Offsite SAN Remote Backup Service
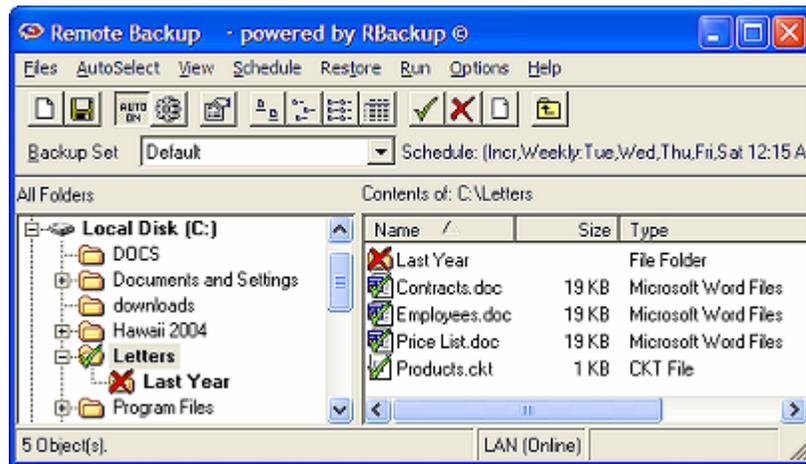
Client User Guide

Table of Contents

Remote Backup Online Client User Guide

Remote Backup is the latest in a family of software and services that founded and defined the Remote Backup industry for microcomputers in 1987. It automatically backs up your critical computer files to a secure, off-site location, giving you the confidence and security big companies have enjoyed for decades.

Remote Backup runs on all 32-bit Windows operating systems including Windows 95, 98, NT, 2000, 2003, ME and XP. It runs in the background, and will not interfere with other programs you run. Through Remote Backup's simple and intuitive user interface, you can control which of your files are backed up, and on what schedule.

Remote Backup operates by defining *Backup Sets*, which are sets of files and a schedule for backing up those files. You can add new Backup Sets, Delete, Copy, and Save them. Backup Sets are automatically executed by Remote Backup according to their schedules.

How Does Remote Backup Work?

Remote Backup works basically like regular data backup software, with one important difference. Instead of sending backups to a tape drive or other media attached to the computer it is backing up, Remote Backup sends the backup over the Internet, regular telephone lines or network connections to another computer safely offsite. It does this (usually) at night while your computers aren't being used.

It's completely automatic. In fact, you may even forget it's working. Most businesses put their lives on the line every night and don't realize it. With businesses depending more and more on the data stored in their computers, proper backups are becoming much more critical.

Remote Backup accomplishes several essential steps that are often overlooked or done improperly by other backup software - especially in the regular non-automated backup systems.

Backups are done on schedule, reliably. Most businesses don't do this. For one reason or another, they don't keep a regular backup regimen. Usually it's because the person responsible for doing backups (if there is one) is too busy doing something else, or someone is using the computer when it's time for a backup, or they simply forget. Since Remote Backups are done with automated software usually at night, when nobody is using the computer, backups are always done on schedule.

The correct files are backed up. Ordinary backup software is often installed with a list of files to be backed up. This set of files usually represents the state of the system when the software was installed, and often misses critical files. Further, it often fails to back up files that get added later. Compounding this problem, VERY few businesses take the trouble to reset their backup software regularly to include new files.

Remote Backup solves this problem by constantly reevaluating your computer system, adding files to the backup as needed. Multiple copies of files are stored using a sophisticated version control system unavailable in most other backup software of any kind. This is much too important to overlook.

Proper Backups

The general definition of "proper" backups requires redundancy. One must keep multiple copies of the same files at different points in their development, called *versions*. As an example, you should have a different copy of each backed-up file for each backup session. Further, you should be able to easily restore any of your files up to any given point in time. Banks do it, big corporations do it, and so should small businesses. Only Remote Backup has such an easy to use version control system.

Backups are encrypted for complete security. Would you want someone to be able to slip one of your backup tapes into a pocket and take it to your competitor? It happens all the time. Tape backups are not generally encrypted, so anyone can read them and gain access to your client database, billing records, payroll, tax info, and everything else on your computer.

Remote Backup encrypts its backups for complete security so nobody, not even your Backup Service Provider can read your files. Finally and most importantly - Backups are immediately sent offsite and stored safely away from your computer and your business. This is where almost every business makes its biggest mistake. Even if you do everything else perfectly, your backups are of little use if your building burns or you are unable to physically recover your tapes from the premises. Most small companies who do backups leave the tapes in the building with the computer, where they can be destroyed right along with the computer.

Of course, you can see that this would be a problem in a fire or flood or an earthquake. But it's also useful in emergencies where businesses are forced to evacuate their offices quickly. Even businesses that do backups and have good, undamaged tapes have to shut down. Many go out of business simply because they don't have access to their data.

Remote Backup solves this problem by automatically storing this valuable data at more than one site. So, a business can be back up and running with new computers and their latest data no matter what catastrophe happens.

Three Major Data Backup Concerns

Security - Data are encrypted before transmission to the off-site storage facility. It is impossible for your Remote Backup Service provider to view your data. It is impossible for anyone to intercept and view your data while it is in transit. You can be sure that your data are completely safe from view. Your files are encrypted with an encryption key known only to you.

Consistency - To be useful, backups *must* be done regularly, on a proper schedule. Remote Backup runs automatically. All you have to do to make sure you get proper backups is to leave your computer turned on. Remote Backup takes care of the rest.

Reliability - You must be able to accurately and repeatedly back up and store your data. Remote Backup's transmission protocol has a built-in method for resuming interrupted transmissions. If a transmission is interrupted halfway through the session, the computer will save the part of the backup session that was transmitted, and resume the transmission with almost no loss of time during the next session.

How Remote Backup Works

Remote Backup has many advanced features. It is the most mature product of its kind, the acknowledged industry leader. Remote Backup runs on all versions of 32-bit Windows, including Windows-95, 98, NT, 2000, 2003, ME, and XP. It works with all networks, including Novell Netware and all Windows networks.

After you install Remote Backup, you will simply leave your computer on at night. Remote Backup "hides" in the background without interfering with any other program. You will notice the Remote Backup icon on the System Tray.

At a predetermined time, Remote Backup "wakes up" and determines which files need backing up, and what kind of backup (out of three possibilities) is scheduled for that night. It then compresses those files into archives that can in many cases be only 10% to 20% of the original file sizes. These archives are then encrypted using an encryption key known only to you.

After your files are compressed and encrypted, Remote Backup activates your Internet connection, modem or other communications device and sends your files off-site to your Service Provider's storage facility. Remote Backup then verifies your files and goes back to sleep.

Your valuable computer files are now safe off-site. If your building burns, or your computer is stolen, your business can be saved by replacing your equipment and restoring your files from the Remote Backup Server.

Backup Sets

Remote Backup saves most of the information it needs in Backup Sets. Each Backup Set can define a set of files to backup, exclude or ignore. It contains a schedule for backing up those files and other options. Remote Backup "runs" its Backup Sets like programs, all at the same time. You can define Backup Sets with an almost unlimited combination of files, schedules and options. Remote Backup will run each Backup Set on schedule, independently.

Creating a New Backup Set

Files:New - This menu option is used to create a new Backup Set. Remote Backup comes with Default Backup Sets. You can create others. Each contains a set of files to be included or excluded from backups.

When you select **Files:New** you will be prompted to enter the name of your new Backup Set. Your new Backup Set will then be created with the file attributes of the currently selected Backup Set. In other words, the current Backup Set will be "cloned" to create a Backup Set with a new name – but the same file selections.

Your new Backup Set will then be automatically selected as the current Backup Set.

Important: The data retention policy of any new Backup Set assumes the default values specified by your Backup Service Provider.
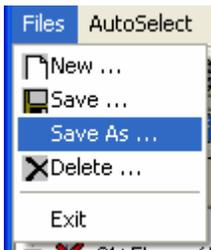
Saving a Backup Set

Files:Save - This menu option is used to save modifications you have made to a Backup Set. Selecting it will write your modifications back to your hard drive.
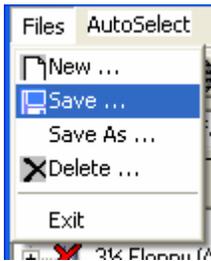

Saving A Backup Set With A New Name

Files:Save As - Use this menu option to save the current Backup Set as a different name. This is similar to Files:New - Creating A New File Set except that instead of the Blank Backup Set being cloned with a new name, the *currently selected Backup Set* is cloned.
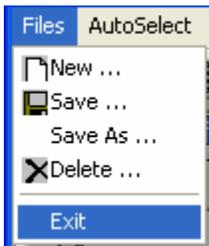
Deleting A Backup Set

Files:Delete - Select this menu option to delete the current Backup Set.
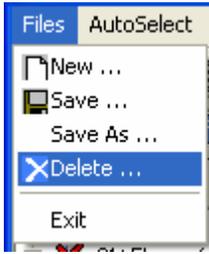
Exiting Remote Backup

Files:Exit - This menu option will exit Remote Backup and remove it from memory and from the System Tray. It will stop Remote Backup from performing backups.
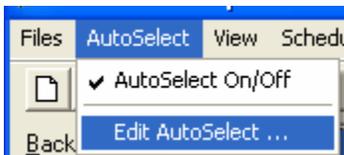

AutoSelect

AutoSelect is one of the most powerful features in this software. It allows you to select or exclude files for backup depending on which software application they belong to. For example, with one simple selection you can back up all Microsoft Word documents throughout your drive, regardless what folder they are in.
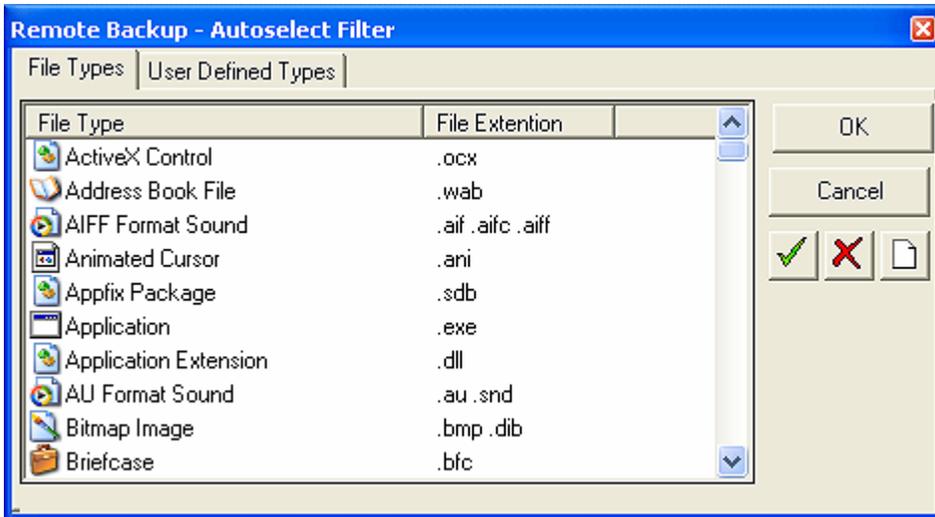
In addition to backing up existing files, AutoSelect picks up files that are added later and automatically adds them to your backups.

There are two ways to use AutoSelect. Both ways require AutoSelect to be turned ON.
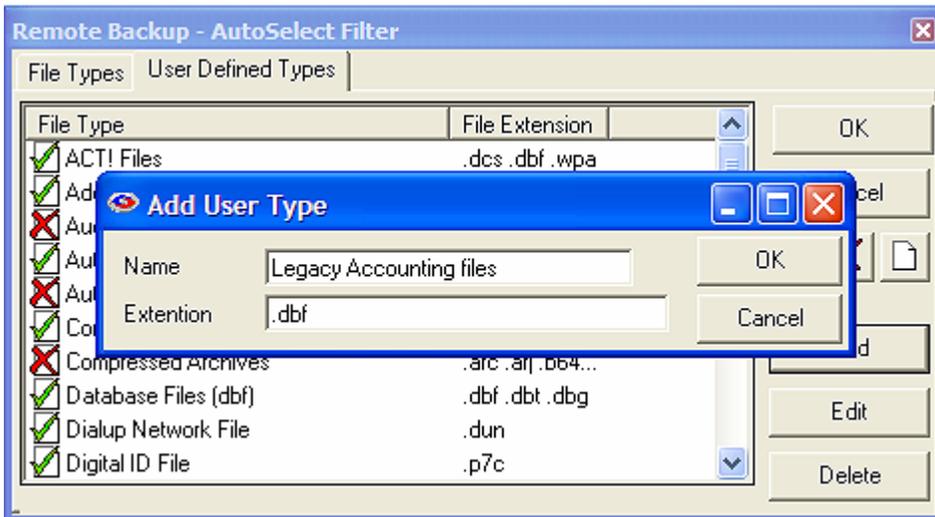
AutoSelect from Menu

With AutoSelect turned ON you can edit the file selections by picking **Edit Autoselect**.

This menu lists all the file types on your computer, in all folders. Right-click on any file type to pick from a menu that lets you include, exclude, or ignore files. You can also highlight a file or group of file types and pick one of the buttons on the right of the screen.
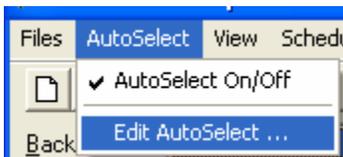
Using the User Defined tab you can add your own file types. There are still many software programs in use which predate Microsoft Windows, and so they might not appear on the AutoSelect's main File Types tab. To add your own file types, click the ADD button.

After adding your new file types you can then select them to include, exclude, or ignore, the same as with all the other file selections.

AutoSelect from Right-Click

Many people find the Right-Click method of AutoSelect easier to work with.
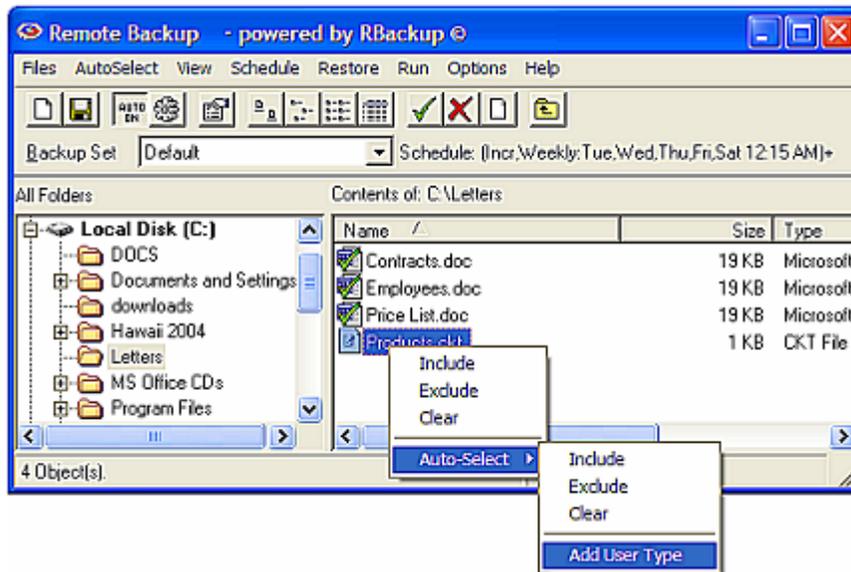
With AutoSelect ON, right-click on any file in the right pane of the normal file selection screen. You will see an AutoSelect menu. Select Include, Exclude, or Clear. You can add the file type you selected to the AutoSelect system and back up all similar file types. If the file type you have selected is already in the AutoSelect list, you can Edit or Delete it here.

More help for selecting files can be found in File Selection Tips and Tricks.
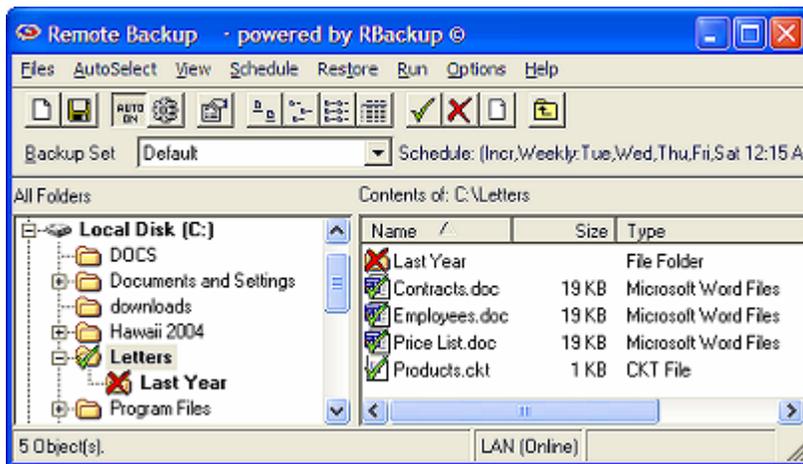
File Selection Screen

The File Selection Screen is the main screen for Remote Backup. It works like the standard Windows Explorer interface. The left pane contains a display of your drives and folders, and the right pane contains more detail on what you have selected in the left pane – usually a list of folders and files.

To select drives, folders, and files to back up or exclude from backups, use the right pane. Left-click over the item you want to mark, then select one of the buttons indicating the green check, the red X or the blank box. You may also use your right mouse button for a menu.

When you place a mark on a folder or drive in the right pane, your selection takes place for all folders and directories within the one you selected. For example, if you place a green check on a folder, all folders and files in that folder will be backed up.

If you place a red X over a folder, every folder and file in that folder will be excluded from the backup.

Once a drive or folder is marked, you can open it and see that many, if not all, of the folders and files within it are marked with the same mark.

This is where things get a bit tricky.

The red X takes precedent over all other marks. If you place a red X over a drive or folder, you will not be able to open that folder and change any of the red X marks.

However, you *can* change the marks on folders and files within drives and folders that have a green check or a blank box.

Within these constraints, you can change any mark on any drive, file, or folder.

More help for selecting files can be found in File Selection Tips and Tricks.

As with most Windows programs, you can click on the column headings in the right pane to sort the display. By default the display is sorted by file name with folders first.

Selecting a Backup Set

The file Selection screen includes a drop-down selection for Backup Sets. Click the Down Arrow to the right of this field to select a different Backup Set. If you have changed the current Backup Set, you may be asked if you'd like to save your work.
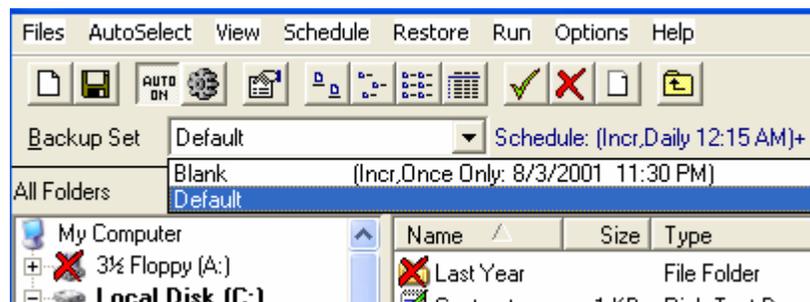
Schedule Menu

This is where you define the dates and times for your Backup Sets to run. The screen has a pull-down menu that you can use to select your Backup Set. It also contains a box called Backup Type, which is where you select the type of backup you will do. Options include:

Incremental – Files will be backed up which have been modified since the last backup. Then, after they are backed up, the files will be marked on the disk as having been backed up. This is the default and most widely-used way to back up data files.

Differential – Files will be backed up which have been modified since the last backup, the same as Incremental. However, after the files are backed up, they will *not* be marked as having been backed up. The reason for this option is in case you also want to do tape backups as well as remote backups. Your tape backup software relies on the marks placed on the files to determine which files need to be backed up. So, you don't want to remove them with your Remote Backup.

**Full** – Files will be backed up regardless of whether they have been changed since their last backup. This is the least-used option because it results in the largest Backup Sets and longest on-line times.
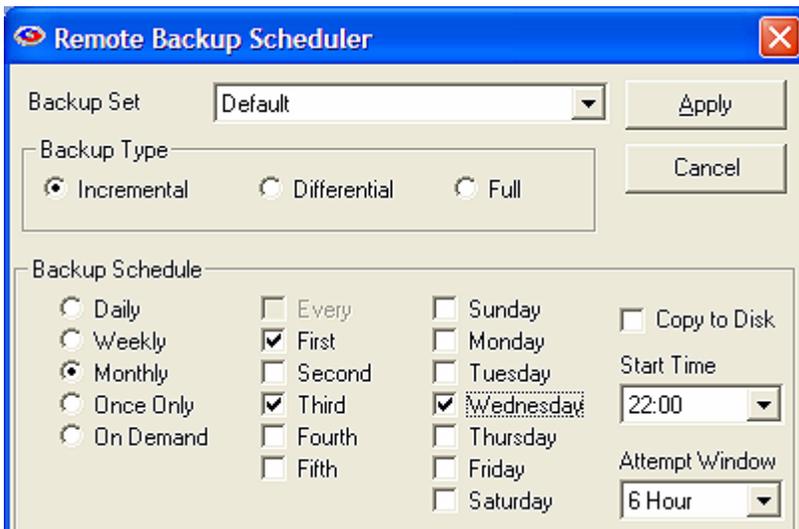
Backup Schedule Options

There's also a box labeled Backup Schedule. Here you can select different schedule types.
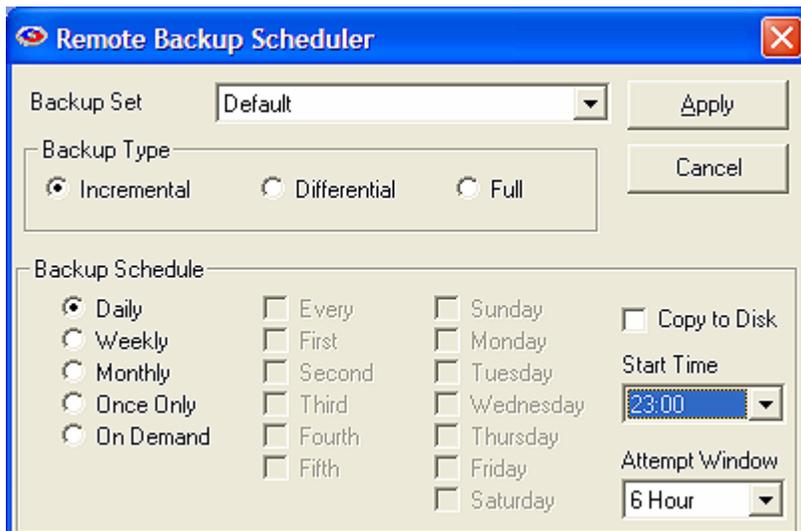
Daily – Selecting this option will launch a backup every day, seven days a week.
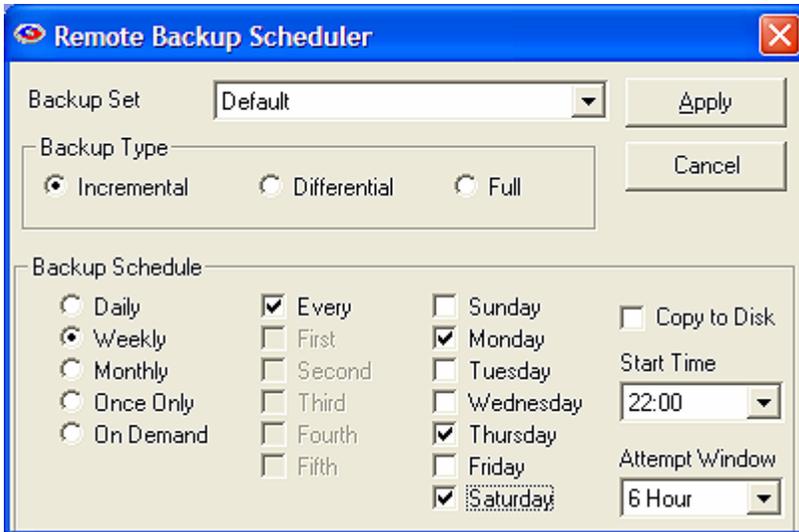
Weekly – This schedule lets you select which days of the week to do a backup. You can select to do a backup every Monday, Thursday, and Saturday.

Monthly – On this schedule you can select the first, second, third, fourth or fifth of any day of the week. Here are some examples: You can pick the first and third Wednesdays of each month. You can select the second Tuesday and Thursdays. There are a lot of possible schedules you can use here.
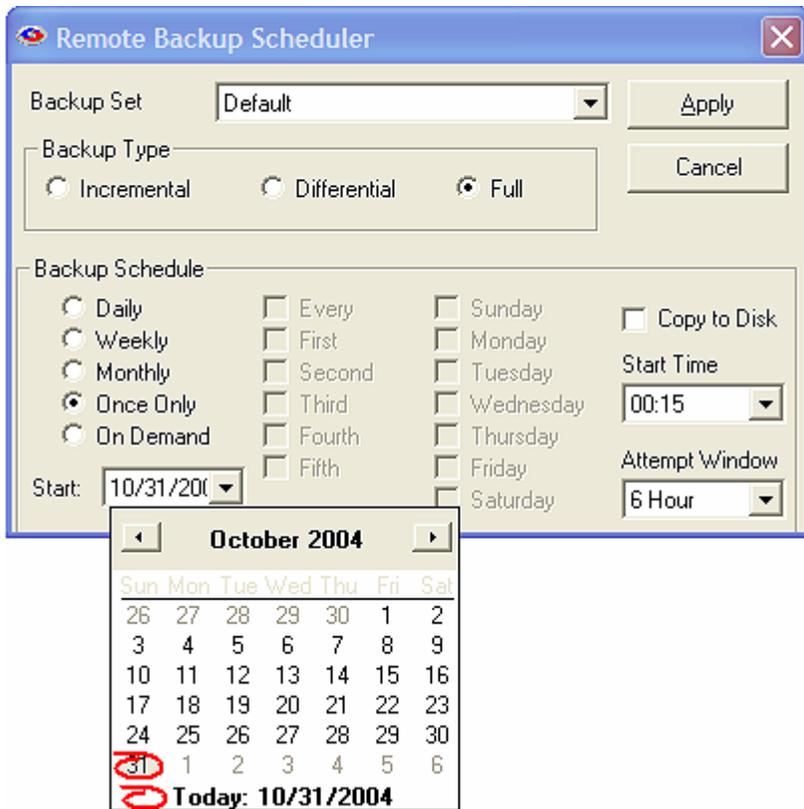
Once Only – This schedule will launch a single backup session, one time only, on a specified date you can pick from a pull-down menu containing a calendar.
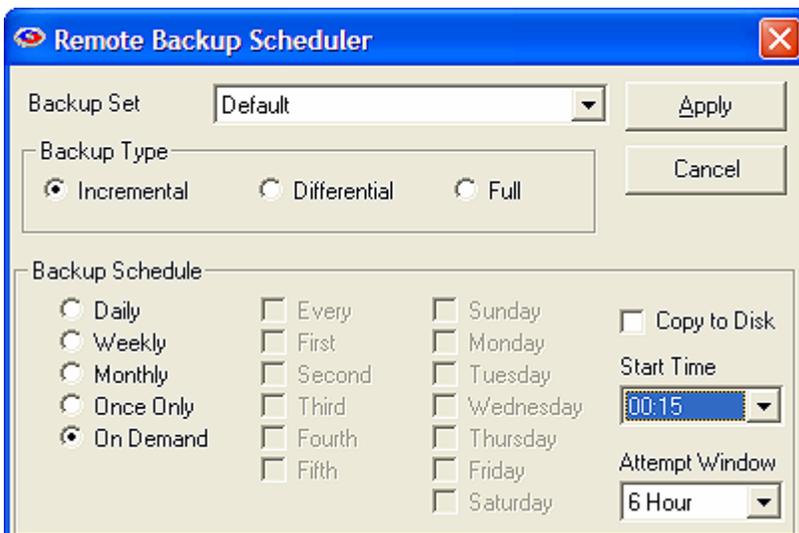
On Demand - Pick this selection if you want this backup set to be launched On Demand only - not through the scheduler. You can then launch this backup set through the **Run: Run Now** menu choice.
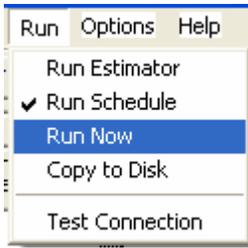
Backup Start Time and Window

For each of these schedules you can select a Start Time and an Attempt Window. Please be aware the Start Time is on a 24-hour schedule, and that anything after midnight is the next day. What this means is that if you want to back up Friday's work, and you want the backup session to take place after midnight, <u>you should select a time early in the morning of Saturday, not Friday.</u>

The Attempt Window is the number of hours Remote Backup will attempt to perform the backup. Selecting a start time of, for example, 1:00am will not necessarily cause the backup session to start at 1:00am, although it might. Remote Backup might not be able to perform a backup for a variety of reasons – the Server is too busy, files are locked, the computer isn't turned on.

In the event that Remote Backup can't perform a backup at the selected Start Time, it will attempt the backup session some time during the next period of time determined by the number of hours you select here.

File Restore

Select this menu choice when you want to restore files. The menu choices allow you to select files to restore, or to specify a location to redirect your files, in case you want to put them somewhere other than where they came from when they were backed up.
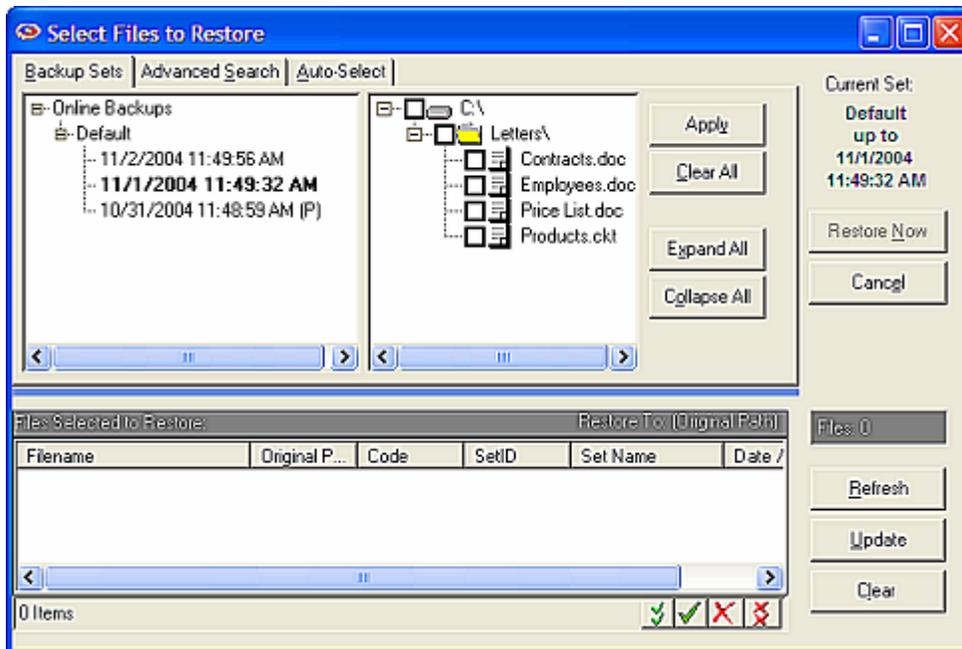
This is the main Restore screen. The left pane contains a list of your named Backup Sessions. The ones with a plus sign (+) beside them have backed-up data associated with them. Click on the plus sign to open the Session List.

Under each Session is a list of backup sessions that have been performed. They have the dates and times they were performed, in ascending order of oldest to most recent.

Double-click on a session to display its contents in the right pane. As with the standard explorer interface, you can click on the plus signs (+) to open the tree view of the backup session to further explore it.

Restore Selection Options

You can click the Expand All button to expand the entire tree view, then scroll through it to see what is in the particular Backup Set. To select a drive, directory, or file to restore, click on the box next to its icon. To deselect a drive, directory, or file, click on its green check to clear it.

Note that if you mark or unmark a drive or folder, all items below it become automatically marked or unmarked.

The **Collapse All** button does the opposite of the **Expand All** button. Click it to collapse the tree view.

To select all files in the currently selected set, click **Select All**.

To deselect all files in the currently selected set, click **Deselect All**.

Click the **Apply** button to apply changes as you make them. Your list of files to restore is displayed in the window at the bottom of the screen.

After you have selected all the files you want to restore, click the **Restore Now** button to begin the restore process, or pick the **Cancel** button to cancel your Restore process.
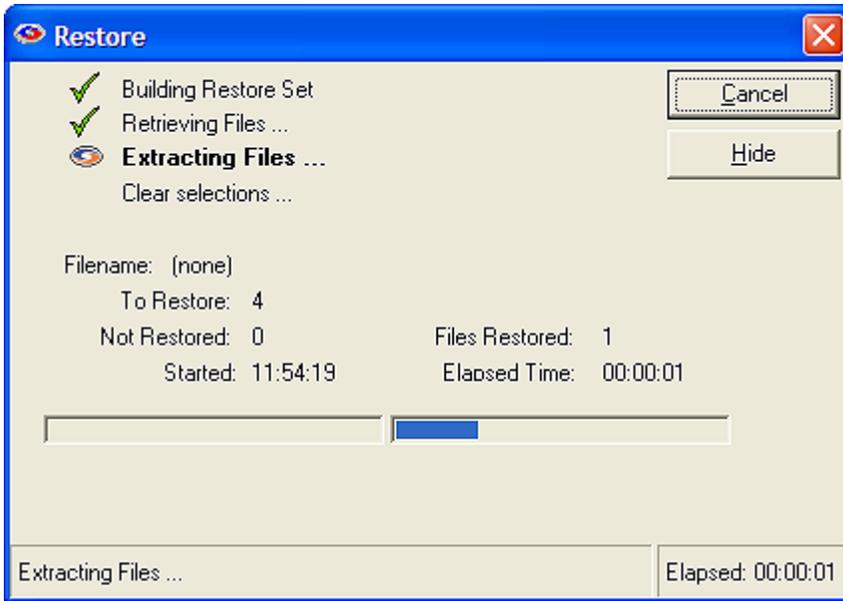
During the restore process you'll see this progress screen. When the restore process is finished you'll see the following screen:
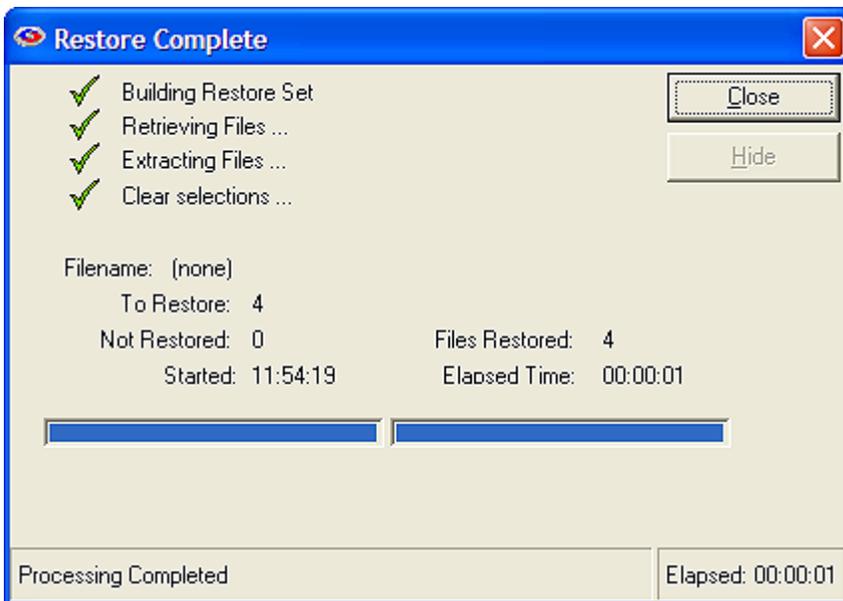
You can also select files for restore by using the **Advanced Search** tab and the **Auto-Select** tab.

Restore - Advanced Search

The Advanced Search feature allows you to find files by using key words and character strings that appear within the file names. For example, if you want to restore a "price list" file, pick the Advanced Search tab, and enter "price list" in the **Find By Mask** field.
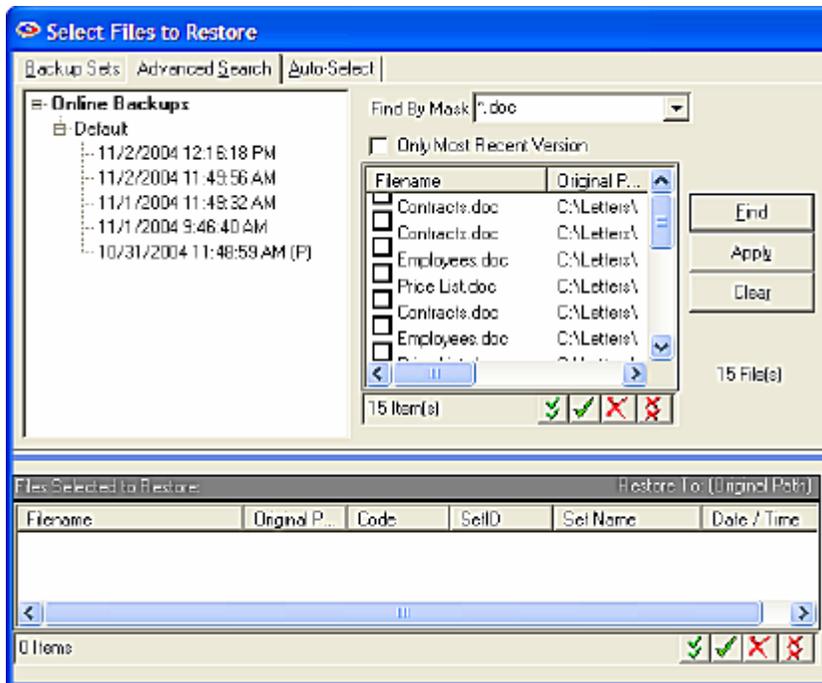
Select the **Only Most Recent** Version checkbox if you only want to display the most recent version of all files found. This is an excellent way to very quickly restore only the most recent version of files, regardless which backup set thee belong to, or when they were backed up.

To restore the latest version of all *Microsoft Word* files that end in ".doc" enter, ".doc" in the **Find By Mask** field, select the **Only Most Recent Version** checkbox, and click the **Find** button.
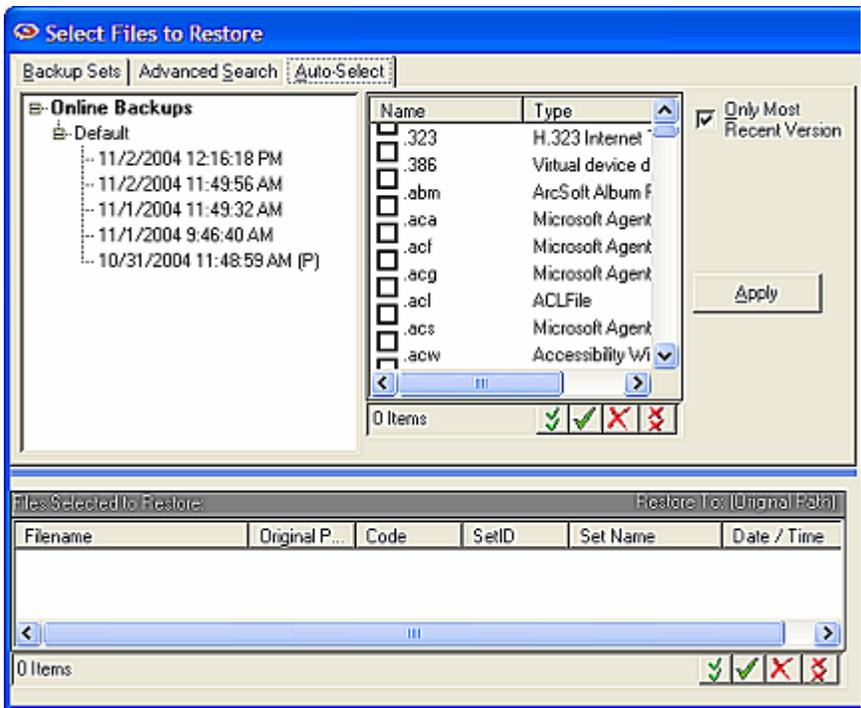
Restore – Auto Select

The **Auto-Select** tab allows you to find files by file type. Select the Auto-Select tab to display a list of all the file types on your computer. All the Windows Registered file types will be listed according to their file extension, with an explanation of what application the files belong to.

For example, to find all your *QuickBooks* files, select the Auto-Select tab, then click the **Type** column header to sort by file type, and scroll down until you locate the QuickBooks file types. Select them, and click **Apply**, then **Restore Now**.
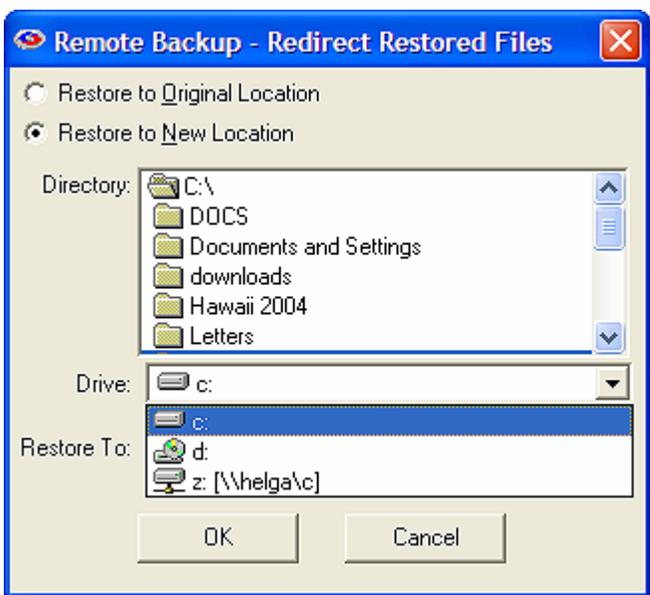
Redirect Restore

This option lets you redirect the files you are about to restore to a different drive or directory other than their original. This is useful if you want to restore files to a different computer, or to a CD drive for a second backup. It's also useful if you have bac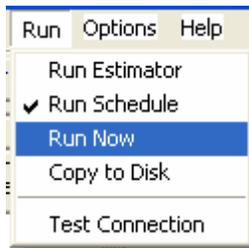ked up files from, for example, drive D:\ on a computer that was stolen, then restore them to a new computer that has only a drive C:\.

You may set Restore to New Location to override the destination of the restored files. Click Create Folders to create the restored files path under the Restore To: folder, or uncheck it to restore files directly to the Restore To: folder.

Run

The Run menu is used to run *Remote Backup* different modes.

Run Estimator

The Estimator is used to estimate the time required for a backup. It works by running a "fake" backup session. While it is running you will see a progress screens that displays Remote Backup's operations required for a backup or estimation.

After Remote Backup is finished estimating your backup time, it displays a report similar to this:
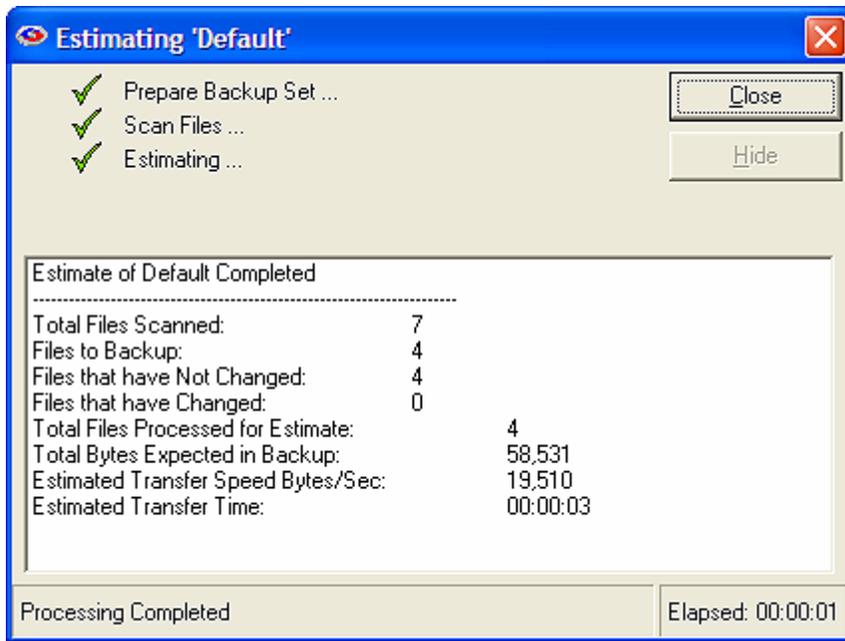
Run Schedule

Select this option to run Remote Backup on its regular schedule.
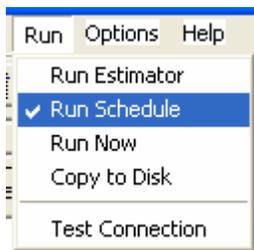
Selecting this option will make Remote Backup minimize to the icon tray and wait until it is time to run one of its Backup Sets. This is the normal way to run Remote Backup.

Run Now
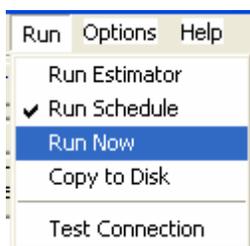
Selecting this option will cause Remote Backup to run the currently selected Backup Set immediately.
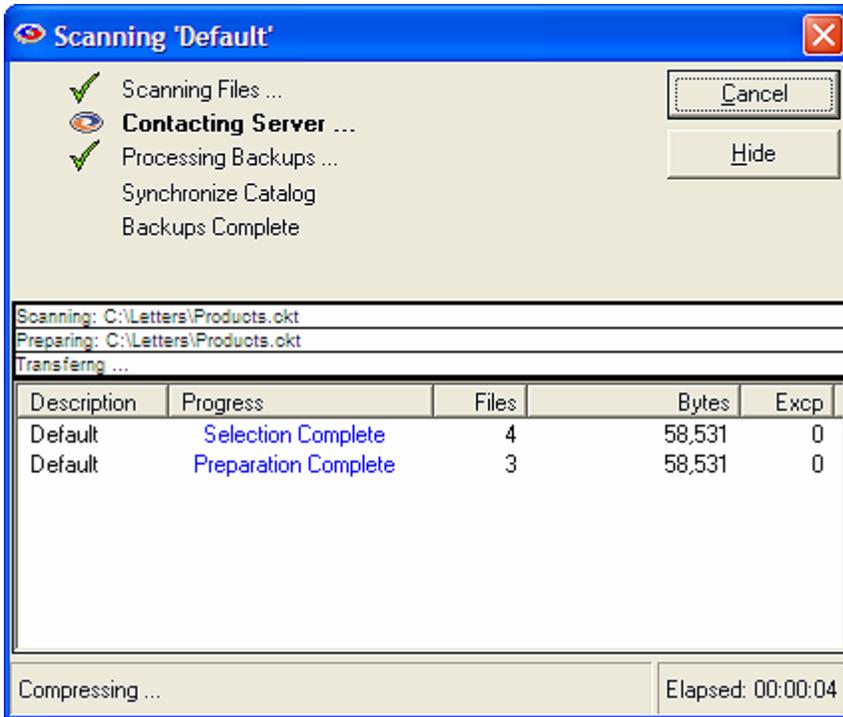
The Progress Dialog shows immediately, indicating the details and completion of each step of the backup. Completed steps are marked with a green check mark. If the process fails, the step that fails will be marked with a red "X". While a step is in progress, the Remote Backup Icon graphic is displayed by that step in an animated fashion to indicate work is being done.

Test Connection
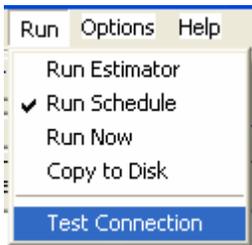
This option tests the connection to the Backup Server. The following screen shows a good connection.
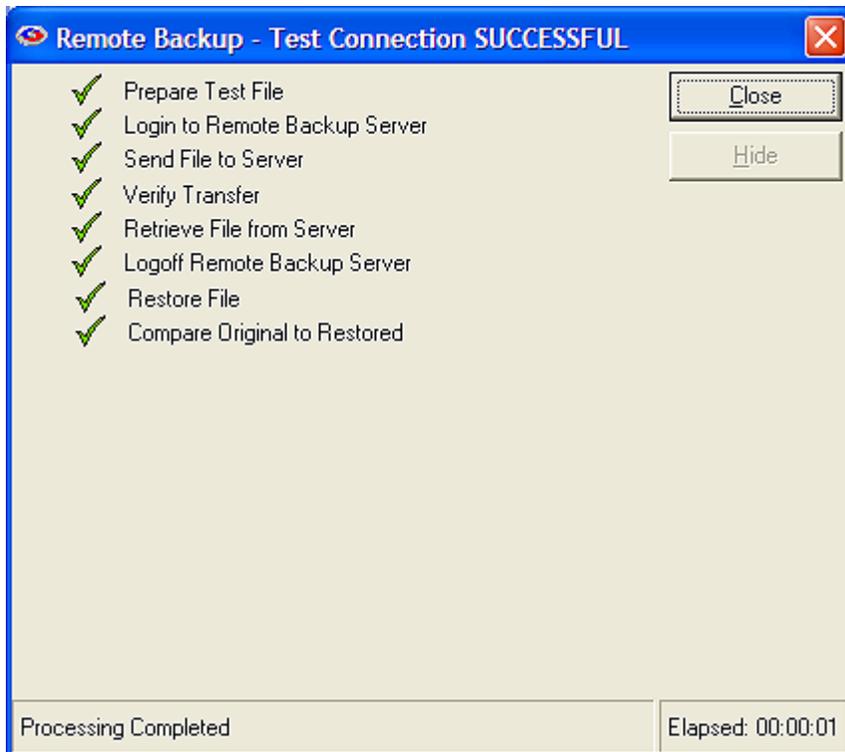
Options Menu

The Options Menu contains choices for Preferences and Registration.
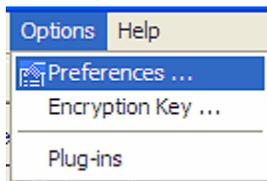
The Preferences menu allows you to change various options of Remote Backup.
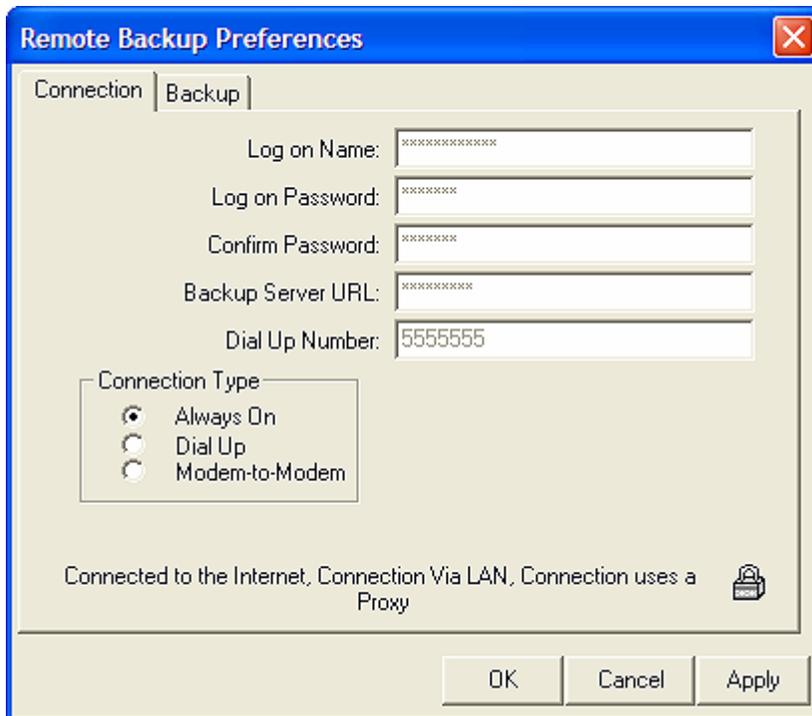
The Connection Tab contains information about your connection to the Remote Backup Server. Because of security concerns, it isn't possible to change most of this information. Much of this information was either entered when you registered, or is required by your Backup Service Provider to make a proper connection.

The Backup Tab is where you change your encryption key. For information on how to change your Encryption Key, see the section on Changing Your Encryption Key.

The padlock icon is a special button used to set the data retention policies of your backup sets. Contact your Backup Service Provider for additional information on how to create custom retention policies for your account.
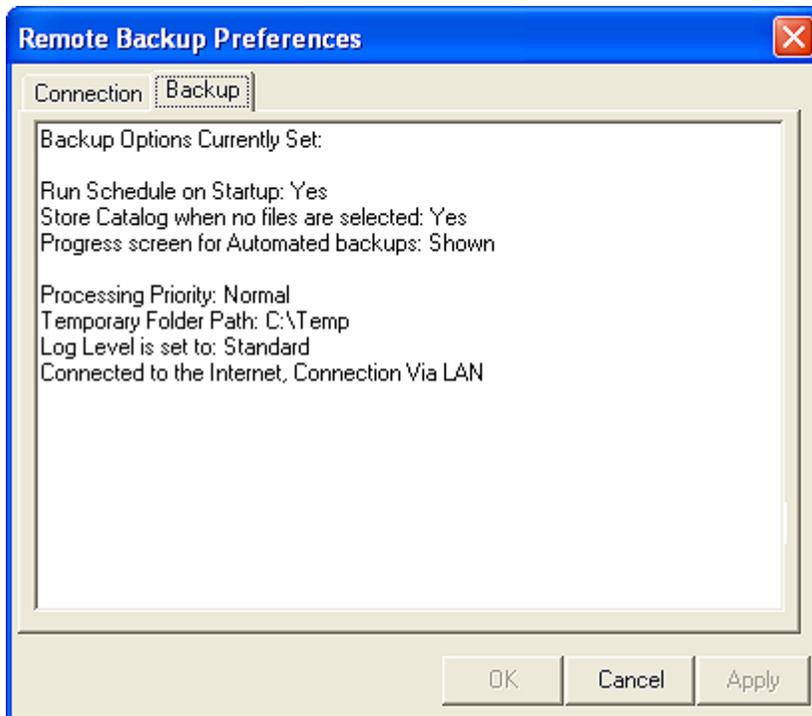
The Backup Tab contains a report of your current settings.

Changing Your Encryption Key

It is usually advisable to change your Encryption Key periodically. Your Encryption Key is literally the key to your data. It is used to lock up your data so nobody else can see it, and like a regular key, if you forget it, you may not be able to recover your data.

When you change your Encryption Key, write it down in a safe place. If you forget it, you may not be able to recover your data.

There are two ways to change your Encryption Key. The first is to select a word or phrase that you can remember. For rules on selecting your encryption key, see the section on Selecting Your Encryption Key.

The second way is to let Remote Backup generate a key for you.

Remote Backup has a way to automatically generate "statistically perfect" encryption keys - the most secure keys. If you want the very highest security, do not pick your own key. Allow Remote Backup to generate it for you.

The way Remote Backup generates a key depends on which encryption standard you have chosen.

Note: All of Remote Backup's encryption standards may not be available in your version of Remote Backup.

DES Encryption

If you pick "DES (8.3 Standard)" Remote Backup will generate a 128 bit key, represented as sixteen letters and numbers.

Generate Key?

You have requested to generate a key for

AES 128-bit

This will replace the current key. Do you wish to continue? (Y/N)

[Yes]   [No]
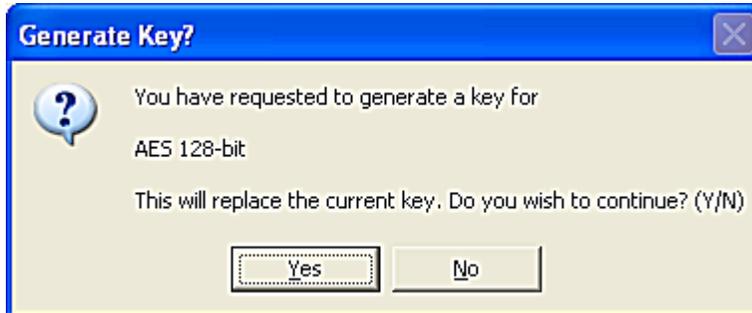
Since these "perfect" encryption keys are hard to remember, it is recommended that they be recorded on paper and kept in a safe place.

Note: Whenever an Encryption Key is changed it is advisable to create a new Key File.

Blowfish Encryption

When generating a key for Blowfish encryption, you will see an additional screen asking how long you want the key to be. Blowfish varies from one to 56 characters. A "character" is eight bits. So, Blowfish varies from eight bits (1 x 8) to 448 bits (56 x 8)

Enter Key Length

Enter Number of Characters for Blowfish Key Generation (from 1 to 56 characters)

[OK]
[Cancel]

16
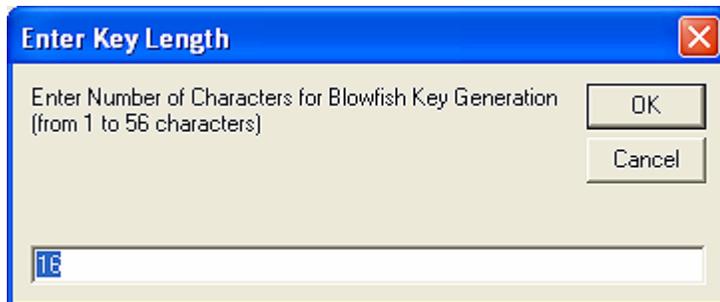
Encryption Key Information

When a new key is created you will have the opportunity to print the new key. Print it or write it down and save it in a secure location.
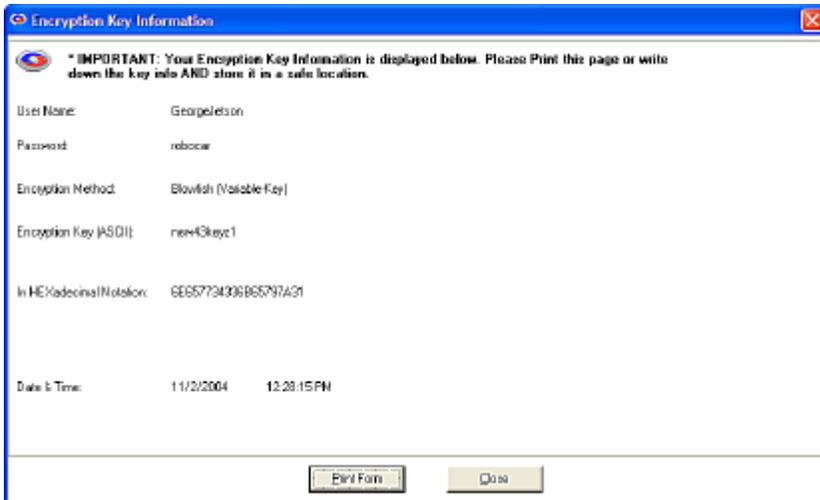
Whenever you change your encryption key or any other setting that is critical in restoring your data, Remote Backup will prompt you with one or more messages indicating an action you should take.
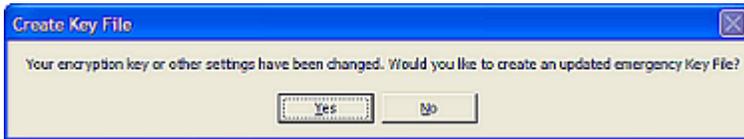
When prompted to create an updated encryption key file, answer **Yes**. Remote Backup will place the key recovery files on the device you select. Select a diskette drive or a network drive to store the Key Files away from the computer they protect.
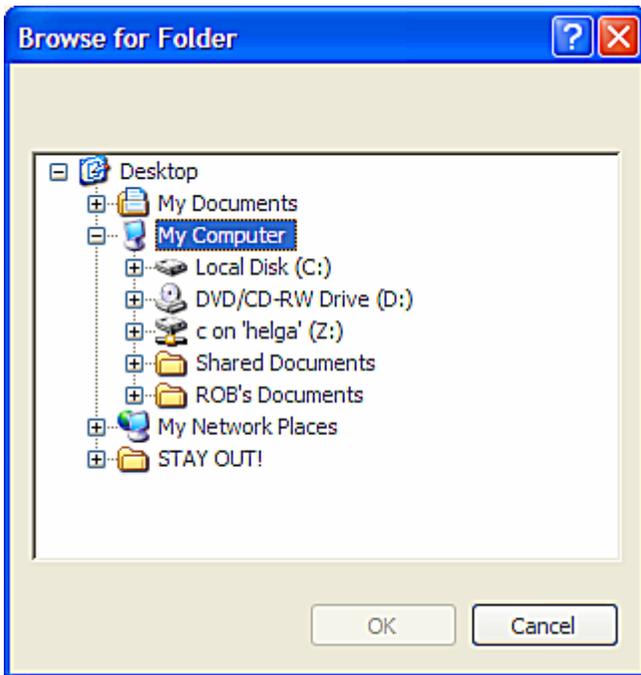
The following screen will be displayed, indicating the file name(s) that were created.

Emergency Recovery File Created

Please note: Disaster Recovery cannot be used until after the first backup subsequent to a key change.

You may use disaster recovery anytime after your next backup.

The Emergency Recovery File(s) are located at:

C:\New Location\recovery.dat

C:\New Location\recovery.dsk

Please copy or move these file(s) to a protected location.

OK

Encryption Standards

DES (8.2 Compatible)
DES (8.3 Standard)
TDES (Triple-DES)
Blowfish (Variable-Key)
AES 128-bit
AES 192-bit
AES 256-bit (Most Secure but s
--Select Encryption Method--

Remote Backup allows you to use various Encryption Standards. Depending on the country you are in and the version of Remote Backup you have, some of these standards may not be available to you.

DES is the old US Federal Standard

TDES is a much more secure form of DES

Blowfish is probably the most secure of all. It uses a key length that is variable from four bits to 448 bits.

AES is the new US Federal Standard. RBackup supports three levels of AES from 128 bits to 256 bits. 256 bit AES is very secure, but it is also slow.

Selecting Your Encryption Key

It is VERY important that you select a proper Encryption Key. This is literally the key to your data security. Remote Backup uses the industry's most secure encryption technology. However, even the latest, most secure encryption technology can be compromised by using a bad Encryption Key. There are some rules.

Never use your name, your dog's name, ANYONE'S name, or part thereof.

Never use any part of your telephone number, address, or any other identifying information about yourself.

Never use a properly spelled common word or proper noun.

Never use a key shorter than ten characters.

Never use the same encryption key and/or password for different services.

Never use the brand of your favorite car, horse, motorcycle, vacation spot, etc.

DO use a key with more than ten characters. The more the better!

DO use a key with mixed letters and numbers.

If you use actual words, misspell them.

Add unnecessary punctuation marks to the end of actual words or phrases.

Remember – the longer and more complex your encryption key is, the more secure your data. There are several ways to crack encryption – guessing, using a Dictionary program, brute force, or hardware-related methods.

Guessing – Hackers use this method first. They try to guess your encryption key by using combinations of information they know about you. Your name, your address, your phone number, your dog's name, your spouse's pet name - all are common encryption keys that can be guessed. If someone who wants to hack your password gains access to your desk, they will look around at your pictures, your "stuff," and try to guess your password based on what they see. They may even look up the middle names of your children and other info about you in public records.

Dictionary Program – An attack with a dictionary program uses a database of words from the dictionary to try to crack your encryption key. If you use a common word or phrase, spelled properly, a Dictionary attack may take only a matter of minutes using a regular home PC.

Brute Force – This method requires an enormous amount of computing power, time, and manpower. But, it has been effective in cracking some low-level encryption techniques. Remote Backup uses extremely high-level encryption technology. In Brute Force attacks, hackers use high-speed computers to try many different combinations of letters and numbers until maybe, some day, one of their combinations work. This is the ONLY way to attack most high-level encryption techniques.

Sniffers – Less common than any of the other three methods, this method and other similar hardware-related methods seem to be born out of science fiction. But, they ARE real. Unauthorized visitors to your company can leave behind devices that send everything on your network or computer to a remote location. There's even a device that can be built out of common electronic parts that lets someone read everything on your computer monitor from as much as 100 meters away – without the need to actually see the monitor. They pick up the electronic pulses generated by your computer monitor as you type and translate them to screen images on the hacker's terminal. Amazing!

Examples of BAD ENCRYPTION KEYS

Robert (my name)

Larry (my dog's name)

555-1212 (my phone number)

Jaguar (my favorite car)

Blackboard (just a regular word)

Examples of GOOD ENCRYPTION KEYS

theAzoRes# (a proper noun, mixed case, and with a trailing punctuation mark)

FrAn1klen-mAKes$-great%-breaD# (a phrase, misspelled, with punctuation and mixed case)

birds!of)a(featuer#flock^together (same as above)

asdASDLFJ#*sdfk98-98-0sdfk;jwq89ASDF3dsfkj9j30kld##cx (absolutely random – the best)

rooleftthetheatrethenwentforawalkdownbytheriver# (a phrase with punctuation mark)

Note: DO NOT use any of these examples!

File Types

Your computer stores its data in files. Some file types need to be backed up, and some usually do not. Although Remote Backup can back up virtually any file on your computer, some files are considered critical and some are not.

Data files are considered critical files because they contain your most recent and critical data like your customer records, accounting files, word processing files and other data you work with on a daily basis.

Program files are usually not considered critical because if they are lost they can be restored from your original distribution diskettes that came with your software. For this reason it is important to store the original copies of your software diskettes away from your computer, not in the same building if possible.

Your computer also has a lot of other non-critical files. These are files that are left over from installations of programs, temporary files, compressed folders and others that would not affect the operation of your computer if they were lost. These should not be backed up.

The vast majority of the files on your computer are probably program files and other non-critical files. They can be identified by their file names. Program files have common extensions like:

.exe   .dll   .ovl   .reg   .cab   .zip   .hlp   .bmp   .sys   .wav

Some file types that probably should be backed up include:

.mdb   .sql   .dbf   .fpt   .ini   .lnk   .doc   .xls   .pst   .msg

These are by far not the only file types that should be backed up, but they are common data file extensions.

File Selection Tips and Tricks

When you select the files you back up, you may get better results if you understand a few tricks of the file selection subsystem.

The system optimizes your selections in different ways depending on the contents of your selection:

1. Folder/File Selection without Auto-Select

2. Auto-Select INCLUDES and EXCLUDES

3. Folder/File Selection with only Auto-Select EXCLUDES

Folder/File selection method one involves simply "green-checking" files and folders, and excluding files and folders within that selection. Method 1 is good for backing up specific files and folders quickly

Auto-Select INCLUDES and EXCLUDES is the most thorough method but takes the longest, and can potentially generate huge backups. This is fine if that's what you want, but it's also easy to pick up a lot of relatively unnecessary files.

Method 3 is a combination of methods 1 and 2.

Methods 1 and 3 are pre-optimized before being fed into the scanning process, scanning root and sublevel folders separately to improve the speed of the process.

Checking the File Selection Results

It's easier to check your results interactively using the Estimator when you first set up the backup set. Estimator displays the file that it is accessing and can often clue you, particularly, to files that you don't wish to be in the selection quickly. When you see these files, cancel the estimate, adjust the selection and rerun it. A few times through this process and most of the selection tricks will become evident.

For deep analysis of file selections, you may change the Log Level setting temporarily to VERBOSE, which will list all file selections and exclusions for files scanned. We don't recommend leaving this setting at this level as the log files generated can be huge.

Interactive Selections

While selecting files, you can use the right-click menus to easily modify your selections based on the files you see, for example, you can right-click on ABC.ZIP and select the Auto-Select exclusion of all ZIP files. You will immediately see any other ZIP files receive a Red X.

User-Types "Trump" File-types

Auto-select offers two method of defining filters. The File Types are taken from the list of file types maintained by windows, and can vary based on applications installed and user modification, so cannot always be depended on from one computer to another.

User-Types are your user-defined collection of file types, by extension. User-Types take precedence over File-Types, and both can contain a list of file extensions. Normally, a Red-X TRUMPS a Green Check except with User-Types, where a Green-Checked user type can reverse a Red-X in a File-Type for the same extension.