BeyondInsight and Password Safe 23.1.0 Release Notes

June 1, 2023

New Features and Enhancements:

General

- Updated remaining areas in management console and user portal UI to abide by newer UX recommendations and improve performance and accessibility.
- Added support to create a Directory Query with new Directory Credential from the Smart Rule editor.
- Added support for sending scan credentials on demand to BeyondTrust Discovery Agent.
- Added support for using an email address as username for login.
- Added Quick Navigation feature, including support for saving favorite destinations within the UI.
- Added option to sync AD groups on a schedule, globally, and with the option to make exceptions for individual groups.
- Removed SQL 2012 from supported installation prerequisites.
- Updated display of local user password policy compliance in **Reset**, **Change**, and initial set password areas.
- Renamed **Send Analysis to Support** section on **About** page to **BeyondInsight Analysis**.
- Removed deprecated **Send Analysis to Support** and the **Request Deletion of Previously Submitted Reports** options from the **About** page.
- Removed all remaining references to Attack and Malware data from **Smart Rules** and **Configuration** areas.
- **Save**/**Submit**/**Update** buttons in configuration cards are now always enabled.
- Updated display names of former McAfee connector types to Trellix.

Analytics and Reporting

- Updated remaining areas in Analytics & Reporting UI to abide by newer UX recommendations and improve accessibility.
- Updated Password Activity Report to include details about who initiated any manual password change.
- Added new report, **Reviewed Sessions**, to provided details on whether sessions were reviewed, when, and by whom.
- Added new report, **Smart Rule Overlap**, to provide diagnostic information about assets or accounts that are selected for management in Password Safe by multiple Smart Rules.
- Added new report, **Application Audit**, to provide a list of who has administrative access to applications.
- Added new report, **User Audit**, to provide capability to report on the activity of BeyondInsight users.
- Removed all remaining Vulnerability Management, Attack, and Malware reports from the product.
- Removed all remaining references to Attack and Malware data from reports in the product.

Endpoint Privilege Management

- Updated remaining Endpoint Privilege Management UI to abide by newer UX recommendations and improve accessibility (on-premises only).

- Added support for integration with 23.4 release of Policy Editor (on-premises only), including:
  - Simplified installation process
  - Support for policy edits initiated by Privilege Management Reporting 23.4
- Added support for integration with Privilege Management Reporting 23.4 (on-premises only), including:
  - AngularJS-free UI
  - Capability to add applications to policies from events in the reporting UI
  - Simplified installation process
- Added support to leverage existing connector types to forward Privilege Management Reporting Events (on-premises only).
- Updated visibility of Privilege Management Reporting configuration card to depend on the associated services being installed.
- Improved display of integration service names and versions on the **About** page.
- Renamed title of **Plugin Configuration** card to **Privilege Management Reporting Database Configuration**.

Password Safe

- Updated Password Safe Web Portal: The updated web portal enhances productivity with fewer tabs and a new menu structure that simplifies access to credentials and systems, and provides an updated look and feel for a streamlined experience and improved accessibility.
  - Please follow this link to take a tour of the updated Password Safe Web Portal: PS 23.1 Portal Tour | BeyondTrust
- Updated remaining areas in management console and user portal UI to abide by newer UX recommendations and improve accessibility.
- OAuth authentication support has been added to the Public API.
- New Secrets Safe DevOps Integrations: Terraform and Azure DevOps.
- Password Safe Cache now supports Secrets Safe secrets (credentials, file, and text secret types).
- Enhanced RDP Session options: added support for multiple monitors, allow client application to detect best resolution, saving RDP settings for future remote sessions, and ability to specify the RDP port on a per-system basis.
- New Password Safe administration permissions, allowing administrators to delegate specific permissions resulting in fewer high level administrative users:
  - Password Safe Configuration Management
  - Password Safe Policy Management
  - Password Safe Agent Management
- Deprecation of multi-system checkout: this release has removed the multi-system checkout capability. Users can still checkout systems individually.

Password Safe Cloud

- Added CSV export format for reports.
- Restored Quarantined Account setting to the UI.
- Improved insights into metrics on product usage by integrating Gainsight to drive future priorities and customer success.

API

- Custom Platform import/export support.
  - New APIs:
    - **GET CustomPlatforms/**
    - **GET CustomPlatforms/{id}**
    - **POST CustomPlatforms/Import}**
    - **POST CustomPlatforms/{id}/Export**
- OAuth and API Registration support.
  - New APIs:
    - **GET ApiRegistrations/**
    - **GET ApiRegistrations/{id}**
    - **POST ApiRegistrations**
    - **PUT ApiRegistrations/{id}**
    - **DELETE ApiRegistrations/{id}**
    - **POST ApiRegistrations/{id}/Rotate**
    - **GET ApiRegistrations/{id}/Key**
    - **POST Users/{id}/RecycleClientSecret**
    - **POST Auth/Connect/Token**
  - Updated APIs:
    - **GET Users/{id}**
    - **GET Users/**
    - **POST Users/**
    - **PUT Users/{id}**
    - **POST Auth/SignAppIn**
- Secrets Safe added additional search/filter capabilities.
  - **GET Secrets-Safe/Secrets**

Issues Resolved:

23.1.0

- Determined that some measures in the pivot grid not accurately representing the value stored in the cube were limited to development systems and ddid not occur on customer environments; removed this from the **Known Issues** list.
- Determined that the display of **UNKNOWN** for some **Asset Advanced Details** fields is expected behavior when this is all that BeyondInsight knows about the asset; removed this from the **Known Issues** list.
- Resolved an issue in new asset creation in which the previously selected asset's details were populated in the new asset creation form.
- Resolved an issue with the **User Type** filter on the **Asset Advanced Details – Users** tab. It now works for domain user, local user, and administrator.

- Resolved an issue with the user fields in the edit panel appearing cleared when editing a user from the **User Details** edit panel.
- Resolved an issue with deletion of directory credentials if the name is longer than 80 characters.
- Resolved an issue with access to Endpoint Privilege Management **Events** page from main menu by a user with read-only permission to Endpoint Privilege Management.
- Resolved an issue which enabled the Global Credential Key when upgrading from 22.3.0.1270. After upgrading from 22.3.0.1270 to 22.4.0.1101, if the Global Credential Key switch was off prior to the upgrade, it will be enabled after the upgrade. Workaround: Update it to the desired setting in the **Configuration** area, either switching it off, or setting a global key for use with any pre-existing.
- Resolved ed an issue with SSH credential edits showing with an error indicating that there are invalid fields if no private key was included in the edit action.
- Resolved an issue with duplicate *Discard Changes?* confirmation prompts when cancelling the creation of a new propagation action.
- Resolved an issue with an error preventing the deletion of an Active Directory managed system that contains one or more Active Directory managed accounts that have at least one propagation action assigned.
- Resolved an issue with filtering by more than one type in the **Configuration - Propagation Actions** grid.
- Resolved an issue with new session mask creation sometimes failing with a *One or more fields are invalid* error message.
- Resolved an issue with the Functional Account domain field being used rather than the Instance URL when using a Jira Connector for ticket system validation.

Known Issues:

23.1.0

- Searching in the **Authentication Type** dropdown in the create form of a MS SQL Server Discovery Credential does not work. Workaround: The list of Authentication Types is very short; use the keyboard up and down arrows or a mouse to select the desired one. This will be fixed in an upcoming release.
- Creating a scan using a new MS SQL Server Credential (added using the **Create New Credential** link within the Scan Wizard) gives an error. Workaround: Either use a pre-existing MS SQL Server credential, or run the Scan Wizard a second time (using the credential created the first time). This will be fixed in an upcoming release.
- In the Scan Wizard, when searching for a subset of credentials, and using **Select All**, all credentials (even those that don't match the search) are selected. Workaround: Manually select the credential(s) to be used, rather than using the **Select All** function. The current and expected behavior is being reviewed with UX and might be updated in the future.
- In the Scan Wizard, when choosing credentials and selecting, then deselecting some or all, (so that none are selected), clicking **Next** prompts to validate credential keys, but does not list any credentials. Workaround: Cancel, and select at least one credential from the list, and then proceed. Alternately, click **Validate**, and a warning will be shown that a credential must be selected from the list. Then select at least one credential from the list and proceed. This will be fixed in an upcoming release.
- In the Scan Wizard, when entering a custom credential, if you've previously selected/deselected any credentials in the **Existing Credentials** list, clicking **Next** prompts to validate credential keys, but does not list any credentials. Workaround: Click **Validate**, then proceed. This will be fixed in an upcoming release.
- When editing Scheduled Scan Detailed Discovery Options, the UI might display a value in the **Deploy Local Scan Service** dropdown, which does not reflect the value that was originally set upon scan creation. Workaround: Do not be alarmed if the UI on the edit screen shows the wrong value. The scanner will respect the original setting. Edits to other aspects of the scheduled scan will not change the value of Deploy Local Scan Service behind the scenes. Editing this field on a scheduled scan may not appear to adhere in the UI, but the value that is chosen will be used behind the scenes.
- In the Scan Wizard, when customizing the options for a detailed discovery scan, a validation error occurs if entering more than 100 users in the Limit accounts returned option. Workaround: this warning can be ignored. It does not prevent you from saving, and the value entered by the user gets submitted to the scanner.

- After saving a change to the target Smart Rule on a recurring scan edit, the user may receive an unsaved changes warning when attempting to navigate away. Workaround: It is safe to click **Discard Changes**; the updated target has been saved. This will be fixed in an upcoming release.
- In the **Schedule** tab of a recurring scan edit, there is an option to change the scan from Recurring to Immediate. Using this option gives an error message and does not save the changes. Workaround: Please do not use this option; it is not valid in this location. If it is desired to run a scheduled scan immediately, use the **Run Now** option from the **Active/Completed Scans** grid. This **Immediate** schedule option will be removed from the UI in an upcoming release
- If a local user sets their password of a given length, and the password policy is later updated to limit password lengths to a shorter length, that user will be unable to enter their current password in the **Change Password** form (as the length restriction is incorrectly applied to this field). Workaround: The user can follow the reset password process to change their password, the administrator can edit the user to give them a new complaint password, or the password policy can be increased to its previous length. This will be fixed in an upcoming release.
- Cloud only: When exporting the Asset report to CSV, the first page of the report is not included in the exported CSV file. This page contains summary data. Workaround: This data can, if desired, be compiled from the individual detail records, which are included in the CSV.
- Cloud only: When exporting the Service, Software, User Account, Operating System, and Port reports to CSV, the **Top 5** and **Bottom 5** sections are missing from the exported CSV file. Workaround: This data can, if desired, be compiled from the individual detail records, which are included in the CSV.
- In the **Asset > Advanced Details > Users** grid row details, the SSH Key Count field might be zero, even if there are SSH Keys that exist for that user. Workaround: None. This will be fixed in an upcoming release.
- In an environment that uses Windows Authentication, Privilege Management Reporting will not load. This is not a typical setup and is unlikely to be encountered. However, in rare situations it might be possible. Workaround: Ensure dbo permissions for NT AUTHORITY/SYSTEM account on the BeyondInsight/RetinaCS database. Restart services and perform IIS reset.
- Any existing access policy which has location restriction enabled with X-Forwarding set to **All**, after upgrading to 23.1 the X-forwarding field will show blank and disabled. Workaround: Toggle the **Location Restriction** switch off and back on to enable the **X-forwarding** field.
- UI: Duration Picker control has help text on each control to show the max allowable value. However, if the bound value is updated after the control has initially rendered, the help text is not updated to reflect the change. Workaround: None; ignore the help text. Proper validation occurs at submit.
- Session archiving: When in a multi-node configuration, the **Archive** option is still available even if archiving is not supported by the node. Workaround: None; ignore error if archive is attempted, or set up archiving on that node.
- Session archiving: When an archive is attempted and the destination path does not exist or is wrong, then the status remains stuck in *Archiving*. Workaround: Fix the archive path, and reset the status in the DB manually.
- Session replay: Firefox: Viewing an active session, terminating it, and then trying to replay the session from **Completed Sessions** results in an error.
- Password rotation: When a view password request has been denied after the password has been viewed but before the request is checked-in or expired, then the password is not triggered for rotation. Workaround: If an Admin/Approver denied a view password request after it has already been approved (and potentially used), then we recommend that they trigger a manual rotation on that account.
- Global AD group sync can sometimes fail in Password Safe Cloud when configured to use a preferred domain controller. Workaround: Don't use a preferred domain controller. This will be fixed in an upcoming release.
- Editing an existing functional account with an assigned DSS key incorrectly requires the DSS key to be re-uploaded when saving any change to the functional account.
- When upgrading the Policy Editor to 23.4, in some cases, the JRE folder becomes corrupted, which causes the Policy Editor to fail to load. Workaround: Uninstall and then reinstall, or, if the latest Privilege Management Reporting is installed, copy the JRE folder from there into the Web Policy Editor location.

- Global keystroke search from the **Completed Sessions** grid is currently not available. Keystroke searching can be accomplished per-session from the **Session Replay** screen and globally across sessions via the API. This functionality will be restored in an upcoming release.
- Registry Monitoring Events are not showing up on the report, and are not normalized to the database. An error about a missing stored procedure may be observed in the logs. Workaround: Contact support to restore the missing stored procedure to the database so subsequent events can be normalized. Once the daily Analytics and Reporting sync job runs, the subsequent events will show up in the report. This stored procedure will be restored to the database in an upcoming release.

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:

- Removed **Status** column from the **Linked Accounts** and **Domain Linked Accounts** grids. This feature will be re-added in an upcoming release.
- Direct upgrades to 23.1.0 are supported from BeyondInsight versions 21.2 or higher.
- This release is available by download for BeyondTrust customers (https://beyondtrustcorp.service-now.com/csm) and by using the BeyondTrust BT Updater.
- The MD5 signature is: ce72fe03e6770e3d171a5bd2f176e376
- The SHA-1 signature is: a83f2d3b09807064323e68e900adce75b360b33b
- The SHA-256 signature is: 573730d220ebcaf57588472c95edfe7e68ee8415c3fff17b131d75d4465f77ab