Identity and Access Management
IAM Lifecycle Committee

October 1, 2014
Wednesday
11 a.m. – 1 p.m.
6 Story Street
Summary: IAM Program News

Quick Demo: Connections Feature To Be Added

Discussion Topics:

– Latest on Alumni
  • Data Model Overview
  • API instead of batch XML file

– Review requirements Analysis Template for Onboarding Schools

– Consolidating Users from the Schools into Identity Management
Please see the handout for the most recent version of the IAM Executive Status Dashboard.
See below for key program accomplishments achieved since the July 2014 IAM Executive Committee meeting:

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>Actual Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>SailPoint IIQ Foundation</td>
<td>University AD accounts now provisioned through SailPoint IIQ application</td>
<td>July 2014</td>
<td>Aug 2014</td>
<td>• 631,963 accounts moved off Waveset&lt;br&gt;• HUIT organization, including Help Desk</td>
</tr>
<tr>
<td>Federation</td>
<td>InCommon Bronze Self-Certification</td>
<td>Submit Bronze self-certification document to InCommon</td>
<td>Sep 2014</td>
<td>Sep 2014</td>
<td>• InCommon Bronze self-certification complete</td>
</tr>
<tr>
<td>Authorization Enhancements</td>
<td>SIS Wave 0</td>
<td>Deploy the FindPerson Identity API to production</td>
<td>Oct 2014</td>
<td>Sep 2014</td>
<td>• Enables integration between IAM database and PeopleSoft SIS</td>
</tr>
</tbody>
</table>
The first production release of SailPoint IIQ was successfully completed August 17.

- University AD accounts for employees and students now managed in SailPoint instead of Waveset
- Successful Fall Start using new provisioning mechanisms, with no major incidents
- Handoff underway to Help Desk for ongoing support

Next steps:
- Support for advanced features associated with “AD Lockout” use cases
- Ongoing stabilization work and data cleanup tasks
- Preparation for next populations (Alumni, HMS) to flow through IIQ
Harvard University Directory Information
The compilation or redistribution of information from Harvard University directories is forbidden.
09/29/14, 07:02 PM

Gleason, Christopher
Email
Phone
Location Harvard Univ Memorial Church
Harvard Yard
Title Counsellor, Denominational
Dept CADM OPR MEM United Ministry

Gleason, Christopher Scott
Email gleasonc@wit.edu
Phone
Location
Title Contin Ed/Spec Prog Instructor
Dept FAS FDCE Other Academic

Gleason, Emily Jean
Email emily_gleason@hms.harvard.edu
Phone
Location Harvard Medical School Genetics, NRB
77 Avenue Louis Pasteur
Title Research Fellow in Genetics
Dept HMS Gene

Gleason, Jessica Ann
Email jagleaso@bidmc.harvard.edu
Phone
Location Beth Israel Deaconess Medical Center
Anesthesia
One Deaconess Rd
Title Clinical Fellow in Anaesthesia
Dept HMS Anaesthesia-BIDMC

Gleason, Kelsey M
Email kmg152@mail.harvard.edu
Phone
Location 1539 Cambridge St
Apt 1
Title
Dept

Gleason, Lauren Jan
Email igleason@bidmc.harvard.edu
Phone
Location Beth Israel Deaconess Medical Center
Medicine/LMOB 1B
330 Brookline Ave
Title Clinical Fellow in Medicine
Dept HMS Medcn-BIDMC

Gleason, Mark
Email mark@gleasonclan.com
Phone
Location
Title
Dept

Gleason, Tim
Email tgleason@camail.harvard.edu
Phone 617-495-5811
Location
Title
Dept
Alumni Data Model

- Review Data Model
- Discussion: Adding Alumni roles to MIDAS
• Preparing to migrate HMS to Sailpoint for User Management and Provisioning

• Discussion: Review the proposed requirements process
Requirements for Onboarding Schools

• System Landscape
  – Database
  – Input systems
  – Frequency of data flowing
  – Feeds to their target systems
  – Exports
  – All systems that connect

• Business context diagrams

• Stakeholders
  – Groups and how they interface with the data
Requirements for Onboarding Schools

• User Populations being managed
  – With HUIDS
  – Without HUIDS
  – Deeper dive on the people without Harvard IDs that are in their local IDM
    • Who are they
    • What level of detail do they have
    • Who owns the business processes

• Data Models for Populations

• Resource Management Matrix
  – Who gets what!
Requirements for Onboarding Schools

• Sponsored Account Requests
  – People
  – Non-People (Service)
    • Types of services

• Self-Registered Accounts

• Device Management

• Historical use of the Central POI processes
  – POI
  – Library

• Inventory: Existing Onboarding/Request Process Flows for various populations
  – End User Account Requests
  – Account claiming
  – Requesting resources for users
    • Self Service
    • Manager based
Requirements for Onboarding Schools

• Targets Needing Provisioned Data
  – Need schema for any targets
  – If they have any meta data information

• Password related information
  – Password policies and rules

• Username policies
  – Naming conventions (anything you are fussy about)

• School-specific
  – Access Management approaches
  – Use of ‘groups’ to authorize access
  – VIP Exception processes
  – Discuss overlapping credentials for populations
    • Duplicate identities, multiple credentials, etc.
Requirements for Onboarding Schools

• Implementation and Rollout
• Support Services Models
• Communication
  – Stakeholders
  – Channels they typically use
  – Key Contact for developing a plan

• Discussion: Are there major dimensions of this analysis missing from this list?
• Merging schools into the central identity registry involves
  – Sharing data models
  – Developing processes that work across Harvard
• Consolidating user name space
  – Handling the case where there are two jhill@
• Local process change for the sake of the global Harvard user experience
• Surfaces Data Quality and Data Flow Issues
  – Example: Preferred Name at HMS is a good example of type of issue we may uncover
Use Case: Preferred Name

• **Background/Issue:** Individuals may optionally use, and display, a different name other than their official name within Harvard systems. This attribute is known as the preferred name, listing name, or display name, depending on the system. The issue is that for HMS, some downstream systems and directories are not displaying an individual’s most current preferred name.

• **User Scenario:** An HMS faculty or staff person gets married and submits the paperwork to HR to change both their Official and Preferred name. Once the change is made in PeopleSoft for both name types, the HMS-AD, HMS White Pages and MARS reports display the changed name, but downstream systems such as Canvas do not display the name change. In addition, once the HMS user is migrated from HMS-AD to O365 their display name may revert back to their maiden name.

• **Root Cause:** Although the preferred name attribute value in PeopleSoft is populated out to the HMS Data warehouse, the HMS IDM and eventually out to the HMS-AD, white pages and MARS, the attribute does not auto-populate to the HUIT IDdb or University-AD. Any downstream systems relying on the HUIT IDdb for preferred/listing/display name will therefore, not reflect the change made in PeopleSoft.

• **Mitigation:** An individual’s preferred name can be updated manually in the HUIT IDdb via the MIDAS interface accessible by directory services personnel or a departmental directory contact.

• **Solution in Progress:** HUIT IAM is in the process of testing a solution to auto-populate the HUIT IDdb “listing_name” attribute from the PeopleSoft “preferred_name” attribute.

• **Compounding Issue:** While it seems this issue might only affect individuals who choose to use a preferred name in PeopleSoft, it appears that data conversions in the past may have auto-populated the “listing_name” in the HUIT IDdb to be equal to the “official_name”. The result is that even individuals who just use their official_name in PeopleSoft may not see their name changes in downstream systems that use the HUIT IDdb “listing_name” attribute over the official_name attribute.
Thank you!
Simplify the User Experience
• Selected and purchased an identity creation toolset that will lead to improved onboarding for all users.
• Implemented a new Central Authentication Service for faster, flexible deployment of applications across Harvard.
• Implemented one-way federation with the Harvard Medical School as proof of concept of credential self-selection by users in order to access services.
• Implemented provisioning improvements that set a foundation for expanded cloud services, support for Active Directory consolidation, and support for email migration.
• Integrated a new ID card application that enables large-scale replacement of expired cards.
• Implemented a new external-facing IAM website for regularly updated information on project purpose and status.
• Migrated University AD users to the SailPoint IdentityIQ provisioning solution.

Enable Research and Collaboration
• Joined the InCommon Federation, enabling authorized Harvard users to access protected material at HathiTrust.
• Enabled access to a planning tool used by Harvard researchers to assist with compliance of funding requirements specific to grants (e.g. NSF, NIH, Gordon and Betty Moore Foundation).

Protect University Resources
• Proposed a new University-wide password policy to the HUIT Security Organization in order to standardize password strength and expiration requirements.
• Drafted a cloud security architecture with the HUIT Security Organization to provide Level 4 security assurance for application deployments using Amazon Web Services.
• Refreshed the AUTH and HU LDAP software and infrastructure to current, supported versions.
• Certified as an InCommon Bronze Identity Provider.

Facilitate Technology Innovation
• Created a conceptual architecture for IAM services to be deployed within the Amazon’s offsite hosting facilities.
• Deployed the Connections directory to the AWS cloud.
The IAM program will be implemented according to the four strategic objectives, and work will be managed as a portfolio of 11 projects:

<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>Improves user account management processes by replacing outdated tools with a new, feature-rich solution that can be expanded for local use by interested Schools across the University.</td>
</tr>
<tr>
<td>Federation</td>
<td>Enables Harvard and non-Harvard users to collaborate and easily gain access to both internal and external applications and tools.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Reduces the number of user-information systems of record while expanding data model and user attributes stored in the central IAM identity repository — enabling quick, consistent, appropriate access across LDAP, AD, and web authentication protocols.</td>
</tr>
<tr>
<td>App Portal</td>
<td>Enables Harvard application owners to learn about and easily integrate applications and software services with central IAM services.</td>
</tr>
<tr>
<td>One-Way Federation</td>
<td>A series of authentication releases and school onboarding efforts that provide Harvard users the flexibility to access applications and services using the credential of their choice.</td>
</tr>
<tr>
<td>Identity &amp; Access Governance</td>
<td>Delivers visibility into IAM program metrics — including in time business intelligence capabilities such as advanced reporting and trend analysis — in support of security requirements.</td>
</tr>
<tr>
<td>Authentication Enhancements</td>
<td>Provides users with a simplified login experience, as well as enhanced security options for sensitive data and applications.</td>
</tr>
<tr>
<td>Authorization Enhancements</td>
<td>Provide application owners and administrators with the ability to manage users via access groups, as well as the ability to manage authorization rules for access to applications or software services.</td>
</tr>
<tr>
<td>External Directories</td>
<td>Securely exposes user identity information inside and outside of the University.</td>
</tr>
<tr>
<td>Expanded Provisioning</td>
<td>Enables identity creation and proofing for non-person users.</td>
</tr>
<tr>
<td>Cloud Migration</td>
<td>Provides the University with a cloud reference architecture for Harvard application deployments, including migrating IAM services from on-premise hosting to Amazon Web Services.</td>
</tr>
</tbody>
</table>