Users

Users in CONTENTdm Administration refer to administrative users with various levels of administration rights, such as adding collections, configuring collections, adding other users, and configuring the CONTENTdm website. These administrative user accounts are set up using their OCLC LDAP accounts. To add someone to CONTENTdm Administration, they must have an OCLC LDAP account.

The Welcome Email you received upon subscribing to CONTENTdm references an initial system administrator account, created from an OCLC LDAP account, with all available server and collection rights. This primary account holder can add additional users and assign the administration rights. There is no limit to the number of users that can be added. One user must have the ability to administer user rights.

Adding new users

Adding new users means granting CONTENTdm-specific rights to user accounts that already exist in OCLC LDAP accounts. To create new user accounts in OCLC LDAP, do one of the following:

1. Go to https://ldap-accounts.oclc.org/create;
2. Go to https://[yourCDMsite].org/digital/login, and click “Create account”.

Note: You will see an existing user called CDMHostingSupport. Please do not remove or change the rights for this existing user. The CDMHostingSupport account is used when CONTENTdm Support needs to access your site and perform debugging operations.

Add a new user

To add a user to CONTENTdm Administration, you must know the user's OCLC LDAP account user name.

1. Open CONTENTdm Administration and select the server tab.
2. Click users. A list of all users with CONTENTdm rights is shown.
3. Click add user.
4. Enter the desired OCLC LDAP account user name.

5. Select the server and collection rights that you wish to assign to the user. (For explanations of these rights, refer to Administration Rights below.)

6. In Select collections, you can assign rights for all collections or a subset of collections by checking Specify collections.

7. Click add.

An updated list containing the added new user is shown.

Administration rights

CONTENTdm has two levels of administration rights: Server Rights and Collection Rights.

Note: All users with a user account on the CONTENTdm Administration can use the Project Client to add items. This is
in addition to any server or collection rights they have been granted.

**Server rights**

There are four **server rights** which are global-level rights that apply to all collections.

<table>
<thead>
<tr>
<th>SERVER RIGHTS</th>
<th>ACTION</th>
</tr>
</thead>
</table>
| Add collections     | • Add collections  
                       | • Reorder collections  
                       | • Configure collection profiles*  
                       | • Harvest with WorldCat Sync and OAI  
                       | • Run reports and export metadata  
                       | • View About CONTENTdm and edit license code |
| Delete collections  | • Delete collections  
                       | • Reorder collections  
                       | • Configure collection profiles*  
                       | • Harvest with WorldCat Sync and OAI  
                       | • Run reports and export metadata  
                       | • View About CONTENTdm and edit license code |
| Administer user rights | • Add user and edit user rights  
                        | • Harvest with WorldCat Sync and OAI  
                        | • Run reports and export metadata  
                        | • View About CONTENTdm and edit license code |
| Setup global website | • Configure CONTENTdm Website at both global and collection-level |

Note: To configure collection profiles, you also need to have *Setup collection* profile right for the collection(s) (see table below).
Collection rights

There are seven Collection rights. These are collection-specific rights.

<table>
<thead>
<tr>
<th>COLLECTION RIGHTS</th>
<th>EDIT LABEL</th>
<th>WHAT IT ALLOWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve items and build indexes</td>
<td>Approve</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Approve items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Index collection</td>
</tr>
<tr>
<td>Edit metadata</td>
<td>Edit</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Find &amp; replace metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Changes are effective after re-indexing.</td>
</tr>
<tr>
<td>Set access rights</td>
<td>Rights</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Set access rights means to set permission for certain contents to be accessed by users (either based on user names or IP addresses). To change item-level permissions, you must also have the right to Edit metadata. To change collection-level permissions, you must also have the right to Setup collection profile.</td>
</tr>
<tr>
<td>Delete and unlock items</td>
<td>Delete</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete items (the user must also</td>
</tr>
</tbody>
</table>

Note: Changes are effective after re-indexing.
<table>
<thead>
<tr>
<th>COLLECTION RIGHTS</th>
<th>EDIT LABEL</th>
<th>WHAT IT ALLOWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup collection profile</td>
<td>Profile</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure collection profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit field properties of collections</td>
</tr>
<tr>
<td>Run reports and export metadata</td>
<td>Reports</td>
<td>• View collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Export metadata</td>
</tr>
<tr>
<td>Setup collection-level website</td>
<td>Website</td>
<td>• Configure CONTENTdm Website at collection-level for selected collections</td>
</tr>
</tbody>
</table>

### Scenarios for rights assignment

The above user rights matrix is complex and can be confusing. Here are a few common scenarios of how to assign rights based on different user functions:

**Site administrators and librarians**

Site administrators and librarians are responsible for administering user rights, adding and deleting collections, configuring collection properties, and working with contents.

They should have the first 3 items in **server rights** (add collections, delete collections, administer user rights) and the first 6 items in **collection rights** (approve items and build indexes, edit metadata, set access rights, delete and unlock items, setup collection profile, and run reports and export metadata).
**Student interns**

Student interns work with scanning and uploading contents and inputting metadata, possibly with specific collections only.

They should have the right to Edit metadata, and based on which collections they are working on, they can be given the rights to Set access rights, Delete and unlock items, Setup collection profile, and Run reports and export metadata for certain collections.

**Web administrators**

Web administrators are in charge of how the website looks and functions for the end-user.

They should have the right to Setup global website, or, if they belong to a consortium, they should have collection right to Setup collection-level website.

**Consortiums**

Consortiums share the use of a CONTENTdm website. With the collection rights assignment capability of CONTENTdm, administrators can easily separate the tasks of their members without overlapping functions.

**Managing User rights**

A user's CONTENTdm administration rights can be edited or deleted.

**Viewing and Editing user rights**

1. Open CONTENTdm Administration and select the server tab.
2. Click users. A list of all users with CONTENTdm rights is shown.
3. Click view or edit next to the user whose rights you wish to review.
4. From the view screen, you can click edit on the upper-right corner to make changes; similarly, if you are in edit, after you save the changes, you will be presented with the view screen.

In viewing user rights:

- **Server rights** shows those rights that this user has out of the four server rights.
- **Collection rights** show the collections in groups. Collections that have the same rights are grouped together. See Collection rights for more information.
In editing user rights, you have more sophisticated controls than when you assign rights to users that are just added.

- **Select server rights**: Check the rights you want to assign to the user and click **save changes**.

**Select collection rights**: Assign certain rights to a subset (or all) of the collections. These new selections will overwrite what was there for those collections previously. You repeat it to assign rights to all collections.

The rights are indicated by one bold word. For example, **Approve** is short for **Approve** items and build indexes.

**Current collection rights** appear below **Select collection rights** and show which existing setting you are working with. The X mark indicates that the user has the right.

For example, if you want to assign a new set of rights for the user in a certain collection:

- Select the collection from the left side.
- Check all of the rights you want to assign.
- Click **save changes**.

If the same rights should be used for multiple collections:

- Select multiple collections from the left side.
  - Use ctrl+click/shift+click on PC and command+click/shift+click on Mac.
- Check all of the rights you want to assign.
- Click **save changes**.

The new selection of rights will replace existing rights for each collection.

This also works to remove rights indirectly. Select the collections you wish to remove rights from, check the rights you want to assign instead, and save changes. Newly assigned rights will overwrite old rights, thus removing the rights you want to eliminate.
Deleting Users

When you delete users using the CONTENTdm Administration interface you are deleting their specific CONTENTdm Administration rights; you are not deleting their accounts from OCLC LDAP accounts.

Note: You cannot delete Administer user rights for the account that you are currently using.

To delete users:

1. Open CONTENTdm Administration and select the server tab.
2. Click users. A list of all users with CONTENTdm rights is shown.
3. Click delete next to the user whose rights you wish to delete. A dialog box asks you if you are sure you want to delete the user.
4. Click OK.

The user list no longer lists the user that was deleted.