



The P-Synch Solution

With more than 7 million users worldwide, P-Synch is the industry's leading password management solution. P-Synch is designed for deployment in days, user enrollment in a weeks and a positive ROI in months.

Hundreds of organizations have eliminated more than 85% of password-related IT support calls using P-Synch's password synchronization, self-service password reset and assisted password reset features.

- ✓ **PASSWORD SYNCHRONIZATION**
Requiring only one or two strong passwords
Transparent password synchronization: When users change one password on an existing system, all other passwords are automatically updated to the same value.

Web-based password synchronization: Prompts users to change all passwords simultaneously through a web interface; includes a clear description of password policy and a list of affected systems.
- ✓ **SELF-SERVICE PASSWORD RESET**
Empowering users to resolve their own password problems
Users with a forgotten or locked out password can access P-Synch from a web browser, from their workstation login prompt or using a telephone. Users authenticate by answering personal questions, providing a biometric sample or with a token. Once authenticated, users reset their own passwords without calling the help desk.
- ✓ **ASSISTED PASSWORD RESET**
Reducing call duration at the help desk
Remaining password calls to the help desk are resolved quickly with a streamlined web interface. This allows help desk analysts to sign in, look up the caller's profile, authenticate the caller, reset passwords and automatically create a closed problem ticket. The entire process takes just one to two minutes.
- ✓ **PASSWORD POLICY ENGINE**
Ensuring strong passwords
Enforce stringent requirements for the composition of new passwords using more than 50 built-in rules.
- ✓ **REGULATORY COMPLIANCE**
Securing your network through industry best practices
Strengthen internal controls with P-Synch by eliminating weak and static passwords and closing "social engineering" back doors.
- ✓ **TOKEN MANAGEMENT**
Reducing token-related calls to the help desk
Users with RSA SecurID token can reset forgotten PINs, re-synchronize the token clock or get emergency access codes without calling the help desk.

The Password Management Challenge

Complexity

Users must remember too many passwords on multiple systems. Each password has a different expiry date and is subject to different composition rules.

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 call to resolve.

Security

Users respond to password complexity by writing down passwords, avoiding password changes or picking easily guessed passwords.

User Productivity

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

Proven Return on Investment

Enterprises that deploy P-Synch typically eliminate 85% or more of the password-related load on the help desk. Peak call volumes, generally after weekends and holidays, are dramatically reduced. Organizations can re-assign support staff from the help desk to focus on more critical business problems.



✓ **SECURITY**

Hardening passwords and authentication processes

P-Synch enforced policy includes password strength rules, expiration schedule and history.

✓ **TELEPHONY INTEGRATION**

Meeting the needs of mobile users

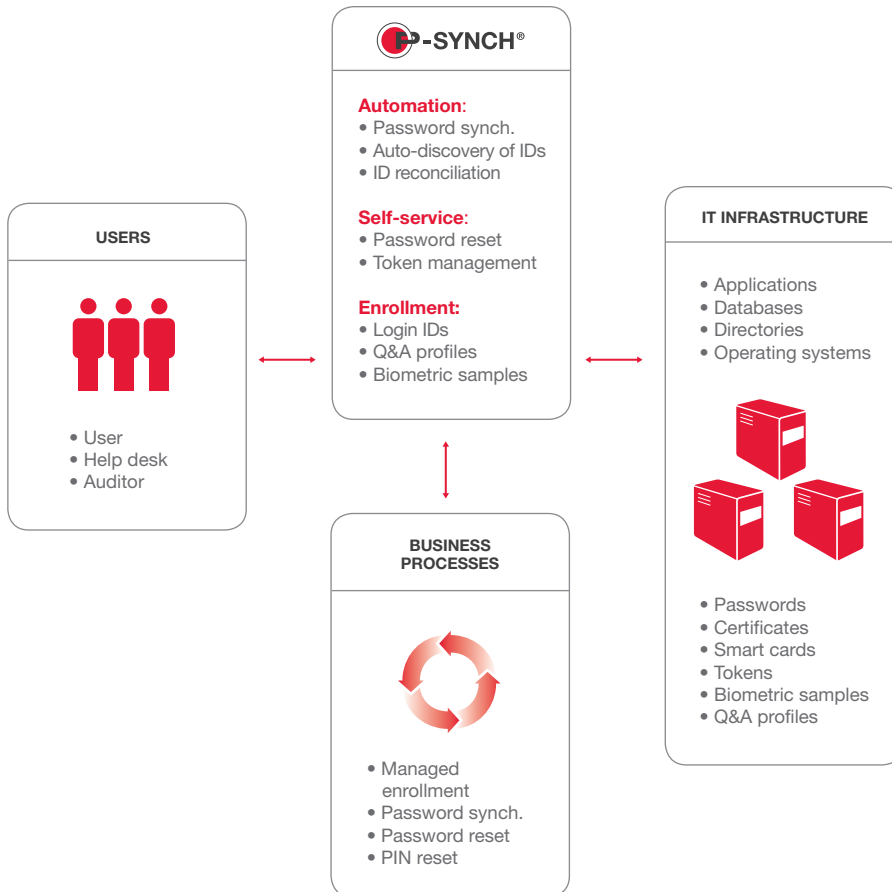
Quickly deploy Hitachi ID's ID-Telephony turnkey IVR system with either touchtone authentication or biometric voice print verification. Alternately, integrate with any existing IVR system using a SOAP web service or C-language API (Windows or Unix).

✓ **RAPID DEPLOYMENT**

Quickly install, integrate and enroll

P-Synch simplifies system integration and automates user enrollment, reducing deployment to days or weeks.

- More than 70 target system integrations out-of-the-box.
- Auto-discovery and self-service reconciliation of login IDs.
- No requirement for client software or agent installation on target systems.
- Managed enrollment of Q & A and login IDs.



TARGET SYSTEMS INTEGRATION

Directory:

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

File/Print:

Windows NT, 2000, 2003; Novell NetWare, Samba, PathWorks, OS2

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:

MVS/OS390/zOS, VM/ESA, Unisys, Siemens Minis: 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
- Magic Service Desk
- Clarify eFrontOffice
- FrontRange HEAT
- HP Service Desk
- CA Unicenter
- Tivoli Service Desk
- Peregrine ServiceCenter
- Remedy AR System

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

P-Synch is part of the Hitachi ID Management Suite, which also includes: ID-Synch® for user provisioning, ID-Archive® for privileged password management, ID-Access® for group management and ID-Certify® for access certification. For more information about Hitachi ID 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.

Hitachi ID Systems, Inc.

© 2008 Hitachi ID Systems, Inc. All rights reserved. Hitachi ID, P-Synch, ID-Synch, ID-Access, ID-Discover, ID-Telephony, AdMax and ID-Certify are trademarks or registered trademarks of Hitachi ID Systems, Inc. in the United States and Canada. All other marks, symbols and trademarks are the property of their respective owners.