

# Overview of User Groups

Last Modified on 08/02/2023 11:29 pm EDT

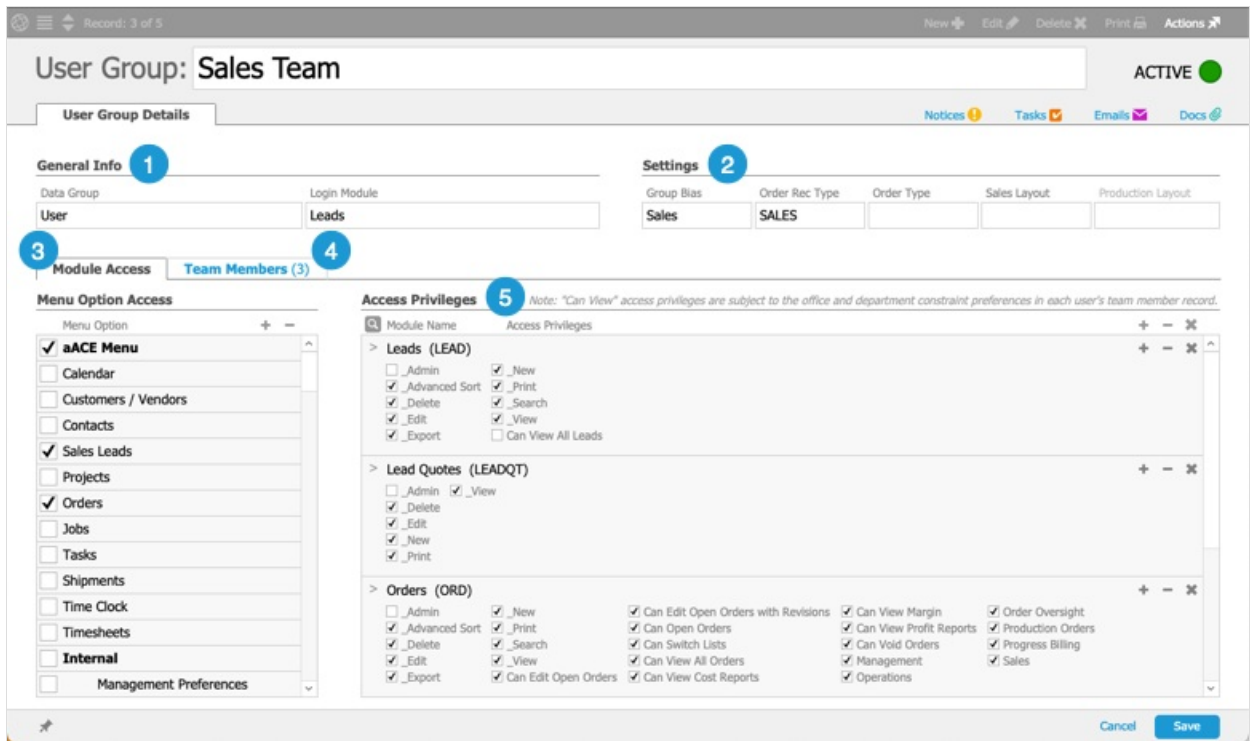
This guide explains aACE functionality used to maintain security and manage privileges. It is intended for system administrators.

aACE uses a security model where users are assigned to groups with varying privileges. The primary function of the user group is to define what the interface will allow (e.g. menu options, allowed activities, etc) for the team members in that group.

System administrators can manage user groups: Main Menu > System Admin > User Groups. After you update settings for a user group, changes will take effect the next time those team members login. When you update the user group you belong to, aACE displays a prompt asking whether you want to implement the changes immediately or the next time you login.

## Sections of the User Groups Module

Read below for information on each numbered section of the User Groups module:



### 1. General Info

You are able to edit the type of group your user group is as well as the login module:

- **Data Group** – Specifies the general data access for a group
- **Login Module** – Specifies the module that aACE will display when members of this group log in

## 2. Settings

You can customize various settings for your particular user group:

- **Group Bias** – Controls which columns display on various layouts.  
You can specify whether these team members will initially see the Operations View, Management View, or Sales View. Each view highlights details most important to that focus. Team members can change the view using the dropdown list in the center of the Orders header.
- **Order Rec Type** – Sets the default record type used when this group creates an order. This group-specific setting takes precedence over the system-wide default located in Internal > Management Preferences > Order Entry. (Note: Even if you specify an order record type here, the Management Preference to allow multiple order record types will still allow users to select the type of order they create.)
- **Order Type** – Notes the purpose of the order.  
You can create custom options by clicking "Edit..." in the dropdown menu (e.g. inventory replenishment).
- **Sales Layout** – Sets the [layout for sales orders](https://aace6.knowledgeowl.com/help/configuring-order-layouts#SalesOrderLayouts).  
Each layout displays slightly different fields to assist with a different focus.
- **Production Layout** – Sets the [layout for production orders](https://aace6.knowledgeowl.com/help/configuring-order-layouts#ProductionOrderLayouts).

## 3. Menu Option Access

You can specify how the aACE menu will appear for this user group. Scroll down the list and mark or clear flags as needed.

This panel combines with Access Privileges (see below) for full functionality. If users have a certain menu option visible, but no privileges set for that module, the system will return an error message when they click the menu option.

## 4. Team Members

Specifies which [existing team members](https://aace6.knowledgeowl.com/help/viewing-team-members-by-office) will be included in the group. Each team member can be in only one user group at a time. If you add team members to a new group, aACE automatically removes them from their previous group.


Note: You can quickly identify team members not included in a user group by using the Team Member module, sorted by user group.

### User Flag


This flag distinguishes between team members that can directly access your system. Clearing this flag prevents access to your aACE system. Even if the person still has an active team member record, they are unable to log in.

This feature can be helpful for production personnel. These team members can be scheduled and assigned to work on tasks tracked in aACE, but they might not need to log in and use aACE. Often, they work with one of the aACE mobile apps (e.g. the Pick app).

### Line-level Actions

Clicking the line-level Actions icon (  ) for a team member displays several options. You can click Reset Password to revert that team member's account back to the [default password you have set](https://aace6.knowledgeowl.com/help/working-with-the-aace-default-password). You can also view logs of past changes related to the team member. If needed, you can remove them from the current user group.

## 5. Access Privileges

Specifies what the members of this user group can do with the records in each module. Click the Search icon (  ) to add / remove modules in this list, then mark or clear the flags for the appropriate privileges.

This panel combines with Menu Option Access (see above) and individual team member privileges for full functionality. Users must have menu options to access modules and their own records. Some users may need to access additional records from other offices and departments.

Note: You can further refine access privileges by navigating to an individual [team member record](https://aace6.knowledgeowl.com/help/controlling-access-to-aace-modules-with-user-groups#ControllingVisibility). Options there

allow you to control whether the team member can edit logs, view or switch to other offices, and view departments outside their assignment.

## Best Practices for Creating User Groups

When aACE is implemented, only the Programmer and System Admin groups are created. The system administrator [creates the other user groups](http://aace6.knowledgeowl.com/help/controlling-user-access-to-aace-modules) (<http://aace6.knowledgeowl.com/help/controlling-user-access-to-aace-modules>) as needed. These two groups are the closest aACE has to pre-defined user group templates. They can serve as a starting point for creating the other groups.

To create a new group, we recommend duplicating an existing group with more privileges, then removing the privileges that are *not* needed by the new group. Often this can start with the System Admin group, which has full system access. Then you can duplicate these 'second-generation' user groups to create other groups with access to even fewer areas of the software. This approach reduces the effort needed to create a group, but helps ensure that the system administrator understands which areas of system access they are granting.

When creating new user groups, we also highly recommend creating a test user and adding them to that group. Log in as that user to confirm that access is enabled and restricted as you intended. When you create additional groups, you can move the test user into each one to verify access.

---