BOMGAR™ External Version

Privileged Access 18.1.1 Release Notes

February 27, 2018

Requirements:

- This version of Bomgar has been certified for the physical Bomgar Appliances (B200P & B300P), virtual Bomgar Appliances (Azure, VMware, & Hyper-V), and cloud deployment models.
- This release requires Base software 5.2.0 or later.

New Features and Enhancements:

- **Automatic Privacy Screen:** Start a session with Privacy Screen enabled by default. Sessions can now be kept private from the start without having to remember to set the control permission during each session. Privacy Screen support has also been extended to Mac clients.
- **Shell Tools:** New tools have been added to command line sessions to help streamline workflows. Most notably, users can now clear, copy, and increase a session's scroll-back history.
- **Pseudonymization Support:** Bomgar administrators can respond to Right to Erasure requests by searching for specific criteria supplied by the requester. Once reviewed, the results can be anonymized with an automatically generated term or a custom replacement.
- **Endpoint User Agreement:** Display a prompt on the remote system requesting permission before beginning a session.
- **More Scalable Jump Client Upgrades:** Jump Clients now upgrade faster than ever. Once a new Bomgar version is installed, users can see which Jump Clients are already upgraded and can begin accessing them right away. When a Jump Client is waiting for its upgrade, users can modify properties without having to wait for the upgrade to complete.
- **Credential Injection Enhancements:** When integrating Bomgar with a credential manager, such as Bomgar Vault, the endpoint credential manager (ECM) now returns up to 100 matched credentials. This is especially helpful when similar credentials (such as local and domain accounts with the same name) are both stored in the manager.

Other Enhancements:

- When creating a new Jump Item in the access console, that Jump Item is automatically assigned to the currently selected Jump Group.
- The "End Session" button in the access console is more noticeable.
- When credentials are used for injection to any Jump Item, the use of those credentials is now logged.

Issues Resolved:

Access Console

- Resolved an issue with the screen sharing loading spinner sometimes not being centered correctly.
- Removed the setting to automatically collapse the side bar, since this is done by default.

Jump Clients

- Resolved a Jump Client resource error.

Jumpoint

- Resolved an issue where local Jumps could lock out accounts when Jumping across domains.

Linux

- Resolved an issue with some Headless Linux Jump Clients not upgrading properly.
- Resolved an issue with running the access console on Ubuntu 17.10.

macOS

- Resolved an issue with Jump Clients leaving behind LaunchAgents on macOS systems after being uninstalled.
- Resolved an issue with uploading sound files for certain alerts on macOS.

Privileged Web Access Console

- Resolved an issue with the mouse cursor not being visible.

RDP
- The RDP keyboard layout is now set to match the connecting user's layout.

Web Jump
- Resolved an issue with credential injection for some websites.

Miscellaneous
- The email address entered during account recovery is no longer case-sensitive.
- Removed the "Diagnostic Status" listing from the /login > Status page.
- Removed the Automatic Elevation Service listing from the /login > My Account page, as there is no session elevation in Privileged Access.
- On /login > Access Console > Access Console Settings, updated the value allowed in the field "Number of lines of available command history" to be 100,000.

Known Issues:
- None.

Notes:
- Supports upgrades from PA 16.1.5+. If on a version prior to this, multiple upgrades will be required.
- Requires API version 1.16.0.
- Requires Integration Client 1.6.3.
- Requires Endpoint Credential Manager 1.2.2.
- Certified with the following Bomgar Mobile versions:
  - iOS Access Console 2.2.3+
  - Android Access Console 2.2.4+
  - Android Unattended Access Client 2.2.0+
- NOTE: The above mobile apps require a trusted CA-signed certificate on the appliance.