

Managing User Accounts

- From the browser
- 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
- Cryptographic properties

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.

From the browser

- Login as an Administrator
- Sidemenu "Access Control" "People"
- Browse or search for the account you wish to modify or delete.

To modify user permissions / group memberships:

- Login as an Administrator
- Sidemenu "Access Control" "Groups"
- Edit the Group
- Search for the EPerson & add/remove them from that group.

To debug issues for a specific user, it's possible to login as (or "impersonate") that user account

- On the backend, first you MUST enable the "assumelogin" feature. This feature is disabled by default. Update this setting in your local.cfg or dspace.cfg

```
# Required to use "Impersonate EPerson" feature
# When enabled, a full Administrator can impersonate any other non-Administrative user
webui.user.assumelogin = true
```

- Then, from the user interface, login as an Administrator
- Sidemenu "Access Control" "People"
- Browse or search for the account you wish to login as
- Edit that User, and click the "Impersonate EPerson" button.
- You are now logged in as that user. You'll see an Impersonate icon/button in the header.
- You are able to temporarily manage any activities as that user.
- Once your are done, click the "Stop impersonating EPerson".
- Optionally, you may wish to disable this feature again in your local.cfg by setting the above configuration to "false" or commenting it out.

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
-c	--requireCertificate	Certificate required? See X.509 Authentication for details.

To list accounts:

```
[dspace]/bin/dspace user --list
```

This simply lists some characteristics of each EPerson.

short	long	meaning
-L	--list	required

To modify an account:

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

short	long	meaning
-M	--modify	required
-m	--email	identify the account by email address
-n	--netid	identify the account by netid
-g	--givenname	First or given name
-s	--surname	Last or surname
-t	--telephone	telephone number
-l	--language	preferred language
-c	--requireCertificate	certificate required?
-C	--canLogIn	is the account enabled or disabled?
-i	--newEmail	set or change email address
-l	--newNetid	set or change netid
-w	--newPassword	set or change password

To delete an account:

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

short	long	meaning
-d	--delete	required
-m	--email	identify the account by email address
-n	--netid	identify the account by netid

The Groomer

This tool inspects all user accounts for several conditions.

short	long	meaning
-a	--aging	find accounts not logged in since a given date
-u	--unsalted	find accounts not using salted password hashes
-b	--before	date cutoff for --aging
-d	--delete	delete disused accounts (used with --aging)

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/dspace 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/dspace 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/dspace dsrun org.dspace.eperson.Groomer -a -b 07/20/1969 -d
```

Cryptographic properties

The cryptographic properties used for generating the salted hashes, to ensure encryption at rest for user passwords, can be found and adjusted in:

<https://github.com/DSpace/DSpace/blob/main/dspace-api/src/main/java/org/dspace/eperson/PasswordHash.java>