BeyondInsight and Password Safe 22.4.0 Release Notes

December 15, 2022

New Features and Enhancements:

General

- Updated multiple areas of the UI to abide by newer UX recommendations and improve accessibility.
    - **Discovery Scans** and most related areas
    - **Assets** and most related areas
    - **Configuration** areas including **Directory Credentials**, **Directory Queries**, **Smart Rules**, **Workgroups**, **User Management**, **Organizations**, **User Audits**, and **Smart Card**
- Replaced the **Scheduled Tasks** list in **Asset Details** with a grid.
- Added support to create a directory query with new directory credential from the Smart Rule editor.
- Added support for local account discovery data from supported Windows Endpoint Privilege Management agents (version 22.9 or later).
- Added an **IP Discovery** scan type, restoring the ability to complete an uncredentialed scan to do the most basic asset discovery.
- Added SAML link to login page for default IDP when environment has SAML configured.
- Streamlined the display of features/permissions to align with which features are licensed in the environment.
- Added a **BaseDN** field to the user group to allow further support for non-standard LDAP configurations.
- Added a read-only view for Smart Rules.
- Changed AWS Instance type selection in Smart Rule editor from a dropdown list to a selection grid, and added a backend cache to refresh the available options as instance types are added by the vendor.
- Removed obsolete CVSS Metric Smart Rule action.
- Updated the compatibility mode of the BeyondInsight and BeyondInsight Reporting databases to match the SQL Server version upon create or upgrade of the database.
- Added **Session Timeout** configuration setting.

Analytics and Reporting

- Updated multiple areas of the UI to abide by newer UX recommendations and improve accessibility.
    - **Clarity**
    - **Report Viewer**
- Added a new report under the **Configuration** folder, **BeyondInsight Entitlement by Group**, which provides a real-time view of group membership and permissions.
- Added a new report folder, **Secrets Safe**.
- Added a new report, **Secrets Safe Entitlement Report**, which provides a list of user groups and the secrets they are entitled to.

Endpoint Privilege Management

- Updated multiple areas of the UI to abide by newer UX recommendations and improve accessibility.
    - **Policy Exclusions**

Password Safe

- Updated multiple areas of the UI to abide by newer UX recommendations and improve accessibility.
    - **Managed Accounts** and most related areas
    - **Managed Systems** and most related areas
    - Configuration areas including **Mail Agents**, **Mail Templates**, **Aliases**, **DSS Key Policies**, **Oracle Internet Directories**, **Session Agents**
- Team Passwords (now Secrets Safe) has been updated with Secrets support.
    - Renamed to Secrets Safe to include broader data types.
    - Added support for file secrets.
    - Added support for generic text secrets.
    - Secrets are now protected from accidental deletion if the secret owner or group has a deletion attempt.
    - Moved Team Password APIs to Secrets Safe URL path. Team Password paths remain but are now considered deprecated.
- Added ability to link Directory-type managed accounts to cloud-type managed systems.
- Propagation scripts have additional parameter options for managed asset and script host name and IP addresses.
- Added support for local account discovery via the Endpoint Privilege Management agent (requires Endpoint Privilege Management 22.9+).

API

- Secrets support has been added to Team Passwords.
    - Existing Team Passwords APIs have been deprecated and replaced with new Secrets Safe APIs:
        - **POST Secrets-Safe/Folders/**
        - **GET Secrets-Safe/Folders/**
        - **PUT Secrets-Safe/Folders/{id}**
        - **DELETE Secrets-Safe/Folders/{id}**
        - **GET Secrets-Safe/Folders/{id}**
        - **POST Secrets-Safe/Folders/{folderId}/secrets/**
        - **POST Secrets-Safe/Folders/{folderId}/secrets/text**
        - **POST Secrets-Safe/Folders/{folderId}/secrets/file**
        - **PUT Secrets-Safe/Secrets/{secretId}**
        - **PUT Secrets-Safe/Secrets/{secretId}/text**
        - **PUT Secrets-Safe/Secrets/{secretId}/file**
        - **GET Secrets-Safe/Secrets/{secretId}**

- **GET Secrets-Safe/Folders/{folderId}/secrets**
- **GET Secrets-Safe/Secrets/{secretId}/text**
- **GET Secrets-Safe/Secrets/{secretId}/file**
- **GET Secrets-Safe/Secrets/{secretId}/file/download**
- **DELETE Secrets-Safe/Secrets/{secretId}**

Issues Resolved:

- Resolved an unsaved changed prompt issue when navigating away from a managed account scan credential that was viewed, but not changed.
- Resolved issue in which, in some sections of the configuration area, the first time you selected a different option from a dropdown, the update button might not have enabled.
- Resolved issue in which the **Load** button did not load the aliases while creating or editing an Oracle database managed system.
- Resolved issue in which only the IP address of the system was used even if DNS was specified when rotating an SAP account credential.
- Resolved issue in which the first attempt to **Test Connector** in the **Connectors** screen might have reported *one or more fields are invalid*.
- Resolved issue in which, in some intances, in the SAML configuration area, after editing the Identifier field, the form might not have saved.
- Resolved issue in which, under certain circumstances, performing an account test on an HP-UX system might have failed with a timeout.
- Resolved issue with Amazon and Salesforce Functional accounts, in which secret keys were not applied properly from the **Functional Account Configuration** screen.

Known Issues:

- Manual creation of a new asset might give incorrect validation message on IP address. Workaround: ignore the warning in the UI; if the IP address is valid, the asset can be created.
- Manual creation of a new asset while a grid item is selected populates the new asset fields with the selected asset details. Workaround: ensure that no asset grid items are selected when clicking the **Create** button.
- When moving an asset from one workgroup to another, on the third and any subsequent move, the assets might be duplicated in multiple Workgroups. Workaround: delete, or ignore the duplicated asset. This issue has been around since at least 22.2 but was only marked as a known issue in 22.4.
- **Asset Advanced Details > General Data > Details & Attributes (current data)** displays *UNKNOWN* rather than dashes (--) for empty fields. Workaround: none, this is informational. The *UNKNOWN* text is displayed in place of -- in this spot; it is not data from a scanner or anything else. It can safely be disregarded; we will resolved this in an upcoming release.
- **Asset Advanced Details > Scheduled Tasks > scheduled task details** might be truncated in some instances. Workaround: none, this has existed since 22.2 but we only just recently verified the root cause of the issue. The Microsoft command that is called by the scanner to retrieve the details is truncating the data.
- **Asset Advanced Details > Users Tab > User Type filter** does not work for domain user or administrator. Workaround: it does work for local user. Oother than that, this will be resolved in an upcoming release.
- After saving an edit to a user from the **User Details** edit panel, all user fields in the edit panel are cleared. Workaround: none, this is informational. The issue will be resolved in an upcoming release.

- Unable to delete a directory credential when the name is longer than 80 characters. Workaround: if the confirmation buttons on the delete modal warning can't be accessed due to a long credential name, first edit the credential name (ideally to 50 characters or less) and then attempt to delete again.
- There is an inconsistency when showing some time details of a Smart Rule in read-only viewer. Workaround: none, this is expected behaviour. The read-only viewer does not know that fields made up of single numbers (hours, minutes) are meant to translate to dates/times, and so they are displayed as single numbers.
- A user with read-only permission to Endpoint Privilege Management can't access the **Events** page from the main menu. Workaround: The **Events** page can be accessed by a read-only user via the tile on the dashboard. The menu permissions will be resolved in an upcoming release.
- Some measures in the pivot grid do not accurately represent the value stored in the cube. Workaround: in most cases, the data is correct, but for some reason, we've found a few discrepancies. It is not consistent which measures are affected but it seems to happen more with larger values than with smaller ones. This issue may also occur in previous releases. Customers are advised to create a custom report from their pivot grid and run that to ensure they are seeing up-to-date values. Our development team continues to investigate the root cause and will advise if any further clarification can be given.
- Canceling the creation of a new propagation action results in two *Discard Changes?* confirmation prompts. Workaround: choose **Cancel** on both confirmation prompts.
- Attempting to delete an Active Directory managed system that contains one or more AD managed accounts that have at least one propagation action assigned results in an error. Workaround: delete the propagation actions from the account(s) or delete the managed account(s) prior to deleting the managed system.
- When filtering by **Type** in the **Configuration > Propagation Actions** grid, if multiple types are selected in the filter then the results show only items matching the first filter in the list. Workaround: filter by a single entry at a time.
- Occasionally when creating a new session mask, the creation fails with a *One or more fields are invalid* error message. Workaround: press the **Create** button again.
- When using a Jira Connector for ticket system validation, the **Functional Account** domain field is used rather than the **Instance URL** as configured in the connector. Workaround: ensure the **Functional Account** domain field is set to the correct value.
- If a file share-based subscription has a longer share name (over 45 characters), the action menu in the subscriptions list is not visible. Email delivery-based subscriptions are not affected. Workaround: Use keyboard controls to select the subscription (up/down arrows), and then use the space bar to open the menu for the item where the menu is not visible. Alternately, an administrator can manage the subscription from the **Analytics & Reporting** configuration page, on the **Subscriptions** grid.
- After upgrading from 22.3 to 22.4, if the **Global Credential Key** switch is 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 credentials.
- If you are saving an edit to an SSH credential, you may see an error indicating there are invalid fields. Workaround: Expand the **Change Private Key** section and upload the file again to edit the credential.

Notes:

- Direct upgrades to 22.4.0 are supported from BeyondInsight versions 21.1 or later.
- 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: b8f6cfa0f351803cfca89851c3ffb0b7
- The SHA-1 signature is: 2631f805c0e59621d34872d54f997c9a57127354
- The SHA-256 signature is: a97399ccb406d5180c11126b9a367b35e43c12e01e73bab3f06844ba4383b575