"This product essentially gives us a 24x7 support desk for password reset requests. Over the past two years, since we put this solution into place, our level of help desk calls has remained constant, while usage of the automated password reset system has increased dramatically. I can only imagine what the burden would have been on our help desk, if we weren't using Password Manager."

— Keith Price,
Systems Administrator,
Johnson & Wales University

- Reduces help desk and IT involvement in routine password management
- Dramatically reduces user downtime
- Provides immediate return on investment
- Improves user and IT satisfaction since the product is simple to use and easy to deploy
- Increases network security
- Integrates with Microsoft Identity Integration Server (MIIS) to synchronize passwords between disparate systems

QUEST SOFTWARE®

Quest® Password Manager

Empower Users, Reduce Support Costs and Strengthen Security

Password resets are the leading source of requests for help desk assistance. The pain of password management is becoming more pervasive as organizations strive for more stringent security policies. And, more complex passwords that must be changed more frequently increase the likelihood that users will forget them and place a call to support. As a result, many organizations are caught between increasing security and reducing user support costs.

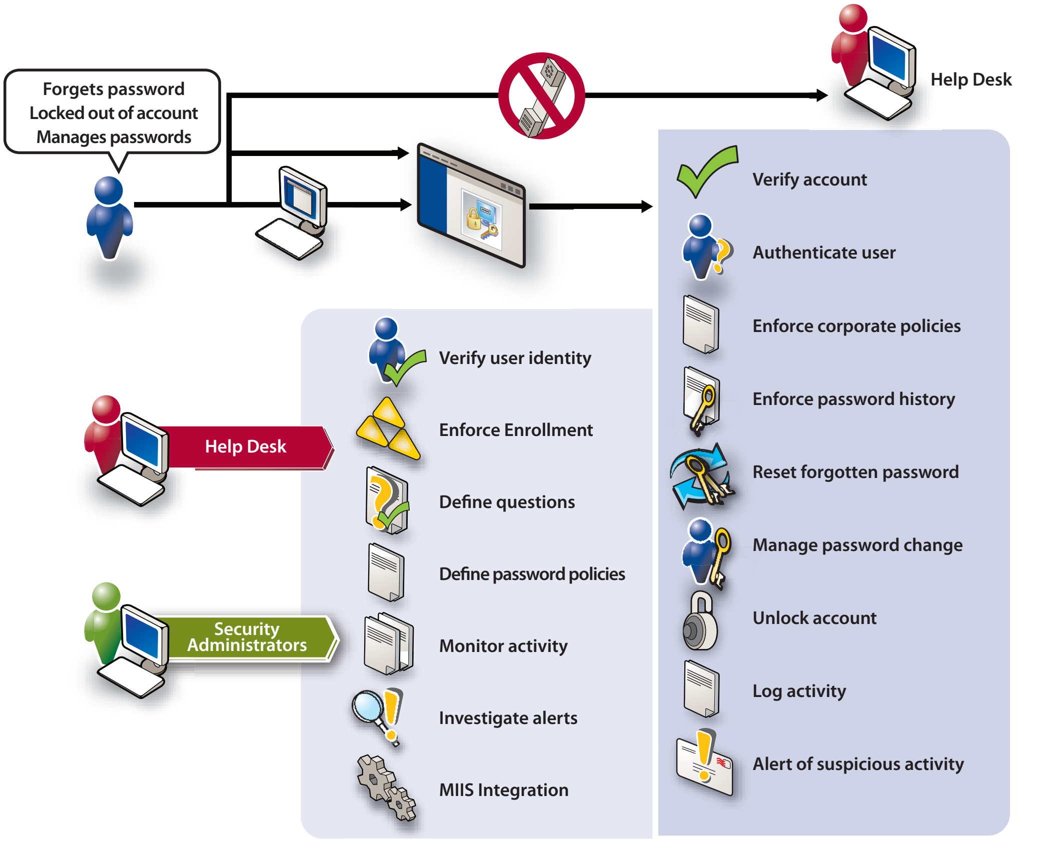
Quest® Password Manager provides a simple, secure, self-service solution that allows end users to reset forgotten passwords and unlock their accounts. It also allows administrators to implement more strict password policies, while reducing the help desk workload. Organizations no longer have to sacrifice security to reduce costs.

Enhance Security

Password Manager allows organizations to adopt more secure data access policies. It increases security by eliminating help desk errors, reducing the need for users to write down their passwords, and making password guessing and break-ins more difficult. Built-in data encryption supports global access, while maintaining data security.

User Participation Secures your Return on Investment

Password Manager provides several mechanisms to ensure that users enroll and use self-service when they need to change passwords, reset forgotten passwords or unlock their account. Without these mechanisms, users will continue making expensive support calls and prevent your organization from realizing a high return on investment.



System Requirements:

Minimum hardware requirements:

- 800 MHz Pentium® compatible CPU
- At least 128 MB RAM (256 MB recommended)
- 80 MB hard disk space

Minimum software requirements:

- Microsoft® Windows® Server™ 2003 SP1 and later
- Microsoft® Internet Information Server 5.0 or later
- Microsoft® Internet Explorer 6.0 or later
- Microsoft® Data Access Components 2.7 or later
- Microsoft® SQL Server™ 2000
- Microsoft® SQL Server™ 2005 Express Edition Service Pack 1 or later
- Acrobat® Reader® 5.0 or later

* See Quick Start Guide for additional requirements for password complexity policies on 32 and 64-bit systems

Minimum software requirments for client computers:

- Microsoft Internet Explorer 6.0 or later
- Mozilla® 1.7.5 or later
- Mozilla® Firefox® 1.0 or later

QUEST SOFTWARE®

www.quest.com/microsoft
e-mail: info@quest.com
Please refer to our Web site for
international office information.

Reduce Help Desk Workload and Cost, Increase User Productivity

With Password Manager, users can reset their own passwords and unlock their own accounts — without involving the help desk or administrative support. As a result, user satisfaction and productivity is improved, while calls to the help desk are dramatically reduced.

Password Manager not only increases your help desk efficiency, it also provides administrators with robust logging and reporting features, making it easy to monitor system activity and correct problems.

Enforce Organizational Standards

Password Manager is designed to accommodate the widest possible range of organization requirements and data security standards. In addition, Password Manager ensures that passwords conform to standards for length, composition, password history and recent use, as well as per group or per organizational unit password polices — well beyond what Active Directory (AD) provides.

Make a Smart Investment

As an extensible and scalable product, Password Manager represents a long-term solution to a growing problem. As part of an integrated, single-source user account management solution, Password Manager is a smart investment for any enterprise seeking to increase IT operational efficiency and improve security.

Builds on Your Existing Active Directory Infrastructure: Password manager leverages your existing Active Directory infrastructure, allowing you to quickly deploy and realize immediate ROI while increasing your equity in Active Directory.

Reliable Authentication: The personal Q&A profiles for each user contain questions with very unique answers that are easy for users to remember, but hard for others to guess.

Strict Policy Enforcement: Password Manager enforces administrator-defined standards, logs unsuccessful authentication attempts and locks the corresponding accounts if necessary.

Enforced Enrollment: No password management solution can provide a return on investment if it isn't used. Password Manager provides several mechanisms that allow you to ensure that users enroll and use the software, guaranteeing its effectiveness.

Proactive User Help: Password Manager makes it easy for users to create unique passwords. This product provides online help that explains password policies. It also provides default feedback if rules are not met and can even auto generate a compliant password for the user.

Security and Simplicity: Password Manager seamlessly integrates with Windows, allowing you to service users from multiple domains, with or without trusts. Strong data encryption and secure communication are provided through support for leading technologies such as 3DES, MD5, SSL and Microsoft's CryptoAPI.

GINA Extensions for the Windows Logon Dialog Box: To make password resets easy, administrators can update the Windows Logon screen to display a button for users to click and reset their passwords prior to logon. This eliminates the need to configure public kiosks or expensive telephone-based systems and compatibility. Most third-party GINAs or GINA extensions ensures simple deployment

Support for Identity Management Initiatives: Password Manager supports multiple Web browsers and provides password management for any system connected to Microsoft Identity Integration Server (MIIS) in addition to non-Microsoft Operating Systems, like Unix and Linux through Quest Vintela Authentication Services. This means Password Manager can be your enterprise-wide password management solution.

About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at **www.quest.com**.

Microsoft GOLD CERTIFIED Partner