Password Self Service: Beyond Mother's Maiden Name

Businesses are increasingly moving to the cloud and that poses a sterner password management challenge to both the IT admins and the end-users. This article discusses the pre-requisites a self-service solution for password management must have to verify and secure users' identities

– Radhakrishnan A, ManageEngine

Today's business environment is dynamic, highly competitive, and laden with security threats. Events like the iCloud celebrity photo hack and the hacking of SONY's corporate network have businesses and their IT departments on their toes. Whenever the term 'security threat' pops up, the first and foremost step taken is to ensure the safety of passwords. There is no better way to secure a password than by enforcing stringent password policy rules.

As long as employees have to remember a multitude of complex passwords, they will keep forgetting them. According to Gartner, 20-50 percent of all calls made to the help desk are related to forgotten passwords and account lockouts. Additionally, employees' productivity is affected because they can't log on and do work. According to Forrester Research, the average cost of a single password reset done by help desk is about $70. Obviously, you can't sacrifice password security to combat the huge volume of password-related help desk calls.

This conundrum demands a solution that ensures the security of password while also freeing help desk team from their workload. And thus, we now have many self-service password management solutions in the market. Like banks, which have empowered their customers with self-service for various tasks to reduce costs, many businesses have deployed self-service solutions to manage password related issues and reduce costs. However, traditional self-service solutions - where end-users go to a web portal, answer some challenge questions, and reset their passwords – are not effective in today's environment. What you need is a password self-service solution that is capable of adapting to both the current and future needs of your business.

This article discusses how the changing business needs may affect the effectiveness of a password self-service solution and provides a guideline to identify the right solution.

Radhakrishnan A.
ManageEngine

"In addition to the multi-factor authentication techniques, there are other security features that you should look for in a password self-service solution like SSL support and option to enforce password policies"

Factors affecting the effectiveness of password self-service solutions

Introducing password self-service within an organization will have a positive impact on the business by reducing the workload of the help desk and costs associated with password management. However, finding an effective password self-service solution is not that simple. There are certain factors that determine the effectiveness of a password self-service solution: user adoption, accessibility, multi-platform support and security.

A self-service solution which has low user adoption is bound to have no effect in reducing the help desk calls. The effectiveness of a password self-service solution is directly proportional to how many users are using it to solve their password problems themselves. No matter how powerful a self-service solution is, low user adoption means calls to the help desk will continue unabated.

Another factor is accessibility. With the popularity of the "bring your own device" trend in the enterprise, users are no longer confined to their desktops and laptops. End-users accomplish many official tasks using just their mobile devices. A self-service solution that can only be accessed via a computer would be of no use to users who are always on the move and have only their mobile devices to do their official tasks. Without easier ways to access, a self-service solution would be of no help in dissuading users from calling the support staff for help.

Then there is the issue of managing users' identities across multiple platforms. Businesses are increasingly moving to the cloud and that poses a sterner password

management challenge to both the IT admins and the end-users. IT admins are now in charge of managing users' identities on multiple platforms such as Office 365, Google Apps, and Windows Active Directory. Users are also affected by "yet another username and password" syndrome. A self-service solution that supports only Windows Active Directory would severely limit its effectiveness in a hybrid environment.

Finally, the most important factor is security. Considering that we are dealing with passwords, a self-service solution for password management must have highly secure and foolproof authentication methods to verify users' identities. Only those users who have proven their identities should be allowed to reset their passwords or unlock their accounts. Additionally, the solution must have measures to tackle common security threats such as bot-based attacks and data theft during transmission.

Choosing a perfect password self-service solution

There are a number of ways you can address the challenges discussed above. Be sure to keep the following in mind when you are in the market hunting for a password self-service solution

Multiple access points

No matter where a user is and what device one is using, it's imperative for a password self-service solution to be readily available to the user. Having multiple access points other than the de facto web-based portal could solve the problem of accessibility. For example: login agents for different systems and applications, as well as mobile apps, will help. With login agents, users can easily access the self-service portal from the login screen of their Windows or Mac machines and reset their passwords.

Not just Windows or Mac, a self-service solution should be flexible enough to be integrated with some of the commonly used applications in a business environment like Outlook Web Access and SharePoint. Mobile apps for password self service would be even more flexible and easy to use. Users will have full freedom to reset their passwords or unlock their accounts remotely from anywhere, at anytime they want with password self-service mobile apps.

Automate or force user enrolment

Enrollment is the process by which users sign up with the password self-service solution by providing certain information. This information will be used to verify their identities when they request password resets or account unlocks. However, in most cases, users would not be aware of such a process, or they are simply too lazy to go through the steps involved. To facilitate enrollment without users' intervention, an option to auto-enroll users by importing their enrollment data from a database or a CSV file is compulsory. Also, an option which forces users to enroll at the time of system login by blocking access to their desktop would ensure an even greater success rate.

Multi-platform support and password synchronization

Whether you have Windows or Mac machines, an on-premise or cloud-based environment, a password self-service solution should support a wide range of most commonly used IT systems and applications. A password self-service solution that supports only Windows machines would still result in password related help desk calls from Mac, Google Apps, and Office 365 users.

What you need in such a case is a solution that supports multiple platforms and is capable of automatically synchronizing password changes across users' various accounts. As the users reset their passwords for any one of their accounts, the new passwords will be automatically synchronized across all the associated IT systems and applications.

Secure multi-factor authentication

Look for a self-service solution that has more than one form of authentication technique to verify users' identities. Though asking users to answer challenge questions is widely used even today, it is not reliable as the boundaries between personal and public information become increasingly blurred in the age of social media. Ensure security by combining the challenge and response verification method with other authentication techniques such as Google Authenticator; SMS- and email-based, one-time passwords; and RSA SecurID. In addition to the multi-factor authentication techniques, there are other security features that you should look for in a password self-service solution like SSL support and option to enforce password policies.

The importance of keeping reports and audit trail

Keeping track of all user actions is highly important to find any misuse of the password self-service solution. Reporting on all password self-service actions; sending notifications as soon as users perform password resets or account unlock; notifying administrators and managers about locked out users and soon to expire password users; and other tracking features will help you take preventive actions before a serious problem occurs.

Empowering end users to manage their passwords on their own can save you a lot of money . For that, you need an effective password self-service solution that can adapt to the changing needs of business. In addition to the above discussed points, you should also evaluate a password self-service solution based on the customization options it offers, availability of non-password-related self-service features, and pricing. □