

# Using encryption while backing up files

Starting from Syncrify version 1.4, users can backup an encrypted version of the files to the server. When files are encrypted they cannot be seen/opened by anyone unless they know the password that was used to encrypt it.

It is important you read this article in its entirety before using this feature.

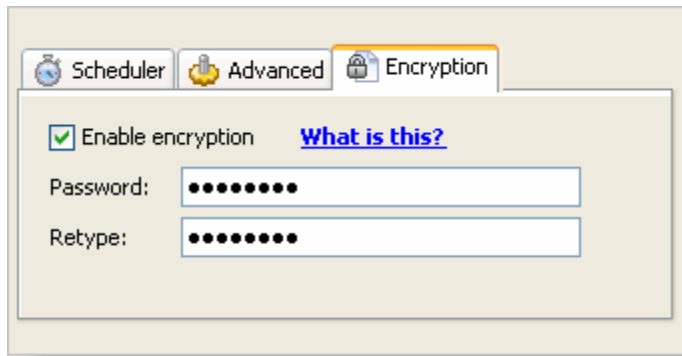
Encrypting files has its pros and cons. The benefit is obvious: the only reason you would want to encrypt any file is to prevent non-authorized users from accessing it.

Below are some disadvantages of using this features.

- **Speed** - When you encrypt files, backups will run slower. Every file that needs to be backed up will be encrypted on the client's end and then will be sent to the server. This time delay is particularly noticeable for large files. For example, encrypting a 1GB file can take approximately 3 minutes.
- **Lost password** - You will NOT be able to recover your file from backup if you forget the password. Syncrify uses 128 bit strong AES encryption to encrypt files. This type of encryption can take years even for a computer to guess a password.
- **Entire backup** - Every file from your local machine gets copied again if you
  - change your password
  - switch from encrypted to unencrypted mode or
  - unencrypted to encrypted mode.
- **Restore** - Syncrify client will be able to restore files without any extra steps. However, if you use the browser to download a file from the server, you will have to manually decrypt it using Syncrify client.

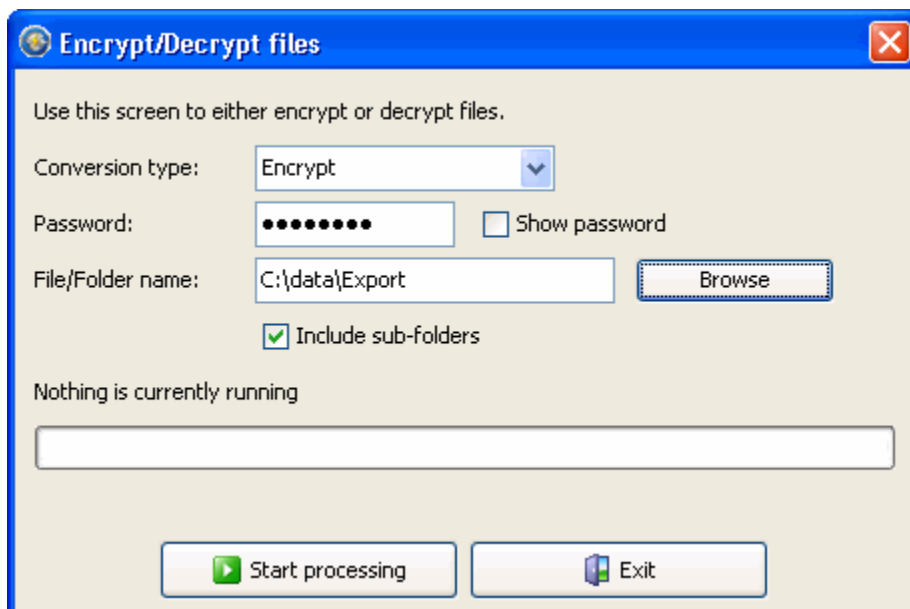
## How to use encryption

To use encryption simply click on the encryption tab, select the option for encryption and specify a password. The password cannot be more than 16 characters long. Refer to the image below.



## Encryption tool in Syncrify client

For your convenience, Syncrify client includes a tool that can be used to encrypt/decrypt files on demand. Click **Encrypt/Decrypt files** from the Tools menu. This opens the following screen.



This screen is used to either encrypt/decrypt a single file or every file in a folder. When Include sub-folders is checked, files will be included recursively.

**IMPORTANT:** This tool does not change the file name when it is either encrypted or decrypted.