Managing User Accounts

- Authorization model
  - Groups
  - Resource policies
- User Accounts
  - From the browser: XMLUI
  - From the browser: JSPUI
  - From the command line
    - The user command
      - To create a new user account:
      - To list accounts:
      - To modify an account:
      - To delete an account:
    - The Groomer
      - Find accounts with unsalted passwords
      - Find (and perhaps delete) disused accounts

Authorization model

The DSpace authorization model is based on group level permissions. Memberships of different groups is not mutually exclusive. As a result, a user's permissions is the sum of all permissions granted through the memberships of each group.

All users are automatically member of the "Anonymous group", which is the group used to grant permissions to non-authorized users. The administrator group, is the one associated with administrator level privileges. These two groups are the only two mandatory ones, but an arbitrary number of additional groups can be used and configured.

Groups

...

Resource policies

...

User Accounts

When a user registers an account for the purpose of subscribing to change notices, submitting content, or the like, DSpace creates an EPerson record in the database. Administrators can manipulate these records in several ways.

Please note that when a user has submitted content, his EPerson record cannot be deleted because there are references to it from the submitted item(s). If it is necessary to prevent further use of such an account, it can be marked "cannot log in".

From the browser: XMLUI

TBS

From the browser: JSPUI

TBS

From the command line

The user command

The `dspace user` command adds, lists, modifies, and deletes EPerson records.

To create a new user account:

```
[dspace]/bin/dspace user --add --email jquser@example.com -g John -s User --password hiddensecret
[dspace]/bin/dspace user --add --netid jquser --telephone 555-555-1234 --password hiddensecret
```

One of the options `--email` or `--netid` is required to name the record. The complete options are:
-a --add   required
-m --email email address
-n --netid "netid" (a username in an external system such as a directory – see Authentication Methods for details)
-p --password a password for the account. Required.
-g --givenname First or given name
-s --surname Last or surname
-t --telephone Telephone number
-l --language Preferred language

To list accounts:

[dspace]/bin/dspace user --list

This simply lists some characteristics of each EPerson.

<table>
<thead>
<tr>
<th>short</th>
<th>long</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-L</td>
<td>--list</td>
<td>required</td>
</tr>
</tbody>
</table>

To modify an account:

[dspace]/bin/dspace user --modify -m george@example.com

<table>
<thead>
<tr>
<th>short</th>
<th>long</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-M</td>
<td>--modify</td>
<td>required</td>
</tr>
<tr>
<td>-m</td>
<td>--email</td>
<td>identify the account by email address</td>
</tr>
<tr>
<td>-n</td>
<td>--netid</td>
<td>identify the account by netid</td>
</tr>
<tr>
<td>-g</td>
<td>--givenname</td>
<td>First or given name</td>
</tr>
<tr>
<td>-s</td>
<td>--surname</td>
<td>Last or surname</td>
</tr>
<tr>
<td>-t</td>
<td>--telephone</td>
<td>telephone number</td>
</tr>
<tr>
<td>-l</td>
<td>--language</td>
<td>preferred language</td>
</tr>
<tr>
<td>-c</td>
<td>--requireCertificate</td>
<td>certificate required?</td>
</tr>
<tr>
<td>-C</td>
<td>--canLogIn</td>
<td>is the account enabled or disabled?</td>
</tr>
<tr>
<td>-i</td>
<td>--newEmail</td>
<td>set or change email address</td>
</tr>
<tr>
<td>-I</td>
<td>--newNetid</td>
<td>set or change netid</td>
</tr>
</tbody>
</table>

To delete an account:

[dspace]/bin/dspace user --delete -n martha

<table>
<thead>
<tr>
<th>short</th>
<th>long</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>--delete</td>
<td>required</td>
</tr>
<tr>
<td>-m</td>
<td>--email</td>
<td>identify the account by email address</td>
</tr>
<tr>
<td>-n</td>
<td>--netid</td>
<td>identify the account by netid</td>
</tr>
</tbody>
</table>
The Groomer

This tool inspects all user accounts for several conditions.

<table>
<thead>
<tr>
<th>short</th>
<th>long</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>--aging</td>
<td>find accounts not logged in since a given date</td>
</tr>
<tr>
<td>-u</td>
<td>--unsalted</td>
<td>find accounts not using salted password hashes</td>
</tr>
<tr>
<td>-b</td>
<td>--before</td>
<td>date cutoff for --aging</td>
</tr>
<tr>
<td>-d</td>
<td>--delete</td>
<td>delete disused accounts (used with --aging)</td>
</tr>
</tbody>
</table>

Find accounts with unsalted passwords

Earlier versions of DSpace used an "unsalted hash" method to protect user passwords. Recent versions use a salted hash. You can find accounts which have never been converted to salted hashing:

Discovering accounts with unsalted password hashes

[DSpace]/bin/dsrun org.dspace.eperson.Groomer -u

The output is a list of email addresses for matching accounts.

Find (and perhaps delete) disused accounts

You can list accounts which have not logged on since a given date:

Discovering disused accounts

[DSpace]/bin/dsrun org.dspace.eperson.Groomer -a -b 07/20/1969

The output is a tab-separated-value table of the EPerson ID, last login date, email address, netid, and full name for each matching account.

You can also have the tool delete matching accounts:

Deleting disused accounts

[DSpace]/bin/dsrun org.dspace.eperson.Groomer -a -b 07/20/1969 -d