ArchivesSpace User Records & Permissions Settings

Produced by the Archival Collection Management Working Group of the Content Creation & Dissemination Team
   Eva Guggemos, Pacific University (chair)
   Mark Carlson, University of Washington (co-author of this document)
   Sarah Shipley, Seattle Municipal Archives (co-author of this document)
   Amber d’Ambrosio, Willamette University
   Nathan Georgitis, University of Oregon
   Jodi Allison-Bunnell, Alliance (ex officio) (author of 1.1 update)

Version 1.1, March 2017

Introduction

System Administrator Accounts
   For Institutions Using Alliance Hosting
   For Institutions Self-Hosting

Adding & Managing User Accounts
   For a System Administrator to create/edit User Accounts for others
   For a User to create his or her own User Account

Assigning Users to Permission Groups

Default Groups & Permission Settings

Editing, Adding and Deleting Permissions for Groups

List of Available Permission Settings

Permission Settings control what users can and cannot do while they are logged in to ArchivesSpace. For example, one user might be allowed to do basic data entry in one repository, while another user might be allowed to set default preferences across multiple repositories. Managing permissions settings is an important means for allowing individuals only the access and editing capabilities appropriate to their position—and avoiding catastrophic data loss! Each user is allowed a specific set of permissions by being added to a “Group.” Groups are sets of users that have varying levels of permissions, such as Managers, Basic Data Entry users or Viewers. Permissions are set at the group level and users are added to a group depending on the level of access you want that particular user to have.

It is important to note that some permissions are granted on the Global level (affecting all repositories in an instance), while others are granted on the Repository level (affecting one repository). Some types of
permissions can only be set on the Global level because they pertain to records that are automatically shared across all your repositories. For example, because Subject, Agent, Vocabulary and Classification Terms are shared across all repositories, if you give a user permission to add or edit those records, the changes will affect all repositories.

System Administrator Accounts

Each institution using AS should have one person designated as their System Administrator. System Administrators have extensive permissions for AS setup and modification and should have sufficient knowledge of AS and/or archival collection management to make informed decisions. The System Administrator is also the point of communication between the Alliance and the institution.

For Institutions Using Alliance Hosting

The Alliance will set up the System Administrator account for your instance. You will need to communicate who your systems administrator is to the Alliance. Your System Administrator will then receive their login and password via secure transmission. Please confirm that you have received it and can login to your instance. Please do not change the password.

The System Administrator should set up and manage all other user accounts. For security reasons, it is highly recommended that you create individual user accounts for each user.

As they do so, they’ll notice the presence of two other accounts: admin and jodiab. These are, respectively, the administrator accounts for LibraryHost and the Alliance; please do not delete them. They are used only for support purposes; we will never make modifications without your permission and knowledge.

For Institutions Self-Hosting

Your institution will need to designate a System Administrator, set up their account, and communicate who systems administrator is to the Alliance.

Your System Administrator should set up and manage all other user accounts, and also set default values, preferences, and controlled value lists according to the Alliance’s documentation.

Adding & Managing User Accounts

To log into AS, each user must have a User Account. New User Accounts can either be created by the System Administrator or by the Users themselves.

For a System Administrator to create/edit User Accounts for others

If your institution is using Alliance-hosted ArchivesSpace, you will be offered the option to have either “System Administrator” or “Manager”-level account (see Default Groups & Permission Settings, below). If you have migrated from Archivists’ Toolkit, old user accounts will migrate, but passwords will need to be reset for each of them. Only System Administrators may edit or create new User Accounts for others. Each user should then be assigned to a Group with the desired level of permissions. To create/edit a User Account as a System Administrator:
1. Log into ArchivesSpace with a System Administrator account

2. Click on the “System” menu on the upper right hand corner, then select “Manage Users”

3. Click on the “Create User” or “Edit” button

4. Fill out all of the desired information fields about that user. Retype the password to confirm it. Note: if the user forgets their password or wants to choose a new one, it can be reset by the System Administrator. As of v. 1.3, users cannot reset their own passwords.

5. Caution: You can grant System Administrator permissions to the new user by checking the box on this page. Please note that this will give that user the ability to change global settings in your instance and transfer or delete all record types, so be careful.

6. Click Save.
   You have created a new User Account, but the User does not yet have permission to do anything. To grant the new user permissions, assign him/her to a Group. See Assigning Users to Permission Groups, below.

For a User to create his or her own User Account

1. Go to ArchivesSpace. Click on the “Sign In” tab, then click on the “Register now” link.

2. Fill out all the fields and re-type the password to confirm.

3. You now have a User Account, but you do not yet have permission to do anything. A user with Manager or System Administrator-level permissions must assign you to a Group before you can begin viewing or editing records. See Assigning Users to Permission Groups, below.
Managing Groups
ArchivesSpace manages permissions through “Groups,” which are sets of users who have the same level of permissions. The System Administrator can keep the default Groups and permission settings that come loaded with ArchivesSpace (see Default Group & Permission Settings, below), or change them (see Editing, Adding and Deleting Permissions for Groups, below).

Assigning Users to Permission Groups
To grant or remove permissions for a user:

1. Log into ArchivesSpace with a System Administrator or Manager-level account

2. If you have multiple repositories, select the one to which you wish to add the User in the menu in the upper-right-hand corner:

3. Click on the Gear symbol, then select “Manage User Access”:

4. Browse to the correct user, then click the “Edit Groups” button:

5. Select the desired permissions Group, then click “Update Account.”

To see more details on what the default settings for each group are, see Default Group & Permission Settings, below. Note that the highest level of permissions (System Administrator) can only be granted by another System Administrator through the Manage Users tool. See: For a System Administrator to create/edit User Accounts for others, above.

Default Groups & Permission Settings
ArchivesSpace comes with default permissions Groups. Though you can edit the permissions as needed (see below), this guide will refer to these default permission Groups when specifying which level of
permissions is needed to do certain tasks. The default Groups are:

<table>
<thead>
<tr>
<th>Default Group Name</th>
<th>Default permissions within a specific repository</th>
<th>Default permissions across all repositories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewers</td>
<td>• Can view Accessions, Resources and Digital Objects</td>
<td>• Can view Agent, Subject and other global records with the exception of contact information</td>
</tr>
</tbody>
</table>
| Basic Data Entry   | • Can view Accessions, Resources and Digital Objects  
                     • Can create & edit Accessions, Resources and Digital Objects  
                     • Can create & edit events  
                     • Can initiate import jobs | • Can view Agent, Subject and other global records with the exception of contact information |
| Advanced Data Entry| • Can view Accessions, Resources and Digital Objects  
                     • Can create & edit Accessions, Resources and Digital Objects  
                     • Can create & edit events  
                     • Can initiate import jobs  
                     • Can create & edit events  
                     • Can initiate import jobs  
                     • Can delete/suppress Accessions, Resources and Digital Objects  
                     • Can view user and repository records | • Can view Agent, Subject and other global records with the exception of contact information  
                     • Can create, edit & delete Agent, Subject and Vocabulary records  
                     • Can view contact info |
| Archivists         | • Can view Accessions, Resources and Digital Objects  
                     • Can create & edit Accessions, Resources and Digital Objects  
                     • Can create & edit events  
                     • Can initiate import jobs  
                     • Can delete/suppress Accessions, Resources and Digital Objects  
                     • Can view user and repository records | • Can view Agent, Subject and other global records with the exception of contact information  
                     • Can create, edit & delete Agent, Subject and Vocabulary records  
                     • Can view contact info |
| Project Managers   | • Can view Accessions, Resources and Digital Objects  
                     • Can create & edit Accessions, Resources and Digital Objects  
                     • Can create & edit events  
                     • Can initiate import jobs  
                     • Can delete/suppress Accessions, Resources and Digital Objects  
                     • Can view user and repository records  
                     • Can view contact info  
                     • Can merge Agent and Subject records | • Can view Agent, Subject and other global records with the exception of contact information  
                     • Can create, edit & delete Agent, Subject and Vocabulary records  
                     • Can view contact info |
| Managers           | • Can view Accessions, Resources and Digital Objects  
                     • Can create & edit Accessions, Resources and Digital Objects  
                     • Can create & edit events  
                     • Can initiate import jobs  
                     • Can delete/suppress Accessions, Resources and Digital Objects  
                     • Can view user and repository records | • Can view Agent, Subject and other global records with the exception of contact information  
                     • Can create, edit & delete Agent, Subject and Vocabulary records  
                     • Can view contact info  
                     • Can merge Agent and Subject records |
records

- Can change Group membership and other settings for the repository. Cannot modify user records or repository records.
- Can manage Rapid Data Entry templates across the repository
- Can edit their own Group to include additional permissions beyond these default settings
- Can set defaults in “My Repository Preferences”

Subject records

- Can edit Group settings to include additional permissions beyond the defaults

| System Administrator | Caution. This user has all permissions across all repositories. | Has all permissions. |

**Editing, Adding and Deleting Permissions for Groups**

ArchivesSpace allows Manager-level and System Administrator-level users to edit each Group’s permissions settings. Each Group contains the same list of permissions that can be granted or denied. You determine what the members of each Group can do by checking or unchecking the boxes for the tasks listed. Checking a task means members of that Group can perform that task; unchecking a box means they cannot perform that task. To manage permissions Groups:

1. Log in to ArchivesSpace as a user with Manager or System Administrator permissions

2. If you have multiple repositories, select the one that you want to manage using the menu in the upper-right-hand corner:

3. Click on the Gear symbol, then select “Manage Groups”:

4. Click “Create Group” or “Edit”

5. Edit the Group and Save. You may:
- Change the description of the Group
- See a list of current members in the Group
- Add or remove members
- Check or Uncheck permissions settings for that group. See the “List of Available Permission Settings,” below, for more information about each setting.
- Delete the Group (Caution: this cannot be undone.)

List of Available Permission Settings

The following table describes the permission settings that can be edited by a Manager or System Administrator using ArchivesSpace’s browser interface.

<table>
<thead>
<tr>
<th>Permission Settings</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer the entire contents of a repository</td>
<td><em>Caution.</em> Allows the user to transfer all records from one repository (such as “Museum”) to another repository (such as “Art Collection”). System Administrators only.</td>
</tr>
<tr>
<td>manage this repository (change groups and other settings)</td>
<td><em>Caution.</em> Allows the user to change preferences and defaults for the entire repository; and to add/edit groups within the repository. System Administrators only.</td>
</tr>
<tr>
<td>create/update accessions in this repository</td>
<td>Allows data entry within Accession Records. Does not allow the user to delete or suppress the records, or to create other kinds of records (e.g. Agent or Subject).</td>
</tr>
<tr>
<td>create/update resources in this repository</td>
<td>Allows data entry within Resource Records. Does not allow the user to delete or suppress the records, or to create other kinds of records (e.g. Agent or Subject).</td>
</tr>
<tr>
<td>create/update digital objects in this repository</td>
<td>Allows data entry within Digital Object Records. Does not allow the user to delete or suppress the records, or to create other kinds of records (e.g. Agent or Subject).</td>
</tr>
<tr>
<td>create/update event records in this repository</td>
<td>Allows data entry within Event Records. Does not allow the user to delete or suppress the records, or to create other kinds of records (e.g. Agent or Subject).</td>
</tr>
<tr>
<td>delete event records in this repository</td>
<td><em>Caution.</em> Allows deletion of Event Records. This action cannot be undone.</td>
</tr>
<tr>
<td>suppress the major record types in this repository</td>
<td>Allows suppression of Accession, Resource and Digital Object records within the repository. Does not affect global records (Agent, Subject, Classification, etc.).</td>
</tr>
<tr>
<td>transfer major record types between repositories</td>
<td>Allows transfer of specific Accession, Resource and Digital Object records between repositories. Does not allow mass-transfer of multiple records.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>delete the major record types in this repository</td>
<td><em>Caution.</em> Allows deletion of Accession, Resource and Digital Object records within the repository. This action cannot be undone. Does not affect global records (Agent, Subject, Classification, etc.).</td>
</tr>
<tr>
<td>view suppressed records in this repository</td>
<td>Allows viewing of suppressed Accession, Resource and Digital Object records within the repository. Does not affect global records (Agent, Subject, etc.).</td>
</tr>
<tr>
<td>view the records in this repository</td>
<td>Allows viewing of Accession, Resource and Digital Object records within the repository as well as global records for Agents, Subjects, Classifications, etc.</td>
</tr>
<tr>
<td>create/update classifications and classification terms (all repositories)</td>
<td>Allows data entry within Classifications and Classification terms. Does not allow the user to delete the records.</td>
</tr>
<tr>
<td>delete classifications and classification terms (all repositories)</td>
<td><em>Caution.</em> Allows deletion of Classifications and Classification terms. This action cannot be undone.</td>
</tr>
<tr>
<td>initiate import jobs (all repositories)</td>
<td>Allows user to start import jobs for EAD, EAC, MARCXML and CSV files.</td>
</tr>
<tr>
<td>cancel an import job (all repositories)</td>
<td>Allows user to cancel an import job.</td>
</tr>
<tr>
<td>create/update/delete subject records (all repositories)</td>
<td><em>Caution.</em> Allows creation, editing and deletion of Subject records. Note: Changes to Subject Records will affect all repositories in your instance. Deletion cannot be undone.</td>
</tr>
<tr>
<td>create/update/delete agent records (all repositories)</td>
<td><em>Caution.</em> Allows creation, editing and deletion of Agent records. Note: Changes to Agent Records will affect all repositories in your instance. Deletion cannot be undone.</td>
</tr>
<tr>
<td>create/update/delete vocabulary records (all repositories)</td>
<td><em>Caution.</em> Allows creation, editing and deletion of Vocabulary records. Note: Changes to Agent Records will affect all repositories in your instance. Deletion cannot be undone.</td>
</tr>
<tr>
<td>merge agent/subject records (all repositories)</td>
<td><em>Caution.</em> Allows user to merge duplicative Agent or Subject records into a single record. Note: Changes to Agent/Subject Records will affect all repositories in your instance. Merges cannot be undone.</td>
</tr>
<tr>
<td>merge the major record types in this repository</td>
<td><em>Caution.</em> Allows user to merge duplicative Accession, Resource and Digital Object records. Cannot be undone.</td>
</tr>
<tr>
<td>manage_rde_templates</td>
<td><em>Caution.</em> Allows user to create and edit repository-wide Rapid Entry Entry templates.</td>
</tr>
<tr>
<td>create/update top container records (all repositories)</td>
<td><em>Caution.</em> Allows creation and editing of top container records.</td>
</tr>
<tr>
<td>delete/bulk update top container records (all repositories)</td>
<td>Caution. Allows deletion and bulk editing of top container records.</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>create/update/delete container profile (all repositories) records</td>
<td>Caution. Allows creation, editing, and deletion of container profile records.</td>
</tr>
<tr>
<td>create/update/delete location profile records (all repositories)</td>
<td>Caution. Allows creation, editing, and deletion of location profile records.</td>
</tr>
</tbody>
</table>