



**I**Secure**D**at

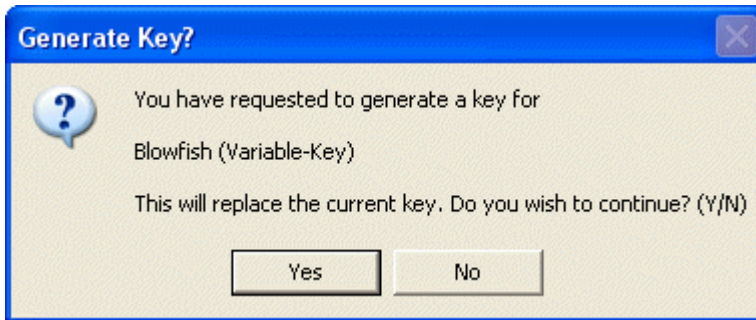
presents

# Understanding Encryption Keys

# Encryption Keys

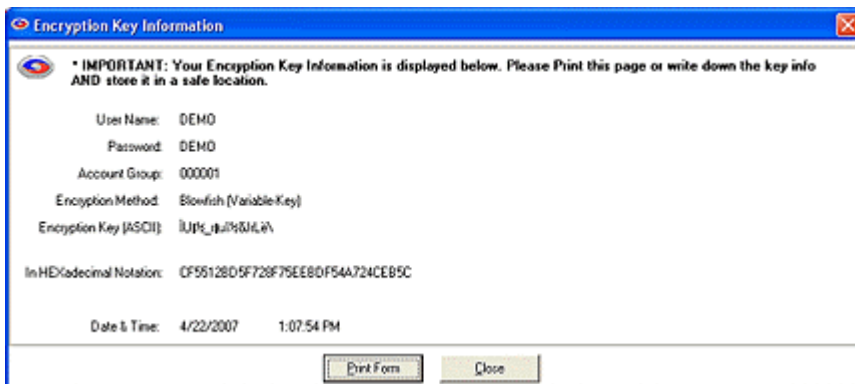
RBackup has a way to automatically generate "statistically perfect" encryption keys - the most secure keys. If you want the very highest security, do not pick your own key. Allow RBackup to generate it for you. The way RBackup generates a key depends on which encryption standard you have chosen.

If you pick "DES (8.3 Standard)" RBackup will generate a 128 bit key, represented as sixteen letters and numbers.

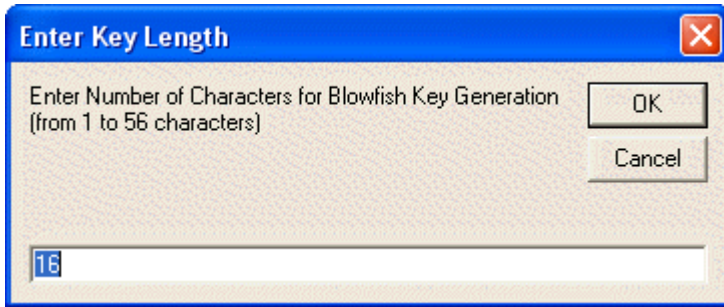


Since these "perfect" encryption keys are hard to remember, it is recommended that they be recorded on paper and kept in a safe place.

The software will display a printable form containing the key information. It should be printed and kept in a safe place away from the computer.



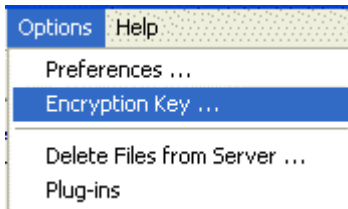
**Whenever an Encryption Key is changed it is advisable to create a new Key Disk using the Key Disk button.**



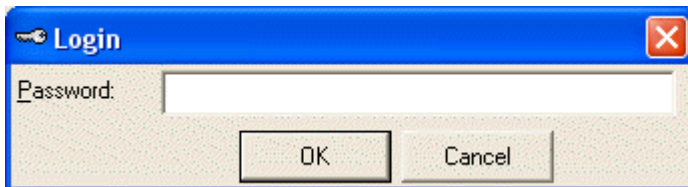
When generating a key for Blowfish encryption, you will see an additional screen asking how long you want the key to be.

Blowfish varies from one to 56 characters. A "character" is eight bits. So, Blowfish varies from eight bits (1 x 8) to 448 bits (56 x 8)

Clients can change their Encryption Keys any time.



To change the key, select "Encryption Key..." from the Options Menu in the Client software.



Enter the Password - either the Administrator's Password or the password assigned to the Client for login.



## Generate Key:

Our encryption support includes the ability to generate a key that, due to its structure, provides stronger encryption of your files.

To generate a key, select the method and then press the Generate Key button.

All methods except Blowfish have a mandated key length. The system will ask for a key length if Blowfish is used.

