IdM
Building Walls while Breaking Down Barriers

By Bry-Ann Yates and Kim McDonnell
Building Walls
What is IdM?

A security discipline enabling the right individuals to access the right resources

-Gartner.
Foundation for Success

- Define and support of IdM Policy from the top down
- Well-rounded team
Benefits of our Initiatives

- Strengthen internal controls
- Educate University on IdM
- Adherence & enforcement of IdM Policy
- Strengthen collaborative relationships
The Trigger
Forced Automated Provisioning & De-provisioning

- BEFORE
- AFTER

UAlbany Mail Accounts

40,000
30,000
20,000
10,000

5,000
34,000
Albany EduPerson Codes

- Foundation of automated processes

- Implementation
  - Based on Internet2’s EduPerson Schema
  - Data from System of Record
  - 63 Customer identification codes and growing!
<table>
<thead>
<tr>
<th><strong>UAlbany Eduperson</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CREG</td>
<td>Current Registered Students</td>
</tr>
<tr>
<td>FULL</td>
<td>Full Time Employees</td>
</tr>
<tr>
<td>FUHS</td>
<td>Former Univ. HS Students</td>
</tr>
<tr>
<td>ELIG</td>
<td>Eligible to Enroll</td>
</tr>
<tr>
<td>PROF</td>
<td>Professional Employees</td>
</tr>
<tr>
<td>STMP</td>
<td>State Operations Employees</td>
</tr>
</tbody>
</table>
Account Lifecycle

Automation of creation & removal of access based on status at the University

- **New user comes in**
  - Provision

- **Wishing faculty/staff & students all the best in their future endeavors**
  - De-provision

- **Someone being rehired, transfer to different department or role change**
  - Re-Provision
Termination Process

- Before UAlbany Mail Conversion
  - Manual

- After UAlbany Mail Conversion
  - Automation Crucial
Complexity of Manual Termination
# De-Provisioning Notification

Automated notification to departments when user’s access level has decreased

<table>
<thead>
<tr>
<th>Account Closure Date</th>
<th>Name</th>
<th>Albany ID</th>
<th>Transaction Type</th>
<th>Manager of Windows Resources groups</th>
<th>Manager of generic windows accounts</th>
<th>Has access to the following Window Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Gomez Addams</td>
<td>123456789</td>
<td>Transfer</td>
<td>None</td>
<td>None</td>
<td>Department Shared Folder: Common Area</td>
</tr>
<tr>
<td>N/A</td>
<td>Morticia Addams</td>
<td>143256799</td>
<td>Transfer</td>
<td>None</td>
<td>None</td>
<td>Network Printer: Printer 1 Managed by Rogers, Network Printer: Printer 2 Managed by Rogers, Departmental Shared Folder: Common Area – Athletics, Room Calendar-administrative access: UDEV UAlbany, Departmental Shared Folder: PAC Managed by Jones.</td>
</tr>
<tr>
<td>N/A</td>
<td>Wednesday Addams</td>
<td>123456780</td>
<td>Role Change</td>
<td>Department Shared Folder: UA Project Departmental UAlbany Mail account: XYZ Mailbox</td>
<td>None</td>
<td>Room Calendar-user access: LC 99 - Conference Departmental UAlbany Mail account: XYZ Mailbox</td>
</tr>
<tr>
<td>N/A</td>
<td>Fester Addams</td>
<td>100056789</td>
<td>Role Change</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>11/5/13</td>
<td>Pugsley Addams</td>
<td>123546789</td>
<td>Pending Closure</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Group Access Manager Portal
Managers update and review users’ access
Breaking Down Barriers
Identify Your Stakeholders

- Data Stewards – 3 HR Departments
- Customers/Departments
- Some departments are “more special” than others
Benefits of our Initiative

- Collaboration
- Helped achieve buy-in from stakeholders
- Developed better understanding of HR’s processes
- Worked with other IT groups
A Seized Opportunity

- HR participated in our de-provisioning sessions
- Gave HR venue to reach mutual stakeholders
- Combined efforts of HR & IT gave customers extra incentive to attend informational sessions
Reach Your Audience

- Talk in language your audience understands
- Conform/tailor presentation to audience
- Create Wiki FAQ/documentation
- Positive approach to change is important
After Go Live: Breathe… But Don’t Think You’re Done

- Continue outreach months after “Go Live”
- Additional de-provisioning follow-up notifications to customers
- Refinements of de-provisioning FAQ based on customer feedback
Lessons Learned

- Training within system(s) of record department is very important
- EduPerson codes are a valuable resource for restricting access to services. Problems can occur without IdM guidance.
- Impossible to incorporate every scenario into an Albany EduPerson code
  - Exception code
- Do not assume you know everything about a department
Recipe for Success

Ingredients:

✓ 1 Part Senior Leadership Commitment (IdM Policy)
✓ Mix 1 Cup Technical & Non-Technical Individuals
✓ Blend Well with Communication
✓ Add 1 Pound Teamwork
✓ Add 1 Pound Collaborative Venture with Human Resources (Data Steward)
✓ Mix in Motivation to Foster New Relationships (In Person, Phone, Email)
✓ Add 1 Pint Positivity Projected to Customers & Audience
✓ Fold in 1 Pint Communication & Respect of Other IT Staff
✓ Mix in 1 Cup Enthusiasm
✓ Add Several Generous Cupfuls of Organization
✓ Add Dash of Persistence & Flexibility
✓ Blend 1 Cup Patience & Identification with Customers (Walk a Mile in their Shoes)
✓ Add 1 Heaping Tablespoon Caring & Empathy Toward Customers
✓ Mix 2 Cups Listening to Customer Feedback (Even if it Entails Additional Work)
✓ Mix All Ingredients & Blend Well Again with Communication!
Questions?
Online Survey