



BeyondTrust

Privileged Remote Access 23.2 Access Console User Guide

Table of Contents

BeyondTrust Access Console	6
Install the Access Console	7
Log in to the PRA Access Console	8
Use Passwordless Login	8
Infrastructure Access Mode	8
Use Kerberos Server	8
Access Console User Interface	10
Change Settings and Preferences in the Access Console	11
Changing Settings	11
Use the CLI for the Access Console	15
Entering Commands	15
Initiate a Session	15
Executing onExternalToolClicked() Callback	15
Use Session Specific Subcommands	16
SSH	16
RDP	16
DB	16
Protocol tunnel	17
Use Other Subcommands	17
List	17
Close	17
Use Infrastructure Access Mode	18
Jump Interface: Use Jump Items to Access Remote Systems	20
Copy Jump Items	20
Jump to a Jump Item	20
Schedule	21
Notification	21
Ticket ID	21
Authorization	22
Use Jump Clients to Access Remote Endpoints	25
Use a Jump Client	25

Sort Jump Clients	25
Search for a Jump Client	25
Jump Client Details Pane	25
Wake-On-Lan (WOL)	26
Copy Jump Items	27
Jump Client Properties	27
Use Remote Jump for Unattended Access to Computers on a Separate Network	29
Create a Remote Jump Shortcut	29
Use a Remote Jump Shortcut	30
Use Local Jump for Unattended Access to Computers on Your Local Network	31
Create a Local Jump Shortcut	31
Use a Local Jump Shortcut	32
Use RDP to Access a Remote Windows Endpoint	33
Create an RDP Shortcut	33
Inject Credentials	35
Use an RDP Shortcut	36
Use VNC to Access a Remote Windows Endpoint	37
Create a VNC Shortcut	37
Use a VNC Shortcut	38
Use a Protocol Tunnel Jump to Make a TCP Connection to a Remote System	39
Create a Protocol Tunnel Jump Shortcut	39
Use a Protocol Tunnel Jump Shortcut	40
Stipulations to Correct Functioning	41
Use Shell Jump to Access a Remote Network Device	42
Create a Shell Jump Shortcut	42
Use a Shell Jump Shortcut	44
Configure Shell Prompt Filtering:	44
Configure Command Filtering:	44
Use Credential Injection with SUDO on a Linux Endpoint	45
Use a Web Jump to Access Web Services	46
Create a Web Jump Shortcut	46
Use a Web Jump Shortcut	48
Upload and Download Files using a Web Jump Shortcut	49

Use Credential Injection	49
Access Toolset	51
Access Session Overview and Tools	51
Session Tools	52
Log Into Remote Systems Using Credential Injection from the Access Console	53
Install and Configure the Endpoint Credential Manager	54
System Requirements	54
Configure a Connection to Your Credential Store	56
Use Credential Injection to Access Remote Systems	57
Choose from Favorite Credentials for Injection	57
Check Out and Check In Vault Credentials	57
Control the Remote Endpoint with Screen Sharing	59
Screen Sharing Options	59
Screen Sharing Tools	60
Use Annotations to Draw on the Remote Screen of the Endpoint	62
Enabling Annotations	62
View Multiple Monitors on the Remote Endpoint	64
Using the Display Icon	65
RDP Session Multi-Monitor Support	65
Using the Displays Tab	65
File Transfer to and from the Remote Endpoint	67
File Transfer Tools	67
Open the Command Shell on the Remote Endpoint Using the Access Console	69
Command Shell Tools	69
View System Information on the Remote Endpoint	71
System Information Tools	72
Access the Registry Editor on the Remote Endpoint	73
Registry Editor Tools	73
Session Management and Team Collaboration	75
View Active Access Sessions	75
Use the Dashboard to Administer Team Members	76
Chat with Other Users	77
Share your Screen with Another User	78

Share My Screen Tools	78
Sharing User	78
Viewing User	79
Share a Session with Other Users	80
Chat with Other Users During a Shared Session	81
Use Extended Availability to Remain Accessible when Not Logged In	82
Email Notification & Invitation	82
Invite an External User to Join an Access Session	83
Ports and Firewalls	85

BeyondTrust Access Console

This guide is designed to help you install the BeyondTrust access console onto your computer and understand the features of the solution. BeyondTrust Privileged Remote Access enables you to access remote endpoints by connecting to them through the BeyondTrust Appliance B Series.

Use this guide only after an administrator has performed the initial setup and configuration of the B Series Appliance as detailed in the [BeyondTrust Appliance B Series Hardware Installation Guide](#). Once BeyondTrust is properly installed, you can begin accessing your endpoints immediately. Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Install the Access Console

In any web browser, go to the URL of your B Series 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 access console. The option defaults 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 access console, you can choose **Run BeyondTrust Access Console Now** and/or **Run at Startup**. Then click **Finish**.



Note: *If you choose **Run BeyondTrust Access Console Now** during installation, a login prompt appears on your screen.*

Log in to the PRA Access Console

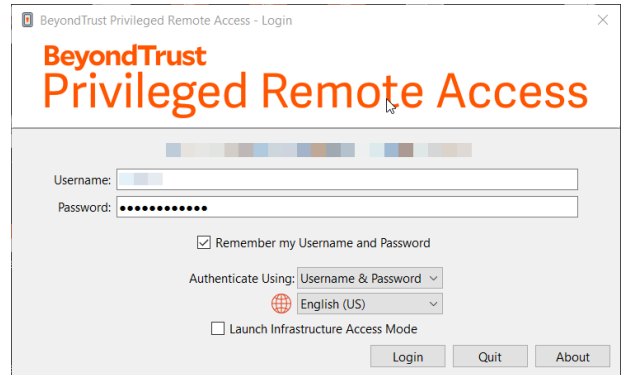
After installing the BeyondTrust console, launch the access console from its directory location as defined during installation.



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

If the **Login Agreement** has been enabled, you must click **Accept** to proceed.

At the prompt, enter your username and password.



Use Passwordless Login


FIDO2-certified authenticators can be used to securely log in to the desktop access console (Windows only), privileged web access console, and the /login administrative interface without entering your password. You can register up to 10 authenticators.

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

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

Infrastructure Access Mode

Advanced users might prefer to use Infrastructure Access Mode. This is primarily for quick access to protocol and database tunneling, and BYOT sessions. If desired, check **Launch Infrastructure Access Mode**. Infrastructure Access Mode is not available on Linux systems.



Note: If more than one language is enabled for your site, select the language you want to use from the dropdown menu.

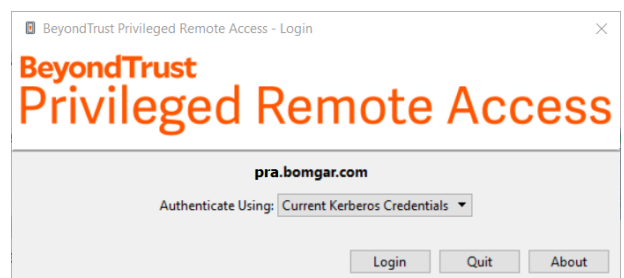
If two-factor authentication is enabled for your account, enter the code from the authenticator app.

Use Kerberos Server

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 access 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 **Enable Saved Logins** to have the console save your username and password. This option can be enabled or disabled from **/login > Management > Security**.



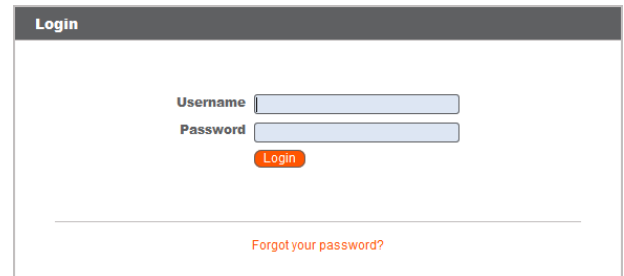
Once you log in, the console opens, and a BeyondTrust icon appears in your computer's system tray.



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

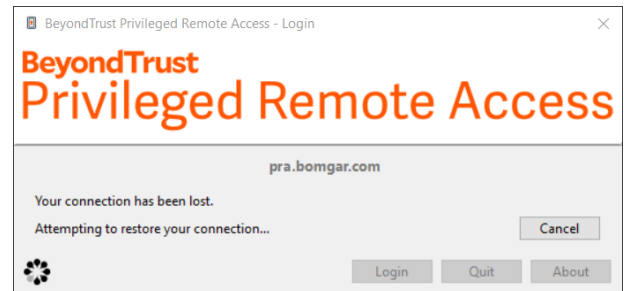


Note: If you forget your password, go to `/login` and click the **Forgot Your Password?** link. This is an option that is set by your administrator. If you do not have this option, please contact your administrator.



If you lose your connection, the access console attempts to reconnect for 60 seconds. If your connection is restored within this time, your access console reopens, restoring all of your open sessions. If the connection cannot be restored within this time, you are prompted to retry login or quit.

If you are logged into the access 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 access console, a **What's New** dialog appears automatically upon login for all non-invited users. This dialog may be viewed at any time through the **Help** menu (**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 user signs in from.

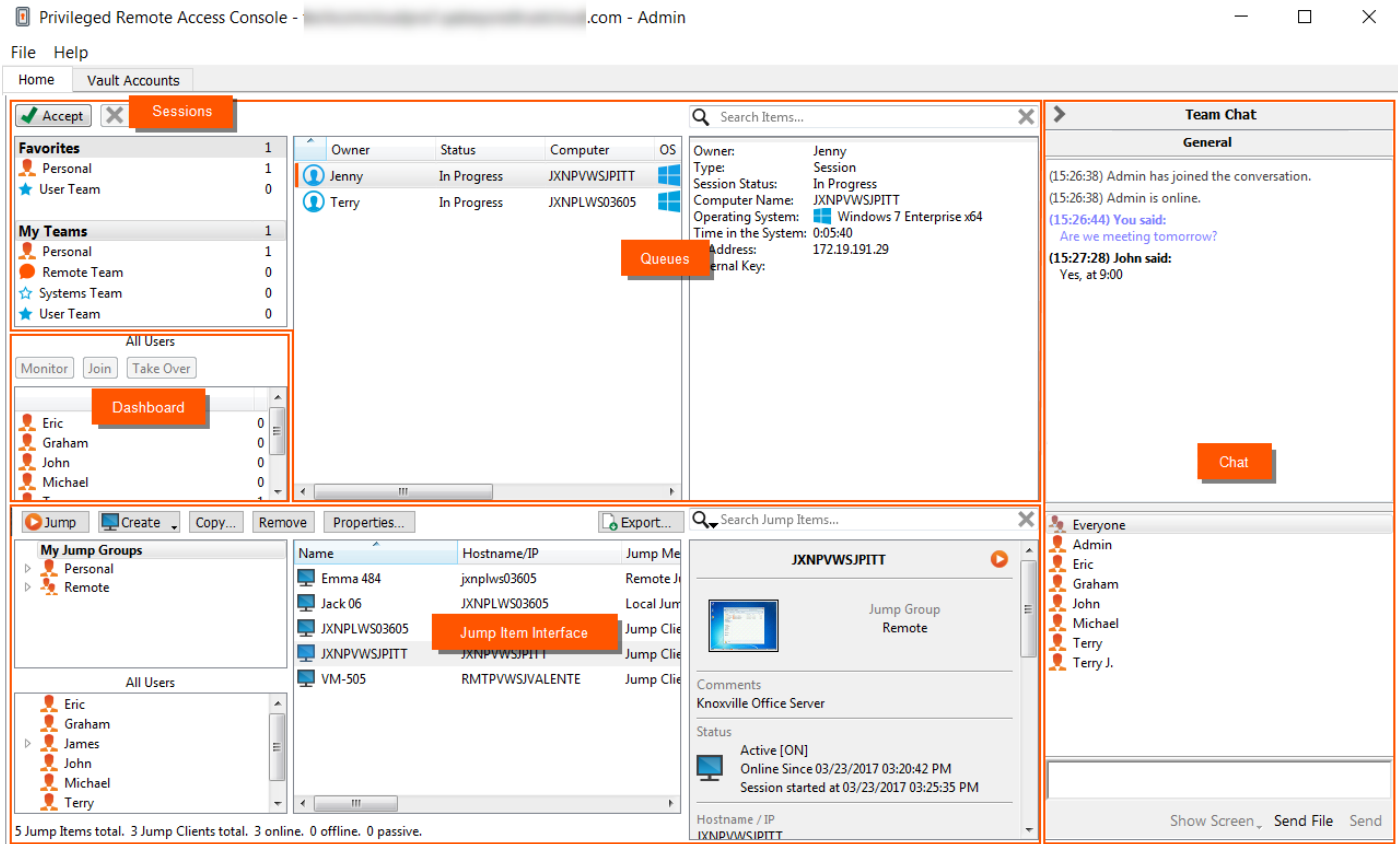


For more information, please see the following:

- On setting up the login agreement, please see [Site Configuration: Set HTTP Ports, Enable Prerequisite Login Agreement](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/site-configuration.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/site-configuration.htm>
- On invited users, "[Invite an External User to Join an Access Session](#)" on page 83
- On using Infrastructure Access Mode, "[Use Infrastructure Access Mode](#)" on page 18

Access Console User Interface

The access console contains several panels, providing tools and information about sessions.



Sessions: Manage multiple remote sessions at the same time.

Queues: Queues list sessions currently running as well as requests to share sessions with any member of a team. Details about the remote system being accessed 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.

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

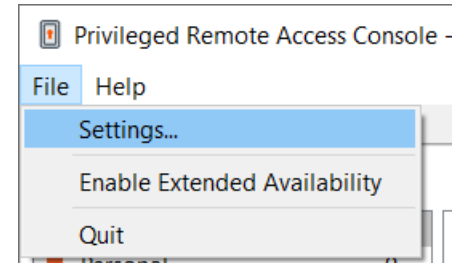
Chat: Chat with other logged in users. You also can share your screen with a team member without requiring a session.

Change Settings and Preferences in the Access Console

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

In general, you can configure the console settings according to your preferences. However, your BeyondTrust administrator might choose to manage your settings, enforcing those managed settings if desired.

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 click **OK** to acknowledge the changes.

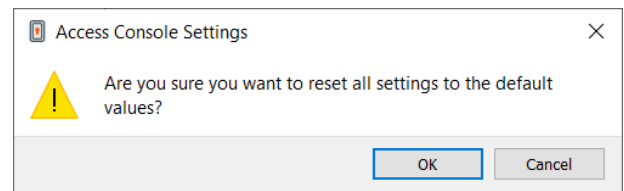


Changing Settings



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 are grayed out, and they are not locally configurable. Please see your administrator or [Manage Access Console Settings at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/access-console-settings.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/access-console-settings.htm) for more information.

The **Access Console Settings** window includes a **Restore Defaults** button in the lower-left corner of the window. This button returns 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: If any of the defaults are forced by your administrator, you are unable to configure them.

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

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.

You can choose to change your display mode. Options include **OS Setting** (default), **Light Mode**, and **Dark Mode**.

 **Note:** *The Dark Mode option applies to Windows and macOS only.*

*In addition to switching the display mode within the access console, users can change it in **OS Settings** by selecting **Themes and related settings > Color > Choose your color**.*

The **CLI** section indicates if a Command Line Interface tool is installed for this installation of the Access Console. If it is not installed, you can choose to install it by clicking **Install**.

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.

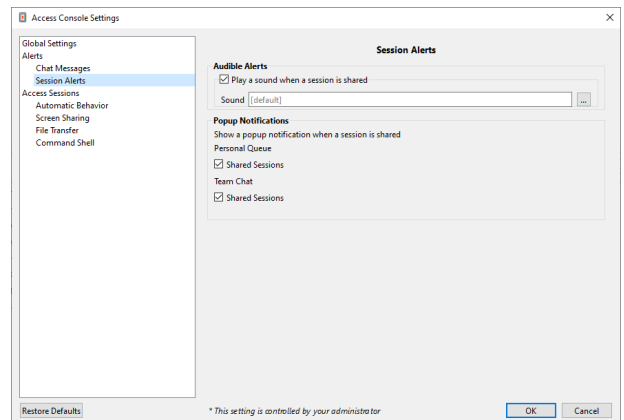
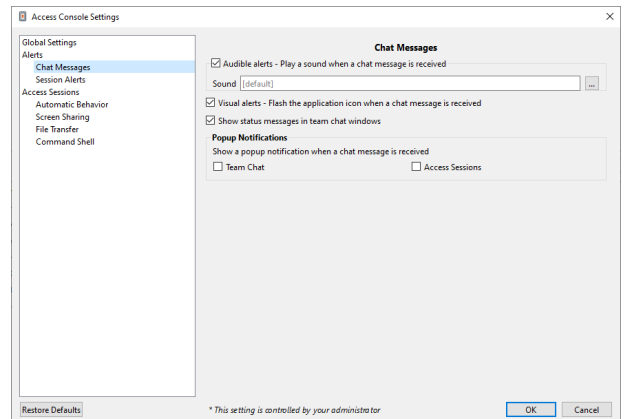
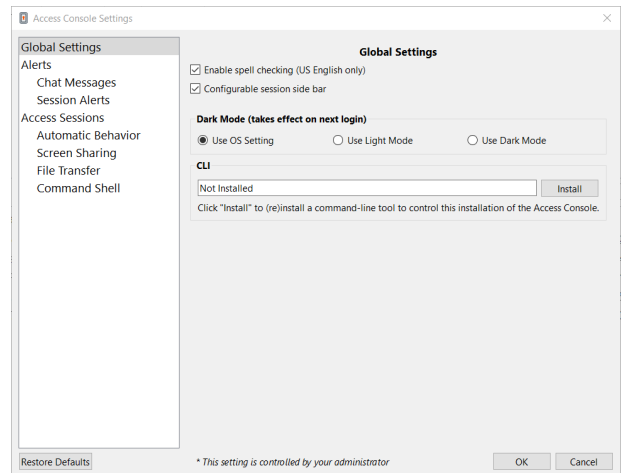
If you would like to upload a custom sound for chat messages, click the [...] button and select a WAV file on your computer. The file can be no larger than 1MB.

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.

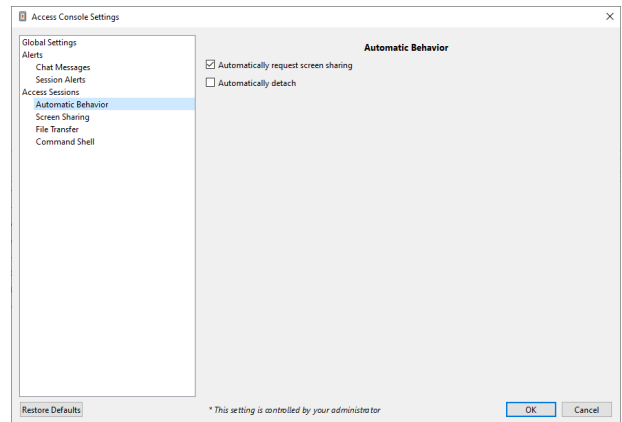
Choose if you want to hear an audible alert when another user requests to share a session with you. If you would like to upload a custom sound for shared sessions, click the [...] button and select a WAV file on your computer. The file can be no larger than 1MB.

You also can choose to receive pop-up notifications for certain events. These notifications will 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 want to automatically start screen sharing when you begin a session.

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

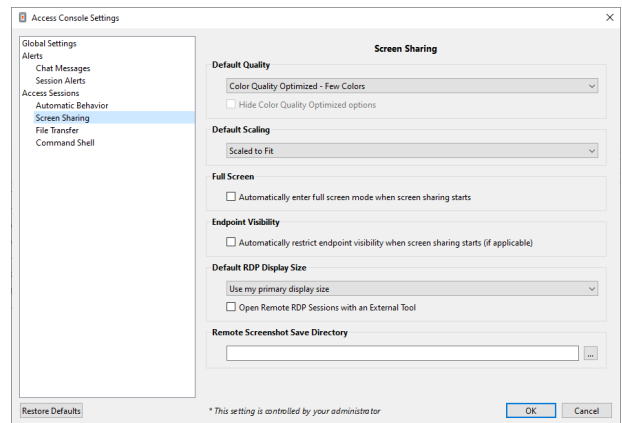


Set the default quality and size for a screen sharing session. When screen sharing starts, you can automatically enter full screen mode, which in turn can automatically collapse the chat bar.

Additionally, 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.

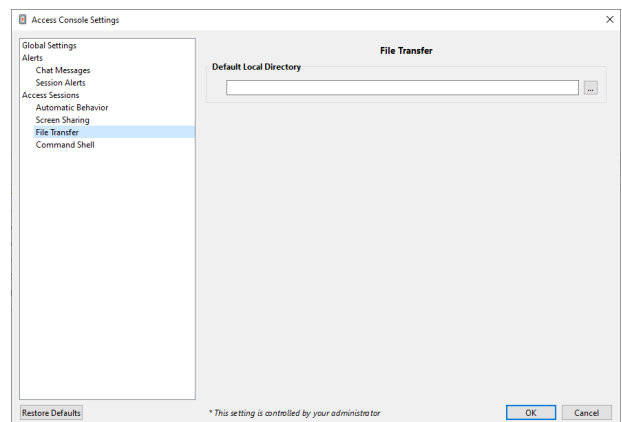
An option allows you to open a PRA connection expanded across all the monitors on the client computer regardless of the client monitor configuration. With this feature, you can fully utilize all the monitors connected to the client computer, therefore being able to adjust screen sizing and scaling during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



If you want to use your own RDP tool, check **Open remote RDP Sessions with an External Tool**.

For easier access to screenshots you capture from the console, set the default directory where you wish to 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.

If you want to use your own SSH tool, check **Open Shell Jump Sessions with an External Tool**. This setting applies to both command shell and Shell Jump.

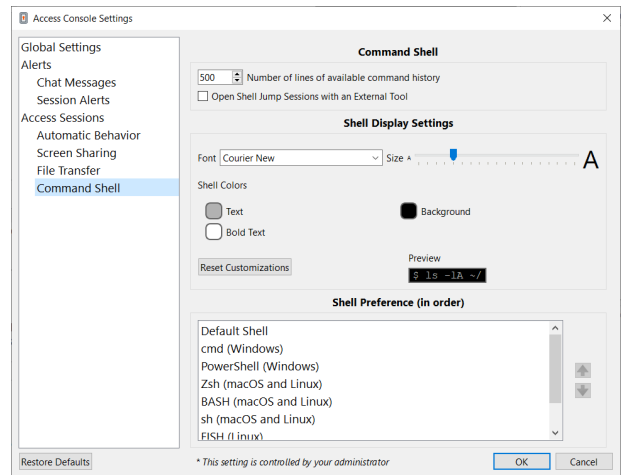


Note: The **Open Shell Jump Sessions with an External Tool** setting has limitations when used with the command shell. The proxy is for the shell only; it is not a full SSH tunnel. File transfers, for example, must still use the existing tools on the Jump Client.



IMPORTANT!

In order to use your own tool, you must enable **Protocol Tunnel Jump** in **/login > Users & Security > Users > Jump Technology > Protocol Tunnel Jump**.



You can change the command shell display by selecting the font type, font size, text color, and background color.

Several options for the default shell are available, including Windows Command Prompt, PowerShell, Zsh, Bash, sh, fish, and tcsh. To set the shell preference order, select each shell and use the arrow buttons beside the list to move the selected shell up or down. Sessions start using the first available shell for the session.



For more information about using the Command Line Interface tool for the access console, please see **"Use the CLI for the Access Console"** on page 15.

Use the CLI for the Access Console

The Command Line Interface (CLI) tool allows you to initiate and manage remote sessions directly from the command line.

To use the CLI tool, you must be logged in to the access console, and the CLI tool must be installed. It is installed from **Global Settings**. During installation, you might receive instructions to add the installation location to the PATH, or it may be added to the PATH by the installation process.

Once installed, enter commands in a terminal or *run* dialog to interact with the logged-in rep instance.



Note: You must be logged in to the access console for commands to work.

Entering Commands

Enter a single CLI command with sub-commands.



Example:

```
lbt ssh <user>@<host>
```

Subcommands take the form:

```
bt <command>
```

Initiate a Session

Search for a Vault account by name (for types that can inject) and a Jump Item by name. Jump Item searches are restricted to the type represented by the command. For example, **bt ssh** searches only Shell Jump Items.

If only one of each searched name is found, the session starts with that Jump Item and credential. If more than one result is found, you are prompted to choose the correct account and/or Jump Item.

A flag can be set flag to output the tunnel information in a format for use by another process or script, so that session calls can be piped to other functions or included in automated tasks such as VS code tasks. If this flag is set, the tunnel information prints, but the connection and external tool do not open.

Executing onExternalToolClicked() Callback

For all types except SSH, the representative can attempt to execute the **onExternalToolClicked()** callback for the given type before returning control to the CLI tool, rather than transferring that logic to the CLI tool itself.

For SSH, the SSH session replaces the CLI tool process.

Use Session Specific Subcommands

SSH

SSH subcommands take the form:

```
ssh <account>@<host>
```

Once the session is established, it directly spawns the SSH process to connect to the local tunnel and exits.



Example: Create an SSH session:

```
bt ssh <user>@<host>
```

RDP

RDP subcommands take the form:

```
rdp <account>@<host>
```

Once the session is established, it

- spawns the default RDP client.
- prints the tunnel information to the CLI for informational purposes.
- exits.



Example: To open the RDP tool, enter:

```
bt rdp <user>@<host>
```

DB

DB subcommands take the form:

```
db <account>@<host>
```

Once the session is established, it:

- spawns the DB client for the selected DB type, if possible. Part of the return value must be DB type and/or command to try.
- prints the DB connection information.

- exits.

Protocol tunnel

Protocol tunnel subcommands take the form:

```
pt <host>
```

There is no credential injection for protocol tunnels.

Once the session is established, it prints the tunnel definitions and exits.

Because the tunnel is generic, it cannot spawn a specific tool.

Use Other Subcommands

List

List subcommands take the form:

```
list
```

The list subcommand shows connected sessions by Jump Item name.

Close


Close subcommands take the form:

```
close <session>
```

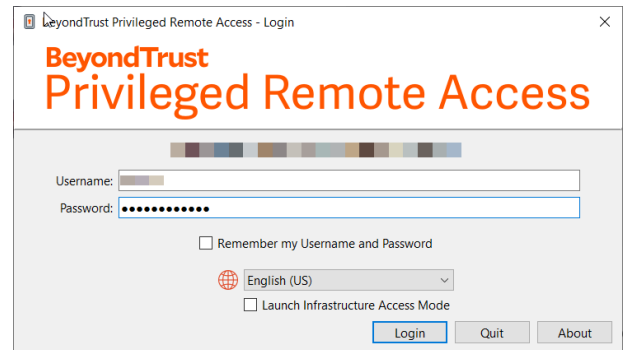
The close subcommand closes the tunnel for the given session.

Use Infrastructure Access Mode

Advanced users, such as developers, can select Infrastructure Access Mode when logging in to the console. This provides a simpler console, available from the system tray or menu bar. This is convenient for protocol and database tunneling, and BYOT sessions, but other session types are also supported.

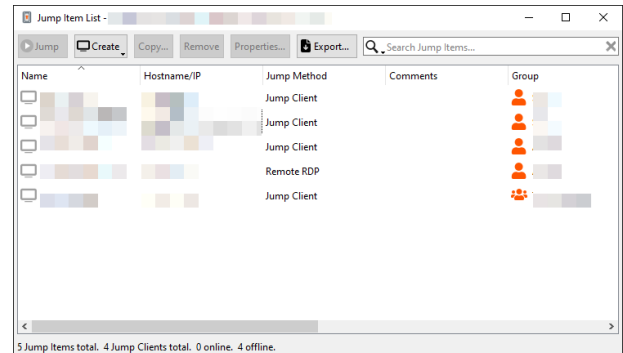
 **Note:** Infrastructure Access Mode is not available on Linux systems.

To start Infrastructure Access Mode, check **Launch Infrastructure Access Mode** on the console authentication screen. If you have previously enabled Infrastructure Access Mode, the option is checked by default.



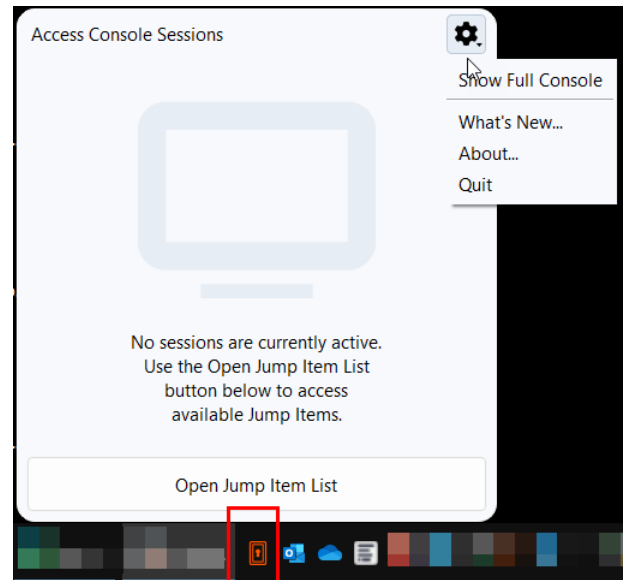
Once logged in, a **Jump Item List** window displays, and an icon appears in the system tray (Windows) or menu bar (macOS). From the list, you can select and open a session in the usual manner. If you close the session window, you can re-open it by clicking the task bar Infrastructure Access Mode icon to open the menu, and then click **Show Session**.

The first time you close all windows, a notification appears to remind you that Infrastructure Access Mode is still running and is available from the icon in the system tray or menu bar.



From the icon, you can open the Jump Item List window. Under the icon settings menu, you can switch to the full access console. The full console is required to begin a chat session or accept a session invite, and for some session types. You can close the full access console when it is no longer required and continue using the console in Infrastructure Access Mode.

You can view and close active sessions from the icon options, and quit Infrastructure Access Mode from the icon settings menu.

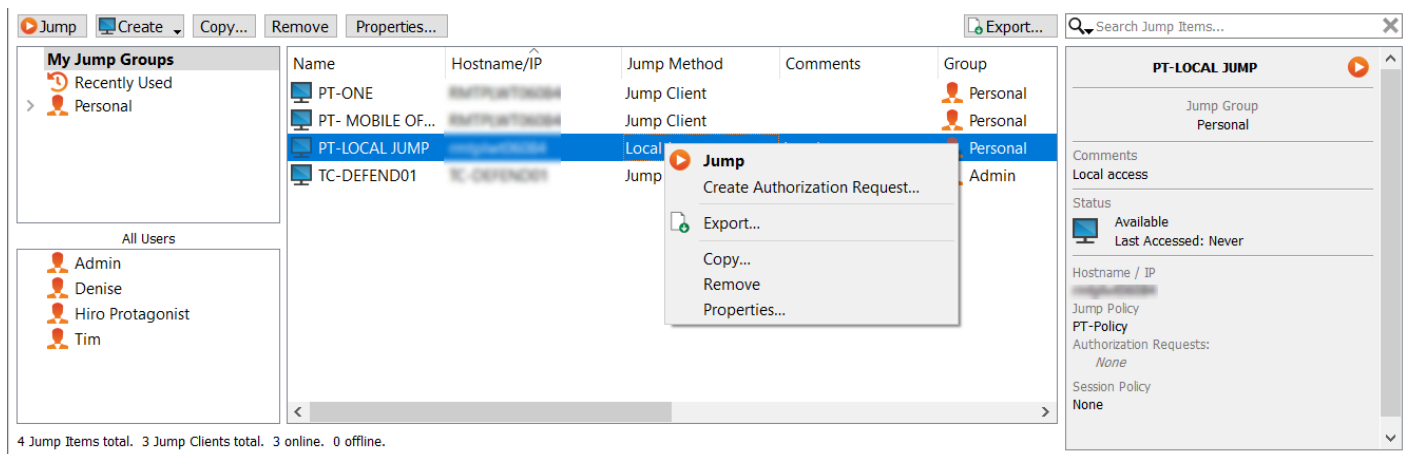


Jump Interface: Use Jump Items to Access Remote Systems

The Jump interface appears in the bottom half of the access console, listing the Jump Items available to you. The list may contain both active and passive Jump Clients, as well as Jump shortcuts for Remote Jumps, Local Jumps, RDP sessions, VNC sessions, Protocol Tunnel Jumps, Shell Jumps, and Web Jumps. Jump Item availability, including whether or not the Jump Item is in use, is listed in the **Status** column.

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.



Copy Jump Items

Jump Items can be copied and can belong to multiple Jump Groups. This includes Jump Client items, providing administrators with the ability to set separate policies and group permissions without requiring an additional Jump Client installation on the target endpoint. Users with the appropriate permissions see the option to **Copy** Jump Items in the Access Console by right-clicking the item. Users can perform this function on multiple Jump Items as well.

This feature enables admins and users to effectively manage different policies for Jump Items and Jump Clients without the need to create a new Jump Item. This functionality enables users to limit the number of clients necessary to enable Jump Client sessions, and limits manual administrative tasks when defining access pathways for users.

Jump to a Jump Item

Browse through groups for the computer you wish to access. To facilitate browsing the Jump Items list, you may drag the columns into any order you wish, and then sort a column by clicking the column header. The access console remembers the column order and the sort order the next time the access console is launched.

Name	Hostname/IP	Jump Method	Comments	Group
Basement Server	172.27.131.161	Shell Jump		Personal
BUILDING 1	RMTPVWSVALENTE	Jump Client		wscott
Gracie Lou Freebush's Lapt...	JXNPLWS03605	Remote Jump		User Systems
JXNPLWS04033	JXNPLWS04033	Jump Client		Admin
LS-RED04	LS-RED04	Jump Client		Admin
RMTPVWS04255	RMTPVWS04255	Jump Client	Jose's laptop	wscott
Scott's Laptop	RMTPVWS04255	Local VNC	Building A Lobby	wscott
Server Room VM	RMTPVWSVALENTE	Jump Client		wscott

In addition to browsing for Jump Items, 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, FQDN, 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 attempts to start a session with the remote computer.

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 starts immediately. If multiple Jump Items are returned, select one of the Jump Items listed in the selection window and click **OK**.

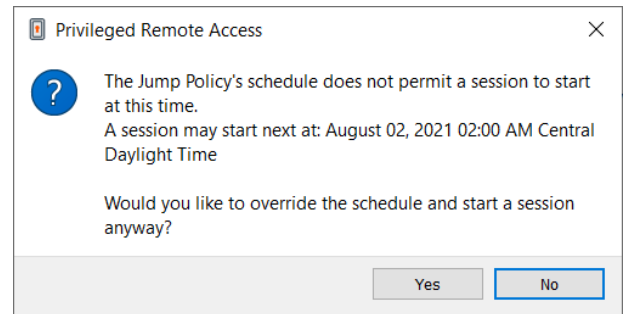


Note: For details about scripting, see [Access Console Scripting and Client Scripting API](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script) at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script.

If a Jump Policy is applied to the Jump Item, that policy affects how and/or when a Jump Item may be accessed.

Schedule

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 from occurring. A prompt informs you of the policy restrictions and provides the date and time when this Jump Item is next available for access.



Notification

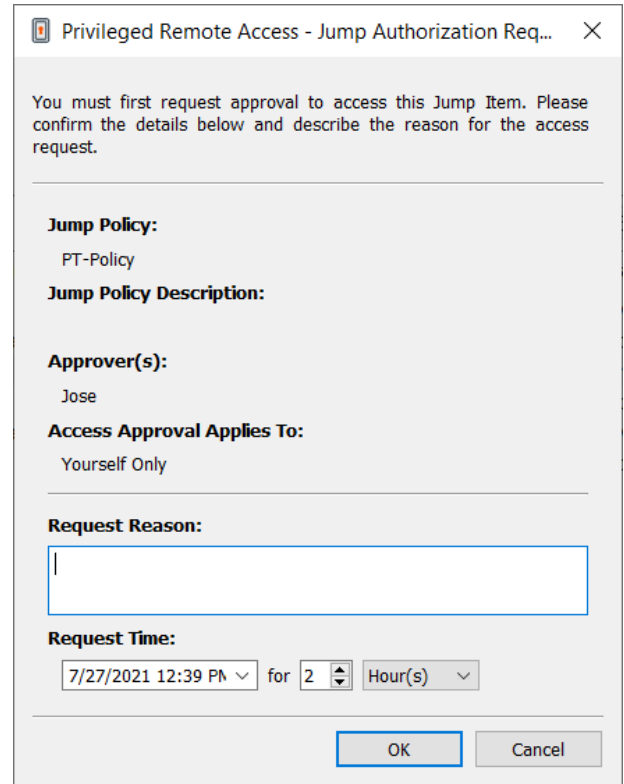
If a Jump Policy is configured to send a notification on session start or end, then an attempt to access a Jump Item alerts you that an email will be sent. You can choose to proceed with the Jump and send a notification, or you can cancel the Jump.

Ticket ID

If a Jump Policy requires entry of a ticket ID from your external ITSM or ticket ID system before the Jump can be performed, a dialog opens. In the dialog, enter the ticket ID you need, authorizing access to this Jump Item.

Authorization

If a Jump Policy requires authorization before the Jump can be performed, a dialog opens. In the dialog, enter the reason you need to access this Jump Item. Then enter the date and time at which you wish authorization to begin, as well as how long you require access to the Jump Item. Both the request reason and the request time are visible to the approver and help them decide whether to approve or deny access.



The screenshot shows a dialog box titled "Privileged Remote Access - Jump Authorization Req...". The main text reads: "You must first request approval to access this Jump Item. Please confirm the details below and describe the reason for the access request." Below this, the following fields are visible:

- Jump Policy:** PT-Policy
- Jump Policy Description:**
- Approver(s):** Jose
- Access Approval Applies To:** Yourself Only
- Request Reason:** A text input field with a vertical cursor.
- Request Time:** A date and time selector showing "7/27/2021 12:39 PM", a duration selector showing "2" and "Hour(s)".

At the bottom right, there are "OK" and "Cancel" buttons.

When you click **OK**, an email is sent to the addresses defined as approvers for this policy. This email contains a URL where an approver can see the request, add comments, and either approve or deny the request.

If a request was approved by one person, a second can access the URL to override approval and deny the request. If a request was denied, then any other approvers accessing the site can see the details but cannot override the denied status. If a user has already joined an approved session, that access cannot be denied. Although other approvers can see the email address of the person who approved or denied the request, the requestor cannot. Based on the Jump Policy settings, an approved request grants access either to any user who can see and request access to that Jump Client or only to the user who requested access.

In the Jump interface, the Jump Item's details pane displays the status of any authorization requests as either pending, approved, approved only for a different user, or denied. When an approver responds to a request, a pop-up notification appears on the requestor's screen alerting them that access has been either approved or denied. If the requestor has a configured email address, an email notification is also sent to the requestor.

When a user Jumps to a Jump Item which has been approved for access, a notification alerts the user to any comments left by the approver.

When approval has been granted to a Jump Item, that Jump Item becomes available either to any user who can see and request access to that Jump Item or only to the user who requested access. This is determined by the Jump Policy.



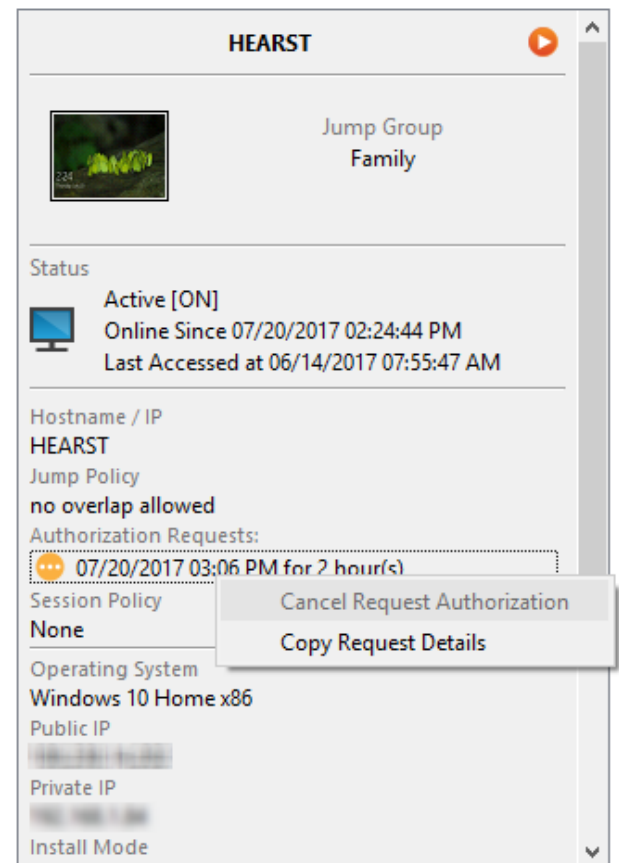
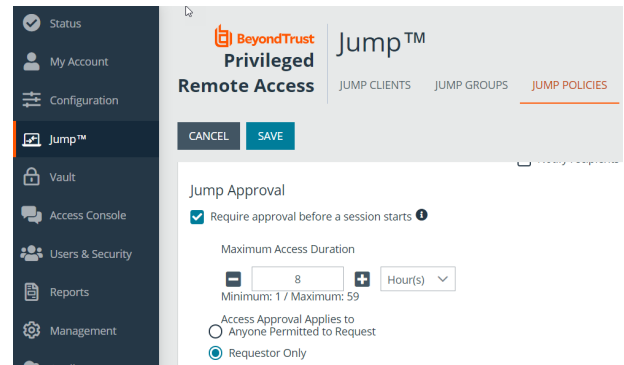
Note: Multiple requests may be sent for different times. The requested access times can overlap if the Jump approval request is for the **Requestor Only**. Access time cannot overlap if the approval is for **Anyone Permitted to Request**. If a request is denied, then a second request may be sent for the same time.

Revoke an Access Approval Request

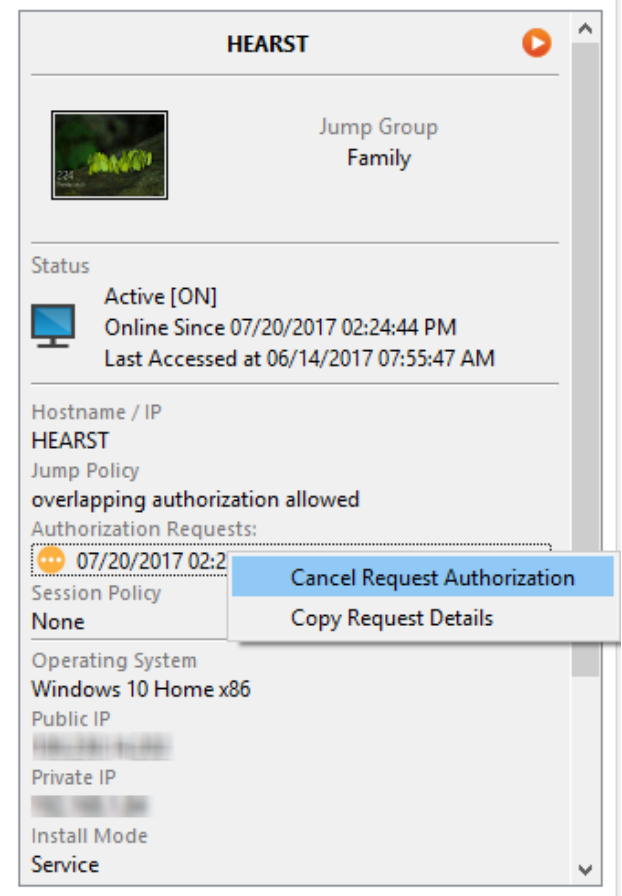
Permission to revoke approved access requests is controlled by Jump Policy. Any user who can approve requests on the Jump Policy can cancel requests, subject to the approval type. In the **/login** web management interface, go to **Jump > Jump Policies**. Under **Jump Approval** you have two options:

- **Anyone Permitted to Request**
- **Requestor Only**

If the Jump Policy is set to **requestor Only**, and an Access Request is presently approved for User A, User B is asked to create a new Access Request if they attempt to Jump to the Jump Item, since that request does not apply to them. Additionally, if User B attempts to cancel the Access Approval Request, the option is grayed out. The only user who can cancel the approved request is User A, because they are the approved user for the request.



However, if the Jump Policy is set to **Anyone Permitted to Request**, and an Access Request is presently approved for User A, User B is allowed to start a new session with the Jump Item if they attempt to Jump to it. In addition, anyone with permission to access the Jump Item is allowed to cancel / revoke the request.



HEARST

Jump Group
Family

Status
Active [ON]
Online Since 07/20/2017 02:24:44 PM
Last Accessed at 06/14/2017 07:55:47 AM

Hostname / IP
HEARST

Jump Policy
overlapping authorization allowed

Authorization Requests:
07/20/2017 02:2

Session Policy
None

Operating System
Windows 10 Home x86

Public IP
[REDACTED]

Private IP
[REDACTED]

Install Mode
Service

Context Menu:
Cancel Request Authorization
Copy Request Details

Use Jump Clients to Access Remote Endpoints

To access an individual Windows, Mac, or Linux computer that is not on an accessible network, install a Jump Client on that system from the **/login > Jump > Jump Clients** page. Jump Clients appear in the Jump interface along with Jump Item shortcuts.

Use a Jump Client

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



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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Sort Jump Clients

Browse through groups for the computer you wish to access. To facilitate browsing the Jump Items list, you may drag the columns into any order you wish, and then sort a column by clicking the column header. The access console remembers the column order and the sort order the next time the access console is launched.

Name	Hostname/IP	Jump Method	Comments	Group
Basement Server	172.27.131.161	Shell Jump		Personal
BUILDING 1	RMTPVWSVALENTE	Jump Client		wscott
Gracie Lou Freebush's Lapt...	JXNPLWS03605	Remote Jump		User Systems
JXNPLWS04033	JXNPLWS04033	Jump Client		Admin
LS-REDD4	LS-REDD4	Jump Client		Admin
RMTPLWS04255	RMTPLWS04255	Jump Client	Jose's laptop	wscott
Scott's Laptop	RMTPLWS04255	Local VNC	Building A Lobby	wscott
Server Room VM	RMTPVWSVALENTE	Jump Client		wscott

Search for a Jump Client

In addition to browsing for Jump Items, 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**, **FQDN**, **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 B Series 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, the scheduled deletion date appears 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.

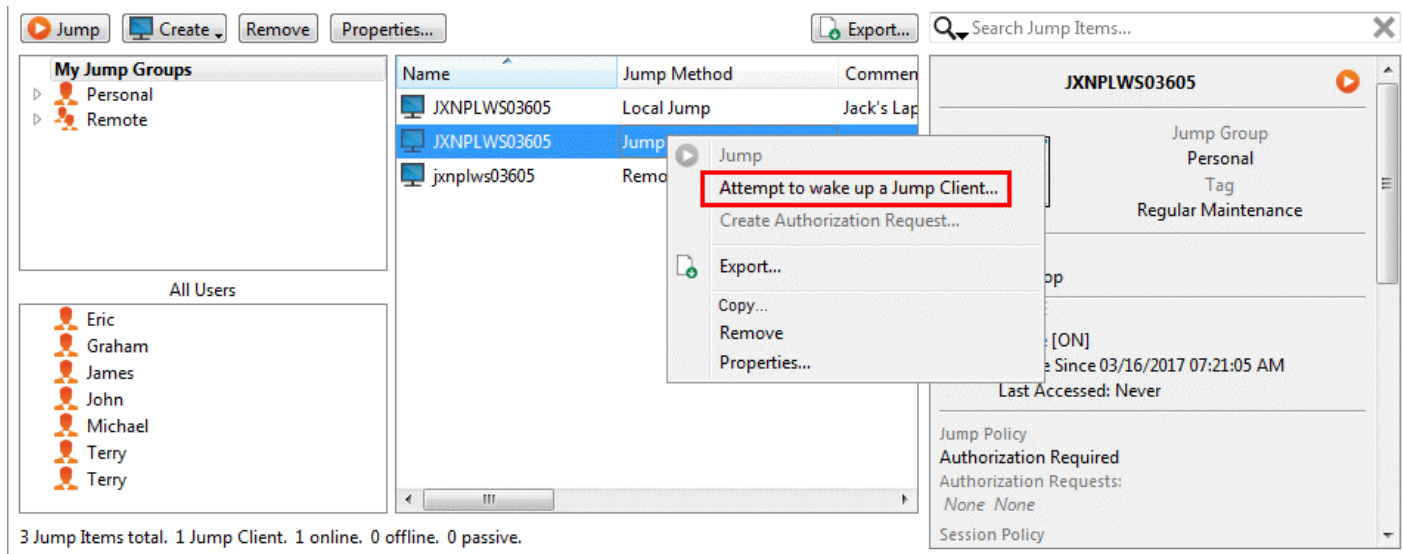


Note: WOL is not a BeyondTrust technology. The BeyondTrust software integrates with existing WOL systems. To use WOL through BeyondTrust, the system must have WOL enabled, and the network must allow WOL packets to be sent.

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 rep console. Attempt to wake the system by clicking the **Attempt to wake up Jump Client** option.



The screenshot displays the BeyondTrust console interface. On the left, there are sections for 'My Jump Groups' (Personal, Remote) and 'All Users' (Eric, Graham, James, John, Michael, Terry, Terry). The main area shows a table of Jump Clients:

Name	Jump Method	Comment
JXNPLWS03605	Local Jump	Jack's Lap
JXNPLWS03605	Jump	
jxnplws03605	Remo	

A context menu is open over the selected client 'JXNPLWS03605', with the option 'Attempt to wake up a Jump Client...' highlighted in red. The menu also includes options like 'Jump', 'Create Authorization Request...', 'Export...', 'Copy...', 'Remove', and 'Properties...'. On the right, a detailed view of the selected client shows its 'Jump Group' (Personal), 'Tag' (Regular Maintenance), and 'Last Accessed' status (Never).

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 B Series Appliance, and the B Series 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 it can 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 rep console.

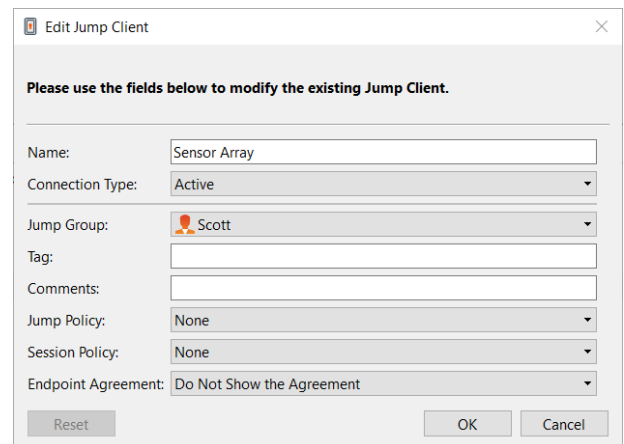
Copy Jump Items

Jump Items can be copied and can belong to multiple Jump Groups. This includes Jump Client items, providing administrators with the ability to set separate policies and group permissions without requiring an additional Jump Client installation on the target endpoint. Users with the appropriate permissions see the option to **Copy** Jump Items in the Access Console by right-clicking the item. Users can perform this function on multiple Jump Items as well.

This feature enables admins and users to effectively manage different policies for Jump Items and Jump Clients without the need to create a new Jump Item. This functionality enables users to limit the number of clients necessary to enable Jump Client sessions, and limits manual administrative tasks when defining access pathways for users.

Jump Client Properties

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




Note: To view the properties of multiple Jump Items, the items selected must be the same type (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.

Change a Jump Client's mode from the **Connection Type** dropdown. Active Jump Clients send statistics to the B Series Appliance on a defined interval. Passive Jump Clients send statistics to the B Series Appliance once a day or upon a manual check in.



Note: This feature is available only to customers who own an on-premises B Series Appliance. BeyondTrust Cloud customers do not have access to this feature.

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.

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

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

Choose an **Endpoint Agreement** to assign to this Jump Item. Depending on what is selected, an endpoint agreement is displayed. If there is no response, the agreement is automatically accepted or rejected.

If you no longer need access to a remote system, select the Jump Item and click **Remove**, or right-click on the Jump Item and select **Remove** from the menu. You may select multiple Jump Items 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 Jump Items list in the access console. If the Jump Client cannot contact the B Series Appliance at the time it is uninstalled, the affected item remains in its offline state. This setting is available at /login > Jump > Jump Clients. If a Jump Client goes offline and does not reconnect to the B Series Appliance for 180 days, it is automatically uninstalled from the target computer and is removed from the Jump interface.*

Use Remote Jump for Unattended Access to Computers on a Separate Network

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 and Linux 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.



Note: *Jumpoint is available for Windows and Linux systems. Jump Clients are needed for remote access to Mac computers. To Jump to a Windows computer without a Jump Client, that computer must have Remote Registry Service enabled (disabled by default in Vista) and must be on a domain. You cannot Jump to a mobile device, though Jump Technology is available from mobile BeyondTrust consoles.*

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, as well as Jump Clients and other types of Jump Item shortcuts.

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



Note: *To view the properties of multiple Jump Items, the items selected must be the same type (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 access console remembers your Jumpoint choice the next time you create this type of Jump Item. 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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

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

Choose an **Endpoint Agreement** to assign to this Jump Item. Depending on what is selected, an endpoint agreement is displayed. If there is no response, the agreement is automatically accepted or rejected.

Use a Remote Jump Shortcut

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

A dialog box opens for you to enter 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.



Note: Because a Remote Jump attempts to connect directly back through the appliance, the end machine must be able to communicate with the appliance as well. If this is not the case, you can use the Jump Zone Proxy feature to proxy the traffic through the Jumpoint.



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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Use Local Jump for Unattended Access to Computers on Your Local Network

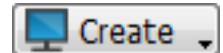
Local Jump enables a privileged user to connect to an unattended remote computer on their local network. Within the local area network, the BeyondTrust user's computer can initiate a session to a Windows system directly without using a Jumpoint, if appropriate user permissions are enabled. A Jumpoint is needed only when the BeyondTrust user's computer cannot access the target computer directly.



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

Create a 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 the same type (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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

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

Choose an **Endpoint Agreement** to assign to this Jump Item. Depending on what is selected, an endpoint agreement is displayed. If there is no response, the agreement is automatically accepted or rejected.

Use a Local Jump Shortcut

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

A dialog box opens for you to enter 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.



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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Use RDP to Access a Remote Windows Endpoint

Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with remote Windows and Linux systems. Because RDP sessions are proxied through a Jumpoint and 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 RDP through BeyondTrust, you must have access to a Jumpoint and must have the user account permission **Allowed Jump Methods: RDP via a Jumpoint**.



Note: You can use your own RDP tool for remote RDP sessions. For more information, please see "[Change Settings and Preferences in the Access Console](#)" on page 11.



IMPORTANT!

In order to use your own tool, you must enable **Protocol Tunnel Jump** in **/login > Users & Security > Users > Jump Technology > Protocol Tunnel Jump**.

Create an RDP Shortcut

To create a 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 with Jump Clients and other types of Jump Item shortcuts.

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



Note: To view the properties of multiple Jump Items, the items selected must be the same type (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 access console remembers your Jumpoint choice the next time you create this type of Jump Item. 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>** (for example, 10.10.24.127:40000).

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

Select the **Quality** at which to view the remote screen. This cannot be changed during the remote desktop protocol (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 **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.



Note: When **RemoteApp** or **BeyondTrust Remote Desktop Agent** is selected in the **SecureApp** section, the **Console Session** checkbox is unchecked. Remote applications cannot run in a console session on a RDP server.

To get more detailed information on the RDP session, check **Session Forensics**. For this feature to work, you must select an **RDP Service Account** for the Jumpoint being used. When checking this setting, the following reminder displays:

Enabling this feature requires the RDP server to be configured to receive the monitoring agent and an RDP Service Account to be configured with this Jumpoint. If these requirements are not met, all attempts to start a session will fail.



Note: In typical installations, the RDP service account requires privileges including access to create and control remote services and write access to remote file systems. We recommend that you create an AD account and use AD group policy settings to configure the permissions, however the exact permissions required depend on your AD configuration.

When **Session Forensics** is checked, the following additional details are logged:

- Focused window changed event
- Mouse click event
- Menu opened event
- New window opened event

To start a session with a remote application, configure the **SecureApp** section. The following dropdown options are available:

- **None:** When accessing a Remote RDP Jump Item, no application is launched.
- **RemoteApp:** The user can configure an application profile or command argument, which executes and opens an application on a remote server. To configure, select the **RemoteApp** option and enter the following information:
 - **Remote App Name:** Enter the name of the application you wish to connect to.
 - **Remote App Parameters:** Enter the profile details or command line arguments needed to open the application.
- **BeyondTrust Remote Desktop Agent:** This option facilitates passing parameters through an agent in order to launch applications on a remote host. To configure, select the **BeyondTrust Remote Desktop Agent** option and enter the following information:
 - **Executable Path:** Enter the path of the application the agent will connect to.
 - **Parameters:** Enter any parameters that you could normally type from a command line when launching the app on the remote system.



For more information on **Session Forensics** and **RDP service account**, please see [Jumpoint: Set Up Unattended Access to a Network > RDP Service Account](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm>.

Inject Credentials

The option to **Inject Credentials** is made available when the **BeyondTrust Remote Desktop Agent** type is selected. This option facilitates passing parameters as well as credentials through an agent in order to launch applications on a remote host. The first set of credentials is in the Jump definition. These are the credentials for the user account you'll use to log into the remote system. There is a secondary prompt for additional credentials, either manually provided or from a password vault. These secondary credentials are made available to the command line you define through the **%USERNAME%** and **%PASSWORD%** macros (additional macros shown below). This allows you to pass additional credentials to the application you are launching (e.g., SQL Server Management Studio). To configure, select the **BeyondTrust Remote Desktop Agent**: option and enter the following information:

- Enter the **Executable Path** and **Parameters** as described above.
- **Target System**: Enter the name of the system running the application.
- **Credential Type**: Enter the credential type as defined by the credential management system (e.g., SQL).

Macro Name	Result
%USERNAME%	username
%USERPRINCIPALNAME%	username@domain
%DOWNLEVELLOGONNAME%	domain\username
%DOMAIN%	domain
%PASSWORD%	password
%PASSWORDDRAW%	password (without any attempt to escape special characters)
%TARGETSYSTEM%	supplied target system value; in the case of SQL Server, this would be the SQL Server name.
%APPLICATIONNAME%	optional application name; in the case of SQL Server, this can be hard-coded to "SQL Server" or something similar.



Note: The **BeyondTrust Remote Desktop Agent** option requires a **BeyondTrust Remote Desktop Agent** to be preconfigured on the target system. This agent can be downloaded from the **My Account** page in the **/login** interface. It is neither version nor site-specific, and thus the same agent can be used for as many applications as the admin wishes to support. Once the agent is installed, you can then use **BeyondTrust** to create RDP Jump Items that are configured to use the **BeyondTrust Remote Desktop Agent** option to launch any application installed on the remote system.



Note: **SecureApp** relies on publishing applications using Microsoft RDS RemoteApps. Please refer to the Microsoft documentation for publishing applications.

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

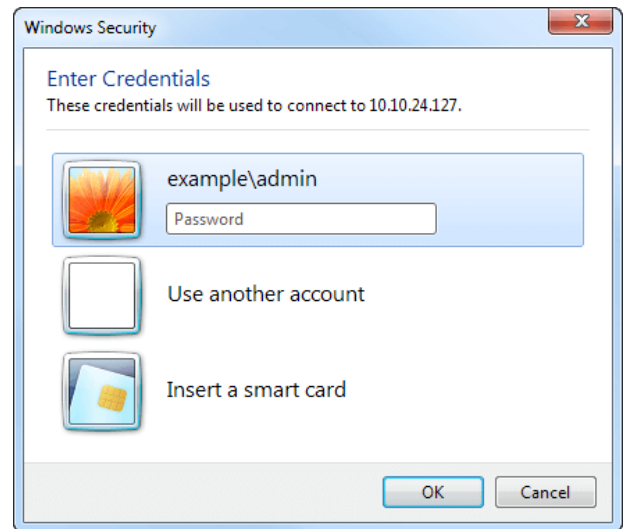


For more information about contained database users, please see [Contained Database Users - Making Your Database Portable](https://docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable) at docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable.

Use an RDP Shortcut

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

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



Your RDP session now begins.



Note: When starting an RDP session, the RDP keyboard automatically matches the language you have set in the access console. This functionality is available for Windows-based access consoles only.

Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, share clipboard contents, use **Alt** and **Shift** commands, and perform key injection. You also can share 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](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Use VNC to Access a Remote Windows Endpoint

Use BeyondTrust to start a VNC session with a remote Windows or Linux system. Because VNC sessions are proxied through a Jumpoint and 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 VNC through BeyondTrust, you must have access to a Jumpoint and have the user account permission **Allowed Jump Methods: Remote VNC via a Jumpoint**.

Create a VNC Shortcut

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

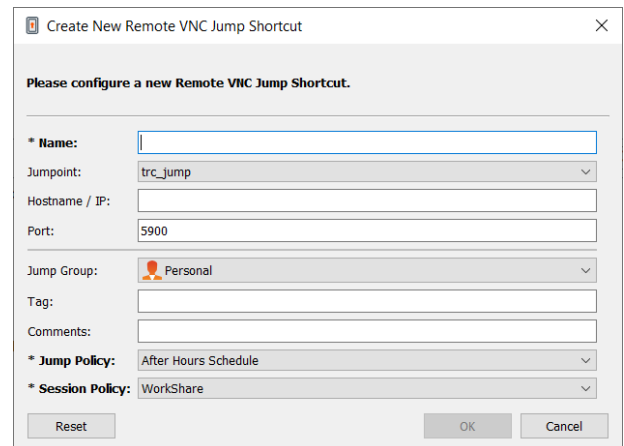
Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.



Note: To view the properties of multiple Jump Items, the items selected must be the same type (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 access console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of the system you wish to access.




Note: 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, add it after the hostname or IP address in the form of **<hostname>:<port>** or **<ipaddress>:<port>** (e.g., 10.10.24.127:40000).

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use 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, select the shortcut from the Jump interface and click the **Jump** button.

When establishing the connection to the VNC server, the system attempts to determine 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.



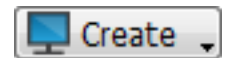
Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to **Join Existing Session**, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not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

Use a Protocol Tunnel Jump to Make a TCP Connection to a Remote System

Using a Protocol Tunnel Jump, make a TCP connection from your system to an endpoint on a remote network. Because the connection occurs through a Jumpoint, the administrator can control which users have access, when they have access, and if the sessions are recorded.

Create a Protocol Tunnel Jump Shortcut

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



Note: Protocol Tunnel Jump shortcuts are enabled only if their Jumpoint is configured for the Protocol Tunnel Jump method on the `/login > Jump > Jumpoint` page.

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 access console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of the system you wish to access.

Specify a **Local Address**. The default address is 127.0.0.1. If you need to connect to multiple systems on the same remote port at the same time, you can enable that connection by changing each Protocol Tunnel Jump Shortcut's address to a different address within the 127.x.x.x subrange.

For **Protocol**, select **TCP Tunnel** or **SQL Server Tunnel**. **SQL Server Tunnel** uses the Microsoft SQL Server Protocol as a database proxy, enabling credential injection for users and improved auditing. Authentication is supported using Windows authentication and SQL login.

In **Local Port**, specify the port that will listen on the user's local system. If you leave this as automatic, the access console allocates a free port.

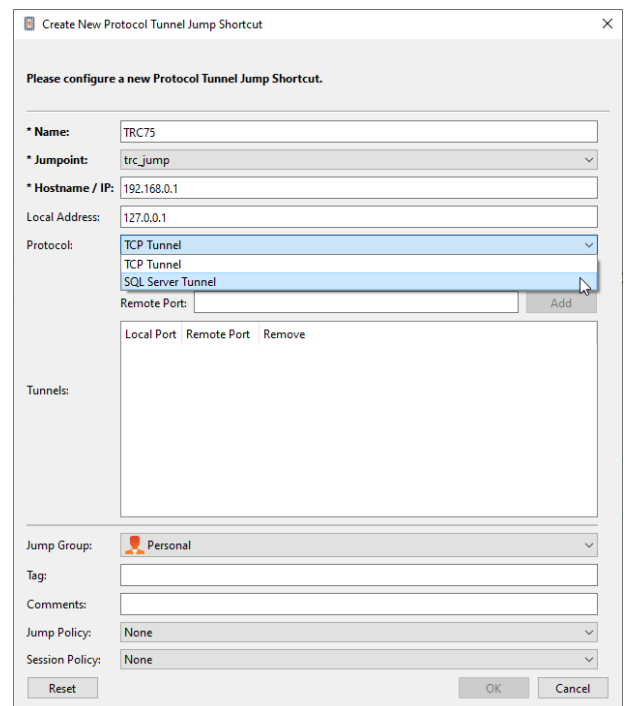
In **Remote Port**, specify the port to connect to on the remote system. This is dictated by the type of server you are connecting to.

You can define multiple pairs of **TCP Tunnels** as necessary for your setup.

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

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

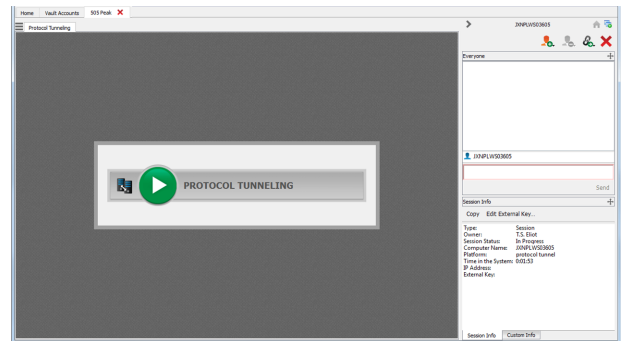


Note: To view the properties of multiple Jump Items, the items selected must be the same type (all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.

Use a Protocol Tunnel Jump Shortcut

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

A session appears in your access console. Click the **Protocol Tunneling** button to establish the connection.

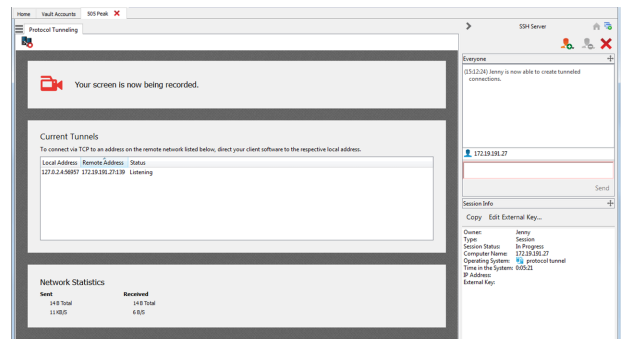


If screen recording is enabled, a prompt appears, informing you that your desktop will be recorded. Click **OK** to continue. If you click **Cancel**, the Protocol Tunnel will not be created.

If screen recording is enabled, an indicator appears at the top of your session screen.

The **Current Tunnels** section displays current connections and their statuses. You also can view brief **Network Statistics**.

You can now open a third-party client to perform tasks on the remote system. Use the ports indicated to connect through the Jumpoint.



Stipulations to Correct Functioning

The Protocol Tunneling feature tunnels network traffic in a way that places some restrictions on how communication must occur between the user's system and the endpoint.

- All traffic must be TCP.
- No more than 256 simultaneous connections can be handled.
- All TCP connections must originate from the endpoint and must be accepted by the listening user's system. The application's protocol cannot require that the user's system make a separate connection back to the endpoint.
- Any TCP connections that the endpoint is to make back to the user's system must be made over tunnels already defined within the Protocol Tunnel Jump Item properties.
- Operating systems typically disallow non-elevated processes from listening on ports less than 1024. Therefore, the local port must generally be greater than 1024. The endpoint software connects to the server by connecting to the local port on which the access console (a non-elevated process) is listening.
- The endpoint software cannot make connections to any system on the remote network other than the one specified in the Protocol Tunnel Jump Item properties.
- The protocol must be agnostic toward the hostname that the endpoint used to connect to the server. Otherwise, other means must be made to satisfy the protocol's requirements, such as mapping a hostname to 127.0.0.1 in the hosts file or applying special configuration to the endpoint client.
- If the tunnel definition has a local port that is different than the remote port (namely, when the local port must be greater than 1024 because the server's port is less than 1024), the protocol must be agnostic toward the port that the endpoint client used to connect to the server.
- Any protocol which goes beyond the case of making a single TCP connection from the endpoint client to the user's system requires the administrator's understanding their specific protocol and the stipulations listed above.

Use Shell Jump to Access 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. Administrators can enable command filtering to help prevent users from inadvertently using harmful commands on SSH-connected endpoints.



Note: You can use your own SSH tool for the SSH protocol. For more information, please see "[Change Settings and Preferences in the Access Console](#)" on page 11.



IMPORTANT!

In order to use your own tool, you must enable **Protocol Tunnel Jump** in **/login > Users & Security > Users > Jump Technology > Protocol Tunnel Jump**.

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, as well as 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 the same type (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 access console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of the 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.

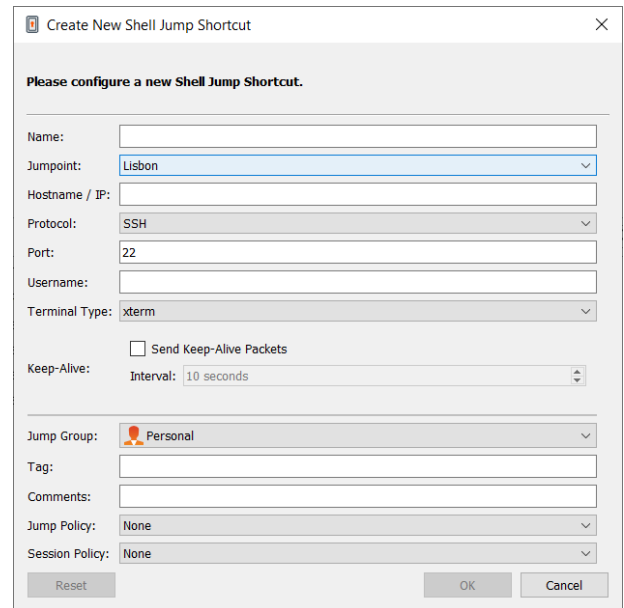
Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

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



Create New Shell Jump Shortcut

Please configure a new Shell Jump Shortcut.

Name:

Jumpoint: **Lisbon** ▼

Hostname / IP:

Protocol: **SSH** ▼

Port:

Username:

Terminal Type: **xterm** ▼

Send Keep-Alive Packets

Keep-Alive: Interval:

Jump Group: **Personal** ▼

Tag:

Comments:

Jump Policy: **None** ▼

Session Policy: **None** ▼

Use a Shell Jump Shortcut

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

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

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

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

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

Administrators can configure command filtering on Shell Jump items to block some commands and allow others in an effort to prevent the user from inadvertently using a command that may cause undesirable results. In the event a user attempts to use a command that matches an expression that is not allowed, they receive a prompt and are not allowed to execute the command.



Note: BeyondTrust's command filter uses extended regular expressions, which are not to be confused with **egrep**. For more information, please see [Regular expressions \(C++\)](https://docs.microsoft.com/en-us/cpp/standard-library/regular-expressions-cpp) at docs.microsoft.com/en-us/cpp/standard-library/regular-expressions-cpp.

Configure Shell Prompt Filtering:

1. Log into the /login interface as a user with permissions to configure Jump Items and session policies.
2. Browse to **Jump > Jump Items** and scroll down to the **Shell Jump Filtering** section.
3. In the **Recognized Shell Prompts** text box, enter regexes to match the command shell prompts found on your endpoint systems, one per line.



Note: Line breaks, or newlines, are not allowed within the command prompt patterns entered. If an endpoint system uses a multi-line prompt, enter an expression that matches only the final line of the prompt in the text box.

4. Click **Save**.



Note: Once you have entered the regexes you wish to use, you can test a shell prompt to determine if it matches any of the regexes in the list. This allows you to test your regexes without starting a session. Enter the expression in the **Shell Prompt** text box and click the **Check** button. A notice displays whether or not the shell prompt you entered matches one of the regexes in the list.

Configure Command Filtering:

1. Browse to **Users & Security > Session Policies** and either create a new policy or edit an existing one.



Note: You can also configure this for users and/or group policies.

2. Locate the **Command Shell** settings in the **Permissions** section.
3. Because you will use command filtering with Shell Jump items, select the **Allow** radio button to allow the use of the command shell.
4. Choose from **Allow all commands**, **Allow the command patterns below**, or **Deny the command patterns below** and specify in the text box which regex patterns you wish to allow or block.



Note: Once you have entered the command patterns you wish to allow or block, you can test commands in the **Command Tester** text box. A notice displays whether or not the command entered would be allowed to run on the remote system based on the regexes specified in the list.

The two possible messages are:

- "The entered command shall be allowed based on your selections."
- "The entered command shall not be allowed based on your selections."

Use Credential Injection with SUDO on a Linux Endpoint

To use credential injection with SUDO, an administrator must configure one or more functional accounts on each Linux endpoint to be accessed via Shell Jump. As the process for configuring the sudoers file is complex and varies by platform, please refer to your platform's documentation for details on completing this process. Each functional account must:

- Allow authenticating via SSH (password or SSH key).
- Have the account credentials stored in the Endpoint Credential Manager (ECM).
- Have one or more entries in `/etc/sudoers` granting the functional account access to one or more commands to be executed as root without requiring a password (**NOPASSWD**).

An administrator must create a Shell Jump Item for the endpoint.

Next, an administrator must configure the ECM and/or password vault to grant users access to the appropriate functional accounts for that Jump Item.

When a user Jumps to the Shell Jump Item, they can choose from the list of functional accounts available for that endpoint. Each functional account has its own set of commands that can be executed using SUDO, as configured by the administrator on the endpoint. The credentials for the account are passed from the ECM to the endpoint.



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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.

Use a Web Jump to Access Web Services

With the proliferation of infrastructure components that have moved to web-based interfaces for configuration, IT administrators are faced with an increasingly complex security management situation. With privileged access to web-based resources, it is a challenge to control, audit, and enforce proper authentication without negatively affecting business productivity. IT administrators need a way to effectively control and audit resources managed via web interfaces, including:

- Externally hosted Infrastructure as a Service (IaaS) servers such as Amazon AWS, Microsoft Azure, IBM SoftLayer, and Rackspace
- Internally hosted servers managed by hypervisor software such as VMware vSphere, Citrix XenServer, and Microsoft Hyper-V
- Modern core network infrastructure that leverages web-based configuration interfaces

The identity and access management capabilities vary significantly between IaaS, hypervisor providers, and core infrastructure systems, and many do not offer native multifactor authentication support, thereby missing that additional layer of security. These inconsistencies across systems create opportunities for business vulnerabilities, such as misuse of accounts and access, leading to leaks of sensitive data. BeyondTrust Web Jump is the extra layer of security for authenticating to these systems.



IMPORTANT!

Web Jump does not support Flash. Be sure to consult your hypervisor documentation and update it to a version that supports HTML5.



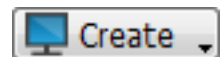
Note: *The Web Jump Item is an add-on for Privileged Remote Access, and requires additional purchase.*

Create a Web Jump Shortcut



Note: *Before creating Web Jump shortcuts, ensure that your user account has the ability to access Web Jumps. This permission is set on your user account in the /login interface under **Access Permissions > Jump Technology**.*

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




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



Note: *To view the properties of multiple Jump Items, the items selected must be the same type (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 Windows or Linux Jumpoint that hosts the computer you wish to access.

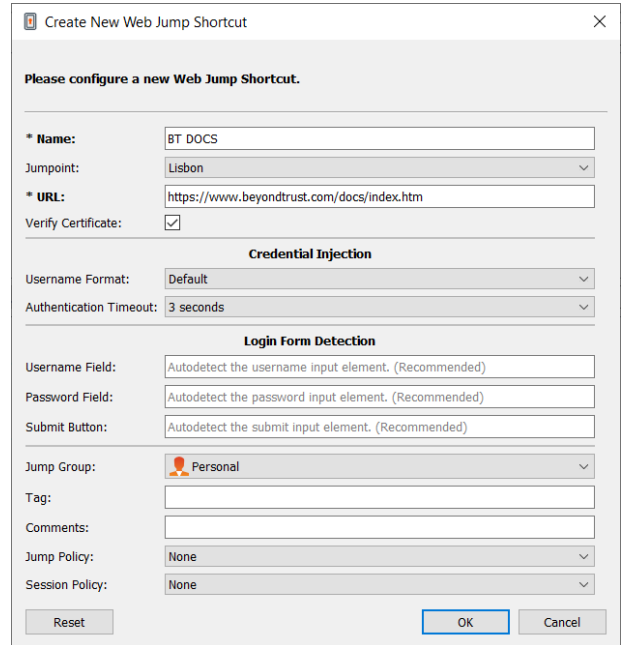
 **Note:** Copy/Paste functionality is not supported for Linux Jumpoints.

Type the **URL** for the web site you wish to access.

Check **Verify Certificate** if you want the site certificate to be validated before the connection is made. If this box is checked and issues are found with the certificate, the session does not start.

 **IMPORTANT!**

You should uncheck **Verify Certificate** only if you are Jumping to a site that you trust but that uses a self-signed certificate.




If you want to use credential injection, first select the **Username Format**:

- **Default:** This is the default value for new and existing Web Jump Items. The username is not modified before injection into the web page and is used in the stored format. For the Endpoint Credential Manager (ECM), the credential may be in either UPN or DLLN format. For Vault, the username is always in UPN format.
- **Username Only:** Independently of the format stored in either Vault or ECM (**username@domain** or **domain\username**), the domain is removed and only the username is used.

Under **Login Form Detection**, the recommended practice is to leave the three fields empty, and allow the system to auto-detect and use the information already stored for login. If auto-detection fails, the injection fails and a message states that the **Username Field**, **Password Field**, and/or **Submit Button** could not be found.

If entering the names of the input elements, enter the HTML id, HTML name, or CSS selector for each element on the login page.

 **Example:** This shows HTML ids with input fields and a submit button, as they might appear on the code view of a login page. The HTML ids here are **user**, **pwd**, and **button**.

```

<form action="/action_page.php">
Username: <input type="text" id="user"><br>
Password: <input type="password" id="pwd"><br>
<input type="submit" value="Submit" id="button">
</form>
```

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 Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

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, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use 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.

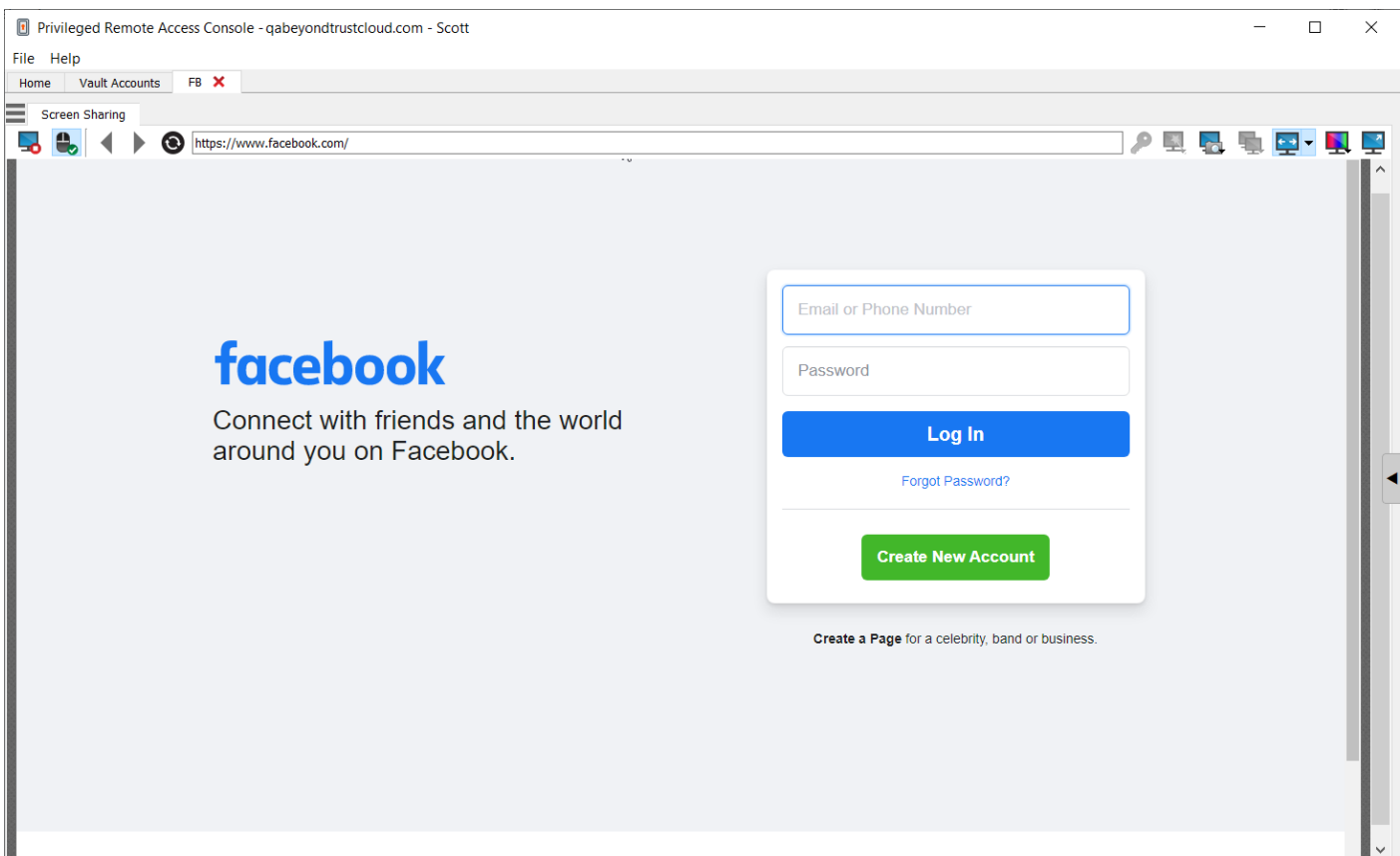


For more information about identifying HTML form fields, please see online resources such as this page explaining the use of [CSS selectors](https://developer.mozilla.org/en-US/docs/Web/CSS/CSS_Selectors) at https://developer.mozilla.org/en-US/docs/Web/CSS/CSS_Selectors.

Use a Web Jump Shortcut

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

Once a connection is made to the web site, click the screen sharing button. The web site's login interface becomes available.



Note: *If you want to open a new tab in Windows or Linux, hold down the **CTRL** key and click the mouse button. For iOS, hold down the **Command** key and click the mouse button.*



Tip: You can copy and paste text to and from the website by using the copy/paste controls of your operating system.

Upload and Download Files using a Web Jump Shortcut

If you click a link to download a file from the web site, a prompt appears in your chat window asking you to accept or decline the download. If you accept, a window opens on your computer allowing you to choose a download location.

Uploading files to the web site works similarly, opening a window to allow you to choose which file to upload.



Note: The privileged web access console does not support uploading files to a web page via a Web Jump. File upload to a web page via Web Jump is supported only by the desktop access console application.

Use Credential Injection



IMPORTANT!

Credential injection is not supported for non-secure sites (non-HTTPS).

When integrating BeyondTrust PRA with a password vault system, you can seamlessly access your web site accounts without viewing the login screen or entering any credentials using credential injection.



Note: Web Jump supports multi-step authentication, in which the username and password are not requested on the same browser page. Web Jump also supports scenarios in which a user connects to an unauthenticated portion of a website, but then attempts to enter an area using basic authentication. Furthermore, Web Jump supports sites that contain CAPTCHAs, by allowing the users to complete the CAPTCHA without ending the credential injection process. Once interaction with a CAPTCHA is complete, the user clicks the key icon in the access console to complete credential injection.



Note: For seamless credential injection on a VMware console, some configuration is required.

1. Go to the computer hosting the Jumpoint.
2. Download and install the VMware Client Integration Plugin.
3. Using admin permissions, open Windows services (**services.msc**) on the Jumpoint host.
4. Right-click the BeyondTrust Jumpoint and select **Properties**.
5. On the **Log On** tab under **Local System account**, check **Allow service to interact with desktop**.
6. Click **OK**.
7. On the user's local system, on which the access console is installed, start a Web Jump with the VMware URL specified above.
8. Select **Use Windows Credentials**.
9. This causes a prompt on the Jumpoint host system to allow services to interact with an external program. Give the service permission.



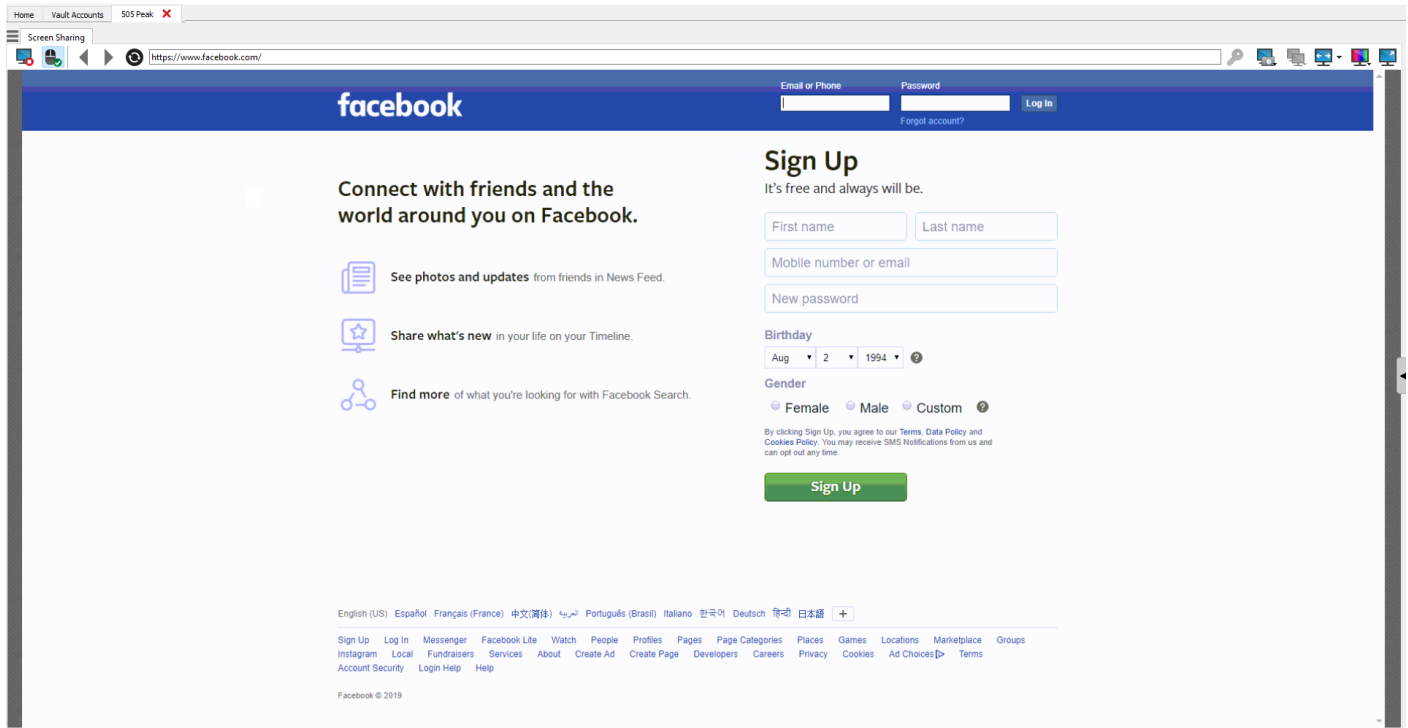
10. A VMware credential injection prompt is displayed. Uncheck the box asking if you want the prompt to be displayed whenever the program is called. Click **Accept**.
11. You can now start Web Jumps to the VMware console using Windows credentials without a prompt.














For more information on downloading the appropriate VMware Client Integration Plugin, please see [Upgrading VMware Client Integration Plug-in to the latest version at https://kb.vmware.com/s/article/2145066](https://kb.vmware.com/s/article/2145066).

Access Toolset

Access Session Overview and Tools



Session Tools

	<p>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. 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 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 from the menu.</p>
 	<p>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.</p>
 	<p>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).</p>
	<p>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.</p>
	<p>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.</p>
	<p>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.</p>
	<p>The session owner can remove another user from a shared session.</p>
	<p>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 endpoint, 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.</p>
	<p>Close your session tab entirely. You can close the session from the sidebar, the session menu, or the session tab.</p>

At the bottom right of the session window is information about the remote system. Also, 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 Access Console

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

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



Note: *Credential injection is not available for Mac or Linux Jump Clients.*

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 Privileged Remote Access.

System Requirements

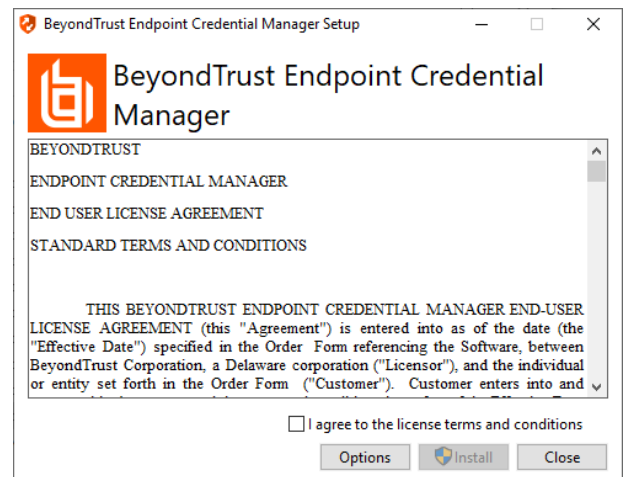
- **Windows Vista or newer, 64-bit only**
- **.NET 4.5 or newer**

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

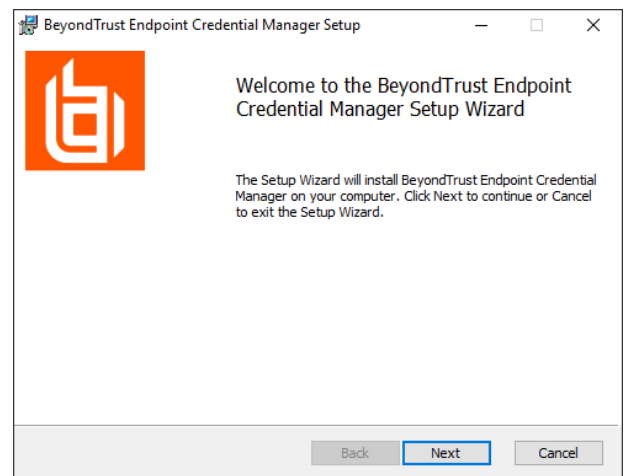
If you need to modify the ECM installation path, click the **Options** button to customize the installation location.



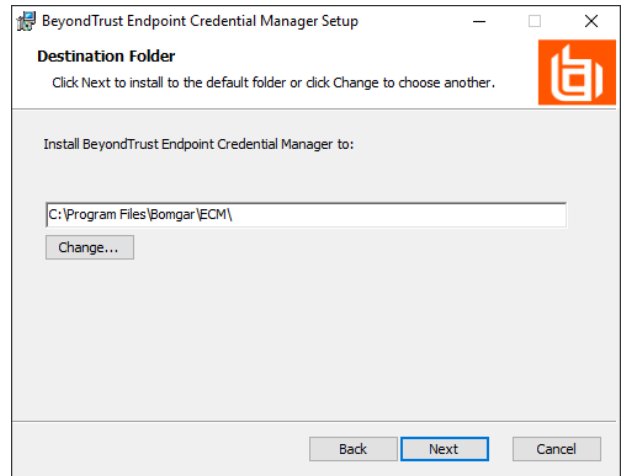
Note: You are not allowed to proceed with the installation unless you agree to the EULA.



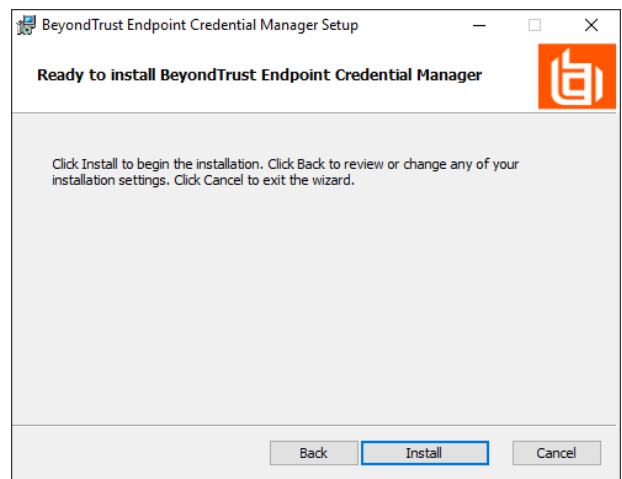
4. Click **Next** on the Welcome screen.



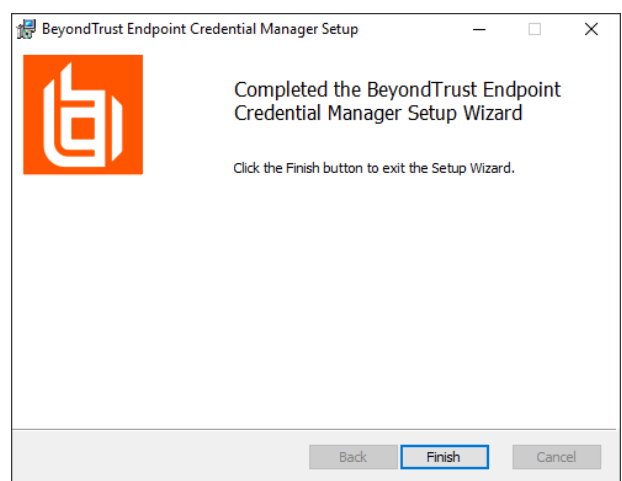
5. Choose a location for the credential manager, and then click **Next**.
6. On the next screen, you can begin the installation or review any previous step.



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



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





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



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



Note: If you get a Windows plugin error during installation, locate and unblock `BeyondTrustVaultRestPlugin.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.

Name	Date modified	Type	Size
Bomgar-ECMConfigurator.exe	2/7/2017 3:40 PM	Application	54 K
Bomgar-ECMConfigurator.exe.config	2/10/2016 10:21 A...	Configuration Sou...	1 K
Bomgar-ECMService.exe	2/7/2017 3:40 PM	Application	24 K
Bomgar-ECMService.exe.config	2/10/2016 10:22 A...	Configuration Sou...	1 K
Configurator.log	2/8/2017 1:00 PM	Text Document	6 K
ECM.dll	2/7/2017 3:40 PM	Application extens...	62 K
ECM.log	2/8/2017 12:48 PM	Text Document	2 K
ECSM.settings	11/14/2016 2:21 PM	SETTINGS File	1 K
log4net.dll	2/10/2016 10:22 A...	Application extens...	294 K
Newtonsoft.Json.dll	12/14/2016 3:25 PM	Application extens...	491 K
Util.dll	2/7/2017 3:40 PM	Application extens...	27 K

Enter the following values:

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

Name	Date modified	Type	Size
ECM.dll	2/7/2017 3:40 PM	Application extens...	62 KB
log4net.dll	2/10/2016 10:22 A...	Application extens...	294 KB
Newtonsoft.Json.dll	12/14/2016 3:25 PM	Application extens...	491 KB
Util.dll	2/7/2017 3:40 PM	Application extens...	27 KB



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.

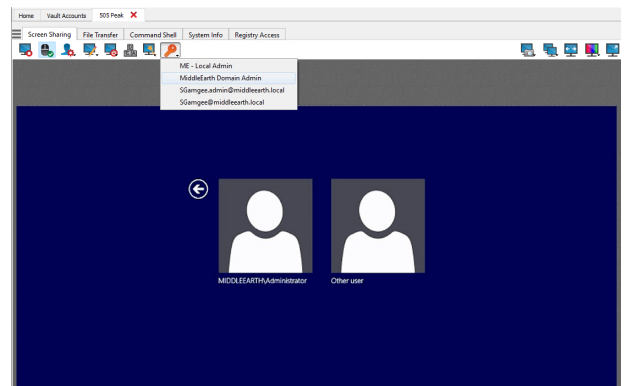

IMPORTANT!

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 access console can begin using credentials in the credential store to log into remote systems.

1. Log into the access 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 into the remote system.



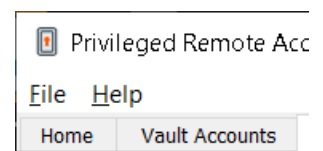
Choose from Favorite Credentials for Injection

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

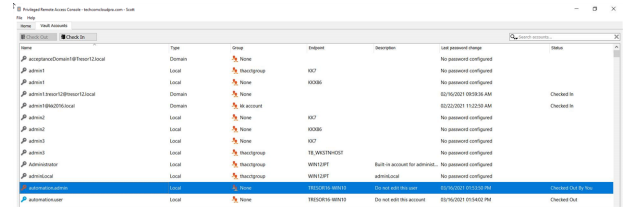
The credential list recommends no more than five credentials.

Check Out and Check In Vault Credentials

You can easily access the Privileged Remote Access Vault directly from the access console. This allows you to check out and check in credentials when needed, either during a session or on your local machine.



Select the **Vault Accounts** tab to see a list of available credentials and associated information.

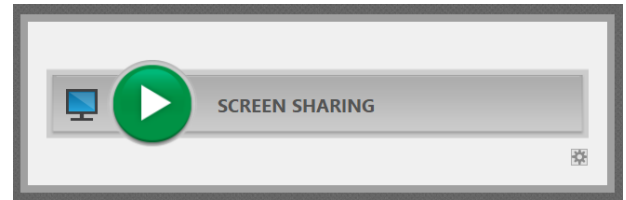


Name	Type	Group	Index	Description	Last password change	Status
acceptanceDomain@resort1.local	Domain	None			No password configured	
admin	Local	Administrators	007		No password configured	
admin	Local	None	00066		No password configured	
admin@resort1.local	Domain	None			03/16/2021 09:38 AM	Checked in
admin@resort1.local	Domain	Administrators			03/23/2021 11:23 AM	
admin	Local	None	007		No password configured	
admin	Local	None	00066		No password configured	
admin	Local	None	007		No password configured	
admin	Local	Administrators	16_A0378400F		No password configured	
administrator	Local	Administrators	WIN12PT	Both in account for admin.	No password configured	
admin@local	Local	Administrators	WIN12PT	admin@local	No password configured	
administrator	Local	None	16324510001F	Do not edit this entry	11/10/2021 03:13 PM	Checked Out By N/A
administrator	Local	None	16324510001F	Do not edit this account	03/16/2021 03:42 PM	Checked Out

Control the Remote Endpoint with Screen Sharing

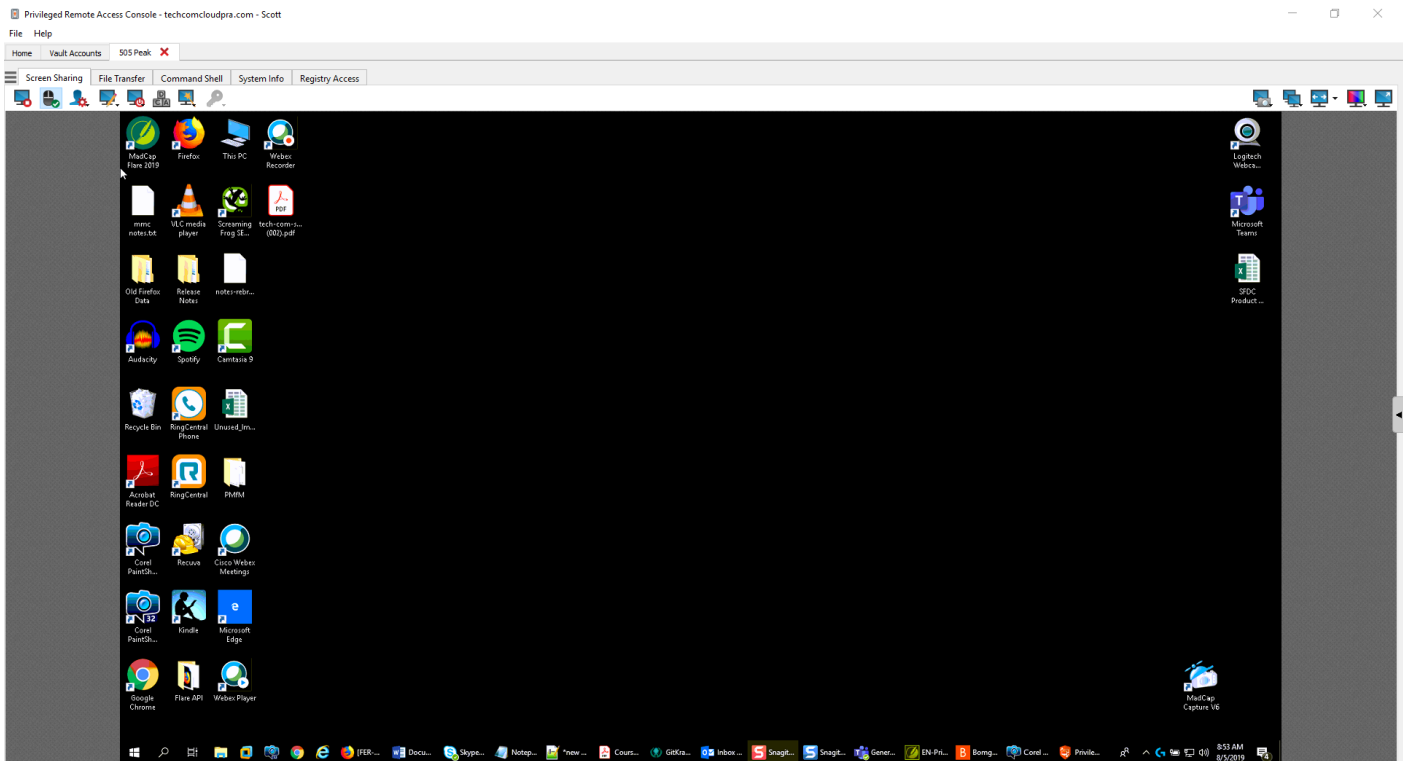
From the session window, click the **Screen Sharing** button to request control of the remote computer if screen sharing does not automatically start. Options may be available below the button depending on your account settings. Click the gear button to view options.

Once you have started a session, the access console immediately starts screen sharing with the endpoint. Depending on the system, you may have full control or view only privileges while screen sharing with the system.




















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 **View Only**, you may see but not control the remote screen.
- **Privacy Screen** starts the session with remote view and control of the endpoint disabled. Privacy screen is not available when supporting Windows 8.



Screen Sharing Tools

	Stop screen sharing.
	<p>While viewing the remote computer, start or stop control of the remote keyboard and mouse.</p> <p>Representatives using a macOS system can send CTRL+Left-Click through the connected screen sharing session to the remote system by using CTRL+CMD+Left-Click.</p>
	<p>If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The end user's view of the privacy screen clearly explains that the BeyondTrust user has disabled the end user's view. The end user can regain control at any time by pressing Ctrl+Alt+Del.</p> <p>Alternatively, disable the end user's mouse and keyboard input while still allowing them to view the screen. When input is restricted, an orange border appears around the end user's monitors, and a message indicates that the BeyondTrust user has mouse and keyboard control. The end user can regain control at any time by pressing Ctrl+Alt+Del.</p> <p>Restricted endpoint interaction is available only when accessing macOS or Windows computers. Restricted customer interaction is available only when supporting Windows computers. In Windows Vista and above, the endpoint client must be elevated. On Windows 8, this feature is limited to disabling the mouse and keyboard.</p>
	Annotation tools allow easier collaboration during shared sessions. A number of tools are available, including shapes and free drawing.
	Reboot the remote system in either normal or safe mode with networking, or shut down the remote system.
	Send a Ctrl-Alt-Del command to the remote computer.
	<p>Perform a special action on the remote system. Based on remote operating system and configuration, available tasks will vary. Canned scripts available to the user appear in a fly-out menu. With the Run As special action on a Windows® system, you may select credentials from an Endpoint Credential Manager. Use of the Endpoint Credential Manager requires a separate services agreement with BeyondTrust. Once a services agreement is in place, you may download the required middleware from the BeyondTrust Support Portal.</p>
	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. The appropriate virtual smart card drivers must be installed on both your local system and the remote system, with their services running.
	<p>To restart iOS device screen sharing. For details, see Supporting Apple iOS Devices at www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/index.htm. 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 access 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.</p>

	<p>Log into the endpoint using credentials provided by an external credential store. Use of the Endpoint Credential Manager requires a separate services agreement with BeyondTrust. Once a services agreement is in place, you may download the required middleware from the BeyondTrust Support Portal. Prior to 15.2, this feature is available only in sessions started from an elevated Jump Client on Windows®. Starting with 15.2, you also may use an Endpoint Credential Manager in Remote Jump sessions, Microsoft® Remote Desktop Protocol sessions, VNC sessions, and Shell Jump sessions.</p>
	<p>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 > Tools menu in the access console. This feature works on Mac, Windows, and Linux.</p>
	<p>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.</p>
	<p>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 disallowed to receive clipboard information from the remote system.</p>
	<p>Select an alternate remote monitor to display. The primary monitor is designated by a P.</p>
	<p>View the remote screen at actual or scaled size.</p>
	<p>Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select Video Optimized; otherwise select between Black and White (uses less bandwidth), Few Colors, More Colors, or Full Color (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.</p>
	<p>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.</p>

Use Annotations to Draw on the Remote Screen of the Endpoint

Use annotation tools to collaborate with other users during shared sessions. Annotations provide an interactive way of communicating visually, reducing potentially frustrating situations and speeding processes.

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.

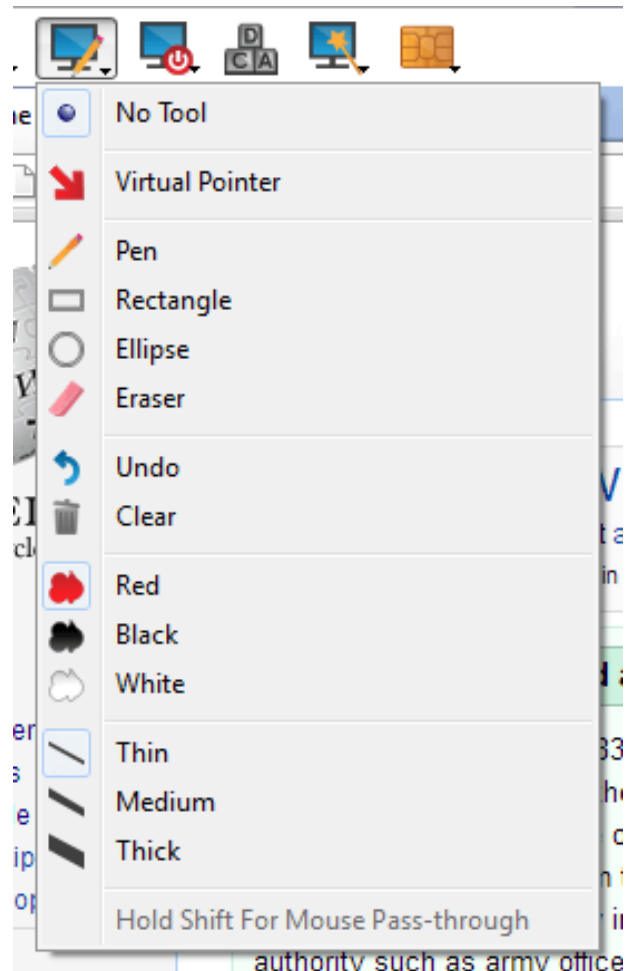
Enabling Annotations

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



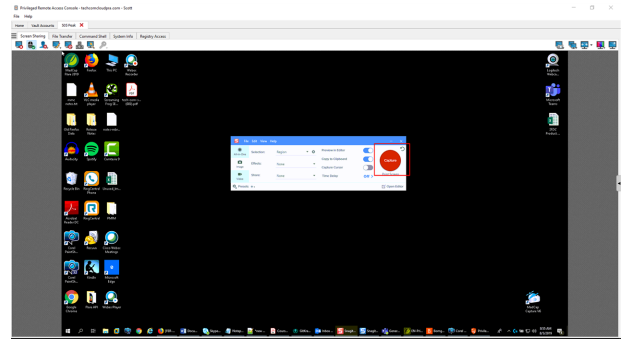
Clicking on any of the dropdown menu items turns the **Annotations** mode on. The following tools and functions are available:

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



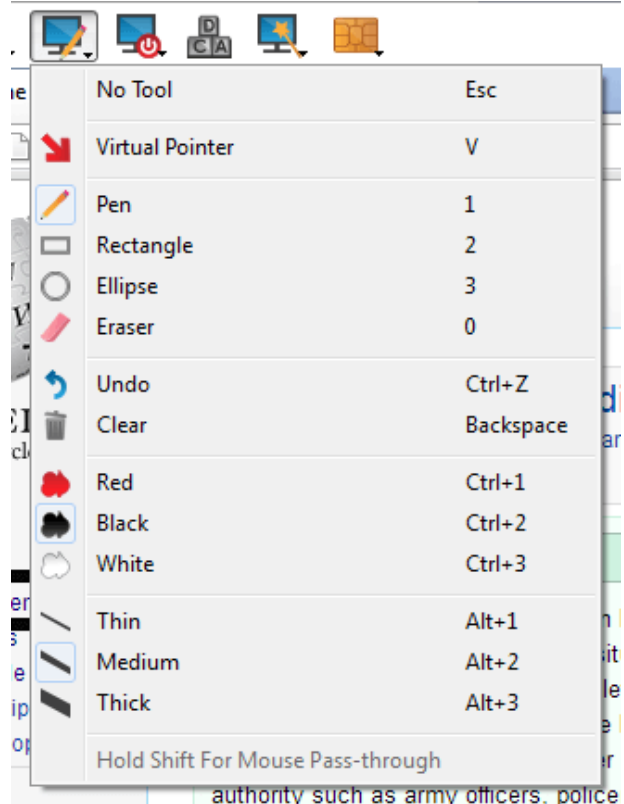
You can select your tool from the **Annotations** dropdown menu or by right-clicking inside the remote screen area. If you click on the areas outside of the remote screen, the dropdown menu does not display.

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



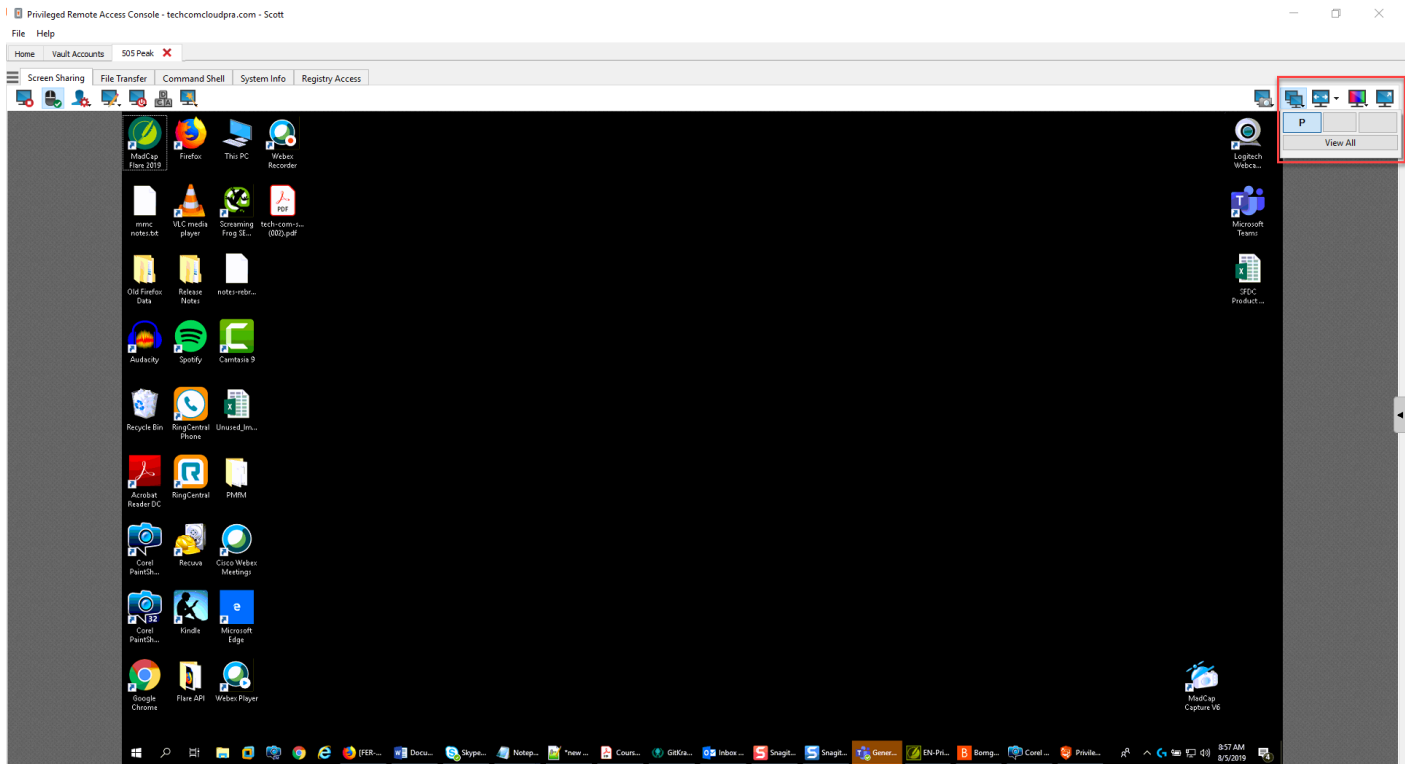
To turn off **Annotations**, select **No Tool** from the dropdown menu, or click **Esc**.

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



View Multiple Monitors on the Remote Endpoint

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.

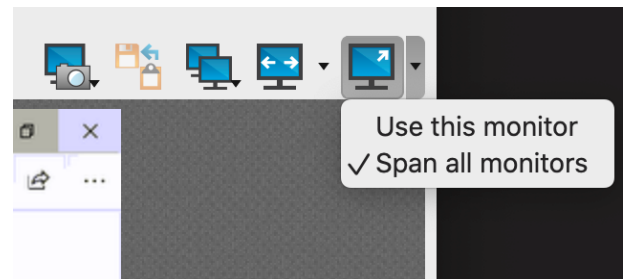


If the remote computer has no additional monitors attached, the **Display** icon will be inactive.



RDP Session Multi-Monitor Support

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

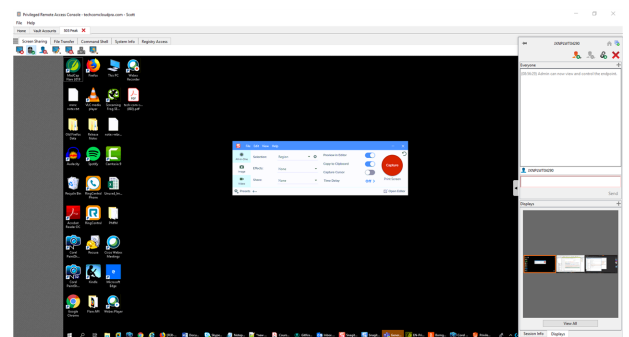


Note: If you are using full screen view while using this feature, the remote system is displayed across all of your monitors.

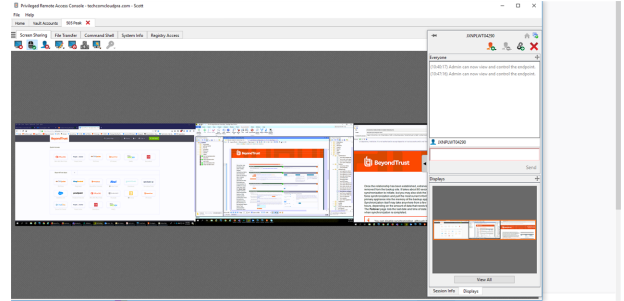
Using the Displays Tab

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.

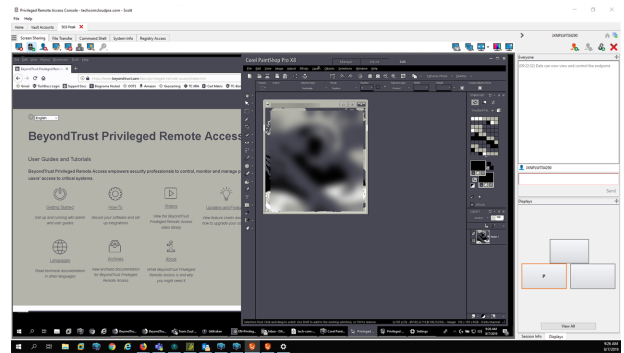
The monitor currently displayed in the **Screen Sharing** tab will be highlighted.



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.



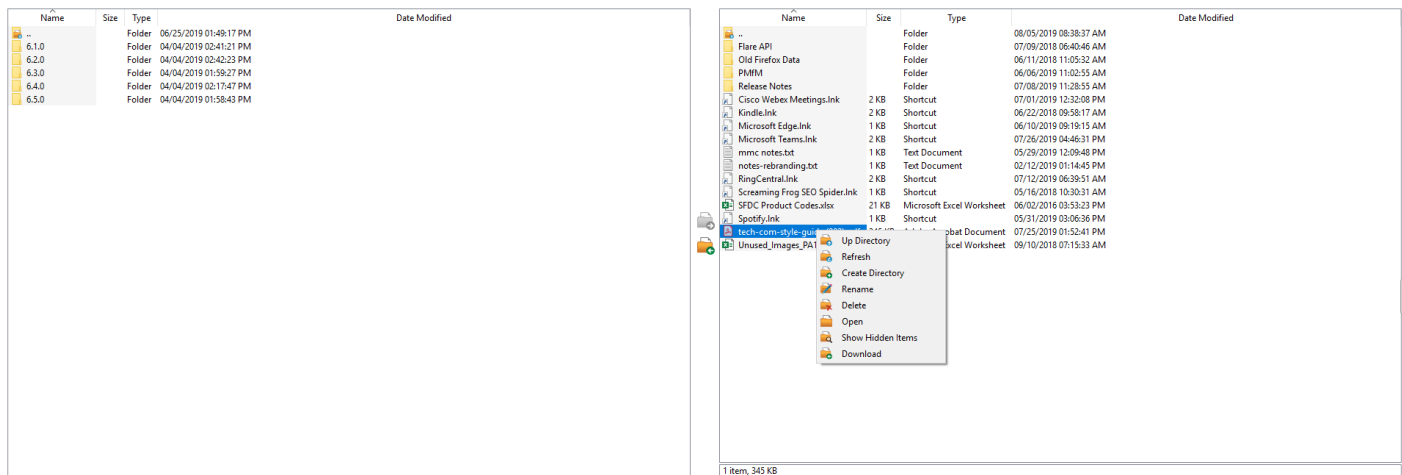
Note: *The refresh cycle of the thumbnail image is about three seconds in ideal conditions but can lag depending on connection speed and data transfer.*

File Transfer to and from the Remote Endpoint

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.





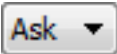






Transfer files by using the upload and download buttons or by dragging and dropping files. Right clicking on a file brings up a context sensitive menu from where you can, among other things, create a new directory; rename, open, or delete the file; or download it directly to your machine.



If an ICAP server is enabled, the file shows as "Scanning" until the transfer ends. During or after a file transfer, the results of the scan appear in the **File Transfer Log**. If malware is detected in the file, it is not transferred. To enable an ICAP server, please see [Security](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm>.

File Transfer Tools

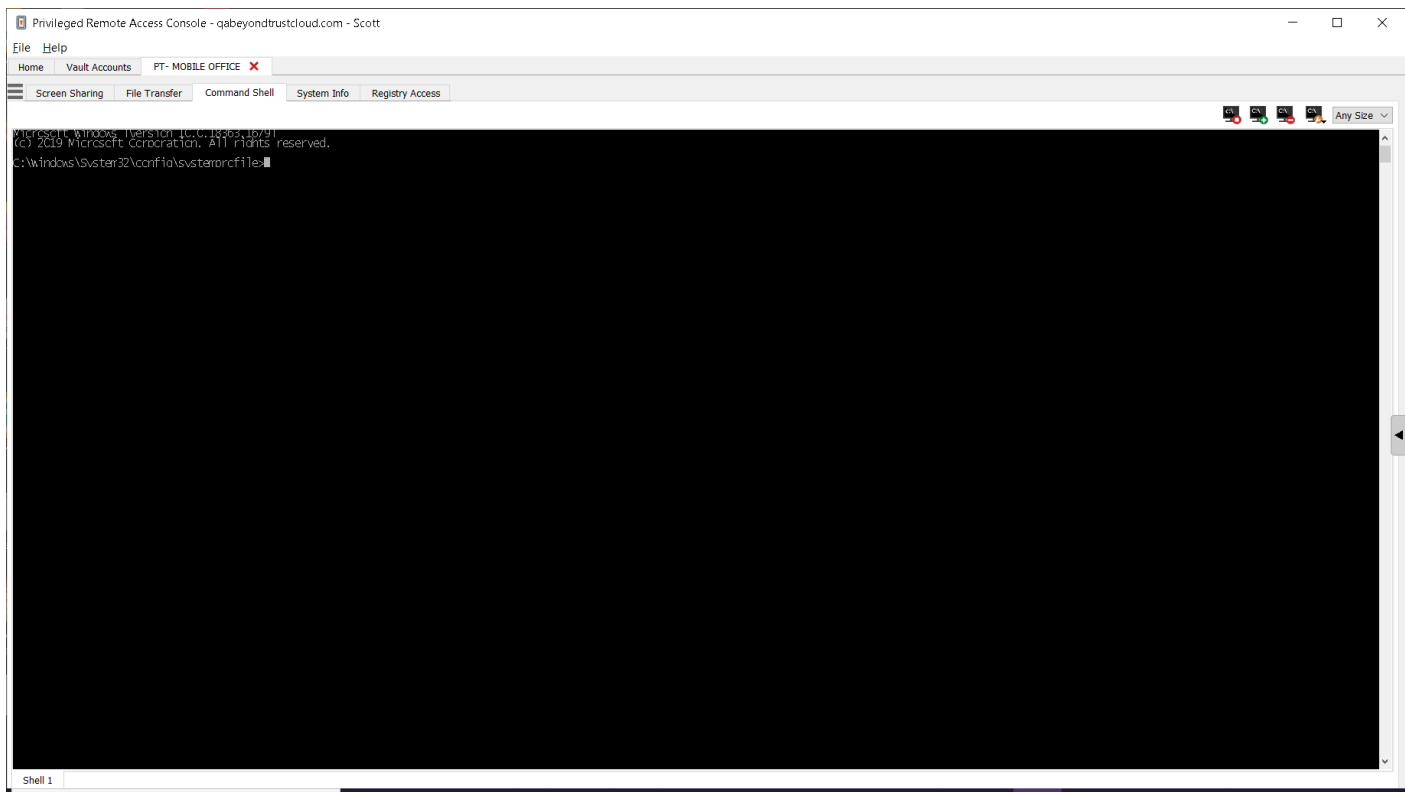
	Stop access to the remote device's file system when it is no longer needed.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Create a new directory.

	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.





Open the Command Shell on the Remote Endpoint Using the Access Console


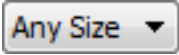
Remote command shell enables privileged users to open a virtual command line interface on remote computers. Users can then type locally but have the commands executed on the remote system. You can work from multiple shells. Note that scripts available to the user may also be executed on the remote computer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

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



Command Shell Tools

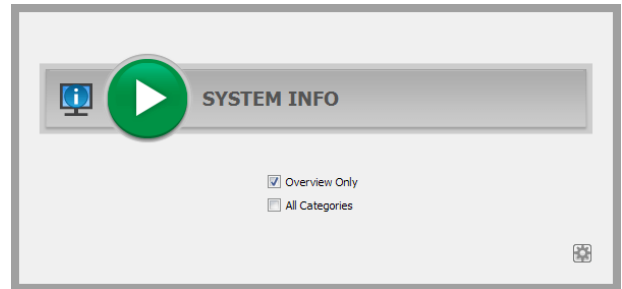
	<p>Stop command prompt access when it is no longer needed.</p>
 	<p>Open a new shell to run multiple instances of command prompt, or close individual shells without relinquishing command prompt access. Shells are tabulated at the bottom of the screen.</p>
	<p>If permitted, access a dropdown of previously 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.</p>

	Access tools to use within the command prompt. Paste the contents of your clipboard either by selecting it from the menu or 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, 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 System Information on the Remote Endpoint

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.



Privileged Remote Access Console - techcomcloudpra.com - Scott

File Help













Home Vault Accounts 505 Peak X

Screen Sharing File Transfer Command Shell System Info Registry Access

Overview Devices Processes Events Programs Services

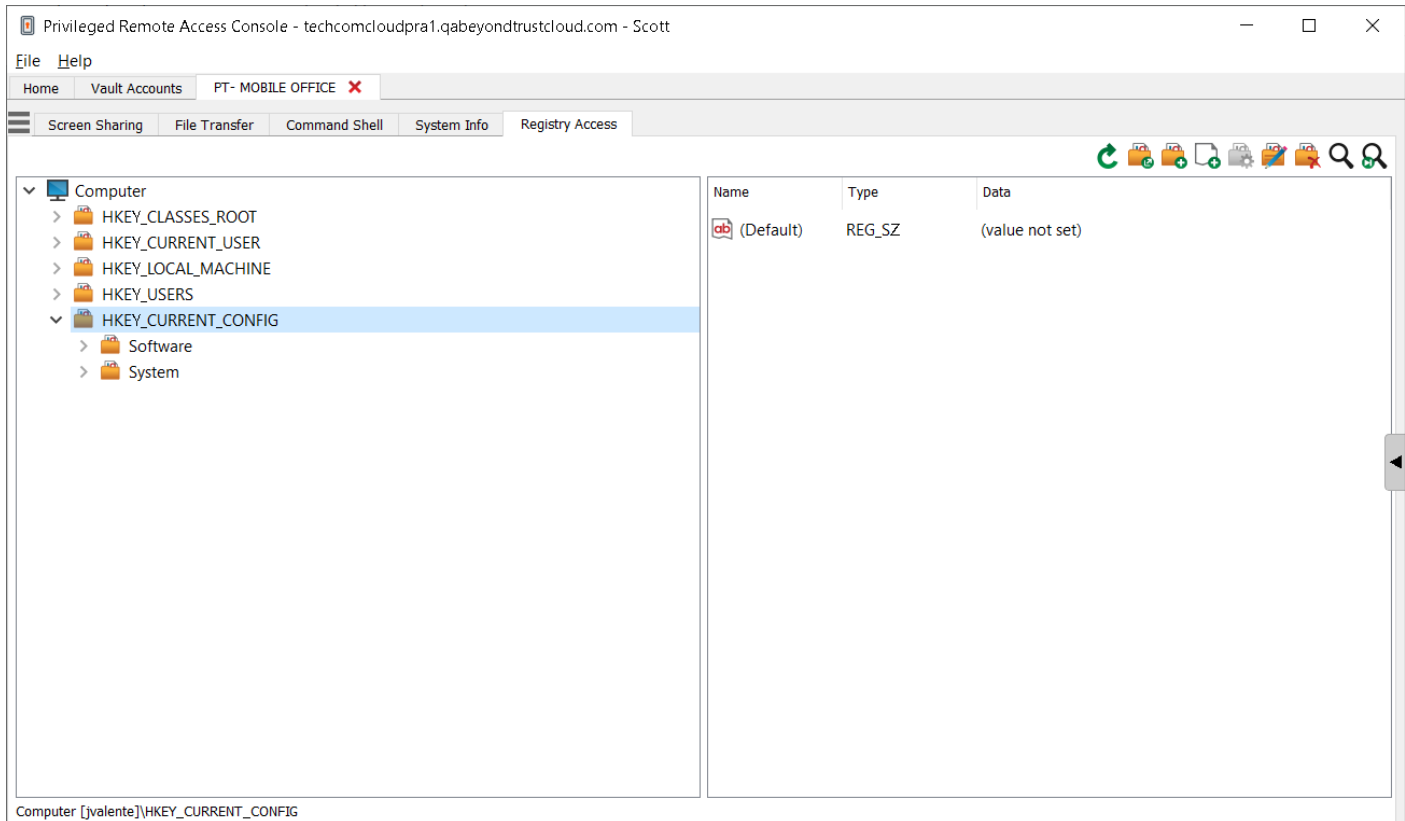
Name	Status	Startup Type	Log On As	Description
ActiveX Installer (AInstSV)	Stopped	Manual	LocalSystem	Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started
Adobe Genuine Monitor Service	Running	Auto	LocalSystem	Adobe Genuine Monitor Service
Adobe Genuine Software Integrity Service	Running	Auto	LocalSystem	Adobe Genuine Software Integrity Service
AdobeUpdateService	Running	Auto	LocalSystem	
AllJoyn Router Service	Stopped	Manual	NT AUTHORITY\LocalService	Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run.
Alps HID Monitor Service	Running	Auto	LocalSystem	Monitor HID device for Alps
App Readiness	Stopped	Manual	LocalSystem	Gets apps ready for use the first time a user signs in to this PC and when adding new apps.
Apple Mobile Device Service	Running	Auto	LocalSystem	Provides the interface to Apple mobile devices.
Application Identity	Stopped	Manual	NT Authority\LocalService	Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.
Application Information	Running	Manual	LocalSystem	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges the
Application Layer Gateway Service	Stopped	Manual	NT AUTHORITY\LocalService	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing.
Application Management	Stopped	Manual	LocalSystem	Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed throug
AppX Deployment Service (AppXSVC)	Stopped	Manual	LocalSystem	Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store applications will not be deployed to the system, and may not function properly.
AssignedAccessManager Service	Stopped	Manual	LocalSystem	AssignedAccessManager Service supports kiosk experience in Windows.
Auto Time Zone Updater	Stopped	Disabled	NT AUTHORITY\LocalService	Automatically sets the system time zone.
AV/CTP service	Running	Manual	NT AUTHORITY\LocalService	This is Audio Video Control Transport Protocol service
Avecto Defendpoint Service	Running	Auto	LocalSystem	Manages application privileges through policy
Avecto IC3 Adapter	Running	Auto	LocalSystem	IC3 Adapter for the Avecto Defendpoint Service.
Background Intelligent Transfer Service	Running	Auto (delayed)	LocalSystem	Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically
Background Tasks Infrastructure Service	Running	Auto	LocalSystem	Windows infrastructure service that controls which background tasks can run on the system.
Base Filtering Engine	Running	Auto	NT AUTHORITY\LocalService	The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduc
BeyondTrust Privileged Remote Access Jump Client [tcpam1.qa.bomgar.com]	Running	Auto (delayed)	LocalSystem	This service is used by the BeyondTrust Privileged Remote Access Jump Client. Please see https://www.beyondtrust.com/ for more information.
BitLocker Drive Encryption Service	Running	Manual	LocalSystem	BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full volume encryption for OS, fixed or removable volumes. This ser
Block Level Backup Engine Service	Stopped	Manual	LocalSystem	The WBEENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may cause the currently running backup or recovery operation to fail. Dis
Bluetooth Audio Gateway Service	Running	Manual	NT AUTHORITY\LocalService	Service supporting the audio gateway role of the Bluetooth Handsfree Profile.
Bluetooth Support Service	Running	Auto	NT AUTHORITY\LocalService	The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent
Bluetooth User Support Service, f164b5	Stopped	Manual	LocalSystem	The Bluetooth user service supports proper functionality of Bluetooth features relevant to each user session.
Bomgar Connection Agent 1.0 [biogame.pam.boom] [Agent Name: BomgarAD]	Running	Auto	LocalSystem	This service is part of Bomgar. It is used to proxy authentication requests from the box to your authentication server.
Bomgar Connection Agent 1.0 [dale1] [Agent Name: BomgarAD_Users]	Running	Auto	LocalSystem	This service is part of Bomgar. It is used to proxy authentication requests from the box to your authentication server.
Bomgar ECM Service	Running	Auto	LocalSystem	A client service between an external credential store and a Bomgar site.
Bomgar Integration Client Scheduler	Running	Auto	LocalSystem	This service is used by the Bomgar Integration client. Please see http://www.bomgar.com for more information.
Bomgar Jump Client [biogame.bomgar.com]	Running	Auto (delayed)	LocalSystem	This service is used by the Bomgar Jump Client. Please see http://www.bomgar.com/ for more information.
Bomgar Jumpoint [tcpam1.qa.bomgar.com]	Running	Auto	LocalSystem	Allows the Bomgar Representative Console to push to hosts on the network on which the Jumpoint resides.
Bonjour Service	Running	Auto	LocalSystem	Enables hardware devices and software services to automatically configure themselves on the network and advertise their presence.
BranchCache	Stopped	Manual	NT AUTHORITY\NetworkService	This service caches network content from peers on the local subnet.
Capability Access Manager Service	Running	Manual	LocalSystem	Provides facilities for managing UWP apps access to app capabilities as well as checking an app's access to specific app capabilities
CaptureService, f164b5	Stopped	Manual	LocalSystem	OneCast Capture Service
Certificate Propagation	Running	Auto	LocalSystem	Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, and, if needed, installs the smart card Plug i
Cisco AnyConnect Secure Mobility Agent	Running	Auto	LocalSystem	Cisco AnyConnect Secure Mobility Agent for Windows
Client License Service (ClipSvc)	Running	Manual	LocalSystem	Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled applications bought using Windows Store will not behave correctly.
Clipboard User Service, f164b5	Running	Manual	LocalSystem	This user service is used for Clipboard scenarios
CMG Key Isolation	Running	Manual	LocalSystem	The CMG key isolation service is hosted in the USA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service
COM+ Event System	Running	Auto	NT AUTHORITY\LocalService	Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and
COM+ System Application	Stopped	Manual	LocalSystem	Manages the configuration and tracking of Component Object Model (COM)-based components. If the service is stopped, most COM-based components will not function properly. If this service is disabled
Computer Browser	Running	Manual	LocalSystem	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled
Connected Devices Platform Service	Running	Auto (delayed)	NT AUTHORITY\LocalService	This service is used for Connected Devices Platform scenarios
Connected Devices Platform User Service, f164b5	Running	Auto	LocalSystem	This user service is used for Connected Devices Platform scenarios

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 Registry Editor on the Remote Endpoint

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.



Registry Editor Tools

	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.

Session Management and Team Collaboration

View Active Access Sessions

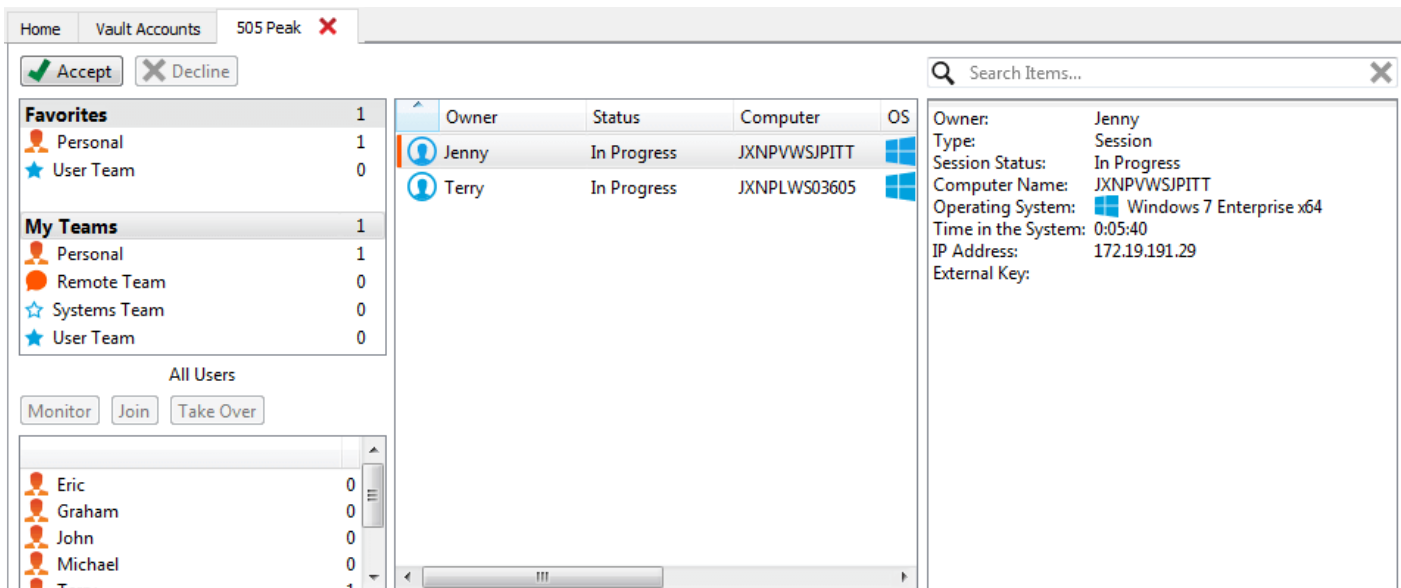
Session queues provide information about and access to currently running sessions. The **Personal** queue contains sessions you are currently running, as well as invitations for you to join a shared session.

You also have queues for any teams of which you are a member. If another user requests any member of a team to join a session, that invitation appears in the team queue. When no specific team is selected, team managers and leads can also see which team members have sessions running.

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.

Sort your queues by several criteria, including the length of time the session has been running, the computer name, external key, etc. 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 access console remembers the column order and the sort order of the session queue the next time the access console is launched.

You can run multiple sessions simultaneously. At the top of the access console, a tab exists for each session you have open.



The screenshot shows the BeyondTrust Access Console interface. At the top, there are tabs for 'Home', 'Vault Accounts', and '505 Peak' (with a red 'X' icon). Below the tabs, there are buttons for 'Accept' (with a green checkmark) and 'Decline' (with a red 'X').

The main interface is divided into several sections:

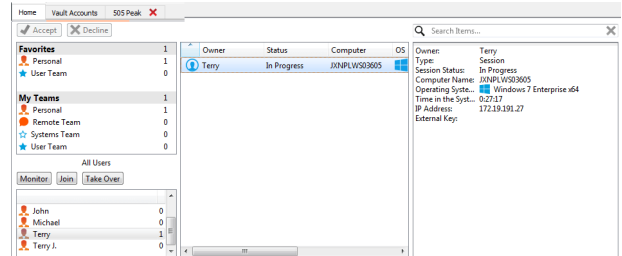
- Favorites:** A list with columns for name and count. Items include 'Personal' (1) and 'User Team' (0).
- My Teams:** A list with columns for name and count. Items include 'Personal' (1), 'Remote Team' (0), 'Systems Team' (0), and 'User Team' (0).
- All Users:** A list with columns for name and count. Items include 'Eric' (0), 'Graham' (0), 'John' (0), 'Michael' (0), and 'Terry' (1).
- Buttons:** 'Monitor', 'Join', and 'Take Over' buttons are located below the 'All Users' list.
- Session Queue Table:** A table with columns: Owner, Status, Computer, OS. It lists two sessions:

Owner	Status	Computer	OS
Jenny	In Progress	JXNPVWSJPITT	Windows 7 Enterprise x64
Terry	In Progress	JXNPLWS03605	Windows 7 Enterprise x64
- Search Items...:** A search bar with a magnifying glass icon and a close 'X' button.
- Session Details Panel:** A pane on the right showing details for the selected session (Jenny):
 - Owner: Jenny
 - Type: Session
 - Session Status: In Progress
 - Computer Name: JXNPVWSJPITT
 - Operating System: Windows 7 Enterprise x64
 - Time in the System: 0:05:40
 - IP Address: 172.19.191.29
 - External Key:

Use the Dashboard to Administer Team Members

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

If a user is a team manager or team lead of one or more teams, selecting one of those queues causes the dashboard pane to appear 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.



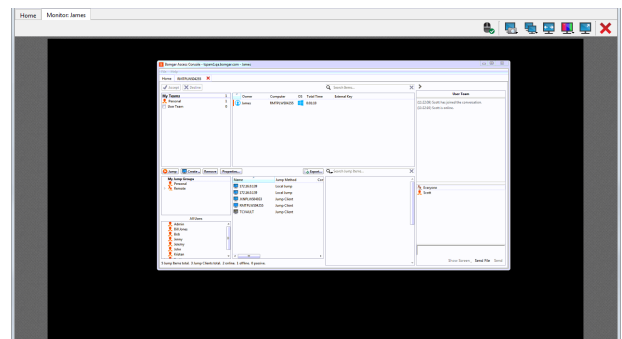
Select a user from the dashboard pane to view any sessions they may be running. A team manager or team lead can take over a session from another user of that team by selecting the appropriate session from the queue and clicking the **Take Over** button. This transfers ownership of that session to the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

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



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

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 is 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, the icon 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 the user's console.

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

Within a team, a user can administer 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 administer another user in one team but not be able to administer that same user in another team.



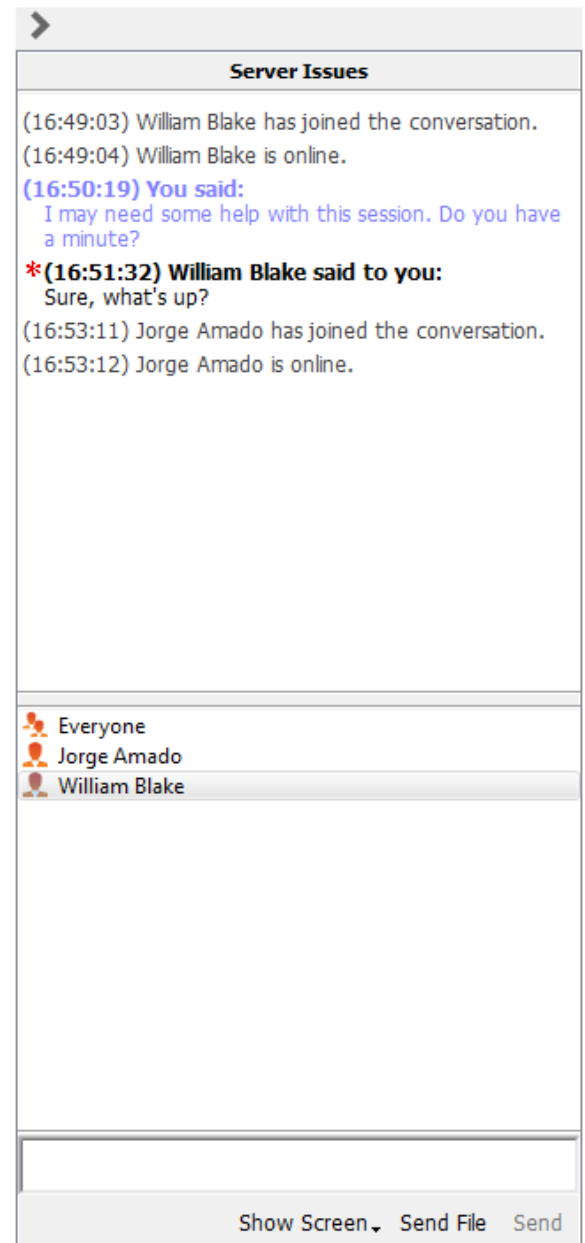
Chat with Other Users

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 that one.

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

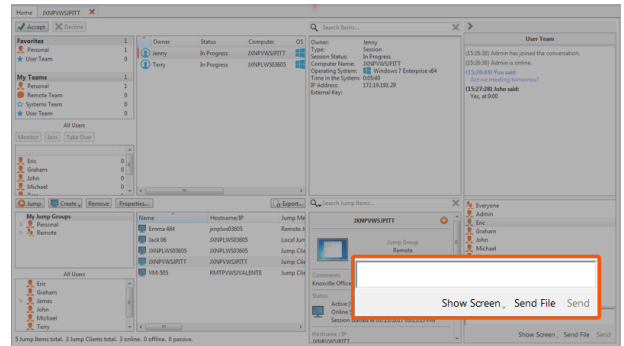
In the settings, you can choose if the team chat should include status messages, such as users logging in and out, or only chats sent between team members.



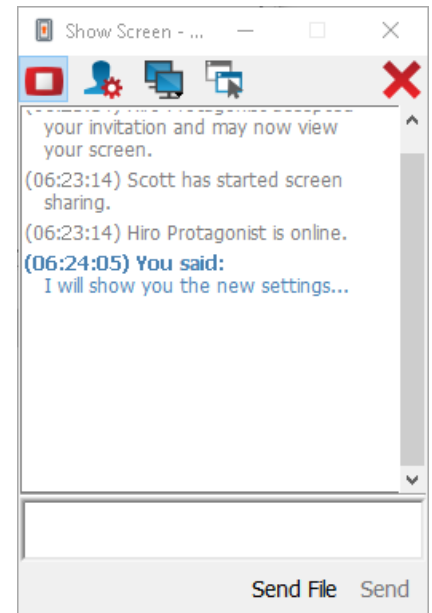
Share your Screen with Another User

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 will be visible to the other user. Once you have made your selection, the receiving user will get 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 will be 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.

Share a Session with Other Users

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.

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

If you select **Any User**, the invitation is sent to the team queue so that any single user in the selected team can join the session. You can send multiple invitations if you want more users 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.

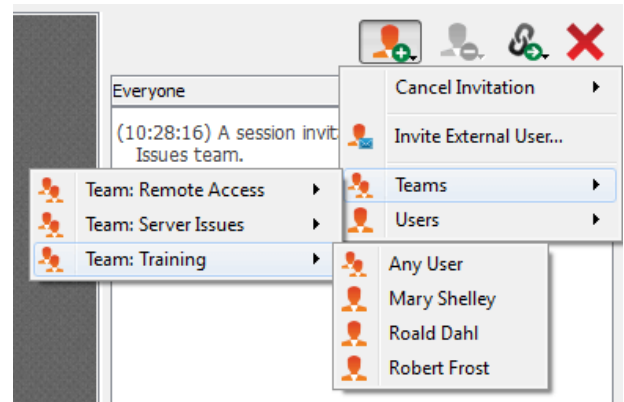
When you invite a user with extended availability enabled, they receive an email notification.

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 session ends
- The invited user accepts the invitation
- The invited user declines the invitation

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



Chat with Other Users During a Shared Session

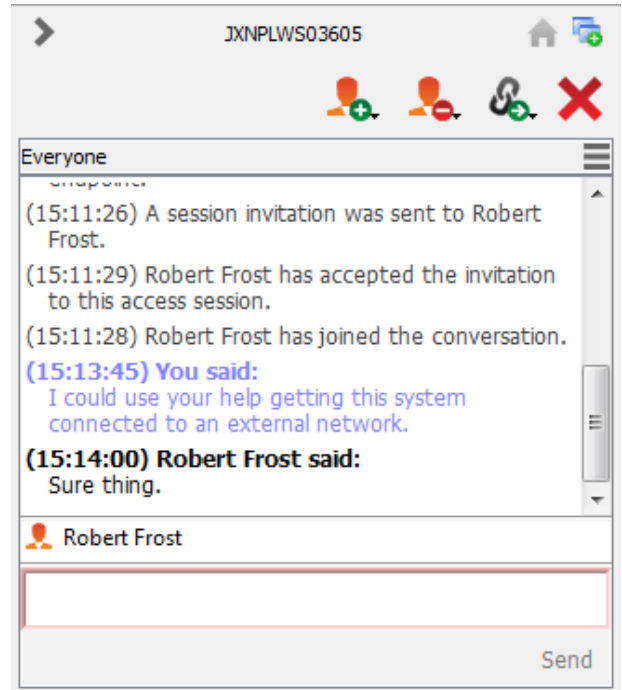
The session chat window serves as a running log of everything that happens throughout the session, including files transferred and tools used.

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

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

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.



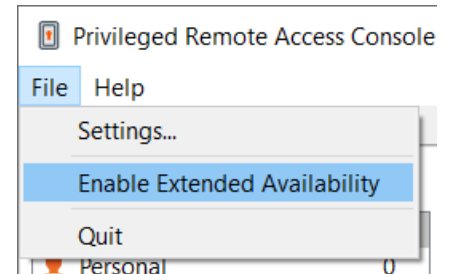
Note: It is possible to reposition the different widget sections displayed on the sidebar, like the chat window, the session info pane, etc. When hovering over the title bar of a section, the cursor turns into a closed hand, allowing you to drag and reposition that section on the sidebar.

Use Extended Availability to Remain 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.

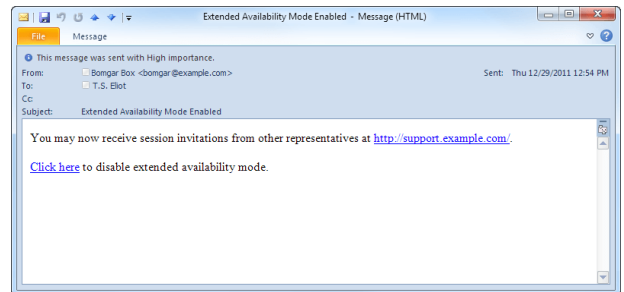
If your account is configured for extended availability, you can enable or disable the functionality from the **File** menu of the access console.

If you have extended availability enabled, you will 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.



Email Notification & Invitation

Each time you enable extended availability mode, the B Series Appliance will notify you via the email address configured for your user account.

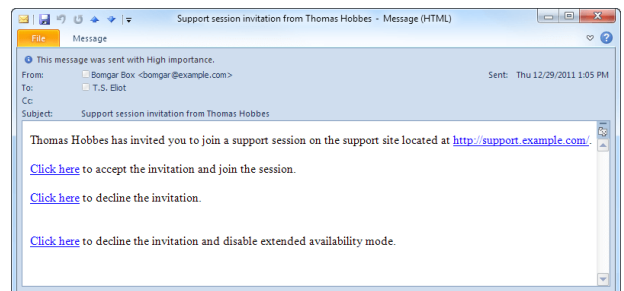


Note: BeyondTrust does not pull email addresses from external LDAP directory stores. The email address must be configured in BeyondTrust in one of two ways:

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.

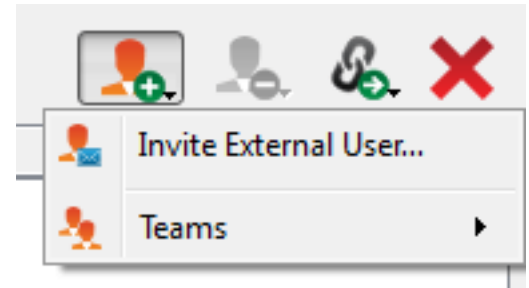
The notification includes the URL of the site as well as a link to quickly disable extended availability mode.

The B Series 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.



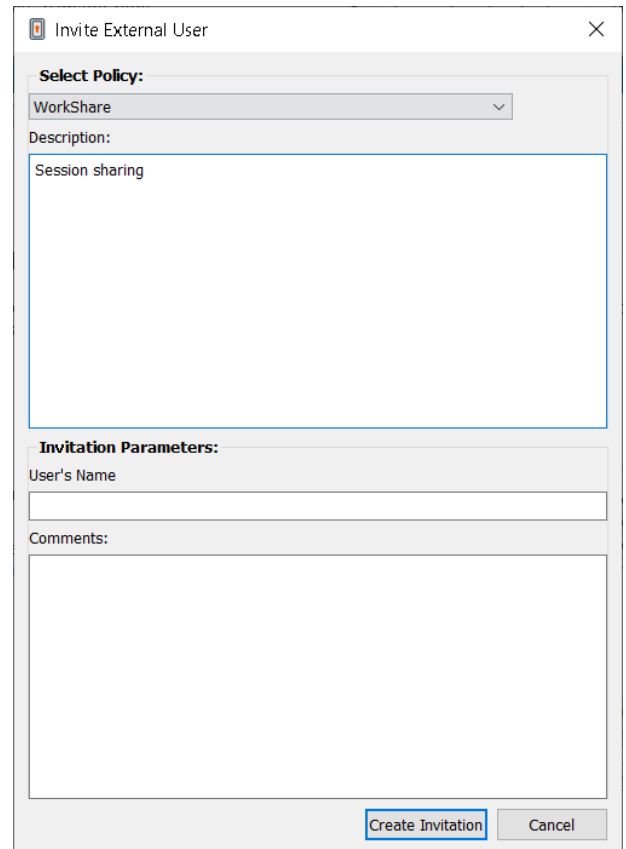
Invite an External User to Join an Access Session

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 User**.

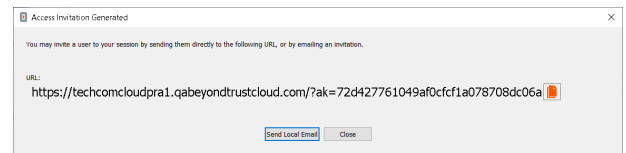


A dialog opens asking the user to select a session policy. These policies are created in the administrative interface and determine the level of permission the external user will have. When you select a policy, the full description displays below.

Enter the invited user's name. This name will appear in the chat window and in reports. Next, enter comments about why this user has been invited. Click **Create Invitation**, and a new dialog containing the invitation URL appears.



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 must download and run the access console installer, which is an abbreviated process from the full access console installation.



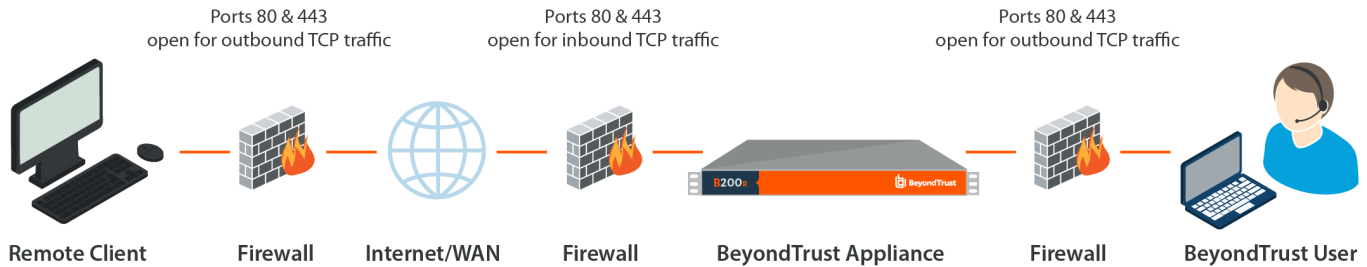
The external user will have access only to the session tab and has a limited set of privileges. The external user can never be the session owner. When the inviting user leaves the session, the external user is logged out.

You can invite more than one external user to a session.

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.

TYPICAL NETWORK SETUP



- 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 [BeyondTrust Appliance B Series Hardware Installation Guide](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/index.htm>.
- 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
 - bomgar-pec-{uid}.exe
 - bomgar-pec.exe

For assistance with your firewall configuration, please contact the manufacturer of your firewall software.

- Example firewall rules based on B Series Appliance location can be found at www.beyondtrust.com/docs/privileged-remote-access/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.