

This chapter describes how to configure a backup set.


A backup set defines the configuration of a backup routine, such as backup schedule, backup source and encryption setting as well as other options.



Click on the [Backup Setting] button to:




Create new backup set –

Select the  button to add a new backup set.

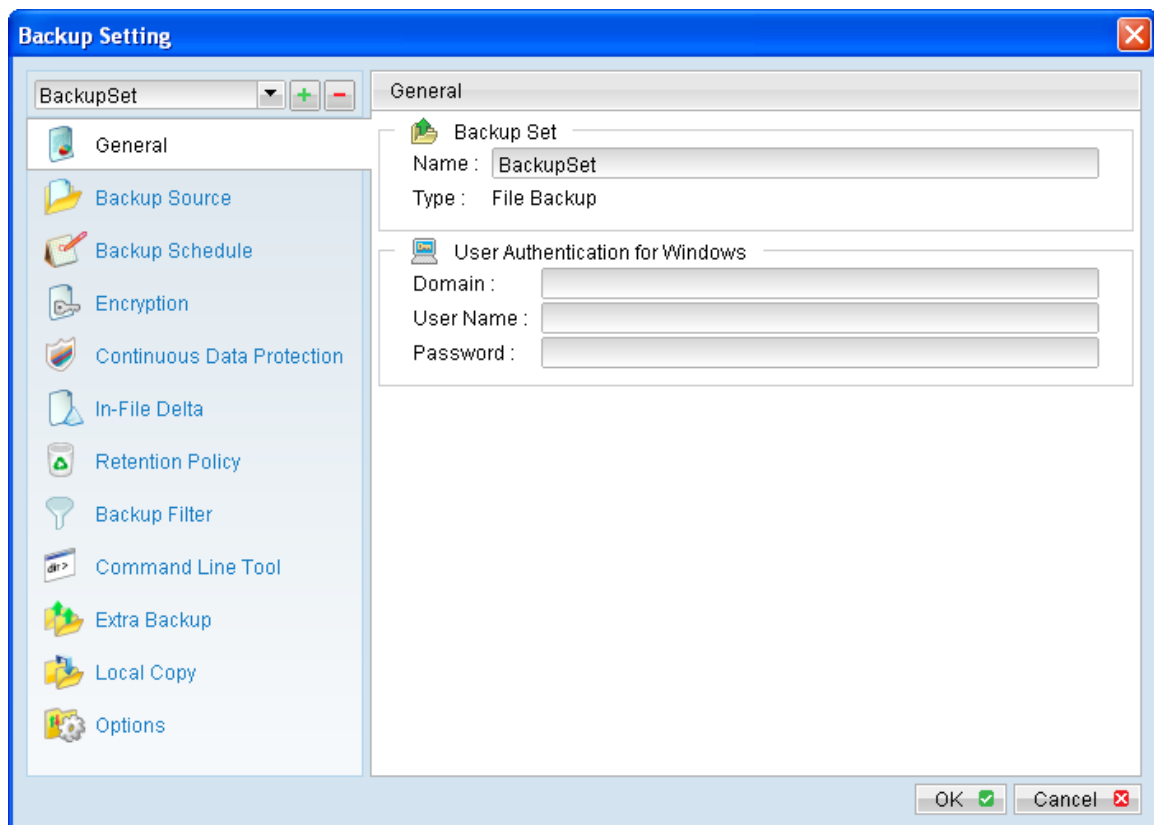














Delete existing backup set –

Select a backup set from the drop down menu, and the  button to remove corresponding backup set.

• Modify existing backup set –


Select a backup set from the drop down menu, and other options from the left panel to modify the backup set.

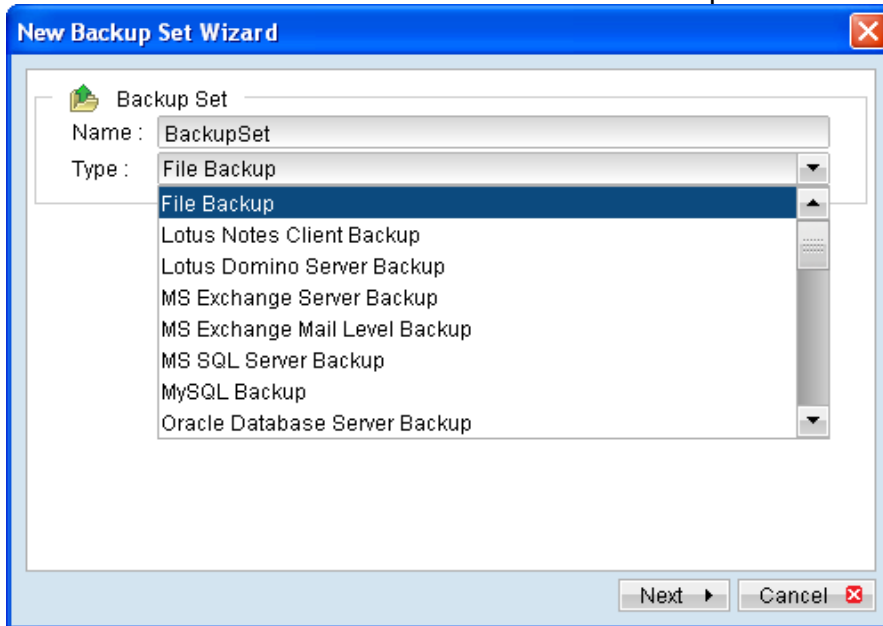


Icon	Menu Item	Description
	General	Click to access the general backup set menu.
	Backup Source	Click to access the backup source selection menu.
	Backup Schedule	Click to access the backup schedule setting menu.
	Encryption	Click to access the encryption setting menu.
	Continuous Data Protection	Click to access the continuous data protection menu.
	In-File Delta	Click to access the In-file delta menu.
	Retention Policy	Click to access the retention policy menu.
	Backup Filter	Click to access the backup filter menu.
	Command Line Tool	Click to access the pre post command line tool menu.
	Extra Backup	Click to access the extra backup setting menu.
	Local Copy	Click to access the local copy backup menu.
	Options	Click to access the option menu.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

New Backup Set Wizard

Select the  button to start the New Backup Set Wizard.



Select the corresponding backup type, in this case, a file backup set.
A backup set can be one of the following types:

Backup Type	Description
File	Backup set type for backup of normal files.
Lotus Domino Server	Backup set type for backup of Lotus Domino server.
Lotus Notes Client	Backup set type for backup of Lotus Notes client.
MS Exchange Server	Backup set type for backup of Microsoft Exchange server.
MS Exchange Mail Level	Backup set type for backup of individual emails (brick level backup).
MS SQL Server	Backup set type for backup of Microsoft SQL server.
MySQL Server	Backup set type for backup of backup MySQL server.

Oracle Database Server	Backup set type for backup of Oracle database server
System State	Backup set type for backup of Microsoft Window's System State.
ShadowProtect System	Backup set type for Bare-Metal backup of your system using StorageCraft's ShadowProtect.
Windows System	Backup set type for Bare-Metal backup of your system using Microsoft's WBAdmin.
MS VM	Backup set type for backup of Virtual Machine on Microsoft Hyper-V server.
VMware VM	Backup set type for backup of Virtual Machine on VMware server (VM Server, ESX, ESXi).

Note:

Backup set type is defined at the backup set creation time, and **cannot be modified afterward.**

Next few steps of a new backup set creation process, including Backup Source, Backup Schedule and Encryption setting configuration are discussed in the following sections of the guide.

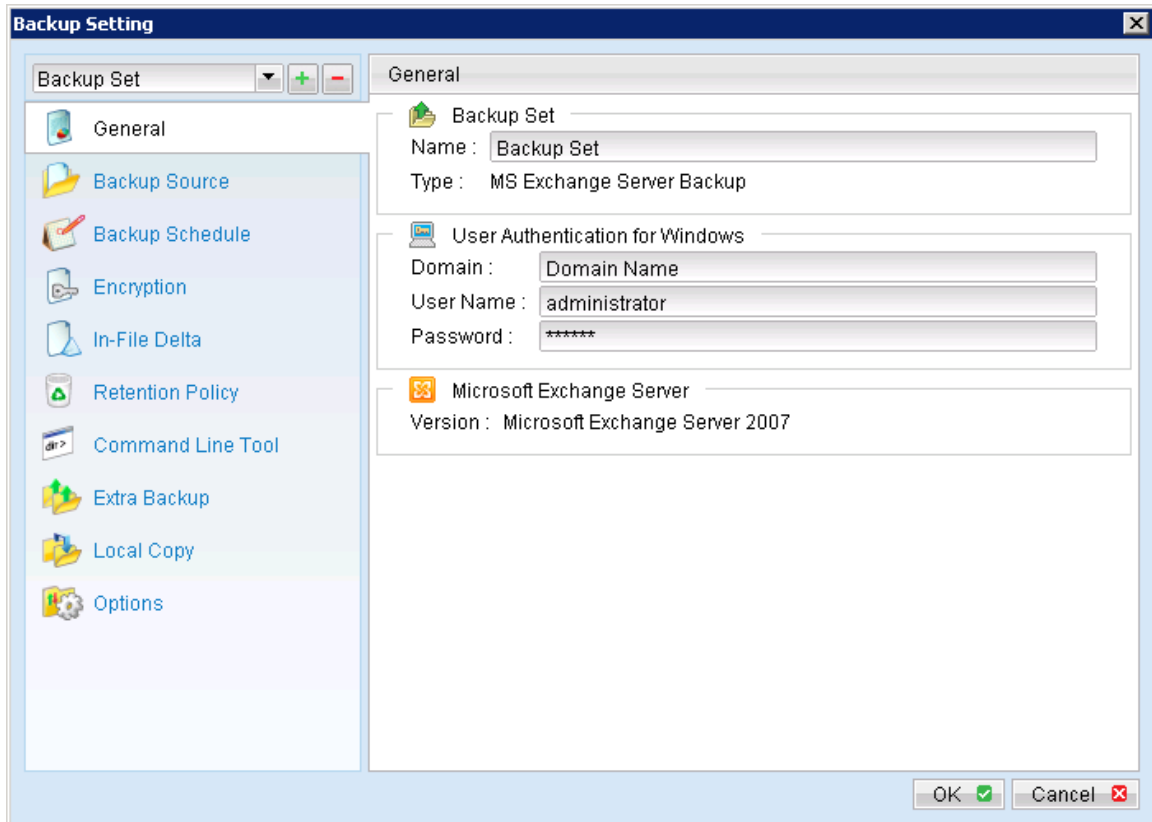
General



Click on the [General] tab to modify the [Backup Set Name] or [User Authentication for Windows] setting.

For backup set with backup schedule and network shared drive selected as backup source, the [User Authentication for Windows] is a **mandatory field** that must be filled in.

Please specify a Windows domain account for the backup client application with sufficient permission to access the network location



Menu Items	Description
Domain	Input box for entering domain of the Windows domain account.
User Name	Input box for entering username of the Windows domain account.
Password	Input box for entering password of the Windows domain account.

Backup Source



Click on the [Backup Source] tab to configure backup source of a backup set.

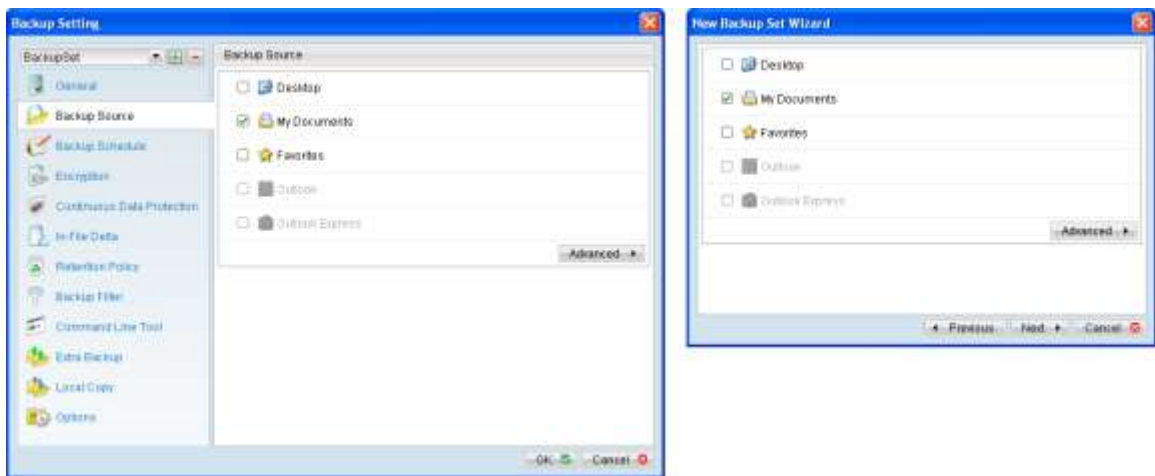
A Backup Source defines the files and directories to be included for backup.

There are two types of backup source: Selected and Deselected.

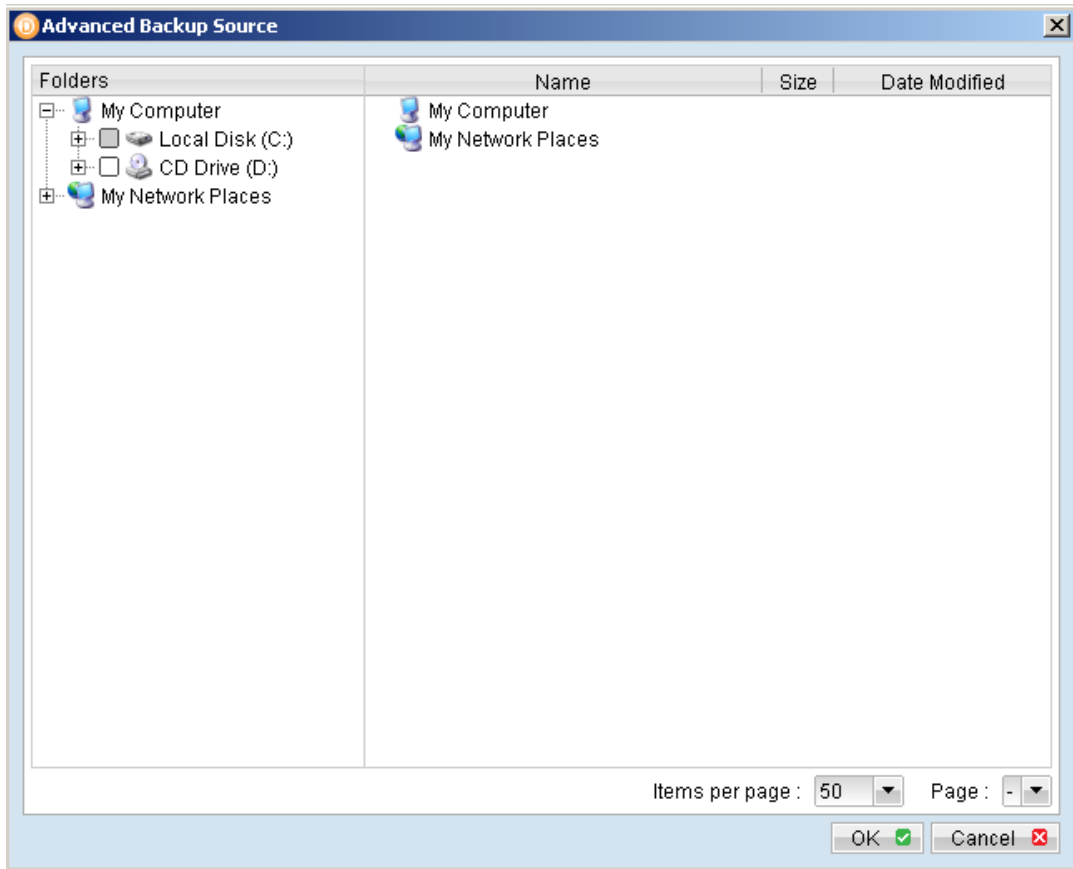
- Selected backup source defines files and directories that are to be included in a backup set.
- Deselected backup source defines files and directories that are to be excluded from a backup set.

On the basic backup source selection dialog, you can select directories that are commonly selected as backup source for backup:

- Desktop folder
- My Documents folder
- Favorites folder
- Outlook and Outlook Express folder



Click on [Advanced] button to access the advanced backup source dialog to select other directories for backup.



The checkbox beside a root drives, directory or file can be in one of the following mode:

Mode	Description
<input checked="" type="checkbox"/>	All directories and files under this directory will be backed up.
<input checked="" type="checkbox"/>	All directories and files under this directory except those explicitly excluded will be backed up. Directories and files selected to this directory in the future will be backed up as well.
<input type="checkbox"/>	Only the checked directories and files under this directory will be backed up. Directories and files selected to this directory in the future will not be backed up.
<input type="checkbox"/>	No directory or file under this directory will be backed up.

Note:

For installation on Windows platforms, hidden directories and files will be displayed only if the [Hide protected operating files] setting of Windows Explorer is disabled.

By selecting a parent directory as backup source, all child directories and files including any hidden directories or files would be backup as well.

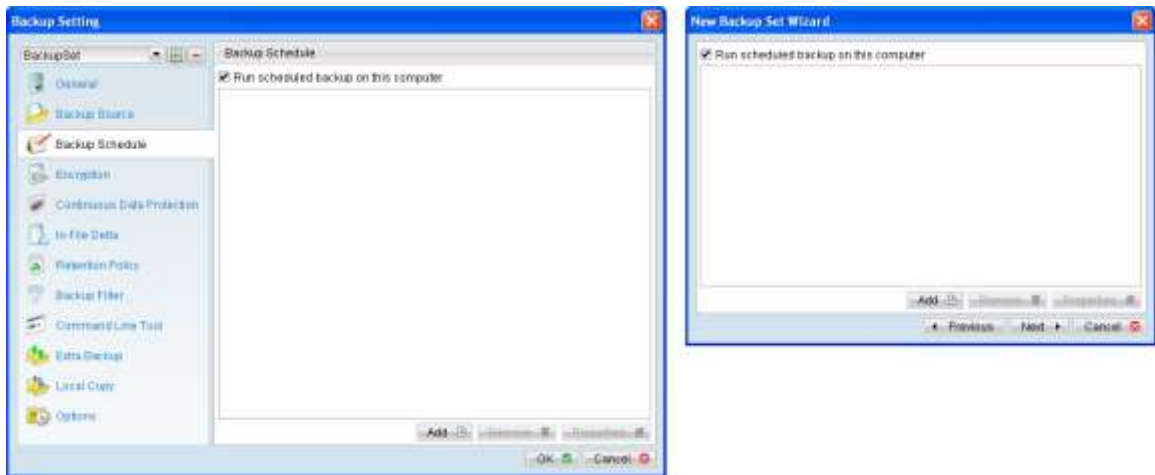
To avoid backing up hidden directories such as the Recycle Bin folder, please select the corresponding directories or files required as backup source directly, instead of selecting the parent directory or root drive letter.

Backup Schedule



Click on the [Backup Schedule] tab of the backup setting menu to configure backup schedule of a backup set.

A Backup Schedule defines the time, time period allowed, and frequency that backup job for an existing backup set should be run automatically.



Menu Items	Description
Run scheduled backup on this computer	Checkbox to enable or disable the corresponding backup set to run on this computer.
Add	Click to add a new backup schedule.
Remove	Click to remove an existing backup schedule.

Properties

Click to modify an existing backup schedule.

Add new backup schedule

Name : New Backup Schedule

Backup File

Type **Daily**

Backup everyday

Time At

Start : 23 : 00

Stop : on completion (Full Backup)
 after 8 hour(s)

OK Cancel

Add new backup schedule

Name : New Backup Schedule

Backup File

Type **Weekly**

Backup on the following day(s) every week :

Sunday Monday Tuesday
 Wednesday Thursday Friday
 Saturday

Time At

Start : 23 : 00

Stop : on completion (Full Backup)
 after 8 hour(s)

OK Cancel

Add new backup schedule

Name : New Backup Schedule

Backup File

Type **Monthly**

Backup on the following day every month :

Day : 1
 First Sunday

Time At

Start : 23 : 00

Stop : on completion (Full Backup)
 after 8 hour(s)

OK Cancel

Add new backup schedule

Name : New Backup Schedule

Backup File

Type **Custom**

Backup on the following day once :

Date (yyy-mm-dd) : 2011 - 03 - 18

Time At

Start : 23 : 00

Stop : on completion (Full Backup)
 after 8 hour(s)

OK Cancel

Menu Items	Description
Name	Input box for entering backup schedule name.
Type	<p>Checkbox to select schedule type.</p> <p>Daily - Backup job will run everyday at a specific time under this schedule type</p> <p>Weekly - Backup job will run on specific</p>

	<p>day(s) of a week, at a specific time under this schedule type.</p> <p>Monthly - Backup job will run on specific day of a month (date, or special criteria such as first weekend, last weekday), at a specific time under this schedule type.</p> <p>Custom - Backup job will run on specific day of a year (date), at a specific time under this schedule type.</p>
Time (At)	<p>To start backup job at a specific time.</p> <p>Start - Dropdown menu to select the start time of a backup job.</p> <p>Stop – Option to allow a backup job to run to completion, or to stop the running backup job after a specified hour.</p>
Time (Periodically)	<p>To start backup job at regular intervals of time.</p>

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

To configure a Daily backup schedule where backup job will run everyday at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Daily] from the schedule [Type] dropdown menu.
4. Select [At] from the [Time] dropdown menu.
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

To configure a Weekly backup schedule where backup job will run on Friday every week at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Weekly] from the schedule [Type] dropdown menu.
4. Select the checkbox beside [Friday].
5. Select [At] from the [Time] dropdown menu.

6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a Monthly backup schedule where backup job will run on first weekend of every month at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Monthly] from the schedule [Type] dropdown menu.
4. Select [First], [Weekend].
5. Select [At] from the [Time] dropdown menu.
6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a Custom backup schedule where backup job will run on Jan 1st of 2012 (2012-01-01) at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Custom] from the schedule [Type] dropdown menu.
4. Enter the date when the backup should be performed (YYYY-MM-DD).
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

Note that multiple backup schedules of different type (e.g. daily, weekly) can also be configured for a single backup set.

For example:

- Daily backup schedule at 00:00
- Daily backup schedule at 12:00
- Weekly backup schedule on Friday at 18:00

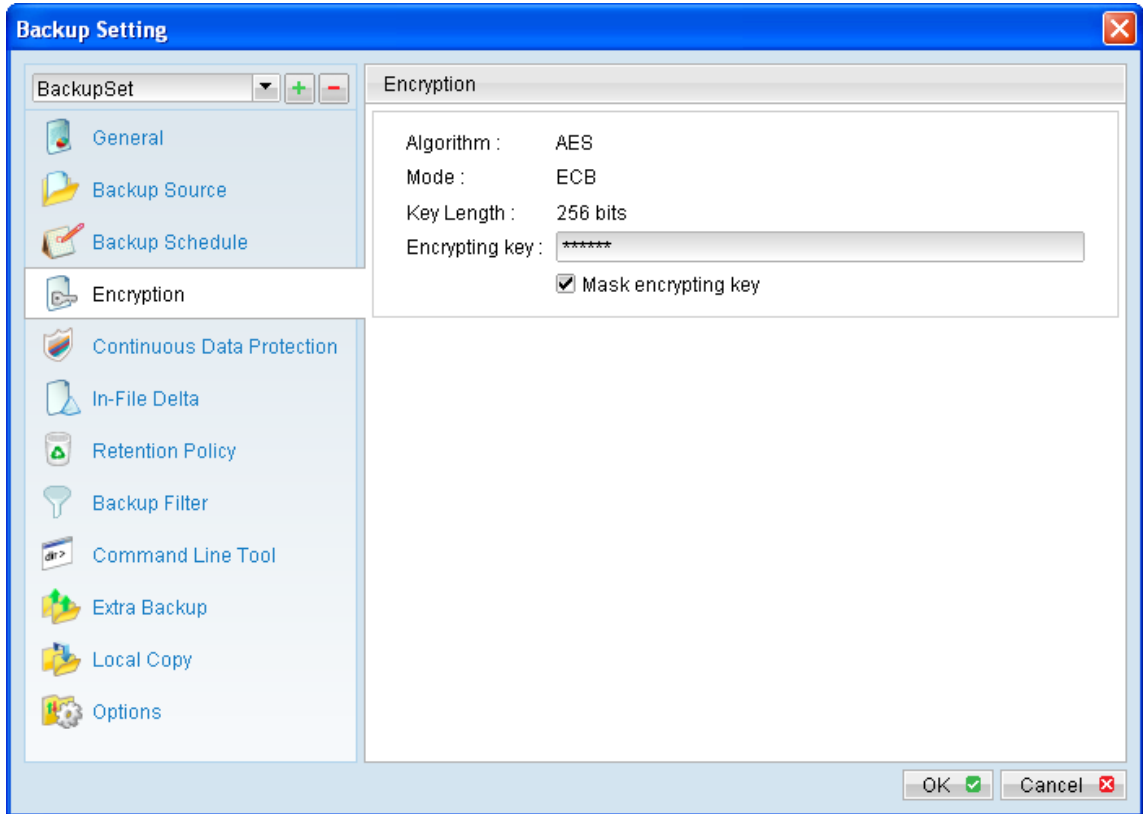
Combination of these schedules effectively creates a schedule for backup at 00:00 and 13:00 everyday, and 18:00 every Friday.

Encryption



Before files are uploaded to the backup server, they are first compressed and encrypted with an algorithm, mode and key of your choice.

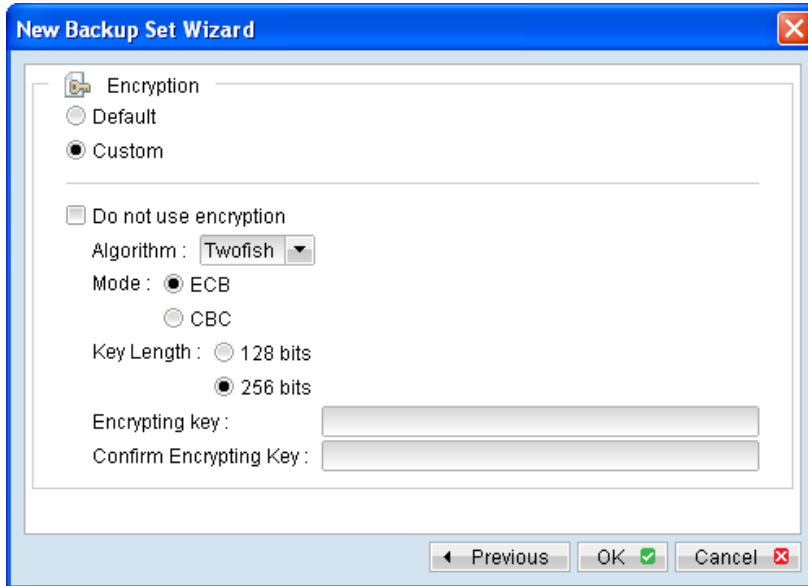
Select the [Encryption] tab to view the current encryption setting of an existing backup set.



Menu Items	Description
Encryption key	Text box displaying the encryption key for the corresponding backup set.
Mask encryption key	Checkbox to enable or disable masking of the encrypting key.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Encryption settings are set at a backup set's creation time in the New Backup Set Wizard.



Menu Items	Description
Default	<p>Radio button to select default encrypting key.</p> <p>Default encryption setting - Encryption algorithm: AES Encryption mode: ECB Key Length: 256 bits Encrypting key: Same as current password</p>
Custom	<p>Radio button to select your custom encryption setting, including:</p> <p>Encryption algorithm Encryption mode Key Length Encrypting key</p>
Do not use encryption	<p>Checkbox to disable encryption (not recommended).</p>
Algorithm (used with Custom)	<p>Dropdown menu to select the encryption algorithm setting:</p> <p>Twofish - Twofish algorithm DESede - Triple DES algorithm</p>

	AES - Advanced Encryption Standard algorithm
Mode (used with Custom)	Radio button to select ECB or CBC encryption mode: ECB - Electronic Cook Book mode CBC - Cipher Block Chaining mode
Key Length (used with Custom)	Radio button to select 128 bit or 256 bit key length.
Encrypting key (used with Custom)	Input box for entering your choice of encrypting key.

Select [Default] encryption setting if you are not familiar with encryption algorithm or mode. The default encryption setting is:

Encryption algorithm: AES
Encryption mode: ECB
Key Length: 256 bits
Encrypting key: Same as current password

Encryption settings are set at a backup set's creation time and cannot be modified afterward.

If you are entering your own encrypting key, please considering selecting an encryption key with more than 8 characters, containing at least two of the following three character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)

Important:

By selecting default encryption setting, password string of the backup account will be configured as encrypting key (for the corresponding backup set).

The encryption key is independent from a backup account's password.

Since encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is **VERY IMPORTANT** that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

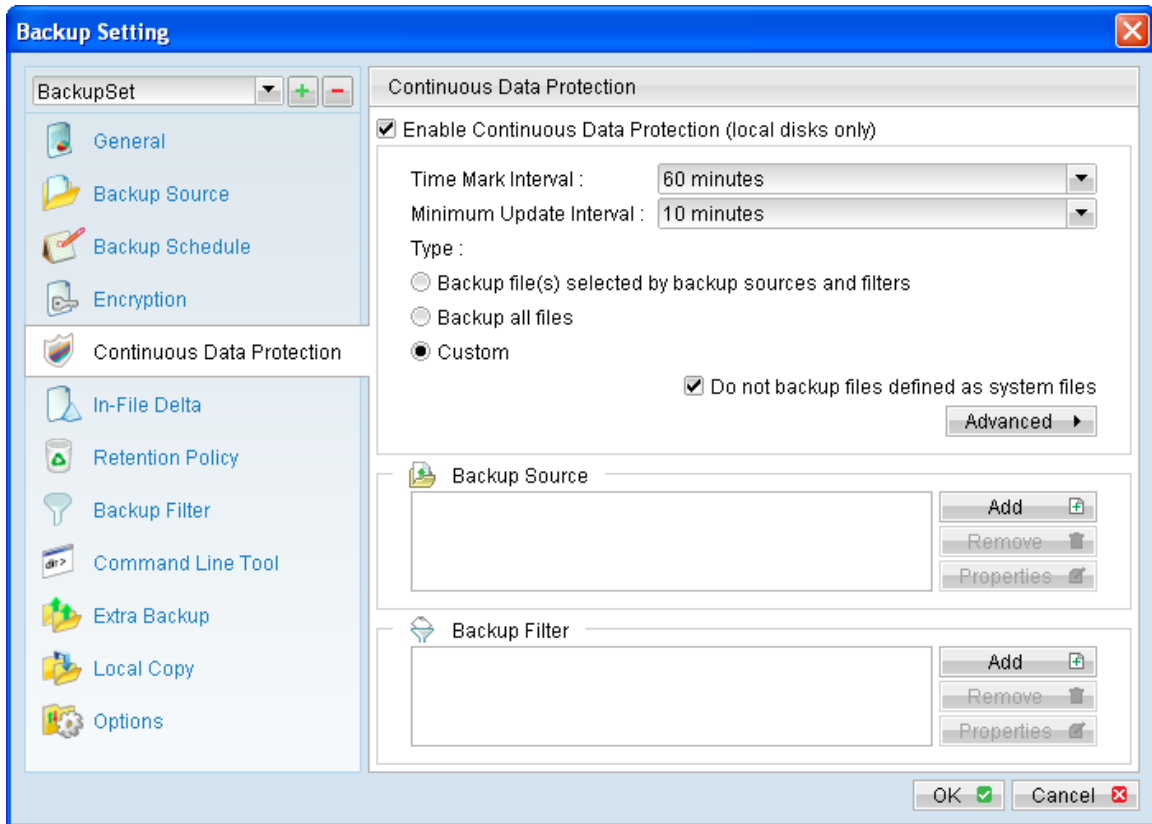
If you lose the encryption key, the data is irretrievable.

Continuous Data Protection (CDP)



Continuous Data Protection (CDP) is a feature providing backup for selective data whenever change is made. Depending on the option selected, every version of a file is backed up close to real time.

To enable CDP, click on the [Continuous Data Protection] tab and select the [Enable Continuous Data Protection] checkbox.



Menu Items	Description
Enable Continuous Data Protection	Checkbox to enable or disable CDP. Note: CDP will only backup directories and files on local drive, but not on floppy drive, removable drive or network

	drive.
Time Mark Interval	<p>Defines a regular interval of time (e.g. every x minutes), with each interval containing one snapshot (the first backup of each interval) available for restore.</p> <p>For example, for [Time Mark Interval] set to 60 minutes, with the file updated every 5 minutes. A restore-able snapshot of the file will be available for each interval:</p> <p>00:05, 01:05, 02:05, 03:05 ... etc.</p>
Minimum Update Interval	<p>Defines how often an updated file is backed up to the backup server.</p> <p>For example, for [Minimum Update Interval] set to [Always], file will be backed up to the server as they are updated.</p>
Backup file(s) selected by backup sources and filters	Radio button to select if CDP will only backup modified directories or files selected as backup source.
Backup all files	Radio button to select if CDP will back up all modified directories and files on all local drive.
Custom	<p>Radio button to select if CDP will backup a custom set of directories and files.</p> <p>Note: This custom set of directories and files can be different than the backup source selected for the backup set.</p>
Backup Source (used with Custom)	Add – Click to select a custom set of directory or file as backup source for CDP backup.

	<p>Remove – Click to remove a selected directory or file as backup source for CDP backup.</p> <p>Properties – Click to modify a selected directory or file as backup source for CDP backup.</p>
<p>Backup Filter (used with Backup all files or Custom)</p>	<p>Add – Click to create a backup filter for CDP backup.</p> <p>Remove – Click to remove a backup filter for CDP backup.</p> <p>Properties – Click to modify a backup filter for CDP backup.</p> <p>Note: Backup filter is case sensitive.</p>
<p>Do not backup files defined as system files</p>	<p>When this option is enabled, CDP will automatically exclude the following files from its backup:</p> <p>C:\hiberfil.sys C:\Pagefile.sys C:\Program Files* C:\RECYCLER C:\System Volume Information C:\Windows* \${App_Data}\Avg7 \${App_Data}\Avg8 \${App_Data}\Kaspersky Lab \${App_Data}\McAfee \${App_Data}\McAfee.com \${App_Data}\Microsoft \${App_Data}\Sophos \${App_Data}\Symantec **.tmp *\Application Data\Macromedia* *\Application Data\Mozilla* *\Local Settings\Application Data\Microsoft* *\ntuser.dat</p>
<p>Advanced</p>	<p>Click to access advanced CDP</p>

	<p>backup control to backup only when:</p> <p>CPU usage is less than a specific percentage. Network traffic is less than a specific Megabyte per second.</p> <p>No keyboard or mouse input exceeding a specific time (in minute).</p>
--	--

Note:

The [Continuous Data Protection] tab is only available for Dsphinx Enterprise installation in Windows platforms.

Configure the [Time Mark Interval] and [Minimum Update Interval] according to your recovery requirement.

Time mark interval defines a regular interval of time, where each interval contains one snapshot available for restore.

For example, when [Time Mark Interval] is configured to 60 minutes. 24 intervals would be marked per day, with each interval spanning across 60 minutes:

Interval 1 – 00:00 to 01:00
Interval 2 – 01:00 to 02:00
Interval 3 – 02:00 to 03:00
Interval 4 – 03:00 to 04:00

To

Interval 23 – 22:00 to 23:00
Interval 24 – 23:00 to 24:00

Assuming that a file is backed up multiple times (by CDP) within each interval, the first backup (e.g. snapshot) of each interval would be available for restore.

Minimum update interval defines the minimum period of time before an updated file is backed up to the backup server.

For example, when [Minimum Update Interval] is configured to 10 minutes, updated file would be backed up to the backup server every 10 minutes. To ensure that updated files are always uploaded to the server

immediately, you can consider setting the [Minimum Update Interval] as Always.

To configure CDP for backup of the **directories and files selected as backup source**:

1. Select the [Backup file(s) selected by backup sources and filters] radio button for [Type].

To configure CDP for backup of **all local drive(s)**:

1. Select the [Backup all files] radio button for [Type].
2. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

To configure CDP for backup of a **custom set of directories or files**:

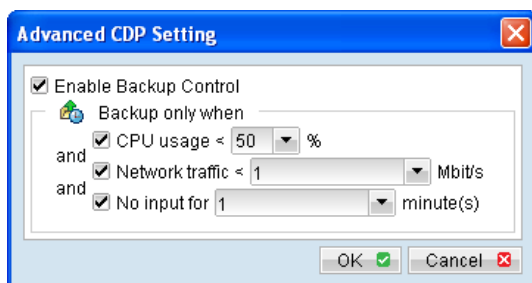
1. Select the [Custom] radio button for [Type].
2. Click [Add] beside the [Backup Source] section (within the CDP tab).
3. Select the custom set of data for backup.
4. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

Note that the backup filter function is only available for CDP type [Backup all files] or [Custom].

Although CDP can be a helpful feature, the protection offered by CDP is often heralded without consideration of the disadvantages that it can present.

Specifically, the continuous CPU, memory and bandwidth usage can adversely affect the corresponding machine's performance.

To enable backup control for CDP backup, select [Advanced] to open the advanced CDP setting dialog:



To allow CDP backup only when CPU usage is under 50%:

1. Select the checkbox beside [CDP usage].

2. Select the corresponding percentage from the [%] dropdown menu.

To allow CDP backup only when network traffic is under 10 Mbit/s:

1. Select the checkbox beside [Network traffic]
2. Enter the corresponding number in the [Mbit/s] textbox.

To allow CDP backup only when there is no keyboard or mouse input for 5 minutes:

1. Select the checkbox beside [No input for].
2. Enter the corresponding number (in minutes) in the [minute(s)]

Important:

Continuous Data Protection (CDP) will only backs up data selected as backup source after the CDP module is enabled. Existing data that are not updated will not be backed up by the CDP module.

Furthermore, CDP is not a replacement for the traditional schedule backup but works along with the scheduled backup to provide timely protection for your data.

CDP will automatically be stopped when a manual or scheduled backup is started, and will resume when the job is completed.

Note: It is not possible to run multiple CDP backup sets on the same machine with different backup user accounts.

In-File Delta

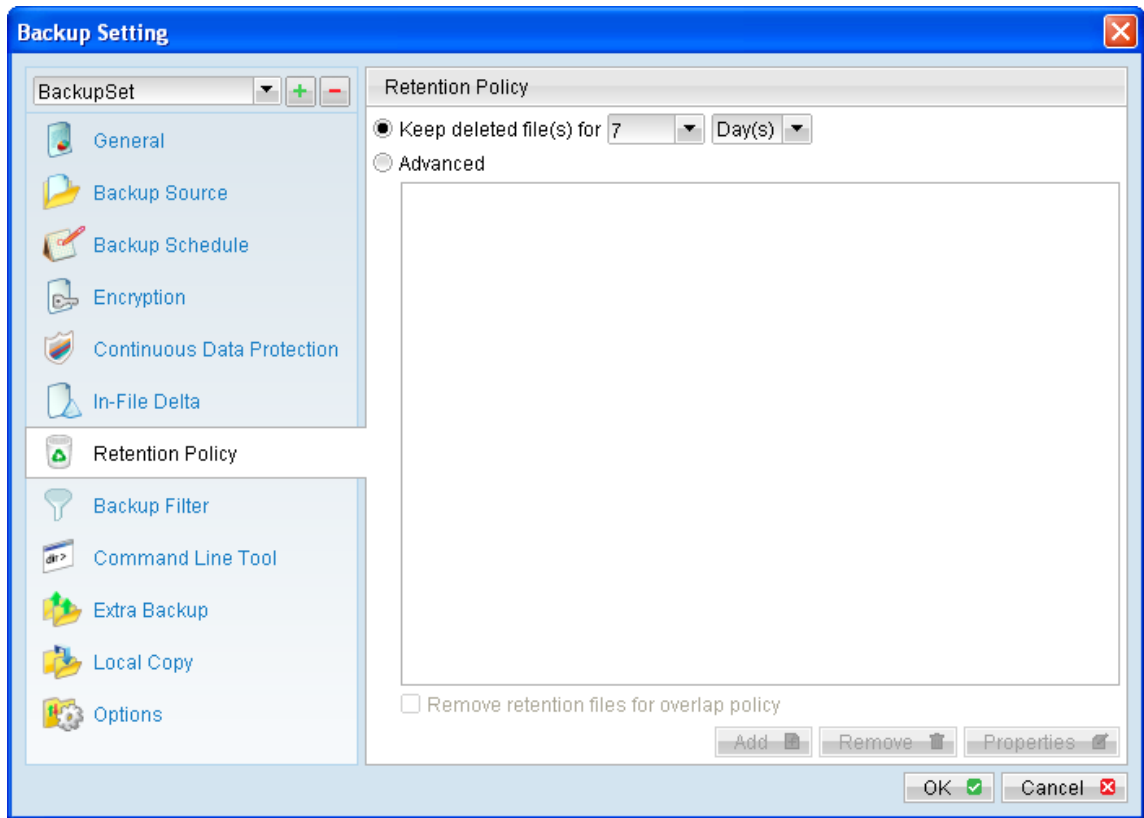


For more details about the In-file delta technology, please refer to the In-File Delta Technology section to be followed in this guide or web site Dsphinx.com.

Retention Policy



Click on the [Retention Policy] tab to modify the retention policy of an existing backup set.



Retention policy defines the policies of persistent data management for meeting business data archival requirements.

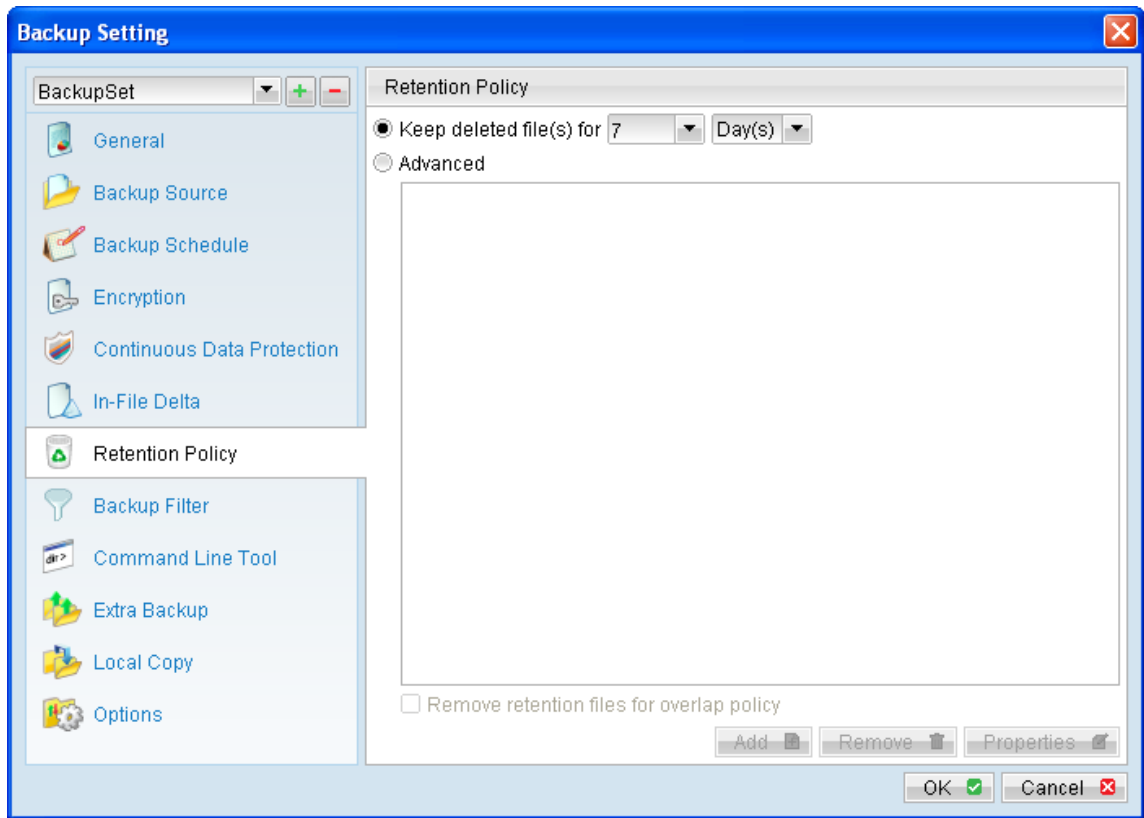
When a backup job is performed, for data that are modified or deleted on the client computer, their existing version on the backup server (backed up previously) would be moved into retention area, while newly backed up file would be placed in the current data area.

Specifically, retention policy setting defines how long are these data kept within the retention area before they are deleted permanently from the backup server.

For backed up data that have not been updated or deleted from the client computer, they are kept in the data area on the backup server and remain untouched.

A **standard retention policy** defines a basic policy where retained file (in the retention area) are removed automatically after a user specific number of days or backup jobs.

To define a standard retention policy, simply modify the [Keep delete file(s) for] drop down menu to your required days or jobs. Press [OK] and save before exiting the backup application to confirm the changes.



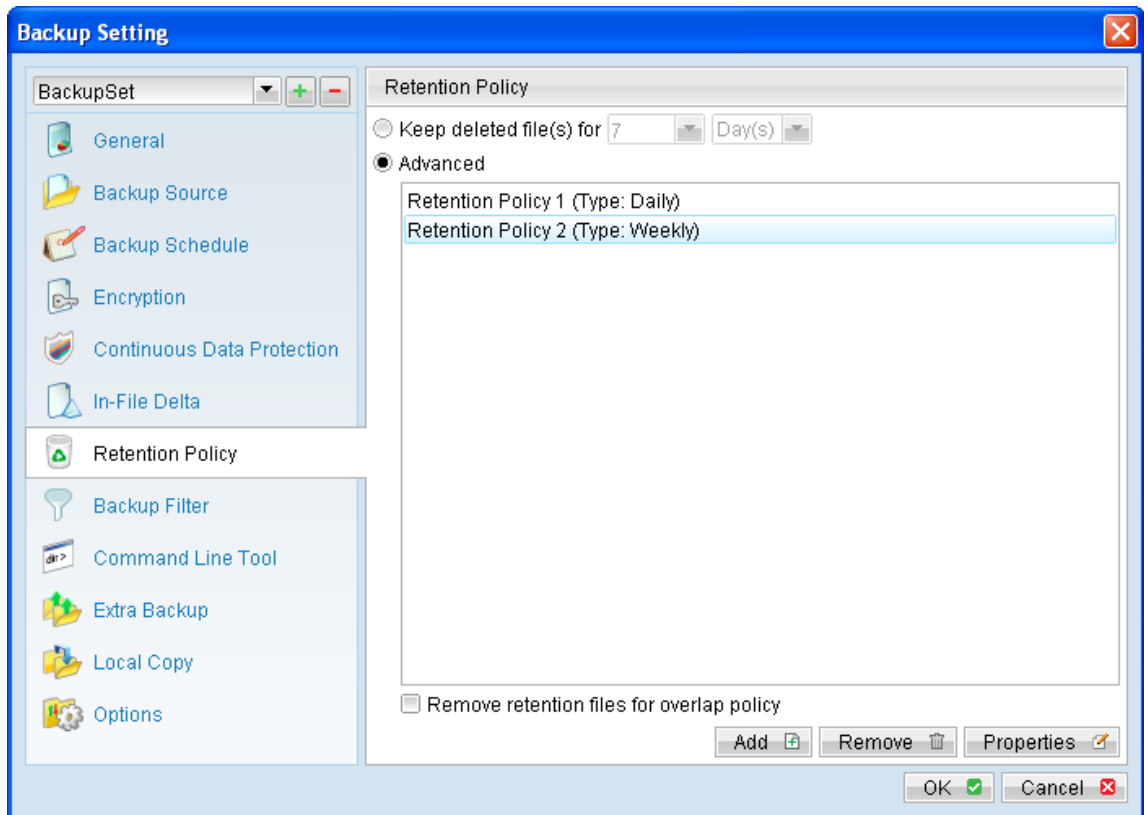
An **advanced retention policy** defines a more advanced and flexible policy where retained file (in the retention area) are removed automatically after a combination of user defined policy, such as:

- A specific number of days
- A specific number of weeks, including the day of the week
- A specific number of months, including the day of the month
- A specific number of years, including the day of the year

To define an advanced retention policy, select the [Advanced] button, and press the:

- [Add] button to add new policy
- [Remove] button to remove existing policy
- [Properties] to edit existing policy

Press [OK] and save before exiting the backup application to confirm the changes.



For example, you can configure the advanced retention policy to keep all data backed up:

- In the last 7 days.
- In the last 4 Saturdays.
- In the 1st day of each month in the last 3 months.
- In the 1st day of each quarter in the last 12 months.
- In the 1st day of each year in the last 7 years.

To achieve the above example policy, configured the advanced retention policy as follows:

- Type: **Daily**
Number of snapshots to keep: **7**
- Type: **Weekly**
Keep retention files for the following days: **Saturday**
Number of snapshots to keep: **4**
- Type: **Monthly**
Keep retention files for the following days: **Day 1**

Number of snapshots to keep: **3**

- Type: **Quarterly**
Keep retention files for the following days:
Month – January, April, July, October
Day 1

Number of snapshots to keep: **4**

- Type: **Yearly**
Keep retention files for the following days: **01-01**
Number of snapshots to keep: **7**

Assuming that a file is updated and being backed up everyday for the past 7 hours, and today is January 11, 2011.

If the option [Remove retention files for overlap policy] is not enabled, a total of 22 snapshots (previous version) of the file would be available for restore:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	14-Jan-2011	01-Jan-2011	01-Jan-2011	01-Jan-2011
15-Jan-2011	07-Jan-2011	01-Dec-2010	01-Oct-2010	01-Jan-2010
14-Jan-2011	31-Dec-2010	01-Nov-2010	01-Jul-2010	01-Jan-2009
13-Jan-2011	24-Dec-2010		01-Apr-2010	01-Jan-2008
12-Jan-2011				01-Jan-2007
11-Jan-2011				01-Jan-2006
10-Jan-2011				01-Jan-2005

If the option [Remove retention files for overlap policy] is enabled, the overlapping snapshots would be removed, with the following snapshots available:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	14-Jan-2011	01-Jan-2011	01-Jan-2011	01-Jan-2011
15-Jan-2011	07-Jan-2011	01-Dec-2010	01-Oct-2010	01-Jan-2010
14-Jan-2010	31-Dec-2010	01-Nov-2010	01-Jul-2010	01-Jan-2009
13-Jan-2010	24-Dec-2010		01-Apr-2010	01-Jan-2008
12-Jan-2010				01-Jan-2007
11-Jan-2010				01-Jan-2006
10-Jan-2010				01-Jan-2005

The weekly policy overrides the daily policy so the snapshots of 10-Jan-2011, 11-Jan-2011, 12-Jan-2011, 13-Jan-2011 and 14-Jan-2011 are removed.

The monthly policy overrides the weekly policy so the snapshots of 24-Dec-2010 and 31-Dec-2010 are removed.

The same applies to the monthly, quarterly and yearly policy giving a total of 11 snapshots.

Important:

The Retention Policy and Delta Merge feature is closely related, as the criteria for file merging is governed by the retention policy setting configured for a backup set.

Please refer to the Delta Merge section in this guide for further details.

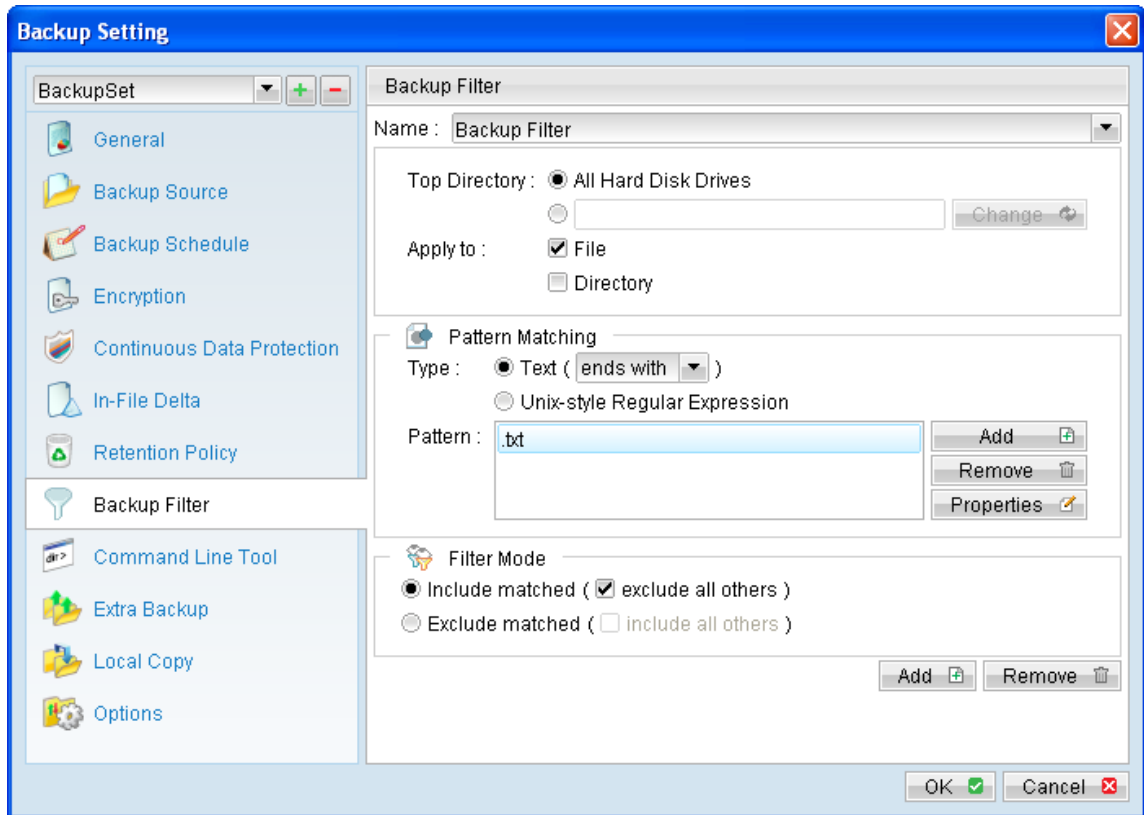
Backup Filter

Backup Filter is a set of user defined criteria to include or exclude directories and files as backup source of a backup set.

There are some basic rules regarding backup filters:

1. Filters are applied in creation order.
2. Inclusion or exclusion made by filter takes precedence over backup source selections.

To add a new filter, press the [Add] button at the bottom of the right panel.



Menu Item	Description
Name	The name of a filter.
Top Directory	<p>The top directory to which this filter is applied. Filtering rules will be applied to all files and/or directories under this directory.</p> <p>All Hard Disk Drives – select all local hard drives as the top directory automatically.</p>
Apply To	Define whether to apply the filtering rule to files and/or directories.
Pattern Matching	<p>It defines the filtering rules of a filter. A filtering rule can be one of the following types;</p> <p>[Starts With] Include/Exclude all files/directories with name starting with a certain pattern.</p> <p>Example: You can use B* to match all file with name starting with a B character.</p> <p>[Contains] Include/Exclude all files/directories with name containing a certain pattern.</p> <p>Example: You can use *B* to match all files with name containing with a B character.</p> <p>[Ends With] Include / Exclude all files / directories with name ending with a certain pattern. e.g. You can use *.doc to match all files with name ending with .doc (all Word Documents)</p> <p>[Regular Expression] Include/Exclude all files/directories with name matching a regular expression.</p> <p>To add a new pattern, press the [Add] button in the [Pattern Matching] area.</p> <p>Note: Backup filter is case sensitive.</p>
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.
--	---

Example 1:

To backup only Word, Excel and PowerPoint documents in the document directory (e.g. C:\My Documents), setup the 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:

To backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Application, setup the backup filter as follows.

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

Example 3:

If C:\ was selected as backup source, to exclude all images (e.g. *.jpg and *.gif) from the backup source selection, setup the 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

Note that the [Include all others] setting is not enabled because it is not necessary to include all other file types under C:\ into the backup set.

Example 4:

To include everything, except the log directory, under C:\Applications, setup the 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:

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, the filter backup can be setup as follows.

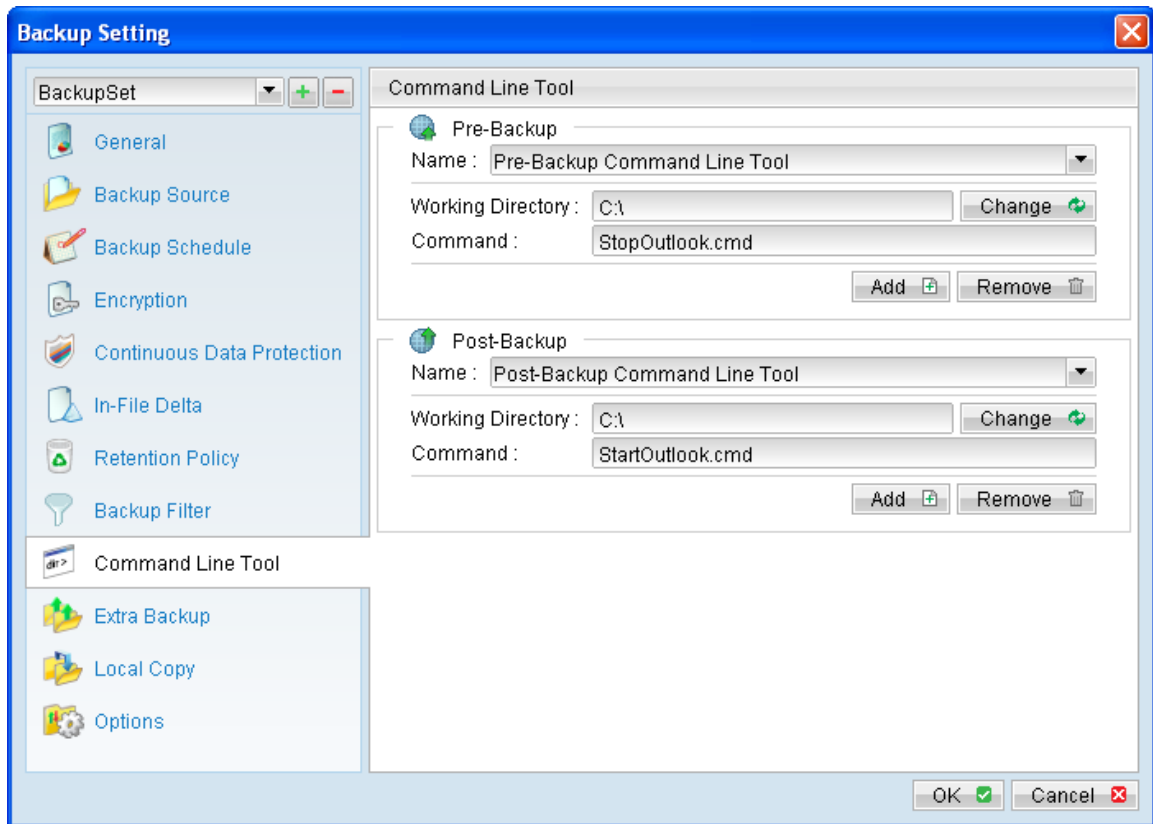
Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = Regular Expression
Matching Patterns = ^B.*\doc\$
Filter Mode = Include
Exclude all others = True

Command Line Tool



Click on the [Command Line Tool] tab to configure a Pre-Backup or Post-Backup command.

Command such as batch file to stop and start an application before and after a backup job is complete, or other command such as to shutdown the computer when a backup job is complete can be configured.



Menu Item	Description
Add	Click to add new pre or post backup command.
Remove	Click to remove existing pre or post backup command.
Name	Input box to enter name of a pre or post backup command.
Working Directory	Directory which the pre or post backup command will run at.
Command	<p>Input box to enter pre or post backup command to be run.</p> <p><u>For Windows:</u> Native command or command to execute a batch , command or VBScript file can be configured:</p> <p>shutdown -s -t 60 batch.bat command.cmd</p>

	<p>script.vbs</p> <p><u>For Linux:</u> Command to execute a script file must be configured:</p> <p>/usr/local/command.sh</p> <p><u>For FreeBSD / Solaris:</u> Command to execute a script file must be configured:</p> <p>./usr/local/command.sh</p> <p>Note: For all platforms, please ensure that control is returned to the backup application once the command is executed.</p>
--	---

For Dsphinx Enterprise installation on Linux / FreeBSD / Solaris platform (without GUI environment installed), you can setup the pre and post backup command on the web console:

Menu Item	Description
Add	Click to add new pre or post backup command.
Remove	Click to remove existing pre or post backup command.
Name	Input box to enter name of a pre or post backup command.
Command	Input box to enter pre or post backup command to be run. Pre and post command must be put into a

	<p>script file. It is also recommended to add the absolute path location of the script, such as:</p> <p>/pathname/scriptname.sh</p> <p>Note: Please ensure that control is returned to the backup application once the command is executed.</p>
Working Directory	<p>Location the script would be working from.</p> <p>This field can be left empty, but please note that any output from the script would be stored under the Dsphinx-Enterprise installation folder.</p>
Update	Click to save the changes.

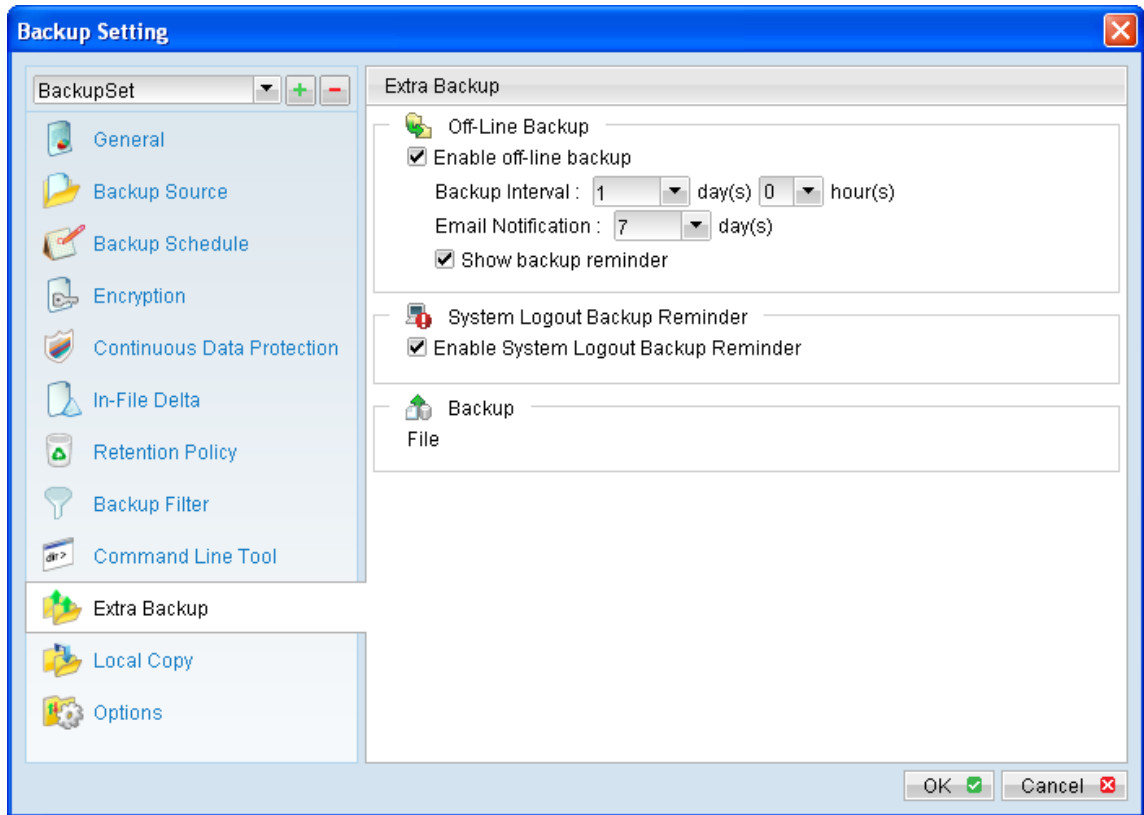
The pre and post backup command may run at different time according to the backup type. The following table outlines when they would be run:

Backup type	When does the Pre-Backup command run?	When does the Post-Backup command run?
File backup type	Before any file is backed up (uploaded) to the backup server.	When the backup (upload) of all files are completed.
Non-file backup type	Before any database file is spooled to the designated temporary directory.	After spooling backup files to temporary directory (i.e. before the first backup file is uploaded).

Extra Backup



Click on the [Extra Backup] tab to enable the Off-Line Backup and System Logout Backup Reminder option.



Note:

The [Extra Backup] tab is only available for AhsayOBM installation on Windows platforms.

Enable off-line backup

Enable off-line backup defines whether to enable the [off-line backup] feature.

The [off-line backup] feature is designed for notebook users who may be off-line most of the time, and cannot rely on backup scheduled for regular backup of their data.

Enable off-line backup	Action
Enabled	Prompt for backup if the time between the last backup to the current time exceeded the [Backup Interval].
Disabled	Do not prompt for backup.
Backup Interval	Time interval between each backup job.
Email Notification	Time interval when email would be sent for backup reminder.
Show backup reminder	To display or hide the confirmation dialog for backup. If the confirmation dialog is disabled, backup will be performed automatically when connection to the Internet is re-established.

With the [off-line backup] setting is enabled, when the computer is connected online and the time between the last backup to the current time elapsed the [Backup Interval], a pop up off-line backup confirmation menu will be prompted, reminding the user to perform a backup.

Menu Items	Description
Yes	Perform the backup job immediately.
No	Do not perform the backup job.

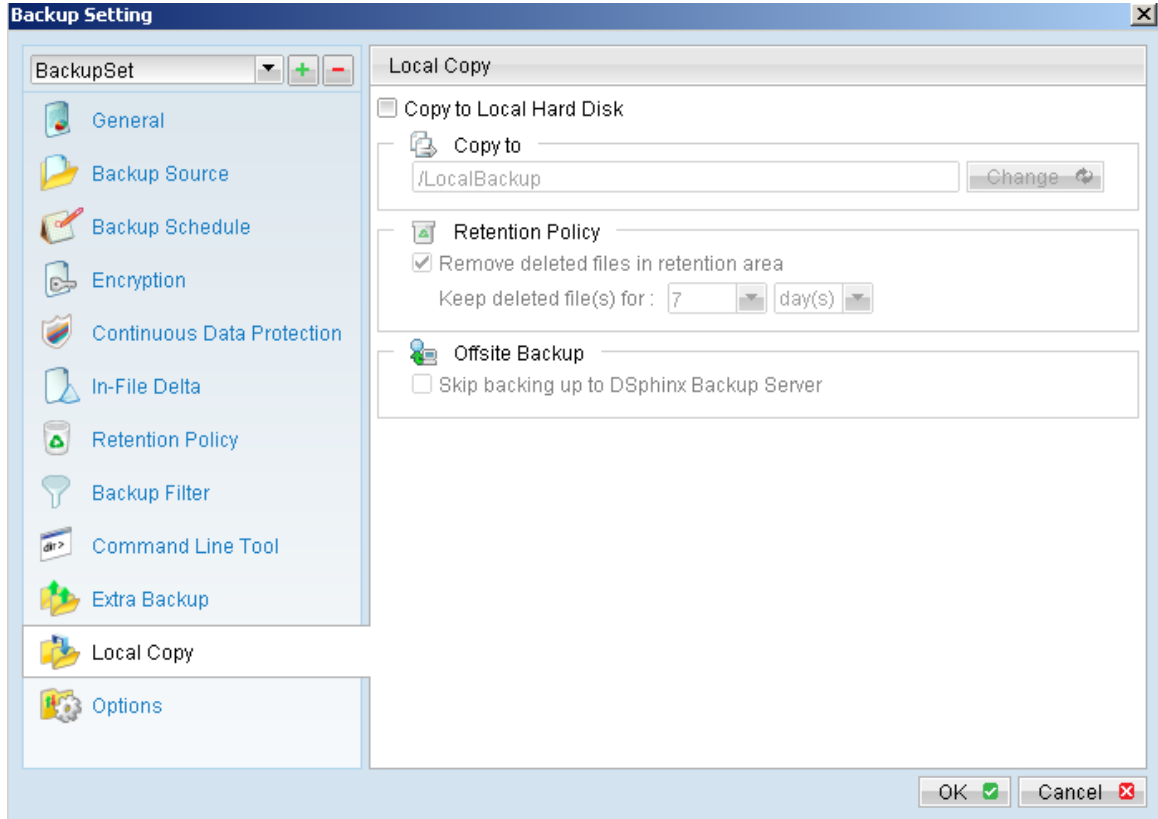
When the [System Logout Backup Reminder] setting is enabled, a pop up logout reminder menu will be prompted, requesting for backup before the user logs out of the system or before shutting down Windows.

Local Copy



To save a copy of back up data locally on the client computer, simply enable the local copy feature of the backup client application.

Click on the [Local Copy] tab to configure a local copy backup.



Menu Items	Description
Copy to Local Hard Disk	Checkbox to enable or disable local copy backup.
Copy to	Directory which the local copy data are stored.
Remove deleted files in retention area	Checkbox to enable or disable the retention policy of the local copy backup.
Keep deleted file(s) for	Dropdown menu to select a basic retention policy. Note: For local copy backup, only basic retention policy can be applied.

Skip backing up to Ahsay Offsite Backup Server	Checkbox to skip or to perform off-site backup for the corresponding backup set.
--	--

Select the corresponding backup set from the drop down menu, and click on the [Local Copy] tab.

Select the checkbox beside [Copy to Local Hard Disk], click the [Change] button and browse to the directory path which you would like to store the local copy backup.

You can enable retention policy for the local copy backup (if necessary). However, note that only basic retention policy can be configured for local copy.

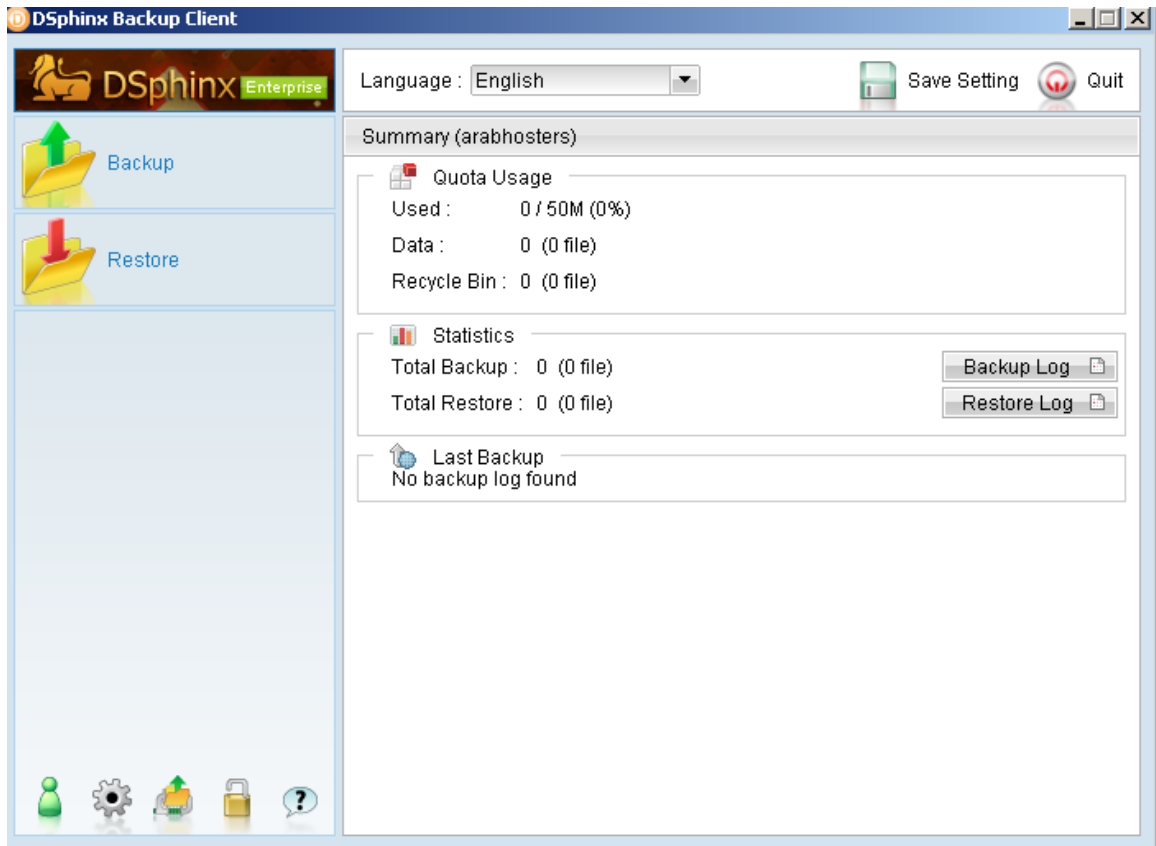
Retention policy of the local copy backup is separate from the retention policy configured for the off-site backup (configured in the [Retention Policy] tab).

For backup set that is intended for local copy backup only, select the checkbox beside [Skip backing up to Dsphinx Backup Server].

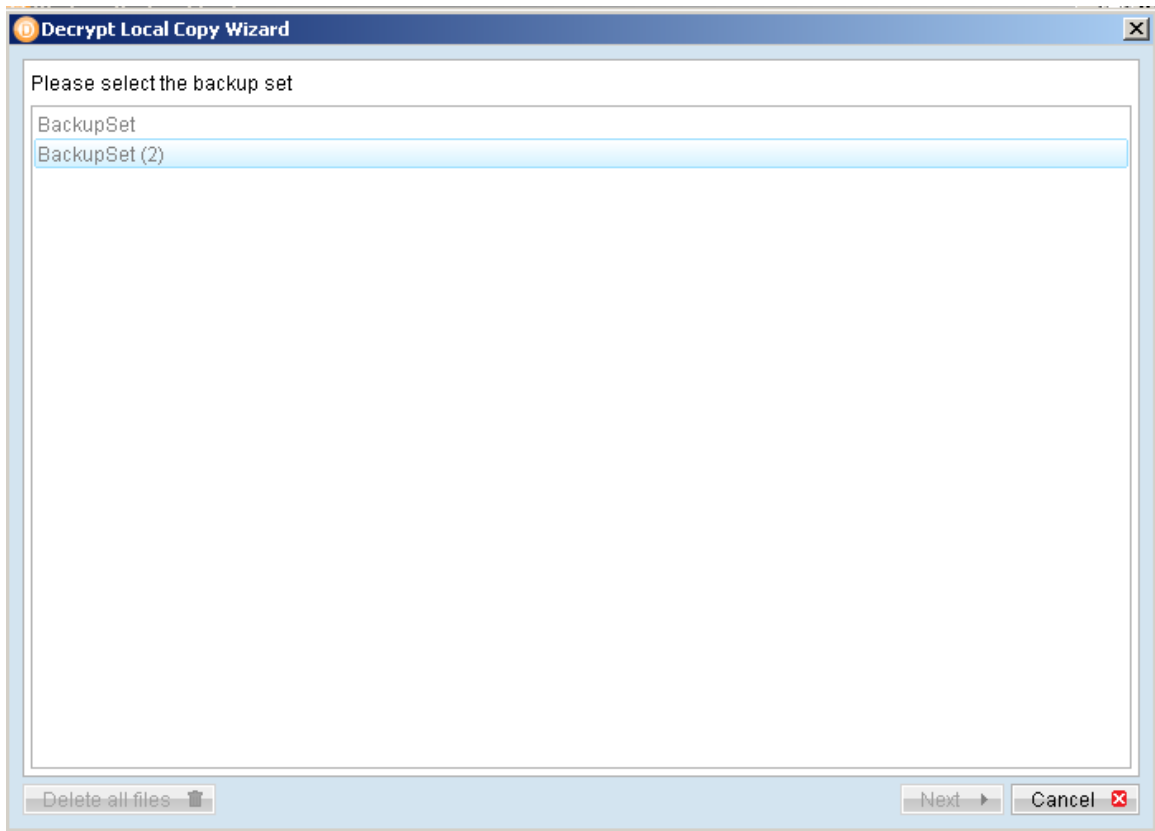


Data that are backed up by the local copy module are compressed and encrypted. To restore local copy backed up files, please refer to the following instruction:

1. Press the [Decrypt Local Copy Wizard] button on the backup application's main window.



2. Select the backup set to be restored and press [Next] to proceed.



3. Follow the normal restore procedure for restoration of your local copy backed up data. For more details, please refer to Chapter 8 of this guide.

