# BeyondTrust Password Safe v21.1

## Feature Release – April 8, 2021

**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.
- Utilize adaptive access control for automated evaluation of just-in-time context for authorization access requests.
- Achieve complete control and accountability over privileged accounts.

See the release notes for details.

## New Feature Highlights

### Team Passwords Public API Support

This release has added an extensive set of additional API endpoints to support working with Team Passwords. With full Create, Read, Update, and Delete (CRUD) functionality for both Folders and Accounts, customers can now use this capability to bulk import accounts from existing solutions and interact with the Team Passwords accounts from scripts and applications. This feature is designed to help customers save time from a manual import, and further enhance their team passwords security.

### macOS Secure Token Accounts

Workstations represent the most likely initial entry point for hackers to gain access to your network, so securing the privileged accounts on and used with workstations (laptops and desktops) remains a top priority in any cybersecurity approach. Password

Safe now supports managing macOS credentials that are configured for Secure Token in addition to standard macOS accounts. This new feature ensures that no systems, especially workstations, are missed when managing access to privileged accounts.

### New Endpoint Privilege Management for Mac functionality: Secure Token Support

Password Safe and Endpoint Privilege Management (EPM) for Windows have long provided the EPM for Windows client's ability to operate as a test and change agent for Windows accounts and enable EPM to use Managed Accounts for process elevation. EPM for Mac now offers the same level of integration, including support for Secure Tokens. Seamless use of the EPM for Mac agent for password test and change activities is particularly useful for scenarios where those endpoints do not accept inbound connections.

### Support for Fortinet Admin Accounts

Fortinet admin accounts are different from other Fortinet accounts, so in Password Safe 21.1, we have added explicit support for them. Now customers can manage access to all Fortinet admin accounts from Password Safe. This feature removes oversights in managing your critical infrastructure.

### Support for Cisco Wireless LAN Controller Accounts

Password Safe can now manage and control access to privileged accounts on Cisco Wireless LAN Controllers. This additional coverage is provided at no additional cost.

### Add to Access Policy - Reason Required

Access Policies now include the ability to define whether users must provide a reason for each access request. This capability, previously a global setting, can now be defined at the Access Policy level, giving maximum flexibility across groups of users and groups of managed accounts and across when, where, and how access is defined.

### Add to Access Policy – Ticket System

Password Safe already provides the option to require a valid ticket from the ticketing system to approve requests. However, more granularity was needed.

In this release, we have enhanced this feature with added granularity and flexibility. Now admins can customize the Access Policy with whether there is a need for a ticket to be provided and which ticket system integration should be used. This selection is

available within the Access Policies that connect users to the accounts they have access to.

This granular approach enables complete control to use tickets where and when needed, while still allowing access where a ticket may not be necessary, for example, in break-glass scenarios. It also allows different requirements for different users, giving total flexibility to adapt to your security model. Lastly, for large organizations that may have multiple ticketing systems, customers can specify which ticket system integration is used with each Access Policy.

### Aggregate Resource Broker Logs

With the release of 21.1, customers with cloud deployments can easily retrieve logs from the resource brokers, aiding in troubleshooting and keeping downtime to a minimum.

## About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance.

Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions can easily deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.