

BeyondInsight and Password Safe 22.1 Release Notes

January 31, 2022

New Features and Enhancements:

- Added support to create a new credential from the Scan Wizard.
- Added support to create a new credential from within directory User Management area.
- Added conditional logic to hide Cluster Analysis and Pivot Grid features if the AngularJS files are removed.
- Added User Audits endpoints to Public API.
- **Endpoint Privilege Management**
 - Now supports integration with EPM Web Policy Editor (WPE) and WPE Azure AD features. Additionally, BeyondInsight supports *policy locking*, which protects a policy that is actively being edited from being modified simultaneously by a different user, removing the possibility of creating conflicts when saving it.



Note: Neither BeyondInsight nor the appliance ship with WPE. WPE must be manually installed in order for WPE to be available in BeyondInsight. Inclusion of WPE within the appliance is planned for a future release.

• Password Safe

- Added Request ID column to the Approvals list, with search and filtering capabilities.
- New service account credential updates: Windows auto-logout, COM+, DCOM, SCOM identities, and Windows clustered services.
 - This feature requires the BeyondTrust Discovery Scanner v22.1.0.940 or higher.
 - The BeyondTrust Discovery Scanner requires .NET Framework v4.7.2 to exist on target endpoints when enumerating service account credentials.
- Updated SRA integration (Endpoint Credential Manager) to version 1.6.0.1135.
- Security enhancements.

• API

◦ New Features

- User Audits support.

API Call	Description
GET UserAudits/	Returns UserAudits descending by CreateDate
GET UserAudits/{id}/UserAuditDetails/	Returns UserAuditDetails by UserAuditID

- **Enhancements**

- **ManagedAccounts: Propagation Target flag support.**
 - Minor model version 3.4 - New properties added to request body
 - **PUT ManagedAccounts/{id}/?version=3.4**
 - **POST ManagedSystems/{systemID}/ManagedAccounts/?version=3.4**
 - **ChangeWindowsAutoLogonFlag: bool** - (default: false) True if Windows Auto Logon should be updated with the new password after a password change, otherwise false.
 - **ChangeComPlusFlag: bool** - (default: false) True if COM+ Apps should be updated with the new password after a password change, otherwise false.
 - **ChangeDComFlag: bool** - (default: false) True if DCOM Apps should be updated with the new password after a password change, otherwise false.
 - **ChangeSComFlag: bool** - (default: false) True if SCOM Identities should be updated with the new password after a password change, otherwise false.
 - Latest version (current 3.4) always returns 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/**

Issues Resolved:

- New managed systems are now immediately available to users granted the **All Managed Systems** Smart Rule.
 - **POST Assets/{id}/ManagedSystems/**
 - **POST Databases/{id}/ManagedSystems/**
 - **POST Workgroups/{id}/ManagedSystems/**
 - **POST Workgroups/{id}/Directories/**
- **GET|POST|DELETE FunctionalAccounts:** Functional Account data access and auditing is now consistent across the product.
- Resolved BeyondInsight issue in which an error was displayed if you filtered the Clarity grid with text containing a colon (:).
- Resolved issue which prevented successfully uploading a Password Safe plugin when FIPS was enabled.
- Resolved Password Safe issue in which the table cell in the One-Click Request interface scrolled unexpectedly.
- Resolved several issues with SCIM integration.
- Resolved issue with SAML login with Name claim having a format of **user@domain.com**.
- Resolved Password Safe Cloud issue in which URLs were improperly specified in the allow-list.
- Fixed Password Safe, Approval, and Deny links in email templates.
- Resolved issue affecting TOTP with DirectConnect.
- Resolved issue in which DirectConnect was unable to check out non-domain accounts that contained an at symbol (@).

Known Issues:

- Directory Queries grid filter by dropdown does not activate when selected within Chrome or Edge. Workaround: Try Firefox or Internet Explorer or manually scroll/page the grid to find what you are looking for.
- When creating a new SAML identity provider, you can get sometimes get into a state that shows an error snackbar message. Workaround: Refresh the screen to view the SAML identity provider that exists/was created, and edit to resolve any issues.
- If you make changes to the fields in the Analytics & Reporting configuration wizard and that causes the deployment process to fail, those changed fields are not discarded even when you choose to cancel out of the wizard and discard your changes. Workaround: Either don't make any changes and use the data that is pre-populated in an upgrade scenario, make sure the details of what you are entering is correct, or be sure to double-check all fields if you are having trouble deploying the Analytics & Reporting updates.

Notes:

- Direct upgrades to 22.1 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: 405d1fb95f5336fe25e5e730ee0f2197
- The SHA-1 signature is: 1622b8937db96d326ffbcf79aec5e7a9e748a256
- The SHA-256 signature is: 1cb35ae19fe47027571aa05981b6c80fa70aab3199c06276d29275336be1b1b2