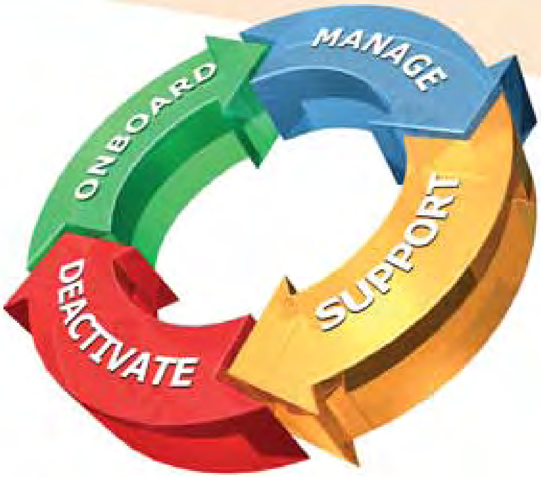
Hitachi ID Identity Manager

hitachi-id.com



Managing identities and entitlements.

Hitachi ID Identity Manager streamlines and secures the management of users and entitlements. It strengthens internal controls with automated access deactivation, Role Based Access Control (RBAC), Segregation of Duties (SoD) policy enforcement and access certification. It reduces IT cost and improves user service with automated, delegated and self-service user management.

Challenges

Internal Controls

Application access controls are only as good as the processes used to assign security entitlements to users. Orphan accounts, dormant accounts and stale privileges are evidence of process problems.

Audit / Compliance

It can be difficult to answer simple questions like, "who has access to this application" or "who approved this entitlement and when?"

IT Cost and Delay

Managing user access to hundreds of applications is expensive. Change management is a costly bottleneck at odds with frequent reorganizations, an increasingly open perimeter and ever growing application inventory.

Lost Productivity

Employees and contractors waste valuable time waiting for needed access.

Return on Investment

Hitachi ID Identity Manager automates the full lifecycle of users and entitlements, from onboarding to deactivation. It has a lower total cost of ownership (TCO) than competing products because connectors, forms, workflows, auto-discovery and reports are all built in.

Hitachi ID Systems, Inc.

Automation

Eliminate manual user setup and deactivation

Identity Manager can detect changes in a system of record (such as HR) and update access rights by creating accounts for new users and deactivating access for departed users.

Request Portal

Empower users to manage identities and entitlements

A simple web portal enables users to update their contact information and request access to applications or network resources.

Managers and application/data owners can request changes to security entitlements. Requests may be to add/remove application access, change roles, assign/revoke groups or schedule deactivation.

Access Certification

Review and clean up security entitlements

Periodically invite business stake-holders to review the users and security entitlements within their scope of authority. Each is either certified or flagged for removal after further approval.

Authorization Workflow

Ensure that change requests are approved before they are completed

All change requests processed by Identity Manager may be subject to approval by one or more stake-holders before being completed.

Identity Synchronization

Consistent user information across all systems

Identity Manager can copy changes to user information from one system to another, on a priority basis, automatically.

Reports

Visibility and accountability

Identity Manager includes a rich set of built-in reports for analyzing entitlements and change history by user, application, role or policy.

HITACHI
Inspire the Next

Read this brochure online:

Security Policy Enforcement

Enforce a policy of least privilege

Identity Manager ensures that users have appropriate security entitlements.

- Role based access control (RBAC).
- Segregation of duties (SoD) policies, both detective and preventive.
- Standard user configuration using template accounts.
- Controls over who can make requests on behalf of any given user.
- Periodic access certification and cleanup of stale entitlements.

Automated Connectors and Human Implementers

Invest in automation where it makes sense

Identity Manager includes over 100 connectors that can automatically provision, update and deactivate access on common systems and applications.

Integrations with vertical market or custom applications can be made via flexible agents or a built-in workflow that invites system administrators to complete requests manually.

Logical Access and Physical Assets

One-stop shopping for all change requests

Built-in inventory tracking and implementer workflows allow Identity Manager to provision physical assets such as building access badges, laptops and phones.

Windows and Sharepoint Integration

Intercept "Access Denied" errors

When users try to open shares, folders or SharePoint libraries where they do not have access, Identity Manager provides an easy link to a web page where they can request appropriate security entitlements.

Included Connectors

Directory

Windows/Active Directory, LDAP, eDirectory, NDS

File/Print

Windows, NetWare, Samba, NAS appliances

Database

Oracle, Sybase, SQL Server, DB2/UDB

Unix

Linux, Solaris, AIX, HP-UX with passwd, shadow, TCB, Kerberos, NIS or NIS+

Mainframes/Mini

z/OS with RACF, TopSecret or ACF/2; iSeries; Scripts for VM/ESA, Unisys, Siemens, OpenVMS, Tandem

Application

Oracle eBiz, PeopleSoft, SAP R/3, JDE and more

Groupware

Exchange 2000-2010, Notes NAB and ID files, GroupWise

Networking

Network devices and VPNs via AD, LDAP, SSH

Cloud/SaaS

WebEx Connect, Google Apps, Salesforce.com, UltiPro HR, Office 365, Cybershift

Incident Management Integrations

Automatically create, update and close tickets on:

- Axios Assyst
- BMC SDE
- Clarify eFrontOffice
- HP Service Manager
- Symantec/Altiris
- ServiceNow
- BMC/Remedy ARS
- CA Unicenter
- FrontRange HEAT
- Numara Track-IT!
- Tivoli Service Desk

Additional integrations via e-mail, ODBC, web services and web forms are available.

Hitachi ID Identity Manager is part of the Hitachi ID Management Suite, which also includes: Password Manager for self-service management of authentication factors and Privileged Access Manager to secure administrator and service accounts.

For more information, please visit: http://hitachi-id.com/
or call: 1.403.233.0740 | 1.877.386.0372

HITACHI
Inspire the Next