



The Hitachi ID Login Manager solution

Hitachi ID Login Manager is an enterprise single signon product that auto-populates application passwords for users without the need for a database containing user IDs or passwords. Hitachi ID Login Manager works by replacing password storage with password synchronization.

Single Signon Challenges

Organizations purchase and deploy enterprise single signon (E-SSO) products to reduce the number of times that users type application login IDs and passwords.

Cost

Traditional E-SSO products work by running scripts to auto-populate application login prompts with IDs and passwords from a database. Building and maintaining scripts and the credential database can be time consuming and expensive.

Security

A database with every user's password to every application is a very attractive target for intruders. Unfortunately, traditional E-SSO products create exactly this kind of database.

Accessibility

As user passwords expire, E-SSO products change them to new, random passwords. This means that, over time, users no longer know their own passwords. This prevents users from accessing their applications using PDAs, home PCs and other devices not equipped with the E-SSO software.

Key Business Benefits

Hitachi ID Login Manager reduces the frequency that users must type their passwords without any of these problems. There is no credential database, there are no application login scripts and users still know their own passwords, so they can still use PDAs, home PCs and other devices.

Hitachi ID Login Manager leverages the password synchronization features in *Hitachi ID Password Manager* to eliminate the need for stored passwords in an enterprise single signon solution. This eliminates cost, security and accessibility problems with traditional E-SSO products:

✓ MODE OF OPERATION

Client software intercepts and reuses Windows credentials

1. The *Hitachi ID Login Manager* software is installed on each user workstation.
2. When users sign into their workstations, *Hitachi ID Login Manager* acquires their network login ID and password from the Windows login process.
3. *Hitachi ID Login Manager* extracts additional login IDs associated with the same user from the user's Active Directory or Novell eDirectory profile. These optional login IDs are the only persistent data stored by *Hitachi ID Login Manager* -- user passwords are never stored on disk.
4. *Hitachi ID Login Manager* monitors the Windows desktop for newly launched applications:
 - It detects when a user types one of their known login IDs or their Windows password into an application dialog box, HTML form or mainframe terminal session. When this happens, the location of the input fields is stored for future reference.
 - Whenever *Hitachi ID Login Manager* detects a previously configured input field, *Hitachi ID Login Manager* automatically populates it with the current values: the primary login ID, a secondary login ID or the current Windows password.

✓ INTEGRATION WITH HITACHI ID PASSWORD MANAGER

Leveraging password synchronization

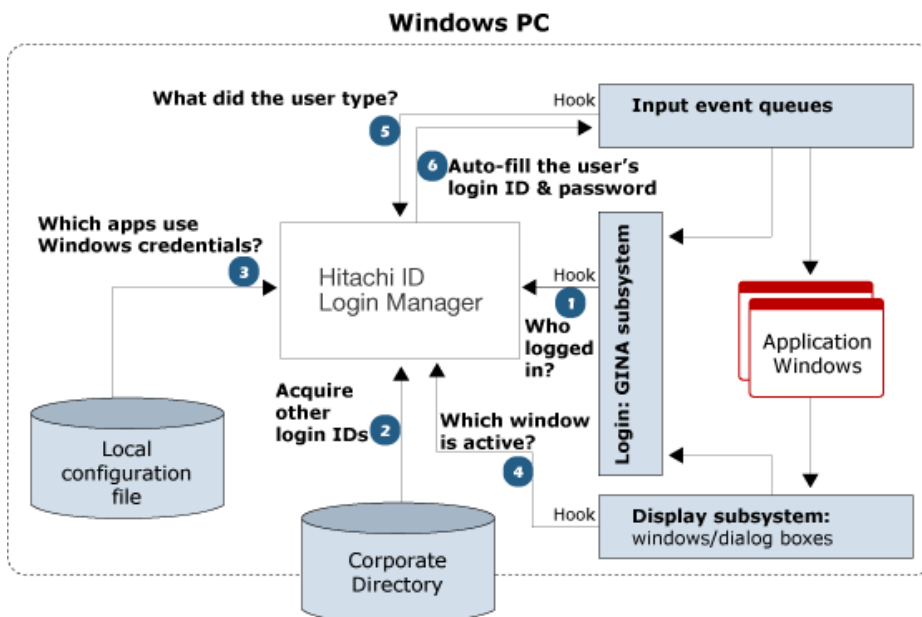
Hitachi ID Login Manager works in organizations that have already deployed *Hitachi ID Password Manager* to synchronize user passwords and reconcile non-standard login IDs. *Hitachi ID Password Manager* manages passwords on existing systems and applications, while *Hitachi ID Login Manager* auto-populates them into application login prompts.



ACCESSIBILITY

Ensuring that users can continue to use mobile and non-corporate devices

Hitachi ID Login Manager does not modify user passwords and will not prevent users from signing into applications from non-traditional devices such as PDAs, smart phones or Internet kiosks. Instead, Hitachi ID Login Manager offers a valuable convenience feature to users by auto-populating the passwords they already know into application login prompts.



CLIENT APPLICATIONS:

Hitachi ID Login Manager can automatically populate login IDs and passwords into the following types of client applications.

- Lotus Notes R6- R8
- Native Windows dialog boxes
- Mainframe terminal emulators
- SAP R/3 GUI
- HTML web forms (IE and Firefox)

TARGET SYSTEMS INTEGRATION

Directory:

Windows domains, Active Directory, eDirectory, Novell NDS, any LDAP

File/Print:

Windows NT, 2000, 2003; Novell NetWare, Samba

Databases:

Oracle, Sybase, SQL Server, DB2/UDB, Informix

Unix:

Linux, Sun, HP, IBM, Compaq, SGI, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+

Mainframes/minis:

MVS/OS390/zOS, VM/ESA, Unisys, Siemens, OS400, OpenVMS, Tandem

Applications:

Oracle, PeopleSoft, SAP; open plug-ins for SQL, ASPs, web services and more

Groupware:

MS Exchange, Lotus Notes/ID files, Lotus Domino/HTTP, Novell GroupWise

Networking:

RAS, routers, firewalls

Flexible Agents:

Target API, Telnet, TN3270, TN5250, HTTP(S), Web Services, command-line, SQL code, LDAP attributes

SUPPORT INTEGRATION

Automatically create, update and close tickets on:

- Axios Assyst
- SupportSoft SmartIssue
- BMC Service Desk
- Clarify eFrontOffice
- FrontRange HEAT
- HP Service Desk
- CA Unicenter
- Tivoli Service Desk
- HP ServiceCenter
- BMD AR System

Additional integrations through e-mail, ODBC, web services and web forms integration.

Hitachi ID Login Manager is part of the Hitachi ID Management Suite, which also includes: Hitachi ID Password Manager, Hitachi ID Identity Manager for user provisioning, Hitachi ID Privileged Password Manager for privileged password management, Hitachi ID Group Manager for group management and Hitachi ID Access Certifier for access certification. For more information about Hitachi ID Systems and its products, please visit the corporate web site at hitachi-id.com, the product web sites at ID-Synch.com, P-Synch.com, ID-Certify.com, ID-Archive.com, ID-Access.org or call 1.403.233.0740.