# Password Safe 22.4

# BeyondInsight 22.4

What's New Documentation

Release Date – December 15, 2022

BeyondTrust Password Safe enables complete visibility and control of privileged credentials and secrets, in a single solution. Password Safe provides automated discovery and onboarding, management, auditing, and monitoring for any privileged credential across on-prem and cloud environments. The solution simplifies audit and compliance, giving enterprises visibility of privileged activity across the network. Password Safe empowers DevOps teams with the confidence to develop and deploy cloud solutions and secure secrets at the speed of DevOps.

With Password Safe, you can:

- Achieve complete visibility and control over privileged accounts.
- Scan, identify, and profile all assets for automated onboarding, ensuring no credentials are left unmanaged.
- Store secrets used for DevOps, including certificates, API keys, tokens, etc., in a secure and audited vault.
- 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.

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

## Release Highlights – Password Safe 22.4

### Secrets Safe now included in Password Safe

Today's enterprises must implement critical security fundamentals when developing and maintaining cloud applications. BeyondTrust continues to provide solutions that adapt to the highly dynamic, automated, and scalable workloads found in these modern environments. With Password Safe 22.4, BeyondTrust helps your teams to improve the security of secrets used in cloud applications and automated processes with the release of a secrets safe built into Password Safe.

The new Secrets Safe satisfies requirements for both traditional PAM needs and for DevOps secrets security in cloud deployments, without having to buy multiple PAM and secrets tools. BeyondTrust has enhanced Team Passwords with new secrets management capabilities with the new Secrets Safe, which provides these capabilities within Team Passwords.

The new Secrets Safe provides the ability to upload files such as certificates, API keys, tokens, etc., in a secure and audited vault. Users easily manage secrets using the new Graphical User Interface (GUI), leveraging complete lifecycle management of secrets in Password Safe. In addition, BeyondInsight 22.4 provides full reporting on secrets management, further helping organizations to improve their security posture and transparency.

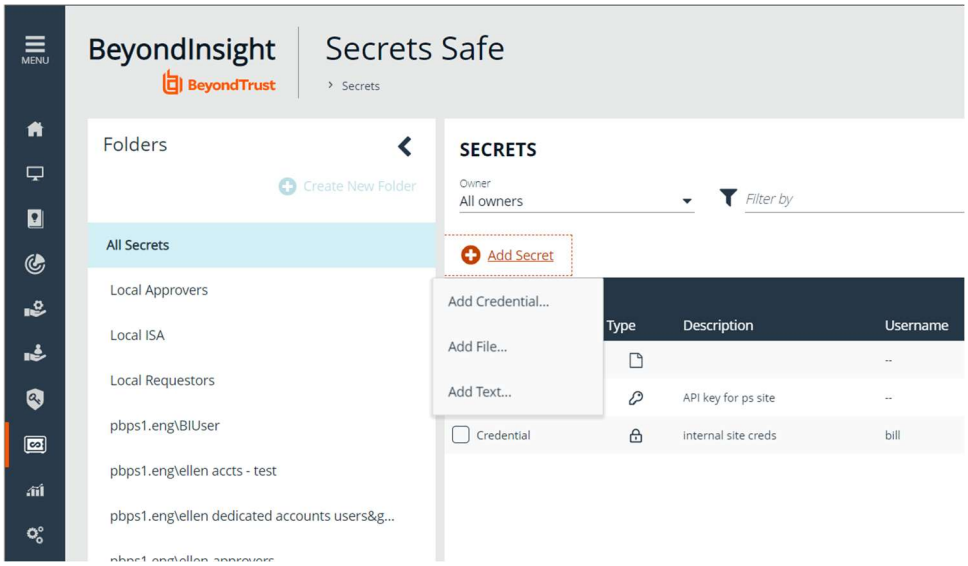


*Figure 1 – New Secrets Safe vault is integrated with Password Safe.*

## Kubernetes Sidecar

Application developers must secure their use of sensitive data without stopping to write API code or other access methods for storing and retrieving secrets, or for managing the storage and the synchronization of secrets. The new Kubernetes sidecar in 22.4 provides managed secrets to containers deployed to Kubernetes. A sidecar helps developers share resources including network interfaces and pod storage when two or more containers are running in a pod.

Customers using Kubernetes deployments will benefit from BeyondTrust's secrets management capabilities with simplified logic for connecting to and retrieving secrets from Secrets Safe. This empowers developers to use easy, built-in automation and helps to eliminate the practice of using plain text secrets in code.

The new Secrets Safe init container helps to accelerate development by abstracting away the specifics of retrieving secrets from the application container. This allows app developers to simplify and streamline their services without the need to write direct integrations, or to rely on insecure methods of accessing secrets.

Applications are kept up to date with the latest secrets because the secrets-agent container in Secrets Safe (sidecar) retrieves secrets on a defined interval. The container is available through the Docker Hub free library and handles all logic for connecting to and retrieving secrets from Secrets Safe.

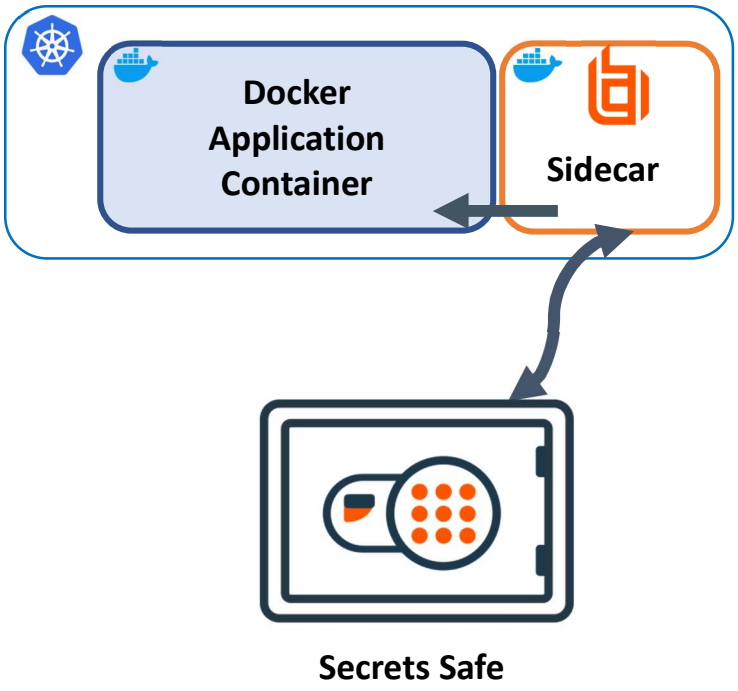


*Figure 2 – Kubernetes sidecar provides managed secrets to containers deployed to Kubernetes.*

## Improved Local Account Discovery

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

In 22.4, Password Safe in conjunction with the 22.9 EPM agent, can now discover, onboard, and provide credential rotation for administrator accounts without requiring Microsoft Local Administrator Password Solution (LAPS). This enhancement significantly simplifies local account discovery and onboarding, helping customers to secure the growing number of disconnected or remote systems.

# Release Highlights – BeyondInsight 22.4

## Two New Entitlements Reports

BeyondInsight 22.4 introduces two new Entitlements reports, supporting Secrets Safe and BeyondInsight entitlements.

- The Secrets Safe Entitlements report provides a list of user groups and the secrets they are entitled to.
- The BeyondInsight Entitlement report provides a detailed, real-time view of BeyondInsight group membership and permissions.

## New SAML Link in Login Page

BeyondInsight 22.4 provides a new **Use SAML Authentication** link on the login page whenever SAML is configured. With this new link, SAML users that land on the main BeyondInsight login page can be redirected to the proper SAML authentication page.

## Smart Rules — Read-Only Support

With BeyondInsight 22.4, an administrator can delegate read-only permissions of Smart Rules to a user. This new read-only permission can be of great benefit to an auditor assessing the solution's setup and configuration since it eliminates any possible mishaps in configuration changes.

## Allow User to Specify Base DN (LDAP Enhancement)

Improving on the Microsoft Lightweight Directory Access Protocol or LDAP enhancements delivered in 22.3, BeyondInsight 22.4 has a new option that allows the user to specify the Base DN. When searching for a user's authentication within your Directory, the LDAP server uses the Base DN as a starting point. This is useful in environments where BeyondInsight cannot automatically determine the Base DN using only the LDAP information provided by the user.

## Definable Session Timeout

Users who log in to the Password Safe console currently have a defined inactivity timeout, which logs the user out when the threshold occurs. Password Safe now provides a new global setting, allowing administrators to set a longer timeout period for Password Safe users, thereby creating a better user experience. In 22.4, a new global session timeout setting allows PWS administrators to set new timeframes for the minimum (2 minutes), default (20 minutes), and maximum amount of time (60 minutes), for session inactivity.

# 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.