



**HARVARD UNIVERSITY**

Information Technology

IDENTITY & ACCESS MANAGEMENT

# **Identity and Access Management PI-2 Demo**

March 10, 2015

Tuesday

11:00a.m.-12:00 p.m.

Lamont Forum Room

# Agenda

- Meeting Purpose and Intended Outcomes (5 min)
- PI-2 Business Objectives (5 min)
- Demo: Alumni Imported from Advance to Identity Registry (5 min)
- Demo: Alumni Registration Using HarvardKey Application (10 min)
- Demo: Alumni Authentication to Manage HarvardKey (10 min)
- Summary and Close

# **Demonstration: Program Increment Accomplishments**

## **Purpose**

To provide the team and invited guests a summary and demonstration of key work accomplished during our second Program Planning Increment (PI-2).

## **Intended Outcomes**

- Share our work in PI-2 and provide a forum for stakeholder feedback
- Continue to build an understanding of the IAM program

## PI-2 Business Objectives

Teams accomplished the following objectives:

Objective	Demonstration
Implement data migration method for Alumni data	<ul style="list-style-type: none"><li>• Import Alumni data into Identity Registry (IdDB) using Identity API</li></ul>
Allow migrated Alumni users to claim and manage their HarvardKey credentials	<ul style="list-style-type: none"><li>• Self-service alumni registration for a new HarvardKey</li><li>• Provision an account and password to credential repository (H-LDAP)</li></ul>
Support Alumni authentication using HarvardKey	<ul style="list-style-type: none"><li>• Authenticate Alumni user via HarvardKey</li></ul>

## PI-2 Business Objectives

Teams accomplished the following objectives:

Objective	Accomplishment
Replace FAS account management and provisioning so that we can decommission Oracle Waveset	Self-service ... <ul style="list-style-type: none"><li>• Password change</li><li>• Password reset</li><li>• Update password recovery email</li></ul>
Retire technical debt to speed future development	<ul style="list-style-type: none"><li>• PIN/CAS to the cloud</li></ul>

## PI-2 Business Objectives

Teams also met these additional commitments:

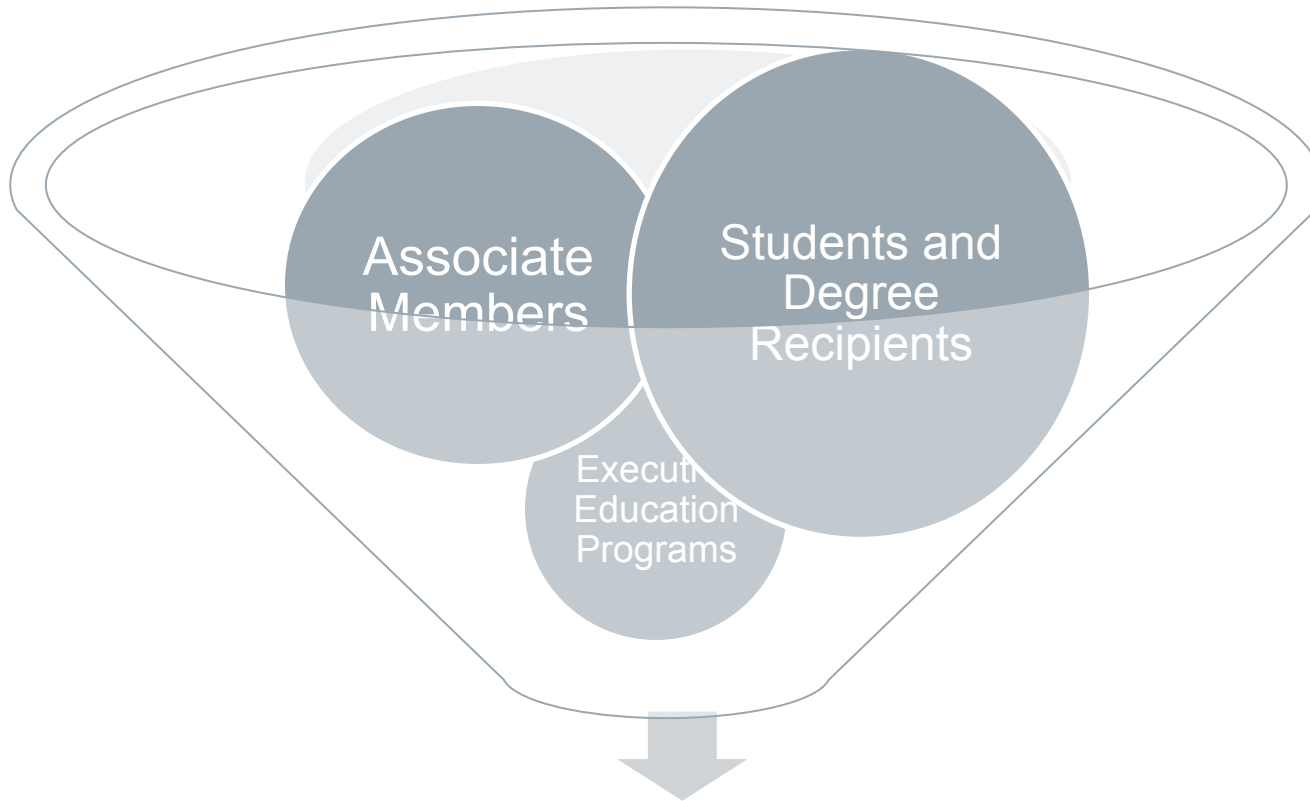
Objective	Accomplishment
Upgrade SHA algorithm to remain compliant with InCommon Bronze standards	<ul style="list-style-type: none"><li>• Upgrade to SHA-2 without any interruption to customer applications</li></ul>
Migrate off Oracle Access Manager (PIN3)	<ul style="list-style-type: none"><li>• Decommissioned servers in order to save \$100K</li></ul>
Implement new Google API before new students onboard	<ul style="list-style-type: none"><li>• Deployed Waveset changes for new Google API design</li></ul>
Capture HMS functional and technical requirements to facilitate further planning of the School's migration to SailPoint IIQ	<ul style="list-style-type: none"><li>• Extensive requirements-gathering work from Marlena Erdos</li></ul>

## Refresher: Identity Registry is the Foundation

- Data are generated by source systems of record and fed to the Identity Database (IdDB), which is an *identity registry*
- IdDB has a master data record of the Harvard user — a source of truth
- SailPoint IdentityIQ (IIQ) aggregates source data on a continuous basis
- Based on eligibility rules determined by the service owner, the provisioning system automatically activates and deactivates individual users and their entitlements
- This streamlines onboarding — and, even more importantly, turns off access when a person separates from Harvard or otherwise loses eligibility

**The right access, for the right people, in a timely manner**

# Various Alumni Populations Comprise the User Base



More than 380,000 Alumni

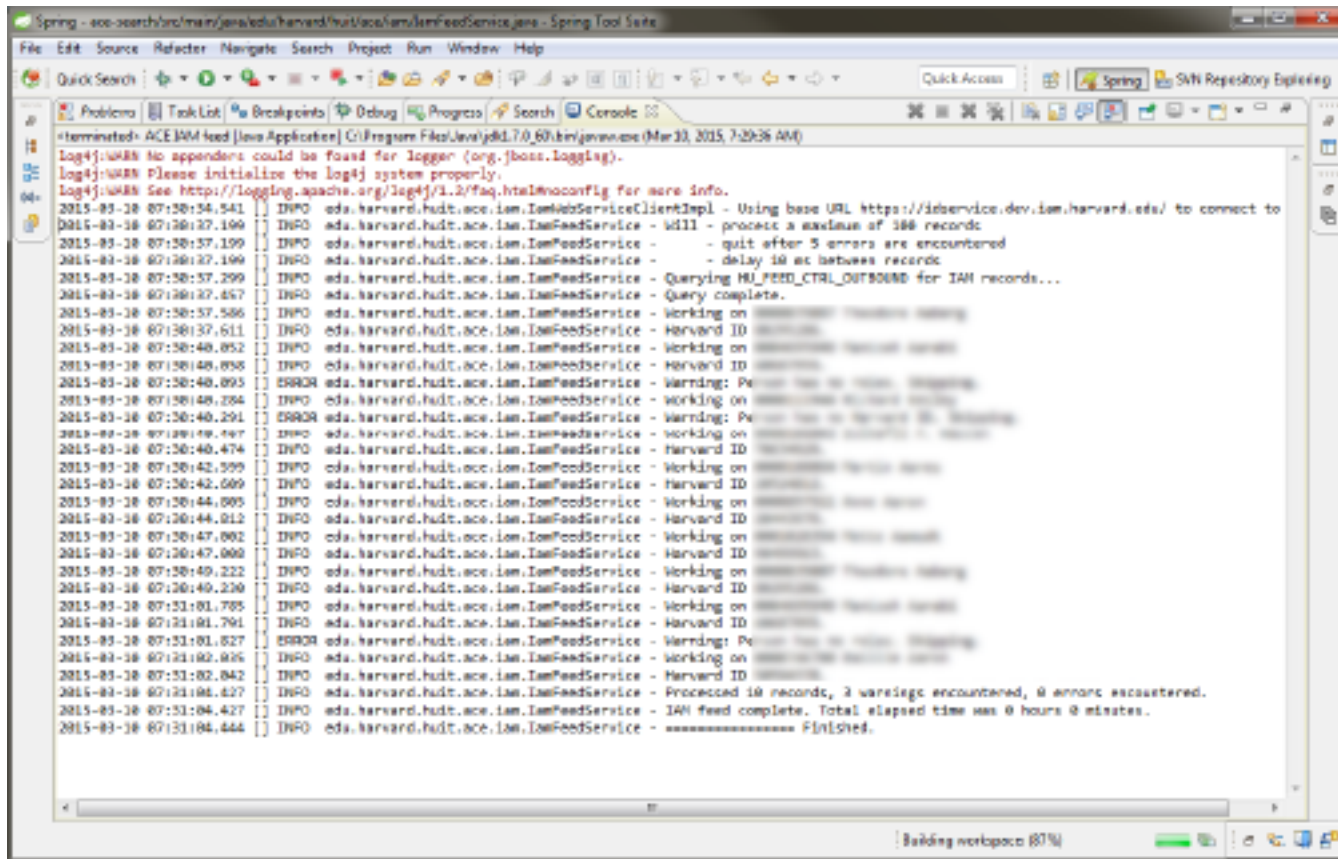
## Alumni Data Being Submitted to Identity API

- Alumni data are managed in HAA's Advance database
- Alumni data will be fed to the identity registry (IdDB) to enable Alumni to get a HarvardKey for login to Harvard resources
- New API-based approach to implementing business rules for data creation in the IdDB identity registry will be employed for import of Alumni data (instead of batch XML imports)
  - Only the data needed to manage access and support users will be transferred to the registry
  - The transition from graduating student to Alumni should be seamless
  - API enables a more near-real-time data transfer if required

# **Demo: Scripted Update from Advance to IdDB**

Mike Thomas, HUIT/Administrative Systems

# Recap: Scripted Update from Advance to IdDB



```
terminated> ACE IAH feed [Java Application] C:\Program Files\Java\jdk1.7.0_60\bin\java.exe (Mar 23, 2015, 7:29:26 AM)
log4j:WARN No appenders could be found for logger (org.jboss.logging).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
2015-03-20 07:30:34.541 INFO edu.harvard.hudt.ace.iam.IamFeedServiceClientImpl - Using base URL https://idservice.dev.iam.harvard.edu/ to connect to
2015-03-20 07:30:37.199 INFO edu.harvard.hudt.ace.iam.IamFeedService - id111 - process a maximum of 100 records
2015-03-20 07:30:37.199 INFO edu.harvard.hudt.ace.iam.IamFeedService - - quit after 5 errors are encountered
2015-03-20 07:30:37.199 INFO edu.harvard.hudt.ace.iam.IamFeedService - - delay 10 ms between records
2015-03-20 07:30:37.299 INFO edu.harvard.hudt.ace.iam.IamFeedService - Querying HUL_FEED_CTRL_OUTBOUND for IAH records...
2015-03-20 07:30:37.457 INFO edu.harvard.hudt.ace.iam.IamFeedService - Query complete.
2015-03-20 07:30:37.586 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:37.611 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:40.052 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:40.058 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:40.095 ERROR edu.harvard.hudt.ace.iam.IamFeedService - Warning: Pe
2015-03-20 07:30:40.284 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:40.291 ERROR edu.harvard.hudt.ace.iam.IamFeedService - Warning: Pe
2015-03-20 07:30:40.474 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:40.474 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:42.599 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:42.609 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:44.095 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:44.012 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:47.002 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:47.000 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:30:49.222 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:30:49.230 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:31:01.795 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:31:01.791 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:31:01.827 ERROR edu.harvard.hudt.ace.iam.IamFeedService - Warning: Pe
2015-03-20 07:31:02.035 INFO edu.harvard.hudt.ace.iam.IamFeedService - Working on
2015-03-20 07:31:02.042 INFO edu.harvard.hudt.ace.iam.IamFeedService - Harvard ID
2015-03-20 07:31:04.427 INFO edu.harvard.hudt.ace.iam.IamFeedService - Processed 10 records, 2 warnings encountered, 0 errors encountered.
2015-03-20 07:31:04.427 INFO edu.harvard.hudt.ace.iam.IamFeedService - IAH feed complete. Total elapsed time was 0 hours 0 minutes.
2015-03-20 07:31:04.444 INFO edu.harvard.hudt.ace.iam.IamFeedService - ***** Finished.
```

- Scripted submission allows control over submission rate and automates error thresholds
- Messages returned through API provide feedback on transactions

## Next: Alumni Online Access Will Require HarvardKey

- Access to many Harvard resources is protected and requires login (authentication)
- The current vendor-based solution for issuing Alumni credentials is being sunsetted, and Harvard is building all the components needed to bring this process “in house”
- As part of this major transition, we need to register Alumni again so they can set secure passwords and provide information to support self-service password management
- The new HarvardKey self-service application will support Alumni registration

# **Demo: Alumni Registration for HarvardKey**

Joe Hardin, HUIT/IAM Team

## Recap: Registering for an Alumni Account

### **We saw:**

- New self-service registration process for Alumni to claim HarvardKey credentials

### **Benefits:**

- In the future, students with a HarvardKey will no longer need to re-register as Alumni
- No more confusing security questions for Alumni – simple password reset over email

# Recap: Registering for an Alumni Account

HARVARD UNIVERSITY HOME

Alumni Identity Information

Please enter your personal information so we can verify you in our system.

HAA ID

Last Name

First Name

Year of Graduation

Clear Submit

HARVARD UNIVERSITY HOME

Create Login Name

Please enter your desired login name. The login name you entered should be in an email address like format.

Login Name

Clear Submit

## Recap: Login Name Provisioned by IIQ

### We saw:

- Login name assigned by or entered with HarvardKey application
  - IIQ automatically provisions the password to back-end systems (Harvard LDAP in the case of HarvardKey)

### Benefits:

- Best of both worlds — a customer-facing user interface integrated with a powerful provisioning solution

# Recap: IIQ Updated Based on Alumni Registration

Dashboard Define Monitor Analyze Manage System Setup

## View Identity iamalumsixfn iamalumsix

Attributes Entitlements Application Accounts Policy History Risk Activity User Rights Events

Edit

Login Name	test-account@mail.com
ADID	iai431
Display Name	iamalumsixfn iamalumsix
FAS User Name	
Display Name Prefix	
Display Name First	iamalumsixfn
Display Name Middle	
Display Name Last	iamalumsix
Display Name Suffix	
Official Name	iamalumsixfn iamalumsix
Birth Date	6/29/1990 0:0:0 AM EDT
DOB Month	6
DOB Day	29
DOB Year	1990
Claim Status	CLAIMED
Recovery Primary Email	iamharv.test@gmail.com
Recovery Alternate Email	
Recovery Primary Phone	
Recovery Alternate Phone	

# Recap: H-LDAP Updated with New Password

The screenshot shows the Active Directory Users and Groups console. On the left, a tree view shows LDAP servers under 'Connections'. The 'Hldap' folder is expanded, and 'h-ldap-dev (LDAPS)' is selected. The main pane displays the details for the user 'iamalumsix'. Three red circles with numbers 1, 2, and 3 highlight specific fields: 'mail', 'userPassword', and 'harvardEduClaimStatus'.

sn	iamalumsix
displayName	iamalumsixfn iamalumsix
eduPersonUniqueId	65fba95a99c94e5180eb2b4bdcfb83b1
givenName	iamalumsixfn
harvardEduADID	iai431
harvardEduDisplaySortName	IAMALUMSIX IAMALUMSIXFN
harvardEduFerpaPastStudentIn...	FALSE
harvardEduFerpaStatus	FALSE
harvardEduIDCardNumber	40965548
harvardEduIDNumber	40965548
harvardEduPersonaNonGrata	FALSE
harvardEduUUID	65fba95a99c94e5180eb2b4bdcfb83b1
mail	test-account@mail.com
o	Harvard University Core
uid	iai431
userPassword	SSHA512 hashed password
createTimestamp	Mar 9, 2015 1:16:28 PM EDT (20150309171628Z)
creatorsName	uid=iiq,ou=ldap-apps,dc=harvard,dc=edu
entrydn	uid=iai431,ou=people,dc=harvard,dc=edu
entryid	57
harvardEduClaimStatus	CLAIMED (2015-03-09T14:00:50.642 EDT)
hasSubordinates	FALSE
modifiersName	uid=iiq,ou=ldap-apps,dc=harvard,dc=edu
modifyTimestamp	Mar 9, 2015 2:00:56 PM EDT (20150309180056Z)
nsUniqueId	f0241405-c67f11e4-aa8ed686-2fdb7127
numSubordinates	0
parentid	5
passwordGraceUserTime	0
passwordRetryCount	0
pwdUpdateTime	Mar 9, 2015 2:00:56 PM EDT (20150309180056Z)
subschemaSubentry	cn=schema

## **Next: HarvardKey - A Better Self-Service Experience**

**The HAA Helpdesk fields thousands of calls a year for forgotten user names and passwords.**

The HarvardKey application supports self-service for these routine interactions:

- I want to update my recovery email or phone number
- I need to change my password
- I have forgotten my login name
- I have forgotten my password and need to reset it

# **Demo: Login to Manage HarvardKey**

Joe Hardin, HUIT/IAM Team

## Recap: Alumni Managing HarvardKey (Self-Service)

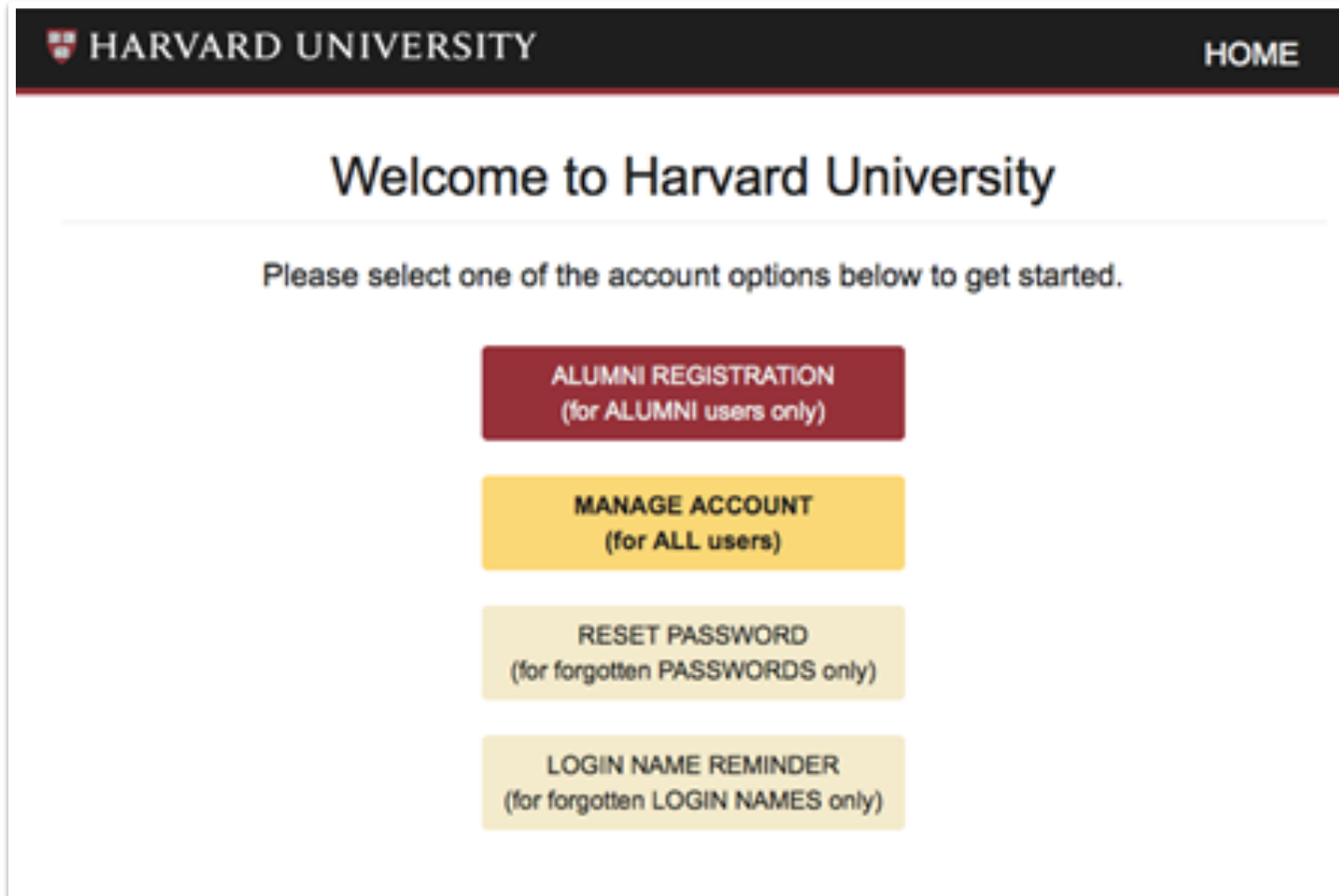
### We saw:

- Logging into HarvardKey application to manage a HarvardKey
  - Authentication with HarvardKey integrated with PIN/CAS


### Benefits:

- Self-service that doesn't rely on security questions or defunct Harvard email addresses

# Recap: Alumni One Option in HarvardKey App



# Recap: Entering an Additional Recovery Email

 HARVARD UNIVERSITY HOME

## WELCOME TO HARVARD ACCOUNT MANAGEMENT

Please provide the information below that you wish to manage.

**Recovery Information**

In case you ever forget the user name and/or password, the information you provide will be used to recover your Harvard University account.

You must provide at least your primary email address for recovering your Harvard University account.

EMAIL ACCOUNTS

**Primary:**

**Alternate:**

# Recap: Viewing the Updates in IIQ and H-LDAP

**View Identity iamalumsixfn iamalumsix**

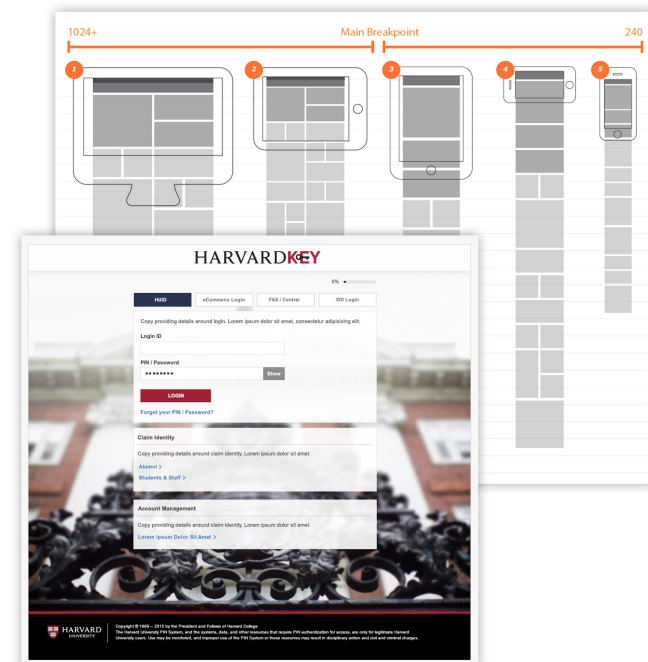
Attributes Entitlements Application Accounts Policy History Risk Activity User Rights Events

Edit

Login Name	test-account@mail.com
ADID	iai431
Display Name	iamalumsixfn iamalumsix
FAS User Name	
Display Name Prefix	
Display Name First	iamalumsixfn
Display Name Middle	
Display Name Last	iamalumsix
Display Name Suffix	
Official Name	iamalumsixfn iamalumsix
Birth Date	6/29/1990 0:0:0 AM EDT
DOB Month	6
DOB Day	29
DOB Year	1990
Claim Status	CLAIMED
Recovery Primary Email	iamharv.test@gmail.com
Recovery Alternate Email	add_alternate@example.com
Recovery Primary Phone	
Recovery Alternate Phone	
Onboarding Email	

# Functionality Completed ... Facelift Pending

- Team has completed the core functionality
- Isobar will be delivering a build kit to Harvard at end of March, which will enable us to align the look and feel of the application with Harvard standards
  - Responsive design (works with different formats/devices)
  - Familiar navigation
  - Level A accessible
  - Nicer looking!



## Wrap-Up: Status of PI-2 Business Objectives

Today's demonstrations illustrated the following objectives:

- Data migration method for Alumni data being used by HAA
- Alumni registration process
- Authentication with HarvardKey using PIN/CAS
- Self-service HarvardKey features

## Other Accomplishments During PI-2

### **Cloud:**

- New Harvard LDAP (H-LDAP) deployed to the cloud
- PIN/CAS migrated to the cloud, ready for testing during PI-3

### **Platform Investment:**

- Database rationalization project
- PIN3 decommissioned
- SHA2 upgrades
- Upgrade for Google API

### **Preparing for Future Development:**

- Sponsored Account requirements analysis
- HMS system and requirements analysis

# Discussion

Questions? Feedback?

# Thank you!



HARVARD UNIVERSITY  
Information Technology