BeyondInsight and Password Safe 21.1 Release Notes

April 13, 2021

New Features and Enhancements:

- Added an option to hide the upcoming maintenance expiry banner.
- Restored the **Scan Progress** column to the **Active/Completed Scans** grid.
- Added **SQL Options** support to Privilege Management Reporting plugin configuration.
- Removed support for Vulnerability type **Smart Rules**.
- Deactivated Smart Rules that rely on Vulnerability specific criteria or actions.
- Added **Deprecated Smart Rules** section to BTAnalyzer report to list Smart Rules that were deactivated on upgrade due to invalid criteria or actions.
- **Analytics and Reporting**
    - Replaced the Analytics and Reporting homepage report with the Report Browser.
    - Removed support for making a saved view into the homepage report.
    - Introduced a **Deprecated** folder for all Vulnerability Management Reports.
    - Migrated a number of areas under Analytics and Reporting off AngularJS.
    - Removed support for Threat Analyzer, a Vulnerability Management function.
- **API:**
    - Team Passwords Support
        - Folders

API Call	Description
GET TeamPasswords/Folders/	Get all Team Passwords Folders
GET TeamPasswords/Folders/{id}/	Get Team Passwords Folder by ID
POST TeamPasswords/Folders/	Create Team Passwords Folder
PUT TeamPasswords/Folders/{id}/	Update Team Passwords Folder by ID
DELETE TeamPasswords/Folders/{id}/	Delete Team Passwords Folder by ID

        - Credentials

API Call	Description
GET TeamPasswords/Folders/{id}/Credentials/	Get Team Passwords Credentials by Folder ID
GET TeamPasswords/Credentials/{id}/	Get Team Passwords Credential by ID
POST TeamPasswords/Folders/{id}/Credentials/	Create Team Passwords Credential in Folder
PUT TeamPasswords/Credentials/{id}/	Update Team Passwords Credential by ID
DELETE TeamPasswords/Credentials/{id}/	Delete Team Passwords Credential by ID

- Team Passwords supporting changes:
  - For all User Group APIs, added the **Description : string** property to the response body.
  - Creating or deleting an existing User Group that has the **Team Passwords** Feature/Permission enabled requires the caller to be an administrator:
    - **POST UserGroups/**
    - **DELETE UserGroups/{id}/**
    - **DELETE UserGroups/?name={name}**
  - Adding or removing the **Team Passwords** Feature/Permission to or from a User Group requires the caller to be an administrator:
    - **POST UserGroups/{id}/Permissions/**
    - **DELETE UserGroups/{id}/Permissions/**

- AD and LDAP Users can now be removed if they do not belong to a User Group: **DELETE Users/{id}/**.
- Access Policy Request Reason and ticket system support:
  - For **GET AccessPolicies/ and POST AccessPolicies/Test/** the following properties have been added to the response body:
    - **RequireReason : bool**
    - **RequireTicketSystem : bool**
    - **TicketSystemID : short?**
  - For **POST Requests** and **POST RequestSets**, the Access Policy Schedule is now used to check ticket system requirements.
- Minor model versioning support for POST|PUT ManagedSystems request body using query parameter **version**:
  - Current/usable versions:
    - 3.0 - Default if not specified
      - **PUT ManagedSystems/{id}/[?version=3.0]**
      - **POST Workgroups/{id}/ManagedSystems/[?version=3.0]**
      - **POST Assets/{id}/ManagedSystems/[?version=3.0]**
      - **POST Databases/{id}/ManagedSystems/[?version=3.0]**
    - 3.1 - Adds support for **RemoteClientType : string** (support for Endpoint Privilege Management)
      - **PUT ManagedSystems/{id}/?version=3.1**
      - **POST Workgroups/{id}/ManagedSystems/?version=3.1**
      - **POST Assets/{id}/ManagedSystems/?version=3.1**
      - **POST Databases/{id}/ManagedSystems/?version=3.1**
  - Latest version (currently 3.1) 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/**
    - VMS Removal:
        - Vulnerability Smart Rules have been removed. Any reference to Smart Rule type **Vulnerability** is now obsolete.
        - The following VMS APIs have been removed and now return *404 Not Found*:
            - **GET Assets/{id}/Vulnerabilities/?smartRuleID={srID}**
            - **POST Vulnerabilities/ExportReport/**
            - **GET Vulnerabilities/{id}/VulnerabilityReferences/**
    - Added model string length validation. String values exceeding maximum length now properly return *400 Bad Request*.
        - AddressGroups
            - **POST AddressGroups/**
            - **PUT AddressGroups/{id}/**
                - **Name** (255)
        - Addresses
            - **POST AddressGroups/{id}/ (deprecated/superceded by POST AddressGroups/{id}/Addresses/)**
            - **POST AddressGroups/{id}/Addresses/**
            - **PUT Addresses/{id}/**
                - **Name** (255)
        - Assets
        - **POST Workgroups/{workgroupID}/Assets/**
        - **POST Workgroups/{workgroupName}/Assets/**
        - **PUT Assets/{id}/**
            - **AssetName** (128)
            - **AssetType** (64)
            - **DnsName** (255)
            - **DomainName** (64)
            - **IPAddress** (45)
            - **MacAddress** (128)
            - **OperatingSystem** (255)

- AttributeTypes
  - **POST AttributeTypes/**
    - **Name** (64)
- Attributes
  - **POST AttributeTypes/{attributeTypeID}/Attributes/**
    - **ShortName** (64)
    - **LongName** (64)
    - **Description** (255)
- Databases
  - **POST Assets/{id}/Databases/**
  - **PUT Databases/{id}/**
    - **InstanceName** (100)
    - **Version** (20)
- Directories
- **POST Workgroups/{id}/Directories/**
- **PUT Directories/{id}/**
  - **DomainName** (50)
  - **ForestName** (64)
  - **NetBiosName** (15)
  - **Description** (255)
  - **ContactEmail** (128)
- FunctionalAccounts
  - **POST FunctionalAccounts/**
  - **DomainName** (50)
  - **AccountName** (245)
  - **DisplayName** (100)
  - **Description** (1000)
  - **ElevationCommand** (80)
- ManagedAccounts
  - **POST ManagedSystems/{systemID}/ManagedAccounts/**
  - PUT ManagedAccounts/{id}/
  - **DomainName** (50)
  - **AccountName** (245)
  - **DistinguishedName** (1000)
  - **UserPrincipalName** (500)
  - **SAMAccountName** (20)

- **Description** (1024)
- **ReleaseNotificationEmail** (255)

- ManagedSystems
- **POST Assets/{assetId}/ManagedSystems/**
- **POST Databases/{databaseID}/ManagedSystems/**
- **POST Directories/{directoryID}/ManagedSystems/**
- **POST Workgroups/{id}/ManagedSystems/**
- **PUT ManagedSystems/{id}/**
  - **HostName** (50)
  - **DnsName** (255)
  - **IPAddress** (45)
  - **InstanceName** (100)
  - **ForestName** (64)
  - **OracleInternetDirectoryServiceName** (200)
  - **NetBiosName** (15)
  - **Description** (255)
  - **ContactEmail** (128)
- QuickRules
  - **POST QuickRules/**
  - **Category** (50)
  - **Title** (75)
- Requests
  - **POST Requests/**
  - **POST Aliases/{aliasId}/Requests/**
    - **TicketNumber** (20)
  - **PUT Requests/{id}/Checkin/**
  - **PUT Requests/{id}/Approve/**
  - **PUT Requests/{id}/Deny/**
  - **POST ManagedAccounts/{managedAccountID}/Requests/Terminate/**
  - **POST ManagedSystems/{managedSystemID}/Requests/Terminate/**
  - **POST Users/{userID}/Requests/Terminate/**
    - **Reason** (1000)
- RequestSets
  - **POST RequestSets/**
    - **TicketNumber** (20)

- Sessions
  - **POST Sessions/Admin/**
  - **HostName** (128)
  - **DomainName** (50)
  - **UserName** (200)
  - **Resolution** (50)
- SmartRules
  - **POST SmartRules/FilterAssetAttribute/**
    - **Category** (50)
    - **Title** (75)
- **POST SmartRules/FilterSingleAccount/** (deprecated)
  - **Title** (75)
- UserGroups
  - **POST UserGroups/**
    - **groupName** (200)
    - **description** (255)
    - **groupDistinguishedName** (500)
    - **hostName** (50)
    - **membershipAttribute** (255)
    - **accountAttribute** (255)
    - **forestName** (300)
    - **domainName** (250)
- Users
  - **POST Users/**
    - **UserName** (64)
    - **DomainName** (250)
    - **DistinguishedName** (255)
    - **FirstName** (64)
    - **LastName** (64)
    - **EmailAddress** (255)
- **POST UserGroups/{id}/Users/**
- **PUT Users/{id}/**
  - **UserName** (64)
  - **FirstName** (64)
  - **LastName** (64)
  - **EmailAddress** (255)

        - Workgroups
            - **POST Workgroups/**
                - **Name** (256)

- **Endpoint Privilege Management:**
    - Added support for Global Endpoint Privilege Management Policy Ordering.
    - Added auditing of changes to Endpoint Privilege Management policies (who made the change, which policy they changed, when the change was made).
    - Added support for future Endpoint Privilege Management Policy Locking functionality.
- **Password Safe:**
    - Additional Access Policy options: Require Reason and Ticket System global settings are now configurable at the Access Policy level.
    - Expanded API: added Team Passwords functionality.
    - Added a **Details and Attributes** section to both Managed Accounts and Managed Systems **Advanced Details** screens.
    - Added new platforms: macOS Secure Token, Cisco WLC, Fortinet Admin.
    - Endpoint Privilege Management for Mac is now supported as a change agent.
    - Added configurable option for background display in RDP sessions.
    - Made security enhancements.
- **Password Safe Cloud:**
    - Resource Broker is now updated when the Password Safe Cloud instance updates.
    - Resource Broker log files are now accessible from the Password Safe Cloud instance.

Issues Resolved:

- Resolved issue in which the **Name** field was editable when adding an asset to Password Safe.
- Resolved issue in which assets scanned using BeyondTrust Discovery v20 and non-functional credentials could be imported without asset names and appear as duplicates in the **Asset** grid.
- Resolved an issue with email validation. Now an email cannot contain extraneous characters after the domain, nor may it end in a number.
- Adjusted ChangeTime validation so that ChangeTime exactly matched the range **00:00** to **23:59**.
- For the API call **POST Auth/SignAppin/**:
    - Authentication failure messages are now valid JSON
    - Subsequent calls now use the current **Authorization** header to reauthenticate.
- **POST Auth/Signout/** can now be called to abandon unwanted MFA challenges.
- The **GET OperatingSystems/** call now properly returns a *401 Unauthorized* message on unauthorized calls.
- For the API call **GET ManagedAccounts/**:
    - Made performance enhancements.
    - Static (non–asset-based) Managed Systems are now properly returned for ISA role based access.
    - The **systemName** query parameter is no longer massaged to match a padded IP. The parameter value now matches the Managed System Name exactly.

- For the API call **GET Directories/**:
  - Made performance enhancements.
  - Resolved an intermittent *500 Internal Server Error* message that displayed under heavy system load.
- QuickRules, SmartRules
  - Made performance enhancements.
  - Resolved an intermittent *500 Internal Server Error* that displayed when the **DELETE QuickRules/{id}/** call was made under heavy system load.
- For the API calls **POST Users/**, **POST UserGroups/{id}/Users/**, and **PUT Users/{id}/**, the Audit record now properly sets the **Audit.Username** value.
- For the API call **POST Users/**, new LDAP users that belong only to BeyondInsight-type user groups can now properly authenticate after being created.
- For the API call **POST Users/**, new directory credentials are automatically enabled for group resolution when there is not a pre-existing directory credential entry for the directory.
- **Password Safe Cloud:**
  - Resolved issue in which omitted IP addresses in an Address Group were included in the scan target list.
  - Resolved issue in which users intermittently encountered a *Form is stale* error.
  - Resolved issue in which propagating password changes to IIS AppPools was problematic.
  - Resolved issue in which propagating password changes to Scheduled Tasks on Server 2016/2019 was problematic when the task RunAsUser was a domain account, the asset was on the domain, and the asset had a local user with the same username.
  - Resolved issue in which recurrent scheduled scans could run an extra 12 hours after their originally scheduled time.

Known Issues:

- **BeyondInsight:**
  - Smart Rules that are deactivated due to reliance on VMS-specific criteria and actions will not process until the criteria and actions are updated.
  - Some areas in Analytics and Reporting are translated while others are not.
  - New optional **Scan Progress** column on **Active/Completed Scans** grid may state *Scanning X of X* even though scan state is complete.
  - Printing a report from Analytics and Reporting using Internet Explorer 11 either suggests the user install SSRS (if cache is cleared) or does nothing (if cache is not cleared).
  - User Login: a newly added LDAP group does not immediately appear in LDAP servers section on login page.
  - Analytics and Reporting Report Styling Preview gives an error message before reloading successfully.
  - Omniworker log file may show log level changes repeatedly on clean installs.
- **Password Safe:**
  - OneClick: When set to *x* amount of max concurrent requests, the last one cannot make multiple sessions.
  - Custom Platform: snackbar error when setting Custom Platform inactive using German language.
  - Updating a schedule advances the enddate (if set) by a day (for each update).
  - Password Safe Cloud only: downloading a report to any format takes too long.
  - Password Safe Cloud only: status image indicator is missing from the Discovery report.

Notes:

- Direct upgrades to 21.1 are supported from BeyondInsight versions 6.9.x or later.
- Removed support for Vulnerability Smart Rules and related criteria/actions.
- 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: fb2c03b2cb7593405cbb8da20e9442f8.
- The SHA-1 signature is: c02e550d41d40699886dcdf2fd9de8a72f9d77c3.
- The SHA-256 signature is: e2c97378c045eea77ae9ea4fe91a8656e1a3ea327d7816f74115857477a517eb.