BeyondInsight and Password Safe 7.0.0 Release Notes

August 18, 2020

New Features and Enhancements:

- **General:**
    - This release does not support Vulnerability Management functions.
    - This release does not include support for the following functions. If you require this functionality after upgrading to 7.0, please contact support for advice.
        - Privilege Management for Unix & Linix Event View, Search, and Session Replay
        - Endpoint Privilege Management powered by PowerBroker Session Monitoring Event View and Session Replay
        - Endpoint Privilege Management powered by PowerBroker File Integrity Monitoring Event View
    - Replaced Flash **Custom Attribute** management UI with HTML5 UI.
    - Added support for parallel smart rule processing to Omniworker.
    - Added threading and failure cool off options for Omniworker.
    - Added 5 new **Dashboard** cards to show information about Omniworker jobs.
    - Added an option to force smart groups to process on a specific worker node.
    - Exposed log level configuration in the user interface.
    - Added support for database error logging functionality.
    - Added new **Dashboard** tile to show recent error and warning counts when database error logging is enabled.
    - Exposed advanced purging options and database maintenance under **Configuration**.
    - Added link to **Smart Rules** grid in main menu.
    - Added a **Scan Wizard** to create new discovery scans on a manually entered list of targets.
    - Added row action to create new discovery scan against a single smart rule from the **Smart Rules** grid.
    - Added row and bulk action to create new discovery scan against selected assets from the **Assets** grid.
    - Added support for installing BeyondInsight with a low privilege SQL application account.
    - Replaced Flash Endpoint Privilege Management **Exclusions** UI with HTML5 UI.
    - Replaced Flash Endpoint Privilege Management **Policy Users** UI with HTML5 UI.
    - Renamed **Policies** tile and menu item to **Policy Users** to accurately reflect the **Policy Users** grid that it links to.
    - Added menu link to **Endpoint Privilege Management Policies** grid.
    - Replaced Flash Scheduled **Scans** UI with HTML5 UI.
    - Replaced Flash Scheduled **Scan Details** UI with HTML5 UI.
    - Replaced Flash and HTML5 Preview of **Active and Completed Scans** UI with fully featured HTML5 **Active and Completed Scans** UI.
    - Restricted viewing of prior non-discovery scan reports to only BeyondInsight Analytics & Reporting.
    - Replaced Flash **Connectors** configuration UI with HTML5.
    - Deprecated the following **Connector** types: Palo Alto Networks, STIX/TAXII, and Third Party Credential Provider.
    - Added support for integration with Privilege Management Reporting.
    - Added memory of previous grid filter selections when returning to a grid.

  - Improved website performance with static compression.
  - Added filtering on **Rule Type**, **Rule Name**, **Arguments**, and **Path** to **Endpoint Privilege Management Events** grid.
  - Updated EULA.
  - Replaced auto-save functionality on API **Registrations** page with **Save/Discard** button pair.
  - Restored ability to filter **Smart Rules** grid by **Smart Rule** action.
  - Added extra logging to instances of TLS communication in which certificate chain validation is invalid.
  - Enhanced **Directory Credentials** edit form to require password entry when changing **domain/user/ssl** field values.
  - Added **User SSH Key** details display under **Asset Advanced Details**.
  - Added support for deleting a single workgroup from an organization.
  - Updated URL to BeyondInsight documentation location.
  - New permissions to delegate smart rule creation.
- **Password Safe:**
  - Platform support: Internet Information Services (IIS) Application Pool
  - Support for Kex Algorithms (ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,and diffie-hellman-group-exchange-sha256)
  - RDP multi-monitor support
  - Replaced Flash UI with HTML5 UI in the following **Configuration** areas:
    - Access Policies
    - Connection Profiles
    - Custom Platforms
    - Global Settings
    - Mail Agent
    - Mail Templates
    - Managed Account Aliases
    - Password Change Agent
    - Password Test Agent
    - Session Agents
    - Session Masks
    - Ticket Systems
  - Managed account aliases now support a single-account mapping.
  - Added the ability to change managed system platform upon editing.
  - Added **Set Attributes** action to managed system smart rules.
  - Added ability to use existing functional account/managed account when testing custom platforms.
  - SSH host key and key exchange algorithms are now configurable.
  - RSA private host key size is now configurable.
  - Local and remote port forwarding (SSH) is now disabled by default.
  - Session countdown timer display period is now configurable.
  - Added support for dynamic delimeter in DirectConnect.

- **API:**
  - **POST Sessions/Admin**: Admin session support.
  - Public API logfile is now named **publicapi<date>.txt**.
  - Single Account Alias support
    - **GET Aliases**, **GET Aliases/{id}**, **GET Aliases?name={name}**
      - New response body property **AliasState : int**, with possible values:
        - Mapped
        - Highly Available

> ***Note:*** *Aliases having State value 0 (zero) Unmapped will not be returned via these APIs. Zero indicates an unmapped alias, which cannot be used for corresponding API* ***POST Aliases/{id}/Requests****.*

- - - **GET Aliases**: New optional query parameter **state**:
      - **state** (optional default: **1**,**2**) - Zero or more **Alias State** values.
- **Other**
  - Delegated Smart Rule Permissions
    - **POST QuickRules**: Now requires Smart Rule Management - Managed Account (Read/Write) in addition to the existing Password Safe Account Management (Read) permission.
    - **POST SmartRules/FilterSingleAccount** (deprecated): Now requires Smart Rule Management - Managed Account (Read/Write) in addition to the existing Password Safe Account Management (Read) permission.

Issues Resolved:

- Ticket System platform exclusion
  - **POST Assets/{id}/ManagedSystems**, **POST Workgroups/{id}/ManagedSystems**: Ticket system-based platforms can no longer be used to create asset-based managed systems.
  - **GET EntityTypes/1/Platforms**: No longer returns ticket system-based platforms.
- **PUT ManagedAccounts/{id}**: Managed accounts that have pre-existing remote application associations now update properly.
- **DELETE ManagedAccounts/{id}**: No longer fails sporadically under heavy system load.
- **POST Users (ActiveDirectory)**: Missing Active Directory user now properly returns a *400 Bad Request*.
- **PUT Users/{id}**: A duplicate username now properly returns a *400 Bad Request*.
- **DELETE UserGroups/{userGroupId}/SmartRules/{smartRuleId}/Roles**: Properly validates **userGroupId** and **smartRuleId**.
- **POST Requests**, **POST RequestSets**: User-created ticket systems now work as expected.
- **POST Requests (`AccessType=App`)**: Properly validates **ApplicationID**.
- **PUT Requests/{id}/Deny**: Excludes Password Safe API **Global Quarantine** permission from allowable permissions/roles.
- **GET DSSKeyRules/{id}**, **GET PasswordRules/{id}**: Now validates **{id}** is in the proper numeric range.
- **POST Keystrokes/Search**: When **Full Text Search** is not installed or is disabled, returns a *400 Bad Request*.
- **POST|DELETE ManagedAccounts/{id}/SyncedAccounts**: Removed Management Console Access Permission requirement.
- **POST FunctionalAccounts**: Properly validates maximum length of **AccountName**, improved performance.
- **POST Vulnerabilities/ExportReport**: Request body now validated properly.

- Resolved issue with debug logging behaving in the opposite manner as intended.
- Resolved issue with Password Safe **accountname** not being displayed in request details page.
- Resolved issue with API only supporting static bind accounts when adding an AD group, in which managed bind accounts did not work.
- Resolved issue in which ArcSight CEF format should have used more predefined CEF fields.
- Resolved issue in which Password Safe xml import didn't work correctly.
- Resolved issue with Password Safe-managed accounts smart rule **User Account Attribute**, in which selecting any option caused an error.
- Resolved issue with not able to edit directory queries that do not appear in the initial list.
- Resolved issue in which certificate validation is not enforced for LDAPS connection in several places.
- Resolved issue in which configured applications were not available to users when no Managed System or Functional Account assigned and associated with a domain linked account.
- Resolved issue with domain controller dropdown not handling domain controllers with missing attributes.
- Resolved issue in which GUI always reverted back to **equals** when editing asset smart groups with user account attribute.
- Resolved issue in which elevation command sendt IP but not hostname.
- Resolved issue in which enable password was lost during the password change when a functional account was auto-managed.
- Resolved issue with PMUL event tables not processing.
- Resolved issue in which event forwarding for scan events ran very slowly with large amounts of scan data.
- Resolved issue in which font smoothing was disabled by default for RDP sessions downloaded from Password Safe.
- Resolved issue in which Internet Explorer failed to detect filename in downloaded RDP files that contained non ascii characters.
- Resolved issue in which Password Safe website did not allow login if the Common Name (CN) of Active Directory user was the same as another.
- Resolved issue in which Jira ticket system could not validate cloud accounts since username has been deprecated.
- Resolved issue in which LDAP directory query smart rules failed if one of the schema attributes existed but had no value for a user object.
- Resolved issue in which LDAP managed accounts no longer worked with directory queries.
- Resolved issue in which logins were very slow when forest contained multiple domains with a mix of trusted and untrusted domains.
- Resolved issue with Managed Account smart rule using asset smart group as filter, in which favorite items did not appear under **Favorites** tab.
- Resolved issue in which onboarding smart rule did not work when managed system auto-manage flag was set to **false**.
- Resolved issue in which Password Safe requested duration day spinner did not show the proper default release duration value.
- Resolved issue in which Policy User LDAP discovery smart rules ran very slowly and had excessive logging in INFO mode.
- Resolved issue with **POST Requests** API not honoring **ConflictOption** for **AccessType App**.
- Resolved issue with RADIUS in which multiple attempts were made against the same server, when multiple servers existed with different filters.
- Resolved issue in which **reportableFlag** was not set to **false** for SNMPv3 traps.
- Resolved issue in which Sailpoint v2 with MS SQL connector failed if the username or password contained a semicolon (**;**) character.
- Resolved issue with scan job refresh stopped working if an AWS load balancer was added as a target.

- Resolved issue in which scan reports did not open for non-administrator users from the **Scan Jobs** page.
- Resolved issue in which SCIM API /v2/ContainerPermissions threw an exception when using *container* in the filter.
- Resolved issue in which ServiceNow user validation fails if casing differed in BeyondInsight vs. ServiceNow.
- Resolved issue with managed account smart rule in which the account options were not maintained on save if the automatic password managed was set to **NO**.
- Resolved issue in which special characters were not escaped correctly when running a scan with CPv2.
- Resolved issue in which SSH authentication switched from **Password** to **Keyboard-Interactive** during the login.
- Resolved issue in which Sybase ASE did not allow for SSL connections.
- Resolved issue with synchronizing LDAPS users after adding a group failed with the error: *System.Runtime.InteropServices.COMException (0x8007200F): The directory service is unavailable*.
- Resolved issue in which Password Safe did not detect Windows 2016/Windows 10 correctly when updating TaskScheduler tasks.
- Resolved issue in which requests for dedicated accounts could not be approved.
- Resolved issue in which custom reports could not be saved to a sub folder in Analytics & Reporting.
- Resolved issue in which updates to **AssetName** did not update Password Safe managed system name.
- Resolved issue in which updating a policy via Privilege Management for Windows Policy Editor took a long time and timed out or threw a concurrency error.
- Resolved issue in which SQL **view vw_UtilMA_API** did not select the correct **SystemName** for DomainLinked accounts.
- Resolved issue in which a managed system did not return any data for a global keyword search when it did not have an associated asset.
- Resolved issue in which smart rule execution failures were not handled correctly and smart rule remained in processing state.
- Resolved issue in which smart rules with reserved SQL keywords in the criteria did not work properly.
- Resolved issue in Password Safe in which a vulnerability in dedicated account mapping allowed access to another account.
- Resolved issue in which attempting to add Qualys Connector caused an error.
- Resolved issue with Password Safe worker nodes in which setting workgroup allocation back to unassigned failed with an error.
- Resolved issue in which event forwarding queue in Omniworker did not correctly send **KeepAlive** events.
- Resolved issue in which NetBIOS cache lookup resolved domains that were not being used for app users.
- Resolved issue in which smart rule status intermittently failed to update, resulting in rules incorrectly showing as failed or long running.
- Resolved issue in which by calling our internal APIs you could create a new request for an RDP session, but subsequently call another API and retrieve the password for that account, even if viewing the password wasn’t valid for that request.
- Resolved issue in which **User Management Features** grid did not display proper data for public API-created user groups.
- Resolved issue in which importing RTD file failed with error: *System.IndexOutOfRangeException: Cannot find table 0*.
- Resolved issue in which large numbers of applications caused the application administration page to become unresponsive.
- Resolved issue with the **GET ManagedAcounts** API call, in which omitting the limit paramter would result in a return of 100,000 items. The defaul maximum is now **1,000** when no limit is specified.
- Resolved issue with CA Service Desk validating CH tickets.
- Resolved issue in which the **Configuration > Address Groups** page did not show the **Groups**.
- Resolved issue in which Function Account test for Telnet causes the error: *Object reference not set to an instance of an object.*
- We now allow configuration of default 2FA user mapping type.
- Resolved issue in which smart card throws an error and user cannot log in when two smart card users have the same name but a different domain or UPN.

- Resolved issue in which an account with username/password greater than 117 characters cannot be added because the user/password field for BI/AD/LDAP users is 117 characters.
- Resolved issue in which manual smart group created from the **Managed Accounts** grid does not show up in the **Smart Group** filter even after refreshing the grid.
- Resolved issue in which deleting an attribute that is in use in a smart rule will cause the smart rule to quietly choose the next attribute in the dropdown upon the next edit and save of smart rule.
- Resolved issue with the list of managed accounts in the **Managed System Advanced Details** list, in which the non-managed cloud platforms showed a **Test** button that was not applicable and did nothing. Workaround: ignore the button.
- Resolved issue in which DSS Keygen used newer OPENSSH client results in a key generated with an OPENSSH header that we don't support.
- Resolved issue in which newly created custom asset attributes did not appear in the smart rule editor attribute dropdown.
- Resolved issue in which the Password Policy dropdown on the **Create New Managed System** form was not long enough.
- Resolved issue in which migration from PowerBroker for Mac to Privilege Management for Mac may see a delay in policy delivery to the asset.
- Resolved issue in which you could not create an **Account Naming** attribute with fewer than 3 characters when onboarding LDAP users.
- Resolved issue in which database compatibility level was still at SQL Server 2008 (100) on upgrades, even though SQL Server 2008 is not supported in v6.10.
- Resolved issue in which managed **Systems Smart Rules** name and description filters used the **Starts With** operator rather than the **Contains** operator.
- Resolved issue in the list of managed accounts under a **Managed System Advanced Details** list, in which the Amazon platforms showed a **Use Own Credentials** switch that was not applicable.
- Resolved issue that occurred when configuring a **Managed System Smart Rule** to match on **Assigned Custom Attributes**, in which changing the operator after selecting the attribute type changed the list of attributes to the default, **Business Unit**, rather than keeping them related to the **Attribute Type** selected.
- Resolved issue in which a limited user with full access to managed systems could not see the functional accounts related to a managed system.
- Resolved issue in the **Server Keys** grid in the **Advanced Details** of a managed system, in which the **Denied Dates** filters did not function.
- Resolved issue in which the **Test Functional Account** of an LDAP Directory Managed System improperly used the **Use SSL** setting from the managed system rather than the functional account, which resulted in the testing of the LDAP functional account to fail if SSL was enabled.

Notes:

- Direct upgrades to 7.0.0 are supported from BeyondInsight versions 6.6.x or higher.
- Adobe Flash Player is not required to use any part of BeyondInsight 7.0.
- The MD5 signature is: 3e595dc8f950211949180d1d4ec94a54
- The SHA-1 signature is: 359a466507f741f7701e2e0b5219a37f02301e68
- The SHA-256 signature is: c8f9042bc93aacfd9fa0b481b7db607e64ef19537a914ff4cef394d88df872a0