Desktop Database Security

The Security Problem for Desktop Database

A desktop database usually is small and can be distributed with your applications. This is convenient for your applications. But it may have a security problem if you want to set password to the database. How to keep the password secure while your users may easily use your applications?

Method 1: Do not save password

The most secure way of using password protected databases is not to save the password in computers. It requires your users to know the password and enter the password each time your application is used. It is secure but may not be convenient.

Method 2: Save password in ApplicationConfiguration

ApplicationConfiguration can be used to encrypt and save the passwords. In your applications, use SetCredential action to pass the passwords to database accessing objects.

The users do not have to enter password every time your application is used. The users still have to enter the database password once for one computer. For more details, see
http://www.limnor.com/support/HideDataInSoftware.pdf

For using ApplicationConfiguration, see "Application Configuration" node in Limnor Studio Tutorials.

Method 3: Encrypt passwords

The Connection Manager allows you to encrypt the passwords:
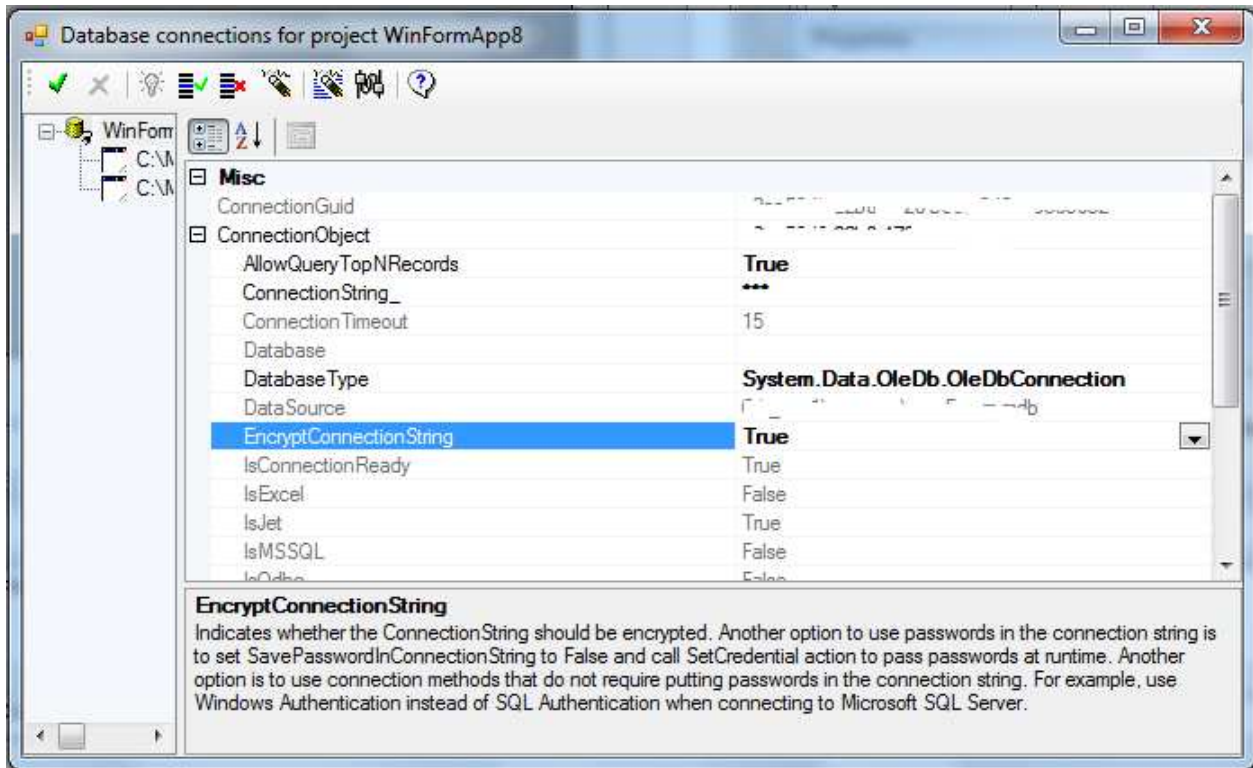
This method is the least secure of the 3 methods mentioned here. But it is the most convenient method for the users because it does not require your users to do anything in order to use your applications.