Privileged Identity v5.5.5.0

New and Updated Features

Product Description

Privileged Identity enables organizations to enhance their security and achieve continuous compliance related to management of their privileged identities, service accounts, certificates, and privileged access requirements. The solution helps security teams protect privileged credentials used by end-users, administrators, applications, processes, and more.

New Feature Highlights

New Web Application Front End

Privileged Identity has a new web application frontend. The new web application is written in Angular 7 in order to provide more speed, better security, and a modern development platform. Customers can expect the frontend to have a sleeker, noticeably faster interface, and a tight integration with PI's web service to provide new features.

The introduction of this new web application has resulted in the removal of the previously included RDP (Remote Desktop Protocol) control, due in part to a lack of compatibility between the new web application technology and the outdated RDP control. Privileged Identity included the native ability to launch an RDP session on behalf of the requesting user to the target system using a specified account. This functionality was provided via a Microsoft supplied, Active-X based RDP control, which Microsoft stopped supporting in 2006.

Given the suspension of support from Microsoft, the lack of a proper security posture for the Active-X control, and the lack of compatibility with the new web application technology, BeyondTrust has chosen to remove it. Customers who leveraged the free control should consider a more robust and secure control with additional capabilities, such as BeyondTrust's Privileged Remote Access (PRA) and/or Remote Support (RS) solutions.

Account Elevation for the Cross-Platform Environment

For some organizations, elevating users into an admin group and automatically de-elevating them within a timeframe provides the ability to generate a different (and sometimes more specific) audit detail. This requires no further infrastructure changes, policies, or agents to be implemented or managed.

Previously, Privileged Identity's account elevation feature supported Windows systems only. With this new release, account elevation capabilities will extend across your heterogeneous environment, including Linux/UNIX, various databases, and cloud platforms.

For those customers who do leverage Windows domains and are already at Windows Server 2016 functional level or higher, account elevation has been extended to support Shadow Groups, as well. This means you can add a user to a group such as Domain Admins and have this membership expired by Active Directory itself. For example, if you specify the membership to end by 5:00 PM, the user's Kerberos tickets will expire at 5:00 PM and can no longer be used to access resources. This provides an enhanced level of secure access.

Native Launch Capability for Privileged Remote Access (PRA) Product

Prior to this release, Privileged Remote Access (PRA) has been able to launch sessions by using credentials from Privileged Identity. Now, PI will be able to launch privileged access sessions using PRA directly from the PI website. This integration helps to minimize the interactions required from a user requiring privileged access and consolidates it into a single interface.

Enhanced Feature Highlights

New Licensing Model

The legacy licensing model has been retired and changed to a TrueUp model, which is more applicable to enterprise customers with highly dynamic environments. Furthermore, the licensing information will be stored in the PI database, allowing better tracking across all components of managed systems. Finally, the licensing changes will allow customers to move from commercial keys to demo keys to better test new add-on features before purchase.

Alternate Administrators

The existing alternate administrators feature has been changed. Prior versions lacked customer-based control over the order in which credentials were leveraged by the application. This could sometimes lead to account lockouts or unnecessary audit findings. This enhancement allows customers to decide the order of credentials that PI can attempt at the program level, management set level, or system level. This will help improve management of environments where PI is not granted the breadth of required rights and permissions necessary, as well as untrusted environments where zone processors cannot be leveraged.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.

BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.