Password Reset for Locked Out Users

1 The Problem

Users often forget their initial network login password or inadvertently trigger an intruder lockout. These users should be able to get assistance, reset their network or local password, clear intruder lockouts and get back to work.

Since these users have a problem with their workstation login, they cannot access a conventional web browser or client/server application with which to resolve their problem. The problem these users face is how to get to a user interface, so that they can fix their login problem and subsequently access their own workstation desktop.

This problem is especially acute for mobile users, who use cached domain passwords to sign into their workstation and who may not be attached to the corporate network when they experience a forgotten password problem.

2 Solution Alternatives

When users forget or lock out their primary password, 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 locked out users. Each of these approaches has its own strengths and weaknesses, as described below:

	Option	Pros	Cons
1	**Do nothing:** *users continue to call the help desk.*	• Inexpensive, nothing to deploy.	• The help desk continues to field a high password reset call volume. • No solution for local passwords or mobile users.
2	**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
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 a lockout on the “help” account, denying service to other users who require a password reset. • Does not help mobile users.
4	**Personalized SKA:** *Same as the domain-wide SKA above, but the universal “help” account is replaced with one personal account per user. For example, each user’s “help” account could have their employee number for a login ID and a combination of their SSN and date of birth for a password.*	• Eliminates the “guest” account on the domain, which does not have a password.	• Requires creation of thousands of additional domain accounts. • Requires ongoing creation and deletion of domain accounts. • These new accounts are special – their passwords do not expire and would likely not meet strength rules.
5	**Local SKA:** *Same as the domain-wide SKA above, but the “help” account is created on each computer, rather than on the domain.*	• Eliminates the “guest” account on the domain. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection).	• Requires a small footprint on each computer (the local “help” account.
6	**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 IVR (interactive voice response) 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 UI. • Does not help mobile users who forgot their cached domain password. • Does not help unlock PINs on smart cards.

	Option	Pros	Cons
8	**Physical kiosks:** *Deploy physical Intranet kiosks at each office location.*	• Eliminates generic or guest accounts. • May be used by multiple applications that are suitable for physically-present but unauthenticated users (e.g., phone directory lookup, badge management, etc.).	• Costly to deploy – hardware at many locations. • Does not help mobile users who forgot their cached domain password. • Users may prefer to call the help desk, rather than walking over to a physical kiosk.
9	**GINA DLL:** *Windows XP: Install a GINA DLL on user computers, which adds a "reset my password" button to the login screen.*	• 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.	• Requires intrusive software to be installed on every computer. • Broken installation or out-of-order uninstallation will render the computer inoperable (i.e., "brick the PC").
10	**GINA Extension Service:** *Similar to the GINA DLL, but uses a sophisticated service infrastructure to modify the UI of the native GINA, rather than installing a GINA DLL.*	• 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). • More robust, fault-tolerant installation process than the GINA DLL.	• Requires software to be installed on every computer. • Does not work on Citrix Presentation Server or Windows Terminal Server – only works on personal computers.
11	**Credential Provider:** *The equivalent of a GINA DLL, but for the login infrastructure on Windows 7 and Windows Vista.*	• 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. • More robust infrastructure than GINA DLLs on Windows XP.	• Deployment of intrusive software to every workstation.

3 Solutions Using Password Manager

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

	Option	Hitachi ID Systems Software Offering	Notes and Recommendations
1	*IVR password reset*	Customers may extend an existing IVR system, using the Hitachi ID Password Manager remote API (application programming interface) (available as Windows DLL, ActiveX DLL, SOAP web service or Unix library), to provide password resets. Alternately, Hitachi ID Systems offers two complete IVR server solutions, using either touch-tone input of answers to (numeric) security questions or biometric voice print verification.	IVR password resets are especially useful for mobile or off-site users who forgot their VPN password.
2	*Global SKA (secure kiosk account)*	Technology to create and lock down a global secure kiosk account is included in Password Manager and works with every flavor of Windows workstations, with Unix workstations and with both Windows (NT, AD) and Novell NetWare network operating systems. Users can be made aware of the availability of the SKA login option by using a network policy to replace the default wallpaper image on the login screen with a corporate logo plus instructions. Users may also be made aware of this option by a voice message on the help desk phone system.	This is the easiest to deploy solution – password reset for locked out users can be deployed to every user in a large organization in just a few hours.
3	*One SKA per user*	This is basically the global SKA, where the policy is applied to a security group, rather than to an individual “help” user. An automated batch process is then implemented to automatically provision and deprovision personalized SKA logins – typically one per employee – and to attach these IDs to the SKA security group.	This is a reasonably easy solution to deploy – a large organization can be enabled for locked out password resets in 3–4 days, once a data feed is available.
4	*Local SKA*	A variant of the global SKA solution is available for desktop deployment, as a standard part of Password Manager.	This solution is appropriate when security policy forbids the global SKA or when mobile users must establish a temporary VPN connection in order to reset local or cached passwords.

	Option	Hitachi ID Systems Software Offering	Notes and Recommendations
5	*GINA (Graphical Identification and Authentication library) Extension DLL*	A Password Manager DLL is available, which can be deployed to Windows XP and Windows 2000 workstations. This DLL is inserted at the head of the chain of GINA DLLs and adds user interface elements to the native GINA dialog boxes. Users launch a self-service password reset UI, in the form of a secure, kiosk-mode web browser, using these UI elements. The GINA Extension DLL is compatible with Terminal Services and Citrix servers, as well as normal workstations.	Incomplete or incorrect installation of GINA extension DLLs can make workstations inoperable. Accordingly, Hitachi ID Systems urges its customers to exercise caution and implement effective quality assurance testing with this option, prior to deployment.
6	*GINA Extension Service*	A Password Manager Windows service is available, which can be deployed to Windows XP and Windows 2000 workstations. This service runs in a privileged user context and, at workstation startup time, adds user interface elements to the native GINA dialog boxes. Users launch a self-service password reset UI, in the form of a secure, kiosk-mode web browser, using these UI elements. Unfortunately, this solution approach is not effective on Terminal Servers and Citrix servers.	The service approach is much safer to deploy than a GINA extension DLL, since it does not alter the GINA DLL chain. Nonetheless, an effective testing program is still recommended, for each workstation image.
7	*Windows 7 and Vista Credential Provider*	A Password Manager Windows 7 and Vista Credential Provider is available, which can be deployed to Windows 7 and Vista workstations. This package adds an authentication option to the Windows 7 and Vista login screen, enabling users who forgot their password to launch a kiosk-mode web browser and reset their password.	As with any client software, a robust quality assurance program is required prior to deployment.

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 customers. Hitachi ID Password Manager technology supports every technically possible solution.