Identity Finder: Managing Your Results

The most important part of running Identity Finder is determining the most effective and secure way of managing the search results. Be sure to carefully read and proceed through each of the following steps.

For help with downloading, installing or configuring Identity Finder, please refer to the documentation found at www.cmu.edu/computing/security/idfinder/.

Contents
1. Determine the File’s Origin................................................................. 2
   Where did the file come from? ....................................................... 2
      Carnegie Mellon Business/Academic Operations or Personal Data ........................................ 2
      Files Left From Previous Owners .................................................. 2
2. Actions and the Password Vault ......................................................... 3
   Actions ................................................................................................ 3
   Shred .................................................................................................... 3
   Scrub ...................................................................................................... 4
   Secure ................................................................................................... 4
   Quarantine ........................................................................................... 5
   Recycle ................................................................................................. 5
   Ignore .................................................................................................... 5
   Password Vault (Windows Only) .......................................................... 6
      Accessing the Password Vault Tool .................................................. 6
3. Acting on Search Results ........................................................................ 7
   Windows ............................................................................................... 7
      Accessing Your Saved Information .................................................... 8
4. Other PII .............................................................................................. 8
   File Shredder ....................................................................................... 9
   Open Secure Zip Files ......................................................................... 9
5. Handling Outlook Email Items ............................................................... 11
   Remove Outlook Password ................................................................ 11
1. Determine the File’s Origin
For each file that contains personally-identifiable information (PII), consider these points:

IMPORTANT NOTE: If you are under a litigation hold, contact the Office of General Counsel (412-268-2000) or jamercoll@andrew.cmu.edu or dmunsch@andrew.cmu.edu) before making any changes.

Where did the file come from?

- Is it your personal file?
- A file from someone who previously used or owned the computer?
- A file from Carnegie Mellon business or academic operations?
- Do you have no idea where it originated?

Carnegie Mellon Business/Academic Operations or Personal Data
If you are unsure whether you need to retain a file containing PII related to Carnegie Mellon business or academic operations, please consult your supervisor/advisor.

- If the file does not need to be retained, shred the file.
- If the file does need to be retained, ask yourself if you need the sensitive PII portions.
  - If no, then scrub (i.e., replace sensitive PII numbers with XXX while leaving the rest of the file unchanged).
  - If yes, then ask yourself if you need it on this computer?
    - Yes, then secure the file.
    - No, then quarantine the file.

Files Left From Previous Owners

- If Carnegie Mellon provided the computer for business or academic operations, consult your supervisor/advisor to learn what to do with the file.
- If your supervisor/advisor does not believe the file was part of Carnegie Mellon business or academic operations AND you share your computer with co-workers, family or friends, please consult the people with whom you share your computer to determine the source of the file and whether it needs to be retained.
- If you still do not know where the file originated after consulting your supervisor/advisor and the people with whom you share your computer, shred the file.
2. Actions and the Password Vault

Actions

After reviewing your search results, you'll need to select the best way to handle this sensitive information. The following actions are available to you:

Shred

The Shred button is located on the Main ribbon and is enabled for all types of results; however, depending on the location of the result, Shred behaves differently. For files, Shred uses a secure 1pass wipe conforming to Carnegie Mellon's Guidelines for Data Protection - Media Sanitization and Disposal. For other locations, shred removes the information from your computer using other, appropriate methods.

Identity matches can be shredded using one of the following methods:

- Single-click the result with the left mouse button to highlight it and click the Shred button on the Main ribbon.
- Single-click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on Shred.
- Highlight the result by single-clicking with the left mouse button or by using the arrow keys and then press the Delete key on your keyboard.

Important Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone. To ensure that you did not click on the shred button accidently, Identity Finder will generate a message after you click on the Shred button asking whether you are sure you want to shred the file.
Scrub
(Text, CSV, and HTML files only as of version 8.0)

When a text file has sensitive identity match information in it and you wish to keep the file on your computer, but do not need the personally identifiable information (PII), you should use the Scrub feature. Scrubbing (also known as redacting) secures files by removing PII information and leaving all other content in place. Identity Finder will replace the data with multiple X characters by default. You can change the replacement character to a number under Settings>Actions>Options for Scrub.

- To secure a single text-based file with the Scrub feature, left-click the file result to highlight it and click the Scrub button on the ribbon.
- To redact multiple text files at one time, check the checkbox of each file and then select Scrub.
- You can choose to redact the personal information and replace it with your default choice from your File>Settings>Actions>Options for Scrub and check the box on Scrub all characters of a result except for the last four option, or you can select any digit from 0 to 9 or an X. Once you click OK for the Scrub action, the personal information will be permanently overwritten and cannot be undone.

Secure
Identity Finder for Windows allow users to select from two types of encryption to password-protect a file; Secure with Profile Password allows users to secure a file with Identity Finder File Vault encryption, and Secure with Alternate Password provides an option to select a new password to secure that particular file. Identity Finder for Mac does not offer application-specific encryption and will always use Identity Finder File Vault encryption.

Important notes on securing
- The Secure action will password-protect the selected file using your profile password.
- Once a file has been password-protected using Identity Finder File Vault encryption, double-clicking it will open Identity Finder to decrypt it and prompt for the password.
- If you forget the password, you will not be able to recover the document.
- If you plan to encrypt files for Carnegie Mellon business or academic operations, make sure you write down your profile password, lock it in a secure location and inform your supervisor of the secure location to ensure business continuity.
Quarantine
Securely moves the highlighted file to a quarantine location and permanently shreds it from its original location. Follow these steps to quarantine a file:

1. Highlight the item you want to quarantine and then click on the Quarantine option in the top Actions menu; the Quarantine dialog box appears.
2. Select the Quarantine folder to which you wish to move the file. This should be a folder that is highly secure, such as an encrypted drive or a storage device to which unauthorized individuals do not have access.

**Note:** You can specify a default Quarantine location in **Settings**. You may also choose to leave behind a warning text document in place of the file as a reminder that the file was moved to another location.

Recycle
This feature is disabled on the Carnegie Mellon installer. Moving a file to the Recycle Bin does not actually delete the file. To truly remove a file, use **Shred**.

Ignore
The “Ignore” feature allows you to designate certain items to be ignored by Identity Finder to prevent that information from being displayed in the future.

Click **Ignore** and choose from the following:

- **This Item Location:** To ignore the currently selected location match of the item(s) selected. Selecting Ignore This Item Location will prevent that location from being searched in the future.
- **This Identity Match:** To ignore the currently selected Identity match in ALL locations in which it appears. Identity matches that you add to the Ignore list during a search will be ignored for the reminder of the current search.
• **Manage 'Ignore List':** The settings window that appears will allow you to add or remove identity information or file locations from Identity Finder's Ignore list. By selecting Manage ‘Ignore List’, the View and manage Ignore List option in the Settings window is displayed.
  1. To add identity information, select the identity type from the list under **Ignore Identity**; enter the identity value in the field next to the type list and then click the corresponding **Add button**. For example a string of numbers that Identity Finder identifies as a license number when in actuality the number is used as dummy data for training.
  2. To add a file location, type or browse to the file next to **Ignore Location**. Click **Add**.
  3. To remove an item from the Ignore list, highlight it and click the Remove button, the Remove All button clears the entire list.

**Password Vault (Windows Only)**

The Password Vault tool allows you to securely store and manage usernames and passwords for websites, encrypted files and other locations inside of your password-protected Identity Finder profile. In other words, the Identity Finder profile password is a single master password that allows you to gain access to the Password Vault. Once you've gained access, the Password Vault houses your list of files or accounts and their respective passwords.

**Note:** The Password Vault tool is not available for Mac operating systems. Consider using Mac OS X's Keychain Access as an alternative.

**Accessing the Password Vault Tool**

To access the Password Vault tool, click the **Password Vault** button on the **Tools** ribbon. Another option to access Identity Finder Password Vault without launching Identity Finder search is through **Windows All Programs>Identity Finder Folder>Password Vault.**
3. Acting on Search Results

Follow these steps to manage any PII-related files through Identity Finder.

Windows

With the Identity Finder Search Summary box displayed, click one of the following options:

- **Wizard** - Choose this option to have Identity Finder help you manage the results using the wizard.
- **Advanced** - Choose this option to manage the results manually.
- **Save As** - See the "Securely Saving Your Results" section of this page.
- **Reminder** - Choose this option to set a reminder to deal with the scan results at a later time.

Mac

The results window will be displayed after the search is complete.

1. For each item, select it and then choose the action you want to apply from the top menu items. For more detailed instruction, refer to the Actions section in this document.
2. If you wish to repeat the scan and select additional identities and locations to clean (e.g. external storage media or folder), select the Start Search Wizard from the Start button’s drop down arrow, and then follow the steps included in this Manage Your Results document.
Securely Saving Your Results

If your list of PII is extensive, you can securely save your results and manage them at a later time. The results file is automatically password-protected by your Identity Finder profile password. Follow these steps:

1. Click the **Save** icon (Mac: **File > Save**) and browse to the location where you wish to save the Identity Finder (.idf) file. The **Save As** dialog box appears.
2. Enter a name for your file and click **Save**.
3. Close the Identity Finder window.

Accessing Your Saved Information

1. Ensure Identity Finder is not running.
2. Double-click the results file you previously saved.
3. Enter your Identity Finder profile password when prompted.

4. Other PII

Identity Finder may not recognize some custom file formats; however, Identity Finder cleanup features can still be used to handle these files.

Use the following Identity Finder Security Tools to handle files NOT listed in the Identity Finder search results:

![Identity Finder Security Tools](image)

**File Vault**

The File Vault tool allows you to secure any file on your computer even if no identity match is found in that file. To use the File Vault tool:

1. Click the **Add to File Vault** button on the Tools ribbon. The File Vault dialog opens.
2. Click the browse button to launch a dialog box that allows you to select any file on your computer.
3. After navigating to your desired location, click the **Open** button and the full path to your selected file will be displayed.
4. Then click **Encrypt** and you will be asked to secure the file with your profile password or other password.
5. Choose the appropriate options and click **OK** to secure your file.
   To open an Identity Finder File Vault file, double-click it to launch Identity Finder and then enter your profile password.

**File Shredder**

The File Shredder allows you to shred any file or folder (and all subfolders and files) on your computer, even if no Identity Match is found.

1. Click the **File Shredder** button.
2. When the File Shredder dialog box opens, browse to the folder or file(s) that you want to shred.

**IMPORTANT: YOU CANNOT UNDO THIS ACTION!**

**Open Secure Zip Files**

Other Tools features include the **Open secure zip files** tool which allows you to open and extract (unzip) the contents of any secure zip file on your computer. This is a very useful feature if you used **Secure a Compressed File** or **Secure a Text Based or Other File** in conjunction with the Strong or Stronger encryption setting in a previous version of Identity Finder (the Secure Zip encryption from Identity Finder 3.4.8 and prior has been replaced by File Vault encryption).

To open a secure zip file:
1. On the Tools ribbon, click **Other Tools > Other Tools**. The **Identity Finder Security Tools** dialog appears.

2. Under the **Open secure zip files** section, browse to the location of the zip file, then click **Open**. The full path to your selected file will be displayed.

3. Browse to the desired target location for the unzipped files. After navigating to your desired location, click **OK** and the full path to your selected folder will be displayed.

4. Type your password and click **Extract**. Your files will be extracted to the desired location and a window will open to display the extracted files.

5. Click **Close** to exit the Identity Finder Security Tools window.

   **Note (Mac Only):** Identity Finder for Mac doesn't offer the Shred File tool for shredding files that aren't found in search results, although it does offer file encryption/decryption. By clicking on the Vault icon on the tool bar, you can encrypt and decrypt any file using the Identity Finder Vault format.

The Identity Finder Vault file type is automatically associated with Identity Finder, so double clicking an Identity Finder Vault file will open it in Identity Finder and prompt you for the password.
5. Handling Outlook Email Items

If you are using Outlook (prior to outlook 2010) or other Exchange clients, Identity Finder will locate PII stored in your Cyrus email account. Follow these steps to handle your Outlook items:

1. When the Identity Finder scan completes, files and data locations that contain PII are listed. Click Next.
2. You will be prompted to establish a password for your Outlook Data File, select No and then click Next.
3. To view more information for each item, select it; details appear in the Preview pane. You can also select the item, and then select Open from the menu bar to view details.
4. You can choose to Secure, Shred or Ignore each item.  
   **Note:** If the messages you shred are from a Cyrus account, the message will be marked for deletion, but not erased. To delete the messages, launch Outlook, select your Cyrus Inbox, and then select Edit > Purge Deleted Messages.
5. If you need to retain the content of emails that contain PII, we suggest that you save the Outlook message as a text file or an MS Word document and use Identity Finder's Secure File option.  
   **Note:** The Quarantine clean up action is not available for Outlook email messages.

Remove Outlook Password

Once you are finished handling your Outlook items, be sure to remove your Outlook password; follow these steps:

1. Launch Outlook.
2. Select Tools > Account settings.
3. The Account Settings dialog box appears. Select your Cyrus account and then click Change.

![Account Settings Dialog Box](http://www.cmu.edu/computing/security/idfinder/identityfinder.png)
4. The Change email account dialog box appears. Under the Logon information, deselect the **Remember password** checkbox.

![Server Information and Logon Information](image)

5. Click **Next**.

6. Click **Finish**.