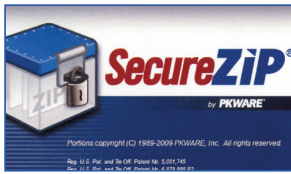


Encrypting Files with SecureZip



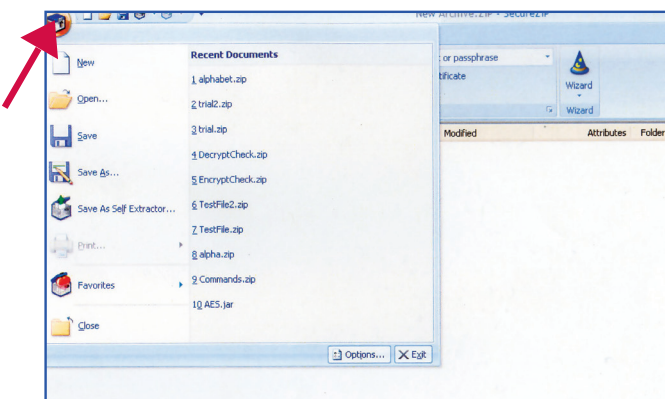
SecureZip is file compression and encryption software for MS Windows users to protect data at rest on computer hard drives, removable media, and e-mail attachments. Encryption algorithms include Advanced Encryption Standard (AES) using a 128-bit, 192-bit, or 256-bit randomly generated key, which is itself encrypted with a key derived from a user-generated passphrase. SecureZip also offers public key-based encryption and digital signature options. An evaluation of SecureZip 12.4 resulted in the setup and configuration guidance presented below.

The guidance in this pamphlet applies only to version 12.4 of SecureZip. Other versions may have different functionality or interface options.

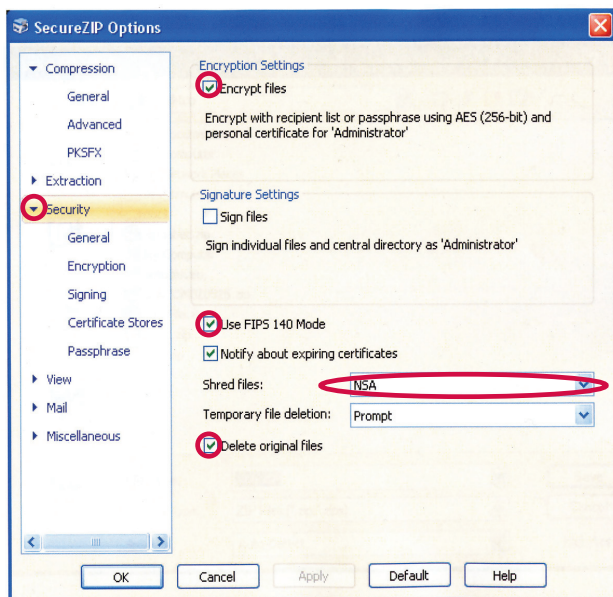
Setup After Installation:

Open SecureZip for Windows (double-click on the desktop icon, or select the program from the Start -> All Programs menu).

Click on the box in the upper left-hand corner and select "Options" (in the bottom right corner of the menu)



Select the "Security" pull down menu on the left side of the window to show the security options.



Select "General" and ensure that "Use FIPS-140 Mode" is checked (select "OK" if a message box pops up). Select "NSA" from the drop-down menu next to "Shred Files," and check the box next to "Delete Original Files." Click "OK" or "Apply." Close SecureZip and then reopen it. Now SecureZip is set up for use.

SecureZip interfaces with Microsoft Office to zip and encrypt files as they are created. Right-clicking on any file in an archive will display a menu with the option to e-mail the file. The menu bar at the top of the window also offers the option to e-mail the entire archive.



Encrypting/Signing

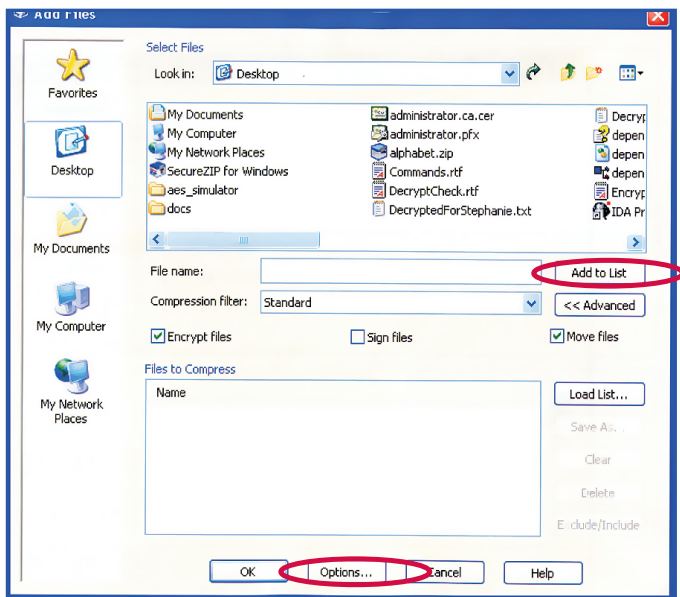
Open an existing archive by clicking the folder icon or create a new archive by clicking the blank document icon at the top of the window.

Select "Add Files" from the menu bar.

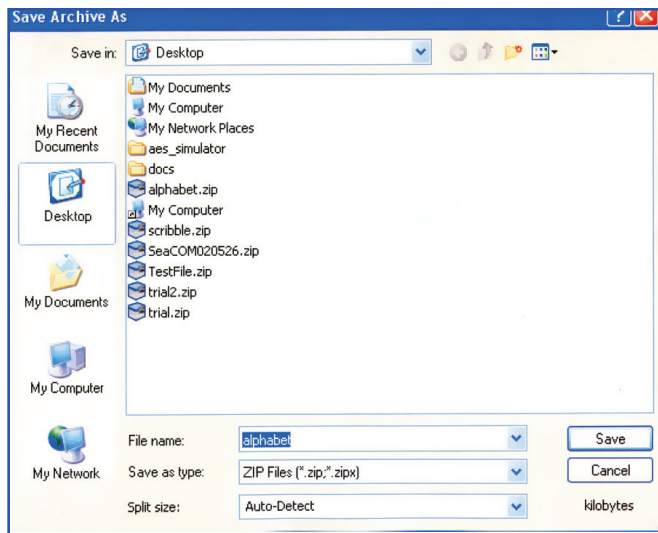
Navigate to the file(s) to add in the browser window and click "Add to List." Choose encrypt/sign as desired and click "Options." Under "Options," use the "Security" pull down menu to select "Encryption." Use "method" to choose one of the strong methods of encryption and "Algorithm" to choose a version of AES depending on the sensitivity of the data to be encrypted. AES-256 is the strongest. Click "OK" (twice).



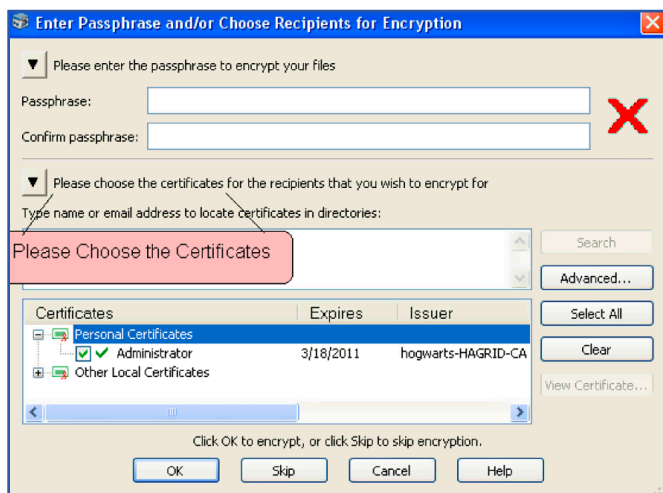
The Information Assurance Mission at NSA



Note: if adding multiple files at one time, the encryption passphrase will be the same for all of these files. If the archive is new, the "Save Archive As" window will pop up. Choose a name for the new archive and a location (if saving on removable media, choose that media as the location), then click "Save."



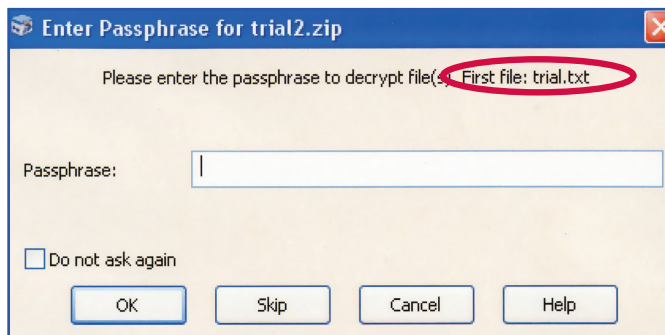
To encrypt files, type in the passphrase (twice) in the passphrase window and/or select the recipients of these files (by e-mail address or certificates listed in the bottom window). If the bottom half of the window is not visible, click on the down arrow next to "Please choose certificates." If encrypting files for storage on the computer, use passphrase encryption and ensure that none of the Personal Certificates are selected. Otherwise, anyone who gains access to the computer will be able to automatically decrypt the files by opening them. After typing in the passphrase (twice) and/or selecting the recipients of the files, click "OK."



Decrypting

To decrypt a file, open the archive it is in. Click "Yes" when asked if you want to open the file. Input the passphrase if needed (if the file encryption is performed via certificate, this is unnecessary) and the file will open. Multiple files may be opened the same way keeping in mind that if there are different passphrases for the files, all of the passphrases will need to be input (carefully correlating the passphrase with each file as the program attempts to open it).

Close the SecureZip program after closing an archive.



Systems and Network Analysis Center

410 854-6632 • DSN: 244-6632 • FAX: 410-854-6604

SNAC DoD, 9800 Savage Rd. Ft. Meade, MD 20755-6704

www.nsa.gov/snac

SNAC@radium.ncsc.mil