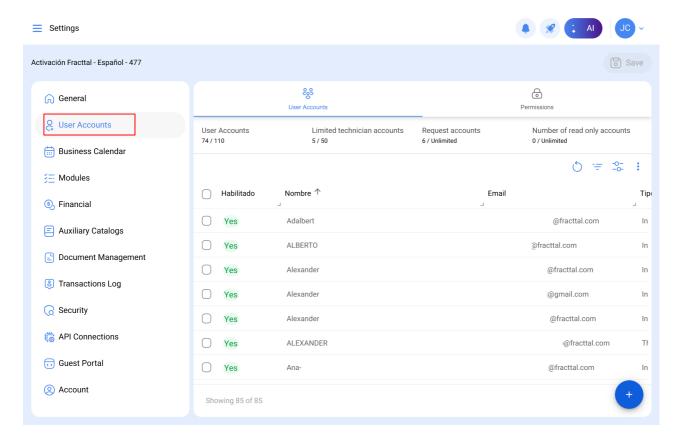
How to customize access in Fracttal One according to your team's roles?

help.fracttal.com/hc/en-us/articles/38097602058765-How-to-customize-access-in-Fracttal-One-according-to-your-team-s-roles

In your daily operations, each member of your team has specific responsibilities and tasks. Therefore, it is essential that access to the modules of **Fracttal One** is configured in a personalized way, so that each person can access only the information and tools necessary to perform their job. This way, you optimize security, workflow, and efficiency within your platform.

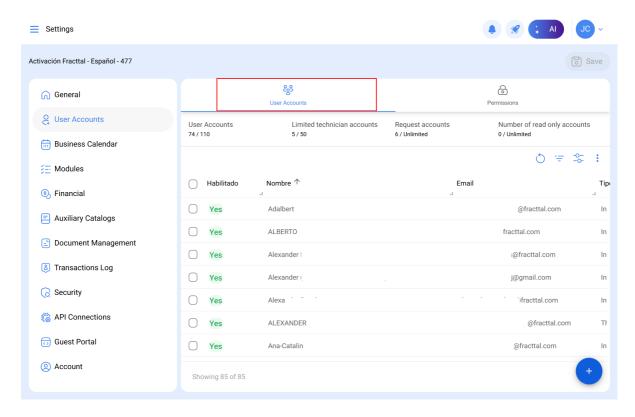


Assignment and customization of permissions

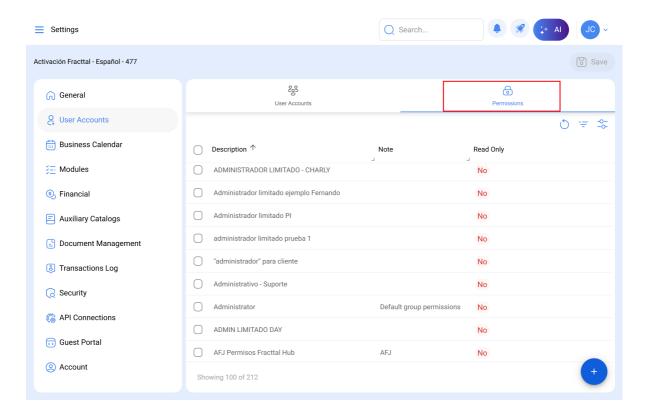
In Fracttal One, access is managed through permission groups that facilitate quick configuration aligned with the team's functions. These groups can be used as they are or adapted according to each user's specific responsibilities.

Steps to configure personalized access

1. **Access the permission settings:** Go to the menu and select *Settings > User Accounts* to view and modify permission groups.

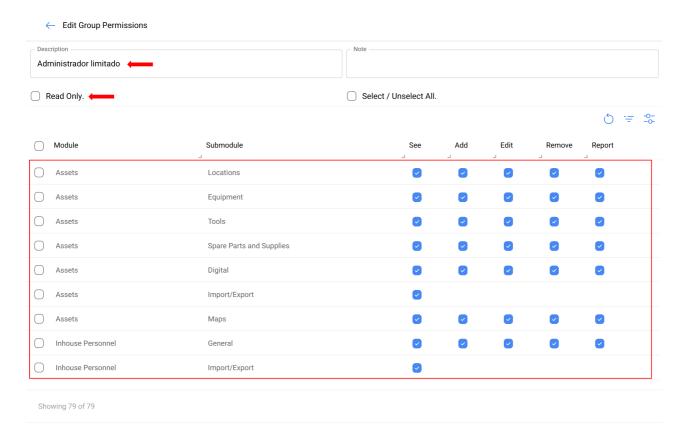


Define the permission group: Assign a permission group based on the user's role or customize the permissions according to the work area and specific responsibilities.



 Customize the accessible modules and submodules: When modifying a group, enable or disable access to modules such as Asset Management, Work Orders, Reports, or User Administration, ensuring that each member sees only what is necessary.

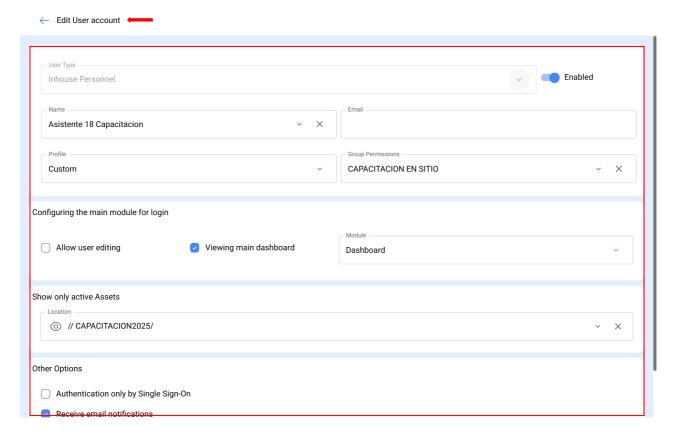
The "**Read-only"** setting ensures that the user has access to relevant information without the risk of making changes, ideal for users who need to monitor processes without intervening in them.



How to individually edit a user account?

By accessing the user's profile from the **User Accounts** module, you can view and modify specific information such as:

- Name, email, and user type.
- Assigned profile and corresponding permission group, with the ability to change it without affecting other users.
- **Main module upon login**, such as the Dashboard, and allow or restrict the option for the user to edit this preference.
- **Visible location**, which allows limiting the visibility of assets to only a specific location if required.
- Additional options, such as enabling access only via SSO, receiving email notifications, or setting up two-step authentication.



Note: For more details on how to manage and customize these permissions, refer to the article: <u>How to add/create permission groups?</u>