



SELF SERVICE

ENHANCE YOUR SECURITY
AND REDUCE HELP DESK
CALLS BY 80%

A photograph of three people sitting on concrete steps outdoors. On the left, a woman with long brown hair is looking at a silver laptop. In the center, a woman with long blonde hair and glasses is smiling and looking at a smartphone. On the right, a man with short brown hair and glasses is looking towards the woman with the phone. The background shows a building with a wooden slat facade.

**Say Goodbye To “Forgot Password” Woes!
Say Hello to self-service password reset!**

Overview

Manual password resets are a huge setback not just for the end users, but also for the IT helpdesk. Every password reset costs about \$23 to the IT helpdesk (Source: Gartner). The costs for multiple password resets for thousands of students could skyrocket and become unbearable sometimes. QuickLaunch Password Manager empowers the end users to reset their passwords on their own without any intervention from helpdesk. The users can reset and retrieve their passwords anytime, anywhere without having to call the IT helpdesk, thereby gaining quick access to their locked accounts due to forgotten/lost passwords.

Benefits

SELF-SERVICE PASSWORD RESET

Users can reset their passwords on their own without the intervention of IT helpdesk.

BOOSTS IT PRODUCTIVITY

Frees helpdesk for other critical tasks as number of password reset requests going through helpdesk gets reduced.

CUTS ORGANIZATIONAL COSTS

As password reset requests going through helpdesk reduces, organizational spent on IT reduces.



Key Features

RECOVERY BY EMAIL

Recover passwords through the use of email (primary/secondary)

MULTIPLE ACTIVE DIRECTORY SUPPORT

You can add multiple Active Directories depending on your requirements

EXPIRY NOTIFICATIONS

Set and manage password expiry notifications to facilitate updating of passwords

SMART HELPDESK

Ability to trigger Password reset email and SMS to an AD user

RECOVERY BY PHONE

Recover passwords through the use of phone or email (primary/secondary)

ROLE BASED FACTOR SUPPORT

Admin can configure factors based on roles defined

CONFIGURE PASSWORD POLICIES

You could draft & publish guidelines and policies for password setting so that your users can set strong passwords that are hard to crack

POWERFUL REPORTING & ANALYTICS

Get insightful & actionable insights on who are your users, apps they're accessing and more

RECOVERY BY SECURITY QUESTIONS

Pick from our pool of questions or set your own questions for recovery

CONFIGURABLE FACTOR SUPPORT

Enterprises can define their own factors

BRANDING

Deliver a seamless user experience through our custom branding capabilities.