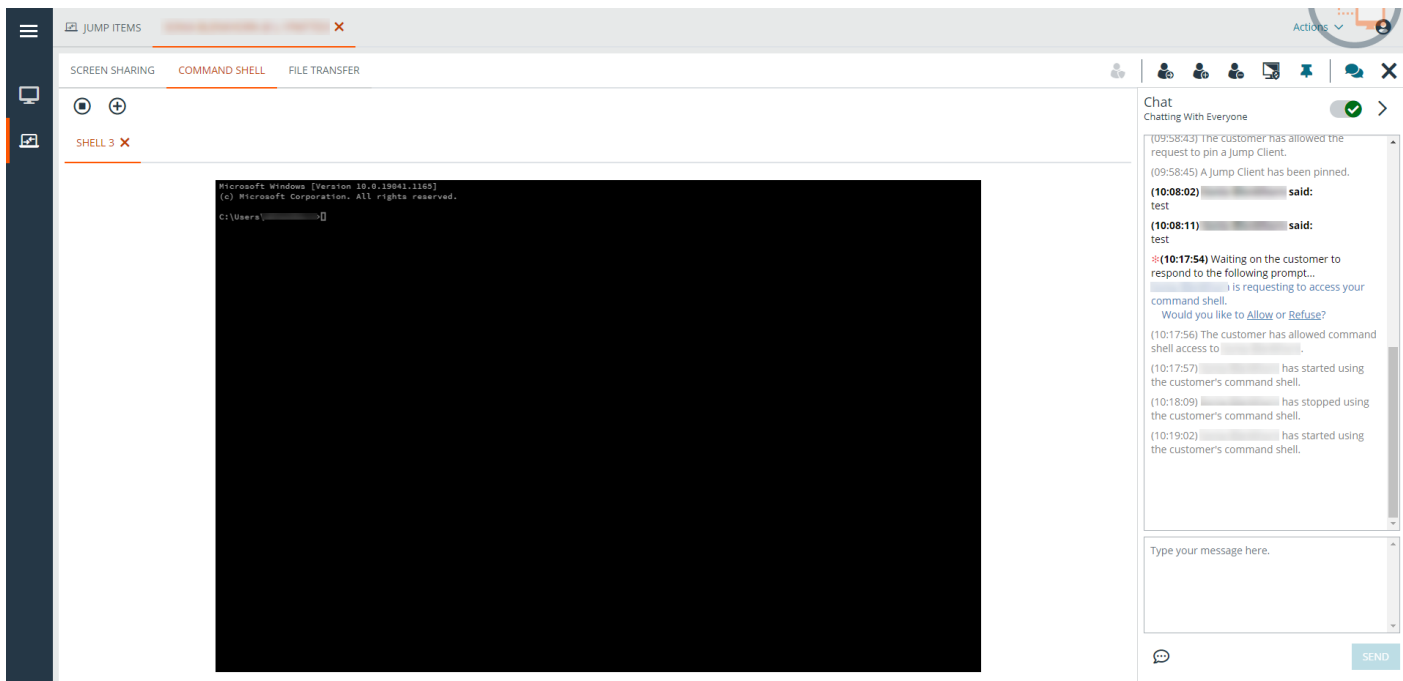
To access the command shell while in an support session, click on **Command Shell** at the top of the screen.

After **Command Shell** is clicked, the command options and prompt appear.



Command Shell Tools

 START THE COMMAND SHELL		Start or stop command prompt access.
		Open a new shell to run multiple instances of command prompt. Shells are tabulated at the top of the screen.



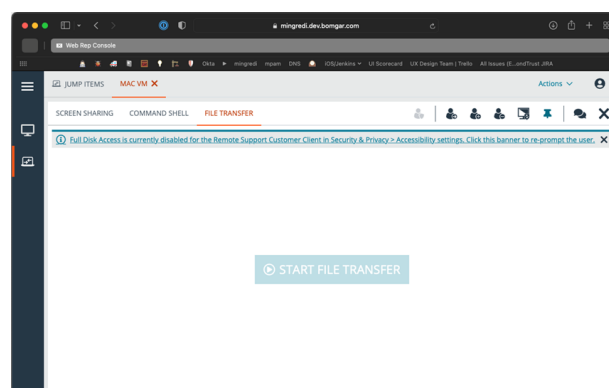
The screenshot displays the BeyondTrust Remote Support console interface. At the top, there's a navigation bar with 'JUMP ITEMS' and a tabbed interface with 'SCREEN SHARING', 'COMMAND SHELL' (selected), and 'FILE TRANSFER'. Below the tabs, there's a sidebar with icons for various tools. The main area shows a terminal window titled 'SHELL 3' with a Windows command prompt. On the right, a chat window is open, showing a list of messages and a 'SEND' button.

Use the Web Rep Console to Transfer Files to and from Remote Systems

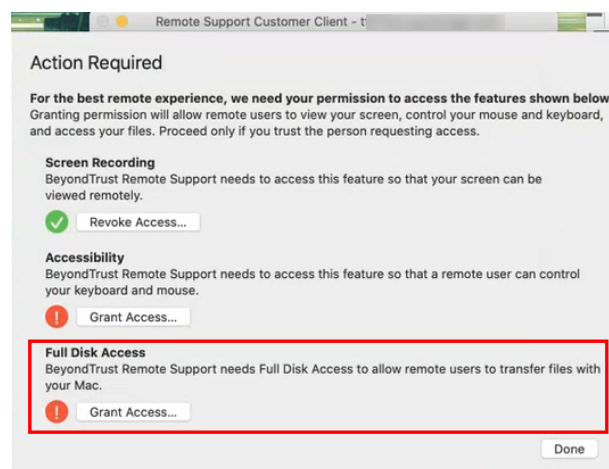
During a session, representatives can transfer, delete, or rename files and directories both to and from the remote system. You do not need to have full control of the remote computer to transfer files.

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

For macOS Catalina (10.15)+ systems, if screen sharing is not enabled, click the link at the top of the **File Transfer** page to prompt the user for permissions to transfer files.



The customer can then grant access when prompted in the Customer Client, and the representative is directed to the correct panes in **Settings** to update the permissions.



Transfer files by using the upload and download buttons. Review transfer and deletion progress by clicking the **Transfer Progress** down arrow at the bottom of the screen. Download, rename, or delete files by clicking on the **More Options** icon.

To start transferring files to a system, click on **File Transfer** at the top of the screen.

Click the **Start File Transfer** button to start transferring files. Then select a place to start browsing from the **Volumes** column. The breadcrumbs at the top show your current location. Double-click on a directory to open it.



SESSIONS

SCREEN SHARING

FILE TRANSFER

Volumes

C:\

Documents [C:\Users\...\Documents\]

Desktop [C:\Users\...\Desktop\]

Home [C:\Users\...\]\

C:\ > Users > Desktop

3 Files, 2 Directories (1 File Selected | [Select All 3 Files](#))

Name	Modified	Size
Go up a directory	-	-
Images	Jul 26, 2021	-
PDFs	Aug 24, 2021	-
Google Chrome.Ink	Jun 29, 2021	2.24 KB
Microsoft Teams.Ink	Aug 31, 2021	2.34 KB
pra-cloud-admin.pdf	Aug 24, 2021	1.78 MB

File Transfer Tools

	Stop access to the remote device's file system.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Show hidden files.
	Create a new directory.
	Upload a file to a directory.
	Download selected files from a directory.
	Delete selected files from a directory.
	Hover over an item and click for more options, such as downloading, renaming, or deleting a directory or file.  Note: When deleting a file or folder, it is permanently deleted. It is not sent to the recycle bin.

Add a Support Button from the Web Rep Console

While in a session, you can deploy a Support Button to the remote computer, providing a quick method for your customers to request support. To begin, click the button to **Deploy a Support Button**. This opens a menu from which you can edit the Support Button details.



Enter a description to be seen by you and any other representatives who will have access to this Support Button.

Choose a profile to apply to this Support Button. Profiles are configured in **/login > Configuration > Support Buttons**.

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 specified queue.

Set how long this Support Button should last. The customer can use this button to start sessions only as long as this specified time. This 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, click **Deploy**. This creates a Support Button on the remote user's system. Your customer can now use the Support Button to quickly request support.

ADD SUPPORT BUTTON

Select the options for deploying the Support Button to the customer.

Description

End User @ Windows® (x64) (

Icon Preview



Support Button
[bomgar.com]

Profile

Default

Queue

Personal

Expiration

1 Month

October 20, 2021, 8:44:19 AM

CANCEL

DEPLOY

You also may delete the Support Button from the remote system by clicking the button to **Remove Support Button**. When prompted to confirm that you would like to remove the Support Button from the customer's computer, click **Yes**.



Pin a Jump Client from the Web 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, click the **Pin the Jump Client** button. This opens a menu to configure the Jump Client.



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 only to members of that group.

If you wish to pin the Jump client without setting a password, you can click **Pin Session** now.

Alternatively, you may set a password for this Jump Client. Setting a password requires 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 click **Pin Session**.

PIN AS A JUMP CLIENT

Select the queue to pin this session to as a Jump Client.

Queue

Personal

Optional Password

Confirm Password

CLOSE PIN SESSION

If you no longer need unattended access to the remote system, remove the Jump Client by clicking the **Unpin the Jump Client** button. When prompted to confirm that you want to uninstall the Jump Client, click **Yes**.



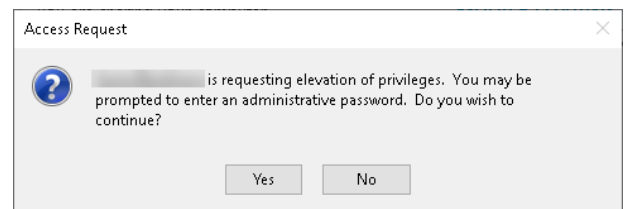
Elevate the Session in the Web Rep Console

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 from a click-to-chat session to the full customer client, click the **Run Full Remote Support Customer Client** button in the center of the screen or the **Elevate** button at the top of the session window.

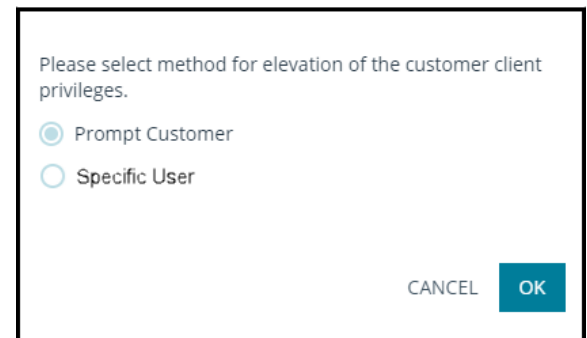
The customer is prompted to download and run the full customer client.


RUN FULL REMOTE SUPPORT CUSTOMER CLIENT

To elevate the customer client to have administrative privileges, click the **Elevate** button at the top of the session window. A prompt for administrative credentials appears.

To request the customer to provide administrative credentials for their computer, select **Prompt Customer** and then click **OK**.

Alternatively, if you possess administrative credentials to the remote computer, select **Specific User** to supply an administrative username and password, yourself. Then click **OK**.



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

If you are the session owner and would like to transfer control of the session to another team or representative, click the **Transfer** button.



Select either **Support Teams** or **Representatives**. Browse the list of available teams or representatives.

TRANSFER SESSION

▼  Support Teams

 Team: Remote Support

 Team: General

▼  Representatives

 Rep:

CANCEL

TRANSFER

Choose the location to which you wish to transfer the session and then click **Transfer**.

When someone accepts the session, you remain in the session as a participant but are no longer the session owner.

Share a Session with Other Users Using the Web Rep Console

Within a session, you can request a team member to participate in a support session. To share a session, click on the **Share Session** icon.



From the menu, select a team name, the **Request Help** option, or the **Representatives** option.

SHARE SESSION

▼

Support Teams

>

Team: General

>

Team: Remote Support

>

Request Help

>

Representatives

CLOSE

SHARE

From the team listing, choose the user with whom you would like to share the session or select **Any Representative**. If you select a representative's name, the invitation is sent to that rep's personal queue. If you select **Any Representative**, the invitation is sent to the team queue so that any single representative in the selected queue can join the session. You can send multiple invitations if you want more representatives from the team to join your session.

Alternatively, you can use **Request Help** to route your request so that it is targeted as a specific support issue. Only issues that have been configured to allow you to request help display on this list.

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.

Once the rep has accepted the invitation and entered the session, you can chat with them by clicking on the **Chat** icon at the top of the screen.

If you have sent an invitation and it is still active, you may revoke the invitation by finding it in the **Cancel Invitation** menu and clicking 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 rep to join the same session. The invitation disappears if:

- 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

When an additional user joins a shared session, they are able to see the entire chat history.



Chat

Chatting With Everyone



*(14:44:04) Waiting on the customer to respond to the following prompt...

Would you like to Allow or Refuse?

(14:44:09) [REDACTED] Waiting for the customer to choose which window or screen to share.

(14:44:09) The customer has allowed view-only screen sharing to [REDACTED].

(14:44:09) [redacted] can now only view the customer's screen.

(14:44:14) [REDACTED] The customer is now sharing their window or screen.

(14:49:39) A session invitation was sent to

(14:49:48) [REDACTED] has accepted the invitation to this support session.

(14:49:48) [REDACTED] has joined the conversation.

(14:50:04) You said:
Hi, how can I help you?

(14:50:24) [REDACTED] said:
My screen is frozen.

Type your message here.



Remove a Member from a Web Rep Console Session

When needed, you can remove another user from a shared support session. To remove a user, click on the **Remove Member** icon.



From the menu, choose the participant you wish to remove, and then click **Remove**.



Note: *You must be the owner of the session to remove another member.*

REMOVE MEMBER

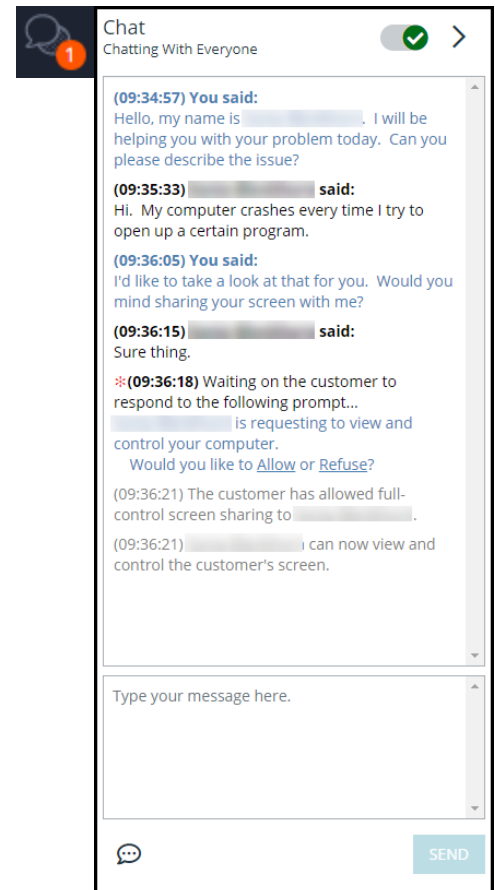
Customer:

Chat with the Remote User from the Web Rep Console

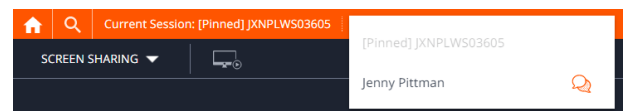
Throughout the support session, you can chat with your remote customer. You do *not* need to have screen sharing permissions before beginning chat.

If you receive a message while the chat area is minimized, the chat icon displays the number of messages waiting. Click the **Chat** button to open or close the chat area.

You can also chat with any other representatives who are sharing the session.



If you are in one session and receive a chat message in another session, a chat icon appears in the active session dropdown at the top of the screen. When you open the dropdown, a chat icon appears to the right of any session that has a waiting chat message.



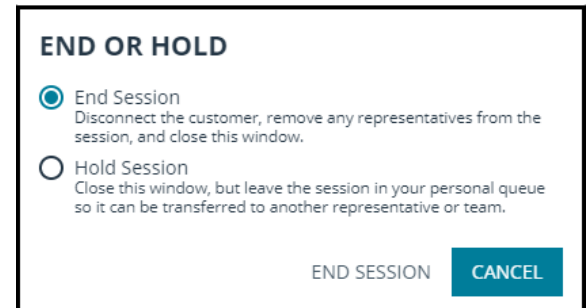
Close the Web Rep Console Session

To exit a session, click the **X** icon in the top-right corner of the screen. A confirmation prompt appears.

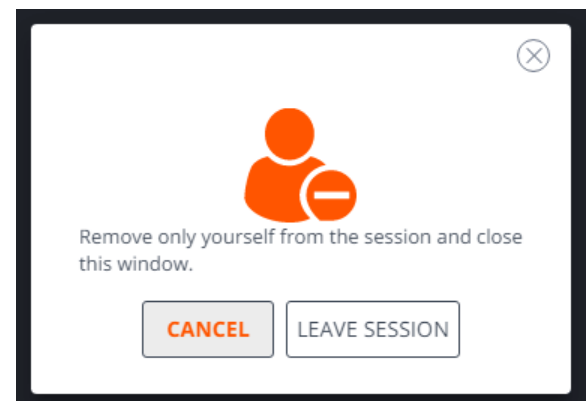


If you are the session owner, choosing **End Session** closes the session in your representative console and removes any additional representatives who may be sharing the session. It also uninstalls the customer client from the remote system. However, it does not delete an installed Jump Client.

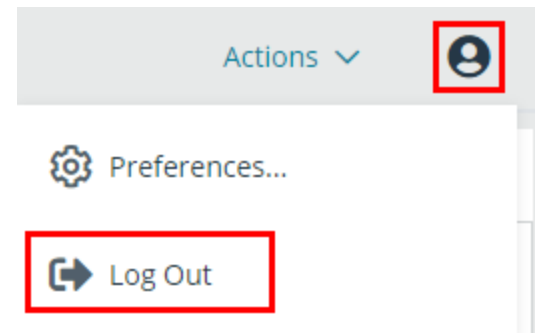
If you choose **Hold Session**, the session closes in your representative console but returns to wait in your personal queue. If any additional representatives are sharing the session, they remain in session.



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



To log out of the web rep console entirely, select the **Logout** menu item under the **User Menu** at the top-right of the screen.



You are immediately logged out, and a message appears confirming this status.