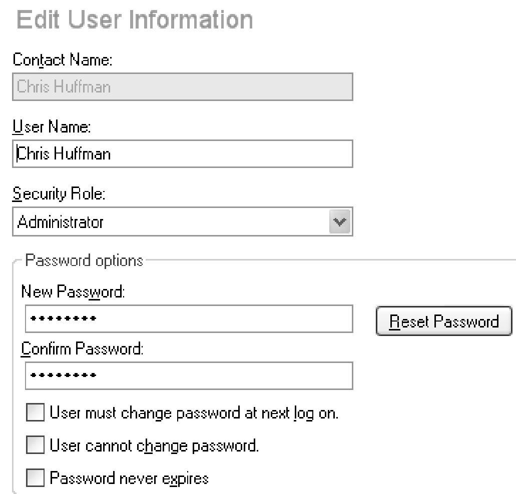
Overriding Password Policy Settings for Individuals

For some users, you may want to override a few of the Password Policies that you have set for individual users.



Those changes are made in the **Tools, Manage Users** dialog box. Select the user and make changes as necessary. For example, **Password never expires** will override the Password Policy of **Password must change every x days**.

Setting a Password for Yourself

You may add a password to your database anytime you decide that you want to password-protect your data.

There are a few ACT! menu commands that only a user with an Administrator role can execute (such as deleting a database or adding users to the database). If you are the only user in your database, you have an Administrator role. However, if several users in your company can access the data, you may want to limit what each user has the ability to do. Consequently, it is a good policy for all users that have been assigned to the Administrator security role maintain a password.

Procedure: ***To add a password to your logon name***

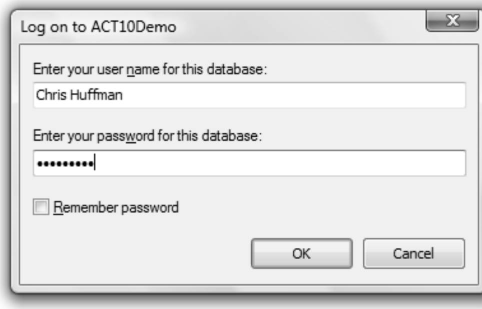
1. **File, Set Password…**. The **Set Password** dialog box appears.

2. If you do not currently have a password, start by entering your **New Password:** and then **Confirm New Password:** As you type, your password will display as ***.

   ☞ *A Password Policy may have been set for your database that requires your password to meet certain criteria (minimum characters, include different characters, etc.).*

3. Click **OK** to confirm that your password has changed.

☞ *If you want to remove your password, use the same procedure as above, except type your current password in the **Current Password:** area and leave the **New Password:** and **Confirm New Password:** areas blank. Click **OK** and your password is replaced with a blank password.*



There is an option that allows ACT! to **Remember password** as you log on. Hello… then what is the point of a password! Either remove the password or clear this option.

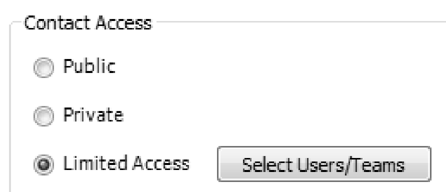
☞ *Actually, in multi-user environments, some users leave it checked to make it easier to log on from their own PC, while others on the network would have to know the password in order to log on as them.*

Team Management Premium

You may want to divide the database into smaller chunks to make it more usable for your sale teams.

- Some users may find dealing with large numbers of contacts rather cumbersome and only wish to view their own contacts' records.
- If your sales staff works in clearly defined geographical areas or vertical market territories, they may wish to access only contacts that fall within those territories.
- Some sales teams that are very competitive may want to restrict access to their contacts to members of their group only.

While each user could mark their contacts as Private, neither members of their sales team nor Management would be able to see those contacts.



Premium ACT! Premium provides a Limited Access feature which allows you to assign a Contact record to a *specific User*, *Users*, or *Team of Users*, thus limiting which users can view which Contacts in the database.

So, while **Roles** define which features in ACT! each user can access (deleting, backing up, importing, etc.), **Teams** are used to define which user can see which Contacts (and their associated notes, history, activities, opportunities, Secondary Contacts, or documents).

A **Team** is a collection of users who have access to the same contacts. While you can **Limit Access** to specific users, it is much easier to manage the Limited Access feature by using Teams. For example, you could create a Team for the West Coast and one for the East Coast. The West Coast Team could be made up of the West Coast sales reps, the inside sales staff, the VP Sales and the Record Manager for the contact. We can add the Limited Access by Team to all of the contacts in our database who are in California, Oregon, and Washington. The East Coast Team would consist of the East Coast sales staff, the VP, and the