BeyondInsight and Password Safe 24.1.0 Release Notes

April 11, 2024

New Features and Enhancements:

General

- New **Configuration > Authentication Management > Installer Activation Keys** page for configuring Endpoint Privilege Management agents to use OAuth authentication.
    - Agents that support OAuth communication is expected in upcoming releases of Endpoint Privilege Management for Windows and Endpoint Privilege Management for Mac.
    - Refer to the Release Notes for those products, once they are released, to confirm which versions support OAuth communication.
- Improved user experience around toast messages, including time-based auto-dismiss of all notification types, pause and resume actions to control the auto-dismiss in real time, and a notification center to view previous warning and error notifications that were not dismissed.
- Added the ability to reactivate scheduled scans that were deactivated.
- Increased the upper limit of the scanner minutes to run input in the **Scan Restrictions** section of the Scan Wizard from 60 to 2880 (equivalent to 48 hours).
- Added the **Scan Restrictions** inputs to the **Edit Scheduled Scans** area, so that scan restrictions can be edited for a scheduled scan.
- Added support for the Workforce Passwords Browser Extension to detect the web browser's language, and use it if it's one that is supported.
- Added support for Workforce Passwords Browser Extension to give the user the choice to leverage their current session if they currently are logged into BeyondInsight in another browser tab.
    - This also resolves previously mentioned known issues with SAML, Windows SSO, and Smart Card login methods for the Workforce Passwords Browser Extension.
- Added **View Results** row action to Smart Rules grid for processed Smart Rules.
- Added warnings to Directory Queries Create and Edit interfaces to remind users that making changes to Directory Queries can have significant impacts if those queries are used by on-boarding Smart Rules. The warning also alerts the user when they have made edits but not tested them before saving.
- Updated the social media icons on the BeyondInsight **Log in** and **About** pages.
- Modified the BeyondInsight and Password Safe installer to prevent attempted installation on Windows Server 2012 or older versions.
- Renamed the **Domain/Domain Controller** field to **Base DN** on the LDAP User and Group Add and Edit forms.
- Added support to allow the manual entry of a **Base DN** in the dropdown if the **Fetch** does not return the one that is required.
- Updated Azure Active Directory references to Microsoft Entra ID across BeyondInsight and Password Safe user interface.
- Updated from Angular 15 to Angular 17.
- Removed references to deprecated **Mac Address** field from BeyondInsight and Analytics & Reporting.
- Removed references to deprecated **Asset Risk** field from BeyondInsight and Analytics & Reporting.

Analytics & Reporting

- Added new **Active Users** report to show BeyondInsight and Password Safe web console user logins. This report can also show users who have never logged in.
- Added new **SSH Keys** report to show discovered and authorized SSH Keys found on assets during the latest scan.
- Removed deprecated **Endpoint Privilege Management Registry Monitoring** report.

Password Safe

- Added **Disable at Rest** functionality for Microsoft Active Directory and Entra ID managed accounts, providing new **Just-in-Time** capabilities.
- Added ability to import credentials from a .csv file for Secrets Safe and Workforce Passwords.
- Added email notifications for failed Propagation Action events.
- Propagation Action events are now included in Event Forwarder connectors.
- Added **Account Status** availability details for Privileged Remote Access (PRA) and Endpoint Credential Manager integrations, so PRA users can identify if accounts are not available.
- Improved support for Cloud managed systems with Privileged Remote Access and Endpoint Credential Manager integrations.
- Updated Password Safe product image in the left sidebar menu and dashboard tile.
- Added ability to filter by **Archive** status on the **Completed Sessions** grid.
- Updated the Twitter/X platform image in the BeyondInsight UI.
- Added **Secret ID** value to various screens in Secrets Safe.
- Added kiosk-mode support to PS_Automate. Additionally, several keyboard shortcuts (i.e: open new window, open browser task manager) are now blocked.
- Implemented a block to prevent the use of the WinSCP client when it is configured in SCP mode. WinSCP in SCP mode causes performance issues when used in conjunction with Password Safe sessions. Use WinSCP in SFTP mode or an alternative SCP client.
- Updated the **Parameters** UI control in the **Applications** configuration screen, to improve the readability when there are multiple parameters.
- Updated verbiage in Password Safe from ‘Domain’ to ‘Directory’ for consistency with other product areas.
- Updated grid column filters in Password Safe to be multi selectable dropdowns for **Directory**, **Platform**, **Node** and **Resolution** columns.
- Added browser spell check capability for various fields (ex: Managed Account and System Description, etc).
- Added ability to approve and deny requests directly from the **Approvals** grid.
- Added ability to check in a request directly from the **Requests** grid.
- Added color icons to values in the **Account Status** column in Password Safe to improve visibility.

Password Safe Cloud

- Added **IP Allow List** configuration, providing the ability to restrict which IPs and ranges are permitted to connect to a Password Safe Cloud instance.

Issues Resolved:

Analytics & Reporting

- Resolved an issue in Endpoint Privilege Management reports where toggling the **Include Excluded** parameter caused the **Event Title** parameter dropdown to clear.
    - The **Event Title** parameter is no longer affected by changes to the **Include Excluded** parameter, allowing the reports to run more easily.
- Resolved an issue in a number of reports where the system did not consistently enforce required parameters to populate before allowing the user to run the report.
    - Now the restrictions are properly enforced, protecting users from inadvertently running reports with incomplete parameter selection.
- Resolved an issue where the **Subscription** list was not refreshed after editing an existing subscription.
    - The **Subscription** list now reflects the new information immediately after editing is complete.
- Removed the **Download Reports** option from the **Subscription** list for on-premises configurations.
    - Now that action, which is not supported on-premises, can't be attempted.
- Resolved a previous known issue in which the **Reviewed Sessions** report may not correctly identify the **Reviewed By** and **Reviewed Date** for reviewed sessions.
    - Now the **Reviewed** parameter, when set to **Yes**, consistently returns the **Reviewed** rows as expected.
- Updated the **Password Safe > Entitlement by Group** report to improve report performance by reducing overall processing time.
- Aligned the permissions required to own and edit subscriptions between cloud and on-premises configurations of Analytics & Reporting.

Configuration

- Resolved a cloud specific session timeout issue where configured session timeout values of more than 20 minutes were not being respected.
    - Administrators can now configure up to a 60 minute timeout, which will be respected by the product web interface in both cloud and on-premise configurations.
- Resolved an issue where some edits to Smart Rule criteria may give an error indicating that "*One of the Smart Rule parameters is invalid. Please review and try again*."
    - The condition that caused this error is no longer possible, so an administrator will not encounter this error when creating or editing Smart Rules. This may speed up the task of creating or editing Smart Rules.
- Resolved an issue where the character limit warning on the **Role Based Access > Password Policy > Default Password Policy** text input fields was not removed after the text input was updated using the **Reset to Defaults** action.
    - The character limit warning is now cleared when the **Reset to Defaults** action is taken in this area.
- Resolved an issue in **User Management** with password validation.
    - Now, if trying to set a password that contains a mix of special characters that are allowed or not allowed, the validation accurately guides the user to remove the characters that are not allowed.
- Resolved a previous known issue which caused the **Name** column in the **Groups** grid of the **User Management** configuration screen to be repeated.

  - Now the **Name** column only appears once as would be expected.
- Resolved an issue where a user may not be able to update their password if the password policy is edited to decrease the max length of a password to a shorter value than the length of the user's current password.
  - Now, a user can update their password even if their current password length exceeds the upper limit on the policy.
- Resolved an issue in the **System Event Viewer** and **User Audits** grids where the row focus and checkmark do not update when viewing details in the right panel by clicking the **Info** button in the row.
  - Viewing the details in the right panel without selecting a new row first, now clears the focus from the previously selected row and places an indicator around the button to show that it's the one being viewed in the right panel.
- Resolved an issue in the **Add New Group** form with new inline credential creation, where now the **Credential** dropdown updates immediately with the newly created credential.
  - The user no longer needs to close and re-open the panel to use the new credential during group creation.
- Updated the **Scan Agents** selection grid in the **Set Scanner Properties** area of the Smart Rules Create and Edit pages.
  - Now, deleted agents are not available for selection, and the **Apply Changes** option remains visible even if there are a large number of agents in the grid.
- Resolved an issue in LDAP search in user and group management, where a **Fetch** action after an invalid entry to the **Base DN** field was failing to show an error to the user.
  - An error is now shown if the input is invalid, so the user is alerted to any possible data input errors.
- Resolved a display issue in **Configuration > Address Groups** where imported IPs do not appear in the user interface until the page is refreshed.
  - The imported IPs now appear immediately.
- Resolved an issue that was preventing the removal of the built in Administrator user from custom user groups.
  - The built-in Administrator account can now be removed from custom user groups.
- Resolved some time zone and start time issues with the **Support > Advanced Purge Options**.
  - The job now runs at the time shown in the UI.
- Resolved sensitive information leak on the **Discovery Credential** configuration screen.

Endpoint Privilege Management

- Resolved a previous known issue which affected the editing of extremely large policies in the Endpoint Privilege Management Policy Editor.
  - Using Endpoint Privilege Management Policy Editor version 23.1.0 or later, policies larger than 20 MB can be created, edited, and saved.
- Updated the BeyondInsight user interface to ensure that links to Endpoint Privilege Management Policy Editor remain in English even if the user has selected another language.
  - This is an indicator that the Endpoint Privilege Management Policy Editor itself is not localized to languages other than English.
- Resolved an issue causing excessive logging in the Privilege Management Reporting Event Collector Service.
  - Now, after restarting, the service log level is set to **Warning**, which reduces the noise in the log file and makes troubleshooting easier.

- Updated the logic that shows and hides the **Privilege Management Reporting** card in the **Configuration** area.
    - Now, the **Configuration** card appears when Privilege Management Reporting UI is installed, rather than relying on Privilege Management Reporting database is installed. This allows for easier configuration in environments where the database is remote.

Password Safe

- Resolved an issue where null date values were displaying incorrectly in the **Managed Account Details** view.
    - Now, if the dates for **Last Changed** or **Next Change** are null, the field displays **--** instead of an invalid date.
- Resolved handling of ssh_proxy\prompts configuration for SSH sessions.
- To prevent false negative password changes, all built-in custom platforms with single-word regex expressions have been updated to look for exact matches.
- Clarified the force termination help text for access policies so that is more about its intended usage.
    - Now, the help text displays "*Forcibly closes the RDP session when the requested time expires*".
- Resolved an issue in Password Safe where an application was showing as associated with all linked systems when it was set to **Run on a Different System** and **No Association** was selected.
    - Now the application only appears for the managed system that the domain managed account is linked to.
- Resolved an issue in the Password Safe public API where **GET UserGroups/{userGroupId}/Users** times out when **auditdetails** page has many rows in the database.
- Resolved an issue in Password Safe where a favorite record for a domain account linked to a managed system remains after the link has been removed.
    - Now when the two are unlinked the favorite no longer displays.
- Resolved an issue that occurred when a Dedicated Account Smart Rule was removed. Previously a reset was required to remove this data from the database.
    - The data is now automatically removed when the Smart Rule is removed.
- Resolved an issue where when a functional account is a directory account, the **Test Agent** was performing the test against all managed systems that the functional account was associated with.
    - Now, **Test Agent** only performs the test against the directory managed system.
- Resolved an issue in the Password Safe Public API where specifying an empty string for the **ApplicationRegistrationIDs** parameter to the **POST UserGroups API** returns *HTTP error code 500 'Internal Server Error'*.
    - This now returns a *201 - Success*.
- Improved error messaging in access policies when attempting to create a schedule with a timeframe set to less than 30 minutes.
    - The error message no longer states "*Schedule duration must be more than 30 min*".
- Resolved an issue where the default Privileged Access Management policy does not contain a section for the **First Character Value**.
    - This section is now added with any character permitted as the first character.
- Resolved an issue where it was not possible to change the **First Character Value** setting from the default value of **Any Character Permitted** when creating or editing a Password Safe password policy.
    - It is now possible to successfully modify this setting.

- Resolved an issue where users without any access to Password Safe were able to successfully log in.
    - Previously, users would log in to the console and be unable to see any data. Now they are prevented from logging in successfully.
- Resolved an issue where when attempting to modify **Selection Criteria** parameters in Smart Rules using an invalid parameter, a non meaningful error message was displaying.
    - Now, when attempting to save a Smart Rule where an invalid parameter has been selected the following message displays: "*One of the Smart Rule parameters is invalid*".
- Optimized database queries that were taking too long to complete to improve their performance.

Secrets Safe

- Log entries are now included in the **System Event Viewer**.
- Resolved an issue in the Secrets Safe public API where secrets created before the time specified were being incorrectly returned when using the **AfterDate** parameter.
    - Now these secrets are not returned.
- Resolved an issue where the Secrets Safe feature permission could not be successfully managed by groups that had the minimum required permissions of **User Account Management**.
    - Now these groups are able to successfully add and remove the Secrets.
- Resolved an issue where user's personal folders were being orphaned in the database if the user was deleted.
    - Now when a user is deleted from BeyondInsight their personal folder is removed as well.
- Resolved an issue in Secrets Safe where line returns were being dropped when being copy and pasted into the **Notes** field.
- Resolved an issue in the Secrets Safe Public API where creating a secret via **POST Secrets-Safe/Folders/{folderId:guid}/secrets** returns a response with an empty string for the **FolderPath** property.
    - This now returns the correct **FolderPath** property.
- Resolved an issue where the owner of personal folder secrets can be changed.
- Resolved an issue in Secrets Safe where the group folder name was not automatically updated when the Active Directory group name changes.
    - The folder name now updates when a group sync is triggered in BeyondInsight.
- Resolved an issue in Secrets Safe where read audit logs for a secret were being generated incorrectly when access was denied due to insufficient permissions.
- Improved error messaging in Secrets Safe when attempting to create a duplicate folder.
    - The error now explicitly states that the folder name already exists.
- Removed extraneous **ID** and **credentialID** entries from the Secrets Safe user audit details.

Other

- Improved **RoleType** validation for user and group creation via API.
- Improved filtering in **Asset Advanced Details > Services** grid.
    - Now, the **Status** column can be filtered by additional options that may appear.

- Resolved an issue that was preventing accurate sorting of the **Last Login** column of the **Asset Advanced Details > Users** grid.
    - Now, that column can be sorted.
- Resolved an issue affecting the removal of tiles when customizing Dynamic Dashboards.
    - Now, tiles added to custom dashboards can be removed.
- Resolved an issue with inconsistent tile sizes in the Dynamic Dashboard.
    - Now, tiles appear the same size even when there are only a few of them.
- Improved performance in the Plugin Event Server in cases where a large number of events are present.
- Resolved an issue in Public API **GET UserAudits** method where it was incorrectly returning data when the date range was set to future dates.
    - Now, only the expected results are returned.
- Updated API query string length validation.
- Removed unused **Angular.js** file and project references.
- Resolved an issue where upgrading BeyondInsight caused the startup type of **Disabled Omniworker** and **Manager Engine** services to change to **Automatic (Delayed)**.
    - Now, upgrading BeyondInsight respects role settings for these services as expected.
- Resolved a number of minor UI issues around form field validation, file uploads, appropriately display of discard modals, long content tool tips, translated text layout, and standardized use of recurrence UI control.

Workforce Passwords

- Resolved a permission issue with running the browser extension in Firefox, where the user had to configure extra steps before they could use the extension.
    - Now the Firefox extension works without any extra configuration steps required by the user.
- Resolved an issue where using the browser extension along with the BeyondInsight web console at the same time with two different user accounts resulted in the extension user details applying to the web console session when signing out of the browser extension.
    - Now, the logged in users remain separate.

Known Issues:

- In the **Configuration > Propagation Actions** grid, applying a filter to the **Last Change Date** column has no effect, and all rows are returned.
    - This is being resolved in a future release.
- When using the Web Policy Editor, on the first attempted edit of a user's session, occasionally (more often in Incognito mode), an additional button save action may appear on the policy editing page. When this occurs, the **Save** and **Save & Unlock** buttons do not work as expected and can cause the editor to hang.
    - **Workaround**: Avoid incognito mode. If a **Save** button appears, discard changes and attempt the create or edit again. The issue should not occur a second time during the user's session.
- On the **Sessions** grid in the Password Safe, the column picker contains a duplicate **Status** column entry, which can be ignored.
    - This is being resolved in a future release.

- When editing the ownership of a secret, navigating away from the page does not prompt with an unsaved changes warning. Ensure you have saved the ownership changes prior to navigating away. This is being addressed in a future release.
- When configuring an **IP Allow List** rule with an IP Range, there is no validation which prevents a user from entering a **From IP Address** value which is higher than the **To IP Address** value. Attempting to save a rule with this misconfiguration displays a generic error message.
    - **Workaround**: Ensure that when configuring IP Range rules that the **From IP Address** value is lower than the **To IP Address**.
- If a Workforce Passwords Browser Extension is in use while the Password Safe instance is upgraded, its extension cache may need to be manually refreshed so that new features appear. This can be achieved by logging out of the extension, then pressing **Shift-F5** on the extension log in page when signing back in.
    - **Workaround**: This can be avoided by not actively using the extension during upgrades.
- When importing a secrets CSV file, if a field contains a comma in the value, then the import fails with a "*Wrong number of arguments*" error on the offending line.
    - **Workaround**: Manually edit the CSV file to remove the comma.
- When modifying the ownership of a secret, if all users are de-selected you are still permitted to save without an error. This results in the secret's ownership being assigned to **Entire Team**.
    - A save validation is being added in a future release.
- It is possible to create a request against an asset that is marked as inactive. However, this request is not visible in the **Requests** grid in Password Safe.
    - **Workaround**: Clear the inactive flag from the asset.
- If a ticket is supplied when creating a request and the ticket validation fails, only a generic validation error is shown to the user. This may be insufficient to troubleshoot the error.
    - Additional details are available in the logs and System Event Viewer. Error messaging is being improved in a future release.
- If you attempt to enable **IP Allow** network restrictions and at least one Resource Broker exists that has not yet been upgraded to 24.1, then the **Save** will fail with an *Internal Server Error* message.
    - **Workaround**: Upgrade all Resource Brokers to 24.1 (or remove unused Resource Brokers) prior to enabling **IP Allow** network restrictions.

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 24.1 are supported from BeyondInsight versions 22.2 or later releases.
- BeyondInsight 24.1 supports SQL Server 2016 SP2 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: c6c24a48eb14521a9ae58c46e5fcd5cf
- The SHA-1 signature is: 4e0c177cc634871d07255220f5e89066c448faf8
- The SHA-256 signature is: 248f3d64925c78d4b491efa1dd35f9de7127a5191ade4bb848e9f6b681b2653b

Note: *Incoming SAML communications (Assertions, Response) can no longer be signed using SHA1 by the Identity Provider. This is disabled for security purposes.*

Deprecation Notice:

BeyondInsight 24.1 still supports the following features, but these are planned to be removed in upcoming releases:

- **Team Passwords Public API Endpoints**: Planned for the 24.2 release. You must update scripts to use the corresponding Secrets Safe API endpoints.
- **Analytics & Reporting > Clarity**: Clarity and related reports and configuration. Release to be determined.
- **About > BeyondInsight Analysis**: Release to be determined.
- **Email notifications for failed API Authentications**: Release to be determined.