

Identity and Access Management Solutions for SAP

Reduce cost, enhance security, improve service

For many companies running SAP, systems administration represents a significant cost. Managing user accounts, providing access to the right systems at the right time, maintaining appropriate security and auditing user management activities is vital.

But all too often these activities rely upon inefficient processes and multiple data entry. The good news is opportunities exist to improve this situation; lowering costs substantially, enhancing security and providing important value-added benefits to the business.

The challenge

All systems need information about their users and in most organizations 'identity data' is held in many different places, including HR, payroll, network operating systems, spreadsheets and application directories. Often this identity data is managed manually (or semi-manually) and relies upon paper-based processes and multiple data entry for each application or service.

Even if it is efficiently managed within each department, the transfer of this information for use in other departments, and in other systems, is often cumbersome and unreliable. Although common, these inefficient practices lead to many negative and costly situations, such as; slow response times for user account management, incorrect access to systems, inconsistency in identity data, and lapses in security.

The solution

The solution lies in 'Identity and Access Management' (IAM) – a structured approach to the creation, management and synchronization of identity and access data throughout your organization.

With an identity and access solution you can:

- Simplify administration by creating a single point of access for the management of identity data
- Ensure all systems are provided with accurate and up-to-date identity data that consistently conforms to your organization's data conventions
- Reduce licensing and administration costs and improve productivity through the implementation of automated, workflow-enabled processes for account creation, deletion and management

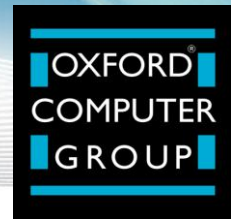
- Create an 'Enterprise Role' model for SAP, allowing greater control of role-based access and more cost-effective administration
- Provide self-service password management to increase staff productivity and reduce security threats
- Improve security and reduce ownership costs by synchronizing users' sign-on credentials (e.g. username and password) across systems and provide facilities for Reduced Sign-on or Enterprise Single Sign-on
- Further improve security by automatically modifying a user's access rights based on their role, and automatically removing those rights when they leave, or their role changes
- Enhance compliance with regulatory standards through improved traceability, audit and reporting of identity data and user management activity

Oxford Computer Group's IAM solutions for SAP

Oxford Computer Group (OCG) designs and delivers solutions specifically for organizations running SAP. By combining the power and flexibility of Microsoft Forefront Identity Manager 2010 (FIM) with our connector for SAP, we have created a cost-effective, easily deployable and high performance solution to address IAM challenges.



FIM 2010



Why FIM 2010?

FIM provides the opportunity to create an 'Enterprise Role' model. This approach leverages your existing investment in SAP roles, making them relevant not just to SAP, but to your other systems. The assignment of SAP composite roles themselves becomes automated, and the assignment of other access rights is automated within other systems.

In addition to the day-to-day efficiencies provided by this approach, it also makes large-scale changes faster and easier to manage, such as company mergers or departmental name changes. Because of this, users' roles more accurately reflect the organization, providing them with higher quality service.

FIM defines and automates the process used to manage the entire lifecycle of digital identities and their associated entitlements. It uses a meta-directory approach to provide identity synchronization, provisioning and credential management. At the same time it supports and maintains multiple identity stores to provide, clean, consistent identity data in each of the connected systems.

Its powerful end user self-service capabilities significantly improve an organization's ability to manage its accounts. It allows end-users to perform self-service tasks such as requesting an Active Directory (AD) user account, or an Exchange mailbox, as well as performing group and distribution list management. Once requests to authoritative sources are approved, FIM's synchronization engine actions them.

Workflow integration

Many business processes require human authorization - for example, a head of department may need to approve the granting of rights to the system that they manage. Integration of workflows into the identity management process can enable the paperless authorization and implementation of user account provisioning.



Automated account management

FIM provides facilities for the automated management of a user and associated entitlements including: provisioning (creation) of new accounts, on-going management of accounts and entitlements, and deprovisioning (those actions required at the end of the life-cycle, such as deletion or disablement of user accounts). These can be driven by business events, such as hiring new staff, staff promotions and moves within the organization.

FIM features at a glance

- Policy management – allowing all enterprise systems to use a common framework for integration, automation and policy management via a SharePoint-based console with workflow capabilities
- Credential management – enabling integrated management of multiple credentials and user self-service from within the Windows logon environment
- User management – for automated, codeless provisioning of users, access rights and resources, and employee self-service
- Group management – enhancing security and compliance, and increasing user productivity via the provision of employee self-service and tight integration with Microsoft Office
- Improved extensibility and developer options



FIM 2010



When an event such as a new hire is initiated, either in the FIM management portal or another system such as HR, automated processes will create accounts and manage entitlements according to the role of the new hire, notifying relevant people, requesting authorizations and seamlessly managing the provisioning process.

Automation of these common processes has many benefits, including:

- Removal of error-prone manual processes, leading to increased productivity for all people involved with the management of identity and access
- Faster response times leading to higher user productivity
- Timely de-provisioning of redundant accounts according to defined business rules, streamlining administration and closing potential security holes
- Reduced software licensing costs through the removal of redundant accounts and the ability to perform accurate user counts
- Improved governance and reporting of change

Self-service password management

In many large organizations password management costs can be significant - with up to 40 percent of all helpdesk calls being password-related.

FIM provides facilities for web-enabled, self-service password management, allowing users to change and re-set passwords in a secure manner without contacting IT support. FIM can also handle the synchronization of user credentials across connected IT systems, updating the relevant identity stores.

Self-service password management can also increase security. It can eliminate word of mouth, paper-based and email password notification processes and can be set to ensure that passwords are changed according to defined business rules. And by removing the burden of password management from the helpdesk, support services budget can be re-assigned to areas of greater value to the business.

Reduced Sign-on and Enterprise Single Sign-on

FIM provides a platform for Reduced Sign-on (RSO) or Enterprise Single-Sign-on (ESSO). With FIM synchronizing identity attributes across your identity stores it becomes far quicker to implement new sign-on solutions. FIM helps to diminish the complexity of this by reducing the number of platforms that actively need to be managed. RSO and ESSO lower the cost of ownership by simplifying password and authentication solutions, reducing support costs and increasing productivity.

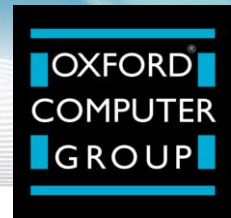
Gain compliance with national and international regulations

Many national and international standards, such as Basel II, Sarbanes- Oxley, BS7799 and EU data protection directives now exist. Being able to demonstrate control of the identity data held within an organization is fundamental to this kind of compliance.

FIM enables a single point of access and consolidated view for the identity data held about systems users. Through the consolidated view it is possible to see, and report on who has what access to which systems; and in combination with workflow enabled processes for provisioning and de-provisioning, a complete audit trail for identity data can be maintained.



FIM 2010



Introducing OCG's FIM integration management agent

As a specialist in the field of IAM and a Microsoft Gold Partner, OCG has been responsible for deploying IAM solutions based on FIM for many global brands. Recognizing the need for a stable, reliable and high performing management agent for FIM/SAP engagements, OCG developed a bespoke SAP Connector, which is proven to outperform existing connectors.

Organizations choose to invest in OCG's SAP Connector for:

- Performance – it is proven to deliver faster and improved performance allowing your organization increased synchronization capacity
- Stability – it is fully supported irrespective of the server your SAP system is hosted on, unlike the out-of-the-box FIM connector provided by Microsoft which is only supported if your SAP system is hosted on a Window platform
- Password synchronization capability – unlike other connectors, it supports password synchronization to SAP, which means users only have to remember one password

SAP connector license

OCG's SAP Connector represents the cumulative experience and development effort of numerous engagements managing SAP as a key enterprise application. OCG can license this connector to organizations and provide supporting services.

Email: info@oxfordcomputergroup.com
 Web: www.oxfordcomputergroup.com

US: Bellevue, WA | New York, NY
 Tel: +1 877 862 1617

UK: Oxford
 Tel: +44 (0)8456 584425

DE: Munich
 Tel: +49 8122 892089-0

BeNeLux: The Hague | Brussels | Antwerp
 Tel: +31 (0)70 36 21 627

What next?

The platform will provide value as deployed or form the first step on the journey to a comprehensive IAM platform. The next stage would be a workshop to review the strategy and approach to extending the solution.

If you would like to learn more about how other organizations have benefitted from OCG's approach to FIM implementations, then please contact us directly. References can be provided upon request.

Oxford Computer Group (OCG) is an IT service company that specializes in Identity and Security with a particular focus on Identity and Access Management (IAM) and Information Protection. With 600+ enterprise projects completed and more than 6000 people trained on Microsoft identity and security technologies we have a wealth of expertise, solution components and training courses to offer. Operating from offices in the US, UK, BeNeLux and Germany, OCG is a Microsoft Gold Partner with Identity and Security Solutions, and Learning Solutions competencies. We understand identity and security – benefit from our experience and capability

Copyright © Oxford Computer Group 2011



2011 PARTNER OF THE YEAR
 Identity and Security
 Finalist