Groups API and federation in Grouper

Chris Hyzer
University of Pennsylvania

Groups API

- Started after ACAMP last year, "next step"
- Benn Oshrin founded FIFER: Free IdM Framework Education and Research
- Part of it is the API

Groups API (continued)

- Volunteers from Jasig, Grouper, Shib, Kuali, uportal…
- Starting on the spec
- Hopefully soon we will have a proof of concept
- Web service, client API

Groups API (continued)

- Vision is pluggability
- Connectors can be written against the FIFER Groups API which can ease integration and reuse

Federated Grouper

- Groups of external members
- Groups which can sync between Groupers (e.g. among institutions)
  - Hopefully this can use the FIFER Groups API at some point

Groups of external members - onboarding

- Various methods, configurable which or all is enabled
- Invite via email
- Enter in user ID (EPPN)
- Self-register

Link from invite screens

EXPLORE

Group summary ⓘ

Current location is:
📁 Root: 📁 aStem: 👥 **aGroup**

Name	aGroup
Path	aStem:aGroup
Description	users to be in astem agroup
ID	aGroup
ID Path	aStem:aGroup
Alternate ID Path	
UUID	0e0262d9be924774914052c12f0e7fd2
Types	base members *List field*

Show entities with ADMIN ▾ privilege

Delete   **Add to Group workspace**   **Edit group**   **Manage members**   **Add members**   M

Invite external people   **Move group**   **Copy group**   **Audit log**   **View entity details**

RNET®

Link from invite screens (continued)

Invite form

Invite external people to participate in groups ⓘ

* indicates a required field

Enter the invitation information

Email addresses of people to invite *

Email subject Register to access applications

Message to users

Hello,

This is an invitation to register at
our site to be able to access our
applications. This invitation expires
in 7 days. Click on the link below and
sign in with your InCommon

Email addresses to notify when registered

Groups to assign to new users Enter search text to find a group

penn:isc:ait:apps:secureSpace:spaces:space_CHRIS_TEST_PAID:chris test paid Secure

Enter search text to find a group

Enter search text to find a group

Invite via userId (EPPN)

Invite external people to participate in groups ⓘ

* indicates a required field

Enter the invitation information

Invite by * ○ Email address   ◉ Login ID

Login IDs of people to invite *
```
a@b.c
GrouperSystem
whatever
```

Groups to assign to new users   Enter search text to find a group

👥 etc:test

Enter search text to find a group

👥 etc:webServiceClientUsers

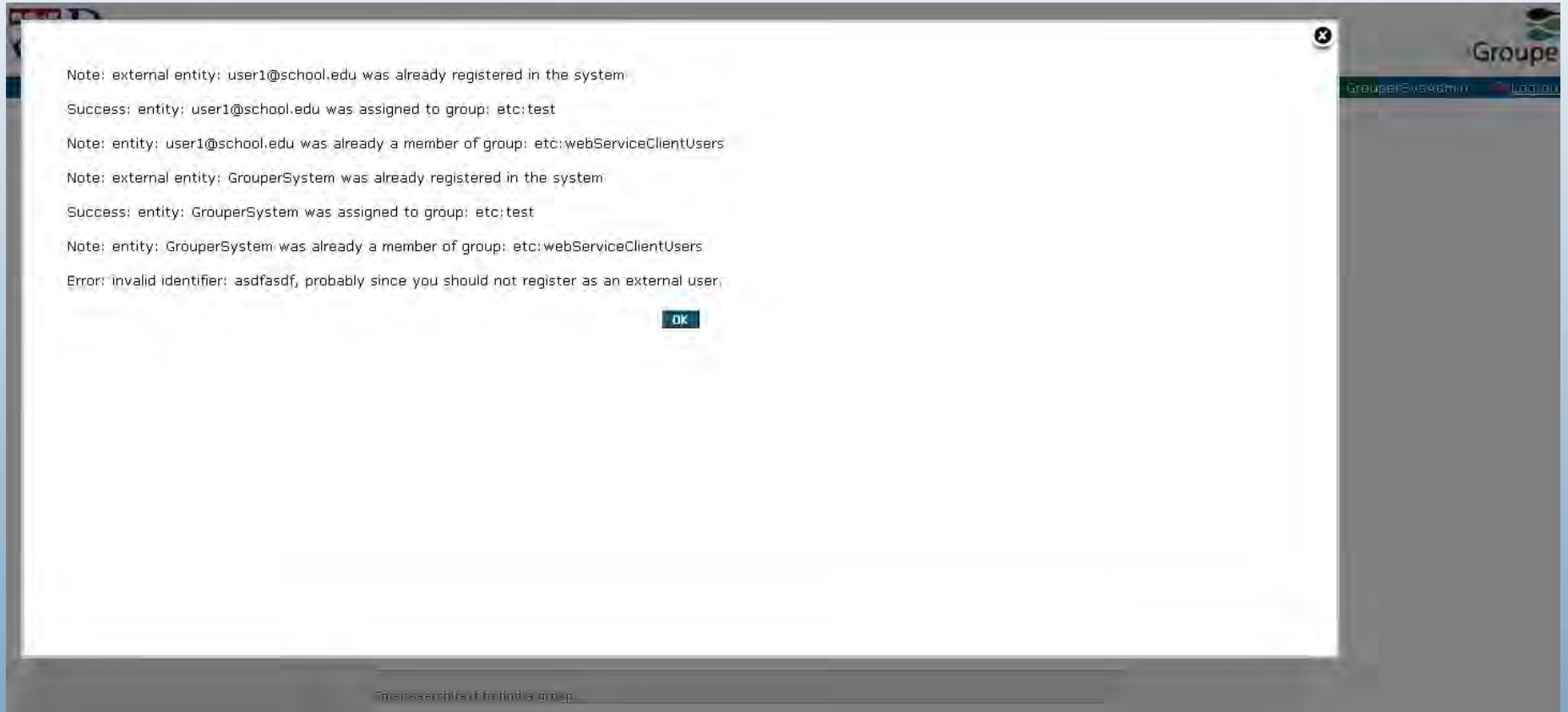Enter search text to find a group

Enter search text to find a group

Enter search text to find a group

Submit

Invite by userID result

Note: external entity: user1@school.edu was already registered in the system

Success: entity: user1@school.edu was assigned to group: etc:test

Note: entity: user1@school.edu was already a member of group: etc:webServiceClientUsers

Note: external entity: GrouperSystem was already registered in the system

Success: entity: GrouperSystem was assigned to group: etc:test

Note: entity: GrouperSystem was already a member of group: etc:webServiceClientUsers

Error: invalid identifier: asdfasdf, probably since you should not register as an external user.

OK

Invite or self registration screen

Invite or self registration screen

- Yes, we should (will?) pre-populate the register screen if attributes are sent

External users in a membership list

Customize where externals can be

Pluggable storage

- You can implement an interface to store external people elsewhere than Grouper DB

Grouper UI can share authn

- URLs in Grouper UI for external / internal are distinct
- At Penn, the registration part is protected by Shib
- The Admin and Lite UI are protected by Cosign
- Of course it could be all Shib (or external)

In use in prod at Penn in Grouper 1.7

- Deployed 1 month ago
- So far so good
- Google "grouper external users" for <u>doc</u>

Syncing groups between groupers

Syncing groups between groupers

- Assumes some sort of external subjects
    - How else could they resolve?
- Configure a connection to another Grouper via the grouperClient
    - Should survive varying versions of Grouper on each side
- Map a group from one to the other
- Map which subjects should sync

INTERNET®

Sync types

- Scheduled pull (destination needs WS creds and privs on source)
- Scheduled push (source needs WS creds and privs on destination)
- Scheduled push + incremental (source needs WS creds and privs on dest)
  - Real time updates with periodic full sync

INTERNET®

Syncing groups between Groupers

- Do this to use groups in other groupers
- Systems in one institution do not need to immediately depend on other institution's resources
- Two Grouper 2.0's on demo server are running this
- Google "Grouper sync" for doc

INTERNET2®