

Creating New Groups

This topic describes how to create a new group with the [Group Permissions wizard](#). The default groups are often sufficient, but if you need to make extensive changes to permissions, you can also create your own groups.




Best Practice Tip

If you're creating multiple groups, start with the group that you think will have the most common permissions. Once you've created the group and set the permissions, you can then copy those permissions to your other groups. For more information, see [Copying Group Permissions](#).

Set General Permissions

General group permissions are configured in the General tab of the Group Permissions wizard.

1. Click the **Setup** gear in the top-right corner, go to **Access > Manage Groups**, and click New. The Group Permissions wizard opens.
2. On the General tab, enter a group name and description.
3. Select whether the group is a Power User or End User group.
4. Select from the following options to configure the basic group permissions, some of which are only available to Power User groups:
 - a. Select whether group members can reset their password with the Allow Sending Password option. If it's set to Yes, members can be sent a new password by clicking Lost Password on the login page.
 - b. Select whether the user can modify their own or all users' left pane, chart collections, dashboards, widgets, and combined reports.
 - c. Choose the type of administrative access for the group:
 - i. No Administrative Access.
 - ii. Table administrative access for selected tables. This provides access to the setup menu of specific tables.
 - iii. System administrative access to the full Setup menu. Groups who have access to the full Setup menu can also alter group permissions, so only admins typically have this access.
 - d. Select whether the group can export the knowledgebase by using **Setup > Export**.
 - e. Select whether the group can access the Messaging wizard, the full team wizard, and the Communications tab in the left pane.
 - f. Select a saved search, edit a search, or create a new saved search to limit the view of the Communications tab for the group.
5. Click Finish to save your basic group permissions, or click the Tables tab and proceed to section below to set group permissions for specific tables.

 The History tab in the Group Permissions wizard keeps a record of all changes made to the group's permissions. This is an essential feature when using Agiloft for applications that require complete audit histories for compliance, such as in governmental systems. It is also useful when multiple administrators may be editing the system so that other administrators can track any changes that have been made.

You can remove all history entries by clicking Truncate History. This is usually not necessary, but it may be helpful if you have completely redesigned a group's permissions and want to start with a new history.

Set Table Permissions

Table permissions for a group are set individually by clicking the Edit icon next to a table in the Tables tab of the Group Permissions wizard. In a number of cases, you can set the same table permissions in both the Table Permissions wizard and the [Table wizard](#).

 Table permissions are saved individually, independent of changes made in the overall wizard.

1. Go to **Setup > Access > Manage Groups** and edit the group for which you want to set table permissions.
2. Click the Tables tab.
3. Click the Edit icon next to the desired table.

Set General Table Permissions

General table permissions are set on the General tab of the Table Permissions wizard. You can control the most basic table permissions here: whether the group has access to the table at all, whether the table appears in the navigation menu, and, if applicable, whether these changes apply to subtables

1. Select whether the group members have access to the table.
2. Select whether the group members see the table on the toolbar, also known as the left pane.


 In most cases, you can allow access to the table and use the "Show table on the Toolbar?" option to control whether users can open the table and work with its records. Set the "Show table" option to No to hide the table on the user's navigation menu, even if the navigation menu is configured to include the table. This makes it easy to use a shared navigation menu while still controlling which tables appear for different user groups.

Table Permissions and Security

Security is built into the core of the system and enforced consistently. Users who do not have access to a table cannot see records and data from that table. This seems obvious, but it can have important implications for tables and permissions.

Example

Consider the Assigned Team field in the Service Requests table. This field is displayed as a drop-down list containing each team name, and it's linked to the Team Name field in the Teams table. Users will not be able to choose a team from the drop-down list or even view the list at all unless they belong to a group with access to the Teams table. That is, they must be granted access to the Teams table and have view permission to the table's records and the Team Name field.

However, if the Assigned Team field in the Service Requests table already has a value selected, the user will be able to see the value if they have view permission to that field, even if they don't have access to the Teams table. They just won't be able to interact with the field by choosing a new value.

This is also an example of a situation when you might want to give a group access to a table but not show the table on the toolbar.

Set Menu Permissions

Menu permissions for a table are set individually by navigating to the Menu tab in the Table Permissions wizard. This tab allows you to specify group permissions for menu items like views and saved searches

1. Click the Menu Permissions tab.
2. Select whether group members can create, edit, and delete saved searches. If permission is not allowed, users can still search, but the ability to save a search is disabled.
3. Set the view options:
 - a. Select whether group members can create, edit, and delete views.
 - b. Select whether group members can publish views and whether they can add Quick Edit fields to their views. These options are unavailable if group members do not have permission to create, edit, and delete views.

☐ Allow publishing Views

☒ Allow members of this group to add editable fields to views they create or edit (Quick Edit).

Settings for publishing views and adding Quick Edit

4. Set the email and SMS options:

- a. Select whether group members can send emails and create, edit, and delete email templates
 - b. Select whether group members can view and send email templates, and whether they can publish email templates. Note that if your system has a dedicated Email Templates table, group members usually require access to that table as well, in order to use email templates.
 - c. Select whether group members can send SMS messages and create, edit, and delete SMS templates
 - d. Select whether group members can view and send SMS templates, and whether they can publish SMS templates.
5. Set the report options, which are only available for Power User groups:
- a. Select whether group members can create, edit, and delete reports.
 - b. Select whether group members can access all reports or only published reports, and whether they can publish reports themselves.
- For more information on publishing reports for general viewing, see [Reports wizard](#).
6. Set the print template options:
- a. Select whether group members can create, edit, and delete print templates.
 - b. Select whether group members can access all print templates or only published templates, and whether they can publish print templates themselves.

✔ In general, if a group can see the toolbar tab and edit other people's records, they should also be able to create, edit, and delete their own saved searches, views, and reports.

Set Record Permissions

Record-level access permissions control which records in a table group members can view, edit, or delete. Note that record ownership is displayed at the top of the screen. Keep this in mind when you set record- and field-level permissions because it can impact how you set a group's permissions.

For instance, if ownership is based on a match of the Company field, but a group should only have permission to edit their own personal records, you will have to create a filter for the Edit Own permission to find only record's created by the currently logged in user.

✔ Setting record-level permissions with the Table Permissions Wizard is best suited for defining permissions that a particular group has for multiple tables. If you want to set record-level permissions that multiple groups have for a particular table, you can use the [Table Wizard](#) to set which groups can view, edit, and delete records in that table.

1. Click the Record Permissions tab.
2. Select whether group members can create records in the table.
 - a. Choose whether they can import multiple records.

- b. Choose whether they can copy records.

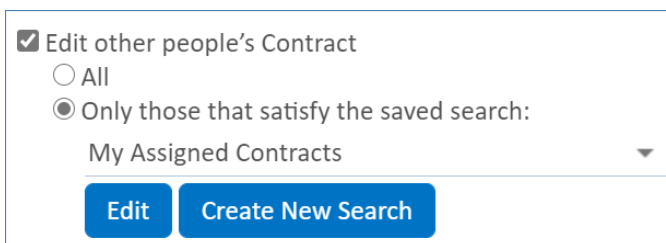


Allow this group to

- ☒ Create Contracts
 - ☒ Import multiple Contracts from a file
- ☒ Copy Contracts

Allow this group to... settings

3. Select whether group members can edit records that they own, that other people own, or both. In either case, you can let them edit all records or limit the records to a saved search. For example, you might allow users to edit only Contract records that are assigned to them, or edit only Company records for companies they belong to.



☒ Edit other people's Contract


☐ All

☒ Only those that satisfy the saved search:

My Assigned Contracts

Edit Create New Search


Edit other people's records

 For a user to edit a record, they must first have view permission for that record. Even if the edit permission options are selected, users won't be able to edit records if they can't view them.

4. Set other permissions related to record editing, selecting whether group members can:
- Mass edit multiple records.
 - Quick edit records from the table view.
 - Link multiple records using the Link menu on the action bar.
 - Print records using the Printer icon.
5. Select whether group members can delete records that they own, that other people own, or both. You can let them delete any records or limit the records to a saved search.
- If you allow group members to delete records, choose whether they can mass delete multiple records.
6. Select whether group members can view records that they own, that other people own, or both. You can let them view any records or limit the records to a saved search.
7. Select whether group members can view FAQs for the records, and whether their viewing is limited by a saved search.
8. Set other permissions related to viewing records, selecting whether group members can:
- Export multiple records.
 - See the Conversion button on the action bar.
 - Interact with conversion rules. This defines whether a conversion action that is supposed to bring up the new record screen will actually do that. If the permission is not granted, and a user in this group runs a conversion action, it will just run in the background and create the record without showing it to the user.

Record Permissions Summary


The options selected on the Record Permissions tab are displayed in Record Permissions column on the Tables tab of the Group Permissions wizard. The permissions are grouped into one line each and are separated by commas. For instance, View Own: All means that the All checkbox was selected. View Own: SS means that the Saved Search checkbox was selected.

<input type="checkbox"/> Edit	Table ↑	Access	Left Pane	Record Permissions
<input type="checkbox"/> 	Contract	Yes	Yes	Ownership: Requester ID matches Person.ID Create, Import, Export, Copy View Own: All, View Others: All Edit Own: All, Edit Others: All, Mass Edit, Quick Edit Delete Own: All, Delete Others: All


If the permission has not been selected, it will not appear in the list. This allows you to scan the table view to see what permissions have been granted without having to read through all the permissions.

Set Field Permissions

Field-level access permissions are only relevant for tables that group members are allowed to view or edit. They control which fields the user can view or edit in records the user can access, which are broken down by fields in records that they own and records that other people own. This enables you to set a very granular level of permission for the table for each group.

-  Setting field-level permissions with the Table Permissions Wizard is best suited for defining permissions that a particular group has for multiple fields. If you want to set field-level permissions that multiple groups have for a particular field, you can use the [Table wizard](#) to set how groups can interact with that field.

1. Click the Field Permissions tab.
2. For each field in the table, select whether group members can:
 - a. View Own: view the field in records that they own.
 - b. Create: set the field value when creating new records.

-  Never give Create permission for the Communications or History fields. No one should be creating an email or altering the history when creating a record.

- c. Edit Own: edit the field in records that they own.
- d. View Other: view the field in records that other people own.

e. Edit Other: edit the field in records that other people own.

Field	View own <input type="checkbox"/>	Create <input type="checkbox"/>	Edit own <input type="checkbox"/>	View other <input type="checkbox"/>	Edit other <input type="checkbox"/>
Company Contact Entry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Company Documents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Company ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Company Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Primary Location ID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Local field per
are set indep

For linked fie
create and
permissions c
the primary lir
while view per
can be set inde

3. Click Finish.

Field Permissions Strategy

It can often be difficult to determine the best field-level permissions to set for each group. There may be specific fields that you know only certain groups should be able to edit—for instance, the publication fields for FAQs—but otherwise, you'll often have to make your best guess which groups should see which fields based on what you know about the use cases.

If you have to guess, use the following general guideline: anyone who can edit a record as a power user should probably have only View Own and View Other permission for all automatically generated fields, and they should have Create, View Other, Edit Own, and Edit Other permission for all other user-entered fields. The ID field is an exception to this guideline. The field is automatically generated, but it's useful to always give Create permission so that people can see it when creating records.

Make sure to also keep field-level permissions clean, even when it is more work:


Example


If a group doesn't have record-level create and edit permissions for the Contracts table, it actually makes no difference if the Create Own and Edit Own field-level permissions are selected for every field in the table, because group members won't be able to edit any contract records at all. However, leaving the field-level permissions this way imply an ability to edit fields, but the record-level permissions would contradict them.

Instead, make permissions consistent. Clear all field-level permissions for the Create, Edit Own, and Edit Other permissions for the Contracts table. Otherwise, someone may accidentally turn on record-level edit permissions, and suddenly users in the group will be able to edit fields for which they shouldn't have permission.

Field Permissions and Related Tables

Field permissions are especially important when using **Related Tables**. In many cases, you may want to prevent certain groups from adding or removing records from a Related Table. To do so, remove a group's Edit permissions for the fields in the linked set in the source table. This prevents the Lookup icon from working to link new records, and it automatically removes the Unlink button from the Related Table's action bar.

 Consider a Related Table of Support Cases contained in a Company record. To prevent a group from adding or removing records from the Related Table, remove the Edit permissions in the Support Cases table for all the fields included in the linked set to the Company table.

 Another way to prevent users from unlinking records in a Related Table is to navigate to the **Permissions** tab of the Field wizard for the Related Table and deselect the option that allows users to unlink records.