Self-Service Password Management
Table of Contents

1. Self-Service Password Management: The Cost-Effective Option 3
   1.1 So Many Passwords, So Little Time... 3
   1.2 Self-Service Reset Utilities 3
   1.3 User Validation 4
   1.4 The Reset Process 4
   1.5 Benefits 5
   1.6 Help Desk 5
   1.7 Compliance 5
   1.8 Strategic Service and Best Practices 6

2 Conclusion 6

3 About Netwrix Corporation 6
Self-Service Password Management: The Cost-Effective Option

So Many Passwords, So Little Time...

In today’s complex IT environments, users typically have multiple passwords to manage for a variety of applications or access levels. 80% of all users have 3 or more passwords to manage, but many more are possible depending on their system access needs. Users end up jotting passwords on note paper, thus threatening the security of the system, or they are simplifying life by reusing passwords or choosing weak ones where the system permits, even though these are unsafe security practices.

Meanwhile, security-minded IT organizations often implement strong password measures which inadvertently add to the burden, requiring users to recall complex formulations and change them frequently. Compliance with auditing and regulatory requirements, such as Sarbanes-Oxley and HIPAA, further tighten the password security net and in turn, further confound the user.

Quite simply, password practices that improve security are by their nature burdensome to the user, resulting in passwords difficult to remember which are often changed about the same time they have finally become memorized. Yet password security remains a cornerstone of system security: as much as 80% of security breaches take place not through arcane hacking and virus attacks, but through system infiltration facilitated by use of a password.

It remains in the best interests of the organization to have strict password requirements that mitigate against system access by hostile parties. These are also the kinds of passwords best designed, it seems, to be forgotten by busy and distracted users.

Given this environment, it is no surprise that industry analysts find that 30% of all help desk calls across the industry are about password issues, at a cost averaging $30 to $60 per call. This support cost when multiplied across an organization can be huge. While necessary to system security, troubleshooting passwords is a large time sink for system administrators or help desk staff. This low-level, repetitive activity siphons valuable support resources away from higher-priority or more productive tasks.

Self-Service Reset Utilities

The solution that has evolved for this problem is the self-service password reset utility. At their simplest, products of this sort enable the user to reset a password or clear an account lockout independently of the help desk, typically through a browser-based portal. Some versions of this product require that users first find a browser to use, which they are unable to do at their desktop, because they cannot log into their system and gain access to their own browser.

A common solution to this problem is for the user to access a special kiosk system installed nearby in the workplace, or to interrupt a colleague for a few minutes to use his or her computer for a few minutes. The better designed reset utilities are activated by a link from the user’s logon prompt, so the individual can proceed with their troubleshooting from their own desk. Self-service reset products validate the user as someone authorized for
access to the system. Then the user is walked through a password change dialog that instantly resets their password and unlocks their account if needed without further intervention from the help desk.

User Validation

Most reset products validate the user via the data previously set up by the user. Typically, the user will have answered multiple personal questions such as favorite pet's name or street lived on, and one or more of these questions are presented to the user by the reset utility.

To guard against unauthorized access attempts, the more advanced reset systems can be set to lock out someone repeatedly entering incorrect answers to these validation questions. The questions are generally pre-selected by the system administrator who set up the reset product, although some allow the user himself to choose what questions he prefers to answer.

To load a propel database with user information, an IT department usually introduces the self-service solution to end users with an email and one-click links to the process. Yet no matter how many admin emails are sent out, some portion of users will fail to set up a password profile if it is a voluntary process. This issue can be avoided with profile preloading, in which an organization may load the profile database with HR data such as SSNs or mothers' maiden names.

In this manner, users will have their profiles already established even if they have never used the system before. Another way around this user roadblock is to employ enforced enrollment: some reset products can be set up to require all users to establish their verification profiles during an initial logon.

Less commonly, some systems require telephone voice verification, or offer biometric validation of the user's identity. Approaches such as biometrics offer an extraordinary degree of security in certain settings, such as, for example, where access to sensitive R&D work or business intelligence is guarded.

The trade-off for that degree of security is the additional expense of the biometrics system, and the additional administrative burden of mapping biometrics for a changing user base. This may be worthwhile in some relatively static places of employment, but in settings such as educational institutions or the shifting population base of e-business, biometrics are as yet an impractical tool to use with a remote or changing user population.

Validation data must be stored somewhere, and some solutions utilize Active Directory for this, either with or without schema extension. However, this is not a recommended practice for data integrity, since AD is not designed to be a catch-all space to load proprietary data from different vendors. Better-designed products store sensitive data in secure local storage and never touch Active Director or alter schema.

The Reset Process

Once the user is validated, a dialog prompts for the creation of a new password. This password is checked against password construction rules that have been established by IT management. Parameters such as necessary
alphanumeric combinations, length, and whether or not the word has been used within a past timeframe are checked.

When a valid password has been created that conforms to system requirements, the utility automates the reset process within the network operating system, eliminating the need for the hands-on administration that is a multi-step process when done manually. If an account has been locked, that lockout is also cleared, and the user is free to log in once more with the new password.

**Benefits**

The immediate benefit of a self-service password reset is that users can resolve their problems themselves and get on with their tasks without having to wait for help desk service. It is quick, easy, and convenient to use, and can be employed at any time of the day or night, regardless whether IT support staff is present or not. User productivity is increased, for there is no down-time while waiting to re-gain systems access.

And while an improved user experience and higher satisfaction certainly have value, even more advantages accrue to the organization from the IT management point of view.

**Help Desk**

Self-service password reset systems offer immediate payoff at the IT help desk. In some shops, the overall volume of calls may be reduced by 30%, freeing up expensive IT resources for more vital tasks. In other shops, where there are often wait queues on the phone or a high volume of call-backs needing service, the help desk is able to focus more exclusively on technically significant issues – i.e., matters that have a correspondingly greater impact on user productivity. While the latter is more difficult to quantify, the impact of the former can be tracked by simple ROI calculators that reckon the labor costs saved by reduced call volume alone.

**Compliance**

Another benefit to password reset automation comes in the improved ability to comply with HIPAA, Sarbanes-Oxley, and Gram-Leach-Bliley. The auditing requirements of these regulations demand that an organization be able to maintain secure access to data, and track who has what access when. Password management solutions are a simple way to facilitate this, since they can create extensive audit trails to track and analyze all password changes and usage in the system. Because these solutions manage password complexity rules, they also help enforce password policies established to meet compliance requirements.

From the human management standpoint, once users can easily resolve access problems, it is easier to get them to comply with password practices and to maintain higher security standards throughout a system. In the end, the organization is in better compliance with legal requirements for access and security, and costs are reduced by the automated tracking and reporting of audit information.
Strategic Service and Best Practices

Organizations that use best-practice frameworks such as COBIT or ITIL will also benefit from the use of a self-service password reset solution. Help desk or service desk management plans must take into consideration where and how resources are allocated to perform necessary tasks. A simple product that frees up 30% of the low-level activity of a help desk is a powerful solution for the strategic management of IT resources. When incorporated into a best practice service strategy, a solution of this sort may offer unexpectedly large benefits in the long term.

Conclusion

The self-service reset of forgotten passwords and account lockouts offers cost-effective management of the most common user problem in virtually every IT-using organization. Netwrix Password Manager offers a self-service solution that incorporates the best of the reset solution design features. Easy to use and simple to deploy, Netwrix Password Manager allows for database preloading of user validation information so users with problems can be self-assisted from Day 1.

The product can be configured for enforced enrollment, guaranteeing that all users will go through the validation information process before logging on to the network. Netwrix Password Manager partitions its data management cleanly, storing sensitive information in a local secure database and enabling resets without making alterations in Active Directory schema.

Netwrix Password Manager uses a Windows Logon Extension to give users a self-help link to follow from a failed logon: users do not need to seek out a functioning browser, but can continue their problem-resolution at their desktop. In the occasional instance where a user may not be able to help themselves – when, for example, they have forgotten their verification answers – the Netwrix product includes the help desk portal.

This connection is part of a common framework for making password resets according to established password policies. This pre-qualifies the exact nature of a user's problem and improves help desk efficiency when assisting with the reset problem. Download a free 20-day trial of Netwrix Password Manager to see how Netwrix can help you deal with forgotten passwords and account lockouts.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solutions with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.