What Are User Roles and Permissions?

Roles

User security roles determine:

- The areas of the application (such as the Contacts menu or Tools menu) that a user can access.
- The tasks (such as adding contacts or running reports) the user can perform.

The five user security roles are: Administrator, Manager, Standard, Restricted, and Browse. Give users the role that lets them access only the functions they need to perform their job.

Permissions allow users with a Standard or Manager role additional access to features and the ability to perform special tasks.

- **Administrator** - Is the highest level role in Act!. Users with this role can access all features, and all records that have public or limited access. Users who are responsible for maintaining the database, ensuring data security, and adding or deleting users, should be Administrators.
- **Manager** - Has access to all features except Manage Users, Delete database, and Password Policy. The Manager role can be expanded by adding or removing permissions for the individual user. Managers have access to all public records. Users who need to Manage Teams, modify database schema, manage records owned by other users, create/edit layouts, import/export data, manage custom activity types, or update product information, should be Managers.
- **Standard** - Represents the typical user. Standard users can access most areas of the application. This role can be expanded by adding or removing permissions for the individual user. Standard users can access public records and their private records. Users who perform a variety of tasks, including creating/modifying word-processing and report templates, but who do not need to modify or maintain the database, should be Standard users.
- **Restricted** – Can access only basic functionality. Restricted users can only access public records and their private records. In addition, users with this role cannot delete any records, even records they own. Typically, Restricted users are assistants, hourly workers, or others requiring only limited access to features.
- **Browse** – Gives users read-only access to information. For example, a Browse user can run reports. Temporary employees and users who only need to reference information should be Browse users.

Permissions

• Permission	Lets the user...
Accounting link tasks	Install and use an Accounting/back-office link (Only applies to accounting/back-office applications that are linked through installing a supported application.
Delete records	Delete contacts, companies, groups, activity series, notes, histories, opportunities, and secondary contacts the user owns.
Emarketing Administration	Send emarketing email campaigns, update email campaign history, view emarketing reports, edit emarketing templates, and run emarketing smart tasks.
Emarketing Web to Lead	Create webforms and get Leads.
Emarketing Send	Removing the permission makes all Send Campaign options unavailable
Export to Excel	Export data in a list view to Excel.
Handheld device sync	Synchronize with handheld devices. Note: This permission is required to use products that provide mobile device data sync capabilities.
Manage sync subscription list	Add contacts to the sync set for a remote database they belong to. Note: This permission is required to use products that provide mobile device data sync capabilities.
Remote administration	Back up, restore, and check and repair, a remote database they belong to. This permission applies to remote databases that are synchronized to a main database. See About Database Synchronization.

Your ability to perform tasks may also be limited by whether or not you are the Record Manager or have access to the records or fields.