Navigation Sheet – User Rights & DAGs

Compliance & Data Office

Research Support Office

Karolinska Institutet

Introduction

When using REDCap in your research project, it is very important to restrict who has access to what information.

It is the project owner's / registered PI's responsibility to add (and remove) relevant users to their project and to make sure that individual user rights and permissions are assigned correctly.

REDCap's *User Rights* section provides the option to limit data access on various different levels. This guide provides an overview of how to add users to your project and how to set each user's permissions appropriately. In addition, this guide explains how to set up Data Access Groups (DAGs) and how to use them.

We also recommend reading through our *Tips & Best Practices* section at the end of this document.

Table of contents

Adding Users to Your Project 1

Creating Roles in Your Project 3

Overview of User Rights 5

- Basic User Privileges 5
- Privileges for Viewing and Exporting Data 7

Data Access Groups (DAGs) 9

- Setting up DAGs and assigning users 9
- Entering/Assigning records in a DAG 10
- Assigning users to multiple DAGs (DAG Switcher) 11

User Access Dashboard 13

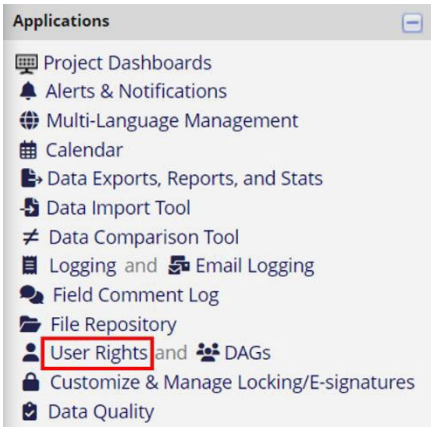
Troubleshooting 14

Tips & Best Practices 15

Adding Users to Your Project

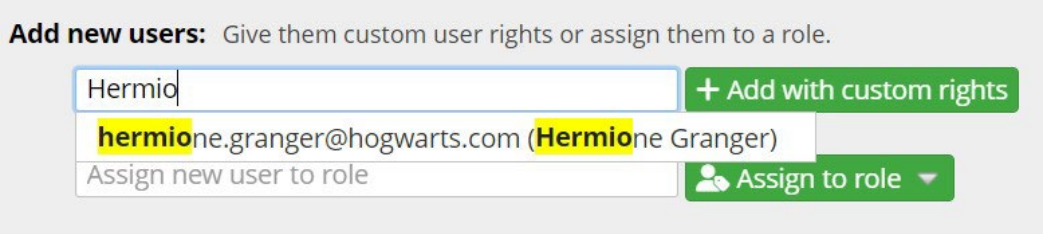
Before being able to access a project in REDCap, the person needs to create a user account. More information on how to create a REDCap user account can be found on the staff portal.

Please note that simply adding someone's email address in your project will not provide that person access to your project if they don't already have an active user account in REDCap. You can only add users to your project after they create their user account.



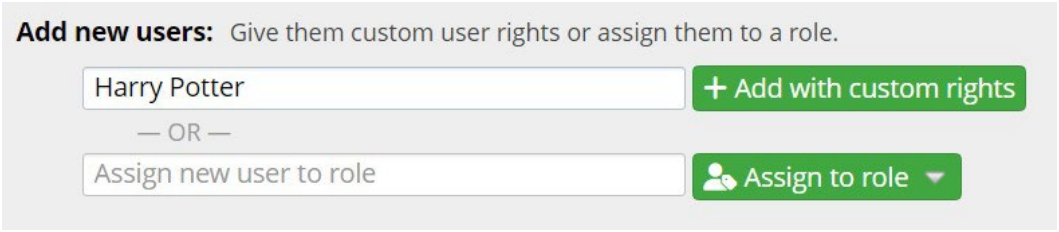
To add an existing user account to your project, navigate to *User Rights* in the menu on the left-hand side.

Type the person's name into the textbox next to *Add with custom rights* and choose the correct user in the appearing drop-down list. For example, you want to add Hermione Granger to your project:

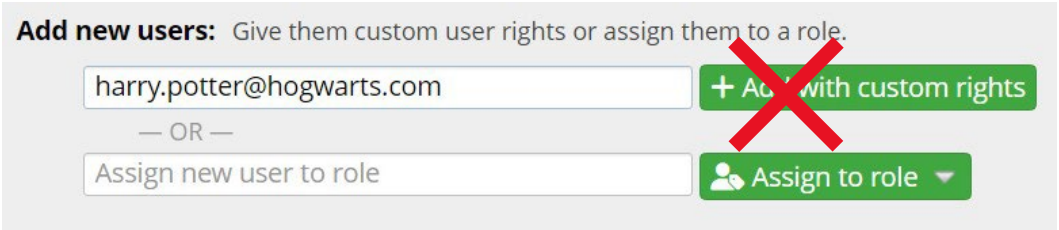


Once you select Hermione's account and click on *Add with custom rights,* REDCap will ask you to set her user rights. **It is important to not simply select all options when setting user rights, but to think carefully about what access each user actually needs.**

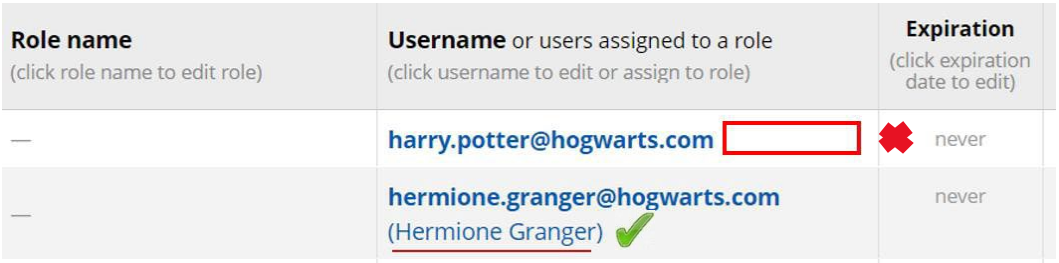
If no drop-down options are generated, the person you are trying to add has not yet created their user account. For example, REDCap does not suggest a user account for Harry Potter below, Harry still has to create his account before he can be added to your project:



If you try to add Harry to your project anyway by writing out his email address, his email will appear in the list of users below, but it will not be connected to a user account and Harry will not automatically be invited to REDCap:



If a user account has been added correctly, their name appears in brackets next to their email address:



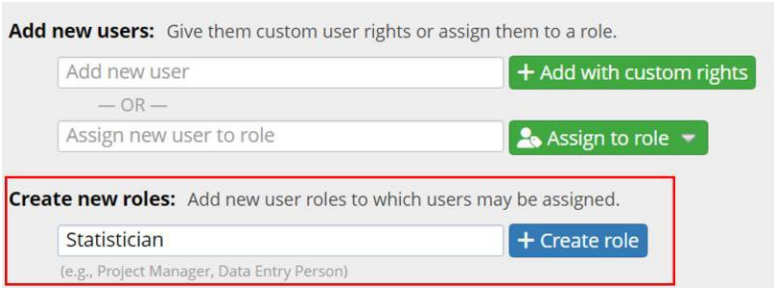
If no name appears next to the email address, no actual user account has been added to your project and that person will not be able to access your project.

Creating Roles in Your Project

Instead of designating user rights individually for each user, it is possible to create user roles with pre-defined user rights.

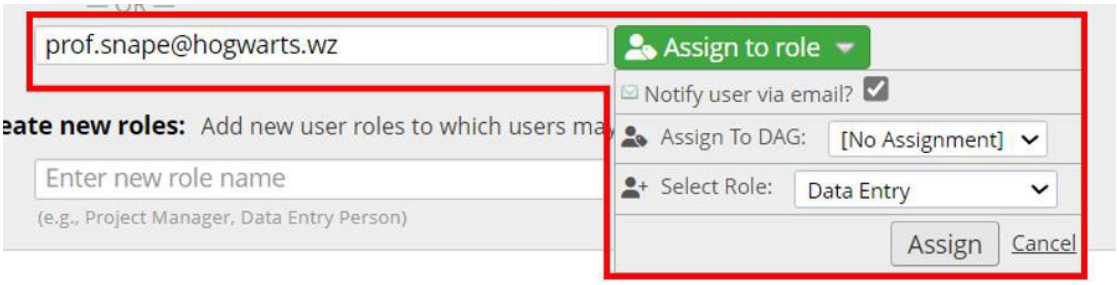
This can be helpful if your project will have several users who require the same user rights, for example, data entry staff. Using roles also streamlines the process of adding users to a project and ensures that each user is given relevant access from the start.

First, you navigate to *User Rights* and create different roles for your project:



Role name (click role name to edit role)	Username or users assigned to a role (click username to edit or assign to role)	Expiration (click expiration date to edit)	Data Access Group (click DAG to assign user)	Project Design and Setup	User Rights	Data Access Groups	Data Viewing Rights	Data Export Rights	Alerts & Notifications
—	hermione.granger@hogwarts.com (Hermione Granger)	never	—	✗	✗	✗	1 View & Edit	1 De-Identified	✗
—	musip-siguz@eduid.se (Josefine Doe)	never	—	✓	✓	✓	1 View & Edit	1 Full Data Set	✓
Data Coordinator	[No users assigned]			✗	✗	✗	1 View & Edit	1 Full Data Set	✗
Data Entry	[No users assigned]			✗	✗	✗	1 View & Edit	1 No Access	✗
Monitor	[No users assigned]			✗	✗	✗	1 Read Only	1 De-Identified	✗
Principal Investigator	[No users assigned]			✓	✓	✓	1 View & Edit	1 Full Data Set	✓
Statistician	[No users assigned]			✗	✗	✗	1 Read Only	1 De-Identified	✗

Once roles with relevant user rights have been created, you can add users via the text box next to *Assign to role*:



Alternatively, it is possible to add existing users to a role by clicking on a username – *Assign to tole* – select relevant role – click on *Assign*:



After assigning users to different roles, their user accounts will show up next to their assigned role:

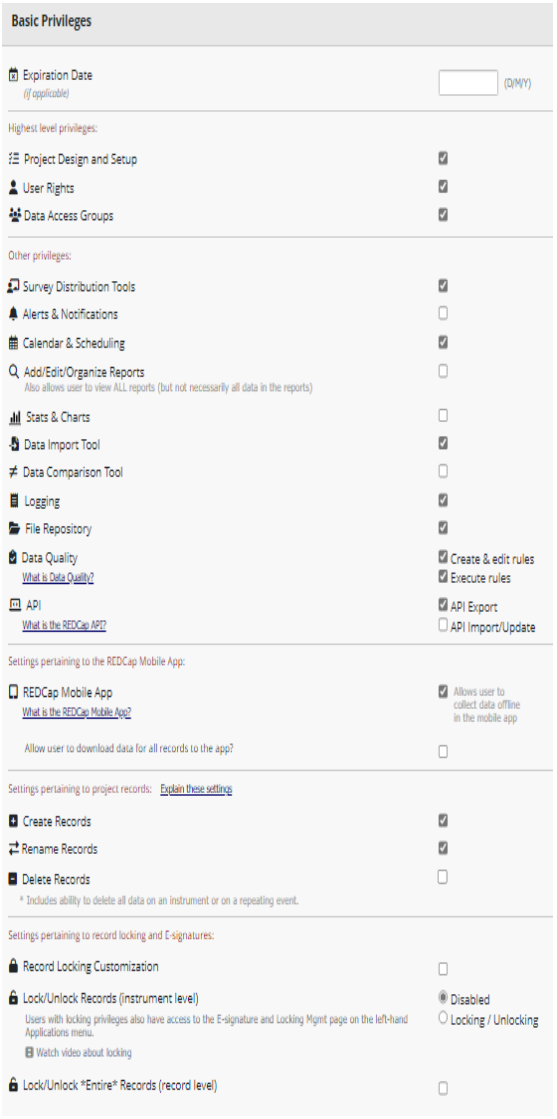
Role name (click role name to edit role)	Username or users assigned to a role (click username to edit or assign to role)	Expiration (click expiration date to edit)	Data Access Group (click DAG to assign user)	Project Design and Setup	User Rights	Data Access Groups	Data Viewing Rights	Data Export Rights	Alert Notifica
—	musip-siguz@eduid.se (Josefine Doe)	never	—	✔	✔	✔	1 View & Edit	1 Full Data Set	✔
Data Coordinator	[No users assigned]			✖	✖	✖	1 View & Edit	1 Full Data Set	✖
Data Entry	prof.snape@hogwarts.wz (Professor Snape)	never	—	✖	✖	✖	1 View & Edit	1 No Access	✖
Monitor	[No users assigned]			✖	✖	✖	1 Read Only	1 De-Identified	✖
Principal Investigator	[No users assigned]			✔	✔	✔	1 View & Edit	1 Full Data Set	✔
Statistician	hermione.granger@hogwarts.com (Hermione Granger)	never	—	✖	✖	✖	1 Read Only	1 De-Identified	✖

Whether using individual user rights or roles, it is important to regularly review all users and their user rights within your project(s).

This can easily be done by reviewing the *User Access Dashboard* (see relevant section below).

Overview of User Rights

Basic User Privileges



Expiration Date: Gives users access to the project until a specified date.

Project Design & Setup: Allows users to make changes to the project (e.g. add instruments / variables, enable / disable project features)

User Rights: Allows users to assign and change user rights for themselves and others.

Data Access Groups (DAGs)*: Allows users to create DAGs and assign other users to DAGs *(see below section "Data Access Groups (DAGs)" for more information).*

Survey Distribution Tools: Gives users access to the public survey link, participant list (which might include email addresses) and survey invitation log.

Alerts & Notifications: Allows users to construct alerts and send customised email notifications to one or more recipients using conditional logic.

Calendar & Scheduling*: Allows users to access the calendar and schedule calendar events.

Add/Edit/Organise Reports*: Allows users to add/edit reports via *Data Exports, Reports and Stats*. However, data viewing rights might affect what data a user actually sees *(see below section "Privileges for Viewing and Exporting Data" for more information on data viewing rights).*

Stats & Charts*: Allows users to view collected data graphically and to view descriptive statistics for all variables in the project.

Data Import Tool: Allows users to import data into the project (as opposed to manual data entry).

Data Comparison Tool: Allows users to compare two records as well as repeated measures of the same record side by side.

Logging: Allows users to view all project activity (which user has done what within the project).

File Repository: Allows users to access the file repository and any files stored there (this might include consent forms if using e-consent).

Data Quality: Gives users access to data quality features (running, creating, and editing data quality rules).

API (Application Programming Interface): Allows users to request API tokens and access API features. API allows external applications to connect to REDCap and is used to programmatically interface REDCap with apps, widgets, and other projects.

REDCap Mobile App*: Gives users the ability to use REDCap's mobile app, which can be installed on mobile devices (e.g. tablets, mobile phones) and used for offline data collection. That data can then be synched with the corresponding project when an internet connection becomes available.

Create Records: Allows users to create new record IDs and add participants to the project.

Rename Records: Allows users to rename existing records (e.g. change the record ID number).

Delete Records: Allows users to delete records from the project.

Record Locking Customisation: Allows users to customise the record-locking text and options as well as e-signature options on data collection instruments.

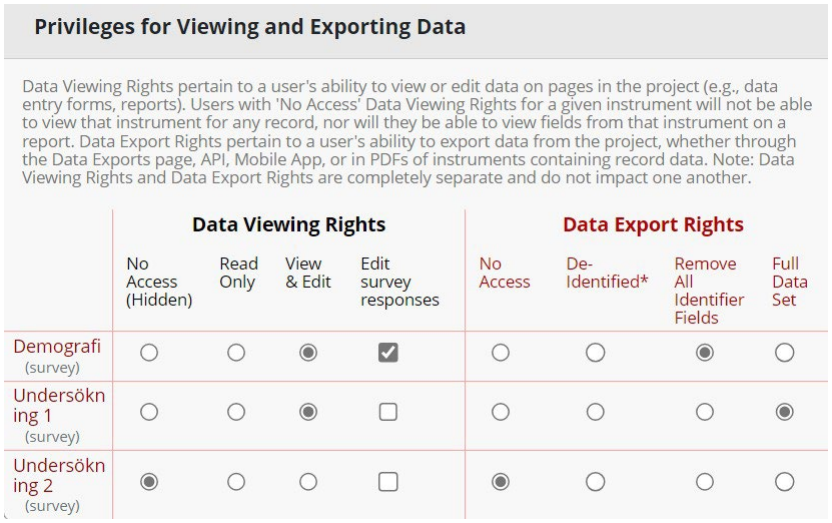
Lock/Unlock Records (instrument level): Allows users to lock and unlock individual instruments (e.g., after data entry is complete).

Lock/Unlock "entire" Records (record level): Allows users to lock and unlock all forms and surveys (instruments) at once for any given record.

*Instruction video can be found in REDCap

Privileges for Viewing and Exporting Data

The section *Privileges for Viewing and Exporting Data* lets you set user rights for each individual instrument in your project.



Privileges for Viewing and Exporting Data

Data Viewing Rights pertain to a user's ability to view or edit data on pages in the project (e.g., data entry forms, reports). Users with 'No Access' Data Viewing Rights for a given instrument will not be able to view that instrument for any record, nor will they be able to view fields from that instrument on a report. Data Export Rights pertain to a user's ability to export data from the project, whether through the Data Exports page, API, Mobile App, or in PDFs of instruments containing record data. Note: Data Viewing Rights and Data Export Rights are completely separate and do not impact one another.

	Data Viewing Rights				Data Export Rights			
	No Access (Hidden)	Read Only	View & Edit	Edit survey responses	No Access	De-Identified*	Remove All Identifier Fields	Full Data Set
Demografi (survey)	○	○	◉	☑	○	○	◉	○
Undersökning 1 (survey)	○	○	◉	☐	○	○	○	◉
Undersökning 2 (survey)	◉	○	○	☐	◉	○	○	○

By default, users have full access to all instruments and can view and edit instruments and survey responses. However, access for both *Data Viewing Rights* and *Data Export Rights* can (and should) be customised per user or role:

Data Viewing Rights

No Access (Hidden): Users cannot view or edit the instrument or any data in it. Users might still be able to view the data in data exports (see "Data Export Rights" below).

Read Only: Users can view the instrument and its data but cannot edit the data.

View & Edit: Users can view the instrument and edit data in data entry forms in REDCap.

Edit Survey Responses: Users can edit survey responses and alter survey data entered directly by participants.

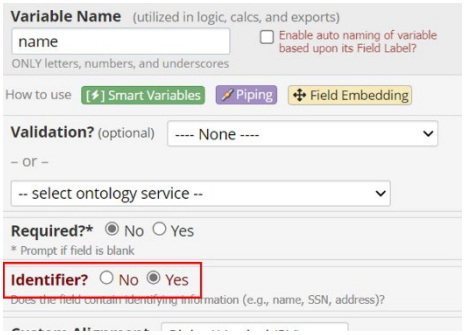
Data Export Rights

No Access: Users are not able to export data for the instrument.

De-Identified: Removes all free-form text fields as well as any date/time fields and Identifier fields from the export file.

Remove All Identifier Fields: Upon export, all data belonging to fields marked as *Identifier* fields is removed.

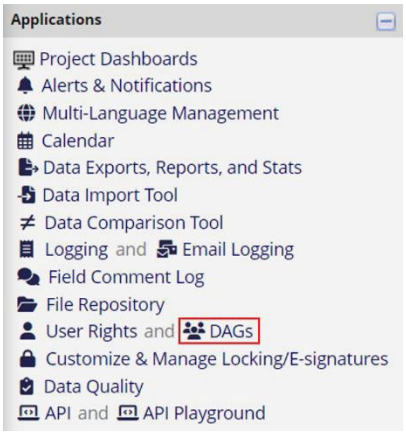
Please note: It is the researcher's responsibility to correctly mark relevant fields as *Identifiers* when building their instruments in *Designer*.



Full Data Set: Users can export the full data set of the instrument without restrictions.

Data Access Groups (DAGs)

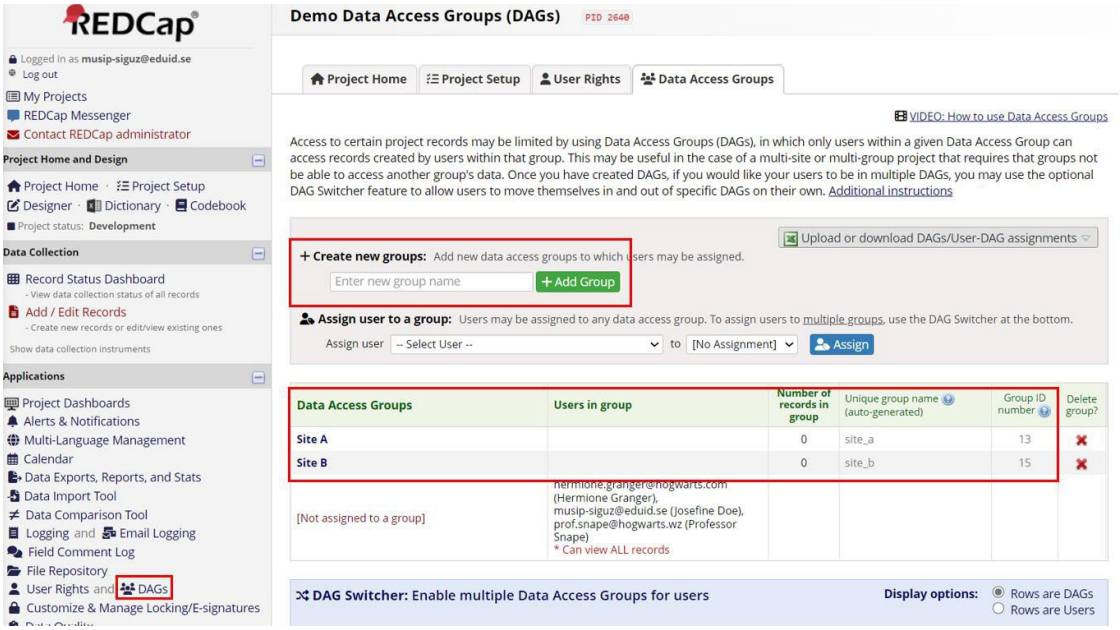
It is possible to limit access to data within REDCap by adding users to so-called Data Access Groups (DAGs). Once added to a DAG, a user can only access records and data created by other users in the same DAG. This might be useful in, for example, multicentre studies where different sites should not have access to each other's data.



Setting up DAGs and assigning users

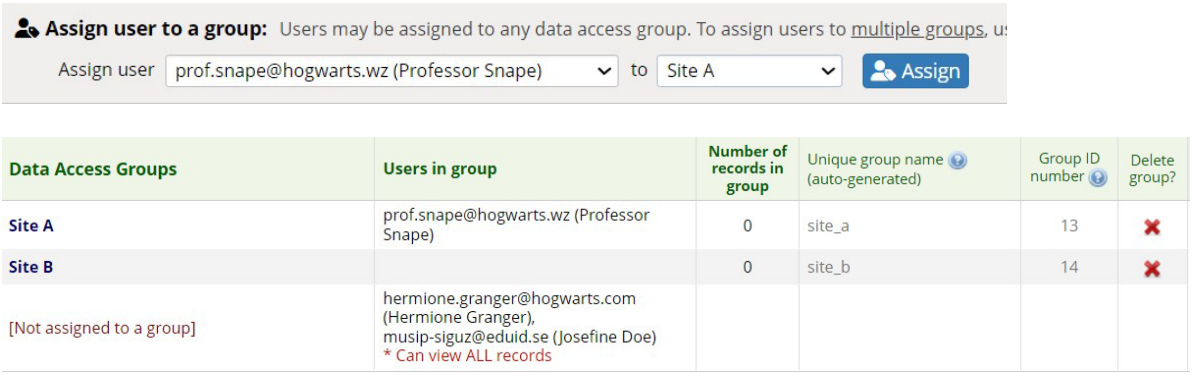
Any user with DAG rights (see "Basic User Privileges" above) can create DAGs and add users as follows:

1. Go to *DAGs* in the left-hand side menu and create new groups. Once a Data Access Group is created, it is assigned a unique group name and ID number:



2. Once all DAGs have been created, you can start assigning users. For example, by assigning Professor Snape to the DAG *Site A* he will now only have access to data generated within that DAG. Likewise, any

records he creates and data he enters will belong to *Site A* and will only be available to other users in *Site A*.

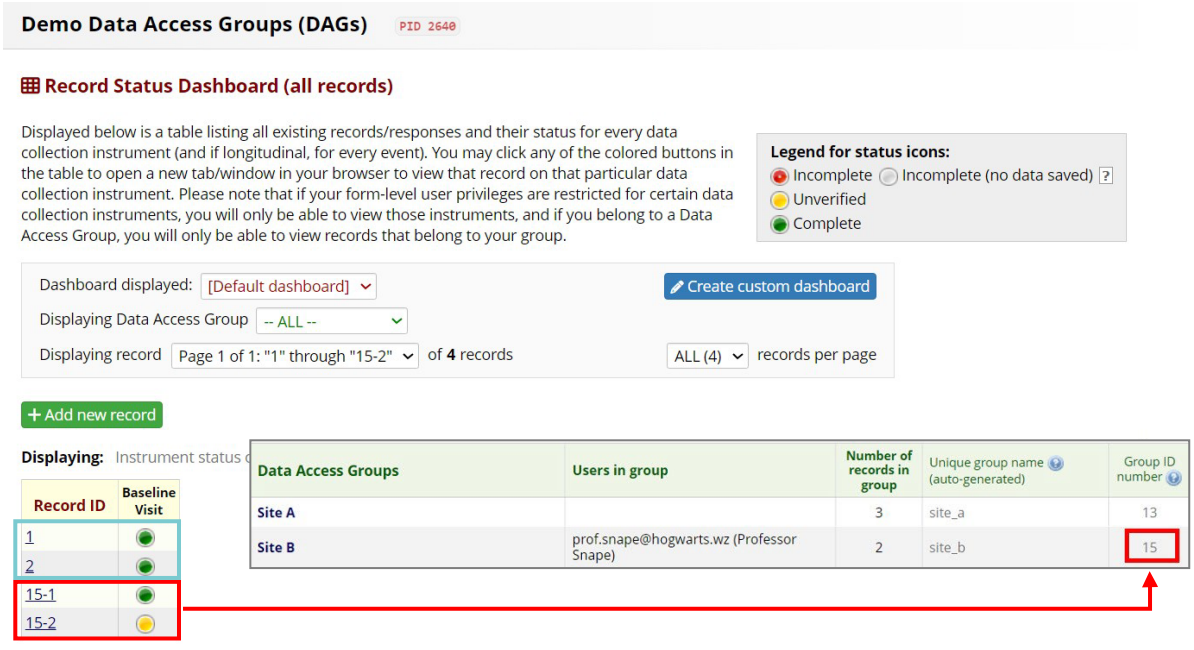


3. Since Hermione is not assigned to any DAG, she has access to all records and data in the project.

Entering/Assigning records in a DAG

Any records created by users who are assigned to a DAG will automatically be assigned to the same DAG.

If auto-numbering of records is enabled, REDCap will use the unique DAG ID-number followed by sequential numbering to create new record IDs. For example, Professor Snape who is in DAG *Site B* has created two records.

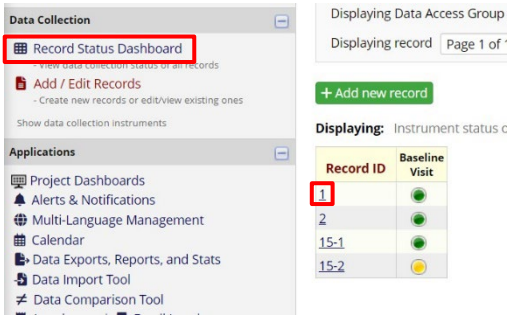


Since *Site B*'s unique group ID-number is 15, any records Professor Snape creates will have ID numbers that start with 15 (outlined in red above).

If auto-numbering is turned off, users may enter custom record IDs as usual. REDCap will alert the user if the same record ID has already been used in a different DAG.

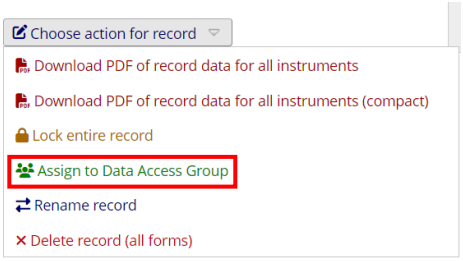
If a user who is not part of any DAG creates a new record, that record will also not be associated with a specific DAG. These records can only be viewed by users who are not assigned a DAG. Records created outside of DAGs follow regular sequential numbering (outlined in blue above).

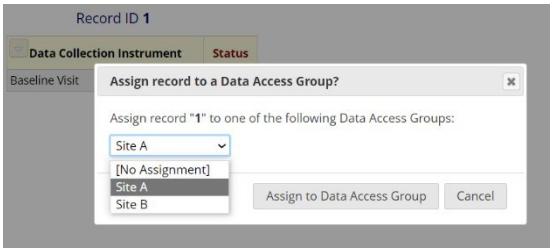
These records can be assigned to a DAG at a later time. To reassign records to a DAG, follow these steps:



- Go to *Record Status Dashboard* and click on the record ID-number you want to update

- Click on *Choose action for record – Assign to Data Access Group*



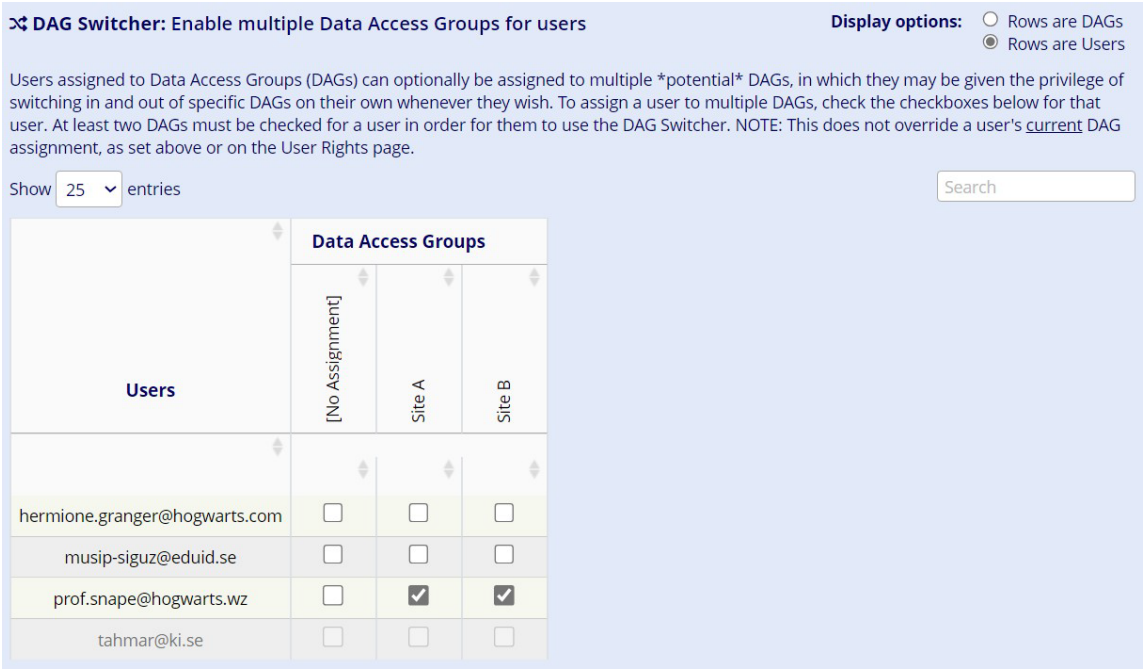


- In the pop-up window, assign to desired group and confirm.

Assigning users to multiple DAGs (DAG Switcher)

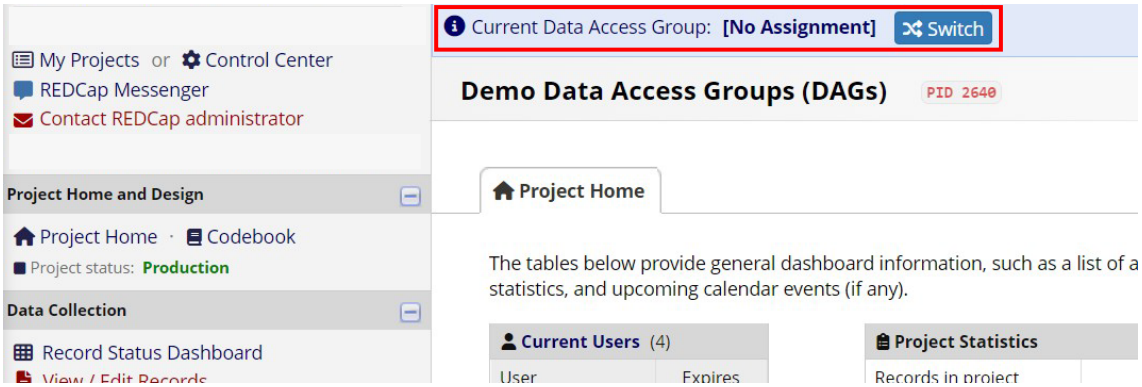
Users can be assigned to multiple DAGs and given permission to switch in and out of those DAGs as they wish. The DAG Switcher can be found in the *DAGs* menu below the list of Data Access Groups.

For example, we want to give Professor Snape access to both *Site A* and *Site B*. Go to DAG Switcher in the *DAGs* menu and tick the relevant boxes for Professor Snape to give him access to these two sites.



Now, Professor Snape can switch in and out of two DAGs (*Site A* and *Site B*) and create records for both.

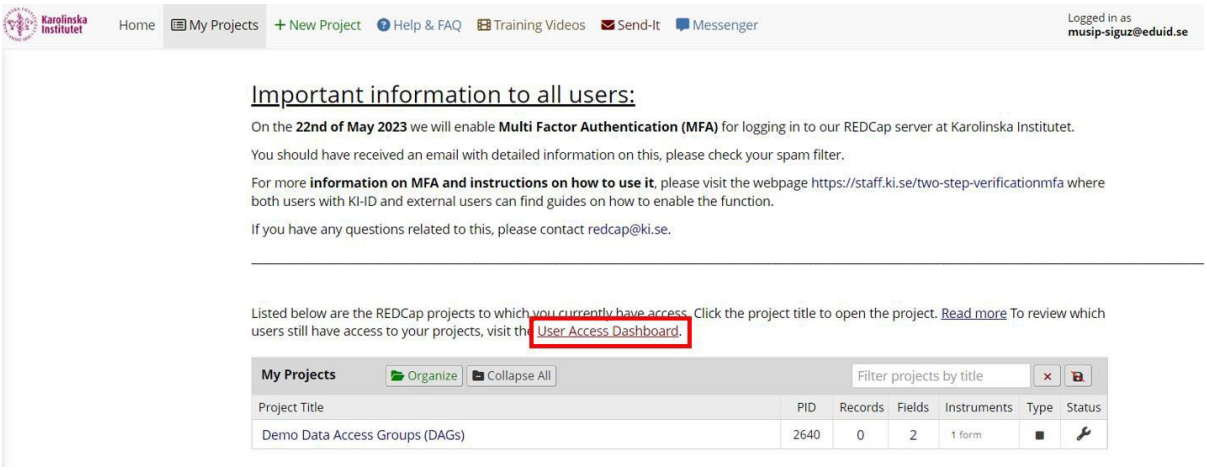
Users who are assigned to multiple DAGs have to make sure they are currently in the correct DAG before creating a new record. This can be done by checking the blue textbox at the top of the page.



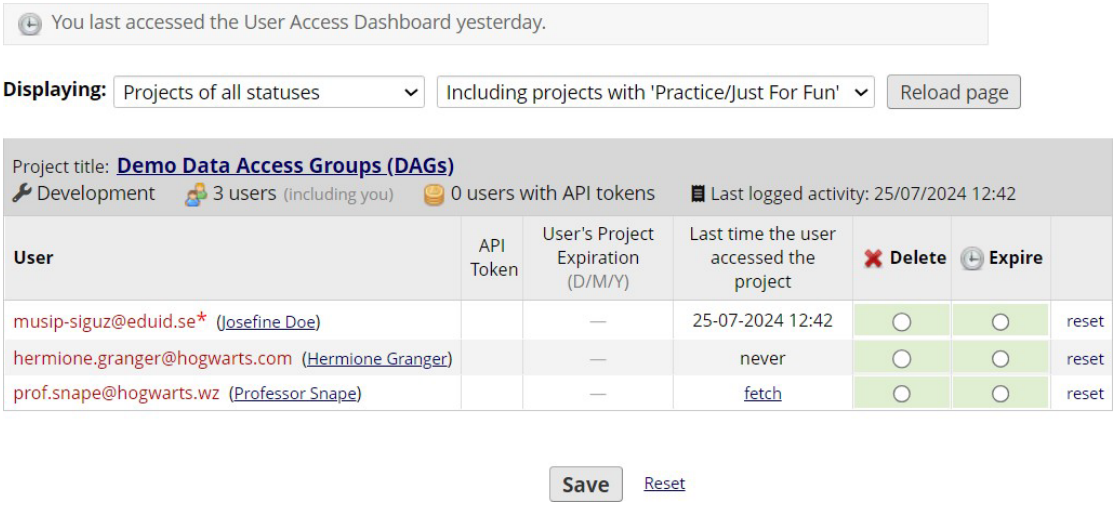
Here, a user may also switch to a different DAG or go to “no assignment” (if they were given access to the “no assignment” group).

User Access Dashboard

The *User Access Dashboard* can be found under the *My Projects* tab if a user has been assigned user rights to at least one project.



This dashboard gives an overview of all users who have access to your projects and enables easy removal or adjustment of users if needed.



For each user, you see whether they hold an API token, whether they were added to the project with an expiration date, and when they last accessed the project.

You can take two actions on the dashboard page:

- **Delete:** deletes the user from the project
- **Expire:** set an expiration date for the user's access to the project

After making changes on the dashboard, don't forget to click on "save."

Troubleshooting

If a collaborator cannot access your project, check the following:

- **Does the person have a REDCap account?**
  Before a person can be added to a project, they have to create a REDCap user account; more information on how to create a REDCap user account can be found on the staff portal.

- **Has the person been added to the project correctly?**
  It is not possible to invite a person to REDCap by adding their email address to your project. To add a person to your project, follow the steps outlined in the section "How to Add Users to Your Project" above.

- **Has the person's user account been suspended?**
  All REDCap user accounts are automatically suspended after two years of inactivity and deleted after a further 6 months. Each user is responsible for keeping their account active by logging in regularly. If a user account has been suspended, they should email redcap@ki.se to get the suspension lifted. If their account has been deleted, the user must create a new account which then needs to be added to relevant projects again.

- **Was the user account added with an expiration date?**
  Check that the user account was either added without an expiration date or is not past its expiration date. If needed, renew the expiration date and/or add the user to your project again.

Tips & Best Practices

Only enable user rights a user actually needs: Do not simply tick all options in the user rights section but consider what access a user needs. Set expiration dates for users where relevant. Make sure users are assigned appropriately and with minimal required user rights.

Review the *User Access Dashboard* regularly: Review who has access to your projects on a regular basis (e.g., every six months) and remove or adjust users as needed.

Make use of user roles: User roles need to only be set up once and provide a pre-determined level of access when adding new users to a project. This makes the process of adding new users easier and faster. Roles are especially useful in projects with many users and projects where the list of users changes frequently.

Make use of Data Access Groups: Using DAGs is recommended for, for example, multicentre studies so that users from different sites can work in REDCap without seeing other sites' data.

Mark sensitive and identifiable data in your project: Mark sensitive and identifiable information in your project and limit who can access and export that data.

Collect sensitive information in one instrument: If your project collects identifiable information but you have users who should not be able to see that kind of information, you could collect all identifiable data in one instrument and restrict users' access to that instrument in REDCap.

Have a process for when project users are leaving: Make sure REDCap access is adjusted (i.e. expired/deleted) when a team member leaves your project group. Before a user is taken off a project, make sure relevant project settings tied to their account are transferred to another user (e.g. API tokens, Automated Survey Invitations).