BeyondInsight and Password Safe 21.3 Release Notes

December 2, 2021

New Features and Enhancements:

- Added support for additional two-factor authentication options via time-based one-time password (TOTP).
- Added support for managing Azure Active Directory users and groups in BeyondInsight.
- Added support for Domain Management to support mapping primary and fallback credentials or managed accounts to specific domains.
- Removed Kenna connector (cleanup related to vulnerability management functionality).
- ServiceNow Ticket System connector now offers option to use SamAccountName, UPN, or email address as identifier.
- Added option to use local scan service for detailed or advanced discovery scans.
- Restored the **IP Address** column in the **Assets** grid.
- Reduced the set of discovery scan ports (cleanup related to vulnerability management functionality).
- Improved scan status display to more accurately reflect status.
- Migrated Clarity user interface off AngularJS technology.
- Added display of patch version number to **About** page (when applicable).
- Widened the audience of legacy scanner warning banner to any user having Scan Management permission.
- Extended legacy scanner end of life in warning banner from December 31, 2021 to March 31, 2022.
- Added support for multiple SAML identity providers in the configuration user interface.
- Added numerous improvements for a more accessible interface.
- Added SAML deprovisioning support for local users.
- Action button is now locked and always visible in grids.
- **Discovery Scanner**
    - Added the identification of user privilege level for Mac/OSX.
    - Added enumeration of domain users who have logged into the target.
- **Analytics and Reporting**
    - Removed **Deprecated Reports** folder and associated reports.
    - Removed **Docker Images by Host** report.
    - Removed **Vulnerabilities VMWare Security Hardening** report.
- **Password Safe**
    - Added modular platform support via a plugin architecture SDK.
    - Improved Secure Remote Access integration.
    - Added support for Oracle database clusters.
    - New setting for domain account checkout concurrency behavior.
    - Auto-managed functional accounts now trigger credential rotation upon creation.
    - Added ability to create new functional account from Smart Rule editor and create managed system.

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- **Password Safe Cloud**
  - Added support for routing RADIUS traffic over Resource Broker.
  - Added support for routing connector traffic over Resource Broker for the following connectors:
    - ArcSight Event Forwarder
    - Exabeam Event Forwarder
    - FireEyeTap Event Forwarder
    - IBM QRadar Event Forwarder
    - LogRhythm Event Forwarder
    - McAfee syslog Event Forwarder
    - NetIQ Sentinel Event Forwarder
    - Syslog Event Forwarder
  - Improved visibility of Resource Broker version in user interface and added **Upgrade** action.
  - Removed non-applicable EPM-related Smart Rule filters and actions.
  - Resource Broker installer now shows list of DNS hosts for firewall allow list.
  - Centralized AD and LDAP certificate enforcement options in **Configuration > Site Settings**, and updated defaults.
- **API**
  - **New Features**
    - Most recently used support

API Call	Description
GET ManagedAccounts/?type=recent	Returns most recently used accounts

    - Improved managed system filtering

API Call	Description
GET ManagedAccounts/[?systemID={systemID}]	Add support for filtering requestable managed accounts by managed system ID
GET ManagedAccounts/?systemName={systemName}	Improved performance

  - **Enhancements**
    - Managed account request: prevent requests when no managed account credential is stored
      - **POST Requests**
      - **POST ISARequests**
    - Managed account provisioning: improved performance and auditing
      - **PUT ManagedAccounts/{id}/**
      - **DELETE ManagedAccounts/{id}/**
      - **POST ManagedSystems/{id}/ManagedAccounts/**
      - **DELETE ManagedSystems/{id}/ManagedAccounts/**

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- Improved secure remote access integration

Issues Resolved:

- Resolved an issue with BeyondInsightin which canceling deletion of an asset resulted in a toaster message notifying you of an error with the deletion.
- Resolved an issue with BeyondInsightin which changing a discovery credential description after changing the key sometimes displayed an error.
- Resolved an issue with BeyondInsightin which breadcrumbs in **Configuration > Secure Remote Access > Database Configuration** referred to **Privileged Remote Access** instead of **Secure Remote Access**.
- Resolved an issue with BeyondInsight andPassword Safe in which some pop-ups may open upward even when there's no room to do so, causing issues with display.
- Resolved an issue in which SAML users can get added to groups incorrectly when that group is in the SAML claim.
- Resolved an issue with SAML logins not respecting the **Use Only Bind Creds tied to Groups** option for new users.
- Resolved an issue in which adding an AD user manually via **User Management** gets slower as more accounts exist.
- Resolved an issue with AD logins and queries not respecting LDAPS settings.
- Resolved an issue with VMWare scan target collector connector saving credentials incorrectly causing scans to fail.
- Resolved an issue with SAML logins failing after an existing user's username is changed in AD.
- Resolved an issue with the daily job failing if a managed database system is deleted.
- Resolved an issue with AD authentication method not using a user's preferred domain controller when configured.
- Resolved an issue with ticket date validation not working correctly.
- Resolved an issue in which a managed account Smart Rule search criteria containing the word *alter* does not work.
- Resolved an issue by adding missing Cloud Provider endpoints to the database.
- Resolved an issue with the Create Managed System API in which a numeric system name with more than 6 characters was truncated to 3 characters.
- Resolved an issue in which workgroups could not be deleted because of associated IP addresses in the dbo.IP table.
- Resolved a performance issue with the Password Safe Cloud report viewer which caused issues loading some reports.
- Resolved an issue with EPM policies in which adding an application to an application group should allow the child processing matching option to be configurable.
- Resolved an issue in which scan jobs could get stuck as Active/Complete if a scan restarted midway.
- Resolved an issue in which the Analytics and Reporting daily job could fail on table size limit when using password cache or a high volume of requests.
- Resolved an issue with SCIM API not accepting the **emails** attribute for users.
- Resolved an issue in which app pools, scheduled tasks, and services could fail to rotate passwords due to name format.
- Resolved an issue in which managed bind accounts used the system setting for SSL and not the managed directory setting.
- Resolved an issue in which the ServiceNow Scan Target Collector only imported one target when there was no **sys_id** field.
- Resolved an issue in which **Open Discovery Report** from the scans grid only worked on scans from the current week.
- Resolved an issue in which **memberUID** could not be selected as the membership attribute for LDAP groups.
- Resolved an issue in which the Endpoint Privilege Management plugin configuration could not be accessed without a Password Safe license.
- Resolved an issue with retrieving the dashboard after permissions change.
- Resolved an issue with password history showing HTTP-encoded special characters.
- Resolved an issue in which stored procedure PMMManagedAccount_FindByVarious failed, due to rowsize exceeding 8060 bytes.

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- Resolved an issue in which Remote App Mode did not launch a second session.
- Resolved an issue in which PWS Activty Report was slow when run by an auditor.
- Resolved an issue in which email subscriptions did not include the report.
- Resolved an issue in which using **Alternate Directory Attribute** for RADIUS on LDAP users did not work.
- Resolved an issue in which the **Asset > Database > Oracle** port number could not be edited when a duplicate already existed.
- Resolved an issue with Omni worker running as a 32bit process.
- Resolved an issue in which Identity Service caused *Unauthorized* errors when the configured host name pointed to a load balancer.
- Resolved an issue in which asset matching could have unexpected behavior.
- Resolved an issue in which users with the **ActiveSessionReviewer** role were unable to cancel sessions for dedicated accounts.
- Resolved an issue with highlight text buttons on the SSH launch page no longer working.
- Resolved an issue in which users with a NULL value for their first name did not get synced to Analytics and Reporting.
- Resolved an issue in which a Smart Rule scan shows all agents instead of only agents selected in the Smart Rule.
- Resolved an issue in which Custom Application Platform specific tags that start with *ah* did not populate.
- Resolved an issue with HTML tags appearing as text in the **Managed Account > Public Key** window.
- Resolved an issue with **Add Dedicated Accounts to Quick Rules**.
- Resolved an issue in which editing Quick Groups created in version 6.9 or earlier removed the contents of the Quick Group.
- Password Safe Cloud only: Resolved an issue in which Password Update Schedule Report returned no data.
- Resolved an issue in which **Entitlement by User** report did not filter the linked asset name correctly.
- Resolved an issue in which selecting **Team Password** logged the user out.
- Resolved an issue in which email validation failed if a capital letter was directly before the @ symbol.
- Resolved an issue in which **Directory Queries - LDAP** test results did not show the **Name Attribute** in the **Name** column of the results.
- Resolved an issue in which address group file import treated integers as IP addresses.
- Resolved an issue in which SCIM filter failed if using dot access on integer with boundaries or complex expressions.
- Resolved an issue in which you could not add accounts via the WebConsole UI when Quick Rules were created via the API.
- Resolved an issue with last login date in last **Account Last Login** report.
- Resolved an issue with *Getpagecomponents()* errors appearing for cloud deployments.
- Resolved an issue in which MongoDB defaulted to the admin database even when an instance was set.
- Resolved an issue in which Smart Rules using the **Set Attribute** action could load incorrectly in the UI.
- Resolved an issue with deadlocks occurring during Smart Rule processing.
- Resolved an issue in which attempting to view nested OUs in a directory query with LDAPS enabled failed.
- Resolved an issue with the Analytics and Reporting Subscription month selector functionality.
- **Discovery Scanner**
    - Resolved an issue by removing trailing nulls from event data which caused a failure parsing in BeyondInsight.
    - Resolved an issue by removing duplicate users from the group members list which could cause an exception.
    - Resolved an issue in which credential reporting for local scans caused the BeyondInsight Discovery Tool to incorrectly report the target as unacquired.
    - Resolved an issue with parsing output of the sudo permissions command to verify the data is not an error message. This was causing an exception.

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- **API**
  - **POST Users**: no longer sporadically fails under heavy load.
  - **DELETE Directories/{id}/**: no longer sporadically fails under heavy load.
  - **DELETE Attributes/{id}/**: now allows deleting attributes that are referenced by assets.
  - **PUT ManagedAccounts/{id}/Credentials/**: invalid SSH key/passphrase combination now returns *400 Bad Request*.
  - **POST QuickRules**: Quick Rules created (and previously created) via the Public API are now compatible with the Smart Rules Editor.

Known Issues:

- **BeyondInsight:**
  - Changing attribute type after selecting an attribute when configuring the **Set Attributes on Account** action on a managed account Smart Rule may cause an error to appear. Workaround: remove the action and re-add it, selecting the appropriate attribute type first, before setting the desired attribute.
  - **Last Login** and **Password Expiry** details of domain users in **Asset Details View** may be incorrect in some cases. Workaround: none. Discovery Scanner does not support utilizing LDAP to return the details for a domain user at this time.
  - Using BeyondInsight Configuration Tool, clicking **Apply** may cause warning messages in the log files if items in the cache are in use when the cache deletion occurs. Workaround: none; this is informational.
  - Some details on the BT Analyzer report may be cut off when viewing via the **View Analysis** button on the **About** page. Workaround: download the analysis and open the report directly from the Analyzer output folder.
  - Using **Analytics and Reporting > Report Styling**, when uploading a report logo banner image, a message indicates the file failed to upload, but the file is in fact uploaded when the style is saved. Workaround: ignore the error; the file is uploaded and will be saved when you save changes in the **Report Styling** area.
  - Scheduling SQL Index Maintenance to **Weekly** causes an error in the Omniworker. Workaround: change the SQL Index Maintenance to a **Daily** schedule and restart the Omniworker service to restore Index Maintenance operations. Other Omniworker functions are not affected.
  - NoSQL U-Series 3.3.1 Configuration Wizard may encounter an *Unable to decrypt credential* error on new setups. Workaround: if you encounter this issue, after configuration, use the Maintenance application to import the crypto key from the Appliance that has the Management Console role enabled. Then use the Maintenance application to update the SMTP credentials if they need to be changed. If these were already set from the Appliance that created the database, then it does not need to be configured again, as that data is already stored in the database.
  - Scanned assets that are virtual machines may not be identified as such when scanned by Discovery Scanner. Workaround: None known, the discovery scans do not bring back a MAC Address, which is what BeyondInsight uses to decide if it's a virtual machine. Other smart rule filters that depend upon MAC Address may also not work if using a disvcovery scanner.
  - **User Mapping** dropdown within the SAML configuration, if it opens towards the top of the screen, may not allow the user to click some options. Workaround: move the cursor toward the right side of the dropdown or scroll to the bottom of the panel before opening the dropdown to encourage it to open toward the bottom of the screen. If these options do not work, use the **Search** function to narrow down the list to just the item you want to select, and then click it.
  - Erroneous **Change Password** link appears when editing an Azure Active Directory credential. Workaround: none; this is safe to ignore. Rather than a **Password** field, an Azure AD credential uses a Client Secret, and that field is shown if the user clicks the **Change Client Secret** link.
  - **Clarity Events Grid** filter fails when a colon symbol (:) is included in the filter text. Workaround: avoid using a colon symbol in the grid filter in this area of the product. Other grids outside the Clarity area are not affected. If you get into this situation, you may have to clear your browser cache to restore this grid's functionality.
  - Using the same credential within domain management if it was also used to onboard the AD group negates the fallback option for login. Workaround: use different credentials for domain management and group onboarding or use SQL script to update **OptionType**, **DefaultValue**, and **UserSetting** to **True** where **OptionTypeID = 375**.

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- When both primary and fallback credentials for a domain are incorrect, an unmapped but correct directory credential could sometimes fail to allow login. Workaround: fix broken credentials and retry or use SQL script to update **OptionType**, **DefaultValue**, and **UserSetting** to **True** where **OptionTypeID = 375**.
- The error *Unable to find fallback working credentials for domain* may be displayed when you are trying to import a user, even when directory credentials are correct and tested successfully. Workaround: make sure the directory credential username is in the format **user@domain.suffix** or use the domain name instead of DC IP address in the **Domain** field during directory credential creation.
- Unable to import users/search for Active Directory group when directory credential username is just name without the @domain suffix. Workaround: ensure DNS is set up correctly and use the domain name rather than DC IP address in the **Domain** field during directory credential creation.
- Directory credential of Azure Active Directory type only supports up to 100 characters for the **Client Secret** field. Workaround: none. If the client secret is over 100 characters, it cannot be entered using this UI. Most client secrets are shorter so we don't expect this to come up. In a future release, we will align the character limit with that in Azure, of 256.
- When using Internet Explorer, the **Asset Advanced Details > Database** screen initially does not render. Workaround: refresh the page or avoid the issue by using a modern browser such as Chrome, Firefox, or Edge.
- When using Internet Explorer, the Clarity **Triggers Help** tooltip is not formatted properly. Workaround: use a modern browser, such as Chrome, Firefox, or Edge.
- When using Internet Explorer, Report Navigation Controls do not work. Workaround: export the report to PDF format to view subsequent pages or avoid the issue by using a modern browser, such as Chrome, Firefox, or Edge.

- **Password Safe:**
  - If an attempt is made to launch an RDP Session with a managed account which has no credential, an error will occur. Workaround: assign a credential or turn on auto-management.
  - Using Discovery Scanner, in rare occasions a scan may abort if there are multiple scans which are running simultaneously. Workaround: schedule scans to run so they don't overlap.
  - Using Discovery Scanner, it may not be possible to resolve a hostname to an IP address when scanning Oracle database clusters. Workaround: ensure DNS is properly configured or manually set the IP Address on the asset.
  - Using Smart Rules, the user interface allows adding multiple **Manage Assets using Password Safe** actions, which is not a proper configuration. Workaround: add only a single action of this type to a Smart Rule.
  - When navigating away from the **Configuration > Oracle Internet Directories** screen where there are unsaved changes, the **Discard Changes** prompt is not displayed. Workaround: ensure all changes are saved prior to navigation.

Notes:

- Direct upgrades to 21.3 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: 6d1f306c628b7f0710f177407001e74b
- The SHA-1 signature is: 8dcbe508da2a329d7e52e540d4288c4928b3e5a0
- The SHA-256 signature is: 1d341c0a2db59a978132f1cb240c4eba0c9a684e1286e6d9961d0b6cb985b46d

©2003-2021 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.