Implement a Secure Password Reset Policy Throughout Your Windows Enterprise

Grant Your Users Secure and Audited Password Reset Rights

KEY FEATURES

SELF-SERVICE RESETS
Users can reset or unlock their own accounts without Help Desk interaction.

HELP DESK RESETS
Help Desk can reset locked user accounts without administrator involvement.

DELEGATED USERS
IT controls which users have access to the application.

VERIFY IDENTITIES
Users validate identity against relational database prior to resetting accounts.

AUTOMATIC ALERTS
Users are notified about passwords set to expire.

STALE ACCOUNTS
Locate and disable expired or stale accounts.

MANDATE RESETS
Require users to reset changed passwords at their next logon.

SCHEDULED REPORTS
Generate regular reports on user account activity.

AUDITED ACCESS
Search and examine a full audit trail of password changes by date or user.

UNIVERSAL ENROLLMENT
Ensure full participation among users by reporting on who has not yet enrolled their accounts.

RESET OPTIONS
Change passwords via a secure website or the Windows logon page.

The escalating number of passwords that are required to safely access systems, applications, and other enterprise assets adds an additional element of complexity to already burdened IT groups. Windows administrators who manage a large base of users are constantly barraged with Help Desk requests to reset forgotten or expiring passwords. Organizations suffer from the wasted time and reduced productivity of employees who are frequently locked out of critical systems, while IT is forced to dedicate resources to manually reset user accounts. Without effective password management controls organizations can suffer from non-compliance with security audits, potential security breaches, reduced productivity, and increased IT expenses.

ACCOUNT RESET CONSOLE

Account Reset Console permits users to reset or unlock their own accounts in a secure, audited, and delegated manner. Passwords can be reset via a user's own Windows logon screen or through any web browser. Users can confirm their identities against a set of relational databases, and then reset their passwords without administrator involvement. This web-based solution resolves one of the most common problems encountered by IT groups in large organizations — users losing access to systems because of forgotten or expired passwords.

Rest passwords through the Windows logon page or a secure web site.

PRODUCTIVITY

By permitting delegated users to change their own passwords, downtime can be significantly minimized and high productivity levels maintained. 45 percent of calls to the Help Desk are requests for password resets, and automating password reset operations can reduce this call volume by approximately one-third.[1]

MASS MANAGEMENT, SECURITY, AND COMPLIANCE FOR THE ENTERPRISE

LIEBERMANSOFTWARE™

Account Reset Console™

KEY BENEFITS

ENTERPRISE SECURITY
Strengthens security policies by enforcing a strict and secure password reset regimen.

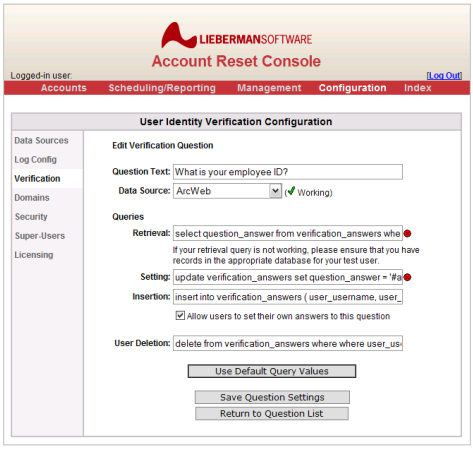
OVERSIGHT CONTROL
Improves existing control measures through scheduled and on-demand reports that identify common account issues across the network.

REGULATORY COMPLIANCE
Assures continuing compliance with the control and auditing requirements of FERPA, HIPAA, and other regulatory standards.

INCREASED PRODUCTIVITY
Prevents end-users from being locked out of critical systems, and reduces 7/24 Help Desk dependency.

SECURITY

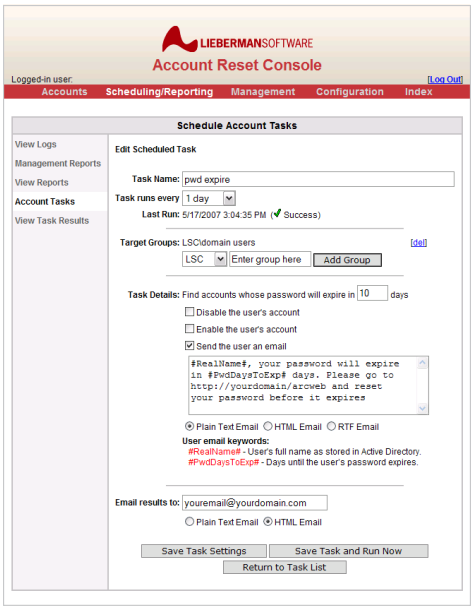
Account Reset Console allows organizations to apply a comprehensive password management policy across the network by: enabling a strict and structured password reset regimen, alerting users and administrators about expiring passwords, requiring identity verification prior to changing passwords, and forcing users to reset recently changed passwords during the next logon. Enterprise security is further enhanced with the product's ability to identify and disable inactive user accounts, which are potentially serious threats.



Create self-reset questions and use any ODBC compliant database to store and retrieve the answers.

COMPLIANCE AND OVERSIGHT

The strong password security provided by Account Reset Console also helps organizations meet FERPA, HIPAA, PCI, and other regulatory compliance regulations. Most industries now face compliance requirements that include periodic password changes, auditable access trails, and strict controls for users with access to internal data. Account Reset Console lets companies maintain compliance with these standards. Oversight control is provided by the product's auditable logs. All successful and failed logon and change requests are recorded to a central file. Scheduled and on-demand reports alert senior management to common account issues across the network, including password reset compliance and the enrollment status of managed users.



Find accounts that have been inactive on the domain, or accounts whose passwords will soon expire.

> *"An organization's Help Desk can be inundated with calls from users asking for password resets. Gartner research estimates that these calls constitute, on average, 30% of Help Desk calls."*
>
> **ANT ALLAN**
> **Gartner, Inc.**
> Best Practices for Question-and-Answer Identity Verification Methods, June 4, 2007

Microsoft GOLD CERTIFIED Partner

CERTIFIED FOR Windows Vista™

RSA SECURED®

1 Microsoft TechNet, "Password Management", M. Baladi, D. Mowers, A. Steven, P. Verwold, June 2006

www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152 | 1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067