BeyondTrust

Privileged Remote Access 23.2
Privileged Web Access Console

TC:8/28/2023

Table of Contents

Privileged Web Access Console Guide

With the BeyondTrust privileged web access console, Information and Cyber Security teams can grant privileged users secure remote access to critical systems, even when those users do not have the ability to install software within their own desktop environments. Instead, they can access endpoints through the web-based access console. This ensures that the necessary access can always be granted and enables system owners to meet business requirements, such as system up-time and any other internal or external regulations without compromising defenses put in place to protect their organization from any sort of malicious cyber threat.

In this guide, we will specifically discuss the privileged web access console and how this browser-based access console accesses endpoints and performs other necessary functions while ensuring that the highest level of security is maintained.

> ***Note:*** *Use this guide only after an administrator has performed the initial setup and configuration of the B Series Appliance as detailed in the BeyondTrust Appliance B Series Hardware Installation Guide. Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.*

Privileged Web Access Console Requirements

To run the privileged web access console on your system, your B Series Appliance must be running software version 15.3 or higher. The privileged web access console is supported on the following platforms and browsers:

Platforms

- Windows
- Macintosh
- Linux

Browsers

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

IMPORTANT!

Your B Series Appliance must be equipped with a valid SSL certificate signed by a certificate authority. Once you have applied a CA-signed SSL certificate to your B Series Appliance, contact BeyondTrust Technical Support. Your support representative will create a new software build that integrates your SSL certificate. With this updated build installed on your B Series Appliance, you can run the BeyondTrust access console on your device to access your endpoints from virtually anywhere.

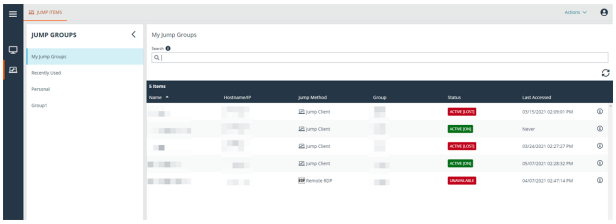
Launch the Web Access Console

The privileged web access console enables you to securely add, access, edit, and remove your endpoints by connecting to them remotely through the B Series Appliance. To begin accessing endpoints using the privileged web access console, launch the console as outlined below.

Launch the Web Access Console Using /console

This is the quickest way to access the web console.

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



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.

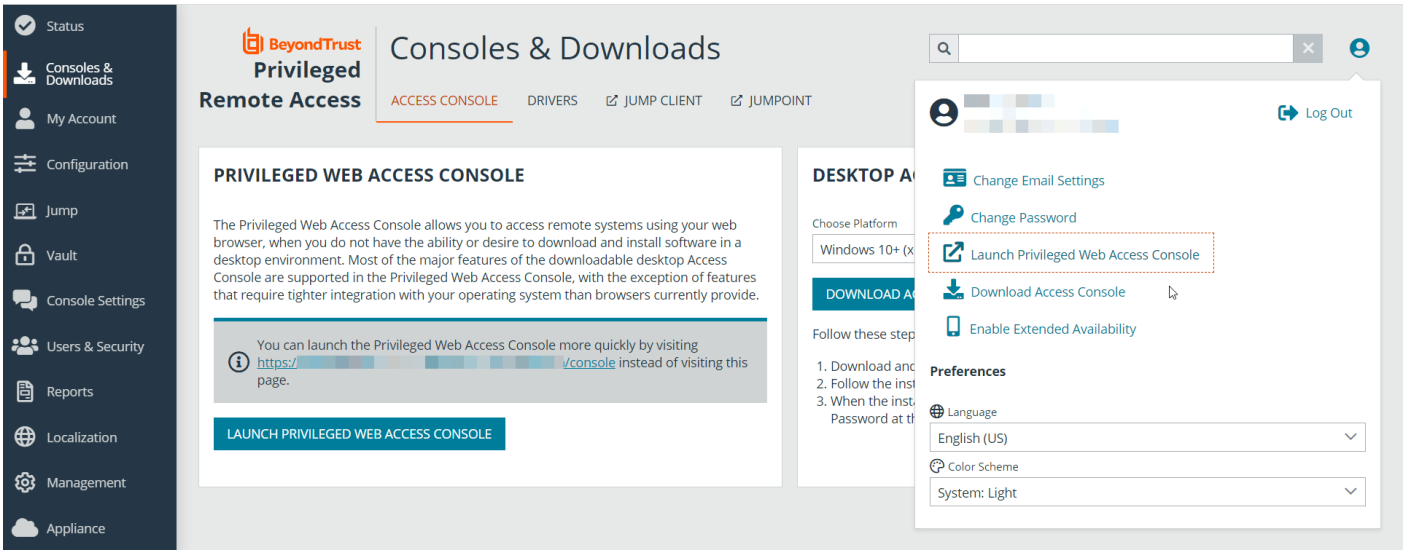
If passwordless login has been enabled, **Authenticate Using** may default to **Passwordless FIDO2**, or it can be selected. The exact process for passwordless login depends on the type of device and manufacturer.

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**.

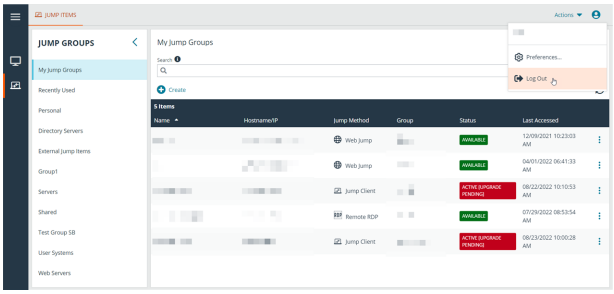
Launch the Web Access Console Using /login

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

1. In the address bar of your browser, enter your BeyondTrust site hostname followed by **/login**, for example, **access.example.com/login**.
2. Enter the username and password associated with your BeyondTrust user account, and click **Login**, or log in using passwordless authentication.
3. Click **Consoles & Downloads** in the left menu, or click the user icon in the upper-right corner of the screen. The image below shows both options selected.



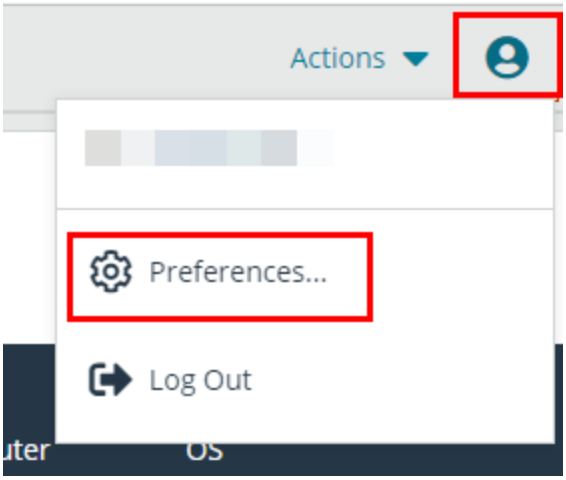
4. Click **Launch Privileged Web Access Console** on the **Consoles & Downloads** screen or on the user options window.
5. The privileged web access console opens in a new tab, and you can begin working with endpoints.



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

Privileged Web Access Console Preferences

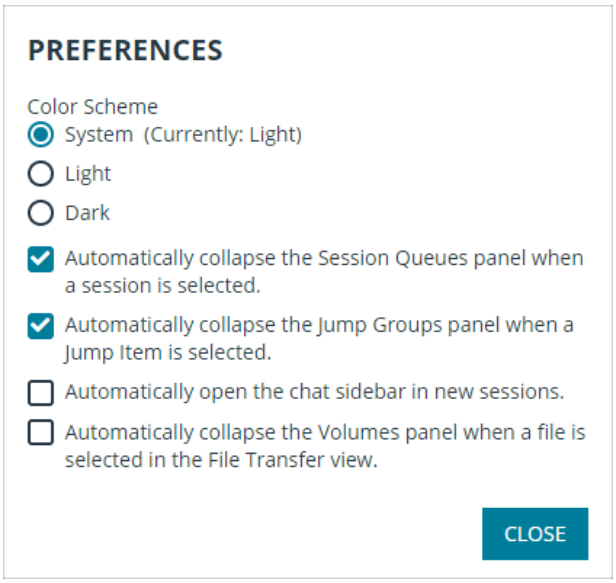
The language and color scheme options visible when the user icon is clicked in the /login administrative interface affect only that interface. To set preferences in the web access console, click the user icon in the upper-right corner of the web access console, and then click **Preferences**. Select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



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

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

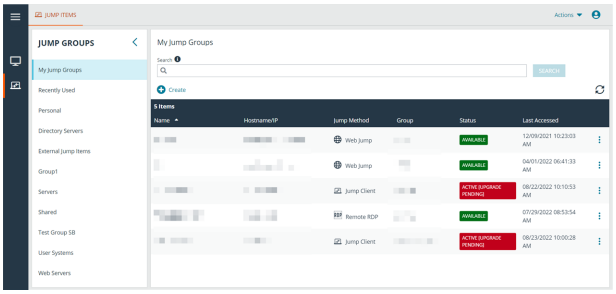
- Automatically collapse the **Session Queues** panel when a session is selected.
- Automatically collapse the **Jump Groups** panel when a Jump Item is selected.
- Automatically open the chat sidebar in new sessions.
- Automatically collapse the **Volumes** panel when a file is selected in the **File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



Use Jump Items to Access Endpoints in the Privileged Web Access Console

To access an endpoint, install a Jump Item. You can install a Jump Item by clicking **Create** at the top of the Jump interface. Full details for creating Jump Items are provided later in this guide. 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, as well as Jump Item shortcuts.

Jump Items are listed in Jump Groups. If you are assigned to one or more Jump Groups, you can access the Jump Items in those groups, with the permissions assigned by your admin.



Your personal list of Jump Items is primarily for your individual use, although your team leads, team managers, and users with permission to see all Jump Items may have access to your personal list of Jump Items. Similarly, if you are a team manager or lead with appropriate permissions, you may see team members' personal lists of Jump Items. Additionally, you may have permission to access Jump Items in Jump Groups you do not belong to and personal Jump Items for non-team members.

There are three ways that you can begin accessing endpoints:

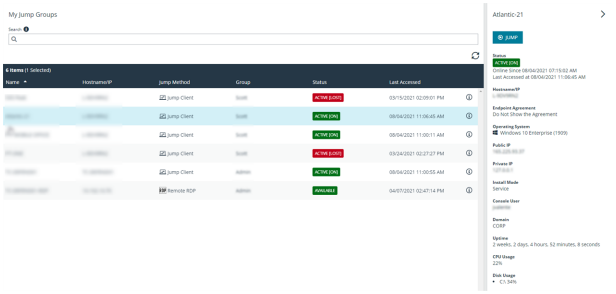
- Locate and select an endpoint from the **My Jump Groups** list.
- Choose a Jump Group and then select an endpoint from that group's listing of endpoints.
- Select a session from the **Frequently Used Jump Items** list.

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

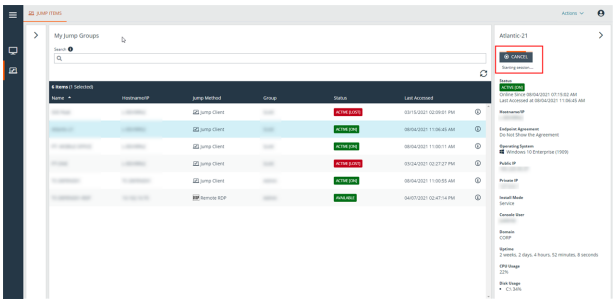
> ***Note:*** *The Jump Items list can only display a maximum of 50 Jump Items.*

To begin accessing Jump Items, follow the steps outlined below:

1. Select a Jump Group and click the **Refresh** button.
2. A list of all Jump Items populates, and you can review details about the Jump Item, including: **Name**, **Method**, **Group**, **Status**, and **Last Accessed**. To review more details about the Jump Item, click on the plus sign beside the Jump Item's name.
3. Click the **JUMP** button to start a session with the endpoint.



4. To cancel a Jump access request, click **Cancel**.

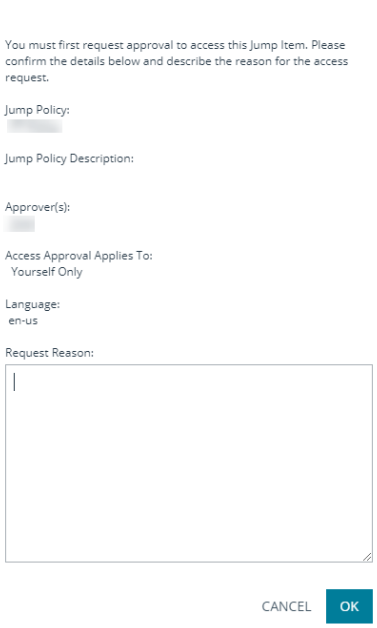


End-User and Third-Party Authorization

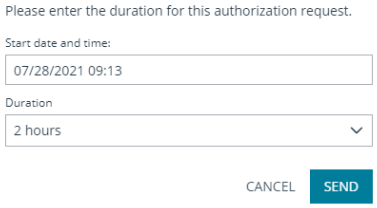
Depending on the configuration of Jump Items within the /login administrative interface, a Jump Item may have a Jump Policy associated with it, and the policy may define an authorization component that forces you to request permission from a third-party or an administrator before you are able to start an access session with the Jump Item.

> *For more information about how to configure third party and end-user notifications and approval, please see Jump Policies: Set Schedules, Notifications, and Approval for Jump Items at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm.*

1. After you have clicked the **JUMP** button and requested access, a prompt appears, and you are required to enter a reason for wanting to access the system.



2. Next, you must indicate when and for how long you will be accessing the system.
3. Once the request has been submitted, the third party or person responsible for approving access requests is alerted through an email notification and has the opportunity to accept or deny the request. Although other approvers can see the email address of the person who approved or denied the request, the requestor cannot.

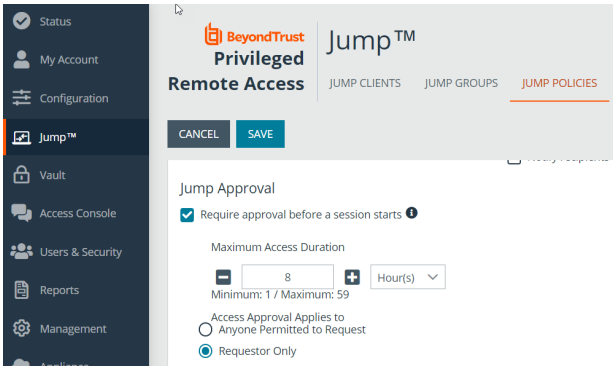


4. After permission has been determined, an authorization notification appears within the Jump Item's information displaying either *approved* or *denied*. If access is granted, you can tap the Jump button to begin accessing the system.
5. Then you are presented with a message asking if you would like to begin an access session.
6. If you choose to begin the session, the approving party's comments appear, and you can begin accessing the system.

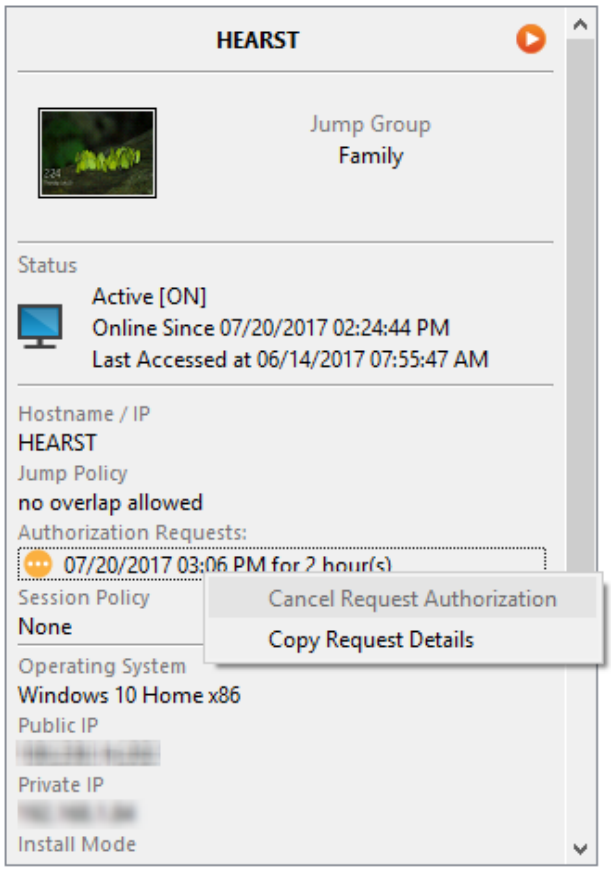
Revoke an Access Approval Request

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:

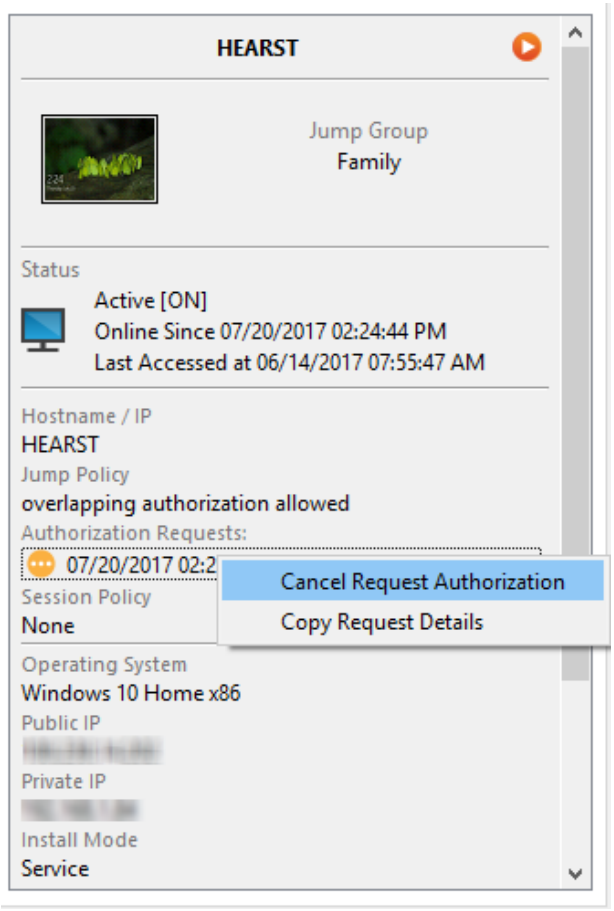
- **Anyone Permitted to Request**
- **Requestor Only**



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.



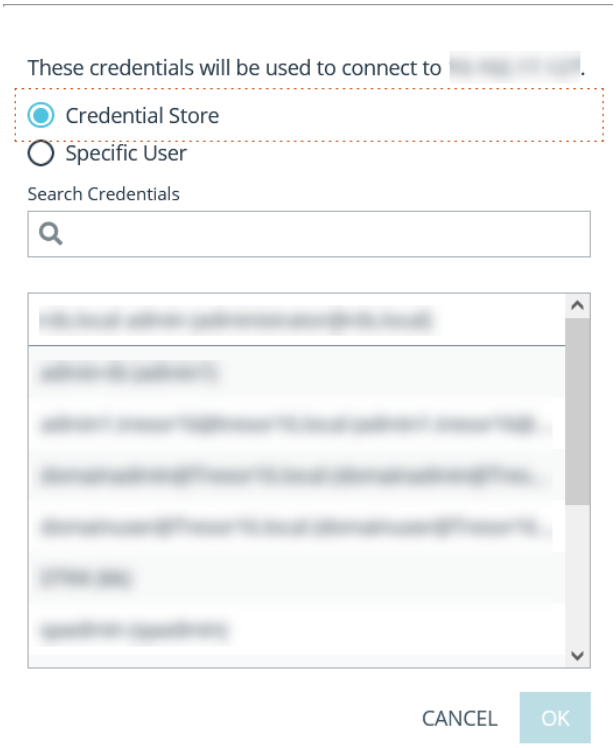
However, if the Jump Policy is set to **Anyone Permitted to Request**, and an Access Request is presently approved for User A, User B is allowed to start a new session with the Jump Item if they attempt to Jump to it. In addition, anyone with permission to access the Jump Item is allowed to cancel /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



Automatic Log On Credentials

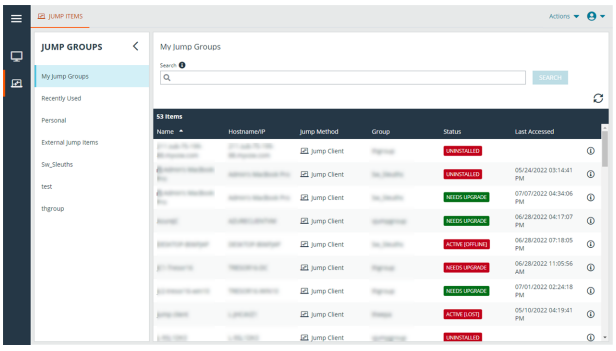
Credentials from the **Endpoint Credential Manager** can be used for RDP and for performing Remote Jump. If a user selects to Jump to a Remote Jump or Remote RDP and no automatic log on credentials are available, a username and password must be entered into the prompt before the access session can begin with the endpoint. If the /login administrative interface has been configured with automatic log on credentials and returns only one set of credentials as being available for a particular user and Jump Item, the credential request is skipped, and the single credential is used to start the session. If there is more than one credential configured in the /login administrative interface, the user has the choice either to choose credentials from the credential store or to enter their own credentials manually.

> *For more information on credential configuration and management, please see Security: Manage Security Settings at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.*

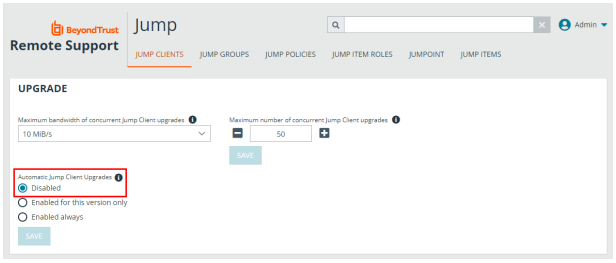


Jump Client Upgrade

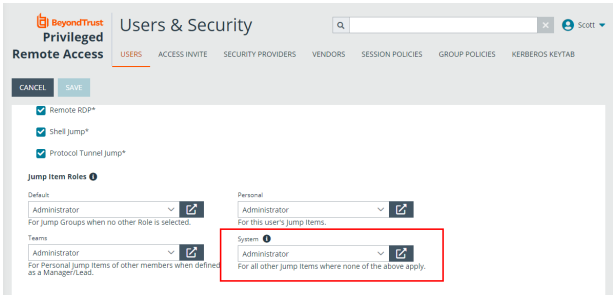
You can upgrade Jump Clients from within the privileged web access console. A **Needs Upgrade** banner displays under **Status**, in green if the Jump Client is online, red if offline. You can only upgrade Jump Clients that are online. To upgrade a given Jump Client, click the green banner.



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



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



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.

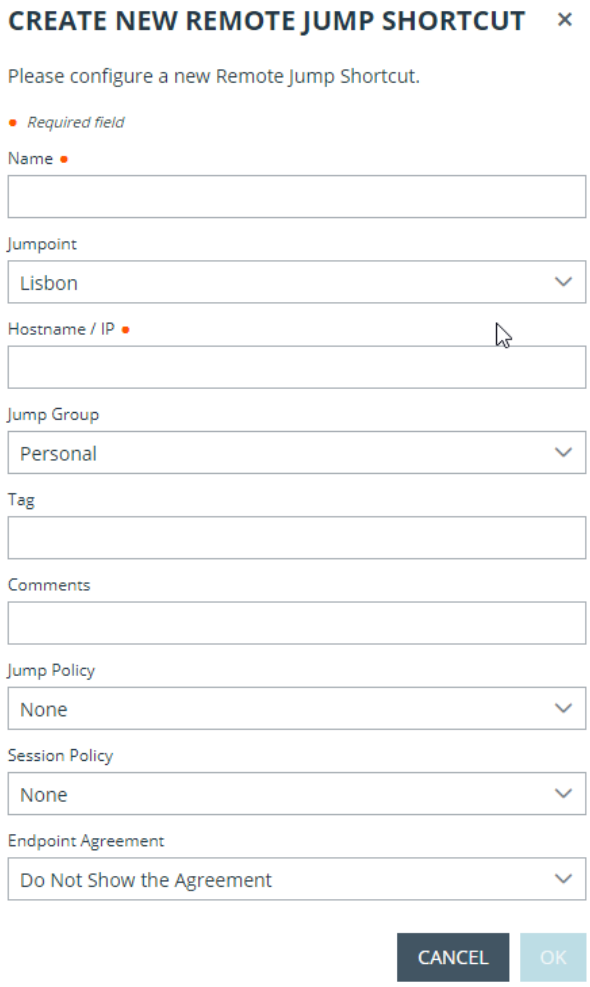
Further organize Jump Items by entering the name of a new or existing **Tag**. Even though the selected Jump Items are grouped together under the tag, they are still listed under the Jump Group in which each Jump Item is pinned. To move a Jump Item back into its top-level Jump Group, leave this field 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 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 at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.*

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.

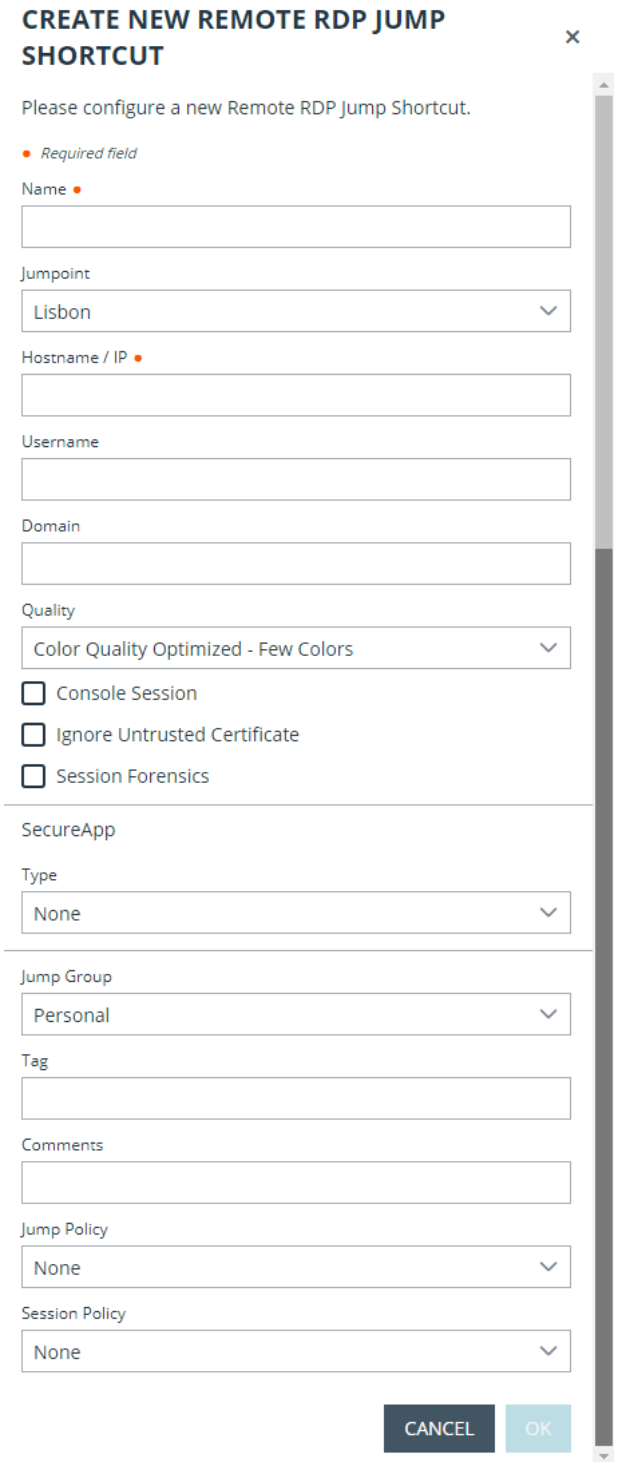
> ***Note:*** *By default, the RDP server listens on port 3389, which is therefore the default port BeyondTrust attempts. If the remote RDP server is configured to use a different port, add it after the hostname or IP address in the form of* ***<hostname>:<port>*** *or* ***<ipaddress>:<port>*** *(for 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 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
%USERPRINCIPLENAME%	username@domain
%DOWNLEVELLOGONNAME%	domain\username
%DOMAIN%	domain
%PASSWORD%	password
%PASSWORDRAW%	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.

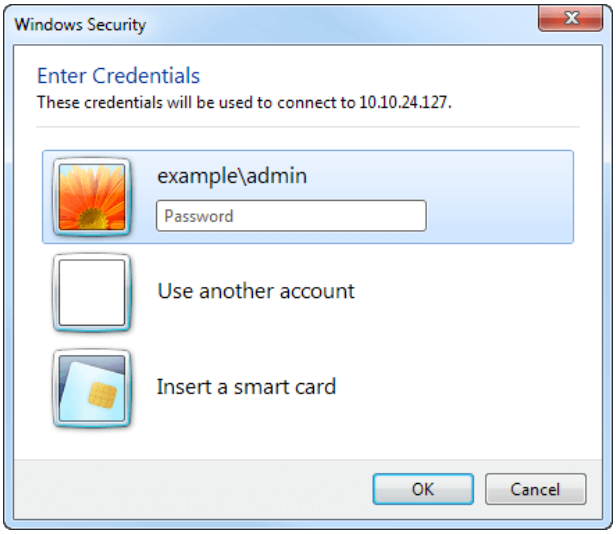
To set when users are allowed to access this Jump Item, if a notification of access should be sent, or if permission or a ticket ID from your external ticketing system is required to use this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the /login interface.

For more information about contained database users, please see Contained Database Users - Making Your Database Portable 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 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

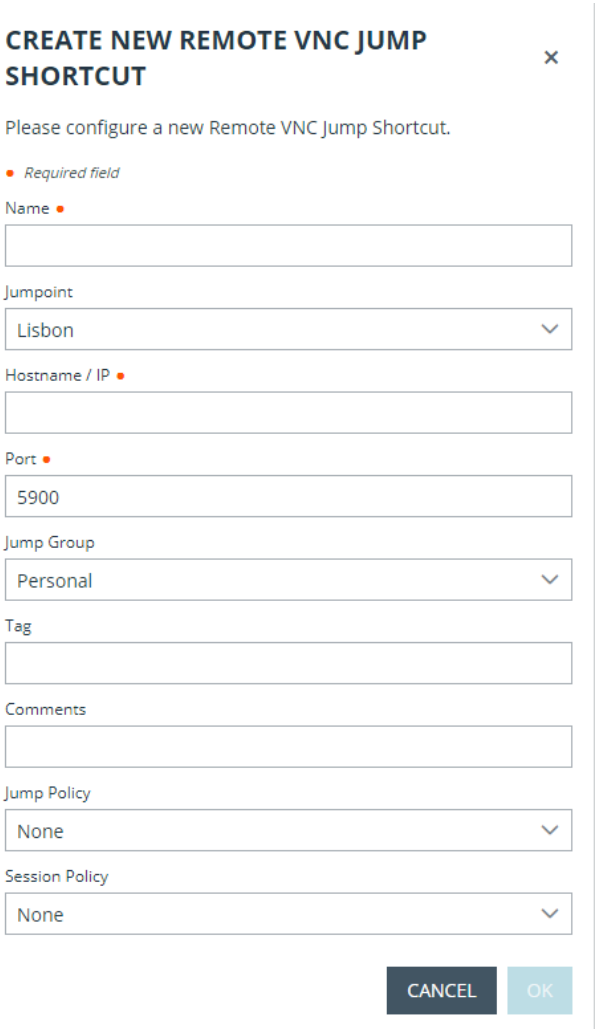
To create a VNC shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote VNC**. VNC shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

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 at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

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 1**.*

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.

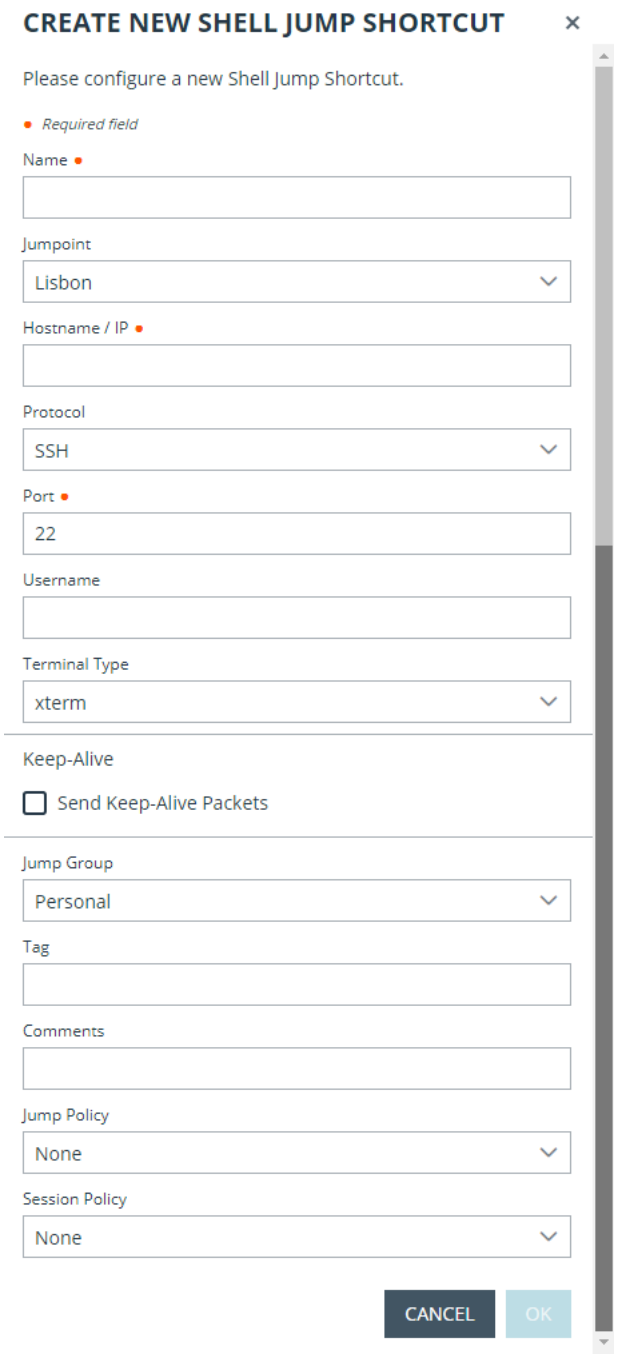
Move Jump Items from one Jump Group to another using the **Jump Group** dropdown. The ability to move Jump Items to or from different Jump Groups depends upon your account permissions.

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.



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 undesireable 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++) 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 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!

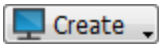
Web Jump does not support Flash. Be sure to consult your hypervisor documentation and update it to a version that supports HTML5.

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.

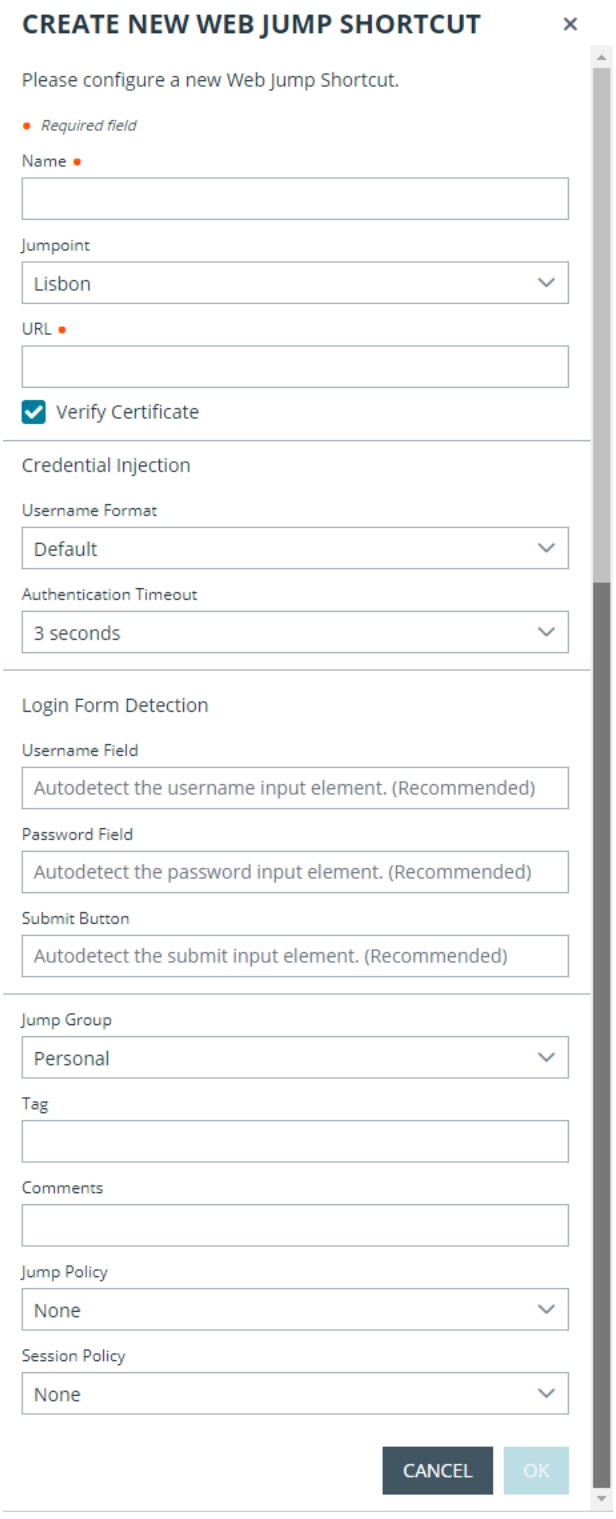
> ***Note:*** *Copy/Paste functionality is not supported for Linux Jumpoints.*

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.

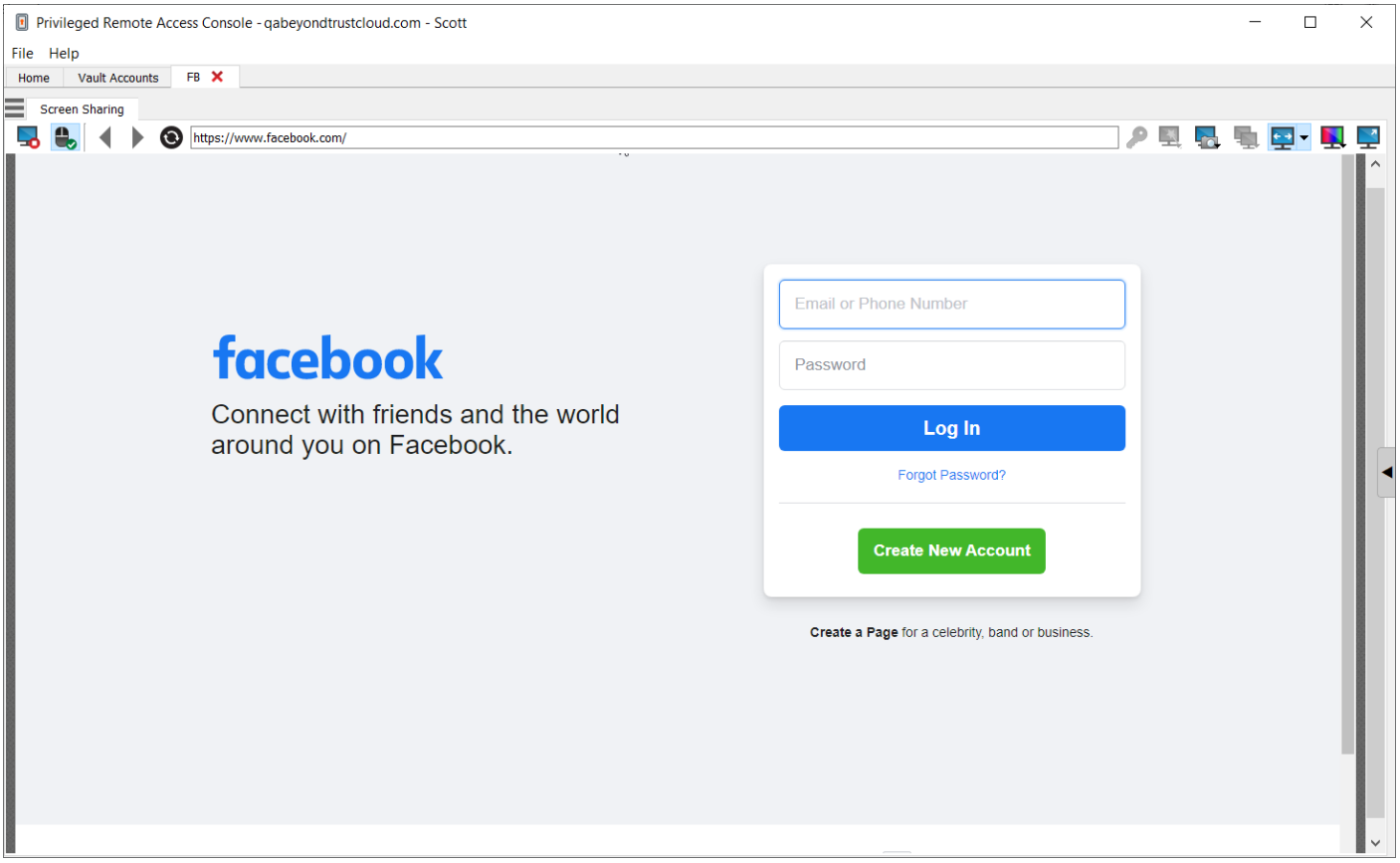
Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

For more information about identifying HTML form fields, please see online resources such as this page explaining the use of CSS selectors 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.

Log Into Endpoints Using Credential Injection

When accessing a Windows-based Jump Item via the privileged web 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.

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.*

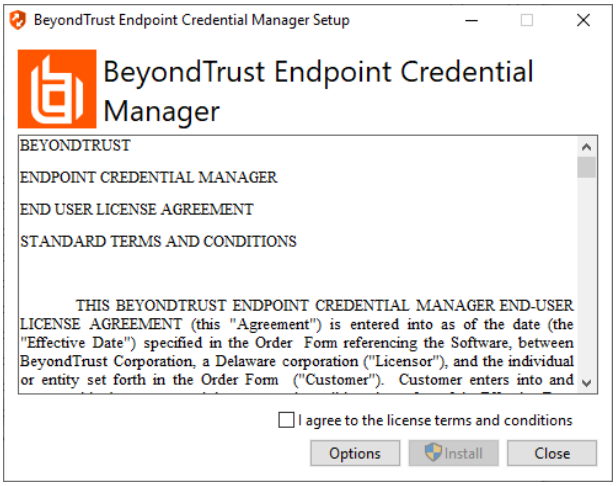
System Requirements

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

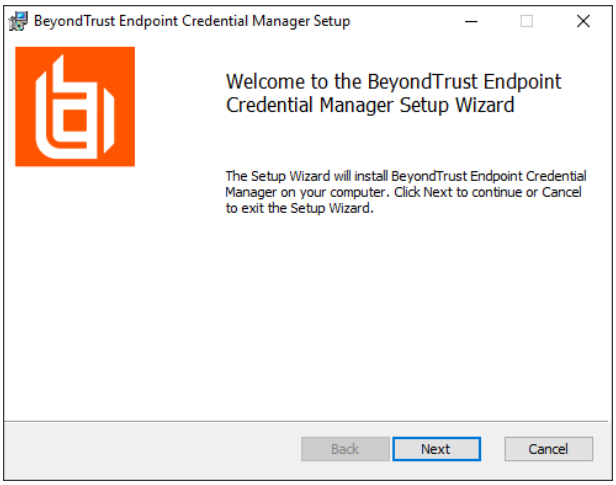
1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from BeyondTrust Support at beyondtrustcorp.service-now.com/csm.
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Check the box if you agree, and then click **Install**.

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

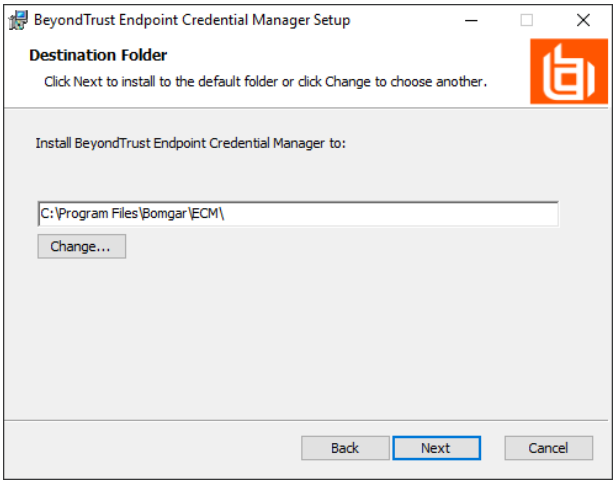
> ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*



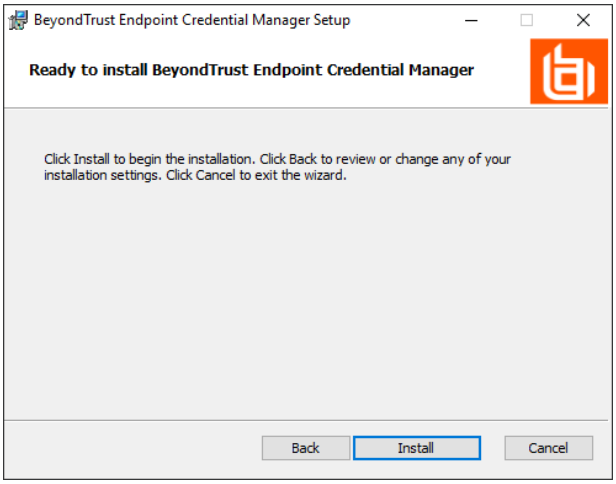
4. Click **Next** on the Welcome screen.



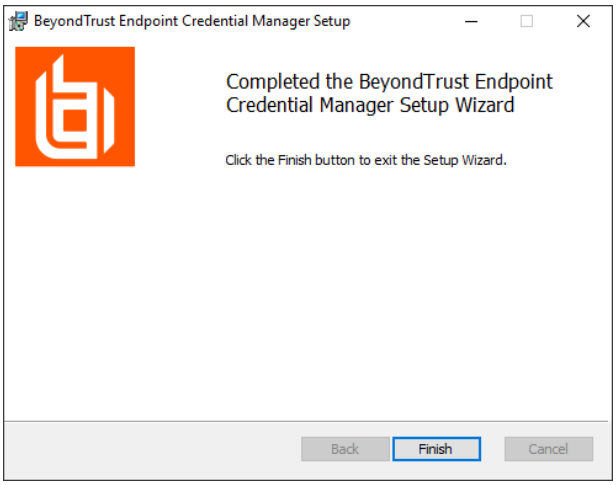
5. Choose a location for the credential manager, and then click **Next**.
6. On the next screen, you can begin the installation or review any previous step.



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



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

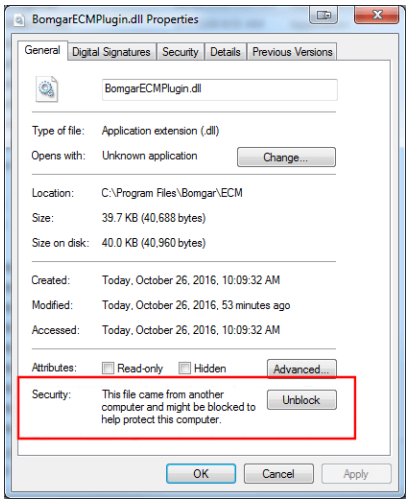


Note: *To ensure optimal up-time, administrators can install up to three ECMs on different Windows machines to communicate with the same credential store. A list of the ECMs connected to the appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

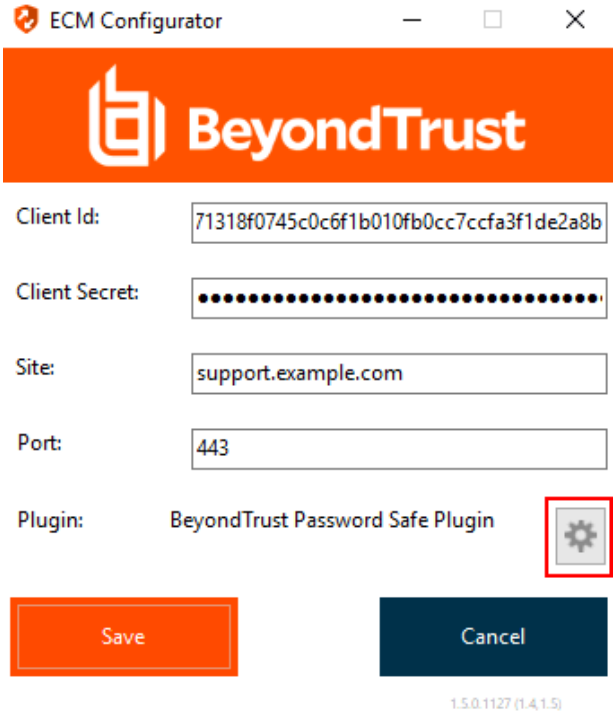
Note: *When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Seriesroutes requests to the ECM in the ECM Group that has been connected to the appliance the longest.*

Install and Configure the Plugin

1. Once the BeyondTrust ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
2. Run the **ECM Configurator** to install the plugin.
3. The Configurator should automatically detect the plugin and load it. If so, skip to step 4 below. Otherwise, follow these steps:
   - First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
   - On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
   - Repeat these steps for any other DLLs packaged with the plugin.
   - In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL.



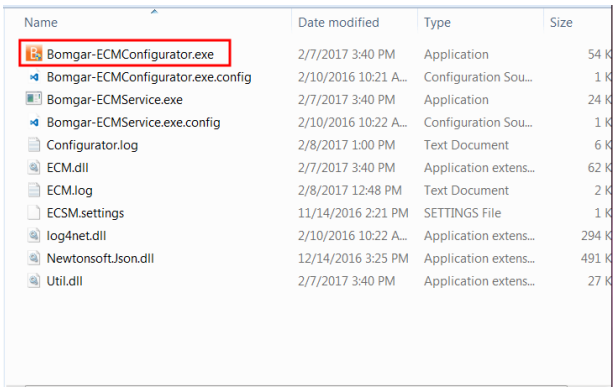
4. Click the gear icon in the **Configurator** window to configure plugin settings.



Configure a Connection to Your Credential Store

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

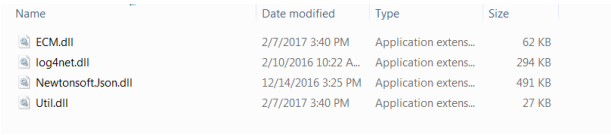
1. Locate the BeyondTrust ECM Configurator you just installed using the Windows Search entry field or by viewing your **Start** menu programs list.
2. Run the program to begin establishing a connection.
3. When the ECM Configurator opens, complete the fields. All fields are required.



Enter the following values:

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

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



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

IMPORTANT!

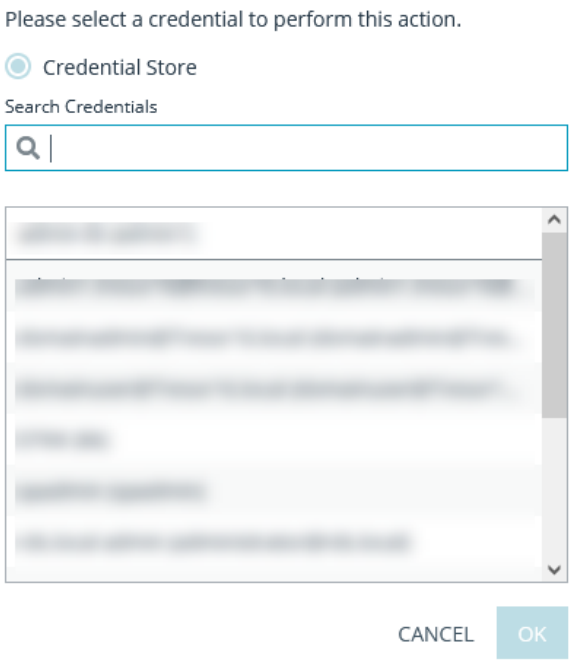
To apply new settings in the configuration, restart the ECM service.

Use Credential Injection to Access Endpoints

After the credential store has been configured and a connection established, the privileged web access console can begin using credentials in the credential store to log into endpoints.

1. Log into the privileged web access console.
2. Jump to an endpoint with a Jump Item installed as an elevated service on a Windows machine.
3. Click the **Play** button to begin screen sharing with the endpoint. If the endpoint 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.

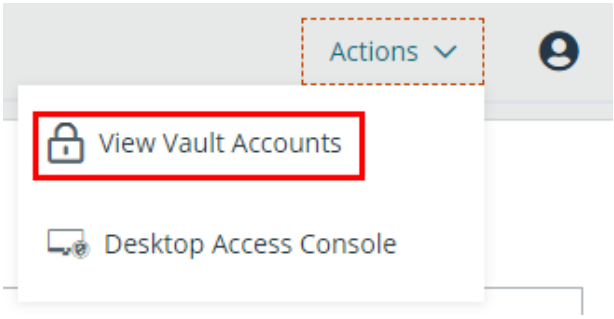
5. Select the appropriate credentials to use from the ECM. The system retrieves the credentials from the ECM and injects them into the Windows login screen.
6. The user is logged in to the endpoint.



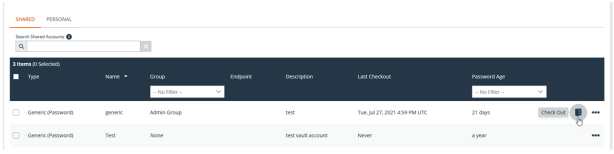
Check In and Check Out Credentials

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

To access the vault, click the **Actions** dropdown in the top navigation bar and select **View Vault Accounts**. You are taken directly to the **Vault > Accounts** page in the **/login** interface, once logged in.



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



Authenticating from the Client Scripting API

This feature allows users to log in to the privileged web access console and Jump to an endpoint using the PRA Client Scripting API (https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api).

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

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

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

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

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

```
https://access.example.com/api/client_script?type=web_console&operation=execute&action=start_
jump_item_session&search_string=ABCDEF02
```

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

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

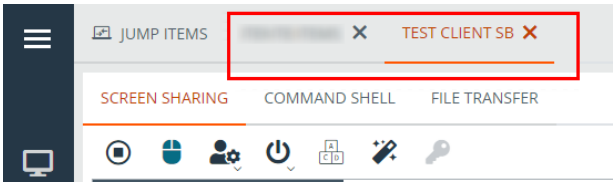
In both cases, if more than one Jump Item matches the search criteria, the user must select the correct Jump Item from a list. If no Jump Items match the search criteria, the privileged web access console shows an error message to the user.

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

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

Return to an Active Session in the Privileged Web Access Console

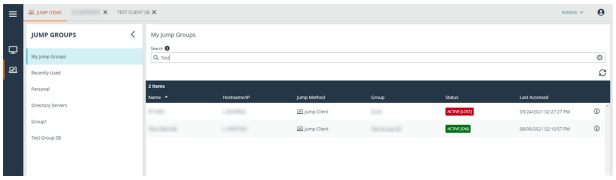
If you have multiple access sessions in progress, you have the ability to return to any of these sessions at any time. To return to an endpoint already accessed in another session, click on the session at the top of the screen.



Search for Endpoints

While using the privileged web access console, you can search for specific endpoints while in an access session. Within the search results, you can also click on the **Start** button to begin a session with that endpoint.

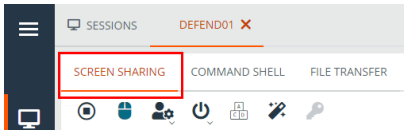
1. Click on the **Search** icon located in the top left of the screen.
2. In the search bar, type in the name of the endpoint.
3. From the results provided, select the endpoint you wish to start a session with and click on the **Jump** button to begin a session.



Control the Remote Endpoint with Screen Sharing Using Privileged Web

To view and control remote systems, use the screen sharing action while in an access session.

1. From the session window, click on the **Screen Sharing** tab at the top of the screen. Or, you can click on the **Start Screen Sharing** icon to begin accessing the endpoint if screen sharing does not start automatically.
2. Use any of the following actions while in a session to perform different functions.



Screen Sharing Tools

	Stop screen sharing.
	While viewing the remote computer, start or stop control of the remote keyboard and mouse. Representatives using a macOS system can send **CTRL+Left-Click** through the connected screen sharing session to the remote system by using **CTRL+CMD+Left-Click**.
	If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The 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**. 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**. 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.
	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.
	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.
	Toggle the clipboard.

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

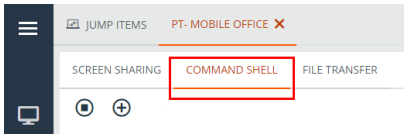
Open the Command Shell on the Remote Endpoint Using the Privileged Web Console

Remote command shell enables a privileged user to open a virtual command line interface to a remote system. The user 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 system from the screen sharing interface.

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

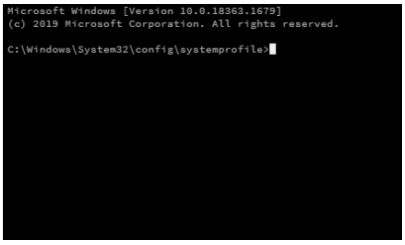
> ***Note:*** *Depending on session policy and type of jump,* ***Command Shell*** *may not be available.*

1. To access the **Command Shell** while in an access session, click on the **Command Shell** tab at the top of the screen.



2. If you are not automatically directed to the command shell, click the **Start the Command Shell** button.

3. The command options and prompt appears.



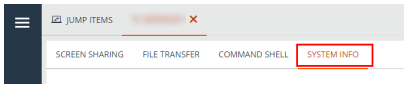
Command Shell Tools

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

View System Information on the Remote Endpoint

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

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



System Information Tools

	Refresh system info.
	Copy to clipboard.
	Save to file.

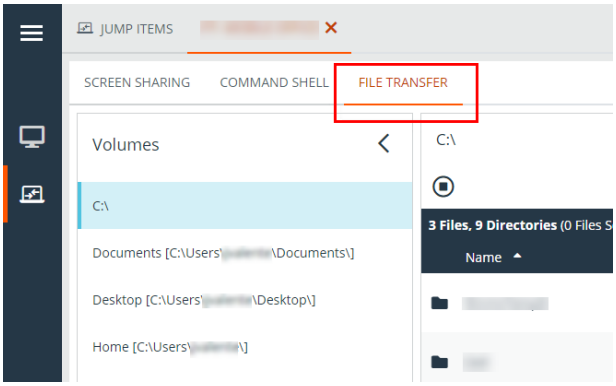
Use the Privileged Web Console to Transfer Files to and from Remote Systems

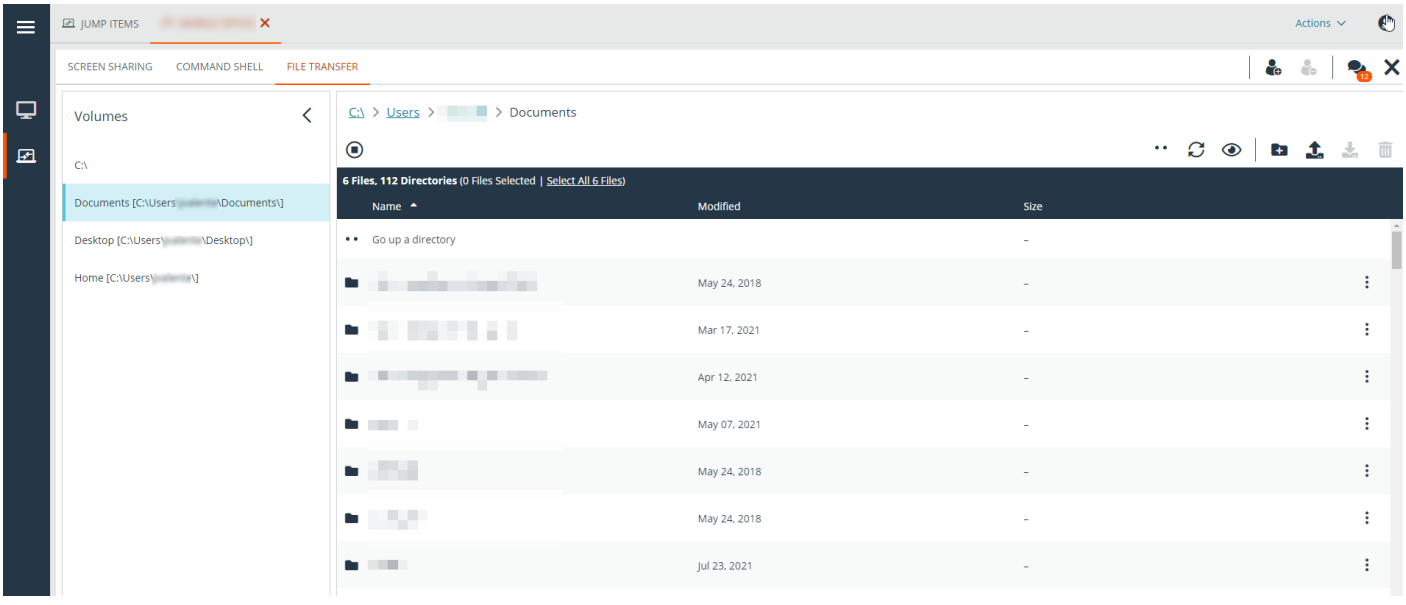
During a session, privileged users can transfer, delete, or rename files and even entire directories both to and from the remote computer, the remote device, and the device's SD card. You do not have to have full control of the remote computer in order to transfer files.

Depending upon the permissions your administrator has set for your account, you may be only allowed to upload files to the remote system or to download files to your local computer. File system access may also be restricted to certain paths on the remote or local system, thereby restricting uploads and downloads to specific directories. Transfer files by using the upload and download buttons. Review transfer and deletion progress by clicking the plus sign at the bottom of the screen. Download, rename, or delete files by clicking on the **More Options** icon.

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

Select a place to start browsing from the **Volumes** column. The breadcrumbs at the top show your current location. Double click on a folder to open it.





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

File Transfer Tools

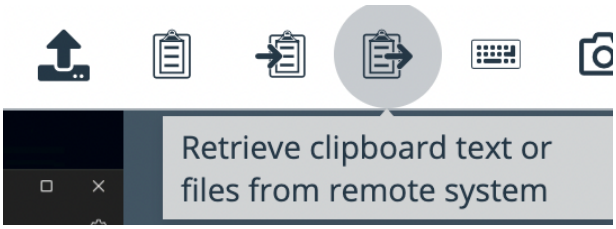
	Stop access to the remote device's file system.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Show hidden files.
	Create a new directory.
	Upload a file to a directory / share files with the RDP clipboard.
	Download selected files from a directory.
	Toggle modifier keys.
	Send clipboard text to remote system.
	Retrieve clipboard text from remote system / retrieve clipboard text or files from remote system (RDP).
	Delete selected files from a directory.
	Download, rename, or delete a directory or file.  ***Note:*** *When deleting a file or folder, it is permanently deleted. It is not sent to the recycle bin.*

RDP File Transfer

Download Files

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

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



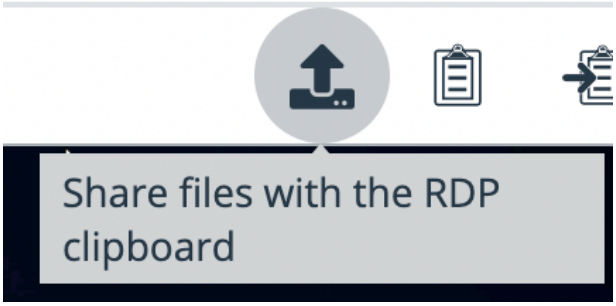
Upload Files

Uploading files in the privileged web access console is a two step process:

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

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

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



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

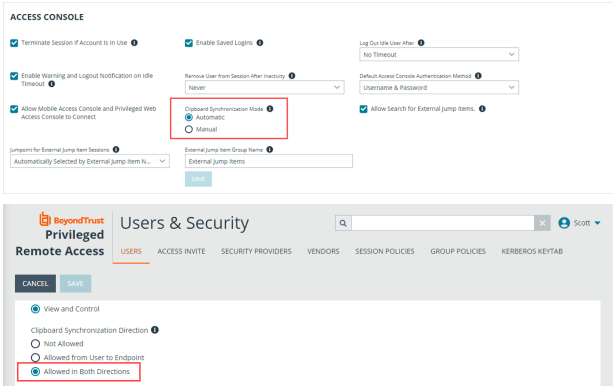
Once you paste on the endpoint, Windows shows the progress of the transfer in a dialog on the endpoint and provide a cancel button.

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

Settings

In order for the file transfer to work as described, you need to ensure that the following settings are as follows:

- **Clipboard Synchronization Mode** is set to **Automatic** (see **/login > Management > Security > Access Console**)
- The user's **Clipboard Synchronization Direction** is set to **Allowed in Both Directions** (see **/login > Users & Security > Users > Session Permissions > Clipboard Synchronization Direction**).



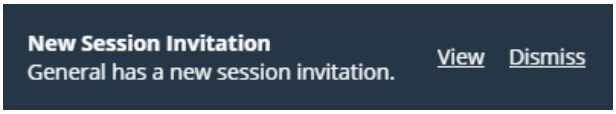
Share a Session with Team Members or External Users Using the Privileged Web Access Console

Invite Team Members

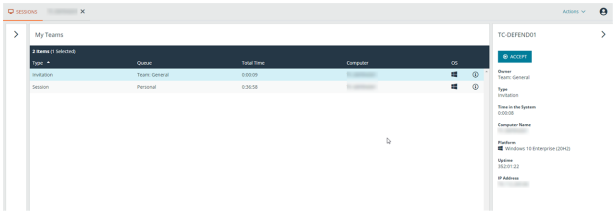
Within a session, you can request for a team member to participate in an access session. To share a session, follow the steps outlined below.

1. Click the **Invite other users into this session** icon.
2. Select the team that the user is a member of from the menu.
3. From the team listing, choose the user with whom you would like to share the session.

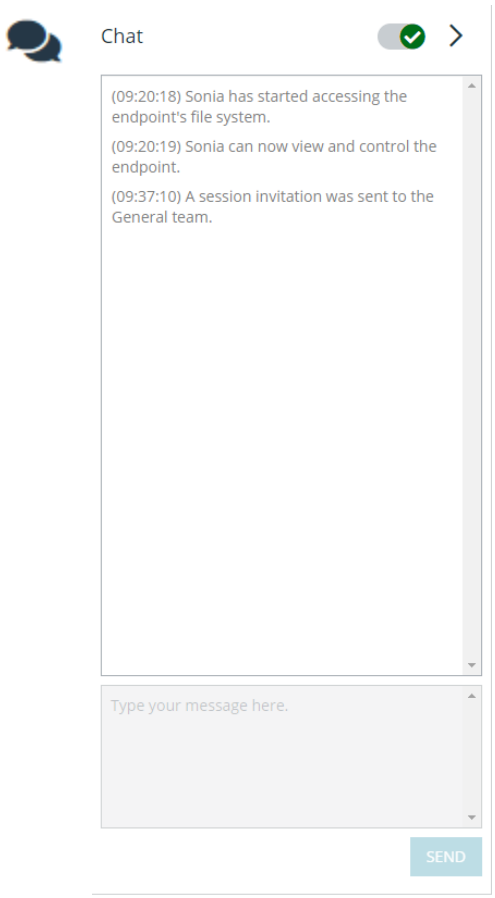
4. The user being invited will see a notification appear in the lower left corner of the screen indicating they have a new session invitation.



5. Clicking **VIEW** on the notification banner displays information regarding the session. The user can then click **ACCEPT** to enter the session.



6. Once the user has entered the session, you can chat with them by clicking on the **Chat** icon at the top of the screen.



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

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

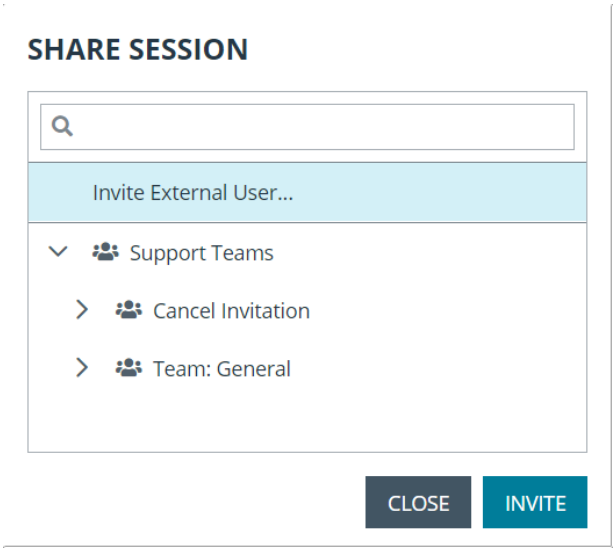
Only the session owner can send invitations. Invitations do not time out as long as you remain the session owner. Multiple active invitations cannot exist for the same user to join the same session. The invitation will disappear if:

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

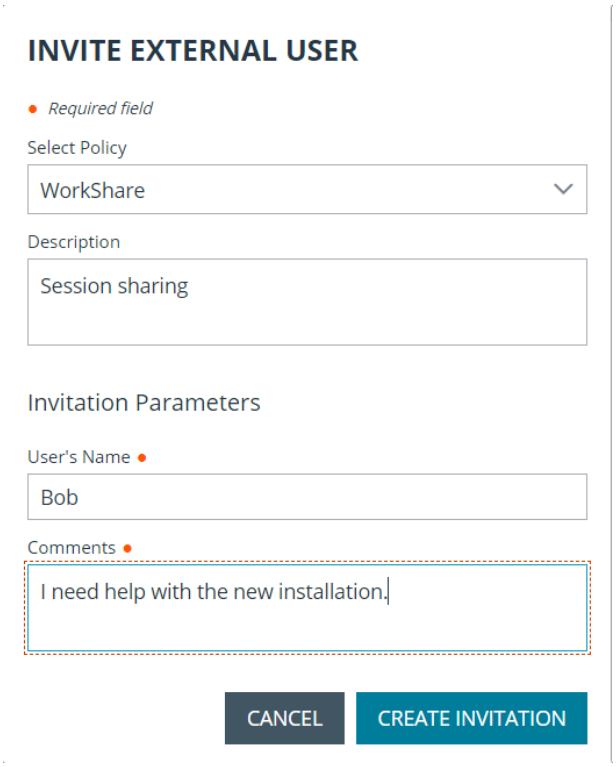
Invite External Users

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

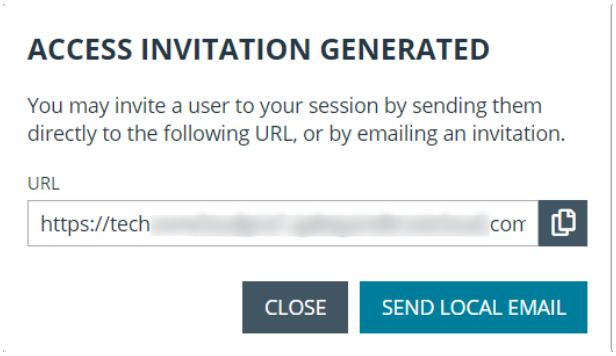
1. Click the **Invite other users into this session** icon.
2. Select **Invite External User...**.



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



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



Remove a Member from a Privileged Web Access Console Session

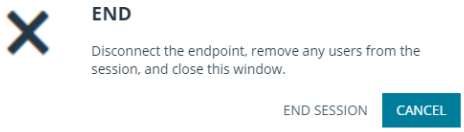
When needed, you can remove another user from a shared access session. To remove a user, click on the **Remove Member** icon.

From the menu, choose the participant you wish to remove. Click **Remove Member**.

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

Close the Privileged Web Access Console Session

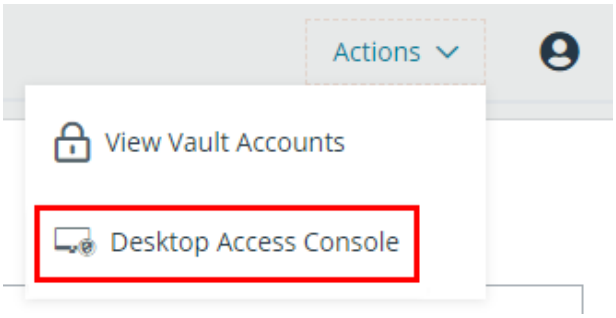
1. To exit an access session, click on the **X** icon in the top right corner of the screen. If you are the session owner, please note that the **End Session** action will close the session page in your access console and will remove any additional members who may be sharing the session.
2. Next, you will receive a prompt asking if you would like to end the session.
3. If you click **OK**, the session will end, and you will be directed back to the **All Jump Items** list.



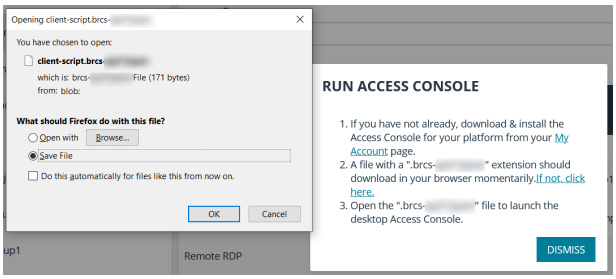
Download the Native Desktop from the Privileged Web Access Console

While working in the privileged web access console, you can choose at any time to download the native desktop access console to your computer.

1. To download the native desktop access console from the privileged web access console, select **Desktop Access Console** located under the **Active** menu in the top right corner of the screen.



2. When the installer appears, follow the instructions to install the software.



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