Identity Finder User Guide

CSU East Bay

Information Security Office (ISO)

January 2015

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 or delete 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.

For CSU East Bay users, the Identity Finder software has been pre-configured:

- Opens directly to the Main tab
- Will search for Social Security Numbers (SSN), Credit Card Numbers (CCN), Bank Accounts, Date of Birth, Driver License numbers, Passport numbers, Passwords
- Set to Search All Files (including compressed files) on all physically connected drives
- Has set CPU utilization to the lowest possible setting
- Will only report last four digits of any findings to the Identity Finder server
- If PII data is found, the application will display the results. Should there be a need to keep PII data on your machine please contact the ISO office and they will guide you on how to properly handle such data.

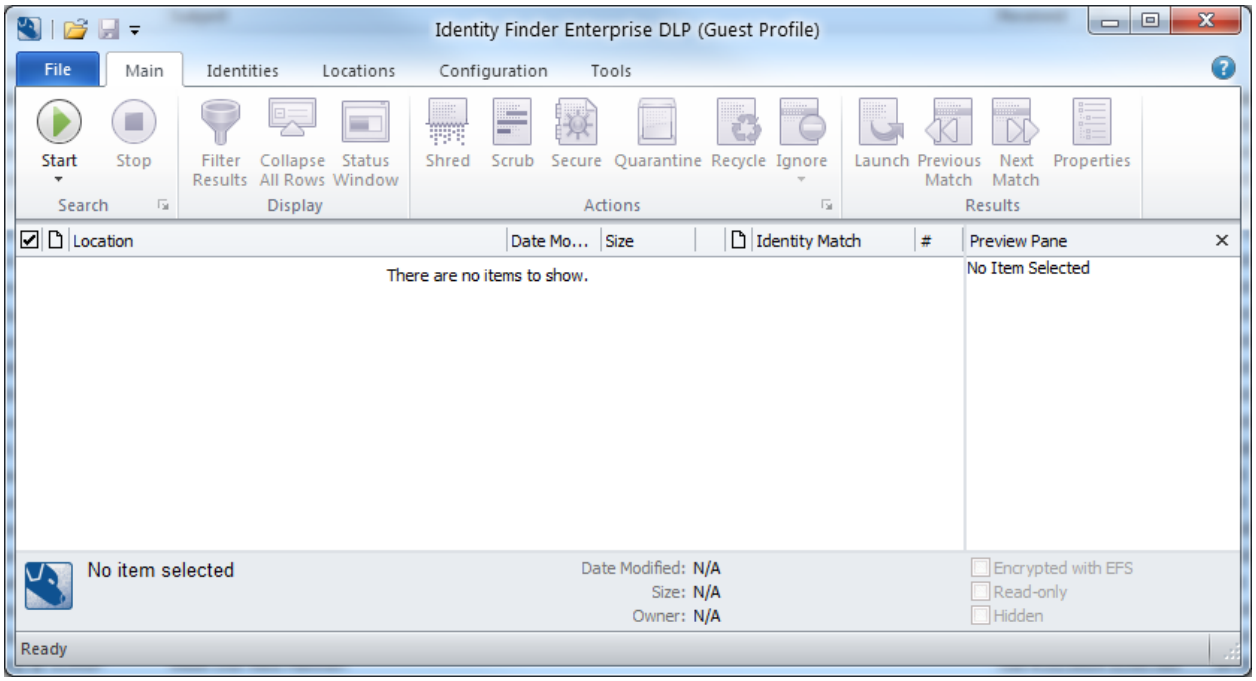
Scanning your computer

To begin a scan, click the Start button. Please note that the scan can produce many false positives.

Examples of false positives:

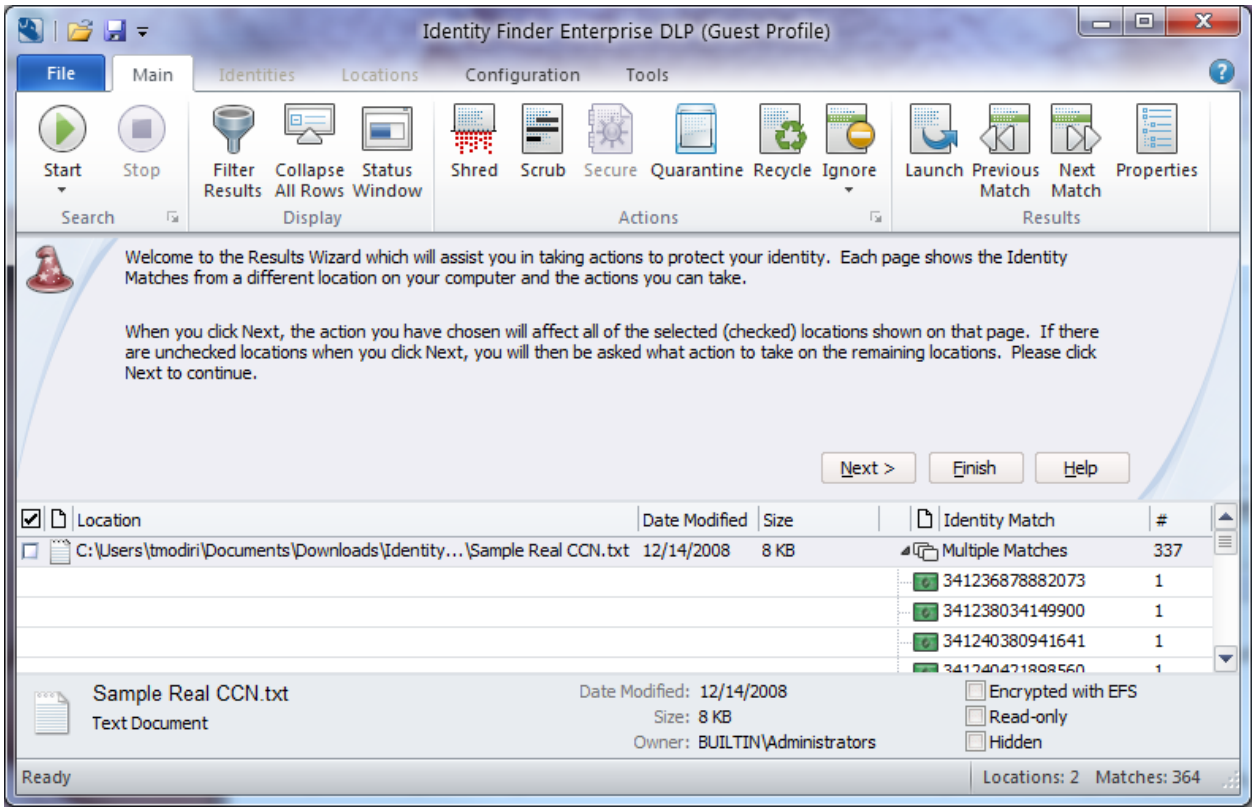
- A file containing the word ‘password’ or ‘username’ in it.
- A file containing abbreviations of keywords, like ‘acct’, which is short for ‘account’. So, a reference in an accounting course to trigger a false positive (i.g. ACCT-3120).
- A training manual on how to handle credit card numbers, containing a made up example number.

If you need assistance in determining if something is a false positive, please contact the Information Security Office (iso@csueastbay.edu).



The first run can take a few hours to complete. Even though the scan will run in the background with low priority not to affect your machine’s performance, we recommend starting your first scan before you leave work in the evening, then press Control-Alt-Delete, and click “Lock this computer” on your way out.

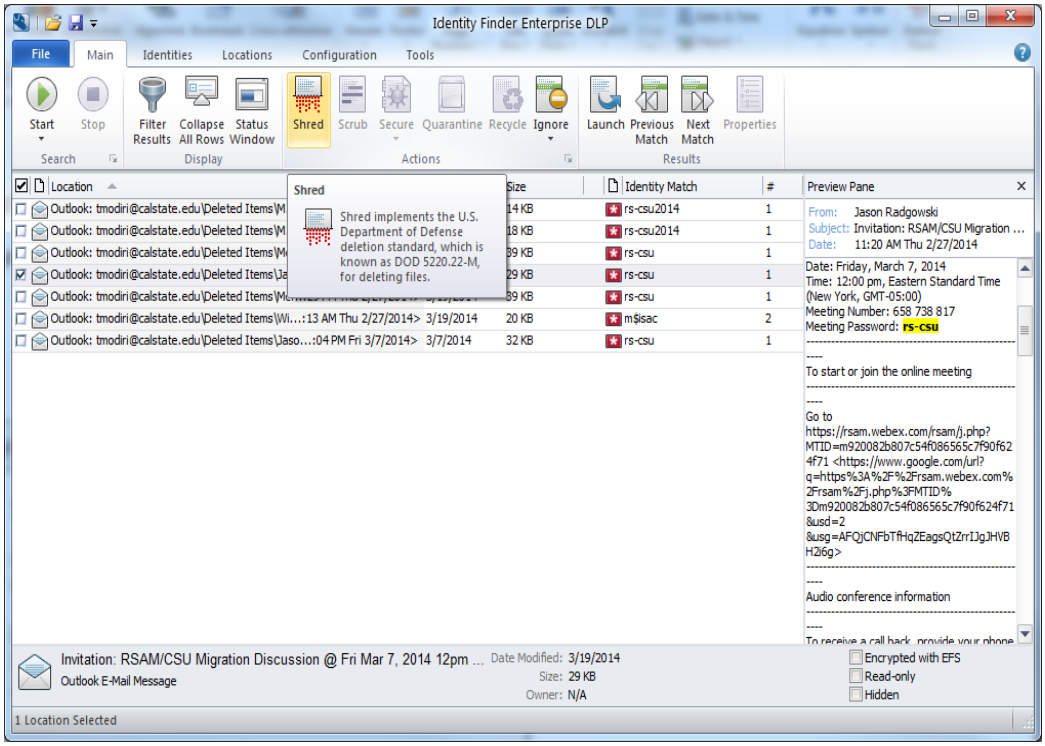
You will be presented with the similar results page below after the scan completes:



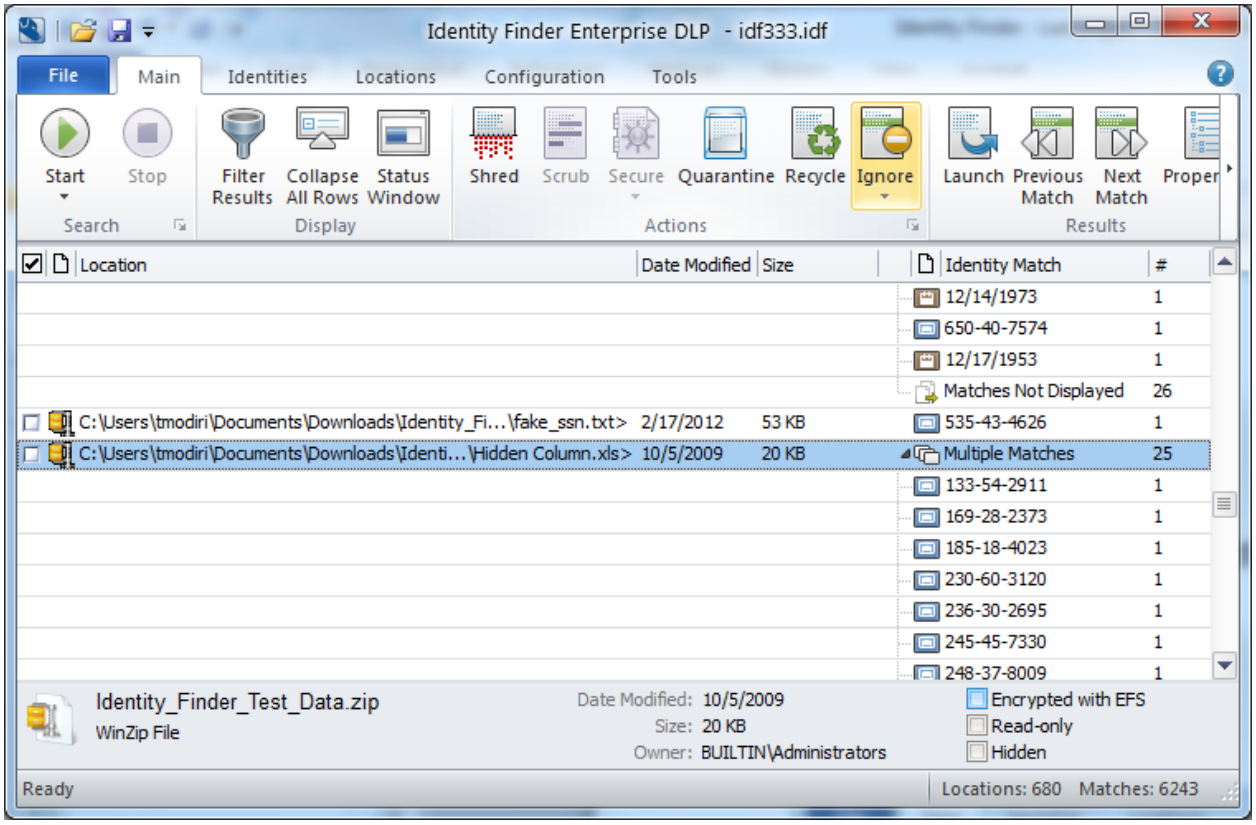
The search result page is where you get to review and remediate your findings and from the File tab, you always want to save the results for future review and to avoid another full scan next time you initiate a search.

Remediating discovered PII or Sensitive Data

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



Ignoring PII or Sensitive Data



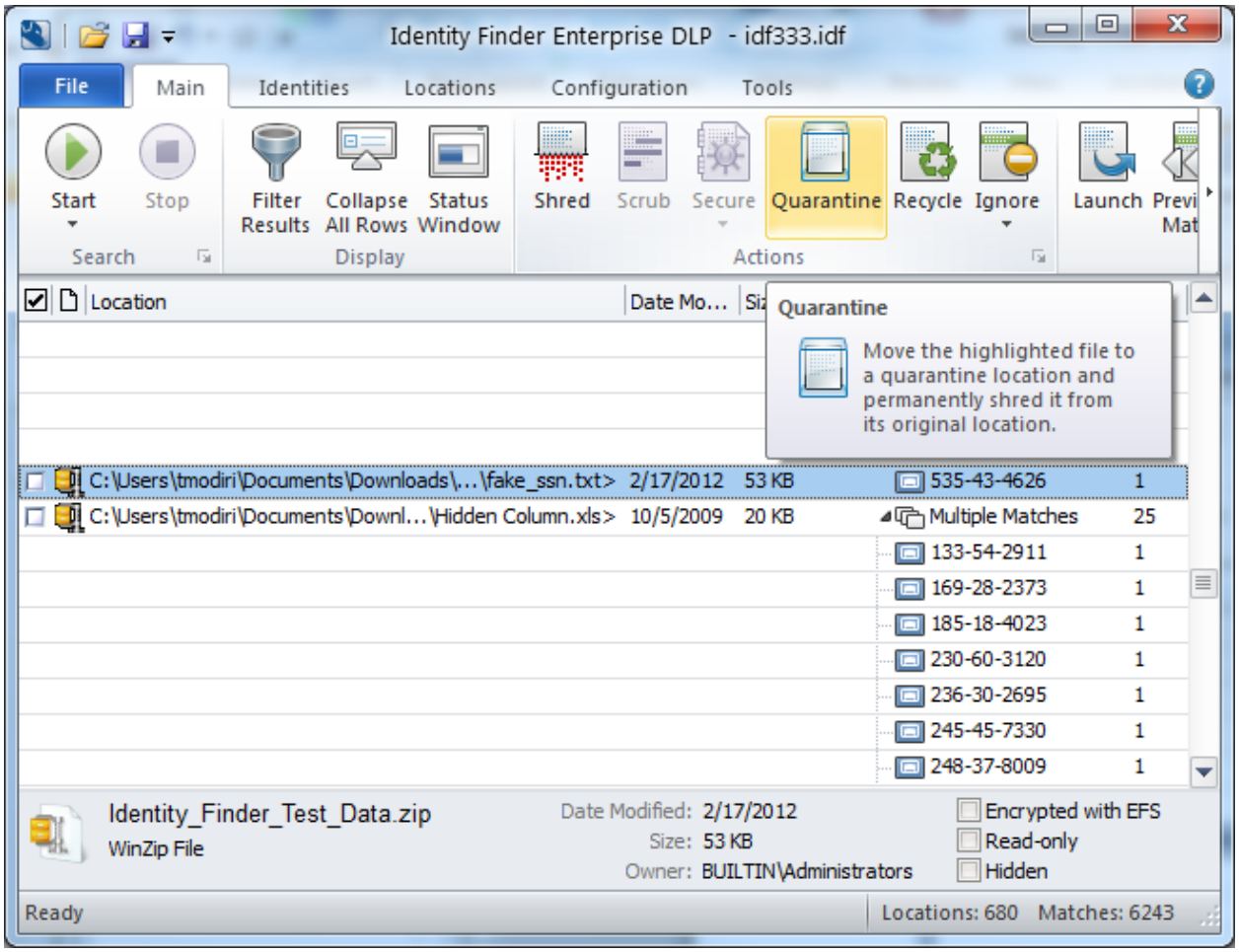
The Ignore option should be utilized when a false positive result is found. A false positive is when Identity Finder marks a file as PII, when it is really not. An example is when Identity Finder picks up a campus 9 digit employee id as a social security number.

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

Quarantining PII or Sensitive Data



The Quarantine function allows you to move your PII data to another location. Though this may seem alluring, this feature is only beneficial if you plan to secure this location. Remember, the goal is to protect all PII data on local machine. This feature would be most effective if you plan to move the data to a secured perhaps departmental file server.

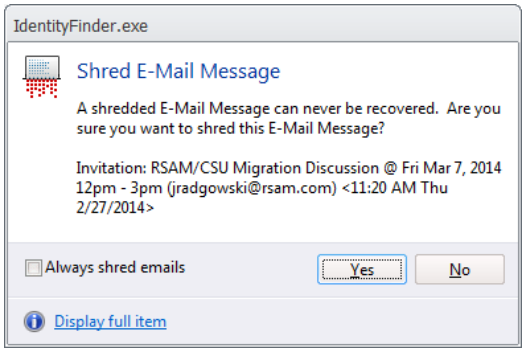
Shredding PII or Sensitive Data

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.

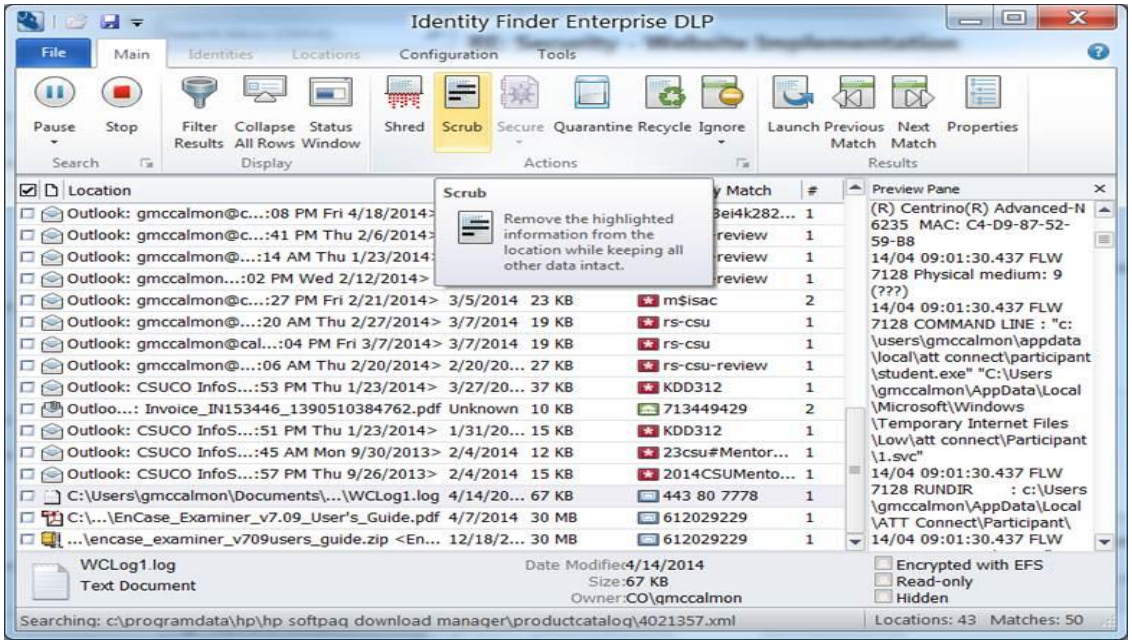
There are three ways to Shred:

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.

Scrubbing or Redacting PII or Sensitive Data



This option should be used when the file found is still needed but the PII part of the file is not. If you wish to keep the found item but remove the personal information only, you should utilize the Scrub feature. Scrub should be selected when you no longer need the personal information but want to keep the original item. This feature is also known as Redact.

Note: Scrub is only available for specific file types searched via the Files search and is not available for email or other Search Locations.

You may only scrub Office 2007 and higher files (that is, *.docx, *.xlsx, *.pptx) and text files (*.txt, *.log, *.ini)

There are two ways to *Scrub* a location:
1. Click the result with the left mouse button to highlight it and click the **Scrub** button.
2. Click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click **Scrub**.

Reset Profile Password

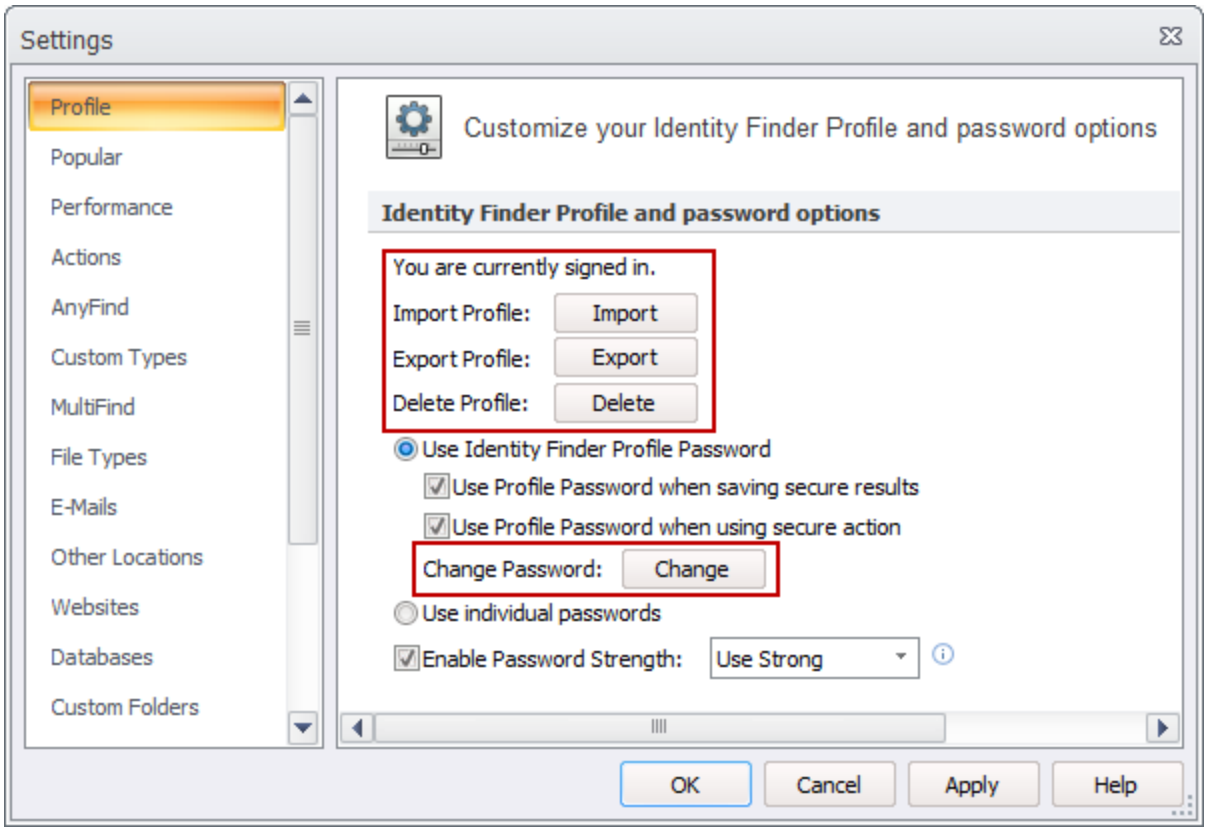
The Identity Finder client application provides the ability to save settings, configuration information, and sensitive data across sessions through the use of a profile password**.** **It is not possible to recover a lost password; however, it is possible to delete a profile and create a new one.** When 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.



More Information

If you have questions about this guide, please contact the Information Security Office via email at iso@csueastbay.edu.

Open new tickets: Call the ITS Service Desk at (510) 885-4357 or email servicedesk@csueastbay.edu

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