UO Libraries

DSpace User & Group Permissions

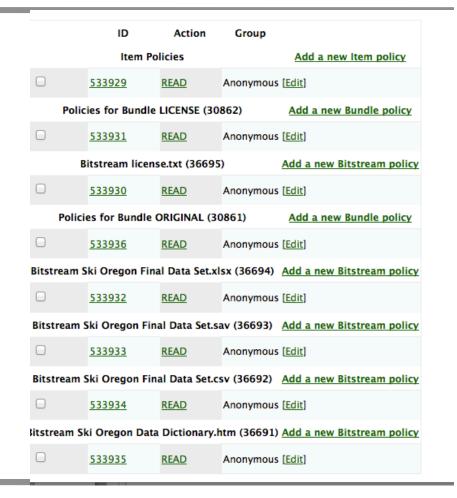
UO NSRC Workshop March 29, 2013

Karen Estlund Head, Digital Scholarship Center



Authorizations

- DSpace
- Community
- Collection
- Item
- Bundle
 - Group of Related Files
- Bitstream / File
 - Document / File
 - Metadata
 - Copyright License, etc.





Registered Users

- S'enregistrer
- A registered user has no permissions on the system until a DSpace administrator assigns permissions.
- Registered users can sign up for RSS notifications for particular collections

Mon compte

- Connecter
- S'enregistrer



Groups

Use Groups for all of the people (E-personne)

Recherche résultats

ID	Nom	Membres	Regroupement / Catégorie de contenu
1	Administrator	7	
0	Anonymous	-	
3	<u>Archivistes</u>	2	
2	COLLECTION_1_ADMIN	2	Cartes Postales [Voir]
7	COLLECTION_2_ADMIN	2	Dossiers Esclavage et Capti [Voir]
6	participants atelier	11	
4	University of Oregon	4	



Automatic Groups

Administrators

- Can create new communities and collections
- Create new users / groups
- Assign rights
- Run Reports and Curation activities

Anonymous

- Anyone on the website that is not logged into Dspace
- Do not add people to this group.



Creating Groups

- Use Groups to manage people working on your system (organization / role)
 - UCAD
 - Archivists
 - Researchers
- Then when assigning rights to a collection or item, assign the Group rather than individuals, best practice



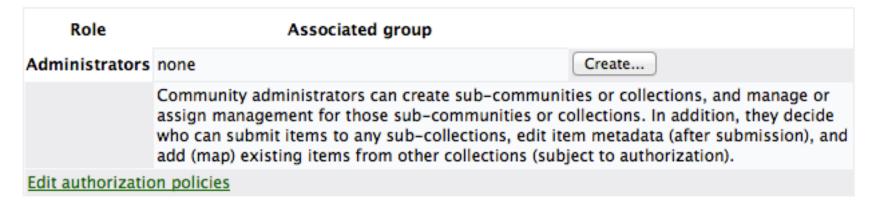
SUBMISSION / EDITING AUTHORIZATIONS



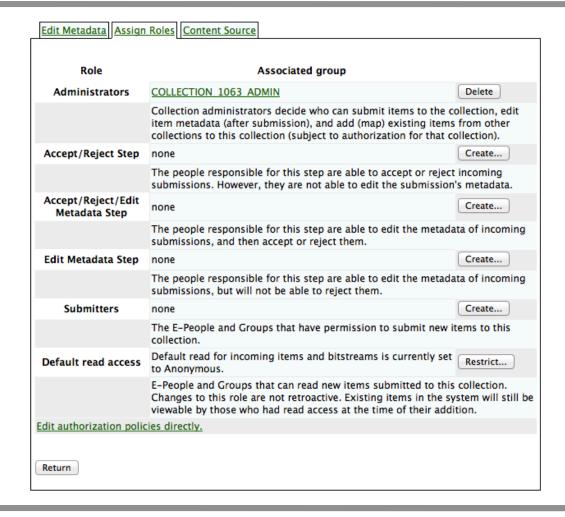
Community Authorizations

Edit Community: Data

- Edit Metadata
- Assign Roles



Collection Authorizations





Collection Authorizations Best Practices

- Administrators
 - Add System Administrators as Administrators, or
 - Make sure someone at institution always has administrative access
- Use "Accept/Reject/Edit Metadata Step"
 - Don't use "Accept/Reject Step" and "Edit Metadata Step"



RESTRICTING ACCESS



Restrict by Collection

Edit Collection: Official University Records - Lariviere



Default read access

Default read for incoming items and bitstreams is currently set to Anonymous.

Restrict...

E-People and Groups that can read new items submitted to this collection.

Changes to this role are not retroactive. Existing items in the system will still be viewable by those who had read access at the time of their addition.

Restricting an Individual Item

- Add a new policy to restrict an item
- Make sure to delete the policy allowing "Anonymous" the ability to READ



