Discover Jump Technology for Access to Remote Systems

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.

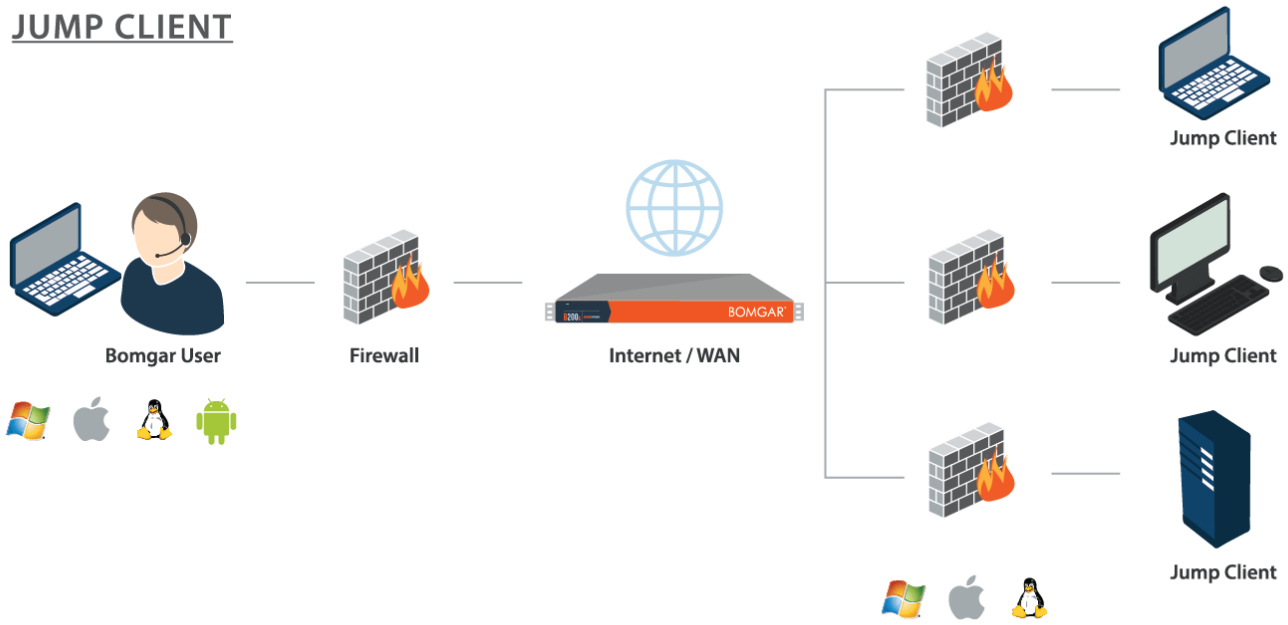
Not every support scenario has a customer at their computer. You can use BeyondTrust Jump Technology in two different ways, depending on your needs for unattended support.

- Use a Jump Client where the network may not be known.
- Use a Jumpoint if your unattended support needs are defined within a network.

Jump Client

Deploy a Jump Client if you need:

- Attended or unattended access to computers and other devices, regardless of network location.
- Stronger management capacities and the control of installing a persistent and secure remote access client.



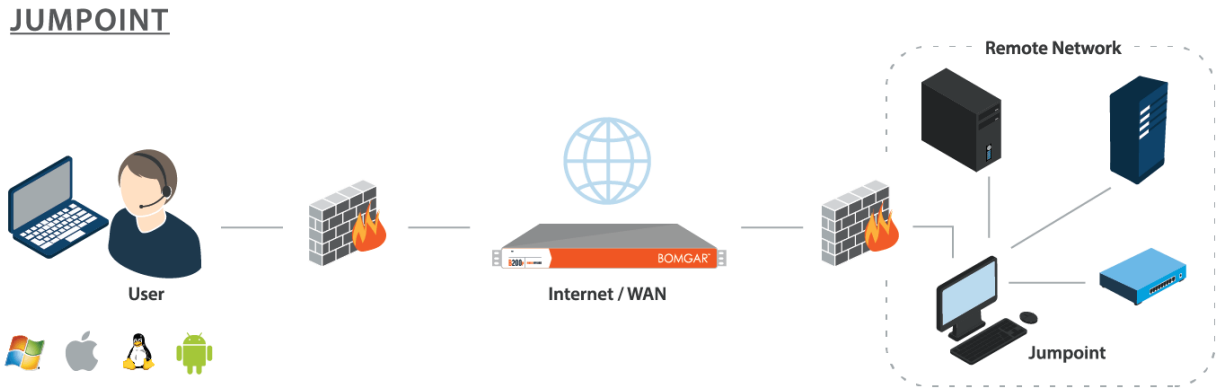
Privileged representatives may deploy Jump Clients dynamically from their access console or download a mass deployable Jump Client from the /login administrative interface. The Jump Client is pinned to a Jump Group, thus enhancing administrative oversight and efficiency, benefiting from the robust management accommodations present throughout BeyondTrust. For example, customers who require unique support handling might be set up with Jump Client deployment to enhance administrative capabilities. A Jump Client management interface in the access console helps you manage your deployments.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Jumpoint

Deploy a Jumpoint if you need:

- To troubleshoot all systems in a network without pre-deploying BeyondTrust clients on each system prior to connecting.
- Access to SSH, Telnet, or vPro systems on that network, like servers, routers, POS systems, or ATMs.
- To run Microsoft Remote Desktop Protocol sessions while maintaining a consistent audit trail.



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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Terms to Know

The following terms and phrases are often used in reference to BeyondTrust's Jump Technology.

Jump, Unattended Access

Jump is a term for accessing a remote system. **Unattended access** refers to accessing remote systems without requiring interaction from a remote user to initiate the access.

Jump Client, Pinned Session

Jump Clients are used to establish a one-to-one encrypted connection between a B Series Appliance and a remote Windows, Mac, Android, or Linux system. A Jump Client must be installed on each remote system you want to access. The installed Jump Clients to which a representative has permission are listed in the bottom pane of the access console. A **Pinned Session** is a BeyondTrust support session that started through a Jump Client.

Jump Clients are state-aware, which means they can determine if a user is present and interact accordingly. They can also be set to automatically uninstall, to meet compliance requirements.

Endpoint

An endpoint is any remote computer or device residing on a network. This can include:

- Windows desktops, laptops, and servers
- MacOS and iOS devices
- Linux systems
- Android phones and tablets.
- Search- and Telnet-enabled devices such as Cisco switches or BeyondTrustSecure Remote Access Appliances.

Jumpoint

A **Jumpoint** extends the reach of Jump functionality, enabling representatives with appropriate permissions to start a session with any remote system. The Jumpoint can be installed on a network remote to any representative or the BeyondTrust Appliance B Series.

Local Jump, Local Push

Local Jump or **Local Push** refer to Jumping from the access console using the local network. This allows a representative to initiate a BeyondTrust session with Windows systems on the same network segment as the access console, without using a Jumpoint. The requirements on the endpoint being assessed and the functionality for Local Jumps are the same as for Remote Jumps with Jumpoints.

Remote Jump, Remote Push

Remote Jump or **Remote Push** refer to Jumping from the access console using a Jumpoint on a remote network.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Jump To, Push and Start, Pushed Session

Jump To, **Push and Start**, and **Pushed Sessions** refer to BeyondTrust sessions started from either Jumpoints or Local Jumps, without distinction. Thus, a pushed session can refer to either of these technologies but not to Jump Client sessions or pinned sessions. Similarly, Push and Start and Jump To can refer to either Jumping through a Jumpoint or a Local Jump but not to Jumping to a Jump Client.

Jump Item

Jump Item is an umbrella term for any pre-defined endpoint, regardless of how it is reached.

Jump Shortcut

A **Jump Shortcut** is any Jump Item that is not a Jump Client.

Jump Group

A **Jump Group** is a collection of Jump Items. Jump Groups can be used to organize Jump Items in any manner that works for your organization. For example, servers could be organized in geographic, departmental, or team Jump Groups. Jump Groups can also be used to manage access. For example, one set of Jump Clients could be accessible by the help desk team, while another set is accessible by the network team.

Jump Policy

A **Jump Policy** is used to control access to Jump Items. For example, access might be restricted to specific hours. Jump Policies can be applied to individual Jump Items or Jump Groups.

Jump Item Role

A **Jump Item Role** is a predefined set of permissions regarding Jump Item management and usage. You assign users to a Jump Item or a Jump Group either through Group Policies or by adding individual users. You can set an individual user's permissions to specific Jump Items in a group, or the entire group.

Use Cases: Putting it All Together

Jump Technology allows you to use Jumpoints or Jump Clients with group and user policies to create workflows for any technical, regulatory, and organizational remote access requirement. These are just two possible cases.

University IT Service Desk

The service receives a request from their online contact form. A board member is using their iOS device to request assistance with their office desktop, while they are taking the train home. The request is automatically routed to a senior representative with the appropriate Jump Item role. The user could not print a document from their office desktop. While securely messaging with the board member, the representative is able to use a Jump Client to access the board member's desktop, log in, use file transfer to install a print driver, then test printing.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Jump Policies restrict unattended access to non-working hours. The messaged conversation and the details of the remote access session, including duration, technician's name, customer's name and session recording are all available for auditing on the Secure Remote Access appliance.

Offshore Drilling Company

An offshore drilling company needs to provide vendor access to devices on rigs, which are located around the world, all on separate remote networks. Before a vendor can gain access, they must have explicit approval from the rig foreman or the application owner on that respective rig. Compliance regulations do not allow deploying agents directly on endpoints of the operational technology or OTC network, so Jump Clients cannot be used. Also, the endpoints don't have native internet access, meaning they cannot communicate directly with our clients, so a proxy is needed to initiate connections.

A Jumpoint can be installed to each rig, which can communicate with the Secure Remote Access appliance and then endpoints downstream on the rigs, local area and network, without those endpoints on the local area network needing native internet access. Connections shortcuts for the endpoint can be RDP, SSH, or other protocols.

The connections can be grouped by vendor to segregate access to the appropriate endpoints, with additional restrictions on some endpoints. For example, a vendor may be able to install software upgrades on some devices but not others. Policies per endpoint or groups of endpoints can send those approval requests to the requisite parties, whether that's the rig foreman or the application owner on that rig. A vendor may report a problem with a device, and a user group can access the same endpoints with higher permissions to diagnose and resolve issues.

For more information about using and configuring Jump Clients and Jumpoints, and their groups, policies, and roles, please see:

- *Jump Client Guide at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/index.htm*
- *Jumpoint Guide at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/index.htm*

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.