Self-Serve Password Reset

ReACT. So your Help Desk doesn't have to.

Lost or forgotten passwords equal lost money. Eliminate password related calls and start saving time and money.

"The resetting of a password was a drain on the Help Desk, but, more importantly, it frustrated their users and distracted them from their primary jobs. ReACT did what it claimed it could do."

- Worldwide manufacturer of construction products

"Not only is ReACT helping us along our intended path, but it is also enabling our Help Desk to grow."

- U.S. sports apparel manufacturer

Password Calls

According to a study by the Gartner Group, up to 40% or more of the calls to your IT Help Desk are a result of the end user forgetting his or her password.

Cost Savings

Gartner estimates about 70% - 90% cost savings from Help Desks that implement a self-serve reset solution.

Compliancy

ReACT can assist with mandate requirements such as PCI compliancy. Ensuring proper user authentication, password management, and verifying user identity before performing password resets can be key to complying with internal, industry and governmental mandates. ReACT also helps facilitate the 90-day password expiration guidelines recommended by Department of Homeland Security, FBI, and NSA.

Password Reset Process in a Typical IT Environment...

COSTLY

The cost in a large organization receiving 2,000 password reset calls per month can be as high as $429,120 each year [2,000 calls x $17.88 per call x 12 months].

TIME CONSUMING

End Users must request a password change and Help Desk personnel must reset passwords manually.

SECURITY EXPOSURE

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

The Product

The Product ReACT™ is a unique application designed to automate the password reset and synchronization process across the entire enterprise. ReACT eliminates the need to reset a password to a temporary value and allows the end user to reset their own password at any time without the need to change their password again at sign-on. ReACT virtually eliminates password reset related calls to the Help Desk.

As part of your identity management protocol, 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 affected systems. ReACT scans all of the target systems to be reset and builds a database of users and resources. Transparent Background Synchronizations allows the end user's password to be synched with all accounts managed by ReACT. As a centralized, enterprise-wide password reset tool, ReACT provides support for virtually all operating systems and applications within the enterprise.

Enterprise Support

AD, z/OS [RACF, ACF2 & Top Secret], Novell/eDirectory, UNIX/Linux [AIX, HP-UX, Datatel], iSeries/AS400, JD-Edwards, Oracle/SQL, LDAP, Lawson, SAP, CAMS, WFM, Gmail, PeopleSoft, AdvantX, Office365 and more.

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 and 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 managers for specific events, such as a consistent reset failure or perceived attempts at hacking.

The Dashboard

The ReACT Dashboard allows administrators to audit, monitor and report on user activity. Administrators can view live user activity, snapshots, failures/activities, & administrative activity. Administrators also have the ability to lock & unlock specific ReACT ID's as well as set multiple parameters for automatic unlocking of accounts.

By offering 24x7x365 self-service password reset capability, ReACT can eliminate some of the costly staff-related issues facing the IT Help Desk. For example, colleges and universities face extremely high password related calls at the beginning of each new semester and at off-hours when students do most of their online work. Companies, with offices and clients in different time zones, also face the challenge of adequately staffing their Help Desks around the clock to accommodate password related calls.

Users who have forgotten a password or triggered an intruder lockout can sign into ReACT using other types of credentials and reset their own password. Non-password authentication options include security questions, image recognition, and random PINs sent to a user's mobile phone using SMS or via email. Access to ReACT is available from a PC web browser, Windows login screen, smart phone or mobile web browser. Users can authenticate to ReACT using any combination of the following mechanisms:

- By typing their current password to a trusted Windows/AD system
- By answering security questions.
- By typing a PIN that was sent to their mobile phone via SMS.
- By typing a PIN that was sent to their inbox via email.
- Using a combination of these mechanisms including Image recognition as a second factor.

Although some companies may use a single sign-on [SSO] solution resulting in only one password to manage, they still need to be able to reset the password when it is forgotten. ReACT can be added to an environment without having to make drastic changes to that environment. Implementing SSO usually requires expensive changes in one or many back-end systems. SSO can take years to deploy whereas ReACT can be deployed quickly, usually within 30 days.

Multi-Factor Authentication

Accessible

ReACT provides easy access to end users through a web interface, desktop Windows login screen, secure dedicated kiosk - even via smart phone or tablet. Additionally, the Help Desk maintains the ability to reset passwords for the user.

Secure

ReACT does not override current security controls and policies. End users can authenticate to ReACT using multiple methods of authentication including Challenge Questions, Email, SMS, Image Recognition and Active Directory. ReACT can also enforce a multi-factor authentication approach using the above authentications. An RSATM interface can be used to handle the authentication method, using RSA's challenge questions and answers. ReACT's SOAP interface is designed to ease the mind of the Security Team while allowing for an incredibly quick and simple configuration experience for system and network administrators.

Flexible

ReACT offers unmatched flexibility. With the option to choose multiple authentication methods [including multi-factor authentication], accessibility options, and roll-out options – you're in control. ReACT also provides the ability to customize the ReACT web portal with your branded corporate identity & custom text. Multi-language support includes English, French, Spanish, German, Polish, Japanese, Italian, Russian, Chinese, Vietnamese, Tagalog, Korean, and Portugese.

Easy

ReACT is easy to use for both end users and administrators – zero learning curve. End users can securely reset their password across the enterprise in just 4 screens. Administrators can manage the user accounts quickly and efficiently with the included interactive ReACT Dashboard. ReACT can be fully implemented within 30 days.

Enterprise

ReACT is a true enterprise password reset and synchronization tool providing support for virtually all operating systems and applications within the enterprise. Scripting assistance is provided at no additional cost. Additionally, open architecture allows for integration with other tools for reporting, tracking and auditing.

Reporting

ReACT provides the ability to report on usage, return on investment and problems encountered. All user interaction with ReACT is stored in a SQL database allowing custom reports to be generated.

Enrollment

ReACT's innovative enrollment portal streamlines the end-user adoption process via its user-friendly enrollment wizard. Also provided is the option for the Help Desk to implement automatic enrollment by pre-populating the ReACT database, which results in increased adoption rates throughout the organization. Synchronization automatically adds new users, reconfiguring accounts that can be reset.

Off-line Access

OAR [Offline Access Recovery] provides remote, traveling, and contractual users device access while not connected to any network. OAR securely allows the approved end user to access their device without requiring network access, VPN credentials, or an Internet connection. This innovative solution utilizes a unique two-part confidential code which provides the user with access to a device when an end user is away from the network and has forgotten their login credentials.

Fast Facts

- The ReACT Web Portal allows end users to reset/ synchronize any of their accounts managed by ReACT
- Eliminates the need to reset your password to a temporary value
- Reset cloud based systems/platform
- Free installation, scripting & customization assistance
- Automatic Enrollment to streamline the registration process. Synchronization automatically adds new users, reconfiguring the accounts that can be reset
- BYOD friendly web portal
- Alternate end user email capability
- Tie into any widely used ticketing system
- Self-serve Change Password option based on the user's old password
- Dynamic Password provides a scaling complexity based on password length.
- Only 4 screens for end users
- Does NOT override current security controls
- Transparent Background Synchronization allows the end user's passwords to be synched with all accounts managed by ReACT
- Open architecture for integration with other tools for reporting, tracking, auditing, etc...
- Extensive Help Desk Dashboard to report, audit and monitor user activity / accounts
- Quick ROI - usually within the first month
- Complements your existing structure & offers customization
- Account Unlock feature
- Full implementation within 30 days
- Easy. Zero learning curve
- Dynamic field validation
- Software as a Service [SAS]
- Captcha support
- Click-a-Tel as a Service
- IVR & Biometrics support

Free 30-day Trial: www.aspg.com

800.662.6090 ● 239.649.1548 ● aspgsales@aspg.com

The Architecture

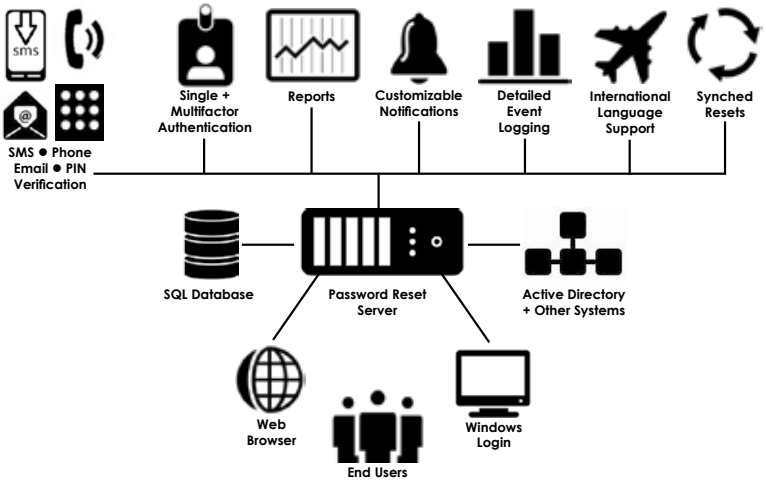
ReACT is comprised of four major components that enable the product to operate as a centralized solution, seamlessly interoperating between users and security systems.

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 platforms/systems.

REACT ADMINISTRATION TOOL: Provides the ReACT Administrator a well-known interface for working with the product.

REACT WEB PORTALS: The ReACT Web-based Portals provide user interfaces for both users & Help Desk. Exclusive Password Administration Dashboard provides LIVE user activity.



Secure Password Reset in 4 Easy Steps

Step 1: "I Forgot My Password" ReACT is accessed through the Web-browser, or optional desktop client. The user accesses ReACT via an account that is secured with Group Policy. It has no authority, but to execute ReACT.

Step 2: "Is it REALLY you?" After users are prompted for their ReACT userid, they must then authenticate to ReACT using 5 possible methods, before being authenticated

Step 3: System 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 indicates reset status.

ReACT. So your Help Desk doesn't have to.

ADVANCED SOFTWARE PRODUCTS GROUP, INC.

www.aspg.com

800.662.6090 ● 239.649.1548
aspgsales@aspg.com

 r1015