BeyondInsight and Password Safe 23.2.0 Release Notes

Sept. 26, 2023

Requirements:

- Requires version 23.1.3.1308 or later release of BeyondTrust Discovery Agent.
- A restart might be required after installing this update.

New Features and Enhancements:

General

- **Workforce Passwords** is a new add-on product that provides enterprise-scale visibility to employee business application password management, leveraging the power of BeyondTrust Password Safe 23.2 and later releases, as follows:
    - Allows users to store their credentials for URLs they access, in secure **Personal Folders** within Secrets Safe, that only the owner of the folder can access and view.
    - Provides mapping of URLs to the stored credentials. Both 1:1 mapping and mapping many credentials to 1 URL is supported.
    - Users can perform Create, Read, Update, and Delete (CRUD) operations within their personal folder for credentials and URL associations. These actions are audited.
    - Users can use Password Safe password policies and password generator for creating new passwords for URLs.
    - Provides a browser extension allowing users to retrieve credentials for their URLs.
- Enhanced auditing of Smart Rule management actions to capture Smart Rule content details and to provide before and after audit details when Smart Rules are edited. Previous releases only captured the create and edit action, without providing any details. Enhanced audit details are useful for SOX compliance auditing.
- Improved navigation between Smart Rule creation and Smart Rule grid by adding the ability to preview the results of a Smart Rule in-line. This allows the user to test and validate the rule at the time of creation or update so that necessary adjustments can be made at that time.
- Added **Download all** option to **Groups** and **Users** grids. This action downloads a CSV file containing grid data based on selected filters.
- Added support for Microsoft SQL Server 2022. Customers can configure BeyondInsight 23.2 and later releases with MS SQL Server 2022 as its external database.
- Added **Run a New Discovery Scan** quick link to the **Scans** page.
- Made minor adjustments to the create and edit forms for creating and editing a discovery management scan credential. Specifically, the layout has been slightly modified and the **Description** field has been renamed to **Credential Name**.
- On the **Create New Directory Query** form, set the default value of the **Name** field for the **Basic Filter** to * .
- Improved Dark Mode styling in the App Menu.
- Improved verbiage around local user password policy compliance. The password policy error text in releases prior to 23.2 is confusing when characters that are not permitted are used.
- Removed support for deprecated FireEye connector.
- Removed deprecated Asset Risk data point from multiple areas in the BeyondInsight user interface.

- Removed reports and user interface elements referencing the deprecated BeyondInsight Ticket system.
- Removed deprecated Clarity Malware Analysis from Clarity Analytics and Configuration areas in the BeyondInsight user interface.
- .NET hosting bundle v3.1.23 is no longer included.
- .NET hosting bundle updated from v6.0.19 to v6.0.21.
- .NET hosting bundle v7.0.10 has been added.

Analytics & Reporting

- Added a new Password Safe report called **Inactive Managed Accounts**, which shows a list of accounts that are inactive or have not been accessed by requester in X days.
- Improved existing **Service Account Usage** report by adding new parameters for **Service Name** and **Service Account is Managed All/Y/N**. This allows admins to discover and report on all service accounts, regardless if the account is under management or not, and also to report on service accounts running with interactive log on permissions.

Password Safe

- Added functionality that simplifies the onboarding of remote applications as follows:
    - Added the ability to use a Managed System Smart Group for associating the application with domain linked accounts.
    - Added a new Smart Rule action that provides the ability to assign applications to managed accounts. In releases prior to 23.2, this was a manual process for each managed account.
- Added support for SAP HANA database platform.
- Oracle database platform now supports the **Unlock accounts on password change** global setting.
- Added **URL** property to all Secrets Safe secret types to allow the storing of URLs in Secrets Safe.
- New Ansible integration, which enables developers to securely access their managed accounts and DevOps secrets from Password Safe.
- Additional user audit event added to Secrets Safe:
    - **ReadSecret** is generated when the encrypted content is accessed.
    - **Read** event is generated when the base details and metadata is accessed.

Password Safe Cloud

- Added the ability to subscribe to reports in BeyondInsight and Password Safe Cloud, allowing users to schedule reports to run automatically and make the report available for download.
- Added the ability to run reports on specific dates and date ranges, allowing users to report on particular time periods in the past. In releases prior to 23.2, users could report only on relative date ranges, which meant the report contained data from that point in time until present, resulting in a large report containing unnecessary information.
- Added support for custom Password Safe Cloud hostnames in Password Reset emails:
    - If a customer has a custom hostname defined for their Password Safe Cloud deployment, then any URLs contained in the Password Reset emails will use this, as opposed to the “customerkey” DNS name.
    - In releases prior to 23.2, when customers received the reset password email for first login, it contained the randomized hostname and not the custom hostname configured, leading them to believe the custom hostname didn't exist.

API

Updated APIs for Remote Applications:

- GET Applications
- GET Applications/{id}
- GET ManagedAccounts/{accountID}/Applications
- POST ManagedAccounts/{accountID}/Applications/{applicationID}

Updated APIs for Workforce Passwords and Secrets Safe:

- POST Secrets-Safe/Folders/{folderId:guid}/secrets
- POST Secrets-Safe/Folders/{folderId:guid}/secrets/text
- POST Secrets-Safe/Folders/{folderId:guid}/secrets/file
- PUT Secrets-Safe/Secrets/{secretId:guid}/
- GET Secrets-Safe/Secrets
- GET Secrets-Safe/Secrets/{secretId:guid}
- GET Secrets-Safe/Folders/{folderId:guid}/secrets
- GET Secrets-Safe/Secrets/{secretId:guid}/text
- GET Secrets-Safe/Secrets/{secretId:guid}/file

New APIs for Report Subscriptions:

- GET Subscriptions/delivery
- POSTSubscriptions/delivery/download

Issues Resolved:

- Resolved an issue where searching in the **Authentication Type** drop down in the **Create New Credential** form when creating an MS SQL Server discovery credential always returned *No options found* error.
- Resolved an issue where creating a scan using the Scan Wizard and adding a new MS SQL Server credential using the **Create New Credential** link resulted in the UI displaying the following error: *An error occurred creating the scan...*.
- Resolved an issue where attempting to add a new credential to a scheduled scan resulted in an error stating that a credential needs to be selected and the credential is not added.
- Resolved an issue where using and then clearing a custom credential in the Scan Wizard caused errors and job creation failure.
- Resolved an issue in the Scan Wizard, where **Select All** on the credentials list did not respect the boundaries of the search criteria, and thus prompted validation for all keys, not just the ones matching the search.
- Resolved an issue in the Scan Wizard, where validation keys were sometimes requested even if no credentials were selected.
- Resolved an issue where, after saving a change to the target Smart Rule when editing a scheduled scan, an unsaved changes warning popped up when attempting to navigate away from the **Targets** tab.
- Resolved an issue where changing the scan from **Recurring** to **Immediate** on the **Schedule** tab for a scheduled scan resulted in an error stating *Nullable object must have a value*, and the changes were not saved. The **Immediate** option was removed for scheduled scans as it is not valid for this type of scan.
- Resolved an issue where the max user limit on detailed discovery scans was not communicated to the scanner.

- Resolved an issue where SSH keys were not being captured when scanning an asset. When viewing the **Advanced Details** of the asset from the **Assets** page, and clicking the information icon for the user in the **Users** grid, the **SSH Key Count** field might have been zero, even if SSH keys existed for that user.
- Resolved an issue where, after upgrading to the 23.1 release, any existing access policy which had location restrictions enabled with **X-Forwarding** set to **All** showed the **X-Forwarded for** field as blank and disabled.
- Resolved an issue with session replay in Firefox where viewing an active session, terminating it, and then trying to replay the session from **Completed Sessions** resulted in an error stating *An error occurred while trying to fetch the session keystrokes*.
- Resolved an issue where editing an existing functional account with an assigned DSS key incorrectly required the DSS key to be re-uploaded when saving any change to the functional account, even though an *already been uploaded* message was displayed.
- Resolved an issue where, in some cases, when upgrading the Web Policy Editor to 23.4, the JRE folder became corrupted, causing the Web Policy Editor to not load and *Error 500* showing in dev tools.
- Resolved an issue where an incorrect session node hostname/address was being used for RDP sessions after upgrading to the 23.1 release.
- Corrected field labels on the settings for managed accounts and managed systems to read as **Default Release Duration** from **Release Duration** to match the label as shown for **Manage Account Settings** action in a Smart Rule.
- Resolved an issue where it was possible to edit an access policy that was created in the past and change its recurrence to **One Time**. This is not a valid scenario.
- Resolved an issue where **Quick Launch** was not available when the access policy end date was the current day and multi-day checkout was enabled.
- Resolved an issue where if the **Auto-select access policy for Quick Launch** setting is enabled and there are two or more access policies available, the shortest policy is not auto-selected.
- Resolved an issue where the **Playback Speed** dropdown does not open when viewing a completed session in full screen mode.
- Resolved an issue where password rotation of a Salesforce platform managed account was failing.
- Resolved an issue where password rotation of a Workday platform managed account was failing.
- Resolved an issue where after creating a new Managed System Quick Group, it would not appear in the Smart Group filter until the page was reloaded.
- Resolved a text wrapping issue where a very long approve or deny comment would not be fully visible in the request details form.
- Resolved an issue where if a user attempted to use **Quick Launch** to access an account where they already had an approved request, they would receive an *Account is already available* error message, instead of reusing the existing request.
- Resolved an issue where if the maximum concurrent request limit is reached, the conflicting request details were not displayed.
- Resolved an issue where replaying an RDP session, in the 23.1 release, could display *An unexpected error has occurred* message and fail to replay the session, if the session was using a large screen resolution or multiple monitors. Prior to the 23.1 release, when this error occurred, the session replay would freeze for a moment, and then continue without crashing. The 23.2 release allows for larger data packets during replay.
- Resolved an issue where the **Allow use for Secrets Safe** option was not enabled by default when creating a new password policy.
- Resolved an issue where when specifying the password for a functional account, if the password contained certain special characters (ex: €), an incorrect validation error was shown.
- Increased the allowed field length for the functional account password to **256** characters from **128** to accommodate the increase in the Jira Cloud ticketing system API key length.
- The minimum password request time has been lowered to **1** minute from **5** minutes, to be consistent between the user interface and the API.
- Resolved an issue where Smart Rules with Dedicated Account mapping actions were not properly triggered when a user logged on for the first time.
- When accessing the Secrets Safe user interface, the default selected folder had been changed from **All Secrets** to the first team shared folder found under **All Secrets**. If the user is enabled for Workforce Passwords, this will be their **Personal Folder**.

- Resolved an issue where certain actions in a Smart Rule could only be added once. Now, multiple instances of the affected actions can be added in a single Smart Rule.
- Resolved validation inconsistencies with scan credential creation using Public Key Authentication Type.
- Improved auditing of manual asset creation and editing actions to show more details about what was created and changed.
- Improved display of details for **Selection Criteria** in Smart Rule Details area.
- Improved Reporting Gateway service resilience when multiple Endpoint Privilege Management Reporting jar files are present, ensuring the proper jar file is chosen and the proper settings are sent.
- Resolved an issue where the RetinaCSAppPool went into a stopped state on the passive node in an HA setup, ensuring that it is restarted if it enters a stopped state.
- Resolved an issue where the **Next Scan Start** date/time for a scheduled scan that is in a remote time zone does not display the correct value in the **Scheduled Scans** grid.
- Resolved an issue where duplicate **Attributes** could not be added across distinct **Attribute Types**.
- Resolved an issue where scheduled sync jobs for AD user groups performed by the system were visible in **User Audits**. Now only manual sync jobs appear in **User Audits**.
- Resolved a filtering issue on the **Directory Credentials** grid **Title** field, where filtering by the underscore character was returning all credentials. It will now return the expected results.
- Resolved an issue where the **Endpoint Endpoint Privilege Management Events** grid could not be viewed by users with **Read Only** permissions to the Endpoint Endpoint Privilege Management feature.
- Resolved an issue where Endpoint Endpoint Privilege Management Event Collector, Reporting Gateway, and Web Policy Editor service logs were recording too many informational messages as warnings.
- Resolved an issue where the **Discard Changes** message was not shown after canceling the **Create Policy** process in Web Policy Editor.
- Resolved an issue with Endpoint Endpoint Privilege Management event processing where failures occurred if an asset had more than one associated Operating System record.
- Resolved an issue where a broken *500 Error* page was appearing after a failed Azure AD or OKTA SAML login.
- Resolved an issue where SAML redirect was not using the incoming host address as it should.
- Resolved an issue where user receiveed an *HTTP 500 error* when attempting to access SAML pages, after upgrading to the 23.1 release.
- Resolved an issue where the logged in user might not display in the **Profile and Preferences** dialog in the BeyondInsight console, when logged in using SAML.
- Resolved an issue with RADIUS authentication failing with an error when using naming attribute **Alternate Directory Attribute** and LDAP domain with non-standard Base DN.
- Resolved an issue with RADIUS configuration not loading when a filter that requires text input was set for that alias.
- Resolved an issue with TOTP descriptions not showing correctly in some authenticator apps.
- Resolved an issue where users with the **Auditor** role did not have access to **Entitlement by User** Password Safe report.
- Resolved an issue with duplicate entries on the **Service Account Usage** report.
- Resolved an issue where the **Password Update Activity** reports might exclude content about functional accounts with no workgroup.
- Resolved an issue where scheduled scans created by a user having a NULL first name could not be deleted.
- Resolved an issue with the **PUT Addresses/{id}** API call creating a new address rather than updating the existing one.
- Resolved an issue with *No Updates* logging excessive rows to the database during Smart Rule processing that onboards managed systems when Endpoint Endpoint Privilege Management is used as the change agent.
- Resolved an issue with X-XSS-Protection header setting for the HTTP response not being set correctly.
- Resolved an issue where Firefox users were always seeing the **Skip to Main Content** keyboard navigation aid on the screen.

- Resolved a number of minor user interface layout issues.
- Resolved a number of keyboard navigation and screen reader functionality bugs.
- Resolved a localization bug where certain labels were not being translated upon language preference change by user.
- Resolved an issue where the auto generation of a password in Secrets Safe could fail, if there were more than 10 password policies.
- Resolved an issue where selecting a domain for a Resource Zone would not work if the domain has already been added to the system via a directory query.
- Resolved an issue where the hostname or host override values were not being displayed in the **Session Node** selector when viewing the advanced details of a request.
- Resolved an issue where attempting an Admin Session when FIPS is enabled on the appliance fails.
- Resolved an issue where viewing a session replay using Firefox had excessive flickering.
- Deactivated access policies no longer appear as an option when creating a request an access request in the Password Safe web portal.
- The wrong Resource Broker is no longer automatically selected on the **Direct Connect Access** form in Password Safe Cloud.

Known Issues:

- After upgrading BeyondInsight, it is not possible to change the date or time on a Scheduled Scan that has a **Schedule Type** set to **One Time**. After changing the **Start Time** or **Start Date** and clicking **Save Schedule**, the following error occurs: *Cannot update a scan schedule from recurring to one time or immediate*.
    - **Workaround:** Delete and recreate the Scheduled Scan to enter the appropriate date and time details. A fix is planned in an upcoming release.
- Running the **Endpoint Endpoint Privilege Management - Event Rollup** report with the **Include Excluded** parameter checked might result in the following error and the report might not complete: *The report cannot execute due to an invalid parameter.*
    - **Workaround:** Avoid checking the **Include Excluded** parameter on this report. A fix is planned in an upcoming release.
- Attempting to subscribe to the Discovery Report accessed from the **Active/Completed Scans** grid results in an empty **Create a New Subscription** dialog and a *500 error* is seen in dev tools.
    - **Workaround:** You can subscribe to the report from the **Analytics & Reporting** area of BeyondInsight. Subscribing to the report from the **Active/Completed Scans** grid is not a valid starting point to set up a subscription. This action will be removed from this location in an upcoming release.
- When using the Workforce Passwords browser extension, if a user has thousands of credentials stored for the same website, there can be a delay before the auto-fill indicator appears on the **Log In** page.
- **Maintenance Expiry Warning** banner might fail to appear in the 30 days before the expiry of the maintenance agreement. Once the agreement expires, the alert banner appears.
- Using the API, it is possible to rename a Secrets Safe folder to be a duplicate of an already existing folder under the same parent. This is not permitted in the user interface. A fix is planned in an upcoming release.
- When using the API to create a Secrets Safe folder with the same name as an existing folder, it fails with a *400 - DuplicateFolderName* error instead of a *409 - Folder already exists* error.
- Using the Workforce Passwords browser extension along with the BeyondInsight web console at the same time with two different user accounts might result in the extension user details being applied to the web console session when signing out of the browser extension.
    - **Workaround:** Log out of the BeyondInsight web console, as well as the browser extension, and either use the same account for both, or don't use them at the same time.

- In **Analytics & Reporting**, the **Event List** and **Events By Hour** reports from the **Endpoint Privilege Management UNIX Linux** folder might give an error in the SSRS log when running. The error might indicate a problem with the [PowerBroker UL Accept Reject Time] dimension.
    - **Workaround:** Use the **Pivot Grid** to navigate the data, or choose a different report to review the data.
- If you attempt to edit a new functional account immediately after creating it, an erroneous *There are one or more invalid fields* validation error displays.
    - **Workaround:** Click **Discard Changes** and edit the functional account again.
- If a MacOS managed account is locked out when a password rotation is attempted, the rotation fails but is reported as successful.
- If a FireEye connector was created in a prior release of BeyondInsight, and remains after upgrading, it is no longer valid and cannot be used or updated. The following error displays: *Object reference not set to an instance of an object*.
    - **Workaround:** Delete the connector.
- If an audit of type **PMR Database Settings** exists, and a call is made to the **PAPI GetUserAudits** for all audits and all details, an error might result.
    - **Workaround:** None at this time, other than to alter the criteria passed to the API to avoid that audit type.
- If you attempt to manually create a MongoDB managed system with a different instance name and same DNS name and port as one which already exists, the creation fails with a uniqueness validation error.
    - **Workaround:** Use a discovery scan and Smart Rule to onboard the database managed system.
- Downloading the client certificate from the **Configuration > System > Downloads** area might fail with an error in some on-premises installations. Error message *Keyset does not exist\r\n* is seen in dev tools.
    - **Workaround:** Use the BeyondInsight Configuration utility to generate the certificate.

> ***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 23.2 are supported from BeyondInsight version 21.3 or later releases.
- This release is available to download for BeyondTrust customers from https://beyondtrustcorp.service-now.com/csm using BeyondTrust BT Updater.
- The MD5 signature is: c12466f856d5b4d0837d7c9a17062f18
- The SHA-1 signature is: 602dc72c59725bee64bec589fbbae5527b4bb4fd
- The SHA-256 signature is: 49164507e470d8bcab5bc621f641914ffe8698398c1fb55b0b7695f352062b88