

Setup your backup today – better safe than sorry

A guide for installing and configuring an automatic backup system using the free software Cobian

Luka Wanjohi, Elizabeth Kamau and, and Jens Riis-Jacobsen, CIP-SSA, Nairobi, July 19, 2011

Introduction

Every day we are generating a lot of data as this is the core of our scientific research. But things often go wrong and data gets corrupted by viruses, a laptop get stolen, hard drives fail, or thumb drives get misplaced and **days, weeks, or months of work is lost**. And your research comes to a screeching halt!

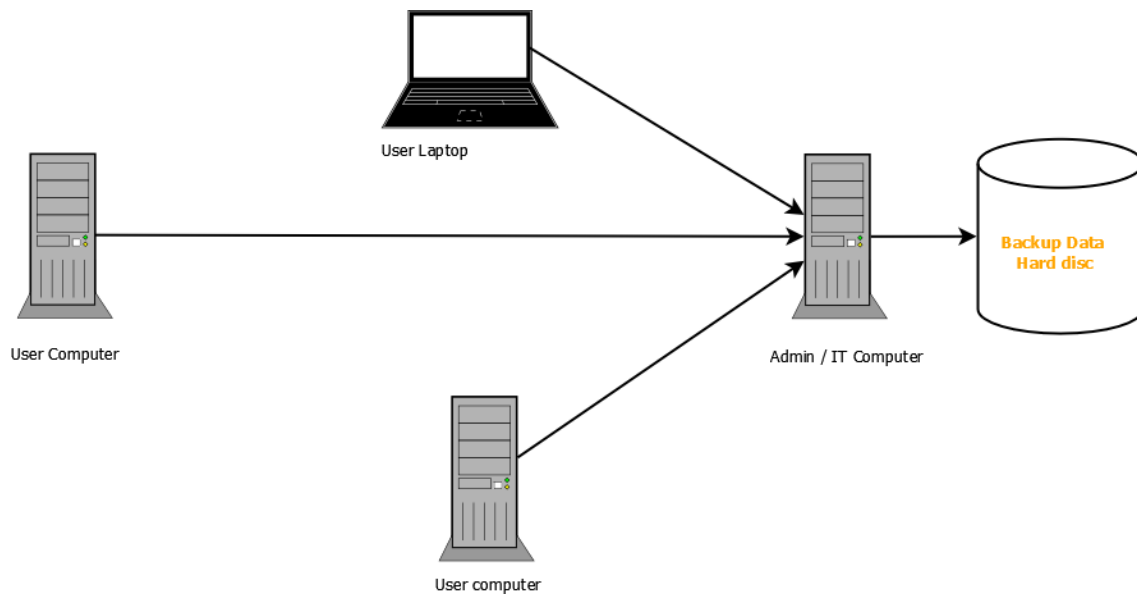
A backup is a copy of your data. It is carried out to ensure that your data can be rescued in case of a problem or disaster. **Backup is like an insurance policy – it must be done before the disaster happens**, if it is to be of any help, so set it up today and not tomorrow.

Backup must be automatic and not an ad hoc thing you do when you remember and have the time, and **this guide will help you set up an efficient and automatic backup system that will protect you against loss of data**. It will help you install and configure a free backup software called Cobian. It is an easy to use and free application which can be downloaded from <http://www.educ.umu.se/~cobian/cobianbackup.htm>. Once you have successfully installed Cobian, the second section will take you through configuring a backup task.

Installing Cobian is not enough; you MUST also configure a backup task. If you only install, but do not configure the backup task, no data will be backed up. The configuration is explained in the second half of this guide.

It is almost no use backing up your data on the same hard disk where it is already stored, as you are likely to lose the whole hard disk in case of a problem occurring. **The best solution is to set up the backup via the network and use another computer for your backup.** If you have a dedicated computer for the purpose that is the best, but you can also use for example the computer of someone who is permanently in the office such as administrative staff. If that is not possible you can use an external hard disk for your backup. The key thing to remember is that **you cannot do backup on your own hard disk, and if you do backup to an external hard drive, you cannot carry that around with your laptop computer, as you are likely to lose both at the same time.**

In figure 1 you can see a diagram of a typical backup system. The two desktop computers and the laptop are all being backed up to a central computer which can either be a dedicated computer such as a server, or the computer of for example an administrative staff where an extra hard disk is added to the computer. For extra security the data is then backed up onto an external hard drive. Ideally, this external hard disk is stored outside the office so that in case of for example fire or theft, the data can still be recovered.



Typical Small Office Backup Set Up

Figure 1: Backup system for a small office

If you are an advanced computer user and you know the setup of your network in the office you may be able to setup the backup system yourself, however, **the recommended option is that your IT support staff should setup the backup system** – if they have not already done so. Making sure all data is backed up is the single most important IT support task.

The proposed backup system is automatic, but as any complex system it may occasionally develop a problem and you must monitor that it is still working. The proposed method is that **someone in your office has the responsibility that once a week they use a checklist to verify that all computers were backed up that week.** If all data is being backed up to the same computer this is a simple question of looking at the date of the files being backed up from each computer. **The monitoring of the backup should not be left to the IT support, but should be done by for example administrative staff** – this is part of the supervision and quality control of the IT support.

Installation of the backup system

This section explains how to download and install the backup software, Cobian

Download installation file for Cobian

Download **Cobian 10.X.X** from <http://www.educ.umu.se/~cobian/cobianbackup.htm>. Save the installer file, *cbSetup.exe*, anywhere on your computer. You will delete the file after the installation.

Minimum requirements

- Windows NT, 2000, 2003, Vista, and Windows 7.
- Microsoft Windows Installer 3.0 and above
- Microsoft Windows .NET Framework 3.5 and above

Installation start and license

Double click *cbSetup.exe* to start of the installation process. Click **yes** to allow Changes if prompted by your operating system. Click **Next**



Figure 2: Install start

Now you have the software license agreement. Read carefully and at the end select **I accept** and click **Next**.

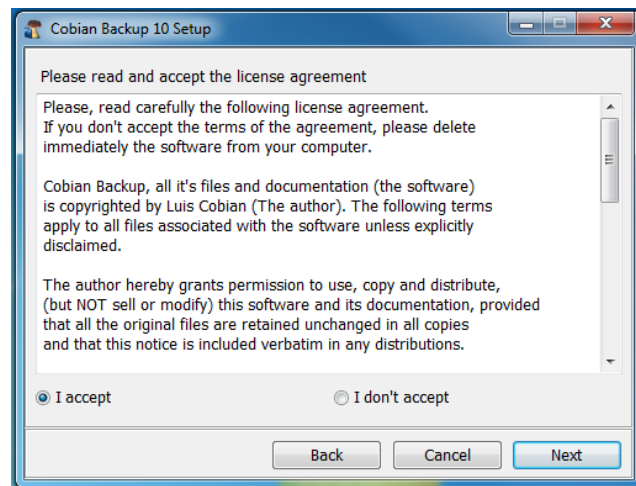


Figure 3: Install License

Install Options

The next screen has the following options, and **typically you will want to leave them as proposed by default**:

- **Create start menu icons**, which Copies Cobian Icons to the startup Menu. Enabled by default and should be left so.
- **Create a script for unattended installations**. This is helpful if you intend to replicate the installation on other computers. This option creates a script that when used subsequently does an installation of the software using similar settings as to the current installation. By default it is not selected and you may leave it as so unless you intend to use the installation script later.
- **Install the volume Shadow Copy requester**. Volume Shadow Copy Services is a technology that can be used to copy files that are locked or in exclusive use by some other application. You will need to have the .NET framework 3.5 and above to be able to use this service. By default it is enabled.

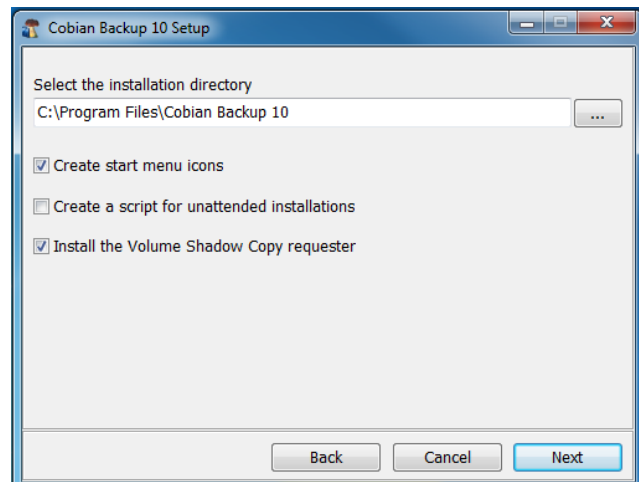


Figure 4: Installation directory and other general settings

Once you have made your selection above, click **Next**.

The next screen requires you to select the startup mode for Cobian and the Windows account it will use.

You want to install Cobian as a windows service because as a backup software it should be running at all times. Installing it as a windows service ensures that it starts running every time you boot your computer. Select the 'Service' option under *installation type*. See figure 4 below.

Service Options gives you two modes of installing Cobian, and the choice we make here is guided by the network setup of the computers to be backed up.

Select the first option '*Use the local System account*' if you are running a standalone computer or a peer-to-peer network. This is typically the case in a small office.

Select the second option '*use the following account*' if you have a windows domain configured to control your network. The account you type here must have domain administrative rights. This ensures that you have the rights to logging into individual computers to copy files or write files (in the event where the computer/device you storing the backups on are on the same domain). This is typically the option to use in a larger institution with a large network.

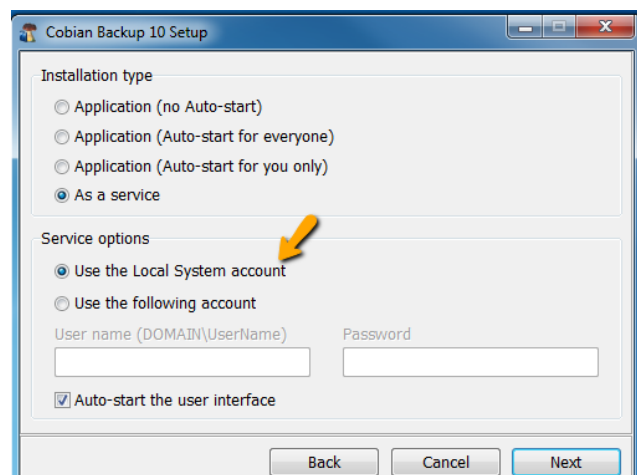


Figure 5: Installation type and Service options

Click **Next**. If you chose the Local System Account service option, you will get a prompt informing you that you might not be able to access network resources. Click **Yes** to continue. See figure 5 below

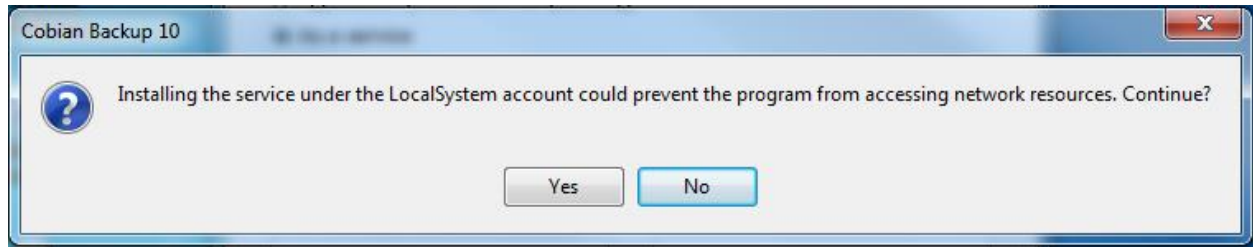


Figure 5: Warning message if you chose the Local System Account in previous step.

Click **Next** to start the installation process. The installation will run and you will be able to see when the process is complete. See figure 6

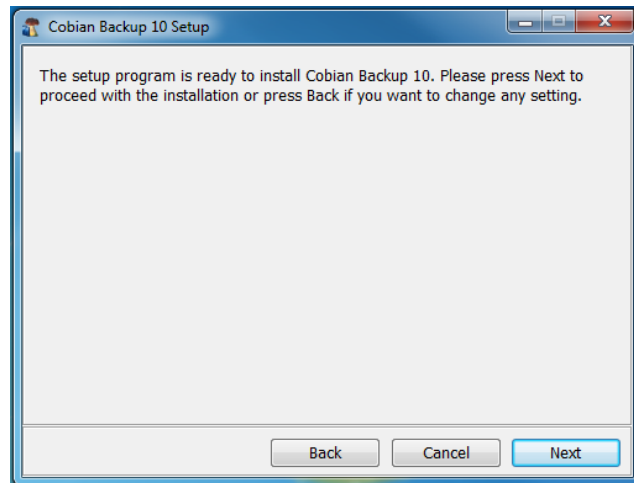


Figure 6: Start the install process

Now Click **Done**. You have successfully installed Cobian backup.

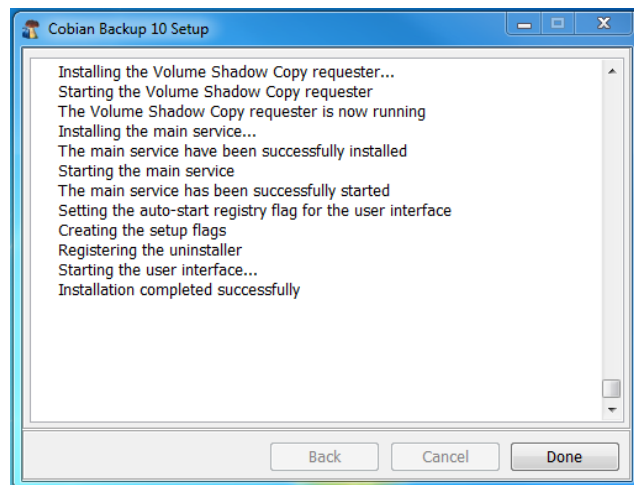


Figure 7: Message after install has been completed

Cobian backup is running on your system now. **You will need to configure a backup task. See the Setting up the automatic backup below.**

Setting up the automatic backup

The automatic backup is set up as one or more tasks. A task typically is set up to make a backup of certain data at a certain frequency, e.g. every day at mid day to back up everything inside Documents.

What should we backup?

Most data will be stored inside My Documents or Documents as it is called in the latest versions of Windows. However, some data will be stored outside this folder either in the Users folder or some applications may create dedicated folders typically directly on the C drive.

- All data within a users profile i.e. : My Documents, Desktop, Outlook files
- Application data: CloneSelector, field books, etc

In different version of windows the users profile data has been stored in folders with different names, so it is unfortunately not easy to exactly where to look but:

- On Windows 7 and Vista the User profile is typically in: C:\Users\username .
- On Windows XP it will usually be C:\winnt\profiles\username or C:\Documents and Settings\username

And this can also be setup to be stored in other places, and some IT departments even create a dedicated drive, typically D, where all the user data is stored. You may want to ask your IT support where your data is stored, if you are not sure.

Ideally files should be backed up every time there is a change.

It is important to stress to the users that they always store their files in the locations indicated to ensure that it is always backed up. For example all trials being done using CloneSelector should always be inside the CloneSelector folder. Projects files for example should be stored in the documents folder, etc.

Finally, users must inform the person responsible for backup in case they change computers. This ensures that configurations for running automated backups are ever present on any computer that is being used for their work.

How to setup a task for backing up data

Click on the **Create a new task** Icon to start the setup of a new backup task.

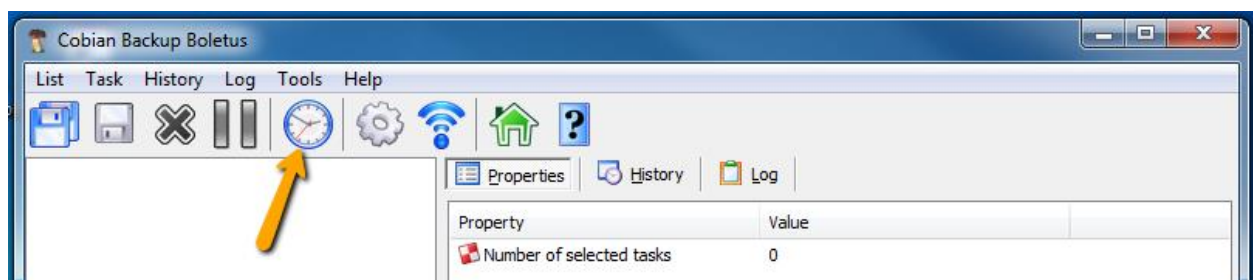


Figure 8 : New Task Icon

Now you have a New Task window. A backup task can be configured to include a specified group of files/folders. It can be set to run on a specified day/time , in addition to being run manually.

The left sidebar contains a list of menus with various associated screens. These are used to setup the various backup options. We shall look at a few important ones. Most of the default settings will be sufficient for our backup configuration.

General options

Some of the options here are:

Task Name: This is the name of the backup task. It could be something like *Luka-Documents*

Disabled: This option is disabled by default and it **MUST** be left so. It is useful when you want to disable a given backup task that has already been setup.

The next four options i.e. *Include subdirectories*, *create separated backups using timestamps*, *use file attribute logic* and *use volume shadow copy* should be left at their default setting. All are enabled at default.

Backup types explained

Under the **Backup type**, select **Differential**. Two backup type options are explained below:

Full: This option means that every single file in the source location will be copied to your backup directory. You will have several copies of the same source (identified by the time and date of the backup in the folder title).

Differential: The program will check if the source has been changed from the last full backup. If there is no need to copy that file, it will be skipped, saving backup time.

The reason we choose the differential backup is because a full backup will take so much time to run to completion, during which time the user may be unable to use their computer to perform other tasks effectively. However, **every 10th time that the backup runs, a full backup is made**. See the last textbox on the above screen **set it to 10**.

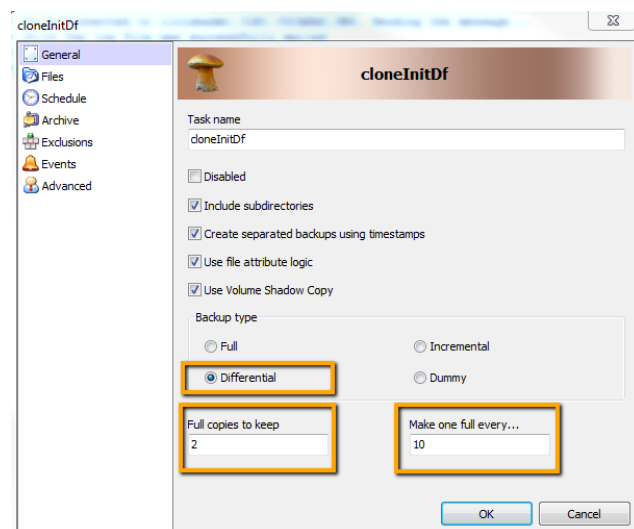


Figure 9 :: New Task Window

We do not want to fill up the backup hard drive. Several *full backups* over short period of time can easily fill up the hard drive your are backing up your data on. To prevent this, we set the **Full copies to keep to 2**. Now at any one time you will only have two full backups from a given backup task. Older *full backups* will be automatically deleted when a backup task runs.

Files options

Now we are at the **Files** tab. You may get a warning *the source cannot be empty*. This is because we have not setup anything on this screen yet, just click **Ok** to begin the setup.

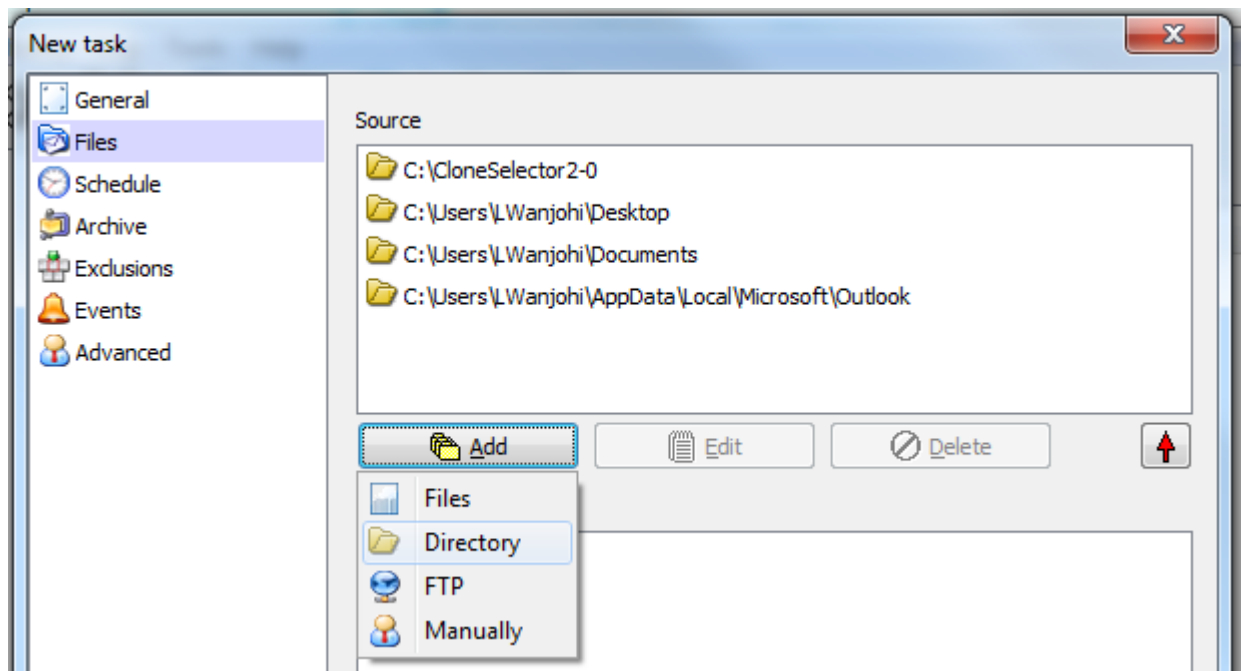


Figure 10 :: New Task Files

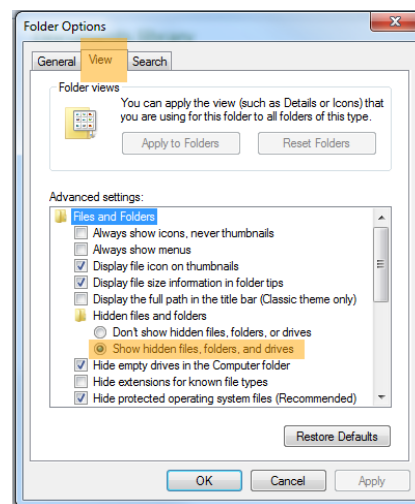
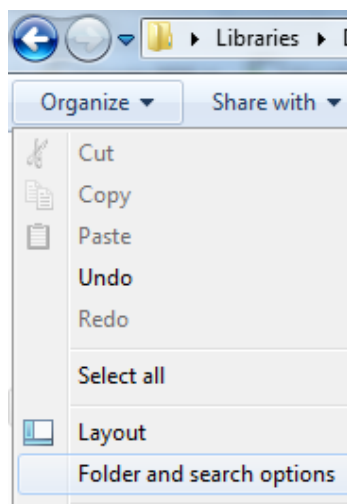
Add the files/folders that you want to be backed up. Selecting file adds a single file. While selecting *directory* adds an entire directory with all the files and subfolders.

Figure10 above shows example of files/folders being backed up. Notice the user profile folders *Desktop*, *My Documents* and *Outlook*. The outlook folder contains PST files for emails. Lastly, take note of the *outlook folder* location. You have to enable hidden files to be able to access it under the *Directory* option. Remember *LWanjohi* will be

username on
E.g. *ANaico*,

replaced by
your
SAngili, etc

your
computer.



Destination options

Below is a pane labeled ***Destination***. This is where your backup will be stored. It could be a single location or multiple locations. Select ***Add*** then ***Directory*** and choose a location of your choice. **THIS LOCATION MUST BE EXTERNAL TO THE COMPUTER YOU ARE BACKING UP. IT SHOULD BE AN EXTERNAL HARD DISK OR A DIFFERENT COMPUTER.**

Schedule options

Next we need to create a schedule for our backup.

To keep it simple, schedule daily backups. Choose a time of the day when the computer is most likely to be available. The most important thing is that the backup is done at least once a day.

Scheduling backup for desktop computers is the easiest since they permanently are in the office. Pick a time of the day when the computers are powered on. It is important that you give the process ample time to run to completion. Do not schedule the backup for the last 30 minutes of a given day for example as a user may shut down her workstation while the backup is in progress.

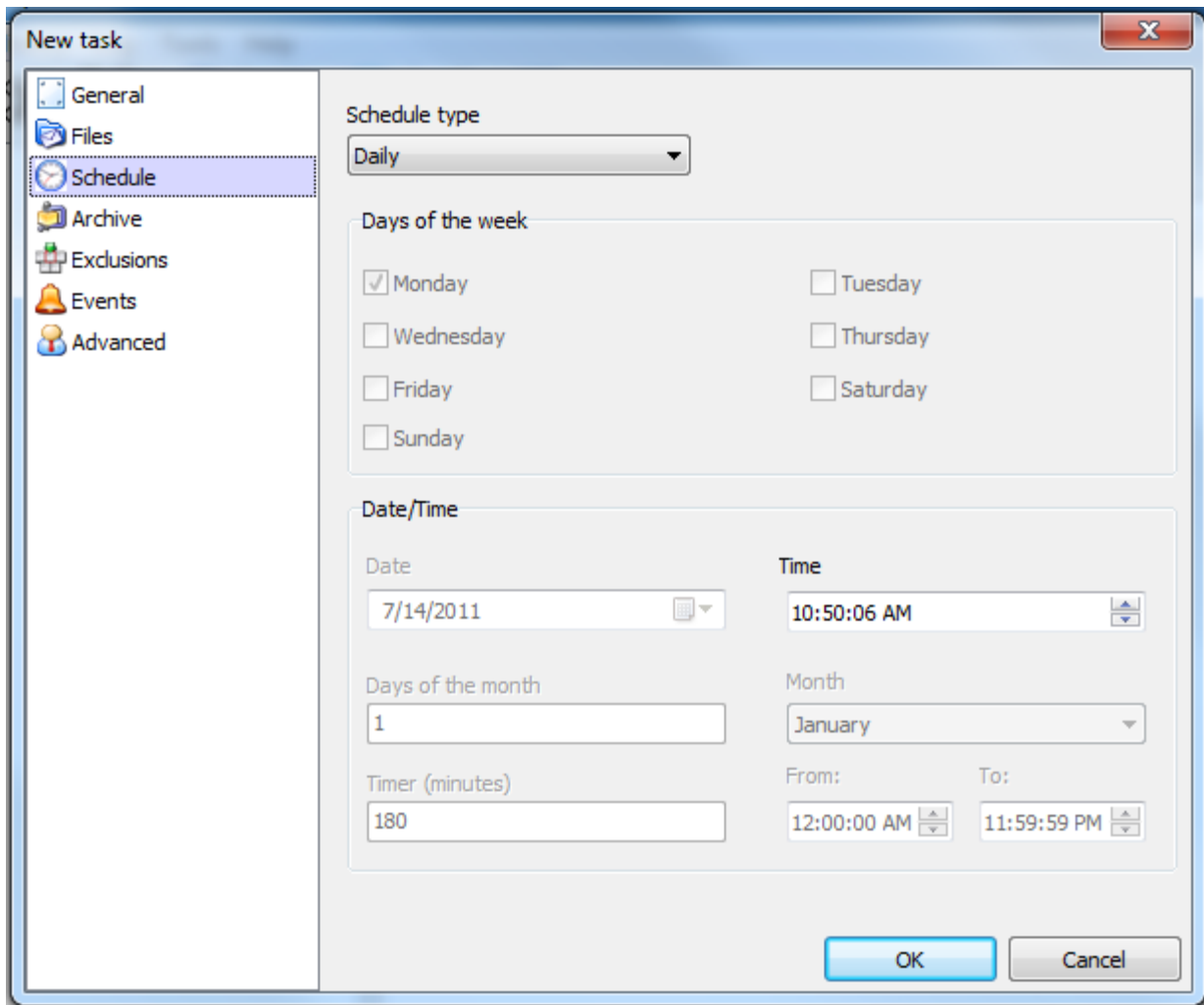


Figure 12 :: New Task Scheduling

The various schedule options are:

Once: The backup will be done once only at the date and time specified in the Date/Time area.

Daily: The backup will be done every day at the time specified in the Date/Time area. In the example above, the backup will be done on Daily at 10:50:06 AM. The backup will be done on all days at the time specified in the Date/Time area.

Weekly: The backup will be done on the days of the week selected.

Monthly: The backup will be done on the days typed into the days of the month box at the time specified in the Date/Time area.

Yearly: The backup will be done on the days typed into the days of the month box, during the month specified, and at the time specified in the Date/Time area.

Timer: The backup will be done repeatedly at intervals specified in the Timer text box in the Date/Time area.

Manually: You will have to run the backup yourself from the main program window.

The backup schedule is the last critical task in setting up a backup task. Your backups will now run on the scheduled times. There other options basically enhance the process, but are not mandatory.

Select **Daily** then choose a suitable time.

Exclusions

We have configured our backup to user profile folders including *My*

Documents folder. These folder contains folders with music, pictures and videos and these may slow down the backup process and the information may not be work related. These are folders such as *My Pictures*, *My Music* and *My Videos* and they should be excluded unless you use them for work purposes. Select Exclusions tab then go to the second pane labeled **Exclude these files** and add the above folders in the user profile.

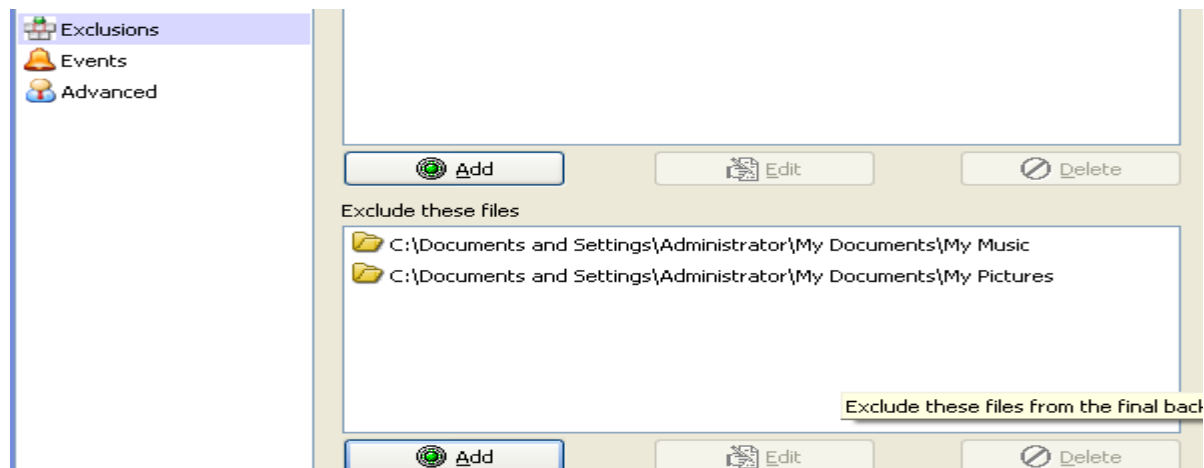
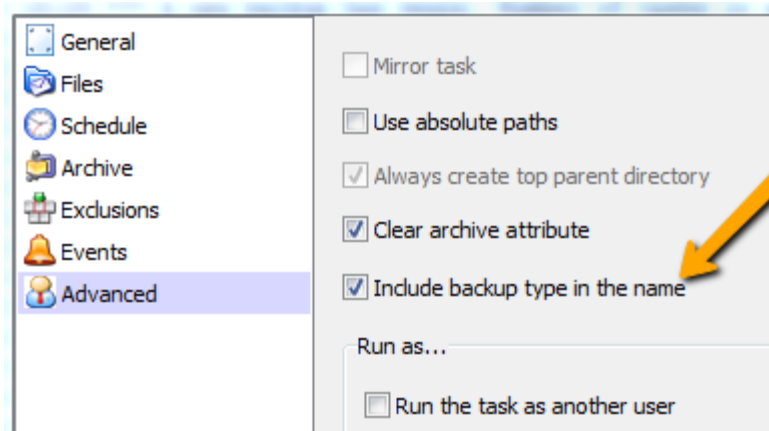


Figure 13 :: Exclusions

Advanced options

This is the last configuration task. We set up our backup type to differential and a full backup every 10th run. To be able to distinguish the differential backups from the full backups go to Advanced then check the option *Include backup type in the name*.

This is useful when you want to restore the information.

Figure 14 :: Advanced

Other options

Archive: This allows for setting up compression and encryption. Compressing files reduces their size and optimizes storage space for the backups. Files must be decompressed so as to be used.

Encryption is basically a way of providing security for your backup files by enforcing a mechanism that only grants you access to the backed up data after you have provided a valid password.

To keep things simple as far as CIP-SSA backup is concerned; we shall worry about establishing a systematic routine of backing up our data. Compressing and encrypting data will be an issue for consideration once that is in place .

Click the **OK** button. Now your backup task is setup and ready.

Recovering your information from backup files

While on your recent working holiday you managed to spill coffee onto your laptop and it's no longer working. Or your computer was stolen and you lost all your precious data. Maybe a virus has cleared out all your data. The good news is you need not worry. Provided you have been running your backups, once you get your new/old computer operational, restoring your data from the backups is a very straight forward affair. In no time you should be up and running like before. Your backup is important as you can use it to restore your data when you need to. This section will take you through the steps of restoring the backups made using Cobian as described in the previous section.

You should have set the backup type to differential. Which means it will create a full backup including all the data in the selected folder, and subsequently the differential backup includes only information that has changed since last full backup. This means to retrieve all your information you need the last full backup, and then you must add the LAST differential backup. Which will then include all data up to the moment of last backup.

All Data = Last Full Backup + Last Differential Backup

Step 1

If you don't remember the destination or target folder on your backup device, open Cobian backup by double-clicking its icon in the system tray. Then, click the "Files" settings in the left-hand pane. Whatever destination you selected when you configured Cobian for the first time, can be seen under the Destination heading.

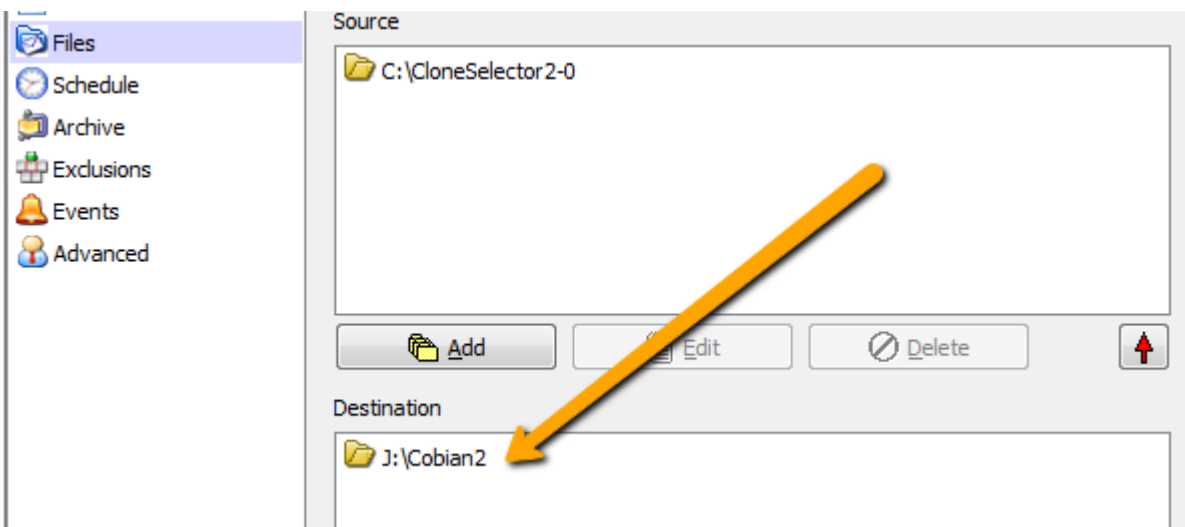


Figure 15 :: Backup Destination

Step 2

Now, open up My Computer or Windows Explorer and go to this folder. You may have to connect your backup device to the computer if it's not already connected. There's a list of all the backed up files. Some of the backups are Full and others are Differential as mentioned in parenthesis along with each backup

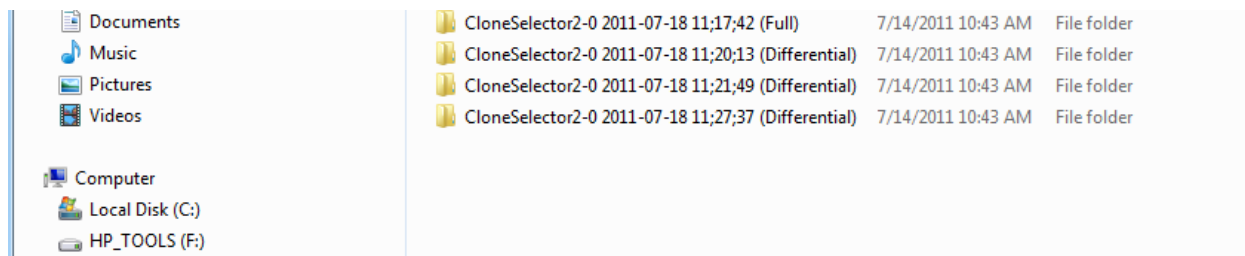


Figure 16 :: Backup Directory Contents

Step 3

Since we backed up using the Differential type of backup, when restoring, we'll have to restore the last Full backup plus the last Differential backup. Since the backup names above include the date and time of backup, we can easily select the two backup files needed for restoring the latest backup.

Step 4

So for instance to restore our CloneSelector2-0 data as shown in figure 16, copy the last full backup and paste it into the location where your previous installation was. Rename the folder appropriately, removing the date/time stamps and backup type information from the name. e.g. **CloneSelector2-0 2011-07-18 11;17;42 (Full)** will be copied to the location where you had the previous CloneSelector2-0 (normally C:\CloneSelector2-0) and renamed to **CloneSelector2-0**.

Then copy the contents of the last differential backup of CloneSelector2-0 i.e. CloneSelector2-0 2011-07-18 11;27;37 (Differential) and paste them into the CloneSelector2-0 folder containing the full backup. We are overwriting the files in the full backup with the files in the newer files in the differential backup. So when prompted to overwrite any file or folder, say **Yes** or **Yes to all**.

Some folders such as *Documents*, *Desktop*, *etc* will already be created even before you start the restoration process since they are operating system folders. For such, simply copy the contents of the respective folder's last full backup from your backup location and paste it into the folder then copy the contents of the folder's last differential backup and paste into the folder. In each case click **Yes** or **Yes to all** to allow overwriting.

Step 5

Repeat the process for every folder of data that you have in your backup.

Step 6

Congratulations, you have successfully restored all your data.