

BeyondInsight and Password Safe 21.2 Release Notes

July 27, 2021

New Features and Enhancements:

- Directory Queries and Directory Credentials Configuration screens now offer improved search, filtering, and pagination functionality.
- Added notification banner if older scanners are detected.
- Updated product so that End User License Agreement only displays to the first administrator login, and not for every new user.
- Asset Advanced Details UI now includes IIS App Pool data.
- Added menu bypass block for improved accessibility.
- Added support for configuring non-standard ports for MySQL, MS SQL, and SSH credentials.
- Enhanced purging options Configuration area to include scheduling recurring index and statistics maintenance.
- Added support to QRadar connector for LEEFFormatV2, which uses a unique identifier generated per event type.
- Removed Audit Viewer report and special permission related to it.
- Removed UI references to light writebacks.
- Removed Shares and Processes from Asset Advanced Details.
- Removed vulnerabilities mapping/export options from the BMC Remedy and ServiceNow Export connectors.
- Added support for downloading the EPM client certificate from the portal.
- **Analytics and Reporting**
 - Migrated remaining areas under Analytics and Reporting off AngularJS. Pivot Grid and Clarity/Cluster Analysis still use AngularJS.
- **API:**
 - Managed System Attributes Support

API Call	Description
GET ManagedSystems/{managedSystemID}/Attributes/	Returns a list of Attributes by ManagedSystem ID.
POST ManagedSystems/{managedSystemID}/Attributes/{attributeID}/	Assigns an Attribute to a ManagedSystem.
DELETE ManagedSystems/{managedSystemID}/Attributes/	Deletes all ManagedSystem Attributes by ManagedSystem ID.
DELETE ManagedSystems/{managedSystemID}/Attributes/{attributeID}/	Deletes a ManagedSystem Attribute by ManagedSystem ID and Attribute ID.

- POST RequestSets: Application support
 - Request body now includes **ApplicationID : int?**.
 - Response Body **Requests** list now includes **ApplicationID : int?**.
- POST ISASessions: Application support
 - Request body now includes **ApplicationID : int?**.

- User Group Smart Rule API

API Call	Description
GET UserGroups/{id}/SmartRules/[?accessLevel=1,3]	Returns a list of Smart Rules to which the given User Group ID has at least Read access.

- ManagedAccounts: Workgroup support

- Minor model version 3.3: New property added to request body.
 - **PUT ManagedAccounts/{id}?version=3.3**
 - **POST ManagedSystems/{systemID}/ManagedAccounts/?version=3.3**
 - **WorkgroupID : int?**: (default: null) ID of the assigned Workgroup.
- Latest version (currently 3.3) 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/**

- Platforms, Managed Systems: Application Host support

- **GET Platforms/**, **GET Platforms/{id}/**: Two new properties added to the response body
 - **ApplicationHostFlag : bool**: True if the Platform supports being used as an Application Host; otherwise false.
 - **RequiresApplicationHost : bool**: True if the platform requires a target Application Host; otherwise false.
- Managed System minor model version 3.2: Two new properties added to request body
 - **POST Assets/{id}/ManagedSystems/?version=3.2**
 - **POST Workgroups/{id}/ManagedSystems/?version=3.2**
 - **PUT ManagedSystems/{id}?version=3.2**
 - **ApplicationHostID : int?**: (default: null) Managed System ID of the target Application Host.
 - **IsApplicationHost : bool**: (default: false) True if the ManagedSystem can be used as an Application Host; otherwise false.
- Latest version (currently 3.2) 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/**
- Increase all System name sizes to 128 chars
 - **POST Workgroups/{id}/Directories/** (DomainName from 64 characters)
 - **PUT Directories/{id}/** (DomainName from 64 characters)
 - **POST Workgroups/{id}/ManagedSystems/** (HostName)
 - **PUT ManagedSystems/{id}/** (HostName from 50 characters)
 - **POST ManagedSystems/{id}/ManagedAccounts/** (DomainName from 50 characters)
- **POST Requests/{id}/Sessions/**, **POST ISASessions**: RemoteApp Mode Support
 - When **SessionType=AppFile** and the target is an RDP host, Application RemoteAppMode setting is now supported in the returned RDP file.
- Team Passwords: Credential multiple-user and group owner support
 - Credential minor model version 3.1: New properties added to request body
 - **POST TeamPasswords/Folders/{id}/Credentials/?version=3.1**
 - **PUT TeamPasswords/Credentials/{id}?version=3.1**
 - **OwnerType : string**: (default: User) The type of Credential owner.
 - **Group**: The owner is a User group.
 - **User**: The owner is one or more Users.
 - One of the following is required:
 - **OwnerId : int?**: (required when **OwnerType=Group**) ID of the Owner (either User ID or User Group ID).
 - **Owners : List<Owners>**: Zero owners when **OwnerType=Group**; One or more owners required when OwnerType=User.
 - **OwnerId : int**: User ID of the owner.
 - Latest version (currently 3.1) always returned in relevant response bodies
 - **POST TeamPasswords/Folders/{id}/Credentials/**
 - **PUT TeamPasswords/Credentials/{id}/**
 - **GET TeamPasswords/Credentials/{id}/**
 - **GET TeamPasswords/Folders/{id}/Credentials/**
 - **OwnerType : string**: The type of Credential owner
 - **Group**: The owner is a User group.
 - **User**: The owner is one or more Users.
 - **OwnerId : int**: ID of the Owner (User ID or User Group ID)



Note: If the credential is owned by multiple users, this will be the value of the first Owner in the **Owners list**.

- **Owners : List<Owners>**: Zero owners when **OwnerType=Group**; One or more when **OwnerType=User**.
 - **OwnerId** : int: User ID of the owner.
 - **Owner** : string: Owner name.
 - **Email**: string: Owner email address.
- **Password Safe:**
 - Added Custom Application Platforms to enable a script-based approach to managing accounts.
 - Team Password credentials now support multiple owners. It is also possible to grant ownership to the entire team.
 - New RemoteApp isolation mode for RDP Applications.
 - Password Safe User Portal enhancements.
 - Functional Accounts and Applications Configuration screens now offer improved search, filtering, and pagination functionality.
 - Managed Account and Managed System Advanced Details screens now offer **Edit** and **Delete** operations.
 - New configuration option to control SSL certificate validation.
 - Jira ticket system integration has been enhanced.
 - Added support for public key authentication on managed accounts using keys in OpenSSH format.
 - Added support for public key authentication on managed accounts using Ed25519 keys.
 - The ECM functionality, which provided integration between SRA and Password Safe, is now included with Password Safe.
- **Password Safe Cloud:**
 - The support area under configuration is no longer available in Password Safe Cloud.
 - Increased the timeout for operations between Password Safe Cloud and Resource Brokers from about 1 minute to 30 minutes.

Issues Resolved:

- Resolved an issue in Analytics and Reporting in which some areas in Analytics and Reporting were translated while others were not.
- Resolved an issue in Analytics and Reporting in which the Report Styling Preview gave an error message before reloading successfully.
- Resolved an issue with the BeyondInsight User Management user login in which a newly added LDAP group did not immediately appear in LDAP servers section on login page.
- Resolved an issue with BeyondInsight logging in which the Omniworker log file could show log level changes repeatedly on clean installs.
- Resolved an issue in BeyondInsight User Management in which attempting to assign the Team Passwords feature as a non-administrator caused an error.
- Resolved an issue in Password Safe Cloud Discovery Scanner in which the discovery tool improperly identified Windows targets with the SSH subsystem enabled as Linux targets.
- Resolved an exception which could occur when the SSH Key authorization file could not be found.
- Resolved an issue in Password Safe Cloud Discovery Scanner in which the discovery tool couldn't identify older Solaris systems due to a command which exceeded the command buffer size limit.

- Resolved an issue in Password Safe Cloud Discovery Scanner in which the discovery tool could have an exception in registry access during software enumeration when the local agent failed to deploy.
- Resolved an issue in Password Safe Cloud Discovery Scanner in which the discovery tool could have an exception when events were written to the database too quickly, resulting in a time stamp collision.
- Resolved an issue in Password Safe Cloud Discovery Scanner in which duplicate user names on a single SSH target could cause an exception.
- Resolved an issue in Password Safe Cloud Discovery Scanner in which the discovery tool could have a handle leak caused by failing to close the local scan session.
- **API:**
 - **GET Requests/?queue=app:** Approver-based request queue now properly returns Managed Accounts on static/standalone Managed Systems.
 - **POST Workgroups/{id}/Directories/, PUT Directories/{id}/:** Adjusted validation; required value checks now occur first, unique/duplicate name check now occurs second.
 - **PUT|DELETE Directories/{id}/:** Audit section now displays *PMM Managed System* rather than *Domain*.
 - **PUT Directories/{id}/:** When not given in the request body, DirectoryID no longer displays in the User Audits as having been changed to 0 (zero).
 - **POST ManagedSystems/{id}/ManagedAccounts/, PUT ManagedAccounts/{id}/:** Setting and changing Managed Account credential values are now audited (masked).

Known Issues:

- If a IIS web proxy is configured, a password test or change of AWS cloud managed passwords ignores the configured proxy. This is true for both forced and scheduled password changes.
- **BeyondInsight:**
 - Breadcrumbs in **Configuration > Secure Remote Access > Database Configuration** refer to *Privileged Remote Access* instead of *Secure Remote Access*. Workaround: none; this is just informational.
 - Changing a discovery credential description after changing the key might give an error. Workaround: Either change both the key and the description at the same time before saving, or navigate away from the credential, unlock with the new key, and then edit the description.
 - A user without full access to Analytics and Reporting configuration can still try to access that area, and if they do, it causes the browser to become unresponsive. Workaround: none; this is just informational.
 - Modifying the Scan Agent Event Processing settings in the UI does not take effect until the service is **RemManagerService** is restarted. Workaround: none; this is just informational.
 - Fresh software install gives conflicting next steps by prompting for a reboot and prompting to configure. Workaround: first reboot, and then open the Configuration Wizard if performing a fresh software install.
 - Choosing an alternate install location during an upgrade does not actually put anything in the alternate location. Workaround: none; alternate install locations don't apply to upgrades.
 - If you cancel deleting an asset, the toaster message notifies you there was an error deleting it. Workaround: none required; the asset was not deleted. This is a false alarm.
 - Scans that get into a completed but not processed state cannot be deleted or marked done. Workaround: none; this happens only occasionally. Those scans will eventually be purged.
 - Some pop-up menus may open upward even when there's no room to do so, causing things to be hard to see. Workaround: none, but the impact is minimal in all cases we have observed.
- **Password Safe:**
 - Using Internet Explorer, dynamic resizing of **Access Policies** grid does not always work properly. Workaround: Use a modern browser like Chrome, Firefox, or Edge.

- Using Internet Explorer, switching between Access Policies while **Schedule** grid is open decreases the size of the **Schedule** grid. Workaround: use a modern browser like Chrome, Firefox, or Edge.
- Using Internet Explorer, editing the steps of a large Custom Platform may cause the browser to become unresponsive. Workaround: use a modern browser like Chrome, Firefox, or Edge.
- Proxy settings are not properly applied when performing password change and tests for Amazon accounts. Workaround: contact Support for instructions.
- When editing an Access Policy Schedule that has a location restriction assigned, the value is not always properly displayed on the form although the setting is not lost. Workaround: no action needed, but can force the value to be displayed by toggling the **Enable Location Restriction** switch off and back on.
- Some advanced details are no longer written to debug log files when performing password test and change to custom platforms. Workaround: full details are shown in the user interface, and are available in the database.
- When editing an existing Oracle managed system that is configured to use an Oracle Internet Directory, the **Load** button does not properly refresh the list of available database service aliases.
- When editing an existing BMC Remedy Connector that has been configured as a Password Safe Ticketing system and has a **Ticket ID** specified, then a change made to other values than the **Ticket ID** field gets incorrectly cleared upon save. Workaround: After save, edit the connector and re-add the Ticket ID.
- It is not possible to perform a successful **Change** or **Test for a Custom Application Platform** from within the Custom Platforms editor. Workaround: use the Change/Test for a Managed Account.
- The **Owners** filter in Team Passwords does not update dynamically when a new user has been added as an owner. Workaround: refresh the page.
- When creating a new Application, the **Create** form is not properly showing the default state of the **Active** and **Launch Application in Remote App mode** flags. These are ON by default, but the form is showing them as OFF. Any changes made are properly applied. Subsequently editing the Application shows the proper values, as well as in the **Applications** grid.
- Password Safe Cloud:
 - When changing the password for a Functional Account from the **Managed System Advanced Details > Functional Account** screen, an error can occur if the changes are not applied before attempting to **Test** the password. Workaround: save changes prior to testing password.
 - **Asset > Advanced Details > Services** may show a local account with an extra backslash (`.\<accountname>`). This results in the inability for Password Safe to automatically update managed account service references.

Notes:

- Direct upgrades to 21.2 are supported from BeyondInsight versions 6.10.x 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: 58D21D39295A202218027B81D67F3402.
- The SHA-1 signature is: E993C81CBD3EE91708DEA8ABEB46F021C5D038F4.
- The SHA-256 signature is: 8C9A3E498C7FB97CA8D4AEB9305C4C3EAD4D9E407A635004C13F0E81AFA12488.