BeyondInsight and Password Safe 7.2.0 Release Notes

December 1, 2020

New Features and Enhancements:

- **General:**
  - Replaced Flash Endpoint Privilege Management (powered by PowerBroker) File Integrity Monitoring Grid with HTML5 UI.
  - Replaced Flash Endpoint Privilege Management (powered by PowerBroker) **Session Monitoring Events** grid with HTML5 UI.
  - Replaced Flash Endpoint Privilege Management (powered by PowerBroker) Session Replay Viewer with HTML5 UI.
  - Added status icons to **Scans** grid.
  - Added version numbers to data in Application Version Analyzer in BT Analyzer for all DLLs.
  - Clarity Malware Analysis Manager is now opt-in, off by default for new installations. No change to upgrades.
  - Added a public API endpoint to support the addition of an application to an application group within an EPM policy.
  - Added an option to set a preferred domain controller for an individual Active Directory login account.
  - Added option to overwriting individual preferred domain controller for all accounts in a group.
  - Added support for Sybase, PostgreSQL, MongoDB, and Terradata credentials (requires minimum scanner version of 20.0).
  - Added support for sending scans to and receiving data from scanner version 20.0.
  - Removed option to share credentials with local scanner users.
  - Removed code and database tables that previously supported Patch Management.
  - Removed code and reports that previously supported Benchmark scanning.
  - Updated a number older UX components for improved experience.
  - Modified smart rule editor Attribute filter, Attribute action, and Email Alert action behaviour to improve performance when large numbers of attributes or email recipients exist.
  - Upgrade process from 7.0 to 7.2 explicitly removes Flex .swf files if present in upgrade scenarios.
  - Reinstated warning to administrator user if license is due to expire in 30 days or less.
  - Added NetBIOS information to asset schema.
  - Added SAML configuration user interface.
- **Password Safe:**
  - Password Safe is now available as-a-service.
  - Salesforce is now a managed platform.
  - IP Address has been added to the **Managed Systems** grid.
  - Added **Remote Session Activity** report.
  - Session check-in will now close the session for the user.
  - Added API Registration setting: **Enforce multi-factor authentication** (default: enabled).
  - NetBIOS information is automatically populated on Managed System from scanned asset data.
  - Added additional session proxy configurable settings.

- **API:**
  - Multi-factor authentication now an optionally enforced setting on the API Registration. The default value is **on/enforced**.
  - **DELETE ManagedSystems/{id}/ManagedAccounts/** : Deletes all Managed Accounts by Managed System ID.
  - New Address Group APIs:
    - **GET AddressGroups/{id}/** : Returns the Address Group by ID.
    - **GET AddressGroups/?name={name}** : Returns the Address Group by name.
    - **POST AddressGroups/** : Creates an Address Group.
    - **PUT AddressGroups/{id}/** : Updates an Address Group by ID.
  - New Address APIs:
    - **GET Addresses/{id}/** : Returns the Address by ID.
    - **POST AddressGroups/{id}/** is now superceded by POST.
    - **AddressGroups/{id}/Addresses/** : Creates an Address in an Address Group.
    - **PUT Addresses/{id}/** : Updates an Address by ID.
    - **DELETE Addresses/{id}/** : Deletes an Address by ID.
  - Minor model versioning support for **POST|PUT ManagedAccounts** request body using query parameter **version**.
  - Current/usable versions:
    - 3.0: Default if not specified
      - **PUT ManagedAccounts/{id}/?version=3.0**
      - **POST ManagedSystems/{systemID}/ManagedAccounts/?version=3.0**
    - 3.1: Adds support for **UseOwnCredentials : bool**
      - **PUT ManagedAccounts/{id}/?version=3.1**
      - **POST ManagedSystems/{systemID}/ManagedAccounts/?version=3.1**
    - 3.2: Adds support for **ChangeIISAppPoolFlag : bool** and **RestartIISAppPoolFlag : bool**
      - **PUT ManagedAccounts/{id}/?version=3.2**
      - **POST ManagedSystems/{systemID}/ManagedAccounts/?version=3.2**
    - Latest version (currently 3.2) always returned in relevant response bodies
      - **PUT ManagedAccounts/{id}/**
      - **POST ManagedSystems/{systemID}/ManagedAccounts/**
      - **GET ManagedAccounts/{id}/**
      - **GET ManagedSystems/{systemID}/ManagedAccounts/**
      - **GET ManagedSystems/{systemID}/ManagedAccounts/?name={name}**
      - **GET QuickRules/{quickRuleID}/ManagedAccounts/**
      - **PUT QuickRules/{quickRuleID}/ManagedAccounts/**
      - **GET SmartRules/{smartRuleID}/ManagedAccounts/**

- **PUT Requests/{id}/Checkin/** : Request check-in now completes/ends related sessions.
- Direct Connect auditing enhancements:
  - Now audited as *Direct Connect*
  - Source/caller IP logged in audit record details

Issues Resolved:

- **DELETE ManagedSystems/{id}/** : Concurrent **ManagedSystem** deletes no longer sporadically fail under heavy load.
- **PUT Assets/{id}/** : **AssetType** now set to default value if not specified.
- Resolved a previous known issue in which Analytics and Reporting process daily job failed if Password Safe Access Policy name exceeded 20 characters in length.
- Resolved an issue in which BeyondInsight created a session cookie for a failed login.
- Resolved an issue in which WebScan URL was a choice available in the type of address to add when setting up an address group, despite not being supported in the product anymore.
- Resolved an issue with SQL connection pool exhaustion.
- Resolved an issue in which EPM Event processing was able to fall behind in processing large quantities of heartbeat events.
- Resolved an issue with assigning tickets to managed accounts that were set to useSelf to login to target host.
- Resolved an issue in which clicking on some parts of the web page did not refresh the session.
- Resolved an issue in which Address Groups list did not show up in Safari.
- Resolved an issue in which Scanner connectivity warning was not accurate.
- Resolved an issue with improper access control on scan credentials page.
- Resolved an issue in which managing passwords on MongoDB was successful on client but failed to update RetinaCS database.
- Resolved an issue in which AD users could not login when customers only partially applied patch.
- Resolved an issue in which **Mail Templates > BI Host URL** only allowed for IP addresses and not hostname/FQDN.
- Resolved an issue in which using **EnableCheckoutAuthorization** directory users received an error on session or password retrieval.
- Resolved an issue with **AssetName** that contained parts of an IP, in which they were padded, but not un-padded.
- Resolved an issue in which API users could no longer sign in after changing user group name.
- Resolved an issue in which email setting reverted to port 25 regardless of SMTP setting in remconfig.
- Resolved an issue in which users could not log into a trusted domain with a managed bind account after adding an Active Directory Group.
- Resolved an issue in which passwords validated on every keystroke, which caused the cursor to *jump* and remove characters.
- Resolved an issue in which BeyondInsight Analytics and Reporting User Account List Report could not list linux host if they did not have a domain.
- Resolved an issue in which the user had to refresh the page to have a new language take effect after changing the language on the **Team Passwords** screen.
- Resolved an issue in which escaped characters (backslashes (\)) in downloaded contents from the **Team Passwords Credentials** grid appeared in a CSV file.

Known Issues:

- **BeyondInsight:**
  - Grids do not remember state correctly using Firefox in Incognito mode. Workaround: Use a different browser, turn off incognito mode, or reset your grid preferences on each visit.
  - UVM Event Viewer Application Windows Logs contains many exceptions related to ASP.NET 4.0.30319.0. Workaround: RDP to the UVM and click **Apply**.
  - Strangely formatted BouncyCastle DLL version number under **BeyondTrust\BIAdmin\BIAdmin folder** path (1.8.6+e72e3a8a96). Workaround: the DLL version numbers are not controlled by BeyondTrust as this is a third party Dll. This can be safely ignored.
  - When executing **Sync Group Users** from the **User** grid under **User Management Group Details** for an AD or LDAP group, the grid does not automatically refresh. Workaround: Navigate away and return, or refresh the browser.
  - Assets scanned using BeyondTrust Discovery v20 and non-functional credentials may import without an asset name and appear as duplicates in the **Asset** grid. Workaround: Delete the duplicate asset after scanning with good credentials.
- **Password Safe:**
  - When adding an asset to Password Safe, the **Name** field is set automatically from the Asset Name; however, the field is still editable. Changing the name here causes an error if attempting to subsequently modify the settings of the Managed System. Workaround: do not change the name of the system when adding it to Password Safe.
  - Only Administrator users can assign the **Team Passwords** feature to a group via User Management. Attempting to assign this feature as a non-Administrator user causes an error.
  - Password Safe Cloud only: When specifying a Change Password Time in a Managed Account Smart Rule for onboarding, the time specified is in UTC/GMT.
  - Password Safe Cloud only: When specifying Access Policy schedule start/end times, the time specified is in UTC/GMT.
  - Password Safe Cloud only: When installing the Resource Broker bundle on a Windows Server 2016 system, an unspecified error might be encountered during the Microsoft .NET Framework 4.7.2 phase. Workaround: disable **IE Enhanced Security** from Server Manager.
  - Password Safe Cloud only: SAP platform is not supported in the 7.2 release. Support is to be added in a forthcoming maintenance release.
  - Password Safe Cloud only: vSphere Web API platform is not supported in the 7.2 release. Support is to be added in a forthcoming maintenance release.
  - Password Safe Cloud only: Propagating password changes to IIS AppPools is problematic.
  - Password Safe Cloud only: Propagating password changes to Scheduled Tasks on Server 2016/2019 is problematic when the task **RunAsUser** is a domain account, the asset is on the domain, and the asset has a local user with the same username.
  - Password Safe Cloud only: Users intermittently encounter *Form is stale* error. A browser refresh resolves the issue.
  - Password Safe Cloud only: Omitted IP addresses in an Address Group may be included in the scan target list. Workaround: ensure the addresses you wish to omit are not included in the Address Group, or delete any unintentionally scanned assets from the asset grid after the scan is completed.

Notes:

- This release does not support most Vulnerability Management functions.
- This release does not include support for the following functions:
  - Privilege Management for Unix & Linux Event View, Search, and Session Replay
- Direct upgrades to 7.2.0 are supported from BeyondInsight versions 6.8.x or higher.

- Adobe Flash Player is no longer required to use any part of BeyondInsight 7.2.
- Adobe Flash SWF files can no longer be patched back into BeyondInsight 7.2.
- This release is available by download for BeyondTrust customers (https://beyondtrustsecurity.force.com/customer/login) and by using the BeyondTrust BT Updater.
- The MD5 signature is: 87ab6592e7ceea4574bb7036bc719562
- The SHA-1 signature is: 34ed30d4f85a1215ed626e1457cf1da040611b0c
- The SHA-256 signature is: d70eb6a1a309b06d18c130da14be4df7b72f90cbeddaf783d5603c78e74e0ce0