



# Identity and Access Solutions for Microsoft Office SharePoint Services

## ■ Enhance SharePoint. Reduce costs. Increase Security. Improve Service.

For companies running SharePoint (Microsoft Office SharePoint Services – MOSS 2007), access control and user profile management are key to a successful deployment and effective ongoing operation. By enhancing your SharePoint investment with Microsoft Identity and Access (IDA) technologies you can:

- Accelerate your SharePoint deployment
- Improve SharePoint user profile management
- Provide an obvious location for enterprise identity and access management
- Provide secure remote access
- Provide federated access

The result is reduced costs, significantly enhanced security and greatly improved services across your entire organization. In addition it can improve the usability and uptake of your SharePoint platform and services.

Oxford Computer Group (OCG) has proven expertise in providing solutions to enhance your user profile management within SharePoint. This is achieved with Microsoft Identity Lifecycle Manager (ILM) combined with OCG's own ILM SharePoint Management Agent.

Placing SharePoint at the centre of your organization's identity management will deliver numerous benefits including:

- User self-service
- Automated provisioning
- Appropriate access rights
- Accurate and consistent identity data across systems

For organizations seeking to open up SharePoint for external users, OCG can also provide secure remote access through Microsoft Intelligent Application Gateway and federated access with Active Directory Federation Services (AD FS).

## ■ SharePoint User Profile Provisioning and Management

SharePoint user profiles provide detailed information about individuals in an organization. A SharePoint user profile organizes and displays all of the properties attributed to each user, together with other related documents and items.

For many companies with complex, heterogeneous environments, the task of managing the entire organization's SharePoint user profiles usually requires manual intervention and multiple data entry. Creating users with appropriate access rights and maintaining them effectively can therefore present a considerable administrative and financial burden.

With a SharePoint IDA solution based on ILM, the creation, deletion and maintenance of up-to-date SharePoint profiles is made significantly easier. The solution allows an organization's SharePoint user profiles to be kept up-to-date by ILM. ILM populates the SharePoint user profiles with data from any of its connected data sources, such as Active Directory, HR systems, company white pages, email Global Address Lists etc.

By utilizing ILM's provisioning and deprovisioning power, an organization's SharePoint user profiles can be created and deleted in line with its business rules. That means a new starter can have access to all the required and approved systems from the minute they join the company. It also means their access privileges can be changed as and when required and removed when they leave. This significantly reduces the possibility of data theft.

## ■ SharePoint as Part of an Identity Management Solution

The implementation of ILM enables the two-way synchronization of identity data across multiple identity stores. Having identity attributes and access rights visible and manageable in SharePoint and then presenting this to enterprise systems is extremely powerful.

When SharePoint is combined with ILM it enables SharePoint to act as the central point of identity management, with ILM providing approvals, workflow, roles, credential management and group management.

### Consistent identity data for all systems:

Within an organization an employee's identity consists of many different attributes, including HR data, payroll data, assignment of company property, building access and systems access data, to name but a few. As a result, identity data is stored in multiple identity stores, databases and directories.

The implementation of ILM enables the synchronization of identity data across all of these stores. As a result you can place the management of each data attribute with the department or person most suited to manage it, and then appoint the associated identity store as the authoritative source from which all other systems take values for that attribute.

This delivers the following benefits:

- Quality of data is significantly improved because it is entered and managed by a department or person with a high level of 'ownership' for the data. This means fewer errors, inconsistencies and duplicates.
- Systems can share common identity data. This removes the need for multiple manual entries of the same data, which greatly improves productivity and reduces the potential for errors and security leaks.
- Consistent data standards can be provided and enforced for all systems.

**Automated account management:**

ILM provides facilities for the automated management of an identity lifecycle, including provisioning (creation) of new accounts, ongoing management of those accounts and deprovisioning (those actions required at the end of the lifecycle, 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.

When an event such as a new hire is initiated in the HR system, automated processes will create accounts and access rights according to the role of the new hire - notifying relevant people, requesting authorizations and seamlessly managing the provisioning process.

Automation of these common provisioning and deprovisioning processes delivers many benefits, including:

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

To complement ILM, OCG has developed a .NET-based ILM Management Agent for SharePoint. This provides added functionality and tighter integration between ILM and SharePoint. The combination of ILM and OCG's .NET Management Agent provides a proven and highly cost-effective solution for Identity and Access Management with many advantages over other solutions including:

- It is suitable for short-term tactical solutions as well as long-term strategic solutions
- The per-server licensing model is typically much less expensive than rival software costs
- It enables quick implementation of ILM and provides a rapid return on investment
- The Visual Studio.Net development environment provides a flexible and cost effective platform for customization and future upgrades
- ILM is a key component of Microsoft's road map for Identity and Access Management, therefore ensuring the long-term future of your investment

**OCG's SharePoint Management Agent – what it does:**

Our solution for provisioning user profiles into SharePoint is in two distinct parts. The first part is a Web Service, running on IIS on the SharePoint server farm. The Web Service is used to pass requests from the ILM SharePoint Management Agent (MA) to the MOSS server via the MOSS Object Model API.

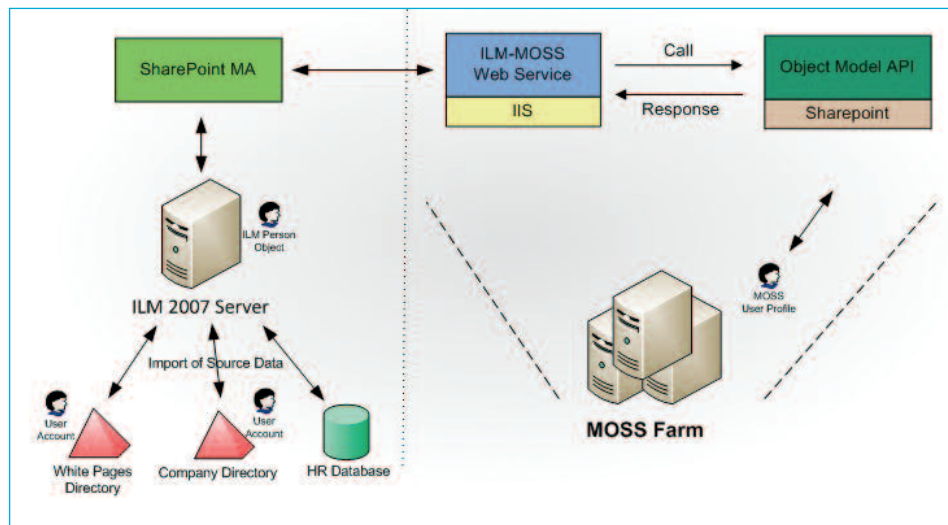
The second part is the SharePoint MA itself which makes calls from the ILM server to the ILM-MOSS Web Service installed on the MOSS server. The MA and the Web Service are described in more detail below.

The SharePoint MA is built as an ILM Extensible Management Agent which allows ILM to connect to systems that do not have an out of the box connector. The MA provides an interface which is used to make calls to the ILM-MOSS Web Service installed in IIS on the MOSS Farm. These calls are made using a 'SOAP over HTTP' call to the Web Service.

**Why ILM & Why OCG?**

ILM uses a meta-directory approach to provide identity synchronization, provisioning and credential management. It also supports and maintains multiple identity stores to provide clean, consistent identity data in each of the connected systems. It is highly robust, scalable and has what we believe to be the best synchronization and provisioning engine available.

**Overview of Solution Architecture**





The Web Service then passes the request into the MOSS Farm via the standard MOSS Object Model API. This service allows requests to be made to create, modify or delete user profiles in the MOSS Farm. The Web Service acts as the intermediary in the conversation between MOSS and ILM and merely passes requests to and from the MOSS API.

The user profiles can be created to match existing user accounts in a company's Active Directory forest or other data source as required. The power and flexibility of ILM provisioning enables user accounts to be controlled so that profiles are only created according to a specific set of business rules.

The user profiles can also be populated with common attributes from the company directory such as location, telephone numbers, roles or titles and department information as required. This is done using ILM attribute flow to ensure changes made in the source system are reflected in the MOSS user profile.

Again, all of the synchronization rules that are setup for attributes are completely flexible and can be tailored to suit each individual situation.

ILM incorporates endpoint detection and cache cleaning with configurable security policies to define the end users experience in the SharePoint portal. This sets the session timeout parameters and user's capabilities, such as whether they are permitted to upload or download data in the SharePoint portal. The cache cleaning ensures that any cached data during the ILM session is removed when the session is terminated.

### Leveraging AD FS and SharePoint:

There may be times when you need to make specific resources from trusted partners available to your users, or vice versa. Traditional solutions for achieving this require the resource owner to either create an account for each user somewhere in the organization or to set up a dedicated directory for this purpose. These solutions can result in inefficient duplication of effort. They also leave the resource owner responsible for authorization, authentication and security and with the burden of managing forgotten passwords. AD FS is a solution that allows the identity provider to be solely responsible for their own authentication, leaving the resource provider free to focus exclusively on the process of secure authorization.

Web-based applications may be published in SharePoint so that users from outside the organization, i.e. those people who do not have an account with the partner hosting the resource, can be authorized to access the application simply by authenticating against their home directory. This distinction between authentication from authorization is one of the key benefits of using AD FS. Users can also enjoy a single sign-on experience, thereby potentially accessing resources hosted by multiple partners and yet only ever authenticating against their home directory.

### Licensing and Delivery:

The OCG SharePoint MA is licensed on the basis of a one-off payment, for which you receive the MA and associated documentation and a number of days consultancy from OCG to help you with implementation of the MA. An annual support agreement can also be purchased to provide you with updates and helpdesk support, should you need it.

Contact us today to discuss your requirements. OCG can help you realize the full potential of your SharePoint investment.

### SharePoint Remote Access and Collaboration

Remote Access and Collaboration provides secure remote access to your systems so that employees, partners and customers can engage with your organization. Providing remote access to key systems such as email and portals enables your organization to be more flexible and operationally robust. It can also significantly reduce overheads and associated costs.

Solutions for remote access can be secure, robust and easy to manage. They provide the highest possible control over who is using your corporate systems and data. Microsoft Intelligent Application Gateway (IAG) allows an organization to publish SharePoint to employees, customers and partners and provide secure access across a wide range of devices.



2008 ADVANCED INFRASTRUCTURE SOLUTIONS PARTNER OF THE YEAR-WINNER  
Active Directory



2008 SECURITY SOLUTIONS PARTNER OF THE YEAR-FINALIST  
Identity and Secure Access

**Oxford Computer Group UK**  
Bignell Park Barns  
Chesterton, Oxfordshire OX26 1TD UK  
**Tel:** +44 (0)8456 584425  
**Fax:** +44 (0)8456 584426  
**Email:** info@oxfordcomputergroup.com  
**www.oxfordcomputergroup.com**

**Oxford Computer Group North America**  
One Microsoft Way  
Building 25, Room 1482  
Redmond, WA 98052  
**Tel:** +1 877 862 1617  
**Email:** info@oxfordcomputergroup.com  
**www.oxfordcomputergroup.com**

**Oxford Computer Group Deutschland**  
Winterlestr. 10b  
D-85435 Erding, Deutschland  
**Tel:** +49 8122 892089-0  
**Fax:** +49 8122 892089-99  
**Email:** info@oxfordcomputergroup.com

**Oxford Computer Group BeNeLux**  
Sweelinckplein 9 (Unit 11)  
2517 GK Den Haag, The Netherlands  
**Tel:** +31 (0)70 36 21 627  
**Fax:** +31 (0)70 36 21 677  
**Email:** BeNeLux@oxfordcomputergroup.com  
**www.oxfordcomputergroup.com**

### About Oxford Computer Group

Oxford Computer Group (OCG) is an IT service company that specializes in identity and access management. With worldwide operations OCG has an enviable repository of expertise, solution components and training courses. OCG has deployed 400+ enterprise-wide identity and access solutions and our instructors have trained over 4000 people on Microsoft IDA technologies. We understand identity and access management – benefit from our experience and capability. Worldwide operations in North America, United Kingdom, Germany and BeNeLux.