Password Reset for Locked Out Users

1 The Problem

Users sometimes forget their primary PC login password or trigger an intruder lockout. It is desirable to enable these users to access self-service to resolve their problem, but there is a catch: they cannot sign into their PC so cannot access a conventional web browser or other PC application. How then can they access self-service?

The technical challenge is how to connect users to a self-service mechanism from a pre-login context. The mechanism offered must be evident (or users won't find it), easy to use and secure.

There are three contexts that complicate this problem:

1. When a user is locked out of the OS login screen; and
2. When a user is physically off-site; or
3. When a user is unable to unlock the encrypted drive of his PC, at a pre-boot password prompt.

2 Solution Alternatives

When users forget their OS login password or trigger an intruder lockout, they are in a Catch-22 situation: they cannot log into their computer and open a web browser but cannot open a web browser to fix their password and make it possible to log in.

Hitachi ID Password Manager includes a variety of mechanisms to address the problem of users locked out of their PC login screen. Each of these approaches has its own strengths and weaknesses, as described below:

	Option	Pros	Cons
1	**Ask a neighbor:** *Use someone else's web browser to access self-service password reset.*	• Inexpensive, no client software to deploy.	• Users may be working alone or at odd hours. • No solution for local passwords or mobile users. • Wastes time for two users, rather than one. • May violate a security policy in some organizations.

	Option	Pros	Cons
2	***Hitachi ID Login Assistant*****:** *Extends the login screen of Windows systems*	• User friendly, intuitive access to self-service. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection). • Works on Windows Terminal Server and Citrix Presentation Manager.	• Deployment of client software to every PC.
3	**Secure kiosk account (SKA):** *Sign into any PC with a generic ID such as "help" and no password. This launches a kiosk-mode web browser directed to the password reset web page.*	• Simple, inexpensive deployment, with no client software component. • Users can reset both local and network passwords.	• Introduces a "generic" account on the network, which may violate policy, no matter how well it is locked down. • One user can trigger an intruder lockout on the "help" account, denying service to other users who require a password reset. • Does not help mobile users.
4	***Hitachi ID Mobile Access*****:** *Deploy a mobile app, combined with a proxy server in the cloud, to allow users to access the password reset system from their smart phone.*	• Secure and convenient.	• Does not help with passwords cached on the user's PC, which are not affected when the user's domain password is changed without connection to the PC.
5	**Telephone password reset:** *Users call an automated system, identify themselves using touch-tone input of a numeric identifier, authenticate with touch-tone input of answers to security questions or with voice print biometrics and select a new password.*	• Simple deployment of centralized infrastructure. • No client software impact. • May leverage an existing interactive voice response (IVR) system. • Helpful for remote users who need assistance connecting to the corporate VPN.	• New physical infrastructure is usually required. • Users generally don't like to "talk to a machine" so adoption rates are lower than with a web portal. • Does not help mobile users who forgot their cached domain password. • Does not help unlock PINs on smart cards.

3 Solutions Using Password Manager

Of the above solutions, the first three require no special software. Hitachi ID Systems offers software for each of the remaining alternatives:

	Option	Hitachi ID Systems Software Offering	Notes and Recommendations
1	Mobile Access	Reset the password using an app on the user's phone.	A proxy server, hosted in the cloud, must broker communication between the user's phone, which is connected to the public Internet and typically has no VPN connection and the on-premises *Hitachi ID Password Manager* server.
2	*IVR password reset*	Either extend the call flow in an existing IVR system or deploy *Hitachi ID Telephone Password Manager*, included with *Password Manager*, to allow users to reset forgotten passwords via phone call. Authentication may be via touch-tone input, speech to text or biometric voiceprint matching.	This mechanism is especially helpful to reset forgotten PINs to OTP tokens, which are often used to sign into the VPN.
3	*Domain secure kiosk account (SKA)*	Allow users to sign into their network-attached PC with a generic domain account, such as "help" (typically with no password). Launch a kiosk-mode web browser instead of the Windows desktop, to connect users to the password-reset system.	Two drawbacks: the user must be on-premises and a generic account is created on the network. One advantage: easy to deploy.
4	*Credential Provider (CP)*	Adds a new tile to the Windows login screen, used to launch the *Login Assistant*, which enables access to self-service for locked out users.	Very popular, especially with VPN integration to support off-site users.

4 Choosing the Right Solution

Ultimately, the choice of technology and business process solutions to the “locked out of login prompt” problem is up to Hitachi ID Systems customers. *Hitachi ID Password Manager* technology supports every technically possible solution.