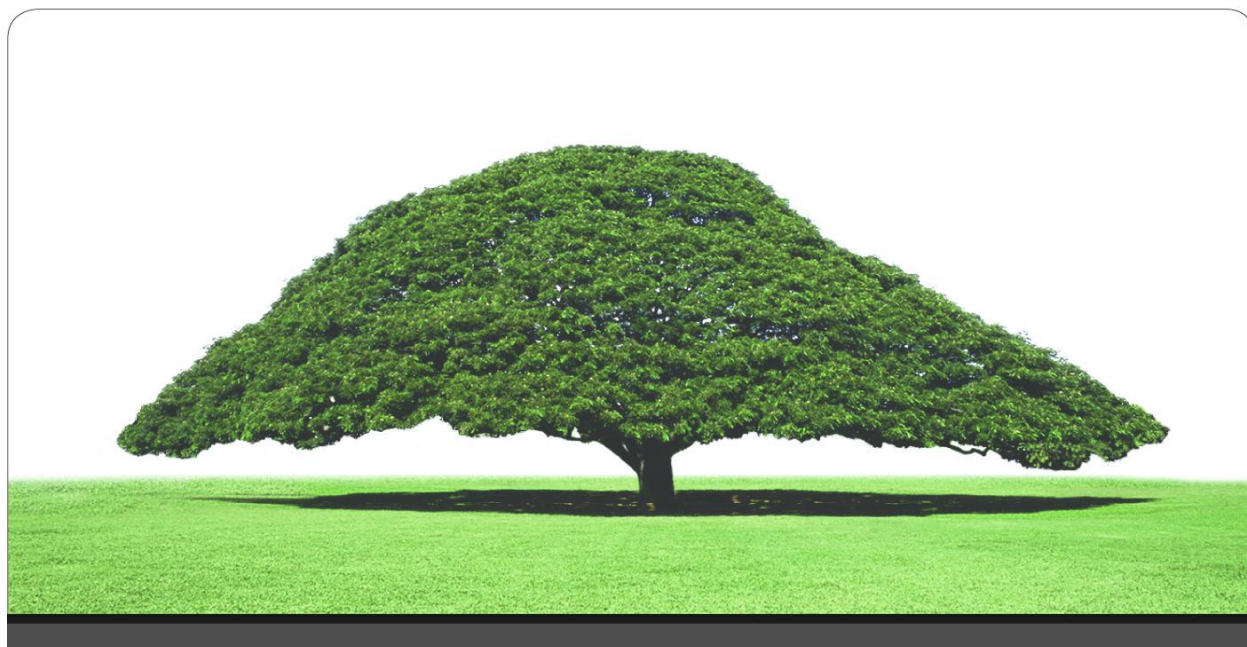


© Hitachi ID Systems, Inc.



Integrating Hitachi ID Management Suite with Meta Directories

Meta directories are becoming a widely deployed tool for managing user identity information, such as login ID, full name, e-mail address and other personal attributes, in a consistent manner across multiple directories.

Meta directories, password management and account provisioning tools are sometimes seen as redundant. In reality, they are complementary tools, with almost no overlapping functionality. Integrating meta directories with password management and provisioning tools provides increased value to organizations with heterogeneous systems.

The strength of meta directories is to synchronize attributes of user objects between directories, H.R. systems and mail systems. Password management tools extend this capability to include the password attribute, which meta directories cannot manage directly, due to inconsistent hashes. Account provisioning tools extend directory management further by adding a workflow for change request entry / routing / authorization, and by supporting creation of password-protected user objects.

Integrating meta directory, password management and account provisioning products yields maximum value for identity management.

This paper discusses how Hitachi ID Password Manager (P-Synch™) and Hitachi ID Identity Manager (ID-Synch™) can be deployed in conjunction with meta directory products, how the technologies interact, and how they complement one another.

Contents

1	Introduction	1
2	Meta directories defined	3
2.1	How meta directories relate to Active Directory	3
3	Password management and provisioning systems defined	5
3.1	Password management systems defined	5
3.2	User provisioning systems defined	5
4	Common components in meta directories, Hitachi ID Password Manager and Hitachi ID Identity Manager	8
5	The value of integration	8
6	Integrated deployment strategies	9
6.1	Meta directory first	9
6.2	The Hitachi ID Management Suite first	9
7	Extending meta directory functionality	11
7.1	Background	11



7.2	Initializing passwords	11
7.3	Connectors	12
8	Summary	13
9	References	13

1 Introduction

Meta directories are becoming a widely deployed tool for managing user identity information, such as login ID, full name, e-mail address and other personal attributes, in a consistent manner across multiple directories.

Meta directories, password management and account provisioning tools are sometimes seen as redundant. In reality, they are complementary tools, with almost no overlapping functionality. Integrating meta directories with password management and provisioning tools provides increased value to organizations with heterogeneous systems.

The strength of meta directories is to synchronize attributes of user objects between directories, H.R. systems and mail systems. Password management tools extend this capability to include the password attribute, which meta directories cannot manage directly, due to inconsistent hashes. Account provisioning tools extend directory management further by adding a workflow for change request entry / routing / authorization, and by supporting creation of password-protected user objects.

Integrating meta directory, password management and account provisioning products yields maximum value for identity management.

This paper discusses how Hitachi ID Password Manager and Hitachi ID Identity Manager can be deployed in conjunction with meta directory products, how the technologies interact, and how they complement one another.

The remainder of this paper is organized as follows:

- **Meta directories defined:**

A brief definition of meta directory products.

- **How meta directories relate 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 and effective password management.

- **Common components and processes:**

Some software components and processes that meta directories have in common with password management and account provisioning tools such as Hitachi ID Password Manager and Hitachi ID Identity Manager.

- **Meta directory first:**

Integration between Hitachi ID Password Manager/Hitachi ID Identity Manager and meta directories in the situation where the meta directory was already deployed when the password management or provisioning project begins.

- **Hitachi ID Password Manager first:**

Integration between Hitachi ID Password Manager/Hitachi ID Identity Manager and meta directories in the situation where the password management or provisioning project precedes deployment of a meta directory.

- **Extending meta directory functionality:**

Integrating Hitachi ID Management Suite with Meta Directories

Some ideas about how technology in Hitachi ID Identity Manager may be used to extend the functionality of a meta directory in the future.

2 Meta directories defined

Meta directories are engines that synchronize data about users between different systems. A meta directory works as follows:

- Connectors to multiple target systems are configured, to read and write user profile data.
- Data streams from integrated systems are merged, to construct a master database of user profile information.
- Where a user's data in the master database differs from that user's profile on a lower-priority target system, the target system is updated to reflect the user's current information.
- Users may be added to or removed from target systems, based on changes detected on systems of record.

Meta directories simplify user administration by propagating changes from systems of record to managed systems, eliminating manual updates.

Since meta directories do not normally expose a user interface, or interact directly with users, they can be thought of as "plumbing" embedded in an enterprise identity management infrastructure.

An excellent meta directory product is ILM from Microsoft.

2.1 How meta directories relate to Active Directory

Many organizations are migrating their network operating system from AD on Windows 2000 or eDirectory on Novell NetWare to Active Directory on Windows 2003 or 2008.

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 meta directories, since their 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. Meta directories and password management continue to serve a valuable function to resolve the directory management issues that remain.

3 Password management and provisioning systems defined

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

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 authentication 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

A user provisioning application is middleware used to create, modify and delete user objects on one or more directories, systems and applications. User provisioning is intended to make the administration of users on multiple systems faster, cheaper and more reliable.

To accomplish these goals, user provisioning applications must automate one or more business processes:

- **Automation / Change Propagation:**
Changes to user profiles on authoritative systems (e.g., HR or contractor management) trigger automatic updates to the same users' profiles on managed systems.
- **Self service / Workflow:**
Users or automatic processes submit change requests – to provision new access, change existing user profiles or deactivate users. Requests are automatically routed to business users with suitable authority, who approve or reject them. Approved changes are applied to managed systems.
- **Consolidation:**
Security administrators with an enterprise-wide scope of authority update user access to multiple managed systems from a single security administration console, that creates a consolidated view of multiple security databases.
- **Delegation:**
Regional or departmental security administrators are granted limited access to manage some users, on some systems, through the consolidated security administration console.
- **Fulfillment:**
This is not so much a process, rather the ability of one user management system to implement changes initiated on another system.

As well, a user provisioning system must be able to map the output of these processes to actual updates to user objects on managed systems. Updates typically include:

- Create new and delete existing accounts for a user.
- Check enabled/disabled status of existing accounts.
- Set enabled/disabled status of existing accounts.
- Change the login ID of an existing account (rename user).
- Read and set attributes of existing user accounts.
- Modify the membership of existing accounts in security groups – for example, attach to / detach from group.
- Change the context of a user in a structured directory – for example, move in LDAP or NDS.

Hitachi ID Identity Manager is a user provisioning system. Organizations deploy it to produce one or more of the following benefits:

Hitachi ID 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

Hitachi ID 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 Common components in meta directories, Hitachi ID Password Manager and Hitachi ID Identity Manager

Meta directory products and the Hitachi ID Management Suite share some common components:

- Agents that list user IDs, privileges and identity 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 each user profiles login IDs, identity attributes and security privileges.

Meta directory products and the 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

Meta directories and the Hitachi ID Management Suite have almost limited 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 a meta directory product and the Hitachi ID Management Suite in a way that maximizes the investment in infrastructure, and minimizes the configuration effort.

6.1 Meta directory first

For organizations that have already deployed a meta directory, prior to installing the Hitachi ID Management Suite, it makes sense to leverage the data set in the meta directory, that correlates user IDs between systems.

Hitachi ID Password Manager includes a plugin point which allows it to access user and account 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 tables become a temporary cache for user and login ID information.

Alternately, the Hitachi ID Management Suite can be configured with either a one-time or periodic batch load of data from the meta directory.

6.2 The Hitachi ID Management Suite first

When the Hitachi ID Management Suite is deployed before a meta directory, or where the join data set in the meta directory is limited in scope or incomplete at the time of the Hitachi ID Management Suite deployment, it may make sense to leverage the Hitachi ID Management Suite's built-in capability to correlate login IDs across systems, and to push this data out to the meta directory.

Where systems have consistent login IDs, the Hitachi ID Management Suite correlates them 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, the Hitachi ID Management Suite 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, as illustrated in [Figure 1](#).

This data can be fed into a meta directory either in real time (using an exit trap such as `UALS UPDATE SUCCESS`) or in nightly batch updates.

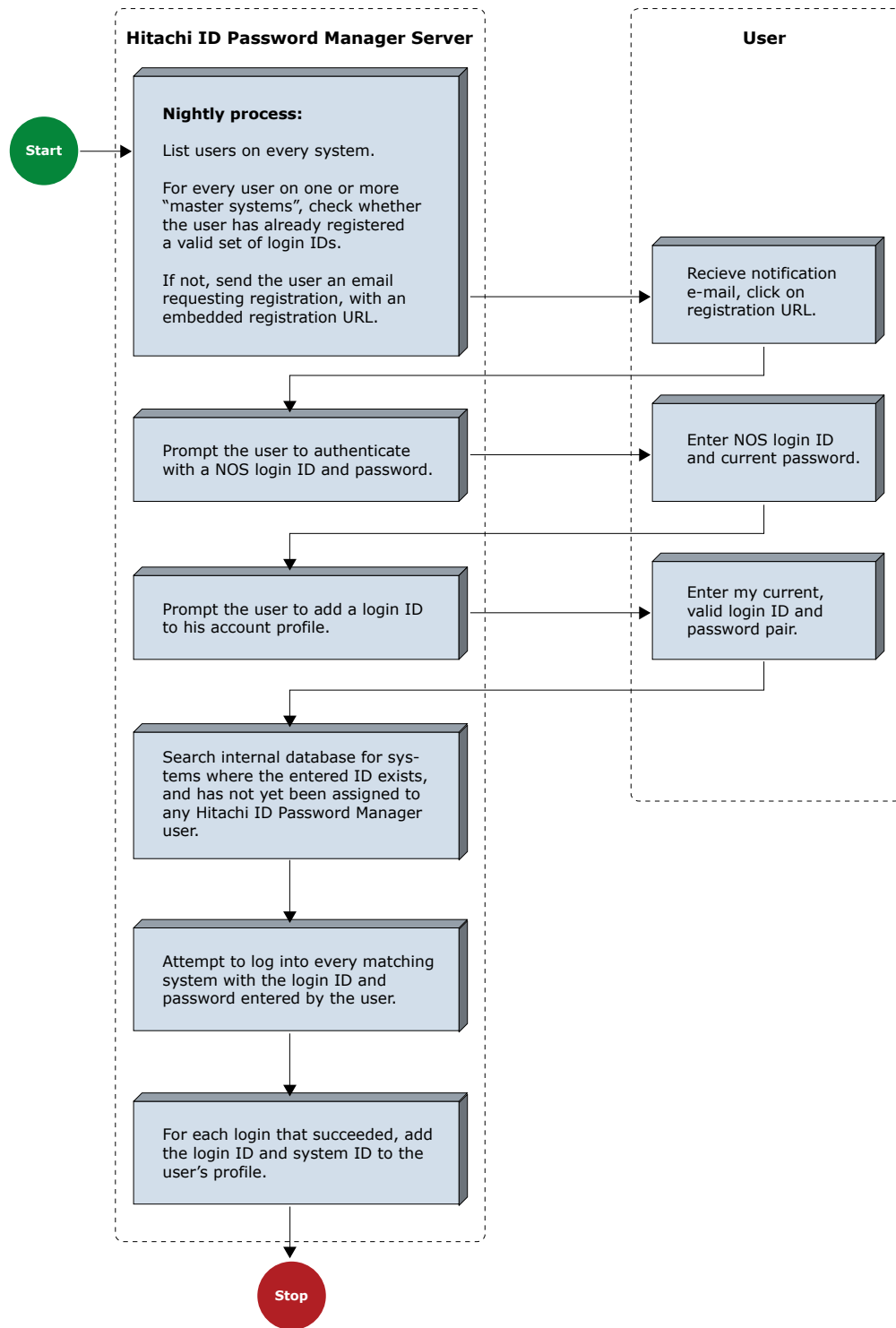


Figure 1: Self-Service Login ID Reconciliation Process

7 Extending meta directory functionality

7.1 Background

Most of the meta directory products currently on the market evolved from products designed to synchronize data among e-mail systems, and between e-mail systems and network operating systems.

As a consequence, they generally support e-mail systems, LDAP directories and network login IDs well, but frequently have limited support for other systems that users log into, such as ERP applications, mainframe systems, DBMS servers, etc.

7.2 Initializing passwords

Meta directories normally operate 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 meta directories can discover new login IDs on one system, and create matching login IDs for the same users on other systems, they cannot set an initial password for newly-created login IDs.

This limitation is resolved with Hitachi ID Password Manager. The meta directory can set initial passwords on new login IDs to a random number, 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 a meta directory 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, the meta directory 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. The meta directory 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 Connectors

The Hitachi ID Management Suite exposes a SOAP API which allows it to provide connectivity to meta directories into systems for which they do not include native connectors. For example, Hitachi ID Management Suite includes powerful SAP R/3, PeopleSoft, JD Edwards, iSeries and zSeries connectors that perform better than anything available from contemporary meta directory products.

The Hitachi ID Management Suite ships with a native “management agent” for the Microsoft metadirectory (formerly called MIIS, currently renamed ILM) which makes it especially easy to connect to these and other systems with the Hitachi ID Management Suite as an intermediary.

8 Summary

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

Deployment of both products (meta directory, the Hitachi ID Management Suite) should be considered together, as installation of components of one system can be leveraged to accelerate deployment of the others.

9 References

Meta directory vendors today include:

Vendor	Product	Web site
Critical Path	CP Meta Directory Server	http://cp.net
Microsoft	ILM/MIIS	http://microsoft.com/ilm
Siemens	DirX	http://siemens.com

Notes: ¹: IBM acquired MetaMerge and intends to package it as a part of an IBM Identity Management suite.

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/>.