Manual for Back4Sure

Version 3.7

1. Quickstart guide

1.1 About Back4Sure

Back4Sure is a program for making backup copies of your documents, pictures, music, videos and anything you find valuable. The files to copy may be distributed all over your computer, even on different drives. Back4Sure will gather all the files you've selected for backup and make a copy of them into a specified target directory. The folder with the drive drive letter of the source drive and the directory structure will be automatically created in the target directory, so all your files will be stored correctly and easy to find. In this process, Back4Sure will only copy files that have changed since the last backup, so even a large number of files is backed up as fast as possible.

You can use a USB flash drive, a second hard drive or a network share as backup target. With the built-in compression of Back4Sure you can save space and especially on flash disks lots of time when you make a backup of thousands of files.

Back4Sure does *not* use a proprietary file format to store your data. All files are simply copied or alternatively stored in standardized Zip or 7Zip containers. This way you don't need Back4Sure to get your files back, your file manager will do the job!

Additionally, Back4Sure has an option to cleanup the target directory. With this option you can remove orphaned files, that only exist in the target directory but do not have correponding source files anymore.

While offering lots of options for the backup process, Back4Sure is still handy and flexible: It occupies less than 10 MB of storage space and can easily be run from a flash disk without installation. It does not leave any traces on the host system and does not install any kind of extensions or services.

1.2 Installing the program

There are two options for installing the Program: A setup file and a zip file. If you want to install Back4Sure permanently on your computer, please choose the setup file. If you want to copy the program to a flash drive for portable use, you should use the zip file instead.

If you want to use the setup file, execute the file "Back4SureSetup.exe" and follow the instructions of the setup wizard. During installation, files will be copied into your program directory, the file extension ".b4j" will be registered with Back4Sure and optionally a link to the program will be placed on your desktop. *No* files will be copied into your system directories. After installation, Back4Sure is immediately ready for use.

If you want to copy Back4Sure on a flash drive for portable use, just unzip the file "Back4Sure.zip" to your flash drive. The program can be directly started from the drive now. No changes to your system are made. The file extension ".b4j" is also not registered with Back4Sure, so you'll have to open backup jobs from within the program. Just double clicking the job file will not open Back4Sure. You can still register job files with Back4Sure later in the program options.

1.3 Creating a backup job

After starting the program, you can see the user interface of Back4Sure. The directory tree on the left side shows your local drives and the tabbed options dialog on the right side allows defining the job settings.

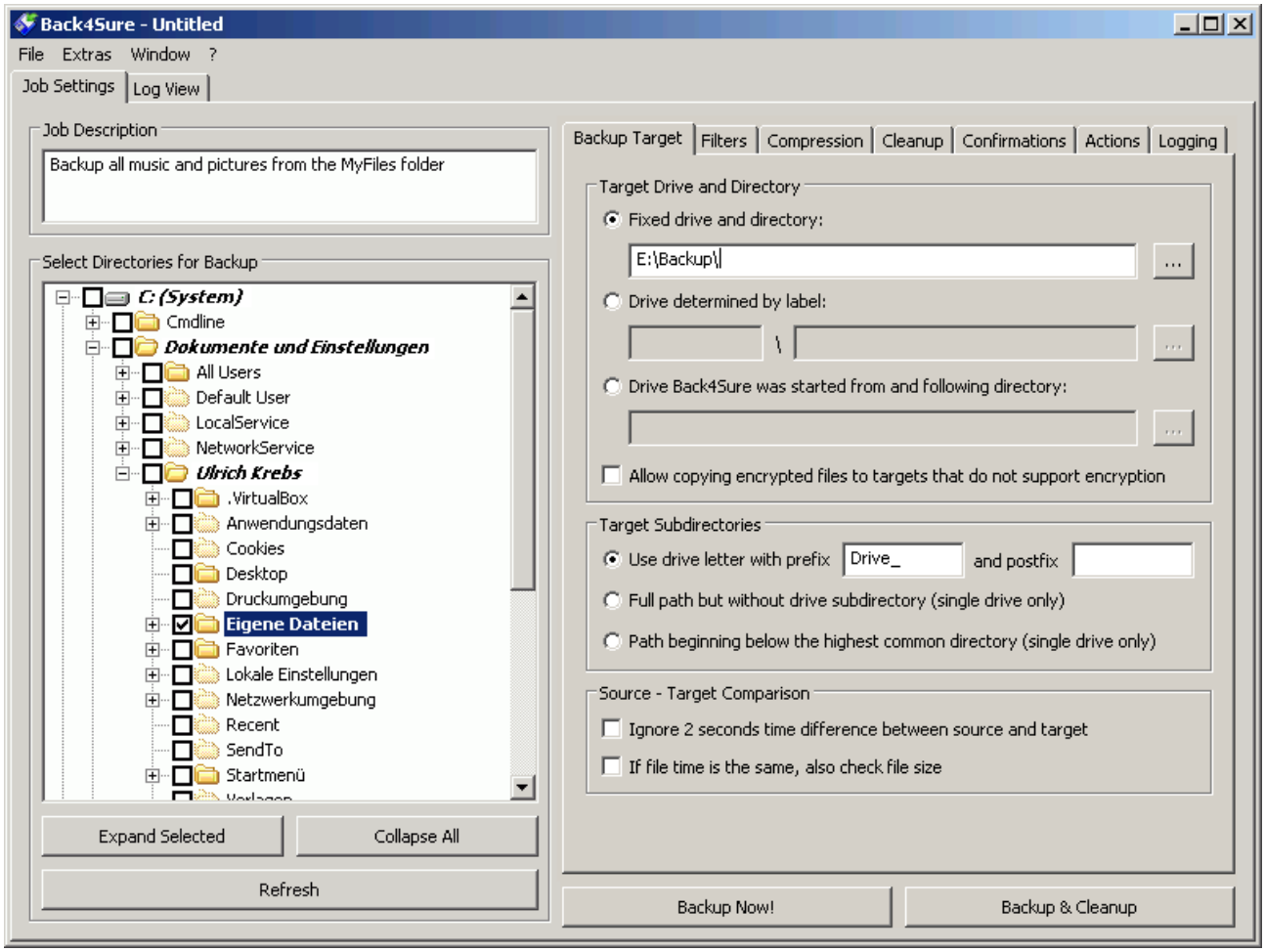

Figure 1.1: Main window of Back4Sure

The directory tree view may differ from what you usually see in your file manager. This is due to the fact, that the directory tree shows the *real* content of your drive, including all normally hidden directories and without special shortcuts like "My Documents". Don't be irritated, all files and folders are there, but probably not where you normally expect them. The folder "My Documents" e.g. is in fact located under "C:\Documents and Settings\<User Name>\My Documents".

The first step is to choose the directories to backup. For this, put a checkmark in front the directory you want to be included in the backup. Directories selected for backup and all their parent directories will be displayed in bold letters. If you want to include a whole drive into the backup, make sure to exclude the system directory "System Volume Information". This folder may not be accessed with the normal copy method and does not contain regular user data. You should also consider to exclude the "Recycler" directory, as it only contains files that were sent to the recycle bin. You may also exclude certain subdirectories from a selected directory. Just extend the selected folder by clicking the "+" sign in front of it and remove the checkmark of the folder you want to exclude.

The next thing to do, is to specify a backup location on the first tab of the options dialog on the right window side. In most cases the option "Fixed drive and directory" is the best choice. Click on the "..." button and select a directory as the backup target. The default

setting "Use drive prefix" under "Target Subdirectories" should be left untouched, as this option will definitely avoid ambiguities when creating the target directories. If you still plan to use one of the other two options, **please specify a directory used by this backup only under "Target Drive and Directory"! Do never make backups directly into the root directory of the backup drive, unless you definitely know what this means during a cleanup run!** Otherwise the cleanup function may erase files that you want to keep.

All required information for a backup job is now specified. You can now save the job under a meaningful name by choosing "File / Save Job As..." from the menu.

Though not absolutely necessary for successful operation, you may want to adjust other options for the backup job. Especially the filter and compression options may be of interest. The filter options allow a more detailed specification which files should be included in the backup and the compression options allow storing the files into compressed container files ("zip files"). These options are discussed in detail in the full manual and will not be considered here.

1.4 Executing the backup job

After saving the backup job, execution is initiated by pressing the "Backup" button. A progress dialog will appear to inform you about the current status of the backup operation.

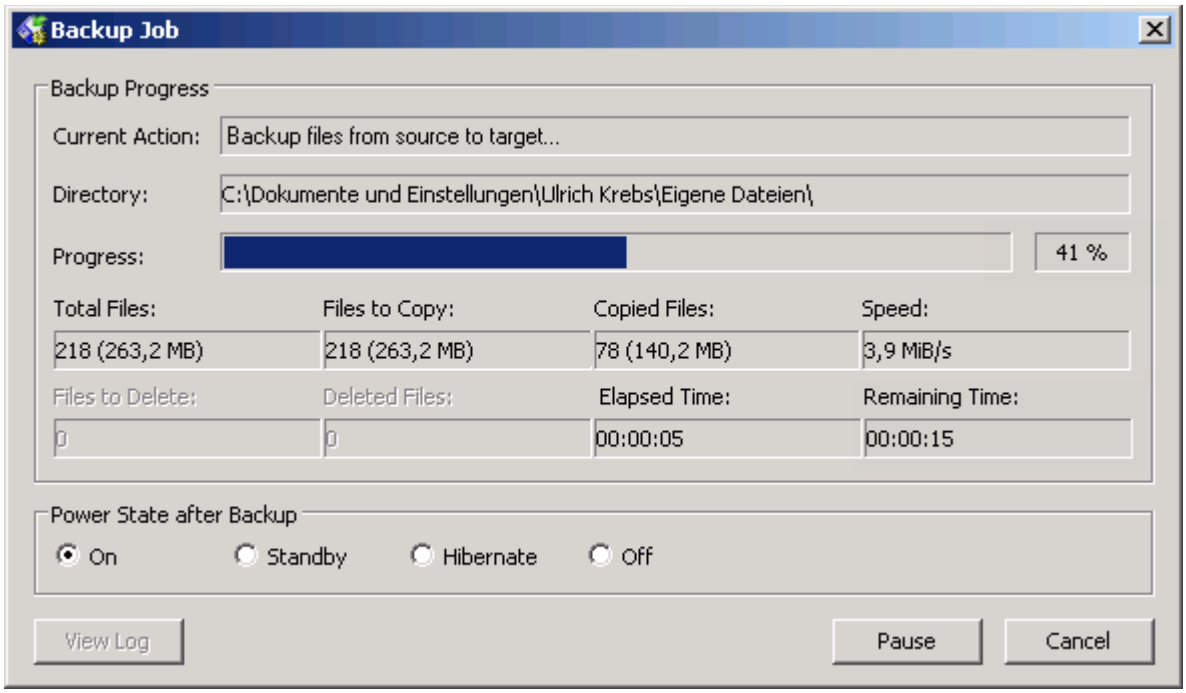

Figure 1.2: Progress of the backup operation

When the backup is finished, you can immediately see in the section "Current action" of the progress dialog, if the backup process was successful. If everything was OK, the display turns green, if there was any error, the display turns red. Backup errors often come from missing access rights or files that are currently locked for processing. To avoid this kind of backup errors, make sure to choose only directories with sufficient access rights for backup and to close all applications that may lock files (mail clients, word processors, etc.).

The reason for a backup error and the affected files can be found in the automatically generated log file. Just press the button "View Log" of the progress dialog. If Windows does not know how to open log files, you'll be prompted to choose an appropriate program

for this kind of files. You can use any unicode capable text editor for opening log files, even Notepad will be sufficient. Later on, you can find the log files on the tab "Log Files" of the main window. Just double click an entry there to open the file in your text editor.

Below you can see an example log file of a backup where an error occurred.

```
*** Job Summary ***
Job name: Test
Job started: 2009-09-13, 22:56:47
Job finished: 2009-09-13, 22:56:47
Elapsed time: 00:00:00
Result code: 1 (There were errors)

*** Backup Summary ***
Total files in backup-set: 38
Total bytes in backup-set: 1038787 (0,99 MiB)
Files to copy: 38
Bytes to copy: 1038787 (0,99 MiB)
Copied files: 37
Copied bytes: 1016319 (0,97 MiB)
Speed: 8,13 MiB/s
Source access errors: 0
Backup errors: 1

*** Source Access Errors ***
No errors occured

*** Backup Errors ***
Source: C:\Documents and Settings\Ulrich Krebs\Application
Data\Mozilla\Firefox\Profiles\cookies.sqlite-journal
Target: E:\Drive_C\Documents and Settings\Ulrich Krebs\Application
Data\Mozilla\Firefox\Profiles\cookies.sqlite-journal
Target state: File is outdated
Backup result: 32 (The process cannot access the file because it is being used
by another process.)
```

Obviously, the file cannot be copied because it is locked by another application, in this case Firefox.

1.5 Cleanup the backup target

It is a good idea to cleanup the target directory every now and then. Due to changed directory structures or file names in the source directories, some files in the target directory become orphaned, i.e. they have no counterpart in the source directory anymore. Back4Sure can delete these orphaned files automatically if you choose "Backup & Cleanup" from the main window. All files in the backup target will be tested for a corresponding source file, then. If there is no such source file, the file in question will be deleted from the backup target.

By default, Back4Sure uses a safe mode when doing the cleanup. In this mode, only files that do not have a counterpart in the source directory will be deleted from the target directory. Files that do not match the backup job and therefore should not exist in the target directory will not be deleted as long as there is a corresponding source file. There are other cleanup modes that do a more exhaustive job, but these options are discussed in detail in the full manual.

2. Program options

Most of Back4Sure's options are per job settings. Usually, each backup job has its very

own requirements concerning the filter, compression or logging settings. Therefore only very few options affect the global behavior of the program. The dialog for program-wide options is available from the menu "Extras / Options...".

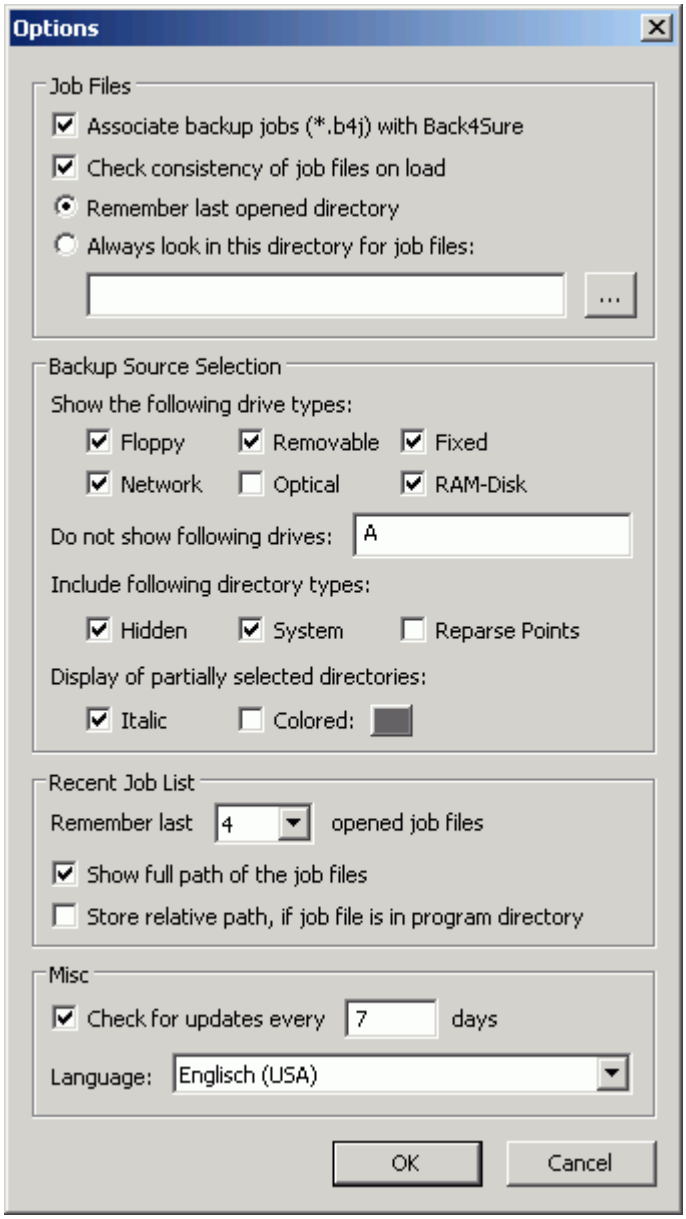

Figure 2.1: Program options

2.1 Job files

In this section all settings concerning the handling of job files are configured. The first option option shows if the backup jobs with the file extension ".b4j" are currently associated with the program Back4Sure. If you want to open backup jobs by double clicking a ".b4j" file in explorer, make sure this option is enabled. By deactivating this option, all corresponding entries from your registry are deleted.

If the option "Check consistency of job files on load" is enabled, Back4Sure automatically checks backup jobs for errors on load. Recognized errors are non-existing source directories or exclude directories. These errors are not critical and will not cause backup errors, still they do not belong into the backup job and should be removed. If Back4Sure detects an error when loading a backup job, it will show you a dialog with the option to remove the erroneous entries. Fixing the errors will only remove the bad links from the job

file, no changes are made to your source or target drive. If you decide to disable automatic error checking, you can still trigger a manual verification by choosing "Extras / Check Job Consistency" from the menu.

The option for automatically checking the job consistency is ignored if you run Back4Sure with command line switches that trigger an action like a backup operation. This behavior ensures that an automatically started backup is not aborted by a rather harmless error in the backup job.

The next two options tell Back4Sure where to look for job files if you choose "File / Open Job..." from the menu. If the first option is activated, the file selection dialog will always open in the last chosen directory. If this is not the desired behavior, you can activate the second option instead and define a fixed directory for job files. The next time you want to open a job file via "File / Open Job...", the file selection dialog will always default to the directory entered here.

2.2 Backup source selection

Under "Show the following drive types" you can choose which kind of drives should be visible in the tree view on the left side of the main window. In many cases you won't need to show all kind of drives for source selection, e.g. optical drives ar usually not required to be backed up. To exclude a certain drive type from source selection, just deactivate the corresponding option. Independent from the drive type you can also selectively exclude certain drives from being displayed in the backup source selection tree. This is especially helpful if you are the proud owner of an ancient floppy drive. Back4Sure often accesses the connected drives to update its views. If a floppy drive is attached to the computer, it will also be examined, producing an unmistakable rattling noise. This option gives you the possibility to make Back4Sure simply ignore the floppy drive. To exclude a drive from display, just enter its drive letter into the edit field. If you want to exclude more than one drive, simply enter all drive letters without separator into the edit box.

You have also an option to exclude certain types of directories from being displayed and backed up. You can choose whether hidden or system folders or so-called Reparse Points should be displayed and backed up or not. Reparse Points usually can be excluded as they are not "real" folders but rather placeholder for other folders. Windows 7 has quite a few Reparse Points inside the user directory, which may not be accessed and therefore cause backup errors. By excluding a certain folder type, all folders with that property will not be displayed in the source selection tree and also be ignored during the backup process. So if you exclude e.g. all hidden folders, all hidden folders will not be part of the backup anymore!

The next option determines how to display partially selected directories in the backup source selection tree. A partially selected directory has at least one subdirectory that is excluded from the backup. To easily recognize such directories, they can be shown italic and/or color marked by activating the corresponding option. The marker color can be selected by clicking on the colored button.

2.3 Recent job list

Back4Sure maintains a list of most recently opened job files. This list is displayed in the file menu to offer an easy way to access the most frequently used job files. You can specify here, how many files the list should contain.

Additionally you can choose whether the full path of the job file should be displayed or only the file name. If the full path is very long, it might appear shortened in the file menu for

display purposes.

Finally, there is a useful option for the portable use of Back4Sure: If you enable the option "Store relative path, if job file is in program directory" Back4Sure will only store the relative part of the path to the job file, if the job file is inside the folder where Back4Sure is located. This has the advantage, that Back4Sure will always find the job file from the recent file list, even if the drive letter of the removable media Back4Sure was started from has changed.

2.4 Automatic check for program updates

Back4Sure can automatically check for updates on startup. Here you can tell Back4Sure how often this update check should be performed. If you don't want Back4Sure to automatically retrieve version information, you can choose "Check for updates" from the help menu instead.

2.5 Language

Here you can select the language of the user interface. You'll have to restart the program for the changes to take effect.

2.6 Default settings for backup jobs

In general, all settings concerning a backup job are stored in the respective job file. Nevertheless it is possible to permanently alter the default settings for new backup jobs. Make all the changes to the job settings as required. It is also a good idea to define all filters that may be of use in job files. The filters will then be available in all new jobs that will be created. Now choose "File / Save As Default". Whenever you'll create a new job, all your settings and filters will be already present, then.

2.7 Location of the program settings

All program settings are stored in a file named "Back4Sure.ini", all default settings for new jobs are read from the file "DefaultJob.b4j". On each start, Back4Sure searches for those files in its own program directory. On success, those files are used. If the files do not exist in the program directory of Back4Sure, the program searches under "Application Data\Back4Sure" of the currently logged in user. If the settings cannot be found there either, internal defaults for all settings are used and you'll be prompted to save the current settings to one of the both possible places.

As all default settings are searched in the program directory first, it is easily possible to run Back4Sure from a removable flash drive. All settings can be stored together with the program on the flash drive, so you'll always carry your preferred settings with you. The profile folder of the currently logged in user makes more sense for fixed installations, as Back4Sure would need administrator access rights to write in its own program directory.

3. Settings for a backup job

The possible settings for a backup job consist of

- the folders to backup and the folders to exclude from the backup,
- the target directory,
- filters for the files to include and the files to exclude,
- the compression options,
- settings for files to delete during a cleanup run,

- confirmations for the backup and the cleanup operations,
- the actions to execute before and after the backup,
- and the desired logging action.

The following chapters will discuss the possible options for configuring a backup job.

3.1 Selecting the backup source folders

On the left side of the main window you can see a directory tree, showing all local drives of the type "Local Disk" and "Removable Disk". By clicking on the "+" sign in front of the drives and folders you can expand the tree to see the subfolders of the chosen branch.

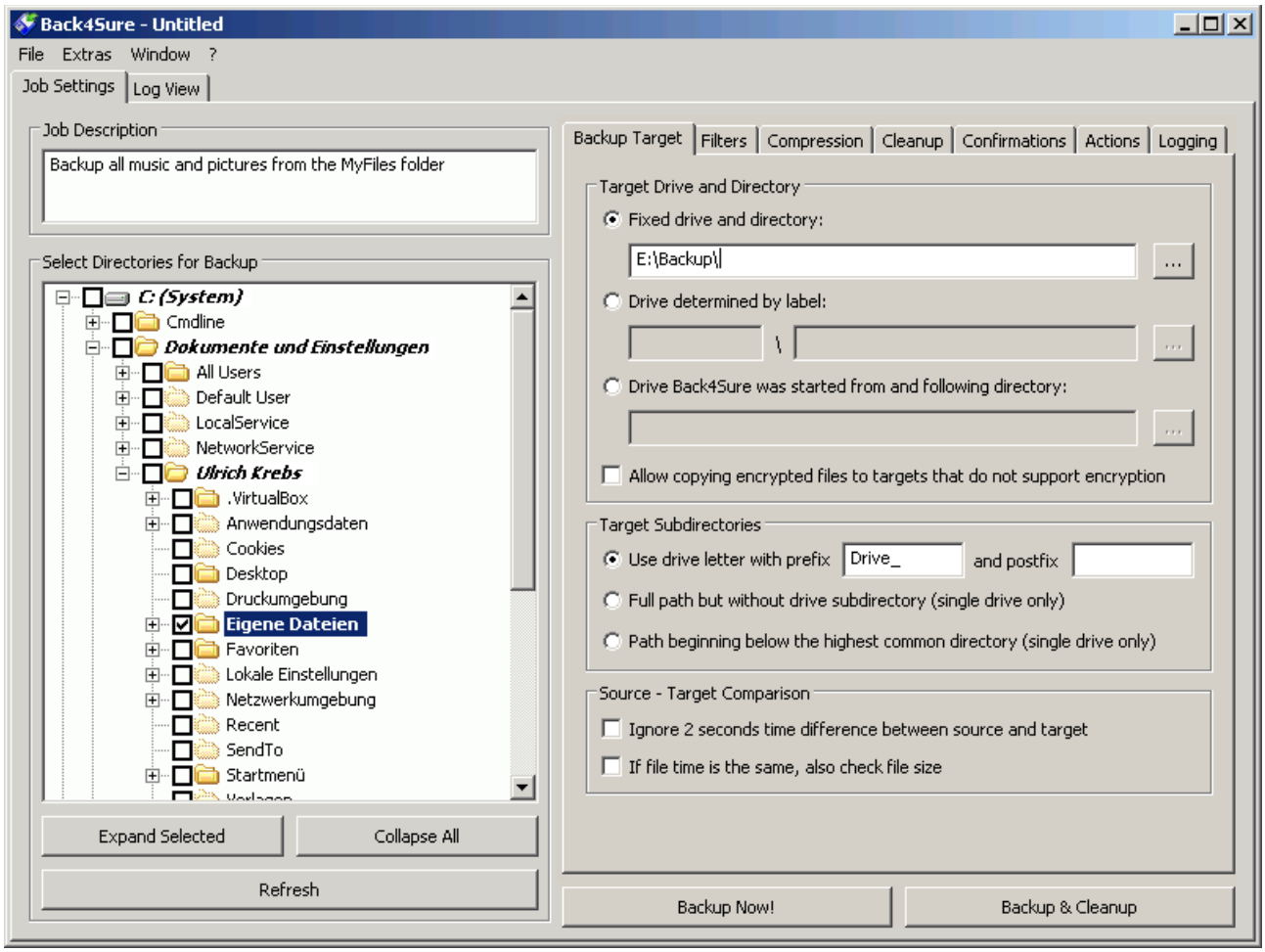

Figure 3.1: Selecting the backup source folders

The directory tree inside Back4Sure does not necessarily match the view you can see inside the Windows Explorer. This is due to the fact, that Back4Sure shows the real content of the drives, while the Windows-Explorer usually shows a filtered view. This may be confusing, as certain folders, e.g. "My Documents", are not where you may expect them. Nevertheless, all the files and folders are there. The folder "My Documents" e.g. is in fact located under "C:\Documents and Settings\<User Name>\My Documents".

Selecting the source directories for backup is quite easy: If you want to backup the complete folder including all subfolders, simply put a checkmark in front of that folder. With this, all folders below the chosen folder will also receive a checkmark. This is also valid for subfolders that are added after creating the backup job. If you want to explicitly exclude certain subfolders from the backup, just remove the checkmark in front of the unwanted subfolder. Removing the checkmark will again affect all subfolders.

Even if all folders are closed you can easily see, if some subfolders are selected for backup. Each folder that contains at least one folder marked for backup is displayed in bold letters. This way you can easily find out which folders are included in a backup set.

If you choose a complete drive for backup, you should exclude certain system folders from backup. Under Windows XP these folders are "Recycler" (the recycle bin) and "System Volume Information". Especially the latter may not be copied even with administrator rights. If you don't exclude these folders from backup, your other files will still be backed up correctly, but you'll receive error notifications that some files could not be saved.

3.2 Specifying the target directory

Of course, Back4Sure needs to know where to store the backup. Therefore it is essential to specify a suitable target directory. On the right side of main window you can see a tabbed dialog. Here you can set all options for a backup job. The first and most important allows the specification of the backup target.

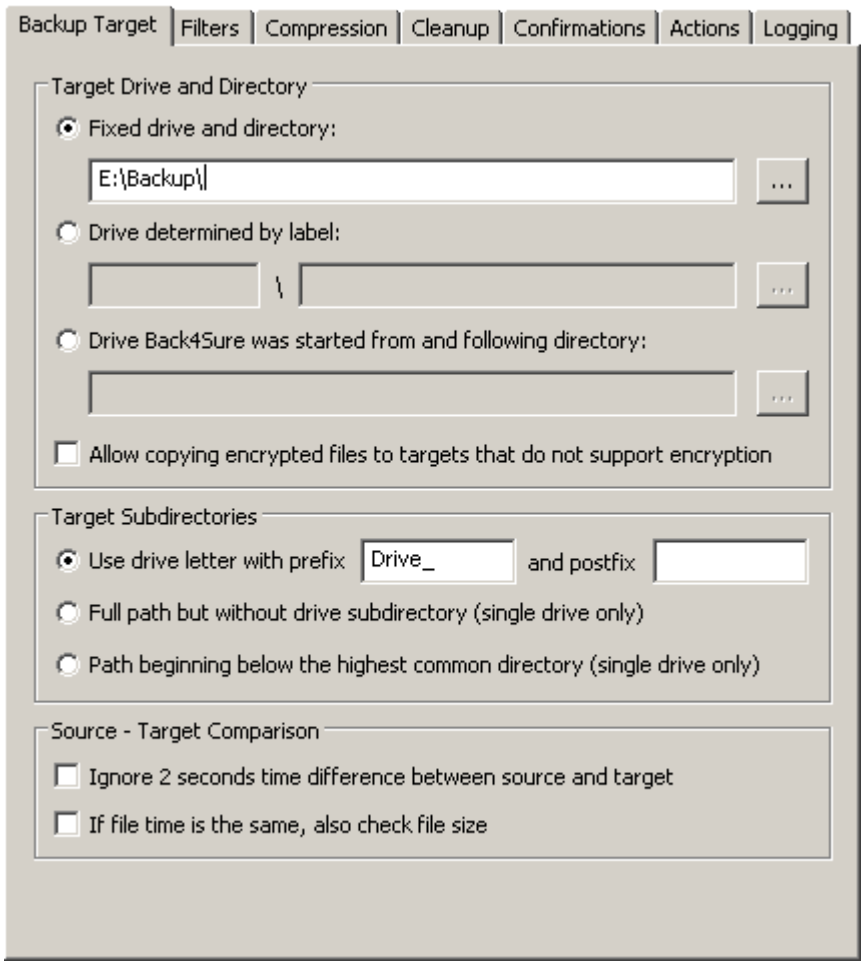

Figure 3.2: Specifying the target directory

In most cases, choosing a fixed drive and directory as target will be the right choice. A fixed drive is a drive which drive letter or UNC path does not change. Just activate the option "Fixed drive and directory" and click on the button with the three dots next to the edit field. A dialog pops up and allows to select a target drive and directory. Your choice will be entered into the edit field, then.

In fact Back4Sure has now all required input to perform the backup operation. After saving the job you can press the "Backup Now!" button to start backing up your data.. Still there are quite a few more options to tailor the backup process to your special requirements.

If you use an external disk via USB, FireWire or eSATA, it may happen that the disk receives different drive letters each time you connect it to your computer. In this case it is probably a better choice to select the second option "Drive determined by label" to specify the target drive. If you select this option, Back4Sure does not care about the assigned drive letter but searches for a disk with the specified disk label. For this function to work it is essential that the external drive has a unique name, e.g. "USB-Backup". You can easily change the drive label by opening "My Computer", selecting the drive and choosing "File / Rename" from the menu.

To select a drive with a certain label you can use the "..." button next to the edit field. In this case, Back4Sure automatically reads out the label of the selected drive and enters it into the edit field.

Finally you can also tell Back4Sure to use its own start drive as backup target by choosing the option "Drive, Back4Sure was started from and following directory". This way you can carry your backups together with Back4Sure on a removable media. Just plug the disk into the computer to backup and start Back4Sure right from that disk. You only need to specify a folder for the backup data if you use this option.

The option "Allow copying encrypted files to targets that do not support encryption" is useful, if you are using the encrypted file system (EFS) of Windows and still want to make a backup copy of your files to a drive that has no EFS, like a FAT32 formatted external hard drive. Normally, Back4Sure will refuse to copy EFS encrypted files to such a drive. If you enable this option, the files will be copied anyway. Be aware that the files on the external drive are not encrypted anymore!

As Back4Sure allows saving data from different source drives into on backup, each source drive will usually be stored into a different target subfolder. Back4Sure takes care about these subfolders and generates them automatically. With the default setting "Use drive letter with prefix and postfix", each subfolder will receive a name that contains the drive letter of the source drive. Additionally a prefix will be prepended and a postfix appended. By default, the prefix is "Drive_" while the postfix is empty. So data from source drive C: will be stored in a folder "Drive_C" on the target drive. If you want a different pre- or postfix or nothing at all, you may change it as required. Even if you leave the edit fields empty, still a subdirectory with the name of the source drive will be created in the target directory. If you don't want any additional drive subdirectory in the target, you may want to use one of the other two options for creating target directories.

The option "Full path but without drive directory" completely switches off the creation of drive specific subdirectories in the target directory. Still the complete paths of the source files are replicated in the target directory. This option may only be selected, if all source files originate from one single drive. If files from more than one drive are selected, the backup will not execute. Despite of this mechanism, this option is less safe than the option "Use drive letter with prefix", as it is still possible to run jobs with files from different drives into one target directory, possibly causing ambiguities. If one job e.g. backs up files from D:\Data and the other one from E:\Data, both saving into F:\Backup, the files from D:\Data and E:\Data will be mixed in the target directory. So please, use this option only if all backup jobs running into one target directory refer to one single source drive.

The last option "Path beginning below the highest common directory" will shorten the source path as much as possible, i.e. the common part of all source files will be discarded. If you plan to backup the "My Music" and the "My Pictures" folders from the "My Documents" folder, only these two folders will be created in the target directory. This option is the most unsafe one with respect to possible ambiguities. It should only be chosen, if there is exactly one job saving into one target directory.

Attention! If you plan to use one of the both options without drive directory, please *always* create a backup subdirectory on the target drive and *never* backup your data directly to the root directory! Otherwise, during a cleanup run, the whole contents of the target drive (except the backup of course) may be deleted. In general, I'd advise against using one these two options, as the benefit usually is disproportionate to the possible risks.

The option for ignoring a 2 seconds time difference between source and target can usually stay deactivated. There are certain constellations, though, where this option can be helpful, e.g. if you save your backup files on a network drive. If you notice that some files are backed up again and again though you know they were not modified between backups, try enabling this option.

With some programs it might happen that the file contents are changed while the file date and time remains the same. This can be useful for e.g. photo editing software, because this way after editing the photo, the file date is still the shooting date. To allow detecting those changes, you can enable the option "If file time is the same, also check file size". Back4Sure will then also backup those files that have the same modification date but a different size.

A brief note about the backup target: The best place to store your files is a drive that is not on the same physical disk as the source data. Of course, this requires a second hard drive in you computer. This second disk can be installed inside your computer or externally connected via USB, FireWire or eSATA. The reason why I recommend a second disk is easy: A common reason for data loss is a physical drive failure. If the disk is broken, a backup on the same disk won't help you. If the backup is on a second disk, you can easily transfer all your data back to a new disk. The best choice for your backups is an external disk that is only connected to the computer for the backup process. This way you'll not only be protected against hardware failure but in most cases also against malware (viruses, trojans) that may want to corrupt your data. The most comfortable way with highest performance is using a second internal disk, though.

3.3 Filter settings for including and excluding files

You may want to backup only certain file types, e.g. your text documents or your photos. Or it is the other way round: You want to save every file type but not videos, as these files consume too much space on the target drive. Back4Sure offers a sophisticated filtering mechanism to exactly specify the files you want to be included in or excluded from the backup.

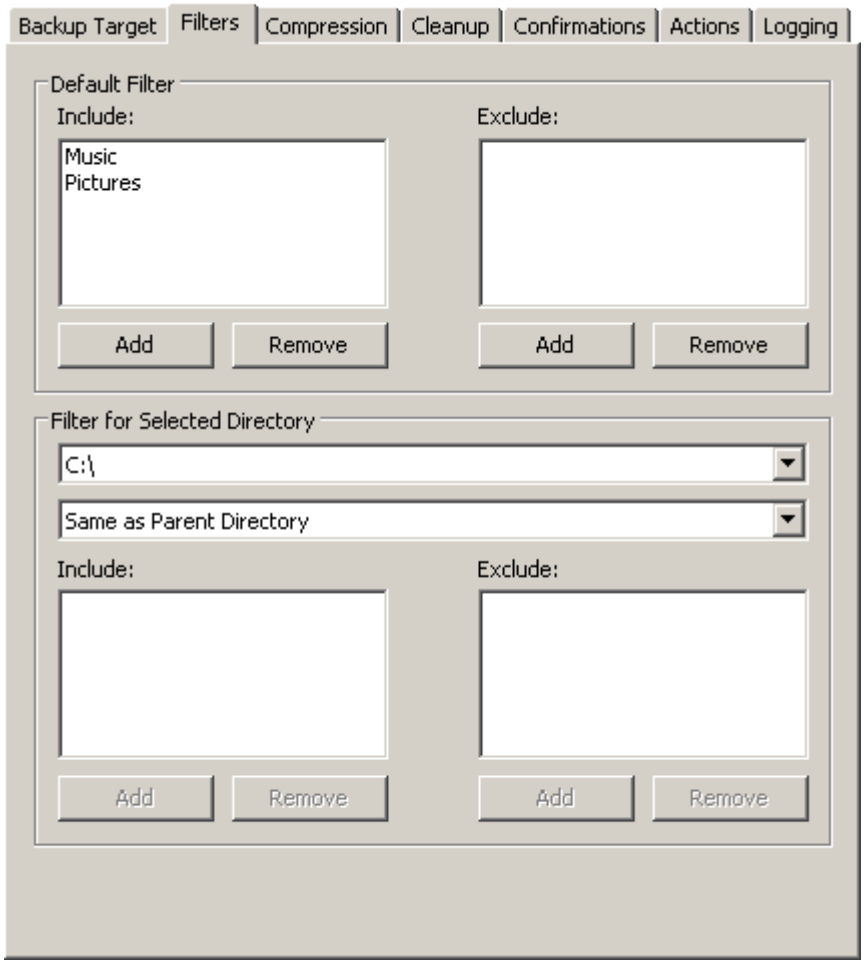

Figure 3.3: Filter settings

Each job has a default filter that is applied to all directories in case no other filter is defined. This filter is configured in the top half of the filter options window. By default, there is neither a filter for included nor excluded files. As a result, all files will be backed up and no file will be excluded. If you want to copy e.g. only your music files and pictures, you'll have to define one or more include filters. For this, press the button "Add" under the include filter list of the section "Default Filter". A window pops up then, allowing you to add previously defined filters to the include filter list.

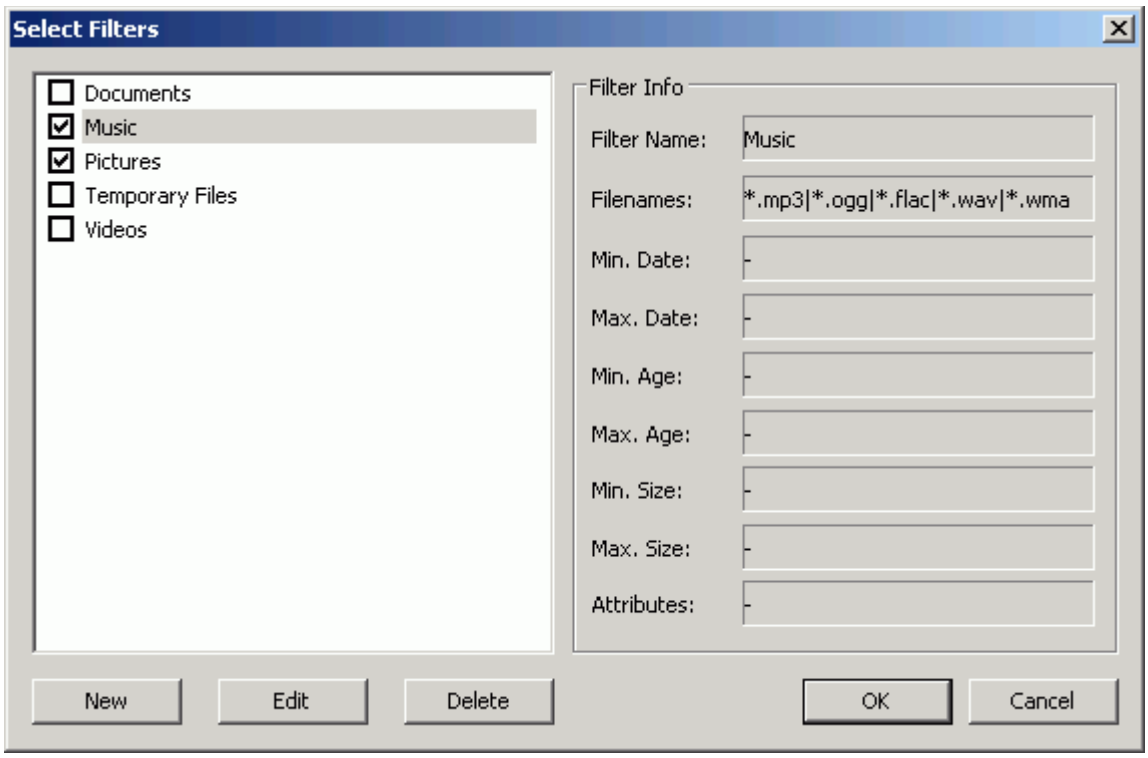

Figure 3.4: Selecting predefined filters

Back4Sure has a "built-in" set of default filters which you can modify or delete as required. Now select filters for the files you want to be included in the backup. Figure 3.4 shows a filter set to only include music and pictures. After selecting all required filters, close the window with the "OK" button. The names of the selected filters will appear in the include list of the filter options. If you didn't find a matching filter for your backup task, you may want to define your own filter. In the "Select Filters" window, press the "New" button. This will bring up the filter editor.

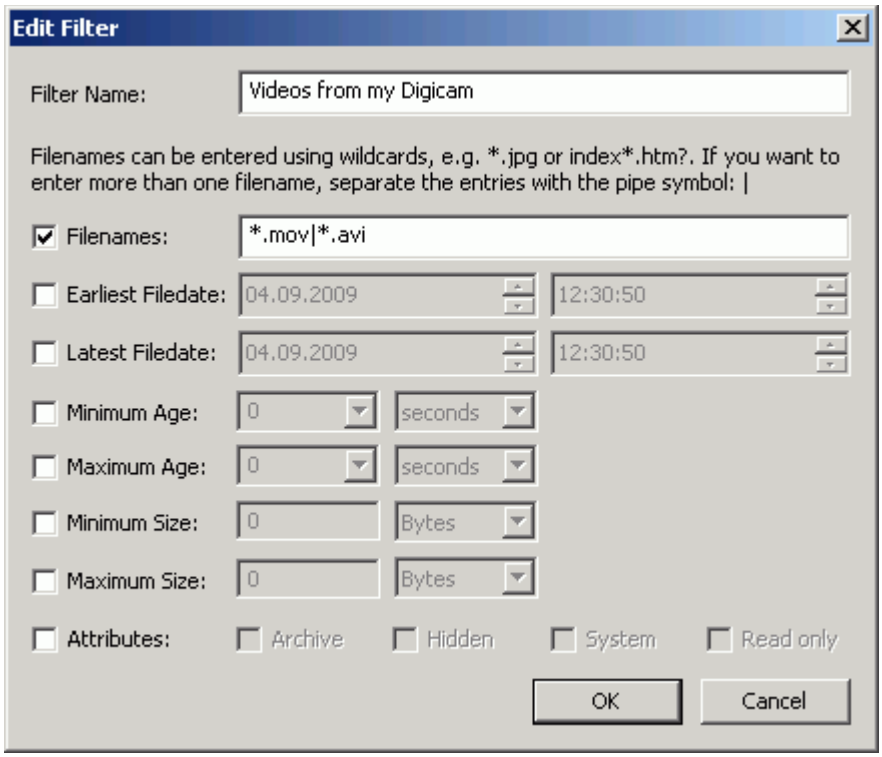

Figure 3.5: Creating a new filter

First you should give the filter a meaningful name, e.g. "Office documents" or "Photos from the last year". Now you can select and configure the filter options. Filtering works that way, that a file must match all selected filter options to pass the filter (AND relation).

The most common filter type is the filename filter. With this filter, you can select certain file types, e.g. jpg images or text files. To activate this filter, just put a checkmark in front of the option "Filenames". You can then define a set of filename patterns that a file must match to pass the filter. These patterns may consist of partial filenames and so-called wildcards. The wildcard "?" represents an arbitrary single character and the wildcard "*" represents any number of arbitrary characters. The pattern "index???.htm*" e.g. will accept the files "index001.htm", "index_ab.html" and "index1b7.htm00", but not the files "_index001.htm", "index0001.html" and "index123.htx". In most cases you'll probably only use the simple patterns of the kind "*.jpg", "*.doc" or "*.txt". With these kind of patterns you can easily select certain file types that are distinguished by their file extensions.

The input field for the filename patterns will accept multiple entries, that must be separated with the pipe symbol "|". Why the heck this strange symbol? Quite easy: This symbol may not appear in a filename, therefore no conflicts with a filename pattern can appear. On an US keyboard you can get this symbol by pressing Shift + Backslash (above the Return key).

The next two options will filter the files depending on their absolute modification date. The first option is for entering the lower date limit (i.e. the oldest allowed date) and the second option is for the upper date limit (i.e. the newest allowed date). Possible usage of this option includes selecting files from within a certain date range for archiving them on CD or DVD.

Instead of using an absolute date you can also specify an age for the files to select with the next two options. The first option is for setting the minimum age and the second one for the maximum age. With this option you can e.g. easily select the altered files of the last week for backup on a special disk.

In some cases it might be also useful to filter the files by size, e.g. to exclude very large audio or video files from backup to save space on the backup media. The options "Minimum Size" and "Maximum Size" are just for this purpose.

Finally, you can also use file attributes as filter criterion. A possible application is the selective exclusion of hidden and system files, which often cannot be copied and therefore produce backup errors. All selected attributes will be ANDed, so if you select the attributes "System" and "Hidden", only hidden system files will pass the filter. If you want to filter out files that are either system *or* hidden files, you'll have to define two exclusion filters, one for system files and one for hidden files.

If you have finished editing the filter settings, close the edit window by pressing "OK". The just defined filter will appear under the given name in the filter list of the "Select Filters" window. Be aware, that this filter will only exist in this backup job! If you want to have this filter available in all future jobs, just add it to the default job. To do this, open Back4Sure without loading a special job file and enter the new filter as described above. Then choose "File / Save As Default" from the menu. From now on, the new filter will be available in all new backup jobs. Already existing jobs will not be affected by this action.

Usually, defining a default filter is sufficient for a backup job. This default filter will be applied to all selected directories when executing the backup job. In special cases it might be useful to apply a different filter for certain drives or directories, which is fully supported by Back4Sure. As it doesn't really improve the clarity of a backup job, this option should be used sparingly, though.

To modify the filter options for a certain drive or directory, select the corresponding item in the directory tree. It will show up in the section "Filter for Selected Directory", then.

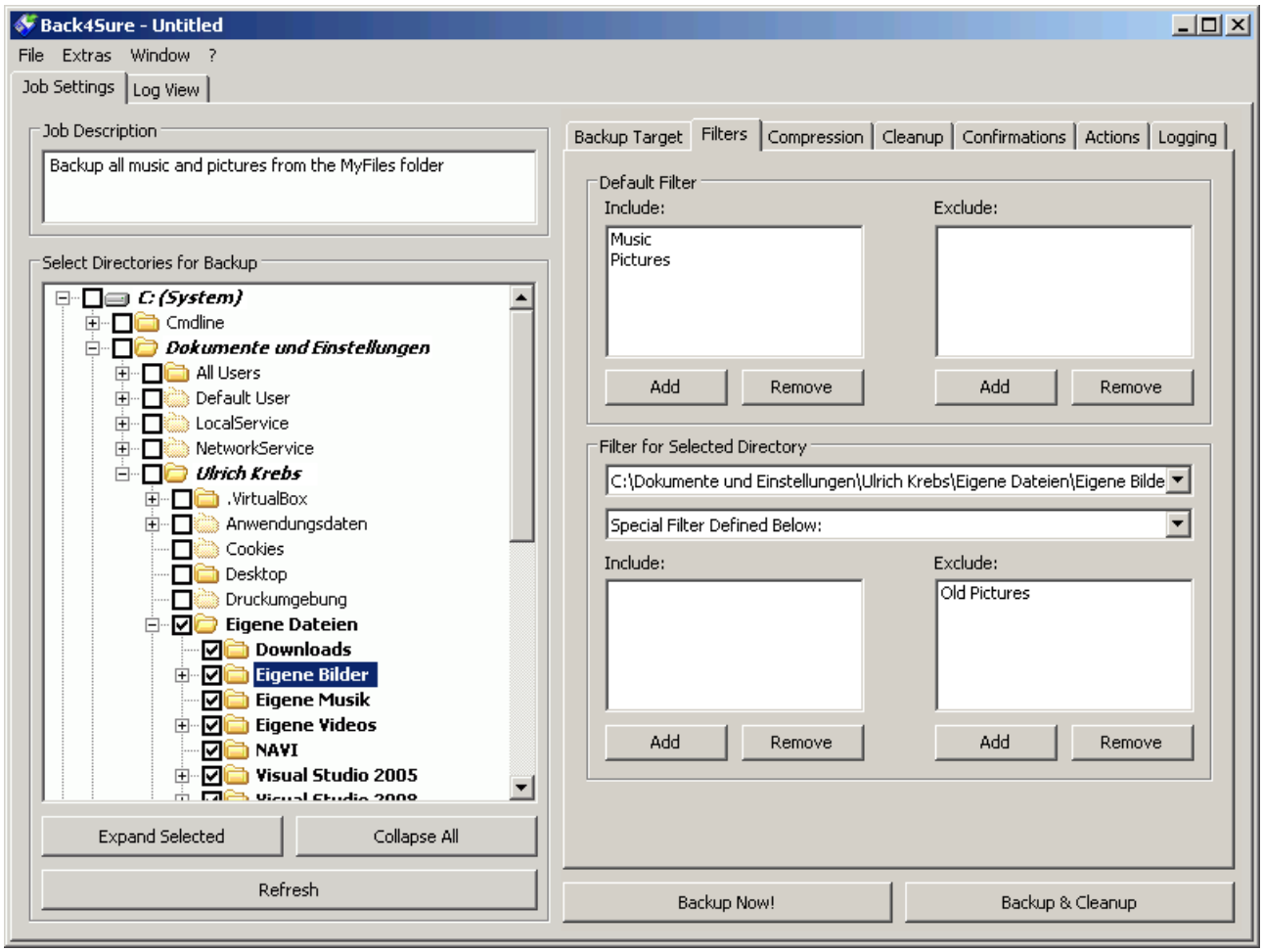

Figure 3.6: Special filters for selected directories

By default, a subdirectory (and all its descendants) inherits the filter rules from its parent directory. Therefore "Same as Parent Directory" is displayed below the directory display. If you want to assign a different filter to the selected drive or directory you can choose one of the other options. If you choose "Default Filter for this Job", the default filter displayed in the upper half of the filter options dialog will be applied. This only makes sense if the parent directory already has a filter set that differs from the default filter and the chosen subdirectory should use the default filter again. With the option "Special Filter Defined Below" you can define a completely different filter set for the specified directory and all its subdirectories. Specifying the alternative filter set works exactly like for the default filter set and is done in the lower filter lists for include and exclude filters.

The special filter sets for certain directories are not as easy to inspect as the default filter. To alter or delete those special filters, select the corresponding directory from the drop down list in the section "Filter for Selected Directory". All directories with special filter settings are listed here. After selecting the wanted directory, editing or deleting filters is done as usual.

As already mentioned, using complex filter rules for certain subdirectories affects the clarity of the backup job and should be used with care. In most cases it's better to only use a default filter.

3.4 Compression settings

Back4Sure has the option to compress the files for archiving. This will save space on the backup media. The amount of saved space strongly depends on the files to backup. While newer office documents, jpg images or mp3 music are very hard to compress, HTML or text files offer some reasonable option for compression. Considering the currently available hard disk sizes, using compression doesn't make much sense in most cases.

There are still some applications for the compression option, especially if you use a flash drive as backup media. By using compression you avoid writing a host of possibly very small files to the flash drive. Such an action would dramatically decrease the write performance from some MB/s to a few kB/s. Using compression will in this case massively increase the backup speed.

The compression option is also very useful, if you have deeply nested folder structures and / or very long filenames, as they might occur if you save web pages from the internet, and if you plan to save the backup to an optical drive (CD-R, DVD-R). This media has strong restrictions concerning directory depth and the length of filenames. Therefore directly saving your backup files might not be possible. If you choose the compression option, all the directories and long filenames will be hidden inside the backup archive and will not conflict with the media restrictions anymore. So depending on the actual backup process you'll have to decide whether compression makes sense or not.

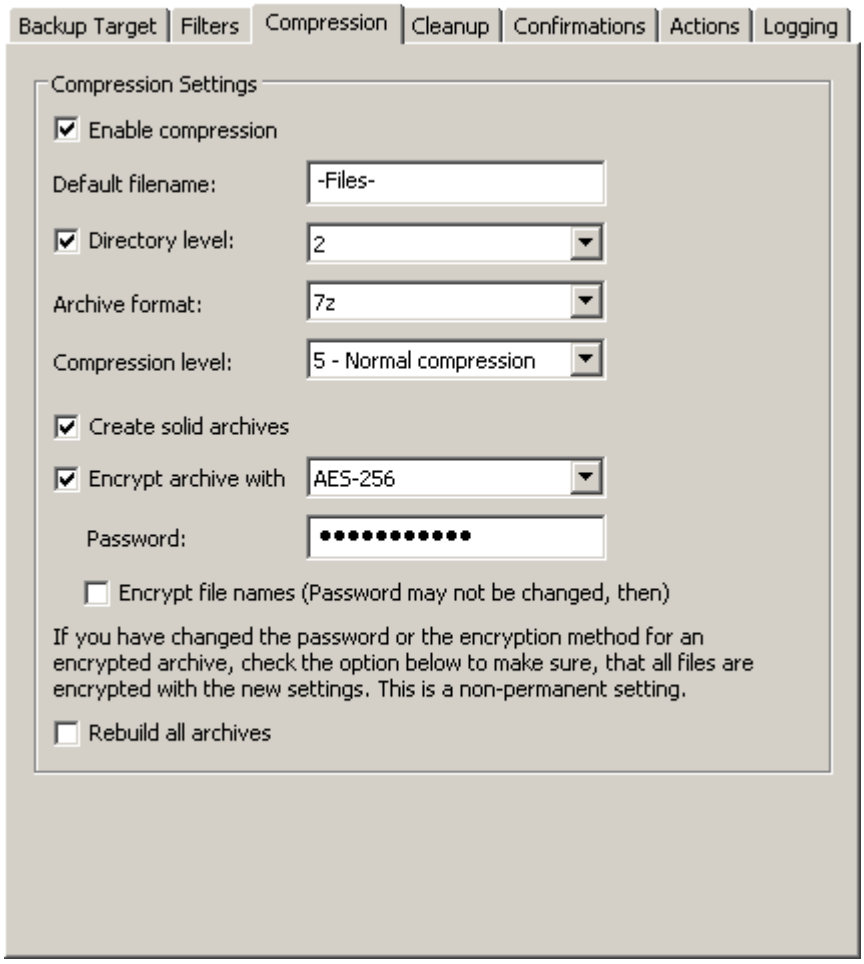

Figure 3.7: Compression settings

To activate compression for the current job, choose the option "Enable compression". No further settings are required, the defaults will usually give suitable results. Nevertheless, Back4Sure has some interesting options which are explained below.

The parameter "Default filename" is used to determine the name for all archives that contain only files but no further subdirectories. This may happen depending on your settings for the "Directory level". If you disable the "Directory level" option, *all* archives will be named as denoted here.

The "Directory level" setting specifies the directory depth from which on all further subdirectories are packed into one archive. If you deactivate this option, all non-empty source directories are created in the target and all files in each directory are packed into an archive named "-Files-.zip". So each folder in the target directory holds exactly *one* archive. This setting is optimal if the backup target is on an internal hard disk and you still want to use the compression feature. If you enable the option "Directory level", all source directories from the specified directory depth on (counted from the root directory) will be packed into an archive. If e.g. the directory level is set to 1, the folder "My Documents" including all subfolders will be packed into the archive "Drive_C\Documents and Settings.zip". If you set the directory level to 2, the files will be stored into "Drive_C\Documents and Settings\<User>.zip". By setting the directory level, you'll also configure the number of archives that will be created in the backup process. In general, it is better for data safety to have the backup split into several files. If one large archive is corrupted, all included files may be lost. If there are several small archives, just the files in the corrupted archive are affected.

Depending on the directory structure of your backup source and the properties of your backup target, it might makes sense to adjust the "Directory level" parameter. Common values are between 1 and 5. Bigger values will finally lead to a behavior as if the "Directory level" option was disabled.

Besides the common Zip format you can also choose the 7Zip format for compression. This format has usually a better compression ratio, but requires more computation time. Finally it's rather a matter of taste which format you prefer, there are only differences if you want to use special features, like file name encryption or solid archives, which are only available if you use the 7Zip format. If you use compression for very long and nested directory structures, 7Zip might be also the better choice, as all 7Zip capable programs are able to read the resulting archives. In contrast, older compression programs or the Windows explorer might not have support for Zip archives containing very long directory structures and unicode file names.

By choosing a compression level you have further control over the amount of disk space required for the backup. You shouldn't overestimate the effect of higher compression levels, though. Especially the highest compression level will rather dramatically decrease backup performance than saving further disk space. Therefore, compression levels beyond "5 - Normal compression" are usually not recommended.

If the amount of space required for a backup is of great importance, e.g. if you want to put the backup on a DVD, you can enable the option "Create solid archives". This option is only available if you choose the 7Zip format. With this option enabled, significantly smaller archives are created, unfortunately at the expense of failure tolerance. In solid archives the loss of a few bytes inside the archive, due to faulty backup media, may cause greater damage than in normal archives, i.e. more files inside the archive may be affected by the data loss. If used for backups on reliable media with limited capacity, e.g. flash drives, the solid option is still a great way to create smaller archives to save some space.

The following options are all used for archive encryption. To encrypt the content of your backup archives, activate the option "Encrypt archive". If someone gets unauthorized access to your backup, he will not be able to extract files from the archives without knowing the correct password. Make sure, you choose a safe password, i.e. one that consists of 8 or more upper and lower case characters and perhaps some numbers and

symbols.

You may also choose the encryption method. For Zip archives the available methods are ZipCrypto and AES-256, 7Zip archives are always encrypted using AES-256. AES-256 is generally considered as a safe method to encrypt files. So if your Zip program supports this encryption method, you should choose this one.

Despite content encryption, the file names are still accessible without knowing the password. As it is sometimes possible to draw conclusions just from the file names, it might be a good idea to hide them also. This option is only available if you choose 7Zip as archive format. File name encryption is also possible, if the backup archives already exist. Be aware that you cannot easily change the password for the backup archives after file name encryption. You'll first have to deactivate file name encryption using the old password and then activate it again using the new password. After changing the password it is also required to enable the option "Rebuild all archives" to ensure, all files within the backup are encrypted with the new password. If you forget to set this option after changing the password, all unchanged files of the backup archive will still be encrypted using the old password. The option for rebuilding all archives will automatically reset itself after a backup run.

3.5 Cleanup settings

After several backup runs, you'll probably have some orphaned files in the backup target, i.e. files that do not have a corresponding source file anymore. This happens, if you have chosen to delete or rename a source file. If you have renamed a complete source directory, there will be immediately a whole bunch of files with no corresponding source files. Those orphaned files still occupy space on the target drive and may cause confusion in case you want to copy some files back to the source drive. So it makes sense to do a cleanup run every now and then, to keep the target directory lean and clean. During this cleanup run, orphaned files will be deleted from the target directory, while no source file will ever be touched.

Attention! The cleanup settings should be chosen with care as there are several "cleanup levels" that will do a more or less thorough job. If misconfigured, you might end up with a cleanup run that deletes more files than desired. Especially if you have disabled the creation of drive subdirectories in the backup target, there is a potential risk of deleting other backups or even completely other directories from the target drive.

Depending on the chosen option for creating target directories (see chapter 3.2) the cleanup function works slightly different. This different behavior will be explained below.

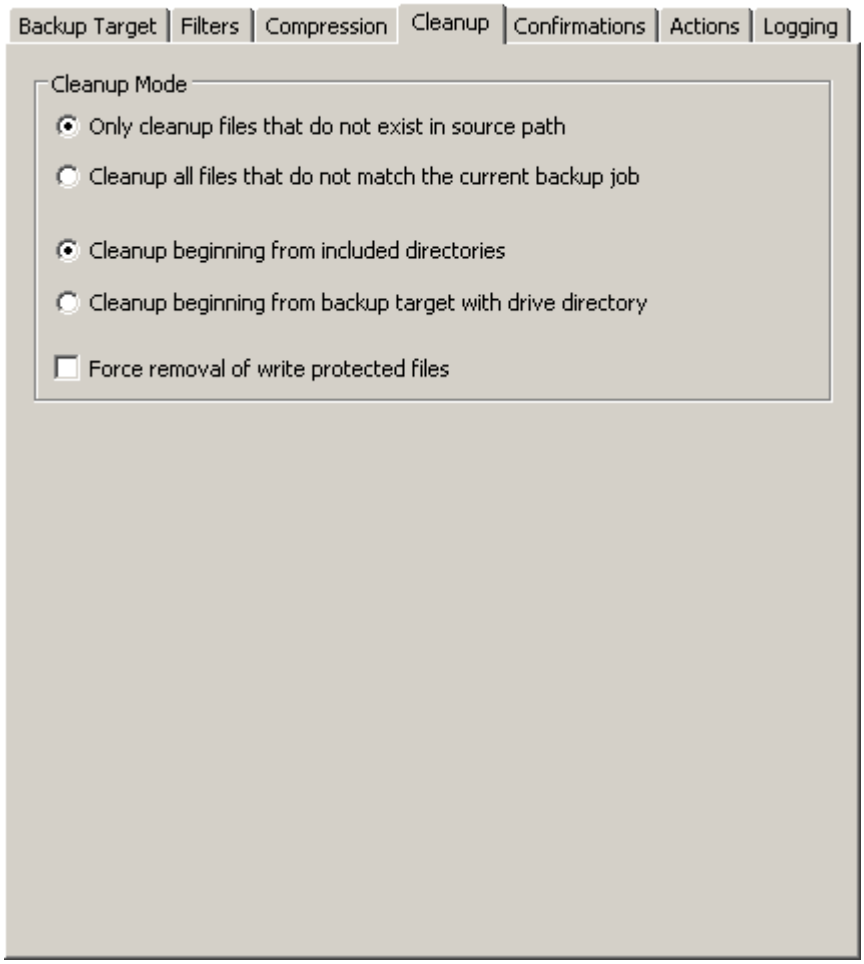

Figure 3.8: Cleanup settings

3.5.1 Cleanup operation, if the option "Use drive letter with prefix and postfix" is enabled

The following explanations are only valid if you didn't disable the creation of drive subdirectories in the backup target. Disabling the drive subdirectories is potentially unsafe and should be used with caution! The differences to the normal behavior are explained chapter 3.5.2.

Figure 3.8 shows the most conservative setting, where only files may be deleted that for sure do not have any matching source file anymore. This setting can be left as is, if you don't make any bigger changes to the backup job. If you remove top level directories (first directory with a checkmark) from the backup, alter the filter settings or change the directory level for compression, many orphaned files will be left in the target directory with this cleanup setting. You may want to select more aggressive cleanup settings then.

The first option specifies the files to delete. If "Only cleanup files that do not exist in source path" is selected, Back4Sure will only delete files during a cleanup run that definitely have no corresponding source file anymore. It doesn't matter if the target file doesn't match the currently selected filter set or if the source file is included in the current backup. If a source file for a target file exists, the target file will be kept. Choose this option, if there is more than one backup job for a certain source directory, e.g. only images from the "My Documents" folder and only documents from the "My Documents" folder.

The alternative setting "Cleanup all files that do not match the current backup job" will remove all files in the target directory that per job definition do not belong into this backup.

This will also delete files that may have a counterpart in the source directory but are due to filter rules or exclude options not part of the backup set. You can safely use this option, if this is the only backup job for a certain source directory, e.g. all files from the "My Documents" folder.

The second option determines the starting point for the search for orphaned target files. If you choose "Cleanup beginning from included directories" only orphaned files and directories below the top level include directory will be deleted. Files and folders of the same or higher level will not be touched. Choose this option, if there is more than one backup job for a certain drive, e.g. one job for "My Documents" and one for "Application Data" from drive C.

The setting "Cleanup beginning from backup target with drive directory" will start the search for orphaned files directly from the "Drive_X" folder, i.e. the topmost folder of the respective drive. This setting will also delete folders that were once top level include folders but were removed from the backup set. You may choose this option, if this backup job is the only job for a certain drive.

If a complete drive is removed from the backup set, there is no cleanup function that will automatically delete the "Drive_X" folder of the removed drive from the backup target. You'll have to manually delete the backup folder, then.

Finally there is also an option to enforce the removal of write protected files. In many cases the write protection originates from copying files from a CD or DVD to the hard disk. By default, Back4Sure will not delete write protected files during a cleanup run. By activating the option "Force removal of write protected files" you can allow Back4Sure to cleanup also write protected orphaned files .

3.5.2 Cleanup operation, if the option "Use drive letter with prefix and postfix" is disabled

If you have disabled the drive directory option, Back4Sure has to guess where the files in the backup target originated from. For this, the selected source directories of the current backup job are concatenated with the target subdirectories, i.e. some information from the backup job is required to obtain the source path from the target path of a backed up file. From this fact may arise problems if several backup jobs with a totally different file set, e.g. from different source drives, run into the same target directory. The bevavior of the cleanup function is therefore different if the usage of drive directories is disabled.

In general, the options for cleaning up the target directory will of course behave just as described in chapter 3.5.1, still there are some important points regarding the starting point of the search for orphaned files.

The option "Cleanup beginning from included directories" still starts just below the highest selected directory, but now this can be the main backup directory or even the root directory of the target drive, depending on the target options and the selected source directories. If you have selected e.g. the complete drive C: as backup source, the cleanup will now start directly in the main backup directory. If no backup subdirectory on the target drive is specified, the cleanup will start directly in the root directory of the target drive. This situation may also occur if you have selected a deeper source directory, e.g. the "My Documents" folder, and enabled the option "Path beginning below the highest common directory". In this case, everything above the "My Documents" folder, i.e. "C:\Documents and Settings\<User>, is discarded, so the starting point for a cleanup run is *always* the main backup directory. Consequentially, it's in most cases a good idea to create a subdirectory on the target drive just for holding the backup data, so no other files and directories may be affected from a cleanup run.

3.6 Backup and cleanup confirmation

During the first test runs of a new backup job, it can be helpful to get an overview of the affected files prior to the actual copy and cleanup action. Back4Sure can show you a list of files to copied and to be deleted, so you can easily verify your backup and cleanup settings.

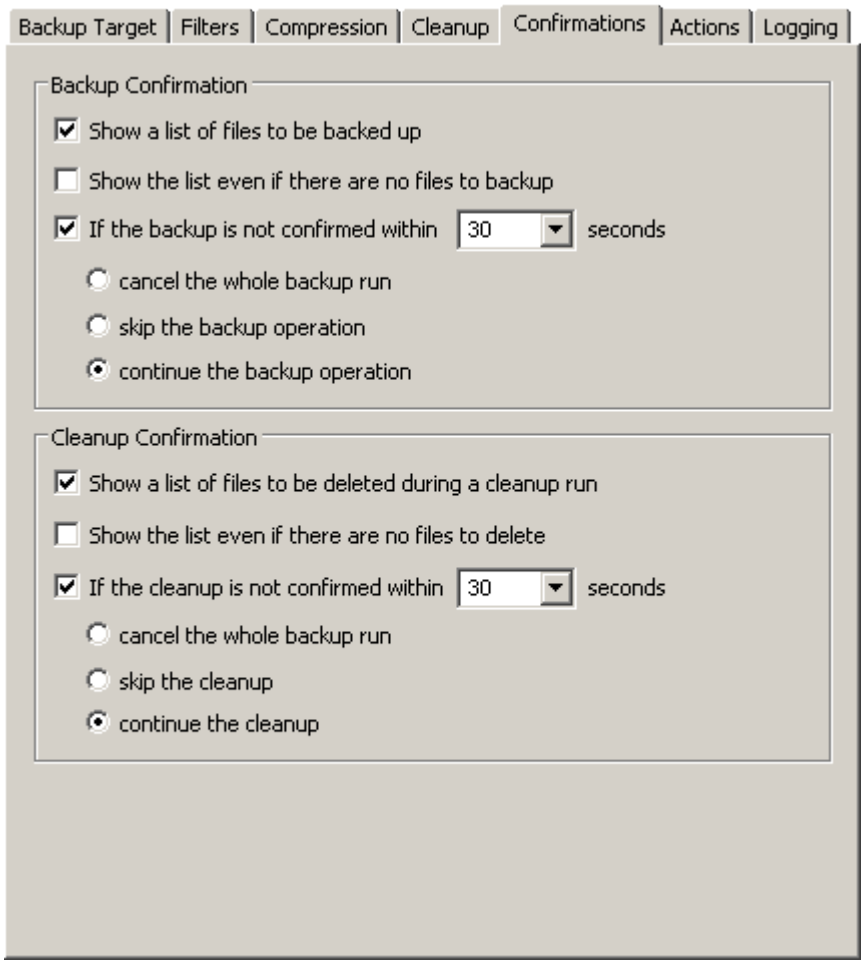

Figure 3.9: Options for the backup and cleanup confirmation

If you enable the option "Show a list of list of files to be backed up", Back4Sure will stop the backup right after comparing the source and the target directory and displays a confirmation dialog with all files that need to be copied.

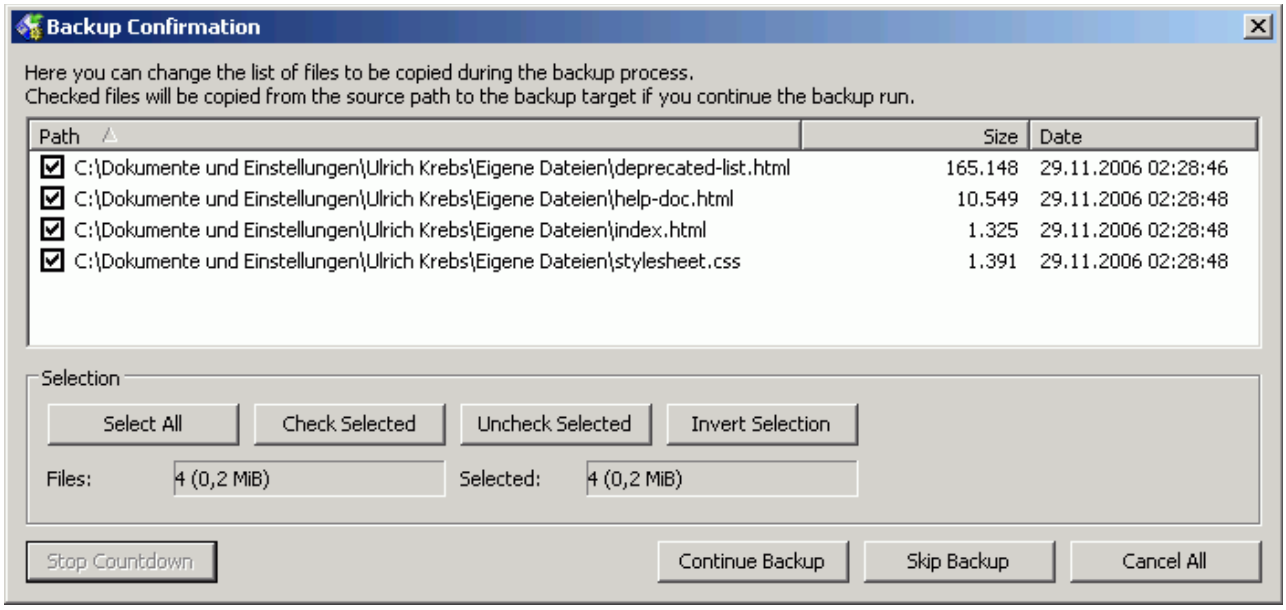

Figure 3.10: Dialog for confirming the backup

Within this dialog you can sort the list of files to be copied by name, size and last modification date. You can easily exclude individual files from the backup process by removing the checkmark. If you want to exclude all files of a certain type (e.g. *.jpg) or all files within a certain directory, *right* click on one of the files in question and choose the appropriate option from the context menu. Now choose "Check Selected" or "Uncheck Selected" to selectively include or exclude the selected files.

If you activate the option "Show the list even if there are no files to backup", the confirmation dialog will always appear, even if there are no files that need to be copied. The empty confirmation dialog can then be considered as a hint, that Back4Sure has digged through all your files and found out that actually no files need to be backed up.

If the setting "If the backup is not confirmed within x seconds" is deactivated, the confirmation dialog will block the backup run until manually confirmed. This is probably not wanted if you run an automatic backup. In this case, activate the mentioned setting and adjust the time Back4Sure should wait for a manual confirmation. You can also specify what to do after the specified time has elapsed without manual interception. If you choose the option "cancel the whole backup run", no further action is taken and the whole backup process will be aborted. If you choose "skip the backup", only the backup part will be skipped. If a cleanup is pending, it will still be performed. The final option "continue the backup operation" will automatically continue the backup process if the waiting time has elapsed. During the countdown for automatic continuation, the remaining time is displayed in the window title of the confirmation dialog. You can always stop the countdown and switch to the manual confirmation mode by clicking the "Stop Countdown" button.

The options for confirming a cleanup run have basically the same meaning as the options for confirming the backup operations.

3.7 Actions before and after the backup process

Back4Sure can be configured to execute predefined actions before and after the backup process. This can be e.g. cleaning up temporary files before doing the backup or sending a mail with the log file after the bakup. Actions are organized in two lists, one for all actions to execute *before* the backup one for all actions to execute *after* the backup. Back4Sure can also be told to wait until all actions are fully processed. This way, even long and complicated tasks can be accomplished without interfering with the actual backup job.

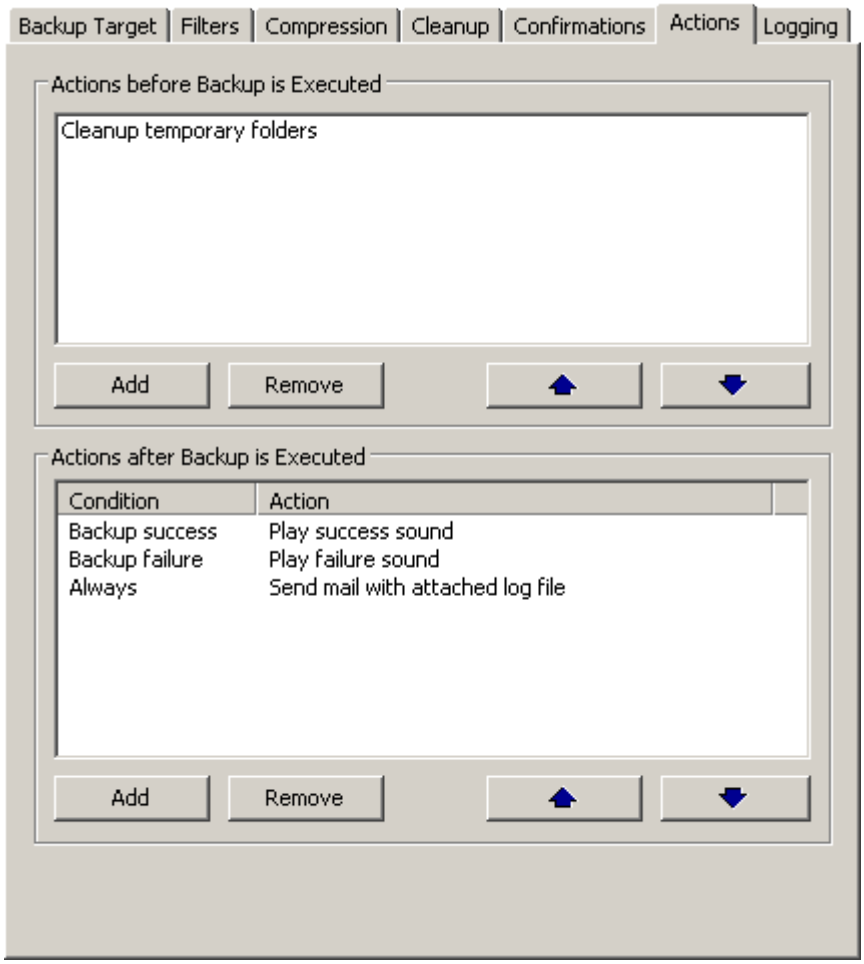

Figure 3.11: Defining actions before and after a backup run

The upper list holds all actions to execute before the backup, the lower list all actions to execute after backup. The entries of a list are processed from the top to the bottom. The order of the entries can be changed by selecting an entry and shifting it up or down using the arrow buttons. You can directly edit a task inside a list by double clicking an entry with the mouse. Keyboard operation is also possible: "Ins" adds a new action, "Del" removes the currently selected action and "Enter" opens the currently selected action for editing.

To enter a new action, click on the button "Add" inside the section "Actions before Backup is Executed". The dialog for selecting the new action will appear, then.

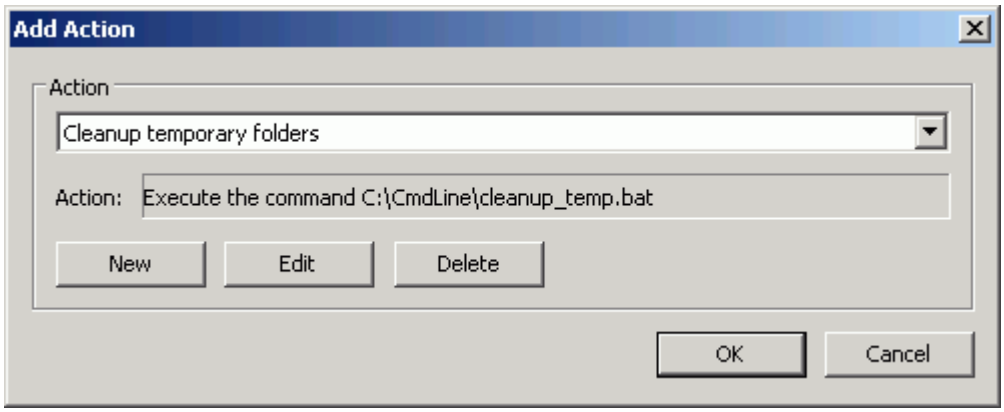

Figure 3.12: Adding a new action to execute before the backup run

Initially there are no actions defined, the dropdown box is empty. To add new actions, press the "New" button. There are three possible types of actions: Executing a command

(e.g. running a program or script), playing a sound and sending a mail. The dialog for entering a new action has tabs for each action type. By selecting one of the tabs you define the action type. Be aware, that only the entries on the activated tab will be taken into account for the just created action.

3.7.1 Action "Execute Command"

Figure 3.13 shows the input for editing a command. A command is often just a program or script to execute. By executing a command nearly all possible tasks can be accomplished, only the given command determines what finally happens. If you are familiar with scripting languages like VBScript, you can also easily define your own commands to be executed here.

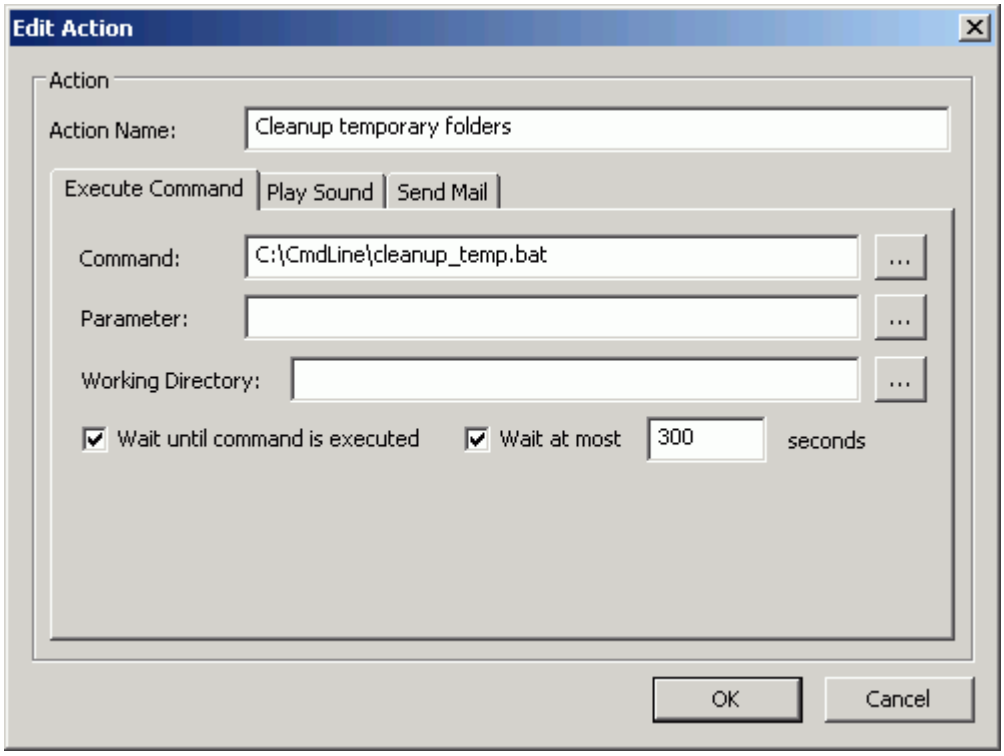

Figure 3.13: Creating an action for executing a user-defined command

The program or script to execute is entered into the "Command" field. You can also use the "..." button to directly select a program or script file. If the program requires parameters, e.g. a file name or command line switches, you can enter them in the "Parameter" field. Again you can use the "..." button to select a file as parameter. The last input field is for specifying a working directory for the program. Some programs require this info, if they work with relative paths. In most cases this field can be left empty, though.

If you call a program or script, it will require more or less time to accomplish the given task. Usually it doesn't make sense to continue with the backup operation, while the command is still executed. If you are e.g. cleaning up temporary folders first, this task should be finished before you start the actual backup process. To ensure that the command has finished execution, you can activate the option "Wait until command is executed". You can also activate the option "Wait at most X seconds" if you want the backup to continue, even if the command did not finish within a sufficient time interval, e.g. due to a failure condition. Without this option, Back4Sure will wait infinite for command completion.

After you have created the new action, you should give it a meaningful name. Later on, this name will be used in the dropdown box of figure 3.12 and in the lists of actions in figure 3.11.

3.7.2 Action "Play Sound"

Back4Sure allows playing WAV sounds without starting an external media player. If you want Back4Sure to make some noise before or after the backup, just choose "Play Sound".

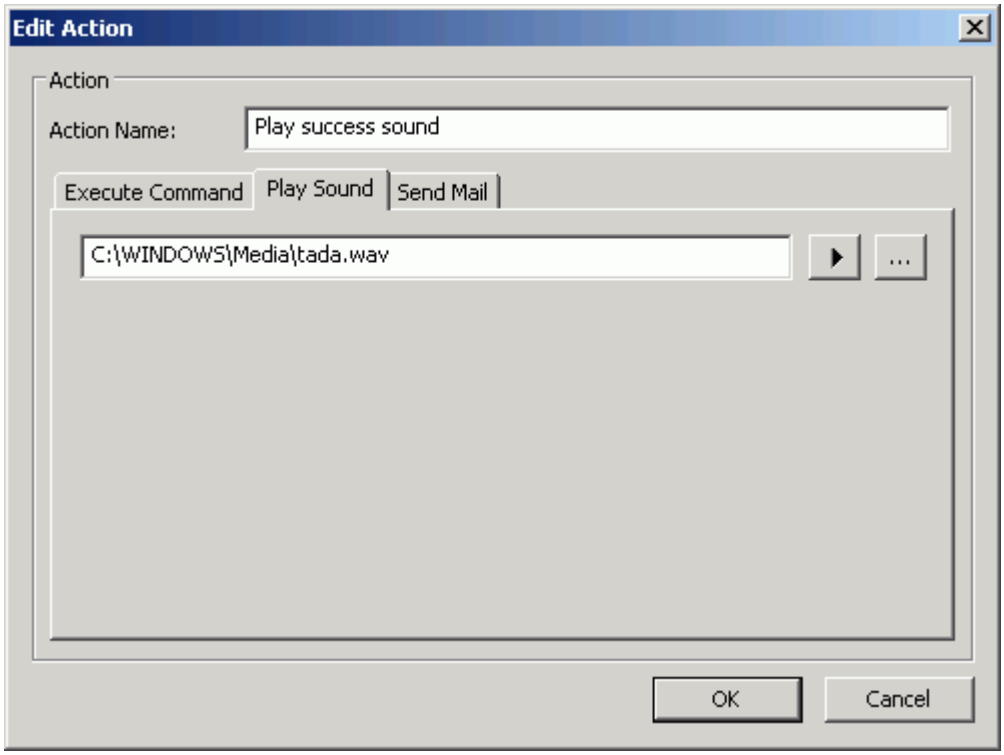

Figure 3.14: Creating an action for playing a sound

The input form has not much to explain. Just use the "..." button to select a WAV file. Use the "Play" symbol to listen to the just selected sound.

3.7.3 Action "Send Mail"

Finally you can also instruct Back4Sure to send you an email. As Back4Sure has an internal mail engine, no external program is required. The mail engine can connect to any SMTP server and handles common authentification methods.

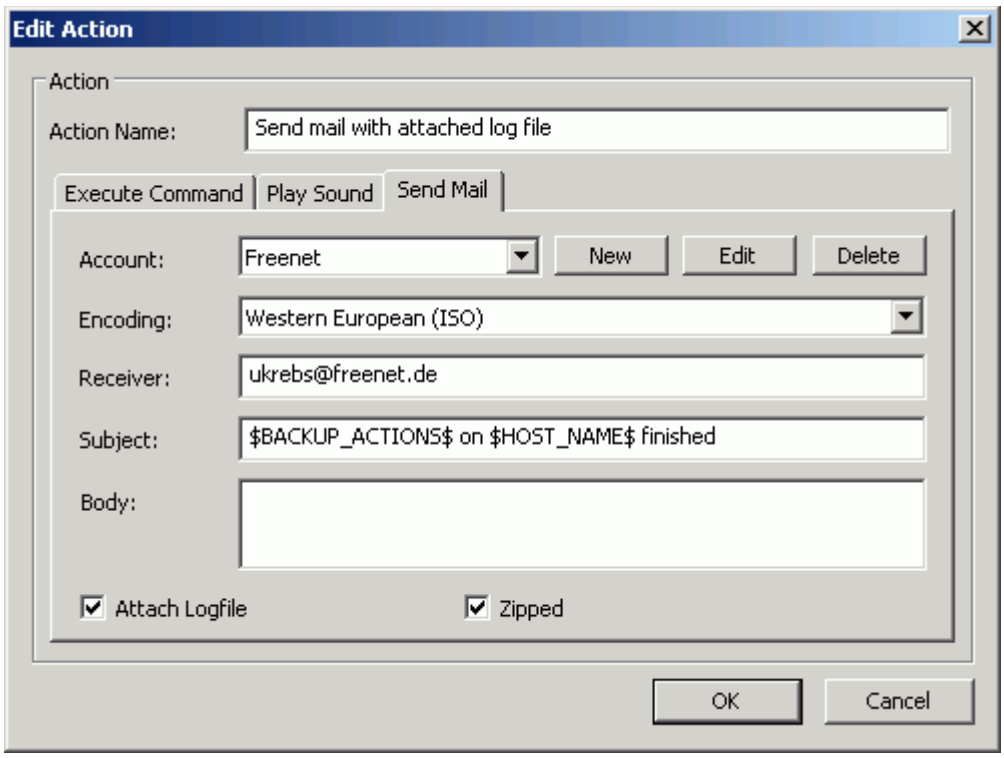

Figure 3.15: Creating an action for sending a mail

To send an email, you'll have to configure the SMTP server access first. Next to the dropdown box for choosing an account is a "New" button to specify a new mail account. If you press this button you'll see the input form for creating a new account.

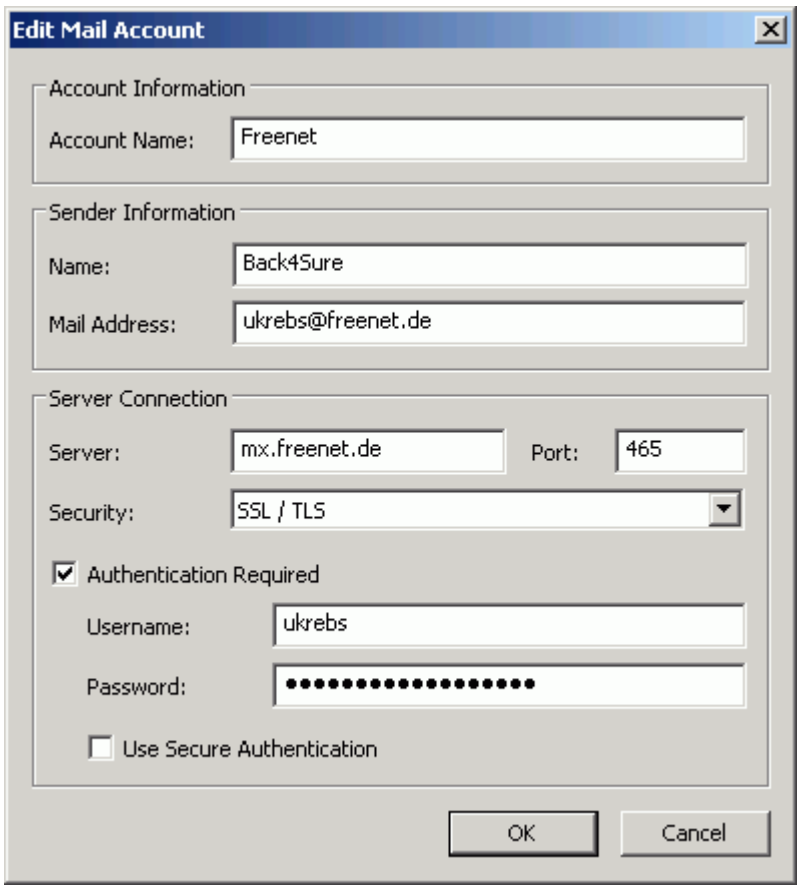

Figure 3.16: Creating a mail account

The first thing to do is to specify an account name. This is the name that will appear in the

dropdown box in figure 3.15. You should enter the name of your mail provider or the mail address associated with this account. The next thing to fill in is the sender information. I suggest to use "Back4Sure" as sender name, as it is easy to recognize if you receive an automatically generated mail from your backup program. The sender address should be set to the regular mail address of this account. Some provider do not allow bogus addresses as sender, so the mails may not be sent if the sender address is incorrect.

Of course you'll also have to specify the address of hte SMTP server to use. Just enter it in the "Server" field. The port number is usually determined by the selected connection security and can be left unchanged. Now choose the security setting for server connection. Possible choices are "None", "STARTTLS" and "SSL/TLS". Be aware that not all servers support all security options. In most cases, authentication is also required to get a server connection. Activate the option "Authentication Required" and enter your user name and password. If you also activate "Use Secure Authentication", your login details will always be transferred encrypted to the SMTP server. Again, not all servers do support secure authentication. You should always do a supervised test run before running automated backup jobs unattended.

After entering the new mail account, you can select it from the dropdown box shown in figure 3.15 and continue configuring the actual mail content. The default setting "Western European (ISO)" for the encoding will usually be correct, except you want to send mails in languages with special character sets. The rest should be quite clear: "Receiver" holds the mail address for sending the mail to, "Subject" holds the subject line and "Text" the mail body.

A pure static mail is probably not very informative (except that you'll see that the backup job was executed). Therefore, Back4Sure offers some dynamically generated information to be included in the mail contents. The first and most important option is to attach the current log file to the mail. For this, just activate the option "Attach Log File". As log files can be quite large, you can tell Back4Sure to zip the log file before sending it by activating the "Zipped" option, which will reduce the size of the log file to something around 50%. Attaching the current log file makes of course only sense, if the mail action is executed *after* the backup process.

A further option to create dynamic content is the usage of "place holders", i.e. certain key words which will be replaced by their respective contents at run time. Figure 3.15 shows such place holders in the subject line. The two key words enclosed by the dollar symbol $BACKUP_ACTIONS$ and $HOST_NAME$ will be replaced just before sending the mail perhaps by "Backup and Cleanup" and "OFFICE_COMPUTER". These key words will not only work when sending a mail but also in all other input fields of all possible actions. Section 3.9 will explain the available key words.

3.7.4 Conditional execution of actions after a backup run

Adding actions to the lower list which holds the actions to execute *after* the backup works nearly the same way as with the upper list. As the backup is now already finished, actions can be bound to the backup result. This means, the actions will only be executed if the execution condition is met, e.g. if the backup was successful. Possible conditions are "Execute always", "Execute on backup success", "Execute on backup failure" and "Execute on following exit codes".

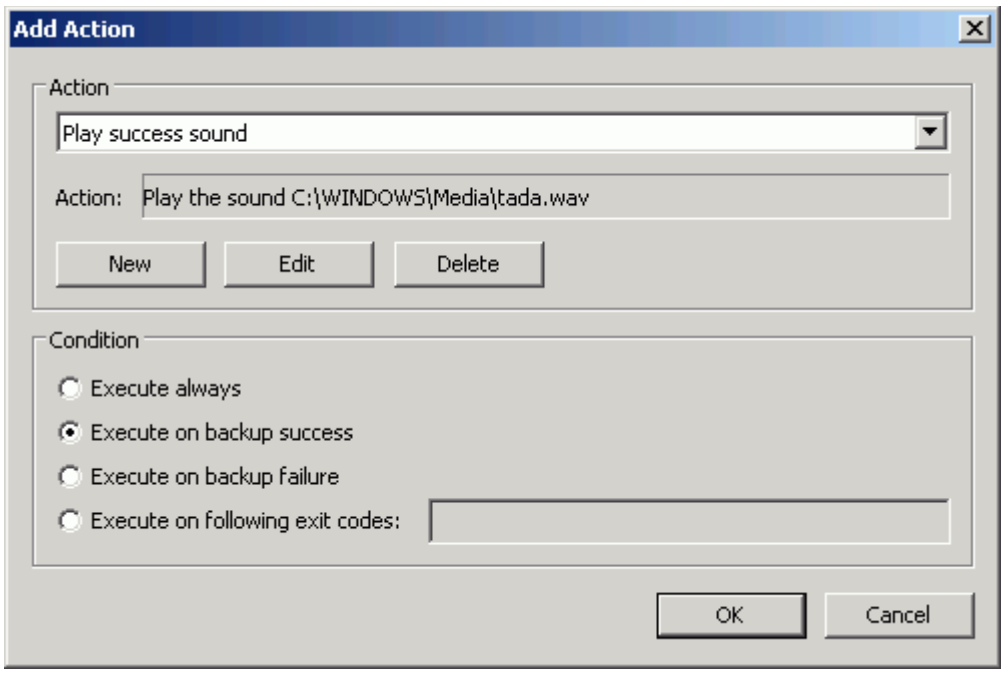

Figure 3.17: Adding a conditional action

You can choose the condition that must be met for the action to execute. If you choose "Execute on following exit codes", you can specify exactly which exitcodes are required. You can also specify more than one value separated by commas or even a range of values by entering the start value, a minus sign and the end value, e.g. "1-5". The list of possible exit codes can be found in the table in chapter 5.2.1.

3.8 Creating log files

Back4Sure will create a log file for each execution of a backup job that holds information about events that occurred during backup. With the logging options you can specify the detail level of this information and the storage location for the log files. The filename of a log file is created from the name of the backup job and the execution date and time using the following scheme: jobname_yyyy_mm_dd_HH_MM_SS.log. Log files are plain unicode text files and may be opened with any unicode capable text editor, e.g. Notepad. For optimal functionality log files should be associated with with your favorite text editor. To create this association, double click on a log file from within Explorer and follow the instructions on the screen, if the log file doesn't already open in a text editor.

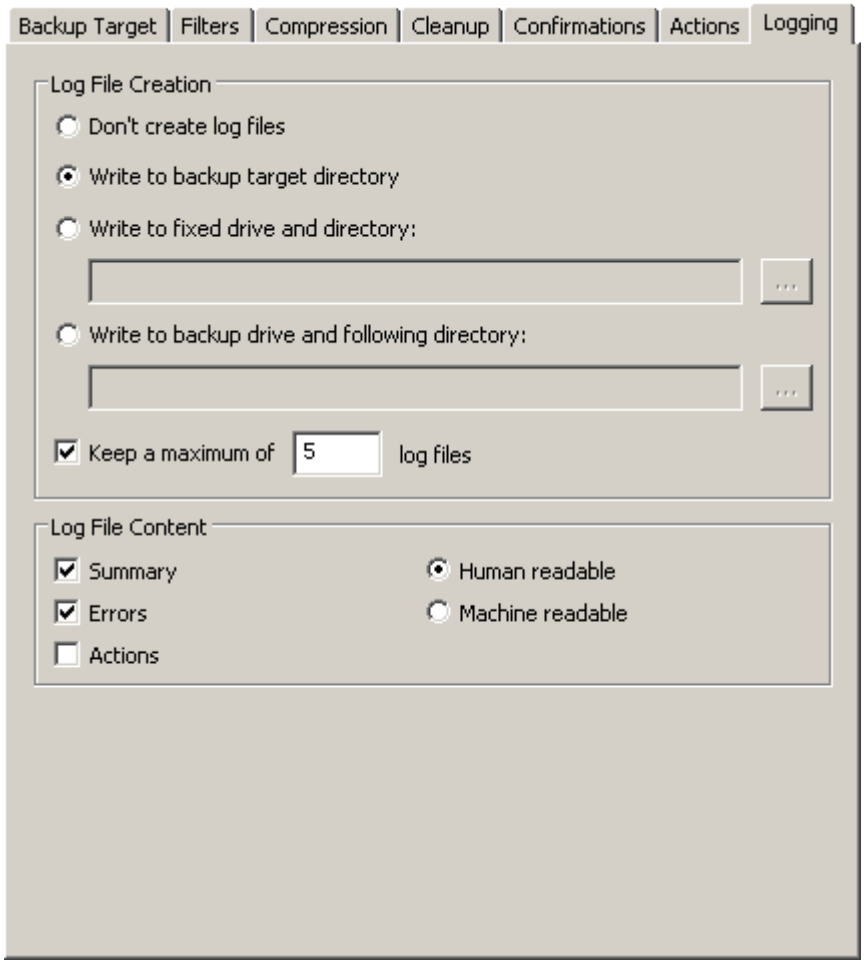

Figure 3.18: Settings for creating log files

In section "Log File Creation" you can specify if, where and how many log files are created. If you choose "Don't create log files", all logging functions are disabled. The default setting "Write to backup target directory" will create a log file each time the current job is executed and write it to the target directory specified in the "Backup Target" options. Alternatively, you can choose "Write to fixed drive and directory" to put the log files always into the same directory somewhere on your computer. The last option "Write to backup drive and following directory" will put the log files into the separate directory on the target drive.

Attention! If you have disabled the drive directory option in the target settings, you should not use the backup target directory for storing log files, as the log files may get deleted during a cleanup run. It's a better choice to store the log files in a separate directory on the target drive, then.

By default, the last five log files will be kept. If there are more than five log files, the oldest ones will be deleted. You may enter a different value for the number of log files to keep or even disable automatic deletion at all. To do so, just remove the check mark in front of "Keep a maximum of X log files".

You can specify the events to log in section "Log File Content". It is recommended to include at least the summary information into the log content, as this part holds the most essential information about the job execution. It is also useful to have the errors listed in the log file, as you can easily see which files weren't saved and also the reason for the failure. Sometimes it might be useful to keep a log of all actions that were performed during backup. If this option is enabled, each action, i.e. each copy or delete operation, will create a log file entry. Be aware that the resulting log file might grow very large, at least at

the first backup run.

Log files may be created in two different formats: The normal human readable format or a format optimized for automated analysis. In the human readable format, most entries of the log file are easy to read and interpret. On the other hand, the machine readable format writes log files in a standard ini-format, that can be easily read by other programs, but are rather hard to read if opened in a text editor. If you do not plan to use an automated analysis of the log files, the human readable format is the better choice.

Hints on the interpretation of log files can be found in chapter 5.2.

3.9 Usage of key words

Back4Sure allows the usage of key words in some input fields, e.g. in the "Target Drive and Directory" fields or in all fields describing an action to execute before or after a backup. The key words in the input fields will be replaced by their actual content at run time. This way, the behavior of a backup can be changed depending on the current conditions of the running backup job. You can e.g. dynamically create the subject of a mail that is sent after a backup run or you can backup your files to different target directories, depending on the current day of the week.

Especially if you use key words within the target definition, you should take care that the resulting backup process matches your expectations. If you include the backup starting time into the target definition, every backup will create a separate directory and always a full backup is performed. If you include just the day of the week into the target definition of a daily backup, only seven directories will be created and the eighth backup will be incremental again.

For the storage location of the log files you should also consider that not all key words may be translated without actually running a job. If you configure Back4Sure to save the log files into the target directory, but the target definition contains the start time of the backup job, the log files will not appear in the log view, as the target directory cannot be determined anymore. In this case, it is more appropriate to save the log files in a separate fixed directory on the target drive.

Following key words are understood by Back4Sure:

Key Word	**Description**
APP_PATH	Directory from which Back4Sure was started
APP_DRIVE	Drive from which Back4Sure was started
JOB_NAME	Name of the currently loaded job
$JOB_DESCRIPTION$	Description of the currently loaded job
$HOST_NAME$	Name of the host computer Back4Sure is running on
$LOGFILE_PATH$	Full path of the log file
$BACKUP_STARTTIME$	Starting time of the backup in the format "Year-Month-Day, Hour-Minute-Second". A different formatting is possible (see below)
$BACKUP_ENDTIME$	Ending time of the backup in the format "Year-Month-Day, Hour-Minute-Second". A different formatting is possible (see below)

$BACKUP_DURATION$	Duration of the backup in the format "Hours-Minutes-Seconds"
$BACKUP_ACTIONS$	Backup actions, either "Backup" or "Backup and cleanup"
$BACKUP_RESULT$	Numerical return value of the backup run (0 if there was no error)
$BACKUP_TEXTRESULT$	Return value of the backup run as text message

When using the date related key words, you can specify a different time format by entering a formatting string right after ...TIME and before the closing dollar symbol. The formatting string is composed from the following variables:

Variable	**Description**	**Example (21.08.2010, 15:36:38)**
%y	Year (two digits)	10
%Y	Year (four digits)	2010
%m	Month of the year	08
%b	Short name of the month	Aug
%B	Full name of the month	August
%d	Day of the month	21
%j	Day of the year	233
%W	Week number	33
%a	Short weekday	Sa
%A	Full weekday	Saturday
%H	Hour (24 hour format)	15
%I	Hour (12 hour format)	3
%p	AM/PM display	PM
%M	Minutes	36
%S	Seconds	38

If you want to include for example only the time part of the backup ending time, you can specify the new formatting by entering $BACKUP_ENDTIME%H:%M:%S$.

All numeric date values will be displayed with their respective maximum number of digits, filled up with leading zeros if necessary. So in January the variable "%m" will be translated to "01". If no leading zeros are required or wanted, you can switch them off by inserting a "#" right after the percent sign. The output "Saturday, 15.8.2010, 15:36" from the example in the table above can be achieved with the formatting string: %A, %#d.%#m.%Y, %H:%M

4. Executing the backup job

The following chapters will explain how to execute a backup job and to run and control Back4Sure from the command line.

4.1 Backup

After configuring a backup job as explained in chapter 3, you are now ready to perform the backup operation. If you didn't already saved the backup job, you should do it now giving it a meaningful name. The name of the job is required for creating the log file.

Just click on the "Backup!" button to start the backup operation. You'll see the progress dialog for the running backup, then.

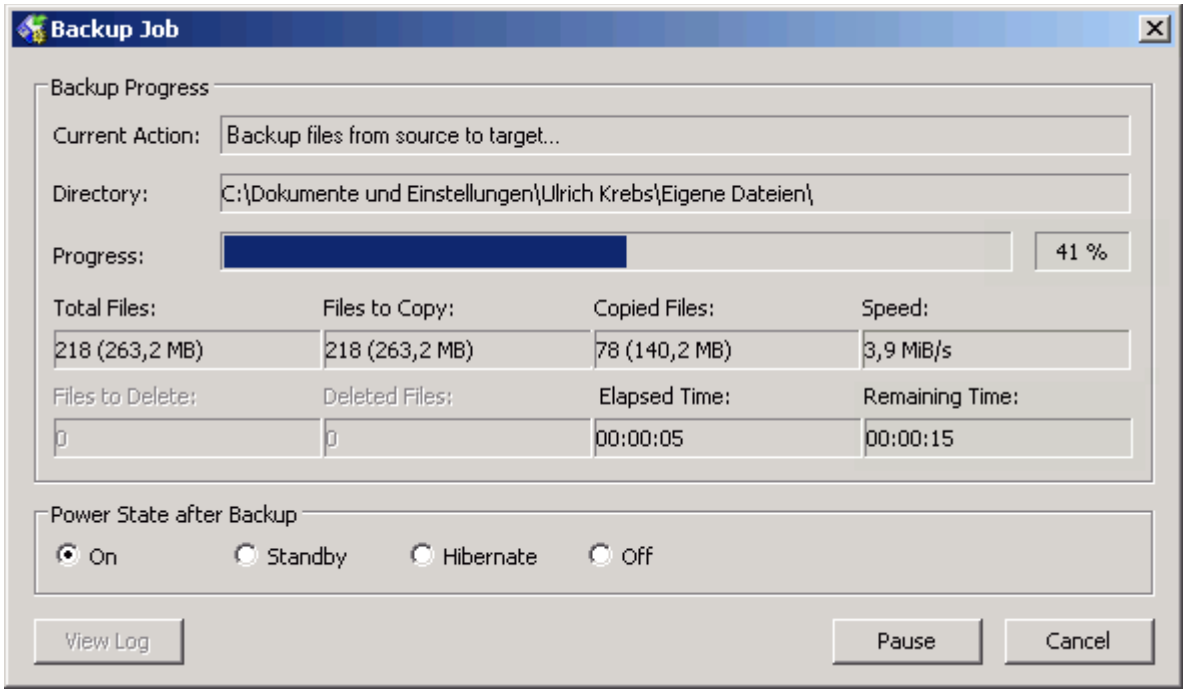

Figure 4.1: Progress dialog for the backup operation

The field "Current Action" shows the currently running stage of the operation. A backup operation is divided into three stages:

1. **Scanning source directories...**
   All source directories are searched for files that meet the selected backup rules.
2. **Checking for outdated files...**
   The target directory is scanned and a list of files to copy is created.
3. **Backup files from source to target...**
   The files from the previously created list are copied from the source to the target directory.

During the first two stages the progress bar doesn't move, as Back4Sure first has to know how much files need to be copied. During these stages, the fields "Total Files" and "Files to Copy" will tell you how many files are included in the backup set and how many of them need to be copied. Additionally, the "Directory" field displays the currently processed folder. During stage three, the progress bar will indicate how much of the data is already backed up.

During the whole process, you have the chance to pause or cancel the backup operation using the corresponding buttons at the bottom of the progress dialog. If you press the "Pause" button, the job will be paused immediately. This can be useful if you are about to copy some files to a slow backup media by hand or if you temporarily require to have the full computational power. You can continue the job later by pressing the "Continue" button. By pressing the "Cancel" button you may also abort the whole backup operation.

While the files are backed up, you can instruct Back4Sure to shutdown the computer after

backup has finished. For this, activate one of the options under "Power State after Backup". With activating one of the possible options to shutdown the computer, the quiet mode is also enabled, so no further dialogs will appear and the progress display will automatically close after backup. This way the computer will be powered off for sure, at least if there is no action to execute after the backup (see chapter 3.7 for details) that may block the process.

At the end of the backup process, there are two more stages, where Back4Sure will set the access times of the target folders so that they match their respective source folders and finally write a log file for the just finished backup run:

1. **Setting access time of the target folders...**
   The access times of the target folder are set to the access times of their corresponding source folders.
2. **Writing log file...**
   The log file for the just finished backup job is created.

In the last two stages, the progress bar will not move anymore. These stages usually only take a few seconds, with very large backups they may take up to a few minutes.

At the end of the backup operation the progress dialog will show you the overall result of the backup. The current action display will turn green if the backup was successful and red if there was an error.

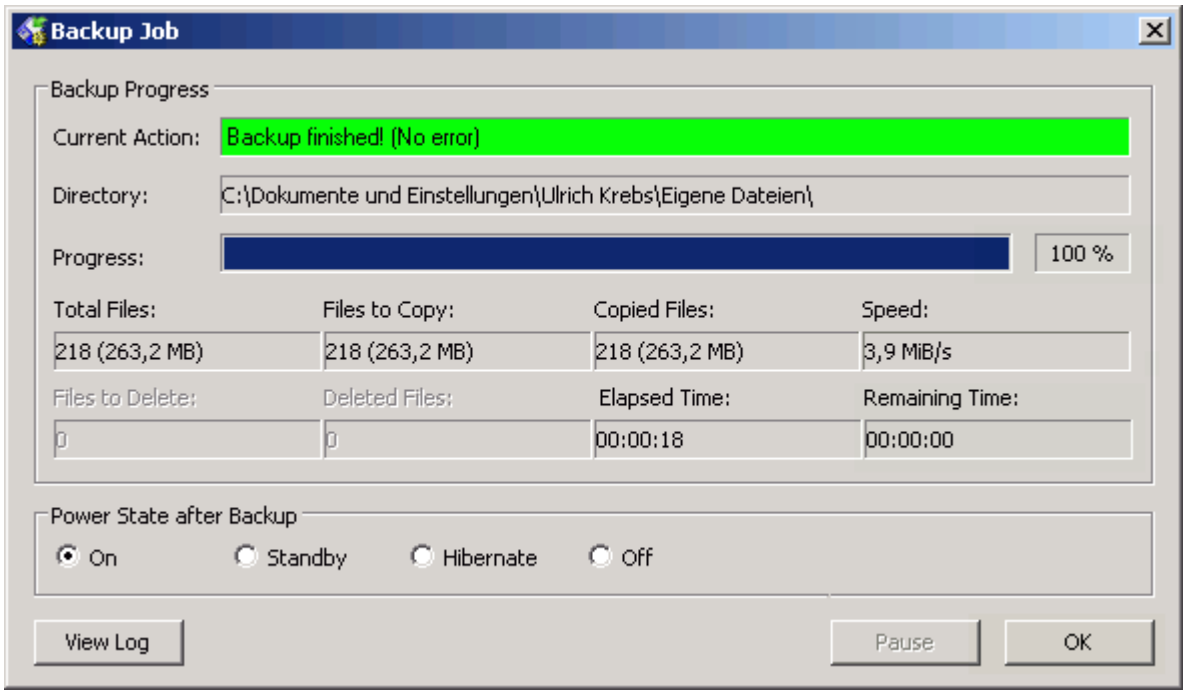

Figure 4.2: Progress dialog after successful backup

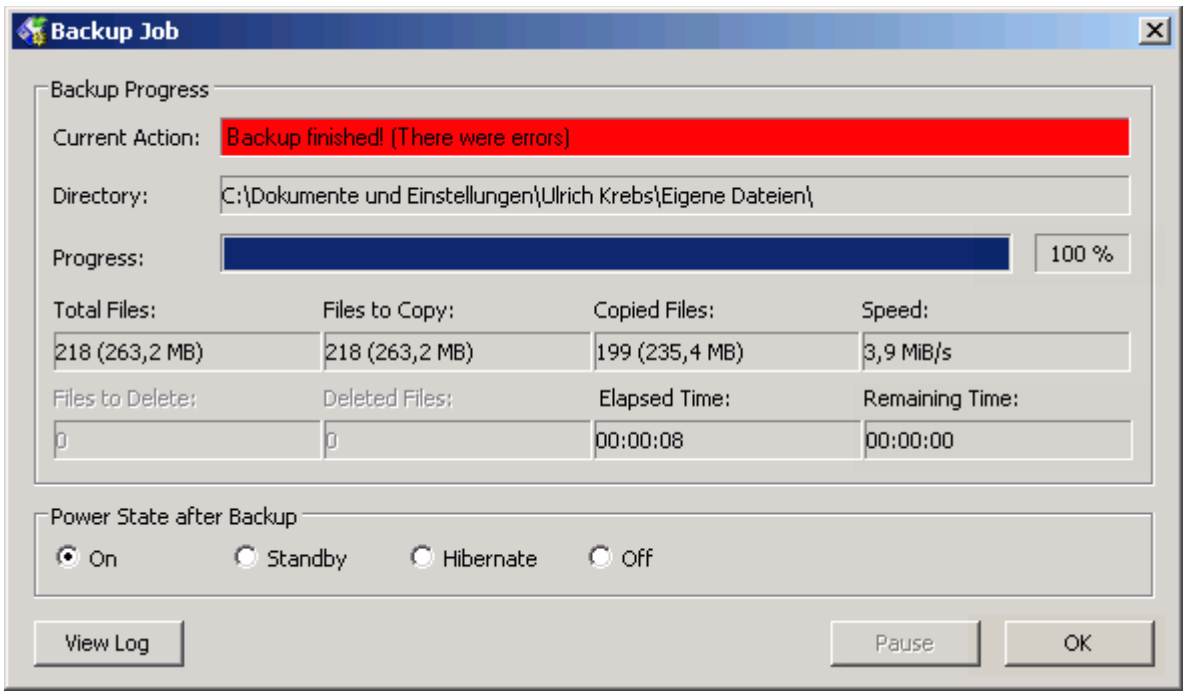

Figure 4.3: Progress dialog after backup failure

Errors during a backup operation are not that rare. Usually only very few files were not copied because they were locked by another program. You can easily see which files were affected if you take a look into the log file. Just press the button "View Log" of the progress dialog. Later on you can find the log files on the tab "Log Files" in the main window. The topmost entry is the log file for the latest executed job. You can open them by double clicking an entry. How to interpret the log file entries is described in chapter 5.2.

4.2 Backup & Cleanup

If you have worked a lot inside the source directories, e.g. reorganized the directory structure or removed or renamed some folders, it is a good idea to do a cleanup run of Back4Sure. During cleanup, depending on the job settings, all files in the target directory that do not have a corresponding source file or do not match the current backup job will be deleted. This operation will free space on the backup media and will also make it easier to do a restore of relevant files.

Attention! To avoid deletion of possibly required parts of the backup, you should thoroughly read the instructions concerning the cleanup options in chapter 3.5!

The cleanup can only be performed together with a backup run. Just press the button "Backup & Cleanup". The progress dialog will pop up again, going through the formerly mentioned three backup stages. After finishing the backup operation two cleanup stages will follow:

1. **Scanning target directories...**
   The target directories are scanned for orphaned or unwanted files.
2. **Cleaning up target directory...**
   All orphaned or unwanted files are deleted from the target directory.

During both stages the currently processed folder is displayed in the "Directory" field. As described in the backup section, the cleanup process can be paused or canceled. At the end of the cleanup run and after setting the folder access times and writing the log file, the overall backup and cleanup result will be displayed in the progress dialog.

4.3 Running backups from the command line

All functions for running backups are also available from the command line. This way you can easily schedule backups at regular intervals using the task scheduler of Windows (or UK's Kalender, of course). During command line execution, all interactive functions of Back4Sure can be disabled, so no "Are you sure..." dialogs will interrupt the automated backup run.

There are only very few options for the command line interface. There are command line options, preceded by a "-" sign, and the path to a backup job definition. There is no special ordering of the options or the path, any part of the command line beginning with a "-" will be considered as option and one entry without preceding "-" will be handled as path to the job definition. Make sure to put the path to the job definition into quotation marks, especially if it contains spaces. Otherwise the job definition cannot be found. Below you'll find all available command line options:

Option	Effect
-b	A backup run with the settings of the given job definition file will be performed
-c	A clenup run with the settings of the given job definition file will be performed
-q	The job will be processed in quiet mode, i.e without any user interaction
-x	Back4Sure will automatically terminated after processing the job
-m	Back4Sure will run with minimized main window
-ps	After backup, the computer will be switched to standby mode. This will also turn on the quiet mode (-q), so the computer is switched off for sure.
-ph	After backup, the computer will be hibernated. The quiet mode is also active here.
-po	After backup, the computer will be switched off. Quiet mode is also activated automatically.

All options may be combined as required. For a fully automated job execution, at least the switches "-b", "-q" and "-x" need to be set and of course the path to the job definition file.

A working command line might look like this:

```
Back4Sure -b -c -q -x "C:\Backup Jobs\FullBackup.b4j"
```

With this command line, Back4Sure will perform a backup and cleanup as specified in the job definition file "FullBackup.b4j". All tasks will be executed without user interaction and Back4Sure will automatically terminate when finished.

4.4 Automated backups using the task scheduler of Windows

Unlike many other backup programs, Back4Sure does not have an own scheduler for performing automated backups. This is not necessarily a disadvantage, though: Windows already has a quite mighty and highly configurable scheduler on board. Using the task scheduler of Windows you can easily set up a backup job that is automatically executed in regular intervals. Discussing all the possible options for scheduling would fill a book on its own, so only a short introduction to the simplest possible case, i.e. running a backup job in a fixed interval at a specified time, will be given. As there are notable differences between Windows XP and Windows 7/8 they'll be discussed separately here.

4.4.1 Scheduling a backup task under Windows XP

In Windows XP, "Scheduled Tasks" can be found in the start menu under "All Programs \ Accessories \ System Tools".

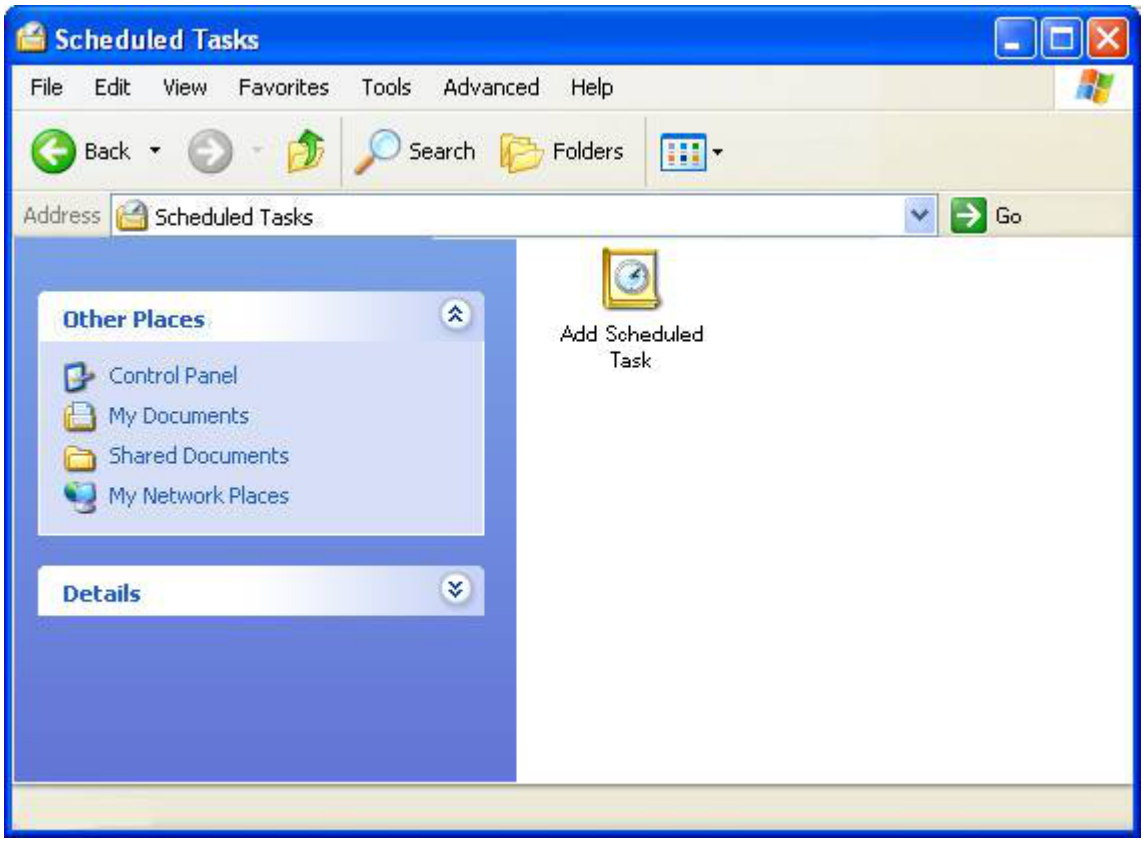

Figure 4.4: Scheduled Tasks in Windows XP

In the Window for scheduled tasks just double click the entry "Add Scheduled Task" to open the "Scheduled Task Wizard".

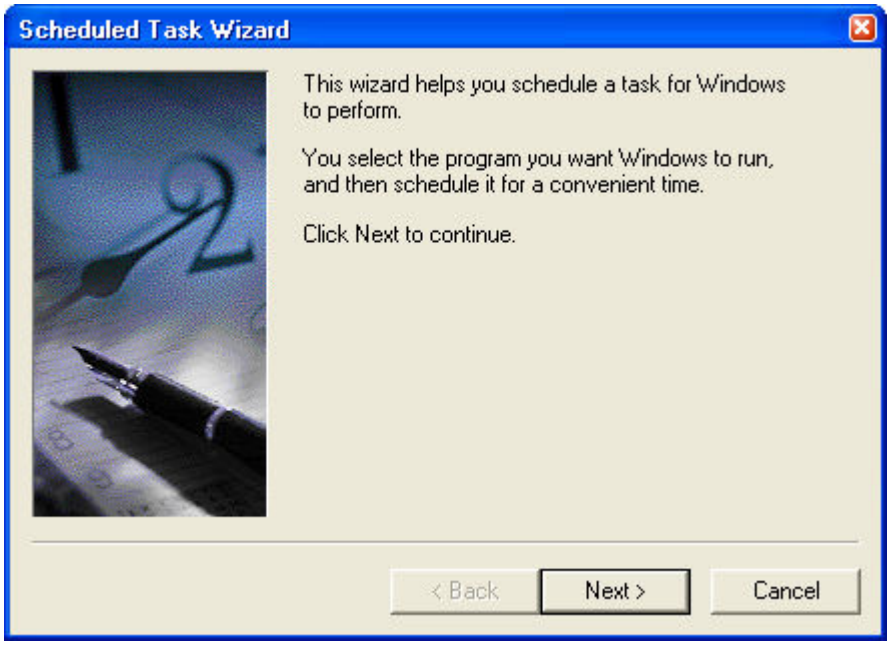

Figure 4.5: Wizard for scheduled tasks

By clicking on the "Next" button, you get a list of all installed programs. If you have installed the setup version of Back4Sure, it will directly appear in this list. If you are using

the zipped version, you can browse for the program file using the "Browse" button. On the next wizard page you can give the schedule a meaningful name, e.g "Full Backup" if the job is for backing up all your data. Just below you can specify the interval for executing the backup job. Usually a daily or weekly backup run is a good choice, depending on how often your data changes. On the next page you can refine the options for the execution interval and also specify the start time. As the task needs to be executed under a user account, on the following page an user name and the corresponding password must be entered. Usually you'll enter your own account information. In any case, the account should have enough rights to access the files to backup. On the final page of the wizard you must enable the option to open the advanced properties of the task, as there is still some vital info missing for Back4Sure to successfully execute the backup job. After pressing the "Finish" button, the window for the advanced task properties will appear.

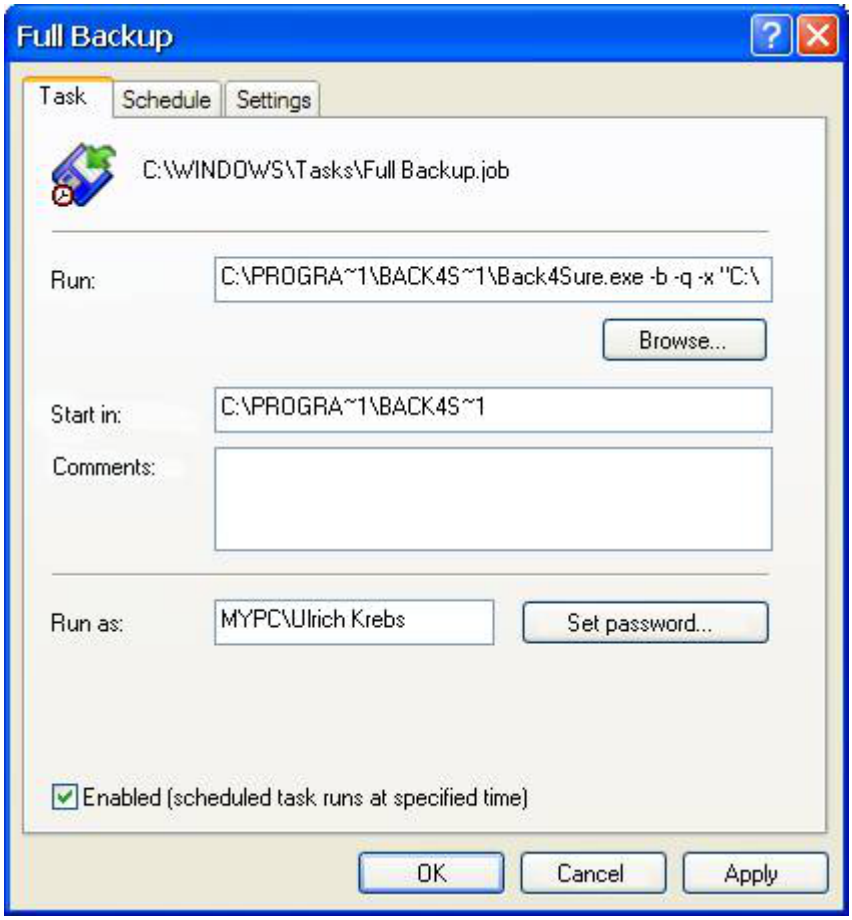

Figure 4.6: Advanced properties of the scheduled task

Under "Run" you'll already find the path to Back4Sure. Don't get irritated by the strange notation, it's a reminiscence of the old DOS times, which seem to be not completely abandoned, yet. In addition to the given path to Back4Sure, the command line options and the path to the backup job must be supplied here. If Back4Sure is installed in "C:\Program Files\", the job file "Full Backup.b4j" in the folder "C:\Backup Jobs\" and you want to make a normal backup without cleanup, the "Run" entry would look like this:

```
C:\PROGRA~1\BACK4S~1\Back4Sure.exe -b -q -x "C:\Backup Jobs\Full Backup.b4j"
```

Make sure, you don't forget the quotation marks around the path to the backup job. These quotation marks are absolutely required for the correct execution of the backup job, at least if the path to the backup job contains spaces. As possible options for executing the backup job all settings discussed in chapter 4.3 may be used. For automatic execution it usually makes sense to specify at least the options -b, -q and -x. This will perform a

backup operation (-b) without user intervention (-q) and finally close the program (-x).

The configuration of the task is now finished, it will be executed at the specified time in the given interval. You can also change all the settings later on by opening the "Scheduled Tasks" again and double clicking the symbol for the backup task.

4.4.2 Scheduling a backup task under Windows 7

Under Windows 7 the task scheduler can be found just like in Windows XP under "All Programs \ Accessories \ System Tools". Alternatively you can also simply type "task" into the edit box "Search programs and files" in the start menu, the task scheduler will immediately appear in the result list.

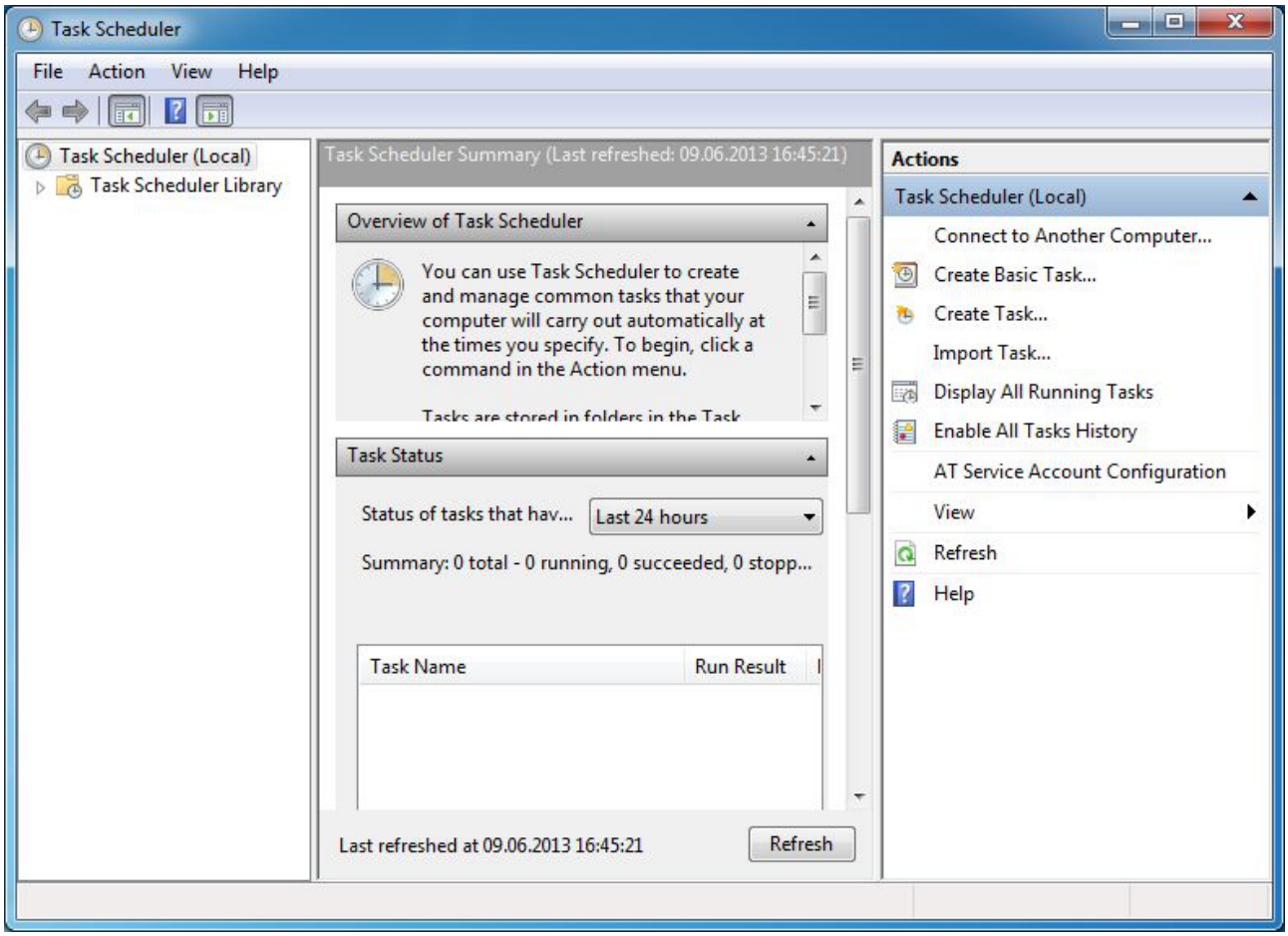

Figure 4.7: Task scheduler under Windows 7

To create a backup task, choose "Create Basic Task..." from the right panel. The "Create Basic Task Wizard" will appear then. On the first page you can enter a meaningful name for the backup, e.g. "Full Backup". On the next page you can specify the recurrence interval for the backup. Usually daily or weekly is a good choice. The next page allows to make some further settings for the start time of the backup. On the following page you must choose "Start a program" as action. If you press the "Next" button, you can browse for Back4Sure as program to start and also enter the required arguments for executing the backup job.

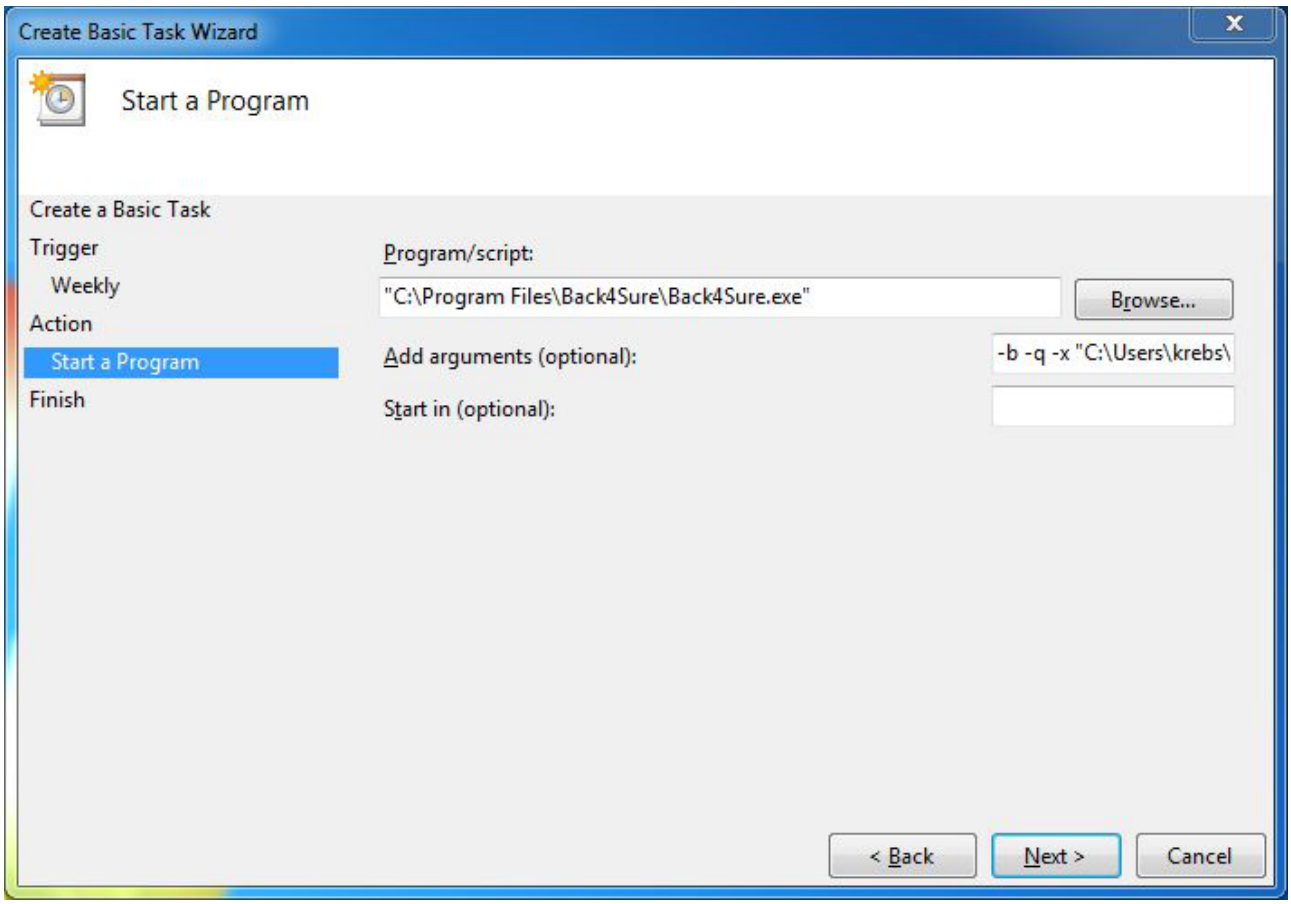

Figure 4.8: Program options for the backup task

Make sure to use quotation marks around every path that contains spaces, otherwise the backup will not be performed. Possible options for performing the backup job are all settings discussed in chapter 4.3. For automatic execution it usually makes sense to specify at least the options -b, -q and -x. This will perform a backup operation (-b) without user intervention (-q) and finally close the program (-x).

To finish scheduling the backup task, just click on "Next" and finally on "Finish". The new backup task appears in the "Task Scheduler Library". To make changes to the backup task you first need to open the "Task Scheduler Library" by clicking on the corresponding entry on the left panel of the task scheduler. In the column in the middle a list of scheduled tasks will appear. The backup task should be stored somewhere inside this list and may be edited by double clicking on it.

4.4.3 Scheduling a backup task under Windows 8

Under Windows 8 it is not so very easy to gain access to the task scheduler. A rather easy method is, to enter the word "task" directly into the Metro interface (i.e. not into an edit box). The result list shows one matching entry under "Settings". If you select "Settings" the task scheduler will appear on the left side of the screen. Just click on the task scheduler symbol to switch to the normal desktop and to start configuring your backup task. Fortunately the task scheduler under Windows 8 works just like the one under Windows 7, so I'll only point to the previous chapter 4.4.2 for a detailed description.

5. Viewing and interpreting log files

5.1 Log file view

The log file view is selected via the tab "Log View". This tab does not offer further configuration options but allows easy access to all log files created for the current job. You'll see a table that holds all available log files and their respective execution dates and backup results for the currently loaded job. The table is sorted by the execution date of the job, most recent entries are at the top of the list.

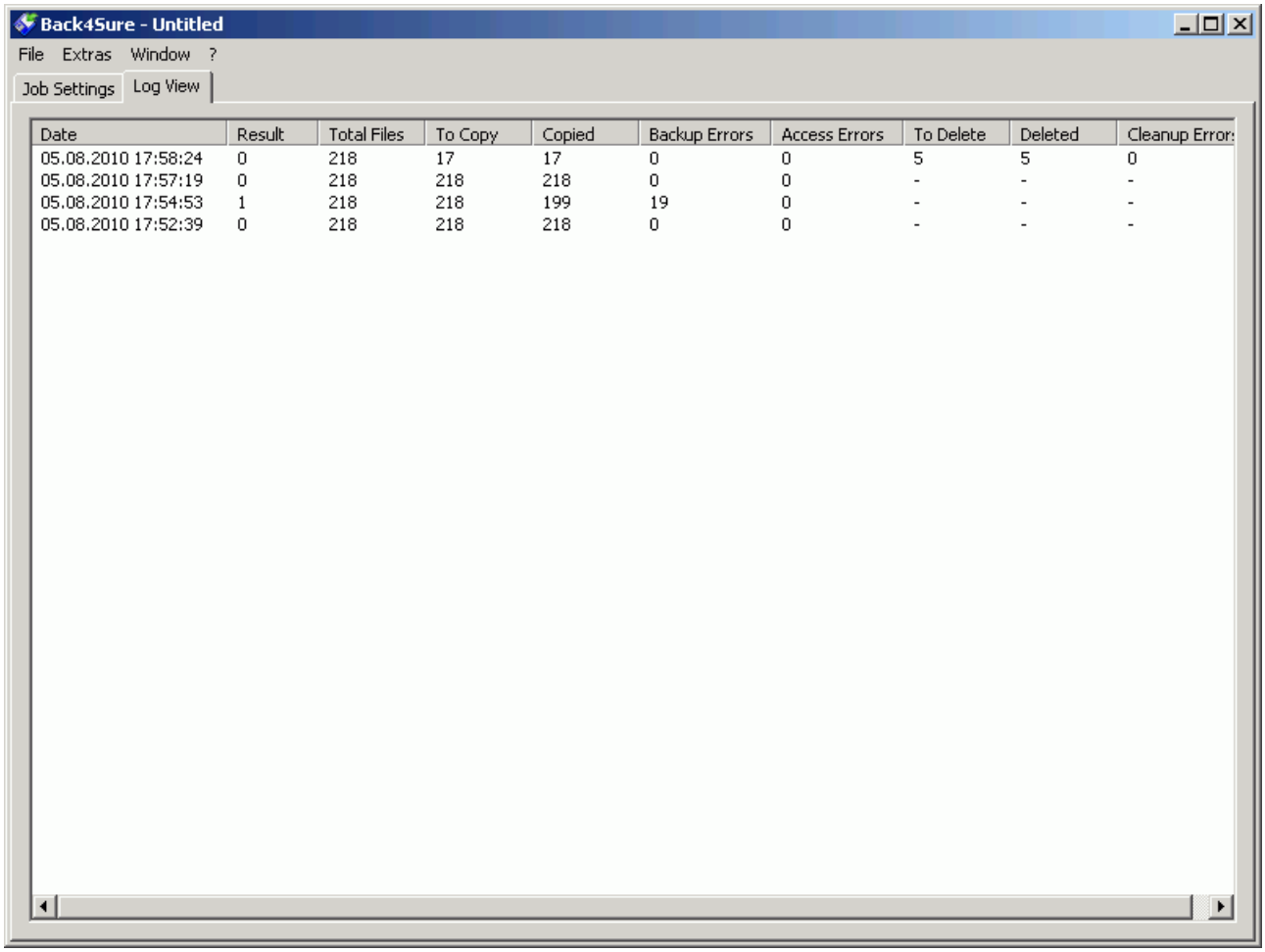

Figure 5.1: List of available log files for the current job

The columns of the table hold the following information:

Column	Content
Date	Date and time of the job execution
Result	Numerical result code of the job execution, 0 means no error
Total Files	Number of files included in this backup job
To Copy	Number of files to be copied to the backup target
Copied	Number of files that were successfully copied during this execution
Backup Errors	Number of files that were not copied due to an error
Access Errors	Number of source folders that cannot be accessed due to missing

	access rights
To Delete	Number of orphaned files in the backup target
Deleted	Number of files that were successfully deleted during the cleanup run
Cleanup Errors	Number of files that were not deleted due to an error

The entries will show you at a glance, if a backup job was successfully executed. In this case, the value 0 must appear under the column "Result". Any other value means that there was a more or less severe error during execution. You should take a look into the "Backup Errors" column, then, to see how many files weren't copied. If there are just one or two errors, the affected files were probably locked during execution. A larger number of copy errors indicate a more severe problem. If the counter for access errors is not zero, the overall backup result will also indicate the failure. In any case, you should take a look into the log file to see the cause for the malfunction.

If your system is configured to open log files with a text editor, you can open the log file by simply double clicking the entry in the table. If your system currently doesn't know how to handle log files, Back4Sure will automatically start the appropriate Windows configuration dialog if you double click on a log file in the list.

Attention! If you see only some hodgepodge when opening a log file, your text editor is probably not capable of displaying unicode files correctly. Use the Windows Notepad or some other unicode capable program like Notepad++ in this case.

Attention! If the format option is set to "Human readable" and you switch the program language from English to German, the column contents of the log file view will not be displayed correctly for older logs. Back4Sure cannot interpret the entries of the log file if they have a different language. Also do not rename the log files, as they wouldn't appear in the log file view anymore.

5.2 Log file interpretation

At each execution of a backup job a log file is created, which contains, depending on the log file settings, a summary or a complete list of all actions taken during the backup run. Chapter 3.8 describes in detail how to customize the content of the log file.

Log files may be created in a human readable format or in a format optimized for atomated analysis. The information of both formats is identical, only the data representation varies. The following two chapters will help you to interpret the log file content.

5.2.1 Human readable log files

The human readable log file has up to seven sections, each containing different aspects of the performed actions. A section always starts with a headline which is enclosed by three asterisks for easy recognition. Following sections exist:

Section	**Content**
*** Job Summary ***	This is the summary of the job execution. Here you'll find the execution date and time, the backup duration and the overall result code. This should be the first section to look at. If the result code is 0, the backup was executed without

<table>
<tr><td></td><td>any error. Possible result codes are:

<table>
<tr><th>Code</th><th>Meaning</th></tr>
<tr><td>0</td><td>The complete job was executed without errors.</td></tr>
<tr><td>1</td><td>There were errors while copying or deleting files. Full information about affected files and the failure reason can be found in the other sections. Probably most of the files were still backed up correctly.</td></tr>
<tr><td>2</td><td>No target directory was specified, no file was saved.</td></tr>
<tr><td>3</td><td>The target drive should be determined by its drive label but no matching drive was found. No file was saved.</td></tr>
<tr><td>4</td><td>The target directory wasn't found. No file was saved.</td></tr>
<tr><td>5</td><td>The target is write protected. No file was saved.</td></tr>
<tr><td>6</td><td>Files from more than one drive were selected for backup and drive prefix generation in the target directory was disabled. To avoid ambiguities, no backup run was performed. No file was saved.</td></tr>
<tr><td>100</td><td>The backup operation was canceled by the user. The number of unsaved files depends on the time of interruption.</td></tr>
</table></td></tr>
<tr><td>*** Backup Summary ***</td><td>This is the summary of all backup activities. This section holds the following entries:

<table>
<tr><th>Entry</th><th>Meaning</th></tr>
<tr><td>Total files in backup set</td><td>The total number of files included in this backup job.</td></tr>
<tr><td>Total bytes in backup set</td><td>The total amount of bytes included in this backup job.</td></tr>
<tr><td>Files to copy</td><td>Number of files that need to be copied to the target directory.</td></tr>
<tr><td>Bytes to copy</td><td>Amount of bytes to be copied during this backup run.</td></tr>
<tr><td>Copied files</td><td>Number of files that were successfully copied to the target directory.</td></tr>
<tr><td>Copied bytes</td><td>Total amount of bytes copied from source to target.</td></tr>
<tr><td>Speed</td><td>The overall backup speed in megabyte per second.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Source access errors</td><td>Number of folders that were selected for backup but cannot be accessed by Back4Sure.</td></tr>
<tr><td>Backup errors</td><td>Number of files where the copy process failed.</td></tr>
</table>
</td></tr>
<tr><td>*** Cleanup Summary ***</td><td>This is the summary of all cleanup activities. This section will only be created if there actually was a cleanup run. This section holds the following entries:

<table>
<tr><th>Entry</th><th>Meaning</th></tr>
<tr><td>Files to delete</td><td>Total number of files that were marked for deletion from the target directory according to the cleanup settings.</td></tr>
<tr><td>Bytes to delete</td><td>Total amount of bytes that were marked for deletion.</td></tr>
<tr><td>Deleted files</td><td>Number of actually deleted files.</td></tr>
<tr><td>Deleted bytes</td><td>Amount of actually deleted bytes.</td></tr>
<tr><td>Cleanup errors</td><td>Number of files where deletion from the target directory failed.</td></tr>
</table>
</td></tr>
<tr><td>*** Source Access Errors ***</td><td>Any directory selected for backup that cannot be accessed by Back4Sure will be denoted here. This section is only created if you have activated error logging in the logging options (chapter 3.8). Each entry consists of the full path of the inaccessible source folder and the result of the access operation as system code and plain text message.

The result code is always non-zero, as only access errors are recorded here. There are usually only two possible error codes, either code 3 (The system cannot find the path specified) or code 5 (Access is denied). Code 3 results from source folders, that were selected for backup but deleted during the backup process. You may fix this error by choosing "Check Job Consistency" from the "Extras" menu. The job file will be checked for invalid source directories, then. The system code 5 will appear, if you don't have sufficient rights to acces one of the selected folders or subfolders of the current backup set. Under Windows Vista or Windows 7 e.g. not even the administrator has the right to view or read the profile folders of other users. In this case, you should restrict the job to your own profile folder and create backup jobs for all other users seperately.</td></tr>
</table>

*** Backup Errors ***	This section holds one entry for each failed copy attempt. It is only created if you have activated error logging in the logging options (chapter 3.8). Each entry consists of the full path of the source file, the full path of the target file, the state of the target file and herewith the reason for copying this file and finally the copy result as system code and plain text message. In this section the result code is always non-zero as only failed copy actions are recorded here. To list all possible system codes would go beyond the scope of this manual, but the most common reason for a failed copy attempt is probably the system code 32 (The process cannot access the file because it is being used by another process). This means, another program claims exclusive access rights to the file in question and prevents other programs from reading it. In this case, close all open programs and retry the backup operation. A different solution is to exclude certain file types (e.g. *.lock) from the backup job by defining an exclude filter (chapter 3.3). This way, the possibly locked files will not be included in the backup set.
*** Cleanup Errors ***	If during a cleanup run certain files cannot be deleted from the target directory, they'll be noted here. This section will only exist if error logging is activated. Each entry consists of the automatically generated path of a source file that corresponds with an existing target file, the full path of the target file, the state of the source file (e.g. source file does not exist) and herewith the reason for deleting the target file and finally the deletion result as system code and plain text message. In this section the result code is always non-zero again as only failed actions are recorded here. A common reason for a deletion failure is represented by the system code 5 (Access denied). This error often results from a write protected target file which cannot be deleted. You can alter the cleanup options (chapter 3.5) to enforce the deletion of write protected files.
*** Backup Actions ***	If you have enabled logging of all actions in the logging options, each successful copy operation will be denoted here. Each entry follows the same scheme as described in section *** Backup Errors ***" and holds the source file, the target file, the reason for copying and the copy result, which is always 0 (The Operation Completed Successfully) here.
*** Cleanup Actions ***	This section will also only be created if you have enabled action logging in the logging options. For each successful file deletion an entry will be created, following the same

	scheme as described in section *** Cleanup Errors ***. Each entry consists of the automatically generated path of a source file that corresponds with an existing target file, the target file, the source state and the deletion result code, which is always 0 (The Operation Completed Successfully) here.

5.2.2 Machine readable log files

Machine readable log files hold the same information as the human readable variant but all entries are created using the ini format and are also invariant against the chosen program language. This allows an easy and reliable way to read and analyze the log file using an external program. Following sections exist:

<table>
<tr><th>Section</th><th>Content</th></tr>
<tr><td>[JobSummary]</td><td>Contain the summary of the backup job execution. Following keys are available:
<table>
<tr><th>Key</th><th>Content</th></tr>
<tr><td>JobName</td><td>Name of the job file (without extension).</td></tr>
<tr><td>JobStart</td><td>Date and time of execution start, using the format yyyy mm dd HH MM SS.</td></tr>
<tr><td>JobEnd</td><td>Date and time of execution end, using the format yyyy mm dd HH MM SS.</td></tr>
<tr><td>ElapsedTime</td><td>Duration of job execution in seconds.</td></tr>
<tr><td>BackupResult</td><td>Overall result code of the backup operation. The result code may be one of the following values:
<table>
<tr><th>Code</th><th>Meaning</th></tr>
<tr><td>0</td><td>The complete job was executed without errors.</td></tr>
<tr><td>1</td><td>There were errors while copying or deleting files. Full information about affected files and the failure reason can be found in the other sections. Probably most of the files were still backed up correctly.</td></tr>
<tr><td>2</td><td>No target directory was specified, no file was saved.</td></tr>
<tr><td>3</td><td>The target drive should be determined by its drive label but no matching drive was found. No file was saved.</td></tr>
<tr><td>4</td><td>The target directory wasn't found. No file was saved.</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>5</td><td>The target is write protected. No file was saved.</td></tr>
<tr><td>6</td><td>Files from more than one drive were selected for backup and drive prefix generation in the target directory was disabled. To avoid ambiguities, no backup run was performed. No file was saved.</td></tr>
<tr><td>100</td><td>The backup operation was canceled by the user. The number of unsaved files depends on the time of interruption.</td></tr>
</table>
</td></tr>
<tr><td>[BackupSummary]</td><td>This is the summary of all backup activities. Following keys are available:
<table>
<tr><th>Entry</th><th>Meaning</th></tr>
<tr><td>TotalFiles</td><td>The total number of files included in this backup job.</td></tr>
<tr><td>TotalBytes</td><td>The total number of bytes included in this backup job.</td></tr>
<tr><td>FilesToCopy</td><td>Number of files that need to be copied to the target directory.</td></tr>
<tr><td>BytesToCopy</td><td>Amount of bytes to be copied during this backup run.</td></tr>
<tr><td>CopiedFiles</td><td>Number of files that were successfully copied to the target directory.</td></tr>
<tr><td>CopiedBytes</td><td>The total amount of bytes copied from source to target.</td></tr>
<tr><td>BytesPerSecond</td><td>Overall backup speed in bytes per second.</td></tr>
<tr><td>SourceAccessErrors</td><td>Number of folders that were selected for backup but cannot be accessed by Back4Sure.</td></tr>
<tr><td>BackupErrors</td><td>Number of files where the copy process failed.</td></tr>
</table>
</td></tr>
<tr><td>[CleanupSummary]</td><td>This is the summary of all cleanup activities. This section will only be created if there actually was a cleanup run. Following keys are available:
<table>
<tr><th>Entry</th><th>Meaning</th></tr>
<tr><td>FilesToDelete</td><td>Total number of files that were marked for deletion from the target directory according to</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>the cleanup settings.</td></tr>
<tr><td>BytesToDelete</td><td>Total amount of bytes that were marked for deletion.</td></tr>
<tr><td>DeletedFiles</td><td>Number of actually deleted files.</td></tr>
<tr><td>DeletedBytes</td><td>Amount of actually deleted bytes.</td></tr>
<tr><td>CleanupErrors</td><td>Number of files where deletion from the target directory failed.</td></tr>
</table>
</td></tr>
<tr><td>[SourceAccessErrors]</td><td>Any directory selected for backup that cannot be accessed by Back4Sure will be denoted here. This section is only created if you have activated error logging in the logging options. All keys belonging to one entry will receive a consecutive number, starting from zero. In the following key description, the position of this number is marked with a "X". Each entry has the following keys:

<table>
<tr><th>Key</th><th>Meaning</th></tr>
<tr><td>SourceDirectory_X</td><td>Full path to the inaccessible source folder.</td></tr>
<tr><td>AccessResult_X</td><td>Result of the access operation as numerical system code. The code is always non-zero as only failed access operations are denoted here. The codes correspond to the return value of the GetLastError() function of the operating system.</td></tr>
</table>
</td></tr>
<tr><td>[BackupErrors]
[BackupActions]</td><td>In these two sections each copy operation will represented by one entry consisting of four keys. Failed operations will appear in section [BackupErrors], successful operations in section [BackupActions]. For these sections to be included in the log file, error and / or action logging must be activated in the logging options. All keys belonging to one entry will receive a consecutive number, starting from zero. In the following key description, the position of this number is marked with a "X". Each entry has the following keys:

<table>
<tr><th>Key</th><th>Meaning</th></tr>
<tr><td>Source_X</td><td>Full path to the source file.</td></tr>
<tr><td>Target_X</td><td>Full path to the target file.</td></tr>
<tr><td>TargetState_X</td><td>State of the target file and herewith reason for the copy operation as numerical code:

<table>
<tr><th>Code</th><th>Meaning</th></tr>
<tr><td>0</td><td>State of the target file could not be determined.</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>
<table>
<tr><td>1</td><td>Target file does not exist.</td></tr>
<tr><td>2</td><td>Target file is outdated.</td></tr>
<tr><td>3</td><td>Target file has the same date and time as the source file, but the file size is different.</td></tr>
<tr><td>4</td><td>Target file is current, no copying required.</td></tr>
</table>
</td></tr>
<tr><td>BackupResult_X</td><td>Result of the copy operation as numerical system code. Zero means successful operation, any other value reflects a failed copy operation. The codes correspond to the return value of the GetLastError() function of the operating system. If compression is enabled, other codes may also appear.</td></tr>
</table>
</td></tr>
<tr><td>[CleanupErrors]
[CleanupActions]</td><td>
During a cleanup run, each file deletion will create one entry consisting of four keys. Failed operations will appear in section [CleanupErrors], successful operations in section [CleanupActions]. For these sections to be included in the log file, error and / or action logging must be activated in the logging options. All keys belonging to one entry will receive a consecutive number, starting from zero. In the following key description, the position of this number is marked with a "X". Each entry has the following keys:
<table>
<tr><th>Key</th><th>Meaning</th></tr>
<tr><td>Source_X</td><td>Full path to the source file. The path will be automatically generated from the path of the existing target file.</td></tr>
<tr><td>Target_X</td><td>Full path of the target file.</td></tr>
<tr><td>SourceState_X</td><td>
State of the source file and herewith reason for target file deletion as numerical code:
<table>
<tr><th>Code</th><th>Meaning</th></tr>
<tr><td>0</td><td>The source file is included in the current backup set and will not be deleted.</td></tr>
<tr><td>1</td><td>The source file does not exist.</td></tr>
<tr><td>2</td><td>The source file is not included in the current backup set.</td></tr>
</table>
</td></tr>
<tr><td>CleanupResult_X</td><td>Result of the delete operation as numerical system code. Zero means successful operation, any other value reflects a failed delete operation. The codes correspond to</td></tr>
</table>
</td></tr>
</table>

			the return value of the GetLastError() function of the operating system. If compression is enabled, other codes may also appear.

5.2.3 Return codes for compressed backups

If compression is enabled for the current backup, the system codes for backup and copy operations may not always correspond to the return value of the GetLastError() function but can be replaced by return values of the compressor. Which codes are used depends on the respective error. Codes from the packer can be recognized by a set bit 29 of the result code (the code is greater than 536870912). The currently used compressor has the following return values:

Code	Meaning
0	The operation completed successfully.
536870913	Warnings were issued.
536870914	Fatal error.
536870919	Command line error.
536870920	Out of memory.
536870921	Can't create list file for archive operation.
536871167	Operation aborted by user.

6. License agreement and registration option

6.1 License agreement

The copyright of "Back4Sure" belongs to the author of this software, Ulrich Krebs.

With installing, copying or any other use of "Back4Sure" you are accepting this license agreement.

1. **Terms of use**
   "Back4Sure" is freeware. You may use this software without charge for any purpose, including commercial use, without time limit.
2. **Copying**
   You may give away exact copies of this software, as long as you do not modify the original contents of the package (adding or removing files, changing file contents) and do not charge a fee for the distribution, except an appropriate fee for the media. You may not bundle this software with a commercial program or program collection without express written consent of the author.
3. **Support**
   You are not entitled for support by the author. Nevertheless the author will try to help on any questions regarding the program. Support is solely offered by email.
4. **NO WARRANTY**
   USAGE OF THE PRORAM "BACK4SURE" IS AT YOUR OWN RISK! IN NO EVENT WILL THE AUTHOR ULRICH KREBS BE LIABLE FOR ANY DAMAGE CAUSED BY THE USE OR THE DISTRIBUTION OF THE PROGRAM "BACK4SURE". IN NO CASE THE AUTHOR CAN BE HELD RESPONSIBLE FOR LOST PROFIT, LOST

DATA OR DIRECT OR CONSEQUENTIAL DAMAGE TO HARD- OR SOFTWARE CAUSED BY THE USE OF OR THE IMPOSSIBILITY TO USE THE SOFTWARE.

6.2 Registration option

If you like Back4Sure and use it on a regular basis, I'd be happy if you support my work with a donation. If you donate 10,- € or more you'll receive a license key, which switches off the occasionally appearing reminder window. This registration is in no case required and will not enable new functions of the program. You'll also get the same support if you decide not to donate.

So why a reminder window? The reminder will only appear if you often create new jobs and do a lot of things using the graphical user interface of Back4Sure. If you only create a few jobs and let them execute automatically, you'll probably never see the reminder window. If you do a lot of interactive work with the program, I assume Back4Sure does a good job for you and you might want to make a donation. The reminder Window will not appear too often, with daily use at maximum every ten days. It will *never* appear during automatic execution.

To make a donation, choose "Register..." from the help menu. In the registration window, press the "Donate" button to open your web browser with my home page, where you can send me a donation via PayPal. As I'll send you the registration key manually, it may last a few days until you'll receive the key via email. After receiving the key, you can enter your name and key in the registration window to turn Back4Sure into a registered version where no further reminder windows will appear.