Encrypt Files

Introduction

There are five secure encryption formats in Encryption Suite Pro:

- **PA encryption** - secure PA encryption, usable only with Encryption Suite Pro. **Most secure format in Encryption Suite Pro!**
- **PAE/PAE2 encryption** - special encryption container format and can be used for all different archives supported in Encryption Suite Pro.
- **ZIP AES encryption** - secure ZIP encryption, usable with newest versions of most popular zip utilities (recommended for compatibility).
- **7-Zip AES encryption** - AES encryption when you use 7-Zip format for compression.
- **OpenPGP Encryption** – Full support for OpenPGP format. From encrypting/decrypting files to creating/importing/exporting OpenPGP keys.

Introduction to .PA encryption

Encryption Suite Pro features the Advanced Codec Pack which enables the .PA format. It has the most secure encryption in Encryption Suite Pro, and is more secure than ZIP and 7z AES. For added security, we use the BWTS algorithm to scramble the data before AES encryption, so attackers can not use LZ compression redundancy and other plaintext attacks to quickly check if given password is valid. This makes the .PA format considerably more secure than ZIP AES. For the AES encryption module, we use FIPS 140-2 validated modules from Windows so you can rest assured that AES implementation has been tested and validated (FIPS 140-2 encryption module is always used). PA format is only used by Encryption Suite Pro.

Using Encrypt tool

To start the Encrypt tool, select "**Encrypt Files**" from the "**Files**" menu in the Encryption Suite Pro main screen.

At the Encrypt dialog window, you will need to do several things:

- **Add Files** - select the file/s that is/are going to be encrypted.
- **Add Folders** - select the folder/s that is/are going to be encrypted. You can add one more more folders to the encryption tracklist.
- **Remove** - Remove one, many or all files from encryption tracklist.

- **Encryption Options** - Select format you want to to encrypt file/archive to.
- **ZIP Encryption Options** - encrypt file/archive in ZIP format encryption including AES encryption. Encryption methods:
    - **AES 128-bits** - creates encrypted ZIP archives with AES 128-bit encryption, readable by Encryption Suite Pro and newer Zip utilities (PowerArchiver 9.xx, PkZip 8.xx, WinZip 9.xx, etc).

    - **AES 192-bits** - creates encrypted ZIP archives with AES 192-bit encryption, readable by Encryption Suite Pro and newer Zip utilities (PowerArchiver 9.xx, PkZip 8.xx, WinZip 9.xx, etc).
    - **AES 256-bits** - creates encrypted ZIP archives with AES 256-bit encryption, readable by Encryption Suite Pro and newer Zip utilities (PowerArchiver 9.xx, PkZip 8.xx, WinZip 9.xx, etc).

- **7-Zip** - encrypt file/archive in 7-Zip AES 256-bits format.
    - **Method** - Choose between “Optimized”, “LZMA”, “LZMA2”, “PPMd” and “Store” methods of compression.
    - **Compression** - Choose the strength of compression of your encrypted archive.
    - **Create Solid Archive** - This option will let you create a Solid archive. All the files in the Solid archives are treated as one big file, which enables much better compression.

- **PA** - creates PA archives with AES 256-bit encryption (most secure).
    - **Secure AES 256-bits** - creates PA archives with AES 256-bit encryption. For added security, we use the BWTS algorithm to scramble the data before AES, so attackers can not use LZ compression redundancy and other plaintext attacks to quickly check if given password is valid. This makes .pa format considerably more secure than ZIP AES. For the AES encryption module, we use FIPS 140-2 validated modules from Windows so you can rest assured that AES implementation has been tested and validated (FIPS 140-2 encryption module is always used).
    - **Encrypt Filenames** - encrypts file names inside archive so they can not be seen before the correct password is used.
    - **Delete Original File after encryption** - will permanently delete the original files once the encryption has occurred. Please use this option carefully as the files will be permanently deleted. In case there is any inconsistency with the created archive and it cannot be extracted.

- **PAE/PAE2** - encrypt selected file/archive in PAE/PAE2 container with following Encryption Methods:
    - **PAE/PAE2** has 5 different methods of encryption available with **AES** (default) being the most secure. We recommend using AES for encryption since it has been elected as a new Advanced Encryption Standard (AES).

- **Compression Options** - select strength and method of compression (ZIP, PA and 7-Zip only).
- Delete original file after encryption“ - when checked, file that was encrypted (source file) will be deleted after encryption.
- Encrypt filename - Encrypts the filename of encrypted file (PAE/PAE2, PA and 7-Zip only).

- **Group Into Single File** - Groups all files/folders in tracklist into one encrypted archive.
- **Encrypt Individually** - Encrypts all files/folders in tracklist into separate archives.
    - **Append Suffix:** - Adds a suffix to the filename of each encrypted archive. “_enc” is the default filename. To change it, place your cursor into the field and type in your own suffix.
- **Destination Folder**
    - **File's Current Folder** - The encrypted archive or archives will be saved in the folder of the originating files that are being encrypted.
    - **Custom Folder** - Saves the encrypted archive or archives in the folder of your choice. To enter the custom folder to save to, either type in the folder location in the shown field or click the browse browse button to navigate to the desired folder of your choice.

After you have selected the options, click “**Encrypt**” to finish the process and encrypt the file. Encryption Suite Pro will then ask you for a password and you will have to enter it two (2) times.

Please note that it is very **IMPORTANT** that you do not forget your password. You will NOT be able to use the file if you forget the password. There is no way you can recover a forgotten PAE/PAE2 password.

PAE Encryption Tips and Tricks

- Encryption Suite's **Password Manager** is able to remember passwords of encrypted files. This option is turned off by default but if you are working in secure environment and use PAE only to send files via the Internet, then you can enable it so you do not have to enter a password each time you want to access your encrypted files. You can do so in "**Options> Configuration> Password Manager**". Your passwords are saved using 256 bit AES encryption.
- You can use Explorer Shell Extensions to encrypt files with one click of the mouse. The Encrypt option is included in right click shell extensions by default and you may remove/add it whenever needed in the Configuration>Shell Extensions section.

From:
https://wiki.powerarchiver.com/espro/ - **Encryption Suite Pro Help**

Permanent link:
https://wiki.powerarchiver.com/espro/en:help:main:files:encrypt_files

Last update: **2018/11/29 04:33**