Access Invite Portal Branding

Upload an image of your company logo to display on the public-facing web pages of your Privileged Access site. This logo is visible when someone accepts an access invite, goes to the public recording page, responds to an extended availability message, or responds to a request for Jump approval.

API Account Enhancements

API accounts have been expanded to allow you to more securely authenticate to the real-time state API and endpoint credential manager.

Auditability Enhancements for Cloud

Send syslog messages over an encrypted TLS connection to one or more syslog servers.

Enhanced Jump Client Maintenance

No more manually deleting uninstalled Jump Clients from your Jump Interface. An administrator can configure Jump Clients to be automatically removed from the access console once uninstalled or to remain in the list until manually removed.

High Availability ECM

Install multiple endpoint credential managers on different systems to avoid downtime. The appliance routes credential requests through the ECM

with the longest uptime. If that ECM cannot be reached, the appliance immediately begins routing requests through the ECM with the next longest uptime and sends an email to alert the administrator of ECM malfunction.

ITSM Workflow Enhancement

When requiring users to enter a ticket ID before they can access an endpoint, you can also choose to treat the ticket ID as sensitive information. If this setting is enabled, the access console shows asterisks instead of text when the user enters the ID, and the ticket ID is treated with the same level of sensitivity applied to other password fields in the system.

Jump Approver Logging

When a user requests access to a Jump Item, the session report now logs the email address of the person who approved the request. This is logged only if the Jump actually occurs. Additionally, if a second person responds to the request, they can see the email address of the person who already approved or denied the request. The requester cannot see who responded to their request unless they have permission to view the session report.

Jump Groups

Administrators now have more granular control over which Jump Items users can access and which permissions they have on those Jump Items. Jump Item permissions have been moved from user accounts and group policies and into a new Jump Item Role. Additionally, Jump Item access has been separated from teams. Instead, Jump Items are collected into Jump Groups, which grant their members varying levels of access to those items. Users are assigned to Jump Groups individually or through group policies.

Low Profile Jump Clients

To prevent end-users from deleting Jump Clients, right-clicking on a Jump Client no longer gives users the option to uninstall. Instead, an uninstall script is included to allow an administrator to uninstall if necessary. Furthermore, Jump Client icons are now a more subdued color to avoid drawing attention.

More Scalable Jump Client Upgrades

Jump Clients can now finish deploying even if they cannot make an immediate connection to the appliance. This allows you to update your Bomgar software, without having to wait on all Jump Clients to finish redeploying.

Jump Client Silent Install

Improvements to the Jump Client installer allow for a truly silent install using a --silent or /quiet flag.Improvements to the Jump Client installer allow for a truly silent install using a --silent or /quiet flag.

Native Multi-Factor Authentication Using Time-Based One-Time Password

Gain the security of multi-factor authentication for your local and LDAP user accounts by enabling time-based one-time passwords. When logging into Bomgar, users must provide a one-time password generated by a separate device or app, such as Bomgar Verify.

Upgrade Notifications

When checking for updates to your Bomgar software, more informative messages tell you if no updates are available or if an update is available but an error occurred when distributing it to your appliance.

Connection Resilience

Network status intelligence in the access console results in better handling of network disruptions. If you should lose your connection, the access console attempts to reconnect for 60 seconds. If your connection is restored within this time, your access console reopens, restoring all of your open sessions.

Enhanced Authentication Choices for iOS

Both SAML authentication and password managers such as 1Password or LastPass can be used to log into the iOS access console for quicker access.

Jump Client List Auto Refresh

When logging into the desktop access console, the Jump Item list now loads automatically. Updates to Jump Items appear in real time. If someone adds, deletes, or modifies a Jump Item, those changes appear immediately.

Jump Client Searchable Host Data

In the Jump interface of the access console, search for Jump Items by their domain or workgroup.

Monitor Privileged Web

In addition to monitoring or taking over a session, a team manager or lead can silently join a session owned by a team member with a lower role. This allows the manager or lead to observe a session taking place in the privileged web access console.

Password Reset via Email

Reset a forgotten password by means of a secure email link.

Updated Android Access Console and Endpoint Client Apps

Both the Android access console and endpoint client apps feature a new interface for a better experience, while the Android access console also supports SAML authentication for logging in.

Updated Privileged Web Access Console

A new sessions tab shows active sessions as well as session invitations. If another user sends you a chat message in a shared session, a notification appears in the browser. A logout button has been added so that you can exit the privileged web access console without closing the browser tab.

User Experience Enhancements

The desktop access console has been tweaked to provide a better experience. Changes include the option to select favorite queues, a count of sessions in each queue, updated icons, a toggled view of the Jump Items details pane and the session details pane, and more.

VNC Jump Item

Connect to VNC servers with new Remote VNC and Local VNC Jump Item types.

Policy-Based Recordings

Configure Jump Policies to opt out of session recordings even when recordings are enabled site-wide. Jump Policies can be applied to Jump Items as well as Jump Groups such that certain endpoints or users are not recorded.

Web Console File Transfer

From the privileged web access console, you can now upload and download files to and from the remote system.

Advanced Web Access Enhancements

When creating a Web Jump Item for a site that uses a self-signed certificate, you can trust that website even if the certificate cannot be verified. Also, you can download files from websites and uploads files to websites.

Smart Card Enhancements

The virtual smart card dropdown has been updated to present more details for the reader, including if a card is present, not present, or not available. Additionally, when elevating a session, the virtual smart card can be used as a credential store.

Multi-Session Jump items

Enhanced Jump Item settings have been added to the /login interface to enable better handling of multiple simultaneous sessions with Jump Items .

Loopback IP

Specify different local IP addresses to connect simultaneously to multiple devices on the same remote port via protocol tunneling .

SecureApp

Configure RDP Jump Items to launch and access remote applications such as SQL Server Management Studio using credentials from your endpoint credential manager.