

# E-People, Groups, and Authorizations

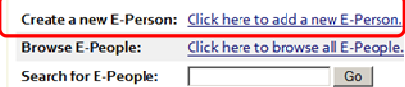
## E-People



DSpace identifies application user accounts as E-People. To create, edit or view E-People accounts, navigate to Access Control located under the Administrative toolbar. Click on the link labeled **People**.

## E-person management

### Actions



From this screen, you can create, browse or search for user accounts. Clicking on the link **Create a new E-Person** will display a blank entry form.

## Create a new user

A screenshot of the 'New E-Person's information' form. The form is titled 'New E-Person's information:' and contains several fields: 'Email Address:', 'First Name:', 'Last Name:', 'Contact Telephone:', 'Can Log In:', and 'Require Certificate:'. Each field has a corresponding input box. At the bottom of the form, there are two buttons: 'Create E-Person' and 'Cancel'.

The system stores the following information about users:

- ❖ Email address
- ❖ First and Last names
- ❖ Telephone number
- ❖ If they can log into the system through the Web User Interface
- ❖ If the user requires an X509 certificate to login.

Fill in the appropriate information and click on the button labeled **Create E-Person**

## E-person management

Clicking on “Browse E-People” will provide you with a list of all E-People accounts.

### Actions

Create a new E-Person: [Click here to add a new E-Person.](#)  
Browse E-People: [Click here to browse all E-People.](#)  
Search for E-People:

## E-person management

### Actions


Create a new E-Person: [Click here to add a new E-Person.](#)  
Browse E-People: [Click here to browse all E-People.](#)  
Search for E-People:

You can also search for E-People by their full name, part of the name, e-mail address, or part of their e-mail address.

To delete, click the box next to the user account you want to delete, scroll to the end of the page and click “Delete E-People”

|                                     |    |                            |                            |
|-------------------------------------|----|----------------------------|----------------------------|
| <input type="checkbox"/>            | 9  | <a href="#">[redacted]</a> | <a href="#">[redacted]</a> |
| <input checked="" type="checkbox"/> | 75 | <a href="#">[redacted]</a> | <a href="#">[redacted]</a> |

Now showing items 1-15 of 71 [Next Page](#)

 This is the website for the Digital Resource Commons, an OhioLINK project. The DRC serves as a repository for the digital intellectual content of academic institutions in Ohio.  
[Contact Us](#) | [Send Feedback](#)



Hint: You cannot delete an E-Person account if they have submitted items.

## ***Groups***

Instead of assigning authorizations on the individual level, groups of users are created with specific authorizations to manage collections. Using groups in conjunction with the “Assign Roles” tab located under the sub menu “Edit Communities” available under “Communities and Collections,” makes managing the granting of privileges more efficient.

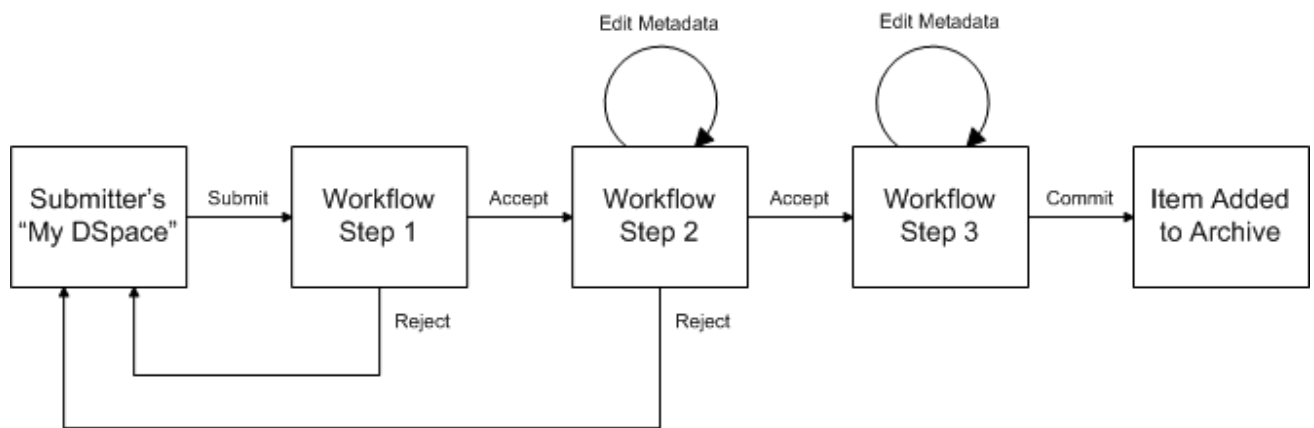
Groups created while assigning roles:

| <b>Role</b>                      | <b>Associated Group</b>    | <b>Description</b>   |
|----------------------------------|----------------------------|--|
| Administrator                    | Collection_Admin           | Collection Administrators decide who can submit items to the collection, withdraw items, edit item metadata (after submission), and add (map) existing items from other collections to this collection (subject to authorization for that collection). |
| Accept/Reject Step               | Collection_Workflow_Step 1 | The people responsible for this step are able to accept or reject incoming submissions. However, they are not able to edit the submission’s metadata.  |
| Accept/Reject/Edit Metadata Step | Collection_Workflow_Step 2 | The people responsible for this step are able to edit the metadata of incoming submissions, and then accept or reject them.  |
| Edit Metadata Step               | Collection_Workflow_Step 3 | The people responsible for this step are able to edit the metadata of incoming submissions, but will not be able to reject them.   |

|                     |                         |   |
|---------------------|-------------------------|---|
| Submitters          | Collection_Submit       | The E-People and Groups that have permission to submit new items to their collection. |
| Default read access | Collection_Default_Read | Default read for incoming items and bitstreams  |



A collection's workflow can have up to three steps. (see above table) Each collection may have an associated E-Person group for performing each step; if no group is associated with a certain step, that step is skipped. If a collection has no E-Person groups associated with any step, submissions to that collection are loaded straight into the main collection.



**Submission Workflow in DSpace**

The alternative method of assigning authorizations is to create a custom group. To create a group, click on "Groups" from the left navigation bar.

## Group Editor: new group

Change group name:

Search members to add:  [E-People...](#) [Groups...](#)

Select a new name for the group, and search for the members, or E-People, you want to assign to the group. Checking the members you want to add will change their status to pending. Clicking Save will add the members to the group.

## Group Editor: ud rice test group (id: 187)

Change group name:

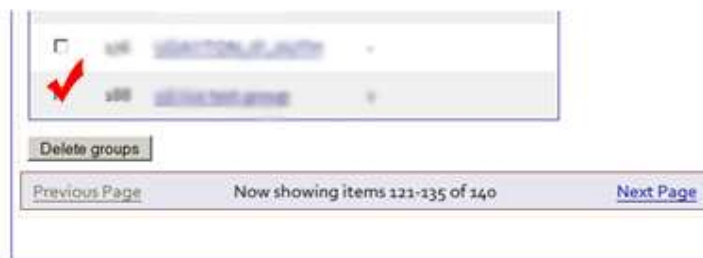
Search members to add:  [E-People...](#) [Groups...](#)

The group editor allows you to add or remove members from the group.

### Members

| ID | Name                      | Email  |                                       |
|----|---------------------------|--|---------------------------------------|
| 35 | <a href="#">Fran Rice</a> | <a href="mailto:rice@udayton.edu">rice@udayton.edu</a> | <input type="button" value="Remove"/> |

To delete, click the box next to the group account you want to delete, scroll to the end of the page and click "Delete groups"



The screenshot shows a list of groups with checkboxes. A red checkmark is placed next to the checkbox for the group with ID 187. Below the list is a "Delete groups" button. At the bottom of the list, there are navigation links: "Previous Page", "Now showing items 121-135 of 140", and "Next Page".

## Authorizations

### Administer Authorization Policies

#### Item authorizations

Look up an item:

Advanced authorizations tool: [Click here to go to the item wildcard policy admin tool](#)

#### Community/collection authorizations

Click on a community or collection to edit its policies.

- [Anthropology](#)
  - [Anthropology 142](#)
- [Antioch College](#)
  - [First Test Collection](#)
- [Art & Architecture](#)

When you click on "Authorizations" from the left toolbar, you are presented with a list of all the collections.

Selecting one collection will allow you to associate policies with that collection.

### Policies for Collection "UD test collection" (123456789/2176, ID: 173)

[Click here to add a new policy.](#)

| ID   | Action                           | Group                                 |
|--|----------------------------------|---------------------------------------|
| <input type="checkbox"/> <a href="#">58948</a> | <a href="#">ADD</a>              | COLLECTION_173_SUBMIT [Edit]          |
| <input type="checkbox"/> <a href="#">58947</a> | <a href="#">ADD</a>              | COLLECTION_173_WORKFLOW_STEP_2 [Edit] |
| <input type="checkbox"/> <a href="#">58946</a> | <a href="#">ADD</a>              | COLLECTION_173_WORKFLOW_STEP_1 [Edit] |
| <input type="checkbox"/> <a href="#">58945</a> | <a href="#">COLLECTION_ADMIN</a> | COLLECTION_173_ADMIN [Edit]           |

Here is an example of the policies associated with a test collection. By clicking on "Click here to add a new policy" you are able to add additional policies. See table below for policy options.

| Authorization | Description                                      |
|---------------|--|
| Read          | Can view item (item metadata is always viewable) |
| Write         | Can modify item                                  |
| Add           | Add items  |
| Remove        | Remove items                                     |

|                         |  |
|-------------------------|--|
| Default_Bit_Stream_Read | By default bitstream can be viewed by all submitters   |
| Default_Item_Read       | By default item can be viewed by all submitters  |
| Collection_Admin        | Collection Administrators decide who can submit items to the collection, withdraw items, edit item metadata (after submission), and add (map) existing items from other collections to this collection (subject to authorization for that collection). |

The Advanced Policy Manager allows you to assign the following authorizations on either the item level or bitstream level

**Search DRC**

[Advanced Search](#)

---

**Browse**

- ◆ All of DRC
  - ◊ [Communities & Collections](#)
  - ◊ [By Issue Date](#)
  - ◊ [Authors](#)
  - ◊ [Titles](#)
  - ◊ [Subjects](#)

---

**My Account**

- ◆ [Logout](#)
- ◆ [Profile](#)
- ◆ [Submissions](#)

---

**Administrative**

- ◆ Access Control
  - ◊ [People](#)

## Administer Authorization Policies

### Item authorizations

Look up an item:

Advanced authorizations tool: [Click here to go to the item wildcard policy admin tool](#)

### Community/collection authorizations

Click on a community or collection to edit its policies.

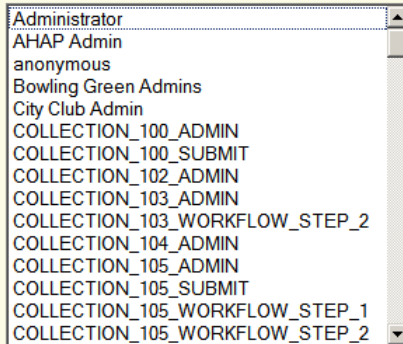
- ◆ [Anthropology](#)
  - ◊ [Anthropology 142](#)
- ◆ [Antioch College](#)
  - ◊ [First Test Collection](#)
- ◆ [Art & Architecture](#)
  - ◊ [Akron Art Museum](#)
  - ◊ [The ART Collection](#)
- ◆ [Art History](#)
  - ◊ [Art History 101](#)

# Advanced Policy Manager

Allows wildcard additions to and clearing of policies for types of content within specific collection(s). WARNING - removing READ permissions from items will make them not viewable!

For all of the selected groups...


Group:



Select a Group from the drop-down

...grant the ability to perform the following action...

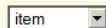
Action:



Select an "Action", refer to table below

...for all following object types...

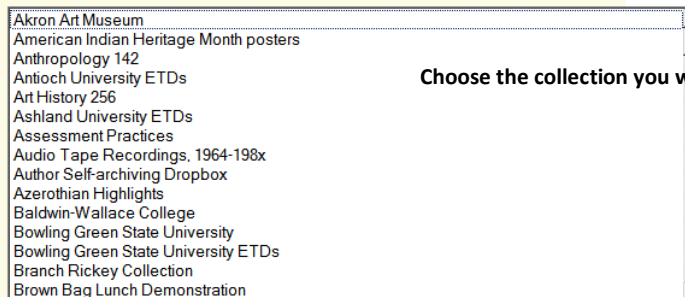
Content Type:



Choose either "item" or "bitstream"

...across the following collections.

Collection:



Choose the collection you want to associate with the policy

Clicking on the “**Action**” drop-down allows you to assign the following policies or rights

| Authorization          | Description  |
|------------------------|--|
| Read                   | Can view item (item metadata is always viewable)   |
| Write                  | Can modify item  |
| Obsolete(Delete)       | Delete items. * need OBSOLETE permission for all collections that contain item.  |
| Add                    | Add items  |
| Remove                 | Remove items   |
| Workflow_Step_1        | Accept or reject incoming submissions, no edits to metadata.   |
| Workflow_Step_2        | Edit the metadata of incoming submissions, and accept or reject them.  |
| Workflow_Step_3        | Edit the metadata of incoming submissions, but not be able to reject them.   |
| Workflow_Abort         | Able to stop the submission workflow   |
| Default_Bitstream_Read | By default, the bitstream can be read by all   |
| Default_Item_Read      | By default, the item can be viewed by all  |
| Collection_Admin       | Collection Administrators decide who can submit items to the collection, withdraw items, edit item metadata (after submission), and add (map) existing items from other collections to this collection (subject to authorization for that collection). |