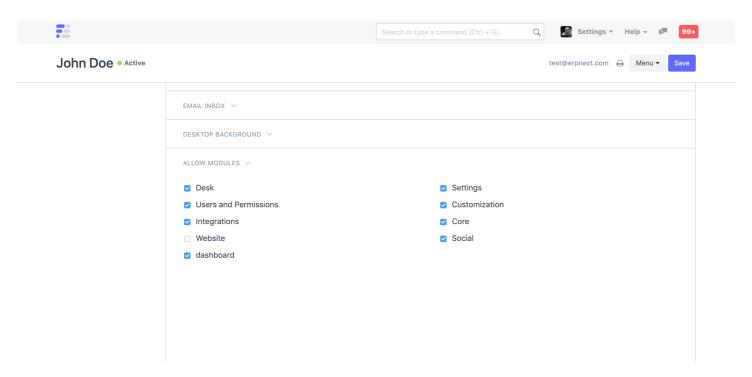
Users and Permissions

- **User and Role**: Each user record represents an authenticated individual with specific roles determining their actions on a DocType.
- **DocType Permissions**: These define what actions a role can perform on a particular DocType. Permissions can be set for actions like reading, writing, creating, deleting, and more.
- **User Permissions**: These are additional rules applied on a per-user basis, allowing for further restrictions on documents based on specific criteria.
- **Automatic Roles**: Some roles, like "Guest," "All," "Administrator," and "Desk User," are automatically assigned based on specific conditions.
- **Restricting Views and Forms**: Frappe allows configuration of visible modules, DocTypes, and views to users, ensuring tailored user experiences.

To configure which modules are shown to a user go to the **Allow Modules** section of the User form.



To hide a doctype from a User, remove the read permission from a Role using the <u>Role Permissions Manager</u>. To control permissions for Pages and Reports, use the **Role Permission for Page and Report** tool.

- **Password Security**: Passwords are hashed and stored securely. Frappe also supports password strength checking and can limit consecutive login attempts for enhanced security.
- **Third Party Authentication**: Integration with third-party login providers, such as Google and Facebook, is facilitated through Social Login Keys.

Key Insights:

- 1. **Granular Permissions**: Frappe's permission system is detailed, allowing for precise control over user actions and data
- 2. Dynamic Role Assignment: Roles can be automatically assigned, simplifying user management.
- 3. **Enhanced Security**: With features like password hashing, strength checking, and third-party authentication, Frappe ensures user data and access remain secure.