

Best Practices

for Identity Management Projects



Contents

- 1 Introduction 1
- 2 Overview: Defining Identity Management 2
- 3 Long Term Commitment 3
- 4 Focus on Business Drivers 6
- 5 Deliver Early and Often 10
- 6 Usability and Adoption 11
- 7 Critical Path and Common Interdependencies 13
- 8 Project Management Methodology 15
- 9 Typical Timeline and Deliverables 17

- APPENDICES 20**

- A Hitachi ID Identity Management Solutions 21**
- A.1 Management Suite Overview 21
- A.2 Identity Manager 22
- A.3 Access Certifier 26
- A.4 Password Manager 28
- A.5 Group Manager 30
- A.6 Privileged Access Manager 31

1 Introduction

This document presents best practices for deploying and operating an identity management infrastructure. It builds on Hitachi ID's years of experience in deploying password management and user provisioning into some of the largest and most complex organizations in the world.

The document is organized as follows:

- **Overview: Defining Identity Management:**

Some basic definitions that help clarify the subsequent material.

- **Long Term Commitment:**

Identity management is more accurately described as a change in the IT organization and business processes than a finite project. Deployment can reasonably be expected to continue indefinitely, with more features and integrations are added over time.

- **Focus on Business Drivers:**

Given the long-term investment in identity management, it makes sense to identify and focus the highest priority business drivers first.

- **Deliver Early and Often:**

To minimize project risk and to ensure a positive return on investment, it is essential to deliver tangible results early in the project, and keep delivering new benefits regularly.

- **Usability and Adoption:**

Identity management is focused on the user – a human being represented on multiple IT systems, by a combination of identity attributes and privileges. It follows that user adoption is a prerequisite to success.

- **Critical Path and Common Interdependencies:**

Some integrations and features depend on others. This section identifies major interdependencies, which impact project timelines.

- **Project Management Methodology:**

A typical methodology for delivering a given project milestone.

- **Typical Timeline and Deliverables:**

Pulling all of the above together, a sample project timeline is developed, step-by-step.

2 Overview: Defining Identity Management

Identity and access management is defined as a shared platform and consistent processes for managing information about users: who they are, how they are authenticated and what they can access.

Enterprise Identity and Access Management (IAM) is defined as a set of processes and technologies to effectively and consistently manage modest numbers of users and entitlements across multiple systems. In this definition, there are typically significantly fewer than a million users, but users typically have access to multiple systems and applications.

Typical enterprise identity and access management scenarios include:

- Password synchronization and self-service password reset.
- User provisioning, including identity synchronization, auto-provisioning and automatic access deactivation, self-service security requests, approvals workflow and consolidated reporting.
- Enterprise single sign-on – automatically filling login prompts on client applications.
- Web single sign-on – consolidating authentication and authorization processes across multiple web applications.

3 Long Term Commitment

Identity management projects tend to be long, and indeed may never end, as deliverables are continually added over the life of the system. Organizations go through both business and infrastructure changes: reorganizations, hardware upgrades, new operating systems, new applications, etc. These changes trigger matching requirements in the identity management infrastructure and consequently lead to implementation and maintenance effort over the life of the system.

This is not to imply that individual deliverables cannot be implemented quickly and operated at low cost. Rather, it means that successful implementation of one feature or integration usually triggers interest by a wider range of stake-holders, who request further work, to deliver more features and integrate with more infrastructure.

With this in mind, it can be helpful to think of identity management implementation in terms of a process of continuous optimization, which is the responsibility of a permanent team, rather than a single, finite project.

As with any long term project, it is important to have clear buy-in from stake-holders and an up-front agreement on project scope, deliverables, duration and cost in order to sustain investment and deliver on business expectations. Without such early commitment by stake-holders, project work may be aborted before deliverables are reached.

BEST PRACTICE	Engage stake-holders early and clearly articulate project deliverables, timeline and cost.
----------------------	--

Identity management automation can impact a wide range of stake-holders, so it is important to understand who they are and engage them early. This reduces the risk that an important decision maker learns about the project later and disrupts it because he or she was not consulted earlier.

Stake-holders who may be interested in an identity management project include:

Stake-holder	Impact
The IdM Infrastructure owner(s)	Someone must be responsible for acquiring, deploying and maintaining infrastructure such as directories, user provisioning automation, password management, single sign-on, etc.
End user support	Impacts range from reduced password reset call volume to a need for user education, support and training for new processes.
System administrators	Identity data will be modified on their systems. They will be asked to hand out administrator-level credentials, and may be asked to install software on their systems.
IT Security	IT security will have to set policies for the new automation.
Audit	The new automation will enforce rules regarding internal controls and also enable audits of user privileges and change history.
Desktop Support	May be impacted, if client software is deployed to user workstations (e.g., GINA extensions, single sign-on components, Notes ID file delivery, smart card readers, etc.).
Network Operations	Need to know about where servers will be racked, what bandwidth will be consumed, etc.
Human Resources	May be asked to provide a data feed from systems of record. May receive updates asking them to correct errors in their system. Are likely the first point of contact for new hires and the last point of contact for terminated users.

BEST PRACTICE Engage all stake-holders from the project's inception, rather than deferring conversations with some of them until later in the project.

Since there may be a large number of stake-holders, they are likely to disagree on many issues. To resolve such disagreements and keep the project moving smoothly, it is important to have strong sponsorship that can motivate this diverse group of stake-holders to cooperate, even when decisions are made that contradict their opinions.

BEST PRACTICE Engage executive-level sponsorship, to resolve conflicts between stake-holders.

It is important to garner business ownership of the solution. A good sponsorship and governance approach will facilitate this, and help to insure that the project is seen favorably by the non-IT side of the organization.

— Kevin Kampman
Senior Analyst
The Burton Group

Technology used to automate identity management can be quite complex and vendor services to implement and maintain it can be expensive. It therefore makes sense to assign a full-time, technical resource to assist

in system deployment and to take responsibility for ongoing technical work, including adding new integrations, adjusting business logic, customizing the user interface, performing upgrades and troubleshooting problems. This reduces project cost, shortens timelines and improves SLA.

BEST PRACTICE	Employ a full-time, technical resource from the start of implementation. This resource will assist in deployment and to manage the system in production.
---------------	--

The technical resource tasked with implementation and maintenance of the identity management infrastructure should have expertise with operating systems, directories, HTML markup and at least one scripting or programming language (e.g., Perl, JavaScript, C++, C#, Java, etc.).

Inevitably, this technical resource will have somewhat different priorities than security officers and architects, such as a strong interest in ease of maintenance and deployment effort. It makes sense for the business owner of the identity management infrastructure to be a part of any product selection and evaluation process, rather than dropping a pre-determined choice of product and architecture on a technical resource and hoping that he or she can subsequently resolve any issues that may come up.

BEST PRACTICE	Engage a technical resource who will become the permanent system administrator of the identity management infrastructure in product selection.
---------------	--

4 Focus on Business Drivers

There are several business drivers for deploying an enterprise identity and access management system, including:

- **Security and regulatory compliance:**

- Reliable access deactivation when users leave the organization.
- Secure access to privileged passwords.
- Enforce segregation of duties policies.
- Periodically review security entitlements and eliminate unneeded ones.
- Ensure that new access is provisioned in compliance with standards.

- **IT support cost:**

- Lower IT support call volume and head count.
- Reduce the amount of manual security administration required.

- **User service:**

- Simplify change request processes.
- Provision required access more quickly.
- Reduce the number of passwords users must manage.
- Reduce the number of login prompts users must complete.

Since it can take a long time to deliver on each and every one of these drivers, it is important to prioritize. As much as possible, high priority deliverables should be completed before work begins on lower priority ones.

For example, if reducing help desk call volume is a primary motivation, then password synchronization and self-service password reset should come first. If security risks associated with orphan and dormant accounts are important, then automated access termination and access certification should come first. If rapid onboarding of new employees is important, then automated provisioning of new users or self-service onboarding requests should be implemented first.

BEST PRACTICE	Prioritize business drivers at the start of the project and focus on only the most urgent deliverables.
----------------------	---

Along with prioritization of work by business drivers, it is important to be able to measure success. This is done by establishing metrics for measuring success in delivering on any given business driver and by measuring these metrics both before and after deployment.

When communicating the benefits of the solution, it is critical to focus on business value. The emphasis may seem subtle and unimportant, but making users more productive faster, improving the user experience, providing more efficient access, and so on have more meaning to your executives than better security and a lower cost of administration.

— Kevin Kampman
Senior Analyst
The Burton Group

BEST PRACTICE Establish metrics to support each business driver and measure results both before and after deployment.

Some sample metrics include:

Driver	Metric	Measured as
C	HD password reset call volume	Password reset help desk calls per month (average and peak).
C	HD FTEs	Number of FTEs required to support peak password reset call volumes.
C	AD group admin workload	Group membership changes that hit the human service desk, monthly.
C	Admin FTEs	Number of FTEs required to support management of AD group membership.
P	Employee setup authorization	Days from HR trigger to setup a new employee.
P	Contractor setup authorization	Days from manager call to setup a new contractor.
C+P	Setup time	Number of IT work hours required to setup a new user.
S	Deactivation time	Days from HR/manager trigger to deactivate a departed user.
C+S	Deactivation effort	Number of IT work hours required to terminate access for a departed user.
S	Termination delay	On average, days from actual termination to when HR notifies IT.
S	Weak passwords	Number of systems that do not enforce length, character set, history and dictionary rules.
S	Standard caller authentication	Number of standardized questions asked to authenticate HD callers.
S	Personalized caller authentication	Number of user-defined questions asked to authenticate HD callers.
S	Standard caller auth (2)	Number of available standardized questions from which authentication process draws random questions.

Driver	Metric	Measured as
S	Personalized caller auth (2)	Number of available user-defined questions from which authentication process draws random questions.
S	Non-expiring systems	Number of systems that currently do not enforce a password expiry policy.
S	User password age	Enforceable maximum age of user passwords.
S	Admin password age	Enforceable maximum age of administrator passwords.
C+S	Orphan accounts	Per enterprise-wide system: number of user objects divided by the number of employees and contractors.
C+S	Dormant accounts	Per system: number of accounts inactive for at least N days.
C+S	Unassociated systems	Number of systems whose unique user identifiers are not mapped to a corporate-wide identifier.
S	Admin password change interval	Per system: frequency of change of admin passwords (days).
S	Password replication scope	Per system: number of other systems that share credentials with this one.
S	Password sharing scope	Per system: number of IT users that know the admin credentials at any given time.
C+P	New user request complexity	Number of different forms used to request new login IDs, on different systems, or for different locations, or for different classes of users.
C+P	New access request complexity	Number of different forms used to request new security rights for an existing user.
C+P	Identity change request complexity	Number of different forms used to request changes to user identity data (name, phone, address, department, location, etc.).
C+P	Passwords per user	Average number of passwords a user must remember for corporation-owned systems.
C+P	Login prompts per user per day	Average number of times per day that a user must sign into some corporate system.

In the table above, a “C” in the business driver column means cost reduction, “P” means user productivity and “S” means security.

Your metrics should also be expressed in terms that are meaningful to the organization. Removing hours and days from the on- or off-boarding cycle is a more compelling success story than consolidating Active Directory groups. Always speak to the business issue that is specific and relevant, even when there is a tremendous amount of technical effort that makes it happen.

— Kevin Kampman
Senior Analyst
The Burton Group

5 Deliver Early and Often

The time required to implement a featureful and well integrated identity management system can span into years. Over such a long span of time, stake-holders may lose interest and withdraw support and/or funding.

Also, requirements change over time, as both business processes and infrastructure evolve. This means that a lengthy project to implement a fixed set of deliverables is likely to fail, simply because by when the work is complete, the original requirements will have changed.

To avoid both of these problems, it is imperative to deliver results in the implementation project early and to deliver new results regularly.

BEST PRACTICE	Deliver functionality that is relevant to the business every 3–6 months.
---------------	--

Since both requirements and priorities will change over time, it makes sense to kick off a long-term identity management project with only a rough outline of project milestones. The sequence of priorities, and which task to undertake next, should be re-evaluated after every one or two milestones.

BEST PRACTICE	Start long identity management projects with a rough outline of business priorities and milestones.
---------------	---

BEST PRACTICE	Re-evaluate priorities after every one or two milestones.
---------------	---

To address the fact that both business processes and technical infrastructure change constantly, it makes sense to capture detailed requirements and construct a solution design for any given function only when the implementation team is ready to start work on that function.

Deferring detailed design until just before a given work phase can commence eliminates situations where a feature is designed, in great detail and at great cost, long before implementation can commence. Such early planning is actually very risky, since requirements are likely to change in the interval between solution design and implementation, which leads to one of two undesirable outcomes: redoing the detailed (but premature) discovery and solution design or implementing a system to meet outdated specifications.

BEST PRACTICE	Defer detailed discovery and solution design for each phase until the team is ready to start implementing that phase.
---------------	---

Finally, it makes sense to build up expertise in the implementation team. Start with small, simple functions and work up to more complex deliverables in later phases. This reduces overall project risk and ensures early return on investment.

BEST PRACTICE	Start with small, simple deliverables. Work up to more complex functions and integrations.
---------------	--

6 Usability and Adoption

The function of an identity management system is to manage data about users: their identity attributes, authentication factors and security privileges. As might be expected, most identity management systems, sooner or later, interact with these users. Such interaction is required to manage passwords, confirm and update identity attributes, request and approve privilege changes, audit user data, etc.

In many scenarios, the business value of the identity management system depends on user adoption. For example, a self-service password reset system only generates user support cost savings if users choose to use it, rather than calling the help desk. Similarly, a user provisioning system can only reduce security administrator workload if users make security change requests through its workflow user interface, and not by calling a security administrator.

To ensure user adoption, the identity management deployment team must incorporate activities designed to engage the user community in the deployment plan:

BEST PRACTICE	Plan for user acceptance testing, pilot tests, user awareness programs and user education.
---------------	--

In addition to engaging users to validate usability, ensure awareness and verify that users understand how to use the system, it is helpful to organize a program to drive high user adoption. This includes usability testing and awareness programs and adds incentives for users to adopt the system and disincentives to users who do not. Example incentives include synchronized passwords, reduced signon and offline items such as prize draws, gift certificates, etc. Example dis-incentives include reduced help desk service for human (as opposed to automated) service, charge-backs, etc.

BEST PRACTICE	Organize a formal program to drive high user adoption for every user-facing component of the identity management system.
---------------	--

An important concept to consider when designing a usable system is that of “one stop shop.” In short, this means that when a user wishes to perform a function – for example, to request that a new login ID be provisioned – the user should not have to first consider which request input system to visit, based on which one happens to be in-scope for the identity management infrastructure, as opposed to managed by a legacy business process.

Since it is impractical to deploy hundreds of integrations at a time and since some infrastructure may not be cost effective to manage with automation (example: an application with 20 users does not merit 5 days of integration effort), partial or “manual” integrations are desirable. It makes sense to provide users with a single change request user interface, to automate whatever actions possible, and to forward the remaining types of changes to human system administrators.

BEST PRACTICE	Provide a consolidated change request user interface and identify “implementers” to fulfill change types for which automation is not available.
---------------	---

Another side effect of engaging users is that they must be informed whenever the system changes. If a system changes often, this creates a flurry of e-mails in user in-boxes, which users learn to ignore. Too-frequent user notifications can act to defeat a user adoption program.

The need to keep users informed means that integrations with target systems should be grouped, so that users can be informed of new integrations less often, in a more meaningful way. For example, a quarterly e-mail about five more systems that have been brought into scope is more helpful than a weekly e-mail about another directory OU.

BEST PRACTICE	To reduce user impact, implement multiple integrations at a time, rather than defining a project milestone around every target system.
----------------------	--

The benefits of minimizing user announcements also acts as a counter-weight to the strategy of multiple, short deliverables. While it makes sense to define milestones every 3 to 6 months, it does not make sense to subdivide a project into weekly or monthly deliverables.

7 Critical Path and Common Interdependencies

When deploying an identity management system, some tasks cannot be started until others are completed. Such interdependencies may delay high priority deliverables until items which appear to be less important, but which are pre-requisite, are completed.

Following are some common implementation tasks that must be performed early in a project, to support later deliverables:

1. Integrate with a source of profile IDs:

Every user must have a unique, global identifier. These identifiers are normally drawn from one or more existing systems, and these existing systems are referred to as sources of profile IDs. Integration with sources of profile IDs, such as Active Directory, e-mail systems or HR data feeds, generally precede all other integrations.

2. Reconcile login IDs:

Users normally have records and login accounts on multiple systems and one of the core functions of an identity management system is to consolidate management of these user objects. It is impossible to manage multiple user objects coherently until they are connected to one another – in other words, until login IDs on different systems are reconciled with one another and attached to global profile IDs.

Login ID reconciliation necessarily precedes password synchronization, password reset, user deprovisioning and access certification, at a minimum.

3. E-mail integration:

An identity management system may, from time to time, have to contact users – either to notify them of an event or to request some action. Examples of this are asking users to complete a personal challenge/response profile, notifying users of failed login attempts relating to their profile, asking authorizers to approve security change requests, etc.

Communication initiated by the identity management system is usually implemented using e-mail. One of the first integrations in a typical deployment is therefore with the e-mail system, to deliver messages to users.

4. Construct an org-chart:

Several functions in an identity management system typically depend on data mapping every user to their direct manager/supervisor:

- (a) Authorization: managers are typically asked to approve security change requests relating to their subordinates.
- (b) Escalation: when a given change authorizer repeatedly fails to respond to a given change request, the simplest choice of an alternate, escalation authorizer is the first authorizer's direct manager.
- (c) Certification: managers are often asked to periodically review a list of their direct subordinates and their security rights, in order to identify and remove inappropriate access rights.

Delivering a process to construct and maintain reliable org-chart data, that covers all users is often an early deliverable in an identity management project.

5. Authorization workflow:

Many changes initiated by or passed through an identity management system require authorization before they can be applied to target systems. This includes creating new user objects, deactivating existing users, modifying user membership in security groups and updating identity attributes.

The authentication process itself is often the same regardless of the change type – all that varies is the identity of the users asked to approve or reject a change.

Since many business processes depend on authorization – user onboarding, user deactivation, access certification, privilege management, identity updates, etc. – it makes sense to implement authorization early and to subsequently link processes to an existing change approval framework.

8 Project Management Methodology

For any given milestone in an IDM project, it makes sense to have a structured sequence of steps, that takes that particular feature or integration from conception through end user adoption.

An effective methodology for delivering IDM functions follows:

1. Project startup:

- (a) Identify the business driver and required integrations.
- (b) Engage the stake-holders.

2. Business Analysis, Technical Discovery, Solution Design and Planning:

- (a) Business Analysis:
 - i. Identify core business drivers and project priorities.
 - ii. Analyze existing business processes and policies, capturing at least their inputs, purpose and outputs.
 - iii. Capture requirements for new / desired business processes.
- (b) Technical discovery:
 - i. Identify all systems, applications and security databases that contain identities that will be managed.
 - ii. Capture details for every system that will be integrated.
 - iii. Map the flow of data attributes from source systems and stake-holders to a consolidated meta directory and from there back to target systems and other human participants.
- (c) Solution Design:
 - i. Identify key metrics and record pre-implementation values.
 - ii. Design a logical and physical architecture for the new system.
 - iii. Map policies, such as login ID assignment and authorizer routing, to decision logic.
 - iv. Develop a user adoption strategy and plan.
 - v. Finalize all integration details.
 - vi. Get sign-off from all stake-holders.
- (d) Project planning
 - i. Document and get sign off on a project plan.

3. Solution Delivery:

- (a) Implement the solution design on development servers.
- (b) Unit test each function / component.

- (c) Stress test as required.
- (d) Carry out user acceptance testing.
- (e) Apply feedback from unit, stress and usability testing to the implementation. Repeat until results are acceptable.

4. Deployment:

- (a) Migrate the solution from development to production.
- (b) Carry out pilot tests with early adopter user communities.
- (c) Apply feedback from pilot tests to the implementation. Repeat until results are acceptable.
- (d) Update deployment and user adoption plans.
- (e) Roll out to remaining users.

5. Training and User Adoption:

- (a) Advertise the solution.
- (b) Develop and publish CBT materials.
- (c) Implement user awareness communication, education programs, incentives and disincentives to drive user adoption.
- (d) Carry out an impact analysis to gauge results on cost, security and user service.

6. Post Deployment:

- (a) Monitor and report on system usage and user adoption.
- (b) Report on post-deployment metrics to project sponsors.
- (c) Periodically produce an impact report illustrating the change in metrics created by the system and estimating the business impact of this change.

9 Typical Timeline and Deliverables

A typical identity management implementation may proceed as follows. This schedule is intended to illustrate what is possible, rather than to suggest that this exact sequence is appropriate to a particular organization.

Month	Phase	Deliverables
1	Business analysis, planning, prioritization	<ul style="list-style-type: none"> • Functional priority list. • Integrations priority list. • Rough project plan. • Milestones.
2–3	Deploy password management	<ul style="list-style-type: none"> • Password synchronization. • Self-service password reset. • 5 major target integrations. • E-mail integration.
4–5	User adoption	<ul style="list-style-type: none"> • Enroll users for password management. • Reconcile login IDs across major systems.
6–7	Manage AD security groups	<ul style="list-style-type: none"> • Delegate management of Windows security rights to end users.
8–9	Construct and update org-chart	<ul style="list-style-type: none"> • Org-chart data for all users. • A process to keep this data current. • Feedback to HR about errors and omissions.
10–12	Localization / language translations	<ul style="list-style-type: none"> • Password management for global user communities. • Extend self-service AD security management globally. • Extend orgchart data globally.
13	Reprioritize	<ul style="list-style-type: none"> • Refresh business priorities. • Design and plan for the next set of milestones.

Month	Phase	Deliverables
14–16	Automated access termination	<ul style="list-style-type: none"> • Implement technical access termination processes on core systems. • Automate mapping from authoritative data feeds to access termination on target systems.
17–19	Automated onboarding	<ul style="list-style-type: none"> • Implement default access setup for new users on core systems. • Automate mapping from authoritative data feeds to new user setup on target systems.
20	Reprioritize	<ul style="list-style-type: none"> • Refresh business priorities. • Design and plan for the next set of milestones.
20–22	Self-service identity update workflow	<ul style="list-style-type: none"> • Push updates to personal identity data to end users. • Advertise and educate users about this infrastructure.
23–25	Access certification	<ul style="list-style-type: none"> • Engage managers to periodically review their subordinates and identify inappropriate security rights. • Clean up orphan, dormant accounts and stale privileges.
26–28	Secure administrator credentials	<ul style="list-style-type: none"> • Randomize local administrator passwords on workstations. • Randomize local service and administrator passwords on servers. • Force IT users to sign into a credential vault to access sensitive passwords.
29	Reprioritize	<ul style="list-style-type: none"> • Refresh business priorities. • Design and plan for the next set of milestones.

Month	Phase	Deliverables
30–31	Enterprise single sign-on	<ul style="list-style-type: none">• Deploy SSO software to user workstations.• Reduce frequency with which users are presented with login prompts.
32–33	Mobile user support	<ul style="list-style-type: none">• Enable self-service password reset for mobile, disconnected users.
34–36	New target systems	<ul style="list-style-type: none">• Add 10 non-core target systems.• Add 100 implementer-style target systems.
37	Application-centric certification	<ul style="list-style-type: none">• Engage application and group owners to periodically certify user privileges within their scope of authority.

APPENDICES

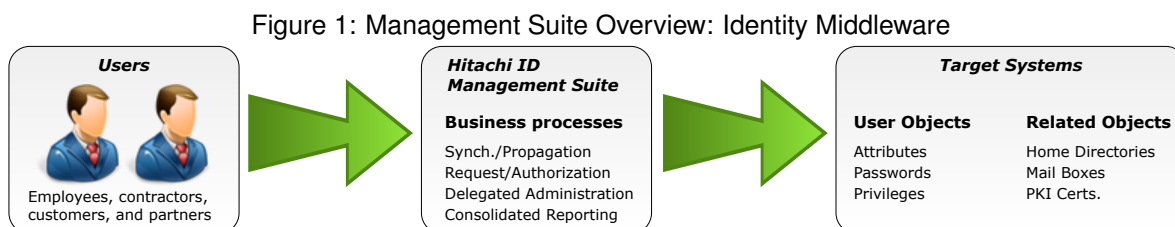
A Hitachi ID Identity Management Solutions

A.1 Management Suite Overview

The Hitachi ID Management Suite is a complete identity and access management solution that enables organizations to more securely and efficiently manage the user lifecycle across enterprise applications and systems.

The Management Suite combines the power of Hitachi ID Systems flagship technologies, Hitachi ID Identity Manager for user provisioning and Hitachi ID Password Manager for password management with more targeted products including Hitachi ID Group Manager to manage user access rights, Hitachi ID Access Certifier to review user rights and clean up stale privileges and Hitachi ID Privileged Access Manager to secure access to privileged accounts.

The Management Suite creates real business value by increasing productivity for users, reducing IT overhead, strengthening network security and providing internal controls to support compliance with privacy protection and corporate governance regulations. The Management Suite is designed as identity and access management middleware, in the sense that it presents a uniform user interface and a consolidated set of business processes to manage user objects, identity attributes, security rights and credentials across multiple systems and platforms. This is illustrated in Figure 1.



The Management Suite includes several functional identity and access management modules:

- **Identity Manager** – *User provisioning, RBAC, SoD and access certification.*
 - Automated propagation of changes to user profiles, from systems of record to target systems.
 - Workflow, to validate, authorize and log all security change requests.
 - Automated, self-service and policy-driven user and entitlement management.
 - Federated user administration, through a SOAP API (application programming interface) to a user provisioning fulfillment engine.
 - Consolidated access reporting.

Identity Manager includes the following modules, at no extra charge:

- Access Certifier – *Periodic review and cleanup of security entitlements.*
 - * Delegated audits of user entitlements, with certification by individual managers and application owners, roll-up of results to top management and cleanup of rejected security rights.
- Group Manager – *Self service management of security group membership.*
 - * Self-service and delegated management of user membership in Active Directory groups.

- Hitachi ID Org Manager – *Delegated construction and maintenance of Orgchart data.*
 - * Self-service construction and maintenance of data about lines of reporting in an organization.
 - **Password Manager** – *Self service management of passwords, PINs and encryption keys.*
 - Password synchronization.
 - Self-service and assisted password reset.
 - Enrollment and management of other authentication factors, including security questions, hardware tokens, biometric samples and PKI certificates.
- Password Manager includes the following modules, at no extra charge:
- **Hitachi ID Login Manager** – *Automated application logins.*
 - * Automatically sign users into systems and applications.
 - * Eliminate the need to build and maintain a credential repository, using a combination of password synchronization and artificial intelligence.
 - **Hitachi ID Telephone Password Manager** – *Telephone self service for passwords and tokens.*
 - * Turn-key telephony-enabled password reset, including account unlock and RSA SecurID token management.
 - * Numeric challenge/response or voice print authentication.
 - * Support for multiple languages.
- **Privileged Access Manager** – *Control and audit access to privileged accounts.*
 - Periodically randomize privileged passwords.
 - Ensure that IT staff access to privileged accounts is authenticated, authorized and logged.
- Group Manager is available both as a stand-alone product and as a component of Identity Manager.

The relationships between the Management Suite components is illustrated in [Figure 2 on Page 23](#).

A.2 Identity Manager

Overview:

Hitachi ID Identity Manager is a complete **identity management** solution that automates and simplifies the tasks of managing users and entitlements across multiple systems and applications throughout the user lifecycle. Organizations depend on **Identity Manager** to ensure that users get appropriate access rights promptly and are deprovisioned reliably and completely.

Identity Manager implements the following business processes to drive changes to users and entitlements on systems and applications:

- **Automation:** grant or revoke access based on data feeds.
- **Synchronization:** keep identity attributes consistent across applications.



Figure 2: Components of the Management Suite

- **Self-service:** empower users to update their own profiles.
- **Delegated administration:** allow business stake-holders to request changes directly.
- **Certification:** invite managers and application owners to review and correct entitlements.
- **Workflow:** invite business stake-holders to approve or reject requested changes.

Features:

Identity Manager enables automated, self-service and policy-driven management of users and entitlements with:

- **Auto-provisioning and auto-deactivation:**

Identity Manager can monitor one or more systems of record (typically HR applications) and detect changes, such as new hires and terminations. It can make matching updates to other systems when it detects changes, such as creating login accounts for new employees and deactivating access for departed staff.

- **Identity synchronization:**

Identity Manager can combine identity information from different sources – HR, corporate directory, e-mail system and more into a master profile that captures all of the key information about every user in an organization. It can then write updates back to integrated systems, to ensure that identity attributes are consistent. This feature is used to automatically propagate updates to data such as names, phone numbers and addresses from one system to another.

- **Self-service updates:**

Users can sign into the Identity Manager web portal and make updates to their own profiles. This includes changes to their contact information and requests for new access to applications, shares, folders, etc.

- **Delegated administration:**

Business stake-holders, such as managers, application owners and data owners can sign into the Identity Manager web portal and request changes to security entitlements. For example, a manager might ask for application access for an employee or schedule deactivation of a contractor's profile.

- **Access certification:**

Business stake-holders may be periodically invited to review the users and security entitlements within their scope of authority. They must then either certify that each user or entitlement remains appropriate or flag it for removal. Access certification is an effective strategy for removing security entitlements that are no longer needed.

- **Authorization workflow:**

All change requests processed by Identity Manager, regardless of whether they originated with the auto-provisioning engine, the identity synchronization engine, with self-service profile updates or with the delegated administration module may be subject to an authorization process before being completed. The built-in workflow engine is designed to get quick and reliable feedback from groups of business users, who may be individually unreliable. It supports:

- Concurrent invitations to multiple users to review a request.
- Approval by N of M authorizers (N is fewer than M).
- Automatic reminders to non-responsive authorizers.
- Escalation from non-responsive authorizers to their alternates.
- Scheduled delegation of approval responsibility from unavailable to alternate approvers.

- **Policy enforcement:**

Identity Manager can be used to enforce a variety of policies regarding the assignment of security entitlements to users, including:

- Role based access control, where security entitlements are grouped into roles, which can be assigned to users.
- Segregation of duties, which defines mutually-exclusive sets of security entitlements.
- Template accounts, which define how new users are to be provisioned.
- Rules for the composition of new IDs, such as login IDs, e-mail addresses, OU directory contexts and more.

- **Reports:**

Identity Manager includes a rich set of built-in reports, designed to answer a variety of questions, such as:

- What users have entitlement X?
- What entitlements does user Y have?
- Who authorized entitlement Z for user W?
- When did user A acquire entitlement B?
- Who requested and who authorized entitlement B for user A?
- What accounts have no known owner (orphaned)?

- What users have no accounts (empty profiles)?
- What accounts have recent login activity (dormant)?
- What users have no active accounts (dormant)?

- **Automated connectors and human implementers:**

Identity Manager can be integrated with existing systems and applications using a rich set of over 110 included connectors. This allows it to automatically provision, update and deprovision access across commonly available systems and applications.

Organizations may opt to integrate custom and vertical-market applications with Identity Manager by using the included flexible connectors. Alternately, the built-in “implementers” workflow can be used to invite human administrators to make approved changes to users and entitlements on those systems.

- **Unified management of logical access and physical assets:**

Identity Manager includes an inventory tracking system, making it suitable for managing requests for physical assets as well as logical access. For example, types and inventories of building access badges, laptops, phones and other devices can be tracked, requested, authorized and delivered using Identity Manager.

Benefits:

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 changes, 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 copied 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?”

A.3 Access Certifier

Overview:

Hitachi ID Access Certifier is a solution for distributed review and cleanup of users and entitlements. It works by asking managers, application owners and data owners to review lists of users and entitlements. These stake-holders must choose to either certify or revoke every user and entitlement.

Access Certifier is included with Hitachi ID Identity Manager at no extra cost.

Features:

Access Certifier enables organizations to review and clean up security entitlements with:

- **Certification of users:**

Access Certifier can invite managers to review a list of their direct subordinates and for each one – certify that the subordinate still works for them, transfer the subordinate to their new manager or indicate that the user in question has left the organization and their access should be terminated.

- **Certification of entitlements:**

Access Certifier can invite both managers and the owners of roles, applications and security groups to review the entitlements which have been assigned to users and either certify that they remain appropriate or ask that they be revoked.

- **Certification of exceptions to policy:**

Identity Manager supports enforcement of two types of policy – role based access control (RBAC) and segregation of duties (SoD). Access Certifier can be used to review approved exceptions to these policies and either certify that they remain appropriate or ask for the user in question to be brought back into compliance.

- **Electronic signatures:**

Access Certifier requires certifiers to sign off on their work. Signatures form a chain of accountability, acting as evidence that entitlements are still needed. The sign-off process also triggers workflow requests to revoke entitlements which certifiers indicated are no longer required.

- **Certification by entitlement owners:**

Application, group and role owners can be invited by Access Certifier to review lists of users with access to their entitlements.

- **Certification by managers:**

Access Certifier can be configured to invite every manager to review his direct subordinates and their entitlements. Managers are prevented from signing-off until managers that report to them have completed their own certification. This process creates downwards pressure on managers to complete their reviews.

- **Authorization workflow:**

Every user deactivation or access revocation request processed by Access Certifier is subject to an authorization process before being completed. The built-in workflow engine is designed to get quick and reliable feedback from groups of business users, who may be individually unreliable. It supports:

- Concurrent invitations to multiple users to review a request.
- Approval by N of M authorizers (N is fewer than M).
- Automatic reminders to non-responsive authorizers.
- Escalation from non-responsive authorizers to their alternates.
- Scheduled delegation of approval responsibility from unavailable to alternate approvers.

- **Reports:**

Access Certifier includes a rich set of built-in reports, designed to answer a variety of questions, such as:

- Who certified user X getting entitlement Y and when?
- What users have entitlement Z?
- What entitlements does user W have?
- Which certifiers are prompt and which procrastinate?
- What accounts have no known owner (orphaned)?
- What users have no accounts (empty profiles)?
- What accounts have recent login activity (dormant)?
- What users have no active accounts (dormant)?

- **Automated connectors and human implementers:**

Access Certifier can be integrated with existing systems and applications using a rich set of over 110 included connectors. This allows it to automatically detect and deprovision entitlements across commonly available systems and applications.

Organizations may opt to integrate custom and vertical-market applications with Identity Manager by using the included flexible connectors. Alternately, the built-in “implementers” workflow can be used to invite human administrators to make approved changes to users and entitlements on those systems.

Benefits:

Access Certifier strengthens security by helping organizations to find and remove inappropriate security entitlements. It makes business stake-holders take direct responsibility for ensuring that users within their scope of authority have appropriate security rights for their jobs.

A.4 Password Manager

Overview:

Hitachi ID Password Manager is an enterprise solution for managing passwords and other types of credentials. 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.

Features:

Password Manager streamlines the management of passwords and other login credentials:

- **Transparent password synchronization:**

When users change their password natively on a system where a password synchronization trigger has been installed, the new password is subjected to an extra password policy and, if accepted, is changed both locally and on other systems where the user has accounts.

Password Manager includes password synchronization triggers for Windows server or Active Directory (32-bit, 64-bit), Sun LDAP, IBM LDAP, Oracle Internet Directory, Unix (various), z/OS and iSeries (AS/400).

Using a familiar and mandatory password change process guarantees 100% user adoption.

- **Web-based password synchronization:**

Users can change some or all of their passwords using a Password Manager web interface. The password policy is clearly explained on-screen and enforced interactively.

Using an interactive web page to change passwords has educational benefits but requires user awareness and cooperation.

- **Self-service password reset:**

Users who have forgotten a password or triggered an intruder lockout can sign into Password Manager using other types of credentials and resolve their own problem. Non-password authentication options include security questions, voice biometrics, smart cards, hardware tokens and random PINs sent to a user's mobile phone using SMS.

Access to self-service is available from a PC web browser, from the Windows login screen, using a telephone or using the mini web browser on a smart phone.

- **Many built-in connectors:**

Password Manager ships with built-in integrations for over 110 systems and applications. That means that it can manage passwords, PINs, smart cards and other login credentials on most servers, directories, network devices, databases and applications without customization.

- **Token and smart card PIN reset:**

Users with a token who have forgotten their PIN or need an emergency pass code can access self-service PIN reset with a web portal or using a telephone. Users with a smart card can also reset their own PIN using an ActiveX control embedded in a web browser – launched from their Windows desktop or login screen.

- **Self-service unlock of a computer with full disk encryption:**

Users with full disk encryption software on their PC, who have forgotten the password that unlocks their computer, can unlock their hard disk using a self-service process accessed via telephone.

- **Enterprise single sign-on:**

Hitachi ID Login Manager client software can be installed on Windows PCs to capture login IDs and passwords from the Windows login screen and automatically insert these same credentials into application login prompts. This eliminates the need for users to repeatedly type their login ID and password into applications whose credentials are consolidated or synchronized with Windows / Active Directory.

- **Assisted password reset:**

Authorized IT support staff can sign into a Password Manager web user interface to look up a caller's profile, authenticate the caller by keying in answers to security questions and reset one or more passwords. A ticket is then automatically submitted to the help desk incident management system.

- **Password policy enforcement:**

Password Manager normally enforces a global password policy to supplement the various policies enforced on each system and application. This policy ensures that passwords accepted by Password Manager will work on every system.

The built-in policy engine includes over 50 built-in rules regarding length, mixed-case, digits, dictionary words and more. Regular expressions and plug-ins enable organizations to define new rules. Password history is infinite by default.

- **Password change notification / early warning:**

Password Manager can invite users to change their passwords with a web portal before they expire. These invitations can be sent via e-mail or launched in a web browser when users sign into their PCs. Users can even be forced to change passwords by launching a kiosk-mode web browser at login time.

Benefits:

Password Manager improves the security of passwords through enforcement of a robust, global policy that requires passwords to be complex, to be changed periodically and to never be reused. It improves the security of IT support processes by requiring strong authentication of both the support analyst and caller prior to any security-related help desk call and by reducing the number of IT support staff who need elevated privileges to assist users who need help with an intruder lockout, forgotten password or PIN or locked-out hard disk.

Password Manager improves user service by reducing the number of passwords users must remember, by automatically populating IDs and passwords into application login prompts and by providing a single, friendly user interface where users regularly change their passwords.

Password Manager lowers the cost of IT support by reducing the frequency of password-related problems experienced by users and by enabling users to resolve a variety of authentication-related problems on their own.

A.5 Group Manager

Overview:

Hitachi ID Group Manager is a self-service **group management** solution. It allows users to request access to resources such as shares and folders, rather than requesting access to groups. Group Manager automatically maps requests to the appropriate security groups and invites group owners to approve or reject the proposed change.

Group Manager is available both as a stand-alone solution and as a no-cost module included with Hitachi ID Identity Manager.

Features:

Group Manager streamlines the process of managing security groups on Active Directory with:

- **A Windows shell extension:**

A shell extension is included with Group Manager which can be deployed on Windows XP, Windows Vista and Windows 7 PCs. If installed, this component can intercept Windows “access denied” error messages and present an expanded message which allows users to open a web browser to the Group Manager application, where they can request membership in the appropriate AD group.

- **Share and folder browsing in a web portal:**

Alternately, users can navigate directly to the Group Manager web portal, which presents a view of shares and folders similar to Windows Explorer. Users can select the share, folder or printer in which they are interested and request membership in the appropriate group.

- **A UI that guides users to appropriate groups:**

When users select a network resource, Group Manager presents several options:

- Groups that have access rights to that resource, with a clear indication as to who owns each group and what access rights the group has.
- Nested groups, that the user might wish to join instead.
- Nested resources (folders) that the user may wish to access instead.

With these options, Group Manager guides users to a selection of the appropriate resource and group.

- **Authorization workflow:**

All change requests processed by Group Manager are subject to an authorization process before being completed. By default, group owners are invited to approve all changes, but this routing can be replaced or augmented as required.

The built-in workflow engine is designed to get quick and reliable feedback from groups of business users, who may be individually unreliable. It supports:

- Concurrent invitations to multiple users to review a request.
- Approval by N of M authorizers (N is fewer than M).
- Automatic reminders to non-responsive authorizers.
- Escalation from non-responsive authorizers to their alternates.
- Scheduled delegation of approval responsibility from unavailable to alternate approvers.

- **Reports:**

Group Manager includes a rich set of built-in reports, designed to answer a variety of questions, such as:

- What users are members of group X?
- What group memberships does user Y have?
- Who authorized membership in group Z for user W?
- When did user A gain membership in group B?
- Who requested and who authorized group B for user A?

Benefits:

Group Manager improves security by ensuring that changes to membership in security groups are properly authorized before being implemented.

Group Manager reduces the cost of IT support by moving requests and authorization for changes to group membership out of IT, to the community of business users.

Group Manager streamlines service delivery regarding the management of membership in security groups by making it easier for users to submit clear and appropriate change requests and automatically routing those requests to the right authorizers. This makes the request process painless and the approvals process fast.

A.6 Privileged Access Manager

Overview:

Hitachi ID Privileged Access Manager is a system for securing access to privileged accounts. It works by regularly randomizing privileged passwords on workstations, servers, network devices and applications. Random passwords are encrypted and stored on at least two replicated vaults. Access to privileged accounts may be disclosed:

- To IT staff, after they have authenticated and their requests have been authorized.
- To applications, replacing embedded passwords.
- To Windows workstations and servers, which need them to start services.

Password changes and access disclosure are closely controlled and audited, to satisfy policy and regulatory requirements.

Features:

Privileged Access Manager secures privileged accounts with:

- **Random passwords:**

Privileged Access Manager is designed to change as many as 2,000,000 passwords per day to new, random values. This minimizes the window of opportunity that hackers and former users have to compromise systems and applications.

- **Encrypted, replicated vault:**

Privileged Access Manager stores randomized passwords in an encrypted and replicated vault. This protects against unauthorized access to passwords and against loss of access to data because of a hardware failure or physical disaster.

- **Many built-in connectors:**

Privileged Access Manager ships with built-in integrations for over 110 systems and applications. That means that it can secure access to sensitive accounts on most servers, directories, network devices, databases and applications without customization.

- **Laptop support with a local service:**

Privileged Access Manager also ships with software that can be installed on laptops running Windows or Linux. This allows it to secure access to computers that are sometimes turned off, unplugged from the network, change IP addresses or physically removed from the premises.

- **Access control policy engine:**

Security officers set policy on Privileged Access Manager to control who can access which accounts. For example, Windows administrators can be granted access to local Administrator accounts, Unix administrators can be allowed to login as root, etc. The policy engine is very flexible, as it connects groups of administrators to named accounts on groups of systems.

- **Workflow for one-time access requests:**

Privileged Access Manager includes a powerful workflow engine that allows users to request one-time access to privileged accounts. Requests are subject to policy (who can ask, who must approve).

The workflow engine leverages e-mail to invite authorizers to act and a secure web form for approvals. Prompt response is assured by inviting multiple authorizers, sending automated reminders, escalating requests from non-responsive authorizers to alternates and more.

- **Flexible access disclosure options:**

Rather than displaying passwords to users, Privileged Access Manager can:

- Launch RDP, SSH, SQL Studio, VMWare vSphere and similar sessions, injecting passwords without displaying them.
- Temporarily attach the authorized user's Active Directory account to a local security group on the target Windows server.
- Temporarily attach the authorized user's SSH public key to the authorized_users key ring on the target Unix or Linux server.

- **Session recording:**

Privileged Access Manager can be configured to record screen, keyboard and other data while users are connected to privileged accounts. The recording may be of just the window launched to connect a user to a privileged account or of the user's entire desktop.

The session recording system is tamper resistant – if users attempt to interrupt recording, their login sessions to privileged accounts are disconnected and an alarm is raised.

Session recordings may be archived indefinitely and may serve a variety of purposes, ranging from knowledge sharing and training to forensic audits. Access to recorded sessions is secured through a combination of access control policies and workflow approvals, designed to safeguard user privacy.

The Privileged Access Manager session monitoring infrastructure is included at no extra cost. It works using ActiveX components and does not require software to be permanently installed on user PCs. There is no footprint on managed systems and no proxy servers are used.

Session monitoring is compatible with all administration programs and protocols, as it instruments the administrator's PC, rather than network traffic.

- **Infrastructure to secure Windows service account passwords:**

In addition to managing access to administrator accounts, Privileged Access Manager can randomize passwords used to run services, scheduled jobs and other unattended processes on Windows computers. It can then notify the Windows Service Control Manager, Scheduler, IIS and other components of the new password, so that tasks can be successfully started in the future.

- **An API to replace static, embedded passwords:**

Privileged Access Manager exposes an API that allows one application to securely acquire a password that will then be used to connect to another application. This mechanism is used to eliminate plaintext passwords in application source code or text files.

- **Auto-discovery:**

Privileged Access Manager includes an advanced infrastructure auto-discovery system, designed to minimize both initial and ongoing configuration. This system can:

1. Extract a list of systems from AD, LDAP or other sources.
2. Apply rules to decide whether a given system should be managed.
3. Apply rules to choose a security policy to apply to each managed system.
4. Probe systems in a massively parallel fashion, to get a list of accounts, groups and services on each one.
5. Apply rules to decide which accounts on each system should be managed.

- **Reports:**

Privileged Access Manager includes a variety of built-in reports, that are used to answer questions such as:

- What computers are on the network?
- Which computers have been unresponsive during the past 30 days?
- Which administrators have signed into this computer?
- Which systems has this administrator managed?
- Who has made a large number of requests for one-off access?

Benefits:

Privileged Access Manager improves the security of privileged accounts by:

- Eliminating static, shared, well-known passwords.
- Ensuring that former IT staff cannot access sensitive infrastructure.
- Requiring strong, personal authentication of users prior to accessing privileged accounts.
- Enforcing robust policy over who can access privileged accounts.
- Recording a detailed audit trail of privileged login sessions.

Privileged Access Manager reduces the cost of managing passwords on privileged accounts by automating the password change, storage and disclosure process.