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, risk or other policies.

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 and streamlines the administration of accounts and entitlements. It offers the lowest TCO among IAM products by including pre-configured processes, forms, integrations and analytics.

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 automation to ensure timely and secure granting and revocation of entitlements to comply with policies and regulations.

Automation

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

Request Portal

A web portal allows users to request access rights for or update profile information about themselves or others. Robust access control policy protects user privacy.

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

Access Governance

Identity Manager enforces access policies, including segregation of duties, role-based access control and risk scores. It blocks violations at request time and finds pre-existing problems. An access certification process is used to invite business stake-holders to review and correct data.

Robust Workflow

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

Analytics and Dashboards

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

Automated Connectors and Manual Fulfillment

Identity Manager includes over 100 connectors that can automatically grant, update and revoke access to systems and applications, on-premises 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.

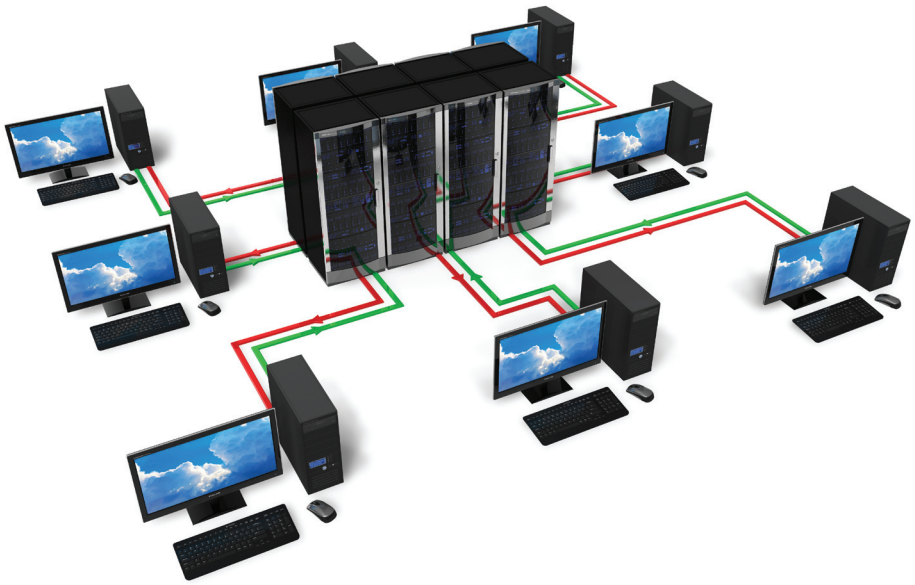
HITACHI
Inspire the Next

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, lookup of co-worker contact details and provides a second authentication factor to all users.

Cloud Friendly

Identity Manager can be deployed on-premises or in the cloud. It can manage systems and applications on-premises, 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, SQL, MySQL

Unix

Linux, Solaris, AIX, HPUX and 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, Office 365

Tokens, Smart Cards

RSA SecurID, SafeWord, Duo Security, RADIUS, ActivIdentity, 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!

HDD encryption

McAfee, CheckPoint, BitLocker, Symantec, Sophos

Cloud

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

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