

Addressing Excess Privileges

using Hitachi ID Access Certifier



1 Introduction

This document describes the business problem of privilege accumulation and the impact of this IT problem on organizations in the context of a growing set of regulatory requirements.

Having defined the business problem, this document then describes the process of access certification, used to respond to privilege accumulation in a manner consistent with regulations such as Sarbanes-Oxley, HIPAA, 21CFR11 and GLB.

2 The Challenge

2.1 The Regulatory Environment

Two common threads running through many regulations are privacy protection (e.g., HIPAA, GLB, PIPEDA, EU Privacy Directive) and corporate governance (e.g., Sarbanes-Oxley, 21-CFR-11). Privacy applies to customers, patients, investors, employees and so forth. Good governance applies to financial data, clinical processes, safety procedures, etc.

2.2 Compliance Requires AAA

Privacy protection and corporate governance both depend on effective internal controls. The challenge is to answer the questions:

Who can access sensitive data?	How are these users authenticated?	What can they see and modify?	Are users held accountable for their actions?
--------------------------------	------------------------------------	-------------------------------	---

These requirements can be restated as AAA: authentication, authorization and audit.

2.3 Problems with AAA

AAA infrastructure is nothing new and has been built into every multi-user application for decades. The problem is that a growing number of systems and applications, combined with high staff mobility, have made it much harder to the manage passwords and entitlements on which AAA rests.

With weak passwords, unreliable caller identification at the help desk, orphan accounts, inappropriate security entitlements and mismatched login IDs, AAA systems often wind up enforcing the wrong rules. The weakness is not in the authentication or authorization technology – it's in the business process for managing security entitlements and credentials.

2.4 Addressing Problems with AAA Requires Identity Management

To address problems with AAA data, it is essential to implement robust processes to manage security, so that only the right users get access to the right data, at the right time.

This is accomplished with:

- Better control over how users acquire new entitlements and when entitlements are revoked.
- Correlating user IDs between systems and applications, so that audit logs can be related to real people.
- Periodic audits of entitlements, to verify that they remain business-appropriate.
- Logging of both current and historical entitlements, to support forensic audits.

- Stronger passwords and more robust authentication in general.

3 Access Certification

Hitachi ID 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:**

Hitachi ID 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 100 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.

3.1 Benefits of Access Certification

Access certification offers substantial benefits over previous approaches:

Hitachi ID 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.

3.2 Previous Approaches

Previous attempts to address the problem of finding and removing excess access rights have focused on policy-enforcement in general, and policy-based provisioning in particular:

Policy-based provisioning is defined as follows:

- Define a set of roles, detailed enough to capture the full access requirements of every user, on every target system.
- Classify users into roles, such that their access requirements are fully specified by role membership.
- Reconcile access privileges predicted by the policy model against the access privileges users actually have on target systems.
- Correct actual privileges to match those predicted by roles, either automatically or after human review and approval.

On an enterprise scale, where there are (tens of) thousands of users, employees, contractors and other principals are constantly hired, moved and terminated. This makes user classification difficult.

Role definition, where user responsibilities are subtly different, and where infrastructure is ever changing, is similarly difficult, because the target (a role model) is complex and moving.

Access privilege reconciliation may also be hard to implement, as it can flag more exceptions than human authorizers can realistically review.

The policy-based provisioning approach is challenging in complex organizations, because defining a comprehensive and appropriate policy is time consuming, difficult and expensive. These challenges apply equally to initial deployment and ongoing system sustainment.

4 Motivating Managers to Participate

In a large organization, there will be many managers, application owners and data owners who must perform periodic audits of user access privileges. It follows that some mechanism is required to ensure that these audits are in fact carried out and performed diligently.

Audits by application and data owners are straightforward – this can be made a core part of the responsibility of these stakeholders, and since there are relatively few such stakeholders, ensuring that they complete periodic user privilege audits.

Audits of users by their direct supervisors can be more difficult, since there may be thousands of such supervisors and it is hard to make them all comply with any single directive.

One approach to motivating managers to review the access rights of their direct subordinates is to require a signature at the end of every such review, but to block such signatures until subordinate managers have completed their own reviews. This signature underlies a legal statement by each manager, certifying that the remaining list of that manager's direct subordinates and their privileges, are appropriate.

With this process, an executive such as the CEO or CFO, who wishes to implement strong controls to support a regulatory compliance program, will pressure his direct subordinates to complete their own reviews. They will be unable to sign off until their own subordinates have finished and so a downward pressure through the organization to complete the audit is created. Whereas pressure to perform the user privilege reviews flows downwards from the top of the organization, results of the audit, including cleaned up user rights, flow back up from the lowest-level managers right to the CEO or CFO.

5 Advantages of the Access Certification Approach

The Hitachi ID Access Certifier process has several advantages that organizations can leverage:

- **Simple to deploy** – This is a practical approach to addressing an important business problem: finding and eliminating obsolete user privileges. Organizations can deploy Access Certifier in just a few weeks, without getting bogged down in role definition or user classification projects, which tend to be lengthy and expensive.
- **Accurate and up-to-date** – The information about who should have what access to what systems is drawn from managers with contextual knowledge, not IT staff far removed from day to day application usage.
- **Auditable** – The process is 100% traceable, providing complete confidence to senior executives about the validity of the cleaned privileges and of the process itself.

Please contact Hitachi ID to learn more about the Hitachi ID Access Certification Process and Hitachi ID's complete line of Identity Management Solutions.

6 About Hitachi ID Systems, Inc.

Hitachi ID Systems, Inc. is a leading publisher of identity and access management software. Hitachi ID Systems products help organizations strengthen network security, lower IT support costs and improve user productivity. Hitachi ID Systems customers achieve these results by implementing automation and self-service processes to more effectively manage passwords and other types of credentials, to provision and deactivate user access and to manage user privileges. Hitachi ID Systems products have been deployed at over 900 organizations world-wide.

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

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

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

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

Hitachi ID's customers include AT&T Wireless, Best Buy, Bristol-Myers Squibb, Ford Motor Company, Kimberly-Clark Corporation, NCR Corporation, Pitney Bowes, Schering-Plough Pharmaceuticals, Sears Roebuck, Siemens, Symantec, United Technologies Corporation, Wendy's International and many more. For more information on Hitachi ID and its products, please visit <http://Hitachi-ID.com/> or call 1.403.233.0740.