BeyondTrust

Remote Support
Jumpoint Guide

TC:3/12/2024

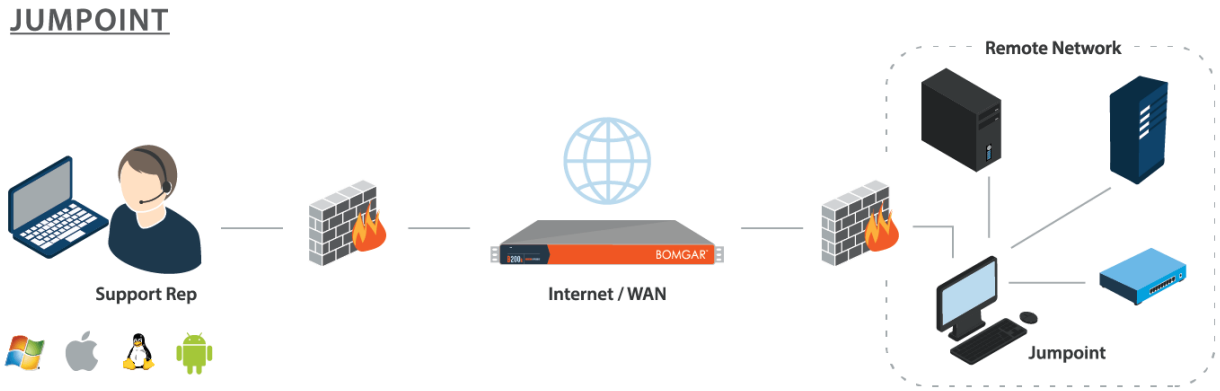
Table of Contents

Remote Support Jumpoint Guide: Unattended Access to Computers in a Network

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 Jumpoint acts as a conduit for access to computers on a known remote network. A single Jumpoint installed on a computer within a LAN is used to access multiple systems, eliminating the need to pre-install software on every computer you might need to access.

Within a LAN, the BeyondTrust user's computer can initiate a session to a system directly without using a Jumpoint, if appropriate user permissions are enabled. This is called a *Local Jump*. A Jumpoint is needed only for a Remote Jump when the BeyondTrust user's computer cannot access the target computer directly.



For more information on Jump Items for mobile devices, please see the following:

- *Use Jump Shortcuts to Access Unattended Computers from the Android Representative Console at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/android/jump-shortcuts.htm*
- *Use Jump Clients to Access Unattended Computers from the Android Representative Console at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/android/jumpclients.htm*
- *Use Jump Shortcuts to Access Unattended Computers from the iOS Representative Console at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/ios/jump-shortcuts.htm*
- *Use Jump Clients to Access Unattended Computers from the iOS Representative Console at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/ios/jumpclients.htm*

Recommended Steps to Implement 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.

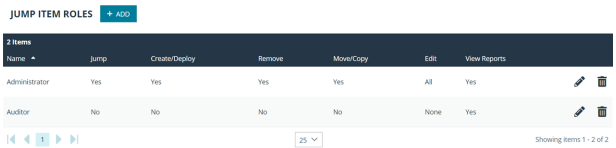
1. **Add Jump Item Roles.** Jump Item Roles determine how users are allowed to interact with Jump Items. These roles are applied to users by means of individual account settings, group policies, and when added to Jump Groups.
2. **Add Jump Policies.** Jump Policies are used to control when certain Jump 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, by means of group policy.
4. **Deploy Jumpoints.** A Jumpoint acts as a conduit for unattended access to computers on a known remote network. A Jumpoint is necessary to use Remote Jumps, Remote RDP, Remote VNC, Shell Jumps, and Intel® vPro sessions. Local Jumps, Local RDP, and Local VNC can be performed to systems on the same local network.
5. **Create Jump Shortcuts.** A Jump Shortcut is a quick way to start sessions with frequently accessed remote systems. Jump Items are created from the representative console or are imported from **/login > Jump > Jump Items**. When creating or importing Jump Items, be sure to set the Jump Group and Jump Policy to determine who can access the Jump Item and with what restrictions.

For more information about Jump Item Roles, Jump Policies, Jump Groups, deploying Jumpoints, and using Jump Shortcuts, 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 7*
- *"Use Jump Groups to Determine Which Users Can Access Which Jump Items" on page 8*
- *"Requirements and Considerations to Install a Remote Support Jumpoint" on page 10*
- *"Configure and Install a Jumpoint for Windows Systems" on page 14*
- *"Configure and Install a Jumpoint for Linux Systems" on page 29*
- *"Use Jump Shortcuts to Jump to Remote Systems" on page 44*

Use Jump Item Roles to Create Permission Sets for Jump Items

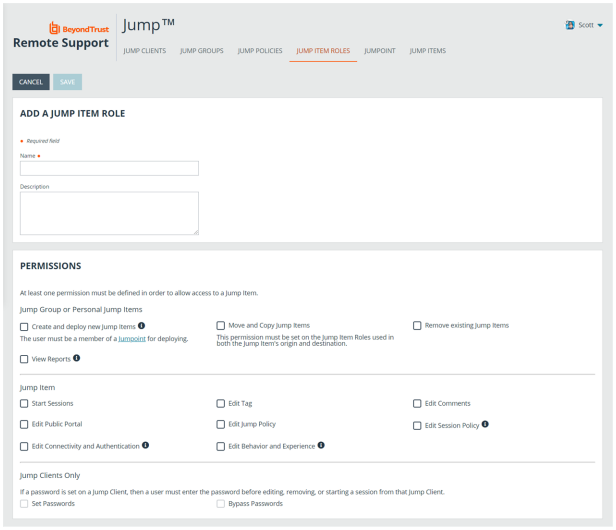
A Jump Item Role is a predefined set of permissions regarding Jump Item management and usage. Jump Item Roles are applied to users from the **Jump > Jump Item Roles** page or from the **Users & Security > Group Policies** page.



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:



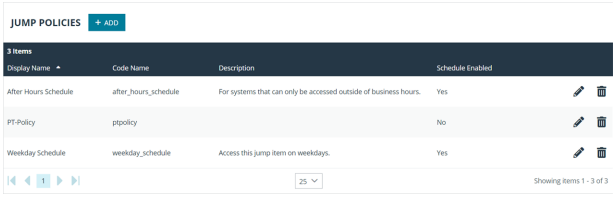
1. Under **Jump Group or Personal Jump Items**, determine if users can create and deploy Jump Items, move Jump Items from one Jump Group to another, or delete Jump Items.
2. Check the **Start Sessions** box to enable users to Jump to any Jump Items they have access to.
3. To allow users to edit **Jump 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.

Create Jump Policies to Apply to Jump Items

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

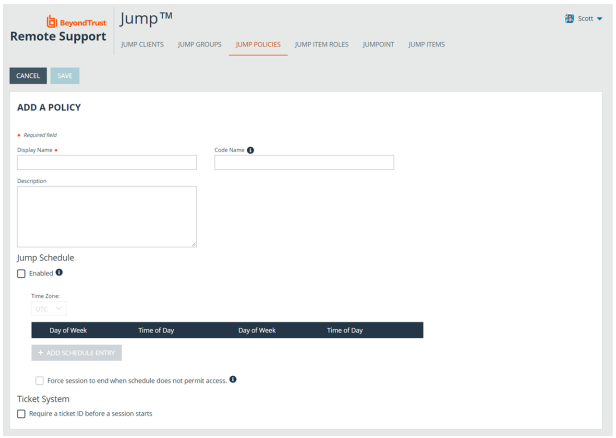
Create a Jump Policy

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.



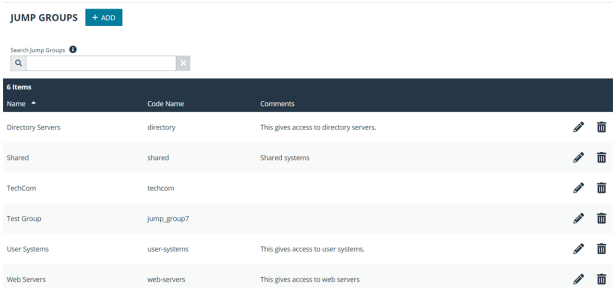
   - Set a schedule to define when Jump Items under this policy can be accessed. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.
   - If, for instance, the time is set to start at 8 PM and 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 this Jump Policy, click **Save**.

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

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.

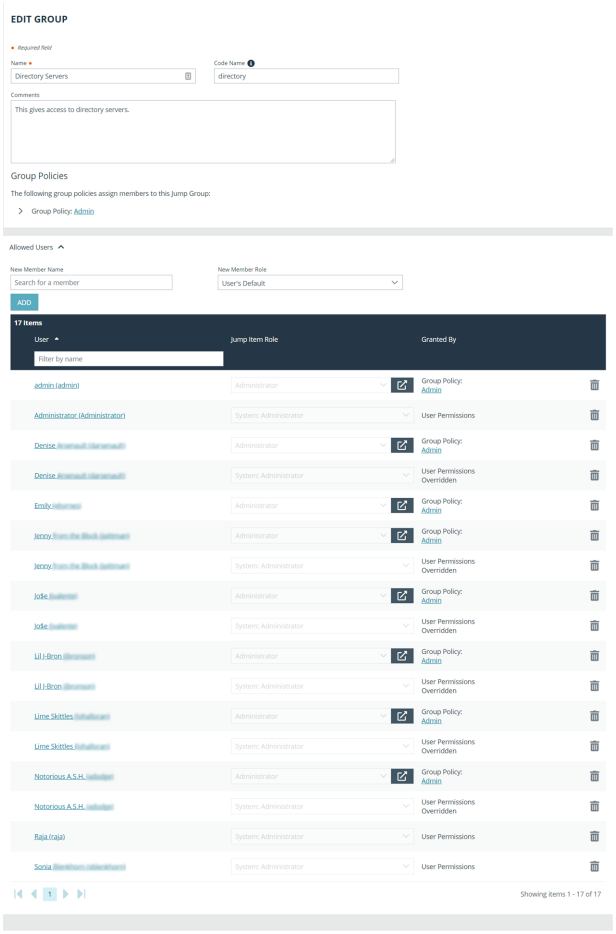


You can create or edit a Jump Group, assigning it a name, code name, and comments. The **Group Policies** section lists any group policies that assign users to this Jump Group.

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.

Requirements and Considerations to Install a Remote Support Jumpoint

A Jumpoint-facilitated BeyondTrust session involves three computers:

- The BeyondTrust user's system
- A computer that hosts the Jumpoint
- The unattended computer targeted for remote control

There are various permission, hardware, software, and port requirements for these systems that must be met or should be considered when installing a Jumpoint.

Review Jumpoint Permission Requirements

The administrator deploying the Jumpoint must have administrative rights on the computer hosting the Jumpoint.

Users must have the following permissions to access the Jumpoint:

- The user must have administrative rights to the target computer.
- In the administrative interface, one or both of the following conditions must be true:
  - The user must have the account permission **Allowed Jump Methods: Local Jump**.
  - The user must have the account permission **Allowed Jump Methods: Remote Jump** and must be granted access to one or more Jumpoints, either individually or via a group policy.

For more information, please see the following:

- *On user permissions, Remote Support Users and Security at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/users.htm.*
- *On Group Policies, Remote Support Group Policies at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/group-policies.htm.*

Review Jumpoint Installation Considerations

The main objective of any BeyondTrust administrator should be to ensure the integrity of the BeyondTrust deployment. The simpler and more straightforward a BeyondTrust deployment is, the easier it is to maintain a level of integrity that is in line with your company's security objectives. Specifically, when deploying a Jumpoint on a remote network, another layer of complexity is introduced to your deployment. Therefore, BeyondTrust recommends using a dedicated resource for a Jumpoint in order to decrease any potential security risks, increase availability, and reduce management complexity. A dedicated resource is most often a virtual machine or sometimes a physical machine with the sole purpose of hosting the Jumpoint.

If a dedicated resource is not readily available, there are several factors to take into consideration before deciding to use a shared resource as a Jumpoint host. When using a shared resource, the BeyondTrust administrator must be aware of everything for which the shared resource is used. For example, the BeyondTrust administrator would need to identify and control any unwanted changes to or repurposing of the resource by other groups, especially in large organizations.

There are many other variables that are unique to any given network or business environment. The questions below are provided to encourage a proactive approach before pursuing the use of a shared resource as a Jumpoint host. BeyondTrust encourages adding your own list of pros and cons before deploying a Jumpoint on a shared resource.

Security Questions

- Who has access to this resource?
- Are file shares accessible on this resource?
- Are there group policies in place that may restrict Jumpoint functionality?
- What is the risk of virus infection or malware due to multi-user access?
- What is the risk of another user changing the system permissions or deleting needed files?

File/Print Sharing Questions

- What other programs will be competing for resources such as disk space, processor availability, bandwidth, and disk access?
- Will the resource be available at all times? How critical is on-demand access?
- What is the risk of permission modification on file shares?
- Will this resource be used frequently for print jobs? Large or frequent print jobs can consume a large amount of resources, adversely affecting Jumpoint performance.

Other Shared Resource Questions

- How critical is availability? What is the risk of the Jumpoint not being available?
- How frequently will this Jumpoint be used?
- What is the potential number of Jump sessions that will need to be run through this Jumpoint at the same time?
- Will shared responsibility of this resource across different departments increase complexity?

Note: *A Jumpoint cannot be used to access itself, because that is an unsupported loopback connection.*

Review Jumpoint Hardware and Software Requirements

Host Hardware and Software Requirements – All Session Types

An average server class machine for a supported operating system, with 16GB of RAM, can readily support 25 concurrent sessions of any type (100 serial-over-LAN sessions, 200 Telnet or SSH sessions). Additional sessions are supported depending on the session types and other factors, or with higher server specifications.

For more information about hardware and software requirements, please see Remote Support Supported Platforms at https://www.beyondtrust.com/docs/remote-support/updates/supported-platforms.htm.

Session-Specific Host and Target Software Requirements

Except as noted, the target and the host must be on the same network.

Remote Jump Sessions – Host System Requirements

A domain account that has local admin rights on the target computer(s).

The following applies to Windows systems:

- By default, the Jumpoint runs under the local system account. This should be changed to an account that has local admin rights on the target computer(s).
- Follow these steps if this account is changed:
    - Log on to the Jumpoint host system as an administrator.
    - Stop the BeyondTrust Jumpoint service using **services.msc**.
    - Navigate to **C:\ProgramData\Bomgar\Jumpoint\hostname** or **C:\Users\All Users\Application Data\Bomgar\Jumpoint\hostname**, depending on the Windows version.
    - Open the properties for **bomgar.ini** and go to the **Security** tab. Click **Continue** to view the security properties.
    - Select the **Users** or **Everyone** group, depending on the Windows version.
    - Uncheck the **Read** permission in the **Deny** column.
    - Apply the changes.
    - The Jumpoint may now be safely changed to be under a different account.
    - Restart the Jumpoint service using **services.msc**.
- File sharing must be turned on, specifically **IPC$** and **ADMIN$**.
- The **Remote Registry** service must be running (check using **services.msc**).

Remote/Local Jump Sessions – Target System Requirements

The following applies to Windows systems:

- The **Workstation** service must be running (check using **services.msc**).
- The **Server** service must be running (check using **services.msc**).
- The **Remote Registry** service must be running (check using **services.msc**).
- The **ADMIN$** share must be available (check using **Computer Management**).
- The **Windows Network** must be running, and printer and file sharing must be activated.
- Make sure firewall settings do not block the connection. If the firewall blocks incoming traffic, open port 445 (and possibly 135) on the target computer for incoming traffic.

Shell Jump Sessions – Host System Requirements

No session-specific host system requirements.

Shell Jump Sessions – Target System Requirements

Any available SSH server.

vPro Sessions – Host System Requirements

No session-specific host system requirements.

vPro Sessions – Target System Requirements

Any pre-provisioned vPro system, running AMT version.

Remote RDP Sessions – Host System Requirements

No session-specific host system requirements.

Remote/Local RDP Sessions – Target System Requirements

Microsoft Remote Desktop Protocol (RDP) must be enabled on the target system.

> ***Note:*** *Remote Support supports only Microsoft's RDP server implementation built into Windows operating systems and Remote Desktop Session (formerly Terminal Services) Hosts.*

Remote VNC Sessions – Host System Requirements

No session-specific host system requirements.

Remote/Local VNC Sessions – Target System Requirements

Listening VNC server supporting RFB protocol 3.8 or earlier, configured for basic or no authentication.

Review Port Requirements for Discovery and Rotation of Vault Accounts

Active Directory:

- Port 389
- Port 636

Local Account Management:

- Port 445

Configure and Install a Jumpoint for Windows Systems

Setup of a Jumpoint on a remote network is a multi-step process that includes configuring from the /login administrative interface, downloading the installer, and running the installation wizard.

Understand Clustered Jumpoints

Before configuring a Jumpoint, it is important to understand the difference between clustered Jumpoints and stand-alone Jumpoints, because they have different feature sets and because a clustered Jumpoint cannot be converted to stand-alone, nor a stand-alone Jumpoint converted to clustered. A clustered Jumpoint allows you to install up to ten redundant nodes of the same Jumpoint on different host systems in the same local network.

A clustered Jumpoint is available as long as at least one of the installed nodes is online. This provides redundancy, preventing the failure of all Jump Items associated with the failure of a single, stand-alone Jumpoint, and improves load balancing across the system.

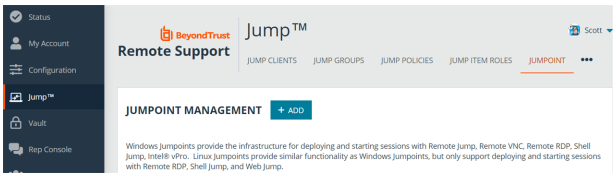
All configuration of clustered Jumpoints is done in **/login**, with no local configuration available on the local host either during or after the installation. This means that if you install a clustered Jumpoint, selecting the **BeyondTrust Jumpoint Configuration** item on the start menu of the Jumpoint host does not result in a configuration window, and only an **About** box is shown. Editing a clustered Jumpoint in **/login** loads the same configuration page that was used to create the Jumpoint. This means clustered Jumpoint configuration lacks the following options which are available to stand-alone Jumpoints:

- Proxy
- Intel vPro
- Shell Jump
- TTL

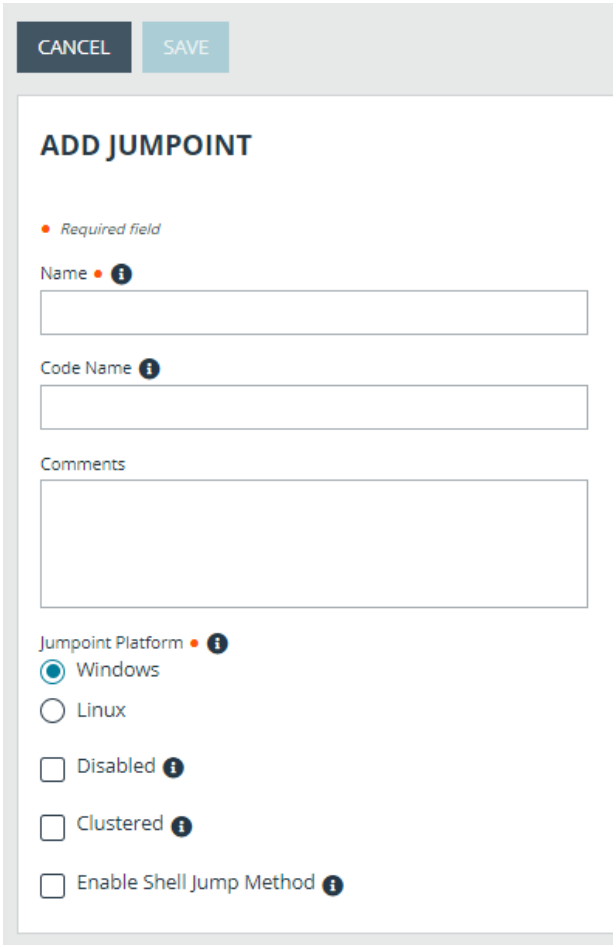
This also means that a clustered Jumpoint cannot be configured as a Jump Zone Proxy. vPro, RDP, VNC, Shell Jump, and normal Jump sessions are all supported when using clustered Jumpoints; however, the advanced configuration of these features is not available. This includes settings such as provisioned SSH hosts, vPro reimaging, Jump Zone Proxy, TTL, etc.

Configure

1. From the administrative interface, go to **Jump > Jumpoint**.
2. Click **Add**.



3. Create a unique name to help identify this Jumpoint. This name should help users locate this Jumpoint when they need to start a session with a computer on its same network.
4. Set a code name for integration purposes. If you do not set a code name, one is created automatically.
5. Add comments to help identify this Jumpoint.
6. Select the **Jumpoint Platform**. Options are Windows and Linux. Once the Jumpoint has been created this options cannot be changed.
7. Leave the **Disabled** check box unchecked.
8. Check the **Clustered** box, if appropriate.



> ***Note:*** *A **Clustered** Jumpoint allows you to install multiple, redundant nodes of the same Jumpoint on different host systems. If this option is selected, the Jumpoint is available as long as at least one of the installed nodes is online. This provides redundancy, preventing the failure of all Jump Items associated with the failure of a single, stand-alone Jumpoint, and improves load balancing across the system. All configuration of clustered Jumpoints is done in /login, with no local configuration available during the install. Once created, a clustered Jumpoint cannot be converted to stand-alone, nor a stand-alone Jumpoint converted to clustered.*

IMPORTANT!

Jumpoint cluster nodes must be installed on hosts residing in the same local area network.

9. If you want users to be able to connect to SSH-enabled and Telnet-enabled network devices through this Jumpoint, check **Enable Shell Jump Method**.
10. From the Jumpoint edit page, you can authorize users to start sessions through this Jumpoint. After the Jumpoint has been created, you can also grant access to groups of users from **Users & Security** > **Group Policies**.
11. Save the configuration. The new Jumpoint appears in the list of configured Jumpoints.

> ***Note:*** *Once you have installed the Jumpoint, the table populates the hostname of the host system, as well as that system's public and private IP addresses. This information can help you locate the Jumpoint's host system in case you need to change the Jumpoint's configuration.*

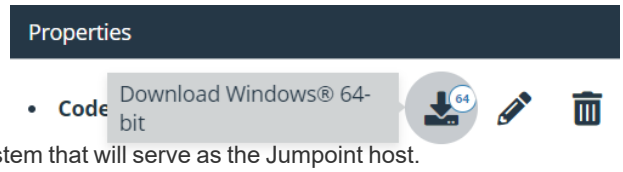
***Note:** At the bottom of the **Jumpoint** page is the option to **Enable network browsing**. If checked, a permitted user can view and select systems from the network directory tree. If unchecked, a user can access a system through a Jumpoint only by entering the system's hostname or IP address. Either way, the user must provide valid credentials to the remote system before gaining access.*

For more information on Shell Jump, please see "Shell Jump" on page 22.

Download

Now that your Jumpoint is configured, you must install the Jumpoint on a single system in the remote network you wish to access. This system serves as the gateway for Jump sessions with other computers on the remote network. You can either install the Jumpoint directly to the host or email the installer to a user at the remote system. If this is to be a clustered Jumpoint, you will be able to add nodes later.

1. From the table, find the appropriate Jumpoint and click the link to download the installer file (**bomgar-jpt-{uid}.exe**).
2. If you are logged into the system you want to use as the Jumpoint host, you can run the installation file immediately.
3. Otherwise, save the file and then transfer it to and deploy it onto the system that will serve as the Jumpoint host.



***Note:** If you need to change the Jumpoint's host system, click **Redeploy**. This uninstalls the Jumpoint from its current location and makes the download links available. You can then install the Jumpoint on a new host. The new Jumpoint replaces the old one for any existing Jump shortcuts that are associated with it. The new Jumpoint does not copy over the configuration from the old Jumpoint and must be reconfigured during installation.*

***Note:** The Jumpoint EXE installer can be deployed through a command line interface or a systems management utility, such as Microsoft Intune. When deploying an EXE installer, the **/S** option can be specified for a silent installation, without any user interaction on the target system. When the **/S** option is used, the Jumpoint installer uses the default installation options.*

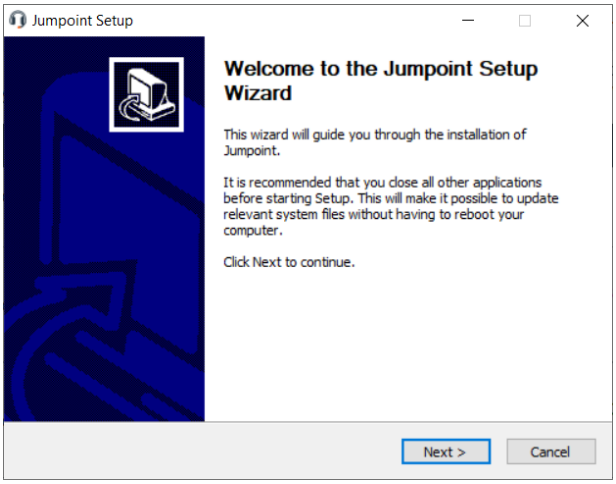
Example:

```
bomgar-jpt-24cf209c6aab939fc418813b9723995ev.exe /S
```

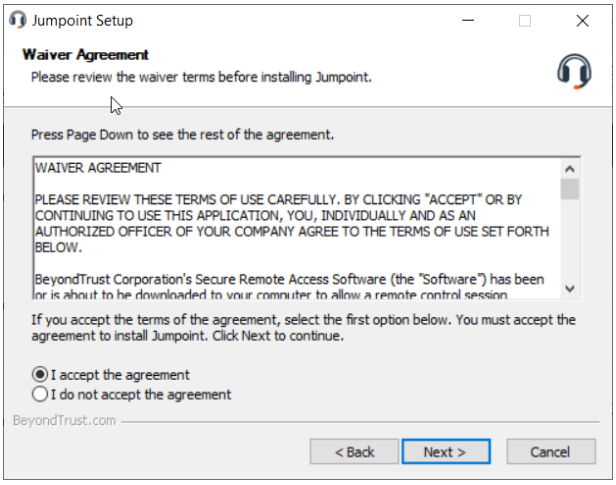
***Note:** The Jumpoint installer expires 7 days after the time of download.*

Install

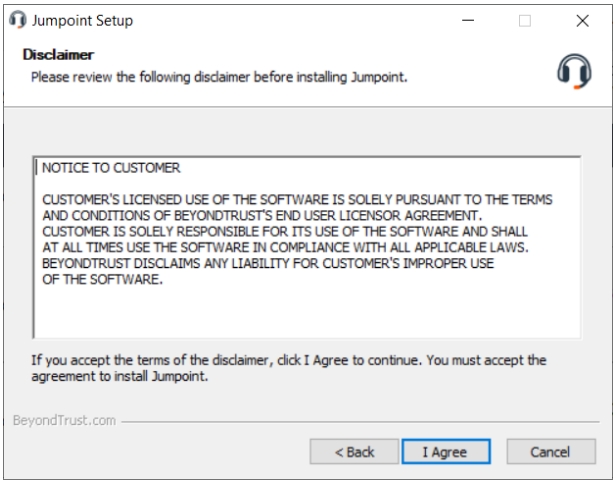
1. From the system that will host the Jumpoint, run the installation package. When the installation wizard appears, click **Next**.



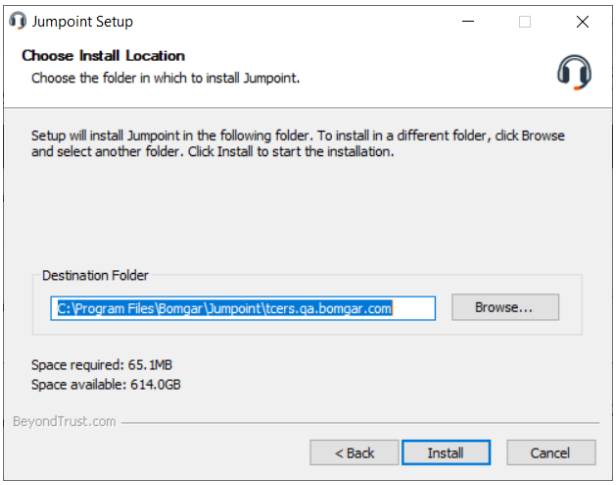
2. Read and accept the waiver agreement. You must accept the agreement to be able to proceed with the installation.



3. Read and agree to the disclaimer.



4. Choose where you would like the Jumpoint to install. The default location is **C:\Program Files\Bomgar\Jumpoint** or **C:\Program Files (x86)\Bomgar\Jumpoint**.
5. Click **Install**. If you are installing a single Jumpoint, the **BeyondTrust Jumpoint Configuration** window opens after a moment. If you are installing a clustered Jumpoint node, the installation finishes.

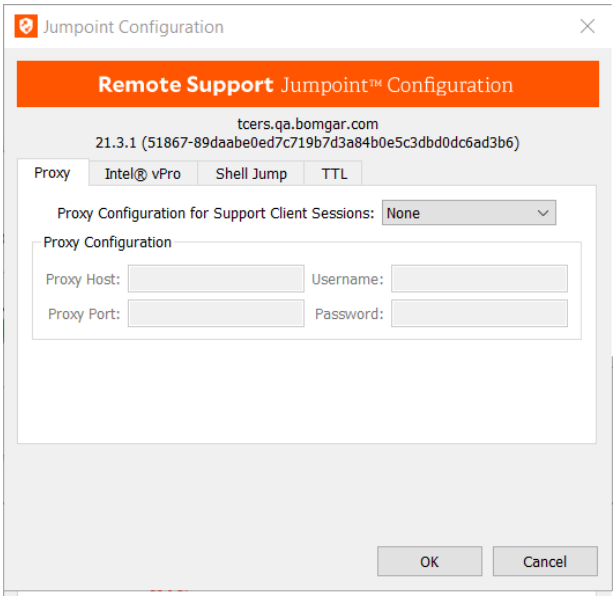


Deploy Behind Proxy

> ***Note:*** *In the case of clustered Jumpoints, keep in mind that there is no customization available at the local level. As a result, you will not see the configuration window that allows for Proxy or other configuration items available for stand-alone Jumpoints. If you are installing a clustered Jumpoint, you may skip the following steps and go directly to* *"Clustered Jumpoint Setup: Adding Nodes" on page 28**.*

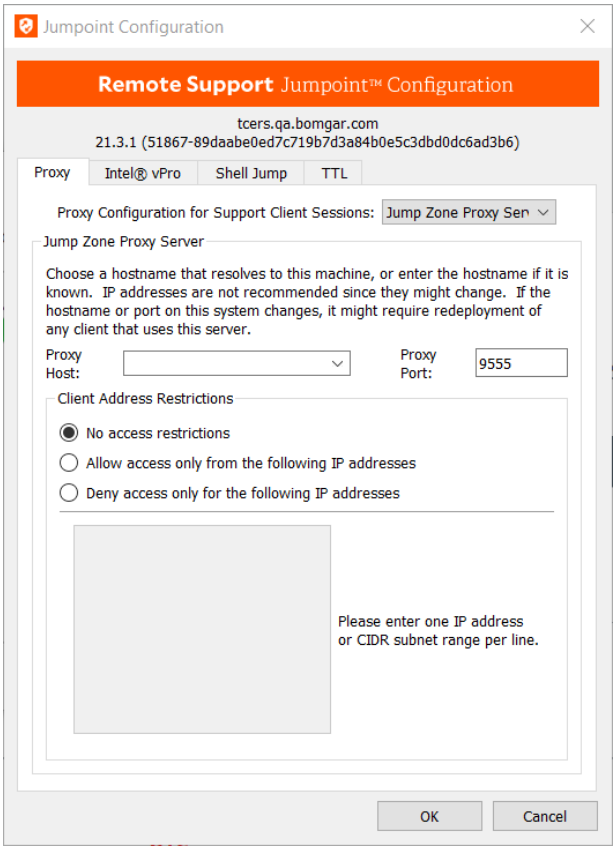
For a Jumpoint to be deployed on a remote network that is behind a proxy, appropriate proxy information may be necessary for the Jumpoint to connect back to the B Series Appliance.

1. From the dropdown on the **Proxy** tab in the **Jumpoint Configuration** application, select **Basic** or **NTLM** to configure proxy settings.
2. Enter the **Proxy Host**, **Proxy Port**, **Username**, and **Password**, and then click **OK**. The Jumpoint supplies this proxy information whenever Jumping to another system on the remote network, providing the credentials necessary to download and run the customer client on the target system.



Configure Windows Jumpoint as a Proxy Server

You can set up this Jumpoint to function as a proxy itself by selecting **Jump Zone Proxy Server** from the dropdown on the **Proxy** tab in the **Jumpoint Configuration** application. With **Jump Zone Proxy Server** selected, this Jumpoint can be used to proxy connections for customer clients and Jump Clients on the network that do not have a native internet connection, such as POS systems. Using a Jumpoint as a proxy routes traffic only to the B Series Appliance. If there is a direct connection available, clients attempt to use that connection in preference to the Jump Zone Proxy.



> *For more information on deploying Jump Clients, see the Jump Client Guide at www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.*

> ***Note:** In order for a Jumpoint to function as a Jump Zone Proxy Server, its host system cannot reside behind a proxy. The Jumpoint must be able to access the Internet without having to supply proxy information for its own connection.*

1. Enter the hostname to use at the listening interface, and set which port to use.

IMPORTANT!

Host and port fields should be set carefully since any Jump Client deployed using this Jumpoint as a proxy server uses the settings available to it at the time of deployment and is not updated should the host or port change. If the host or port must be changed, the Jump Client must be redeployed.

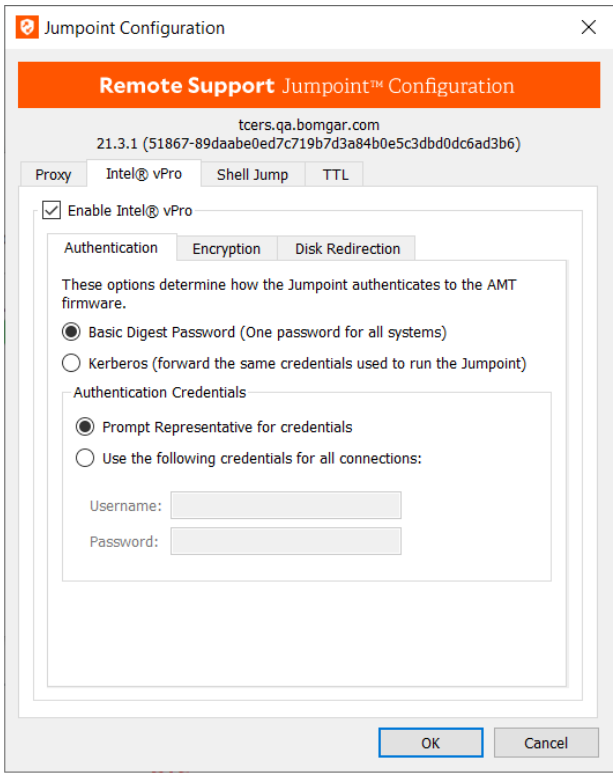
2. Set whether to allow all IP addresses or to limit the IPs that can connect through this proxy.
3. If allowing or denying access, enter one IP address or CIDR subnet range per line.

> ***Tip:** It is a best practice to make an exception in the Windows firewall for the port on which the proxy server listens for the process which accepts connections.*

Intel® vPro

> ***Note:** Intel vPro configuration is available only for stand-alone Jumpoints. Clustered Jumpoints do not have this option.*

Using Intel® Active Management Technology, privileged users can support fully provisioned Intel vPro Windows systems below the OS level, regardless of the status or power state of these remote systems. Configure this Jumpoint to enable vPro connection by going to the **Intel® vPro** tab and checking **Enable Intel® vPro**.



> ***Note:*** *For a representative to use Intel® vPro support, they must be granted access to a Jumpoint with Intel® vPro enabled and must have the user account permission* ***Allowed Jump Methods: Intel® vPro****.*

Authentication

1. Under **Authentication**, designate how the Jumpoint should attempt to authenticate to vPro-provisioned computers. Regardless of the authentication method, the provided credentials must match the authentication settings in the AMT firmware on the vPro systems.
2. To require representatives to provide credentials each time they connect to a vPro computer, select **Basic Digest Password** and then **Prompt Representative for credentials**.

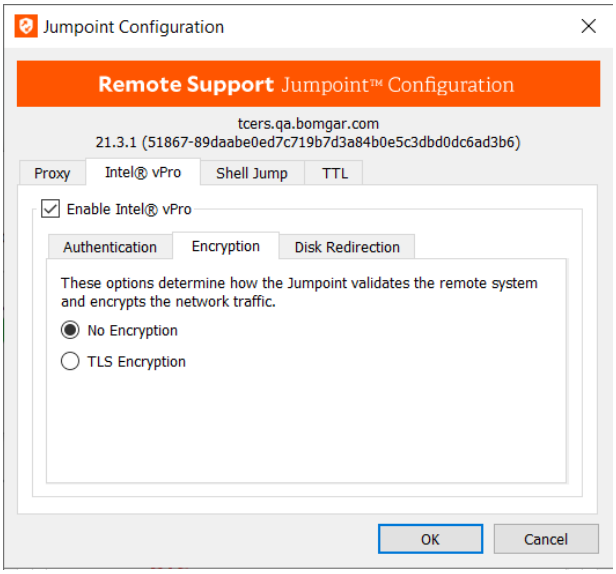
   Prompting for credentials is useful if the vPro systems on this network do not share a common username and password. However, since the vPro AMT firmware is entirely separate from any user accounts on the computer, administrators frequently provision all vPro systems to have the same credentials.

> ***Note:*** *There is little security risk in storing credentials in the Jumpoint. To use vPro support, a representative must have not only the vPro user account privilege but also access to the vPro-enabled Jumpoint. Therefore, prompting for credentials may be an unnecessary measure.*

3. If the same credentials are used for all vPro systems on the network, you can select **Basic Digest Password** and then **Use the following credentials for all connections**. With this configuration, representatives are never prompted for vPro credentials; the Jumpoint automatically supplies the stored username and password for all vPro connections.
4. If you select **Kerberos**, the Jumpoint supplies the credentials for the account that the Jumpoint service is running as. These credentials can be modified to be a specific account that has permissions to access the AMT system. This configuration assumes that the account hosting the Jumpoint uses the same credentials as all provisioned vPro systems to which you wish to connect. With this configuration, representatives are never prompted for vPro credentials.

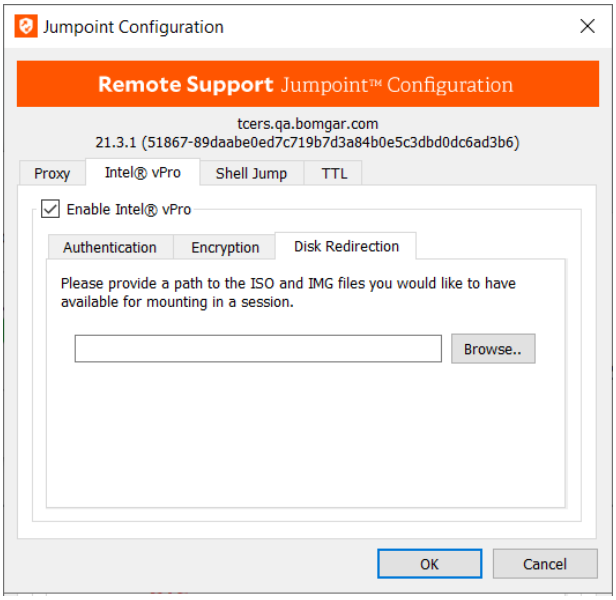
Encryption

5. On the **Encryption** tab, set how the Jumpoint encrypts vPro network traffic.
6. If the remote vPro systems are provisioned not to use TLS encryption, simply select **No Encryption**.
7. Otherwise, select **TLS Encryption** and define the path to the Base 64-encoded CER file which contains the certificates used during the provisioning of the remote vPro systems.



Disk Redirection

8. Under **Disk Redirection**, specify the folder location of any ISO or IMG disk images you would like to make available for mounting in a vPro session. Representatives can use these files for IDE-R, booting the remote vPro system to a disk image rather than the hard drive.

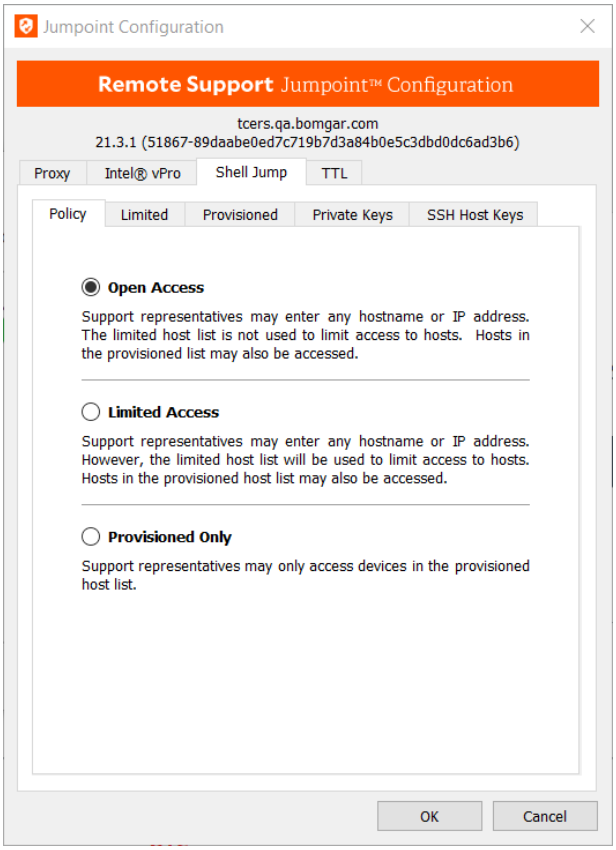


Shell Jump

> ***Note:*** *While Shell Jump can be enabled and disabled from* ***/login*** *for both stand-alone Jumpoints and clustered Jumpoints, further configuration is available only to stand-alone Jumpoints; therefore, this section of the guide applies to stand-alone Jumpoints only.*

The **Shell Jump** tab determines how this Jumpoint can be used to connect to SSH-enabled and Telnet-enabled network devices.

> ***Note:*** *Shell Jump must also be enabled on the* ***Jump > Jumpoint*** *page of the administrative interface. For a representative to use Shell Jump, they must be granted access to a Jumpoint with Shell Jump enabled and must have the user account permission* ***Allowed Jump Methods: Shell Jump****.*



Policy

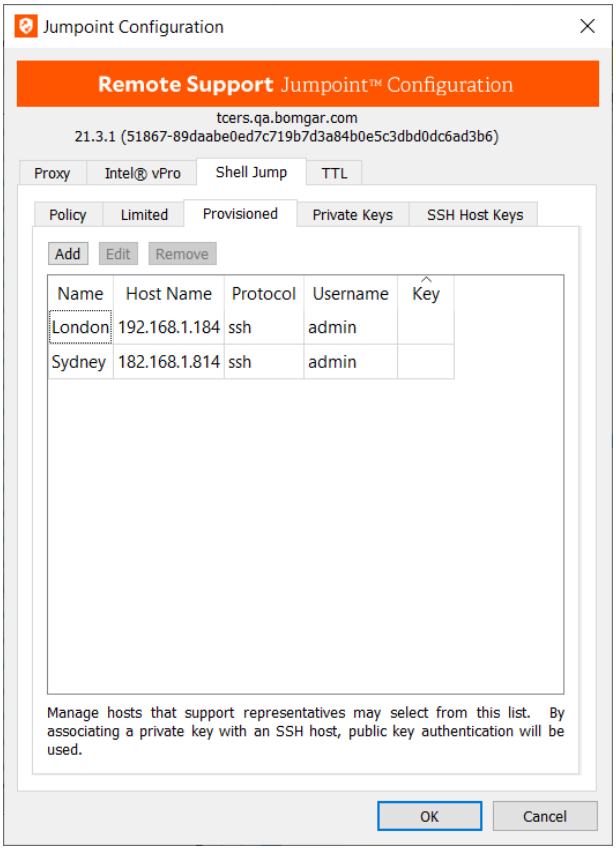
1. On the **Policy** tab, if **Open Access** is selected, permitted representatives can Shell Jump to any remote device by entering its hostname or IP address or by selecting it from a list of provisioned devices.
2. If **Limited Access** is selected, representatives can Shell Jump to provisioned devices or can enter a device's hostname or IP address, provided that it falls within the parameters set by the host list on the **Limited** tab.
3. If **Provisioned Only** is selected, representatives can Shell Jump only to provisioned devices.

Limited

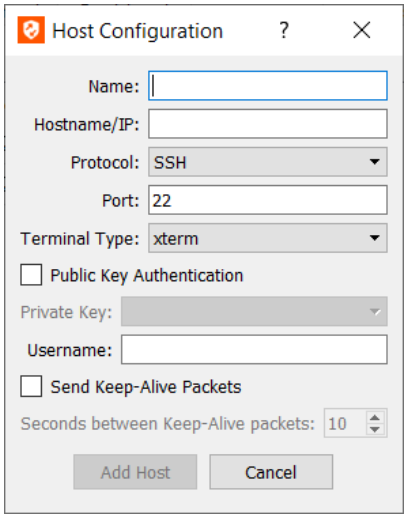
4. If limited access is enabled on the **Policy** tab, the **Limited** list accepts IP addresses and CIDR subnet masks to which Shell Jump access is limited.

Provisioned

5. Configure access to provisioned Shell Jump targets by going to the **Provisioned** tab and clicking **Add**.

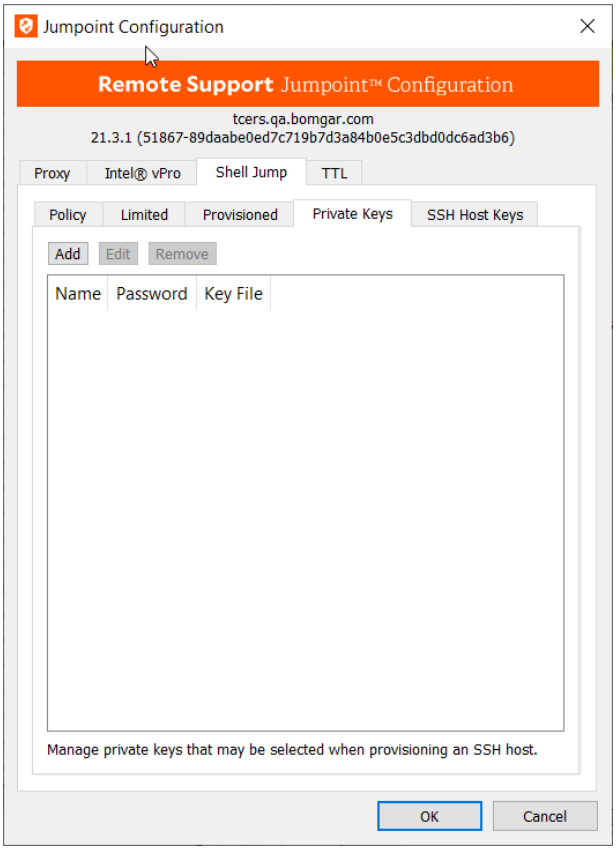


6. Enter a **Name** to help representatives identify this device when starting a Shell Jump session with it.
7. Enter the device's hostname or IP address.
8. Choose the **Protocol** to use, either **SSH** or **Telnet**.
9. **Port** automatically switches to the default port for the selected protocol but can be modified to fit your network settings.
10. Select the **Terminal Type**, either **xterm** or **VT100**.
11. If you are using SSH, you can choose to use **Public Key Authentication**. If you choose to do so, select a **Private Key** to use. Private keys are configured from the **Private Keys** tab.
12. Representatives Shell Jumping to this provisioned device may connect only with the **Username** you provide.
13. You can also select to **Send Keep-Alive Packets** to keep idle sessions from ending. Enter the number of seconds to wait between each packet send.

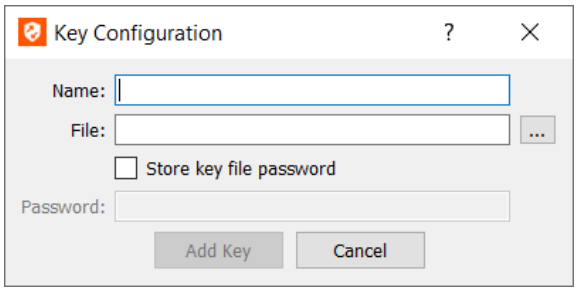


Private Keys

14. If you are using SSH, you can upload a key file to use by going to the **Private Keys** tab and clicking **Add**.

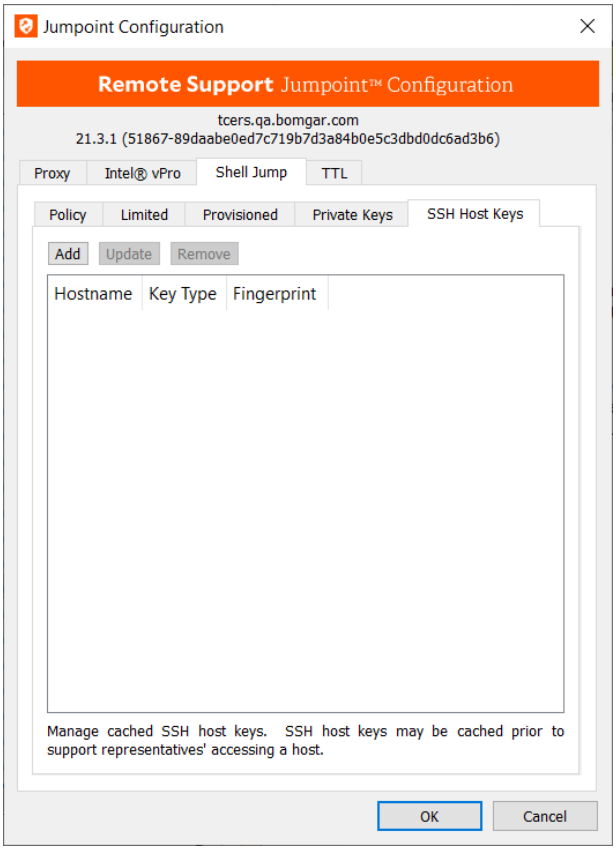


15. Give this key a **Name** and click the ellipsis to browse to the key **File** you wish to use. Keys must be in OpenSSH format. The ssh-keygen utility can be used to generate an OpenSSH format key file if needed.
16. If a **Password** is required, you can check **Store key file password** to save the password for all representatives to use, or you can require representatives to enter the key file password each time they connect to a provisioned device using this key.

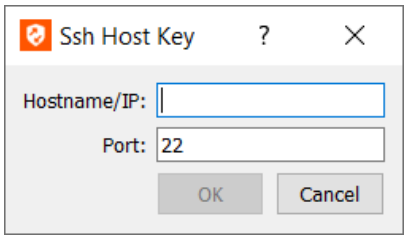


SSH Host Keys

17. You can add **SSH Host Keys** prior to a representative's Jumping to that host. If no host key is cached, the representative receives a message alerting them that the server's host key is not cached and that there is no guarantee that the server is the computer they think it is. Caching a server's host key prior to connection can help prevent confusion.

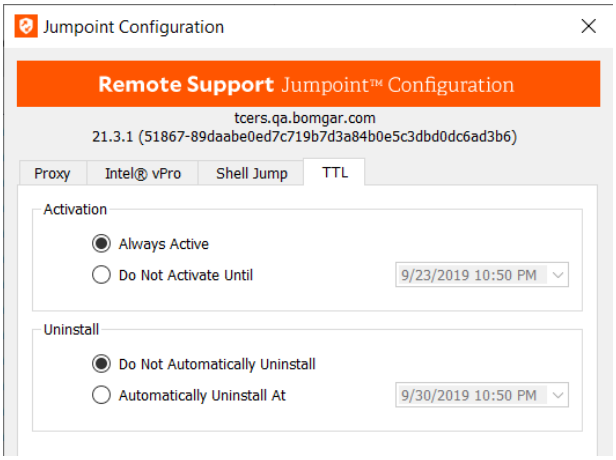


18. Enter the **Hostname** or **IP** address.
19. Enter the **Port** the device uses.
20. The server then returns its host key, which you should verify.
21. Click **Update** to poll the device for its host key; the device lets you know if the host key has changed.



TTL

> ***Note:*** *TTL configuration is available only for stand-alone Jumpoints. Clustered Jumpoints do not have this option.*

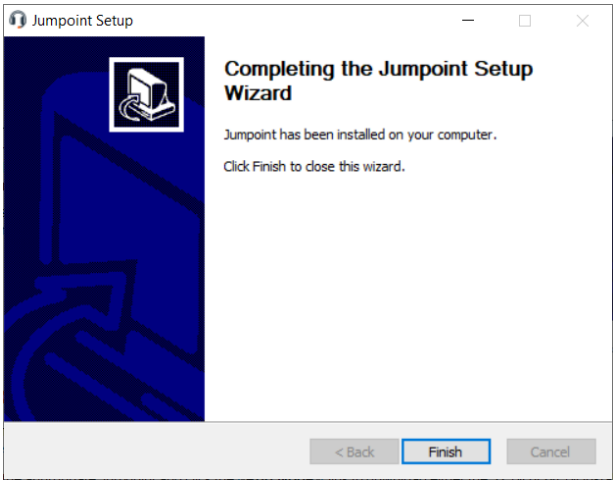


A date and time can be set to specify when the Jumpoint should become active and when it should automatically uninstall. Setting these delimiters determines the duration of time for which users can access the remote network through this Jumpoint.

1. To activate this Jumpoint as soon as its setup is complete, select **Always Active**.
2. Alternatively, select **Do Not Activate Until**, and then set a date and time upon which this Jumpoint should become active.
3. To keep this Jumpoint available without a designated uninstall date, select **Do Not Automatically Uninstall**.
4. Otherwise, select **Automatically Uninstall At**, and then set a date and time upon which this Jumpoint should uninstall itself.

Jumpoint Setup Completion and Revision

After installing the Jumpoint, you receive a confirmation message. Click **Finish**.



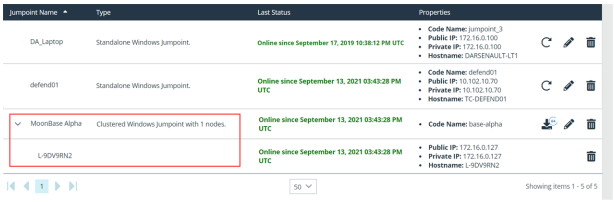
If you installed a stand-alone Jumpoint, the configuration options can be modified by locating the **Bomgar** folder in the Windows **All Programs** or **Programs and Features** menu, opening the site subfolder, and running **BeyondTrust Jumpoint Configuration**.

If you installed a clustered Jumpoint, selecting the **BeyondTrust Jumpoint Configuration** item on the start menu of the Jumpoint host does not result in a configuration window, and only an **About** box is shown

Clustered Jumpoint Setup: Adding Nodes

The steps for creating a clustered Jumpoint in /login are the same as for one that is stand-alone, with only one difference: once you have created the clustered Jumpoint, you can add nodes to it. At least one node needs to be installed for the Jumpoint to be online.

1. From the administrative interface, go to **Jump > Jumpoint**.
2. From the table of existing Jumpoints, find the appropriate Jumpoint and click the **Add Node** link to download the installer file (**bomgar-jpt-{uid}.exe**).
3. If you are logged into the system you want to use as the Jumpoint host, you can run the installation file immediately.
4. Otherwise, save the file and then transfer it to and deploy it onto the system that will serve as the Jumpoint host.
5. Follow the prompts and install the node. Note that there are no configuration screens of any kind.
6. In the Jumpoint table, the clustered Jumpoint now shows information about each installed node, including public and private IP addresses and online or offline status.



Nodes can be deleted but cannot be individually edited. In the representative console, none of the nodes are visible; only the clustered Jumpoint under which they are installed is visible. Nodes function as redundant connection points. When a user needs to use the Jumpoint, one of the nodes is selected randomly. At least one node must be online for the Jumpoint to work.

Configure and Install a Jumpoint for Linux Systems

Linux Jumpoints can be used for the following session types:

- RDP
- SSH/Telnet
- VNC

Setup of a Jumpoint on a remote network is a multi-step process that includes ensuring dependencies are met, configuring from the /login administrative interface, downloading the installer, and running the installation wizard.

Install Dependencies

Several Linux libraries must be installed on the Jumpoint host. Exact requirements depend on the distribution of Linux, however the following libraries are recommended.

- libopengl0
- libglx0
- libxkbcommon-dev
- libfontconfig
- libx11 (for X server). X server does not need to be running.

Note: *If the Jumpoint installation fails due to missing libraries, the error message includes information on what is missing.*

For more information about X servers, please see What is X11? at https://developer.ibm.com/tutorials/l-lpic1-106-1/ or other online resources.

Understand Clustered Jumpoints

Before configuring a Jumpoint, it is important to understand the difference between clustered Jumpoints and stand-alone Jumpoints, because they have different feature sets and because a clustered Jumpoint cannot be converted to stand-alone, nor a stand-alone Jumpoint converted to clustered. A clustered Jumpoint allows you to install up to ten redundant nodes of the same Jumpoint on different host systems in the same local network.

A clustered Jumpoint is available as long as at least one of the installed nodes is online. This provides redundancy, preventing the failure of all Jump Items associated with the failure of a single, stand-alone Jumpoint, and improves load balancing across the system.

All configuration of clustered Jumpoints is done in **/login**, with no local configuration available on the local host either during or after the installation. This means that if you install a clustered Jumpoint, selecting the **BeyondTrust Jumpoint Configuration** item on the start menu of the Jumpoint host does not result in a configuration window, and only an **About** box is shown. Editing a clustered Jumpoint in **/login** loads the same configuration page that was used to create the Jumpoint. This means clustered Jumpoint configuration lacks the following options which are available to stand-alone Jumpoints:

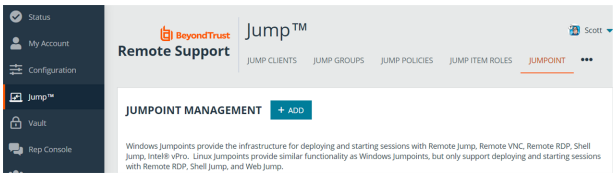
- Proxy
- Intel vPro

- Shell Jump
- TTL

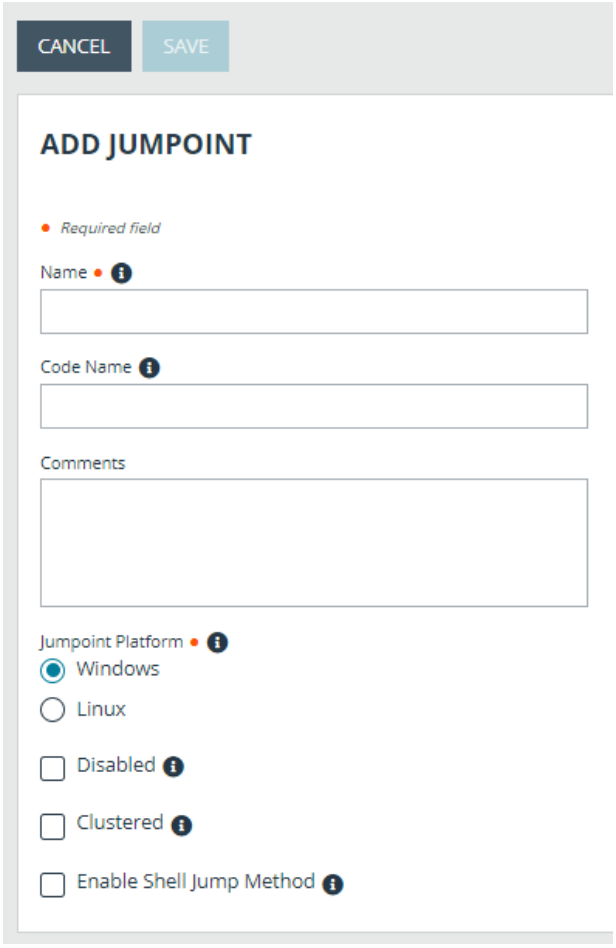
This also means that a clustered Jumpoint cannot be configured as a Jump Zone Proxy. vPro, RDP, VNC, Shell Jump, and normal Jump sessions are all supported when using clustered Jumpoints; however, the advanced configuration of these features is not available. This includes settings such as provisioned SSH hosts, vPro reimaging, Jump Zone Proxy, TTL, etc.

Configure

1. From the administrative interface, go to **Jump** > **Jumpoint**.
2. Click **Add**.



3. Create a unique name to help identify this Jumpoint. This name should help users locate this Jumpoint when they need to start a session with a computer on its same network.
4. Set a code name for integration purposes. If you do not set a code name, one is created automatically.
5. Add comments to help identify this Jumpoint.
6. Select the **Jumpoint Platform**. Options are **Windows** and **Linux**. Once the Jumpoint has been created, this setting cannot be changed.
7. Leave the **Disabled** box unchecked.
8. Check the **Clustered** box, if appropriate.



> ***Note:*** *A* ***Clustered*** *Jumpoint allows you to install multiple, redundant nodes of the same Jumpoint on different host systems. If you select this option, the Jumpoint is available as long as at least one of the installed nodes is online. This provides redundancy, preventing the failure of all Jump Items associated with the failure of a single, standalone Jumpoint, and improves load balancing across the system. Once created, a clustered Jumpoint cannot be converted to standalone, nor a standalone Jumpoint converted to clustered.*

Note: *Linux Jumpoints can only be used for RDP, SSH/Telnet, and VNC sessions, allowing for credential injection from user or Vault, as well as RemoteApp functionality and Shell Jump filtering. Clustered Jumpoints can only add new nodes of the same OS. You cannot mix Windows and Linux nodes.*

IMPORTANT!

Jumpoint cluster nodes must be installed on hosts residing in the same local area network.

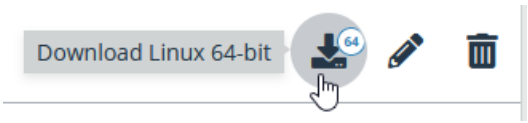
9. If you want users to be able to connect to SSH-enabled and Telnet-enabled network devices through this Jumpoint, check **Enable Shell Jump Method**.
10. From the Jumpoint edit page, you can authorize users to start sessions through this Jumpoint. After the Jumpoint has been created, you can also grant access to groups of users from **Users & Security** > **Group Policies**.
11. Save the configuration. The new Jumpoint appears in the list of configured Jumpoints.

Note: *Once you have installed the Jumpoint and started it for the first time, the table populates the hostname of the host system, as well as that system's public and private IP addresses. This information can help you locate the Jumpoint's host system in case you need to change the Jumpoint's configuration.*

Download

Now that the Jumpoint is configured, you must install the Jumpoint on a single system in the remote network you wish to access. This system serves as the gateway for Jump sessions with other computers on the remote network. You can either install the Jumpoint directly to the host or email the installer to a user at the remote system. If this is to be a clustered Jumpoint, you add nodes after the Jumpoint is installed.

1. From the table, find the appropriate Jumpoint and click the link to download the installer file.
2. If you are logged into the system you want to use as the Jumpoint host, you can run the installation file immediately.
3. Otherwise, save the file and then transfer it to and deploy it onto the system that will serve as the Jumpoint host.



Note: *If you need to change the Jumpoint's host system, click* ***Redeploy****. This uninstalls the Jumpoint from its current location and makes the download links available. You can then install the Jumpoint on a new host. The new Jumpoint replaces the old one for any existing Jump shortcuts that are associated with it.*

Install

1. Once the installer file is on the remote system, use a command interface to install the file and specify any desired parameters. The Jumpoint must be installed within 7 days of downloading it. The exact install process depends on the Linux distribution and version, but general steps are provided below.
    - Install the Jumpoint using **--install-dir <path>**. You must have permission to write to this location, and the path must not already exist.

```
sh ./bomgar-jpt-{uid}.bin --install-dir /home/username/jumpoint
```

- 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 Jumpoint installs under the user context that is currently running.

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

IMPORTANT!

*We do not recommend installing the Jumpoint 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*

2. After installing the Jumpoint, you must start its process.

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

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

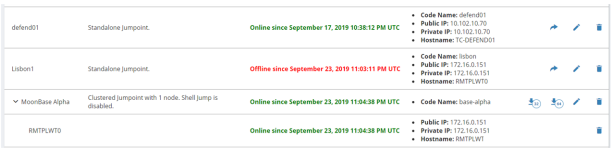
3. You must also arrange for **init-script start** to run at boot in order for the Jumpoint to remain available whenever the system restarts. An example **system.d** service displays once the Jumpoint is installed. Copy this information and create the new service for the Jumpoint, **filename.service** (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:
        - Run **sudo systemctl start filename.service** to start the service file.
        - Run **sudo su -** to get to root.
        - Run **systemctl enable filename.service** to enable the service file, so the Jumpoint service will automatically start after every reboot.
        - Reboot the Jumpoint machine.
4. To remove the files, use the **uninstall.sh** script included in the installation.

***Note:** If the Jumpoint installation fails due to missing libraries, the error message includes information on what is missing.*

Clustered Jumpoint Setup: Adding Nodes

The steps for creating a clustered Jumpoint in /login are the same as for a standalone, with one difference: once you have created the clustered Jumpoint, you add nodes to it. At least one node needs to be installed for the Jumpoint to be online.

1. From the administrative interface, go to **Jump** > **Jumpoint**.
2. From the table of existing Jumpoints, find the appropriate Jumpoint and click the **Add Node** link to download the installer file (**bomgar-jpt-{uid}.bin**).
3. If you are logged into the system you want to use as the Jumpoint host, you can run the installation file immediately.
4. Otherwise, save the file and then transfer it to and deploy it onto the system that will serve as the Jumpoint host.
5. Install the node following the same steps for "Install" on page 31, as above.
6. In the Jumpoint table, the clustered Jumpoint now shows information about each installed node, including public and private IP addresses and online or offline status.



Nodes can be deleted but cannot be individually edited. In the representative console, none of the nodes are visible; only the clustered Jumpoint under which they are installed is visible. Nodes function as redundant connection points. When a user needs to use the Jumpoint, one of the nodes is selected randomly. At least one node must be online for the Jumpoint to work.

Configure Linux Jumpoint as a Proxy Server

You can set up a Linux Jumpoint to function as a proxy server so it can be used for proxy connections for clients on the network that do not have a native internet connection, such as POS systems. Using a Jumpoint as a proxy routes traffic only to the B Series Appliance.

To configure proxy settings on a Linux Jumpoint, modify the **jumpzone.ini** file, which is located in the directory where you installed the Jumpoint. Below is the content of the **jumpzone.ini** file, which includes all of the applicable settings and a description of each:

```
[General]
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; BeyondTrust Jump Zone Proxy Configuration ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; ALL configuration changes require a restart
; of the Jumpoint process/service/daemon

; * Enable the Jump Zone Proxy feature
; * Default is disabled.
;enable_proxy=1

; * Allow HTTP GET requests through the proxy
; * to the BeyondTrust appliance.
; * Default is to not allow HTTP GET requests.
;allow_http=1

; * Hostname or IP that resolves to this machine
; * Jump Clients will be deployed with and use
; * this information to connect back to this machine
; * Default hostname is detected using gethostname(2)
;proxy_host=myhost.local
```

```
; * Port number on this machine that should
; * listen for incoming Jump Client connections
; * Default port is 9995
;proxy_port=9995

; * Comma seperated IP addresses or CIDR subnets
; * that incoming connections should be restricted to.
; * Default is allow all connections.
; * Only one of allowOnlyIPs or denyOnlyIPs may be used.
;allowOnlyIPs=1.2.3.4,4.3.2.1/16

; * Comma seperated IP addresses or CIDR subnets
; * that should be denied incoming connections.
; * Default is allow all connections.
; * Only one of allowOnlyIPs or denyOnlyIPs may be used.
;denyOnlyIPs=1.2.3.4,4.3.2.1/16
```

Note: *In order for a Jumpoint to function as a Jump Zone Proxy Server, its host system cannot reside behind a proxy. The Jumpoint must be able to access the Internet without having to supply proxy information for its own connection.*

IMPORTANT!

The proxy host and port should be set carefully since any Jump Client deployed using this Jumpoint as a proxy server uses the settings available to it at the time of deployment and are not updated should the host or port change. If the host or port is changed, the Jump Client must be redeployed.

Tip: *It is a best practice to make an exception in the firewall for the port on which the proxy server listens for the process to accept connections.*

Use a Jumpoint to Jump to a Remote System

Once a Jumpoint has been installed on a remote network, permitted representatives can use the Jumpoint to initiate sessions with Windows and Linux computers on that same network, even if those computers are unattended. Additionally, a permitted representative can Jump to computers on the same network segment as their local system, even without a Jumpoint.

A Jumpoint can be used to start a standard support session, to start a Remote Desktop Protocol session or VNC session, to Shell Jump to a SSH-enabled or Telnet-enabled network device, or to start a session with an Intel® vPro Windows system. Support sessions, RDP sessions, and VNC sessions can also be started with systems on the same network segment.

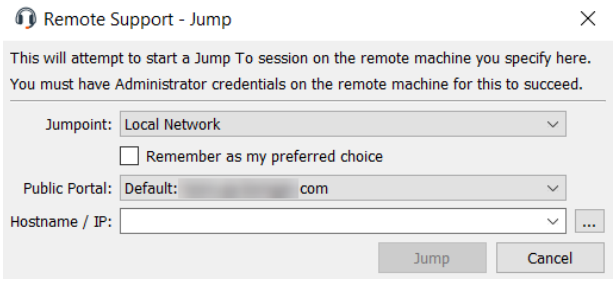
> ***Note:*** *Linux Jumpoints can only be used for RDP and SSH/Telnet sessions.*

Start a Local or Remote Jump Session

To Jump through a Jumpoint, you must have access to a Jumpoint and must have the user account permission **Allowed Jump Methods: Remote Jump**. To Jump on your local network, you must have the user account permission **Allowed Jump Methods: Local Jump**.

To Jump without a pre-installed client, open the **Jump to…** dialog from:

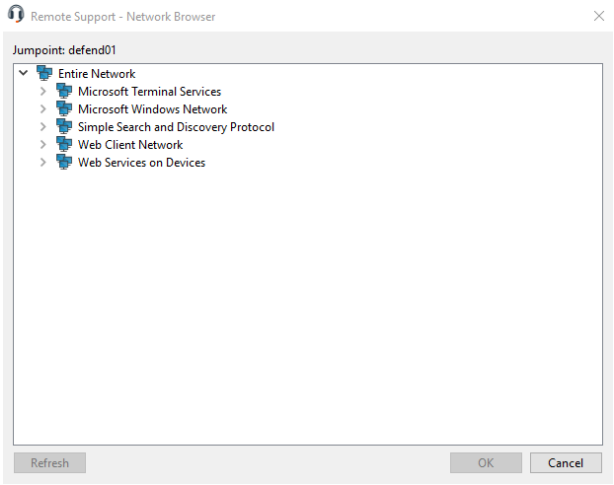
- The **Support** menu of the representative console
- The **Start** button at the top of the representative console
- The **Jump To** button at the top of the representative console
- Or **Create** a Remote Jump in the web rep console



From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. Depending on your account permissions, you can Jump to a system on your local network or to a network on which a Jumpoint is installed.

Select the public portal you wish to associate your session with. This lets the system know what customer agreement behavior should occur.

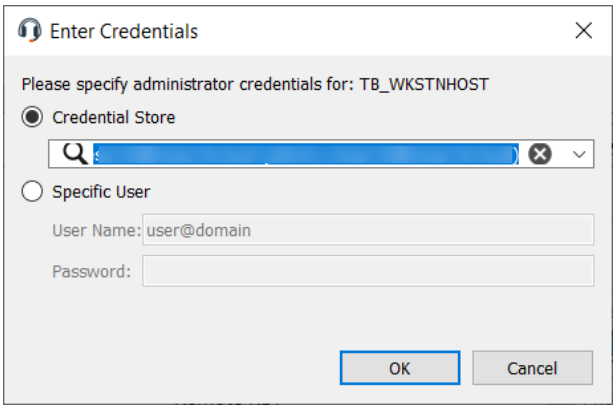
> *For more information, please see Customer Client: Modify the Invitation Email, Display Options, Connection Options at https://www.beyondtrust.com/docs/remote-support/getting-started/admin/customer-client.htm.*



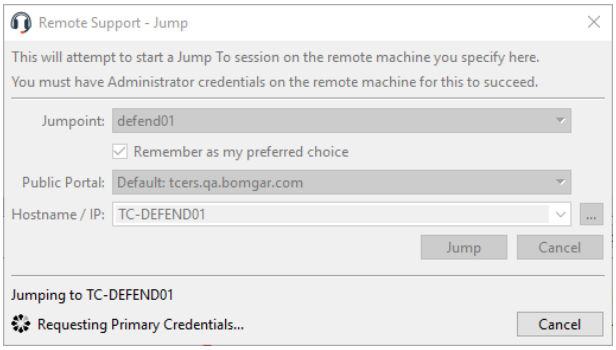
Enter the hostname or IP address of the system you wish to access. Alternatively, if network browsing is enabled from the **/login > Jump > Jumpoint** page, you can click the **[...]** button to browse the directory tree.

Once you have located the computer you wish to access, click **Jump**.

You must provide administrative credentials to the remote computer in order to complete the Jump. The administrative rights must be either a local administrator on the remote system or a domain administrator.



The client files are pushed to the remote system, and a session attempts to start. Depending on the session permissions, the end-user may be prompted to accept or deny the session. If no response is received within a defined interval of time, the session either starts or cancels, again depending on the session permissions.



Note: *If you need to access systems through a Jumpoint when no user is available, make sure the public portal permissions and your account permissions are set either to disable prompting or to default to* ***Allow****.*

Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access. For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.*

Start a Local or Remote RDP Session

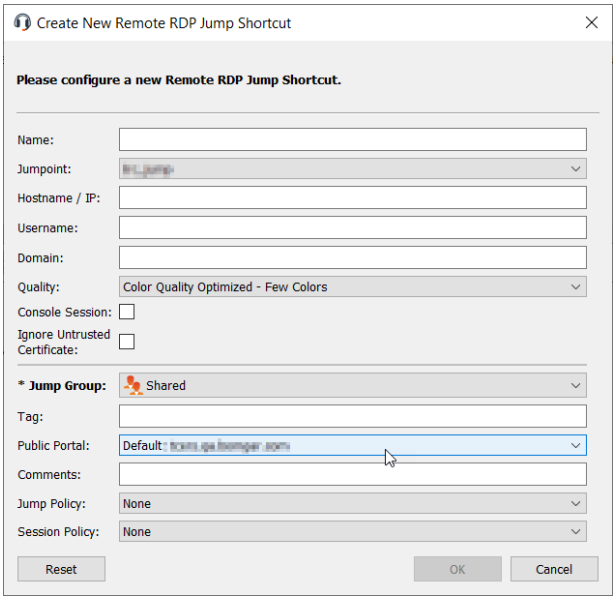
Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a remote Windows or Linux System. Because RDP sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as your administrator has defined for your site.

To use Local RDP through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local RDP**.

To use Remote RDP through BeyondTrust, you must have access to a Jumpoint and must have the user account permissions **Allowed Jump Methods: Remote RDP**.

To start an RDP session, open the **Remote Desktop Protocol** dialog from:

- The **Support** menu of the representative console
- The **RDP** button at the top of the representative console
- Or **Create** a Remote RDP Jump in the web rep console



From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the system you wish to access.

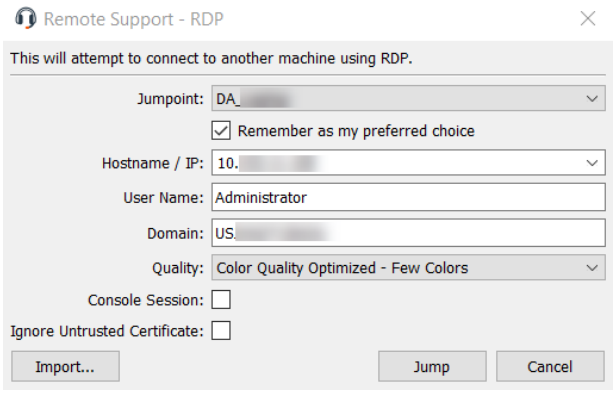
By default, the RDP server listens on port 3389, which is therefore the default port BeyondTrust attempts. If the remote RDP server is configured to use a different port, add it after the hostname or IP address in the form of **<hostname>:<port>** or **<ipaddress>:<port>** (for example, 10.10.24.127:40000).

Provide the **Username** to sign in as, along with the **Domain**.

Select the **Quality** at which to view the remote screen. This cannot be changed during the RDP session. Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select **Video Optimized**; otherwise, select between **Black and White** (uses less bandwidth), **Few Colors**, **More Colors**, or **Full Color** (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.

To start a console session rather than a new session, check the **Console Session** box.

If the server's certificate cannot be verified, you receive a certificate warning. Check **Ignore Untrusted Certificate** to connect to the remote system without seeing this message.



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.

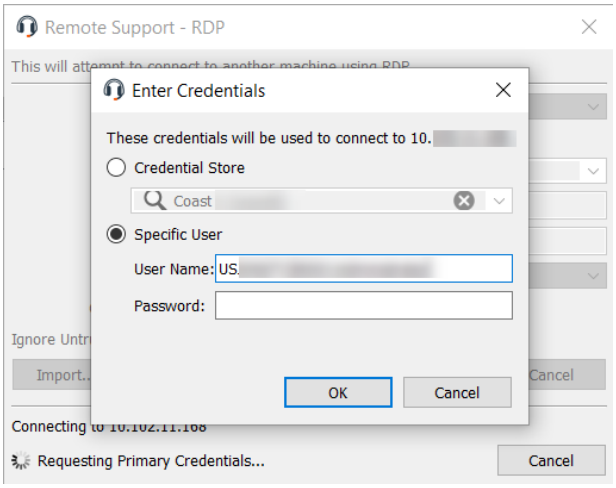
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

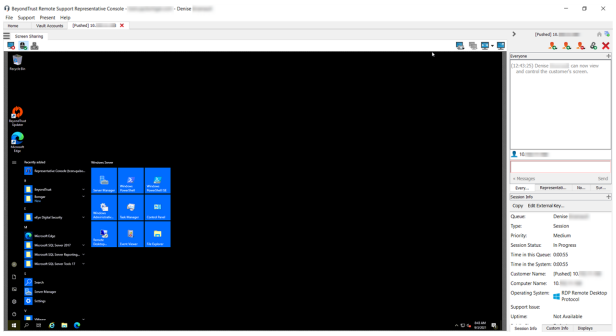
To import an RDP file, click the **Import** button. This prepopulates some of the fields required for the RDP connection.

To begin the RDP session, click **Jump**.

You are prompted to enter the password for the username you specified earlier.



Your RDP session now begins. Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, and share clipboard contents. You can also share or transfer the RDP session with other logged-in BeyondTrust users, following the normal rules of your user account settings.



Multi-Monitor Support

An option allows you to open a Remote Support connection expanded across all the monitors on the client computer regardless of the client monitor configuration. With this feature, you can fully utilize all the monitors connected to the client computer, therefore being able to adjust screen sizing and scaling during an RDP session across multiple monitors.

Note: *If you are using full screen view while using this feature, the remote system is displayed across all of your monitors.*

Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Start New Session****, then a new independent session starts for each user who Jumps to a specific RDP Jump Item. The RDP configuration on the endpoint controls any further behavior regarding simultaneous RDP connections.*

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Start a Local or Remote VNC Session

Use BeyondTrust to start a VNC session with a remote system. Because VNC sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as defined by your administrator for your site.

To use Local VNC through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local VNC**.

To use Remote VNC through BeyondTrust, you must have access to a Jumpoint and must have the user account permission **Allowed Jump Methods: Remote VNC**.

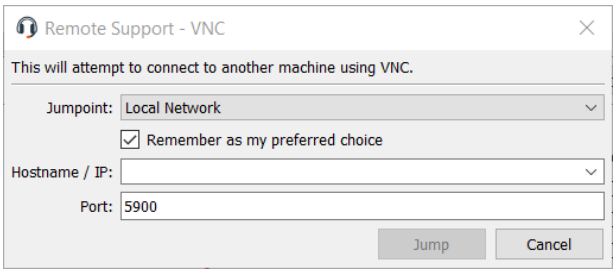
To start a VNC session, open the **VNC** dialog from:

- The **Support** menu of the representative console
- The **VNC** button at the top of the representative console
- Or **Create** a Remote VNC Jump in the web rep console

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the system you wish to access.

By default, the VNC server listens on port 5900, which is, therefore, the default port BeyondTrust attempts. If the remote VNC server is configured to use a different port, enter it in the **Port** field.

To begin the VNC session, click **Jump**.



> ***Note:*** *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access. For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.*

Start a Shell Jump Session

With Shell Jump, quickly connect to an SSH-enabled or Telnet-enabled network device to use the command line feature on that remote system. For example, run a standardized script across multiple systems to install a needed patch, or troubleshoot a network issue.

To perform a Shell Jump through BeyondTrust, you must have access to a Jumpoint with Shell Jump enabled, and you must have the user account permission **Allowed Jump Methods: Shell Jump**.

To start a Shell Jump session, open the **Shell Jump** dialog from:

- The **Support** menu of the representative console
- The **Shell Jump** button at the top of the representative console
- Or **Create** a Shell Jump in the web rep console

Your Jumpoint may be configured for provisioned Shell Jump access only.

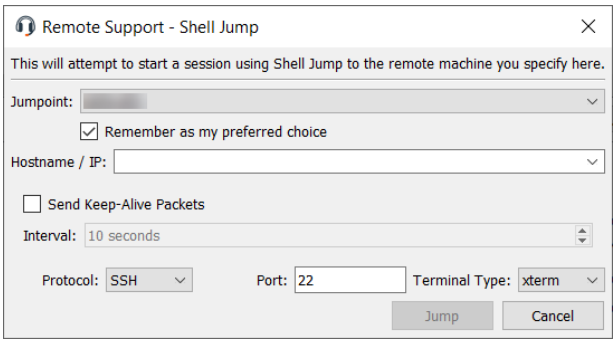
From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Select the provisioned system you wish to access.

Alternatively, your Jumpoint may be configured for open access or limited access.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**.

To access a provisioned system, check **Use Provisioned** and select the system from the dropdown.

Alternatively, enter the **Hostname / IP** of the system you wish to access. If your Jumpoint is configured for limited access, the remote system must be in the delimited IP address range.



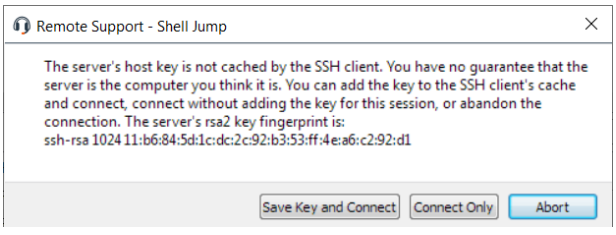
You can choose to **Send Keep-Alive Packets** to keep idle sessions from ending. Enter the number of seconds to wait between each packet sent.

Choose the **Protocol** to use, either **SSH** or **Telnet**.**Port** automatically switches to the default port for the selected protocol but can be modified to fit your network settings.Select the **Terminal Type**, either **xterm** or **VT100**.

Then click **Jump**.

If attempting to Shell Jump to an SSH device without a cached host key, you receive an alert that the server's host key is not cached and that there is no guarantee that the server is the computer you think it is.

If you choose **Save Key and Connect**, then the key is cached on the Jumpoint's host system so that future attempts to Shell Jump to this system do not result in this prompt. **Connect Only** starts the session without caching the key, and **Abort** ends the Shell Jump session.



If you Shell Jump to an SSH device with keyboard interactive MFA enabled, there is a secondary prompt for input.

When you Shell Jump to a remote device, a command shell session immediately starts with that device. If you Shell Jump to a provisioned SSH device with an unencrypted key or with an encrypted key whose password has been cached, you are not prompted for a password. Otherwise, you are required to enter a password. You can then send commands to the remote system.

Start an Intel vPro Session

Using Intel® Active Management Technology, privileged users can support fully provisioned Intel vPro Windows systems below the OS level, regardless of the status or power state of these remote systems. To use Intel vPro, you must have access to a Jumpoint with Intel vPro enabled and must have the user account permission **Allowed Jump Methods: Intel® vPro**.

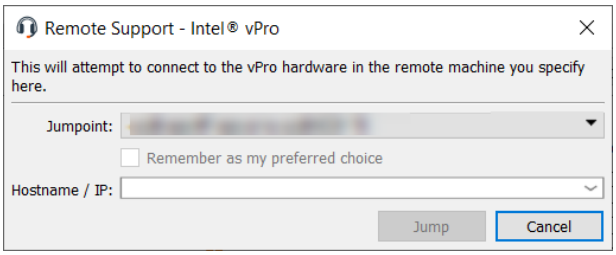
> ***Note:*** *Remote systems using vPro with AMT version 5 or higher may be supported with BeyondTrust.*

> ***Note:*** *While vPro is supported by clustered Jumpoints, configuration options are available only to standalone Jumpoints. Clustered Jumpoints have no configuration options for Intel vPro.*

To start a session with an Intel vPro system, open the **Intel® vPro** dialog from:

- The **Support** menu of the representative console
- The **Intel® vPro** button at the top of the representative console

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. If you generally access the same Jumpoint, check **Remember as my preferred choice**. Enter the **Hostname / IP** of the system you wish to access.

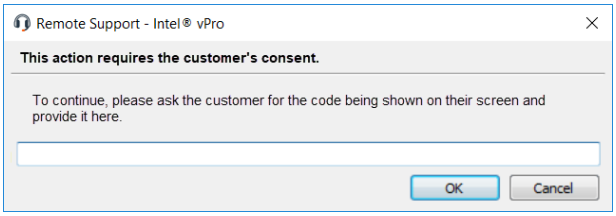


Click **Jump**.

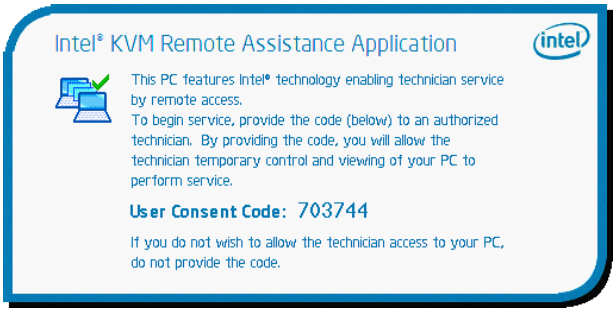
Depending on your Jumpoint setup, you might be prompted to enter a username and password.

The Jumpoint detects the provisioned vPro hardware. If the credentials, provided during either the Jumpoint configuration or the Jump attempt, match the credentials of the vPro-provisioned system, the connection is initiated.

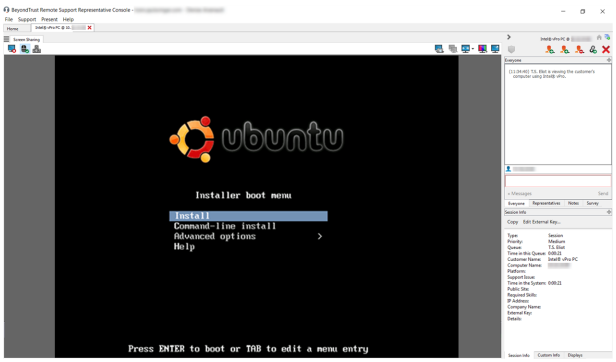
Depending on how the vPro computer is provisioned, you might be prompted to enter a user consent code before performing certain actions.



If a consent code is required, a pop-up appears on the remote screen. An end user must provide you with this code before you can gain hardware access.



Once the connection is made, you have control of the remote vPro hardware. You can then use the vPro session tools to work on the remote system.



Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access. For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.*

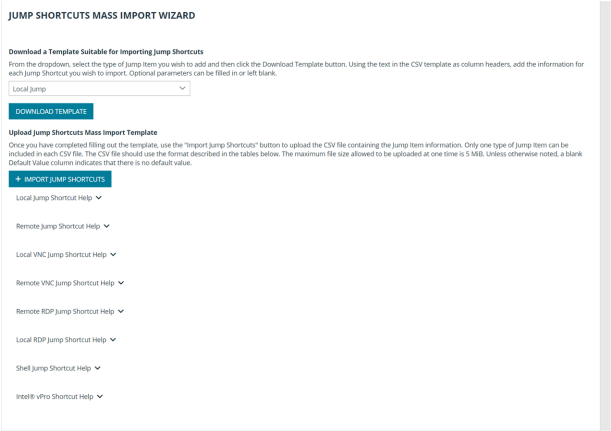
For more information on supporting Intel® vPro systems, see the Representative Guide at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/intel-vpro-support.htm.

Use Jump Shortcuts to Jump to Remote Systems

Create Jump Shortcuts to start standard support sessions, to start Remote Desktop Protocol sessions or VNC sessions, to Shell Jump to SSH-enabled or Telnet-enabled network devices, or to start Intel® vPro sessions.

When creating a large number of Jump shortcuts, it may be easier to import them via a spreadsheet than to add them one by one in the representative console. Go to **/login > Jump > Jump Items**. From the dropdown in the **Jump Shortcuts Mass Import Wizard section**, select the type of Jump Item you wish to add, and then click **Download Template**. Using the text in the CSV template as column headers, add the information for each Jump shortcut you wish to import. If any required fields are missing, import fails. Optional fields can be filled in or left blank.

Once you have completed filling out the template, use **Import Jump Shortcuts** to upload the CSV file containing the Jump Item information. The maximum file size allowed to be uploaded at one time is 5 MB. Only one type of Jump Item can be included in each CSV file. The CSV file should use the format described in the tables below.



Local Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Customer Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is present.
Customer Not Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is not present.

Remote Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Customer Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is present.
Customer Not Present Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item when a customer is not present.

Local VNC Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Port (optional)	A valid port number from **100** to **65535**. Defaults to **5900**.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024

Parameter	Description
	characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote VNC Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Port (optional)	A valid port number from **100** to **65535**. Defaults to **5900**.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated.  ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote RDP Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.

Parameter	Description
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Domain (optional)	The domain the endpoint is on.
Quality (optional)	The quality at which to view the remote system. Can be **low** (2-bit gray scale for the lowest bandwidth consumption), **best_perf** (default - 8-bit color for fast performance), **perf_and_qual** (16-bit for medium quality image and performance), **best_qual** (32-bit for the highest image resolution), or **video_opt** (VP9 codec for more fluid video). This cannot be changed during the remote desktop protocol (RDP) session.
Console Session (optional)	**1**: Starts a console session. **0**: Starts a new session (default).
Ignore Untrusted Certificate (optional)	**1**: Ignores certificate warnings. **0**: Shows a warning if the server's certificate cannot be verified.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Local RDP Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Username (optional)	The username to sign in as.
Domain (optional)	The domain the endpoint is on.
Quality (optional)	The quality at which to view the remote system. Can be **low** (2-bit gray scale for the lowest bandwidth consumption), **best_perf** (default - 8-bit color for fast performance), **perf_and_qual** (16-bit for medium quality image and performance), **best_qual** (32-bit for the highest image resolution), or **video_opt** (VP9

Parameter	Description
	codec for more fluid video). This cannot be changed during the remote desktop protocol (RDP) session.
Console Session (optional)	**1**: Starts a console session. **0**: Starts a new session (default).
Ignore Untrusted Certificate (optional)	**1**: Ignores certificate warnings. **0**: Shows a warning if the server's certificate cannot be verified.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated.  ***Note:*** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Shell Jump Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Protocol	Can be either **ssh** or **telnet**.
Port (optional)	A valid port number from **1** to **65535**. Defaults to **22** if the protocol is **ssh** or **23** if the protocol is **telnet**.
Terminal Type (optional)	Can be either **xterm** (default) or **VT100**.
Keep-Alive (optional)	The number of seconds between each packet sent to keep an idle session from ending. Can be any number from **0** to **300**. **0** disables keep-alive (default).
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated.

Parameter	Description
	Note: *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.

Intel vPro Shortcut Help

Parameter	Description
Hostname	The hostname of the endpoint to be accessed by this Jump Item. This string has a maximum of 128 characters.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Name	Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.
Jump Group	The code name of the Jump Group with which this Jump Item should be associated. **Note:** *When using the import method, a Jump Item cannot be associated with a personal list of Jump Items.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Public Portal (optional)	The public portal through which this Jump Item should connect.

Create and Use Remote or Local Jump Shortcuts

Remote Jump enables a privileged user to connect to an unattended remote computer on a network outside of their own network. Remote Jump depends on a Jumpoint.

A Jumpoint acts as a conduit for access to computers on a known remote network. A single Jumpoint installed on a computer within a LAN is used to access multiple systems, eliminating the need to pre-install software on every computer you might need to access.

Local Jump enables a privileged user to connect to an unattended remote computer on their local network. Within the local area network, the BeyondTrust user's computer can initiate a session to a Windows or Linux system directly without using a Jumpoint.

> ***Note:*** *Remote Jump and Local Jump are available only for Windows systems. Jump Clients are needed for remote access to Mac computers. To Jump to a Windows computer without a Jump Client, that computer must have Remote Registry Service enabled (disabled by default in Vista) and must be on a domain.*

Create a Remote Jump Shortcut

To create a Remote Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote Jump**. Remote Jump shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

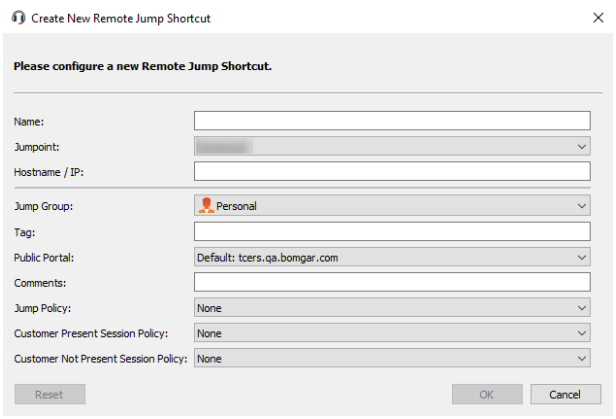
> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

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 a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

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.

Create a Local Jump Shortcut

To create a Local Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Local Jump**. Local Jump shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

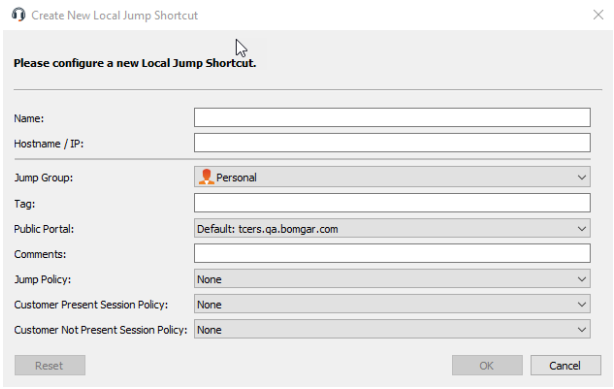
> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

Enter the **Hostname / IP** of the system you wish to access.

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 a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

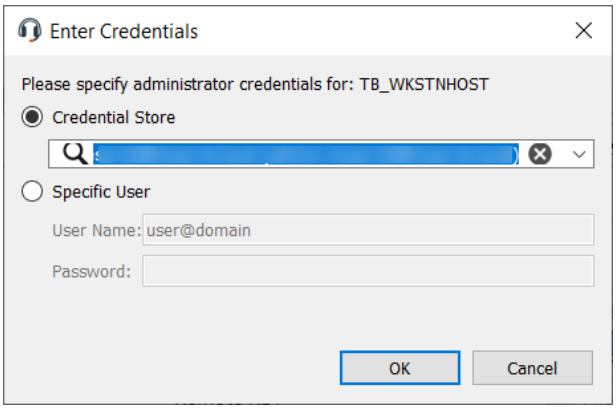
Choose session policies to assign to this Jump Item. Session policies assigned to this Jump Item have the highest priority when setting session permissions. The **Customer Present Session Policy** applies when the end user is determined to be present. Otherwise, the **Customer Not Present Session Policy** 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.

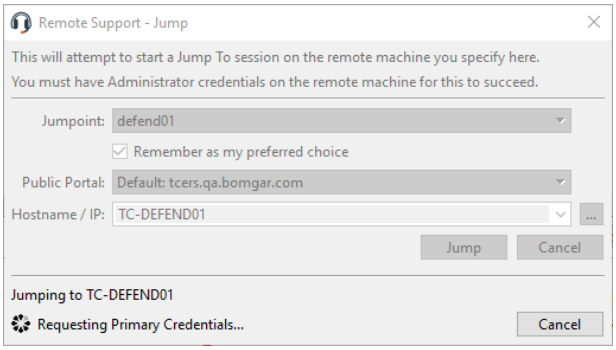
Use a Jump Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

You must provide administrative credentials to the remote computer in order to complete the Jump. The administrative rights must be either a local administrator on the remote system or a domain administrator.



The client files are pushed to the remote system, and a session attempts to start. Depending on the session permissions, the end-user may be prompted to accept or deny the session. If no response is received within a defined interval of time, the session either starts or cancels, again depending on the session permissions.



Note: *If you need to access systems through a Jumpoint when no user is available, make sure the public portal permissions and your account permissions are set either to disable prompting or to default to* ***Allow****.*

Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access. For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.*

Create and Use Local or Remote RDP Shortcuts

Use BeyondTrust to start a Remote Desktop Protocol (RDP) session with a remote Windows or Linux System. Because RDP sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as your administrator has defined for your site.

To use Local RDP through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local RDP**.

To use Remote RDP through BeyondTrust, you must have access to a Jumpoint and must have the user account permissions **Allowed Jump Methods: Remote RDP**.

Create a Local RDP Shortcut

To create a Local Microsoft RDP shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Local RDP**. RDP shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

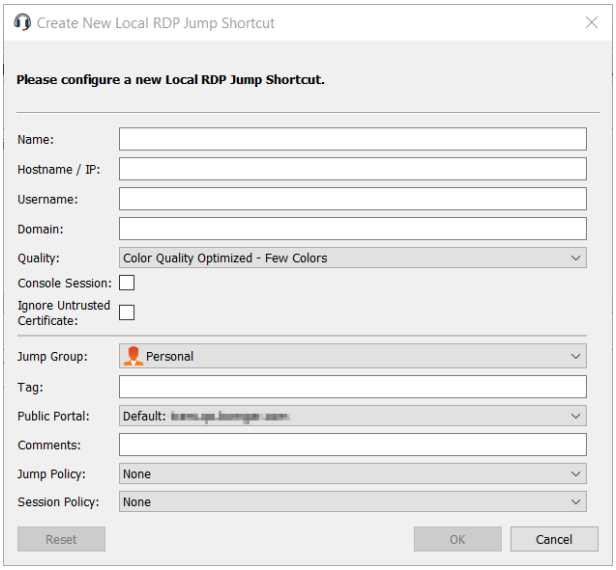
Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.).To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

Enter the **Hostname / IP** of the system you wish to access.

> ***Note:*** *By default, the RDP server listens on port 3389, which is therefore the default port BeyondTrust attempts. If the remote RDP server is configured to use a different port, add it after the hostname or IP address in the form of* ***<hostname>:<port>*** *or* ***<ipaddress>:<port>*** *(for example, 10.10.24.127:40000).*



Provide the **Username** to sign in as, along with the **Domain**.

Select the **Quality** at which to view the remote screen. This cannot be changed during the RDP session. Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select **Video Optimized**; otherwise, select between **Black and White** (uses less bandwidth), **Few Colors**, **More Colors**, or **Full Color** (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.

To start a console session rather than a new session, check the **Console Session** box.

If the server's certificate cannot be verified, you receive a certificate warning. Checking **Ignore Untrusted Certificate** allows you to connect to the remote system without seeing this message.

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 a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

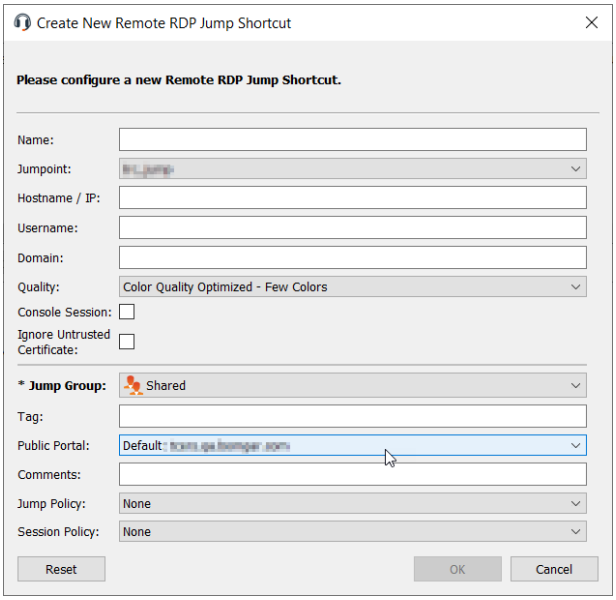
Create a Remote RDP Shortcut

To create a Remote Microsoft RDP shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote RDP**. RDP shortcuts appear in the Jump interface with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.



From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

> ***Note:*** *By default, the RDP server listens on port 3389, which is therefore the default port BeyondTrust attempts. If the remote RDP server is configured to use a different port, add it after the hostname or IP address in the form of* ***<hostname>:<port>*** *or* ***<ipaddress>:<port>*** *(for example, 10.10.24.127:40000).*

Provide the **Username** to sign in as, along with the **Domain**.

Select the **Quality** at which to view the remote screen. This cannot be changed during the RDP session. Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select **Video Optimized**; otherwise, select between **Black and White** (uses less bandwidth), **Few Colors**, **More Colors**, or **Full Color** (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.

To start a console session rather than a new session, check the **Console Session** box.

If the server's certificate cannot be verified, you receive a certificate warning. Checking **Ignore Untrusted Certificate** allows you to connect to the remote system without seeing this message.

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.

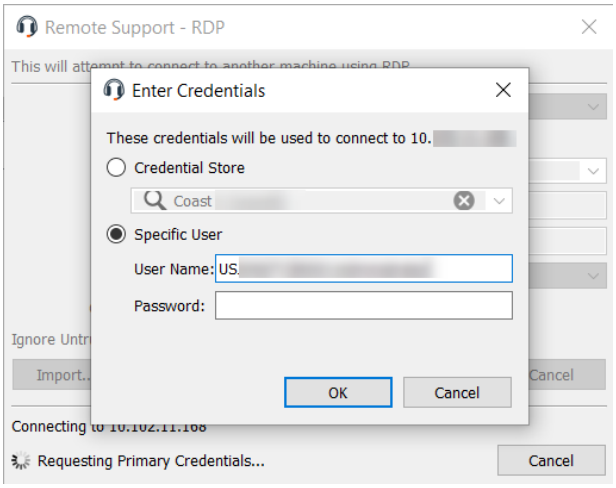
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

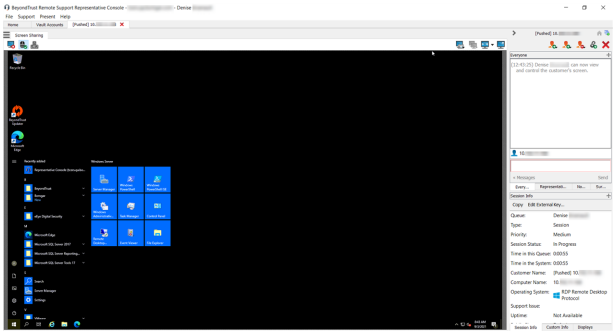
Use an RDP Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

You are prompted to enter the password for the username you specified earlier.



Your RDP session now begins. Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, and share clipboard contents. You can also share or transfer the RDP session with other logged-in BeyondTrust users, following the normal rules of your user account settings.



Multi-Monitor Support

An option allows you to open a Remote Support connection expanded across all the monitors on the client computer regardless of the client monitor configuration. With this feature, you can fully utilize all the monitors connected to the client computer, therefore being able to adjust screen sizing and scaling during an RDP session across multiple monitors.

Note: *If you are using full screen view while using this feature, the remote system is displayed across all of your monitors.*

Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Start New Session****, then a new independent session starts for each user who Jumps to a specific RDP Jump Item. The RDP configuration on the endpoint controls any further behavior regarding simultaneous RDP connections.*

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Create and Use Local or Remote VNC Shortcuts

Use BeyondTrust to start a VNC session with a remote system. Because VNC sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as defined by your administrator for your site.

To use Local VNC through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local VNC**.

To use Remote VNC through BeyondTrust, you must have access to a Jumpoint and must have the user account permission **Allowed Jump Methods: Remote VNC**.

Use BeyondTrust to start a VNC session with a remote system. Because VNC sessions are converted to BeyondTrust sessions, users can share or transfer sessions, and sessions can be automatically audited and recorded as defined by your administrator for your site.

To use Local VNC through BeyondTrust, you must be on the same network segment as the target system and must have the user account permission **Allowed Jump Methods: Local VNC**.

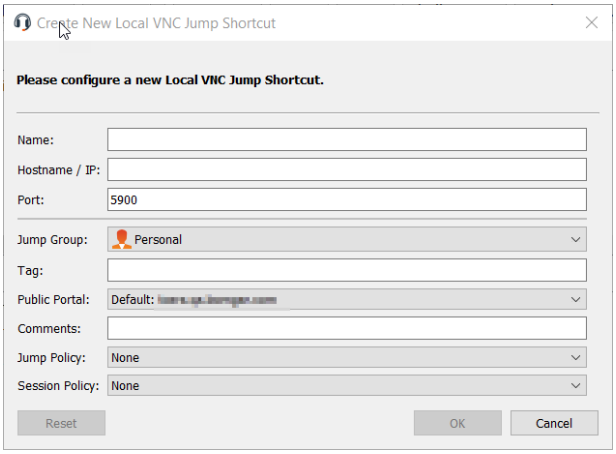
To use Remote VNC through BeyondTrust, you must have access to a Jumpoint and have the user account permission **Allowed Jump Methods: Remote VNC**.

Create a Local VNC Shortcut

To create a Local VNC shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Local VNC**. VNC shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*



Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

Enter the **Hostname / IP** of the system you wish to access.

By default, the VNC server listens on port 5900, which is, therefore, the default port BeyondTrust attempts. If the remote VNC server is configured to use a different port, enter it in the **Port** field.

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 a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

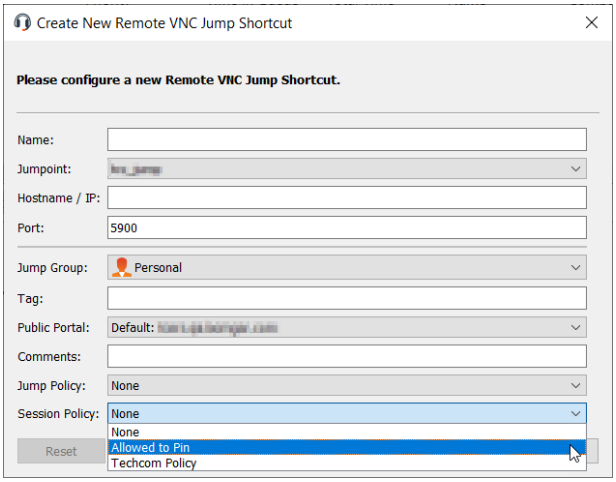
Create a Remote VNC Shortcut

To create a Remote VNC shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Remote VNC**. VNC shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.



From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

By default, the VNC server listens on port 5900, which is, therefore, the default port BeyondTrust attempts. If the remote VNC server is configured to use a different port, enter it in the **Port** field.

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.

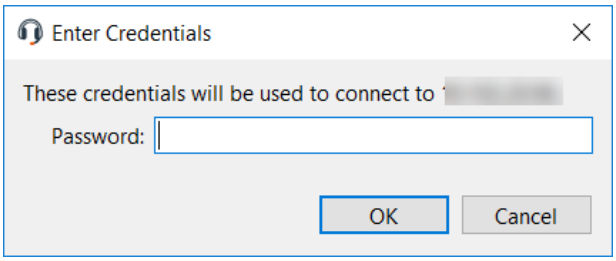
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

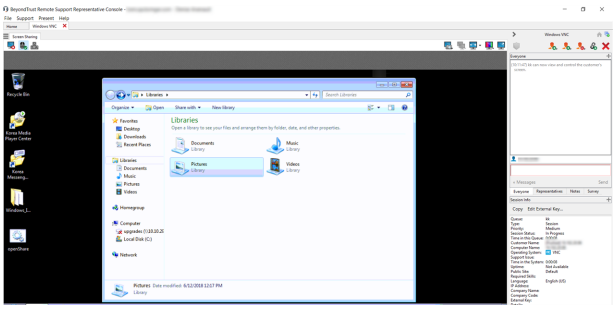
Use a VNC Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

When establishing the connection to the VNC server, the system prompts you to enter the user name and password.



Your VNC session now begins. Begin screen sharing to view the remote desktop. You can send the **Ctrl-Alt-Del** command, capture a screenshot of the remote desktop, and share clipboard text contents. You also can share, transfer, or record the VNC session, following the normal rules of your user account settings.



Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access.*

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

Create and Use Shell Jump Shortcuts

With Shell Jump, quickly connect to an SSH-enabled or Telnet-enabled network device to use the command line feature on that remote system. For example, run a standardized script across multiple systems to install a needed patch, or troubleshoot a network issue.

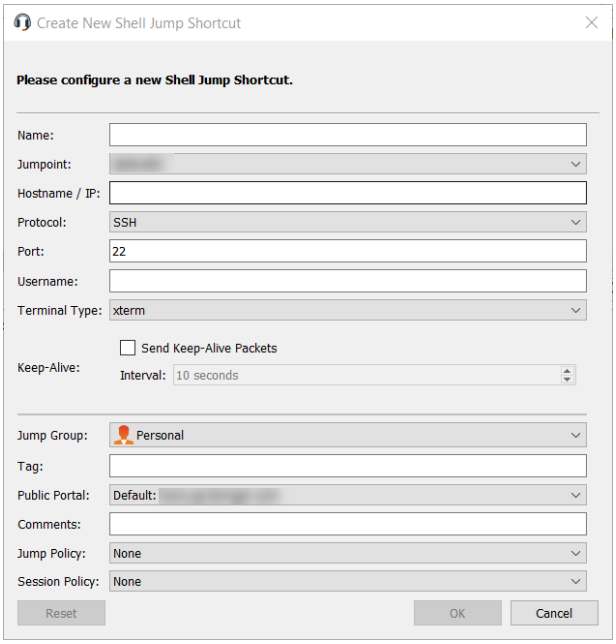
Create a Shell Jump Shortcut

To create a Shell Jump shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Shell Jump**. Shell Jump shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.

> ***Note:*** *Shell Jump shortcuts are enabled only if their Jumpoint is configured for open or limited Shell Jump access.*

Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be all the same type (e.g., all Jump Clients, all Remote Jumps, etc.). To review properties of other types of Jump Items, please see the appropriate section in this guide.*



Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

Choose the **Protocol** to use, either **SSH** or **Telnet**.

Port automatically switches to the default port for the selected protocol but can be modified to fit your network settings.

Enter the **Username** to sign in as.

Select the **Terminal Type**, either **xterm** or **VT100**.

You can also select to **Send Keep-Alive Packets** to keep idle sessions from ending. Enter the number of seconds to wait between each packet send.

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.

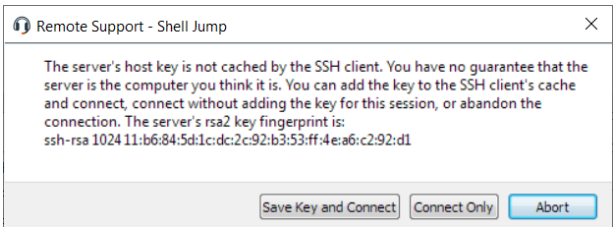
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Choose a **Session Policy** to assign to this Jump Item. The session policy assigned to this Jump Item has the highest priority when setting session permissions. The ability to set a session policy depends on your account permissions.

Use a Shell Jump Shortcut

To use a Jump shortcut to start a session, select the shortcut from the Jump interface and click the **Jump** button.

If attempting to Shell Jump to an SSH device without a cached host key, you receive an alert that the server's host key is not cached and that there is no guarantee that the server is the computer you think it is.



If you choose **Save Key and Connect**, then the key is cached on the Jumpoint's host system so that future attempts to Shell Jump to this system do not result in this prompt. **Connect Only** starts the session without caching the key, and **Abort** ends the Shell Jump session.

If you Shell Jump to an SSH device with keyboard interactive MFA enabled, there is a secondary prompt for input.

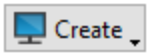
When you Shell Jump to a remote device, a command shell session immediately starts with that device. If you Shell Jump to a provisioned SSH device with an unencrypted key or with an encrypted key whose password has been cached, you are not prompted for a password. Otherwise, you are required to enter a password. You can then send commands to the remote system.

Create and Use Intel vPro Shortcuts

Using Intel® Active Management Technology, privileged users can support fully provisioned Intel vPro Windows systems below the OS level, regardless of the status or power state of these remote systems.

Create an Intel® vPro Shortcut

To create an Intel® vPro shortcut, click the **Create** button in the Jump interface. From the dropdown, select **Intel® vPro**. Intel® vPro shortcuts appear in the Jump interface along with Jump Clients and other types of Jump Item shortcuts.



Organize and manage existing Jump Items by selecting one or more Jump Items and clicking **Properties**.

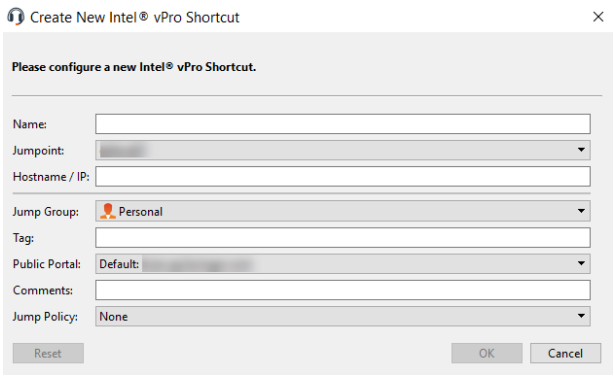
> ***Note:*** *To view the properties of multiple Jump Items, the items selected must be the same type (e.g., all Jump Clients, all Remote Jumps, etc.).*

Enter a **Name** for the Jump Item. This name identifies the item in the session tabs. This string has a maximum of 128 characters.

From the **Jumpoint** dropdown, select the network that hosts the computer you wish to access. The representative console remembers your Jumpoint choice the next time you create this type of Jump Item. Enter the **Hostname / IP** of system you wish to access.

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.

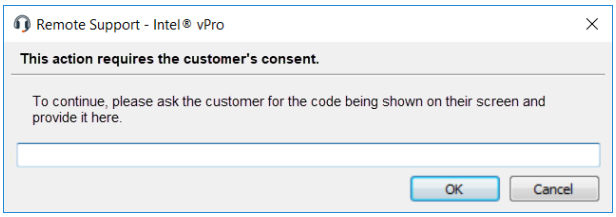
To set when users are allowed to access this Jump Item, choose a **Jump Policy**. These policies are configured by your administrator in the **/login** interface.

Use an Intel® vPro Shortcut

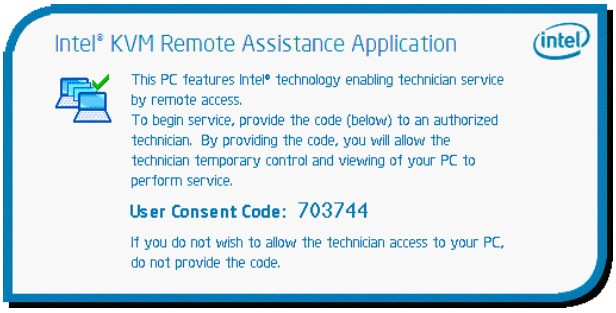
Depending on your Jumpoint setup, you may be prompted to enter a username and password.

The Jumpoint detects the provisioned vPro hardware. If the credentials, provided during either the Jumpoint configuration or the Jump attempt, match the credentials of the vPro-provisioned system, the connection is initiated.

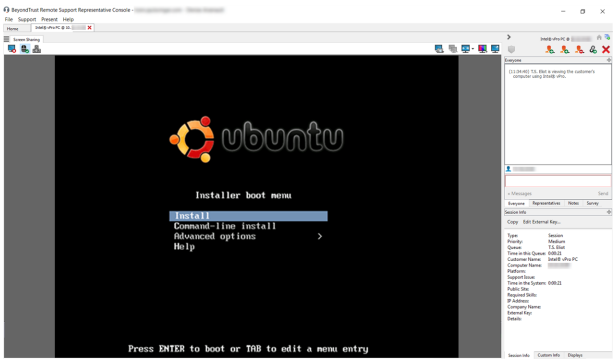
Depending on how the vPro computer is provisioned, you might be prompted to enter a user consent code before performing certain actions.



If a consent code is required, a pop-up appears on the remote screen. An end user must provide you with this code before you can gain hardware access.



Once the connection is made, you have control of the remote vPro hardware. You can then use the vPro session tools to work on the remote system.



Note: *Jump Items can be set to allow multiple users to simultaneously access the same Jump Item. If set to* ***Join Existing Session****, other users are able to join a session already underway. The original owner of the session receives a note indicating another user has joined the session, but is not allowed to deny them access.*

For more information on simultaneous Jumps, please see Jump Item Settings at www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.

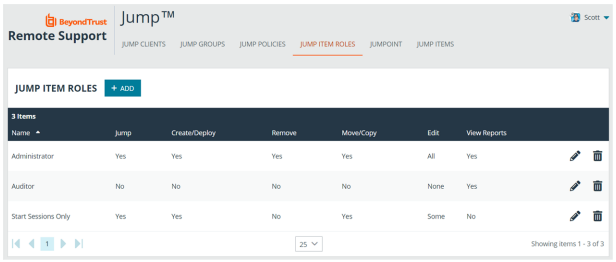
Use Cases for Jump Item Implementation

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

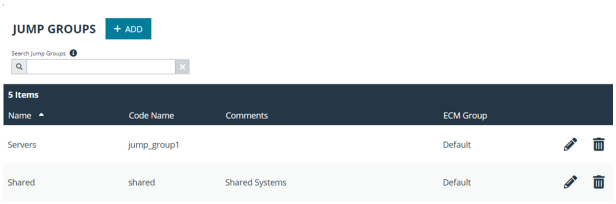
Basic Use Case

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

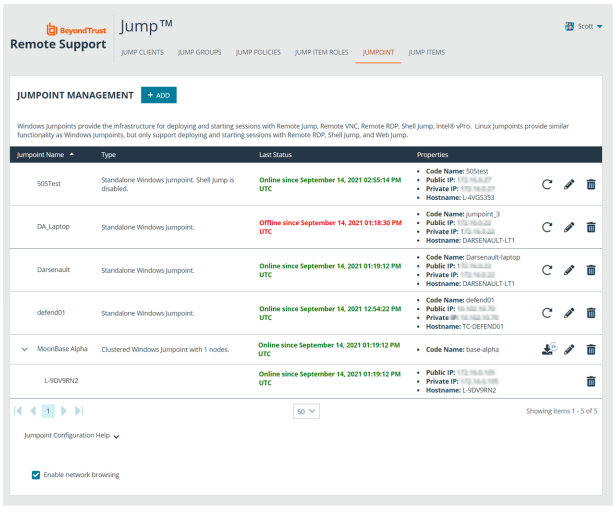
1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**.
    a. The **Administrator** role should have all permissions enabled.
    b. The **Start Sessions Only** role should have only **Start Sessions** enabled.



2. Create a **Shared** Jump Group that will contain all shared Jump Items. Personal Jump Items can also be created.

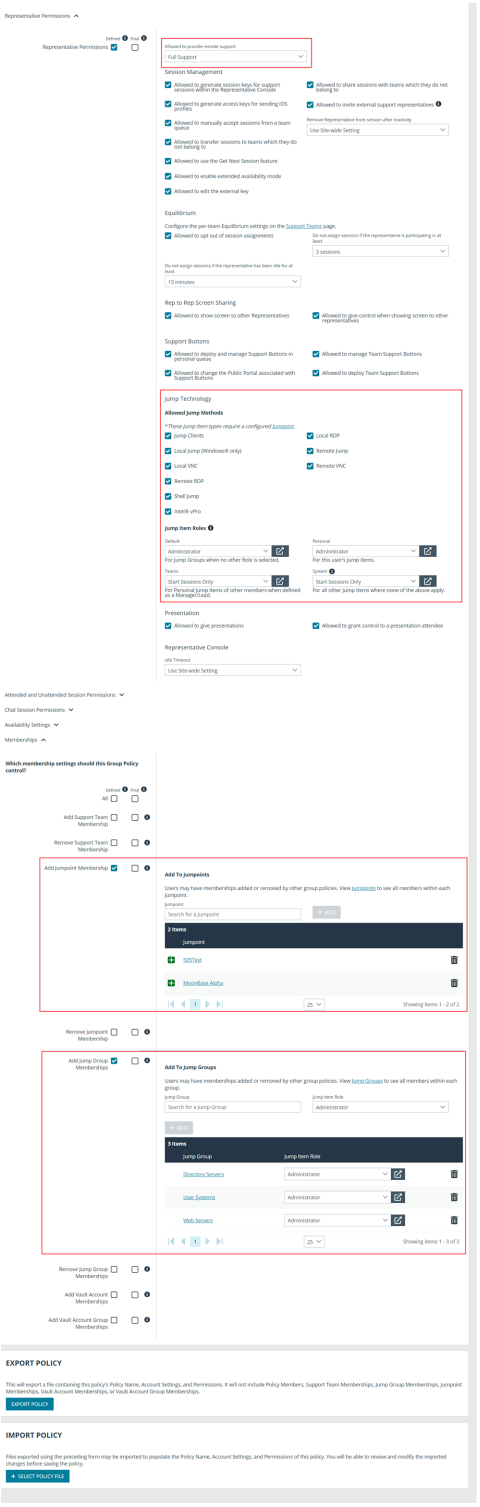


3. Deploy a Jumpoint to each remote network segment where Jump Items will be deployed.

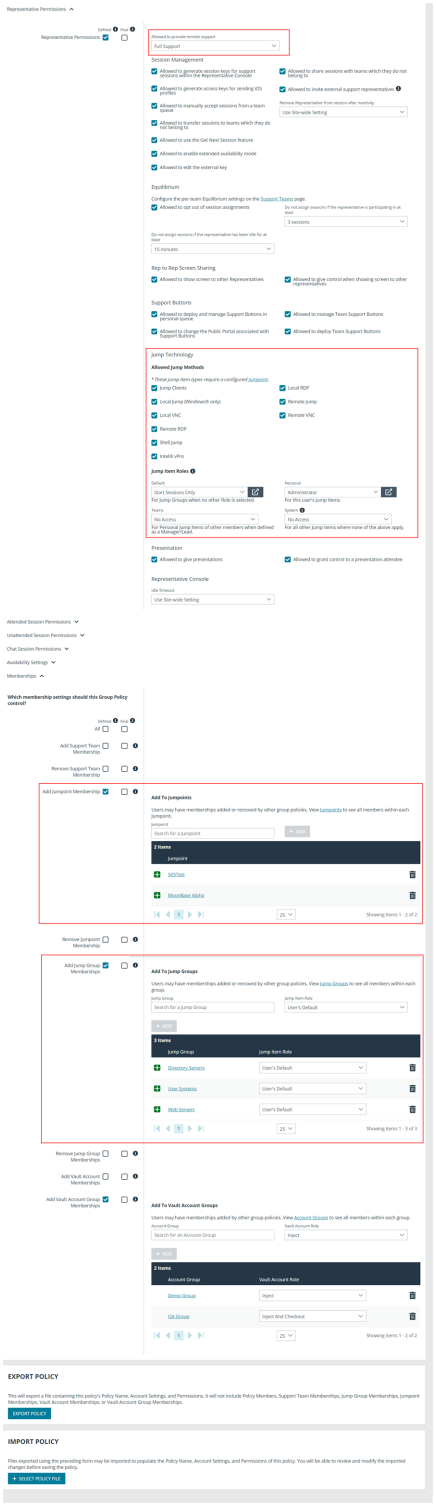


4. Put users into two group policies, **Admins** and **Users**.

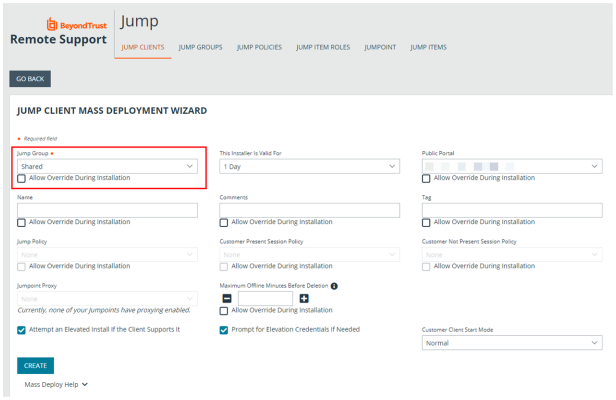
5. In the **Admins** group, configure settings and permissions as appropriate. The permissions should include the following:
    a. Define **Representative Permissions** and enable **Allowed to provide remote support**.
    b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    c. Under **Jump Item Roles**, set the **Default** and **Personal** roles to **Administrator**.
    d. Set the **Teams** and **System** roles to **Start Sessions Only**.
    e. Under **Memberships**, define **Add Jumpoint Membership**.
        i. In the **Jumpoint** field, search for and select each Jumpoint.
        ii. Click **Add** to grant the members of this group policy access to the Jumpoint.
    f. Under **Memberships**, define **Add Jump Group Memberships**.
        i. In the **Jump Group** field, search for and select **Shared**.
        ii. Set the **Jump Item Role** to **Administrator**.
        iii. Click **Add** to assign the members of this group policy to the Jump Group.
    g. Save the group policy.



6. In the **Users** group, configure settings and permissions as appropriate. The permissions should include the following:
    a. Define **Representative Permissions** and check **Allowed to provide remote support**.
    b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    c. Under **Jump Item Roles**, set the **Default** to **Start Sessions Only**.
    d. Set the **Personal** Jump Item Role to **Administrator**.
    e. Set the **Teams** and **System** roles to **No Access**.
    f. Under **Memberships**, define **Add Jumpoint Membership**.
        i. In the **Jumpoint** field, search for and select each Jumpoint these users will need to access.
        ii. Click **Add** to grant the members of this group policy access to the Jumpoint.
    g. Under **Memberships**, define **Add Jump Group Memberships**.
        i. In the **Jump Group** field, search for and select **Shared**.
        ii. Set the **Jump Item Role** to **Start Sessions Only**.
        iii. Click **Add** to assign the members of this group policy to the Jump Group.
    h. Save the group policy.



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



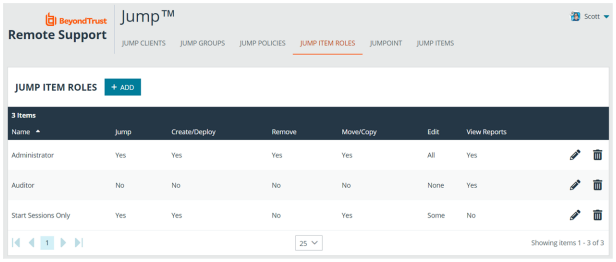
8. Now, administrators can deploy and start sessions with Jump Items in the **Shared** Jump Group. They can also manage their personal lists of Jump Items and start sessions with all other Jump Items.

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

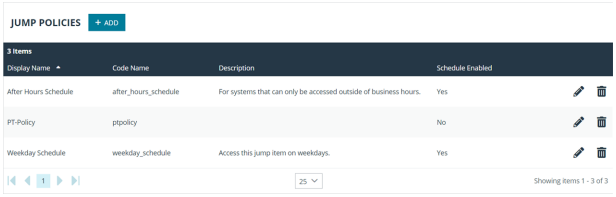
Advanced Use Case

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. Some Jump Items should be accessible at all times, while others should be accessible only on weekdays.

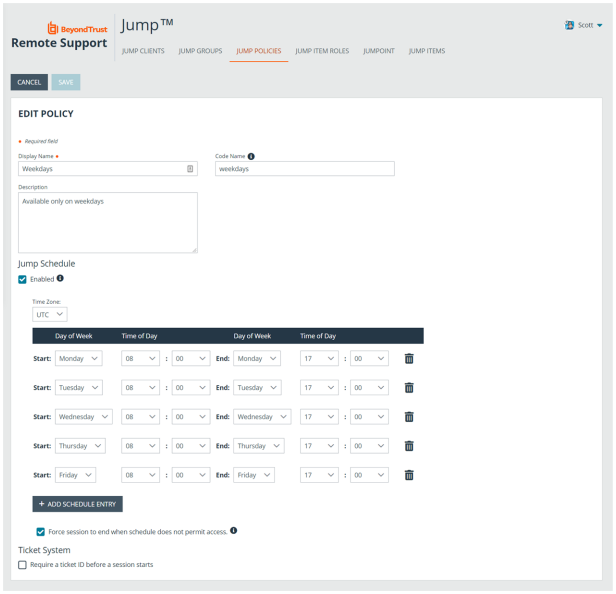
1. Create two Jump Item Roles, **Administrator** and **Start Sessions Only**.
   a. The **Administrator** role should have all permissions enabled.
   b. The **Start Sessions Only** role should have only **Start Sessions** enabled.



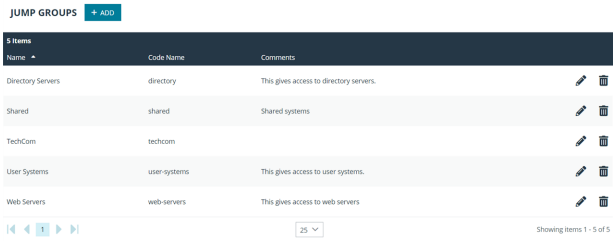
2. Create a Jump Policy, **Weekdays**.



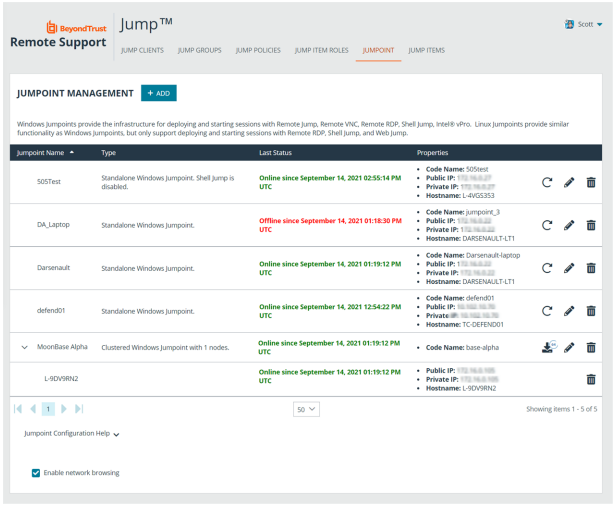
3. In the Jump Policy, enable the **Jump Schedule**.
    a. Click **Add Schedule Entry**.
    b. Set the **Start** day and time to **Monday 8:00** and the **End** day and time to **Monday 17:00**.
    c. Click **Add Schedule Entry** and repeat the process for the remaining weekdays.
    d. Save the Jump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



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

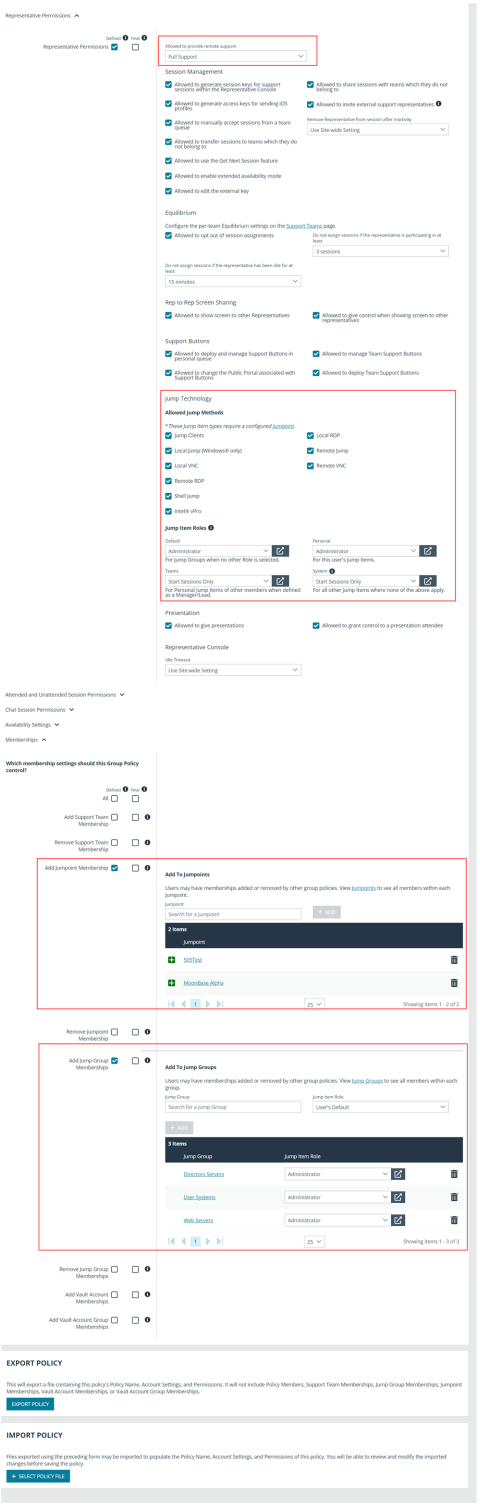


5. Deploy a Jumpoint to each remote network segment where Jump Items will be deployed.

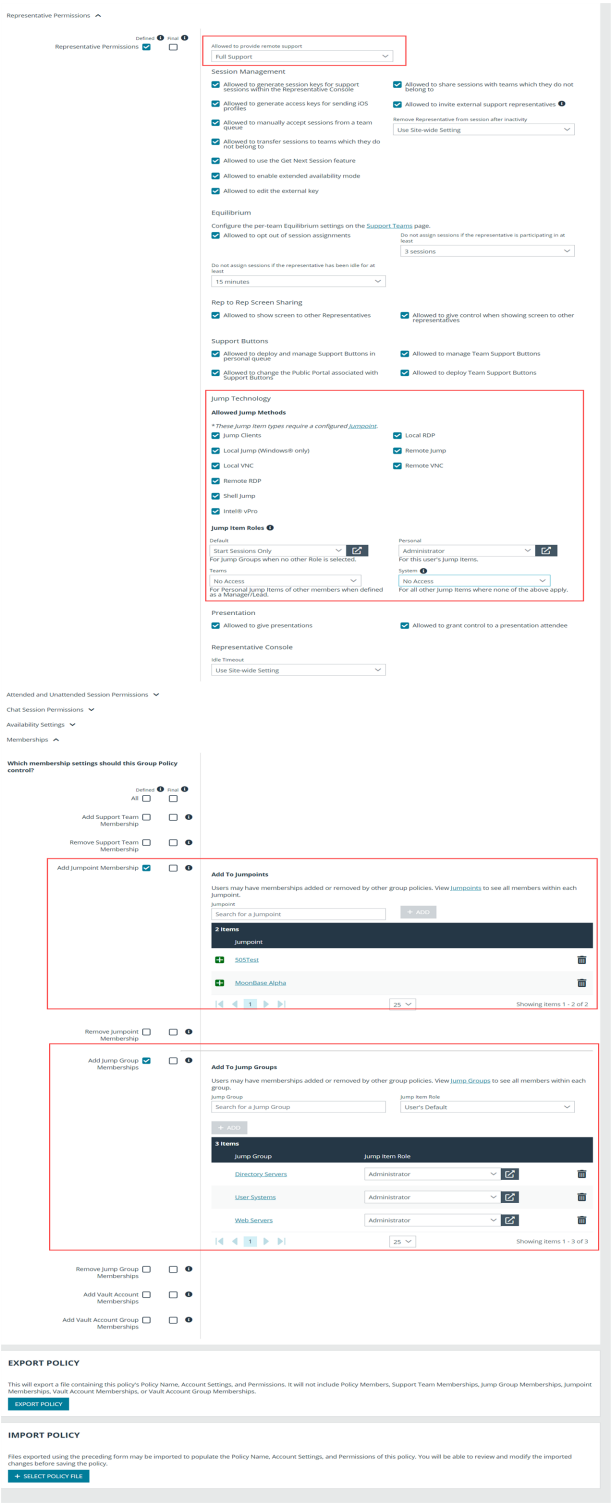


6. Put users into two group policies, **Admins** and **Users**.

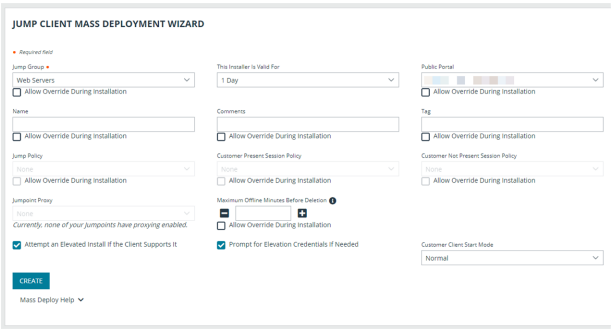
7. In the **Admins** group, configure settings and permissions as appropriate. The permissions should include the following:
    a. Define **Representative Permissions** and enable **Allowed to provide remote support**.
    b. Under **Jump Technology**, check all **Allowed Jump Methods** that your organization will use.
    c. Under **Jump Item Roles**, set the **Default** and **Personal** roles to **Administrator**.
    d. Set the **Teams** and **System** roles to **Start Sessions Only**.
    e. Under **Memberships**, define **Add Jumpoint Membership**.
        i. In the **Jumpoint** field, search for and select each Jumpoint.
        ii. Click **Add** to grant the members of this group policy access to the Jumpoint.
    f. Under **Memberships**, define **Add Jump Group Memberships**.
    g. In the **Jump Group** field, search for and select **Web Servers**.
        i. Set the **Jump Item Role** to **Administrator**.
        ii. Click **Add** to assign the members of this group policy to the Jump Group.
    h. In the **Jump Group** field, search for and select **Directory Servers**.
        i. Set the **Jump Item Role** to **Administrator**.
        ii. Click **Add** to assign the members of this group policy to the Jump Group.
    i. In the **Jump Group** field, search for and select **User Systems**.
        i. Set the **Jump Item Role** to **Administrator**.
        ii. Click **Add** to assign the members of this group policy to the Jump Group.
    j. Save the group policy.



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



9. 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.



10. 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.

    Specified Jump Items can be accessed only on weekdays.

Appendix: Require a Ticket ID Workflow for Jump Item Access

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

What Users See

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

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

How It Works

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

If the request is allowed, the external ticket ID system assigns the allowed session. Optionally, your external ITSM or ticket ID system may send a list of custom session attributes in its response to assign to the allowed session.

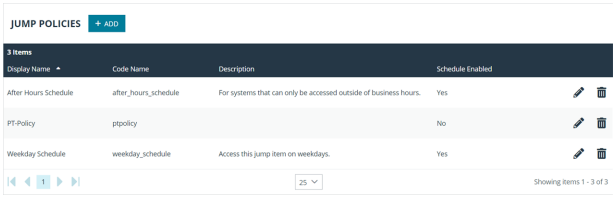
Follow the steps below to set up a ticket ID requirement for access.

> *For more information on using the BeyondTrust API see the Remote Support API Programmer's Guide at https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/index.htm.*

Create a Jump Policy Requiring Ticket ID Approval

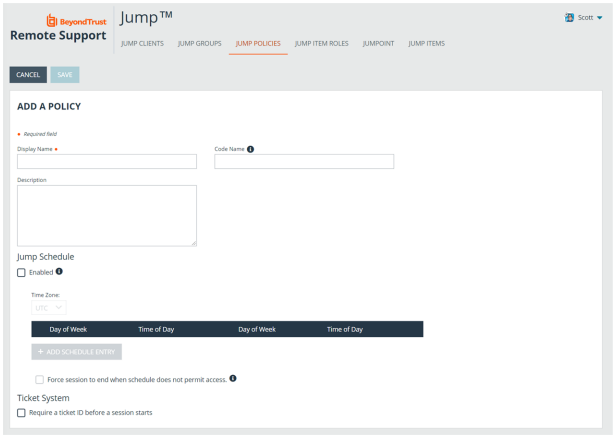
First, create a Jump Policy with the requirement of **ticket ID approval** enabled.

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



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

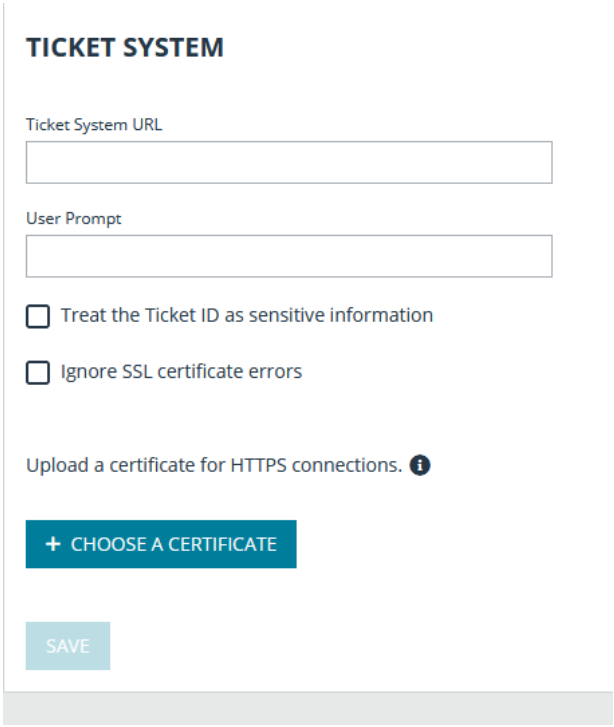
3. Enter a **Display Name**, **Code Name**, and **Description** in the corresponding locations to enable you to effectively apply this Jump Policy appropriate to your purposes after its creation.
4. Optionally, complete the configuration for **Jump Schedule** and **Jump Notification**, if appropriate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



Connect External Ticket ID System to Jump Policies

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

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



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

6. In the **User Prompt** field, enter the dialog text you want representative console users to see when they are requested to enter the ticket ID required for access.
7. In the **User Prompt** field, enter the dialog text you want representative console users to see when they are requested to enter the ticket ID required for access.
8. If your company's security policies consider ticket ID information as sensitive material, check the **Treat the Ticket ID as sensitive information** box.
9. Click **Save**.

API Approval Request

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

request_id	Unique ID that identifies the approval request. ***Note:*** *The request ID must be sent from the external ticketing system to BeyondTrust RS in the response. The maximum length is 255 characters, and the ticketing system must treat the request ID as an opaque value.*
ticket_id	ticket ID entered by the user.
response_url	URL to which the integration should POST its response.
jump_item.computer_name	Hostname or IP address of the endpoint the user is requesting access for.
jump_item.type	Type of Jump Item being accessed: • client (for Jump Clients) • shell (for Shell Jump Shortcuts) • RDP • VNC • push_and_start (for Remote Jump and Local Jump) • vPro
jump_item.comments	Comments noted about the Jump Item.
jump_item.group	Group associated with the Jump Item.
jump_item.tag	Tags associated with the Jump Item.
jump_item.jumpoint_name	Name of the Jumpoint.
jump_item.public_ip	Public IP address of the Jump Item. ***Note:*** *This is not provided for Jumpoints.*
jump_item.private_ip	Private IP address of the Jump Item.

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

API Approval Response

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

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

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

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

Error Messages

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

- *Ticket System URL is required because one or more Jump Policies still require a ticket ID*: A Jump Policy exists requiring the entry of a ticket ID for access.
- *Invalid ticket ID*: The external ticket system explicitly denied the request. If the external ticket system sends the error message, that message is shown.
- *The Ticket System URL must start with "https://" when the Ticket ID is sensitive*: You must enter an HTTPS URL when the **Treat the Ticket ID as sensitive information** option is checked.

- *Cannot ignore SSL errors when the Ticket ID is sensitive*: When this option is checked, you cannot ignore SSL errors and must provide a valid SSL certificate.
- *The given host was not resolved*: An invalid ticket system URL was attempted.
- *The ticket system failed to respond in time*: The external ticket system failed to respond in a timely manner.

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

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

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

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

Appendix: Jumpoint Error Message Reference

This appendix provides a reference for error messages that may occur while attempting to start a session with a remote computer via Jumpoint. It is assumed that a Jumpoint has already been installed on the remote network.

Below are a few helpful definitions of terms that will be used throughout this appendix.

Term	Definition
<hostname>	Placeholder for the unique name of the remote computer to which a Jump session is being attempted.
target system	The remote computer which a support representative is attempting to access. Because the scope of this document covers only Jumpoints, it is assumed, though not required, that target systems are unattended.

Below is a list of possible error messages that may occur, accompanied by a brief description of each message.

Message	Description
Access denied for <hostname>	The credentials specified did not have sufficient permissions to enable the Jump connection to be established. A Windows user account with administrative credentials for the target system is required.
Access denied to host <hostname>	The credentials specified did not have sufficient permissions to enable the Jump connection to be established. A Windows user account with administrative credentials for the target system is required.
An unknown error occurred while trying to contact host <hostname>	The attempt to obtain information about the target system failed. This message covers any failure which is not explicitly defined.
Another representative is currently pushing to this host. Please try again in a few moments.	Someone else is already attempting to Jump to the specified target system via this Jumpoint.
Cannot detect host settings for <hostname>	The Remote Registry service may not be running on the target system. Note that Windows Vista and XP both have this service turned off by default.
Couldn't detect host settings for <hostname>	The Jumpoint could not read the registry of the target system and therefore could not perform the Jump.
Couldn't push the installer to <hostname>	The BeyondTrust customer client installer was not able to be pushed to the target system.
Couldn't trigger installation on <hostname>	Though the Jumpoint was able to install the BeyondTrust customer client on the target system, it failed to start the service on the target system.
Failed to communicate properly with <hostname>	Though the Jumpoint was able to push the BeyondTrust customer client installer to the target system, it failed to actually install the service on the target system.

Message	Description
Failed to establish a connection to <hostname>. Please verify the following: - remote system is accessible through network (ping) - remote system is running NT or higher (not 9x or XP Home) - you have administrator privileges on the remote system - XP Pro Local Security Policy is using Classic model for authentication (workgroup connections only)	The attempt to create a connection for a Jump has failed for any reason. Several probable reasons are listed within the error message.
Invalid credentials for <hostname>	While attempting to establish a connection to the target system, the credentials were denied by the target system.
Network error disconnecting from host <hostname>	The Jumpoint failed to disconnect a network connection that already existed between its host computer and the target system, most likely because that connection was actively in use. For security reasons, a Jumpoint must always disconnect any existing network connections that exist between the system hosting the Jumpoint and the target system (e.g., mapped drives, shared folders, remote registry manipulation, etc.). Otherwise, the Jumpoint could potentially perform a Jump via the existing network connection. This would create a vulnerability through which a support representative could gain access to a target system to which they should not have access. Therefore, this disconnect must occur before the Jump connection is made. It is highly recommended that the system hosting the Jumpoint not share folders or map drives to any systems to which it might need to Jump, since those attempts to Jump will fail.
Sorry, but the Jumpoint is too busy at the moment to process your request. Please try again later.	The Jumpoint is overloaded with too many Jump requests.
The host <hostname> refused to accept the file.	This is usually caused by a permission issue with the user account (on the target system) used to push to the target system. Try to open **\\hostname\admin$** on the target system from your local system.
The Jumpoint could not download the customer client	The Jumpoint failed to download the customer client from the BeyondTrust Appliance B Series. The first time a Jumpoint attempts a Jump, it must download a copy of the BeyondTrust customer client installer. From then on, it pushes that cached customer client to the target systems. Note that upgrading a site also causes the Jumpoint to download a new customer client.
Unable to prepare target system	The user context under which the representative console is running does not have access to the remote registry. Make sure the host system requirements are met as described in "Review Jumpoint Hardware and Software Requirements" on page 11.

Message	Description
Unknown host <hostname>	The target system could not be found on the network.