



r e a c t

reset **enterprise** access control tool

**Self-Service
Password
Reset Tool
For Your
Entire IT
Enterprise**



According to a study by the Gartner Group, up to 35% or more of the calls to your IT help desk are a result of the end user forgetting his or her password...

Password Reset Process in a typical IT environment...



Costly

35% or more of the calls to your Help Desk are a result of the end user forgetting his or her password. The manual process of resetting a single password represents an average cost of \$38 per incident.



Time Consuming

Help Desk personnel must reset passwords manually.



Security Exposure

Help Desk teams may lack true authentication mechanisms to validate user requests.

Forgotten passwords result in an enormous hidden cost for the corporation. For example, the cost for a large organization receiving 3000 password reset calls per month can be as high as \$1,368,000 each year.



Resetting Passwords

An IT fact of life is that users forget their passwords. After a long weekend, a vacation or any gap of time between accesses systems or applications, passwords are forgotten.

Forgotten passwords typically result in calls to the corporate Help Desk. In fact, according to studies conducted by Gartner Group and the META Group, nearly 35% of all calls to the Help Desk are from users requesting that their passwords be reset. These industry-leading analysts also estimate that it costs businesses an average of \$38 per incident for the manual, time-consuming process of resetting a password.

Forgotten passwords result in an enormous hidden cost for the corporation. For example, the cost for a large organization receiving 3000 password reset calls per month can be as high as \$1,368,000 each year (3000 calls x \$38 per call x 12 months).

The forgotten password problem increases exponentially in organizations with a multitude of distinct operating systems and distributed applications that continue to grow and evolve. For instance, while a user may request a password reset from the Help Desk team for the RACF application they need to access today, another call will be made to the Help Desk for the Windows or Novell system they need to access tomorrow.

In the midst of password amnesia, the corporation is faced with several security exposures:

- Passwords between the differing systems and applications remain unsynchronized, often resulting in even greater confusion for the end user that, in turn, results in even more calls to the Help Desk.
- Passwords reset by the Help Desk are typically set into a temporary mode that require the user to devise a new name that may or may not meet corporate standards. Either way, it creates another step in the process as well as another opportunity for confusion and/or amnesia.
- Help Desk teams typically lack true authentication mechanisms to validate user requests. This provides an unauthorized user with the ability to request a password reset that will subsequently enable them to access systems.

The forgotten password problem has always existed but has worsened and increased over time, as a greater number of users, business partners and even customers, require access to more systems than ever before. Corporate initiatives such as B2B, B2C, e-commerce, Web-enablement and others will continue to expand the problem.

Reducing the costs and the security exposures inherent with the forgotten password problem is made possible through user self-service employing mechanisms that securely authenticate users, reset and synchronize passwords across the enterprise, while leveraging the power and control of existing security systems. That solution is named ReACT, the Reset Enterprise Access Control Tool from Advanced Software Products Group, Inc.



The Solution

ReACT is a non-invasive, self-service, centralized tool that provides users with the ability to simultaneously reset and synchronize all of their passwords for all of the systems and applications they are authorized to access. With user self-service capabilities, ReACT helps eliminate password reset calls to the Help Desk.

ReACT helps close the security exposures opened by a forgotten password. It securely authenticates user requests for a password reset and then establishes a permanent, immediately-usable password on all effected systems. ReACT eliminates the need to reset passwords to a temporary value.

ReACT interoperates with, and supplements, existing security systems. While passwords and naming standards remain under the control of each individual security tool, ReACT maintains a database of users, systems and applications, and authentication mechanisms. In addition, ReACT allows for password rules above and beyond what the target systems require. ReACT does not maintain passwords and ensures that security control remains in the realm of the established security systems. ReACT helps organizations ensure that existing password naming conventions are employed whenever passwords are reset throughout the enterprise.

ReACT provides security professionals, Help Desk teams and corporate Auditors with additional information security assurance by logging and reporting all activities related to a password reset. It captures user information when a reset is requested, logs all successful or failed authentication activities as well as any successful or failed password reset activities. Additionally, ReACT has the ability to provide automated alerts to responsible personnel for specific events, such as a consistent reset failure or perceived attempts at hacking.

The Architecture

ReACT is comprised of four major components that enable the product to operate as a centralized solution, seamlessly interoperating between users and security systems.

ReACT Server - Supports all of the ReACT functionality and interfaces with all components. The ReACT Server resides on any Windows Server.

ReACT Database - Contains all of the associations between userids, challenge questions and operating systems.

ReACT Administration Tool - Provides the ReACT Administrator a well-known interface for interacting with the product.

ReACT Web Portal - The ReACT Web Portal provides the web based user interface with customizable user screens.

- **Web based user interface**
- **End users can securely reset their own passwords**
- **Eliminates the need to reset your password to a temporary value.**
- **Scans all of the target systems to be reset and builds a database of users and resources**
- **Supports virtually all enterprise operating systems and applications including RACF, Novell/NDS, Windows domain, Windows Active Directory, and more.**
- **Custom scripting engine for building extensions for other systems and custom applications**
- **Straight-forward, secure authentication process**
- **Minimal learning curve: Only 4 screens for end users**
- **Does NOT override current security controls**
- **The ReACT Web Portal allows end users to reset/synchronize any of their accounts managed by ReACT**
- **Transparent Background Synchronization module allows the end user's passwords to be synced with all accounts managed by ReACT when the user performs a password change via the normal Windows password change process**
- **Open architecture for integration with other tools for reporting, tracking, auditing, etc.**
- **Quick ROI is usually realized within the first month**

Easy as 1 - 2 - 3 - 4

With ReACT in place, users never again need to contact the Help Desk to reset passwords. Instead, in a simple four-step process, they merely access ReACT, correctly answer the challenge questions and have their passwords reset for all systems they are authorized to access and have selected.

Step 1: "I Forgot My Password"

ReACT is accessed through the Web-browser. The user accesses ReACT by logging on with a kiosk account that has no authority but to execute ReACT.



Step 2: "Is it REALLY you?"

Users are prompted to enter their ReACT userid and provide the correct responses to their unique challenge questions. This functionality authenticates the user to the ReACT system. ReACT does not store any passwords. ReACT userids are defined by the ReACT Administrator and are unique to each individual.



Step 3: Systems Selection

Once the user is authenticated, ReACT provides a display of all the systems to which the user maintains authorized access. This display enables the user to select the system(s) on which they would like to have their password reset. The user can select one system, multiple systems or with a single click, all systems.



Step 4: ReACT Reacts

Following the rules provided for length, case sensitivity, allowable characters, etc., the user simply enters and confirms their new password. A single click puts ReACT to work resetting all of the accounts. ReACT then shows the status of each reset operation through to completion.



**Call today for
a FREE 30-day
evaluation!**



Phone: +44 (0)207 060 6601
Email: sales@e3sciences.com
www.e3sciences.com