

CREATING CAPABILITY FOR ASSOCIATE SUPPORT THROUGH IDENTITY MANGEMENT

Dave Kerr

Programme Manager – Identity Management, Information Services Division, 1st Floor, Ashworth Building, University of Salford, The Crescent, Salford, Greater Manchester, M5 4WT, United Kingdom. d.g.kerr@salford.ac.uk

Abstract

Following a successful proof of concept project exploring the potential benefit of an institution-wide Identity Management (IdM) solution, the University of Salford has embarked on a five year programme to implement a comprehensive and ambitious IdM solution across the entire organisation. The programme has attracted widespread interest from both academic and commercial arenas and the University has already been awarded with the prestigious *Centre of Excellence for Identity Management* status. Working closely with our selected partner - Sun Microsystems - the IdM programme will revolutionise the way in which a wide range of resources are made available to the University community including staff, students and associate members (i.e. individuals who are neither staff nor students).

For most institutions, a number of problems concerning the management, administration and control of access for associate members (visiting lecturers, associate college staff, research collaborators and external examiners etc.) are likely to exist. Associate members are not typically recorded in any centrally held database, system or information store and there are usually large gaps in what an organisation knows about this important but diverse group. Associate members themselves are also likely to experience some difficulty in gaining access to the resources they may require due to the level of manual effort and intervention often needed. This results in negative customer experiences and unnecessarily impedes an associate member in carrying out their duties or critical business activities. Significant opportunities for revenue generation and radically improving levels customer service are often lost as a result.

This paper will explore how the University of Salford has radically transformed the way in which associate members are supported throughout their entire lifecycle whilst reducing administration and management overheads, reducing helpdesk call volumes, improving security and dramatically enhancing levels of customer service across the organisation.

In particular, the paper will provide an overview of the extent of associate support now in place including:

- The creation of a dedicated authoritative store for associates,
- Account request and account creation processes,
- Resource provisioning by associate type,
- Controlled account-activation processes through self-service,
- Password resets through self-service.

CREATING CAPABILITY FOR ASSOCIATE SUPPORT THROUGH IDENTITY MANGEMENT

The History of Identity Management at the University of Salford

It was the University of Salford's Integrated Information Infrastructure (III) strategy developed in 2003 that first highlighted the potential of an Identity Management (IdM) system in solving many of the organisation's challenges. This strategy recognized IdM as a crucial building block in the Information Services Division's long-term aim to bring previously disparate systems and applications together into a more coherent whole, whilst ensuring that a *single version of the truth* could exist at any one time.

In addition, the III strategy highlighted Identity Management as a solution to a number of issues relating to the controlled provisioning and de-provisioning of accounts (and a wide range of resources) to the University population in secure, effective and controlled ways.

The IdM Proof of Concept Project and Executive Buy-In

In May 2005 the University completed a proof of concept project exploring the potential benefit of an institution-wide Identity Management (IdM) solution and as a vehicle to gain executive buy-in and support for further investment.

The proof of concept integrated a number of key University systems including SAP (the University's Human Resource Management System and the authoritative source for staff information), Novell e-Directory (the main authentication directory for network access) and Active Directory and Exchange.

The system demonstrated how key resources (such as University network and email accounts) could be automatically provisioned for new starters, and how access rights to resources such as University intranet sites could be amended automatically as individuals were recorded as having changed organizational units. The potential for IdM self-service and controlled workflow to request and approve resource requests, as well as the resetting of individual passwords was also shown.

The proof of concept also illustrated, using Novell e-Guide, how real-time updates of online contact or "white pages" information could be achieved (currently requiring ad-hoc manual effort to maintain and administer). Finally, as individuals were recorded as having left the organisation in SAP, the system demonstrated the automatic de-provisioning of resources in the disablement of accounts and removal of relevant access rights, as well as the automatic reflection of this in the online contact directory.

The success of the proof of concept was realized in the subsequent approval from University executive to seek further investment. There is no doubt that this project itself enabled senior decision makers to gain a better of understanding of how such a system could dramatically improve the administration and management of key resources, whilst demonstrating how the user experience for staff and students alike could be significantly enhanced.

A Third, “Hidden” University Population

However, the concept of a third University population outside of the traditional staff and student populations had existed for some time at the University of Salford. Individuals belonging to this group were often referred to as “grey members”, “guests” or “associate members” across the organisation. Whilst the requirements of staff and students and their resource requirements were well documented, very little was known or understood about the variety, size or needs of this amorphous community.

Across ISD, there was a growing realization that any enterprise-wide Identity Management system would also need to administer and support the requirements of these individuals alongside staff and students throughout their association with the University. Whilst preparations began to obtain HEFCE funding and launch a European wide tender for an enterprise-wide Identity Management solution, the *Associate Members Project* was launched to investigate and obtain further details and knowledge concerning this third, “hidden” University population ...

The Associate Members Project

“Associate Members” (or simply “Associates”) at the University of Salford are now defined as “individuals engaged in some of activity with the University who need access to one or more University resources but do not satisfy either of the two traditional criteria of university membership - that of being students or staff - and as such are not recorded in the University’s Human Resource Management System (HRMS) or Student Information System (SIS).” Typically, associate members will be referred to as a range of terms across institutions with example typically including Honorary and Visiting Lecturers, contract staff, estates contractors, short course students, corporate visitors etc.

The Associate Members Project was a five-month long analysis of associates at Salford, and comprised interviews with around 100 key stakeholders across the organisation representing a total of 45 distinct organisational units. The completion of the Associate Members Project was seen as a pre-requisite to any subsequent IdM programme initiation. Key objectives of the project included obtaining a clearer understanding of associate types and their current and future resource requirements, as well as a clear understanding of the organisation’s data requirements concerning these individuals.

It is important to note that pre-project expectations estimated somewhere between 2,500 to 5,000 associate members in existence, amounting to around 12 differing types, and somewhere between 12 to 15 University resources needing to be accessed at any one time. However, the key deliverables of the Associate Members Project were in stark contrast to our initial expectations and resulted in some startling findings as follows:

- Approximately **40,000** associates (excluding Alumni) were estimated to interact with the University over a 12-month period,
- Belonging to one or more of **77 distinct types or “classes”** of associate members,
- Each requiring access to one or more of **85 distinct resources** at any one time.

The Associate Members Project also highlighted and documented a wide range of issues relating to the creation, management and administration of associate members. Whilst these were documented from a University of Salford perspective there are likely to be familiar to any Higher Education institution across the world.

Issues included:

- A wide range of ad-hoc, manual and largely ineffective account creation and provisioning processes existed,
- Large gaps in knowledge, and the absence of any centrally held data store containing associate member information,
- Limited key information or data was stored or available concerning individuals themselves (such as the duration of their association, their requestor, contact numbers, their organisation or company, and in some instances their name),
- Significant security concerns, (mainly around de-provisioning and the controlled removal of access rights and disablement of accounts on a timely basis),
- Typical delays experienced in the creation of accounts (particularly relating to PC setup), resulting in slow lead times to productivity,
- Negative customer experiences throughout the account creation and induction process.

In short, the Associate Members Project highlighted significant concerns relating to the capability of the University to provide adequate levels of support to the associate member population. Failure to significantly enhance the level of support for associates would ensure the continued existence of all kinds of barriers in a wide range of day-to-day activities, across the entire organisation.

Whilst key initiatives in the Higher Education (such as Shibboleth and EduRoam) serve to extend an institution's capability to open specific resources to their research and academic communities, many of these initiatives are in relatively early stages of adoption and provide limited opportunities for organisations to support their entire associate communities and across the full range of their resources.

Meanwhile, during the Associate Members Project, significant progress had made in the securing of initial funding and the completion of the University's European wide tender. This resulted in the eventual selection of Sun Microsystems as the key strategic supplier and the planned implementation of their Identity Management suite (part of the Sun Java Enterprise System).

The completion of the Associate Members Project coincided with the initiation of the University's Identity Management Programme in October 2005. However, as will be seen, the findings of the Associate Member Project continued to inform and guide numerous aspects of the early activities, goals and desired outcomes of the IdM programme itself.

The Identity Management Programme at the University of Salford

Initial activities of the programme focussed on the creation of an appropriate governance framework, the definition and agreement of the IdM roadmap, and the eventual successful completion of recruitment of a core Identity Management team in August 2006.

The IdM programme now underway will revolutionise the way in which a wide range of resources are made available to the University community including staff, students and associate members (i.e. individuals who are neither staff nor students), ensuring that the right IT resources are provided to the right people at the right time.

Over the next five years, the IdM programme will:

- Provide increased visibility and control over resource access entitlements for all (staff, students and associate members) associated with the University,
- Ensure that the creation and removal of access to university resources occurs in a controlled and consistent manner, whilst safeguarding the security of these resources as far as possible,
- Streamline existing business processes to reduce administrative overhead and enhance levels of customer service,
- Simplify an individual's interaction with university resources and reduce the visible barriers to protected resources,
- Provide a solid basis for the integration of all existing and future systems into a seamless whole, whilst ensuring that individuals can access the resources they need painlessly and effectively, and
- Provide greater opportunities for enhanced collaboration with associated institutions.

During the definition of the IdM roadmap, it became abundantly clear that the success of the IdM programme was dependent on the early replacement of the University's existing Account Management system called "AccMan", developed in-house in 1999.

AccMan was developed utilizing a graphical user interface written in Borland Delphi, a MySQL database (running on FreeBSD), and a large number of back-end Perl scripts to trigger a variety of account provisioning processes across a number of applications (including Network, file store, email, Library access, VLE access etc.) for staff, students and associate members. Systems similar to AccMan are known to exist across a large number of universities across the UK.

The current AccMan system has grown substantially since this time, not always in controlled ways. Very little documentation concerning the inner workings of the system exists and the University is reliant on a single member of staff to support and maintain this mission critical system. The University is also somewhat limited in the extent to which this system can be supported, since the individual responsible for developing and maintaining the AccMan graphical user interface left the organisation over three years ago and has not been replaced. For these reasons, any amendment to AccMan system functionality is considered a high risk activity.

The AccMan Replacement Project

The AccMan Replacement Project is one of the first major projects to be undertaken within the IdM programme.

The project will address a number of significant flaws in the existing system, as follows:

- Currently, there is no capability for providing access to University resources on a granular basis. All individuals processed by AccMan will be given access to all University resources regardless of need or licensing considerations.
- There are significant security issues relating to the absence of any mechanisms to ensure that accounts are de-provisioned on a controlled basis when an individual leaves the organisation.
- Finally, there are some issues relating to the timely provisioning of resources, resulting in substantial delays before individuals have access to required resources.

A number of separate projects have already been undertaken in parallel to design, implement and configure a highly-available infrastructure and platform for the IdM programme itself.

A variety of approaches to the AccMan Replacement Project were considered, and each approach was assessed according to a variety of criteria that included the need to reduce risk whilst delivering early business benefits to the organisation. The outcomes and findings of the Associate Members Project were seen to be directly informing the consideration of approaches and AccMan replacement strategies, and early opportunities for addressing the issues surrounding associate members were sought...

Early Opportunity to Enhance Associate Member Support

The approach chosen (and now in the process of being implemented) is based on a four stage replacement of specific AccMan components over time, with the phased transition of staff and students into the new Identity Management system.

Importantly, the selected approach also provided - **during the first stage of the project** - the following deliverables:

- The creation of an authoritative store for associate members,
- The design, development and implementation of controlled associate account request and creation processes (and the subsequent provisioning to a number of University resources and applications),
- The design, development and implementation of controlled account self-activation processes, and
- The design, development and implementation of self-service functionality for password resets and support for the provision of key account information.

Prior to the completion of this stage of the project in May 2007, the processes for requesting, managing and administering associate members were known to be ad hoc, ineffective and prone to considerable risk of security breaches. Information captured about associate members and their account requestors (called “sponsors”) was also sparse and there were no adequate mechanisms in place to enforce data capture.

The first stage of the AccMan replacement project now completed, utilizing Sun’s Identity Manager, has provided the University of Salford with significantly enhanced capability to create, administer and support associate members across the entire organisation.

In doing so, we have already solved many of the challenges we are likely to face when staff and students accounts are transitioned over to the Identity Management system in subsequent stages of the project. In addition, since associate members are currently so poorly supported across the organisation, this has been achieved with minimal risk prior to the completion of more highly visible components for staff and students in the future. In particular, the secure self-activation and self-service functions and processes developed for associate members provide a solid foundation for all future development, and we are confident that these can be rolled out to the remaining user community of staff and students with minimal amendment.

The remainder of this paper will provide further insight into, and exploration of, the design and development of key components of this solution that together provide significantly enhanced capability for associate member support through Identity Management.

These include:

- Creation of a single, authoritative source for associate members,
- Controlled, consistent associate account request and creation processes,
- Resource provisioning according to type or class of association,
- Controlled, consistent account self-activation processes, and
- Self-Service functionality for password-resets and additional account support.

Creation of a Single, Authoritative Source for Associate Members

One of the major findings of the Associate Members Project was the need to create a third, trusted source of identity data for associates. This need arose largely from the range of ineffective and ad-hoc processes for account creation as well as the limited range of data captured concerning associate members themselves. The creation of a single, authoritative source would also ensure that a single repository for associates could be created that provided the foundations for further integration and improved management reporting in the future.

A wide variety of solutions to this are known to have been implemented by other institutions in the past, and a mixture of home-grown “guest management” systems are known to coincide alongside the existing student and staff administration systems that have been extended (not always in appropriate ways) to handle specific types of guest or associate, where possible.

Whilst the appropriateness of such solution architectures can be endlessly disputed, we felt that implementing similar designs would ensure that the range of inconsistent and ad-hoc account creation processes (as well as the known issues relating to the extent, validity and accuracy of associate data) would persist.

However, we did examine a number of options. These included:

- The development a brand new SAP instance outside of our existing HRMS system,
- The development of entirely separate applications for associate member creation, outside of Identity Management system,
- The extension of existing authoritative data sources for staff **and** students to hold associate member data, and
- The embedding of an associate member authoritative source within the Identity Management fabric itself.

Our decision was predicated by a number of overriding concerns. These included the need to minimise the cost of doing this (also taking into consideration any additional licensing costs that might be payable), whilst meeting performance and resilience requirements. At the same time, we wanted to minimise the complexity of any resultant solution, and to make use of existing resources where possible this avoiding the need for any further reliance on additional internal or external resources than was necessary.

We recognised the potential of Sun's Directory Server to serve as our single authoritative data store for associate members, and to utilise and extend the user creation functionality inherent within Identity Manager to provision this store as illustrated below:

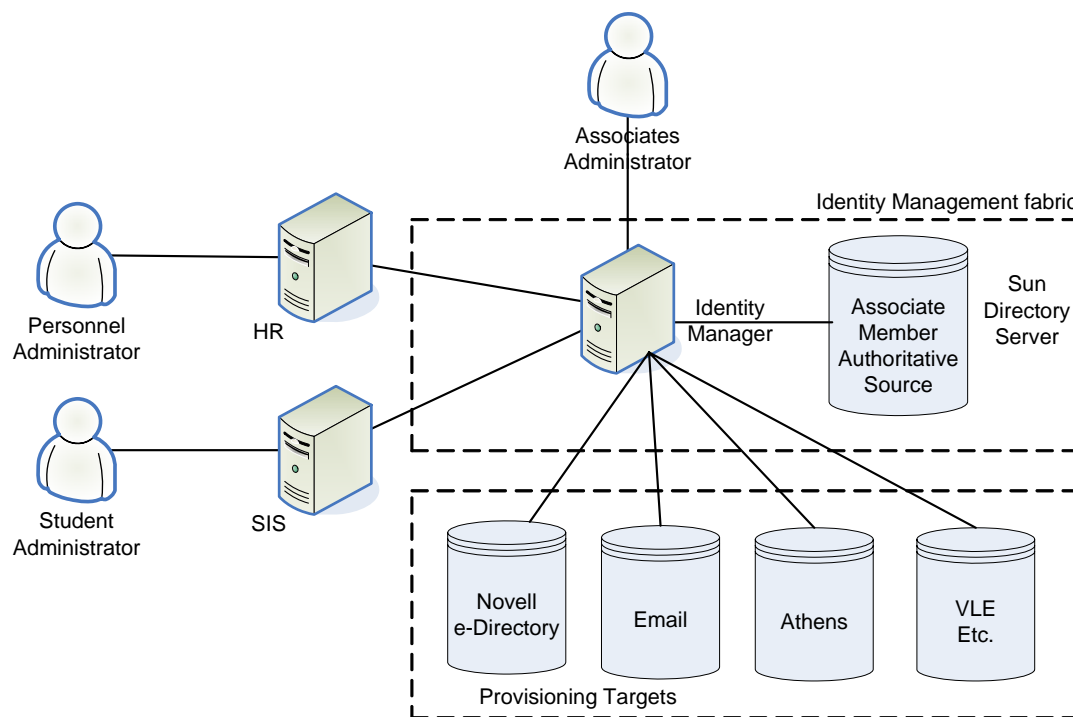


Figure 1 – A Single, Authoritative Source for Associate Members

This decision – to embed the authoritative store within the Identity Management fabric - quite neatly addressed all of our concerns. It meant that we could make use of existing technology within the Identity management suite without incurring any additional licensing costs (since the JES subscription is based on the number of staff/faculty members). It also meant that the solution could be developed utilising skills and experience within the IdM team itself.

It became clear that Identity Manager could also be amended to ensure that data requirement rules could be specified for each specific class of associate member. More importantly, the utilisation of Identity Manager itself for the creation and management of associate accounts ensures that, at a later date, we can make use of the delegated administration capabilities inherent within the Identity Management suite, without substantial development.

A useful by-product of this decision was the adoption of a look and feel for associate data capture and account administration consistent with that of account administration functions, thereby resulting in the eradication of any further need for user education and training.

The design and creation of the authoritative source for associate members in Sun Directory Server, led to the subsequent need to design, develop and implement a clear and consistent process for account request and creation ...

Associate Member Account Request and Creation Process

For the first time, the University of Salford now has a consistent process for how associate accounts are requested and created, whilst being able to ensure a consistent standard of service. A depiction of the associate member account creation and request process now in place is provided below:

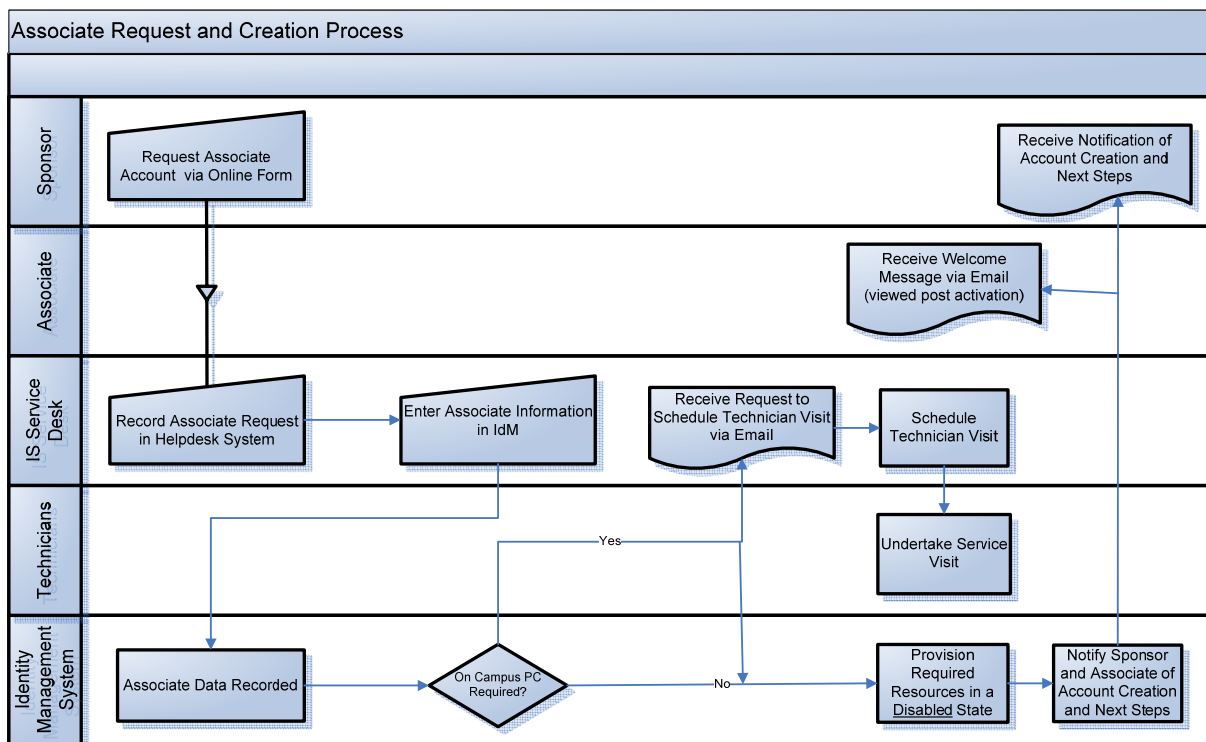


Figure 2 – Account Request and Creation Process

In order for an associate member to obtain access to any University of Salford resources, a staff member must first request that an account is created for them on behalf of the associate member. This staff member (i.e. the requestor) is the associate member's **sponsor**, and is responsible for ensuring that the resources requested are appropriate to the relationship the associate member has with the University of Salford.

Access to University of Salford resources is a privilege which can only be provided to people who have a legitimate reason to use them. Registered students and employed staff members have a direct legal relationship with the University and right to use its resources. Associate members do not have the same direct legal relationship with the University and therefore, someone who does have such a relationship (i.e. a staff member) needs to confirm that each associate member has a legitimate reason for using University of Salford resources.

A wide range of support material has been provided via the University intranet to inform and guide potential sponsors through the associate account request process. This includes support material to help sponsors determine the appropriate class of association, as well as the creation of an online request form that enables a sponsor to enter the necessary information required prior to the request being submitted ...

The screenshot shows a web browser window displaying the University of Salford intranet. At the top, a breadcrumb trail reads: "You are in: University home > ISD home > Getting help from ISD Service Desk > Request to set up a new Associate Member". The University of Salford logo and name are visible on the left. On the right, there are links for "Student Channel", "Staff Channel", and "Channel search". The main heading is "Information Services Division" followed by "Request to set up a new Associate Member". A left-hand navigation menu lists various services like "ISD home", "Library", "Computing", "Training", "Electronic resources", "Audio Visual Services", "Getting help from ISD Service Desk", "Services", "Book a room", "Log a problem", "Support for AV", "IDM for Associate Members", "User guides and links", and "Statistics". The main content area is titled "Request to set up a new Associate Member" and contains "Instructions" and two form sections. The first section, "Sponsor Information", asks for "Name", "Email", and "Job title" with corresponding text input fields. The second section, "Associate Member information", includes a "Title" dropdown menu, a text input for "If you cannot find the title you require please include it:", and a "First name" text input field.

Figure 3 – The Online Associate Request Form

The online request form validates each request to ensure that base information (such as information relating to the sponsor themselves, the associate name and contact details, and the associate start and end date etc.) is always supplied. In addition, the form allows the sponsor to specify the class of association required, and this in turn determines the range of resources that will be provisioned, as well as determines any additional data that may be required (such as date-of-birth, or the name of associate's own organisation).

The request form also allows a sponsor to specify whether the associate requires access to a dedicated on-campus PC, and this information, when subsequently entered into Identity Manager, will trigger specific workflow designed to request and schedule a technician visit.

Once all necessary information has been entered, the form is submitted to the Information Services Division’s service desk for processing by a service desk representative, following the formal recording of the request in the department’s helpdesk system. **Note:** Further development is planned at a later date to rollout delegated administration that will enable a sponsor to create an associate account within Identity Manager itself.

Whilst new identities for staff and students will be automatically created by Identity Manager following the recording of these individuals in either the HRMS or SIS systems, new accounts for Associate Members are created within Identity Manage itself.

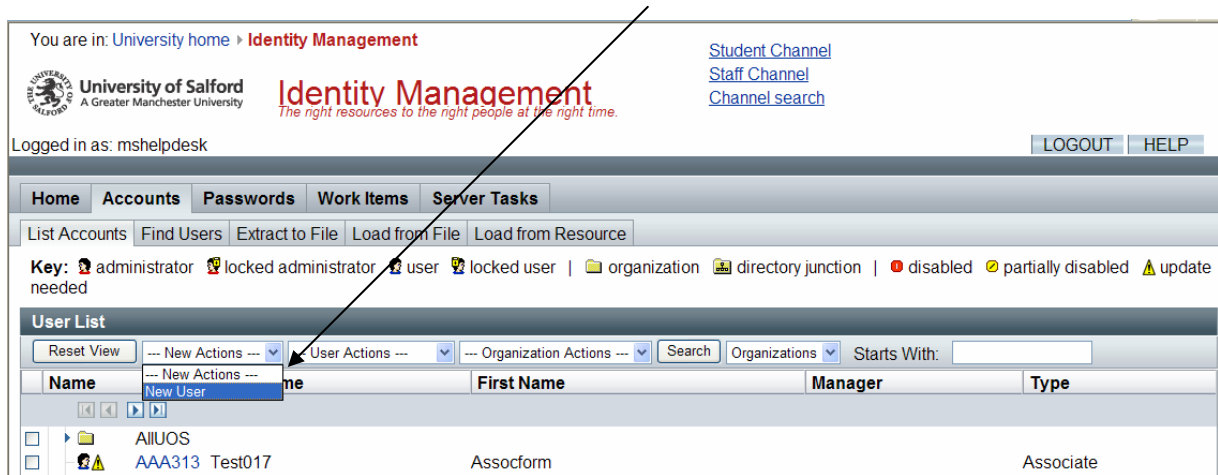


Figure 4 – The Creation of a New Associate

The service desk representative is then required to enter the information specified by the sponsor into a number of specific tabs within the main Create Associate form. This includes base information relating to the associate’s identity as follows:

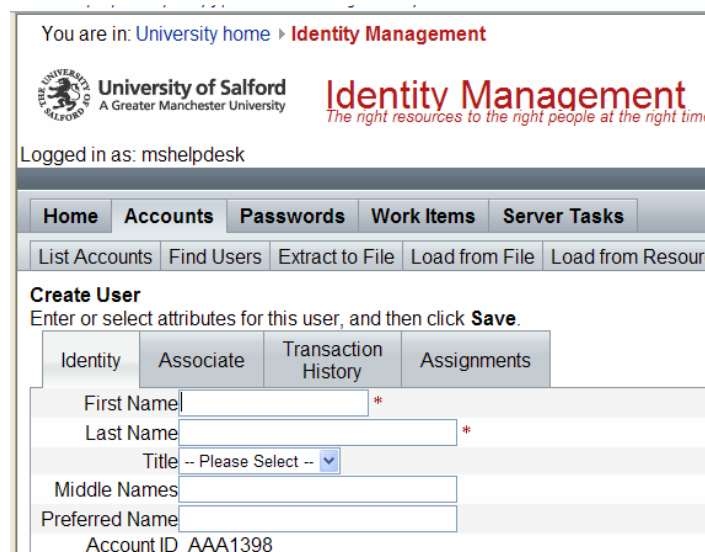


Figure 5 – Base Associate Identity Data

Following this, further information relating to the associate is required, including the category of association and specific class of association, as well as additional information relating to the associate themselves (such as address, contact details etc.).

The screenshot shows the Identity Management interface for the University of Salford. The user is logged in as 'mshelpdesk'. The main navigation bar includes 'Home', 'Accounts', 'Passwords', 'Work Items', and 'Server Tasks'. Below this, there are links for 'List Accounts', 'Find Users', 'Extract to File', 'Load from File', and 'Load from Resource'. The 'Create User' section is active, with a prompt to 'Enter or select attributes for this user, and then click Save'. The 'Associate' tab is selected, showing 'Resource Name: Associate' and 'Associate Attributes'. The 'Associate Type' is set to 'Academic Staff Related' and the 'Associate Class' is 'Artists in Residence'. The 'Department' is set to 'Please Select --'. The 'Person Details' tab is selected, showing fields for 'Permanent Contact Address' (Address 1, Address 2, Town, County, Post Code, Country), 'Contact Phone No' (09999887766), 'Contact Email Address', 'Date of Birth (DD/MM/YYYY)' (15/12/1920), 'Emergency Contact Name', 'Emergency Contact Phone', and 'On Campus PC?' (Yes). A red asterisk indicates a required field.

Figure 6 – The Person Details Tab

It should be noted that the category and class of association will determine what, if any, additional data attributes are required before the identity can be created, as well as determining the range of resources that will be provisioned for the associate.

In addition, in the event that the associate requires a dedicated on-campus PC, at the end of the associate creation process an email will be sent by Identity Manager to the department's helpdesk system to formally request the scheduling of a technician visit. This significant amendment to the existing account creation process ensures that technicians can be scheduled to visit a PC well in advance of an associate arriving on campus, eradicating sometime significant delays due to technician availability.

This close-up screenshot focuses on the 'Person Details' tab of the 'Create User' form. It shows the following fields: 'Permanent Contact Address' (Address 1, Address 2, Town, County, Post Code, Country), 'Contact Phone No' (09999887766), 'Contact Email Address', 'Date of Birth (DD/MM/YYYY)' (15/12/1920), 'Emergency Contact Name', 'Emergency Contact Phone', and 'On Campus PC?' (Yes). A red asterisk indicates a required field. A red arrow points to the 'On Campus PC?' dropdown menu. A red asterisk at the bottom right indicates a required field.

Figure 7 – Specification of an On-Campus PC

Further work is planned to further integrate the Identity Management systems and the helpdesk system such that jobs will be created automatically within the helpdesk system itself, further reducing the administration load of service desk staff.

At the same time, significant security flaws have been addressed by ensuring that information about an associate’s sponsor are stored within the associate member authoritative store (upon completion of the creation process), as well as ensuring that information concerning start and end dates are entered. This, in turn, ensures that accounts cannot be enabled prior to a formal start date, and that accounts will be automatically disabled once an account end date is reached.

Person Details	Association Details	Organisation Details
	Sponsor's Name *	
	Sponsor's Job Title *	
	Sponsor's Email *	
	Start Date (DD/MM/YYYY) *	
	End Date (DD/MM/YYYY) *	
	Joining Credentials	
	Sponsor Authorisation <input type="checkbox"/>	Passport <input type="checkbox"/>
	Driving Licence <input type="checkbox"/>	Birth Certificate <input type="checkbox"/>
	Registration / Naturalisation Certificate <input type="checkbox"/>	Home Office Indefinite Stay Letter <input type="checkbox"/>
	National ID Card <input type="checkbox"/>	

* indicates a required field

Figure 8 – Capture of Association Details

In particular, the automatic disablement of relevant accounts upon expiry of the association is a significant improvement over previous processes. Notification of impending account termination is, however, sent to both sponsors and associates (30 days and 3 days prior to expiry) along with an overview of what action must be taken to extend the account.

The system also stores the joining credentials provided by the associate member in order to demonstrate that they are who they say they are. In future, as the organisation decides what joining credentials are required (based on the class of association), logic can be embedded in Identity Manager to enforce these access policies and to validate that the correct joining credentials have been presented.

Additional organisational details that may be required (such as the name of the associate’s organisation and their job title) may also be specified, if required. Again, the system will enforce the capture of specific data (such as Organisation Name and Job Title), if these are required for the specific class of association that has been chosen by the sponsor.

Person Details	Association Details	Organisation Details
		Organisation Name: Wooster Sauce Ltd
		Job Title: Entertainer
		Organisation Address 1
		Organisation Address 2
		Organisation Town
		Organisation County
		Organisation Post Code
		Organisation Country: -- Please Select --
		Organisation Telephone No

Figure 9 – Capture of Additional Organisational Details

In contrast to the “all or nothing” approach of AccMan in providing access to all University resources regardless of need, the range of resources to be provisioned is based on the resource requirements of the type (or “class”) of associate member.

The screenshot shows a web interface for creating a user. At the top, there are tabs for 'Home', 'Accounts', 'Passwords', 'Work Items', and 'Server Tasks'. Below these are buttons for 'List Accounts', 'Find Users', 'Extract to File', 'Load from File', and 'Load from Resource'. The main section is titled 'Create User' with the instruction 'Enter or select attributes for this user, and then click Save.' Below this is a row of tabs: 'Identity', 'Associate', 'AD', 'Athens', 'Email', 'NDS', 'Transaction History', and 'Assignments'. The 'Associate' tab is selected. Underneath, there is a section for 'Resource Name: Associate' and 'Associate Attributes'. This section contains three dropdown menus: 'Associate Type' (set to 'Academic Staff Related'), 'Associate Class' (set to 'Artists in Residence'), and 'Department' (set to '-- Please Select --'). Arrows from the 'AD', 'Athens', 'Email', and 'NDS' tabs point to the 'Associate Class' dropdown menu, indicating that these resources are provisioned based on the selected class.

Figure 10 – Resources Provisioned According to Associate Class

Hence, network (“NDS”) access only may be provisioned for associates such as corporate visitors or conference delegates (for wireless internet access) whilst network, active directory, Athens, email, Library and VLE access may be provisioned for other associates such as Visiting Lecturers.

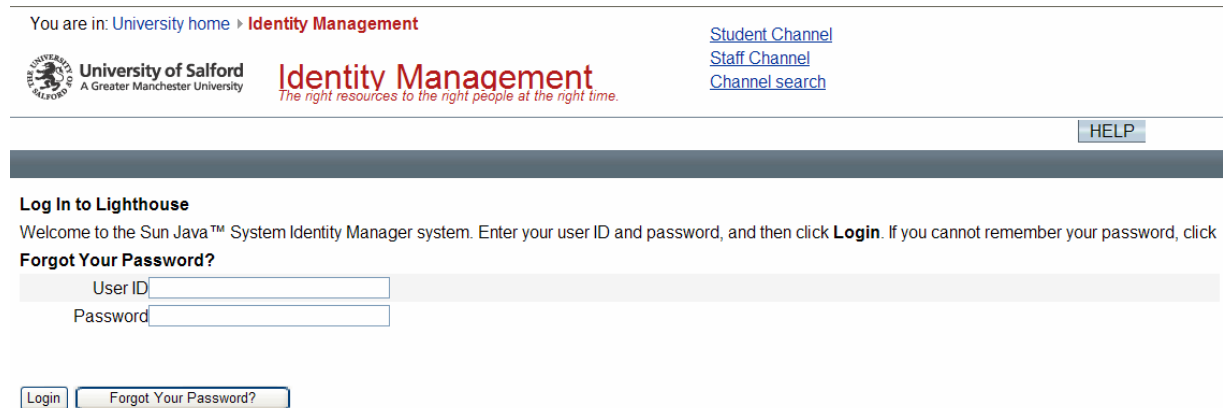
Once required data has been entered and validated, the system will first provide an email containing formal notification of the associate account creation, along with specific details of the main University account username, email address etc., as well as information on how the associate’s initial password is to be derived. This represents the eradication of a significant security flaws relating to how usernames and password were previously defined and communicated. Initial passwords are now derived from information that is likely to be known only to an associate themselves and their sponsor. The email provided to the sponsor also contains important information concerning what the associate member must do in order to activate their main University login account and any other additional resources provisioned. These next steps require an associate to log in to the Identity Management Self-Activation web page using their University username and initial password (described in detail below).

In the event that an associate is also to be provided with an Exchange email account, the system will send a “Welcome to the University of Salford” email to trigger the Exchange account creation process and provide additional information on the use of Outlook, if required.

Finally, dramatic enhancements have also been made to the depth of information available (and amendable where a user has the required level of authority) concerning each associate’s key resource such as NDS e-Directory access, email, active directory etc. In contrast to the existing AccMan system, the Identity Management system now provides service desk representatives with the capability to, for example, specify email account redirections or emails, or to amend Novell group memberships for an associate without invoking second line support, and increasing the volume of call that can be resolved immediately by service desk staff.


Controlled Account Self-Activation Process

The successful completion of self-activation via the Identity Management Self-Activation web page is essential to the activation of an associate's main University account as well as the activation of any additional resources that may be provided.



You are in: [University home](#) > **Identity Management**

[Student Channel](#)
[Staff Channel](#)
[Channel search](#)

 **University of Salford**
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

[HELP](#)

Log In to Lighthouse

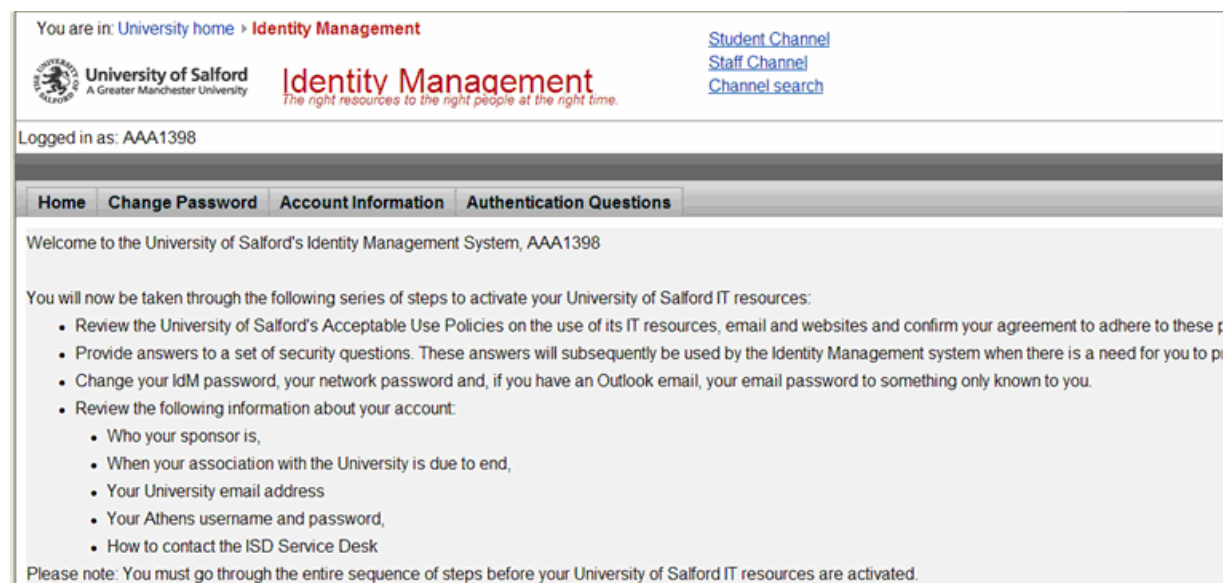
Welcome to the Sun Java™ System Identity Manager system. Enter your user ID and password, and then click **Login**. If you cannot remember your password, click **Forgot Your Password?**

User ID

Password


Figure 11 – The Identity Management Self-Activation Page

Once an associate has correctly entered their University network username and their initial password, they will be presented with a Welcome screen that provides an overview of the steps required for account activation.



You are in: [University home](#) > **Identity Management**

[Student Channel](#)
[Staff Channel](#)
[Channel search](#)

 **University of Salford**
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

Logged in as: AAA1398

[Home](#) [Change Password](#) [Account Information](#) [Authentication Questions](#)

Welcome to the University of Salford's Identity Management System, AAA1398

You will now be taken through the following series of steps to activate your University of Salford IT resources:

- Review the University of Salford's Acceptable Use Policies on the use of its IT resources, email and websites and confirm your agreement to adhere to these p
- Provide answers to a set of security questions. These answers will subsequently be used by the Identity Management system when there is a need for you to p
- Change your IdM password, your network password and, if you have an Outlook email, your email password to something only known to you.
- Review the following information about your account:
 - Who your sponsor is,
 - When your association with the University is due to end,
 - Your University email address
 - Your Athens username and password,
 - How to contact the ISD Service Desk

Please note: You must go through the entire sequence of steps before your University of Salford IT resources are activated.

Figure 12 – Self-Activation Step 1: The Welcome Screen

Once an associate has chosen to continue, they are then required to confirm and agree adherence to the terms of the University of Salford's Acceptable Use Policies on the use of its IT resources, email and websites. Previously, the requirement for associates to confirm their acceptance of acceptable use policies was often overlooked.

This same mechanism will be applied to all new staff and students at a later date, with the potential for further eradication of manual effort and improvement in recruitment and registration processes.

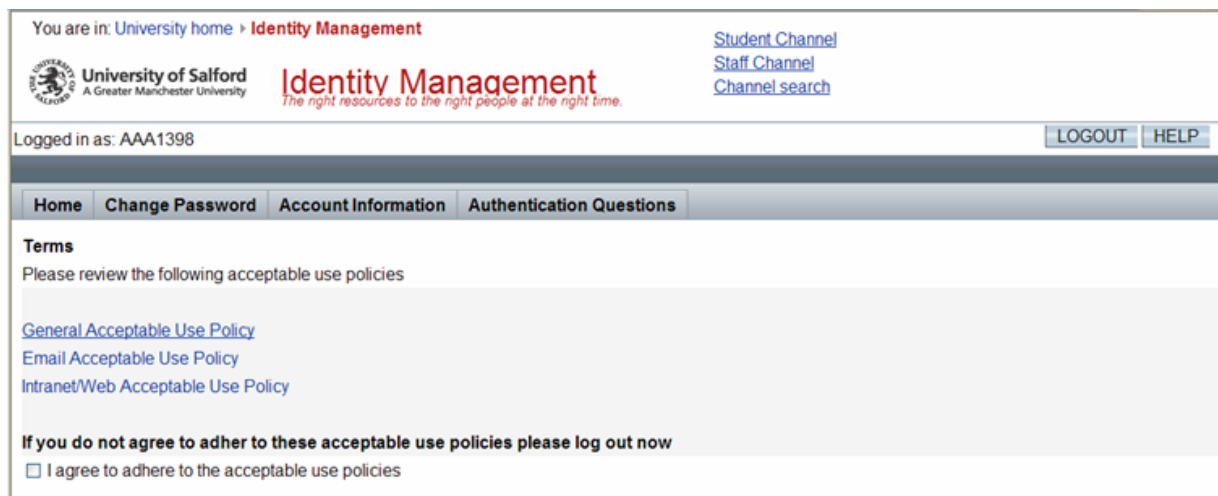


Figure 13 – Self-Activation Step 2: Acceptable Use Policy Adherence

The next stage of the self activation process is the recording of the associate member’s responses to a number of security questions. The responses to these questions may be requested at any time in the future by either the Identity Management self-service system itself or a service desk or enquiry desk agent when an associate is required to authenticate themselves - particularly in the event that they wish to reset their password.

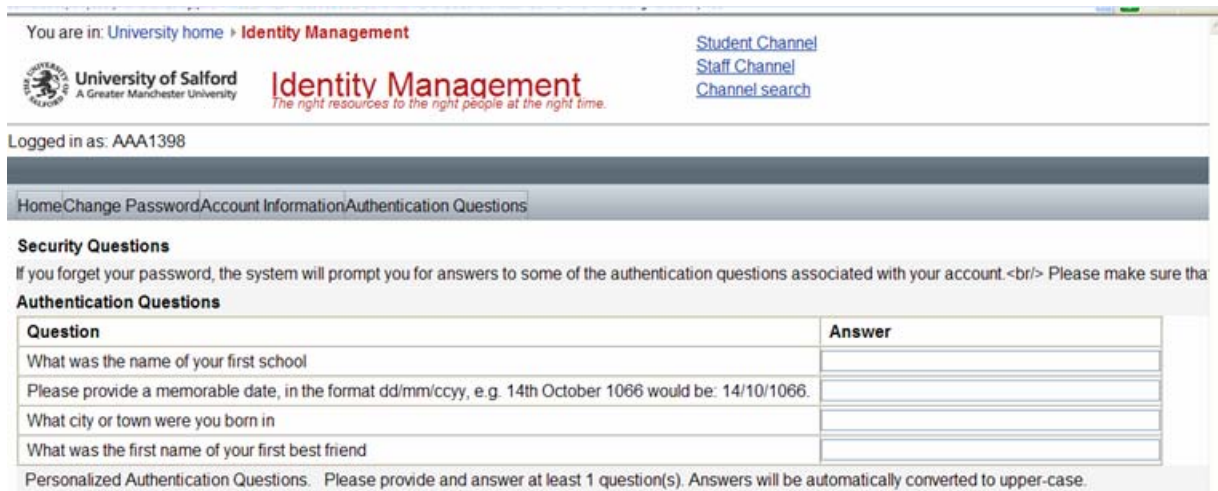


Figure 14 – Self-Activation Step 3: Responding to Security Questions

Once answers to each security question have been successfully provided, the associate will be required to change their password to something known only to them. This password will then become their new password for accessing the network and other resources, as well as the Identity Management system again to use the Self-service Functions.

During this step of the process, the current password policy to be applied is also clearly presented.

You are in: [University home](#) > **Identity Management** [Student Channel](#) [Staff Channel](#) [Channel search](#)

University of Salford
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

Logged in as: AAA1398 [LOGOUT](#) [HELP](#)

[Home](#) [Change Password](#) [Account Information](#) [Authentication Questions](#)

Change Password
Change the password on your accounts
Your password must have the following:

- A minimum of 1 lowercase letter
- A minimum of 1 uppercase letter
- A minimum of 1 numeric
- A minimum of 8 characters in length
- You must not have used this password before

Password *

Confirm *

Password *

* indicates a required field

Figure 15 – Self-Activation Step 4: Entering a New Password

Once a valid password has been entered and also successfully confirmed by the associate, the system presents a final confirmation that all necessary information has been provided and the activation process has been completed successfully. The associate is given the choice of continuing to see a summary of their resources account information, or logging out of the self-activation process.

You are in: [University home](#) > **Identity Management** [Student Channel](#) [Staff Channel](#) [Channel search](#)

University of Salford
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

Logged in as: , AAA139 [LOGOUT](#) [HELP](#)

[Home](#) [Change Password](#) [Account Information](#) [Authentication Questions](#)

Thank you. You have now provided all the information necessary to activate your University of Salford IT resources.
When you press the 'Continue' button, you will be able to view important information about your account. This will complete the activation process.
After you have viewed your account information, you may:

- Find out which services are available to you via IdM self-service, by selecting 'Home'.
- Log out by clicking on the 'LOGOUT' button in the top right hand corner of the screen.


Once you have completed the activation process, you will be able to access the University of Salford network immediately. You will be able to access your other IT resources after an hour.

[Continue](#)

Figure 16 – Self-Activation Step 5: Confirmation of Successful Completion

In the event that associate chooses to continue, a range of important information about the resources they have access to, as well as their association with the University, is presented.

You are in: [University home](#) > **Identity Management**

 **University of Salford**
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

[Student Channel](#)
[Staff Channel](#)
[Channel search](#)

Logged in as: AAA1398

[Home](#) [Change Password](#) [Account Information](#) [Authentication Questions](#)

General Information about your Association with the University
Your association with the University of Salford is currently set up to run from **23/03/2007** to **23/03/2008**.

This means that, subject to abiding by the terms of the Acceptable Use Policy, you will be able to use the University of Salford IT resources provided to you within these dates.

Your University of Salford sponsor is **P. G. Wodehouse**. You should contact your sponsor if you wish to change the nature or dates of your association with the Unive

All usernames and passwords are for your personal use only and must be kept confidential.

Network Username
You should use your normal network username and password for logging in to email and most other services.

Email
Your email address is: B.Wooster@salford.ac.uk

Athens
The Athens username allows you to use many electronic information resources.

It is your network username with the prefix 'SAL'.

Figure 17 – Account Summary Information

Once the self-activation process has been successfully completed, a number of subsequent back-end processes will be triggered that change the state of their specific resource accounts from a “disabled” to an “active” state. Previously, account activation for key resources could take up to 24 hours or more whereas now activation for all resource accounts is typically processed after an hour.

Associate members can also utilize the same self-service web page to carry out a number of activities at any time including:

- Viewing their account summary information,
- Changing their password, or
- Reviewing or amending any of their security responses.

Password Reset via Identity Management Self-Service

Finally, this same self-service web page can be utilized by associate members to reset their password even in the event that they have forgotten their password. In this event, the associate is required to enter their University network username, prior to clicking the “Forgot Your Password?” button as indicated below.

You are in: [University home](#) > **Identity Management** [Student Channel](#) [Staff Channel](#) [Channel search](#)

University of Salford
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

[HELP](#)

Log In to Lighthouse
Welcome to the Sun Java™ System Identity Manager system. Enter your user ID and password, and then click **Login**. If you cannot remember your password, click **Forgot Your Password?**

Forgot Your Password?

User ID: AAA1398

Password: _____

Figure 18 – Forgot Your Password?

The system then displays a form requesting the associate member to enter responses to three, randomly-selected authorisation questions which were answered during self-activation.

If the answers supplied match the answers provided during self-activation, and the user presses the ‘Login’ button (as shown below, they will be presented with a subsequent form that allows them to enter and confirm a new password.

You are in: [University home](#) > **Identity Management** [Student Channel](#) [Staff Channel](#) [Channel search](#)

University of Salford
A Greater Manchester University

Identity Management
The right resources to the right people at the right time.

[LOGOUT](#)

Identify User
Please answer the following questions. Answers will be automatically converted to upper-case.
Account ID: AAA1398

What city or town were you born in: *****

What was the first name of your first best friend: *****

Who's the man?: *****

Figure 19 – Authentication

Summary

This paper has outlined how the principles of Identity Management have enabled the University of Salford to radically transform the way in which associate members are created, managed and administered.

In particular, the paper has demonstrated how Sun Microsystems' Identity Manager product (part of the Sun Identity Management suite) has been utilized and developed by the University to include the following:

- Significantly enhanced data accuracy and integrity relating to associate members,
- The modelling and enforcement of specific access policies and data requirements appropriate to each class of associate,
- Selective resource provisioning according to the needs of each associate class,
- Controlled, automatic de-provisioning upon account end dates,
- Controlled account self-activation and self-service processes and functionality, and
- Password Reset capability through self-service functionality.

The capabilities for associate member support now in place provide a stable foundation for all future development within the Identity Management programme. In addition, the associate members experience has been dramatically improved, and a range of **significant** opportunities for future marketing and potential revenue generation are anticipated as a result.

Work is now ongoing to further improve the organisation's capability for associate member support in the future through the following:

- Ongoing extension of provisioning targets to include Virtual Learning Environment (VLE) access, Library access, building and car park access.
- Provision of a bulk creation processes to enable several hundred accounts to be created at once for conference delegates, for example.
- Provision of delegated administration to enable individuals outside of Information Services to create and administer associate member accounts, without IS intervention.
- The extension of self-service functionality to enable associate members to request access to additional resources that they are not immediately provided with, with subsequent approval processes from sponsor and application representatives.