Secure and Manage SSH Keys

Privileged Password Management and Privileged Session Management

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

Secure Shell (SSH) is a tool used to enable secured systems management, file transfers, and application automation that ships standard with every Unix, Linux, and Mac system and is widely used on Windows. SSH keys are commonly used by privileged users and applications to automate secured sessions by enabling login over SSH without typing a password. As with passwords, unmanaged SSH keys create an opportunity for compromise by both insiders and external hackers. Common challenges include:

- Inappropriate sharing of SSH keys with unauthorized persons
- Loss of SSH keys providing a backdoor to systems and resources
- Stolen SSH keys by insiders or external hackers
- SSH key sprawl

Traditional methods of SSH key management are very labor intensive, causing many organizations to not properly rotate their keys. Additionally, 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. To highlight the risks associated with unmanaged SSH keys, the National Institute for Standards and Technology (NIST) published *NIST IR 7966* in 2016. This provides guidance for enterprises, government agencies, and auditors for properly managing and securing SSH implementations. Best practice recommendations include SSH key discovery, rotation, usage, and monitoring.

SIMPLIFIED SSH KEY MANAGEMENT WITH POWERBROKER PASSWORD SAFE

PowerBroker Password Safe adds security and simplifies the management of SSH keys by automatically rotating SSH keys according to a defined schedule and enforcing granular access control and workflow. Private keys stored in Password Safe can be leveraged to automatically log users onto systems through a proxy with no user exposure to the key, and with full privileged session recording.

- Automatically discover assets and unmanaged SSH keys
- Create a SSH Key Management Group DSS Key rule to specify key type, bit size, and passphrase controls
- Assign SSH key rule to managed accounts, specify password failover, and set key rotation interval
- Configure access policy to include factors such as location, certificate, date/time controls, and real-time alerts
- Configure access policy to include options for integrated session recording of all privileged activities
- Configure approval processes for SSH key usage and tracking
- From a central console, view SSH key usage, approved/unapproved activity, and session logs through delegated reporting mechanisms
- Directly connect and automatically launch SSH sessions by simply passing a connection string to the proxy

Key Differentiators

NETWORK-BASED ASSET DISCOVERY

Scan, identify, and profile all users and services; automatically onboard systems and accounts under management, speeding time to value.

DYNAMIC RULES & ASSET GROUPINGS

Build Smart Rules to trigger alerts or auto-provision based on system categorization, speeding time to resolution.

SIMPLIFIED SSH KEY MANAGEMENT

Schedule SSH key rotation and enforce granular access control and workflow.

UNIFIED PASSWORD AND SESSION MANAGEMENT

Use a single solution for both password management and session management, lowering cost and complexity.

AGENTLESS SESSION MANAGEMENT

Utilize native tools including Microsoft® Remote Desktop and PuTTY to connect to systems without the need for Java.

APPLICATION PASSWORD MANAGEMENT

Get control over scripts, files, code, and embedded keys by automatically eliminated hard-coded or embedded credentials.

ADVANCED WORKFLOW CONTROL

Add context to workflow requests by considering the day, date, time, and location when a user accesses resources.

THREAT ANALYTICS & REPORTING

Leverage a central data warehouse to collect, correlate, trend, and analyze key threat metrics; customize reports to meet specific needs.

The PowerBroker Privileged Access Management Solution

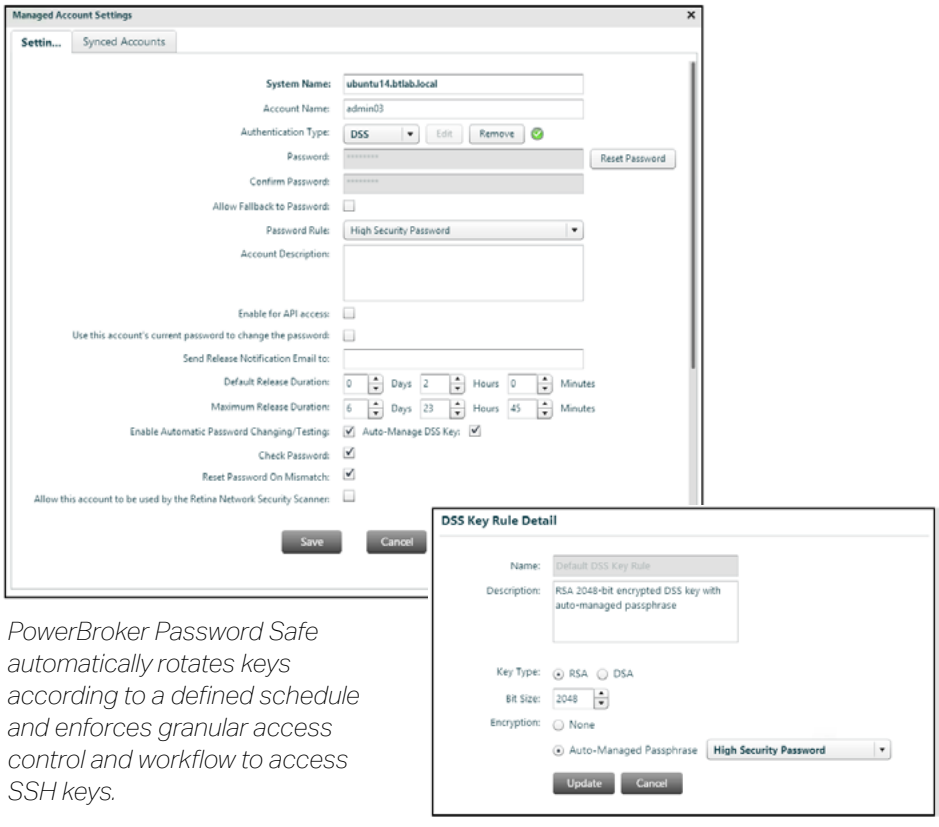
PowerBroker Password Safe is part of the PowerBroker Privileged Access Management Platform, which is a modular, integrated solution that provides visibility and control over all privileged accounts and users. By uniting capabilities that many providers offer as disjointed tools, the platform simplifies deployments, reduces costs, improves system security, and reduces privilege risks. Solutions include:

- **Server Privilege Management:** Control, audit, and simplify access to business critical systems.
- **Enterprise Password Security:** Provide accountability and control over privileged credentials and sessions.
- **Endpoint Least Privilege:** Remove excessive user privileges and control applications on endpoints.

SECURE SSH KEYS WITH POWERBROKER PASSWORD SAFE

PowerBroker Password Safe greatly simplifies the management and secures the use of SSH keys for better control, accountability, and security over Unix and Linux systems. Password Safe SSH key management features include:

- Storing private keys, like any other privileged credential
- Automatically rotating SSH keys according to a defined schedule
- Manual upload of externally generated keys, or automatic key pair generation according to defined DSS key policy
- Automatic push of the public key into the managed account's authorized keys file
- Allowing designated 'secondary' accounts and SSH keys to be grouped to a 'primary' account to manage rotation interval, complexity, and duration of SSH keys
- Enforcing granular access control and workflow
- Alerting when a key is released
- Automatically logging users onto Unix or Linux systems through the proxy with no user exposure
- Enabling users to request access to SSH key sessions instantly, or via workflow
- Never revealing SSH keys to the end-user
- Real-time alerting of SSH key release
- Recorded, full-motion video playback of all SSH key usage
- Offering failover to a managed password for complete redundancy



PowerBroker Password Safe automatically rotates keys according to a defined schedule and enforces granular access control and workflow to access SSH keys.

CONTACT

North America
Tel: 800.234.9072 or 480.405.9131
info@beyondtrust.com

EMEA
Tel: +44 (0)1133 970445
emeainfo@beyondtrust.com

APAC
Tel: +65 6701 8267
apacinfo@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

© 2016 BeyondTrust Corporation. All rights reserved. BeyondTrust, BeyondInsight and PowerBroker are trademarks or registered trademarks of BeyondTrust in the United States and other countries. Microsoft, Windows, VMware, and other marks are the trademarks of their respective owners. August 2016