Transcript: Jumpoint Configuration for Unattended Access

Introduction

With a Bomgar Jumpoint, a support representative can access and control unattended Windows computers on a remote network without installing a client on each remote system.

Add New Jumpoint

To configure Jumpoints, go to your Bomgar Appliance /login interface. Click on the **Jump** tab and then go to the **Jumpoint** page.

At the bottom of the page is the option to enable network browsing. If this box is checked, you can search for the remote computer you wish to access by browsing the network's directory structure. If the box is unchecked, you must enter the remote system's hostname or IP address.

Create a Jumpoint by clicking **Add New Jumpoint**. Enter an identifying name. Jumpoints can also have an optional codename which is useful for integrations and scripting

If you want this Jumpoint to be available to connect to SSH-enabled and Telnet-enabled network devices, check **Enable Shell Jump Method**.

If you want this to be a clustered Jumpoint, check the **Clustered** check box. Keep in mind that Jumpoint cluster nodes must be installed on hosts residing in the same local area network.

Under **Allowed Users**, click the **User** field to add users from the dropdown menu. These are the users who will be authorized to use this Jumpoint. Users can also be added via group policy.

Finally, click **Add Jumpoint**.

Jumpoint Installation

From the list of Jumpoints, find your new Jumpoint and download the appropriate 32 or 64-bit installer to a system on the remote network you wish to access. This system will serve as the initiation point for Jump sessions with other computers on that network. Deploying the Jumpoint to a virtual system is the ideal setup scenario if such a system is available.

The installation wizard will walk you through the first part of the setup process.

For a Jumpoint to be deployed on a remote LAN behind a proxy, appropriate proxy information may be necessary for the Jumpoint to connect back to the Bomgar Appliance. You can configure proxy settings to be supplied whenever Jumping to another system on the remote network, providing the credentials necessary to download and run the customer client on the target system.

You also can set up this Jumpoint to function as a proxy itself. If **Jump Zone Proxy Server** is selected, this Jumpoint can be used to proxy connections for clients on the network that do not have a native internet connection. Using a Jumpoint as a proxy will route traffic only to the appliance.

Enter the DNS or IP address to use as the listening interface, and set which port to use. Set whether to allow all IP addresses or to limit the IPs that can connect through this proxy.

vPro

If desired, you can configure the Jumpoint to enable vPro connection by going to the Intel® vPro tab and checking **Enable Intel® vPro**. 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**.

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.

On the **Encryption** tab, set how the Jumpoint encrypts vPro network traffic. If the remote vPro systems are provisioned not to use TLS encryption, simply select **No Encryption**. 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.

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

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

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.

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.

If **Provisioned Only** is selected, representatives can Shell Jump only to provisioned devices.

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.

If **Provisioned Only** is enabled on the Policy tab, configure access to provisioned Shell Jump targets and click **Add**.

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

Because many SSH hosts use keys for identification and authentication, administrators will want to configure these ahead of time so that support reps have quick, easy and secure access.

On the **TTL** tab, you can set whether the Jumpoint is always active, or set a date and time for the activation to take place. Likewise, you can set a date and time to automatically uninstall the Jumpoint, or set it so that it will not automatically uninstall.

Click **Finish**, and the installation will complete.

Starting Sessions Via 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.

To connect to a remote computer via Jumpoint, open your representative console and access the Jumpoint dialog by clicking the **Jump To** button above the Jump interface or by selecting **Jump To** from the **Support** menu.

From the dropdown, select the network you wish to access. Check **Remember as my preferred choice** have the representative console remember your latest selection or leave it unchecked to have the dropdown return to the default the next time you open the Jumpoint dialog.

Enter the hostname or IP address of the remote system you wish to access. If network browsing is enabled, you also can click on the small browse button to search the network directory for the computer you want. Then click **Jump**. You will be prompted for credentials to the remote system. Once valid credentials are supplied, the customer client will install on the remote system, and a support session will begin.

Other Methods: Starting Sessions Via RDP

To start a Local RDP session from the representative console, open the Remote Desktop Protocol dialog from either the **Support** menu or **RDP To** button. Choose **Local Network** for your Jumpoint option, then enter the hostname or IP address of the computer you wish to support.

Provide the username to sign in as and select a domain. Choose the resolution at which to view the remote system. This can be the same size as your primary monitor, the size of all of your monitors combined, or one of several standard sizes.

Select the quality at which to view the remote screen. To start a console session rather than a new session, check the **Console Session** box. If the server's certificate cannot be verified, you will receive a certificate warning. Checking **Ignore Untrusted Certificate** allows you to connect to the remote system without seeing this message.

To import an RDP file, click the **Import** button. This pre-populates some of the fields required for the remote desktop protocol connection.

To begin the remote desktop (RDP) session, click **Jump**. When prompted, enter the password for the username you specified earlier. Click **OK** to start your RDP session.