

## Self-Service, Anywhere



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Mobile users warned of password expiry</b>	<b>2</b>
<b>3</b>	<b>Reset forgotten, cached password while away from the office</b>	<b>2</b>
<b>4</b>	<b>Unlock encrypted hard disk</b>	<b>3</b>
<b>5</b>	<b>Smart card PIN reset</b>	<b>3</b>
<b>6</b>	<b>Low cost multi-factor authentication using mobile phones</b>	<b>4</b>

## 1 Introduction

Many organizations depend on self-service technologies in general and self-service password reset in particular to lower the cost of IT support by moving problem resolution out of the help desk and into the user community.

Traditional self-service password reset solutions offer a web-based process where a user who has forgotten or locked out his password can identify himself, authenticate with something other than the lost or locked password – for example, by answering a series of security questions – and reset or unlock his password.

Since users who forgot their primary Windows password cannot launch a web browser, two additional user interfaces are commonly deployed – first, a GINA extension DLL (on Windows XP) or a Credential Provider (on Vista or Windows 7) allows users to access self-service from their PC's login screen. Second, an integrated voice response (IVR) system may allow users to reset or unlock their passwords using their telephone.

These solutions have worked well for years, but two important market trends are making them inoperable:

1. Many organizations are deploying full disk encryption. This means that users may forget or lock out the password used to activate their PC, before an operating system even boots up. Self-service in this case depends on key recovery, not password reset.
2. Many organizations have an increasingly mobile and telecommuting workforce. Their users sign into their laptops using locally cached passwords. When the help desk resets a remote user's password, the change cannot propagate to the local cache, so the login problem is not resolved. These users have to physically visit an office and attach their PC to the corporate network before their login problem can be resolved.

This document explains how Hitachi ID Password Manager addresses these important problems and enables modern organizations – who have a mobile and/or remote workforce and who deploy full disk encryption – can continue to realize the benefits of self-service password-reset, PIN reset and key recovery.

To the best of Hitachi ID Systems' knowledge, no other commercially available password management or identity management software is able to address these issues.

## 2 Mobile users warned of password expiry

Problem	Solution	Business impact
Mobile users are not notified by Windows when their passwords are about to expire. Users who infrequently connect their laptop to the office network, instead checking e-mail with a solution such as Outlook Web Access, suffer regular password expiry and require frequent password resets.	Password Manager sends users e-mails warning of imminent password expiry. Users change passwords using a web browser. An ActiveX control refreshes the password on their laptop.	Fewer login problems that cause a work interruption. Lower IT call volume and support cost.

## 3 Reset forgotten, cached password while away from the office

Problem	Solution	Business impact
Laptop users sometimes change their password before leaving the office and may forget the new password when they need to use it while not attached to the corporate network. Without a technical solution, the IT help desk cannot resolve these users' problem until they return to the office. User laptops are rendered inoperable until they return to the office.	A Password Manager client software component allows users who forgot their primary, cached Windows password and cannot sign into their PC to connect to the Internet over a WiFi hotspot or using an air-card. Locked out users can also establish a temporary Internet connection using their home Internet connection or a hotel Ethernet service. Once the user's laptop is on the Internet, Password Manager establishes a temporary VPN connection and launches a kiosk-mode (full screen, locked down) web browser. The user steps through a self-service password reset process and Password Manager uses an ActiveX component to reset the locally cached password to the same new value as was set on the network back at the office.	Forgotten passwords are a major work disruption for mobile users, since they cannot be resolved until the user visits the office. Password Manager allows users to re-enable their laptop in minutes.

## 4 Unlock encrypted hard disk

Problem	Solution	Business impact
<p>Organizations deploy full disk encryption (FDE) software to protect against data leakage in the event that a corporate laptop is lost or stolen. Users with FDE on their PCs have to type a password to unlock their hard disk, before they can boot up an operating system. If a user forgets their FDE activation password – which normally synchronized with their primary Windows login password – they cannot start an OS and their computer is rendered inoperable.</p>	<p>Most FDE packages include a key recovery process at the PC boot prompt. This normally involves a challenge/response process between the FDE software, the user, an IT support analyst and a key recovery server. Password Manager can front-end this process using an integrated telephony option, so that users can perform key recovery 24x7, from any location, using their telephone and without talking to a human help desk technician.</p>	<p>Key recovery is an essential IT support service for organizations that have deployed FDE. Password Manager lowers the IT support cost of key recovery by moving the process to a self-service model.</p>

## 5 Smart card PIN reset

Problem	Solution	Business impact
<p>Organizations deploy smart cards to strengthen their authentication processes. Users typically sign into their PC by inserting their smart card into a reader and typing a PIN. If users forget their PIN or leave their smart card at home, they cannot sign into their PC. PIN reset is a complex support process since the new PIN has to be physically installed on the user's smart card. This means that IT support may trigger a physical visit to the help desk.</p>	<p>Password Manager allows users to access a self-service web portal from anywhere, including from the locked out login screen of their laptop, even away from the office (even using WiFi, as described earlier). Once a user signs into the self-service portal, Password Manager can download an ActiveX component to the user's web browser, to communicate with the smart card and reset the forgotten PIN. Password Manager can also be used to assign a user a temporary login password (often a very long and random one) to be used in the event that a user left his smart card at home.</p>	<p>While forgotten PINs are infrequent – PINs are not usually set to expire – when they do happen, they are extremely disruptive. Assigning temporary passwords is just as important for users who left their smart card at home, which happens quite often.</p>

## 6 Low cost multi-factor authentication using mobile phones

Hitachi ID Password Manager can be used to implement low cost multi-factor authentication, with user mobile phones acting as a secondary authentication factor (i.e., “what you have”).

This solution is implemented using two technologies included with Password Manager:

1. Managed user enrollment, used to prompt users to enter their mobile telephone number and provider.
2. Authentication chains, used to define how users can sign into Password Manager itself. For example, end users who forgot their password might be asked to answer a series of security questions and then (if this was successful) to key in a randomly generated PIN that was sent to their mobile phone via an e-mail-to-SMS gateway. Alternately, help desk staff and administrators might be required to sign into Password Manager using a combination of their Active Directory password and a random PIN, also delivered via SMS.