JBackpack Manual

JBackpack Manual

Version 0.9.3

Abstract

JBackpack is a personal backup program. It features incremental backups, network transparency and encryption.

Table of Contents

List of Figures

Chapter 1. Overview

JBackpack uses rdiff-backup (http://www.nongnu.org/rdiff-backup) for all backup and restore functions. The most interesting feature of rdiff-backup is *incremental backups*.

An incremental backup is a backup method in which multiple backups are kept (not just the last one). Each original piece of backed up information is stored only once, and then successive backups contain only the information that changed since a previous backup. This way it becomes possible to restore changed or deleted files, even when several backups have been run since changing or deleting these files.

JBackpack offers a build-in increment browser. This makes the file selection before restoring very easy.

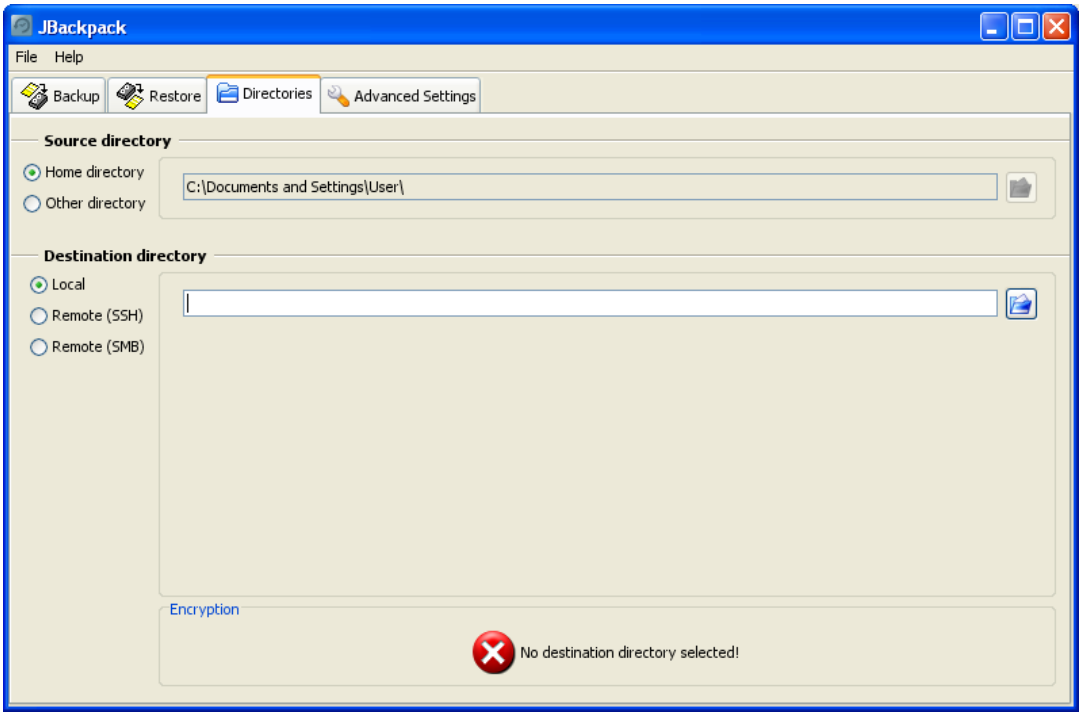
JBackpack uses SSHFS (http://fuse.sourceforge.net/sshfs.html) and SMB (http://en.wikipedia.org/wiki/Server_Message_Block) to access remote file systems. This way it is possible to store backups on remote systems. This increases the availability of the backups in case of a local system failure but slows down the backup process because the available bandwidth for remote file systems tends to be much smaller than the available bandwidth for local file systems.

JBackpack uses EncFS (http://www.arg0.net/encfs) to encrypt backup destination directories. Encryption provides confidentiality but also slows down backup and restore.

Chapter 2. Directories

When you start JBackpack for the first time it will open the "Directories" tab.

Figure 2.1. Directories tab



Here you can configure the directories used for the backup process.

2.1. Source directory

The first directory is the source directory. Only files in this directory are included in backups. JBackpack uses your home directory per default. When you want to backup a different directory you must click the "Other directory" radio button. Then you can type the path of the other directory into the textfield or use the file browser button right of the textfield to browse to the directory you want to backup.

2.2. Destination directory

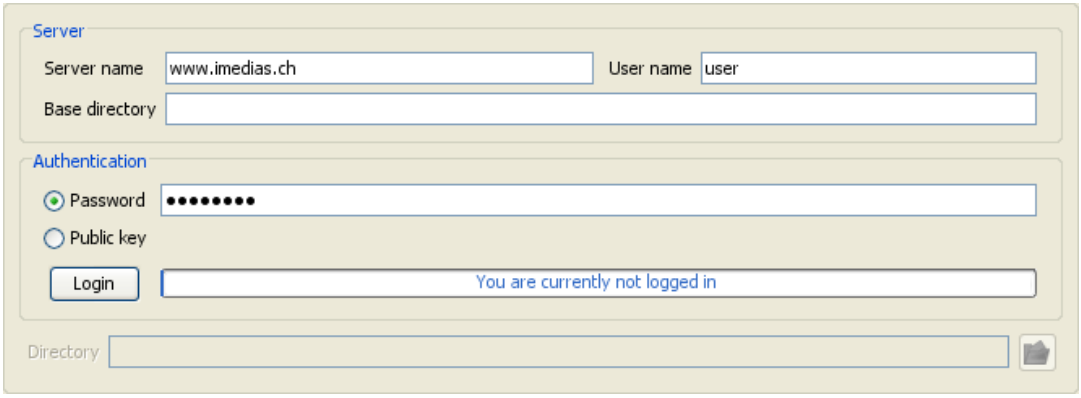
The second directory is the destination directory. This is the location where the backup files and increments are stored. The destination directory can either be:

- local
- remote via SSH (more information about SSH can be found here: http://en.wikipedia.org/wiki/Secure_Shell)
- remote via SMB (more information about SMB can be found here: http://en.wikipedia.org/wiki/Server_Message_Block)

When you select a local destination directory you can type the path of your destination directory into the textfield or use the file browser button right of the textfield to browse to your destination directory.

When you select a remote destination directory via SSH you have to configure some additional settings:

Figure 2.2. SSH settings

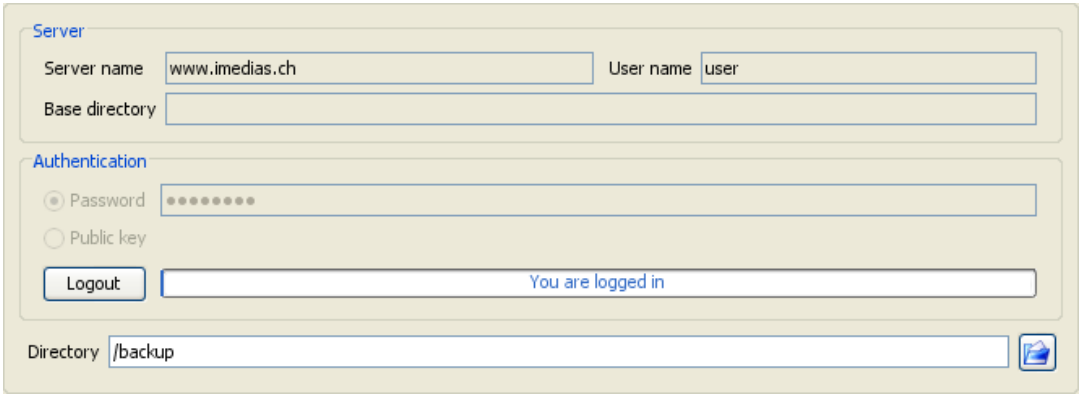


Please insert the host name of the server where you want to store the backup data (you must be able to connect via SSH to this server) and your user name on this remote server. Directory browsing on the remote server is based on your home directory on the remote server. If your remote destination directory is not a subdirectory of your home directory on the server you can specify a custom base directory to start remote file browsing somewhere else.

You can authenticate at your remote backup server with either a password or a public key. If you choose public key authentication please make sure that everything is correctly set up. Some details about setting up SSH public key authentication can be found here: http://www.debian-administration.org/article/SSH_with_authentication_key_instead_of_password

After successfully logging in, the remote backup destination directory can be configured:

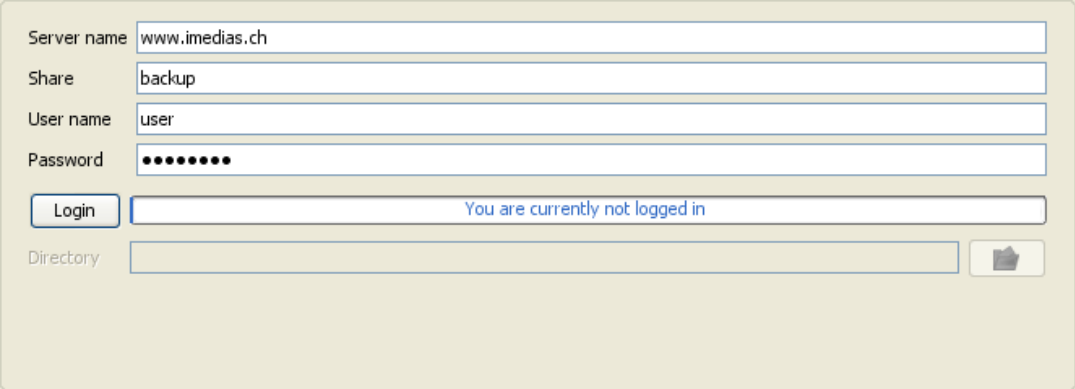
Figure 2.3. Logged in



If you know the path of the directory you can type it directly into the textfield, otherwise you can use the file browser button right of the textfield to browse to your directory.

When you select a remote destination directory via SMB you have to configure some additional settings:

Figure 2.4. SMB settings

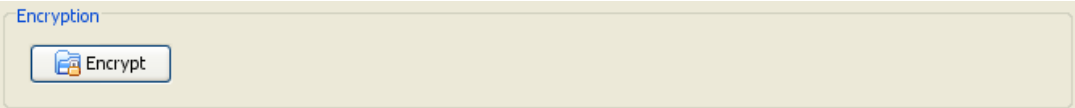


Please insert the host name of the server where you want to store the backup data (you must be able to connect via SMB to this server), the name of the share, your user name and password on this remote server.

After successfully logging in, the remote backup destination directory can be configured.

When you have selected a valid (and still unencrypted) destination directory a button for encryption appears:

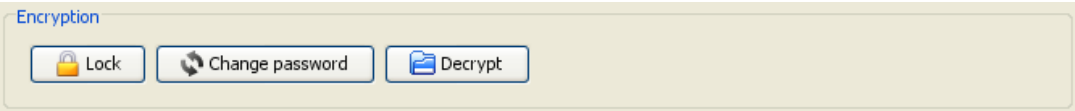
Figure 2.5. Encryption button



By clicking on this button you can encrypt your destination directory with a password.

When your destination directory is encrypted, the encryption control panel appears:

Figure 2.6. Encryption control panel



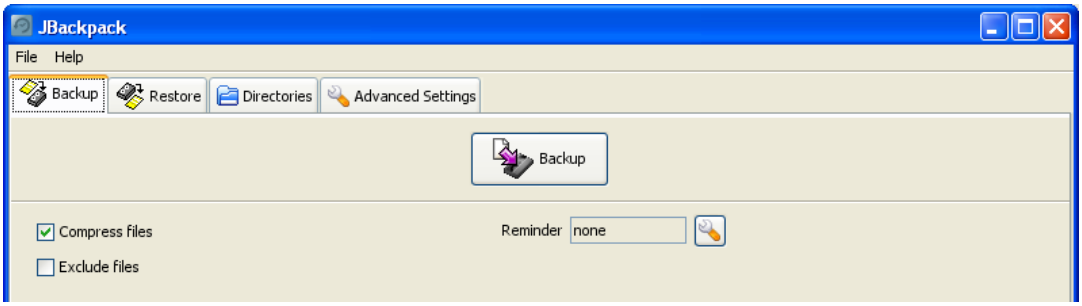
There you can lock and unlock the backup destination directory, change the encryption password and (if you no longer need the additional security provided by encryption) decrypt the destination directory.

Encrypted directories can only be accessed for backup and restore operations when they are unlocked. Unlocking is only possible with the encryption password. *There is no recovery mechanism. You really have to remember the encryption password!*

Chapter 3. Backup

If you have configured all your directories you may switch to the backup tab:

Figure 3.1. Backup



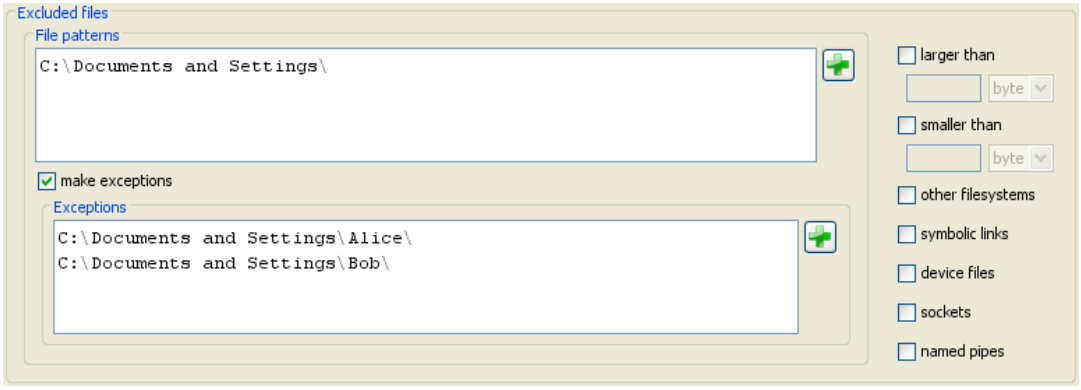
You can start the backup process by pressing the big "Backup" button at the top.

The only option activated by default is “Compress files”. File compression can save a considerable amount of storage space in your destination directory but also slows down the backup and restore process.

You can also configure JBackpack to remind you to backup your data at a given interval.

If you do not want to backup *all* the data of your source directory, you can select the checkbox “Exclude files”. This enables another set of options:

Figure 3.2. Excludes



In the file patterns textarea you can define files or directories you want to exclude. Die file patterns are regular expressions (see http://en.wikipedia.org/wiki/Regular_expression). The button on the right hand side (with the big green “plus” icon) opens a filechooser that simplifies selecting and adding files and directories you want to exclude.

On Windows you have to follow two special rules because there the file separator is a backslash (“\”) and this is also the escape character for the just mentioned regular expressions:

- In the part of the path that is equal to the source directory, the backslashes have to be doubled.
- In the remainder the backslashes have to be replaced by normal slashes (“/”).

You can also make exceptions from the exclusions. This is very helpful in more complicated backup settings, like in the following example. Assume that you have this directory structure:

```
C:.
####Documents and Settings
    ####Alice
    ####Bob
    ####Other1
    ####Other2
    ####...
    ####OtherN
```

If you only want to backup `C:\Documents and Settings\Alice\` and `C:\Documents and Settings\Bob\` you have to configure `C:\Documents and Settings\` as the source directory, add `C:\\Documents and Settings` as excluded file pattern and add `C:\\Documents and Settings/Alice` and `C:\\Documents and Settings/Bob` to the exceptions.

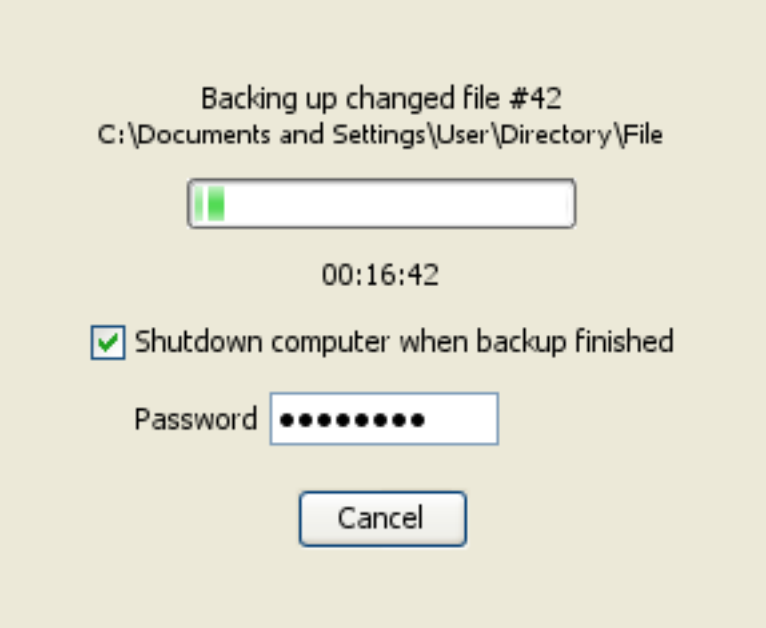
On the right hand side you can exclude files by their features:

- size (you can specify a minimum and a maximum size)
- if it is located on the same filesystem as the source directory
- if it is a symbolic link
- if it is a device file
- if it is a socket
- if it is a named pipe

More information about symbolic links, device files, sockets and named pipes can be found here: http://en.wikipedia.org/wiki/Unix_file_types

If you start the backup process you see the following progress information:

Figure 3.3. Running backup



It shows:

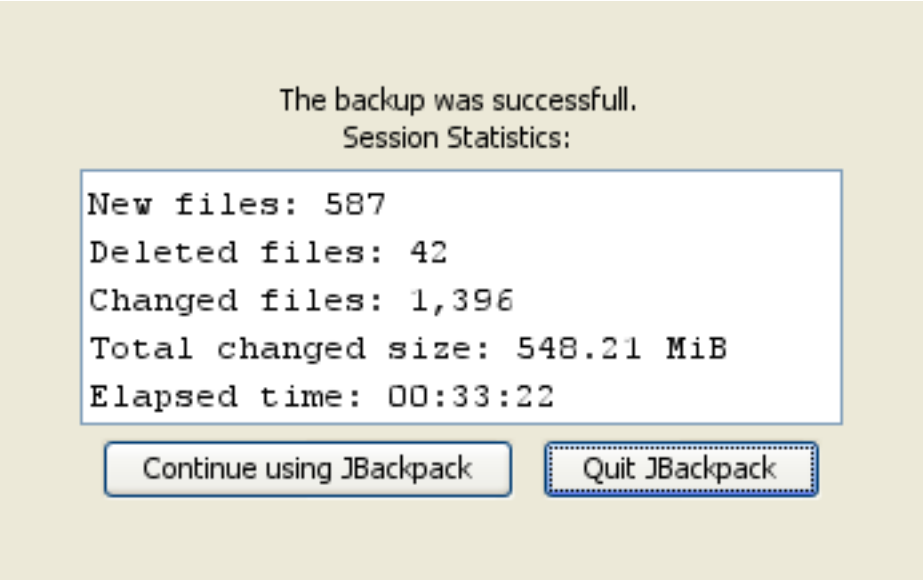
- the number of already backed up files

- the currently backed up file
- the time already spent

You can also choose to shutdown the computer when the backup operation is finished. You have to have administrative privileges and provide your password. You can also cancel the backup operation.

When the backup operation finishes, the following summary is displayed:

Figure 3.4. Backup summary

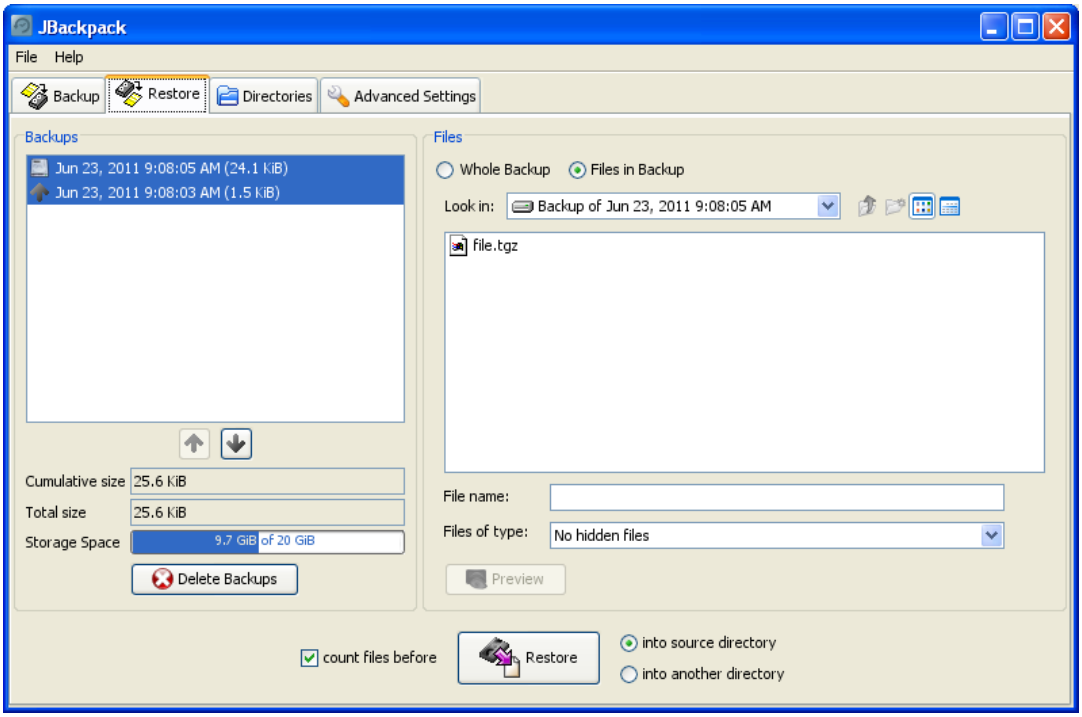


Most of the time there is not much else to do after running a backup. Therefore JBackpack sets the default focus to the “Quit JBackpack” button. You can just press **Enter** or click on the “Quit JBackpack” button. If you really want to continue using JBackpack, please use the “Continue using JBackpack” button.

Chapter 4. Restore

If you want to restore files, you have to select the restore tab:

Figure 4.1. Restore



On the left hand side you have the list of available backups. For every backup you see its type, timestamp and its storage usage. There are two backup types: The top backup is called the “mirror”. It contains all files of the last backup and is labeled with a harddisk icon. All other backups are called “increments” and only store the differences relatively to the younger backup (and therefore usually need much less storage space than the mirror). They are labeled with an arrow icon.

If you select a backup from the list, the file hierarchy of this backup is shown in the file chooser on the right hand side. With the help of the two arrow buttons at the bottom of the backups list you can easily navigate through the list of backups without constantly moving and aiming your mouse pointer.

Below the arrow buttons several storage size values are displayed:

- the cumulative size (the size sum of the currently selected backup and all older backups)
- the total size of all backups
- the storage space usage of the selected destination directory

With this information at hand you can decide if and how many backups you want to keep or delete. You can also automate the deletion of old backups. For more details see Section 5.1, “Automatic deletion of old backups” [10].

At the top of the right hand side you can select between either to restore the whole selected backup or just certain files or directories from the selected backup.

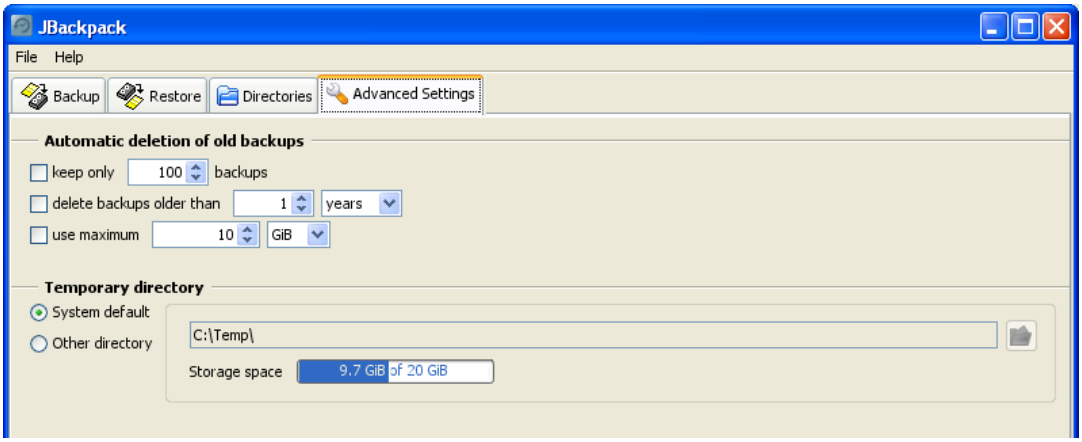
You can preview selected files by clicking the “Preview” button below the file chooser. The selected files will then be restored read-only into a temporary directory and will be opened with the associated program for preview.

At the bottom of the window you can start the restore operation. You can select to count the selected files before starting the restore operation. This makes it possible to display a progress bar during the backup operation but may take some additional seconds. You can also choose where to restore the files, either into the original source directory or another directory.

Chapter 5. Advanced Settings

Here you can configure optional features of JBackpack.

Figure 5.1. Advanced Settings



5.1. Automatic deletion of old backups

Every backup consumes storage space in your destination directory. Eventually you have to delete old backups. You can do so manually in the "Restore" tab but manual deletion can become tiring and sometimes you just forget about it. Automatic deletion of old backups relieves you of this work. You can specify with three different features how many old backups are deleted:

- number of backups
- age of backups
- storage space usage

5.2. Temporary directory

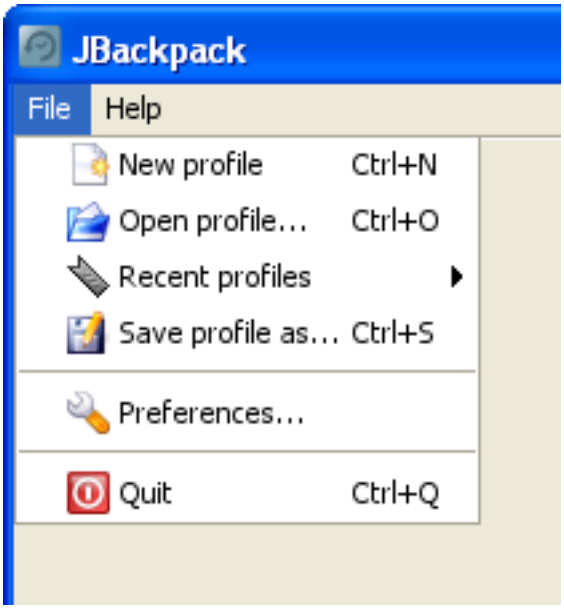
The temporary directory is used to store files that are only temporarily created during backup and restore. It usually needs to have as much free space as the size of the largest file in a backup or restore operation.

In most cases it is a good idea to use the system default directory. In case of a too small system default directory you can configure a different directory. The storage usage of the currently configured temporary directory is shown below the path.

Chapter 6. Working with profiles

There are quite a number of configuration options in JBackpack. You can manage these configuration options by using so-called profiles, files that bundle all these configuration options. If you open the File menu, there are several menu items for working with profiles:

Figure 6.1. File menu



You can

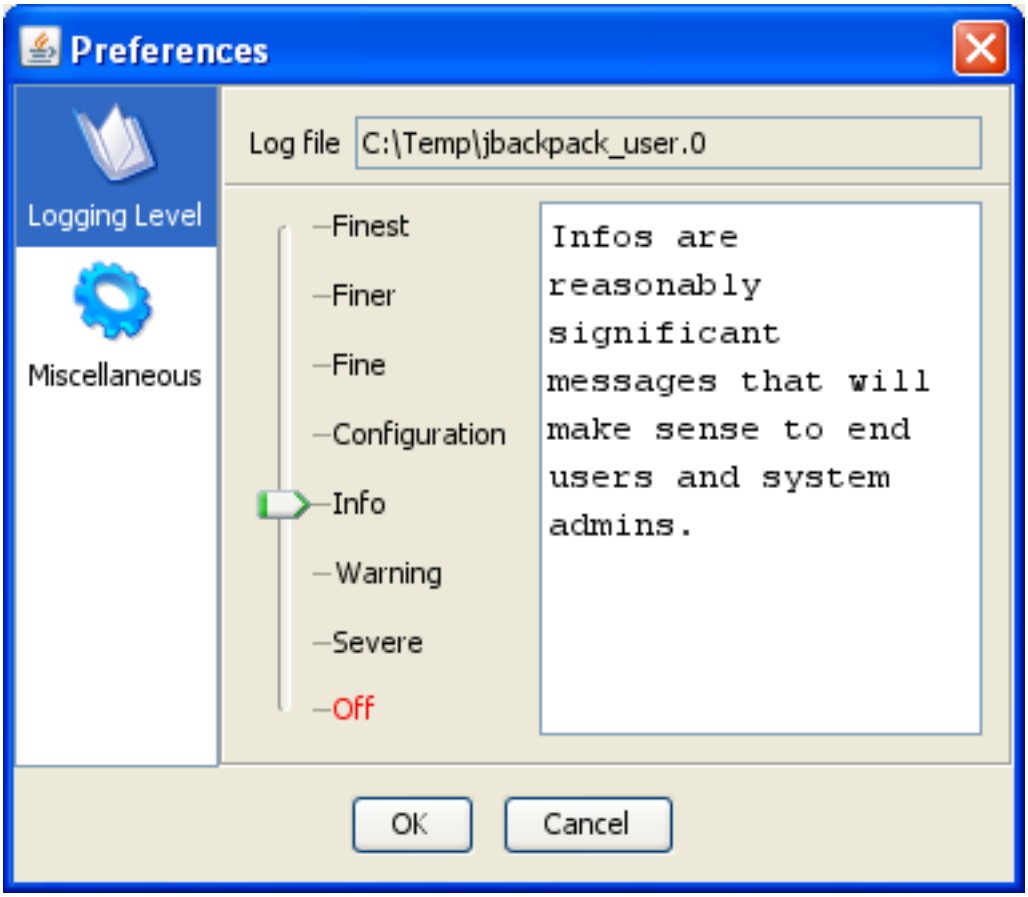
- create a new profile (this resets all configuration options to their default value)
- open saved profiles
- open recently used profiles
- save profiles

Working with profiles makes it easy to copy the JBackpack configuration from one machine to another and makes it possible to try something out without the risk to lose a usable configuration.

Chapter 7. Program settings

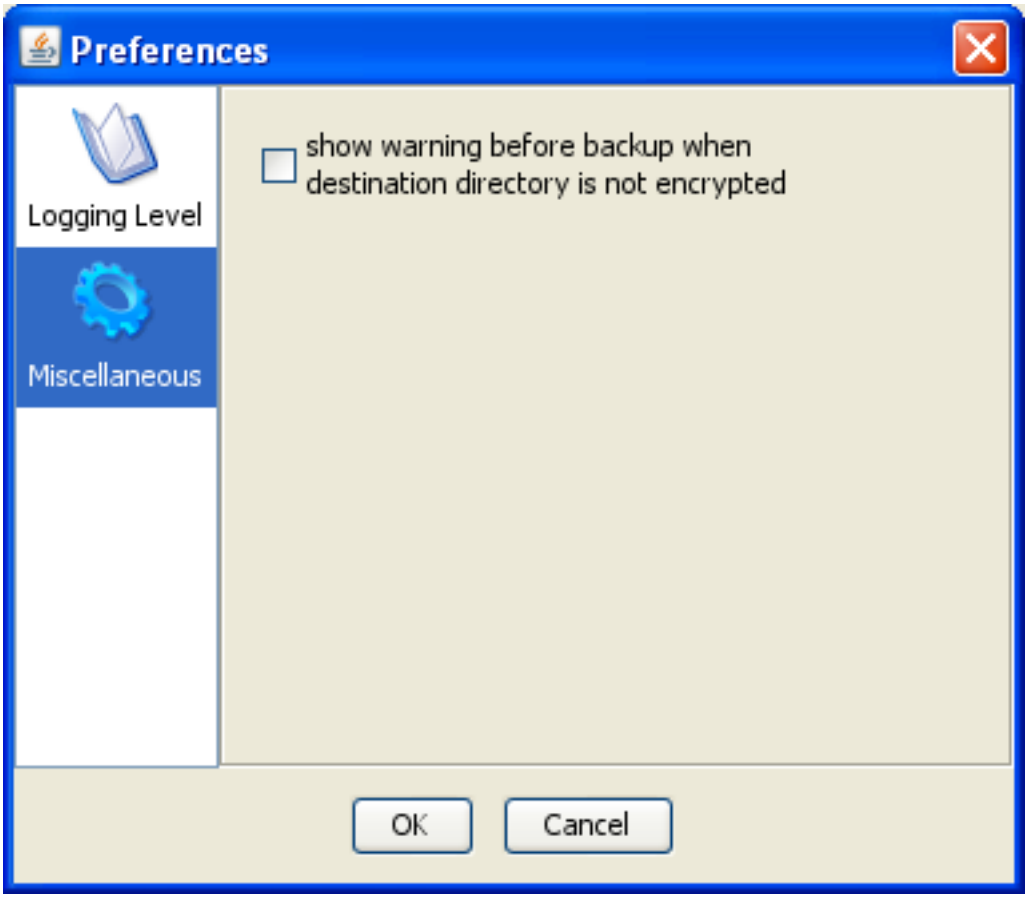
There are also some settings in JBackpack that are not directly affecting the backup and restore operations but the way JBackpack itself operates. These settings can be configured by selecting File > Preferences....

Figure 7.1. Logging Level



JBackpack records the details of its on operation into a log file. This is useful in case of a program error so that all actions before and after the error as well as the details of the error itself can be reconstructed and hopefully fixed by the JBackpack developers. Here you can configure how much information is recorded into the log files. The higher the level the more information gets recorded and the slower JBackpack operates.

Figure 7.2. Miscellaneous



JBackpack usually warns users when the destination directory is not encrypted. There are certain special cases, e.g. when the destination directory is located on an encrypted harddrive or when the destination directory is located in a trusted zone, when this warning is not necessary. Therefore you can disable this warning here.