



Zen Internet

Online Data Backup

Zen Vault Express for Mac®

Issue: 2.0.08



Contents

1	Introduction.....	3
1.1	System Requirements	3
2	Installation	5
2.1	The Setup Wizard	5
2.2	Backup Monitor	7
3	Backup Client	9
	How to Backup.....	10
3.1	Selecting files for backup.....	10
3.2	Filters	11
3.3	Profiled Sections	11
3.4	Manual Backups	11
3.5	Backup Resume.....	12
	How to Restore	13
3.6	How to restore files and folders	13
3.7	Finding Files.....	14
	Options and Settings	16
3.8	Account and Security	16
3.9	Connections	17
3.10	Backup Schedule	17
3.11	Disk Usage.....	17
3.12	Performance and Limits.....	18
3.13	Advanced Options.....	19
3.14	Logging	20
	Additional Settings	21
3.15	Remote Management	21
3.16	Health Check	21
3.17	Dynamic Profiling	22
3.18	Language	22
3.19	Look and Feel	22
4	Security	23
4.1	Blowfish Encryption.....	23
4.2	SSL Communication	23



1 Introduction

Congratulations on choosing Online Data Backup. We believe you will find our Zen Vault Express product to be the most secure, scalable and efficient solution in addressing the business risk associated with the protection of critical data in a distributed environment.

If you experience any difficulty installing Online Data Backup, please don't hesitate to contact us on 0845 058 9000.

Online Data Backup is a remote storage solution that utilises client/server architecture to securely replicate data from the client device to a central data server. Data is compressed to minimise bandwidth utilisation and transferred using a secure SSL connection to the server. The data is stored in an encrypted format, using an encryption key known only to you.

Online Data Backup minimises risk, maximises productivity and allows businesses to regain control of their most valuable asset – their data.

1.1 System Requirements

1.1.1 Operating System

- Mac OS X (from version 10.4)

1.1.2 Processor

- PowerPC G3, G4, or G5 processor
- Intel Core (note that you need a separate installer for this processor)

1.1.3 Memory

- Memory requirements mainly depend on the amount of files selected for backup.
- Required: 128MB RAM above operating system and application requirements
- Recommended: 256MB RAM above operating system and application requirements

1.1.4 Disk Space

- Required: 50MB plus space for local cache.
- Recommended: Amount of free space equal to the backup account limit. The local cache can be as large as the total size of all files selected for backup; a file selection of 100MB needs up to 100MB extra disk space for the cache.



1.1.5 Minimum Video Settings

- 800 x 600 Resolution, 256 colours

1.1.6 Other Hardware

- Network interface card or a virtual network adapter card
- CD-ROM drive or Internet access to download and install the software



2 Installation

To install the Online Data Backup service, copy the installation file to a local disk and then double-click on the file.

Note

Ensure that you use the correct installer, as there are separate installers for the Mac PowerPC and Intel Core processors.

A file, ZenVault Express.pkg will be extracted. Double click on this installation file to start the installation wizard. Run through the installation steps and provide the necessary information, e.e. the destination volume.

Two shortcuts are automatically created in the Applications menu at the end of the installation process, Zen Vault Express and Backup Monitor. The Backup Monitor is used to automatically start the Desktop and Laptop Edition client when a scheduled backup must be initiated. Double-click on the Zen Vault Express icon to start the Backup Client. If you need to uninstall the Backup Client, move these two shortcuts to the Trash folder.

When you open the Backup Client for the first time, the Setup Wizard will start automatically. You need to create an account for the Client on the Storage Platform before you can initiate any backups.

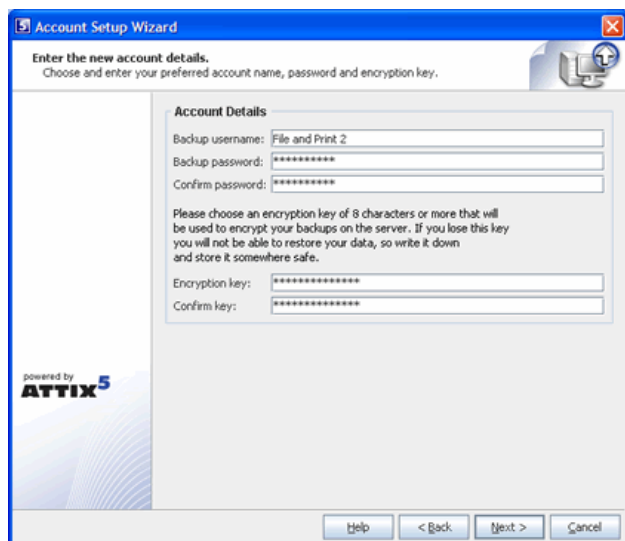
2.1 The Setup Wizard

Step 1 of 6

If you are installing the software for the first time, select "**I want to create a new backup account**". If you have an existing account that you want to reconnect to select the "**I want to reconnect to an existing backup account**" option. Click **Next** to continue.

Note

You cannot connect from different computers to the same backup account. Each computer must have a separate account.



Step 2 of 6

Enter your backup username, password and encryption key, which can be found in your 'Welcome to Online Data Backup' email.

Note

For security reasons, please change your password and encryption key prior to performing your first backup.

The password and encryption key can be changed within the ZenVault software by clicking on "**Tools**", "**Options**" and selecting the "**Account and Security Tab**". The backup username and password can consist of any keyboard combination between 4 and 20 characters. The encryption key can be any keyboard combination between 8 and 56 characters. Click **Next**.

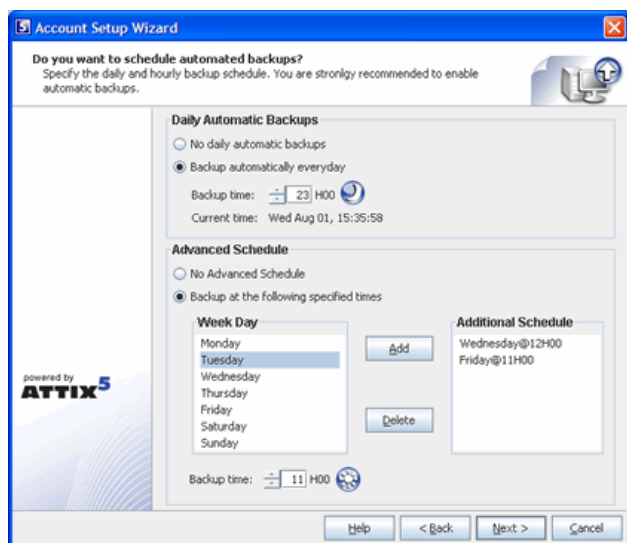
IMPORTANT INFORMATION

Please note that we only keep a record of the **original encryption key**. We do not store the original password. In order to ensure maximum security, we recommend that you change both the encryption key and the password prior to your first data backup.

In the event that you lose your encryption key, we can provide the original. However, if you have chosen to change the encryption key, the original will be of no use. In this case, **please make a note of the changed encryption key and keep it in a secure location**. Should you forget your encryption key and lose access to your data, we cannot re-enable access to your data.

Step 3 of 6

Select the connection type that you want to use to connect to the Storage Platform. Use the **Configure Proxy** button to specify any Proxy settings needed for communications to the Internet. Click **Next** to continue. If you select the modem/dialup connection, the next step will prompt you to supply the connection that you want to use.



Step 4 of 6

In this step you can configure the daily and hourly automatic backup schedule. The default backup time is 19h00. It is advised to backup at night when the server is not in use. The server must be powered at the time of scheduled backups, but you do not have to be logged in.

Note

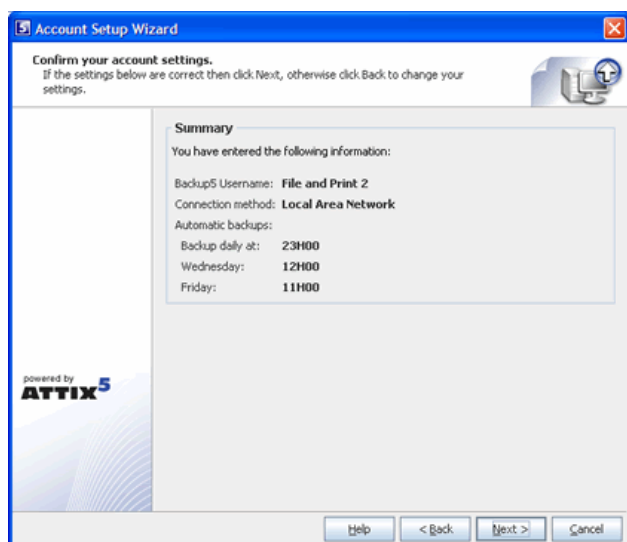
If you do not schedule any backups, you will have to manually backup your data. We strongly recommend that you run automated backups.

Step 5 of 6

If you have limited space on the drive where the Backup Client is installed, you can move the Cache, Logs, Temporary folders and the selection database to another location.

Note

Always keep these folders and the selection database on the same drive/volume.



Step 6 of 6

Confirm that the information you supplied is correct, and click **Next**.

The Backup Client will connect to the Storage Platform and configure your account. A message will be displayed to confirm that your account was created successfully. Click **OK** to close the message box. Next, you must select files and folders, to create your selection list.

2.2 Backup Monitor

The Backup Monitor must be launched when your Mac is started to initiate automatic backups in the background at the scheduled times. Note that with the online data backup service, you do have to be logged in, in order for the scheduled backups to take place.

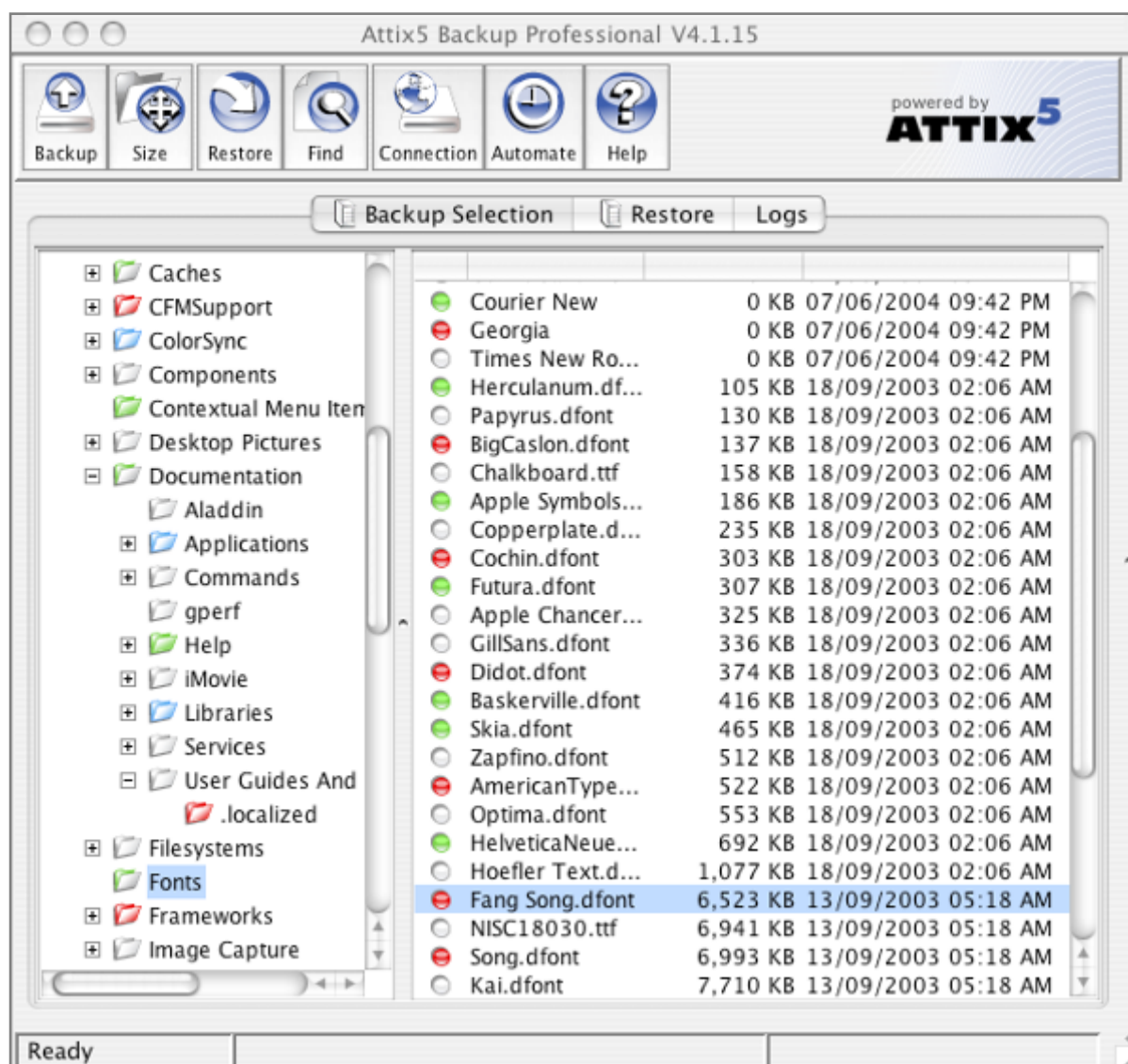


To add the Backup Monitor to the list of applications to start during the login process, open the **Backup Monitor** from the **Applications** folder. Click on the tray icon and select **Launch at Login**.

The Online Data Backup client can be opened from the Backup Monitor. Click and hold on the Backup Monitor icon in the Dock until a menu is displayed and click **Open**.

3 Backup Client

Online Data Backup keeps your most valued data secure. It allows you to select files and initiate backups, and to restore lost or corrupted files. You can also find and restore files from previous backups and schedule automatic backups.




While you are using the Backup Client, you may select **Help** from the **Help** menu, should you require any help. This additional windowpane on the right of the window above, will guide you through the operation of the Backup Client.



How to Backup

The next sections describe how to select files and folders for backup, how to add filters to folders to automate the file selection of certain file types, and how to backup your files to the Storage Platform.


3.1 Selecting files for backup

To select files that you would like to backup, click on the  **Backup Selection** tab. The folder structure of your computer is displayed in the left-hand pane. If you click on a folder, its contents will be displayed in the right-hand pane. Subfolders are only shown in the left-hand pane. Once a file or folder is selected for backup any changes, additions or deletions to that file or folder are automatically backed up.




3.1.1 To select an individual file

Browse to the individual file that you would like to backup. In the right-hand pane, Command-click on the file and choose **Select** or click in the box next to the file. A selected file is displayed with a  green icon. To deselect a file you can either Command-click on the box again or Command-click on the file and **Deselect** it. Folders that have some files selected are displayed with a  green tint.

3.1.2 To select an entire folder

Ctrl-click on the folder and select **Include Folder**. Included folders are displayed with a  green folder. All files in the included folder and its subfolders are now selected for backup. Any changes made within this folder or its subfolders will automatically be included as well. To deselect a folder, Ctrl-click on the folder name and select **Deselect Folder** from the selection list.

3.1.3 To exclude a file or folder

If an entire folder is included but you want to exclude a particular file or subfolder, Ctrl-click on the file or folder and select **Exclude**. Excluded items are displayed with  red icons or  red folders. Folders that have been selected but have some files or subfolders excluded are green with a red  tint.

To verify the size of your backup, select **Calculate Size** from the **File** menu or click on the **Size** button in the toolbar. If your backup set is larger than your allocated limit you have to reduce the size of your selection. To remove files, Ctrl-click on a file that you want to exclude and click on **Deselect**. Alternatively, you can ask your backup administrator to upgrade your account limit.

Note

The Backup Client compares your backup account size with the size of your backup selection at the beginning of the backup process. The backup process will stop and an error message will be displayed if the selection size is over your account limit.

If you do not want to wait for the next automated backup, you can select **Backup Now** from the toolbar to manually start the backup process.



3.2 Filters

You can use filters to automate the file selection of particular file types from a specific folder and its subfolders. For example, a *.doc filter will include all existing Word documents, as well as any new Word documents that may be added later. To add a filter to a specific folder, Ctrl-click on the folder, select **Filters** and choose one of the available filters from the list.







A few filters have been provided for you to start with. You can create, modify and delete any of the filters. To modify a filter, Ctrl-click on any folder, select **Filters** and click on **Edit filters**. Select one of the filters and Add or Remove any of the file types. The **New filter** option allows you to add additional filters. Supply a name that describes the filter and then enter the file type(s).

Example

AutoCAD users may want to only select their drawing files as the rest are generated by AutoCAD and do not need to be backed up. The filter could be called Drawings and the filter type would be *.dwg.

Files that are included by applying a filter are displayed with the green selection icons with a blue checkbox, e.g.  for files, and  for folders. Filtered files or folders cannot be deselected, but you can exclude particular filtered files or folders by Ctrl-clicking on the file or folder and then selecting **Exclude**. A filtered folder with exclusions is displayed with a red tint. More than one filter can be applied to a specific folder. To remove filters from a folder, right-click on the folder, select **Filters** and clear the checkbox next to the specific filter(s) that you want to remove.

3.3 Profiled Sections

You may notice another group of icons in the Backup Client. Dynamic Profiling selections, which can be specified by the Backup Administrator, are displayed with the following images:  for file inclusions,  for filtered inclusions and  for excluded files. On folder level, the images are  for included folders,  for filtered folders, and  for excluded folders.

3.4 Manual Backups

After you have selected the files and folders for backup, you can manually initiate the backup process by selecting **Backup Now** from the File menu or by clicking on the **Backup** button in the toolbar. You **may** close the Backup Client after you have started the backup process by clicking **Hide**. This will not cancel the backup process and you can at any stage open the Backup Client to view the progress of the backup. Backup log information can be viewed in the **Logs** tab. Backup entries are displayed in blue.



3.5 Backup Resume

The Backup Client can try to resume a backup, if the previous request failed for whatever reason. If you select **Backup Now** from the **File** menu or you click on the **Backup** button in the toolbar and the previous backup was not successful, the Backup Client will prompt “*Do you want to resume the failed backup?*” If you select **Yes**, the Backup Client will try to continue from where the process failed during the previous backup. Select **No** to initiate a new backup or **Cancel** to return to the Backup Client.


Note


A new backup will be initiated after the countdown has elapsed.

How to Restore

The next section describes how to select the files that you want to restore, how to search for specific backed up files, and finally how to restore files from the Storage Platform.

3.6 How to restore files and folders

Open the  **Restore** tab. From this tab, you can gain access to your backed up files. Your latest backup is shown in the **Last Backup** folder. If you expand the **Previous Backups** folder, the Backup Client will connect to the Storage Platform and retrieve a list of all previous backup dates.

Select the files and/or folders you want to restore. To select a single file, Command-click on the file and click on **Select** or you can click in the box next to the file. To select an entire folder, Ctrl-click on the folder and then choose **Select folder**. Selected files are displayed with  green icons. To start the restore process, select **Restore** from the **File** menu or click on the **Restore** button in the toolbar.

Note

Automatic backups are disabled during the restore process.

The Backup Client will prompt for a restore location to where the file(s) must be restored. If you select **Original location**, the files will automatically be restored to the same location from where they were backed up.

Note

If you choose this option, the restored files will overwrite any existing files with the same name in that location. You will be warned before the Backup Client overwrites any files.

If you do not want to overwrite the current copy of these files, select the **Folder** option. The default path is a **Restore** subdirectory in your user account (home) folder. You can also **Browse** to another folder if you want to restore the files to a different location.

3.6.1 Restore Options

Option	Explanation
Recreate directory structure	<p>By default, the folder structure is recreated in the restore folder. If you want all files to be restored to one location, uncheck the Recreate folder structure option.</p> <p>Note <i>If you are restoring files from different folders with the same filename, you must recreate the folder structure or they will overwrite each other.</i></p>

Restore empty folders	You can choose whether empty folders must be created if the Recreate directory structure option is enabled.
Overwrite files	Enable this option if you do not want the Backup Client to prompt you before overwriting an existing file.
Use compression (faster over the Internet)	<p>Tick the Use compression option to enable compression. With this setting enabled, the Storage Platform will compress the files before transferring them to the Backup Client.</p> <p>Note</p> <p><i>You are advised to always enable this setting if you have a slow connection to the Internet as the files are smaller with this option enabled.</i></p>

Restore log information can be viewed in the Logs tab. Restore entries are displayed in green.

3.7 Finding Files

The **Find files in Backups** option enables you to search through your previous backups to find a specific file. You have the option to do a local search from your last backup, or you can connect to the Storage Platform to search through your previous backups.

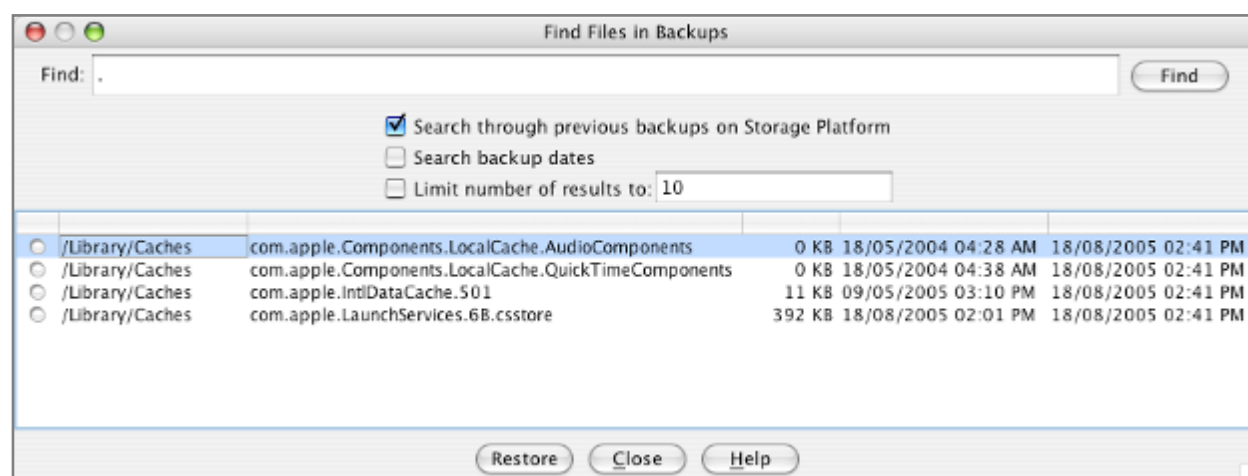
To search for a file from your latest backup, select **Find files in backups** from the **File** menu or click on the **Find** button in the toolbar. Enter the filename in the textbox and click on **Find**.

Example

If you enter *help* in the textbox, the Backup Client will display a list of all backed up files from your last backup that contain help in either the filename or the folder.

Note

*You can use the * and ? wildcards for advanced search queries to find the files that you are looking for.*



To search for files from previous backup sets, enable the **Search through previous backups** on server checkbox.



File dates can also be specified and you can and limit the number of results that must be displayed.

Note

The Backup Date is used if you enable Search file dates and not the file create or file modified dates.

To restore the located files, select them individually and then click on the Restore button.

Options and Settings

From this Tools menu item you can view and configure the primary Backup Client options and settings. To open this section, select Options... from the Tools menu. The various options and settings are grouped according to their functions and displayed in different tabs.

Note

Please read through this section carefully before you change any of these settings. Incorrect settings could cause serious problems or even stop the Backup Client from protecting your data.

3.8 Account and Security

3.8.1 Account Information

This section displays your backup account information as it is configured in the Storage Platform. You can use the **Retrieve Settings** button to update your account settings from the Storage Platform. This tool is useful to verify that your account limit has been modified after requesting a change from your Backup Administrator, or to update Backup Group Profiling settings.

3.8.2 Account Setup

If you need to change your password or encryption key, select either the **Change Password** or **Change Encryption Key** buttons. Changing your encryption key involves intensive processing on the Storage Platform and may take several minutes. It should therefore not be done unless your encryption key was compromised.

3.8.3 Security Settings

The Security window allows you to select whether the Backup Client should remember the backup account password when running a backup or a restore.

There are three options available:

- **Remember password for backup and restore:** The Backup Client remembers the user password when doing a backup or restore. This is the default setting.
- **Prompt for password on restore:** The Backup Client prompts for the user password during the restore process.
- **Prompt for password to open the backup client and to restore:** Use this option to enable access control. The Backup Account password must be supplied before you will be able to open the backup client to change the backup selection or any of the application settings. Backups will continue as normal.

3.9 Connections

3.9.1 Connection Settings

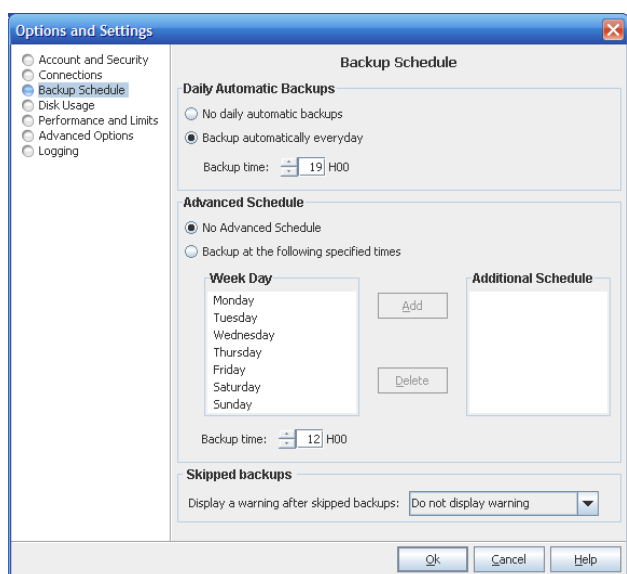
In this section, you can change the connection that the Backup Client must use to connect to the Storage Platform. You can choose between a network/permanent or dial-up connection.

The Dial-up Settings button is enabled if you select the Dial-up option. Click on this button to select an existing dial-up connection configured on the computer, and supply the username and password for that Internet connection.

3.9.2 Proxy Server

Enable the Use a proxy server for you network or dial-up connection checkbox if you connect to the Internet via a proxy server, and supply the necessary information.

3.10 Backup Schedule



The Backup Client can be scheduled to backup your selected files and folders automatically. Note that if you configure the Backup Client to backup at night, the server must be powered, but you do not have to be logged in. The backup schedule can be changed by selecting **Automatic Backups** from the **Tools** menu or by clicking on the **Automate** button in the toolbar.

Use the **Daily Automatic Backups** section to configure a once-off daily backup. The **Advanced Schedule** can be used to specify hourly backups. Backup logs can be viewed in the **Logs** tab. Backup entries are marked in blue.

Note

You are advised not to disable automatic backups as you will then have to manually backup your files.

3.11 Disk Usage

3.11.1 Working Folders

If you have limited space on the drive where the Backup Client is installed, you can move the Cache, Logs, Temporary folders and the selection database to another location. The Temp folder is used for temporary workspace when the files are patched, compressed and encrypted, the Logs folder stores all backup and restore logs, and the Cache folder keeps a local, compressed and encrypted, copy of the selected files for a specified



amount of days. The selection database compares the latest backup selection with the previous backup to determine the changes.

Note

Always keep these folders and the selection database on the same drive. If you move these folders and the database to a network share, please ensure that the Backup Client has the correct permissions to reconnect and write to that share.

3.11.2 Cache

When modifications are made to a file, the Backup Client only transmits the changes to that file, as opposed to transmitting the complete file again. This is accomplished by keeping a compressed copy of the file in a local cache and then using a sophisticated patching technique to extract the difference between the file in the cache and the one ready to be backed up.

Files are only kept in the cache for a certain amount of days. Files are added to the Cache folder if the file was modified within the **Days to keep files in Cache** window. Once a file has been flushed from the cache, a full copy must be backed up when any modifications are made to the file. The longer files are kept in the cache, the better the chance of only transmitting patches instead of full copies and thus reducing the amount of data that needs to be transmitted. If you have limited disk space, you may want to consider shortening the time files are kept in the cache.

Note

If you select 0 days, patching is disabled, any files in the Cache folder will be deleted, and complete files are backed up to the server during each backup.

To delete the current cache, use the **Clear Cache...** button. If you delete the cache, full copies of your selected files will be re-sent to the server during the next backup. You may notice that the Backup Client will log the message *Doing monthly cache cleanup* once a month. This maintenance task is to ensure that the cache folder is up to date by deleting any files that fall outside the **Days to keep files in Cache** window.

3.12 Performance and Limits

3.12.1 Processor Usage and Disk Access

The Backup Client uses a fair portion of the available processor power to patch, compress and encrypt files while during the backup process. If you use the computer at the same time, you may experience some performance deterioration. You can lessen this effect by lowering the **Processor Usage**.

Disk Access is another setting that you can modify to limit performance deterioration. If this setting is set to high, the Backup Client will continuously use all available disk access to write to the disk, ensuring that the process completes as fast as possible. The process will take longer if you lower this setting but your other applications will function without any interruptions.

3.12.2 Limits

Outgoing transfer limit - The outgoing transfer bandwidth can be limited (in Kilobytes/second) in case you need to allocate only a certain amount of bandwidth to the Backup Client.

Backup size restriction - You can limit the total amount of data that may be transferred during each backup.

Note

If you enable this option, it may take several backups before all your files are backed up to the Storage Platform. This feature is especially useful if you have a poor Internet connection and you encounter problems with transferring large backups.

3.13 Advanced Options

3.13.1 Options and Retries

The Backup Client can be configured to **Always connect to the Storage Platform** during each backup to update its last backup date stamp, even if there were no changes made to the backup set. With this setting enabled, the Storage Platform will always be up to date with the latest backup date.

Number of Backup/Restore attempts before cancelling

By default, the Backup Client tries to connect to the Storage Platform four times before cancelling the backup process. If you have a poor connection to the Internet, you may want to consider increasing the number of attempts. The backup will continue from the previous point of failure. It will not resend the entire backup.

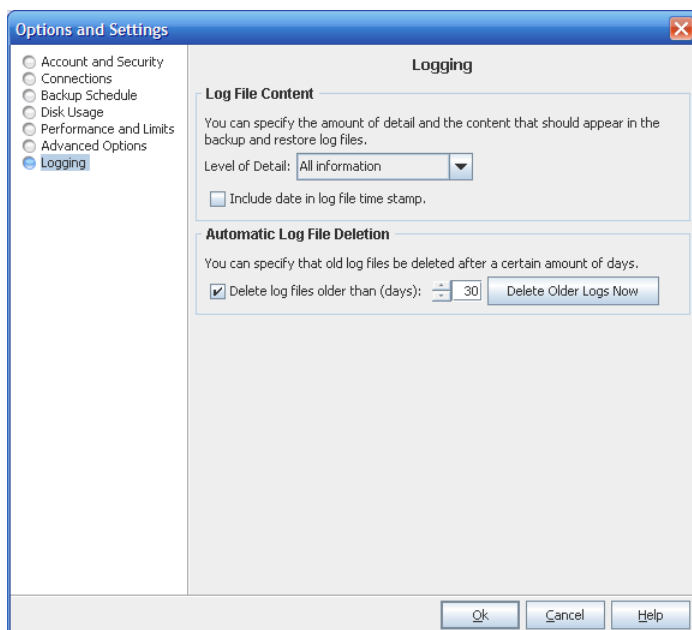
Connection Retries

By default, the Backup Client will try to reconnect to the Storage Platform after 60 seconds, should the connection be dropped. This setting enables you to increase/ decrease the duration between the retries.

Socket Timeout

The socket timeout is, by default, 60 seconds. If the Backup Client is connected to the Storage Platform and there is no communications between the two, this amount (in seconds) is the duration that the Backup Client will stay connected before dropping the connection.

3.14 Logging



The Logs tab in the backup client provides detailed information about each backup and restore. This section enables you to modify the structure of these log files. You will notice an additional toolbar button when you open the Logs tab; the Summary button can filter the information to only display the last 14 lines.

Log File Content

You can specify the level of information that must be included in the log files. Choose between:

- Log all messages
- Suppress detail messages
- Only log errors and warnings

Enable the Include date in log file time stamp checkbox to add the date to the backup and restore log files.

Automatic Log File Deletion

A log file retention period can be enabled to delete files older than e.g. 30 days by enabling the checkbox and specifying the duration in days.

Additional Settings

The **Tools** menu provides you with various options and settings that you can modify to enhance and streamline your Backup Client. You can also modify your account settings from this menu.

3.15 Remote Management

Remote Management enables you to remotely access and configure the Backup Client from the Storage Platform Console.

To enable this feature, select **Remote Management** from the Tools menu and enable the checkbox next to **Enable Remote Management**. The **Allow SP controlled access** option enables backup administrators with the correct access permissions to use their Storage Platform User Access Management username and password to connect to and administer this Backup Client. If you disable this checkbox, Storage Platform administrators will not have remote access.

Specify the port number (the default port is 9091) that must be used for Remote Management. If the server has multiple IP addresses available, you can specify whether the Remote Service must bind to **All** or **Only** to one IP by specifying the address in the textbox.

Enable the **Allow custom access** option and supply a username and password if you do not want to make use of the above-mentioned Storage Platform Access Accounts. This custom access username and password must be specified in the Storage Platform Console to gain remote access. Click Ok to save your settings. After the service has been restarted, click on Ok to close the window.

3.16 Health Check

The Backup Client Health Check provides information to pre-emptively highlight possible issues, for example free disk space problems or SE service access rights to files and folders. It can also provide the estimated line speed to the Storage Platform.

Five sections are available:

- **Memory** – Memory utilisation statistics from the last backup as well as overall memory usage to date.
- **Data Protected** – Information includes the number of files and directories selected for backup.
- **Disk Usage** – Free space availability for all local drives.
- **Line Speed** – Line Speed estimate to the FileServer by transmitting data for 10 seconds.
- **Service Rights** – Information about the service account name and access rights to the working folders.



You can decide which checks you want to run by enabling/disabling the checkboxes next to the entries. Use the **Show Last Health Check** button to see the last report. You have the option either Print or **Export** the Health Check reports.

3.17 Dynamic Profiling

Dynamic Profiling enables your Backup Administrator to propagate certain client side settings from the Storage Platform to your Backup Client.

Note

These settings take priority over any settings specified in the Backup Client.

These settings include:

- *Changing the backup schedule*
- *Specifying system file exclusions*
- *Adding additional filters to the filter list*

When the Backup Client connects to the Storage Platform, it will receive a list of any Dynamic Profiling settings specified by the Backup Administrator and these changes will be implemented in the Backup Client. If you modify any of these settings with Dynamic Profiling enabled, it will revert back to the Dynamic Profiling settings during each backup.

3.18 Language

If multiple languages are available, the Backup Client will select and display the default OS language. You have the option to change this setting. From the **View** Menu, go to **Languages** and select one of the available options.

3.19 Look and Feel

You have the option to change the look and feel of the Backup Client. From the **View** Menu, go to **Look & Feel** and select one of the available options.



4 Security

The Online Data Backup service uses a combination of Blowfish encryption and SSL secure data transmission to ensure the safety of your data.

When the Backup Client has to transfer data to the Storage Platform, it connects using a secure SSL (1024 bit RSA key exchange, 128 bit RCA stream cipher and SHA-1 integrity checking) connection to transfer the data. Signed SSL certificates and Certificate Revocation Lists (CRLs) are used to verify server integrity. Data is stored using 448-bit Blowfish encryption to encode the data on the Server. This is considerably greater than the encryption used for Internet banking and online credit card transactions.

Your encryption key is seen as a passphrase by the Storage Platform. A random encryption key is automatically generated when any account is created and this random key (and not the passphrase specified by you) is used to encrypt your files. The encryption key is protected by the passphrase (your encryption key) and without this passphrase you cannot decode the actual encryption key. When you change the encryption key in the Backup Client, the actual key is decrypted and re-encrypted with the new passphrase.

The data is never touched. All data since the initial backup is encrypted with the same random encryption key even when the passphrase is changed. If you change your encryption key, you do not have to remember the previous encryption keys for future restores – the Backup Client will be able to retrieve the data from the Storage Platform.

Your encryption key is not stored anywhere on the Storage Platform, and is only known to you. If you forget this encryption key, it will render your data unrecoverable.

Security standards and techniques employed by our Online Data Backup service were audited by PricewaterhouseCoopers to ensure that sensitive corporate data remains safe from prying eyes when transferred over the Internet or stored on a server.

4.1 Blowfish Encryption

Blowfish is an encryption algorithm. It is a symmetric block cipher, which uses a variable-length key from 32 bits to 448 bits. The Online Data Backup service uses the maximum strength 448-bit key.

4.2 SSL Communication

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of data transmission. Online Data Backup makes use of the SSL protocol (1024 bit RSA key exchange, 128 bit RC4 stream cipher and SHA-1 integrity checking) for secure communication between the Backup Clients and the Storage Platform, including data transmission.