



## Managing Active Directory security.

Hitachi ID Group Manager moves the responsibility for managing Active Directory groups from IT to users. It lowers IT costs and improves user service by intercepting user attempts to access network resources and redirecting users without appropriate access rights to a web portal where they request appropriate group memberships.

### Active Directory Group Management Challenges

#### Lost Productivity

In medium to large organizations, managing user access to network resources such as shares and folders can be a slow business process. The result is lost productivity whenever users change roles or projects.

#### IT Support Cost

The help desk is inundated with calls requesting access. Few users understand the security infrastructure, so calls usually begin with "I got an access denied message."

The process usually proceeds by identifying the resource that the caller tried to access, finding groups that have read or write rights to it, finding group owners and verifying that access for the caller is appropriate – all before granting access. This sequence can be both time-consuming and costly.

### Return on Investment

*Hitachi ID Group Manager* reduces the complexity of group management by leveraging self-service. This results in increased user productivity and reduced support costs.

#### ✓ A WINDOWS SHELL EXTENSION

*Offer help when users first get an "Access Denied" error*

When installed on Windows workstations, this component replaces the native "access denied" dialog with one that includes a link to the appropriate access request web page.

#### ✓ A WEB BROWSER VIEW OF SHARES, FOLDERS AND PRINTERS

*Intuitive navigation without client software*

Alternately, users can find their network resource using a Windows explorer-like web portal without installing any software on their PCs.

#### ✓ A PORTAL THAT GUIDES USERS TO APPROPRIATE GROUPS

*Easy to understand requests for access*

When users select a share or folder, Group Manager presents appropriate access options:

- Groups that have rights to that resource.
- Nested groups.
- Nested resources (folders).

#### ✓ AUTHORIZATION WORKFLOW

*Change requests are subject to secure, reliable approvals*

Requests for group membership must be approved before being completed. Default routing is to group owners but organizations can extend this.

Prompt and reliable approvals are achieved by:

- Concurrent invitations to multiple approvers.
- Approval by X of Y authorizers.
- Automatic reminders.
- Escalation.
- Scheduled delegation.



## ✓ REPORTS

### *Auditable security, transparent change control*

Group Manager can report on:

- Which users are members of group X?
- Which group memberships does user Y have?
- Who authorized membership in group Z for user W?
- When did user A gain membership in group B?
- Who requested and who authorized group B for user A?

## INCLUDED CONNECTORS

### **Directory:**

Windows/Active Directory

### **File/Print:**

Windows, Samba, NAS appliances

## INCIDENT MANAGEMENT INTEGRATIONS

Automatically create, update and close tickets on:

- Axios Assyst
- BMC SDE
- Clarify eFrontOffice
- HP Service Manager
- Symantec/Altiris
- 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 Group Manager** is part of the Hitachi ID Management Suite, which also includes: Password Manager for self-service management of authentication factors, Identity Manager for user provisioning, and Privileged Access Manager to secure administrator and service accounts.

Hitachi ID Group Manager is available as a stand-alone product and is included at no additional cost with Hitachi ID Identity Manager.

For more information, please visit  
<http://hitachi-id.com/>

or call

1.403.233.0740

1.877.386.0372