

DSPACE

The DSpace Course

Module – User management and authentication options

- By the end of this module you will:
 - Understand the concepts of authentication and authorization
 - Fully understand user and group management in DSpace
 - Have added and removed users from groups
 - Have a high level understanding of some advance authentication options

- Two important concepts:
 - Authentication (AuthN)
 - The process of establishing the identity of a user
 - Authorization (AuthZ)
 - The granting of privileges to a user to perform an action on a resource



- User creation
 - Covered in module 'An introduction to users and groups'
- User management
 - Modify users
 - Administer menu -> E-People -> Select E-person -> Edit
 - Delete users
 - Administer menu -> E-People -> Select E-person -> Delete...

Administer EPeople

Choose an action:

[Help...](#)

Add EPerson...

OR

Stuart Lewis (stuart.lewis@aber.ac.uk)

Select E-person...

then

- Referential integrity
 - Database theory of relational databases
 - Data cannot be deleted if it referred to elsewhere
 - So...
 - Users cannot be deleted if they own anything
 - Submitted items
 - Items in a workflow
 - Items part way through submission
 - This maintains the integrity of the data

- Group management
 - Administer menu -> Groups
 - Create new groups 'Create New Group' button
 - 'Edit' or 'Delete' groups
 - Users or groups can be members of groups

Group Editor

[Help...](#)

Note that you do not need to manually add users to the "anonymous" group - all users are members implicitly.

Warning - if you try to delete a group that is referred to by an authorization policy or is a workflow group you will get an internal server error.

Create New Group

ID	Name		
1	Administrator	Edit	Delete
0	Anonymous	Edit	Delete

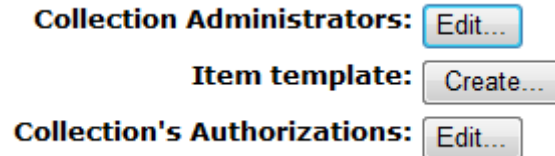
- Edit an item's authorizations
 - Edit an item

**Item's
Authorizations:**

Edit

- Assign policies to:
 - The item
 - It's bundles
 - It's files
- Policies assigned to groups not users
 - ANONYMOUS group for anonymous access

- Edit a collection's authorizations
 - Edit a collection



- Collection administrators can act as administrators for a collection (edit items)
- Assign policies to the collection:
 - READ / WRITE / ADD / REMOVE
 - DEFAULT_ITEM_READ / DEFAULT_BITSTREAM_READ
 - COLLECTION_ADMIN

- Create a new user
 - [dSPACE]/bin/create-administrator
- Log in to ensure they are an administrator
- Remove them from the Administrator group
- Log back in to ensure the user is not an administrator anymore

- LDAP
 - Lightweight Directory Access Protocol
 - Most institutions run an LDAP system to provide a central user password system
 - Active Directory has an LDAP interface
 - Users can be created using LDAP queries
 - Passwords not stored in DSpace

- Shibboleth
 - A devolved authentication system
 - Allows users to log in to systems outside their institution
 - A user's local institution performs the authentication

- IP authentication
 - IP address of user (no login required)
 - If the IP address matches (e.g. is ‘on campus’) then the user becomes a member of a special group (e.g. ‘Internal-users’).
 - That group can be assigned privileges
 - Can be used to protect internal resources, and fallback to a requiring a login
 - Stackable authentication

- These slides have been produced by:
 - Stuart Lewis & Chris Yates
 - Repository Support Project
 - <http://www.rsp.ac.uk/>
 - Part of the RepositoryNet
 - Funded by JISC
 - <http://www.jisc.ac.uk/>

