Access Security and E-Mail Lists

Hitachi ID Group Manager replaces manual processes for managing groups in directories such as AD and LDAP with a combination of automation and self-service. This makes the administration of security groups and mail distribution lists faster, cheaper and more secure.

Manage Groups and Membership

Group Manager can create or manage group objects and assign or revoke membership. It supports nested groups (containing child groups). Groups can have metadata, such as owners and descriptions. Membership can be either calculated, or requested, in which case it should also be approved and later reviewed and possibly revoked.

Challenges

Access Security

Groups underpin security in most systems and applications. If users are assigned to inappropriate groups, they gain inappropriate access to applications or data. It is essential to assign groups based on business need and in compliance with policy.

Lost Productivity

When users shift responsibilities, for example by being assigned to new projects, they need new access rights. Delays in the access request, approval and fulfillment process block their ability to work.

Audit Findings

Internal controls problems arise when there are more groups than users and where the existence of groups and the assignment of membership are not supported by change history or business context.

Automation and Self-Service

Group Manager can create or delete groups in response to changes in authoritative data. For example, a group for each department, location or manager. It can calculate group membership based on identity attributes, such as cost centers or country codes.

For less predictable groups, Group Manager offers a request portal, combined with approval workflows. Since users never ask to revoke group memberships, Group Manager also includes a periodic review process, where stakeholders such as managers or group owners either certify members or flag them for revocation.

User Friendly Requests

Most users don’t understand access control models, so are challenged by typical request portals. Group Manager helps users formulate unambiguous requests with a number of features:

- **Roles**, which encapsulate multiple groups and model understandable business functions.
- **Comparison**, where a requester can select items that a model user has but the recipient does not.
- **Intercepting “Access Denied” error dialogs**, navigating users to an appropriate request page.
- **Suggestions**, offering requesters items that are popular among the peers of a recipient.

Policy Controls

Group manager enforces a variety of policies to ensure that groups and their membership are business-appropriate. This includes rules for selecting authorizers, segregation of duties, risk scoring, temporary assignment, naming and container (OU) selection.

A real time connector to Active Directory enables Group Manager to respond to changes as they happen, with the option to reverse them and raise alerts immediately.

Actionable Analytics

A rich set of reports can find groups with overlapping membership, clusters which might serve as roles, nesting cycles, too-small, too-large groups and more. A feedback path from reports to requests can automate problem remediation.
Administration Cost

The second most requested service in most IT support help desks, after password resets, is access requests. These requests are often time consuming because users know what they want to access but not what security groups control that access or who must approve changes.

Deciphering user requests and identifying the appropriate authorizers is time consuming, leading to high cost per incident.

In addition, poor controls over groups lead auditors to spend a lot of time with access administrators, increasing their workload.

Included Connectors

Directories
Active Directory and Azure AD; any LDAP; NIS/NIS+

Server OS: X86/IA64
Windows: NT thru 2016

Messaging and collaboration
Microsoft Exchange, Lync and Office 365

Tokens, smart cards and 2FA apps
Any RADIUS service or SAML, IdP: Duo Security; RSA SecurID; SafeWord; Vasco; Activedirectory and Schlumberger.

Help desk incident management (ITSM):
ServiceNow; BMC Remedy, RemedyForce and Footprints; JIRA; HPE Service Manager; CA Service Desk; Axios Assyst; Ivanti HEAT; Symantec Altiris; Track-IT; MS SCS Manager and Cherwell.

HR / HCM
WorkDay; PeopleSoft HR; SAP HCM and SuccessFactors.

Extensible / scriptable:
CSV files; Google Sheets; SCIM; SSH; Telnet/TN3270/TN5250; HTTP(S); SQL; LDAP; PowerShell and Python.

Filesystems and content platforms
Windows/CIFS/DFS; SharePoint

Security Incident / Event Management:
Splunk; ArcSight; RSA Envision and QRadar. Any SIEM supporting SYSLOG or Windows events.

Hitachi ID Group Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Password Manager for self-service credential management plus federated single sign-on and Privileged Access Manager to secure administrator and service accounts. Group Manager is available as a stand-alone product and is also included in Identity Manager, which provides identity and access management. For more information, please visit: https://hitachi-id.com/ or call: 1.403.233.0740 | 1.877.386.0372

Requesting a group after selecting a shared folder.

Group Management portal.