BeyondTrust

Remote Support 19.2
Representative Guide

TC:12/19/2019

Table of Contents

BeyondTrust Representative Console

This guide is designed to help you install the BeyondTrust representative console onto your computer and understand the features of the solution. BeyondTrust enables you to support your customers remotely by connecting to them through the Secure Remote Access Appliance.

Install the Representative Console

In any web browser, go to the URL of your Secure Remote Access Appliance followed by **/login** and enter the username and password set by your administrator. You may be prompted to change your password the first time you log in.

From the **My Account** page, download and install the BeyondTrust representative console. The option will default to the appropriate installer for your operating system.

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

When the installation wizard appears, follow the instructions to install the software. After installing the representative console, you can choose **Run Representative Console Now** and **Run at Startup**, and then click **Finish**.

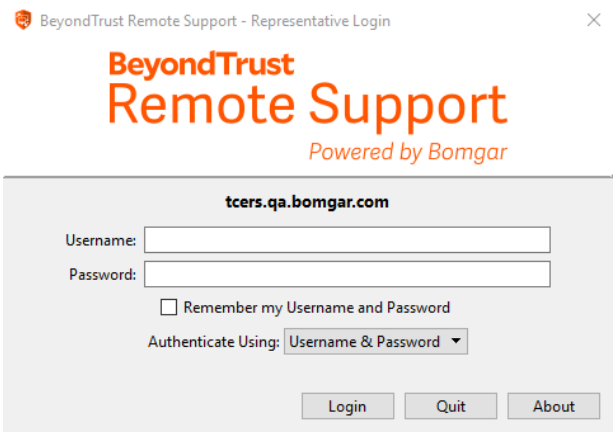
> ***Note:*** *If you choose* ***Run Representative Console Now*** *during installation, a login prompt will appear on your screen.*

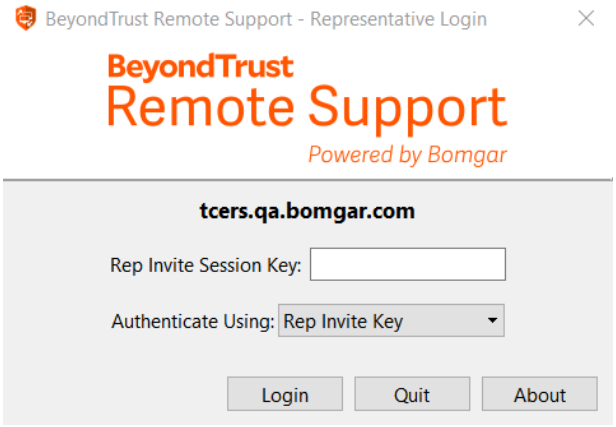
Log into the Representative Console

After installing the BeyondTrust representative console, launch the console from its directory location as defined during installation.

> ***Note:*** *By default, in Windows, you can access the console from* ***Start Menu > All Programs > BeyondTrust > support.example.com****, where* ***support.example.com*** *is the hostname of the site from which you downloaded the console.*

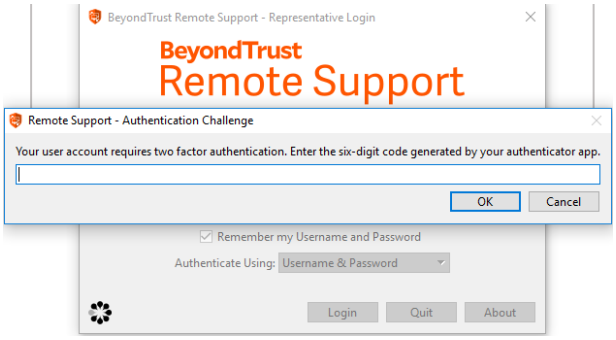
At the prompt, enter your username and password.

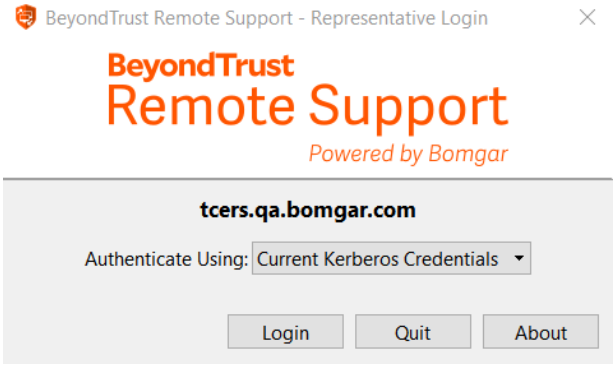




If two-factor authentication is enabled for your account, enter the code from the authenticator app.

> ***Note:*** *Users who were authenticating using email codes will be automatically upgraded to two-factor authentication (2FA), although they may continue to use email codes until they register an app. Once they begin to use 2FA, the email code option is permanently disabled.*





Alternatively, if your administrator has configured a Kerberos server to enable single sign-on, you can log into the console without entering your credentials. The representative console remembers the last used login mechanism, whether it used local credentials, Kerberos, or another security provider.

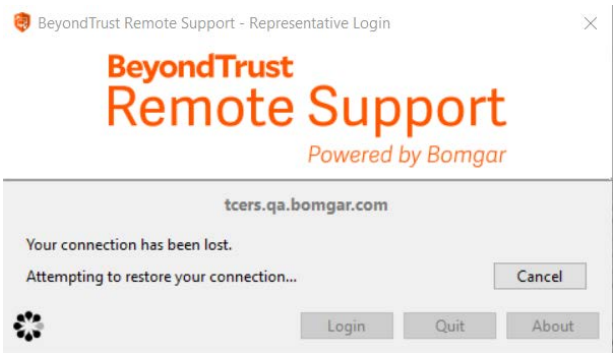
Invited users can also enter a session key to join a shared session on a one-time basis.

Check **Remember my login information** to have the console save your username and password. This option can be enabled or disabled from **/login > Management > Security**.

If you have multiple languages enabled for your site, select the language you wish to use from the dropdown beside the globe icon. If you wish to change the selected language after logging in, you must log back out to choose another language.

Once you log in, the console will open, and a BeyondTrust icon will appear in your computer's system tray. If you close the console but remain logged in, you can reopen the window by double-clicking the system tray icon or by right-clicking the icon and selecting **Show Window**.

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



If you lose your connection, the representative console attempts to reconnect for 60 seconds. If your connection is restored within this time, your representative console reopens, restoring all of your open sessions. If the connection cannot be restored within this time, your sessions fall back according to the rules set on **/login > Configuration > Options**, and you are prompted to retry login or quit.

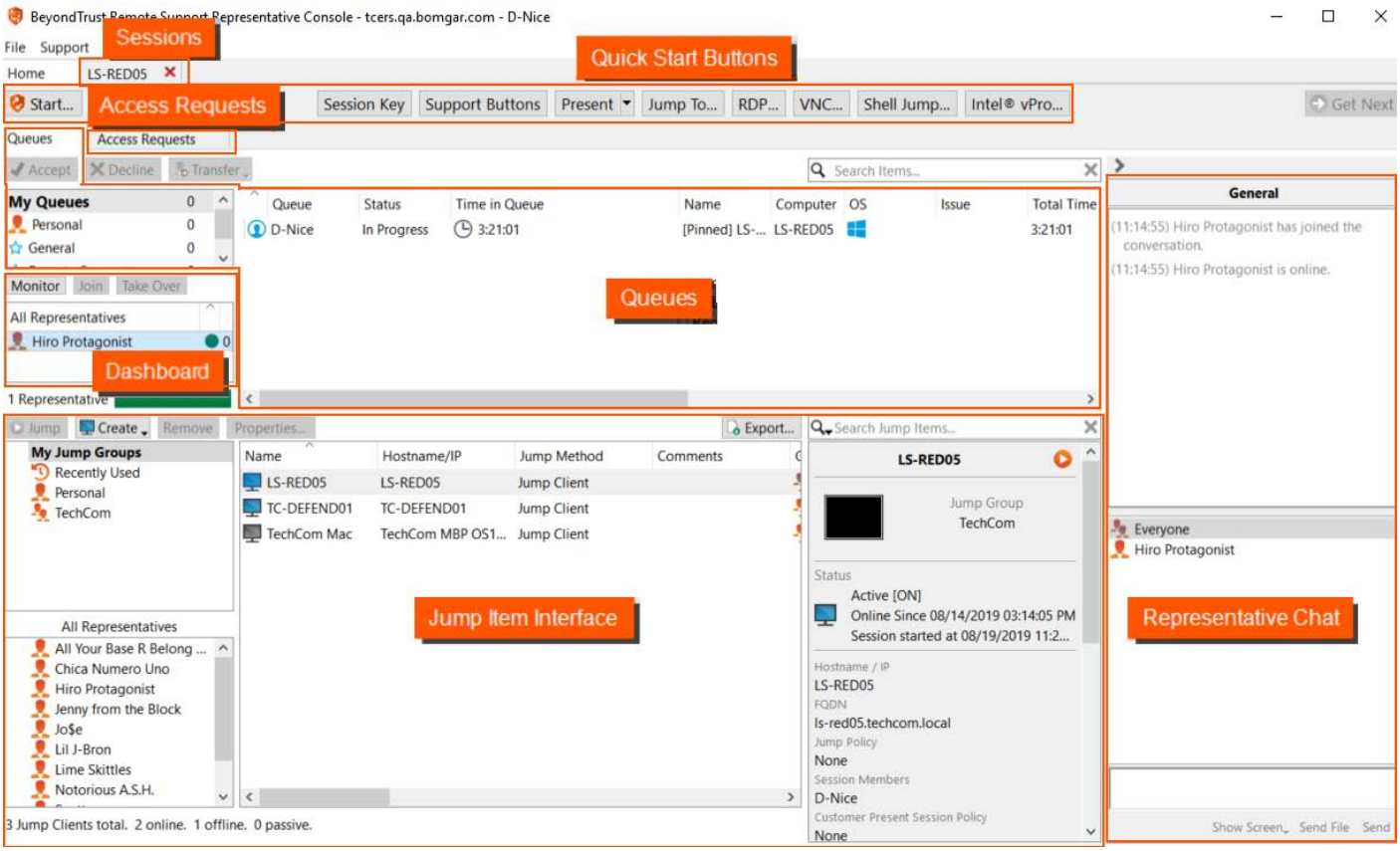
If you are logged into the representative console in one location and then log in from another, your open sessions are maintained.

Note: *To log in with an account already in use and forcibly close the connection on the other system, the setting* ***Terminate Session If Account Is In Use*** *must be checked on the* ***/login > Management > Security*** *page.*

After an upgrade or at first launch of the desktop representative console, a **What's New** dialog appears automatically upon login for all non-invited representatives. This dialog may be viewed at any time through **Help > What's New** and shows new release information for current and past releases. This is a roaming preference per account, so the dialog appears just once regardless where a representative signs in from.

For more information about invited users, please see Rep Invite: Create Profiles to Invite External Representatives to Sessions at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/rep-invite.htm.

Representative Console User Interface



Sessions: Manage multiple remote sessions at the same time.

> ***Note:*** *Session tabs can be moved and reordered to help you organize and prioritize your workload. Simply click and drag a session tab to a new position. Session tabs can also be detached from the main representative console window.*

Quick Start Buttons: Easily access frequently needed tools. Quick start buttons can be turned on or off from **File > Settings**.

- **Start**: Open a dialog for a quick-reference guide to starting a session.
- **Session Key**: Begin sessions with randomly generated, one-time use session keys.
- **Support Buttons**: View details and usage statistics of deployed Support Buttons.
- **Present**: Share your screen with one or more remote attendees. Start a presentation immediately or schedule a presentation for a later time.
- **Jump To**: Jump to a computer on a remote network via Jumpoint or on your local network. BeyondTrust's Jump Technology enables privileged representatives to connect to an unattended remote computer to start a session without end-user assistance.
- **RDP**: Start a Remote Desktop Protocol session with a remote Windows system.
- **VNC**: Start a VNC session with a remote Windows system.
- **Shell Jump**: Quickly connect to SSH-enabled and Telnet-enabled network devices through a deployed Jumpoint.

- **Intel® vPro**: Using Intel®Active Management Technology, support fully provisioned Intel®vPro Windows systems below the OS level.

Queues: Queues list customers who are waiting for support or who are in a session. Details about the remote system being supported appear in this section.

Dashboard: Privileged users can view and monitor ongoing sessions and teammates of a lower role, providing administrative oversight to help manage staff. Status indicators show whether representatives are available, are idle, are busy, or have auto-assign turned off. A bar at the bottom of the dashboard shows the percentage of representatives in each state.

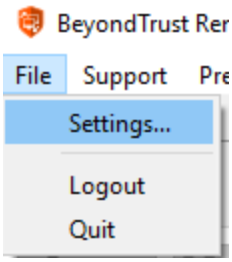
Access Requests: If a representative is a sponsor in one or more Access Sponsor groups, they see an Access Requests tab in the representative console. When a representative makes a request, all sponsors in the selected access sponsor group see a new request in the Access Requests tab of the representative console.

Jump Item Interface: Installed Jump Clients and Jump shortcuts appear here, grouped according to who can access them.

Representative Chat: Chat with other logged in users. You also can share your screen with a team member without requiring a session.

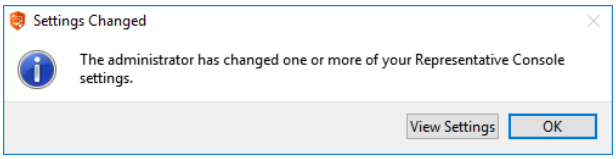
Change Settings and Preferences in the Representative Console

Click on **File > Settings** in the upper left-hand corner of the console to configure your preferences.



In general, you may configure the console settings according to your preferences. However, your BeyondTrust administrator may choose to manage your settings, possibly enforcing those managed settings.

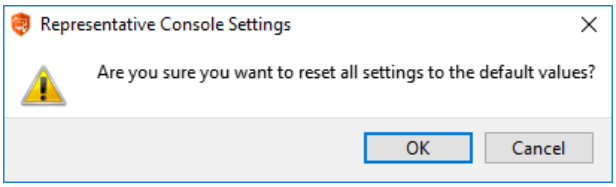
If your BeyondTrust administrator has changed and applied the default settings, then you will see a **Settings Changed** alert the next time you log into your console. Click **View Settings** to open your settings window to view the changes, or simply click **OK** to acknowledge the changes.



Changing Settings

> ***Note:*** *These instructions assume you are allowed to choose the settings used in your console. Settings enforced by your administrator appear marked with an asterisk and grayed out, and they are not locally configurable. See your administrator or the administrative guide representative console settings topic for more information.*

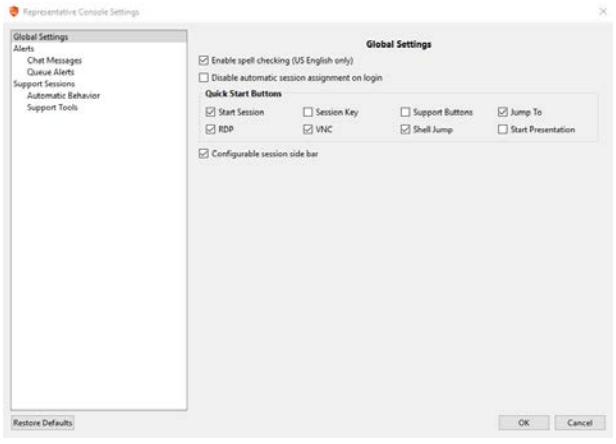
Each console settings window includes a **Restore Defaults** button in the lower left-hand corner of the window which will return all of your settings to the BeyondTrust default settings or to the default settings applied by your administrator if any have been set. An alert dialog asks you to confirm that you wish to change to the defaults. Click **Cancel** if you wish to return to your locally saved preferences. Note that if any of the defaults are forced by your administrator, you are unable to configure them.



From the **Global Settings** section, you may choose to enable or disable spell check for chat and session notes. Currently, spell check is available for US English only.

If automatic session assignment is disabled on login, then you will not be assigned sessions automatically until you choose to opt in.

If, under **Quick Start Buttons**, you select **Start Session**, you will see a **Start** button at the top of your representative console. Clicking this button walks you through the ways your customer can start a support session. You also can select **Session Key** to display a session key generation button, and select **Support Buttons** to display a button to launch the Support Button management interface. Select **Jump To**, **RDP**, **VNC**, **Shell Jump**, and **Intel® vPro** to display buttons to launch those respective Jump connections. **Start Presentation** allows you to easily start a new presentation.



Choose if you want the session menu icon to display, if the sidebar can be detached, and if the widgets on the session sidebar can be rearranged and resized.

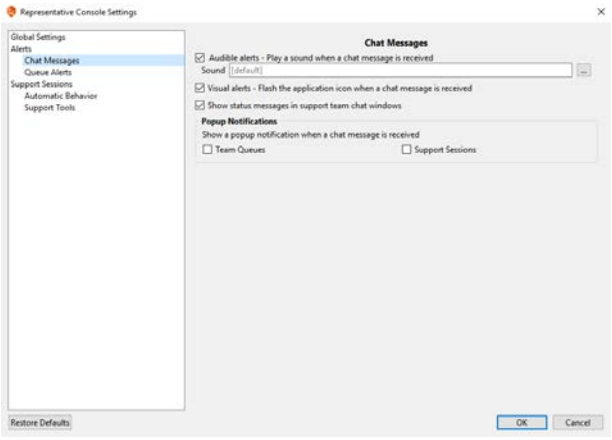
If real-time chat translation is enabled for your site, select your preferred chat language from the dropdown menu. This lets the rep console know what language you type in so that chat messages can be translated to the customer's selected language and vice-versa..

Choose your alert settings for chat messages. When you receive a chat message, you can choose to hear a sound and to see the application icon flash.

If you would like to upload a custom sound for chat messages, click the **[…]** button and select a WAV file on your computer. The file can be no larger than 1MB.

Choose if the team chat should include status messages, such as users logging in and out, or only chats sent between team members.

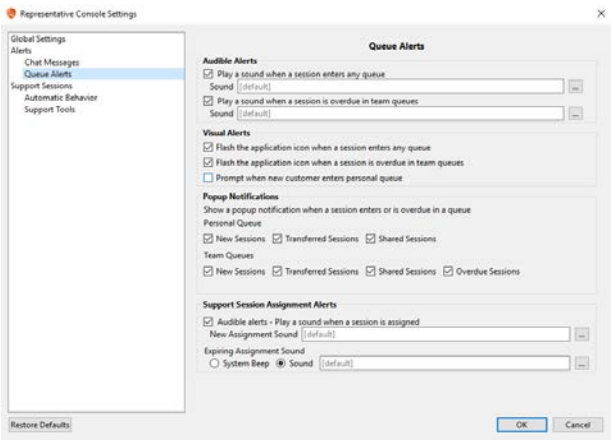
Choose if you want to receive pop-up notifications for messages received in a team chat and/or in a session chat.



Choose if you want to hear an audible alert when a customer enters one of your queues and/or when a waiting session has been marked as overdue. If you would like to upload a custom sound for either of these alerts, click the **[…]** button and select a WAV file on your computer. The file can be no larger than 1MB.

Also choose if you want to see the application icon flash when a customer enters one of your queues and/or when a waiting session has been marked as overdue. Additionally, when a customer enters your personal queue, such as by clicking on your name or entering a session key on the public site, the session can start immediately or prompt for your acceptance.

You also can choose to receive pop-up notifications for certain events. These notifications appear independent of your console and on top of other windows. Set where you wish to see pop-ups and how long they should display.



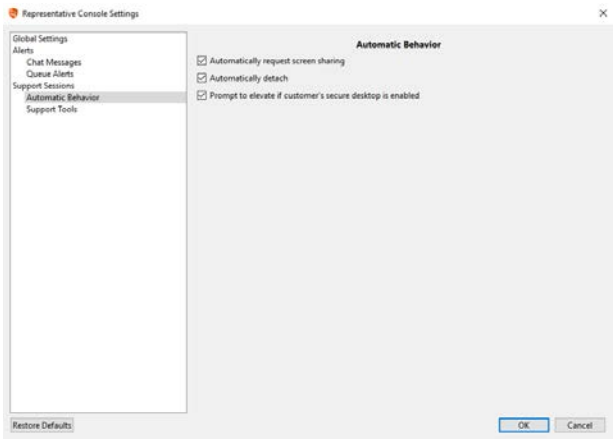
Choose if you wish to hear an alert when a support session is automatically assigned to you. You can designate a custom sound for session assignments.

Additionally, you can choose to be alerted when an automatically assigned session invitation is about to expire. You can choose a custom sound or select **System Beep**, which will play your default system sound.

Choose whether you want to start sessions with chat only or to immediately request screen sharing.

You can choose to open sessions as tabs in the console or to automatically detach sessions into new windows.

For situations where you might experience issues because a customer's secure desktop is enabled, you can be prompted to elevate to run with administrative rights when the session begins.



Set the default quality and size for a screen sharing session. When screen sharing starts, you can automatically enter full screen mode, which in turn can automatically collapse the chat bar.

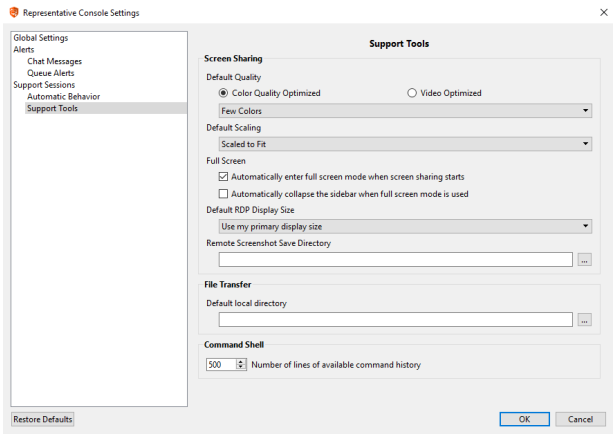
Also when screen sharing starts, the remote system can automatically have its display, mouse, and keyboard input restricted, providing a privacy screen.

Select the default RDP display size for all RDP sessions.

For easier access to screenshots you capture from the console, set the default directory where you will save your console-captured remote screenshots.

For easier file transferring, set the default directory from which you wish to start browsing your local file system.

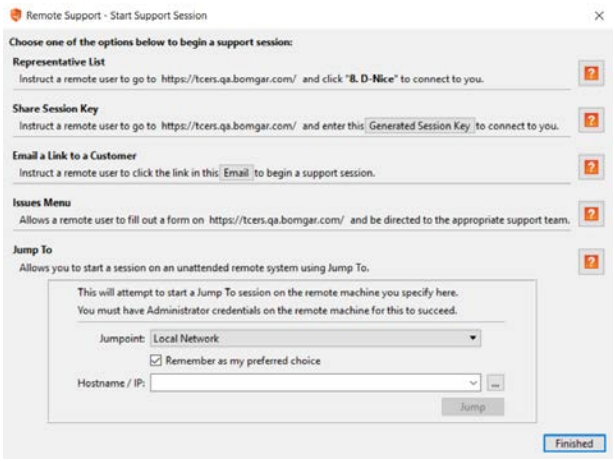
Set the number of lines to save in the command shell history.



Supporting Users

Support Session Start Options

For a quick reference of the ways to start a session, click the **Start** button at the top of your representative console. Note that the available options vary depending on your site configuration and account permissions.



Customer-Initiated Sessions

There are multiple ways for customers to initiate a remote support session with a rep.

Email

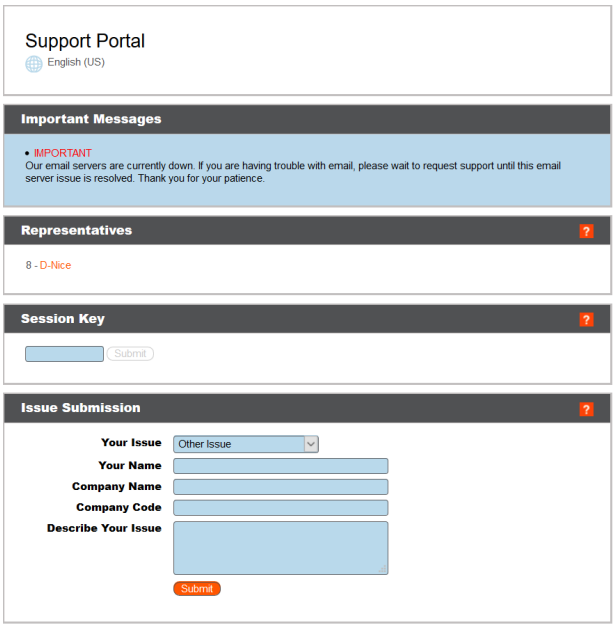
Reps can generate an email message containing a hyperlink. To receive support, the recipient of the email clicks the link, triggering the customer client to download on their system. This establishes a secure connection to the rep who issued the invitation.

URL

Reps can generate a hyper linked URL for the remote user through a variety of methods such as a text chat.

BeyondTrust Web Portal

BeyondTrust allows you to create web support portals, or public web sites, for your Secure Remote Access Appliance. These portals allow your customers to request support utilizing BeyondTrust's remote support software. Each support portal can be configured to support your organization's branding and support processes. This includes customizing logos and allowing customers to start a BeyondTrust session using click-to-chat.



For more information about support portals, please see How to Customize Support Portals at https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/index.htm.

- **Representatives**:You can present a list of logged-on reps, allowing customers to click on a rep's name to begin the customer client download. When the download is complete, a session is started with the rep.
- **Session Key**: A rep may generate a seven-character, alphanumeric session key to share with a customer. From there, the customer visits the support portal and enters the session key into the text entry field. This triggers the customer client to download and establishes a secure connection to the rep who issued the invitation.
- **Issue Submission**: The support portal page can be configured to offer a selection of issues which the customer can choose from when seeking support. Customers may select an issue from the dropdown to trigger the customer client to download. This action generates a request in the team queue associated with that specific issue. For example, if the user selects **Email Problems**, the request is routed to a team of reps skilled in supporting email systems.

Support Button

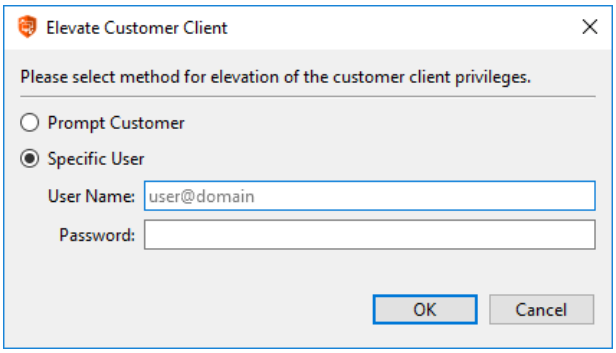
The Support Button is a desktop shortcut previously installed on a customer's workstation that triggers the customer client. When the user clicks the Support Button, they are prompted to enter a session key or describe their issue. Additionally, they may be able to directly join the queue configured for the Support Button.This specific session initiation method may be pre-installed to a standard image and does not require the customer client to be downloaded.

***Note:** A Support Button cannot be deployed from a session that was started from a SAML authenticated public portal and a Support Button cannot be used to start a session with a public portal that requires SAML authentication.*

For more information about Support Buttons, please see Support Button: Quickly Request Support at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm.

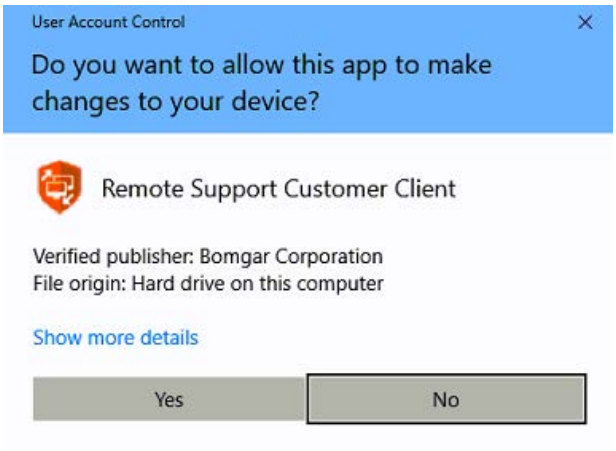
Elevation

For each customer-initiated session start method, the customer client runs in the context of the logged-on user. As a result, the Windows User Access Control (UAC) prompt presents challenges to providing support. To allow support in these situations, BeyondTrust offers the ability to elevate the customer client. This simply means the customer client running as the logged-on user can be elevated to a system service by providing administrative credentials to the customer's system.



This process generates a UAC prompt not seen through screen sharing and must be answered by the customer. This prompt does not require end-user credentials. They only need to click **Yes**.

Once completed, the customer client runs as a system service. As a result, all subsequent UAC prompts are visible when screen sharing.



Rep-Initiated Session

BeyondTrust Jump Client (pre-installed running agent)

The BeyondTrust Jump Client is a running service that allows a rep to initiate a support session to a specific remote system through the representative console.This can be used to initiate sessions to unattended systems where no user is present, or can be used as the default method for providing support to customers. Although the session is rep-initiated, permissions within BeyondTrust allow flexibility on whether or not reps need to prompt the customer for access and can even check for the presence of a logged-on user. Furthermore, access to the individual Jump Clients can be controlled individually or by grouop membership within BeyondTrust, and different groups can have different permissions.

> For more infomation on Jump Clients, please see Remote Support Jump Client Guide: Unattended Access to System in Any Network at https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.

Jump To (ad-hoc)

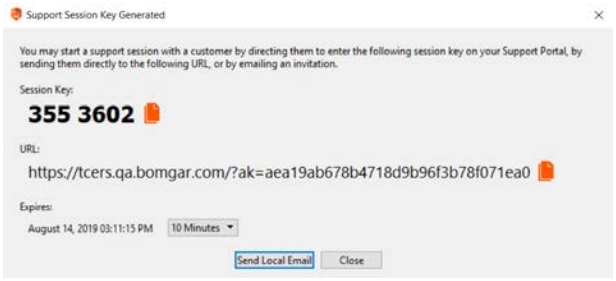
The second rep-initiated method for starting a support session is BeyondTrust Jump To. Jump To allows reps to use the representative console to push the customer client to a remote workstation to initiate a support session. Like downloading the client

from a portal page, this is an ad-hoc session in which no items are pre-installed and everything is removed once the session is completed. Unlike most of the other methods, there are several dependencies for this session initiation method. First of all, it is available for Windows only. Secondly, it depends on several Windows services to execute, and there are several remote TCP ports that must be accessible on the remote machine. For that reason, BeyondTrust offers a technology called Jumpoints which can help initiate sessions on a remote network.

For more information about Jumpoints, please see Remote Support Jumpoint Guide: Unattended Access to Computers in a Network at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.

Generate a Session Key to Start a Support Session

Dependent upon your account permissions, one method of starting a support session is through the use of one-time, randomly generated session keys. Session keys are not used for authentication. They simply route the customer to the appropriate team or rep and are valid for a limited time. The methods by which the Secure Remote Access Appliance generates session keys are proprietary information. When your customer calls with a support request, generate a new session key from:



- The **Support** menu of the representative console
- The **Start** button at the top of the representative console
- The **Session Key** button at the top of the representative console
- Pressing **Ctrl + F4** or **Command + F4**

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.

> For more information, please see "Maximum Session Key Timeout" in Security: Manage Security Settings at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/security-options.htm.

You also can select the public portal through which you want your customer to enter the session. The representative console remembers your choice the next time you generate a session key.

Depending on the options selected by your administrator, you may be able to send the invitation from your local email, from a server side email, or by SMS.

Direct your customer either to go to the unique URL or to enter the session key on your public site. After running the customer client, your customer will appear in your personal queue.

View Support Sessions in Queue

Queues

Session queues provide information about and access to customers who are waiting for support. The **Personal** queue contains customers with whom you are currently in session or who are waiting for a session with you specifically. A waiting session appears in your personal queue if it was transferred to you or if the customer initiated it by entering a session key you generated, by selecting your name from the public site, or by clicking a Support Button tied to you. This queue also contains invitations for you to join a shared session.

You also have queues for any teams of which you are a member. If a customer initiates a session by selecting an issue type from an issue submission form, that customer enters a specific team queue based on which team owns that issue. A customer also enters a team queue if they click a Support Button tied to a team. A session may also enter a queue if it is transferred intentionally or due to waiting session rules, or if the representative's connection is lost in the middle of a session. These queues also contain invitations for any representative in the team to join a shared session.

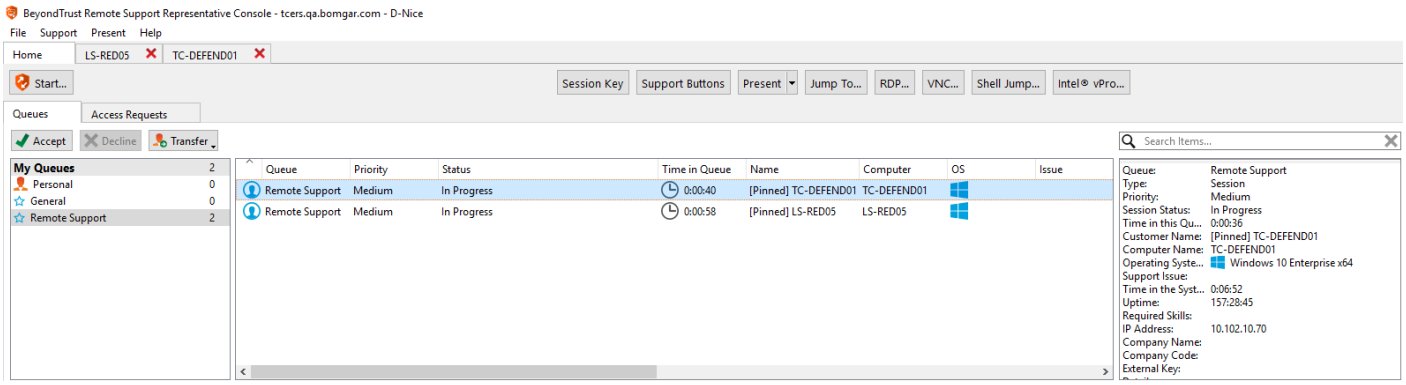
Click the star to the left of a team name to mark that queue as a favorite. If a team chat message is sent, an orange chat bubble appears in place of the star.

Customers can also request assistance directly from a web page which contains a help link. This initiates a browser sharing session, which allows a representative to chat and view the customer's web page. Administrators can generate custom links in order to direct browser sessions to the correct representative or team queue. In the queue, browser sharing sessions are identified by the **[Browser]** prefix next to the customer's name.

Sort your queues by several criteria, including the length of time the customer has been in queue, the customer's name, issue category, etc. All criteria may not be available depending on the manner in which the customer initiated the session. You can also search for an active session. Click on an item in queue to view its details. Click it again to close the details pane. The representative console remembers the column order and the sort order of the session queue the next time the representative console is launched.

Once the customer is in queue, either double-click the customer entry or select the entry and click the **Accept** button. Accepting a session opens a new tab for that session at the top of the representative console. You can run multiple sessions simultaneously. A new tab will be created for each session.

For additional ways to accept support requests, please see "Accept a Session to Start Support" on page 20.



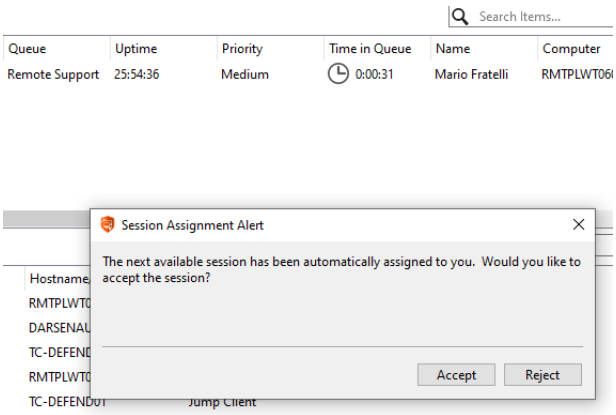
Accept a Session to Start Support

Once the customer is in queue, there are several ways you can accept the session. If the session is in your personal queue or if you have permission to manually accept sessions from a team queue, either double-click the customer entry or select the entry and click the **Accept** button. If allowed to use the feature, start supporting the oldest queued session from among your team queues by selecting to get the next session from:

- The **Support** menu of the representative console
- The **Get Next** button at the top of the representative console

Session Assignment Rules

You also can accept sessions that are assigned using Equilibrium. When a session enters a queue that has Equilibrium enabled, that session is automatically assigned to the best qualified and least busy representative, based on matching skills, the number of sessions that representative is supporting, and how long they have been available.



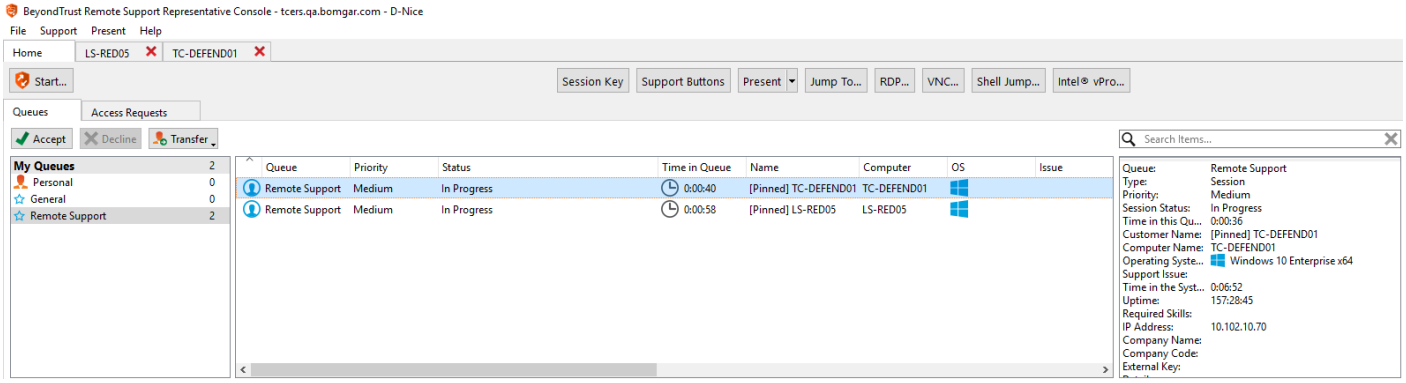
When a session is assigned to you, you are given a prompt to accept or reject the session, along with visual and audible alerts if enabled. When the invitation is about to expire, visual and audible alerts warn you. If you reject the invitation or the invitation times out, the session is reassigned to the next best qualified and least busy representative for that queue.

A rejected session is never assigned to the same representative twice unless it is manually transferred into another queue for which that representative is available. If a session cycles through all available representatives for the queue and is not accepted, it remains in queue until someone manually accepts or transfers it.

Alternatively, if your administrator has set up a waiting session rule for this queue, the session is either given an audible and visual alert when it is overdue, or it is transferred to an overflow queue. If that overflow queue has a waiting session rule set up that transfers the session back to the first queue, the session could potentially bounce back and forth between the queues until it is accepted.

A session is not assigned to a representative if that representative is unavailable. If you lock your computer or switch to the login screen, you are marked as unavailable. Also, rules within the user permissions mark you as unavailable if you are participating in more than a set number of sessions or have been idle longer than a specified length of time. Finally, if you have permission to opt out of session assignments, you may choose not to receive automatic session assignments. Set auto assignment from:

- The **Support** menu of the representative console
- The **Auto Assign** button at the top of the representative console
- The right-click menu of the system tray icon



Accepting a session opens a new tab for that session at the top of the representative console. You can run multiple sessions simultaneously. A new tab is created for each session.

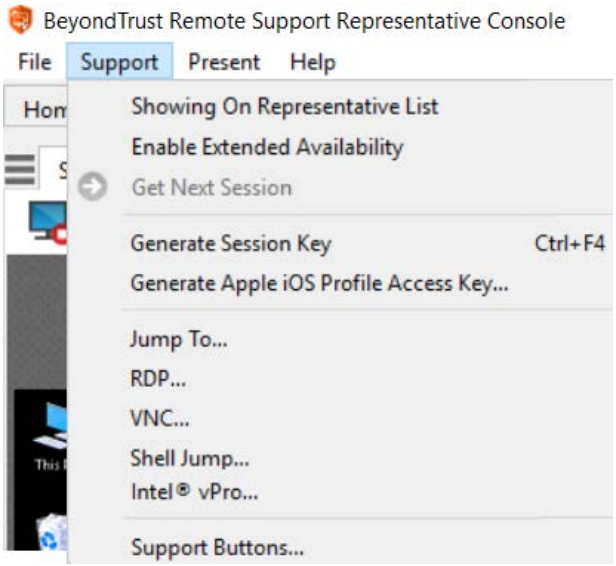
Note: *Session tabs can be moved and reordered to help you organize and prioritize your workload. Simply click and drag a session tab to a new position. Session tabs can also be detached from the main representative console window.*

Generate an Apple iOS Profile Access Key

To distribute your BeyondTrust-enabled public and private profiles to Apple iOS device customers, generate an Apple iOS profile access key from the **Support** menu of the representative console.

The setting **iOS Configuration Profiles Link Enabled** must be selected in **/login > Public Portals > iOS Configuration** for this option to be available.

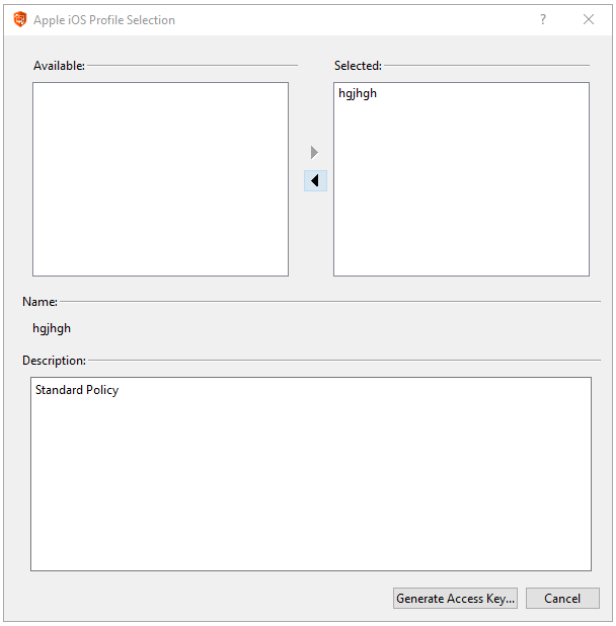
Click **Generate Apple iOS Profile Access Key** to launch the **Apple iOS Profile Selection** interface.



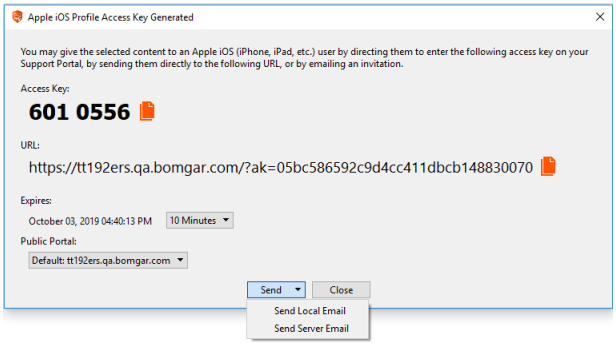
The **Apple iOS Profile Selection** interface contains available public or private profiles previously configured in the /login interface.

While the public site can be made to show public iOS profiles to anyone who knows the URL, generating an access key is the only way to give a customer access to a private iOS profile.

Here you may select any public or private profiles to securely distribute to your Apple iOS device customers via your iOS-browsable support portal. Click the **Generate Access Key** button.



When you click the **Generate Access Key** button, a unique **Access Key Generated** screen launches containing special options for sending an email invitation to your Apple iOS device customer. Depending on the options selected by your administrator, you may be able to send the invitation from your local email, from a server side email, or by SMS.



Jump Interface

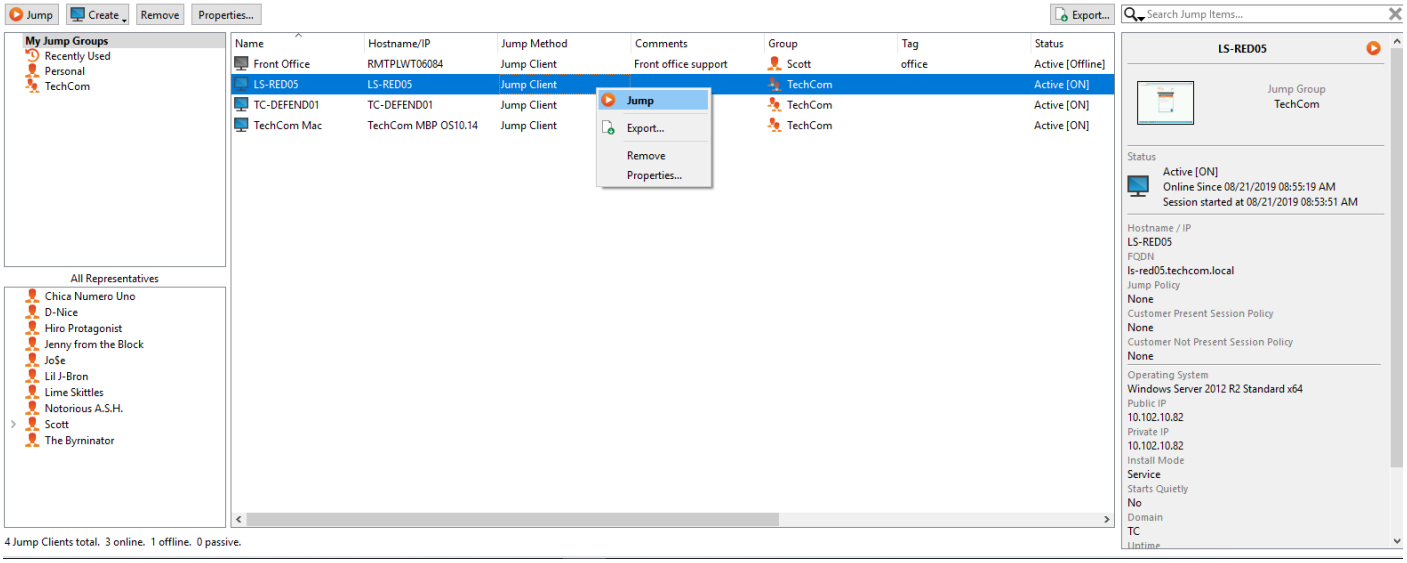
Use Jump Items to Support Remote Systems

BeyondTrust Jump Technology enables privileged users to connect to an unattended remote system to start a session without end-user assistance. Dependent upon your permissions, you may Jump to any computer on your LAN/VPN or on a network with a Jumpoint agent. You can save Jump Shortcuts for frequently accessed machines. To Jump to a non-Windows computer or a system which is not on a network, you can install a Jump Client.

The Jump interface appears in the bottom half of the representative console. The list may contain both active and passive Jump Clients, as well as Jump shortcuts for Remote Jumps, Local Jumps, Remote and Local RDP sessions, Remote and Local VNC sessions, Shell Jumps, and Intel® vPro Jumps.

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. Selecting a Jump Group and then clicking **Create** auto-selects that Jump Group in the Jump Item configuration window.

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.



Jump to a Jump Item

Browse through groups or dynamically search for computers.

To facilitate browsing the Jump Clients list, you may drag the columns into any order you wish, and then sort a column by clicking the column header. The representative console remembers the column order and the sort order the next time the representative console is launched.

In addition to browsing for Jump Clients, you can search based on multiple fields. Enter a string in the search field and then press **Enter**. To change the fields you are searching, click on the magnifying glass and check or uncheck any of the available fields.

Searchable fields include **Comments**, **Console User**, **Domain, Group**, **Hostname/IP**, **Jump Method**, **Last Accessed**, **Name**, **Private IP**, **Public IP**, **Status**, **Tag**, and **Workgroup**.

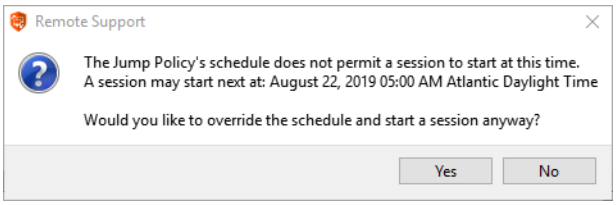
Once you have found the computer you wish to access, double-click the entry, or select the entry and click the **Jump** button. This will attempt to start a session with the remote computer.

> ***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.*

You may programmatically connect to a Jump Item directly from your systems management or ticketing tool. If your search results in only one Jump Item, the session will start immediately. If multiple Jump Items are returned, select one of the Jump Items listed in the selection window and click **OK**.

> For more information about scripting, please see Representative Console Scripting and Client Scripting API at www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script.

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



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

Use Jump Clients to Access Unattended Computers

To access an individual computer without end-user assistance, install a Jump Client on that system either from within a session or from the **Jump Clients** page of the administrative interface. Your account settings determine what Jump Item permissions you have, including which Jump Groups you can access and which types of Jump Items you are allowed to use.

Sort Jump Clients

To facilitate browsing the Jump Clients list, you may drag the columns into any order you wish, and then sort a column by clicking the column header. The representative console remembers the column order and the sort order the next time the representative console is launched.

Search for a Jump Client

In addition to browsing for Jump Clients, you can search based on multiple fields. Enter a string in the search field and then press **Enter**. To change the fields you are searching, click on the magnifying glass and check or uncheck any of the available fields. Searchable fields include **Comments**, **Console User**, **Domain, Group**, **Hostname/IP**, **Jump Method**, **Last Accessed**, **Name**, **Private IP**, **Public IP**, **Status**, **Tag**, and **Workgroup**.

Jump Client Details Pane

When you select a Jump Client, a details pane appears to the right of the Jump interface. Which details are shown here is determined by the **Jump Client Statistics** setting in the /login interface as well as by the remote operating system.

If a Jump Client goes offline and does not reconnect to the Secure Remote Access Appliance for the number of days set by the **Jump Client Settings** in the /login interface, it is labeled as lost. No specific action is taken on the Jump Client. It is labeled as lost only for identification purposes, so that an administrator can diagnose the reason for the lost connection and take action to correct the situation. In the details pane, you will see the scheduled deletion date should the Jump Client not come back online.

After a software update, Jump Clients update automatically. The number of concurrent Jump Client upgrades is determined by settings on the **/login > Jump > Jump Clients** page. If a Jump Client has not yet been updated, it is labeled as **Upgrade Pending**, and its version and revision number appear in the details pane. While you can modify an outdated Jump Client, you cannot Jump to it. Attempting a Jump does, however, move that Jump Client to the front of the upgrade queue.

Wake-On-Lan (WOL)

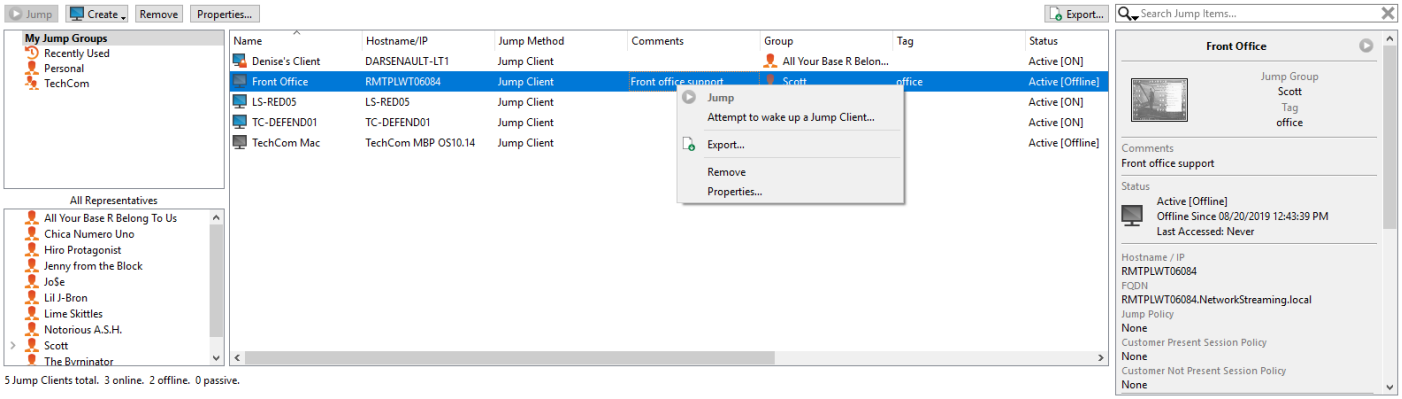
Wake-On-Lan (WOL) allows you to remotely turn on or wake up machines configured for WOL from BeyondTrust. In a configured environment, customers can power off their machine but still receive BeyondTrust support, if needed.

Note: *WOL is not a BeyondTrust technology. The BeyondTrust software integrates with existing WOL systems. To use WOL through BeyondTrust, the system must have WOL enabled, and the network must allow WOL packets to be sent.*

To enable support for WOL in BeyondTrust, turn on the WOL setting in the administrative /login interface under **Jump > Jump Clients**. When enabling the WOL option, keep the following items in mind:

- WOL does not work for wireless clients. A wired network connection is required.
- WOL is supported by the underlying system hardware, which is independent of the installed OS.
- WOL is supported only by active Jump Clients. Passive Jump Clients, Jumpoints, and Local Jump from representative consoles do not support WOL.

To wake an active Jump Client using WOL, right-click an existing Jump Client from within the representative console. Attempt to wake the system by clicking the **Attempt to wake up Jump Client** option.

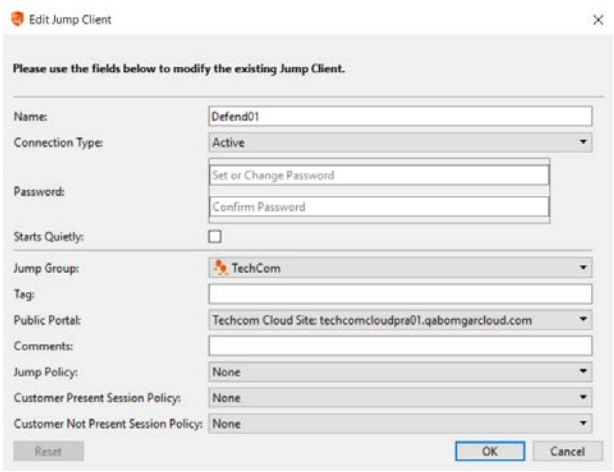


The wake option is only available when selecting a single Jump Client. It is not available when multiple Jump Clients are selected.

WOL packets are sent from other Jump Clients residing on the same network as the target machine. When an active Jump Client is installed or checks-in, it registers its network information with the appliance, and the appliance uses this information to determine which Jump Clients are on the same network.

Once attempting to wake up a selected Jump Client, the WOL option greys out for 30 seconds before being able to attempt to send another wake up request. If no other Jump Clients are available on that same network to send WOL packets to the target machine, the rep receives a message indicating that no other Jump Clients are available on the network. When sending a WOL packet, the rep has an advanced option to provide a password for WOL environments requiring a secure WOL password. A WOL packet is a one-way packet, and no confirmation of success is given to the rep besides seeing the client come online in the representative console.

Jump Client Properties



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

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

Change a Jump Client's mode from the **Connection Type** dropdown. Active Jump Clients send statistics to the Secure Remote Access Appliance on a defined interval. Passive Jump Clients send statistics to the Secure Remote Access Appliance once a day or upon a manual check in. Based on the options your administrator sets, these statistics may include the remote computer's logged-in console user, operating system, uptime, CPU, disk usage, and a screen shot from the last update.

Once a Jump Client has a password set, its icon shows that it is locked, and its screen shot is also locked. In order to Jump to a locked Jump Client, you must provide its password. Also, you must provide the password to remove a locked Jump Client via the Jump Client interface; you do not need the password to unpin from within a session, as you would already have provided the password to Jump into the session.

If **Starts Quietly** is checked, the customer client does not take focus and remains minimized in the taskbar or dock when a session is started.

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.

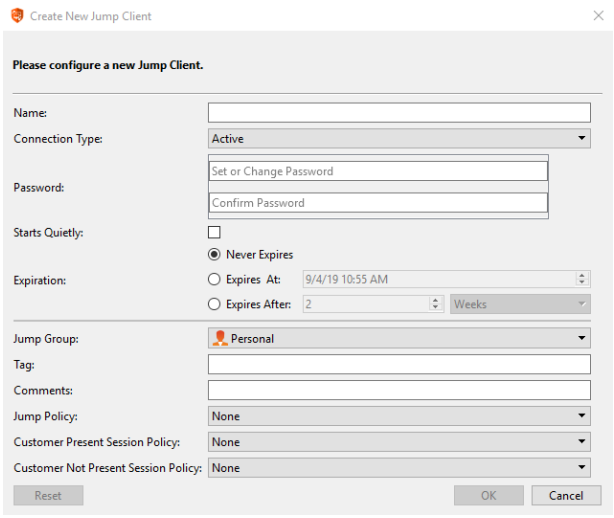
Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

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 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.

When pinning a Jump Client from within a session and customizing its properties beforehand, you also have the option to set when the Jump Client expires. This can be never, at a specific time and date, or after a certain length of time. An expired Jump Client automatically uninstalls from the remote system and is removed from the list in the Jump Client interface.



If you no longer need access to a remote system, select the Jump Client and click the **Remove** button, or right-click on the Jump Client and select **Remove** from the menu. You may select multiple Jump Clients to remove them all at the same time.

> ***Note:*** *If the remote user manually uninstalls a Jump Client, the deleted item is either marked as uninstalled or completely removed from the list of Jump Items in the representative console. This setting is available at* ***/login > Jump > Jump Clients****. If the Jump Client cannot contact the Secure Remote Access Appliance at the time it is uninstalled, the affected item remains in its offline state. If a Jump Client goes offline and does not reconnect to the Secure Remote Access Appliance for 180 days, it is automatically uninstalled from the target computer and is removed from the Jump interface.*

<table>
<tr><th colspan="2">Active and Passive Jump Clients</th></tr>
<tr><th>Active Jump Client</th><th>Passive Jump Client</th></tr>
<tr><td>Maintains a persistent connection to the Secure Remote Access Appliance.</td><td>Listens for a remote access request from the Secure Remote Access Appliance.

Note: Some firewall configuration may be required.</td></tr>
<tr><td>Sends statistics to the Secure Remote Access Appliance at regular intervals.</td><td>Sends statistics to the Secure Remote Access Appliance once a day, upon manual check-in, or when a new user logs in (if this feature is enabled).</td></tr>
<tr><td>Enables remote access to any desktop operating system supported by BeyondTrust.</td><td>Enables remote access to any desktop operating system supported by BeyondTrust.</td></tr>
<tr><td>Number of installable clients is limited by your Secure Remote Access Appliance model.

<table><tr><th>B200</th><th>B300</th><th>B400</th></tr><tr><td>Up to 1,000 Active Jump Clients</td><td>Up to 10,000 Active Jump Clients</td><td>Up to 25,000 Active Jump Clients</td></tr></table></td><td>50,000 passive Jump Clients supported on all Secure Remote Access Appliance models.

If you need more passive Jump Clients, contact technical support at www.beyondtrust.com/support.</td></tr>
</table>

The maximum number of Jump Clients available to a Virtual Appliance is based on allocated resources. For more information, please see the Virtual Appliance Sizing Guidelines at www.beyondtrust.com/docs/remote-support/getting-started/deployment/virtual/sizing.htm.

Use Jump Clients to Access Unattended Android Devices

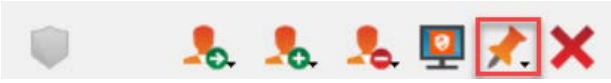
Beginning with BeyondTrust 16.1, a persistent connection can be established with an Android device by pinning a Jump Client to the device. This provides the ability to have unattended support sessions with Android devices. You can deploy Jump Clients using either of the methods below.

Note: *Bandwidth usage and battery life are minimally affected by establishing a persistent connection.*

Persistent connections to an unattended Android device can occur only when the devices have both the **BeyondTrust Support Client App 2.2.7** and **BeyondTrust Jump Client App 2.2.0** installed from the Google Play Store. For more information, please see Download the BeyondTrust Support Client and BeyondTrust Jump Client Apps at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-download-app.htm.

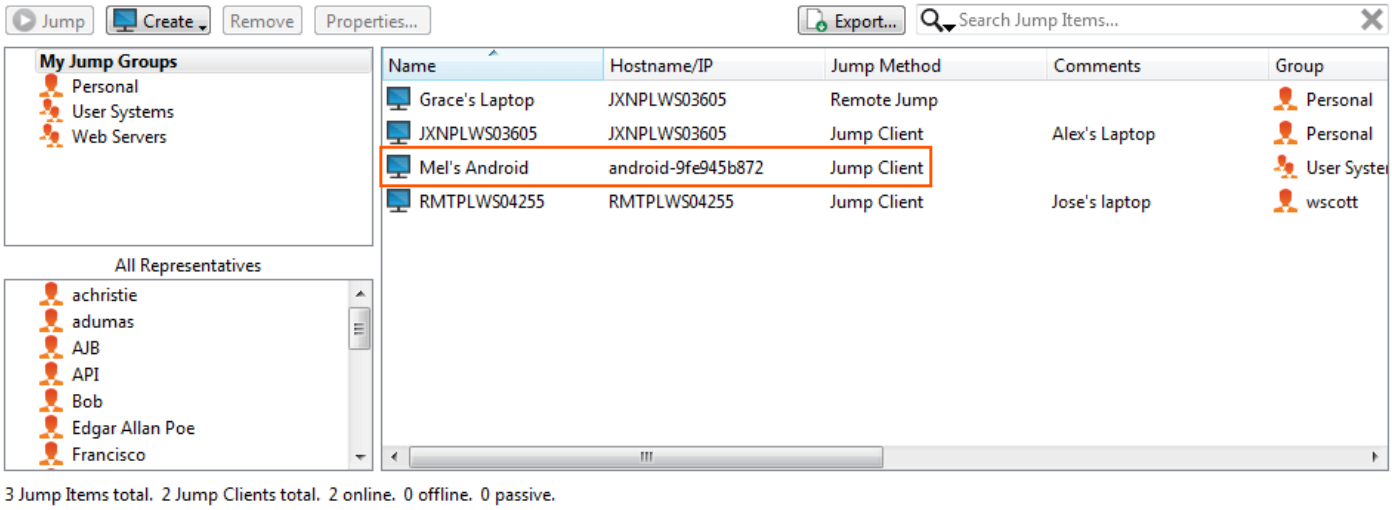
Pin an Android Jump Client from the Representative Console

1. While in a support session with the Android device, click on the **Pin as Jump Client** icon.



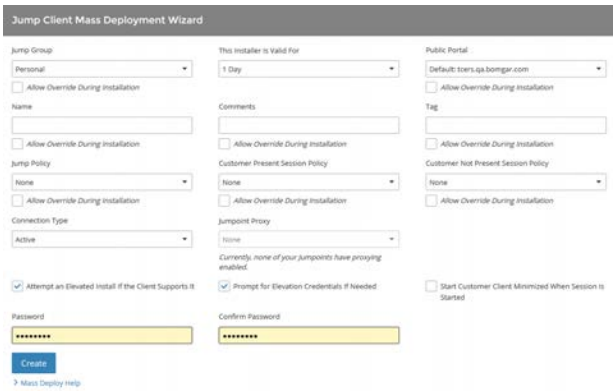
2. After pinning, click the **Refresh** option located above the Jump Items list, and the Android device will appear as a Jump Item in the Jump Item list. If the **Pin a Jump Client** icon is gray, the Android Jump Client has not been installed on the Android device.
3. Meanwhile, the BeyondTrust Jump Client app on the device should show the client as pinned with a date and timestamp.

> ***Note:*** *Options are available for the Jump Client to be disabled if the device is relying on battery power or on data to connect.*



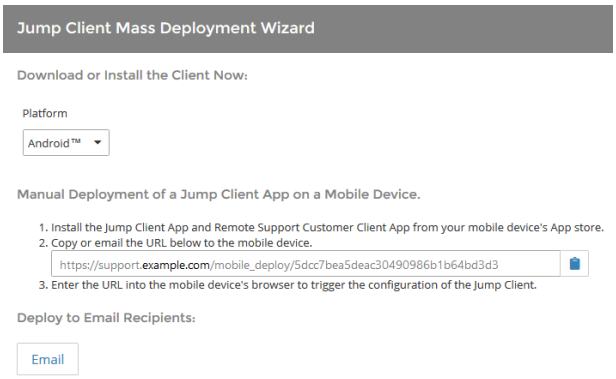
Email a Link from the /login Interface to Install and Android Jump Client

1. From the /login interface, navigate to **Jump > Jump Clients > Jump Client Mass Deployment Wizard**.



2. Complete the information needed for your Jump Client, such as **Jump Group**, **Public Portal**, etc.
3. Click **Create**.

4. From the **Download or Install the Client Now** section, choose **Android** as your platform.
5. Verify that the **BeyondTrust Jump Client** app is installed on the Android device. If not, navigate to the Google Play App store to download the app.



6. To download the Jump Client to the device, open a browser on the Android device and go to the URL provided by the mass deployment wizard.

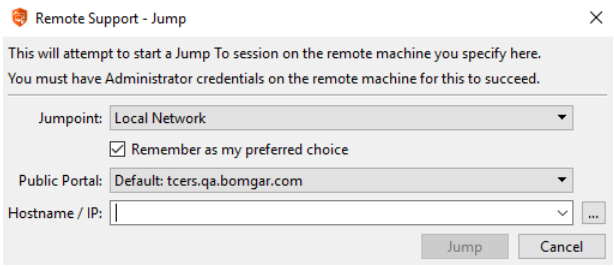
> ***Note:*** *You can also email the URL to the Android device by clicking on the* ***Email*** *link located in the* ***Deploy to Email Recipients*** *section.*

Create and Use Local Jump Shortcuts

> ***Note:*** *Jumpoint is only available for Windows systems. Jump Clients are needed for remote access to Mac or Linux 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. If you need to access remote computers via Jumpoint when no user is available, make sure your account permissions are set either to disable prompting or to default to* ***Allow****. You cannot Jump to a mobile device, though Jump Technology is available from mobile BeyondTrust consoles.*

To Jump without a pre-installed client, open the **Jump to…** dialog from:

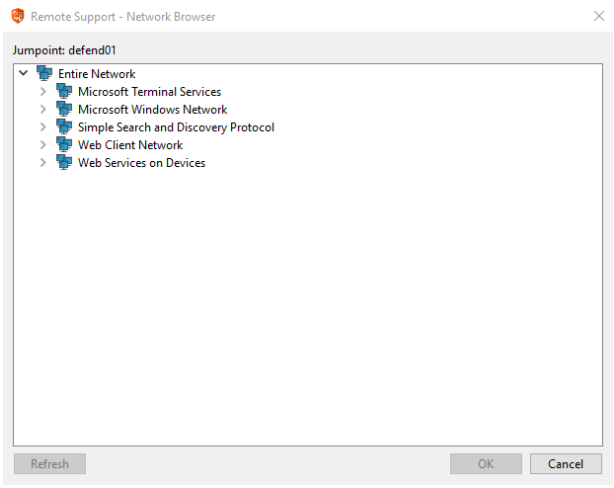
- The **Support** menu of the representative console
- The **Start** button at the top of the representative console
- The **Jump To** button at the top of the representative console



From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. Depending on your account permissions, you can Jump to a system on your local network or a network on which a Jumpoint is installed.

Select the public portal you wish to associate your session with. This lets the system know what customer agreement behavior should occur.

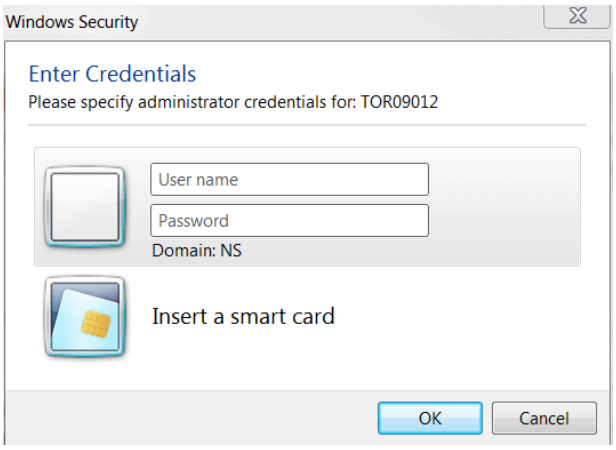
> For more information, please see Customer Client: Modify the Invitation Email, Display Options, Connection Options at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/customer-client.htm.



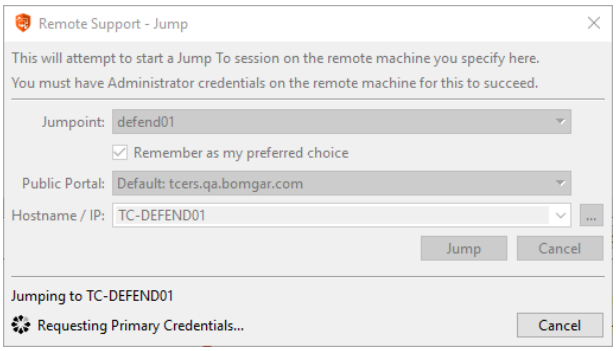
Enter the hostname or IP address of the system you wish to access. Alternatively, if network browsing is enabled from the **/login > Jump > Jumpoint** page, you can click the **[...]** button to browse the directory tree.

Once you have located the computer you wish to access, click **Jump**.

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.



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****.*

Create and Use Remote and Local Jump Items

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.

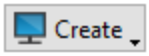
A Jumpoint acts as a conduit for unattended access to Windows computers on a known remote network. A single Jumpoint installed on a computer within a local area network is used to access multiple systems, eliminating the need to pre-install software on every computer you may need to access.

Local Jump enables a privileged user to connect to an unattended remote computer on their local network. Within the local area network, the BeyondTrust user's computer can initiate a session to a Windows system directly without using a Jumpoint.

> ***Note:*** *Remote Jump and Local Jump are available only for Windows systems. Jump Clients are needed for remote access to Mac or Linux 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 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**.

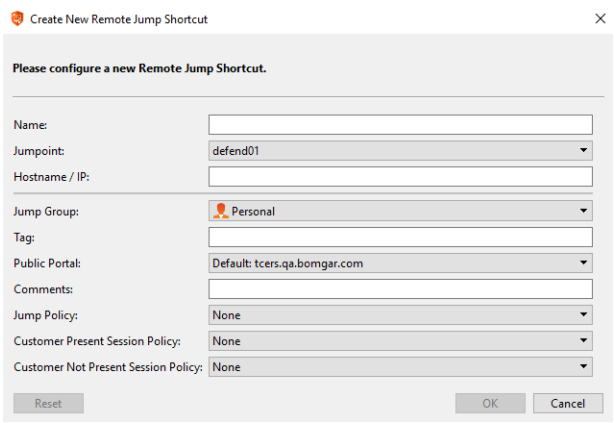
> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be all the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

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.

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.

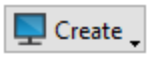
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose 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.

Create a Local Jump Shortcut

To create a Local Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Local Jump**. Local Jump 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**.

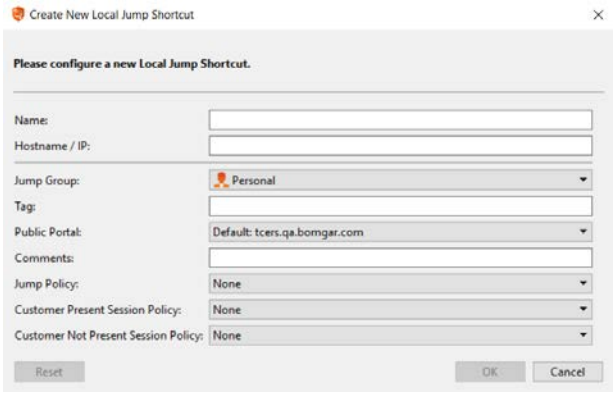
> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be all the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

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

Enter the **Hostname / IP** of the 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.

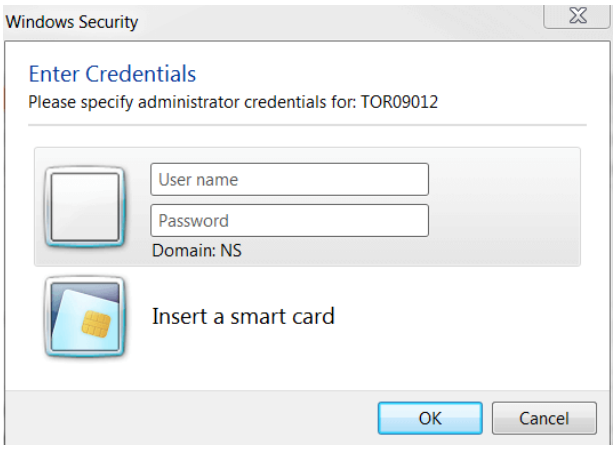
Choose session policies to assign to this Jump Item. Session policies assigned to this Jump Item have the highest priority when setting session permissions. The **Customer Present Session Policy** applies when the end user is determined to be present. Otherwise, the **Customer Not Present Session Policy**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

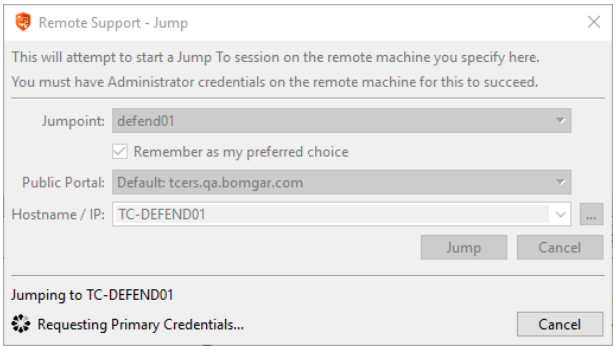
Use a Remote Jump Shortcut or Local Jump Shortcut

To use a Jump shortcut to start a session, simply 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.



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****.*

RDP to a Remote Windows System

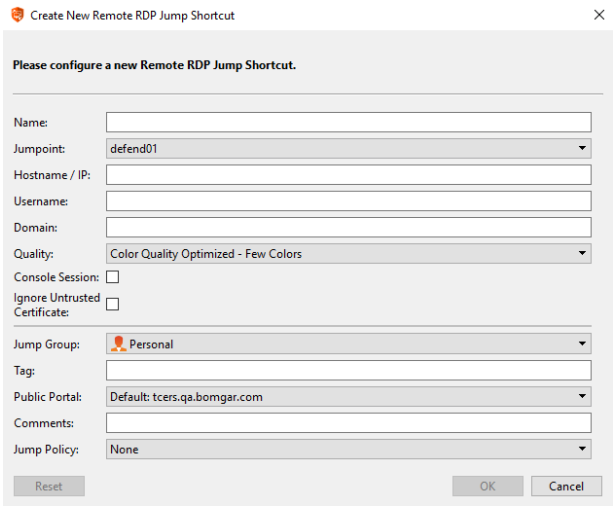
Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a remote Windows system. Because remote desktop protocol sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as your administrator has defined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

To use Local RDP through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local RDP**.

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**.

To start an RDP session, open the **Remote Desktop Protocol** dialog from:

- The **Support** menu of the representative console
- The **RDP To** button at the top of the representative console

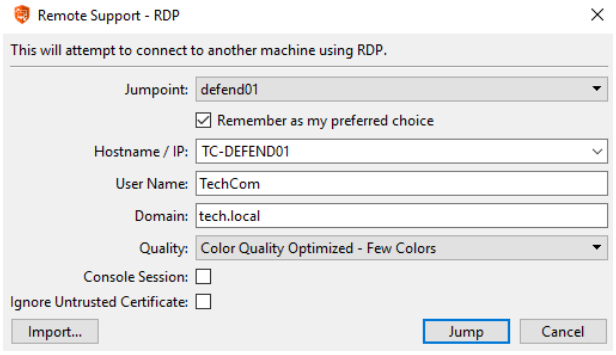


From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the system you wish to access.

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>** (e.g., 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.

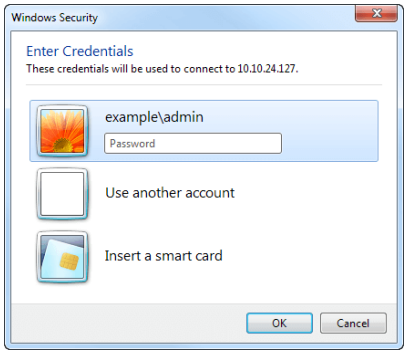
Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

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.

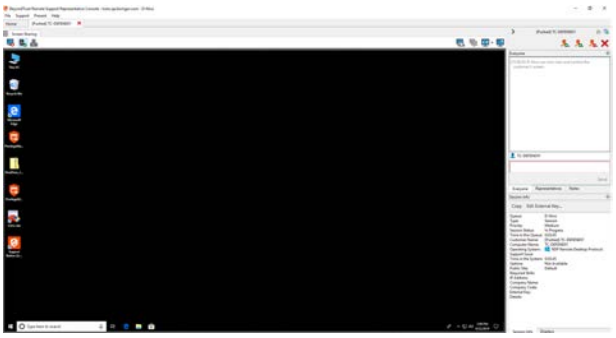
To import an RDP file, click the **Import** button. This pre-populates some of the fields required for the remote desktop protocol connection.

To begin the remote desktop (RDP) session, click **Jump**.

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



Your remote desktop protocol (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 also can share or transfer the RDP session with other logged-in BeyondTrust users, following the normal rules of your user account settings.

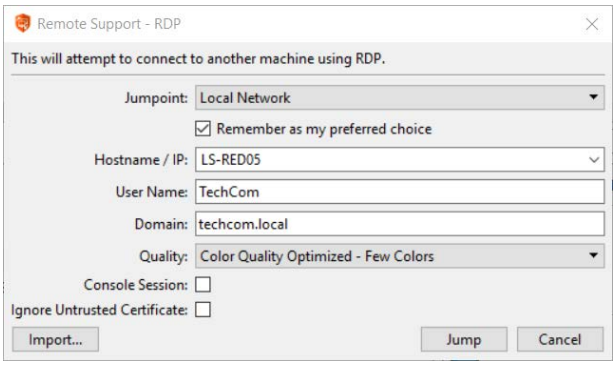


***Note:** Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to **Start New Session**, then a new independent session starts for each user who Jumps to a specific RDP Jump Item. The RDP configuration on the endpoint controls any further behavior regarding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

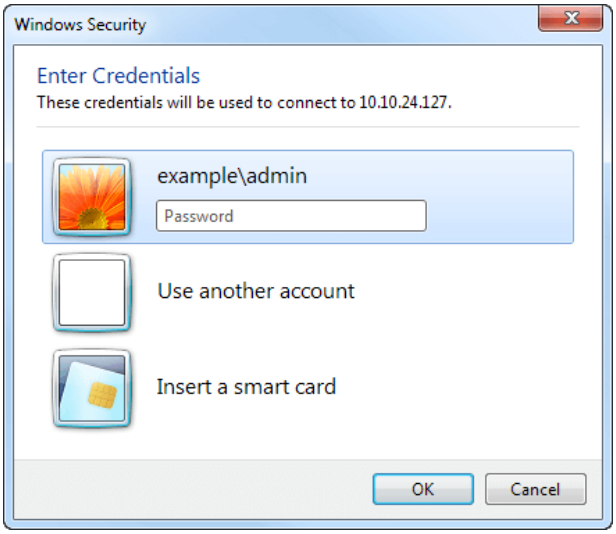
For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Use Local RDP for Access to Windows Systems

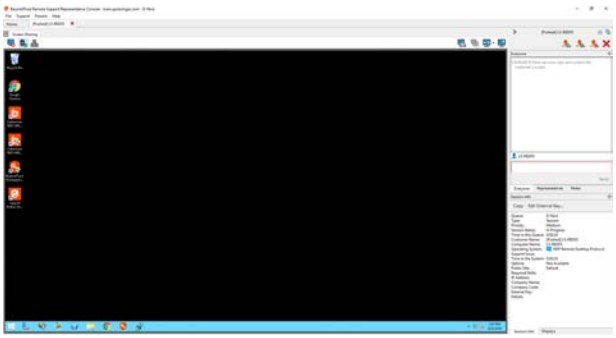
Use BeyondTrust to start a Local Remote Desktop Protocol (RDP) session with a remote Windows system. Unlike a typical BeyondTrust RDP session, Local RDP sessions are not proxied through a Jumpoint, which means that users can Jump only to systems within their local network. To use Local RDP through BeyondTrust, you must have the user account permission **Allowed Jump Methods: Local RDP via the local network**.



1. To start a Local RDP session from the representative console, open the **Remote Desktop Protocol** dialog from either the **Support** menu or **RDP To** button.
2. Choose **Local Network** for your Jumpoint option.
3. Enter the hostname or IP address of the computer you wish to support.
4. Provide the username to sign in as.
5. Select a domain.
6. 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.
7. To start a console session rather than a new session, check the **Console Session** box. If the server's certificate cannot be verified, you will receive a certificate warning. Checking **Ignore Untrusted Certificate** allows you to connect to the remote system without seeing this message.
8. To import an RDP file, click the **Import** button. This pre-populates some of the fields required for the remote desktop protocol connection.
9. To begin the remote desktop (RDP) session, click **Jump**.
10. You will be prompted to enter the password for the username you specified earlier.



11. Your remote desktop protocol (RDP) session will now begin.



Create and Use Remote or Local RDP Jump Items

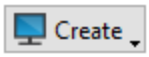
Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a remote Windows system. Because remote desktop protocol sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as your administrator has defined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

To use Local RDP through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local RDP**.

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 Local RDP Shortcut

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



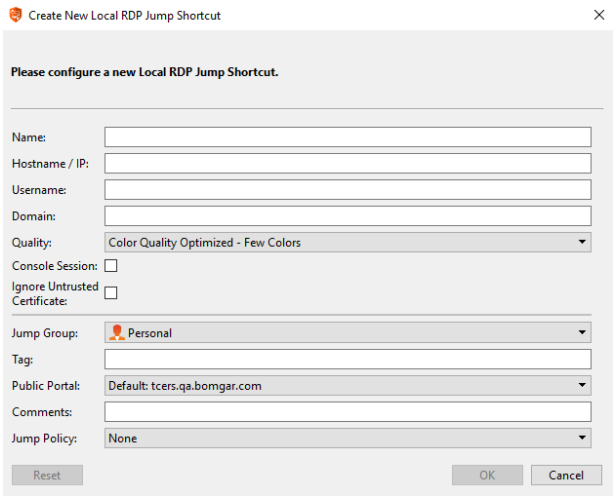
Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be 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.

Enter the **Hostname / IP** of the 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>*** *(e.g., 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.

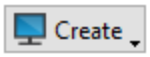
Select the **Public Portal** through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

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

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.

Create a Remote RDP Shortcut

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

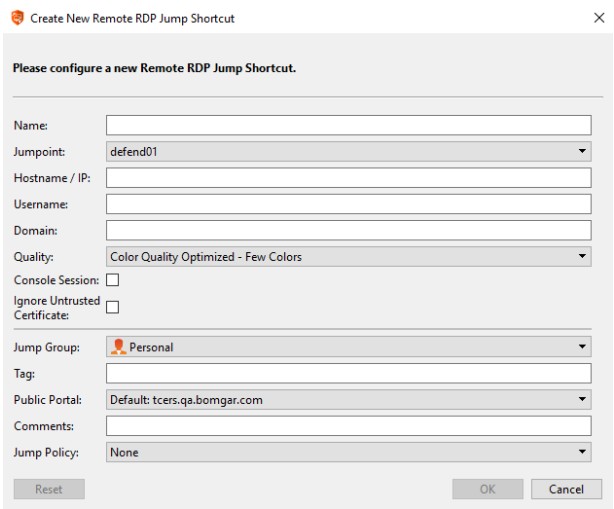


Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be 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.



> ***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>*** *(e.g., 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.

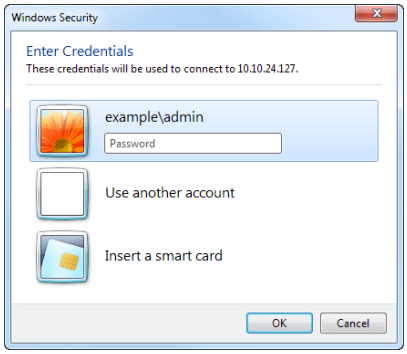
Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

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.

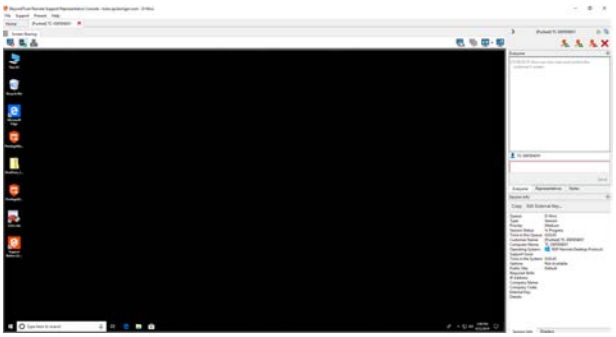
Use an RDP Shortcut

To use a Jump shortcut to start a session, simply 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.



Your remote desktop protocol (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 also can share or transfer the RDP session with other logged-in BeyondTrust users, following the normal rules of your user account settings.



***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.

VNC to a Remote System

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.

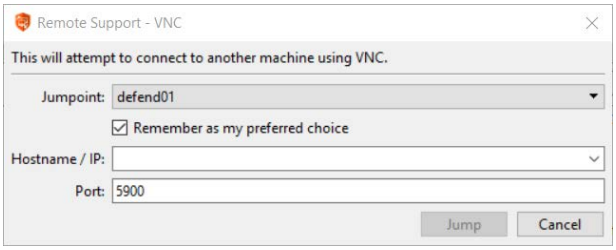
To use Local VNC through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local VNC**.

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

To start a VNC session, open the **VNC** dialog from:

- The **Support** menu of the representative console
- The **VNC** button at the top of the representative console

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the 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.

To begin the VNC session, click **Jump**.

Create and Use VNC Shortcuts

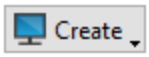
Use BeyondTrust to start a VNC session with a remote system. Because VNC sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as defined by your administrator for your site.

To use Local VNC through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local VNC**.

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

Create a Local VNC Shortcut

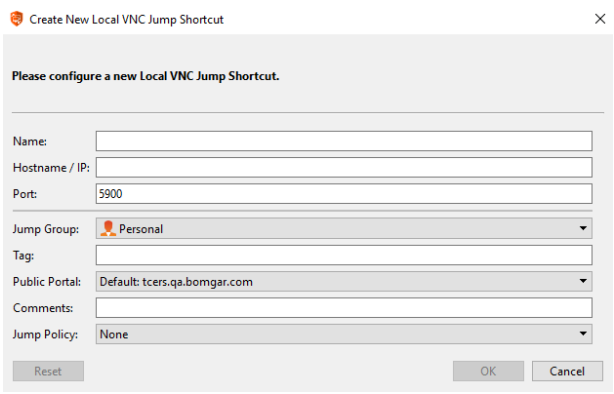
To create a Local VNC shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Local VNC**. VNC shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.



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 all the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*

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



Enter the **Hostname / IP** of the 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.

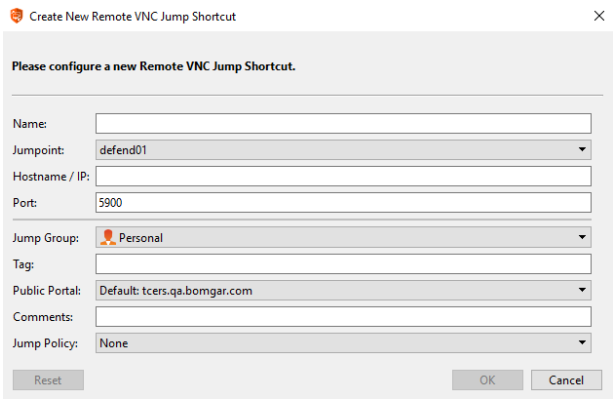
Create a Remote VNC Shortcut

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 all the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*

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.

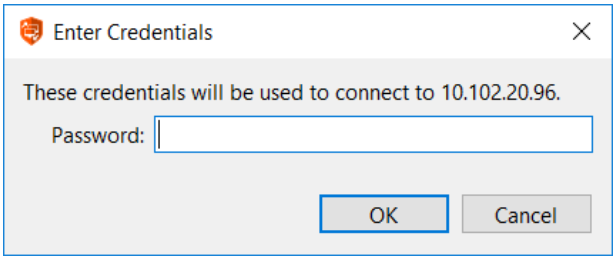
Jump Items include a **Comments** field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

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.

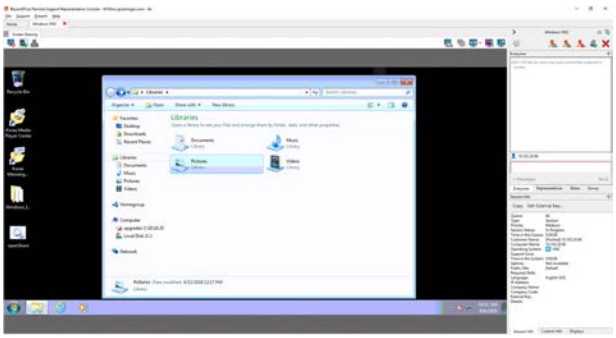
Use a VNC Shortcut

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

When establishing the connection to the VNC server, the system determines if there are any credentials associated. If so, it prompts you to enter them.



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.



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.

Shell Jump to a Remote Network Device

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.

To perform a Shell Jump through BeyondTrust, you must have access to a Jumpoint with Shell Jump enabled, and you must have the user account permission **Allowed Jump Methods: Shell Jump**.

To start a Shell Jump session, open the **Shell Jump** dialog from:

- The **Support** menu of the representative console
- The **Shell Jump** button at the top of the representative console

Your Jumpoint may be configured for provisioned Shell Jump access only.

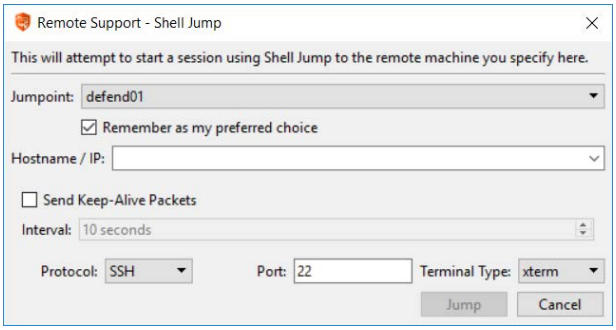
From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Select the provisioned system you wish to access.

Alternatively, your Jumpoint may be configured for open access or limited access.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**.

To access a provisioned system, check **Use Provisioned** and select the system from the dropdown.

Alternatively, enter the **Hostname / IP** of the system you wish to access. If your Jumpoint is configured for limited access, the remote system must be in the delimited IP address range.



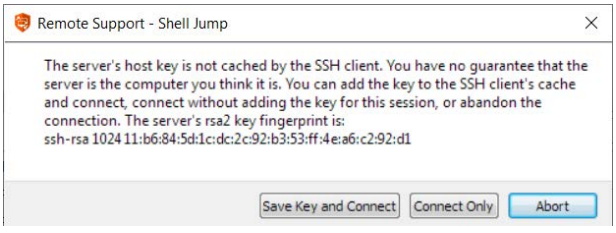
You can choose to **Send Keep-Alive Packets** to keep idle sessions from ending. Enter the number of seconds to wait between each packet sent.

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

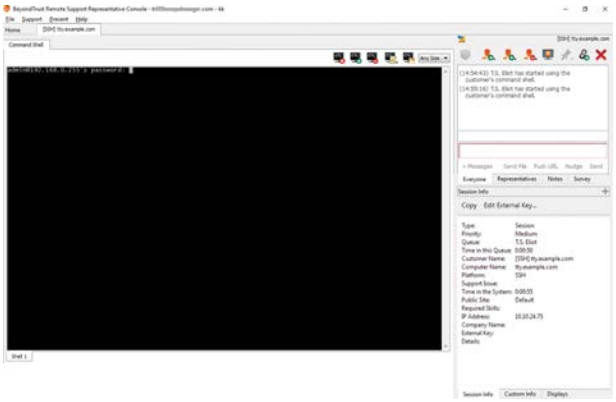
Then click **Jump**.

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.



When you Shell Jump to a remote device, a command shell session immediately starts with that device. If you are Shell Jumping 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.

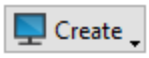


Create and Use Shell Jump Shortcuts

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

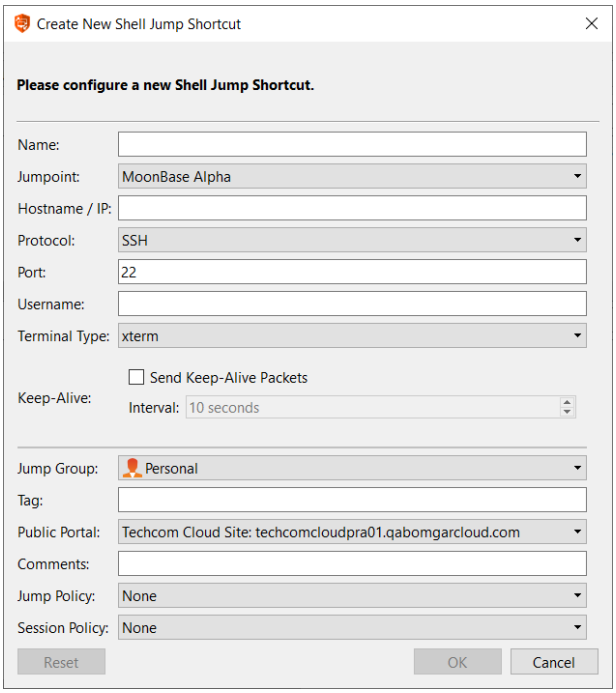
To create a Shell Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Shell Jump**. Shell Jump shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.



> ***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.

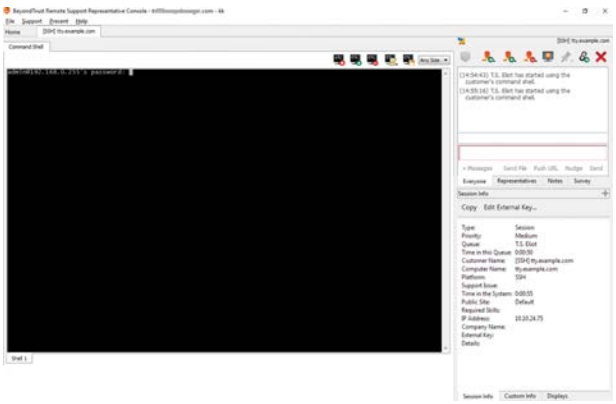
Use a Shell Jump Shortcut

To use a Jump shortcut to start a session, simply 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.

When you Shell Jump to a remote device, a command shell session immediately starts with that device. If you are Shell Jumping 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.



Support Intel® vPro Windows Systems

Using Intel® Active Management Technology, privileged users can support fully provisioned Intel® vPro Windows systems below the OS level, regardless of the status or power state of these remote systems. To use Intel® vPro, you must have access to a Jumpoint with Intel® vPro enabled and must have the user account permission **Allowed Jump Methods: Intel® vPro**.

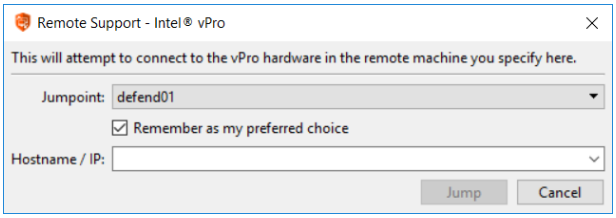
Note: *Remote systems using vPro with AMT version 5 or higher may be supported with BeyondTrust.*

Note: *While vPro is supported by clustered Jumpoints, configuration options are available only to standalone Jumpoints. Clustered Jumpoints have no configuration options for Intel® vPro.*

To start a session with an Intel® vPro system, open the **Intel® vPro** dialog from:

- The **Support** menu of the representative console
- The **Intel® vPro** button at the top of the representative console

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the system you wish to access.

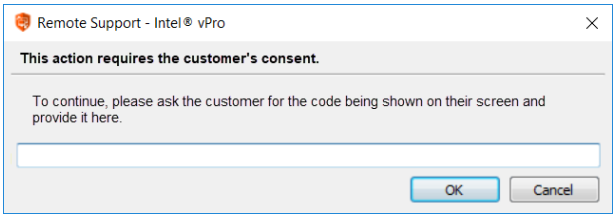


Click **Jump**.

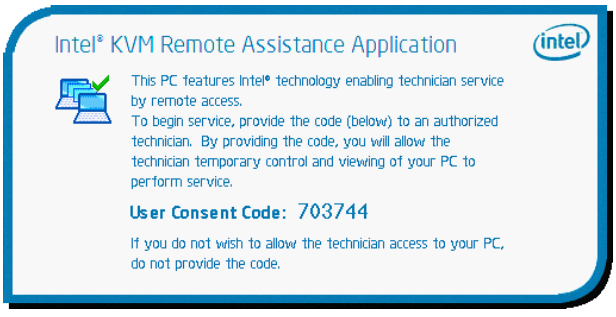
Depending on your Jumpoint setup, you may be prompted to enter a username and password.

The Jumpoint detects the provisioned vPro hardware. If the credentials, provided during either the Jumpoint configuration or the Jump attempt, match the credentials of the vPro-provisioned system, the connection is initiated.

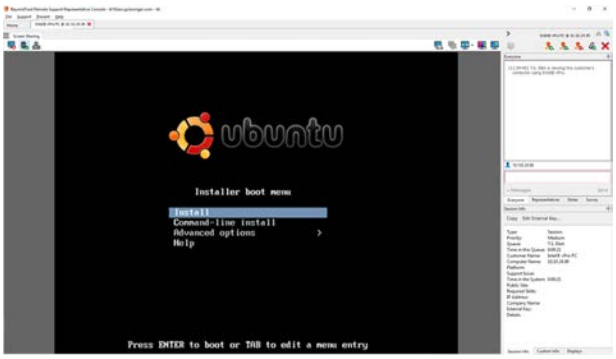
Depending on how the vPro computer is provisioned, you may be prompted to enter a user consent code before performing certain actions.



If a consent code is required, a pop-up appears on the remote screen. An end-user must provide you with this code before you can gain hardware access.



Once the connection is made, you have control of the remote vPro hardware. You can then use the vPro session tools to work on the remote system.

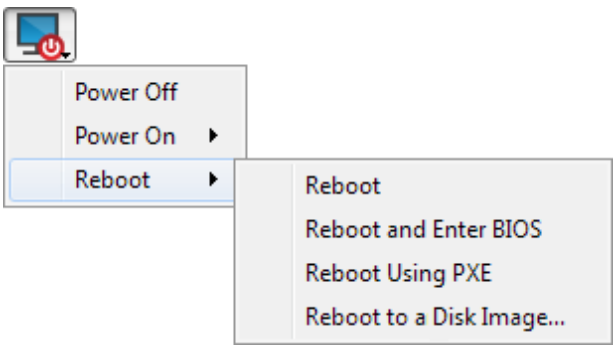


vPro Session Tools

	Reset the vPro connection.
	Power off or power on the host machine. You may also reboot the host machine normally, to BIOS, to PXE, or to a selected disk image.
	Select an ISO or IMG file to mount on the remote system. File location is set during Jumpoint configuration.
	Start or stop viewing the remote system's display using KVM.
	Send **Ctrl-Alt-Delete** to the remote computer.
	While screen sharing, capture a screenshot of the remote screen or screens at their full resolution, saved in PNG format. Save the image file to your local system or to your clipboard. The capture action is recorded in the chat log with a link to a locally saved image. The link remains active even after the customer has left the session, but it does not persist in the BeyondTrust session report. You can adjust the directory where screenshots are saved by going to the **File > Settings > Support Tools** menu in the representative console. This feature works on Mac, Windows, and Linux.
	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.

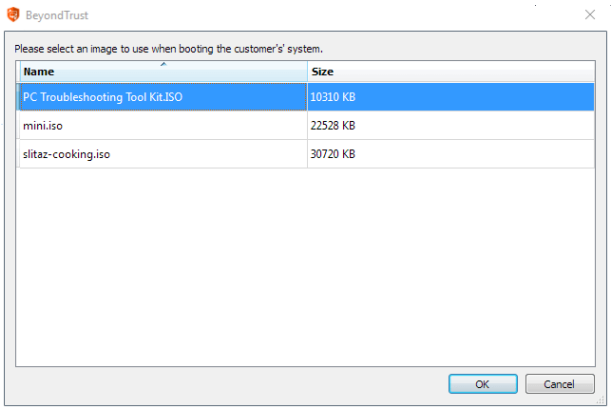
From the **Reboot** menu, select **Reboot and Enter BIOS** to start the BIOS boot process on the remote vPro system. You will then have access to the BIOS for troubleshooting purposes.

Select **Reboot Using PXE** to boot the remote system using a network interface independently of data storage devices or installed operating systems.



Reboot to a Disk Image uses IDE-R to boot the remote system to a specified ISO or IMG file.

Note that the remote system will display the screen exactly as you see it, even when booting to another image.

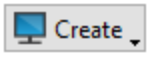


Create and Use Intel vPro Jump Shortcuts

Using Intel® Active Management Technology, privileged users can support fully provisioned Intel® vPro Windows systems below the OS level, regardless of the status or power state of these remote systems.

Create an Intel® vPro Shortcut

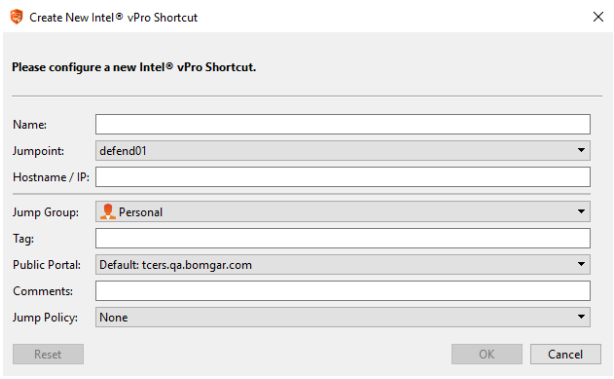
To create an Intel® vPro shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Intel® vPro**. Intel® vPro shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.



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 all the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*

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.

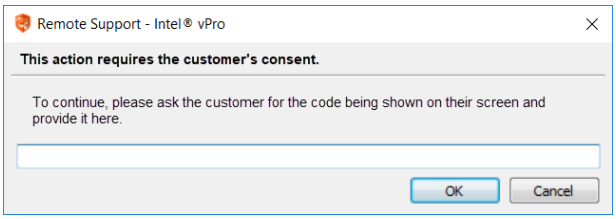
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Use an Intel® vPro Shortcut

Depending on your Jumpoint setup, you may be prompted to enter a username and password.

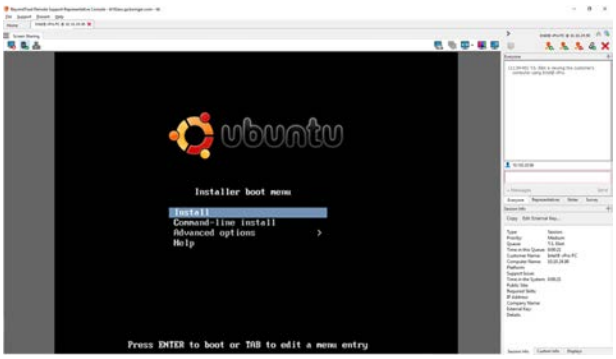
The Jumpoint detects the provisioned vPro hardware. If the credentials, provided during either the Jumpoint configuration or the Jump attempt, match the credentials of the vPro-provisioned system, the connection is initiated.

Depending on how the vPro computer is provisioned, you may be prompted to enter a user consent code before performing certain actions.



If a consent code is required, a pop-up appears on the remote screen. An end-user must provide you with this code before you can gain hardware access.

Once the connection is made, you have control of the remote vPro hardware. You can then use the vPro session tools to work on the remote system.

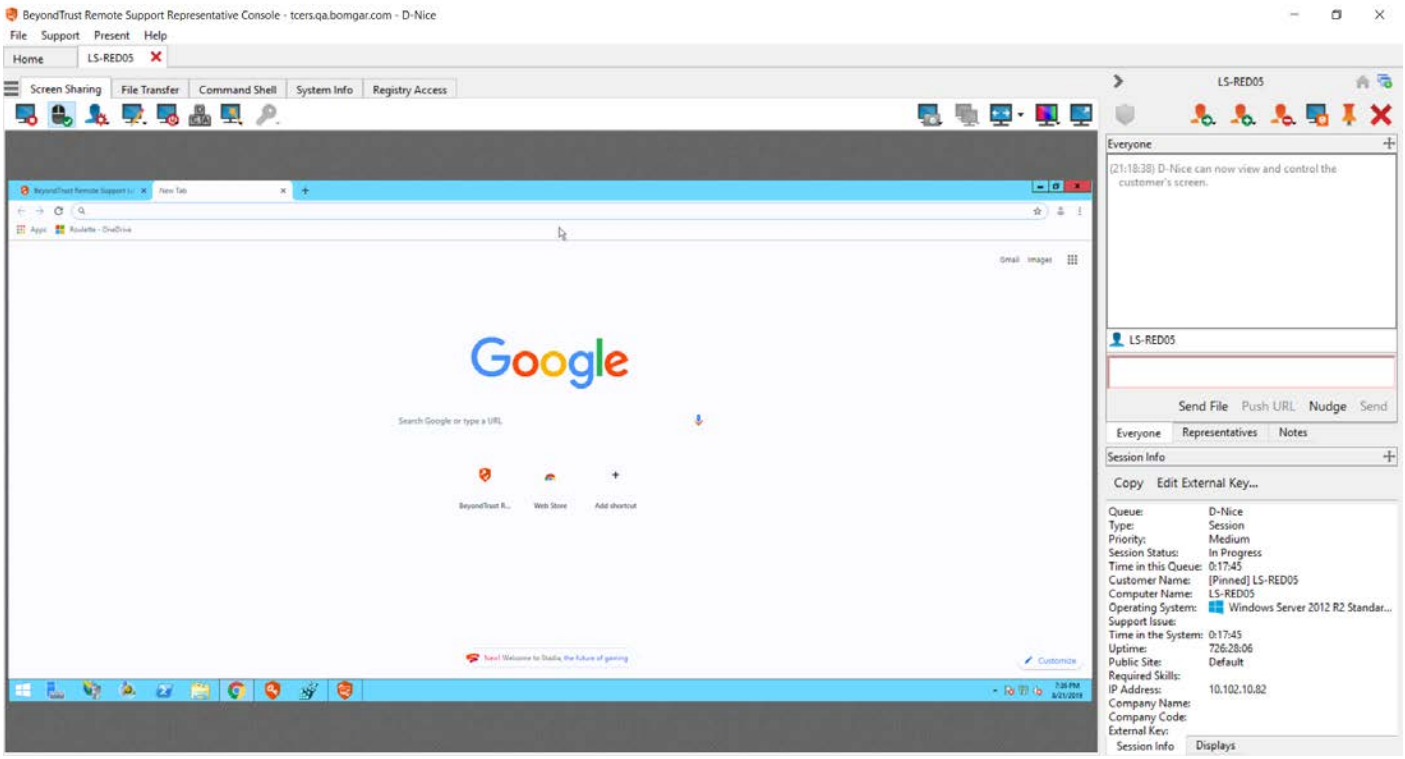


Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is 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.

Toolset

Support Session Overview and Tools



Session Tools

	Click the menu icon at the top left of the session window to open session controls for your session. You can also right-click the session tab to see session controls. Several of these controls have dedicated icons elsewhere in the interface and are described below (**Transfer**, **Invite**, **Remove Participant**, **Elevate**, **Deploy Support Button**, **Deploy Jump Client**, **Custom Links**, **Close**). From the menu, select **Detach Session Tab** to separate the session from the console, or click the session tab and drag it away from the main window. The menu icon remains with your session even if you detach the session tab, allowing you to position the session tab anywhere, such as on a separate monitor, and retain session tool access. Reattach the session using the **Attach Session Tab** selection in the menu, or simply by clicking the X to close the detached window. Additionally, from the menu, select **Locate Sidebar** to find the sidebar for the session, which can be helpful if you have several detached session sidebars (see below) scattered on your screen. You can also rename the session or revert the name to the default.
	Collapse the sidebar to maximize your session workspace. To pin the sidebar again, hover over the collapsed sidebar arrow and click the **Pin Sidebar** icon.
 	Click this icon to detach the sidebar. Once detached, the sidebar can be positioned anywhere on your desktop or placed on a separate monitor. The sidebar also can be resized according to your needs, or resize the panes in the sidebar for more viewing space. Click on the **Attach Sidebar** icon to reattach the sidebar. When the sidebar is detached, the **Home** icon is enabled (see below).
	This **Home** icon is enabled whenever the sidebar is detached. In the case where you might have several sessions going on at the same time and several detached sidebars on your screen, clicking on a sidebar's **Home** icon brings up the associated session, saving time and avoiding confusion when trying to identify which sidebar goes with which session.
 	It is possible to reposition the different widget sections displayed on the sidebar, like the chat window, the session info pane, etc. When hovering over the title bar of a section, the cursor turns into a closed hand, allowing you to drag and reposition that section on the sidebar.
 	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** to supply an administrative username and password, yourself. 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 or an external user. You can also request an access sponsor to perform certain actions on your behalf.
	The session owner can remove another user from a shared session. Additionally, you can disconnect the customer but remain in the session tab to add notes or review the last captured system information.
 	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. To set details, including password, comments, group, and so forth, select **Customize**.
	Open a web browser on your computer to any sites defined by your administrator. This button can be configured to include detailed information about the session, the end customer, and/or the BeyondTrust user who is opening the custom link. If, for instance, the external key matches the unique identifier of a case in your customer relationship management system, clicking this button could pull up the associated case in the external system.
	When a compatible iOS device is detected, the **Special Actions** icon appears, allowing the representative to push iOS screen sharing instructions to the device. For more information about 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.
	Close your session tab entirely. If you have ownership of the session, you can either uninstall the customer client from the remote machine or leave the customer in queue for another representative to resume the session. You can close the session from the sidebar, the session menu, or the session tab.

At the bottom right of the session window is information about the remote system along with any other information the customer may have provided in the issue submission form. This can include the following:

- **Type**: The session type.
- **Priority**: The priority level (Low, Medium (default), or High) of the request, depending on the support issues defined by your BeyondTrust administrator.
- **Queue**: The Personal queue of the representative who owns the session.
- **Session Status**: Waiting (no rep has joined), In Progress (rep and customer have joined), or Customer Absent (rep has joined but customer has left).
- **Customer Name**: This is either the name entered by the customer when starting the session, the username of the logged-in user, the hostname of the customer machine (for pushed and pinned sessions), or service (for elevated sessions).
- **Computer Name**: The hostname of the customer's machine as reported in System Settings.
- **Platform**: The operating system of the customer's machine
- **Support Issue**: If an issue was selected, this reports the name of the issue the customer selected.
- **Time in the System**: This tracks the amount of time from the moment the session entered its first queue.
- **Public Site**: Typically, this is listed as Default; however, if non-default sites are present, other sites may be available.
- **Required Skills**: Skills associated with the specific issue selected by the customer. Skills are created and associated with issues by the BeyondTrust administrator from the BeyondTrust /login interface.
- **IP Address**: The public and/or private IP address of the customer's local system.

If your administrator has enabled the XML API, you may designate an external key for use in session reports. Any custom session attributes enabled by your administrator will appear in a **Custom Info** tab. Click **Copy** to copy all information to your clipboard.

Another option that your administrator may choose to enable is the ability to log out the Windows user automatically or lock the remote computer when the session closes. When you have been working on an unattended system, for example, locking the computer is recommended to prevent unauthorized users from viewing private information. Set the action to take from the dropdown at the bottom of the pane.

Log Into Remote Systems Using Credential Injection from the Representative Console

When accessing a Windows-based Jump Item in the Representative Console, you can use credentials from a credential store to log into the endpoint or to run applications as an admin.

Before using credential injection, make sure that you have a credential store or password vault available to connect to BeyondTrust Remote Support.

Install and Configure the Endpoint Credential Manager

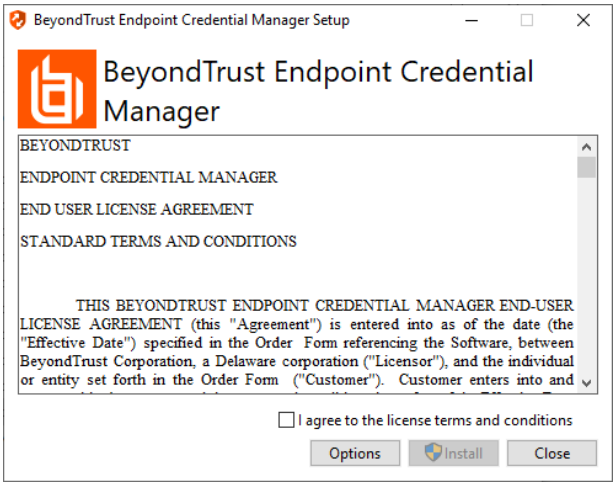
Before you can begin accessing Jump Items using credential injection, you must download, install, and configure the BeyondTrust Endpoint Credential Manager (ECM). The BeyondTrust ECM allows you to quickly configure your connection to a credential store, such as a password vault.

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

System Requirements

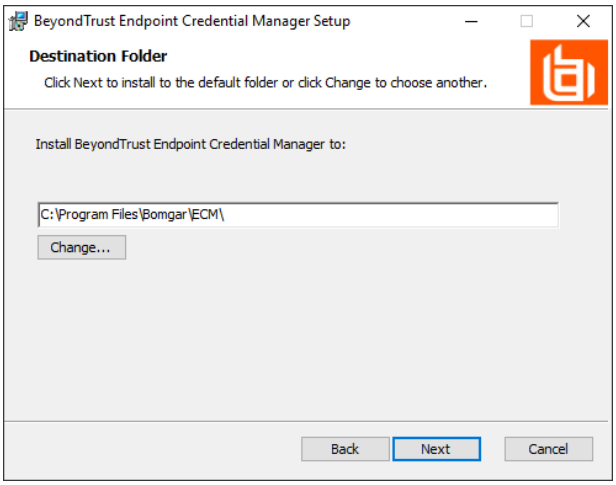
- **Windows Vista or newer, 64-bit only**
- **.NET 4.5 or newer**

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. Mark the checkbox if you agree, and click **Install**. If you wish to modify the installation path, click the **Options** button to customize the installation location.

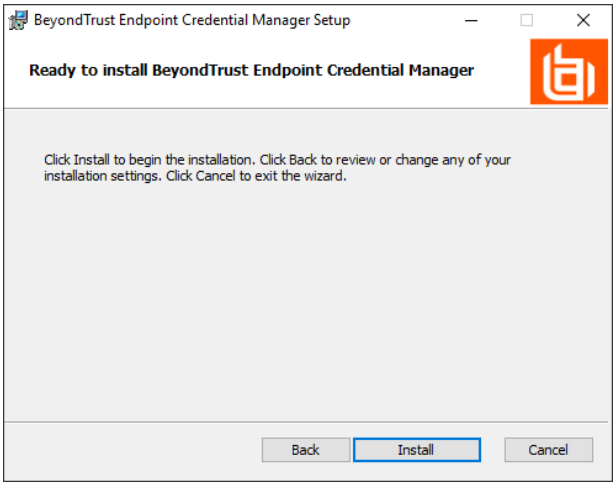


> ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*

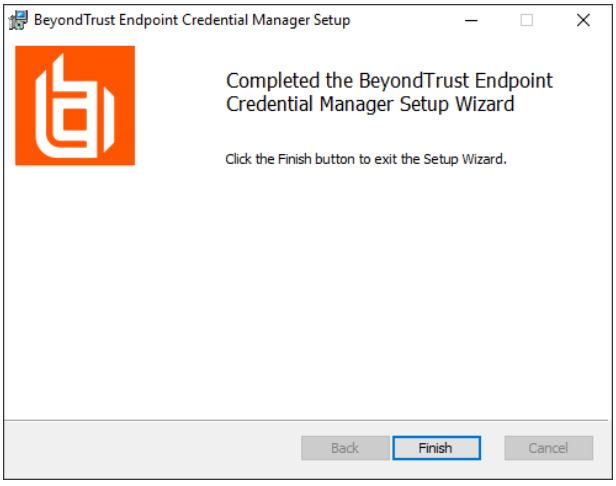
3. Choose a location for the Credential Manager and click **Next**.
4. On the next screen, you can begin the installation or review any previous step.



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



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



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

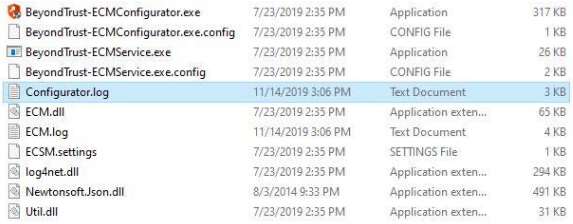
> ***Note:*** *When multiple ECMs are connected to a BeyondTrust site, the Secure Remote Access Appliance routes requests to the ECM that has been connected to the appliance the longest.*

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

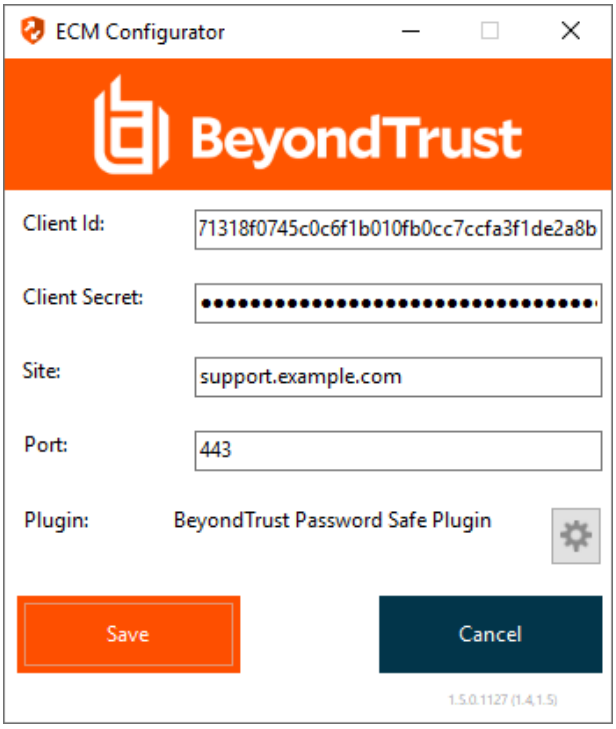
Configure a Connection to Your Credential Store

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

1. Locate the BeyondTrust ECM Configurator you just installed using the Windows Search entry field or by viewing your **Start** menu programs list.
2. Run the program to begin establishing a connection.



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



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!

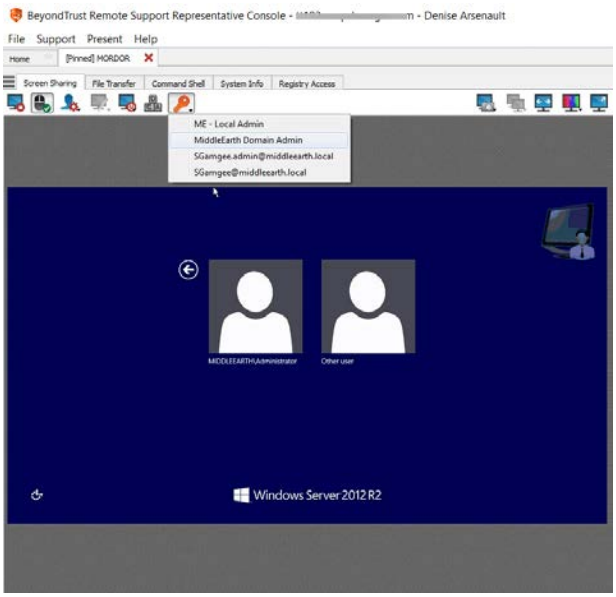
To apply new settings in the configuration, restart the ECM service.

Use Credential Injection to Access Remote Systems

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

1. Log into the representative 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.



Choose from Favorite Credentials for Injection

After a representative has used a set of credentials to log into an endpoint, the system stores the user's preferred credentials for the endpoint and the context in which they were used (to login, to perform a special action, to elevate, or to push) in the appliance database. The next time the user wants to use credentials to access the same endpoint, the credential injection menu makes a recommendation for which credentials to use. The credentials are displayed at the top of the credentials list, followed by any remaining credentials. If no credential history exists for an endpoint, the appliance simply displays all the possible credentials.

No more than 5 credentials are recommended to the representative in the credentials list.

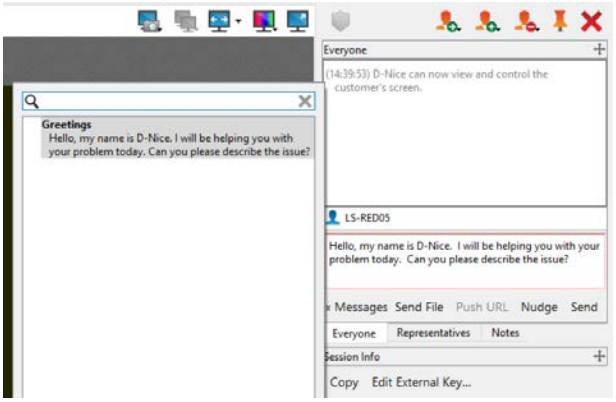
> ***Note:*** *When using BeyondTrust Vault, the maximum number of credentials that can display in the dropdown menu is 2,000. When using the ECM, the limit is 200.*

Chat with the Customer During a Session

Throughout the support session, you can chat with your remote customer. You do not need to have screen sharing permissions before beginning chat. If enabled in the representative console settings, you receive pop-up notifications when chat messages are received. If you have uploaded your photo or any avatar image, it displays on the customer's chat window once the chat begins.

Click the arrow icon at the top left of the sidebar to collapse the sliding sidebar. If the sidebar is collapsed, hover over the arrow by the hidden window to reveal it. Click the pin icon that replaced the arrow icon at the top left of the sidebar to re-pin the sliding sidebar.

When typing in English, misspelled words will be underlined in red. Right-click to view spelling suggestions or to ignore that spelling for the current console login.



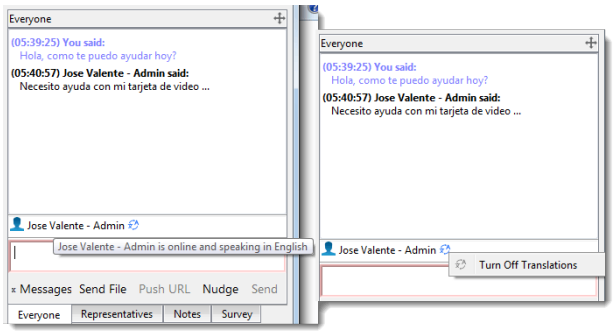
If real-time chat translation is enabled, customers can chat with a representative in their own language. As an example, a customer whose main language is English could chat with a representative who speaks only Dutch, with the chat traffic being automatically translated in real time.

For more information on real-time chat translation, please see Real-time Chat Translation at https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm.

For more information on configuring real-time chat translation, please see Real-Time Chat: Translate Chat Messages Between Rep and Customer at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm.

Hovering the mouse pointer over the representative's name shows which language is being used to translate the messages sent to the customer. In the example shown, the representative is shown as "online and speaking in English", even though the representative is typing in Spanish.

You can turn off translations by right-clicking on the translation icon and then clicking **Turn Off Translations**. To turn translations back on, right click the icon and click **Turn Translations On**. It is not possible for the customer to turn the translation process off from their side.



If your administrator has configured canned messages, you can click on the **Messages** button at the lower left of the chat input area to insert previously written messages into the chat. Click the arrow to the left of a category name to see its messages and subcategories. Type in the search box to find a specific message.

Messages appear as plain text in the chat input area. You can add or edit BBCode tags within a message to add text formatting. Formatting will be applied once the message has been sent.

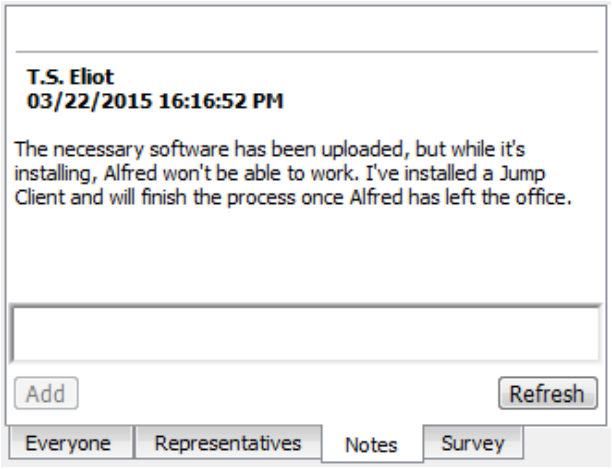
To push a file through the chat interface, click the **Send File** button. Pushing a URL through the chat interface will automatically open a browser on the remote system and direct it to the designated site. In order to push a URL, the web address must be the only text in the field.

To attract the attention of your customer, click **Nudge**. This gives focus to the customer client, jiggles the customer client, and plays an audible alert on the remote system. The nudge is logged in the chat history. After sending a nudge, you must wait several seconds before you can send another nudge.

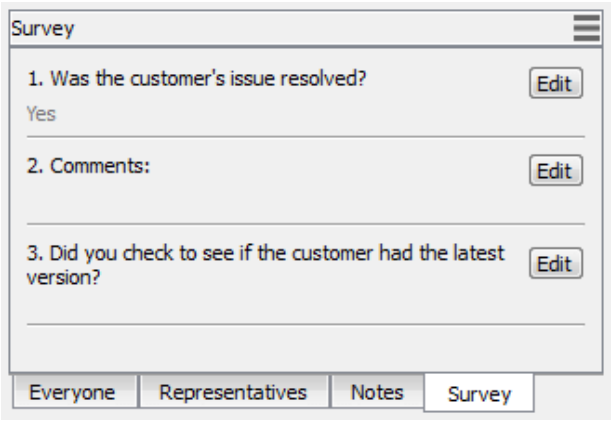
The chat window records not only the messages and the time they were sent; it also serves as a running log of everything that happens throughout the session, including files transferred and permissions granted.

If one or more representatives are sharing the session, you can choose to chat with all participants or to chat privately with only the other representatives. When an additional user joins a shared session, they are able to see the entire chat history.

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



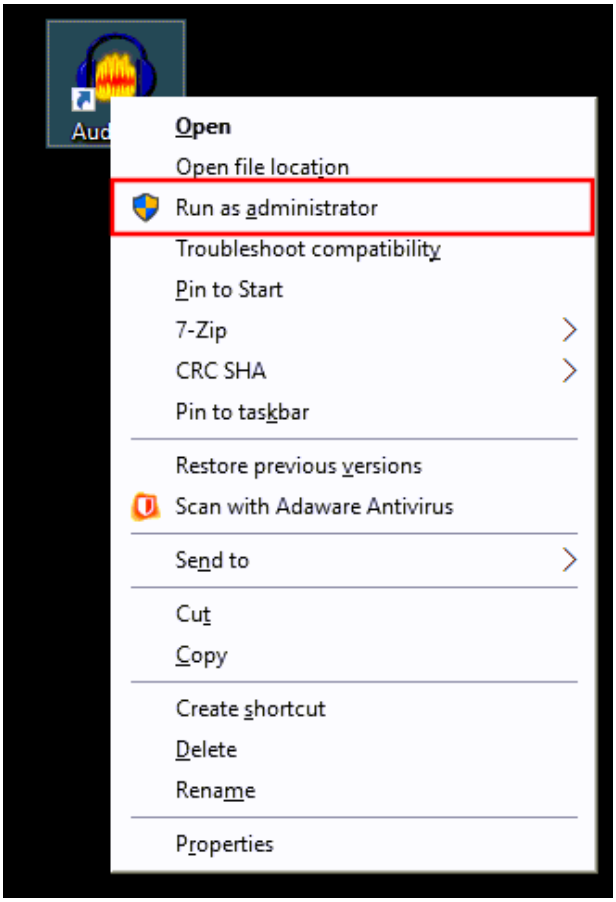
Your administrator may also choose to allow you access to the representative survey during a session. In this scenario, the survey can be used as a workflow template, allowing your administrator to push a series of questions and/or check mark points, as well as specific links you may use in your support session.



> ***Note:*** *It is possible to reposition the different widget sections displayed on the sidebar, like the chat window, the session info pane, etc. When hovering over the title bar of a section, the cursor turns into a closed hand, allowing you to drag and reposition that section on the sidebar.*

Manual vs Automatic Elevation

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. Once you have elevated a session, you can log out of the existing user and back in with an administrative account, or use **Run as administrator** to run commands or programs within the admin user context.

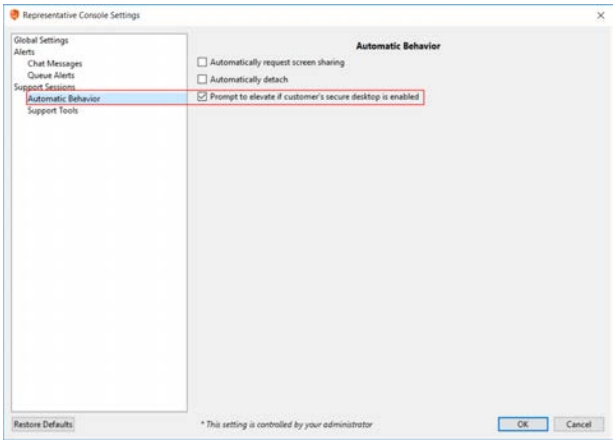


Manual Elevation

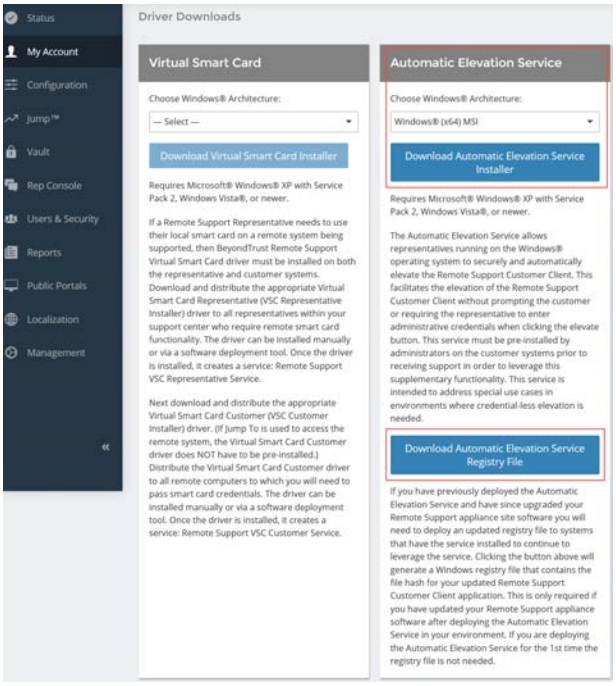
To elevate the customer client to have administrative privileges, click the **Elevate** button at the top of the session window.

A prompt for administrative credentials appears. A prompt to elevate will also appear if the representative attempts to perform an action which requires administrative rights in an unelevated session.

You may also configure settings in the representative console so that the user at the remote device is automatically prompted if their secure desktop is enabled. This setting can be found by navigating to **File > Settings > Support Sessions > Automatic Behavior**. This setting can also be globally configured in the /login interface on the **Rep Console > Rep Console Settings** page under **Manage Rep Console Settings**.



Automatic Elevation



In special cases, you may need a session to start with the customer client already in elevated mode, or you may need to elevate the customer client without providing credentials. To securely elevate the customer client without the prompt, download the **Automatic Elevation Service** from **/login > My Account** and install it beforehand on the remote Windows systems to which you need credential-less elevation access. You must install the elevation service using an account that has administrative privileges to the local machine.

When the elevation service runs, it adds to the registry a hash unique to your BeyondTrust site. Then, when the remote system begins a session through that site, the elevation service matches the registry hash against the hash in the client. If they match, the client attempts automatic elevation.

Elevation occurs following the rules set in **/login > Public Portals > Customer Client > Other Options**. If the rules set for the customer client do not allow it to elevate automatically, a matching hash will still make the elevation service the means for elevation when the representative clicks the **Elevate** button in the representative console. When the elevation service is used, neither the representative nor the customer is prompted for credentials.

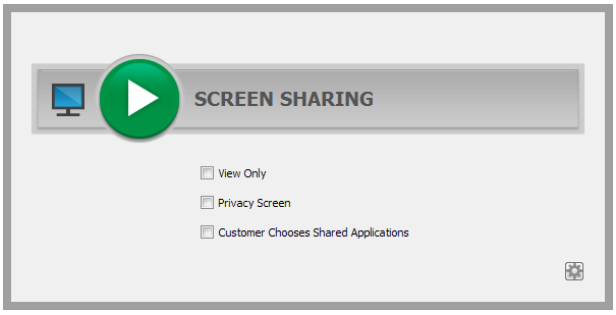
After a BeyondTrust software update, your site hash changes. Download and run the elevation service registry file to update the registry hash on systems which already have the elevation service installed. You must run the elevation service registry file using an account that has administrative privileges to the local machine.

For more information on elevation, please see the following articles:

- Elevate the Session in the Web Rep Console
- Elevate Rights in the Customer Client from the Android Representative Console
- Elevate Rights in the Customer Client from the iOS Representative Console
- Install a Jump Client, Jumpoint, or Elevation Service for Elevated Session Start

Screen Share with the Remote Customer for View and Control

From the session window, click the **Screen Sharing** button to request control of the remote computer. Options may be available below the button depending on your account settings. Click the gear button to view options.



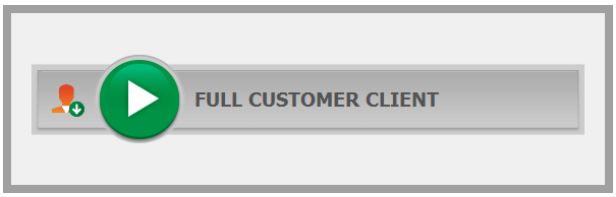
Screen Sharing Options

- Leaving all options unchecked requests full screen sharing, which grants view and control of the remote system's entire desktop and all applications.
- If you check **Full Access**, available only in a customer-initiated session, you will request both screen sharing and all other privileges at once.
- If you check **View Only**, you may see but not control the remote screen.
- **Privacy Screen**, available only when Jumping, starts the session with the remote customer's view and control of the system disabled. Privacy screen is not available when supporting Windows 8.
- **Customer Chooses Shared Applications**, available only when supporting a Windows or Mac computer, allows the customer to limit which applications to share.

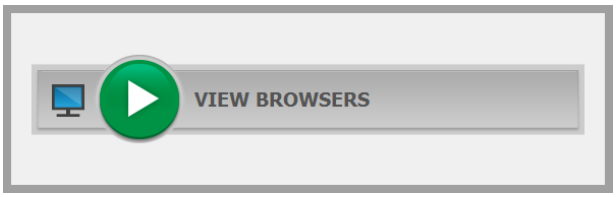
If your administrator has set your account to require that the customer select which applications to share, you will only be allowed to request limited screen sharing. Alternatively, you may only be allowed to request full screen sharing, or you may be allowed to choose which level of access to request. Note that a site-wide setting may allow your customer to limit applications after beginning screen sharing, regardless of the level of access requested.

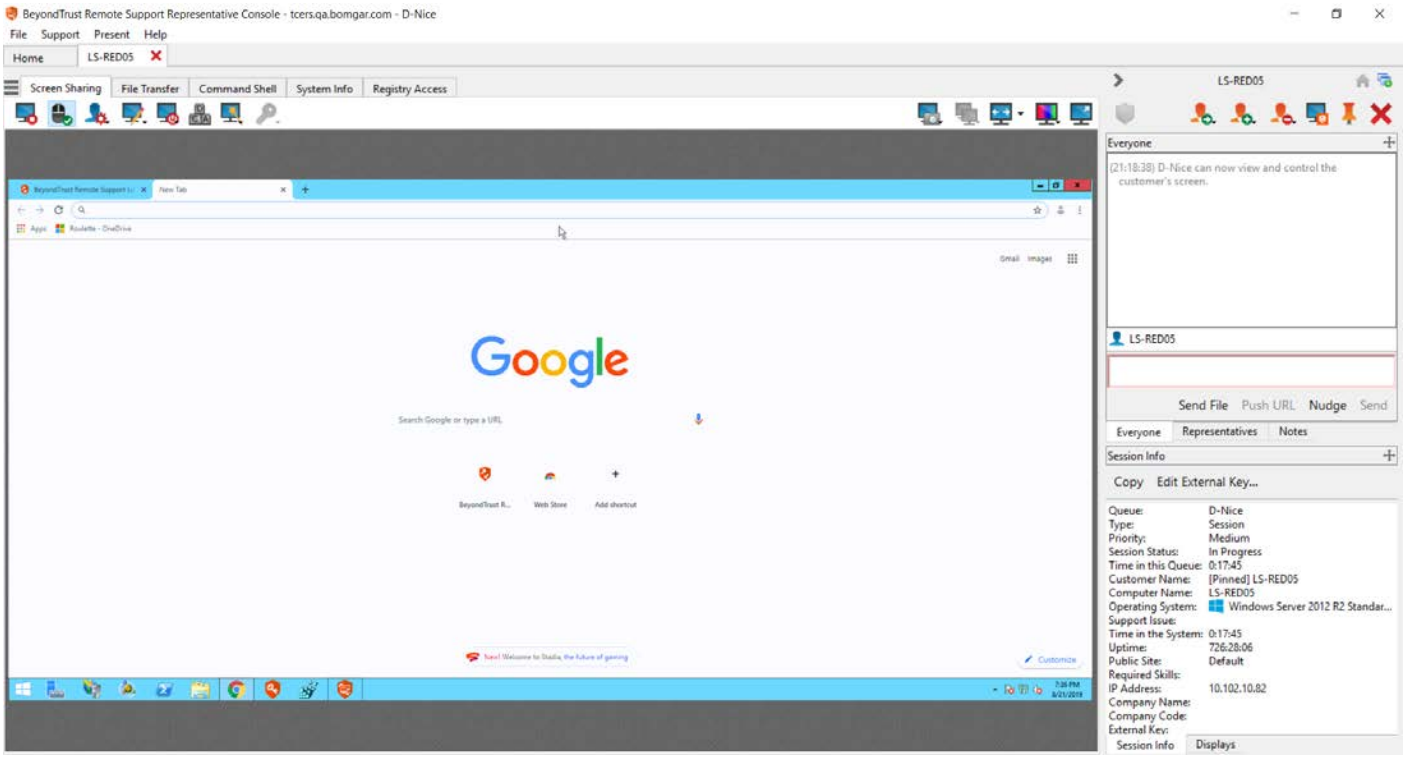
Once the customer has granted permission, the enabled applications of the remote desktop will appear in your window. Your customer can choose to grant you view-only access or, if your permissions allow, full mouse and keyboard control, enabling you to work on the remote computer as if you were really there. You can request to elevate your permission level at any time during the session.

In a click-to-chat session, you can only chat with the customer and see basic session information. If you need to provide deeper support, request to elevate the session to the full customer client.



For browser sharing sessions, screen sharing is available only in limited mode, as only the remote browsers can be viewed. Representatives can still use Annotations to draw on the customer's screen and use the virtual pointer. With browser sharing, the **File Transfer**, **Command Shell**, and **System Info** tabs are not available. If screen sharing recording is enabled, browser sharing sessions are recorded.





Screen Sharing Tools

	Stop screen sharing.
	While viewing the remote computer, start or stop control of the remote keyboard and mouse.
	If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The customer's view of the privacy screen clearly explains that the representative has disabled the customer's view. The customer can regain control at any time by pressing **Ctrl+Alt+Del**. 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.
	Annotation tools enable you to guide customers through more complex tasks and to train remote employees, reducing the number of call-backs and lowering training costs. A number of tools are available, including shapes and free drawing. BeyondTrust InSight allows annotations on the a live camera feed from an Android or iOS device. Note that annotations have special requirements for certain mobile platforms. To learn more about BeyondTrust InSight, please see BeyondTrust InSight for iOS or BeyondTrust InSight for Android.
	Reboot the remote system in either normal or safe mode with networking, or shut down the remote system. You can also request the end user to enter valid credentials so that after a reboot the representative can log back on with the provided credentials without requiring the customer to be present. For further details, see "Automatic Log On Credentials: Reboot and Reconnect" on page 119.
	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.
	Access a dropdown of available smart card readers on your local system. Use the virtual smart card to perform administrative actions, running programs in another user context or even logging in as another user. To use smart card credentials on a remote system, you must start the session using an elevated Jump Client, a Jumpoint, a local network Jump, or the BeyondTrust automatic elevation service. The appropriate virtual smart card drivers must be installed on both your local system and the remote system, with their services running.
	Begin iOS device screen sharing. For details, see Supporting Apple iOS Devices at www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios. When supporting an Apple OS X 10.10+ system attached to an Apple iOS 8.0.1+ mobile device, click this button to begin or end view-only screen sharing on the attached iOS device. Note that this button is not visible unless you are in a standard screen sharing support session with an Apple OS X Yosemite system, and that the button is not enabled unless an Apple iOS 8.0.1+ device is connected to the OS X Yosemite system being supported.

	While screen sharing, capture a screenshot of the remote screen or screens at their full resolution, saved in PNG format. Save the image file to your local system or to your clipboard. The capture action is recorded in the chat log with a link to a locally saved image. The link remains active even after the customer has left the session, but it does not persist in the BeyondTrust session report. You can adjust the directory where screenshots are saved by going to the **File > Settings > Support Tools** menu in the representative console. This feature works on Mac, Windows, and Linux.
	Manually send the contents of your clipboard to the remote computer. This tool icon is not visible if you are permitted to automatically send the contents of your clipboard or if you are disallowed to send clipboard information to the remote system.
	Manually receive the contents of your clipboard from the remote computer. This tool icon is not visible if you are permitted to automatically receive the contents of your clipboard or if you are disallwoed to receive clipboard information from the remote system.
	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.

Use Annotations to Draw on the Remote Screen

Use annotation tools to guide customers through complex tasks and to train remote employees, reducing the number of call-backs and lowering training costs. Representatives are offered an interactive way of dealing with customers, reducing potentially frustrating situations and increasing customer satisfaction.

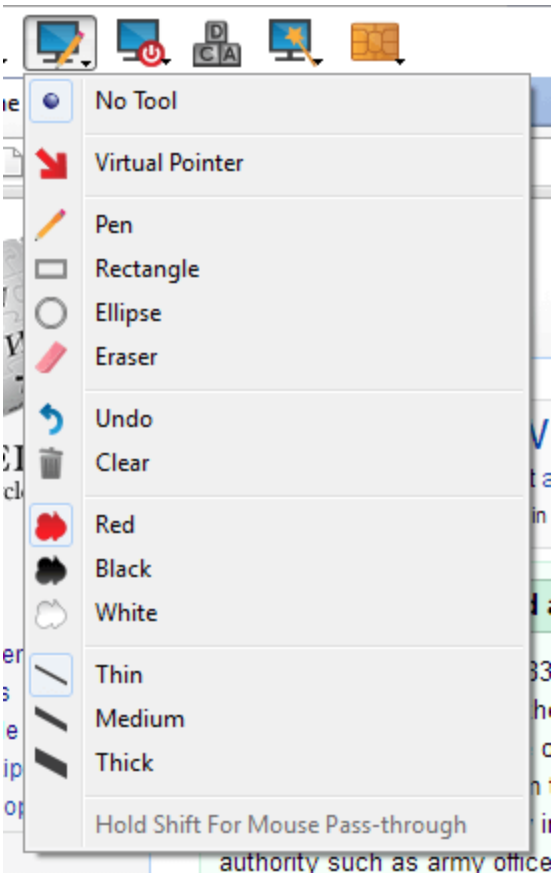
While in annotation mode you can still use your mouse to move or control items on the remote desktop. Holding down the **Shift** key temporarily suspends annotation mode.

Enabling Annotations

To start using **Annotations**, click on its icon.

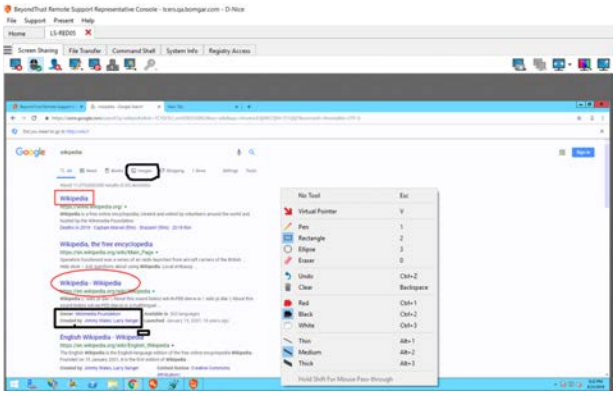
Clicking on any of the dropdown menu items turns the **Annotations** mode on. You can select from a number of tools to help you guide a customer through a series of steps, or to enhance a training session. The following tools and functions are available:

- Virtual Pointer
- Pen
- Rectangle drawing tool
- Ellipse drawing tool
- Eraser
- Undo
- Clear
- Red, Black, or White colors
- Thin, Medium, or Thick line



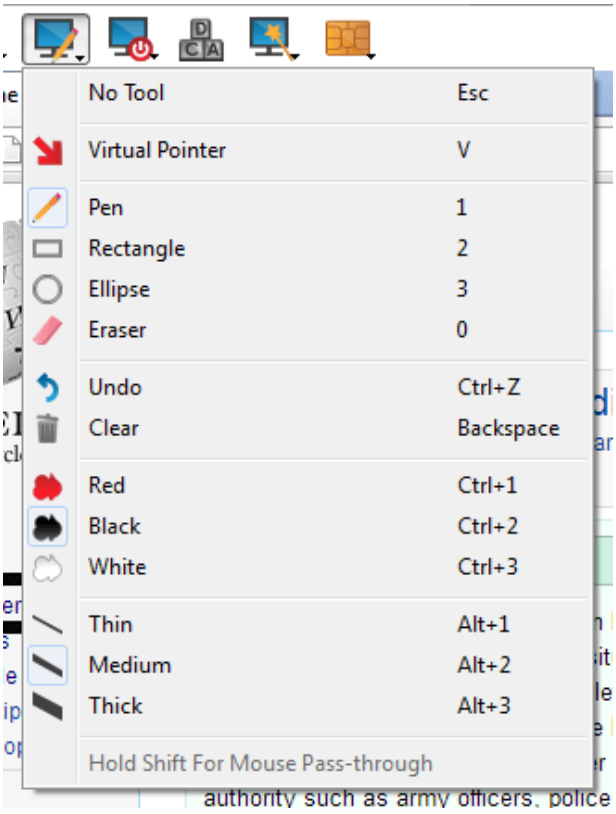
You can select your tool from the **Annotations** dropdown menu or by right-clicking inside the remote screen area. If you click on the areas outside of the remote screen, the dropdown menu does not display.

Annotations appear on the remote screen to draw attention to specific points of interest or highlight areas as needed.



To turn off **Annotations**, select **No Tool** from the dropdown menu, or click **Esc.**

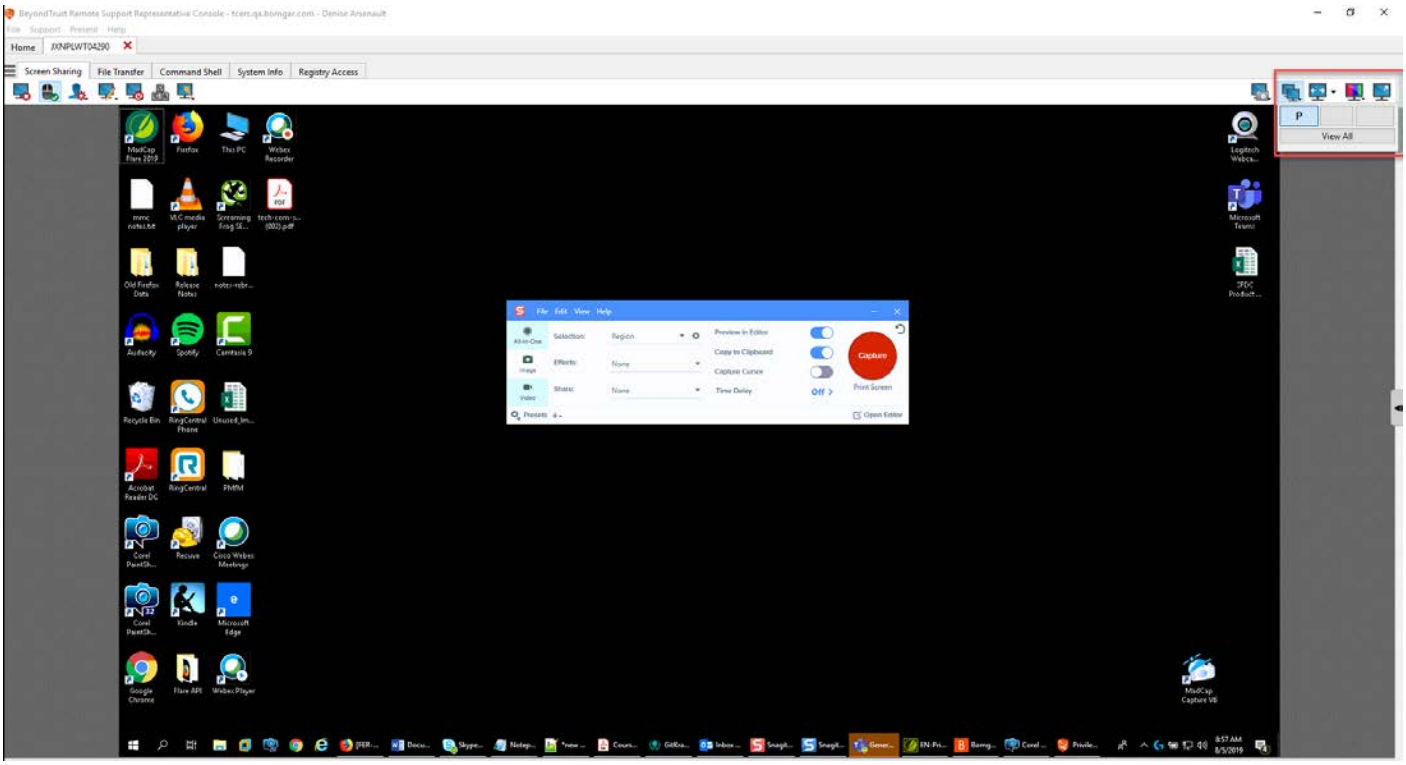
All annotations are deleted from the customer's screen when the session terminates.



Annotations are also available during presentations. For more information, please see "Give a Presentation to Remote Attendees" on page 90.

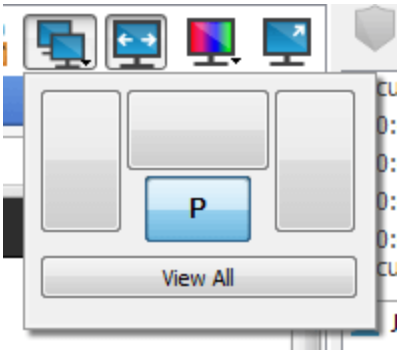
View Multiple Monitors on the Remote System

BeyondTrust supports remote desktops configured to use multiple monitors. When you first connect to a remote desktop, you will see the primary monitor in the **Screen Sharing** tab. If additional monitors are configured, a **Display** icon will appear active in the **Screen Sharing** toolbar, and a **Displays** tab will appear in the bottom right corner of the console.



Using the Display Icon

Select the **Display** icon to see all the displays attached to the remote computer. In this view, the remote monitors are represented by rectangles rather than thumbnail images. The position of each rectangle corresponds to the position configured for each monitor on the remote desktop.



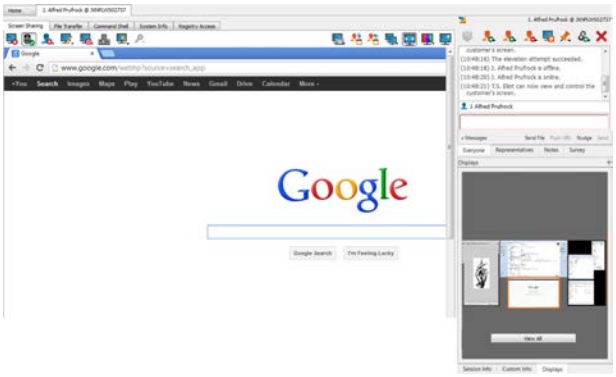
The primary monitor appears in the **Screen Sharing** window by default. To change your view, click on the rectangle that represents the monitor you wish to see. You can also select **View All** to show all the displays attached to the remote computer in the **Screen Sharing** window.

If the remote computer has no additional monitors attached, the **Display** icon will be inactive.

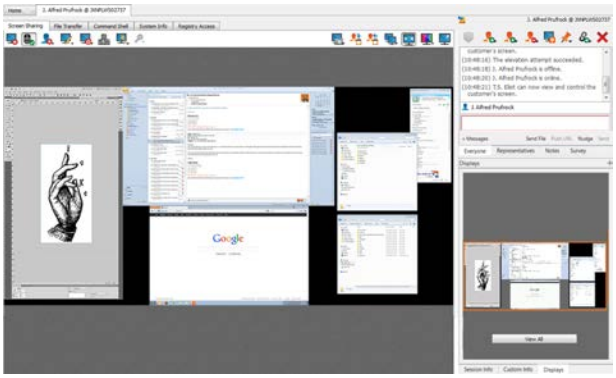
Using the Displays Tab

Select the **Displays** tab to see thumbnail images of all the displays attached to the remote computer. The position of each thumbnail image corresponds to the position configured for each display on the remote desktop.

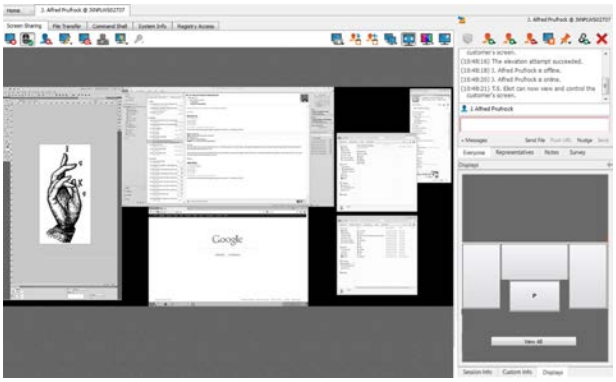
The monitor currently displayed in the **Screen Sharing** tab will be highlighted.



The primary monitor appears in the **Screen Sharing** window by default. To change your view, click on the thumbnail of the monitor you wish to see. You can also select **View All** to show all the displays attached to the remote computer in the **Screen Sharing** window.



If the session is in grayscale mode, the remote monitors are represented by rectangles rather than thumbnail images. The position of each rectangle corresponds to the position configured for each monitor on the remote desktop.



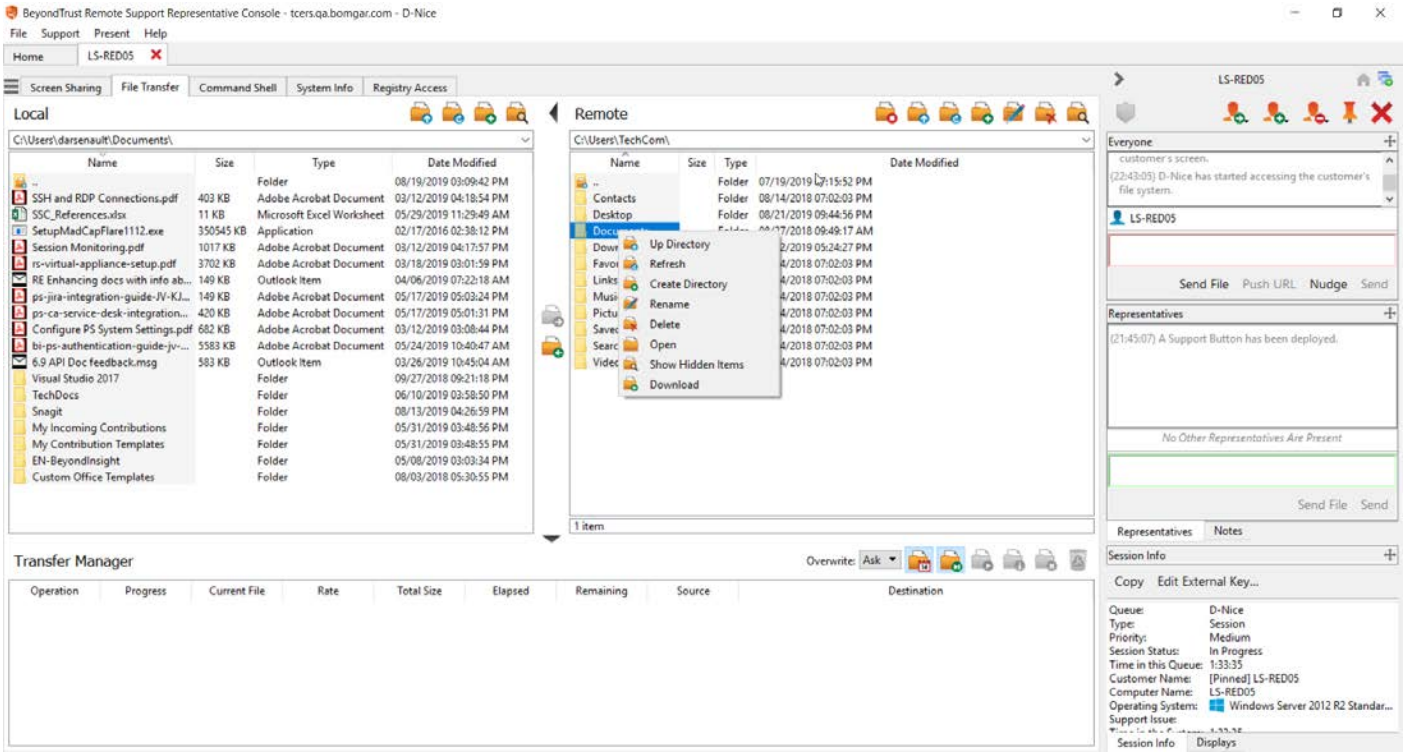
> ***Note:*** *The refresh cycle of the thumbnail image is about three seconds in ideal conditions but can lag depending on connection speed and data transfer.*

File Transfer to and from the Remote System

During a session, privileged users can transfer, delete or rename files and even entire directories both to and from the remote computer, or from the remote device and to or from the device SD card. You do not have to have full control of the remote computer in order to transfer files.

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

Transfer files by using the upload and download buttons or by dragging and dropping files. Right clicking on a file brings up a context sensitive menu from where you can, among other things, create a new directory; rename, open, or delete the file; or download it directly to your machine.



File Transfer Tools

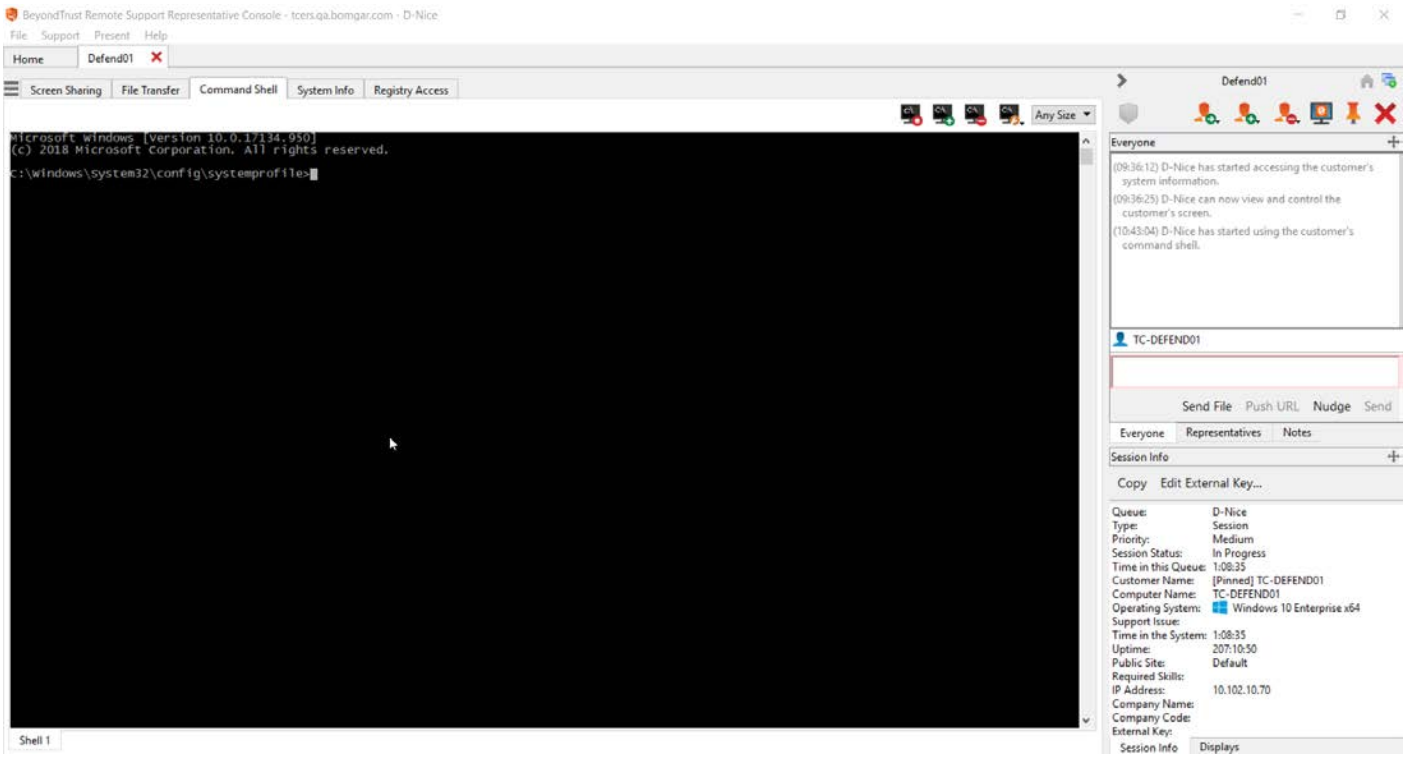
	Stop access to the remote device's file system when it is no longer needed.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Create a new directory.
	Rename a directory or file.
	Delete a directory or file. Note that deleting a file or folder permanently deletes it. It is not sent to the recycle bin.
	Show hidden files.
 	Select one or more files or directories and then click the appropriate button to upload the files to the remote system or download to your local system. You can also drag and drop files to transfer.
	If a file of the same name already exists in the location to which you are attempting to transfer a file, choose whether to respond by automatically overwriting the existing file, canceling the transfer, or prompting for each file of identical name. Note that if the content of the files is identical, the upload will be skipped and will result in a warning message.
	Preserving file information will keep the file's original timestamp. If this option is disabled, the file's timestamp will reflect the date and time when it was transferred.
	If automatic file transfer is enabled, transfers will begin as soon as the upload or download button is clicked or a file is dragged from one file system to the other.
	If automatic file transfer is not enabled, select from the transfer manager the files you wish to transfer and then click the **Start** button to begin the transfer.
	From the transfer manager, select a file and then click the **Details** button to view information such as the date and time of the transfer, the origin and destination of the files, and the number of bytes transferred.
	Select one or more files from the transfer manager and then click **Cancel** to stop the transfer from completing.
	Clear all information from the transfer manager.

Access the Remote Command Shell

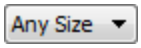
Remote command shell enables a privileged user to open a virtual command line interface to the remote computer. The user can then type locally but have the commands executed on the remote computer. You can work from multiple shells. Note that scripts available to the user may also be executed on the remote computer from the screen sharing interface.

Your administrator can also enable remote shell recording so that a video of each shell can be later viewed from the session report.

> ***Note:*** *Localization is limited to 1-byte characters for this feature. The use of 2-byte characters (certain language packs) may change expected behavior of some features.*



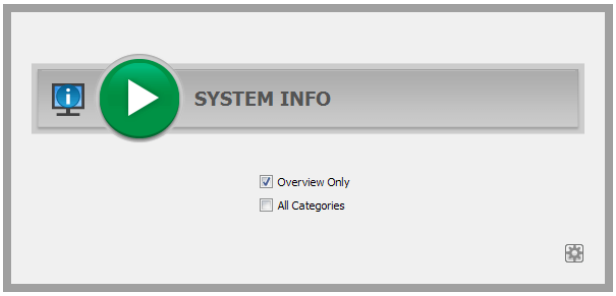
Command Shell Tools

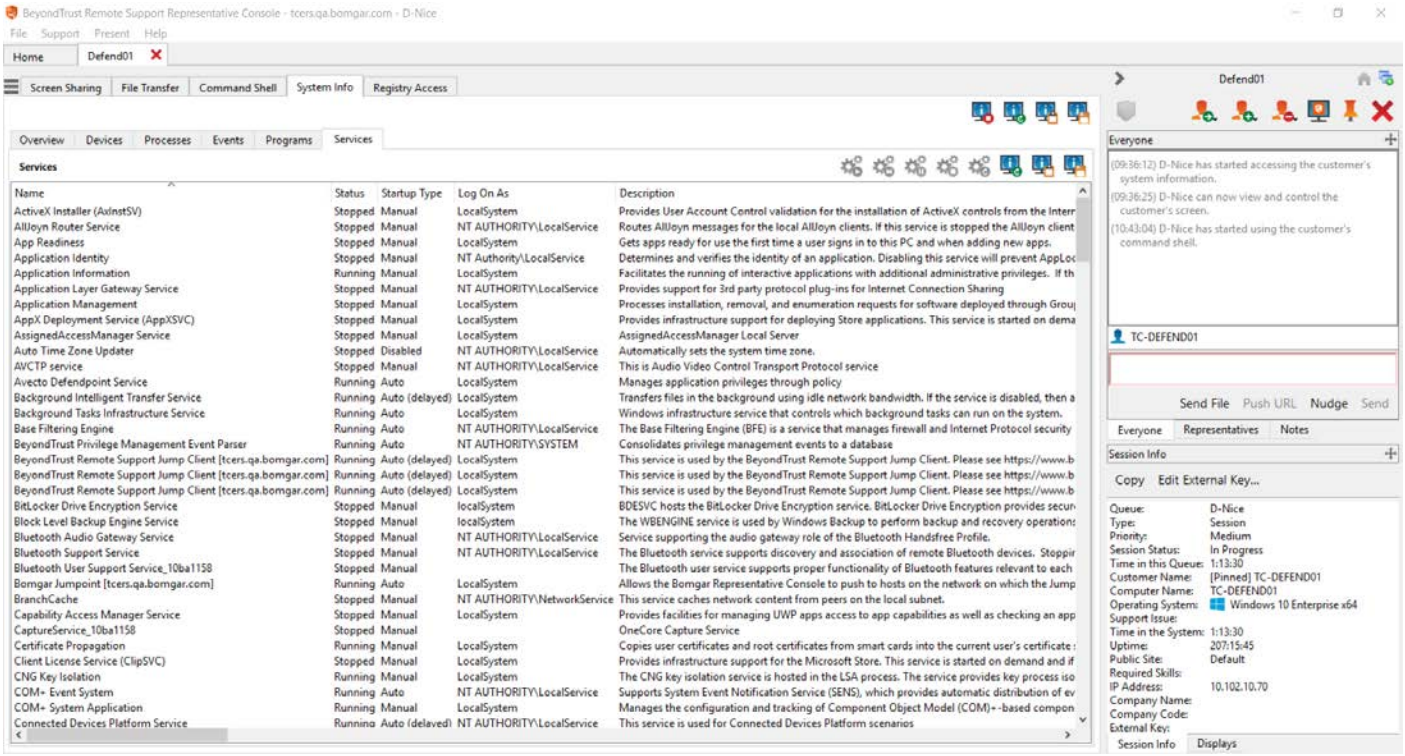
	Stop command prompt access when it is no longer needed.
 	Open a new shell to run multiple instances of command prompt, or close individual shells without relinquishing command prompt access. Shells are tabulated at the bottom of the screen.
	If permitted, access a dropdown of previously written scripts. When you select a script to run, you will see a prompt with a brief description of the script. When you click **Yes**, the script will run in the active command shell.
	Access tools to use within the command prompt. Paste the contents of your clipboard either by selecting it from the menu or simply by right-clicking in the terminal window. Copy a log of the current shell to your clipboard or save it to your computer. To copy a portion of the text, simply select it. Clear any lines not currently in sight, or clear all content from the terminal. Tools can also be accessed by pressing Ctrl+right-click within the terminal window.
	Select the size at which to view the display. Choose from 80x50, 80x25, or any size.

View Remote System Information

Privileged users may view a complete snapshot of the remote device's or computer's system information to reduce the time needed to diagnose and resolve the issue. The system information available varies depending on the remote operating system and configuration. Users with appropriate permissions may also kill processes; may start, stop, pause, resume, and restart services; and may uninstall programs.

Because the large amount of data that can be pulled may result in slow transmission times, you can choose to start your view with only the **Overview** tab or to pull data for all tabs. If you choose to start with **Overview Only**, you can gather data from the other tabs by going to the section you need to view and clicking the **Refresh** button at the top of that section.



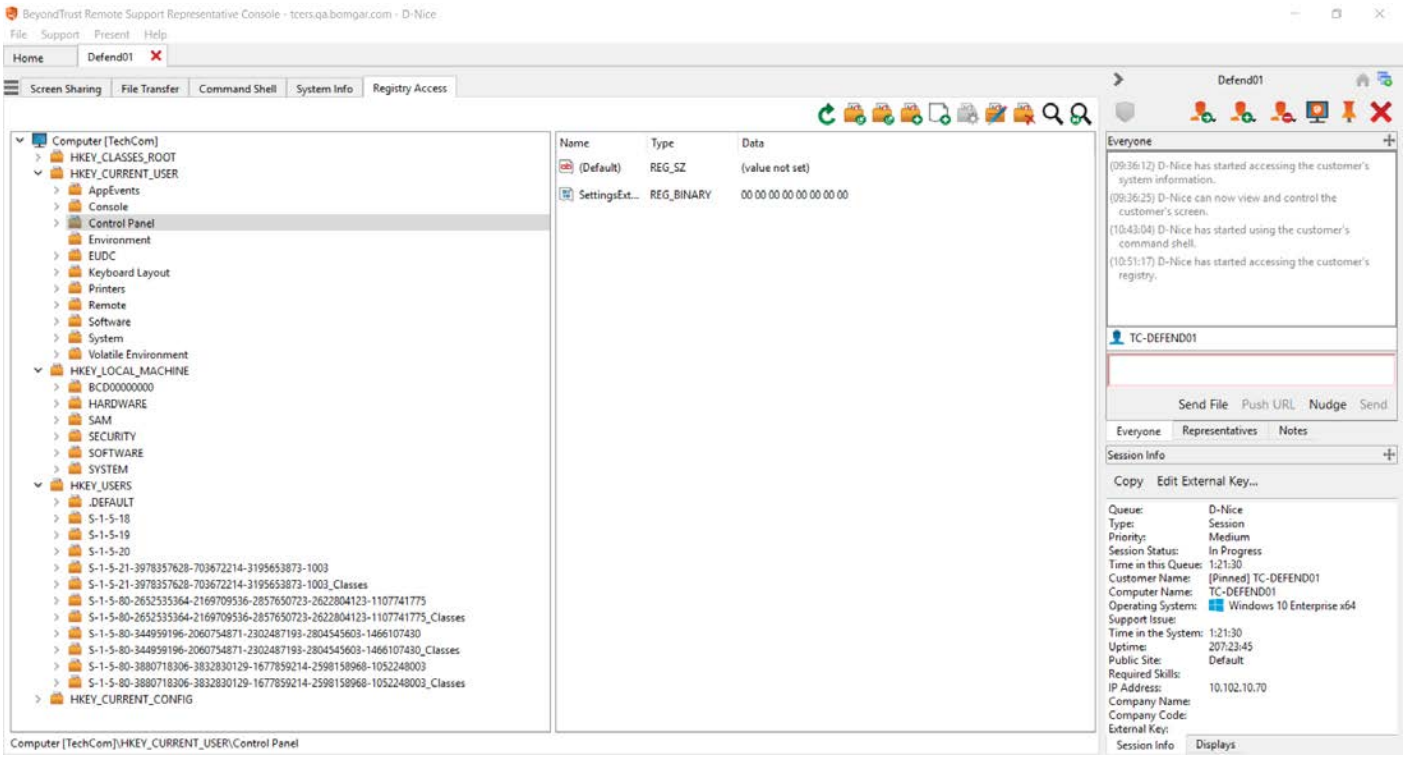


System Information Tools

	Stop pulling information about the remote system. Stopping will leave the last updated information available to view but will not pull current data.
	Refresh your view of system information or pull information for tabs to which you did not initially request access. Refresh can take place for individual sections or for all sections of the selected tab.
	Auto-refresh a category of system information.
	Copy the information to your clipboard. Copy individual sections or all sections of the selected tab.
	Save a text file of the system information to your local computer. You can save individual sections or all sections of the selected tab.
	End a running process on the remote system.
	Uninstall an app on the remote system.
	Start a stopped service on the remote system.
	Resume a paused service on the remote system.
	Pause a running service on the remote system.
	Stop a running service on the remote system.
	Restart a running service on the remote system.

Access the Remote Registry Editor

Access a remote Windows registry without requiring screen sharing. While in the virtual registry editor, you can add new keys, delete keys, edit keys, search, and import or export keys. Use of the virtual registry editor without screen sharing causes fewer interruptions to your customer and allows you to resolve issues more quickly.



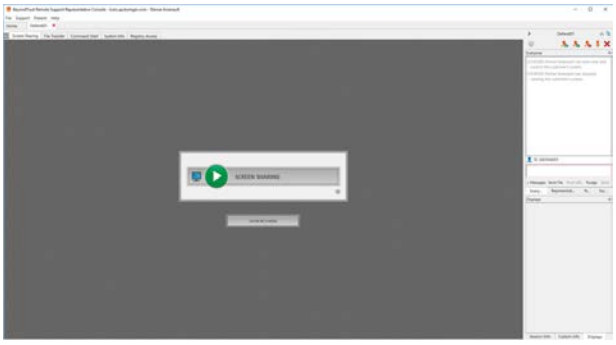
	Refresh the registry.
	Import registry entries from a file.
	Export registry entries to a file.
	Create a new registry key.
	Create a new registry value.
	Modify the selected registry value.

	Rename the selected registry entry.
	Delete the selected registry entry.
	Search the registry.
	Find next.

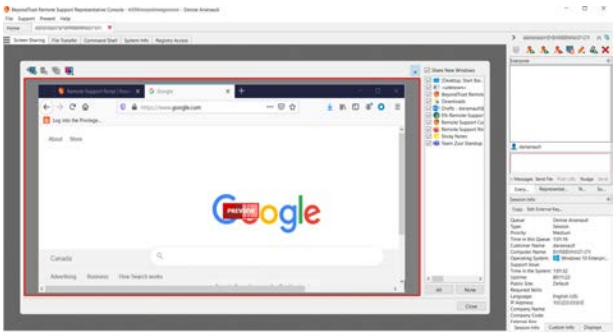
Show My Screen to the Customer

A privileged representative can share their screen with a customer at any time, aiding effectiveness of support sessions or training.

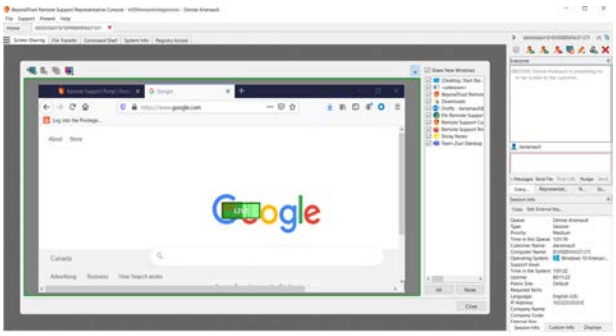
Privileged representatives begin support sessions with **Screen Sharing** or **Show My Screen** options immediately available. If you are screen sharing, you must stop screen sharing if you wish to begin a Show My Screen session.



The representative console displays a preview of what your customer's viewing experience will be when you make the session live. When you share your screen with your customer during a support session, your customer will be able to see either your entire desktop or only those applications you have chosen to present. You may also choose whether to share new windows automatically. Show or hide the application selector by clicking the arrow at the top of the **Show My Screen** window.



Click the **Present Your Screen to the Customer** icon at the top left of the window to begin your live Show My Screen session. You can continue chatting with your customer throughout the session.



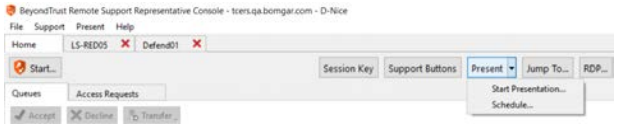
Note: *Show My Screen activity is recorded for reporting purposes if so configured in* ***/login > Configuration > Options****. The recording is not available to your customer on the post-session landing page.*

Show My Screen Tools

 	Show your entire screen or selected applications to the remote user, or stop showing your screen.
	While showing your screen, request or stop your customer's control of your keyboard and mouse, as when you are training a customer.  ***Note:*** *The Linux customer client does not support control of the representative's screen.*
	Select the display monitor for your Show My Screen session. The primary monitor will be designated by a **P**.

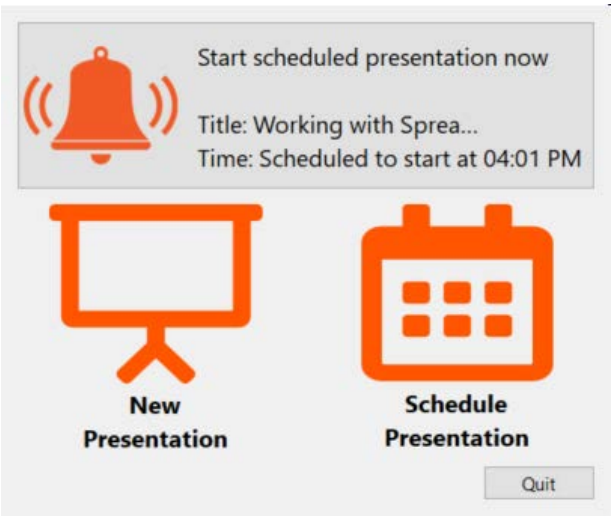
Give a Presentation to Remote Attendees

A representative with permissions to give presentations, or alternatively a representative with only presentation permission, can share their screen with one or more remote attendees. Start a presentation from:



- The **Present** menu of the representative console
- The **Present** quick start button at the top of your representative console
- The Presentation-Only interface selection window (representatives without permission to provide remote support)

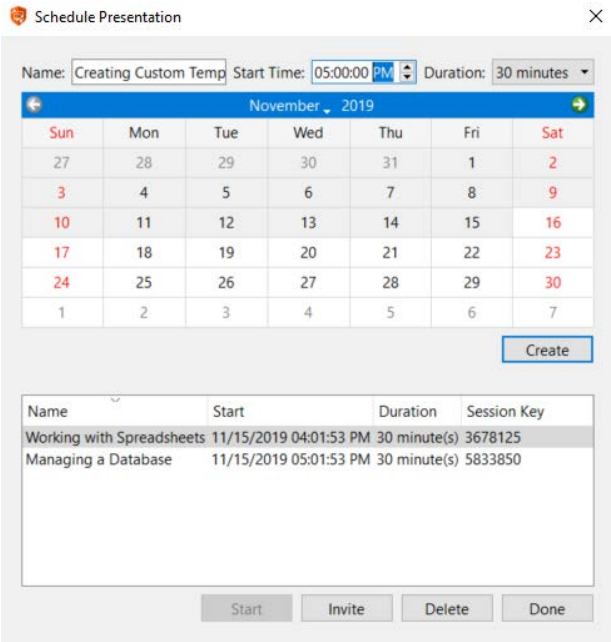
If you choose to start a presentation immediately by clicking either the **Present** button or by selecting **Start Presentation...**within the representative console, you will open the BeyondTrust Presentation interface. If you have Presentation-Only permissions you will begin a presentation first by clicking the **New Presentation** button in the Presentation-Only selection window.



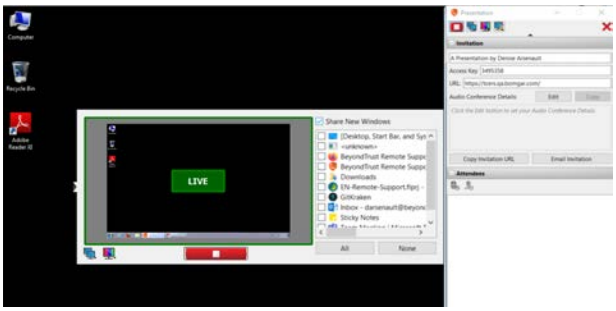
Alternatively, schedule a presentation for a later date. A scheduler will prompt you to enter a name for your presentation, a start time and date, and the expected duration of the event. Once you have entered this information, click **Create**. Your presentation will now appear in a list of your upcoming presentations. Presentation times cannot overlap. If you delete a presentation prior to its scheduled time, any invitations you have sent will be invalid, and attendees will not be able to connect. When you are ready to begin a scheduled presentation, select the presentation from the list and then click **Start** to open the presentation interface.

From the scheduler, you can send attendees an email invitation containing a unique URL and any audio conference details for your presentation, or you can direct your attendees to visit your public site and enter the unique session key. You can also send an email invitation from the presentation interface.

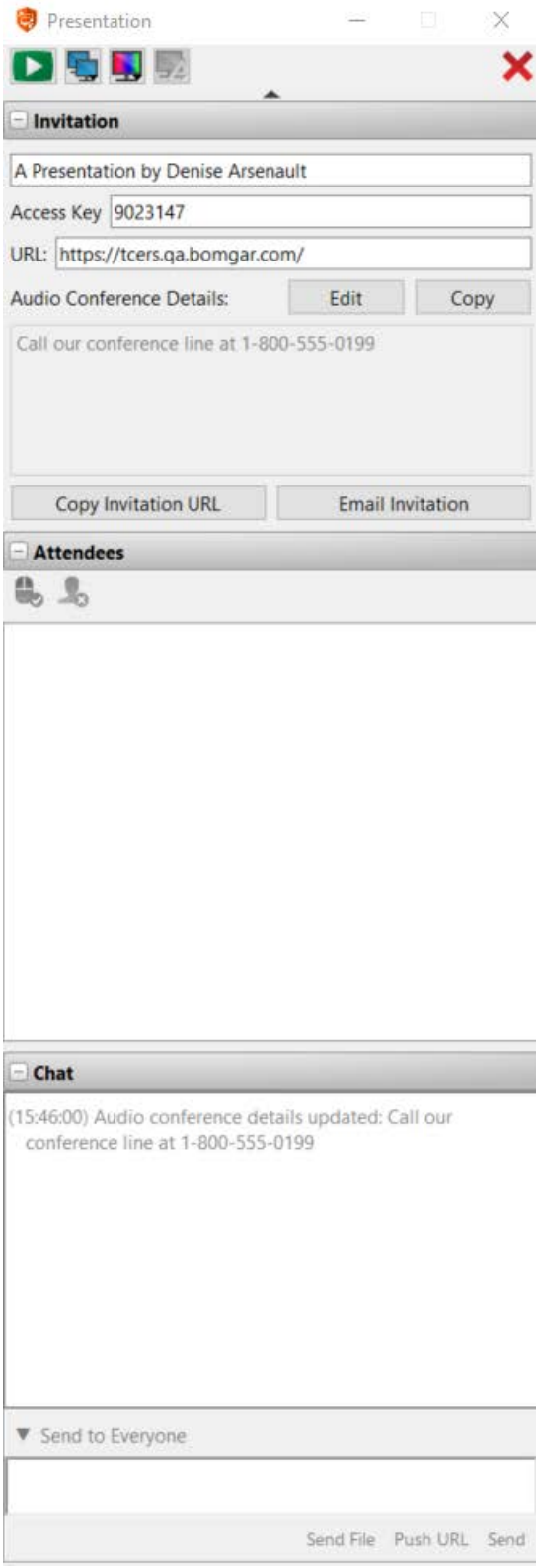
If a presentation is scheduled to start soon, a button at the top of the Presentation-Only selection window allows you to begin the presentation directly. You can also start a scheduled presentation from the schedule window.



The presentation interface consists of an unobtrusive vertical sidebar with three collapsible sections: **Invitation**, **Attendees**, and **Chat**. A sliding, horizontal side panel contains a previewing window that displays a status indicator which changes when you click the start/stop button to indicate that you are presenting live. An application selector, display selector, and resolution selector, described below, are also available.



In the **Invitation** section you may enter a name for your presentation if you wish, or you may use the default generic entry including the representative's name. Enabled fields for the presentation's **Access Key** and **URL** are displayed, and you may choose to enter and save audio conference details, which are retained from one presentation to the next, and are logged in the chat window. This information is sent to all attendees when they connect and is redistributed any time you update the information during a presentation. If your public site has the presentation list enabled, you can select **Showing on Public List** to display a link attendees can click to join your presentation. Buttons are provided to quickly and efficiently **Copy Invitation URL** and also to **Email Invitation**.



If the **Invite** button is missing in the presentation schedule dialogue, confirm that client side emails have been configured and enabled on your instance. For more information, please see Email Configuration: Configure the Software to Send Emails at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/email-configuration.htm.

The **Attendees** section lists those attendees who have joined your presentation. A button allows you to grant or discontinue an attendee's control of your mouse and keyboard, if permitted. Also, you may choose to remove attendees from your presentation by clicking the button to remove attendees.

Note: *When your attendee has control of your mouse and keyboard, the attendee will see a red bar across the bottom of the attendee window. If the attendee is in actual size or full screen mode, attendee will drop out of those modes when taking control from you. An attendee using a mobile device cannot take control.*

The **Chat** section of the presentation interface logs your actions in the interface as well as messages you send to all attendees or to selected attendees. Your attendees may chat with you alone or with everyone.

Clicking the arrow above the presentation interface sections minimizes the interface to mini-mode containing only the presentation controls themselves.

When previewing the presentation or presenting, you can open or close the Preview/Live pane by clicking the handle at its left. From this pane, select which applications to share. You can choose whether to present new windows automatically or not.If you have more than one display for your computer, click the monitors icon to select which monitor to present. The primary monitor is designated by a **P**. You may also choose to present all of your displays.

You can also choose the presentation color depth - **low bandwidth**, **best performance**, **performance and quality**, or **best quality**.

The start, stop, monitors, and color depth buttons are available whether or not you have the Preview or Live pane open, or whether or not you have collapsed the BeyondTrust Presentation interface to its minimal screen presence, or mini-mode. The annotations button is also available when you are presenting.

Presentation Tools

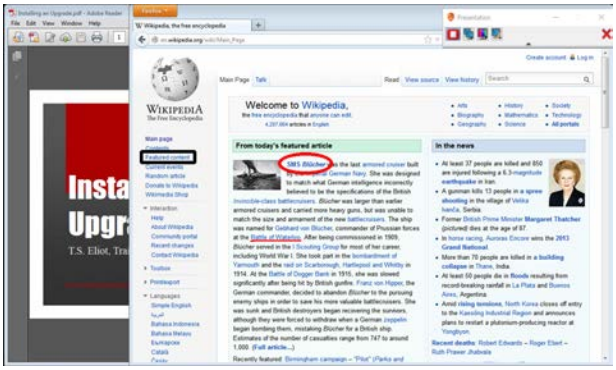
	Begin presenting. A live presentation will be reflected in the presentation interface pull-out panel with a translucent green **LIVE** indicator.
	Stop presenting. The presentation interface pull-out panel will display a translucent red **PREVIEW** indicator.
	Select the display monitor for your presentation session. The primary monitor will be designated by a **P**.
	Present the screen in 2-bit gray scale for the lowest bandwidth consumption, 8-bit color for fast performance, 16-bit for a medium quality of image and performance, or 32-bit for the highest image resolution.
	Begin using annotations in your live presentation.
	If permitted, grant control of your mouse and keyboard to an attendee. Only one attendee at a time can have control of your computer. You always maintain overriding control, and you can cancel the attendee's control at any time. An attendee using a mobile device cannot take control. You cannot transfer a presentation to another presenter.
	Remove attendees from the presentation without ending the presentation.
	End the presentation altogether and close the presentation interface.

Annotations

If you have permission to use Annotations, this tool is also available during presentations, allowing you to highlight areas of the screen and draw attention to specific areas and items.

Once you have started using annotations, right-click anywhere in your presentation to select from the annotation tools. To turn off **Annotations**, select **No Tool** from the dropdown menu, or click **Esc.**

Tools available include free drawing, rectangle and circle shapes, erase, undo, delete, color (red/black/white) and line thickness (thin/medium/thick).



Collaboration

Chat with Other Representatives

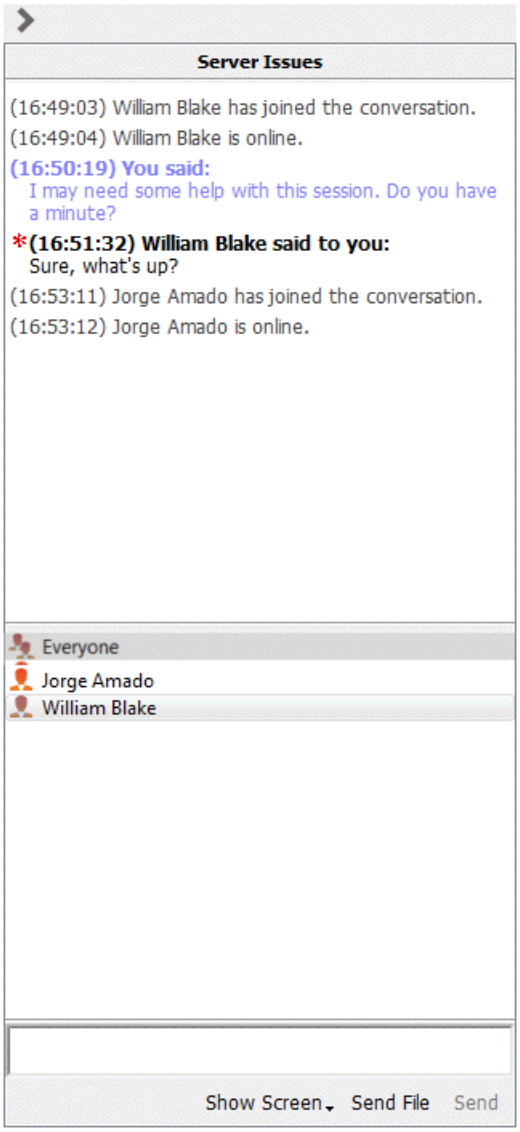
From the **Home** tab of the console, you can chat with other logged-in users. If you are a member of one or more teams, select whichever team you would like to chat with from the list of queues at the left of the **Home** tab. You can chat with all members of that team or chat with just one user.

When you go back to your personal queue or select **All Queues**, you will remain in the chat for the queue you just left.

Click the arrow icon at the top left of the sidebar to collapse the sliding sidebar. If the sidebar is collapsed, hover over the arrow by the hidden window to reveal it. Click the pin icon that replaced the arrow icon at the top left of the sidebar to re-pin the sliding sidebar.

When typing in English, misspelled words will be underlined in red. Right-click to view spelling suggestions or to ignore that spelling for the current console login.

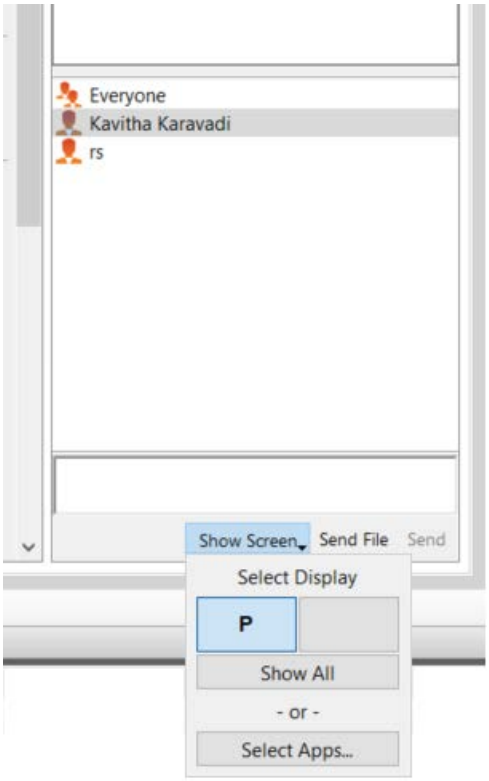
In the settings, you can choose if the team chat should include status messages, such as users logging in and out, or only chats sent between team members.



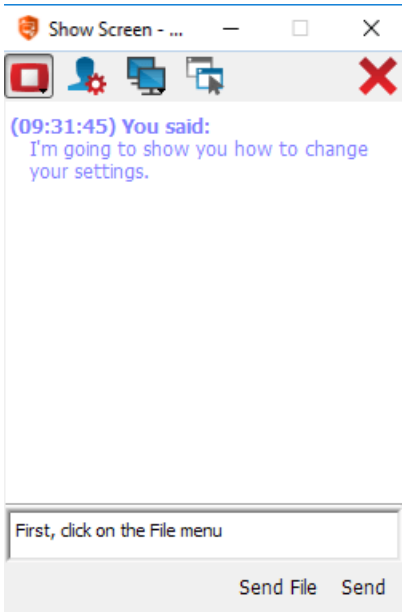
Share your Screen with Another Representative

If your administrator has enabled this permission, you can share your screen with another user without the receiving user having to join a session. This option is available even if you are not in a session.

From a team queue, select a user, and click **Show Screen**. If working with more than one monitor, you can select which one to share or which apps should visible to the other user. Once you have made your selection, the receiving user gets a notification with the option to accept or decline the invitation.



A **Show Screen** window appears, showing the name of the user that is now viewing your screen. This window contains a chat box and the options to stop screen sharing, grant the receiving user control, and select which monitor and which apps to share. You can stop sharing your screen but keep this window open, or you can close the sharing session completely. If you leave the **Show Screen** window open, you can restart sharing your screen.



Share My Screen Tools

Sharing User

	Temporarily stop sharing your screen with another user. This pauses screen sharing but does not close the **Show Screen** window, allowing you to restart screen sharing.
	(Re)start screen sharing.
	Grant mouse and keyboard control to the user viewing your screen.
	Select the monitor to share with another user. The primary monitor is designated by a **P**.
	Select which apps to share with the user viewing your screen.
	End the screen sharing session. This closes the user screen sharing interface.

Viewing User

	The user sharing their screen with you has granted you keyboard and mouse control.
	Turn on a virtual pointer, visible on the sharing user's screen.
	Capture a screenshot of the sharing user's screen at its full resolution.
	View the remote screen at actual or scaled size.
	View the remote desktop in full screen mode or return to the interface view.
	End screen sharing session. This closes the user screen sharing interface.

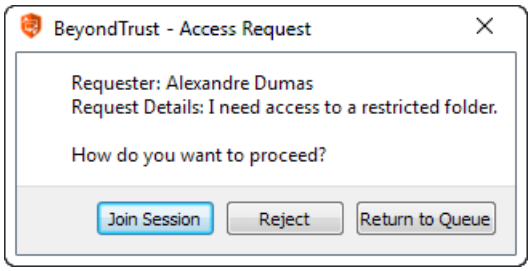
Accept an Access Request to Offer Elevation Help

Based on predefined access sponsor groups, a representative with restricted permissions can request a more highly privileged representative to perform certain actions on their behalf, such as elevating a customer client to administrative rights or entering credentials for a remote system.

If a representative is a sponsor in one or more access sponsor groups, they will see an **Access Requests** tab in the representative console.

When a representative makes a request, all sponsors in the selected access sponsor group will see a new request in the **Access Requests** tab of the representative console.

When a sponsor accepts the request, they will be prompted to join the session, reject the request and enter a reason for the rejection, or return the request to the queue.



Share a Session with Other Representatives

Invite another user to join a session by clicking the **Share** button in the session tools. By default, only teams to which you belong will be listed.

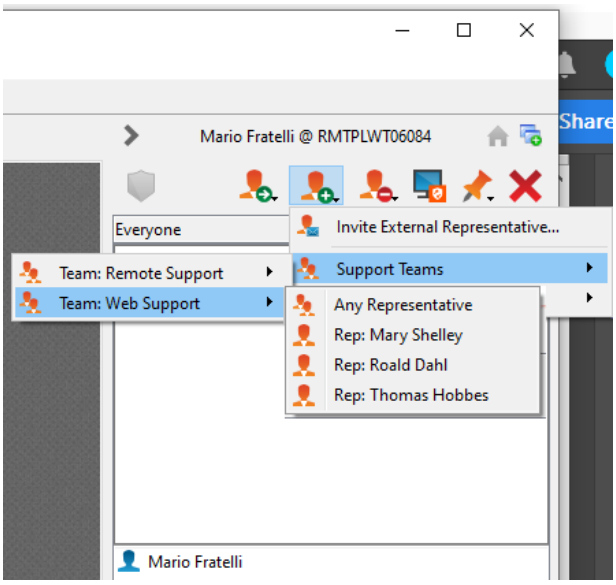
There are several ways you can invite a representative to join a session. You can use **Request Help** to route your request so that it is targeted at a specific support issue. Only issues that have been configured to allow you to request help are displayed on this list.

You can select a user listed in the teams displayed to invite them to join the session.

If you select **Any Representative**, the invitation is sent to the team queue so that any single representative in the selected team can join the session. You can send multiple invitations if you want more representatives from the team to join your session.

Users are listed here only if they are logged into the console or have extended availability enabled.

If you are permitted to share sessions with users who are not members of your teams, additional teams are displayed, provided that they contain at least one member logged in or with extended availability enabled.



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

If you have sent an invitation and it is still active, you may revoke the invitation by selecting it from the **Cancel Invitation** menu. Only the session owner can send invitations. Invitations do not time out as long as you remain the session owner. Multiple active invitations cannot exist for the same user to join the same session.

An invitation is made inactive when one of the following events occurs:

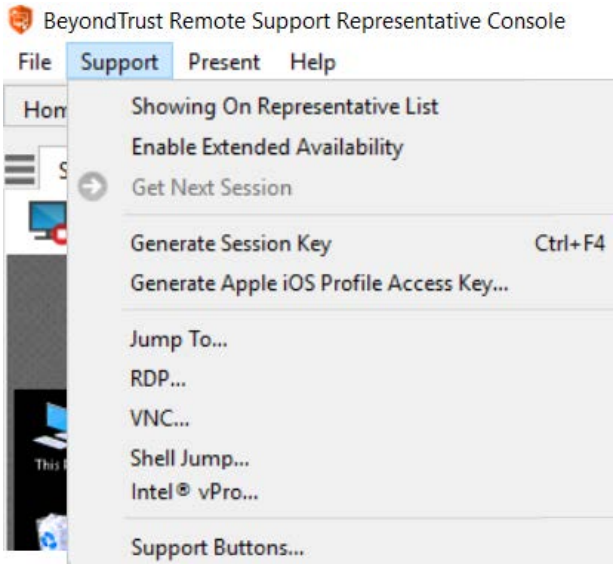
- The inviting user cancels the invitation
- The inviting user leaves or transfers ownership of the session
- The session ends
- The invited user accepts the invitation
- The invited user declines the invitation

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

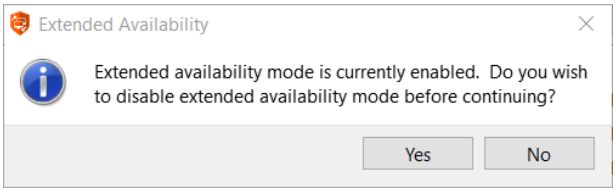
Use Extended Availability to Stay Accessible when Not Logged In

With extended availability, privileged users can receive email invitations to share sessions, even if they are not logged into the console. When sending an invitation, you may invite fellow team members. If permitted, you may also invite users from teams to which you do not belong. The ability to share sessions with users outside of your teams as well as to receive session invitations when logged out of the console extends your availability as a support representative.

If your account is configured for extended availability, you can enable or disable the functionality from the **Support** menu of the representative console.



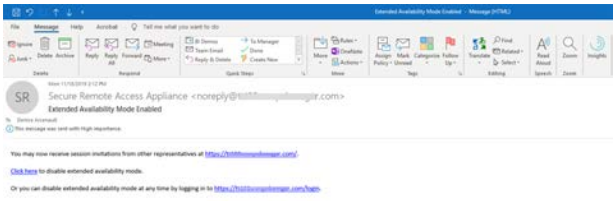
If you have extended availability enabled, you see a notification when you log into the console. From this dialog, you can easily disable extended availability to avoid distraction while in a session, for example.



Note: *If you choose to keep extended availability enabled, a license slot is reserved for you until such time as extended availability is disabled. This ensures that if you are invited to join a session, you are not denied login due to license usage restrictions*

Email Notification & Invitation

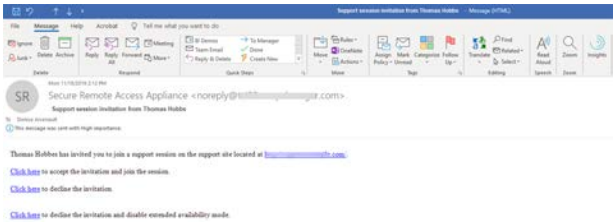
Each time you enable extended availability mode, the appliance notifies you via the email address configured for your user account, in the language you have specified, if available.



> ***Note:***
> *BeyondTrust does not pull email addresses from external LDAP directory stores. The email address must be configured in BeyondTrust in one of two ways:*
>
> 1. *An administrator can add an email address to a user account by going to **/login > Users & Security > Users** and editing the account.*
> 2. *The user can set their own email address by going to the **/login > My Account** page.*

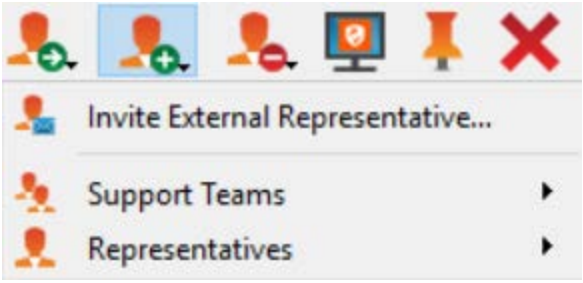
The notification includes the URL of the site as well as a link to quickly disable extended availability mode.

The appliance also sends an email notification when you are invited to a session. This allows you to join a session even if you are not currently logged into the console. The email notification includes links to accept or decline the invitation, as well as to decline the invitation while disabling extended availability mode.



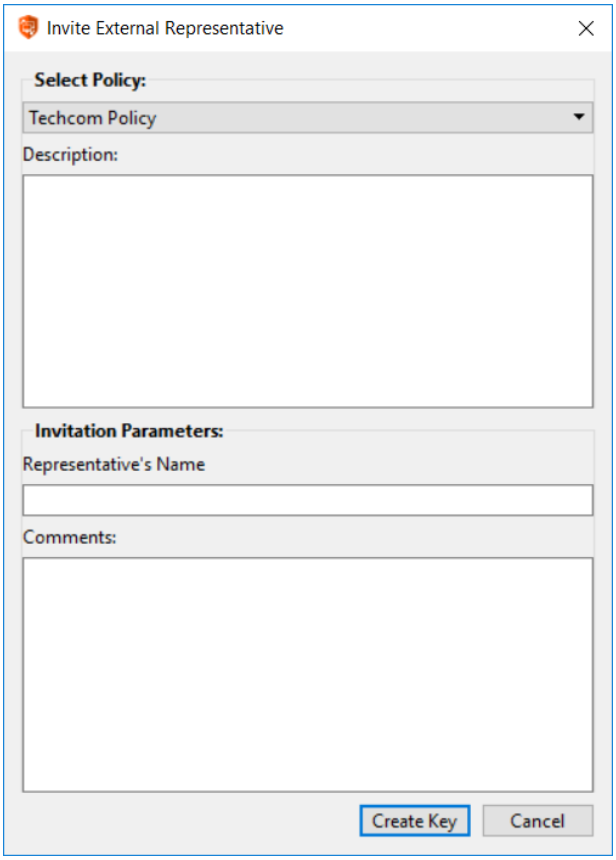
Invite an External Representative to Join a Session

Within a session, a user can request an external user to participate in a session one time only. The inviting user should click on the **Share Session** button and then select **Invite External Representative**.

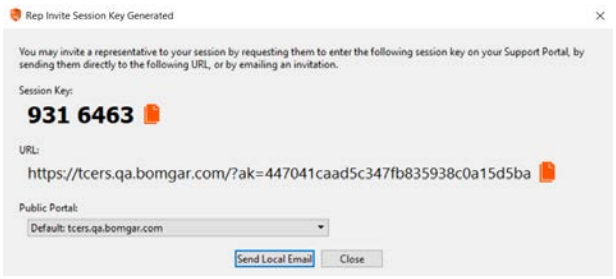


A dialog opens asking the user to select a security profile. These profiles are created in the administrative interface and determine the level of permission the external user will have. When you select a profile, the full description displays below.

Enter the invited user's name. This name will appear to the customer and in reports. Next, enter comments about why this user has been invited. Click **Create Key**, and a new dialog containing the session key and direct URL will appear.



Click the **Send** button to select how to send the session key to the external User. Depending on the options selected by your administrator, you may be able to send the invitation from your local email or from a server side email. You also can copy and paste the direct URL to the external user. The external user will need to download and run the representative console installer, which is an abbreviated process from the full representative console installation.



The invited user will have access only to the session tab and has a limited set of privileges. The invited user can never be the session owner. If the inviting representative leaves the session without another session owner, the external representative will be logged out.

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

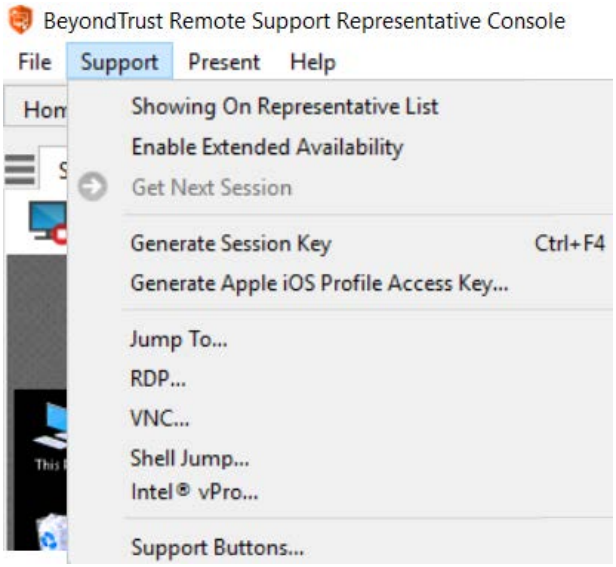
Management

Manage Support Buttons

Support Buttons allow customers to initiate a support session to their assigned support team, enter a session key, or submit an issue to a support queue. Deployed Support Buttons can be managed from the Support Button management interface. Note that a mass-deployed Support Button installed in system-wide mode must be removed using Add/Remove Programs or system management tools.

Access the Support Button management interface from:

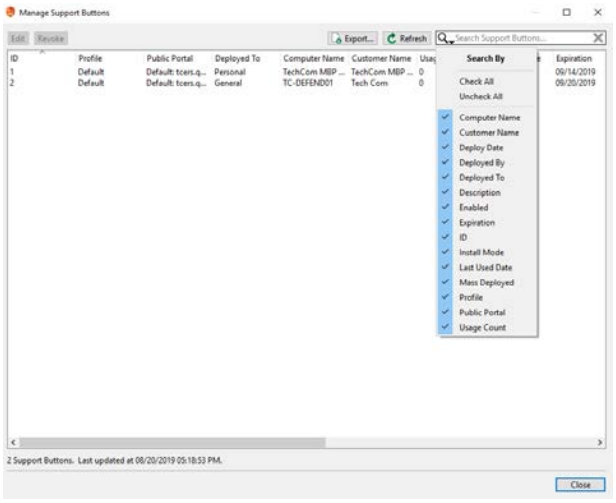
- The **Support** menu of the representative console
- The **Support Buttons** button at the top of the representative console



The Support Button management interface displays a list of deployed Support Buttons along with usage statistics.

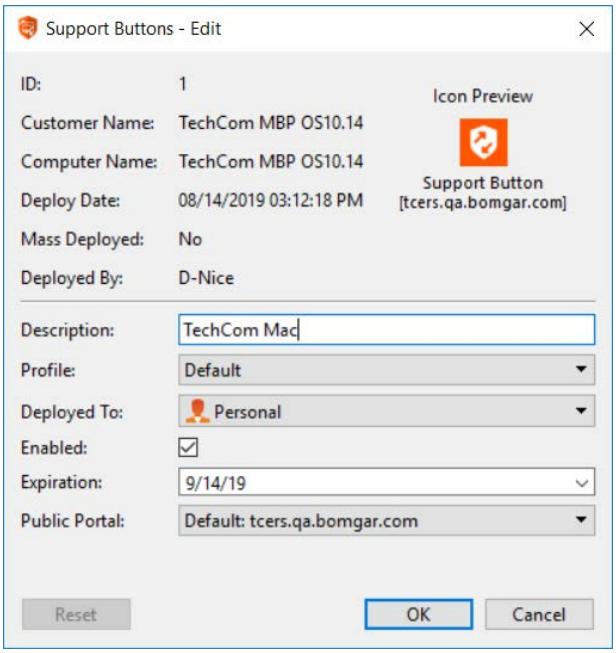
Administrators see all deployed Support Buttons, while privileged users can see the buttons associated with their personal queue and their team queues.

Click the search icon to select which fields to search. Then type in the text entry box and press enter to perform a search. Additionally, you can sort the data rows by clicking on a column header.



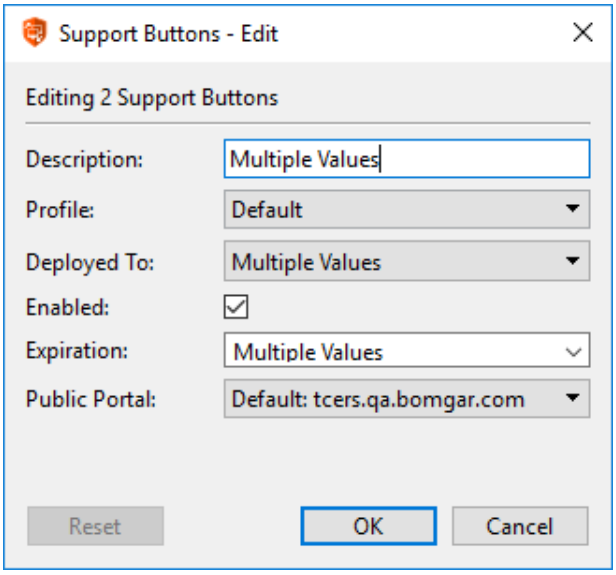
The Support Button usage statistics include:

- Static fields:
  - **ID**
  - **Customer Name**
  - **Computer Name**
  - **Deploy Date**
  - **Mass Deployed** (Yes/No)
  - **Deployed By** (Representative Private Display Name)
  - **Usage Count**
  - **Last Used Date** (or Never if none yet)
  - **Install Mode** (User or System)
  - **Icon Preview**
- Dynamic (allowed to edit) fields:
  - **Description**
  - **Profile**
  - **Deployed To** (Queue)
  - **Enabled** (Yes/No)
  - **Expiration**
  - **Public Portal**

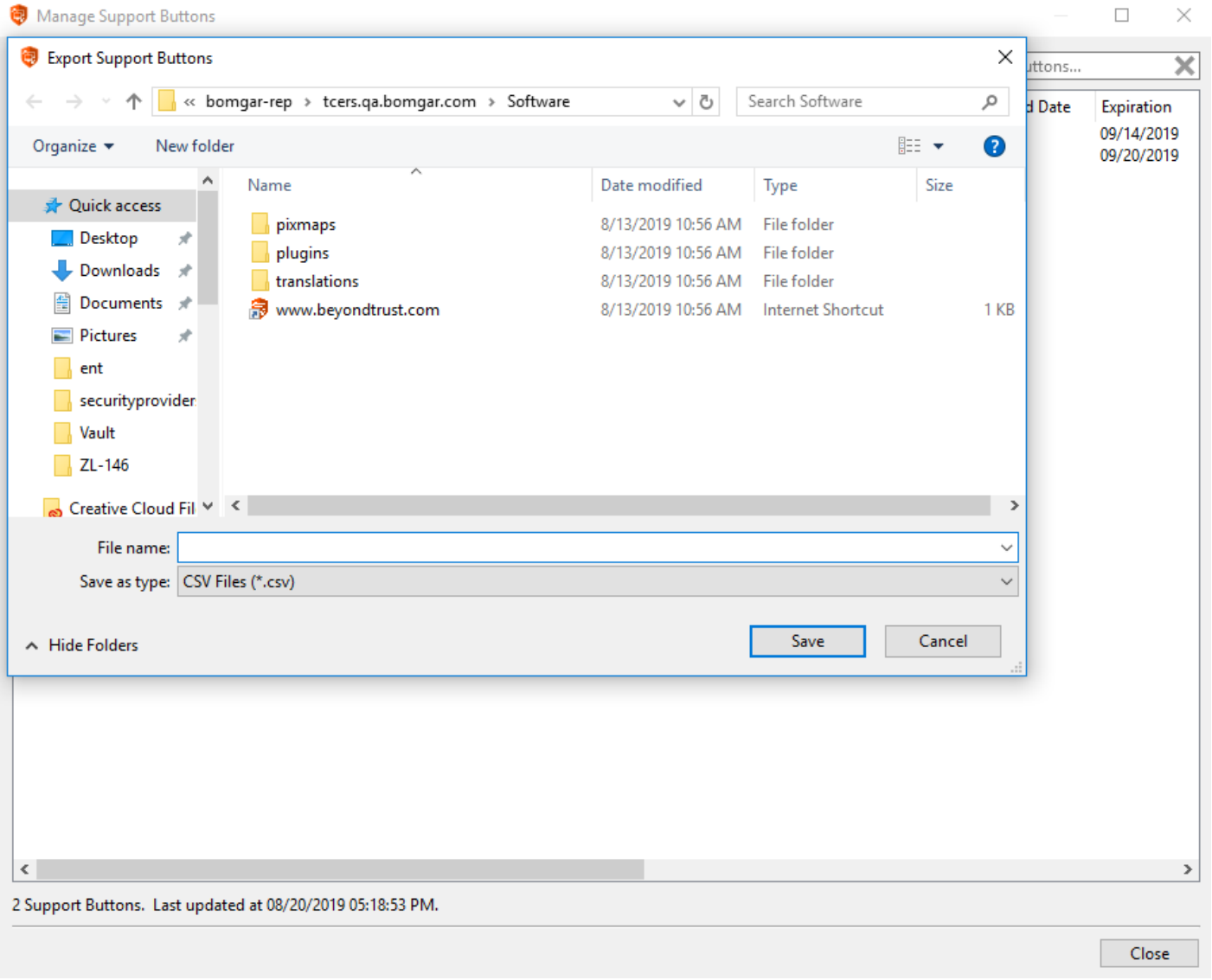


You can also **Edit** the dynamic fields, **Revoke** a Support Button, or **Export** the Support Button usage statistics to a *.csv file. If you revoke a mass-deployed Support Button installed for all users of a system, the button may be removed only by using the system Add or Remove Programs control panel or systems management tools.

If you select **Edit** from the **Support Button Management Interface**, you can edit any of the dynamic fields. If multiple Support Buttons are selected to edit, **Multiple Values** is displayed in any dynamic fields that have different values.



If you select to **Export** the usage statistics, the file selection screen is shown. You can enter the file name desired and the location where you wish to save the *.csv file.



Monitor Team Members in the Dashboard

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

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

Status indicators show whether users are available to take sessions (green), are idle (gray), are busy (yellow), or have auto-assign turned off (red). If a user is in more than one state, their status color shows the most important information in order of auto-assign turned off, busy, idle, and available. Hover over the user's name to view full details. A bar at the bottom of the dashboard shows the percentage of users in each state. Hover over this bar to view the number or users with each status. Users cannot manually alter how their statuses are displayed.

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

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

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

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

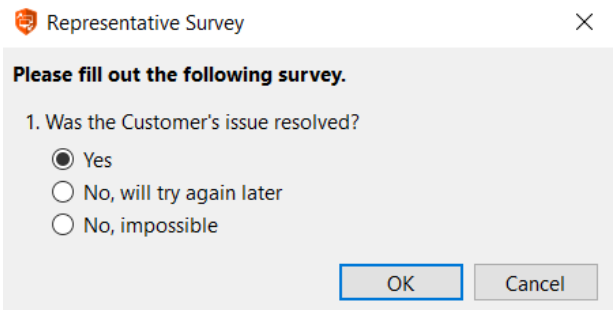
To gain control of the user’s computer, click the **Enable Mouse/Keyboard Control** button.

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

Representative Survey

At the end of the session, you may be prompted to fill out a short survey regarding the session. Your administrator can fully customize the questions through the administrative interface and can review the results from the session reports. If one or more of the questions is required, you will not be allowed to close the session until you have answered those questions.

Your administrator may also choose to allow you access to the representative survey during a session. In this scenario, the survey can be used as a workflow template, allowing your administrator to push a series of questions and/or check mark points, as well as specific links you may use in your support session.



What Your Customer Sees: The BeyondTrust Customer Client

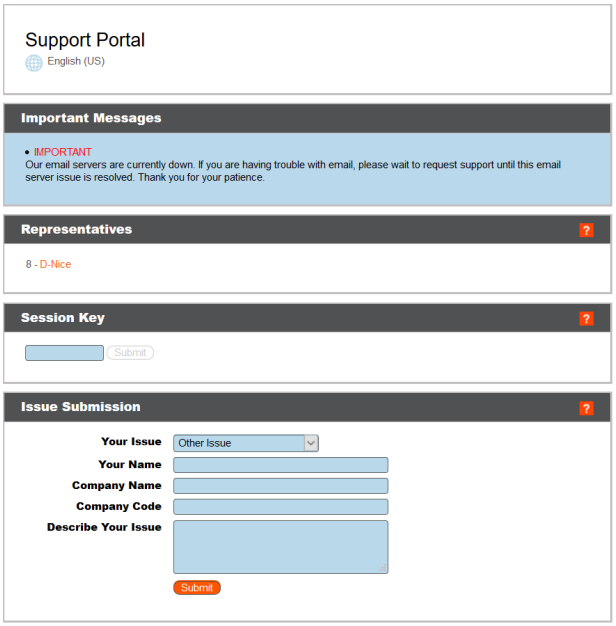
Customers on remote desktops, smartphones, and other devices interact with support reps primarily through the BeyondTrust customer client.

They may also see prompts and messages in the context of the public site or support portal. This section details the customer-facing elements of a BeyondTrust remote support session on a desktop or laptop.

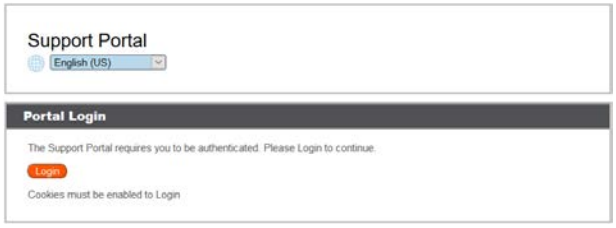
For more information on supporting other devices, including Apple iOS and Android, please see https://www.beyondtrust.com/docs/remote-support/getting-started/index.htm.

Public Site: Request Support

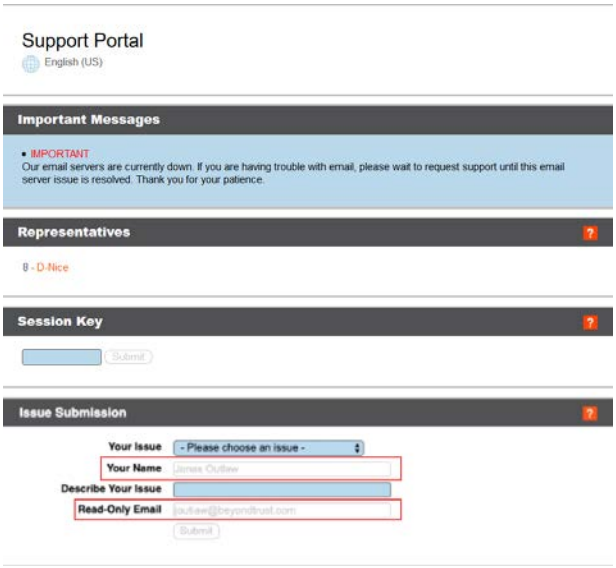
The public site is the support portal for your Secure Remote Access Appliance, where your customers go to request a support session or join a presentation. On this page, your customer can initiate a session by clicking a representative's name, submitting a session key, or filling out an Issue Submission form. Your customer can also join a presentation by clicking on a presentation link or submitting a session key.



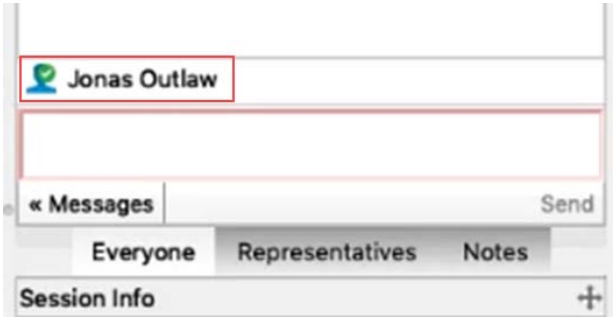
A customer can access the public support portal using the URL provided by a representative. If SAML authentication is configured and enabled for the public site, the customer is presented with the **Portal Login** window. The customer must click **Login** and then provide credentials to authenticate with the identity provider.



The customer is then taken to the support portal page where they can submit their request for support. The customer's name and any custom fields that are configured, such as email, are automatically populated and are not editable.



***Tip:** A green check mark is displayed next to the customer's name in the representative console chat window to indicate the user is public portal authenticated.*



For more information, please see SAML for Single Sign-On Authentication at https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.

If real-time chat translation is enabled, customers can chat with a representative in their own language. As an example, a customer whose main language is English could chat with a representative who speaks only Dutch, with the chat traffic being automatically translated in real time.

For more information on real-time chat translation, please see Real-time Chat Translation at https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm.

If the issue submission survey is enabled, your customer will be asked to select either a representative name or a specific type of issue, depending upon the settings your administrator has put in place. Your customer can also enter their name, company name, and a description of the problem. Your administrator optionally might include a **Company Code** field to help with issue tracking.

Based on the method of session initiation, your customer will be placed either in the selected representative's support queue or in the support queue for the team assigned to handle the selected issue, or your customer will join the specified presentation.

For your Apple iOS device customers, your iOS-configured support portal is a secure repository of public and private profiles you uploaded in the **/login** interface. Private profiles are only accessible if the representative has generated an iOS access key.

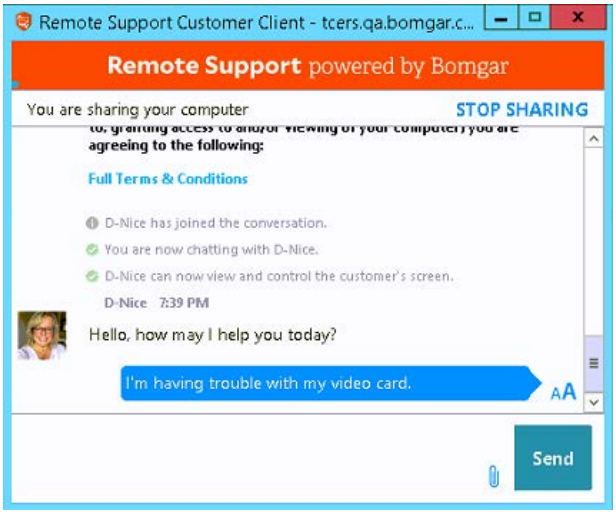
If any customer notices are active for this site, they will be displayed in the **Important Message** section. Notices can alert customers to broadly impacting IT outages for which no support may be needed at this time, thereby eliminating the need for the customer to join a support session unnecessarily.

If a schedule is set for this public site and the current time is outside of the scheduled business hours, session start methods other than session keys are removed from the site, and a portal closed message displays.

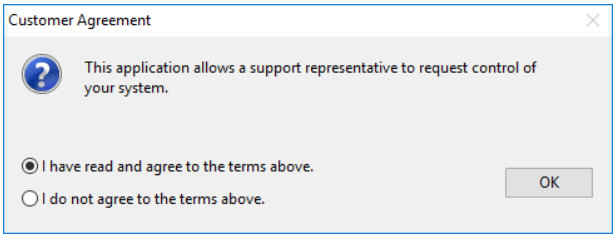
Customer Client: Support Session Interface

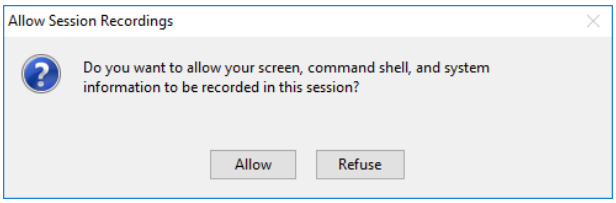
When your customer starts a support session with you, that session starts either as web-based chat or with the full customer client download, depending on your site settings. If you uploaded a photo avatar to be used with your account, the photo displays in the chat window. Please note that this only works with the full customer client, not the HTML one.

If starting a session as an HTML5 web-based chat, your customer is asked to allow notifications, enabling pop-up notifications to help make your communications with customers more efficient.



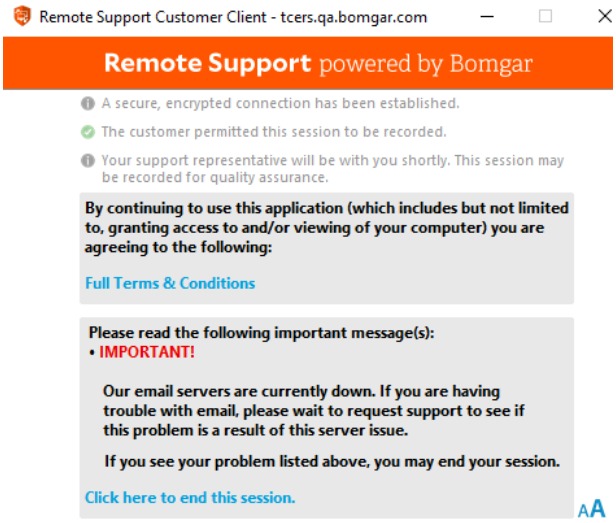
Your administrator can determine which messages your customer sees before the session begins. Among the messages that may be displayed are a customer agreement, requiring the customer to accept the terms of entering a support session; a prompt to allow or refuse session recordings; and a greeting, which may include the estimated wait time and the customer's position in queue.



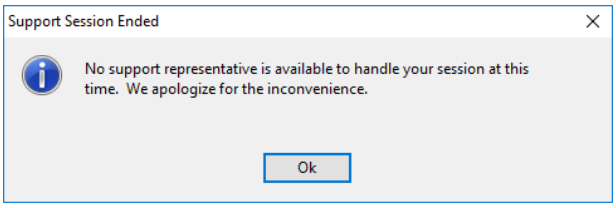


If any customer notices are active, they may be displayed automatically or sent manually to the customer client, giving customers the chance to leave the session if they are experiencing a known issue described in the notice. Customers leaving the session in this manner are not taken to the **Exit Survey** page, since no service was actually provided by a representative.

A hold message may display periodically, reassuring the customer that they are still in queue and will be attended to shortly. This message may include the estimated wait time and the customer's position in queue.



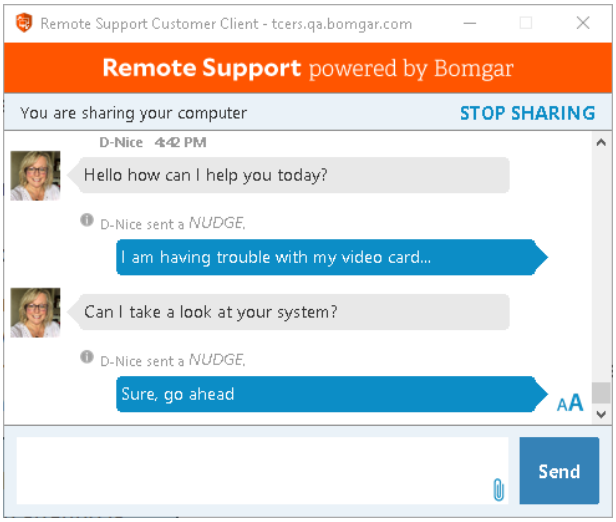
If no representative is available to take the session, an orphaned session message may be displayed. Optionally, the customer's web browser can then be automatically opened to a specified URL, such as a knowledge base or contact page.



During the session, the customer can chat with you and can request to send files to your computer. Your customer also can change the font size of the chat display.

If you send a nudge, the customer client is given focus and jiggles, and an audible alert sounds. The chat display shows that a nudge was sent.

To immediately stop screen sharing and disable any permissions the representative might have had, click the **STOP SHARING** link on the right side of the banner at the top of the chat The customer can also choose to close the session entirely by closing the chat window. This uninstalls the software from their machine.



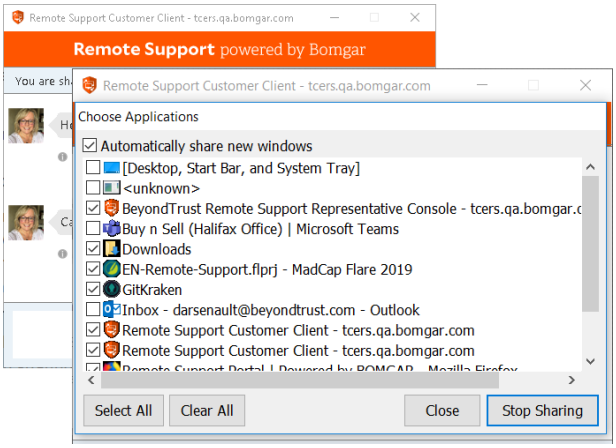
> ***Note: STOP SHARING*** *appears when screen sharing is done without any restrictions. If you allow the customer to select which applications to choose, then* ***MODIFY SHARING*** *is displayed, allowing the customer to change or select which applications to share, or to stop sharing altogether, if so desired. In either case, the session can always be terminated by closing the chat window.*

Additionally, depending on your site settings, a watermark may appear on your customer's screen while you are in a session. This applies only to Windows systems.

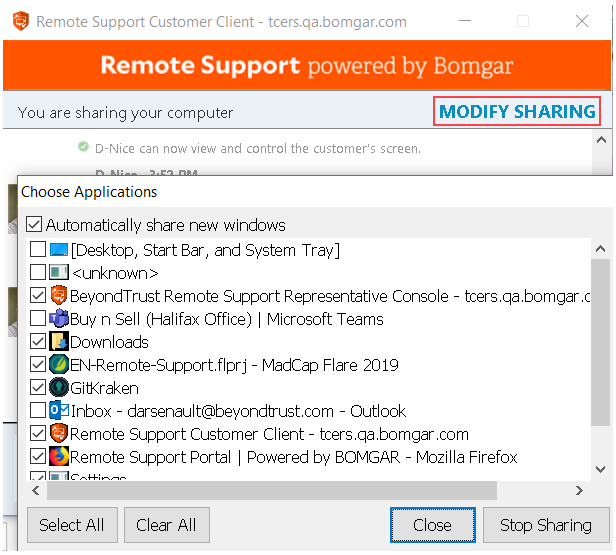
> ***Note:*** *Customers running Linux must mark the customer client download file as executable before they can install it.*

Application Sharing: Limit What the Representative Can See

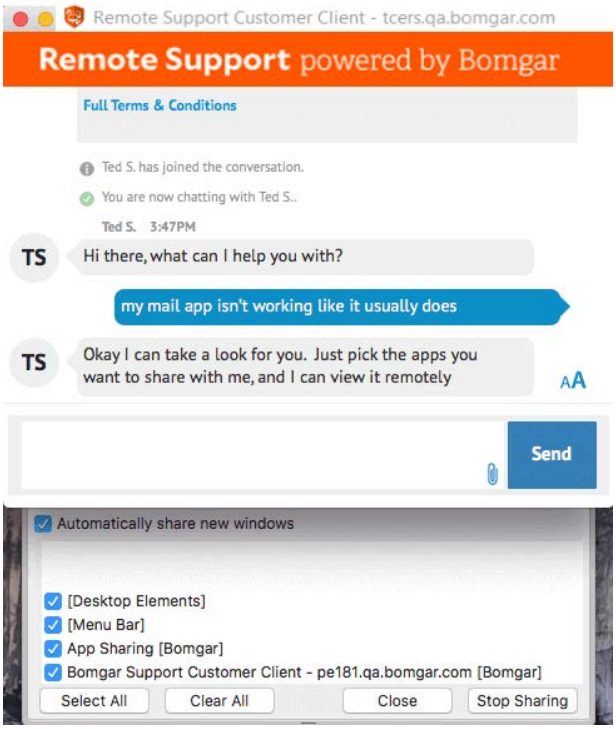
When you request limited screen sharing, a selection window will pop up in front of the customer client chat window.



After screen sharing is granted, the application selection window can be accessed by clicking the **Modify Sharing** link.

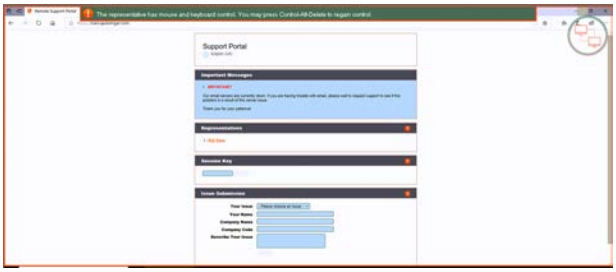


Depending on your site settings, your customer may always be able to select applications from the fly-out menu, even if limited screen sharing was not specifically requested. Application sharing is available when supporting Windows or Mac computers. You may have pre-defined application sharing restrictions applied to the support session by your support team administrator.



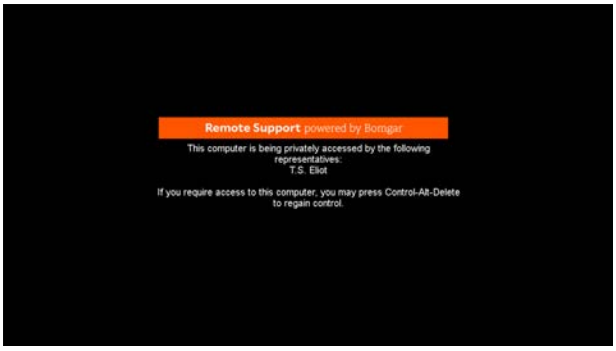
Restricted Customer Interaction: Privacy Screen, Disable Remote Input

To expedite your support of a remote computer, you can avoid customer interference by disabling the remote user's mouse and keyboard input. The remote user will still be able to see the active desktop. While input is disabled, each remote monitor will display an orange border.



Should you need to work on the remote computer privately, you can enable a privacy screen so that the remote user or passersby cannot see what you are doing. Instead, a courtesy message will be displayed. Your customer can regain control at any time by pressing **Ctrl-Alt-Del**.

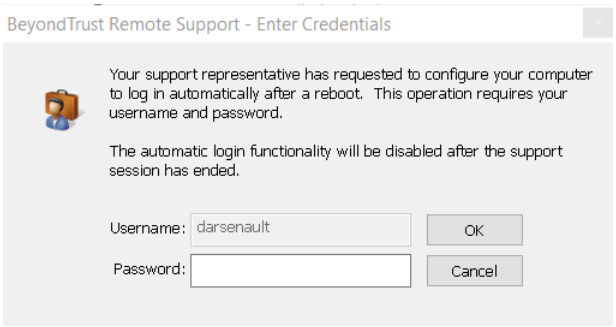
Restricted customer interaction is available only when supporting macOS or Windows computers. In Windows Vista and above, the customer client must be elevated. On Windows 8, privacy screen is not available, and the representative can only disable the mouse and keyboard.



This feature is enabled from the **Screen Sharing** tab of a support session in the representative console. For more information, please see "Screen Share with the Remote Customer for View and Control" on page 72.

Automatic Log On Credentials: Reboot and Reconnect

You can prompt your customer to enter a valid username and password which will allow you to reboot the remote computer and automatically log back into the system without having to know their credentials or requiring them to be present. Follow the steps below to use the automatic log on credentials feature:



Note: *To perform this function, your administrator must have enabled the /login security option to Allow Reboot with Cached Login Credentials.*

Tip: *Before you can use this feature, you must elevate the support session and start screen sharing.*

Note: *The credentials are stored by the OS and not by BeyondTrust. We leverage a secure function native to Windows to accomplish this functionality. At no time are the credentials exposed on the network in any form. This functionality is available for Windows OS only and cannot be performed on remote systems running a Mac OS.*

1. Click on the **Power Control Special Action** from the menu.
2. Select **Request Automatic Login Credentials**.
3. The user should enter their credentials into the prompt.
4. Once done, the Power Control Special Actions menu text changes from **Request Automatic Login Credentials** to **Clear Automatic Login Credentials**.
5. Upon the next reboot, the system will log in with the credentials entered by the user.

Show My Screen: Reverse Screen Share

When you share your screen with your customer during a support session, your customer will be able to see either your entire desktop or only those applications you have chosen to present. You can continue chatting with your customer throughout.

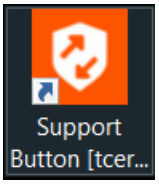
To enlarge the screen viewing area, your customer can hide the side chat bar by clicking the show/hide arrow on the divider between the chat bar and the presentation window. If your customer receives a message while the chat bar is hidden, the show/hide arrow will flash orange.

Your customer can further manage the presentation display by choosing to view your screen at its actual size or scaled to fit in the client window. Your customer can also choose to view your screen at 8 bits for the fastest performance, 16 bits for a medium quality of image and performance, or 32 bits for the highest image resolution. You can also choose to share mouse and keyboard control with your remote customer.

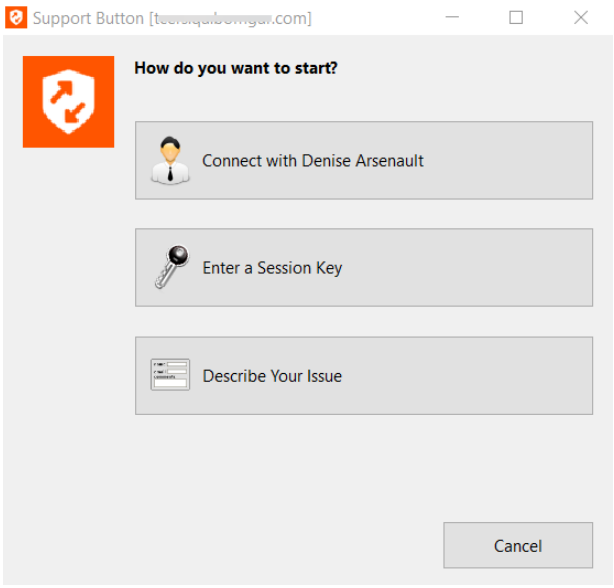
Note: *The Linux customer client does not support control of the representative's screen.*

Support Button: Quickly Request Support

If you have installed a Support Button on your customer's computer, that button will appear as a desktop or menu shortcut on their computer. If the Support Button has been customized, it will appear on your customer's computer with a custom image and title.



Clicking this button opens a dialog prompting your customer to start a session. If this button has been preconfigured to start a session with a specified representative or team, your customer can begin a session by clicking the **Connect** button.



Alternatively, your customer can enter a session key or describe their issue. When entering a session key, the customer will connect with whichever representative generated the key, regardless of whether the representative is associated with that Support Button or not.

> ***Note:*** *A Support Button cannot be deployed from a session that was started from a SAML authenticated public portal and a Support Button cannot be used to start a session with a public portal that requires SAML authentication.*

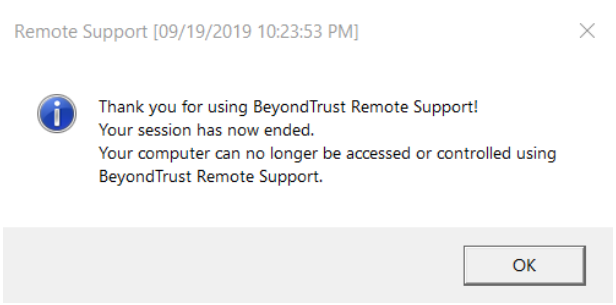
If any customer notices are active for the public site this Support Button is associated with, those messages are displayed at the top. Notices can alert customers to broadly impacting IT outages for which no support may be needed at this time, thereby eliminating the need for the customer to join a support session.

If a schedule is set for this public site and the current time is outside of the scheduled business hours, session start methods other than session keys are removed from the Support Button, and a portal closed message displays.

If you have embedded a Support Button in an external application, that Support Button will appear as a link in the title bar of the application. Clicking this link may open the dialog for all of the session start options, may open the issue submission survey with an issue pre-selected, or may send your customer directly into a team queue with an issue pre-selected.

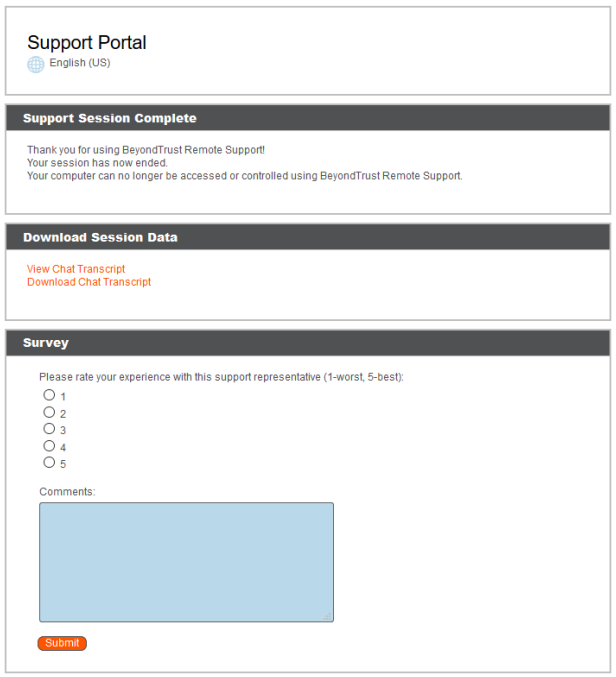
Customer Exit Survey: Submit Feedback

After the session is complete and if a Jump Client is not installed for later access, your customer will be notified that you can no longer see or access their computer and that BeyondTrust has been completely uninstalled.



If your administrator has enabled an exit survey, your customer will then be directed to a survey asking them to rate the session experience. Your administrator can fully customize this survey from the administrative interface and review the answers later from the session reports.

Alternatively, if your administrator has set up a post-session redirect URL, a browser window will open on your customer's computer, taking them to the specified site.

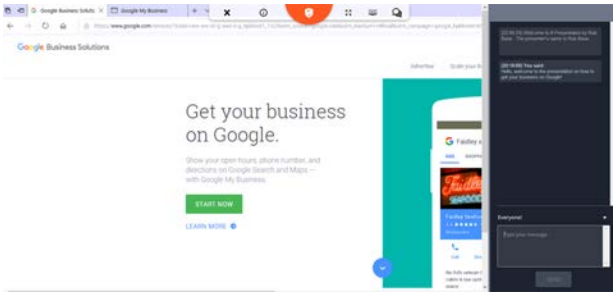


Presentation Attendee Client: Join a Presentation

To join a presentation from a computer, your attendee connects immediately and seamlessly through a browser using HTML5. Your attendee can join a presentation through any of several methods.

Attendees can also join a presentation from an iOS or Android device. To do so, they must download the BeyondTrust presentation app. For details, see the BeyondTrust documentation for supporting the appropriate device.

Your administrator can determine which messages your attendee sees, if any, before the presentation begins. Messages that may be displayed include an attendee agreement and a greeting. Depending on the presentation state, your attendee may see a message that the presenter has stopped presenting, or that the presentation has ended and they may close the browser. If no one is available to give the presentation, an orphaned presentation message may also be displayed.

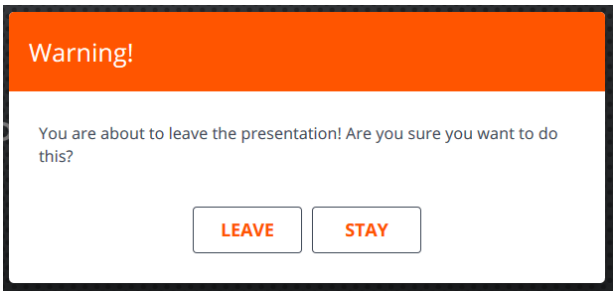


During a presentation, attendees can view your desktop or selected applications and can also chat with you alone, or with you and other attendees.

By clicking on the orange B icon, attendees can choose actions to perform from the tool bar. They can leave the session, view presentation details, go to fullscreen, change the screen size, and toggle the chat panel.

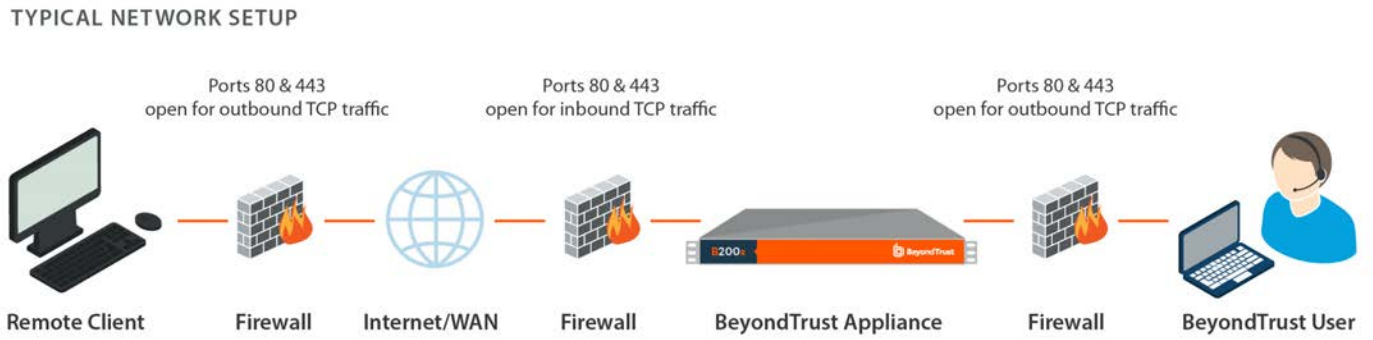
You can also choose to share mouse and keyboard control with attendees. The tool bar and chat panel locks in place when they have control. Only one attendee at a time can have control of your computer. You can always cancel the attendee's control at any time.

At the end of the presentation, attendees receives a message asking if they would like to leave the presentation.



Ports and Firewalls

BeyondTrust solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.



- Ports 80 and 443 must be open for outbound TCP traffic on the remote system's and local user's firewalls. More ports may be available depending on your build. The diagram shows a typical network setup; more details can be found in the Secure Remote Access Appliance Hardware Installation Guide.
- Internet security software such as software firewalls must not block BeyondTrust executable files from downloading. Some examples of software firewalls include McAfee Security, Norton Security, and Zone Alarm. If you do have a software firewall, you may experience some connection issues. To avoid such issues, configure your firewall settings to allow the following executables, wherein {uid} is a unique identifier consisting of letter and numbers:
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe

  For assistance with your firewall configuration, please contact the manufacturer of your firewall software.
- Example firewall rules based on appliance location can be found at www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/firewall-rules.htm.

If you should still have difficulty making a connection, contact BeyondTrust Technical Support at www.beyondtrust.com/support

Troubleshoot BeyondTrust Representative Console Connections

1. Make sure you are logged into the representative console.
2. If you have selected to use the representative list, make sure that your display name is visible on your public site. You can change this status from the **Support** menu or the system tray icon by selecting or deselecting **Showing on Representative List**.
3. Try going through the initial steps of starting a BeyondTrust session on your own computer. Are you able to download the customer client?
4. Verify that the remote customer has internet connectivity. Is your customer able to get to your public site?
5. Lead your customer through the same steps you took when testing the customer client download in step 3 of this troubleshooter. Is your customer able to download the customer client?
6. If the download does not initiate when your customer clicks on your name, enters a session key, or enters a support request, have the customer hold down the **Ctrl** key and press **F5**. This should clear the browser cache, ensuring that the customer is not attempting to download an expired version of the customer client.
7. If clearing the browser cache does not work and your customer is not prompted to save or run a file, the firewall your customer is behind may be blocking the download. Contact BeyondTrust Technical Support at www.beyondtrust.com/support for a work-around.
8. Have your remote customer uninstall the BeyondTrust client, reboot their computer, and then run the executable file again.
9. Make sure your remote customer has disabled any software firewalls that might be blocking outbound connections. Some examples of these include McAfee Security, Norton Security, and Zone Alarm. These firewalls will occasionally block outbound connections even after being disabled and may need to be uninstalled.
10. Alternately, your customer may have been prompted to allow or disallow/block the customer client when they ran the downloaded client. If the customer clicked **Disallow/Block**, have them open the internet security software on their computer and change the entry for **bomgar-scc.exe** to **Allow/Permit**. Have your customer go through the download process again but click **Save** rather than **Run**. Then have them run the executable again and click **Allow/Permit**. If the session still does not connect, have the customer run the saved executable again - they should not be prompted the second time, and the session should connect.
11. Check if your customer is behind a proxy server. Ensure that your customer has correctly entered their credentials to permit the customer client to connect to you.
12. If following these steps fails to make a connection, contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Disclaimers, Licensing Restrictions, and Tech Support

Disclaimers

This document is provided for information purposes only. BeyondTrust Corporation may change the contents hereof without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. BeyondTrust Corporation specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionality, services, and processes described herein are subject to change without notice.

Licensing Restrictions

One BeyondTrust Remote Support license enables one support representative at a time to troubleshoot an unlimited number of remote computers, whether attended or unattended. Although multiple accounts may exist on the same license, two or more licenses (one per concurrent support representative) are required to enable multiple support representatives to troubleshoot simultaneously.

Tech Support

At BeyondTrust, we are committed to offering the highest quality service by ensuring that our customers have everything they need to operate with maximum productivity. Should you need any assistance, please contact www.beyondtrust.com/support.

Technical support is provided with annual purchase of our maintenance plan.