BeyondTrust

Privileged Remote Access
Jump Client Guide

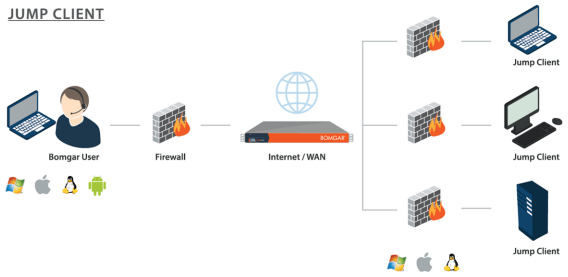
TC:3/22/2024

Table of Contents

Privileged Remote Access Jump Client Guide: Unattended Access to Systems in Any Network

With BeyondTrust Jump Technology, a user can access and control remote, unattended computers in any network. Jump Technology is integral to the BeyondTrust software offerings.

A Jump Client is an installable application that enables a user to access a remote computer, regardless of its location. The remote computer does not need to reside on a known network. Jump Clients are persistently connected to the B Series Appliance, thus helping you reach systems on remote networks anywhere in the world. By pre-installing Jump Clients on remote systems, a user can establish sessions with unattended Windows, Mac, and Linux computers.



Although BeyondTrust Jump Clients are not limited by system, they are limited by hardware, as described below:

B Series Appliance Comparison

B200	B300	B400	PRA Virtual Appliance	Cloud
Up to 1,000 Active Jump Clients	Up to 10,000 Active Jump Clients	Up to 25,000 Active Jump Clients	Depends on deployment method and allocated resources. See the PRA Virtual Appliance Installation Guide.	Up to 20 Active Jump Clients per license

If more Jump Clients are needed, contact BeyondTrust Technical Support.

Recommended Steps to Implement Jump Technology

When working with Jump Technology, there are a lot of moving parts. Here is a recommended order of implementation to make full use of your software.

1. **Add Jump Item Roles.** Jump Item Roles determine how users are allowed to interact with Jump Items. These roles are applied to users by means of individual account settings, group policies, or when added to Jump Groups.

> *For more information about Jump Item Roles, please see Use Jump Item Roles to Configure Permission Sets for Jump Clients.*

2. **Add Jump Policies.** Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules, sending email notifications when a Jump Item is accessed, or requiring approval or user entry of a ticket system ID before a Jump Item may be accessed. Jump Policies are applied to Jump Items upon creation and can be modified from the access console. Additionally, Jump Policies can be applied to users when associating a user or group policy with a Jump Group.

> *For more information about Jump Policies, please see Create Jump Policies to Control Access to Jump Clients.*

3. **Add Jump Groups.** A Jump Group is a way to organize Jump Items, granting members varying levels of access to those items. Users are assigned to Jump Groups either individually or by means of group policy.

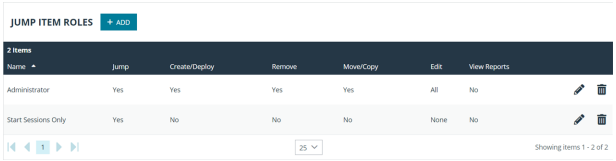
> *For more information about Jump Groups, please see Use Jump Groups to Configure Which Users Can Access Which Jump Clients.*

4. **Deploy Jump Clients.** Jump Clients can be deployed to Windows, Mac, and Linux systems and do not require those systems to be on a network. Jump Clients are deployed from **/login > Jump > Jump Clients**. When creating the installer in the mass deployment wizard, be sure to set the Jump Group and Jump Policy to determine who can access the Jump Client and with what restrictions.

> *For more information about Jump Clients, please see Deploy Jump Clients from the Administrative Interface.*

Use Jump Item Roles to Configure Permission Sets for Jump Clients

A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. Jump Item Roles are applied to users either from the **Jump > Jump Groups** page or from the **Users & Security > Group Policies** page.



If more than one role is assigned to a user, then the most specific role for a user is always used. The order of specificity for Jump Item Roles, from most specific to least specific, is:

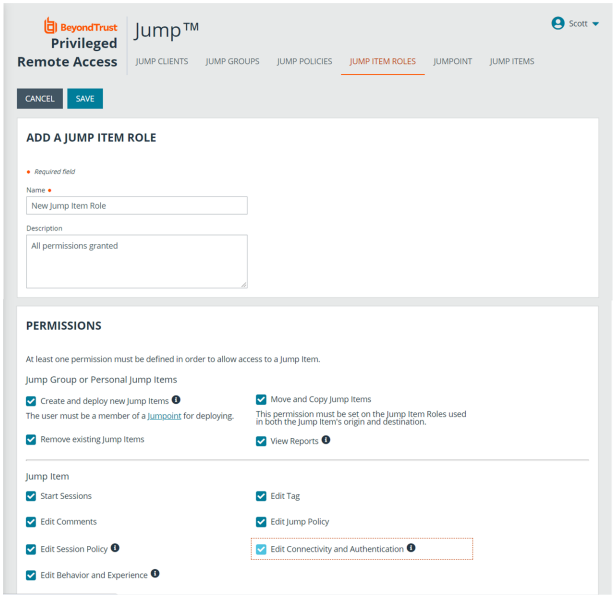
- The role assigned to the relationship between a user and a Jump Group on the **Jump > Jump Groups** page.
- The role assigned to the relationship between a user and a Jump Group on the **Users & Security > Group Policies** page.
- The **Jump Item Roles** configured for a user on the **Users & Security > Users** page or the **Users & Security > Group Policies** page.

Create or edit a Jump Item Role, assigning it a name and description. Then set the permissions a user with this role should have.

Under **Jump Group or Personal Jump Items**, determine if users can create and deploy Jump Items, move Jump Items from one Jump Group to another, and/or delete Jump Items.

Check **Start Sessions** to enable users to Jump to any Jump Items they have access to.

To allow users to edit Jump Item details, check any of **Edit Tag**, **Edit Comments**, **Edit Jump Policy**, **Edit Session Policy**, **Edit Connectivity and Authentication**, and **Edit Behavior and Experience**.

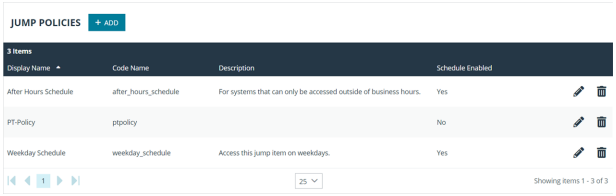


Create Jump Policies to Control Access to Jump Clients

To control access to particular Jump Items, create Jump Policies. Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules, sending email notifications when a Jump Item is accessed, or requiring approval or user entry of a ticket system ID before a Jump Item may be accessed. A Jump Policy can be applied to Jump Clients as well as to Jump shortcuts.

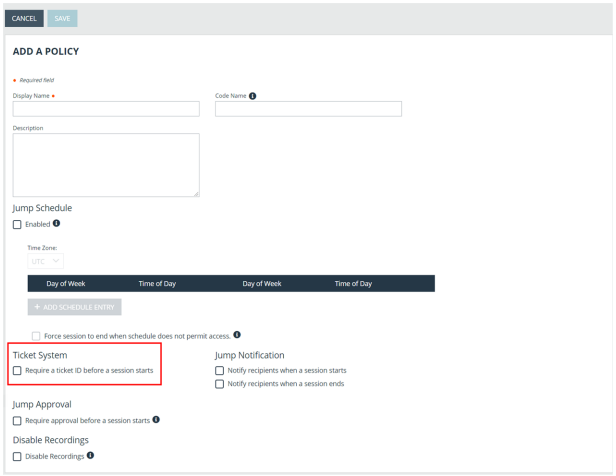
Create a Jump Policy

1. From the /login administrative interface, go to **Jump > Jump Policies**.
2. Click **Add**.



> ***Note:*** *A Jump Policy does not take effect until you have applied it to at least one Jump Item.*

3. Create a unique name to help identify this policy. This name should help users identify this policy when assigning it to Jump Items.
4. Set a code name for integration purposes. If you do not set a code name, PRA creates one automatically.
5. Add a brief description to summarize the purpose of this policy.
6. If you want to enforce an access schedule, check **Enable**. If it is disabled, then any Jump Items that use this policy can be accessed without time restrictions.



   - Set a schedule to define when Jump Items under this policy can be accessed. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.
   - If, for instance, the time is set to start at 8 am and end at 5 pm, a user can start a session using this Jump Item at any time during this window but may continue to work past the set end time. Attempting to re-access this Jump Item after 5 pm, however, results in a notification indicating that the schedule does not permit a session to start. If necessary, the user may choose to override the schedule restriction and start the session anyway.
   - If stricter access control is required, check **Force session to end**. This forces the session to disconnect at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected.

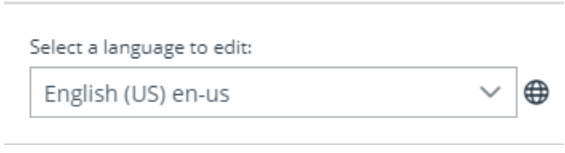
> ***Note:*** *Jump schedule and Jump approval cannot both be enabled on the same policy.*

7. You may choose to trigger an email notification whenever a session starts or ends with a Jump Item that uses this policy.
    - Check **Notify recipients when a session starts** to send an email at the beginning of a session. When a user attempts to start a session with a Jump Item that uses this policy, a prompt states that a notification email will be sent and asks if the user would like to start the session anyway.
    - Check **Notify recipients when a session ends** to send an email at the end of a session. When a user attempts to start a session with a Jump Item that uses this policy, a prompt states that a notification email will be sent at the end of the session and asks if the user would like to start the session anyway.
    - Enter one or more email addresses to which emails should be sent. Separate addresses with a space.This feature requires a valid SMTP configuration for your B Series Appliance, set up on the **/login > Management > Email Configuration** page.
    - Enter the name of the email recipient. This name appears on the prompt the user receives prior to a session with a Jump Item that uses this policy.
    - If more than one language is enabled on this site, set the language in which to send emails.
8. If you check **Require a ticket ID before a session starts**, a valid ticket ID from your external ticket ID approval process must be entered by the user whenever a session is attempted with any Jump Item that uses this Jump Policy. When a user attempts to start a session with a Jump Item that uses this policy, a configurable dialog prompts the user to enter the approved ticket ID from your external ITSM or ticket ID system.
9. If you check **Require approval before a session starts**, an approval email is sent to the designated recipients whenever a session is attempted with any Jump Item that uses this Jump Policy. When a user attempts to start a session with a Jump Item that uses this policy, a dialog prompts the user to enter a request reason and the time and duration for the request.
    - Set the maximum length of time for which a user can request access to a Jump Item that uses this policy. The user can request a shorter length of access but no longer than that set here.
    - When approval has been granted to a Jump Item, that Jump Item becomes available either to any user who can see and request access to that Jump Item or only to the user who requested access.
    - Enter one or more email addresses to which emails should be sent. Separate addresses with a space.This feature requires a valid SMTP configuration for your B Series Appliance, set up on the **/login > Management > Email Configuration** page. A PRA user name can be entered instead of an email address.
    - Enter the name of the email recipient. This name appears on the prompt the user receives prior to a session with a Jump Item that uses this policy.
    - If more than one language is enabled on this site, set the language in which to send emails.

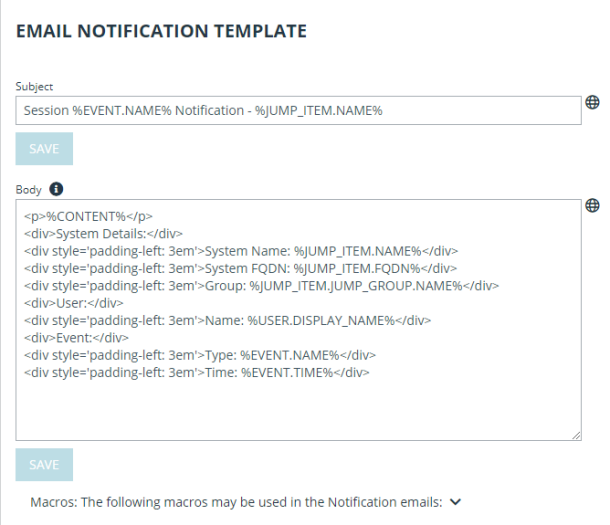
> ***Note:*** *Jump schedule and Jump approval cannot both be enabled on the same policy.*

10. If you check **Disable Session Recordings**, sessions started with this Jump Policy are not recorded, even if recordings are enabled on the **Configuration > Options** page. This affects screen sharing recordings, protocol tunnel Jump recordings, and command shell recordings.
11. When you are finished configuring this Jump Policy, click **Save**.

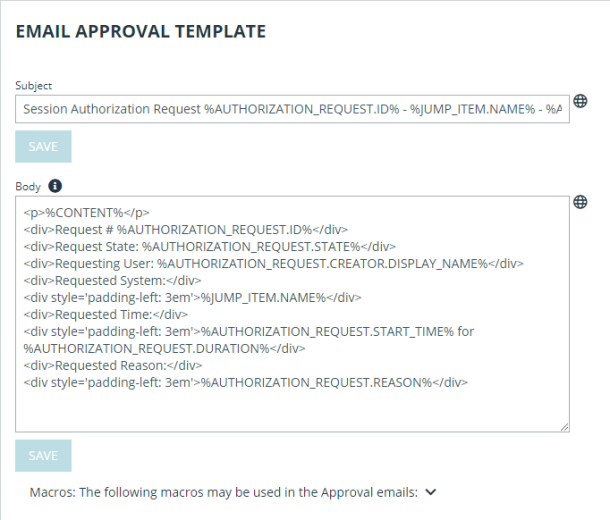
> ***Note:*** *If you have more than one language enabled on your site, you can select the language you want to use on the screens below from the dropdown menu. Fields that display the language globe icon can display content in the language you select.*



12. You can modify the notification email template. Click the link below the **Body** field to view the macros that can used to customize the text in your emails for your purposes.



13. You also can modify the approval email template. Click the link below the **Body** field to view the macros that can used to customize the text in your emails for your purposes.

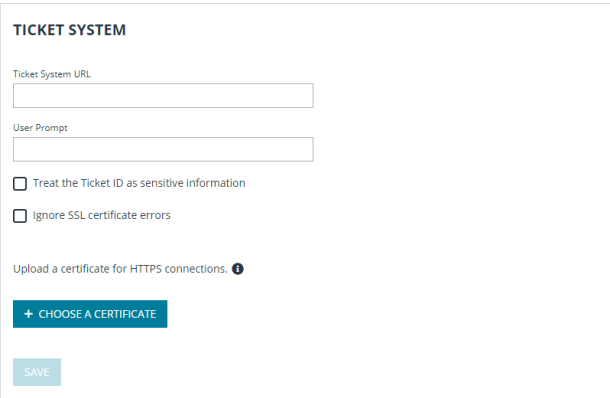


14. If you enabled the requirement of a ticket ID in the Jump Approval section, configure access to your external ticket ID system.

    In **Ticket System URL**, enter the URL for your external ticket system. If an HTTPS URL is entered, upload the certificate for the HTTPS ticket system connection to the B Series Appliance.

    In **User Prompt**, enter the dialog text you want access console users to see when they are requested to enter the ticket ID required for access.

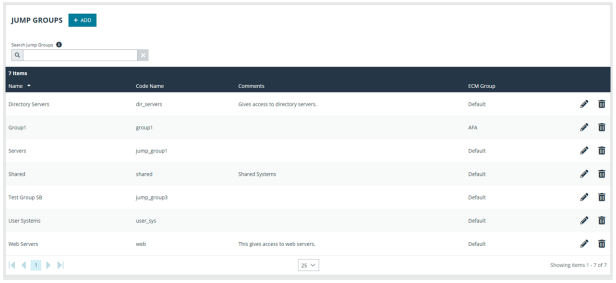
    If your company's security policies consider ticket ID information as sensitive material, check the **Treat the Ticket ID as sensitive information** box.



After the Jump Policy has been created, you can apply it to Jump Items either from the /login interface or from the access console.

Use Jump Groups to Configure Which Users Can Access Which Jump Clients

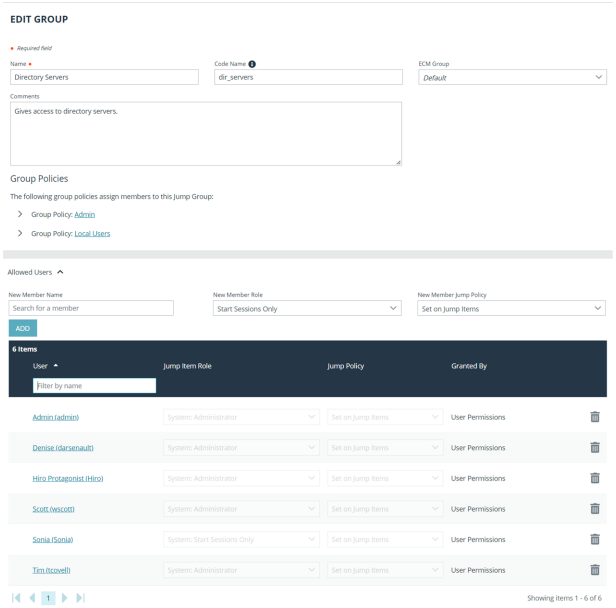
A Jump Group is a way to organize Jump Items, granting members varying levels of access to those items. Users are assigned to Jump Groups either from the **Jump > Jump Groups** page or from the **Users & Security > Group Policies** page.



To quickly find an existing group in the list of **Jump Groups**, enter the name, part of the name, or a term from the comments. The list filters all groups with a name or comment containing the entered search term. The list remains filtered until the search term is removed, even if the user goes to other pages or logs out. To remove the search term, click the **X** to the right of the search box.

You can create or edit a Jump Group, assigning it a name, code name, and comments. The **Group Policies** section lists any group policies that assign users to this Jump Group.

In the **Allowed Users** section, you can add individual users if you prefer. Search for users to add to this Jump Group. You can set each user's **Jump Item Role** to set their permissions specific to Jump Items in this Jump Group, or you can use the user's default Jump Item Roles as set on the **Users & Security > Group Policies** or **Users & Security > Users** page. A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage.



You can also apply a **Jump Policy** to each user to manage their access to the Jump Items in this Jump Group. Selecting **Set on Jump Items** instead uses the Jump Policy applied to the Jump Item itself. Jump Policies are configured on the **Jump > Jump Policies** page and determine the times during which a user can access this Jump Item. A Jump Policy can also send a notification when it is accessed or can require approval to be accessed. If neither the user nor the Jump Item has a Jump Policy applied, this Jump Item can be accessed without restriction.

Existing Jump Group users are shown in a table. You can filter the list of users by entering a username in the **Filter** box. You can also edit a user's settings or delete the user from the Jump Group.

To add groups of users to a Jump Group, go to **Users & Security > Group Policies** and assign that group to one or more Jump Groups.

> ***Note:*** *Edit and delete functionality may be disabled for some users. This occurs either when a user is added via group policy or when a user's system Jump Item Role is set to anything other than* ***No Access****.*

You can click the group policy link to modify the policy as a whole. Any changes made to the group policy apply to all members of that group policy.

You can click the user link to modify the user's system Jump Item role. Any changes to the user's system Jump Item role apply to all other Jump Groups in which the user is an unassigned member.

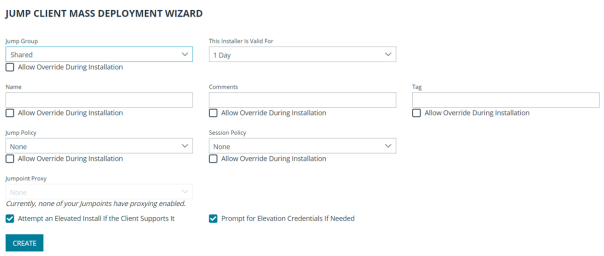
You also can add the individual to the group, overriding their settings as defined elsewhere.

Deploy Jump Clients from the Administrative Interface

Jump Clients can be preinstalled on remote computers in anticipation of the need for remote access. This method of installation may be applied to one system or multiple systems simultaneously. You can easily automate the mass deployment of your Jump Client network by allowing customization during installation. The Jump Client command line installer has switches that allow a script to modify a variety of Jump Client parameters when executed. This allows you to create custom mass deployment scripts to pull in variables from other sources and use the variables to modify the Jump Client parameters at install time.

You can easily manage active installers from the Jump Client Installer list. This list shows all previously installed active Jump Client installers. Administrators and privileged users can view, download, delete, or extend Jump Client installers. A warning message appears at the top of the list: *Installing more than one Jump Client on the same system is being phased out in a future release. In the Access Console you may use the **copy** action on a Jump Client to apply different policies to the same endpoint.* Click **Dismiss** to remove the warning message.

1. From the /login administrative interface, go to **Jump > Jump Clients**.
2. At the top of the Jump Client Installer List, click **Add**.
3. From the **Jump Group** dropdown, select whether to pin the Jump Client to your personal list of Jump Items or to a Jump Group shared by other users. Pinning to your personal list of Jump Items means that only you can access this remote computer through this Jump Client. Pinning to a shared Jump Group makes this Jump Client available to all members of that Jump Group.



4. You may apply a Jump Policy to this Jump Client. Jump Policies are configured on the **Jump > Jump Policies** page and determine the times during which a user can access this Jump Client. A Jump Policy can also send a notification when it is accessed or can require approval to be accessed. If no Jump Policy is applied, this Jump Client can be accessed without restriction.
5. You may choose a Session Policy to assign to this Jump Client. Session policies are configured on the **Users & Security > Session Policies** page. A session policy assigned to this Jump Client has the highest priority when setting session permissions.
6. If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. That way, if these Jump Clients are installed on computers without native internet connections, they can use the Jumpoint to connect back to your B Series Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.
7. Add **Comments**, which can be helpful in searching for and identifying remote computers. Note that all Jump Clients deployed via this installer have the same comments set initially, unless you check **Allow Override During Installation** and use the available parameters to modify the installer for individual installations.
8. The installer remains usable only as long as specified by the **This Installer is Valid For** dropdown. Be sure to leave adequate time for installation. If someone should attempt to run the Jump Client installer after this time, installation fails, and a new Jump Client installer must be created. Additionally, if the installer is run within the allotted time but the Jump Client is unable to connect to the B Series Appliance within that time, the Jump Client uninstalls, and a new installer must be deployed. The validity time can be set for anywhere from 10 minutes to 1 year. This time does NOT affect how long the Jump Client remains active.

   Once a Jump Client has been installed, it remains online and active until it is uninstalled from the local system either by a user from the Jump interface or by an uninstall script. It can also be uninstalled, or extended, from the Jump Client Installer List. A user cannot remove a Jump Client unless the user is given appropriate permissions by their admin from the /login interface.

9. If **Attempt an Elevated Install if the Client Supports It** is selected, the installer attempts to run with administrative rights, installing the Jump Client as a system service. If the elevated installation attempt is unsuccessful or if this option is deselected, the installer runs with user rights, installing the Jump Client as an application. This option applies only to Windows and Mac operating systems.

Note: *A Jump Client pinned in user mode is available only when that user is logged in. In contrast, a Jump Client pinned in service mode, with elevated rights, allows that system to always be available, regardless of which user is logged in.*

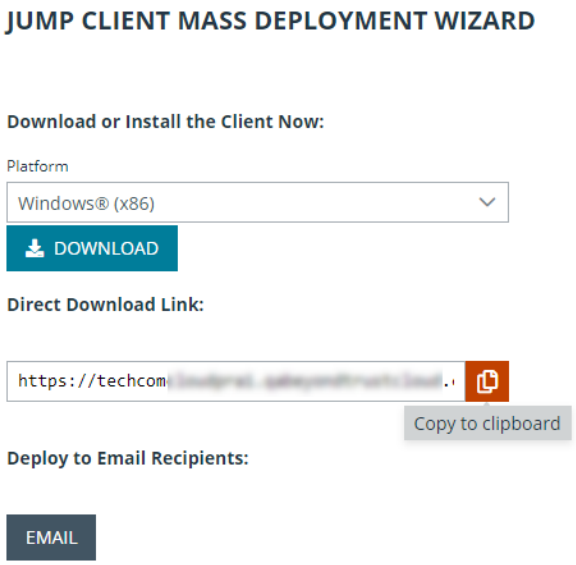
Note: *This option does not apply to headless Linux Jump Clients or Raspberry Pi Jump Clients.*

10. You can set the **Maximum Offline Minutes Before Deletion** of a Jump Client from the system. This setting overrides the global setting, if specified.

11. If **Prompt for Elevation Credentials if Needed** is selected, the installer prompts the user to enter administrative credentials if the system requires that these credentials be independently provided; otherwise, it installs the Jump Client with user rights. This applies only if an elevated install is being attempted.

Note: *This option does not apply to headless Linux Jump Clients or Raspberry Pi Jump Clients.*

12. Once you click **Create**, you can download the Jump Client installer immediately if you plan to distribute it using a systems management tool or if you are at the computer that you need to later access. You can also email the installer to one or more remote users. Multiple recipients can install the client from the same link. Click on the **Direct Download Link** to copy the link. The **Platform** option defaults to the appropriate installer for your operating system. You can select a different platform if you plan to deploy the Jump Client on a different operating system.



Note: *Once the installer has run, the Jump Client attempts to connect to the B Series Appliance. When it succeeds, the Jump Client appears in the Jump interface of the access console. If the Jump Client cannot immediately reach the B Series Appliance, then it continues to reattempt connection until it succeeds. If it cannot connect within the time designated by* ***This Installer Is Valid For****, then the Jump Client uninstalls from the remote system and must be redeployed.*

For more information, please see the following:

- *Jump Policy at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm*
- *Session Policy at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/session-policies.htm*

Install on Windows, Linux, or Mac Systems

For system administrators who need to push out the Jump Client installer to a large number of systems, the Windows, Mac, or Linux executable or the Windows MSI can be used with your systems management tool of choice. You can include a valid custom install directory path where you want the Jump Client to install.

> ***Note:*** *It is common for receive an error message during the install, regarding a layout or appearance issue. This can be disregarded.*
>
> *Duplicate installations of Jump Clients or large numbers of installations can lead to installation failures or degraded performance. Please see* *"Review Best Practices for Jump Client Mass Deployment — Windows" on page 24**.*

You can also override certain installation parameters specific to your needs. When you mark specific installation options for override during installation, you can use the following optional parameters to modify the Jump Client installer for individual installations. Note that if a parameter is passed on the command line but not marked for override in the /login administrative interface, the installation fails. If the installation fails, view the operating system event log for installation errors.

Command Line Parameter	Value	Description
--install-dir	<directory_path>	Specifies a new writable directory under which to install the Jump Client. This is supported only on Windows and Linux. When defining a custom install directory, ensure that the directory you are creating does not already exist and is in a location that can be written to.
--jc-name	<name...>	If override is allowed, this command line parameter sets the Jump Client's name.
--jc-jump-group	user:<username>jumpgroup:<jumpgroup-code-name>	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-session-policy	<session-policy-code-name>	If override is allowed, this command line parameter sets the Jump Client's session policy that controls the permission policy during an access session.
--jc-jump-policy	<jump-policy-code-name>	If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.
--jc-max-offline-minutes	<minutes>	The maximum number of minutes a Jump Client can be offline before it is deleted from the system. This setting overrides the global setting if specified.
--jc-ephemeral		Sets the maximum number of minutes a Jump Client will be offline before it is deleted from the system to 5 minutes. This is a convenience option that specifies the Jump Client as being ephemeral and is functionally equivalent to specifying **--jc-max-offline-minutes 5**
--jc-tag	<tag-name>	If override is allowed, this command line parameter sets the Jump Client's tag.

--jc-comments	<comments ... >	If override is allowed, this command line parameter sets the Jump Client's comments.
--silent		If included, the installer shows no windows, spinners, errors, or other visible alerts.

Note: *When deploying an MSI installer on Windows using an msiexec command, the above parameters can be specified by:*

1. *Removing leading dashes (--)*
2. *Converting remaining dashes to underscores (_)*
3. *Assigning a value using an equal sign (=)*

MSI Example:

```
msiexec /i bomgar-pec-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

When deploying an EXE installer, the above parameters can be specified by:

- *Adding dashes*
- *Adding a space between the parameter and the value*

EXE Example:

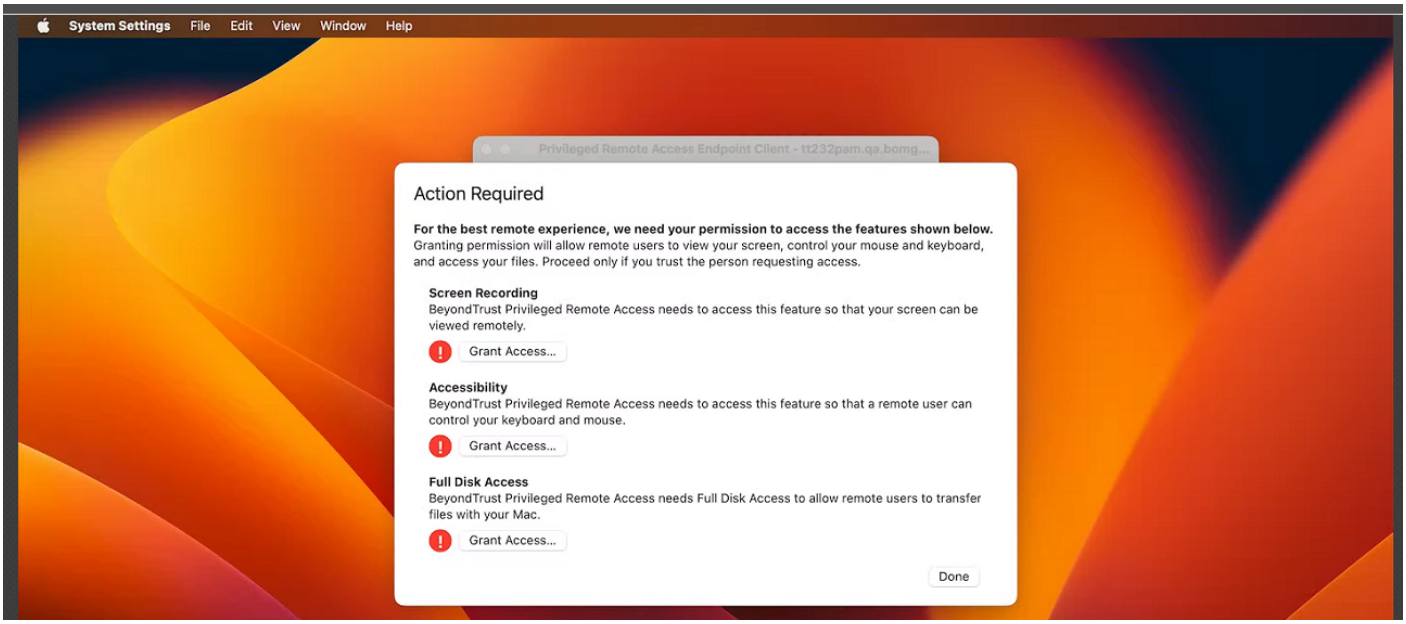
```
bomgar-pec-[unique id].exe --jc-jump-group jumpgroup:servers --jc-tag servers
```

Other rules to consider:

- ***installdir*** *has a dash in the EXE version but no dashes in the MSI version.*
- ***/quiet*** *is used for the MSI version in place of* ***--silent*** *in the EXE version.*

Enable a Jump Client on a Mac System

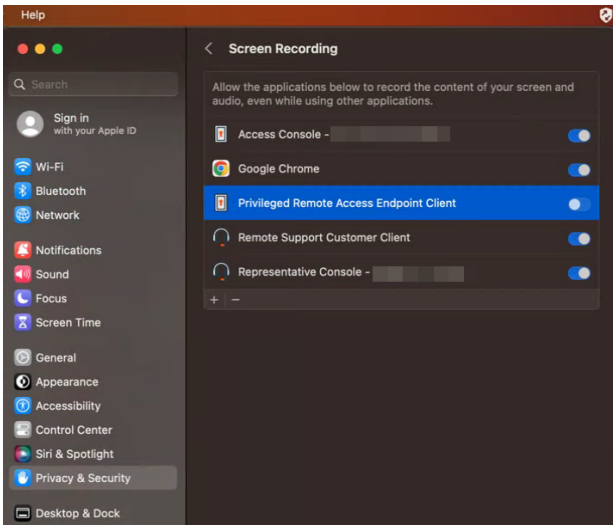
After a Jump Client is installed on a Mac system, it must be enabled by the end user. The exact steps, wording, and screen displays vary depending on the device and software version.



Three types of access are requested: **Screen Recording**, **Accessibility**, and **Full Disk Access**. For the best remote support experience, grant access for all three. Limited support is available if only one or two types of access are granted.

To grant access, the user takes the following steps for each type of access:

1. Click **Grant Access...**
2. Under **Privacy & Security**, applications that have requested access for the selected feature are listed. Toggles indicate if access has been granted. The newly installed client is disabled by default. Click the toggle to grant access to the client for this feature.



3. For the feature **Full Disk Access**, granting access requires stopping and restarting the client application. Click **Quit & Reopen** to grant access immediately. Jump Client icon disappears and re-appears within a few minutes.

The end user can grant or deny access at any time by clicking **Settings > Privacy & Security**, selecting the feature, **Accessibility**, **Screen Recordings**, or **Full Disk Access**, and then clicking the toggle.

Install a Linux Jump Client in Service Mode

> ***Note:*** *To install a Jump Client in service mode on a Linux system, the Jump Client installer must be run by root, but the Jump Client service should not be run under the root user context. A service mode Jump Client allows the user to start a session even if no remote user is logged on, as well as to log off the current remote user and log on with different credentials. A Linux Jump Client installed in user mode cannot be elevated within a session.*

Use the following syntax to add executable permissions to the file, wherein {uid} is a unique identifier consisting of letter and numbers:

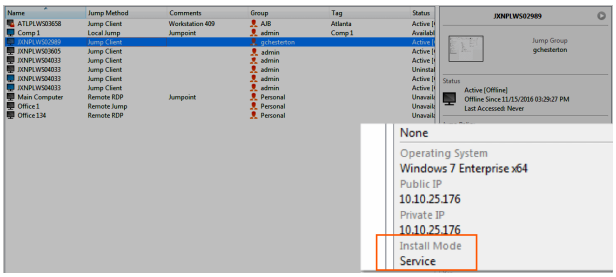
1. Add executable permissions to the file:

```
sudo chmod +x ./Downloads/bomgar-pec-[uid].desktop
```

2. Run the installer as the root user using the **sudo** command:

```
sudo sh ./Downloads/bomgar-pec-[uid].desktop
```

Linux Jump Clients may be installed in service mode. The current status of any Jump Client is shown in the info panel that appears when a Jump Client is highlighted in the representative console's list of Jump Clients. If a Jump Client shows the **Install Mode** as **Service**, it is installed as a service; otherwise, this field reads **User**, indicating it is installed in single-user context.



A service-mode Jump Client allows the user to start a session even if no remote user is logged on, as well as to log off the current remote user and log on with different credentials. A Linux Jump Client installed in user mode cannot do this, nor can it be elevated to service mode within a session.

To install a Jump Client in service mode on a Linux system, the Jump Client installer must be by run by root, but the Jump Client service should not be run under the root user context. This causes the Jump Client to run as a system service. If a previous Jump Client was installed in user mode, uninstall the existing Jump Client and install a new one as root. The process for doing this varies slightly depending on the distribution of Linux being used, but what follows is typical.

1. Log into the access console, right click the existing user mode Jump Client (if there is one), and then click **Remove**.
2. Log into the **/login** admin web interface of the BeyondTrust site and download a Jump Client installer for Linux from the **Jump > Jump Clients** tab.
3. Launch a terminal and add the executable permission to the installation file:

```
sudo chmod +x ./Downloads/bomgar-pec-[uid].desktop
```

4. Execute the installation file with sh as the root user using the sudo command:

```
sudo sh ./Downloads/bomgar-pec-[uid].desktop
```

Once the installation is complete, a new entry appears in the list of available Jump Clients displayed in the representative console. To test whether the Jump Client is installed as a service or not, you can Jump to the client and log out the active user. If you can still control the screen after logging out, this proves the client is running as a service.

Uninstall the Jump Client Installed Using Service Mode

If you wish to uninstall the Jump Client, you must run its uninstall script.

1. Navigate to the uninstall script in the following location: **/opt/bomgar/bomgar-pec-xxxxxx**.
2. Run the uninstall script:

```
sudo sh ./uninstall
```

3. Remove the Jump Client from the access console.

> ***Note:*** *If the uninstall script is run but the client is not removed from the console, the client is visible but not accessible. Similarly, if the client is removed from the console but the uninstall script is not run, the client is not accessible but the Jump Client files remain on the Linux system.*

Install on Headless Linux Systems

To install a Jump Client on a remote Linux system with no graphical user interface, be sure you have downloaded the headless Linux Jump Client installer, and then follow these additional steps:

1. Using your preferred method, push the Jump Client installer file to each headless Linux system you wish to access.
2. Once the installer file is on the remote system, use a command interface to install the file and specify any desired parameters.
    - Install the Jump Client in a location to which you have write permission, using **--install-dir <path>**. You must have permission to write to this location, and the path must not already exist. Any additional parameters must also be specified at this time, as described below.

      ```
      sh ./bomgar-pec-{uid}.bin --install-dir /home/username/jumpclient
      ```

    - If you wish to install under a specific user context, you can pass the **--user <username>** argument. The user must exist and have rights to the directory where the Jump Client is being installed. If you do not pass this argument, the Jump Client installs under the user context that is currently running.

      ```
      sh ./bomgar-pec-{uid}.bin --install-dir /home/username/jumpclient --user jsmith
      ```

IMPORTANT!

*We do not recommend installing the Jump Client under the root context. If you attempt to install when the current user is root, you receive a warning message and are required to pass **--user <username>** to explicitly specify the user that the process should run as.*

    - You can also override certain installation parameters specific to your needs. When you mark specific installation options for override during installation, you can use the following optional parameters to modify the Jump Client installer for individual installations. Note that if a parameter is passed on the command line but not marked for override in the /login administrative interface, the installation fails. If the installation fails, view the operating system event log for installation errors.

      ```
      sh ./bomgar-pec-{uid}.bin --install-dir /home/username/jumpclient --jc-jump-group
      jumpgroup:jump_group2
      ```

Command Line Parameter	Value	Description
--jc-jump-group	user:<username> team:<team-code-name>	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-jump-policy	<jump-policy-code-name>	If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.

--jc-tag	<tag-name>	If override is allowed, this command line parameter sets the Jump Client's tag.
--jc-comments	<comments ... >	If override is allowed, this command line parameter sets the Jump Client's comments.

3. After installing the Jump Client, you must start its process. The Jump Client must be started for the first time within the time frame specified by **This Installer Is Valid For**.

```
/home/username/jumpclient/init-script start
```

This init script also accepts the **stop**, **restart**, and **status** arguments. You can use **./init-script status** to make sure the Jump Client is running.

4. You must also arrange for **init-script start** to run at boot in order for the Jump Client to remain available whenever the system restarts. An example **system.d** service displays once the Jump Client is installed. Copy this information and create the new service for the Jump Client, **filename.service** (where *filename* is any name you choose), following these steps:

   - **cd /etc/systemd/system**
   - **vi filename.service**
   - Paste copied information
   - run **chmod 777 filename.service**
   - Reload the **systemctl** daemon
   - Enable and start the service file

Uninstall the Jump Client Installed on a Headless Linux System

1. If you wish to uninstall the Jump Client, you must run its uninstall script.

```
/home/username/jumpclient/uninstall
```

2. Remove the Jump Client from the access console.

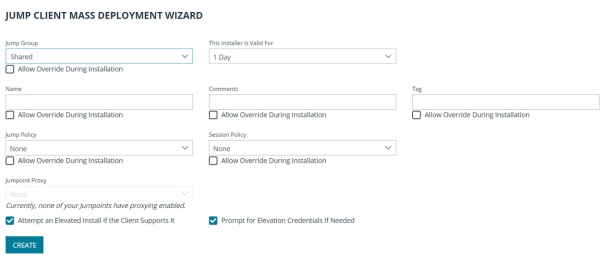
> ***Note:*** *If the uninstall script is run but the client is not removed from the console, the client is visible but not accessible. Similarly, if the client is removed from the console but the uninstall script is not run, the client is not accessible but the Jump Client files remain on the Linux system.*

Deploy a Jump Client on a Raspberry Pi

To access the File System, Command Shell, and System Info of a remote Raspberry Pi system, you can deploy a Jump Client to that system.

1. From the /login administrative interface, go to **Jump > Jump Clients**.

2. From the **Jump Group** dropdown, select whether to pin the Jump Client to your personal list of Jump Items or to a Jump Group shared by other users. Pinning to your personal list of Jump Items means that only you can access this remote computer through this Jump Client. Pinning to a shared Jump Group makes this Jump Client available to all members of that Jump Group.



3. You may apply a Jump Policy to this Jump Client. Jump Policies are configured on the **Jump > Jump Policies** page and determine the times during which a user can access this Jump Client. A Jump Policy can also send a notification when it is accessed or can require approval to be accessed. If no Jump Policy is applied, this Jump Client can be accessed without restriction.
4. You may choose a **Session Policy** to apply to this Jump Client. A session policy assigned to this Jump Client has the highest priority when setting session permissions.

> ***Note:*** *We recommend that you not set a session policy for a headless Jump Client.*

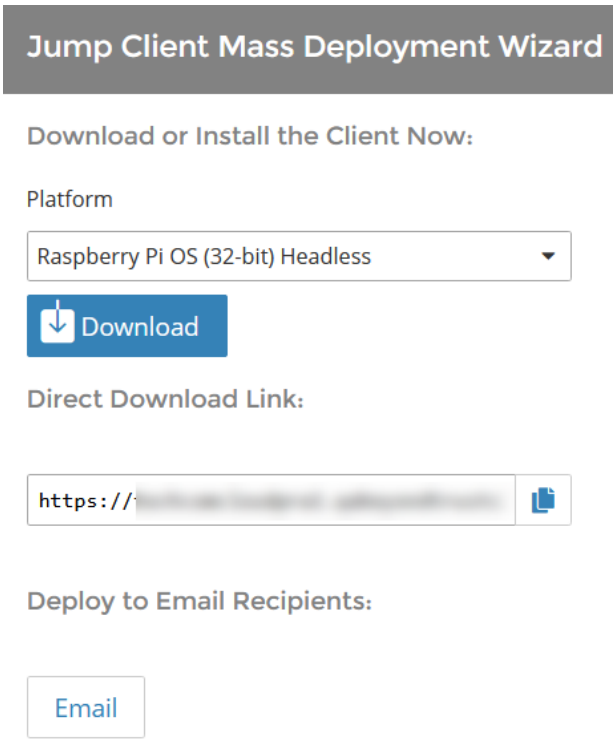
5. Adding a **Tag** helps to organize your Jump Clients into categories within the access console.
6. Set the **Connection Type** to **Active** or **Passive** for the Jump Clients being deployed. An active Jump Client maintains a persistent connection to the B Series Appliance, while a passive Jump Client instead listens for connection requests.
7. If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. That way, if these Jump Clients are installed on computers without native internet connections, they can use the Jumpoint to connect back to your B Series Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.
8. Add **Comments**, which can be helpful in searching for and identifying remote computers. Note that all Jump Clients deployed via this installer have the same comments set initially, unless you check **Allow Override During Installation** and use the available parameters to modify the installer for individual installations.
9. The installer remains usable only as long as specified by the **This Installer is Valid For** dropdown. Be sure to leave adequate time for installation. If someone should attempt to run the Jump Client installer after this time, installation fails, and a new Jump Client installer must be created. Additionally, if the installer is run within the allotted time but the Jump Client is unable to connect to the B Series Appliance within that time, the Jump Client uninstalls, and a new installer must be deployed. The validity time can be set for anywhere from 10 minutes to 1 year. This time does NOT affect how long the Jump Client remains active.

   In addition to expiring after the period given by the **This Installer is Valid For** option, Jump Client mass deployment packages invalidate when their B Series Appliance is upgraded. The only exception to this rule is live updates which change the license count or license expiration date. Any other updates, even if they do not change the version number of the B Series Appliance, invalidate the Jump Client installers from before the upgrade.

   Once a Jump Client has been installed, it remains online and active until it is uninstalled from the local system either by a user from the Jump interface or by an uninstall script. It can also be uninstalled, or extended, from the Jump Client Installer List. A user cannot remove a Jump Client unless the user is given appropriate permissions by their admin from the /login interface.

10. The options **Attempt an Elevated Install if the Client Supports It** and **Prompt for Elevation Credentials If Needed** do not apply to headless Jump Clients.

11. Once you click **Create**, select the **Raspberry Pi OS** option, and then click **Download**.



12. Using your preferred method, push the Jump Client installer file to each headless system you wish to access.
13. Once the installer file is on the remote system, install the file in a location to which you have write permission, using **--install-dir <path>**. You must have permission to write to this location, and the path must not already exist. Any additional parameters must also be specified at this time, as described below.

```
sh ./bomgar-pec-{uid}.bin --install-dir /home/pi/<dir>
```

14. You can also override certain installation parameters specific to your needs. When you mark specific installation options for override during installation, you can use the following optional parameters to modify the Jump Client installer for individual installations. Note that if a parameter is passed on the command line but not marked for override in the /login administrative interface, the installation fails. If the installation fails, view the operating system event log for installation errors.

Command Line Parameter	Value	Description
--jc-jump-group	user:<username> jumpgroup:<jumpgroup-code-name>	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-public-site-address	<public-site-address-hostname>	If override is allowed, this command line parameter associates the Jump Client with the public portal which has the given hostname as a site address. If no public portal has the given hostname as a site address, then the Jump Client will revert to using the default public site.

--jc-session-policy-not-present	<session-policy-code-name>	If override is allowed, this command line parameter sets the Jump Client's session policy that controls the permission policy during a support session if the customer is not present at the console.
--jc-jump-policy	<jump-policy-code-name>	If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.
--jc-tag	<tag-name>	If override is allowed, this command line parameter sets the Jump Client's tag.
--jc-comments	<comments ... >	If override is allowed, this command line parameter sets the Jump Client's comments.

15. After installing the Jump Client, you must start its process. The Jump Client must be started for the first time within the time frame specified by **This Installer Is Valid For**.

```
/home/username/jumpclient/init-script start
```

This init script also accepts the **stop**, **restart**, and **status** arguments. You can use **./init-script status** to make sure the Jump Client is running.

16. You must also arrange for **init-script start** to run at boot in order for the Jump Client to remain available whenever the system restarts. An example **system.d** service displays once the Jump Client is installed. Copy this information and create the new service for the Jump Client, **filename.service** (where *filename* is any name you choose), following these steps:

- **cd /etc/systemd/system**
- **vi filename.service**
- Paste copied information
- run **chmod 777 filename.service**
- Reload the **systemctl** daemon
- Enable and start the service file

17. If you wish to uninstall the Jump Client, you must run its uninstall script.

```
/home/pi/<dir>/uninstall
```

Note: *Separately and in addition to running the uninstall script, you must remove the Jump Client via the access console. Otherwise, the Jump Client remains in the access console, though it is not accessible. Relatedly, removing the Jump Client via the access console only prevents it from being accessed but leaves the Jump Client files on the system.*

For more information, please see the following:

- *Jump Policy at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm*
- *On setting up Jumpoints as proxies, the Jumpoint Guide at www.beyondtrust.com/docs/Privileged-Remote-Access/how-to/jumpoint/index.htm*

Review Best Practices for Jump Client Mass Deployment — Windows

Avoid Deploying Duplicates

When mass-deploying the SRA Jump Client MSI with tools such as SCCM or Altiris, it is important to avoid installing duplicate clients, because this can cause multiple deployment failures. BeyondTrust does not provide any utilities for deploying clients, but there are some basic methodologies you can use to script a deployment system that will only install Jump Clients on systems that do not have one installed already. These methods depend on whether you already have Jump Clients installed.

If you have already installed Jump Clients, your script can be modified to prevent duplicates. If you have installed Jump Clients, you can use the INSTALLDIR.MSI variable or a custom file as described below. When you use INSTALLDIR, the MSI installation package itself automatically aborts if it finds the directory you specify already exists. If you choose the custom file option, you must script the install to check for this file prior to running the MSI installation package.

Prevent Additional Duplicates

If your deployment tool has already deployed duplicate clients, edit your script so that the tool aborts installation if the target system matches either of these conditions:

- The system has any **bomgar-pec.exe** processes running.
- The system has any **DisplayName** registry entries matching *BeyondTrust Privileged Remote Access Jump Client [support.example.org]*, where *support.example.com* matches the hostname of your SRA appliance.

Prevent Duplicates Before Deployment

If your deployment tool has not yet deployed any clients, you can script the tool to use the INSTALLDIR variable or deploy a custom file during the install process.

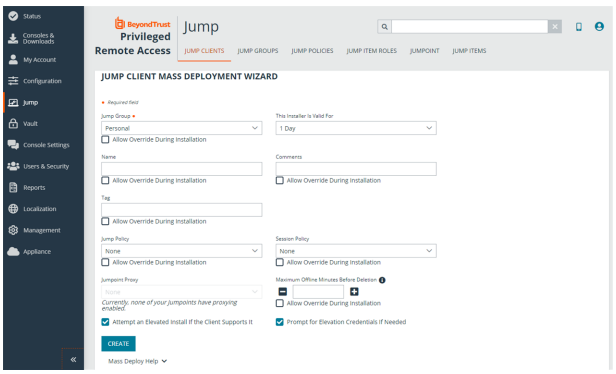
Use INSTALLDIR

Follow these steps to use the INSTALLDIR variable:

1. From the /login administrative interface, go to **Jump > Jump Clients**.
2. At the top of the **Jump Client Installer List**, click **Add**.
3. Enter the appropriate mass deployment wizard parameters.
4. Click **Create**.
5. Select **Windows (x64) MSI**, copy the string after *KEY_INFO=*, and then click **Download/Install**.
6. Load the downloaded MSI into your deployment tool and script the tool to install it using the following command:

   msiexec /i bomgar-scc-win64.msi KEY_INFO=<key_info_string> INSTALLDIR=<installDir> /quiet

   where *<key_info_string>* is the *KEY_INFO* string you copied earlier and *<installDir>* is the install directory of your choice.



7. Configure the deployment tool to abort installation if it finds the install directory you have chosen is already present.

Use a Custom File

You have the option of deploying a custom file during installation and automatically aborting subsequent duplicate installation if this file is found. To do this:

1. Save a small text file with a descriptive title such as **PRAJumpClient.txt** to a shared network location accessible from all systems on which Jump Clients will be deployed.
2. Follow the above steps for using INSTALLDIR to create and download an MSI installation file.
3. Configure the script to abort if the **PRAJumpClient.txt** file already exists, or copy it to the local system and install the MSI file if the text file does not exist.

Manage Deployment Rate

It is important to consider rate of deployment if mass deploying on a large scale. A large number of simultaneous client installations can cause network traffic delays.

Depending on the deployment method used, the granular control allowed may vary. We recommend deploying no more than 60 clients per minute to avoid installation failures and degraded performance. For reference, 60 clients per minute equates to:

- 1 client install per second
- 60 client installs per minute
- 3,600 client installs per hour

Performance impact may vary with environmental factors, usage patterns, and appliance resources. BeyondTrust recommends starting mass deployment conservatively with smaller scale pushes at slower rates to confirm acceptable performance before gradually scaling up the number and rate of deployment.

For more information, please see "Deploy Jump Clients from the Administrative Interface" on page 12.

Review Additional Considerations for Jump Client Mass Deployment — macOS

The installer files for access consoles and Jump Clients allow you to mass deploy BeyondTrust software to your macOS devices. This guide provides examples of how to mass-deploy BeyondTrust software using generally accepted deployment concepts. Actual deployment steps may vary.

Set Privacy Policy Preference Control

Starting with macOS Mojave (10.14), Apple introduced new privacy controls for end users. These controls require that applications be granted permission to access sensitive data or use macOS accessibility features. As an administrator, you can grant these permissions to an MDM-managed Mac using a Privacy Policy Preference Control (PPPC) profile. To ensure proper functionality of the BeyondTrust Privileged Remote Access Customer Client, deploy a PPPC profile targeting the following app bundle:

- **Identifier**: com.bomgar.bomgar-pec
- **Identifier Type**: Bundle ID
- **Code Requirement**: identifier "com.bomgar.bomgar-pec" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = B65TM49E24

Service	Purpose	Allowed
Accessibility	Screen Sharing	true
SystemPolicyAllFiles (Full Disk Access)	File Transfer	true
ScreenCapture (Screen Recording)	Screen Sharing	AllowStandardUserToSetSystemService

Note: *Screen recording can only be configured via MDM to allow a non-admin user to provide consent. IT administrators cannot grant screen recording permissions on behalf of end users. This preference is applicable for systems running macOS Big Sur (11.0) and later.*

Configure Managed Login Items

Starting with macOS Ventura 13, Apple introduced a new framework for managing background tasks such as LaunchAgents, LaunchDaemons, and Login Items. BeyondTrust's Jump Client for Privileged Remote Access leverages background tasks to ensure the client is running at all times. Administrators can manage these background tasks using a Managed Login Items payload delivered to managed devices. To ensure proper functionality, deploy a configuration profile targeting the below values:

Rule Type	Rule Value
Label Prefix	Bomgar
Team Identifer	B65TM49E24
Label Prefix	com.bomgar

Configure Appliance

When deploying the Jump Client, there are two prerequisites that must be completed in Privileged Remote Access.

- A user account with administrative permission to access the /login interface is required. This user can create Jump Clients only for Jump Groups where they have appropriate permissions.
- To ensure that a single Jump Client installer can be used to pin a system to any Jump Group, a service account with **Manage** permissions on all Jump Groups must be created.

Create a Service Account User for Jump Client Package Creation

1. Log in to the Privileged Remote Access user interface.
2. Click **Users & Security**.
3. Click **Add**.
4. Fill in the basic details for the user account.
5. Expand **Account Settings**.
6. Check **Account Never Expires**, if necessary.
7. Expand **Access Permissions**.
8. Ensure **Allowed to access endpoints** is checked.
9. Uncheck all boxes under the **Session Management** and **User-to-User Screen Sharing** areas.
10. Under **Allowed Jump Item Methods**, ensure:
    - **Jump Clients** is checked
    - All other methods are uchecked
11. Under **Jump Item Roles**, ensure:
    - **Default** dropdown is set to **Administrator**
    - **System** dropdown is set to **Administrator**
12. Click **Save**.

Create a Jump Client Installer Package

1. Log in to the Privileged Remote Access appliance using the new account created above.
2. Click **Jump**.
3. Click **Add** to add a new Jump Client Installer.
4. Select a default Jump Group within the **Jump Client Mass Deployment Wizard**.
5. Check **Allow Override During Installation** for all available options.
6. Select your desired validity period from the **This Installer is Valid For** dropdown .
7. Check **Start Customer Client Minimized When Session is Started**, to ensure a completely silent deployment.
8. Click **Create.**
9. From the **Platform** dropdown, select **macOS** (for programmatic installation).
10. Click **Download**. A DMG file downloads. This is later imported into your management platform.

Note: *Do not rename the downloaded DMG file.*

Deploy Manually

The BeyondTrust Privileged Remote Access Jump Client installer is delivered as a uniquely generated and named DMG file. This file has the format **bomgar-pec-<uid>.dmg**.

For deployment, the sequence of steps includes:

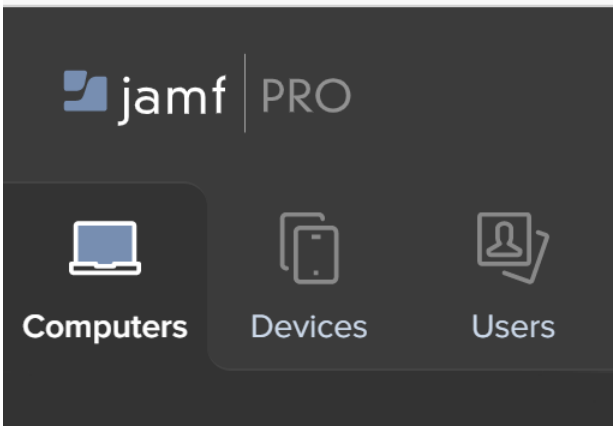
1. Stage the DMG file in a temporary location.
2. Mount the DMG file.
3. Install the Remote Support Jump Client.
4. Unmount the disk image.
5. Remove the DMG from the temporary location.

Deploy using JAMF Pro

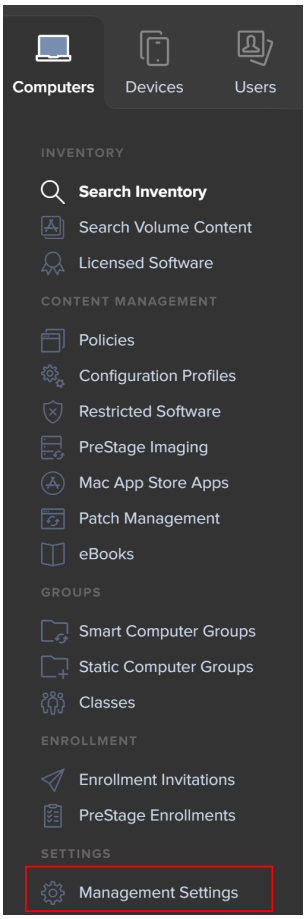
> ***Note:*** *This information is provided for general assistance when using JAMF Pro, however BeyondTrust cannot provide support for third-party products, and their requirements and operations may change.*

Upload Package to Jamf Software Server

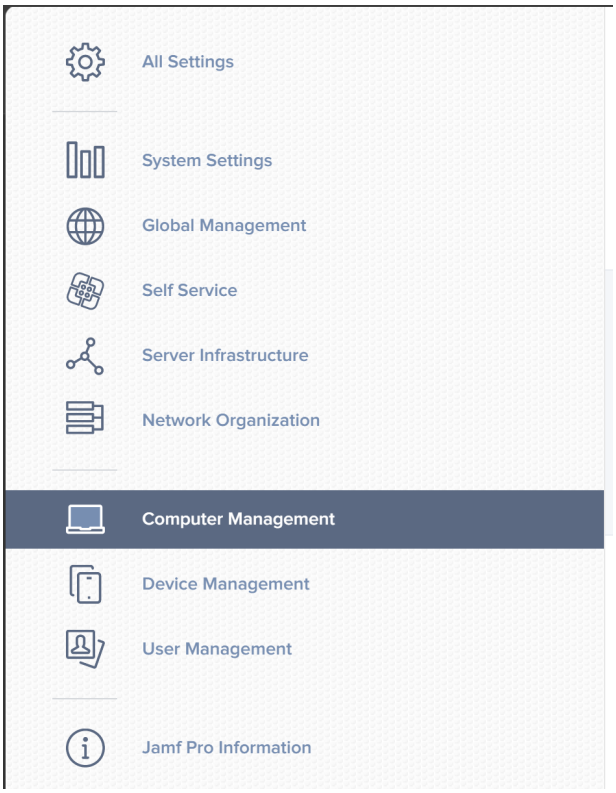
1. Log in to your Jamf Software Server (JSS) via a web browser.
2. Click **Computers**.



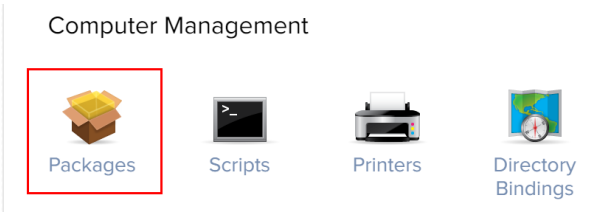
3. Click **Management Settings**.



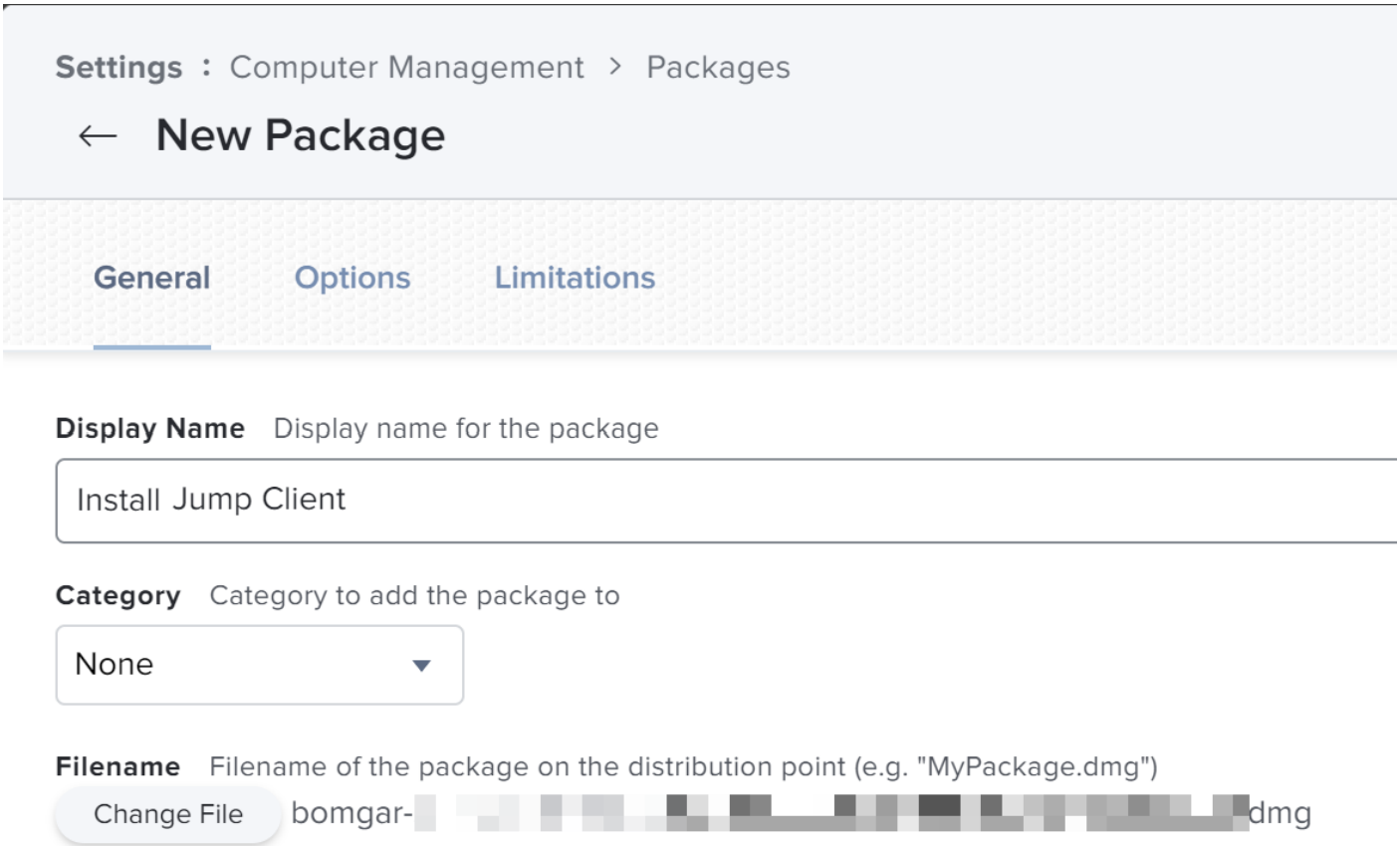
4. Click the **Computer Management** tab.



5. Click **Packages**.
6. Click **New**.



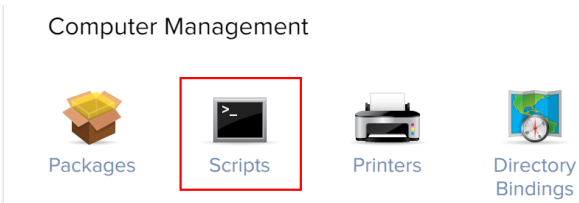
7. Fill out a display name, and choose a category (if applicable).



8. Click **Upload** to choose the DMG file.
9. Click **Save**.

Upload Deployment Script

10. If necessary, log in to the JSS via a web browser.
11. Click **Computers**.
12. Click **Management Settings**.
13. Click the **Computer Management** tab.
14. Click **Scripts**.
15. Click **New**.



16. Copy and paste this sample deployment script on the **Script** tab:

```
hdiutil attach /Library/Application\ Support/JAMF/Waiting\ Room/bomgar-scc-<uid>.dmg

sudo /Volumes/bomgar-scc/Open\ To\ Start\ Support\ Session.app/Contents/MacOS/sdcust --silent

sleep 15
```

17. Update the file name to match the DMG file downloaded from your appliance. For Privileged Remote Access, this includes updating *bomgar-scc* to *bomgar-pec*.
18. Click **Save**.

Note: *Some networks or environments may have configurations that prevent endpoints from checking for malicious software. This can addressed by adding*

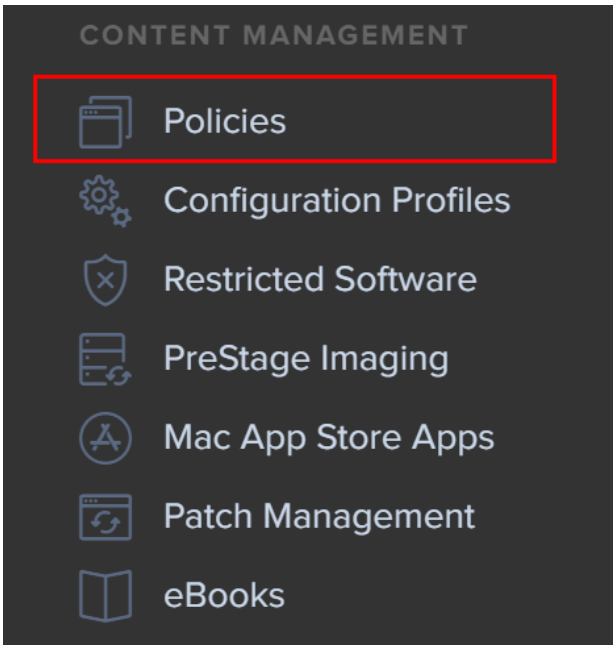
```
xattr -d com.apple.quarantine bomgar-scc-[uid].dmg
```

to the script, or by enabling Stapled Mac Notarization. Administrators should evaluate which approach is more appropriate for their environment.

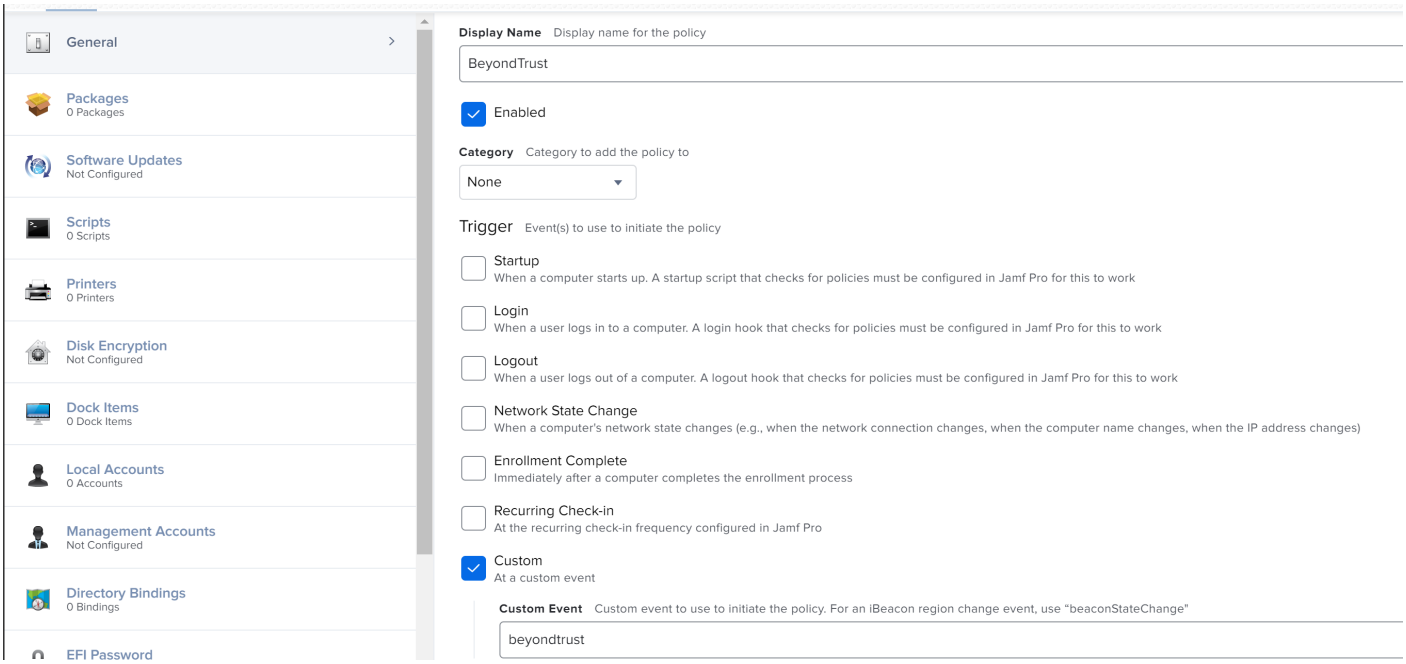
*For detailed information on **sdcust** usage, see **Mass Deploy Help** located within the /login interface on **Jump > Jump Client**.*

Create Deployment Policy

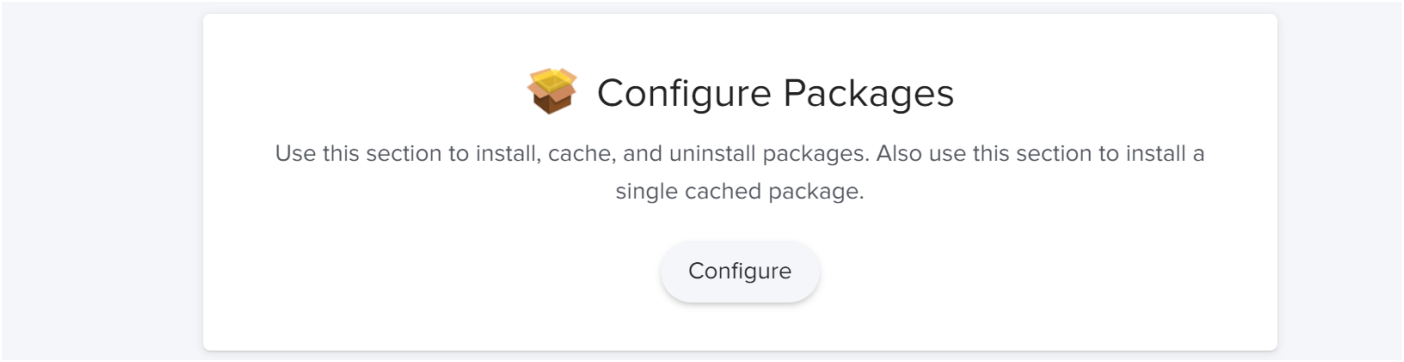
19. If necessary, log in to the JSS via a web browser.
20. Click **Computers**.
21. Click **Policies**.
22. Click **New**.



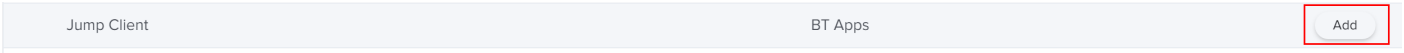
23. Provide a policy name, configure desired policy triggers, and ensure **Execution Frequency** is **Once Per Computer**.



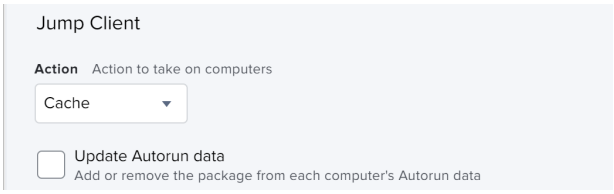
24. Click **Packages**, and then click **Configure**.



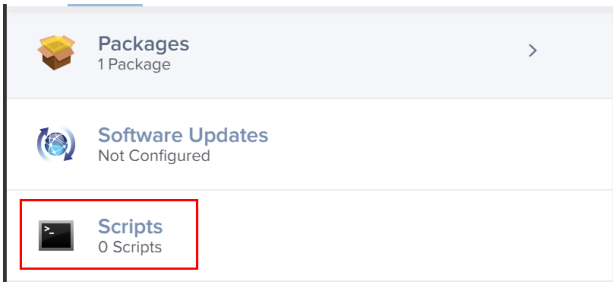
25. Click **Add** to select the Jump Client package from the list of available packages.



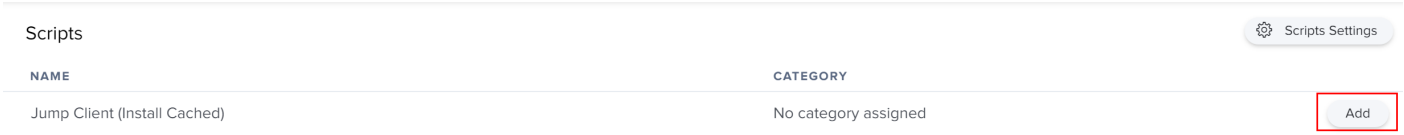
26. Select **Cache** as the action. This makes the packages available in the JAMF downloads folder for use by the deployment script created earlier.



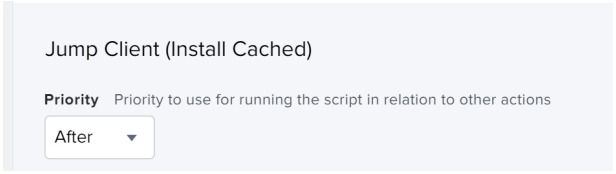
27. Click **Scripts** from the left navigation menu.



28. Click **Add** to select the deployment script created above.



29. Confirm that the **Priority** is set to **After**.
30. Click **Save**.



The created policy now runs based on the defined trigger(s) to install the BeyondTrust Jump Client.

For more information, please see "Deploy Jump Clients from the Administrative Interface" on page 12.

Manually Modify Windows Jump Client Proxy Information

In some cases, the proxy settings of an existing Windows Jump Client must be manually modified to accommodate changes in the proxy environment. The Jump Client has built-in logic to automatically detect updated proxy information within a 24-hour period. However, if the proxy enforces authentication, then the end-user is prompted to enter authentication credentials. If the system is unattended, then credentials and/or other proxy information may need to be manually entered.

The following steps guide you through manually modifying proxy-related sections of the **settings.ini** file used by the Jump Client.

***Tip:** If a large number of systems must be manually modified, the process can be automated. You can develop a script to do this, or contact BeyondTrust Technical Support at www.beyondtrust.com/support to engage the BeyondTrust Professional Services group.*

To manually modify the proxy information for a pre-existing Jump Client on a Windows system:

1. Go to **C:\ProgramData\bomgar-scc-<uid>**, where **<uid>** is the Jump Client's unique ID.
2. Locate and edit the **settings.ini** file.
3. Within **settings.ini**, locate the proxy-related section, titled **[Proxy]**. An example existing proxy section is shown below.

```
[Proxy]
version=2
detect_failed=0
[Proxy\access.example.com:443\LastGood]
Proxy=DIRECT
[Proxy\access.example.com:443\Detected\1]
Proxy=DIRECT
```

4. Remove all of the settings within the **[Proxy]** section and replace them with the settings as follow. Replace all <bracketed> text with the appropriate information.

```
[Proxy]
version=1
ProxyUser=<domain\user>
ProxyPass=<password>
[Proxy\Manual]
ProxyMethod=<numeric value of 0=DIRECT, 100=HTTP CONNECT, 200=SOCKS4>
ProxyHost=<proxy hostname/ip>
ProxyPort=<proxy port>
```

An example of a manually modified section is below.

```
[Proxy]
version=1
ProxyUser=myDomain\proxyUser
ProxyPass=MyPassword
[Proxy\Manual]
ProxyMethod=200
ProxyHost=myproxyserver.example.com
ProxyPort=8443
```

5. Save and close the **settings.ini** file.
6. Either reboot the system or stop/start the BeyondTrust Jump Client service for the new information to apply.
7. The Jump Client nows use the manually defined proxy information.

Note: *After making the above changes to the* ***settings.ini*** *file, the defined username and password which were entered in plain text will be hashed into an unreadable format.*

Manage Jump Client Settings

From the /login administrative interface, go to **Jump > Jump Clients**.

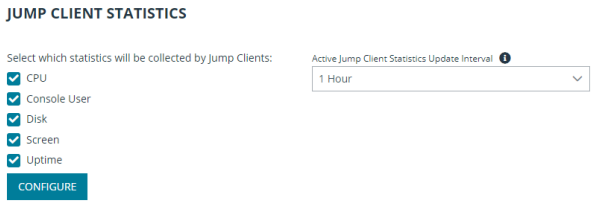
Manage Installers with the Jump Client Installers List

This list shows all previously installed active Jump Client installers. Administrators and privileged users can view, download, delete, or extend Jump Client installers.

A warning message appears at the top of the list: *Installing more than one Jump Client on the same system is being phased out in a future release. In the Access Console you may use the **copy** action on a Jump Client to apply different policies to the same endpoint.* Click **Dismiss** to remove the warning message.

Choose Statistics

An administrator can choose which statistics to view for all Jump Clients on a site-wide basis. These statistics are displayed in the access console and include CPU, console user, disk usage, a thumbnail of the remote screen, and uptime.



The **Active Jump Client Statistics Update Interval** determines how often these statistics are updated. Managing which statistics are viewed and how often can help to regulate the amount of bandwidth used. The more active Jump Clients you have deployed, the fewer the statistics and the longer the interval may need to be.

Manage Upgrades

> ***Note:*** *Regulating bandwidth applies to on-premises installations only.*

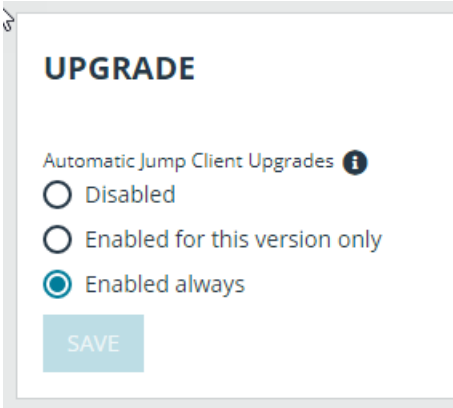
You can regulate the bandwidth used during upgrades by setting **Maximum bandwidth of concurrent Jump Client upgrades**.

Also set the maximum number of Jump Clients to upgrade at the same time. Note that if you have a large number of Jump Clients deployed, you may need to limit this number to regulate the amount of bandwidth consumed.

> ***Note:*** *In order to manually update Jump Clients in the privileged web access console, you must first disable automatic Jump Client upgrades.*

Use the radio buttons below to control automatic Jump Client upgrades. You can:

- Permanently disable Jump Client upgrades.
- Temporarily enable Jump Client upgrades for the current upgrade cycle.
- Permanently enable Jump Client upgrades.



IMPORTANT!

When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.

Choose Maintenance Options

Set the global connection rate for disconnected Jump Clients to try to reconnect.

If a Jump Client goes offline and does not reconnect to the B Series Appliance for the number of days specified by the **Number of days before Jump Clients that have not connected are automatically deleted** setting, it is automatically uninstalled from the target computer and is removed from the Jump interface of the access console.

Note: *This setting is shared with the Jump Client during normal operation so that even if it cannot communicate with the site, it uninstalls itself at the configured time. If this setting is changed after the Jump Client loses connection with the B Series Appliance, it uninstalls itself at the previously configured time.*

If a Jump Client goes offline and does not reconnect to the B Series Appliance for the number of days specified by the **Number of days before Jump Clients that have not connected are automatically deleted** setting, it is labeled as lost in the access console. No specific action is taken on the Jump Client at this time. It is labeled as lost only for identification purposes, so that an administrator can diagnose the reason for the lost connection and take action to correct the situation.

Note: *To allow you to identify lost Jump Clients before they are automatically deleted, this field should be set to a smaller number than the deletion field above.*

Note: *You can set Jump Clients to allow or disallow simultaneous Jumps from the* ***Jump > Jump Items > Jump Settings*** *section. If allowed, multiple users can gain access to the same Jump Client without an invitation to join an active session by another user. If disallowed, only one user can Jump to a Jump Client at a time. Only an invitation by the user who originated the session can allow for a second user to access the session.*

Uninstalled Jump Client Behavior determines how a Jump Client deleted by an end user is handled by the access console. Depending on dropdown option selected, the deleted item can either be marked as uninstalled and kept in the list or actually be removed from the Jump Items list in the access console. If the Jump Client cannot contact the B Series Appliance at the time it is uninstalled, the affected item remains in its offline state.

Manage Other Options

Allow users to attempt to wake up Jump Clients provides a way to wake up a selected Jump Client by broadcasting Wake-on-LAN (WOL) packets through another Jump Client on the same network. Once a WOL is attempted, the option becomes unavailable for 30 seconds before a subsequent attempt can be made. WOL must be enabled on the target computer and its network for this function to work. The default gateway information of the Jump Client is used to determine if other Jump Clients reside on the same network. When sending a WOL packet, the user has an advanced option to provide a password for WOL environments that require a secure WOL password.

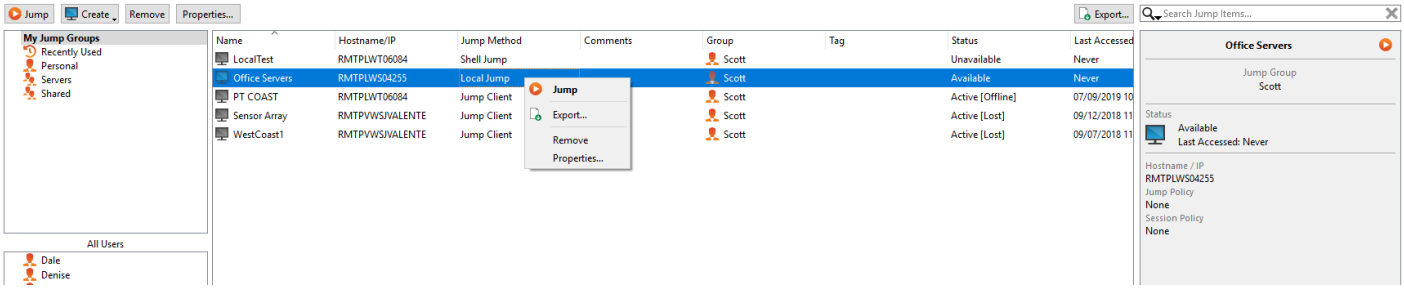
Start an Access Session through a Jump Client

Once a Jump Client has been installed on a remote computer, permitted users can use the Jump Client to initiate a session with that computer, even if the computer is unattended.

From the Access Console

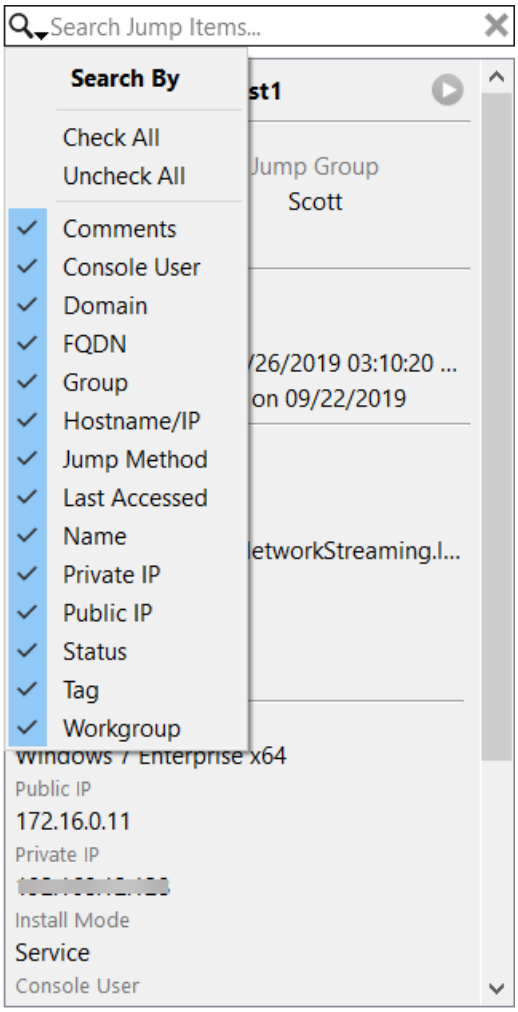
Your Jump Clients are listed in the Jump Interface.

> ***Note:*** *In addition to Jump Clients, you may also see Jump shortcuts for Remote Jumps, Local Jumps, RDP sessions, VNC sessions, and Shell Jumps. Collectively, Jump Clients and Jump shortcuts are referred to as Jump Items. For more information about Jump shortcuts, see the Jumpoint Guide.*



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.



If a Jump Group contains tagged Jump Items, an arrow appears to the left of the Jump Group name. Click the arrow to show or hide the tags.

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

To view additional statistics about a Jump Item, select the Jump Item. Available statistics appear in the right pane.

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

IMPORTANT!

When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.

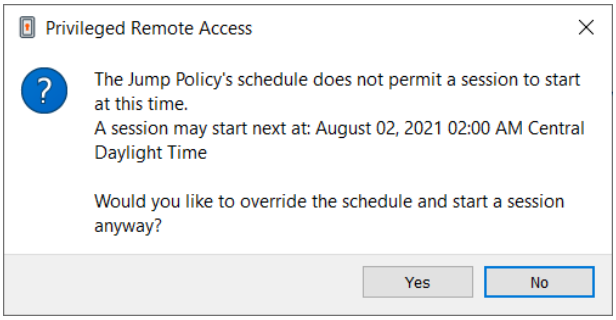
To start a session, double-click the Jump Item or select the Jump Item and click the **Jump** button from:

- above the Jump interface
- the right-click menu of the Jump Item
- the top of the Jump Item statistics pane

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

Schedule

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



Notification

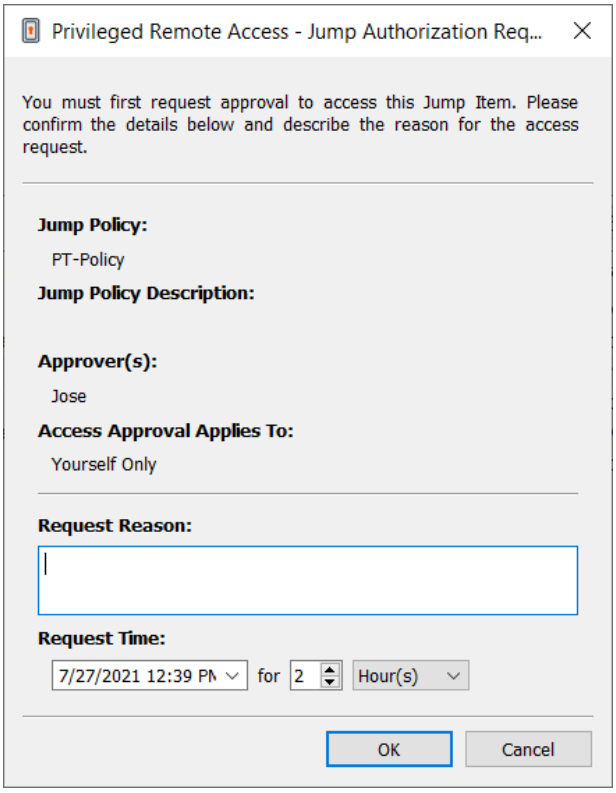
If a Jump Policy is configured to send a notification on session start or end, then an attempt to access a Jump Item alerts you that an email will be sent. You can choose to proceed with the Jump and send a notification, or you can cancel the Jump.

Ticket ID

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

Authorization

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



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

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

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

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

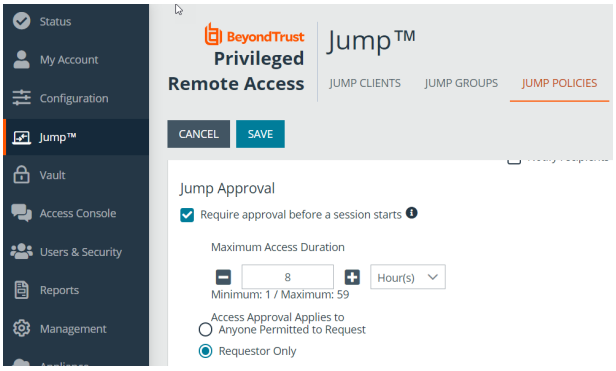
When approval has been granted to a Jump Item, that Jump Item becomes available either to any user who can see and request access to that Jump Item or only to the user who requested access. This is determined by the Jump Policy.

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

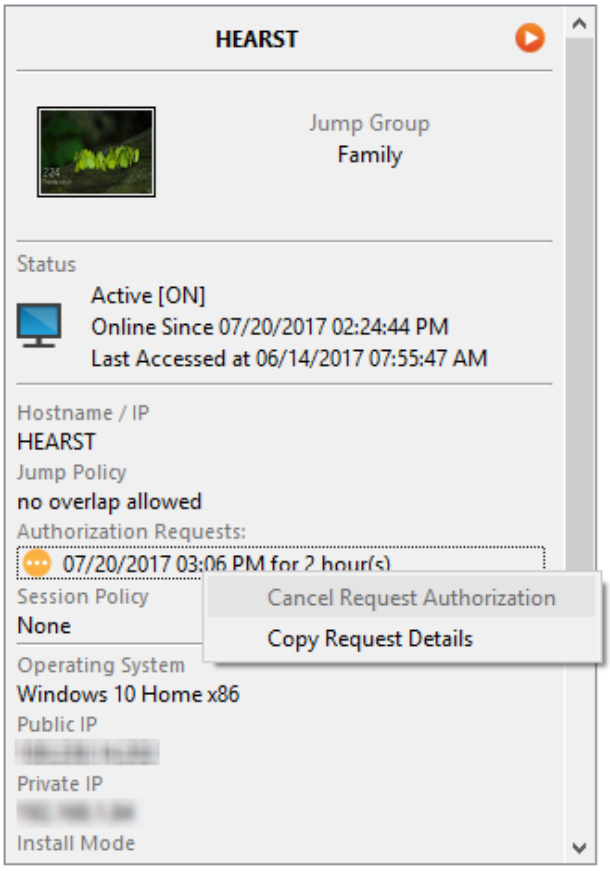
Revoke an Access Approval Request

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

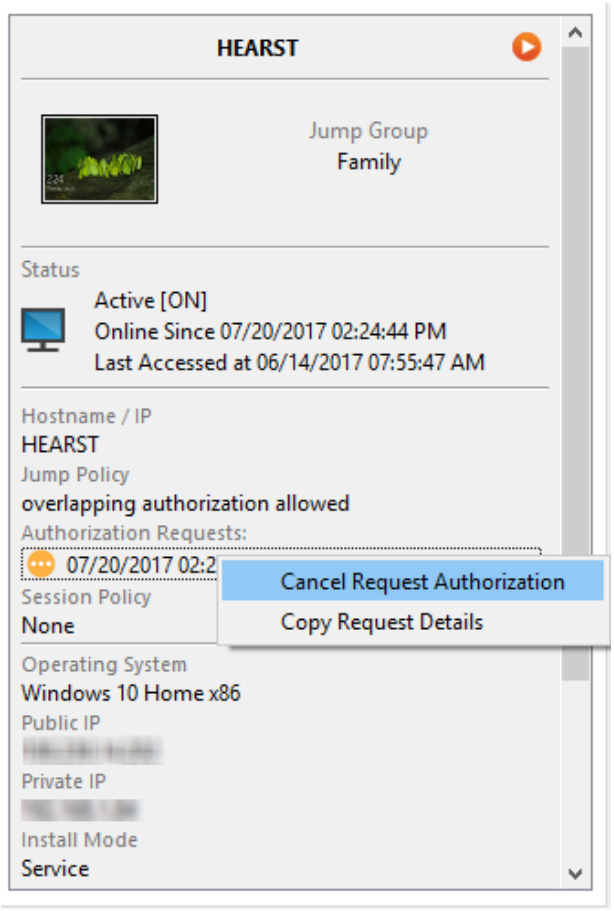
- **Anyone Permitted to Request**
- **Requestor Only**



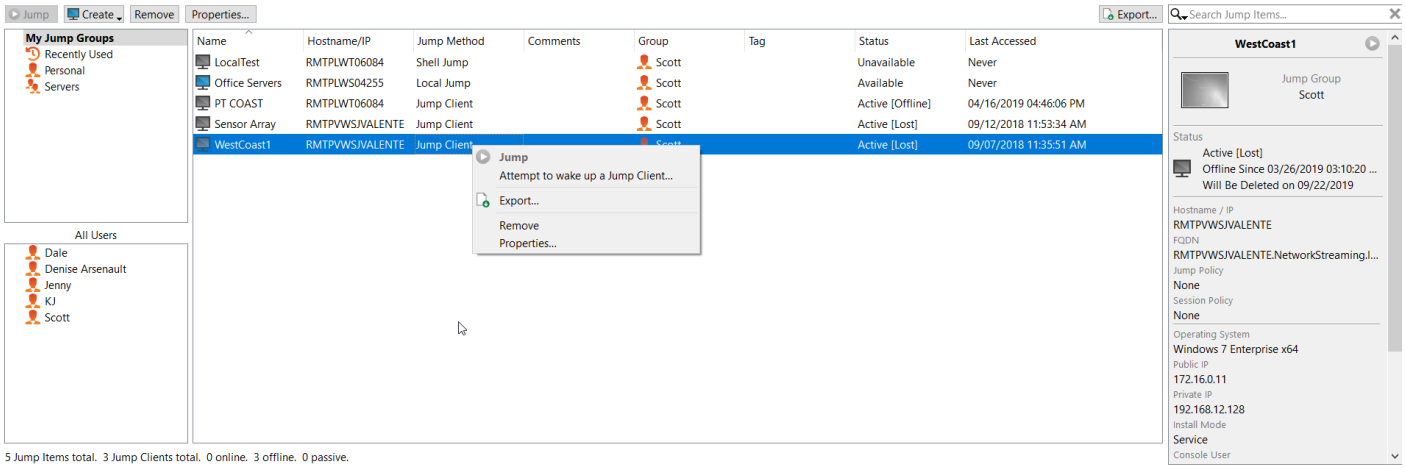
If the Jump Policy is set to **requestor Only**, and an Access Request is presently approved for User A, User B is asked to create a new Access Request if they attempt to Jump to the Jump Item, since that request does not apply to them. Additionally, if User B attempts to cancel the Access Approval Request,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



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



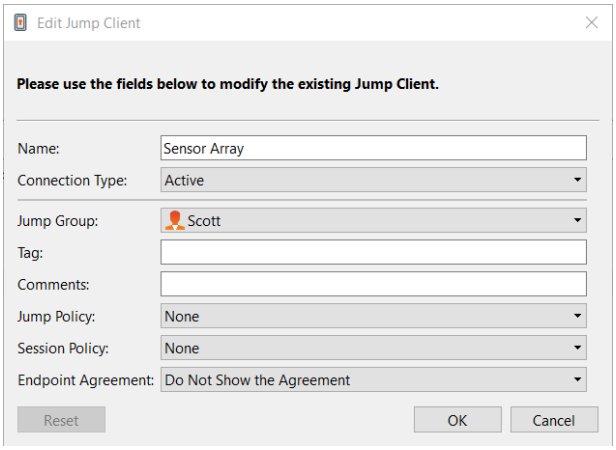
Depending on the permissions set by your administrator, you may also be able to wake up a selected Jump Client by broadcasting Wake-on-LAN (WOL) packets through another Jump Client on the same network. Once a WOL is attempted, the option becomes unavailable for 30 seconds before a subsequent attempt can be made. WOL must be enabled on the target computer and its network for this function to work. The default gateway information of the Jump Client is used to determine if other Jump Clients reside on the same network. When sending a WOL packet, the user has an advanced option to provide a password for WOL environments that require a secure WOL password.



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

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

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.).*

Jump Client Properties

- 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.

From the API

By integrating with the BeyondTrust API, you may programmatically connect to a Jump Item directly from your systems management tool or ticketing system. To start a session with a Jump Item from an external program, you will need to use a BeyondTrust Console Script (BRCS). A BRCS contains a sequence of commands to be executed by the access console. Double-click a BRCS file to have it automatically executed by the access console, or incorporate it into an external application to send commands to the access console from that application.

One method of creating a BRCS is through the client scripting API. This API is located on your B Series Appliance at **https://access.example.com/api/client_script**, where **access.example.com** is your BeyondTrust site hostname.

> ***Note:*** *By default, access to the API is SSL-encrypted; however, you can choose to allow HTTP access by checking the* ***Allow HTTP Access to XML API*** *option on the* ***Management > API Configuration*** *page of the* ***/login*** *administrative interface.* ***It is highly recommended that HTTP remain disallowed as a security best practice****.*
>
> *This option has been deprecated as of 16.1 and does not appear to new users. For users upgrading from a version prior to 16.1, the option is still available if you continue to use the deprecated method of authenticating to the API with a user account. If you switch to the preferred method of authenticating with an API account, all API traffic must occur over HTTPS.*

Optional Parameters for the start_jump_item_session Command

jump.method	If specified, only Jump Items using the designated Jump method are included in the results. Acceptable values for this field are **push** (remote push), **local_push**, **pinned** (Jump Client), **rdp**, **vnc,** and **shelljump**.
credential_id	If specified, only a Jump Item with that specific credential ID associated is returned. This field has a maximum length of 255 characters.
search_string	Identifies the search criteria used to select and return specific Jump Items as results. ***Note:*** *This parameter is required only if no of the client fields below are specified.*
client.comments	If specified, only Jump Items with the given comments are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.

client.hostname	If specified, only Jump Items with the given hostname are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.
client.private_ip	If specified, only Jump Clients with the given private IP address are included in the results. This search field applies only to pinned clients. This field has a maximum length of 255 characters. Search is partial and case-insensitive.
client.public_ip	If specified, only Jump Clients with the given public IP address are included in the results. This search field applies only to pinned clients. This field has a maximum length of 255 characters. Search is partial and case-insensitive.
client.tag	If specified, only Jump Items with the given tag are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.
session.custom.[custom field]=[string]	The code name and value of any custom fields. These fields must first be configured in **/login > Management > API Configuration**. Each attribute must be specified as a different parameter. Each custom field has a maximum length of 1024 characters. The maximum total size of all combined custom fields, including the external key, must be limited to 10KB.

IMPORTANT!

*At least one **client.*** parameter must be specified. If multiple **client.*** parameters are specified, then only clients matching all criteria are returned.*

Query Examples: start_jump_item_session

Start a session with a Jump Item whose hostname contains "ABCDEF02"	https://access.example.com/api/client_script?type=rep&operation=generate&action=start_jump_item_session&client.hostname=ABCDEF02
Start a session with a Jump Item whose comments contain "maintenance" and whose tag contains "server"	https://access.example.com/api/client_script?type=rep&operation=generate&action=start_jump_item_session&client.comments=maintenance&client.tag=server
Start a session with a pinned Jump Client whose private IP address begins with "10.10.24" and associate custom attributes with the session	https://access.example.com/api/client_script?type=rep&operation=generate&action=start_jump_item_session&client.private_ip=10.10.24&jump.method=pinned&session.custom.custom_field1=Custom%20Value&session.custom.custom_field2=123

> ***Note:*** *If more than one Jump Item matches the search criteria, then a dialog opens, giving the user the option to select the appropriate Jump Item.*

Sending one of the above requests to the API prompts the user to download a BRCS file. After downloading the file, the user can run it to automatically open the access console and start a session with a Jump Item.

In addition to generating a script from the API, you can run a BRCS via the command prompt. From the command prompt, go to the directory which contains the access console. Enter the name of your BeyondTrust access console (e.g., bomgar-acc.exe), followed by one of two commands:

```
--run-script [BRCS command]
--run-script-file [path to BRCS file]
```

Examples:

```
bomgar-acc-x64.exe --run-script "action=start_jump_item_session&client.hostname=ABCDEF02"
bomgar-acc-x64.exe --run-script-file my_script_file.brcs-beta60
```

All Jump Items which this user is permitted to access are searched. If the search results in only one Jump Item, the session starts immediately. If multiple Jump Items are returned, select one of the Jump Items listed in the selection window and click **OK**.

For more information about BeyondTrust Access Console Scripting, see the API Guide at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm.

> ***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.*

> *For more information on Jump Items for mobile devices, please see the following:*
>
> - *Use Jump Items to Access Endpoints from the Android Access Console at www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/android/jump-items.htm*
> - *Use Jump Items to Access Endpoints from the iOS Access Console at www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/jump-items.htm*

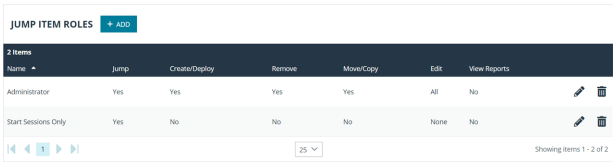
Use Cases for Implementing Jump Clients

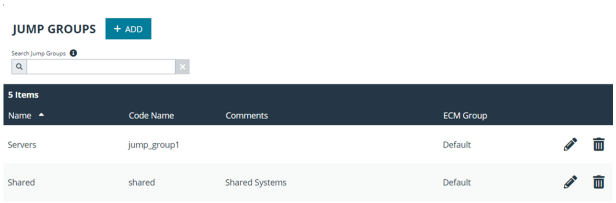
To offer you the most flexibility and control over your Jump Items, BeyondTrust includes quite a few separate areas where permissions must be configured. To help you understand how you might want to set up your system, we have provided two use cases below.

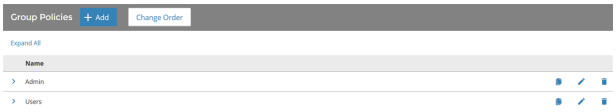
Basic Use Case

You are a small organization without a lot of Jump Items or users to manage. You want your administrators to manage all of the Jump Item setup steps and your users to only be able to Jump to those items.

1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**.
    - The **Administrator** role should have all permissions enabled.
    - The **Start Sessions Only** role should have only **Start Sessions** enabled.
2. Create a **Shared** Jump Group that will contain all shared Jump Items. Personal Jump Items can also be created.
3. Put users into two group policies, **Admin** and **Users**.

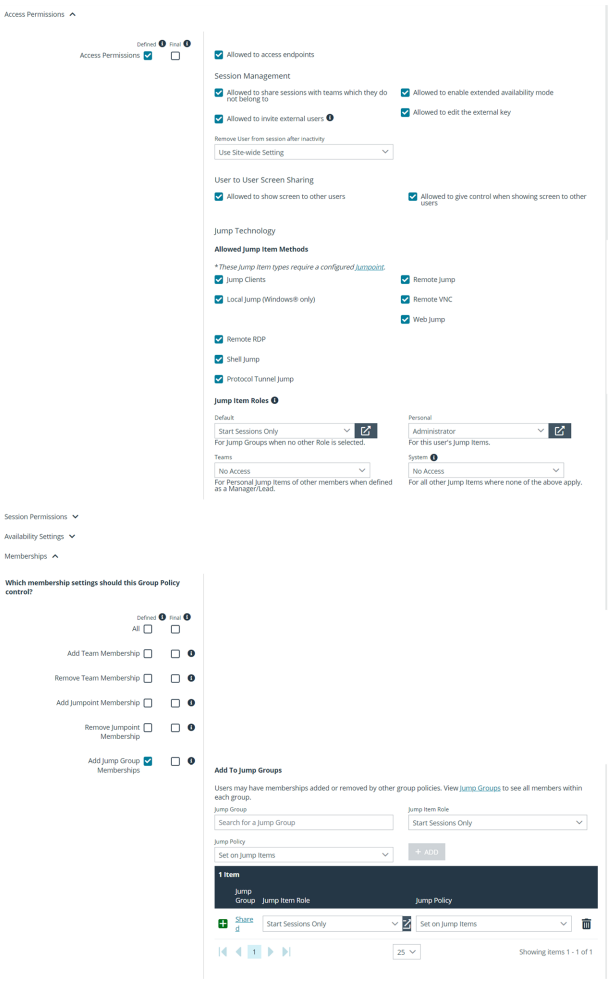




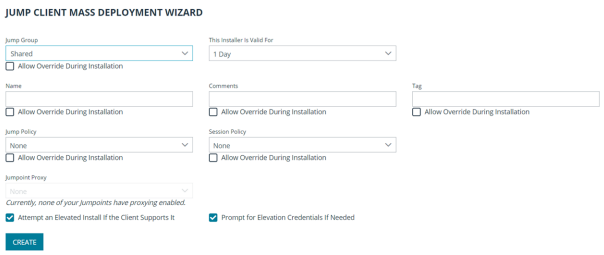


4. In the **Admin** group, configure settings and permissions as appropriate. The permissions should include the following:
    - Define **Access Permissions** and check **Allowed to access endpoints**.
    - Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    - Under **Jump Item Roles**, set the **Default** and **Personal** roles to **Administrator**.
    - Set the **Team** and **System** roles to **Start Sessions Only**.
    - Under **Memberships**, define **Add to Jump Groups**.
    - In the **Jump Group** field, search for and select **Shared**.
    - Set the **Jump Item Role** to **Administrator**.
    - Click **Add** to assign the members of this group policy to the Jump Group.
    - Save the group policy.

5. In the **Users** group, configure settings and permissions as appropriate. The permissions should include the following:
    - Define **Access Permissions** and check **Allowed to access endpoints**.
    - Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    - Under **Jump Item Roles**, set the **Default** to **Start Sessions Only**.
    - Set the **Personal** Jump Item Role to **Administrator**.
    - Set the **Team** and **System** roles to **No Access**.
    - Under **Memberships**, define **Add to Jump Groups**.
    - In the **Jump Group** field, search for and select **Shared**.
    - Set the **Jump Item Role** to **Start Sessions Only**.
    - Click **Add** to assign the members of this group policy to the Jump Group.
    - Save the group policy.



6. Deploy Jump Items, assigning them to the **Shared** Jump Group.



7. Now, administrators can deploy and start sessions with Jump Items in the **Shared** Jump Group. They can also manage their personal lists of Jump Items and start sessions with all other Jump Items.

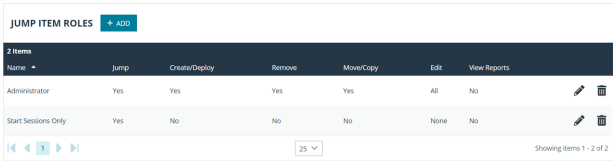
    Likewise, users can now start sessions with Jump Items in the **Shared** Jump Group. They can also manage their personal lists of Jump Items.

Advanced Use Case

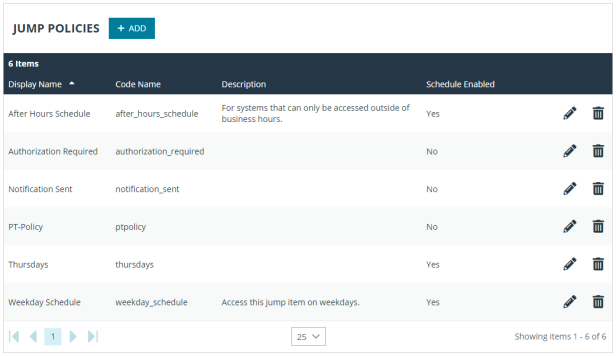
You are a large organization with a lot of Jump Items to manage and with users to manage in three different departments. You want your administrators to manage all of the Jump Item setup steps and your users to only be able to Jump to those items. In addition to your local

users, you have some third-party vendors who need occasional access. Some Jump Items should be accessible at all times, while others should be accessible only once a week.

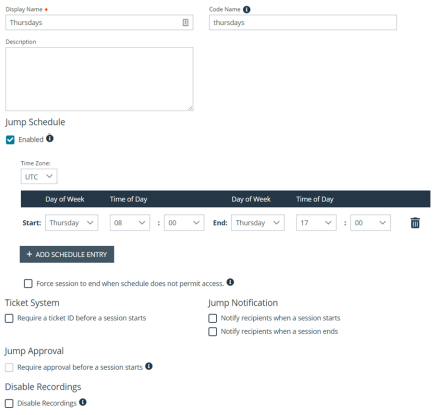
1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**.
    - The **Administrator** role should have all permissions enabled.
    - The **Start Sessions Only** role should have only **Start Sessions** enabled.



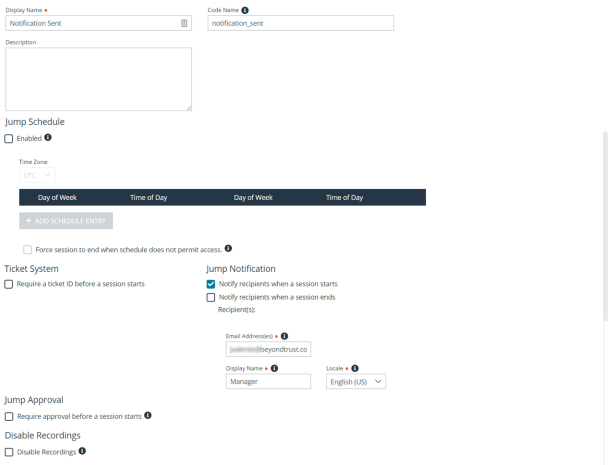
2. Create three Jump Policies, **Thursdays**, **Notification Sent**, and **Authorization Required**.



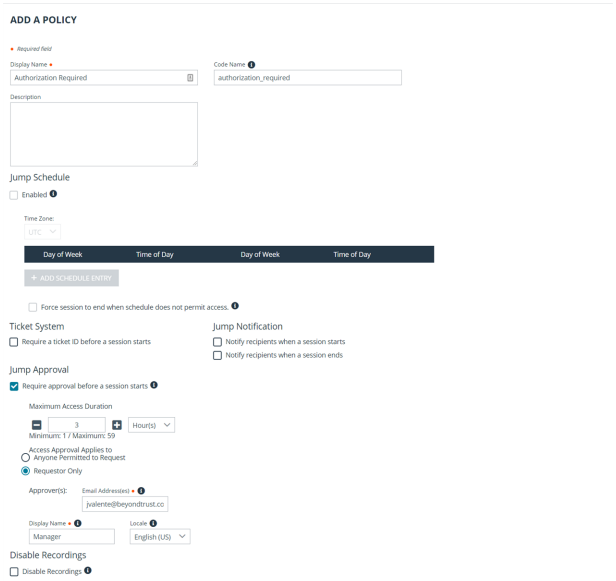
3. For the **Thursdays** policy, enable the **Jump Schedule**.
    - Click **Add Schedule Entry**.
    - Set the **Start** day and time to **Thursday 8:00** and the **End** day and time to **Thursday 17:00**.
    - Save the Jump Policy.



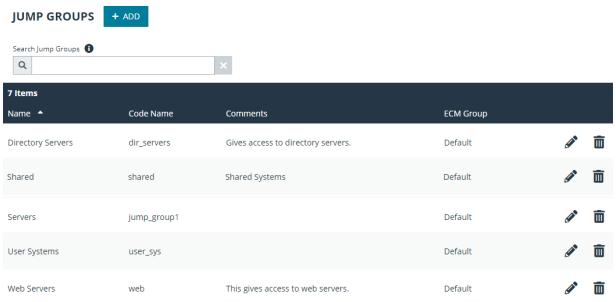
4. For the **Notification Sent** policy, check **Notify recipients when a session starts**.
    - Add the **Email Addresses** of one or more recipients who should be notified when a session starts.
    - Add a **Display Name** such as **Manager**. When a user attempts to start a session with a Jump Item that has this policy applied, the user sees an alert that a notification will be sent to the name set here.
    - Save the Jump Policy.



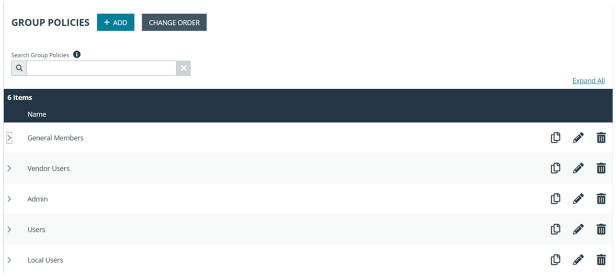
5. For the **Authorization Required** policy, check **Require approval before a session starts**.
    - Set the **Maximum Access Duration** to **3 Hours**.
    - Under **Access Approval Applies to**, select **Requestor Only**.
    - Add the **Email Addresses** of one or more recipients who can approve or deny access to Jump Items.
    - Add a **Display Name** such as **Manager**. When a user requests access to a Jump Item that has this policy applied, the user must fill out a request for authorization form. On that form, the approver's name is displayed as set here.
    - Save the Jump Policy.



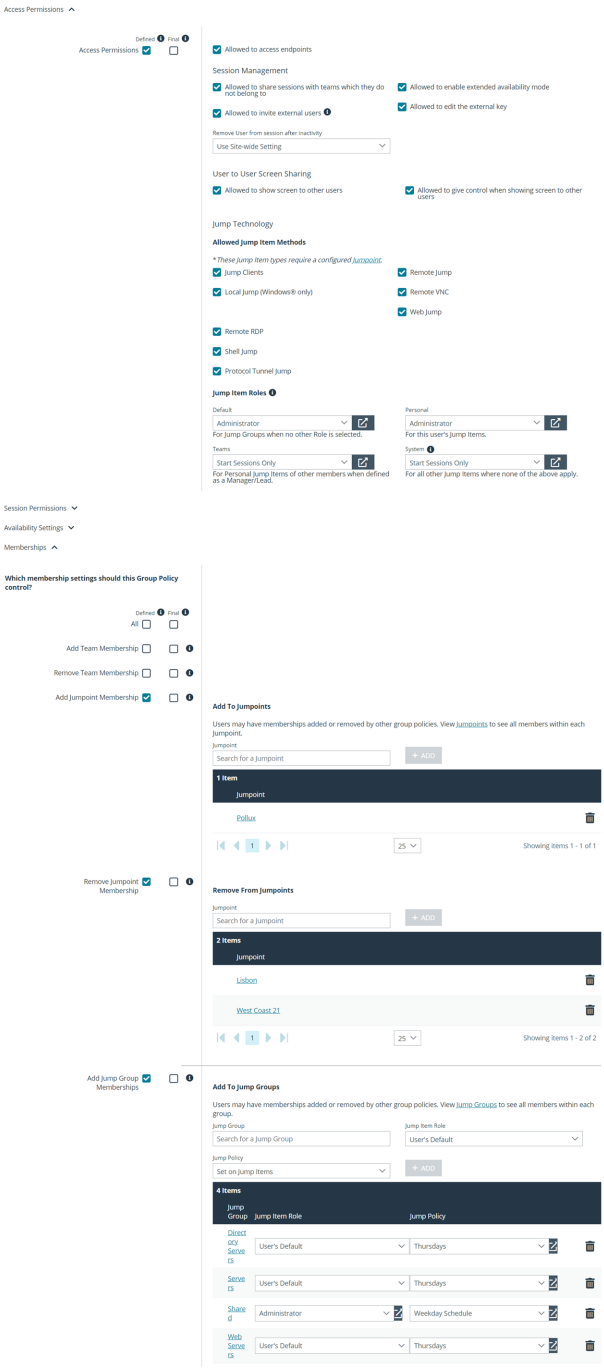
6. Create three Jump Groups, **Web Servers**, **Directory Servers**, and **User Systems**. Personal Jump Items can also be created.



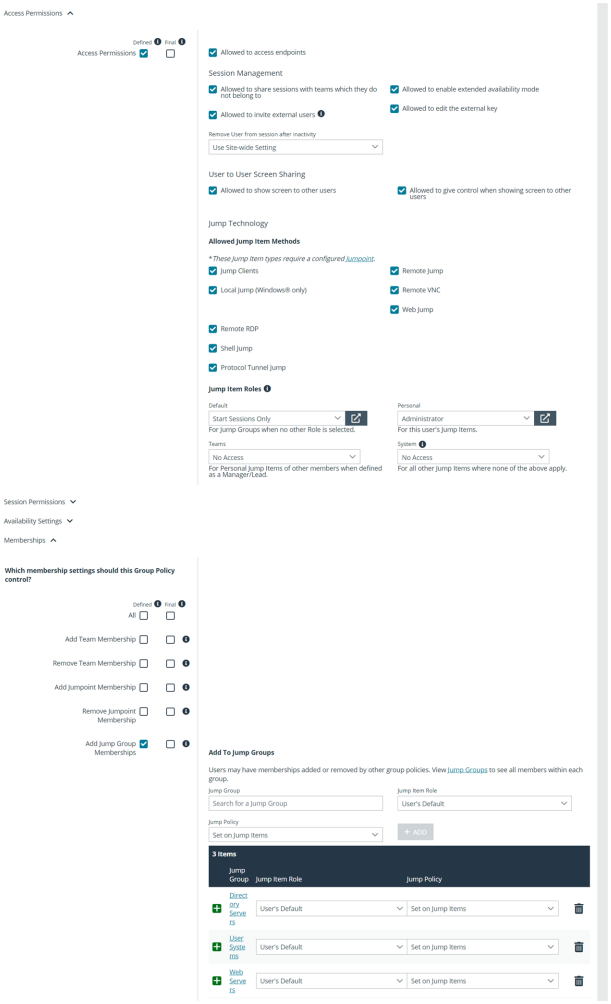
7. Put users into three group policies, **Admin**, **Local Users**, and **Third-Party Users**.



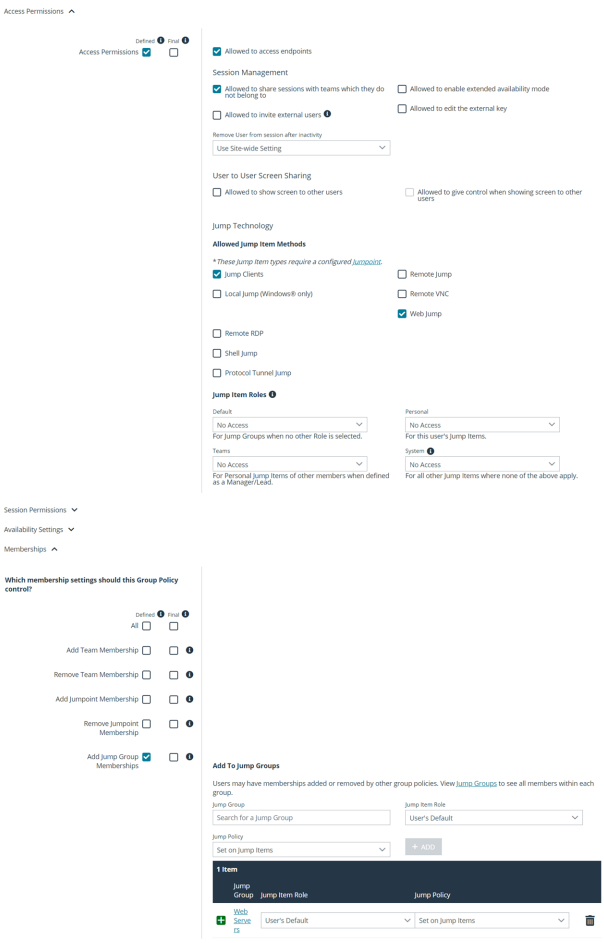
8. In the **Admin** group, configure settings and permissions as appropriate. The permissions should include the following:
    - Define **Access Permissions** and check **Allowed to access endpoints**.
    - Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    - Under **Jump Item Roles**, set the **Default** and **Personal** roles to **Administrator**.
    - Set the **Team** and **System** roles to **Start Sessions Only**.
    - Under **Memberships**, define **Add to Jump Groups**.
    - In the **Jump Group** field, search for and select **Web Servers**.
        - Set the **Jump Item Role** to **Administrator**.
        - Leave **Jump Policy** set to **Set on Jump Items**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - In the **Jump Group** field, search for and select **Directory Servers**.
        - Set the **Jump Item Role** to **Administrator**.
        - Leave **Jump Policy** set to **Set on Jump Items**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - In the **Jump Group** field, search for and select **User Systems**.
        - Set the **Jump Item Role** to **Administrator**.
        - Leave **Jump Policy** set to **Set on Jump Items**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - Save the group policy.



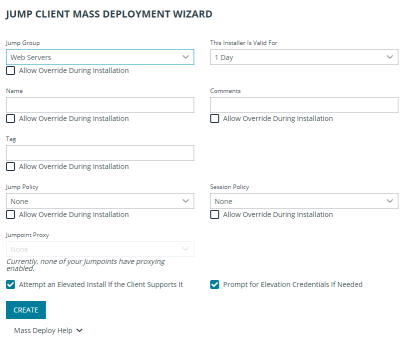
9. In the **Local Users** group, configure settings and permissions as appropriate. The permissions should include the following:
    - Define **Access Permissions** and check **Allowed to access endpoints**.
    - Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    - Under **Jump Item Roles**, set the **Default** to **Start Sessions Only**.
    - Set the **Personal** Jump Item Role to **Administrator**.
    - Set the **Team** and **System** roles to **No Access**.
    - Under **Memberships**, define **Add to Jump Groups**.
    - In the **Jump Group** field, search for and select **Web Servers**.
        - Set the **Jump Item Role** to **Start Session Only**.
        - Set **Jump Policy** to **Notification Sent**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - In the **Jump Group** field, search for and select **Directory Servers**.
        - Set the **Jump Item Role** to **Start Session Only**.
        - Set **Jump Policy** to **Notification Sent**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - In the **Jump Group** field, search for and select **User Systems**.
        - Set the **Jump Item Role** to **Start Session Only**.
        - Set **Jump Policy** to **Thursdays**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - Save the group policy.



10. In the **Third-Party Users** group, configure settings and permissions as appropriate. The permissions should include the following:
    - Define **Access Permissions** and check **Allowed to access endpoints**.
    - Under **Jump Technology**, check all **Allowed Jump Methods** that these users should be allowed to use.
    - Under **Jump Item Roles**, set all roles to **No Access**.
    - Under **Memberships**, define **Add to Jump Groups**.
    - In the **Jump Group** field, search for and select **Web Servers**.
        - Set the **Jump Item Role** to **Start Session Only**.
        - Set **Jump Policy** to **Authorization Required**.
        - Click **Add** to assign the members of this group policy to the Jump Group.
    - Save the group policy.



11. Deploy Jump Items, assigning them to the three Jump Groups as appropriate. If any particular Jump Item requires a different Jump Policy, assign that, as well.



12. Now, administrators can deploy and start sessions with Jump Items in all three Jump Groups. They can also manage their personal lists of Jump Items and start sessions with all other Jump Items.

    Likewise, local users can now start sessions with Jump Items in all three Jump Groups, with a notification sent upon session start and with user systems accessible only on Thursdays. They can also manage their personal lists of Jump Items.

    Finally, third-party users can start sessions with Jump Items in the **Web Servers** Jump Group, with approval required before they can complete the Jump. They cannot deploy personal Jump Items.

Appendix: Require a Ticket ID Workflow for Jump Client Access

If your service requests use ticket IDs as part of the change management workflow, connect your ticket IDs to endpoint access in BeyondTrust. By leveraging BeyondTrust Jump Technology with your existing ticket ID process, your change management workflow integration lets you restrict a BeyondTrust access request by requiring a Ticket ID to be entered as part of the access request process before an access session begins.

What Users See

When users of the BeyondTrust access console attempt to access a Jump Item that uses a Jump Policy configured to require a ticket ID, a dialog opens. In the administrator-configured dialog, users enter the ticket ID needed, authorizing access this Jump Item.

To set up the connection to your existing ITSM or ticket ID system, create a Jump Policy you can apply to those Jump Items you want to only be used if a ticket ID from your external system is entered.

How It Works

After the user enters the required ID and clicks **OK**, the B Series Appliance posts an HTTP outbound request to the ticket system URL configured in Jump Policies. The request contains information about both the ticket ID and the Jump Item, as well as user information. Your external system then replies asynchronously to either allow or deny access.

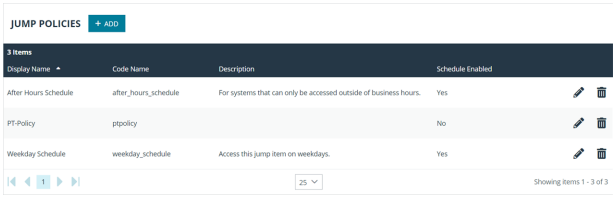
If the request is allowed, the external ticket ID system assigns the allowed session. Optionally, your external ITSM or ticket ID system may send a list of custom session attributes in its response to assign to the allowed session. For more information on using the BeyondTrust API see the Privileged Remote Access API Programmer's Guide at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api.

Follow the steps below to set up a ticket ID requirement for access.

Create a Jump Policy Requiring Ticket ID Approval

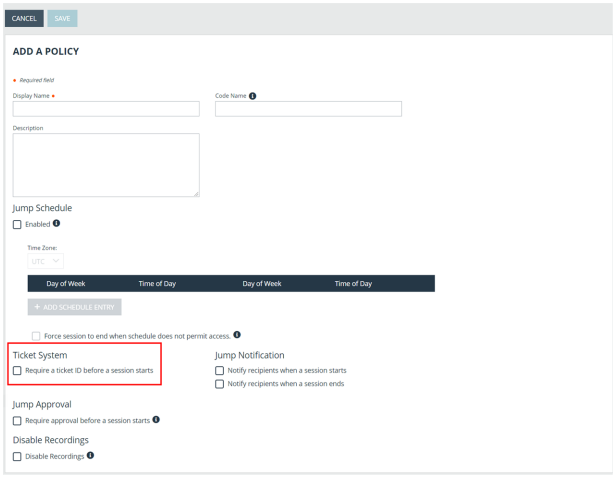
First, create a Jump Policy with the requirement of ticket ID approval enabled.

1. From your BeyondTrust /login administrative interface, go to **Jump > Jump Policies**.
2. In the **Jump Policies** section, click the **Add** button.



Note: *A Jump Policy does not take effect until you have applied it to at least one Jump Client item.*

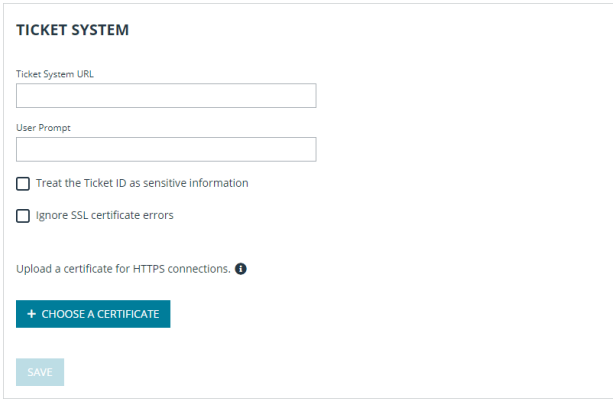
3. Enter a **Display Name**, **Code Name**, and **Description** in the corresponding locations to enable you to effectively apply this Jump Policy appropriate to your purposes after its creation.
4. Optionally, complete the configuration for **Jump Schedule** and **Jump Notification** if appropriate for the access control desired on this Jump Policy.
5. In the **Jump Approval** section, check **Require a ticket ID before a session starts**. To instantly disable ticket ID approval on this policy, simply uncheck this box. If ticket ID approval is enabled on a policy that does not have a ticket system URL configured, users attempting to access a Jump Item to which the policy is applied receive a message to contact the administrator.
6. Optionally, complete any additional approval configuration you wish this Jump Policy to enforce.
7. Click **Save**.



Connect External Ticket ID System to Jump Policies

Next, connect your existing ITSM or ticket ID system to the B Series Appliance.

1. Remain in your BeyondTrust /login administrative interface on the **Jump > Jump Policies** page.
2. At the bottom of the **Jump Policies** page, locate the **Ticket System** section.



3. In **Ticket System URL**, enter the URL for your external ticket system. The B Series Appliance sends an outbound request to your external ticketing system. The URL must be formatted for either HTTP or HTTPS. If an HTTPS URL is entered, the site certificate must be verified for a valid connection. If a Jump Policy requiring a ticket ID exists, a ticket system URL must be entered or you will receive a warning message.
4. The **Current Status** field is shown only when a valid status value exists to report the connection to the ticket system configured in **Ticket System URL**. Any ticket system configuration change resets the value.
5. Click **Choose a certificate** to upload the certificate for the HTTPS ticket system connection to the B Series Appliance. If your certificate is uploaded, the B Series Appliance uses it when it contacts the external system. If you do not upload a certificate and the **Ignore SSL certificate errors** box below this setting is checked, the B Series Appliance optionally falls back to use the built-in certificate store when sending the request.

> ***Note:** When the **Ignore SSL certificate errors** box is checked, the B Series Appliance will not include the certificate validation information when it contacts your external ticket system.*

6. In **User Prompt**, enter the dialog text you want access console users to see when they are requested to enter the ticket ID required for access.

7. If your company's security policies consider ticket ID information as sensitive material, check the **Treat the Ticket ID as sensitive information** box.

   If this box is checked, the ticket ID is considered sensitive information and asterisks are shown instead of text. You must use an HTTPS Ticket System URL. If an address with HTTP is entered, an error message appears to remind you HTTPS is required.

   When this feature is enabled you cannot bypass issues with SSL certificates by checking the **Ignore SSL certificate errors** box. This means you must have a valid SSL certificate in place. If you try to check the **Ignore SSL certificate errors** box, a message appears stating that you cannot ignore SSL certificate errors.

   When the Ticket ID is sensitive, the following rules apply:

   - Both the desktop and the web access consoles show asterisks instead of text.
   - The ticket is not logged anywhere by the access console or on the B Series Appliance.

8. Click **Save**.

API Approval Request

BeyondTrust PRA sends an HTTP Post request to the ticketing system URL. The POST request contains the following key-value pairs:

request_id	Unique ID that identifies the approval request. ***Note:*** *The request ID must be sent from the external ticketing system to BeyondTrust PRA in the response. The maximum length is 255 characters, and the ticketing system must treat the request ID as an opaque value.*
ticket_id	ticket ID entered by the user.
response_url	URL to which the integration should POST its reponse.
jump_item.computer_name	Hostname or IP address of the endpoint the user is requesting access for.
jump_item.type	Type of Jump Item being accessed: • client (for Jump Clients) • shell (for Shell Jump Shortcuts) • rdp • vnc • push_and_start (for Remote Jump and Local Jump) • vpro
jump_item.comments	Comments noted about the Jump Item.
jump_item.group	Group associated of the Jump Item.
jump_item.tag	Tags associated with the Jump Item.
jump_item.jumpoint_name	Name of the Jumpoint.
jump_item.public_ip	Public IP address of the Jump Item.

	Note: *This is not provided for Jumpoints.*
jump_item.private_ip	Private IP address of the Jump Item. **Note:** *This is not provided for Jumpoints.*
jump_item.custom.<code>	Key-value pair designated for the Jump Item custom field. **Note:** *Only one key-value pair is permitted for each Jump Item custom field.*
user.id	The requesting user's unique ID.
user.username	Username used by the requesting user for authentication.
user.public_display_name	The requesting user's public display name.
user.private_display_name	The requesting user's private display name.
user.email_address	Email address listed for the requesting user.

API Approval Response

The external ticketing system sends an HTTP POST request to the B Series Appliance URL at https://example.beyondtrust.com/api/endpoint_approval.

Note: *The API must be accessed over HTTPS.*

The POST request can contain the following key-value pairs in the POST body:

response_id	Request ID sent in the approval request. *Required
response	Response to the request; either allow or deny. *Required
message	Message displayed to the requesting user if the request is denied. *Optional **Note:** *The maximum length set for the message is 255 characters.*
session.custom.<code name>	One or more custom session attributes set for the access session. *Optional

Error Messages

In certain circumstances, an error message displays in the **Ticket System** section:

- *Ticket System URL is required because one or more Jump Policies still require a ticket ID.* - A Jump Policy exists requiring the entry of a ticket ID for access.
- *Invalid ticket ID.* - The external ticket system explicitly denied the request. If the external ticket system sends the error message, that message is shown.
- *The Ticket System URL must start with "https://" when the Ticket ID is sensitive.* - You must enter an HTTPS URL when **Treat the Ticket ID as sensitive information** is checked.
- *Cannot ignore SSL errors when the Ticket ID is sensitive*. - When this option is checked, you cannot ignore SSL errors and must provide a valid SSL certificate.
- *The given host was not resolved.* - An invalid ticket system URL was attempted.
- *The ticket system failed to respond in time.* - The external ticket system failed to respond in a timely manner.

Users who are unable to connect due to misconfiguration or user error will see explanatory pop-up messages in the access console for the error state of the configuration.

- *No ticket system URL is configured. Please contact your administrator* - A ticket ID system URL is not configured in the /login administrative interface.
- *User Prompt Not Configured.* - The User Prompt is not configured in the /login administrative interface.
- *The ticket system returned an invalid response.* - An invalid ticket ID was entered.

The following errors can be returned by the B Series Appliance:

404	Returned when no ticketing system URL is configured in /login
403	Returned when the request_id is not valid ***Note:*** *This error message is received when the request has timed out.*

Appendix: Jump Client Error Messages

This appendix provides a reference for error messages that may occur while working with Jump Clients. Below is a list of actions that may take place with Jump Clients along with error messages that may occur during each action. Each error message is accompanied by a brief description.

Action	Error Message	Explanation and Reproduction Notes
Deploying a Jump Client from the Mass Deployment Wizard	The total number of deployable Jump Clients for this site has been reached.	The build limit has been reached.
	The total number of deployable active Jump Clients for this site has been reached.	The build limit has been reached.
	The associated Jumpoint is not currently online.	The Jumpoint designated as the Jumpoint Proxy is offline before mass deployment is generated.
	The associated Jumpoint-proxy no longer exists.	The Jumpoint designated as the Jumpoint Proxy is deleted before mass deployment is generated.
Taking an Action on a Jump Client besides Jumping (Set Comments, etc.)	The Jump Client does not exist.	Race condition: A Jump Client has been deleted, but another access console has attempted to Jump to that Jump Client before being notified.
	The Jump Client is offline.	Race condition: A Jump Client has gone offline, but an access console has attempted to Jump to that Jump Client before being notified.
	The specified Jump Client has been uninstalled.	Race condition: A Jump Client has been uninstalled, but an access console has attempted to Jump to that Jump Client before being notified.
Jumping	Permission denied joining existing access session.	Simultaneous user access to a Jump Client is disabled while Jumping into a Jump Client which already has a session. This permission is controlled by the **Allow simultaneous user access to a single Jump Client** setting under **/login > Jump > Jump Clients :: Jump Client Settings**.
	The server is currently too busy. Please try again later.	More than twenty users are starting sessions at the same time on different Jump Clients.
	An internal error occurred while spawning the access session.	Internal for active Jump Client starts.
	An internal operation was taking too long while trying to spawn a access session.	Internal for active Jump Client starts.
	The active Jump Client is not connected.	Race condition: An active Jump Client disconnected before the access console was notified.
	Timeout while trying to connect to the Jump Client.	Took too long to connect to any of the hostnames or IPs.
	The Jump Client identification check failed. This	The server was able to connect and handshake, but

Action	Error Message	Explanation and Reproduction Notes
	may indicate that a new system has obtained the network address of the Jump Client you are attempting to access.	the Jump Client gave the wrong identification token, meaning that it is not the Jump Client you are attempting to reach or that the Jump Client has lost its token.
	The Jump Client has been disabled by the user and will not allow a session to start at this time.	The Jump Client has been disabled on the remote computer.
	The Jump Client is running a different version and will not attempt to upgrade. Please try again after the upgrade completes.	BeyondTrust version mismatch. This should cause a check-in, which causes an upgrade.
	The Jump Client does not exist.	Race condition: A Jump Client has been deleted, but another access console has attempted to Jump to that Jump Client before being notified.
	The Jump Client is offline.	Race condition: A Jump Client has gone offline, but an access console has attempted to Jump to that Jump Client before being notified.
	The specified Jump Client has been uninstalled.	Race condition: A Jump Client has been uninstalled, but an access console has attempted to Jump to that Jump Client before being notified.

IMPORTANT!

When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.