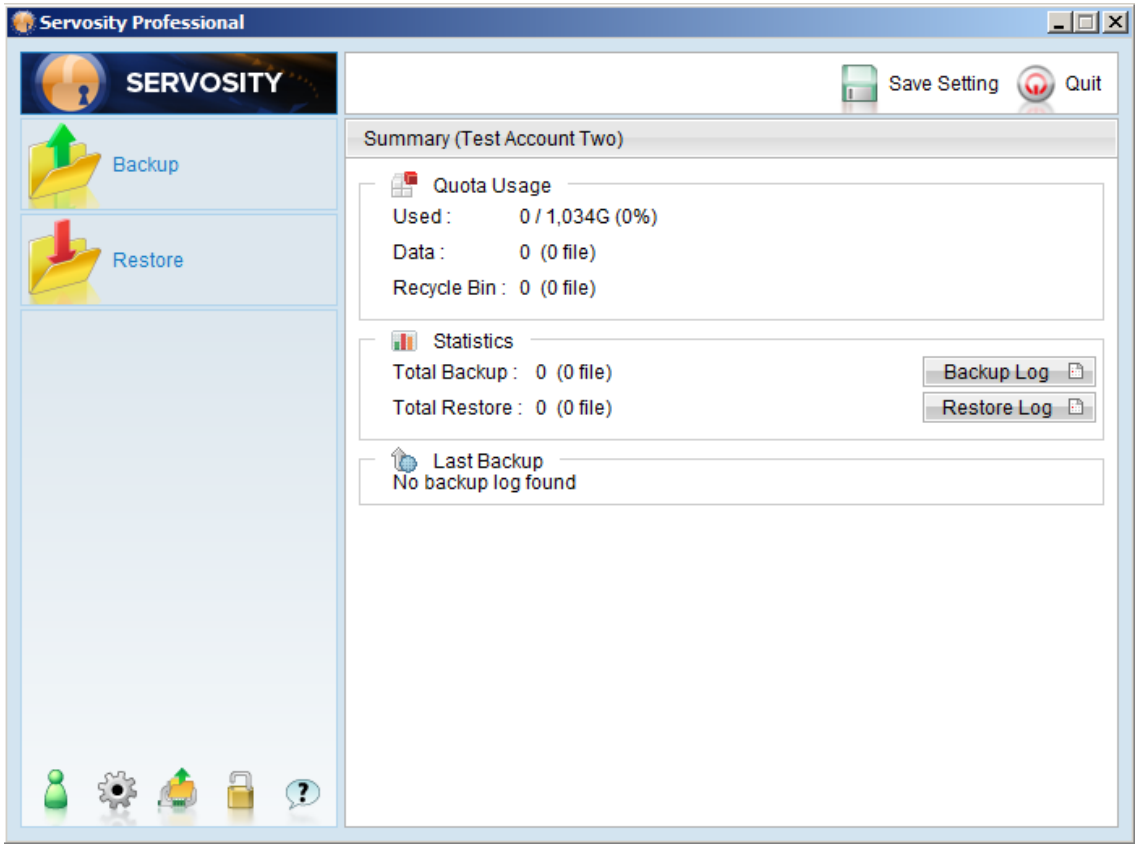
Servosity PRO/STD Backup Setup Features and Functions

Setting up Backup Sets

A backup set contains all of the backup settings required for a backup operation to complete successfully. This section will describe all of the features available within a backup set and explain how you can use each of them to achieve various tasks.

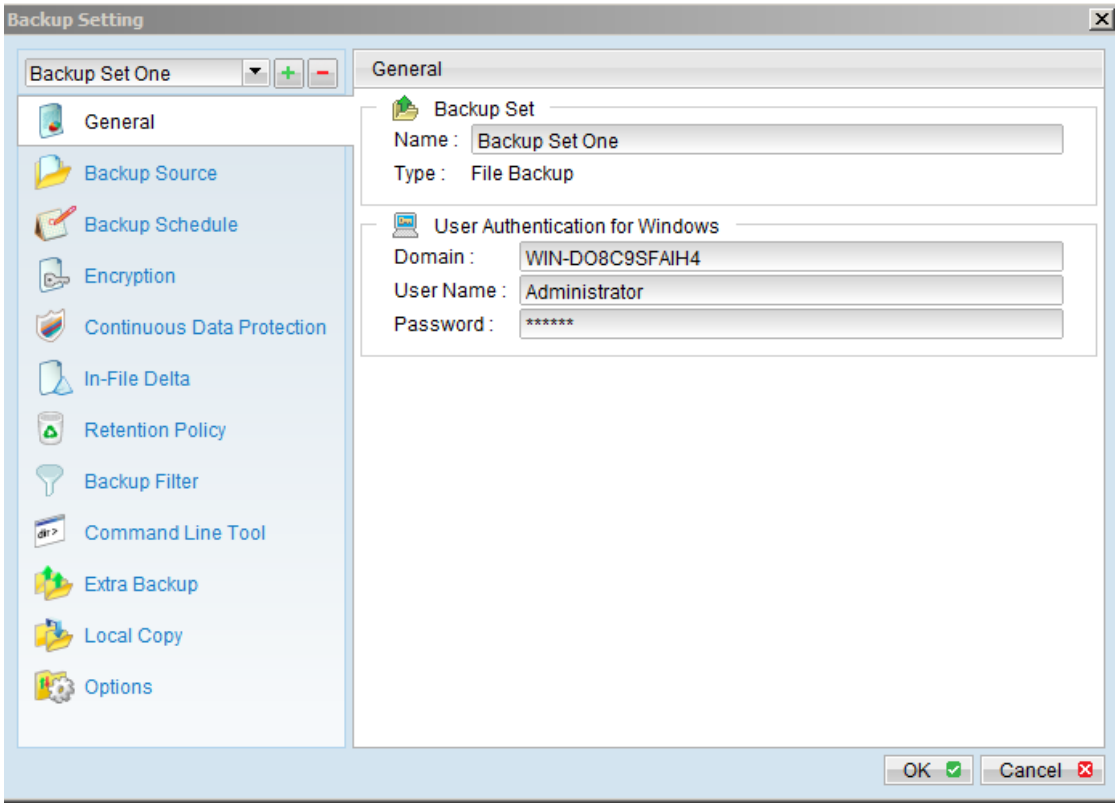
Each backup account can contain multiple backup sets. Each backup set is an individual and independent entity. For example, if you want one directory to be backed up during the day and another directory to be backed up during the night, you can create two backup sets, each with a different backup schedule and backup source, to serve this need.

To start setting up backup sets, click the  button on the lower left-hand corner of the [**Backup Setting**] dialog box.



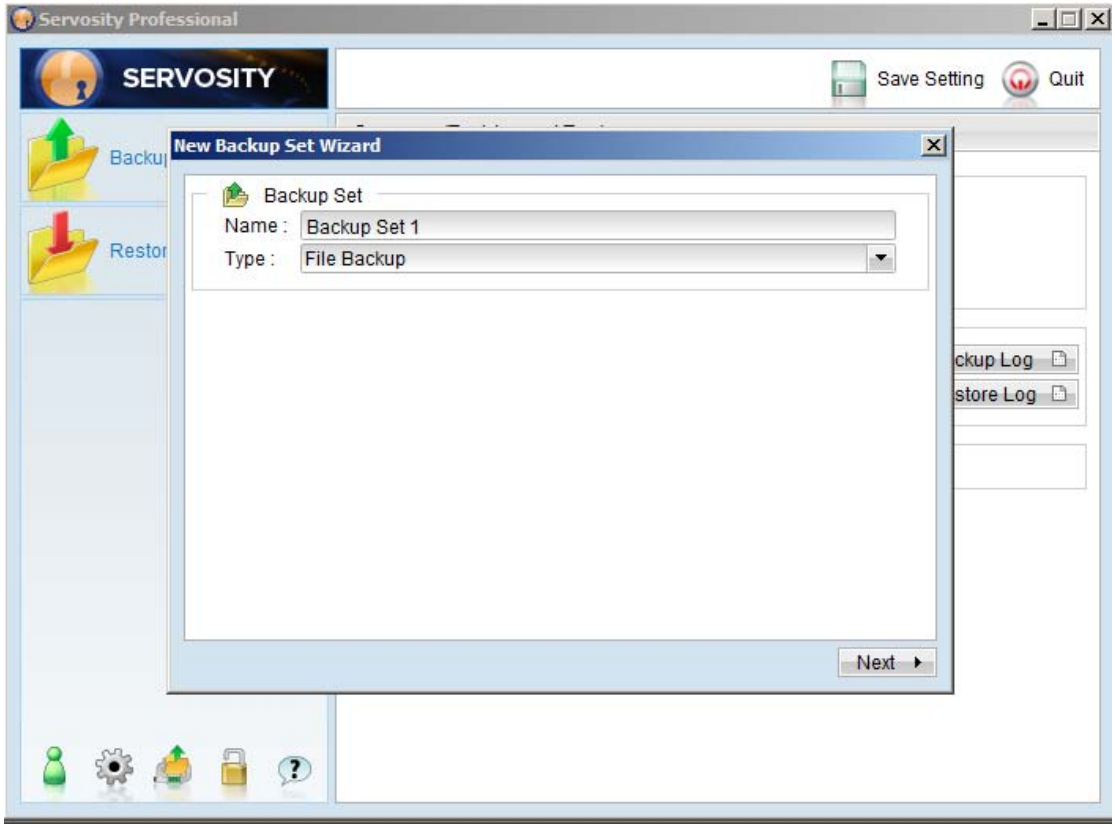
For the purposes of this guide we will create an example “File Backup Set”.

On the upper left-hand side of the backup setting panel, press the  button to create a new backup set



1.1 Backup Set Type

Once you have given your backup set a name you will need to establish the **Backup Set Type**. A backup set can be of one of the following types:



Backup Type	Description
File	Backup set type to backup common files/directories
Lotus Domino Server	Backup set type to backup Lotus Domino
Lotus Notes Client	Backup set type to backup Lotus Notes
MS Exchange Server	Backup set type to backup Microsoft Exchange Server 2000 / 2003 / 2007
MS Exchange Mail Level	Backup set type to backup individual emails, contacts, calendars, tasks etceteras from Microsoft Exchange Server 2000 / 2003 /2007
MS SQL Server	Backup set type to backup Microsoft SQL Server 7.0 / 2000 / 2005
MySQL Server	Backup set type to backup MySQL Server
Oracle Database Server	Backup set type to backup Oracle 8i/9i/10g database
System State	Backup set type to backup Microsoft Window's System State

The Backup Set Type is defined at the backup set creation and cannot be modified. If you want to change the backup set type, you have to create another backup set using the steps outlined previously to establish a new Backup Set.

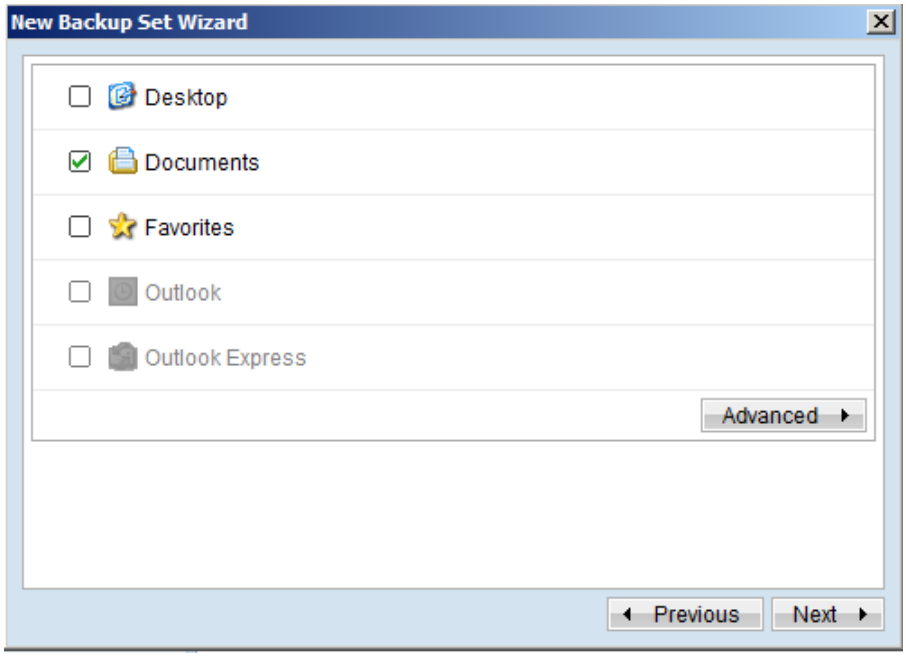
1.2 Backup Source

Next, you will define the Backup Source. A “Backup Source” defines the files and/or directories that are to be included in a Backup Set.

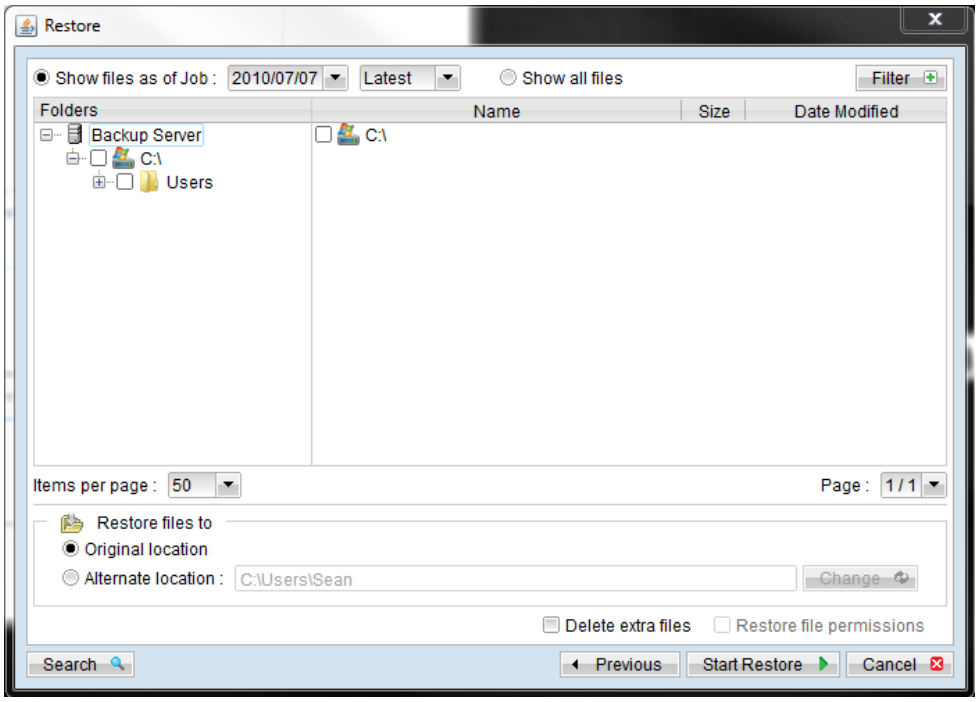
***Please note that for Windows operating systems, if the “Hide protected operating files (Recommended)” setting is enabled for the file explorer, system folders/files will not be shown in the backup source. By selecting the parent folders however, all subfolders (including system folders/files) will be included in the backup set. Thus if you want to exclude system folders (e.g. recycle bin) from the backup, please select the desired folders/files directly rather than selecting the parent folder. Alternatively, you can enter the corresponding system path to the [**Exclude List**] of the backup set using the web interface.

On the first screen of the [**New Backup Set Wizard**] dialog box , you can easily select the following common folders to be backed up:

1. “Desktop” folder
2. “My Documents” folder
3. “Favorites” folder
4. “Outlook” and “Outlook Express” mail store folder

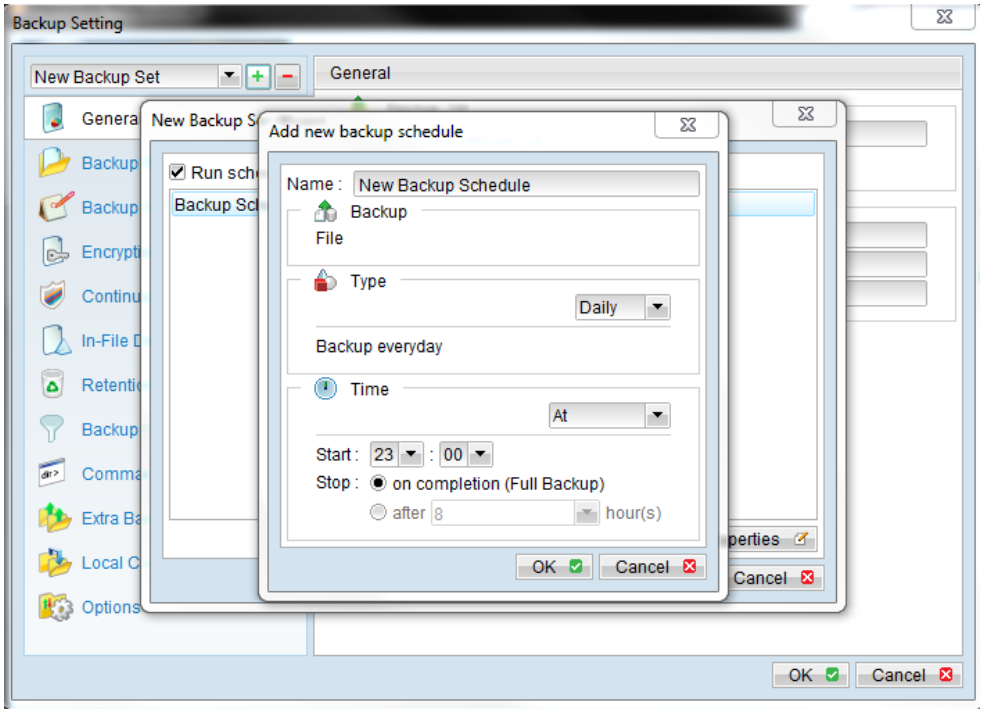


If you click the [**Advanced**] button, you can easily select other common folders to be backed up as well.



1.3 Backup Schedule

A “Backup Schedule” defines the frequency and the time that backups should run automatically. By clicking the [**Add**] button at the bottom of the [**New Backup Set Wizard**] dialog box you can adjust the backup schedule.



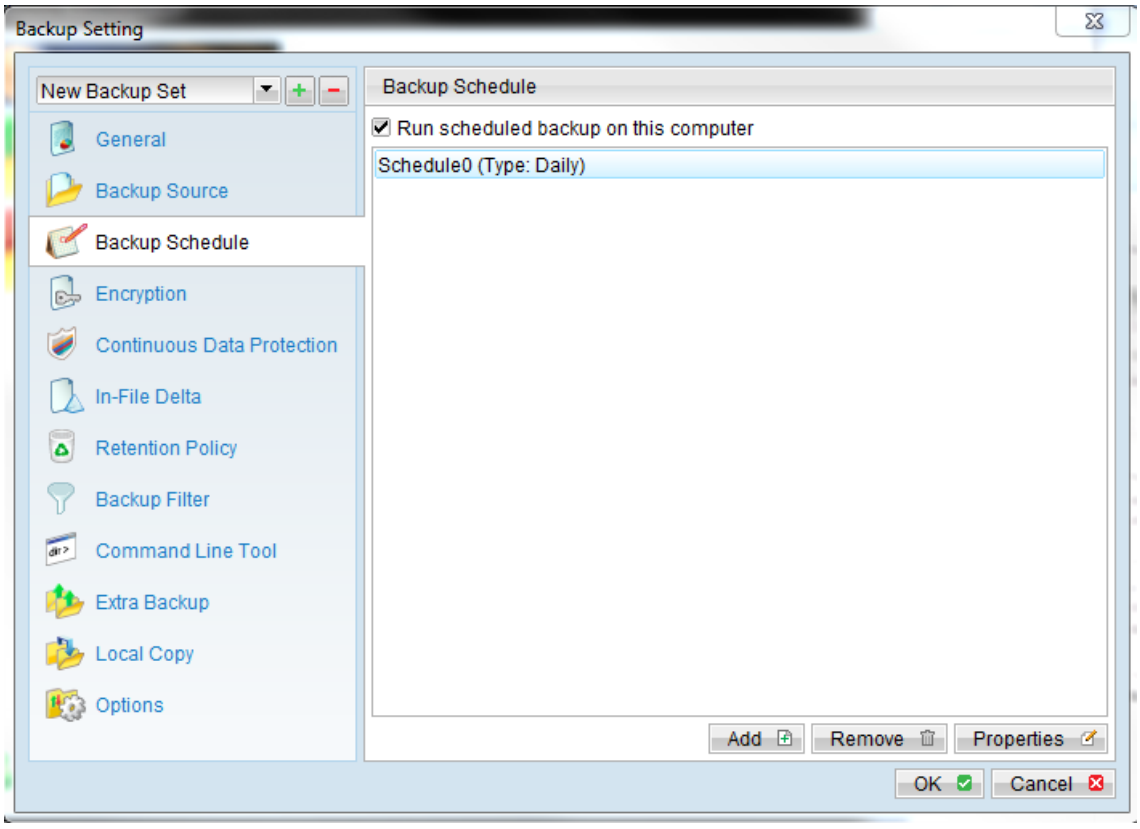
Backup schedules can be created as one of the following types:

Type	Description
Daily	Backup Jobs will run everyday
Weekly	Backup Jobs will run on the specified day(s) of every week
Monthly	Backup Jobs will run on the specified day or on a day with a given criteria (e.g. first weekend, last weekday) of every month
Custom	Backup job will run once on any particular date

For each schedule type above, a backup will run at the scheduled time for a maximum of the duration specified (or until all data is backed up if the [**Stop on backup completion**] option is chosen). If a backup job does not finish within the maximum duration specified, it will be interrupted.

***Please note that you can have more than one schedule within a backup set. For example, you can have a daily backup scheduled to run at 13:00(1:00pm) and another daily backup schedule that runs at 00:00(Midnight). The combination of these schedules effectively creates a backup schedule that runs twice daily at 00:00 and 13:00.

You can change the backup schedules anytime after creating the backup set by clicking the [**Backup Schedule**] node of the left panel on the **[Backup Setting**] dialog box.



1.4 Continuous Data Protection (CDP)

The Servosity PRO/STD Continuous Data Protection (CDP) feature enables files to be backed up automatically at the time when there are changes made to files on the local hard disks. The benefits of using CDP are:

1. **Continuous Incremental Backups:**

    a. All intra-day interim changes are backed up automatically. Even if the computer breaks down completely before the users have had the chance to backup their data. This is especially helpful when the data is normally scheduled to be backed up at the end of the day using the Logout Backup Reminder. This function ensures that all changes within the day have been backed up safely by CDP and no data is lost.

2. **Continuous Data Scanning:**

    a. Occasionally users do not save their data in the folders designated as backup source path folders. This results in data not being backed up even when a backup runs. Since CDP continuously tracks all changes made to files on the local hard disk, all changes made by the users are automatically backed up no matter if the files are located in the backup source paths or not. This makes defining a backup set a much easier task for both administrators and users.

Although CDP is a very helpful feature, it does have some drawbacks:

1. **High Demand for Resources:**

    a. A memory resident program, which continuously tracks file changes to the file system and backs up files automatically in the background consumes both a computer's CPU and memory resources. It can potentially slow down a computer considerably.

        i. An alternative for application servers like Microsoft Exchange Server or Microsoft SQL Server, that do not require CDP features can use the Transaction Log Backup Interval set to a frequency of every 1 minute to mimic a continuous backup strategy.

        ii. This is set by turning off CDP. This can be done by following these simple steps:

            1. Open your computer's [**Start**] menu
            2. Click on the [**Control Panel**] and open the menu
            3. Now open the [Administrative Tools] menu
            4. Click on [Services]
            5. Click on [**Continuous Data Protection (Servosity PRO/STD)**]
            6. Click on [**General**]
            7. Click on [**Startup type**] and set to "manual".

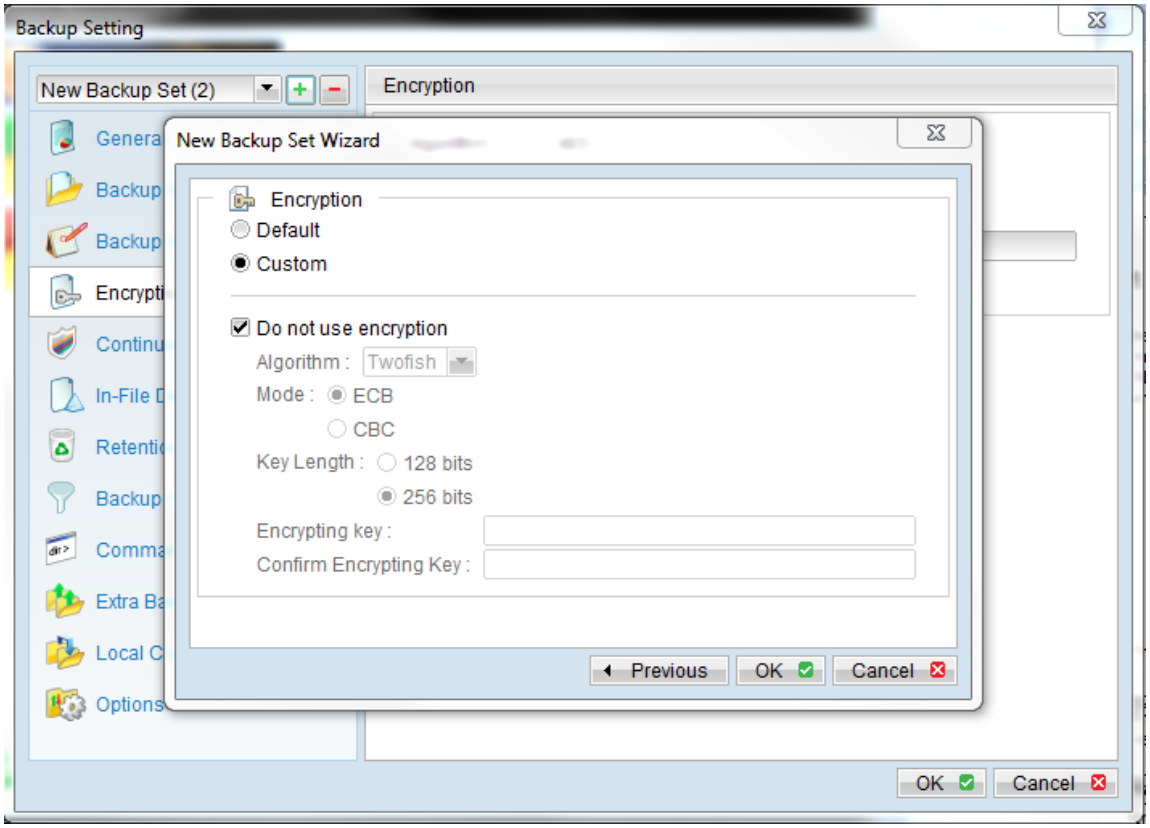
The following table goes into more detail about all of the CDP parameters available within a backup set.

Parameter	Description
Enable Continuous Data Protection (local disk only)	Defines whether CDP is enabled in this backup set. Please note that CDP will only backup files on local hard disks, not files on floppy drives, removable drives and network mapped drives.
Time Mark Interval	Defines the interval of point-in-time views generated by CDP. For example, if this setting is set to “60 minutes”, the point-in-time views selectable under Servosity PRO/STD restore wizard and File Explorer will be “00:00”, “01:00”, “02:00” etc, for each day.
Minimum Update Interval	Defines the minimum interval that repeatedly updated files are backed up. For example, if a file is updated every minute and the [**Minimum Update Interval**] is set to “10 minutes”, CDP backs up this file every 10 minutes instead of every minute. If you want all changes to be backed up instead, please change this setting to “Always”. However, since Servosity PRO/STD keeps only 1 snapshot of file within a single point-in-time view (“Time Mark Interval”), only the last backup file within each point-in-time view is restorable from Servosity PRO/STD; all other interim backup files are overwritten automatically without notice. ***Please note that this applies to all full file backup only, but not for files that are backed up incrementally by in-file delta. To maintain a valid in-file delta chain for incremental delta files, Servosity PRO/STD will not delete incremental delta files automatically. If you are interested in restoring any of these backed up snapshots, you can use the [**Show all files**] view to display all of the interim incremental backup files.
Type	[**Backup file(s) selected by backup sources and filters**] – When this option is selected, CDP will only back up all changed files selected by backup set’s sources and filters settings [**Backup all files**]– When this option is selected, CDP will only back up all changed files. [**Custom**] – When this option is selected, CDP will only back up changed files selected by CDP backup sources and CDP backup filters settings.
Do not backup files defined as system files	If this option is enabled, CDP will exclude the following files from its backup: 1. '[WINDOWS_DIR]' (e.g. C:\WINDOWS*) 2. '[PROGRAM_DIR]' (e.g. C:\Program Files*) 3. '[RECYCLE_BIN_DIR]' (e.g. C:\RECYCLER, D:\$Recycle.Bin) 4. '[ALL_LOCAL_DRIVE]:\Pagefile.sys' (e.g. C:\Pagefile.sys, D:\Pagefile.sys) 5. '[ALL_LOCAL_DRIVE]:\hiberfil.sys' (e.g. C:\hiberfil.sys, D:\hiberfil.sys) 6. '[ALL_LOCAL_DRIVE]:****.tmp' (e.g. C:\xxx\abc.tmp, D:\yyy\abc.tmp) 7. '[ALL_LOCAL_DRIVE]:\System Volume Information' (e.g. C:\System Volume Information, D:\System Volume Information) 8. '[APP_DATA]\Microsoft' 9. '[APP_DATA]\Kaspersky Lab' 10. '[APP_DATA]\Symantec' 11. '[APP_DATA]\Avg7' 12. '[APP_DATA]\Avg8' 13. '[APP_DATA]\McAfee' 14. '[APP_DATA]\McAfee.com' 15. '[APP_DATA]\Sophos' 16. '*\ntuser.dat' 17. '*\Application Data\Mozilla*' 18. '*\Local Settings\Application Data\Microsoft*' 19. '*\Application Data\Macromedia*' 20. '~$*.(doc|dot|ppt|xls|DOC|DOT|PPT|XLS)' 21. '*\Local Settings\(Temp|Temporary Internet Files|History)*' 22. '*\LOCALS~1\(Temp|Tempor~1|History)*' where [APP_DATA] = "C:\Documents and Settings\All Users\Application Data\" (XP) or "C:\ProgramData" (Vista)

	If you are interested in contributing to the maintenance of this by adding your suggestions, please contact us.
Backup Source	This option is only available when the [**Custom**] CDP type is selected. When this option is used, CDP will only backup the files under the paths defined and all other files are ignored.
Backup Filter	This defines whether any file will be backed up by CDP. When the CDP type is [**Backup all files**], it is only possible to exclude files from the CDP backup. The CDP backup filter is similar to the Backup Set Filter; please refer to Backup Filter section for more information.

1.5 Encryption

Before your files are sent to Servosity PRO/STD, all of your files are compressed and encrypted using your choice of encryption algorithms, modes and keys. Once you have set the backup schedule and clicked the [**Next**] button in the [**New Backup Setup Wizard**], you will have the choice to with accept the default encryption setting or choose to customize the encryption settings for your backup set.



The following table explains all of the encryption parameters available within a backup set.

Note:
Encryption settings are set at the Backup Set Creation Time and cannot be modified. You need to create a new backup set if you want to change your encryption settings.

Parameter	Description
Encryption Algorithm	Defines the encryption algorithm used to encrypt your backup files. There are three encryption algorithms available: [AES] Advanced Encryption Standard algorithm [DESede] Triple DES algorithm [Twofish] Twofish algorithm We recommend the use of AES as your preferred algorithm since it is the typical encryption standard for most commercial uses. Please refer to references on Cryptography for more information about encryption algorithms.
Encryption Mode	Defines the encryption mode used to encrypt your backup files. There are two encryption modes available: [ECB] Electronic Cook Book Mode [CBC] Cipher Block Chaining Mode We recommend the use of CBC as it offers better security. Please refer to references on Cryptography for more information about encryption modes.
Encrypting Key	This is the key used to encrypt all files within a backup set. **Please write it down on paper and keep it in a safe place. If the key is lost, you will not be able to recover your files from the encrypted backup files.**

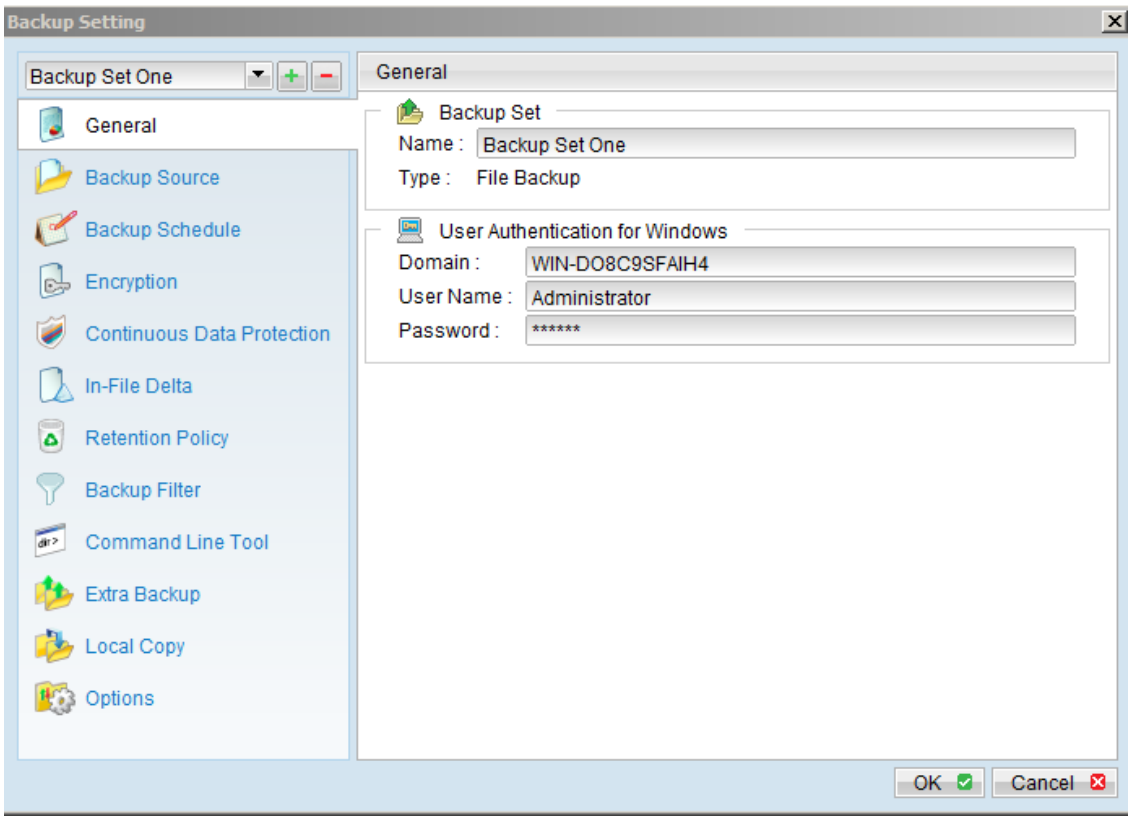
If you are not familiar with cryptography, it is recommended to use the [**Default**] encryption settings. By selecting **[Default]**, the encryption key will be your login password.

1.6 Mapped Network Drives

If you need to backup a mapped network drive on a Windows operating systems (This option is only available for Windows NT/2000/XP/2003/Vista), you must enter your Window's domain, username and password into the [**User Authentication for Windows**] section as shown below. It is required because scheduled backups will always run under the context of a Window's "Local System" account which does not have the privileges required to access network resources by default. Servosity PRO/STD needs to collect your Windows username, password and domain name to authenticate itself to the windows domain controller. This allows it to acquire the required access privileges to the network files so they can be backed up. If you don't supply a username and password, Servosity PRO/STD will have problems accessing the network resources needed to complete its scheduled backup Jobs.

If you need to back up a mapped network drive in a scheduled backup, please follow these steps:

i. Select the backup set from the drop down list at the top of the left pane of the [**Backup Setting**] dialog box. Click the [**General**] tab. In the middle of the screen you will see the [**User Authentication for Windows**] section.

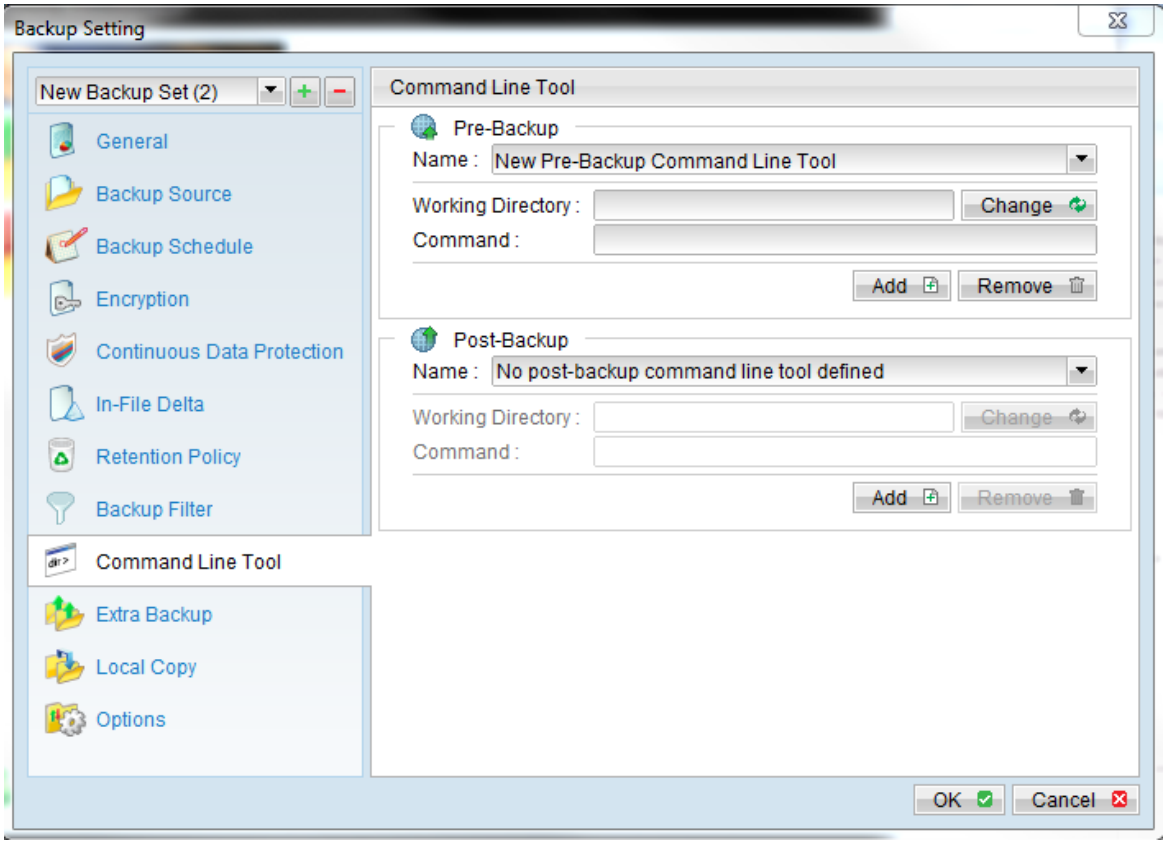


ii. Enter your Windows domain, username and password into the right panel and press [**OK**]

iii. Press the [**OK**] button to save.

The steps above apply only to computers running in a Windows domain. If you don't have a windows domain with your network and you are using a workgroup or using a NetWare server, please use the "net use" command to authenticate the running backup process against the computer hosting the mapped drive. Otherwise, you will get "Access Denied" error from the backup report.

For example, if you want to backup \\SERVER\SHARE that is located on a NetWare server (or another computer in a windows workgroup) and you are getting a "Network drive is not accessible" error message, please try adding the following command as a [**Pre-backup command**] under the [**Command Line Tool**] tab of the [**Backup Setting**] dialog box.



net use \\SERVER\SHARE [PASSWORD] /USER:[DOMAIN | MACHINE_NAME]\[USERNAME]

Click the [Add] button and enter one of the following commands directly into the Command Line of the New Pre-Backup Command:

1. `net use \\Netware/Data password /USER:peter`
2. `net use \\WorkgroupCOmputer1\Data password/USER:WorkgroupCOmputer1\peter`

This will authenticate the current process with the NetWare server (or another computer in a windows workgroup) and the backup will then run correctly.

1.7 Backup Filter

A “Backup Filter” defines the file selection rules that allow the user to easily include or exclude files into or from the backup set by applying user defined criteria(s) to the file names or directory names.

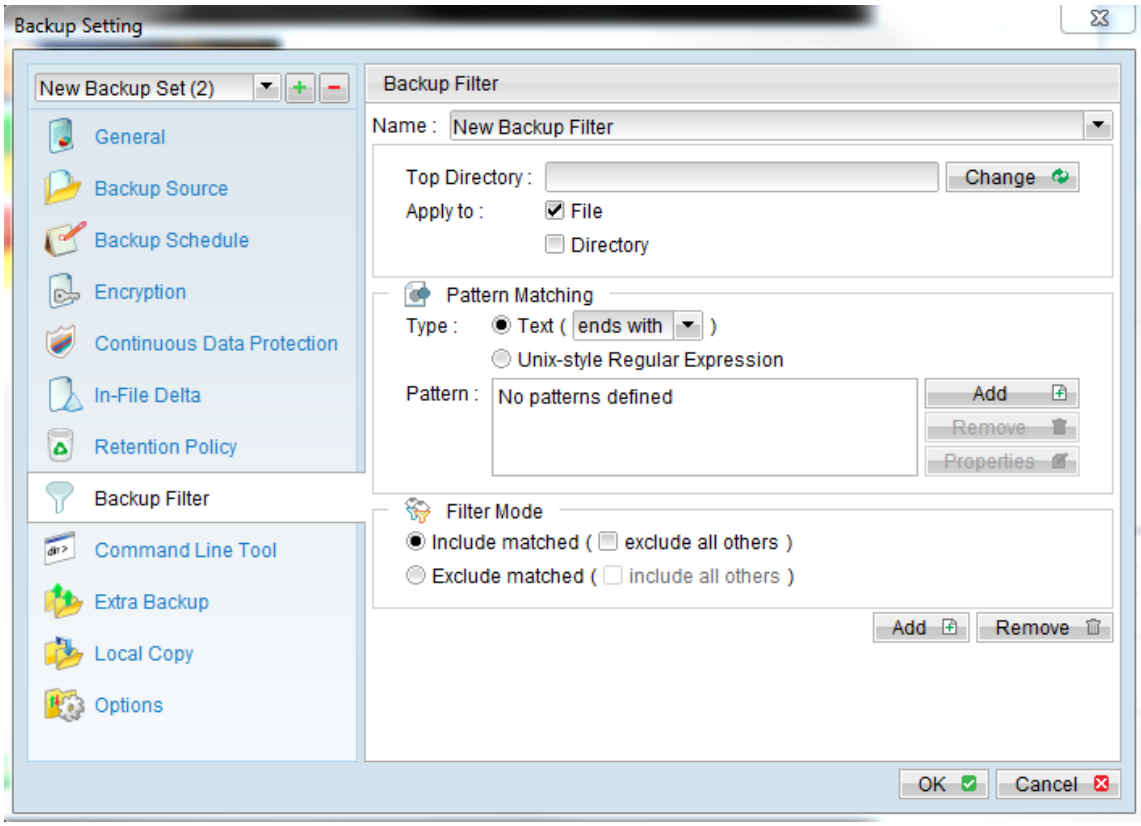
There are some basic rules regarding backup filters:

i. Filters are checked in order of creation. Once inclusion or exclusion has been identified, the remaining filters won't be checked.

ii. Inclusions or Exclusions made by filters always take precedence over backup source selections.

iii. If all filters do not apply to a particular file, then the file is checked for inclusion or exclusion backup source selections

To add a new filter, press the [**Add**] button at the bottom right-hand side of the Backup Filter panel.



The table below explains in more detail the filter options available to be applied:

Key	Description
Name	The name of a filter
Top Directory	The top directory to which this filter is applied. Filtering rules will be applied to all files and/or directories under this directory.
Apply To	Defines whether to apply the filtering rule to files and/or directories
Pattern Matching	Defines the filtering rules of to be applied. A filtering rule can be of one of the following types: [Starts With] Include/Exclude all files/directories with name starting with a certain pattern. For example: You can use B* to match all files with name starting with a 'B' character [Contains] Include/Exclude all files/directories with name containing a certain pattern. For example: You can use *B* to match all files with name containing with a 'B' character [Ends With] Include/Exclude all files/directories with name ending with a certain pattern. For example: You can use *.doc to match all files with name ending with '.doc' (all Word documents) [Regular Expression] Include/Exclude all files/directories with name matching a regular expression. To add a new pattern, press the [**Add**] button in the [**Pattern Matching**] area.
Filter Mode	Defines whether you want to include or exclude matched files into/from the backup set. Also, for those unmatched files, you can choose to exclude (if include filter type) or include (if exclude filter type) them into/from the backup set.

Below are some examples of filtering options that can be employed when creating a new backup set.

Example 1:
If you want to backup only Word, Excel and PowerPoint documents in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows.

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.doc, *.xls, *.ppt
Filter Mode = Include
Exclude all others = True

Example 2:
If you want to backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Applications, you should setup your backup filter as follows.

Top Directory = C:\Applications
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.exe,*.dll, *.tmp
Filter Mode = Exclude
Include all others = True

Example 3:
If you have made your selection of files (all under C:\) from the backup source setting but you want exclude all images (e.g. *.jpg and *.gif) from your selection, you should setup your backup filter as follows.

Top Directory	= C:\
Apply To	= File (true)
Matching Type	= End With
Matching Patterns	= *.jpg, *.gif
Filter Mode	= Exclude
Include all others	= false

Please note that the [Include all others] setting is not enabled because you don't want to include all other files (NOT *.jpg, *.gif) under C:\ into the backup set.

Example 4: (advanced)

If you want to include everything, except the "log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows.

Top Directory	= C:\Applications
Apply To	= Directory (true)
Matching Type	= Regular Expression
Matching Patterns	= ^log$
Filter Mode	= Exclude
Include all others	= True

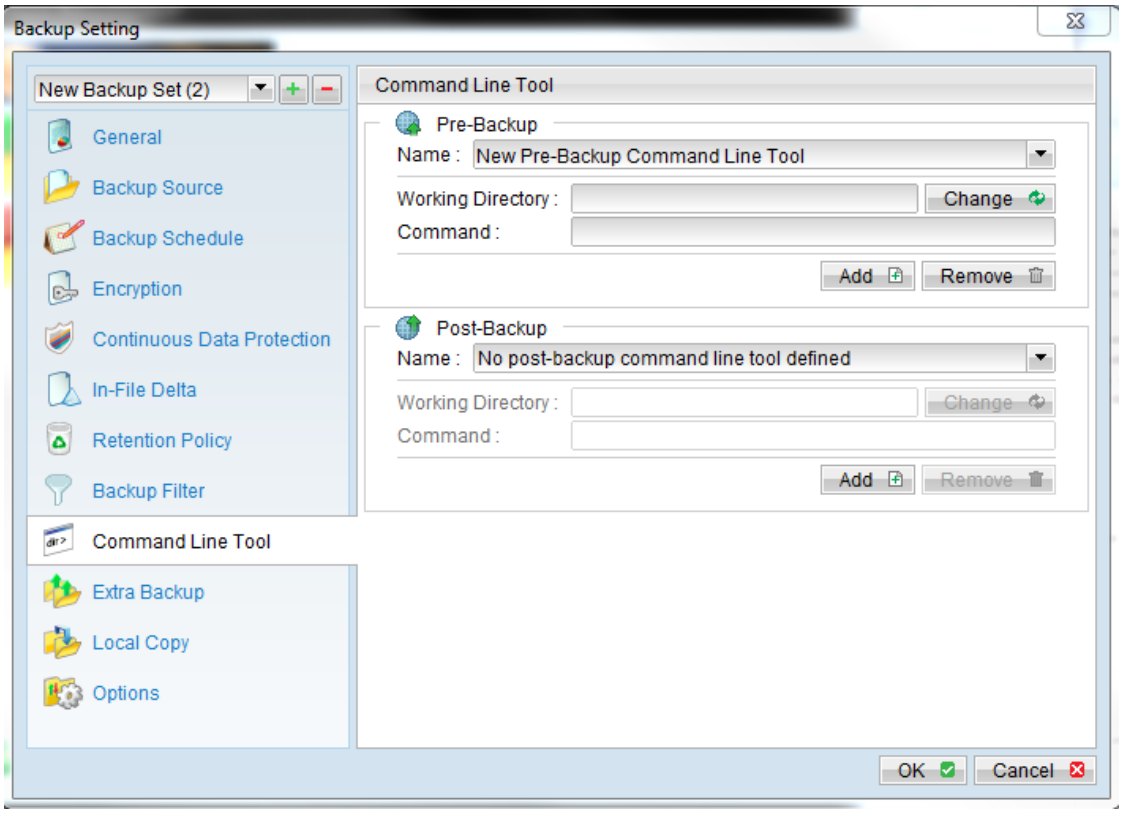
Example 5: (advanced)

If you want to include all directories named "log" from the backup set files with file name starting with "B" and ending with "*.doc" under C:\My Documents into the backup set, you can use a regular expression of "^B.*\.doc$" to do your selection. The filter backup can then be setup as follows.

Top Directory	= C:\My Documents
Apply To	= File (true)
Matching Type	= Regular Expression
Matching Patterns	= ^B.*\.doc$
Filter Mode	= Include
Exclude all others	= True

1.8 Pre/Post-Backup Command

The [**Command Line Tool**] feature has two major components, the [**Pre-Backup**] command and the [**Post-Backup**] command. You can use the [**Pre-Backup**] or [**Post-Backup**] commands to run any native OS (operating system) commands before or after running a backup job.



Both the [**Pre-Backup**] and **[Post-Backup**] commands are comprised of the following parameters:

Key	Description
Name	Name of the Command
Command	The command to be run (e.g. C:\My Documents\Application.exe or C:\My Documents\BatchJob.bat)
Working Directory	The directory in which this command will run

The type of backup set affects the time at which the [**Pre-Backup**] and [**Post-Backup**] commands will run. The following table outlines when these commands will run in different types of backup sets.

Backup Set Type	When Pre-Backup Commands run?	When Post-Commands run?
File	Before uploading backup files	After uploading all backup files
Non-File Backup Sets (e.g. Microsoft SQL Server)	Before spooling backup files to temporary directory	After spooling backup files to temporary directory (i.e. before the first backup file is uploaded)

Note: ***You should never backup an application while it is running as this can result in inconsistent and unusable files getting backed up. In order to avoid this problem you will need to use the “Volume Shadow Copy” feature found in the [**Options**] tab, if you’re running Windows XP/2003/Vista. Another option is to make use of the Pre-Backup Command feature to shut down your application before running a backup job and use the Post-Backup Command feature to restart your application after the backup job has completed.

For Example

You want to stop Microsoft Outlook using the Pre-Backup Command and restart it after the backup using the Post-Backup Command. In order to accomplish this you need to create the following text files and assign the files to Pre-Backup and Post-Backup Commands.

1. Pre-Command: Create a text file named “OutlookClose.vbs” using notepad with the following two lines:

```
Set objOLK = createObject(“Outlook.Application”)
```

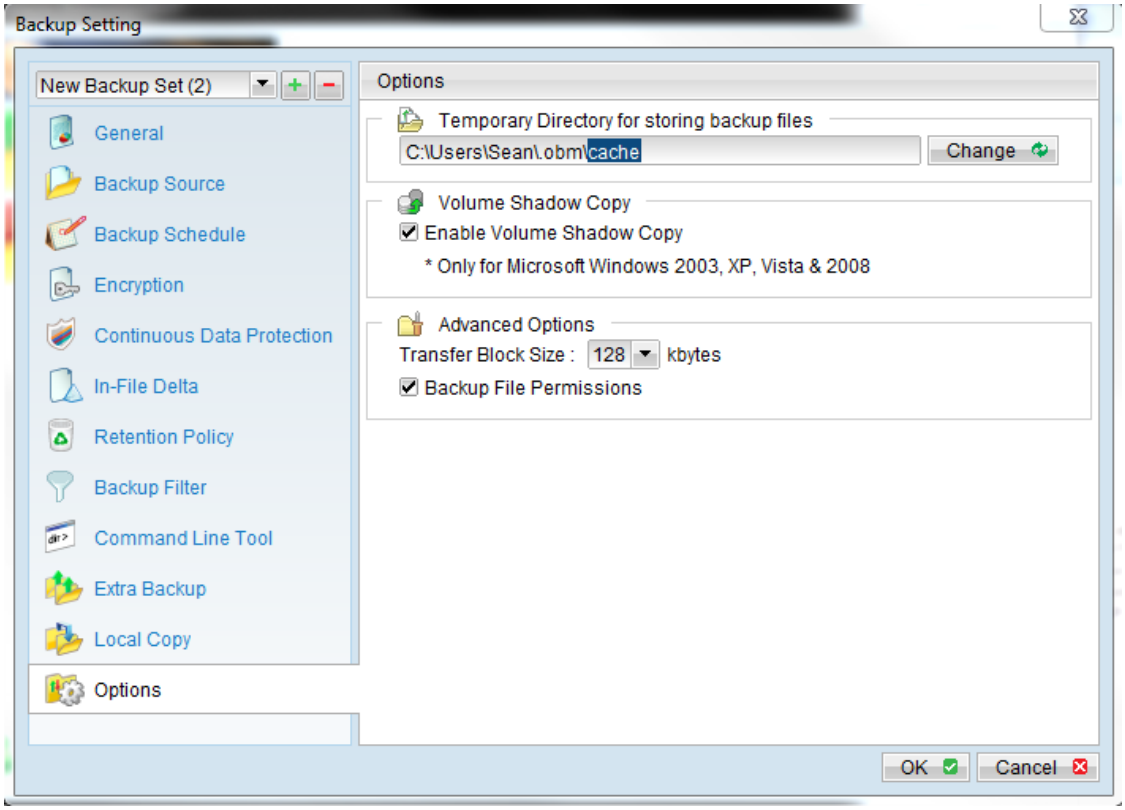
```
objOLK.quit
```

2. Post-Command: Create a text file named “OutlookStart.bat” using notepad with the following line:

```
“C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE”
```

1.9 Temporary directory

If you are running a file backup job with in-file delta enabled or a database type backup job, Servosity PRO/STD will generate temporary files and the directories that will be used to store these files. These directories are defined by accessing the [**Options**] menu and selecting the [**Change**] option in the “Temporary Directory for storing backup files” section of the menu. Please set this to a location that has enough free space to avoid resource problems.



You can set the [**Temporary directory for storing backup files**] to a mapped network drive. If you choose to do this, please use a UNC path (e.g. \\SERVER\SHARE). You will also need to access the [**General]** menu and configure the [**User Authentication for Windows**] setting.

1.10 Transfer Block Size

Transfer block size defines the block size, or the amount of data, that Servosity PRO/STD will use to transfer your backup data. Generally, backup jobs using a larger block size will have better performance, because of the smaller number of connections involved.

However, some firewalls or proxy servers may block out-going network traffic (HTTP/HTTPS POST method) with large block sizes for security reasons. If you are in a network with this type of restriction, please lower the transfer size value and try again.

To change the transfer block size of any backup set, please select the [**Options**] menu on the left panel Backup Setting dialog box. Then select the [**Transfer Block Size**] option under [**Advanced Options**] section of the menu. After you have made your changes, just press the [**OK**] button to save your changes.

1.11 Microsoft's Volume Shadow Copy Service (VSS)

Microsoft Volume Shadow Copy Service (VSS) allows you to backup files that are exclusively opened. Without VSS, you will get the error message "The process cannot access the file because another process has locked a portion of the file," if you try to backup a file that is exclusively opened (e.g. Outlook PST file).

Please note that VSS is only available on Windows XP / 2003 / Vista and you must have administrative privileges to start the VSS service on a computer. It is also important to note that VSS will only work if at least one of your partitions is formatted using NTFS.

If you are running Windows 2003, please install the Windows 2003 VSS hot fix available in http://support.microsoft.com/default.aspx?scid=kb;en-us;887827 before running VSS.

If you are running into problems with VSS running on Windows XP / 2003, Microsoft's recommendation is to try re-registering the Volume Shadow Copy Service again. Simply run the script **[OBM Home]\bin\RegisterVSS.bat** to do so.

For more information, please take a look at the following page for a technical introduction to Volume Shadow Copy Services (VSS):

http://technet2.microsoft.com/windowsserver/en/library/2b0d2457-b7d8-42c3-b6c9-59c145b7765f1033.mspx

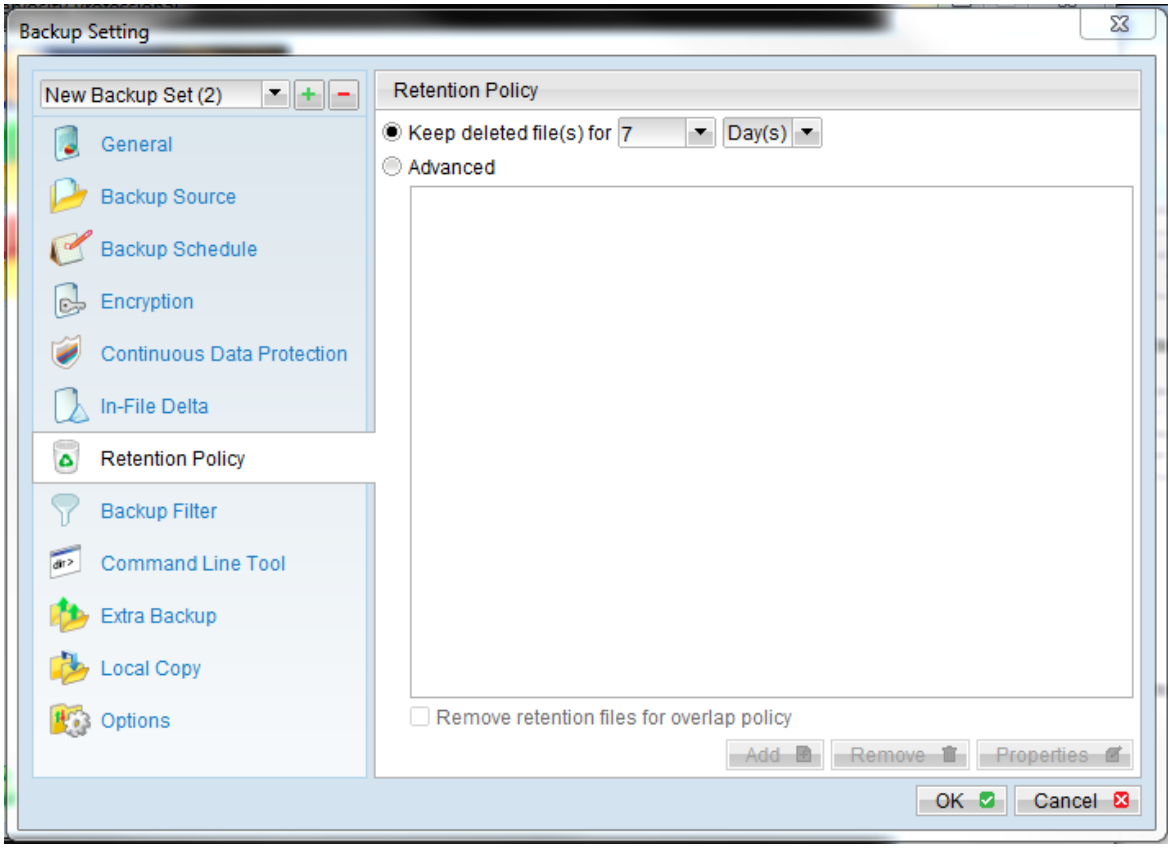
1.12 Retention Policy

The Retention Policy setting defines how long files inside the “Retention Area” will be kept on the backup server before they are deleted automatically. During a backup, if Servosity PRO/STD finds that you have deleted a file, or updated a file on your computer, it will put the corresponding deleted, or updated file already backed up on the server into a retention area.

The Retention Policy will only affect “retained” files (i.e. files that have already been deleted or updated on your computer and thus are moved to the retention area of the backup server). For those files that have not been updated, the backup of these files is kept in the data area on the backup server and won’t be affected by the setting of the Retention Policy. The backup of unchanged files will stay on the backup server forever until the original files are removed (or updated) from your computer.

Standard Retention Policy

The standard retention policy allows you to delete retained files automatically after a user defined number of days or after a user defined number of backup Jobs. To change the retention policy setting of any backup set, please select the [**Retention Policy**] menu on the left-hand panel of the Backup Setting dialog box. You can then make changes to your retention policy here. After you have made your changes, just press the [**OK**] button to save.



Advanced Retention Policy

The [**Advanced**] section of the retention policy allows you to configure a more flexible retention policy. You can add advanced policies by clicking the [**Advanced**] radial button and then clicking the [**Add**] button on the bottom of the Retention Policy window. This function allows you to keep a set of snapshots of all backup files based on the time of the backup Jobs. For example, you can configure the advanced retention policy to keep the following sets of backup files to mimic the retention policy of the old days when you were still doing tape rotations:

- All files available within the last 7 days
- All files available on the last 4 Saturdays within the last 28 days
- All files available on the 1st day of each month within the last 3 months
- All files available on the 1st day of each quarter within the last 12 months
- All files available on the 1st day of each year within the last 7 years

To do so, you need to setup your advanced retention policy as follows:

- Type = Daily; Number of copy to keep = 7
- Type = Weekly; Frequency = Saturday; Number of copy to keep = 4
- Type = Monthly; Frequency = Day 1; Number of copy to keep = 3
- Type = Quarterly; Frequency = Day 1 of Jan, Apr, Jul, Oct; Number of copy to keep = 4
- Type = Yearly; Frequency = Date 01-01; Number of copy to keep = 7

Assuming today is 17-Jan-2006, if the [**Remove retention files for overlap policy**] is NOT enabled, a total of 22 snapshots (provided you have run backups daily for more than 7 years) will be kept on the server accordingly, i.e.:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2006	14-Jan-2006	01-Jan-2006	01-Jan-2006	01-Jan-2006
15-Jan-2006	07-Jan-2006	01-Dec-2005	01-Oct-2005	01-Jan-2005
14-Jan-2006	31-Dec-2005	01-Nov-2005	01-Jul-2005	01-Jan-2004
13-Jan-2006	24-Dec-2005		01-Apr-2005	01-Jan-2003
12-Jan-2006				01-Jan-2002
11-Jan-2006				01-Jan-2001
10-Jan-2006				01-Jan-2000

If the [**Remove retention files for overlap policy**] is enabled, only the following snapshots are kept:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2006	14-Jan-2006	~~01 Jan 2006~~	~~01 Jan 2006~~	01-Jan-2006
15-Jan-2006	07-Jan-2006	~~01 Dec 2005~~	~~01 Oct 2005~~	01-Jan-2005
~~14-Jan-2006~~	~~31-Dec-2005~~	~~01-Nov-2005~~	~~01-Jul-2005~~	01-Jan-2004
~~13 Jan 2006~~	~~24 Dec 2005~~		~~01 Apr 2005~~	01-Jan-2003
~~12-Jan-2006~~				01-Jan-2002
~~11 Jan 2006~~				01-Jan-2001
~~10 Jan 2006~~				01-Jan-2000

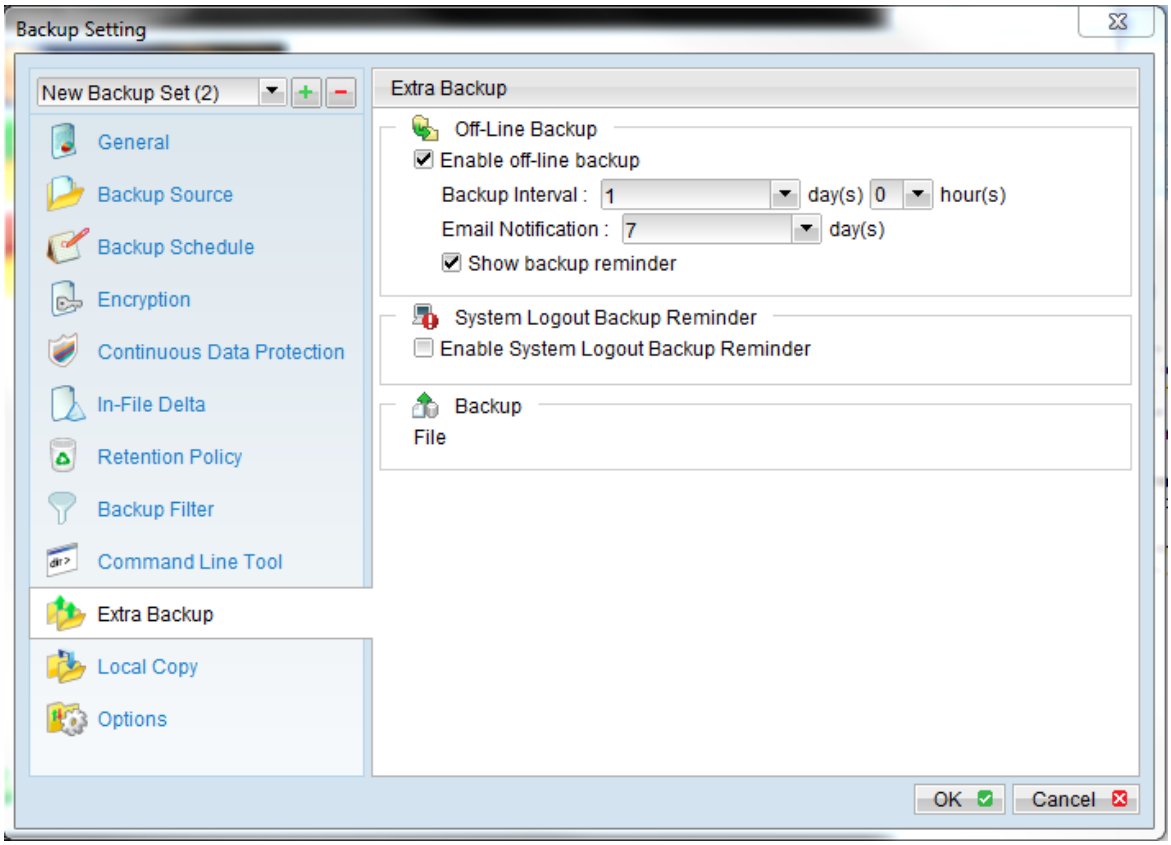
The weekly policy overrides the daily policy so the snapshots of 10-Jan-2006, 11-Jan-2006, 12-Jan-2006, 13-Jan-2006 and 14-Jan-2006 are removed. The monthly policy overrides the weekly policy so the snapshots of 24-Dec-2005 and 31-Dec-2005 are removed. The same applies to the monthly, quarterly and yearly policy giving a total of 11 snapshots.

1.13 Extra Backup (Off-Line backup, Logout Reminder)

Off-line backup is specifically designed for notebook users who are off-line most of the time and cannot rely on the backup schedule to backup their files regularly. The "Backup Interval" allows notebook users to specify the interval that they would like their data to be backed up. When the machine is online and this interval has elapsed, the backup will run automatically. If the [**Show Backup Reminder**] is enabled, a popup message box will ask the user to confirm starting the backup.

The [**Email Notification**] setting is the number of days since the last backup that triggers the backup server to send email notifications to the client to remind him or her to run an off-line backup.

When the [**System Logout Backup Reminder**] setting is enabled, a popup message box will ask the user to start a backup before logging out / shutting down Windows.



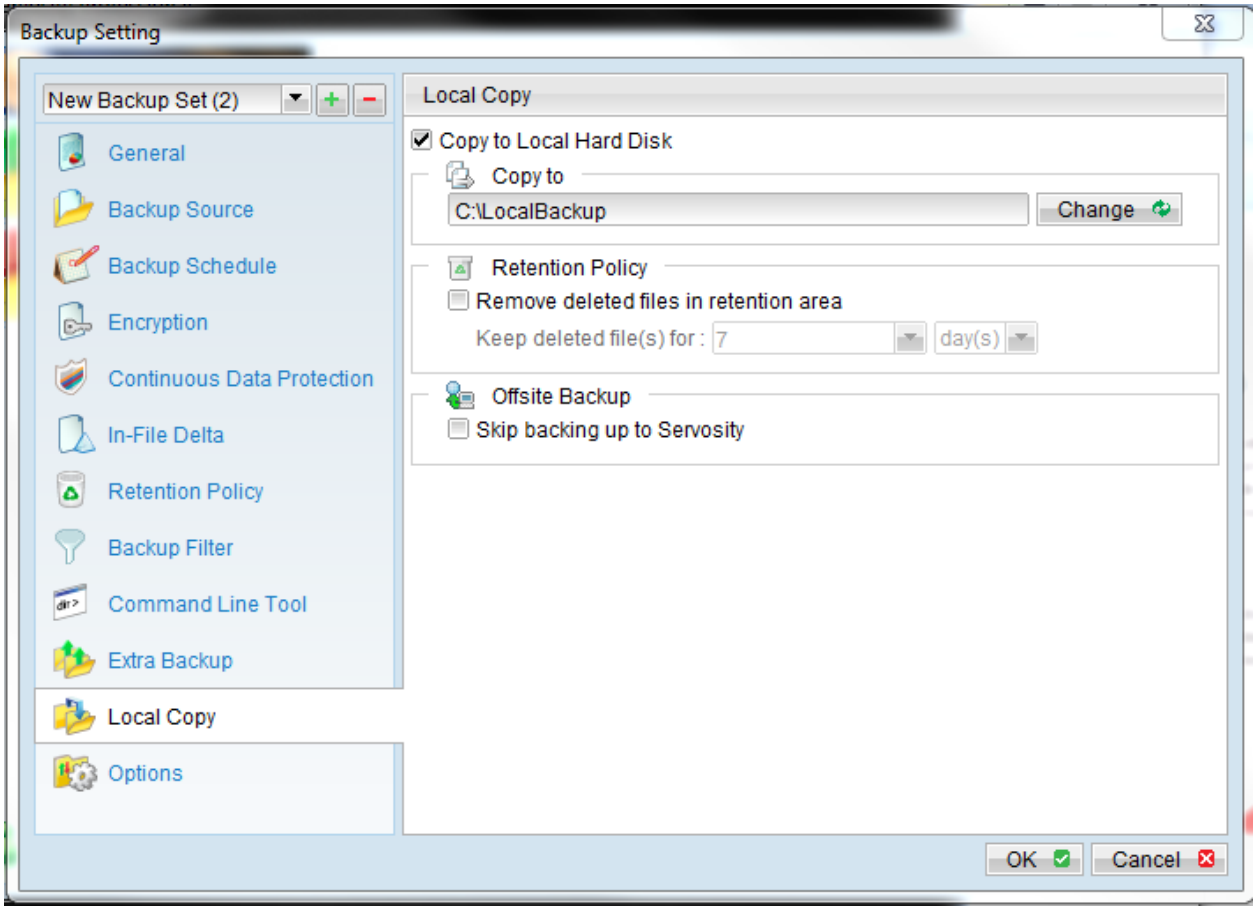
1.14 In-File Delta

Please refer to the in-file delta section for more information on this topic.

1.15 Local Copy

Servosity PRO/STD gives you the option to save an extra copy of your backup data on the local hard disk (in addition to a copy of backup data stored on the backup server) to minimize file-restoration time and/or to provide an extra safety precaution. Once you select the [Local Copy] menu in the Backup Setting dialog box, you will have the ability to enable the local copy function.

By clicking the [Copy to Local Hard Disk] option you can choose the location to copy the files to, you can set the retention policy for those files, and you can also choose to skip backing up your files to Servosity all together and just copy your files to the local backup.



If you want to make a local copy to a directory located on a NetWare server (or another computer is a windows workgroup) and you are getting "Network drive is not accessible" error message, please try adding the following command as a [**Pre-backup command**]

```
netuse\\SERVER\SHARE[PASSWORD]/USER:[DOMAIN|MACHINE_NAME\[USERNAME]
```

E.g.

```
C:\>netuse\\Netware\Data password/USER:peter
C:\>netuse\\WorkgroupComputer1\Datapassword/USER:WorkgroupComputer1\peter
```

This will authenticate the current process with the NetWare server (or another computer is a windows workgroup). Backup will then be allowed to run correctly.

How to restore "Local Copy" files

"Local Copy" files are stored in the [**Copy to**] directory (under the [**Local Copy**] setting). The following steps will walk you through how to restore your backup files:

i. Press the  button in the lower left-hand side of the main page of Servosity PRO/STD dialog box.

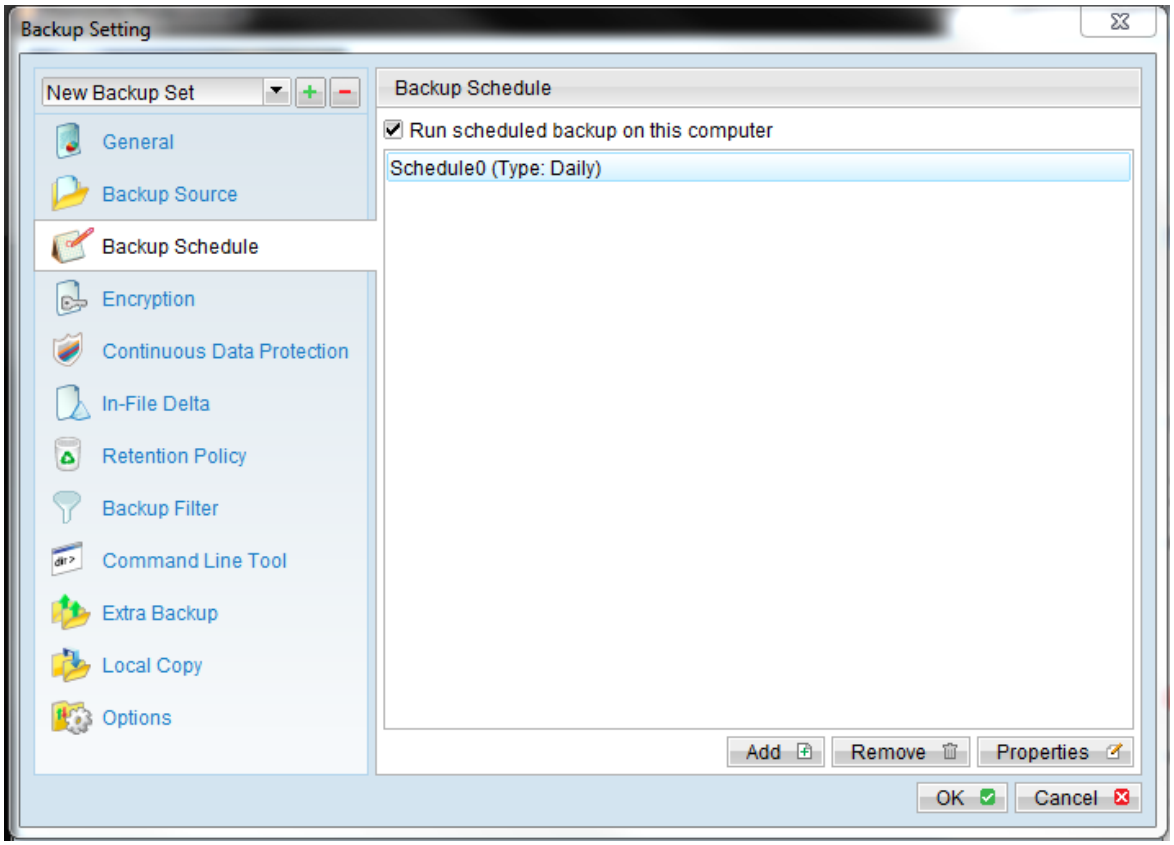
ii. Select the required [**Backup Set**] from the list and press [**Next**] to proceed.

iii. Fill in the [**Source Directory**] (directory where the "Local Copy" files are stored) and [**Destination Directory**] (directory to where you want the "Local Copy" files to be restored)

iv. Click [**Start Decrypt**]. When it finishes you can see something similar to the following on the screen:

1.16 Using One Backup Account for Multiple Computers

Servosity PRO/STD allows you to run backups on multiple computers using a single backup account. To backup multiple computers, you need to create different backup set to backup each individual computer and to configure the [**Run scheduled backup on this computer**] checkbox, which is placed under the [**Backup Schedule**] menu of the Backup Setting dialog box.



For version 5.2 or above

Since the computer that created the backup set will have its computer name associated with the backup set. The backup scheduler running on each computer will only run backup sets with the same computer name as itself. Thus, you need to make sure that all of your computer names using a single backup account are unique.

For version 5.1 or Earlier

You must configure Servosity PRO/STD on each computer so that it only runs scheduled backups for the intended backup sets. If this is not setup properly, scheduled backup jobs of the same backup set from different computers will be started simultaneously. This will result in lots of checksum errors and files being deleted on the backup server.

To allow multiple computers to be backed up under a single backup account, you are required to do the following **for each computer** that has installed Servosity PRO/STD under the same backup account:

i. Logon to one of the computers that has Servosity PRO/STD installed under the same backup account.

ii. Open Servosity PRO/STD and select a backup set that is not intended to run on this computer from the left panel.

iii. Make sure that the [**Run scheduled backup on this computer**] checkbox on the right panel is not checked.

iv. Repeat the previous step for the rest of the backup sets that are not intended to run on this computer.

v. Repeat steps ii to iv for each computer that has Servosity PRO/STD installed under the same backup account.

IMPORTANT If you create a new backup set or want to backup another computer using the same backup account at a later date (this implies that you need to create an additional backup set under this backup account for the new computer), please make sure to repeat the procedure above (i.e. uncheck the [**Run scheduled backup on this computer]** checkbox for the added backup set) for each computer.