Syncovery is a tool for file synchronization and backup

Syncovery User Manual

Introduction

This powerful tool now comes with an all-new design and helps you keep your data   synchronized in various locations, including backup storage on fixed or removable media.   It runs all versions of **Microsoft Windows** starting with Windows 2000 up to Windows 8.1 / Server 2012R2. A **Macintosh** version is also available. There are two modes: **Wizard Mode** and **Advanced Mode**. Please choose the mode that you feel most comfortable with in the menu bar.

Synchronizing - A Way to Back Up Your Data

Today's computers are often equipped with technology (or embedded in a network) that makes it feasible to back up your data by keeping a complete backup copy of it in another location. This can be another PC connected via network, or a second hard disk in your computer, or a removable storage medium.

The purpose of **Synchronizing** is to have two identical copies of your data. This synchronizing software enables you to create and maintain such copies. While the first creation of a complete copy may take a while, subsequent updates are usually fast! Just run the job again, and it will detect all changed files and perform a swift update of your copy.

Left or Right - the program will automatically detect which files are newer on the **Left** side, and which ones are newer on the **Right** side, by comparing the last modification dates of the files. The program will automatically prepare to copy the newer file to the other side, so that both sides end up with the latest versions of all files. The only problem is when a file has been modified independently in both storage locations. In that case, the software cannot merge the various changes within the file. It will simply take the version with the latest modification date and copy it over to the other side. For this reason, it is recommended that you take a minute to look at the **File List View** which shows the results of the comparison before the actual copying is performed. Please verify that all the actions proposed by the software match your intentions.

Key Features

(see the Features List on our web site for all the details):

- **Synchronize Files** (for example, between a PC and a laptop)
- **Synchronize Files with or between Cloud storages** (for example, between a PC and GoogleDrive, between GoogleDrive and OneDrive)
- **Multiple Profiles** (sets of saved settings)
- **Detects Moved Files** (such as reorganized folders)
- **With Scheduler** (for automated backups)
- **Support for FTP, SSH, SSL, WebDAV, Amazon S3, Microsoft Azure, Google Docs, Google Drive**
- **SmartTracking** (detects on which side changes have occurred)
- **Scheduler Service** (runs scheduler without users logging on to start a Windows session)
- **Unicode and Long File Path Support** (during synchronization)
- **Copy Locked Files** (on local drives, requires Windows XP or later)
- **Partial File Updating** (using a SmartTracking database or a Remote Service)
- **Keep Multiple Backup Versions Of Each File** (optional)
- **Can Use Recycle Bin** (for older versions of files that are replaced)
- **Email Notification** (of Sync Results)
- and much more

Feature Matrix

Feature Matrix	Standard	Professional
HARD DISK BACKUP	✔	✔
ONE-WAY SYNCHRONIZATION	✔	✔
TWO-WAY SYNCHRONIZATION	✔	✔
EXTREMELY FAST MULTI-THREADED FOLDER SCANNING	✔ new in V7!	✔ new in V7!
PROPAGATE DELETED FILES AND FOLDERS	✔	✔
DETECT MOVED FILES AND FOLDERS	✔	✔
SMARTTRACKING - SMART TWO-WAY SYNCS	✔	✔
ATTENDED MODE WITH SYNC PREVIEW	✔	✔
UNATTENDED MODE WITH NO QUESTIONS ASKED	✔	✔
SELECT WHICH FOLDERS TO PROCESS	✔	✔
INCLUSION AND EXCLUSION MASKS	✔	✔
NUMEROUS FILTERING OPTIONS	✔	✔
SELECT SPECIFIC FILES IN FOLDERS	(Windows only)	(Windows only)
AVAILABLE IN 32 AND 64 BIT	new in V7! (Windows only)	new in V7! (Windows only)
UNLIMITED NUMBER OF PROFILES (JOBS)	✔	✔
SCHEDULER FOR AUTOMATED RUNS	✔	✔
REAL-TIME SYNCHRONIZATION		✔
COPY SEVERAL FILES IN PARALLEL	✔	✔
PARALLELIZED FILE DELETIONS, RENAMES, MOVES	✔ new in V7!	✔ new in V7!
RUN SEVERAL JOBS IN PARALLEL		✔
LOG FILES	✔	✔
EMAIL NOTIFICATIONS	✔	✔
VERSIONING - KEEP MULTIPLE VERSIONS OF FILES	✔	✔
COMPRESSION (ZIP FORMAT)		✔
STRONG AES-256 ENCRYPTION		✔
FTP, WEBDAV, SSH		✔

Feature Matrix	Standard	Professional
DROPBOX, BOX.COM, ONEDRIVE, RACKSPACE CLOUD FILES, SUGARSYNC		✔ (now on Mac too!)
AMAZON S3, MICROSOFT AZURE, GOOGLE DOCS		✔
SEND/RECEIVE FILES BY EMAIL		✔ new in V7!
BLOCK LEVEL COPYING (PARTIAL FILE UPDATING)		✔
SYNTHETIC BACKUP (BLOCK LEVEL WITH ZIPPING AND VERSIONING)		✔
REMOTE SERVICE: GENERATE REMOTE LISTINGS FAST		✔
REMOTE SERVICE: UNZIP INCOMING ZIP PACKAGES		✔
REMOTE SERVICE: GENERATE MD5 CHECKSUMS		✔

System Requirements

Syncovery runs on:

Windows
All versions of Windows since Windows 2000 are fully supported, including Windows 8.1 and Server 2012 and all other versions and editions of Windows that have a graphical user interface. It runs on both 32-bit and 64-bit operating systems. The software itself (up to version 6) is mostly 32-bit code, but includes some 64-bit code to enable Volume Shadowing on 64-bit Windows. Version 7 is being released in both 32-bit and 64-bit editions.

Macintosh
Syncovery runs on all Intel Macs, and on all Mac OS X versions since 10.4 "Tiger" up to including the latest version (currently 10.9 "Mavericks").
To install it, you may need to go to the Mac OS System Preferences, Security & Privacy, and specify that you want to allow apps downloaded from: Anywhere.

An older version 5.73 is also available if you need to run it on older PowerPC Macs. This version also requires at least Mac OS 10.4 "Tiger".

Linux
A version of Super Flexible File Synchronizer is available for Linux. It may or may not run on your Linux distribution. See the Linux download page for more details.

Installing Syncovery

IMPORTANT: You must install Syncovery on each device on which you will use the application.

Install From Downloaded File:

- Double-click SyncoverySetup.exe installer package to start the installation process.

- Click Continue and follow the on-screen prompts. Then click Install to complete the installation.
- After installation is complete, navigate to your Applications folder and double-click Syncovery to start the application.

- Syncovery V7 can be installed on top of an existing version and will use the same configuration and database files.
- The 32-bit version 7 will replace an existing V6 unless you specify a separate installation folder.
- The 64-bit version will automatically be installed into a new folder and can be used side-by-side with any 32-bit version.
- You can always go back to version 6 without any issues, because all configuration and database files are 100% comptible.

Main Form

Profile Overview Tab
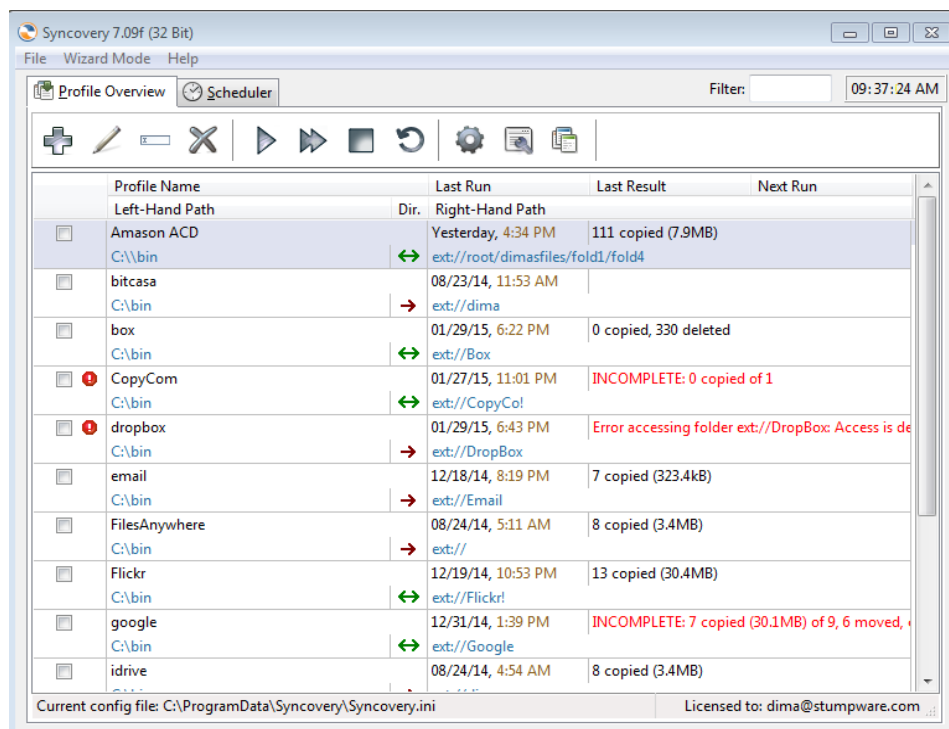
This tab sheet shows an overview of all stored profiles and allows you to manage your profiles.

Here's the meaning of the symbols in the toolbar:
- Add New Profile, Edit, Rename, Delete
- Run Selected Profile(s), Run Checked Profile(s), Stop, Restore Wizard
- Tools and Settings

When editing a profile from the Profile Overview, you will automatically edit in in Advanced Mode and see all available options.

There are two ways to select profiles.
- Click on the rows in the table to select them with a light blue bar. You can select multiple profiles by dragging or ctrl- and shift-clicking. Selected profiles can be run with the single Play button.
- Click on the checkmarks to choose a combination of profiles which is remembered even after you exit the program. These profiles can be run with the double Play button (or fast forward, symbolizing "Start Many").

Also make sure you try the context menu which you get by right-clicking on profiles. You have three choices of how to start a profile:

Run In Attended Mode
In attended mode, the profile will run in the foreground and you will see all the progress information related to building the file list. You will then see the Synchronization Preview and you can check the copying actions that the program wants to make. You can make changes in the Preview and then continue with the execution or cancel the profile.

Run In Unattended Mode
In unattended mode, the profile will also run in the foreground but it will not wait for any user input or offer you to examine the Sync Preview. It will start copying right away, but you can cancel it at any time.

Run In Background
When run in the background, the profile will be executed by a separate process which will show in Task Manager as SyncoveryService.exe. You will not see a lot of details, but some progress information is shown in the Profile Overview. You can stop the profile with the Stop button in the toolbar.

Running profiles in the background is the only way to run several profile simultaneously. The scheduler can also run profiles in the background and simultaneously, see the option "Start Profiles In Parallel" in the Tools and Settings menu on the Scheduler tab sheet.

The Scheduler Tab
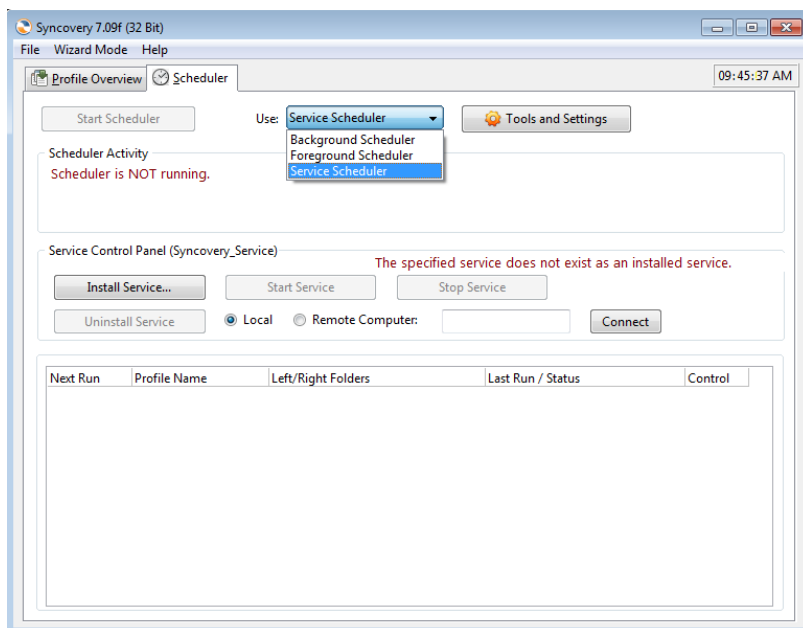
You have the choice between three schedulers: the Background Scheduler (default), the Foreground Scheduler, and the Service Scheduler (Professional Edition only).

Background Scheduler
This is the default scheduler. It will run in the background in a separate process. All status and progress information can be seen on the Scheduler tab sheet. You can actually make the background scheduler visible by right-clicking on its tray icon and selecting "Reveal Background Windows".

The Background Scheduler usually starts when you log in to Windows. You can select this in the Tools and Settings menu. You can also choose whether to start profiles in parallel (simultaneously).

Foreground Scheduler
While the Foreground Scheduler is running, you cannot access any other parts of the software. For that

reason, this scheduler type is no longer recommended but you may use it if you prefer.

Service Scheduler
The service scheduler is a bit more difficult to set up. Please note that the word "install" is used in a double sense when speaking about services. First, the service's file must be installed (=copied) onto the computer. Second, the service must be installed (=registered) with the Windows operating system so that it is known as a service and automatically started when Windows boots up.

Install Service / Uninstall Service buttons
These buttons register the Syncovery Service with Windows. A registered/installed service can be started and stopped, and by default it will start automatically when Windows boots up.

Local Service / Remote Computer
You have the choice between administration of the service on your local computer, or on a remote machine. To connect to a remote system, enter that system's network name and click on "Connect".

Start / Stop
When the service has been installed properly, it can be started and stopped. **Start** launches the Syncovery Service process and activates its scheduler. **Stop** cancels whatever the service is currently doing and terminates its process. Please note that several seconds may pass after clicking on either of these buttons before the operation has completely finished.

See also:
The Syncovery Service

Other Related topics:
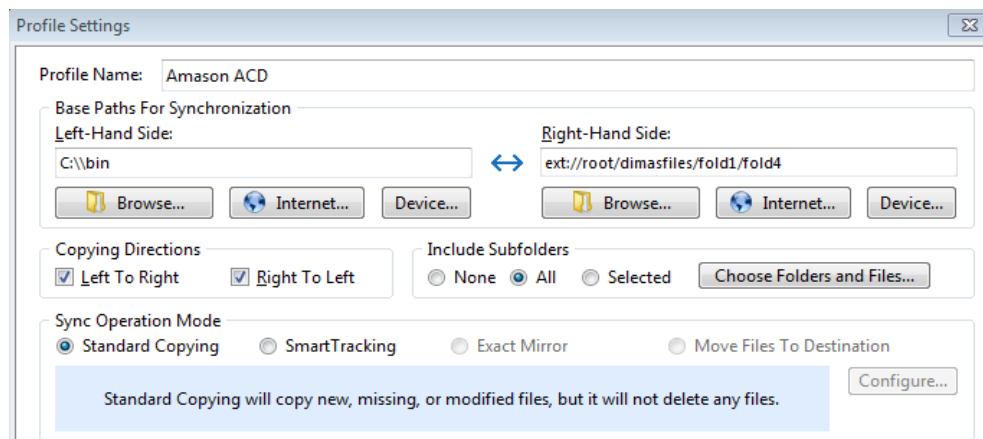Edit Profiles - More Profile-Specific Settings (Schedule)

Profile Settings Dialog

In order to create new Profile, click   'New Profile',

In order to edit a Profile, click   'Edit Profile' in toolbar of the Main From.
You will be shown Profile Settings dialog, where you can set-up custom options for synchronization profile.

Upper Part Of Dialog Box

In this area, you can
- specify the **profile name**
- choose the **paths** or folders to synchronize
- choose an **Internet** protocol (cloud server) or choose an **MTP Device** (such as a camera or smart phone)
- choose the **copying direction**
- choose **subfolders and files**
- specify the **Sync Operation Mode**

Profile Name
In this field, you can enter or change the profile's name. To create profile groups, just create several profiles whose names that start with the same first word, for example:
Backup Documents
Backup Music
Backup SQL Databases

When you change the name of an existing profile here, you will be asked if you want to also keep it under the original name when you click OK. The **Save As** button is an alternative way to creating a second copy of a profile.

Left-Hand Side
In this field, you enter the left path for the comparison or backup. Click the folder icon to browse for a folder. In the Professional Edition, you can use the **Internet button** to access Cloud Storage, FTP, SSH, WebDAV and many other server types. Click the **Device** button to choose a folder on an MTP device, such as a camera or smartphone.

Right-Hand Side Path
In this field, you enter the right path for the comparison or backup. The buttons work the same as for the left-hand side.

Copying Directions: Left To Right / Right To Left
It is very important to select the correct direction(s) for the synchronization. You may want to allow the synchronization to copy files in both directions, so that the newest version of either location is selected for each file. On the other hand, especially for backup purposes, you may already know that only one copying direction will be needed. Somer other settings are also dependent on the copying directions: some checkboxes will be disabled when only one direction is chosen, while others are only available when both directions are checked.

Include Subfolders
Specify if no, all, or selected subfolders on both sides are to be included in the synchronization process.

Choose Folders and Files...
This option will enable you to select files and directories from the main left/right folders. A new dialog window will come up. This dialog will show the folder trees of both synchronization sides. Please note that in most cases, you should only select files on one side in this dialog, because all folders selected on one side will automatically also be considered on the other.

Sync Operation Mode
The operation modes are also explained briefly on the dialog when you choose them.

Standard Copying
Standard copying will compare the files and folders present on each side, using the filenames, the "Last Modified" timestamps as well as the file sizes for comparison. Newer files and files that only exist on one side will be copied over to the other side. No files are deleted (except if you choose Real Time Synchronization and specify so on the Real Time settings dialog).

SmartTracking
SmartTracking uses a local database in order to track changes that have been made between the various invocations of the profile. That way, the software will know whether a file has been moved on the left side, or on the right side. It can also detect whether a file has been deleted on one side, or whether the file has

actually been added on the other. SmartTracking should always be used whenever you want to keep two locations in sync, both of which are being used for work. SmartTracking is not needed when you do a backup or mirror, or any other case where you synchronize in one direction only. SmartTracking has various additional features which you will see in the SmartTracking dialog box (click on the Configure button).

Exact Mirror
This option is available when copying in one direction only. The purpose is to create an exact mirror of the source path. This may even include deleting files, or overwriting newer files with older ones. Therefore, the option should be used with caution. However, before overwriting newer files or deleting files, confirmation will be demanded from the user - unless the process is running unattended or scheduled, and the Unattended options allow these actions to be carried out without user confirmation.

WARNING: if you want to run the profile in unattended or scheduled mode, be sure to go to the Unattended tab sheet and make the appropriate checkmarks there so that the software will indeed delete files etc. - if you want that to happen.

You can click the **Configure...** button to fine-tune the Exact Mirror behavior. In particular, you can specify a delay for deletions, and you can choose that excluded files are removed from the destination even if they exist on the source side.

Move Files To Destionation
This option will move the files from the source to the destination. The files will be deleted from the source side. You can also move files to two destinations at the same time: one is specified as the Right-Hand Side, and the other one is specified under Files->Deletions: Move Deleted Files Into A Specified Folder.

Advanced Settings
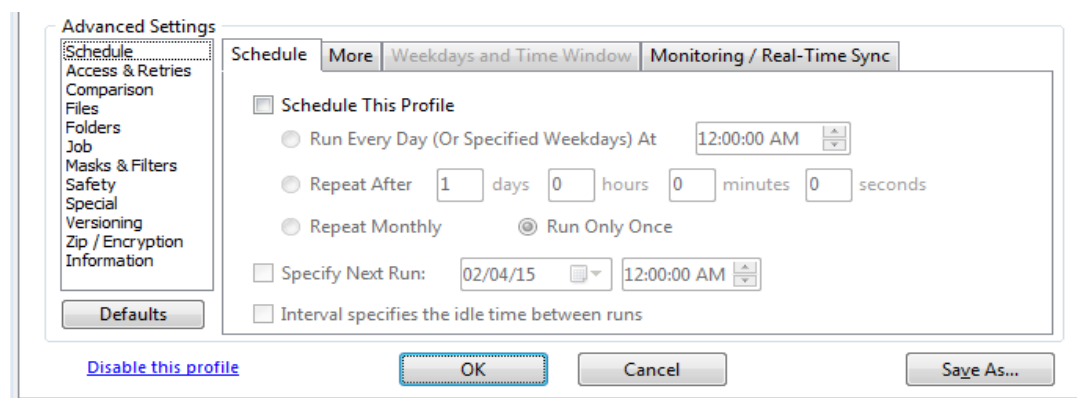
The Advanced Settings are available on the following tab sheets. The **Defaults** button resets the options on these tab sheets. It leaves the remaining options of the dialog box alone.

Schedule
- Profile Settings - Schedule
- Profile Settings - Schedule/More
- Profile Settings - Weekdays and Time Window
- Profile Settings - Monitoring / Real-Time Sync

Access & Retries
- Profile Settings - File Access
- Profile Settings - Waiting and Retrying

Comparison
- Profile Settings - Comparison
- Profile Settings - Comparison/More

Files

- Profile Settings - Files
- Profile Settings - Deletions
- Profile Settings - Files/More

Folders
- Profile Settings - Folders

Job
- Profile Settings - Job-Related Settings

Masks & Filters
- Profile Settings - Inclusion Masks
- Profile Settings - Exclusion Masks
- Profile Settings - General Filters
- Profile Settings - File Age and Size

Safety
- Profile Settings - Safety/Attended Mode
- Profile Settings - Special Safety
- Profile Settings - Safety/Unattended Mode

Special Features
- Profile Settings - Special Features
- Profile Settings - Database

Versioning
- Profile Settings - Versioning
- Profile Settings - Synthetic Backup
- Profile Settings - Versioning/More

Zipping & Encryption
- Profile Settings - Zipping
- Profile Settings - Encryption

See also: Profile Settings - Upper Part Of Dialog Box

Schedule

Schedule/Schedule

On this tab sheet, you specify whether the profile should run automatically when the Scheduler is turned on.

Schedule This Profile
Place a checkmark here in order to set up your profile for repeated automatic execution. As soon as the schedule is configured on this page, you can invoke the Scheduler by choosing its tab sheet from the main dialog and starting it there.

Run Every Day (Or Specified Weekdays)
To set up the profile to be scheduled once every day, select this option and specify the desired time of day. Also select this option if you want to run it once per day on specified weekdays only, even if it is only one day in the week. The weekdays are selected on a different tab sheet.

Repeat After
Select this radio button and specify the exact interval that you want to have between each profile run. If you want to run it several times a day, make sure the number for days is zero (0).

Specify Next Run
Place a checkmark here to set the time for the next profile run. You can remove this checkmark to have the scheduler choose a time on its own.

Interval specifies the idle time between runs
With this checkbox seleted, the scheduler will wait for the specified amount of time after a profile has completed before starting it again. For example, if the interval is one hour, and the profile takes one hour to complete, then it will be started every two hours. Without this checkbox, it would be started every hour. Or if it takes longer than an hour, it would be started again immediately after having completed.

Schedule/More

Run Upon Windows Login
This checkbox will cause the profile to be run in the background as soon as you log in to Windows. This is related to the scheduler setting "Auto-Start Background Scheduler With Windows Login" so you must leave that checked too.

Run Upon Windows Logout and Shutdown
With ths checkbox selected, the profile will run when you log out or shut down the computer. This will work as long as at least one Syncovery process is running and you see the icon in the system tray. The background scheduler would be sufficient for this to work. The timer running as a service cannot perform this task however.

Run Missed Daily Jobs Immediately When Scheduler Starts
Jobs might be missed due to the computer being turned off or the scheduler not running. This setting causes missed jobs to be started immediately, when the scheduler is started again, rather than waiting for their next scheduled time.

Add a Random Delay
This option is useful if you want to use irregular intervals, or a different time of day for each profile invocation. One reason for this could be many computers trying to back up their data to the same server, so that you want to have the load spread over a period of time.

Warn If Profile Not Run For X Days
Syncovery can remind you if a profile has not been run for a number of days. This feature is actually independent from the other scheduling settings, and it can be used for profiles that you run only manually also. If a profile has not run for the specified number of days, a dialog will pop up allowing you to run it, or to dismiss the warning.

Additional Times
You can specify additional times of day where the profile should run. However make sure to specify a main schedule first. These times will only be used if the profile has a schedule on the "Schedule" tab sheet.

See also:
Upper Part Of Dialog Box Advanced Settings

Schedule/Tab Weekdays and Time Window

Weekdays

If you don't want the profile to run each day, please uncheck some of the week days. Specify the time of day or the interval of profile invocation on the Basic or Advanced tab sheets.

Time Window - Run Only Between

Here, you can specify a time window during which the profile may be executed. However, this setting alone will not cause the profile to be run by the scheduler. Specify the time of day or the interval of profile invocation on the Schedule tab sheet.

You can choose to **Ignore this limitation on Saturdays and Sundays**, as well as specify whether running profiles should be **interrupted** at the end of the time window, and whether copying should stop even **in the middle** of a file.

Schedule/ Tab Monitoring /Real-Time Sync

This tab sheet serves two different purposes:
- Real-Time Synchronization
- Automatically running a profile when a drive becomes available or is connected

In addition, you will find the **Continuous Sync** checkmark, which may be useful when connecting to servers with Internet Protocols. It causes the syncs to occur as one profile "run" that repeats continuously without logging out from the server connection - as opposed to the normal behavior where Syncovery completes each profile run and logs out, and starts a new run at the next scheduled time, or when the next real-time events occur.

The setting at the bottom, **Minimum pause between actions** applies to all of these features. It can be used to avoid constant activity and to make sure that the profile isn't run too often.

For all of these features, the Scheduler must be running because it manages the monitoring and profile running.

Real-Time Synchronization - please see **Real-Time Synchronization chapter.**

**Run profile as soon as the drives or volumes involved become available**
This feature will cause the invocation of the profile to be triggered by the presence of network paths or other devices such as USB drives.

The profile will be executed as soon as a drive becomes available, or as soon as this computer is connected to the LAN.

The presence of a drive is detected by simply trying to access it at regular intervals. Specify the delay between access attempts here. In addition, you will usually want the profile to pause for a longer time when it has run successfully. You can specify the pause after a successful run by specifying a **Minimum pause between actions**.

Access & Retries

Access & Retries/File Access
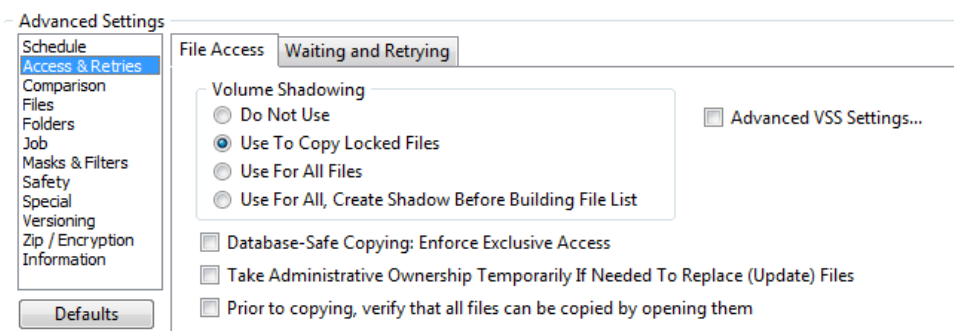
Volume Shadowing
Volume Shadowing is a feature available since Windows XP which allows the program to copy locked files (files which are in use by another program). You can specify if volume shadowing should be used, and when it should be used.

Since volume shadowing takes some time and causes additional CPU and disk usage, the default setting is to use it only to copy locked files. If there are no locked files, it is not used at all.

However, in many cases it is better to use the option "Use For All, Create Shadow Before Building File List". This ensures that a consistent snapshot of the folders is copied. It avoids changes or discrepancies between the building of the file list and the copying phase.

Using volume shadowing for all files also avoids any problems with applications trying to write to a file while it is being copied.

Volume shadowing is only available for local drives, not for network drives. This means that the software must be installed on the computer where the data is stored, rather than another computer on the network.

Dabase-Safe Copying: Enforce Exclusive Access
The database-safe mode makes sure that no other application can have a file open with write access while it is being copied. If an application is currently working with the file, the program will try to use volume shadowing, or it can be set up to wait until the file is free. If volume shadowing is not used while it is being copied, an application trying to access the file in read/write mode will fail and issue an error message. As soon as the copying is finished, the file can be used nomally again.

Take Administrative Ownership Temporarily If Needed To Replace (Update) Files
This feature works when the program is running "as administrator", or the scheduler is installed as a service and it has administrative privileges. It can help copying files which are normally not copyable by the account that the program is running under.

Prior to copying, verify that all files can be copied by opening them
This setting is rarely used. It ensures (as much as possible) that the copying is only done if all files can actually be copied. That way, you will either get all files copied successfully, or none. To make this possible, a separate step (checking all files) is added before the actual copying starts. If any file is not accessible on the source side or is not writeable on the destination, then the profile will be stopped. Usually this setting is used when profiles are run via scheduler, so that another attempt to copy the files will be made at the next scheduled time.

Access & Retries/Waiting and Retrying

Wait For File Access
In both Database-Safe and normal mode, it can occur that other applications prevent the program from accessing a file that needs to be copied. When that happens, the program doesn't just abort or skip the file. Instead it will continue copying the remaining files, and then (depending on this option setting) start retrying the files that couldn't be processed yet. You can specify for how long the program should retry the files. It will use only minimal resources during this period, so don't be afraid to set the retry-time to a high number.

Wait And Retry If Transfer Or Reading Problem
This checkmark can make the copying extremely fault tolerant. If there are any connectivity problems, the program will retry for as long as you specify.

Re-run the profile if an error occurs
• while the building file list
• while running the profile

These settings allow you to have the whole profile re-run automatically if any error has occured. You can specify whether to re-run only once, or to re-run until it has completely succeeded. Also specify the number of seconds to wait before each re-run.

Comparison

Comparison/Comparison
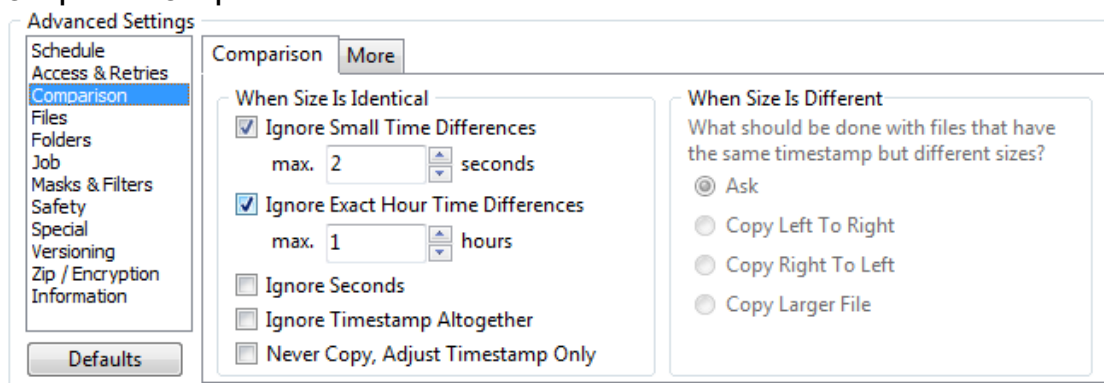
Normally, files are compared primarily based on their timestamp - the time and date of the last modification. However, in some cases, the timestamp may be (slightly) different, but the files are really the same. To cope with that, some special cases can be recognized by Syncovery.

So, If and only if the file sizes are identical:

Ignore 2 Second Time Differences
If this option is checked, timestamps with deviations of two seconds or less are considered identical. This is needed when synchronizing files between FAT and NTFS file systems, because FAT file systems can only store even numbers as seconds.

Ignore Exact 1 Hour Time Differences
This setting may often be useful to compensate for different computers or filesystems and how they treat **daylight savings time**. Sometimes, the timestamps reported by the operating system differ by exactly one hour even though they are really the same. With this option checked, this problem will be solved, and it is irrelevant whether the left or the right side of the comparison is one hour behind.

Ignore Seconds
This setting causes the program to ignore seconds when comparing the timestamps of two files.

Ignore Timestamp Altogether
This setting should be rarely used. Files of the same size are assumed to be identical regardless of the timestamp. You should only use this setting if you know exactly why.

Never Copy, Adjust Timestamp Only
Sometimes you may have a copy of your files where the timestamps do not match. This function will adjust the destination timestamps to match the source. It works only in one-way sync scenarios. By adjusting the timstamps, you can avoid having to re-copy the files just to get the timestamps correct. However, you should only use this feature if you know that all files with the same size actually have the same content. Usually, this option is used only for a single, manual profile run, rather than using it permanently for regularly executed profiles.

When Size Is Different:

Some program tend to modify the file size but keep the original timestamp when you open a file, even if you don't make any changes or save it. When you run a synchronizing job in attended mode, the program will ask you what to do. To avoid the question, and to specify a behavior for unattended mode, please specify what to do in such cases here.

Comparison/More
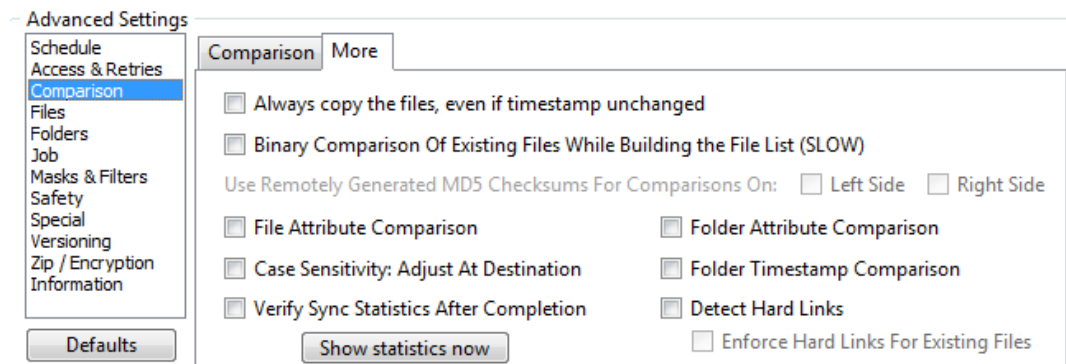
Always copy the files, even if timestamp unchanged
The program normally copies files only if they don't exist on the other side yet, or if the "Last Modified" timestamp has changed. However, some programs don't update the files' timestamps even if their content changes. This checkmark causes all files to be copied even if apparently unchanged.

Binary Comparison Of Existing Files While Building the File List (SLOW)
If you want to verify that the file contents of existing files is 100% identical on both sides, use this setting. Only files which would normally be considered identical by looking at the file size and timestamp will be verified. If the binary comparison shows that the files are different, they will be marked for copying in the profile's main copying direction. If the profile has both directions checked, then the Synchronization Preview will show such files with the word CONFLICT and it will not do any copying by default. You can then set the desired copying direction in the Synchronization Preview.

This checkmark should not usually be used for jobs that run regularly, because it causes a lot of disk usage or network traffic. Moreover, this checkmark does not cause newly copied files to be verified. To verify files after copying, use the checkmark *Verify copied files* on the Files tab sheet.

Use Remotely Generated MD5 Checksums For Comparisons
This checkmark will make the program use MD5 checksums for verification rather than a complete binary verification. To make this work, the Syncovery Remote Service must be running on the other end, or an FTP server must support the MD5 command.

Attribute comparison
This setting causes the program to compare file attributes, such as *Read-Only*, *Hidden*, and *Archive*. When files are identical except for the file attribute, the file is not copied again. Only the attribute is changed on the destination side.

Folder Attribute Comparison
Folder attributes can be compared/copied also. Most folders don't have special attributes, but some folders do - for example folders with a customized folder icon. The icon will only appear on the copy if this setting is chosen.

Case Sensitivity: Adjust At Destination
Filenames on Windows are not case-sensitive. This means that myfile.doc would be the same file as MyFile.DOC. However, you may want your files to look identical. So, if you have a folder where some spellings are different in terms of case, then you may use this setting in order to adjust the case at the destination. You can only use this option when the profile has only one main copying direction.

Folder Timestamp Comparison
If you are synchronizing in one direction, you may want the folders on the destination to have the same timestamps as on the source side. Newly created folders are automatically adjusted in this way, but existing folders may deviate. To have existing folders adjusted on the destination side, use this checkbox.

Verify Sync Statistics After Completion
This checkmark should be used only rarely! It will cause the left and right folder trees to be scanned completely again after the synchronization has completed. This verification stage will end in detailed

statistics which are used to verify that the backup or mirror is complete. Any files or folders that still don't exist on both sides are listed.

Detect Hard Links
On recent versions of Windows, a file can have an entry in several folders. But it is the same physical file. Normally, the program would copy such files to independent copies in the folders on the destination. To keep the files hard-linked on the destination, this checkmark must be chosen.

Enforce Hard Links For Existing Files
This checkmark can be chosen to update the hard-link status for existing files so that it matches the source side.

Files

Files/Files
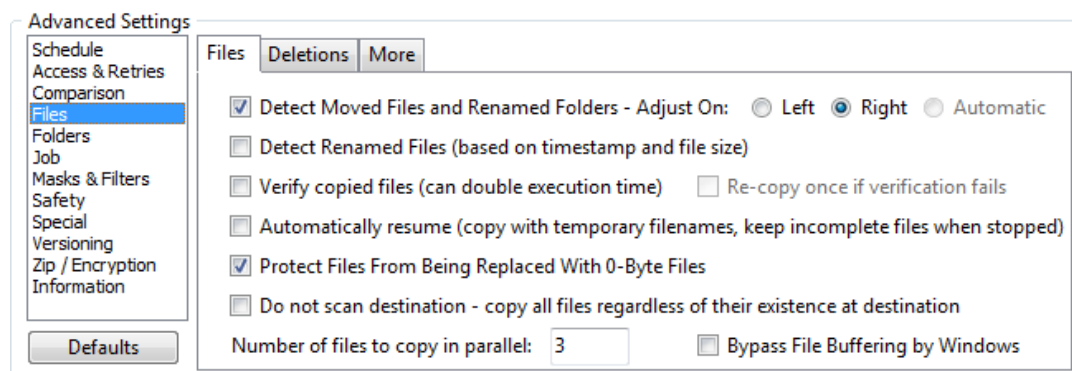
Detect Moved Files and Renamed Folders
When files have been moved into different folders, or even when the folder structure has been reorganized, Syncovery can detect this. Rather than creating duplicates by merely copying files between the left and right locations, it will perform the same moves that you have done on one side, on the other side. Select this option to enable the detection of moved files.

A limitation of this feature is that moved files can only be recognized as such if they haven't been edited on one side. If they still carry the same timestamp and they still have the same size on both sides of the synchronization, then this software is able to detect that they are identical, even if they are not in the same folders.

You also need to specify whether the location of moved files should be adjusted on the left-hand side or on the right-hand side. On the side that you choose, the file will be moved in such a way that its new location matches that of the other side. Note that these radio boxes are automatically adjusted when you change the main direction of the synchronization.

If you don't want to specify a fixed side (left or right) where the location of files should be adjusted to match the other side, you can use **SmartTracking**.

Detect Renamed Files (based on timestamp and file size)
This feature can detect renamed files. It works only when file deletions are processed. If it sees a file that is to be deleted, and another one that is to be copied, and they have the same timestamp and file size, it will transform these two actions into a rename action.

Verify copied files (can double execution time)
This checkmark will cause the program to verify the file contents after copying. The verification is done by reading the complete source and destination files once more and comparing them. So this will potentially double the execution time, drive access and network traffic. To avoid this, it is possible to use a remotely

generated MD5 checksum for verification. The checksum can be calculated by the Syncovery Remote Service running on the other end, or by an FTP server supporting the MD5 command. The MD5 comparison option must be chosen under Comparison/More.

Automatically resume (copy with temporary filenames, keep incomplete files when stopped)
This checkmark will enable resuming of interrupted copying operations even when the job is stopped and run again later. During copying, the destination filename will have an additional extension, flagging it as a temporary file. When the copy is complete, the destination file will be renamed to the actual file name. The checkmark is recommended in many cases, because it can prevent incomplete copies on the destination from replacing good files, and thus avoid data corruption. It is also useful to prevent incomplete files from being processed by other software, or from being copied by other profiles.

Protect Files From Being Replaced With 0-Byte Files
This checkmark prevents empty files from being copied over a non-empty file.

Do not scan destination - copy all files regardless of their existence at destination
When copying only in one direction or moving files, you can select that the program does not check to see which files are currently present on the destination side. The purpose is usually speeding the profile up. This however means that all files will be copied each time unless filters are applied. For backup purposes, you may want to combine this setting with the Archive filter (*Copy Only Files With Archive Flag* and *Clear Archive Flags*).

Number of files to copy in parallel
Copying several files in parallel threads can be a great way to speed up the process. It may make better use of your network bandwidth, but may not be a good idea if you are copying extremely large files.

Bypass File Buffering by Windows
In some cases, the file buffering done by Windows can lead to problems, such as excessive memory usage for caching. Bypassing the buffer can solve such problems, and can speed up the copying in some cases. In other cases, it might slow it down. Whether this option improves the performance needs to be tried out. The default setting is not to bypass the file buffering.

Files/Deletions
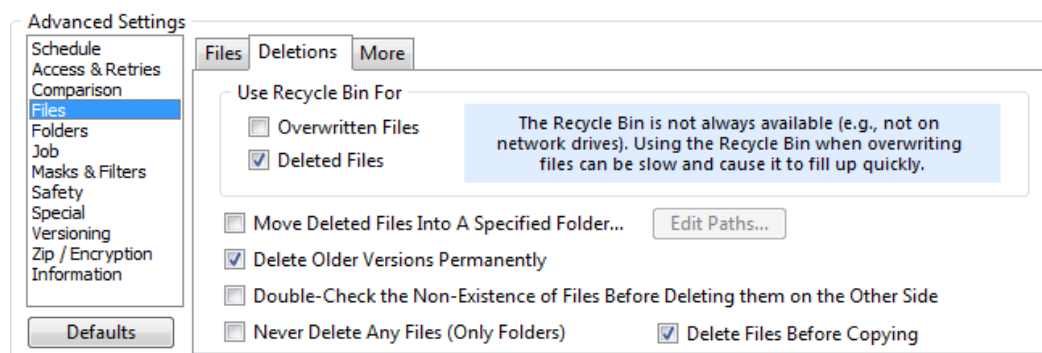
Use Recycle Bin
These options cause Syncovery to try to use the recycle bin for overwritten files and/or files to be deleted. That way, you will have a chance of retrieving older versions that were replaced or deleted, if necessary. Please note that the recycle bin is not always available, especially not on network drives or FTP servers.

Move Deleted Files Into A Specified Folder...
This setting provides a more reliable alternative to the recycle bin. Rather than deleting files, they will be moved into a special folder which you specify. This setting works even with network drives or FTP servers.

Delete Older Versions Permanently
This setting causes older versions of deleted files to be removed from the destination.

Double-Check the Non-Existence of Files Before Deleting them on the Other Side

This checkmark causes the program perform a double-check of files before deleting them from the other side. Deletions can occur in Exact Mirror and SmartTracking mode if files have been removed from one side. However to rule out any uncertainty the program can double-check if such files are really no longer there. This might be necessary if unstable network connections might cause files not to be seen even though they are still there.

Never Delete Any Files (Only Folders)
This checkmark allows Exact Mirror to be used to mirror the folder structure but prevent any files from being deleted from the destination.

Delete Files Before Copying
To free space on the destination, file deletions normally take place before new and updated files are copied. However to protect the integrity of the data on the destination better, you can uncheck this option so that the deletions are done last.

Files/More
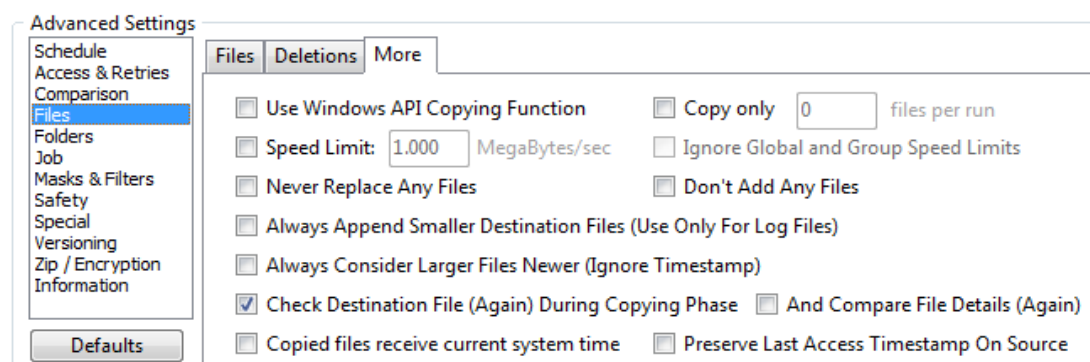
Use Windows API Copying Function
This option causes the program to use a file copying algorithm provided by Windows, rather than using its own copying routine. This affects only the copying process of each individual file, not the general behavior of the software when processing a profile. The Windows API Copying function is sometimes more compatible with some devices, so this option is automatically checked for removeable devices, network drives, and drives connected via USB. However, the Windows API Copying function may sometimes be slower than the internal copying routine.

Copy only X files per profile execution
When this option is selected, the profile will stop after copying the specified number of files. The remaining files, or another X files, will be copied during the next profile run.

Speed Limit
If you want to limit the bandwidth that the copying process will use, you can specify it here. Note that while the copying is running, you will still be able to turn this limitation on or off.

Ignore Global and Group Speed Limits
This causes the global speed limits to be ignored. The global speed limit can be specified on the Program Settings dialog. Group Speed Limits can be specified by right-clicking a profile on the Profile Overview screen. This option is enabled only if the Global Speed Limit Mechanism is activated on the Program Settings dialog, tab sheet Advanced.

Never Replace Any Files
A rarely used option. This setting causes missing files to be copied over, but existing files won't be updated even if newer versions exist on the other side of the synchronization.

Don't Add Any Files
Use this setting if you want to update existing files only and not copy any new files from one side to the other. This is also rarely used.

Always Append Smaller Destination Files (Use Only For Log Files)

This setting causes destination files to be resumed when the source file is larger. The program does not verify if the file is still the same, so this option is not usually employed in order to resume transfers. For general resuming, use the Auto-Resume feature from the Files tab sheet. A good example of where the Auto-Resume feature cannot be used so that you must use the setting "Always Append..." would be log files which get bigger each day, and you only want to copy the new information each time. In some cases, you may need to combine this option with the following one so that the program uses the suitable copying direction.

Always Consider Larger Files Newer (Ignore Timstamp)
This settings causes the timestamp to be ignored, and files to be compared only by their size. This is not normally recommended but may sometimes be necessary.

Check Destination File (Again) During Copying Phase
Normally, the program checks the existence of the destination file just prior to copying each file, in order to see if it is going to be overwritten. However, some NAS devices respond slowly to these checks if the folder contains many files. Therefore, you can disable this setting in order to speed up the process.

And Compare File Details (Again)
This checkmark also causes the Last Modification timestamp of the files to be compared again just prior to copying. If the situation has changed and the file no longer needs to be copied, it is skipped.

Copied files receive current system time
This option is rarely used. Normally, files copied to the destination are given the same timestamp that they had on the source side.

Preserve Last Access Timestamp On Source
By default, Windows may update the Last Access Timestamp of the source files when they are accessed for copying. Using this checkmark can prevent that.

Folders
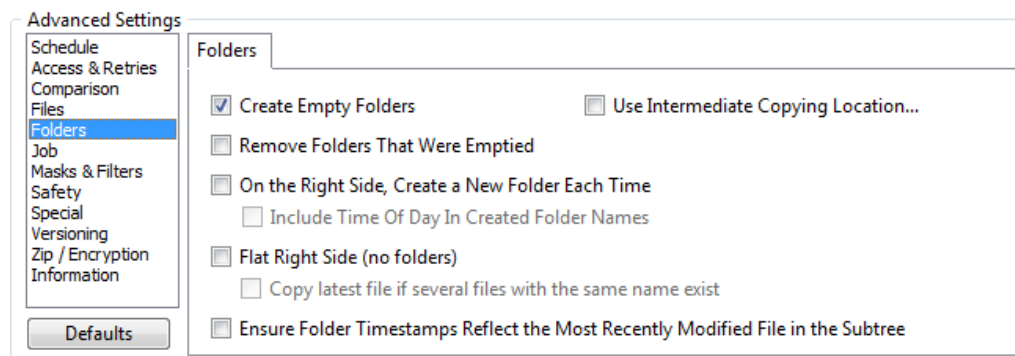
Create Empty Folders
Here, you can specify whether emtpy folders are replicated. The setting can also be used to avoid creating a empty folders which are shown as empty only because of your filename masks (inclusions/exclusions).

Remove Folders That Were Emptied
Rarely Used! This is not necessary to create an Exact Mirror. In Exact Mirror mode, non-existent folders are deleted from the destination by default. In SmartTracking mode, deleted folders are deleted from the other side without this setting, too. This option is something different (see below).

If you would like folders that are emptied during the profile run to be removed also, activate this setting. One use case for the setting is the operating mode "Move Files To Destination" where you can choose to delete emptied folders on the source side with this checkmark.

On the right side, create a new folder each time
If you are using the profile for backup purposes, you may want to direct your regular backup into a new folder each time. This folder will be created, and it will contain the current date of the backup in the folder

name. You must combine this setting with the two "Archive" flag settings on the Filters tab sheet. The "Archive" flags will signal to the software that a file needs to be backed up. Because older backups are contained in various separate folders, the software cannot check whether a file is already contained in an older backup. Therefore, it must depend on the "Archive" flag if you are directing each backup into a separate folder.

Flat Right Side (no folders)
This is a rarely used setting. If you would like to move or copy files from a folder tree on the left side into a flat folder without subfolders on the right side, then use this setting. Files from any subfolder on the left-hand side will be copied into the base folder on the right-hand side.

Ensure Folder Timestamps Reflect the Most Recently Modified File in the Subtree
This option offers a solution to the following problem: in Windows, folder timestamps are updated when a file in the folder changes or a new file is added. However, only the direct parent folder of changed files are updated. Folders further up in the hierarchy will still show an older modification date. For this reason, folder timestamps cannot safely be used as a filter because an older date in a folder doesn't mean that there aren't newer files in any subfolder.

When making a copy of a folder hierarchy, Syncovery can make sure that on the destination side, the folder timestamps do really reflect the most recently modified file in the complete subtree. This folder timestamp adjustment is only made on the destination side. The use case for this is that if you use additional profiles to distribute your files further from this profile's destination, then you will be able to use folder timestamps for filtering.

Use Intermediate Copying Location
This setting will copy the files to an intermediate location first. When this part of the copying is complete, the files will then be moved to their final destination. This is rarely used.

Job

Job/Job-Related Settings
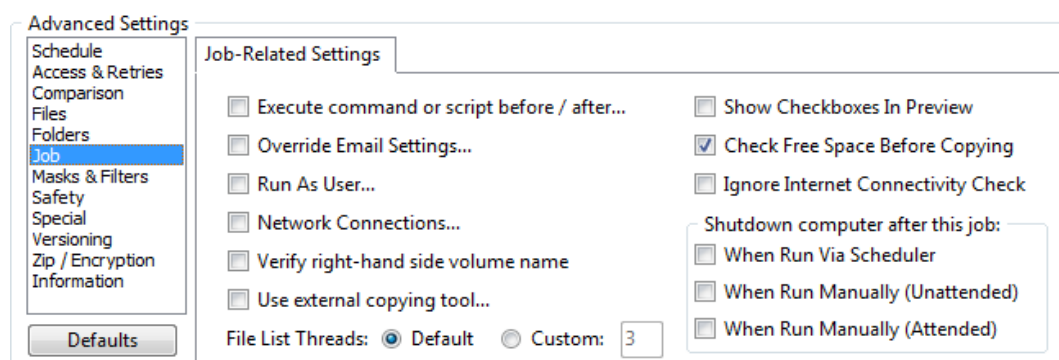
Execute command or script before / after...
This option allows you to execute programs or script at the beginning and/or at the end of the profile.

Override Email Settings...
A separate dialog box will appear which allows you to override some of the email notification settings in each profile. For example, you can specify whether emails are sent for this profile, and override the recipients list.

Run As User...

If you need to run this profile under a different user account in order to be able to access specific files, then you can specify the credentials here.

Network Connections...
Click here to specify network connections that should be made when the profile is run. In most cases, this is not needed because network connections are already active.

Verify right-hand side volume name
This setting is used when you make sure that the profile is only run with the correct backup medium inserted. When you click on this checkbox, the current volume label is read from the drive containing the right path. In the future, the Syncovery will verify that the disk inserted has the same volume label before running this profile. You may, however, use multiple disks with the same volume label. If the volume label does not match, the program will check if any other drive letter matches and will replace the drive letter automatically. As an alternative to this checkbox, you can simply write the volume label in the left or right base path for the synchronization, for example:
USBSTICK:\My Files *(where USBSTICK is the volume label of the desired drive to use)*

Use external copying tool...
This option allows you to set up external command-line tools which will do the copying instead of the internal copying algorithms.

File List Threads
Specify how many parallel threads should be used when scanning the folders. The default numbers are specified on the Program Settings dialog, tab sheet *Performance*. A higher number of threads may make the "building file list" step faster, but will also use more CPU. The number should not be too high. In most cases, between 3 and 10 seems reasonable, but you can go much higher. Some settings and cloud servers may cause only one thread to be used, so the setting may be ignored in some cases.

Show Checkboxes In Preview
This setting causes checkboxes to be shown in the Sync Preview to allow you to easily choose the files to be copied. It is mostly used by the Restore Wizard.

Check Free Space Before Copying
This checkmark allows you to turn off the free-space check in case of problems.

Ignore Internet Connectivity Check
On the Program Settings dialog, tab sheet *Startup*, you can choose to run jobs only if a specific Internet connection is active. The feature allows you to avoid making cloud backups while on a mobile connection, for example. This checkmark here allows you to skip the Internet connectivity check for this profile, which you may want to do for local copying.

Shutdown after this job
Specify in which situations the computer should be shut down when the job completes.

Masks & Filters

Mask&Filters/Inclusion Masks
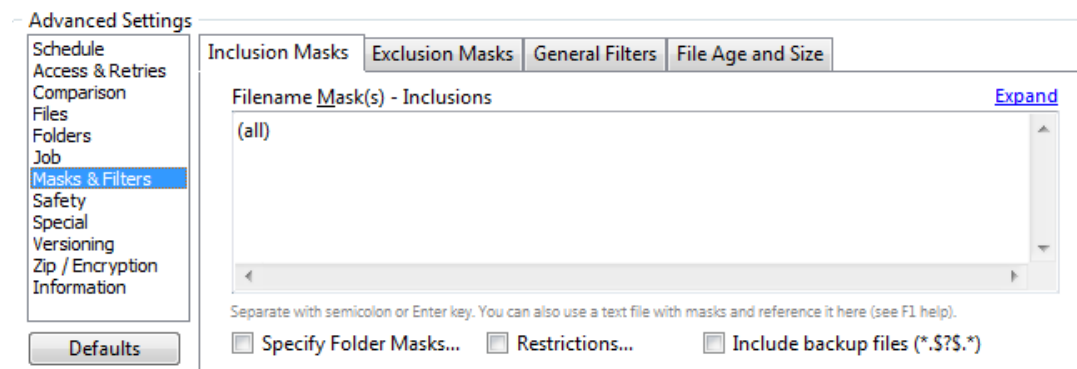
Filename Mask(s)
Specify which files to process. Normally, **(all)** or ***** means all files. Alternatively, you can specify filename masks such as *.doc or *.xl?. You can also specify complete file names here, but no folders.

The masks, or the file list to copy, can also be read from a text file. In that case, start the line in the Inclusion Masks edit field with a colon : and type the full path of the text file directly after it.

If the text file contains only subfolder selections, start the line with :+ like this:
:+C:\subfolders.txt

The subfolder text file can contain lines such as:
\folderA
\folderB

Specify Folder Masks...
A separate dialog will come up allowing you to specify folder name masks. For example, you can use this in order to find all folders with the word ARCHIVE in their names and have them processed.

Restrictions...
Rarely used. Allows you to specify separate file masks for one of the two possible copying directions.

Include backup files (*.$?$.*)
When using the setting to keep multiple backup versions of the same file (see More), this software may create backup files such as MyFile.1.doc. In order to avoid these files being copied back from the backup location to the main data location, these backup files are normally not included in any synchronization. However, if you want to override this hard-wired exclusion, you can place a checkmark next to this setting.

Mask&Filters/Exclusion Masks
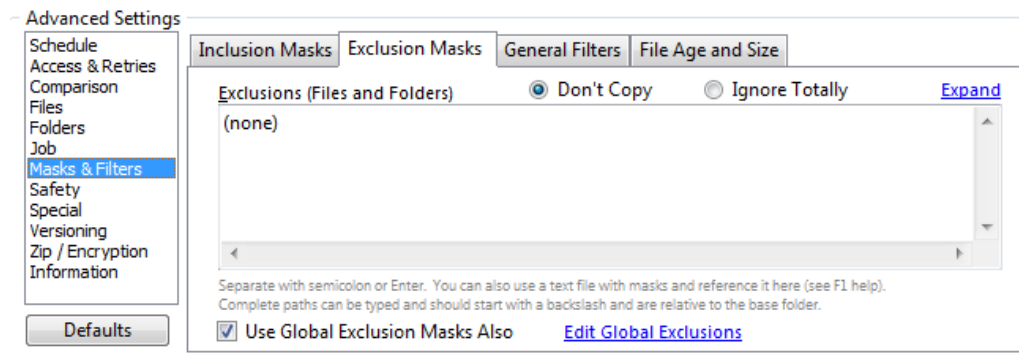
Exclusions (files & folders)
You can exclude certain files or folders such as *.tmp or *.bak. You can also specify complete file or folder names here. You can enter only the name to exclude, or full paths or a part of the name combined with wildcards. Wildcards to use are * and ?.

Trailing backslashes are not allowed. Folders are specified in the same way as files. Wildcards are only allowed in the name itself. So if you specify a full path, only the last part (the name) can contain wildcards.

The recommended way to enter full paths is to use them relative to the profile's base paths. So you start with a backslash and then type only those folders in the path that are relative to the base.

Examples:
*.tmp
\TEMP
\Users\All Users
.*
\My Documents*.jpg

The exclusion masks can also be read from a text file. In that case, start the line in the Masks edit field with a colon : and type the full path of the text file directly after it.

Don't Copy versus Ignore Totally
When the Exclusion Masks are processed in **Don't Copy** mode, this means that such files won't be copied but they will still be processed for deletion if they exist at the destination and not at the source, and if you are using Exact Mirror Mode. In contrast, the **Ignore Totally** mode will not process files that match the exclusion masks in any way. This can sometimes lead to a situation where such files are left at the destination and folders that should be deleted can't be deleted because they still contain these files. Therefore, **Don't Copy** is the default setting.

Use Global Exclusion Masks Also
The Global Exclusion Masks are specified on the Program Settings dialog and they are applied to all profiles unless this checkmark is deselected. They contain masks that avoid copying of some temporary files as well as the Recycle Bin contents and other system folders that cannot and should not normally be copied.

Mask&Filters/General Filters
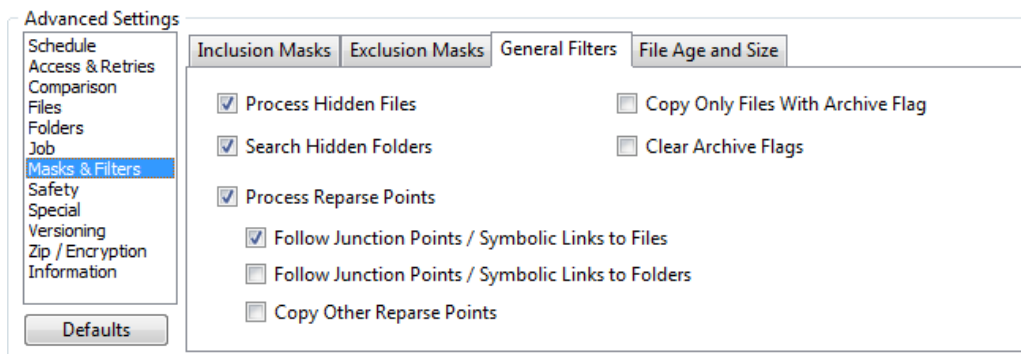
Process Hidden Files
This option determines whether hidden files are seen and handled by the program.

Search Hidden Folders
This option determines whether hidden folders are seen and examined by the program.

Copy Only Files With Archive Flag
This option is used for data backup purposes. Whenever a file is changed, Windows will normally set the Archive flag for that file. This signals that the file needs to be backed up. For normal synchronizations, the flag is not needed because the software looks at the left and right sides and decides for itself which files have been updated or added. However, in a data backup context you may sometimes use the software in such a way that the backup medium doesn't always contain all the files from previous backups. In that case, the software would start to back up old files again. To avoid that, you can use this setting. Use it in conjunction with the following setting:

Clear Archive Flags
This setting is used in conjunction with the previous one, also related to the Archive flag. For the preceding option to be useful, the last backup job for any given data folder should clear the Archive flag so that in order to signal that the file has been backed up, and doesn't need to be backed up again unless it is modified. If you have only one backup job for your data, and you are using the filter "Copy Only Files With Archive Flag", then you should check this setting too. If you have several backup jobs for the same data, please make sure that the last backup job that runs clears the Archive flag. Again, you only need to do this if you are working with Archive flags at all (and the preceding option is checked).

Process Reparse Points
This checkmark determines whether Reparse Points / Junction Points such as Symbolic Links are processed or ignored. You may want to ignore them if you get errors and don't need them copied, which happens sometimes with some of the default links that Windows creates, such as "My Music". The detection and processing of reparse points may depend on whether the job is being run under an Administrator account or not. For this reason, you may be getting different results in manual profile runs from those runs initiated by the scheduler when it is running as a service, because the service is not limited by Windows UAC (User Account Control).

Follow Junction Points / Symbolic Links to Files
This checkmark determines whether symbolic links (soft links) to files are followed (i.e. the content is copied even if it is actually saved in a different location on the source side). If it is not followed, Syncovery tries to recreate the link as a link on the destination side.

Follow Junction Points / Symbolic Links to Folders
This checkmark determines whether symbolic links (soft links) to folders are followed (i.e. the linked subtree is scanned as if it were a normal folder). If it is not followed, Syncovery tries to recreate the link as a link on the destination side.

Copy Other Reparse Points
Specify whether Syncovery should try to copy other reparse points as they are. These can be custom reparse

points from other applications, as an example.

Mask&Filters/File Age and Size

File Sizes Must Be Within
This option enables you to copy only files within a certain range of file sizes. Sample file sizes are: 512, 2.12k, 5M, 2G.

File Dates Must Be Withing
Using these settings, you can limit the synchronizing to files last modified or created within a certain period of time.

File Age
Rather than specifying a fixed date range, you may want to choose a certain age for the files that you want to synchronize. The age that you specify is always seen relative to the current date when the profile is executed.

Filter By: Last Modification / Creation
By default, the above timestamp filters take into account the date and time of the last modification of each file. In some cases, you may want to filter by creation date, so you can choose it here.

Apply To: Files | Folders | Both
To get the most reliable operation of the file date filter, please use the default setting of **Apply To: Files** only.

Folder timestamps under Windows are not consistent in such a way that they would be reliable for filtering. Applying timetamp filters to folders will often result in undesired exclusions of files.

However, there are some use cases where you may want to apply the filter to both files and folders, or even to folders only. For example, if you are distributing files from a copy of your folders made by another Syncovery profile, then you may filter by folder timestamps if the other profile has the option "Ensure Folder Timestamps Reflect the Most Recently Modified File in the Subtree" chosen on the Folders tab sheet.

Target Date for Restore
This option is mainly used by the Restore Wizard. By specifying a date in the past, the program can automatically choose the appropriate older versions of files when restoring (i.e. copying from the right-hand side to the left-hand side). This works for backups created with the Versioning settings.

Safety

Safety/Attended Mode
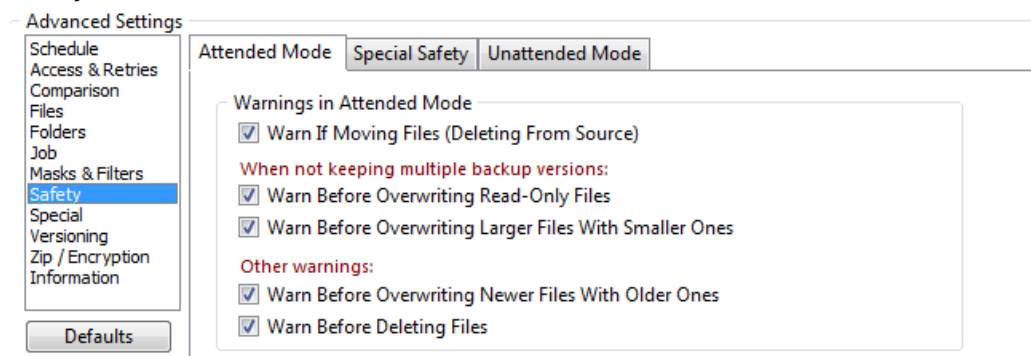
These options specify which warnings Syncovery is going to generate in certain situations encountered during file synchronization. These options are only in effect when the program is running in attended mode (i.e. not scheduled, and not otherwise invoked in unattended mode).

Warn before running a profile that moved files and deletes from source

This warning will come up when a profile with the "Move Files" mode is started. The warning can be confirmed and disabled for the future when it appears, so you do not need to remove the checkmark on this tabsheet (it will be removed when the warning is permanently confirmed).

When not keeping multiple backup versions:

Warn before overwriting read-only files

In Windows Explorer, when you right-click a file and choose "Properties", you can choose to protect a file by choosing its *read-only* attribute. Some applications also protect important files by marking them read-only. This option determines whether read-only files are replaced with or without requiring confirmation from the user. Note that this warning only occurs when the program is not configured to keep multiple backup versions of each replaced file (see Edit Profiles - More Profile-Specific Settings (More)).

Warn before overwriting larger files with smaller ones

This is the warning that is most frequently turned off. When editing documents, the files don't always become larger. It often happens that the most current version is smaller than a previous one. If you don't want to have to manually confirm such cases, you can uncheck this option. Like the previous one, this warning only occurs when the program is not configured to keep multiple backup versions of each replaced file (see Edit Profiles - More Profile-Specific Settings (More)).

In Exact Mirror Mode, or when manually specified:

Warn before overwriting newer files with older ones

In Exact Mirror Mode, the program will try to make the mirror match the model exactly. This can mean that sometimes, files need to be replaced by ones with an older modification date. In that case, the software will normally require confirmation from the user. To avoid having to confirm this replacement, uncheck this option.

Warn before deleting files

Another thing that can occur in Exact Mirror Mode is that files need to be deleted from the mirror because they no longer exist on the "model" side. In that case, the software will normally require confirmation from the user. To avoid having to confirm these deletions, uncheck this option.

Safety /Special Safety

Special Safety Warnings

Syncovery includes additional safety checks to avoid accidental deletion of files. It is important to be aware of these safety checks because they can prevent intended deletions from being carried out if you ignore them. The safety checks must be individually configured or turned off in each profile.

To turn the safety checks on for Unattended Mode, please see Profile Settings - Safety/Unattended Mode.

When a profile is executed and more files are going to be deleted than allowed by the new safety checks, then the user must confirm the deletions even in unattended mode. Without the confirmation, the profile will be executed without the deletions.

The safety checks have been designed to catch the following situations:
• files have been accidentally deleted on one side of a synchronization
• incomplete or empty FTP directories are received due to bad communication

Especially when incompletely received FTP directory listings could cause the profile to delete files, it is recommended to turn these safety checks on (but you can change the pecentages that trigger the warnings).

Again, to turn the safety checks on for Unattended Mode, please see Profile Settings - Safety/Unattended Mode.

Safety/Unattended Mode

These options specify how Syncovery behaves in unattended mode, and at which times unattended mode is in effect.

Overwrite Read-Only Files
When this option is checked, the software will automatically overwrite read-only files when running in unattended mode. In attended mode, it always demands a confirmation from the user. When this option is unchecked and the profile is run in unattended mode, then read-only files are skipped without any notification whatsoever.

Overwrite Larger Files With Smaller Ones If File Dates Require It
When this option is checked, the software will automatically overwrite larger files with smaller ones when running in unattended mode - if the files' modification dates require it. In attended mode, it always demands a confirmation from the user in this case. When this option is unchecked and the profile is run in unattended mode, then such files are skipped.

Exact Mirror Mode May Overwrite Newer Files
In order to create an exact mirror, the Exact Mirror Mode may sometimes have to overwrite newer files with older ones. Normally, it would ask the user to confirm this. However, when run unattended, this option must be checked or those files will not be replaced.

Exact Mirror Mode May Delete Files
In order to create an exact mirror, the Exact Mirror Mode may sometimes have to delete files. Normally, it would ask the user to confirm this. However, when run unattended, this option must be checked or those files will not be deleted. In addition, please specify a percentage of files that may be deleted. For example, if you leave the figure at 90%, the profile would **not be executed** at all if more than 90% of the files currently present on either side would be deleted.

The program will **never delete all files** from either side of the synchronization, even if you specify 100% here. If deletion of all files can occur and you really want it to happen, then you need to create a dummy (text) file which always stays on both sides and which disables this security mechanism, simply by being there. If this is not feasible and you really need the profile to delete all files regularly, please contact support@syncovery.com for a solution.

Enable Special Safety Checks
These are new safety checks to prevent accidental deletion of files. **They may prevent your profile from being executed at all**. Please see the Attended tab sheet for details.

Special

Special/Special Features
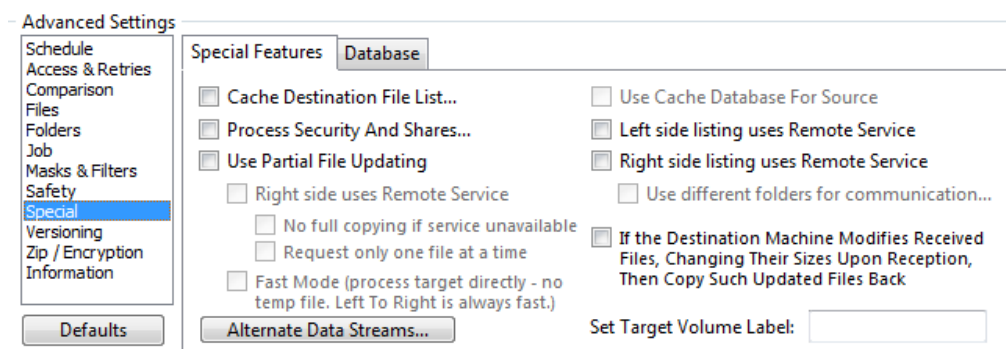
Cache Destination File List...
The file list of the destination side can be buffered in a cache, which is stored as a database on your computer. When this database is used, building the file list can be much quicker. However, you need to make sure that no other program or persons modifies the destination side, because otherwise it would get out of sync with the cache.

This setting will speed up running a profile by using a database as cache for the destination file list. It can be used in the following case:
• you are copying only from source to destination (not in both directions)
• nobody else, and no other profile, is modifying the files on the destination
• you want to speed up building the file list, and it needs the speed-up because the destination is

relatively slow (such as FTP or WebDAV)

Note that the cache may actually **slow down** building the file list in some cases, so you need to try it out. Local scanning and even folder scanning over a local network, or with a recursive listing from an Internet Protocol, is usually faster when done directly rather than with the cache.

There are many other ways to speed up building the file list. Please see the documentation on our web site:
https://www.syncovery.com/documentation/faq/fastlist/

Use Cache Database For Source
This setting is only used by the Restore Wizard. It enables you to use the database cache for the source side rather than the destination. This is not usually reasonable for profiles that run regularly. The typical application is a restore operation.

Process Security And Shares...
A separate dialog will appear where you can specify how the program copied file security settings and/or folder shares.

Use Partial File Updating (Block Level Copying)
Partial file updating can speed up backing up very large files of which only a portion changes each day. For example, SQL database files may be a good candidate for this setting. For more information, please see Partial File Updating.

Left/Right side listing uses Remote Service
The Syncovery Remote Service can speed up building the file list if you are synchronizing across a network or even over the Internet. It is installed on the other end and generates the file list so that the main program can download it. These checkmarks are used in the main program to activate this feature. See also www.syncovery.com/remoteservice.

If the Destination Machine Modifies Received Files, Changing Their Sizes Upon Reception, Then Copy Such Updates Files Back
In some cases, when uploading documents to a server such as a Sharepoint Server, the server may add some additional information to the file. The file size then no longer matches. To fix the mismatch, this checkbox will cause Syncovery to copy the updated file back from the server shortly after having uploaded it.

Alternate Data Streams
Alternate Data Streams are normally copied along with the file without any special setting. If you need special handling of Alternate Data Streams, you will find some options via this button. Note that Alternate Data Streams are not copied when zipping or encrypting files, or when copying via Internet Protocol.

Set Target Volume Label
This function modifies the volume label of the destination drive (when copying only in one direction).

Special/Database

These settings enable the program to share the same database between several profiles. Normally, you don't need to edit any of the fields on this tab sheet. When saving a profile under a new name, you will be

asked if you would like to continue using the same database.

Sharing the same database may be useful or necessary only in special cases, for example if you have more than one profile that work on the same folders but with different file masks or subfolder selections.

In most cases, you will want to avoid two jobs from using the same database. You will find a checkmark on the *Database* tab sheet of the Program Settings dialog to "never allow two profiles to share the same database". If two profiles do share the same database, only one of them can run at the same time.

Open Database Read-Only
This setting is used by the Restore Wizard when using the database as a file list cache for the source side to ensure that the restore operation can't modify the database.

Fast Mode: Don't Check All DB Entries
When using SmartTracking or *Cache Destination File List* or Exact Mirror with Delayed Deletions, the program depends on the database containing a complete, up-to-date list of all files with their details and properties. For this reason, the whole database is checked against the actual file list when a job is run in attended mode. To save time, you can choose this **Fast Mode** checkmark.

Versioning

Versioning/ Versioning
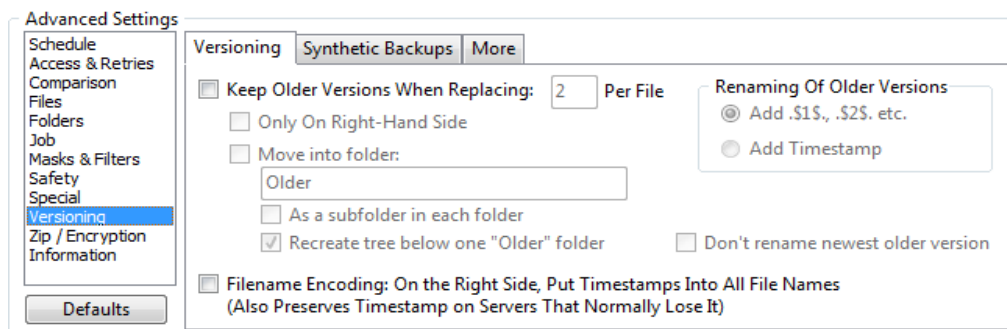
Keep Older Versions When Replacing
When files on one side are replaced by newer versions from the other, Syncovery can keep the older versions by renaming and/or moving them. You can specify how many backup versions to keep.

You can choose between various renaming ways:

Add .1., .2. etc.
For example, a file named letter.doc would be renamed to letter.1.doc. The next older version would be letter.2.doc, and so forth.

Add Timestamp
This way of renaming adds the timestamp to the filename.

Filename Encoding: On Right Side, Put Timestamp Into All File Names
(Also Preserves Timestamp on Servers That Normally Lose It)
Filename Encoding is the recommended way to do a versioning backup as well as preserve the timestamps on sites that don't accept timestamps.

Putting the timestamp into the file names can serve two purposes when backing up data:
- Some cloud servers don't accept the original file timestamps natively. To serve as a fully transparent side for the synchronization, the timestamp has to be retained somehow. Filename Encoding can be the solution because the time stamp will be shown fully correct in future runs of the profile. The encoded filename will be decoded by Syncovery and the original filename will be shown with the correct timestamp.
- To keep multiple versions of the same file on the destination.

Filename Encoding is also the way of renaming used when using Synthetic Backup.
See also Versioning and Filename Encoding on our web site.

Versioning /Synthetic Backups
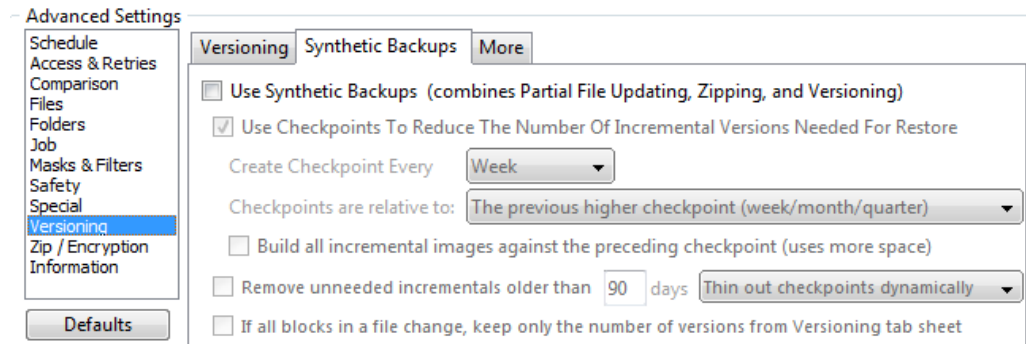
Synthetic Backup is the combination of Partial File Updating with Versioning, Filename Encoding and Zipping. It can be used with any backup storage location, including FTP and other Internet Protocols. The zip files can be encrypted. Synthetic Backup can be described as Differential Versioning.

Checkbox to choose:
- tab sheet Versioning->Synthetic Backups: "Use Synthetic Backups"

The following dependent options are then checked automatically:
- tab sheet Special: "Partial File Updating" (without Remote Service)
- tab sheet Zipping: "Zip Each File Individually"
- tab sheet Versioning: "Filename Encoding"

       All incremental versions must be kept in the same folder.

Be sure to keep all zip files on the destination as they may all be needed to reassemble the file upon restore. However, the number of older incremental parts that need to remain on the backup storage can be limited thru the new "Checkpoint" feature. You will find its settings on the new tab sheet Versioning->Synthetic Backup.

A checkpoint is an incremental backup just like the daily backups. However, it is a little larger because it includes the changed blocks of a longer period of time, so that many preceding incrementals become unnecessary.

Any older version can be restored by choosing the desired target date in the Restore Wizard, or by right-clicking the file in the Sync Preview and choosing the desired version. The option "Keep multiple files" is implied and does not need to be checked. It cannot be used to limit the number of older versions. However, if this option is specified on the Versioning tab sheet, it will be used as a minimum number of versions to keep even if the Checkpoints feature would allow to keep fewer versions.

A restore of the synthetic backup files can be done independently from the original job, to any destination. No database is needed for the restore - just the files.

Block-level copying is applied to files which are at least 400,000 bytes in size. The granularity of the differential backup is determined dynamically for each file, based on its size. The smallest block size used will be 2048 bytes.

Each partial backup includes an MD5 checksum for each file, so that restored files can be verified to be 100% correct. You can see this in the file MD5.TXT that the partial zips contain.

The Zip file sizes can now be limited too so that large files can be split (only in conjunction with Partial File Updating). The transfer can be stopped any time and zip parts already uploaded won't be lost.

Versioning/More
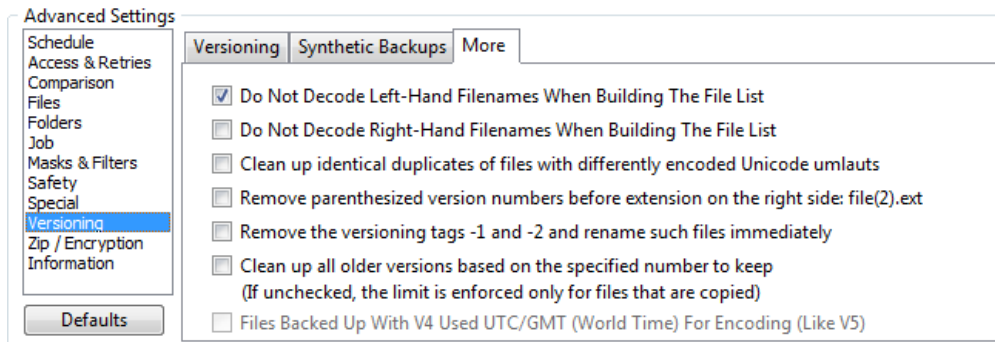
Do Not Decode Left/Right-Hand Filenames When Building The File List
Filenames where the program has encoded additional information into the filename are normally shown in their original, unencoded form. However, if you would like to make a 1:1 copy of a backup location which contains mangled filenames, then you need to use this setting so that files are copied without decoding their filenames.

Clean up identical duplicates of files with differently encoded Unicode umlauts
Unicode allows accented characters and some symbols to be encoded in different ways - for example, as one accented character, or as the base character followed by the accent as a separate character. Due to the different encoding, files whose names look identical can exist in the same folder. This option will attempt to clean them up.

Remove parenthesized version numbers before extension on the right side: file(2).ext
Rarely used. This option will remove the version numbers in parentheses, like the example, from files on the right side, when copying right to left. Note that this checkmark is unrelated to any other versioning settings. The parenthesized version numbers are not something that Syncovery uses itself, it can only remove them.

Remove the versioning tags -1 and -2 and rename such files immediately while building the file list
Rarely used. This option helps cleaning up versioned files. These versioning tags may have been added by the conflict detection in SmartTracking mode.

Clean up all older versions based on the specified number to keep
If you change your versioning settings, you can use this checkmark to clean up the files and delete older versions which are no longer supposed to be kept. If unchecked, the limits are enforced only for files being copied.

Files Backup Up With V4 Used UTC/GMT (World Time) For Encoding (Like V5)
Up to version 4, filename encoding could use either the local time or world time. Because this was ambiguous, the filename encoding was changed to always use world time in version 5. If you still have older files, this checkmark is used to tell the program how to interpret the encoded timestamps.

Zip/Encryption

Zipping
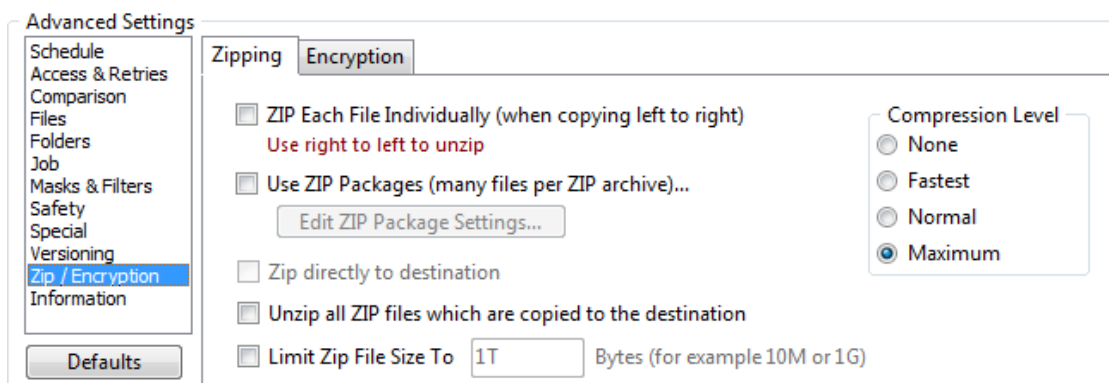
There are two ways of using ZIP files. You can either
- ZIP the source files individually. On the right side, one ZIP file will be created for each file that is copied from the left-hand side to the right-hand side. The advantage of this method is that in future synchronizations, the zipped files are fully transparent and they will be shown in the Synchronization Preview as normal files. Since future synchronizations will see the zipped files as normal files, they will know exactly if they are still identical to the left-hand side. When copying these zipped files back (from right to left), they are unzipped automatically.
- Put many files in each ZIP file. The program calls these files ZIP Packages. In future runs, the files inside the ZIP Packages are not seen by the software. Therefore, you need to resort to the "Archive" flag in order to determine which files are new or changed and need to be backed up. ZIP Packages cannot be encrypted by Syncovery. ZIP Packages can also be used in order to speed up file transfer over a small or medium bandwidth network connection. If used that way, the Syncovery Remote Service must be installed on the destination machine and be configured properly.

ZIP Each File Individually (when copying left to right)
This method ZIPs each file individually as described above. The ZIP file will have the same name, plus a few digits encoding the uncompressed size of the file, plus the .zip extension. The uncompressed size needs to be encoded in the file name in order to make the ZIP file transparent for future synchronizations.

Use ZIP Packages (many files per ZIP archive)
This settings enables the use of ZIP Packages as described above. A separate dialog with some related options will appear when this option is chosen.

ZIP directly to destination
Normally, ZIP files are generated in a temporary folder and then copied to the destination. This setting changes that and generates the ZIP files directly in the destination folder. This setting cannot be used for FTP transfers.

Unzip all ZIP files which are copied to the destination
Normally, the program unzips only ZIP files that it has generated itself during a previous run. To unzip any ZIP file, when copying from right to left, use this setting.

Limit Zip File Size
This option allows you to specify a maximum file size for the zip files. When the size is reached, the program will begin a new split zip file. This works with both the individual zipping mode and the ZIP Package mode.

Encryption
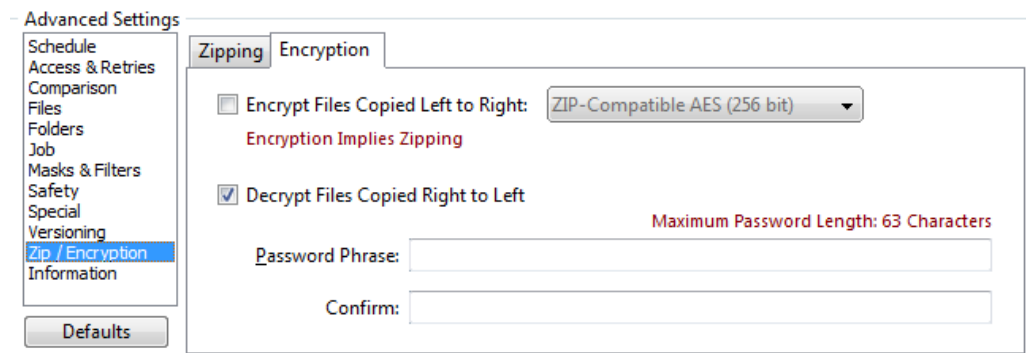
Encryption can be performed when files are copied from the left-hand side to the right-hand side. Copying in the opposite direction or using the Restore Wizard will decrypt the files.

Encryption is always done along with zipping. The recommended method is ZIP-Compatible AES encryption (256 bit). This encryption can be decrypted with some popular zipping tools, such as WinZip, WinRAR, and PowerArchiver.

The password phrase should be longer than normal passwords since it is used to generate an encryption key. However, the maximum length that can be saved in a profile is currently 63 characters.

Information
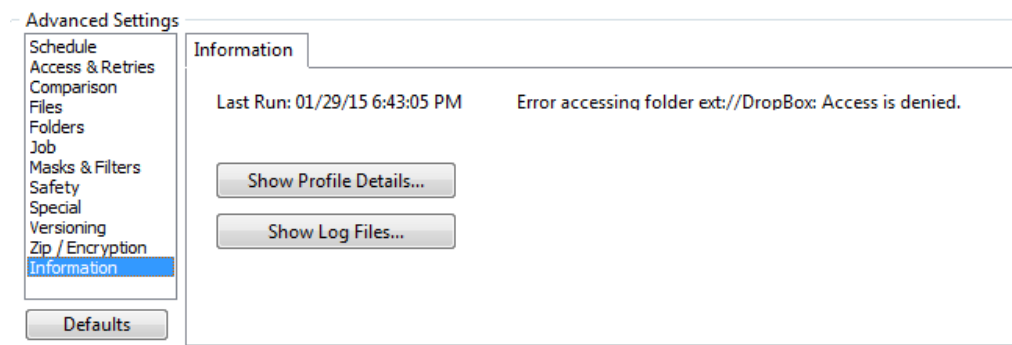
Sync Operation Mode

SmartTracking

SmartTracking is used when synchronizing two locations, and new or updated files can be expected on both sides. SmartTracking can detect on which side a file has been changed, moved, or deleted.

SmartTracking uses a local database in order to track changes that have been made between the various invocations of the profile. That way, the software will know whether a file has been moved on the left side, or on the right side. It can also detect whether a file has been deleted on one side, or whether the file has

actually been added on the other. SmartTracking should always be used whenever you want to keep two locations in sync, both of which are being used for work. SmartTracking is not needed when you do a backup or mirror, or any other case where you synchronize in one direction only. SmartTracking has various additional features which you will see in the SmartTracking dialog box.

SmartTracking keeps information in a database linked to the profile name. On the first run, SmartTracking will record the state of each file. Starting with the second run, the SmartTracking settings will become active. Do not rename the profile, because then it will not be able to find its original database. Do not use more than one profile for synchronization of the same folders.

The SmartTracking dialog has four tab sheets:

Detection of Moved Files
"Moved files" refers to files that have been moved into a different folder on one side, but not on the other. By looking at these files only, it is not possible to determine on which side the file has been moved - in other words, it is hard to tell which of the folders the desired new location for the file is. SmartTracking solves this problem by comparing the current locations against the previous locations stored in its database. That way, the software can find out on which side the move has been performed, and it can then perform the same move on the other side as part of the synchronization process.

Files Deleted On One Side
In many cases, when the synchronization is started, there will be files that exist only on one side of the synchronization. These files are usually new files that should be copied over to the other side. But sometimes, this situation occurs because a file has been deleted on one side. The user will normally not want to have this file copied back from the other side. The desired action is often to have it deleted on the other side too.

SmartTracking can detect these cases, but ultimately you are responsible for what the program does, so please verify the actions in the Synchronization Preview before starting it. To ensure that no important files can get lost accidentally, the software will not actually delete these files. It will move them into a special folder which you need to specify as the last setting in this dialog box. That way, you can always retrieve files that have been deleted but for some reason shouldn't have.

Files Changed On Both Sides
Traditionally, when synchronizing bidirectionally, this synchronization software would always copy the file with the latest timestamp to the other side, overwriting the older file that is already there. This is usually fine, but in some cases it may be a problem: what if the file has been edited by two different persons on both sides of the synchronization? One of the files may have a later timestamp, but it is not clear that this is the (only) version that should continue to exist on both sides.

So, you can choose to have such files be **labeled as CONFLICT**. Then, you will need to look closely at the Synchronization Preview window and resolve these conflicts manually by specifying a copying direction for each file. Or you can specify that both versions of the file, from the left and right sides, should be kept. To keep both versions, one of them is renamed and then both are copied.

Consider different files with the same name, not present in database, a conflict
This covers a very specific case, where a file exists on both sides, but it is not identical, and it's not in the database either. Normally the program would simply copy the newer version of this file and overwrite the older version on the other side with it. To prevent that, you can use this checkbox. It will make the program consider these files a conflict and treat the conflict according to the settings in the upper part of this tab sheet.

OPTIONS

Detect Unchanged Files
Some storage locations, such as FTP or WebDAV servers, always give uploaded files the current system time as Last Modified timestamp. This is generally a problem for synchronization, because you can never get the timestamps to match on both sides. If you are synchronizing in both directions, to and from the problematic server, then you may want to have SmartTracking detect whether files with new timestamps are really changed or not. It does so by querying the timestamp of freshly uploaded files immediately after the upload. This timestamp is stored in the SmartTracking database. On the next run, if the timestamp is still the same,

the program will know that the file has not changed.

Real-Time Synchronization
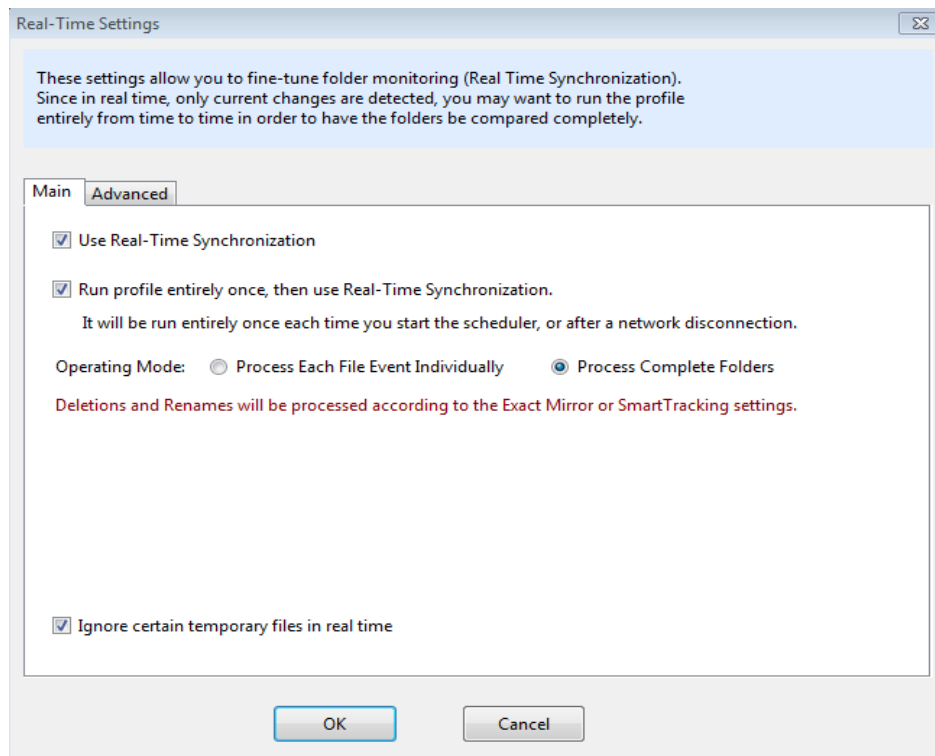
Real Time Synchronization will monitor folders for changes and copy new or modified files with a very short delay after the change has occurred. Because the folders are monitored, they don't have to be scanned - the "Building File List" step does not occur. Real Time Synchronization can be very convenient and speeds up the synchronization process considerably. However, it will only copy new and modified files and it may not be appropriate in all situations.

Real Time Synchronization is chosen in each profile, on the right-most tab sheet among the Schedule settings. The scheduler must be started in a separate step to start the monitoring.

Because Real-Time Scheduling does not compare the source and destination folders completely, it is recommended to also schedule a complete profile run, for example once a day. This can be done on the "Schedule" tab sheet.

Partial File Updating

Syncovery can detect which parts of a larger file have changed, and copy only the changed blocks rather than the complete file. This feature works similar to Rsync (but it's not the same).

Copying only the changed blocks can save bandwidth and time, especially over a slow connection. When copying between local disks or in a LAN environment, it can save bandwidth too, but may not always save much copying time, because the source file has to be read in its entirety every time in order to determine the changed blocks.

Only block-oriented file types are eligible for block-level copying. These include database files such as SQL or Outlook PST, as well as drive images and virtual hard disk images (VMs). Stream-based files, on the other hand, will usually cause all blocks to be changed whenever they are modified (for example text documents, spreadsheets, zip files, and photos). Thus block-level copying won't be able to save much bandwidth with stream-based files.

In Syncovery, block-level copying is called "Partial File Updating". In many cases, you need to choose only this one checkmark, which is on the Special settings category in the profiles (in Advanced Mode).

The program needs to have fast access to at least one of the sides of the synchronization. The other side may be a low-bandwidth connection. If you are using an Internet Protocol, please note that only SSH/SFTP supports block-level updating directly. The other protocols can only be used with Synthetic Backup (see further down below).

Please note: Block level copying with SSH/SFTP has only been implemented for uploads, not downloads.

Partial File Updating can work in three different ways:

Mode 1: With Database:
- Source access must be fast
- Destination may be slow
- MD5 checksums are stored in database
- Destination files must not be modified by any other profile, person, or tool
- Destination must be accessed via LAN, VPN, or SSH/SFTP

Mode 2: With Remote Service:
- Syncovery Remote Service computes MD5 checksums on remote computer
- The "slow" side can be both source or destination
- MD5 checksums are newly calculated each time
- Files on both sides can be modified by other profiles, persons, or tools
- One side must be local or LAN/VPN, the other can be LAN, VPN, or SSH/SFTP

Mode 3: Synthetic Backup:
- similar to Mode 1, plus:
- adds Zip compression, versioning, and filename encoding
- can work locally or with any Internet Protocol for the destination side
- the changed blocks are uploaded in a new, separate zip file every time
- all older zip files must stay on the backup storage, but can be thinned out
- all connection types and Internet Protocols are supported

Mode 1: Slow Destination
In this mode, the speed-up is available when you copy files from a location to which you have fast access (preferably your own hard disk). The destination can be a slow connection, but it must be a normal file system (either LAN or VPN) or SSH/SFTP. For other connections, you can use Synthetic Backup.

Instructions for Mode 1
In your profile, make the following checkmark: Use Partial File Updating, which is on the Special tab sheet when editing the profile in Advanced Mode. The next time you run the profile, a database is created on your hard drive where information needed for the speed-up is stored. The second time you run the profile, you should notice the speed-up.

Mode 2: With Remote Service
This mode can speed up updating large files in both directions. The remote computer can be both source and/or destination. This is achieved by running a small service application on the remote computer, which will create the necessary checksums on the fly, when requested by the main application running on a different machine. See more information on the Syncovery Remote Service here.

The other (local) computer, where the main Syncovery program is running, needs to have normal file system access to the remote computer (LAN or VPN), or it can use SSH. It needs to have write access to the remote computer so that it can save the checksum request file there. The MD5 checksums are created when needed, so that no database is being used.

Instructions for Mode 2

On the remote system, run the Setup program and install the Syncovery Remote Service along with its control panel. Start the control panel from the Syncovery group in the Start menu. On the tab sheet Configure Checksummer, enter the base folders that will be used for synchronization. Click Apply. On the tab sheet Service Configuration, click on Install Service and Start. The service will be using the Windows System account by default. If this account doesn't have sufficient access privileges, you may have to change the account in Windows Control Panel -> Administrative Tools -> Services.

On the local system, you are running the main Syncovery program. In your profile, the right-hand side must be the remote system. Specify one of the folders which you have specified for the remote service to monitor. The left side should be your local folders, or a network drive with relatively fast access. On the Specials tab sheet in Advanced Mode, make the following checkmarks: Use Partial File Updating and Right side uses Remote Service.

Mode 3: Synthetic Backup
This feature is intended for backing up from a local storage to any type of backup storage. The backup can be local or online.

Choose "Synthetic Backup" on the tab sheet Versioning->Synthetic Backup. This will automatically place these additional checkmarks:
- Use Partial File Updating (under Special)
- Filename Encoding (under Versioning)
- Zip Each File Individually (under Zip/Encryption)

See also Profile Settings - Synthetic Backups.

Please see the most current information on our web site.

Synchronization Preview Dialog
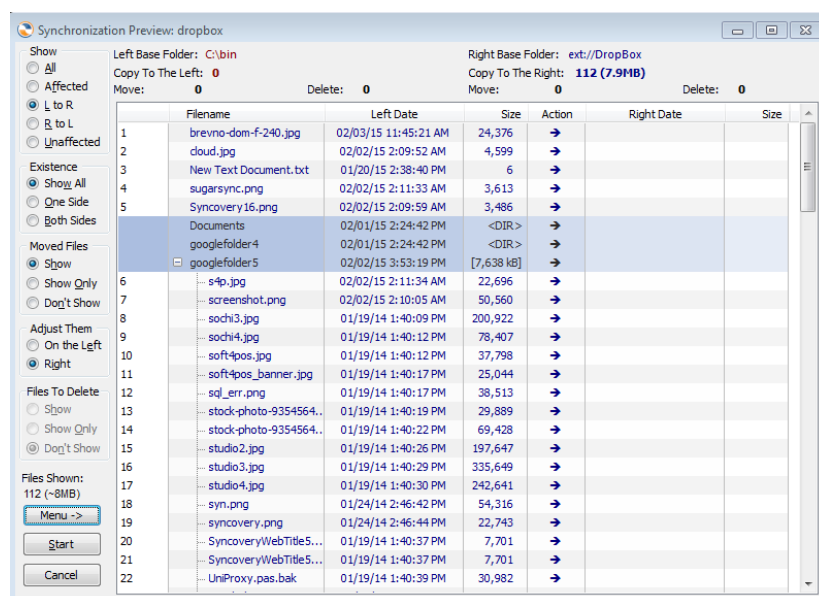
This window shows all files found on both sides. You can see on which side(s) a particular file currently exists by looking into the **Date** and **Size** columns. On the left, you have various options to control which kinds of files will be shown. When you hit the **Start** button, only the files shown will be affected, and only if they have an **Action** specified in the Action column (see below the screenshot). To change actions for specific files, select the files and use the Menu button or right-click the file list invoked by the right mouse button.

Possible Actions

□ : copy to the right side
□ : copy to the left side

MOVE
File will be moved into a different folder on one side. Use the radio buttons on the lower left to control on which side moved files will be adjusted.

DELETE
File will be deleted. This can only occur in Exact Mirror Mode, or if deletion has been manually selected for a file.

CONFLICT
The items and the left or right side are different, but the software cannot detect the correct action. This can be because on one side, it is a file, and a folder on the other side, or it can be caused by a failed binary comparison of a file. SmartTracking also causes this label when a files has been changed on both sides.

time-> / <-time
The timestamp of the folder should be adjusted.

case-> / <-case
The spelling of the file should be adjusted to match the case of the source side.

Menu in File List View
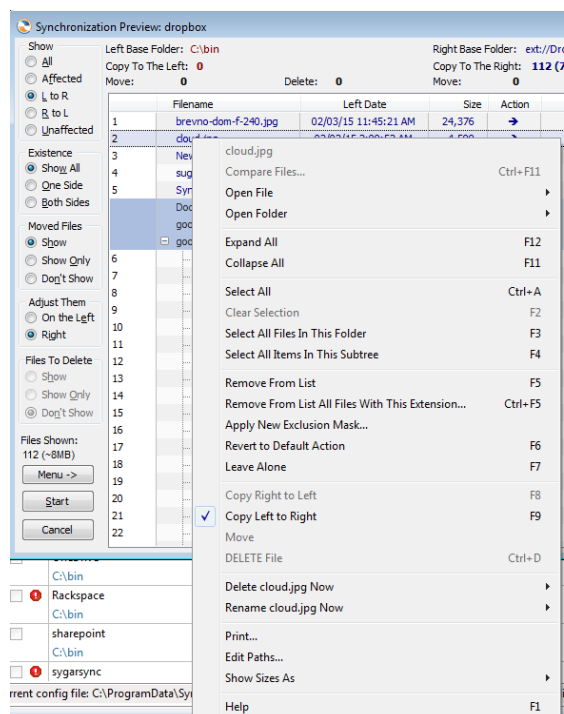
This is the context menu that you can use with selected files in the file list view. To bring it up, select some items and click the right mouse button within the selected rows. Or, click on the **Menu** button.

Using this context menu, you can manually select the action that should be performed with the selected files and/or folders. In addition, you can remove the items from the list, as well as delete files immediately. The menu also informs you about the keyboard shortcuts that can be used in the File List View.

Note that these menu items can be very useful:
Select All Files In This Folder (F3):
This command extends the selection so that it includes all files in the folder that belongs to the top of the selection. Combining F3 with some of the other commands, you can quickly change the action for or deselect or remove complete folders in the list.

Select All Items In This Subtree (F4):
This command extends the selection so that it includes all files and folders in the folder that belongs to the top of the selection, as well as all sub-folders. Combining F4 with some of the other commands, you can quickly change the action for or deselect or remove complete subtrees in the list.

Program Settings Dialog
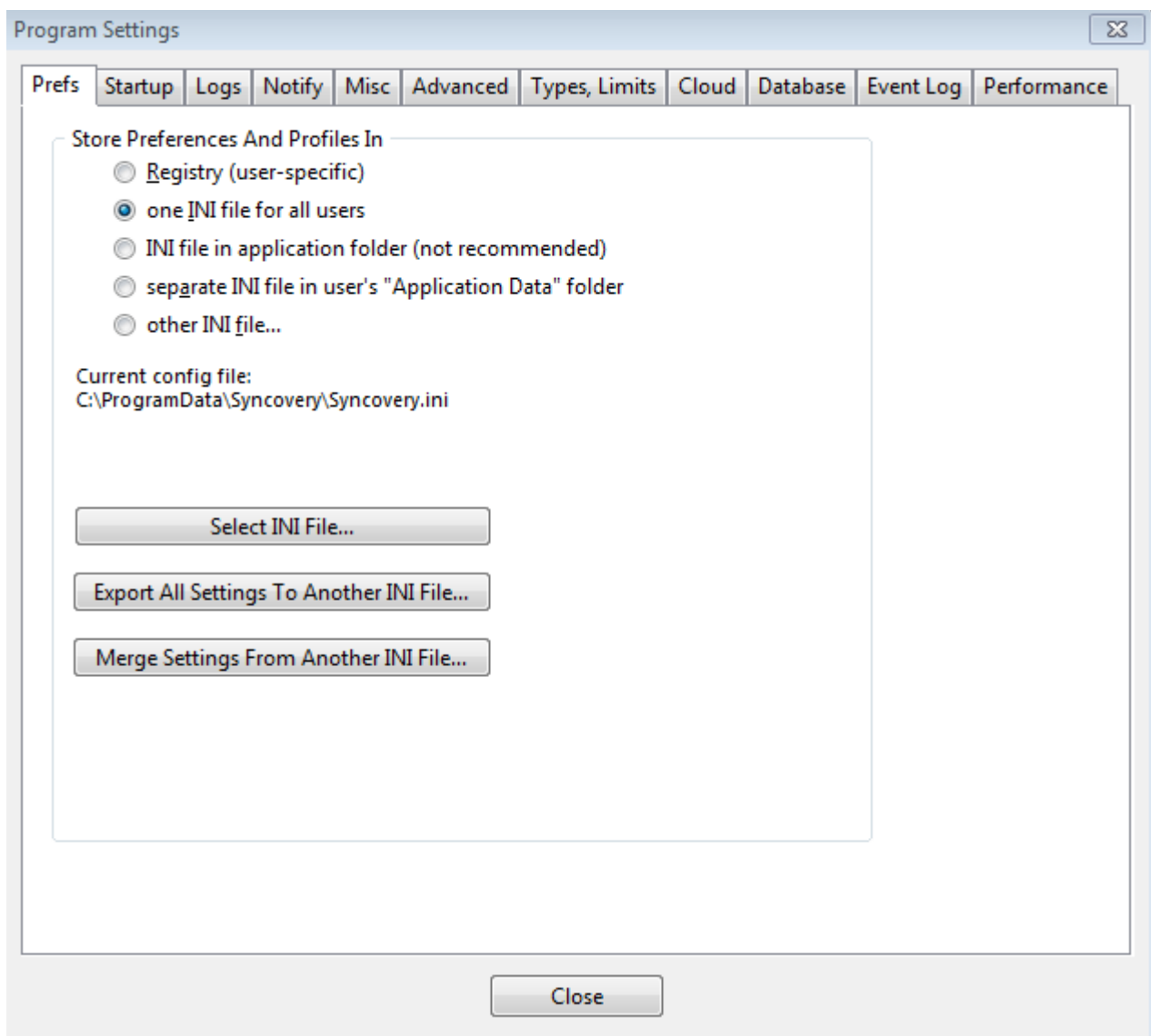
These are some settings that affect how Syncovery behaves in general. None of these options are profile-specific.

For other advanced information, please see Advanced Information.

Store Preferences
You can select the location where to store the profiles and settings. To do this, select the appropriate option here.
The new INI file location (the exact file path) will be displayed here when you restart the program. Note that the INI file location can be overriden using the /INI=xxx command line option, see Advanced Information.

Startup Options

These options specify how the background scheduler should behave when Windows is started.

Log files
On the Options tab sheet, you can also activate logging:
Each log file will contain detailed information about all operations that the program carries out while running a profile, including the start and end time and date.

Notification Preferences

If desired, the program can send an email whenever a profile has been run. Be sure to go into the Email Settings dialog and specify the recipient(s) and the SMTP server details.

Miscellaneous
You can specify a folder where the databases are stored (when using SmartTracking, Cache Destination File List, or Partial File Updating).

You can also specify an external diff tool which is used to show a text comparison of two files with the same name on each side. In the Sync Preview, you can use the right-click (context) menu to invoke the diff tool.

Advanced Options
Use Windows API File Copying Function (slower)
If you experience any problems with the file copying, try this option. In particular, it may solve performance problems with MacOS 10.3 (Panther) network drives, as well as solve compatibility problems with buggy drivers for removeable media. Sometimes it may also improve working with Netware servers. For normal copying, this option should not be used, since it slows copying down a bit.
Buffer size for copying files
The main reason that the integrated copying algorithm is faster than many others is the large buffer that is normally used. You can adjust the size to optimize working with some types of media.

SmartTracking

SmartTracking is used when synchronizing two locations, and new or updated files can be expected on both sides. SmartTracking can detect on which side a file has been changed, moved, or deleted.

SmartTracking uses a local database in order to track changes that have been made between the various invocations of the profile. That way, the software will know whether a file has been moved on the left side, or on the right side. It can also detect whether a file has been deleted on one side, or whether the file has actually been added on the other. SmartTracking should always be used whenever you want to keep two

locations in sync, both of which are being used for work. SmartTracking is not needed when you do a backup or mirror, or any other case where you synchronize in one direction only. SmartTracking has various additional features which you will see in the SmartTracking dialog box.

SmartTracking keeps information in a database linked to the profile name. On the first run, SmartTracking will record the state of each file. Starting with the second run, the SmartTracking settings will become active. Do not rename the profile, because then it will not be able to find its original database. Do not use more than one profile for synchronization of the same folders.

The SmartTracking dialog has four tab sheets:

Detection of Moved Files
"Moved files" refers to files that have been moved into a different folder on one side, but not on the other. By looking at these files only, it is not possible to determine on which side the file has been moved - in other words, it is hard to tell which of the folders the desired new location for the file is. SmartTracking solves this problem by comparing the current locations against the previous locations stored in its database. That way, the software can find out on which side the move has been performed, and it can then perform the same move on the other side as part of the synchronization process.

Files Deleted On One Side
In many cases, when the synchronization is started, there will be files that exist only on one side of the synchronization. These files are usually new files that should be copied over to the other side. But sometimes, this situation occurs because a file has been deleted on one side. The user will normally not want to have this file copied back from the other side. The desired action is often to have it deleted on the other side too.

SmartTracking can detect these cases, but ultimately you are responsible for what the program does, so please verify the actions in the Synchronization Preview before starting it. To ensure that no important files can get lost accidentally, the software will not actually delete these files. It will move them into a special folder which you need to specify as the last setting in this dialog box. That way, you can always retrieve files that have been deleted but for some reason shouldn't have.

Files Changed On Both Sides
Traditionally, when synchronizing bidirectionally, this synchronization software would always copy the file with the latest timestamp to the other side, overwriting the older file that is already there. This is usually fine, but in some cases it may be a problem: what if the file has been edited by two different persons on both sides of the synchronization? One of the files may have a later timestamp, but it is not clear that this is the (only) version that should continue to exist on both sides.

So, you can choose to have such files be **labeled as CONFLICT**. Then, you will need to look closely at the Synchronization Preview window and resolve these conflicts manually by specifying a copying direction for each file. Or you can specify that both versions of the file, from the left and right sides, should be kept. To keep both versions, one of them is renamed and then both are copied.

Consider different files with the same name, not present in database, a conflict
This covers a very specific case, where a file exists on both sides, but it is not identical, and it's not in the database either. Normally the program would simply copy the newer version of this file and overwrite the older version on the other side with it. To prevent that, you can use this checkbox. It will make the program consider these files a conflict and treat the conflict according to the settings in the upper part of this tab sheet.

OPTIONS

Detect Unchanged Files
Some storage locations, such as FTP or WebDAV servers, always give uploaded files the current system time as Last Modified timestamp. This is generally a problem for synchronization, because you can never get the timestamps to match on both sides. If you are synchronizing in both directions, to and from the problematic server, then you may want to have SmartTracking detect whether files with new timestamps are really changed or not. It does so by querying the timestamp of freshly uploaded files immediately after the upload. This timestamp is stored in the SmartTracking database. On the next run, if the timestamp is still the same, the program will know that the file has not changed.

Partial File Updating

Syncovery can detect which parts of a larger file have changed, and copy only the changed blocks rather than the complete file. This feature works similar to Rsync (but it's not the same).

Copying only the changed blocks can save bandwidth and time, especially over a slow connection. When copying between local disks or in a LAN environment, it can save bandwidth too, but may not always save much copying time, because the source file has to be read in its entirety every time in order to determine the changed blocks.

Only block-oriented file types are eligible for block-level copying. These include database files such as SQL or Outlook PST, as well as drive images and virtual hard disk images (VMs). Stream-based files, on the other hand, will usually cause all blocks to be changed whenever they are modified (for example text documents, spreadsheets, zip files, and photos). Thus block-level copying won't be able to save much bandwidth with stream-based files.

In Syncovery, block-level copying is called "Partial File Updating". In many cases, you need to choose only this one checkmark, which is on the Special settings category in the profiles (in Advanced Mode).

The program needs to have fast access to at least one of the sides of the synchronization. The other side may be a low-bandwidth connection. If you are using an Internet Protocol, please note that only SSH/SFTP supports block-level updating directly. The other protocols can only be used with Synthetic Backup (see further down below).

Please note: Block level copying with SSH/SFTP has only been implemented for uploads, not downloads.

Partial File Updating can work in three different ways:

Mode 1: With Database:
- Source access must be fast
- Destination may be slow
- MD5 checksums are stored in database
- Destination files must not be modified by any other profile, person, or tool
- Destination must be accessed via LAN, VPN, or SSH/SFTP

Mode 2: With Remote Service:
- Syncovery Remote Service computes MD5 checksums on remote computer
- The "slow" side can be both source or destination
- MD5 checksums are newly calculated each time
- Files on both sides can be modified by other profiles, persons, or tools
- One side must be local or LAN/VPN, the other can be LAN, VPN, or SSH/SFTP

Mode 3: Synthetic Backup:
- similar to Mode 1, plus:
- adds Zip compression, versioning, and filename encoding
- can work locally or with any Internet Protocol for the destination side
- the changed blocks are uploaded in a new, separate zip file every time
- all older zip files must stay on the backup storage, but can be thinned out
- all connection types and Internet Protocols are supported

Mode 1: Slow Destination

In this mode, the speed-up is available when you copy files from a location to which you have fast access (preferably your own hard disk). The destination can be a slow connection, but it must be a normal file system (either LAN or VPN) or SSH/SFTP. For other connections, you can use Synthetic Backup.

Instructions for Mode 1
In your profile, make the following checkmark: Use Partial File Updating, which is on the Special tab sheet when editing the profile in Advanced Mode. The next time you run the profile, a database is created on your hard drive where information needed for the speed-up is stored. The second time you run the profile, you should notice the speed-up.

Mode 2: With Remote Service
This mode can speed up updating large files in both directions. The remote computer can be both source and/or destination. This is achieved by running a small service application on the remote computer, which will create the necessary checksums on the fly, when requested by the main application running on a different machine. See more information on the Syncovery Remote Service here.

The other (local) computer, where the main Syncovery program is running, needs to have normal file system access to the remote computer (LAN or VPN), or it can use SSH. It needs to have write access to the remote computer so that it can save the checksum request file there. The MD5 checksums are created when needed, so that no database is being used.

Instructions for Mode 2
On the remote system, run the Setup program and install the Syncovery Remote Service along with its control panel. Start the control panel from the Syncovery group in the Start menu. On the tab sheet Configure Checksummer, enter the base folders that will be used for synchronization. Click Apply. On the tab sheet Service Configuration, click on Install Service and Start. The service will be using the Windows System account by default. If this account doesn't have sufficient access privileges, you may have to change the account in Windows Control Panel -> Administrative Tools -> Services.

On the local system, you are running the main Syncovery program. In your profile, the right-hand side must be the remote system. Specify one of the folders which you have specified for the remote service to monitor. The left side should be your local folders, or a network drive with relatively fast access. On the Specials tab sheet in Advanced Mode, make the following checkmarks: Use Partial File Updating and Right side uses Remote Service.

Mode 3: Synthetic Backup
This feature is intended for backing up from a local storage to any type of backup storage. The backup can be local or online.

Choose "Synthetic Backup" on the tab sheet Versioning->Synthetic Backup. This will automatically place these additional checkmarks:
- Use Partial File Updating (under Special)
- Filename Encoding (under Versioning)
- Zip Each File Individually (under Zip/Encryption)

Connecting to Cloud storages overview

Syncovery just provides the software – the choice for a specific storage provider is made by the customer. You can pick almost any storage you want, because most types of online storage can be accessed via these standard Internet protocols

Google Drive (formely Google Docs)	http://www.google.com/drive

OneDrive	http://onedrive.live.com
OneDrive for bussiness Sharepoint	
Box.net	http://www.box.net
DropBox	http://www.dropbox.com
Rackspace	http://www.rackspace.com
SygarSync	http://www.sugarsync.com
Flickr	http://www.flickr.com
Files Anywhere	http://www.filesanywhere.com
Amazon Cloud Drive	http://www.amazon.com/clouddrive
IDrive	http://www.idrive.com
CopyCom	http://www.copy.com
Bitcasa	http://www.bitcasa.com
Asus	http://www.asuswebstorage.com
Email protocol	http://www.syncovery.com
MTP (as hardware protocol)	http://www.syncovery.com

Most of cloud storages nowdays requre OAuth athentication with internet browser involved. That guarantees high level of security access to your personal cloud. When setting up connection to OAuth based cloud service for the first time it is adviced to make sure you are logged off(signed out) your account of the cloud service in browser, becasue browser keeps your cookeis and in some cases establishing connection might be rather messy.

To set up a backup job over the Internet, have your access details for the online storage ready and follow these steps:
- choose your local data folder on the left-hand side
- click the Internet button on the right-hand side
- choose the Protocol to use and specify the folder, user name and password
- click OK to make some more settings in the profile
- under "Zip/Encryption", choose: "ZIP Each File Individually"
- under "Encryption", choose: "Encrypt Files Copied Left to Right"
- specify a password phrase for the encryption
- under "Versioning", choose if you want to keep older versions of updated files
- for some servers, it is also necessary to choose "Filename Encoding" in order to preserve the files' modification dates.

You can now save your backup job, start it manually, or give it a schedule and/or choose real-time synchronization.

below given scenario for particular storages

Authenticating with Google Drive

- Set up target folder (Left or Right side) for Google Drive in profile settings dialog,
- Start synchronization session.
You will be presented OAuth login/password window in your standalone browser.

- Input your personal login and password into web form and press 'Sign In'
- On the next web page presented press 'Accept'
- On the next web page there will be message confurming that connection is successfull.
- Close your browser.

Synchronization dialog of syncovery with list of files in your cloud will be presented

By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Authenticating with OneDrive

- Set up target folder (Left or Right side) for OneDrive in profile settings dialog,
- Start synchronization session.

You will be presented OAuth login/password window in your standalone browser.

Microsoft account

Sign in

Microsoft account What's this?

Password

☐ Keep me signed in

Sign in

Can't access your account?

Don't have a Microsoft account? Sign up now

Privacy & Cookies | Terms of Use | PC site
© 2015 Microsoft

- Input your personal login and password into web form and press 'Sign In'
- On the next web page presented press 'Accept'
- On the next web page there will be message confurming that connection is successfull.
- Close your browser.
  Synchronization dialog of syncovery with list of files in your cloud will be presented

www.syncovery.com/oauthresult.php

Would you like Password Manager to save the password for this page?   Save   Never   ×

You have successfully authorized Syncovery. You can close this window now.
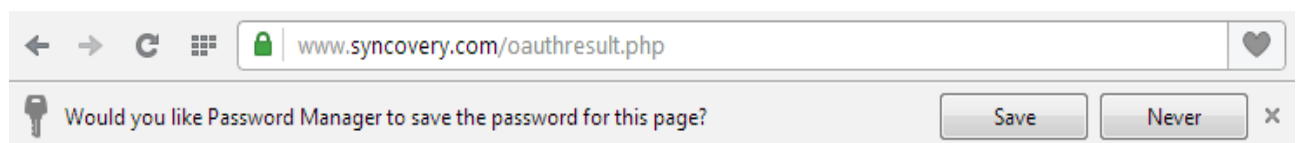
Authenticating OneDrive for bussiness

OneDrive for bussiness does not require OAuth procedure, you should input your login and password into Internet Protocol Settings dialog, AccountID/Access Key fields
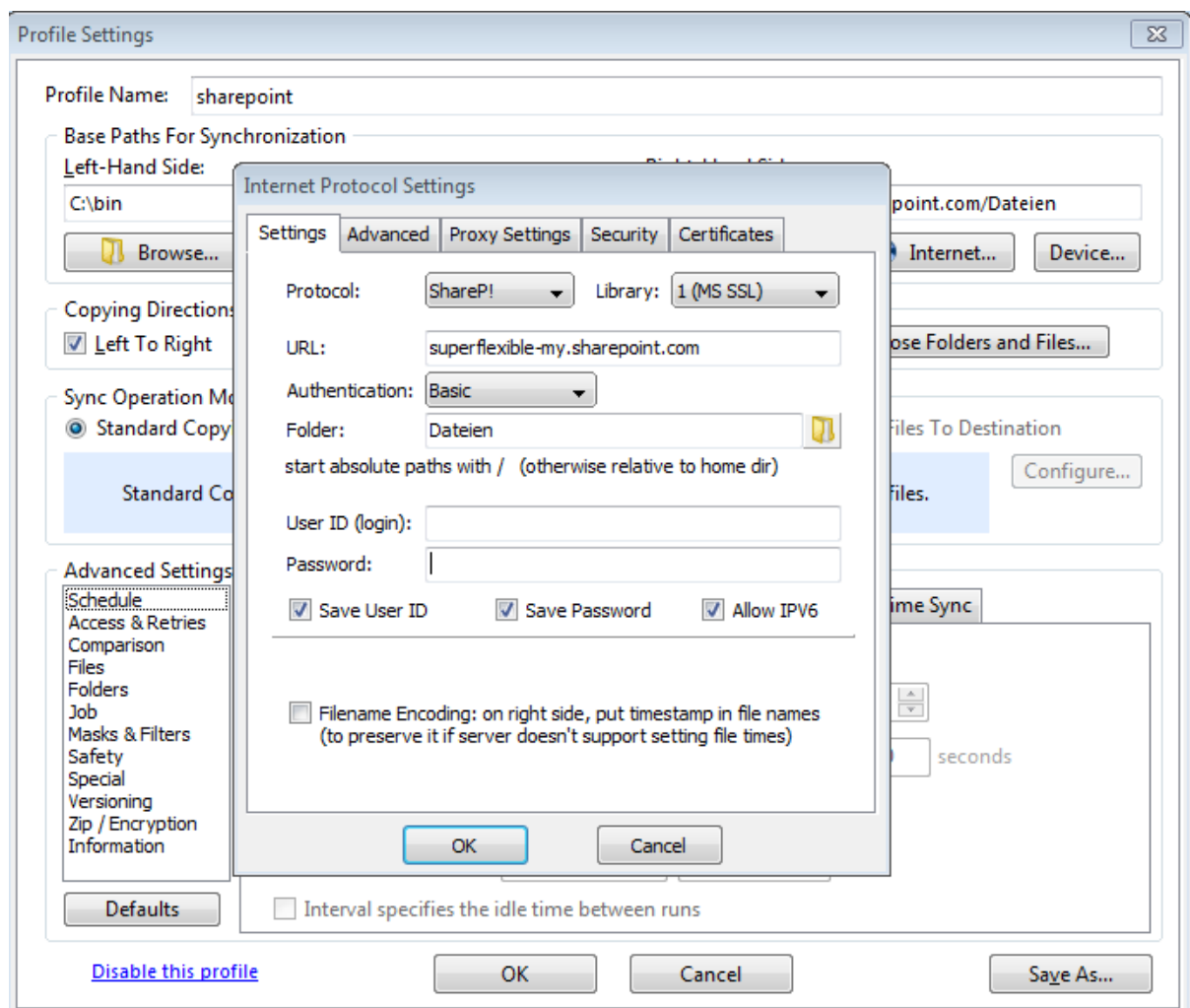
Authenticating Box.Net

- Set up target folder (Left or Right side) for Box.Net in profile settings dialog,

- Start synchronization session.
  You will be presented OAuth login/password window in your standalone browser.
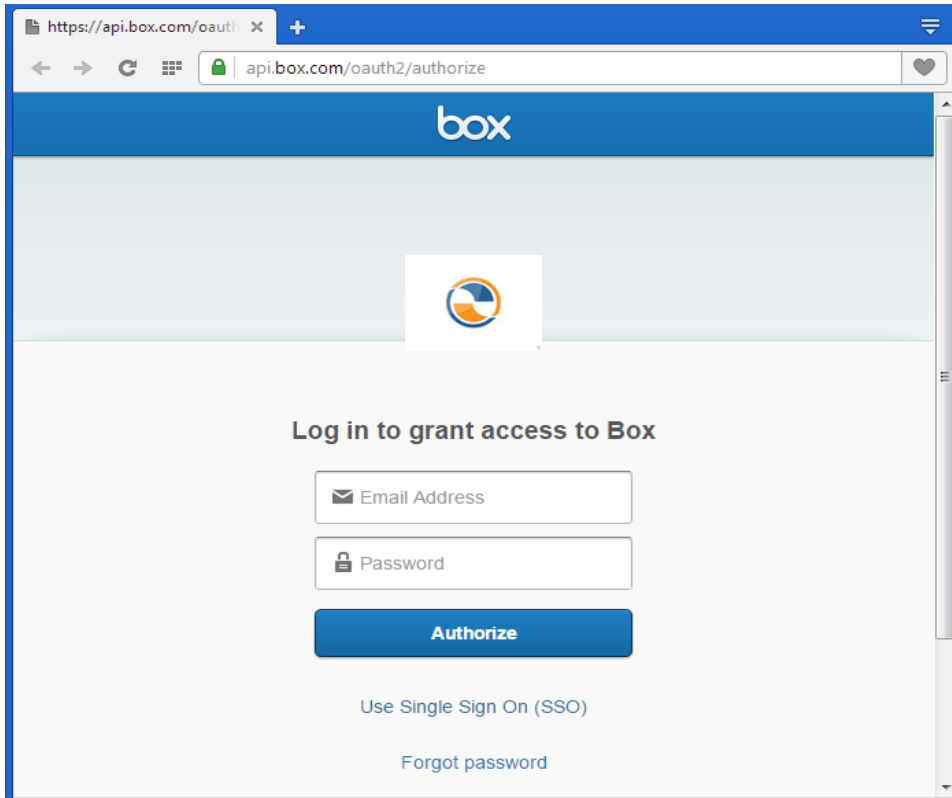
- Input your personal login and password into web form and press 'Authorize'
- On the next web page presented press 'Grant access to Box'
- On the next web page there will be message confurming that connection is successfull.
- Close your browser.
  Synchronization dialog of syncovery with list of files in your cloud will be presented
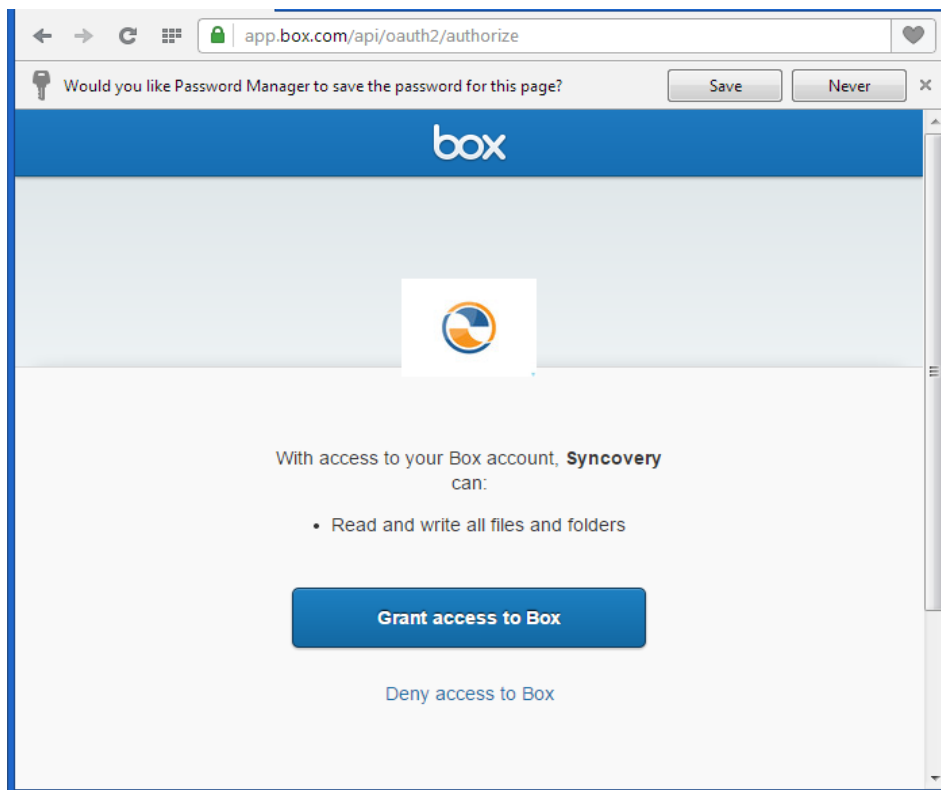
Authenticating with DropBox

- Set up target folder (Left or Right side) for DropBox in profile settings dialog,
- Start synchronization session.
  You will be presented OAuth login/password window in your standalone browser.
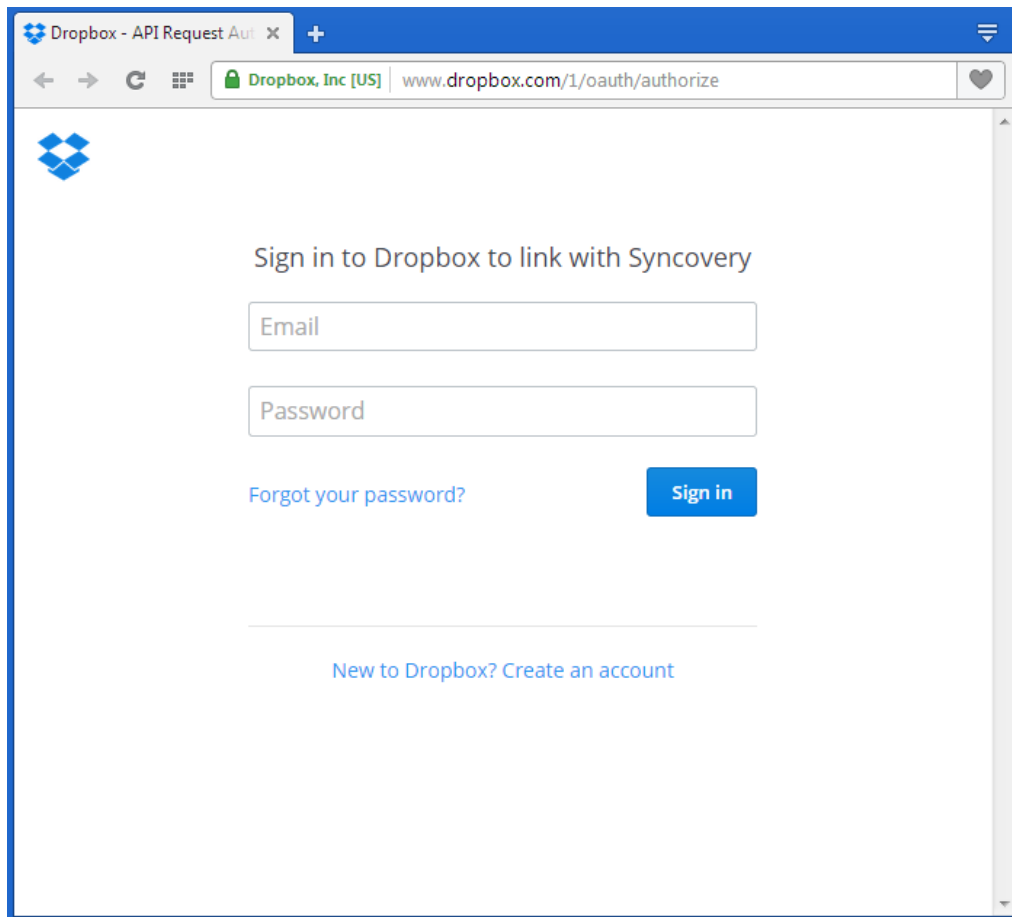
- On the next web page presented press 'Accept'
- On the next web page there will be message confurming that connection is successfull.
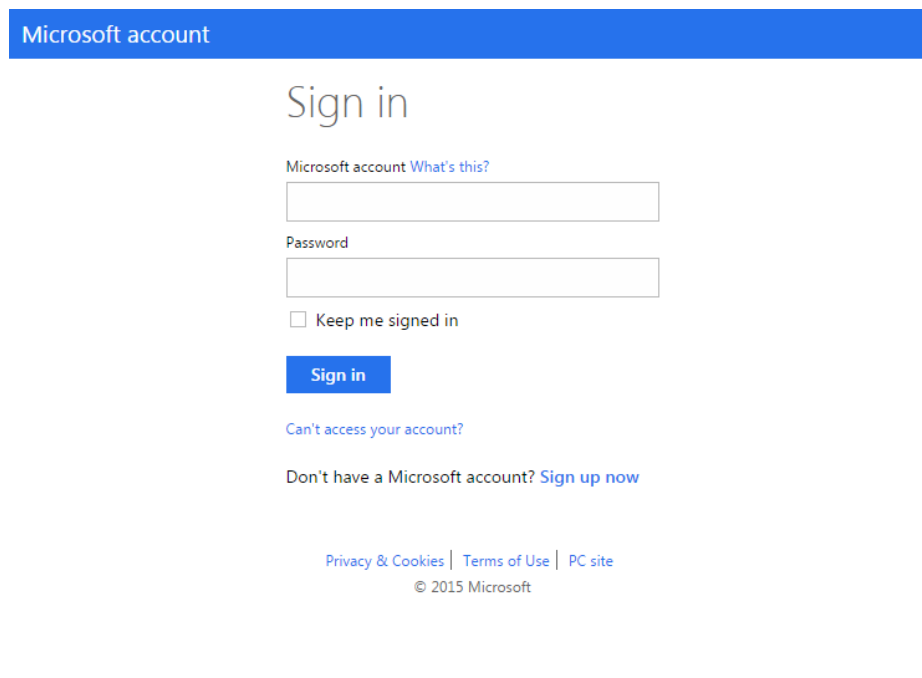- Close your browser.
  Synchronization dialog of syncovery with list of files in your cloud will be presented

Authenticating with Rackspace

Rackspace does not require OAuth procedure, you should input your login and password of Rackspace into Internet Protocol Settings dialog, AccountID/Access Key fields
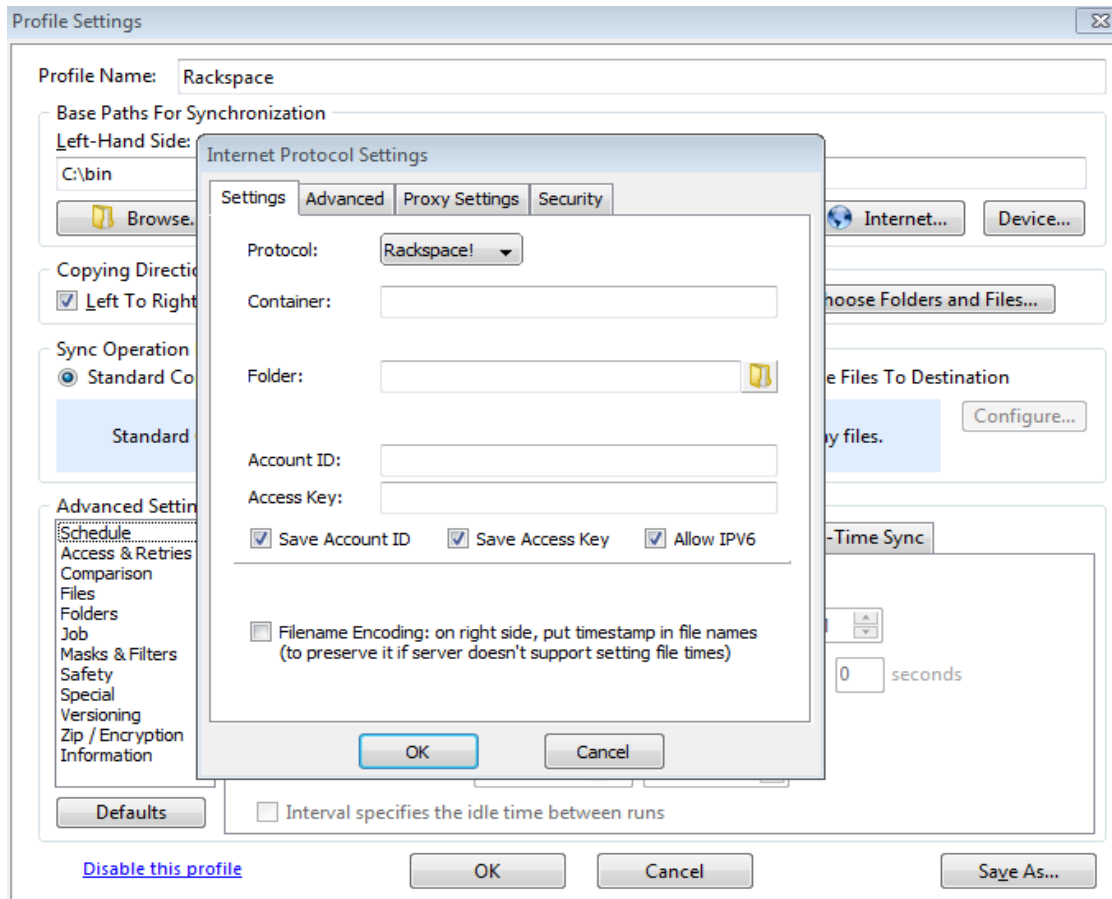
Authenticating with SygarSync

SygarSync does not require OAuth procedure, you should input your login and password into Internet Protocol Settings dialog, AccountID/Access Key fields
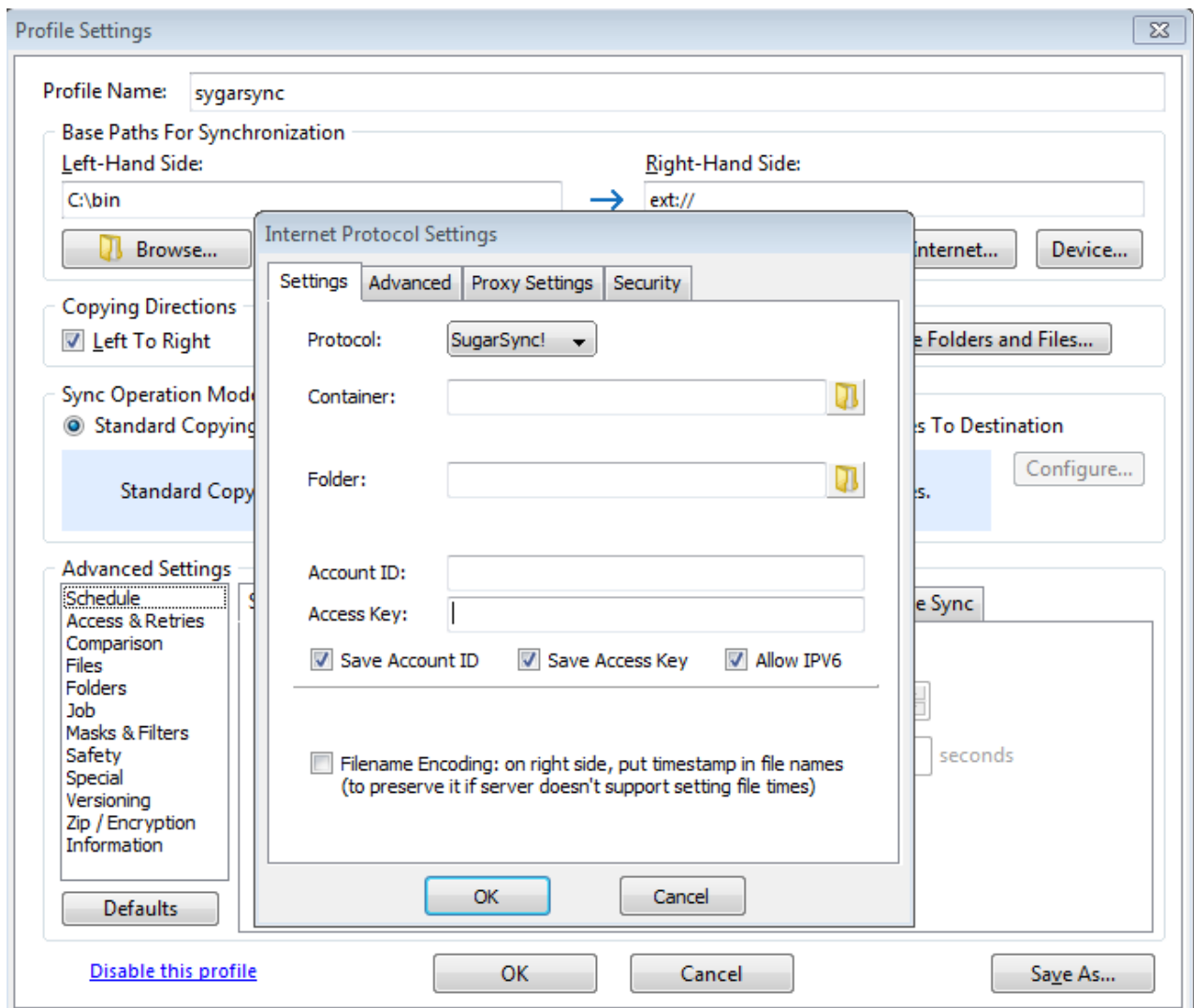
FAQ

Locking the log file location

You can specify a folder for the log files on the Program Settings dialog. However, if at any time Syncovery cannot create a log file in the folder, it will switch to a user-specific folder. Some customers have reported that the log folder location changes against their wish. To freeze the location, add the following line in the [Main] section of the INI file:

LockLogFolder=1

This article applies only to the Windows version of Syncovery

Licenses are perpetual – software updates free for two years.

FAQ: is the Syncovery license perpetual or per year?
It is a perpetual license. There are no yearly recurring fees. You can also use the registration code again after replacing a computer, without any additional fees. When replacing a computer, simply uninstall the software and use your registration code again on the new one.

Updates and upgrades of the software are included for two years. After that, you can still use the last version you got, or if you decide to upgrade to the newer version that we may be offering, 50% of your original payment will be credited against the new order, so in most cases, the new licenses costs 50% of the regular price.

Confirmations missing, deletions disabled and similar warnings

When a job runs in unattended mode, there can be some conditions which have to be confirmed when the profile is configured. For example, file deletions have to be confirmed specially, in addition to configuring the sync operating mode to include deletions.

To give the confirmations, please edit your profile in Advanced Mode, go to the Safety section at the bottom and choose the tab sheet "Unattended Mode".

For an Exact Mirror profile, you would usually make sure that the top four checkmarks are chosen and that the last one is not chosen (Special Safety Checks). The first four checkmarks allow things like replacing files and deleting files. The last checkmark would impose additional safety checks which can prevent file deletions, so you'll want to remove that checkmark.

In addition, you should specify a percentage of files which may be deleted during a profile run. You should not set this to 100% unless you expect that nearly all files are regularly going to be deleted. This is a safety percentage. If more files than allowed need to be deleted, the program realizes that something is wrong and disables the deletions completely. This will protect you against rare error conditions like disk errors or network communication errors, which can sometimes cause empty folders to be reported on the source side. Due to the percentage limit, the program will not delete everything from the destination if suddenly the source seems to be empty, or nearly empty.

However, even if you do specify 100% for deletions, the program will never delete all files in order to protect your data. If the source side is empty, it will throw an error and refuse to delete everything from the destination. This should be a good safety measure for most use cases. Some customers, on the other hand,

have use cases where deleting all files is a regular, normal requirement. These customers can disable the 100% deletion protection by adding the following line to the [Main] section of the INI file:

UnattendedDeleteAllIsOK_IfDelPercIs100=YES

(Add this only if you need to delete 100% of files in a destination folder in unattended mode!)

Keeping 5-7 Full Backup Copies of Your Data in Separate Folders

There are different ways to keep several versions of your files on your backup storage. Firstly, in the profile under Versioning, you can specify to keep a number of
older versions for each file. Each file will be versioned independently, and the Restore Wizard can restore your newest data, or restore according to a specified target date in the past.

However, some customers prefer to have 5 to 7 complete and independent copies of their data. To achieve this, you can use the variable **$WEEKDAY** in the destination path. In that case, you would not use anything from the Versioning tab sheet.
This will keep seven days of complete folder copies, if the profile runs on every day of the week. It will cause your backup folders to be named Monday, Tuesday, Wednesday, etc. and the next week's backup is simply going to re-use the same folder from the week before.

For example, your destination path could be like this:
D:\Daily Backups\$WEEKDAY
Use Exact Mirror Mode to make sure that the backup is always identical even though the folder is re-used. Under Safety->Unattended Mode, allow file deletions as well as overwriting newer files with older ones (which will hardly ever be necessary, but should be chosen).

Copying NTFS File Security (Permissions)

Syncovery can copy NTFS security along with files.

On the tab sheet Special in the profiles, you will find a checkmark called "Process Security and Shares". On the dialog that pops up, you need at least three checkmarks on the left-hand side (Copy Owner/Group/Permissions).

In addition, the program needs to be running "As Administrator". To ensure it runs as admin, you need to right-click its icon and choose
"Run As Administrator", unless you have Windows versions older than Vista, or you have disabled UAC.

If using the scheduler, it probably needs to run as a service. Please see
Installing the scheduler as a service

How to deal with changing USB drive letters easily

A lot of customers ask how they can define a job so that it always copies to or from a USB drive, even if that drive's letter changes. For example, on one day, your external hard drive might be drive F: and on another day, Windows changes it to drive G:.

The solution is to change the "Base Path" for the external drive in the profile. Instead of the drive letter, type the volume label (volume name). For example, if your drive is named MyUSBDrive, then you would type MyUSBDrive:\FolderA instead of F:\FolderA.

FTP over HTTP Proxy or SOCKS

One of the new features in Syncovery version 6 is the ability to connect to an FTP server via an HTTP Proxy as well as SOCKS. This feature is somewhat hidden in the software, so here's how to find it.

If you are using the FTP protocol, then on the Internet/FTP dialog, change the FTP library to 2. Then on the Proxy tab sheet, you will see the option to use an HTTP Proxy or to use SOCKS to connect.

If you are using SSH/SFTP, Web Tunneling and SOCKS is also supported via the Proxy tab sheet. In that case, use library 1 (SFTP).

Amazon Glacier Backup

Since version 6.20, Syncovery can upload files to Amazon Glacier. To set up Glacier as the destination, click on the Internet button for the right-hand side and choose Glacier as the Internet Protocol.

Amazon Glacier is intended for long term archiving and backup with the expectation that most operations are uploads and not downloads. Downloads should be a rare exception, since they can be extremely slow. To download a file, Syncovery needs to initiate a job with Amazon Glacier, and even with small files, it takes at least three hours for Amazon Glacier to retrieve the item. The same is true for file listings. Therefore, Glacier cannot be used for two-way synchronizations. It is intended only for backing up and archiving.

Please be aware that there is a **download fee** from Amazon if you download more than 5% of your data per month (or something like that). It seems that in some special cases, the download fee can be extreme. If you intend to make a full backup and restore for testing, please read the fee schedule closely, and also read articles such as this one:
Is There a Landmine Hidden in Amazon's Glacier?

Two methods to use Glacier

- Choose S3 inside our software, and use a lifecycle rule in S3 to move files to Glacier to reduce costs. See the Amazon Web Services Blog
- Choose Glacier directly in our software. The rest of this article describes this method.

Because there is no quick way to get a file listing from Glacier, Syncovery maintains a local database with the information of all the files on Glacier. This database is automatically maintained and it is independent from the checkmark "Cache Destination File List". Therefore, with Glacier, there is no need to use the caching option. The local databases used for Glacier are separate for each vault, but shared among all profiles. When you create a new profile that accesses an existing vault, it will alraedy know the vault contents, if the vault has been used on the same machine.

Glacier also cannot rename items which have been uploaded. When you rename or move files on the local side, they have to be uploaded again.

In version 6.20, the download process is still inefficient if you need to download many files. It will initiate the download job for each file and wait for it to complete, then download the file, and then proceed to the next file. You can specify a number of files to copy in parallel in this fashion (on the Files tab sheet), but the limit

is 30. So, you can download up to 30 files in 3 to 5 hours, but downloading 300 files will take 30 to 50 hours. This limitation will be removed in a future update.

In light of this, if there is a chance you will need a complete restore, it may make sense to use "Zip Packages" with many files per zip archive, instead of uploading individual files.

This information will be updated as support for Glacier is optimized and more experiences are made with Amazon's new service.

Mountain Lion Compatibility

A Mountain Lion compatible update of Syncovery is **now available**. The version number must be **6.03** or higher.
To be able to continue using your old configuration and profiles, please use at least version **6.04**or higher. The migration wizard should appear automatically, or you can invoke it via the File menu. You can also manually import config files via the File menu.

Since version 6.04, no special action is required any more to migrate your settings.

Rsync and Syncovery

Syncovery supports the Rsync protocol by using an rsync.exe command line utility. Here's how to set it up:

On the Program Settings dialog, you need to specify which rsync.exe to use. There's also a button to download an rsync for Windows installer.

In the profile, you click on the Internet button for one of the two sides of the sync. Choose Rsync as protocol. You can securely connect via SSH or use rsync directly (unsecured). The unsecured connection can be used within a LAN or VPN, for example.

When using it via SSH, you need to have a client certificate and configure it on the Certificates tab sheet, as well as choose it on the Security tab sheet.

Because of limitations of the rsync.exe command line, some features are not working. For example, Syncovery cannot delete any files via rsync.

Because of rsync limitations, it is often better to use SFTP/SSH. It can do block level copying, too, and also it can get a recursive listing similar to rsync (on Unix/Linux servers). The recursive listing checkmark is on the second tab sheet of the Internet/FTP dialog.

Please see the following page for details about block level copying with SFTP:
Block Level Copying
The limitation with block level copying and SFTP is currently that it does block level for uploads only

Confirmations missing, deletions disabled and similar warnings

When a job runs in unattended mode, there can be some conditions which have to be confirmed when the profile is configured. For example, file deletions have to be confirmed specially, in addition to configuring the sync operating mode to include deletions.

To give the confirmations, please edit your profile in Advanced Mode, go to the Safety section at the bottom and choose the tab sheet "Unattended Mode".

For an Exact Mirror profile, you would usually make sure that the top four checkmarks are chosen and that the last one is not chosen (Special Safety Checks). The first four checkmarks allow things like replacing files and deleting files. The last checkmark would impose additional safety checks which can prevent file deletions, so you'll want to remove that checkmark.

In addition, you should specify a percentage of files which may be deleted during a profile run. You should not set this to 100% unless you expect that nearly all files are regularly going to be deleted. This is a safety percentage. If more files than allowed need to be deleted, the program realizes that something is wrong and disables the deletions completely. This will protect you against rare error conditions like disk errors or network communication errors, which can sometimes cause empty folders to be reported on the source side. Due to the percentage limit, the program will not delete everything from the destination if suddenly the source seems to be empty, or nearly empty.

However, even if you do specify 100% for deletions, the program will never delete all files in order to protect your data. If the source side is empty, it will throw an error and refuse to delete everything from the destination. This should be a good safety measure for most use cases. Some customers, on the other hand, have use cases where deleting all files is a regular, normal requirement. These customers can disable the 100% deletion protection by adding the following line to the [Main] section of the INI file:

UnattendedDeleteAllIsOK_IfDelPercIs100=YES

(Add this only if you need to delete 100% of files in a destination folder in unattended mode!)

Keeping 5-7 Full Backup Copies of Your Data in Separate Folders

There are different ways to keep several versions of your files on your backup storage. Firstly, in the profile under Versioning, you can specify to keep a number of
older versions for each file. Each file will be versioned independently, and the Restore Wizard can restore your newest data, or restore according to a specified target date in the past.

However, some customers prefer to have 5 to 7 complete and independent copies of their data. To achieve this, you can use the variable $WEEKDAY in the destination path. In that case, you would not use anything from the Versioning tab sheet.
This will keep seven days of complete folder copies, if the profile runs on every day of the week. It will cause your backup folders to be named Monday, Tuesday, Wednesday, etc. and the next week's backup is simply going to re-use the same folder from the week before.

For example, your destination path could be like this:
D:\Daily Backups\$WEEKDAY
Use Exact Mirror Mode to make sure that the backup is always identical even though the folder is re-used.
Under Safety->Unattended Mode, allow file deletions as well as overwriting newer files with older ones (which will hardly ever be necessary, but should be chosen).

See also: **Variables to use in your sync paths**

Command Line

You can run, create, edit, rename and delete profiles via command line.

Windows

You can invoke either Syncovery.exe or SyncoveryService.exe with the command line parameters shown on this page. SyncoveryService.exe is only capable of running jobs, while Syncovery.exe can perform all these actions. SyncoveryService.exe is more lightweight and it can run totally invisible as well as report progress to the main GUI.

Command Line Examples for Running a Job on Windows:

- Run a job minimized:
  Syncovery.exe /RUNX="Profile Name" /S /M
- Run a job invisible but with progress reporting to the GUI:
  SyncoveryService.exe /RUNX="Profile Name" /S /M /P /T

Macintosh

On Mac, you can use the command line parameters in a shell script like in this example:
open ./Syncovery.app --args /RUNX="Profil Name" /U

Parameters for Running a Job

- **/RUN="Profile Name" and /RUNX="Profile Name"**
  With these options, you can invoke a specific profile from the command line for immediate execution. /RUN= starts the profile and leaves the program running. /RUNX= starts the profile and exits the program after the profile has been executed.
  You can use the asterisk wildcard at the end of this option, for example:
  /RUN=* or /RUNX=* or /RUNX=Office*
  You can also add this to cause a shutdown when done by adding /SHUTDOWN
- **/O** (show only results)
  Runs the job without Sync Preview but shows a dialog with the results.
- **/U** (unattended mode)
  The profile is started and executed without further user interaction. When this option is not specified, the file list is being shown, but the actual synchronization must be started manually. In unattended mode, the program will only show an error message if one of the synchronization paths cannot be accessed.
- **/S** (silent mode)
  Like /U but there will not be any error messages whatsoever.
- **/M** (minimized mode)
  The program is minimized to the system tray while executing the profile. This option implies /U.
- **/P** (progress reporting – SyncoveryService.exe only)
  SyncoveryService.exe will report progress information to the main program, in the same way the   scheduler starts background jobs.
- **/T** (run in threads – SyncoveryService.exe only)
  SyncoveryService.exe will run the job in a separate thread rather than in the main process thread, in   the same way the scheduler starts background jobs when the option "Start profiles in parallel" is   chosen.
- **/LEFT="Folder Path"**
  allows you to specify a left path that is different from the one stored with the profile.
- **/RIGHT="Folder Path"**
  allows you to override the profile's right path.

- **/MASK="File1.txt;*.doc"**
  allows you to override the profile's inclusion masks, or simply specify one or more files to copy.
- **/EXCL="*.bak"**
  allows you to override the profile's exclusion masks.
- **/SHUTDOWN** (Windows only)
  Shutdown after running the profile(s) specified with /RUNX="Profile Name".
- **/CHOOSESUBFOLDERS**
  The subfolder selection dialog is shown prior to running the job. The selection that is made is not saved permanently unless you also specify the /SAVE parameter. Alternatively, you can add /SAVEONLY in order to save the new selection without running the job. In all cases, the profile name should be specified with /RUNX, even if you use /SAVEONLY.

General-Purpose Parameters
- **/INI="Path to configuration file"**
  Specifies the configuration file to be used. For example,
  /INI="C:\ProgramData\Syncovery\Syncovery.ini"
- **/IMPORT="Path to XML or CSV file"**
  Import profiles from XML or CSV. To find out how to make such files, please create a sample profile and export it by right-clicking it on the Profile Overview.
-

Command Line Parameters for Managing Profiles

The command line to create any given profile can be seen by creating it manually first, then going to Information->Show Profile Details… in the profile editor.
Here's an example:
Syncovery.exe ADD /Name="Documents Backup" /Left="C:\Users\Me\Documents" /Right="D:\Backup\Docs" /L2R /Deletes /ReplaceNewer /MaxParallelCopiers=2
Alternatives to ADD
RUN (creates & runs a job without creating a permanent profile)
DELETE "Profile Name" (deletes a profile)
CHANGE "Profile Name" (changes an existing profile, keeping any existing settings which are not set on the command line)
RENAME "Old Profile Name" "New Profile Name"
ADD can be used to completely replace an existing profile with new settings.

Variables

Variables that can be used in the sync paths
(in addition to standard Environment variables such as %TEMP%)

$PROGDRIVE	= drive specification where the software is installed
$DATE	= current date
$TIME	= current time
$WEEKDAY	= day of week
$2WEEKSDAYS	like $WEEKDAY but for two weeks, i.e. A Monday … A Sunday, then = B Monday … B Sunday, then starts over
$DWMQ	rotation with separate folders for each day of the week, week, month, quarter (see example). Keeps one copy for each quarter, then one copy for each month in the last quarter, one copy for each week in the last month, = and one copy for each day in the last week.

$MYDOCUMENTS	= current user's My Documents folder
$ALLUSERSPROFILE	All Users folder, for example = C:\Documents And Settings\All Users
$USERPROFILE	= Current user's profile folder
$APPDATA	= Current user's Application Data folder

$DAYOFMONTH or**$MONTHDAY**	= today's day number in the month (01-31)
$DAYOFMONTHSD	= today's day number single digit (1-31)
$WEEKDAYNUM	= today's day number in the week (1=Monday)
$WEEKOFYEAR	= The week number.
$MONTH	= this month's name
$MONTHNUM	= this month's number (01-12)
$MONTHNUMSD	= single digit month (1-12)
$YEAR	= current four-digit year number
$HOUR	= Hour the profile was started (two-digit)
$MINUTE	= Minute the profile was started (two-digit)
$SECOND	= Second the profile was started (two-digit)
$HHMMSS	= Time the profile was started

$YESTERDAY	= yesterday (01-31)
$YESTERDAYSD	= yesterday single digit (1-31)
$YDWEEKDAY	= yesterday's name
$YDMONTHNUM	= yesterday's month (01-12)
$YDMONTHNUMSD	= yesterday's month single digit (1-12)
$YDYEAR	= yesterday's year

$LEFTPATH	= Adds the left-hand path (for use in right path only)
$RIGHTPATH	= Adds the right-hand path (for use in left path only)
$PROFILENAME	= The name of the profile.

Variables that can be used in the Execute before/after paths

$LEFT   = left base path of synchronization

$RIGHT   = right base path of synchronization

$LEFTDRIVE = Drive letter or UNC file share of the left-hand side

$RIGHTDRIVE = Drive letter or UNC file share of the right-hand side

$MSG   = Short result summary

$RESULT   = GOOD or BAD (if an error has occurred)

$PROFILE   = Profile name

$LOGFILE   = Path and name of log file

Running the scheduler as a service on Windows

This article applies only to Microsoft Windows.
Running the scheduler as a service is a little more difficult to set up, but it has some advantages. The service will start up automatically with Windows, even while no user has logged on yet. The
service runs invisibly in the background without users noticing it. A user can also log out while the service is running a job. Neither will disturb the other. The name of the service is the Syncovery Service.

Tips
- The scheduler can run as a Windows Service. This means that scheduled synchronizations take place without users having to log on.
- The service is installed and started from the Scheduler tab sheet of the main application window. If the "Background Scheduler" is running, please stop it and then choose **Use: Service Scheduler**. Then you will see the service-specific install/uninstall, start/stop buttons.
- In order to access network drives, the service must be given a log on account. This is done when clicking on the **Install…** button on the Scheduler tab sheet to install the service. To change the log on account, please uninstall and then re-install the service. Make sure that you specify a user account where you know that Windows Explorer has access to the volumes that you need. Choose an account that has network access without Windows Explorer asking for a password for the network drive. Windows Explorer should have already stored the password.
- Also in order to enable access to a network drive, please try using a UNC path such as\\servername\sharename\foldername rather than a mapped drive letter.
- If this is not sufficient, you can provide a username and password for the network resource in each profile. Use this setting on the Job tab sheet in the profile: **Network Connections…**However, in many cases this is not needed. Rather than specifying the full path for the network connection, you can also try specifying just \\servername
- Deleting to the recycle bin is not supported by the service.
- Even though the service is normally invisible, you can get a pretty good picture of what it's currently doing or planning to do, using the Scheduler tab sheet of the main application window. You can even connect to a remote computer and control and watch the service running there.

Block level backup – Block Level Copying with Syncovery

Syncovery can detect which parts of a larger file have changed, and copy only the changed blocks rather than the complete file. This feature works similar to Rsync (but it's not the same).

Copying only the changed blocks can save bandwidth and time, especially over a slow connection. When copying between local disks or in a LAN environment, it can save bandwidth too, but may not always save much copying time, because the source file has to be read in its entirety every time in order to determine the changed blocks.

Only block-oriented file types are eligible for block-level copying. These include database files such as SQL or Outlook PST, as well as drive images and virtual hard disk images (VMs). Stream-based files, on the other hand, will usually cause all blocks to be changed whenever they are modified (for example text documents, spreadsheets, zip files, and photos). Thus block-level copying won't be able to save much bandwidth with stream-based files.

In Syncovery, block-level copying is called "Partial File Updating". In many cases, you need to choose only this one checkmark, which is on the Special settings category in the profiles (in Advanced Mode).

The program needs to have fast access to at least one of the sides of the synchronization. The other side may be a low-bandwidth connection. If you are using an Internet Protocol, please note that only SSH/SFTP supports block-level updating directly. The other protocols can only be used with Synthetic Backup (see further down below).

Please **note**: Block level copying with SSH/SFTP has only been implemented for uploads, not downloads.

Partial File *Updating* can work in three **different ways:**
Mode 1: With Database**:**
- **Source access must be fast**
- **Destination may be slow**
- **MD5 checksums are stored in database**
- **Destination files must not be modified by any other profile, person, or tool**
- **Destination must be accessed via LAN, VPN, or SSH/SFTP**
Mode 2: With Remote Service**:**
- **Syncovery Remote Service computes MD5 checksums on remote computer**
- **The "slow" side can be both source or destination**
- **MD5 checksums are newly calculated each time**
- **Files on both sides can be modified by other profiles, persons, or tools**
- **One side must be local or LAN/VPN, the other can be LAN, VPN, or SSH/SFTP**
Mode 3: Synthetic Backup**:**
- **similar to Mode 1, plus:**
- **adds Zip compression, versioning, and filename encoding**
- **can work locally or with any Internet Protocol for the destination side**
- **the changed blocks are uploaded in a new, separate zip file every time**
- **all older zip files must stay on the backup storage, but can be thinned out**
- **all connection types and Internet Protocols are supported**

Mode 1: Slow Destination
In this mode, the speed-up is available when you copy files from a location to which you have fast access (preferably your own hard disk). The destination can be a slow connection, but it must be a normal file system (either LAN or VPN) or SSH/SFTP. For other connections, you can use Synthetic Backup.
Instructions for Mode 1
In your profile, make the following checkmark: Use Partial File Updating, which is on the Special tab sheet when editing the profile in Advanced Mode. The next time you run the profile, a database is created on your hard drive where information needed for the speed-up is stored. The second time you run the profile, you should notice the speed-up.

Mode 2: With Remote Service
This mode can speed up updating large files in both directions. The remote computer can be both source and/or destination. This is achieved by running a small service application on the remote computer, which will create the necessary checksums on the fly, when requested by the main application running on a different machine. See more information on the Syncovery Remote Service here.
The other (local) computer, where the main Syncovery program is running, needs to have normal file system access to the remote computer (LAN or VPN), or it can use SSH. It needs to have write access to the remote computer so that it can save the checksum request file there. The MD5 checksums are created when needed, so that no database is being used.

Instructions for Mode 2
On the remote system, run the Setup program and install the Syncovery Remote Service along with its control panel. Start the control panel from the Syncovery group in the Start menu. On the tab sheet Configure Checksummer, enter the base folders that will be used for synchronization. Click Apply. On the tab sheet Service Configuration, click on Install Service and Start. The service will be using the Windows System account by default. If this account doesn't have sufficient access privileges, you may have to change the account in Windows Control Panel -> Administrative Tools -> Services.
On the local system, you are running the main Syncovery program. In your profile, the right-hand side must be the remote system. Specify one of the folders which you have specified for the remote service to monitor. The left side should be your local folders, or a network drive with relatively fast access. On the Specials tab sheet in Advanced Mode, make the following checkmarks: Use Partial File Updating and Right side uses Remote Service.

Mode 3: Synthetic Backup
This feature is intended for backing up from a local storage to any type of backup storage. The backup can be local or online.
Choose "Synthetic Backup" on the tab sheet Versioning->Synthetic Backup. This will automatically place these additional checkmarks:
- Use Partial File Updating (under Special)
- Filename Encoding (under Versioning)
- Zip Each File Individually (under Zip/Encryption)

Syncovery Remote Service

The Remote Service is a useful tool to enable some special features which are somewhat less frequently used. There are two kinds of services, the Syncovery Service, which is the scheduler and runs profiles in the background, and the Syncovery Remote Service, which is not needed to run any profiles.
The Syncovery Remote Service is installed on the "other end". For example, if you use Syncovery on a client which exchanges files with a server, then Syncovery Remote Service can be installed on the server to perform one or more of the following tasks:

- Unzip incoming ZIP packages. This feature is used in conjunction with the ZIP Package capability in order to speed up the transfer of files.

- Generate a Remote Listing. This feature is used to speed up the "Building File List" phase.

- Generate MD5 Checksums for Partial File Updating.

Installation of the Syncovery Remote Service

The Remote Service is installed using the same Setup program from our download page that you use to install Syncovery. When running the Setup, make sure you include the Syncovery Remote Service and its Control Panel.

You will find the Syncovery Remote Service Control Panel in the Syncovery program group in your Windows Start menu. Please run it and install the service with it.
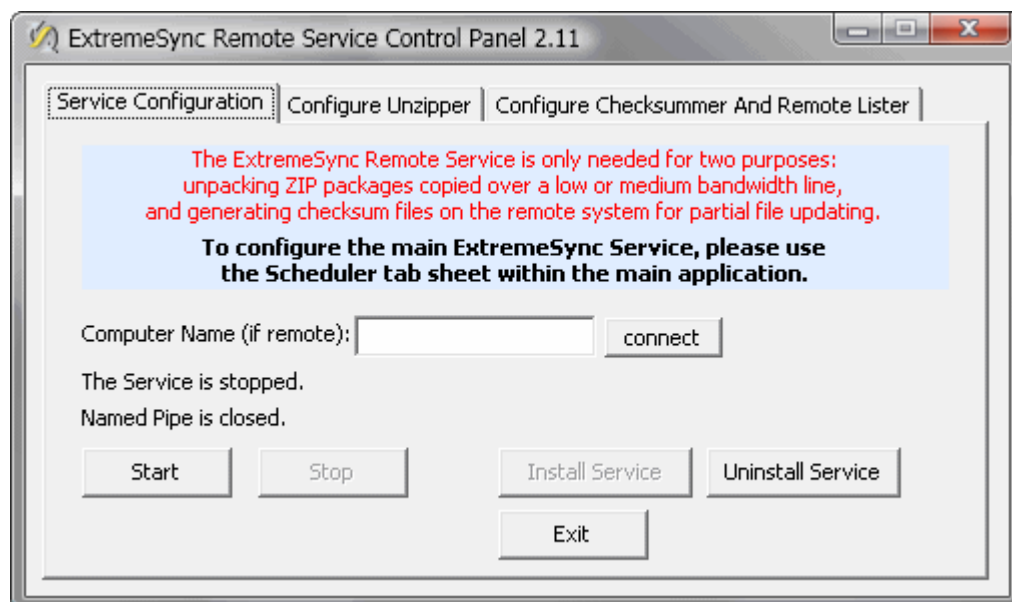
Configure Unzipper

To use the unzipping capability, you need to specify the "folders to watch" on the tab sheet "Configure Unzipper". Each folder must be the same one that you specify as destination folder in the Syncovery profile on the other computer. Except that here, you specify local folders, but they must be the same ones. If you have several profiles with different destination folders, each one must be specified here on a separate line, even if they are all on the same drive.

The Syncovery profile on the sending maching needs to be set up to "Use ZIP Packages" and on the ZIP Package Configuration dialog, you need to use the setting "Syncovery Remote Service will be used".

The Syncovery main program will put the ZIP packages into a subfolder called "Incoming Syncovery Packages". This is actually the folder that the Remote Service's unzipper will watch, but you don't specify it. You specify the same folder that is used in the profile.

Configure Checksummer and Remote Lister

The checksummer and the remote lister are configured on the third tab sheet. Like the unzipper, they watch certain folders for incoming files. The incoming files are special request files sent by the synchronizer on the other machine. So, the Synchronizer does not communicate with the Remote Service using any kind of network protocol. Instead, it puts a "request file" with a special filename into the folder on the server, and the Remote Service sees the file, reads it and then knows what to do and deletes the request file.

You need to specify the "folders to watch" for incoming checksum or remote listing request files. Each folder must be the same one that you specify in the Syncovery profile on the other computer. Except that here, you specify local folders, but they must be the same ones. If you have several profiles accessing different folders on this machine, each one must be specified here on a separate line, even if they are all on the same drive.

Using the Remote Listing Feature

Once the Remote Service has been set up correctly, you can speed up the "Building File List" phase considerably by using the checkmark "Left/Right side listing uses Remote Service", which can be found in the profiles on the "Specials" tab sheet, when editing them in Advanced Mode.

Using the Checksummer Feature for Partial File Updating

Purchasing

For purchasing information, please visit our web site:

www.syncovery.com

For further information, please write to support@syncovery.com

Company Information

Super Flexible Software Ltd. & Co. KG
Tobias Giesen

Registered in Germany, Amtsgericht Münster HRA 9716

Internet Site: www.syncovery.com

Electronic Mail: support@syncovery.com

Telephone: +49 251/20897745
FAX: +49 251/9520-9011

Postal address
Buddenstr. 29-31
48143 Münster
Germany