Identity Finder Encryption FAQ

Overview

Identity Finder is a DLP (Data Loss Prevention) tool that finds sensitive data on computers, network drives and databases, and can either digitally shred or encrypt that data. This FAQ will explain how to encrypt and decrypt files and discuss the importance of passwords for this encryption/decryption.

Encrypting Files

When "Restricted" information is stored on the network, it should be encrypted for an extra level of protection. Identity Finder encrypts files through the use of passwords. This means that anyone with the password can de-crypt a file.

To encrypt a file, do as follows:
1. Open Identity Finder by clicking the icon on your desktop or going to Start->All Programs->Identity Finder and click the Identity Finder icon.
2. Click the "**Tools**" tab and select the "**Other Tools**" button.

3. Click "**Other Tools**" on the left navigation. Browse to the file you want to secure. If you have more than one file, continue to browse and add files.
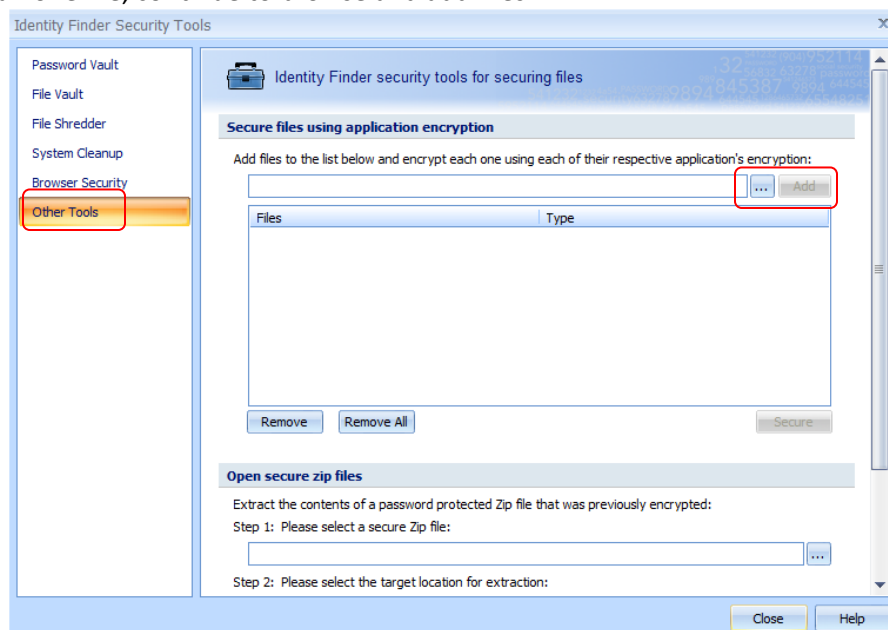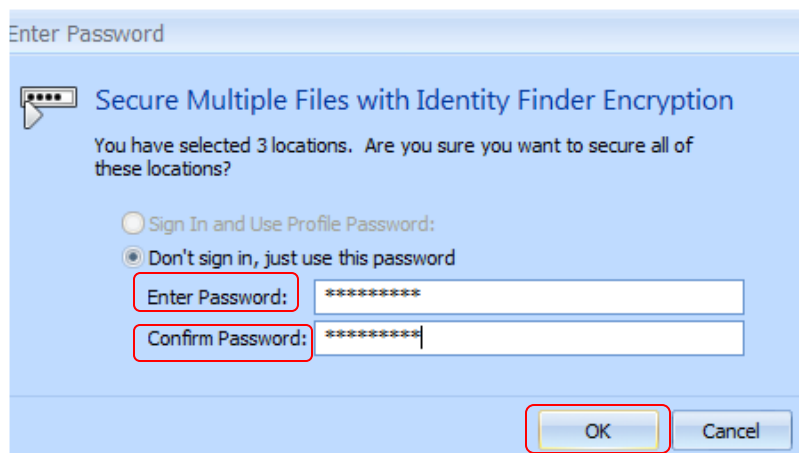
4. Highlight the file or files you want to sure. To select multiple files, hold down the CTRL button and click all files. They files will be highlighted in yellow as noted below.
5. Click the "**Secure**" Button.
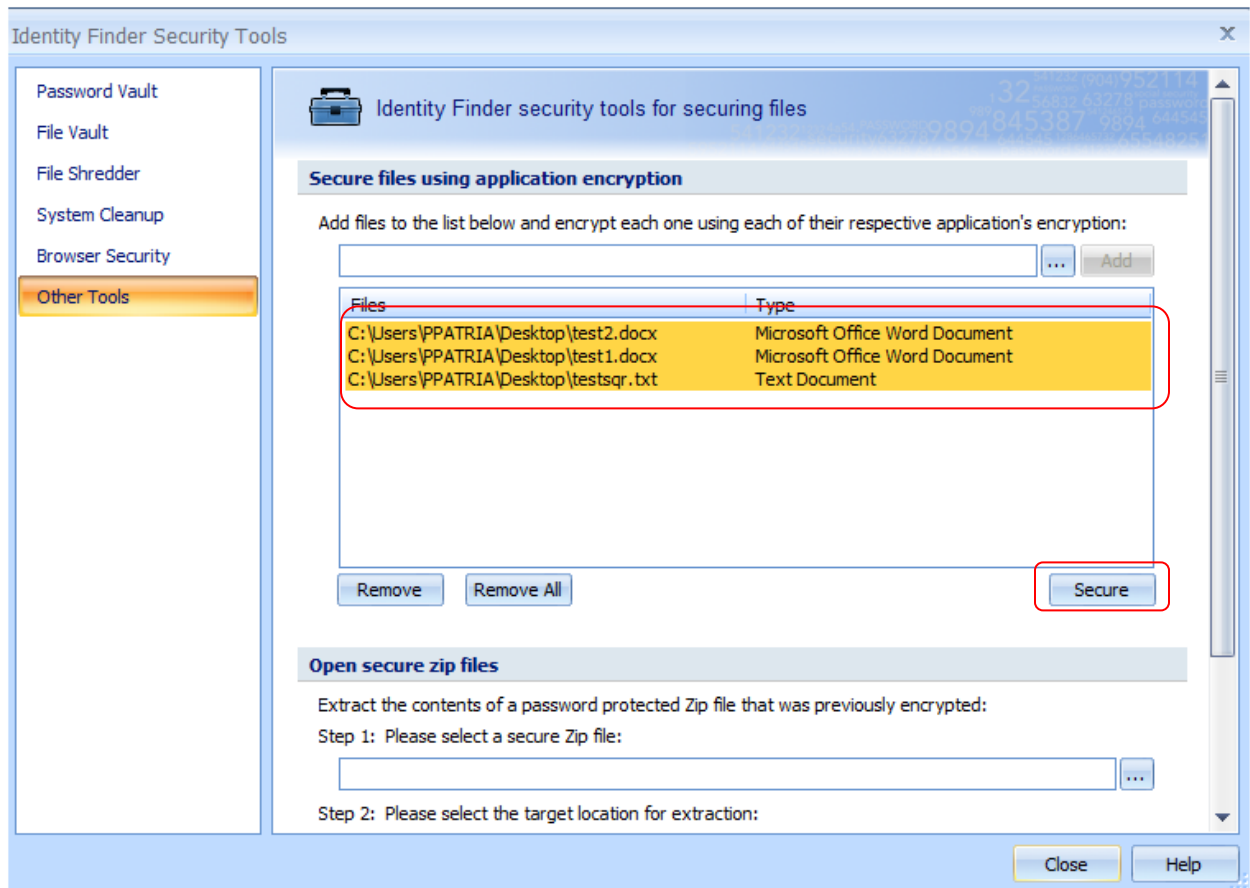
6. You will be prompted to enter a password and confirm the password to encrypt the files. Enter both and click "**OK**" and close "**Close**." You can now close Identity Finder.
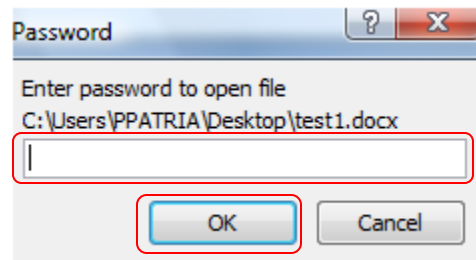
Opening an Encrypted File Office, PDF or Zip File

To open an encrypted file, do as follows:

1. Double click on the file you want to open or open it from the application you normally use (Word, Excel, Access or Adobe PDF). You will be prompted to enter the password used to encrypt the file. Enter it and Click "*OK*".

2. View or make changes as you normally would and save the file. The file will remain encrypted and you can use the same process identified in item 1 above to open the file again.

Decrypting an Office, PDF or Zip File

To decrypt a file, do as follows:

1. Open the application used for editing the file (i.e. Word, Excel, Access).
2. Use the password to open the document.
3. Click the Microsoft Office Button , point to "*Prepare"*, and then click "*Encrypt Document"*.
4. In the Encrypt Document dialog box, in the Password box, delete the encrypted password, and then click OK.
5. Save the file. The encryption will now be removed.

Using or Decrypting other File Types

For files other than Office, PDF and Zip files (i.e., .csv or .lis files), follow the instructions below:

1. In Windows Explorer, Right Click (RMB) on the file you want to use or decrypt. Select Identity Finder->Extract from Vault.
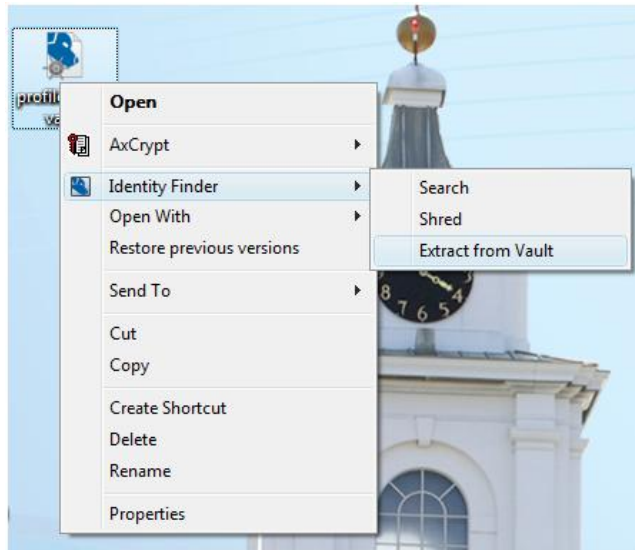
2. The file will be decrypted and available for use.
3. To encrypt the file again after use, Right Click (RMB) on the file you want to encrypt. Select Identity Finder->Secure with Vault.

Important Information on Identity Finder Encryption

- Because Identity Finder uses passwords to encrypt files instead of keys, if you forget the password, you will not be able to open the file.
- If encryption is being used in departments for departmental information, it is recommended that each department create a standard password or pass phrase that is known by at least 2 people; if one person is unavailable or leaves the university, the other person will always know the password.
- If the department chooses to write the password down, it should be stored in a locked cabinet.