BeyondTrust Privileged Remote Access Version 22.2

New and Updated Features

BeyondTrust Privileged Remote Access empowers IT teams to control, manage, and audit remote privileged access by authorized employees, contractors, and vendors, without compromising security. Enforce least privilege and exert granular control and visibility over remote access for both insiders and third parties, while enabling user productivity.

Privileged Remote Access version 22.2 introduces a host of new market-leading features and enhancements to its password management Vault, included with Privileged Remote Access. The Vault protects privileged credentials with discovery, management, rotation, auditing, and monitoring for any privileged account – from local or domain shared administrator, to a user’s personal admin account – even SSH keys, cloud, and social media accounts.

This new release offers security-bolstering features like the rotation of Windows service accounts for management, enforceable password length for Vault, vendor user expiration notifications, and more. Please see the release notes for additional details on these important enhancements.

New Feature Highlights

NEW! Windows Service Account Rotation

One of the most daunting challenges for IT professionals is managing service accounts. These are the privileged accounts that run automated business processes and are used by applications, not people. A single service or process account may be referenced in multiple places. Since these accounts are interconnected, a password change can potentially lock out the account and cause cascading system failures if performed incorrectly. Knowing this, many organizations simply choose to ignore the issue, rather than risk downtime.

To manually change these credentials, you are required to identify everywhere the service account is in use. But that’s only half the battle. You must also change the service account password wherever it is used.

To ease this burden and building upon the 22.1 ability to discover and import Windows service accounts, in 22.2, the Privileged Remote Access vault can now rotate local Windows service accounts (local) and Active Directory Service Accounts (domain).

NEW! Password Safe External Search

Users of both Privileged Remote Access and Password Safe can now use this integration to search for and remotely access Password Safe Managed RDP and shell systems that are accessible with Jumpoints. The 22.2 release includes support for multiple Jumpoints, expanding upon the 22.1 version where only a single Jumpoint was supported. This functionality extends the already complementary relationship that exists between these two products.

NEW! API – Group Policy Access Permissions

Organizations can more effectively scale their growing remote access needs by integrating and automating the management of manual administrative tasks using APIs. This new capability enables organizations to set permissions en masse and apply attribution via the Group Policy API.

NEW! Syslog Access from UI

Most organizations managing remote access, especially privileged remote access, must meet certain compliance and regulatory conditions regarding the auditability of privileged actions and identities. While session data recordings are vital, it is also important that administrative actions are recorded and auditable to prevent misuse, trigger remediation workflows, and notify the organization of specific events. Now, Privileged Remote Access customers can easily download this information directly from the administrative console.

NEW! Group Policy and Jump Group Search

Administrators can now save time and enjoy an improved experience when searching for Group Policies or Jump Groups.

NEW! Vault – Password Length

Organizations that require specific password lengths based on compliance or security policies can now do so, providing additional flexibility and security regarding the management of Windows Local, AD, and Azure AD credentials under Vault management.

NEW! Vendor Admin – PRA User

Administrators now have additional flexibility when managing Vendor Groups and Users. While some organizations elect to delegate certain onboarding rights to a trusted Vendor User who manages the Vendor Team, many organizations prefer to use an internal resource for this function. Now, whether an organization prefers an internal or external resource, the administrator can effectively and securely manage Vendor Groups and Users.

NEW! Vendor – User Expiration Notification

Managing the onboarding/offboarding of Vendor Users is itself a difficult task for many administrators. With little visibility and even less time, the ability to offload administrative tasks to other users saves the PRA Administrator time and improves their ability to meet their organization's requirements as they scale. Now, both administrators and users will have more visibility (via notifications) regarding the onboarding and offboarding workflows.

NEW! Linux Jumpoint – Protocol Tunneling

This functionality has previously only been available for Windows Jumpoints. However, now, Privileged Remote Access users can utilize protocol tunneling through a Linux Jumpoint. This ability to make protocol-based connections greatly extends connectivity scenarios, and now, this connectivity is available across an increased number of networks.