Resco Backup Pro for Palm OS®

This manual is an extension of the documentation to the standard Resco Backup and concentrates on the added features only.

Remarks:
This guide refers to the Resco Backup Pro v2.11.

1 Introduction

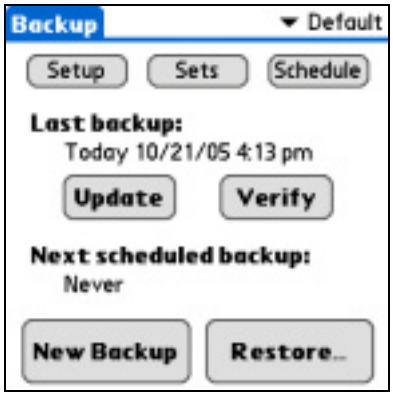

Fig. 1 –Main screen - Advanced mode

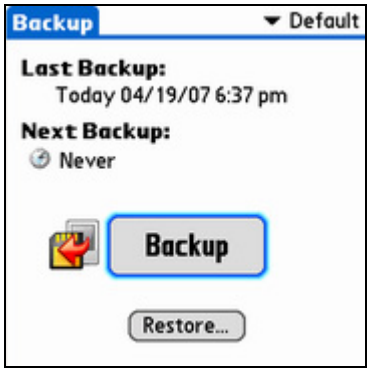

Fig. 2 – Same screen in Basic mode

Added features with respect to standard Resco Backup

- Optional strong AES encryption (WinZip compatible)
- Backup set upload/download to/from an FTP server
- Free FTP account offered by our partners from www.DriveHQ.com
- Secure FTP login (requires FTP server support)
- FTP backup sets management (update, download, delete, Diff)
- Optimized data traffic (true updates etc.)
- Support for the device migration

Requirements: Palm OS 5+

Installation:

Add RescoBackupPro.prc file to the Palm Desktop Install Tool and Hotsync. You can install RscBackup+ on the card, but then you use the ability to perform automatic (scheduled) backups. Apart from this, there is no difference between the card and RAM installations.

Uninstallation

Delete RescoBackup from the handheld. You might want additionally:

- Delete RscBackup from the card.
- Delete card backup folder /Palm/Backups

Upgrade from standard Resco Backup

Both basic and Pro version share the same creatorID, settings and other data, i.e. they cannot co-exist on the same PDA.

To install the Pro version just Hotsync the .prc file over existing Resco Backup installation. To return to the standard version just Hotsync the .prc file over existing „Pro“ installation.

Note:
Existing Resco Backup users can purchase the Pro version for the differential price between both packages. More info on the Resco web page.

Compatibility to standard Resco Backup

Settings and data (backup sets) are compatible except AES-encrypted backup sets. Such backup sets will be treated as corrupted by standard Resco backup.

Compatibility to public Zippers

AES encrypted backup sets can be opened by WinZip, 7Zip, PowerArchiver. On the Palm PDA you need to use Resco Explorer v3.20.
Note that you should switch on CRC computation (Project Setup > Advanced) if you intend to access the backup sets with other zippers.

Acknowledgment

AES code is based on the code from Dr Brian Gladman. Following conditions apply:

<AES>
* Copyright (c) 2002, Dr Brian Gladman < >, Worcester, UK.
* All rights reserved.
*
* LICENSE TERMS
*
* The free distribution and use of this software in both source and binary
* form is allowed (with or without changes) provided that:
*
* 1. distributions of this source code include the above copyright
*   notice, this list of conditions and the following disclaimer;
*
* 2. distributions in binary form include the above copyright
*   notice, this list of conditions and the following disclaimer
*   in the documentation and/or other associated materials;
*
* 3. the copyright holder's name is not used to endorse products
*   built using this software without specific written permission.
*
* ALTERNATIVELY, provided that this notice is retained in full, this product
* may be distributed under the terms of the GNU General Public License (GPL),
* in which case the provisions of the GPL apply INSTEAD OF those given above.
*
* DISCLAIMER
*
* This software is provided 'as is' with no explicit or implied warranties
* in respect of its properties, including, but not limited to, correctness
* and/or fitness for purpose.
* ---
* Issue Date: 24/01/2003
</AES>

2 Strong encryption

2.1 AES and security

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption technique adopted as common standard for safe encryption.

AES provides significantly better security than standard ZIP 2.0 encryption that is used in standard Resco Backup.

When talking about the security, there is no such thing as absolutely secure algorithm. A better attitude is to talk about the costs needed to break the code. (Remember that DES was considered as secure for years until the computers improved to the extent that the costs of the code breaking decreased to a reasonable value.)

To illustrate AES safety this way, here is a citation from a security expert (2004):

"Correctly implemented AES-128 is likely to protect against a million dollar budget for 50+ years and against individual budgets for at least another 10 years."

To conclude, protocol, implementation, computer security and user practices are much more important than crypto algorithm! The by far most critical thing is the password quality. Remember, if you use your initials as the password, then you could equally well leave your data unencrypted. A well-known general advice: Always use a mix of lowercase/uppercase letters, digits and special characters.

2.2 AES implementation

RscBackup+ uses the same backup set format as the standard version, i.e. a set of zip archives. The only difference is that these archives may internally use AES encryption.

Note that older ZIP-utilities mostly do not support AES encryption and thus will not be able to unzip RscBackup+ archives. The chosen implementation is **compatible with WinZip, 7Zip, PowerArchiver** etc.

Only the content of files stored in a ZIP-file is encrypted. The file name, date, size and attributes are stored in unencrypted form in the ZIP-file header and can be viewed without a password, by any tool that can access a ZIP-file.

Other implementation details:

- Empty databases are not encrypted.
- User can (and should) choose not to encrypt publicly known files. The idea behind is that it has no meaning to encrypt files that can be found on the web;[1] in fact the encryption of such files just adds on computational complexity.

[1] This enables so-called plain-text attack, when the cracker has both source and encrypted data. Such an attack can be successful for weaker encryption schemes. However, AES is that good that plain-text attacks have no chance either. Here a citation from a crypto expert:
"Even if your drive was so bit that it contained every byte of data in the world, and the attacker had both the plaintext and encrypted versions, there is still no published way to get the AES key given that data."

2.3 Safety and scheduling

Unfortunately these two things go against each other. If you want to have unattended automatic backup, the password must be stored somewhere so that it could be applied when the backup is created. RscBackup stores this password in an encrypted form, of course, but a good hacker (not necessarily an encryption expert) can simply debug the application and get access to the password. It is the same story as the copy-protection schemes: Every scheme can be broken, it is just a question of time and money.

Default project is a bit specific: Project definition resides in memory, while the data (backup sets) are on the card. In this respect, a card loss presents no risk at all – the encrypted password stays on the PDA.

However, for non-default projects all data is stored on the card and the risk is greater.

Summary:
Do not use scheduling if the safety of the encrypted data is the top priority.

2.4 Setting up the encryption

The process is simple:

- Open Project Setup dialog
- Switch on Password checkbox
- Type the password. As explained above, you should choose a complex password that cannot be guessed.
- If you intend to use automatic backup, the switch on the *Store* checkbox
- Go to *Advanced* options
- Switch on *Strong Encryption* if you want AES instead of default zip-based encryption
- The option *Encrypt Known Files* should be left unchecked

2.5 Encryption speed

AES processing brings speed penalty. The reason for the slow-down is the safety. AES initialization is made computationally complex to prevent brute force attacks.[2]

Our sample tests showed that:

- A typical backup will slow down by 50% (if known files are not encrypted).
- Impact on the Verify procedure is even larger.

Still, the time needed for backup remains very favorable when compared to other backup solutions.

[2] Attacks based on the enumeration of all possible passwords.

3 FTP backup

FTP (File Transfer Protocol) is a standard protocol for exchanging files over TCP/IP networks. RscBackup+ allows for storing the backup sets on a remote FTP server placed somewhere on the Internet, which gives you an additional dimension of safety.

There are two basic conditions in order to use FTP backup:

- You need working network connection. It does not matter whether the connection goes via PC or is phone-based.
- You need an account on some FTP server.

3.1 Network connection

You will need any type of a web connection. In other words, if you can use Blazer to access web pages, you will be able to use the FTP, too.

Alternatives:

- Built-in phone connection (GPRS, CDMA etc.)
- WiFi
- BT (Bluetooth) connection to a PC. Needs a cheap BT adapter for your PC and some setup work. Gives you a fast connection over your PC (no payments involved) as long as you are within a close distance from your computer. More info about how to build this connection can be found in the Resco Explorer documentation (ExplorerNetworking.pdf); explains also how to access your PC files from your PDA.

3.2 About FTP

FTP communication involves two sides: a server and a client. FTP server listens for client connection requests. Once connected, the client can do file manipulations such as uploads, downloads, rename, delete etc.

Full description of an FTP server account looks like this:

URL: ftp.microsoft.com (or its equivalent - the IP address)
user: MyName
password: MyPassword

Client connection starts with a login, i.e. supplying user name and password. These parameters determine the user rights, i.e. what is the user allowed to do.

Resco Backup implements FTP client. If you want to make use of the FTP feature, you need the other side - FTP server.

There exist public FTP servers such as ftp.microsoft.com. Besides they can serve as a data source and for training, their value is limited.

What remains is FTP server of your company (many companies have one), building your own private FTP server or ftp hosting services such as DriveHQ discussed later.

How to build your own FTP server

If you look for information, do the easiest step - Google for "ftp server".

There exist ready FTP servers for each platform and many of them are free - at least for personal use. **Make sure FTP server allows passive mode.** They usually do, but if not, you need to go for another server. Implementation of active mode is rather difficult under Palm OS.

Newer Windows versions include basic FTP support as part of the IIS (Internet Information Services). Can be enough for personal use, but 3rd party FTP servers perform better.

While the installation uses to be straightforward, setup may require more work: At the minimum you need to specify the data storage (folders) and users with their access rights.

One problem you will have to solve is the IP address of the FTP server. You can either purchase a fixed IP address (a cheap option) or employ additional software that enables the use of the dynamic IP address. (Basically it takes care that whenever the dynamic address changes, the DNS server gets this information so that the symbolic name of your server always links to the current IP address.)

FTP servers listen by default on the port 21 for incoming connections from FTP clients. (Your firewall must allow this port.)

FTP security

FTP servers as a rule use plain-text login and file contents are sent in clear text. Data sent is not encrypted either. Neither of these properties is particularly pleasant.

Some servers allow at least for a secure login. (It means your name and password are encrypted.) Resco Backup supports one common protocol called TLS authentication.

Our suggestion is to use FTP in combination with AES encryption.

FTP Reliability

- Data is as safe as the underlying tcp protocol. (Not bad, but today standards are higher.)
- FTP protocol itself does not have any check on the receiver side. However, Explorer implementation is safer due to additional checks.
- File transfers may fail if the file is simultaneously modified by another client. (A theoretical possibility in this case.)

Traffic requirements

Estimate for a Treo 650: Say you have 12 MB of RAM data and one backup set takes 7 MB.

GPRS (64 kbit/s) will take 15-20 min to upload the whole backup set. (FTP itself has some overhead.)

Edge might be 2-3 times faster, i.e. it won’t help too much.

It appears, that unless you have a fast connection (CDMA, EVDO, WiFi, local connection to PC via BT), uploading the whole RAM backup is a pain. (Situation for higher Palm models is even worse as they have substantially larger memory.)

It does not mean that you can't make use of FTP when you have a slow connection. You still can create a custom project for just the most important data. E.g. if you decide to backup your PIM data over FTP, the data traffic will be many times lower.

Another thing to note is that after you make first upload (which can be done over a fast line), subsequent updates will be much smaller.[3]

3.3 DriveHQ FTP hostig service

For those users who have no concrete FTP experience we have an offer from our partners from Drive Headquarters – www-dot-drivehq-dot-com. They provide a free FTP account (one per user) with very liberal limits – 1 GB storage and 1 GB downloads/month.

We do not claim that this is the best service, but from the web searches we did, it appears that DriveHQ offers conditions that are hard to beat. In any case it looks like a good chance for FTP startup.

Note that at present DriveHQ does not support secure login protocol as implemented in RscBackup+.

3.4 Using FTP

3.4.1 FTP Setup dialog

RscBackup can have one FTP account and you need to enter it via *FTP Setup* dialog accessible from the main menu.

As already explained, you need to enter FTP server web address (URL) and your account (name + password). Those who do not have an FTP account can create a free DriveHQ account using the combo box at the bottom of the setup dialog.

Once you finish the setup and press OK, RscBackup will attempt a test login in order to make sure that the setup is correct. If incorrect, you will see the communication log. Unfortunately, the content is too technical, yet sometimes it is possible to identify the source of the problem.

Advanced options offer two flags:

- *Use only secure login*: RscBackup always starts with secure a login attempt. If refused and this checkbox is unchecked, a second trial with plain-text[4] login follows. Use this option if you positively know that your server supports TLS authentication.

- *Auto-backup: Reset if Internet connect dialog cannot be closed*: This attempts to help with the problem, when the Internet connect dialog requires user action (such as entering PIN number) that cannot be canceled. If this happens, there are just 2 options: Reset or wait until the user arrival; the second possibility may result even in the battery discharge.

[3] Well, it's more complex. An update will be naturally much faster. But the scheduler will perform full updates until the number of backup sets specified in the Project Setup dialog is reached.
[4] Non-encrypted

3.4.2 FTP Backup Sets dialog

The dialog must be familiar to any Resco Backup user. Indeed, it looks very similar to the standard Backup Sets dialog.

Every backup set that is listed can be located on the card (such sets have a card icon in the leftmost column), on the server (the icon in the rightmost column) or in both locations. (Both icons are present.)

Backup sets with error display error icons[5]. (True for both local and remote sets.)

Actions that can be performed on the selected backup set:

- **Diff** compares the contents of the local and remote sets. The comparison is based on the download of the backup set information file (called *manifest*) from the server, hence it is fast.
- **Upload:** The result of the upload is an exact copy of the local backup set disregarding whether an update was performed (synchronization) or a full copy. Upload algorithm is discussed in the chapter Implementation.
- **Download**: The result of the download is again an exact copy of the remote set, i.e. the download works like synchronization (copying over existing set) or a full copy.
- The last action is the backup set **delete** – can be performed both locally and remotely.

Treatment of error backup sets:

- Upload of a local backup set with error is considered a normal upload and the result (in case of successful upload) is a correct remote backup set. (I.e. the error is "lost" in the upload process.)
- Download of a remote set with error: If the local set with the same name exists, the download is refused.[6] Otherwise the download is carried out.

3.4.3 Scheduled FTP updates

To enable them, go to the Project Scheduler, select *Advanced* and *Upload to FTP*.

If there is a limit set for the number of backup sets (Project Setup > *Max # of Backup Sets*), this limit will be respected for FTP upload as well.

The scheduler update method (*Update* or *Full*) is not respected for automatic FTP uploads; instead the FTP uploader always uses the *Update* method. In particular it means that:

- In the initial phase a full upload is used until the maximum number of allowed backup sets is reached on the FTP server,
- After that always the oldest FTP backup set is updated (i.e. just the differences are transferred) with the backup set being uploaded.

Note that **pinned backup sets** copied to FTP server are never updated by the scheduler. It is the same behavior as for the locale sets. The only difference is that the remote sets do not display the pin attribute in the *FTP Backup Sets* dialog.

---

[5] v2.11 is the first RescoBackup version that introduced the mechanism to catch up backup errors and store them as a backup set atribute. On the other hand, FTP upload errors cause an error status of the remote set. (See the Implementation chapter.)

[6] The reason: Remote set does not contain the manifest file; hence the synchronization cannot be performed. If you want to download such a set, you need to delete/rename its local equivalent.

3.5 Implementation

3.5.1 Connection details

- RscBackup implementation uses exclusively passive mode and does not support transfer resume.
- In case a file transfer fails, there is an attempt to repeat the transfer, but just once per file.
- RscBackup uses port 21 (unless you specify explicitly another port).
- If you always work with a nested directory on the server side, then you can specify it directly in the connection string, e.g. ftp.microsoft.com/pub/my_dir
- "..." wait message appears whenever a single send or receive communication takes too long. If you see the ellipsis for a considerable time, then there is a connection problem or the server is overloaded.

3.5.2 FTP Log

Checking the FTP log:

The log contains complete history of the commands sent and server responses received since the last connect. (Excl. data communication, of course.) To display the log use the menu command *FTP log*.

Analyzing the log:

The log is created in the interaction of RscBackup and remote FTP server and as such is technically oriented. Disregarding this, it is often possible to detect the problem from the log. (After all, there is no other possibility.)

Sent commands are numbered for easier orientation.

Server responses always start with a numerical code, e.g. the 5xx codes denote a negative reply. (The meaning of the codes can be easily found on the web.)

Comparing against another FTP client:

In case of problem you may verify the server functionality using independent FTP client.

There are plenty of free desktop clients. Just pay attention that you correctly setup the connection. (Use passive mode.) You can even compare the logs from both programs and come closer to the problem.

3.5.3 Upload algorithm

Here is the sequence of the steps involved in any backup set upload:

- The name of the backup set that is being uploaded is prefixed with “~”. Concerns both first upload and any update of the backup set.
- Upload of individual files follows.
- Manifest file[7] is uploaded as the last file.
- After all uploads are successfully completed, the “~” prefix is removed from the remote backup set.

[7] Manifest file collects the information about the backup set files such as the name, date and checksum.

Above algorithm guaranties that any remote set with a standard name (i.e. not starting with a "~") is correct and contains a valid manifest file. All remaining remote sets have an error.

In case of an update of a remote backup set the sequence is modified: The manifest file is downloaded first and compared to the contents of the local backup set. This yields the list of files that need to be uploaded.

As a result the backup set upload is both efficient and safe.

4 Migration support

This is a bit risky topic as it has a potential of causing support nightmares from users with unrealistic expectations. Despite that we decided to include it, as it seems to be a helpful tool.

In short, the Restore allows (beyond the traditional full and partial restore) also 3rd option called *Device Migration*. If you select this option, you get eventually into the traditional Restore screen with lots of files unselected.

Actually a successful migration means nothing more but correct selection of the files that will be transferred. And that's the whole problem. We did what we considered correct based on the analysis of several handhelds and a number of 3rd party applications, extensions, drivers, hacks, DA's, exchange libraries etc. etc. etc. You know what I mean? Given a huge multitude of Palm OS software that often uses undocumented or system-dependent tricks and given many official patches, often accessible just to selected user groups, a reliable algorithm for device migration does not exist.

So take our selection as a suggestion. You may accept it or go your own way. Most probably there is a large group of users where it will work.

Some general remarks you might find helpful:

- Normally the migration is done so that you hard reset the device and insert a card with a backup set created on another device and perform a Restore.
- Restore between the devices of the same type is no migration. In this case just go for a full reset.
- If you migrate between Garnet devices (or more generally between devices with very similar Palm OS version), there is a fair chance that you won't have any problem.
- It is a good idea to copy FileZ or Resco Explorer to the card before starting the restore.
- If you get a reset loop, remember to try a warm reset. If it helps, then start the file manager from the card and try to delete suspected software.
- Saved Preferences are switched off by default as they contain a lot of system settings. You may try to allow this file – finally it's here where the program settings (and registrations) use to be stored.
- 3rd party apps usually do not cause problems. However, there are exceptions – skins, cache files etc. If you identify a cache file by the name, do not restore it.
- Alternatively, do not hard reset the device; instead restore backup set part by part. But even here you can go via Device Migration option as it gives you valuable hints.
- Finally, a migration using Hotsync is a possibility, too. (Search the web.)