

## Identity Lifecycle Management for Higher Education

*Higher education's high user turnover and user complexity demands an efficient solution for generation, upkeep, and deprovisioning of identities within its IT infrastructure.*

The university environment places a number of unique challenges on its IT personnel; one of the largest demands on staff is the maintenance of a user list that can change by as much as 30% from year to year. This turnover rate is an aggregation of new students entering the system as freshman or by transfer, current students leaving the system because of graduation, transfer, or dropping out, and changes in faculty and staff. Adding to this high turnover ratio is the complexity of each user who can be identified as a student, an alumni, a member of staff, a volunteer, or in many cases a combination of these classifications. The upkeep of these identities represents an enormous expenditure of time and energy by the technology staff, and a source of frustration to users in the environment who are unable to access some of the resources that should be available. A complete, thorough, and efficient method of Identity Management (IDM) is now a requirement in the dynamic IT infrastructure of higher education.

Recently, the technology staff of a major research university in Kansas sought to implement a stable, commercial IDM architecture to replace their aging self developed system. They were suffering with maintenance problems inherent with many in house systems, primarily the issue was a lack of knowledge about the system among the administrators. This lack of support knowledge stems from the design process, where a member of staff will undertake the development of the architecture, most often with aid from some the university's computer science students. They are able to design a very custom solution to the problem at hand and then support it after it has been implemented; however, the problems begin as those students and staff involved with the creation of the software begin to leave after

graduating, or move to jobs away from the university system. Eventually the attrition of knowledgeable administrators will necessitate a change in the IDM architecture, the first decision that must be made is the sourcing of the new solution. The choice is between once again self sourcing the solution or bidding the project out for a commercial implementation. The in-house path has the advantage of low cost, being that you can pay some of the developers with class credit, but it has the inherent disadvantage of restarting the cycle that will inevitably end in a partially unsupported system that will once again require replacement.

Within the higher education community purchasing a commercial IT solution is often viewed as too expensive, especially when a "free" solution is available given enough time. While initial investment in a mainstream product is higher due to licensing and consultation fees; the long term advantages of productivity gains, ease of supportability, published upgrades, and low time commitment from the technology staff, ultimately make the off the shelf solution more budget friendly. The university came to the conclusion that it was in their best interest to seek an efficient, supported solution, to replace their current IDM system. Identity Automation won the bid for the project over many other major players in the IDM industry, and by selecting Identity Automation the university tapped into a fourth benefit in the replacement of their old system, a rapid and organized implementation schedule.

The IT system structure at the public university was more complicated than most, but had the advantage of previous IDM integration, their student ID served as a common attribute in all identities campus wide.

## Identity Lifecycle Management for Higher Education

They had no less than seven authoritative sources including three HRM pools, orientation systems for students and newly hired employees, campus housing, and their ID card control suite, each of these systems could serve as a first point of entrance for identities on the network. Users could then be granted downstream access to a number of applications including, Active Directory and Exchange, eDirectory, and a host of network accessible software suites bound by a SUN Directory Server implementation. The total integration spanned software from more than ten vendors, and in the final implementation all were to be controlled from a single point source.

Adding to the complexity of the implementation was the fact that each user could be classified as a student (both credited and non-credited continuing education students), an employee, an alumni, or a university volunteer. In many cases the user was a combination of the previous classifications, which required that a classification priority list be created to ensure that each person was granted rights to the correct resources on the network. All of these factors together influenced the IT directors to create a time line spanning 15 months from award of the project through completion of work. This time frame was affirmed by most vendors as they stated that it would take at the very minimum 12 months to complete the scope of work. Identity Automation, the chosen consultant, was the exception to the one year rule; their statement of work initially required only four months from the signing date to the estimated date of delivery.

Though excited by the prospect of getting a system deployed one full school year earlier than first thought, Identity Automation's time was not without its skeptics. "The advertised time line was preferable, however, we were taking any estimate with a grain of salt because there were so many unknowns", states the IT Systems

Development Manager at the University.

The disparity in completion time between Identity Automation and every other vendor on the market is due to Identity Automation's development and adoption of a solution they have aptly named, RAPiDiDENTiTY. RAPiDiDENTiTY is a Rapid Deployment Methodology, which dramatically reduces implementation time by developing configurable drivers that interface with a majority of the most common software applications that organizations look to integrate. By utilizing prebuilt logic Identity Automation is able to reduce the assessment, development, and testing phases substantially and thus concentrate on the systems that do not already have a baseline configuration profile. In the case of the state university both directory services platforms and a number of hosted applications already had configuration profiles. In addition RAPiDiDENTiTY's support for text file exchanges, allowed for an immediate connection to some of the university's HRM systems.

Identity Automation's ability to bypass the standard process of assessing each system individually, allows their system architects to focus on the systems that require custom connection solutions much earlier in the project cycle. This in turn accelerates each step, from testing and training, to implementation, and most importantly the go-live, after which benefits can be realized. Identity Automation completed the design of the solution in four short months. The testing, training, and deployment of the solution filled the last two months of the time line.

Just because the solution was rapidly designed and deployed, does not mean that it was incomplete in scope or thoroughness. Identity Automation implemented a primary data warehouse that served as a single point depository for all information related to a user and bound to their student ID, this facilitated an automatic

## Identity Lifecycle Management for Higher Education

updating of information across the authoritative systems. This allows for a large reduction in the number of processes required to update users, for example, if an address of a student is changed in the student information system (SIS), and that student happens to also work for the university, the address change will be automatically migrated into the HRMS. This centralization also allowed for automatic provisioning of users in the system, and because a priority list was developed the user would have access according to their highest group membership. If that status changed, the provisioning will now automatically follow suit, to demonstrate, if a student who also works for the university quits their job, their access to employee applications would cease as soon as the employment status was changed.

In addition, the technology staff at the university leveraged Identity Automation's involvement to institute best practice solutions in user security. The help desk staff was constantly tasked to aid users in resetting passwords for the various systems at the university, each which had its own password requirements. Some systems did not meet the university's minimum security standards and could not be altered because the maximum requirements were hard-coded into the software. The metadirectory synchronized all of a users passwords to a single sign-on, and because the password was generated at the top of the system, the requirements could be set at the metadirectory and those secure passwords would be passed on to the connected systems, guaranteeing that all user authentications met security standards. In addition an automatic password reset feature was deployed allowing students and staff to reset their forgotten password by answering security questions that were included in the user profile at the time of registration.

Although the implementation is new and requires students, staff, and faculty to adjust to the new way of do-

ing things, the IT staff is already reaping benefits. The staff has seen a 90% reduction in the number of users that require manual touch points to complete their provisioning. A rapid deprovisioning of a user in the case of a security breach, or immediate employment termination, can now be accomplished in minutes with only a few keystrokes. For the overwhelming majority of users who are successfully provisioned automatically, the wait time for fully functional access to the university's computer system has been reduced from 3-5 days to less than 10 minutes. Most importantly all of the above benefits plus many others began making an impact many months ahead of schedule thanks to a RAPIDiDENTITY implementation.

An efficient, supported, Identity Management system is a huge asset for most organizations, but this is especially true in the field of higher education. The turnover and complexity of users within the system can place a huge amount of work on staff dedicated to making sure that the information technology resources run smoothly. An effective IDM implementation greatly reduces the need for upkeep and manual corrections, allowing the technology staff to spend their time looking forward, rather than maintaining the present.

