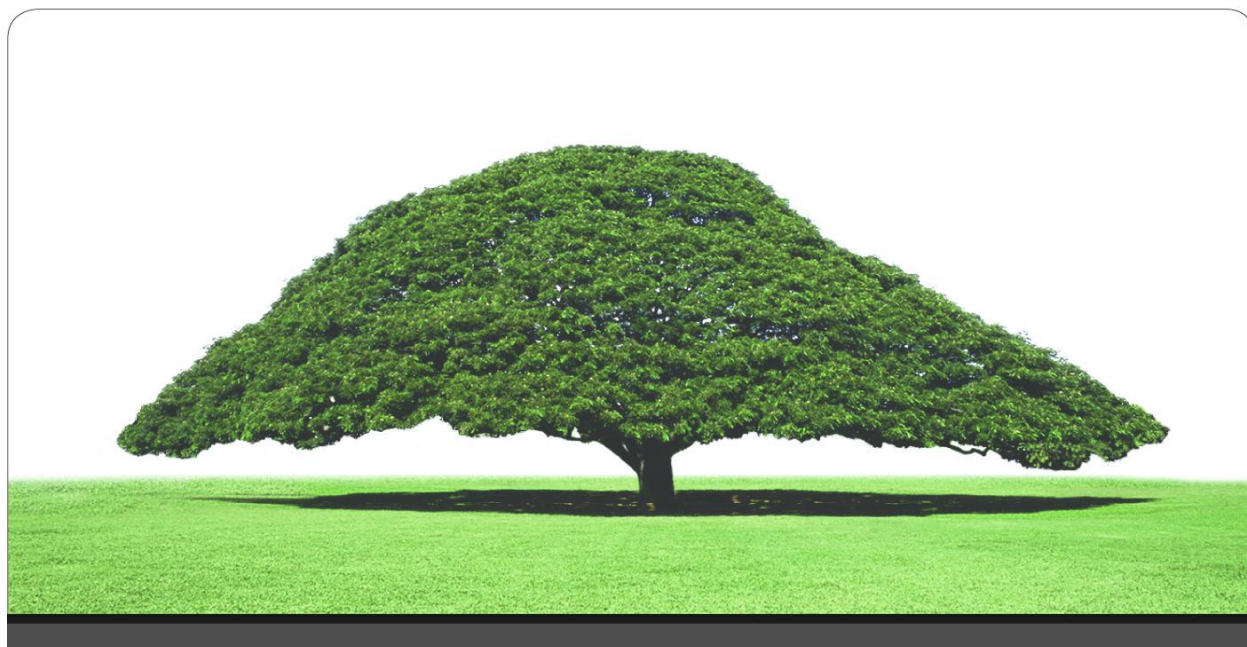


© Hitachi ID Systems, Inc.



## **Hitachi ID Password Manager (P-Synch™)**

### **Frequently Asked Questions for Network Architects**

## Contents

1	How does Hitachi ID Password Manager reset passwords?	1
2	How does Hitachi ID Password Manager synchronize passwords?	1
3	What kind of database does Hitachi ID Password Manager use?	2
4	What systems does Hitachi ID Password Manager support?	3
5	On what platform does Hitachi ID Password Manager run?	3
6	In what ways can Hitachi ID Password Manager be customized?	4
7	How does Hitachi ID Password Manager compare to the “password reset disk” in Windows XP and .NET?	6

## 1 How does Hitachi ID Password Manager reset passwords?

Hitachi ID Password Manager resets passwords by signing into the target system with its own privileged password, looking up a user record, setting the password attribute for that user and logging off from the target system.

At least one pair of user ID and password pair is encrypted into the Hitachi ID Password Manager database for each managed system.

On systems that support it, the Hitachi ID Password Manager target administrator ID can be given just the rights to list users, look up users, reset passwords and set/clear related attributes such as intruder lockout.

Hitachi ID Password Manager is web based. Client communication to the web server is HTTPS, while the server communicates with the managed systems directly using their various native protocols or via a Hitachi ID Password Manager proxy server (128-bit AES encrypted TCP socket) or using a server-side agent (Unix, OS/390, RSA Authentication Managers) with the same TCP socket encryption.

---

## 2 How does Hitachi ID Password Manager synchronize passwords?

Since passwords are typically hashed on each system in a non-reversible, fashion and since different systems use incompatible password hashes, password synchronization must be an active process that takes place whenever users change their passwords.

There are really just two ways to synchronize passwords. Hitachi ID Password Manager supports both of the possible mechanisms for password synchronization:

- **Transparent synchronization:**

Hitachi ID Password Manager can be configured to intercept native password changes on certain systems and:

- Apply a password policy beyond the one built into the system where a native password change first happened and potentially reject the initial password change
- Automatically synchronize the user's other passwords, on other systems, to the same value

Systems that can trigger password synchronization are Windows NT, Active Directory (32-bit, 64-bit), Sun LDAP, IBM LDAP, Oracle Internet Directory, Unix (various), OS/390 and OS/400

- **Web-based synchronization:**

Users authenticate to the Hitachi ID Password Manager web GUI, using any browser, by keying in their NOS or directory ID and password. They can then set a single password on one or more of their own IDs on one or more systems.

### 3 What kind of database does Hitachi ID Password Manager use?

In most deployments, Hitachi ID Password Manager does not require an external database. Rather, it defers to current state on target systems as authoritative.

Hitachi ID Password Manager uses a built-in identity cache to store system configuration information and to cache user profile data drawn from managed systems. The cache significantly improves the run-time performance of Hitachi ID Password Manager, as it eliminates the need to repeatedly connect to managed systems or to an external directory, to look up the same user attributes again and again during the course of a session. The cache is not an authoritative data source – it simply holds copies of user profile data close to the application, to improve performance.

The identity cache built into Hitachi ID Password Manager:

- Is not an authoritative source of data – it is flushed nightly.
- Stores data in an industry standard format (xBase/DBF), which most third-party query and reporting programs tools can read directly or through a standard Windows ODBC driver.

Note that third party software should only be used to query copies of Hitachi ID Password Manager data files, not from the live dataset.

- Is extremely fast (e.g., 1,000,000 record updates/second) and scalable (1 billion records/table).
- Includes automatic data replication between multiple Hitachi ID Password Manager servers (implemented by an included Hitachi ID Password Manager data replication service), which provides for both scalability and high availability out of the box.

In Hitachi ID Password Manager up to version 6.x and other products up to 4.x, the identity cache is implemented using the CodeBase embedded database engine. This is an open (ODBC-accessible, standard file format) system which does not require a separate software license or a DBA. It is installed as an integral component of Hitachi ID Password Manager.

Starting with Hitachi ID Password Manager version 7.x and other products 5.x, all in 2008, customers must choose either MS SQL Server or Oracle Database for holding the identity cache and other Hitachi ID Password Manager data. The free “express” editions of these products are acceptable.

In almost all deployments, Hitachi ID Password Manager rebuilds the internal identity cache nightly, by pulling information from target systems. This process is fault tolerant (i.e., failure to reach a target system causes older information to be retained).

Some organizations already have user profile data, such as login IDs for each user on each system or Q-A (Question-and-Answer) data suitable for user authentication, in an existing database or directory. Hitachi ID Password Manager is designed to plug into existing user profile databases or directories (using LDAP, ODBC, etc.), looking up user data at run-time, as required.

A set of built-in plug-in programs is provided to draw user profile data from LDAP, Active Directory or any ODBC database. This can either be done in real-time, or in batch imports (for example, nightly).

## 4 What systems does Hitachi ID Password Manager support?

Directories	File/print	Mainframes
LDAP (any), Active Directory, Windows NT domains, Novell eDirectory, Novell NDS, Unix NIS and NIS+, Kerberos/DCE (any)	Windows NT/2000/2003/2008, Novell NetWare, OS2 LanManager, Samba	MVS / OS/390 / zOS, RACF, CA-ACF2, CA-TopSecret, VM/ESA, Siemens BS2000, Tandem NonStop, Unisys MCP
Unix	Midrange	Database
AIX, DGUX, Digital Unix, HPUX, IRIX, Linux, NCR, OSF4, SCO OS, Solaris, SunOS, Tru64, UnixWare, Unisys, passwd, shadow, Trusted Computing Base	HP MPE, OS/400/iSeries, OpenVMS	DB2/UDB, Informix, MSSQL, ODBC, Oracle, Sybase
ERP	Messaging	WebSSO
SAP R/3 4.0+, PeopleSoft 7.5+, Oracle Applications 11i+, JDE OneWorld	MS Exchange 5.5, MS Exchange 2000/03/07, Novell GroupWise, Lotus Domino/HTTP, Lotus Notes/ID files, HP OpenMail	IBM TAM, RSA ClearTrust, Entrust getAccess, CA SiteMinder, Oracle COREid, SAP portal
Flexible agents	Hardware tokens and Smartcards	Miscellaneous
API integration, LDAP attributes, MQ Series, SQL commands, Telnet/TN3270/TN5250 sessions, Unix/Windows cmd-line integration, web forms, web services (SOAP, XML)	RSA SecurID, Secure Computing SafeWord, Vasco Digipass, GemPlus, Precise Biometrics	BMC Service Desk Express, Clarify eFrontOffice, Connected Backup, IBM OLAP, IBM Tivoli Access Manager, Local and cached Windows passwords, HP ServiceCenter, RADIUS (various), BMC Remedy ARS and Tivoli ADSM,

## 5 On what platform does Hitachi ID Password Manager run?

Hitachi ID Password Manager must be installed on a Windows 2003 or Windows 2008 server.

Installing on Windows 2003 or Windows 2008 allows Hitachi ID Password Manager to leverage client software for most types of target systems, which is available only on the “Wintel” platform. In turn, this makes it possible for Hitachi ID Password Manager to manage passwords and accounts on target systems without installing a server-side agent.

The Hitachi ID Password Manager server must also be configured with a web server. Since the Hitachi ID Password Manager application is implemented as CGI executables, any web server will work. The Hitachi ID Password Manager installation program is aware of and can automatically configure IIS, Apache and Sun ONE web servers for use with Hitachi ID Password Manager.

Hitachi ID Password Manager is a security server and should be locked down accordingly. Please refer to the Hitachi ID document about hardening Hitachi ID Password Manager servers to learn how to do this. In short, most of the native Windows services can and should be removed, leaving a very small attack surface, with exactly one inbound TCP/IP port (443):

1. IIS is not required (Apache is a reasonable substitute).
2. No ASP, JSP or PHP are used, so these engines should be disabled.
3. .NET is not required on the web UI, so should be disabled on IIS.
4. No ODBC or DCOM are required inbound.
5. File sharing should be disabled.
6. Remote registry services should be disabled.
7. Inbound connections should be filtered, allowing only port 443 and possibly terminal services (for certain configuration tasks).

---

## 6 In what ways can Hitachi ID Password Manager be customized?

The entire Hitachi ID Password Manager user interface is customizable and translatable. This includes graphical changes, text changes, layout changes, language translations, etc. No user interface elements are hard-coded into Hitachi ID Password Manager.

User interface customization is simple to implement. Common elements, such as page layout and HTML preambles, are factored out into standard macros using a freely-available macro language (M4). Modifications made to M4 files are propagated across the entire user interface, without having to touch or understand product source code.

Note that M4 (at least as it is used in Hitachi ID Password Manager) is really just 3 keywords: include, define and ifelse. It is not something that administrators really have to learn – what they really need to understand is HTML and CSS and what they will learn while customizing Hitachi ID Password Manager is where to find the right macro to modify.

An override mechanism is used to clearly separate user interface customizations from the core UI. This allows most customizations to survive Hitachi ID Password Manager version upgrades with minimal intervention. For example, customers may define a new HTML markup for table headings. This markup is placed in an override file and takes higher precedence than the (still present) default markup. When the software is upgraded, the customization will still override the new version's default HTML code.

In addition to modifying HTML and CSS markup, customers can change the values of a number of system variables which alter Hitachi ID Password Manager behavior. For example, password policy, intruder lockout frequency and duration, non-password authentication rules and more can all be adjusted. System variables also survive version upgrades.

Hitachi ID Password Manager behavioral modifications are made using plug-in points, rather than (as is common with some web applications) by modifying the source code of Hitachi ID Password Manager itself. Plug-ins are external programs, called by Hitachi ID Password Manager, that are sent strictly defined inputs and whose outputs modify Hitachi ID Password Manager behavior. For example, plug-in program can be used to:

- Look up a user's known, existing login accounts.
  - Default implementations are provided for looking up login IDs in LDAP or SQL.
- Look up a user's challenge/response profile.
  - Default implementations are provided for looking up login IDs in LDAP or SQL.
- Assign a new login ID to a newly created user.
  - Sample scripts are provided that illustrate this process.
- Validate form inputs when creating or modifying a user profile.
  - Sample scripts are provided that illustrate this process.
- Assign appropriate authorizers to a request to create or modify a user.
  - Default authorizer routing is typically to resource owners and the recipient's manager.
  - Sample scripts are provided that illustrate this process.
- Find new authorizers to replace unresponsive ones.
  - Default escalation is typically to an authorizer's manager.

This architecture, which contains business logic in separate executable programs or script files, has two important benefits:

- It is significantly easier for Hitachi ID customers to adjust Hitachi ID Password Manager behavior, since all such modifications are made in simple, self-contained files.
- Business logic implemented in this way survives version upgrades, since upgrades do not in any way alter these files.

Hitachi ID Password Manager includes over 163 exit points. Whereas plug-in points are interactive, altering Hitachi ID Password Manager behavior, exit points are uni-directional and are used strictly to pass information from Hitachi ID Password Manager to other applications.

Example uses of plugins include sending e-mails to users or administrators and creating, updating or closing incident records in a help desk application.

Exit points may be triggered by many events, including attempts to sign into Hitachi ID Password Manager (successful or failed); one user looking up the profile of another; changes to a user's profile, such as creating a new user or altering an existing one; changing Hitachi ID Password Manager's configuration; running a report; triggering an intruder lockout and more.

Various pre-built plug-in program binaries are included with Hitachi ID Password Manager. They are generally scriptable and allow customers to quickly integrate Hitachi ID Password Manager with help desk applications and e-mail systems. .

---

## 7 How does Hitachi ID Password Manager compare to the “password reset disk” in Windows XP and .NET?

Starting with Windows XP, users can create a “password reset disk” whenever they change their passwords.

If a user forgets his login password, he can log into his workstation by typing his login ID but leaving the password field blank and instead inserting a previously-created password reset disk.

This feature is helpful for home users, but is significantly less useful than self-service password reset with Hitachi ID Password Manager:

- **Does not work for domain users:** The password reset disk feature does not work for domain passwords – only local ones.
- **Inconvenient:** Users must create a new disk whenever they change their passwords. In comparison, users register with Hitachi ID Password Manager just once.
- **Inconvenient:** Mobile must carry the password reset disk with them. In comparison, users can access Hitachi ID Password Manager from any computer, at any time.
- **Insecure:** Anyone who can touch the password reset disk can steal or copy it and subsequently log into the user's account. There is no comparable vulnerability in Hitachi ID Password Manager.