

## Wield the power of many users — protection and profitability come hand-in-hand

Application: ACT! 2006/2007



### AT A GLANCE

Busy professionals need to work fast — and few things halt your productivity like an application that's designed for someone else or one that's been tampered with. Creating separate ACT! user accounts for every person who uses ACT! allows you to boost usability with customization and security through user-specific permissions.

To maximize ACT! productivity and security, we'll:

- Describe how separate users provide enhanced usability and security.
- Examine the various user security roles you can apply to a user so you can decide which role to assign each user in your organization.
- Create a new user and apply appropriate permissions so you can speed through the steps yourself.

For all but the most basic ACT! usage — such as in an owner-operated business with only one user — you need separate ACT! user accounts for each person who uses ACT!. Without separate users, every person who accesses the computer on which ACT! is installed must use the database in the same way. Furthermore, they can access all sensitive customer data, even if you don't want them to. Worse: People who have no business in ACT! can delete users, corrupt your layout, and otherwise wreak havoc on your data. Before they have the chance, we'll show you how to configure separate user accounts for every person in your organization.

### Gain personalization

Each user who logs in to ACT! with his user name and password gets his own My Record. A person can use data from his My Record to automatically fill in his return address and signatures on enve-

lopes and letters. Additionally, each user can have his own calendar, program preferences, toolbars, layouts, and more.

### Boost security

Every organization should be concerned with securing their data. With separate user accounts you can control who has access to the ACT! database, and how much access they have. By creating separate ACT! user accounts and applying permissions, you can protect your ACT! installation and database from accidental corruption, and can protect your contacts' personal information from identity thieves.

### Determine user roles

The first time you launch ACT! after installation you must create a user account to continue. ACT! automatically grants that user Administrator rights and creates the My Record. If you have Administrative

privileges you can create additional users in the Manage Users wizard.

During the creation process, you must designate a security role for each new user. You can change these roles later, but you'll save time by initially selecting the security role that best fits the privileges you want each person to have. Let's take a look at each role, from greatest privileges to least, so you can choose roles for your users.

### Administrator

Administrators can perform all tasks in ACT! and can access all the data that isn't private. You can't take away permissions from an Administrator. Specifically, Administrators can:

- Perform database maintenance
- Restore or delete databases
- Create and manage users
- Customize the database
- Run database-wide reports



The on-going challenge of increasing productivity and decreasing inefficiencies can be overwhelming — often leaving business owners wondering where to begin. By Design Solutions helps you put together the pieces of the complex puzzle of accounting and business management systems. We not only help you evaluate and **S**elect the right version of QuickBooks, but help you **I**mplement it, **M**aximize it's use, **P**erform tasks more efficiently, **L**earn through hands on training, and then **E**nlist our help when you need support! It's just that **SIMPLE!** View our website for more information at [www.ByDesignSolutions.com](http://www.ByDesignSolutions.com)

As you can see, it's critical to your database's integrity and your customer's security that you limit the users with this security role. Grant the Administrator role to an IT person in charge of supporting the technical aspects of the ACT! installation and to anyone who must manage the overall operation of ACT!.

**Essential:** Only Administrators can create and modify users, so ACT! should always have at least one user with Administrator rights.

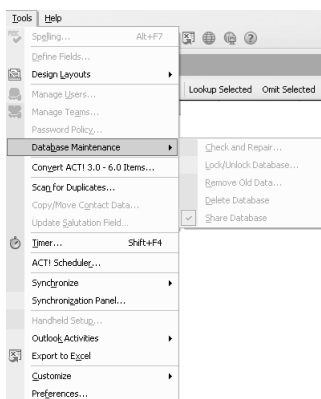
## Manager

You'll grant the Manager role privilege to most managers in your organization whose direct reports use ACT!. Managers can access the entire database, but can't create or manage users or perform database maintenance. Managers can perform the following important tasks:

- Create and manage teams (in ACT! Premium for Workgroups)
- Delete non-private records
- Customize fields and layouts
- Set up synchronization tasks

## Standard

ACT!'s default role for new users is the Standard user role. With this role, users can access most records and data in the database, but can't perform administrative tasks, such as customizing the layout. Standard users can:



**1:** A Standard user will find many disabled options in the Tools menu.

- Create groups, companies and contacts
- Modify templates
- Synchronize data
- Set up automatic syncs and backups
- Customize menus and toolbars (but not layouts)

**Figure 1** demonstrates how ACT! blocks access to certain features by disabling the menu option.

## Restricted

Restricted users can access far fewer features in ACT! than can Standard users. In addition to the features Browse users can use, which we'll outline next, Restricted users can:

- Create contacts, activities and opportunities
- Perform mail merges
- Schedule an Outlook activity sync task with ACT! Scheduler
- Change record access for records they manage

## Browse

People with the Browse role are the most restricted in their access. Browse users can't create records, but they can view data and run and print reports. They can also:

- Perform basic and advanced lookups
- Scan for duplicates

- Print calendars, address books, etc.
- Set user preferences
- Customize the navigation bar and columns
- Back up and restore their own supplemental files
- Check for software updates

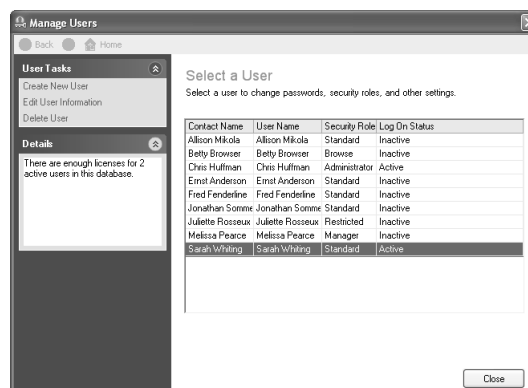
Now that you understand which features each security role grants a user, decide which role best fits each user you must create.

## Create and modify users

As the Administrator, you can create and modify users and assign them permissions. When creating new users, you'll choose to create one from scratch or to create a new user from a contact in your ACT! database.

### To create a new user:

1. Open your ACT! database and log on as a user with Administrator rights.
2. Select Tools | Manage Users to open the Manage Users wizard shown in **Figure 2**.
3. In the Users Tasks task pane, click on the Create New User link.
4. On the Create New User page, select the Create User From Contact or the Create New User option button. Click Next.
5. If you're creating a user from a contact, the Choose Contact page



**2:** Start with the Manage Users wizard to create, modify or delete a user account.

displays, as shown in **Figure 3**. Select the desired contact and click Next.

### To configure a user's user name and permissions:

1. On the Enter User Information page, enter a name in the User Name text box, as shown in **Figure 4**.

**Note:** When you create a user from an existing contact, the User Name does *not* need to match the Contact Name.

2. Select a security role from the Security Role dropdown list.
3. In the Password options section, assign a password by typing it in the New Password and Confirm Password text boxes.
4. If you want the user to create his own password, select the User Must Change Password At Next Log On check box.

**Smart idea:** Users will have an easier time remembering their passwords if they pick them rather than you assigning them. To give them that responsibility and save yourself the effort of creating separate passwords for yourself, use a generic password for new users and configure ACT! to require new users to change their passwords.

5. To prohibit a user from changing his password or to set a password to never expire, select the corresponding check boxes. Click Next.

6. On the Specify Access page, select the Active – Pending Log On option button to activate the user. Click Next.
7. As shown in **Figure 5**, you can add or remove specific permissions depending on the security role you chose for that user. Highlight a permission you want to remove or add and use the left and right arrows to move permissions between the Available Permissions (Optional) and Added Permissions list boxes. Click Next. (In ACT! Standard, click Finish.)
8. On the Add A User To A Team page in ACT! Premium for Workgroups, click the Add button to choose a team or teams. When done, click Finish.

ACT! adds the user to the Select A User page of the wizard. When the person logs in with his user name and password, ACT! will activate the user and require that he change the password, if you selected that option.

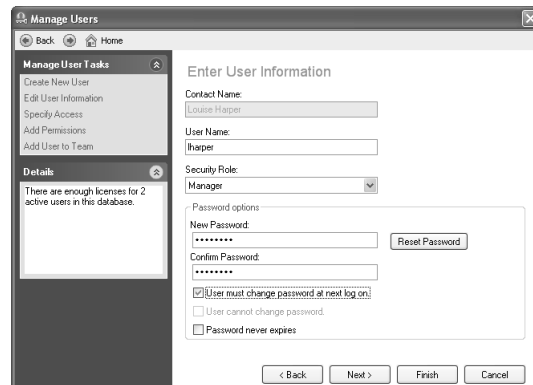
## Modify users

You can modify users later if you determine that you need to change a user's user name, security role, password or permissions. To do so:

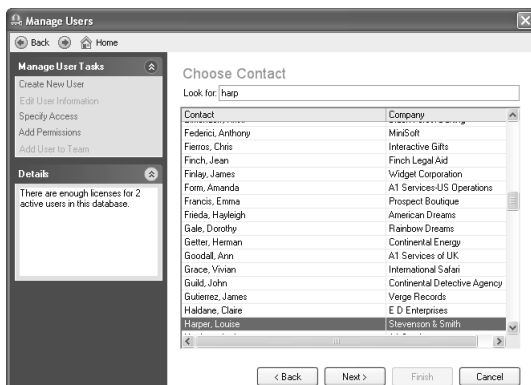
1. Open the Manage Users wizard and select the user you want to modify.
2. Click on the Edit User Information link in the Manage Users task pane to switch to the Edit User Information page of the wizard.
3. Step through the wizard pages or skip to a specific task by clicking on the appropriate link in the Manage User Tasks task pane (e.g., Specify Access).

## Get all the specifics of user permissions

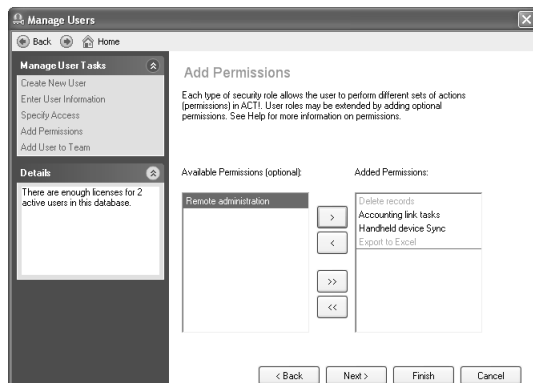
We've provided an overview of the permissions for each user roles in ACT!. Feel free to contact us with any questions you have.



**4:** Enter a user name for your new user and set his role and password options.



**3:** Create a new user from an existing contact to speed up the creation process.



**5:** Some permissions for a role are optional — you choose which of those permissions to grant each user.