

Assigning User Rights/Adding Users to a Project: Guidance and Troubleshooting

*** It is solely the responsibility of the project manager, PI or the PI's designee to assign users to their project(s) and give them the appropriate rights/permissions. The REDCap Team **cannot add users** to a project **or change an existing user's permissions** (with the exception of removing them from the project), per the UF IRB and the UF Security & Privacy Office ***

In summary, the **User Rights** page enables you to:

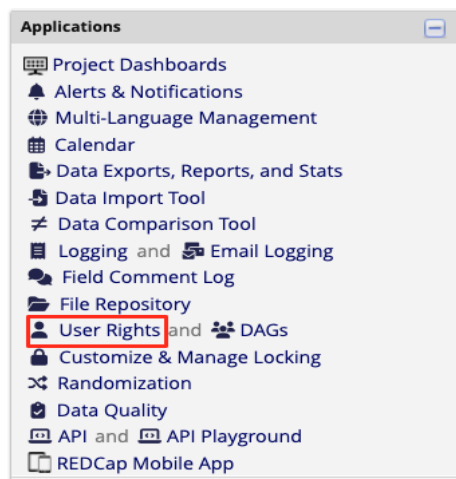
- Add and remove access to your project for other REDCap users, including yourself.
- Control which Applications each user can access for your project.
- Control the record operations that each user is permitted to perform.
 - Create records
 - Rename records (i.e., edit a record ID)
 - Delete records
- Control the level of access each user is permitted to each specific data collection form.
 - No access
 - Read-only access
 - Full edit access
- Define roles – templates of permissions – to which users may be assigned.

In general, users should be given access only to the modules that they require, and no more. This will increase the security of your project and aid usability by removing unnecessary clutter from a user's view.

Tip: There should always be *at least two* users (including yourself) on your project to avoid no one having access to the project due to employee turnover.

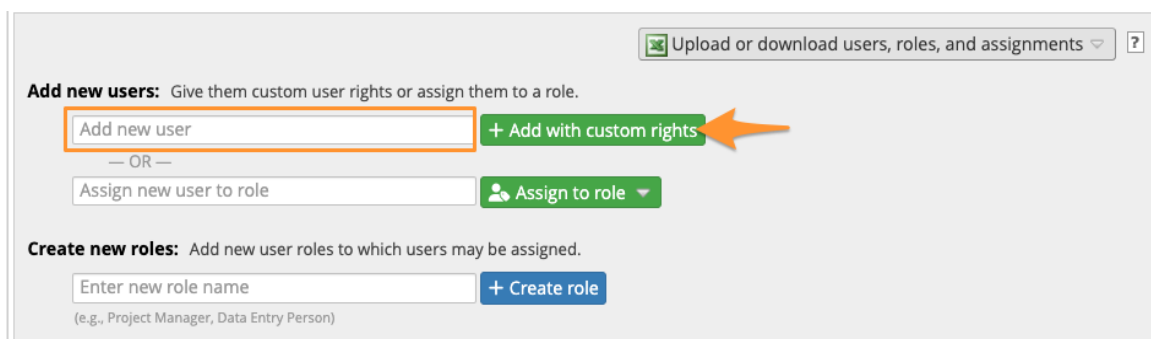
Steps for Adding a New User

Once you are in your project, go to “User Rights” which is listed on the left-hand side bar under the Applications menu.



Note: If you do not see “User Rights” under the Applications menu, then you do not have permission to add users to this project. You’ll need to contact someone on the project who does have this permission.

To add a new user, type their **GatorLink username** (NOT their UF email address or departmental email address) into the “Add new user” box and hit the *Add with custom rights* button.

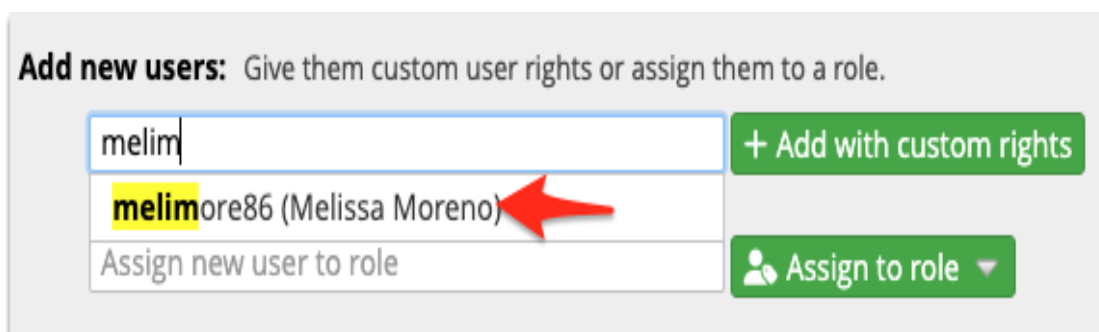


IMPORTANT NOTE: for the user named “John Doe,” if their GatorLink email is john.doe@ufl.edu, their GatorLink username would be **john.doe** (**do not add the @ufl.edu**). Therefore, you would enter **john.doe** into the *Add new user* box.

Correct way: john.doe

Incorrect way: john.doe@ufl.edu

The user’s full name should appear when you type in their GatorLink username. Click on their name to ensure you are adding them to the project correctly. If it doesn’t appear, they either do not have a REDCap account or you are not entering in their correct GatorLink username.



Once you have entered in the new user’s **GatorLink username** and hit the “Add with custom rights” button, another screen will appear that lists all the rights that are available. Now you are ready to assign this user their rights! The *default settings* for each new user are shown below.

You may set the rights for the user below by checking the boxes next to the application tools to which you wish to grant them access. You may also grant them or deny them access to individual data collection instruments, if so desired. To save your selections, click the "Add user" button at the bottom of the page.

Basic Privileges

📅 Expiration Date
(if applicable)

(M/D/Y)

Highest level privileges:

Project Design and Setup

User Rights

Data Access Groups

Other privileges:

Survey Distribution Tools

Alerts & Notifications

Calendar & Scheduling

Add/Edit/Organize Reports
Also allows user to view ALL reports (but not necessarily all data in the reports)

Stats & Charts

Data Import Tool

Data Comparison Tool

Logging

File Repository

Randomization
What is randomization?

Data Quality
What is Data Quality?

API
What is the REDCap API?

Settings pertaining to the REDCap Mobile App:

REDCap Mobile App
What is the REDCap Mobile App?

Allows user to collect data offline in the mobile app

All user can download data for all records to the app?

Settings pertaining to project records:
Explain these settings

Create Records

Rename Records

Delete Records

* Includes ability to delete all data on an instrument or on a repeating event.

Settings pertaining to record locking and E-signatures:

Record Locking Customization

Lock/Unlock Records (instrument level)
Users with locking privileges also have access to the E-signature and Locking Mgmt page on the left-hand Applications menu.
Watch video about locking

Lock/Unlock *Entire* Records (record level)

NOTE: It is important to note that instrument level locking and record level locking are independent features that are governed by separate user privileges (as seen above). You must have explicit permission to either one in order to perform that specific locking action. Also, record locking is a higher-level locking than instrument locking, which means that an entire record may be locked or unlocked while one or more instruments are currently locked, but an instrument cannot be locked or unlocked while the entire record is locked.

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
Informed Consent (survey)	☐	☐	☒	☒	☒	☐	☐	☐
Demographics (survey)	☐	☐	☒	☒	☒	☐	☐	☐
Labs	☐	☐	☒	☐	☒	☐	☐	☐
Concomitant Medications	☐	☐	☒	☐	☒	☐	☐	☐
Imaging	☐	☐	☒	☐	☒	☐	☐	☐
GDS (survey)	☐	☐	☒	☒	☒	☐	☐	☐
GCSI (survey)	☐	☐	☒	☒	☒	☐	☐	☐
PHQ 9	☐	☐	☒	☐	☒	☐	☐	☐
PROMIS Bank v1.0 - Anxiety (survey)	☐	☐	☒	☒	☒	☐	☐	☐
PROMIS Bank v1.1 - Pain Interference (survey)	☐	☐	☒	☒	☒	☐	☐	☐
Charlson Comorbidity Index Scored	☐	☐	☒	☐	☒	☐	☐	☐
PTSD Checklist for DSM-5 (PCL-5) Scored	☐	☐	☒	☐	☐	☐	☐	☒

* De-identified means that all free-form text fields will be removed, as well as any date/time fields and Identifier fields.

Assign user to a Data Access Group

Assign To DAG: [No Assignment] ▼

External Modules: Configuration Permissions

Privileges may be defined regarding whether the user can set or modify the configuration of an External Module that has been enabled on this project. Below are the currently enabled modules. NOTE: Only administrators may modify the module configuration permissions here.

Auto Populate Fields *

Data Driven Project Banner *

Export permission roles and data access group.*

Image Map *

Modify Contact Admin Button *

nedCAPTCHA *

Prevent Past or Future Dates *

Project Ownership *

REDCap Chart Field *

REDCap Entity API *

Survey Participant IP *

Survey UI Tweaks *

*Permissions based on user's Project Design/Setup rights

Summary of Basic User Rights

Expiration Date – Gives user access up until a specified date. Used mostly for temporary employees, such as students performing data entry.

Project Design and Setup – Allows user to design/setup project. Allows user to rename a project. Allows user to make changes to a project. Allows user to delete the project. It is highly recommended that only the highest-level users be given this privilege since editing and deleting a project could cause permanent data loss.

User Rights – Allows user to assign and change user rights for all those assigned to the project, including themselves.

Data Access Groups – Allows user limited access to certain project records by using Data Access Groups, in which only users within a given Data Access Group can access records created by users within that group. This may be useful in the case of a multi-site or multi-group project that requires that groups not be able to access another group's data.

Survey Distribution Tools – Allows user to distribute surveys via links, survey invitations, survey reminders, and create custom survey links.

Alerts & Notifications – Allows user to use the Alerts & Notifications feature to construct alerts and send customized notifications to project users and participants. These notifications may be sent to one or more recipients and can be triggered or scheduled when a form/survey is saved and/or based on conditional logic whenever data is saved or imported.

Calendar & Scheduling – Allows user to view calendar and schedule patients (internally only, not connected to EPIC, etc.) using the scheduling module and the Calendar Application.

Add/Edit/Organize Reports – Allows user to build and save custom reports, which will query the project in real time and display the resulting data in a table format. Allows user to view ALL reports (but not necessarily all data in the reports).

Stats & Charts – Allows user to view all project data in aggregate graphical format and as descriptive statistics.

Data Import Tool – Allows user to import data into a project using the data import template (.CSV).

Data Comparison Tool – Allows user to compare two records currently in the project.

Logging – Allows user to view all project activity (which users have done what) under 'Applications.'

File Repository – Allows user to view and open the files that are stored in the file repository under 'Applications.'

Randomization – The randomization module in REDCap will help you implement a defined randomization model within your project, allowing you to randomize your subjects (i.e., records in your project).

Setup: Allows user to define the randomization model and all its parameters, as well as upload the custom allocation table.

Dashboard: Allows user to access the Allocation Dashboard tab on the Randomization page, in which they may view the overall allocation progress and assignments for subjects that have been randomized.

Randomize: Allows the user to be able to view the Randomize button on the data collection form that contains the randomization field, thus allowing them to perform the randomization on the subject/record you are viewing.

Data Quality - Allows user to execute data quality rules upon project data to check for discrepancies in the data, such as missing values, field validation errors, and outliers.

Create & Edit Rules: Allows user to create/edit Data Quality Rules.

Execute Rules: Allows user to execute existing Data Quality Rules.

API – The REDCap API is an interface that allows external applications to connect to REDCap remotely, and is used for programmatically retrieving or modifying data or settings within REDCap, such as performing automated data imports/exports from a specified REDCap project.

API Export: Allows user to export data via the API.

API Import/Update: Allows user to import and update data via the API

REDCap Mobile App – Allows user to install/initiate the project on their mobile device and to collect data offline in the REDCap mobile app.

Allow user to download data for all records to the app?: Allows user to download existing data for all records to the REDCap Mobile app.

Create Records – Allows user the ability to create new records. If users do not have this privilege, they will not see the option to create new records, but will only be able to access existing records.

Rename Records – Allows user the ability to change record names. If a user attempts to rename a record to a value that matches the name of another record that already exists, they will be prevented from doing so.

Delete Records – Allows user the ability to permanently delete all data for a given record. **Once performed, there is no automatic way to retrieve the data that was deleted. It is highly recommended that only the highest-level users be given this privilege since it causes permanent data loss.**

Record Locking Customization – Allows user to have access to the Record Locking Customization Application, used for customizing the Record Locking option on data collection instruments.

Lock/Unlock Records (instrument level) – Allows user to lock a record's form in the project for an individual subject so no further data can be entered or modified.

Disabled: User cannot lock or unlock records

Locking/Unlocking: User can lock and unlock records

Locking / Unlocking with E-signature authority: **The E-signature feature is not available at UF due to our authentication method (Shibboleth (aka GatorLink)).**

Lock/Unlock *Entire* Records (record level): Allows user to lock all records across the project for an individual subject.

At the bottom of the page are three buttons:

- Save Changes (must be clicked to finish adding user or update existing user rights)
- Cancel: leave page or cancel any changes that were not yet saved.
- Remove User: removes the user from your project.

Summary of Data Entry Rights

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
Informed Consent (survey)	☐	☐	☒	☒	☐	☐	☐	☒
Demographics (survey)	☐	☐	☒	☐	☐	☐	☐	☒
Labs	☐	☐	☒		☐	☐	☐	☒
Concomitant Medications	☐	☐	☒		☐	☐	☐	☒
Imaging	☐	☐	☒		☐	☐	☐	☒
GDS (survey)	☐	☐	☒	☐	☐	☐	☐	☒
GCSI (survey)	☐	☐	☒	☐	☐	☐	☐	☒
PHQ 9	☐	☐	☒		☐	☐	☐	☒
PROMIS Bank v1.0 - Anxiety (survey)	☐	☐	☒	☐	☐	☐	☐	☒
PROMIS Bank v1.1 - Pain Interference (survey)	☐	☐	☒	☐	☐	☐	☐	☒
Charlson Comorbidity Index Scored	☐	☐	☒		☐	☐	☐	☒
PTSD Checklist for DSM-5 (PCL-5) Scored	☐	☐	☒		☐	☐	☐	☒

Data Entry Rights – The Data Entry Rights section allows you to control access to individual forms and surveys. The default setting is that all users will have access to view and edit every form in the project but this can be changed by selecting either “No Access” or “Read Only” for each form.

No Access: User cannot view or edit data on the form at all.

Read Only: User can view the data on the form but cannot change or add data to the form.

View & Edit: User can view and change data to the form.

Edit Survey Responses: User can change/update/delete survey responses.

Summary of Data Export Rights

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
Informed Consent (survey)	☐	☐	☒	☒	☐	☐	☐	☒
Demographics (survey)	☐	☐	☒	☐	☐	☐	☐	☒
Labs	☐	☐	☒		☐	☐	☐	☒
Concomitant Medications	☐	☐	☒		☐	☐	☐	☒
Imaging	☐	☐	☒		☐	☐	☐	☒
GDS (survey)	☐	☐	☒	☐	☐	☐	☐	☒
GCSI (survey)	☐	☐	☒	☐	☐	☐	☐	☒
PHQ 9	☐	☐	☒		☐	☐	☐	☒
PROMIS Bank v1.0 - Anxiety (survey)	☐	☐	☒	☐	☐	☐	☐	☒
PROMIS Bank v1.1 - Pain Interference (survey)	☐	☐	☒	☐	☐	☐	☐	☒
Charlson Comorbidity Index Scored	☐	☐	☒		☐	☐	☐	☒
PTSD Checklist for DSM-5 (PCL-5) Scored	☐	☐	☒		☐	☐	☐	☒

Data Export Rights – The Data Export Rights section allows you to control data export access to individual forms and surveys. The default setting is that all users will have Full Data Set access to download data from every form in the project but this can be changed by selecting either “No Access,” “De-identified,” or “Remove All Identifier Fields” for each form.

No Access: No data exporting can be done.

De-identified: De-identified means that all free-form (non-validated) text fields will be removed, as well as any date/time fields and fields tagged as PHI.

Remove All Identifier Fields: Excludes tagged PHI fields from data export.

Full Data Set: All data can be exported, including PHI, from the project.

Guide for Assigning Individuals Certain Rights (based on roles)

The Project Investigator / Project Owner is responsible for assigning, restricting and maintaining the roles and authorizations for project members to use specific features and functions in REDCap via the application's User Rights module.

Users should be assigned minimum necessary rights and access to protected health information (PHI) based on job requirements.

In addition to the above and specific to projects collecting sensitive data it is the responsibility of the PI/Project Owner to assign only Full Data Export rights for projects with PHI to those individuals trained to protect PHI.

While we can provide general guidelines for granting User Rights, it's important to keep in mind the specifics in your protocol when granting permissions. These lists provide an idea of what would likely be necessary in a typical research project:

PI/Lead Coordinator/Project Owner:

- Project Setup and Design
- User Rights
- Data Access Groups
- Export full data sets
- Add/edit reports
- Manage survey participants
- Logging
- Create/Rename/Delete records
- View/Edit all forms

Other Coordinators/Research Assistants

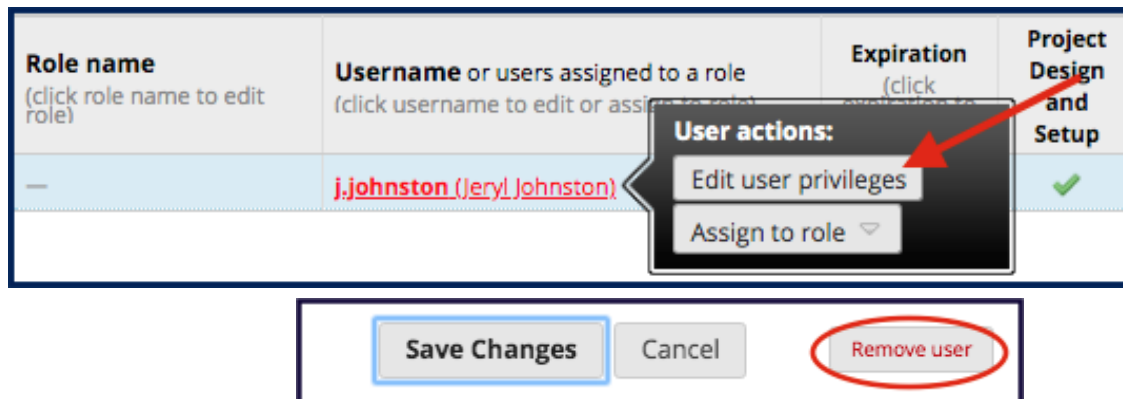
- Add/edit reports
- Manage survey participants
- Logging
- Create records
- View/edit forms as needed

Data Entry Personnel

- Create records
- View/edit forms for which they are entering data

Removing a User from a Project or Role

To remove a user from your project, select their name from the User Rights list and click on Edit User Privileges. You then click on the “Remove User” button:



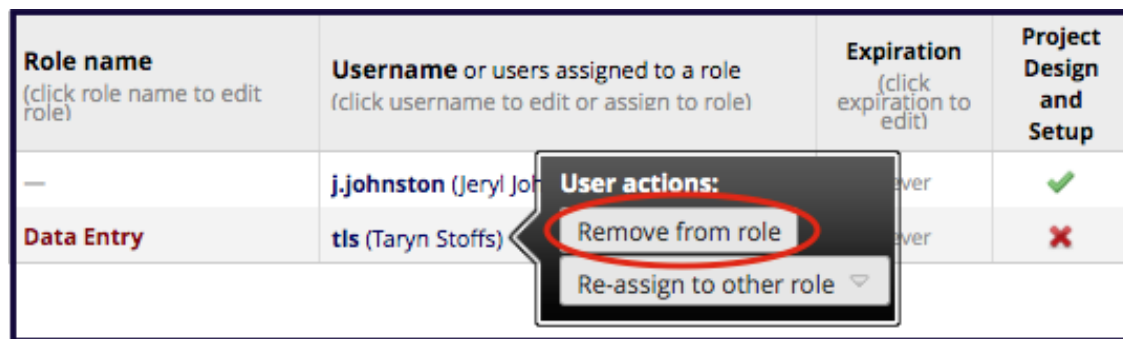
Role name (click role name to edit role)	Username or users assigned to a role (click username to edit or assign to role)	Expiration (click expiration to edit)	Project Design and Setup
—	j.johnston (Jeryl Johnston)	never	✓
Data Entry	tls (Taryn Stoffs)	never	✗

User actions:

- Edit user privileges
- Assign to role

Buttons: Save Changes, Cancel, Remove user

Please note, if you wish to remove a user from your project and that user has been assigned to a role, you must first remove them from the role and then remove them as a user.

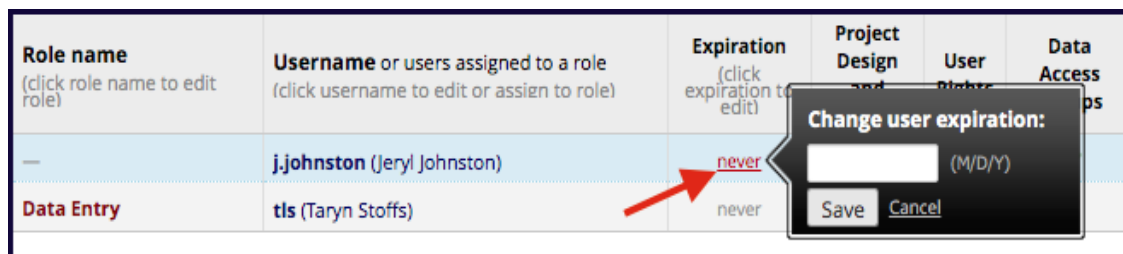


Role name (click role name to edit role)	Username or users assigned to a role (click username to edit or assign to role)	Expiration (click expiration to edit)	Project Design and Setup
—	j.johnston (Jeryl Johnston)	never	✓
Data Entry	tls (Taryn Stoffs)	never	✗

User actions:

- Remove from role
- Re-assign to other role

An alternative to removing the user is to expire them as a user by putting the last date they should have access to the project in the expiration date field of their user rights.



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 to edit)	Project Design and Setup	User Privileges	Data Access
—	j.johnston (Jeryl Johnston)	never	✓		
Data Entry	tls (Taryn Stoffs)	never	✗		

Change user expiration:

Expiration date (M/D/Y):

Buttons: Save, Cancel

Creating a User Role

User roles are useful when you will have several users with the same privileges because they allow you to easily add many users to a role in a much faster manner than setting their user privileges individually. Roles are also a nice way to categorize users within a project.

Creating a role is similar to creating a user with custom rights: enter a name for the role (e.g. “Project Manager”, “Data Entry” etc.) and click “**Create Role**”.

Add new users: Give them custom user rights or assign them to a role.

— OR —

Create new roles: Add new user roles to which users may be assigned.

(e.g., Project Manager, Data Entry Person)

Configure the rights associated with the role and click **“Create role”**. You can now add users to that role.

Adding a New User to a Role

Enter the user’s name or username into the “Assign new user” text box, click **“Assign to role”** and select the role to which the user should be assigned.

Add new users: Give them custom user rights or assign them to a role.

— OR —

☐ Notify user via email?

Create new roles: Add new user roles to which users may be assigned.

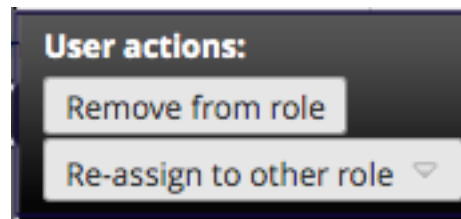
(e.g., Project Manager, Data Entry Person)

Changing a User’s Role

You can change a user’s role (or assign an unassigned user to a role) by clicking on the user’s name, then clicking **“Assign to role”** or **“Re-assign to other role”** and then selecting the role.

Role name (click role name to edit role)	Username or users assigned to a role (click username to edit or assign)	Expiration (click)	Project Design and Setup
—	j.johnston (Jeryl Johnston)		✓
Data Entry	tls (Taryn Stoffs)		✗

User actions:



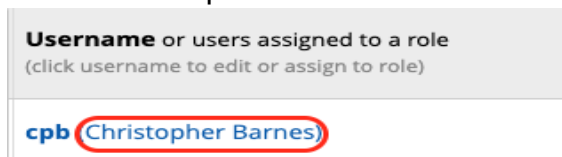
FAQs:

Q: I added a user to my project but when they log in, they do not see the project. Why not?

A: Most likely, they were not added to the project correctly.

Verify you added them with their correct GatorLink username (not by their email address).

- Does their full name appear next to their GatorLink username on the User Rights page (see below)? If not, either that is not their GatorLink username, they do not have a REDCap account and need to register for one, or, if they do have a REDCap account *and* you have verified their GatorLink username is correct, that means their REDCap account is suspended.



- If their REDCap account is suspended, the user should submit a service request at: <https://redcap.ctsi.ufl.edu/redcap/surveys/?s=DUPrXGmx3L> to have the account unsuspended.

Q: I do not see User Rights under the Applications menu. How can I get access to it?

A: If you do not see User Rights under the Applications menu it is because you were not given the user right of “User Rights” when added to the project. You will need to contact someone on the project who has ‘User Rights’ user rights to add this user right for you.

Q: Can I add someone to my project who does not have GatorLink credentials?

A: Yes, if your project has funding. The REDCap team can create what are called “table-based accounts” for any non-UF person who is sponsored by another active (non-suspended) UF REDCap user. In terms of REDCap functionality, these accounts are the same as having a GatorLink account, except the user is using a different authentication method when logging into REDCap.

Each account costs \$32.50 for its creation and then costs \$32.50 every 6 months thereafter (if the account is still active).

To request table-based accounts, please fill out the account creation request survey at:

<https://redcap.ctsi.ufl.edu/redcap/surveys/?s=9XN9RDPALYP7HX7M>

Q: How do I register for a REDCap account so I can be added to a project?

A: Navigate to <https://www.ctsi.ufl.edu/research/study-design-and-analysis/redcap/> and click on the orange “LOG IN OR REGISTER FOR REDCAP” button:



Click on “Log in with Gatorlink” then provide your GatorLink username and password on the GatorLink login page.

Click the image below to login using Gatorlink



Lastly, provide your name and email address for your REDCap account.