Enforcive Password Self Service (PSS)

for IBM i, Windows, Linux, AIX and Open LDAP

Overview

Passwords are the most common form of authentication used to control access to information. Businesses use passwords because they are a well-known, convenient, and inexpensive authentication mechanism. Yet, the problem with passwords is that they are only as strong as their human creators. Organizations may have hundreds or thousands of password-protected accounts and only one needs to be compromised to create significant data vulnerability.

To mitigate this vulnerability, Security Officers need to enforce strict guidelines on users when creating passwords or resetting passwords when they are forgotten. Security Officers also need to audit password activity with alerts and automated system responses to any suspicious activity.

Organizations most often depend on their helpdesk professionals to assist and oversee routine password maintenance. Many organizations that have implemented procedures to streamline and automate password management still require helpdesk teams to manually respond to each request in some capacity, whether it's answering a call to receive the request or closing a ticket. This is a costly misuse of the value helpdesk professionals bring to an organization.

Enforcive Password Self Service (PSS) streamlines password management into an autonomous process that enables end-users of IBM i, Windows, Linux, AIX, and Open LDAP to securely manage their passwords independently. End-users who do not remember their password for a particular system or want to synchronize a new password across all or select systems can now be given the ability to do so instantly on their own – without escalating to the helpdesk.

Key Benefits

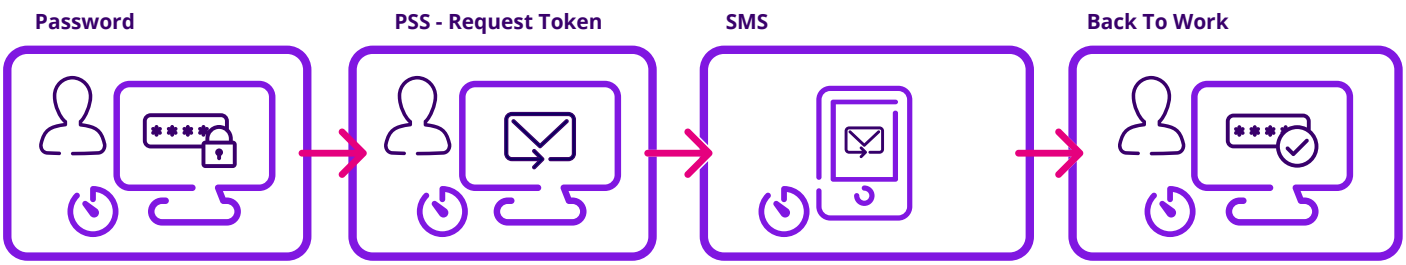
Enforcive PSS Helps Your Organization:

- Offload administrative password management procedures from helpdesk teams
- Improve security through highly customizable user identification processes
- Enforce password criteria and expiration interval controls
- Synchronize new passwords across multiple systems and platforms
- Maintain an audit trail of password reset activity

Figure 1: CPSS Solution Guide - Set Up

How It Works

Password management is conducted through a web-facing portal that guides the user through a three-step process that is both user-friendly and highly secure. PSS uses secured SSL-3 protocol to maintain the privacy of conversations with the authentication server, which can be on a private network or on a secured cloud. Non-password authentication options include security questions and a randomly generated token sent to the user by email or SMS. A user can also authenticate to another server.



Simple Setup

From a single interface, Security Officers simply select the identification mode to implement for particular users or user groups (the list of active users and user groups automatically populates from the User Management module). Security Officers can then define password criteria (e.g., length, special characters) and expiration intervals according to the policy they desire. Rules for password criteria can be defined so that they meet system-specific requirements across all available platforms. A full audit trail of user password management activity is available for Security Officers and auditors.

6 Implementation Types*:

- Windows Active (Directory Direct or via Web Portal)
- Windows Server (via Web Portal)
- IBM i (via Web Portal)
- Linux (via Web Portal)
- AIX (via Web Portal)
- Open LDAP (via Web Portal

* Implementation types can be combined