Transcript: Manage and Deploy Jump Clients

With Bomgar Jump Clients, a support rep can access and control unattended computers.

From the **/login** admin interface, click on the **Jump** tab and then the **Jump Clients** page. From here, you can deploy Jump Clients to multiple computers simultaneously.

To begin, choose which **Jump Group** this Jump Client should belong to. This determines which reps can access this Jump Client.

To determine which session features will be available for sessions with this Jump Client, you can choose a public portal, customer present session policy, and customer not present session policy.

Select which policy to apply for sessions where a customer is present or not present.

If you want this Jump Client to be available on a schedule, you can associate it with a Jump Policy.

Enter a name to identify this Jump Client.

You can use a tag if you'd like to have multiple Jump Clients appear under the same heading within a Jump Group.

Choose whether the connection type should be active or passive. Active Jump Clients maintain a persistent connection to your Bomgar Appliance. Passive Jump Clients are non-persistent and listen for connection requests.

If you are going to install these Jump Clients on computers without native internet connections, you can select a Jumpoint already installed on the remote network to proxy the Jump Client connections back to the Bomgar Appliance.

The **Comments** field gives you the option to enter a short note or description associated with this Jump Client. Comments appear on the Rep Console.

Next, set how long the Jump Client installer will remain available.

To install the Jump Client with administrative rights, as a system service, select **Attempt an Elevated Install**. Check **Prompt for elevation credentials** if you suspect the remote system will require the end-user to enter administrative credentials before installation as a system service.

When a Jump Client session is initiated, this Jump Client can display the customer client on the remote screen or start minimized to the task bar.

If you choose to set a password, the password must be entered for a representative to use this Jump Client.

Please note that the **Tag**, **Comments**, and **Password** fields are optional.

You'll see that some of these options have a check box that allows them to be overridden during installation. This lets you to customize individual Jump Client fields without having to create a separate installer for each. The **Mass Deployment Help** section expands to show you the command line parameters that can be used in each case.

Once you click **Create**, you can select the operating system for which to create the installer. The Platform option defaults to the appropriate installer for your current operating system. If you happen to be at the computer you want to later access, you can install the Jump Client immediately.

You can also download the installer file, allowing you to email it to multiple remote users or to distribute it through a systems management tool.

To help manage bandwidth usage, choose which statistics should be displayed in the representative console. Then set how often Active Jump Client statistics should update. You can also set the maximum number of Jump Clients to upgrade concurrently and the maximum bandwidth to be used.

Next, set the maximum number of concurrent connections per second to the appliance that will be allowed. This applies when all jump clients are disconnected and are attempting to re-establish a connection to the appliance, a situation that can occur after an upgrade or a major network outage.

Restricting local uninstall and disable of Jump Clients prevents end-users from disabling the Jump Client via its right-click context menu.

You can set how an uninstalled Jump Client is handled by the rep console. If a user uninstalls a Jump Client at the endpoint, the rep console can either keep the Jump Client in the list and mark it as "Uninstalled" or remove it from the list entirely.

Representatives can also attempt to wake up Jump Clients. When enabled, reps can use Jump Clients on the same network to broadcast Wake-on-LAN (WOL) packets in an attempt to wake up the selected Jump Client.

If using the screen state to detect customer presence, 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. This setting determines whether customer present or customer not present session policy is used.

Privileged reps can deploy Jump Clients during support sessions. Set whether these clients should be active or passive by default.

Network administrators can also set the default port that passive Jump Clients use to listen for support session requests.

Finally, set the number of days before a jump client that has failed to connect to the site should be automatically deleted. Also set the number of days used to determine when a jump client that has failed to connect is considered lost. A lost Jump Client shows up as such in the rep console, allowing an admin to determine if there’s a problem with the Jump Client that needs to be resolved.