BeyondInsight and Password Safe 23.3.0 Release Notes

December 14, 2023

Requirements:

- A restart might be required after installing this update.

New Features and Enhancements:

General

- **Workforce Passwords** (Browser Extension) now offers the ability to create, update, and delete saved credentials directly from the browser.
- **Workforce Passwords** (Browser Extension) now has support for localization to the same languages as supported by BeyondInsight and Password Safe.
- All Azure Active Directory functionality (Users, Groups, Directory Credentials, Policy Editor Azure AD Search, Managed Accounts Test and Change) now support communication through a web proxy (not applicable to Password Safe Cloud).
- Modified scheduled, active, and completed scans features to ensure history of completed scans is maintained. Scheduled scans can now be deactivated instead of deleted. Completed scans can no longer be deleted. Data retention limits still apply to completed scans.
- Removed the **Minimum Password Age** and **Maximum Password Age** options from the **Configuration > Role Based Access > Local Account Settings** page in BeyondInsight. Guidance from experts in the field indicates that these settings no longer offer significant value.

Password Safe

- Added an **Advanced Details** view for remote applications, providing a simplified read-only view of the application configuration, as well as a global view of all associated managed accounts.
- Added a new global configuration setting for sessions, **Hide record check box for Admin Sessions**, which allows the user to control whether the admin session is recorded.
- Added a new **Account Status** column to the Password Safe **Accounts** grid, which shows whether the specified account is currently available for use (Available / Not Available).
- Added a new default filter to the Password Safe **Approvals** grid to show pending requests from the last 7 days.
- Updated the integrated BeyondTrust Endpoint Credential Manager (ECM) to version 1.6.1 and the ECM Plugin for Password Safe to version 23.1.2.

Password Safe Cloud

- BeyondTrust Identity Insights App Switcher is now supported in BeyondInsight and Password Safe Cloud (not applicable to BeyondInsight on-premises).
- Completed recorded sessions older than 6 months are now automatically archived to Azure Blob Storage (ABS). Recordings in ABS are unavailable to be replayed without first using the **Restore** action on the recorded session.

- For BeyondInsight and Password Safe Cloud only, discovery scan data is now purged after 30 days. Previously it was purged after 90 days.
- For BeyondInsight and Password Safe Cloud only, added optional **Processing Elapsed Time** and **File Format** columns in the **Report Subscriptions** grid on the **Download Reports** window.
- Optimized architecture for resource brokers, as follows:
    - In previous versions of Password Safe, there was a limit of 10 resource brokers per zone. With the release of 23.3, we have optimized the architecture to expand to 200 resource brokers across 50 zones.
    - In previous versions of the resource broker, it was necessary to include a list of Azure endpoints when configuring customer firewall rules. With the release of 23.3, this process has been streamlined, and now only a single outbound rule is needed for "<customer-key>.ps.beyondtrustcloud.com" on port 443. This top level DNS also points to a static IP that can be used in the creation of firewall rules.

Issues Resolved:

Analytics and Reporting

- Removed the **Subscribe to Report** option from the **Discovery** report when launched from the **Completed Scans** grid, since a subscription cannot be created from this location. This prevents users from being taken to a dialog that does not load properly.
- Corrected the report title that appears in the header of the **Managed Account Password Age** report to properly reflect the name of the report. Now the report title and the report name in the report list both reflect the correct name of **Managed Account Password Age**.
- Corrected the display name of the blank value in the **Authentication Alert** parameter on the **Authentication Alert Summary** report. The blank label in the parameter has been replaced with (Blank), and selecting it returns any records that have a blank **Authentication Alert**.
- Resolved an issue where some previously deprecated reports displayed in the report list in **Analytics & Reporting** when this upgrade path was taken: 7.2.1 to 22.1 to 23.3. This fix ensures that reports that have been deprecated remain removed from the application report list regardless of upgrade path.
- Resolved an issue with the **Workforce Passwords Usage Summary** report, which showed an error instead of the header when run from the **Console Reports > Licensing** folder. Now the report shows the header regardless of which path it is run from.
- Resolved an issue with the **Managed** filter and data point on the **Service Account Usage** report. The **Managed** data point now displays correctly and the **Managed** parameter selection filters the report data accordingly.
- Updated several Password Safe Cloud reports (**Admin Session Activity**, **Entitlement by User**, **Password and Session Activity**, and **Remote Session Activity**) to exclude records related to built-in system activity.
- Resolved an issue in the **Days Since Last Login** column of the **Managed vs Unmanaged Account Details** report in Password Safe. If the last login date was between the 1st and 9th of any month, this column displayed **Never**, even though a last login date was known. This fix improves report data integrity.
- Resolved an issue with the **Event List** and **Events by Hour** reports from the **PBUL** folder returning an error in the SSRS log when running, indicating a *problem with the PowerBroker UL Accept Reject Time dimension*. Now the report runs without error as expected.
- Resolved an issue in Password Safe Cloud, where a report subscription listed under **Subscriptions** was not automatically moved from the **New** tab to the **All** tab upon completion. Now the report subscription shows up in the **All** tab when it has successfully completed. This makes it easier for users to find.
- Removed deprecated **Risk** field from the **Asset > Software** report. This ensures that the report reflects only data that is currently relevant.
- Resolved an issue where the **Asset > Software** report often included recently removed software, not respecting the selected scan parameter. Now the report displays the software associated with the selected scan.

Active Directory Group Sync

- Improved Active Directory Group Sync logic to reduce database usage in instances where the sync fails repeatedly. Reduced database usage in this scenario has less impact on other database activities, which might result in improved performance.
- Corrected inaccurate labeling of success messages as warnings in the Active Directory Group Sync processing to reduce noise in the Omniworker log file. Fewer warnings in the logs might mean smaller log files and less irrelevant data points there.

Minor Localization, Keyboard Navigation, Verbiage, and UI Changes

- Removed grid refresh and expand buttons, as well as the grid page navigation bar, from the **Query Test Results** grid in a **Directory Query**, as they are not helpful to have here. Now the **Query Test Results** grid is simplified and does not contain extra actions that could confuse users.
- Resolved some minor issues with focus, localization, verbiage, spelling, translation and screen reader announcements in various places in the application. This improves keyboard navigation and screen reader usage for all users, and should aid non-English users in reading labels on our UI.
- Aligned UI with UX guidelines by replacing **Save** buttons with the more specific **Update** and **Create** buttons on pages including **Scan Details** and **Configuration > Mail Templates**, **Worker Nodes**, and **Ticket Systems**. This improves consistency across the application.
- Resolved an issue where an incorrect validation message appeared on IP address during the manual creation of a new asset.
- Resolved an issue in the **Smart Rules** grid where the right **Details** panel stayed open even if the grid filters and contents changed. Now the side panel is closed whenever the user changes the filters, removing a potential cause for confusion.
- Improved the **Smart Rule** grid so that after requesting a Smart Rule to process, upon grid refresh, the grid scrolls to the selected Smart Rule. This makes it easier to see the current status of that Smart Rule.
- Resolved an issue where the deprecated **Use Private IP Address** option appeared unexpectedly in the Smart Rule configuration **Selection Criteria** section, when **Cloud Asset Connectors to Filter With** criteria was added. This option is no longer valid and no longer appears in the user interface.
- Resolved an issue where the **Server Keys** panel would not load under **Advanced Details** for a managed system if no server keys were present. Now the panel loads whether or not there are server keys present.
- Resolved an issue where the format of the **Account** string on a new Password Safe request contained a forward slash (/) character instead of the correct backslash (\) character. Now if a user copies this string and pastes it elsewhere, they won't have to edit the text in order to use it.
- Resolved an issue where the configured resource zone did not appear after saving a change to the RADIUS alias. The change was being saved, but did not show up in the user interface. Now it shows up.

Discovery Scanning

- Resolved an issue where editing the start date and time on a one time scheduled scan gave an error message. Now the start date and time on a one-time scheduled scan can be edited, so customers can fine tune the timing of an upcoming one-time scheduled scan.
- Resolved an issue where, occasionally, editing some scan credentials resulted in the edit form missing several fields. All form fields now display properly when editing these credentials.
- Resolved an issue with the **Credentials** list in the Scan Details and Scan Wizard so that it now refreshes when changing organizations. Customers editing scheduled scans in multi-org environments now see a **Credentials** list refresh if they switch to another organization while on this screen.
- Resolved an issue in the Scan Wizard where a newly added credential did not show up in search results on the **Enter Credentials** step without a refresh. Now, when a new credential is added, it shows up in the **Credentials** list and can be found in searches. This might improve a customer's experience in finding appropriate credentials to use during a scan.

- Resolved an issue with 1200 x 800 screen resolution where a number of UI elements were not displayed properly on the **Enter Credentials** step of the Scan Wizard. Now the UI elements align properly at all supported screen resolutions. This might make it easier for a customer to use this screen if they are using a 1200 x 800 screen resolution.
- Resolved an issue where key validation is prompted in the Scan Wizard if a stored credential with a key was selected, then deselected and replaced with a custom credential. We have improved the logic used to determine when to show the key validation panel, so users should only see it when it's truly needed.
- Resolved an issue where when viewing scan details for a scheduled scan, and selecting the **Deselect All** action in the Credentials list, and then clicking **Update Credentials**, did not save the changes appropriately in some cases. A change was made to improve the logic used to determine which credentials in the **Credentials** list are selected at any given time, so that updating credentials should now reflect the user's choices.
- Resolved an issue where when editing the details for an existing scheduled scan, changes made to **Deploy Local Scan Service** under **Detailed Discovery Options** was not always sent to the scanner. Now, regardless of the selected choice for the **Deploy Local Scan Service** value, the appropriate value is sent to the scanner.
- Resolved an issue where the count on the **History** section of the **Scan Data** details of a scheduled scan was not updating to reflect the items in the history for the scanner selected in the **Details and Attributes** section. Now, when saving the change to select a different scanner (only possible on scans originally set up with multiple scanners), the count beside the **History** section is updated to reflect the number of items in the corresponding **History** grid.
- Improved the credential key validation workflow in the scheduled scan details editing process, so that if the user has already typed the key to validate a credential, they are not prompted to do so again if another credential requires validation, as long as they have not left the page.
- Added validation so that a one-time scan cannot be scheduled to start in the past. This reduces the opportunity for users to encounter errors.
- Resolved an issue where the **Abort** setting configured for a one-time immediate scheduled scan was not always passed to the scanner, causing the scanner to ignore the scan restrictions in those instances.
- Resolved an issue where occasionally, editing the schedule details of a scheduled scan showed blank fields for some of the schedule data points. This might have been misleading as the schedule details were still present and stored in the database.

Endpoint Privilege Management

- Resolved an issue that prevented the Policy Editor in BeyondInsight from accommodating policies that are between 10 and 20 MB in size in anticipation of an increase in maximum policy size coming in Policy Editor 24.1.
- Resolved an issue where changing the selected organization did not refresh the **Policies** grid until the user did so manually. Now, changing the organization triggers the grid to refresh automatically. This contributes to a better user experience.
- Added required field validation to most fields in **Configuration > Endpoint Privilege Management > Privilege Management Reporting**. Now all fields except **SQL Connection Options** are required to successfully save this configuration. This reduces the likelihood of invalid configuration settings in this area.
- Restored a clickable **Events** link under **Asset Details** for **Endpoint Privilege Management Events**, taking the user to the appropriate grid and filtered to show the events for the currently selected asset. Now the events for a particular asset can be viewed via a single click instead of having to load and filter the **Events** grid.

Password Safe

- Resolved an issue where if a local functional account is configured to be used as a login account on a managed system and also enabled for automatic rotation, the password rotation fails. Now all functional accounts that have automatic rotation enabled, rotate properly even if used only as a login account.
- Resolved an issue where case mismatches between a system's local user account name and that same account name stored in BeyondInsight caused the account to be excluded from managed account Smart Rules with a user account attribute selection criteria that would otherwise have included it.

- Resolved an issue causing the MSSQL functional account test in on-premises environments to always return a bad gateway error.
- Resolved an issue causing the Password Safe Omniworker log to incorrectly log an error. Now that error is no longer logged.
- Resolved an issue where linking applications to managed system Smart Rules was not working as expected. Now you see the application listed on all managed systems of the Smart Rule.
- Resolved an issue with the PUT and POST Secrets Safe Secret APIs where trying to add a URL with more than 2048 characters returned the wrong error code. Now the request fails with an error that the URLs max length was exceeded.
- Resolved an issue in the **PUT Secrets-Safe/Folders/{id}** API where users were able to update the **ParentID** of Secrets Safe folders. This parameter is now ignored.
- Resolved an issue in the **PUT Secrets-Safe/Secrets/{id}/file** API where the URL field was not being properly updated. Now the URL is successfully updated when changed to a valid value.
- Resolved an issue were where RDP direct connect sessions always fail when the passwords start with the character used as the delimiter and multi-factor authentication is not enabled. Now the RDP direct connect session can successfully connect in this scenario.
- Resolved an issue where MSSQL password rotation fails in cloud environments. The password now successfully rotates.
- Resolved an issue where searching for a requestor's name in the **Approvals** tab failed to find results when the search included a space. Now the correct results are returned.
- Resolved an issue where testing the functional account fails with an unauthorized error when testing against SAP and vSphere Web API platforms. Now the test successfully completes.
- Resolved an issue where a managed system for MongoDB can't manually be created or edited if a database already exists using the same port.
- Resolved an issue with a naming inconsistency when displaying the SSH-DSS Key authentication type. All areas previously displaying DSS now correctly display SSH-DSS Key.
- Resolved an issue where users were able to update the name of a Secrets Safe folder to an already existing folder name using the public API.
- Resolved an issue with the HTTP error code being returned in the public API when a user attempts to create a duplicate Secrets Safe folder name. Now *error 409, Folder already exists* is returned.
- Resolved an issue where functional accounts always fail to update the first time they are edited. Now functional accounts update on the first attempt with valid settings.
- Resolved an issue where the public API incorrectly returned a success code when attempting to create a Secrets Safe folder with invalid parameters. The API now returns an error code.
- Resolved an issue where disabled user groups were visible to users in Secrets Safe.
- Resolved an issue where users who should only be able to access Secrets Safe were also able to navigate to an empty configuration menu. Now these users have no option to access the configuration menu.
- Resolved an issue in Secrets Safe where some symbols were shown as html code in the toast messages. Now the symbols are displayed correctly.
- Resolved an issue in Secrets Safe when navigating the menu with a keyboard, where the focus does not shift to the correct input after clicking to edit a secret. Now the focus shifts to the correct input automatically.
- Resolved an issue in Secrets Safe where a user would receive an incorrect HTTP error code when refreshing the page if that user was already logged into the console and had been deleted from the server. Now a 403 error code is returned.
- Resolved an issue where the **Include Disabled Accounts** Smart Rule criteria was not being honored for all database platforms. Now this criteria affects the results being returned.
- Resolved an issue in **User Audits** where the audit details were potentially confusing when changing the owner of a secret in Secrets Safe to or from an entire team. Now **OwnersDisplay** detail shows the ownership change details for both users and groups.
- Corrected a formatting issue when viewing the schedule for an access policy where there was an unnecessary gap between the **All Day** and schedule entries.

- Resolved an issue where inaccessible sections of the configuration screens were displayed to read-only users. Now these sections are hidden from view.
- Resolved an issue in **User Audits** which showed the owner being set to null when assigning ownership of a secret to the entire team.
- Resolved an issue in **Secrets Safe** with displaying the selected owners when managing ownership on multiple pages of users. Now when navigating between pages all selected owners remain checked.
- Resolved an issue where the audit log was not displaying the change when modifying an attribute in a secret's value from null. Now the audit log displays the original and new values.
- Resolved an issue where the account and system concurrency behavior was not being calculated correctly. Now the correct availability is calculated.
- Resolved an issue where users were unable to start cloud application sessions when a directory account is linked with a Cloud MS. Previously the user would receive an error that the TargetURL was not assigned. Now the session successfully opens.
- Resolved an error where the **Direct Connect Connection String** and **Connection Command** values do not include the host name value after a host name override has been removed. Now the host name value is added when the override is removed.
- Resolved an issue in the Password Safe **Accounts** grid where sorting columns did not work after applying a filter. Now the columns sort with a filter applied.
- Resolved an issue in the **Linked Systems** section of managed accounts when the **Show** filter is set to **Linked** and **Filter by** is set to **Platform**. Previously cloud platforms were not listed for selection.
- Resolved an issue in **Quick Launch** where users were unable to create a request for the maximum configured duration. Previously the calculation of end time was incorrectly calculating the max duration.
- Resolved an issue where a Mac managed account with temp lock applied gave a false positive when testing the account.
- Resolved an issue in Password Safe where starting a session from an existing request sent a preferred node when not expected. Now, when node selection is not enabled, a node is not included when creating a session from an existing request
- Resolved an issue with the Password Safe Enhanced Session Utility standalone installer where the scheduled task was unable to start the service after an installation was performed. Now the scheduled task is able to successfully start the service.
- Resolved an issue in the **PSAutomate** utility where the correct browse webdriver was not always successfully downloaded, which would prevent successful remote application launches.

Other

- Resolved an issue that prevented session timeout configuration change from working properly in Password Safe Cloud. Now session timeout updates take effect within 30 seconds and do not require any manual intervention from the user or administrator
- For BeyondInsight on-premises only, restored the **Machine Name** column to the **System Event Viewer** grid so it is now visible and can be filtered on. There is no change to the **System Event Viewer** grid when using BeyondInsight Cloud.
- Resolved an issue that was preventing the **Hide All Maintenance Banners** setting on the **About** page being retained. Now the toggle retains the user’s preferred setting. This ensures that the maintenance banner remains hidden if the administrator has set the toggle for it to do so.
- Resolved an issue where Azure AD API Authentication was not working if the user in question is also a member of a local group in BeyondInsight. Now, API logins succeed even if the Azure AD user is a member of a local group.
- Ensured that the deprecated, unused Event Server Windows Service has been removed in any new installation scenarios. Removing deprecated elements of the software improves engineering quality of life and reduces complexity.
- Resolved an issue in **User Audits** where an LDAP directory query edit might result in the audit record indicating that a platform changed, even if the platform did not change. This improves the integrity of the **User Audits** data.
- Resolved an issue that caused an error when the API **GetUserAudits** endpoint is called for all audits and all details, if an audit of type **PMR Database Settings** existed. Now, the presence of this particular type of audit record does not cause errors with this API call.

- Resolved an issue on the **SAML Configuration** page to ensure that the URLs are validated appropriately. Now URLs with uppercase letters, custom ports, and longer TLDs do not fail validation, so SAML configuration can be completed in more cases without having to obtain assistance from support.
- Resolved an issue where Azure AD API Authentication was not working if the user in question is also a member of a local group in BeyondInsight. Now, API logins succeed even if the Azure AD user is a member of a local group's shared folder found under **All Secrets**. If the user is enabled for Workforce Passwords, this is their **Personal Folder**.
- Resolved an issue in the Smart Rules editor for a managed account Smart Rule, where selecting the domain when using the action to **Assign preferred Domain Controller on each Active Directory account** might have caused an error to appear. Now this action does not cause an error.
- Improved performance of Azure Active Directory logins when the API user is a member of a large number of Azure Active Directory groups in BeyondInsight.
- Resolved an issue where the **Configuration > Authentication Management > Authentication Options > Disable Forms Login for new directory accounts** setting was not applying to new directory users if their account was created via forms login.

Known Issues:

- Endpoint Privilege Management Policy Editor version 23.9 or earlier cannot open any policy that is 20 MB or larger. If a policy of this size is created (for example, by merging 2 large policies) in the Policy Editor, it can be saved in BeyondInsight 23.3, but not checked out for edit. If this occurs, it could cause delays in making edits to very large policies.
  - **Workaround:** Avoid creating policies that are of a size close to 20 MB, upgrade to Policy Editor 24.1 or newer (when available), or work with support to edit the policy XML outside of the editor if the policy has already been created and upgrading is not an option.
- When creating or editing a Password Safe Password Policy, it is not possible to change the **First Character Value** setting from the default value of ***Any Character Permitted***.
  - **Workaround:** None, this will be addressed in a future release.
- When accessing a report subscription in an on-premises installation of BeyondInsight and Password Safe, the **Download Reports** menu item is non-functional. This option is for Password Safe Cloud only, and should not be visible in the user interface.
  - **Workaround:** None needed, this menu item is being removed in a future release.
- When viewing the details of a user in the **User Management** configuration screen, the **Groups** grid is incorrectly repeating the group name in the group **Type** column.
  - **Workaround:** To determine the group type, navigate to the **User Management > Groups** configuration screen.
- When attempting to use a remote application that is configured to not use **RemoteApp Mode** and the assigned functional account has administrative privileges on the RDS server, the application fails to launch.
  - **Workaround:** Enable **RemoteApp Mode** for the application.
- If a user has marked a domain linked account as a favorite in Password Safe and the domain account link is subsequently removed (but the managed account and target managed system still exist), then the favorite entry still remains in the users **Favorites** list but will be non-functional.
  - **Workaround:** Un-favorite the domain linked account. This is being addressed in a future release.
- When making a call to the **GET UserGroups** API, the **GroupType** field is incorrectly (since version 23.2) returned as an int value, when it was previously documented as a string. This is being addressed in a hotfix and included in a future release.
- If an Active Directory group has been granted the **Secrets Safe** feature and is subsequently renamed, the new group name is not reflected in the **Secret Safe** folder name.
  - **Workaround:** None - this does not affect access to the folder or its secrets, and the folder name display is being resolved in a future release.

- The **Reviewed Sessions** report in **Analytics & Reporting** may not correctly identify the **Reviewed By** and **Reviewed Date** for reviewed sessions. As a result, the **Reviewed** parameter, when set to **Yes**, may not return the **Reviewed** rows as expected.
    - **Workaround:** None, this is being fixed in a future version and may be available earlier in a hotfix.
- In some environments with a large amount of request data, attempting to view request details can take an excessive amount of time to load, or returns in an error causing the details not to be displayed. Improvements have been made in this release; however, further improvements are in progress and will be available as a hotfix.
- If a user attempts to use SAML Login for the Workforce Passwords extension, while already logged into the web interface using SAML, they cannot log into the extension.
    - **Workaround:** If using SAML, and needing to be logged into the extension and web interface at the same time on the same browser, log into the Workforce Passwords extension first and then log into the web interface.
- Creating a new secret via the API **POST Secrets-Safe/Folders/{folderId:guid}/secrets** returns an empty string in the **FolderPath** property of the response body. This is being addressed in a hotfix.

> ***Note:*** *Issues discovered after release can be found within our product Knowledge Base at https://beyondtrustcorp.service-now.com/csm?id=csm_prod_kb_view.*

Notes:

- Direct upgrades to 23.3 are supported from BeyondInsight version 22.1 or later releases.
- .NET hosting bundle updated from v6.0.21 -> 6.0.25
- .NET hosting bundle updated from v7.0.10 -> 7.0.14
- This release is available to download for BeyondTrust customers from https://beyondtrustcorp.service-now.com/csm using BeyondTrust BT Updater.
- The MD5 signature is: e701bcaa470a98c974f3bbb8a7b0b36d
- The SHA-1 signature is: 46efbf297bf9f84b5636f4e2a4150bf3d40eb813
- The SHA-256 signature is: ade9b8b642848fbe19adb10b37de35421f1347744793a91afcc6175bcb18ac21

> *For information on which operating systems, platforms, BeyondTrust product integrations, and third party product integrations are supported, please see Supported Platforms at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/supported-platforms/index.htm.*