The Identity Management Challenge
As enterprises deploy ever more systems and applications, and as organizations change ever more quickly, managing user profiles and security rights becomes a major challenge. Each system and application constitutes its own "silo" -- with users, passwords, roles, rights and administrators. Managing users separately on each system and application is no longer an option.

Regulatory Compliance:
Orphan accounts, dormant accounts, stale privileges, unlinked accounts and weak passwords all violate regulatory requirements, which call for strong security in support of privacy protection (HIPAA, GLB, 95/46/EC, ...) and strong corporate governance (SOX, HSPD12, ...).

User Productivity:
New hires waste days waiting for basic access. Current staff wait days for new rights. Time is money, and managing security efficiently can save a lot of both.

IT Support Cost:
Help desk password reset volume and routine access create / modify / delete work can consume up to half of the workload of an IT support group. These are routine tasks better served by automation, not costly human resources.

The M-Tech Identity Management Suite
The M-Tech IDM Suite is designed to alleviate the management pain of too many users on too many systems. Automation, self-service and consolidated user administration streamline access maintenance processes, strengthen security, eliminate user wait times and lower IT support costs.

ID-Synch® User Provisioning
Users spend too much time filling out, shuffling and signing forms in order to setup new hires or get new rights. With ID-Synch, a web- and mail-enabled workflow engine automates request input, validation, routing and approval. Approved security change requests trigger automatic fulfillment.

ID-Certify® Access Certification
Users always ask for more privileges -- never for less. As a result, there is privilege accumulation: orphan accounts, dormant accounts and stale privileges. ID-Certify automatically prompts business stake-holders to audit users and privileges within their scope of authority, to clean up these excess rights. Managers review their direct subordinates, application owners review users of their application, and group owners review their membership. Privilege reductions are sent to appropriate business staff to approve, and are automatically deactivated.

Sage ERM® Enterprise Role Management
Some organizations require a formal model to manage user privileges. A formal, role-based model makes it easier to manage policies regarding separation of duties (SoD) policies and access to sensitive information. Moreover, a role-based approach simplifies management of user rights where many users share the same access requirements.

Using Sage ERM, organizations can quickly identify privilege clusters -- expediting the role engineering process. Anomalous users, who collect too many rights, or whose rights are in variance with their peers, are easy to identify and audit. User rights can be compared to the role model both initially and on an ongoing basis, as part of a regulatory compliance program.

Sage ERM is available from M-Tech and is tightly integrated with the M-Tech IDM Suite: it draws data about current user rights from ID-Synch, can send proposed security change requests to the ID-Synch workflow, and can highlight possible policy violations in ID-Certify.
Enterprise Role Management

Eurekify Sage ERM is a solution for role management:

- The only solution that provides the full lifecycle of role management.
- Collaborative environment for role managers, security administrators, business managers, and auditors.
- Powerful analytical tools for the creation and ongoing management of a consistent, secure, and business-aligned role-based access model.

1 - Survey

- Analyze individual systems and groups of systems.
- Review suitability of bottom-up and top-down strategies.
- Develop a role management project plan.

2 - Engineer:

- Create Initial roles in as little as 1–2 weeks.
- Combine automated and manual cluster analysis.
- Evaluate role model against actual data.
- Iterate to refine and extend the model.

3 - Certify:

- Audit user privileges against the role model.
- Certify and cleanup privileges.

4 - Manage:

- Manage user rights, role definitions and role assignments.
- Enable security, business users and auditors to collaborate.
- Automate regular compliance checks.
- Periodically repeat reviews and certification.

Technical Specifications

Target System Integration
File/Print: Windows NT, 2000, 2003; Novell NetWare, Samba, PathWorks, OS/2
Databases: Oracle, Sybase, SQL Server, DB2/UDB, Informix
Unix: Linux, Sun, HP, IBM, Compaq, SGI, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+
Mainframes: MV5/SOS390/OS15, VM/ESA, Unisys, Siemens
Minis: OS400, OpenVMS, Tandem
Applications: Oracle, PeopleSoft, SAP; open plug-ins for SQL, ASPs, web services and more
Groupware: MS Exchange, Lotus Notes/ID files, Lotus Domino/HTTP, Novell GroupWise
Networking: RAS, routers, firewalls
Flexible Agents: Target API, Telnet, TN3270, TN5250, HTTP(S), Web Services, command-line, SQL code, LDAP attributes
Support Integration
Automatically create, update and close tickets on:
- Axios Assyst
- SupportSoft Smartissue
- Magic Service Desk
- CA Unicenter
- Tivoli Service Desk
- Clarify eFrontOffice
- Peregrine ServiceCenter
- FrontRange HEAT
- Remedy AR System

Addtional integrations through e-mail, ODBC, web services and web forms integration.