PowerBroker for Windows Version 6.7
New and Updated Features

BeyondTrust PowerBroker for Windows reduces the risk of privilege misuse on physical and virtual Microsoft Windows servers and desktops. By eliminating Windows administrator privileges, simplifying the enforcement of least-privilege policies, maintaining application access control, and logging privileged activities, IT closes security gaps, improves operational efficiency and achieves compliance objectives faster. Key capabilities include:

- Least-privilege access and application control for applications with patented, rules-based technology to elevate application privileges without elevating user privileges
- Patented Vulnerability-Based Application Management (VBAM) for least-privilege access to applications based on an application's and system's vulnerability profile – such as vulnerability age, risk, or compliance mandate
- Windows Event Log Monitoring for documenting system changes during privileged sessions where key system runtime parameters are modified
- Optional: File Integrity Monitoring for reporting on privileged access to the file system for all users
- Optional: Session Monitoring for screen capturing and keystroke logging of privileged access
- Optional: Centralized monitoring and reporting using the BeyondInsight® IT Risk Management Platform
- Optional: Integration into other BeyondTrust technologies like PowerBroker Password Safe to meet the demanding needs of Privileged Account Management across all assets

PowerBroker for Windows version 6.7 adds several new features that add business context to security exposures and make it easy to understand, prioritize and communicate privileged access risk within the organization.

New Feature Highlights

PowerBroker Password Safe Integration

The primary enhancement in this release, PowerBroker for Windows version 6.7 now integrates with Password Safe 5.4 to create an industry unique approach to solving remote password change challenges and elevation of applications for real user credentials. This section explains two such use cases.

Use case #1: Password changes in a remote/mobile environment

In a traditional model Password Safe, on a scheduled basis, remotely contacts a host to change a local password. If the device is unreachable, the Password Safe manager will retry to contact the host and change the password until the policy for retries is exceeded. If the device is mobile, on the other side of the firewall, or remotely connected, the manager may not always be able to connect to the target. This negates the capabilities of a password management solution.

To overcome the challenge of remote/mobile password management, Password Safe 5.4 features integration with PowerBroker for Windows 6.7 to enable PowerBroker for Windows to act as an agent for Password Safe account password changes.

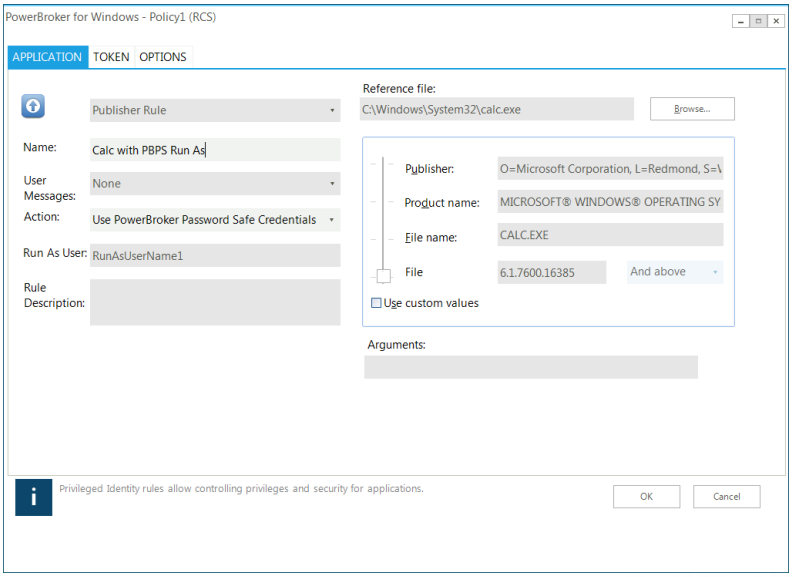
With PowerBroker for Windows 6.7, upon a scheduled heartbeat connection, the agent will ask Password Safe if it has any accounts that require a password change. If Password Safe has a change, the password changes are transmitted back to the agent fully encrypted and then verified with the remote client to ensure they have been incorporated successfully.

This integration allows PowerBroker Password Safe, via PowerBroker for Windows, to change a password at any time, and in any location, and overcome the limitations of network segmentation.

Use case #2: Elevating applications that communicate across the network without exposing credentials to the end user

In some cases, primarily involving applications that need to communicate across the network, PowerBroker for Windows is unsuccessful in elevating an application's security token for proper operation. The only way to properly elevate the application is to use a real username and password combination with administrator permissions. This problem then requires the distribution of these credentials to users, which defeats the purpose of least privilege.

With PowerBroker for Windows 6.7, a new Action has been defined which can transparently request a username password combination from PowerBroker Password Safe 5.4 and perform a "Run As" with no user intervention and record all actives in both PowerBroker for Windows and Password Safe.



This technique only exposes the username in the PowerBroker for Windows Rule, and never exposes either the username or password to the end user during normal operations with true "Run As" elevation of the application. This allows specialty applications to operate correctly, operating system functions like MMC or Regedit to operate across the network, and the suppression of credentials to end users that need to execute these applications.

Expanded Vulnerability Based Application Management

The patented technology for Vulnerability Based Application Management (Risk Compliance) leverages the Retina database to identify vulnerable applications. In versions prior 6.7, this feature was limited to applications that had specific entries for executables in the Retina database. With the new release of

PowerBroker for Windows, the agent will also process registry entries and DLL's that are called and associated with vulnerabilities. This expands the capabilities of Vulnerability Based Application Management to include other components, besides user launched applications, for Risk Compliance:

- User launched executables are compared to the Retina database and the runtime of the application and security token are decided within a rule
- Any process, service, or application that reads from the Windows registry that contains a matching vulnerability in Retina, will send an alert to BeyondInsight
- Any DLL called by a process or service within a rules monitoring path, that matches a vulnerability check within Retina, will send an alert to BeyondInsight
- Alerts are suppressed by frequency such that common DLLs and registry calls due not create a message storm. They will send a maximum of one event per occurrence in a user defined interval
- Only executables can have token modifications or be denied execution. DLL's and registry vulnerability matching provide alerting only. These represent Active Detection of vulnerabilities by executing applications (see previous whitepaper)
- Dormant vulnerabilities for applications, DLL's, and registry entries still require a full vulnerability assessment with Retina (network or agent based)

The Retina database for application, DLL, and registry matching vulnerabilities is automatically obtained from BeyondInsight during normal communications with the agent and automatic updates of vulnerability data from BeyondTrust.

Tamper Protection User and Group Protection

PowerBroker for Windows 6.6 introduced advanced capabilities for system and agent tamper protection to harden and monitor an installation of the technology. With version 6.7, BeyondTrust has expanded this capability to protect local user accounts. The capability has a dedicated setting that:

- Prohibits the creation of local accounts
- Prohibits.adding new members to local Administrator and Remote Desktop User groups for any user

This enhancement ensures that whether a user is a local admin or has permission elevated with a PowerBroker Rule, they can never tamper with local users and their local group membership.

Simplified Installer

BeyondTrust recognizes that PowerBroker for Windows can truly be implemented for any size organization. This includes businesses with just a few employees and organizations with hundreds of thousands of users. To that end, PowerBroker for Windows now contains a simplified approach to installing the technology for any size business. After launching the Snap In Installer, an administrator is presented with a simple question:

Do you plan to use BeyondInsight for Management and Reporting?

(Yes or No)

If the user answers **Yes**, the product behaves just like previous versions requesting BeyondInsight IT Risk Management Server information and deploys the full solution.

If the user answers **No,** the product will not install several components and suppress all functionality related to an enterprise deployment of the technology. The user interface will be tailored just to their needs. Small businesses can than leverage PowerBroker for Windows for best of breed least privilege management without deploying a dedicated server. The chart below summaries the differences:

Feature	***Yes* – with BeyondInsight**	***No* – without BeyondInsight**
Least Privilege	**Y**	**Y**
User Messages	**Y**	**Y**
Active Directory Based Rules	**Y**	**Y**
Passcode Generator	**Y**	**Y**
Rules Library	**Y**	**Y**
Risk Compliance	**Y**	**N**
File Integrity Monitoring	**Y**	**N**
Session Monitoring	**Y**	**N**
Event Log Monitoring	**Y**	**N**
Web Services Rules	**Y**	**N**

Finally as businesses grow, they can add BeyondInsight at a later time to take advantage of all the advanced functionality the solution can offer. For clients wishing to test drive this functionality, BeyondTrust has a sample BeyondInsight lab available at https://demo.beyondtrust.com to demonstrate these capabilities without deploying the technology within your environment. Login details can be obtained from your sales representative or by contacting: sales@beyondtrust.com.

About BeyondTrust

BeyondTrust is a global cyber security company dedicated to proactively eliminating data breaches from insider privilege abuse and external hacking attacks. Corporate and government organizations rely on BeyondTrust solutions to shrink attack surfaces and identify imminent threats. The company's integrated risk intelligence platform presents a unique competitive advantage in its ability to reveal critical risks hidden within volumes of user and system data. This unifies IT and Security departments, empowering them with the information and control they need to jointly prevent breaches, maintain compliance, and ensure business continuity. BeyondTrust's Privileged Account Management and Vulnerability Management solutions are trusted by 4,000 customers worldwide, including over 50% of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.