

# PowerBroker Password Safe Version 5.5

## New and Updated Features

BeyondTrust [PowerBroker Password Safe](#) automates password and session management, providing secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user’s personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts. By improving the accountability and control over privileged access IT organizations can reduce security risks and achieve compliance objectives. With Password Safe, customers can:

- Secure and control privileged passwords to close critical security gaps and reduce risk
- Monitor, audit and report on activity to achieve compliance requirements
- Automate password request and approval processes to simplify administration and improve security
- Gain greater insights on their security environments through integration with the [BeyondInsight IT Risk Management platform](#)

Password Safe version 5.5 improves on key features and capabilities with unmatched levels of security, accountability and control.

## New Feature Highlights

### Integration with BeyondInsight Clarity Provides Advanced Threat Analytics

---

BeyondTrust introduced [Clarity Threat Analytics](#) in BeyondInsight version 5.4. Clarity Threat Analytics correlates data from [Retina CS Enterprise Vulnerability Management](#) and other third-party vulnerability management solutions, privileged user and account data from [PowerBroker for Windows](#) and [PowerBroker for UNIX and Linux](#), and threat data from the [PowerBroker Endpoint Protection Platform](#).

With version 5.5 BeyondInsight now supports data feeds from PowerBroker Password Safe, which enables the patent-pending Clarity Threat Analytics engine to analyze privileged password, user and account behavior. BeyondInsight Clarity includes the PowerBroker Password Safe Event View Report (seen below), with Password Safe included in the top level Clarity reports as well.

Since many exploits involve the abuse of privileged credentials in concert with a vulnerability, this integration makes it easier for customers to uncover emerging risks in the organization, pinpoint specific at-risk systems, report on the findings, and take action to eliminate the threat.

## Clarity PBPS Event Review

Report Description



Alerts Triggered					Release ID	Release Event Time	Managed Account	Managed System	Reason	Status	Threat Level
Outlier	Asset Risk	Event Timing	Untrusted User	Concurrent Request							
*			*	*	13	March 19, 2015 3:13:13 PM	holly	10.200.31.199	Requesting password for pre-approved SQL update	Open	3
*			*	*	11	March 19, 2015 11:50:17 AM	holly185	QA-R2X64-6	testing request to a win account with approval required	Approved	2
*			*	*	15	March 19, 2015 3:14:54 PM	holly185	QA-R2X64-6	Have to fix a configuration issue on this box	Approved	2
*			*	*	14	March 19, 2015 3:13:26 PM	holly187	qa-retina	Requesting password for pre-approved SQL update	Open	2
*			*		16	March 19, 2015 3:15:54 PM	holly	10.200.31.199	Need the password again	Approved	1
*				*	12	March 19, 2015 3:12:59 PM	holly185	QA-R2X64-6	Requesting password for pre-approved SQL update	Cancelled	1

*Clarity Threat Analytics provides a view of PowerBroker Password Safe events, helping to assess threats from misuse.*

### Simplified SSH Key Management for Better Control and Accountability

Traditional methods of SSH key management are very labor intensive, with many organizations not properly rotating their keys. As well, it is common practice for administrators to share keys. Between the lack of rotation and the sharing of keys, organizations lose accountability over their systems which could lead to those systems being vulnerable to exploits.

With version 5.5, PowerBroker Password Safe has simplified this process, automatically rotating keys according to a defined schedule and enforcing granular access control and workflow to access SSH keys. In addition to key management capabilities, private keys that are stored in Password Safe can be leveraged to automatically log users onto UNIX or Linux systems through the proxy with no user exposure to the key. If SSH key authentication fails through the proxy, session authentication can failover to a managed password for complete redundancy. Users simply log on through Password Safe, select the system/account combination, and the session is connected without exposure to the key. All sessions can be recorded for full accountability together with full key usage auditing.

This capability greatly simplifies the management and secures the use of SSH keys for better control, accountability and security over UNIX and Linux systems.

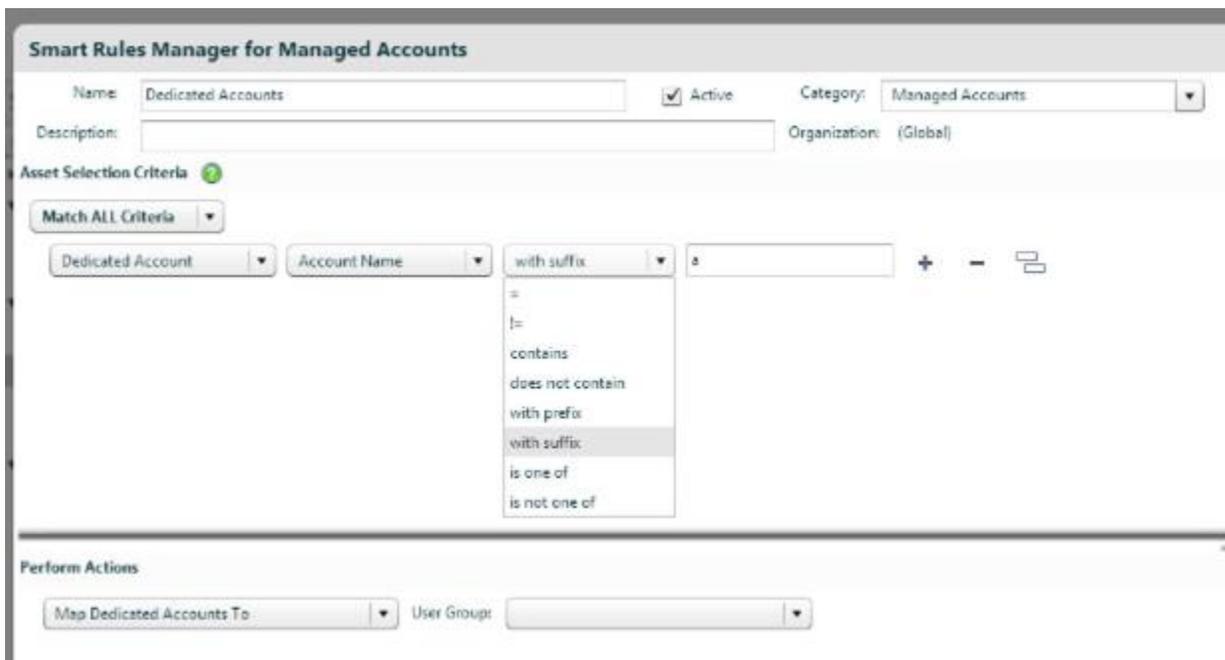
### Dedicated User Account Mapping Simplifies Administration

Nearly every organization makes use of dual accounts, a mapped association between a user's basic account and their administrative account. The typical use case involves adding a prefix or suffix (more

common) to a user's Active Directory account name, with common suffixes being 'a', '.adm', '.admin', '.sec'.

Managing these dedicated, dual accounts for users normally involves many administrative steps. Existing solutions available in the market force you to create a mapping for every user to their account on every authorized system – a many-to-many administrative process that only amplifies the issue of time and complexity.

With version 5.5, however, PowerBroker Password Safe simplifies the association between a user and their administrative account through a simple two-line Smart Rule (see screen shot below). This simple process can associate hundreds or even thousands of users with their administrative accounts with one simple rule. This capabilities dramatically reduces the time, complexity and cost of administration.



*Password Safe simplifies the association between a user and their administrative account through a simple two-line Smart Rule.*

## New Deployment Options Provide Choice and Flexibility

With version 5.5, PowerBroker Password Safe now offers a software-only deployment option. Customers will no longer be required to utilize the UVM appliance if they choose not to use it.

This new deployment option is ideal for smaller customers, or for those who have already installed BeyondInsight and wish to add Password Safe functionality by adding only a new license key.

## Reporting, Workflow and Administration Enhancements

PowerBroker Password Safe version 5.5 adds several new capabilities to further simplify management and reporting and improve workflow. Reporting enhancements include:

- Ad-hoc (admin) session data has been added to the Password Safe Password and Session Activity report
- New role-based approval capabilities
- The ability to view/edit/delete report subscriptions from the Report Subscriptions tab has been added

Workflow enhancements include improvements to approval email templates, and the ability for requestors to see who has an account checked out.

Administration enhancements include UI improvements (sortable/filterable data grid columns, and managed account data grid improvements), the ability to set a 'Default Release Duration' on an asset, ticket system improvements, and a new bulk asset import utility and API.

### Expanded Platform and Device Support

---

PowerBroker Password Safe 5.5 includes the following newly-supported applications, protocols, databases, devices and integrations:

#### Applications & Protocols:

- SAP
- LDAP
- Windows SSH
- TOAD Application Proxy
- Radius Two Factor Authentication
- Custom Platform Connector for SSH and Telnet

#### Databases:

- MySQL
- Teradata

#### Devices:

- Fortinet

#### SIEM:

- Integration with syslog

## 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 customer 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](http://www.beyondtrust.com).