Identity and Access Management
Technical Oversight Committee

July 31, 2014  Thursday  3-4 P.M.  6 Story Street, Ground Floor
Agenda

• Meeting Purpose and Intended Outcome
• Approval of Previous Minutes
• Chair’s Report
• Shared Topics of Interest: SailPoint IIQ Technical Overview
• Shared Topics of Interest: Revised IAM Password Policy
• Survey Results: Technical Oversight Committee Meeting Topics
• General Discussion
Meeting Purpose and Intended Outcome

Purpose

• Present latest status of program plan adjustments resulting from changes to the Collaboration Program/Office 365 and revised SailPoint foundation release date

• Present and discuss a technical overview of SailPoint IIQ

• Present changes to IAM password policy

Intended Outcome

• An understanding of SailPoint IIQ to bring back to your organizations

• Familiarity with changes to IAM password policy
Approval of Previous Minutes

May 15 Meeting

- Status updates: InCommon, cloud migration, dashboard review, O365 single-tenant review
- “Get Started” section on IAM site
- Find Person and Create/Manage ID
- Team priorities shifted toward accelerated provisioning

- **Action Item:** App portal is available and deployed internally; need to implement additional security and audit requirements before piloting

- **Action Item:** Committee materials distributed prior to meetings
Chair’s Report: Change in Focus to the Collaboration Program

In order to meet revised requirements, the three IAM teams will prioritize development efforts for the Provisioning and Directory Services projects until December 2015. Overall schedule impact slides can be found in Appendix B.

Benefits

- SailPoint IIQ to allow for automated provisioning/deprovisioning across the University for ~35,000 users
- Future IAM releases will be less complex due to centralized user population, and will allow for improved user experience for IAM services and HUIT shared services
- New onboarding and account management features will be delivered earlier in the schedule
- The ability for users to find contact and calendar (free/busy) information across participating Harvard schools will be advanced by six months

Impact

- Cloud Migration project work will continue in order to realize projected infrastructure savings
- Decommissioning of PIN3 will be advanced in order to realize projected infrastructure savings
- SSN Truncation project work will continue in order to mitigate unnecessary security exposure
- Project work to support SIS and Alumni releases will continue
- Delays to most release work in all other projects due to resource constraints and new priorities
Chair’s Report: July Executive Meeting Notes

The SailPoint IIQ foundation release has been postponed to August 16.

The Cause

- A race condition is created by IdDB changes processed into IIQ while changes are being made in FAS and University AD
- This condition was found late in integration testing

The Solution

- Communicate the need to migrate direct access to a SailPoint IIQ-managed approach to impacted AD system administrators
- Design and develop additional interfaces for direct and batch updates into University AD
- Work in collaboration with Unified Communications to update O365 processes and scripts
- Define and execute coordinated test cases
- Prepare support documentation and train the University AD community and HUIT Help Desk staff
- Reschedule production go-live through change management process
Chair’s Report: July Executive Meeting Notes

Although minor delays will take place as a result of delaying the provisioning release, larger overall timelines will not be affected.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Impact</th>
<th>Plan Date</th>
<th>New Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Services</td>
<td>Identity APIs</td>
<td>QA Resource contention</td>
<td>Delay to Find Person service deployment</td>
<td>August 2014</td>
<td>September 2014</td>
</tr>
</tbody>
</table>
Chair’s Report: Program Status

Download the latest executive status dashboard at iam.harvard.edu/resources

Current Program Status:

- The team is making progress against a remediation plan that includes additional functionality intended to replace the need to edit user accounts via AD
- Anticipated go-live date of the foundation release is August 16
- Timeline shift has no significant impact on the SailPoint expansion (Office 365) release
Shared Topics of Interest: SailPoint IIQ Technical Overview

- What is SailPoint IIQ?
- Workflow
- SailPoint IIQ Overview and Demo
- Upcoming Releases
- Future Functionality
SailPoint IIQ Technical Overview: What is SailPoint?

- SailPoint IdentityIQ (IIQ) is a fully functional Identity Management System
- Information is gathered across all connected applications to create an Identity Cube, which includes all attributes related to all the connected applications
- Business logic can be defined programmatically via BeanShell
- SailPoint IIQ itself is a .war file that can be deployed into a Tomcat server
- Development of rules or custom connectors can be done in IntelliJ/netbeans/Eclipse IDEs
- RESTful APIs exist to integrate custom applications with IIQ — one example is our new Claim Account application
- Online resources for learning more:
  - IIQ Support community portal with good training materials and programmer resources
  - IdentityIQ product overview and brochure
SailPoint IIQ Technical Overview: What is SailPoint?

IAM Services and Solution Modules
- Single Sign-On
- Password Management
- Access Certification
- Access Request & Provisioning
- Advanced Policy & Analytics

- Compliance Manager
- Lifecycle Manager
- Access Manager

Unified Governance Platform
- Policy Model
- Role Model
- Identity Warehouse
- Risk Model
- Workflow Engine

Open Connectivity Foundation
- Resource Connectors
- Provisioning Integration
- Service Desk Integration
- Cloud Gateway

SaaS
SailPoint IIQ Technical Overview: Workflow
Let’s see firsthand how it works.
SailPoint IIQ Technical Overview: Upcoming Releases

Foundation

- Identity Cubes created from data in IDDB
- Configured applications (endpoints) aggregated and correlated to Identity Cubes
- Assignment of role based on certain attributes triggers provisioning to University AD
- Changes to selected attributes in University AD via batch or web interface within IIQ

Near-Term

- Claiming application written in Java/Spring environment communicates to IIQ via RESTful interface
- Provisioning to additional connectors through IIQ:
  - Google Apps (University/College)
  - School-specific Active Directories/LDAP
  - FAS:
    - HomeDIR (Home Directories)
    - Kerberos (Unix password management)
    - FAS LDAP
    - FAS AD
    - FASMAIL
- Provisioning/updates to these applications governed by birthright roles
SailPoint IIQ Technical Overview: Future Functionality

- Replacement of FIM with IIQ for provisioning of Office 365
- Configuration of identities and management of access to additional shared applications such as Jira or Salesforce
- General availability of IIQ GUI (end-user access)
  - Example: Manage Access windows, where people can request access to applications and app managers can review and accept/deny requests
- Access governance available via reports and analysis based on others in a particular group
  - Example: When a staff member changes roles, locations, or departments, access rights can be adjusted based on comparisons with others and/or general group rights
Shared Topics of Interest: Revised IAM Password Policy

Harvard IT Security Policy includes provisions on acceptable default password policies. The policy remains under review and has not yet been ratified. The unpublished draft includes three possible approaches:

- 8 characters with annual expiration
- 10 characters with no expiration
- Multi-factor

There are additional points that need to be considered with each approach.

As we plan deployment and updates to HUIT services, selecting the most appropriate password policy is an important consideration. Pending the outcome and final publication, IAM will be utilizing a 10-character password without expiration.
### Revised IAM Password Policy: AD Example

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Length</td>
<td>10</td>
</tr>
<tr>
<td>Password Complexity Requirements</td>
<td>Windows complexity</td>
</tr>
<tr>
<td>Force Password Change Frequency</td>
<td>None</td>
</tr>
<tr>
<td>Minimum Password Age</td>
<td>0 days</td>
</tr>
<tr>
<td>Lockout on Failed Login Attempts</td>
<td>Yes</td>
</tr>
<tr>
<td>Lockout on Number of Attempts During Period</td>
<td>20 attempts in 10 minutes</td>
</tr>
<tr>
<td>Lockout Duration</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Number of Previous Passwords Remembered</td>
<td>5</td>
</tr>
<tr>
<td>Store Passwords Using Reversible Encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Survey Results: Technical Oversight Committee Meeting Topics

“My stuff is so dependent upon IAM, I want to know all about it. And the technology you are using is stuff I want to know about too.”

Key topic areas:

- Migration to the cloud; cloud topics in general
- SailPoint/Provisioning (Discussed in this session)
- Find Person API/identity creation and related authentication
- Overall IAM service offerings

Please continue to send us your requests for meeting topics!
General Discussion
Appendix A
Technical Oversight Committee Members
# Technical Oversight Committee Members

**Chair:** Magnus Bjorkman, Director of IAM Engineering

<table>
<thead>
<tr>
<th>Name</th>
<th>School/Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steve Duncan</td>
<td>Harvard Kennedy School</td>
</tr>
<tr>
<td>Tyson Kamikawa</td>
<td>Harvard Medical School</td>
</tr>
<tr>
<td>Sherif Hashem</td>
<td>Harvard Law School</td>
</tr>
<tr>
<td>Indir Avdagic</td>
<td>SEAS</td>
</tr>
<tr>
<td>Ken Ho</td>
<td>GSE</td>
</tr>
<tr>
<td>Jake Yerdon</td>
<td>HSPH</td>
</tr>
<tr>
<td>David Faux</td>
<td>HUIT Admin Tech/FAS &amp; College</td>
</tr>
<tr>
<td>Jonah Pollard</td>
<td>Unified Communication/Cloud</td>
</tr>
<tr>
<td>Tim Gleason</td>
<td>HUIT IAM/AD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>School/Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carolyn Brzezinski</td>
<td>SIS</td>
</tr>
<tr>
<td>Sara Sclaroff</td>
<td>HUIT Admin Tech/HR</td>
</tr>
<tr>
<td>Rich Ohlsten</td>
<td>HUIT Admin Tech/Alumni</td>
</tr>
<tr>
<td>Colin Murtaugh</td>
<td>HUIT Academic</td>
</tr>
<tr>
<td>Dan Fitzpatrick</td>
<td>Partners</td>
</tr>
<tr>
<td>Eileen Flood</td>
<td>Campus Services</td>
</tr>
<tr>
<td>Randy Stern</td>
<td>Library IT</td>
</tr>
<tr>
<td>Micah Nelson</td>
<td>HUIT Security</td>
</tr>
</tbody>
</table>
## Program Plan Schedule Impact: Provisioning

Adjustments to the Provisioning project enable the IAM program to implement accelerated user management and provisioning across Schools.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>New Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>HUIT Expansion Role TransitionExpanded Provisioning</td>
<td>Combine and rename release “Expansion (Office 365)” and track 0365 milestones within this updated release.</td>
<td>December 2016</td>
<td>August 2015</td>
<td>Delivery date for functionality significantly improved. Scope of prior releases still achievable, including updates for POI.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>PIN/AD Credentials Management</td>
<td>Give end users the ability to use Active Directory credentials for any PIN-protected system or application they are permitted to access.</td>
<td>August 2015</td>
<td>November 2015</td>
<td>Delay new functionality.</td>
</tr>
</tbody>
</table>
**Program Plan Schedule Impact: Federation**

Adjustments to the Federation project reflect a reduced need for federation resulting from the move to a single Office 365 tenant.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>New Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation</td>
<td>idP Functionality Expansion</td>
<td>Incorporate additional attributes and profiles into Identity Provider in order for partners to gain access to expanded services and resources.</td>
<td>November 2014</td>
<td>May 2015</td>
<td>Low volume of demand. Partners continue customization of their applications to use legacy protocols.</td>
</tr>
<tr>
<td>Federation</td>
<td>Federation for Hospitals</td>
<td>Allow hospital credentials to be used to access University resources.</td>
<td>June 2016</td>
<td>November 2016</td>
<td>Use cases and ongoing discussions with HMS will continue. Pilot with Partners targeted as an interim step.</td>
</tr>
</tbody>
</table>
Program Plan Schedule Impact: Directory Services/External Directories

Adjustments to the Directory Services and External Directories projects reflect delays to LDAP consolidation and enhancement, with no impact to end users resulting from the prioritization of accelerated provisioning.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>New Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Services</td>
<td>Consolidated LDAP</td>
<td>Collapse HU and Auth LDAP attributes in the cloud</td>
<td>February 2015</td>
<td>May 2015</td>
<td>No impact to new or existing users. Delay improvements for new application set-up and integration.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>LDAP Functional</td>
<td>Expand attributes to provide clearer role and affiliation information, and incorporate standard attributes to support federation</td>
<td>July 2015</td>
<td>October 2015</td>
<td>Delay new functionality.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Identity APIs</td>
<td>Create utility and additional APIs to enable identity administration for UUIDs to support expanded school provisioning.</td>
<td>New</td>
<td>November 2015</td>
<td>New release required to support accelerated provisioning.</td>
</tr>
<tr>
<td>External Directories</td>
<td>Expose LDAP Directory Data</td>
<td>Expose enhanced LDAP directory data through alternative protocols to fit application needs (e.g., SAML, CAS, AD)</td>
<td>September 2015</td>
<td>April 2016</td>
<td>Delay new functionality.</td>
</tr>
</tbody>
</table>
Program Plan Schedule Impact: App Portal

The App Portal project is a discrete track providing new functionality to University application owners who wish to more efficiently integrate with IAM. Delivering the new functionality needed to support accelerated provisioning will incur a delay.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>New Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Portal</td>
<td>Application Registration</td>
<td>Enable application owners to register their applications with IAM</td>
<td>July 2014</td>
<td>Complete</td>
<td>Internal release delivered. Application teams to continue consultation with the IAM team for registration.</td>
</tr>
<tr>
<td>App Portal</td>
<td>IAM Reference Implementation</td>
<td>Expand the App Portal to include examples of reference implementations of pre-developed code</td>
<td>February 2015</td>
<td>January 2016</td>
<td>Delay new functionality. Continue consulting with the IAM team for set-up and integration needs.</td>
</tr>
</tbody>
</table>
The need for One-Way Federation is greatly reduced due to the decision to move to a single Office 365 tenant.

<table>
<thead>
<tr>
<th>Project</th>
<th>Release</th>
<th>Description</th>
<th>Plan Date</th>
<th>New Date</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-Way Federation</td>
<td>OWF Onboarding</td>
<td>Expand school targets for OWF</td>
<td>February 2015</td>
<td>Remove</td>
<td>Bridging strategy of OWF is no longer required due to accelerated provisioning. If need exists for HBS, new release will be created under Federation Project.</td>
</tr>
<tr>
<td>One-Way Federation</td>
<td>Credential Mapping</td>
<td>Incorporate additional users from schools and departments into the identity store with local user credentials.</td>
<td>November 2014</td>
<td>Remove</td>
<td>Identity API release within the Directory Service project will deliver this capability.</td>
</tr>
<tr>
<td>One Way Federation</td>
<td>OWF Onboarding for HBS</td>
<td>Proposed release for HBS OWF integration with IAM.</td>
<td>New</td>
<td>April 2016</td>
<td>HBS-specific OWF work tentatively planned.</td>
</tr>
</tbody>
</table>