



**I**Secure**D**at

presents

**Brief Details Concerning  
BitBackup's Storage and  
Recovery System  
Idiosyncrasies**

BitBackup has a couple of idiosyncrasies not well documented or noted until too late. By that we mean, the encryption method has already been implemented and changing over to another system can be taxing, perhaps a bit of a risk and not necessarily the most prudent move, but certainly possible.

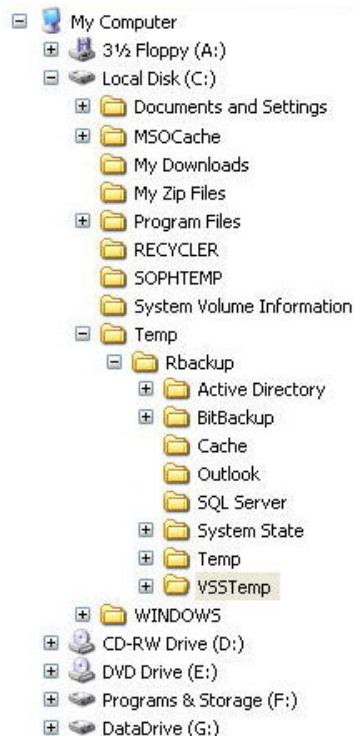
**The purpose of this white paper is to inform you a bit of how BitBackup works, what can happen if you're not paying attention and to present options for consideration if this particular issue does occur.**

**BitBackup needs a “local storage” area.** In other documentation this is usually stated as a 5 GB minimum requirement. It does not say this is dependant on file size, just that this is the minimum. Also as noted in other documentation, BitBackup is perfect for large files sizes such as a data base or MS Outlook .pst files. However, BitBackup does actually require at least one and one-half (1½) times the space size of the original data selected for backup to work. So if you have 50 GB of data for backup, you will require an additional 75 GB of free space for it to work with.

There are two locations created and used by BitBackup as a “Local Store” and as a “conversion area”

**C:\Temp\Rbackup and  
C:\Temp\Rbackup\BitBackup**

**C:\Temp\Rbackup** is where the “client agent” temporarily transfers files in batches of 250 – 500 files during a backup process to encrypt and compresses them prior to transmission. This location is cleared automatically upon backup completion and is therefore not an issue.



The second area **C:\Temp\Rbackup\BitBackup** is where the “Local Store” is located by default. This “Local Store” will always be present and have a full-copy (most up-to-date) of all the files in the backup set PLUS the latest “Patch Files” for all those files. This “Patch File” location also called the “Local Store” and is a must have for BitBackup.

Both of these paths are customizable and can be changed to a different location. This location can reside on a different drive, USB drive or other removable drive.

BitBackup uses the “Local Store” to hold a full copy of all files being transferred to ISecureDat servers. These files are used for comparison and patch creation in addition to being encrypted and compressed in preparation for transmission. It’s the “threshold” settings that determine how much data must change (patches) or the number of new files that are added before a new full copy is created.

Original documentation says, “Roll-Forward Threshold and Threshold Size are used with BitBackup and will not keep increasing in size depending on how you have your threshold settings set.” But, there are exceptions to every rule as you’ll see following the threshold set details.

**Roll-Forward Threshold:** This is the **number** of BitBackup patches that will be performed (created) before a full backup is transmitted again.

**Threshold Size:** This refers to the **percentage** of the BitBackup full file size. When patches reaches 50% in size of the original files size (default threshold setting), BitBackup performs a “Roll-Forward” transmission. The patches are consolidated into a new “full backup” and new patches are created anew. This can be adjusted to whatever percentage you prefer. The smaller the Threshold Size percentage, the greater the number of transmissions plus the more up-to-date your backup files will be on the ISecureDat servers. It is suggested you do not go above the 50% default.

**The Exception:** ISecureDat has come across a situation which has prompted the writing of this white paper regarding the use of BitBackup. One of our clients was (is) using BitBackup to backup her \*.pst files (Microsoft Office Outlook e-mail application files) which is a very good use for BitBackup.

The issue came about because in her business, she had to retain all e-mails and replies for legal reasons. This meant nothing could be deleted (other than SPAM) and the file became larger and larger, for years. MS \*.pst files are cumulative by nature which simply means as more e-mail come in and replies sent out the file continues to grow; even if new folders are created to segregate clients or topics.

It came to a point where she had in excess of 110 GB in her C:\Temp\Rbackup\BitBackup “Local Store”. This effectively filled all the remaining free hard drive space and made BitBackup unable to operate and therefore backups were not being performed. The automatic notification system at ISecureDat then sent out a notice that read:

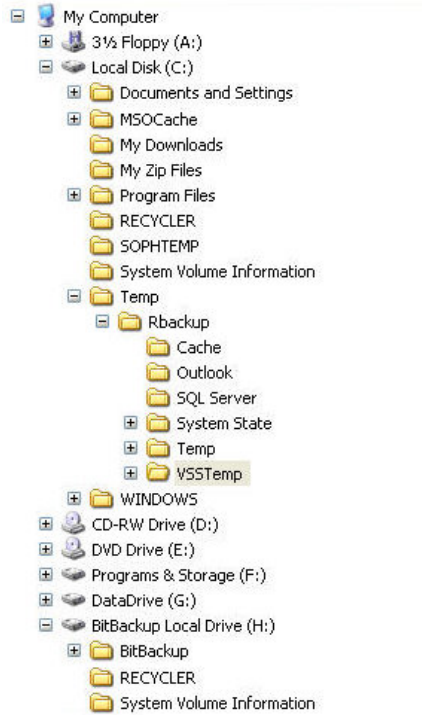
NOTE: Exception Message: Backup was stopped due to limitations on available free disk space on the client computer.

To help prevent this problem, ISecureDat suggests a separate external hard drive (either a USB drive or network drive) be dedicated as the “Local Store” leaving your workstation free for operations. There are a couple of possible setups you might consider which would be applicable to either USB or network option.

The 1<sup>st</sup> option is to leave the C:\Temp\Rbackup “preparation area” as and where it is. As mentioned earlier, this folder is cleared automatically after each transmission, and should not be a problem.

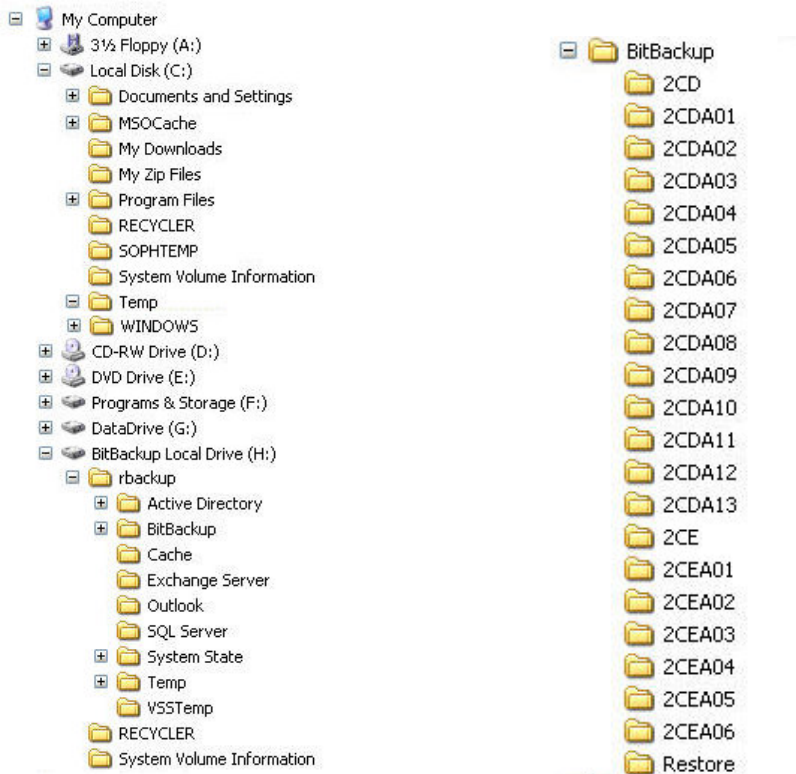
Notice in the following image, the “Temp\Rbackup” folder remains on C:\. The other sub-folders will be there as well, just leave them. The actual “full backup” or “Local Store” has been redirected to “H:\”, an external USB connected hard drive. The hard drive name was changed to remind the user of its purpose.

The only possible draw back to using a USB connected hard drive, other than the lack of USB ports which could be corrected with a USB hub, is the fact that the USB drive will have to stay on all the time. Your backup will fail if this drive is not accessible.



The 2<sup>nd</sup> option is the same as the 1<sup>st</sup> except both the “Temp\Rbackup” and “Temp\Rbackup\BitBackup” are now both directed to the external hard drive. This has the same effect as option 1 except now you don’t have to try to remember what these temp files were for on your C:\ drive nor will they get cleaned out by “Disk Clean” each time it’s ran.

The image on the right displays the sub-folder structure within BitBackup in Hexadecimal notation. These are the encrypted full copies on your system that will eventually be compressed and transmitted to the ISecureDat servers.

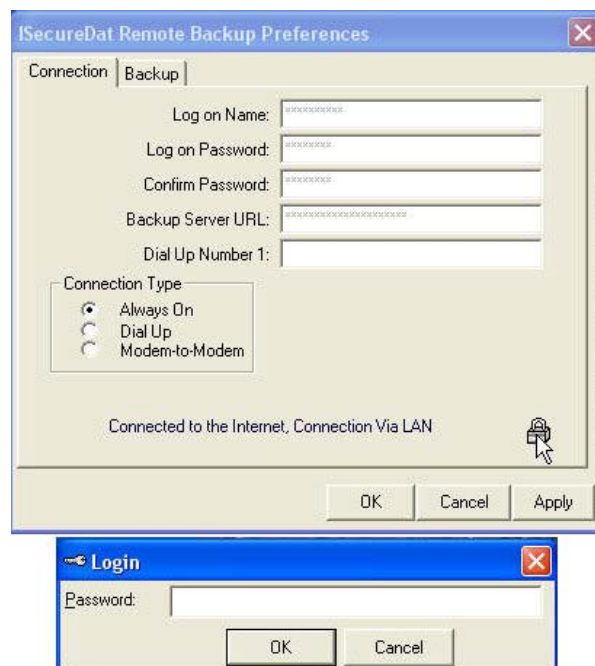


Follow the instructions below if you are currently using BitBackup as your primary encryption type and would like to re-direct the “Local Store” or if you wish to change the backup encryption type altogether. To create a new set see [http://www.isecuredat.com/download/PDFs/Creating\\_Backup\\_Sets.pdf](http://www.isecuredat.com/download/PDFs/Creating_Backup_Sets.pdf)

Remember, BitBackup is not the recommended method for complete backups. Use it for huge files and to backup files that might be considered “normal”, use an incremental backup type. You can also use different encryption systems for different file type sets in tandem.

To make the change to an external hard drive you need to open your client agent by double clicking the ISD icon on the lower right tool bar of your operating system. On the top menu bar of the “Client Agent”, click “Options” and select “Preferences...”

A new window will open as shown here. Double clicking the “Lock” icon will request a password. Please contact [techsupport@isecuredat.com](mailto:techsupport@isecuredat.com) for this information. As it is password protected, the information is not made public.



Once the password has been entered, the following window will appear. Select the “Backup” tab which will display your current encryption method.

To change the location of your “C:\Temp\Rbackup” (the location where files are encrypted and compressed and automatically cleared upon transmission) click the “Temporary File Path:” browse button and select your preferred, new location.

Use the same process to change your “Local Store” (the “C:\Temp\Rbackup\BitBackup”). This can be another partition on your hard drive, another external drive or other removable drive.

Once completed click the “Apply” button and you will get a notice your encryption system has been changed. “Would you like to create a new registry key?” Select “Yes” and make a copy of this new key for your files.

