Site Administrator Help

Help Contents

Close this window

- General Information
- Creating a Top-level Community
- Creating a Sub-community
- Editing a Community
- Creating a Collection
- Editing a Collection
- E-people
- Groups
- Items
- Supervision Orders
- Dublin Core Registry
- Bitstream Format Registry
- Workflow
- Authorization
- Edit News
- Edit Default License

General Information

As of DSpace 1.2, many administration tools can now be accessed via the regular DSpace UI. However, they only appear if you are logged in as an administrator. The easiest way to do this is to go to your 'My DSpace' page.

Some tasks must be performed entrally using the administration user interface, part of the Web UI. To access the administration UI, enter the base URL of your DSpace followed by `/dspace-admin`, for example:

`https://dspace.myu.edu/dspace-admin`

You will need to authenticate as an administrator to be able to access the page. Then, click on the relevant tool on the left-hand navigation bar.

Creating a Top-level Community

To add a top-level community, go to the community/collection listing page while logged in as an administrator. On the right there will be an option to *Create Top-Level Community...*. Clicking on this will create the new top level community and take you to the 'Edit Community' page.

Creating a Sub-community

To create a sub-community, go to the community home page of the community that is to be the parent of the new sub-community. Then, click on the 'Create sub-community' in the 'Admin Tools' box at the top right-hand corner of the page. This will create the new community and take you to the 'Edit Community' page for that community.

Editing a Community

- Fill out the form as needed. 'Name', 'short description' and 'Introductory text' are required; the rest of the fields are optional.
- The 'short description' appears on the community list page below the community name, and should be one or two sentences of plain text describing the community.
- The 'introductory text,' 'side bar' and 'copyright text' fields are displayed on the community's home page. 'Introductory text' and 'side bar text' are both HTML fields, which means you should place text in <P> </P>
- To add a logo to be displayed on the community's home page, click on the **Upload Logo** button. On the next screen either type in a path to the logo file or browse to the logo file, then click on the **Upload** button. Note, if you're creating a community, it's best to fill out the rest of the form, click 'Update' and then come back to do this. Note that in general, relatively small logo sizes look best due to the design of the collection home page.
- When all information for the Community Page is entered, click on the **Create** button.

Creating a Collection

Creating a collection is done with a 'wizard' style tool that should be familiar to most people who've used modern operating systems user interfaces. It's rather similar to the submission interface in DSpace.

Note: You cannot add new e-people records with this wizard. All the e-person records must be loaded into the system first. However, you will be able to add more e-people and/or groups to each group associated with the collection later if required.

To create a collection, ensure you're logged in, go to the community home page for the community in which the collection is to appear, and click 'Create Collection' on the top-right hand corner of the page. This will start the wizard.

Describe the Collection (Checkboxes)

The first page of the wizard will ask you some questions about the new collection. Check those that apply and click on the 'Next >'

button. Note that after you've completed the wizard, you will be able to edit the collection later, so decisions you make here are not permanent.

However, also note that this wizard is a little less polished than the submission UI, which basically means there are no 'back' buttons, so if you want to change something you entered on one page after clicking 'next', you need to finish the wizard and then go back and edit the collection.

When you have completed the wizard, you're dropped into the Edit Collection screen. This allows you to review what you've entered and make any necessary tweaks.

Note 1: If the **New items should be publicly readable** option is checked, it means that new items arriving via the submission UI or batch importer will, by default, will get anonymous READ permissions for both the item and all the bitstreams). You can change this later so that e.g. items get anonymous READ permissions but bitstreams do not. Items that are 'mapped' or included from other collections will not have their authorizations changed.

Note 2: **New items should be publicly readable** is just a default; an item's permissions may later changed.

Note 3: If **New items should be publicly readable** is *not* checked, you will be asked later in the wizard who is allowed to read new items. Again, this is just a default, and can be changed later.

Describe the Collection (Information)

The next page allows you to fill in some basic information about the collection. The **Name**, **Short Description** and **Introductory Text** fields are mandatory, the others are not. (Note that the wizard is not strict, however, and will not enforce this.)

Copyright Text is simply text that will appear at the bottom of the collection's home page.

License is the *deposit license* (the license that submitters must grant when they submit an item) for this collection. This overrides the site default (which is stored in *[dspace]*/config/default.license and must be edited by a systems adminstrator). If you leave this field blank, the site default license is used.

Provenance is a free-text field you can put any provenance information in you feel like. It is not visible to end-users.

Collection Authorization

Depending on the boxes you checked on the first page of the wizard, you will go through a number of screens asking you which e-people and/or groups can or should perform which actions, for example who can submit, and who should perform the *accept/reject* submission workflow step. These pages work exactly the same as the group editor. Click 'Next >' when you have selected all the e-people and/or groups to appear in the relevant permissions group.

Note: You cannot add new e-people records with this wizard. All the e-person records must be loaded into the system first. You can add more e-people and/or groups to each group later if required.

Enter Default Item Metadata

On this screen you can specify some Dublin Core values that new submissions will have pre-filled out. Some of the values you can set here do not appear in the submission UI, so end-users may not have the chance to edit them. This can be a good or a bad thing! (FIXME?) Also note that these Dublin Core values will be added to items imported via the batch importer.

Editing a Collection

The Edit Collection page allows you to change collection metadata (such as name and introductory text), configure authorization and workflow, or delete the collection entirely.

The 'Delete' button (located at the top of the page) will remove the collection (including all its items) from the repository.

The **Name**, **Short Description** and **Introductory Text** fields are mandatory, the others are not. Note that this is not enforced, but is highly recommended.

Copyright Text is simply text that will appear at the bottom of the collection's home page.

License is the *deposit license* (the license that submitters must grant when they submit an item) for this collection. This overrides the site default (which is stored in *[dspace]*/config/default.license and must be edited by a systems adminstrator). If you leave this field blank, the site default license is used. There are some substitution variables that can be used to create personalized licenses:

- **%1$s** will be translated in the "submitter first name"
- **%2$s** will be translated in the "submitter last name"
- **%3$s** will be translated in the "submitter email"
- **%4$s** will be translated in the current date
- **%5$s** will be translated in the collection info
- **%6$s** will be translated in the item info
- **%7$s** will be translated in the eperson info

If you need to embed in the license text the % symbol you need to escape it with a second %, i.e. you need to write %%. It is recommended to use a dummy submission to check the license change: **check the resulting license in the Accept/reject Licence step.**

Provenance is a free-text field you can put any provenance information in you feel like. It is not visible to end-users.

To add or change the logo to be displayed on the collection's home page, click on the Upload Logo button. On the next screen either type in a path to the logo file or browse to the logo file, then click on the Upload button.

To add or change authorisations, submitters or collection administrators click on the appropriate buttons to create/edit groups and their actions.

To edit the workflow groups, select the workflow step whose group you want to create or change and follow the group edit process

Click on the 'Item Template' button to display the default item metadata page where you can set default values for metadata fields for all items added to the collection.

E-people

Use this tool to register e-mail addresses and other information about people you wish to authorize to play a role in the system, either as submitters, administrators, submission workflow participants, subscribers, or users with permissions to read restricted content.

Users can also get onto this list by self-registering (if the site configuration allows this). This does not give them any authorization, however. All people you wish to add to a group for submitter or workflow authorization must first be registered here.

Register an E-Person

To register someone, click on the **Add EPerson** button and add their information.

- If the user will be logging in with a password, *do not* check **Can Log In** as this informs the system the user has a registered, active account, which isn't the case for a new e-person--they'll need to register using the UI to set a password first.
- The 'require certificate' checkbox is used by MIT's X509 certificate authenticator. Ignore this unless you are using the `MITAuthenticator` authenticator.

If you check 'require certificate', you may also check 'can log in'. This means the user can log straight in with their certificate without registering. If you want users to go through the registration process (so that they enter their name etc.) then do not check 'can log in'.

Click on **Save Edits** when done.

Delete an E-Person or Edit Information About an E-Person

Click on the **Select EPeople...** button to get a pop-up list of e-people in the system. The links at the top and bottom of the pop-up let you page through the list. You can also sort the list by e-mail address, last name or ID by clicking on the relevant column heading. On the left of each e-person in the list is a 'select' button. Click this next to the relevant e-person, and the pop-up will close and the e-person will appear in the box on the main 'Adminster EPeople' page. Now you can click the 'edit' or 'delete' buttons which let you edit information about a user or to delete them from the system.

Groups

Use this section to create, edit and delete groups of e-persons and/or groups who can be authorized for specific functions in the system.

The 'Anonymous' group is a 'special' group that represents every person using the system. This group exists so that authorization policies can be specified for anonymous access ('everyone in the world can read this item').

Members of the 'Administrator' group are allowed to perform any action in the system, so be careful who you put in this group!

Other groups can be used for a variety of purposes. Groups may represent e-people who are allowed to submit to a particular collection; e-people who are responsible for performing a particular workflow step such as reviewing incoming submissions; or groups of e-people who have permission to access some restricted content. Information about what each group is allowed to do is controlled using the authorization section.

Groups may contain other groups to provide greater flexibility in assigning actions and to simplify maintenance. This is useful for reflecting hierarchical group structures, where a group of e-people with particular responsibilties are also part of a larger group with differing reponsibilities and/or scope of responsibility.

Groups can have names. Names automatically created by the system follow a convention depending on the what the group is for. The general form of this is:

`OBJECTTYPE_OBJECTID_ACTION`

For example, the group of e-people who are authorized to submit to collection XYZ would be called:

`COLLECTION_XYZ_ADD`

Note that XYZ in this case is the *internal* ID (the database primary key) of the collection, rather than the Handle. You can find out the internal ID of a collection or community by clicking on 'Communities/collections'. The second number in brackets beside a community or collection name is that object's internal ID.

It is recommended that you follow this convention for manually created groups so it's easy to find the group you need. The admin UI will automatically create groups for workflow steps, but you need to create groups for submitters manually.

Create and Editing Groups

To manually create a group, click on **Create New Group**. Change the default group name at top to desired name and click on **Update Name**.

Instructions for using the group editor

Items

Use this tool to edit, withdraw or delete an item. You can enter an item's Handle or internal ID (database primary key) into the relevant box. Alternatively, you may find it easier to go to the relevant item's display page and then click the **Edit** button on the page which appears if you're logged in as an administrator.

Instructions for editing items

Instructions for withdrawing items

Note that the 'expunge' function will expunge the item and its metadata from the system without leaving a trace. Note that this functionality hasn't been fully tested (and it's not recommended), so there may be problems. For example, since there's no record of the deletion, the fact that the item has been deleted isn't exposed to OAI harvesters.

Supervision Orders

Select *Supervisors* in the administration area and you are presented with three options:

- Add a Supervision Order
- View Current Supervision Orders
- Clean Supervision Order Database

The sections below detail how to deal with common supervision order tasks.

Note: The option to Clean Supervision Order Database should be used once in a while just to perform basic maintenance operations on the database. It is completely automatic and takes a very short time to execute.

Viewing Current Supervision Orders

Select *View Current Supervision Orders* and you are presented with a list of all supervision orders currently in effect. From this page you can modify the policies for the supervision order or remove the supervision order. (see the sections below).

The details you have on this page allow you to see the name of the group doing the supervising, the author of the item being supervised and the title of that item.

You may also add a supervision order from this page as per the section **Adding Supervision Orders** below.

Adding Supervision Orders

Select *Add a Supervision Order* from either the main supervision order page or the Current Supervision Orders page.

To set a supervision order you need to define the group to do the supervising and the item in the workspace to be supervised. In addition, this page gives you the option to set a default set of policies for the supervising group to have over the item.

Select the desired group from the pull down list of groups on this page; this box contains all the groups that currently exist on the system. Next select the WorkSpace item to be Supervised. This means clicking on the round select box on the right of the item in the listing you can see on this page, which shows all items currently in user workspaces.

Note: the ID that is in the left hand column of the item listing is the database id for the workspace item, and is there for the reference of system administrators.

Once you have chosen the group and the workspace item to be connected you may also select a default policy from the *Initial Policy Setting* pull down box. The default policy options that this provides are:

- **None** - The supervision order is created but the supervising group is not given any policies regarding the item to be supervised. This usually indicates that the administrator has decided to manually set policies for this supervision order.
- **Observer** - The supervising group is given READ access to the item (but not to any bundles or bitstreams that already exist). Any new bundles or bitstreams inherit the supervision group's policy to permit READ operations.
- **Editor** - The supervising group is given ADD, WRITE, and READ access to the item (but not any bundles or bitstreams that already exist). Any new bundles or bitstreams inherit the supervising groups's policy to permit ADD, WRITE and READ operations.

Once happy with your selection click on *Submit Supervision Order* and your settings will be applied, and you will be returned to the supervision order main page.

Removing Supervision Orders

Go to the *View Current Supervision Orders* page and select *Remove* from the supervision order that to wish to remove. You will be asked to confirm the removal of the order, upon confirmation of which it will be removed from the system.

Customising Supervision Order Policies

Go to the *View Current Supervision Orders* page and select *Policies* for the supervision order for which you would like to customise the policies. You will be taken to the *Policies for Item* page. From here you may customise the policies for the particular item.

In order to set policies for the supervisor group you should select, for example, *Add New Policy* for the item or any of its component parts, then select the supervisor group that you are wanting to configure from the given list of groups. You can then select the Action that you want to perform and hit *Save Policy*.

Metadata Registry

By default DSpace uses a qualified version of the Dublin Core schema based on the Dublin Core Libraries Working Group Application Profile (LAP). You can also configure other flat metadata schemas in the registry. The metadata registry provides a list of the elements and qualifiers, with comments.

You can edit the registry to suit your needs with this tool, but note that:

- You can only edit one element/qualifier at a time. Make the edits to one row, and click the relevant 'update' button. Only edits you've made to that row will be saved.
- If you delete an element and qualifier, all instances of that element and qualifier in items' metadata will be deleted
- If you update an element or qualifier, for example changing 'contributor' to 'creator' and clicking 'Update', all instances of 'contributor' in items' metadata will be changed to 'creator'.
- Some Dublin Core elements/qualifiers are used by the system for various functions, such as `date.available` for OAI harvesting, and `title` for the item display and search index. You can change the scope notes for these but you shouldn't change or remove the element or qualifier. To see which elements/qualifiers are used by the system, check out the *`[dspace-source]`*`/config/registries/dublin-core.xml` file.

Also note that the `dublin-core-types.xml` is only used during the build process to populate the metadata registry in the database, which is the 'live' version. Changes you make with this UI will only be reflected in the database registry, and not the XML file (and vice versa.)

Bitstream Format Registry

This list of bitstreams provides information about known bitstreams and their support level. You can edit or add new bitstream formats with this tool. Please take note of the following:

- You can only edit one bitstream format at a time. Make the edits to one row, and click the relevant 'update' button. Only edits you've made to that row will be saved.
- 'Extensions' are file extensions that are used to automatically identify the format of uploaded files. You can enter several comma-separate extensions for each format.
- The 'Name' of each format must be unique, though the MIME type need not be. For example, you might have separate format registry entries for different versions of Microsoft Word, even though the MIME type will be the same for each of them.
- 'Internal' formats are hidden from the user, and are used for administrative purposes. For example, the licenses that submitters grant are stored as 'License' format bitstreams, and these aren't shown to end users.
- If you delete a bitstream format, any bitstreams in the system of that format will be reverted to the 'Unknown' format.
- Do not delete the 'Unknown' or 'License' formats!

Also note that the `config/registries/bitstream-formats.xml` is only used during the build process to populate the format registry in the database, which is the 'live' version. Changes you make with this UI will only be reflected in the database registry, and not the XML file (and vice versa.)

Workflow

Use this tool to clear out workflows that have been abandoned and will never be completed.

Authorization

This section is used to set specific authorization policies for communities, collections, and items. In order for users to perform an action on an object, they must have permission; DSpace operates a 'default deny' policy. Permissions do not 'commute'; for example, if an e-person has READ permission on an item, they might not necessarily have READ permission on the bundles and bitstreams in that item.

Manage a Collection's Policies

Use this tool to authorize collection-related groups to perform their roles.

- Click on **Manage a Collection's Policies**.
- Select the name of the collection for which you wish to set authorizations and click on **Edit Policies**.
- Click on **Add New**.
- Select the group for which you wish to set authorizations, and then select an action for that group from the drop-down menu.
- Click on **Save Policy**.
- Repeat until all policies are in place.

Note:

- Newly-submitted items accepted into a collection inherit the **DEFAULT_ITEM_READ** and **DEFAULT_BITSTREAM_READ** authorization policies associated with the collection, which become the **READ** policies for the item and its bitstreams. However, if you change a collection's default policies after items have been accepted, policies for existing items will not be changed automatically. You would have to change the permissions on those items using the **Advanced Policy Admin Tool** to make them accessible.
- All collections must have an **ADD** policy for a submitter group, or else no one will be able to submit items to the collection.

Manage a Community's Policies

This tool allows you to edit a community's policies in much the same way as a collection's are edited, described above.

Presently, since administration is done centrally, this tool doesn't have a lot of use--usually you will just add **READ** permission for the **Anonymous** group just after you create a community, and leave it at that. This permission is applied to the community's logo if there is one, which allows people to see the logo when they go to the community home page.

A community's policies are set to a default **Anonymous READ**.

Manage an Item's Policies

This tool allows you to edit the policies for individual items. When you wish an item's policies to be different from those of the rest of those in a collection, you can use the item policy editor to customize the policies. It is a good practice long term management of a collection however, for all of the items in a collection to share the same authorizations.

Advanced Policy Admin Tool

Use this tool to set and clear policies for items or bitstreams across a whole collection. Be careful about using the **Clear Policies** button.

Select the collection from the top list and the group you want to give or remove permission for from the bottom list. Then select the type of object (item or bistream) that you want to edit permissions for. Then select the action from the drop-down.

For example, say you wanted to give everyone in a group 'privileged_users' **Read** access to all of the bitstreams in a restricted collection. You'd select 'privileged users' from the top list, 'bitstream' from the 'content type' drop-down, 'privileged_users' from the 'group' list, 'Read' from the 'action' drop-down, and click 'Add policy'.

Edit News

You can use this tool to edit the text ("news") in two places on the DSpace home page: the top box of the center frame, and the right sidebar.

After clicking on "Edit News" on the admin menu, click on the **Edit** button next to the news item you wish to edit. A text box will be displayed with the current news, which can be deleted or modified by typing directly in the box. You can use HTML tags to format the text, but note that the html won't be validated here.

Edit Default License

You can use this tool to edit the default license of DSpace

The default license is used when no collection specific license is defined.

Note that changing the default license has no effect on allready published items.

Some substitution variables are available to make possible configure a contextual submission license:

- **%1$s** will be translated in the "submitter first name"
- **%2$s** will be translated in the "submitter last name"
- **%3$s** will be translated in the "submitter email"
- **%4$s** will be translated in the current date
- **%5$s** will be translated in the collection info
- **%6$s** will be translated in the item info
- **%7$s** will be translated in the eperson info

If you need to embed in the license text the % symbol you need to escape it with a second %, i.e. you need to write %%. It is recommended to use a dummy submission to check the license change: **check the resulting license in the Accept/reject Licence step.**