Permissions for Jackrabbit Users

Last Modified on 05/27/2024 3:28 pm EDT

User Permissions and **Access Restrictions** allow you to safeguard your data by controlling what a Jackrabbit User can see, and what they can do, in your database.

- Assign permissions to Jackrabbit User IDs based on job function
- Limit a User ID's access so they see only the data related to specific Category1s
- Grant access to your database by Location (if you have **multiple Locations** in your database)

Permissions

When you add a new Jackrabbit User ID, not all User Permissions are granted (checkboxes selected). This allows you to control who can perform sensitive tasks, or see certain areas of your database.

> It is a Best Practice to select one or two Users to be your **System Administrator**(s). Grant those User IDs with ALL permissions and they should be the only ones tasked with creating new User IDs.

User Permissions are managed from within each individual User ID profile. To adjust a user's permissions, go to the **Gear** icon > **Settings** > **Users & Permissions** > **User IDs** (click on a UserID) > **User Permissions** (left menu).

User Permissions are grouped into categories based on the areas of the database they affect. Search fields help you to locate permissions related to the task of the User you are creating/editing.

Check out **Protect Your Account - Guidelines for User Permissions** for a deeper dive into permissions including the identification of permissions related to financial information, the permissions that control areas of caution (sensitive information), and the permissions that should be granted with extreme caution (delete records).

Example

You are creating a new User ID for Dianne Harris. She will be responsible for email correspondence for your organization.

To find all permissions related to emailing in Jackrabbit, enter the keyword "email" in the *Description* search field. Select the checkboxes for the tasks you want this User ID to have permission to do and **Save Changes**.

> A User must log out and log back in again to see new permissions take effect.

Access Restrictions

To manage User access for Locations and Category 1s, go to the**Gear** icon > **Settings** > **Users & Permissions** > **User IDs** (click on a UserID).

User Access-Locations

If your database has multiple Locations, the System Administratorcan limit which Family, Student, and Class information a User can access based on **Location**. ***Note:*** Staff information is not limited by Location.

The Location "ALL LOCATIONS" overrides any other values.

User Access-Category 1

From this area, the *System Administrator* can select which class categories the User can access. This is often used if a User is only allowed to enroll students in specific types of classes.

Select the appropriate settings and**Save Changes**.