QUEST SOFTWARE®

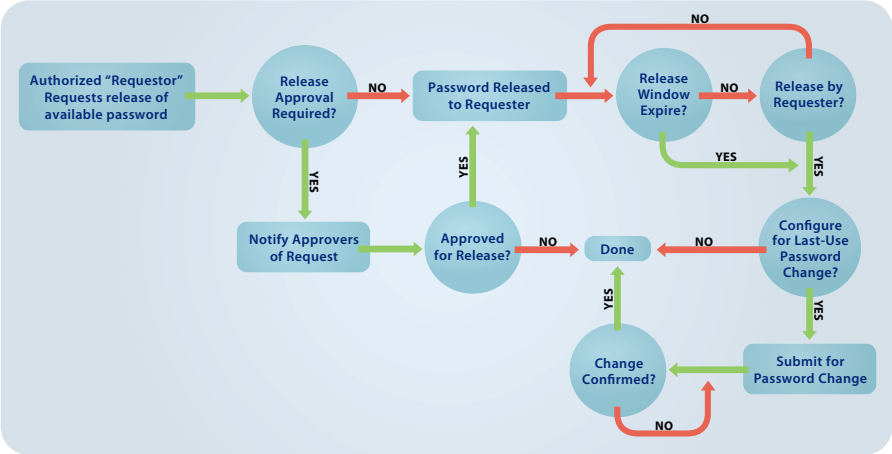
DATASHEET

Quest® One Privileged Password Manager

Comprehensive Privilege Safe Functionality for Your Most Important Administrative Access Credentials

Managing elevated and shared access credentials is one of the biggest challenges facing complex heterogeneous organizations today. On the one hand, administrators must be able to access the systems they manage with sufficient rights to do their jobs; on the other hand, to ensure security and regulatory compliance, organizations must control that access in a manner that far exceeds the native capabilities available on those systems.

The answer is Quest One Privileged Password Manager. This tool automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. Privileged Password Manager is a critical component of the Quest One Identity Solution's privileged account management suite and is deployed on a secure, hardened appliance.



With Quest One Privileged Password Manager, password request approvals can be fully automated or configured for one or more levels of manual approvals.

Privileged Password Manager ensures that when administrators require elevated access (typically through shared credentials such as the Unix root password), that access is granted according to established policy (with appropriate approvals), that all actions are fully audited and tracked, and that the password is changed immediately upon its return. It's a secure, compliant, and efficient solution to the age-old "keys to the kingdom" problem.

Closing the Embedded Application Password Hole

One of the most vulnerable—but often overlooked—aspects of IS security is the embedded passwords required as applications talk to each other or to databases. Often these passwords are hard-coded in scripts, procedures and programs with simple CLI or API calls. As a result, passwords that grant access to some of an organization's most sensitive data are vulnerable: they can be known by a high number of knowledge workers, haven't been evaluated (or changed) in years and may exist outside of established security and compliance practices. Privileged Password Manager's application password management capabilities replace hard-coded passwords with programmatic calls that dynamically retrieve the account credential, eliminating this security exposure.

Quest One Privileged Password Manager was named the "Best Regulatory and Compliance Solution" for 2010 by SC Magazine.

"With [Quest One Privileged Password Manager] I don't have to worry about someone not being able to take care of a machine if something goes wrong after hours or if we have a disaster. And I don't have to worry about unaudited use of powerful credentials that people aren't supposed to use on a daily basis."

— John Campbell
Information Security Officer
School Employees Credit Union of Washington

Key Privileged Password Manager Capabilities:

- Provides compliant management of shared, privileged and critical account passwords
- Delivers individual accountability for shared account access
- Easily deployed as secure, scalable, purpose-built appliance
- Easily expands to include session audit and recording and command control

Privileged Password Manager Features and Benefits

- Release control: Manages password requests from authorized users, programs and scripts—via a secure web browser connection—for the accounts they are entitled to access. The request for one or more passwords can be automatically approved or require any level of manual approvals.
- Change control: Supports configurable, granular change control of shared credentials, including time-based, last-use-based, and manual or forced change.
- Application password support: Replaces hard-coded passwords in scripts, procedures and other programs. Application password management capabilities include:
    - Programmatic access: Includes both a command-line interface (CLI) and an application programming interface (API) with access for C++, Java, .NET and Perl. Connectivity is via SSH with DSS key exchange.
    - Role-based access: Supports role-based access for the CLI and API. You add a "programmatic" user with either "basic" access or "admin" access: Basic access enables the CLI or API to request account passwords and be granted access for authorized targets or accounts; this is appropriate, for example, for a "Requestor." Admin access enables the CLI or API to perform administrative tasks.
    - Optimal performance: Natively executes approximately 100 call requests per minute. For applications requiring higher performance, the appliance supports an optional cache that executes more than 1,000 password requests a second, satisfying the requirements of your most demanding applications.
    - Extensive command set: A comprehensive set of commands can be executed via the Application Password Management CLI or API. Beyond simple "Get Password" commands, the solution supports extensive admin-level commands to provide tight integration with existing enterprise tools and workflows.
- Enterprise-ready: Integrates with existing directories, ticketing systems and user authentication sources, including Active Directory and LDAP. Also fully supports two-factor authentication through Quest Defender or other third-party, two-factor authentication products. A robust CLI/API supports end-to-end integration with existing workflows and tools, including reviewer notification and escalation workflows.
- Scalable appliance: Provides secure, hardened, enterprise-ready access and management of shared credentials for more than 250,000 accounts at once.
- Secure password storage: Encrypts all passwords stored in Privileged Password Management using RSA B-Safe AES 256 encryption. In addition, the appliance also includes full disk encryption using Guardian Edge AES-256.
- Robust target support: Manages shared credentials on the widest range of target servers, network devices and applications.
- Handheld device support: Includes full support for password request, approval and retrieval via handheld devices, configurable on a per-user basis.

The Quest One Approach to Privileged Account Management

The Quest One Identity Solution includes the most comprehensive set of privileged account management solutions, ideally suited to the needs of any organization. In addition to the powerful privilege safe functionality of Privileged Password Manager, Quest One also includes network-based session audit and command control running from the same hardened secure appliance. Quest One also delivers targeted agent-based solutions for granular delegation of the Unix root account and the Active Directory administrator account; add-ons to make open-source Sudo enterprise ready; and keystroke logging for Unix root activities—all tightly integrated with the industry's leading Active Directory bridge solution.

About Quest Software, Inc.

Established in 1987, Quest Software (Nasdaq: QSFT) provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, and user workspace management to Windows management. For more information, visit **www.quest.com**.

QUEST SOFTWARE®

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | EMAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.