BOMGAR™

Privileged Access
Privileged Web

TC:9/12/2018

Table of Contents

Privileged Web Access Console Guide

With the Bomgar 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 Bomgar Appliance as detailed in the Bomgar Appliance Hardware Installation Guide. Should you need any assistance, please contact Bomgar Technical Support at help.bomgar.com.*

Privileged Web Access Console Requirements

To run the privileged web access console on your system, your Bomgar 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 Bomgar 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 Bomgar Appliance, contact Bomgar Technical Support. Your support representative will create a new software build that integrates your SSL certificate. With this updated build installed on your appliance, you can run the Bomgar access console on your device to access your endpoints from virtually anywhere.

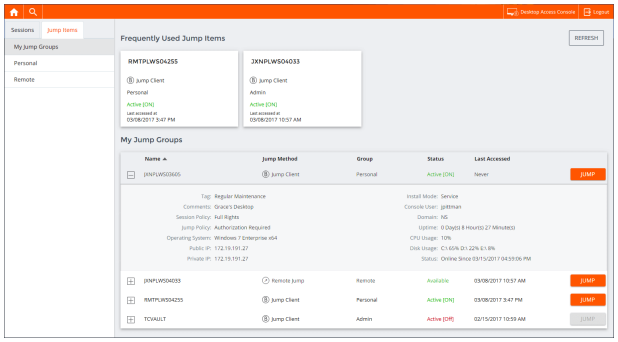
Launch the Web Access Console

The privileged web access console enables you to use a web-based access console to securely access your endpoints by connecting to them remotely through the Bomgar Appliance. To begin accessing endpoints using the privileged web access console, follow the steps outlined below.

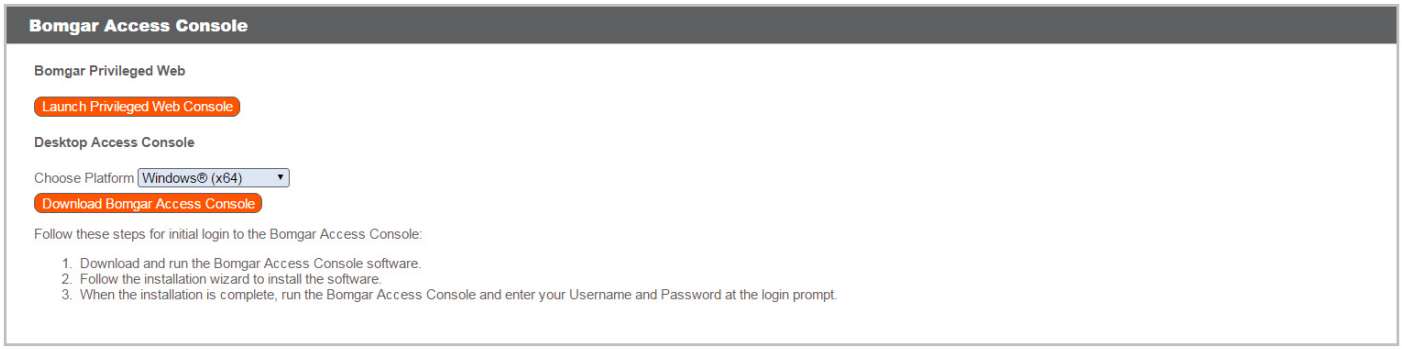
***Note:** By default, the privileged web access console button is not available. You must navigate to **Management > Security** and check **Allow Mobile Bomgar Access Console and Bomgar Privileged Web Access Console to Connect** to activate the console.*

Launch the Web Access Console using /console

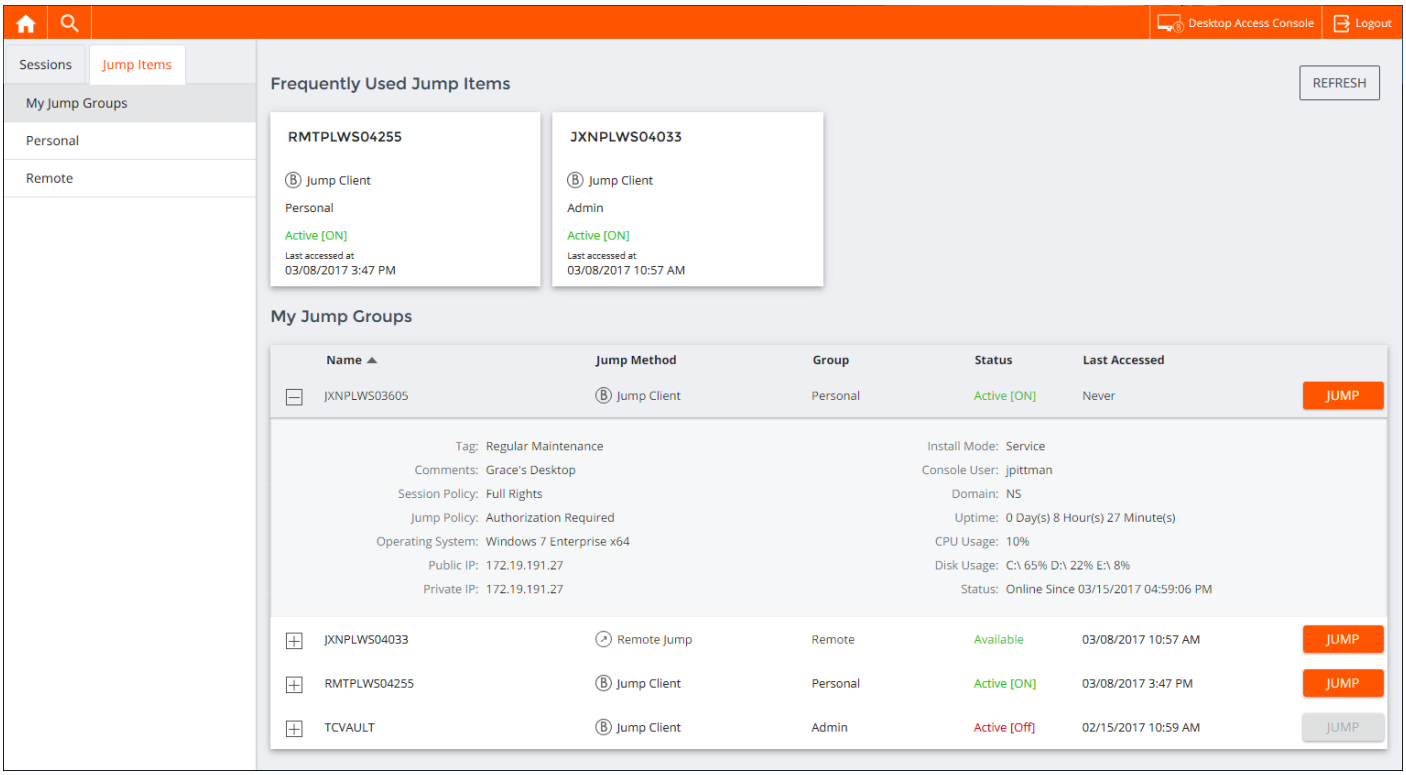
1. In the address bar of your browser, enter your Bomgar site hostname followed by **/console** (e.g., access.example.com/console).
2. Enter the username and password associated with your Bomgar user account.
3. Click **Login** to start your web-based access console session.



Launch the Web Access Console using /login



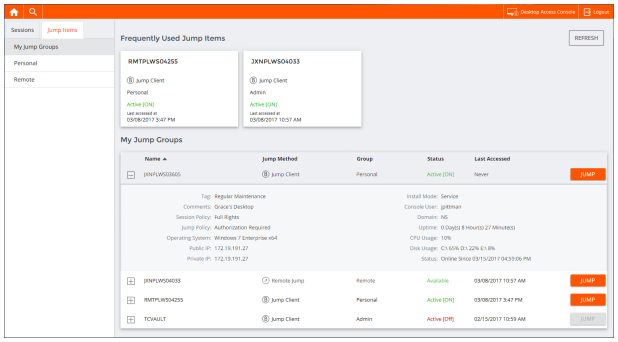
1. In the address bar of your browser, enter your Bomgar site hostname followed by **/login** (e.g., access.example.com/login).
2. Enter the username and password associated with your Bomgar user account.
3. Click **Login**.
4. Once you have logged into the /login administrative interface, click on the **My Account** tab.
5. Click on the **Launch Privileged Web Access Console** button located in the **Bomgar Access Console** section.
6. The privileged web access console opens in a new tab, and you can begin accessing endpoints.



To log out of the access console, click the **Logout** icon in the upper right corner of the screen.

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

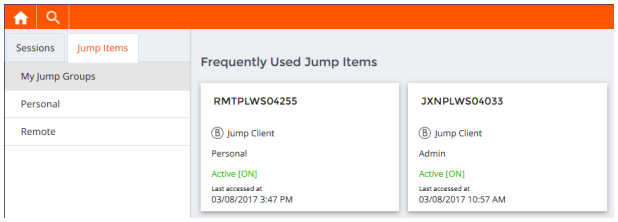
To access an endpoint, install a Jump Item on that system from the **Jump Clients** page of the /login administrative interface.



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.

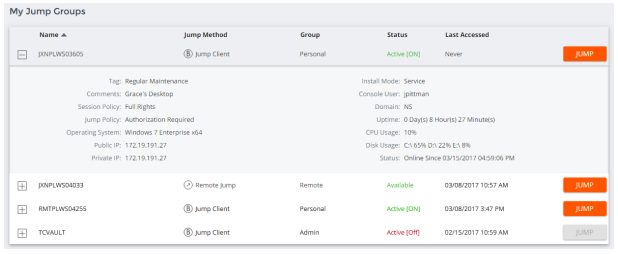
There are three ways that you can begin accessing endpoints:



- Locate and select an endpoint from the **My Jump Groups** list.
- Choose a Jump Group and 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**.*

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



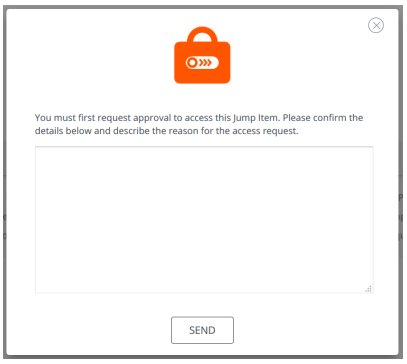
1. Select a location and click on the **Refresh All** button.
2. A list of all Jump Items populates, and you can review details about the Jump Item, including: **Name**, **Method**, **Group**, **Status**, and **Last Accessed**. To review more details about the Jump Item, click on the plus sign beside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

End-User and Third-Party Authorization

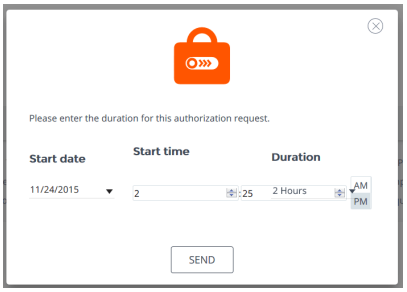
Depending on the configuration of Jump Items within the /login administrative interface, a Jump Item may have a Jump Policy associated with it, and the policy may define an authorization component that forces you to request permission from a third-party or an administrator before you are able to start an access session with the Jump Item. To learn more 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.bomgar.com/docs/privileged-access/getting-started/admin/jump-policies.htm.

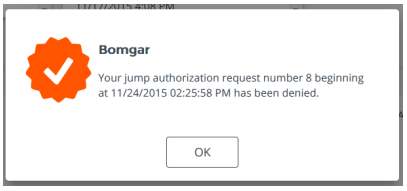
1. After you have clicked the **JUMP** button and requested access, a prompt appears, and you are required to enter a reason for wanting to access the system.



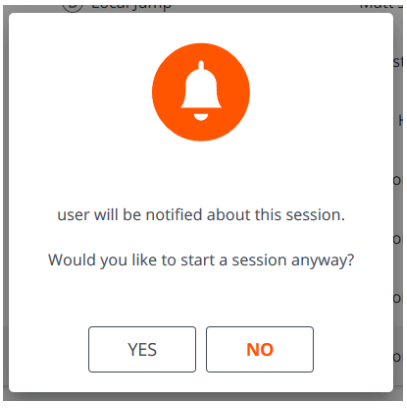
2. Next, you must indicate when and for how long you will be accessing the system.
3. Once the request has been submitted, the third party or person responsible for approving access requests is alerted through an email notification and has the opportunity to accept or deny the request. Although other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

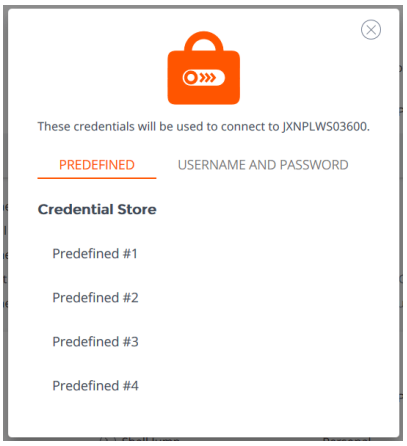


4. After permission has been determined, an authorization notification appears within the Jump Item's information displaying either "approved" or "denied." If access is granted, you can tap the Jump button to begin accessing the system.



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.





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.bomgar.com/docs/privileged-access/getting-started/admin/security.htm.

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 Bomgar Privileged 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 Bomgar Endpoint Credential Manager (ECM). The Bomgar 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 Bomgar ECM Service and to use credential injection in Bomgar Privileged Access.*

System Requirements

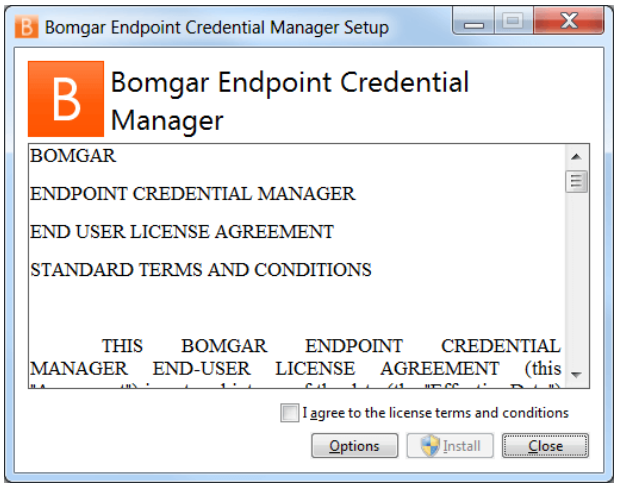
- **Windows Vista or newer, 64-bit only**
- **.NET 4.5 or newer**

1. To begin, download the Bomgar Endpoint Credential Manager (ECM) from Bomgar Support at ssc.bomgar.com. Start the Bomgar Endpoint Credential Manager Setup Wizard.
2. Agree to the EULA terms and conditions. Mark the checkbox if you agree, and click **Install**.

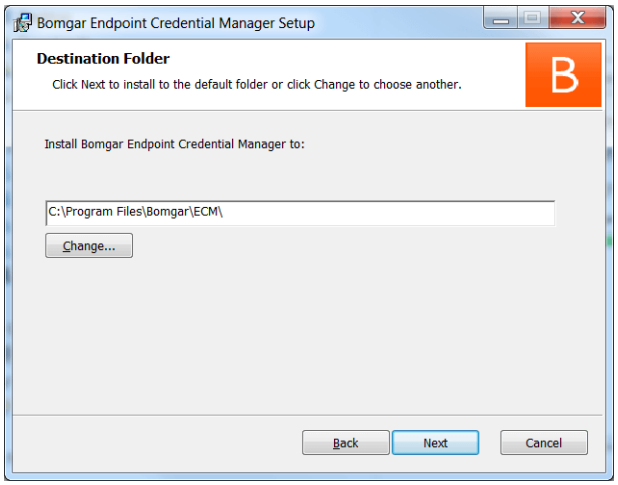
   > ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*

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

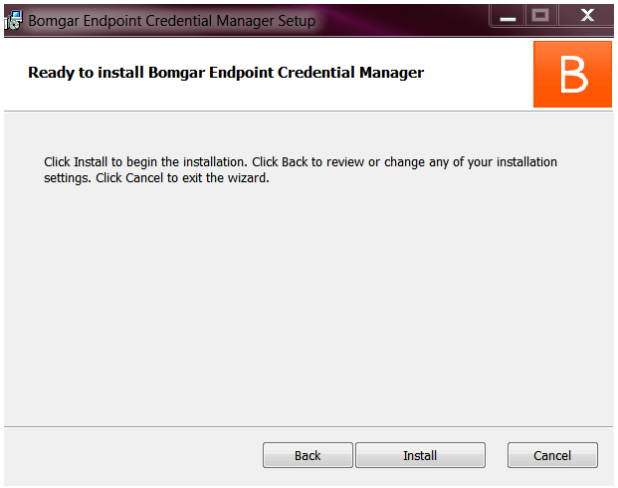
3. Click **Install**.



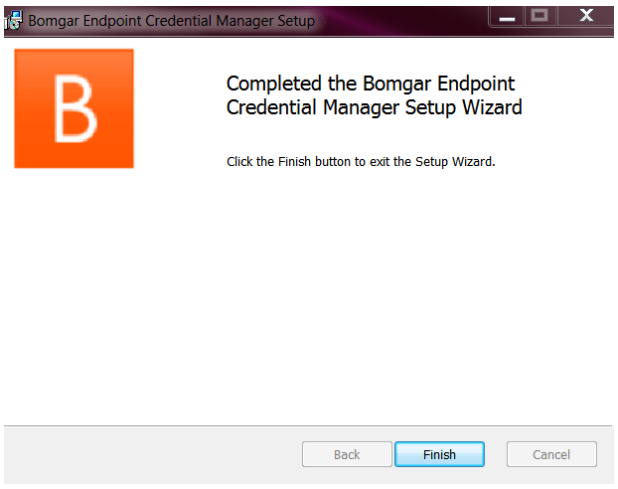
4. Choose a location for the credential manager and click **Next**.
5. On the next screen, you can begin the installation or review any previous step.



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



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



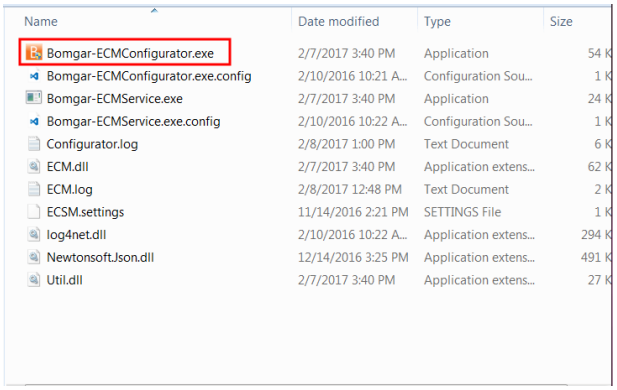
Note: *To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the Bomgar Appliance. A list of the ECMs connected to the appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

Note: *When multiple ECMs are connected to a Bomgar site, the Bomgar Appliance routes requests to the ECM that has been connected to the appliance the longest.*

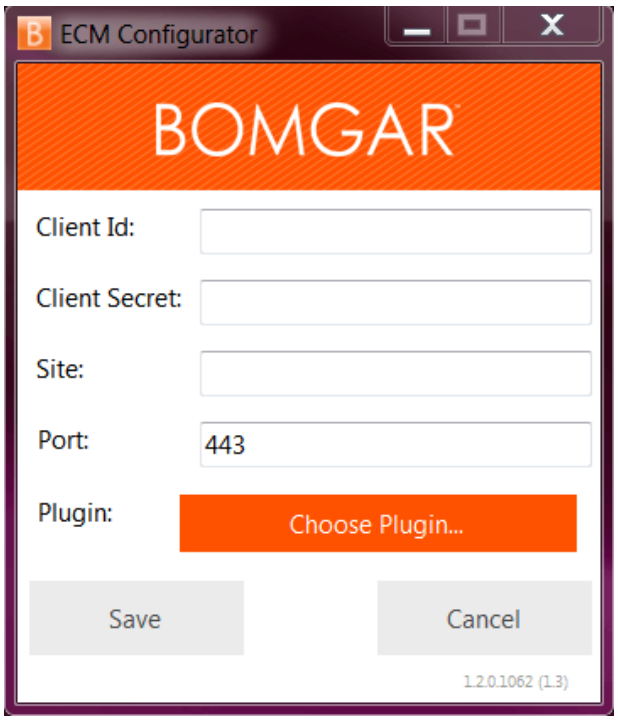
Configure a Connection to Your Credential Store

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

1. Locate the Bomgar 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.



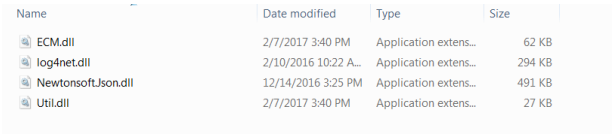
3. When the ECM Configurator opens, complete the fields. All fields are required.



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

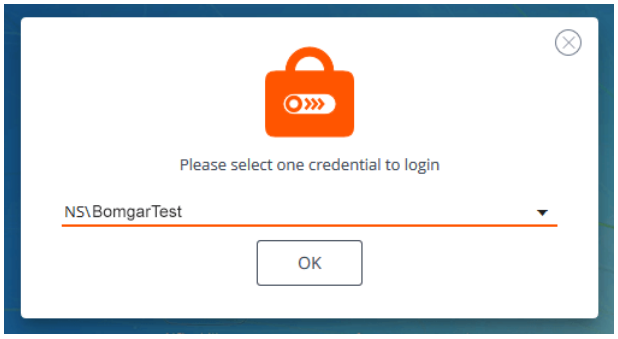
To apply new settings in the configuration, restart the ECM service.

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.



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 PA Client Scripting API (https://www.bomgar.com/docs/privileged-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 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 other session at any time. To return to an endpoint you are already accessing in another session, follow the steps outlined below:

1. Click on the **Sessions** drop down menu.

> ***Note:*** *The number listed in the* ***Sessions*** *drop down menu indicates how many active sessions you are accessing simultaneously.*

2. Select an endpoint from the list.

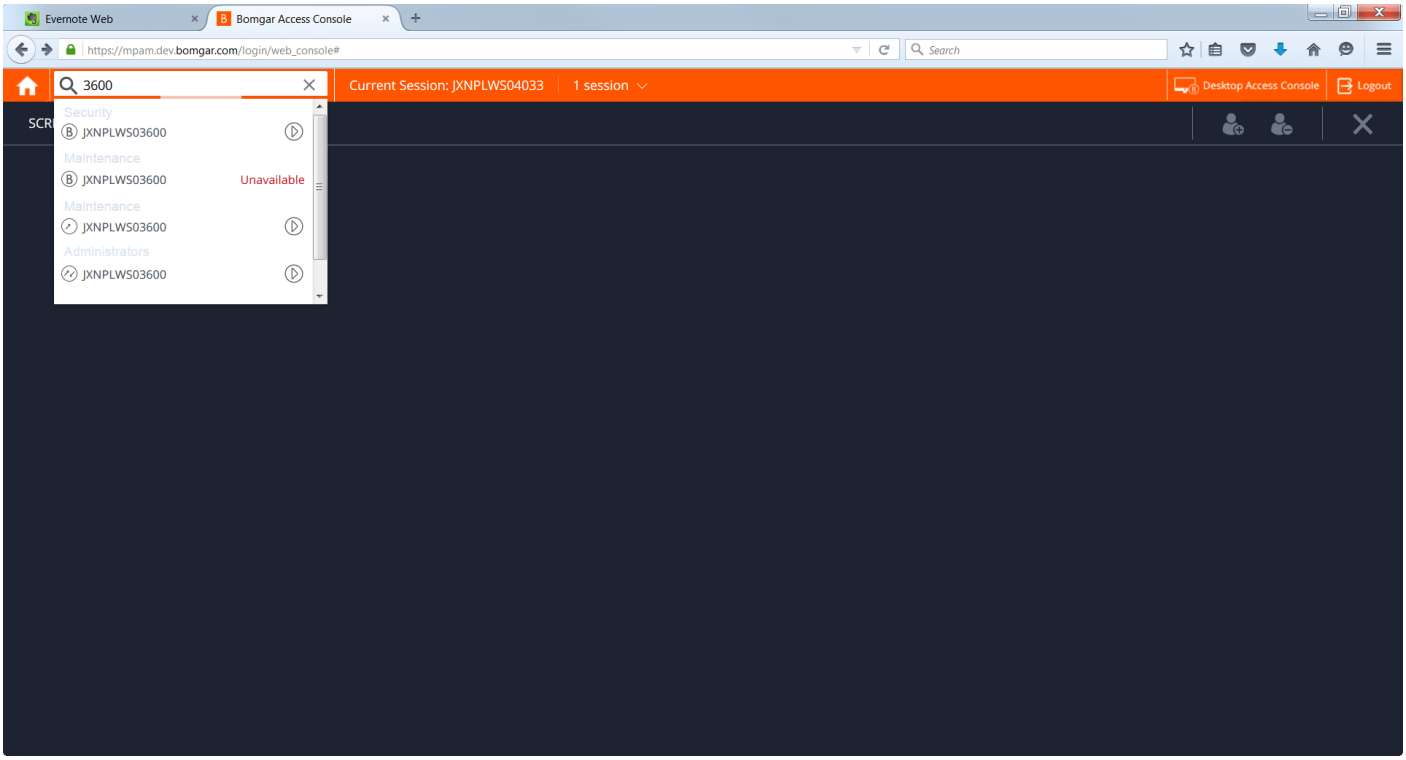
3. Then you will be taken to that specific endpoint's session.

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.

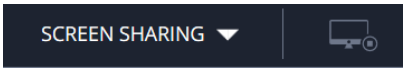
2. In the search bar, type in the name of the endpoint.
3. From the results provided, select the endpoint you wish to start a session with and click on the **Start** button to begin a session.



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.

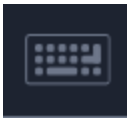
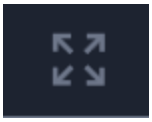
1. From the session window, click on the **Screen Sharing** drop down menu and choose the **Screen Sharing** option. Or, you can click on the **Start Screen Sharing** icon to begin accessing the endpoint if screen sharing does not start automatically.



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.
	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 Bomgar user has disabled the end user's view. 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 Bomgar. Once a services agreement is in place, you may download the required middleware from the Bomgar self-service center.

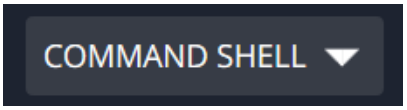
	Toggle the virtual keyboard.
	Toggle the clipboard.
	Select an alternate remote monitor to display. The primary monitor is designated by a **P**.
	View the remote screen at actual or scaled size.
	Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, 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.

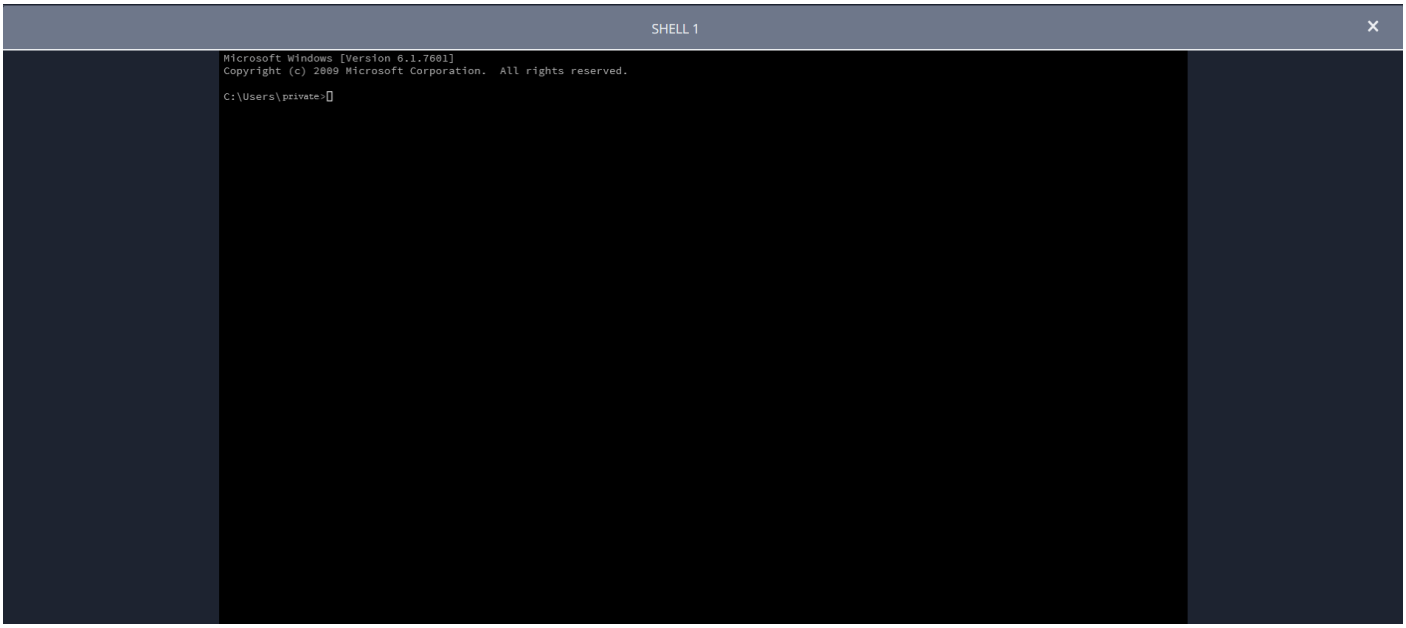
Open the Command Shell on the Remote Endpoint Using the Privileged Web Console

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.

1. To access the **Command Shell** while in an access session, click on the **Screen Sharing** drop down menu in the top corner of the screen.
2. Select the **Command Shell** option.
3. After the **Command Shell** option is chosen, the command options and prompt will appear.





Command Shell Tools

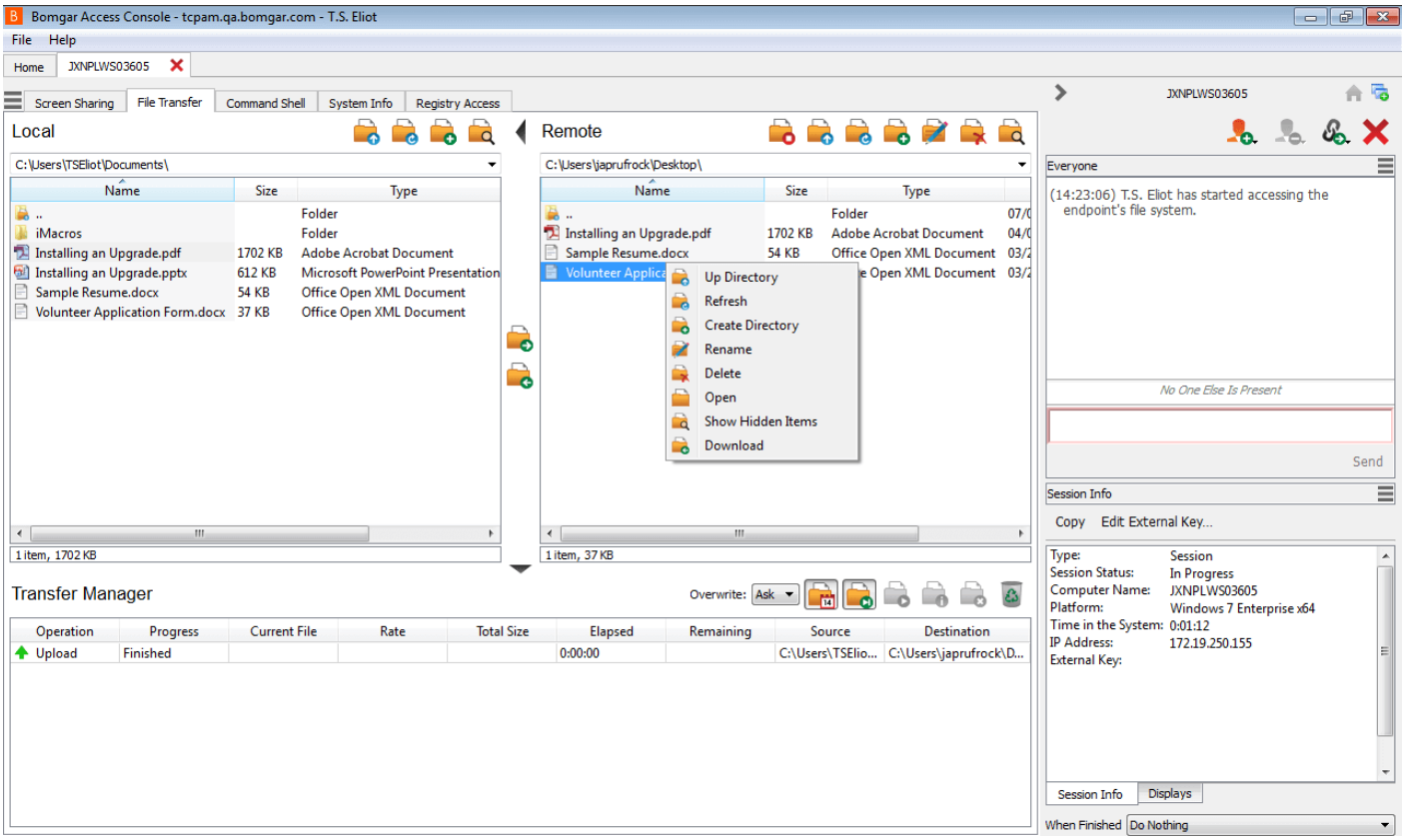
	Stop command prompt access when it is no longer needed.
	Open a new shell to run multiple instances of command prompt, or close individual shells without relinquishing command prompt access. Shells are tabulated at the bottom of the screen.

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.



File Transfer Tools

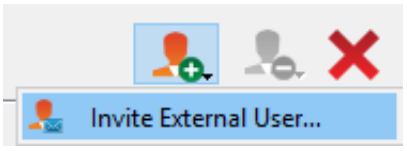
	Stop access to the remote device's file system when it is no longer needed.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Create a new directory.
	Rename a directory or file.
	Delete a directory or file. Note that deleting a file or folder permanently 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.

Share a Session with Other Users using the Privileged Web Access Console

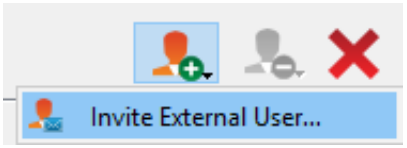
Within a session, you can request for a team member to participate in an access session. To share a session, follow the steps outlined below.

1. Click on the **Share Session** icon.

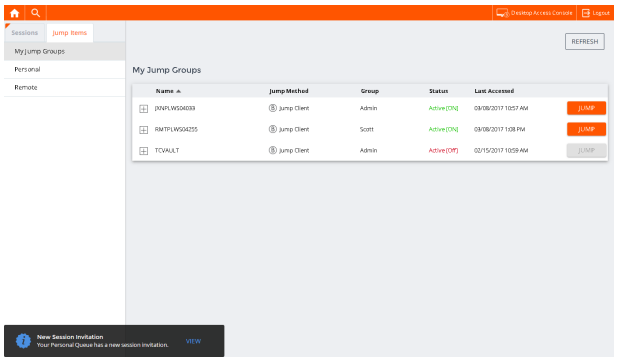
2. Select the team that the user is a member of from the menu.



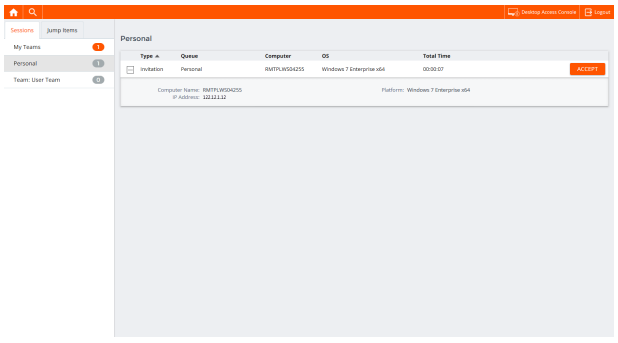
3. From the team listing, choose the user with whom you would like to share the session.



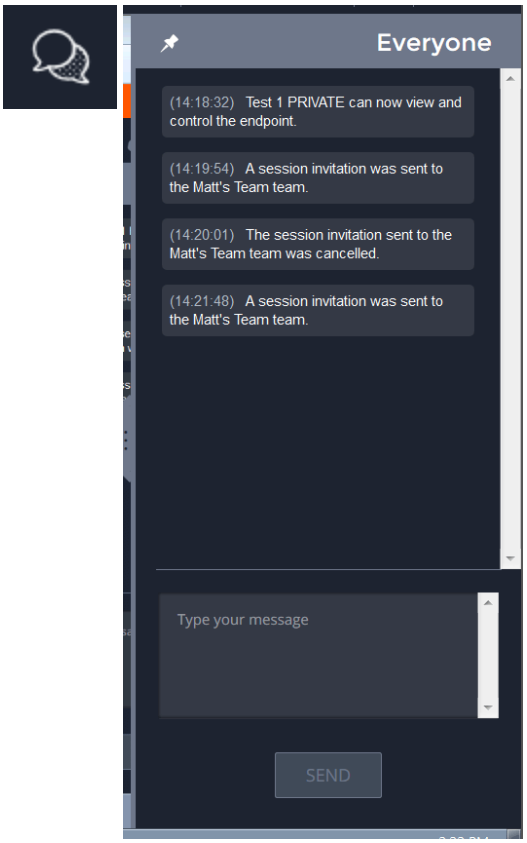
4. The user being invited will see a notification appear in the lower left corner of the screen indicating they have a new session invitation.



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.

Remove a Member from a Privileged Web Access Console Session

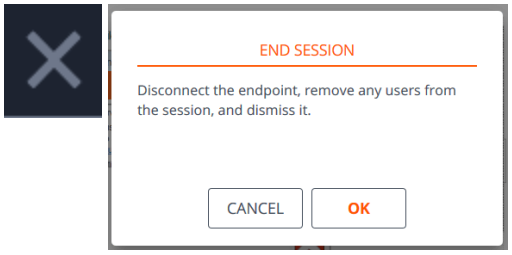
When needed, you can remove another user from a shared access session. To remove a user, click on the **Remove Member** icon.

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

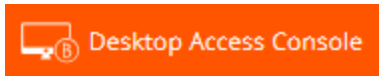
1. To exit an access session, click on the **X** icon in the top right corner of the screen. If you are the session owner, please note that the **End Session** action will close the session page in your access console and will remove any additional members who may be sharing the session.
2. Next, you 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, click on the **Run Native Access Console** button located 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.*