

### Smart Account and Password Management

Controlling access with user accounts and passwords, for both physical network and application access, is the most widely adopted security technology to date. One of the major problems with account and password credentials is the ability for users to securely manage them. As each new application or access method is introduced, additional accounts and passwords are distributed to users – forcing them to manage one account and one password for each application they need to access.



Managing too many accounts and passwords creates problems for both users and IT administrators alike. With computer usage policies requiring mandatory scheduled password changes and password policies requiring the use of tough passwords, users often forget their passwords and lock themselves out of their accounts. Administrators and help desk personnel are called on a routine basis to help reset passwords and unlock accounts – raising operational costs and causing unnecessary user non-productivity.

A10 Networks' IDsentry is a network identity management appliance designed to simplify organizations' Identity and Access Management (IAM) infrastructures. The User Self-Help Service within IDsentry reduces costs associated with password resets and account updates by empowering users to manage their own passwords and accounts.

IDsentry provides several key technologies to simplify password resets and automate user account management activities. User Self-Help Service empowers users with the ability to update passwords, reset locked accounts, recover from lost passwords, and change account profile information. Combined with IDsentry's Central Password Policy, Password Synchronization, and Password Expiration Notification technologies, customers can create sophisticated and easy-to-use IAM solutions to maximize efficiency.

Using a standard web browser to service simple but frequent user account and password requests can recover many hours of valuable help desk and IT resources per week. With the ability to change and reset their own accounts and passwords, users are much more productive as non-productivity time caused by locked accounts is minimized.

#### User Self-Help Service Screenshot



### The Need to Simplify

When users are forced to use and remember multiple dissimilar accounts and passwords for all of their business and personal applications, they often get confused as to which passwords are associated with which accounts and applications. To simplify, users often document account and password information on sticky notes or notepads, enter them into unsecured text files stored on cell phones or laptops, use personal passwords for business applications and vice versa, share passwords with friends and family members, and select easy-to-guess passwords – circumventing corporate security policies and increasing risk.

Password Synchronization, the process of migrating users to one user account and synchronizing passwords between the accounts, can help companies mitigate security risks and improve operational efficiency very quickly. With Password Synchronization, users only have to remember one user account and enter one password to access the majority of their applications.

### Hiding the Complexity

With IDsentry, administrators can quickly deploy automated IAM features to offload mundane account and password reset requests that are over running help desks.

- User Self-Help provides an easy way for users to select new passwords, reset locked accounts, recover lost passwords, and change account profile information.
- Central Password Policy enforces password selection to ensure that strong "tough-to-guess" passwords are selected.
- Password Synchronization automatically synchs password changes to all data stores required and reduces the number of passwords users have to remember and manage.
- Password Expiration Notification sends customizable email reminders to help users select new and secure passwords.
- Custom Forms provide administrators the ability to limit the information displayed on the Self-Help portal and enforce which attributes are modifiable by end users.

## Return-on-Investment

Businesses of all sizes can realize the benefits of Identity & Access Management with just a few IDsentrie features enabled. According to many independent analyst firms, such as IDC and The 451 Group, user account and password resets can easily account for 20 to 30% of total help desk volumes. By empowering users to self-service these requests, businesses can recover large amounts of IT and help desk resources and eliminate user non-productivity.

IDC estimates that each account or password reset request costs companies an average of \$30 to \$70 USD per resolution, depending on the help desk's geographical location and wage scale. A big part of the monetary cost is due to user non-productivity as users sit idle waiting for their accounts and passwords to be reset.

## ROI Example

ABC Company employs 1500 users around the world and uses three separate data stores (LDAP, Active Directory, Linux) to control access to their network and business applications. Each employee uses one account on each data store to conduct business. To enforce the company's Computer Usage Policy, administrators enforces tough password selection and rotation on each of the three data stores every 90 days (once per quarter) and users cannot use previously selected passwords. Currently, ABC Company does not use any IAM productivity tools and performs manual account provisioning to each of the three data stores.

The company will use an average of \$50 to calculate the cost per incident. The cost per incident takes into account the time a user takes to log a trouble-ticket with the help desk dispatch, the time taken to dispatch the ticket to a technician, the technician's time to resolve the problem, the technician's time to close the trouble-ticket in the help desk system, and the non-productivity time experienced by the user who's account was locked out.

ABC's help desk application has shown a historic ratio with password issues accounting for 30% of the total help desk volume. The system also shows that 25% of their user population generates nearly all of the password help desk tickets – not all users have problems managing their accounts and passwords.

## ROI Calculations

- 1500 users X 3 accounts each = 4500 total user accounts
- 4 mandated password changes per year X 4500 user accounts = 18000 password changes / year
- 25% problematic user base X 18000 password changes = 4500 possible password issues / year
- \$50 average cost X 4500 password issues = \$225K USD spent on password issues / year

ABC's estimated annual cost for password related issues = \$225,000 USD

## Network Identity Management Solutions

IDsentrie is the industry's only appliance delivering integrated features that resolve IP addresses to identity (IP-to-ID) instantly, improve help desk efficiency, simplify user account management, and enhance network authentication and access control. For more information, visit A10 Networks at <http://www.a10networks.com>.

© 2005, 2006, 2007 A10 Networks, Inc. All rights reserved. A10 Networks and IDsentrie are registered trademarks of A10 Networks, Inc. All other trademarks are the property of their respective owners.