CALIFORNIA STATE UNIVERSITY
Stanislaus
OFFICE OF INFORMATION TECHNOLOGY

Identity Finder
Windows User Guide

Office of Information Technology - OIT

Stanislaus State

Identity Finder for Windows Users

Introduction

Identity Finder is a software application that can help find Personally Identifiable Information (PII) that matches data such as Social Security Number (SSN) or Credit Card Number (CCN) format. In some cases, this type of data can be found in files that are not easy to find, especially older documents that you may have forgotten about. Identity Finder assists you in preventing identity theft by finding personally identifiable information and providing you with the ability to easily and quickly protect it before it is stolen.

The Identity Finder client application provides the ability to save settings, configuration information, and sensitive data across sessions through the use of a profile password. It is not possible to recover a lost password; however, it is possible to delete a profile and create a new one. When the profile password is created, that password is used to encrypt the profile. The profile password is not stored anywhere and therefore if it is lost or forgotten, then all of the information in the profile will be lost. Because the password is not recoverable, some of the user options have been disabled and grayed out from the client window. This is to prevent loss of data in case of lost or forgotten profile passwords.

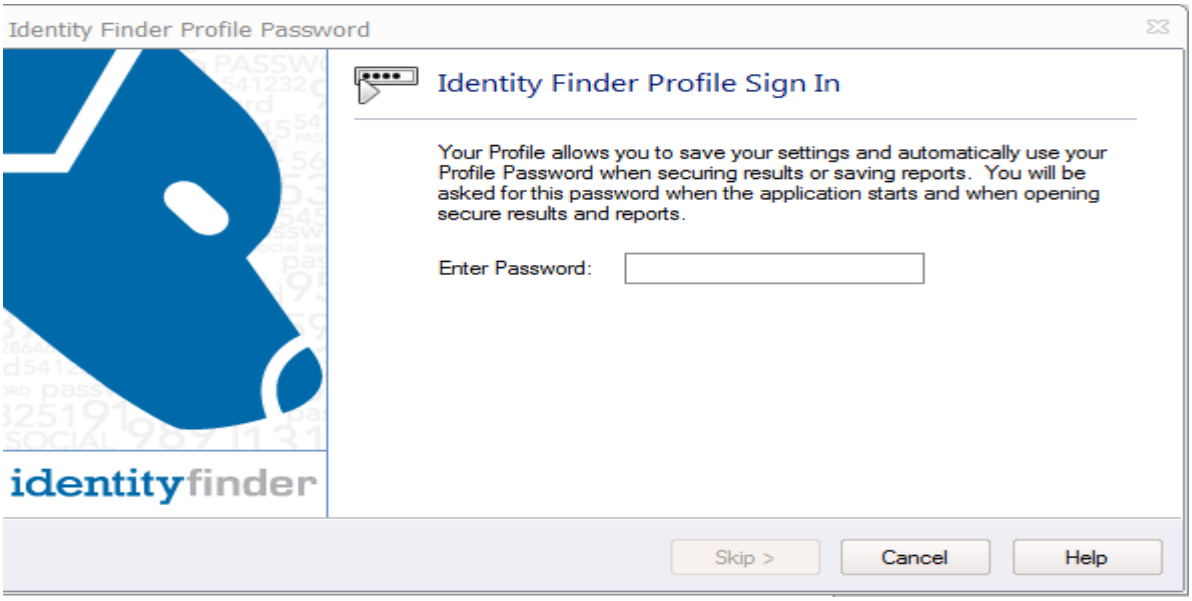
The application will be deployed to your PC. You should go to: Start → All Programs and look for Identity Finder, then double click on the application to launch it.

In case, Identity Finder did not deploy successfully, you could still install it manually.

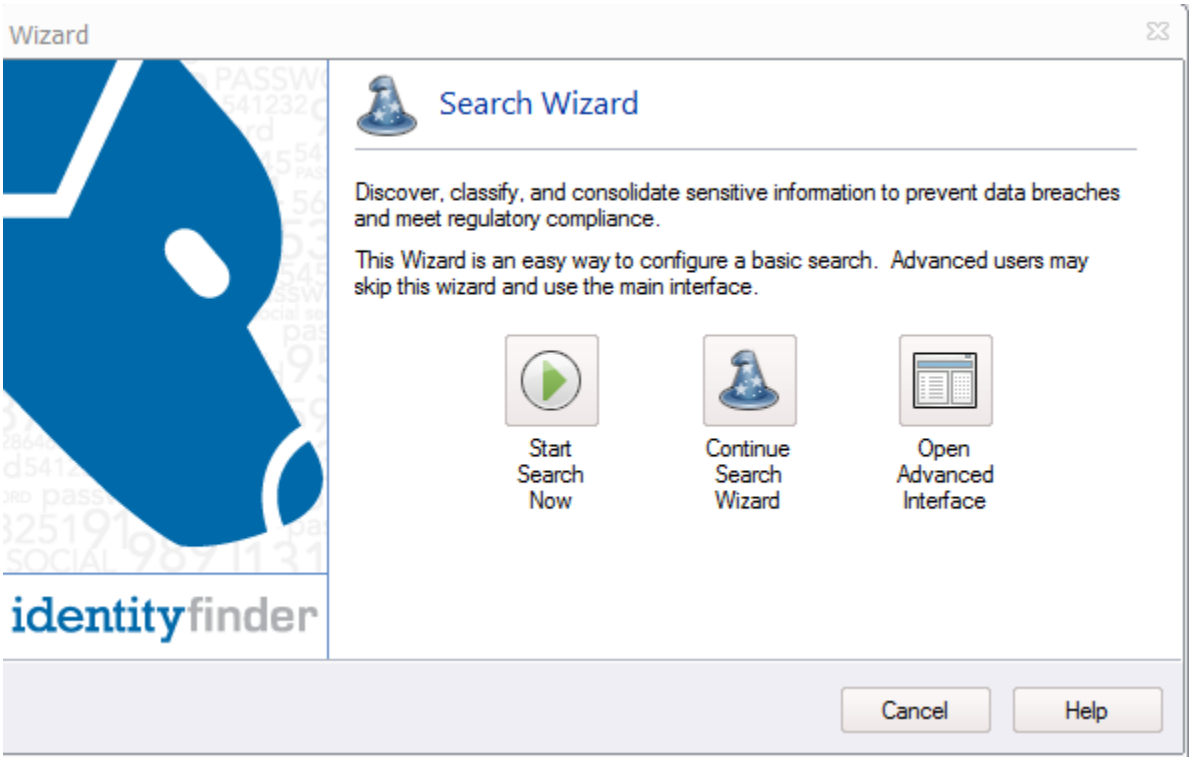
The software location path:

\\staffdrive.csustan.edu\Departments_Shared\OIT-Software\Campus Wide\Identity Finder\IdentityFinder_msi-Windows

Installing the software takes just a few minutes. You should create a user password during this process. Once the installation is complete, start the program and enter your password:



From this windows choose "Open Advanced Interface":



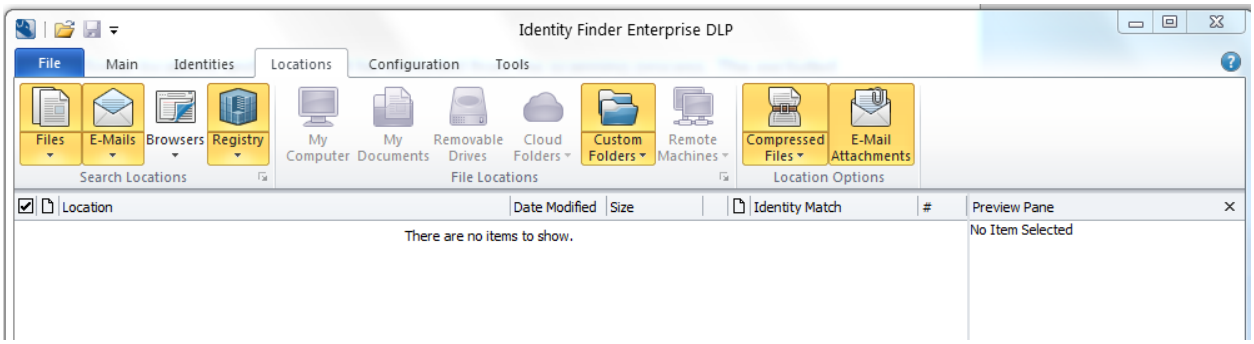
Some locations and files could be excluded from the scanning process. The excluded areas would include for example:

P:

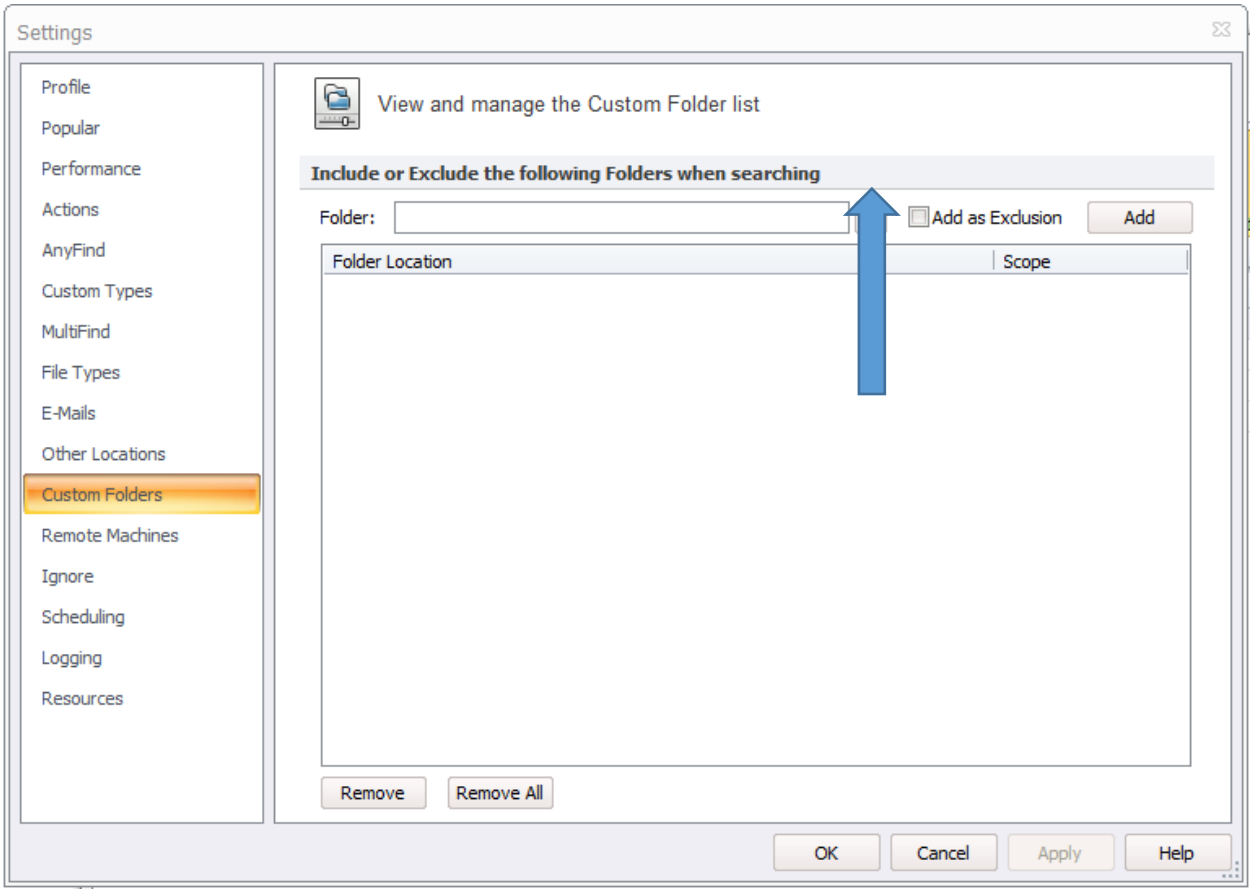
W:

And the excluded program files could be Adobe.

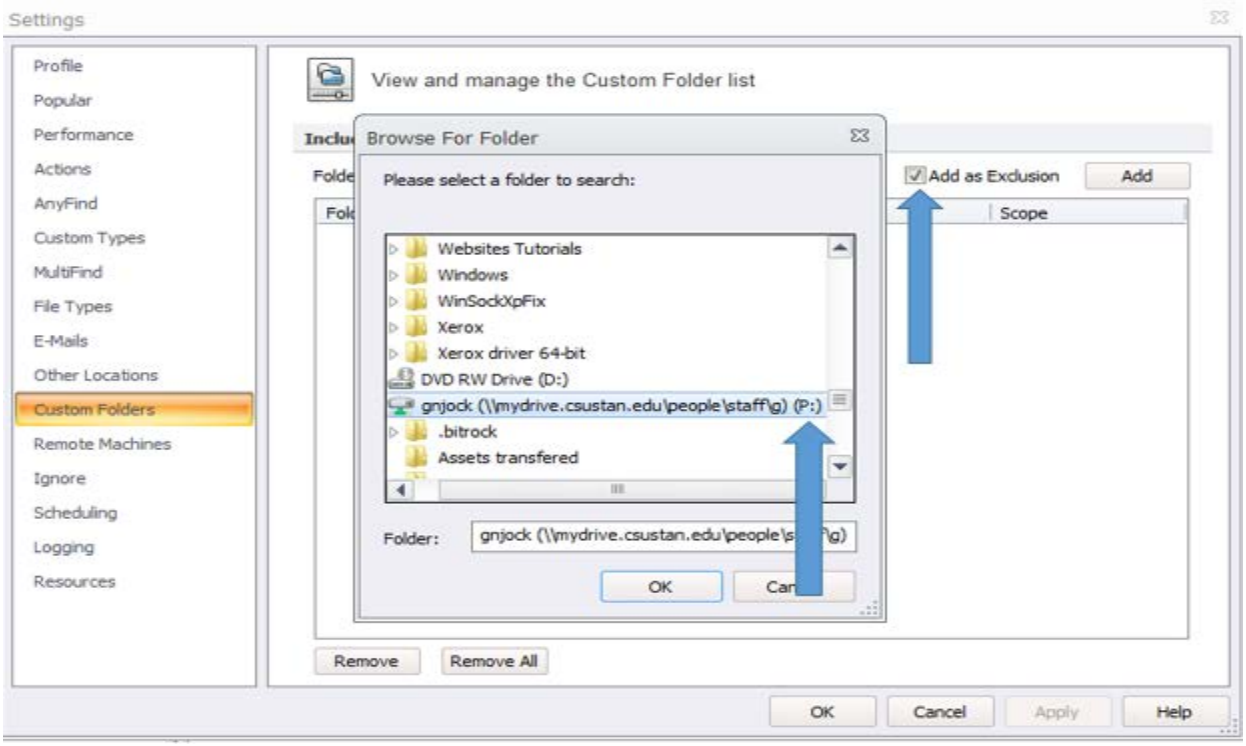
On the menu, choose the "Location" tab, then "Custom Folders" and "Customize folder list"



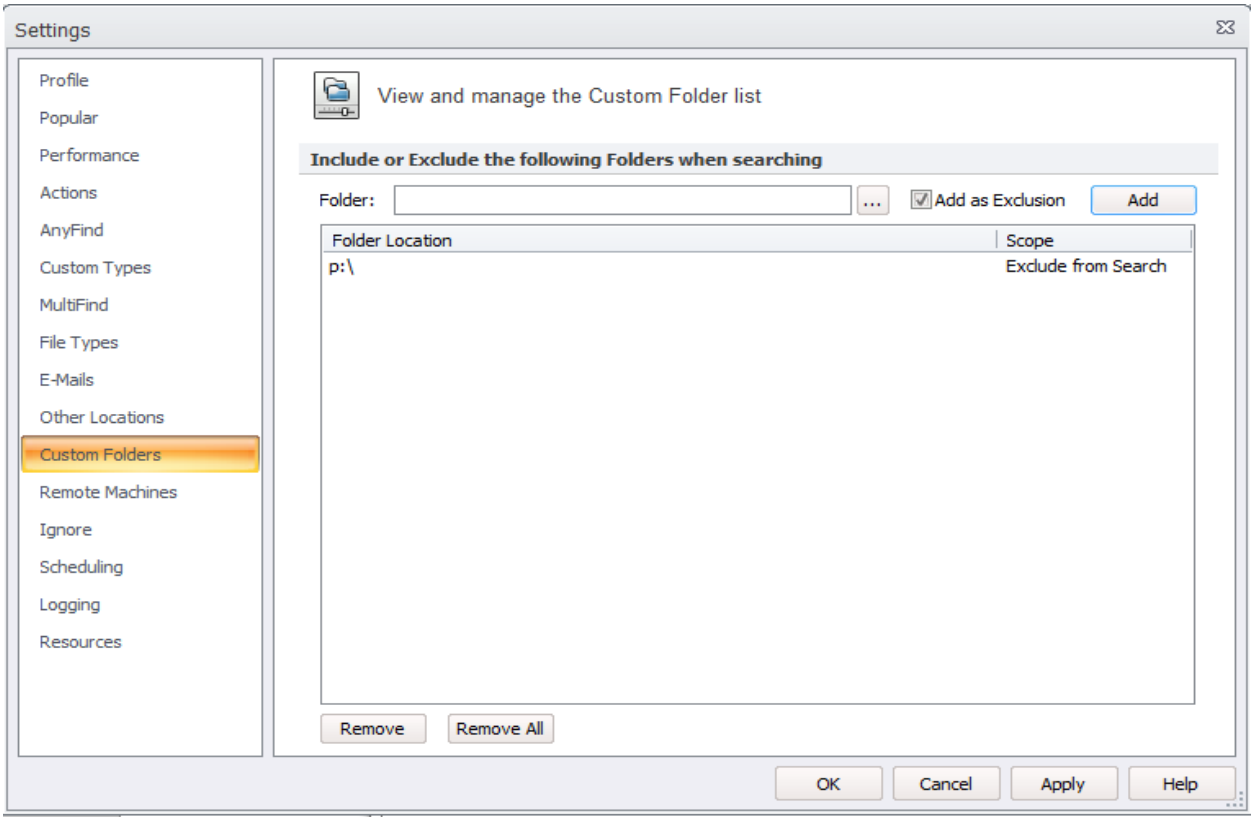
To exclude your P - drive; browse to the location by following the screenshot below:



Then select your P - drive, click OK and check the box next to "Add as Exclusion" and click OK:

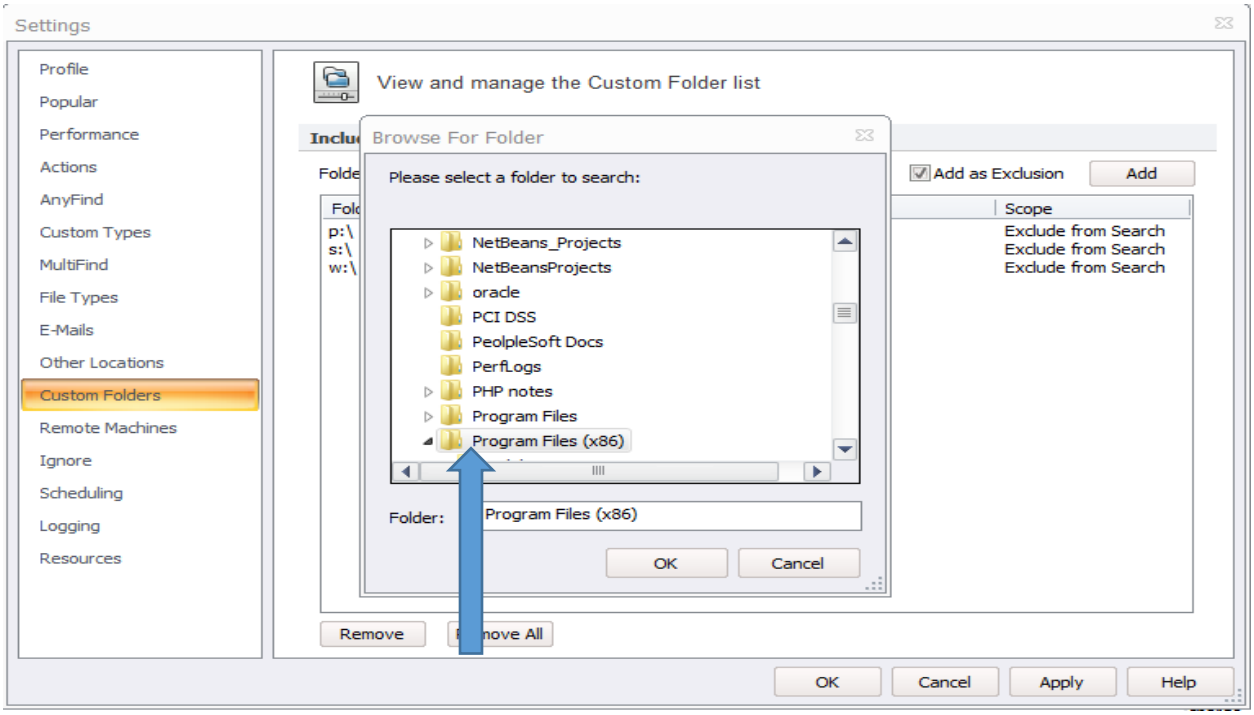


Now P - drive will be excluded from the search:

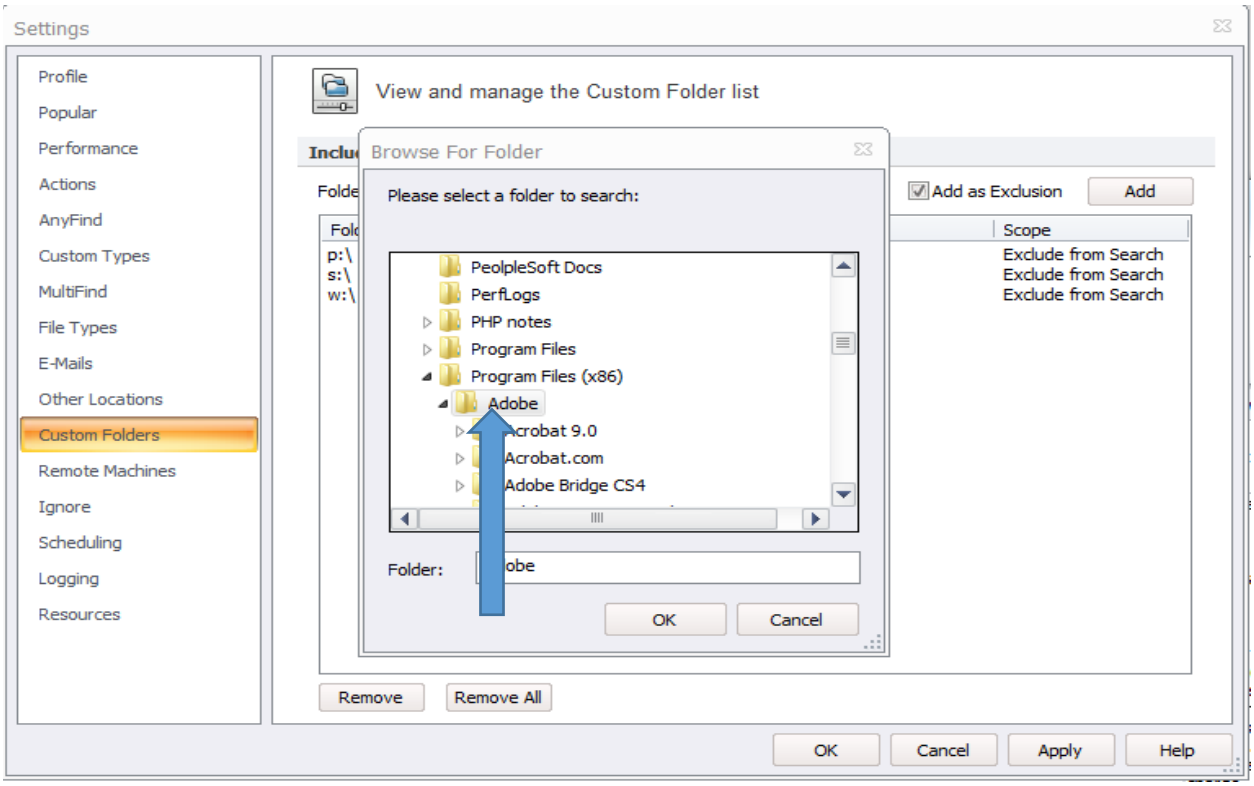


Follow the same process to exclude other search areas such as S and W drives.

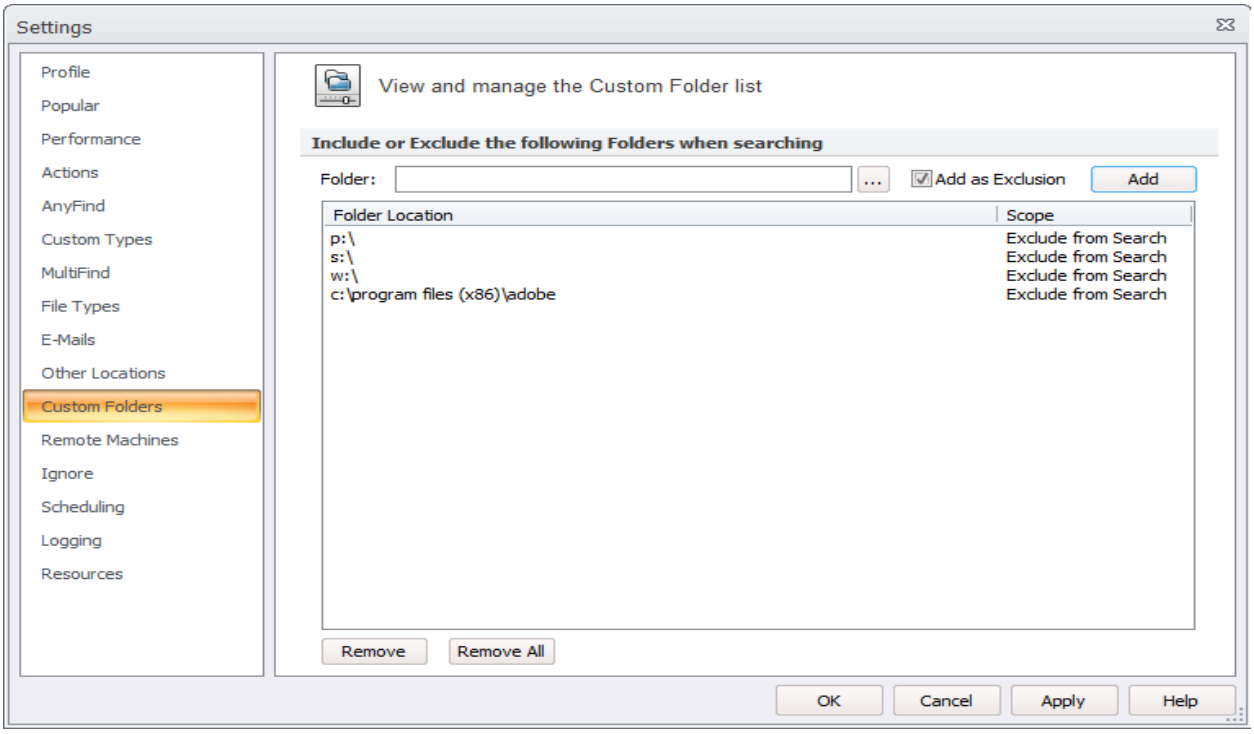
Customize an application such as Adobe; browse to the program folder:



Choose the program to exclude from the search and click OK.

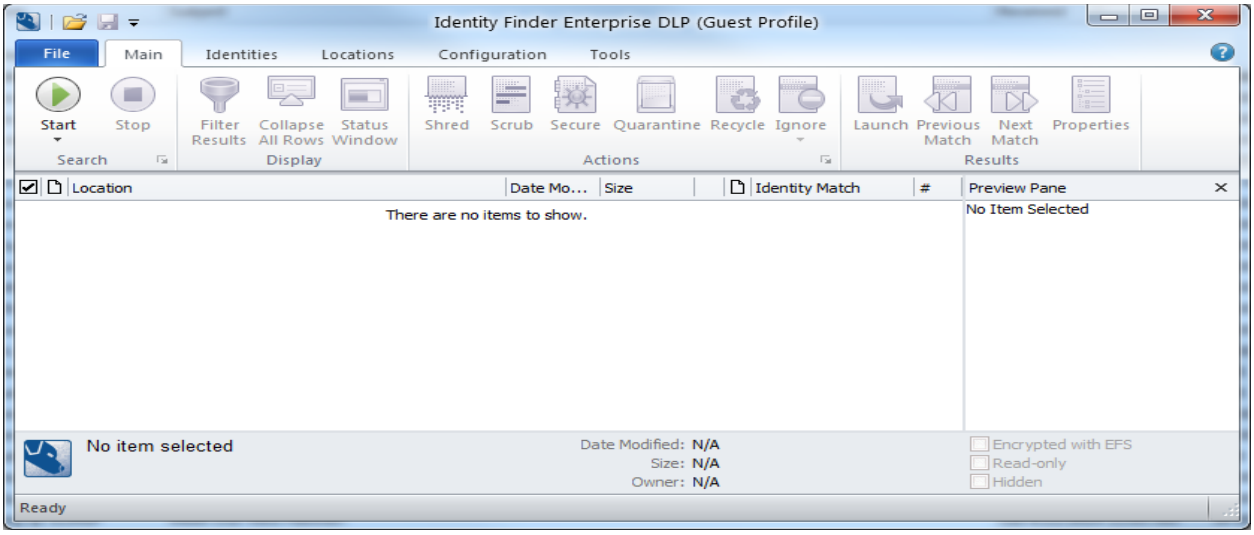


The result below will be display.

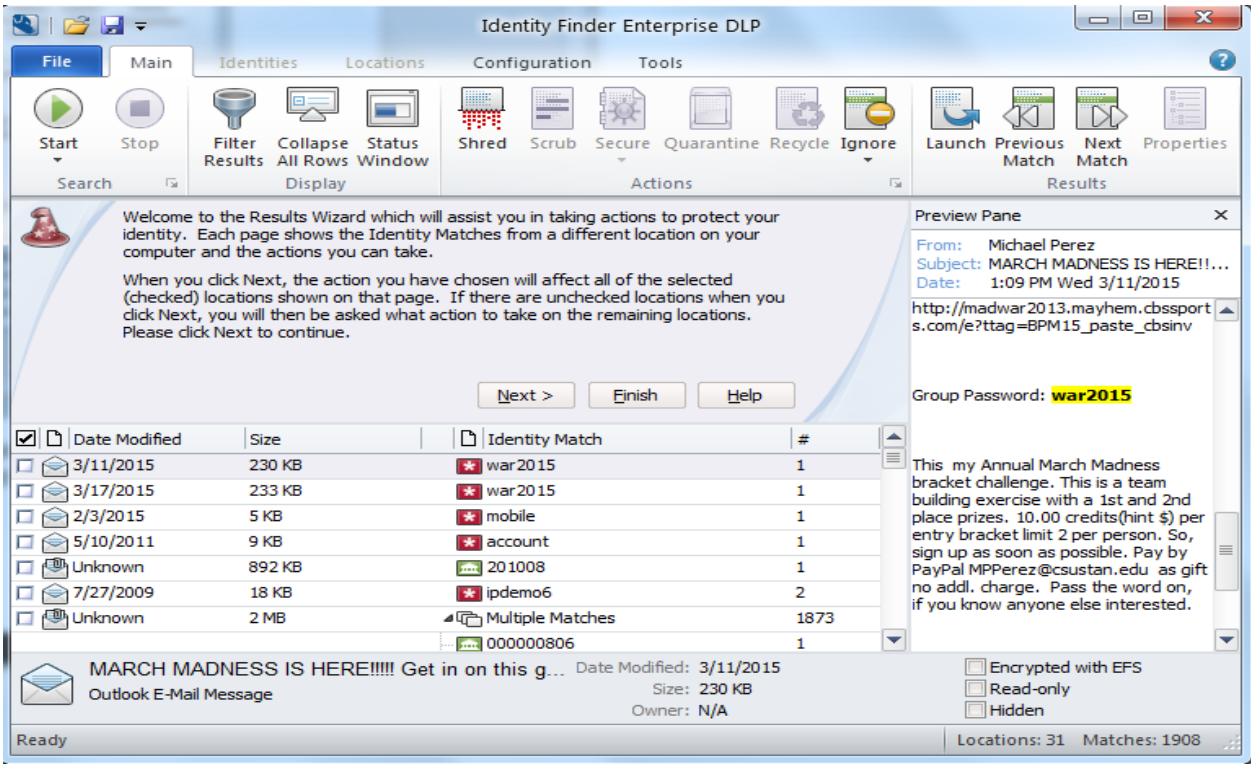


Scanning your computer

To begin a scan, click the Start button.



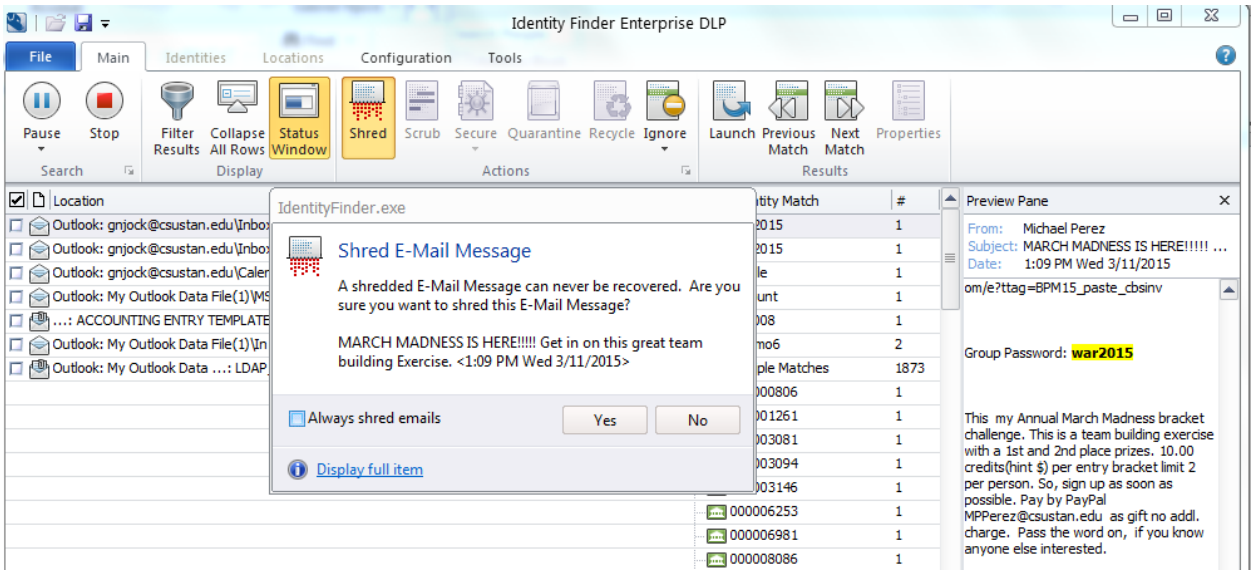
It is recommend to start your first scan before you leave work in the evening, then press Control-Alt-Delete, and click "Lock this computer" on your way out. You will be presented with the similar results page below after the scan completes:



The search result page is where you get to review and remediate your findings and from the File tab, you always want to save the results for future review and to avoid another full scan next time you initiate a search. To save a copy of the search results, click **File** and **Save As - Identity Finder (secure file)**.

Remediation of discovered PII or Sensitive Data

Identity Finder has options to process PII or sensitive data – Ignore, Quarantine, Recycle, Shred or Scrub.



Shredding PII or Sensitive Data

If you wish to permanently remove a file that contains SSN or CCN data, select the Shred option. For files, Shred utilizes a secure United States Department of Defense wiping standard known as DOD 5220.22-M. For other locations, Shred removes the information from your computer using other appropriate methods. This option should be used when the file found is no longer needed on the user's computer

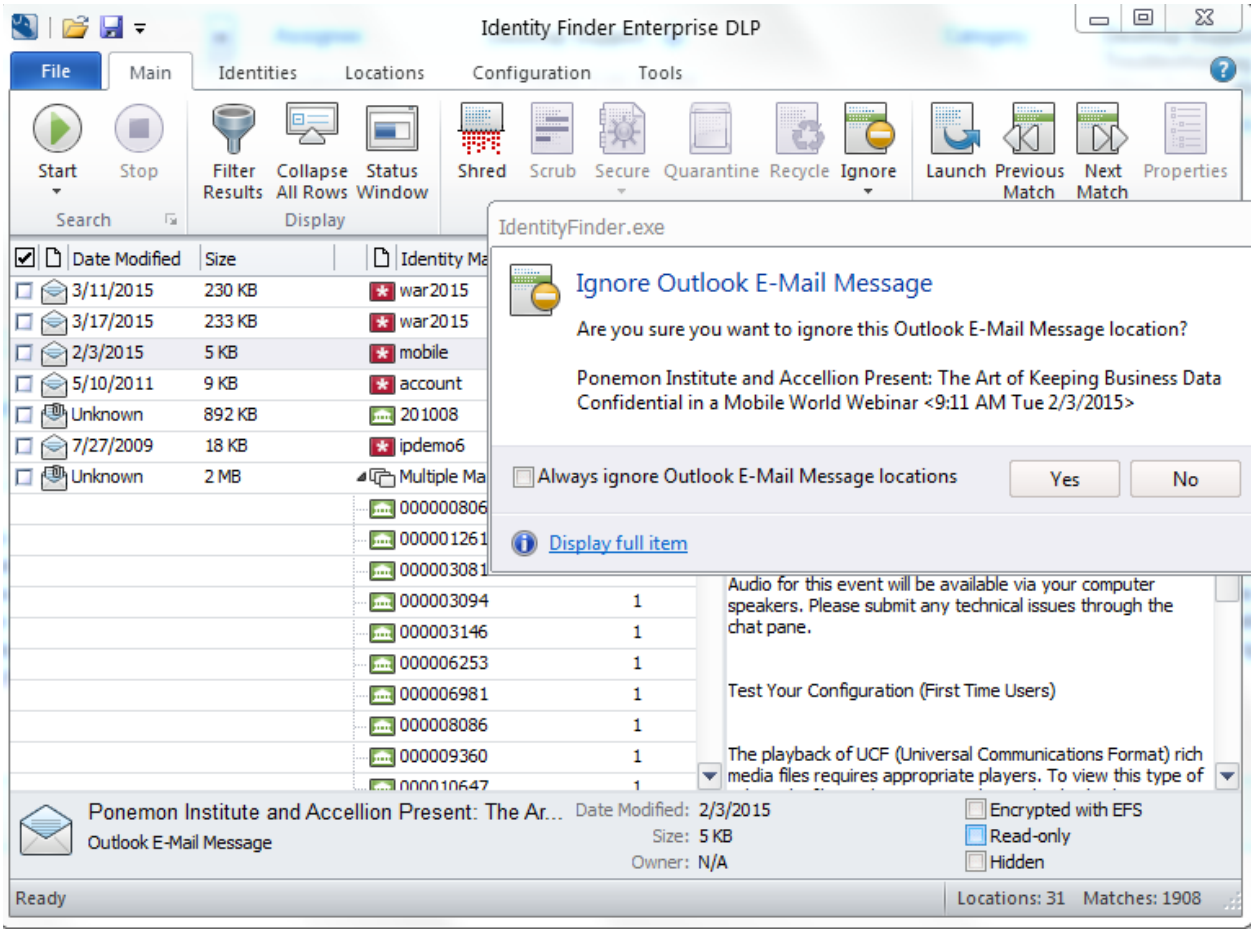
Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.

There are three ways to Shred:

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

Shred is effective at protecting your identity because it is permanent. While this means you can never get your data back, it also means a hacker or malicious intruder also cannot get this data.

Ignoring PII or Sensitive Data



The Ignore option should be utilized when a false positive result is found. A false positive is when Identity Finder marks a file as PII, when it is really not. An example is when Identity Finder picks up a campus 9 digit employee id as a social security number.

The ignore option will allow the user to tell Identity Finder to ignore this piece of data, and for this and all subsequent searches run on that computer. This can be used to manage PII that you plan on securing or disposing of by other means, or the function can be used to handle false positives.

Why the Secure option is not available

The Secure function is useful when Identity Finder locates a piece of PII that a user would like to keep on their local machine. The Secure feature will encrypt the file and may only be accessed with the password set at the time of encryption. Though this feature may seem advantageous, it has its drawbacks. For example, if a user were to forget the password to the file, the data will not be recoverable.

Reset Profile Password

The Identity Finder client application provides the ability to save settings, configuration information, and sensitive data across sessions through the use of a profile password. It is not possible to recover a lost password; however, it is possible to delete a profile and create a new one. When the profile password is created, that password is used to encrypt the profile. The profile password is not stored anywhere and therefore if it is lost or forgotten, then all of the information in the profile will be lost.

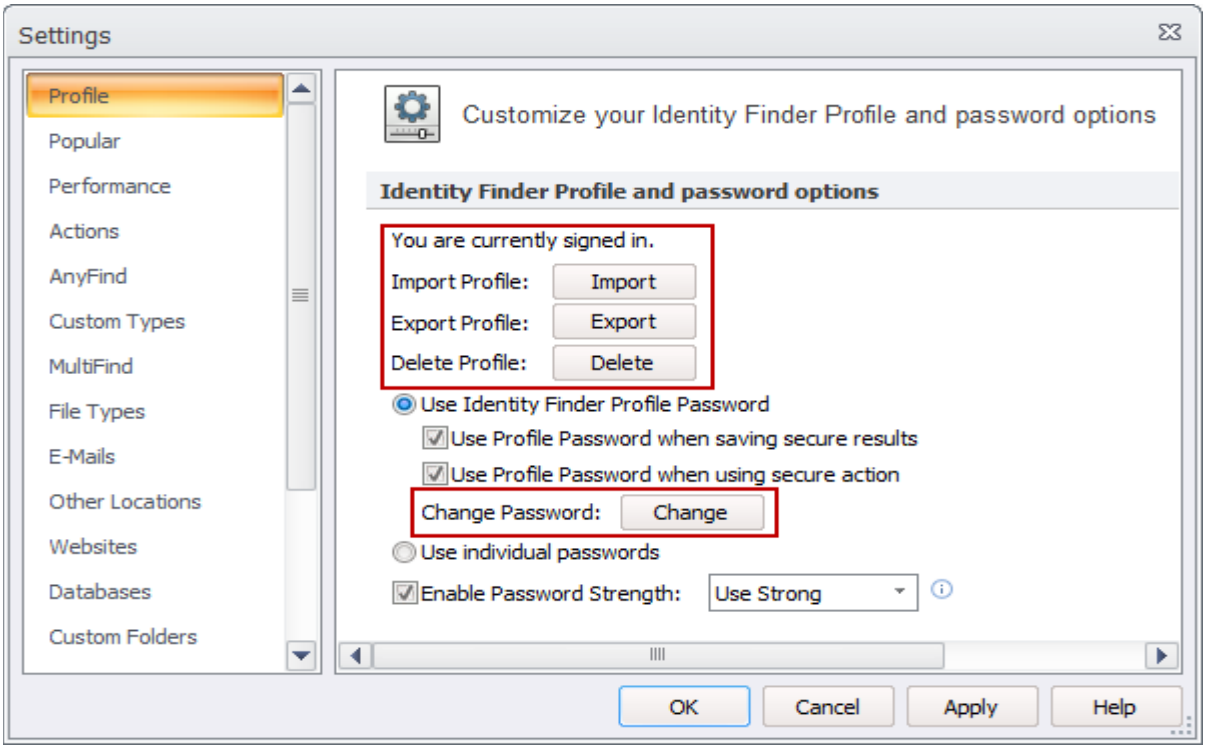
Using Identity Finder to Delete a Profile

A profile can be deleted by logging into Identity Finder as a guest by skipping the password screen, opening the Profile page within Settings/Preferences (Select the Configuration menu item and then select Settings), and clicking the Delete profile button.

Managing Your Profile

Identity Finder uses a single master password to securely store all your personal information related to Identity Finder inside a Profile. If you want to delete this file and all the information

contained within, press the *Delete* button. You can also change your password. To change the password first sign into your profile then click the *Change* button.



Resource links:

Identity Finder Knowledge Base
http://www.identityfinder.com/kb/

Identity Finder Profile
Settings https://www.identityfinder.com/help/client_win/index.htm#ProfileSettings.htm

DLP Endpoint for Windows
User Guide http://www.identityfinder.com/Help/Client_Win

DLP Endpoint for Mac
User Guide http://www.identityfinder.com/Help/Client_Mac