User and Team Permissions – Last Updated May 2025

Record owners and Teams control which users are allowed to see each record. The permission mechanism controls the ways in which users are allowed to create, modify, and delete them.

A user has two sets of permissions:

1. **User Permissions**: Control the ability to perform operations that impact the entire database, including the ability to control if a user can delete records that *are not their own.*
2. **Team Permissions**: Control the ability to operate on records which belong to a specific team. Each user can have a different set of permissions in each team they belong to. This makes it possible for groups of people working together on shared data to define their own working policies.

Skip to User Permissions

Skip to Team Permissions

User Permissions

User administrator: An administrator can control access to RealNex CRM by creating accounts for other users and controlling their user permissions. A User administrator is also the only permission that allows for changing any users' permissions for team "**- <everyone> -**"

Super user: A super user can edit or delete any record in the database, regardless of its owner or team assignment. **Use this permission sparingly, if at all.**

Change Record Owners: A user with this permission can reassign ownership of any record to a different user.

Edit Field Definitions: This permission allows a user to change the field captions, edit number field formatting, and various other database field properties.

Edit Pop-up Tables: This permission allows a user to edit the pop-up tables (drop down lists) associated with text fields.

Edit System Tables: Allows a user to modify various database-wide tables, such as: the list of Event types for Event and History records; the list of Property Types; Project Types and Statuses, etc.

Import Data: Allows a user to import data from an external data source by using a spreadsheet file. Restricting access to this feature lets an administrator protect the database against careless additions of useless or poorly structured data.

Export Data: Allows a user to export data to external programs or data files. Restricting access to this feature lets an administrator safeguard an organization's proprietary data.

Create teams: This permission allows a user to create and administer his or her own teams.

Delete Contacts/Companies; Delete Properties; Delete Events; etc.: Allows a user to delete records from the database. These permissions are intended to protect against accidental data loss through careless use of the "delete" feature. **Note: These permissions ONLY control if a user can delete data that they are not the owner of. There are no Delete permissions that prevent a user from deleting their own data.**

Backup database: This permission grants the user the right to use the File | Backup menu in CRM to make backups of the database.

Global replace: This permission gives the user access to the global replace menu. This gives them the ability to mass update fields in CRM. Once you replace a field in CRM there is no way to undo that change. This permission should be disabled for most users of your database.

Synchronize with Outlook/Gmail: This person will be able to sync information between Outlook/Gmail and RealNex CRM.

Allow setting team - <everyone> -: This permission gives the user the ability to add records to the "- <everyone> -" team, granting access to everyone within the company.

Delete layouts: This permission grants the user the ability to delete layouts, regardless of who is the Layout owner. **Users are able to delete Layouts that they themselves create.**

Manage layouts: This permission grants the user the ability to manage the visibility of any Layout and assign Layouts as company-default. **Only users in a database administrator role should have this permission enabled.**

Team Permissions

A team owner or administrator can set these permissions for other users that belong to that team.

Only a User administrator can set these permissions for users in the ”**- <everyone> -**“ team.

Individual Team permissions are under the Teams Membership tab.

Team administrator: Different from the "User administrator" permission, a team administrator can control which users are members of the team and set their permissions. The owner of a team can always act as an administrator.

Add Contacts/Companies; Add Properties; Add Events; etc.: Allow a user to add records to the team's data set. Adding a record can mean either creating a new record or reassigning one from a different team. To reassign a record, the user must also have permission to edit it (either by being the record owner or by having edit permission in its old team).

Edit Other Users' Contacts/Companies; Edit Other Users’ Properties; etc.: Controls whether a user can edit records that belong to the team, but which they do not own.

Delete Other Users’ Contacts/Companies; Delete Other Users’ Properties; etc.: Controls whether a user can delete records that belong to the team, but which they do not own.

Export Others’ Records: Controls whether a user can export data that belongs to the team, but which they do not own.

Merge Others’ Records: Controls whether a user can merge records that belong to the team, but which they do not own.