

BOMGAR™

**Privileged Access
Privileged Web**

Table of Contents

Privileged Web Access Console Guide	3
Privileged Web Access Console Requirements	4
Launch the Privileged Web Access Console through /login	5
Use Jump Items to Access Endpoints in the Privileged Web Access Console	7
Log Into Endpoints Using Credential Injection	10
System Requirements	10
Authenticating from the Client Scripting API	14
Return to an Active Session in the Privileged Web Access Console	15
Control the Remote Endpoint with Screen Sharing	16
Access the Command Shell on the Remote Endpoint	18
Share a Session with Other Users using the Privileged Web Access Console	19
Invite An External User to Join a Session	21
Remove a Member from a Privileged Web Access Console Session	22
Close the Privileged Web Access Console Session	23
Download the Native Desktop from the Privileged Web Access Console	24

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

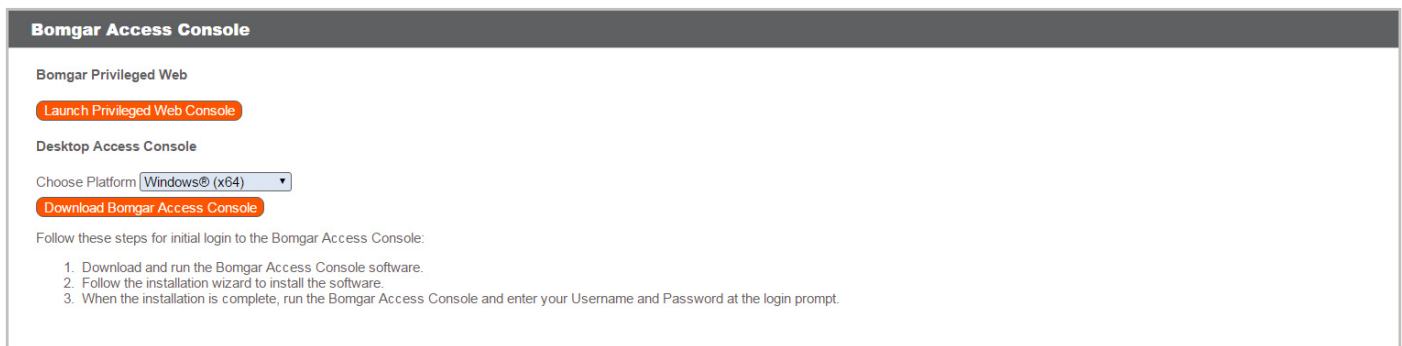
Browsers

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

Launch the Privileged Web Access Console through /login

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 utilizing the privileged web access console to access endpoints, follow the steps outlined below:

Note: By default, the **Launch 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.



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.

B
Access Console

- All Jump Items
- Personal
- Team: Administrators
- Team: Maintenance
- Team: Security

Frequently Used Jump Items

REFRESH ALL

All Jump Items

Name ▲	Method	Group	Status	Last accessed	
<input type="checkbox"/> IE11WIN7	<input type="radio"/> Jump Client	Security	Passive [Unknown]	Never	<input type="radio"/>
<input type="checkbox"/> judges	<input type="radio"/> Shell Jump	Administrators	Available	11/20/2015 3:57 PM	<input type="radio"/>
<input type="checkbox"/> JXNPLWS03600	<input type="radio"/> Jump Client	Maintenance	Active [Online]	11/20/2015 3:51 PM	<input type="radio"/>
<input type="checkbox"/> JXNPLWS03600	<input type="radio"/> Local Jump	Security	Unavailable	Never	<input type="radio"/>
<input type="checkbox"/> JXNPLWS03600	<input type="radio"/> Remote Jump	Maintenance	Available	11/17/2015 4:08 PM	<input type="radio"/>
<input type="checkbox"/> JXNPLWS03600	<input type="radio"/> RDP	Administrators	Available	11/10/2015 8:59 AM	<input type="radio"/>

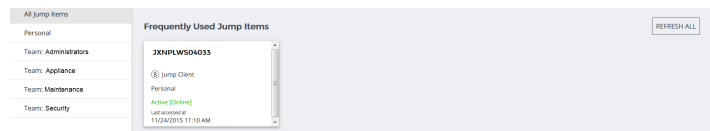
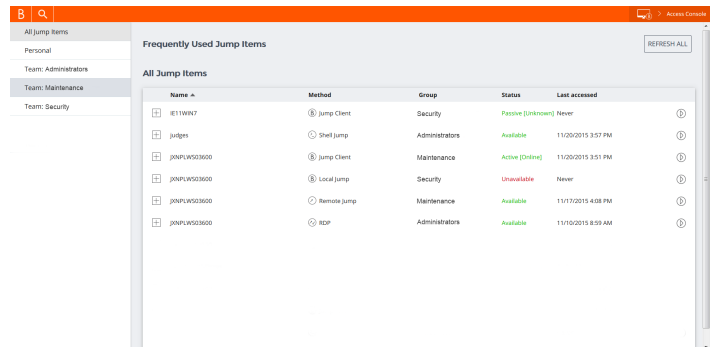
Use Jump Items to Access Endpoints in the Privileged Web Access Console

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

Note: Your account permissions may disallow you from using Jump Items, or you may be allowed to initiate Jump Items within your personal queue or one of your team queues only.

Jump Items are grouped according to who can access them - only the user who created them or a particular team. There are three ways that you can begin accessing endpoints:

- Locate and select an endpoint from the **All Jump Items** list.
- Choose a team queue and select an endpoint from that team's listing of endpoints.
- Select a session from the **Frequently Used Jump Items** list.

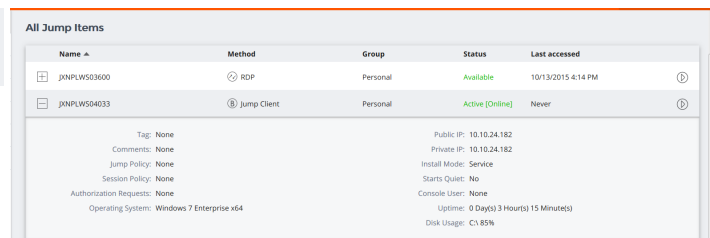


Note: The **Frequently Used Jump Items** list displays all of the Jump Items that you access on a regular basis. To start a session with a frequented item, hover your mouse over the session and click **Start Session**.

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 will populate, 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 on the **Start** button to start a session with the endpoint.

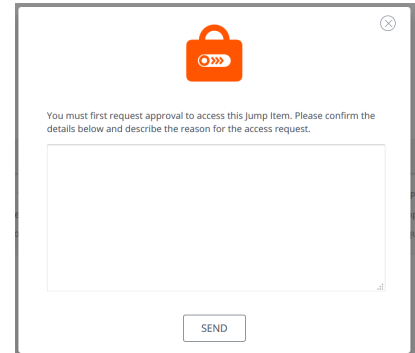
REFRESH ALL



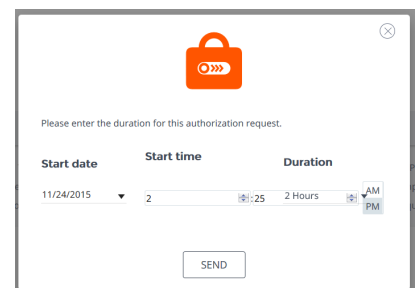
End-User and Third-Party Authorization

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 will be 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](#).

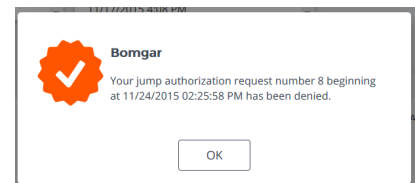
1. After the **Start** button has been clicked and access requested, a prompt will appear, and you will be required to enter a reason for wanting to access the system.
2. Next, you will need to indicate when and for how long you will be accessing the system.
3. Once the request has been submitted, the third party or person responsible for approving access requests will be alerted through an email notification and will have the opportunity to accept or deny the request.
4. After permission has been determined, an authorization notification appears displaying either "approved" or "denied." If access is granted, you can click **OK** 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 will appear, and you can begin accessing the system.



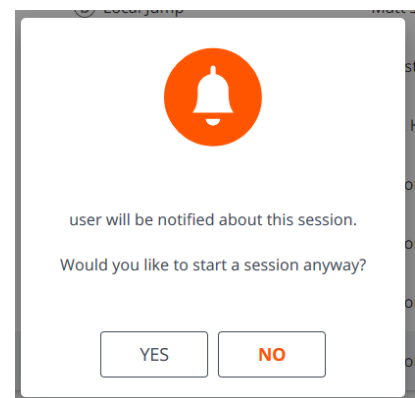
This screenshot shows a dialog box with a red padlock icon and a right-pointing arrow. The text reads: "You must first request approval to access this jump item. Please confirm the details below and describe the reason for the access request." Below the text is a large empty text area for input. At the bottom right is a "SEND" button.



This screenshot shows a dialog box with a red padlock icon and a right-pointing arrow. The text reads: "Please enter the duration for this authorization request." Below the text are three input fields: "Start date" (with a dropdown menu showing "11/24/2015"), "Start time" (with a dropdown menu showing "2" and a time selector showing ":25"), and "Duration" (with a dropdown menu showing "2 Hours" and a time selector showing "AM/PM"). At the bottom right is a "SEND" button.



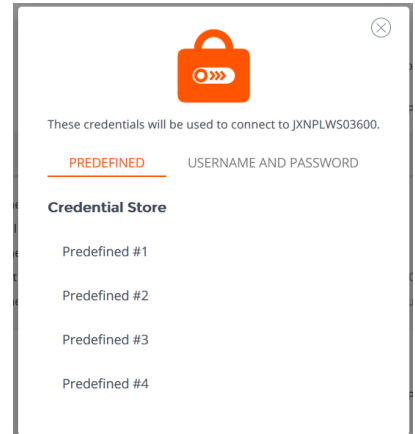
This screenshot shows a notification dialog box with a red checkmark icon. The text reads: "Bomgar Your jump authorization request number 8 beginning at 11/24/2015 02:25:58 PM has been denied." At the bottom right is an "OK" button.



This screenshot shows a dialog box with a red bell icon. The text reads: "user will be notified about this session. Would you like to start a session anyway?" At the bottom are two buttons: "YES" and "NO".

Automatic Log On Credentials

Credentials from the **Endpoint Credential Manager** can be used for RDP login and for performing Remote Push. If a user selects to Jump to a Remote Jump or Remote RDP Jump Item 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 will have 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](http://www.bomgar.com/docs/privileged-access/getting-started/admin/security.htm) 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.

Note: Don't have a password vault? Learn more about **Bomgar Vault** at <https://www.bomgar.com/vault>.

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

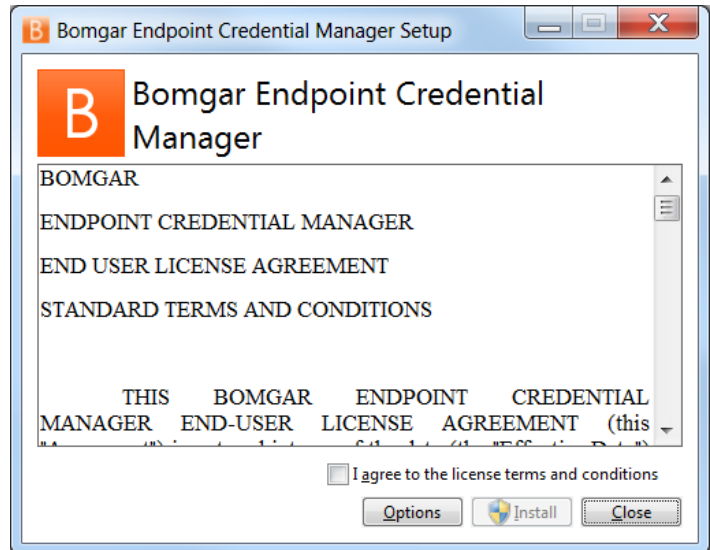
Note: When installing the Endpoint Credential Manager for use with Bomgar Vault, we recommend installing it on a machine with a static IP address to avoid potential issues with Vault's IP whitelisting for the API.

1. To begin, download the **Bomgar Endpoint Credential Manager** from [Bomgar Support](#) at <https://help.bomgar.com/>. Start the **Bomgar Endpoint Credential Manager Setup Wizard**.

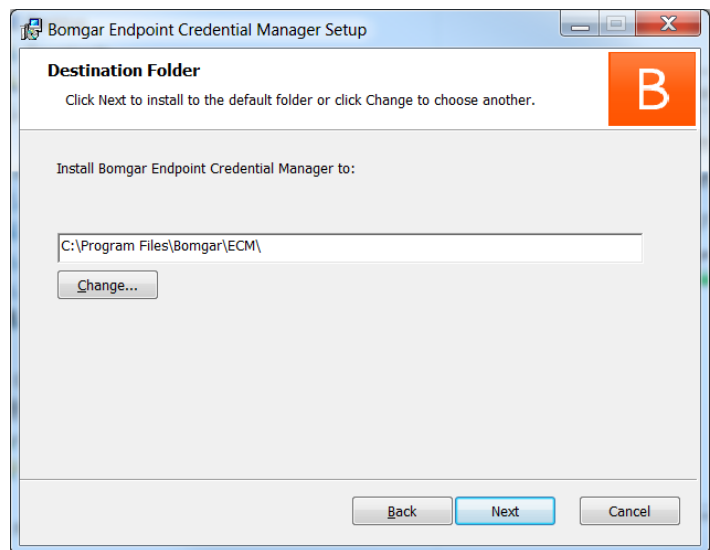
2. Agree to the EULA terms and conditions. Mark the checkbox if you agree, and click **Install**.

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

3. Click **Next**.



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



Configure a Connection to Your Credential Store

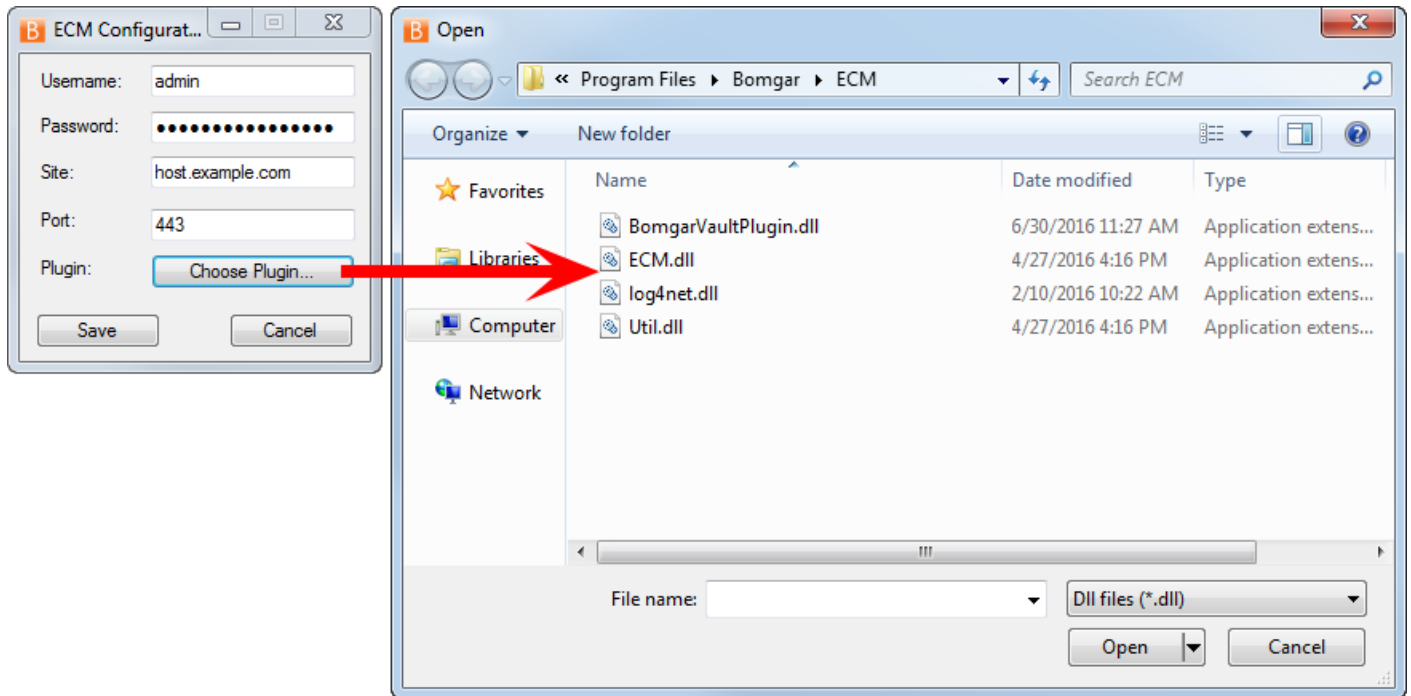
Using the ECM Configurator, set up a connection to your credential store.

1. Locate the 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
Username	The Admin username for your credential store.
Password	The Admin password 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.

- When you click the **Choose Plugin...** button, the ECM location folder opens.
- Paste your plugin files into the folder.
- 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.

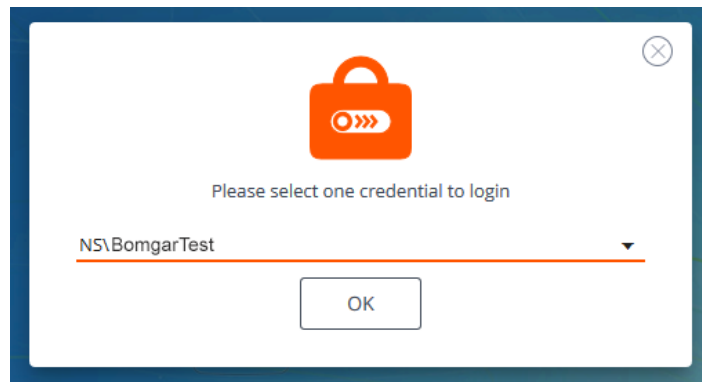
IMPORTANT

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 \(https://www.bomgar.com/docs/privileged-access/how-to/integrations/api/client-script/index.htm#client-scripting-api\)](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 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.

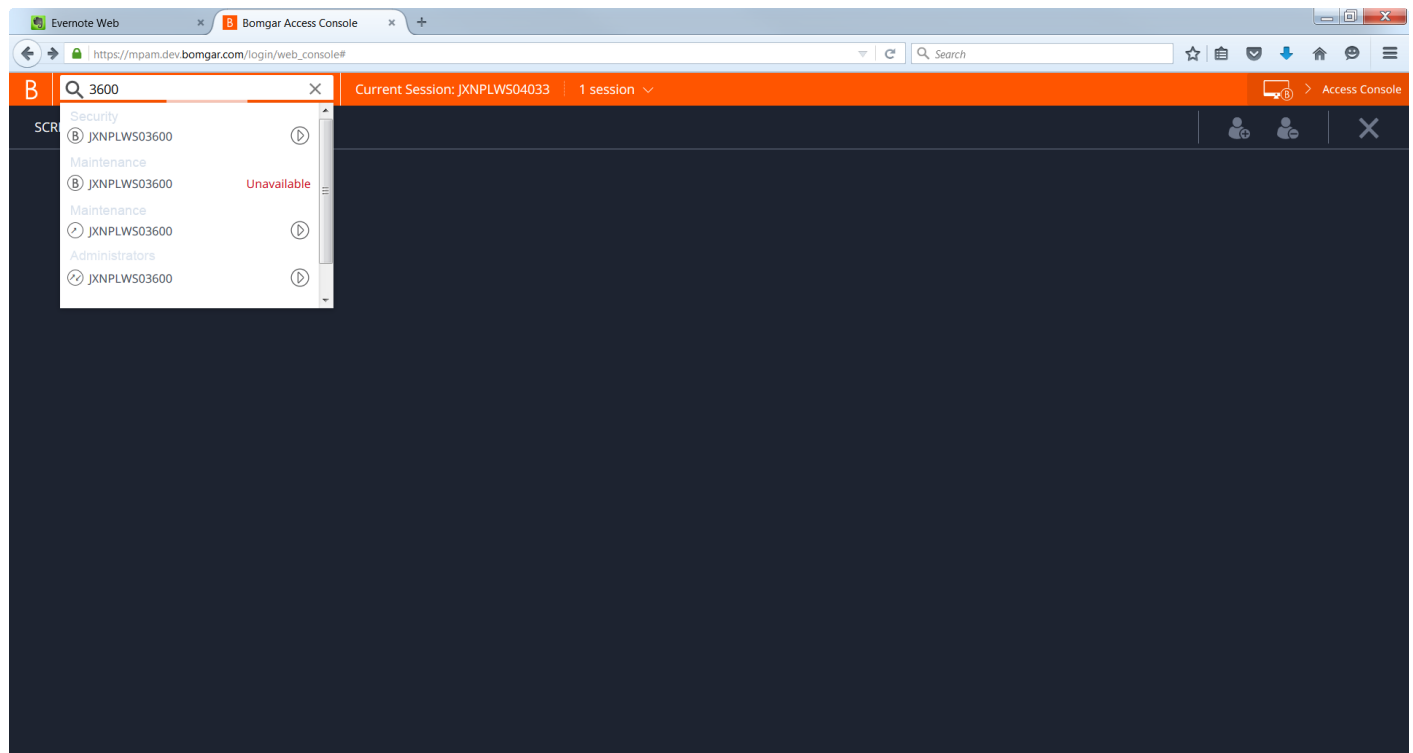
2. Select an endpoint from the list.
3. Then you will be taken to that specific endpoint's session.



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.

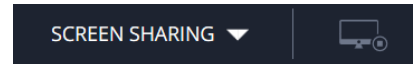
1. Click on the **Search** icon located in the top left of the screen.
2. In the search bar, type in the name of the endpoint.
3. From the results provided, select the endpoint you wish to start a session with and click on the **Start** button to begin a session.










Control the Remote Endpoint with Screen Sharing

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.
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.
	<p>If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The end user's view of the privacy screen clearly explains that the Bomgar user has disabled the end user's view. The end user can regain control at any time by pressing Ctrl+Alt+Del.</p> <p>This feature is available only for Windows. In Vista and above, the endpoint client must be elevated. On Windows 8 and above, this feature is limited to disabling the mouse and keyboard.</p>
	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.



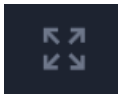
Select an alternate remote monitor to display. The primary monitor is designated by a **P**.



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).



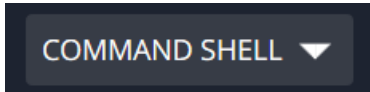
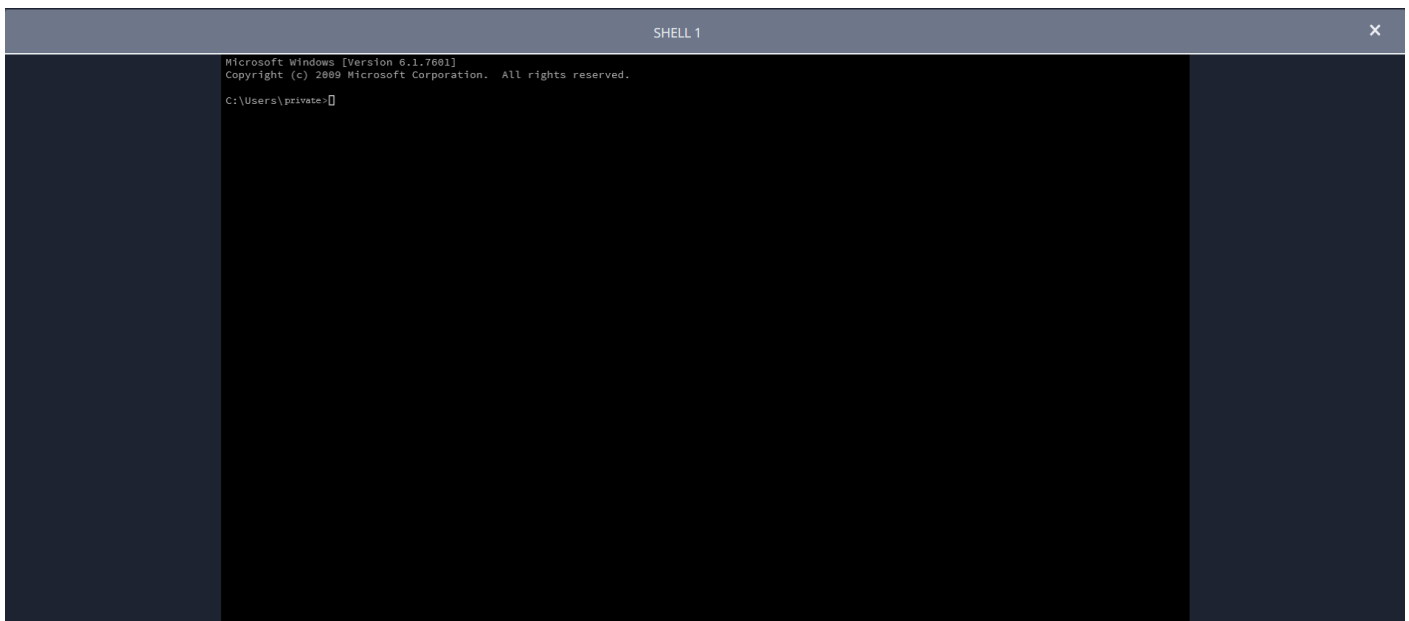
View the remote desktop in full screen mode or return to the interface view. When in full screen mode, special keys are passed through to the remote system. This includes but is not limited to modifier keys, function keys, and the Windows Start key. Note that this does not apply to the **Ctrl-Alt-Del** command.

Access the Command Shell on the Remote Endpoint

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 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.

A dark grey rectangular button with the text 'COMMAND SHELL' in white uppercase letters and a small white downward-pointing triangle on the right side.

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.

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.



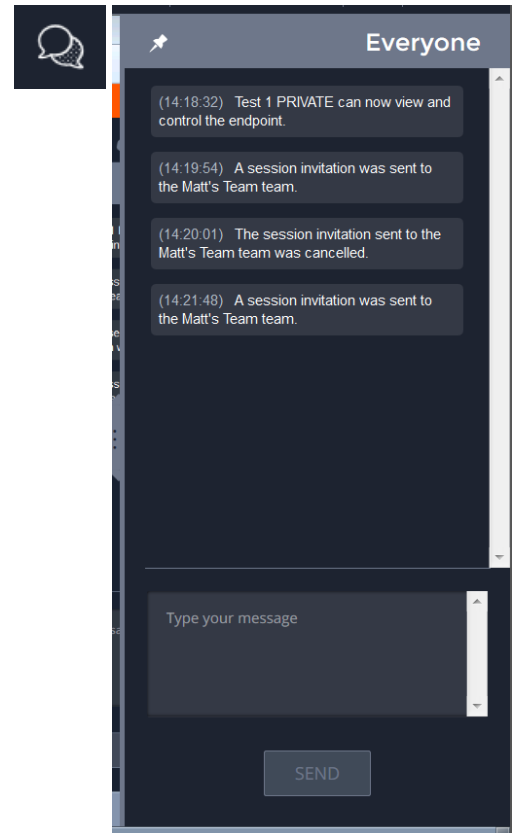
- Once the user has entered the session, you can chat with them by clicking on the **Chat** icon at the top of the screen.

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 An External User to Join a Session

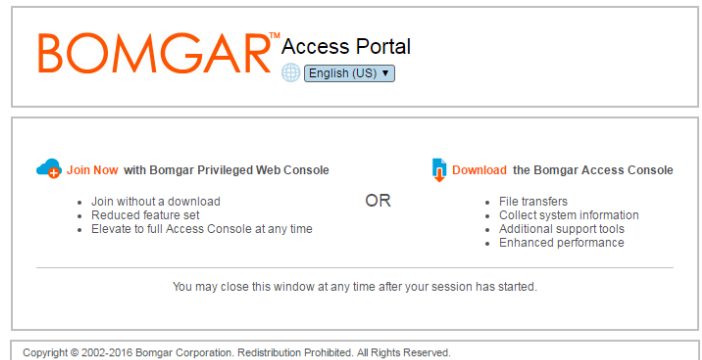
Within a session, you can request an external user to participate in a session one time only. To invite an external user to a session, follow the steps outlined below.

1. While in a session, click on the **Share Session** button.
2. From the menu, select **Invite External Representative**.
3. Select a security policy. These policies are created in the /login administrative interface and determine the level of permission the external user will have. When you select a policy, the full description displays below.
4. Enter the invited user's name. This name appears in the chat window and in reports.
5. Next, enter comments about why this user has been invited.
6. Click **Send**, and a new dialogue containing the invitation URL appears.
7. Depending on the options selected by your administrator, you may be able to send the invitation from your local email or from a server side email. You can also copy and paste the direct URL and send it to the user.
8. When the external user clicks the access invite URL, they are given the option to join the session using the privileged web access console or to download and install the desktop access console.
9. Once they have selected privileged web access console or installed the desktop access console, they can join the session.



Note: Here are some tips for using the external user invite feature:

- The external user has access to only the session tab and has a limited set of privileges.
- The external user can never be the session owner.
- When the inviting user leaves the session, the external user is logged out.
- You can invite more than one external user.
- The external user can elevate to the desktop access console. When the **Elevate** button is clicked, a new browser tab opens that redirects the user to the Access Invite URL for the desktop access console.



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.

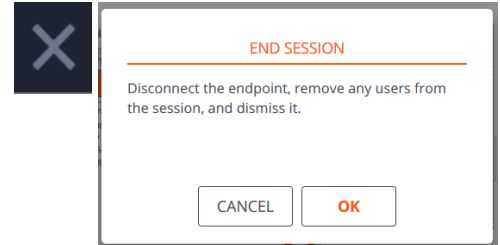


From the menu, choose the participant you wish to remove. Click **Remove Member**.

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.

