Introduction to Grouper

Chris Hyzer

University of Pennsylvania and Internet2

Bill Thompson

Unicon

Agenda

- Part I
  - Intro, basic concepts
  - Grouper Quickstart
- Part II
  - Grouper in Action @ Penn
  - Qualtrics, Confluence, Kuali,...
- Part III
  - Hands on Grouper
  - Folder, Groupers, Roles
  - Grouper Loader, Subject API,...

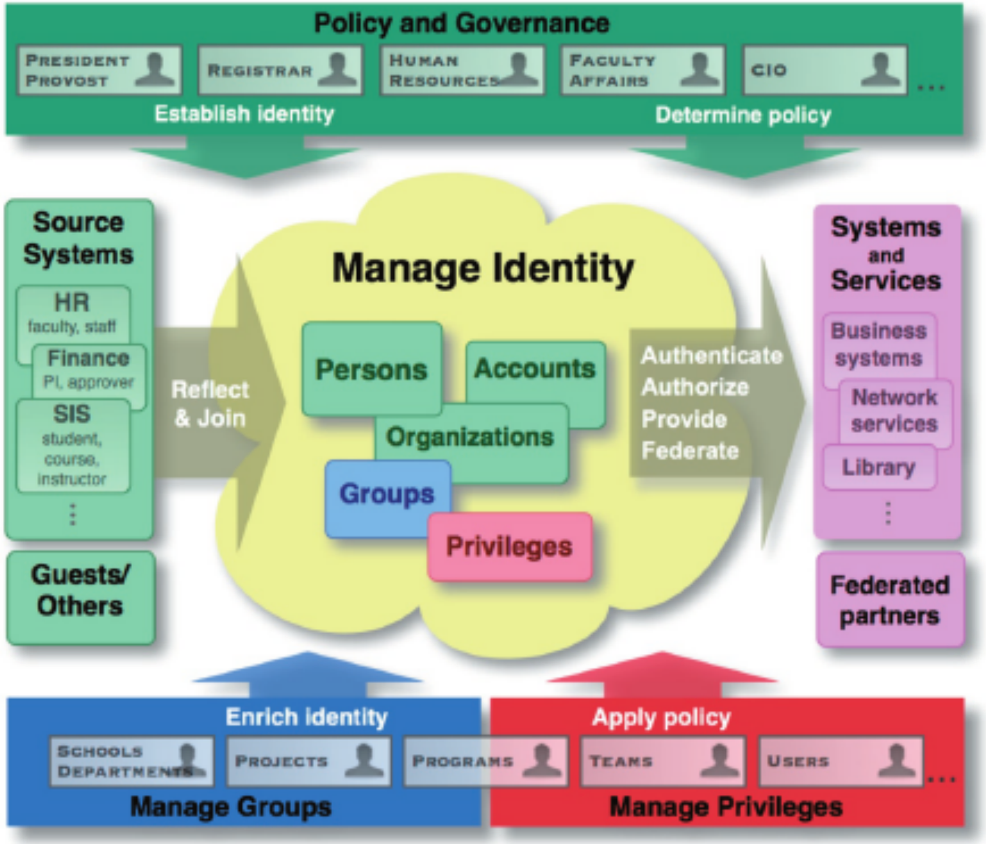
CIFER, Shib, CAS, OR, CPR, Grouper?

- Name, Role, Institution
- CAS? Shib? CAS/Shib?
- Person Registry? OR? CPR?
- Enterprise Directory? OpenLDAP? AD?
- Group/permission management today?

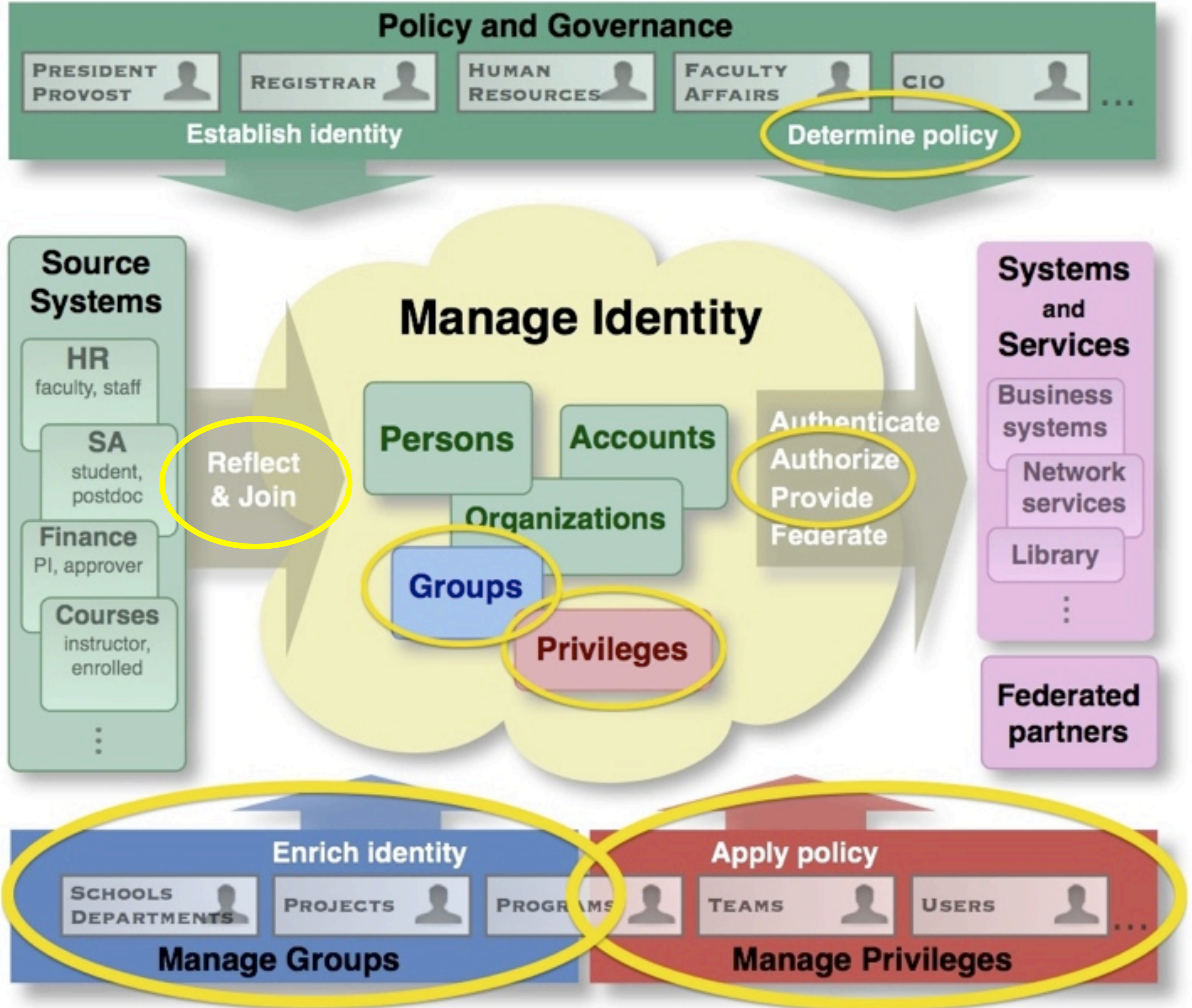
Identity & Access Management (IAM)

- Identity
  - You
- Authentication
  - Log in
- Authorization
  - What you can do
- Access management
  - Map policy & authority to authorization

Access management strategy



- Tools & processes to translate IAM concepts into typical campus environment
  - Which people?
  - What systems & business processes?
  - What policies?
  - What purposes?
  - Whose authority?



Policy and Governance

President Provost

Registrar

Human Resources

Faculty Affairs

CIO

...

Establish identity

Determine policy

Source Systems

HR faculty, staff

SA student, postdoc

Finance PI, approver

Courses instructor, enrolled

⋮

Reflect & Join

Manage Identity

Persons

Accounts

Organizations

Groups

Privileges

Authenticate

Authorize

Provide

Federate

Systems and Services

Business systems

Network services

Library

⋮

Federated partners

Enrich identity

Schools Departments

Projects

Programs

Manage Groups

Apply policy

Teams

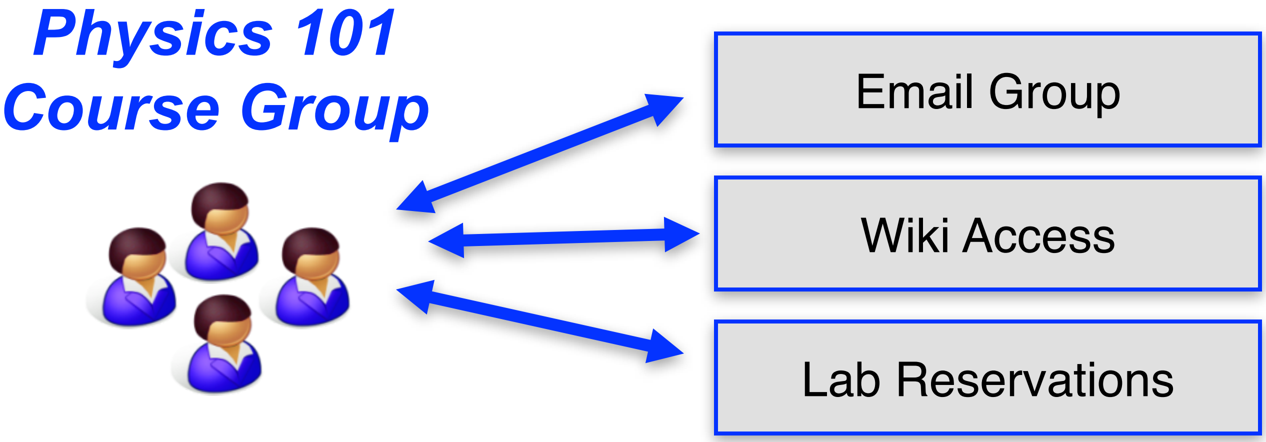
Users

...

Manage Privileges

Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify and make consistent by using the same group or role in many places

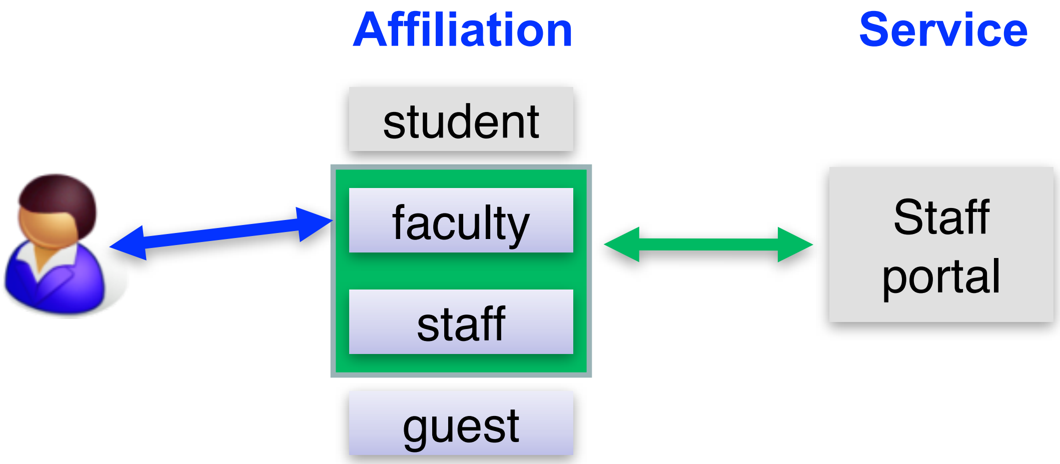


Additional benefits of access management

- Empower the right people to manage access. Take central IT out of the loop.
- See who can access what, with a report rather than a fire drill

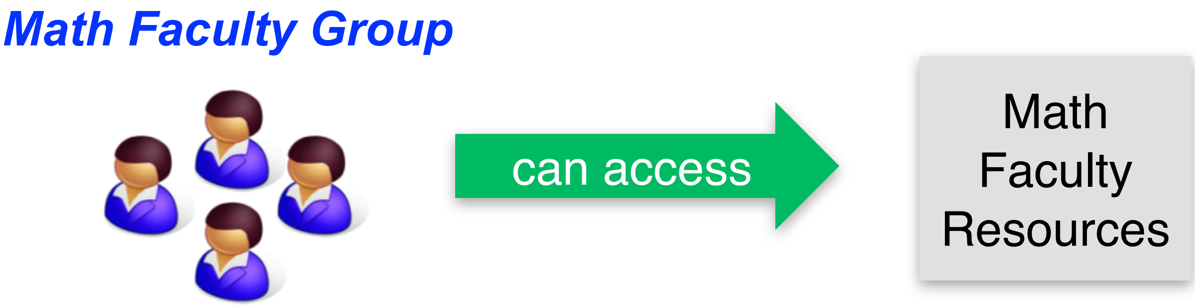
Access management stages: authorization > authentication

1. Start out using a single user attribute, *affiliation*, in LDAP or Active Directory. This lets services implement simple access policies.



Access management stages: authorization > authentication

2. Enrich & centralize access management with groups determined from systems of record
   - Courses, financial accounts, departments
   - Define service-specific access policies in the centralized access management system



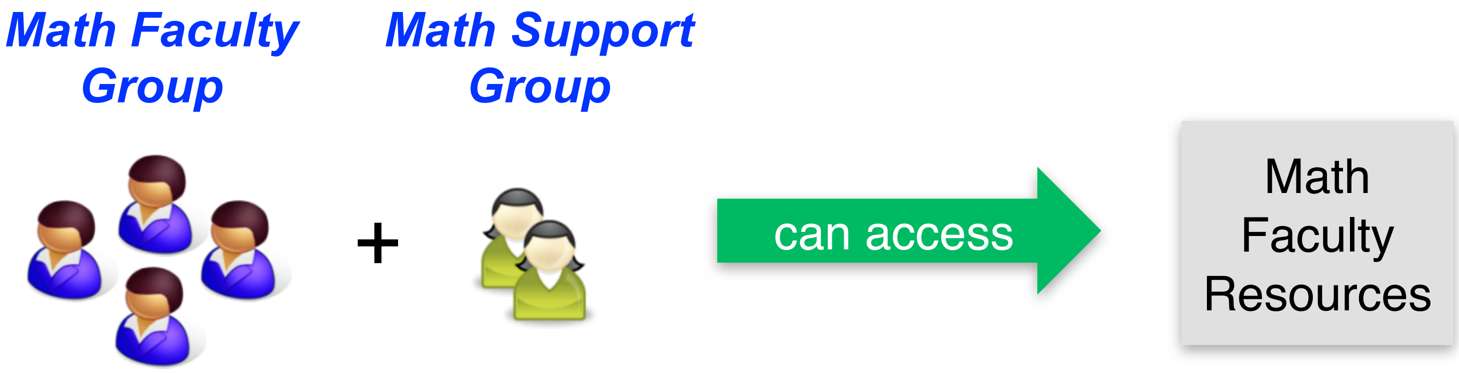
Math Faculty Group

can access

Math Faculty Resources

Access management stages: authorization > authentication

3. Get central IT out of the loop
    - Distributed management
    - Exceptions
    - Departmental applications



Math Faculty Group

+

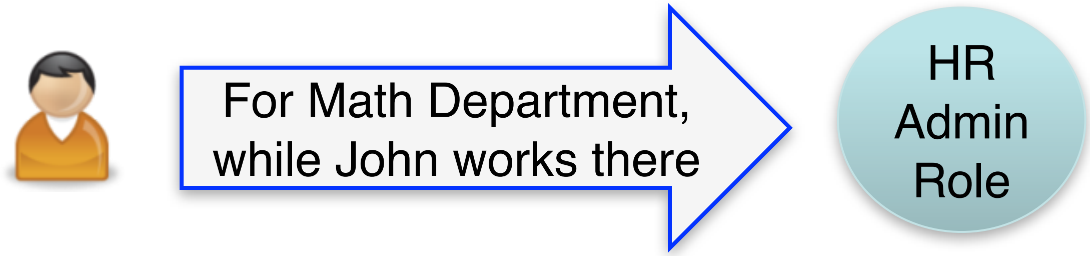
Math Support Group

can access

Math Faculty Resources

Access management stages: authorization > authentication

4. Increase integration of access management
   - Direct integration with applications using web services
     - SOAP/REST/ESB
   - Roles & privileges to support applications more deeply

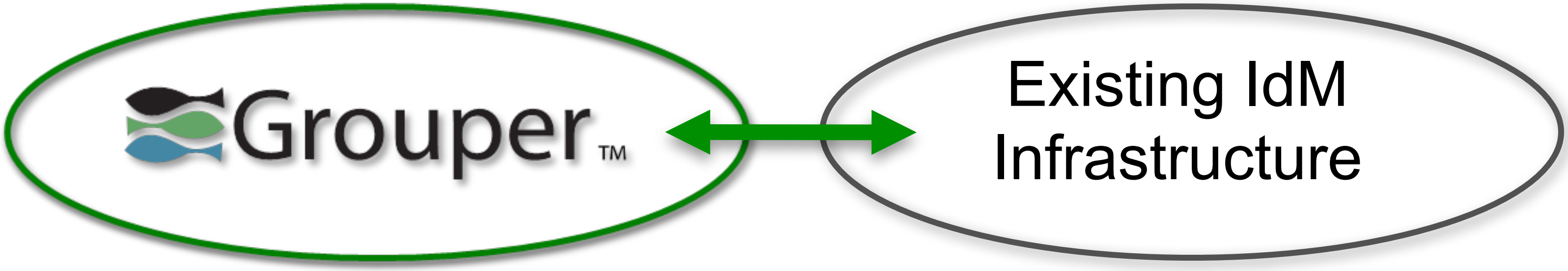


The Grouper Story

- Open source, community-driven project of the Internet2 Middleware Initiative
  - Initial release v0.5 in December 2004

The Grouper Story

- Key aims
  - Delegation and distributed management
  - Integration with most any existing Identity Management infrastructure



Existing IdM Infrastructure

The Grouper Story

- Grouper v2.X expanded beyond groups
  - Roles & permissions

HR-Admin

  - Rules

```
-  If
       removed from group A
-  then
        remove from group B
```

Contributing organizations, so far

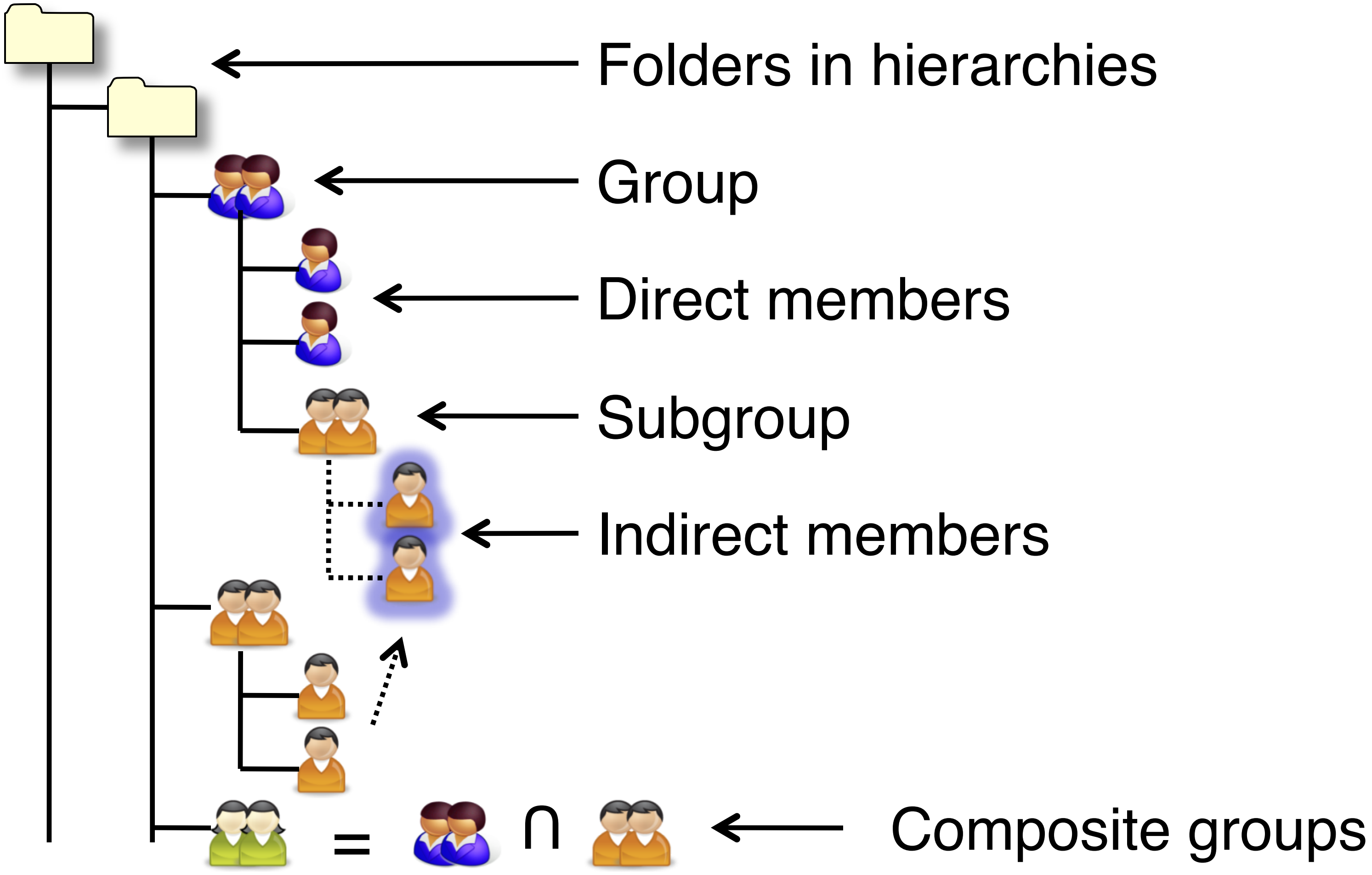
- Brown University
- California Polytech
- Cardiff University
- Campus Crusade for Christ International
- Cornell University
- Duke University
- Freie Universität Berlin
- GIP RECIA
- LIGO
- Newcastle University
- Northern Arizona University
- Ohio State University
- SURFnet
- University of Bristol
- University of Chicago
- University of Kansas
- University of Memphis
- University of Pennsylvania
- University of Washington
- University of West Bohemia

Latest addition to the community

UNICON®

- Unicon offers IT Services for Education, Specializing in Open Source
  - Cooperative Support Program for Grouper, Shibboleth, CAS, uPortal, uMobile, Sakai
  - Annual subscription, 4 levels, provides access to and funds dedicated support team who work directly with the open source projects

Grouper: core concepts


Folders in hierarchies

Group

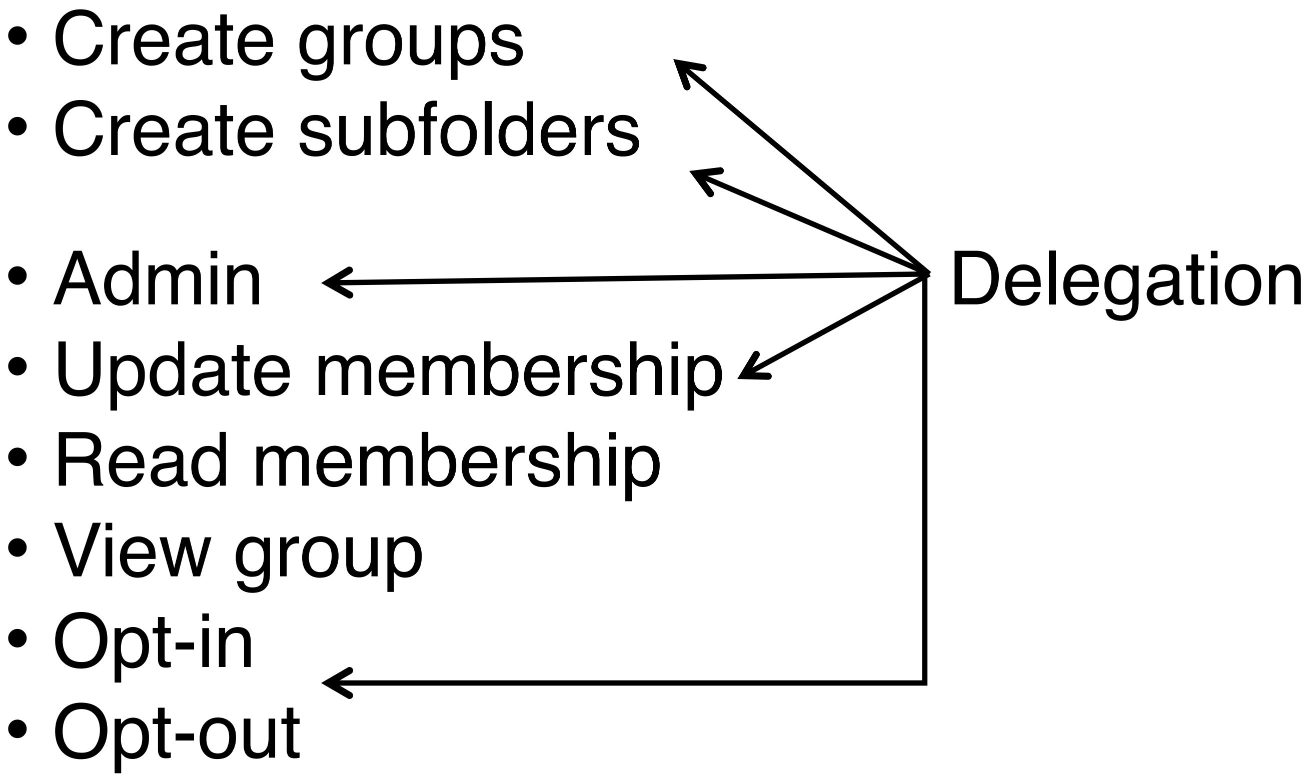
Direct members

Subgroup

Indirect members

Composite groups

Security & delegation

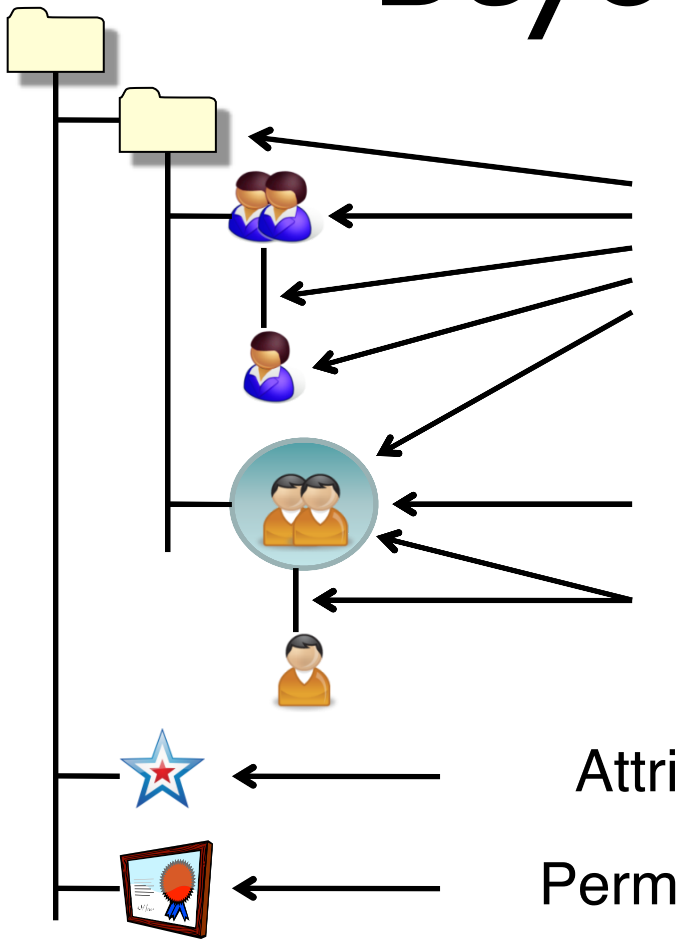


- Create groups
- Create subfolders

- Admin
- Update membership
- Read membership
- View group
- Opt-in
- Opt-out

Delegation

Beyond groups...



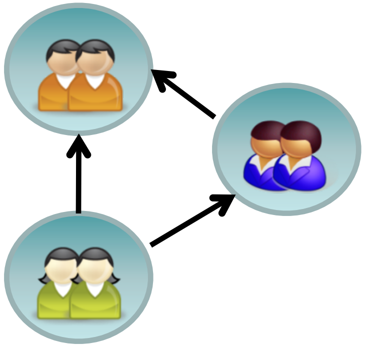
Attributes

Roles

Permissions

Attribute definition

Permission definition



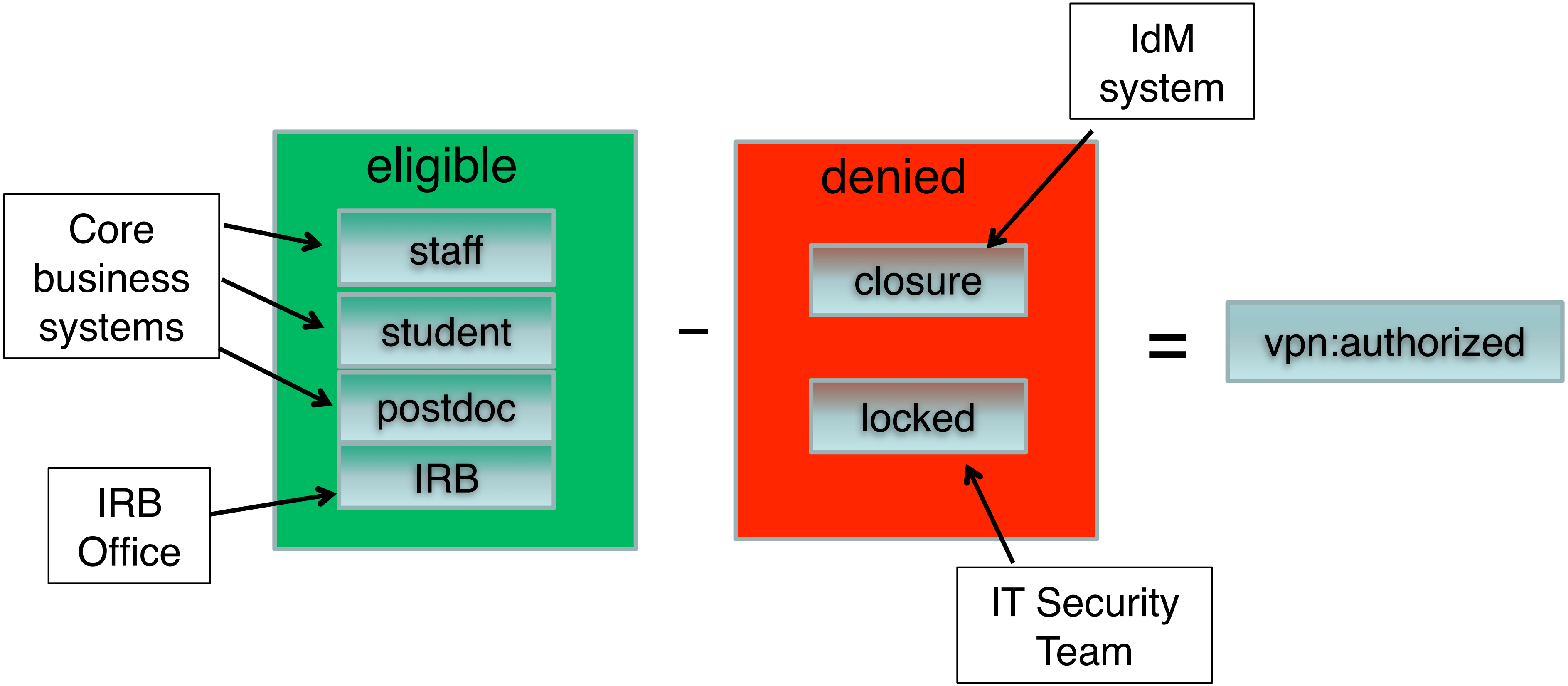
Role inheritance

Delegation model extends that for Groups

Access management lifecycle support

- Membership start & end times (optional)
- Move or copy folders, groups, etc
- User audit
- Point in time audit
- Rules

Distributed Authorization Management

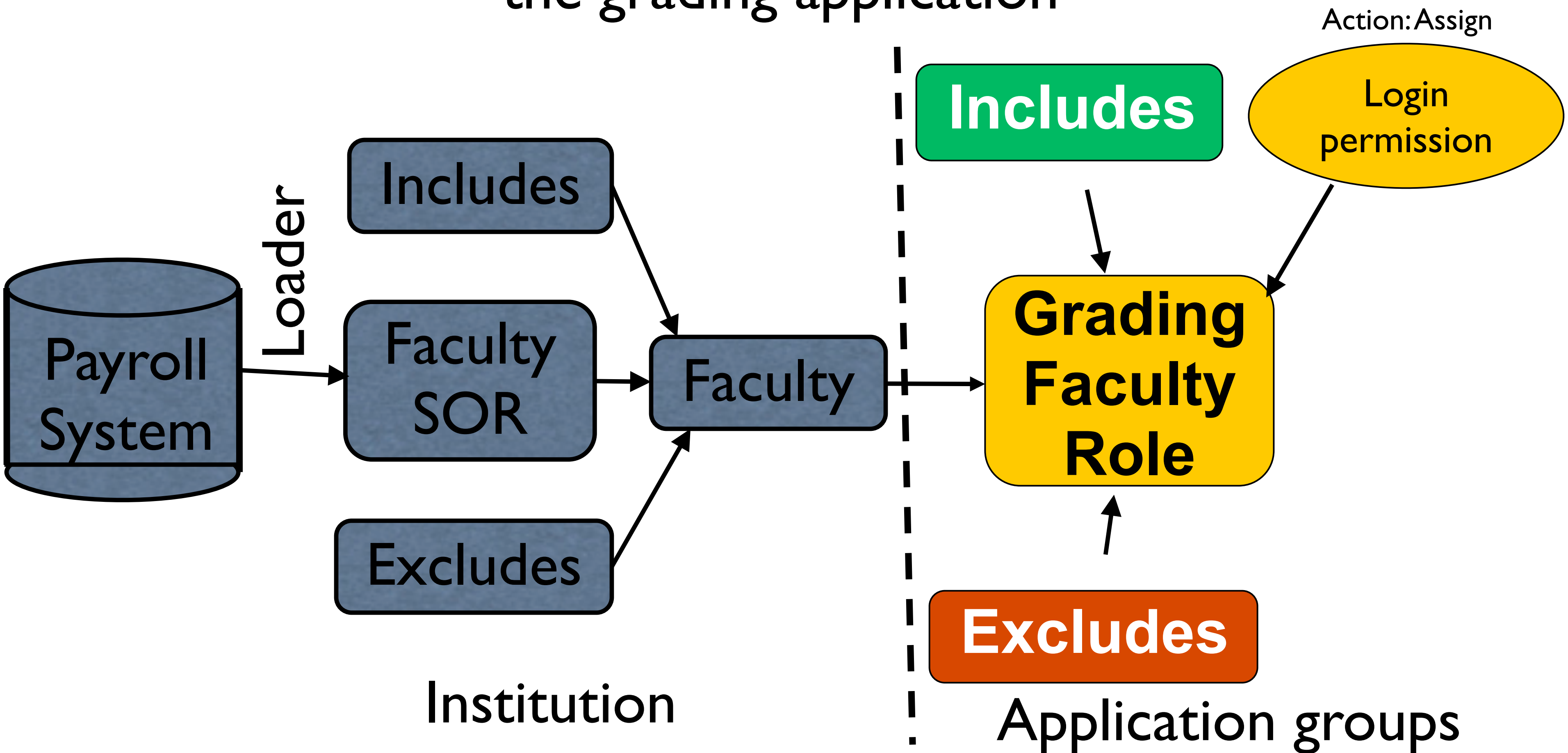


Different groups, different authorities

VPN only uses "vpn:authorized"

Deprovisioning

Only Active faculty members can login to the grading application

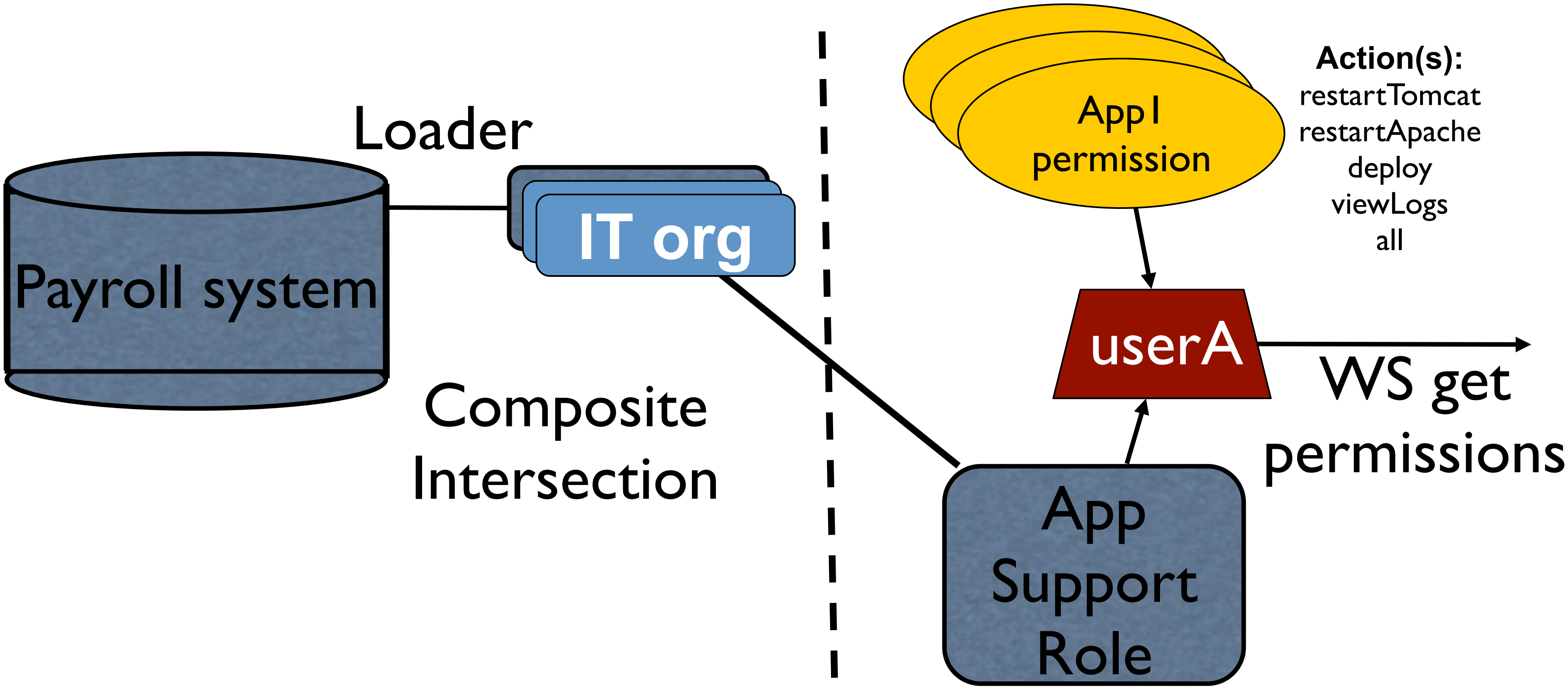


Institution community groups

Application groups and permissions

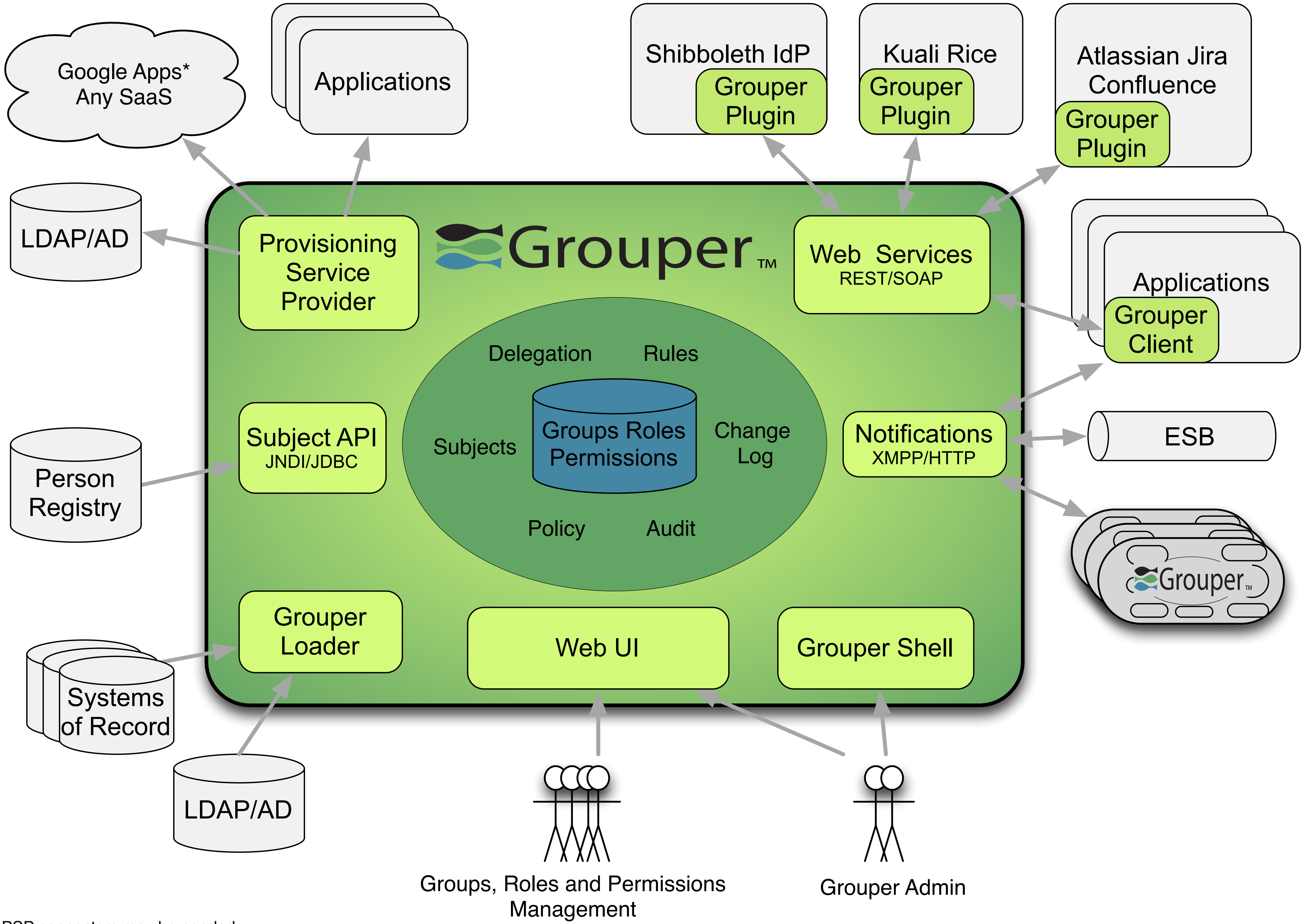
Fine-grained Permissions Management

Active IT support staff can manage applications that they work on



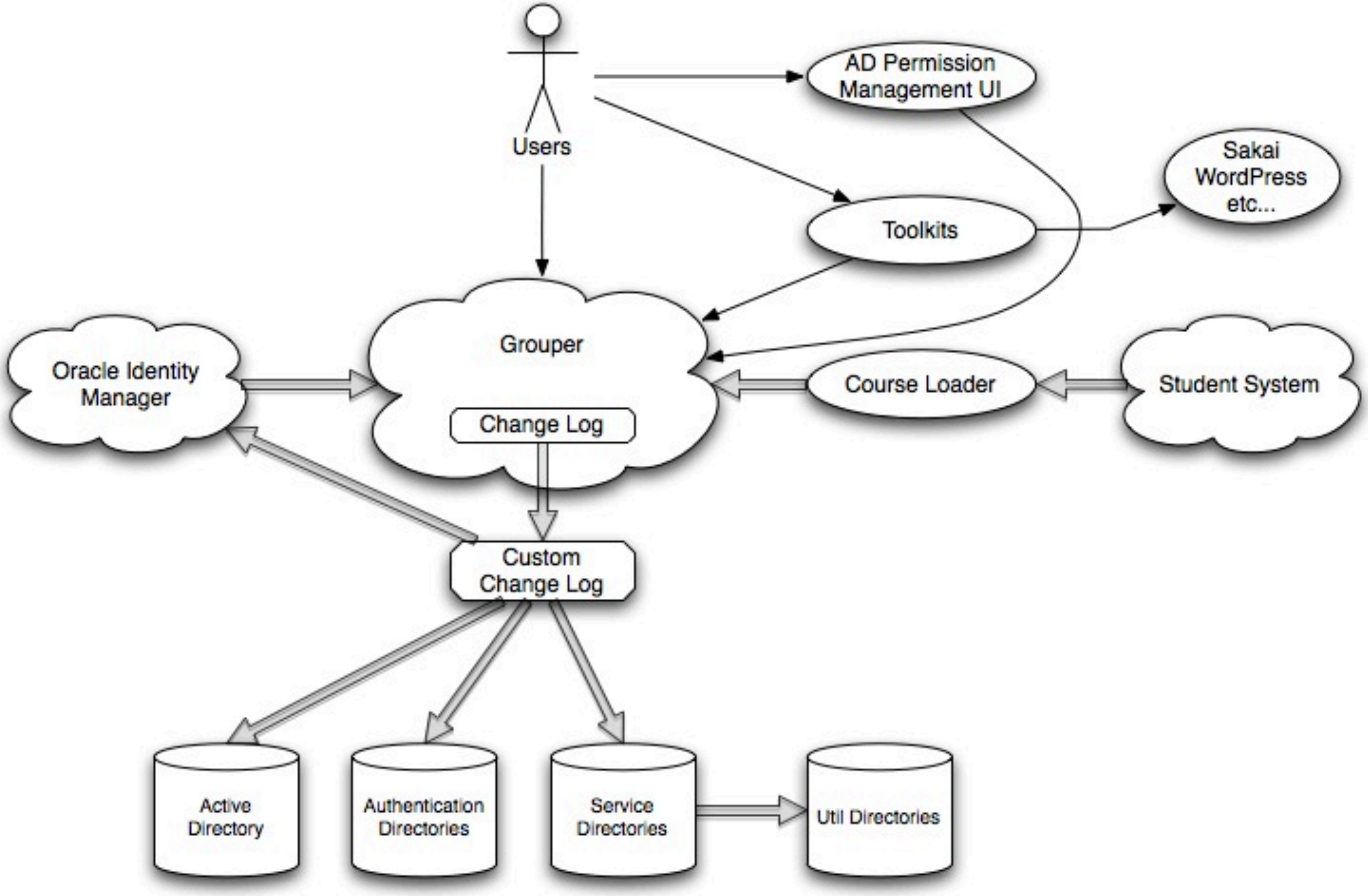
Institution community groups

App groups / permissions

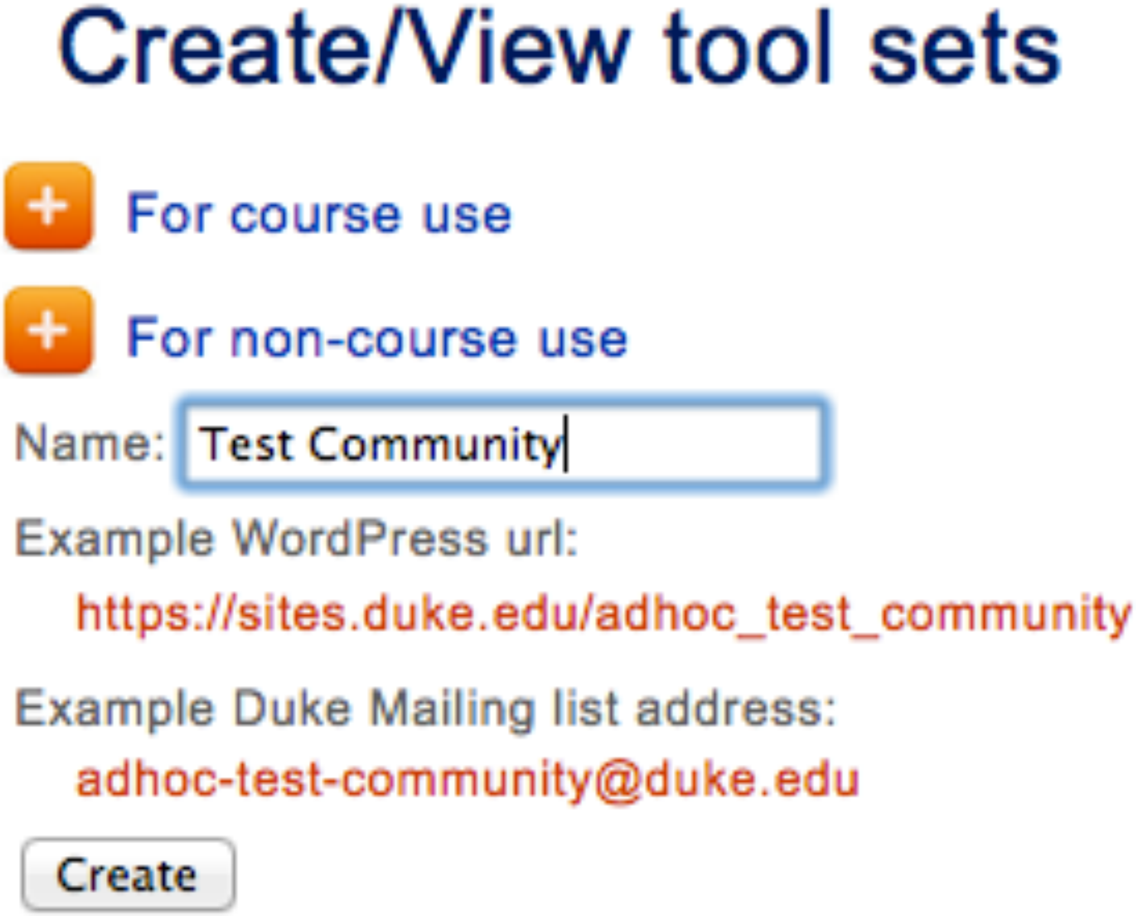


* PSP connectors may be needed

Provisioning Authorization Data



Ad-hoc Collaboration Communities
Creates various groups in Grouper



Create/View tool sets

+ For course use

+ For non-course use

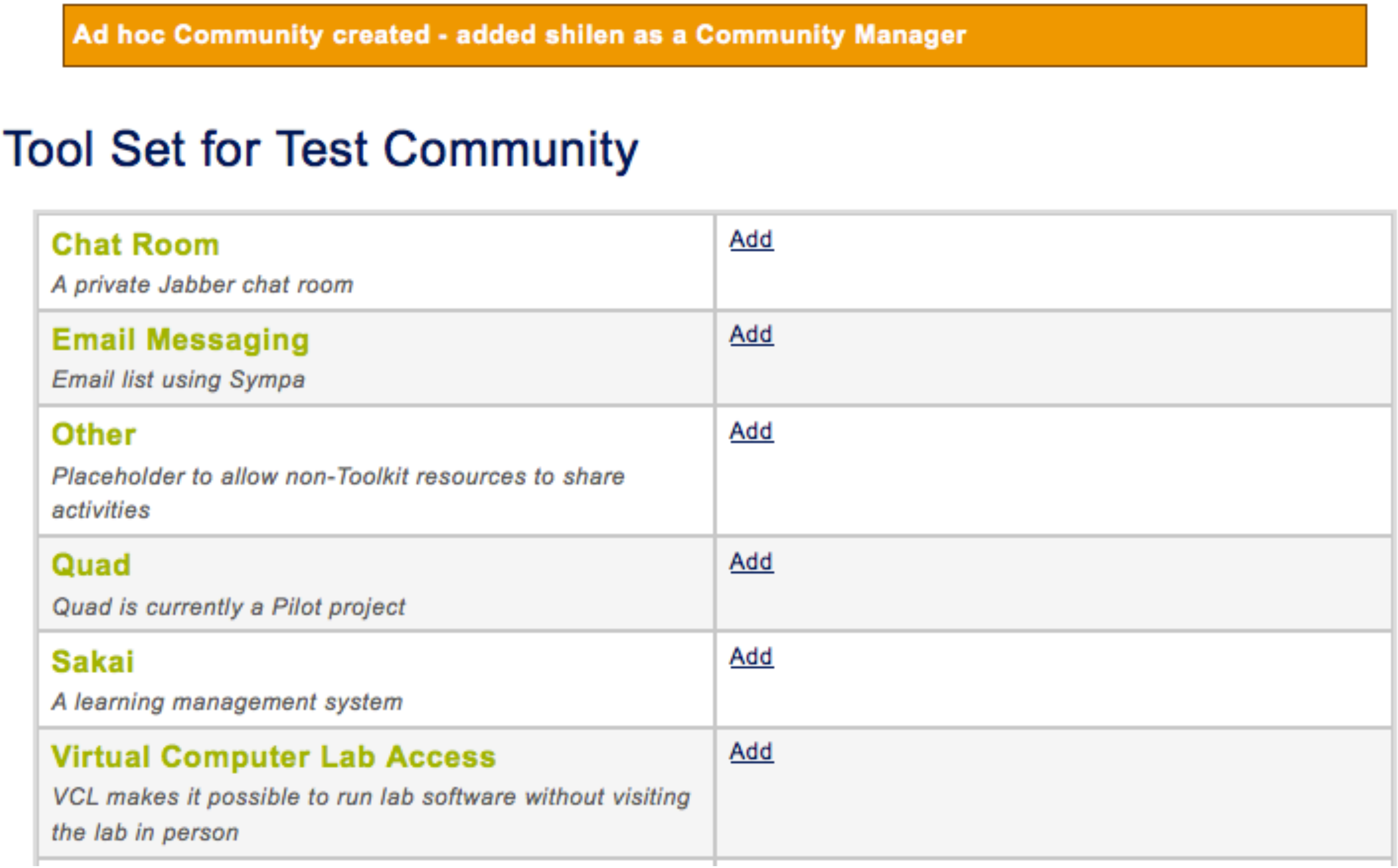
Name: Test Community

Example WordPress url:

https://sites.duke.edu/adhoc_test_community

Example Duke Mailing list address:

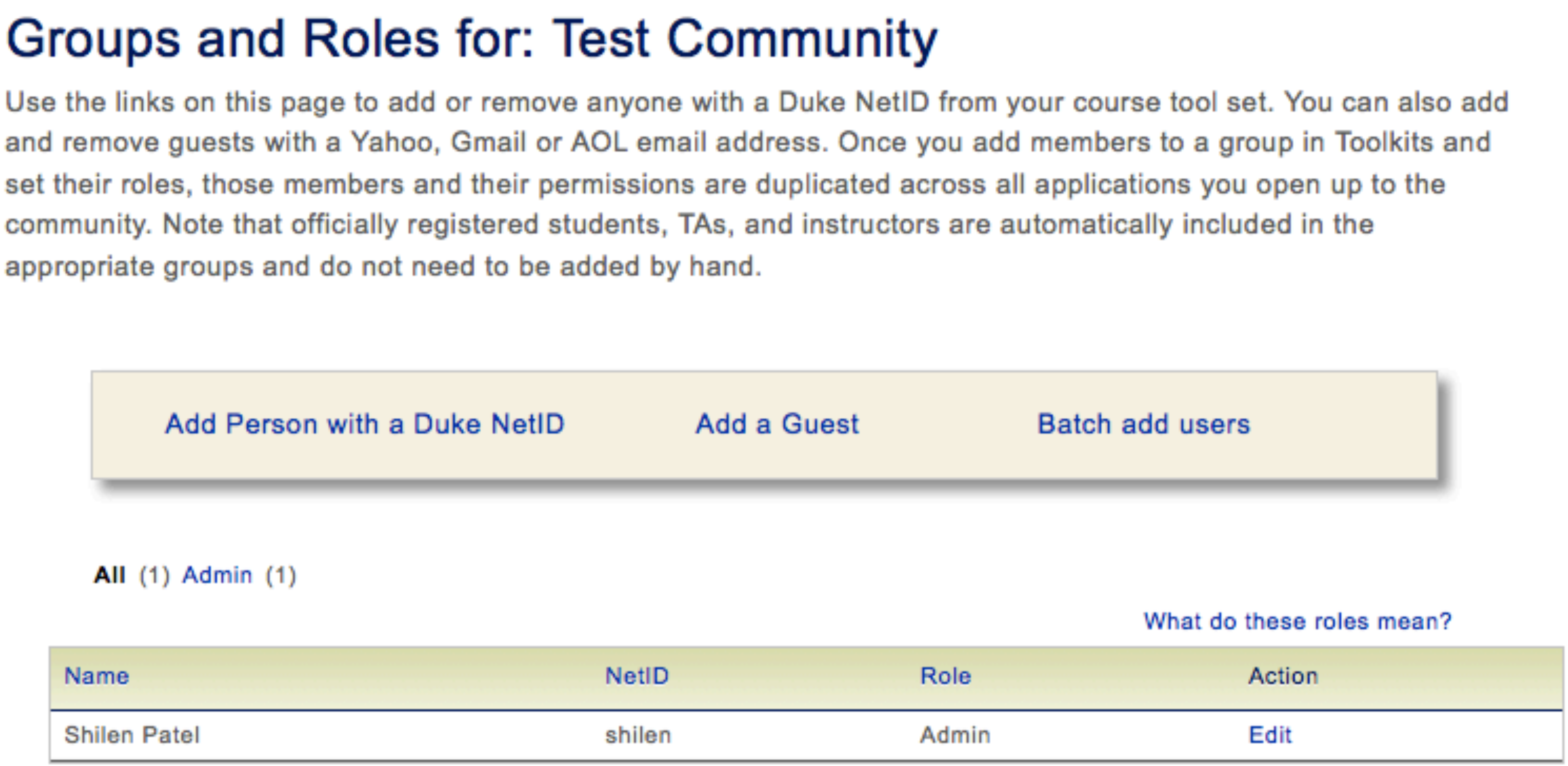
adhoc-test-community@duke.edu



Ad hoc Community created - added shilen as a Community Manager

Tool Set for Test Community

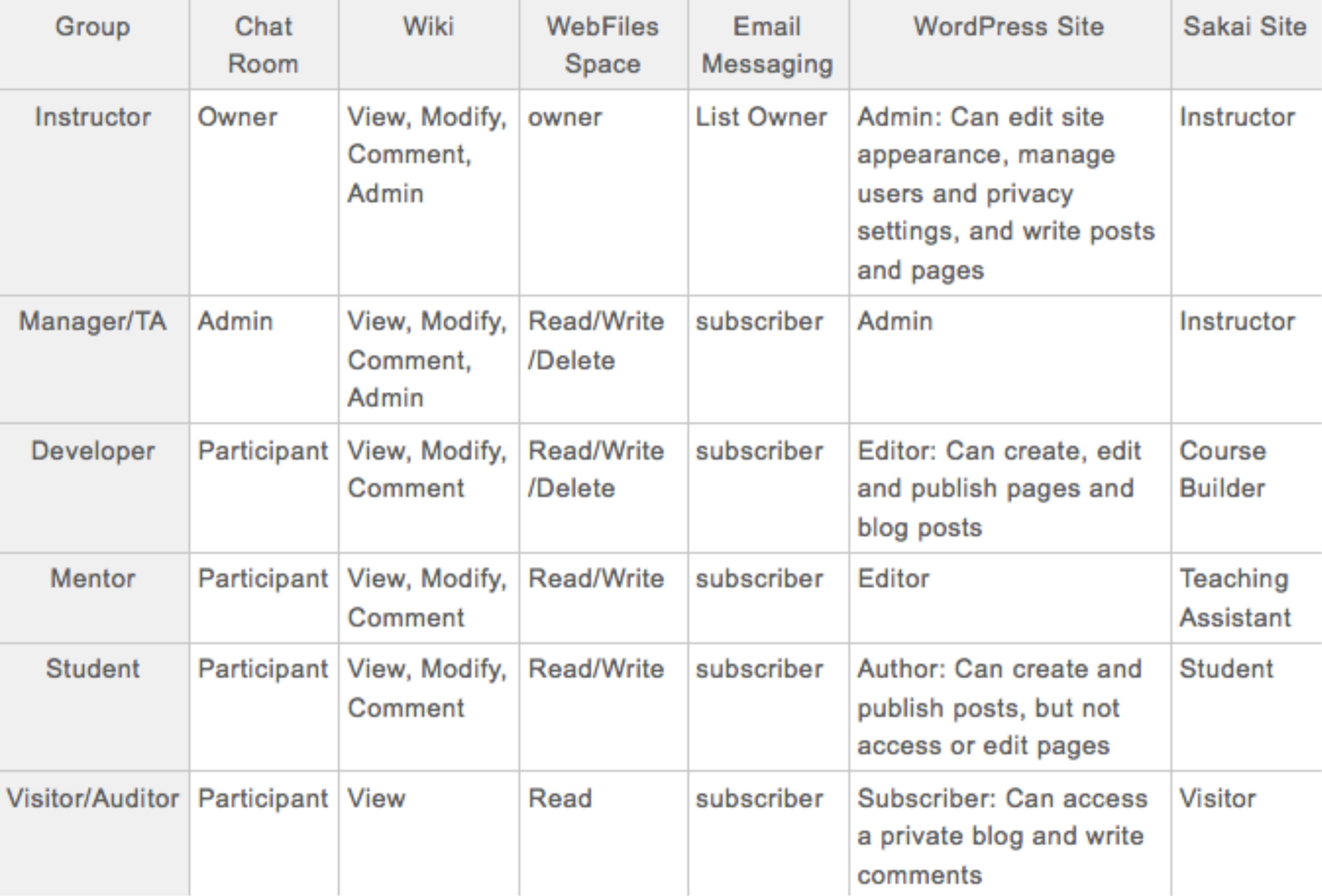
Chat Room *A private Jabber chat room*	Add
Email Messaging *Email list using Sympa*	Add
Other *Placeholder to allow non-Toolkit resources to share activities*	Add
Quad *Quad is currently a Pilot project*	Add
Sakai *A learning management system*	Add
Virtual Computer Lab Access *VCL makes it possible to run lab software without visiting the lab in person*	Add



Groups and Roles for: Test Community

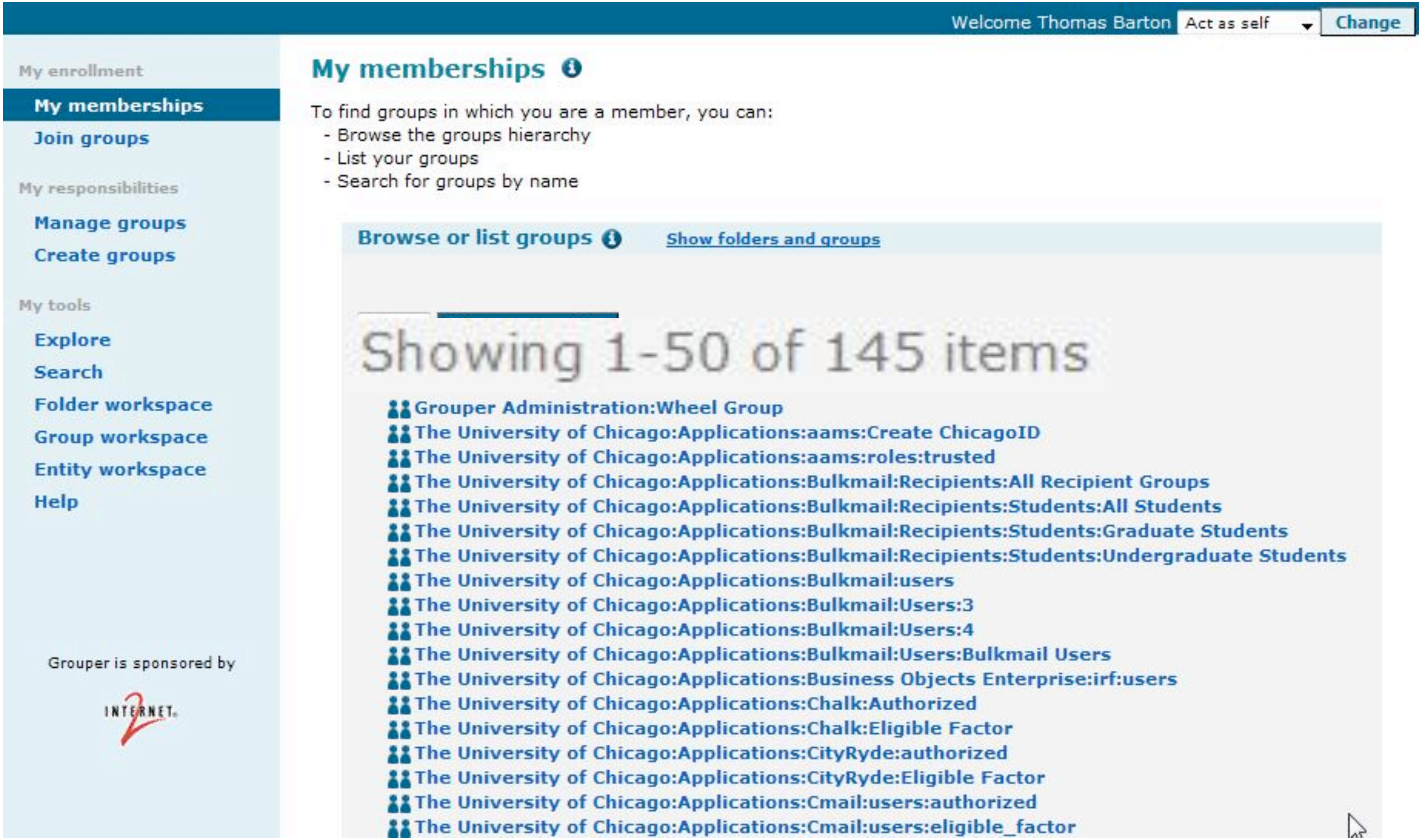
Use the links on this page to add or remove anyone with a Duke NetID from your course tool set. You can also add and remove guests with a Yahoo, Gmail or AOL email address. Once you add members to a group in Toolkits and set their roles, those members and their permissions are duplicated across all applications you open up to the community. Note that officially registered students, TAs, and instructors are automatically included in the appropriate groups and do not need to be added by hand.

Name	NetID	Role	Action
Shilen Patel	shilen	Admin	Edit



Group	Chat Room	Wiki	WebFiles Space	Email Messaging	WordPress Site	Sakai Site
Instructor	Owner	View, Modify, Comment, Admin	owner	List Owner	Admin: Can edit site appearance, manage users and privacy settings, and write posts and pages	Instructor
Manager/TA	Admin	View, Modify, Comment, Admin	Read/Write /Delete	subscriber	Admin	Instructor
Developer	Participant	View, Modify, Comment	Read/Write /Delete	subscriber	Editor: Can create, edit and publish pages and blog posts	Course Builder
Mentor	Participant	View, Modify, Comment	Read/Write	subscriber	Editor	Teaching Assistant
Student	Participant	View, Modify, Comment	Read/Write	subscriber	Author: Can create and publish posts, but not access or edit pages	Student
Visitor/Auditor	Participant	View	Read	subscriber	Subscriber: Can access a private blog and write comments	Visitor

Tom Barton's UChicago group memberships



Welcome Thomas Barton Act as self Change

My memberships

To find groups in which you are a member, you can:
- Browse the groups hierarchy
- List your groups
- Search for groups by name

Browse or list groups Show folders and groups

Showing 1-50 of 145 items

- Grouper Administration:Wheel Group
- The University of Chicago:Applications:aams:Create ChicagoID
- The University of Chicago:Applications:aams:roles:trusted
- The University of Chicago:Applications:Bulkmail:Recipients:All Recipient Groups
- The University of Chicago:Applications:Bulkmail:Recipients:Students:All Students
- The University of Chicago:Applications:Bulkmail:Recipients:Students:Graduate Students
- The University of Chicago:Applications:Bulkmail:Recipients:Students:Undergraduate Students
- The University of Chicago:Applications:Bulkmail:users
- The University of Chicago:Applications:Bulkmail:Users:3
- The University of Chicago:Applications:Bulkmail:Users:4
- The University of Chicago:Applications:Bulkmail:Users:Bulkmail Users
- The University of Chicago:Applications:Business Objects Enterprise:irf:users
- The University of Chicago:Applications:Chalk:Authorized
- The University of Chicago:Applications:Chalk:Eligible Factor
- The University of Chicago:Applications:CityRyde:authorized
- The University of Chicago:Applications:CityRyde:Eligible Factor
- The University of Chicago:Applications:Cmail:users:authorized
- The University of Chicago:Applications:Cmail:users:eligible_factor

Memberships become LDAP attributes

dn: uid=tbarton,ou=people,dc=uchicago,dc=edu
ucismemberof: uc:org:nsit:integration:techag
ucismemberof: uc:org:nsit:srdirs
ucismemberof: uc:org:nsit:integration:iteco:wr
ucismemberof: uc:applications:confluence:NSIT:esx
ucismemberof: uc:org:nsit:integration:iteco:rd

ucIsMemberOf :
uc:applications:vpn:authorized

ucismemberof: uc:applications:bulkmail:users
ucismemberof: uc:org:library:gnet:admins
ucismemberof: uc:applications:gnetid:admins
ucismemberof: uc:applications:wireless:authorized
ucismemberof: uc:applications:cmail:users:authorized
ucismemberof: uc:reference:affiliations:effective:staff

UChicago applications managed by Grouper, so far

- aams
- Ad Astra
- Bulkmail
- Business Objects Enterprise
- Chalk
- CityRyde
- Cmail
- cnet
- Confluence
- Directory Administration
- dmca
- Facilities SIMS
- gnetid
- grouper
- im
- isx
- IT Ecosystem
- Lab School
- LDAP
- lists
- Mail Forwarding
- Mail Quarantine
- Microsoft Exchange
- modem pool
- monitoring
- myUChicago
- Non-po
- Onecard
- online directory
- password expiration
- Service Now
- sharepoint
- shibboleth
- statements portlet
- SVN
- tank
- unifiedcomm
- versions
- virtualization
- voip
- vpn
- web hosting
- webproxy
- webshare
- webspace
- wireless

Roadmap – v2.2

Release	Item	Description
2.2	New Grouper UI	Provide new UI capabilities that better meet community needs.
2.2	Services in Grouper	Tag objects in Grouper so that folders, groups, permissions can be associated with a "service“ to make it easier for users to perform tasks in Grouper.
2.2	Improved Grouper configuration	Make Grouper more easily deployable and upgradeable across environments with cascaded config files and expression language in config file entries.
On-going	Grouper Core	Continue adding capabilities to meet requirements from the field.
On-going	Community contributions	Solicit and publicize community contributions of extensions and complements to Grouper.

Roadmap – v2.2

Release	Item	Description
2.2	Legacy attribute migration	Migrate legacy attributes into the new attribute framework.
2.2	Unix GID management	Built-in support for managing unix GIDs

Penn and Grouper

- Used Grouper centrally at Penn for 5 years
- 120k groups
- 2.7 million immediate memberships
- 10k permission assignments
- We use: UI, WS, GSH, loader, LDAP, client, external users, workflow with Kuali Rice edoclite, heavily delegated

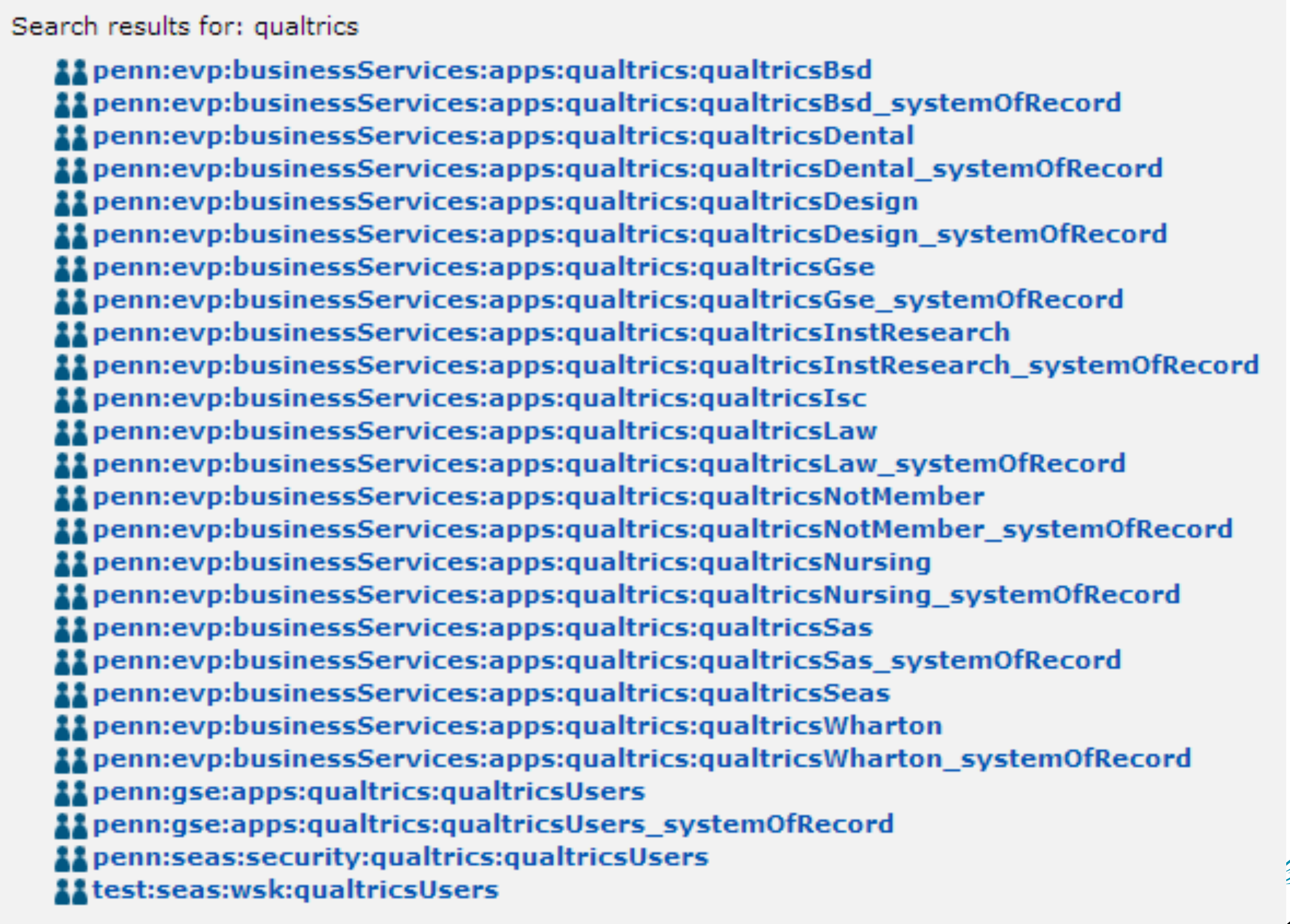
Penn Grouper project team

- ~20% technical person
- ~20% data analyst
- Small requirements from various other people: manager, sysadmins, ldap admins, etc
- Note: during upgrades time requirements increase, these are average times

Example application: Qualtrics

- Cloud survey tool which is not licensed to everyone at Penn
- People in various schools or centers see a different branded site
- Loader manages affiliate groups
- Responsible parties can add ad hoc members
- Shib entitlements communicate rights to

Example application: Qualtrics (continued)



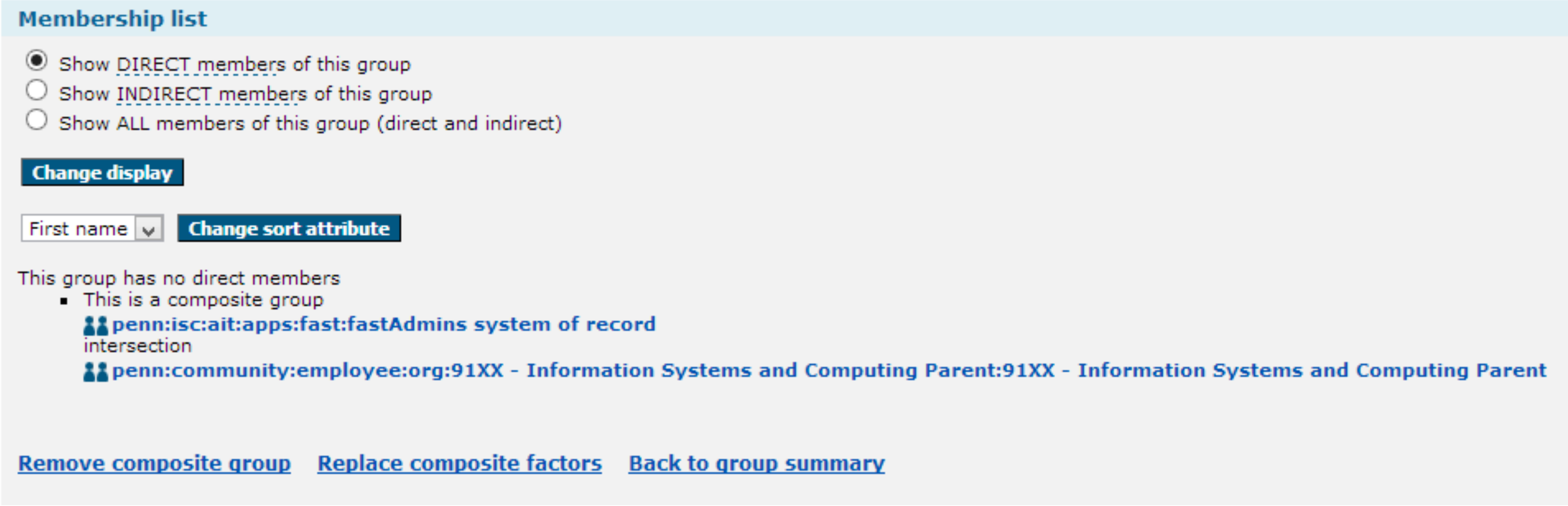
Search results for: qualtrics

- penn:evp:businessServices:apps:qualtrics:qualtricsBsd
- penn:evp:businessServices:apps:qualtrics:qualtricsBsd_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsDental
- penn:evp:businessServices:apps:qualtrics:qualtricsDental_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsDesign
- penn:evp:businessServices:apps:qualtrics:qualtricsDesign_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsGse
- penn:evp:businessServices:apps:qualtrics:qualtricsGse_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsInstResearch
- penn:evp:businessServices:apps:qualtrics:qualtricsInstResearch_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsIsc
- penn:evp:businessServices:apps:qualtrics:qualtricsLaw
- penn:evp:businessServices:apps:qualtrics:qualtricsLaw_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsNotMember
- penn:evp:businessServices:apps:qualtrics:qualtricsNotMember_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsNursing
- penn:evp:businessServices:apps:qualtrics:qualtricsNursing_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsSas
- penn:evp:businessServices:apps:qualtrics:qualtricsSas_systemOfRecord
- penn:evp:businessServices:apps:qualtrics:qualtricsSeas
- penn:evp:businessServices:apps:qualtrics:qualtricsWharton
- penn:evp:businessServices:apps:qualtrics:qualtricsWharton_systemOfRecord
- penn:gse:apps:qualtrics:qualtricsUsers
- penn:gse:apps:qualtrics:qualtricsUsers_systemOfRecord
- penn:seas:security:qualtrics:qualtricsUsers
- test:seas:wsk:qualtricsUsers

Example application: custom app admin console

- Custom app framework does groups (pre-dated Grouper)
- Integrated so groups could be linked externally to Grouper
- For admins (all powerful), it is required that users be in the

Example application: custom app admin console (continued)



Membership list

● Show DIRECT members of this group
○ Show INDIRECT members of this group
○ Show ALL members of this group (direct and indirect)

This group has no direct members

- This is a composite group

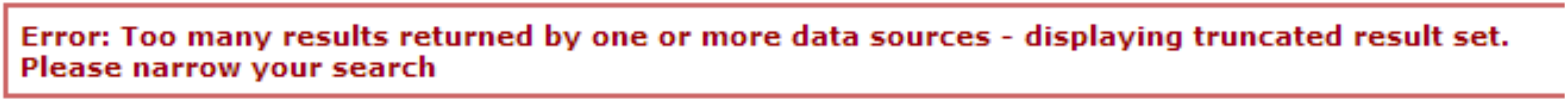
penn:isc:ait:apps:fast:fastAdmins system of record
intersection
penn:community:employee:org:91XX - Information Systems and Computing Parent:91XX - Information Systems and Computing Parent

Example application: Confluence wiki

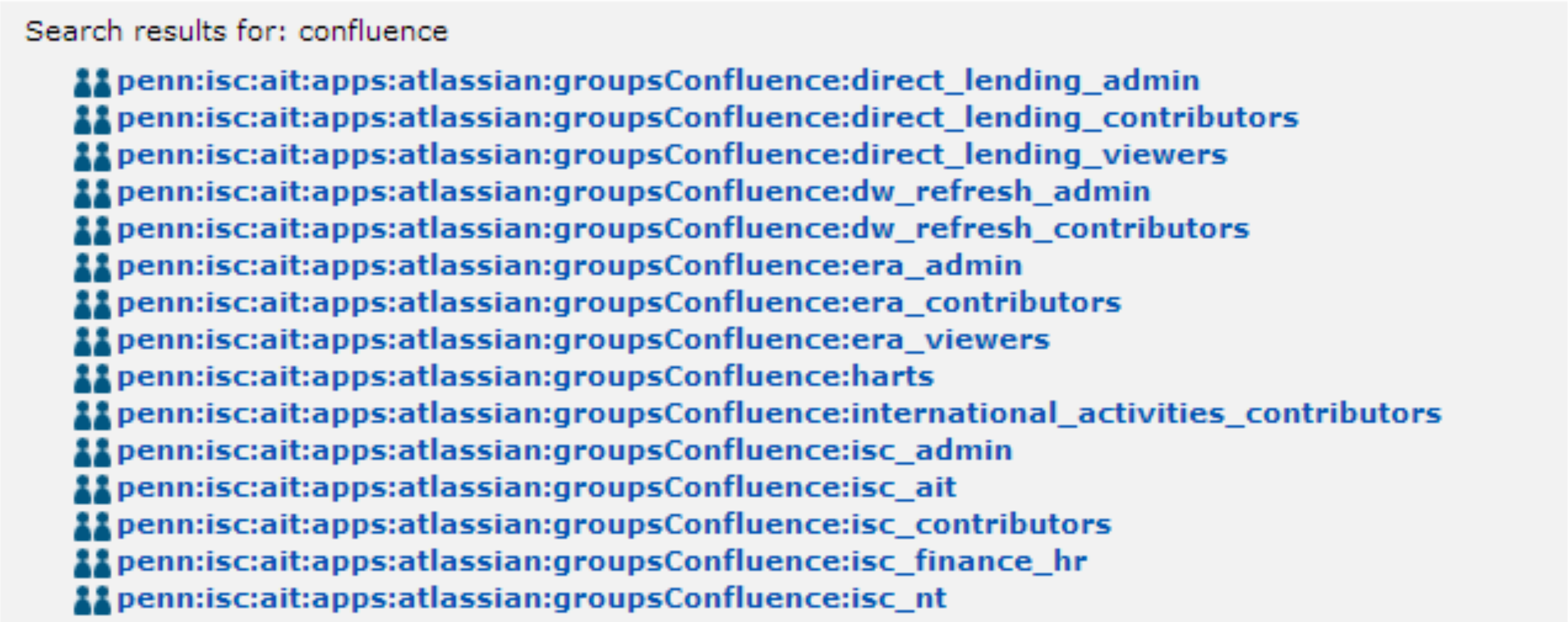
- Confluence (our version at least) can have external groups (hopefully ldap)
- We externalized users and groups so we have single signon, and ability to use Grouper features:
  - Loader - Auto-deprovisioning
  - Reuse groups in other apps
  - Central report to see who has what

Example application: Confluence wiki

- Note: we have a rule for auto-assigning privileges



Error: Too many results returned by one or more data sources - displaying truncated result set. Please narrow your search



Search results for: confluence

- penn:isc:ait:apps:atlassian:groupsConfluence:direct_lending_admin
- penn:isc:ait:apps:atlassian:groupsConfluence:direct_lending_contributors
- penn:isc:ait:apps:atlassian:groupsConfluence:direct_lending_viewers
- penn:isc:ait:apps:atlassian:groupsConfluence:dw_refresh_admin
- penn:isc:ait:apps:atlassian:groupsConfluence:dw_refresh_contributors
- penn:isc:ait:apps:atlassian:groupsConfluence:era_admin
- penn:isc:ait:apps:atlassian:groupsConfluence:era_contributors
- penn:isc:ait:apps:atlassian:groupsConfluence:era_viewers
- penn:isc:ait:apps:atlassian:groupsConfluence:harts
- penn:isc:ait:apps:atlassian:groupsConfluence:international_activities_contributors
- penn:isc:ait:apps:atlassian:groupsConfluence:isc_admin
- penn:isc:ait:apps:atlassian:groupsConfluence:isc_ait
- penn:isc:ait:apps:atlassian:groupsConfluence:isc_contributors
- penn:isc:ait:apps:atlassian:groupsConfluence:isc_finance_hr
- penn:isc:ait:apps:atlassian:groupsConfluence:isc_nt

Grouper loader

- Daemon that periodically sync'ed external sources with Grouper
- Can work for groups or permissions (e.g. org chart)
- SQL or LDAP sources (note: PSP does LDAP too)
- Grouper admins can configure jobs based on attributes

Grouper loader (continued)

- Can sync multiple groups from one query/filter (e.g. courses or orgs)
- Penn has 92 SQL Grouper Loader jobs
- Generally we run these daily, though some run a handful of times throughout the day

Provisioning

- Grouper PSP can provision grouper data to LDAP or AD (other targets can be created)
- Grouper change log can send notifications to XMPP, ESB, etc (other targets can be created)
- Generally we aim for periodic full refresh, with near real time updates

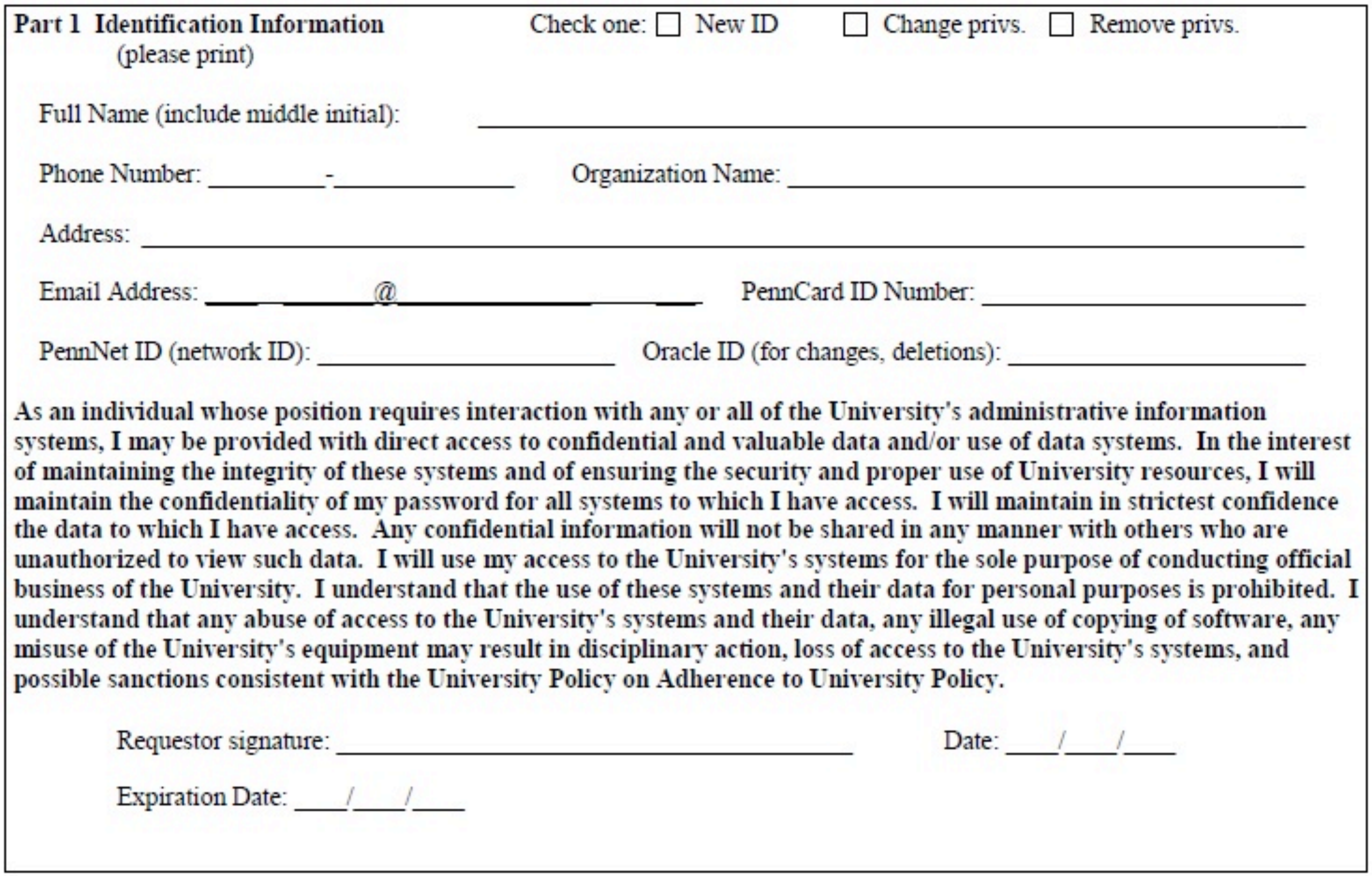
Auditing

- “User audit” will audit who does what
- Point-In-Time auditing will keep track of the history of the repository
  - Who was in this group at a point in time (or time range) in the past
  - Who are all the people who have been in this group
  - What groups was this person in at a point in the past (or time range)

Grouper Kuali Rice edoclite workflow

Paper form screenshot

- In 2009 Penn wanted to convert paper access management forms to eForms



Part 1 Identification Information (please print)

Check one: □ New ID □ Change privs. □ Remove privs.

Full Name (include middle initial): ____

Phone Number: _________-______________ Organization Name: ______________________________

Address: ____

Email Address: ____ _______@______________ ___ PennCard ID Number: ____________________

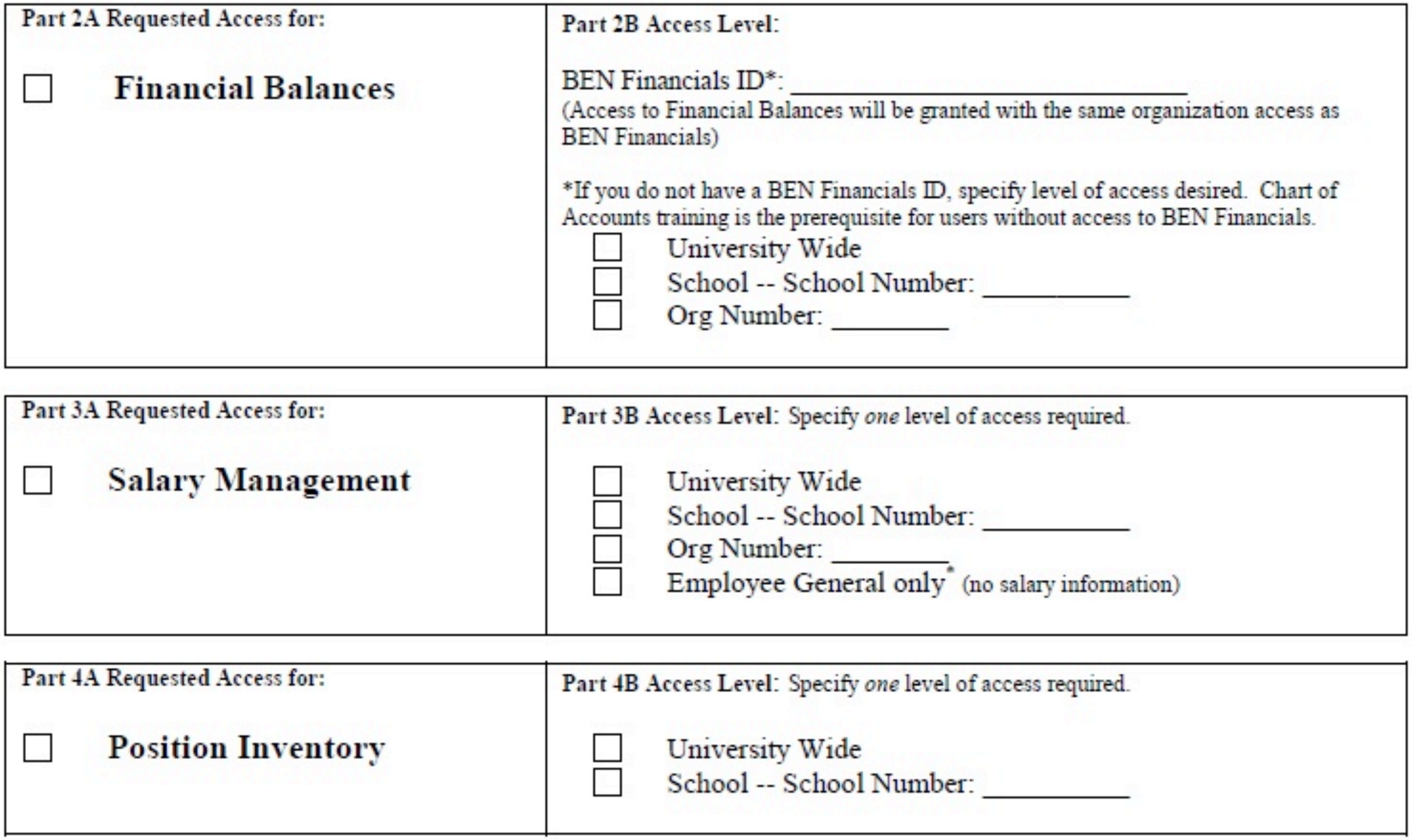
PennNet ID (network ID): ______________________ Oracle ID (for changes, deletions): ____________________

As an individual whose position requires interaction with any or all of the University's administrative information systems, I may be provided with direct access to confidential and valuable data and/or use of data systems. In the interest of maintaining the integrity of these systems and of ensuring the security and proper use of University resources, I will maintain the confidentiality of my password for all systems to which I have access. I will maintain in strictest confidence the data to which I have access. Any confidential information will not be shared in any manner with others who are unauthorized to view such data. I will use my access to the University's systems for the sole purpose of conducting official business of the University. I understand that the use of these systems and their data for personal purposes is prohibited. I understand that any abuse of access to the University's systems and their data, any illegal use of copying of software, any misuse of the University's equipment may result in disciplinary action, loss of access to the University's systems, and possible sanctions consistent with the University Policy on Adherence to University Policy.

Requestor signature: ____ Date: ____/____/____

Expiration Date: ____/____/____

Paper form screenshot (continued)



Part 2A Requested Access for:

□ **Financial Balances**

Part 2B Access Level:

BEN Financials ID*: ______________________________

(Access to Financial Balances will be granted with the same organization access as BEN Financials)

*If you do not have a BEN Financials ID, specify level of access desired. Chart of Accounts training is the prerequisite for users without access to BEN Financials.

□ University Wide
□ School -- School Number: ___________
□ Org Number: _________

Part 3A Requested Access for:

□ **Salary Management**

Part 3B Access Level: Specify *one* level of access required.

□ University Wide
□ School -- School Number: ___________
□ Org Number: _________
□ Employee General only* (no salary information)

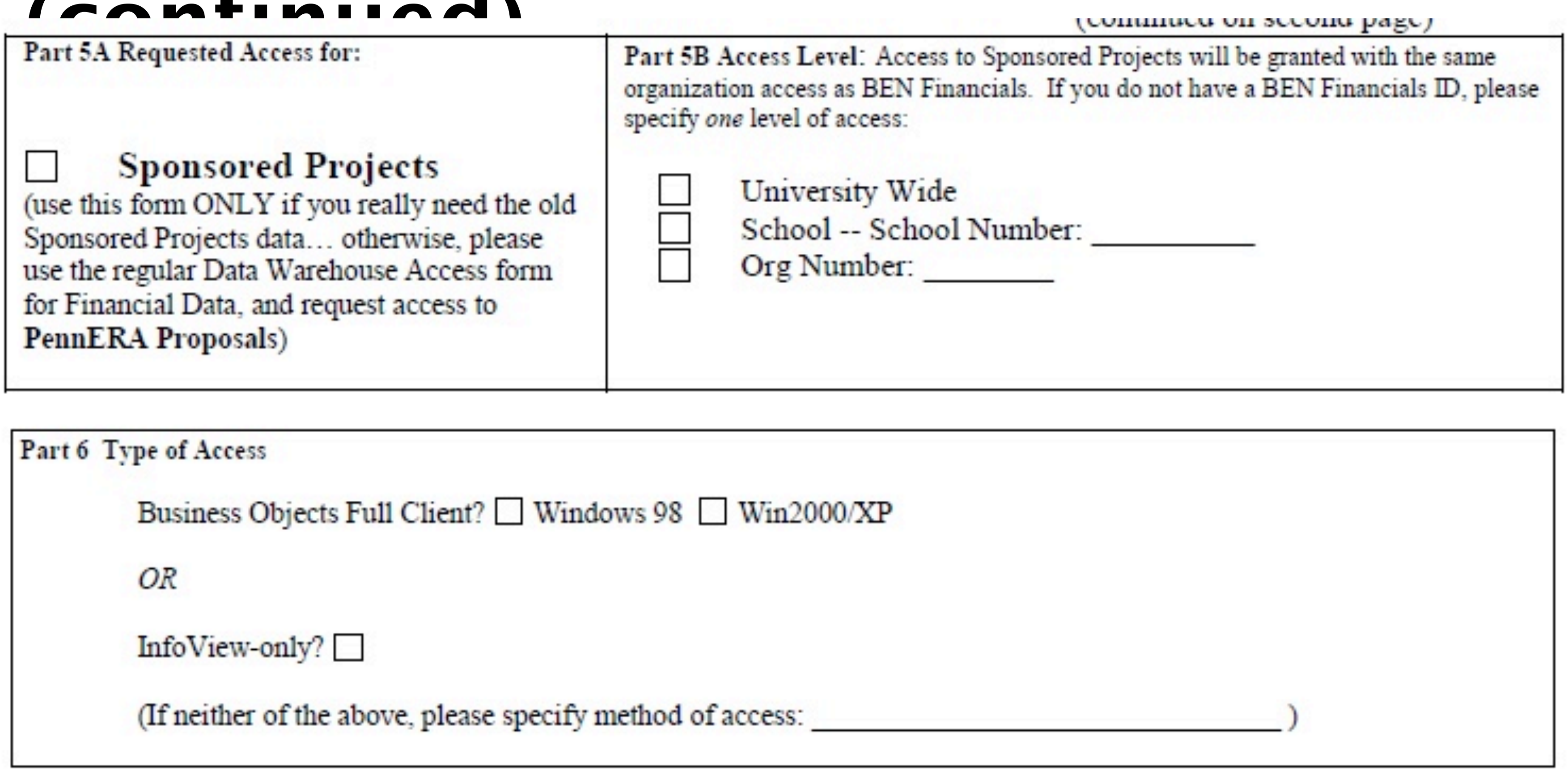
Part 4A Requested Access for:

□ **Position Inventory**

Part 4B Access Level: Specify *one* level of access required.

□ University Wide
□ School -- School Number: ___________

Paper form screenshot (continued)



(continued on second page)

Part 5A Requested Access for:

□ **Sponsored Projects**
(use this form ONLY if you really need the old Sponsored Projects data… otherwise, please use the regular Data Warehouse Access form for Financial Data, and request access to **PennERA Proposals**)

Part 5B Access Level: Access to Sponsored Projects will be granted with the same organization access as BEN Financials. If you do not have a BEN Financials ID, please specify *one* level of access:

□ University Wide
□ School -- School Number: ___________
□ Org Number: _________

Part 6 Type of Access

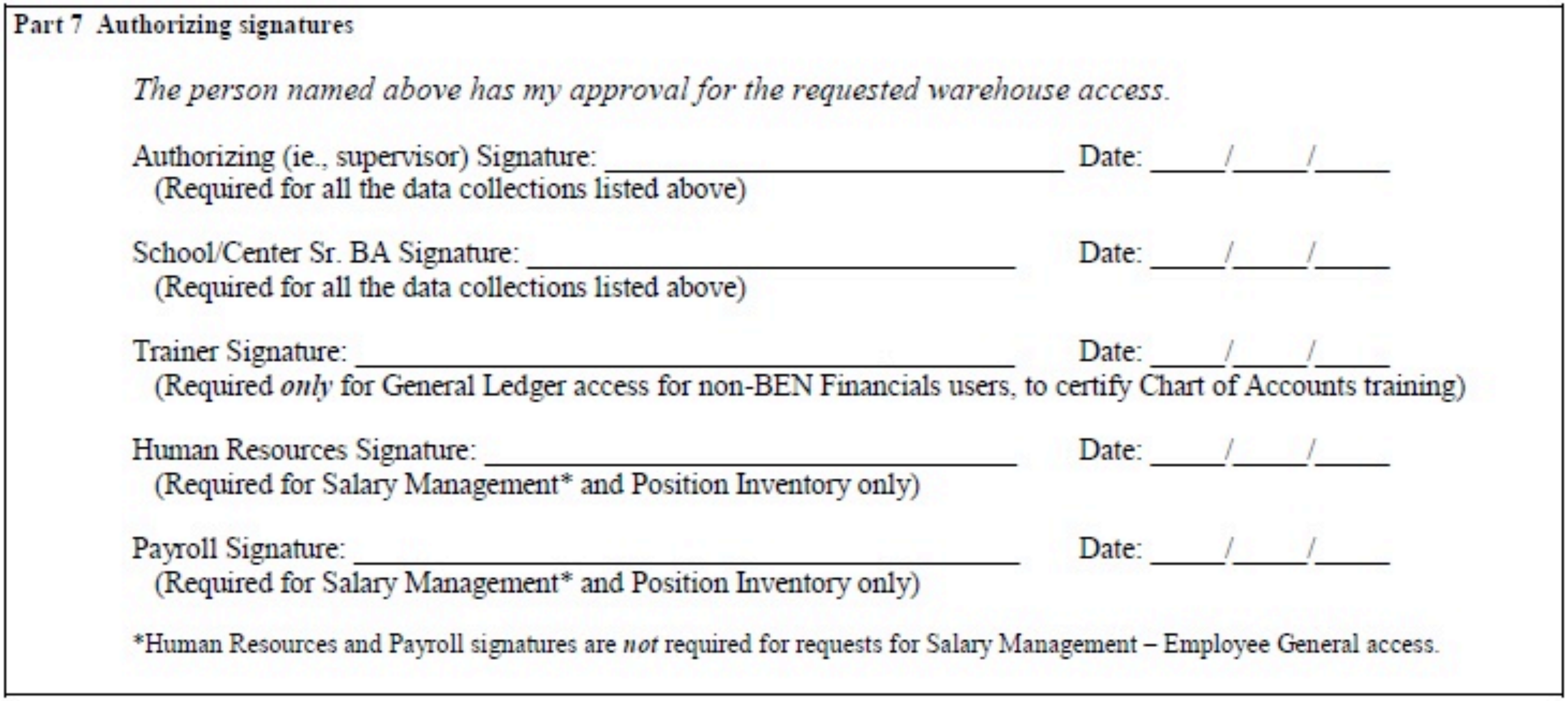
Business Objects Full Client? □ Windows 98 □ Win2000/XP

OR

InfoView-only? □

(If neither of the above, please specify method of access: _________________________________)

Paper form screenshot (continued)



Part 7 Authorizing signatures

The person named above has my approval for the requested warehouse access.

Authorizing (ie., supervisor) Signature: ______________________________ Date: _____/_____/_____
(Required for all the data collections listed above)

School/Center Sr. BA Signature: ________________________________ Date: _____/_____/_____
(Required for all the data collections listed above)

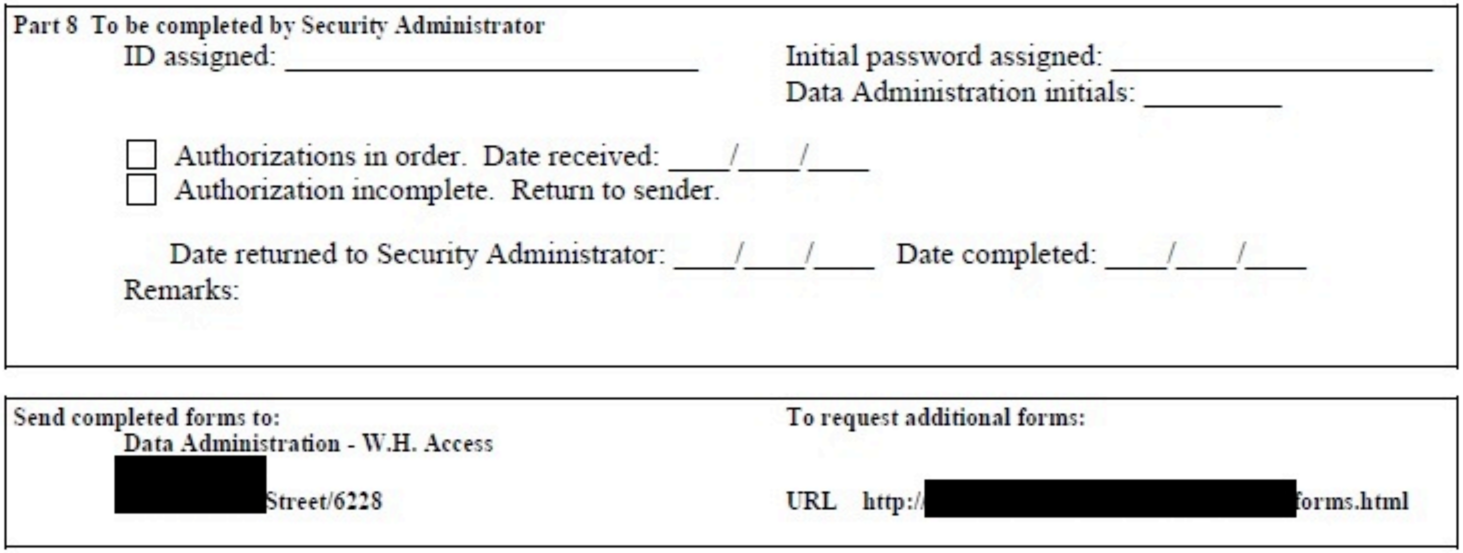
Trainer Signature: ____ Date: _____/_____/_____
(Required *only* for General Ledger access for non-BEN Financials users, to certify Chart of Accounts training)

Human Resources Signature: ___________________________________ Date: _____/_____/_____
(Required for Salary Management* and Position Inventory only)

Payroll Signature: ____ Date: _____/_____/_____
(Required for Salary Management* and Position Inventory only)

*Human Resources and Payroll signatures are *not* required for requests for Salary Management – Employee General access.

Paper form screenshot (continued)



Part 8 To be completed by Security Administrator

ID assigned: ______________________________

Initial password assigned: ______________________

Data Administration initials: __________

□ Authorizations in order. Date received: ____/____/____

□ Authorization incomplete. Return to sender.

Date returned to Security Administrator: ____/____/____ Date completed: ____/____/____

Remarks:

Send completed forms to:

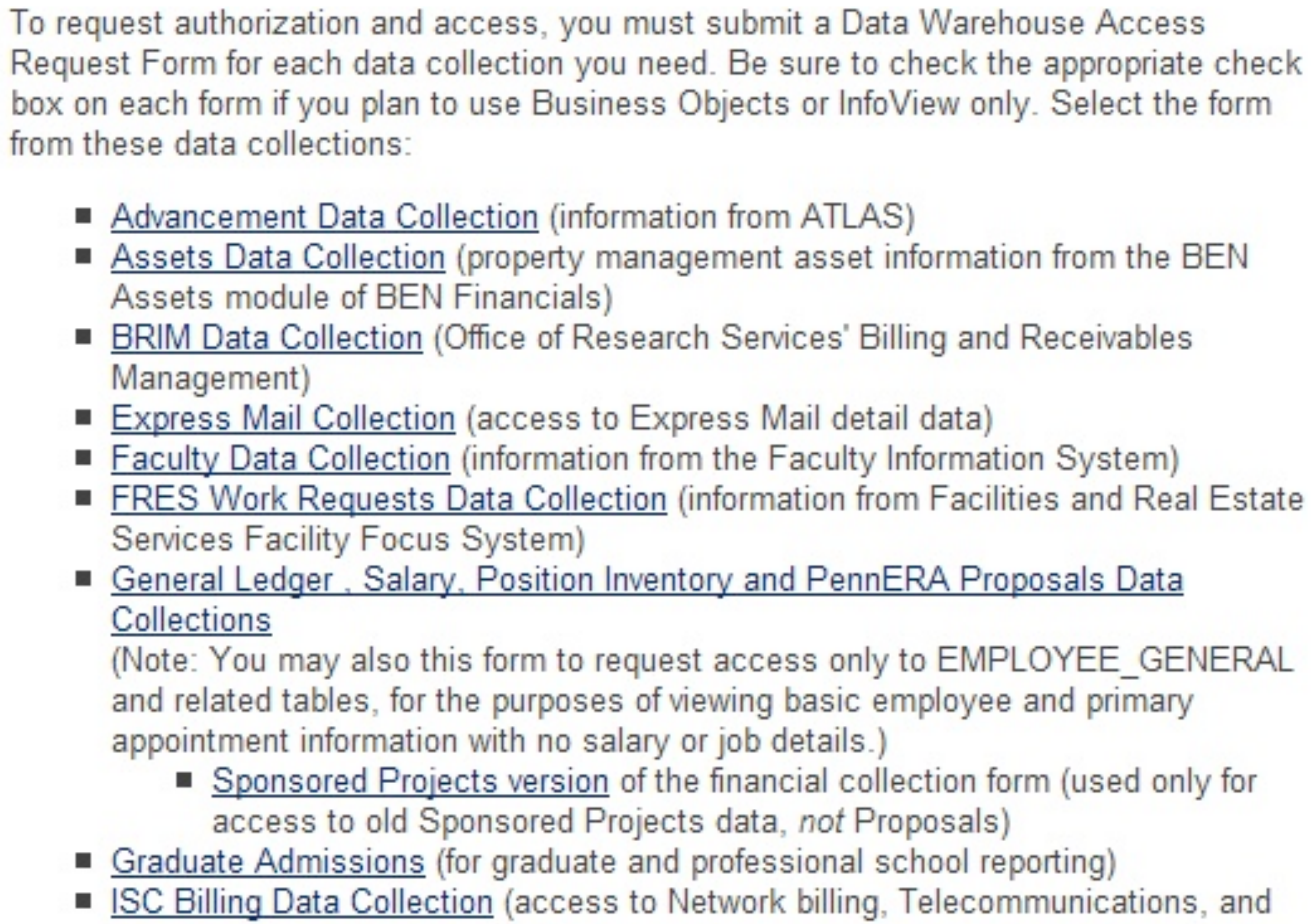
Data Administration - W.H. Access

[redacted]Street/6228

To request additional forms:

URL http://[redacted]forms.html

Paper form existing list



To request authorization and access, you must submit a Data Warehouse Access Request Form for each data collection you need. Be sure to check the appropriate check box on each form if you plan to use Business Objects or InfoView only. Select the form from these data collections:

- Advancement Data Collection (information from ATLAS)
- Assets Data Collection (property management asset information from the BEN Assets module of BEN Financials)
- BRIM Data Collection (Office of Research Services' Billing and Receivables Management)
- Express Mail Collection (access to Express Mail detail data)
- Faculty Data Collection (information from the Faculty Information System)
- FRES Work Requests Data Collection (information from Facilities and Real Estate Services Facility Focus System)
- General Ledger , Salary, Position Inventory and PennERA Proposals Data Collections
  (Note: You may also this form to request access only to EMPLOYEE_GENERAL and related tables, for the purposes of viewing basic employee and primary appointment information with no salary or job details.)
    - Sponsored Projects version of the financial collection form (used only for access to old Sponsored Projects data, *not* Proposals)
- Graduate Admissions (for graduate and professional school reporting)
- ISC Billing Data Collection (access to Network billing, Telecommunications, and

Requirements

- Autofill personal information
- Common includes (privacy statement)
- Fill out form on behalf of someone else
- Org chart picker for data access
- Person picker from group (employee)
- Notification to requester when complete
- Report on form data
- Should require no Java to create forms

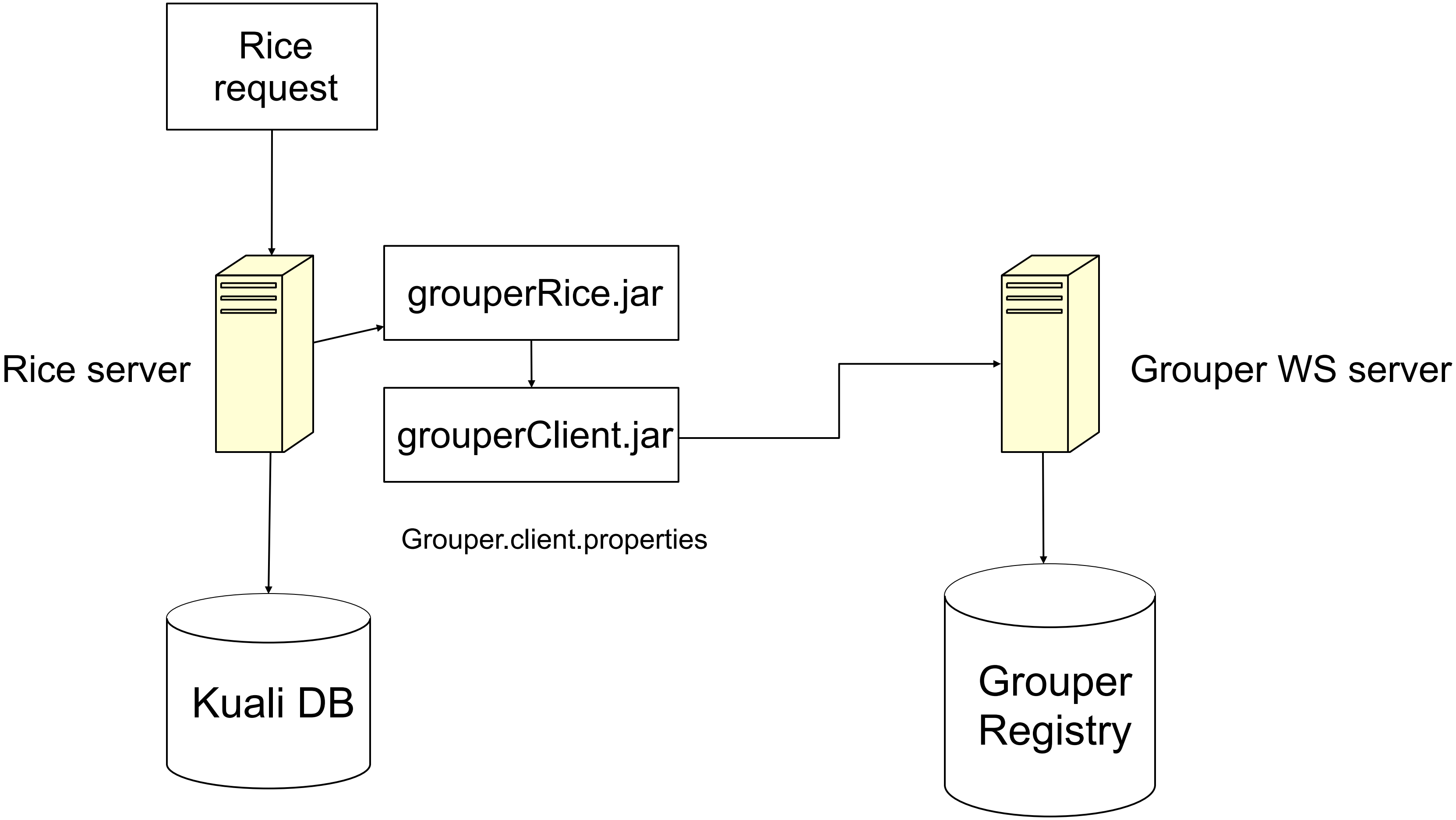
Routing requirements

- Route to members of Grouper group
- Route to selected group (pick school)
- Ability to return to previous route node
- Route to multiple groups at once
- Conditional routing
- Dynamic routing to someone entered on form

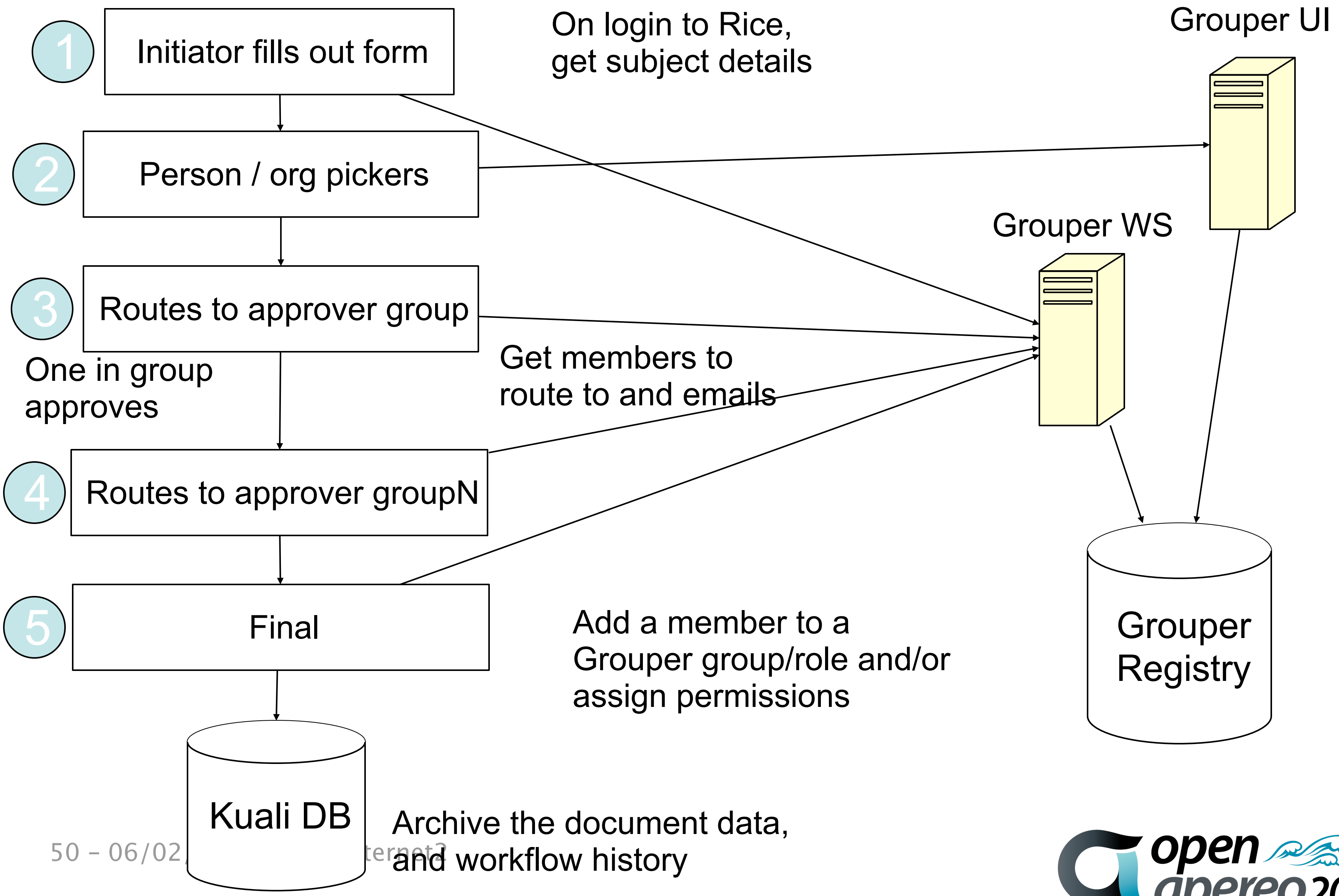
Security requirements

- Submitters can see current and past forms
- Approvers can see current and past forms
- Certain people can edit certain forms

Kuali Rice overridable services



eForms workflow with Grouper



1 Initiator fills out form

On login to Rice, get subject details

2 Person / org pickers

Grouper UI

Grouper WS

3 Routes to approver group

One in group approves

Get members to route to and emails

4 Routes to approver groupN

5 Final

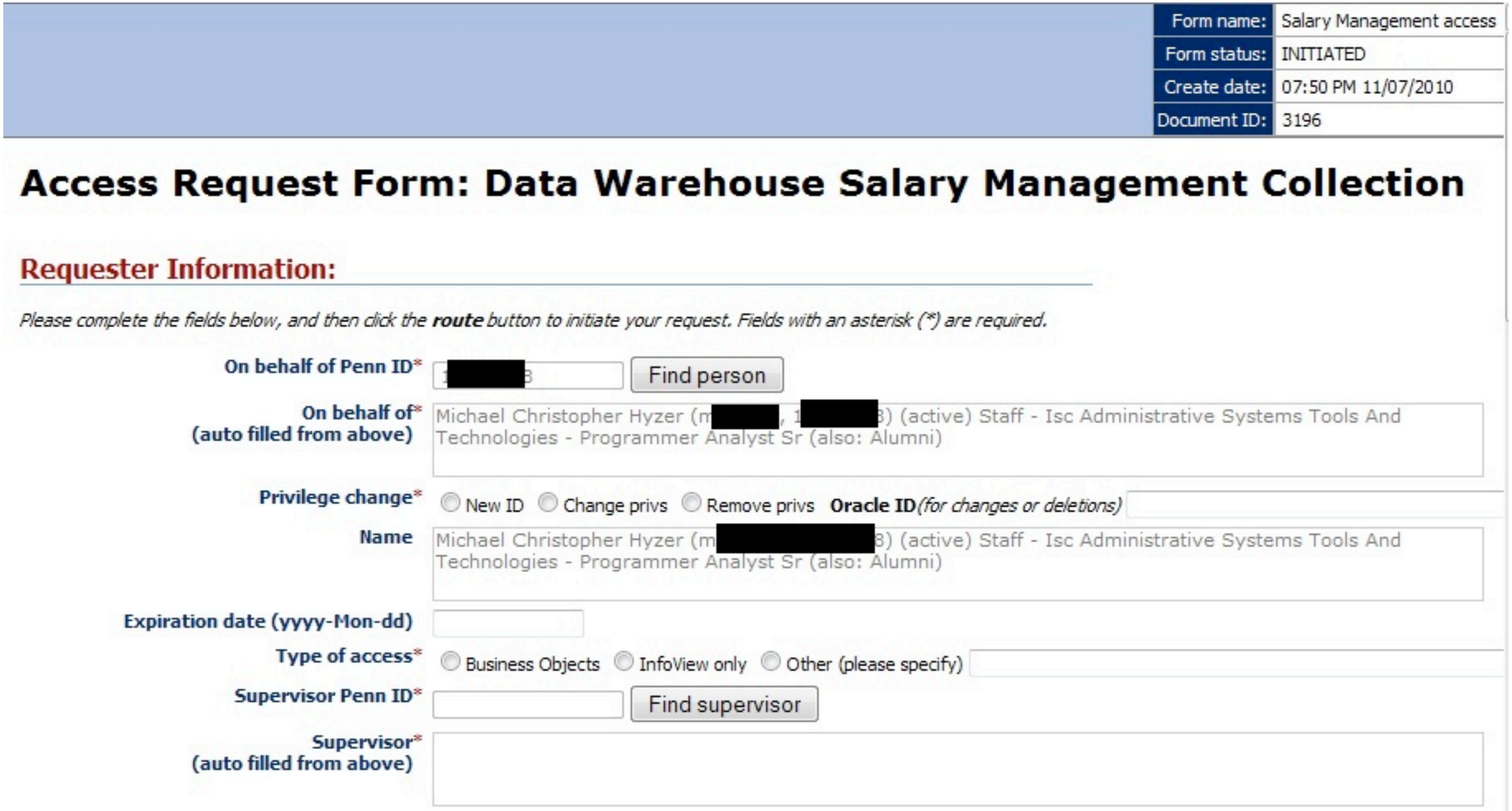
Add a member to a Grouper group/role and/or assign permissions

Grouper Registry

Kuali DB

Archive the document data, and workflow history

Salary management eForm



Form name:	Salary Management access
Form status:	INITIATED
Create date:	07:50 PM 11/07/2010
Document ID:	3196

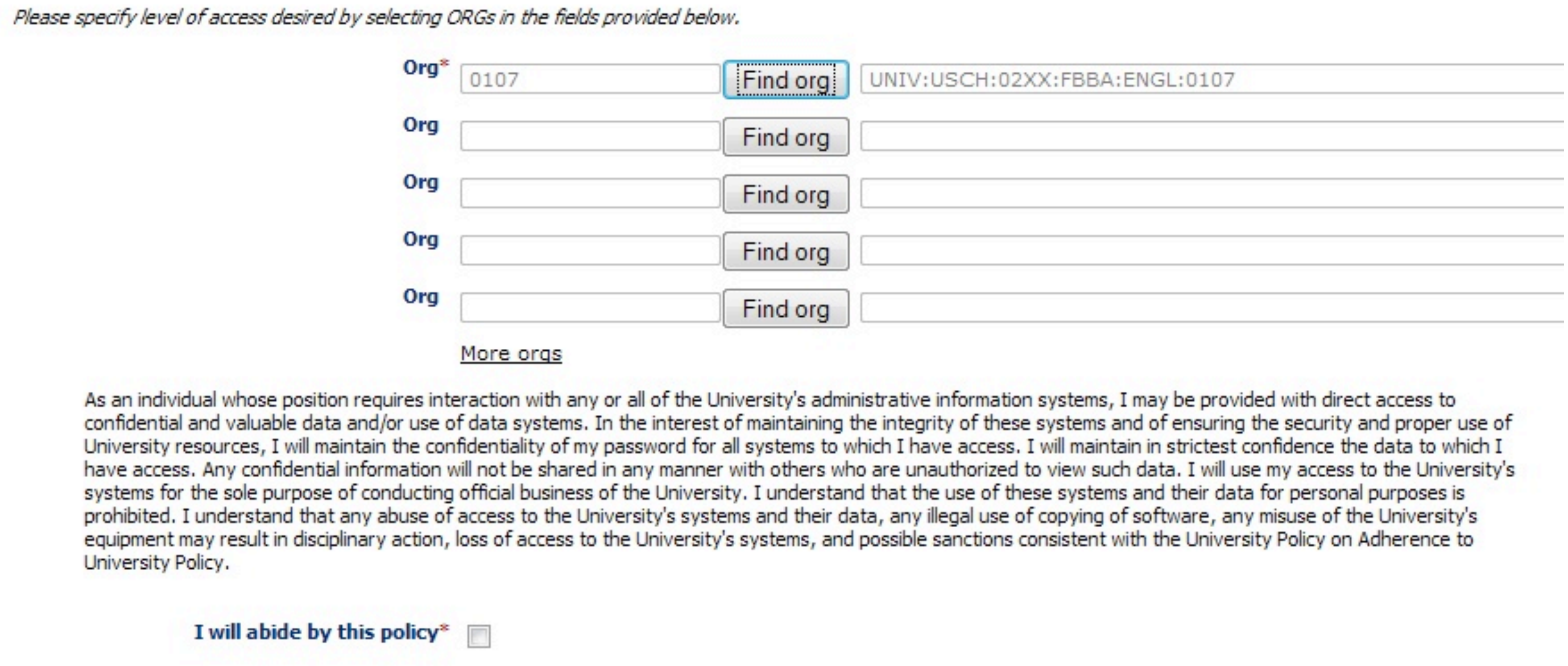
Access Request Form: Data Warehouse Salary Management Collection

Requester Information:

Please complete the fields below, and then click the ***route*** *button to initiate your request. Fields with an asterisk (*) are required.*

On behalf of Penn ID*	[redacted] Find person
On behalf of* (auto filled from above)	Michael Christopher Hyzer ([redacted], [redacted]) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)
Privilege change*	○ New ID ○ Change privs ○ Remove privs **Oracle ID** *(for changes or deletions)*
Name	Michael Christopher Hyzer ([redacted]) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)
Expiration date (yyyy-Mon-dd)	
Type of access*	○ Business Objects ○ InfoView only ○ Other (please specify)
Supervisor Penn ID*	Find supervisor
Supervisor* (auto filled from above)	

Salary management eForm (continued)



Please specify level of access desired by selecting ORGs in the fields provided below.

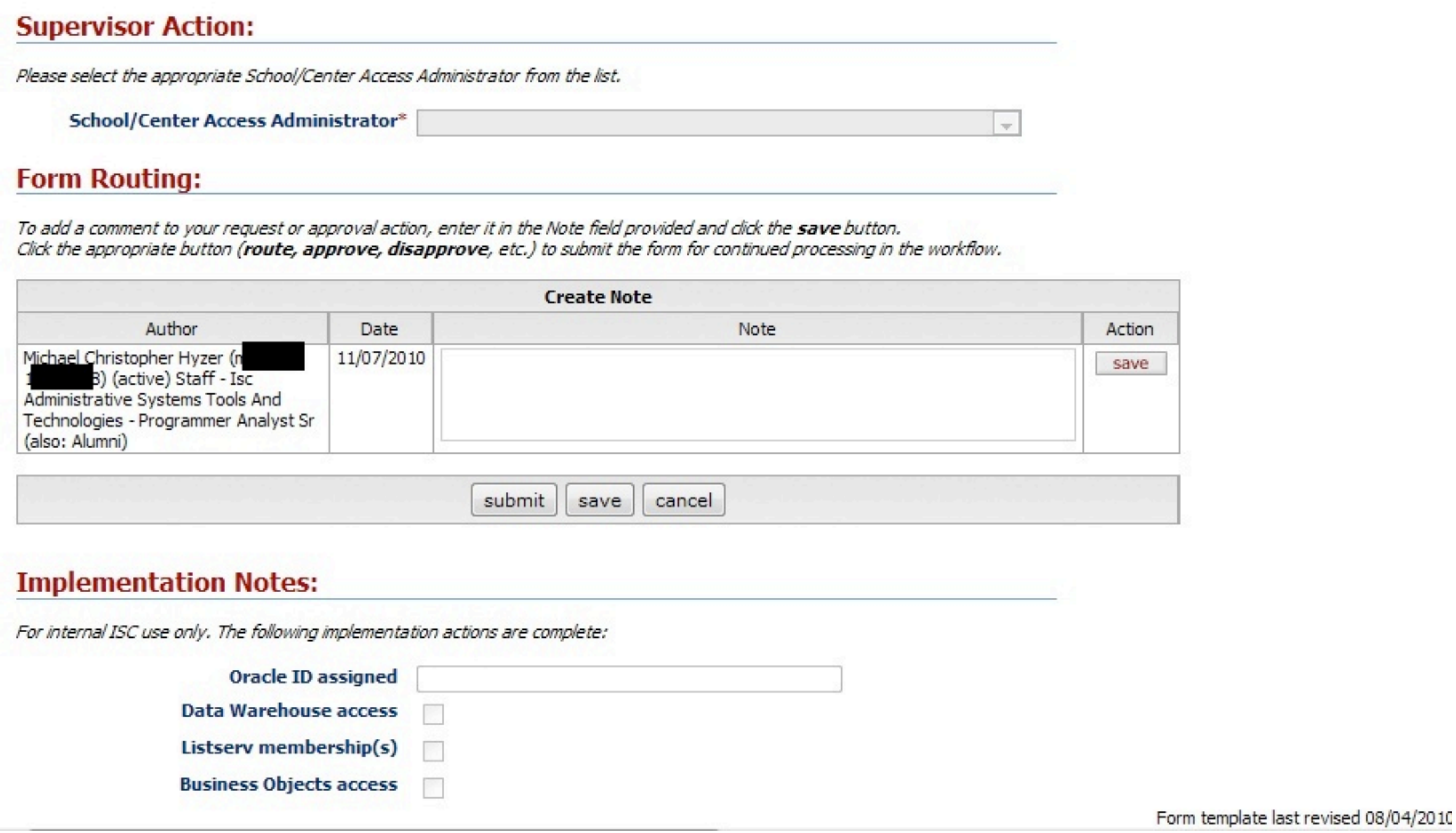
Org*	0107	Find org	UNIV:USCH:02XX:FBBA:ENGL:0107
Org		Find org	
Org		Find org	
Org		Find org	
Org		Find org	

More orgs

As an individual whose position requires interaction with any or all of the University's administrative information systems, I may be provided with direct access to confidential and valuable data and/or use of data systems. In the interest of maintaining the integrity of these systems and of ensuring the security and proper use of University resources, I will maintain the confidentiality of my password for all systems to which I have access. I will maintain in strictest confidence the data to which I have access. Any confidential information will not be shared in any manner with others who are unauthorized to view such data. I will use my access to the University's systems for the sole purpose of conducting official business of the University. I understand that the use of these systems and their data for personal purposes is prohibited. I understand that any abuse of access to the University's systems and their data, any illegal use of copying of software, any misuse of the University's equipment may result in disciplinary action, loss of access to the University's systems, and possible sanctions consistent with the University Policy on Adherence to University Policy.

I will abide by this policy* □

Salary management eForm (continued)



Supervisor Action:

Please select the appropriate School/Center Access Administrator from the list.

School/Center Access Administrator* [▾]

Form Routing:

*To add a comment to your request or approval action, enter it in the Note field provided and click the **save** button.*
*Click the appropriate button (**route, approve, disapprove**, etc.) to submit the form for continued processing in the workflow.*

Create Note			
Author	Date	Note	Action
Michael Christopher Hyzer ([redacted] [redacted]) (active) Staff - Isc Administrative Systems Tools And Technologies - Programmer Analyst Sr (also: Alumni)	11/07/2010		save

Implementation Notes:

For internal ISC use only. The following implementation actions are complete:

Oracle ID assigned [ ]

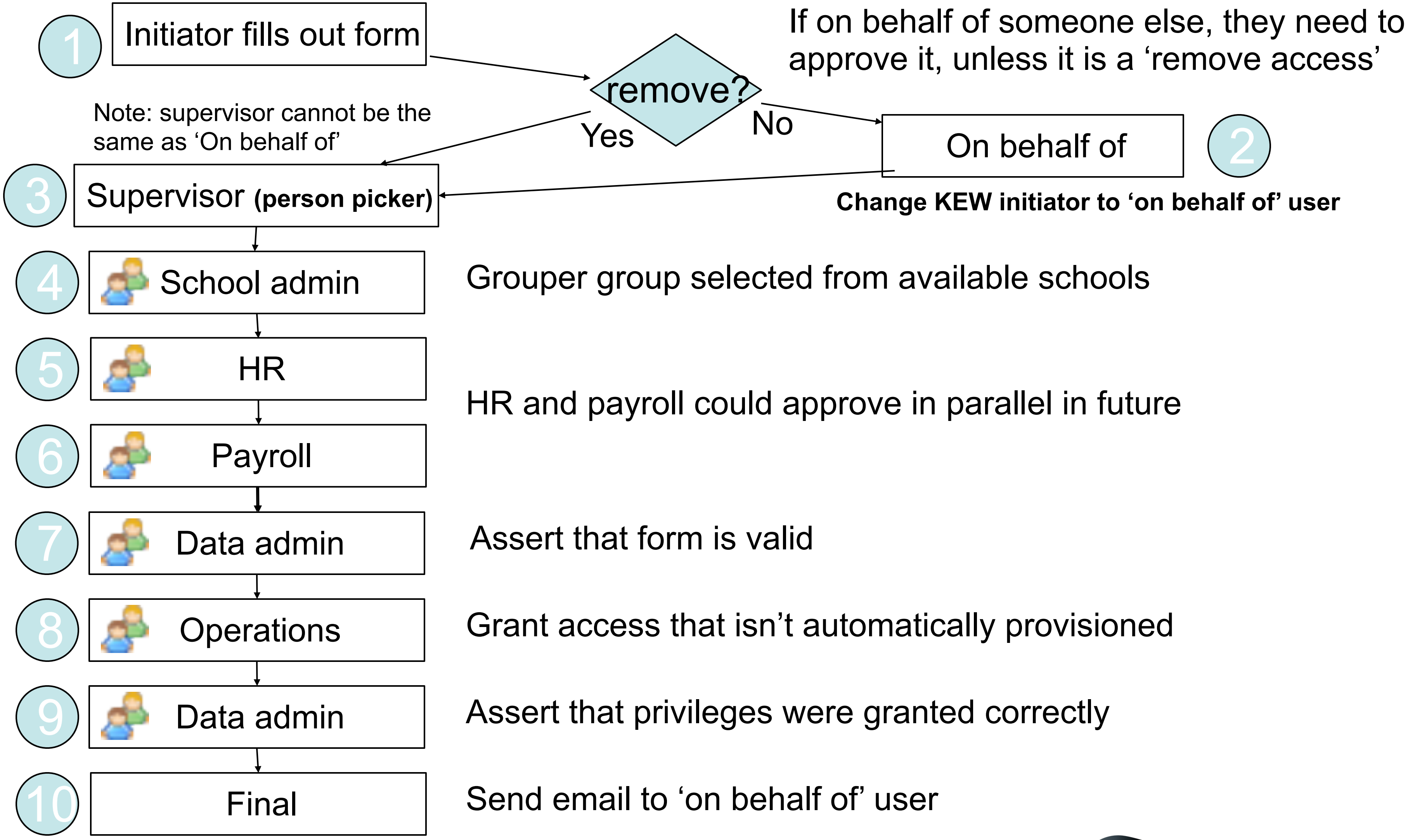
Data Warehouse access □

Listserv membership(s) □

Business Objects access □

Form template last revised 08/04/2010

eForms demo workflow



1 Initiator fills out form

remove?

If on behalf of someone else, they need to approve it, unless it is a 'remove access'

Note: supervisor cannot be the same as 'On behalf of'

Yes

No

On behalf of 2

Change KEW initiator to 'on behalf of' user

3 Supervisor **(person picker)**

4 School admin

Grouper group selected from available schools

5 HR

6 Payroll

HR and payroll could approve in parallel in future

7 Data admin

Assert that form is valid

8 Operations

Grant access that isn't automatically provisioned

9 Data admin

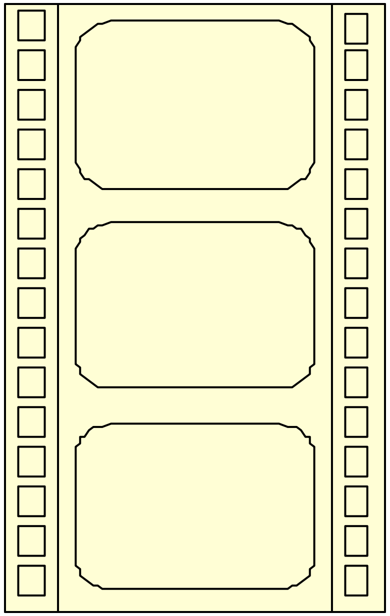
Assert that privileges were granted correctly

10 Final

Send email to 'on behalf of' user

Grouper Rice demo

- Demo movie



Grouper Rice group provisioning

- Grouper can provision groups and permissions when forms are complete, so generally Penn does not use it that way

Grouper and external users

Penn’s Secure Space

- Penn launched Secure Space in Fall 2010
- Initially it was for PennKey holders only
- 2011 we enabled external users
- 2013 we will retire this service in favor of Box.net

Penn’s Secure Space (continued)

- Secure Space is built on Grouper with three groups per space: admins, users, readonly
- When logging in, the grouper client / WS is used to cache the list of groups for user
- On create/delete space, GC/WS is used to create/delete groups
- Group memberships are managed via the membership lite UI screen

Penn’s Secure Space (continued)

- Penn’s Grouper has rules to only allow external users in certain SS folders
- Penn’s Grouper external users must be invited to be able to register
- SecureSpace uses InCommon
- EPPN is required for external users
- External users self-register their name, email, institution

Penn’s Secure Space (continued)

- Penn installed Shibboleth Discovery Service (DS/WAYF), customized:
  - Pennify
  - Support channel
  - Make it easy for Penn users
  - Recommend ProtectNetwork for users who don’t have an InCommon account which releases EPPN

Penn’s Secure Space (continued)

- Grouper shows external users with different icon, and description:
- [unverifiedInfo] First Last - institution [externalUserId] userId@institution.suf
- External users do not show in results for groups which do not allow external users
- Demo

Thanks!

Further information:

Infosheets, mail lists, wiki, downloads, etc:
www.internet2.edu/grouper

Grouper demo server:
https://grouperdemo.internet2.edu/