



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

User Administration 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 network 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 everything is built-in: connectors, forms, workflows, auto-discovery, reports and more.

- ✓ **AUTO-PROVISIONING AND AUTO-DEACTIVATION**
Eliminate manual user setup and teardown
Identity Manager can monitor systems of record, detect changes and make matching updates to other systems, such as creating accounts for new employees or deactivating access for departed contractors.
- ✓ **IDENTITY SYNCHRONIZATION**
Consistent information about users on every system
Identity Manager can combine identity information such as names, phone numbers, department codes and e-mail addresses from multiple sources. It detects changes and either copies them to other systems or removes them, depending on priority.
- ✓ **SELF-SERVICE UPDATES**
Empower users to manage their own profiles
A web UI enables users to update their contact information, request access to applications and more.
- ✓ **DELEGATED ADMINISTRATION**
Move the responsibility for change management to the business
Managers and application/data owners can request changes to security entitlements. Requests may be to add/remove application access, change roles, change groups or schedule deactivation.
- ✓ **ACCESS CERTIFICATION**
Review and clean up security entitlements
Business stake-holders are periodically invited to review the users and security entitlements within their scope of authority. Each is either certified or flagged for removal, subject to further approvals.
- ✓ **AUTHORIZATION WORKFLOW**
Ensure all change requests are approved before they are fulfilled
All change requests processed by Identity Manager may be subject to approval by one or more stake-holders before being completed.

✓ SECURITY POLICY ENFORCEMENT

Appropriate security entitlements

Identity Manager ensures that users have just the security entitlements they need using:

- Role based access control (RBAC) enforcement.
 - 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.

REPORTS

Visibility and accountability

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

✓

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 most systems and applications.

Integrations with vertical market or custom applications can be via included flexible agents or a built-in workflow that invites “implementers” to fulfill approved requests.

✓

LOGICAL ACCESS AND PHYSICAL ASSETS

One stop shopping for all change requests

Built-in inventory tracking and implementer workflows extend the reach of Identity Manager to physical assets -- building access badges, laptops, phones, etc.

INCLUDED CONNECTORS

Directory:

Windows/Active Directory, LDAP, eDirectory, NDS

File/Print:

Windows, NetWare, Samba, NAS appliances

Databases:

Oracle, Sybase, SQL Server, DB2/UDB

Unix:

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

Mainframes/minis:

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

Applications:

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

Groupware:

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

Networking:

Network devices and VPNs via AD, LDAP, SSH.

Flexible Agents:

API, SSH, Web service, Browser emulation, Telnet, TN3270, TN5250, HTTP(S), SQL injection, LDAP attributes and command-line

Cloud / SaaS:

WebEx Connect, Google Apps, SOAP agent

INCIDENT MANAGEMENT INTEGRATIONS

Automatically create, update and close tickets on:

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

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

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 Password Manager to secure administrator and service accounts.

For more information, please visit

<http://hitachi-id.com/>

or call

1.403.233.0740