Remote Support
Jump Client Guide
Table of Contents

Recommended Steps for Implementing BeyondTrust Jump Technology ......................  4
Use Jump Item Roles to Create Permission Sets for Jump Clients ..........................  5
Set Jump Client Pinning and Unpinning Permissions .............................................  6
Create Jump Policies to Apply to Jump Clients ..................................................  10
   Create a Jump Policy ......................................................................................... 10
Use Jump Groups to Determine Which Users Can Access Which Jump Clients ........... 11
Deploy Jump Clients During a Support Session or Prior to Support ......................... 12
   During a Support Session .................................................................................. 12
   Prior to Support ................................................................................................. 13
Installation on Windows, Linux, or Mac Systems ..................................................... 16
Installing a Linux Jump Client in Service Mode ..................................................... 18
Installation on Headless Linux Systems ................................................................. 19
   Use Jump Clients to Access Unattended Android Devices ................................. 20
Pin an Android Jump Client from the Representative Console ............................. 21
   Email a Link from the /login Interface to Install and Android Jump Client .......... 22
Configure Jump Client Settings .............................................................................. 23
   Active vs. Passive Jump Clients ....................................................................... 24
Start a Support Session through a Jump Client ...................................................... 27
   From the Representative Console .................................................................... 27
   From the API .................................................................................................... 29
Use Cases for Jump Client Implementation ............................................................ 32
   Basic Use Case ................................................................................................. 32
   Advanced Use Case ......................................................................................... 34
Appendix: Jump Client Error Message Reference .................................................... 39

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. Because BeyondTrust Remote Support is licensed per active representative and not per remote system, Jump Technology is a cost-effective way to reach every device in your enterprise.

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 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.

BeyondTrust Jump Clients are not limited by license count; instead, they are limited by hardware as described below.

<table>
<thead>
<tr>
<th>Appliance Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>B200</td>
</tr>
<tr>
<td>Up to 1,000 Active Jump Clients</td>
</tr>
<tr>
<td>Up to 50,000 Passive Jump Clients</td>
</tr>
</tbody>
</table>

If more Jump Clients are needed, contact BeyondTrust Technical Support.
Recommended Steps for Implementing BeyondTrust 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 Create Permission Sets for Jump Clients" on page 5.

2. **Add Jump Policies.** Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules. Jump Policies are applied to Jump Items upon creation and can be modified from the representative console.

   - For more information about Jump Policies, please see "Create Jump Policies to Apply to Jump Clients" on page 10.

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 Determine Which Users Can Access Which Jump Clients" on page 11.

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 or from the representative console during a customer-initiated session. When creating the installer in the mass deployment wizard or during a session, 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 During a Support Session or Prior to Support" on page 12.
Use Jump Item Roles to Create 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 from the Jump > Jump Item Roles 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 Item Roles 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, 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 Start Sessions, Edit Tag, Edit Comments, Edit Public Portal, Edit Jump Policy, Edit Session Policy, Edit Connectivity and Authentication, and Edit Behavior and Experience. Click the blue info icons next to the last three options to see exactly what is affected by these fields.

Under Jump Clients Only, choose if users can set passwords on Jump Clients. Also choose if they can access password-protected Jump Clients without needing to know the password.
Set Jump Client Pinning and Unpinning Permissions

Allow Users to Pin Jump Clients

Permission to deploy, remove, and modify Jump Items always grants the user permission to download and install Jump Clients prior to support as described in "Deploy Jump Clients During a Support Session or Prior to Support" on page 12. However, this does not necessarily mean that the user has permission to pin Jump Clients during a support session. To pin a Jump Client during a support session, the user must have the permission **Jump Clients Pinning/Unpinning**. This permission can be defined in any of the following locations in /login:

- Users & Security > Users
- Users & Security > Group Policies
- Users & Security > Session Policies

If you need to assign the permission to only one or two users, do so from the Users page.

If you need to assign the permission to one or two groups of users, do so from the Group Policies page.

If you need to assign the permission to three or more groups of users, to specific Jump Clients, or to one or more of your public portals, do so from the Session Policies page.

Regardless of where you set this permission, the configuration works the same. Locate the **Jump Clients Pinning/Unpinning** permission and select Allow.

**Note:** Selecting Deny prevents pinning/unpinning of Jump Clients. Selecting **Not Defined** falls back to a lower priority session policy or the global session policy.

If you allow this permission for a specific user on the Users page, then that user can pin/unpin any session they start.

If you allow this permission for a specific Group Policy, then any members of that group can pin/unpin any session they start.

However, if you allow this permission for a specific Session Policy, no change occurs until you assign this policy to one or more users, group policies, Jump Items, or public portals.

Assign a Session Policy to a User or Group

To assign a session policy to a user account, group policy, or public portal, set the **Availability** of the session policy to allow **Users**.

**Note:** Making the pin/unpin permission available to rep invite is meaningless. External representatives cannot have ownership of sessions, and only the owner of a session can pin/unpin Jump Clients.
To assign a session policy to a user or group policy, edit the user or group, scroll down to the **Attended and Unattended Session Permissions** section, and select the session policy you want from the dropdown.

### Assign a Session Policy to a Public Portal

Public portals allow you to assign additional DNS hostnames to your Secure Remote Access Appliance and specify a different look and feel for each one, along with different behavior and permissions. You can define public portals on the `/login > Public Portals > Public Sites` page.

If you allow pinning/unpinning for a public portal, then all sessions started through that portal allow the representative to pin/unpin, regardless of any permissions assigned to the representative's user account or group policy.

To assign a session policy to a public portal:

1. Go to `/login > Public Portals > Customer Client.`
2. At the top of the page, check the **Select a different public site to edit** dropdown to make sure you have the desired portal selected.
3. Under **Session Policy**, use the dropdown to select a policy.
Assign a Session Policy to a Jump Item

To assign a session policy to a Jump Item, set the Availability of the session policy to allow Jump Items. While Jump Items include more than just Jump Clients, the pin/unpin permission applies only to Jump Clients.

When a session policy which allows pinning/unpinning is assigned to a Jump Client, then any user who starts a session with that Jump Client can unpin it, even if that user is denied permission to unpin Jump Clients in all other sessions.

To assign a session policy to a Jump Client, the user must have permission to change the session policies associated with Jump Items. This is determined by Jump Item Role.

When a user has this permission, they can right-click any Jump Client they are allowed to modify, click Properties, and assign a session policy to the Jump Client using the Customer Present Session Policy and Customer Not Present Session Policy dropdowns.

**Note:** The way customer presence is determined is set by Use screen state to detect customer presence on the /login > Jump > Jump Clients page under Jump Client Settings. If checked, the customer is determined to be present only if a user is logged in, the screen is not locked, and a screen saver is not running. If unchecked, the customer is considered present if a user is logged in, regardless of screen state.

Troubleshoot Settings with the Session Policy Simulator

If a specific user is unable to pin/unpin Jump Clients during a session, you can use the session policy simulator to troubleshoot the issue.

1. Log into /login as an admin and go to Users & Security > Session Policies.
2. Scroll to the Session Policy Simulator section and enter the Representative and Session Start Method in question.
3. Click the Simulate button and check the result for the permission Jump Clients Pinning/Unpinning.
If the simulator indicates that the user should be able to pin/unpin for a given session, and yet in practice this is not the case, then verify that the user has permission to modify Jump Clients:

1. Log into /login as an admin and go to Users & Security > Users.
2. Edit the user in question and locate their Jump Group Memberships.
   a. If a Jump Group specifies a specific Jump Item Role for the user, click on the role to see its settings. If the role is set on the user, scroll down to the user account's Jump Technology section and click Show for the associated Jump Item Roles.
   b. At least one of the associated Jump Item Roles should give the user permission to Create and deploy new Jump Items or Remove existing Jump Items.
3. If a Jump Group Membership is defined by a group policy and/or if the Jump Item Roles are not editable, then modify the group policy which is controlling these memberships and/or permissions.
   a. There may be multiple policies involved, so you may need to check each one.
   b. If the same permission is defined in multiple policies, you may need to reorder them or change the option Allow this policy to be overridden? for Add To Jump Groups, Remove From Jump Groups, or Representative Permissions.
   c. If you reorder policies or allow override, remember that a group policy listed further down in the list of policies overrides policies further up in the list only when the permission in question allows override on the first/topmost group policy; otherwise, the first group policy takes precedence.
Create Jump Policies to Apply to Jump Clients

To control access to particular Jump Clients, create Jump Policies. Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules.

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, one is created automatically.
5. Add a brief description to summarize the purpose of this policy.
6. If you want to enforce an access schedule, check Enabled. 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 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 when schedule does not permit access. 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.
7. When you are finished configuring this Jump Policy, click Save.

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

For more information, please see "Deploy Jump Clients During a Support Session or Prior to Support" on page 12.
Use Jump Groups to Determine 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 from this page or from the Users & Security > Group Policies page.

Create or edit a Jump Group, assigning it a name, code name, and comments. The Group Policies section lists any group policies which 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 Role as set on the Users & Security > Group Policies page or the Users & Security > Users page. A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage.

Existing Jump Group users are shown in a table, along with their assigned role and information who grants that role. You can filter the view by entering a string in the Filter by name text box. You can also edit a user's settings or delete a 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: You may see some users whose Edit and Delete options are disabled. 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. 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 can also add the individual to the group, overriding their settings as defined elsewhere.
Deploy Jump Clients During a Support Session or Prior to Support

There are two ways to install a Jump Client. During a BeyondTrust support session, a Jump Client can be installed ad-hoc by the representative. Alternatively, an administrator can mass-deploy Jump Clients for a larger rollout. These two methods of installation are outlined below.

During a Support Session

A Jump Client may be installed ad-hoc during a support session. This allows the support representative to access this computer at a later time, even if the computer is unattended. This method of installation is also known as session pinning and is achieved by clicking the Pin as Jump Client button.

**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:** Support representatives can access unattended Android devices through session pinning. To learn more, please see [Initiate an Android Support Session](https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-support.htm).

1. From within a support session, click the Pin as Jump Client button in the session toolbar at the top right corner of the representative console.
2. From the dropdown, you may select to customize the Jump Client before deploying it.
   a. Enter a Name for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
   b. Change a Jump Client's mode from the Connection Type dropdown. Active Jump Clients send statistics to the Secure Remote Access Appliance on a defined interval. Passive Jump Clients send statistics to the Secure Remote Access Appliance once a day or upon a manual check-in. Based on the options your administrator sets, these statistics may include the remote computer's logged-in console user, operating system, uptime, CPU, disk usage, and a screen shot from the last update.
   c. Once a Jump Client has a password set, its icon shows that it is locked, and its screen shot is also locked. In order to Jump to a locked Jump Client, you must provide its password. Also, you must provide the password to remove a locked Jump Client via the Jump Client interface; you do not need the password to unpin from within a session, as you would already have provided the password to Jump into the session.
   d. If Starts Quietly is checked, the customer client does not take focus and remains minimized in the taskbar or dock when a session is started.
   e. You also have the option to set when the Jump Client expires. This can be never, at a specific time and date, or after a certain length of time. An expired Jump Client automatically uninstalls from the remote system and is removed from the list in the Jump Client interface.
   f. 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.
g. 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 is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.

h. Select the Public Portal through which this Jump Item should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Item. The ability to set the public portal depends on your account permissions.

i. Jump Items include a Comments field for a name or description, which makes sorting, searching, and identifying Jump Items faster and easier.

j. To set when users are allowed to access this Jump Item, choose a Jump Policy. These policies are configured by your administrator in the /login interface.

k. Choose session policies to assign to this Jump Item. Session policies assigned to this Jump Item have the highest priority when setting session permissions. The Customer Present Session Policy applies when the end user is determined to be present. Otherwise, the Customer Not Present Session Policy applies. The way customer presence is determined is set by the Use screen state to detect Customer Presence Jump Item setting in the /login interface. When enabled, a customer is considered present only if a user is logged in, the system is not locked, and a screensaver is not running. When disabled, a customer is considered present if a user is logged in, regardless of the screen state. Customer presence is detected when the Jump Item session starts. The session policy used for the session does not change throughout the session, regardless of any changes in the customer's presence while the session is in progress. The ability to set a session policy depends on your account permissions.

3. Alternatively, you can simply select a Jump Group to which to pin the Jump Client, not setting any properties. From the 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. Depending on the session permissions, the customer may receive a message that you are requesting to install a Jump Client. The customer is asked to allow or refuse the request.

5. Once the Jump Client is installed, the remote computer appears in the Jump interface of the representative console. You may have to refresh the interface to see the new Jump Client.

Prior to Support

Jump Clients can be pre-installed 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 which 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.

1. From the /login administrative interface, go to Jump > Jump Clients.
2. From the 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. Select the Public Portal through which this Jump Client should connect. If a session policy is assigned to this public portal, that policy may affect the permissions allowed in sessions started through this Jump Client.

4. Choose session policies to assign to this Jump Client. Session policies assigned to this Jump Client have the highest priority when setting session permissions. The Customer Present Session Policy applies when the end user is determined to be present. Otherwise, the Customer Not Present Session Policy applies. The way customer presence is determined is set by the Use screen state to detect Customer Presence Jump Client setting. Customer presence is detected when the Jump Client session starts. The session policy used for the session does not change throughout the session, regardless of any changes in the customer's presence while the session is in progress.

5. 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. If no Jump Policy is applied, this Jump Client can be accessed at any time.

6. Adding a Tag helps to organize your Jump Clients into categories within the representative console.

7. Set the Connection Type to Active or Passive for the Jump Clients being deployed.

For more information on active versus passive Jump Clients, please see "Active vs. Passive Jump Clients" on page 24.

8. 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 Secure Remote Access Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.

For more information on setting up Jumpoints as proxies, please see the Jumpoint Guide at www.beyondtrust.com/docs/remote-support/how-to/jumpoint.

9. 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.

10. 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 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 Secure Remote Access 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 appliance, invalidate the Jump Client installers from before the upgrade. If these installers are MSI packages, they can still be used to uninstall Jump Clients if necessary.
Once a Jump Client has been installed, it remains online and active until it is uninstalled from the local system either by a logged-in user, by a representative from the representative console’s Jump interface, or by an uninstall script. A representative cannot remove a Jump Client unless the representative is given appropriate permissions by their admin from the /login interface.

11. 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.png)
   
   **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.png)
   
   **Note:** This option does not apply to headless Linux Jump Clients.

12. 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.png)
   
   **Note:** This option does not apply to headless Linux Jump Clients.

13. By selecting **Start Customer Client Minimized When Session Is Started**, the customer client does not take focus and remains minimized in the taskbar or dock when a session is started through one of these Jump Clients.

   ![](Note.png)
   
   **Note:** This option does not apply to headless Linux Jump Clients.

14. You can also set a **Password** for these Jump Clients. If a password is set, this password must be provided to modify or use any one of these Jump Clients.

15. 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. 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. Once the installer has run, the Jump Client attempts to connect to the appliance. When it succeeds, the Jump Client appears in the Jump interface of the representative console. If the Jump Client cannot immediately reach the 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.
Installation on Windows, Linux, or Mac Systems

**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:**

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

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

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

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.

You can also override certain installation parameters specific to your needs. These parameters can be specified for both the MSI and the EXE using a systems administration tool or the command line interface. 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.

<table>
<thead>
<tr>
<th>Command Line Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-install-dir</code></td>
<td><code>&lt;directory_path&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-jc-name</code></td>
<td><code>&lt;name...&gt;</code></td>
<td>If override is allowed, this command line parameter sets the Jump Client's name.</td>
</tr>
<tr>
<td><code>-jc-jump-group</code></td>
<td><code>user:&lt;username&gt; jumpgroup:&lt;jumpgroup-code-name&gt;</code></td>
<td>If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.</td>
</tr>
<tr>
<td><code>-jc-public-site-address</code></td>
<td><code>&lt;public-site-address-hostname&gt;</code></td>
<td>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 reverts to using the default public site.</td>
</tr>
</tbody>
</table>
### Session Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--jc-session-policy-present &lt;session-policy-code-name&gt;</td>
<td>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 present at the console.</td>
</tr>
<tr>
<td>--jc-session-policy-not-present &lt;session-policy-code-name&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>--jc-jump-policy &lt;jump-policy-code-name&gt;</td>
<td>If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.</td>
</tr>
<tr>
<td>--jc-tag &lt;tag-name&gt;</td>
<td>If override is allowed, this command line parameter sets the Jump Client's tag.</td>
</tr>
<tr>
<td>--jc-comments &lt;comments ... &gt;</td>
<td>If override is allowed, this command line parameter sets the Jump Client's comments.</td>
</tr>
<tr>
<td>--silent</td>
<td>If included, the installer shows no windows, spinners, errors, or other visible alerts.</td>
</tr>
</tbody>
</table>

**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-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhzefggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

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

- Adding dashes
- Add a space between the parameter and the value instead of an equal sign

**EXE Example:**

```
bomgar-scc-[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.
Installing a Linux Jump Client in Service Mode

In BeyondTrust Remote Support 15.2.1 and above, 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 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 representative console, right click the existing user mode Jump Client (if there is one), and 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 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.
Installation 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.
   a. 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.

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

b. 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.

```bash
sh ./bomgar-scc-{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.*

c. You can also override certain installation parameters specific to your needs. These parameters can be specified for both the MSI and the EXE using a systems administration tool or the command line interface. 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.

```bash
sh ./bomgar-scc-{uid}.bin --install-dir /home/username/jumpclient --jc-jump-group team:"Linux Admins" --jc-tag "Headless Linux Systems"
```

<table>
<thead>
<tr>
<th>Command Line Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--jc-jump-group</td>
<td>user:&lt;username&gt;</td>
<td>If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.</td>
</tr>
<tr>
<td></td>
<td>jumpgroup:&lt;jumpgroup-code-name&gt;</td>
<td></td>
</tr>
<tr>
<td>--jc-public-site-address</td>
<td>&lt;public-site-address-hostname&gt;</td>
<td>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 reverts to using the default public site.</td>
</tr>
</tbody>
</table>
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.

**IMPORTANT!**

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.

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

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

**Note:** Jump Clients installed in service mode are found in the `/Opt/bomgar/bomgar-scc-*` folder.

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

---

**Use Jump Clients to Access Unattended Android Devices**

Beginning with BeyondTrust 16.1, a persistent connection can be established with an Android device by pinning a Jump Client to the device. This provides the ability to have unattended support sessions with Android devices. You can deploy Jump Clients using either of the methods below.

**Note:** Bandwidth usage and battery life are minimally affected by establishing a persistent connection.
Persistent connections to an unattended Android device can occur only when the devices have both the BeyondTrust Support Client App 2.2.7 and BeyondTrust Jump Client App 2.2.0 installed from the Google Play Store. For more information, please see Download the BeyondTrust Support Client and BeyondTrust Jump Client Apps at https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-download-app.htm.

Pin an Android Jump Client from the Representative Console

1. While in a support session with the Android device, click on the Pin as Jump Client icon.

2. After pinning, click the Refresh option located above the Jump Items list, and the Android device will appear as a Jump Item in the Jump Item list. If the Pin a Jump Client icon is gray, the Android Jump Client has not been installed on the Android device.

3. Meanwhile, the BeyondTrust Jump Client app on the device should show the client as pinned with a date and timestamp.

**Note:** Options are available for the Jump Client to be disabled if the device is relying on battery power or on data to connect.
Email a Link from the /login Interface to Install and Android Jump Client

1. From the /login interface, navigate to Jump > Jump Clients > Jump Client Mass Deployment Wizard.

2. Complete the information needed for your Jump Client, such as Jump Group, Public Portal, etc.

3. Click Create.

4. From the Download or Install the Client Now section, choose Android as your platform.

5. Verify that the BeyondTrust Jump Client app is installed on the Android device. If not, navigate to the Google Play App store to download the app.

6. To download the Jump Client to the device, open a browser on the Android device and go to the URL provided by the mass deployment wizard.

Note: You can also email the URL to the Android device by clicking on the Email link located in the Deploy to Email Recipients section.
Configure Jump Client Settings

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

You may further regulate the bandwidth used during upgrades by setting **Maximum bandwidth of concurrent Jump Client upgrades**. The maximum upgrade bandwidth is 100 MIB/s.

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.

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. The maximum number allowed is 500.

---

**Note:** Neither of these settings affects representative console upgrades or Support Button deployments.

---

**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.*

**Global connection rate for Jump Clients** determines the maximum rate per second of Jump Clients able to connect to the appliance at the same time during an upgrade or after a major network outage. The default is 50 connections and the maximum allowed is 300.

**Restrict Local Uninstall/Disable of Jump Clients** limits the remote user’s ability to uninstall or disable Jump Clients from the right-click context menu, reducing the need to reinstall Jump Clients that should not have been uninstalled. If this option is enabled, only users with appropriate privileges on the target machine may uninstall the Jump Client via the host system's "uninstall programs" mechanism.

**Uninstalled Jump Client Behavior** determines how a Jump Client deleted by an end user is handled by the representative console. Depending on the option made in the dropdown, the deleted item can either be marked as uninstalled and kept in the list or actually be removed from the list of Jump items in the representative console. If the Jump Client cannot contact the Secure Remote Access Appliance at the time it is uninstalled, the affected item remains in its offline state.

**Allow Representatives 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.

Use screen state to detect Customer Presence sets how customer presence is determined. Customer presence is used when choosing whether to use the Customer Present Session Policy or the Customer Not Present Session Policy. If checked, the customer is determined to be present only if a user is logged in, the screen is not locked, and a screen saver is not running. If unchecked, the customer is considered present if a user is logged in, regardless of screen state.

With Jump Client Default Connection Type, set whether Jump Clients pinned during a customer-initiated session should by default be active or passive.

The Passive Jump Client Port specifies which port a passive Jump Client will use to listen for a "wake up" command from the appliance. The default port is 5832. Ensure that firewall settings allow inbound traffic on this port for your hosts with passive Jump Clients. Once awake, Jump Clients always connect to the appliance on port 80 or 443 outbound.

If a Jump Client goes offline and does not reconnect to the Secure Remote Access 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 representative 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 appliance, it uninstalls itself at the previously configured time.]

![Note: The setting must be configured for 15 days or more.]

If a Jump Client goes offline and does not reconnect to the Secure Remote Access Appliance for the number of days specified by the Number of days before Jump Clients that have not connected are considered lost setting, it is labeled as lost in the representative 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: The setting must be configured for 15 days or more.]

**Tip:** 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.

### Active vs. Passive Jump Clients

Jump Clients allow for one of two modes of behavior, active or passive. The default mode can be set from the Jump > Jump Clients page, and the mode can be switched from the Jump interface of the representative console.
A Jump Client in active mode maintains a persistent connection to the Secure Remote Access Appliance, waiting for session requests. It sends statistics updates as frequently as once per minute, as defined in the Jump Client Settings on the Jump > Jump Clients page.

A passive Jump Client does not maintain a connection to the appliance but rather listens for connection requests. It sends statistics updates only once per day or upon manual check-in. By setting Jump Clients to passive mode, you can have a larger number of deployed Jump Clients without markedly increasing the appliance load.

Note: If Console User is checked in Jump Clients > Jump Client Statistics, passive Jump Clients check in whenever they detect a new console user and report the user’s name.

In order to use a passive Jump Client, the appliance must be able to initiate contact with the computer on which the passive Jump Client is installed. This requirement may necessitate that you modify firewall rules to allow incoming connections to the target computer through the configured listen port. By default, this port is 5832; this can be modified from the Jump > Jump Clients page.

Passive mode may best be used on internal systems rather than external ones, although with correct firewall configurations, it may be used in either implementation. The following table presents key differences between the two modes.

<table>
<thead>
<tr>
<th>Active and Passive Jump Clients</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Jump Client</strong></td>
<td><strong>Passive Jump Client</strong></td>
</tr>
<tr>
<td>Maintains a persistent connection to the Secure Remote Access Appliance.</td>
<td>Listens for a remote access request from the Secure Remote Access Appliance.</td>
</tr>
<tr>
<td>Sends statistics to the Secure Remote Access Appliance at regular intervals.</td>
<td>Sends statistics to the Secure Remote Access Appliance once a day, upon manual check-in, or when a new user logs in (if this feature is enabled).</td>
</tr>
<tr>
<td>Enables remote access to any desktop operating system supported by BeyondTrust.</td>
<td>Enables remote access to any desktop operating system supported by BeyondTrust.</td>
</tr>
<tr>
<td>Number of installable clients is limited by your Secure Remote Access Appliance model.</td>
<td>50,000 passive Jump Clients supported on all Secure Remote Access Appliance models.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>B200</th>
<th>B300</th>
<th>B400</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 1,000 Active Jump Clients</td>
<td>Up to 10,000 Active Jump Clients</td>
<td>Up to 25,000 Active Jump Clients</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Appliance (S)</th>
<th>Virtual Appliance (M)</th>
<th>Virtual Appliance (L)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 1,000 Active Jump Clients</td>
<td>Up to 10,000 Active Jump Clients</td>
<td>Up to 25,000 Active Jump Clients</td>
</tr>
</tbody>
</table>

If you need more passive Jump Clients, contact technical support at www.beyondtrust.com/support.
The maximum number of Jump Clients available to a RS Virtual Appliance is based on allocated resources. For more information, please see the RS Virtual Appliance Sizing Guidelines at www.beyondtrust.com/docs/remote-support/getting-started/deployment/virtual/sizing.htm.
Start a Support 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 Representative 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, VNC sessions, RDP 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 at www.beyondtrust.com/docs/remote-support/how-to/jumpoint.
From the left pane, select the Jump Group for which you want to view pinned Jump Clients.

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 you are allowed to view Jump Clients in other users’ personal lists of Jump Items, those users appear in a second pane to the left.

If a Jump Group contains tagged Jump Clients, 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 Clients, 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.

If a Jump Client goes offline and does not reconnect to the Secure Remote Access Appliance for the number of days set by the Jump Client Settings in the /login interface, it is labeled as lost. No specific action is taken on the Jump Client. It is labeled as lost only for identification purposes, so that an administrator can diagnose the reason for the lost connection and take action to correct the situation. In the details pane, you will see the scheduled deletion date should the Jump Client not come back online.

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

---

**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
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 Client and click the **Remove** button, or right-click on the Jump Client and select **Remove** from the menu. You may select multiple Jump Clients 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 list of Jump Items in the representative console. This setting is available at **Login > Jump > Jump Clients.** If the Jump Client cannot contact the Secure Remote Access Appliance at the time it is uninstalled, the affected item remains in its offline state. If a Jump Client goes offline and does not reconnect to the Secure Remote Access 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**.

Jump Item properties are described in the section "Deploy Jump Clients During a Support Session or Prior to Support" on page 12.

**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 must use a BeyondTrust Representative
Console Script. A BRCS contains a sequence of commands to be executed by the representative console. Double-click a BRCS file to have it automatically executed by the representative console, or incorporate it into an external application to send commands to the representative console from that application.

One method of creating a BRCS is through the client scripting API. This API is located on your Secure Remote Access Appliance at https://support.example.com/api/client_script, where support.example.com is your BeyondTrust site hostname.

**Optional Parameters for the start_pinned_client_session Command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>search_string=[string]</td>
<td>If specified, then this is the search criteria used to select a Jump Client. The comments, hostname, private IP, public IP, and tag fields are matched against the search string. This field has a maximum length of 1024 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>client.comments</td>
<td>If specified, only Jump Clients with the given comments are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>client.hostname</td>
<td>If specified, only Jump Clients with the given hostname are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>client.private_ip</td>
<td>If specified, only Jump Clients with the given private IP address are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>client.public_ip</td>
<td>If specified, only Jump Clients with the given public IP address are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>client.tag</td>
<td>If specified, only Jump Clients with the given tag are included in the results. This field has a maximum length of 255 characters. Search is partial and case-insensitive.</td>
</tr>
<tr>
<td>session.custom.[custom field]=[string]</td>
<td>The code name and value of any custom fields. These fields must first be configured in /login &gt; Management &gt; 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.</td>
</tr>
</tbody>
</table>

**IMPORTANT!**

Either `search_string` or `client.*` parameters must be specified, but not both. It is an error to specify both the `search_string` and a `client.*` parameter. It is also an error to not specify either one.
**Query Examples: start_pinned_client_session**

<table>
<thead>
<tr>
<th>Description</th>
<th>API Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start a session with a Jump Client which has any field containing the string &quot;ABC&quot;</td>
<td><a href="https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;">https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;</a> action=start_pinned_client_session&amp;search_string=ABC</td>
</tr>
<tr>
<td>Start a session with a Jump Client whose hostname contains &quot;ABCDEF02&quot;</td>
<td><a href="https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;">https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;</a> action=start_pinned_client_session&amp;client.hostname=ABCDEF02</td>
</tr>
<tr>
<td>Start a session with a Jump Client whose comments contain &quot;maintenance&quot; and whose tag contains &quot;server&quot;</td>
<td><a href="https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;">https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;</a> action=start_pinned_client_session&amp;client.comments=maintenance&amp; client.tag=server</td>
</tr>
<tr>
<td>Start a session with a Jump Client whose private IP address begins with &quot;10.10.24&quot; and associate custom attributes with the session</td>
<td><a href="https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;">https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp;</a> action=start_pinned_client_session&amp;client.private_ip=10.10.24&amp; session.custom.custom_field1=Custom%20Value&amp;session.custom.custom_field2=123</td>
</tr>
</tbody>
</table>

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

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 representative console and start a session with a Jump Client.

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 representative console. Enter the name of your BeyondTrust representative console (e.g., bomgar-rep.exe), followed by one of two commands:

```
--run-script "action=start_pinned_client_session&search_string=[string]"
--run-script-file [path to BRCS file]
```

**Examples:**

```
bomgar-rep.exe --run-script "action=start_pinned_client_session&search_string=Example%20Co"
bomgar-rep.exe --run-script-file C:\Users\admin\Desktop\rep.script.brcs-support_example_co
```

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

For more information about BeyondTrust Representative Console Scripting, see the [API Guide](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api) at [www.beyondtrust.com/docs/remote-support/how-to/integrations/api](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api).
Use Cases for Jump Client Implementation

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.
   a. The Administrator role should have all permissions enabled.
   b. 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, Admins and Users.
4. In the **Admins** group, configure settings and permissions as appropriate. The permissions should include the following:

   a. Define **Representative Permissions** and enable **Allowed to provide remote support**.
   b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
   c. Under **Jump Item Roles**, set the **Default** and **Personal** roles to **Administrator**.
   d. Set the **Teams** and **System** roles to **Start Sessions Only**.
   e. Under **Memberships**, define **Add Jump Group Memberships**.
   f. In the **Jump Group** field, search for and select **Shared**.
   g. Set the **Jump Item Role** to **Administrator**.
   h. Click **Add** to assign the members of this group policy to the Jump Group.
   i. Save the group policy.

5. In the **Users** group, configure settings and permissions as appropriate. The permissions should include the following:

   a. Define **Representative Permissions** and check **Allowed to provide remote support**.
   b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
   c. Under **Jump Item Roles**, set the **Default** to **Start Sessions Only**.
   d. Set the **Personal** Jump Item Role to **Administrator**.
   e. Set the **Team** and **System** roles to **No Access**.
   f. Under **Memberships**, define **Add Jump Group Memberships**.
   g. In the **Jump Group** field, search for and select **Shared**.
   h. Set the **Jump Item Role** to **Start Sessions Only**.
   i. Click **Add** to assign the members of this group policy to the Jump Group.
   j. 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 on weekdays.

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

2. Create a Jump Policy, Weekdays.
3. In the Jump Policy, enable the **Jump Schedule**.
   a. Click **Add Schedule Entry**.
   b. Set the **Start** day and time to **Monday 8:00** and the **End** day and time to **Monday 17:00**.
   c. Click **Add Schedule Entry** and repeat the process for the remaining weekdays.
   d. Save the Jump Policy.

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

5. Put users into two group policies, **Admins** and **Users**.
6. In the **Admins** group, configure settings and permissions as appropriate. The permissions should include the following:

   a. Define **Representative Permissions** and enable **Allowed to provide remote support**.
   
   b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
   
   c. Under **Jump Item Roles**, set the **Default** and **Personal roles to Administrator**.
   
   d. Set the **Team** and **System roles to Start Sessions Only**.
   
   e. Under **Memberships**, define **Add Jump Group Memberships**.
   
   f. In the **Jump Group** field, search for and select **Web Servers**.
      i. Set the **Jump Item Role to Administrator**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   
   g. In the **Jump Group** field, search for and select **Directory Servers**.
      i. Set the **Jump Item Role to Administrator**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   
   h. In the **Jump Group** field, search for and select **User Systems**.
      i. Set the **Jump Item Role to Administrator**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   
   i. Save the group policy.
7. In the **Users** group, configure settings and permissions as appropriate. The permissions should include the following:
   a. **Define Representative Permissions** and check **Allowed to provide remote support**.
   b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
   c. Under **Jump Item Roles**, set the **Default** to **Start Sessions Only**.
   d. Set the **Personal Jump Item Role** to **Administrator**.
   e. Set the **Team** and **System** roles to **No Access**.
   f. Under **Memberships**, define **Add Jump Group Memberships**.
   g. In the **Jump Group** field, search for and select **Web Servers**.
      i. Set the Jump Item Role to **Start Session Only**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   h. In the **Jump Group** field, search for and select **Directory Servers**.
      i. Set the Jump Item Role to **Start Session Only**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   i. In the **Jump Group** field, search for and select **User Systems**.
      i. Set the Jump Item Role to **Start Session Only**.
      ii. Click **Add** to assign the members of this group policy to the Jump Group.
   j. Set the **Jump Item Role** to **Start Sessions Only**.
   k. Click **Add** to assign the members of this group policy to the Jump Group.
   l. Save the group policy.

8. Deploy Jump Items, assigning them to the three Jump Groups as appropriate. If any particular Jump Item requires a Jump Policy schedule to be enforced, assign that, as well.
9. 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. 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. They cannot deploy personal Jump Items.

Specified Jump Items can be accessed only on weekdays.
# Appendix: Jump Client Error Message Reference

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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Error Message</th>
<th>Explanation and Reproduction Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pinning a Jump Client from within a Session</td>
<td>The total number of deployable Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The total number of deployable active Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The total number of deployable passive Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The support session already has a pending request to pin.</td>
<td>Race condition (Reproduction is UI-limited).</td>
</tr>
<tr>
<td></td>
<td>The support client is already pinned.</td>
<td>Race condition (Reproduction is UI-limited).</td>
</tr>
<tr>
<td></td>
<td>No customer could be found within the support conference.</td>
<td>Race condition (Reproduction is UI-limited).</td>
</tr>
<tr>
<td></td>
<td>The customer within the support conference is not online.</td>
<td>Race condition (Reproduction is UI-limited).</td>
</tr>
<tr>
<td>Deploying a Jump Client from the Mass Deployment Wizard</td>
<td>The total number of deployable Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The total number of deployable active Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The total number of deployable passive Jump Clients for this site has been reached.</td>
<td>The build limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>The associated Jumpoint is not currently online.</td>
<td>The Jumpoint designated as the Jumpoint Proxy is offline before mass deployment is generated.</td>
</tr>
<tr>
<td></td>
<td>The associated Jumpoint-proxy no longer exists.</td>
<td>The Jumpoint designated as the Jumpoint Proxy is deleted before mass deployment is generated.</td>
</tr>
<tr>
<td></td>
<td>Bad Password: The password must contain at least ___ characters and contain at least one uppercase letter, one lowercase letter, one number, and one special character.</td>
<td>The password designated for the Jump Client does not meet security standards. (Reproduction is UI-limited.)</td>
</tr>
<tr>
<td></td>
<td>Bad Password: The password must contain at least ___ character(s).</td>
<td>The password designated for the Jump Client does not meet security standards. (Reproduction is UI-limited.)</td>
</tr>
<tr>
<td>Action</td>
<td>Error Message</td>
<td>Explanation and Reproduction Notes</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Taking an Action on a Jump Client besides Jumping (Set Comments, etc.)</td>
<td>The Jump Client does not exist.</td>
<td>Race condition: A Jump Client has been deleted, but another representative console has attempted to Jump to that Jump Client before being notified.</td>
</tr>
<tr>
<td></td>
<td>The Jump Client is offline.</td>
<td>Race condition: A Jump Client has gone offline, but an representative console has attempted to Jump to that Jump Client before being notified.</td>
</tr>
<tr>
<td></td>
<td>The specified Jump Client has been uninstalled.</td>
<td>Race condition: A Jump Client has been uninstalled, but an representative console has attempted to Jump to that Jump Client before being notified.</td>
</tr>
<tr>
<td></td>
<td>The password is incorrect.</td>
<td>The provided password is incorrect.</td>
</tr>
<tr>
<td></td>
<td>The number of active Jump Clients has been reached.</td>
<td>The build limit has been reached when changing from passive to active.</td>
</tr>
<tr>
<td></td>
<td>The number of passive Jump Clients has been reached.</td>
<td>The build limit has been reached when changing from active to passive.</td>
</tr>
<tr>
<td></td>
<td>Bad Password: The password must contain at least ____ characters and contain at least one uppercase letter, one lowercase letter, one number, and one special character.</td>
<td>The password designated for the Jump Client does not meet security standards.</td>
</tr>
<tr>
<td></td>
<td>Bad Password: The password must contain at least ____ character(s).</td>
<td>The password designated for the Jump Client does not meet security standards.</td>
</tr>
<tr>
<td>Jumping</td>
<td>Permission denied joining existing support session.</td>
<td>Simultaneous representative access to a Jump Client is disabled while Jumping into a Jump Client which already has a session. This permission is controlled by the <strong>Allow simultaneous representative access to a single Jump Client</strong> setting under /login &gt; Jump &gt; Jump Clients :: Jump Client Settings.</td>
</tr>
<tr>
<td></td>
<td>The server is currently too busy. Please try again later.</td>
<td>More than twenty users are starting sessions at the same time on different Jump Clients.</td>
</tr>
<tr>
<td></td>
<td>An internal error occurred while spawning the support session.</td>
<td>Internal for active Jump Client starts.</td>
</tr>
<tr>
<td></td>
<td>An internal operation was taking too long while trying to spawn a support session.</td>
<td>Internal for active Jump Client starts.</td>
</tr>
<tr>
<td></td>
<td>The active Jump Client is not connected.</td>
<td>Race condition: An active Jump Client disconnected before the representative console was notified.</td>
</tr>
<tr>
<td></td>
<td>Timeout while trying to connect to the Jump Client.</td>
<td>Took too long to connect to any of the hostnames or IPs.</td>
</tr>
<tr>
<td>Action</td>
<td>Error Message</td>
<td>Explanation and Reproduction Notes</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Failed to connect to the Jump Client.</td>
<td>Could not connect to any IP address or hostname of a passive Jump Client.</td>
<td></td>
</tr>
<tr>
<td>Timeout while communicating with the Jump Client.</td>
<td>Timeout during a passive connect handshake.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client sent a bad protocol version.</td>
<td>The Jump Client has informed the server of a protocol version error during a passive connect handshake.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client identification check failed. This may indicate that a new system has obtained the network address of the Jump Client you are attempting to access. Or, there is possibly more than one passive Jump Client deployed to the system, and only one of them can acquire the listen port (___) at a time.</td>
<td>The server was able to connect and handshake, but 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.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client has been disabled by the user and will not allow a session to start at this time.</td>
<td>The Jump Client has been disabled on the remote computer.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client is running a different version and will not attempt to upgrade. Please try again after the upgrade completes.</td>
<td>BeyondTrust version mismatch. This should cause a check-in, which causes an upgrade.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client does not exist.</td>
<td>Race condition: A Jump Client has been deleted, but another representative console has attempted to Jump to that Jump Client before being notified.</td>
<td></td>
</tr>
<tr>
<td>The Jump Client is offline.</td>
<td>Race condition: A Jump Client has gone offline, but an representative console has attempted to Jump to that Jump Client before being notified.</td>
<td></td>
</tr>
<tr>
<td>The specified Jump Client has been uninstalled.</td>
<td>Race condition: A Jump Client has been uninstalled, but an representative console has attempted to Jump to that Jump Client before being notified.</td>
<td></td>
</tr>
<tr>
<td>The password is incorrect.</td>
<td>The provided password is incorrect.</td>
<td></td>
</tr>
</tbody>
</table>

**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.*