Hitachi ID Identity Manager

hitachi-id.com

Challenges

Internal Controls

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

Audit / Compliance

It is often difficult to trace entitlements back to requesters or authorizers. Weak controls mean that entitlements may violate SoD, privacy protection or other polices.

IT Cost and Delays

Managing and auditing user access is time consuming and costly. Cumbersome processes and large teams are at odds with a mandate for efficiency and agility.

Lost Productivity

Users lose valuable time waiting for access, because request forms are hard to find and complete, approvals are slow and too many people are involved in fulfillment.

Return on Investment

Hitachi ID Identity Manager automates the user lifecycle and entitlements, automating predictable access and streamlining request/approval processes. It offers the lowest TCO among IAM products by including pre-configured processes, forms, integrations and analytics out of the box.

Managing Identities and Entitlements

Hitachi ID Identity Manager is an integrated solution for managing identities and security entitlements across multiple systems and applications. Organizations depend on automated Identity Management solutions to ensure timely and secure processing of user entitlements that comply with their policies.

Automation

Identity Manager monitors both systems of record, such as HR, and integrated directories, such as Windows Active Directory. It responds to changes by propagating them to other systems or raising requests to approve or undo them.

Request Portal

Identity Manager includes a web portal where users request access rights for or update profile information about themselves or others. Identity Manager is a robust access control solution that controls and protects user privacy.

Innovative features such as intercepting “Access Denied” error dialogs on Windows and Sharepoint, searching for relevant entitlements and comparing entitlements with recipient users simplify the request process.

Access Governance

Identity Manager enforces access policies, including segregation of duties, role-based access control, risk scores and controls data visibility. It blocks violations and finds pre-existing or out-of-band problems. An access certification process is used to invite business stake-holders to review reporting relationships and access rights.

Robust Workflow

Users may be invited to participate in access change processes as authorizers, reviewers or implementers. A robust workflow engine invites multiple users concurrently, sends reminders, escalates unresponsive participants, schedules time off and more.

Analytics and Dashboards

With over 150 built-in reports, dashboards and analytics, Identity Manager identifies many kinds of entitlement and identity problems: SoD violations, out-of-role entitlements, empty or orphan groups, orphan and dormant accounts and more. Actionable analytics link problem identification to requests for remediation.

Automated Connectors and Human Intervention

Identity Manager includes over 100 connectors that can automatically grant, update and revoke access to systems and applications, on-premise and in the cloud. Flexible connectors simplify integration with custom or specialized applications. Implementer workflows invite people to complete approved access requests, making it cost effective to manage both automatically- and manually-provisioned access with a single request, approval and audit system.

Hitachi ID Systems, Inc.

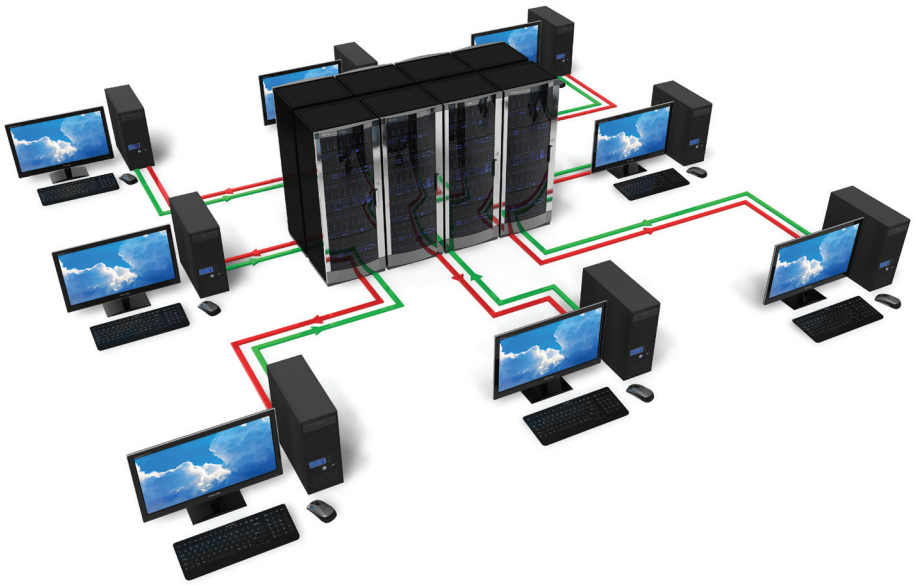
HITACHI
Inspire the Next

BYOD Friendly

Identity Manager is accessible on smart phones and tablets, even if there is no public URL to its portal. A mobile proxy deployed to the cloud or corporate DMZ plus an app for Android and iOS enables convenient approvals, contact lookups 24x7 and provides a second authentication factor to all users.

Cloud Friendly

Identity Manager can be deployed on-premise or in the cloud. It can manage systems and applications on-premise, in the cloud and on isolated network segments.



Included Connectors

Directories

Any LDAP, AD, eDirectory, NIS/NIS+

Servers

Windows 2000-2012, Samba, Sharepoint

Databases

Oracle, Sybase, SQL Server, DB2/UDB, ODBC, Informix, Progress

Unix

Linux, Solaris, AIX, HPUX, many more

Mainframes

z/OS with RAC/F, ACF/2 or TopSecret

Midrange

iSeries (OS400), OpenVMS

ERP

JDE, Oracle eBiz, PeopleSoft, SAP, Siebel, Business Objects

Collaboration

Lotus Notes, Exchange

Tokens, Smart Cards

RSA SecurID, SafeWord, Duo Security, RADIUS, ActiveIdentity, Schlumberger

WebSSO

CA SiteMinder, IBM TAM, Oracle AM, RSA Access Manager

Ticket Systems

ServiceNow, Remedy, BMC SDE, HP SM, CA, Assyst, HEAT, Altiris, Clarify, Track-It!, RSA Envision, MS SCS Manager

HDD Encryption

McAfee, CheckPoint, BitLocker, Symantec, Sophos

Cloud

Salesforce.com, WebEx, Google Apps, Office 365, Concur, AWS, vCloud

Miscellaneous

OLAP, Hyperion, iLearn, Cache, Success Factors, vSphere

Extensible

SPML, SCIM, SAML, SSH, Telnet, TN3270, HTTP(S), SQL, LDAP, ODBC, CSV, Python/web services

Hitachi ID Identity Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Password Manager for strong authentication, federation and credential management and Privileged Access Manager to secure elevated privileges and passwords to administrator, service and embedded passwords.

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

HITACHI
Inspire the Next