

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?	3
6	How does Password Manager improve security?	4
7	How does Password Manager compare to single sign-on?	4
8	Is there an ROI model for Password Manager deployments?	5
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., formerly M-Tech Information Technology, Inc., is a leading publisher of identity management software. Hitachi ID products help organizations strengthen network security, lower IT support costs and improve user productivity. Hitachi ID 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 products have been deployed at over 780 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 management solutions.

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

Hitachi ID currently has 140 employees. Hitachi ID has enjoyed strong financial performance, with 64 consecutive quarters of growth and profitability.

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

2 What is Password Manager?

Hitachi ID Password Manager is the industry's leading password management solution. Password Manager helps organizations manage passwords and other forms of authentication more effectively to reduce IT support costs, increase productivity and enhance corporate security. Password Manager features include password synchronization, self-service reset, token management, biometric enrollment, certificate management and more.

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 strong, enterprise-wide password policy enforcement facility
- Effective user authentication, especially for self-service and assisted password resets
- Password synchronization, to help users remember, rather than write down, their passwords
- The ability to securely delegate the right to reset passwords to front-line support staff
- Accountability for password resets
- Encryption of all transmitted passwords

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

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 across multiple systems. Enterprise-scale organizations depend on Identity Manager to ensure that their employees and contractors are securely and efficiently connected to vital systems and information.

Identity Manager implements the following business processes to drive updates to users and entitlements on managed systems:

- **Automation:** copies changes from one system to another.
- **Self service:** delegates change requests and approvals to users.
- **Consolidation:** allows administrators to manage multiple systems at once.
- **Delegation:** empowers departmental or regional administrators with limited authority.
- **Fulfillment:** gives other systems the ability to manage users through Identity Manager.

Identity Manager reduces the cost of user provisioning using:

- Automated user administration, which leverages information in other systems (HR, corporate directory) to automatically create or delete systems access
- Self-service user administration workflow, allowing users to request security changes, automatically routing them to suitable authorizers, tracking approvals and automatically implementing authorized changes
- Consolidated and delegated user administration, making security administrators more productive by enabling administration of multiple systems from a single point

Identity Manager strengthens security by:

- Enabling prompt and complete access deactivation across multiple systems.
 - Automatically deactivating access for terminated users.
 - Automatically detecting and deactivating or deleting orphan and dormant accounts.
 - Enforcing authorization rules over security change requests.
 - Implementing standards for the privileges assigned to new users.
 - Subjecting security administrators to personal authentication, authorization and audit logs.
 - Providing consolidated reports on user access to systems, which can be used to review compliance with security policy.
 - Providing an audit log of all provisioning / deprovisioning events.
-

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 help desk:

- **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.
 - **Reduced Help Desk Call Volume:** Password problems are resolved by self service.
Of problems that remain after activating password synchronization, the majority are resolved by self service and never generate a help desk call.
 - **Reduced Help Desk Cost Per Call:** Password problem calls are resolved quickly.
Remaining password problem calls are resolved by the Password Manager web interface, which handles every aspect of the call and allows a support analyst to resolve a password problem call in about 1 minute.
-

5 How does Password Manager improve user service?

Hitachi ID Password Manager improves user service by simplifying password management:

- 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.
 - In the event of a password or login problem, users can quickly resolve their own problem, rather than calling the help desk.
 - Password expiration notices are delivered to all users, not just those who log into the NOS daily.
-

6 How does Password Manager improve security?

Hitachi ID Password Manager improves the security of authentication processes:

- A global password policy ensures that no passwords are easily guessed, and all passwords are regularly changed.
 - Password synchronization helps users remember their passwords, rather than writing them down.
 - Strong authentication ensures that users are properly authenticated prior to a self-service or assisted password reset.
 - Delegation allows help desk analysts to reset passwords for users without having administrative access on managed systems.
 - Extensive audit logs create accountability for password resets.
 - Encryption ensures that no sensitive data is 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 the 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 signon, may be attractive, because of some problems with enterprise single signon software:

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

- **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.

- **Remote Access to Applications:**

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 PDAs, smart phones and Internet kiosks.

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 identity management solutions at:

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

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

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

Hitachi ID Password Manager is key element in an organization's identity 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 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 managed 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.
- **Pre-built agents for 70+ systems** eliminating the need for customers to develop their own connectors to common, off-the-shelf target systems.
- **Remote agents** mean that Password Manager can manage users and passwords on systems without requiring the installation of intrusive local software on each target system.
- **Flexible agents** 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 managed 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 Q-A (Question-and-Answer) profile (above) 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 help desk 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	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	z/OS, 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 Service Manager, RADIUS (various), BMC Remedy ARS and Tivoli ADSM,

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 and support for all target systems. A one-time purchase grants customers the perpetual right to use Password Manager.

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, redun-

dancy 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 managed 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 1/4 FTE.