Groups

Group membership defines the access permissions each user has within Agiloft. For example, groups define which records a user may view, edit, or delete, and which fields within the record the user may view or edit. Strategic group configuration is essential to efficient permissions management.

Users can belong to many groups and enjoy the combined permissions of all the groups that they belong to. With this in mind, there are two possible strategies for group permissions: using groups as permission layers, which are combined to give appropriate permissions; or creating self-sufficient groups, so each user might be a member of just one group that contains all the permissions they need.

	Layer Groups	**Self-sufficient Groups**
Pros	Easier maintenance, where you can edit just one group to modify all users' permissions	Easier troubleshooting, where each user is in just one or two groups for you to check
Cons	Harder to troubleshoot, with many groups to check for issues	Harder to maintain, with many groups to modify to control overall permissions

Groups are designated as either End User or Power User, often called a staff user. The type of group determines which license type is required. End User groups cannot access the Power User Interface or edit records created by other users. By placing users who only need to create, or submit, records and use the FAQ only in an End User group, you limit their access and reduce licensing costs. Power Users use an individual named or floating license and can access either interface and can perform all functions permitted to them. If a user is a member of both End User and Power User groups, the system logs the user in as a Power User with the associated access and license usage.

Configuration Tips

- Every knowledgebase comes with several predefined groups. You can modify or delete them as needed, and you can create an unlimited number of new groups.
    - If you aren't sure whether a group is being used, you can add a z to the front of the label to move the group to the bottom of the list. If you use this method, you can filter the Group field in the People table to show only groups whose Group Name does not contain z.
    - Generally, you should not delete predefined groups with admin, guest, or anonymous in the name.
- It can be useful to create groups as early as possible in the process so the groups can be referenced in other configurations, such as restricting a group from editing a field when some specified condition is true. This saves time that would be spent later going back and adding these restrictions.
- Field permissions are controlled in the field directly and in group permissions. You can use either option, but sometimes one is preferable:
    - If you're already working in a table, or if you're updating permissions in many groups for one field, it's usually easier to edit permissions in the field.

    - If you're setting up a lot of fields with the same base permissions, you can set up a few fields just for that purpose. For example, create a field named `...PermSettings_General` with the permissions you use most often. The `...` keeps the field at the top of the selection list.
- Take advantage of the ability to copy permissions from another group. This can make permission management much simpler.
- It's usually best to keep Power Users and End Users in separate groups because they have different roles and access the system through different interfaces.

Group Permissions

Group permissions control access to:

- Saved searches
- Tables and records
- Views and reports

You can modify the permissions for each group in the Group Permissions wizard.

Configuring permissions for a new group can be time consuming, due to the fine level of access control offered by Agiloft. To simplify this process, copy an existing group with permissions similar to those you need for the new group, and then modify the copy to suit the new requirements. Groups are only used for access permissions. If users share a common function and need to be notified or assigned to issues collectively, they are placed in the same Teams.

Printing Group Permissions

You may wish to print a group's permissions as either a hard copy or to a file to get a sense of what tables are active for each group. This allows you to quickly scan the existing settings for each table, and saves you the trouble of clicking through the wizard. When the groups are customized and finalized, you can store these files and have them act as a reference for the system's permissions.

In **Setup > Access > Manage Groups,** hover over the printer icon and select one of the reports:

- Groups permissions comparison report: This report can be used to review a detailed historical log of permission changes, or to compare several groups in detail, point by point. This report can take a long time if many groups are selected.
- Summary Permissions as CSV: This report shows every table and group in the system, with the access level summary for each combination. For example, you can check the Approval table and see the Contract Creator group has Read All permission, while the Contract Manager group might have Create/Read All /Update All permissions. This report offers only a summary of the permission level, rather than a detailed, point-by-point analysis, and is a quicker and less detailed alternative to a Groups permissions comparison report.

These options allow printing of permissions or a history log of changes. You can also print a comparison report that shows differences between selected groups.

