

Hitachi ID Password Manager

Frequently Asked Questions
for Prospective Customers



Contents

1	Who is Hitachi ID?	1
2	What is Password Manager?	1
3	What does Identity Manager do, and how does it relate to Password Manager?	2
4	How does Password Manager reduce help desk costs?	3
5	How does Password Manager improve user service?	4
6	How does Password Manager improve security?	4
7	How does Password Manager compare to single sign-on?	5
8	Is there an ROI model for Password Manager deployments?	6
9	How does Password Manager compare to products from other vendors?	6
10	What platforms does Password Manager support?	8
11	How is Password Manager licensed?	8
12	How long does it take to deploy Password Manager?	9
13	How much work is needed to manage Password Manager in production?	9

1 Who is Hitachi ID?

Hitachi ID Systems, Inc. is a leading publisher of identity and access management software. Hitachi ID Systems products help organizations strengthen network security, lower IT support costs and improve user productivity. Hitachi ID Systems customers achieve these results by implementing automation and self-service processes to more effectively manage passwords and other authentication factors, to provision and deactivate user access and to manage user privileges. Hitachi ID Systems products have been deployed at over 840 organizations world-wide.

Originally founded in 1992 as M-Tech Information Technology, Inc. and acquired by Hitachi, Ltd. in 2008, Hitachi ID Systems, Inc. is a leading provider of identity and access management solutions.

Hitachi ID Systems first identity and access management product, Hitachi ID Password Manager, has been commercially available since 1995. Today, Hitachi ID Systems is the leading password management vendor world-wide and a leading provider of identity management solutions.

Hitachi ID Systems currently has 140 employees. Hitachi ID Systems has enjoyed strong financial performance, with 76 consecutive quarters of growth and profitability.

Hitachi ID Systems is headquartered in Calgary, Canada and has regional offices in: Canada: Vancouver, Barrie, Ottawa and Montreal; United States: Denver, Dallas and New York, Australia: Brisbane.

2 What is Password Manager?

Hitachi ID Password Manager is an enterprise solution for managing passwords and other authentication factors. It improves the security of passwords and related IT support processes, reduces the cost of user support and improves user productivity. This is done with features such as password synchronization, self-service password reset, enterprise single sign-on, PIN resets for tokens and smart cards, enrollment of security questions and biometrics and emergency recovery of full disk encryption keys.

Password Manager reduces the cost of password management using:

- Password synchronization, which reduces the incidence of password problems for users
- Self-service password reset, which empowers users to resolve their own problems rather than calling the help desk
- Streamlined help desk password reset, to expedite resolution of password problem calls

Password Manager strengthens security by providing:

- A powerful password policy engine.
- Effective user authentication, especially prior to password resets.
- Password synchronization, to help eliminate written-down passwords.
- Delegated password reset privileges for help desk staff.
- Accountability for all password changes.
- Encryption of all transmitted passwords.

To find out more about Password Manager, visit <http://Hitachi-ID.com/Password-Manager>.

3 What does Identity Manager do, and how does it relate to Password Manager?

Hitachi ID Identity Manager is a separate product built on the same infrastructure as Hitachi ID Password Manager. Where Password Manager manages passwords, Identity Manager creates, deletes and manipulates user accounts.

Identity Manager is a complete user provisioning solution that automates and simplifies the routine tasks of managing users and entitlements across multiple systems and applications. Organizations depend on Identity Manager to ensure that their users get appropriate access rights promptly and are deprovisioned reliably and completely.

Identity Manager implements the following business processes to drive administrative updates to users and entitlements:

- **Automation:** grant or revoke access based on data feeds.
- **Synchronization:** keep identity attributes consistent across applications.
- **Self-service:** empower users to update their own profiles.
- **Delegated administration:** allow business stake-holders to request changes directly.
- **Workflow:** invite business stake-holders to review and either approve or reject proposed changes.

Identity Manager strengthens security by:

- Quickly and reliably removing access to all systems and applications when users leave an organization.
- Finding and helping to clean up orphan and dormant accounts.
- Assigning standardized access rights, using roles and rules, to new and transitioned users.
- Enforcing policy regarding segregation of duties and identifying users who are already in violation.

- Ensuring that changes to user entitlements are always authorized before they are completed.
- Asking business stake-holders to periodically review user entitlements and either certify or remove them, as appropriate.
- Reducing the number and scope of administrator-level accounts needed to manage user access to systems and applications.
- Providing readily accessible audit data regarding current and historical security entitlements, including who requested and approved every change.

Identity Manager reduces the cost of managing users and security entitlements:

- Auto-provisioning and auto-deactivation leverage data feeds from HR systems to eliminate routine, manual user setup and tear-down.
- Self-service eliminates IT involvement in simple updates to user names, phone numbers and addresses.
- Delegated administration moves the responsibility for requesting and approving common requests, such as for new application or folder access, to business users.
- Identity synchronization means that corrections to user information can be made just once, on an authoritative system and are then automatically propagated to other applications.
- Built-in reports make it easier to answer audit questions, such as “who had access to this system on this date?” or “who authorized this user to have this entitlement?”

4 How does Password Manager reduce help desk costs?

Hitachi ID Password Manager realizes cost savings and enhanced productivity for both users and the IT support organization:

- **User productivity:** Users experience fewer password problems.
This is a result of password synchronization, which helps users to remember one or two passwords, rather than forgetting or writing down many different passwords.
- **Fewer IT support calls:** Login problems are resolved by users, without calls to the help desk.
Users can reset forgotten passwords, clear intruder lockouts, recover hard disk encryption keys and reset PINs on their smart cards and tokens – all via self-service.
- **Reduced cost per support incident:** Calls that still reach the help desk are resolved more quickly.
Remaining login-related support calls are resolved with a streamlined Password Manager process, which includes analyst authentication, caller authentication, problem resolution and which automatically submits a ticket to the help desk incident management system.

5 How does Password Manager improve user service?

Hitachi ID Password Manager improves user service by simplifying system and application login processes for users:

- Users only have to remember one or two passwords.
 - All passwords are managed through a single, friendly interface.
 - Password policy is the same everywhere and is clearly defined.
 - Application login prompts can be automatically filled in using Hitachi ID Login Manager.
 - In the event of a password or login problem, users can quickly resolve their own problem, rather than calling the help desk and waiting for service.
 - Password expiration notices are delivered to all users, including mobile users with cached credentials, who currently do not receive them.
-

6 How does Password Manager improve security?

Hitachi ID Password Manager improves the security of authentication processes:

- A strong, uniform password policy prevents the use of easily guessed passwords and ensures that all passwords are changed regularly.
 - Password synchronization discourages written passwords (“sticky notes”).
 - Consistent, reliable authentication processes ensures that users are reliably identified before accessing sensitive services, such as a help desk password reset.
 - IT support staff can be empowered to assist callers without having administrator accounts on every system and application.
 - Extensive audit logs create accountability for password resets.
 - Encryption ensures that passwords are not stored or transmitted in plaintext.
-

7 How does Password Manager compare to single sign-on?

Hitachi ID Password Manager is not a single sign-on system. Rather, it manages and reduces the number of passwords that users must remember, but does not eliminate the need for users to type their own passwords.

Password management, rather than single sign-on, may be attractive, because of some problems with enterprise single sign-on software:

Previous approaches to enterprise single sign-on systems had problems, all related to the password database where user IDs and passwords are kept:

- **Remote Access and Mobile Devices:**

Over time, a traditional E-SSO system will respond to applications expiring passwords by choosing new, random password values, allowing the application to change passwords and storing the random password value for future reference.

With this process in place, over time users lose knowledge of their own passwords and become dependent on the E-SSO system to sign into their applications. This means that users cannot access their applications from devices that are not equipped with the E-SSO software, such as smart phones or even their home PCs.

- **Cost to Deploy:**

Building and maintaining a database of every login ID and every password on every application can be both costly and time consuming.

- **Cost to Reset Passwords:**

Login IDs and passwords stored in a traditional E-SSO system are typically encrypted using a key derived from the user's primary network password. When users forget their primary password, they lose this key and can no longer decrypt their application passwords. As a result, password problems may be less frequent with E-SSO, but resolving them is more complicated, time consuming and expensive.

- **Security and Availability:**

In the event that the password database in a traditional E-SSO system is compromised, every user ID and every password would be exposed.

If the password database suffers an outage, every user would be locked out of every application.

It should be noted that Web single sign-on software (WebSSO) are less ambitious than enterprise SSO, but have none of its drawbacks. When users first access an Intranet page, they are diverted to an authentication page. Thereafter, whenever they access another page, their browser sends an encrypted authentication cookie to the web server, which validates it and does not prompt for a second login screen.

With agent-based WebSSO, there is no client software, no credential database and no costly password reset processes.

Password Manager can synchronize passwords across both legacy systems (network operating systems, applications, mainframes, etc.) and WebSSO systems, which typically authenticate users with an LDAP directory and password.

8 Is there an ROI model for Password Manager deployments?

There is a detailed ROI (return on investment) model for Hitachi ID Systems identity and access management solutions at:

<http://Hitachi-ID.com/Password-Manager/roi/>

ROI from Hitachi ID Password Manager is principally due to improved user productivity (fewer password problems) and reduced workload for the help desk.

9 How does Password Manager compare to products from other vendors?

Hitachi ID Password Manager is key element in an organization's identity and access management infrastructure. Other components may include user provisioning automation, such as Hitachi ID Identity Manager, directories, meta directories, web single sign-on (WSSO) and web access management (WAM) products.

Password Manager may be compared to other identity and access management products as follows:

- **Core technology found only in Password Manager**

Password Manager is built for rapid deployment. Rapid deployment is accomplished with some key technologies that are not available in any other product, including:

Password Manager is designed for rapid deployment:

- **No client software required**, even for access to self-service password reset from the workstation login prompt.
- **Automated discovery** of every login ID on every target system, nightly.
- **Self-service login ID reconciliation** where login IDs on different systems are different and there is no pre-existing correlation data.
- **A built-in identity cache** that captures user profile data and eliminates the need to install or manage a database or directory before installing Password Manager.
- **Built-in connectors for every common system and application** eliminating the need for customers to develop their own connectors to common, off-the-shelf target systems.
- **Remote connectors** mean that Password Manager can manage users and passwords on systems without requiring the installation of intrusive local software on each target system.

- **Flexible connectors** enable organizations to integrate Password Manager with custom applications, vertical market software, application service providers (ASPs) and service bureaus quickly – taking just 2 hours to 4 days per new target system.

- **Password reset products**

Some password management products focus solely on password reset.

Password Manager's advantage over such products is a fundamentally different strategy. With Password Manager, customers first seek to eliminate problems, through password synchronization. Self-service is used to divert remaining problems, rather than as a primary tool for call volume management.

This approach generates better returns, through higher user adoption rates and better user service. Typically synchronization, self-service and assisted password resets together reduce help desk password problem load by 95%, as compared to about 60% for just self-service password reset.

Password Manager is also less expensive to purchase and deploy than products that offer just self-service password reset.

- **Password synchronization products**

Products that offer just password synchronization typically require agents to be installed on every target system. This triggers extensive change control and delays project roll-out.

Most products that focus on password synchronization require either a mainframe or large Unix server. This makes deployment more costly.

Synchronization-only products do not yield full value. Typically about 80% of password problems are eliminated by synchronization. Including self-service password reset improves the product's impact on the service desk to 90% or better.

Password Manager is also less expensive to purchase and deploy than products that offer just password synchronization.

- **User provisioning products**

Products designed primarily to provision and manage systems access typically include a light-weight password management capability. This most often consists of two web-based screens:

- *Enrollment*: users authenticate with an LDAP password and store one or two question/answer pairs for future reference.
- *Password reset*: users authenticate with their LDAP password or by answering security questions and can reset their LDAP password or passwords on select other systems.

This capability is much simpler than Password Manager:

- Non-password authentication depends on trivial data and is consequently insecure.
- There is no password synchronization capability.
- There is no access to self-service from a workstation login screen or a telephone.
- There is no integration with incident management systems.
- Only very few passwords can be managed.

- User ID reconciliation is a complex and costly process.

This capability does not meet the requirements of many enterprises, and organizations who install such user provisioning systems are well served by also deploying Password Manager.

- **WAM / WSSO products**

The password management capability in WAM / WSSO products is similar to that in user provisioning products, except that it is normally only possible to manage a single LDAP password.

There is little real functional overlap between Password Manager and WAM / WSSO products.

10 What platforms does Password Manager support?

Directories:	Servers:	Databases:
Any LDAP, AD, NDS, eDirectory, NIS/NIS+.	Windows 2000, 2003, 2008, Samba, Novell, SharePoint.	Oracle, Sybase, SQL Server, DB2/UDB, ODBC.
Unix:	Mainframes:	Midrange:
Linux, Solaris, AIX, HPUX, 24 more.	z/OS with RAC/F, ACF/2 or TopSecret.	iSeries (OS400), OpenVMS.
ERP:	Collaboration:	Tokens, Smart Cards:
JDE, Oracle eBiz, PeopleSoft, SAP R/3, Siebel, Business Objects.	Lotus Notes, Exchange, GroupWise, BlackBerry ES.	RSA SecurID, SafeWord, RADIUS, ActivIdentity, Schlumberger.
WebSSO:	Help Desk:	HDD Encryption:
CA Siteminder, IBM TAM, Oracle AM, RSA Access Manager.	BMC Remedy, BMC SDE, HP Service Manager, CA Unicenter, Assyst, HEAT, Altiris, etc.	McAfee, CheckPoint.

11 How is Password Manager licensed?

Hitachi ID Password Manager pricing is based on the number of users (people, not login accounts). This includes all features, all connectors, all client software components and the right to run as many servers and CPUs as desired. A one-time purchase grants customers the perpetual right to use Password Manager.

Password Manager pricing is calculated using a smooth curve – as the number of users increases, the price per user steadily decreases. This means that customers do not have to base their purchase volumes on price bands or tiers. Instead, customers purchase for the number of users actually required, knowing they will get the best price for that volume.

Customers are encouraged to, over time, extend their deployment of Password Manager to manage new target systems and to activate new features, at no additional charge.

Customers may run as many Password Manager servers as required, to provide high availability, redundancy and a test/QA environment, at no additional charge.

12 How long does it take to deploy Password Manager?

Hitachi ID Password Manager deployment typically requires from 5 to 15 days of work.

Initial Password Manager activation normally includes all features, platforms, access channels and users. Once the software is active, user enrollment may be required. Global user enrollment is an ongoing process, especially as new staff are hired. In most cases, 80% or more of users can be asked to enroll and can be expected to complete registration, within 1-2 months of deployment.

13 How much work is needed to manage Password Manager in production?

Hitachi ID Password Manager does not require active ongoing administration of user profiles and system functionality. Users are automatically detected on target systems, enrolled and prompted to register if additional information is required.

A Password Manager administrator **is** required to monitor the servers, promote consistent password management to application owners, answer questions from the user community and perform periodic software upgrades.

These responsibilities typically amount to approximately 0.25 FTE.