Oracle Identity Management: Making the Most of Your HR Data

Jennifer McGurk
Douglas County School District

Niklas Iveslatt
Arisant, LLC

Douglas County School District, south of Denver, Colorado, recently completed a successful implementation of Oracle's Identity Management Suite. The district operates a plethora of custom and third party applications. It undertook a very thorough ROI analysis before making the decision to invest in this technology. The Oracle product was selected because of how it integrates with the Oracle E-Business Suite, which is the triggering source of record for all staff identities.

Douglas County has changed from a primarily rural county to a suburban population. Although the district has only 52,000 students it is one of the fastest growing districts in the county. The growth, coupled with the inherit characteristics of a school district population; have resulted in account maintenance consuming a large part of the day for IT support staff. The county population as a whole has grown by 33% in the last five years, yet the student population has grown by 44% reflecting a younger more urban household. The number of employees has grown by 42%. Projections for the next 20 years indicate this trend will continue.

Every school district faces a concentrated hiring season that coincides with the beginning of the school year, a re-occurring shift of employees and students between physical locations over the summer, and a high number of part-time employees who share jobs. The user population is physically dispersed across approximately 80 locations, with inconsistent security and access policies.

The growth in technology solutions also manifests itself in K-12 education. There are a large number of third party COTS applications. The number of enterprise applications operated by the district has grown from 12 five years ago, to 25, with another 5 projected to come on-line during the next school year. In addition, the district strategic plan for IT initiatives includes systems that have not yet been defined, such as a Learning Management System, a comprehensive data warehouse and BI solution, and on-line education opportunities for all students. As a public sector entity that is ultimately accountable to the taxpayers, hiring additional support staff to do more of the same in terms of managing applications is not an efficient use of resources.

Account Management: The Way It Used to Be - Historically, the responsibility for account maintenance was decentralized. Depending on the application, accounts could be managed by central IT staff, local IT staff, computer resource teachers, or even by super users in some departments. This of course led to problems such as users having multiple accounts, ex-users still having active accounts, manual processes to revoke access when users moved between jobs, users with access to systems they no longer needed, etc. This was a costly process in terms of labor hours spent maintaining accounts, and the risk of liability.

The school district recently implemented a centralized Student Information System (SIS) that enabled us to start putting controls in place. This system contains student grades, health information and address information which is all data that the district is required to protected under FERPA. The new system is centralized, which also opened the door to broader liability because a rogue user had access to more data. An incident in another school district of an unauthorized employee gaining access to the SIS made us realize Douglas County School District was at risk as well.

With each system being managed independently, and each user having a unique login for each system, the number of systems being bought on-line, the first step in completing a cost-benefit analysis was to quantity this effort. The details were staggering. On average, every employee has accounts in seven different systems: network, e-mail,

voicemail, help desk, employee badge system, and a call-in system used to substitutes. Most employees also have at least one other application, either the SIS, time keeping system or a departmental specific system. The IT plan for the district included implementing 4 new systems by the end of the school year, all of which required individual user accounts. In addition, every student has accounts in 2 systems. Every student has a network acct and this year the district is implementing a centralized library system.

Implementation Timeline - The Information and Technology Services (ITS) department first started looking for an automated solution in October 2006. At that time Oracle had just released its Identity Management Suite. Although there are other products on the market, the appeal of the Oracle toolset was its integration with Oracle E-Business Suite, and the flexibility of reading any type of data source. In the spring of 2007, the district worked closely with Oracle to complete a return on investment (ROI) and a proof-of-concept (POC). The purpose of the POC was to validate that the toolset would work with the disparate applications that the district has in place today, including:

- Oracle E-Business (*source system* for employee information)
- Infinite Campus (SQL Server based *source system* for student information)
- Active Directory (*target system*)
- First Class (*target system* that is 3rd party proprietary email)
- Oracle Portal (*target system* for location and role-specfic content)

It took about 4 weeks to complete, and concluded with a live demo showing that students could be moved between schools in Active Directory as a result of an enrollment change, and that system privileges were granted / revoked to employees as a result of job changes.

The Numbers Justified the Project - The analysis for the ROI began with determining the number of triggering events that occurred during a given year. A triggering event is a change to a source record that will affect the target systems to which a user has access, or affect the configuration of their account in a target system. The standard username for the district is first_initial concatenated with middle_initial concatenated with last_name. Queries were run against Oracle E-Business to determine the number of employees that were new to the district, then number of employees who terminated, and the number of employees who changed jobs, changed schools, or changed their names. Similar queries were run against Infinite Campus to determine the number of new students including kindergarten registration or transfer, and the number of kids that left the district either through graduation or transfer.

	New	Separated	Changed	Total Number of Changes	Total Number Of Users	% of Total
Employees	1147	629	2277	4053	6502	62%
Students	9200	3703	11234	24,137	52,245	46%

Number Of Annual Triggering Events By User Type

The table above indicates that of the 6502 users that are employees, 4053 or 62% required some sort of manipulation to one or more of their accounts. If the employee was of the type that had seven or more accounts, the amount of time to correct the roles and access to proportionately longer and may have required more than one support person to affect the change. Of the 52,245 users that were students, 46% of them required manipulation. Although some of the pieces are automated, there was no standardized process for collecting, passing or making consistent information available to all the necessary support staff. For example, in order to get the appropriate access for a new programmer, a minimum of five help desk tickets had to be entered: the badge, the network, email, Oracle database access, a phone and voicemail. Communicating account names to the new employee was a problem as well.

The next step of the ROI was to look at the number of accounts that were managed across the enterprise. Each system was looked at and the number of active accounts was documented, along with the official name of the

positions for the users. We found that a total of 123, 772 accounts were being maintained and accessed across the 25 enterprise applications. However this is projected to increase to 222,739 by the end of next year. This is partial due to the implementation of a new Library Automation System for all students, and new on-line systems for insurance enrollment, employee appraisals and print shop job requests that all employees will have access to. Additionally there will be growth in the number of users accessing current applications if the accounts were provisioned automatically.

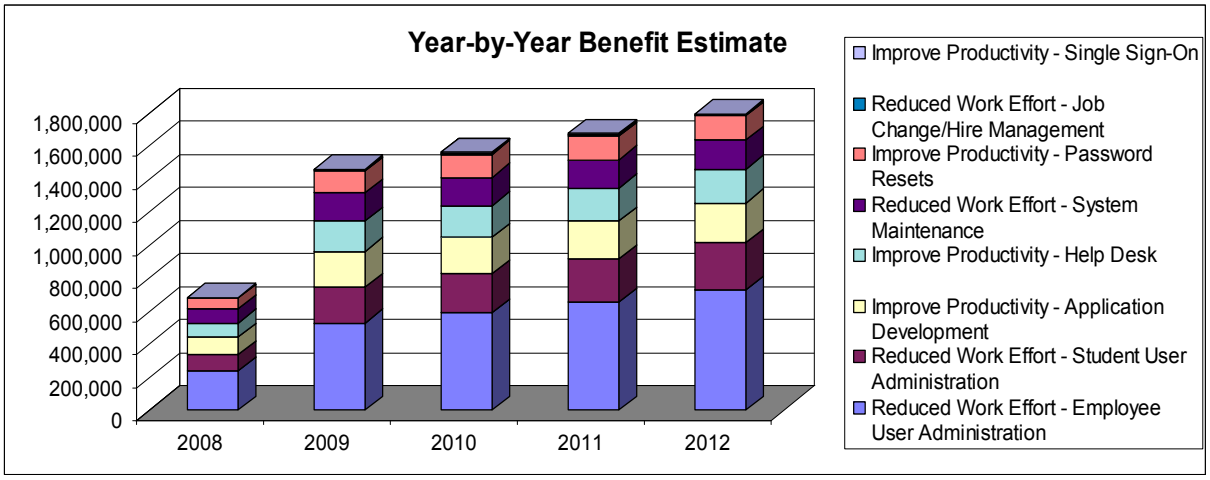
The types of people that perform the support tasks were reviewed and fully-loaded average salaries were documented. Then average amount of time to complete each type of task was documented, so that cost of doing business under the current methodology could be documented. This allowed is to compute a dollar value to represent the value of the support staff that could be repurposed into performing other tasks.
For example, the Application Support Team is responsible for training, testing and support. However they were spending a disproportionate about of time on account maintenance, limiting the amount of training they were able to provide. Each school is staffed with instructional and technical Computer Resource Teachers. This group of support staff was spending their time maintaining accounts rather than instructing or addressing the forward looking technology tasks for their location.

Benefits were categorized by type so that they could be valued. The district growth factor was applied and a 5-year benefit was computed. The assumption was made that during the first year (2008), only half the accounts that could be provisioned would be brought under Identity Management.

Employee User Administration	• Reduced time, effort, cost to administer user accounts • Improved level of service to end-users • Users have correct access to systems they need
Student User Administration	• Reduced time, effort, cost to administer user accounts • Improved transition when students change schools
Self-Service Password Reset	• Reduced help desk costs • Ability to focus on higher value assignments • Better system security – fewer passwords
Help Desk Productivity	• Reduced help desk costs • Improved level of service to end-users • Ability to focus on higher value assignments
Application Development	• Improved responsiveness to the district • Reduced system development costs • Security governance and consistency
Application Maintenance	• Reduced costs to maintain existing systems • Focus staff on new capabilities for the district

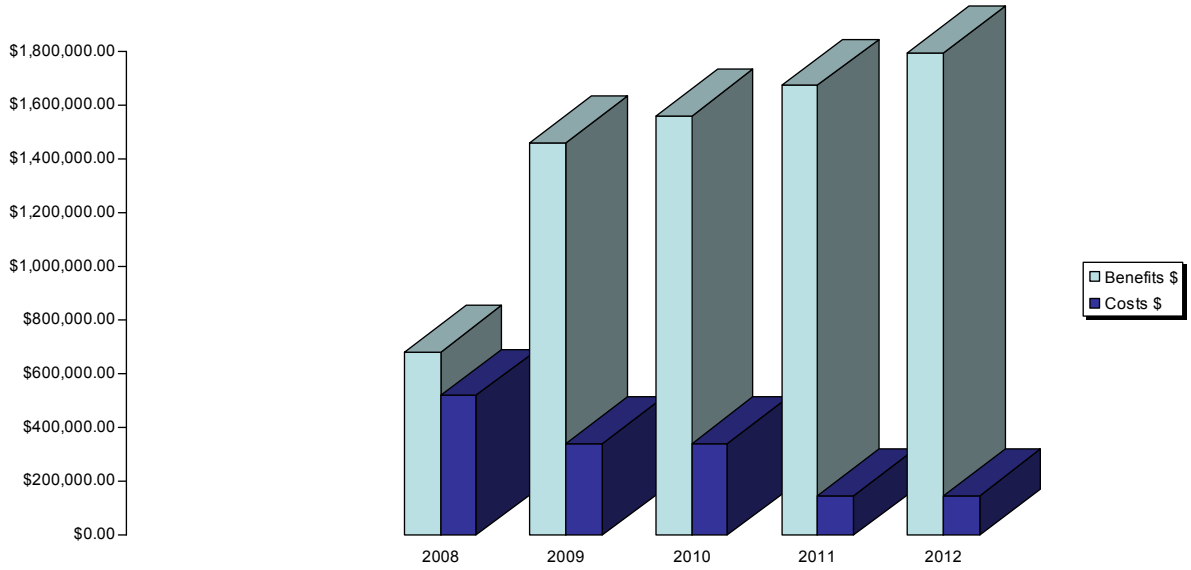
Benefits quantified for ROI Analysis

There are also intangible benefits that became apparent after the system went live. Account maintenance is a high-priority task when a user cannot get access. It is also tedious and boring, and no one wants to do it. Users were ecstatic about reducing their number of passwords. Implementing Identity Management has caused users to identify other systems that are in operation that were unknown to ITS.



Five-year Benefit Savings in Dollars by Year and Type

Costs were computed based on the number of users licenses required. The Suite is licensed by user, and there are differing prices for internal users and external users. Funds were added for implementation support and for annual Oracle support costs. The district chose to spread the purchase cost over three years, hence the drop in costs in year 4 and 5.



Cost-Benefit Comparison over Five-year Period

The decision to purchase and implement was based on the successful demonstration of the product within the current district infrastructure given the current district run applications.

Process Changes - Like the implementation of any other automated system the legwork to identify and document current processes was a manual process. At DCSD this meant looking at the internals of every potential target application. This was done after the technical viability of the tools had been proven. For each one, we identified the existing users and what positions they held. Then the lists were confirmed with the Business Owners to validate that the existing users *should* have access or if the accounts should be disabled, what other positions *could* have access and how they were currently doing their account maintenance. What we found across the board was that when users were given accounts, the administrators set them up "just like Joe", regardless of whether "Joe" was set up correctly or not.

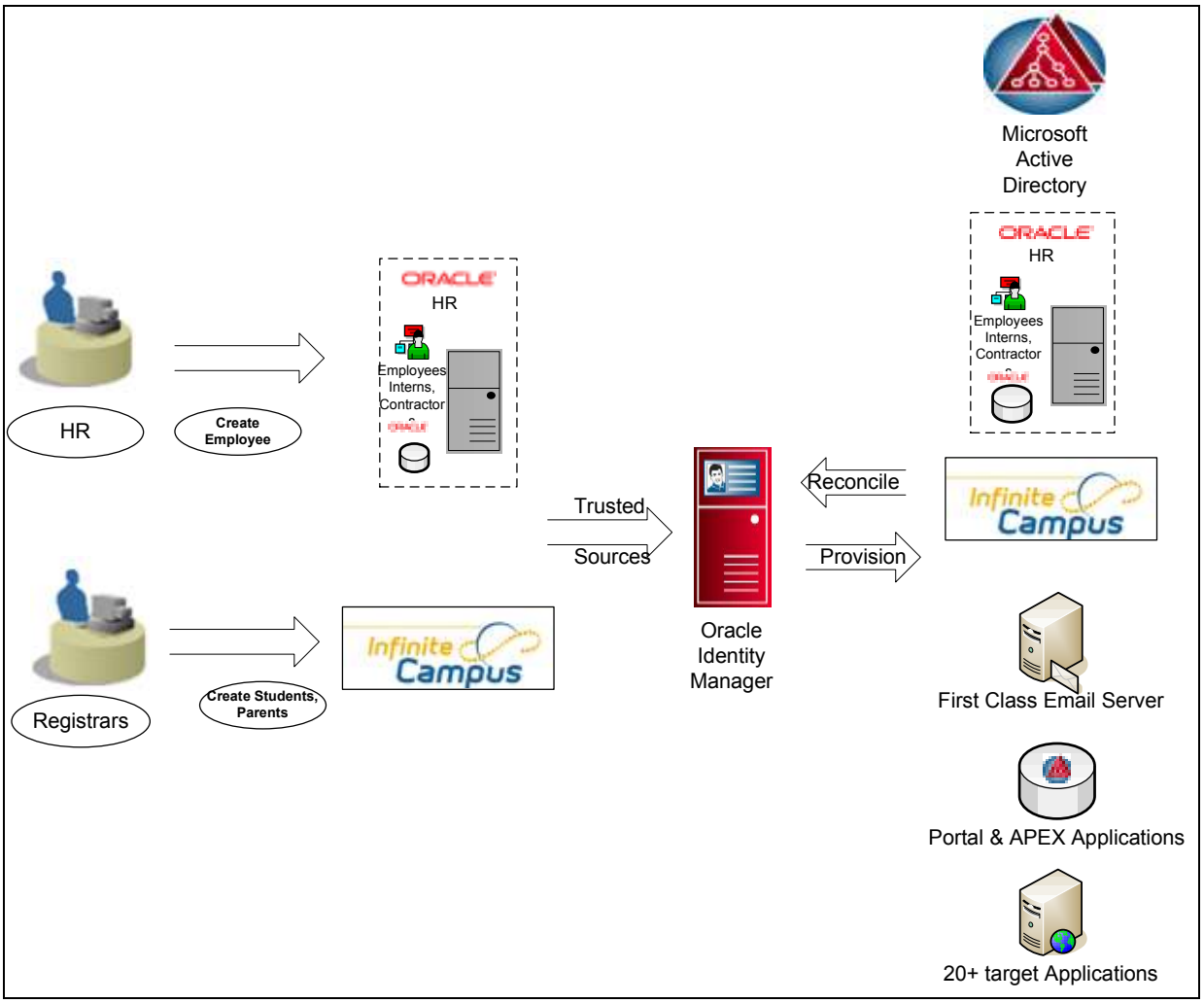
The impact on the organizations within the district did not go unnoticed. As we reviewed the data and talked to managers in the field it became clear that the account management was much more splintered than we thought. There were many new employees that waited weeks to get access to the systems they needed to do their jobs. This led to employees sharing accounts and passwords. This puts the district in a libelous position with regards to our regulatory requirements to protect student and financial data from un-necessary exposure.

The characteristics of the password policies in each target system were identified. Some systems already required strong passwords and other systems didn't ever require a password change. Microsoft Active Directory is used for both employees and students, and thus the district had a single password policy that applied to kindergarteners and teachers alike. A working group was established made up of the application owners for the target applications. As a group they came to consensus and defined a district-wide password policy to apply across all information systems. This included defining minimum length, character mix, and expiration policy. This was then approved by the computer resources teachers in the district.

There was no process to disseminate usernames and email address information to new users. Along with formally defining standards for user names, an automated workflow was defined for distributing account information. A procedure was written that identified the physical location for the new employee, identified the employee that holds the secretary job at the location, and then sends the secretary an email.

A unique business process in any school district is that teachers work under an annual contract. This affects how employees are entered into the HRMS system. All teachers have a contract start date of August 1 and an effective start date of August 1st. DCSD operates about half of its elementary schools on a year-round calendar, which means that many teachers start working in July but may not be entered into the HR system until August. Initially we tried to trigger provisioning from the effective dates on the assignments, but user testing revealed that ideally the teachers would be set up in the SIS prior to the start of the school year so that the students could be rostered into their classes. Two date fields were added to the assignment records to capture the date the user needed access to district systems and the date that access should be revoked. This was important because it separated the access dates from the dates used for payroll purposes.

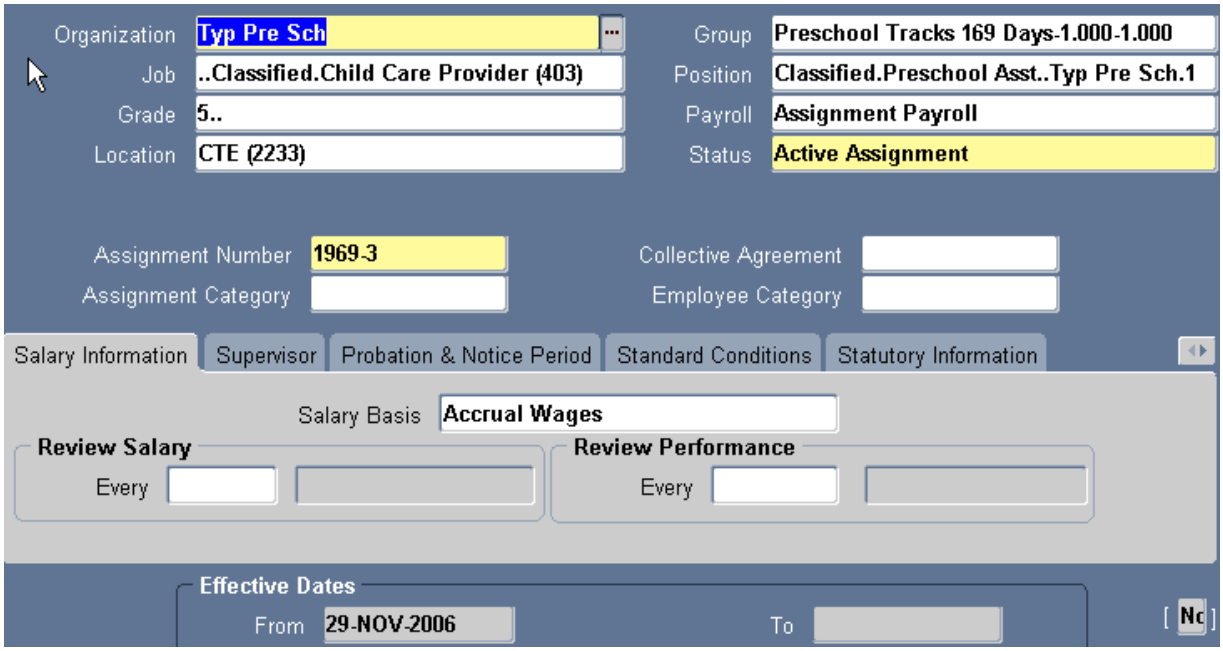
The architecture for the DCSD implementation is shown below. There are two source systems: E-Business for employees and Infinite Campus for students. Regardless of user type, we wanted them to be provisioned through the same process. The goals for the first phase were to 1) put the infrastructure in place for future growth, 2) define the standard process rules, 3) provision and control access for the heavily used systems including Active Directory, email, Infinite Campus, Oracle Portal, and 4) create connectors for an Oracle system, a proprietary system, a SQL Server system, a custom APEX application, and a position-specific content system. These connectors will then be used as examples for building connectors to additional systems.



DCSD Identity Management Architecture

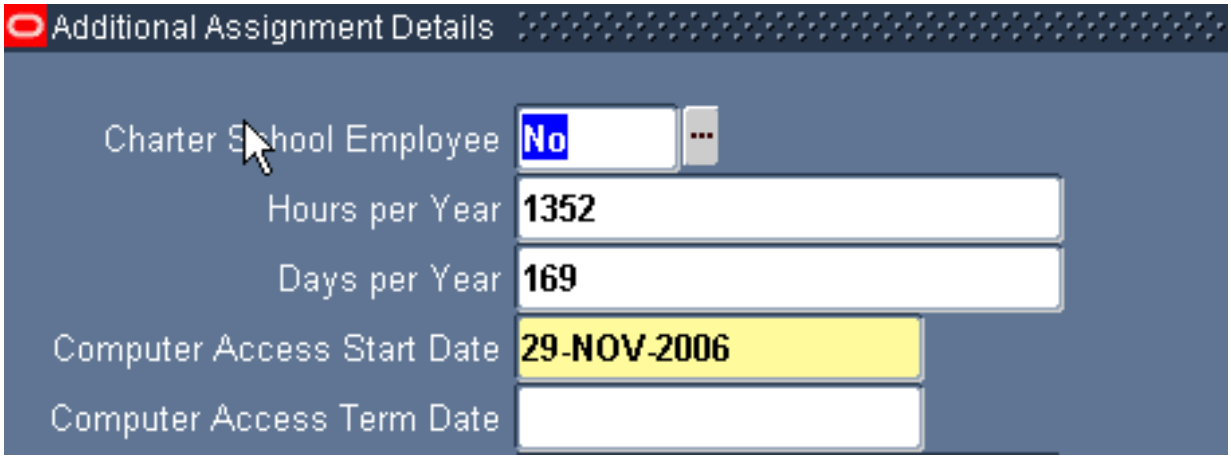
The Relationship to Oracle E-Business – The HR module in Oracle E-Business is the single source of truth for all employee related data. The HR department is the first to see new positions, new hire paperwork, start dates, and job descriptions. From the technical perspective, a triggering event correlates to a new or changed Person or Assignment record. When a new Person record is entered and saved, it triggers off the custom.pll that is standard functionality contained in the PERWSHRG.fmb. Additional PL/SQL code was added to search across all target applications and identify the next unique UserID that meets the standard naming convention. This value is stored in the Person record, and is the value that will be provisioned into the target systems. The email address is also stored in E-Business. When a name change occurs, the same procedure is executed which generates a new userID for the employee with their new last name.

Each target system was analyzed (regardless of phase) and the elements that identified the personnel that have currently have access were identified. It was quickly determined that the identifying elements were Position Name and Location. These are stored in the Assignment record. Any given employee can have more than one assignment, leading us to trigger the account access/cutoff from the Assignment effective dates rather than the Person effective dates. Common systems for all employees such as e-mail and network access could be triggered from the Person record dates, but one of the strategic directives for the district is to provide department/school specific portal content. E.g., if an employee moves from a position in the Benefits department to a position in a school, their default portal content should change as well as the systems to which they have access.



Standard Assignment Screen from E-Business

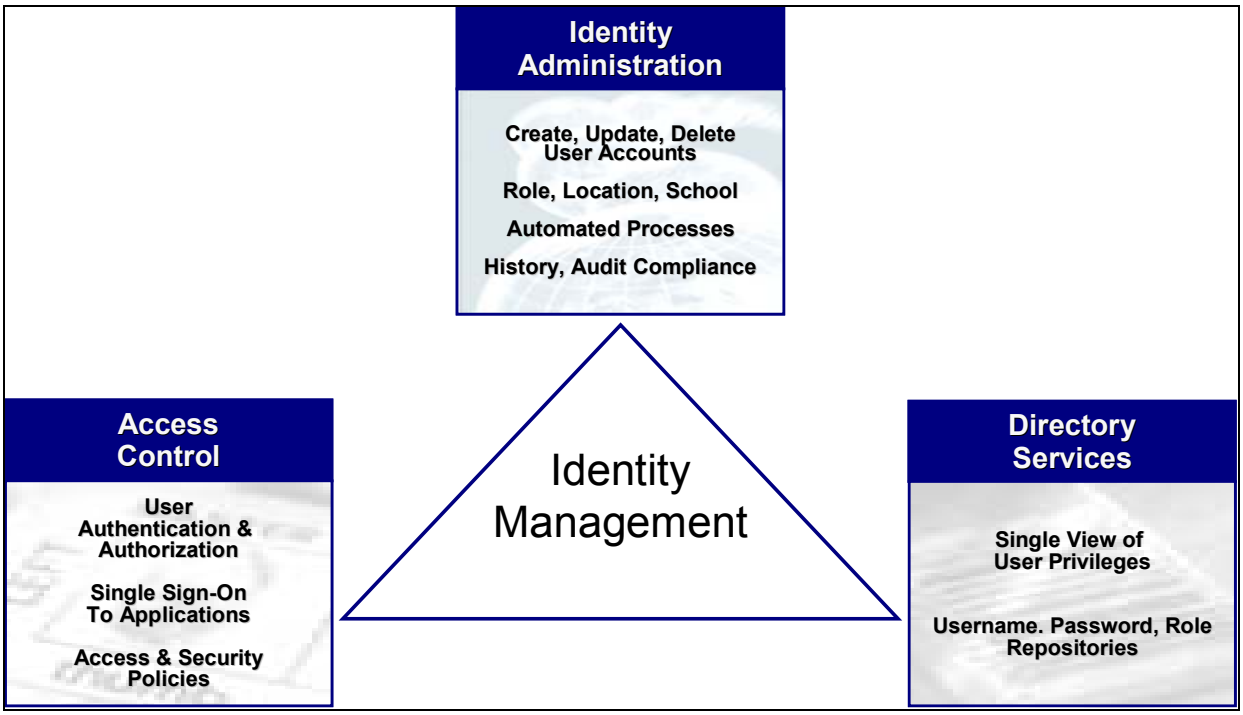
At first we tried to drive the provisioning connector off the effective dates on the Person and Assignment. This worked well for the standard personnel transaction, but resulted in inconsistent when entering back- and future-dated transactions because the effective dates are designed to be used by the Payroll module. This led us to normalize our data base design and create two new flex fields that are used for the sole purpose of provisioning.



New Flex Fields on Assignment Screen in E-Business

What is Identity Management? - Identity Management is the keystone for Oracle Fusion. Through recent acquisitions, Oracle now has a dozen or more tools that are all designed to protect data, identity, and ease the transition from application to application, whether internal to an organization or external. It is the glue that holds everything together. It gives us the ability to standardize the systems that any given user has access to, based upon the job that they are in.

The DCSD solution for Identity Management is comprised of three pieces: Identity Administration, Access Control, and Directory Services. This is like a three-legged stool; it cannot stand without all three legs. Each piece is described in detail below.



Identity Management Implementation Model

Identity Administration - The main function of Identity Administration is to provision user accounts from trusted data sources. *Provisioning* is the process of creating, deleting or changing a users' account. Roles are defined based on the attributes that are available in the source data. At DCSD, these roles are based on the positions the employee occupies and the physical locations where the employee works. DCSD also uses it to enable password synchronization by creating target accounts with synchronous passwords to start with. The audit portion of this leg is the standardization of systems based on position name and the automated creation of those accounts.

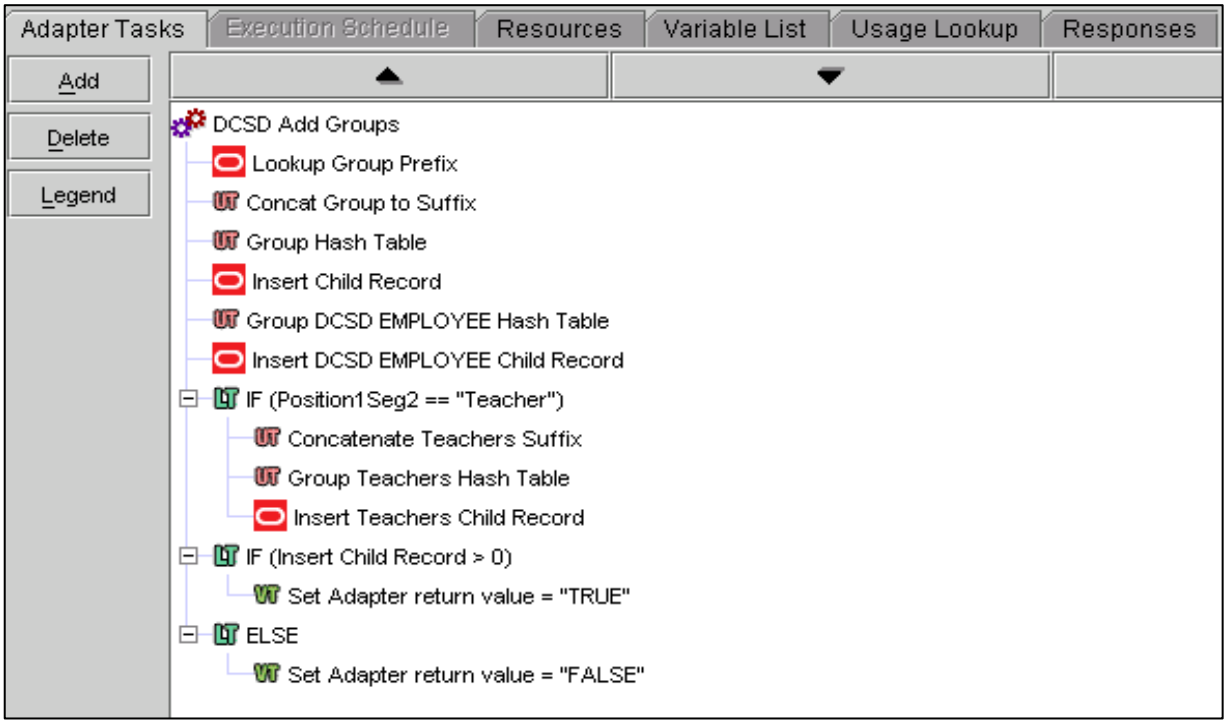
Access Control - Access Control is the process of identifying who a user is (by a unique username), authenticating them (by a password), and then granting access or admission to target systems based on the roles that they have. Access also includes the concept of Single Sign-on (SSO). Once a user has logged in, they can access all other systems that are SSO enabled without having to log in again. Not all applications can be configured for SSO. It is particularly challenging for third-party hosted applications.

Directory Services - Directory Services enables multiple source systems to be integrated into a single view, much like a view in a database. These sources can be anything: Oracle databases, SQL Server databases, flat files, etc. However, one system must be defined as the primary. This is key functionality for the school district because it provides a single view of employee user data and student user data.

The Oracle Identity Management Products - The DCSD solution for Identity Management is shown below and is built as a long-term solution. Oracle Identity Manager (OIM), Oracle Access Manager (OAM) and Oracle Virtual Directory (OVD) were implemented. The goal for the district is to manage both employees and students through a single architecture. As the district expands its on-line learning environment, the need for secure student accounts expands as well. Education options now or in the near future will include on-line courses, electronic portfolio management, assessment and learning management.

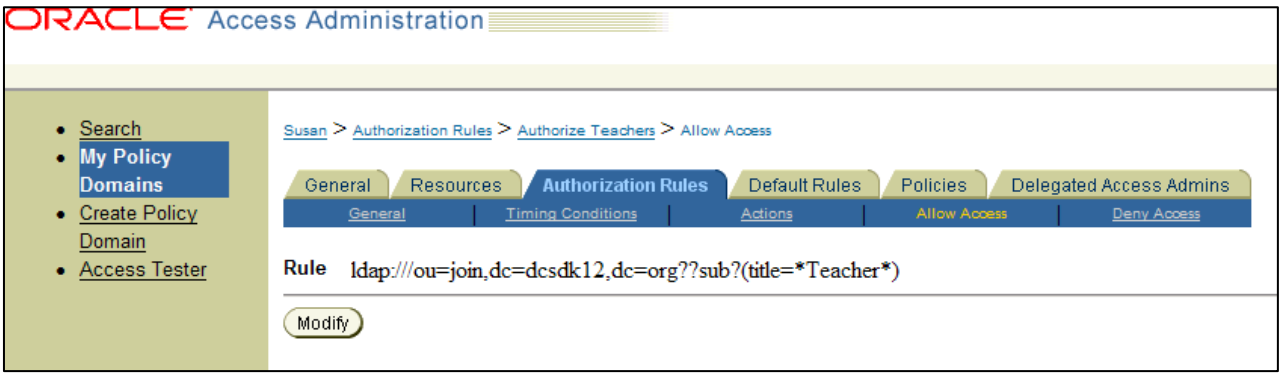
Oracle Identity Manager (OIM) is the product that the district uses to manage employee accounts. There are many, many pre-build connectors, and the list is growing. It includes Oracle E-Business Suite, IBM Lotus Notes, Microsoft Exchange, Novell Groupwise, Database Application Table, Database Application User, Microsoft Active Directory, Novell eDirectory, Oracle Internet Directory, Sun Java System Directory Server, JD Edwards,

Oracle Retail, Peoplsoft, SAP Enterprise Applications, SAP Enterprise Portal, Siebel Enterprise Applications, BMC Remedy, IBM OS400, UNIX, Microsoft Windows, CA ACF2 Advanced, CA Top Secret Advanced, IBM RACF, RSA Authentication Manager, RSA Clear Trust, etc. Although there is a pre-built connector for E-Business Suite we were not able to use it because it only works with a flat 1:1 relationship between the person record and the assignment record. The same issue exists with the Oracle database connector; it is designed to connect to a single table only. OIM also comes with a Custom Connector Factory, which is a GUI tool to build custom connectors. This is the tool that we used to build both provisioning and reconciliation connectors to E-Business. It can be used to manage any resource or asset. For example, it could be used to provision cell phones for new employees as well.



Oracle Identity Manager Provisioning Engine

Oracle Access Manager (OAM) is the tool that applies a Unified Password Policy across applications. It is used to configure policies for lockouts, forced password changes, password complexity and password history rules. The Rules engine in the product authenticates the user, and based on the rules, allows them into the system or not. It also has built in features for self-service password reset. The single-sign-on feature has to be configured for each application. We decided on a fairly limited implementation because of the number of employees who share computers. OAM also includes a built-in White Pages Search which is similar to a white pages phone book. It is configurable to operate against any data source.



Oracle Virtual Directory (OVD) makes any data source look like a LDAP Directory and is used to consolidate user identity data from multiple sources. This includes databases (Oracle, SQL/Server, etc.) or flat files. It is a system integrators best friend because it can modify attributes in transit, much like an Oracle view in the database. Additionally it caches this data for improved performance. It is easy to install and setup, can get more complex depending on feature usage.

Lessons Learned - The major lesson learned from this project was that is as much a business process improvement project as a technical project, and appropriate focus on process change and data should be given. The DCSD IT environment had evolved over a period of 10+ years and thus there were many inconsistencies and manual process that were not evident when the project started existed. A considerable amount of effort was spent on data cleanup and also on figuring out exactly how a user was provisioned into a specific target system. Implementation by IT from solely a technical perspective will not be successful.

Some other lessons learned include:

1. Get HR involved!
   After an IdM implementation, HR will be leading the provisioning tasks. No longer, will IT staff manually provision and tweak account data. It is now very important that HR enters the correct data. Otherwise users might be de-provisioned or be given the wrong system access.
2. Know your systems!
   In order to control access into the different systems, it is important to understand how access is granted today. In many cases it was inconsistent and it is worth taking the time to standardize and get buy in from the Business Owner.
3. There will be process changes!
   Shifting from manual provisioning to automatic means the users will have to be re-trained to not do manual tweaks anymore. If they continue doing this, the value of the overall solution is greatly diminished.
4. Create table driven roles and system access!
   In order to be able to hand-over the definition of rules and roles to other teams, consider creating a simple to use application that can be used by a novice user. This way, rules and roles can be updated by functional staff and then published into identity management when it is ready.
5. Create table driven roles and system access!
   If the number of roles exceeds 50 or so, consider putting the decision making data into a table. The benefit is that it is easily accessible for verifying the provisioning rules, and the Roles in OIM can be coded to read the tables. This makes it easy to add new decision making criteria.
6. Be careful and meticulous about reconciling!
   There is no conversion in the traditional sense, but user IDs must be reconciled across all of the target systems. Failure to do this will result in the creation of duplicate additional accounts where there is missing key information, or misspelled information. This was much more time-consuming than anticipated. Some of this was automated by means of PL/SQL procedures that compared user IDs.

