Privileged Access Management 15.2.1 Release Notes

August 25, 2015

Requirements:

- This version of Bomgar has been certified for the virtual and Bomgar appliance (B300P).
- Both Physical and Virtual Appliances require Base software 4.3.0 or later before installing Bomgar PAM 15.2.1.

New Features and Enhancements:

- **Language Support for PAM**
  - Dutch
  - French
  - German
  - Italian
- **License Reporting and Auditing** – Keep track of the number of endpoint licenses used. Download a zip file containing detailed information on your Bomgar license use.
- **Cloud Access Control** – By leveraging Bomgar's Jump Technology, Privileged Cloud Access Control allows multiple authorized users to securely connect to and manage their cloud infrastructure. Cloud Access Control supports Windows, RedHat, CentOS, and Ubuntu Linux VMs powered by AWS, Azure, VMware, and other IaaS providers. Headless Linux configurations are also supported.
- **Enterprise Credential Manager Enhancements** – Use credentials stored in a password vault to authenticate to end systems, or to use Run As with privileged credentials.
- **Session Forensics** – Search across all sessions based on session events. The feature empowers administrators to quickly and effectively identify critical security events, and aids in the prevention of potential security breaches, as well as evidence discovery.
- **Enhancements to Outbound Events** – Additional macros are now available to the Access Session End event and are available in the email's subject and body.
- **Mobile Access Consoles** – Allow privileged users to access endpoints securely using their mobile devices.

Issues Resolved:

Access Console

- Resolved an issue where Whitelisting applications using hashes would sometimes fail if the application was opened multiple times.
- Resolved an issue with being able to Jump twice to an Endpoint almost instantly if Jump Notifications were enabled.
- The Sidebar is now automatically collapsed when joining a session.
- Resolved an issue with Whitelisting permissions not being applied when a User is joining a Shared session.
- Automatically request screen sharing is the default value for new users now.
- Resolved an issue with not being able to view the desktop after a reboot if Whitelisting was enabled with the Desktop selected.

Security Providers

- Resolved an issue with Security Provider objects being removed when the search base was changed.
- Resolved an issue with Radius and Kerberos non-authenticated whitelisted users not showing as available for Group Policies.
- Resolved an issue with not being able to create local users with the same Name/Display Name as Security Provider accounts.
- Resolved an issue with Users from Security Providers with default Group Policies being shown twice in Teams.

Session Permission Policies

- Resolved an issue with the Jump Policy deletion window not showing some Jump Shortcuts that are associated with the policy.
- Resolved an issue with the Jump Policy drop down menu not hiding when there were not policies configured.

Text Updates
- Resolved an issue with the Failover Sync Time showing the wrong time zone.
- Removed an extra "-" from the Mass Deploy Help documentation.

Miscellaneous
- Resolved an issue with the warning message not appearing after deleting an admin user in an Atlas environment.
- Resolved an issue with the Team Report heading not properly showing the Team Name.
- Reformatting the Session Recording Viewer page.
- Resolved an issue with the links to edit teams still being shown after the user was removed from the permission, "Allowed to edit Teams".
- Resolved an issue with invalid characters not being converted to spaces in Outbound Event Subject lines.

Known Issues:
- None

Notes:
- Requires API version 1.13.0.
- Requires Integration Client 1.3.10+.
- Internet Explorer 8 is no longer supported for the /login interface.
- Bomgar PAM 15.2.1 release is certified with the following Bomgar Mobile versions:
  - iOS™ Access Console (version 2.2.0+)
  - Android Access Console (version 2.2.0+)
  - NOTE: The above mobile apps require trusted CA-signed certificates on the appliance.