Oracle Identity Management: Making the Most of your Oracle HR Data

Jenny McGurk – Douglas County School District
Niklas Iveslatt – Arisant, LLC

April 15, 2008

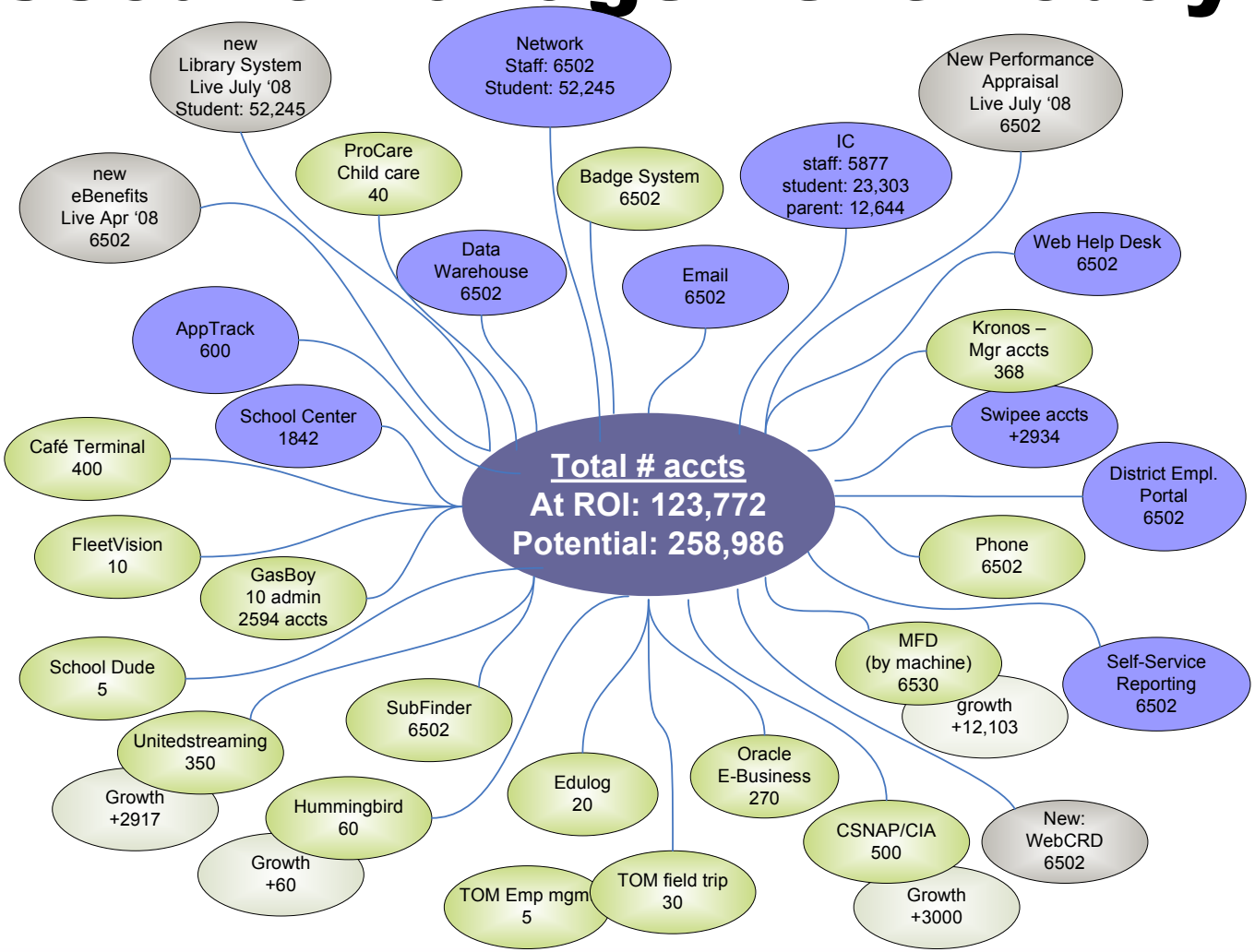
Overview

- Why is Identity Management important?
  - Immediate and long-term problems
  - Business case
- What is Identity Management (IdM)?
- How does it integrate to Oracle HR?
- What lessons did we learn?

"Work smarter, not faster"

- How did we get here?
  - Limited support staff
  - Physically dispersed
  - High turnover
  - Staff shuffle in August
  - Multiple systems
  - New systems
  - Growth: new schools and department re-orgs

Account Management Today

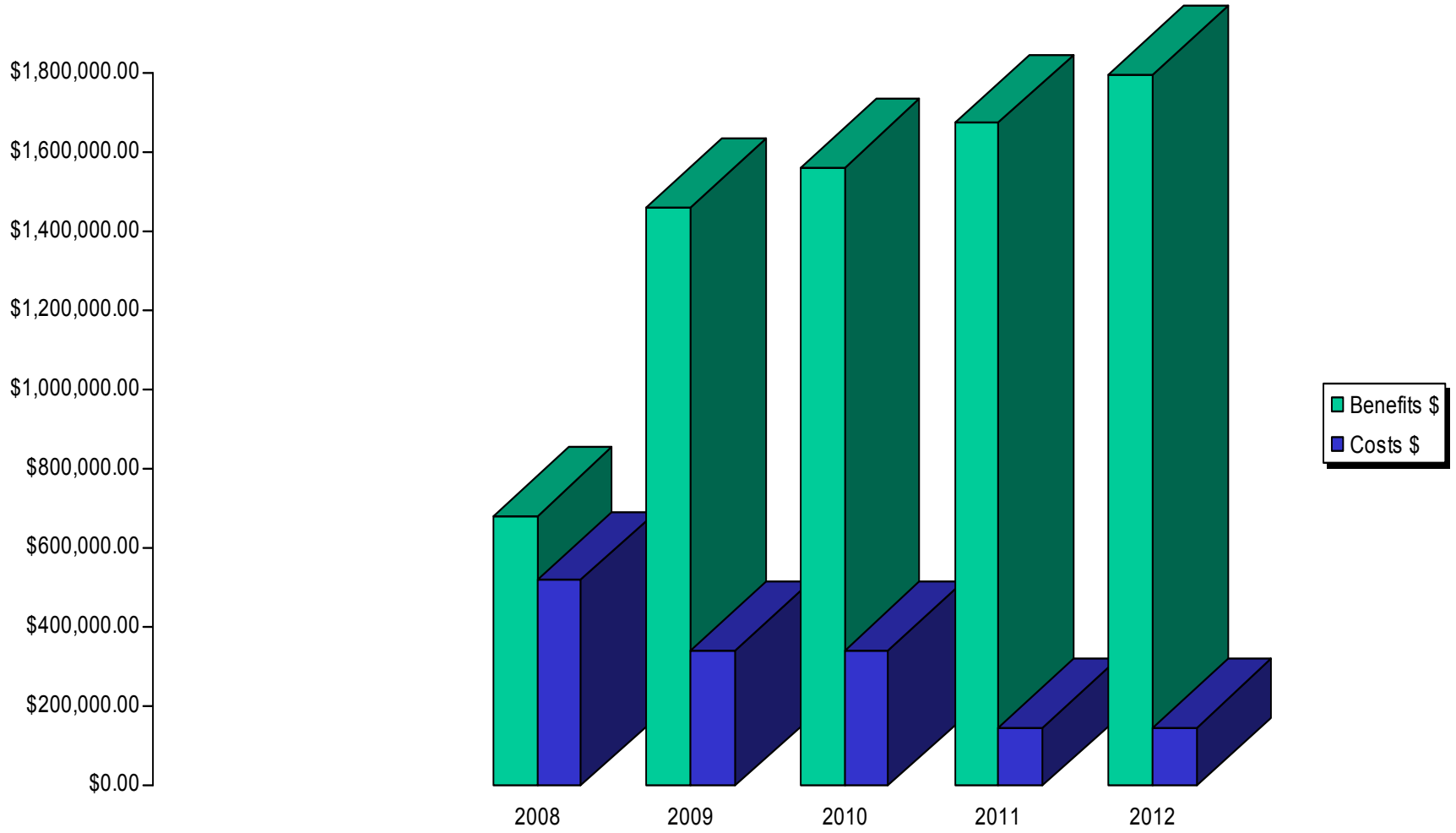


Annual Triggering Events

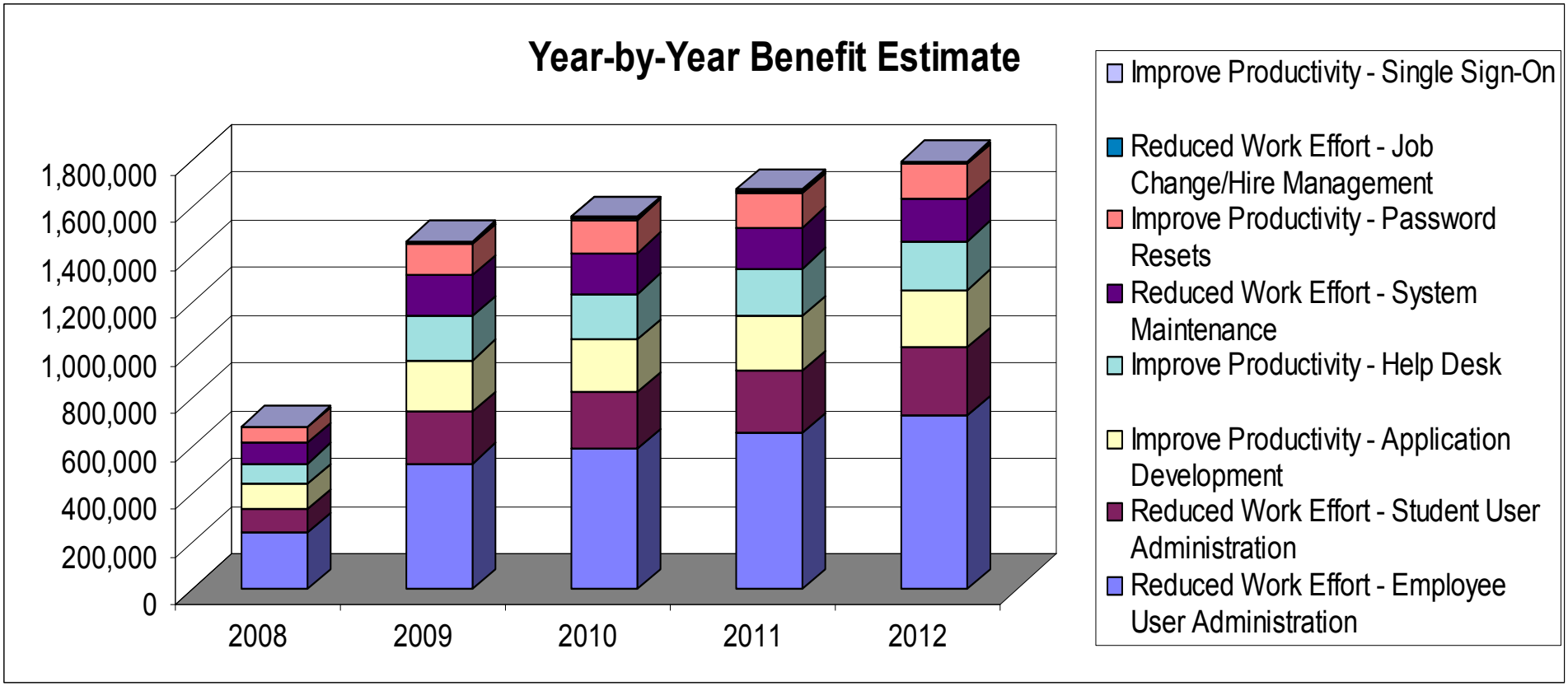
	New	Separated	Changed	Total Changes	Total People	% of Total
Students	9200	3703	11234	24,137	52,245	46%
Employees	1147	629	2277	4053	6502	62%

- Employee accounts: average 7 per employee
  - Current: network, e-mail, voicemail, help desk, badge, SubFinder
  - This year: portal, eBenefits, Reporting Services, Balanced Scorecard
  - Employees also use at least one other application: Kronos, IC, AppTrack, etc.
- Student accounts
  - Every student has an network acct
  - Change in school requires re-provisioning of network account

Return on Investment



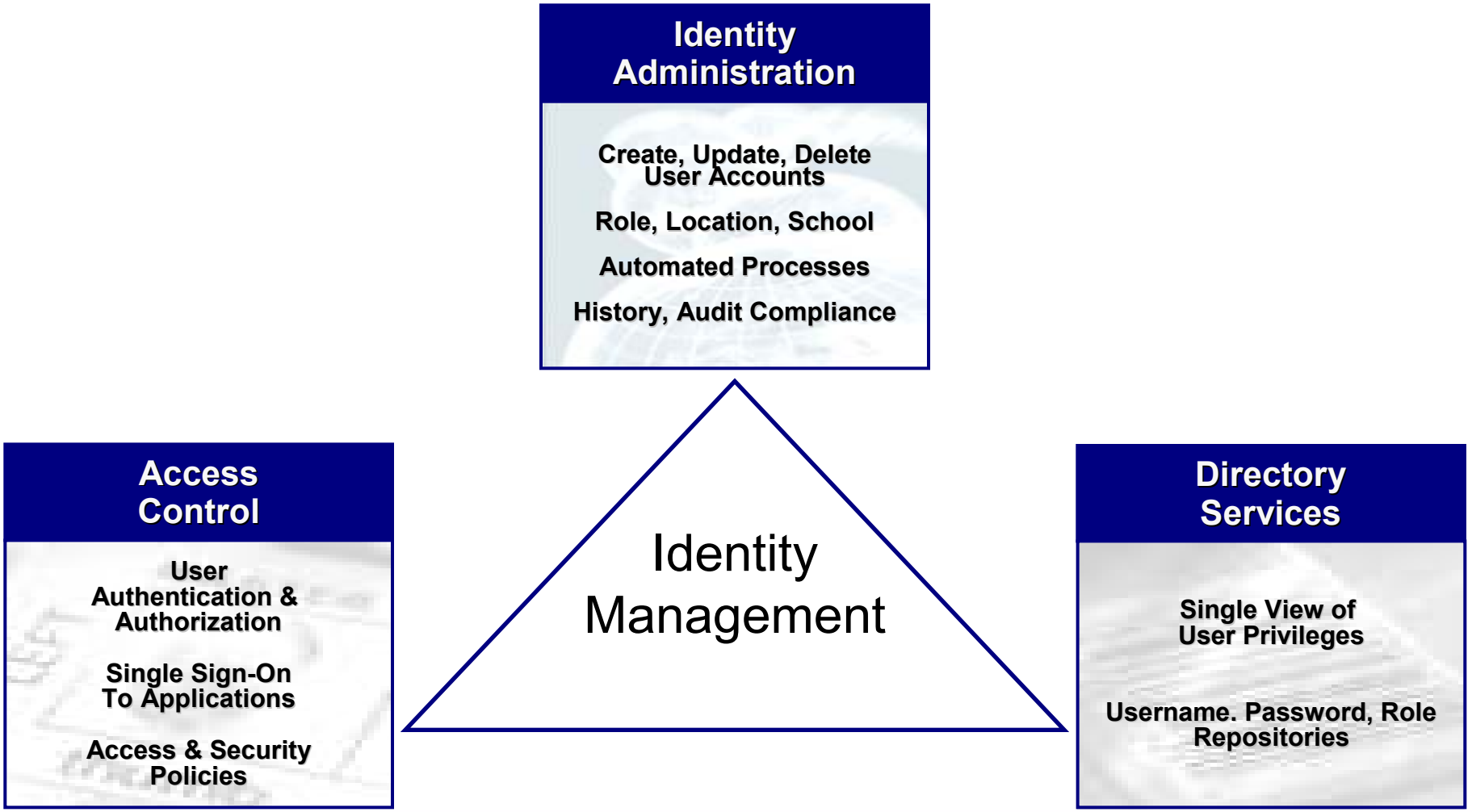
Breakdown of Benefits



Measurable Benefits

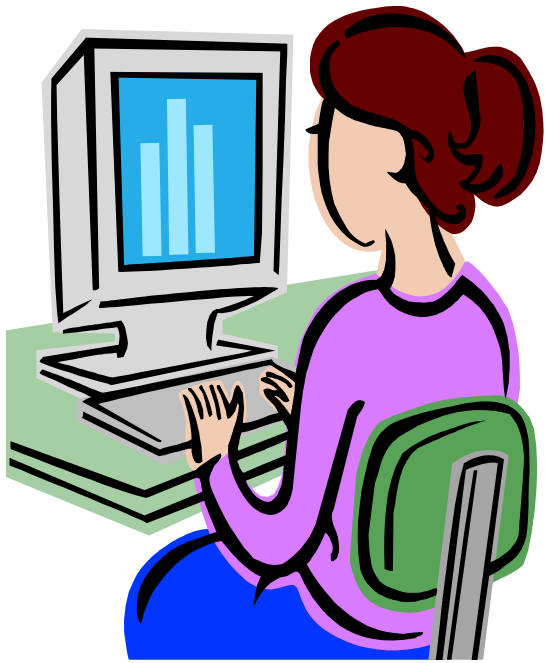
Employee User Administration	• Reduced time, effort, cost to administer user accounts • Improved level of service to end-users • Users have correct access to systems they need
Student User Administration	• Reduced time, effort, cost to administer user accounts • Improved transition when students change 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

What is Identity Management?

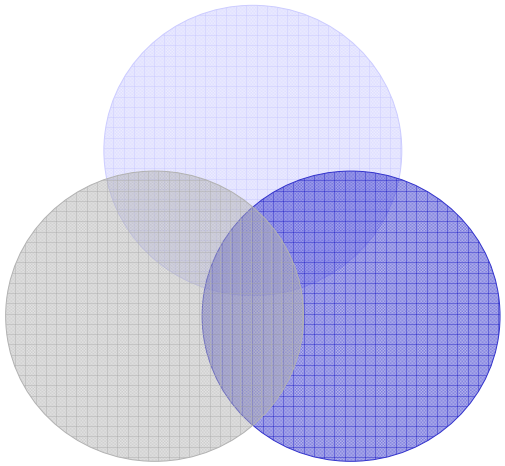


Identity Administration

- Provisioning
  - Creating accounts
  - Reviewing accounts
  - Changing accounts
  - Disabling accounts
- Adding roles to accounts
- Changing attributes (name change)



Directory Services



- Single view of user profiles from multiple sources
- Primary source is Active Directory
- Employee data from E-Business
- Student data from Infinite Campus

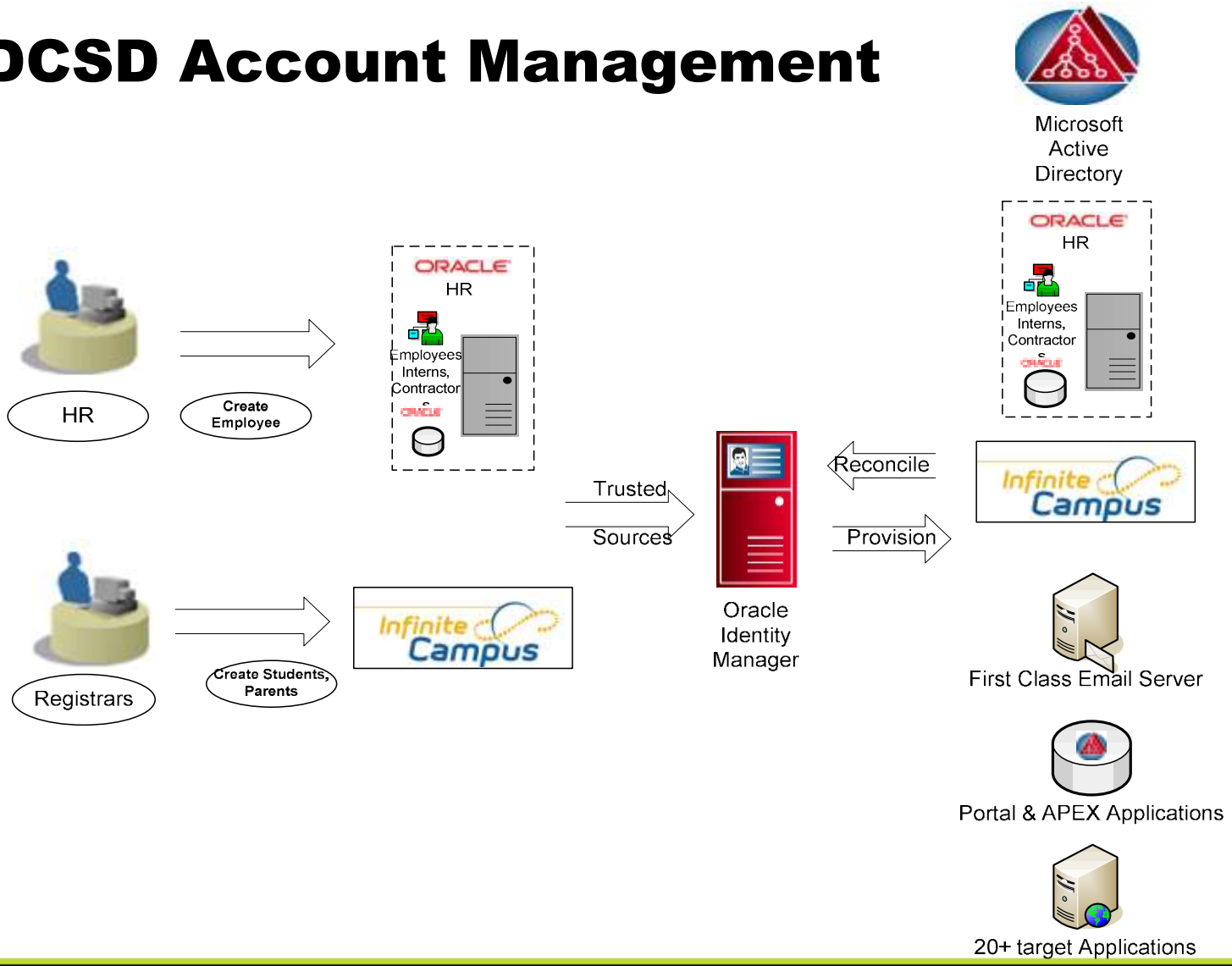
Access Control

- Authentication – who are you?
- Authorization – what are you allowed to access?
- Roles
- Self-service password reset

Auditing…Last But Not Least

- Determine if a given user has access
  - *By application - Who has accessed a given application in the last month? (OIM)*
  - *By user account – What applications has a user accessed? (OAM)*
- Historical and real-time
- Justify to auditors
- Raise confidence level of business owners that their data is protected
- Regulatory compliance

DCSD Account Management



Person – Assignment Structure

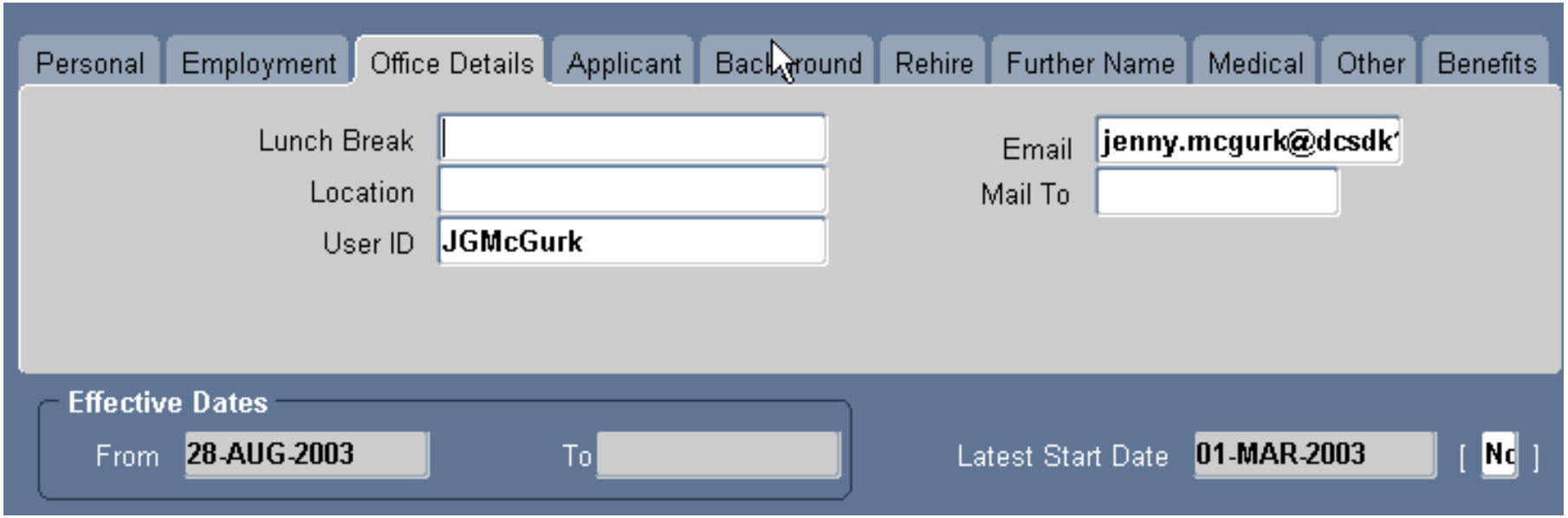
- Utilizing Position Control
- Position Segments
  - Job Class (admin, certified, classified, prof, tech)
  - Job Name (teacher, programmer, principal)
  - Job Description
  - Reporting Organization
- Location
  - Physical location where employee works
  - Used to identify Active Directory Organizational Unit (OU) for */home* folder

School District Anomalies in HR

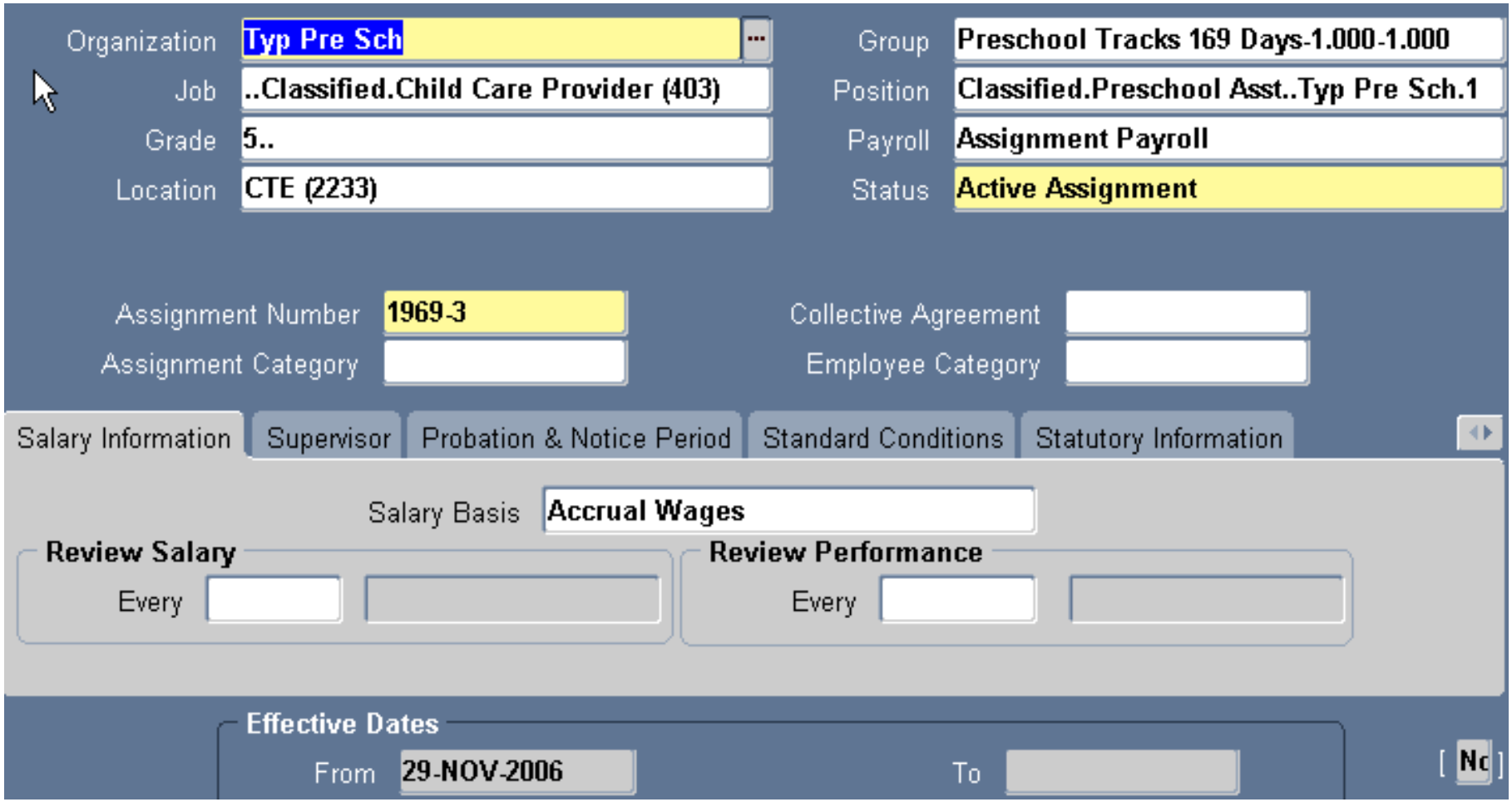
- Multiple assignments per employee
- Overlapping assignments
- Must be set up with user accounts prior to starting on the job
- Union Contracts

Person Record

- Populate User ID and Email when record is saved via custom.pll (create and update)
- Standard for User ID is legal name || sequence



Assignment Record



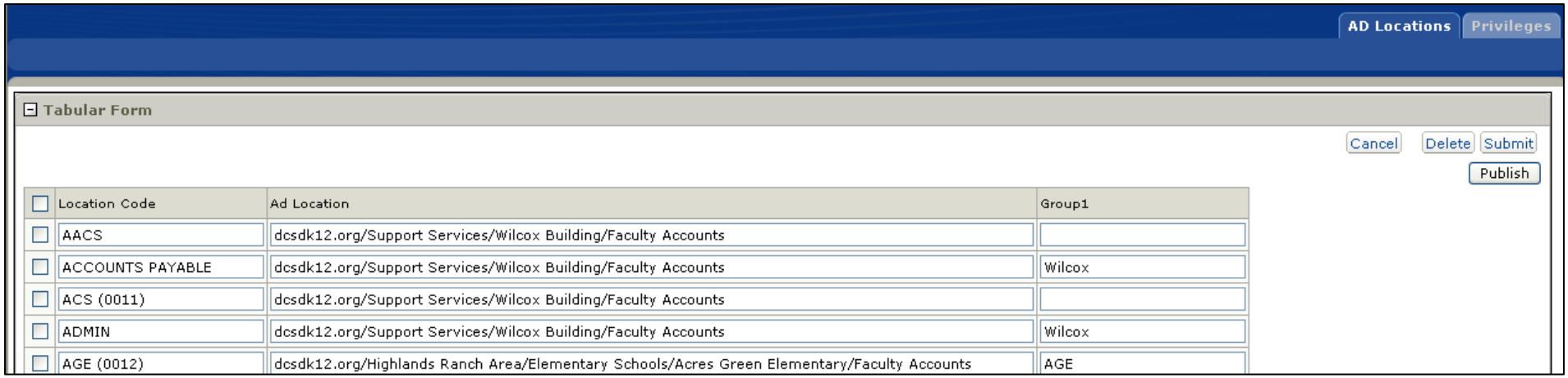
Implementation Strategy

- Methodology and Organizational Impact
- Define
  - Data and Rules
  - Workflows
  - As-Is and To-Be Access Policies
- Document
  - Use Cases
  - Manual Processes
- Product Selection

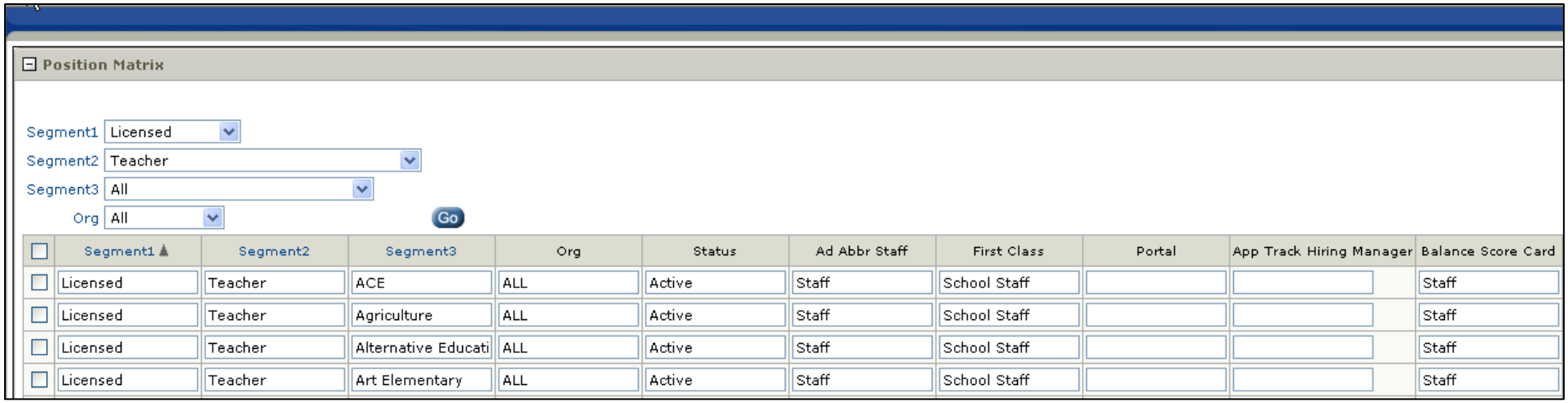
Functional Roles Management

- Less than 50 roles is ideal
- We needed hundreds
  - Assignment-based Portal content
  - Additional duties beyond official position
- Table driven
  - Matrix of locations and position segments
  - Approval in Position Control triggers insert into table
- Built APEX application so HR can manage

Physical Roles Management

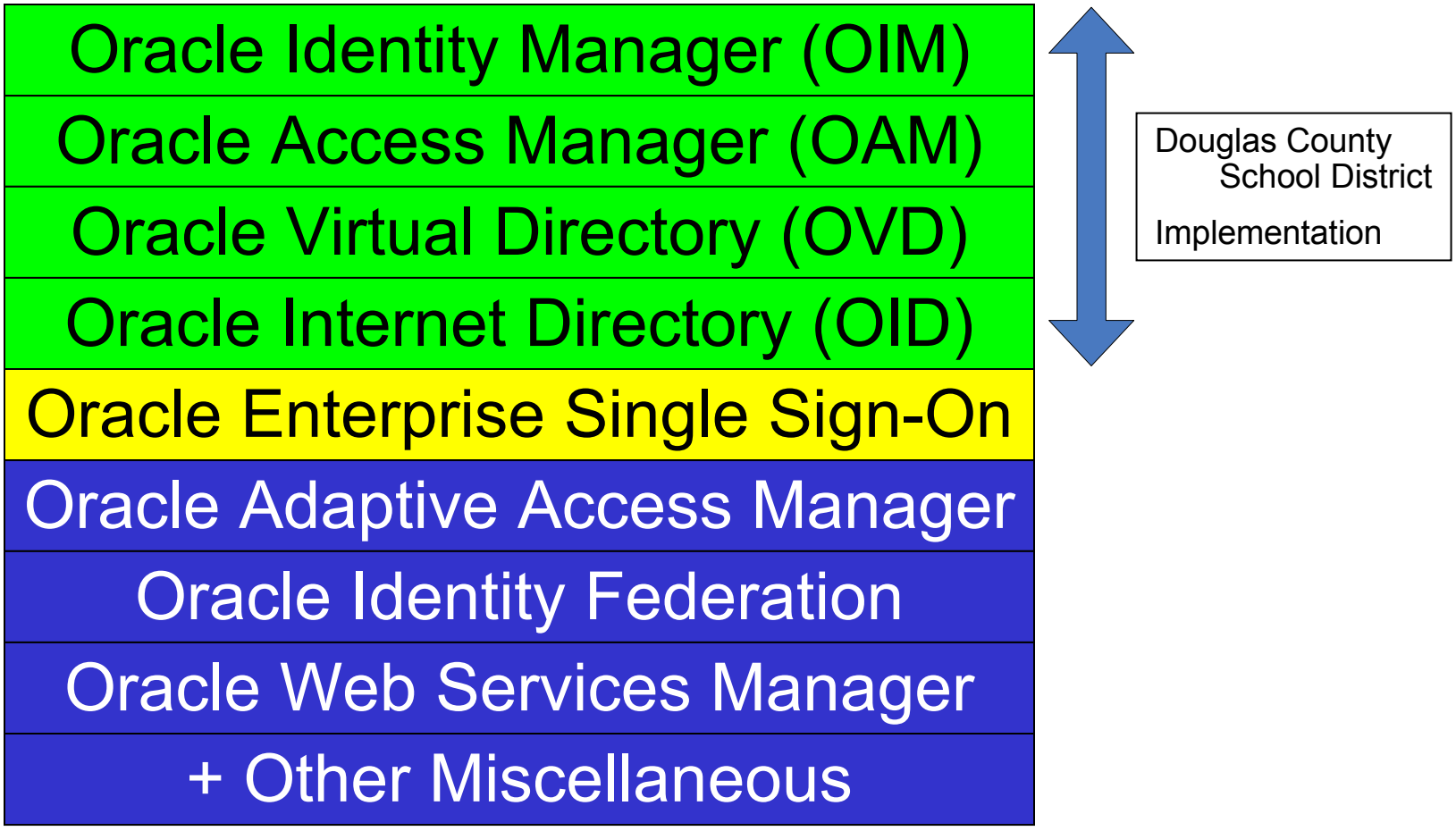


Location Code	Ad Location	Group1
AACS	dcsdk12.org/Support Services/Wilcox Building/Faculty Accounts	
ACCOUNTS PAYABLE	dcsdk12.org/Support Services/Wilcox Building/Faculty Accounts	Wilcox
ACS (0011)	dcsdk12.org/Support Services/Wilcox Building/Faculty Accounts	
ADMIN	dcsdk12.org/Support Services/Wilcox Building/Faculty Accounts	Wilcox
AGE (0012)	dcsdk12.org/Highlands Ranch Area/Elementary Schools/Acres Green Elementary/Faculty Accounts	AGE



Segment1	Segment2	Segment3	Org	Status	Ad Abbr Staff	First Class	Portal	App Track Hiring Manager	Balance Score Card
Licensed	Teacher	ACE	ALL	Active	Staff	School Staff			Staff
Licensed	Teacher	Agriculture	ALL	Active	Staff	School Staff			Staff
Licensed	Teacher	Alternative Educati	ALL	Active	Staff	School Staff			Staff
Licensed	Teacher	Art Elementary	ALL	Active	Staff	School Staff			Staff

Oracle Identity Management Products



Oracle Identity Manager (OIM)

- Provisioning / Identity Administration
- Pre-Built Connectors for:
  - Oracle E-Business Suite
  - Databases
  - Oracle Portal
  - Microsoft Active Directory
  - SAP
  - Windows
  - Many more
- Custom Connector Integration
  - Tool-set and Glue
- Self-Service

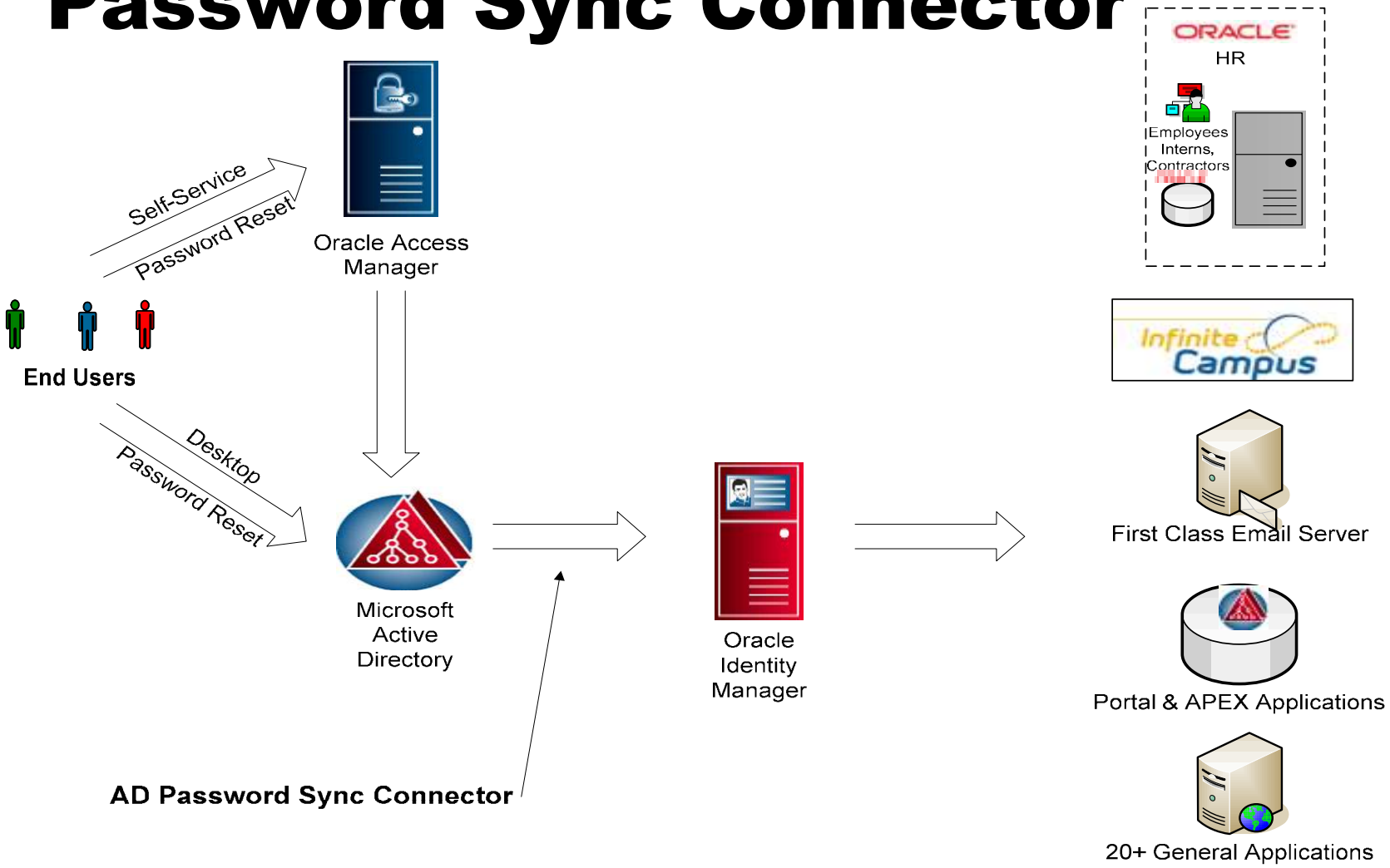
Connector Types

- Provisioning
  - Password Synchronization
  - Create, Modify, Delete User
- Reconciliation
  - Detect Target System Changes and bring back into OIM for audit and logging

Connectors Implemented at DCSD

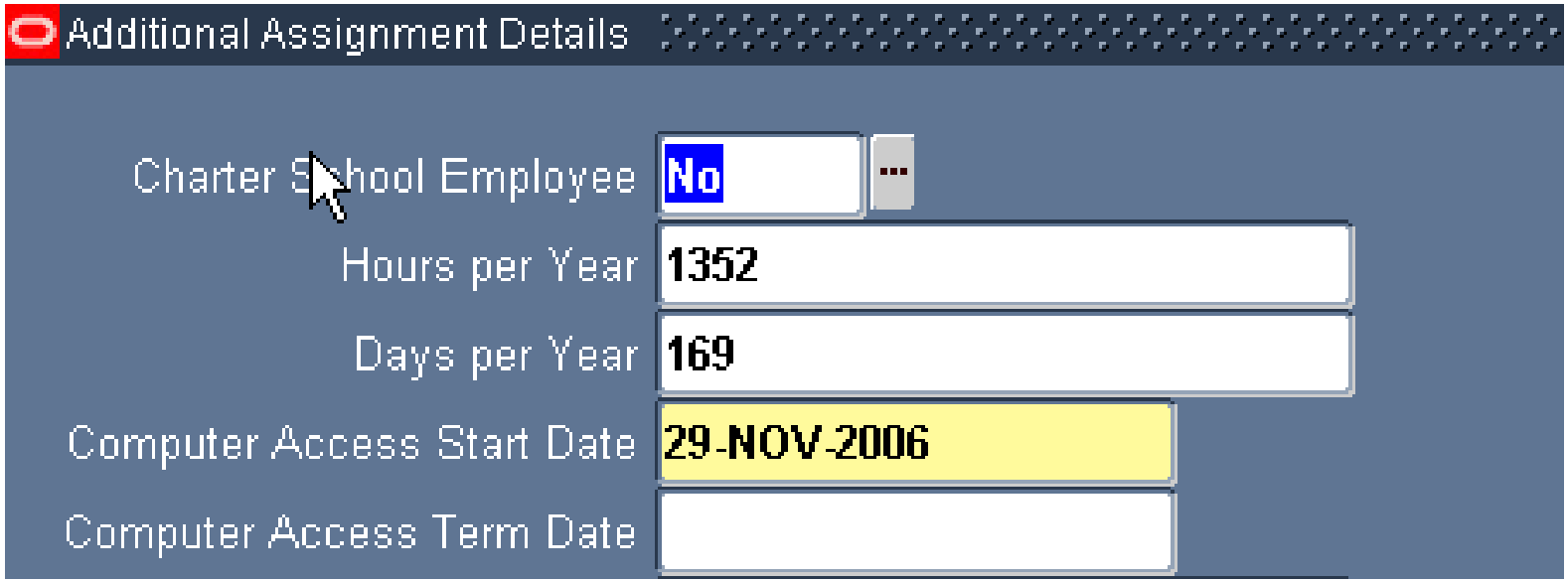
- Standard Connectors for Active Directory, Portal
- Custom Connector for
  - E-Business Suite
    - Not able to use out-of-box connector
      - Complicated assignments, e.g. Teacher and Bus-Driver
      - Standard effective dates designed for Payroll, not access
    - Built custom connector in PL/SQL and Java
    - Submitted Oracle Enhancement Requests
  - Infinite Campus (SQL Server)
  - First Class – Email (proprietary 3rd party software)
  - Kronos Automated Time Management (recon only)

Password Sync Connector



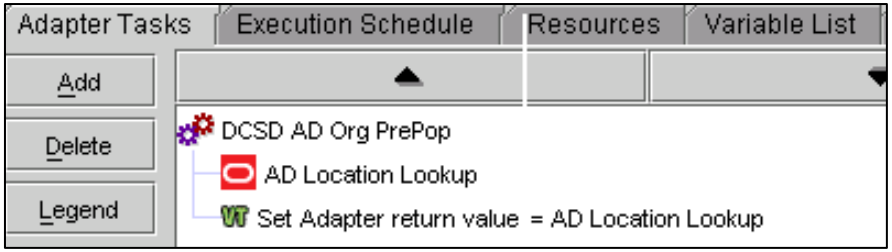
Assignment Record Flexfields

- Problem with using Effective dates
- Solution - added two new flexfields for connector



Location Drives AD Organization

- E-Business Suite Location determines Active Directory Organization



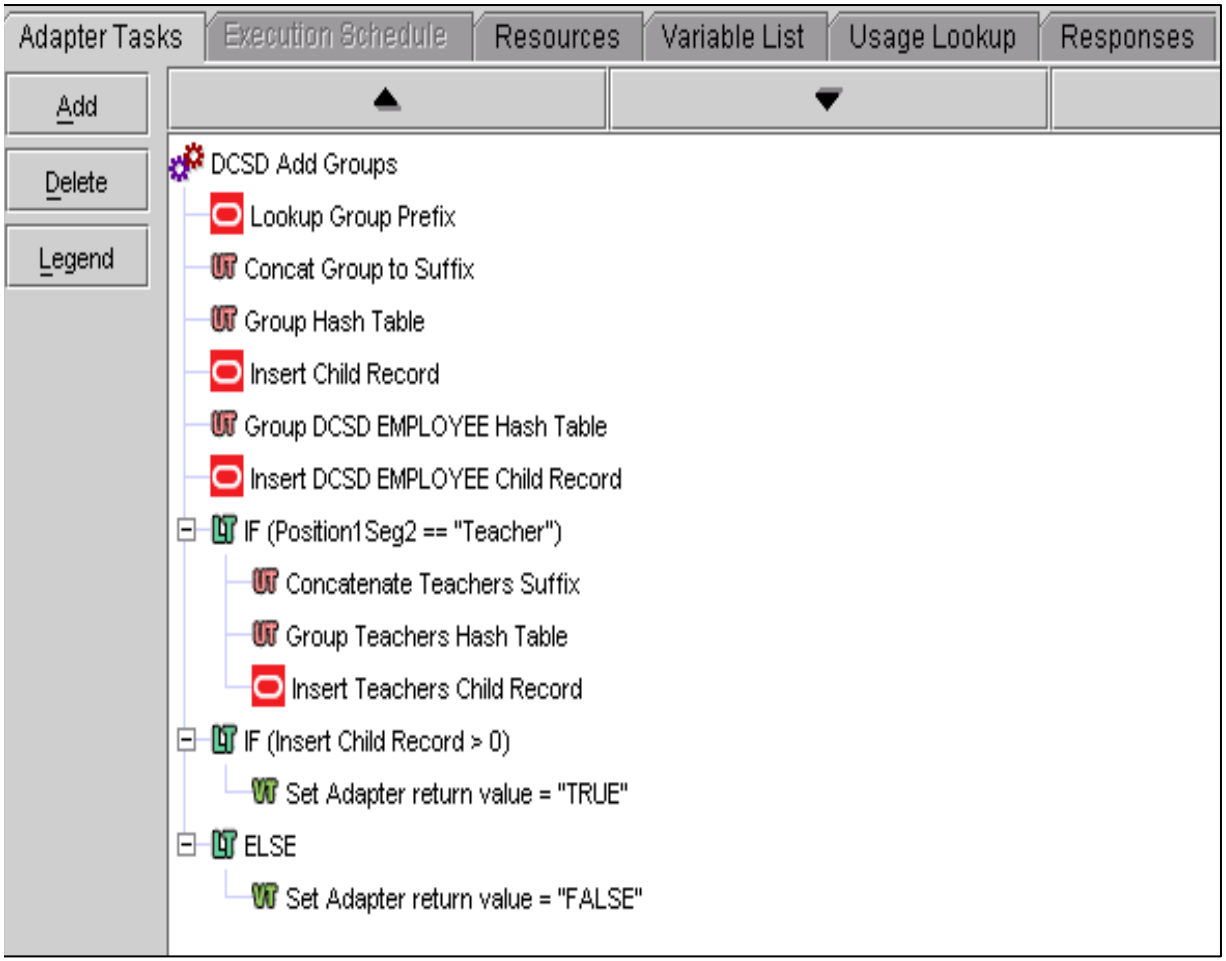
Position String	Licensed.Teacher.Grade K
School Name	
Street Address	1291 Firewood Tr
City	Franktown
State	CO
Zip Code	80116
Phone 1	303-555-3531
Phone 2	303-555-2593
Work Telephone Number	
Person Id	11774
EBS Status	
Position 1 Location Code	AGE

Lookup Code Information

Add
Delete

	Code Key	Decode
1	ITS	OU=Faculty Accounts,OU=Technology Support Center,OU=Support Services
2	AGE	OU=Faculty Accounts,OU=Acres Green Elementary,OU=Elementary Schools,OU=Highlands Ranch Area

Provisioning Rules for AD Groups



Lookup Location = AGE

Create user in groups

AGE-Staff

AGE-Teachers

DCSD_EMPLOYEE

Lookup Code Information

Add

Delete

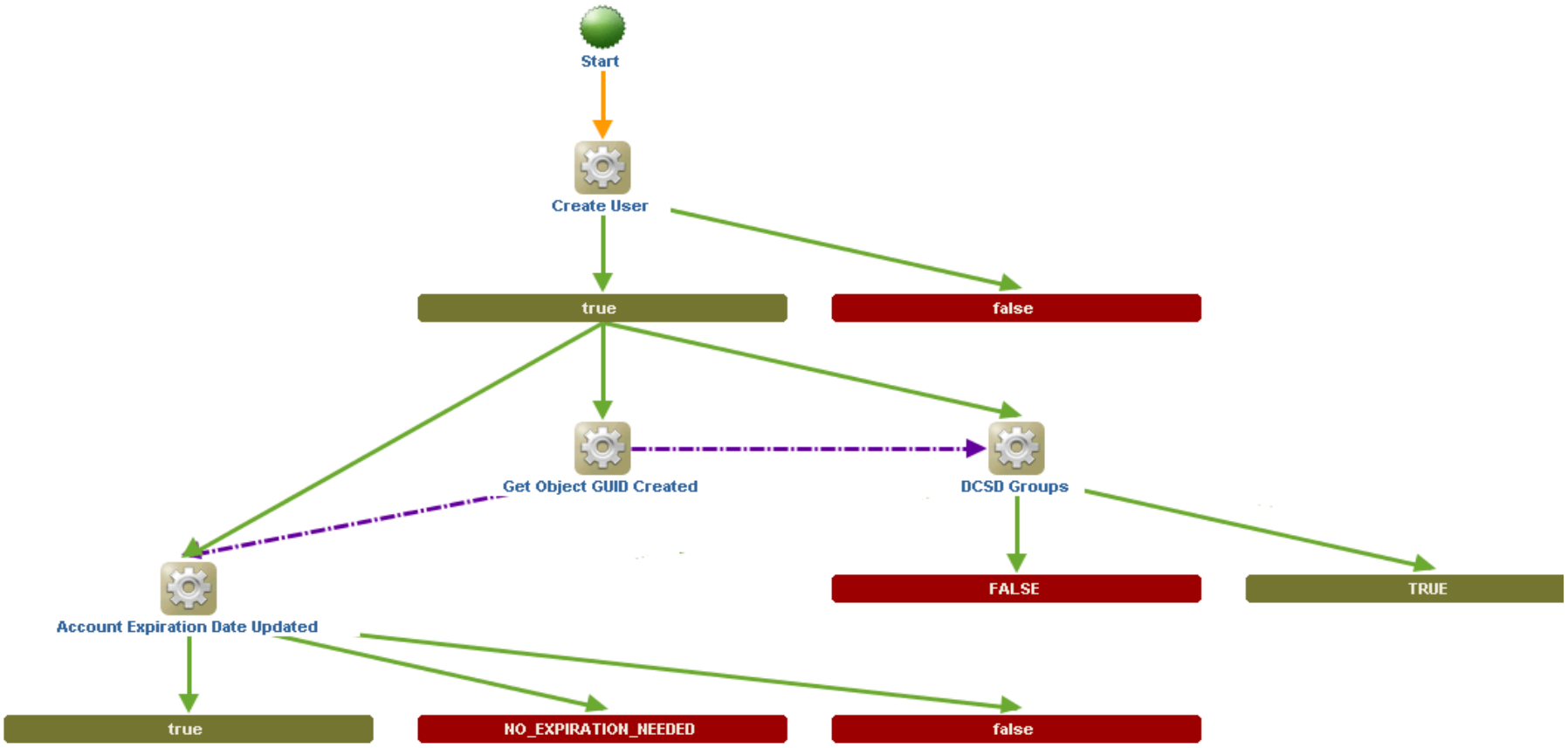
	Code Key	Decode
1	SMS	SMS
2	CCC	Coyote
3	AGE	AGE
4	ITS	Wilcox

Workflow Visualizer

Workflow Name : **AD User**
Workflow Type : **Provisioning [Default]**
For Resource : **AD User**
Form Name : **UD_ADUSER**

Display Options | Generate Image | Reload Workflow | Legend

Provisioning | Reconciliation | Service Account | User Event | Org Event | Resource Event | Form Event | Attestation



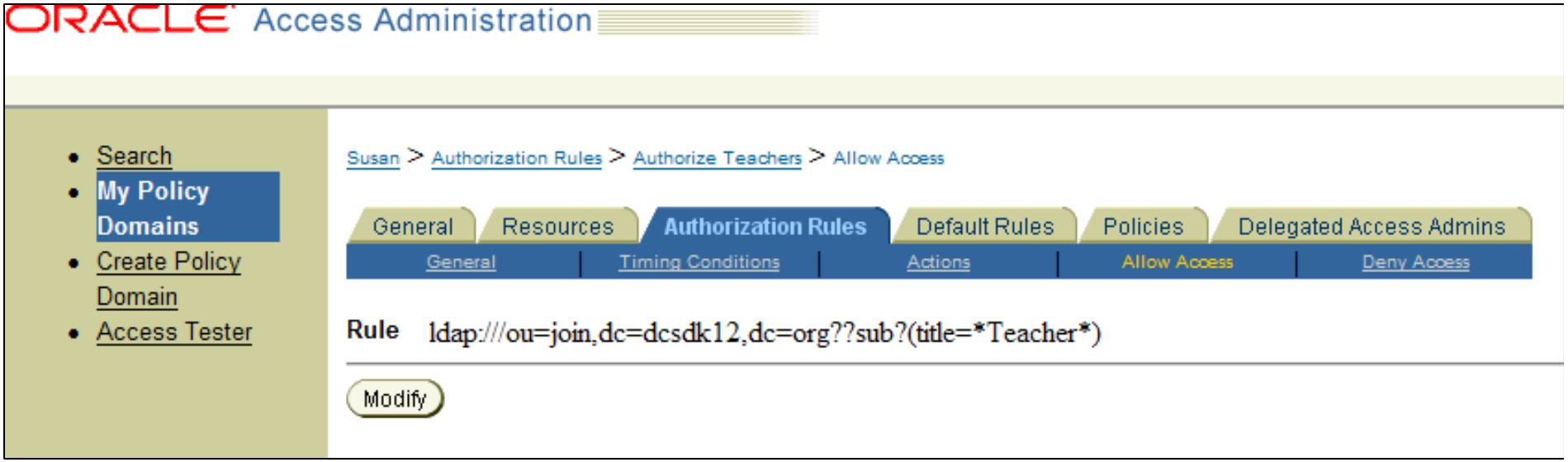
OIM Feature Summary

- Does the “heavy lifting” of Identity Management
- Should be named Oracle Resource Manager
- State of the Art Rules & Workflow Engine
- Extensible Normalized Data Model
- Compatible with everything (just about)
- Requires Java programming skills to configure

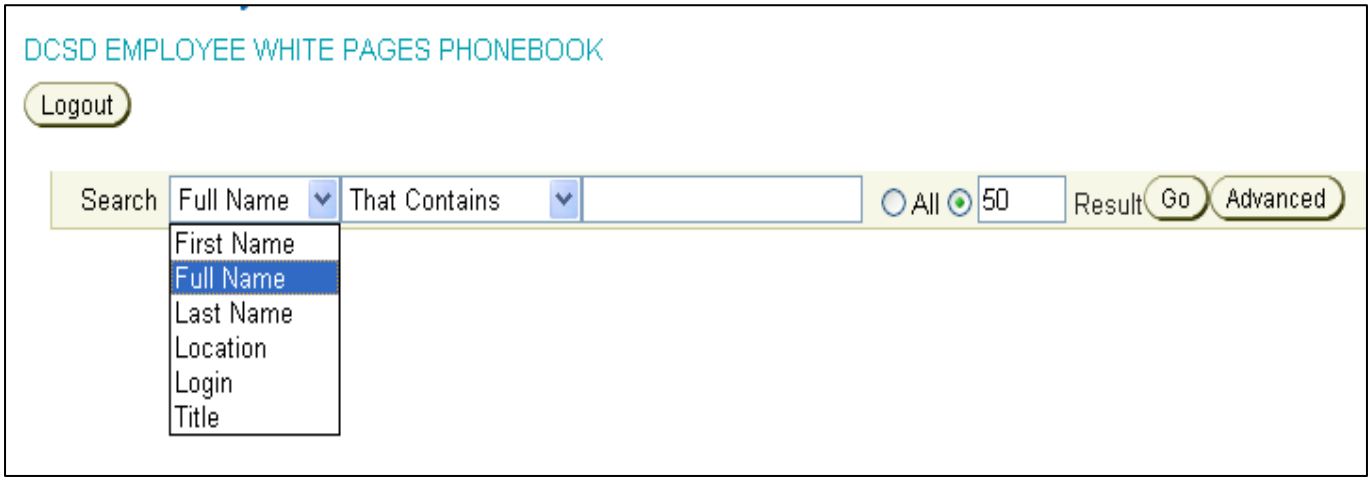
Oracle Access Manager (OAM)

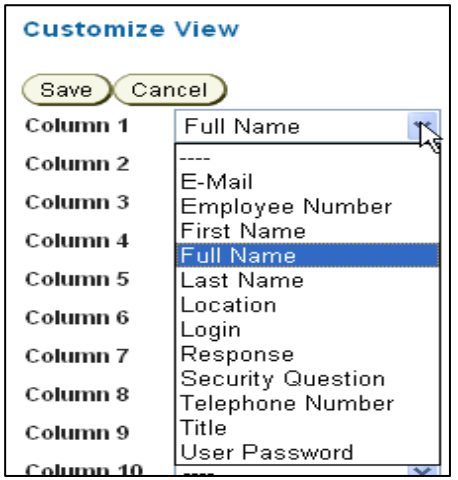
- Unified Password Policy across applications
  - Lockouts, Forced Password Change, Password Complexity, Password history etc.
  - Specific policies for different groups of users
- Self Service Password Reset
- Single Sign-On (SSO)
- Role and Rule Based Access Control
- Auditing
  - Who did what, when, failed authorizations, etc.
- White Pages Search

Rule / Role Based Access



White Pages Phonebook





OAM Summary

- Very flexible because of LDAP Rules
- Customizable
- Light-weight
- Complex to configure
  - Requires personnel skilled in LDAP directories and web servers
- Easy tool for Support staff to use

Oracle Virtual Directory (OVD)

- Makes any data source look like a LDAP Directory
  - Databases (Oracle, SQL/Server, etc.)
  - Flat Files
  - Convert Active Directory to inetOrgPerson
- Can modify attributes in transit
- Caches Directory Data for improved performance
- Creates a unified view of a split user profile

DCSD OVD Setup

Student Profile

Ella Iveslatt

Kindergarten
Thunderridge

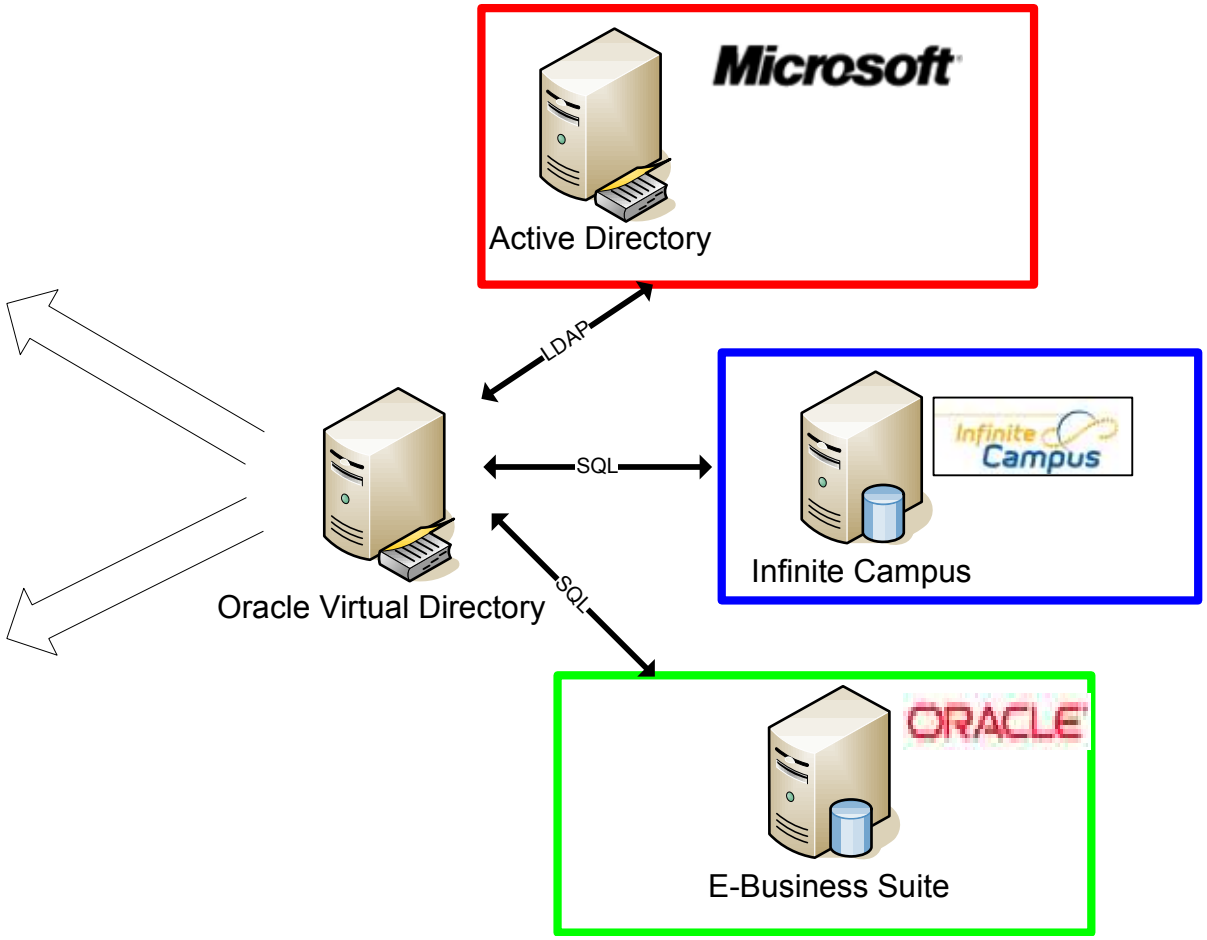
Teacher Profile

Niklas Iveslatt

303-882-4461

Positions

Lunch Lady – Highlands Ranch High School
Art Teacher – Acers Green Elementary



OVD Summary

- A system integrators best friend!
- Unifies Active Directory and Oracle Access Manager
  - Lockout flags
  - Password expired
- Easy to install and setup, can get more complex depending on feature usage
- Python programming skills a +

Lessons Learned

1. Know your systems
2. There will be process changes
3. Get HR involved
   - Access depends on them
   - Their processes changed as well
4. Almost everything needs a custom connector
5. Create table driven roles and system access
6. Be careful and meticulous about reconciling

Contact Us

Jenny McGurk
Application Development Manager
Douglas County School District
Jenny.McGurk@dcsdk12.org
303-387-9321

Niklas Iveslatt
Managing Partner
Arisant, LLC
Niklas.Iveslatt@arisant.com
303-882-4461