

Hitachi ID Password Manager

(Formerly P-Synch™)

HITACHI
Inspire the Next



Managing passwords and PINs across on-premise and cloud-based applications.

With over 10 million users worldwide, Hitachi ID Password Manager is the leading authentication management solution. It lowers IT support cost and improves user service by eliminating problems and diverting resolution to self-service. Password Manager includes password synchronization, single sign-on and self-service password reset.

Password Management Challenges

Security

Users cope with complexity by choosing easily guessed passwords, writing down their passwords or never changing their passwords.

Support Cost

Expired or forgotten passwords force users to call the help desk for assistance, accounting for 30% of call volume and costing \$25 to \$35 per incident to resolve.

Productivity

Valuable time is lost when users wait for the help desk to reset their forgotten or locked-out passwords.

Return on Investment

Organizations that deploy *Hitachi ID Password Manager* typically eliminate 85% of the password-related help desk workload. Peak call volume, generally after weekends and holidays, is reduced.

Organizations can re-assign support staff to more important work.

✓ PASSWORD SYNCHRONIZATION

Fewer passwords for users to manage and remember

Transparent password synchronization: When users change one password, others are automatically set to the same value.

Web-based password synchronization: Users are reminded to change their passwords before expiration. They choose a single, new password with a web user interface (UI) that explains policy and the systems that will be affected.

✓ SELF-SERVICE PASSWORD AND PIN RESET

Users can resolve their own login problems

Users who forget their password or trigger a lockout can access Password Manager from a web browser, PC login screen, smart phone or voice call. They sign in using security questions, biometrics, a smart card, a one-time password token or mobile phone authentication and can reset passwords or clear lockouts without calling the help desk.

RSA SecurID token users can reset their token PIN, resynchronize its internal clock with the server or get emergency passcodes using a browser or telephone.

Smart card users can reset their PIN from the PC login screen or a web browser.

✓ DISK ENCRYPTION KEY RECOVERY

Self-service for users who cannot boot Windows

Users whose PCs have full disk encryption and who have forgotten their boot password can access a self-service key recovery process via telephone, eliminating help desk calls and user down-time.

✓ SINGLE SIGN-ON

Automatically sign users into applications

Hitachi ID Login Manager (included with Password Manager) detects applications that use the same ID or password as Windows and automatically inserts those credentials. Users enjoy single sign-on without having to maintain a password wallet.



✓ ASSISTED SERVICE

Reduce call duration at the help desk

Calls to the help desk are resolved quickly by combining analyst authentication, caller authentication, password or PIN reset and incident tracking into a simple web portal.

✓ SECURITY POLICY ENGINES

Password complexity, expiry, authentication and delegated administration

- New passwords must satisfy complexity, history and dictionary checks.
- Users are reminded and can be forced to change passwords regularly.
- Authentication is subject to contextual rules, such as “VPN users must use a token.”
- The right to reset another user’s passwords can be based on relationships, such as “help desk users in Florida can reset AD passwords for users in the Southeast.”
- Robust security questions module, including:
 - Multiple sets of multiple questions
 - Random sampling
 - Standard and user-defined questions
 - Unlimited number of questions per user
 - Answer complexity checking
 - Approximate answer at authentication time

✓ ALWAYS AVAILABLE

Meeting the needs of mobile users

Hitachi ID Password Manager is available where users need it: from a full size or mini web browser, over a telephone, from the login screen of a PC connected to the corporate network or **even from the login screen of an off-line laptop with cached credentials, using a temporary VPN connection, via a public WiFi hot spot.**

✓ RAPID DEPLOYMENT

Quickly install, integrate and enroll

Included connectors and built-in processes minimize deployment effort.

- Over 100 connectors to common systems and applications are included.
- Built-in auto-discovery constructs and populates user profiles.
- Self-service and automated login ID mapping across applications.
- Built-in process to manage the pace of enrollment invitations.
- Single sign-on technology is included and requires minimal configuration.
- Telephony integration is included and pre-configured.

INCLUDED CONNECTORS

Directory:

Windows/Active Directory, LDAP, eDirectory, NDS

File/Print:

Windows, NetWare, Samba, NAS appliances

Database:

Oracle, Sybase, SQL Server, DB2/UDB

Unix:

Linux, Solaris, AIX, HP-UX with passwd, shadow, TCB, Kerberos, NIS or NIS+

Mainframes/mini:

z/OS with RACF, TopSecret or ACF/2; iSeries; Scripts for VM/ESA, Unisys, Siemens, OpenVMS, Tandem

Application:

Oracle eBiz, PeopleSoft, SAP R/3, JDE and more.

Groupware:

Exchange 2000 thru 2010, Notes NAB and ID files, GroupWise

Networking:

Network devices and VPNs via AD, LDAP, SSH.

Flexible Agents:

API, SSH, Web service, Browser emulation, Telnet, TN3270, TN5250, HTTP(S), SQL injection, LDAP attributes and command-line

Cloud / SaaS:

WebEx Connect, Google Applications, SOAP agent, Salesforce.com, UltiPro HR

Full Disk Encryption:

McAfee Endpoint Encryption, Check Point Full Disk Encryption

Authentication Technology:

RSA SecurID, ActivIdentity ActivClient

INCIDENT MANAGEMENT INTEGRATIONS

Automatically create, update and close tickets on:

- Axios Assyst
- BMC SDE
- Clarify eFrontOffice
- HP Service Manager
- Symantec/Altiris
- BMC/Remedy ARS
- CA Unicenter
- FrontRange HEAT
- Numara Track-IT!
- Tivoli Service Desk

Additional integrations via e-mail, ODBC, web services and web forms are available.

Hitachi ID Password Manager is part of the Hitachi ID Management Suite, which also includes: Identity Manager for user provisioning and Privileged Access Manager to secure administrator and service accounts.

For more information, please visit <http://hitachi-id.com/>

or call

1.403.233.0740

1.877.386.0372