BeyondInsight and Password Safe 22.2 Release Notes

June 14, 2022

New Features and Enhancements:

- Scan workflow improvements:
  - Added support for Custom Scan Settings.
  - Removed uncredentialed discovery scan.
  - Added **Run Now** option for completed and scheduled scans.
  - Improved messaging around attempted use of older unsupported scanners.
  - Scan jobs can now be reassigned to a different scanner.
  - Scanner status is now displayed on the **Discovery Scanners** grid.
  - Updated the **Discovery Scan** icon.
  - Added warnings if attempting a scan including database enumeration without the proper credential type.
- Migrated pivot grid off AngularJS technology.
- Added new customizable password policy for BeyondInsight local users.
- Added new global configuration setting to disable forms login for new directory accounts, for use when SAML, smart card, or claims-aware is configured.
- Added new U-Series Appliance management action to **Assets** grid, for use with U-Series Appliances at or after version 3.5.
- Removed deprecated Cluster Analysis feature from user interface and reports.
- Renamed **Multi-Factor Authentication** card in configuration to **Authentication Management**; made related changes to the **Multi-Factor Authentication** section on **User Details**.
- Added **User Status** filter to **Users** grid in **Configuration User Management** area.
- Confirmed that SQL Azure database can be used as main BeyondInsight database.
- Removed **Certificate and Hardware** display from **Asset Details**.
- **Web Policy Editor**:
  - Added support for Designated User Authorization to the Mac message configuration.
  - Added SHA-256 as a matching criteria for Windows and Mac app types.
- **Analytics and Reporting**
  - Modified **Entitlement by Group** report with a new parameter and data field to allow inclusion of users that are currently disabled in Active Directory.
  - Added report to show registry monitoring event data.
  - Updated operating systems on reports to include Windows Server 2019 and Windows 11.

  Endpoint Privilege Management

  - Added version information to **About** page for Web Policy Editor plugin.
  - Added version information to **About** page for Privilege Management Reporting plugin.

- **Password Safe**
  - Asset and account onboarding improvements:
    - Added ability to manage assets and scanned accounts from the **Asset Advanced Details** screen.
    - Added navigation links between associated entities (**Asset > Managed System > Managed Account**).
    - Added link to **Advanced Details** screen on the **Edit Managed System** and **Edit Managed Account** forms.
    - Password Safe Cloud: administrator dashboard usability improvements.
    - Password Safe Cloud: improved Resource Broker download progress notification.
  - Dedicated account attribute mapping:
    - Password Safe now provides the ability to automate the process for mapping users on unique directory attributes (such as employeeID), simplifying the processes for managing users.
  - Added new global configuration setting to bypass password test when launching an SSH session.
  - Added new global configuration setting to control the password request display timeout.
  - Enhanced the **Managed System** grid to allow the ability to create Managed System Quick Groups.
  - Password Safe now streamlines the process of starting new web sessions for modern websites.
  - Added new feature: Managed Account Propagation:
    - Service account rotations are migrated to new propagation actions.
    - New script actions for any post credential rotation tasks.
    - All post credential rotation tasks can now optionally be assigned to a managed system Smart Group.
  - Added new delegable permission for admin session playback.
  - Session proxy improvements:
    - FIPS support is now bundled without needing an additional distributable.
    - Added support for the following SSH key exchange algorithms:
      - diffie-hellman-group14-sha256
      - diffie-hellman-group16-sha512
      - diffie-hellman-group18-sha512
- **API**
  - **New Features**
    - Propagation Action Support
      - Propagation Action Definitions
        - Propagation Action Types
          - **GET PropagationActionTypes** - returns a list of propagation action types.
        - Propagation Actions
          - **GET PropagationActions** - returns a list of propagation actions.
          - **GET PropagationActions/{id}/** - returns a propagation action by ID.
      - Managed Account Propagation Action Assignment
        - **GET ManagedAccounts/{id}/PropagationActions/** - returns a list of assigned propagation actions by managed account ID.

- **POST ManagedAccounts/{id}/PropagationActions/{propagationActionID}** - assigns a propagation action to the managed account referenced by ID.
- **DELETE ManagedAccounts/{id}/PropagationActions/** - unassigns all propagation actions from the managed account by ID.
- **DELETE ManagedAccounts/{id}/PropagationActions/{propagationActionID}** - unassigns a propagation action from the managed account by ID.

- Managed Accounts - Backwards compatibility with Propagation Actions - Translates legacy propagation action model flags to/from Propagation Action Mapping records
  - Sets legacy propagation action model flags from the existence or lack of propagation action mappings
    - **GET ManagedAccounts/{id}/**
    - **GET ManagedSystems/{id}/ManagedAccounts/ (all permutations)**
    - **PUT ManagedAccounts/{id}/**
    - **POST ManagedSystems/{id}/ManagedAccounts/**
    - **GET SmartRules/{id}/ManagedAccounts/**
    - **GET QuickRules/{id}/ManagedAccounts/**
    - **PUT QuickRules/{id}/ManagedAccounts/**
    - **GET ManagedSystems/{systemID}/LinkedAccounts/**
    - **POST ManagedSystems/{systemID}/LinkedAccounts/{accountID}/**
    - **GET ManagedAccounts/{id}/SyncedAccounts/**
    - **POST ManagedAccounts/{id}/SyncedAccounts/{syncedAccountID}/**
  - Creates propagation action mappings as appropriate for the given legacy model flags
    - **POST ManagedSystems/{id}/ManagedAccounts/**
  - Creates propagation action mappings as appropriate for the given legacy model flags and deletes any that should be removed
    - **PUT ManagedAccounts/{id}/**

- Managed System Quick Rules
  - Existing APIs
    - **GET QuickRules**
      - Now returns all Quick Rules (managed account and managed system)
      - Add optional query parameter type (default: all - all, ManagedAccount, ManagedSystem) - i.e.:
        - **GET QuickRules/[?type=all]**
        - **GET QuickRules/?type=ManagedAccount**
        - **GET QuickRules/?type=ManagedSystem**
    - **POST QuickRules**
      - New optional request body property RuleType : string (default: ManagedAccount - ManagedAccount, ManagedSystem)

- New APIs
  - **GET QuickRules/{quickRuleID}/ManagedSystems/** - returns a list of managed systems by Quick Rule ID.
  - **PUT QuickRules/{quickRuleID}/ManagedSystems/** - updates the entire list of managed systems in a Quick Rule by removing all **Managed System - Quick Rule** filters and adding a new one with the nanaged systems referenced by ID.
  - **POST QuickRules/{quickRuleID}/ManagedSystems/{systemID}/** - adds the managed system referenced by ID to the Quick Rule by adding it to the first **Managed System - Quick Rule** filter found.
  - **DELETE QuickRules/{quickRuleID}/ManagedSystems/{systemID}/** - removes the managed system referenced by ID from the Quick Rule by removing it from all **Managed System - Quick Rule** filters found.

- **Enhancements**
  - Smart Rule Processing Enhancements
    - **POST SmartRules/{id}/Process/[?queue=false|true]** - add queue query parameter for deferred Smart Rule processing.
    - Add new **ProcessingRequested : bool** property to Smart Rule responses - true if deferred processing has been requested, otherwise false.
  - Cloud-based managed system access URL.
    - Managed system minor model version 3.3 - New property added to request body.
      - **POST Workgroups/{id}/ManagedSystems/[?version=3.0]** (Note: On create, **AccessURL** can be set using **version=3.0**. If not set, will use the default URL for the Platform)
      - **PUT ManagedSystems/{id}/?version=3.3**
        - **AccessURL : string** - (default: default URL for the selected Platform) The URL used for cloud access (applies to cloud systems only). Max string length is 2048.
    - Latest version (currently 3.3) always returned in relevant response bodies:
      - **PUT ManagedSystems/{id}/**
      - **POST Workgroups/{id}/ManagedSystems/**
      - **POST Assets/{id}/ManagedSystems/**
      - **POST Databases/{id}/ManagedSystems/**
      - **GET ManagedSystems/{id}/**
      - **GET ManagedSystems/**
      - **GET Assets/{id}/ManagedSystems/**
      - **GET Databases/{id}/ManagedSystems/**
      - **GET FunctionalAccounts/{id}/ManagedSystems/**
      - **GET Workgroups/{id}/ManagedSystems/**
      - **GET SmartRules/{id}/ManagedSystems/**
      - **GET QuickRules/{id}/ManagedSystems/**
      - **PUT QuickRules/{id}/ManagedSystems/**

- **GET ManagedAccounts** - New property added to the response body
  - **UserPrincipalName : string** - User Principal Name of the directory-based account.
- Managed account **NextChangeDate** and **ChangeState** improvements
  - **GET ManagedAccounts**, **GET Aliases**
    - **NextChangeDate** - Now returns the next **Password Change Date** regardless of **Change Reason** (previously returned only the next **Scheduled Change Date**).
  - **GET ManagedAccounts** (all permutations)
  - **GET ManagedAccounts/{id}/**
  - **GET ManagedSystems/{id}/ManagedAccounts/** (all permutations)
  - **PUT ManagedAccounts/{id}/**
  - **POST ManagedSystems/{id}/ManagedAccounts/**
  - **GET SmartRules/{id}/ManagedAccounts/**
  - **GET QuickRules/{id}/ManagedAccounts/**
  - **PUT QuickRules/{id}/ManagedAccounts/**
  - **GET ManagedSystems/{systemID}/LinkedAccounts/**
  - **POST ManagedSystems/{systemID}/LinkedAccounts/{accountID}**
  - **GET ManagedAccounts/{id}/SyncedAccounts/**
  - **POST ManagedAccounts/{id}/SyncedAccounts/{syncedAccountID}**
    - Add **ChangeState : int** to response body
      - **0** = Idle / no change taking place or scheduled within 5 minutes
      - **1** = Changing / managed account credential currently changing
      - **2** = Queued / managed account credential is queued to change or scheduled to change within 5 minutes
- Improved Secure Remote Access Integration - Cloud System support.

Issues Resolved:

- Resolved issue affecting **Directory Queries** grid **filter by** dropdown activation within Chrome or Edge.
- Resolved issue with creating a new SAML identity provider sometimes getting into a state that shows an snackbar error message.
- Resolved issue affecting the Analytics and Reporting Configuration Wizard where changes were not properly discarded.
- Resolved an upload issue in the Analytics and Reporting **Report Styling** area.
- Resolved issue in which unsaved changes to the **Organizations** and **Oracle Internet Directory** configuration areas did not prompt to save or discard upon navigating to a different area.
- Resolved issue in which domain name was not shown for a functional account assigned in the Applications configuration.
- Resolved incorrect tab order issue in the **Create Functional Account** form when launched from the Smart Rule editor or **Managed System** form.
- Resolved issue in which a Smart Rule could be created with multiple conflicting **Manage Assets using Password Safe** actions.
- Resolved issue in which **Save** had to be pressed twice when editing a Connection Profile - Match condition.
- Resolved issue in which the grid filtering controls did not render properly in Firefox.
- Resolved issue in which an *Invalid port number: 0" error message* was sometimes incorrectly displayed when updating a functional account password.

- Udpated error notification text to be more precise when attempting to deactivate an asset Smart Rule that is used in another Smart Rule.
- Resolved a graphical issue in which an unnecessary **Upload** button was displayed when modifying the DSS key of a managed account.
- Resolved issue in which an HTML tag was improperly displayed in the delete confirmation prompt when attempting to delete a folder in Team passwords.
- Direct Connect now abides by location restrictions defined in the Access Policy Schedule.
- Improved connection time.
- **Web Policy Editor**
    - Account filters now work correctly when a SID is left empty.
- **API**
    - **GET ManagedAccounts**
        - Improved performance for requesters in environments with a large number of assets, managed systems, and managed accounts.
        - Improved performance when **accountName** and **systemName** are both given in environments containing a large number of identically-named accounts.
    - **GET UserAudits** - Query parameters **startDate** and **endDate** are now validated for lower date bounds. Values must be between **1/1/1753 12:00:00AM** and **12/31/9999 11:59:59PM**.
    - **GET UserAudits/{id}/UserAuditDetails/** - Team passwords audit entries no longer throw a *500 Internal Server Error*.
    - **POST ManagedSystems/{id}/ManagedAccounts/** - Concurrent managed account creation no longer intermittently results in *500 Internal Server Error* under heavy system load.
    - Concurrent managed system creation no longer intermittently results in 500 Internal Server Error under heavy system load.
        - **POST Workgroups/{id}/ManagedSystems/**
        - **POST Assets/{id}/ManagedSystems/**
        - **POST Databases/{id}/ManagedSystems/**
        - **PUT ManagedSystems/{id}/**
    - Managed system functional account is no longer required when **version** >= **3.1** and **RemoteClientType=EPM**.
        - **POST Workgroups/{id}/ManagedSystems/**
        - **POST Assets/{id}/ManagedSystems/**
        - **POST Databases/{id}/ManagedSystems/**
        - **PUT ManagedSystems/{id}/**

Known Issues:

- When using the **ps_automate** session utility and configured to use the Firefox browser to a website using a self-signed certificate and the **IgnoreCerts** flag, the login is successful but the webpage does not respond. Workarounds: use a different browser, use a valid (not self-signed) certificate, after login click shift-refresh and manually accept the browser security warning for the session, or add the necessary steps to the automate configuration file to accept the warning prompt.
- When creating a new password policy or DSS key policy, an unnecessary success toast message displays: *Changes have been discarded*. This notification can be ignored.

- When modifying a **Set attributes on account** Smart Rule action, if you change the attribute type from one, which is a numeric name (i.e. **1**) to a different attribute type, an error will occur: *Key type must be int for this method of adding items*. Workaround: delete the **Set Attributes** action and recreate.
- In a FIPS-enabled environment, attempting an RDP Admin Session will be unsuccessful and an error message shown. Workaround: use a standard managed RDP session if possible.
- In rare cases, if the time zone of the scanner has changed, a scheduled scan may not start at the scheduled time. Workaround: The scan will run at the next scheduled time.
- If forms login is disabled for a user when another login method is not setup, that user cannot login. Workaround: ensure that another login method is setup before setting **Disable Forms Login** to **yes** globally or for any user.
- Upgrading after installing BeyondInsight to a location other than the default displays an error message. Workaround: if you manually upgrade, select the alternate install folder during the upgrade.
- **Scan Data Users** grid may incorrectly display *Password Expired* for some accounts. Workaround: log in with the affected user, or force them to change/set the password.
- Analytics and Reporting: The **Retina Product Usage Details by Organization** report may not show any results in environments that do not have Retina scanners. Workaround: none, this report is no longer valid and will be removed in an upcoming release.
- **Scan Data User Details** shows the user **Description** in the **Full Name** field, and may show a blank description. Workaround: none, this is informational and does not have any impact on the onboarding of the user.
- In rare cases, installing BeyondInsight 22.2 on a U-Series Appliance may crash due to BIAdmin service not starting. Workaround: delete all JSON files from the BIAdmin directory, then repair the BeyondInsight installation from **Programs and Features**.
- Configure HSM Credentials utility may crash when testing a new HSM Credential if you don't fill in the **Key Name** field. Workaround: be sure to fill in all the fields before testing the credential.
- Deleting a user that has an active Password Safe Request or related SSH Session will not succeed, and the error message is vague. Workaround: none, this is expected behavior. The error message may be improved in an upcoming release.
- The first attempt to edit a BeyondInsight user from the **User Details Edit** form results in a form validation error on fields that were not changed. Workaround: discard the changes and try again, or edit the user from the grid row action.
- Analytics and Reporting: changes to saved views or snapshots do not reflect right away in the list. Workaround: refresh the page to see the changes.
- In the Configure HSM Credentials utility, selecting the **Hardware Security Module User Guide** from the **Help** menu displays an error. Workaround: this documentation is now avaiable online on the BeyondTrust documentation site.
- The **No Enumerations Selected** banner may not display in the Scan Wizard if the **Unlimited Users** box is unchecked. Workaround: ensure you select the enumeration options needed for the scan.
- The **Scan Data Ports** grid shows a limited number of ports, with fewer details. Workaround: none; this is informational. The new BeyondTrust Discovery Agent does not perform protocol detection and returns only the standard database and remote access ports here.
- Naming a scan with a name belonging to a previously deleted scan appends a counter to the end of the scan name. Workaround: the deleted scan still exists behind the scenes and the name cannot be reused. Give your scan a new name.
- Using a low/least privilege user as proxy during Analytics and Reporting configuration may lead to this user not being able to download the Analytics and Reporting log files. Workaround: add this user to the **msdb.dbo** table so they can download the logs.
- It is possible to create multiple SAML providers with the same name. Workaround: none; this is not an issue because name is not the unique identifier. If the user finds it confusing, they can edit the names to be unique.
- If a credential description begins with text matching the name of the scan it is used in, the scan is displayed as though an ad-hoc credential was used. Workaround: edit the credential description to be something other than the scan name.
- Analytics and Reporting: pivot grid chart may display blank if the data was recently pivoted. Workaround: expand the data after pivoting, or remove/re-add the chart.
- System Event Viewer may display errors with sources of *SideBySide* or *AppBus*. Workaround: none; this is informational. The errors do not cause any system issues and will be cleaned up in a future release.

- If the Endpoint Privilege Management plugin is configured but the corresponding MSI is not installed, the Event Service log may contain error messages such as *System.Net.Http.HttpRequestException*. Workaround: be sure that the MSI is installed and complete the plugin configuration to use this feature.
- IIS App Pool users may be displayed in the **Scan Data Users** grid if those accounts have logged into the scanned asset. Workaround: none; this is expected behavior.
- Some long field names from BeyondInsight password policy changes or directory credential changes might be truncated in the **User Audit Details** view. Workaround: none; this is informational. Some field names can be inferred from the parts that are visible before they are truncated.

Notes:

- Direct upgrades to 22.2.0 are supported from BeyondInsight versions 7.0 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: 16226c09095b61f1a4e176ab6347073d
- The SHA-1 signature is: 4aba0916a6391769fae0ca6d2de2fd33d5a733e2
- The SHA-256 signature is: 1ff5a869c0257bf9fb0e16c30181cd354530ae6ae139537252380354521a91fc