BeyondTrust

Remote Support
Jump Client Guide

TC:3/4/2024

Table of Contents

Get Unattended Access to Systems with Remote Support Jump Client

With BeyondTrust Jump Technology, authorized users can securely access and control remote computers, attended and unattended, as well as switches and other network devices in any network. Jump Technology is integral to the BeyondTrust software offerings. All sessions are logged for reporting and auditing. 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 B Series Appliance, thus helping you reach systems on remote networks anywhere in the world. By preinstalling Jump Clients on remote systems, a user can establish sessions with unattended Windows, Mac, Linux, and Raspberry Pi computers.

System administrators can push the Jump Client installer to a large number of systems. The Windows, Mac, Linux, or Raspberry Pi executable, or the Windows MSI, can be used with your systems management tool of choice. You can override some installation parameters and include a valid custom install directory path where you want the Jump Client to install.

> *Some of the information in this guide is applicable to Jump Items. For more information about the differences between Jump Clients and Jump Items, and the use of other Jump technology terms, please refer to the Jump Technology Overview at https://www.beyondtrust.com/docs/remote-support/how-to/jump/index.htm.*

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

B Series Appliance Comparison

B200	B300	B400	Cloud
Up to 1,000 Active Jump Clients	Up to 10,000 Active Jump Clients	Up to 25,000 Active Jump Clients	Up to 150 Active Jump Clients per license

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

> *For RS Virtual Appliance, please see SRA Virtual Appliance Installation at https://www.beyondtrust.com/docs/remote-support/documents/infrastructure/sra-virtual-appliance-setup.pdf.*

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.

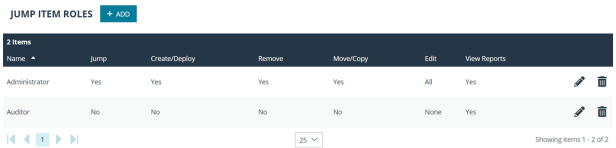
1. **Add Jump Item Roles.** Jump Item Roles determine how users are allowed to interact with Jump Items. These roles are applied to users by means of individual account settings, group policies, or when added to Jump Groups.
2. **Add Jump Policies.** Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules. Jump Policies are applied to Jump Items upon creation and can be modified from the representative console.
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.
4. **Deploy Jump Clients.** Jump Clients can be deployed to Windows, Mac, Linux, and Raspberry Pi systems. 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, please see the following:

- *"Use Jump Item Roles to Create Permission Sets for Jump Items" on page 6*
- *"Create Jump Policies to Apply to Jump Items" on page 13* .
- *"Use Jump Groups to Determine Which Users Can Access Which Jump Items" on page 11*
- *"Deploy Jump Clients During a Support Session or Prior to Support" on page 14*

Use Jump Item Roles to Create Permission Sets for Jump Items

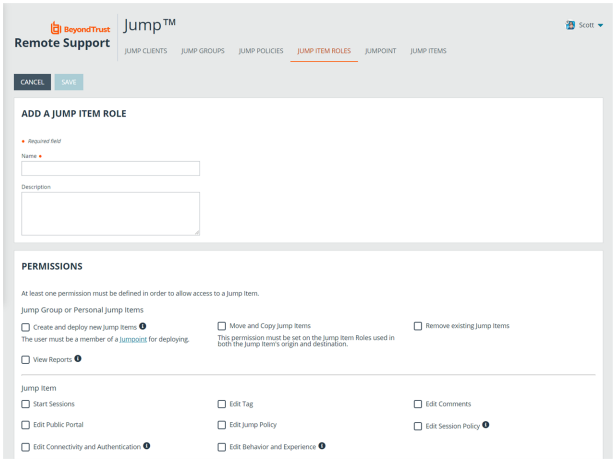
A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. Jump Item Roles are applied to users from the **Jump > Jump Item Roles** page or from the **Users & Security > Group Policies** page.



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

To create or edit a Jump Item Role, enter or update the name and description. Then set the permissions a user with this role should have:



1. 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.
2. Check the **Start Sessions** box to enable users to Jump to any Jump Items they have access to.
3. To allow users to edit **Jump Item** details, enable any of the options including:
    - **Start Sessions**
    - **Edit Tag**
    - **Edit Comments**
    - **Edit Public Portal**
    - **Edit Jump Policy**
    - **Edit Session Policy**
    - **Edit Connectivity and Authentication**
    - **Edit Behavior and Experience**.
    - Click the blue info icons next to the last three options to see exactly what is affected by these fields.

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 14. 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 three following locations in **/login**:

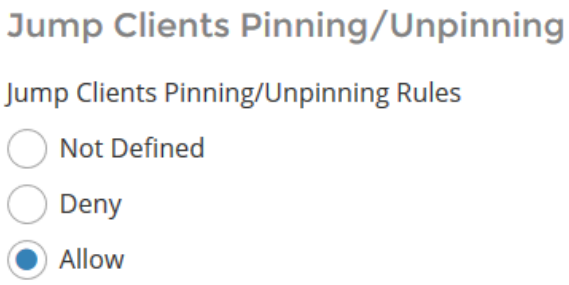
- **Users & Security > Users**
- **Users & Security > Group Policies**
- **Users & Security > Session Policies**

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 or unpinning 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 or unpin any session they start.

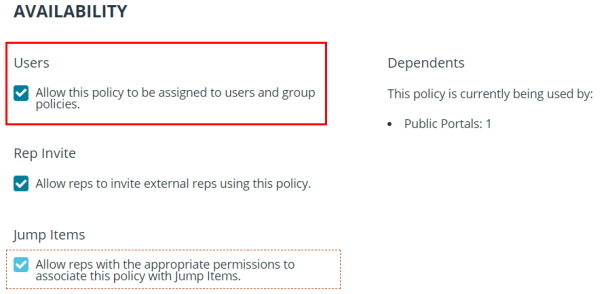
If you allow this permission for a specific **Group Policy**, then any members of that group can pin or unpin any session they start.

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.

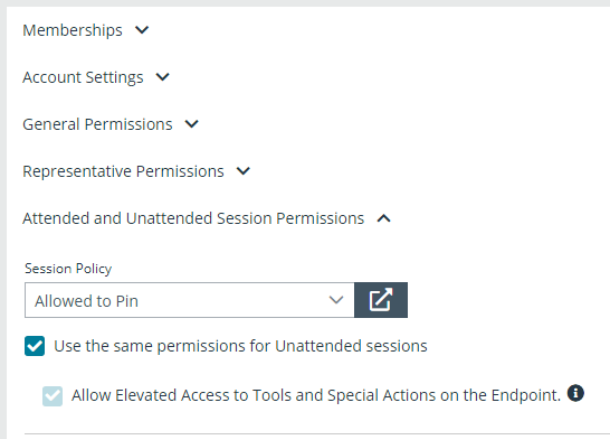
Assign a Session Policy to a User or Group

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 **Jump Clients Pinning/Unpinning** permission available to rep invite is meaningless. External representatives cannot have ownership of sessions, and only the owner of a session can pin or unpin Jump Clients.*

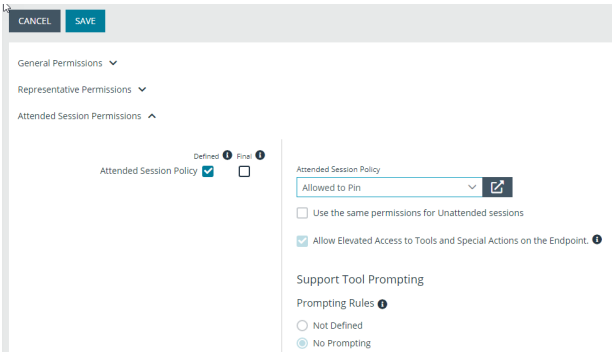


To assign a session policy to a user, edit the user, scroll down to the **Attended and Unattended Session Permissions** section, expand the section, and select the appropriate session policy from the dropdown. Click **Save**.



To assign a session policy for attended sessions to a group policy, edit the group policy, scroll down to the **Attended Session Permissions** section, and expand the section. Check **Defined**,and **Final** if applicable. From the **Attended Session Policy** dropdown, select **Custom** to define a policy and complete the options below, or select an existing policy. For an existing policy, the options can be viewed but not changed. Click **Save**.

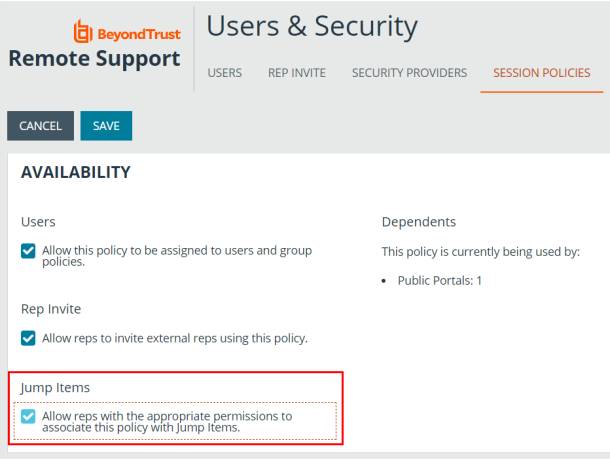
Follow the same process to assign a session policy for unattended sessions. Edit the group policy, scroll down to the **Unattended Session Permissions**, and expand the section. Check **Defined**,and **Final** if applicable. For the **Unattended Session Policy** dropdown, select **Custom** to define a policy and complete the options below, or select an existing policy. For an existing policy, the options can be viewed but not changed. Click **Save**. Click **Save**.



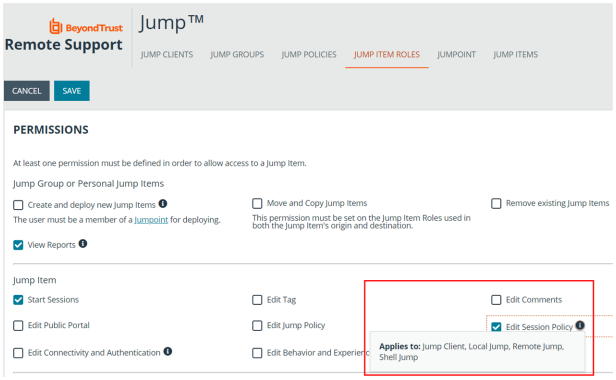
Assign a Session Policy to a Jump Item

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 Jump Clients, the pin or unpin permission applies only to Jump Clients.

When a session policy with the **Jump Clients Pinning/Unpinning** permission enabled 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.

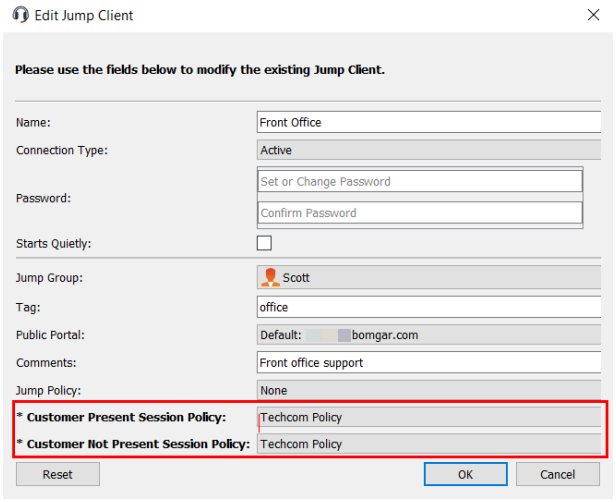


To assign a session policy to a Jump Client, the user must have permission to change the session policies associated with Jump Items. This is determined by Jump Item Role.



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 the option is enabled, 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 the option is disabled, 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 or unpin Jump Clients during a session, you can use the session policy simulator to troubleshoot the issue.

1. Log in to **/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 and 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:

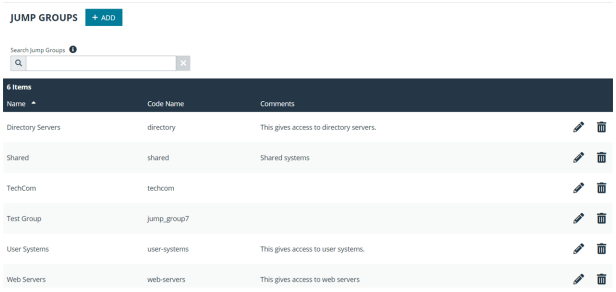
1. Log in to **/login** as an admin and go to **Users & Security > Users**.
2. Edit the user in question and locate their **Jump Group Memberships**.
    - If a Jump Group specifies a specific Jump Item Role for the user, click on the role to see its settings. If the role is set on the user, scroll down to the user account's **Jump Technology** section and click **Show** for the associated **Jump Item Roles**.
    - At least one of the associated Jump Item Roles must give the user permission to **Create and deploy new Jump Items**.

3. If a **Jump Group Membership** is defined by a group policy, or if the **Jump Item Roles** are not editable, or both, then modify the group policy which is controlling these memberships and/or permissions.
    - If multiple policies are involved, you might need to check each one.
    - If the same permission is defined in multiple policies, you might 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**.
    - If you reorder policies or allow override, remember that a group policy listed further down in the list of policies overrides policies above when the permission in question allows override on the topmost group policy; otherwise, the first group policy takes precedence.

Use Jump Groups to Determine Which Users Can Access Which Jump Items

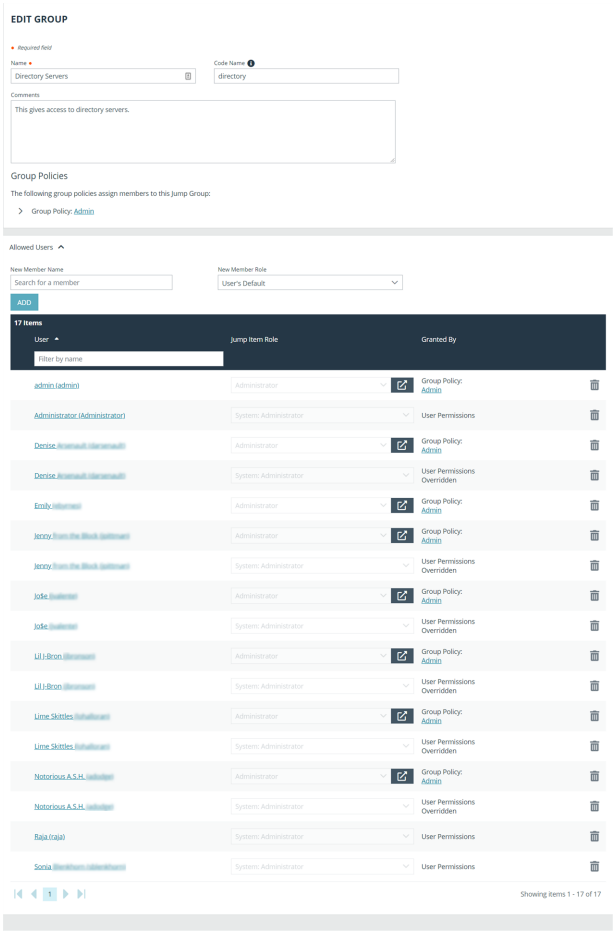
A Jump Group is a way to organize Jump Items, granting members varying levels of access to those items. Users are assigned to Jump Groups from this page or from the **Users & Security > Group Policies** page.

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 make 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 how the role was granted. 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: *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.

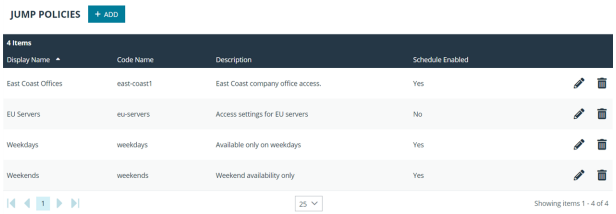
You also can add the individual to the group, overriding their settings as defined elsewhere.

Create Jump Policies to Apply to Jump Items

Jump Policies place additional conditions on access to particular Jump Items. Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules.

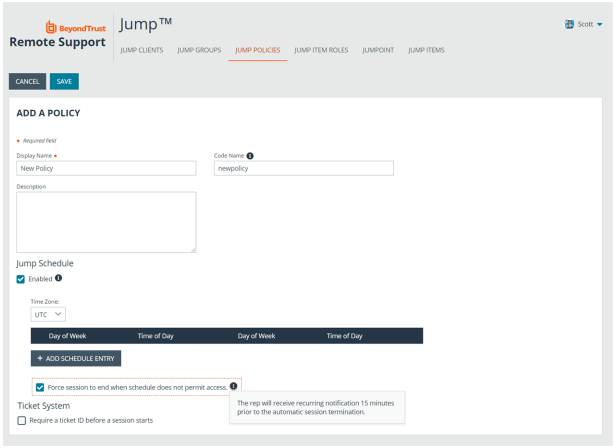
Create a Jump Policy

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. Use a name that clearly identifies 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 PM 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 the 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 14.*

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 as required by the representative.
- Alternatively, an administrator can mass-deploy Jump Clients for a larger rollout.

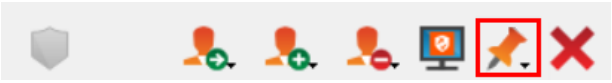
These two methods of installation are outlined below.

During a Support Session

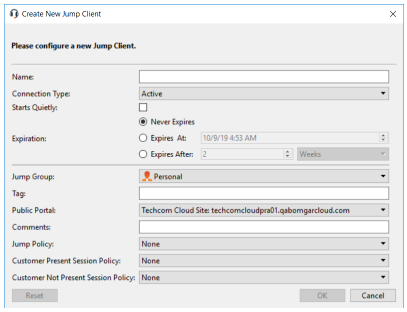
A Jump Client can be installed during a support session. This allows the support representative to access this computer at a later time, even if the computer is unattended. This method of installation is also known as *session pinning* and is achieved by clicking the **Pin as Jump Client** button.

> ***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.*

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 can select to customize the Jump Client before deploying it.



   - Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
   - 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.
   - 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.
   - 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 is pinned. To move a Jump Item back into its top-level Jump Group, leave this field blank.
   - 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.
   - 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, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

     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 screen saver 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 select a Jump Group to which to pin the Jump Client, not setting any properties. 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 (and higher ranking roles on your team, such as Team Lead and Team Manager if you are a Team Member, and Team Manager if you are a Team Lead) 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 could 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 might have to refresh the interface to see the new Jump Client.

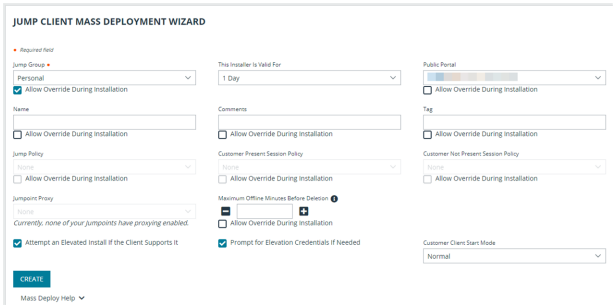
Support representatives can access unattended Android devices through session pinning. For more information, please see Initiate an Android Support Session at www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-support.htm.

Prior to Support

Jump Clients can be installed on remote computers in anticipation of the need for remote access. This method of installation can 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 enables 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 as the same user or more than one Jump Client as a service on the same system is being phased out in a future release. In the Representative 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 (and higher ranking roles on your team, such as Team Lead and Team Manager if you are a Team Member, and Team Manager if you are a Team Lead) 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. Select the **Public Portal** through which you want this Jump Client to 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.



5. 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.
6. You can 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.
7. Adding a **Tag** helps to organize your Jump Clients into categories within the representative console.
8. If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. As a result, if these Jump Clients are installed on computers without native Internet connections, they can use the Jumpoint to communicate with your B Series Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.
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 attempts 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 logged-in admin user with appropriate permissions, 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.

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.*

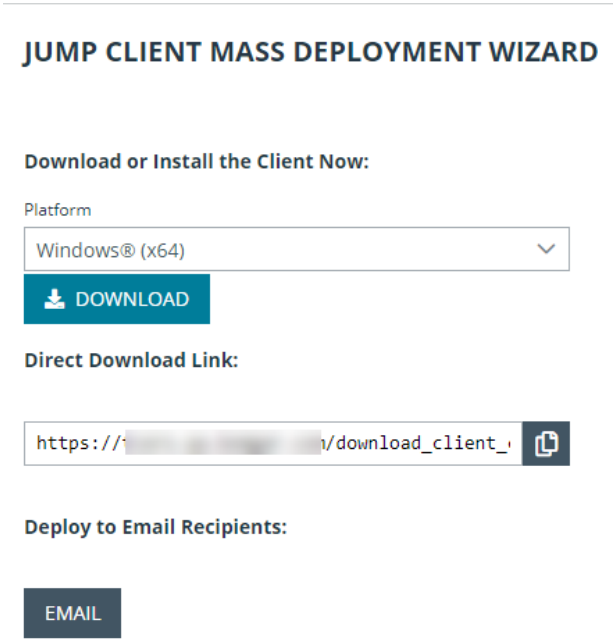
11. You can set the **Maximum Offline Minutes Before Deletion** of a Jump Client from the system. This setting overrides the global setting, if specified.
12. If **Prompt for Elevation Credentials if Needed** is selected, the installer prompts the user to enter administrative credentials if the system 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: *This option does not apply to headless Linux or Raspberry Pi Jump Clients.*

13. Select **Minimized** to start the customer client minimized. It does not take the focus, and appears only in the taskbar or dock when a session is started through this Jump Client.Select **Hidden** to start the customer client hidden. It does not take the focus, and appears only as an icon in the system tray when a session is started through this Jump Client.

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

14. 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. 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 representative 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 Jumpoint Guide at www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.

Install a Jump Client on a Windows System

Installation parameters can be specified for both the MSI and the EXE installers 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.

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 22**.*

Command Line Parameter	Value	Description
--install-dir	**<directory_path>**	Specifies a new writable directory under which to install the Jump Client. 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-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 host name as a site address. If no public portal has the given host name as a site address, then the Jump Client reverts to using the default public site.
--jc-session-policy-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 present at the console.
--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.

Command Line Parameter	Value	Description
--silent		If included, the installer shows no windows, spinners, errors, or other visible alerts.

Note: *If **--silent** is selected, run as Administrator must be used, otherwise the installation will fail as a prompt during installation does not display.*

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=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90
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 (--install-dir) but no dashes in the MSI version (installdir).*
- ***/quiet** is used for the MSI version in place of **--silent** in the EXE version.*

Tip: *A Jump Client can also be installed in service mode.*

Uninstall a Jump Client

To uninstall a Jump Client, remove it from the Representative Console.

If the client is not connected when it is removed from the console, the files are removed next time the client authorizes with the server.

Jump Clients can be removed from a device using a script. This will leave an entry in the Representative Console interface. The entry is automatically marked uninstalled or deleted, depending on your Jump Client Settings.

For information about Jump Client settings, please see "Configure Jump Client Settings" on page 47.

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\support.example.com:443\LastGood]
Proxy=DIRECT
[Proxy\support.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.*

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-scc.exe** processes running.
- The system has any **DisplayName** registry entries matching *BeyondTrust Remote Support 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.

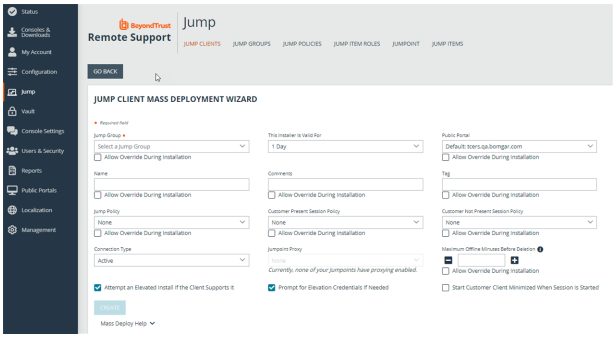
Use INSTALLDIR

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 **RSJumpClient.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 **RSJumpClient.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 "Install a Jump Client on a Windows System" on page 18.

Install a Jump Client on a Mac System

You can override certain installation parameters specific to your needs. These parameters can be specified 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.

> ***Note:*** *It is common to receive an error message during the install, regarding a layout or appearance issue. This can be disregarded.*

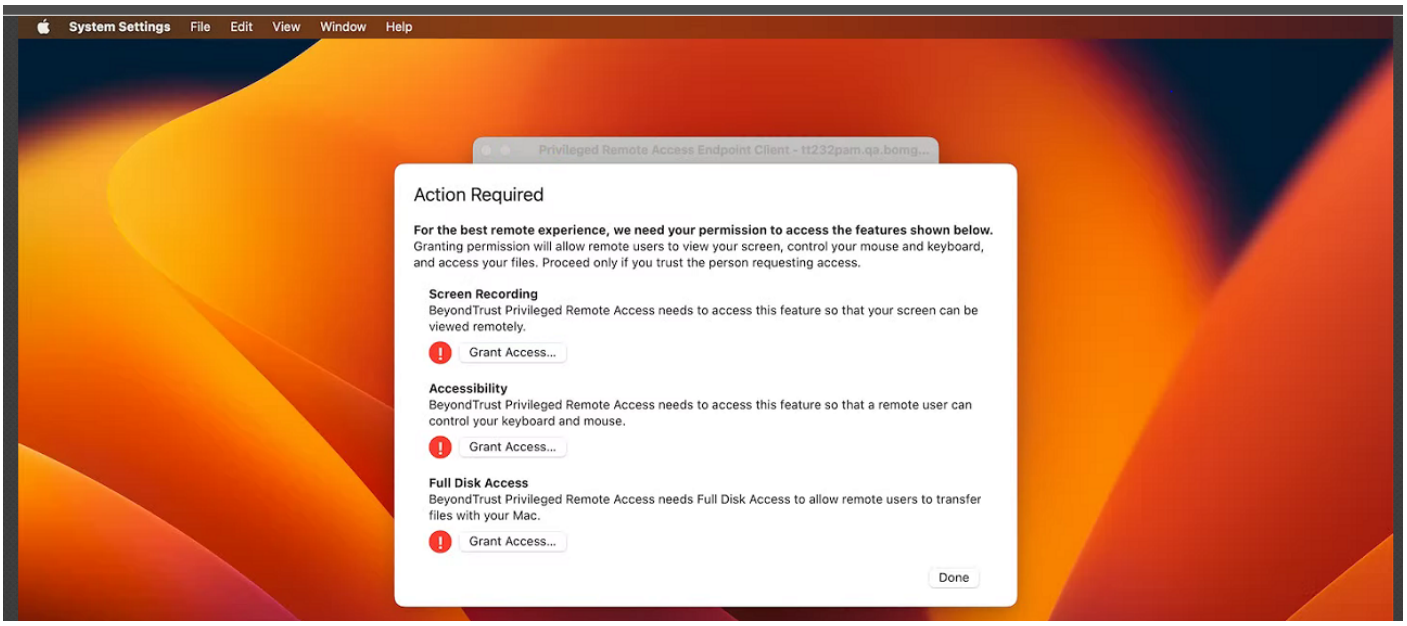
Command Line Parameter	Value	Description
--jc-name	**<name...>**	If override is allowed, this command line parameter sets the Jump Client's name.
--jc-jump-group	**user:<username> jumpgroup:<jumpgroup-code-name>**	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-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 host name as a site address. If no public portal has the given host name as a site address, then the Jump Client reverts to using the default public site.
--jc-session-policy-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 present at the console.
--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.
--silent		If included, the installer shows no windows, spinners, errors, or other visible alerts.

> ***Note:*** *If **--silent** is selected, sudo must be used, otherwise the installation will fail as a prompt during installation does not display.*

> ***Tip:*** *A Jump Client can also be installed in service mode.*

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. Screen images show the Privileged Remote Access endpoint client, installed on a macOS desktop, however the process is similar for the Remote Support customer client and with other devices.

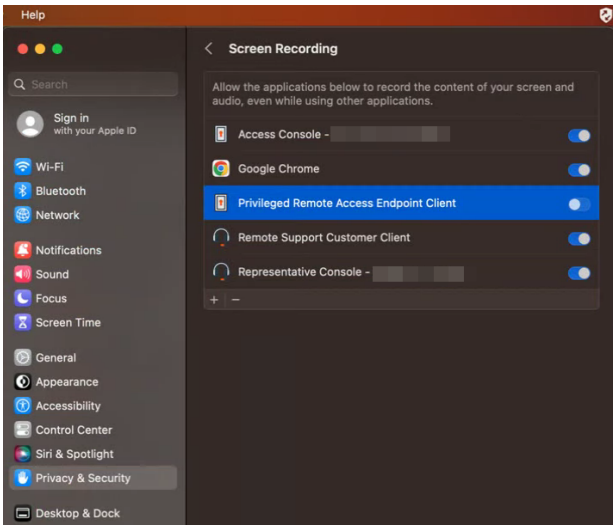


Three types of access are requested: **Screen Recording**, **Accessibility**, and **Full Disk Access**. For the best remote support experience, grant access for all three. Limited support is available if only one or two types of access are granted.

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.

Uninstall a Jump Client

To uninstall a Jump Client, remove it from the representative console.

If the client is not connected when it is removed from the console, the files are removed next time the client authorizes with the server.

> *For information about Jump Client settings, please see "Configure Jump Client Settings" on page 47.*

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 Remote Support Customer Client, deploy a PPPC profile targeting the following app bundle:

- **Identifier**: com.bomgar.bomgar-scc
- **Identifier Type**: Bundle ID
- **Code Requirement**: identifier "com.bomgar.bomgar-scc" 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 Remote Support 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 Remote Support:

- 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 Remote Support 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 Remote Support 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 Remote Support Jump Client installer is delivered as a uniquely generated and named DMG file. This file has the format **bomgar-scc-<uid>.dmg**.

For deployment, the sequence of steps includes:

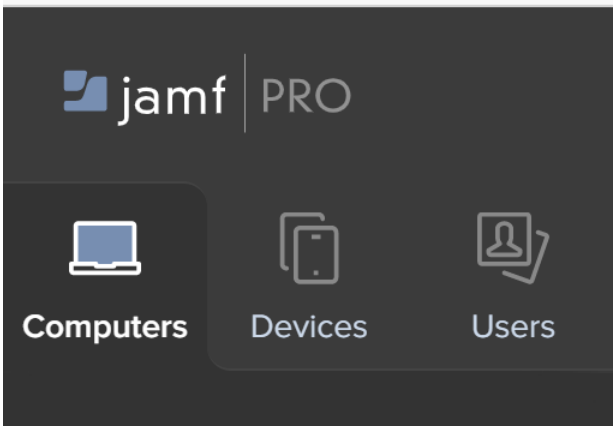
1. Stage the DMG file in a temporary location.
2. Mount the DMG file.
3. Install the Remote Support Jump Client.
4. Unmount the disk image.
5. Remove the DMG from the temporary location.

Deploy using JAMF Pro

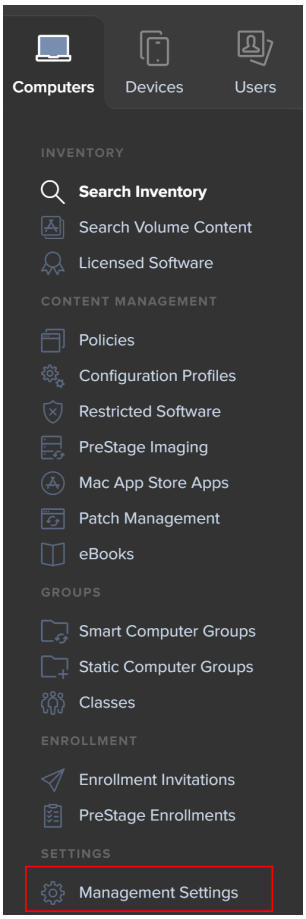
> ***Note:*** *This information is provided for general assistance when using JAMF Pro, however BeyondTrust cannot provide support for third-party products, and their requirements and operations may change.*

Upload Package to Jamf Software Server

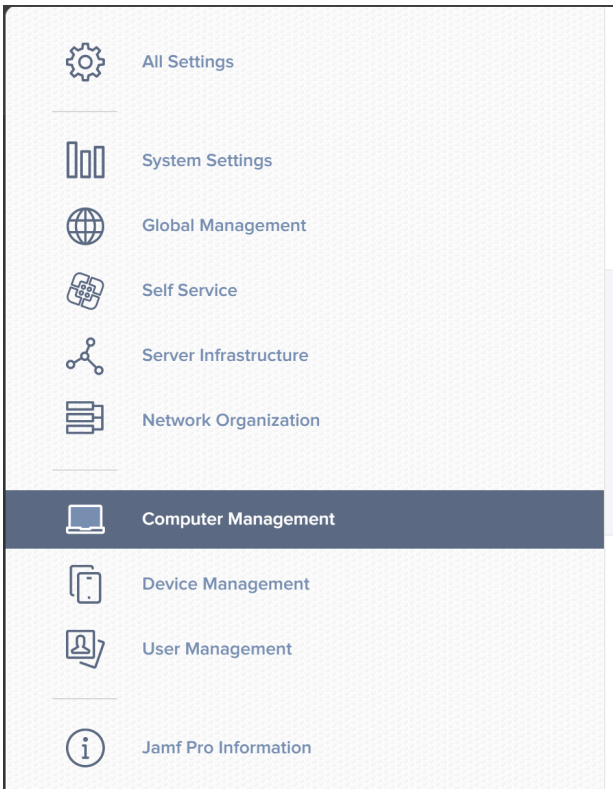
1. Log in to your Jamf Software Server (JSS) via a web browser.
2. Click **Computers**.



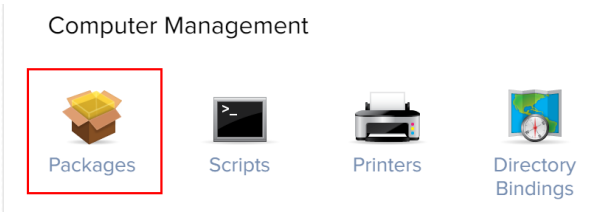
3. Click **Management Settings**.



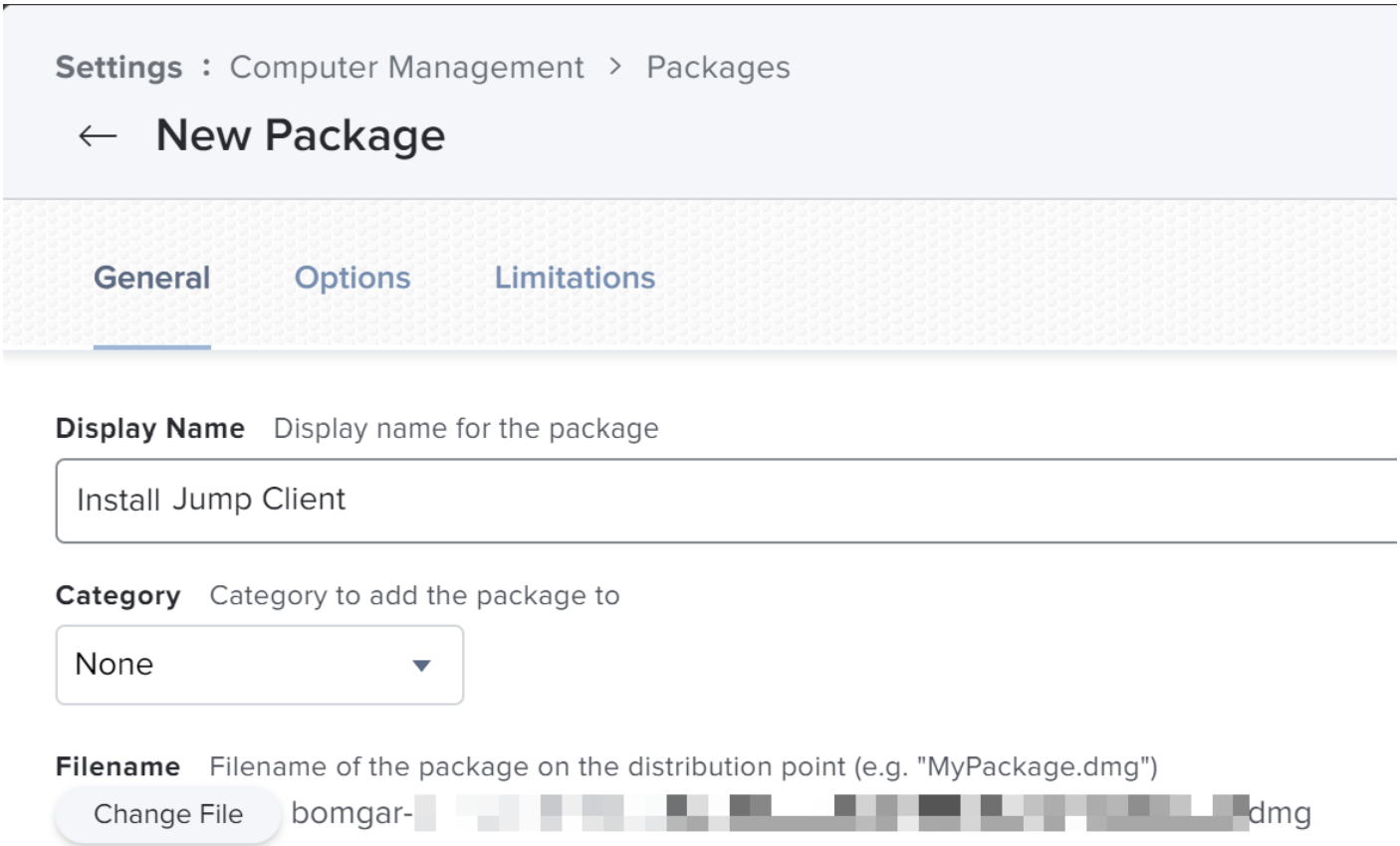
4. Click the **Computer Management** tab.



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



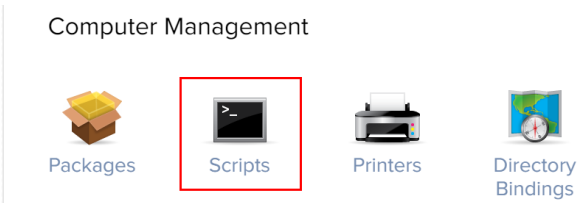
7. Fill out a display name, and choose a category (if applicable).



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.
18. Click **Save**.

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

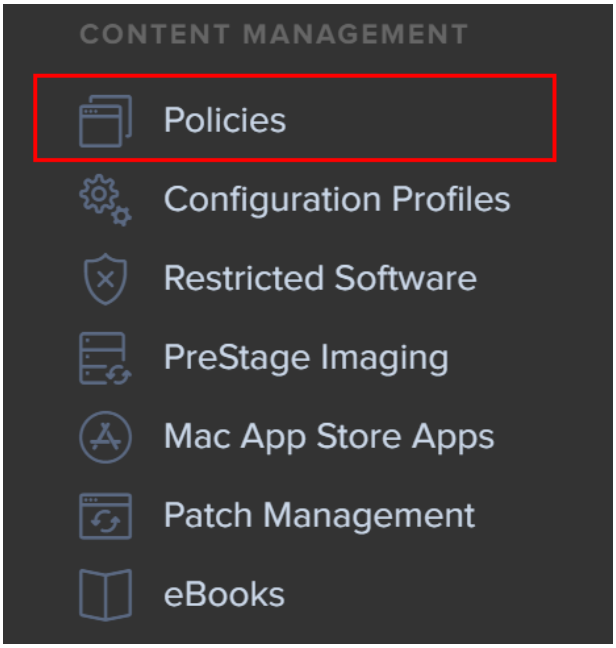
```
xattr -d com.apple.quarantine bomgar-scc-[uid].dmg
```

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

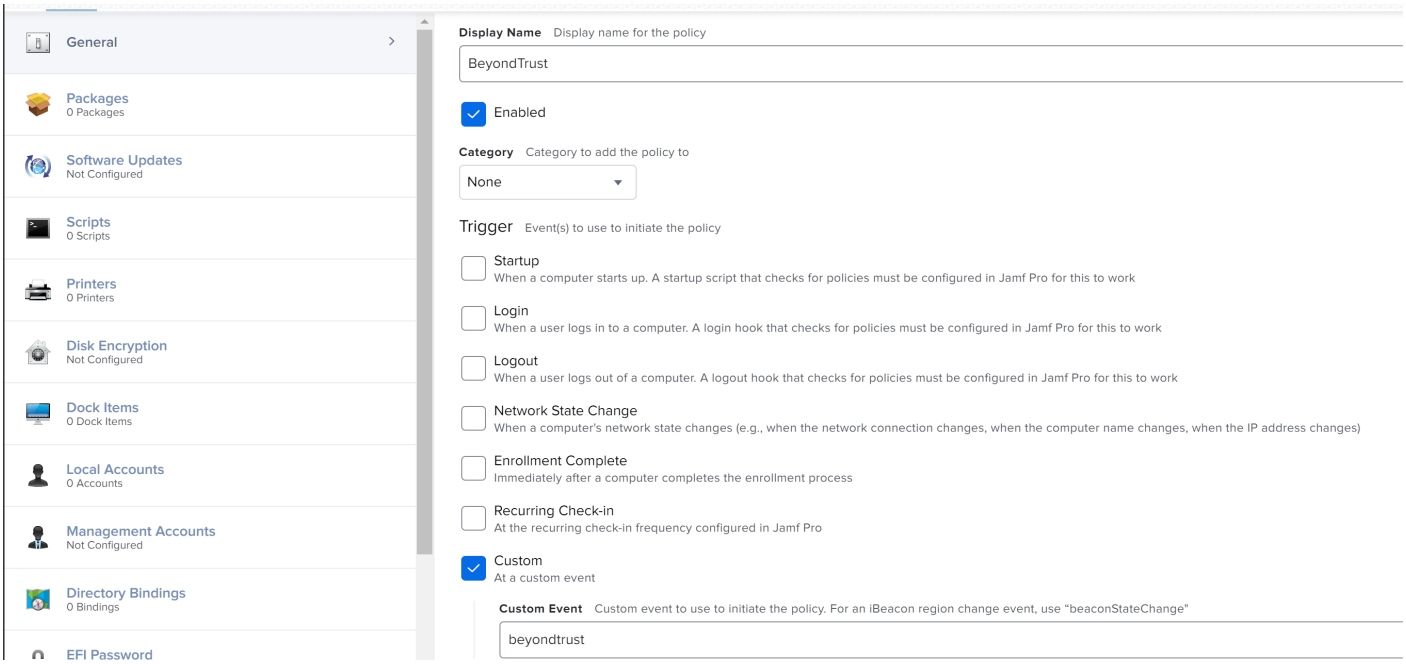
*For detailed information on **sdcust** usage, see **Mass Deploy Help** located within the /login interface on **Jump > Jump Client**.*

Create Deployment Policy

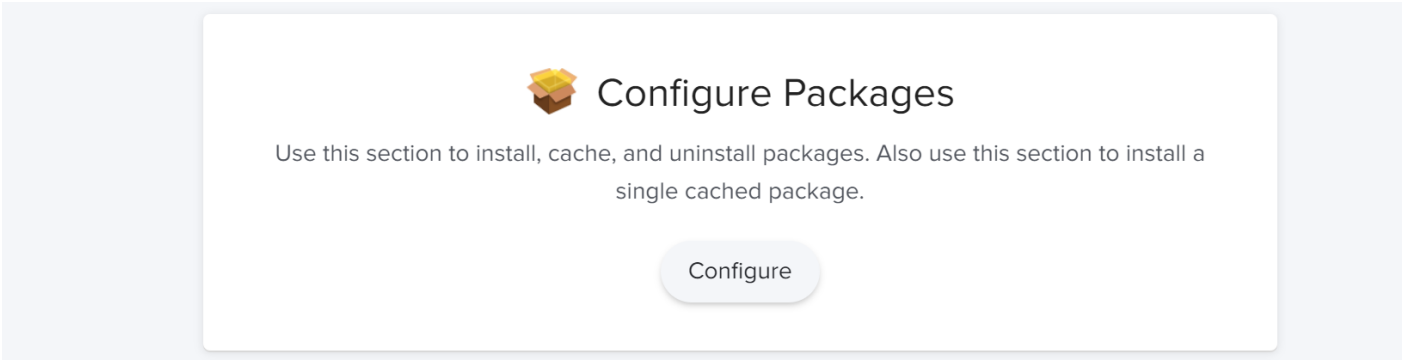
19. If necessary, log in to the JSS via a web browser.
20. Click **Computers**.
21. Click **Policies**.
22. Click **New**.



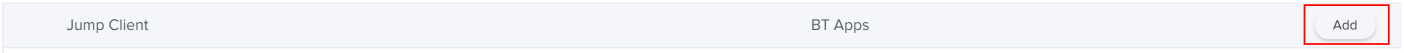
23. Provide a policy name, configure desired policy triggers, and ensure **Execution Frequency** is **Once Per Computer**.



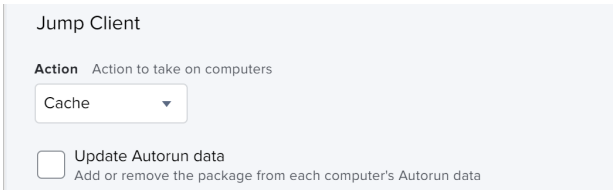
24. Click **Packages**, and then click **Configure**.



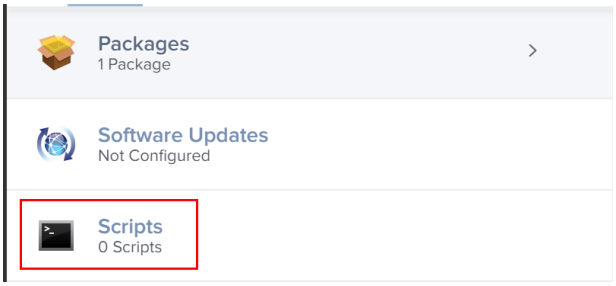
25. Click **Add** to select the Jump Client package from the list of available packages.



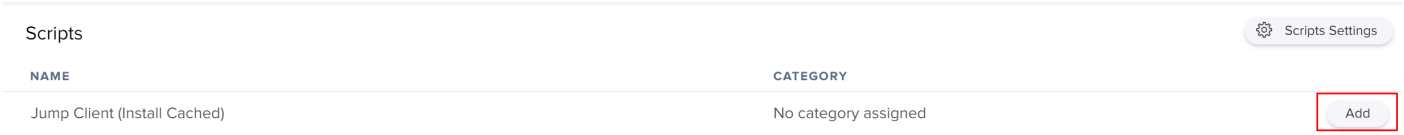
26. Select **Cache** as the action. This makes the packages available in the JAMF downloads folder for use by the deployment script created earlier.



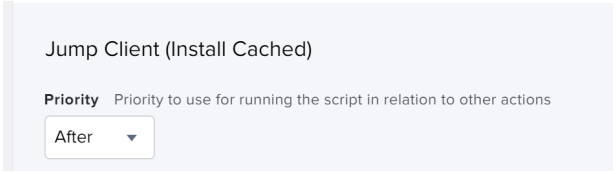
27. Click **Scripts** from the left navigation menu.



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 "Install a Jump Client on a Mac System" on page 24.

Install a Jump Client on a Linux System

You can override certain installation parameters specific to your needs. These parameters can be specified 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.

Note: *It is common to receive an error message during the install, regarding a layout or appearance issue. This can be disregarded.*

Command Line Parameter	Value	Description
--install-dir	**<directory_path>**	Specifies a new writable directory under which to install the Jump Client. 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-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 host name as a site address. If no public portal has the given host name as a site address, then the Jump Client reverts to using the default public site.
--jc-session-policy-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 present at the console.
--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.
--silent		If included, the installer shows no windows, spinners, errors, or other visible alerts.

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:

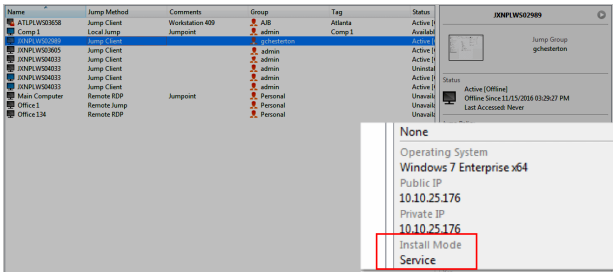
1. Add executable permissions to the file:

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

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

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

Remote Support Linux Jump Clients can be installed in service mode. The 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.

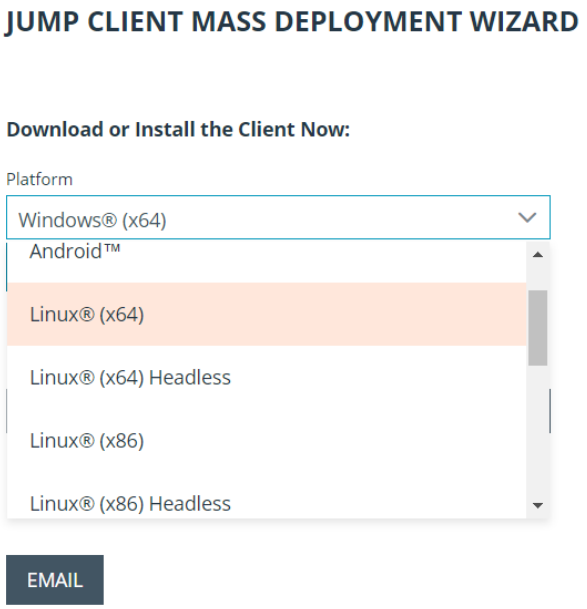


A service-mode Jump Client allows the user to start a session even if no remote user is logged on, as well as to log off the current remote user and log on with different credentials. A Linux Jump Client installed in user mode cannot do this, nor can it be elevated to service mode within a session.

To install a Jump Client in service mode on a Linux system, the Jump Client installer must be by run by root, but we recommend that you not run the Jump Client service 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 in to the representative console, right click the existing user mode Jump Client (if there is one), and click **Remove**.

2. Log in to 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-scc-[uid].desktop
```

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

```
sudo sh ./Downloads/bomgar-scc-[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.

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

Uninstall a Jump Client Installed Using Service Mode

Follow the steps below:

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

```
sudo sh ./uninstall
```

This leaves an entry in the representative console interface. The entry is automatically marked as **uninstalled** or **deleted**, depending on your Jump Client settings. Manual changes made for service mode Jump Client or headless Jump Client to start on boot are not removed by the script.

Install a Jump Client on a Headless Linux System

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-scc-{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-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.*

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

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 host name as a site address. If no public portal has the given host name as a site address, then the Jump Client reverts 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.

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 a Jump Client Installed on a Headless Linux System

To uninstall a Jump Client, remove it from the representative console.

- If the client is not connected when it is removed from the console, the files are removed the next time the client authorizes with the server.
- Manual changes made for service mode Jump Client or headless Jump Client to start on boot are not removed.

Jump Clients can be removed from a device by using a script:

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

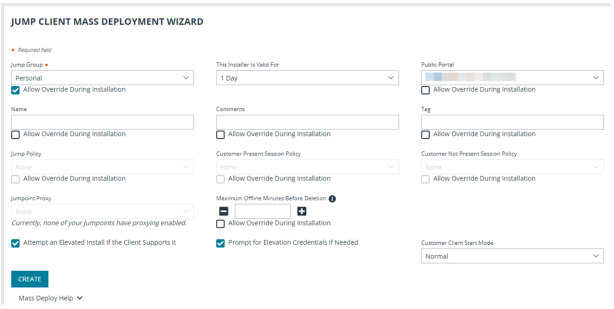
This leaves an entry in the representative console interface. The entry is automatically marked as **uninstalled** or **deleted**, depending on your Jump Client settings. Manual changes made for service mode Jump Client or headless Jump Client to start on boot are not removed by the script.

For information about Jump Client settings, please see "Configure Jump Client Settings" on page 47.

Install a Jump Client on a Raspberry Pi System

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. 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 (and higher ranking roles on your team, such as Team Lead and Team Manager if you are a Team Member, and Team Manager if you are a Team Lead) 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. Select the **Public Portal** through which you want this Jump Client to 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.
5. The **Customer Present Session Policy** does not apply to headless Jump Clients.
6. You can choose a **Customer Not Present Session Policy** to apply to this Jump Client. A session policy assigned to this Jump Client has the highest priority when setting session permissions.

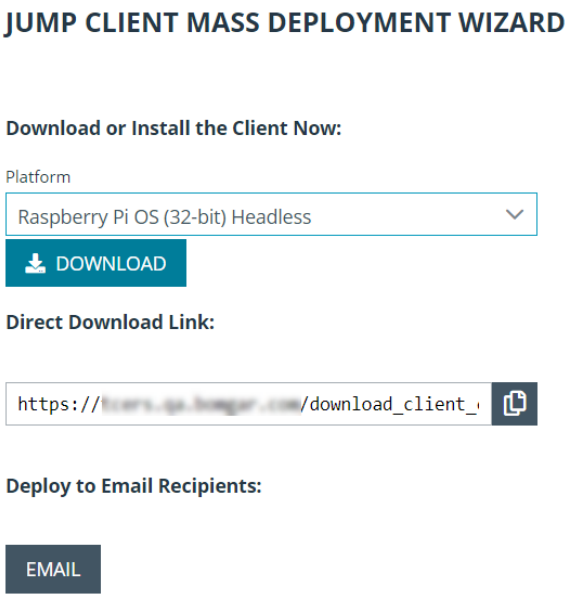
> ***Note:*** *We recommend that you not set a session policy for a headless Jump Client.*

7. You can 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.
8. Adding a **Tag** helps to organize your Jump Clients into categories within the representative console.
9. If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. As a result, if these Jump Clients are installed on computers without native Internet connections, they can use the Jumpoint to communicate with your B Series Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.
10. 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.
11. 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 BeyondTrust Appliance B Series 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 logged-in admin user with appropriate permissions, 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.

12. The options **Attempt an Elevated Install if the Client Supports It**, **Prompt for Elevation Credentials If Needed**, and **Start Customer Client Minimized When Session Is Started** do not apply to headless Jump Clients.
13. Once you click **Create**, select the **Raspberry Pi OS** option and click **Download**.



14. Using your preferred method, push the Jump Client installer file to each headless system you wish to access.
15. 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-scc-{uid}.bin --install-dir /home/pi/<dir>
```

16. 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 host name as a site address. If no public portal has the given host name as a site address, then the Jump Client reverts to using the default public site.

Command Line Parameter	Value	Description
--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.

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

```
/home/pi/<dir>/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.

18. 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 a Jump Client

To uninstall a Jump Client, remove it from the Representative Console.

- If the client is not connected when it is removed from the console, the files are removed next time the client authorizes with the server.
- Manual changes made for the Jump Client to start on boot are not removed.

Jump Clients can be removed from a device using a script:

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

This will leave an entry in the Representative Console interface. The entry is automatically marked uninstalled or deleted, depending on your Jump Client Settings. Manual changes made for the Jump Client to start on boot are not removed by the script.

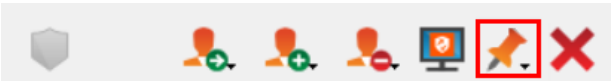
For information about Jump Client settings, please see "Configure Jump Client Settings" on page 47

Install a Jump Client on an Android System

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. You can deploy Jump Clients using either of the methods below.

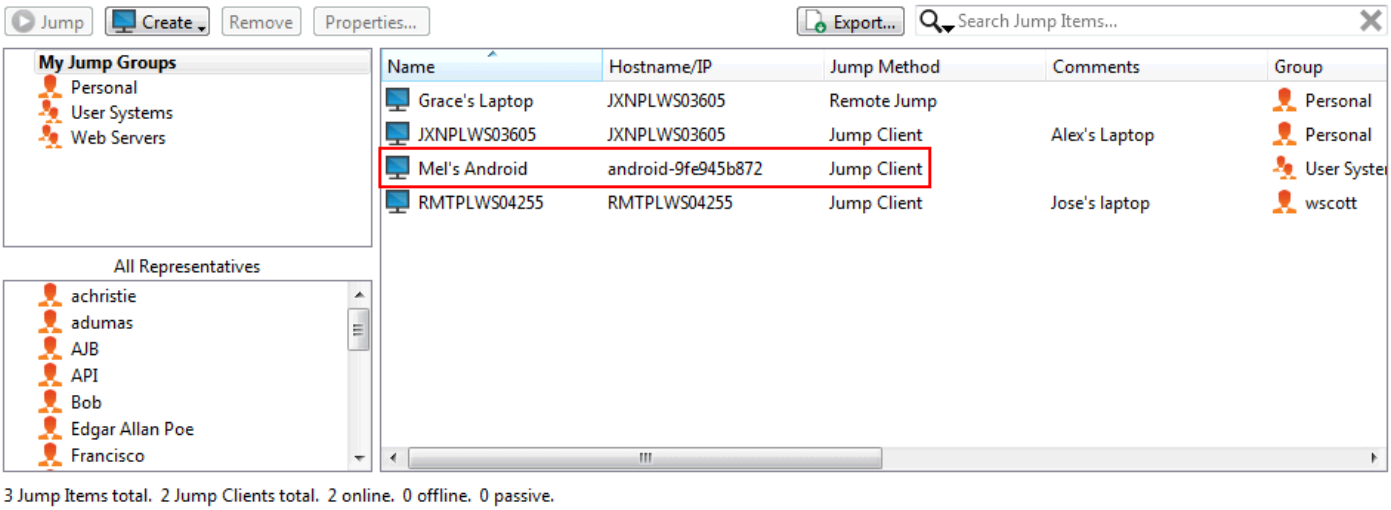
> ***Note:*** *Bandwidth usage and battery life are minimally affected by establishing a persistent connection.*
>
> *Persistent connections to an unattended Android device can occur only when the devices have both the* ***BeyondTrust Support Client*** *and* ***BeyondTrust Jump Client App*** *installed 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



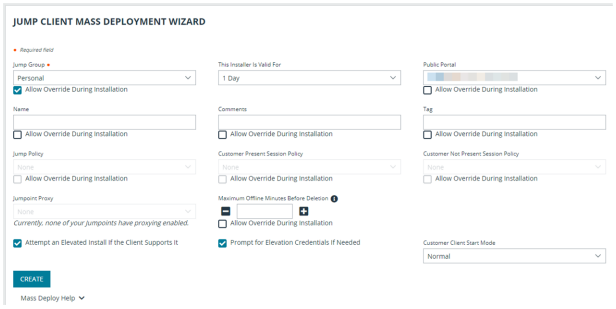
1. While in a support session with the Android device, click on the **Pin as Jump Client** icon.
2. After pinning, the Android device appears as a Jump Item in the Jump Item list. If the **Pin a Jump Client** icon is gray, the Android Jump Client is not installed on the Android device.
3. Meanwhile, the BeyondTrust Jump Client app on the device displays the client as pinned, with a date and timestamp.
4. The BeyondTrust Jump Client app on the device also has a dropdown list of possible device names. The agent can select the **Device Name** reported by the device, or another option such as the reported value for the **IP Address**, **Hostname**, or **Device Model**. Values for some options may not be available due to permissions.

> ***Note:*** *Options are available for the Jump Client to be disabled if the device relies on battery power or on data to connect.*

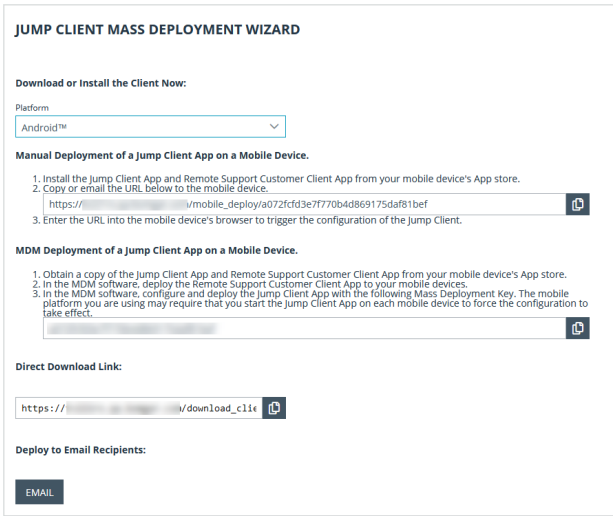


Email a Link from the /login Interface to Install and Android Jump Client

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.*

> ***Note:*** *Android prevents the application from being fully functional until the user opens the app at least once. This should be done after the application has been installed, and before attempting to pin a session to it.*

Uninstall a Jump Client

To uninstall a Jump Client, remove it from the Representative Console. The client remains on the device, but reverts to unpinned. If the client is not connected when it is removed from the console, the client reverts to unpinned the next time the client authorizes with the server.

Jump Clients can be removed from a device using a script. This will leave an entry in the Representative Console interface. The entry is automatically marked uninstalled or deleted, depending on your Jump Client Settings.

For information about Jump Client settings, please see "Configure Jump Client Settings" on page 47.

Configure Jump Client Settings

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

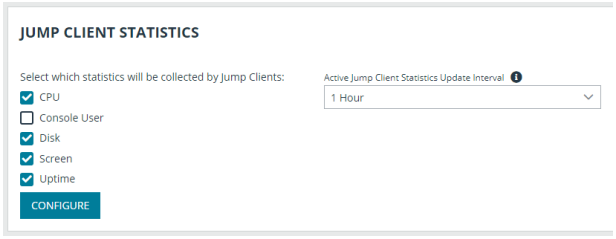
Manage Installers with the Jump Client Installers List

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

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 representative 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**. The maximum upgrade bandwidth is 100MiB/s.

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.*

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

Global connection rate for Jump Clients determines the maximum rate per second of Jump Clients able to connect to the B Series 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.

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 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 B Series 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 B Series 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, set this field to a smaller number than the deletion field above.*

Note: *The setting must be configured for 15 days or more.*

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 B Series Appliance at the time it is uninstalled, the affected item remains in its offline state.

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.

Manage Other Options

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.

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.*

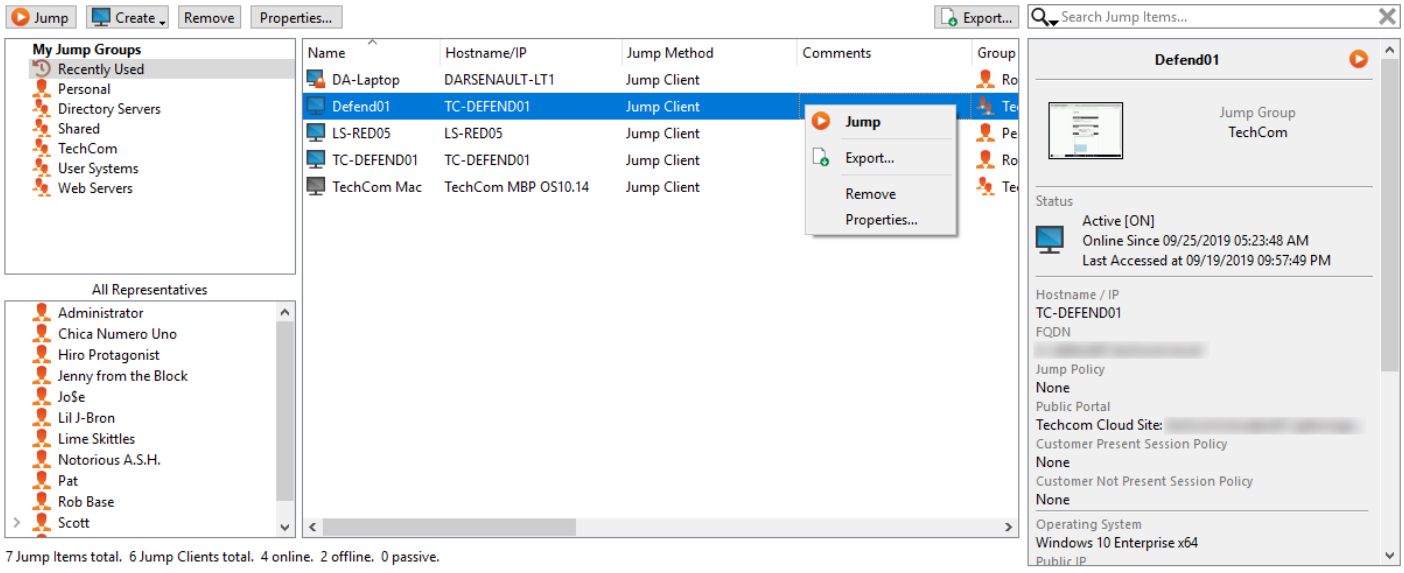
Start a Support Session through a Jump Client

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

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.*



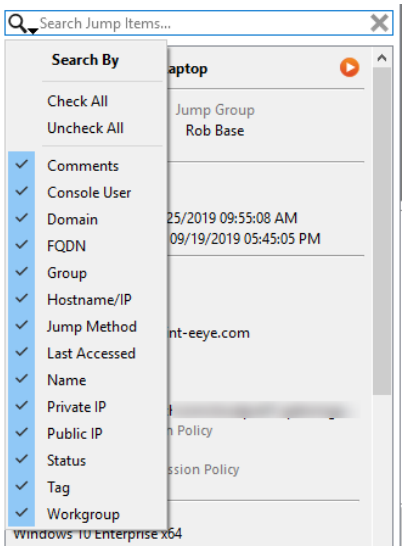
From the left pane, select the Jump Group for which you want to view pinned Jump Clients.

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 might have access to your personal list of Jump Items. Similarly, if you are a team manager or lead with appropriate permissions, you might see team members' personal lists of Jump Items. Additionally, you might 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 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 B Series 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 if the Jump Client does not come back online.

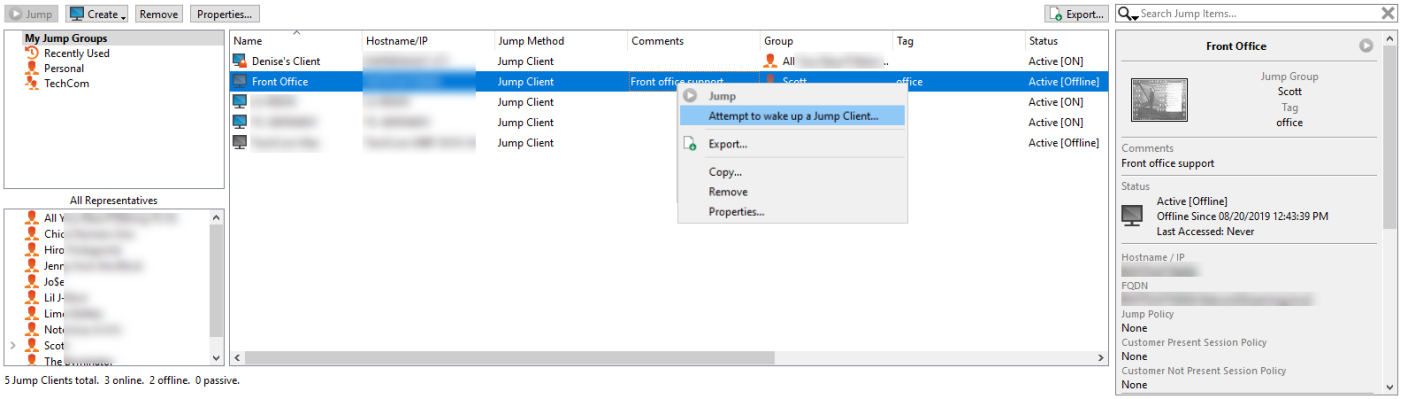
After a software update, Jump Clients update automatically. The number of concurrent Jump Client upgrades is determined by settings on the **/login > Jump > Jump Clients** page. If a Jump Client has not yet been updated, it is labeled as **Upgrade Pending**, and its version and revision number appear 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

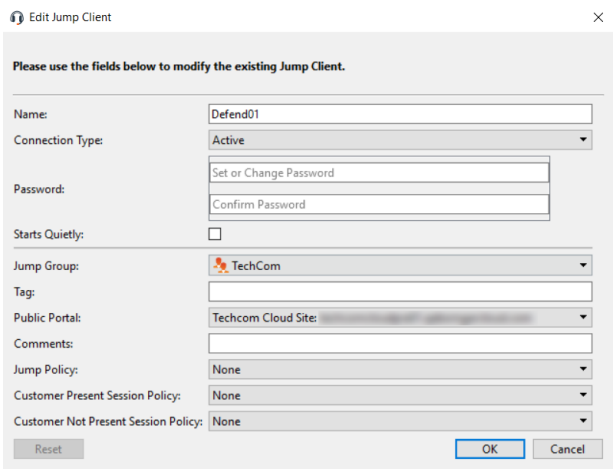


Depending on the permissions set by your administrator, you might also be able to wake up a selected Jump Client by broadcasting Wake-on-LAN (WOL) packets through another Jump Client on the same network. Once a WOL is attempted, the option becomes unavailable for 30 seconds before a subsequent attempt 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 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 B Series 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 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**.



From the API

By integrating with the BeyondTrust API, you can 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 BeyondTrust Appliance B Series at **https://support.example.com/api/client_script**, where **support.example.com** is your BeyondTrust site host name.

Optional Parameters for the start_pinned_client_session Command

search_string=[string]	If specified, then this is the search criteria used to select a Jump Client. The comments, host name, 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.
client.comments	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.
client.hostname	If specified, only Jump Clients with the given host name 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 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 field has a maximum length of 255 characters. Search is partial and case-insensitive.
client.tag	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.
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!

*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.*

*If multiple **client.*** parameters are specified, then only Jump Clients matching all criteria are returned.*

Query Examples: start_pinned_client_session

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

***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 **(bomgar-rep.exe**, for example), followed by one of two commands:

```
--run-script "action=start_pinned_client_session&search_string=[string]"
```

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

Example: *Run a BRCS script from the command prompt:*

```
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, please see the following:

- *"Deploy Jump Clients During a Support Session or Prior to Support" on page 14*
- *On Beyondtrust Representative Console Scripting, the API Guide at www.beyondtrust.com/docs/remote-support/how-to/integrations/api/*
- *On Jump shortcuts, please see the Jumpoint Guide at www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.*

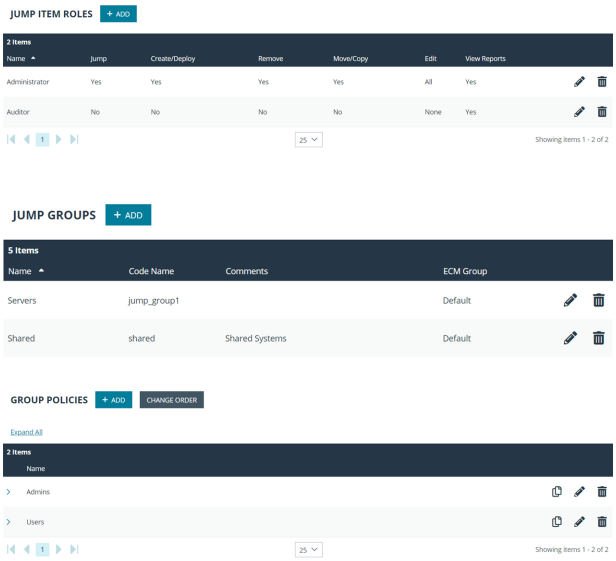
Use Cases for Jump Client Implementation

To offer you the most flexibility and control over your Jump Items, BeyondTrust includes several areas where permissions must be configured. To help you understand how you might want to set up your system, there are 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 be able to Jump to only those items.

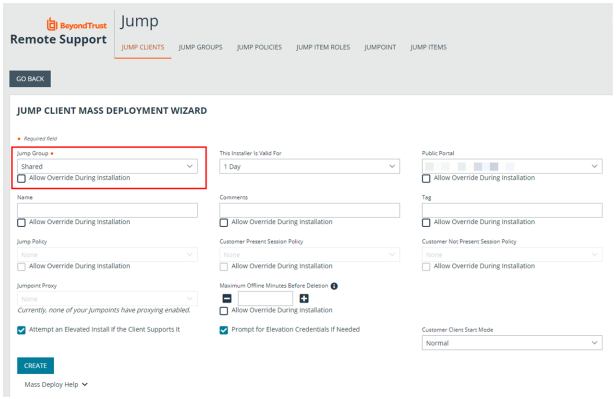
1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**. Ensure the following:
    - The **Administrator** role has all permissions enabled.
    - The **Start Sessions Only** role has only **Start Sessions** enabled.
2. Create a **Shared** Jump Group to contain all shared Jump Items. 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. Include the following permissions:
    - Define **Representative Permissions** and enable **Allowed to provide remote support**.
    - 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 **Teams** and **System** roles to **Start Sessions Only**.
    - Under **Memberships**, define **Add Jump Group Memberships**.
    - 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. Include the following permissions:
    - Define **Representative Permissions** and check **Allowed to provide remote support**.
    - 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 Jump Group Memberships**.
- 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.



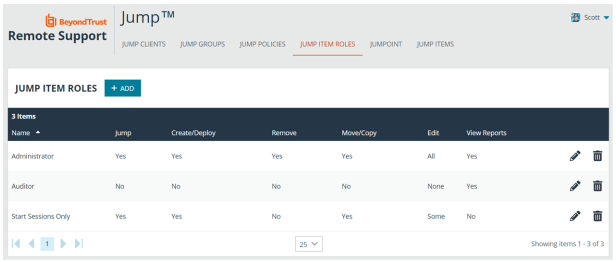
7. Now administrators can deploy and start sessions with Jump Items in the **Shared** Jump Group. They can also manage their personal lists of Jump Items and start sessions with all other Jump Items.

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

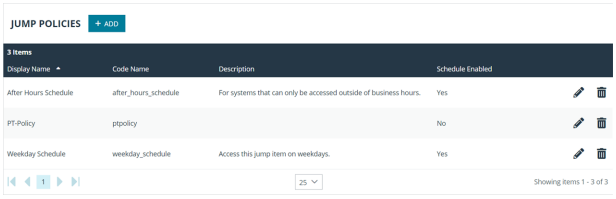
Advanced Use Case

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 must be accessible at all times, while others must be accessible only on weekdays.

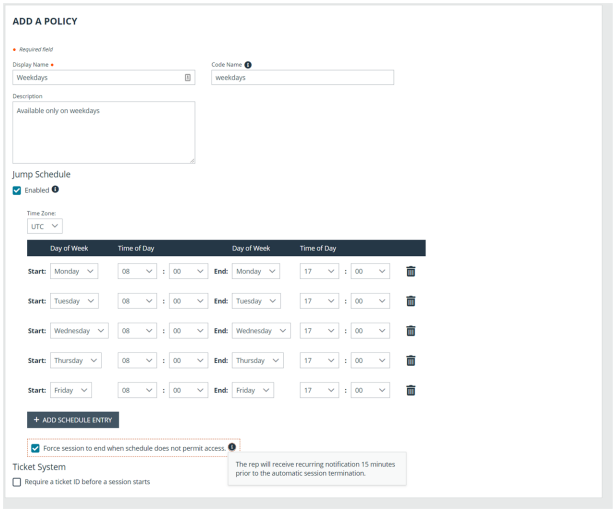
1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**. Ensure the following:
   - The **Administrator** role has all permissions enabled.
   - The **Start Sessions Only** role has only **Start Sessions** enabled.



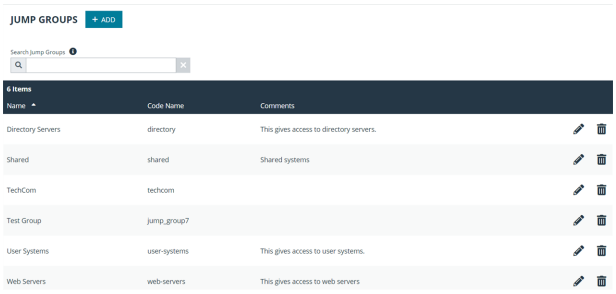
2. Create a Jump Policy, **Weekdays**.



3. In the Jump Policy, enable the **Jump Schedule**.
    - Click **Add Schedule Entry**.
    - Set the **Start** day and time to **Monday 8:00** and the **End** day and time to **Monday 17:00**.
    - Click **Add Schedule Entry** and repeat the process for the remaining weekdays.
    - Save the Jump Policy.



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

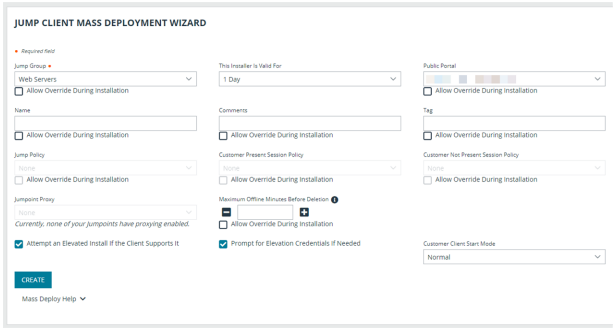


5. Put users into two group policies, **Admins** and **Users**.

6. In the **Admins** group, configure settings and permissions as appropriate. Include the following permissions:
    - Define **Representative Permissions** and enable **Allowed to provide remote support**.
    - 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 Jump Group Memberships**.
    - In the **Jump Group** field, search for and select **Web Servers**.
        - Set the **Jump Item Role** to **Administrator**.
        - 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**.
        - 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**.
  - Click **Add** to assign the members of this group policy to the Jump Group.
- Save the group policy.

7. In the **Users** group, configure settings and permissions as appropriate. Include the following permissions:
   - Define **Representative Permissions** and check **Allowed to provide remote support**.
   - 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 Jump Group Memberships**.
   - In the **Jump Group** field, search for and select **Web Servers**.
     - Set the Jump Item Role to **Start Session Only**.
     - 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**.
     - 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**.
     - Click **Add** to assign the members of this group policy to the Jump Group.
   - 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.
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.

Jump Client Error Message Reference

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

Action	Error Message	Explanation and Reproduction Notes
Pinning a Jump Client from within a Session	The total number of deployable Jump Clients for this site has been reached.	The build limit has been reached.
	The total number of deployable Jump Clients for this site has been reached.	The build limit has been reached.
	The support session already has a pending request to pin.	Race condition (Reproduction is UI-limited).
	The support client is already pinned.	Race condition (Reproduction is UI-limited).
	No customer could be found within the support conference.	Race condition (Reproduction is UI-limited).
	The customer within the support conference is not online.	Race condition (Reproduction is UI-limited).
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 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 representative 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 representative 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 representative console has attempted to Jump to that Jump Client before being notified.
Jumping	Permission denied joining existing support session.	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 **Allow simultaneous representative access to a single Jump Client** setting under **/login > Jump > Jump Clients ::**

Action	Error Message	Explanation and Reproduction Notes
		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 support session.	Internal for active Jump Client starts.
	An internal operation was taking too long while trying to spawn a support session.	Internal for active Jump Client starts.
	The active Jump Client is not connected.	Race condition: An active Jump Client disconnected before the representative console was notified.
	Timeout while trying to connect to the Jump Client.	Took too long to connect to any of the host names or IPs.
	Failed to connect to the Jump Client.	Could not connect to any IP address or host name of a Jump Client.
	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.	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.
	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 representative 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 representative console has attempted to Jump to that Jump Client before being notified. Also see note below.
	The specified Jump Client has been uninstalled.	Race condition: A Jump Client has been uninstalled, but an representative 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.