Internet2 Techex 2017

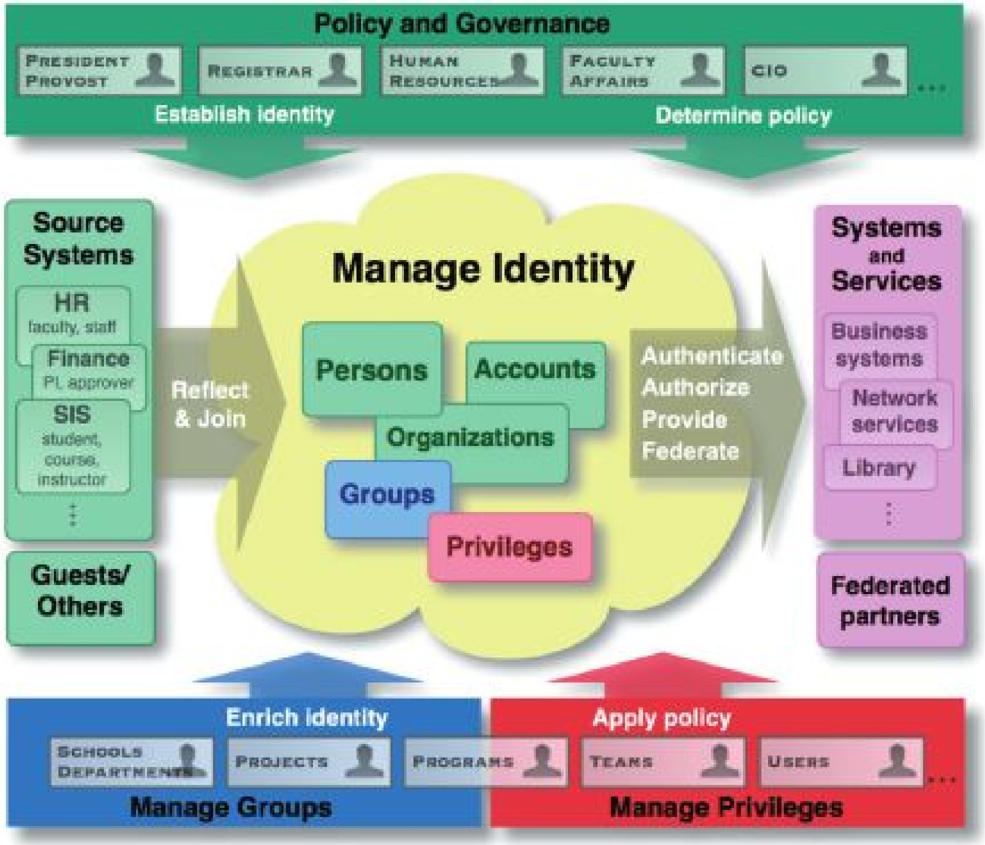
Grouper in Action

Chris Hyzer, University of Pennsylvania
Bill Thompson, Lafayette College
Carl Waldbieser, Lafayette College
Bert Bee-Lindgren, Georgia Tech

Agenda

1. **Introduction to Grouper**
   a. Grouper Overview
   b. Features and capabilities
   c. What’s new
2. **Hands on Grouper**
   a. Folder and group management
   b. Searching and adding subjects
   c. Direct vs indirect membership
   d. Grouper loader jobs
   e. Composite group
3. **TIER deployment guide**
4. **Grouper @ LaFayette**
5. **Grouper @ GaTech**
6. **Open Q&A**

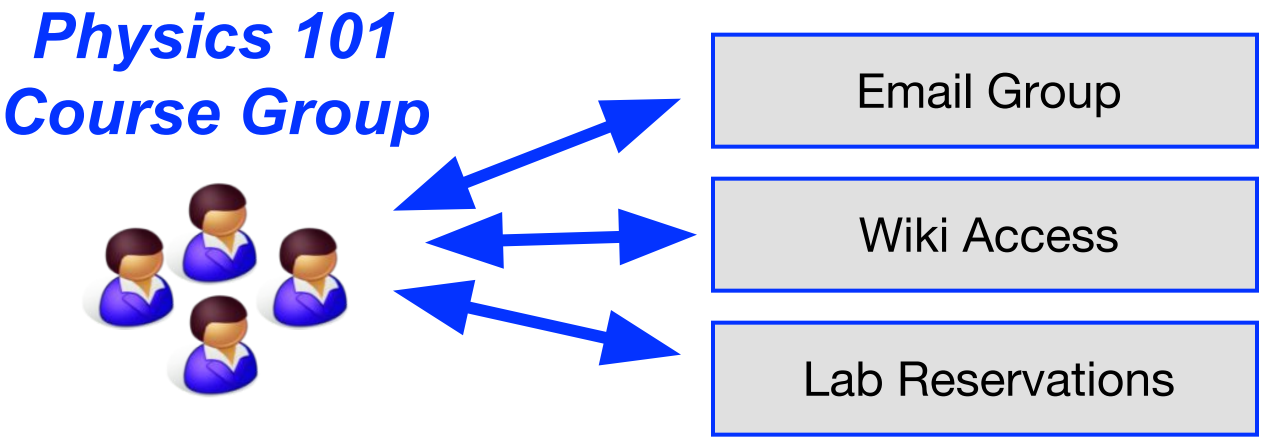
Access management strategy



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

Why have an access management strategy?

- Lower cost and time to deliver a new service
- Simplify access management by using the same group in many places
- Empower the right people to manage access
- Answer who can access what



Physics 101 Course Group

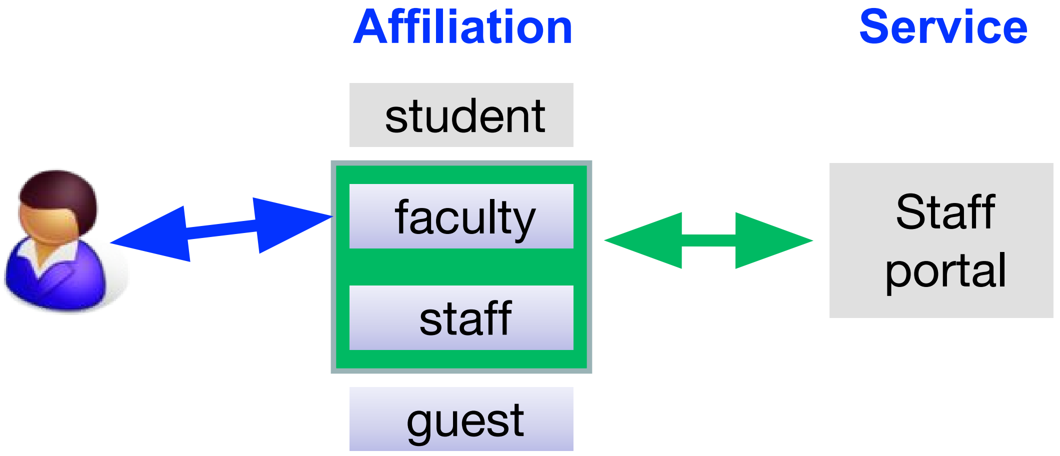
Email Group

Wiki Access

Lab Reservations

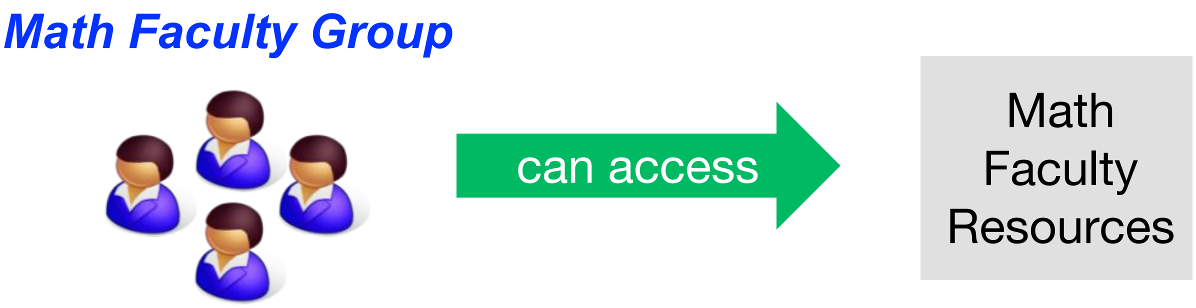
Access management stages:

1. Start out using a single user attribute, *affiliation*, in an Enterprise Directory. Services implement simple access policies.



Access management stages

2. Maintain access groups determined from systems of record
    - Courses, departments,…
    - Define service-specific access policies in the centralized access management system



Math Faculty Group

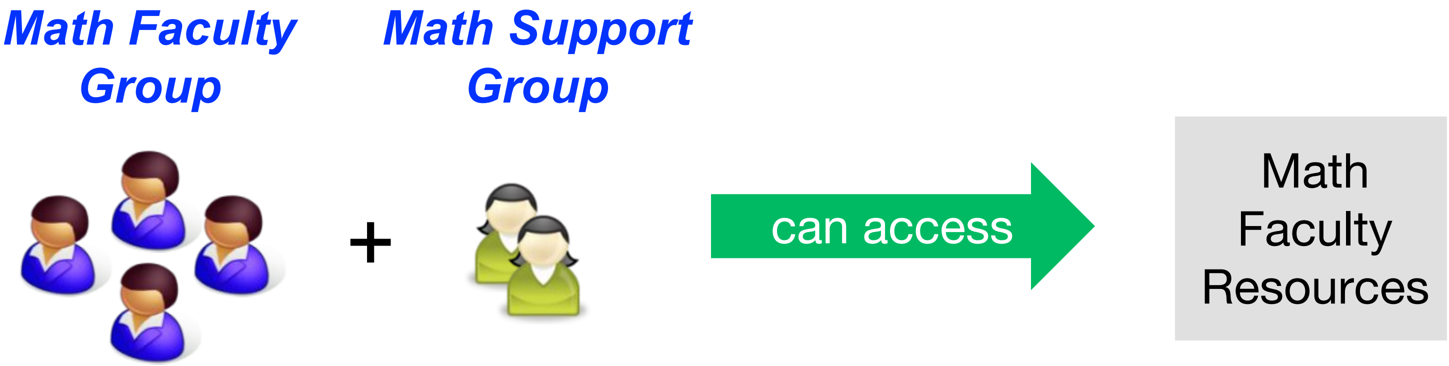
can access

Math Faculty Resources

Access management stages

3. Distributed management

- Departmental applications
- Ad-hoc teams
- Exceptions



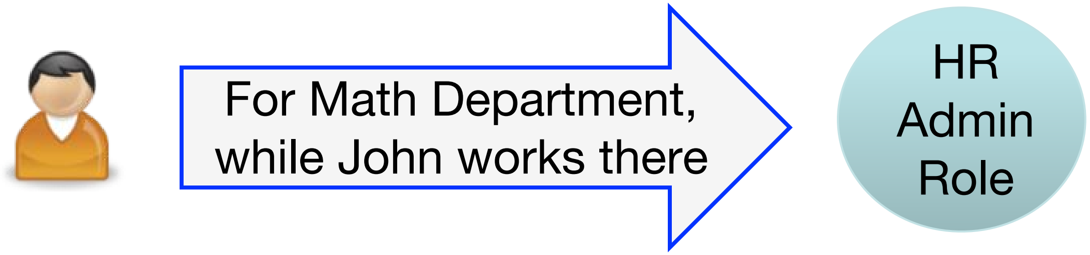
Math Faculty Group + ***Math Support Group***

can access

Math Faculty Resources

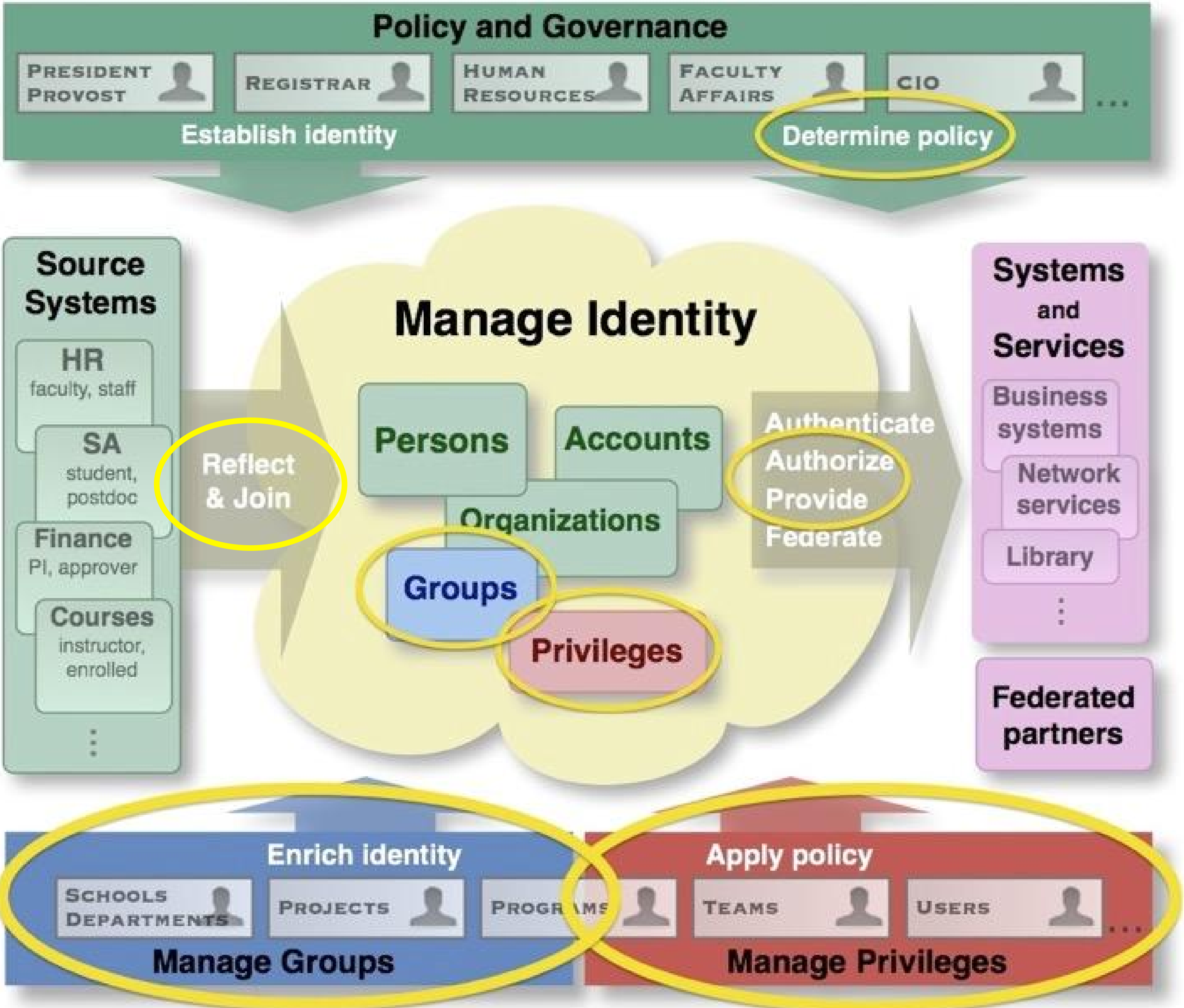
Access management stages

4. Increase integration
   - Direct integration with applications
   - Roles & privileges to support applications more deeply



For Math Department, while John works there

HR Admin Role


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
Apply policy
Teams
Users
...
Manage Groups
Manage Privileges

Grouper is…

Grouper is an **enterprise access management system** designed for the highly distributed management environment and heterogeneous information technology environment common to Universities.

- Coordinated Collaboration
- Single Point of Control
- Distributed Management

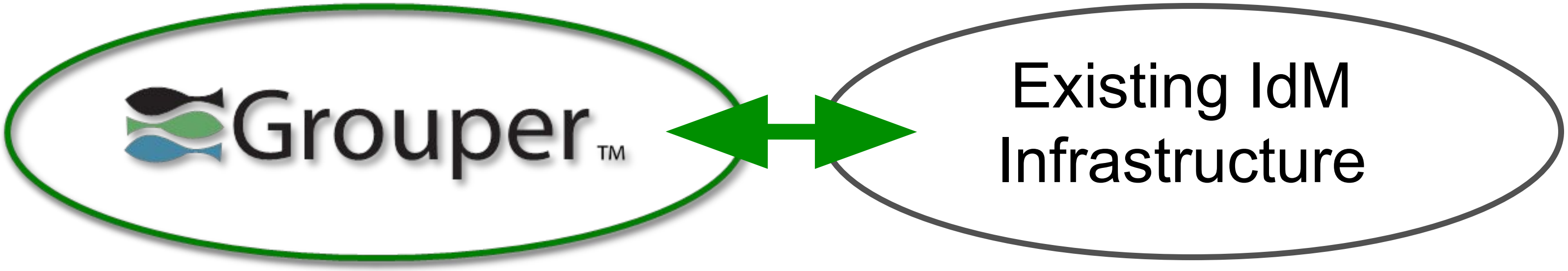
The Grouper Story

- Mature, community driven project (2005 initial release)
- Internet2
- National Science Foundation (NSF) Grant No. OCI-0330626, OCI-0721896, and OCI-1032468
- Joint Information Systems Committee (JISC) (UK)
- University of Chicago, University of Pennsylvania, Duke University, University of Washington, University of Memphis, University of Bristol (UK)

Grouper

The Grouper Story

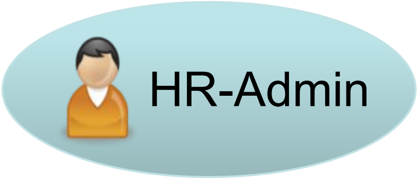
- Key aims
  - Delegation and distributed management
  - Integration with most any existing Identity Management infrastructure



Existing IdM Infrastructure

The Grouper Story

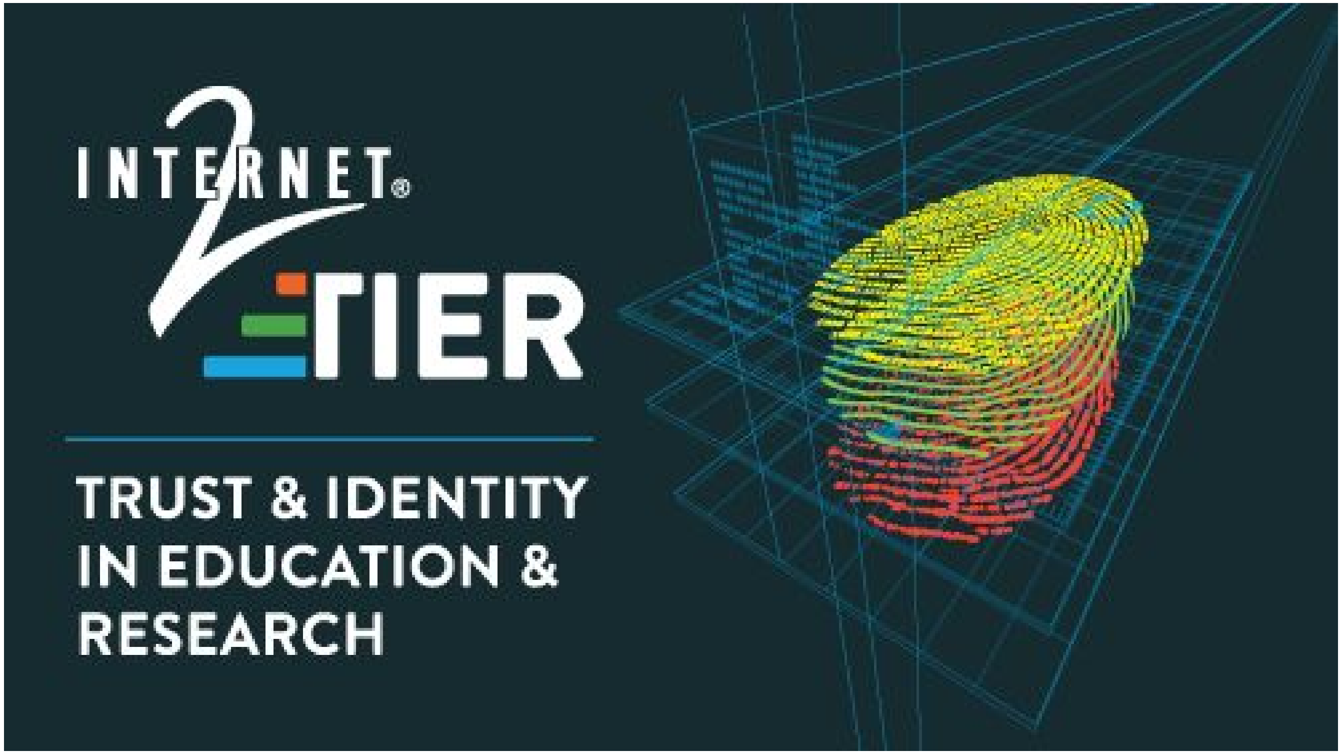
- Grouper v2.X expanded beyond groups
  - Roles & permissions



HR-Admin

  - Rules

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

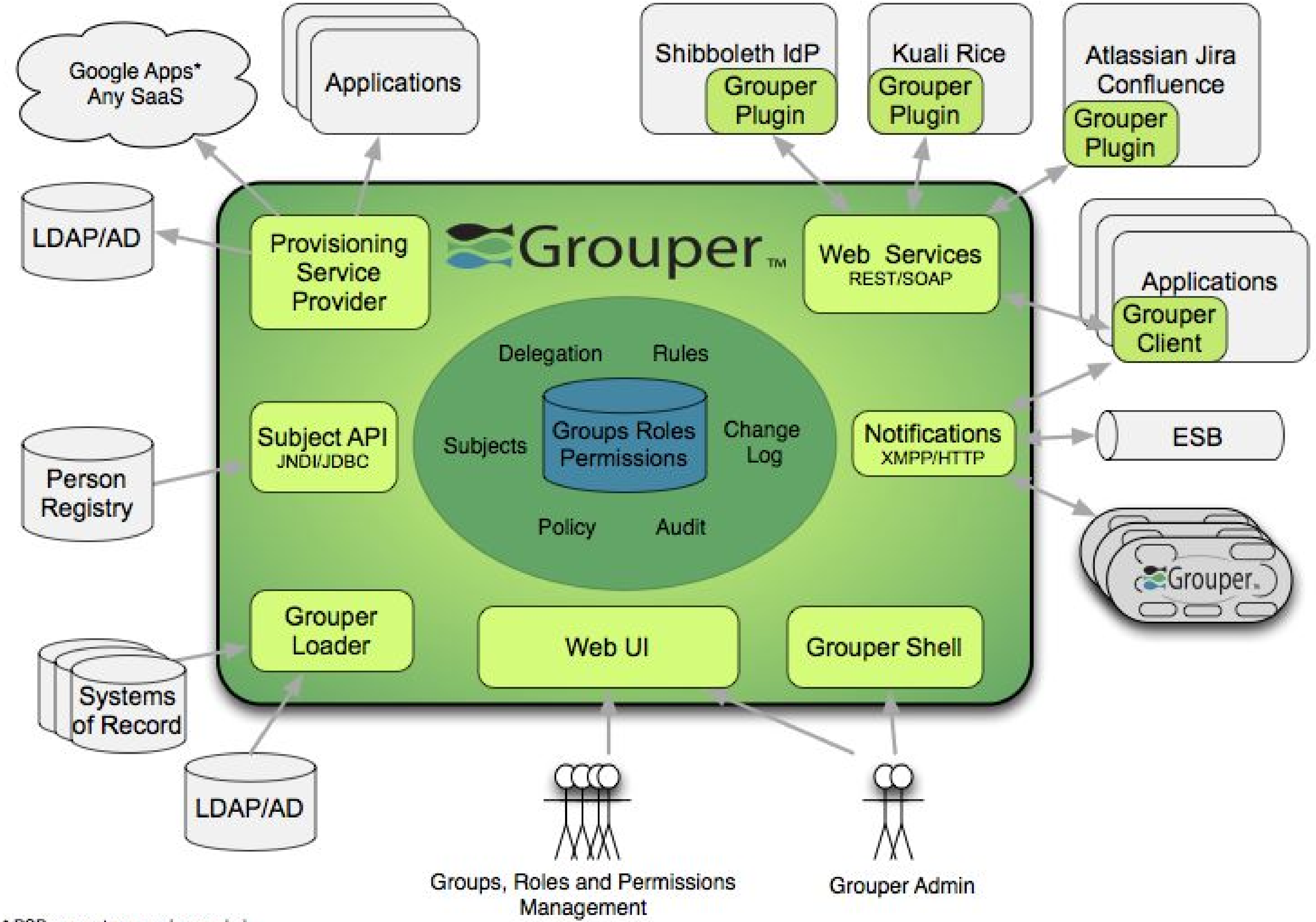


*"We view TIER as a **coordinated approach to enable trust and identity in education and research** at scale for thousands of institutions and service providers while also satisfying diverse local use cases."*

—Ron Kraemer, Vice President and CIDO, University of Notre Dame

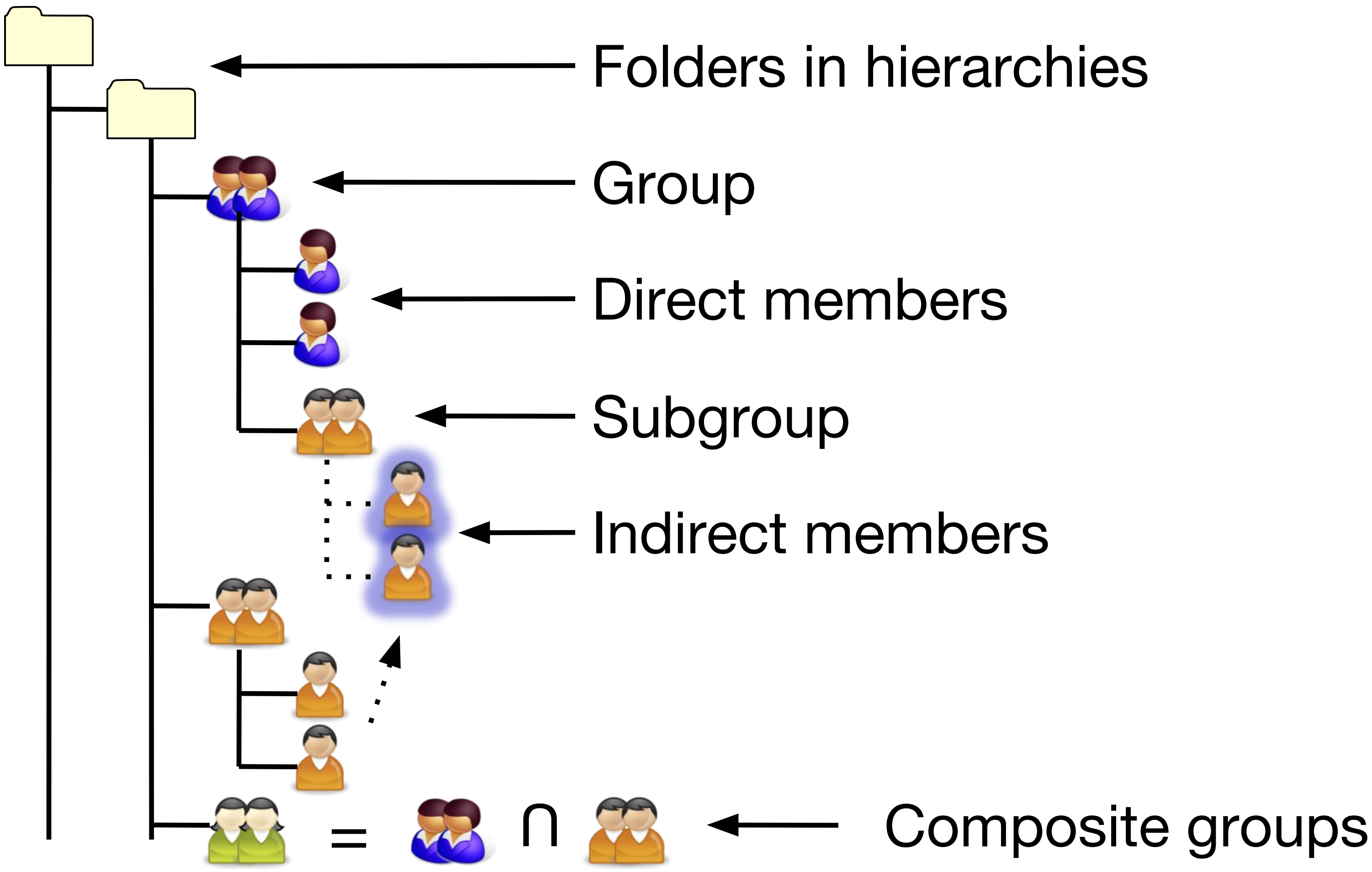
*“It’s not just about federation, it’s about **enabling high-value collaboration across thousands of disciplines and millions of people.** Hence agreement on attribute and authorization management, application integration, administration procedures,...”*

— RL ‘Bob’ Morgan



* PSP connectors may be needed

Grouper Concepts



Folders in hierarchies

Group

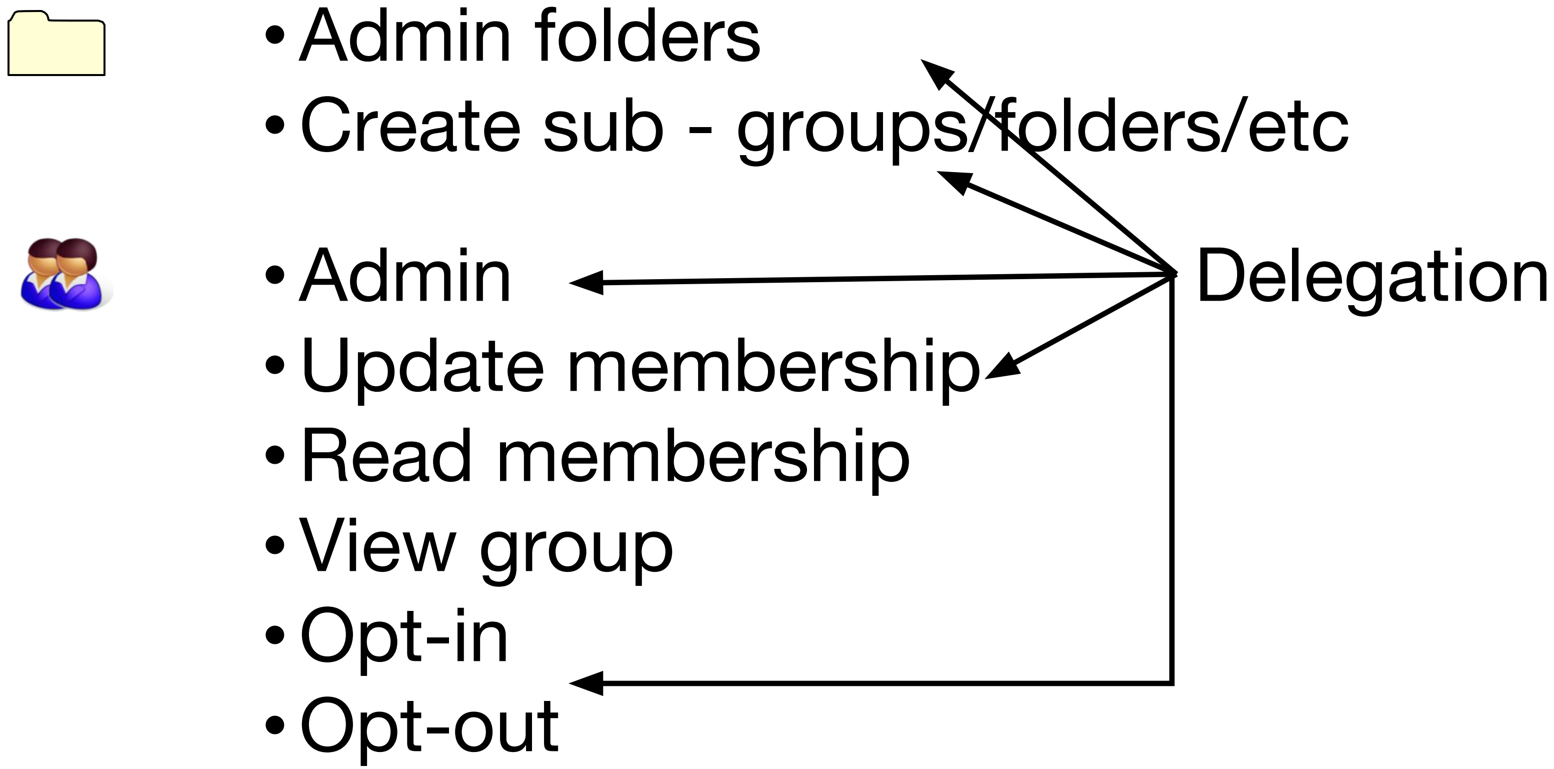
Direct members

Subgroup

Indirect members

Composite groups

Security and Delegation



- Admin folders
- Create sub - groups/folders/etc

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

Delegation

Access management lifecycle support

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

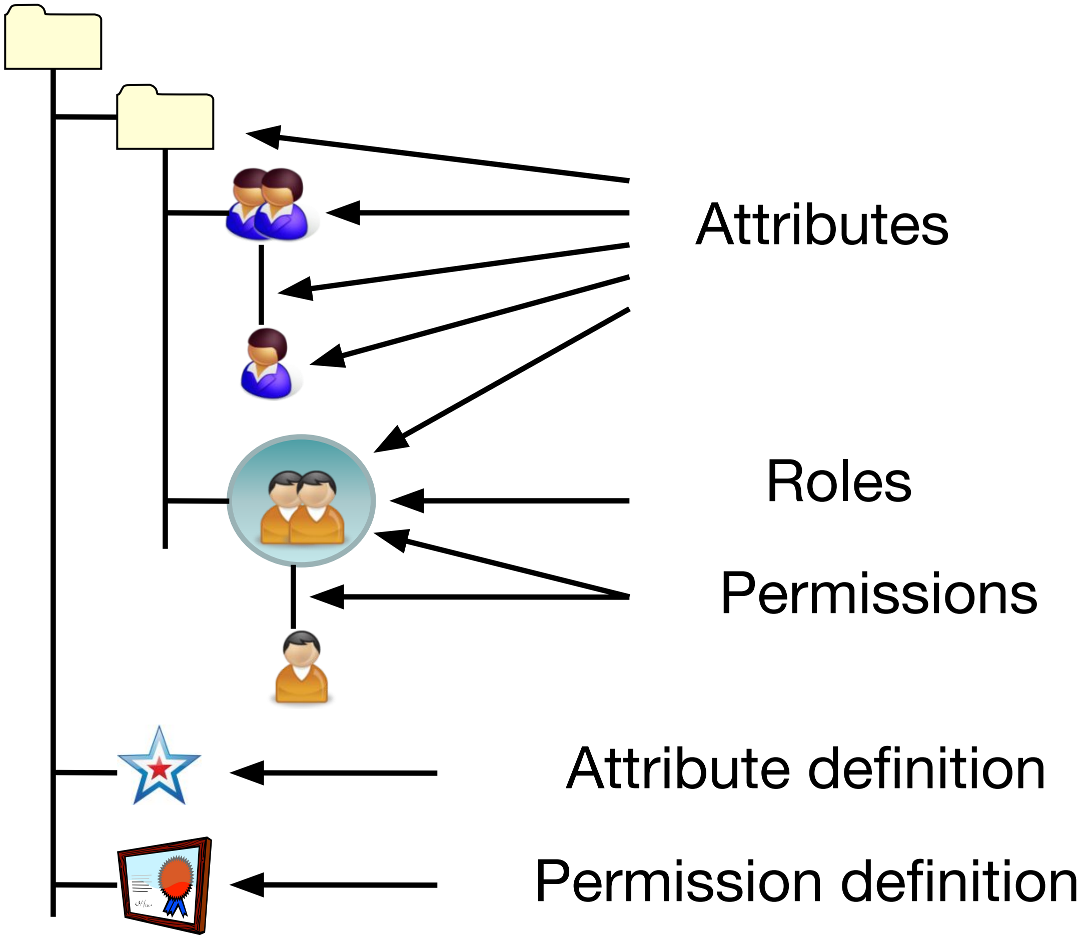
Auditing

- “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 loader

- Daemon that periodically syncs external sources with Grouper
- Can work for groups or permissions (e.g. org chart)
- SQL or LDAP sources
- Grouper admins can configure jobs based on attributes

Beyond groups...



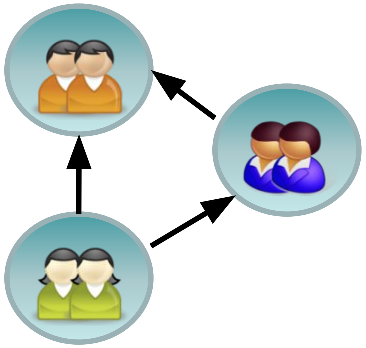
Attributes

Roles

Permissions

Attribute definition

Permission definition



Role inheritance

Delegation model extends that for Groups

Internet2 Techex 2017

Grouper - What’s new?

Grouper in Action

Release 2.3.0.patch new features

See release notes for full list

https://spaces.internet2.edu/display/Grouper/v2.3+Release+Notes

(google “grouper release notes”)

- Grouper loader improvements for real time updates
- External subject web services
- Find bad memberships daemon
- TIER instrumentation (with UI)
- Migrate XML config to properties overlays

Release 2.3.0.patch new features (continued)

- Subject API diagnostics
- Grouper loader in UI
- Attestation
- New GSH command line utility
- Messaging implementation, WS, and service bridge
- Many UI usability improvements
- Provisioning fixes and improvements
- Lots of other improvements

Grouper roadmap

- Migrate to New UI
- Deprovisioning in UI
- Provisioning in UI
- Other UI features:
  - Membership reports
  - Migrate entitlements from one user to another
- Configuration stored in database

Internet2 Techex 2017

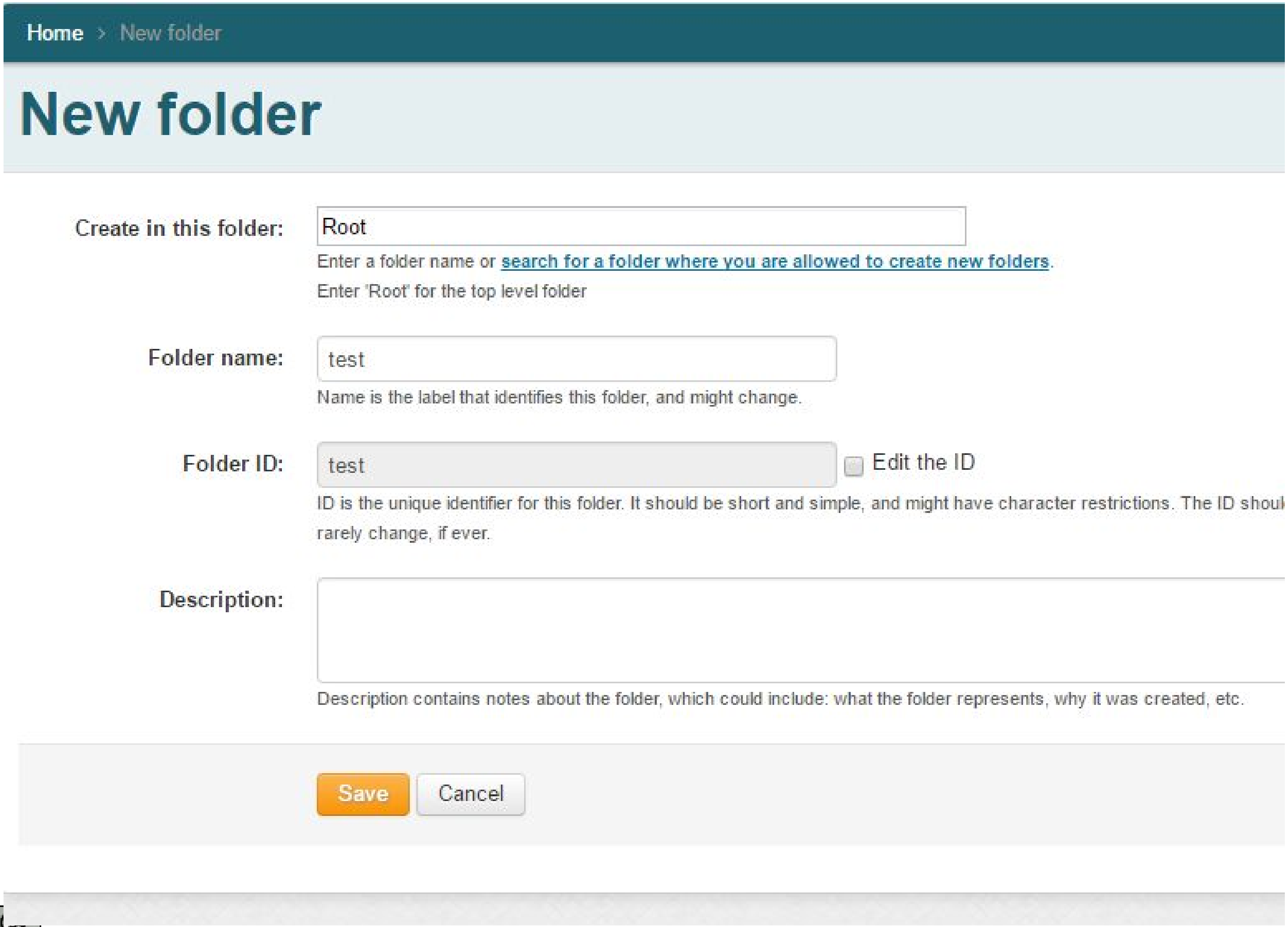
Grouper - Hands on Grouper

Grouper in Action

Create new folder

- Go to grouper demo (google “grouper demo”)
- https://grouperdemo.internet2.edu
- Click on UI 2.3
- Go to the folder: training:techEx2017
- Create a folder based on your netID (e.g. mchyzer).
  - Dont use special chars except maybe underscore.
- Click into that folder

Create new folder



New folder

Create in this folder: Root

Enter a folder name or search for a folder where you are allowed to create new folders.

Enter 'Root' for the top level folder

Folder name: test

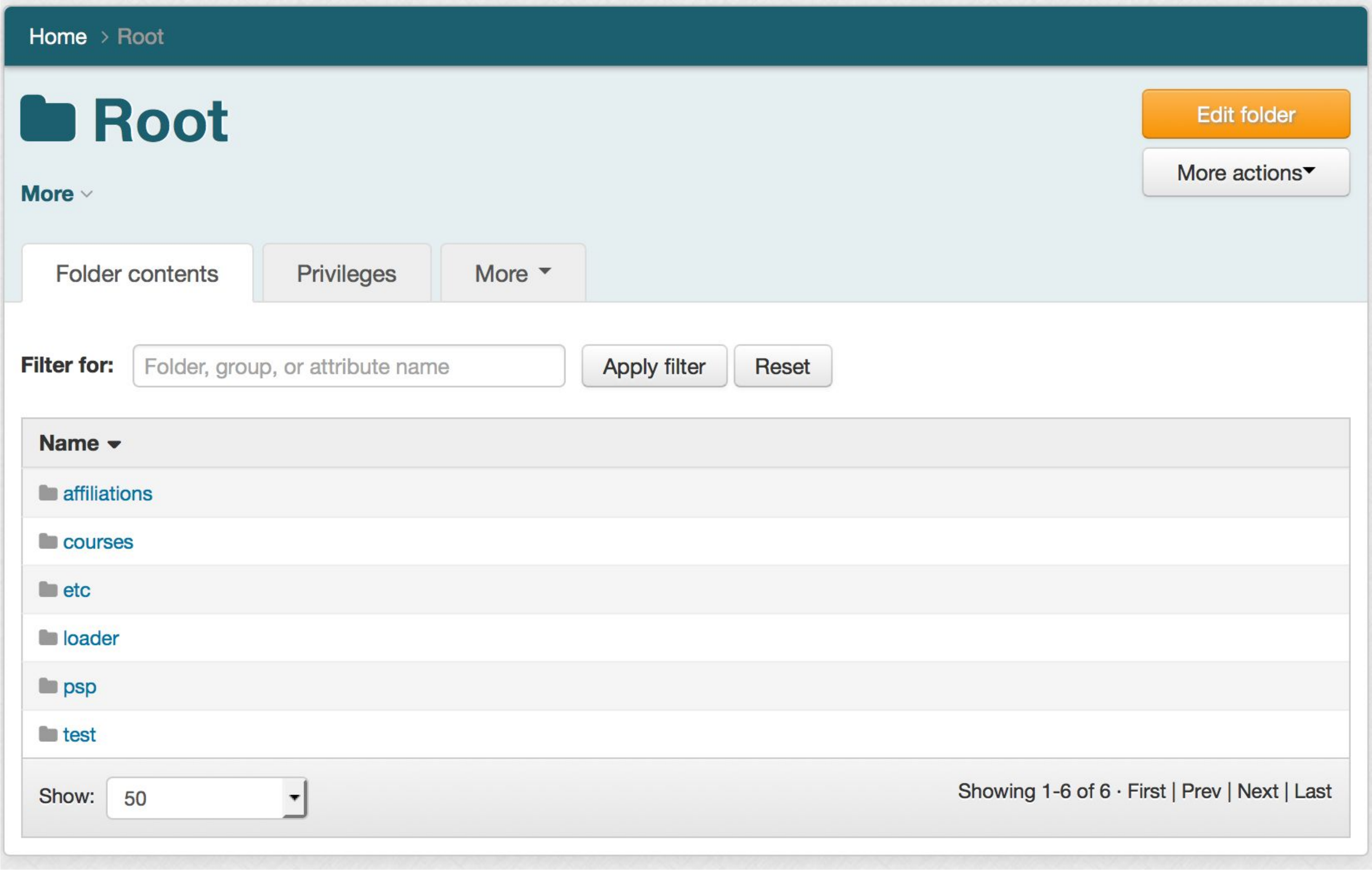
Name is the label that identifies this folder, and might change.

Folder ID: test □ Edit the ID

ID is the unique identifier for this folder. It should be short and simple, and might have character restrictions. The ID shoul rarely change, if ever.

Description:

Description contains notes about the folder, which could include: what the folder represents, why it was created, etc.



Root

Filter for: Folder, group, or attribute name

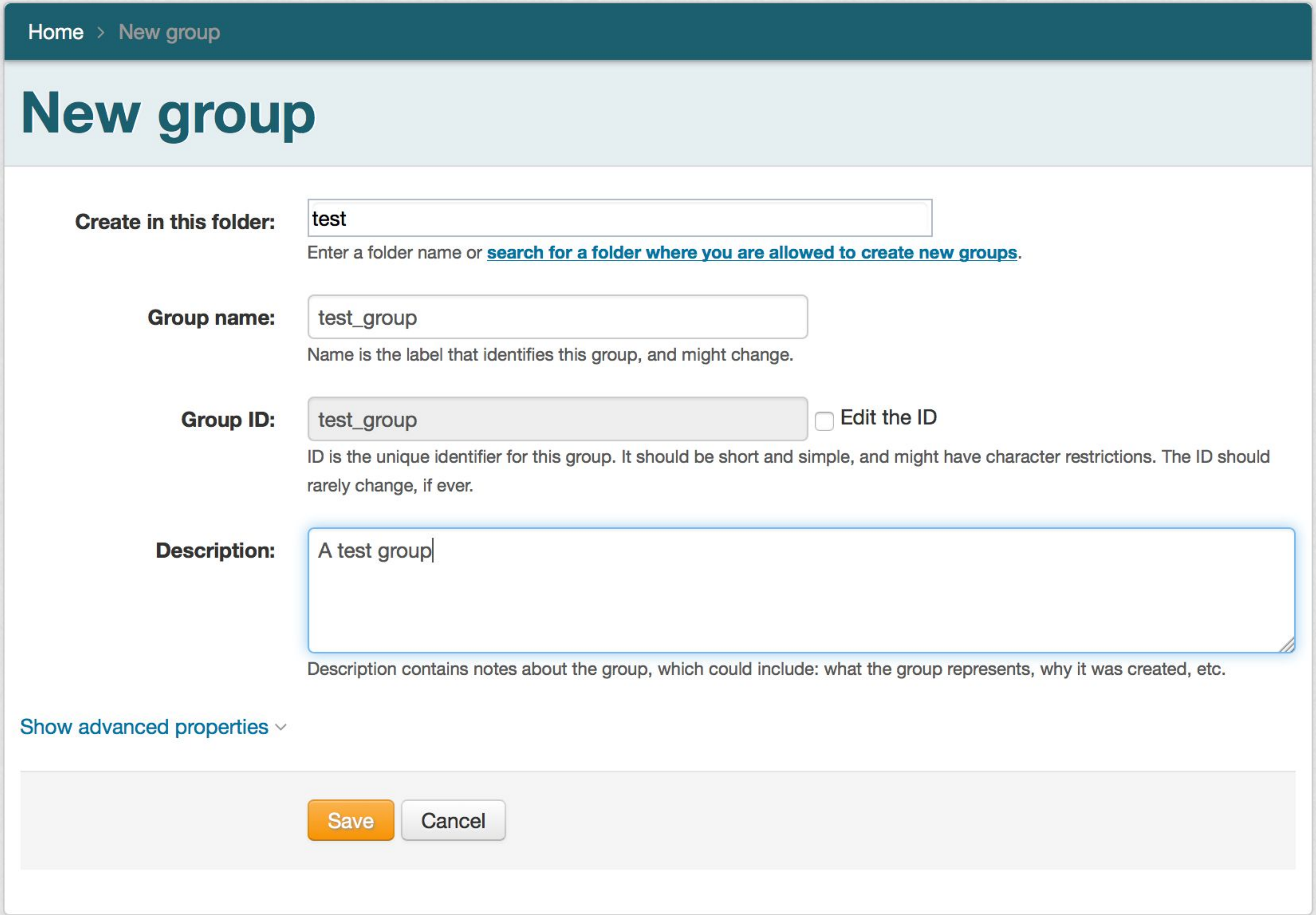
Name
affiliations
courses
etc
loader
psp
test

Show: 50

Showing 1-6 of 6 · First | Prev | Next | Last

Create an “apps” folder in your folder

- In “apps”, make a “wiki” folder
- In “wiki”, make an “etc” folder
  - Sometimes the extension of the folder shows in the UI, so make it unique-ish e.g. “wikiEtc”
- In “etc”, make an admins group
  - Sometimes the extension of the group shows in the UI, so make it unique-ish e.g. “wikiAdmins”
- Talk to your neighbors, get their name, add them to the wiki admins group



New group

Create in this folder: test

Enter a folder name or search for a folder where you are allowed to create new groups.

Group name: test_group

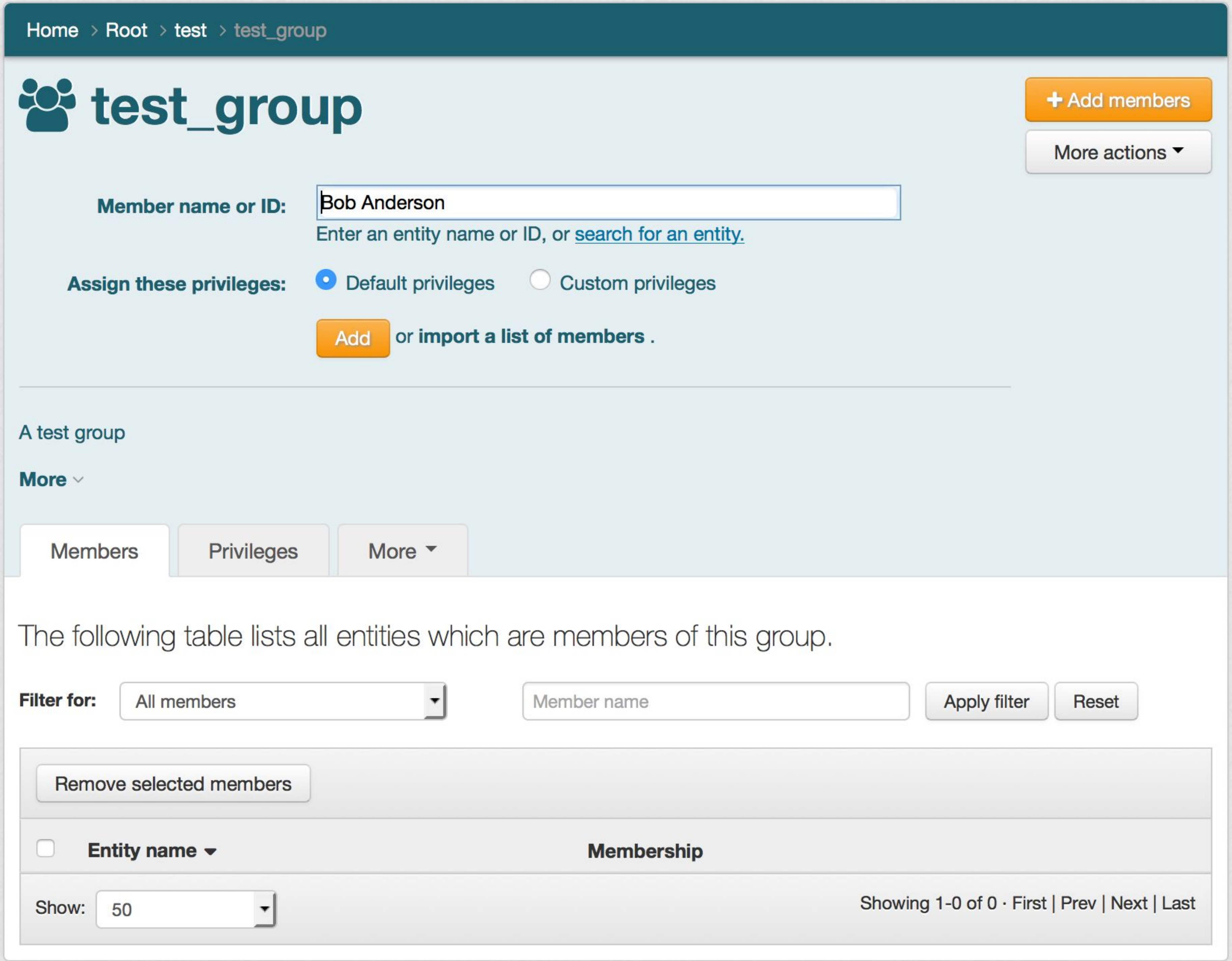
Name is the label that identifies this group, and might change.

Group ID: test_group ☐ Edit the ID

ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

Description: A test group

Description contains notes about the group, which could include: what the group represents, why it was created, etc.



test_group

Member name or ID: Bob Anderson

Enter an entity name or ID, or search for an entity.

Assign these privileges: ● Default privileges ○ Custom privileges

Add or **import a list of members** .

A test group

More

The following table lists all entities which are members of this group.

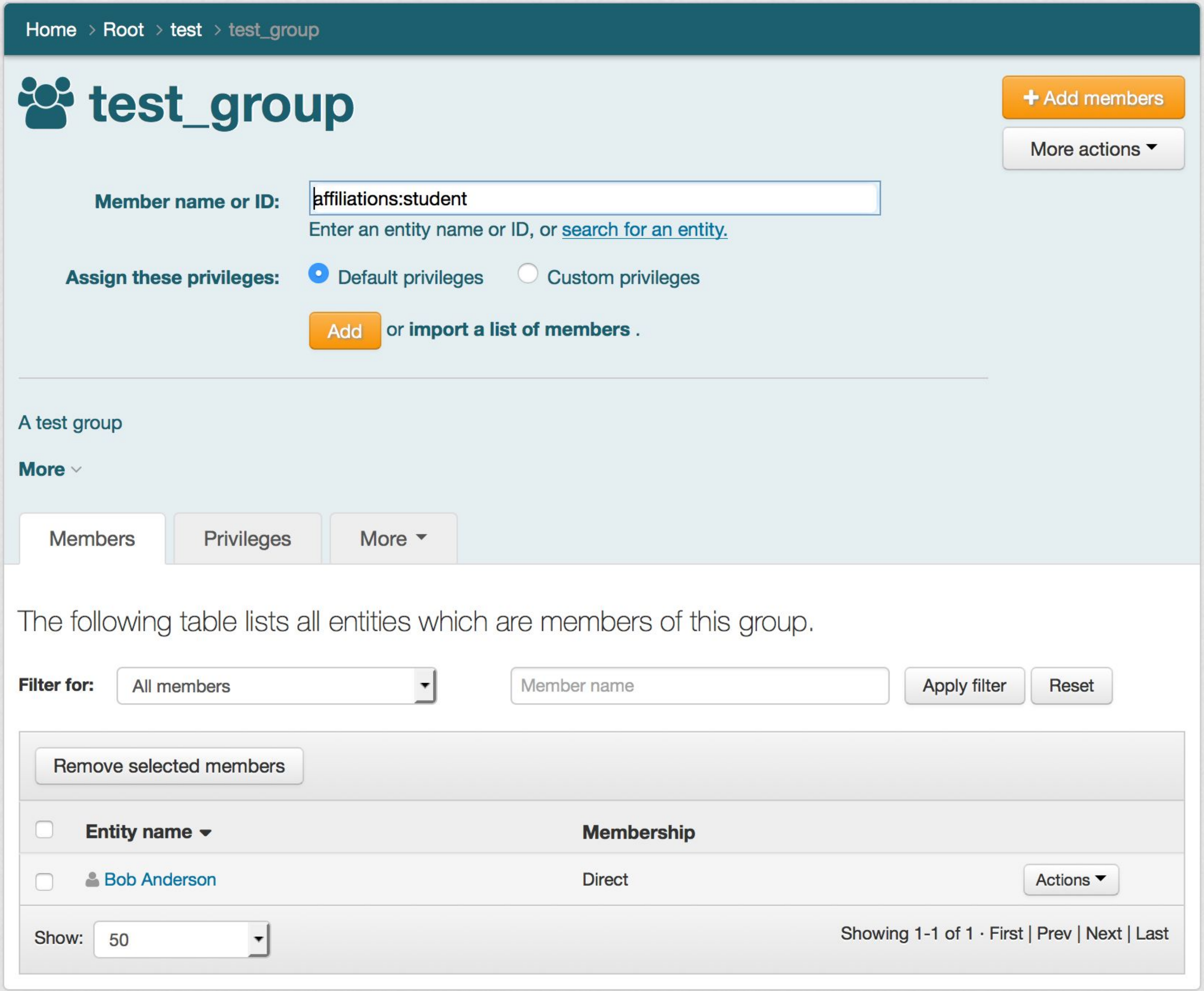
Filter for: All members

Member name

□	Entity name	Membership

Show: 50

Showing 1-0 of 0 · First | Prev | Next | Last



Home > Root > test > test_group

test_group

Member name or ID: affiliations:student

Enter an entity name or ID, or search for an entity.

Assign these privileges: ● Default privileges ○ Custom privileges

Add or **import a list of members** .

A test group

More

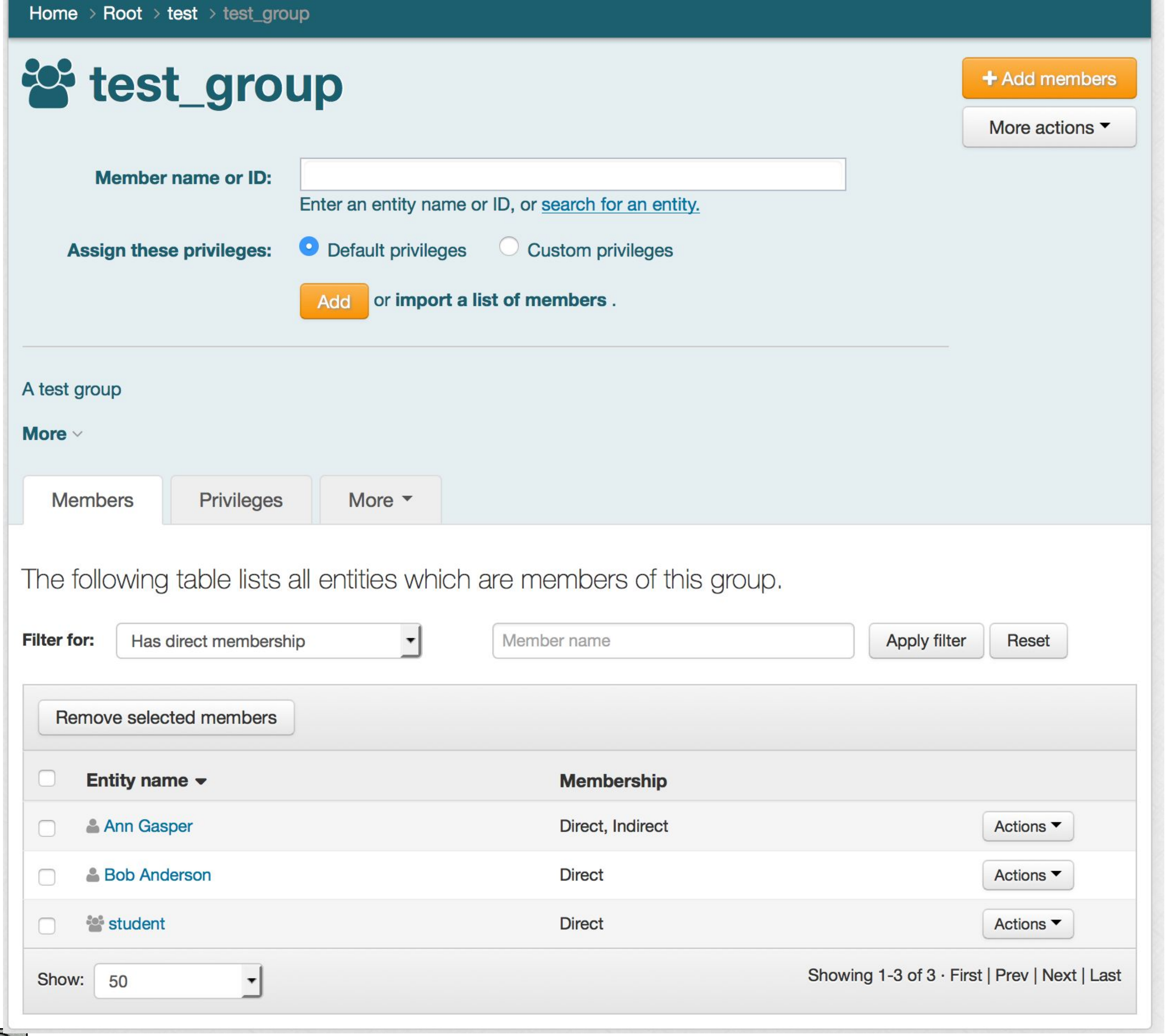
The following table lists all entities which are members of this group.

Filter for: All members — Member name

□	Entity name	Membership	
□	Bob Anderson	Direct	Actions

Show: 50

Showing 1-1 of 1 · First | Prev | Next | Last



test_group

Member name or ID:

Enter an entity name or ID, or search for an entity.

Assign these privileges: ● Default privileges ○ Custom privileges

Add or import a list of members .

A test group

More ⌄

The following table lists all entities which are members of this group.

Filter for: Has direct membership ▾ Member name

□	Entity name ▾	Membership	
□	Ann Gasper	Direct, Indirect	Actions ▾
□	Bob Anderson	Direct	Actions ▾
□	student	Direct	Actions ▾

Show: 50 ▾

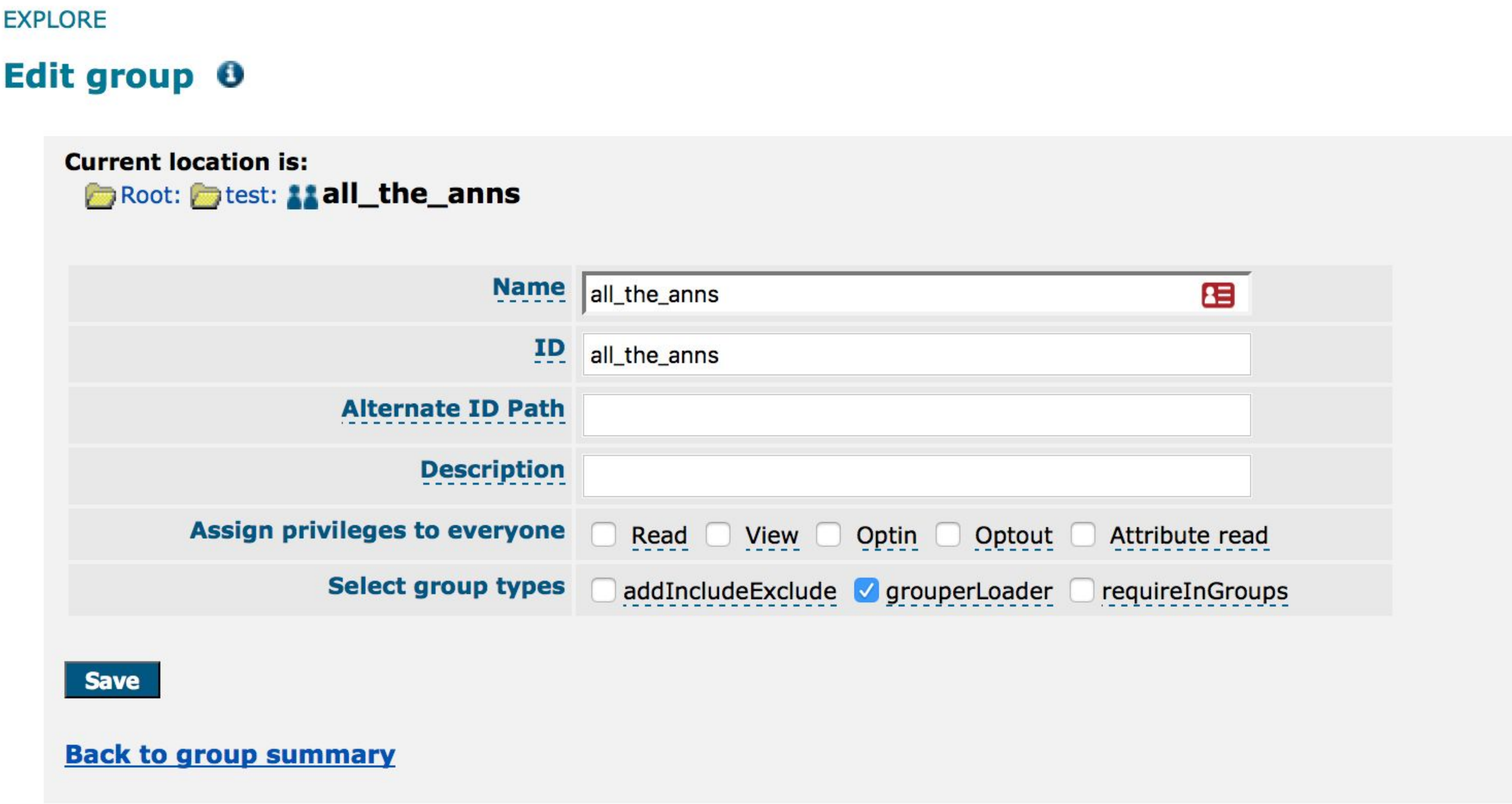
Showing 1-3 of 3 · First | Prev | Next | Last

Assign hierarchical privs to wiki folder

- Go to wiki folder
- On the “More” tab
- Click “privileges inherited to objects in folder”
- Add
- Find your wiki admins group
- Assign to all types: ADMIN
- Create a wikiUsers group
- Have your neighbor verify that they can add/remove members to that group

Turn the group into include/exclude

- Click on Admin UI
- Find the group
- Edit
- “Add include/exclude”
- Save
- Go back to New UI



EXPLORE

Edit group

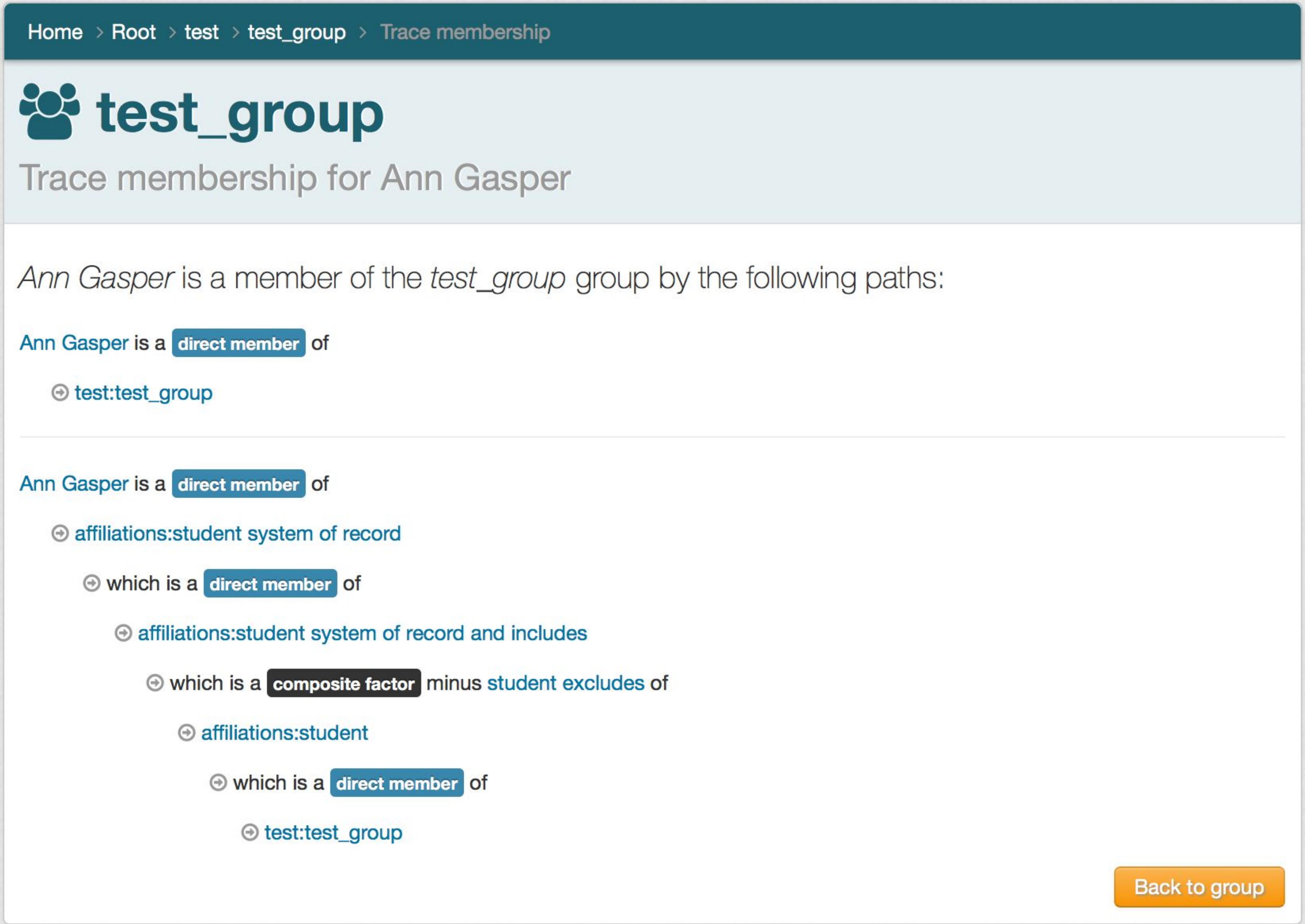
Current location is:

Root: test: **all_the_anns**

Name	all_the_anns
ID	all_the_anns
Alternate ID Path	
Description	
Assign privileges to everyone	□ Read □ View □ Optin □ Optout □ Attribute read
Select group types	□ addIncludeExclude ☑ grouperLoader □ requireInGroups

Go back to New UI, analyze membership

- Go to overall group
- See a membership
  - If none there, then add one to the system of record
- Actions -> trace membership



test_group

Trace membership for Ann Gasper

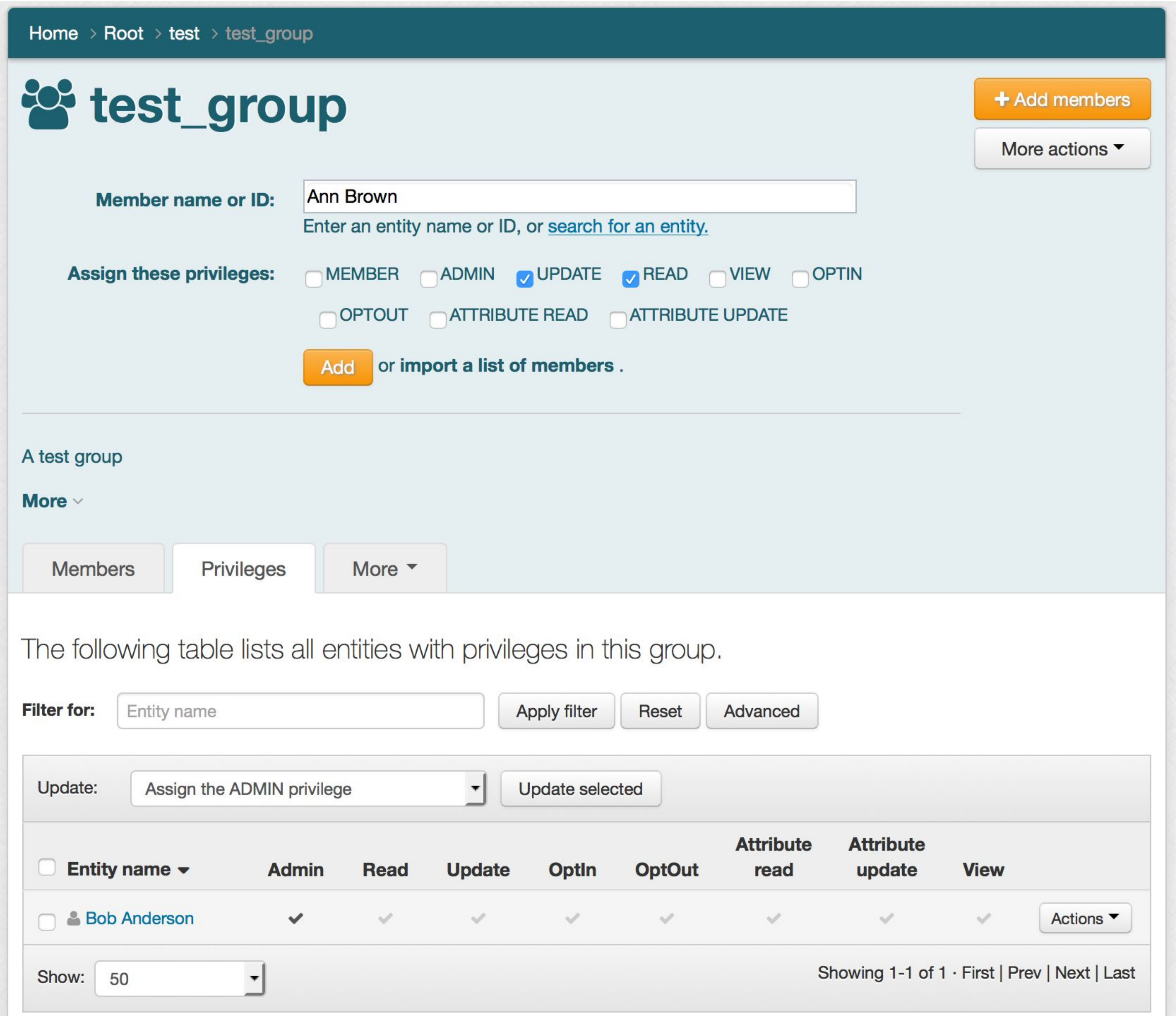
Ann Gasper is a member of the *test_group* group by the following paths:

Ann Gasper is a **direct member** of

- test:test_group

Ann Gasper is a **direct member** of

- affiliations:student system of record
  - which is a **direct member** of
    - affiliations:student system of record and includes
      - which is a **composite factor** minus student excludes of
        - affiliations:student
          - which is a **direct member** of
            - test:test_group



Home > Root > test > test_group

test_group

+ Add members

More actions

Member name or ID: Ann Brown

Enter an entity name or ID, or search for an entity.

Assign these privileges: □ MEMBER □ ADMIN ☑ UPDATE ☑ READ □ VIEW □ OPTIN □ OPTOUT □ ATTRIBUTE READ □ ATTRIBUTE UPDATE

Add or **import a list of members** .

A test group

More

Members | Privileges | More

The following table lists all entities with privileges in this group.

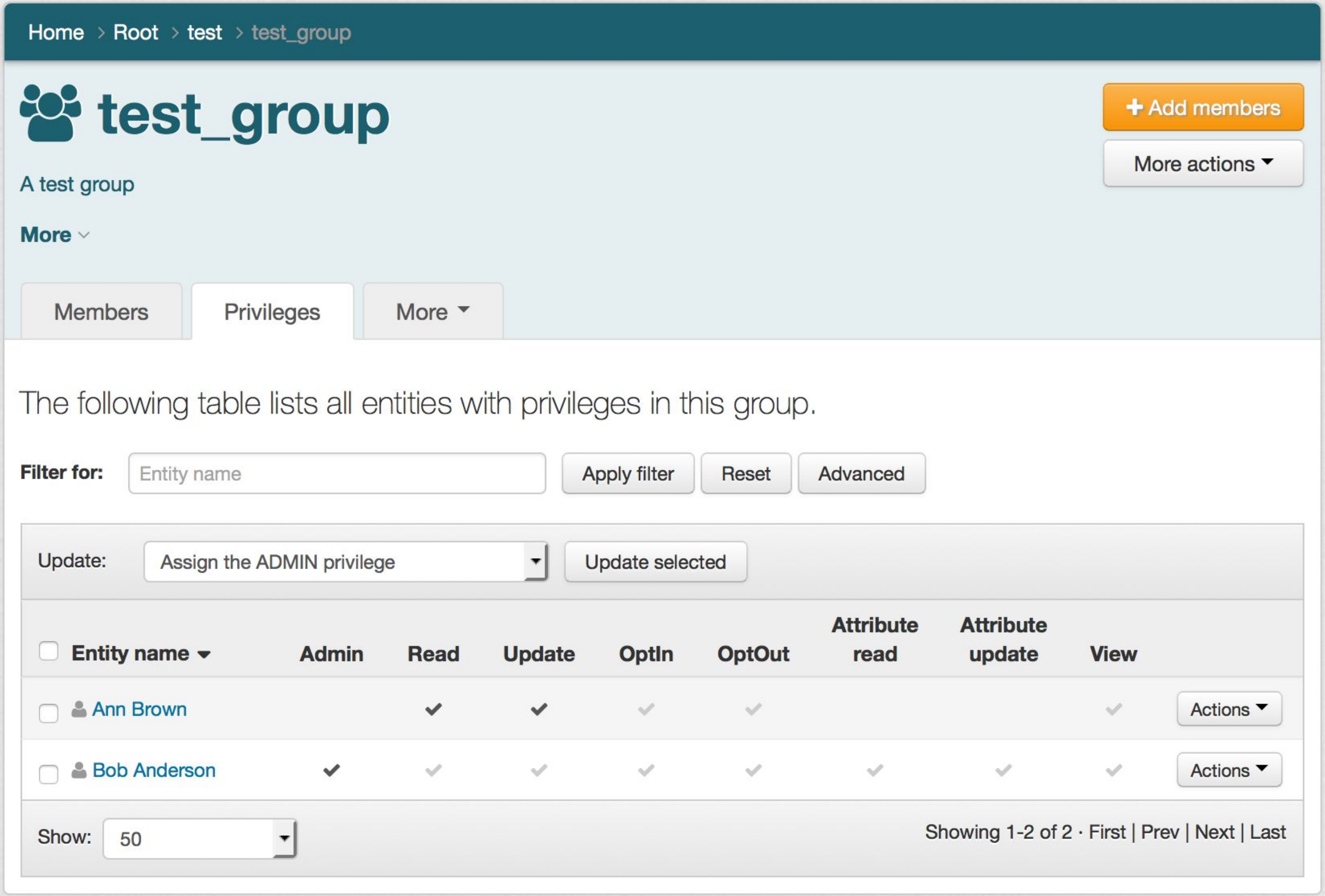
Filter for: Entity name | Apply filter | Reset | Advanced

Update: Assign the ADMIN privilege | Update selected

□ Entity name	Admin	Read	Update	OptIn	OptOut	Attribute read	Attribute update	View	
□ Bob Anderson	✓	✓	✓	✓	✓	✓	✓	✓	Actions

Show: 50

Showing 1-1 of 1 · First | Prev | Next | Last



Home > Root > test > test_group

test_group

+ Add members

More actions ▾

A test group

More ﹀

Members | Privileges | More ▾

The following table lists all entities with privileges in this group.

Filter for: Entity name [Apply filter] [Reset] [Advanced]

Update: Assign the ADMIN privilege ▾ [Update selected]

□	Entity name ▾	Admin	Read	Update	OptIn	OptOut	Attribute read	Attribute update	View	
□	Ann Brown		✓	✓	✓	✓			✓	Actions ▾
□	Bob Anderson	✓	✓	✓	✓	✓	✓	✓	✓	Actions ▾

Show: 50 ▾

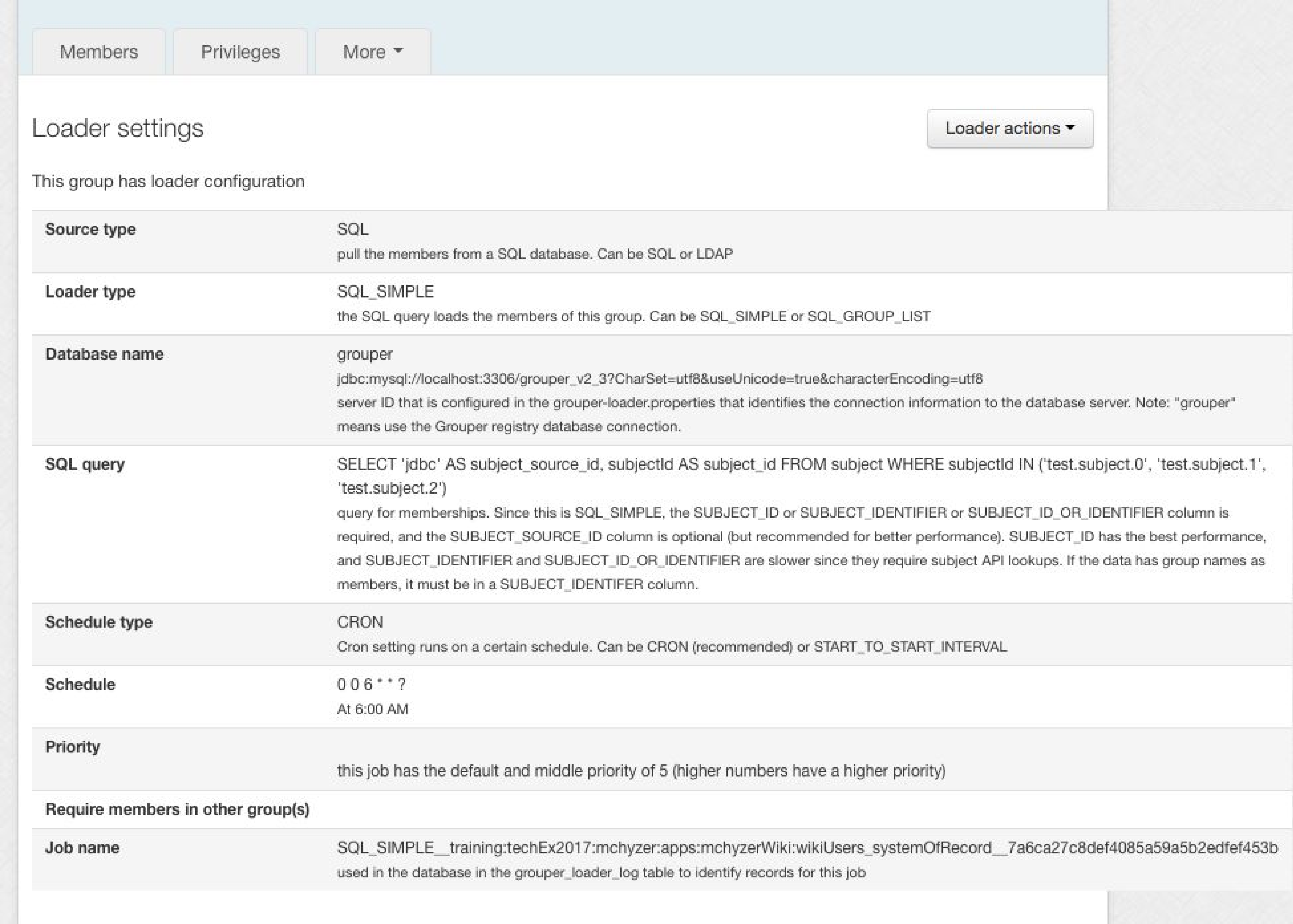
Showing 1-2 of 2 · First | Prev | Next | Last

Go to system of record, make loader

- Go to system of record group
- More tab - > Loader
- Edit
- Copy settings from

  https://spaces.internet2.edu/display/Grouper/Grouper+loader+SQL+simple+example

- Can google “grouper loader SQL simple loader”
- SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2')



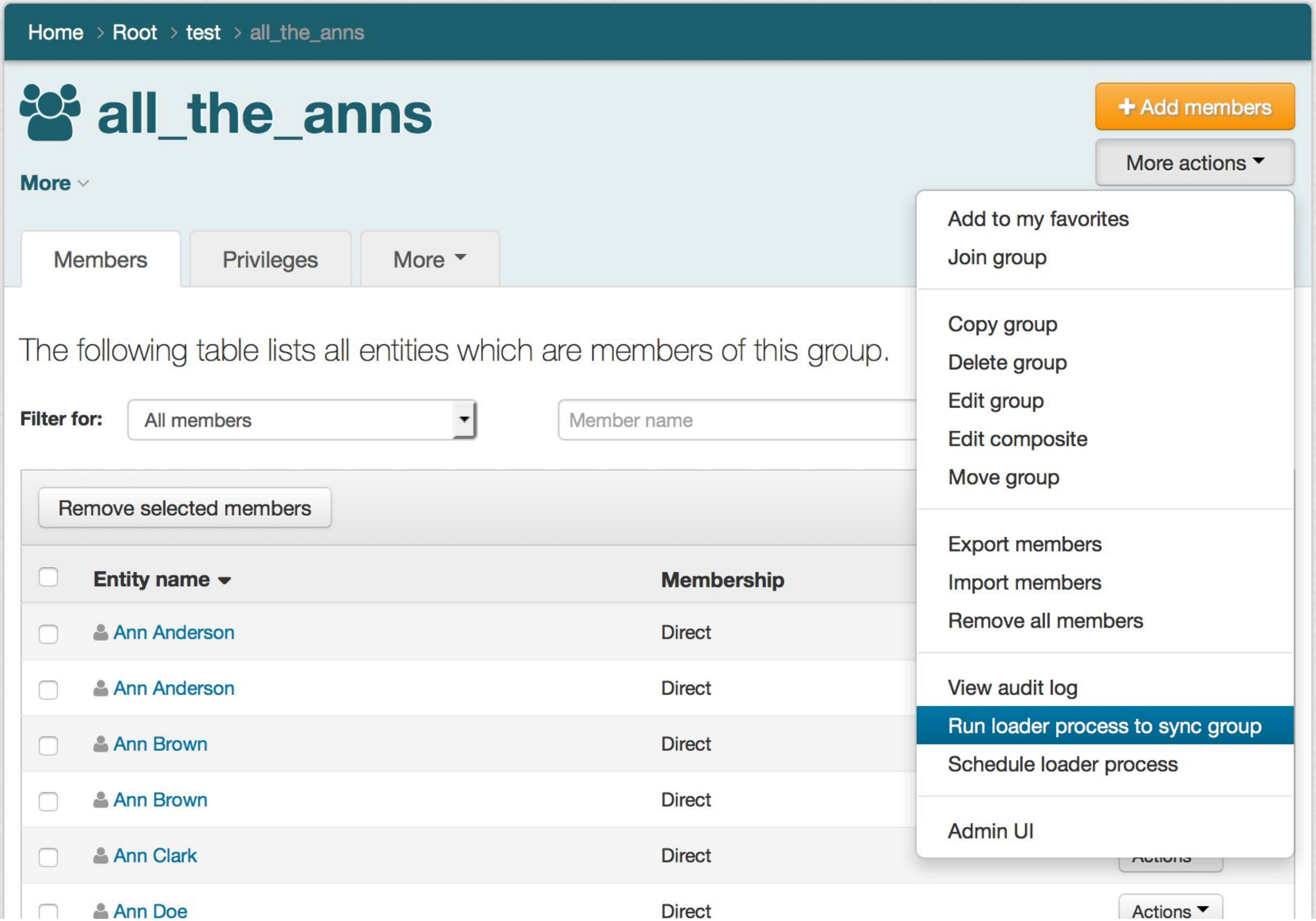
Loader settings

This group has loader configuration

Source type	SQL pull the members from a SQL database. Can be SQL or LDAP
Loader type	SQL_SIMPLE the SQL query loads the members of this group. Can be SQL_SIMPLE or SQL_GROUP_LIST
Database name	grouper jdbc:mysql://localhost:3306/grouper_v2_3?CharSet=utf8&useUnicode=true&characterEncoding=utf8 server ID that is configured in the grouper-loader.properties that identifies the connection information to the database server. Note: "grouper" means use the Grouper registry database connection.
SQL query	SELECT 'jdbc' AS subject_source_id, subjectId AS subject_id FROM subject WHERE subjectId IN ('test.subject.0', 'test.subject.1', 'test.subject.2') query for memberships. Since this is SQL_SIMPLE, the SUBJECT_ID or SUBJECT_IDENTIFIER or SUBJECT_ID_OR_IDENTIFIER column is required, and the SUBJECT_SOURCE_ID column is optional (but recommended for better performance). SUBJECT_ID has the best performance, and SUBJECT_IDENTIFIER and SUBJECT_ID_OR_IDENTIFIER are slower since they require subject API lookups. If the data has group names as members, it must be in a SUBJECT_IDENTIFER column.
Schedule type	CRON Cron setting runs on a certain schedule. Can be CRON (recommended) or START_TO_START_INTERVAL
Schedule	0 0 6 * * ? At 6:00 AM
Priority	this job has the default and middle priority of 5 (higher numbers have a higher priority)
Require members in other group(s)	
Job name	SQL_SIMPLE__training:techEx2017:mchyzer:apps:mchyzerWiki:wikiUsers_systemOfRecord__7a6ca27c8def4085a59a5b2edfef453b used in the database in the grouper_loader_log table to identify records for this job

Run loader features

- Schedule the job
- Run the job
- Run diagnostics
- See members
- See overall members
- Add one of them to the excludes group
- See the overall group



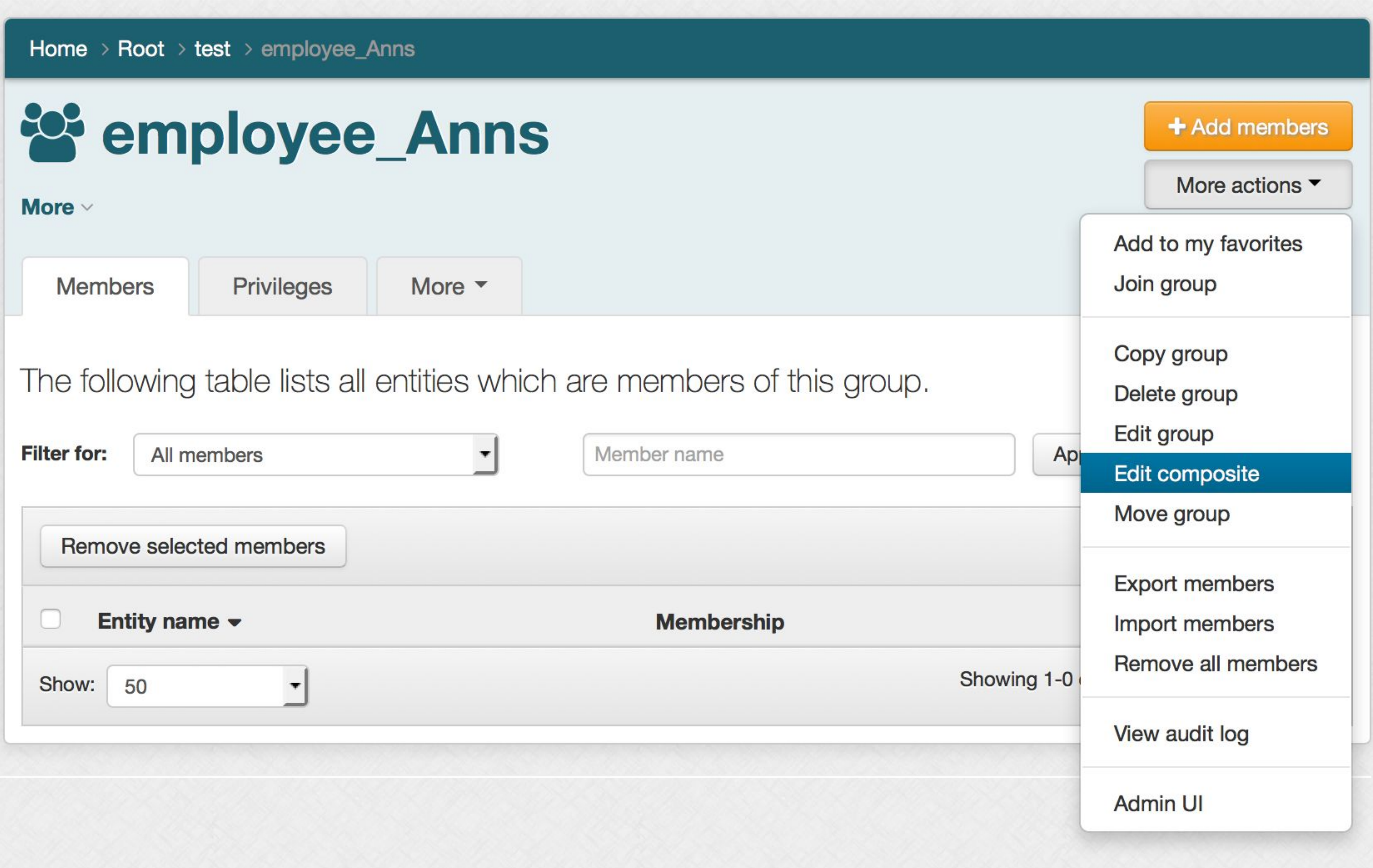
The following table lists all entities which are members of this group.

Filter for: All members ▾ Member name

□	Entity name ▾	Membership	
□	Ann Anderson	Direct	
□	Ann Anderson	Direct	
□	Ann Brown	Direct	
□	Ann Brown	Direct	
□	Ann Clark	Direct	Actions
□	Ann Doe	Direct	Actions ▾

See composite

- Go to some of the groups
- More actions, edit composite
- Dont make changes, but see which groups are composites
- Draw out how the groups are related
- Which takes precedence, includes or excludes
    - I.e. if someone were in both, would they be in the overall?



Home > Root > test > employee_Anns

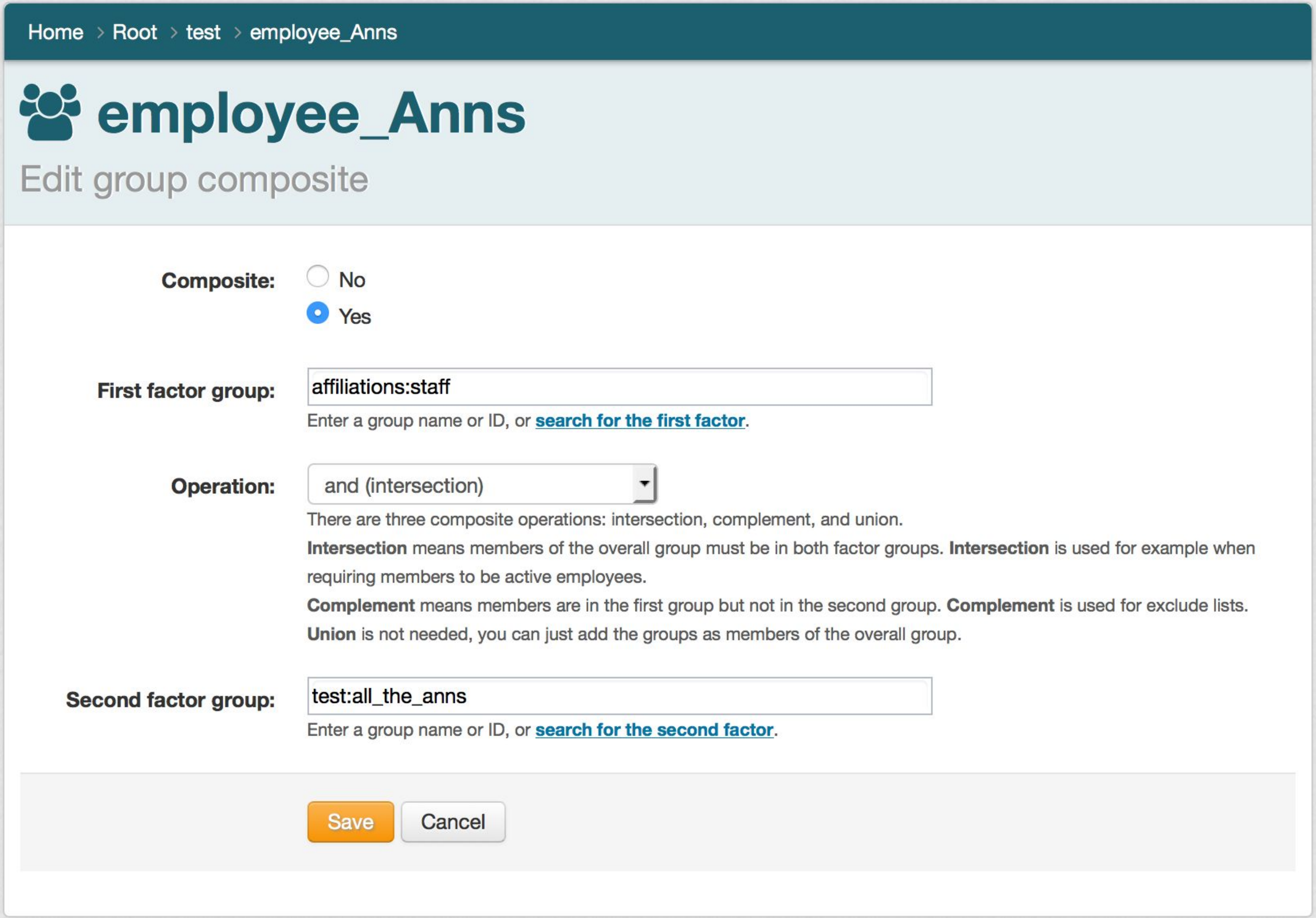
employee_Anns

The following table lists all entities which are members of this group.

Filter for: All members

Show: 50

Showing 1-0



Home > Root > test > employee_Anns

employee_Anns

Edit group composite

Composite: ○ No ● Yes

First factor group: affiliations:staff

Enter a group name or ID, or search for the first factor.

Operation: and (intersection)

There are three composite operations: intersection, complement, and union.

Intersection means members of the overall group must be in both factor groups. **Intersection** is used for example when requiring members to be active employees.

Complement means members are in the first group but not in the second group. **Complement** is used for exclude lists.

Union is not needed, you can just add the groups as members of the overall group.

Second factor group: test:all_the_anns

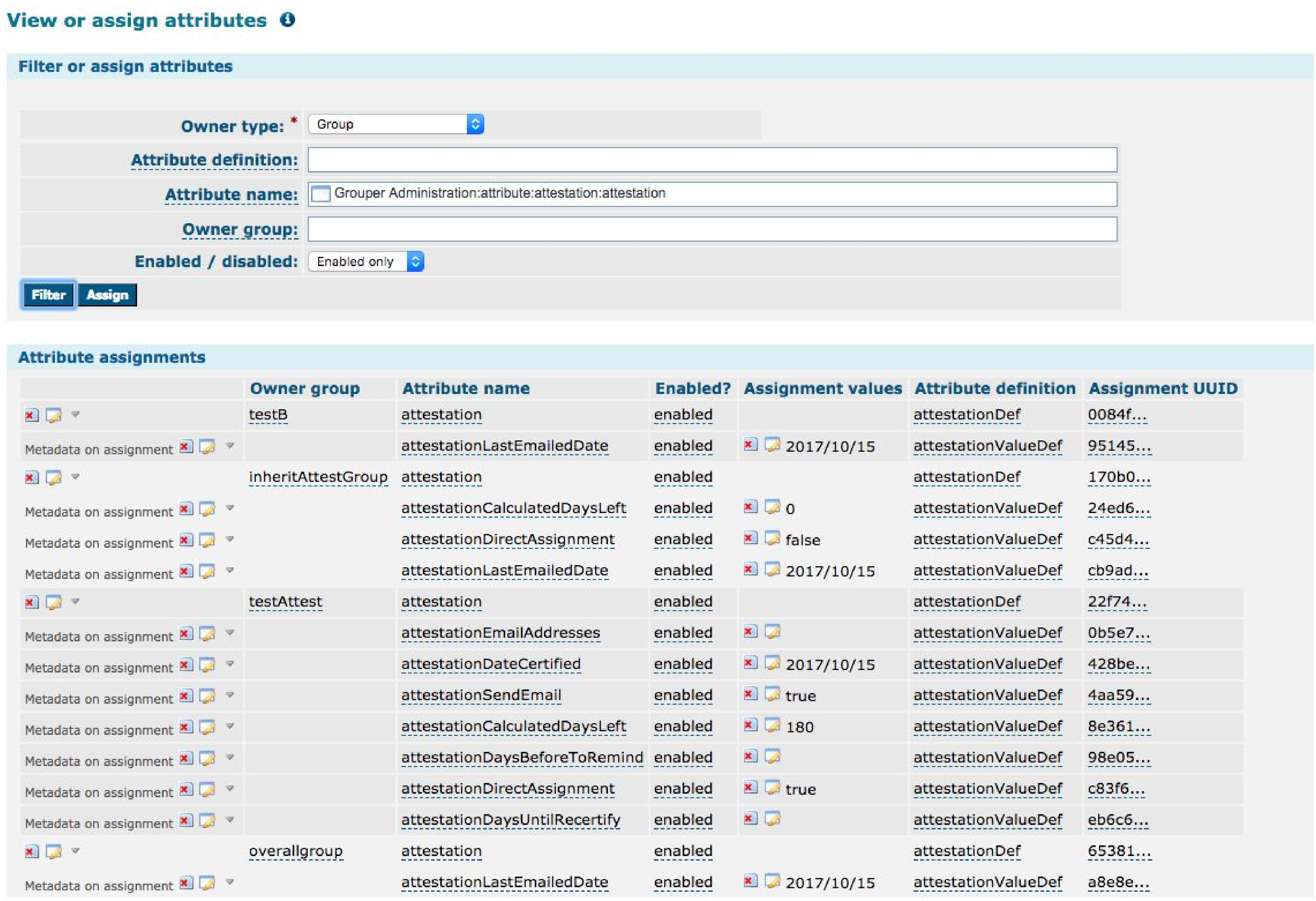
Enter a group name or ID, or search for the second factor.

Make the excludes group attestable

- Go to the excludes group
- More actions -> attestation
- Edit attestation
- Yes, has attestation
- Dont set as attested (or clear it afterwards if you set it)
- Save
- Should say needs attestation
- I can run daemon as admin
- Maybe we will get emails?
  - If subject source and record setup correctly

See more attestation screens

- Global attestation
- Global settings
- Folder attestation
- Folder settings
- Group audit history
- Set an attestation
- See the history again
- Go to Lite UI and see attributes



View or assign attributes

Filter or assign attributes

Owner type: *	Group
Attribute definition:	
Attribute name:	Grouper Administration:attribute:attestation:attestation
Owner group:	
Enabled / disabled:	Enabled only

Attribute assignments

	Owner group	Attribute name	Enabled?	Assignment values	Attribute definition	Assignment UUID
☒ ✎ ▾	testB	attestation	enabled		attestationDef	0084f...
Metadata on assignment ☒ ✎ ▾		attestationLastEmailedDate	enabled	☒ ✎ 2017/10/15	attestationValueDef	95145...
☒ ✎ ▾	inheritAttestGroup	attestation	enabled		attestationDef	170b0...
Metadata on assignment ☒ ✎ ▾		attestationCalculatedDaysLeft	enabled	☒ ✎ 0	attestationValueDef	24ed6...
Metadata on assignment ☒ ✎ ▾		attestationDirectAssignment	enabled	☒ ✎ false	attestationValueDef	c45d4...
Metadata on assignment ☒ ✎ ▾		attestationLastEmailedDate	enabled	☒ ✎ 2017/10/15	attestationValueDef	cb9ad...
☒ ✎ ▾	testAttest	attestation	enabled		attestationDef	22f74...
Metadata on assignment ☒ ✎ ▾		attestationEmailAddresses	enabled	☒ ✎	attestationValueDef	0b5e7...
Metadata on assignment ☒ ✎ ▾		attestationDateCertified	enabled	☒ ✎ 2017/10/15	attestationValueDef	428be...
Metadata on assignment ☒ ✎ ▾		attestationSendEmail	enabled	☒ ✎ true	attestationValueDef	4aa59...
Metadata on assignment ☒ ✎ ▾		attestationCalculatedDaysLeft	enabled	☒ ✎ 180	attestationValueDef	8e361...
Metadata on assignment ☒ ✎ ▾		attestationDaysBeforeToRemind	enabled	☒ ✎	attestationValueDef	98e05...
Metadata on assignment ☒ ✎ ▾		attestationDirectAssignment	enabled	☒ ✎ true	attestationValueDef	c83f6...
Metadata on assignment ☒ ✎ ▾		attestationDaysUntilRecertify	enabled	☒ ✎	attestationValueDef	eb6c6...
☒ ✎ ▾	overallgroup	attestation	enabled		attestationDef	65381...
Metadata on assignment ☒ ✎ ▾		attestationLastEmailedDate	enabled	☒ ✎ 2017/10/15	attestationValueDef	a8e8e...

Thanks!

Further information:

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

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