Password Safe 22.3

BeyondInsight 22.3

What's New Documentation

Release Date – October 6, 2022

BeyondTrust Password Safe combines privileged password and session management capabilities to discover, manage, and audit all privileged credential activity. Password Safe enables control of privileged user accounts, applications, SSH keys, cloud admin accounts, RPA, and more, with a searchable audit trail for compliance and forensics.

With Password Safe, you can:

- Scan, identify, and profile all assets for automated onboarding, ensuring no credentials are left unmanaged.
- Monitor and record live sessions in real-time and pause or terminate suspicious sessions.
- Use adaptive access control for automated evaluation of just-in-time context for authorization access requests.
- Achieve complete control and accountability over privileged accounts.

Please see the release notes for additional details on these important enhancements.

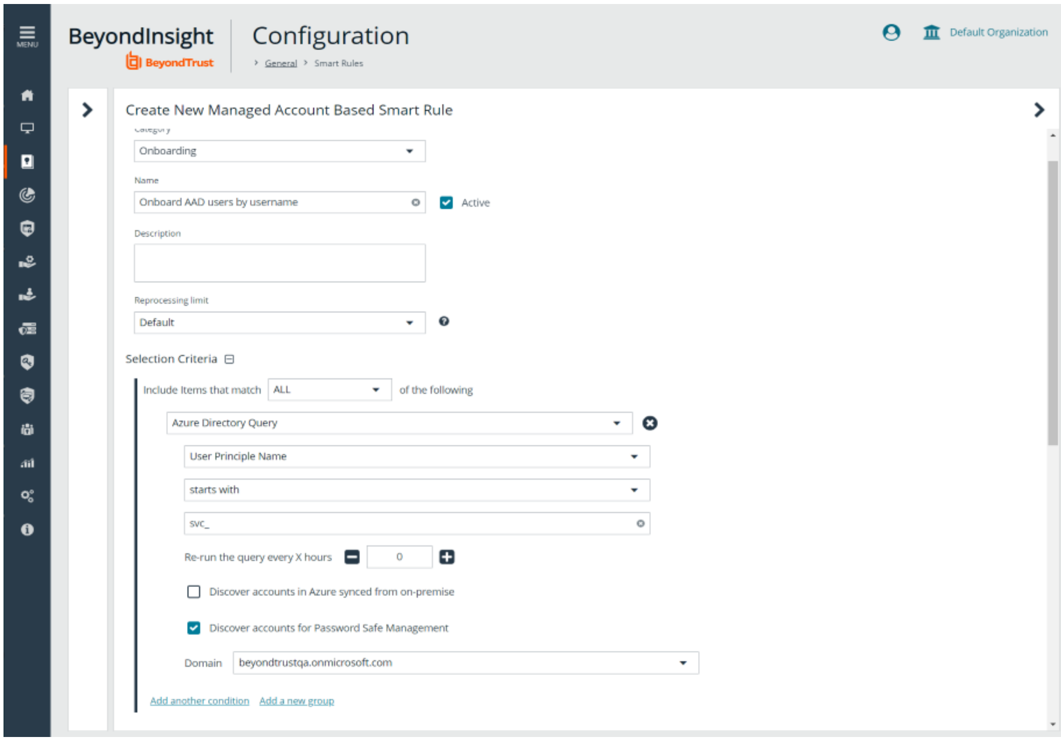
Release Highlights – Password Safe 22.3

Managed Azure Active Directory

As organizations continue to adopt Azure Active Directory (AAD) as an identity provider (IdP) source of truth, Password Safe must be able to recognize and process these identities for credential management tasks. In addition, Password Safe needs to be able to manage credentials of the local accounts residing on the AAD endpoints.

In 22.3, BeyondTrust has expanded the ability to perform credential discovery and management with the Managed AAD platform within Password Safe. Your admins will now be able to automate the onboarding of privileged accounts within your AAD with the automation built into Smart Rules, thereby allowing Password Safe to manage Azure AD credentials. Customers on the cloud deployment of Password Safe have the ability to perform RDP sessions leveraging AAD credentials to an Azure-joined virtual machine (VM).

With this new feature, BeyondTrust continues to evolve our solutions to meet customers' credential management challenges and continually adapt to the way they work, helping to reduce risk and improve their security postures.



Create New Managed Account Based Smart Rule

Category: Onboarding

Name: Onboard AAD users by username ☑ Active

Description:

Reprocessing limit: Default

Selection Criteria

Include Items that match ALL of the following

Azure Directory Query

User Principle Name

starts with

svc_

Re-run the query every X hours 0

□ Discover accounts in Azure synced from on-premise

☑ Discover accounts for Password Safe Management

Domain: beyondtrustqa.onmicrosoft.com

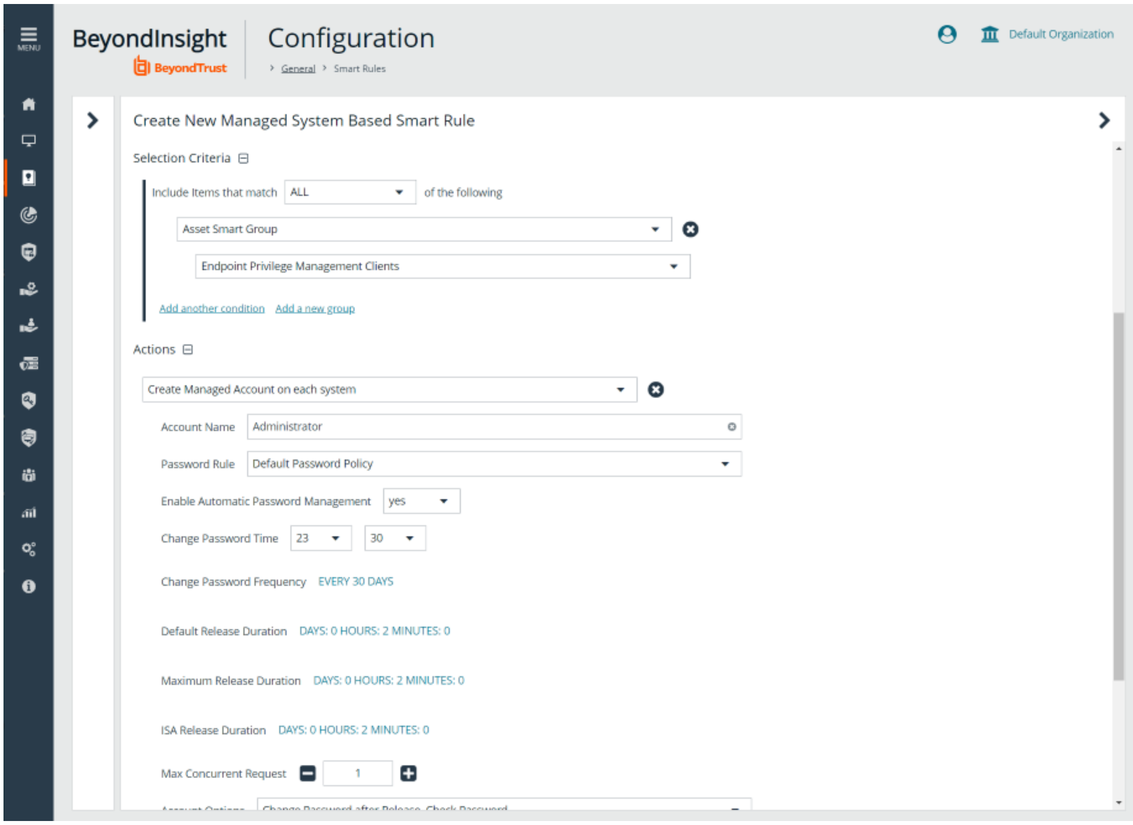
Figure 1 – Create Smart Rule for onboarding AAD users by username

Known Account Onboarding

Integration between cloud deployments of Password Safe and Privilege Management for Win & Mac provides customers the ability to connect disparate or disconnected systems into Password Safe. Through this integration and by leveraging the Privilege Management for Win & Mac agent, customers can rotate local passwords in disconnected systems.

However, earlier versions of Password Safe did not have the ability to perform scanning on the remote-disconnected endpoints, which presented challenges to discover all local accounts. This resulted in a lack of visibility into the local administrator accounts, prompting the creation of cumbersome manual entries or complex scanning rules.

In 22.3, Password Safe can now onboard and provide credential rotation for known administrator accounts without the need for full discovery or other onboarding workflows. This enhancement significantly simplifies local account discovery and onboarding, helping customers secure the growing number of disconnected or remote systems.



Create New Managed System Based Smart Rule

Selection Criteria ⊟

Include Items that match: ALL of the following

Asset Smart Group

Endpoint Privilege Management Clients

Add another condition   Add a new group

Actions ⊟

Create Managed Account on each system

Account Name: Administrator

Password Rule: Default Password Policy

Enable Automatic Password Management: yes

Change Password Time: 23 30

Change Password Frequency: EVERY 30 DAYS

Default Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

Maximum Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

ISA Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

Max Concurrent Request: 1

Account Options: Change Password after Release, Check Password

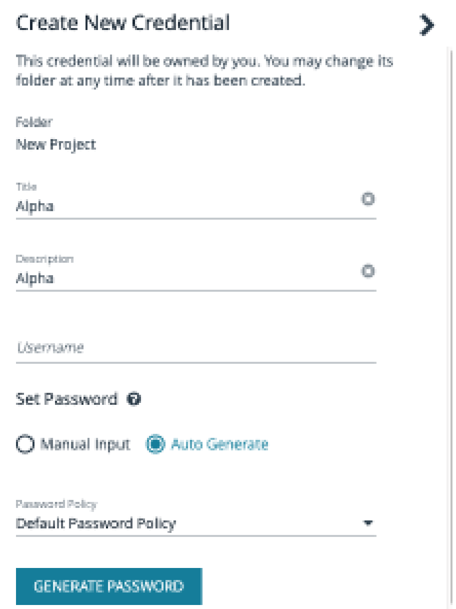
Figure 2 – Create Smart Rule for onboarding local accounts

Team Passwords: Generate Passwords

In prior versions, creating new credentials within Team Passwords, administrators were required to manually enter a password, which, depending on complexity requirements, could be time-consuming and risky.

In 22.3, Password Safe simplifies the process of creating Team Password credentials by allowing users to leverage password policies within Password Safe to generate a password. Users can leverage the Generate Password button multiple times, as needed. This feature also allows users to randomly generate a new password for an existing credential within Team Passwords.

This enhancement to the Team Passwords capability was requested by multiple customers through our Ideas Portal. We continue to listen to our customers and improve the usability of our solutions in ways that enhance their security and productivity.



Create New Credential

This credential will be owned by you. You may change its folder at any time after it has been created.

Folder
New Project

Title
Alpha

Description
Alpha

Username

Set Password

○ Manual Input ● Auto Generate

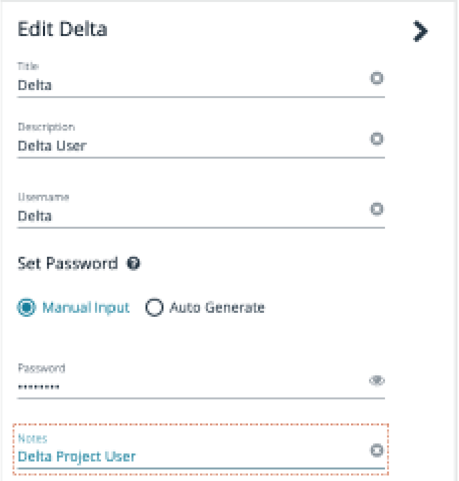
Password Policy
Default Password Policy

Figure 3 – Auto Generate Password for Teams Passwords

Team Passwords: Additional Notes Field

Team Password users leverage many shared passwords to various websites, applications, etc., which can create confusion as to which password is the correct one needed to access the website, application, etc. Sometimes, Team Passwords users exit the tool to find out more details as to which password is needed.

In 22.3, Team Passwords now provides an additional section called "Notes" in the credential details screen, as well as a new "Notes" column. This allows our customers to add additional details about the credential, minimizing confusion and keeping them from exiting the tool.



Edit Delta

Title
Delta

Description
Delta User

Username
Delta

Set Password

● Manual Input ○ Auto Generate

Password
••••••••

Notes
Delta Project User

Figure 4 – New Notes Field in Team Passwords

Enhancement: Email Notifications

To ensure visibility of potential issues, Password Safe automatically sends email notifications to all users who are administrators of Managed Domains/Assets. At times, this results in excessive outbound emails and unnecessary notifications to system admins who may not be asset owners.

In 22.3, Password Safe now provides a global setting to configure the automatic notification to administrators if a failed password rotation occurs. This new setting reduces the amount of outbound emails Password Safe sends, eliminating unnecessary tasks that could reduce productivity.

Enhancement: Session Auto-Reconnect

Previously, if a session was disconnected for any reason, there is no automated attempt to reconnect, even if the disconnect was brief due to poor network connections. These interruptions forced users to establish a new session.

In 22.3, Password Safe introduces RDP reconnect capabilities for sessions that drop due to poor network connectivity. Password Safe reconnect attempts are limited to the connection between the proxy and the endpoint; connections between the user and the proxy are not affected.

By introducing this session auto-reconnect feature, Password Safe helps teams be more productive, saving valuable time by re-establishing ongoing sessions.

Release Highlights – BeyondInsight 22.3

Enhancement: Optional Scan Credential Key

In previous BeyondInsight versions, the user was required to enter a key when managing (creating, editing, or selecting) a scan credential. With BeyondInsight 22.3 the use of the scan credential key is now optional. The new option can be accessed in System - Site options > Global Discovery Credential Keys. This enhancement further simplifies the discovery process and offers customers additional customization options.

Enhancement: Support Multiple Ports per Scan Credential

Currently, for scan credentials whose type allows for the specification of a non-standard port, only one port per credential can be entered. If the same credential can be used across different instances running on different ports, the user is forced to create the same credential multiple times, each with its own unique port.

With BeyondInsight 22.3, a scan credential can now accept multiple ports, significantly simplifying the scanning process.

Enhancement: Support Amazon Relational Database Service (RDS)

For appliance-based deployments of BeyondInsight, customers can now leverage BI 22.3 and the U-Series 4.0 appliance to use Amazon RDS as an external database. The U-Series Appliance 4.0 is slated to be released later in 2022.

About BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats, while creating a superior user experience and operational efficiencies. With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.