

Overview of User Groups

Last Modified on 05/02/2022 10:44 am 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 and those groups are granted 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 work with user groups: navigate to 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:

The screenshot shows the 'User Group: Sales Team' configuration page. It includes a top navigation bar with 'Record: 3 of 4' and action buttons like 'New', 'Edit', 'Delete', 'Print', and 'Actions'. The main content area is divided into several sections:

- 1. General Info:** Fields for 'Data Group' (User) and 'Login Module' (Leads).
- 2. Settings:** Fields for 'Group Bias' (Sales), 'Order Type' (SALES), 'Sales Layout' (Price-Based), and 'Production Layout'.
- 3. Module Access:** A list of 'Menu Option Access' with checkboxes for various modules like aACE Menu, Customers / Vendors, Contacts, Sales Leads, Projects, Orders, Jobs, Tasks, Shipments, and Time Clock.
- 4. Access Privileges:** A table showing 'Access Privileges' for 'Leads (LEAD)' and 'Orders (ORD)' modules, with columns for 'Module Name' and 'Access Privileges'.
- 5. Team Members:** A tab labeled 'Team Members'.
- 6. Preferences:** A section with checkboxes for 'Can edit logs', 'Can switch offices', 'Can view all offices', and 'Can view all departments'.

1. General Info

Data Group – This drop-down list controls the overall data access for a group.

Login Module – This module will automatically display when members of this group login. The setting is also noted on the User Groups list view as the Default View.

2. Settings

Group Bias – This drop-down list controls which columns display on various layouts depending on the users' role.

Order Type – This drop-down list sets the default record type used when this group creates an order. This setting takes precedence over the system-wide default order type (located in System Admin > Preferences > Order Entry). However, the system preference to allow multiple order record types takes precedence over this setting, allowing users to select between Sales and Production when they create orders.


Sales Layout / Production Layout – These drop-down lists control which fields are shown and where they're placed on the Orders detail view for each order type.

3. Menu Option Access

Specifies how the aACE menu will appear for this user group. Scroll down the list and mark/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, when they click that menu item the system will return an error message.

4. 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 Preferences (see below) for full functionality. Users must have menu options to access modules and their own records. Likewise, users may need to access additional records from other offices and departments.


Understanding "Negative" Privileges

Each user group privilege grants additional functionality. This functionality may involve removing a default constraint, so the privilege is phrased as a negative. As examples, the Companies module includes the privilege of "No Restricted Access Constraint" and other modules include a privilege phrased as "No my<Record> Constraint". This second privilege applies separately to transactions such as leads, orders, shipments, invoices, projects, jobs, tasks, purchase orders, purchases, etc.

Marking these flags will remove the constraint. It grants the privilege for group members to [view or manage additional records](https://aace5.knowledgeowl.com/help/controlling-access-to-transactions-with-user-groups) (i.e. they are *not* constrained to only view "my" records).

5. Team Members

Specifies which [existing team members](https://aace5.knowledgeowl.com/help/viewing-team-members-by-office) will be included in this 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: The User Group list view displays only a single name; this serves as an efficient reminder of what the group is responsible for. The Team Members module can also be useful for sorting by user group and identifying those who are not yet included in a group.

The User flag is an easily visible way to deactivate and activate user accounts. If this flag is cleared, the team member will *not* be able to login. In additions, each team member line includes an Action menu () icon. This control also allows you to activate and deactivate the account, as well as edit credentials and view logs.

6. Preferences

These flags allow you to refine the group's privileges:

- Can edit logs – Enables users to put the [Log Viewer](http://aace5.knowledgeowl.com/help/overview-of-record-logs) into editing mode, where they can modify manually entered comments
- Can switch offices – Enables users to change their office assignment using the [Main Menu footer](http://aace5.knowledgeowl.com/help/the-aace-main-menu#MainMenuFooter)
- Can view all offices – Enables users to view the records linked to *all* offices
When this flag is cleared, users in the group only see records associated with the office specified on their [Team Member records](http://aace5.knowledgeowl.com/help/creating-new-users).
- Can view all departments – Enables users to view the records linked to *every* department in their assigned office

When this flag is cleared, users in the group only see records associated with the department specified on their Team Member records.

To give a user group maximum visibility on system records, mark the flags to view all offices and all departments. To create the most limited view, clear both these flags.

Best Practices for Creating User Groups

When aACE is implemented, only the Programmer and System Admin groups are created. Later on the system administrator [creates the other user groups](#) (<http://aace5.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 *not* needed by the new group. Often this can start with the System Admin group, which has full system access. Then these 'second-generation' user groups can be duplicated and used 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.
