BeyondTrust

Remote Support 24.1
Web Rep Console

Table of Contents

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 Applianceas detailed in the BeyondTrust Appliance B Series Hardware Installation Guide at https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware-sra/index.htm. 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

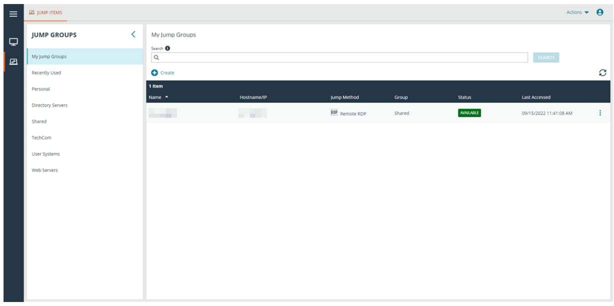
The web rep console enables you to use a web-based representative console to securely support customers and access remote systems by connecting to them remotely through the B Series Appliance. To begin using the web rep console to support customers, follow the steps outlined below.

> ***Note:** Representatives using a Chrome OS device to support customers can use only the web rep console.*

Launch the Web Rep Console Using /console

This is the quickest way to access the web console.

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



1 Item

Name	Hostname/IP	Jump Method	Group	Status	Last Accessed
[redacted]	[redacted]	Remote RDP	Shared	AVAILABLE	09/15/2022 11:41:08 AM

FIDO2-certified authenticators can be used to securely log in to the desktop representative console, web rep console, and the /login administrative interface without entering your password. You can register up to 10 authenticators.

If passwordless login has been enabled, **Authenticate Using** may default to **Passwordless FIDO2**, or it can be selected. The exact process for passwordless login depends on the type of device and manufacturer.

You can enable passwordless login and set the default authentication after logging into the /login administrative interface, by navigating to **Management > Security**, and then registering passwordless authenticators at **My Account > Security**.

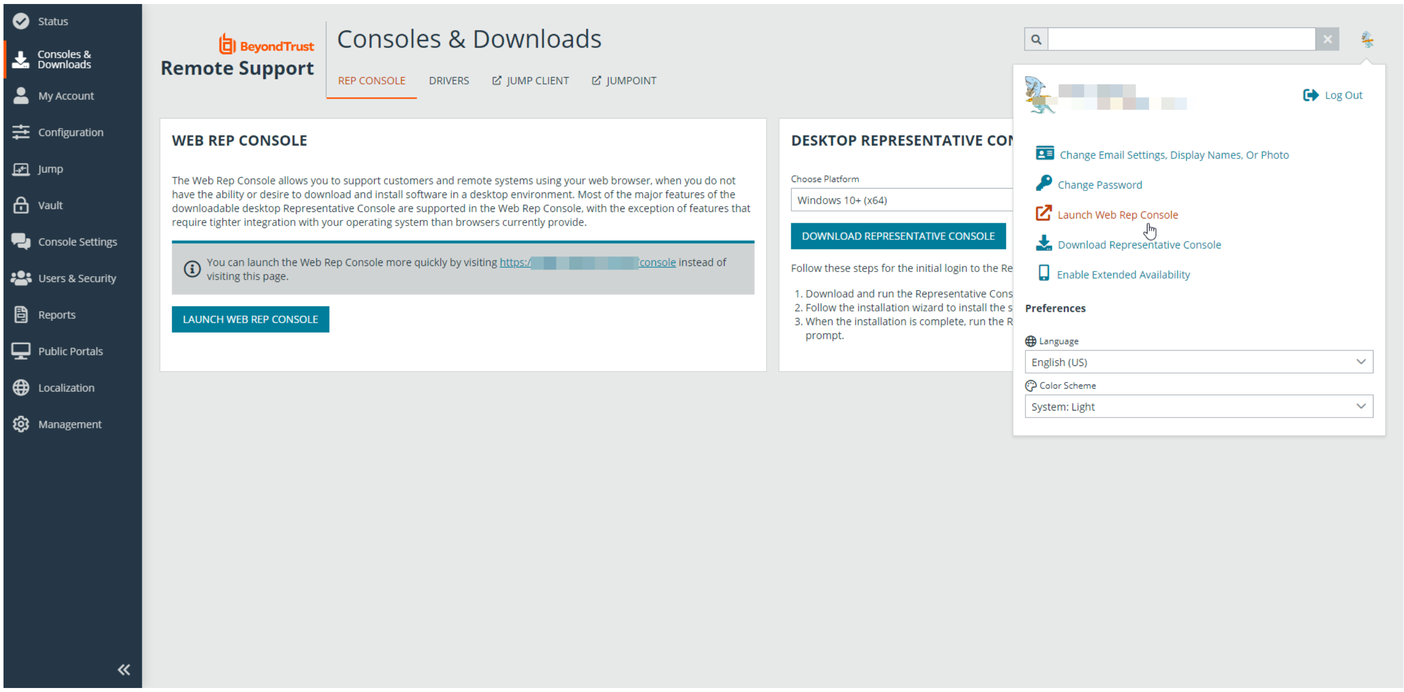
> ***Note:** Passwordless login for the desktop representative console on macOS or Linux systems is supported only for roaming authenticators (such as the YubiKey hardware security keys). Platform or integrated authenticators (such as Face ID and fingerprint scanners) are not supported for the desktop desktop representative console login when using macOS or Linux systems.*

Launch the Web Rep Console Using /login

> ***Note:** By default, this option is not available. To launch the web console from the /login administrative interface, you must navigate to **Management > Security** and check **Allow Mobile Representative Console and Web Rep Console to Connect**.*

1. In the address bar of your browser, enter your BeyondTrust site host name followed by **/login**, for example, **access.example.com/login**.
2. Enter the username and password associated with your BeyondTrust user account, and click **Login**, or log in using passwordless authentication.

3. Click **Consoles & Downloads** in the left menu, or click the user icon in the upper-right corner of the screen. The image below shows both options selected.



Consoles & Downloads

WEB REP CONSOLE

The Web Rep Console allows you to support customers and remote systems using your web browser, when you do not have the ability or desire to download and install software in a desktop environment. Most of the major features of the downloadable desktop Representative Console are supported in the Web Rep Console, with the exception of features that require tighter integration with your operating system than browsers currently provide.

You can launch the Web Rep Console more quickly by visiting https:/[redacted]console instead of visiting this page.

DESKTOP REPRESENTATIVE CON

Choose Platform: Windows 10+ (x64)

Follow these steps for the initial login to the Re

1. Download and run the Representative Cons
2. Follow the installation wizard to install the s
3. When the installation is complete, run the R prompt.

[redacted]

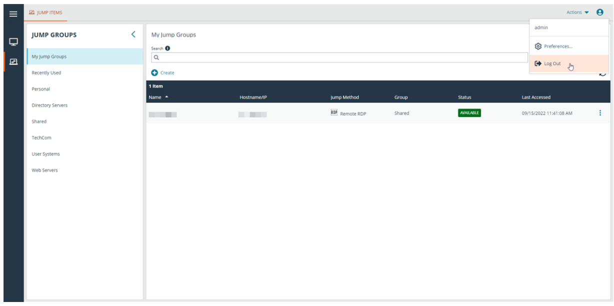
Preferences

Language: English (US)

Color Scheme: System: Light

4. Click **Launch Web Rep Console** on the **Consoles & Downloads** screen or on the user options window.
5. The web rep console opens in a new tab, and you can begin working with endpoints.

To log out of the web rep console, click the user icon in the upper-right corner of the screen and click **Log Out**. This does not log you out of the /login administrative interface. To log out of the /login administrative interface, click the user icon in the upper-right corner of that screen and click **Log Out**.



My Jump Groups

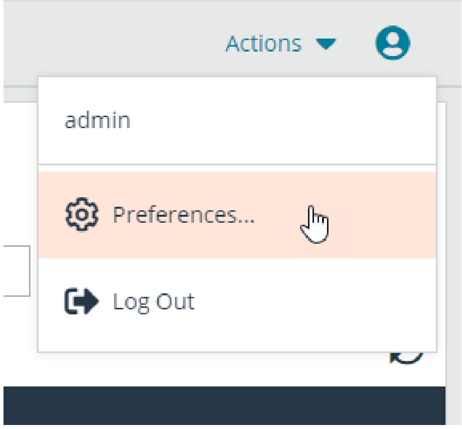
Search

1 Item

Name	Hostname/IP	Jump Method	Group	Status	Last Accessed
[redacted]	[redacted]	Remote RDP	Shared	AVAILABLE	09/15/2022 11:41:08 AM

Web Rep Console Preferences

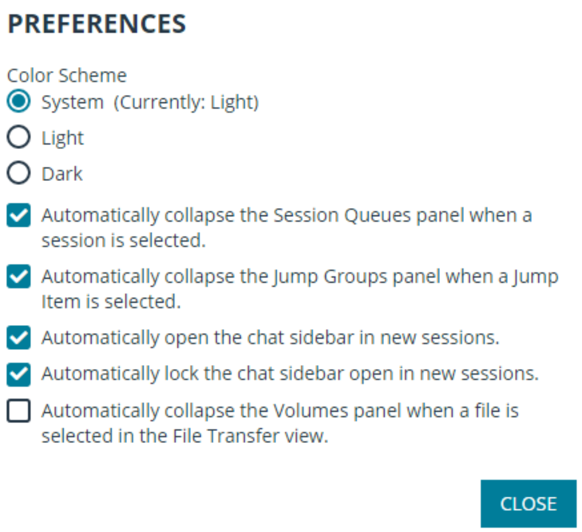
The language and color scheme options visible when the user icon is clicked in the /login administrative interface affect only that interface. To set preferences in the web rep console, click the user icon in the upper-right corner of the web rep console, and then click **Preferences**. Select your preferences in the pop-up window.



Select your preferred color scheme. You can switch between **Light** and **Dark** modes, or **System**, which uses whatever mode is selected for your system.

Select any of the automatic options you would like to use:

- Automatically collapse the **Session Queues** panel when a session is selected.
- Automatically collapse the **Jump Groups** panel when a Jump Item is selected.
- Automatically open the chat sidebar in new sessions.
- Automatically lock the chat sidebar open in new sessions.
- Automatically collapse the **Volumes** panel when a file is selected in the **File Transfer** view.



PREFERENCES

Color Scheme

● System (Currently: Light)
○ Light
○ Dark

☑ Automatically collapse the Session Queues panel when a session is selected.
☑ Automatically collapse the Jump Groups panel when a Jump Item is selected.
☑ Automatically open the chat sidebar in new sessions.
☑ Automatically lock the chat sidebar open in new sessions.
□ Automatically collapse the Volumes panel when a file is selected in the File Transfer view.

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).

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."

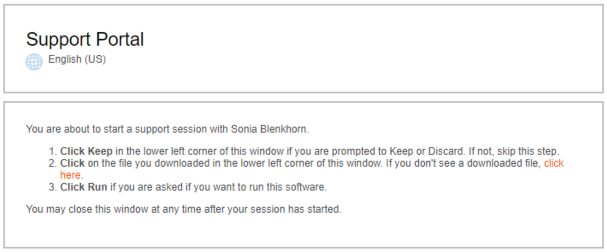
In both cases, if more than one Jump Item matches the search criteria, the user must select the correct Jump Item from a list. If no Jump Items match the search criteria, the web rep console shows an error message to the user.

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, representatives with the appropriate permission and session policy can invite external representatives to participate in a session, for the duration of that session only. When an 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.



Support Portal

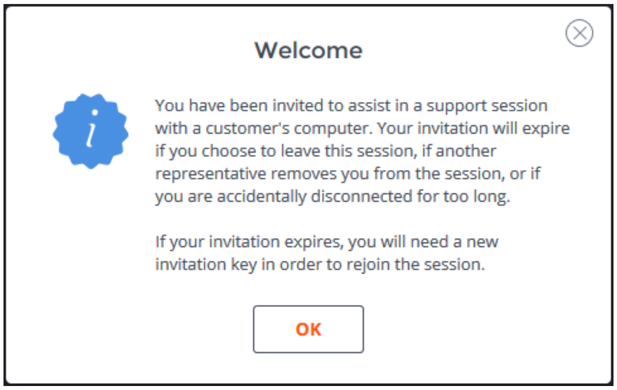
English (US)

You are about to start a support session with Sonia Blenkhorn.

1. **Click Keep** in the lower left corner of this window if you are prompted to Keep or Discard. If not, skip this step.
2. **Click** on the file you downloaded in the lower left corner of this window. If you don't see a downloaded file, click here.
3. **Click Run** if you are asked if you want to run this software.

You may close this window at any time after your session has started.

When an 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. Invited representatives can never be the session owner. If the inviting representative leaves the session without another session owner, any external representatives are logged out.



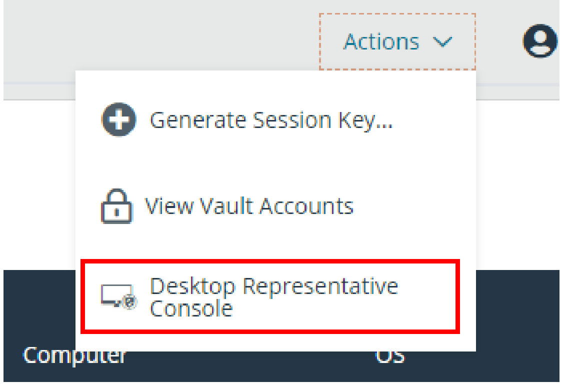
Welcome

You have been invited to assist in a support session with a customer's computer. Your invitation will expire if you choose to leave this session, if another representative removes you from the session, or if you are accidentally disconnected for too long.

If your invitation expires, you will need a new invitation key in order to rejoin the session.

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.

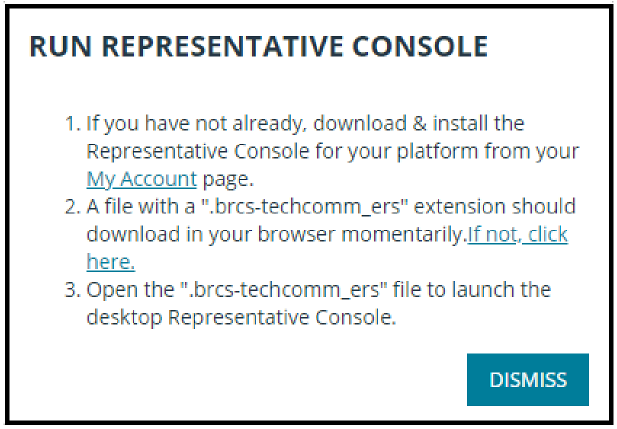


Note: Representatives using Chrome OS devices cannot download and use the desktop rep console.

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.

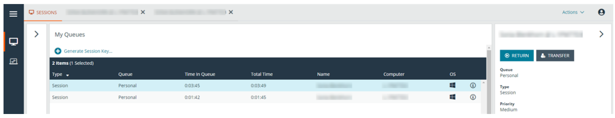
*Note: On a Linux system, you must save the file to your computer and then open it from its download location. Do not use the **Open** link that appears after downloading a file from some browsers.*


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.

View Support Sessions in Queue in the Web Rep Console

Queues



2 Items (1 Selected)

Type	Queue	Time In Queue	Total Time	Name	Computer	OS
Session	Personal	0:03:45	0:03:49	[redacted]	[redacted]	⊞
Session	Personal	0:01:42	0:01:45	[redacted]	[redacted]	⊞

Queue
Personal
Type
Session
Priority
Medium

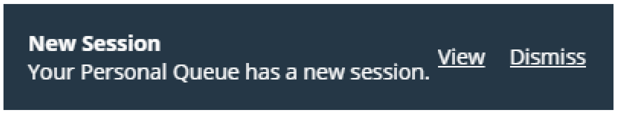
Session queues provide information about and access to customers who are waiting for support. The **Personal** queue contains customers with whom you are currently in session or who are waiting for a session with you specifically. A waiting session appears in your personal queue if it was transferred 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.

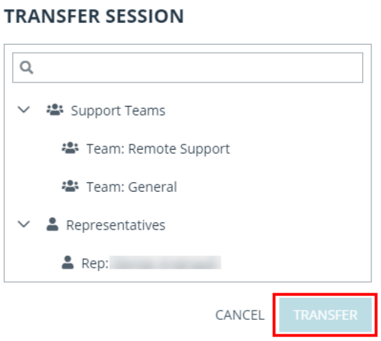
Customers can also request assistance directly from a web page which contains a help link. This initiates a browser sharing session, which allows a representative to chat and view the customer's web page. Administrators can generate custom links in order to direct browser sessions to the correct representative 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.


New Session
Your Personal Queue has a new session.

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.



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.

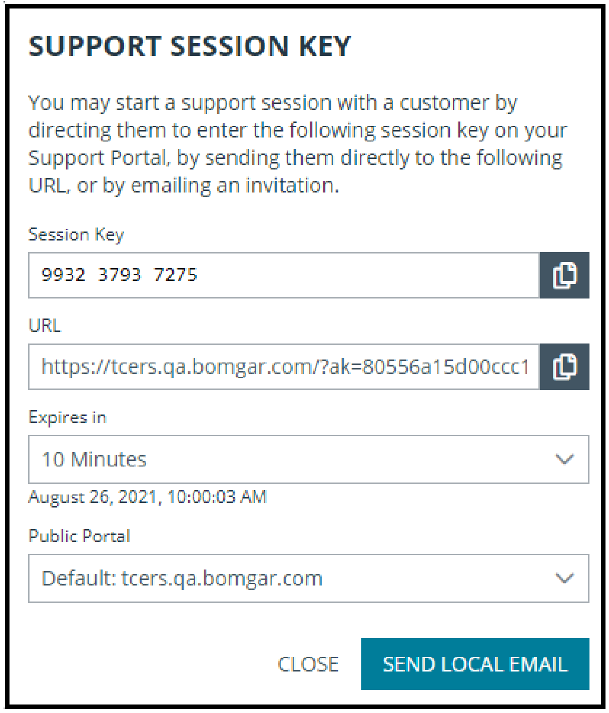
Set how long you want this session key to remain valid. The expiration time applies only to the length of time the key can be used to start a session and does not affect the length of the session itself.

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

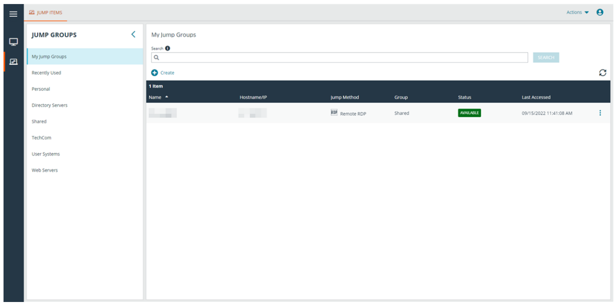
Public Portal: Default: tcers.qa.bomgar.com

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 representative console. Some types of Jump Items can be created in the web rep console. To create a Jump Item in the web rep console, click **Create** at the top of the Jump interface. Full details for creating different Jump Items are provided later in this guide.

> ***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.*



Name	Hostname/IP	Jump Method	Group	Status	Last Accessed
[redacted]	[redacted]	Remote RDP	Shared	AVAILABLE	09/15/2022 11:41:08 AM

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.

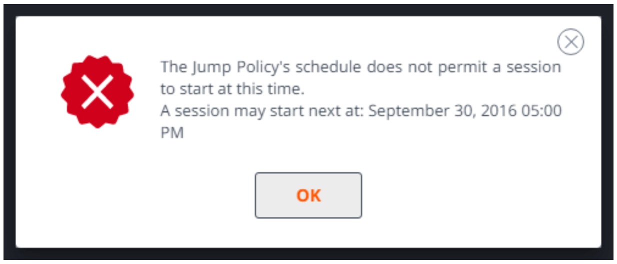
To view details about a Jump Item, or to copy or edit a Jump Item, click the vertical ellipsis at the right end of the of the Jump Item's row. To start a session with a Jump Item, click the **Jump** button at the right of the Jump Item entry.

> ***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.*

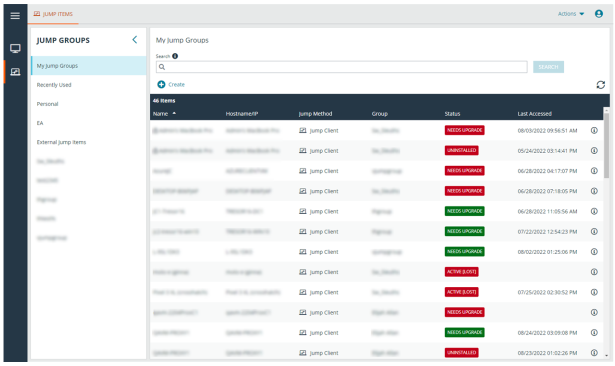
If a Jump Policy enforces a schedule for this Jump Item, an attempt to access the Jump Item outside of its permitted schedule prevents the Jump. A prompt informs you of the policy restrictions and provides the date and time when this Jump Item is next available for access.


The Jump Policy's schedule does not permit a session to start at this time.
A session may start next at: September 30, 2016 05:00 PM

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

Jump Client Upgrade

You can upgrade Jump Clients from within the web rep console. A **Needs Upgrade** banner displays under **Status**, in green if the Jump Client is online, red if offline. You can only upgrade Jump Clients that are online. To upgrade a given Jump Client, click the green banner.



[redacted]

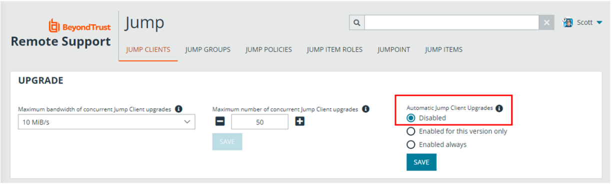
My Jump Groups

Search

46 Items

Name	Hostname/IP	Jump Method	Group	Status	Last Accessed
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	08/03/2022 09:56:51 AM
[redacted]	[redacted]	Jump Client	[redacted]	UNINSTALLED	05/24/2022 03:14:41 PM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	06/28/2022 04:17:07 PM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	06/28/2022 07:18:05 PM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	06/28/2022 11:05:56 AM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	07/22/2022 12:54:23 PM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	08/02/2022 01:25:06 PM
[redacted]	[redacted]	Jump Client	[redacted]	ACTIVE (LOST)	
[redacted]	[redacted]	Jump Client	[redacted]	ACTIVE (LOST)	07/25/2022 02:30:52 PM
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	
[redacted]	[redacted]	Jump Client	[redacted]	NEEDS UPGRADE	08/24/2022 03:09:08 PM
[redacted]	[redacted]	Jump Client	[redacted]	UNINSTALLED	08/23/2022 01:02:26 PM

In order to be able to upgrade a Jump Client from the Web Rep Console, you must make sure that **Automatic Jump Client Upgrades** is disabled in /login. To do so, go to **/login > Jump > Jump Clients > Upgrades** and disable **Automatic Jump Client Upgrades**. If automatic upgrading is not disabled, Jump Clients needing to upgrade display an **Upgrade Pending** banner instead.



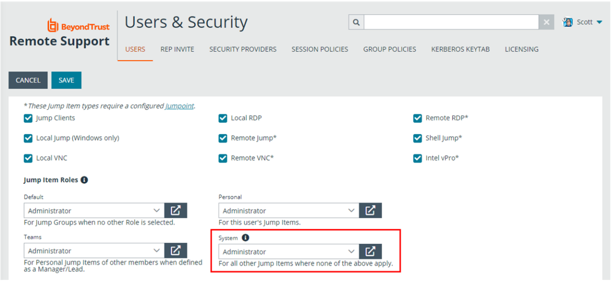
UPGRADE

Maximum bandwidth of concurrent Jump Client upgrades: 10 MiB/s

Maximum number of concurrent Jump Client upgrades: 50

Automatic Jump Client Upgrades
● Disabled
○ Enabled for this version only
○ Enabled always

The rep must also have the right to perform the update. This can be set in **/login > Users & Security > Users > Access Permissions > Jump Item Roles**. Make sure that **System** is also set to **Administrator**.



*These Jump Item types require a configured Jumpoint.

☑ Jump Clients ☑ Local RDP ☑ Remote RDP*
☑ Local Jump (Windows only) ☑ Remote Jump* ☑ Shell Jump*
☑ Local VNC ☑ Remote VNC* ☑ Intel vPro*

Jump Item Roles

Default: Administrator
For Jump Groups when no other Role is selected.

Personal: Administrator
For this user's Jump Items.

Teams: Administrator
For Personal Jump Items of other members when defined as a Manager/Lead.

System: Administrator
For all other Jump Items where none of the above apply.

Create and Use Remote Jump Shortcuts

Remote Jump enables a privileged user to connect to an unattended remote computer on a network outside of their own network. Remote Jump depends on a Jumpoint.

A Jumpoint acts as a conduit for access to computers on a known remote network. A single Jumpoint installed on a computer within a LAN is used to access multiple systems, eliminating the need to pre-install software on every computer you might need to access.

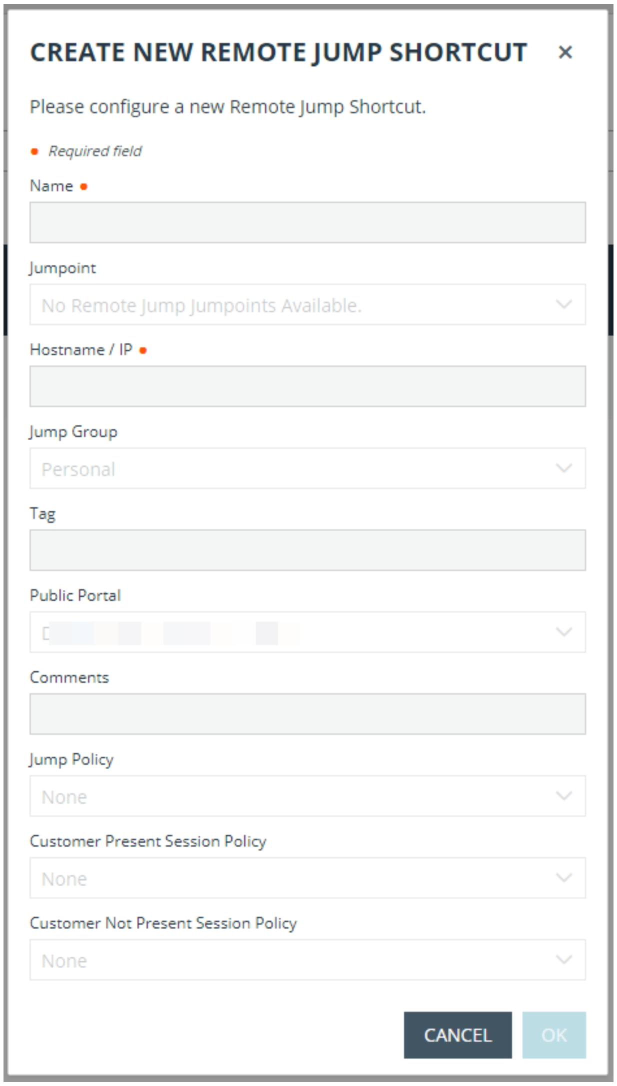
> ***Note:*** *Remote Jump and Local Jump are available only for Windows systems. Jump Clients are needed for remote access to Mac computers. To Jump to a Windows computer without a Jump Client, that computer must have Remote Registry Service enabled (disabled by default in Vista) and must be on a domain.*

Create a Remote Jump Shortcut

To create a Remote Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote Jump**. Remote Jump shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*



CREATE NEW REMOTE JUMP SHORTCUT ×

Please configure a new Remote Jump Shortcut.

● *Required field*

Name ●

Jumpoint: No Remote Jump Jumpoints Available.

Hostname / IP ●

Jump Group: Personal

Tag

Public Portal: [redacted]

Comments

Jump Policy: None

Customer Present Session Policy: None

Customer Not Present Session Policy: None

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

Further organize Jump Items by entering the name of a new or existing **Tag**. Even though the selected Jump Items are grouped together under the tag, they are still listed under the Jump Group in which each is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

Select the **Public Portal** through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

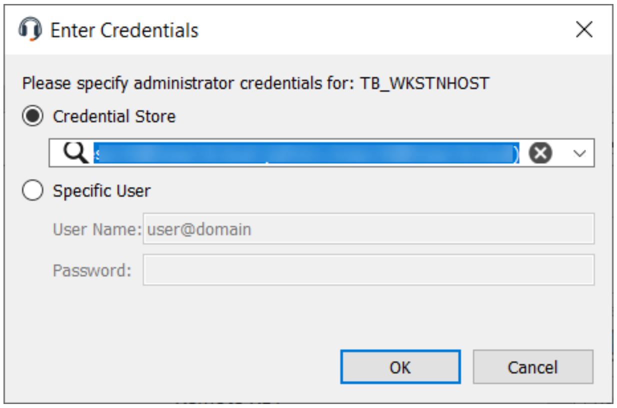
Choose session policies to assign to this Jump Item. Session policies assigned to this Jump Item have the highest priority when setting session permissions. The **Customer Present Session Policy** applies when the end user is determined to be present. Otherwise, the **Customer Not Present Session Policy** applies.

The way customer presence is determined is set by the **Use screen state to detect Customer Presence** Jump Item setting in the /login interface. When enabled, a customer is considered present only if a user is logged in, the system is not locked, and a screen saver is not running. When disabled, a customer is considered present if a user is logged in, regardless of the screen state. Customer presence is detected when the Jump Item session starts. The session policy used for the session does not change throughout the session, regardless of any changes in the customer's presence while the session is in progress. The ability to set a session policy depends on your account permissions.

Use a Jump Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

You must provide administrative credentials to the remote computer in order to complete the Jump. The administrative rights must be either a local administrator on the remote system or a domain administrator.



Enter Credentials

Please specify administrator credentials for: TB_WKSTNHOST

● Credential Store

[redacted]

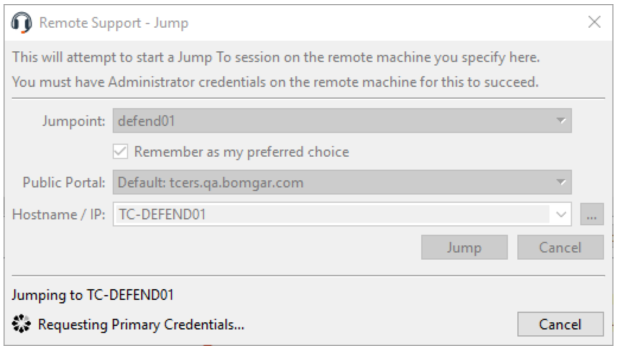
○ Specific User

User Name: user@domain

Password:

The client files are pushed to the remote system, and a session attempts to start. Depending on the session permissions, the end-user may be prompted to accept or deny the session. If no response is received within a defined interval of time, the session either starts or cancels, again depending on the session permissions.

> ***Note:** If you need to access systems through a Jumpoint when no user is available, make sure the public portal permissions and your account permissions are set either to disable prompting or to default to **Allow**.*



Remote Support - Jump

This will attempt to start a Jump To session on the remote machine you specify here.
You must have Administrator credentials on the remote machine for this to succeed.

Jumpoint: defend01

☑ Remember as my preferred choice

Public Portal: Default: tcers.qa.bomgar.com

Hostname / IP: TC-DEFEND01

Jumping to TC-DEFEND01

Requesting Primary Credentials...

> ***Note:** Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to **Join Existing Session**, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access. For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.*

Create and Use Remote RDP Shortcuts

Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a remote Windows or Linux System. Because RDP sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as your administrator has defined for your site.

To use Remote RDP through BeyondTrust, you must have access to a Jumpoint and must have the user account permissions **Allowed Jump Methods: Remote RDP**.

Create a Remote RDP Shortcut

To create a Remote Microsoft RDP shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote RDP**. RDP shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

> ***Note:*** *By default, the RDP server listens on port 3389, which is therefore the default port BeyondTrust attempts. If the remote RDP server is configured to use a different port, add it after the hostname or IP address in the form of* ***<hostname>:<port>*** *or* ***<ipaddress>:<port>*** *(for example, 10.10.24.127:40000).*

Provide the **Username** to sign in as, along with the **Domain**.

Select the **Quality** at which to view the remote screen. This cannot be changed during the RDP session. 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.

To start a console session rather than a new session, check the **Console Session** box.

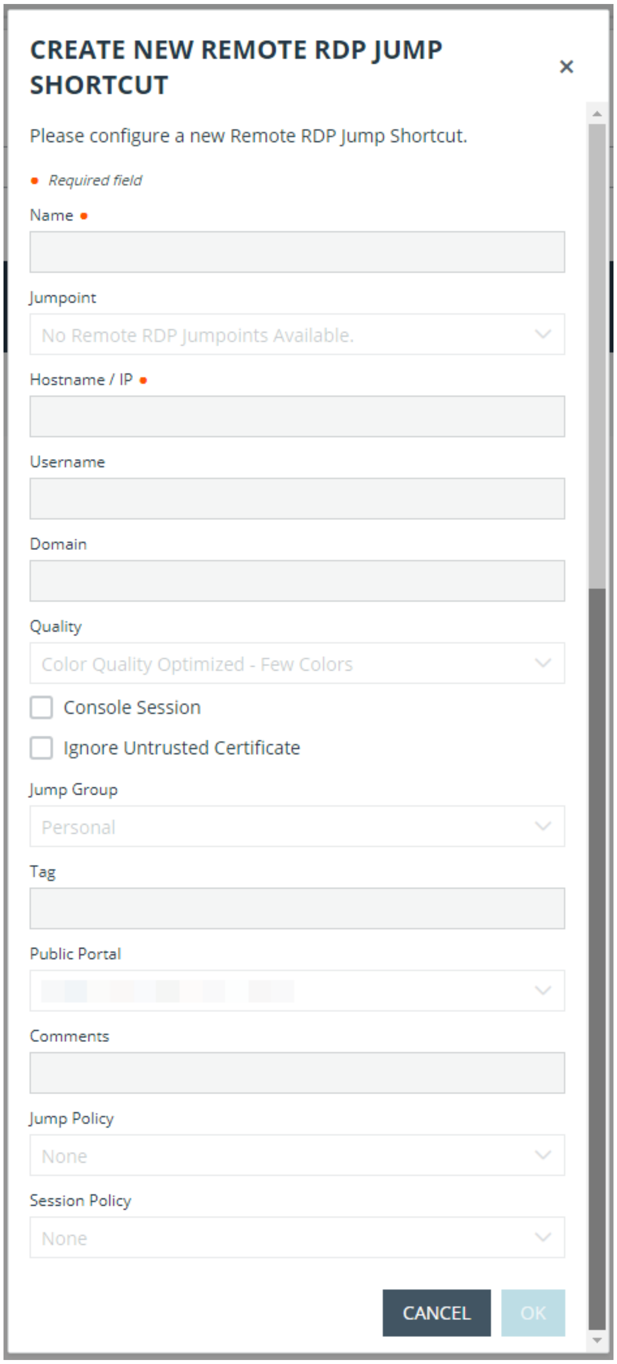
If the server's certificate cannot be verified, you receive a certificate warning. Checking **Ignore Untrusted Certificate** allows you to connect to the remote system without seeing this message.

Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

Further organize Jump Items by entering the name of a new or existing **Tag**. Even though the selected Jump Items are grouped together under the tag, they are still listed under the Jump Group in which each is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

Select the **Public Portal** through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.



CREATE NEW REMOTE RDP JUMP SHORTCUT

Please configure a new Remote RDP Jump Shortcut.

● *Required field*

Name ●

Jumpoint: No Remote RDP Jumpoints Available.

Hostname / IP ●

Username

Domain

Quality: Color Quality Optimized - Few Colors

□ Console Session

□ Ignore Untrusted Certificate

Jump Group: Personal

Tag

Public Portal: [redacted]

Comments

Jump Policy: None

Session Policy: None

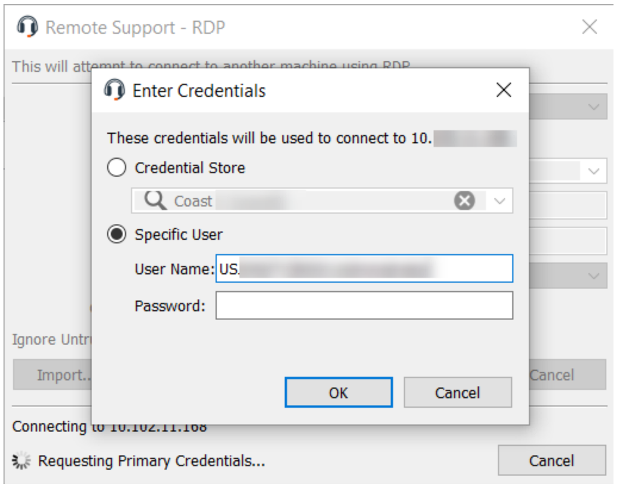
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

Use an RDP Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

You are prompted to enter the password for the username you specified earlier.



Remote Support - RDP

This will attempt to connect to another machine using RDP.

Enter Credentials

These credentials will be used to connect to 10.[redacted]

○ Credential Store

Coast [redacted]

● Specific User

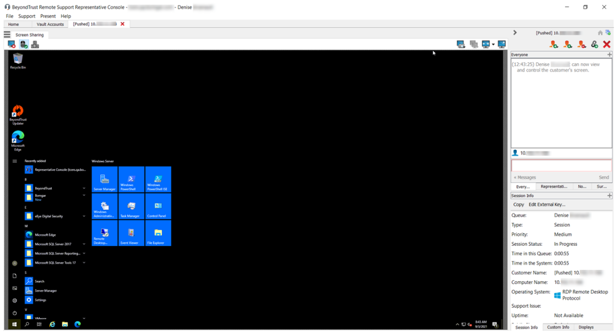
User Name: US[redacted]

Password:

Connecting to 10.102.11.168

Requesting Primary Credentials...

Your RDP session now begins. Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, and share clipboard contents. You can also share or transfer the RDP session with other logged-in BeyondTrust users, following the normal rules of your user account settings.



Multi-Monitor Support

An option allows you to open a Remote Support connection expanded across all the monitors on the client computer regardless of the client monitor configuration. With this feature, you can fully utilize all the monitors connected to the client computer, therefore being able to adjust screen sizing and scaling during an RDP session across multiple monitors.

> ***Note:*** *If you are using full screen view while using this feature, the remote system is displayed across all of your monitors.*

> ***Note:*** *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to **Start New Session**, then a new independent session starts for each user who Jumps to a specific RDP Jump Item. The RDP configuration on the endpoint controls any further behavior regarding simultaneous RDP connections.*

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Create and Use Remote VNC Shortcuts

Use BeyondTrust to start a VNC session with a remote system. Because VNC sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as defined by your administrator for your site.

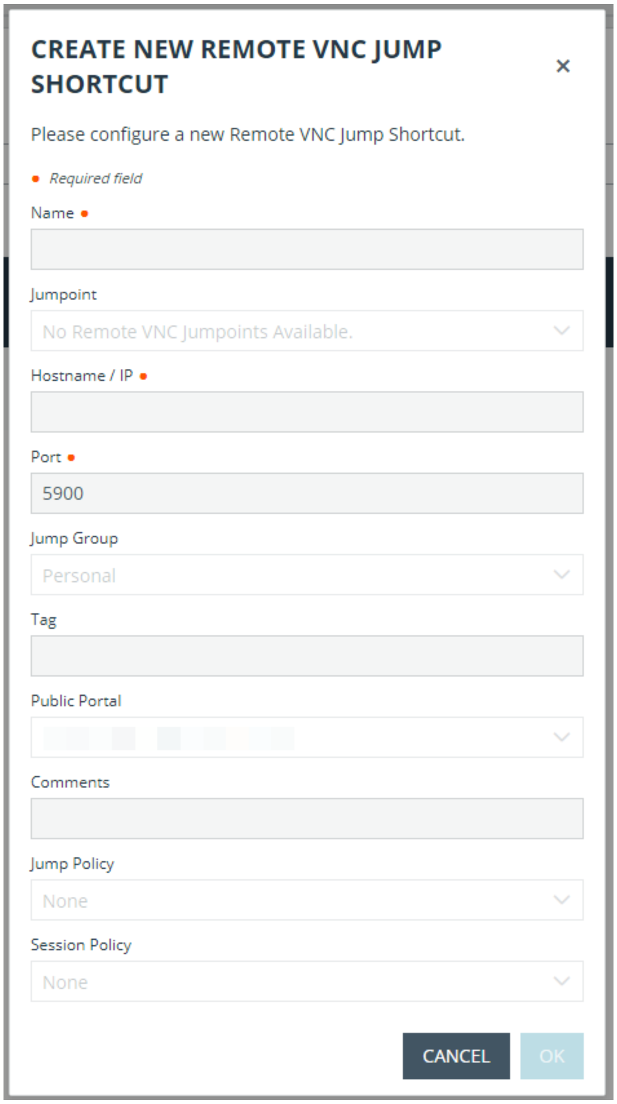
To use Remote VNC through BeyondTrust, you must have access to a Jumpoint and have the user account permission **Allowed Jump Methods: Remote VNC**.

Create a Remote VNC Shortcut

To create a Remote VNC shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote VNC**. VNC shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

***Note:** To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*



CREATE NEW REMOTE VNC JUMP SHORTCUT

Please configure a new Remote VNC Jump Shortcut.

● *Required field*

Name ●

Jumpoint: No Remote VNC Jumpoints Available.

Hostname / IP ●

Port ●: 5900

Jump Group: Personal

Tag

Public Portal: [redacted]

Comments

Jump Policy: None

Session Policy: None

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

By default, the VNC server listens on port 5900, which is, therefore, the default port BeyondTrust attempts. If the remote VNC server is configured to use a different port, enter it in the **Port** field.

Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

Further organize Jump Items by entering the name of a new or existing **Tag**. Even though the selected Jump Items are grouped together under the tag, they are still listed under the Jump Group in which each is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

Select the **Public Portal** through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

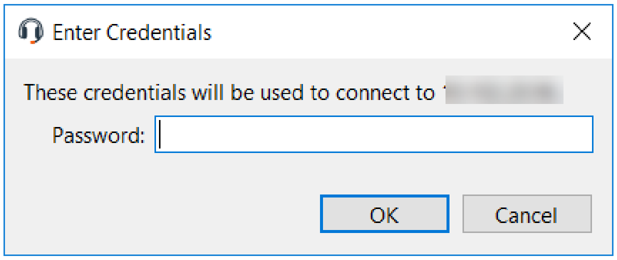
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

Use a VNC Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

When establishing the connection to the VNC server, the system prompts you to enter the user name and password.

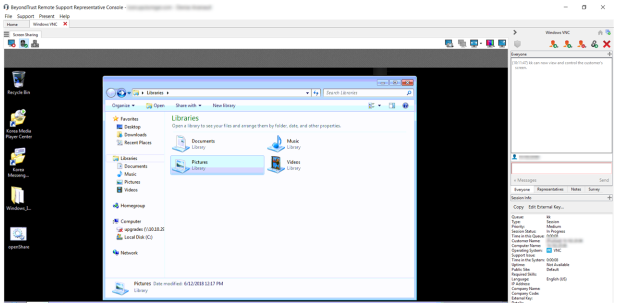


Enter Credentials

These credentials will be used to connect to [redacted]

Password:

Your VNC session now begins. Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, and share clipboard text contents. You also can share, transfer, or record the VNC session, following the normal rules of your user account settings.



(10:11:47) kk can now view and control the customer's screen.

Queue: kk
Type: Session
Priority: Medium
Session Status: In Progress
Time in this Queue: 0:00:08
Customer Name: [redacted]
Computer Name: [redacted]
Operating System: VNC
Support Issue:
Time in the System: 0:00:08
Uptime: Not Available
Public Site: Default
Required Skills:
Language: English (US)
IP Address:
Company Name:
Company Code:
External Key:

__Note:__ Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to __Join Existing Session__, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access.

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Create and Use Shell Jump Shortcuts

With Shell Jump, quickly connect to an SSH-enabled or Telnet-enabled network device to use the command line feature on that remote system. For example, run a standardized script across multiple systems to install a needed patch, or troubleshoot a network issue.

Create a Shell Jump Shortcut

To create a Shell Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Shell Jump**. Shell Jump shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

> ***Note:*** *Shell Jump shortcuts are enabled only if their Jumpoint is configured for open or limited Shell Jump access.*

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be all the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

Choose the **Protocol** to use, either **SSH** or **Telnet**.

Port automatically switches to the default port for the selected protocol but can be modified to fit your network settings.

Enter the **Username** to sign in as.

Select the **Terminal Type**, either **xterm** or **VT100**.

You can also select to **Send Keep-Alive Packets** to keep idle sessions from ending. Enter the number of seconds to wait between each packet send.

Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

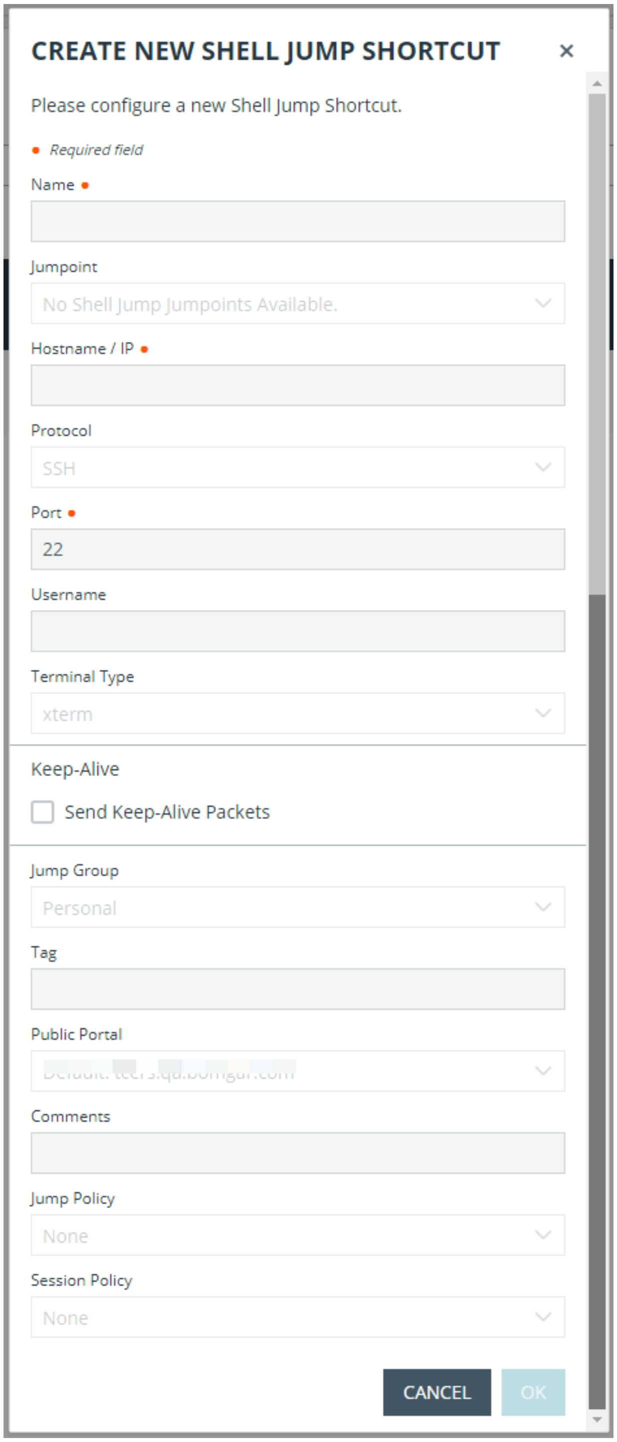
Further organize Jump Items by entering the name of a new or existing **Tag**. Even though the selected Jump Items are grouped together under the tag, they are still listed under the Jump Group in which each is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

Select the **Public Portal** through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.



CREATE NEW SHELL JUMP SHORTCUT

Please configure a new Shell Jump Shortcut.

● *Required field*

Name ●

Jumpoint: No Shell Jump Jumpoints Available.

Hostname / IP ●

Protocol: SSH

Port ●: 22

Username

Terminal Type: xterm

Keep-Alive

□ Send Keep-Alive Packets

Jump Group: Personal

Tag

Public Portal: [redacted]

Comments

Jump Policy: None

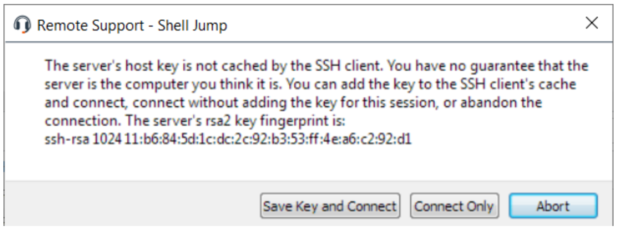
Session Policy: None

Use a Shell Jump Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

If attempting to Shell Jump to an SSH device without a cached host key, you receive an alert that the server's host key is not cached and that there is no guarantee that the server is the computer you think it is.

If you choose **Save Key and Connect**, then the key is cached on the Jumpoint's host system so that future attempts to Shell Jump to this system do not result in this prompt. **Connect Only** starts the session without caching the key, and **Abort** ends the Shell Jump session.



The server's host key is not cached by the SSH client. You have no guarantee that the server is the computer you think it is. You can add the key to the SSH client's cache and connect, connect without adding the key for this session, or abandon the connection. The server's rsa2 key fingerprint is:
ssh-rsa 1024 11:b6:84:5d:1c:dc:2c:92:b3:53:ff:4e:a6:c2:92:d1

If you Shell Jump to an SSH device with keyboard interactive MFA enabled, there is a secondary prompt for input.

When you Shell Jump to a remote device, a command shell session immediately starts with that device. If you Shell Jump to a provisioned SSH device with an unencrypted key or with an encrypted key whose password has been cached, you are not prompted for a password. Otherwise, you are required to enter a password. You can then send commands to the remote system.

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.

> ***Note:*** *This feature is not supported for ARM-based Windows systems.*

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

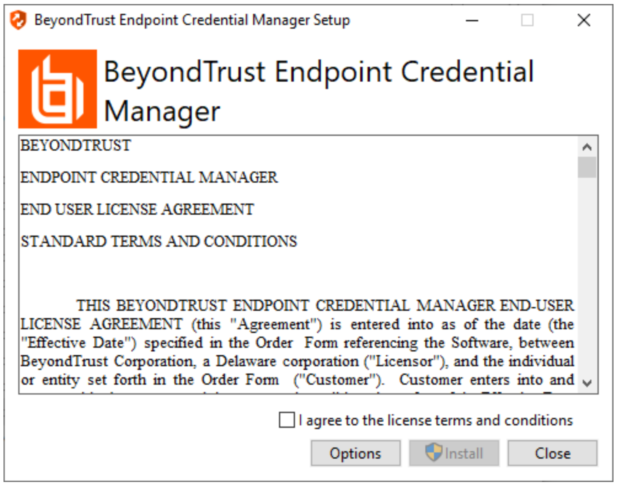
- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from BeyondTrust Supportat 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**.


BeyondTrust Endpoint Credential Manager Setup
BeyondTrust Endpoint Credential Manager
Options
Install
Close

BEYONDTRUST

ENDPOINT CREDENTIAL MANAGER

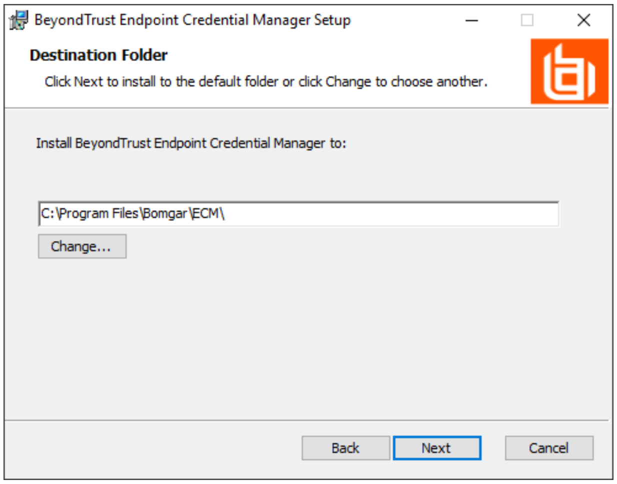
END USER LICENSE AGREEMENT

STANDARD TERMS AND CONDITIONS

THIS BEYONDTRUST ENDPOINT CREDENTIAL MANAGER END-USER LICENSE AGREEMENT (this "Agreement") is entered into as of the date (the "Effective Date") specified in the Order Form referencing the Software, between BeyondTrust Corporation, a Delaware corporation ("Licensor"), and the individual or entity set forth in the Order Form ("Customer"). Customer enters into and

□ I agree to the license terms and conditions

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.



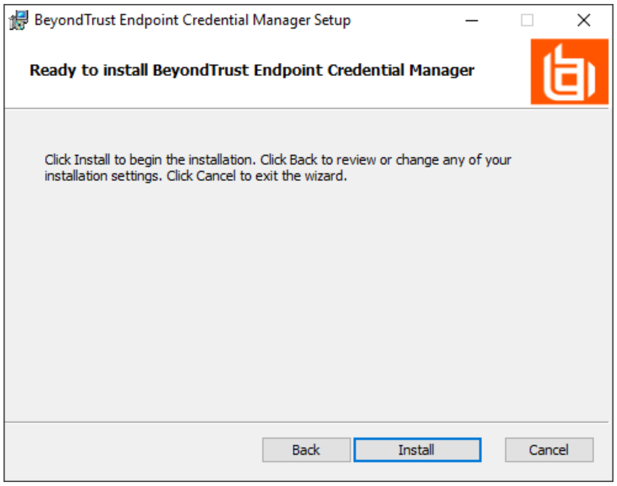
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install BeyondTrust Endpoint Credential Manager to:

C:\Program Files\Bomgar\ECM\

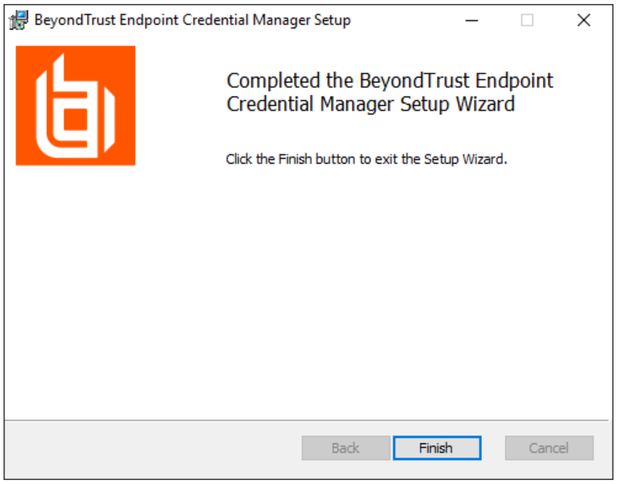
6. Click **Install** when you are ready to begin.



Ready to install BeyondTrust Endpoint Credential Manager

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

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



BeyondTrust Endpoint Credential Manager Setup

Completed the BeyondTrust Endpoint Credential Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

> ***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**.*

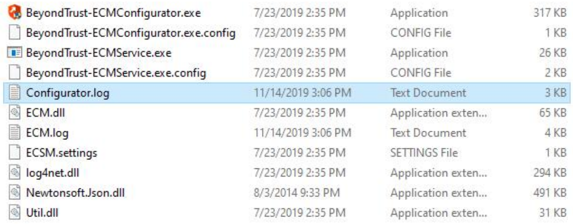
> ***Note:** When multiple ECMs are connected to a BeyondTrust site, the B Series Appliance routes requests to the ECM that has been connected to the B Series Appliance the longest.*

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

Configure a Connection to Your Credential Store

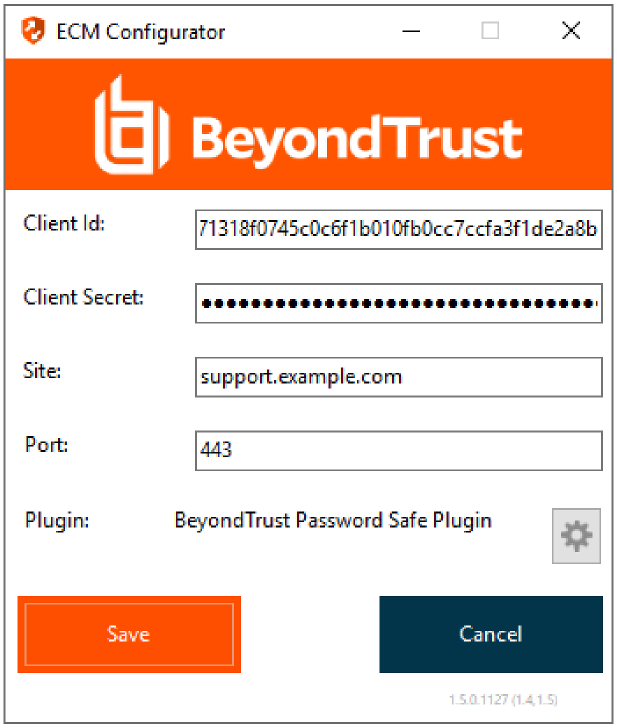
Using the ECM Configurator, set up a connection to your credential store.

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.



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
ECSM.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

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



ECM Configurator

Client Id: 71318f0745c0c6f1b010fb0cc7ccfa3f1de2a8b

Client Secret: ••••••••••••••••••••••••••••••••

Site: support.example.com

Port: 443

Plugin: BeyondTrust Password Safe Plugin

Enter the following values:

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

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

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

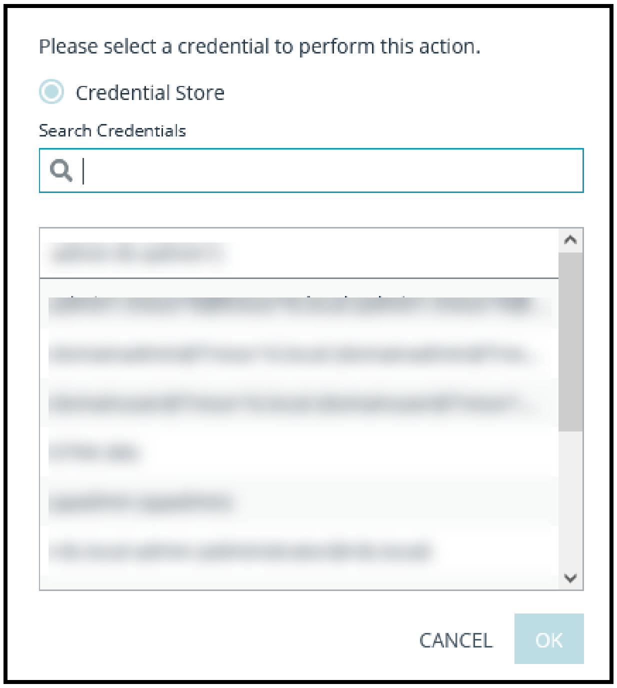
IMPORTANT!

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.



Please select a credential to perform this action.

○ Credential Store

Search Credentials

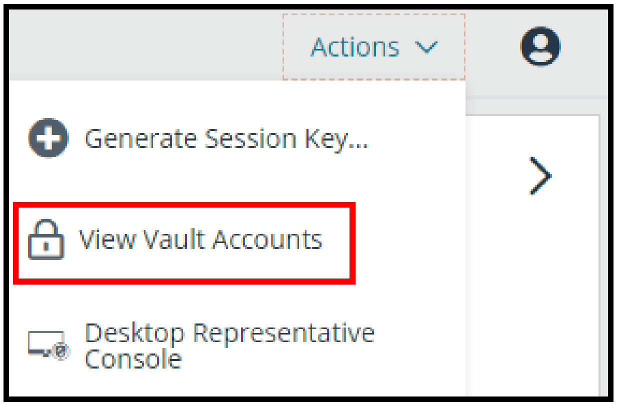
> ***Note:** When using BeyondTrust Vault, the maximum number of credentials that can display in the dropdown menu is 2,000. When using the ECM, the limit is 200.*

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.

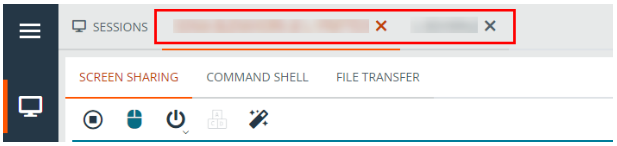
You can then locate and check out or check in a Vault account.



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.

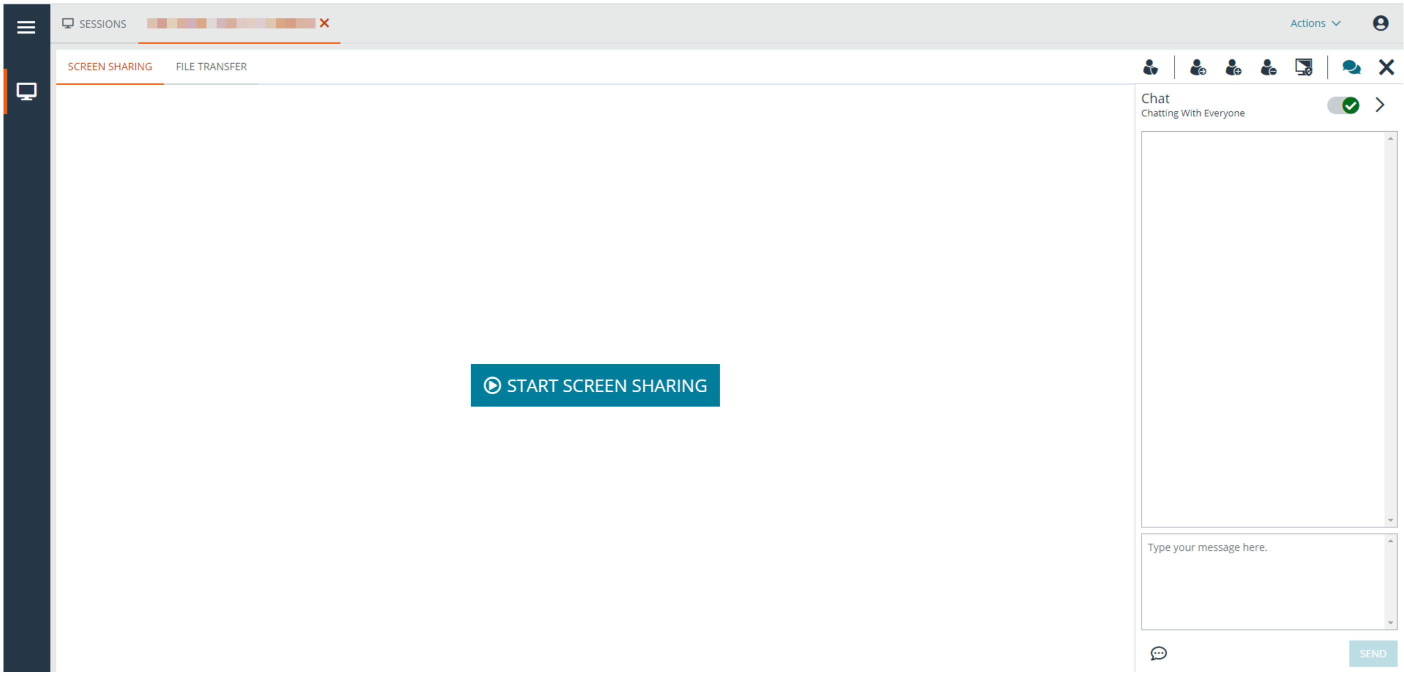


When a new session enters one of your queues, a popup alert appears in the lower- left corner of your screen. You can click **View** to see the session details in queue.

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.

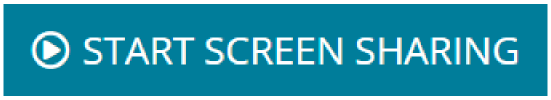
	Elevate a click-to-chat session to the full customer client, or elevate the customer client to have administrative rights by clicking the shield button. Select **Prompt Customer** to request admin credentials from the remote user. If you possess administrative credentials to the remote computer, select **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 at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm.

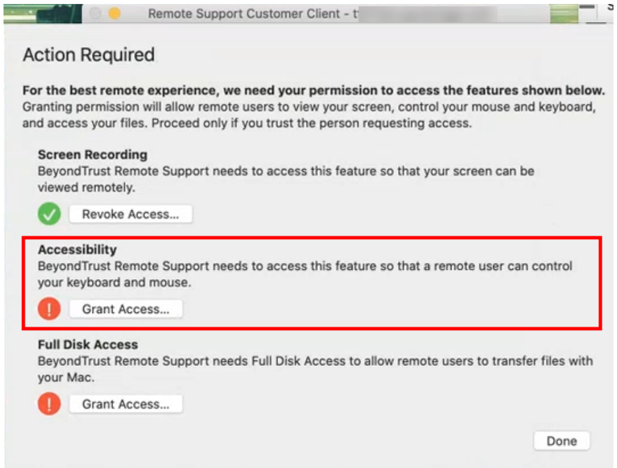
Control the Remote System with Screen Sharing in the Web Rep Console

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.*



Action Required

For the best remote experience, we need your permission to access the features shown below. Granting permission will allow remote users to view your screen, control your mouse and keyboard, and access your files. Proceed only if you trust the person requesting access.

Screen Recording
BeyondTrust Remote Support needs to access this feature so that your screen can be viewed remotely.

Accessibility
BeyondTrust Remote Support needs to access this feature so that a remote user can control your keyboard and mouse.

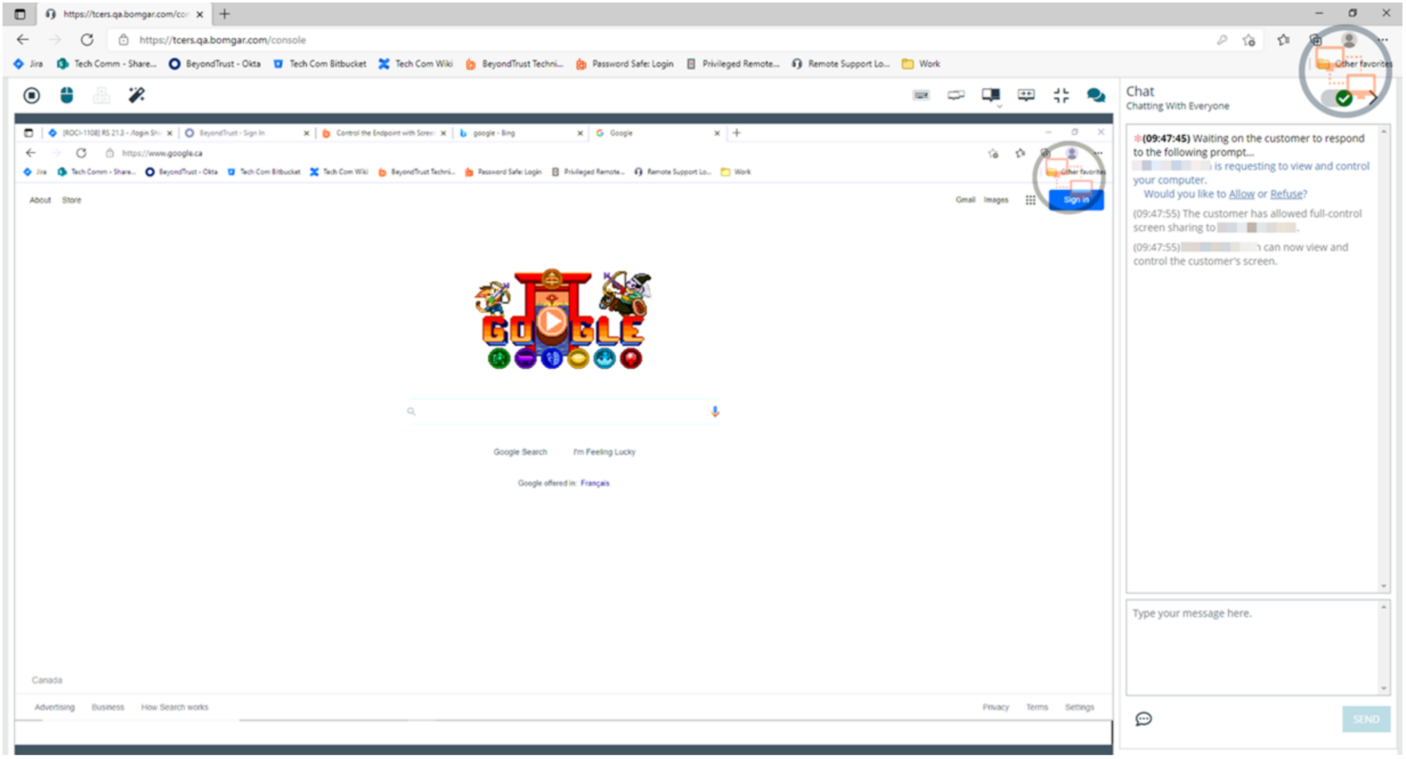
Full Disk Access
BeyondTrust Remote Support needs Full Disk Access to allow remote users to transfer files with your Mac.

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. Representatives using a macOS system can send **CTRL+Left-Click** through the connected screen sharing session to the remote system by using **CTRL+CMD+Left-Click**.
👤⚙	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**. Alternatively, disable the customer's mouse and keyboard input while still allowing them to view the screen. When input is restricted, an orange border appears around the customer's monitors, and a message indicates that the representative has mouse and keyboard control. 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.
A C D	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.
📷	Take a screenshot. You can save it to a file or to the clipboard.
🖥	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.



(09:47:45) Waiting on the customer to respond to the following prompt...
[redacted] is requesting to view and control your computer.
Would you like to Allow or Refuse?

(09:47:55) The customer has allowed full-control screen sharing to [redacted].

(09:47:55) [redacted] can now view and control the customer's screen.

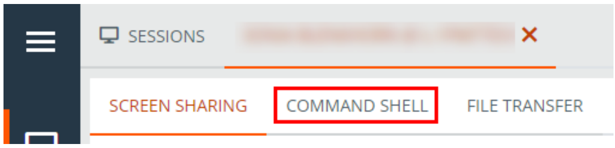
Access the Command Shell on the Remote System through the Web Rep Console

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.

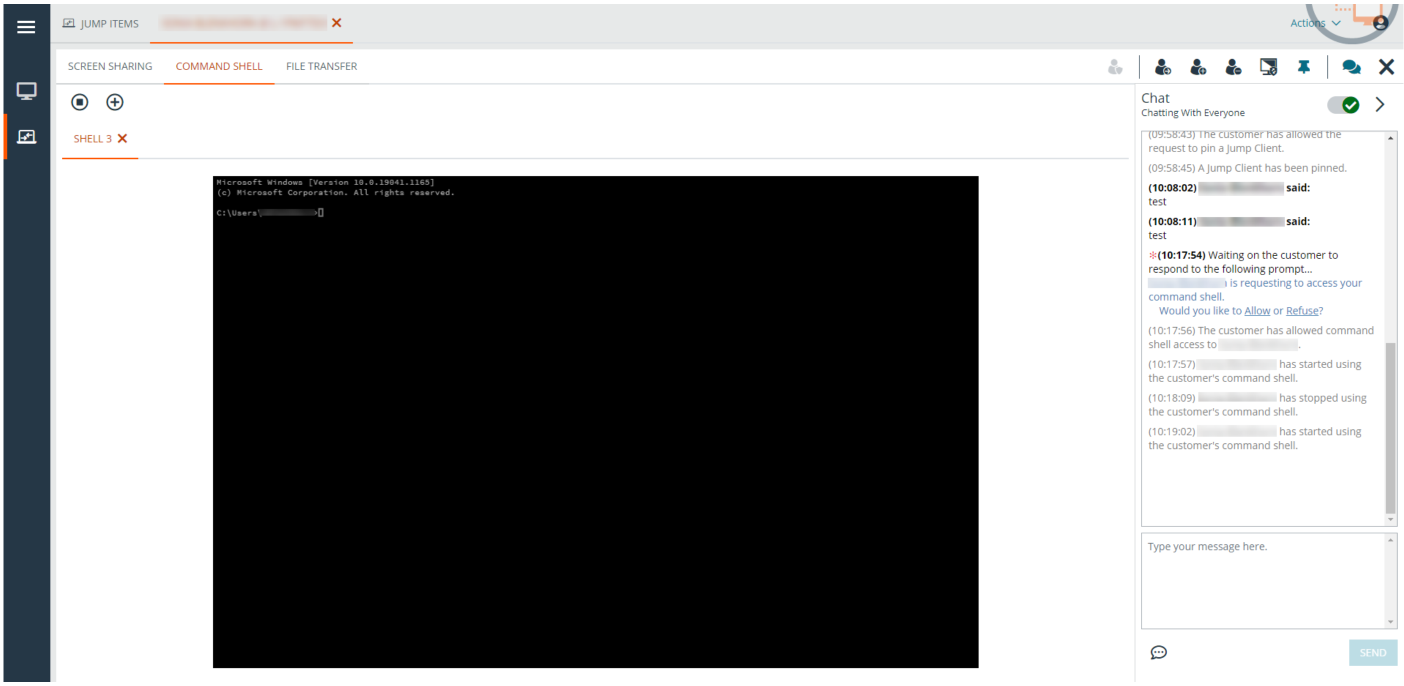
To access the command shell while in an support session, click on **Command Shell** at the top of the screen.

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.



```
Microsoft Windows [Version 10.0.19041.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>
```

(09:58:43) The customer has allowed the request to pin a Jump Client.

(09:58:45) A Jump Client has been pinned.

(10:08:02) [redacted] **said:**
test

(10:08:11) [redacted] **said:**
test

✻**(10:17:54)** Waiting on the customer to respond to the following prompt...
[redacted] is requesting to access your command shell.
Would you like to Allow or Refuse?

(10:17:56) The customer has allowed command shell access to [redacted].

(10:17:57) [redacted] has started using the customer's command shell.

(10:18:09) [redacted] has stopped using the customer's command shell.

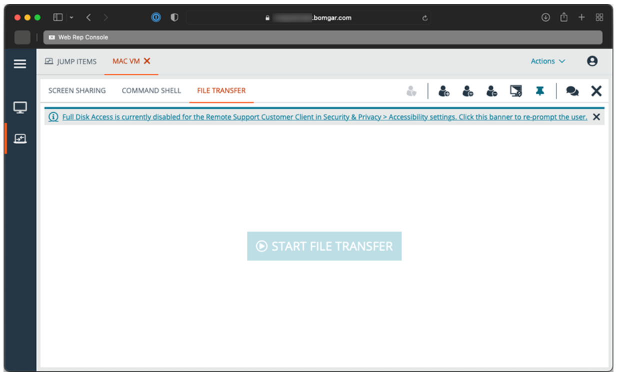
(10:19:02) [redacted] has started using the customer's command shell.

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

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

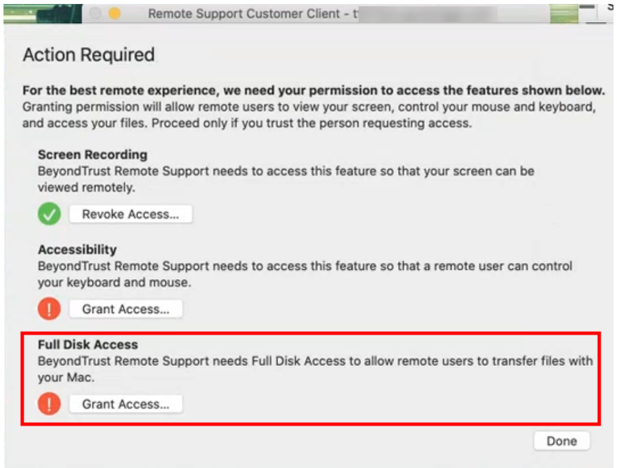
Depending upon the permissions your administrator has set for your account, you might be allowed only to upload files to the remote system or to download files to your local computer. File system access might also be restricted to certain paths on the remote or local system, thereby restricting uploads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



Full Disk Access is currently disabled for the Remote Support Customer Client in Security & Privacy > Accessibility settings. Click this banner to re-prompt the user.

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



Action Required

For the best remote experience, we need your permission to access the features shown below. Granting permission will allow remote users to view your screen, control your mouse and keyboard, and access your files. Proceed only if you trust the person requesting access.

Screen Recording
BeyondTrust Remote Support needs to access this feature so that your screen can be viewed remotely.

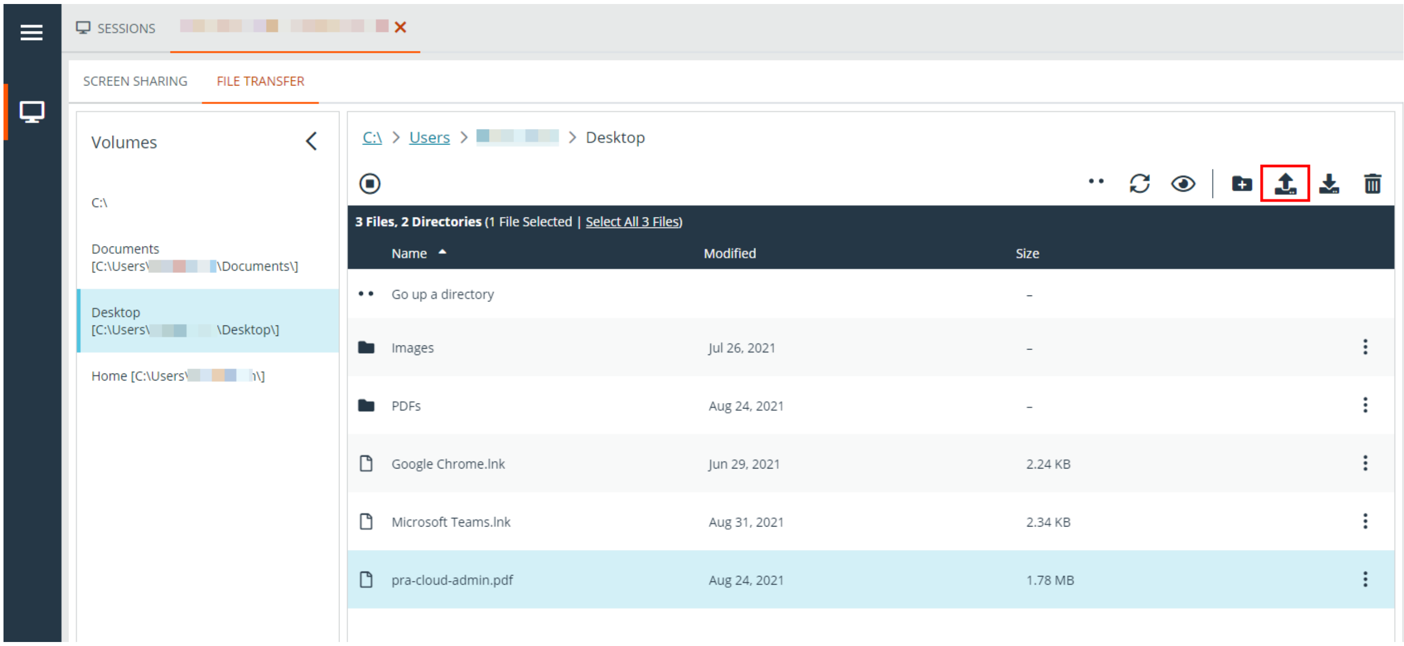
Accessibility
BeyondTrust Remote Support needs to access this feature so that a remote user can control your keyboard and mouse.

Full Disk Access
BeyondTrust Remote Support needs Full Disk Access to allow remote users to transfer files with your Mac.

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 the **More Options** icon.

To start transferring files to a system, click **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 a directory to open it.


SESSIONS [redacted]
SCREEN SHARING
FILE TRANSFER
Volumes
C:\
Documents [C:\Users\[redacted]\Documents\]
Desktop [C:\Users\[redacted]\Desktop\]
Home [C:\Users\[redacted]\]
C:\ > Users > [redacted] > 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.lnk	Jun 29, 2021	2.24 KB
Microsoft Teams.lnk	Aug 31, 2021	2.34 KB
pra-cloud-admin.pdf	Aug 24, 2021	1.78 MB

***Note:** If an ICAP server is enabled, any file transfers using FTP are scanned for malware. If malware is detected in the file, it is not transferred. Details regarding a failed file transfer might be displayed on the file transfer screen, and are available in session or team reports. To enable an ICAP server, please see Security at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/security.htm.*

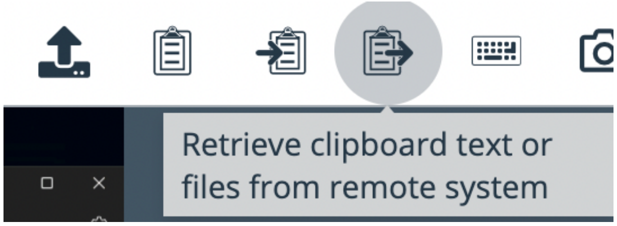
File Transfer Tools

⏹	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.
⌨	Toggle modifier keys.
📋	Send clipboard text to remote system.
📋	Retrieve clipboard text from remote system / retrieve clipboard text or files from remote system (RDP).
🗑	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.*

RDP File Transfer

Download Files

You can transfer files during RDP sessions by using **Ctr+C** to copy to the clipboard, right-click **Copy** from a context menu, or click a copy button in the Explorer toolbar. *These files are copied to the endpoint's clipboard*.

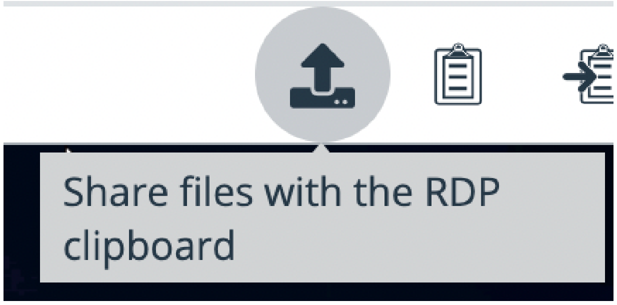

Retrieve clipboard text or files from remote system

Copying files or directories on the remote endpoint triggers a file download in your browser. The selected file downloads into the folder you have specified on your machine. Depending on your browser settings, you may be asked to specify a download location.

Upload Files

Uploading files in the web rep console is a two-step process:

1. Tell the browser which files you want to share with the remote clipboard.
2. Perform a paste on the remote endpoint.


Share files with the RDP clipboard

There are two ways to tell the browser which files to share:

1. Click a toolbar button that shows a standard system file picker, similar to uploading files in the file transfer tab.
2. Drag files into the screen sharing view.

After you select one of these methods, a toast message at the bottom of the page reminds you to paste on the remote endpoint.

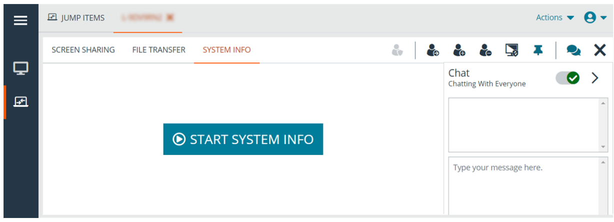
Once you paste on the endpoint, Windows shows the progress of the transfer in an endpoint dialog and provides a cancel button.

***Note:** If you select more than one file using the file picker or drag files before pasting the previous file selection on the endpoint, the first file selected is overwritten.*

View System Information on the Remote Endpoint

Remote Support users can view a complete snapshot of the remote device's or computer's system information to reduce the time needed to diagnose and resolve the issue. The system information available varies depending on the remote operating system and configuration.

1. From the session window, click the **System Info** tab at the top of the screen. You can click the **Start System Info** button if system information doesn't open automatically.
2. Use any of the following actions while in a session to perform different functions:



System Information Tools

↻	Refresh system info.
📋	Copy to clipboard.
⤓	Save to file.

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.

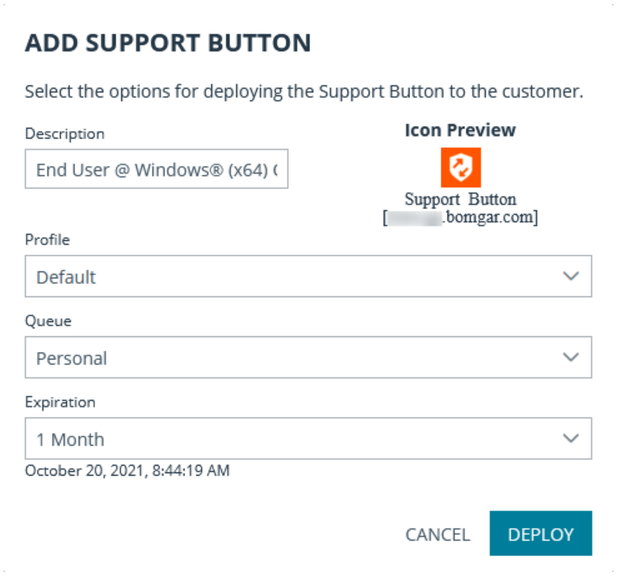
Enter a description to be seen by you and any other representatives who will have access to this Support Button.

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
[[redacted].bomgar.com]

Profile: Default

Queue: Personal

Expiration: 1 Month

October 20, 2021, 8:44:19 AM

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.

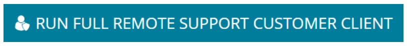
If you no longer need unattended access to the remote system, remove the Jump Client by clicking the **Unpin the Jump Client** button. When prompted to confirm that you want to uninstall the Jump Client, click **Yes**.

Elevate the Session in the Web Rep Console

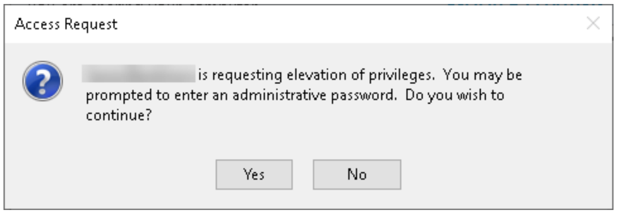
When a session starts in click-to-chat mode, only chat is available. If you wish to have access to more robust support features such as screen sharing, you must elevate the customer client.

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.

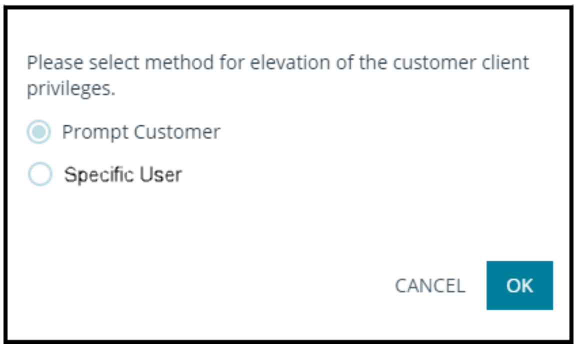


[redacted] is requesting elevation of privileges. You may be prompted to enter an administrative password. Do you wish to continue?

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**.


Please select method for elevation of the customer client privileges.

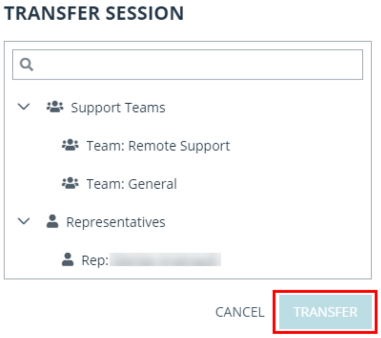
● Prompt Customer

○ Specific User

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.



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

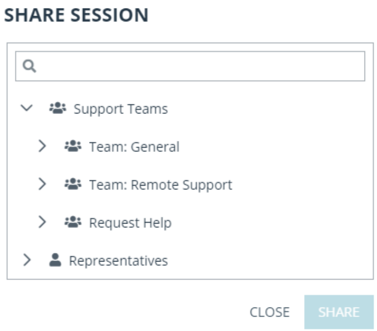
When someone accepts the session, you remain in the session as a participant but are no longer the session owner.

Share a Session with Team Members or External Users Using the Web Rep Console

Invite Team Members

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.



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.

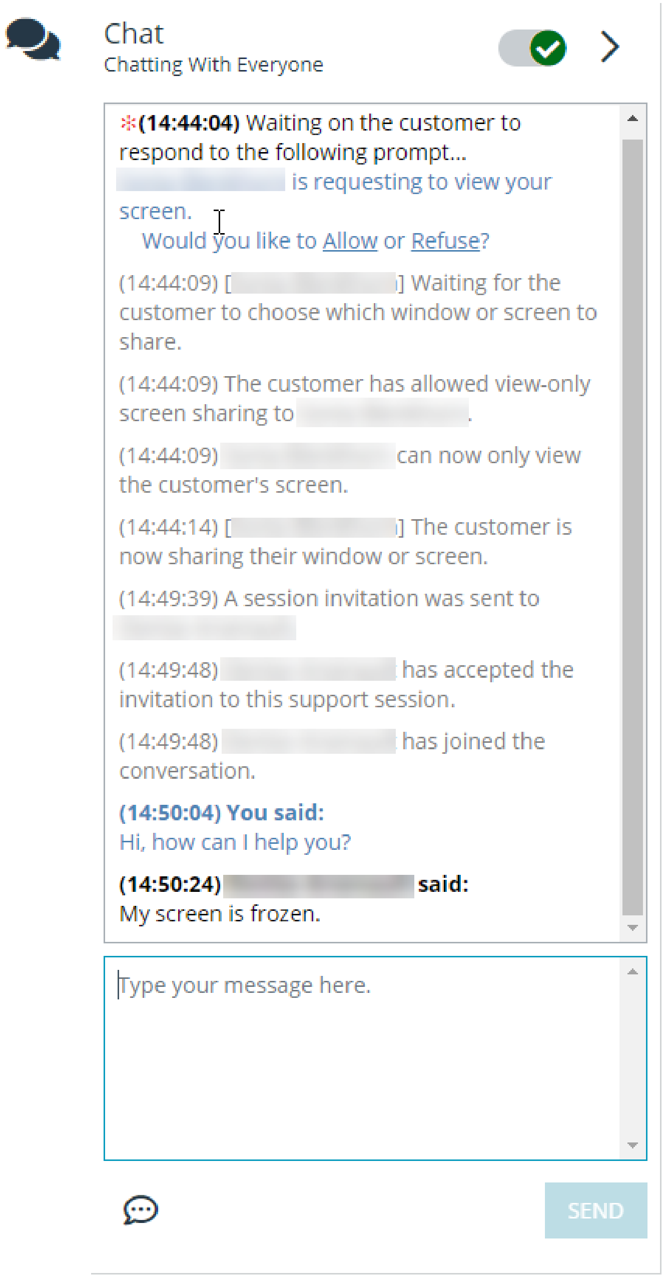
Once the rep has accepted the invitation and entered the session, you can chat with them by clicking on the **Chat** icon at the top of the screen.

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.



*(14:44:04) Waiting on the customer to respond to the following prompt...
[redacted] is requesting to view your screen.
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 [redacted]

(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?

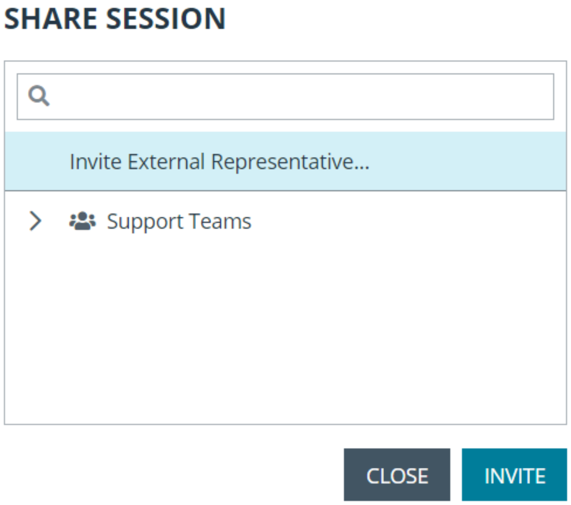
(14:50:24) [redacted] **said:**
My screen is frozen.

Type your message here.

Invite External Users

You can invite an external user or vendor to participate in an access session. To share a session, follow the steps outlined below:

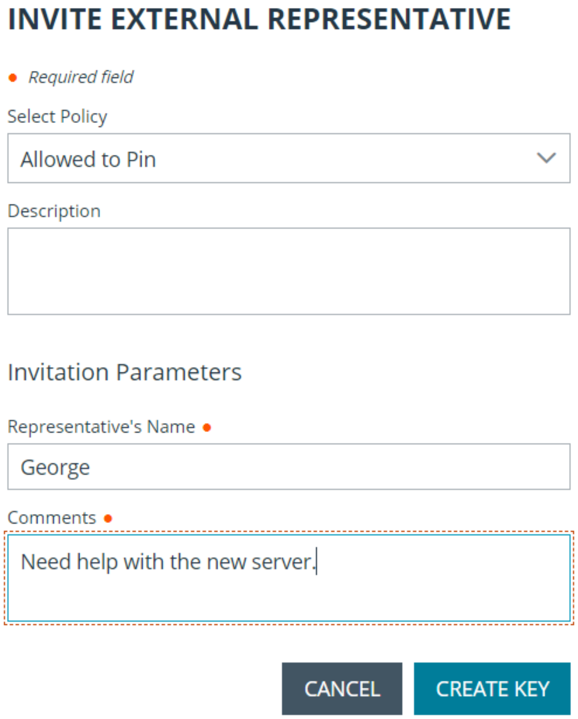
1. Click the **Invite other representatives into this session** icon.
2. Select **Invite External Representative...**.


SHARE SESSION

Invite External Representative...

Support Teams

3. Select a policy, if applicable, and enter a short description for the type of invitation.
4. In the **Invitation Parameters** area, enter the name of the person being invited, plus some comments to include with the invitation.
5. Click **Create Key**.


INVITE EXTERNAL REPRESENTATIVE

● *Required field*

Select Policy: Allowed to Pin

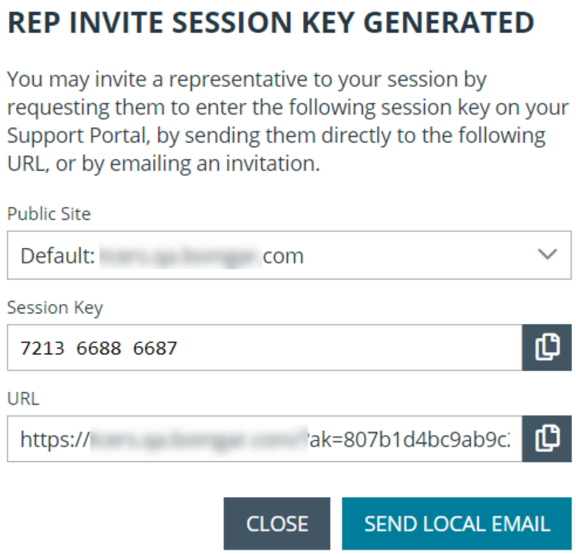
Description:

Invitation Parameters

Representative's Name ●: George

Comments ●: Need help with the new server.

You can now invite an external user by either clicking on the **Copy to Clipboard** icon and providing the user with the link to the session URL, or by sending an email invitation.



REP INVITE SESSION KEY GENERATED

You may invite a representative to your session by requesting them to enter the following session key on your Support Portal, by sending them directly to the following URL, or by emailing an invitation.

Public Site: Default: [redacted].com

Session Key: 7213 6688 6687

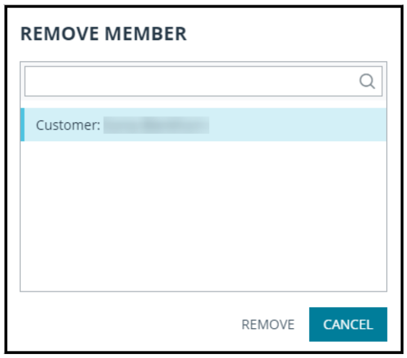
URL: https://[redacted]ak=807b1d4bc9ab9c

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

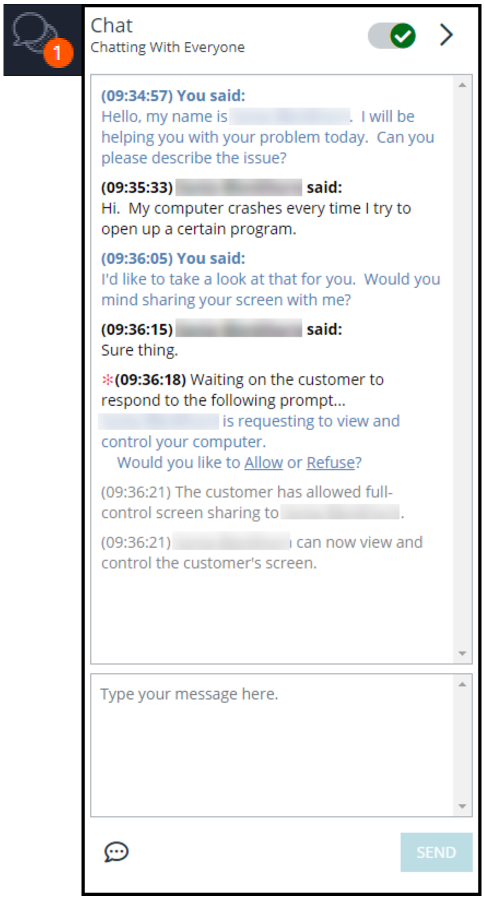
Customer: [redacted]

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.



Chat
Chatting With Everyone

(09:34:57) You said:
Hello, my name is [redacted]. I will be helping you with your problem today. Can you please describe the issue?

(09:35:33) [redacted] **said:**
Hi. My computer crashes every time I try to open up a certain program.

(09:36:05) You said:
I'd like to take a look at that for you. Would you mind sharing your screen with me?

(09:36:15) [redacted] **said:**
Sure thing.

✻**(09:36:18)** Waiting on the customer to respond to the following prompt...
[redacted] is requesting to view and control your computer.
Would you like to Allow or Refuse?

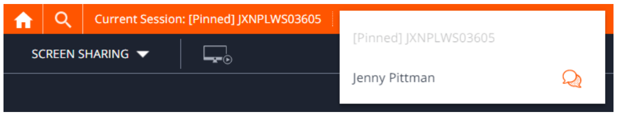
(09:36:21) The customer has allowed full-control screen sharing to [redacted].

(09:36:21) [redacted] can now view and control the customer's screen.

Type your message here.

SEND

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.

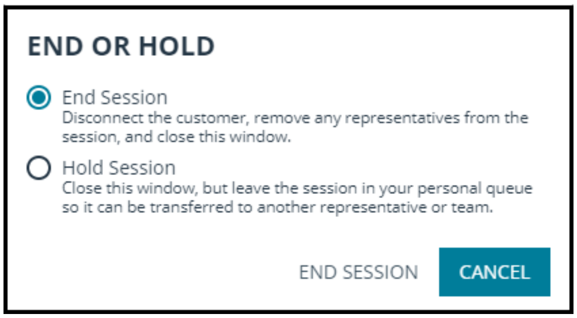


Close the Web Rep Console Session

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.

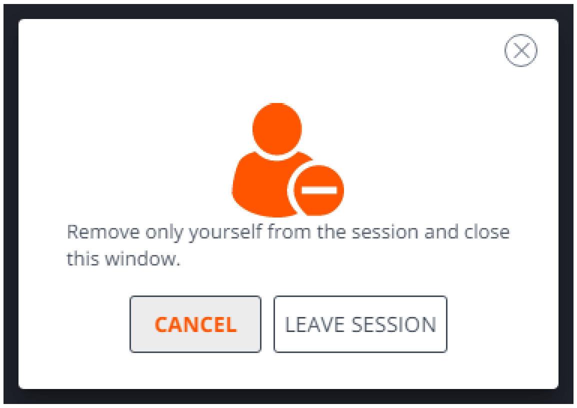
If you choose **Hold Session**, the session closes in your representative console but returns to wait in your personal queue. If any additional representatives are sharing the session, they remain in session.


END OR HOLD

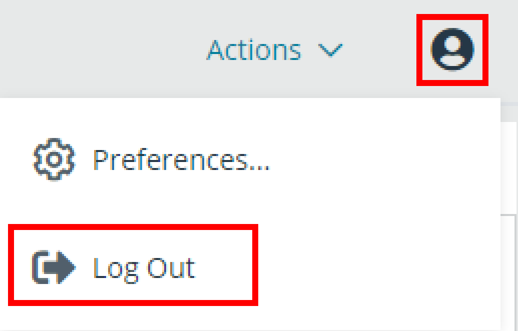
● End Session
Disconnect the customer, remove any representatives from the session, and close this window.

○ Hold Session
Close this window, but leave the session in your personal queue so it can be transferred to another representative or team.

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.


Remove only yourself from the session and close this window.

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.