IAM Online
Managing Affiliate, Alumni, and Other Identities with Comanage
Wednesday, April 18, 2018
Janemarie Duh, Lafayette College
Jeff Ruch, Colorado State University
Benn Oshrin, Spherical Cow Group
COmanage:
An Introduction

Benjamin Oshrin
April 2018 • IAM Online
What Is COmanage [Registry]?

Registry Is The **Product**

*(Like “Shibboleth” and “IdP”)*

A Person* Registry: A place to store information about people associated with your organization

*also groups, departments, email lists, services, authenticators, and some other things*

Enrollment, Lifecycle, and Attribute Management

Complex representations of people with multiple components to their identity
COmanage History

Originally funded by NSF / Internet2 for Virtual Organizations (obLIGO)

*Turns out, VO Identity needs are similar to Institutional Identity needs*

As adoption grows, contributions are too (financial, patches, bug reports, etc)

CILogon (NSF), CTSC (Indiana University), GÉANT, Lafayette, MLA (Mellon), NIH/NIAID (NETE), SUNET, SURFnet, etc
What Can You Do With COmanage Registry?

Virtual Organization / Collaboration Management

Guest / Non-Traditional Population Management

University Identity Registry

*Some Integration Work May Be Required*
Integration Architectures
Registry Capabilities

Most non-core features are designed to provide common capabilities out of the box, but allow replacement or integration with more comprehensive products, eg:

- Group Management → Grouper
- Provisioning → (eg) midPoint

UI driven configuration and operation

REST API
Registry Capabilities

Person & Role Attribute Management
   Normalization
   Attribute Enumerations
   Multi-valued Names, Addresses, Email Addresses, etc

Identifier Assignment and Management
   Pattern based sequential or random identifier assignment
   Tracking of external (non-Registry) identifiers

Population Organization
   COUs & Departments
   Basic Group Management
Registry Capabilities

Self Service & Delegated Enrollment & Lifecycle Management
- Enrollment Flows
- Early Onboarding
- Duplicate Management / Relinking
- Sponsors
- Expiration Policies
- Basic Matching (*more to come
- Terms & Conditions

Human Readable Transaction History
- Person / Group / Email List / Petition

Database Level “Changelog” (Copy-On-Write)
Product Roadmap

Current Release: Registry v3.1.0

Registry v3.2.0 due soon
  - ID Match via API
  - voPerson
  - Dashboards

Registry v4.0.0 (tbd)
  - Framework Migration
More Info

Wiki

https://spaces.internet2.edu/display/COmanage
Technical Documentation
Data Model
https://spaces.internet2.edu/display/COmanage/Email+Lists

Git

https://github.com/Internet2/comanage-registry

TIER Packaging

https://spaces.internet2.edu/display/TPD
Docker
Rescue Remedy: COmanage
For Affiliate Identity Lifecycle Management

Lafayette College
Janemarie Duh
Identity Management Architect

Image: Vintage rescue squad mobile
Things to know

**Sponsor**
Authorized person requesting the account

**Enrollee**
An affiliate is called an enrollee

**Lafayette’s ERP is Banner**
The SPRIDEN_ID is called the L Number

**Sponsored account**
Provides access to services beyond that provided by a temporary guest wireless account
Lafayette’s Identity Management System

Accounts Workflow
  Custom-engineered system for employees

Web-based forms
  Double data entry with Banner

L numbers required
  Key that matches identities between our enterprise
directory (OpenLDAP) and Banner
The problem space

Intake process using the Other Employees Accounts Workflow form not a good fit for affiliates
   Form required an employment end date. Many times, this wasn’t known.

Identity lifecycle of affiliates was unmanaged
   Are the people still here or gone?

No process was in place for deprovisioning
   It was uncertain who to even contact
Image: Girl reading newspaper about moon landing
Moonshot

Could COmanage be used as a system of record for affiliates, provision DNs in LDAP, and track sponsored accounts?

Lafayette engaged with Spherical Cow Group and worked with Benn Oshrin
IAM architecture diagram
Initial use case

Initial deployment focused on supporting consultant use case

Once deployed, we quickly started using COmanage for outsourced Dining Services employees, external reviewers of academic departments, and auditors
Key integration considerations

Location of DNs in LDAP
   Stored in separate OU

NetID generation
   NetIDs are in the same namespace as other accounts
   Rules for composing NetID configured for identifier assignment
Attributes COmanage is to populate

COmanage tracks three identifiers: NetID, L number, uidNumber

uidNumber is based on L number

Integration of lafayettePerson LDAP schema for bannerLNumber, mailAlternateAddress

Recovery and official email addresses

eduPersonAffiliation

Samba attributes
  Plug-in added
Provisioning target

Organizational identity source

In addition to affiliates, sponsors must be added to COmanage

There are two COUs: one for sponsored accounts and one for sponsors
Enrollee induction
Enrollee induction

<table>
<thead>
<tr>
<th>Password Recovery Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid From</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid From</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Valid Through</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Through</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number (Mobile)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Code</td>
</tr>
<tr>
<td>Area Code</td>
</tr>
</tbody>
</table>

* indicates required fields if you populate this section.
Enrollee induction

<table>
<thead>
<tr>
<th><strong>Number (Mobile)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>* denotes required fields if you populate this section</td>
</tr>
<tr>
<td>Country Code</td>
</tr>
<tr>
<td>Area Code</td>
</tr>
<tr>
<td>Number</td>
</tr>
<tr>
<td>Extension</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>L~Number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>L~Number</td>
</tr>
<tr>
<td>Identifier*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UID Number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>UID Number</td>
</tr>
<tr>
<td>Identifier*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Affiliation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Affiliation*</td>
</tr>
<tr>
<td>Affiliate</td>
</tr>
</tbody>
</table>

* denotes required field
Intake process for COmanage

Sponsors contact Help Desk or IAM directly

What we require to create a sponsored account

- Sponsor name and email address
- Enrollee legal name, business email address, and phone
- Services enrollee needs to access
  - Sponsor requests for additional access after provisioning go to Help Desk
- Begin date and end dates
- Birth date for the enrollee
Sponsored account creation

IAM requests an L number (SPRIDEN_ID) from enterprise data team uidNumber based on L number

IAM enters data into the Enrollee Induction enrollment flow

COmanage collects the petitioner attributes, and finalizes the flow to provision the DN and send a notification

Account claim notification contains NetID and self-service password set instructions
Enrollee induction flow results

* denotes required field

<table>
<thead>
<tr>
<th>Action</th>
<th>Actor</th>
<th>Comment</th>
<th>Timestamp (America/New_York)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Janemarie Duh</td>
<td>Petition created from enrollment flow &quot;Enrollee Induction (19)&quot;</td>
<td>Mon, Apr 16th 2018, 12:59</td>
</tr>
<tr>
<td>AU</td>
<td>Janemarie Duh</td>
<td>Petition attributes updated</td>
<td>Mon, Apr 16th 2018, 13:03</td>
</tr>
<tr>
<td>IA</td>
<td>Janemarie Duh</td>
<td>Identifiers Assigned (netid)</td>
<td>Mon, Apr 16th 2018, 13:03</td>
</tr>
<tr>
<td>SU</td>
<td>Janemarie Duh</td>
<td>Petition changed status from Created to Finalized</td>
<td>Mon, Apr 16th 2018, 13:03</td>
</tr>
<tr>
<td>NS</td>
<td>Janemarie Duh</td>
<td>Approval notification sent to Alisha Bowers</td>
<td>Mon, Apr 16th 2018, 13:03</td>
</tr>
</tbody>
</table>
Some manual work involved

Requesting L number and adding enrollee’s personal information into the enrollment flow

Modifying/adding email values

Creation of other accounts besides LDAP

Access policy group memberships in Grouper

Any Lafayette email addresses created are written back to Banner by a separate process
Renewals and Expirations

COmanage has flows for renewals and expirations
   6-month max validity period for sponsored accounts that requires sponsors to re-authorize enrollees’ access

Automated expiration messages sent at intervals to sponsors and enrollees
   Sponsor emails us to re-up

Upon expiration, account disabled administratively in LDAP
   COmanage would typically remove it
COmanage delivered three key benefits

It ensured that each sponsored account has an L number for the purpose of identity matching

There is a known and tracked sponsor for each enrollee

The entire identity lifecycle of affiliates is managed
Possibilities for phase two

Integrate with Banner or management of a reserved pool of L numbers

Provision to Zimbra and write back Lafayette email address

Solve the access-related issue with respect to finalizing enrollment
  Or a button to finalize the flow

Resend button would also be useful
COmanage now manages 123 Sponsored Accounts people
Image: Partridge Family bus

Janemarie Duh
duhj@lafayette.edu

Lafayette College
TIER Adopter Profile
External Identities with COmanage

Jeff Ruch
April 18, 2018

Colorado State University
Table of Contents

- Project Drivers
- Solution
- User Experience
- Existing IAM environment
- Role of COmanage
- Role of Cirrus Identity
- Role of Azure Service Bus
- Architecture & Flow
- What’s in COmanage
- What’s Next?
- Questions?
Project Driver - Overview

• Advancement - Donor Connect
  • In house application (2010)
  • Get receipts for taxes
  • See giving history
  • High end endowment balance
Project Driver - Pain Points

• Trouble Remembering Credentials
Project Driver - Pain Points

• Credential Management
  • Advancement Specific
  • Maintenance Overhead
  • Liability
Solution

Social Login
• more secure
• remember credentials
• take liability away from CSU

Unique CSU Identifier that could be used across multiple systems/technologies.
User Experience
User Experience
User Experience

![Microsoft login screen with email jruch@live.com and a password input field with 'Back' and 'Sign in' buttons, along with 'Keep me signed in' checkbox and 'Forgot my password' link.]
User Experience

[Image of a web interface asking for permission to access user info]
Existing IAM at CSU

- Shibboleth
- Grouper
  - Subjects through source data (SQL)
  - Groups from source data, ad-hoc
  - Applications used API to authorize
- Existing Identity Management System (eID)
  - Home grown from 2007
  - Pulls data from SIS
  - External users require HR system entry
Role of COmanage

- Centralized Person Registry
- Unique Identifier
- Account Linking
Role of Cirrus Gateway (Social to SAML)
  • Just Another IDP
  • Social Discovery Service (iframe & embedded)
  • Handles oAuth, OpenID to Social Services
  • Returns SAML assertions back to SP

• Identity Provider Proxy Service
  • Supports single unique identifier for social account.
Role of Azure

- Service Bus – Messaging
  - Ensure all requests are processed
  - Allows web applications to continue without waiting for a response from API.
What’s in COmanage

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Fred Weasly (Primary, official, English)</td>
</tr>
<tr>
<td>Identifiers</td>
<td>R2548607 (co:stated:edu:Person:SUITS)</td>
</tr>
<tr>
<td></td>
<td>feasley (co:stated:edu:Person:ID)</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:feasley@colorado.edu">feasley@colorado.edu</a> (co:stated:edu:Person:UPN)</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:feasley@colorado.edu">feasley@colorado.edu</a> (co:stated:edu:Person:PrincipalName)</td>
</tr>
<tr>
<td></td>
<td>1154069 (co:stated:edu:Person:ID)</td>
</tr>
<tr>
<td></td>
<td>1079152 (co:stated:edu:Person:ArmeeID)</td>
</tr>
<tr>
<td></td>
<td>151467 (co:stated:edu:Person:AniseID)</td>
</tr>
<tr>
<td></td>
<td>Fred <a href="mailto:Weasly@colorado.edu">Weasly@colorado.edu</a> (Mail)</td>
</tr>
<tr>
<td>Email Addresses</td>
<td><a href="mailto:Fred.Weasly@colorado.edu">Fred.Weasly@colorado.edu</a> (Official Unverified)</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:feasley@colorado.edu">feasley@colorado.edu</a> (Delivery Unverified)</td>
</tr>
<tr>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>cotmember: member</td>
</tr>
<tr>
<td></td>
<td>extern: member</td>
</tr>
<tr>
<td>Person Attributes</td>
<td>Status: active</td>
</tr>
</tbody>
</table>
What’s in COmanage cont.

<table>
<thead>
<tr>
<th>Role Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>COU</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Guest Associate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSH Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizational Identities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>Fred Weasley</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Log</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit, ReLink</td>
</tr>
</tbody>
</table>
What’s Next April 21st GO LIVE
What’s Next

• Store of External Identities
• Invitation Enrollment Flow
• Expand External Users
  • Transcripts
  • Parents
  • Ad hoc Teams
What’s Next **midPoint**?
What’s Next - Containerization
Questions?
Please Evaluate Today’s Session

https://www.surveymonkey.com/r/IAMOnline-April2018
Shibboleth Installation Workshops

Two Workshops Offered in 2018

May 22-23, 2018 – Unicon Headquarters – Gilbert, Arizona

July 10-11, 2018 – University of Pittsburgh – Pittsburgh, Pennsylvania

Identity Provider and Service Provider installation. Identity Provider uses the TIER container version, configured to work well with InCommon

www.incommon.org/shibtraining