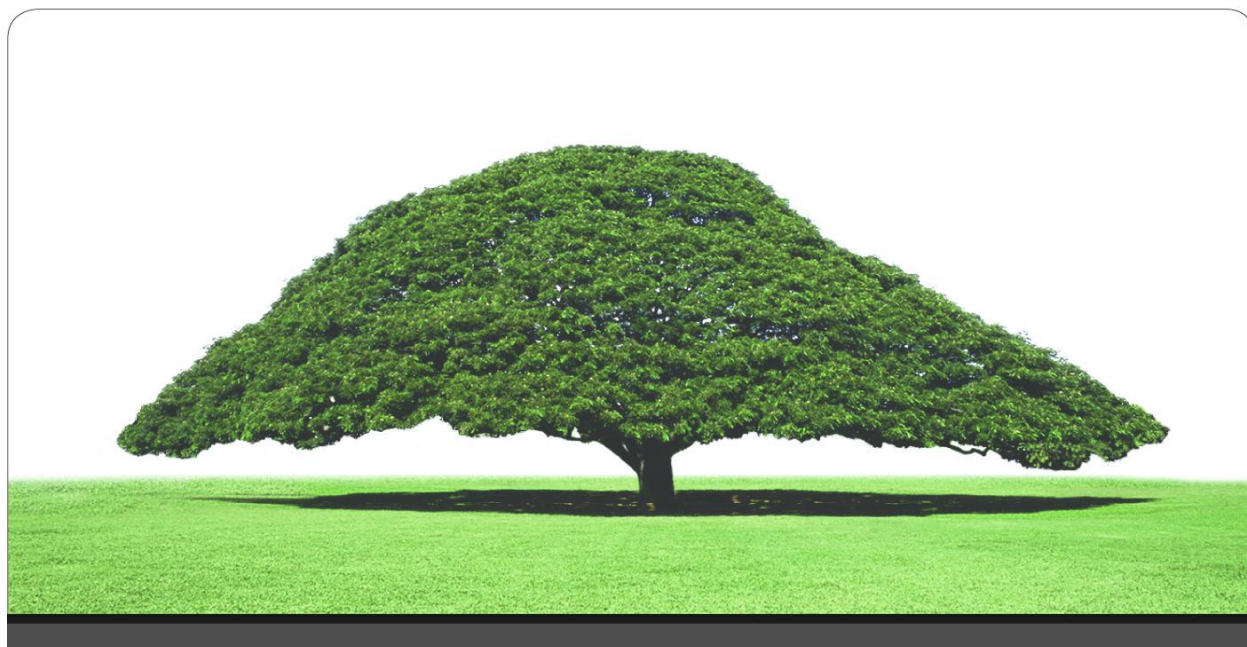


© Hitachi ID Systems, Inc.



Integrating Hitachi ID Management Suite with Microsoft Identity Lifecycle Manager 2007

Hitachi ID Password Manager (P-Synch™) is a Synchronization and Self-Service Password Reset, which offers password synchronization, self-service and assisted password reset and management of other authentication factors, such as tokens or biometric samples, to enterprise organizations.

Hitachi ID Identity Manager (ID-Synch™) is a Automated Onboarding, Synchronization and Deactivation, which can create, delete, enable, disable, rename, change attributes and change group membership for users on a wide variety of systems. Hitachi ID Identity Manager includes a automated change propagation capability; a self-service workflow for requesting, validating, routing and authorizing changes; consolidated and delegated user administration and consolidated access reporting.

Hitachi ID Password Manager and Hitachi ID Identity Manager are two key parts of Hitachi ID Management Suite. Hitachi ID Management Suite can manage users on over 65 types of systems, and includes a number of flexible agents for quick integration with new target systems – vertical market applications, custom software, ASPs and service bureaus.

This document describes how Hitachi ID Password Manager and Hitachi ID Identity Manager can be deployed in conjunction with ILM how the technologies interact, and how they complement one another.

Contents

- 1 Introduction** **1**
- 2 Meta Directories Defined** **2**
 - 2.1 How ILM2007 Relates to Active Directory 2
- 3 Password Management and User Provisioning Systems Defined** **4**
 - 3.1 Password Management Systems Defined 4
 - 3.2 User Provisioning Systems Defined 5
- 4 Common Components in ILM2007 and Hitachi ID Management Suite** **6**
- 5 The Value of Integration** **6**
- 6 Integrated Deployment Strategies** **7**
 - 6.1 ILM2007 First: Leverage Existing Login ID Profiles 7
 - 6.2 Hitachi ID Password Manager First: Self-Service Login ID Reconciliation 7
- 7 Extending ILM2007 Functionality** **8**
 - 7.1 Background 8
 - 7.2 Initializing Passwords 8
 - 7.3 Increased Reach: Leveraging Hitachi ID Identity Manager Agents 9

1 Introduction

Integrating ILM2007, password management and user provisioning products yields maximum value for identity management.

Hitachi ID Management Suite includes both the Hitachi ID Password Manager Synchronization and Self-Service Password Reset and the Hitachi ID Identity Manager Automated Onboarding, Synchronization and Deactivation.

This document discusses how Hitachi ID Management Suite can be deployed in conjunction with ILM2007, how the technologies interact, and how they complement one another.

The remainder of this document is organized as follows:

- **Meta directories defined:**

A brief definition of meta directory products in general (and ILM2007 in particular).

- **How ILM2007 relates to Active Directory:**

A description of Microsoft's Active Directory, followed by an explanation of how it reduces but does not eliminate the requirement for both meta directories such as ILM2007 and effective password management and user provisioning.

- **Common components and processes:**

Some software components and processes that ILM2007 has in common with password management and user provisioning systems such as Hitachi ID Management Suite.

- **ILM2007 first:**

Integration between Hitachi ID Management Suite and ILM2007 in the situation where ILM2007 was already deployed when the password management or provisioning project begins.

- **Hitachi ID Password Manager first:**

Integration between Hitachi ID Password Manager and ILM2007 in the situation where the password management project precedes deployment of ILM2007.

- **Extending ILM2007 functionality:**

How technology in Hitachi ID Password Manager and Hitachi ID Identity Manager can extend the functionality of ILM2007.

2 Meta Directories Defined

ILM2007 is a meta directory product.

Meta directories are programs that synchronize the contents of multiple user directories. They typically read a list of user and user-attribute data from multiple directories, build a master directory of users and their attributes, and push new or changed data from the master directory back to some or all of the managed directories.

This directory synchronization process is normally run in a batch, in several steps:

1. Read data from existing systems.
2. Join data into a master directory, where all users and all user attributes are represented in the form of one entry with many attributes per user.
3. Write a subset of the data, using some attributes and applying to just some users, from the master directory to some of the managed directories.

The net effect of ILM2007 deployment is that information entered about users on one system is automatically propagated to other systems. For example, if a user's home phone number is changed in a company's human resources database, the new phone number might be automatically applied to his profile on the corporate e-mail system and network operating system.

This propagation of user information means that data about users can be made consistent amongst diverse systems. In some cases, it is also possible to cease manual administration of some systems entirely, and rely on ILM2007 to forward changes (add, modify, delete) to the user directory from one system to another.

In addition to propagating changes from one directory to another, ILM2007 provides an organization with a view into the master directory, called a metaverse. A single repository houses data about every user on every system, and global access reporting is therefore possible.

2.1 How ILM2007 Relates to Active Directory

Many organizations are migrating or have migrated their network operating system from Windows NT or Novell NDS to Microsoft Active Directory, using Windows 2000 / or Windows 2003 servers.

Active Directory (AD) can simplify the process of managing user identity data by centralizing it in one place. User records for the network login, for e-mail (using MS-Exchange) and for Intranet applications are all resolved in a single, LDAP-compliant directory.

Applications running on Windows, Unix and even OS390 mainframes can validate user IDs and passwords against the same system, and using Kerberos can even implement single sign-on so that users don't have to sign in separately to each system.

In effect, AD allows organizations to **consolidate** user identity management into a single, enterprise-wide directory. This consolidation reduces the need for ILM2007, since its job is to **integrate** information from multiple, diverse systems. It also reduces the frequency of password problems that users experience, as they have fewer login IDs and passwords, and consequently the need for password management is reduced.

Despite the clear benefits of AD, most organizations find that they continue to have multiple user directories. For example, they may integrate the NOS login, e-mail system and some Intranet content with AD, but they might still have mainframes, legacy applications, non-Microsoft DBMS servers.

Non-IT-related user information will still be managed in multiple places, including an H.R. system, a payroll system, a contracts management system, a phone directory, etc.

Many organizations also choose to consolidate to multiple directories, rather than just one directory. For example, some companies deploy a Sun or IBM directory service to support web applications, and Active Directory to support network login and other Microsoft server products.

Other organizations may deploy multiple AD directories, and some users will log into more than one.

The net result is that while AD reduces the problems that arise from too many user directories, organizations are almost never able to reduce the number of directories to just one. ILM2007, password management and user provisioning continue to serve a valuable function to resolve the directory management issues that remain.

3 Password Management and User Provisioning Systems Defined

Another class of systems targeted at medium to large organizations streamline heterogeneous management of passwords, provisioning of login access, and termination of that access:

Hitachi ID Management Suite includes both the Hitachi ID Password Manager Synchronization and Self-Service Password Reset and the Hitachi ID Identity Manager Automated Onboarding, Synchronization and Deactivation.

3.1 Password Management Systems Defined

Password management systems are designed to reduce the cost of ownership of password-based authentication, and to improve the security of password authentication.

Hitachi ID Password Manager is a password management system that supports:

- Password synchronization, both automated and web-based, to reduce the password management burden on users.
- Self-service password reset, allowing users to reset their own passwords if they forget them or trigger an intruder lockout, without calling the help desk.
- Assisted password reset, which streamlines resolution of password problem calls made to the help desk.

Hitachi ID Password Manager yields cost savings by:

- Reducing the frequency of password problems (synchronization).
- Diverting password problem calls away from the help desk (self-service reset).
- Shortening password call resolution at the help desk (assisted reset).

Hitachi ID Password Manager improves security by:

- Reducing the number of written passwords (synchronization).
- Enforcing strong, global password quality rules.
- Enforcing sound authentication prior to all password resets.
- Encrypting all network traffic and data storage related to password management.
- Making it possible to delegate the password reset privilege to support analysts without giving them other rights.

3.2 User Provisioning Systems Defined

User provisioning systems are designed to streamline change management to login systems. They reduce the delay between organizational change and matching changes in user access to I.T. infrastructure, and ensure that user access is terminated once it is no longer required.

Hitachi ID Identity Manager is an user provisioning system that supports:

- An automated, rules-based provisioning system that monitors organizational changes on other systems (e.g., H.R. system) and makes matching updates to login systems.
- A web + mail self-service workflow system for entering change requests, routing them to authorizers, reviewing and approving change requests, and automatically updating system access based on approved requests.
- A web-based central administration system where a security officer can make global changes to user access rights, across heterogeneous systems, and local, delegated administrators can do the same for users within their jurisdiction.

Hitachi ID Identity Manager yields cost savings by:

- Reducing the time users must wait for new or changed access.
- Reducing the number of security administrators that must be engaged to manage systems access changes.
- Streamlining system migrations.
- Cleaning up orphan accounts, which can reduce software license costs.

Hitachi ID Identity Manager improves security by:

- Ensuring effective and rapid access termination.
- Removing orphan accounts.
- Enforcing standards when creating new users.
- Enforcing proper authorization rules on all changes.
- Maintaining a forensic change and audit log for all changes.

4 Common Components in ILM2007 and Hitachi ID Management Suite

ILM2007 and Hitachi ID Management Suite share some common components:

- Agents that list user IDs and user attributes from managed systems.
- Agents that create, modify and delete users on managed systems.
- An internal database or directory that represents a master list of users, and what each user's login ID is on each system.

ILM2007 and Hitachi ID Management Suite also share at least one key process, which is to correlate possibly different user IDs on different systems to one-another, and to users. This “join” process is frequently the most complex part the deployment of any identity management system.

5 The Value of Integration

ILM2007 and Hitachi ID Management Suite have almost no overlapping functionality, but do share some infrastructure, as described above.

Integration between these systems yields value by minimizing the total deployment effort of the products. For example, once an infrastructure is activated to collect login IDs and ID correlation with one system, the resulting data set should be shared with the other two systems, rather than regenerated.

Similarly, once agents have been configured on one system to manage users, passwords or other attributes on one directory, it makes sense to leverage the same infrastructure for the other systems, rather than deploying a new set of agents in each case.

6 Integrated Deployment Strategies

The following sections describe two alternate strategies to deploy both ILM2007 and Hitachi ID Management Suite in a way that maximizes the investment in infrastructure, and minimizes the total effort required to configure the two systems.

6.1 ILM2007 First: Leverage Existing Login ID Profiles

For organizations that have already deployed ILM2007, prior to installing Hitachi ID Password Manager or Hitachi ID Identity Manager, it makes sense to leverage the data set in ILM2007, that correlates user IDs between systems.

Hitachi ID Password Manager and Hitachi ID Identity Manager both include a plugin point which allows them to access user and user profiles on an external directory rather than internally. This is accomplished using the `PARSE ACCOUNT EXT` plugin point. When this plugin is used, the Hitachi ID Password Manager user and account databases become a temporary cache for user and login ID information.

Alternately, Hitachi ID Password Manager or Hitachi ID Identity Manager can be configured with either a one-time or periodic batch load of data from ILM2007.

6.2 Hitachi ID Password Manager First: Self-Service Login ID Reconciliation

When Hitachi ID Password Manager is deployed before ILM2007, or where the join data available to ILM2007, which might be used to link accounts on different systems, is limited in scope or incomplete at the time of Hitachi ID Password Manager deployment, it may make sense to leverage Hitachi ID Password Manager's built-in capability to correlate login IDs across systems, and to push this data out to ILM2007.

Where users have consistent login IDs across multiple systems, either ILM2007 or Hitachi ID Password Manager can correlate login IDs automatically, using data from a nightly auto-discovery process.

Where users have different login IDs across multiple systems, and there are no convenient, reliable or consistently filled-in attributes to correlate user objects across systems, Hitachi ID Password Manager provides a self-service process, which automatically prompts users to fill in their own login IDs, prove possession of these IDs by typing their own passwords, and dynamically writing this data out to a global directory (e.g., an LDAP directory or a central database).

This process leverages the users' own knowledge of their login ID profiles to quickly assemble a comprehensive and validated set of login ID correlation data.

Each user's login IDs on other systems can be written into new attributes in Active Directory either in real time or in nightly batch updates, where it is available to ILM2007 as a key field for connecting user objects on other systems to Active Directory.

7 Extending ILM2007 Functionality

7.1 Background

ILM2007 has built-in management agents for Windows, NetWare, Lotus Notes, Sun LDAP and DBMS servers. It also has management agents for various types of file formats, but these are only intermediaries with actual target systems.

ILM2007 does not have built-in connectors to ERP applications such as SAP R/3, to mainframe systems such as zOS or OS390, to Unix or Linux servers, or to custom or vertical applications.

7.2 Initializing Passwords

ILM2007 operates in batch mode, and can only read password hashes stored on managed directories. Since every kind of managed system uses a different password hashing algorithm, it is impossible to copy a usable password from one directory to another.

This limitation means that while ILM2007 can discover new login IDs on one system, and create matching login IDs for the same users on other systems, it cannot set a matching password for newly-created login IDs. Rather, it must set initial passwords using an algorithm, for example based on the user's name, department code, login ID, etc. Such initial passwords are typically set to expire on first use.

Initial passwords assigned algorithmically based on user attributes are predictable, and so less secure than passwords synchronized from other systems where the user already has an active account.

This limitation is resolved with Hitachi ID Password Manager. ILM2007 can set initial passwords on new login IDs to a random string, which the user does not know. Users are then prompted to use Hitachi ID Password Manager's password synchronization system to change all of their passwords – including the password on the new login ID – to a single new value.

This solution makes it possible to use ILM2007 to create new login IDs on password-protected systems, without using default passwords or sending initial passwords to users in an insecure e-mail.

This is best illustrated by an example:

1. An administrator adds user X to Active Directory (AD).
2. User X logs into AD.
3. At night, ILM2007 detects the new login ID (User X on AD), and creates a new login ID for the same user on a Sun ONE directory (User X on SONE). The new login ID has a random password.
4. ILM2007 sends user X an e-mail, asking him to change his passwords in order to activate his Sun ONE login account.
5. User X logs into AD, and changes his password.
6. Hitachi ID Password Manager synchronizes the password from AD to SONE.
7. User X logs into SONE, with the same password he just set on AD.

7.3 Increased Reach: Leveraging Hitachi ID Identity Manager Agents

Another form of integration is to use Hitachi ID Identity Manager agents to increase the reach of ILM2007 to new platforms. Hitachi ID Management Suite includes agents for mainframe systems (e.g., zOS), enterprise resource planning systems (e.g., SAP R/3), Unix servers and more. It also has more functional agents for some systems – for example, it can provision Lotus Notes ID files and deliver them to workstations.

Hitachi ID Identity Manager exposes a SOAP web service, which can be used to connect ILM2007 indirectly to target systems for which it does not have native connectors.

8 Summary

There is significant shared infrastructure, but almost no functional overlap, between password management, user provisioning and meta directory products such as ILM2007. All three form valuable components of an identity management infrastructure.

Deployment of the three products (ILM2007, Hitachi ID Password Manager, Hitachi ID Identity Manager) should be considered together, as installation of components of one system can be leveraged to accelerate deployment of the others.

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

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

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