

White Paper

Password Management with Passpro

Table of Contents

Password Management with Passpro

Introduction	3
Passpro Password Self-Reset Benefits for End-Users	4
Passpro Password Security Management Administrator Tools	5/6
Conclusion	7
About Pacific Coast Information Systems Ltd.	8
About Boonbox	8

Introduction

Password self-reset and better password policy enforcement are password management objectives that have the potential to significantly reduce IT costs for organizations while improving productivity.

It is now common practice for employees with any type of organization to use passwords to prevent data loss and security breaches. However, the rising number of applications for which employees must create passwords, combined with an increasing amount of complexity in those passwords, has made fast and secure password reset a prized capability for larger organizations.

Industry analysts estimate that each password reset helpdesk call in an office could cost \$70 per call. If everyone in a workplace has to call a helpdesk to reset their password just a few times a year, then organizations can reap cost savings worth several hundred thousand dollars annually from investing in Passpro (Boonbox White Paper: "The Return On Investment (ROI) For Passpro").

Passpro is a boxed service password reset business solution from Boonbox, a division of Pacific Coast Information Systems Ltd.

This white paper will outline the benefits of Passpro for end-users and administrators to lower IT costs while improving productivity. Two of its important benefits are:

Passpro allows users to manage and reset passwords themselves.

Passwords policies can be managed by administrators to ensure a secure IT environment.

Passpro Password Self-Reset Benefits for End-Users

Passpro is an application which allows users to reset their own (Active Directory) passwords. This eliminates the need for a helpdesk to service these requests when a user forgets their password.

Passpro provides a number of user benefits:

A. Reduced use of IT staff and resources.

Users can reset their password without having to wait until the helpdesk or system administrator can service their requests.

Once a user has enrolled with Passpro, resetting a password is simply a matter of clicking a "forgot password" link on the Passpro logon dialog box and answering a series of challenge questions.

This convenience will significantly reduce the number of calls to your helpdesk.

The return on investment through cost-savings can be very impressive for an organization with several hundred employees. Password resets and user ID issues are responsible for about 30 per cent of all helpdesk calls. Using Passpro these calls will be reduced close to zero. Cost savings may accrue on the scale of tens of thousands or even hundreds of thousands of dollars.

B. Improved productivity.

As Passpro users can reset their password without having to wait for the helpdesk, there is a reduction of user downtime. It bears repeating here that the cost of a helpdesk call is not just for the use of helpdesk resources, but also diversion of the user's time while they are locked out of the organization's network.

C. Improved security for users.

Security is improved by eliminating possible helpdesk errors. Furthermore, as employees will not have to write down passwords, security threats such as password guessing and break-ins will be minimized.

Passpro Password Security Management Administrator Tools

Passpro gives administrators a varied toolkit of password management capabilities to ensure security:

1. Set rules for a minimum and maximum number of characters allowed in a password.
2. Enforce combinations of letters and numbers.
3. Force mandatory password resets on a scheduled basis.
4. Define challenge-response credentials.
5. Set number of grace log-ins allowed after password has expired.

This section describes each benefit in more depth.

A. Setting Minimum and Maximum Number of Allowed Characters

A password that is too short may be easier for an ID thief or maliciously-motivated insider to guess or discover. Meanwhile, a password that is too long may be more likely to be forgotten.

There is no definitive number of characters in a password that provides the perfect balance of security and ease of use. Passpro allows administrators to set minimum or maximum numbers of characters in passwords to comply with the organization's unique standards and environment.

B. Enforcing Combinations of Numbers and Letters

Passwords consisting solely of numbers or entirely of letters may be easier for intruders to crack. Without rules enforcing combinations of numbers and letters, employees may be tempted to use easier-to-guess passwords like personal phone numbers or nicknames.

Combining numbers and letters in a non-intuitive series as a password is thought to provide better password security. As well, administrators can ensure users employ a mix of upper and lower case letters. They may even choose to enable special characters such as punctuation marks in a password, or to enable passwords according to the Microsoft complexity policy. Passpro allows administrators to enforce better password procedures for their unique workplace environments.

C. Forcing Mandatory Password Resets on a Scheduled Basis

Passwords can and do get compromised. Even worse, if a malicious intruder takes no action that would alert the victim such as altering emails or documents, the intrusion may go on indefinitely. Forcing mandatory password resets is a proactive and simple solution to ensure that if security breaches have occurred, the damage of an intrusion may at least be contained within a shorter time frame. Passpro allows administrators to force regular mandatory password reset.

D. Defining challenge and response credentials

Challenge questions allow unauthenticated users who have forgotten a password to authenticate another way. Requiring ID challenge questions increases security, as a user must prove their identity by giving correct responses before receiving a forgotten password or setting a new one. Passpro allows administrators to use this valuable security protocol.

E. Setting Number of Grace Log-Ins Allowed After Password Has Expired

Depending on security needs, administrators may choose to allow one or more log-ins after a password has expired in order to facilitate ease of use for employees. Passpro allows administrators to set this number of log-ins.

Conclusion

The self-password reset and password security management features of Passpro provide organizations with powerful tools to reduce IT costs while improving workplace efficiency and security.

Employees benefit from password-self reset through ease of use, better productivity and better security. Employees are empowered by having quick access to the tools and information they need to do their jobs. The ability of employees to reset their own passwords quickly and easily prevents needless waste of helpdesk resources on menial but costly tasks.

As well, the wide range of tools for administrators to enforce better password procedures puts better data control and security instantly within reach of any organization that uses Passpro.

Passpro offers an efficient and cost effective password management solution for organizations looking do more with less.

About

Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS provides technical assessment & services, business analysis, and IT project management. More information about PCIS can be found at www.pcis.com

Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox specializes in productivity solutions that deliver immediate results in support of business challenges like security compliance, password protection and data backup issues. More information about Boonbox can be found at www.boonbox.net