

## Password Management

Passwords are used to further control access to your ACT! database. They are not required to use the database, but are easy to implement.

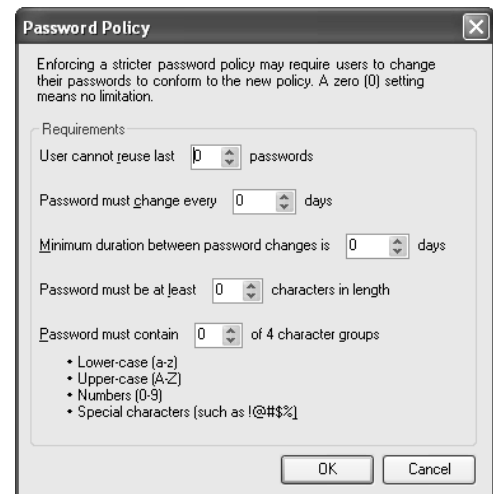
- ✓ An Administrator can set global password options for all users in the database.
- ✓ An Administrator can define individual password requirements for each user name that can override some of the global requirements.
- ✓ Even if no password options have been set, a user can opt to add their own password.

### Defining a Global Password Policy

To help protect your valuable contact information from unauthorized access, Administrators can define a Password Policy which applies to all users of the database. The policy can control the length, the complexity, the expiration options, and reuse of a password.

The Policy can be defined using these options...

- ✓ **User cannot reuse last \_\_\_ passwords** – indicates the number of previous passwords that can not be reused. The maximum is 9. A setting of 0 indicates that a password may be reused.
- ✓ **Password must change every \_\_\_ days** – indicates how frequently a user must change their password. Once a year is the longest time allowed. If the option is set to 0, then the user never needs to change their password. Administrators can override this option by setting the “Password never expires” and/or “User cannot change password” options on individual records.
- ✓ **Minimum duration between password changes is \_\_\_ days** – indicates the minimum number of days a password must be in use before a user is allowed to change it. A year is the longest time, but if the option is set to 0, the user can change their mind about their password the second they click **OK**.
- ✓ **Password must be at least \_\_\_ characters in length** – indicates the minimum number of characters for a password. The maximum can be set to 25 (now that would take a long time to log on). If the setting is 0, then the user can determine their own length. If you set it to 1, then it is

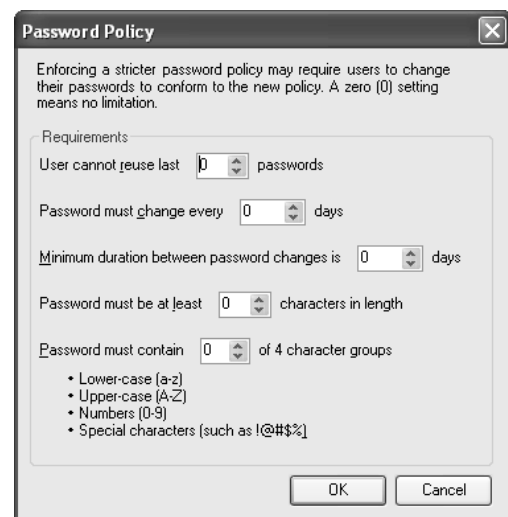


the same as requiring a password for all users. The value that you set for this option must be equal to or greater than the value in the next option concerning character groups. (After all...if a password must contain two character groups, then you have to input at least two characters.)

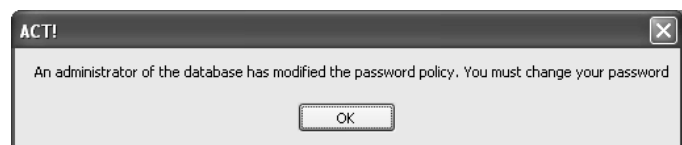
- ✓ **Password must contain \_\_\_ of 4 character groups** – determines the complexity of the password, such as requiring a combination of lowercase, uppercase, numeric, or special characters. A setting of 1 is effectively the same as 0, since any password you could type would have at least one character group.

**Procedure:** *To define a global Password Policy*

1. **Tools, Password Policy....**
2. Change the requirements as desired. The explanation of each option is described above.
3. Click **OK**.




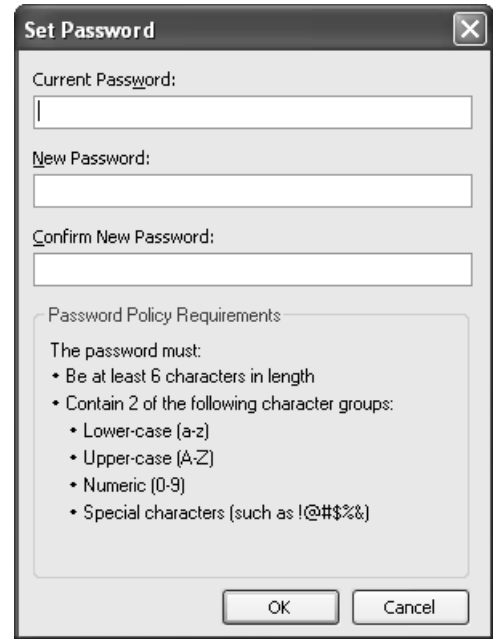
When a Password Policy is implemented or changed, all users will be prompted to enter a password the next time they log on to the database (unless their current password happens to already comply with the new policy).



After clicking **OK**, the user will be presented with the **Set Password** dialog. If the user has never had a password, then they should leave the **Current Password:** blank and enter the **New Password:** according to the Policy Requirements listed.

Enter the password again in the **Confirm New Password:** box to avoid assigning a password with a typo, and click **OK**.

 *With every change of a password, ACT! warns the end-user that the change affects handheld links, the Outlook® address book, or other third-party applications. When you change your password in ACT!, you will need to update your passwords in the Palm linking software as well as the one you entered for the Outlook Address Book.*



**Mini-Exercise: Define a Global Password Policy**

Step	What to do	How to do it/Comments
1.	Define a Password Policy for the ACT9Demo database that requires a password that is a minimum of six characters coming from three character groups.	Practice with this on the ACT9Demo database before implementing in your own database. It is always a good idea to <b>File, Backup Database...</b> prior to implementing this policy.  <b>Tools, Password Policy...</b> Change “Password must be at least...” to 6 and change the last option to 3. Click <b>OK</b> .
2.	Log off the ACT! Database and log back on as Chris Huffman.	<b>File, Close.</b> <b>File</b> , click the <b>1 ACT9Demo.pad</b> (above the Exit option). Click <b>OK</b> to acknowledge the Password Policy change. Unless you have set up a password previously for Chris, the <b>Current Password:</b> is blank. Enter a <b>New Password</b> (and retype it in the Confirm area) conforming to the new Password Policy requirements. Click <b>OK</b> to acknowledge that you might need to update other links.

Step	What to do	How to do it/Comments
3.	<p><b>IMPORTANT:</b> Remove the Password Policy from the database and then remove Chris' password! (So you can log on later to do more exercises.)</p> <p>Really, this is important... don't skip this step or you may not remember how to get back into the ACT9Demo database.</p>	<p><b>Tools, Password Policy...</b>, starting with the bottom option, change all options back to 0, and click <b>OK</b>.</p> <p><b>Tools, Manage Users</b>, double-click Chris Huffman, click the <b>Reset Password</b> button, and clear the "User must change password at next log on" option. Click <b>Finish</b>, then <b>OK</b>, and finally <b>Close</b>.</p>

### 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.



*If you select the "User cannot change password" option for a user, and you set the "Password must change every \_ days" option in the Password Policy, the individual user will be locked out of the database. To allow the user to access the database, clear the "User cannot change password" option.*

#### Edit User Information

Contact Name:  
Chris Huffman

User Name:  
Chris Huffman

Security Role:  
Administrator

Password options:

New Password:  
\*\*\*\*\*

Confirm Password:  
\*\*\*\*\*

User must change password at next log on.  
 User cannot change password.  
 Password never expires

### Setting a Password for Yourself

If you are the only user of your database, you may not want to go to the trouble of using a password. However, should your laptop ever get lost, would you want your client list falling into the hands of just anyone? 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 your 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, all users that have been assigned to the Administrator security role should probably have a password.