BOMGAR™ External Version

Privileged Identity 5.5.4.0 Release Notes

October 23, 2018

New Features:

- **Bomgar Branding:** Bomgar Privileged Identity has been updated with the latest Bomgar branding, including title bars, logos, desktop icons, etc.
- **Disconnected Account Management Elevation:** The Disconnected Account Management (DAM) client now includes self-elevation capabilities. While disconnected from the network, approved endpoint users can generate a time-limited code, enter the code into a DAM agent, and use it to elevate themselves to the local administrators group.
- **Application to Application Password Management:** By installing a host-based agent on Windows endpoints, you can enable embedded application authentication and enforce application attributes such as:
  - Full path of the calling application
  - Matching SHA256 hash of the calling application
  - Authorization of the calling user executing the application
- With this new functionality, developers can securely embed credentials into compiled applications, subject to compliance mandates for rotation. Bomgar Privileged Identity administrators can further lock down these applications, leveraging one or all of the attributes listed above.
- **Shared Credential Lists:** Additional API commands have been added to help administrators manage shared credential lists programmatically. Using the new API commands, administrators can manage comments, names, descriptions and URLs for shared credential lists.
- **Personal Vault:** The personal vault user experience has been improved. Users can sort all columns in their personal password vault, share passwords with others, view password histories, and add custom search panels on the web application's landing page.

Other Enhancements:

- Bomgar Privileged Identity now uses HTML for in-app documentation.
- Added improvements for supporting Cisco devices:
  - Discover user accounts on Cisco devices.
  - Gather system information from Cisco devices.
  - Add administrator account information and connection information when adding a Cisco device.
- The ssh_config file is now checked for alternate AuthorizedKeyFile locations.
- Added “Description” and “Web Site” as fields available for shared credential list text file import.
- Added the ability to update entries in the personal password store without having to update all fields.
- Added a dropdown menu to configure multiple domain groups and local groups for self-service account elevation.
- Added the ability for the requesting user or an administrator to cancel password requests.
- New password requests can now replace pending password requests.
- Administrators are now prompted to set a recovery password upon attempting to view stored passwords for the first time. Alternatively, admins can set the recovery password on the last page of the installer.
- Two unique error codes now show for Linux systems: one for when a system is offline and another for invalid credentials.
- All steps are now shown in SSH jobs.
- Added the ability to configure the utility account when adding Linux systems.
- Job listings are now sorted with the most recent job displayed at the top.
- Machine Name has been added to the end of the Comment field in the Current Elevation Jobs listing. If more than one machine is targeted, the comment displays “Multiple systems”.
- The customer is no longer forced to accept the upgrade check message in the installer.

- Added a permission for shared credential lists, "Alert on Recover", that will send an email alert to the delegation identity.
- Improved the logging of extension components.
- The SAP extension now supports SNC.

Issues Resolved:

- Updated the warning message when cancelling an import of web application SSH key permissions.
- Updated the warning message when installing Privileged Identity without an email address.
- Resolved an issue where saving a blank label in SSH Key View would not reset the value back to default.
- Corrected a text formatting issue on the Import SSH Key window.
- Resolved an issue with SSH certificates discovered during a system scan showing errors in the log window.
- Resolved an issue with the link to the SQL server at the bottom of the Database Data Store Configuration window.
- Added a timeout to jobs set to pre-post run operations before exiting.
- Resolved an issue with the navigation window not appearing in the web application for users with View Accounts permissions.
- Resolved an issue with details not being displayed for shared password requests.
- Resolved an issue where double-clicking on an empty Per Management Set permission, Per System permission, or Per Account permission would bring up the edit window instead of the new window.
- Updated the windows displayed when cancelling a web service installation.
- Resolved an issue with the RDP button not working in the Managed Passwords widget of the web application.
- Manual additions and removals are now logged for all supported platform types.
- Resolved an issue with email alerts displaying the wrong UTC time.
- Resolved an issue with parsing the SUDOers file when multi-line command were used.
- Resolved an issue with "\r" not being correctly escaped in email notifications.
- Removed MindTerm, requiring a different terminal emulator for SSH sessions.
- Resolved an issue where management set filters did not display results as expected.
- Resolved an issue where some scanned information was not removed from the database after deleting Linux systems.
- Resolved several issues with personal password updates not taking effect.
- Resolved an issue where password change jobs against management sets would randomize all passwords except the one targeted for the job creation.
- Resolved an issue with the Asset Tag field not displaying correctly after being saved.
- Updated when buttons are enabled/disabled on the App Data Store Maintenance tab.
- Resolved an issue with cancelling the deferred processor installation.
- Resolved an issue with installing zone processors but not including any existing compliance reporting data store keys.
- Resolved an issue with the operations filters not including a filter for compliance reporting.
- Resolved an issue with the "DO NOT DELETE" flag not displaying the correct value in PowerShell.
- Resolved an issue with running password change jobs against management sets with SAP targets.
- Resolved an issue with app launcher stopping unexpectedly a few seconds after starting.

Notes:

- Supports upgrades from 5.5.3.0+. If on a version prior to this, multiple upgrades will be required.
- Supports the Bomgar PI Endpoint Credential Manager plugin 18.3.1+.